Dominion SX II

Administrators Guide

v2.4.0

DSX2-v2.4.0-0E-E
April 2021
255-60-0005-00

What's New in Dominion SX II v2.4.0

The following sections have changed or information has been added to the SX II User Guide based on enhancements and changes to the equipment and/or user documentation.

- SSH certificate authentication:
  - ***Add SSH Client Certificates for Users*** (on page 81)
  - ***Enable SSH Access (Optional)*** (on page 104)
- Custom Ciphers: ***Configure Encryption & Share*** (on page 156)
- Encrypted discovery port: ***Change the TCP Discovery Port*** (on page 107)
- Support for ***802.1X Security*** (on page 113)
- New port configuration options for Port Detection: ***Configure Ports from the Remote Console*** (on page 143)
- Enabling Force HTTPS for Web Access
- ***Host Allowlist*** (on page 160)
- ***Certificate and Smart Card Authentication*** (on page 168)
- Encrypted Backup and Restore: ***Backup and Restore*** (on page 184)
- ***Browser Tips for HSC*** (on page 51)
- ***TLS Ciphers for Web Access*** (on page 167)

Please see the Release Notes for a more detailed explanation of the changes applied to this version of the SX II.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は, クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.

Contents

CS03 Certification - DSX2-16 and DSX2-48

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor.
- When using a backup UPS, power the computer, monitor and appliance off the supply.

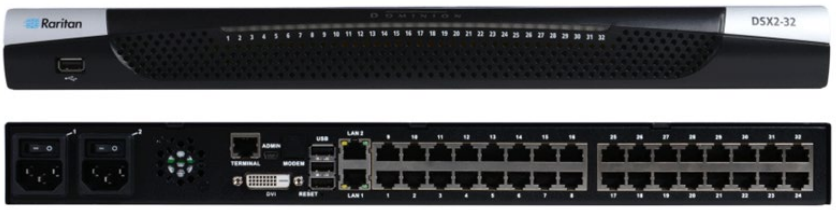
NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation IC, before the registration number, signifies that registration was performed based on a Declaration of Conformity, indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 01. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

AVIS : Le présent matériel est conforme aux spécifications techniques d’Industrie Canadaapplicables au matériel terminal. Cette conformité est confirmée par le numérod'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie quel’enregistrement s’est effectué conformément à une déclaration de conformité et indique queles spécifications techniques d'Industrie Canada ont été respectées. Il n’implique pasqu’Industrie Canada a approuvé le matériel.

AVIS : L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 01. L'IESassigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent êtreraccordés à une interface téléphonique. La terminaison d'une interface peut consister en unecombinaison quelconque de dispositifs, à la seule condition que la somme d'indicesd'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Chapter 1 Features and Benefits



Next-Generation Console Server	
Raritan's Next-Generation Serial Console Server	The Dominion SX II is Raritan's next-generation Serial Console Server (also known as Terminal Server) that provides IT and network administrators secure IP access and control of serial devices, anytime, anywhere. The new SX II is the most powerful, secure, reliable, easy-to-use and manageable serial-over-IP console server on the market. SX II provides convenient and productive access to networking devices, servers, PDUs, telecommunications and other serial devices.
Ten Years of Serial Console Experience	For over ten years, thousands of customers have relied on the first generation Dominion SX for access and control of hundreds of thousands of serial devices, representing over 500 million hours of total operation. The SX II builds upon that experience with a wide range of advancements and innovations.
Dominion Platform, User Interface and Management	Starting with a powerful, Dominion hardware platform providing performance, reliability and security, the SX II includes virtually all the Serial-over-IP features of its predecessor, Dominion compatible user interfaces and management features, plus exciting new capabilities.
Full CLI-based Configuration and Auto-Configuration	The SX II offers complete CLI access and management via SSH, Telnet and web-based user interface, with convenient direct port access. Two script-based automatic configuration methods are available for a fast installation and for subsequent configuration changes.
Exciting New Features and Innovations	The SX II new features include: military grade security features with 256-bit AES encryption and FIPS encryption mode, automatic DTE/DCE serial port detection, innovative at-the-rack access options, wireless modem support, IPv6 networking, script based auto-configuration and Dominion compatible user interfaces and management.
CommandCenter Management & Scalability	With Raritan's CommandCenter, organizations can manage hundreds or even thousands of serial devices, spread across multiple locations, including branch offices.
Powerful Hardware Platform	

Powerful New Hardware Platform	Powerful new hardware platform with 1GHz CPU engine, with an 8-fold increase in RAM. Increased flash memory, up to 8 GB, for storage and logging. Front panel LED's show port connection status.
Wide Variety of 1U Models	Rackable, 1U models available in 4, 8, 16, 32 and 48 ports. All have dual power supplies and dual Gigabit Ethernet LAN ports. Models are available with an optional built-in modem. At-the-rack access includes RJ-45/serial, USB and KVM console.
Powerful Serial Processing Engine	The Dominion SX II with its powerful hardware platform provides high-powered serial processing for the most extreme use cases. Up to 10 users can simultaneously connect to a serial device connected to a SX II port. Up to 200 simultaneous user sessions are supported by a given SX II console server. Port configuration time is up to 23 times faster than the original SX. Connection times are over 50 times faster.
Dual AC Power Supplies	All models have dual, 100-240 volt AC, auto-switching power supplies with automatic failover for increased reliability.
Dual DC Powered Models	Dual power and dual LAN, 8, 32 and 48 port DC powered models are available. These models provide the same features, serial access and performance as the AC powered models.
Dual Gigabit Ethernet LAN on all Models	Dual gigabit Ethernet LAN ports, which can be configured for simultaneous operation or automatic failover. Dual stack IPv4 and IPv6 networking.
Five USB Ports	The Dominion SX II has four USB 2.0 ports, three on the back panel and one on the front panel. These are available for local keyboard/mouse, 3G/4G cellular modem and for automatic configuration via USB drive. A USB 2.0 mini-B port is available for local laptop connection.
Optional Telephone Modem	All models have the option for an internal, 56K telephone modem with RJ11 connection for emergency access and disaster recovery.
Innovative Local Console	The Dominion SX II's local console provides multiple ways for at-the-rack access. The console includes a traditional RJ45 serial port, USB mini-B port, and even a DVI/USB KVM console.
Productive Serial-over-IP Access	

Widest Variety of Serial-over-IP Access	The Dominion SX II supports the widest variety of serial-over-IP connections via SSH/Telnet Clients, web-browser, CommandCenter, telephony modem, cellular modem and at-the-rack access. This includes CLI, GUI and multiple Direct Port Access methods.
SSH/Telnet Client Access	SSH/Telnet client access from a desktop, laptop, or handheld device. Direct Port Access via SSH Client using a username/port string syntax. Customer can upload, view and delete SSH keys for greater security.
Web Browser Access	Web browser access via Dominion SX II or CommandCenter user interfaces and the Raritan Serial Client (RSC).
Convenient Direct Port Access	Convenient Direct Port Access methods via SSH, Telnet & HTTP. IP address and TCP port-based access for Telnet and SSHv2 clients. Independent IP addresses or TCP port numbers can be assigned to access each SX II port. HTTPS-based direct access via URL. Com Port Redirection can be supported for third-party software redirectors.
Cellular and Telephone Modem Access	Optional external Cellular (3G/4G) modem and internal Telephone modem access for emergency access, business continuity and disaster recovery.
Innovative At-the-Rack Access	With the Dominion SX II, you get multiple types of local access at-the-rack. This includes: (1) Traditional RJ45 serial port, (2) Mini-USB port for laptop connection, and (3) DVI & USB-based KVM console for connection to a rackmount keyboard tray or even a KVM switch.
Port Keyword Monitoring and Alerting	Users can define up to 14 keywords per port. The SX II will scan the data coming from the port, and if one of the keywords is detected, it will send an alert via SNMP or e-mail. Serial devices are monitored, even when no user is connected! This results in faster notification that reduces Mean Time to Repair (MTTR).
Port Logging to Syslog, NFS and Local File	Port activity to and from serial devices can be logged to a Syslog server, Network File System (NFS) server or locally to the SX II device with up to 8 Gb of storage.
NFS Logging Features	Allows logging of all user keystrokes and server/device responses to NFS server(s). Can even be stored on the NFS server with user-defined encryption keys for greater security. Keep-alive messages in the NFS log allow easy monitoring if the managed server/device goes down.
SecureChat Instant Messaging	Allows for secure, instant messaging among SX II users. Enables collaboration of distributed users to increase their productivity, troubleshoot, reduce the time to resolve problems and for training purposes.
Automatic Serial Device Logoff	Once a user is timed out for inactivity, a user defined "logoff" command can be sent to the target. Improved security of user sessions results as serial sessions are automatically closed upon time out and not left open for possible un-authorized access.
Comprehensive Serial Device Access	

Over Ten Years of Serial Device Management	The first generation Dominion SX has been serving customers for over ten years, with over 500,000 ports sold. This represents hundreds of millions of hours of operation across a wide variety of serial devices.
Automatic DTE/DCE Serial Port Detection	This feature allows for a straight Cat5 connections to Cisco equipment (and other compatible devices), without rollover cables. It also means that a SX II can replace the first generation SX with its existing serial device connections.
Support for the Widest Variety of Serial Devices	Supports the widest variety of serial equipment including: networking routers, Ethernet switches, firewalls, UNIX/LINUX servers, Windows Servers, virtual hosts, rack PDU's, UPS systems, telecom/wireless gear. Supports multiple operating systems including SUN® Solaris, HP-UX, AIX, Linux®, Windows® Server 2012, and UNIX®.
Up to 230,400 Baud Serial Connections	Supports operating speeds of 1,200 to 230,400 bits-per-second for serial connections.
Flexible Serial Port Options	Flexible per-port serial options, including BPS, emulation, encoding, parity, flow control, stop bits, character and line delays, always-active connections and more. Can define an exit command when the user times out, as well as enable an in-line menu for port commands and power control.
VT100/220/320/ANSI support	Increased choice of terminal emulation options, allows support of a broader range of devices. SX II supports the following code-sets: US-ASCII (ISO 646); ISO 8859-1 (Latin-1); ISO 8859-15 (Latin-9); UTF-8 and others.
Remote Power Control of Raritan PDU's (With Power Control Menu)	Raritan rack PDU's (PX, PX2, PX3, RPC) can be connected to the Dominion SX II for remote power control of the equipment connected to the PDU. Remote power control can be done via the SX II GUI, SSH/Telnet Client or CommandCenter. Outlet associations can be created for serial devices with multiple power supplies, such that these outlets can be controlled with a single power command. The SX II has "Control P" style menu commands for power control available during a serial session.
Security - Encryption	

Strong 256 Bit AES Encryption	The SX II utilizes the Advanced Encryption Standard (AES) encryption for added security. 128- and 256-bit AES encryption is available. AES is a U.S. government-approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.
Validated FIPS 140-2 Cryptographic Module	For government, military and other high security applications, the Dominion SX II utilizes a validated FIPS 140-2 Cryptographic Module for enhanced encryption. Modules tested and validated as conforming to FIPS 140-2 are accepted by federal agencies of the U.S. and Canada for the protection of sensitive information.
Enhanced Encryption Options	Support more encryption options: web-browser security through 256 and 128-bit SSL encryption; for SSHv2 connections, AES and 3DES are supported (client-dependent).
Security - Authentication	
External authentication with LDAP, Radius, TACACS & Active Directory	Dominion SX II integrates with industry-standard directory servers, such as Microsoft Active Directory, using the LDAP, RADIUS and TACACS protocols. This allows Dominion SX II to use pre-existing username/password databases for security and convenience. SecureID is supported via RADIUS for added security.
Upload Customer-Provided SSL Certificates	Customers can upload to the Dominion SX II digital certificates (self-signed or certificate authority provided) for enhanced authentication and secure communication.
Configurable Strong Password Checking	The Dominion SX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.
Configurable Security Banner	For government, military and other security-conscious customers requiring a security message before user login, the SX II can display a user-configurable banner message and require acceptance before user login.
SSH Client Certificate Authentication	In addition to authentication via login/password, on the SSH interface users can be authenticated via SSH certificates. Each local user can be assigned up to 10 SSH keys. The key authentication takes the place of the login/password
Local Authentication with Users, Groups and Permissions	In addition to external authentication, the Dominion SX II supports local authentication. Administrators can define users and groups with customizable administration and port access permissions.
Login and Password Security	The SX II includes multiple login and password security features including password aging, idle timeout, user blocking and login limitations. Failed login attempts can be result in lockouts and user deactivation.
SHA-2 Certificate Support	Support for the more secure SHA-2 certificates.

Security - Networking	
Dual Stack IP Networking – IPv4 and IPv6	The Dominion SX II provides dual-stack IP networking with simultaneous support of IPv4 and IPv6.
IPTables Firewall support	Fully configurable "iptables" firewall support. User selectable and customizable system security levels catering to wide range of security needs.
Selective Static Routing Support	Supports connections between modem and LAN 1, modem and LAN 2 or LAN 1 and LAN 2. This allows users to utilize two different networks (Public and Private) and modem access to KVM or Ethernet controlled devices. When used with the firewall function, secure access can be enabled.
TCP/IP Port Management	Can disable TELNET and SSH access if desired. Ability to change these ports in addition to HTTP, HTTPS and discovery ports
Prevent Man In The Middle Attacks	Enhanced security of communication channels by using client and server SSL certificates.
Modem Dial-Back Security	For enhanced security, Dominion SX supports modem dial-back.
Rejects SSHv1 Requests	Due to the many known security vulnerabilities of the SSHv1 protocol, the Dominion SX will automatically reject SSHv1 connections.
End User Experience	
Multiple User Interfaces	The SX II supports multiple user interfaces giving the user the freedom to use the interface best suited for the job at hand. This includes remote access via Raritan or third party serial client via CLI, Raritan graphical user interface (GUI), Admin-only GUI, at-the-rack access or via CommandCenter. Convenient direct port access methods available.
Full Modern CLI – GUI Equivalence	Full CLI management and configuration, thereby allowing scripting of any command.
Broad Range of Supported Browsers	Offers broad range of browsers: Firefox, Safari, Internet Explorer, Chrome, Edge.
International Language Support	The web-based user interface supports English, Japanese and Chinese languages. The Raritan Serial Console can support four languages: English, Japanese, Korean and Chinese
PC Share Mode	Up to ten users can connect and remotely access each connected serial device up to a maximum of 200 serial sessions. Sharing feature is very useful for collaboration, troubleshooting and training.
Easy to Install and Manage	

Full CLI-based Configuration and Management	The SX II offers complete CLI administration and management via SSH, Telnet and web-based user interface. Two script-based automatic configuration methods are available for a fast installation and for subsequent configuration changes.
Automatic Configuration via USB Drive	The SX II can be optionally configured via a CLI script on a USB drive connected to one of its USB ports. This can be used for initial configuration or subsequent updates.
Automatic Configuration via TFTP Server	The SX II can be optionally configured via a second method, i.e. via a CLI script contained in a TFTP server. This can be used for initial configuration or subsequent updates. The TFTP server address can be retrieved via DHCP or set by the administrator.
Dominion-Compatible Management	Dominion-compatible management features are available via a web-based user interface or CLI. This includes Dominion-style User Management, Device Settings, Security, Maintenance, Diagnostic and Help features. Firmware update via web browser without the use of an FTP server.
Easy to Install	Installation in minutes, with just a web browser, CLI or automatic configuration. Some competitive products require burdensome editing of multiple files to complete a basic installation.
Configurable Event Management and Logging	The SX II generates a large variety of device and user events including: device operation, device management changes, security, user activity and user administration. These can be selectively delivered to: SNMP, Syslog, email (SMTP) as well as stored on the SX II in the audit log. Support for SNMP v2 and v3,
Raritan CommandCenter® Management and Scalability	

Raritan's CommandCenter Centralized Management	Like the rest of the Dominion series, Dominion SX II features complete CommandCenter Secure Gateway integration, allowing users to consolidate all Dominion SX II and other Raritan devices into a single logical system, accessible from a single IP address, and under a single remote management interface.
Manage Hundreds of Serial Devices	When deployed with CommandCenter Secure Gateway, hundreds of Dominion SX II devices (and thousands of serial devices) can be centrally accessed and managed.
Single IP Address for Administration and Device Connection	Administrators and users can connect to a single IP address via CommandCenter Secure Gateway to manage the SX II or access the attached serial devices. This connection can be via web browser or through SSH. Option for SX II at-the-rack access while under CC-SG management.
Bulk Firmware Upgrades	Administrators can schedule firmware upgrades (and other operations) for multiple SX II devices from CommandCenter.
Remote Power Control via CommandCenter Secure Gateway	CommandCenter supports remote power control of Raritan PX rack PDU's connected to serial ports on the Dominion SX II. For equipment with multiple power feeds, multiple power outlets can be associated together to switch equipment on or off with a single click of the mouse.

In This Chapter

Package Contents

Each SX II ships as a fully-configured stand-alone product in a standard 1U 19" rackmount chassis.

The SX II package includes -

- 1 - SX II appliance
- 1 - Rackmount kit
- 2 - AC power cords
- 1 - Set of 4 rubber feet (for desktop use)
- 1 - Warranty card
- 1 - SX II Quick Setup Guide

SX II Models

The following SX II models are available.

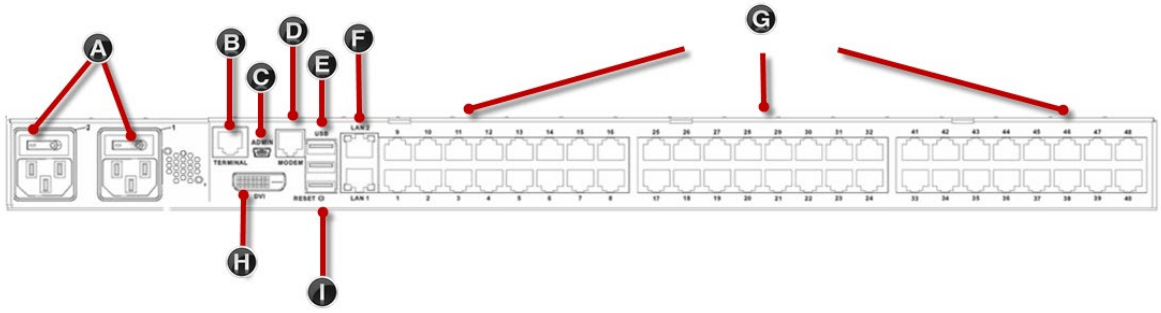
Models with an **M** include an internal modem in addition to the standard features that are provided on all SX II models. For a list of standard features, see ***Features and Benefits*** (on page 1).

- DSX2-4 and DSX2-4M - 4-port serial console server
- DSX2-8 and DSX2-8M - 8-port serial console server
- DSX2-16 and DSX2-16M - 16-port serial console server
- DSX2-32 and DSX2-32M - 32-port serial console server
- DSX2-48 and DSX2-48M - 48-port serial console server

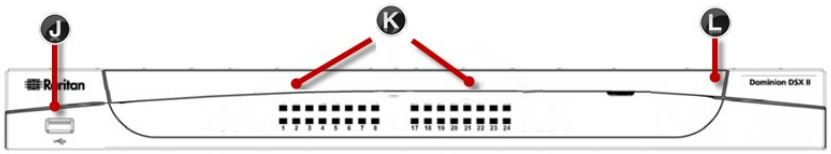
Model size, weight, temperature and other specifications are found in ***SX II Dimensions and Physical Specifications*** (on page 240).

SX II Appliance Diagram

Note the image shown here is an example, so it may be different from your model.



Appliance diagram key	
A	AC power outlet(s) 1 and 2 with independent power on/off switches
B	Terminal port/console port
C	Admin Mini-USB port
D	Modem port (based on model)
E	3 USB ports
F	LAN1 and LAN2 ports
G	Server ports
H	DVI-D port
I	Reset button



Appliance diagram key	
J	USB port
K	LED port indicators
L	Power status (Note SX II 48 port models have their power status located above the front-panel USB port.)

Supported Serial Devices

- Routers
- LAN switches
- Rack PDUs
- Wireless modems
- Telecom modems
- Windows servers
- UNIX servers
- Linux servers
- Virtual hosts
- Firewalls

SX II Access Clients

HTML Serial Client (HSC)

HSC is the default client and will launch when you connect to a serial device. The HSC is an HTML-based, Java-free Serial Client.

See ***HTML Serial Console (HSC) Help*** (on page 41)

Standalone Raritan Serial Console (RSC) (RSC)

RSC is the standalone Java-based client. RSC was the default client in releases earlier than 2.1. You can download standalone RSC by connecting to **<SX II IP Address>/rscs**

See Raritan Serial Console (RSC) Help

Direct Port Access

Direct Port Access allows users to bypass having to use the SX II's Login dialog and Port Access page.

This feature also provides the ability to enter a username and password directly to proceed to the target, if the username and password is not contained in the URL.

Command Line Interface (CLI)

Connect using CLI via SSH or Telnet.

See Command Line Interface Help for SX II

Admin-Only Interface

Access the Admin Client at: https://<SX2 IP/Hostname>/admin.

The Admin Client does not allow target access. Use the Admin Client to perform administrator functions without using Java.

All admin functions available in the Remote Console are available in the Admin-Only Interface.

iOS Support

SX II supports iOS SSH apps, both with and without VPN, to allow users access via iOS mobile devices.

See ***Access SX II Using an iOS Device*** (on page 27)

Chapter 2 Configure SX II for the First Time

SX II can be configured from the Remote Console or command line interface (CLI).

In This Chapter

Default Login Information

SX II appliances are shipped with the following defaults. Use the defaults when you initially access SX II.

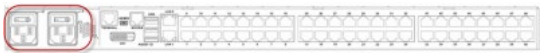
- IP address - `192.168.0.192`
- IP netmask - `255.255.255.0`
- Username - `admin` (all lowercase)
- Password - `raritan` (all lowercase)

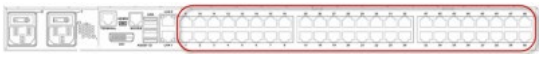
Important: For backup and business continuity purposes, it is strongly recommended you create a backup administrator username and password. Keep the information in a secure location.

Initial SX II Configuration from the Remote Console

1. After you have installed the SX II at the rack, connect the power cord(s) between the power connector on the SX II and an external, AC or DC power source (depending on your model).
2. You can connect the second power connector to a backup power source.

   Use the power cords that came with SX II.

   
3. Connect an external modem to a USB port on the SX2 (optional). See ***Connect and Enable Global Access to an External USB-Connected Broadband Modem*** (on page 132)Online Help
4. Connect your target devices or other serially managed devices to the server ports on the SX II.

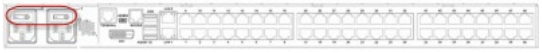
   Use a standard Cat5 cable to connect your target device to an available port on the back of SX II.

   Note: Check the pin definition of the RJ45 port on the target. It should match the pin definition on SX II.

Or

If needed, connect a Raritan Nulling Serial Adapter to the serial port on your target, then plug a standard Cat5 cable into the adapter. Connect the other end of the cable to an available port on the back of SX II.

5. Flip the power switch(s) to turn SX II on.



Next, connect SX II to your network and configure your network settings for the first time.

See ***Initial SX II Configuration Using Command Line Interface (Optional)*** (on page 13) or Configure SX II Network Settings from the Remote Console.

Connect a Laptop to SX II Using a Cross-Over Cable (Optional)

The first time you configure SX II, if you are connecting from the LAN port on laptop to the LAN1 port on SX II using a crossover cable, do the following -

1. Use cross-over cable to connect between SX II LAN1 and the laptop LAN port.
2. Set the Static IP of the LAN port that is connected to SX II to `192.168.0.191` and Network Mask to `255.255.255.0`.
3. Launch your browser and access SX II via `192.168.0.192`.

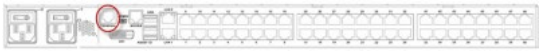
Initial SX II Configuration Using Command Line Interface (Optional)

Ensure that the port settings (serial communication parameters) are configured as follows:

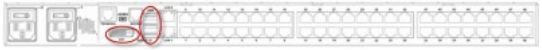
- Bits per Second (BPS) = 115200
- Data bits = 8
- Parity = None
- Stop bits =1
- Flow Control = None

To configure SX II for the first time using CLI:

1. Connect to SX II using any one of the following -
   - Connect a computer to the Terminal port for serial console access.



   - Connect a keyboard tray or KVM console to the DVI-D and USB ports.



   - Connect a laptop to the MiniUSB Admin port.

2. The emulator interface opens once you are connected to SX II. Press the Enter key on your keyboard.
3. When the `Login` prompt appears, enter the default username `admin` and password `raritan`. Use all lowercase letters.
4. You are prompted to change the default password. When creating a password via CLI, it cannot begin with a space or end with a space. This does not apply to creating passwords in using the Remote Console.

   By default, the network is configured for a static IP address.
5. At the `admin >` prompt, enter `config` and at the next prompt enter `network`.
6. At the `admin > config > network >` prompt, enter `interface if lan1 ipauto none ip <ip address> mask <mask> gw <gateway ip address>`

   To use DHCP, enter `interface if lan1 ipauto dhcp`
7. Give the device a name to help identify it.

   Enter "`name devicename <DSX2 name>`".

   Up to 32 characters are supported for the name. Spaces and special characters not supported.
8. At the `admin > config > network` prompt, enter `quit` to get into upper menu `admin > config`, then enter `time`.
9. At the `admin > config > time >` prompt, set the date and time on the SX II.
   - Enter `timezonelist` and find the number code that corresponds to your time zone.
   - Enter `clock tz <timezone code> date <date string> time <time string>`

     where `<timezone code>` is the time zone code, `<time string>` is the current time in "HH:MM:SS" format and `<date string>` is the current date in "YYYY-MM-DD" format (quotes included, uses 24-hour time).

     Example: `clock tz 9 date "2015-08-15" time "09:22:33"`
10. Enter `top` to return to the top level prompt.
11. Next, enter `config` and then enter `ports` at the next prompt.

    You can now configure each server port that has a target device connected to it.
12. Enter `config port` then hit `?` to see the port parameters.

    For example:

    ```
    config port 1 name cisco1700 bps 9600 parity odd
    flowcontrol none emulation vt100
    ```

    You can also use port ranges or the wildcard asterisk *, such as `config port * bps 115200`

    This configures all ports for a communications speed of 115200 bps.

Or

`config port 3-7 bps 115200`

This configures ports 3 through 7 for 115200 bps.

Or

`config port 1,2,7-9 bps 115200`

This configures ports 1, 2, 7 through 9 for 115200 bps.

Repeat this step for each port with a device connected to it.

13. When done, enter `top` to return to the top level prompt.

Set Terminal Emulation on a Target

The setting for terminal emulation on SX II is a property associated with the port settings for a particular target device.

Ensure that the settings for terminal emulation in the client application, such as Telnet or SSH, are capable of supporting the target device.

Ensure that the encoding in use on the host matches the encoding configured for the target device.

For example, if the character set on a Sun™ Solaris™ server is set to ISO8859-1, the target device should also be set to ISO8859-1.

Ensure that the terminal emulation on the target host connected to SX II serial port is set to VT100, VT220, VT320 or ANSI.

On most UNIX® systems, `export TERM=vt100` (or `vt220|vt320|ansi`) sets the preferred terminal emulation type on the UNIX target device. So, if the terminal type setting on a HP-UX® server is set to VT100, the Access Client should also be set to VT100.

Set the CLI Escape Sequence

The escape key sequence is user-configurable and can be configured per port.

The escape sequence is programmable per port because different target operating systems and host applications may trap different escape key sequences.

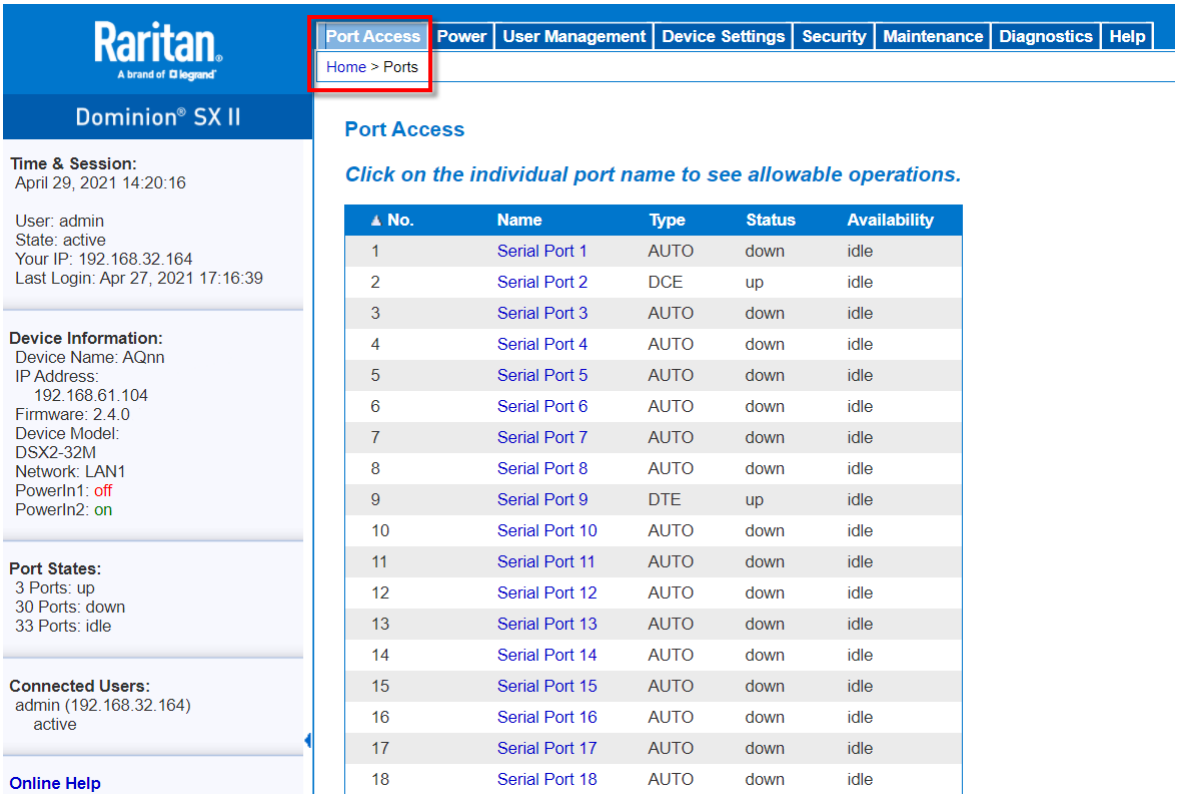
Ensure the default escape sequence set on the SX II server does not conflict with a key sequence required by either the access application or the host operating system.

The console sub-mode should be displayed when the default escape key sequence ^] is pressed.

Raritan recommends that you *do not* use [or Ctrl-[. Either of these may cause unintended commands, such as invoking the Escape Command unintentionally. This key sequence is also triggered by the arrow keys on the keyboard.

Chapter 3 Access and Use Remote Console Features

The Remote Console is a browser-based interface accessed when you log in to SX II via a network connection. See ***Log In to SX II and HSC*** (on page 23)



Administrator Functions in the Remote Console

Administrators perform SX II configuration and maintenance functions from the Remote Console, such as configuring network access, adding and managing users, managing device IP addresses and so on.

Administrators can also use a version of the Remote Console that does not include any target access. See ***Log In to SX II Admin-Only Interface*** (on page 27).

End User Functions in the Remote Console

From the Remote Console, end users access targets, change passwords and so on. End users can choose from two Serial Clients: HTML Serial Client, and Raritan Serial Client. See ***HTML Serial Console (HSC) Help*** (on page 41) and Raritan Serial Console (RSC) Help.

Note that these functions can also be performed via command line interface.

In This Chapter

Allow Pop-Ups

Regardless of the browser you are using, you must allow pop-ups in order to launch the SX II Remote Console.

Installing a Certificate

You may be prompted by the browser to accept and validate the SX II's SSL certificate.

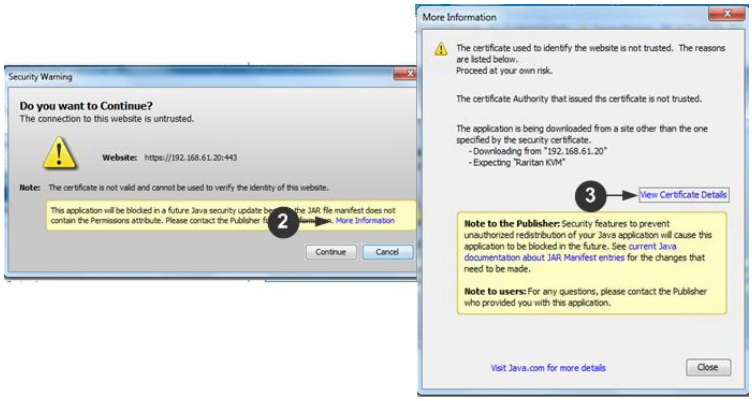
Depending on your browser and security settings, additional security warnings may be displayed when you log in to SX II.

It is necessary to accept these warnings to launch the SX II Remote Console. For more information, see Security Warnings and Validation Messages.

Two sample methods on how to install an SSL Certificate in the browser are provided here. Specific methods and steps depend on your browser and operating system. See your browser and operating system help for details.

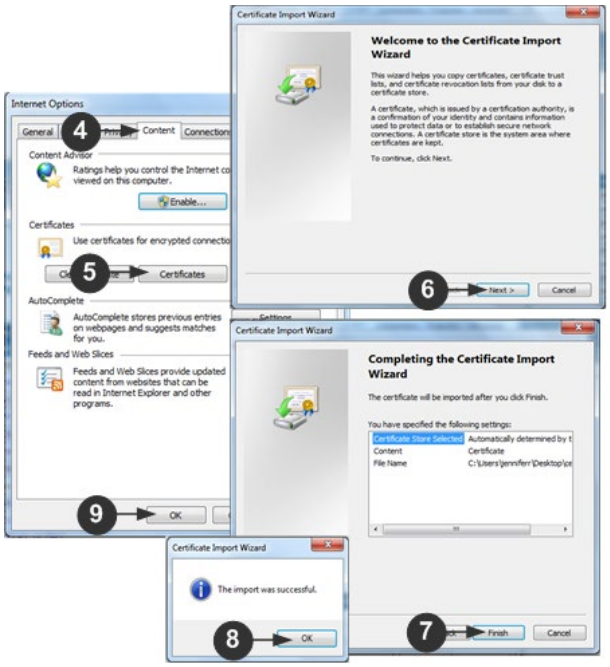
Example 1: Import the Certificate into the Browser

In this example, you import the Certificate into the browser.



1. Open a browser, then log in to SX II.
2. Click More Information on the first warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

Note: If you are not prompted by the browser, manually select the Settings or Options for your browser, and import the certificate. The following example shows the IE > Tools > Internet Options method.



1. Click the Content tab.
2. Click Certificates.

The Certificate Import Wizard opens and walks you through each step.

- File to Import - Browse to locate the Certificate
- Certificate Store - Select the location to store the Certificate

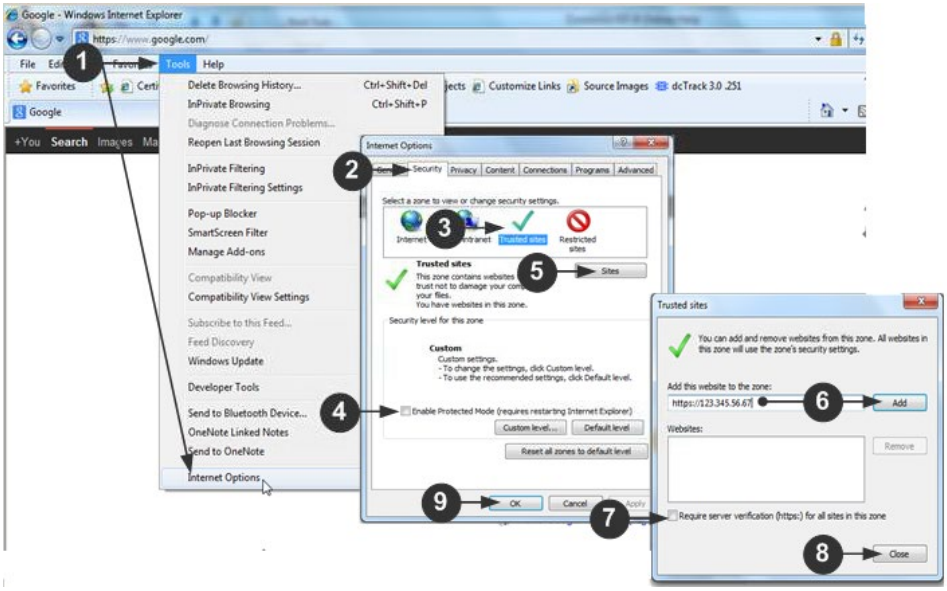
3. Click Finish on the last step of the Wizard.

   The Certificate is imported. Close the success message.

4. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

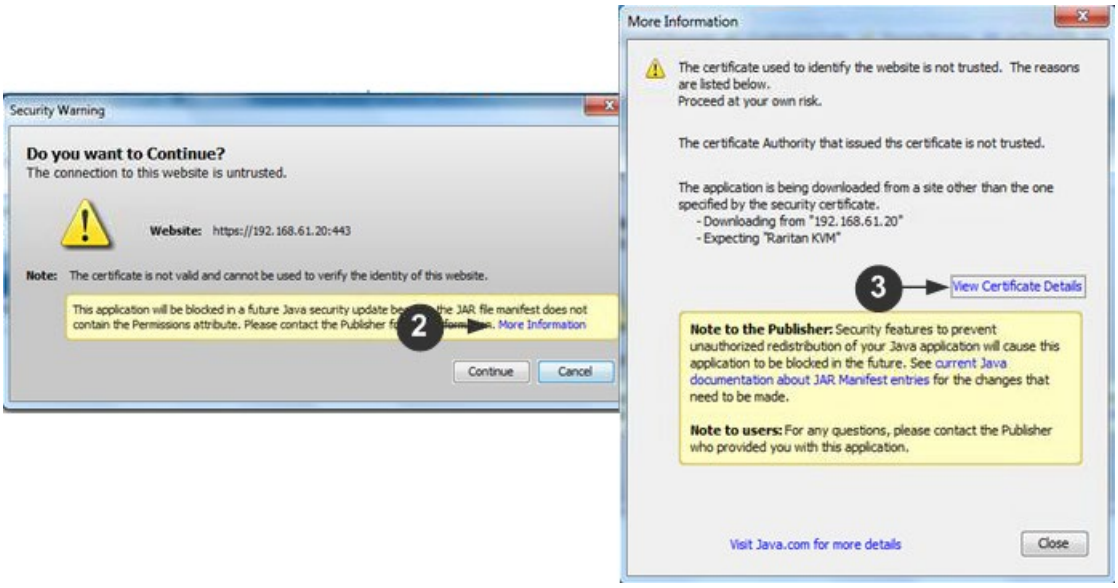
Example 2: Add the SX II to Trusted Sites and Import the Certificate

In this example, the SX II's URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.



1. Open an IE browser, then select Tools > Internet Options to open the Internet Options dialog
2. Click the Security tab.
3. Click on Trusted Sites.
4. Disable Protected Mode, and accept any warnings.
5. Click Sites to open the Trusted Sites dialog.
6. Enter the SX II URL, then click Add.
7. Deselect server verification for the zone (if applicable).
8. Click Close.
9. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Next, import the Certificate.



1. Open an IE browser, then log in to SX II.
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

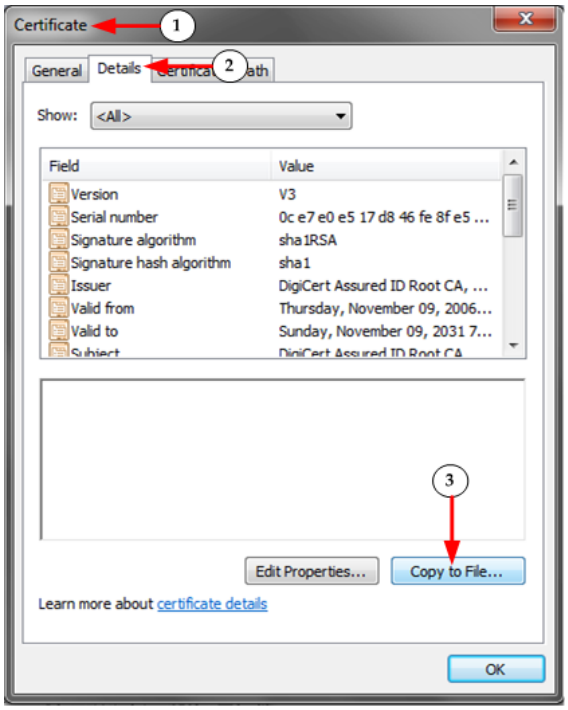
   For details see, ***Example 1: Import the Certificate into the Browser*** (on page 18).

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

SX II requires an SSL certificate in either Base64-Encoded DER format or PEM format.

If you are using an SSL certificate in binary format, you cannot install it.

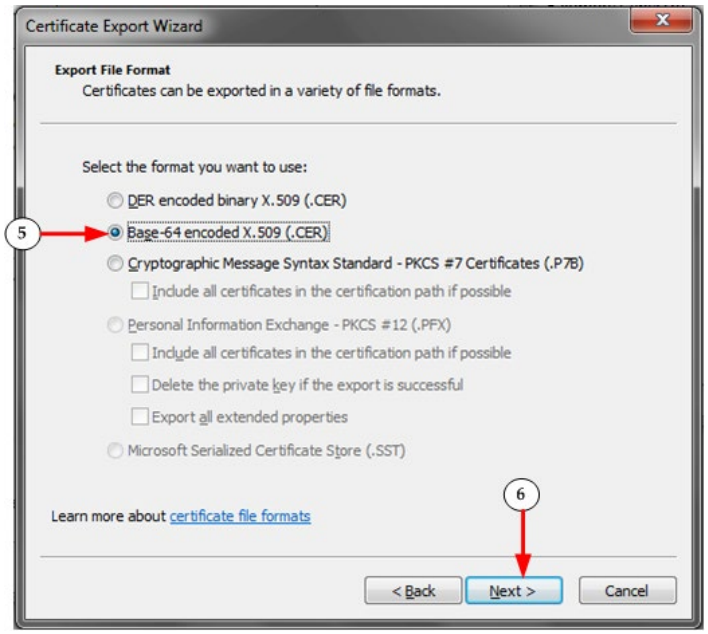
However, you can convert your binary SSL certificate.



1. Locate the DEGHKVM0001.cer binary file on your Windows machine. Double-click on the DEGHKVM0001.cer file to open its Certificate dialog.
2. Click the Detail tab.

3. Click "Copy to File...".

4. The Certificate Export Wizard opens. Click Next to start the Wizard.



5. Select "Base-64 encoded X.509" in the second Wizard dialog.
6. Click Next to save the file as a Base-64 encoded X.509.

You can now install the certificate on your SX II.

Log In to SX II and HSC

This login procedure gives you access to the default HTML Serial Client (HSC) for target connections. If you must use RSC, see ***Log In to SX II and Standalone RSC*** (on page 23).

1. Launch a supported web browser.
2. Enter the SX II HTTP, HTTPS or DNS address provided to you by your Administrator.

   Note: You are always redirected to the IP address from HTTP to HTTPS.
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, accept and/or allow access.

Log In to SX II and Standalone RSC

This login procedure gives you access to the Java-based access client, RSC, which is a downloaded client.

Note: Check the release notes for supported Java versions. If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

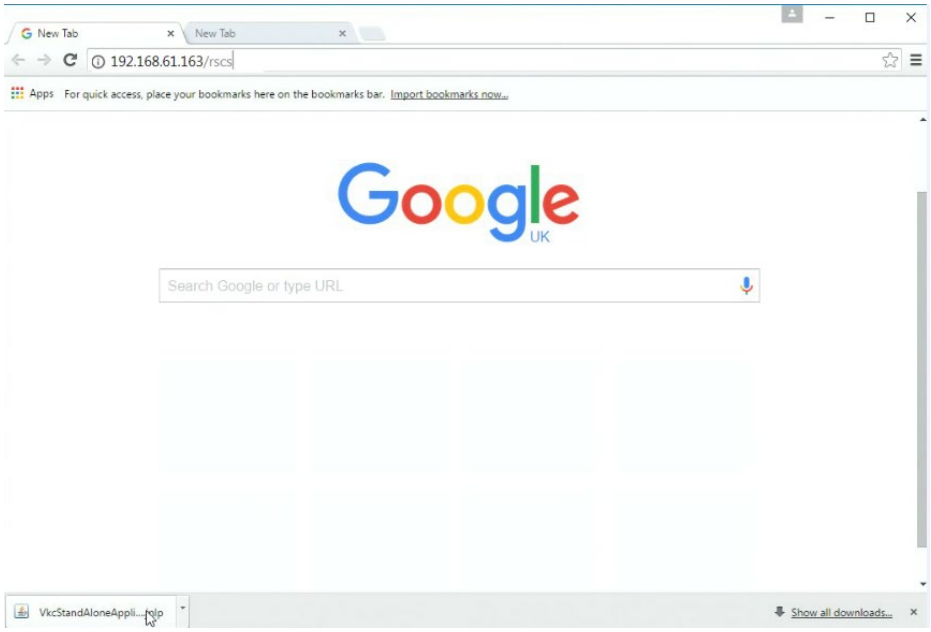
To log in:

1. Launch a supported web browser.
2. Connect to: **https://SX2 IP Address/rscs**
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, accept and/or allow access.

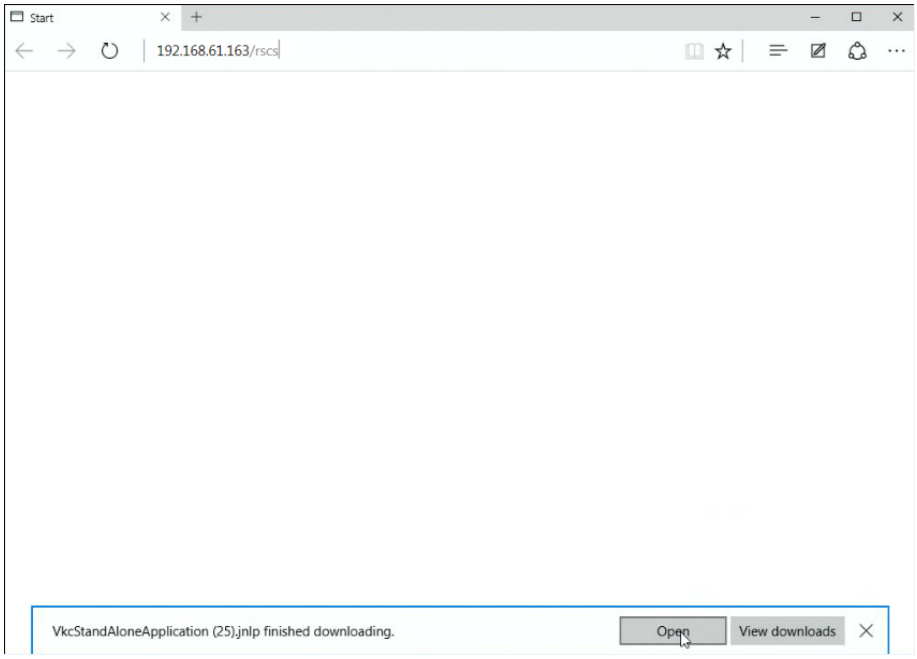
Examples:

For all browsers, the RSCS standalone application needs to be downloaded every time you use it.

- Chrome: The downloaded jnlp file must always be clicked at bottom left corner of browser window to launch. The filename is VKCStandAloneApplication.jnlp.



- Edge: You must click Save, then click Open at the bottom of the browser to launch.



- Internet Explorer: Launches automatically.
- Firefox: Use the option "Do this automatically for files like this from now on", when the jnlp file downloads, and it will launch automatically in future.

Firefox from a Linux PC: Download the RSCS client to a directory on the Linux PC. The filename is VKCStandAloneApplication.jnlp. From a Linux console window, issue the following command to launch the RSCS client from the directory it was saved to: `javaws <VkcStandAloneApplication.jnlp file>`

Security Warnings and Validation Messages

When logging in to SX II, security warnings and application validation messages may appear.

These include -

- Additional security warnings based on your browser and security settings

  See ***Additional Security Warnings*** (on page 26)
- If you choose to use the Raritan Serial Client (RSC/RSCS), you may see Java™ security warnings and requests to validate SX II.

  See ***Java Validation and Access Warning*** (on page 26) and ***Installing a Certificate*** (on page 17).

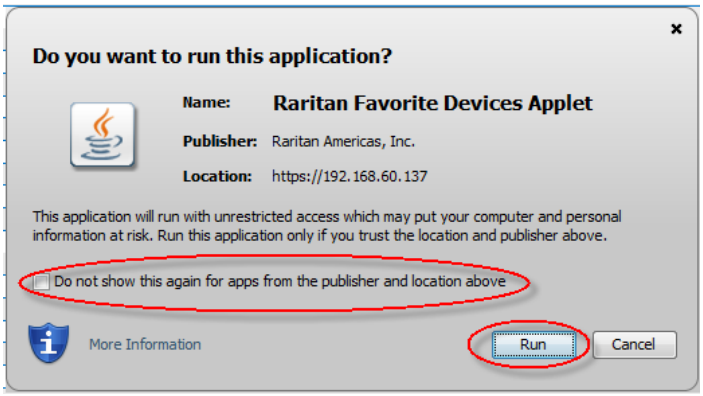
Note! Use the HTML Serial Client (HSC) instead to avoid Java. The HSC is Java-Free. See **Log In to SX II and HSC** *(on page 23).*

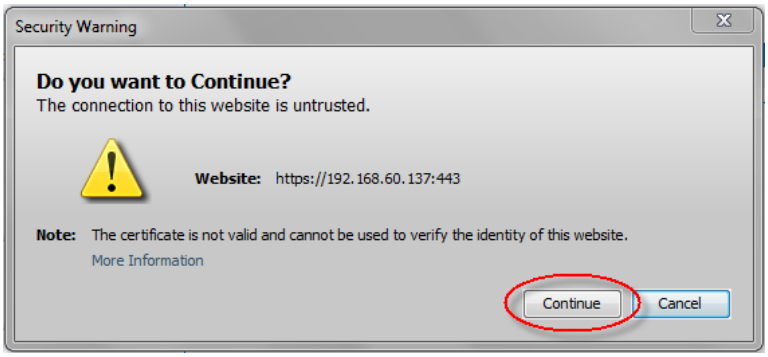
Java Validation and Access Warning

When logging in to SX II using the Java-based client, Java prompts you to validate SX II, and to allow access to the application.

Installing an SSL certificate in each SX II device is recommended to reduce Java warnings, and enhance security.

See ***SSL and TLS Certificates*** (on page 162)





Additional Security Warnings

Even after an SSL certificate is installed in the SX II, depending on your browser and security settings, additional security warnings may be displayed when you log in to SX II.

It is necessary to accept these warnings to launch the SX II Remote Console.

Reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

- In the future, do not show this warning
- Always trust content from this publisher

Log In to SX II Admin-Only Interface

You cannot connect to targets using the admin-only interface.

1. Launch a supported web browser.
2. Enter the SX II HTTP, HTTPS or DNS address provided to you by your Administrator, followed by /admin. For example: IP Address/admin

   Note: You are always redirected to the IP address from HTTP to HTTPS.
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, accept and/or allow access.

Access SX II Using an iOS Device

You can access SX II using your iOS device when certificates are properly installed on the device. iOS requires that the certificate and all certificates in the certificate chain be installed on the device to connect properly. This can be done by emailing the certificates to the iOS device. When all certificates are installed, the Profile will be listed as Verified. If the profile is "Not Verified" for any reason, or if the certificate is not signed with the IP or DNS entry used to connect to the SX II, the connection will fail.

The following procedure shows how to generate and install valid certificates with openssl.

To access SX II using an iOS device:

1. Create a simple CA.

   ```
   openssl genresa -out localCA.key 2048
   openssl req -x509 -sha256 -new -key localCA.key -out localCA.cer -days 356 -subj /CN="Local CA"
   ```
2. Generate key,CSR, and cer for SX II.

   ```
   openssl genrsa -out sx2.key 2048
   openssl req -new -out sx2.req -key sx2.key -subj /CN=<SX IP ADDRESS>
   openssl x509 -req -sha256 -in sx2.req -out sx2.cer -CAkey localCA.key -CA localCA.cer -days 355 -CAcreateserial -CAserial serial
   ```
3. Email the localCA.cer and sx2.cer files created to an email account that can be opened on the IOS device.
4. Open the email through the iOS device mail app and click on the localCA.cer to install the certificate. Follow prompts and trust the certificate.
5. Repeat for the sx2.cer.
6. Install the sx2.key and then the sx2.cer onto the SX II.

7. Reboot the SX II.
8. Use any browser on the iOS device to connect to the SX II. If there is any error in the certificate or it is not trusted, the javascript client will immediately disconnect when attempting to connect.

Change Your Password from the Remote Console

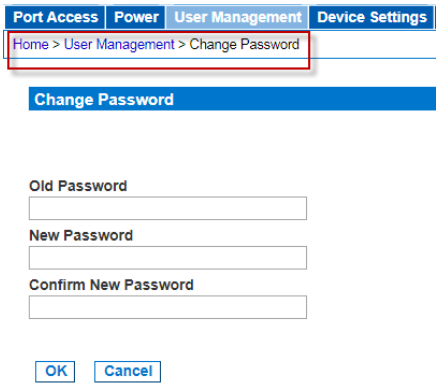
Note: You can also update passwords using command line interface. See **Change Your Password Using CLI** *(on page 197).*

- To change your password, open the Change Password page by selecting User Management > Change Password.

A confirmation that the password was successfully changed is displayed after you change it.

If strong passwords are in use, this page displays information about the format required for the passwords.

For more information, see Strong Passwords.

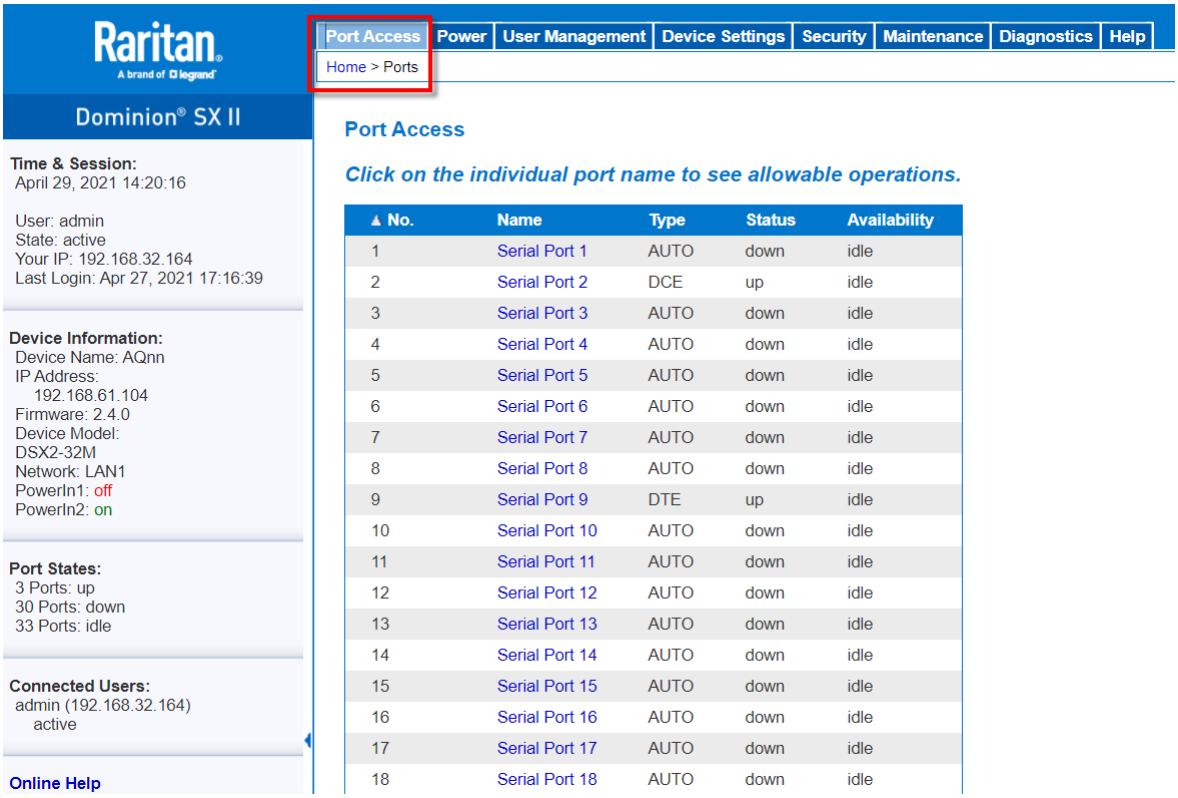


Important: If the administrator password is forgotten, SX II must be reset to the factory default from the Reset button on the rear panel and the initial configuration tasks must be performed again.

SX II Port Access Page

After a successful login, the Port Access page opens listing all ports along with their status and availability.

Note that target access is not enabled in the Admin-Only Interface version of the Remote Console.



No.	Name	Type	Status	Availability
1	Serial Port 1	AUTO	down	idle
2	Serial Port 2	DCE	up	idle
3	Serial Port 3	AUTO	down	idle
4	Serial Port 4	AUTO	down	idle
5	Serial Port 5	AUTO	down	idle
6	Serial Port 6	AUTO	down	idle
7	Serial Port 7	AUTO	down	idle
8	Serial Port 8	AUTO	down	idle
9	Serial Port 9	DTE	up	idle
10	Serial Port 10	AUTO	down	idle
11	Serial Port 11	AUTO	down	idle
12	Serial Port 12	AUTO	down	idle
13	Serial Port 13	AUTO	down	idle
14	Serial Port 14	AUTO	down	idle
15	Serial Port 15	AUTO	down	idle
16	Serial Port 16	AUTO	down	idle
17	Serial Port 17	AUTO	down	idle
18	Serial Port 18	AUTO	down	idle

Ports are numbered from 1 up to the total number of ports available for the SX II. For example, Port_1 - Port_48, Port_1 - Port_32.

"SerialPort"_"Port #" are what make up the default name the physical port until a name is configured for the port. Once a name is designated for a port, the name stays with the port until the name is edited or SX II is factory reset.

Port type includes:

- Auto - No target connected
- DTE - DCE target is connected or this port is forced to be configured as DTE.
- DCE - DTE target is connected or this port is forced to be configured as DCE.

Sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

Click on any port that listed and marked as Available to open its Port Action menu so you can then manage the target. For more information, see ***Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 32).

Note that in the Remote Console, you can also quickly access a powerstrip's page from the Port Access page by clicking on the Powerstrip link in the Type column.

SX II Left Panel

The left panel contains the following information.

Note that some information is conditional - meaning it is displayed based on your role, features being used and so on. Conditional information is noted here.

Information	Description	Displayed when?
Time & Session	The date and time the current session started	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the amount time the session has been idle.	Always
Your IP	The IP address used to access SX II.	Always
Last Login	The last login date and time.	Always

Information	Description	Displayed when?
Under CC-SG Management	The IP address of the CC-SG device managing the SX II.	When SX II is being managed by CC-SG.
Device Information	Information specific to the SX II you are using.	Always
Device Name	Name assigned to the SX II you are accessing.	Always
IP Address	The IP address of the SX II you are accessing.	Always
Firmware	Current version of firmware installing on the SX II.	Always
Device Model	The model of the SX II you are accessing.	Always
Network	LAN1, or LAN1 and LAN2 if you are in dual LAN mode.	Always
PowerIn1	Status of the power 1 outlet connection. Either on or off, or Auto-detect off	Always
PowerIn2	Status of the power 2 outlet connection. Either on or off, or Auto-detect off	Always
Port States	The statuses of the ports being used by SX II - up, down, idle.	Always
Connected Users	The users, identified by their username and IP address, who are currently connected to SX II.	Always
Online Help	Links to online help.	Always
FIPS Mode	FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant	When FIPS is enabled

Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets

Once you log in to SX II via a web browser, the SX II Port Access page displays. For more information on the Port page, see ***SX II Port Access Page*** (on page 29).

From the Port Access page, use the Port Action menu to connect, disconnect, or control power of targets and power strips that are connected to SX II.

Once connected, you can manage a target with either Serial Client, HSC or RSC. See ***HTML Serial Console (HSC) Help*** (on page 41) and Raritan Serial Console (RSC) Help.

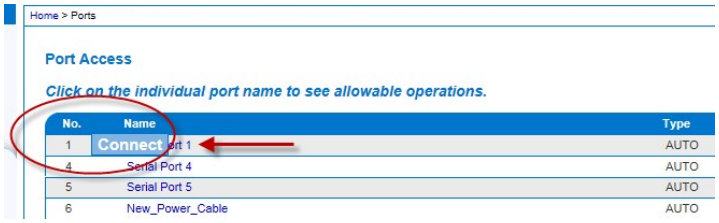
Note that you must have permissions to a target or power strip in order to access it.

To access the Port Action menu for a target or power strip:

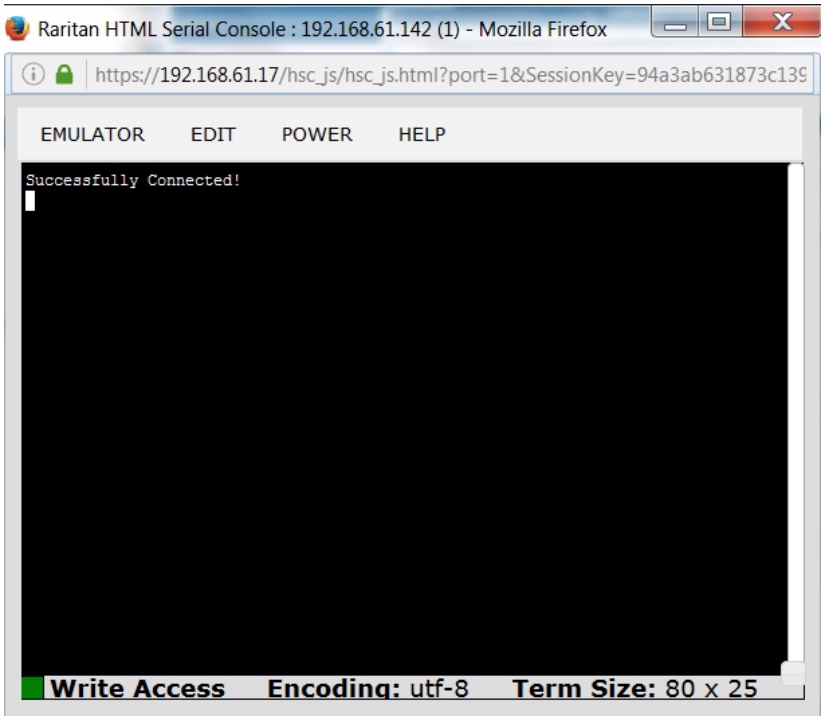
1. Hover your mouse over a target's port name in the list and click on your mouse.

   The Port Action menu appears.

   Note that only currently available options, depending on the port's status and availability, are listed in the Port Action menu.
2. Choose the desired menu option for that port to execute it.
   - ***Connect to a Target*** (on page 34)
   - ***Disconnect from a Target*** (on page 34)
   - ***Power On a Target*** (on page 35)
   - ***Power Off a Target*** (on page 36)
   - ***Power Cycle a Target*** (on page 37)



You can then connect using the Serial Client. When you connect to a target, the serial client opens in a new window. This screenshot shows an HSC connection.



Alternatively, you can connect via Direct Port Access, if SX II is configured for Direct Port Access.

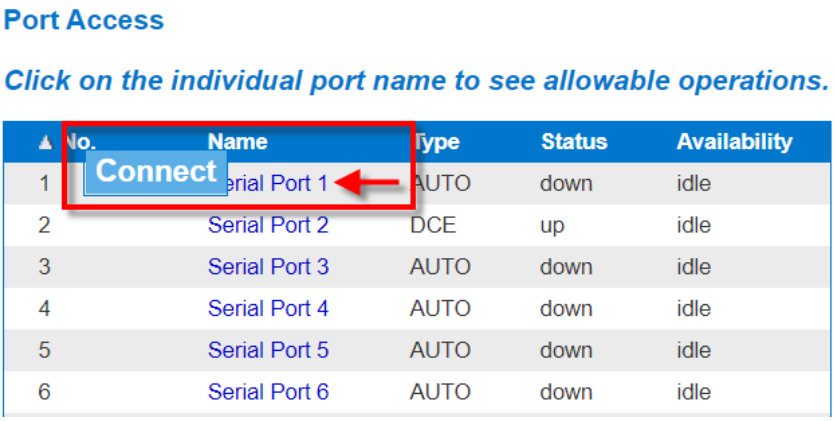
Note that you can also connect to targets via command line interface. See ***Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 37).

Connect to a Target

Creates a new connection to the target device.

From the SX II Remote Console, HSC or RSC opens in a new window and you manage the target from there.

If you are connected to the SX II from the Local Console port, you access the target via command line interface. See Raritan Serial Console (RSC) Help and ***Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 37).

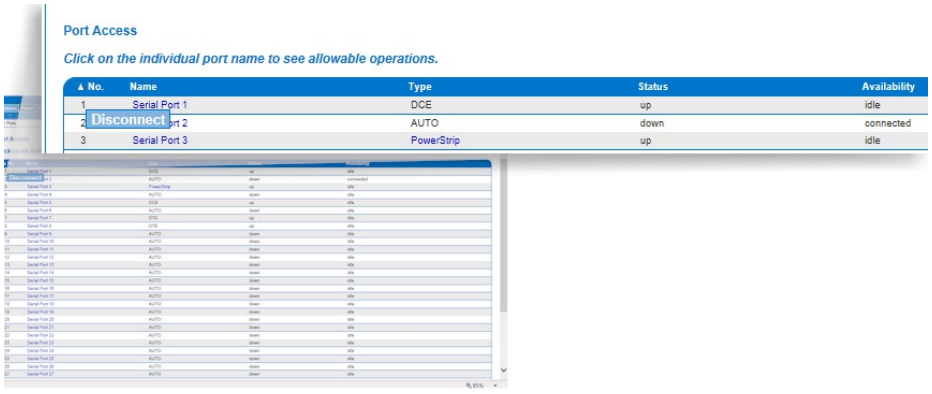


Disconnect from a Target

Once connected to a target, the Disconnect menu option is available in the Port Action menu.

Clicking on the Disconnect option disconnects from a target, and closes the HSC or RSC window. You can also click the X icon on the window or use the Exit menu option.

See ***Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 37).

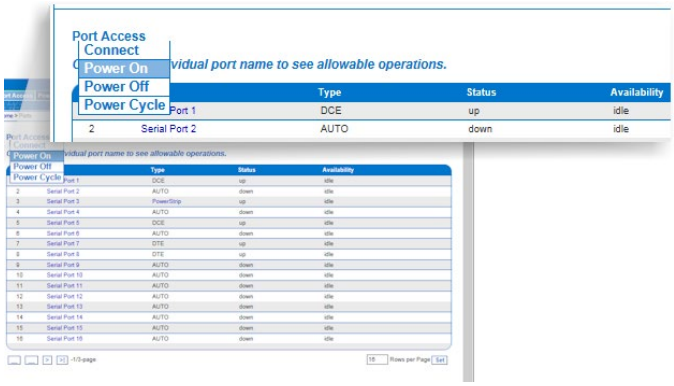


Power On a Target

Power on the target from the Remote Console through the associated outlet.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

You can also perform these actions through HSC, RSC, and command line interface. See ***HTML Serial Console (HSC) Help*** (on page 41), Raritan Serial Console (RSC) Help, and ***Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 37).



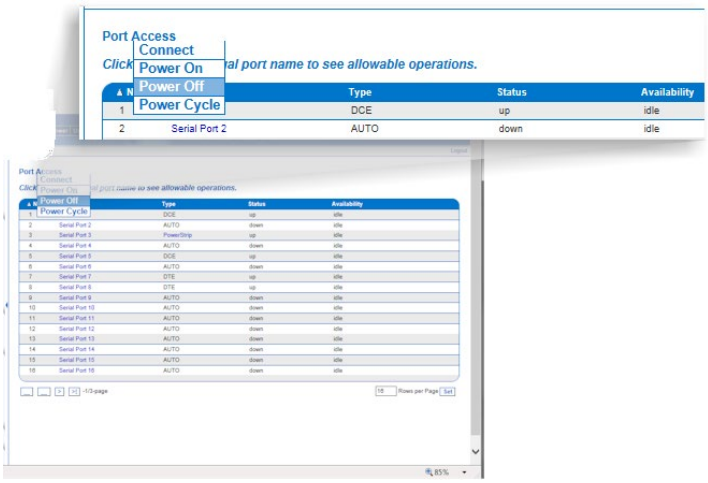
Power Off a Target

Power off the target through the associated outlet.

This option is visible only when -

- there are one or more power associations to the target or power strip
- you have permission to manage the power

You can also perform these actions through HSC, RSC, and command line interface. See ***HTML Serial Console (HSC) Help*** (on page 41), Raritan Serial Console (RSC) Help, and ***Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 37).



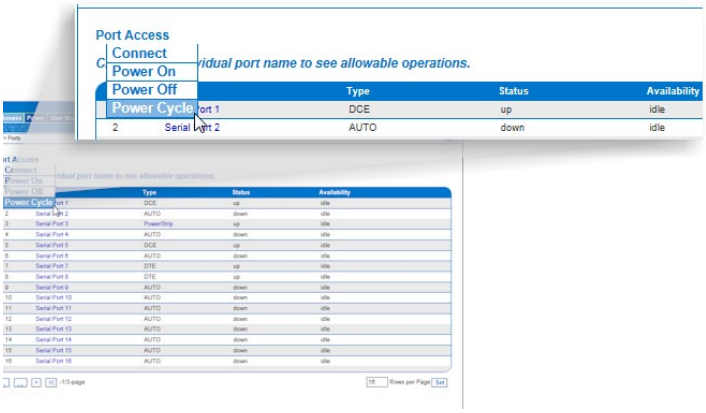
Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- The power strip is connected to SX II and configured properly.
- There are one or more power associations to the target.
- You have permission to manage the power.

You can also perform these actions through HSC, RSC, and command line interface. See ***HTML Serial Console (HSC) Help*** (on page 41), Raritan Serial Console (RSC) Help, and ***Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 37).



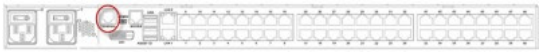
Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets

Before connecting to a target, the terminal emulation and escape sequence must be configured. See ***Set Terminal Emulation on a Target*** (on page 15) and ***Set the CLI Escape Sequence*** (on page 15).

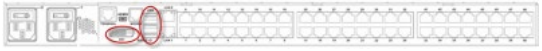
Connect the SX II While at the Rack

While at the rack, do one of the following depending on your needs -

- Connect a computer to the Terminal port with a CAT-5 cable and Raritan Adapter ASCSDB9F.



- Connect a keyboard tray or KVM console to the DVI-D and USB ports.



- Connect a laptop to the Mini-USB Admin port.

Note that connecting to the SX II Local Console via the Local port is an independent access path to each connected target device.

Video Resolution

The default, Local Console port video resolution is 1024x768@60.

By default, monitors are typically set to the highest resolution they support.

Once a monitor is connected to the SX II Local Port DVI, SX II retrieves EDID information from the monitor, including its native, preferred resolution. SX II uses the monitor's preferred, native resolution as long as it is a resolution that SX II supports. If it is not, SX II switches to a resolution it supports and that most closely matches the monitor's resolution.

For example, if a monitor with a native resolution of 2048x1600@60Hz is connected to SX II, SX II detects that it is not an SX II supported resolution and selects a resolution it does support, such as 1280x1024@60Hz.

Note that you can connect to targets using the Remote Console and manage them using Raritan Serial Console (RSC). See Raritan Serial Console (RSC) Help and ***Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets*** (on page 32) .

Connect Commands

Connect to a port using port number or port name. Use double quotes around port names that contain space symbols. For example: "Serial Port 1".

```
admin > connect <port number>
```

OR

```
admin > connect <port name>
```

Port Sub-Menu Commands

The port sub-menu can be reached using the escape key sequence.

Clear history buffer for this port.

```
admin > [portname] > clearhistory
```

Close this target connection. When a target is disconnected, the appropriate disconnect message appears.

```
admin > [portname] > close, quit, q
```

Display the history buffer for this port.

```
admin > [portname] > gethistory
```

Get write access for the port.

```
admin > [portname] > getwrite
```

Return to the target session.

```
admin > [portname] > return
```

Send a break to the connected target.

```
admin > [portname] > sendbreak
```

Lock write access to this port.

```
admin > [portname] > writelock
```

Unlock write access to this port.

```
admin > [portname] > writeunlock
```

Query Power status of this port.

```
admin > [portname] > powerstatus
```

Toggle Power On/Off of this port.

```
admin > [portname] > powertoggle
```

Power on the target.

```
admin > [portname] > poweron
```

Power off the target.

```
admin > [portname] > poweroff
```

Power cycle the target.

```
admin > [portname] > powercycle
```

Command Line Interface Protocols

- SSH (Secure Shell) via IP connection
- Telnet via IP connection
- Local Console via the Local Port and Mini-USB port
- Terminal port

If SX II has an internal modem and console mode is enabled, the modem interface can also be accessed from CLI.

Many SSH/TELNET applications are available such as PuTTY, SSH Client and OpenSSH Client. These can be located and downloaded from the Internet.

Command Line Interface Partial Searches

Enter the first few characters of command and press the Tab key on your keyboard in order to locate a specific command.

The command line interface (CLI) completes the entry if the characters form an exact match.

For example entering

```
admin > Config > us
```

and then pressing the Tab key, returns the result `users`.

If an exact match is not found, all of the commands at the same level the CLI hierarchy that are potential matches are listed.

For example, entering

```
admin > Config > User > add
```

and then pressing the Tab key, returns results for `addgroup` and `adduser`.

If needed, enter additional text to make the entry unique and press the Tab key to complete the entry. Alternatively, use a command from the list.

Command Line Interface Tips

- When commands are displayed as a list, they are in alphabetical order.
- Commands are not case sensitive.
- Commands without arguments default to show current settings for the command.
- A command's parameters are usually parameter-value pairs in which the parameter name is followed by a space and the value.
- Typing a question mark (`?`) after a command displays help specific to the command.

Command Line Interface Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter on your keyboard to execute the command.
- Press Tab on your keyboard to complete a command. Tab also completes parameters and values (if the value is part of an enumerated set).

Command Line Interface High-Level Commands

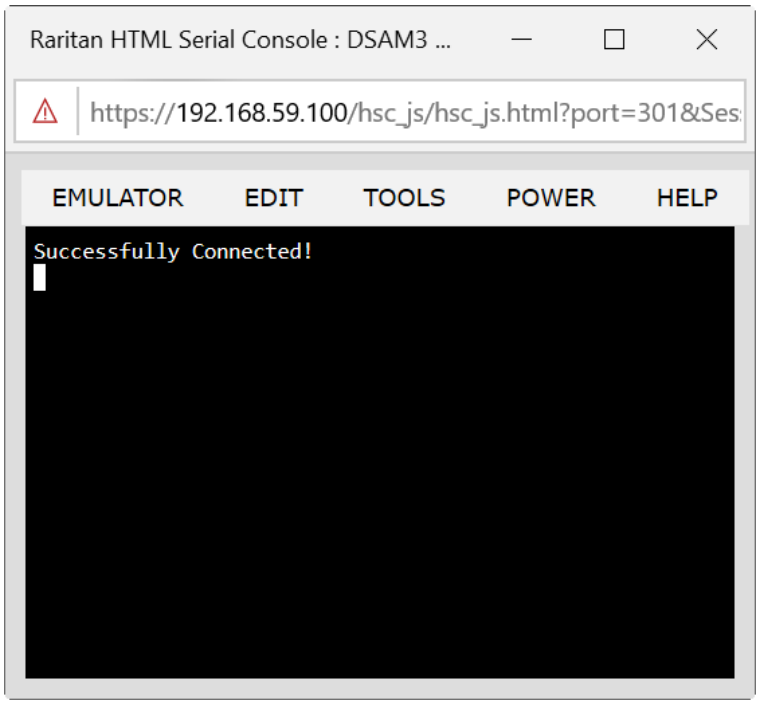
The CLI is menu based. Some commands move to a menu with a different command set.

The following common commands can be used at all levels of the command line interface (CLI):

- `top` – Return to the top level of the CLI hierarchy, or the `username` prompt.
- `history` – Displays the last 200 commands the user entered into the SX II CLI.
- `logout` – Logs the user out of the current session.
- `quit` – Moves the user back one level in the CLI hierarchy.
- `help` - Displays an overview of the CLI syntax.

HTML Serial Console (HSC) Help

You can connect to serial targets using HSC. HSC is supported with several Raritan products that offer serial connections. Not all products support all HSC features. Differences are noted.



Emulator

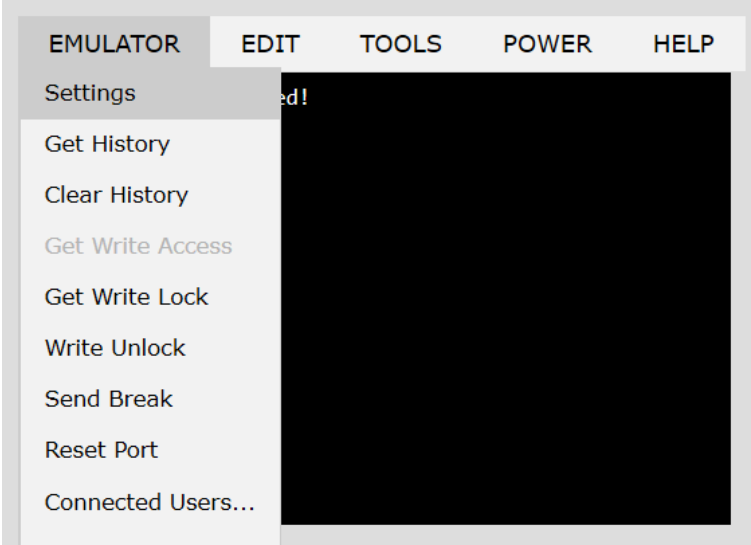
IMPORTANT: HSC sessions are affected by the SX II Idle Timeout.

If you have not changed the SX II Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.

Change the default Idle Timeout setting and then launch the HSC. See *Login Limitations* **(on page 153) for details on changing the Idle Timeout setting.**

Access Emulator Options

1. Select the Emulator drop-down menu to display a list of options.



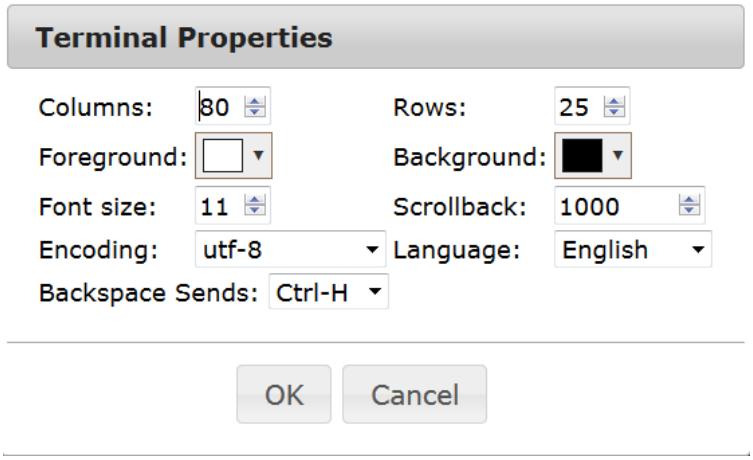
Settings

Note:

KX3 administrators can set Terminal emulation settings in Setup > Port Configuration.

KX4-101 administrators can set terminal emulation settings in DSAM Serial Ports > Settings.

1. Choose Emulator > Settings. The Terminal Properties dialog displays the default settings.



2. Set the terminal size by selecting the number of Columns and Rows. Default is 80 by 25.
3. Set the Foreground and Background colors. Default is white on black.
4. Set the Font size. Default is 11.
5. Set the Scrollback number to indicate the number of lines available for scrolling.
6. Choose one of the following from the Encoding drop-down menu:
   - UTF-8
   - 8-bit ascii
   - ISO-8859-1
   - ISO-8859-15
   - Shift-JIS
   - EUC-JP
   - EUC-KR
7. Choose one of the following from the Language drop-down menu:
   - English
   - Japanese
   - Korean
   - Chinese
   - Bulgarian

8. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.
9. Click OK to save. If you changed the Language setting, the HSC changes to that language when the Display Settings window is closed.

Get History

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.
- Displays up to 512KB of recent console message history. This allows a user to see target device events over time.

When the size limit is reached, the text wraps, overwriting the oldest data with the newest.

Notes: History data is displayed only to the user who requested the history.

To view the Session History, choose Emulator > Get History.

Clear History

- To clear the history, choose Emulator > Clear History.

Get Write Access

Only users with permissions to the port get Write Access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the HSC via the Get Write Access command.

To enable Write Access, choose Emulator > Click Get Write Access.

- You now have Write Access to the target device.
- When another user assumes Write Access from you:
  - The HSC displays a red block icon before Write Access in the status bar.
  - A message appears to the user who currently has Write Access, alerting that user that another user has taken over access to the console.

Get Write Lock

Write lock prevents other users from taking the write access while you are using it.

1. To get write lock, choose Emulator > Get Write Lock.
2. If Get Write Lock is not available, a request rejected message appears.

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the OK prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

Only users with Write Access privileges can send a break.

To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Choose Emulator > Send Break. A Send Break Ack (Acknowledgement) message appears.
3. Click OK.

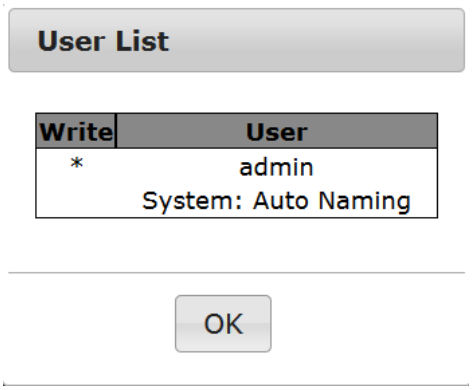
Reset Port

Reset Port resets the physical serial port on the SX2 and re-initializes it to the configured values regarding bps/bits, and so on.

Connected Users

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Choose Emulator > Connected Users.



2. A star appears in the Write column for the User who has Write Access to the console.

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste and Copy All

Data on the current visible page can be selected for copying. Copy and Paste are accessible in the HSC by right click in the terminal window. Select Copy or Paste in the context menu that appears.

To copy all text, use the Copy All option in the Edit menu.

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See ***Send Text File*** (on page 46).

When pasting data to a port, the end of a line is sent as a carriage return.

The Cut option on the right-click menu is disabled.

Do not use the Delete option that appears in the right-click menu of IE and some versions of Firefox. This Delete option will remove display lines entirely from the emulator window.

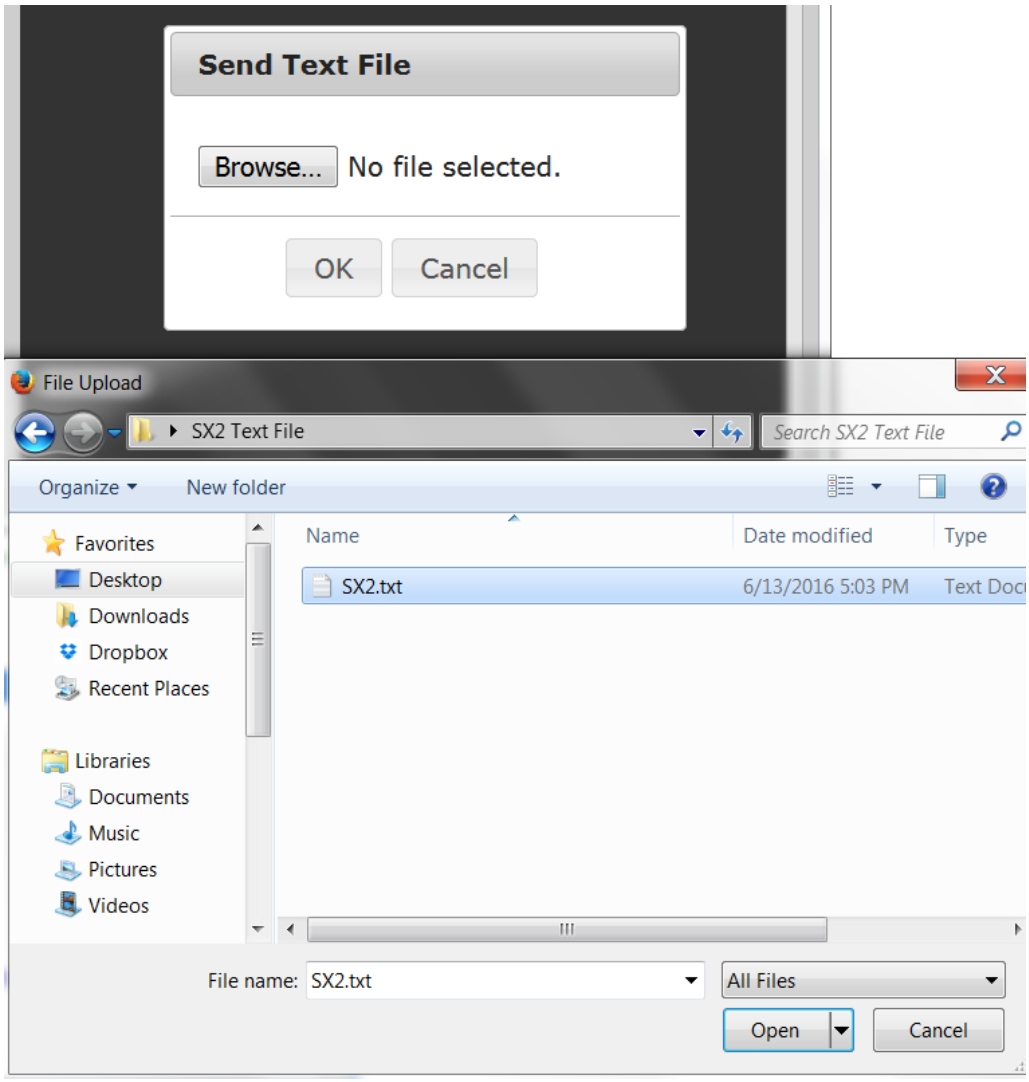
Browser-specific behaviors

When copying from IE or Edge browsers, there are no end of line characters in the copied data. The pasted data appears to be all in one line and contains many spaces. When pasting back into a HSC window, the data may appear to be misaligned, but the data is complete.

Send Text File

1. Select Edit> Send Text File.
2. In the Send Text File dialog, click Browse to find the text file.
3. Click OK.
   - When you click OK, the selected file sends directly to the port.

- If there is currently no target connected, nothing is visible on the screen.



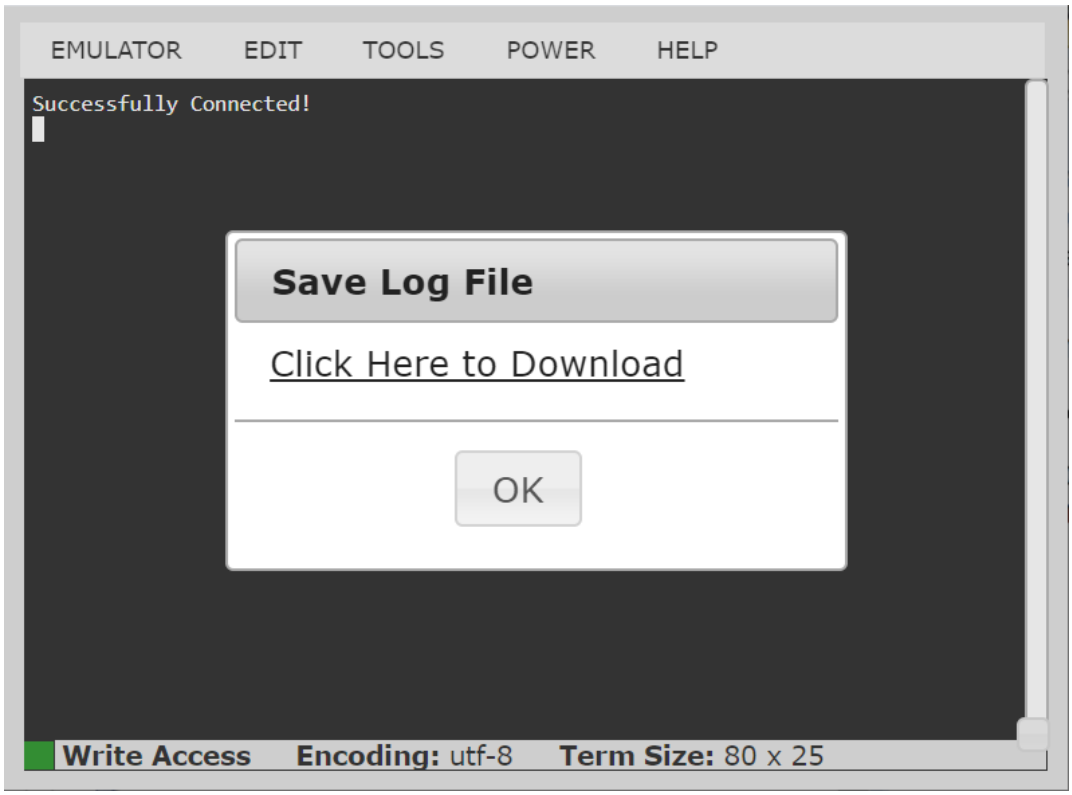
Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:

1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"
3. Click on the SX II website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

Tools: Start and Stop Logging

The Tools menu contains options for creating a data history file and downloading it.

1. Choose Tools > Start Logging to start the storage of serial port data in memory.
2. Click Stop Logging to save the log file. A pop up message appears with a download link. Click to download the memory buffer into a text file.

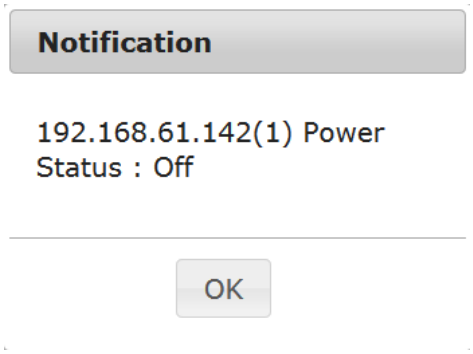


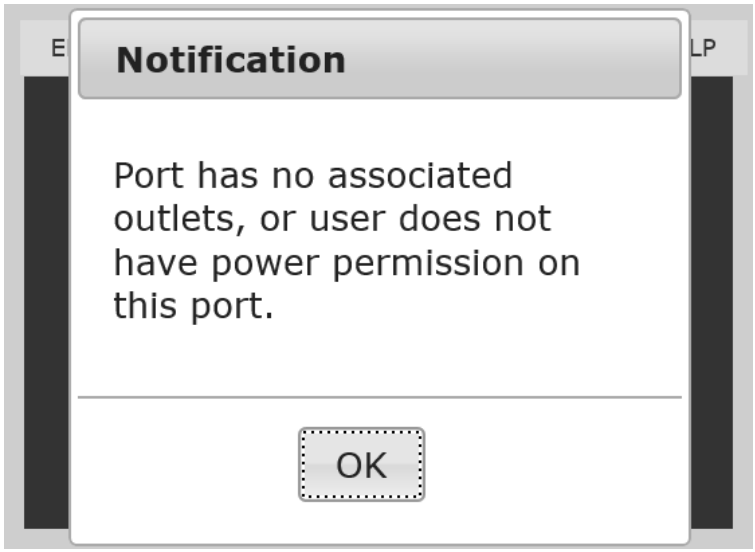
Power Status

Power Status in HSC shows the status of the outlet the target is plugged into.

1. Choose Power > Power Status.
2. The Notification dialog shows the status of the outlet as ON or OFF.

Status may also show no associated outlet, or no power permission to the port.





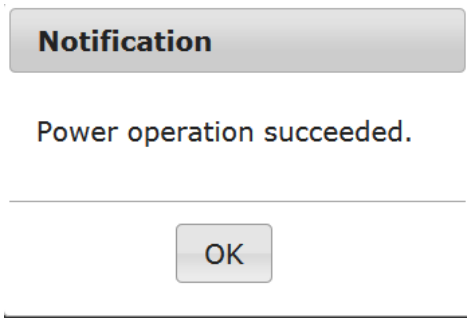
Power on a Target

Use this option to power on a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power On.

2. Click OK in the success message.

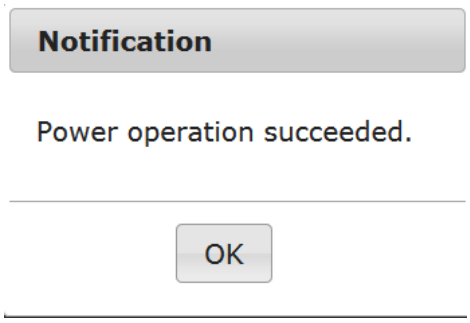


Power Off a Target

Use this option to power off a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power Off.
2. Click OK in the success message.



Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- there are one or more power associations to the target
- the target is already powered on (the port status us Up)
- you have permission to manage the target's power

1. Choose Power> Power Cycle.
2. Click OK in the success message.

Browser Tips for HSC

Some browsers have limitations that affect HSC.

- Browser option to select certificate for authentication displayed on Edge and Chrome after session is idle for about 5 minutes, due to internal browser SSL caching and timeouts. If certificate is selected promptly, reconnection is successful. With longer idle times, authentication is not successful, and the browser should be restarted to reconnect. Issue is not observed in Firefox or IE 11.
- Internet Explorer has an internal limitation on the number of websockets that are allowed to be created to a single server (6). This can be changed by modifying a registry variable as shown here : https://msdn.microsoft.com/en-us/library/ee330736(v=vs.85).aspx#websocket_maxconn.
- Internet Explorer 11, Safari, and Edge have a limitation when connecting to IPv6 devices. Using the numerical URL will not work when it attempts to establish a websocket connection. In these browsers, use the device hostname or literal IPv6 as UNC to connect to the SX II. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- When using HSC in IOS Safari, the keyboard may not appear in some pages if the "request desktop website" setting is enabled. To change the setting, go to Settings > Safari >Request Desktop Website, then make sure All Websites is not selected, and the device address is not selected. You can also set this per address by clicking the "aA" in Safari's URL pane when connected to the HSC port, then select "Website Settings" and make sure that "Request Desktop Website" is not selected.

Raritan Serial Console (RSC) Functions

The following functions are available when accessing targets via Raritan Serial Console (RSC) from the SX II Remote Console and when accessing targets via standalone RSC.

You can access RSC by connecting to **<SX II IP Address>/rsc**

Emulator

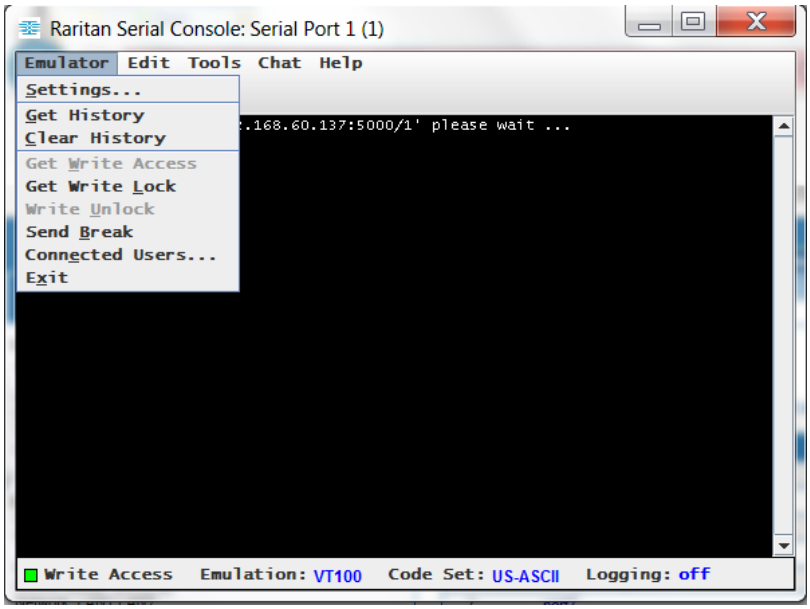
IMPORTANT: Raritan Serial Console (RSC) sessions are affected by the SX II Idle Timeout.

If you have not changed the SX II Idle Timeout setting from the default, your RSC session could be closed automatically if it exceeds the Idle Timeout period.

Change the default Idle Timeout setting and then launch the RSC. See *Login Limitations* **(on page 153) for details on changing the Idle Timeout setting.**

Access Emulator Options

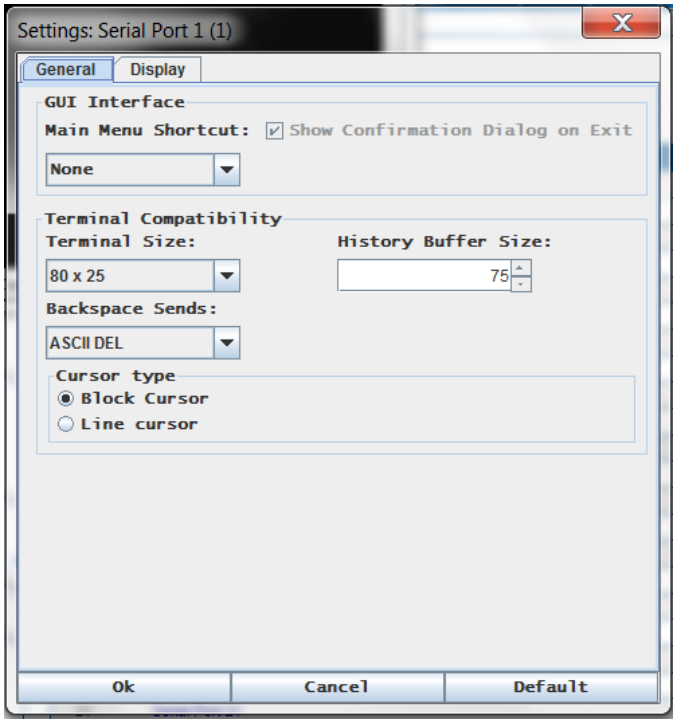
1. Select the Emulator drop-down menu to display a list of options.



Settings

Note: An Administrator can set Terminal emulation settings using Setup > Port Configuration.

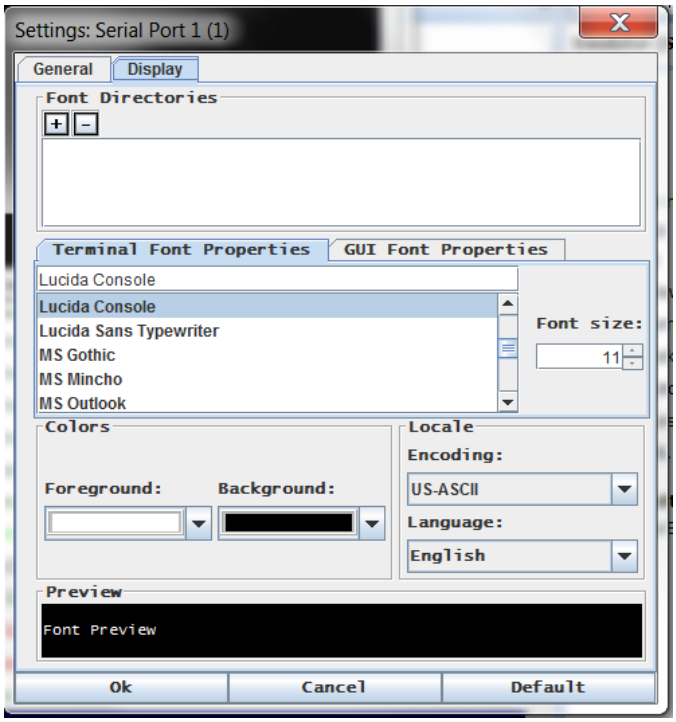
1. Choose Emulator > Settings. The Settings screen displays the General tab with the default settings.



2. The Main Menu Shortcut default is None; accept this, or choose one of the following from the Main Menu Shortcut drop-down menu:
   - F10
   - Alt
3. The Show Confirmation Dialog on Exit checkbox is selected by default, but you can deselect it based on preference.
4. The Terminal Size default is selected, or you can choose a different size from the drop-down menu.
5. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.
6. The History Buffer Size default is 75. Type a value or use the arrows to change the buffer size.
7. The Cursor type default is Block Cursor, or you can select the Line Cursor radio button.
8. Click OK.

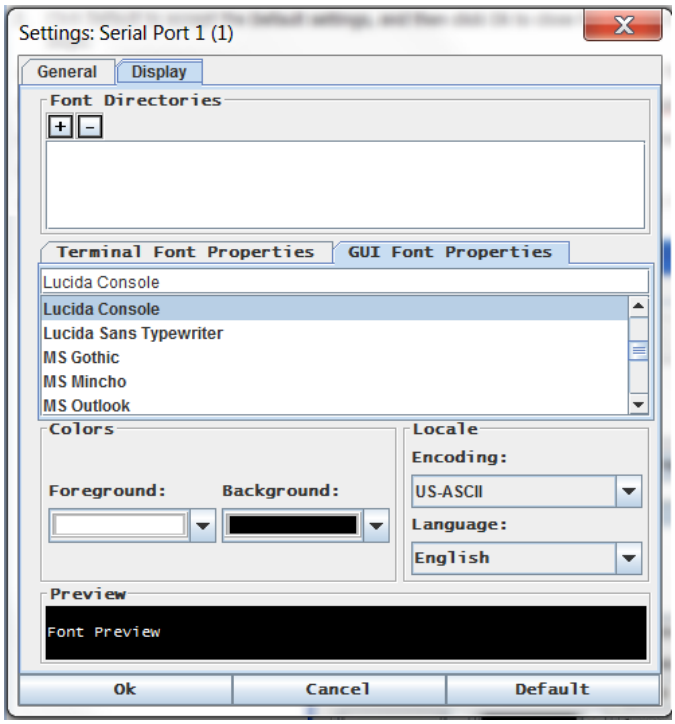
Display Settings

1. Choose Emulator > Settings and click the Display tab.



2. Click Default to accept the Default settings, and then click Ok to close the Display Settings window. To change the settings, follow these steps:
   a. The Terminal Font Properties default is Arial, or you can choose a font from the Terminal Font Properties scrolling list.
   b. Click the GUI Font Properties tab.

c. The default font property is Monospace, or you can choose a font from the GUI Font Properties scrolling list.



Note: For Simplified Chinese characters, RSC supports EUC-CN encoding system.

3. Choose the following from their respective drop-down menus:
   - Foreground Color
   - Background Color
4. Choose one of the following from the Encoding drop-down menu:
   - US-ASCII
   - ISO-8859-1
   - ISO-8859-15
   - UTF-8
   - Shift-JIS
   - EUC-CN
   - EUC-JP
   - EUC-KR
5. Choose one of the following from the Language drop-down menu:
   - English
   - Japanese
   - Korean
   - Chinese

- Bulgarian

6. Click Ok to close the Display Settings window. If you changed the Language setting, the RSC changes to that language when the Display Settings window is closed.

Note: In case of unrecognized characters or blurry screens that might appear when RSC is launched, due to localization support, try changing the font to Courier New.

Get History

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.
- Displays up to 512KB of recent console message history. This allows a user to see target device events over time.

When the size limit is reached, the text wraps, overwriting the oldest data with the newest.

Notes: History data is displayed only to the user who requested the history.

To view the Session History, choose Emulator > Get History.

Clear History

- To clear the history, choose Emulator > Clear History.

Get Write Access

Only users with permissions to the port get Write Access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the RSC via the Get Write Access command.

To enable Write Access, choose Emulator > Click Get Write Access.

- You now have Write Access to the target device.
- When another user assumes Write Access from you:
  - The RSC displays a red block icon before Write Access in the status bar.
  - A message appears to the user who currently has Write Access, alerting that user that another user has taken over access to the console.

Get Write Lock

Write lock prevents other users from taking the write access while you are using it.

1. To get write lock, choose Emulator > Get Write Lock.
2. If Get Write Lock is not available, a request rejected message appears.

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the OK prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

Only users with Write Access privileges can send a break.

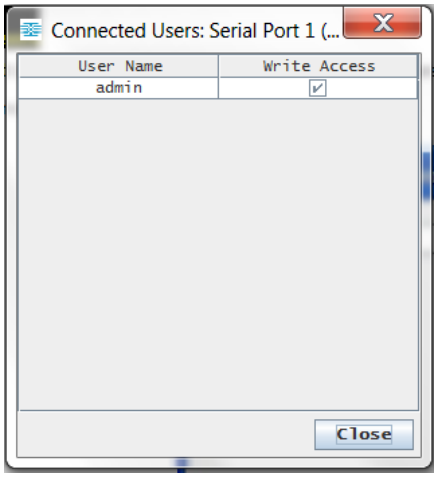
To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Choose Emulator > Send Break. A Send Break Ack (Acknowledgement) message appears.
3. Click OK.

Connected Users

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Choose Emulator > Connected Users.



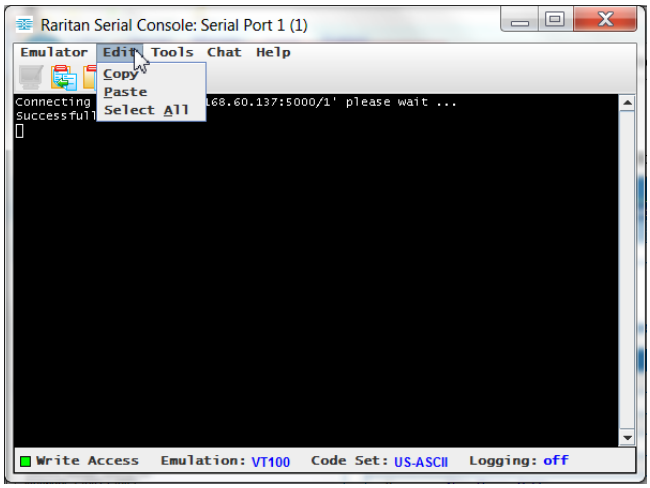
2. A check mark appears in the Write Access column after the name of the User who has Write Access to the console.
3. Click Close to close the Connected Users window.

Exit

1. Choose Emulator > Exit to close the RSC. The Exit Confirmation dialog appears.
2. Click Yes.

Edit

Use the Copy, Paste, and Select All text commands to relocate and/or re-use important text.



To copy and paste all text:

1. Choose Edit > Select All.
2. Choose Edit > Copy.
3. Position the cursor at the location where you want to paste the text.
4. Click once to make that location active.
5. Choose Edit > Paste.

Note: The copy-paste limit of text in RSC is 9999 lines.

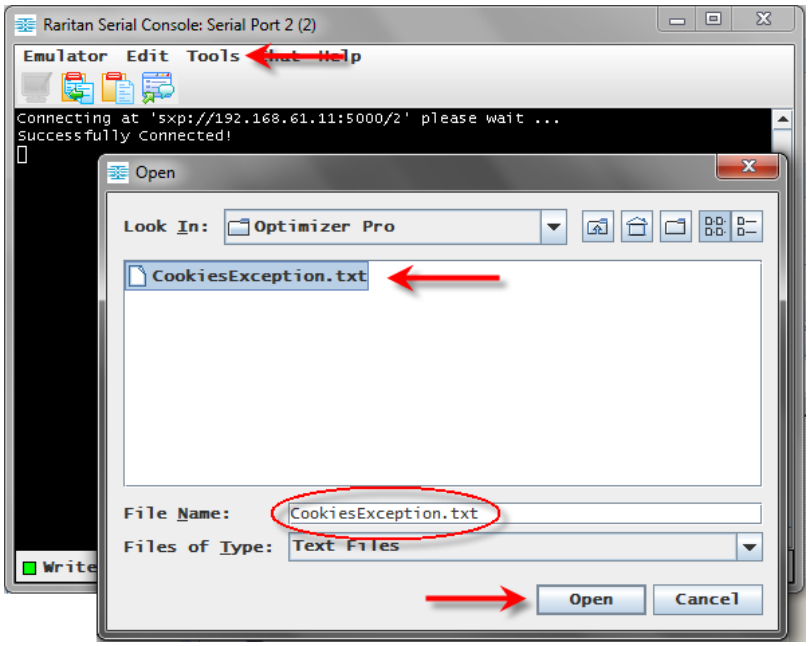
Keyboard shortcuts to highlight, copy, and paste all or partial lines of text:

- Click and drag your mouse over the text you wish to copy.
- Use Ctrl+C to copy text.
- Position the cursor where you want to paste the text and click in that location to make it active.
- Use Ctrl+V to paste text.

Send a Text File

1. Select Tools > Send Text File. A Send Text File screen appears.
2. Open the directory of the Text file.
3. Click on or enter the file name of the text file.

4. Click Open.



- When you click Open, Raritan Serial Console (RSC) sends whatever file you selected directly to the port.
- If there is currently no target connected, nothing is visible on the screen.

Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:

1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"
3. Click on the SX II website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

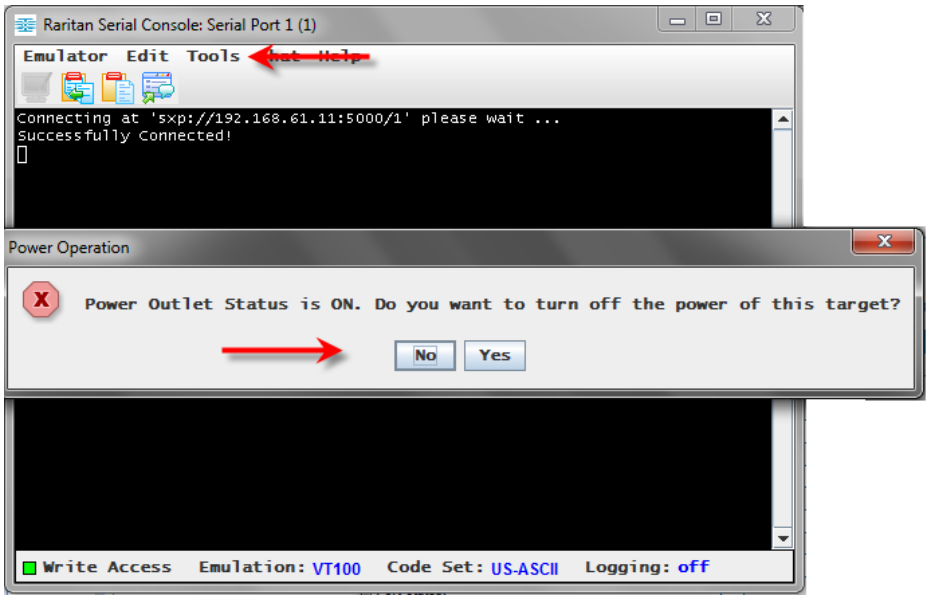
Toggle Power

The Toggle Power function lets you power on or off the device that is connected to the associated outlet on a Power Distribution Unit (PDU). For example, if a router is connected to one of the outlets on the PDU, you can toggle the router's power on or off.

You must configure the association of outlets to the target port of the device before you can use the Toggle Power feature. Assign a power port to the serial target from the Device Settings > Port Configuration tab of the device. If you have not done this, the system displays a message stating that the target is not associated with a power outlet.

You must have power control permissions to the port to perform these functions.

1. Select Toggle Power to turn the device (router) on or off. A prompt appears displaying the current status of the outlet(s). You can turn the device on or off depending on its current status.
2. If you select No, the system returns you to the RSC screen.
3. If you select Yes, the system sends the power command to either turn on or off the outlets associated to the target port of the device.



If you receive a hardware error message, this means the PDU command failed.

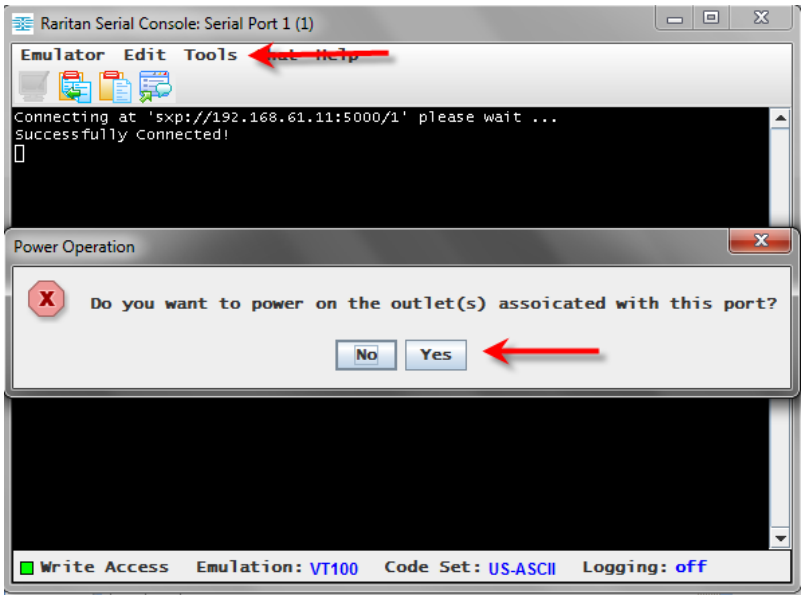
If you receive a software error message, this means another user is controlling the power outlet and the power control command cannot be sent.

Power On a Target

Use this option to power on a target from Raritan Serial Console (RSC).

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Tools > Power On.
2. Click Yes when prompted to confirm.



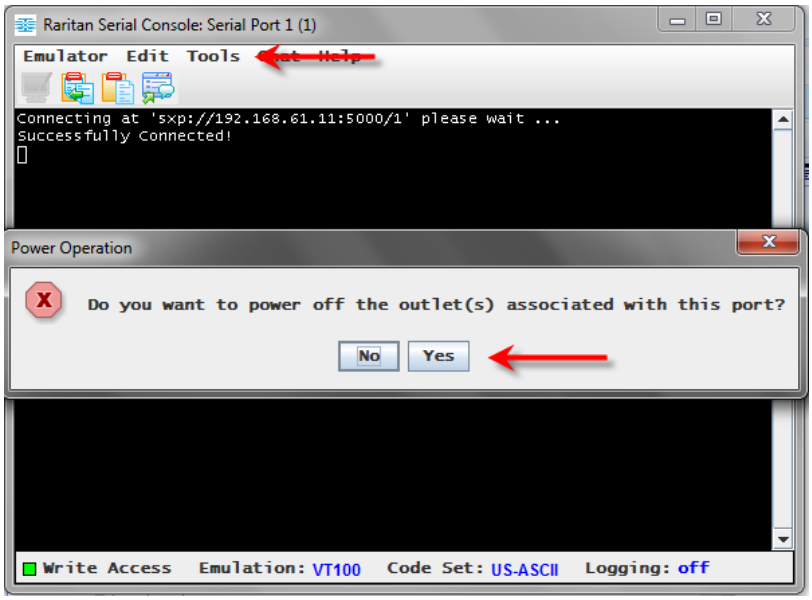
Power Off a Target

Use this option to power off a target from Raritan Serial Console (RSC).

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Tools > Power Off.

2. Click Yes when prompted to confirm.



Power Cycle a Target

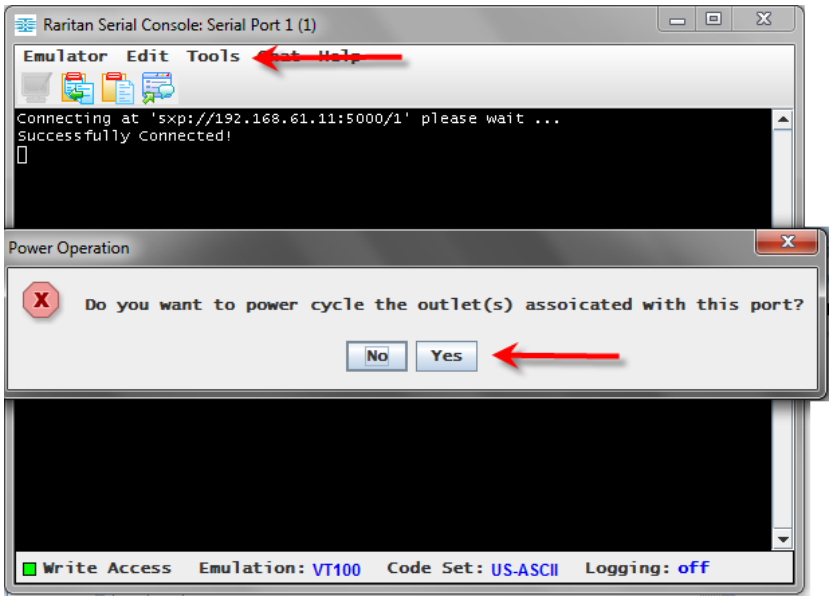
Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- there are one or more power associations to the target
- the target is already powered on (the port status us Up)
- you have permission to manage the target's power

1. Select Tools > Power Cycle.

2. Click Yes when prompted to confirm.



Standalone Raritan Serial Console Requirements

The following requirements must be met to support the Raritan Serial Console (RSC):

- Minimum 1 GHz PC with 512 MB RAM.
- Java™

  See SX II release notes for the required version.

  If you do not have a compatible version of the JRE, go to ***http://www.java.com*** (***http://www.java.com***) and click the Download Now button.

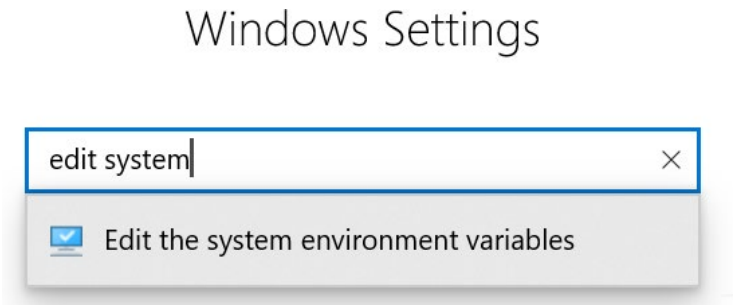
Your system may require configuration adjustments depending on the operating system and browser. The JRE provides configuration instructions with the JRE download. See ***http://www.java.com/en/download/help/testvm.xml*** (***http://www.java.com/en/download/help/testvm.xml \o http://www.java.com/en/download/help/testvm.xml***) to determine the JRE version currently installed on your system.

Ensure that Java can be started from the command line.

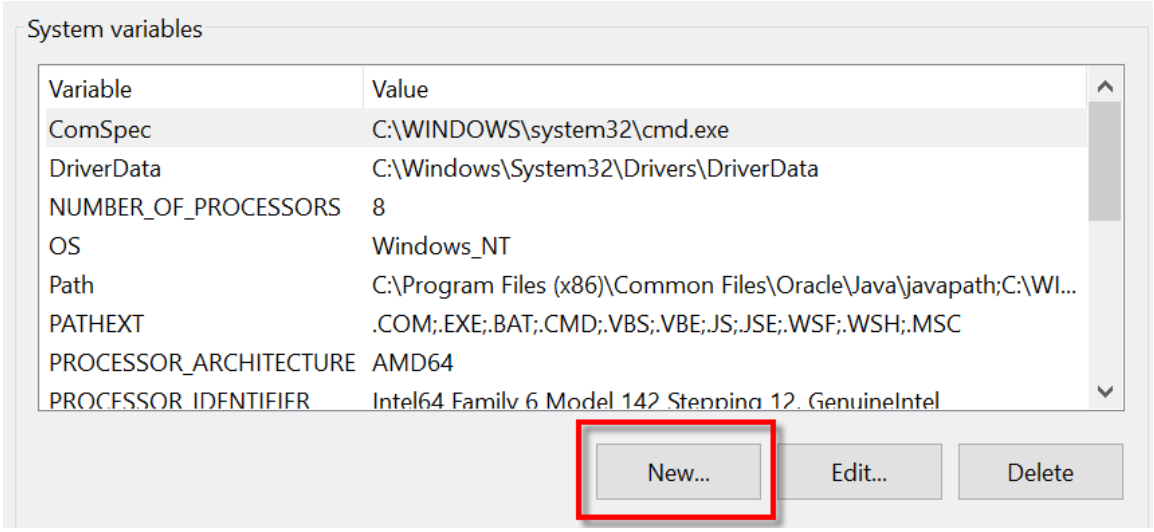
To do this, you must configure environment variables. Make a note of the exact path where Java was installed (the path information is used later).

Set Windows OS Variables and Install Standalone Raritan Serial Console (RSC)

1. Open the Windows Settings, then search for "Edit the system environment variables."

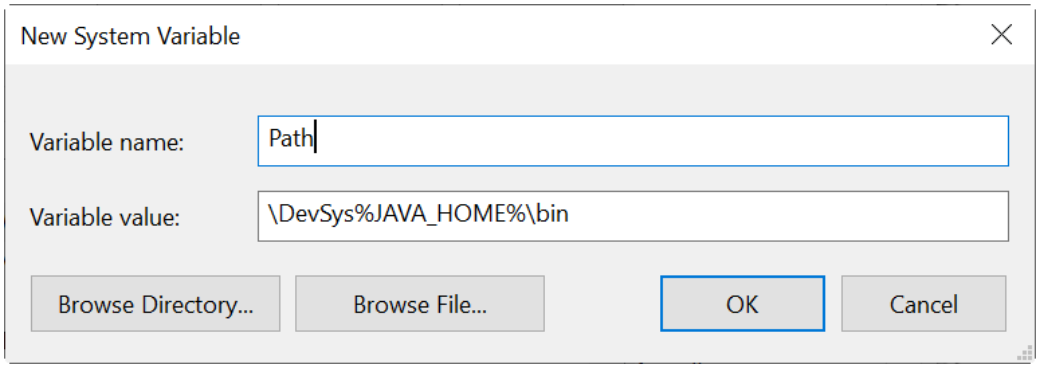


2. In the System Properties > Advanced dialog, click Environment Variables.
3. In the System variables section, click New.



4. Write down the installed Java path.
5. In the Variable value block field of the New System Variable dialog, add JAVA_HOME to the Variable name block and the Java path you wrote down earlier.
6. Click OK.
7. Select the PATH variable and click Edit.
8. Add %JAVA_HOME%\bin to the end of the current Variable value. Ensure a semicolon (;) separates the new value from the last value in the string.

9. Click OK.



10. Select the CLASSPATH variable and click Edit.
11. Ensure the CLASSPATH Variable value is configured properly; that is, its value must have a period (.) in it. If, for any reason, there is no CLASSPATH variable defined, create one.

Next, install Raritan Serial Console (RSC) on your Windows OS.

You must have administrative privileges to install RSC.

1. Log in to a Windows® machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Double-click on the executable file to start the installer program. Install following the prompts.
4. Click Done.

Set Linux OS Variables and Install Standalone Raritan Serial Console (RSC) for Linux

To set Java™ for a specific user, open and edit the **.**profile file located in the /home/Username folder.

To set Java for all users, open the .profile file in your /etc folder:

1. Find the line where you set your path:

```
export
PATH=$PATH:/home/username/somefolder
```

2. Before that line you must set your JAVA_HOME and then modify your PATH to include it by adding the following lines:

```
export
JAVA_HOME=/home/username/j2sdk1.8/
export PATH=$PATH:$JAVA_HOME/bin
```

3. Save the file.

You must have administrative privileges to install Raritan Serial Console (RSC).

1. Log in to your Linux™ machine.

2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Open a terminal window and change to the directory where the installer is saved.
4. Type *java -jar RSC-installer.jar* and press Enter to run the installer.
5. Click Next after the initial page loads. The Set Installation Path page opens.
   a. Select the directory where you want to install RSC and click Next.
   b. Click Browse to navigate to a non-default directory.
   c. Click Next when the installation is complete.
   d. Click Next again. The installation is complete. The final page indicates where you can find an uninstaller program and provides the option to generate an automatic installation script.
6. Click Done to close the Installation dialog.

Setting UNIX OS Variables

To check the latest JRE™ version on Sun Solaris™:

1. Launch a terminal window on the Sun Solaris desktop.
2. Type `java-version` in the command line and press Enter. The currently-installed version of Java™ Runtime Environment (JRE) appears.
   - If your path variable is not set to where the Java binaries have been installed, you may not be able to see the JRE version.
   - Assuming JRE is installed in /usr/local/java: you must set your PATH variable.
   - To set a path for the bash shell:

     ```
     export
     PATH=$PATH:/usr/local/java/j2re1.8/bin
     ```

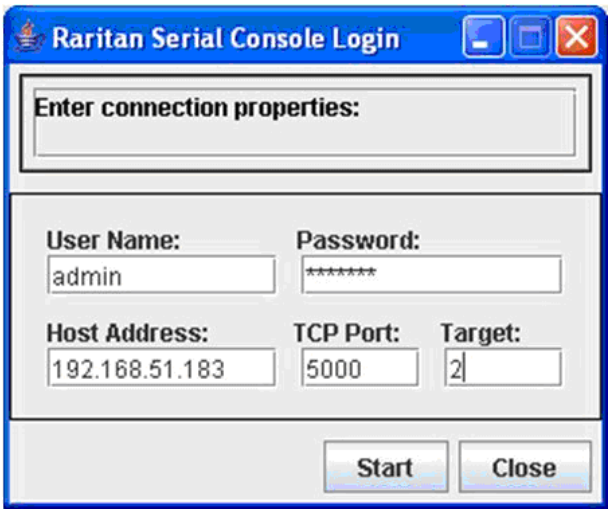
   - To set path for tcsh or csh:

     ```
     set
     PATH = ($PATH /usr/local/java/j2re1.8/bin)
     ```

   - These commands can either be typed at the terminal each time you log in, or add them to your .bashrc for bash shell or .cshrc for csh and tcsh so that each time you log in, the path is already set. See your shell documentation if you encounter problems.
3. If the JRE is installed, proceed with the RSC installation; download JRE if it is not, and then install RSC.

Launching RSC on Windows Systems

1. Double-click the shortcut or use Start Programs to launch the standalone Raritan Serial Console (RSC). The RSC Login connection properties dialog appears.



2. Enter the Dominion SX II IP address, account information, and the desired target (port).
3. Click Start. RSC opens with a connection to the port.

Note: In case of unrecognized characters or blurry screens in RSC window due to localization support, try changing the font to Courier New. Choose Emulator > Settings > Display, and select Courier New for Terminal Font Properties or GUI Font Properties.

Chapter 4 SX II Administration

This help contains information on tasks typically performed by Administrators, such as managing user groups and users, managing authentication and security, configuring network settings and so on.

Note that the same tasks can be performed from the Remote Console, the Admin Client or command line interface (CLI), so this section is divided into a Remote Console and CLI section.

In This Chapter

Administering SX II from the Remote Console and Admin-Only Interface

This section is specific to tasks performed in the SX II Remote Console, including the Admin-Only Interface

For information on performing tasks using command line interface, see ***Administering SX II Using command line interface*** (on page 196).

Configure Power Strips from the Remote Console

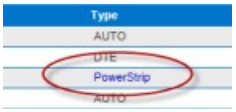
You can control Raritan PX rack PDU outlets (power strips) and Baytech rack PDU power strip outlets that are connected to SX II.

For details on how to connect a PX to SX II, see ***Connect and Configure a Rack PDU (Powerstrip)*** (on page 71).

Once connected to SX II, the rack PDU and its outlets can be configured.

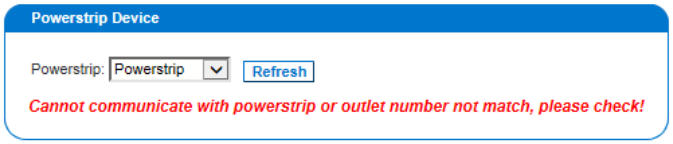
Configure power strips from the Remote Console as shown here, or using command line interface. See ***Configure Power Strips Using CLI*** (on page 198).

Note that in the Remote Console, you can also quickly access a powerstrip's page from the Port Access page by clicking on the Powerstrip link in the Type column.



If no power strips are connected to SX II, a message stating "No power strips found" is displayed in the Powerstrip Device section of page.

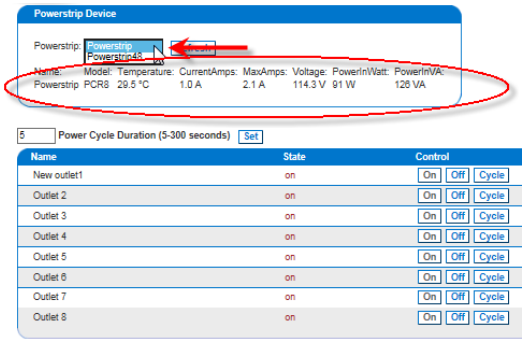
If power strips are down or cannot be reached, the message "Cannot communicate with power strip or outlet number not match, please check!" is displayed on the page in red.



All of the power strips you have permissions to access and that are connected to SX II are listed in the Powerstrip drop-down.

Information about the currently selected power strip is displayed under the Powerstrip drop-down -

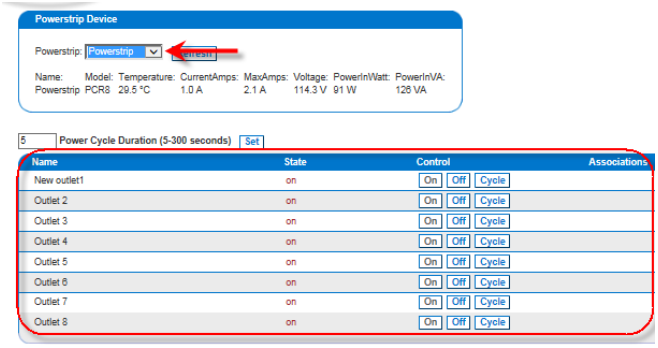
- Name
- Model
- Temperature
- Current Amps
- Maximum Amps
- Voltage
- Power in Watts
- Power in Volts Ampere



The currently selected powerstrip's outlet names, their current state, and their associated ports, if applicable, are displayed below the powerstrip information.

Use the On, Off and Cycle buttons on the page to control each of the powerstrip's outlets.

Select another powerstrip from the drop-down to view its information and control its outlets.



Control Powerstrip Outlets

To turn an outlet on:

1. From the Powerstrip drop-down, select the rack PDU (power strip) you want to turn on.
2. Click On next to the outlet you want to power on.
3. Click OK to close the Power On confirmation dialog. The outlet will be turned on and its state will be displayed as 'on'.

To turn an outlet off:

1. Click Off next to the outlet you want to power off.
2. Click OK on the Power Off confirmation dialog. The outlet will be turned off and its state will be displayed as 'off'.

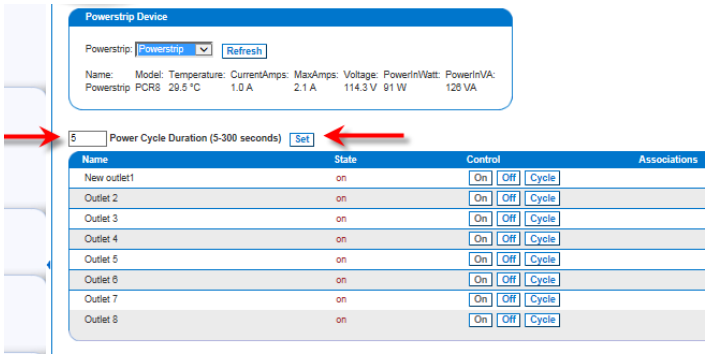
To cycle the power of an outlet:

1. Click Cycle next to the outlet you want to cycle. The Power Cycle Port dialog opens.
2. Click OK. The outlet then cycles (note that this may take a few seconds).
3. Once the cycling is complete a dialog will open. Click OK to close the dialog.

Specify Power Cycle Duration

To specify the duration between powering an outlet off and on when the cycle command is given, enter it in the "Power Cycle Duration (5-300 seconds)" field and select Set.

Note: If you are connecting a PX to SX II, it is recommended you set the power cycle time to 5 seconds.



Connect and Configure a Rack PDU (Powerstrip)

SX II allows you to connect rack PDUs (power strips) to SX II ports. You must configure these ports as power port via the SX II Port Configuration page.

A special Raritan cable or CSCSPCS -1 Rev.0C adapter is required to connect an SX II port to the Feature port of rack PDU.

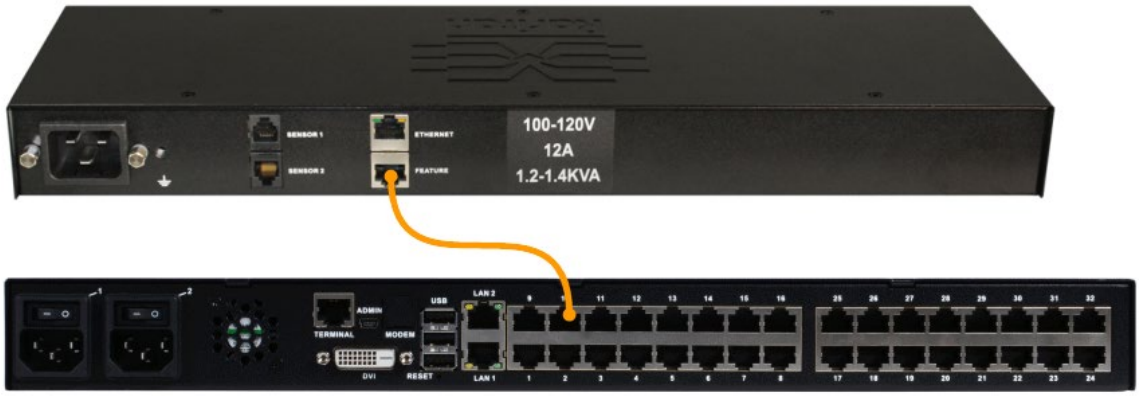
Important: When configuring your PDU, make sure the Feature port setting is "Power CIM".

Only Raritan rack PDUs are supported.

1. Configure an SX II port as power port.
2. On the Port Configuration page, click the port connected to power strip to open its Port Edit page.
3. Change the port type from "Serial" to "Power Strip".
4. change the port name, if needed.
5. Click OK. SX II attempts to communicate with the power strip. If communication is successful, the port is configured as a power port.

   Note: If the power strip is in not in support mode, a communication failure occurs. Update the power strip to support mode from the power strip application, then configure the port in SX II again..

6. Once a port is configured as power port, you can change outlet names on the Port Edit page, as well.



Remove a Power Association

When disconnecting target servers and/or rack PDUs from the device, all power associations should first be deleted. When a target has been associated with a rack PDU and the target is removed from the device, the power association remains. When this occurs, you are not able to access the Port Configuration for that disconnected target server in Device Settings so that the power association can be properly remove.

To remove a rack PDU association:

1. Select the appropriate rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That rack PDU/outlet association is removed and a confirmation message is displayed.

To remove a rack PDU association if the rack PDU has been removed from the target:

1. Click Device Settings > Port Configuration and then click on the active target.
2. Associate the active target to the disconnected power port. This will break the disconnected target's power association.
3. Finally, associate the active target to the correct power port.

Configure and Manage Users and Groups from the Remote Console

Note: These functions can also be performed using command line interface. See **Configure and Manage Users and User Groups Using CLI** *(on page 199).*

SX II stores an internal list of all user profiles and user groups.

User profiles and groups are used to determine access authorization and permissions. This information is stored internally. User passwords are stored in an encrypted format.

SX II allows the administrator to define groups with common permissions and attributes. They can then add users to the groups, and each user takes the attributes and permissions of that group.

Since the group permissions are applied to each individual in the group, permissions do not have to be applied to each user separately. This reduces the time to configure users.

For example, create a group called Modem Access that has permission to manage modems. Each user assigned to the Modem Access group can then manage the modem function; you do not have to assign each user a separate permission.

View a List of Users

- Click User Management > User List.

The User List page shows every user profile created to date, and for each one, lists:

- Username
- Full name
- User group

Users belong to a group and groups have privileges. Organizing the various users of your SX II into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose not to associate specific users with groups. In this case, you can classify the user as “Individual.”

Upon successful authentication, the appliance uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the appliance is allowed, and other features.

Note: These functions can also be manged using command line interface, see **Configure and Manage Users and User Groups Using CLI** *(on page 199) .*

User Groups

Every SX II is delivered the default user groups. These groups are listed in the User Groups drop-down on the Add User page.

- Admin

  Users that are members of this group have full administrative privileges to all functions.

  The original, factory-default user is a member of this group and has complete system privileges.

  In addition, the Admin user must be a member of the Admin group.

- Unknown

  Additionally, if the remote server does not identify a valid user group, the Unknown group is applied.

  This is the default group for users who are authenticated remotely using LDAP/LDAPS, RADIUS or TACACS+.

  Any newly created user is automatically put in this group until they are assigned to another group.

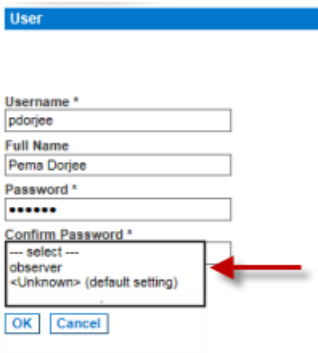
- Individual Group

  An individual group is essentially a "group" of one. That is, the specific user is in its own group and not affiliated with other groups.

  Use an individual group when you need a user account can have the same rights as a group.

  Individual groups can be identified by @ in the Group Name.

The default user groups cannot be deleted but you can create additional user groups that meet your needs and assign users to them, if needed.



User Profiles

User profiles serve two purposes:

- To provide users with a username and password to log in to SX II.
- To associate the user with a user group. The user group determines which functions and ports the user can access.

SX II is shipped with one user profile built in, the Admin user.

This user profile is associated with the Admin user group and has full system and port permissions. This profile cannot be modified or deleted.

Up to 254 user profiles per group are supported by SX II.

You can create a profile that is unique to each SX II user.

Alternatively, you can create a profile and assign multiple people to it. Each person assigned to the profile will then have the same privileges. This saves time but requires caution to ensure a user is not given inappropriate access to a function. Use this function to limit permissions as well. See ***Create a Group with Limited Access to SX II (IP Access Control List)*** (on page 78).

Local and Remote Authentication

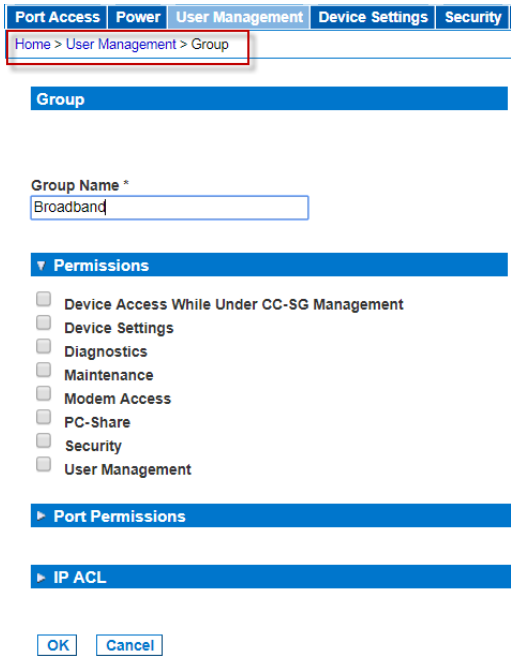
All users must be authenticated to access SX II.

SX II can be configured to authenticate users locally and/or remotely using LDAP/LDAPS, RADIUS or TACACS+. Remote user authentication is processed before local authentication if remote authentication is enabled. For details, see ***Configure User Authentication from the Remote Console*** (on page 85).

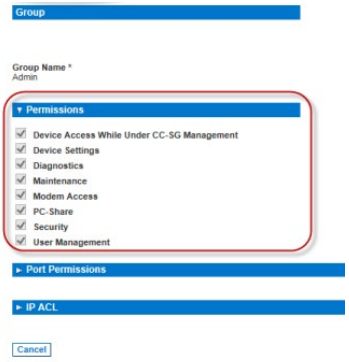
Add a User Group

1. Select User Management > Add New User Group or click Add on the User Group List page.

2. Type a descriptive name for the new user group into the Group Name field.



Set Group Permissions



3. Select the permissions to assign to the group.
   - Device Access While Under CC-SG Management - Allows users and user groups with this permission to directly access the SX II while it is under CC-SG management.

     SX II is accessed using an IP address when Local Access is enabled for the device in CC-SG.

     When a device is accessed directly while it is under CC-SG management, access and connection activity is logged on SX II.

     User authentication is performed based on SX II authentication settings.

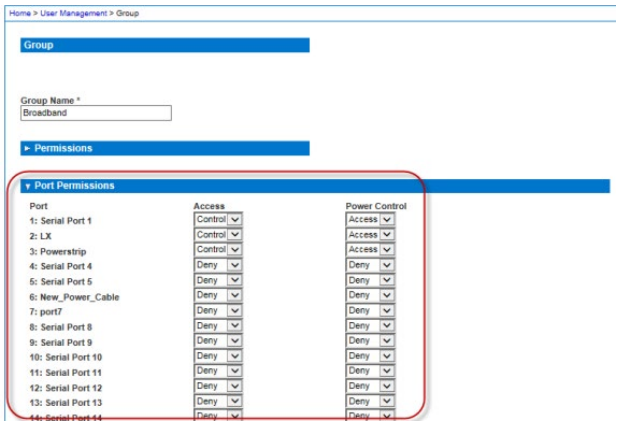
Note: The Admin user group has this permission by default.

- Device Settings - Network settings, date/time settings, port configuration, event management (SNMP, Syslog), and so on.
- Diagnostics - Network interface status, network statistics, ping host, trace route to host, SX II diagnostics.
- Maintenance - Backup and restore database, firmware upgrade, factory reset, reboot.
- PC-Share - Simultaneous access to the same target by multiple users.
- Security - SSL certificate, security settings, IP ACL.
- User Management - User and group management, remote, authentication, login settings.

***Important**: Selecting User Management allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions.*

- Modem Access - Displayed on the page when an external modem is connected to SX II. Select this option if you want the group to have access to the external modem. If broadband access is enabled for a supported Sierra Wireless modem, this permission allows the group to access SX II via the wireless modem, as well. See ***Connect and Enable Global Access to an External USB-Connected Broadband Modem*** (on page 132).

Set Port Permissions



4. Select the access permissions the group has to server ports and power control. The default is Deny.

   Select each port individually, or use the checkboxes at the bottom of the page to apply permissions to all ports.

   - Deny - Denied access completely.
   - View - View but not interact with the connected target.

- Control - Control the connected target.

  Control must be assigned to the group if power control access will also be granted.

5. Click OK to create the group and apply permissions.

For information on IP ACL, see ***Create a Group with Limited Access to SX II (IP Access Control List)*** (on page 78).

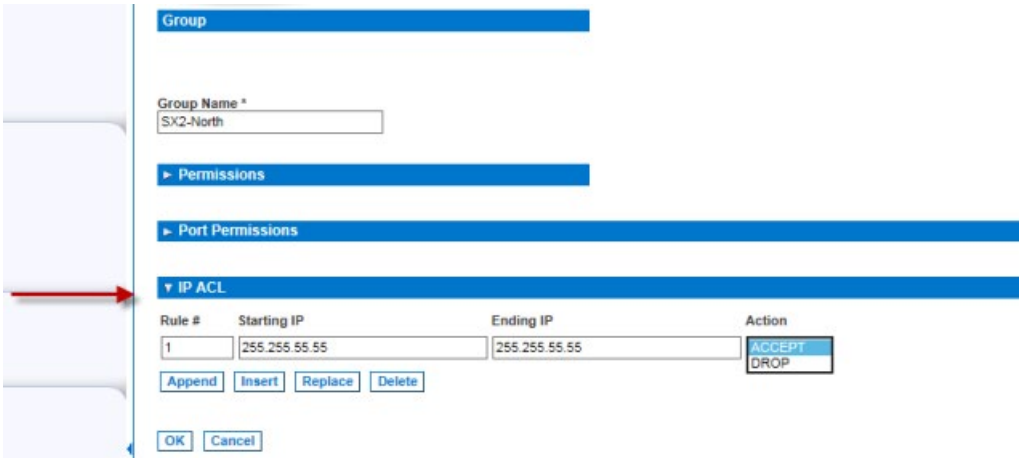
Create a Group with Limited Access to SX II (IP Access Control List)

Important: Exercise caution when using group-based IP access control. It is possible to be locked out of your SX II if your IP address is within a range that has been denied access.

This feature limits a user's access to the SX II by allowing you to assign them to a group that can only access the device through specific IP addresses.

This feature applies only to users belonging to the specific group. This is unlike the IP Access Control List feature that applies to all access attempts to the device. IP access control takes priority over group-based IP ACL and is processed first.

Use the IP ACL section of the Group page to add, insert, replace, and delete IP access control rules on a group-level basis.



To add (append) rules:

1. Type the starting IP address in the Starting IP field.
2. Type the ending IP address in the Ending IP field.
3. Choose the action from the available options:
   - Accept - IP addresses set to Accept are allowed access to the SX II device.
   - Drop - IP addresses set to Drop are denied access to the SX II device.
4. Click Append and then click OK. The rule is added to the bottom of the rules list. Repeat steps 1 through 4 for each rule you want to enter.

To insert a rule:

1. Enter a rule number (#). A rule number is required when using the Insert command.
2. Enter the Starting IP and Ending IP fields.
3. Choose the action from the Action drop-down list.
4. Click Insert and then click OK. If the rule number you just typed equals an existing rule number, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

To replace a rule:

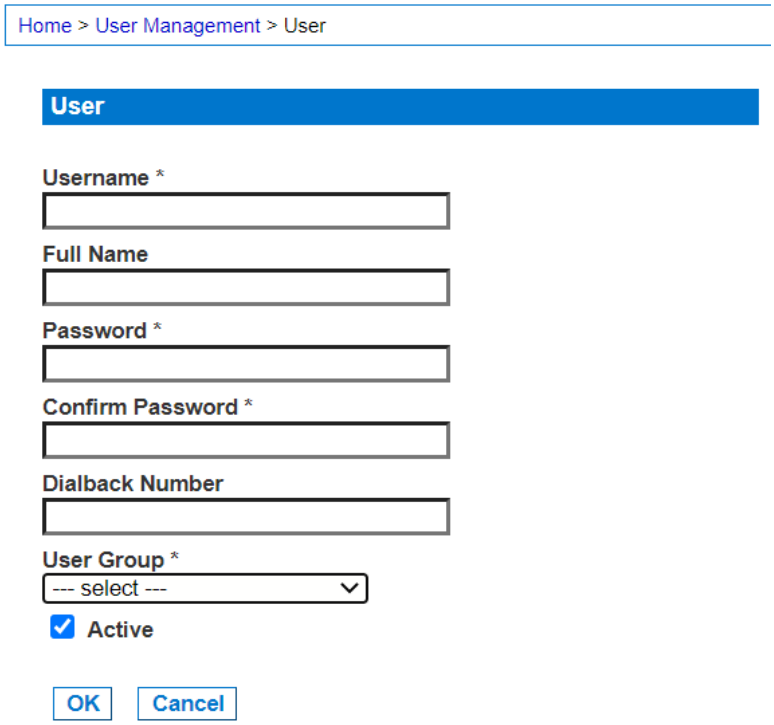
1. Specify the rule number you want to replace.
2. Type the Starting IP and Ending IP fields.
3. Choose the Action from the drop-down list.
4. Click Replace and then click OK. Your new rule replaces the original rule with the same rule number.

To delete a rule:

1. Specify the rule number you want to delete.
2. Click Delete.
3. When prompted to confirm the deletion, click OK and the click OK on the page to save the changes.

Create and Activate a User

1. Choose User Management > Add User.



2. Type a login name in the Username field. This is the name the user enters to log in to SX II. **Required**
3. Type the user's full name in the Full Name field.
4. Type a password in the Password field, and then type it again in the Confirm Password field. **Required**
   - The password is case sensitive.

   Note: If the strong password feature is enabled, there are other password requirements. See Strong Passwords for details.
5. Associate the user with a user group by selecting from the User Group drop-down. **Required**

   If you do not want to associate this user with an existing User Group, select Individual Group from the drop-down list. For more information about permissions for an Individual Group, see Setting Permissions for an Individual Group.
6. Enter a Dialback Number for modem usage.
7. Decide whether or not to activate this profile immediately. By default, the Active checkbox is selected.

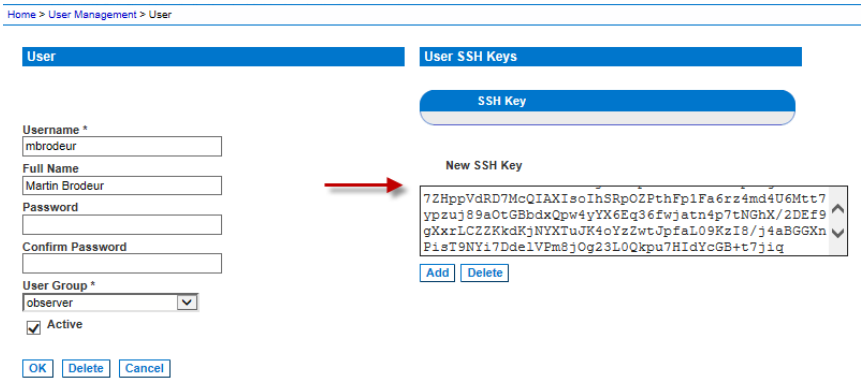
To deactivate this account, deselect this checkbox. You can return at any time and activate the user when necessary.

8. Click OK. The page closes.
9. The user profile is created and should appear in the User List page. Reopen the user's page and the SSH key section is enabled. If needed, assign an SSH key to the user profile. See ***Add SSH Client Certificates for Users*** (on page 81).

Add SSH Client Certificates for Users

If needed, SSH (Secure Shell) Client Authentication keys can be added to a user. The user must first be created before the client certificate can be added. Up to 10 SSH keys can be added for a user.

1. Select User Management > User List, then click on the name of the user you want to add a SSH client certificate to. The User's page opens.



2. Enter the SSH key data in the SSH Key Data box. This data is the rsa_id.pub key generated for your client.

   Linux users should delete "name@local host" that appears at the end of the generated key when adding public keys.
3. Click Add.

   The SSH key data is validated in several ways:

   a. Specified keytype is validated: [ssh-rsa|ssh-dsa|ecdsa-sha2-nistp256| ecdsa-sha2-nitsp384| ecsda-sha2-nitsp512]

   b. Keytype is followed by whitespace, followed by the base64 data.

   c. Base64 data is validated.

   d. Whitespace and any characters after the base64 are dropped from the key data.
4. The key data should be used for authentication and you should not have to enter a password.

To delete an SSH key:

1. Click the checkbox next to the key you want to delete.

2. Click Delete.
3. Click OK when prompted to confirm.

Edit or Deactivate a User

Note: This function can also be performed using command line interface. See **Configure and Manage Users and User Groups Using CLI** *(on page 199).*

1. Choose User Management > User List. The User List page opens.
2. Click the checkbox the user profile you want to edit or deactivate.
3. You can change any of the fields except the Username field.
4. For security reasons, the password is not displayed. To change the profile's password, type a new password in the Password and Confirm Password fields. If you leave these fields as is, the password is unchanged.
5. Click OK when finished. The user profile is modified.

Delete a User

Note: This function can also be performed using command line interface. See Delete Users Using CLI.

1. Choose User Management > User List. The User List page opens.
2. Click the checkbox to the left of the user profile you want to delete. You can select more than one.
3. Click Delete. You are prompted to confirm the deletion.
4. Click OK. The selected user profiles are deleted.

View Users by Port

The User By Ports page lists all authenticated local and remote users and ports they are being connected to.

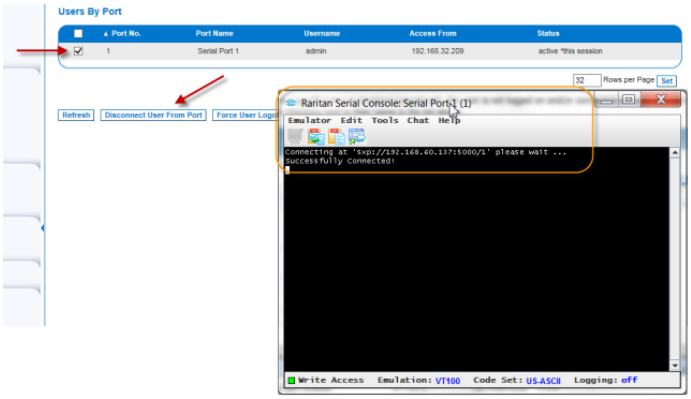
- If the same user is logged on from more than one client, their username appears on the page for each connection they have made. For example, if a user has logged on from two (2) different clients, their name is listed twice.
- This page contains the following user and port information:
- Port Number - port number assigned to the port the user is connected to
- Port Name - port name assigned to the port the user is connected to
- Note: If user is not connected to a target, 'Local Console' or 'Remote Console' is displayed under the Port Name.
- Username - username for user logins and target connections
- Access From - IP address of client PC accessing the SX II
- Status - current Active or Idle status of the connection

To view users by port:

- Choose User Management > User by Port. The Users by Port page opens.

Disconnect a User from a Port

You can disconnect a user from a specific port *without* logging them off of SX II. For example, if a user is connected to Serial Port 1 via Raritan Serial Console (RSC), you can disconnect them from the port.



This is unlike the force user logoff SX II function that disconnects users from the target port and logs them off of SX II. See Logging Users Off the SX II (Force Logoff) for information.

1. Choose User Management > Users by Port. The Users by Port page opens.

2. Select the checkbox next to the username of the person you want to disconnect from the target.
3. Click "Disconnect User from Port".
4. Click OK on the confirmation message to disconnect the user.
5. A confirmation message is displayed to indicate that the user was disconnected.

If the "Disconnect User from Port" is disabled, the user is not logged on to a port at the current time or you did not select the checkbox next to their name in the list above..

Log a User Off of SX II (Force Logoff)

If you are an administrator or have user management permissions, you are able to log off any authenticated user who is logged on to SX II. Users can also be disconnected at the port level. See Disconnecting Users from Ports.

1. Choose User Management > Users by Port. The Users by Port page opens.
2. Select the checkbox next to the username of the person or persons you want to disconnect from the target.
3. Click "Force User Logoff".
4. Click OK on the Logoff User confirmation message.

If the "Force User Logoff" button is disabled (grayed out), the user is not logged on and/or connected to a port at the time or you have not selected the checkbox next to their name in the list above.

Configure User Authentication from the Remote Console

SX II requires users be authenticated to access the appliance.

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

Users can be authenticated via SX II locally or remotely.

By default, users are authenticated locally; you must enable remote authentication. When remote authentication is enabled, there is an option to allow or deny local authentication as a fallback. See Fallback to Local Authentication.

When the SX II is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

SX II provides several options to remotely authenticate users -

- LDAP/LDAPS
- RADIUS
- TACACS+

For information on configuring LDAP, RADIUS and TACACS+ servers, see Configure LDAP, RADIUS and TACACS+ Servers.

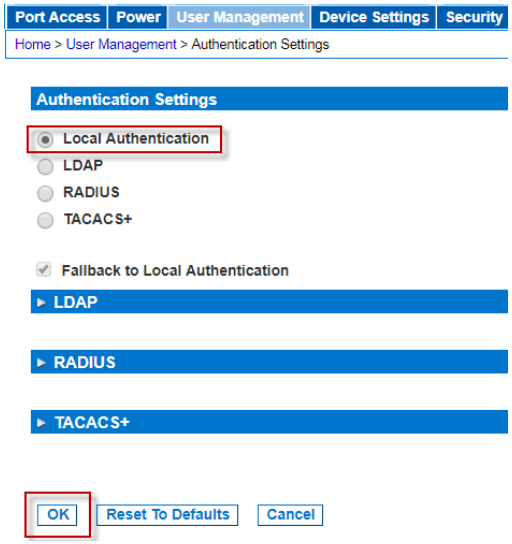
For information on enabling Telnet and SSH in SX II, see ***Enable Telnet (Optional)*** (on page 105) and ***Enable SSH Access (Optional)*** (on page 104).

Note: You can also configure remote authentication via command line interface. See **Configure User Authorization and Authentication Services Using CLI** *(on page 203).*

Enable Local User Authentication

Users are validated based on their username and password from a local database.

When Fallback to Local Authentication is enabled, local authentication will be used when remote authentication is enabled but the user is not found, or when remote servers are not available. See Fallback to Local Authentication.



1. Choose User Management > Authentication Settings. The Authentication Settings page opens.
2. Select Local Authentication.
3. Click OK to save.

To return to factory defaults:

- Click Reset to Defaults.

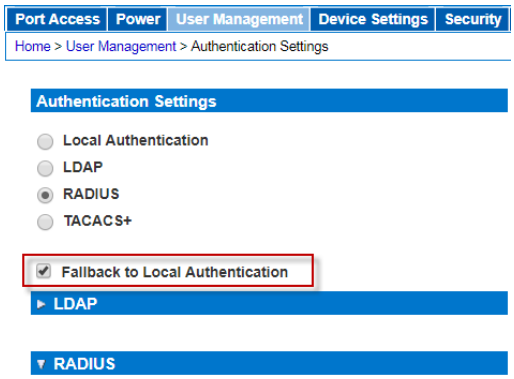
Fallback to Local Authentication

Fallback to Local Authentication allows local authentication to be performed when remote authentication fails for any reason. A remote authentication server is considered available if the server can be pinged and ICMP communication is available between the SX II and the authentication server.

Fallback is enabled by default. Deselect the fallback option if you do not want local authentication to be used.

CC-SG users can always connect to SX II regardless of the fallback setting.

To configure fallback to local authentication:



1. Choose User Management > Authentication Settings. The Authentication Settings page opens.
2. Select or deselect the Fallback to Local Authentication checkbox. This option works with remote authentication, so another remote authentication option must be selected when fallback is selected.
3. Click OK to save.

Enable LDAP/LDAPS Authentication

Note: When configuring the LDAP server, the query string format on the server should contain the name of the group configured on SX II.

You can use the Lightweight Directory Access Protocol (LDAP) to authenticate SX II users instead of local authentication.

Lightweight Directory Access Protocol (LDAP/LDAPS) is a networking protocol for querying and modifying directory services running over TCP/IP.

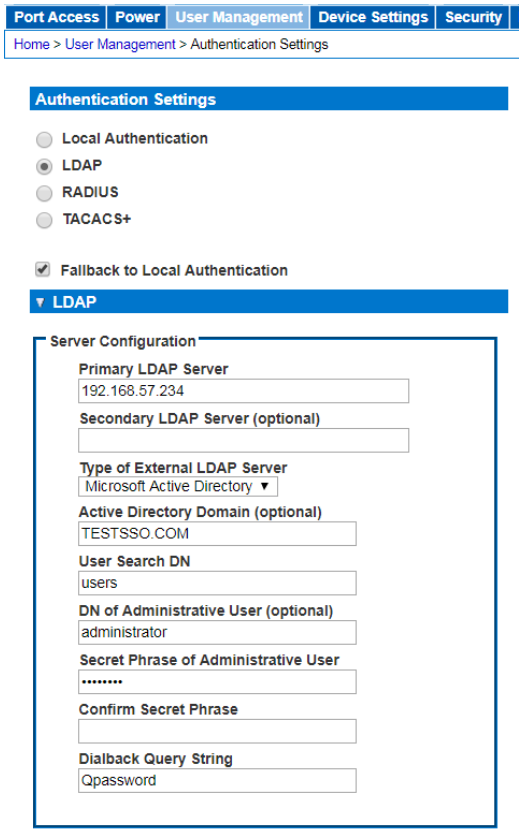
A client starts an LDAP session by connecting to an LDAP/LDAPS server (the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

Reminder: Microsoft Active Directory functions natively as an LDAP/LDAPS authentication server.

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Select the LDAP radio button to enable the LDAP section of the page.

   The LDAP section expands. If it does not, click on the LDAP section header.
3. Select Fallback to Local Authentication if you want local authentication to be performed if remote authentication fails. See ***Fallback to Local Authentication*** (on page 87).

Server Configuration



4. In the Primary LDAP Server field, type the IP address or host name of your LDAP/LDAPS remote authentication server.
5. **Optional** In the Secondary LDAP Server field, type the IP address or host name of your backup LDAP/LDAPS server (up to 256 characters). When the Enable Secure LDAP option is selected, the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field.
6. Select the type of External LDAP Server.
   - Generic LDAP Server.
   - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.

- Type the name of the Active Directory Domain if you selected Microsoft Active Directory. For example, acme.com. Consult your Active Directive Administrator for a specific domain name. **Optional**

7. In the User Search DN field, enter the Distinguished Name of where in the LDAP database you want to begin searching for user information. An example base search value might be: cn=Users,dc=raritan,dc=com. Consult your authentication server administrator for the appropriate values to enter into these fields.
8. DN of Administrative User: Optional. Complete this field if your LDAP server only allows administrators to search user information using the Administrative User role.

   Consult your authentication server administrator for the value. Example: cn=Administrator,cn=Users,dc=testradius,dc=com.
9. If you entered a Distinguished Name for the Administrative User, you must enter the password that will be used to authenticate the Administrative User's DN against the remote authentication server.

   Enter the password in the Secret Phrase field and again in the Confirm Secret Phrase field.
10. Dialback Query String: Enter the string. Ifyou are using Microsoft Active Directory, enter the following string: msRADIUSCallbackNumber

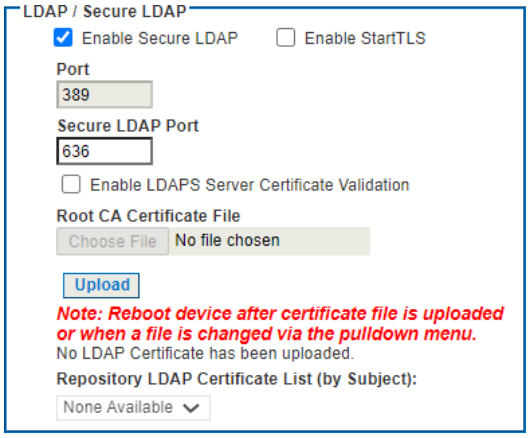
    LDAP/Secure LDAP
11. For an encrypted connection, select the Enable Secure LDAP checkbox to use SSL, or select the Enable StartTLS checkbox to use StartTLS. Both options enable the Enable LDAPS Server Certificate Validation checkbox.
    - For an unsecured connection, do not enable Secure LDAP or StartTLS. The default port for unsecured connections is 389. Use the standard LDAP TCP port or specify another port.
    - SSL is a cryptographic protocol that allows SX II to communicate securely with the LDAP/LDAPS server. The default Secure LDAP port is 636, or you may specify another port. This field is used only when Enable Secure LDAP is selected.
    - StartTLS is a command that upgrades an unsecured connection to a secure connection using SSL/TLS. StartTLS does not require a specific port. The standard LDAP port 389 is default.
12. Select the Enable LDAPS Server Certificate Validation checkbox to use the previously uploaded root CA certificate file to validate the certificate provided by the server. If you do not want to use the previously uploaded root CA certificate file, leave this checkbox deselected. Disabling this function is the equivalent of accepting a certificate that has been signed by an unknown certifying authority. This checkbox is only available when the Enable Secure LDAP checkbox has been enabled.

Note: When the Enable LDAPS Server Certificate Validation option is selected, in addition to using the Root CA certificate for validation, the server hostname must match the common name provided in the server certificate.

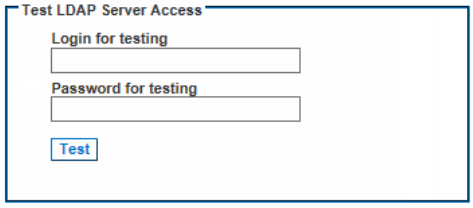
13. If needed, upload the Root CA Certificate File. This field is enabled for secured connections only. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use Browse to navigate to the certificate file.

    If the certificate has been uploaded to the Certificate Repository, select it in the Repository LDAP Certificate List (by Subject) list. See Certificate Repository for details.

    Note: You must reboot the device after the certificate file is uploaded or when a different file is chosen from the repository.



Test LDAP Server Access



14. To test the LDAP configuration, enter the login name and password in the "Login for testing" field and the "Password for testing" field, respectively. Click Test.

    This is the username and password you entered to access the SX II. It is also username and password the LDAP server uses to authenticate you.

    The SX II then tests the LDAP configuration from the Authentication Settings page. This is helpful due to the complexity sometimes encountered when configuring the LDAP server and SX II for remote authentication.

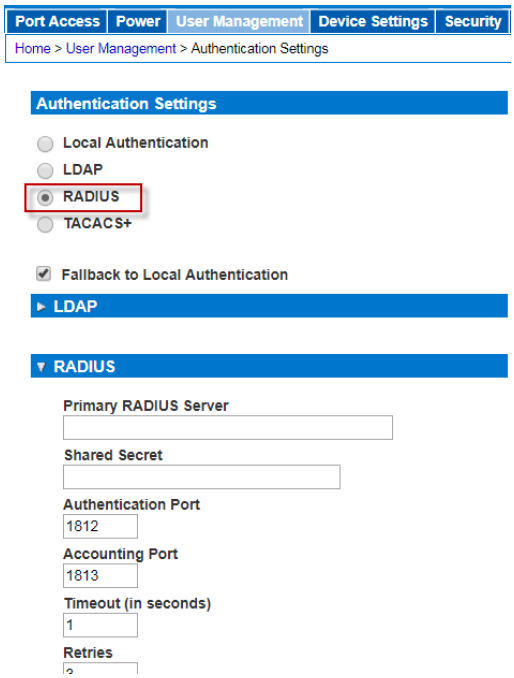
Once the test is completed, a message is displayed that lets you know the test was successful or, if the test failed, a detailed error message is displayed. It also can display group information retrieved from remote LDAP server for the test user in case of success.

Enable RADIUS Authentication

Note: When configuring the RADIUS server, the Filter-ID format for the users on the server should have the following format "Raritan:G{GroupOnSX}:D{DialbackNumber}".

You can use Remote Authentication Dial-In User Service (RADIUS) to authenticate SX II users instead of local authentication. RADIUS is an AAA (authentication, authorization, and accounting) protocol for network access applications.

The following authentication types are supported: PAP, CHAP, MS-CHAPv1, and MS-CHAPv2.



1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click the RADIUS radio button to enable the RADIUS section of the page. The section expands. If it does not, click the section header to expand it.
3. Select Fallback to Local Authentication if you want local authentication to be performed if remote authentication fails. See ***Fallback to Local Authentication*** (on page 87).

4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively.
5. In the Shared Secret fields, type the server secret used for authentication.

   The shared secret is a character string that must be known by both the SX II and the RADIUS server to allow them to communicate securely. It is essentially a password.
6. The Authentication Port default is port is 1812 but can be changed as required. Port range is 1-65535.
7. The Accounting Port default port is 1813 but can be changed as required. Port range is 1-65535.
8. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.
9. The timeout is the length of time the SX II waits for a response from the RADIUS server before sending another authentication request.
10. The default number of retries is 3 Retries.

    This is the number of times the SX II will send an authentication request to the RADIUS server.
11. Choose the Global Authentication Type from among the options in the drop-down list:
    - PAP - With PAP, passwords are sent as plain text. PAP is not interactive. The user name and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.
    - CHAP - With CHAP, authentication can be requested by the server at any time. CHAP provides more security than PAP.
    - MS-CHAPv2 - MS-CHAPv2 provides stronger security than the above two. Selecting this option will support both MS-CHAPv1 and MS-CHAPv2

Test RADIUS Server Access

To test the configuration, enter the login name and password in the "Login for testing" field and the "Password for testing" field, respectively. Click Test.

This is the username and password you entered to access the SX II. It is also username and password the RADIUS server uses to authenticate you.

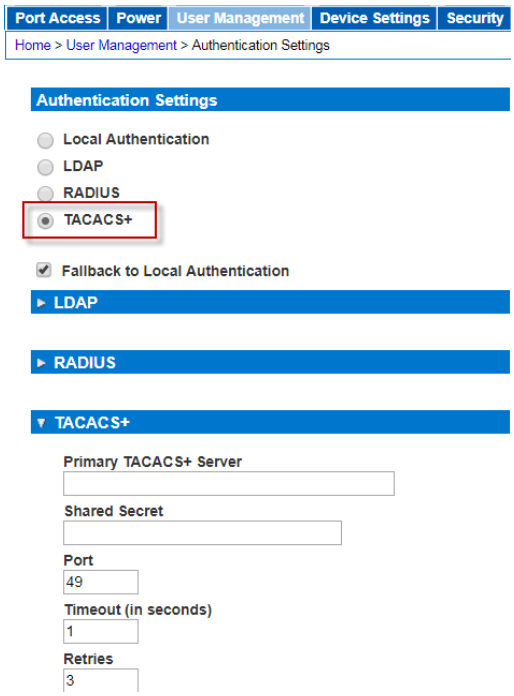
The SX II then tests the configuration from the Authentication Settings page. This is helpful due to the complexity sometimes encountered when configuring the server and SX II for remote authentication.

Once the test is completed, a success message or a detailed error message is displayed. It also can display group information retrieved from remote server for the test user in case of success.

Enable TACACS+ Authentication

Note: When configuring the TACACS+ server, a dominionsx service should be added. A user-group attribute under this service should contain the name of a group configured on the SX II . A user-dialback field under this service would contain the modem dialback number for this user.

You can use the Terminal Access Controller Access-Control System Plus (TACACS+) to authenticate SX II users instead of using local authentication.

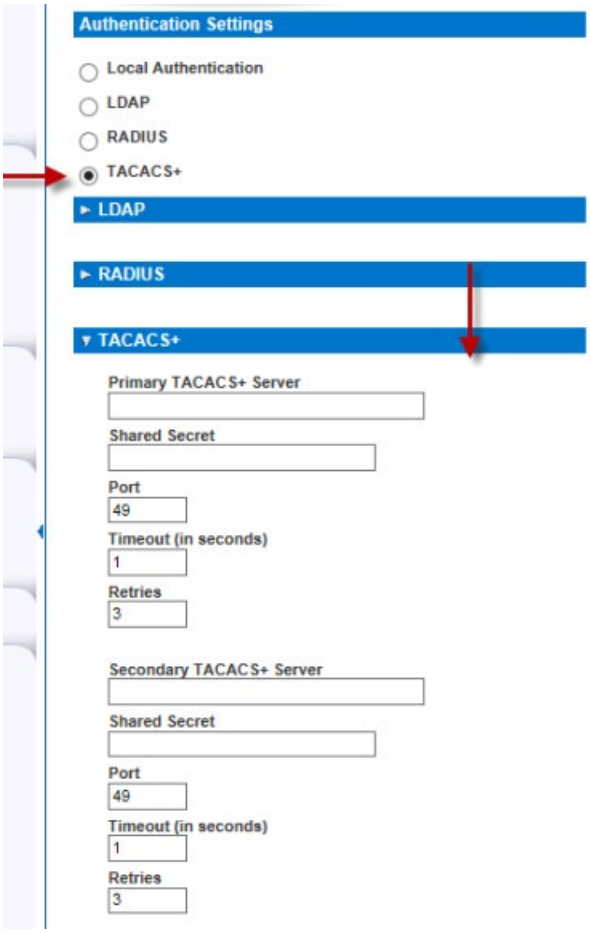


1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click the TACACS+ radio button to enable the TACACS+ section of the page.

   The section expands. If it does not, click the section header to expand it.
3. Under Primary TACACS+, type the IP address of the TACACS+ server and the port on which it is listening (default is 49) in the IP Address and Port fields.
4. Fill in the Shared Secret field. Also known as a key, this field is necessary for encryption and mutual identification with the TACACS+ server.
5. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.
6. The timeout is the length of time the SX II waits for a response from the TACACS+ server before sending another authentication request.
7. The default number of retries is 3 Retries.

This is the number of times the SX II will send an authentication request to the TACACS+ server.

8. If you have a backup TACACS+ server, enter the same information in the Secondary TACACS+ fields.
9. Click OK. TACACS+ authentication is enabled.



Configure SX II Network Settings from the Remote Console

The configuration settings described in ***Initial SX II Configuration from the Remote Console*** (on page 12) are the same that apply when making any changes.

Choose Failover or Isolation Mode

Configure SX II for Dual LAN Failover Mode (on page 96): In failover mode, LAN status is used to determine which LAN port is used in failover. LAN port #1 is switched as default. If the switched LAN port status is down, then the other LAN port will be switched to until a LAN port whose status is on is found.

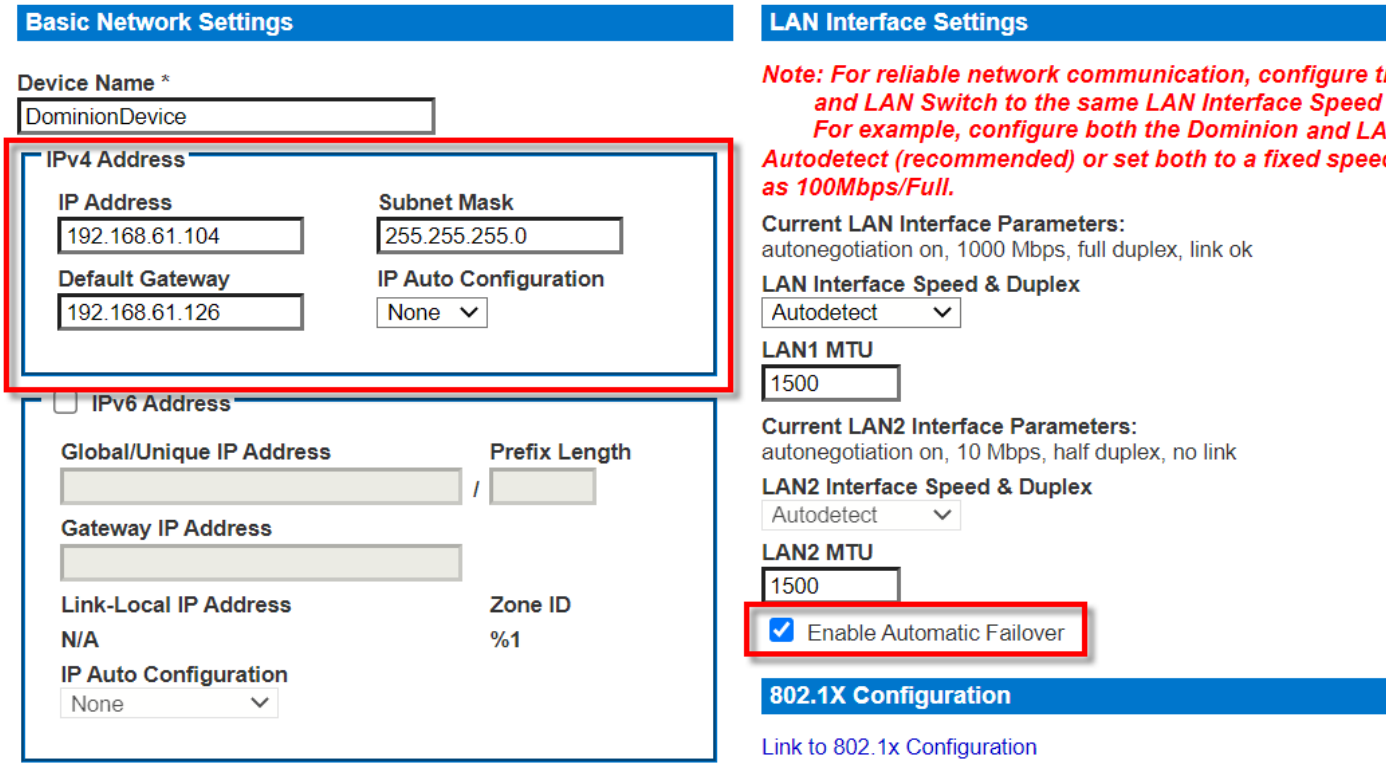
Configure SX II for Dual LAN Isolation Mode (on page 97)

Configure SX II for Dual LAN Failover Mode

LAN1 and LAN2 share the same IP address to support automatic failover.

LAN1 is the primary port. If LAN1 fails, LAN2 is used to access SX II.

1. Select Device Settings > Network to open the Device Network Settings page.
2. Set the IP Auto Configuration to *None* in the IPv4 section.
3. Select the "Enable Automatic Failover" checkbox under LAN Interface Settings to enable failover.
4. Manually specify the network parameters by entering the Default Gateway.
5. Enter the IPv4 IP Address, if needed. The default IP address is 192.168.0.192.
6. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.
7. The LAN1 settings are applied to LAN2 if failover occurs.



8. Complete the IPv6 sections, if applicable.
9. Select the IP Auto Configuration.

   If *None* is selected, you must manually specify -

- Global/Unique IP Address - this is the IP address assigned to SX II.
- Prefix Length - this is the number of bits used in the IPv6 address.
- Gateway IP Address.

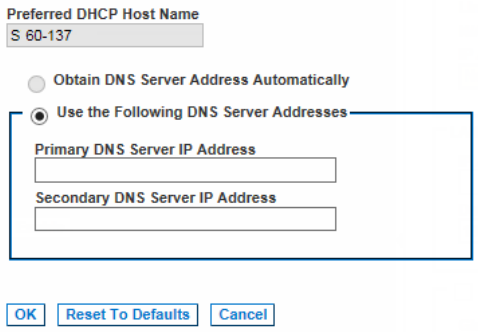
Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with. Read-Only

10. Next, select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when SX II is configured in DHCP mode



11. Set the LAN 1/LAN 2 Interface Speed and Duplex, and the LAN 1/LAN 2 MTU.
    - Valid range for MTU is 576 - 1500.
12. When finished, click OK. Your SX II device is now network accessible.

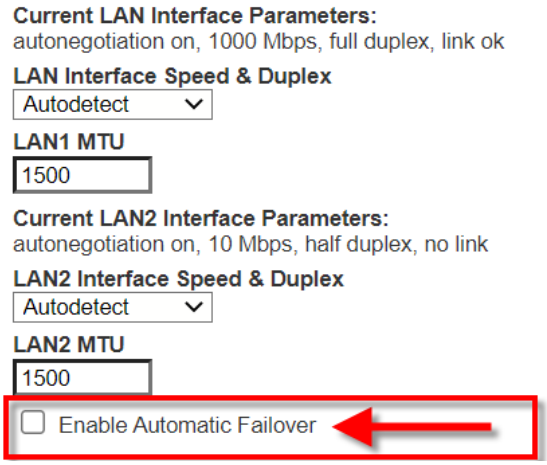
Configure SX II for Dual LAN Isolation Mode

Isolation mode allows you to access each LAN port independently using different IP addresses.

Failover is not supported in this mode.

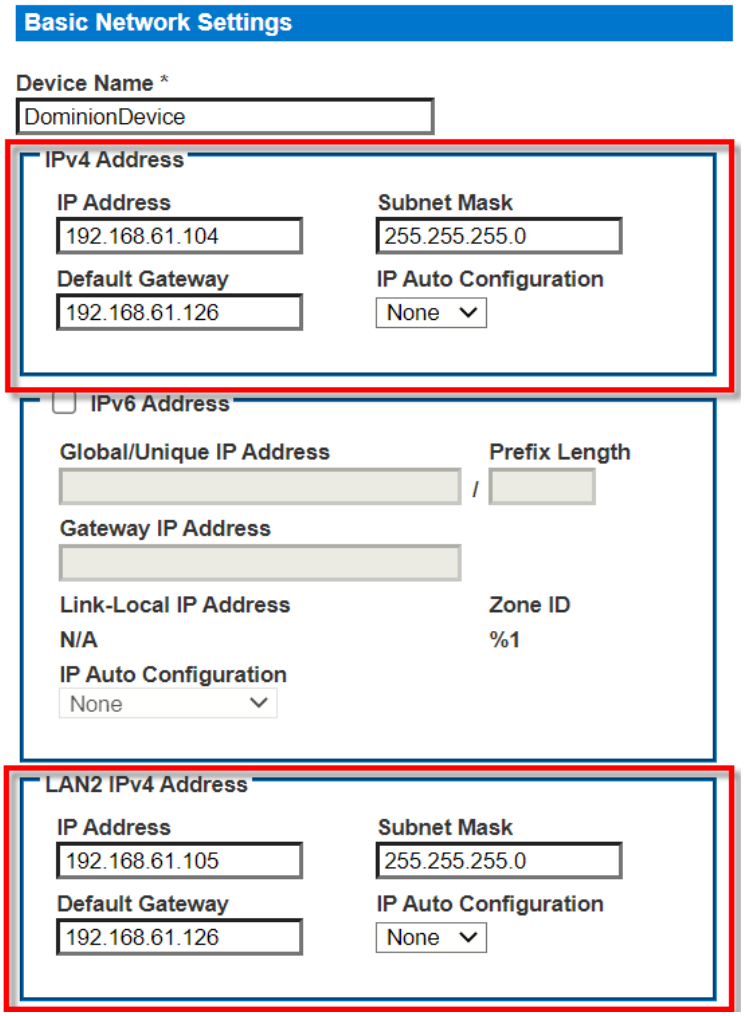
1. Select Device Settings > Network to open the Device Network Settings page.
2. Set the IP Auto Configuration to *None* in the IPv4 section.

3. Ensure the "Enable Automatic Failover" checkbox is not selected.



4. If needed, manually specify the network parameters by entering the Default Gateway and then complete the steps that follow.
5. Enter the IP address you want to use to connect to the SX II LAN1. The default IP address is 192.168.0.192.
6. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.
7. In the LAN2 IPv4 section, set the IP Auto Configuration to *None*.
8. Enter the IP address you want to use to connect to the SX II LAN2.

9. Enter the LAN2 IPv4 Default Gateway and Subnet Mask.



10. Complete the IPv6 sections, if applicable.
11. Select the IP Auto Configuration.

    If *None* is selected, you must manually specify -

    - Global/Unique IP Address - this is the IP address assigned to SX II.
    - Prefix Length - this is the number of bits used in the IPv6 address.
    - Gateway IP Address.

    Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

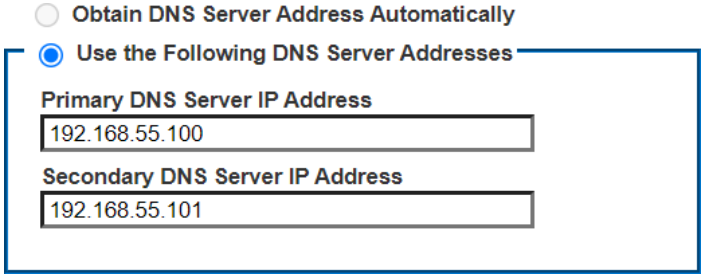
    Note that the following additional, read-only information appears in this section -

    - Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.

- Zone ID - Identifies the device the address is associated with. Read-Only

12. Select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when SX II is configured in DHCP mode



13. Set the LAN 1/LAN 2 Interface Speed and Duplex, and the LAN 1/LAN 2 MTU.
    - Valid range for MTU is 576 - 1500.
14. When finished, click OK.

    Your SX II device is now accessible via the LAN1 IP address and the LAN2 IP address.

Reset Network Settings to Factory Defaults

1. Select Device Management > Network to open the Network Settings page.
2. Click "Reset to Defaults" at the bottom of the page.

Enable Auto Script from the Remote Console for Use with TFTP or a USB Stick

Use this feature to copy the same settings to each of your SX IIs.

To do this, a configuration script file with the SX II's settings is created.

Example Script

```
config
localport
config enable false
```

Script Result Example

```
config
Config > localport
Config > LocalPort > config enable false
Local port configuration successful.
Config > LocalPort >
```

Create the file and then do one or both of the following to distribute it to the appliances -

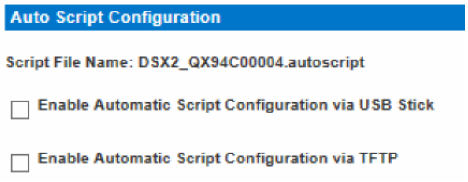
- Save the file to a TFTP server with the same name DSX2_SERIAL.autoscript. The first time a new SX II boots up, it contacts the DHCP server and retrieves the IP address of the appliance, and the DHCP server sends the SX II the TFTP server IP address.

  Once contacted, the configuration file is sent from the TFTP server, the configuration settings are applied to the appliance, and the appliance reboots.

  No manual intervention is required with this method.

  Note that SX II must receive the TFTP server address from one of these settings:

  - DHCP next-server (siaddr)
  - TFTP server address (option 66). This option takes precedence if both are specified.
- Save the file to USB stick. The file can then be brought to each appliance and used to configure it.

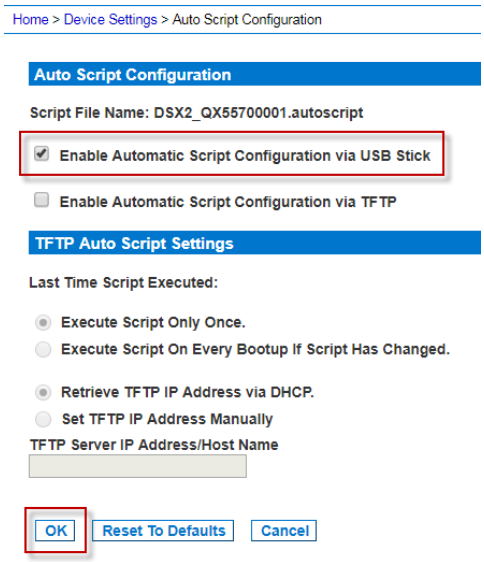


1. Access and configure the SX II you want to create a configuration file from.
2. Select Device Settings > Auto Configuration.
3. The name of the script is listed at the top of the Auto Script Configuration section. Read-only

Enable automatic script configuration via USB stick:

1. Prepare your USB stick and then plug it in to a USB port on the front or back of SX II. See ***Prepare a USB Stick for an Auto Configuration File*** (on page 103).
2. Select the "Enable Automatic Script Configuration via USB Stick" checkbox.

3. Click OK to create the script. A success message is displayed on the page.



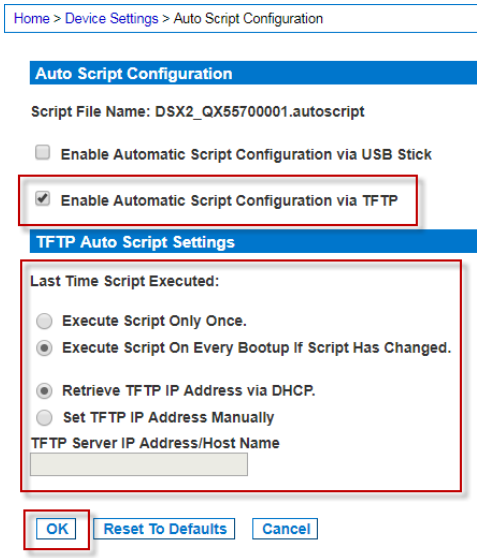
Enable automatic script configuration via TFTP server:

1. Select the "Enable Automatic Script Configuration via TFTP Stick" checkbox.
2. The TFTP Auto Script Settings section is enabled.
3. Select when scripts are run on the appliances -
   - Execute Script Only Once - the script will only be executed on the appliance the first time it boots up and not again. Changes must be made manually afterward.
   - Execute Script On Every Bootup If Script Has Changed - updates are applied to the appliances upon bootup when the script changes.

     Note that SX II only runs a script if it is different from the last script that was run. This applies regardless of the option selected here.

     SX II remembers most recently executed script, including the time the script was run.
4. Select how the IP address is configured -
   - Retrieve TFTP IP Address via DHCP - Note that to do this, IP auto configuration must set to DHCP and enabled on the SX II. See Disable or Enable DHCP in SX II.
   - Set TFTP IP Address Manually - enter the IP address in the field provided.

5. Click OK.



Prepare a USB Stick for an Auto Configuration File

Do the following in order to prepare your USB stick -

1. Plug the USB stick into a client machine.
2. Create an empty file named `!automatic_config`.
3. Create a file named `credential` that contains the SX II username and password. Use the following syntax -

   ```
   username=<user name>
   password=<password>
   ```

   Note: This is an Administrator user only. No other level user can use this function.

4. Create a script file named `<Device_Type>_<Serial_Number_Of_Device>.autoscript` containing all of the scripts that need to be executed on the appliance to configure it.
5. Copy all above files to the top directory of the USB stick.
6. Remove any file named `<Device_Type>_<Serial_Number_Of_Device>_result.txt`.
7. Following are examples of the files you should have on your USB in the end.

   ```
   !automatic_config
   credential
   DSX2_QVY4C00007.autoscript
   ```

8. Add other script files for other devices on the same USB stick, if needed.

9. Safely remove the USB stick from the client machine when done.

Execute Auto Configurations with a USB Stick

Following are steps to configure SX IIs using an auto configuration from a USB stick.

Prepare the USB stick and put the auto configuration file on it. See and , if you have not already done so.

1. Make sure device is in working condition.
2. Plug the prepared USB stick in to a USB drive on either the front or back of the SX II you are configuring.
3. The script executes automatically after validating the username and password credentials.
4. Once the script finishes, SX II beeps twice and the `<Device_Type>_<Serial_Number_Of_Device>_result.txt` file is generated and saved at the top directory of the USB stick.
5. You can then unplug the USB stick.

Important - the script will stop executing if you unplug the USB stick prior to its completion.

Configure Device Settings from the Remote Console

Enable SSH Access (Optional)

SSH is enabled by default.

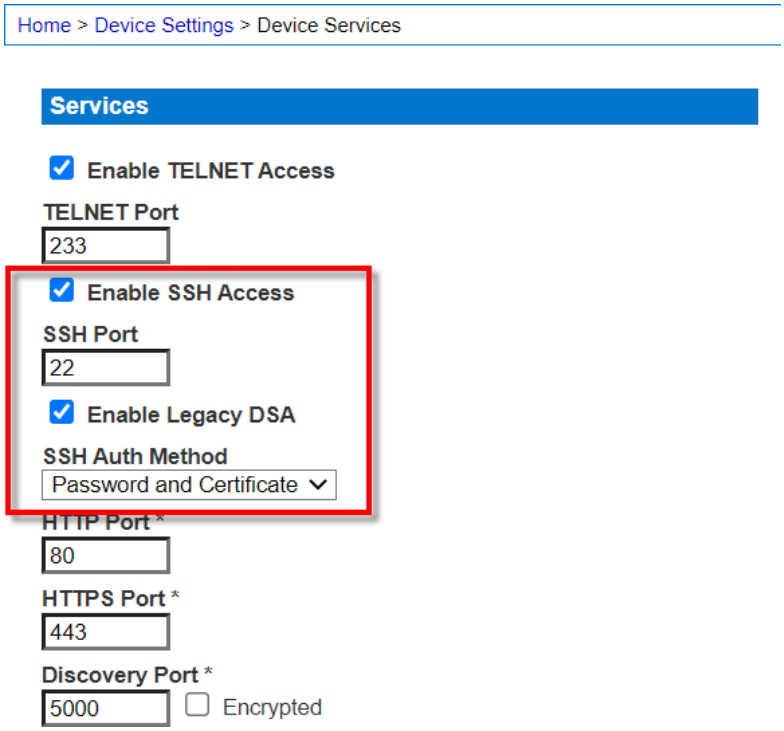
For information on required open ports and port protocols, see ***Port Access Protocol Requirements*** (on page 241).

Note that SSH can be disabled or enabled via Remote Console or command line interface (CLI). See ***Configure Device Settings Using CLI*** (on page 211).

1. Select Device > Device Settings to open the Device Services page.
2. Check the Enable SSH Access checkbox and complete the SSH Port.
3. If needed, select the Enable Legacy DSA checkbox.
4. Select the SSH Auth Method:
   - Password Only: Do not allow any configured certificate authentication
   - Certificate Only: Do not allow any password login to the SSH
   - Password and Certificate: Allow both authentication methods access to the device

   See ***Add SSH Client Certificates for Users*** (on page 81) for help with certificates.

5. Click OK to save.



Enable Telnet (Optional)

Due to the lack of security, the username, password and all traffic is in clear-text on the wire.

Telnet must be enabled before it can be used; is disabled by default.

Note that Telnet can be disabled or enabled via Remote Console or command line interface (CLI). See ***Configure Device Settings Using CLI*** (on page 211).

For information on required open ports and port protocols, see ***Port Access Protocol Requirements*** (on page 241).

1. Select Device Settings > Device Services to open the Device Services page.
2. Change the default port, if needed.
3. Check the Enable Telnet Access checkbox and enter the Telnet Port. Click OK to save.

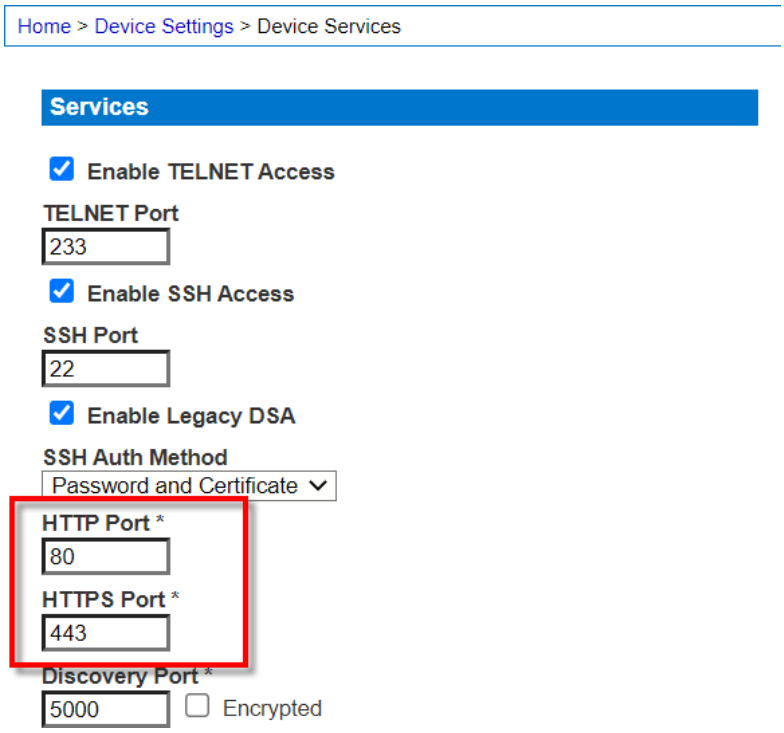
Change HTTP and HTTPS Port Settings

If needed, change HTTP and/or HTTPS ports used by SX II. For example, if you are using the default HTTP port 80 for another purpose, changing the port ensures the appliance does not attempt to use it.

For information on required open ports and port protocols, see ***Port Access Protocol Requirements*** (on page 241).

Note that HTTP/HTTPS can be disabled or enabled via Remote Console or command line interface (CLI). See ***Configure Device Settings Using CLI*** (on page 211).

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the new ports in the HTTP Port and/or HTTPS Port fields.
3. Click OK.



Change the TCP Discovery Port

SX II discovery occurs over a single, configurable TCP Port.

The default is Port 5000, but you can change it to use any TCP port except 80 and 443.

To access SX II from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured on this page.

The device will transmit information about itself (make,model,firmware version,encryption) in clear text unless the encryption option is selected.

For information on required open ports and port protocols, see ***Port Access Protocol Requirements*** (on page 241).

Note that TCP discovery port can be configured via Remote Console or command line interface (CLI). See ***Configure Device Settings Using CLI*** (on page 211).

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the Discovery Port.
3. Select the Encrypted checkbox to encrypt the transmission of device information.
4. Click OK.

Enable Direct Port Access

Direct Port Access allows users to bypass having to use the SX II's Login dialog and Port Access page.

There are three methods to access ports directly.

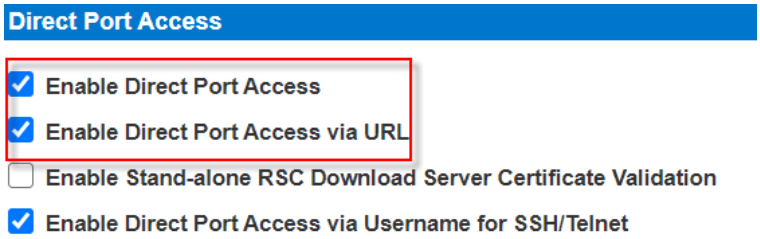
Note that Direct Port Access can be configured via Remote Console or command line interface (CLI). See ***Configure Direct Port Access Using CLI*** (on page 212).

"Enable Direct Port Access" and "Enable Direct Port Access via URL":

- Direct Port Access via URL - This feature provides the ability to directly access a port via HTTP/HTTPS by using one of following syntax:
  - `https://IPaddress/dpa.asp?username=username&password=password&port=port number`
  - `https://IPaddress/dpa.asp?username=username&password=password&portname=port name`
- Use the following URL syntax for direct port access in RSC (IE only):
  - `https://IPaddress>/dpa.asp?username=username&password=password&port=<port number>&useJava=true`

This feature also provides the ability to enter a username and password if the username and password is not contained in the URL.

1. To enable this feature, select Device Settings > Device Services. The Device Service Settings page opens.
2. In the Direct Port Access section, select the "Enable Direct Port Access" checkbox and "Enable Direct Port Access via URL" checkbox.
3. Click OK to apply the settings.

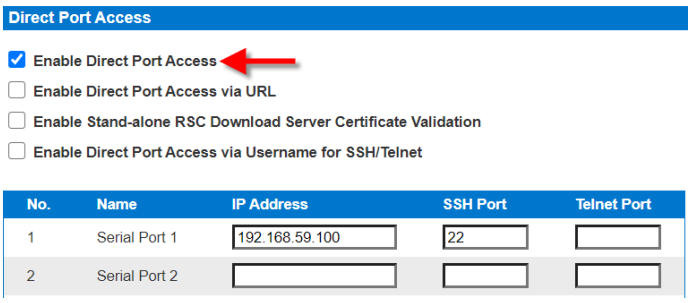


Enable Direct Port Access via SSH/Telnet Using a Unique TCP Port or Unique IP Address

To use this feature, you must configure a unique IP address or a unique TCP port for a server port that SSH/Telnet can use to access SX II. The address must be different from the SX II IP address and TCP port.

When an anonymous user attempts DPA via SSH/Telnet, username and password prompts will not appear. See ***Login Limitations*** (on page 153) for details about anonymous user access.

1. Select Device Settings > Device Services.
2. In the Direct Port Access section, select the "Enable Direct Port Access" checkbox.
3. Locate the port in the table below the checkboxes, then enter the IP address you want to assign to the port.
4. Click OK to apply the settings.



Example:

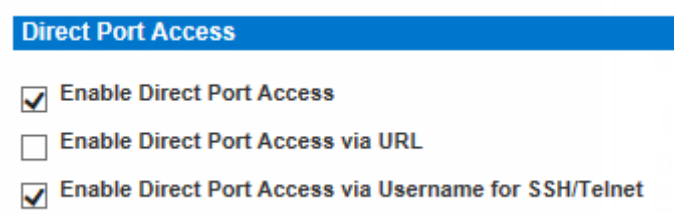
```
ssh -l [user] -p [SSH Port] [SX2 IP/Hostname]
ssh -l [user] [Serial Port IP]
telnet -l [user] [SX2 IP/Hostname] [Telnet Port]
telnet -l [user] [Serial Port IP]
```

Enable Direct Port Access via Username for SSH/Telnet

This feature provides the ability to access DPA through a username and port combination without requiring a unique IP address or TCP port.

When an anonymous user attempts DPA via SSH/Telnet, no login prompt will be shown, and user is directly connected to the port. See ***Login Limitations*** (on page 153) for details about anonymous user access.

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. In the Direct Port Access section, select the "Enable Direct Port Access" checkbox and "Enable Direct Port Access via Username for SSH/Telnet" checkbox.
3. Click OK to apply the settings.



Example:

```
ssh -l [user]:[Serial Port Name] [SX2 IP/Hostname]
ssh -l [user]:[Serial Port Number] [SX2 IP/Hostname]
telnet -l [user]:[Serial Port Name] [SX2 IP/Hostname]
telnet -l [user]:[Serial Port Number] [SX2 IP/Hostname]
```

Example of access port-#1 as admin:

- `ssh -l admin:1 192.168.51.101`

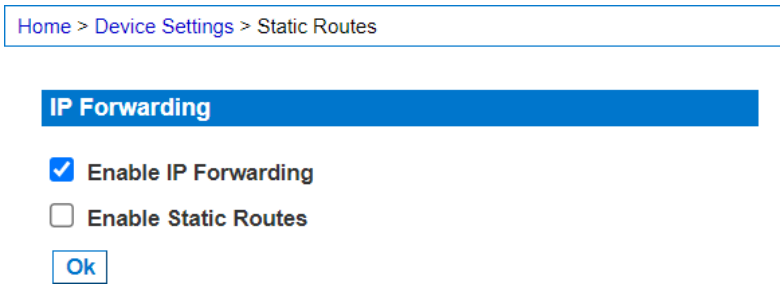
IP Forwarding and Static Routes

Enable IP forwarding, or create static routes if SX II has two LAN ports or is configured for modem access.

To enable IP forwarding and static routes:

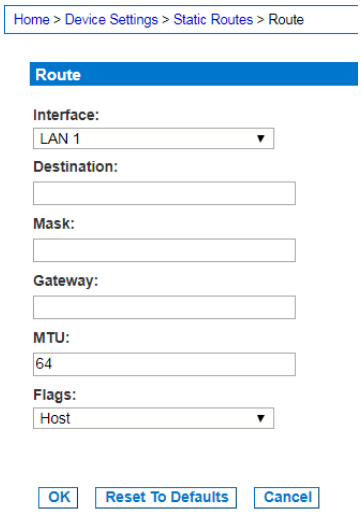
1. Select Device Settings > Static Routes. The Static Routes page opens.

2. Select the checkboxes to enable each feature, then click OK.



To add a static route:

1. When Static Routes is enabled, click Add, then enter the Route details.



2. Select the LAN you want to configure from the drop-down menu in the Interface field.
   - LAN1 = eth0
   - LAN2 = eth1
3. Type the IP address, subnet mask, and gateway of the destination host in the Destination, Mask, and Gateway fields.
4. Enter the maximum transmission unit (MTU) in bytes in the MTU field.
5. Type the TCP windows size for connections over this route in bytes in the Window field.
6. Select your route type from the Flags drop-down menu.
   - Host means this route is for a host machine.
   - Net means this route is for a subnet.
7. Click OK.

To reset a static route:

1. Select Device Settings > Static Routes. The Static Routes page opens.
2. Click Reset To Defaults to reset the route fields to the factory defaults.

To delete a static route:

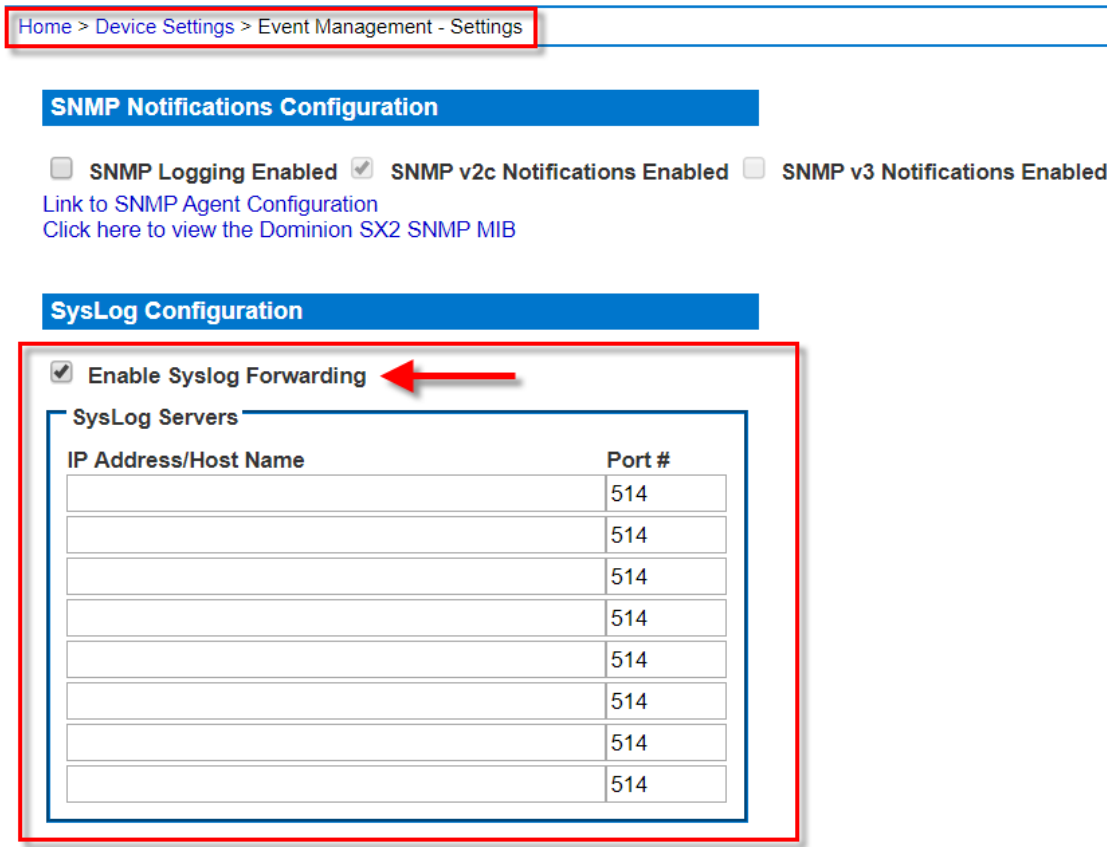
1. Select Device Settings > Static Routes. The Static Routes page opens.
2. Go to the Static Routes List and select the checkbox next to the route you want to delete.
3. Click Delete. You are prompted to confirm the deletion.
4. Click OK. The route is deleted.

Enable Syslog Forwarding

This feature logs all system activities and forwards them to remote Syslog servers. You can configure up to 8 different servers. All messages will be forwarded to all configured servers. If you need to focus on specific messages per server, you should apply message filters at the server level. Messages are sent even if some servers are experiencing errors.

1. Choose Device Settings > Event Management. The Event Management - Settings page opens.
2. Select Enable Syslog Forwarding to log the appliance's messages to remote Syslog servers.
3. Type the IP Address/Hostname of your Syslog servers in the IP Address/Hostname fields. IPv4 and IPv6 are supported.
4. Enter the port number for each server. Default is 514.

5. Click OK at the bottom of the page.



Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

- Click Reset to Defaults at the bottom of the page to remove the setting.

802.1X Security

IEEE 802.1X authentication can be configured independently on each LAN port to give the SX II secure access to your wired LAN.

Supported authentication methods include:

- EAP_TLS
- EAP_TTLS
- EAP_PEAP

If your network switch does not allow access to the network without 802.1X in effect, you will not be able to configure SX II remotely using a web browser. You can use the Local Port of the SX II or a crossover cable to the switch itself.

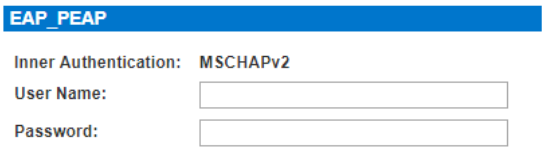
Before proceeding, upload your certificate in the Certificate Repository so that it can be accessed from the 802.1X configuration page. See ***Certificate Repository*** (on page 173).

Important: Do not delete certificates that are in use from the Certificate Repository.

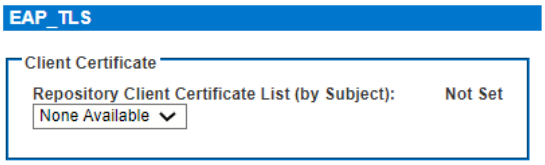
To configure 802.1X security:

1. Choose Device Settings > 802.1X Security. The settings page opens. Note that LAN and LAN2 settings are separate.
2. In the LAN or LAN2 sections, select the Enable 802.1X Security checkbox to begin.
3. In the CA Certificate section, select Enable Verification of TLS Server Certificate if your configuration requires a certificate.
   - If your certificate has been uploaded, select it in the Repository CA Certificate List (by Subject) field.
   - If your certificate doesn't appear, you must add it to the Certificate Repository. See ***Certificate Repository*** (on page 173).
   - Select the option for "Allow expired and not yet valid certificates" to enable if needed.
4. Select your Authentication Method to activate the necessary fields in the form:
   - **EAP_PEAP**: Inner Authentication is set to MSCHAPv2. Enter the user name and password.

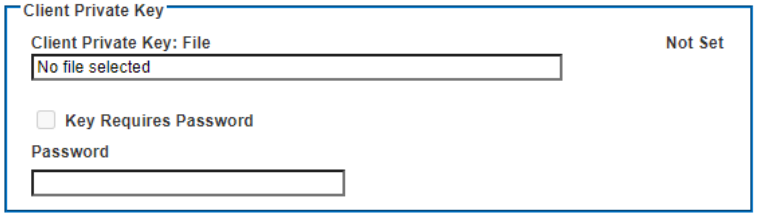
- Username: Numerals: 0-9, Lower case letters: a-z, Upper case letters: A-Z, Printable special characters: ASCII codes 33-47, 123-126, Space (ASCII code 32) is not allowed. Up to 32 characters.
- Password: Numerals: 0-9, Lower case letters: a-z, Upper case letters: A-Z, Printable special characters: ASCII codes 33-47, 123-126, Space (ASCII code 32) is allowed. Up to 64 characters.



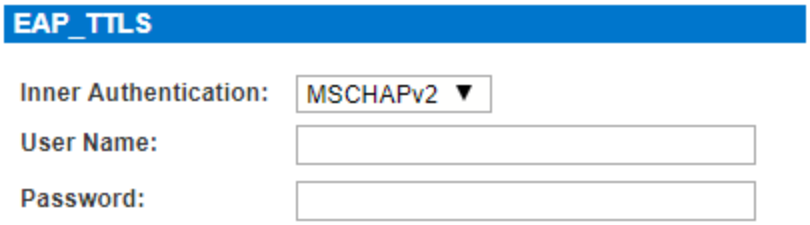
- **EAP_TLS:**
  - If your certificate has been uploaded, select it in the Repository Client Certificate List (by Subject) field.
  - If your certificate doesn't appear, you must add it to the Certificate Repository. See ***Certificate Repository*** (on page 173).



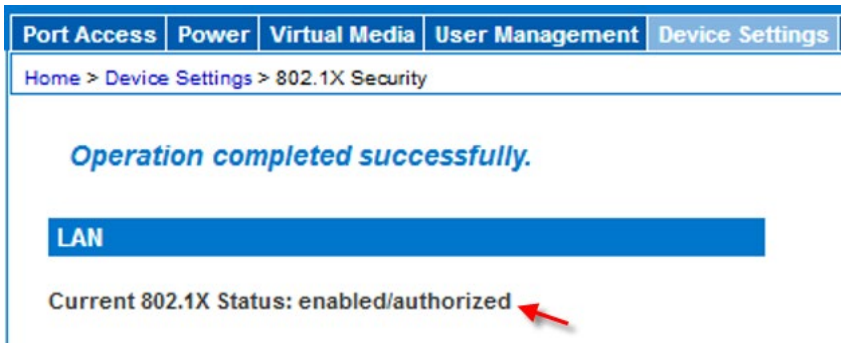
  - If the certificate uploaded to the repository requires a password, the Key Requires Password and password fields will populate automatically.



- **EAP_TTLS:** Select the Inner Authentication method from the list: MSCHAPv2, CHAP, or PAP. Enter the user name and password.



5. Click OK and wait for authentication. This may take several minutes. You can check the status at the top of the 802.1X settings page. After clicking OK the status will be "enabled/pending". If authentication is successful, the status changes to "enabled/authorized". If authentication fails, the status changes to "enabled/failed".



802.1X Status

Check the 802.1X status at the top of the settings page. Go to Device Settings > 802.1X Security.

Interface State	Authentication State	Status
Enabled	Pending	Wait
Enabled	Authorized	Success
Enabled	Failed	Failed/Troubleshoot
Disabled		802.1X Disabled

Troubleshooting 802.1X Authentication Failure

The following tips may help you troubleshoot 802.1X authentication failure.

- Wait for the authentication to complete – it may take several minutes.
- Double-check that the SX II 802.1X settings you have entered match how 802.1X is configured on your network switch.
- Check the 802.1X Status under Device Settings>802.1X Security, in the Audit Log, and the status on the network switch
- On the network switch: Make sure Periodic Reauthentication is enabled. Set the Reauthentication Period to the lowest possible value. The switch will reauthenticate when the Reauthentication Period expires
- Switches may have a way to trigger reauthentication immediately, for example, a 'Reauthenticate Now' checkbox that can be selected to restart authentication immediately on the switch.
- Reboot the SX II.
- Make sure all certificates are uploaded and remain in the Certificate Repository. See ***Certificate Repository*** (on page 173).

Configure Date and Time Settings from the Remote Console

Use the Date/Time Settings page to specify the date and time for the SX II. There are two ways to do this:

- Manually set the date and time.
- Synchronize the date and time with a Network Time Protocol (NTP) server.

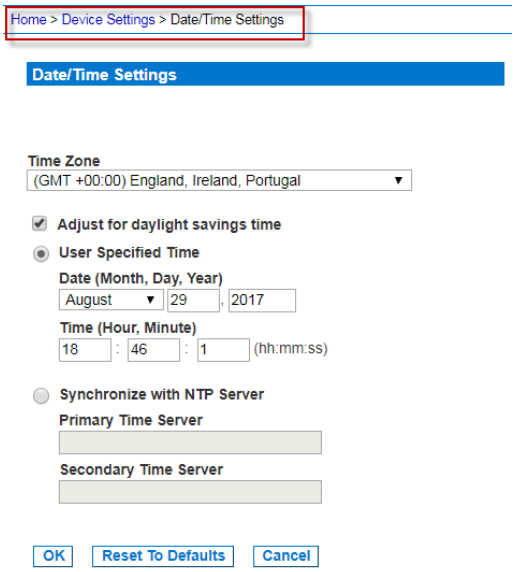
To set the date and time:

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.
2. Choose your time zone from the Time Zone drop-down list.
3. Adjust for daylight savings time by checking the "Adjust for daylight savings time" checkbox.
4. Choose the method to use to set the date and time:
   - User Specified Time - use this option to input the date and time manually. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
   - Synchronize with NTP Server - use this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. For the Synchronize with NTP Server option:
   a. Enter the IP address of the Primary Time server.
   b. Enter the IP address of the Secondary Time server. **Optional**

Note: If DHCP is selected for the Network Settings on the Network page, the NTP server IP address is automatically retrieved from the DHCP server by default. Manually enter the NTP server IP address by selecting the Override DHCP checkbox.

---

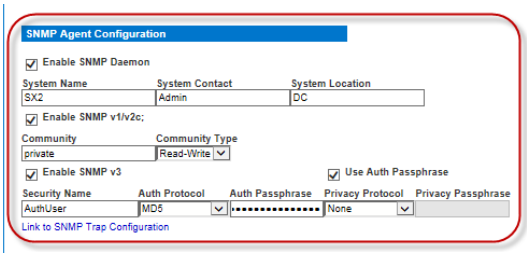
6. Click OK.



Configure SNMP Agents from the Remote Console

See ***Viewing the SX II MIB*** (on page 121) for information on viewing the SX II MIB.

SX II supports SNMP logging for SNMP v2c and/or v3. SNMP v2c defines message formats and protocol operations when SNMP logging is enabled. SNMP v3 is a security extension of SNMP that provides user authentication, password management and encryption.



1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select the Enable SNMP Daemon checkbox to activate to the SNMP section.
3. Provide the following SNMP agent identifier information for the MIB-II System Group objects:
   - System Name - the SNMP agent's name/appliance name
   - System Contact - the contact name related to the appliance
   - System Location - the location of the appliance

4. Select either or both Enable SNMP v1/v2c and Enable SNMP v3. At least one option must be selected. **Required**
5. Complete the following fields for SNMP v2c (if needed):
   - Community - the appliance's community string
   - Community Type - grant either Read-Only or Read-Write access to the community users

   Note: An SNMP community is the group to which appliances and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.
6. Complete the following fields for SNMP v3 (if needed):
   - Select Use Auth Passphrase if one is needed. Select this option if you want to use the same pass phrase for the authorization pass phrase and privacy pass phrase without having to re-enter it.
   - Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters).
   - Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent. Note: When FIPS is enabled, SHA must be used for v3 traps for FIPS compliance.
   - Authentication Passphrase - the pass phrase required to access the SNMP v3 agent (up to 64 characters).
   - Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt data.
   - Privacy Passphrase - if applicable, the pass phrase used to access the privacy protocol algorithm (up to 64 characters).

Next, configure SNMP traps. This is done on the Event Management - Settings page, which can be quickly accessed by clicking the SNMP Trap Configuration link at the bottom of the Device Services page. See ***Configuring SNMP Notifications*** (on page 119)for information on creating SNMP traps and List of SX II SNMP Traps for a list of available SX II SNMP traps.

The events that are captured once an SNMP trap or inform is configured are selected on the Event Management - Destination page. See Configuring Event Management - Destinations.

Configuring SNMP Notifications

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions.

SNMPv2 provides for both traps and informs to be sent out over a network to gather information. The basic difference between traps and informs is that when the remote application receives an inform it sends back an acknowledgment, while traps are not acknowledged. In SNMPv3, there are further capabilities and restrictions on how the messages are handled.

The traps and informs are configured on the Event Management - Settings page. See List of SX II SNMP Traps for a list of supported traps and informs.

SNMP agents are configured on the Device Services page. See Configuring SNMP Agents for information on configuring SNMP agents and ***Viewing the SX II MIB*** (on page 121) for information on viewing the SX II MIB.

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Select the SNMP Logging Enabled checkbox to enable to remaining checkboxes in the section. **Required**
3. Select either or both SNMP v2c Notifications Enabled and SNMP v3 Notifications Enabled. At least one option must be selected.

   Once selected, all related fields are enabled. **Required**
4. Complete the following fields for SNMP v2c (if needed):
   - Destination IP/Hostname - the IP or hostname of the SNMP manager. Up to five (5) SNMP managers can be created

   Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

   a. Port Number - the port number used by the SNMP manager

   b. Community String - the appliance's community string

   Note: An SNMP community is the group to which appliances and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.

   c. Type - notification type, either Trap or Inform

   d. Retries and Timeout - for Informs, enter the number of retries to be attempted, and the timeout period in seconds.

   WARNING: Non-responding destinations may significantly slow system response if informs are configured with large values for retries and/or timeouts.
5. If it is not already, select the SNMPv3 Notifications Enabled checkbox to enable the following fields. Complete the following fields for SNMP v3 (if needed):

- Destination IP/Hostname - the IP or hostname of the SNMP manager. Up to five (5) SNMP managers can be created

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

a. Port Number - the port number used by the SNMP manager

- Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters).
- Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent. Note: When FIPS is enabled, SHA must be used for v3 traps for FIPS compliance.
- Authentication Passphrase - the pass phrase required to access the SNMP v3 agent (up to 64 characters).
- Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt data.

a. Privacy Passphrase - if applicable, the pass phrase used to access the privacy protocol algorithm (up to 64 characters).

Note: If you are accessing the Event Management - Settings page from the local console and are using a screen resolution lower than 1280x1024, the Privacy Passphrase column may not be displayed on the page. If this occurs, hide the SX II's left panel. See Left Panel

b. Type - notification type, either Trap or Inform.

c. Retries and Timeout - for Informs, enter the number of retries to be attempted, and the timeout period in seconds.

6. Click OK to create the notifications.

Use the Link to SNMP Agent Configuration link to quickly navigate to the Devices Services page from the Event Management - Settings page.

The events that are captured once an SNMP trap or inform is configured are selected on the Event Management - Destination page. See Configuring Event Management - Destinations.

SX II supports SNMP logging for SNMP v2c and/or v3. SNMP v2c defines message formats and protocol operations when SNMP logging is enabled. SNMP v3 is a security extension of SNMP that provides user authentication, password management and encryption.

To edit existing SNMP notifications:

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Make changes as needed and click OK to save the changes.

Note: If you disable SNMP settings at any time, the SNMP information is retained so you do not have to reenter if you re-enable the settings.

To delete SNMP notifications:

- Clear all of the SNMP fields and save.
- Use the reset to factory defaults feature to remove the SNMP configuration and set the SX II to its original factory default.

To reset to factory defaults:

- Click Reset To Defaults.

WARNING: When using SNMP notifications over UDP, it is possible for the SX II and the router that it is attached to fall out of synchronization when the SX II is rebooted, preventing the reboot completed SNMP notification from being logged.

Viewing the SX II MIB

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Click the 'Click here to view the 'SNMP MIB' link. The MIB file opens in a browser window.

Performance Information in the MIB

The following Gets() have been added to the MIB.

CPU (processor)

- systemUsageCPU: Current usage as percentage

Memory

- systemUsageMemory: Current usage as percentage.

Power supply status

- systemPowerSupplyTable: Table of up to two power supplies' on/off status.

Port utilization and Port status

- portDataTable: Table of the portDataStatus for each port with the possible states below:
  - inactive - Target cannot be accessed. (UI Status:down, Availability:idle)
  - available - Target can be accessed. (UI Status:up, Availability:idle)
  - connected - A user is connected but capacity is available. (UI Status:up/down, Availability:connected)

- busy - Reached maximum access capacity. (UI Status:up/down, Availability:busy)

Configure Event Management - Destinations

If system events are enabled, SNMP notification events (traps and informs) are generated. The events can be logged to the syslog or audit log.

Events and where the event information is sent is configured on the Event Management - Destinations page.

Note: SNMP, Syslog, and SMTP logging only works when enabled in the Event Management - Settings page.

To select events and their destinations:

1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens.

   System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.
2. Select the checkboxes for those event line items you want to enable or disable, and where you want to send the information.

   Tip: Enable or disable entire categories by checking or clearing the Category checkboxes, respectively.
3. Click OK.

To reset to factory defaults:

- Click Reset To Defaults.

WARNING: When using SNMP notifications over UDP, it is possible for the SX II and the router that it is attached to fall out of synchronization when the SX II is rebooted, preventing the reboot completed SNMP notification from being logged.

Home > Device Settings > Event Management - Destinations

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Syslog events will only be generated if the "Enable Syslog Forwarding" option is checked. SMTP messages will only be generated if the "SMTP Logging Enabled" option is checked. Event destination settings can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	SMTP	Audit Log
Device Operation		☑	☑	☑	☑
	System Startup	☑	☑	☑	☑
	System Shutdown	☑	☑	☑	☑
	Power Supply Status Changed	☑	☑	☑	☑
	Powerstrip Outlet Status Changed	☑	☑	☑	☑
	Network Parameter Changed	☑	☑	☑	☑
	Port Status Changed	☑	☑	☑	☑
	Network Failure	☑	☑	☑	☑
	Ethernet Failover	☑	☑	☑	☑
	802.1x Authentication Failure				☑
	Automatic Script Configuration	☑	☑	☑	☑

Enable Email (SMTP) Notifications from the Remote Console

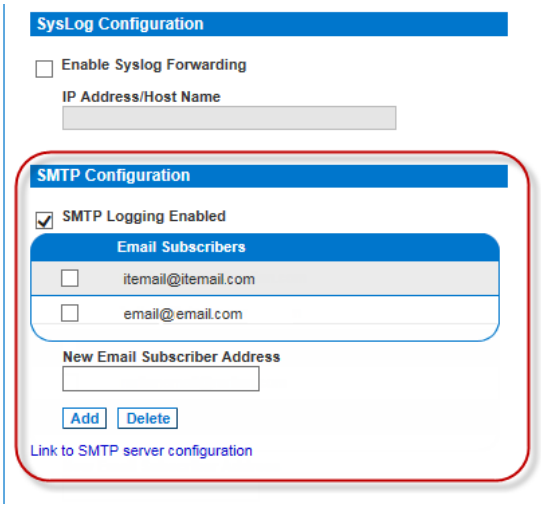
Enable email notifications for users on the Event Management - Settings page.

Each person for whom SMTP is enabled receives notification when an event is triggered. Up to ten (10) users can be added.

Configure SMTP server settings on the SMTP Settings page. Use the "Link to SMTP server configuration" quick link at the bottom of the Event Management - Settings page. See ***Configure and Test SMTP Server Settings*** (on page 124).

To enable SMTP Notifications:

1. Select Device Settings > Event Management - Settings to open the Event Management - Settings page.
2. Go to the SMTP Settings panel and select the Enable SMTP Server checkbox.



3. Type the email address of the SMTP subscriber in the New Email Subscriber Address field and then click Add.
4. Click OK.

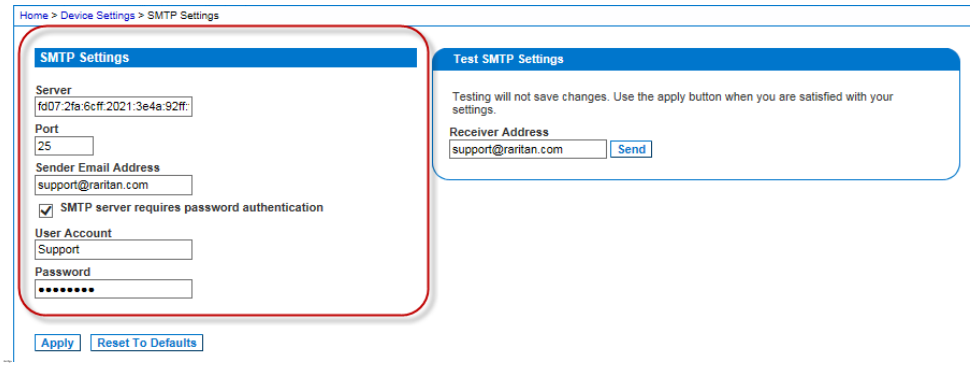
Configure and Test SMTP Server Settings

Enter the information required for a connection to your SMTP server on the SMTP Server Settings page.

Note that if the server requires STARTTLS, SX II automatically uses it.

1. Select Device Settings > SMTP Settings.
2. Provide the server address, port and the email address used to send SMTP notifications.
3. If the server requires a username and password authentication to send emails, provide them in the User Account and Password fields, respectively.

4. Click Apply.



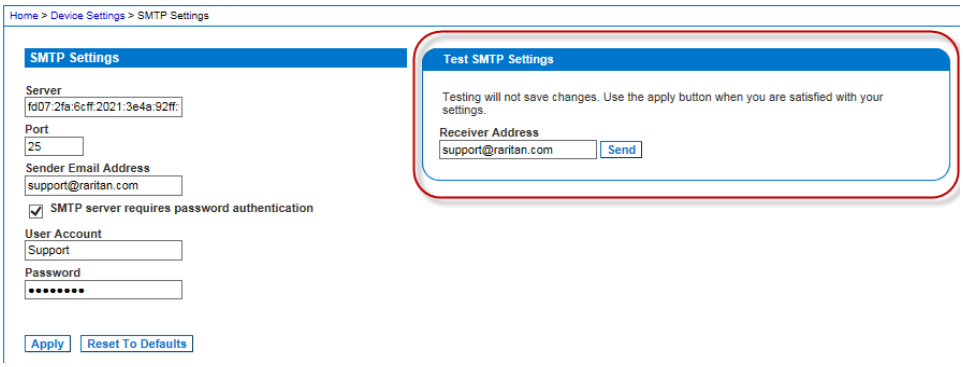
It is important that the SMTP server information be accurate so that the SX II appliance can send messages using that SMTP server.

This test sends an email using the settings displayed on the page in the SMTP Settings pane. SX II saves the settings once you click Apply.

1. Send a test email by entering a destination email address to receive the test message

   Note that the receiver email is not saved.

2. Verify the message was received by the intended email target. If there are problems, contact your SMTP administrator to make sure your SMTP server IP address and authorization information are correct.



Configure Modem Settings from the Remote Console

Configure modem settings for SX II models with internal, analog modems on the Modem Settings page. You can also configure modem settings via command line interface. See ***Configure a Modem Using CLI*** (on page 205).

Note: SX II models without internal modems do not have access to the Modem Settings.

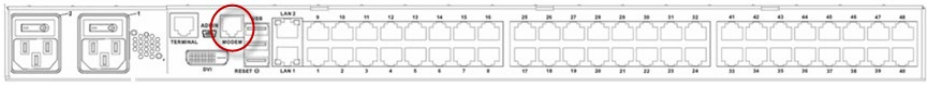
SX II models with internal modems are indicated by an **M** in the model, such as DSX2-4M. For a list of models. see ***SX II Models*** (on page 9). You model number is in Device Information in the left panel of the Remote Console.

Restrictions of PPP dialup:

When accessing SX II over dialup, the Port Access tab in the web interface is disabled, but administrative features are available. Port access cannot load over slow dialup connections. When using PPP dialup, use SSH CLI for port access.

Connect to the Internal Modem via the Modem Port

- Use a telephony cable to connect to the Modem port on the SX II.



Configure the Internal Modem

1. Choose Device Settings > Modem Settings to open the Modem Settings page.

   Note: The Enable Broadband Modem feature is specific to use of an external, wireless modem. See **Connect and Enable Global Access to an External USB-Connected Broadband Modem** *(on page 132).*

2. Select Enable Modem. Default is enabled.
3. Select the Modem Access Mode.
   - All - allows modem access through both PPP and console access.

     If a PPP signal is not detected, uses console access.

- PPP_Only - allows only PPP connections that will access the SX II through the configured PPP server IP address.
- Console_Only - allow only Local Console connections, meaning CLI access through a terminal emulation program such as Hyperterminal.

4. If you selected All or PPP_Only as the modem access mode, enter the IP address information.
   - Enter the PPP server IP address.

     This is address assigned to SX II when a connection is established via dial-up. **Required**
   - Enter the PPP client IP address.

     This is the internet address SX II assigns to the Remote Client when a connection is established via dial-up. **Required**

   Note: The PPP server IP address and PPP Client IP address must be different and cannot conflict with the network addresses used by the server or the client.
5. PPP_Only mode supports dialback. Select the Enable Modem Dial Back checkbox to enable the dialback feature.

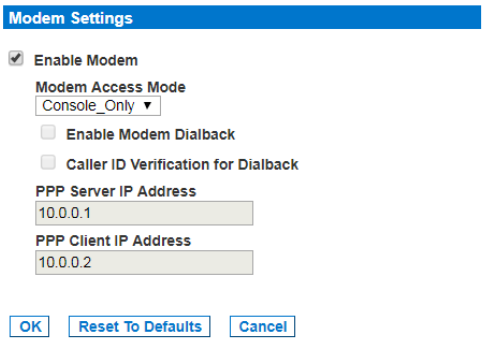
   Only tone dial back is supported; pulse dial back is not supported.

   Both Dial-in and Dialback must be enabled on the modem, and the dialback numbers for a user must be configured in the authentication service (local, RADIUS, LDAP, or TACACS+). See ***Create and Activate a User*** (on page 80).

   Users who belong to a user group with Modem Access permission but who do not have a dial-in number cannot establish a connection.

   Each user accessing the SX II via modem must have a call-back number defined in their profile. A Comma (,) character is supported to enable a pause, such as in dialing a 9 before a phone number. Add up to 8 dialback numbers per user. See ***Configure Multiple Dialback Numbers and Caller ID Verification*** (on page 129).
6. Select the Caller ID Verification for Dialback checkbox to enable. When enabled, numbers used to access the modem will be verified against the dialback numbers listed for a user. See ***Configure Multiple Dialback Numbers and Caller ID Verification*** (on page 129) for more details.
7. Select Enable Modem Dialout to allow outbound modem connections. When enabled, an access point called "Internal Modem" is added to the end of the port list that will launch an HSC interfaces directly with the modem. AT commands can then be given to initialize and dial out from the modem.

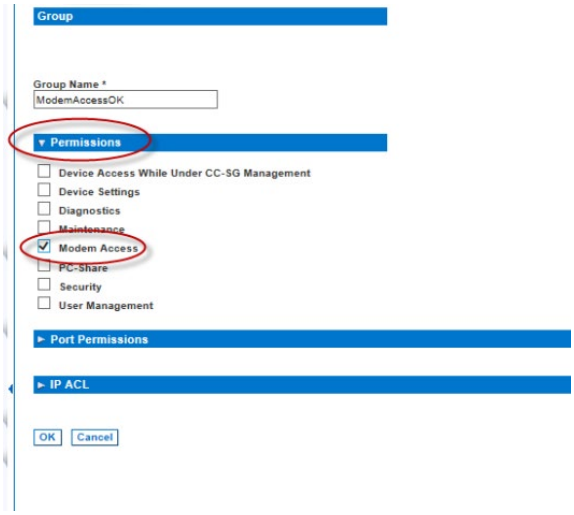
8. Click OK to commit your changes or click Reset to Defaults to return the settings to their defaults.



Assign User Groups Modem Access Permissions

- If needed, assign users to a group with Modem Access permissions.

  Modem Access permission is assigned to a user group on the Group page, and the user is then assigned to the group on the User page. For more information, see ***Configure and Manage Users and Groups from the Remote Console*** (on page 73).



Configure Multiple Dialback Numbers and Caller ID Verification

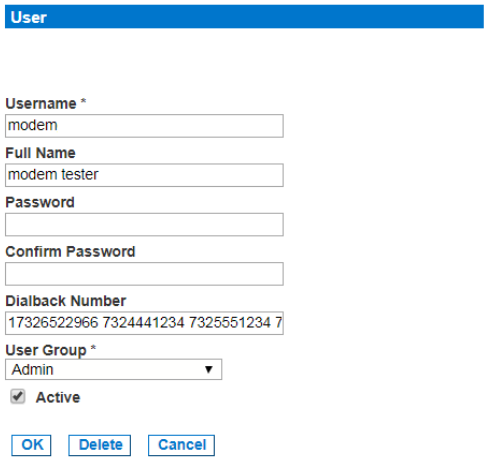
You can associate multiple phone numbers with a user for dialback from the modem. Caller ID verification can be enable to validate and dial back to the proper number in the list.

When a user logs in via the modem, and Caller ID Verification is enabled, the system will check the phone number used to log into the device. If the Caller ID number is found in the user's configured dialback numbers, dialback will be allowed to continue and dial back to the number in the CallerID. When Caller ID Verification is diabled, and the user has multiple numbers configured, the system will always dial back the first number that is in the list of numbers in the dialback field.

Multiple dialback numbers and caller ID verification work the same way with both PPP dialback and console dialback implementations.

To configure dialback numbers:

1. Choose User Management, then select a user or create a user. See ***Create and Activate a User*** (on page 80). When your SX II model has an internal modem, the user profile contains modem-specific fields.

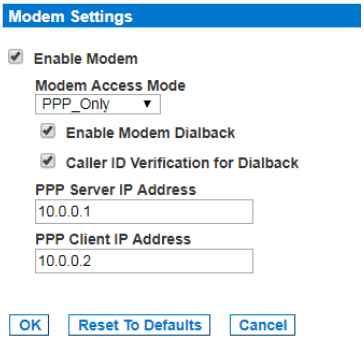


2. In the Dialback Number field enter the list of phone numbers for this user. Use a space between each complete phone number. Up to 128 characters total.
3. Click OK.

To configure caller ID verification:

1. Choose Device Settings > Modem Settings to open the Modem Settings page.
2. Verify PPP_Only is selected for Modem Access Mode.
3. Verify Enable Modem and Enable Modem Dialback checkboxes are selected.

4. Select the Caller ID Verification for Dialback checkbox.
5. Click OK.

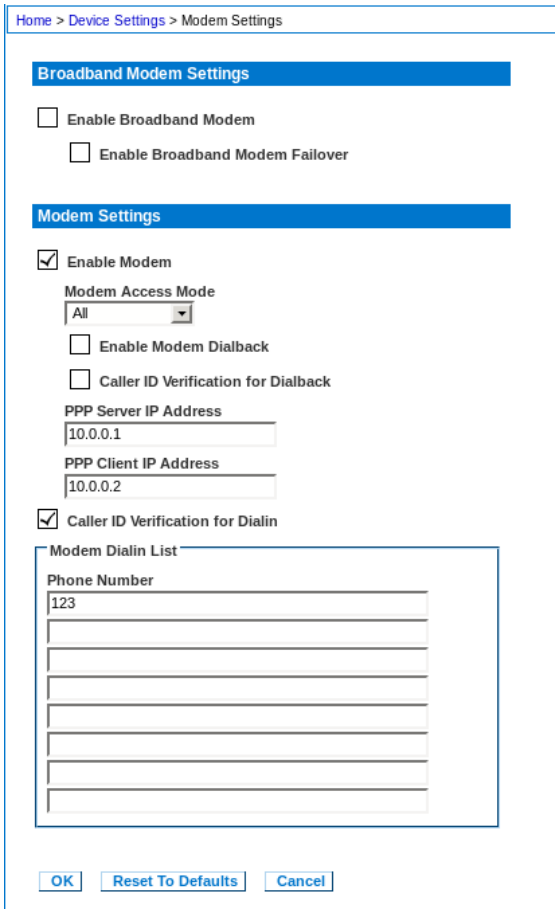


Configure Caller ID Verification for Dialin Numbers

Caller ID verification for dialin numbers allows you to configure a list of 8 approved dialin numbers from which analog phone calls will be accepted.

When enabled, if a call is received from a number that is not present in the dialin list, the phone does not answer the line.

If the phone number is present in the dialin list, the connection will take place after the third ring of the phone.



To configure caller ID verification for dialin numbers:

1. In Device Settings > Modem Settings, make sure a modem is enabled.
2. Select the Caller ID Verification for Dialin checkbox.
3. Enter the approved dialin numbers in the Modem Dialin List.
4. Click OK.

External Modem Support

There are two supported options for external broadband modems. One option may be better for your configuration.

USB-connected modem:

- All SX II models support an external, 3G/4G wireless modem connection with USB using a Sierra Wireless AirLink® GX440, GX450, or ES450 gateway modem.
- With this modem configuration, you can set permissions on SX II that control who can access using this modem. See ***Connect and Enable Global Access to an External USB-Connected Broadband Modem*** (on page 132)

LAN-connected modem:

- All SX II models support an external 4G modem connection via Ethernet using a Cradlepoint AER1600 or Cradlepoint IBR200 modem. See ***Connect to a LAN Connected External Modem*** (on page 135).
- With this modem configuration, the modem is unknown to SX II because it is Ethernet-connected. You cannot control the modem using SX II permissions.
- The "Failover to Modem" feature does not apply to this modem configuration.
- This configuration can be used with VPN access.

Connect and Enable Global Access to an External USB-Connected Broadband Modem

Users who need access to SX II via the Sierra Wireless modem must be assigned to a user group with Modem Access permissions. This is a security measure that helps control who can access SX II via the modem. For example, create a user group called Sierra Wireless Users and give the group Modem Access permissions, then assign only users who need access to the modem to that group.

The Enable Broadband Modem feature must be enabled in SX II in order for users to access SX II via the Sierra Wireless modem. This is a global-level feature, so it is disabled by default in order to prevent all users from being able to access SX II via the modem.

Sierra Wireless Software and Firmware Versions

Sierra Wireless must have at least ALEOS Software Version 4.4.1.014

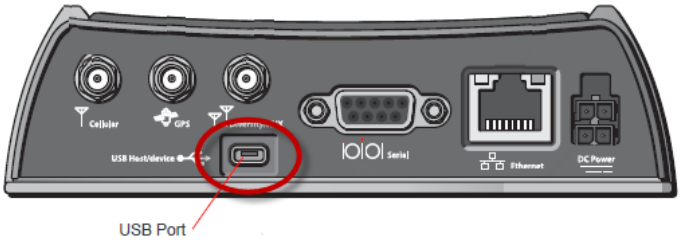
This configuration has been tested with the Verizon Wireless MC7750 Radio Module using firmware version 3.05.10.13.

Connect the External, Wireless Modem

USB Connection

Use either a Micro A or Micro B to USB Type A cable to connect the Sierra Wireless to the SX II.

- Connect the Sierra Wireless USB port to any of the USB ports on back of the SX II or to the USB port on the front of the SX II.



Note: Only USB connections are supported for this modem.

Configure the Sierra Wireless Modem

Configure the Sierra Wireless modem for use with SX II using these connections. These settings are configured on the Sierra Wireless modem, not SX II.

Configure the Sierra Wireless Modem for a Cellular Connection

- A SIM card must be purchased from your service provider and installed in the Sierra Wireless modem.
- Get a static IP address from your service provider, then assign it to the Sierra Wireless modem.
- Sierra Wireless must be configured for Public mode.
- Host Connection Mode must be set to "USB Uses Public IP".
- USB Device Mode must be set to "USBNET".

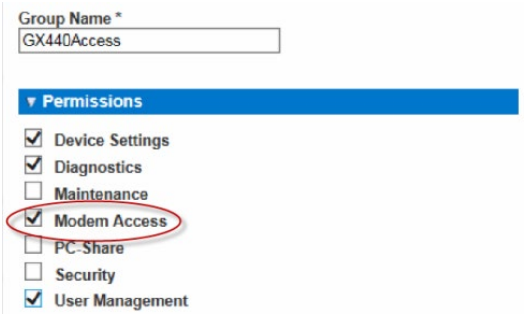
Change Default Username

For security reasons, change the default Admin account username to a new name before using the Sierra Wireless .

Assign User Groups Modem Access Permissions

Following are settings applied in SX II.

- Modem Access permission is assigned to a user group on the Group page, and the user is then assigned to the group on the User page. For more information, see ***Configure and Manage Users and Groups from the Remote Console*** (on page 73).



Enable Global Access and Failover Settings to External USB-Connected Broadband Modem

Use this feature to enable or disable access to an external Sierra Wireless modem.

Note: These settings do not apply to the Cradlepoint LAN-connected modem option.

Cellular (broadband) access is disabled by default. Since this is a global-level feature, it is disabled for all users.

Once it is enabled, only users who belong to a user group with Modem Access permissions can access SX II via the Sierra Wireless modem.

Broadband can be enabled from the Remote Client and via CLI.

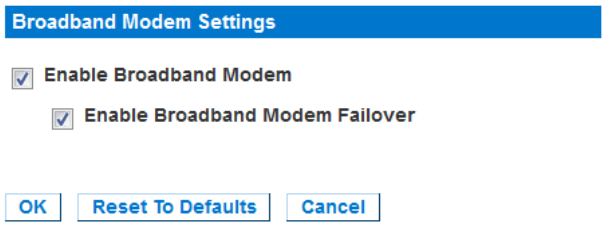
To enable broadband from the Remote Client:

1. Enable broadband by selecting Device Settings > Modem Settings and selecting the Enable Broadband Modem checkbox.
2. Click OK to apply the change.

   SX II is now accessible using the Sierra Wireless modem.
3. If you want your modem automatically enabled only when both LAN ports go down, also select the Enable Broadband Modem Failover checkbox.

   Once either LAN port comes back up, the model will be automatically disabled. All active sessions will be dropped.

4. Click OK to apply the change.



External Modem Connection Status and Checks

The connection event is logged in the SX II audit log.

Once the devices are on and the connection is active, the gateway IP address is displayed in the Remote Console in the left panel under the Network section.

Additionally, the gateway IP address is displayed on the Network Settings page in the IPv4 section's Default Gateway field.

As with other targets connected to SX II, you can perform diagnostics, ping and perform a trace of the Sierra Wireless modem using the SX II Diagnostics tools.

Connect to a LAN Connected External Modem

Cradlepoint AER1600 or IBR200 are supported for LAN-connected external modem access.

To connect Cradlepoint modems to SX II:

- Connect the AER1600's or IBR200's LAN port to the SX II LAN1 or LAN2 port.
- The SX II LAN port must be configured for DHCP so that the AER1600 DHCP server can provide it with the IP address. It is possible to reserve an IP address on the AER1600 so that the user can configure the SX II LAN port with a static IP address.
- In the SX II network settings, Enable Automatic Failover should be disabled. Choose Device Settings > Network, then deselect the Enable Automatic Failover checkbox.

To configure VPN access:

OpenVPN client on Windows 7 works with the AER1600 when configured according to the instructions provided by Cradlepoint. A Cradlepoint prime license is required:

http://knowledgebase.cradlepoint.com/articles/Support/OpenVPN-Bridged-Client-Server-Configuration

- Note: If VPN is not in use, port forwarding must be configured in the AER1600 to forward the IP packets to the SX II.

Power Supply Setup

SX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies.

When both power supplies are used, SX II automatically detects them and notifies you of their status. Additionally, both the PowerIn1 and PowerIn2 Auto Detect checkboxes are automatically selected on the Power Supply Setup page.

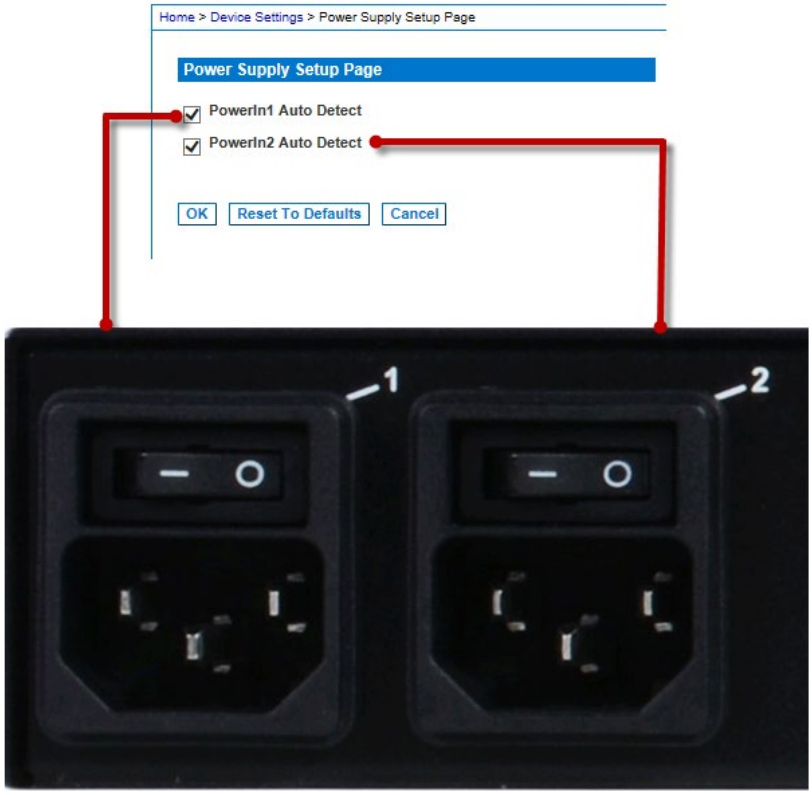
If you are using only one power supply, you can enable automatic detection for only the power supply in use.

Proper configuration of power supplies ensures SX II sends the appropriate notifications should a power supply fail. For example, if power supply number one fails, the power LED at the front of the unit will turn red.

The Power LED on the front of the SX II appliance is red when the checkbox is selected for an unconnected power supply. The LED is blue when the checkbox is not selected for an unconnected power supply.

To enable automatic detection for the power supplies in use:

1. Choose Device Settings > Power Supply Setup. The Power Supply Setup page opens.



2. If you are plugging power input into power supply number one (left-most power supply at the back of the unit), then select the PowerIn1 Auto Detect option.
3. If you are plugging power input into power supply number two (right-most power supply at the back of the unit), then select the PowerIn2 Auto Detect option.
4. Click OK.

To turn off the automatic detection:

- Deselect the checkbox for the appropriate power supply.

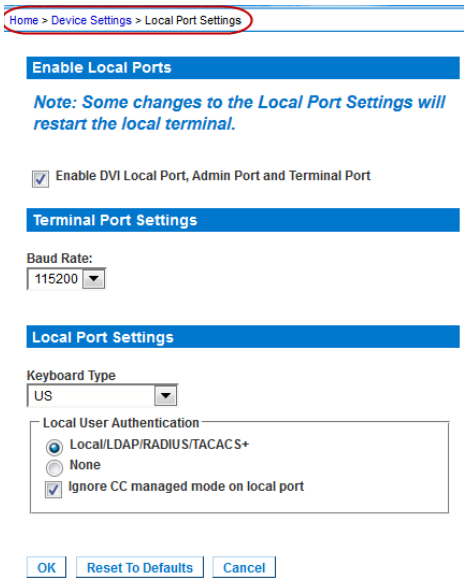
To reset to factory defaults:

- Click Reset To Defaults.

Configure Local Port Settings from the Remote Console

Configure Local Console port settings on this page.

Some changes you make to the settings on the Local Port Settings page restart the local terminals. If a local terminal restart occurs when a setting is changed, it is noted here.



1. The "Enable DVI-D Local Port, Admin Port and Terminal Port" checkbox is selected and the ports are enabled by default. Deselecting the checkbox disables the ports.

   The local terminal is restarted when this change is made.
2. In the Terminal Port Settings, choose the terminal port's Baud Rate.
3. Choose the appropriate keyboard type from among the options in the drop-down list. These keyboard options apply only to the Remote Console; they do not apply to the Local Console.

The local terminal is restarted when this change is made.

- US
- US/International
- United Kingdom
- French (France)
- German (Germany)
- German (Switzerland)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- JIS (Japanese Industry Standard)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)
- Hungarian
- Spanish
- Italian
- Slovenian

Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for SX II Local Console functions.

4. Choose the type of Local Console authentication.
   - Local/LDAP/RADIUS/TACACS+ - This is the recommended option.
   - None - There is no authentication for Local Console access.

     Important - If local port authentication is set to None, users only need to hit a character key on their keyboard and are automatically logged in as admin user.

     This option is recommended for secure environments only. For default settings, users are required to login to the local port via username and password.
5. Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the SX II even when the appliance is under CC-SG management. Alternatively, use the direct device access while under CC-SG management feature.

   If you do not ignore CC manage mode on the local port now and decide at a later time to remove the appliance from CC-SG management, you must remove the device from within CC-SG and then return to this page to deselect this checkbox.

Changing the Default GUI Language Setting from the Remote Console

The SX II web-based interface defaults to English, but also supports the following localized languages. These languages are not applied to the Local Console.

- Japanese
- Simplified Chinese
- Traditional Chinese

To change the GUI language:

1. Select Device Settings > Language. The Language Settings page opens.
2. From the Language drop-down, select the language you want to apply to the GUI.
3. Click Apply. Click Reset Defaults to change back to English.

Note: Once you apply a new language, the online help is also localized to match your language selection.

Configure Port Logging Settings from the Remote Console

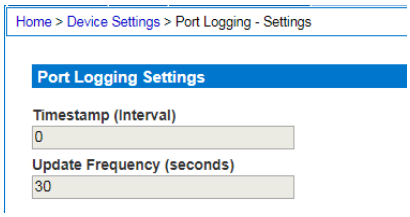
- Select Device Services > Port Logging Settings to access the Port Logging - Settings page and configure the local log settings.

Timestamp and Update Frequency

SX II logs the port status at regular intervals as defined by the Timestamp value. Enter a time in seconds between 0 – 99999. Note that entering 0 disables timestamps for port logging. Changes to the timestamp interval will go into effect after the current interval has passed and that port status timestamp has been logged. The default value is 0 seconds, so port status logging is disabled by default.

The update frequency is the interval between each data push to the port log file, port syslog and NFS port logging, if they are enabled. The default value is 30 seconds.

Data is buffered in SX II during the time between the intervals or until the appliance buffer is full. This feature manages the logging traffic so it is not pushed continuously.

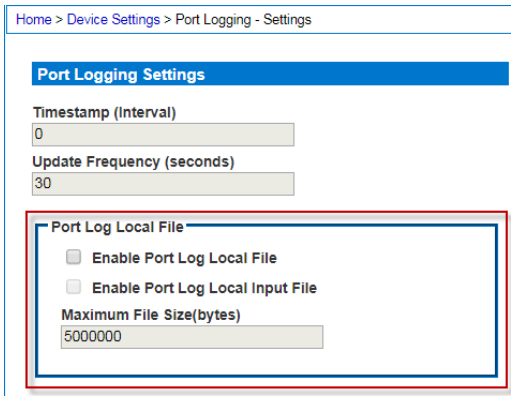


Port Log Local File and Port Log Local Input File

Enable the Port Log Local File to capture data for each port locally on SX II. To capture inputs for each port, enable the Port Log Local Input File.

Log files are stored on SX II's internal flash drive. 8 and 16 port models have a 2GB internal flash drive. All other models have an 8GB flash drive.

If needed, enter a maximum file size. When files reach the maximum size, the oldest data is overwritten to maintain size. To retrieve the files, see ***Manage Port Logging - Local Files from the Remote Console*** (on page 143).



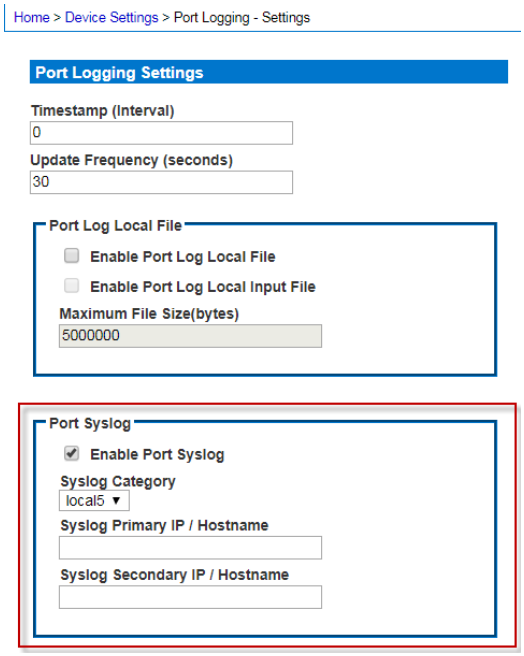
Port Sys Log

This feature sends port log data to a remote Syslog server. The messages from the SX II appliance are sent to the LOCAL5 category of the Syslog server for more efficient parsing.

Note: Local5 is the default category, but it is configurable to other local categories.

Since all messages are sent from the same category on the syslog server, all port output resides in the same file. Use NFS Port Logging if you prefer separate files for each port's data.

1. Go to the System Logging panel and select the Enable Port Syslog checkbox.



2. Type the IP address of the remote Syslog server in the Primary IP Address field.
3. If you have a backup Syslog server, type its IP address in the Secondary IP Address field.

Network File System (NFS) Logging

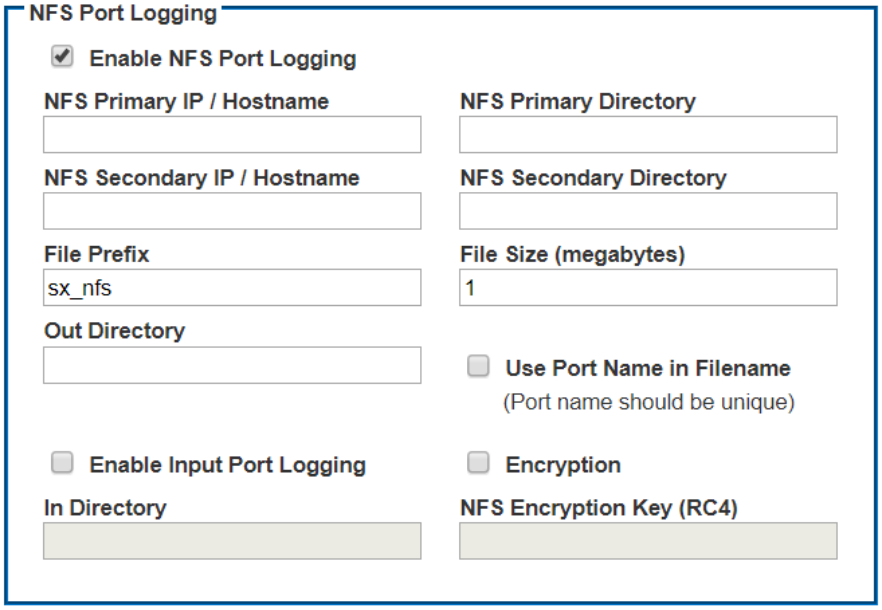
Network File System (NFS) logging allows you to log all port activity to an NFS shared directory. All user activity and user port logins and logouts are logged. There are two log files:

- Input: Records all input (keystrokes) from users.
- Output: Contains all the messages that come from the server into the console server. This includes all user input that is echoed back from the managed device/server.

You must also enable port logging. For more information on port logging, see Enable Port Logging.

Note: The NFS server must have the exported directory with write permission for the port logging to work.

1. Select the Enable NFS checkbox to enable NFS logging.
2. Type the IP address or hostname of the NFS server in the Primary IP/Hostname field, and then enter the path to the log file in the NFS Primary Directory field.
3. If you have a backup NFS server, enter the IP/hostname in the Secondary IP/Hostname field and NFS Secondary Directory fields. If the primary server fails, port logging is redirected to the secondary server.
4. Enter a File Prefix to be added to all filenames. Use " " for a blank prefix.
5. Enter a maximum File Size in megabytes.
6. Specify the directory for output of log files in the Out Directory field.
7. If needed, activate the Enable Input Port Logging feature and type a directory for input in the In Directory field. To turn this feature off, deselect this checkbox.
8. Use Port Name in Filename: select to customize log file names with the port name.
9. Select the Encryption checkbox to enable encryption of log files.
   - Enter the RC4 key in the NFS Encryption Key (RC4) field.



Manage Port Logging - Local Files from the Remote Console

To delete log files:

1. Select checkbox for log files.
2. Click Delete Log File.

To retrieve a log file:

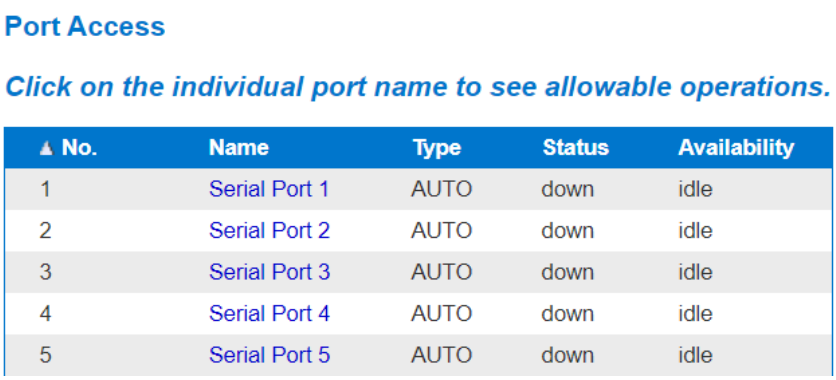
- Click the Download link for a log file's "OutputFile" or "InputFile".

Note that power string data is not saved in port log files.

For information on configuring local log files for ports, see ***Configure Port Logging Settings from the Remote Console*** (on page 139).

Configure Ports from the Remote Console

The Port Configuration page displays a list of the SX II ports.



1. To access the Port Configuration page, choose Device Settings > Port Configuration.

   This page is initially displayed in port number order, but can be sorted by Name or Type by clicking on the column heading.
2. To access a port's page to configure it, click the Port Name for the port you want to configure.
3. Select the Type of target, either Serial or Powerstrip.
4. Provide a meaningful name for the serial target or power strip. Or, click Auto Name Search to use the configured autoname search settings to retrieve the System Name. Auto Name does not work for power ports. See ***Port Auto Name*** (on page 149).

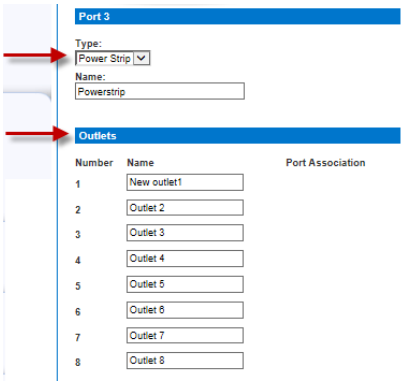
Note: CommandCenter Secure Gateway does not recognize rack PDU names containing spaces.

Configure Powerstrips

1. If you selected Power Strip, change the Power Strip Name and click OK. If a power strip is detected, you are returned to the Port Configuration page.
2. Select the port again to edit it and its outlet names, if desired. Outlet names default to the outlet number.

Note: When a rack PDU is associated with a target device (port), the outlet name is replaced by the target device name, even if you assigned another name to the outlet.

3. Click OK to save, or Reset to Defaults to start over.



Configure Target Devices

If you selected a target device, there are various settings you can configure.

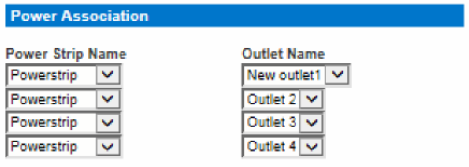
Note: When a rack PDU is associated to a target device (port), the outlet name is replaced by the target device name (even if you assigned another name to the outlet).

1. Enter or update the Target Name.
2. If an outlet is connected to the same server that the port is connected to, a power association can be made with the target device.

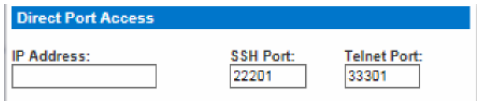
   A port can have up to four associated outlets, and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

   To use this feature, you need Raritan remote rack PDU(s).
3. Select the Power Strip Name and associate an name with each of the power strip's outlets by selecting from the Outlet Name drop-down.

4. Click OK. A confirmation message is displayed.



5. To allow direct port access to the target's port, enter the port's IP address, and the SSH port and Telnet port.



Configure Port Settings

Configure the remaining port settings, as needed or required.

1. Select the terminal emulation type from the drop-down menu in the Emulation field. This is the terminal emulation mode used to match the serial targets connected to the ports. The choices are:
   - VT100
   - VT220
   - VT320
   - ANSI
2. Set Encoding if you want Raritan Serial Console (RSC) to always use a specific character encoding for this port.

   Encoding overrides the global RSC setting for the port to whatever value you set.

   The choices are: DEFAULT,US-ASCII,ISO8859-1, ISO8859-15,UTF-8, Shift-JIS, EUC-JP, EUC-CN, EdUC-KR.
3. In the Equipment Type field, indicate whether you want the SX II to automatically detect a physical connection to the target. The default is Auto Detection.
   - Auto Detection
   - Force DTE: SX II acts as a piece of data terminal detection equipment to detect targets connected to it.
   - Force DCE: SX II acts as a piece of data communications equipment to detect equipment connected to it.

   Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. SX II does not support autodetection of both DCE and DTE on the same port.
4. Select the value of Bits Per Second from the Bits Per Second drop-down menu.
5. Select the Parity Bits from the Parity Bits drop-down menu.

6. Select the Flow Control from the Flow Control drop-down menu.
7. If you need to configure the delay between when individual characters are sent via the port, enter the time in milliseconds in the Char Delay field.
8. To configure the delay between when lines of text are sent via the port, enter it in the Line Delay field.
9. Configure the sendbreak duration by entering the send break time in the Send Break Duration field. The send break is configurable from 0ms - 1000ms.
10. The Always Active setting affects port data logs. Select Always Active if you want to log activities coming into a port even if no user is connected.

    The default option is to not maintain port access without a connected user, which means ignore data coming into a port when no user is connected.
11. Port Detection: When disabled, the port will always be shown as "UP", bypassing port detection. This can be useful for targets that show issues conflicting with the Port/DTE/DCE detection.
12. Select from the Multiple Writers drop-down if you want multiple clients to be able to write to the port at the same time. The default behavior is that only one user may have write access to the port at a single time.
13. Select Suppress Messages to prevent messages from being displayed to anonymous users connecting to SX II via Direct Port Access.
14. Select the Escape Mode: Control or None.

    The escape sequence affects only the CLI. When entering escape mode, the user is given a menu of commands that can be performed (for example, gethistory, power commands, and so forth), a command to return to the port session, and a command to exit the port connection.

    The default is None.
15. Type the character in the Escape Character field. The default for the SX II is] (closed bracket).

    Raritan recommends that you *do not* use [or Ctrl-[. Either of these may cause unintended commands, such as invoking the Escape Command unintentionally. This key sequence is also triggered by the arrow keys on the keyboard.
16. Type a command in the Exit Command field, such as `logout`.

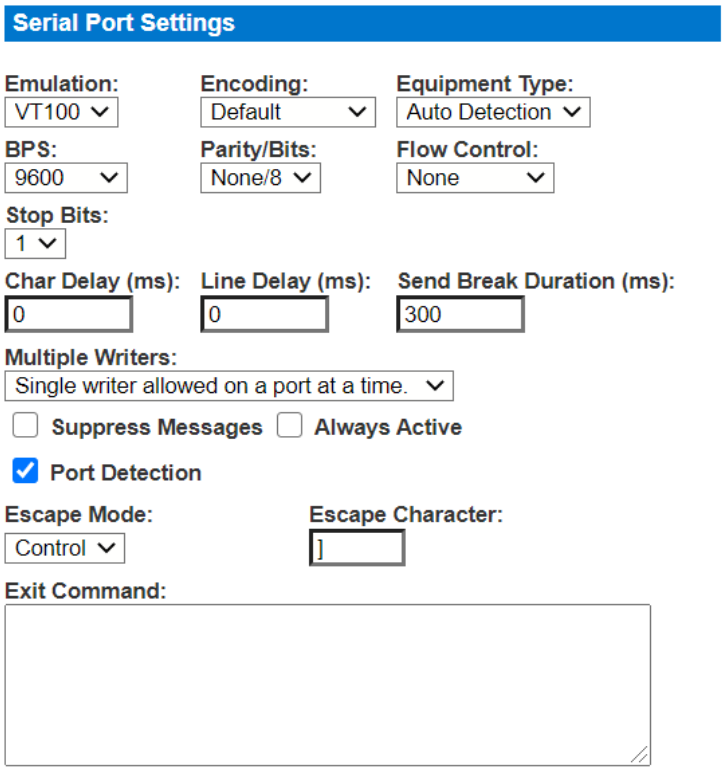
    This is the command that is sent to your system when a user with write permission disconnects from the port.

    The main function of this command is to ensure that the user's session on the target machine is closed; however, it is not imperative to have an Exit command configured on a port.

Note: See Configure Discovery Port Using CLI for details on port configuration commands.

---

17. Click OK to save, or click Reset to Defaults to start over.



Apply Settings to Other Ports

Once finished, you can apply the same port settings to other ports.

1. Select the ports from the Apply Serial Port Settings To Other Ports section of the page by selecting them individually or using the selection buttons at the bottom of the page.

2. Click OK to apply the port configuration settings.

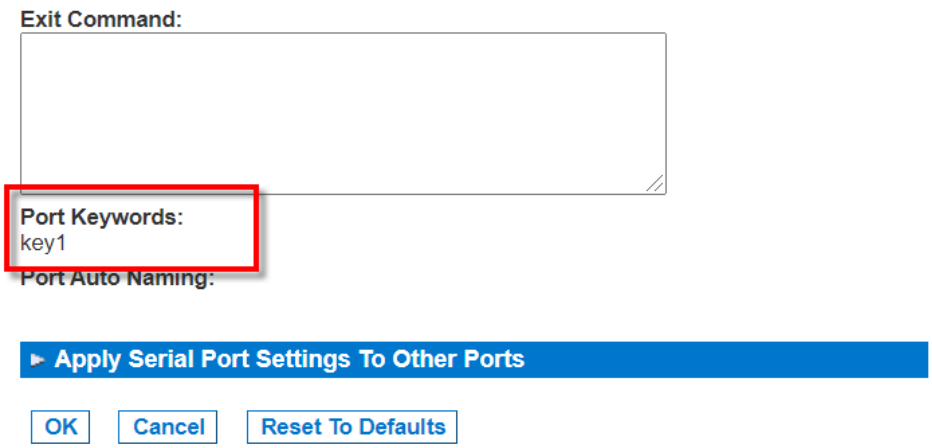
Port Keyword List

Port keywords work as a filter. You can create port keywords and associate them with Event Management Destinations, such as Audit Log, SNMP, Syslog, SMTP for "Serial Alert" under User Activity.

If a keyword is detected -

- A corresponding event is sent via SMTP (if configured).
- A corresponding trap is sent via SNMP (if configured).

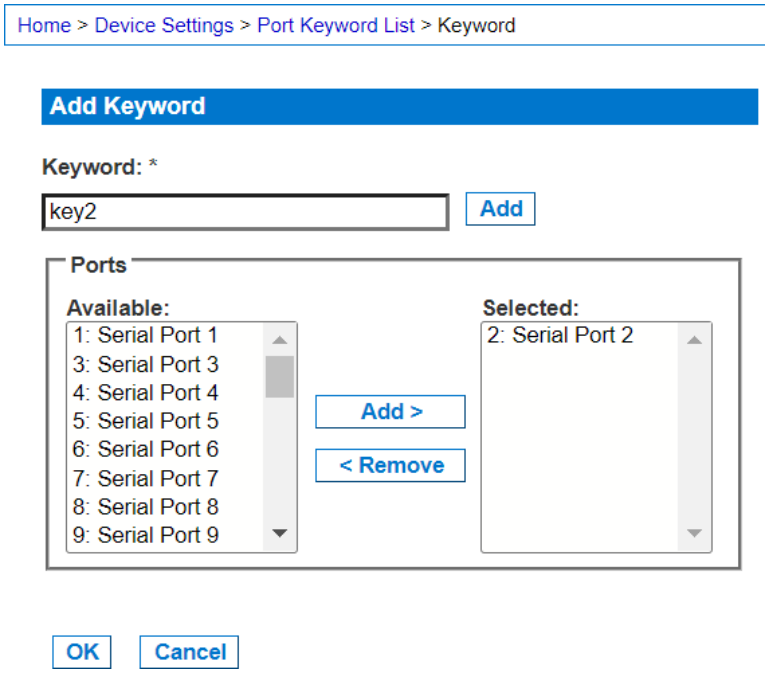
This feature is useful for notifying administrators if a particular event occurs on a port. For keywords to trigger when no users are connected to a port, "Always Active" must be selected on the port's Port Configuration page. A list of existing port keywords is displayed on the Port Configuration page, at the bottom of the page, near Exit Command.



The Serial Alert event is selected from the Event Management - Destinations page.

1. Choose Device Settings > Port Keywords. The Port Keyword List page opens.

2. Click Add at the bottom of list on the page. The Keyword page opens.



3. Type a keyword in the Keyword field.
4. Select the Port(s) you want to associate with that keyword.
5. Click Add to add them to the Selected box.
6. Click OK.

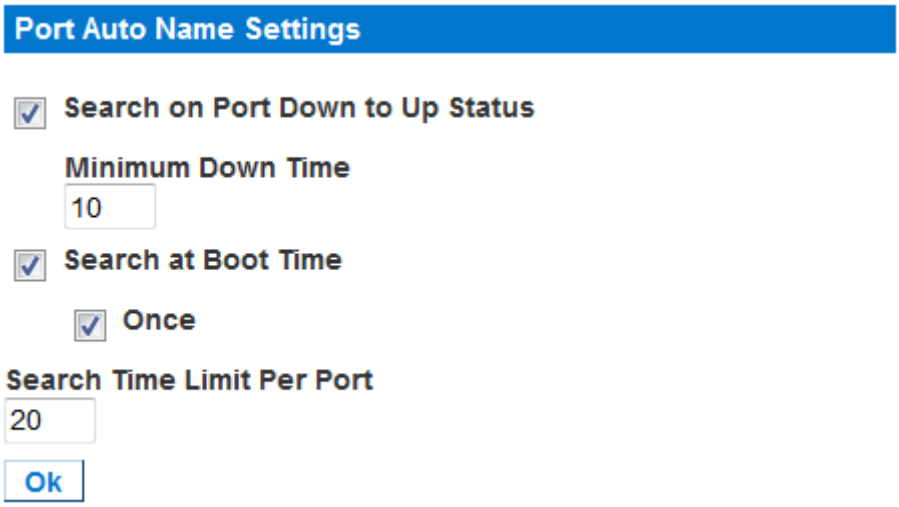
Port Auto Name

Port Auto Name automatically detects a port's System Name from the target output. You can configure when you want auto naming to run, and select the trigger and matching string pattern pairs to assign to each port. These pairs form the basis of the search. When the auto name process begins, the trigger string is sent to a target and the time limit begins. As data is returned, ANSI color codes are filtered out and the pattern match strings are applied against the data to seek a match. When a matching name is found, the port's name field is updated and saved. Names are not unique in SX II. If a name is too long, it is rejected. If a name is not found for a port, the name is set to default: Serial Port #

To configure Port Auto Name:

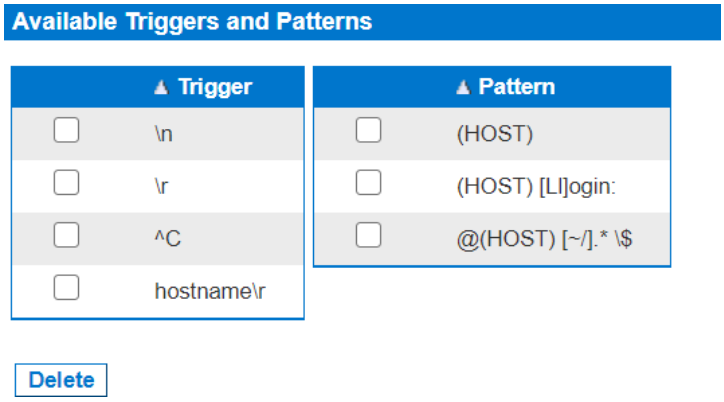
1. Choose Device Settings > Auto Port Name.

2. Select when Auto Name will run:



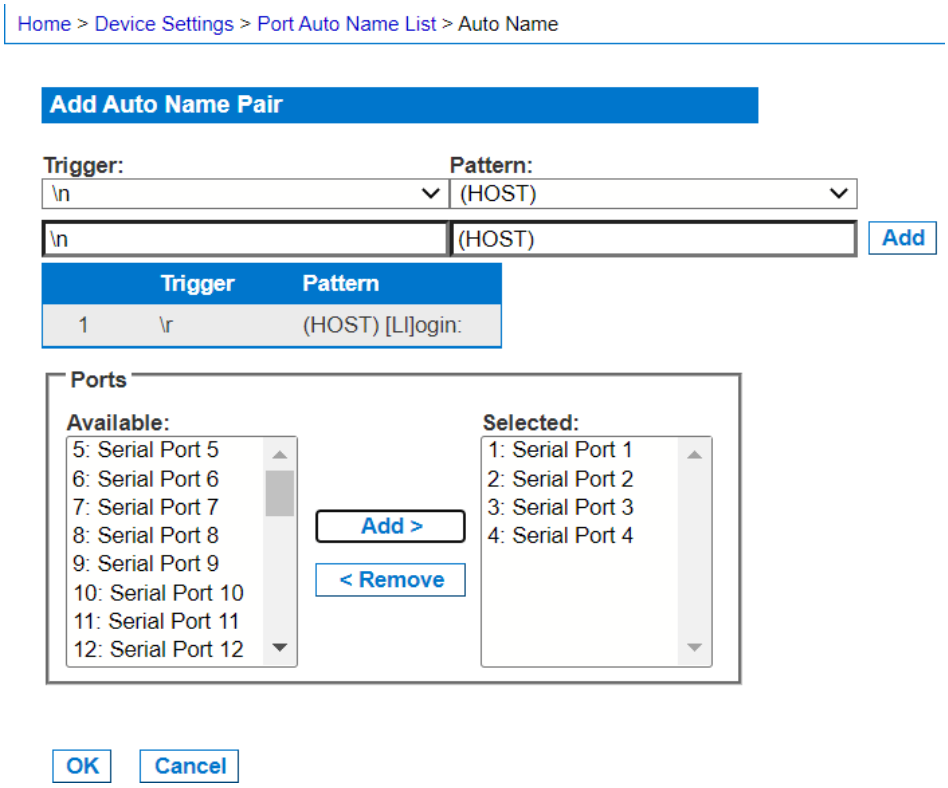
   - Search on Port Down to Up Status: Port name search will start when a port changes from Down to Up status, if the port has been down for the specified Minimum Down Time.
     - Minimum Down Time: Enter the time in seconds.
   - Search at Boot Time: Port name search will start for all configured ports as soon as the system starts.
     - Select Once to allow the Port Auto Name search process to happen once, and then the setting will be turned off when search completes.
3. Search Time Limit Per Port: Enter the time in seconds to allow for each port name search. If the search times out, the default port name is saved.
4. Click OK to save.
5. Select the triggers and patterns you want to use in the search. Triggers prompt a response from the target. Patterns are the strings to match in a found name:

- Available Triggers and Patterns: Select the checkbox of any trigger or pattern you want to exclude and click Delete. **Optional.**



- Port Pairs: Click Add to open the Add Auto Name Pair dialog. Select a common Trigger and Pattern, or type directly in the text fields below the lists, then click Add. Select the ports to assign these search terms, then Add to the Selected list. Click OK to save.

- Supported special characters: \n, \r, ^C, \xXX (an octet in hexadecimal)
- \ and ^ may be escaped as \\ and \^ to negate their special operation.
- (HOST) indicates the expected location of the host name.



- Your assigned Port Pairs display in the main page.

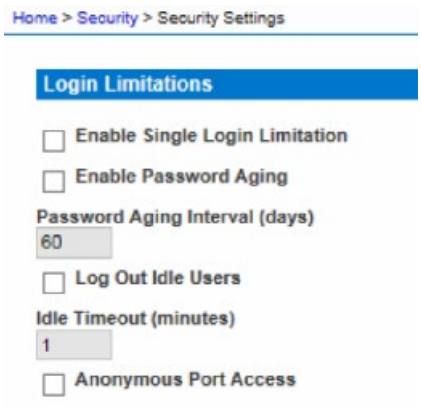
Configure Security Settings from the Remote Console

Login Limitations

Using login limitations, you can specify restrictions for single login, password aging, and the logging out idle users.

Login limitations are configured on the Security Settings page.

- Select Security > Security Settings.



- Enable Single Login Limitation

  When selected, only one login per user name is allowed at any time. When deselected, a given user name/password combination can be connected into the appliance from several client workstations simultaneously.

- Enable Password Aging

  When selected, all users are required to change their passwords periodically based on the number of days specified in Password Aging Interval field.

  This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password change is required. The default is 60 days.

- Log Out Idle Users and Idle Timeout

  When selected, users are automatically disconnected after the amount of time you specify in the Idle Timeout (minutes) field. If there is no activity from the user, all sessions and all resources are logged out. Range is 1-365 minutes.

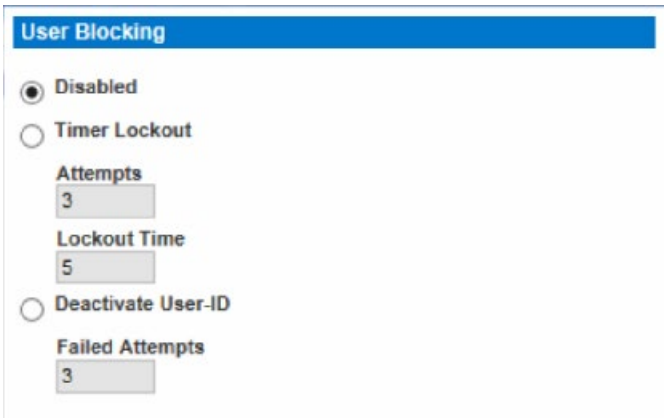
- Anonymous Port Access

  When selected, users can access ports via SSH and Telnet using username anonymous only, so long as Direct Port Access is enabled for the port. When the setting is enabled, a user group called "@anonymous" is added. The permissions of this group determine which DPA ports the anonymous user can access.

User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts.

- Select Security > Security Settings.



The three options are mutually exclusive:

- Disabled

  The default option. Users are not blocked regardless of the number of times they fail authentication.

- Timer Lockout

  Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:

  - Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10 and the default is 3 attempts.
  - Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes and the default is 5 minutes.

  Note: Users in the role of Administrator are exempt from the timer lockout settings.

- Deactivate User-ID

  When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field:

  Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.

When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the User page.

Strong Passwords

Enable and configure strong passwords on the Security Settings page.

- Select Security > Security Settings to configure strong passwords.

Strong passwords provide more secure local authentication for the system. Using strong passwords, you can specify the format of valid SX II local passwords such as minimum and maximum length, required characters, and password history retention.

Users with passwords not meeting strong password criteria are automatically required to change their password on their next login.

When not enabled, only the standard format validation is enforced.

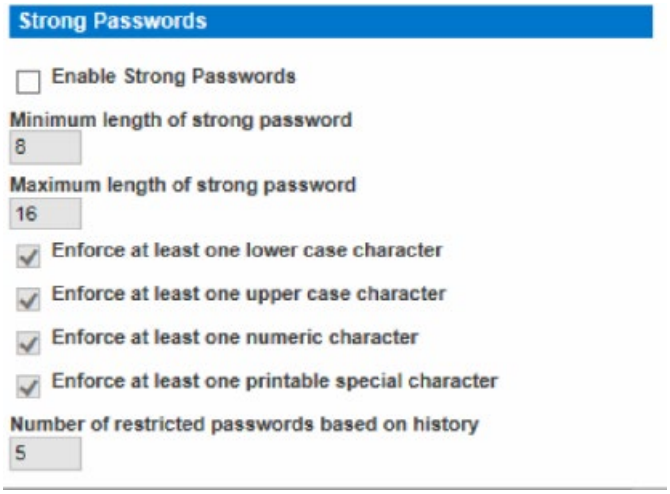
The minimum, general requirements when strong passwords are enabled are that -

- Passwords must be at least 8 characters long
- Have at least one alphabetical character
- Have at least one nonalphabetical character such as a punctuation character or number
- The first four characters of the password and the user's username cannot match

  A password cannot begin with a space or end with a space

To enforce this use of a special character, select "Enforce at least one printable special character".

"Number of restricted passwords based on history" enforces the number of prior passwords that cannot be repeated. The range is 1-12 and the default is 5.



Configure Encryption & Share

Using the Encryption & Share settings you can specify the type of encryption used, PC share modes, and the type of reset performed when the SX II Reset button is pressed.

WARNING: If you select an encryption mode that is not supported by your browser, you will not be able to access the SX II from your browser.

1. Choose one of the options from the Encryption Mode drop-down list. When you select a mode, the associated cipher displays in the Cipher Configuration box.

   When an encryption mode is selected, ensure that your browser supports it, or you will not be able to connect to the SX II.

   - Auto: This is the recommended option. The SX II autonegotiates to the highest level of encryption possible.

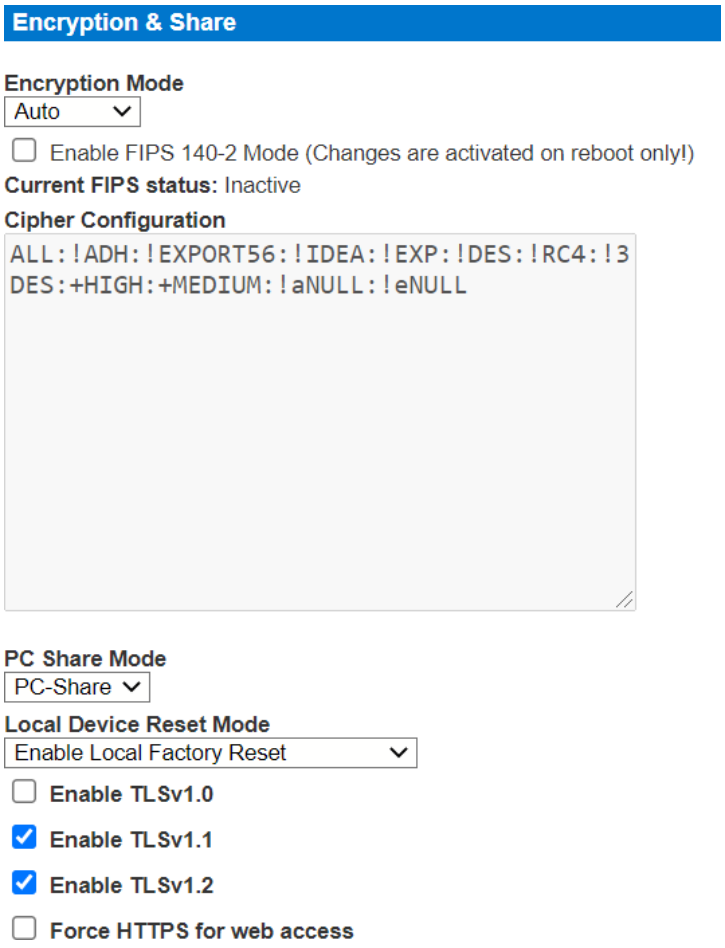
     You must select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms.
   - AES - 128: 128 is the key length. See ***Checking Your Browser for AES Encryption*** (on page 158) for more information.
   - AES - 256: 256 is the key length. See ***Checking Your Browser for AES Encryption*** (on page 158) for more information.
   - Custom: Enter your own custom cipher. Openssl v1.0.2 ciphers are accepted as values.
2. For government and other high security environments, enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox. See***FIPS 140-2 Support Requirements*** (on page 158).
3. PC Share Mode - Determines global concurrent remote access, enabling up to remote users to simultaneously log into one SX II and concurrently view and control the same target device through the device. Click the drop-down list to select one of the following options:
   - Private - No PC share. This is the default mode. Each target device can be accessed exclusively by only one user at a time.
   - PC-Share - targets can be accessed by up to ten users (administrator or non-administrator) at one time. One user will have write permission to the port and others will have read only, unless this port is configured in multi-write mode.
4. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button at the back of the device is depressed. For more information, see Resetting the SX II Using the Reset Button. Choose one of the following options:
   - Enable Local Factory Reset (default) - Returns the SX II device to the factory defaults.
   - Enable Local Admin Password Reset - Resets the local administrator password only. The password is reset to *raritan*.

- Disable All Local Resets - No reset action is taken.

5. Select the checkboxes of each TLS protocol version you want to enable. TLS v1.2 is the most secure protocol option. Select the most secure version that your environment supports. All versions are enabled by default. Unchecked protocols are not used. You should uncheck the lesser options to ensure they are not used. At least one protocol must be enabled.

   Note for Users with CC-SG: CommandCenter Secure Gateway v6.2 and below only support TLS v1.0. If you are using CC-SG v6.2 or below, TLS v1.0 will be used to connect with SX II even if it is disabled here. If you are using CC-SG 7.0 and higher, CC-SG and SX II use the most secure protocol.

6. Click OK to apply the settings.



Checking Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer or navigate to the https://www.fortify.net/sslcheck.html website using the browser with the encryption method you want to check. This website detects your browser's encryption method and displays a report.

AES 256-bit encryption is supported on the following web browsers:

- Edge
- Firefox
- Internet Explorer
- Chrome
- Safari

In addition to browser support, AES 256-bit encryption requires the installation of Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files if you are using VKC/VKCS with Raritan KVM products, or RSC with Raritan serial products.

Jurisdiction files for various JREs™ are available at the “other downloads” section the Java download website.

FIPS 140-2 Support Requirements

The SX II supports the use of FIPS 140-2 approved encryption algorithms. This allows an SSL server and client to successfully negotiate the cipher suite used for the encrypted session when a client is configured for FIPS 140-2 only mode.

Following are the recommendations for using FIPS 140-2 with the SX II.

SX II

Set the Encryption & Share to Auto on the Security Settings page. See ***Configure Encryption & Share*** (on page 156).

Microsoft Client

FIPS 140-2 should be enabled on the client computer and in Internet Explorer®.

To enable FIPS 140-2 on a Windows® client:

1. Select Control Panel > Administrative Tools > Local Security Policy to open the Local Security Settings dialog.
2. From the navigation tree, select Select Local Policies > Security Options.
3. Enable "System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing".
4. Reboot the client computer.

To enable FIPS 140-2 in Internet Explorer:

1. In Internet Explorer, select Tools > Internet Options and click on the Advanced tab.
2. Select the Use TLS 1.0 checkbox.
3. Restart the browser.

Enable FIPS 140-2

For government and other high security environments, enabling FIPS 140-2 mode may be required.

The SX II uses an embedded FIPS 140-2-validated cryptographic module running on a Linux® platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.

Once this mode is enabled, the private key used to generate the SSL certificates must be internally generated; it cannot be downloaded or exported.

Note that performance may be impacted once FIPS 140-2 mode is enabled.

To enable FIPS 140-2:

1. Access the Security Settings page.
2. Enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox in the Encryption & Share section of the Security Settings page.

   You will utilize FIPS 140-2 approved algorithms for external communications once in FIPS 140-2 mode.

   The FIPS cryptographic module is used for encryption of session traffic.
3. Reboot the SX II. **Required**

   Once FIPS mode is activated, 'FIPS Mode: Enabled' will be displayed in the Device Information section in the left panel of the screen.

   For additional security, you can also create a new Certificate Signing Request once FIPS mode is activated. This will be created using the required key ciphers. Upload the certificate after it is signed or create a self-signed certificate. The SSL Certificate status will update from 'Not FIPS Mode Compliant' to 'FIPS Mode Compliant'.

   When FIPS mode is activated, key files cannot be downloaded or uploaded. The most recently created CSR will be associated internally with the key file. Further, the SSL Certificate from the CA and its private key are not included in the full restore of the backed-up file. The key cannot be exported from SX II.

Enabling Force HTTPS for Web Access

Force HTTPS for web access is disabled by default. When enabled, SX II forces HSC/RSC to launch using HTTPS, and SX II will perform validation of server certificate for downloads even if Device Settings>Device Services>Enable RSC Download Server Certificate Validation is not checked.

If you are using HSC/RSC with this setting enabled, make sure that the Device CA or self-signed certificate is added to the Trusted Root CA store of the browser.

To enable or disable Force HTTPS for web access:

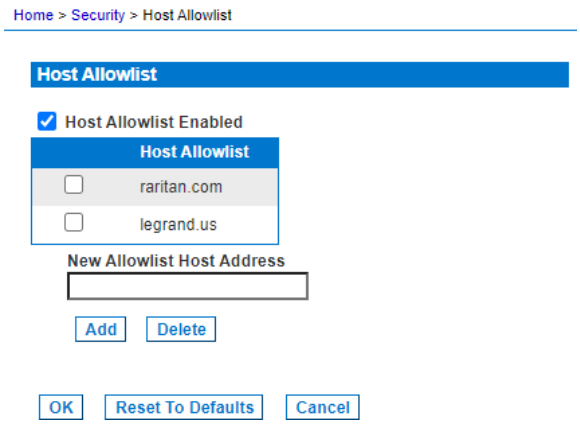
1. Choose Security > Security Settings.
2. In the Encryption and Share section, select the Force HTTPS for Web Access checkbox to enable, or clear the checkbox to disable.

3. Click OK to save.
   - When disabling the feature, restart your browser after saving. Switching between enabled/disabled may require a refresh of the browser cache.

Host Allowlist

The Host Allowlist feature helps prevent host header attacks by limiting what a web client can send in the HOST header of an HTTP request.When enabled, the HOST header is checked and only addresses or hostnames that are in the allowlist are permitted. If the HOST header contains a domain or IP that is not in the list, then the client HOST specified will be removed and replaced with the device IP address. Redirection to non-allowed domains is prevented.

You must have the Security and Device Settings permission to manage this feature.



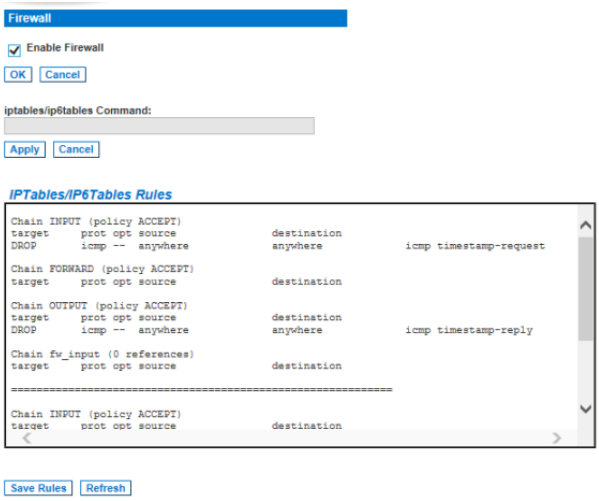
To configure the host allowlist:

1. Click Security > Host Allowlist.
2. To enable or disable the feature:
   - Select the Host Allowlist Enabled checkbox to enable the feature. Clear the checkbox to disable.
3. To add or delete host addresses:
   - Enter an approved domain in the New Allowlist Host Address field, then click Add to add it to the list.
   - Select a host address checkbox in the Host Allowlist, then click Delete to remove it.
4. Click OK to save.

Firewall

The SX II has a firewall function to provide protection for the IP network and to control access between the internal router and LAN 1, LAN 2, and the modem interfaces.

Disabling the firewall deletes your configured rules, but default rules will return when the firewall is enabled again.



1. Choose Security > Firewall. The Firewall page opens, displaying the existing IPTables rules.
2. Select the Enable Firewall checkbox.
3. Click OK.

   Note: When you enable IP forwarding for Dual LAN units, use IPTables rules to create policies for traffic being forwarded between LAN interfaces

   Add IPTable rules as needed. When you enable IP forwarding for Dual LAN units, use IPTables rules to create policies for traffic being forwarded between LAN interfaces.

   These rules take effect immediately but persist permanently only after clicking the Save button. If there is a mistake in the rules and as a result, the appliance becomes inaccessible, this allows you to recover from the mistake. Reboot the system. If you do not Save the rules, you lose them in the reboot.

   Rules are added using the IPTables command to the kernel.
4. Enter a rule in the IPTables Rule field the click Apply. Add as many rules as are needed.
5. Click Save. The rule is displayed on the screen.
6. You can delete some or all of the default rules if you choose to.

SSL and TLS Certificates

SX II uses the Transport Layer Security (TLS) for any encrypted network traffic between itself and a connected client.

When establishing a connection, SX II has to identify itself to a client using a cryptographic certificate.

SX II can generate a Certificate Signing Request (CSR) or a self-signed certificate using SHA-2.

The CA verifies the identity of the originator of the CSR.

The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

Important: Make sure your SX II date/time is set correctly.

When a self-signed certificate is created, the SX II date and time are used to calculate the validity period. If the SX II date and time are not accurate, the certificate's valid from - to date range may be incorrect, causing certificate validation to fail. See Configuring Date/Time Settings.

Note: The CSR must be generated on the SX II.

Note: When upgrading firmware, the active certificate and CSR are not replaced.

To create and install a SSL certificate:

1. Select Security > Certificate.
2. Complete the following fields:
   a. Common name - The network name of the SX II once it is installed on your network (usually the fully qualified domain name). The common name is identical to the name used to access the SX II with a web browser, but without the prefix “http://”. In case the name given here and the actual network name differ, the browser displays a security warning when the SX II is accessed using HTTPS.
   b. Organizational unit - This field is used for specifying to which department within an organization the SX II belongs.
   c. Organization - The name of the organization to which the SX II belongs.
   d. Locality/City - The city where the organization is located.
   e. State/Province - The state or province where the organization is located.
   f. Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.
   g. Email - The email address of a contact person that is responsible for the SX II and its security.

h. Subject Alternative Name (SAN) - Optional. Add up to ten SANs, which may include alternate hostnames. Maximum of 64 characters. This allows devices that are reachable under different names to pass the TLS hostname validation for each name registered in the TLS certificate. Enter the SAN in the Enter Hostname/IP address field, then click Add to create the list of SANs. Select a SAN and click Remove to delete.

i. Challenge Password - Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). Applicable when generating a CSR for CA Certification.

j. Confirm Challenge Password - Confirmation of the Challenge Password. Applicable when generating a CSR for CA Certification.

k. Key length - The length of the generated key in bits. 1024 is the default. Up to 4096 is supported.

3. To generate, do one of the following:

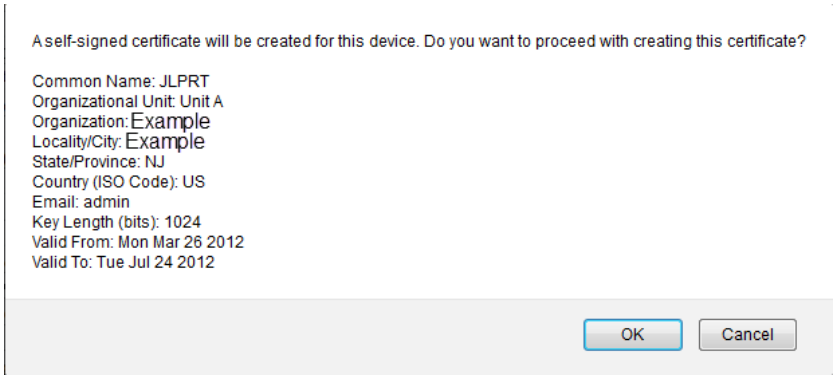
- To generate self-signed certificate, do the following:

a. Select the Create a Self-Signed Certificate checkbox if you need to generate a self-signed certificate. When you select this option, the SX II generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.

b. Specify the number of days for the validity range. Ensure the SX II date and time are correct. If the date and time are not correct, the certificate's valid date range may not be calculated correctly.

c. Click Create.

d. A confirmation dialog is displayed. Click OK to close it.

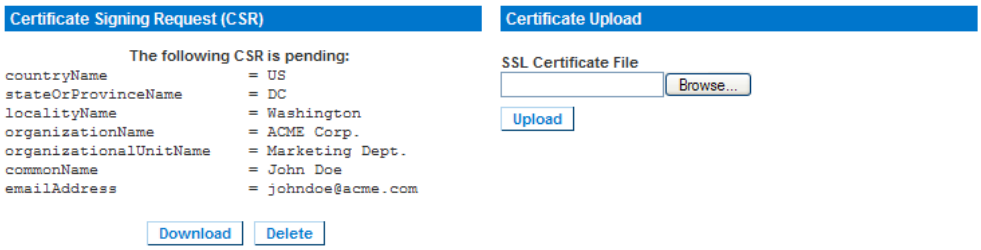


e. Reboot the SX II to activate the self-signed certificate.

- To generate a CSR to send to the CA for certification:

a. Click Create.

b. A message containing all of the information you entered appears.



c. The CSR and the file containing the private key used when generating it can be downloaded by clicking Download CSR.

d. Send the saved CSR to a CA for certification. You will get the new certificate from the CA.

Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

- Once you get the certificate from the CA, upload it to the SX II by clicking Upload.
- Reboot the SX II to activate the certificate.

After completing these steps the SX II has its own certificate that is used for identifying itself to its clients.

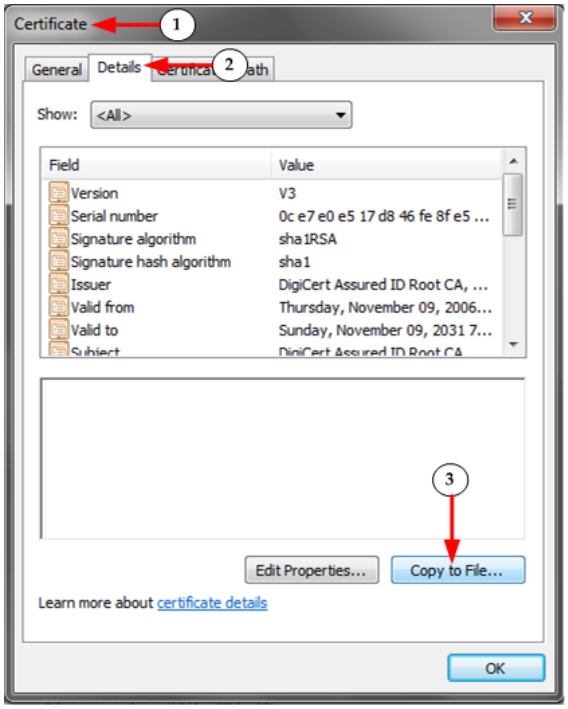
Important: If you destroy the CSR on the SX II there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above. To avoid this, use the download function so you will have a copy of the CSR and its private key.

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

SX II requires an SSL certificate in either Base64-Encoded DER format or PEM format.

If you are using an SSL certificate in binary format, you cannot install it.

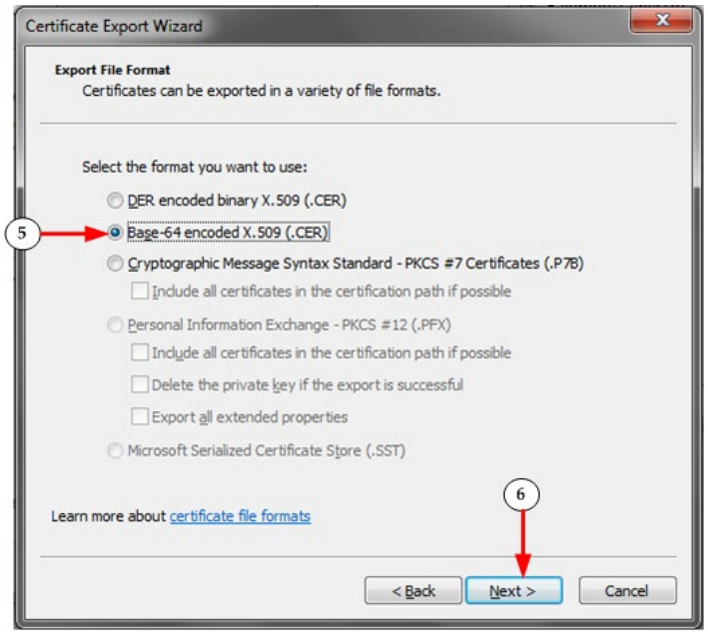
However, you can convert your binary SSL certificate.



1. Locate the DEGHKVM0001.cer binary file on your Windows machine. Double-click on the DEGHKVM0001.cer file to open its Certificate dialog.
2. Click the Detail tab.

3. Click "Copy to File...".

4. The Certificate Export Wizard opens. Click Next to start the Wizard.



5. Select "Base-64 encoded X.509" in the second Wizard dialog.
6. Click Next to save the file as a Base-64 encoded X.509.

You can now install the certificate on your SX II.

TLS Ciphers for Web Access

When set to AUTO, the following TLS ciphers are used on the web port.

TLS v1.0

- | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

TLS v1.1

- | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

TLS v1.2

- | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
- | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
- | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- | TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
- | TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
- | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
- | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
- | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- | TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
- | TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
- | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

Certificate and Smart Card Authentication

Remote Smart Card Authentication Overview

Remote Smart Card Authentication enables users to login to SX II using a smart card reader connected to their client computer. Users can be verified through local or LDAP authentication. Radius and TACACS+ authentication is not supported. This process works exactly like PKI Certificate Authentication, except the client certificates are stored in the smart card instead of in the browser.

Steps to Configure Remote Smart Card Authentication:

Step 1: Use a CA to generate client certificates to be used in authentication.

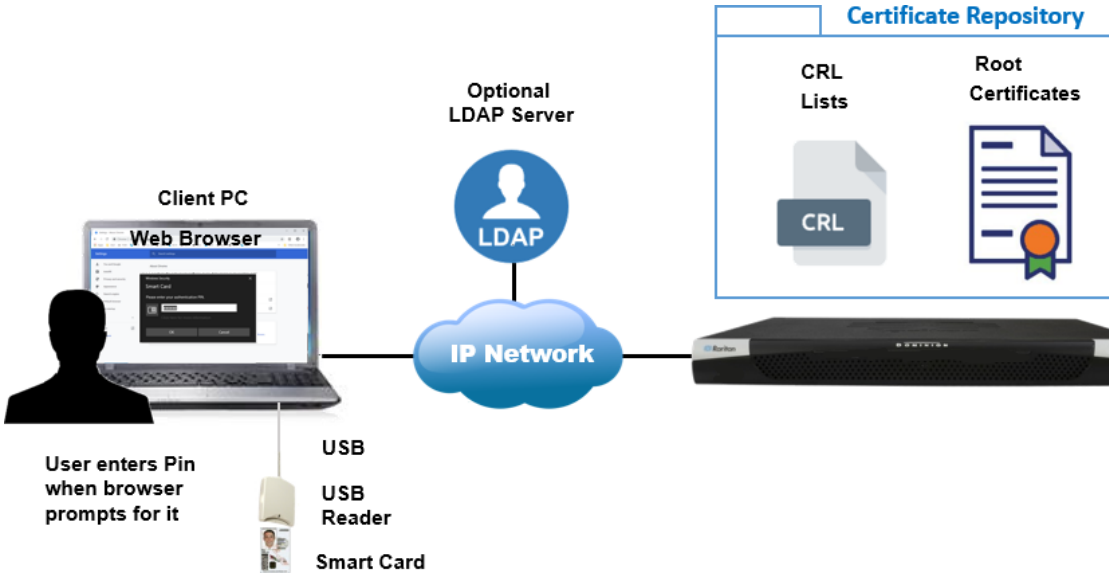
Step 2: Add the CA certificate to the repository: ***Certificate Repository*** (on page 173)

Step 3: Add Client certificates to cards and connect a Smart Card reader to the client computer: ***Supported Smart Card Readers and Cards*** (on page 173)

Step 4: Enable and configure Client Certificate Authentication: ***Client Certificate Authentication Settings*** (on page 170)

Step 5: Configure users on LDAP or locally on the SX II: User Management

Step 6: Use a Smart Card for Remote Login: ***Using a Smart Card at the Client Computer*** (on page 179)



PKI Certificate Authentication Overview

PKI Certificate Authentication enables users to login to SX II using a certificate installed in the browser on their client computer. Users can be verified through local or LDAP authentication. Radius and TACACS+ authentication is not supported. This process works exactly like Remote Smart Card Authentication, except the client certificates are stored in the browser instead of in the smart card.

Steps to Configure PKI Certificate Authentication:

Step 1: Use a CA to generate client certificates to be used in authentication.

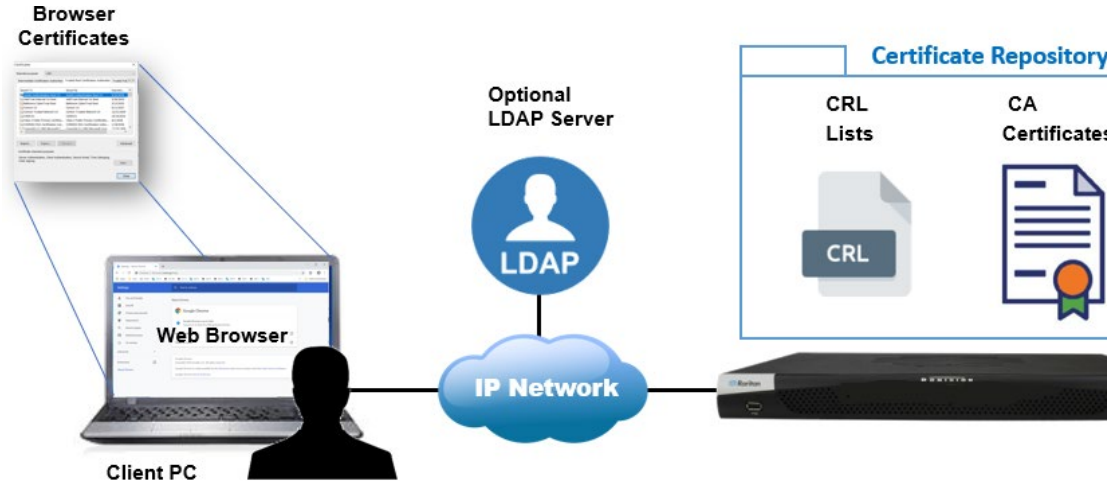
Step 2: Add the CA certificate to the repository: ***Certificate Repository*** (on page 173)

Step 3: Add Client certificates to the browsers of each client computer: Tips for Smart Card and PKI Certificate Authentication

Step 4: Enable and configure Client Certificate Authentication: ***Client Certificate Authentication Settings*** (on page 170)

Step 5: Configure users on LDAP or locally on the SX II: User Management

Step 6: Login with a PKI Certificate in the Browser: ***Login with a PKI Certificate in the Browser*** (on page 180)



Client Certificate Authentication Settings

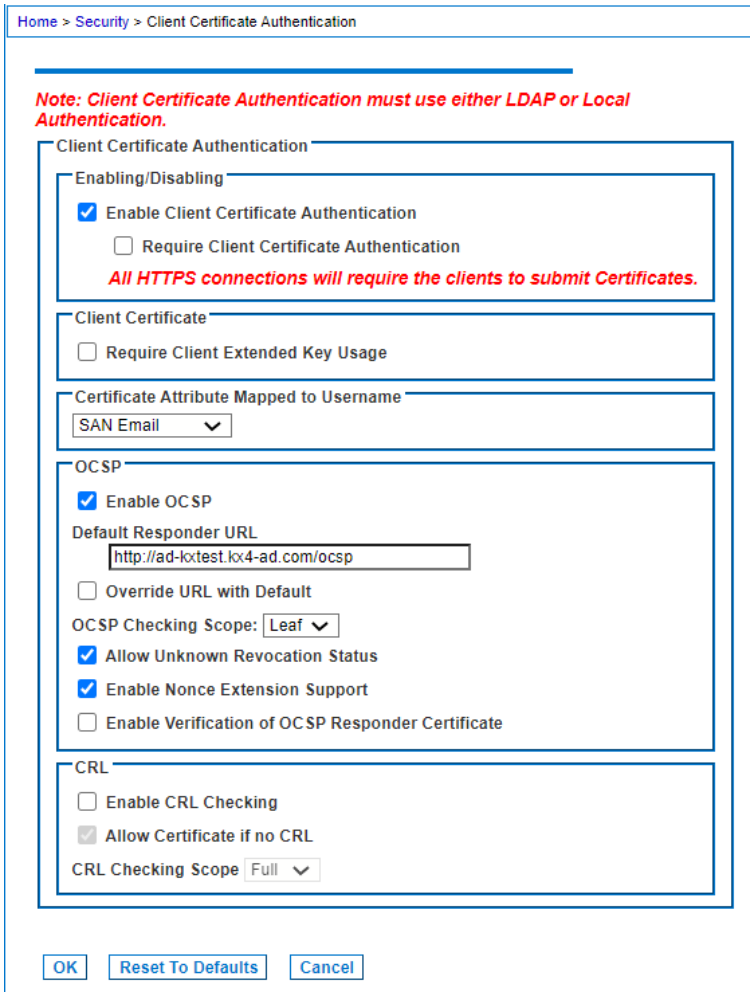
When enabled, Client Certificate Authentication applies to smart card and certificate authentication.

All Client Certificate Authentication settings are disabled by default.

IMPORTANT: Selecting "Require Client Authentication" will lock out standard username/password access to the web interface. Do not enable this setting until you have tested all other settings to verify successful authentication. Another option for ensuring continued access would be to make sure you have access to the SX II Local Port while configuring and testing these settings.

Both OCSP and CRLs are supported as methods to validate certificates against a certificate authority. To use CRLs, you must add them to the repository. See ***Adding CRL (Client Revocation Lists) to the Repository*** (on page 178).

To configure client certificate authentication settings:



1. Click Security > Client Certificate Authentication.
   - You can also access this page via hyperlink at Security > Remote Smart Card Authentication.
2. Enabling/Disabling:
   - Enable Client Certificate Authentication: Select this checkbox to enable client certificates for authentication. When enabled, client certificate authentication will be in effect for smart card authentication and PKI certificate authentication.
   - Require Client Certificate Authentication: **IMPORTANT**-Test and verify all other client certificate settings before using this setting. Removes the ability to authenticate on HTTPS connections via username/password. All access must be authenticated using client certificates, whether by smart card or certificates in the browser.

3. Require Extended Key Usage: Extended Key Usage enforces that the certificate's public key is being used for it’s intended purpose of authentication. When this setting is selected, login will be unsuccessful for certificates without extended key usage or those determined to be intended for purposes other than authentication.
4. Certificate Attribute Mapped to Username: Select the certificate attributes that should be used as the SX II user's login name. The login determines which group the user is in.
   - Common Name
   - emailAddress
   - Other Name
   - DNS Name
   - SAN Email
   - URI
   - UID
5. OCSP: Enable OCSP to use this method to validate certificates against a certificate authority.
   - Default Responder URL: Enter a default responder URL to be used if the certificate does not contain an OCSP server.
   - Override URL with Default: Restricts all OCSP communications to the URL entered in Default Responder URL.
   - OCSP Checking Scope: Leaf will check only the final client certificate for revocation. Full will check the entire chain.
   - Allow Unknown Revocation Status: Possible certificate statuses are Good, Revoked, or Unknown. When selected, SX II will still allow access for certificates with an Unknown status. When not selected, access will only be allowed for certificates with a Good status.
   - Enable Nonce Extension Support: Sends a nonce with the OCSP protocol to help prevent timing attacks. This requires support on the OCSP server side. Make sure that date/time is synced between SX II and the OCSP server.
   - Enable Verification of OCSP Responder Certificate: Ensure that the OCSP response is signed with a trusted CA key. This requires either that the OCSP server send the CA certificate it uses in the OCSP response data, or that the CA certificate for the OCSP server is added into the Certificate Repository.
6. Enable CRL Checking: Enables checking of CRLs to see if a certificate is revoked. CRLs must be added to the Certificate Repository.
   - Allow Certificate if no CRL: Allows access to the device if there is no CRL uploaded.
   - CRL Checking Scope: Leaf will check only the client certificate. Full requires that the entire certificate chain’s CAs and their CRLS are added to the repository.

7. Make sure you haven't selected Require Client Certificate Authentication unless you have already verified your access with these settings, or you have access to the SX II local port.
8. Click OK to save.

Supported Smart Card Readers and Cards

Supported Smart Card Readers

A card reader must be USB-based and CCID compliant.

A complete list of card readers supported by CCID driver version 1.4.30 is available at:

https://ccid.apdu.fr/#readers (***https://ccid.apdu.fr/#readers***)

The following readers were tested with the SX II:

- SCR331 – firmware 0518 or later
- SCM Microsystems SCR3310
- HID Global 3121
- Dell Smarcard Reader Keyboard

Supported Smart Cards

- DOD Common Access Card (CAC)
- Personal Identity Verification (PIV) Card

The following card was tested with the SX II:

- PIVKey C910 – The client authentication certificate must be mapped to 9A.

Certificate Repository

The Certificate Repository enables a central location and management point for all X509 certificates and Certificate Revocation Lists except for the SX II's own server authentication certificate.

Upon upgrade to Release 2.4.0, all previously loaded certificates shall be automatically populated in the repository, with the exception of the SX II device certificate.

The Certificate Repository enables you to store the necessary security certificates for several purposes:

- CA Certificates:
  - LDAP over TLS/SSL
  - 802.1X Security
  - Client Certificate Authentication

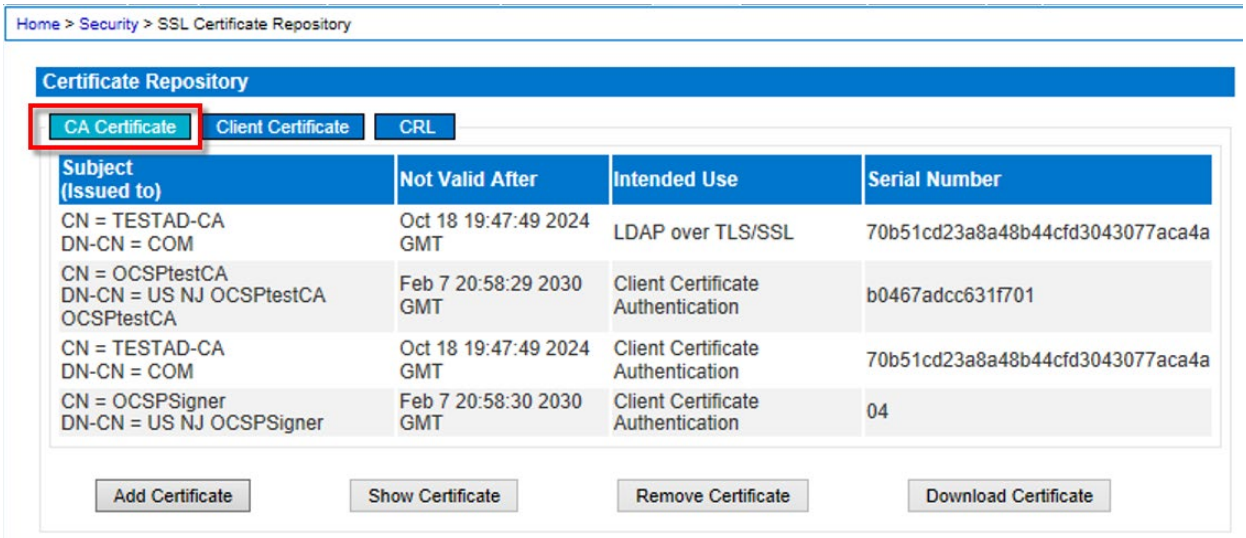
- Client Certificates for 802.1X
- Certificate Revocation Lists for Client Certificate Authentication

Once you load certificates into the repository, they are available for selection in the appropriate feature configuration page.

Important: Do not delete certificates that are in use from the Certificate Repository. The associated feature will fail.

To access the Certificate Repository:

- Click Security > Certificate Repository.



- Click the category you want to view a list of all stored certificates in that category. In the screenshot above CA Certificate is selected.
- In any category, click a certificate to select it, then click Show Certificate to view it, or Download Certificate to download a copy.
- To remove a certificate, select it, then click Remove Certificate. You should only remove certificates that are not in use by any feature.
- To add a certificate, first click the category button (CA Certificate, Client Certificate, or CRL), then click Add Certificate to open the addition form.
  - ***Adding CA Certificates to the Repository*** (on page 175)
  - ***Adding Client Certificates to the Repository*** (on page 176)
  - ***Adding CRL (Client Revocation Lists) to the Repository*** (on page 178)

Adding CA Certificates to the Repository

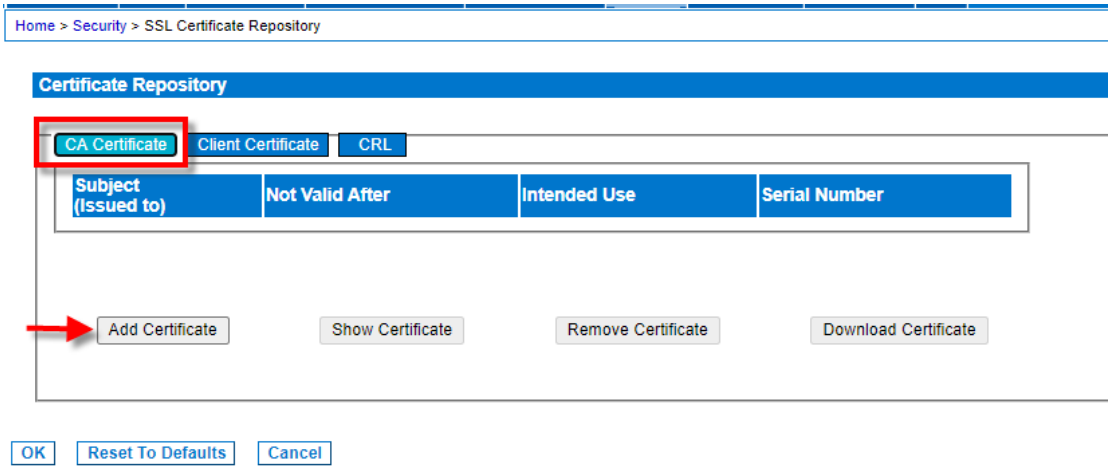
When adding CA Certificates, you must select an "Intended Use" to make the certificate available to the selected function. The same CA Certificate can be added multiple times with different intended uses. For example, a CA certificate added with Intended Use: Client Certificate Authentication may be added again with Intended Use: LDAP over TLS/SSL.

CA certificates added to the repository must be in PEM (Privacy Enhanced Mail) format.

A maximum of 10 CA Certificates can be stored in the repository.

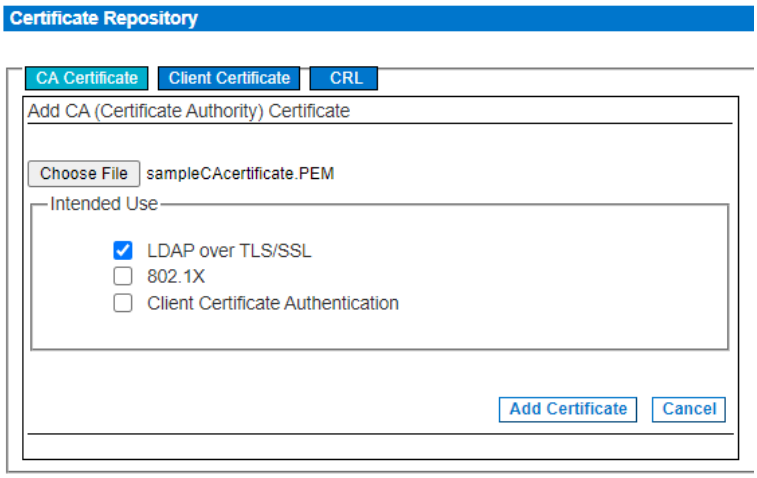
To add CA certificates to the repository:

1. Click Security > Certificate Repository.
2. Click the CA Certificate button, then click Add Certificate.

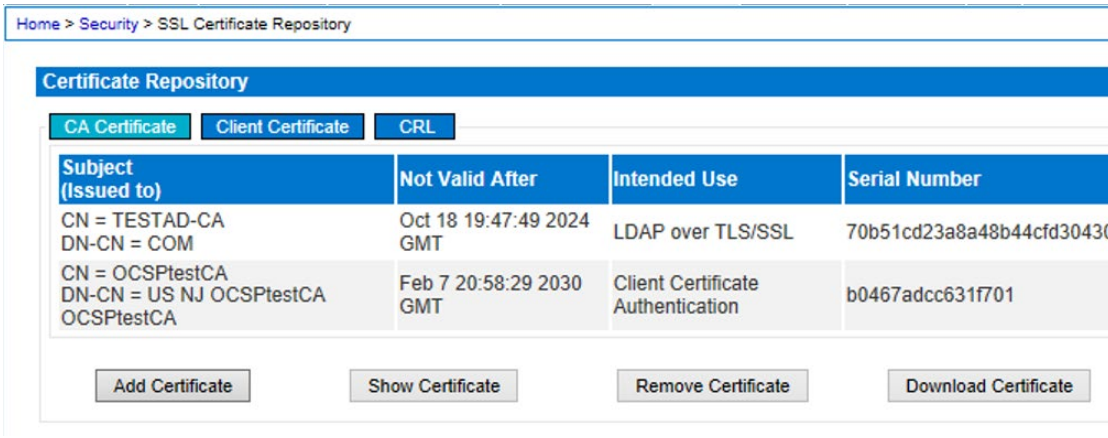


3. The Add CA (Certificate Authority) Certificate tool opens. Click Choose File and select the certificate file.
4. Select the checkbox for the certificate's Intended Use.
   - LDAP over TLS/SSL
   - 802.1X

- Client Certificate Authentication



5. Click Add Certificate.
6. The newly added certificate appears in the list on the main Certificate Repository page, in the CA Certificate category.



Adding Client Certificates to the Repository

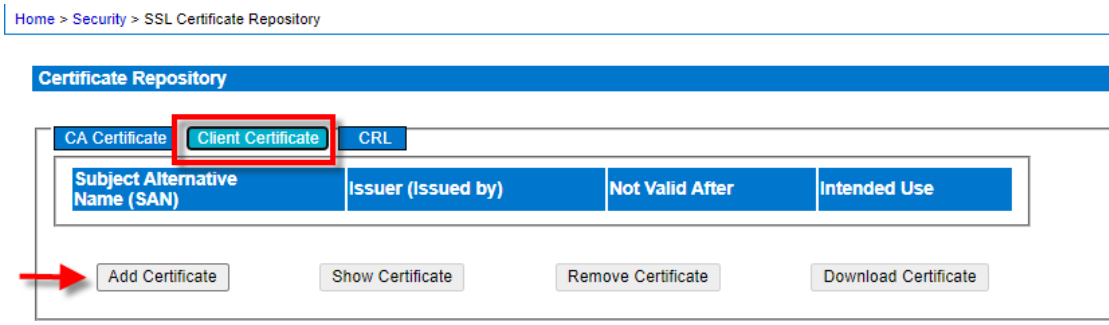
Client Certificates in the repository can be used for 802.1X security. See ***802.1X Security*** (on page 113).

Client certificates must be in PEM (Privacy Enhanced Mail) format. A maximum of 2 Client Certificates can be stored in the repository.

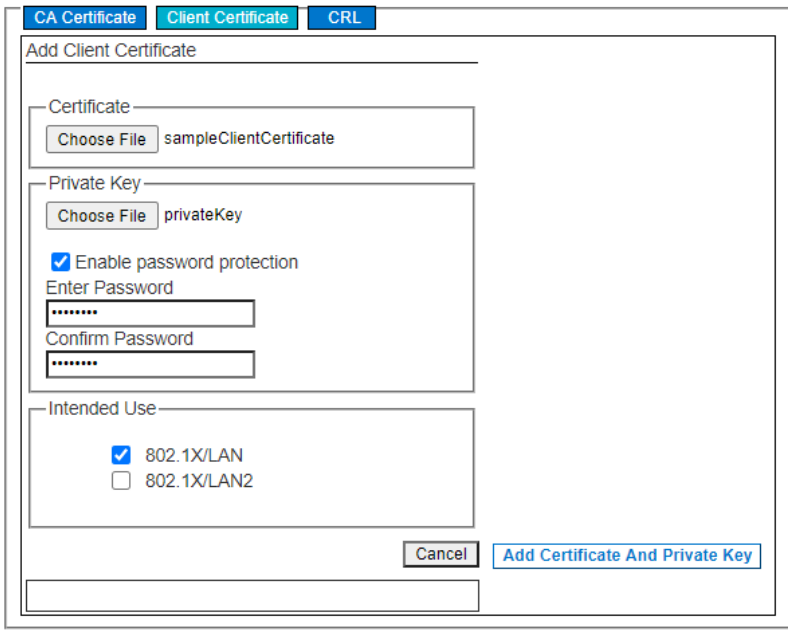
To add client certificates to the repository:

1. Click Security > Certificate Repository.

2. Click the Client Certificate button, then click Add Certificate.



3. The Add Client Certificate tool opens. In the Certificate section, click Choose File and select the certificate file to add it.
4. In the Private Key section, click Choose File and select the private key file to add it.
5. If needed, select Enable Password Protection checkbox, then enter and confirm the password.
6. Select the checkbox for the certificate's Intended Use.
   - 802.1X/LAN
   - 802.1X/LAN2



7. Click Add Certificate and Private Key.
8. The newly added certificate appears in the list on the main Certificate Repository page, in the Client Certificate category.

Adding CRL (Client Revocation Lists) to the Repository

A Certificate Revocation List (CRL) contains certificates that were revoked before they expired. A certificate authority might revoke a certificate if it has been compromised. For more information on CRLs, see RFC 5280.

The CRL has a limited validity period, and updated versions of the CRL are published when the previous CRL's validity period expires. Certificate revocation lists are considered valid until they expire. The URL of the CRL can usually be found in the CRL Distribution Points extension of an X.509 Certificate.

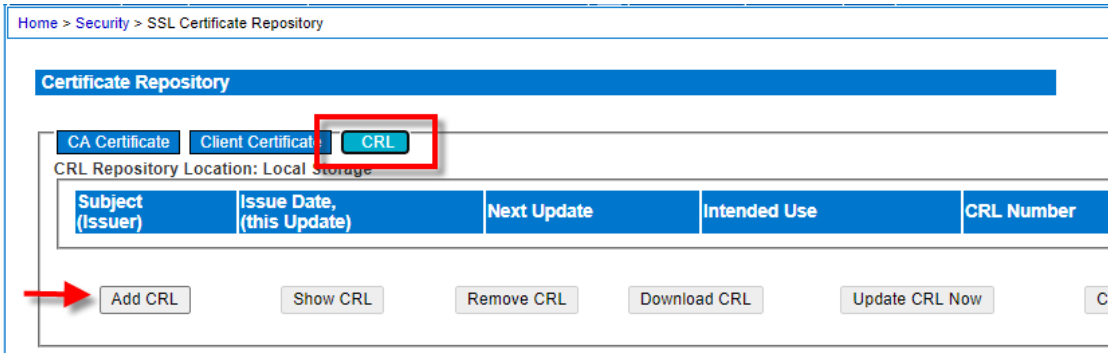
CRLs must be in DER (Distinguished Encoding Rules) format. A maximum of 10 CRLs can be stored in the repository.

A limited amount of internal memory is provided to store CRL files, with an option to use USB storage. CRL files can be large, so additional storage space may be required. An error message will appear if external storage is needed. Inserting a USB stick into the SX II USB port will automatically cause the repository to store CRL files there instead. Any existing CRL's will be copied to the USB stick when it is inserted. You must pre-format the USB stick with a fat32 file system and a **/crl** directory for this purpose.

Note: To add a CRL, the repository must already contain the corresponding CA certificate of the CA that issued and signed the CRL.

To add CRL to the repository:

1. Click Security > Certificate Repository.
2. Click the CRL button, then click Add CRL.



3. The Add CRL (Certificate Revocation List) tool opens. Click Choose File and select the CRL file to add it.
4. The Intended Use is pre-selected as Client Certificate Authentication.
5. Specify the URL for updates to the CRL.
6. Click Add CRL to save.

Reset Certificate Repository to Default

The Certificate Repository can be reset to default, which will delete all existing certificates, CRLs and supporting data from the repository. Using the Reset to Defaults option will leave the SX II with no certificates or CRLs except for the SX II's own device certificate.

To reset the certificate repository:

IMPORTANT: Using reset to defaults will delete all certificates that have been added, for all intended uses.

1. Click Security > Certificate Repository.
2. Click the Reset to Defaults button.
3. Click OK to confirm.

Tips for Smart Card and PKI Certificate Authentication

Various client and browser combinations may behave differently depending on your chosen access client. Check these tips for recommendations.

- For RSCs certificate login from Linux, the certificate needs to be imported to JAVA.
- Browser option to select certificate for authentication displayed on Edge and Chrome logins after session is idle for about 5 minutes, due to internal browser SSL caching and timeouts. If certificate is selected promptly, reconnection is successful. With longer idle times, authentication is not successful, and the browser should be restarted to reconnect. Issue is not observed in Firefox or IE 11.
- Unable to perform Smart Card login on Linux and Apple Mac OS. The login menu is displayed instead. Users are recommended to use HKC. The JRE does not have the capabilities to interface directly with smart card devices as it cannot access the certificate in the browser
- Smart card login fails in Safari. Apple keychain does not see the reader.
- Clicking Cancel at the smart card PIN login will not cause the local username/password login page to display. Instead, either a blank page or "Application Error - Unable to launch the Application" displays. If a local login with username and password is needed, remove the smart card and reload the client.

Using a Smart Card at the Client Computer

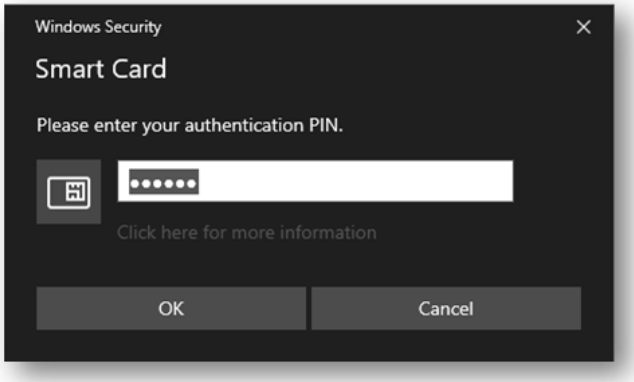
When Client Certificate Authentication is enabled and configured, you can access SX II with a smart card at the card reader connected to your client computer.

To use a smart card at the at the client computer:

1. Insert the smart card into the reader.
2. Launch a browser and go to the SX II URL.

3. When prompted by the browser, enter the smart card PIN. If approved, you will be logged in.

   If login fails, check the Audit log for failure information.

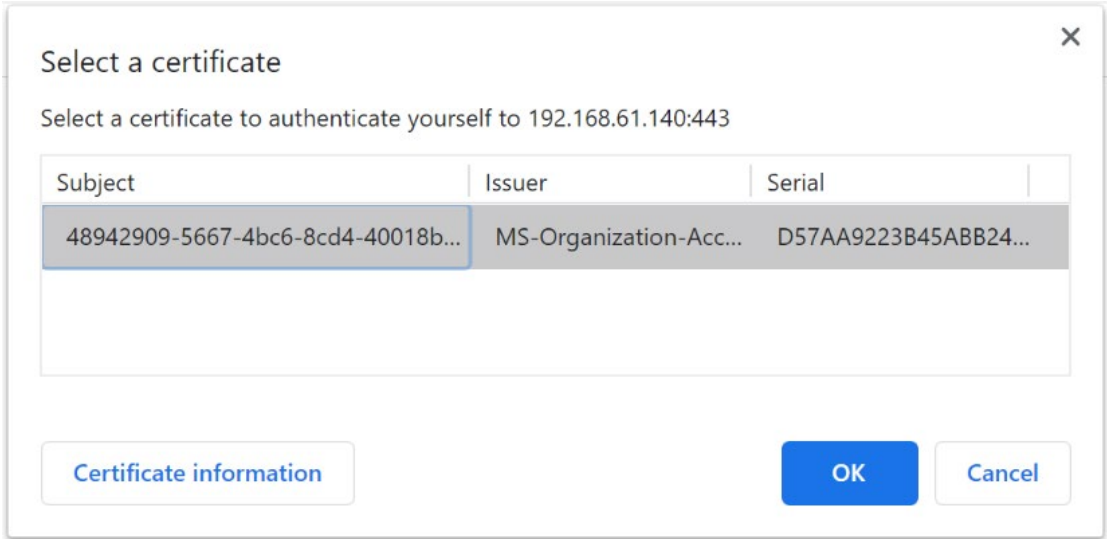


Login with a PKI Certificate in the Browser

When Client Certificate Authentication is enabled and configured, you can access SX II with a client certificate installed in your browser.

To login with a PKI certificate in the browser:

1. Launch a browser and go to the SX II.
2. The browser presents a dialog to select the certificate for authentication. Select the correct certificate, then click OK. If approved, you will be logged in.



Security Banner

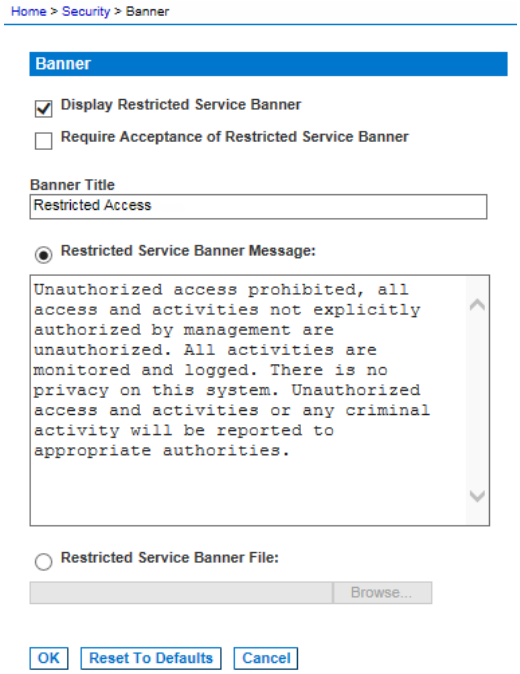
SX II provides you with the ability to add a security banner to the SX II login process. This feature requires users to either accept or decline a security agreement before they can access the SX II. The information provided in a security banner will be displayed in a Restricted Service Agreement dialog after users access SX II using their login credentials.

The security banner heading and wording can be customized, or the default text can be used. Additionally, the security banner can be configured to require that a user accepts the security agreement before they are able to access the SX II or it can just be displayed following the login process. If the accept or decline feature is enabled, the user's selection is logged in the audit log.

To configure a security banner:

1. Click Security > Banner to open the Banner page.
2. Select Display Restricted Service Banner to enable the feature.
3. If you want to require users to acknowledge the banner prior to continuing the login process, select Require Acceptance of Restricted Service Banner. In order to acknowledge the banner, users will select a checkbox. If you do not enable this setting, the security banner will only be displayed after the user logs in and will not require users acknowledge it.
4. If needed, change the banner title. This information will be displayed to users as part of the banner. Up to 64 characters can be used.
5. Edit the information in the Restricted Services Banner Message text box. Up to 6000 characters can be entered or uploaded from a text file. To do this, do one of the following:
   a. Edit the text by manually typing in the text box. Click OK.

b. Upload the information from .txt file by selecting the Restricted Services Banner File radio button and using the Browse feature to locate and upload the file. Click OK. Once the file is uploaded, the text from the file will appear in the Restricted Services Banner Message text box.



Configure Maintenance Settings from the Remote Console

Audit Log

A log is created of SX II system events.

The audit log can contain up to approximately 2000 lines worth of data before it starts overwriting the oldest entries.

To avoid losing audit log data, export the data to a syslog server or SNMP manager. Configure the syslog server or SNMP manager from the Device Settings > Event Management page.

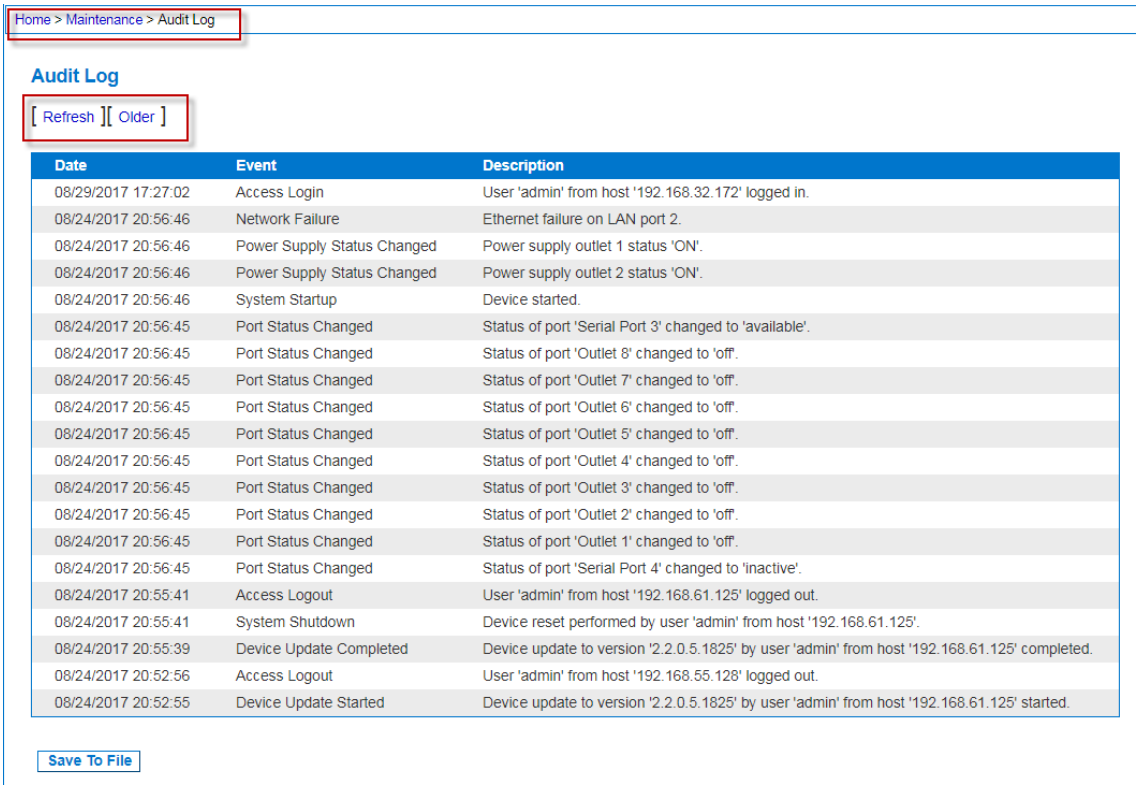
1. Choose Maintenance > Audit Log. The Audit Log page opens.

   The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

   - Date - The date and time that the event occurred based on a 24-hour clock.
   - Event - The event name as listed in the Event Management page.
   - Description - Detailed description of the event.

2. Click Save to File. A Save File dialog appears.

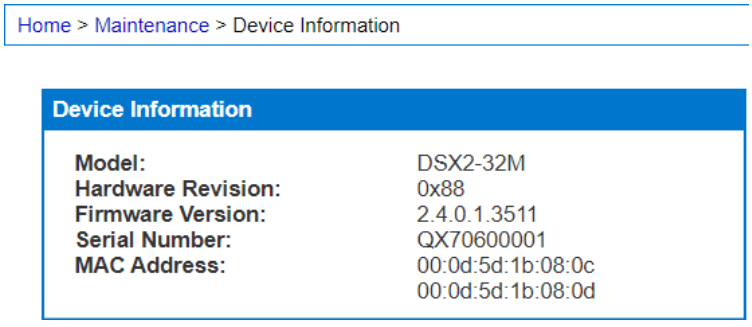
3. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.
4. Click Refresh to refresh the list. Click Older to view older log entries.
5. To page through the audit log, use the [Older] and [Newer] links.



Date	Event	Description
08/29/2017 17:27:02	Access Login	User 'admin' from host '192.168.32.172' logged in.
08/24/2017 20:56:46	Network Failure	Ethernet failure on LAN port 2.
08/24/2017 20:56:46	Power Supply Status Changed	Power supply outlet 1 status 'ON'.
08/24/2017 20:56:46	Power Supply Status Changed	Power supply outlet 2 status 'ON'.
08/24/2017 20:56:46	System Startup	Device started.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Serial Port 3' changed to 'available'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 8' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 7' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 6' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 5' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 4' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 3' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 2' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Outlet 1' changed to 'off'.
08/24/2017 20:56:45	Port Status Changed	Status of port 'Serial Port 4' changed to 'inactive'.
08/24/2017 20:55:41	Access Logout	User 'admin' from host '192.168.61.125' logged out.
08/24/2017 20:55:41	System Shutdown	Device reset performed by user 'admin' from host '192.168.61.125'.
08/24/2017 20:55:39	Device Update Completed	Device update to version '2.2.0.5.1825' by user 'admin' from host '192.168.61.125' completed.
08/24/2017 20:52:56	Access Logout	User 'admin' from host '192.168.55.128' logged out.
08/24/2017 20:52:55	Device Update Started	Device update to version '2.2.0.5.1825' by user 'admin' from host '192.168.61.125' started.

Device Information

Selection Maintenance > Device Information to view information specific to your SX II. This is useful for support.



Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your SX II.

In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism.

For instance, you can quickly provide access to your team from another SX II by backing up the user configuration settings from the SX II in use and restoring those configurations to the new SX II.

You can also set up one SX II and copy its configuration to multiple SX II devices.

Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.

To create a backup file:

1. Choose Maintenance > Backup/Restore.
2. To password protect the backup file, enter a password in the Password Protection field. Optional.
3. Click Backup. The backup file is created and displays as a downloaded file in your browser. Download location varies based on browser.

To restore your SX II:

WARNING: Exercise caution when restoring your SX II to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the SX II.

In addition, if you used a different IP address at the time of the backup, that IP address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

1. Choose the type of restore you want to run:
   - Full Restore - A complete restore of the entire system. Generally used for traditional backup and restore purposes.
   - Protected Restore - Everything is restored except appliance-specific information such as IP address, name, and so forth. With this option, you can setup one SX II and copy the configuration to multiple SX II appliances.
   - Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both:

- User and Group Restore - This option includes only user and group information. This option *does not* restore the certificate and the private key files. Use this option to quickly set up users on a different SX II.
- Device Settings Restore - This option includes only device settings such as power associations and Port Group assignments. Use this option to quickly copy the device information.

2. Click Browse. A Choose File dialog appears.
3. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
4. If the backup is password-protected, enter the password.
5. Click Restore. The configuration (based on the type of restore selected) is restored.

CLI Script

The CLI Script function generates a CLI script file that can be used to configure a different SX II device with the settings of the current SX II. The script follows the model of the SX II CLI.

Scripts created on CC-SG managed SX II devices can be used only for other SX II devices under CC-SG management. Scripts created on SX II models with internal modem include commands that will cause the script to fail on non-modem models. If two devices have a different number of ports, errors will be reported, but the script can continue to run successfully.

Upload the file to another SX II to configure it. Or, you can incorporate the script into your own CLI files.

You must be logged in as admin, or a member of the default ADMIN group to use this function.

To generate the CLI script:

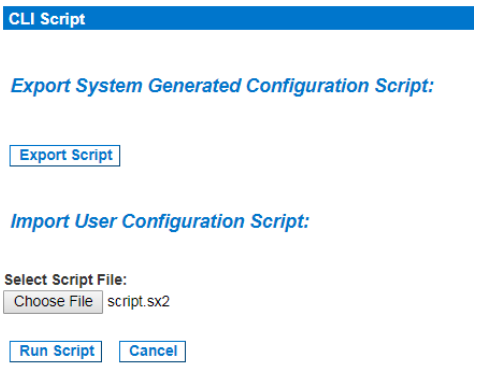
1. Log into the SX II whose configuration you want to use as a script.
2. Choose Maintenance > CLI Script.
3. Click Export Script. The script.sx2 file generates into your browser's download location.
4. Examine the script for any unneeded parameters and delete them, such as extra ports.
5. For security, passwords are not exported. Instead, you will see the password parameter name, such as "secret", "privpass", "authpass", and so on, with a placeholder for the password, for example: "secret_Enter_password_here". To add passwords before importing:

   Search the script for the text "_Enter_password_here", and replace "_Enter_password_here" with the required password. For example, if the parameter name is "secret" and the password is "password":

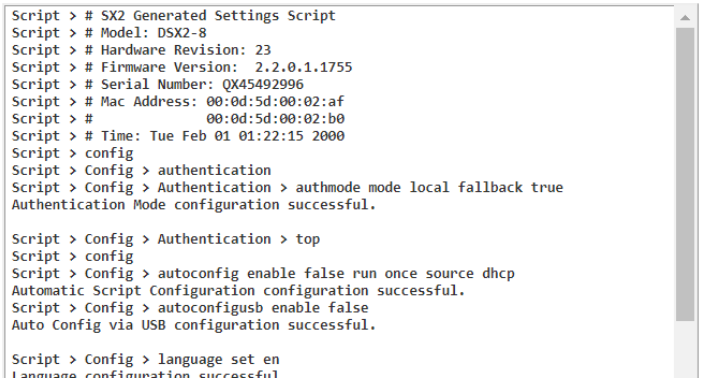
`secret_Enter_password_here` should be replaced by: `secret password`

To import and run the CLI script:

1. Log into the SX II you want to configure with the script.
2. Choose Maintenance > CLI Script.
3. Click Choose File to select the script.sx2 file you generated and click OK. The file name displays next to the Choose File button.



4. Click Run Script. A status message box appears in the same page. As each setting is processed, the results appear in this status box.



5. When your script completes successfully, you will see a Status: Successful. If your script cannot complete due to an error, see ***CLI Script Errors*** (on page 187).

CLI Script Errors

Errors are presented just as they are in the interactive CLI. A caret below the command indicates the position of a syntactic error. Syntactic errors , such as malformed commands, will halt the script. Semantic errors, such as settings that are not possible given the SX II model, will display an error without interrupting processing. Examples of semantic errors are number of ports or overriding settings.

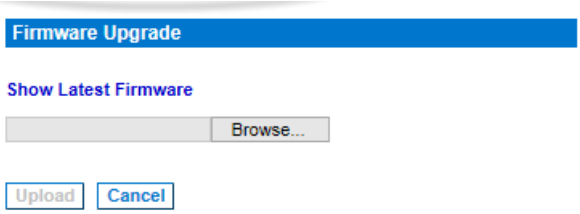
If you encounter errors, you can correct the script and run it again. Some commands will emit an error if run again without a factory reset or otherwise undoing the settings. For example, adding a user or group that already exists. Depending on your goals for your script, you could fix errors and run again, remove the successful commands and run again with corrected failed commands, run the failed commands individually on the interactive CLI, or factory reset the machine and run a completely fixed script again.

Firmware Upgrade

Use the Firmware Upgrade page to upgrade the firmware for your SX II, as well as upgrade from CC-SG if SX II is under CC-SG management.

Important: Do not turn off your SX II appliance or disconnect targets while the upgrade is in progress - doing so will likely result in damage to the appliance.

1. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.



2. Click the Show Latest Firmware link to locate the appropriate Raritan firmware distribution file (*.RFP) on the Raritan website on the Firmware Upgrades web page.
3. Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

   Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.
4. Click Browse to navigate to the directory where you unzipped the upgrade file.
5. Click Upload from the Firmware Upgrade page.

6. Information about the upgrade and version numbers is displayed for your confirmation (if you opted to review target information, that information is displayed as well).

   Note: At this point, connected users are logged out, and new login attempts are blocked.

7. Click Upgrade.

   Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the appliance reboots (1 beep sounds to signal that the reboot has completed).

8. As prompted, close the browser and wait approximately 5 minutes before logging in to SX II again.

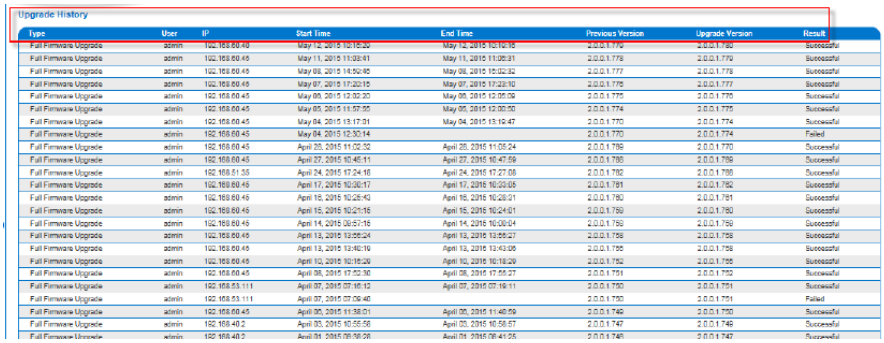
Upgrade History

The SX II provides information about upgrades performed on the SX II and attached devices.

- Choose Maintenance > Upgrade History to view the upgrade history.

Information is provided about the SX II upgrade(s) that have been run, the final status of the upgrade, the start and end times, and the previous and current firmware versions. Information is also provided about the targets, which can be obtained by clicking the show link for an upgrade. The target information provided is:

- Type - The type of target
- User - The user who performed the upgrade
- IP - IP address firmware location
- Start Time - Start time of the upgrade
- End Time - end time of the upgrade
- Previous Version - Previous firmware version
- Upgrade Version - Current firmware version
- Result - The result of the upgrade (success or fail)



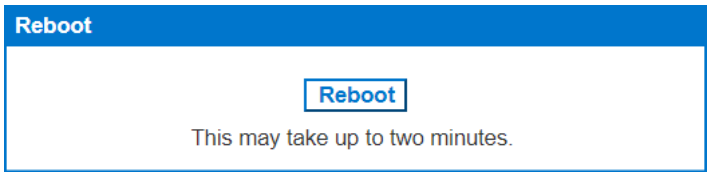
Rebooting the SX II

The Reboot page provides a safe and controlled way to reboot your SX II. This is the recommended method for rebooting.

Important: All connections will be closed and all users will be logged off.

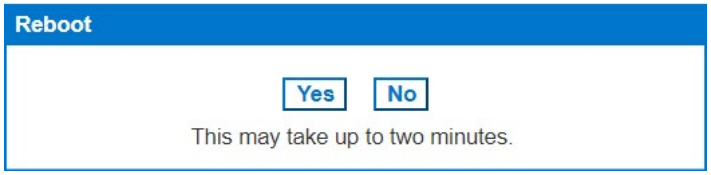
To reboot your SX II:

1. Choose Maintenance > Reboot. The Reboot page opens.



2. Click Reboot. You are prompted to confirm the action. Click Yes to proceed with the reboot.

Rebooting the system will logoff all users.
Do you want to proceed with the reboot?



Reset the SX II Using the Reset Button on the Appliance

On the back panel of the appliance, there is a Reset button. It is recessed to prevent accidental resets, so you need a pointed object to press this button.

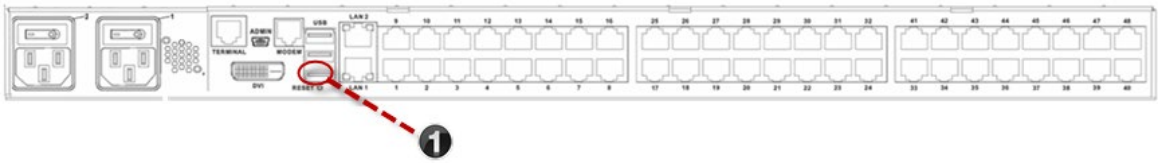
The actions that are performed when the Reset button is pressed are defined on the Encryption & Share page. See ***Configure Encryption & Share*** (on page 156).

Note: It is recommended that you save the audit log prior to performing a factory reset.

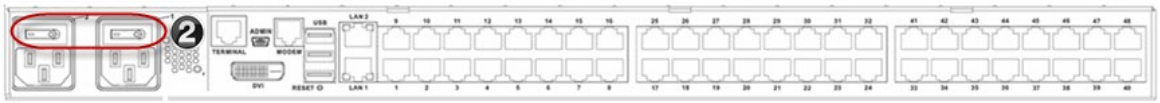
The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see **Audit Log** *(on page 182).*

---

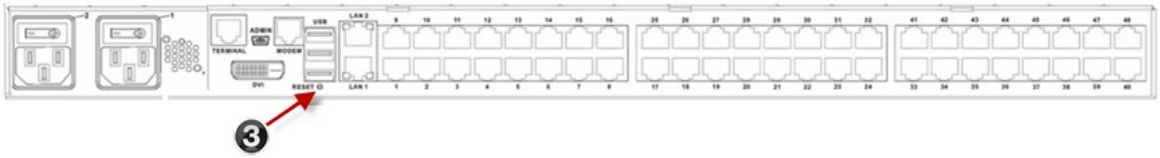
1. To ensure you are able to properly access and press in the Rest button, remove the bottom USB cable that is closest to the Reset button.



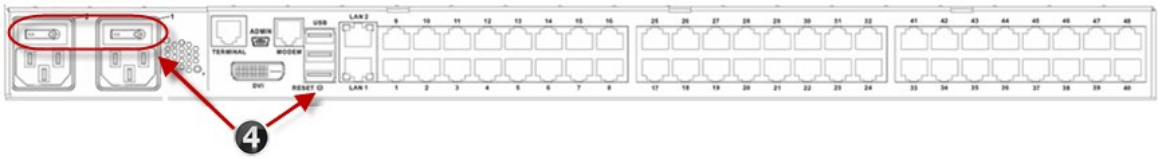
2. Power off SX II.



3. Use a pointed object such as a paperclip to press and hold the Reset button.



4. While continuing to hold the Reset button, power the SX II device back on. Continue holding the Reset button until you hear a beep that is about one second long.



Once the device is successfully reset, two (2) beeps are emitted from the appliance.

Configure Diagnostic Options from the Remote Console

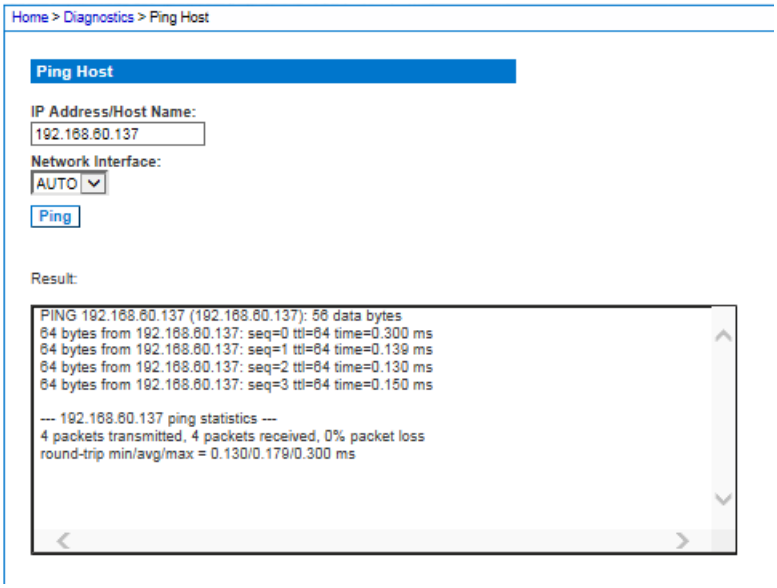
Ping Host Page

Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another SX II is accessible.

1. Choose Diagnostics > Ping Host. The Ping Host page appears.
2. Type either the hostname or IP address into the IP Address/Host Name field.

   Note: The host name cannot exceed 232 characters in length.

3. Click Ping. The results of the ping are displayed in the Result field.
4. Select the interface in the Network Interface drop-down box to ping on a specified interface. **Optional**



Trace Route to Host Page

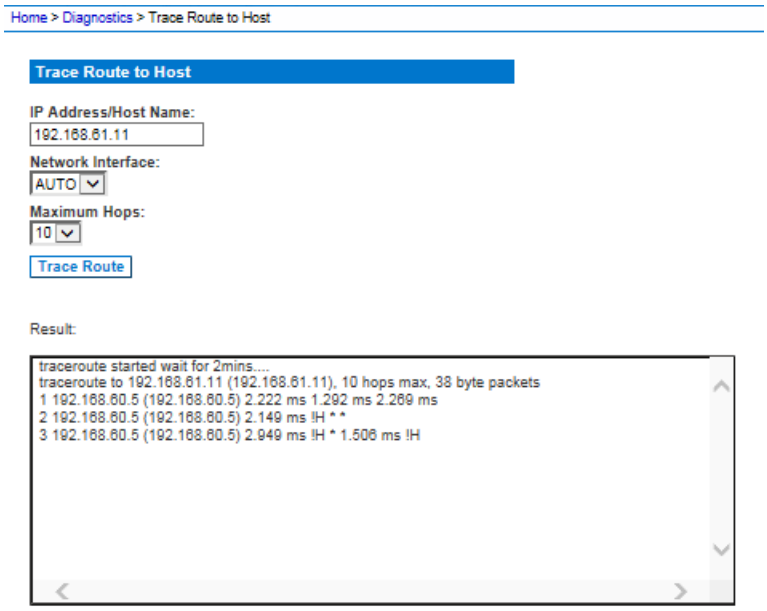
Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

To trace the route to the host:

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type either the IP address or host name into the IP Address/Host Name field.

   Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).
4. Click Trace Route. The trace route command is executed for the given hostname or IP address and the maximum hops. The output of trace route is displayed in the Result field.
5. Select the interface in the Network Interface drop-down box to trace route on a specified interface. **Optional**



Execute a Diagnostics Script and Create a Diagnostics File

Note: This page is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

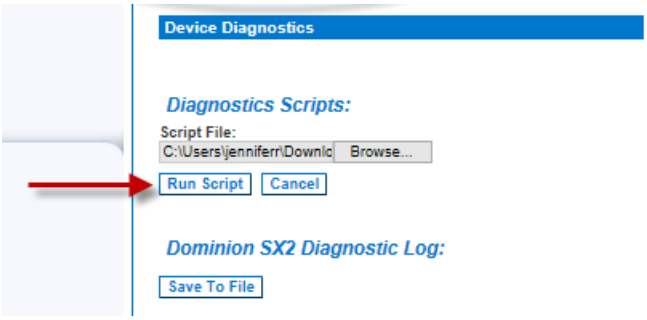
Use this feature to download diagnostic information from the SX II to the client machine.

Three operations can be performed on this page:

- Execute a special diagnostics script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the appliance and executed. Once this script has been executed, you can download the diagnostics messages using the Save to File function.
- Download the device diagnostic log for a snapshot of diagnostics messages from the SX II appliance to the client. This encrypted file is then sent to Raritan Technical Support. Only Raritan can interpret this file.
- Export the configuration database in a readable text file. No passwords are exported.

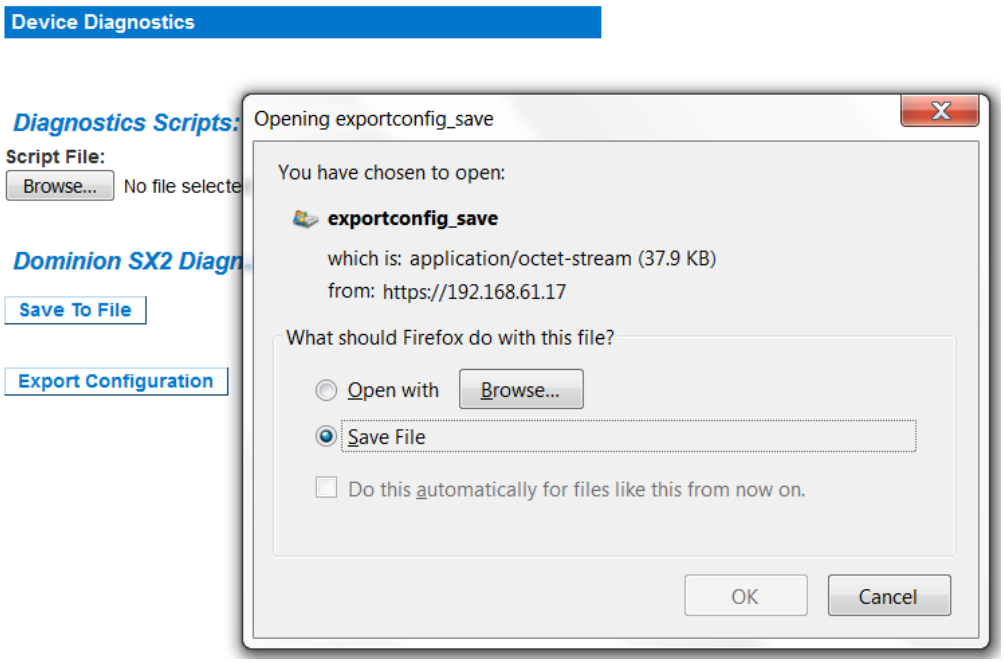
Note: This page is accessible only by users with administrative privileges.

1. Choose Diagnostics > SX II Diagnostics. The SX II Diagnostics page opens.
2. To execute a diagnostics script file emailed to you from Raritan Technical Support, retrieve the diagnostics file supplied by Raritan using the browse function.
3. Click Run Script. Send this file to Raritan Technical Support.



4. To create a diagnostics file to send to Raritan Technical Support, click Save to File and save the file locally from the Save As dialog.
5. Email this file as directed by Raritan Technical Support.

6. To export the configuration file, click Export Configuration, then save the file.



Network Interface Page

The SX II provides information about the status of your network interface.

To view information about your network interface:

- Choose Diagnostics > Network Interface. The Network Interface page opens.

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

To refresh this information:

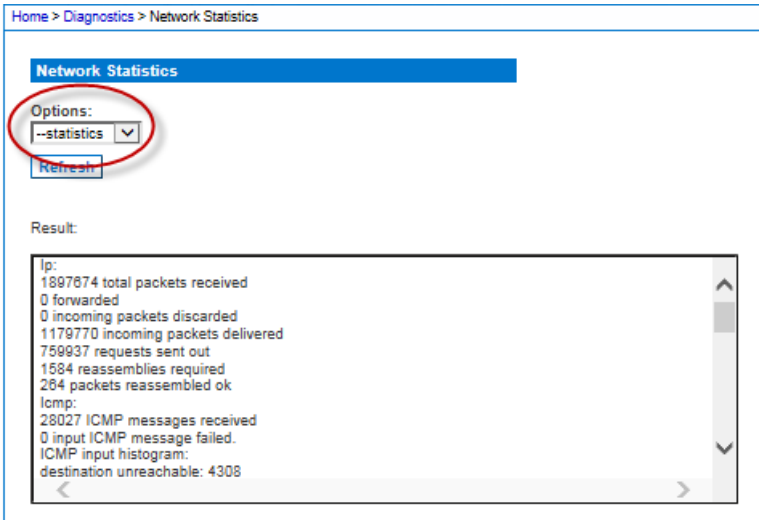
- Click Refresh.

Network Statistics Page

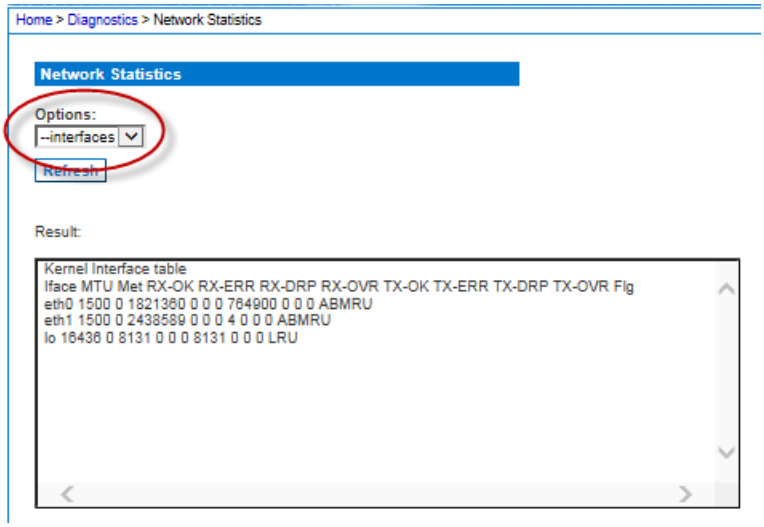
The SX II provides statistics about your network interface.

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list.
3. Click Refresh. The relevant information is displayed in the Result field. See examples.

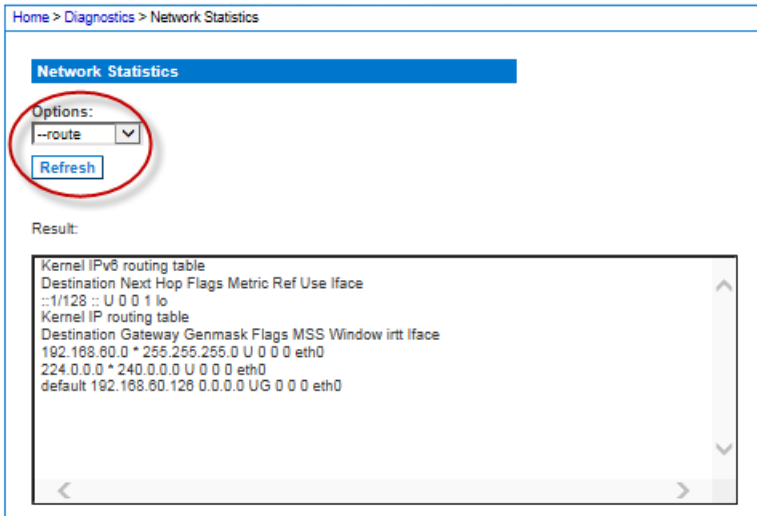
- Statistics



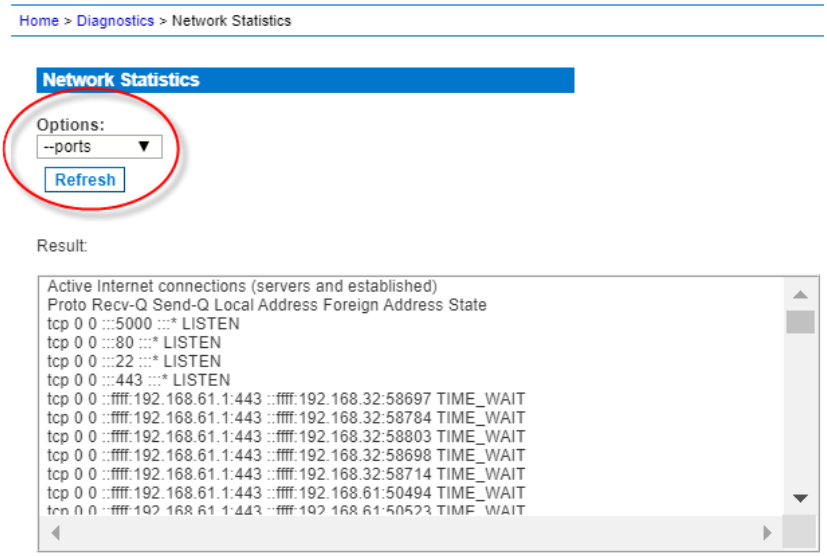
- Interfaces:



- Route:



- Ports:



Administering SX II Using command line interface

This section is specific to tasks performed using command line interface.

For information on performing tasks in the SX II Remote Console, see ***Administering SX II from the Remote Console and Admin-Only Interface*** (on page 68).

USB Local Admin Port

The USB local admin port is used to add the SX II as a com port on an external PC to allow this PC direct access to the SX II's CLI.

Requirements:

- USB to mini-USB cable to connect
- Serial communication program such as putty, tera term, or minicom

To use the USB local admin port:

1. Connect the mini-USB cable to the SX II and USB to the laptop. The laptop should attempt to install a serial driver.
   - If the driver does not install: In Windows, open the Device manager.Look for Gadget Serial v2.4 under "Other Devices". Click to select Gadget Serial v2.4, then click Update Driver Software. Search the Microsoft network for the driver, and it should install properly.
2. Note the COM port that is associated with this newly added USB serial device.
3. Launch a serial communication program and open up the COM port with bps 115200.
4. The SX II's CLI will appear for login and administration of the device.

Change Your Password Using CLI

Note: This feature can also be configured from the Remote Console. See **Change Your Password from the Remote Console** *(on page 28).*

Important: If the administrator password is forgotten, SX II must be reset to the factory default from the Reset button on the rear panel and the initial configuration tasks must be performed again.

Enter `admin > password` to access the menu.

When creating a password via CLI, it cannot begin with a space or end with a space. This does not apply to creating passwords in using the Remote Console.

Command	Description	Parameters
`password`	Create a new password, if needed.	▪ new password

Configure Power Strips Using CLI

Note: These functions can also be managed from the Remote Console. See **Configure Power Strips from the Remote Console** *(on page 68).*

The following power commands allow you to manage power strips attached to SX II.

Enter `admin > power` to access the menu.

Command	Description	Parameters
`associate`	Associate a power strip outlet to a SX II port.	▪ <port number> - SX port number to associate ▪ <powerstrip name> - Name of power strip to access ▪ <outlet number> - Outlet number on power strip to associate
`cycle`	Power cycle specified power strip. *Note: If you are connecting a PX to SX II, it is recommended you set the power cycle time to 5 seconds.*	▪ <port number> - SX port number to cycle ▪ <powerstrip name> - Name of power strip to access ▪ <outlet number> - Outlet number on power strip to cycle
`off`	Power off a specified power strip.	▪ <port number> - SX port number to turn off ▪ <powerstrip name> - Name of power strip to access ▪ <outlet number> - Outlet number on power strip to turn off
`on`	Power off a specified power strip.	▪ <port number> - SX port number to turn on ▪ <powerstrip name> - Name of power strip to access ▪ <outlet number> - Outlet number on power strip to turn on
`powerdelay`	Configure global power strip delays.	▪ <cycle value> - Delay between power off/on
`powerstatus`	Get the status of a specified power strip.	▪ <powerstrip name> - Name of power strip to access
`powerstrip`	Get power strip information.	▪ <powerstrip name> - Name of power strip to access
`setpowerport`	Configure an SX II Port to contain a power strip.	▪ <port number> - SX port number
`unassociate`	Remove a power outlet association from a SX II port.	▪ <port number> - SX port number to unassociate ▪ <powerstrip name> - Name of power strip to access ▪ <outlet number> - Outlet number on power strip to unassociate

Command	Description	Parameters
`unsetpowerport`	Configure an SX II Port to remove a power strip.	▪ <port number> - SX port number

Configure and Manage Users and User Groups Using CLI

Note: These functions can also be performed from the Remote Client. See **Configure and Manage Users and Groups from the Remote Console** *(on page 73).*

SX II stores an internal list of all user profiles and user groups.

User profiles and groups are used to determine access authorization and permissions. This information is stored internally. User passwords are stored in an encrypted format.

SX II allows the administrator to define groups with common permissions and attributes. They can then add users to the groups, and each user takes the attributes and permissions of that group.

Since the group permissions are applied to each individual in the group, permissions do not have to be applied to each user separately. This reduces the time to configure users.

For example, create a group called Modem Access that has permission to manage modems. Each user assigned to the Modem Access group can then manage the modem function; you do not have to assign each user a separate permission.

Enter `admin > Config > Users` to access the menu.

Command	Description	Parameters
`addgroup`	Creates a group with common permissions.	group <groupname> - Group name ▪ control <number | range | *> - Port(s) the user group has full control permissions to (users assigned to this group have read and write access to the listed ports). Control must be assigned to the group if power control access will also be granted. Applies to a single port or range of ports (1-n or 1,3,4 or * for all ports). ▪ power <number | range | *> - Port(s) the user group has full power control permission to. Permitted (true), denied (false). ▪ pcshare <true | false> PC-Share Access - Indicate whether users in the group are allowed to access a port that already has users connected to it if the port access mode is set to Share. Permitted (true), denied (false). ▪ settings <true | false> Permission to change device

Command	Description	Parameters
		settings. ▪ viewonly settings <number range *> <true or false><true | false> - User group has view only permissions to the port. Permitted (true), denied (false). ▪ cc <true | false> - Allow access under CC-SG management commands. Permitted (true), denied (false). ▪ diagnostics <true | false> - Permission to access diagnostics commands. Permitted (true), denied (false). ▪ maintenance <true | false> - Permission to access maintenance commands, backup and restore the database, firmware upgrade, factory reset, and reboot. Permitted (true), denied (false). ▪ security <true | false> - Permission to access security commands. SSL certificate, security settings, IP ACL. Permitted (true), denied (false). ▪ manage user <true | false> - Permission to access user management commands. User and group management, remote, authentication, login settings. Permitted (true), denied (false). **Important**: manage user allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions. ▪ modem <true | false> - Permission to access the modem. Displayed on the page when a built-in modem is connected to SX II. Select this option if you want the group to have access to the external modem. If broadband access is enabled for a modem, this permission allows the group to access SX II via the wireless modem, as well. Permitted (true), denied (false).
`editgroup`	Command to edit an existing user group.	▪ deny <number | range | *> - Deny permissions to listed ports. ▪ powerdeny <number | range | *> - Deny power permissions to listed ports. ▪ All commands listed under addgroup can be used to editgroup.
`showgroup`	Shows the details of existing user groups. If there is no group specified, the command displays all groups in the system.	▪ <group name> - Group to display.

Command	Description	Parameters
`deletegroup`	Deletes an existing user group.	▪ <group name> - Group to delete.
`adduser`	Add an individual user to SX II.	▪ user <loginname> - User's login name ▪ full name <user's fullname> - User's full name ▪ group <groupname > - The group the user us associated with ▪ password <password> - User's password. When creating a password via CLI, it cannot begin with a space or end with a space. This does not apply to creating passwords in using the Remote Console. ▪ active <true | false> - Activate (true) or deactivate (false) the user account ▪ <dialback> - User's dialback phone number
`addsshkey`	The `addsshkey` command adds SSH key data for the user. This data is the rsa_id.pub key generated for your client. The user must exist in SX II before you can add an SSH key for them. The key data should be used for authentication and users should not have to enter a password. Linux users should delete "name@local host" that appears at the end of the key when adding non-default public keys. This is not necessary if using the corresponding private key. The SSH key data is validated in several ways. Specified keytype is validated: [ssh-rsa|ssh-dsa|ecdsa-sha2-nistp256| ecdsa-sha2-nitsp384| ecsda-sha2-nitsp512]. Keytype is followed by whitespace, followed by the base64 data. Base64 data is validated. Whitespace and any characters after the base64 are dropped from the key data.	▪ user <loginname> - User's login name ▪ key <value> - User's SSH key

Command	Description	Parameters
viewsshkey	Displays the SSH key data for the specified user.	▪ user <loginname> - User's login name ▪ index <index> - View the index of the SSH key
deletesshkey	Delete the SSH key for a specified user.	▪ user <loginname> - User's login name ▪ index <index> - Delete the SSH key index
edituser	Update information for a specified user.	▪ See addgroup parameters.
deleteuser	Delete a specified user.	▪ user <loginname> - User to delete
showuser	Displays the details for an existing user.	▪ user <loginname> - User to display
insertgroupacl	Insert Group ACL Rule	▪ group: Affected group name ▪ id: id number ▪ start: Beginning IP address of range <ipaddress> ▪ stop: Ending IP address of range <ipaddress> ▪ policy: <ACCEPT/DROP>
replacegroupacl	Replace Group ACL Rule	▪ group: Affected group name ▪ id: id number ▪ start: Beginning IP address of range <ipaddress> ▪ stop: Ending IP address of range <ipaddress> ▪ policy: <ACCEPT/DROP>
deletegroupacl	Delete Group ACL Rule	▪ group: Affected group name ▪ id: id number or <all>
showgroupacl	Display Group ACL Rules	▪ group: Group name
addgroupacl	Add Group ACL Rule	▪ group: Group name ▪ start: Beginning IP address of range <ipaddress> ▪ stop: Ending IP address of range <ipaddress> ▪ policy: <ACCEPT/DROP>

Configure User Authorization and Authentication Services Using CLI

Note: These functions can also be performed from the Remote Console. See **Configure User Authentication from the Remote Console** *(on page 85).*

SX II requires users be authenticated to access the appliance.

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

Users can be authenticated via SX II locally or remotely.

By default, users are authenticated locally; you must enable remote authentication. When remote authentication is enabled, there is an option to allow or deny local authentication as a fallback. See Fallback to Local Authentication.

When the SX II is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

SX II provides several options to remotely authenticate users -

- LDAP/LDAPS
- RADIUS
- TACACS+

Enter `admin > Config > Authentication` to access the menu.

Authentication Method

Command	Description	Parameters
`authmode`	Set the authentication mode and fallback.	▪ mode <local|ldap|radius|tacacs> ▪ fallback <true | false> Enable or disable fallback to local authentication if remote is unreachable

LDAP Configuration

The LDAP configuration menu offers commands to set up LDAP and LDAPS.

Enter `admin > Config > Authentication > ldap` to access the menu.

Command	Description	Parameters
`ldap`	Configure secure LDAP authentication mode.	▪ primip <ipaddress | hostname> - Primary server IP address ▪ secip <ipaddress | hostname> - Secondary server IP address ▪ port <value> - LDAP port ▪ basedn <Base DN> - Admin user DN ▪ secret <value> - Admin user authentication secret ▪ search <value> - User search DN ▪ dialback <value> - Dialback search query ▪ domain <Active Directory Domain> - Active Directory domain ▪ server <generic | ads> - Server type, Active Directory or Generic
`ldaps`	Set/Get secure LDAP authentication mode.	▪ port <value> - Secure LDAP port ▪ enable <true | false> - Secure LDAP enable (true), disable (false) ▪ verify <true | false> - LDAPS certificate validation enable (true), disable (false)
`testldap`	Used to test LDAP settings.	▪ login <LDAP user> - LDAP login to test ▪ password <LDAP users password>

RADIUS Configuration

The RADIUS menu provides access to commands used to configure access to a RADIUS server.

Enter `admin > Config > Authentication > RADIUS` to access the menu

Command	Description	Parameters
`primaryradius`	Access to configure the primary RADIUS settings.	▪ ip <ipaddress | hostname> - IP Address ▪ secret <value> - RADIUS authentication secret ▪ authport <value> - RADIUS authentication port ▪ acctport <value> - RADIUS accounting port ▪ timeout <value> - RADIUS timeout (in seconds) ▪ retries <value> - RADIUS retries ▪ chap <true | false> - CHAP enable/disable (true/false)
`secondaryradi`	Access to configure the secondary	▪ ip <ipaddress | hostname> - IP Address

Command	Description	Parameters
us	RADIUS settings.	▪ secret <value> - RADIUS authentication secret ▪ authport <value> - RADIUS authentication port ▪ acctport <value> - RADIUS accounting port ▪ timeout <value> - RADIUS timeout (in seconds) ▪ retries <value> - RADIUS retries ▪ chap <true | false> - CHAP enable (true), disable (false)

TACACS+ Configuration

The TACACS+ menu offers commands used to configure access to a TACACS+.

Enter `admin > Config > Authentication > TACACS+` to access the menu.

Command	Description	Parameters
primarytacacs	Used to configure the primary TACACS+ settings.	▪ ip <ipaddress | hostname> - IP Address ▪ secret <value> - TACACS+ authentication secret ▪ port <value> - TACACS+ port ▪ timeout <value> - TACACS+ timeout (in seconds) ▪ retries <value> - TACACS+ retries
secondarytacacs	Used to configure the secondary TACACS+ settings.	▪ ip <ipaddress | hostname> - IP Address ▪ secret <value> - TACACS+ authentication secret ▪ port <value> - TACACS+ port ▪ timeout <value> - TACACS+ timeout (in seconds) ▪ retries <value> - TACACS+ retries

Configure a Modem Using CLI

Note: You can also configure modems from the Remote Console. See **Configure Date and Time Settings from the Remote Console** *(on page 116).*

Enter `admin > Config > Modem` to access the menu.

Command	Description	Parameters
dialback	Enable dialback and caller ID verification	▪ enable <true | false> - enable or disable dialback, enable (true), disable (false) ▪ callerid <true | false> - enable or disable caller id verification of dialback
dialin	Configure dialin settings.	▪ enable <true | false> - Enable or disable modem, enable (true), disable (false) ▪ mode <All/PPP_Only/Console_Only> Modem access mode ▪ serverip PPP <IPv4 address> - PPP server IP address ▪ clientip PPP <IPv4 address> - PPP client IP address ▪ callerid <true | false> - enable or disable caller id for dialin numbers
dialinadd	Add phone number to dialin.	▪ [number phonenumber] - add a phone number to the approved list of dialin numbers
dialindel	Delete phone number from dialin.	▪ [number phonenumber] - delete a phone number from the approved list of dialin numbers
dialout	Enable internal modem dialout feature.	▪ enable <true/false>
bmodem	Enable/Disable broadband modem.	▪ enable <true | false> - enable or disable broadband modem access, enable (true), disable (false)
bmodemfailover	Enable/Disable broadband modem failover ▪ The command is available if bmodem is enabled.	▪ enable <true | false> - enable or disable broadband modem failover, enable (true), disable (false)

Assign User Groups Modem Access Permissions

If needed, assign users to a group with Modem Access permissions.

Modem Access permission is assigned to a user group on the Group page, and the user is then assigned to the group on the User page.

For more information, see ***Configure and Manage Users and User Groups Using CLI*** (on page 199) or ***Configure and Manage Users and Groups from the Remote Console*** (on page 73).

Server Settings to Support Modems

Primary (or/and Secondary) RADIUS Server Settings should be configured correctly and enabled on SX II.

- On the Remote RADIUS Server, the user's configuration should contain the following line.

```
Filter-Id = "Raritan:G{<local user group>}:D{<number for dialback>}"
```

The LDAP server user's configuration should contain the dialback number in the attribute that is configured as the 'dialback search string' on SX II.

Dialback with remote LDAP user (OpenLdap v.2 & v.3)

- Dialback with remote TACACS+ user (TACACS++ v.4.0.3a)

Dial-in and Dialback should be enabled on SX II used for modem communication. Primary (or/and Secondary) TACACS+ Server Settings should be configured correctly and enabled on SX IIs.

On the Remote TACACS+Server user's configuration should own the following line .

```
user-dialback='129'
```

Run an Autoconfiguration Script Using CLI

Note: These functions can also be configured from the Remote Console. See **Enable Auto Script from the Remote Console for Use with TFTP or a USB Stick** *(on page 100).*

Enter `admin > config >` to access the menu.

Command	Description	Parameters
`autoconfig`	Set and get Automatic Script Configuration.	▪ enable <true/false> - enable (true), disable (false) ▪ run <once/every> - Run script once or at every boot ▪ source <manual/dhcp> - Use TFTP address provided by DHCP or manually set ▪ tftp address <ipaddress | hostname> - TFTP server address
`autoconfigusb`	Set/Get Automatic Script via USB Configuration.	▪ enable <true/false> - enable (true), disable (false)

Enter `admin >` to access the menu.

Command	Description	Parameters
`scriptget`	Retrieves the remote configuration script.	▪ address <ipaddress | hostname> - Address of FTP server ▪ port <FTP port> - Port of FTP server (1..65535) ▪ path <path to file> - FTP server path for config file. e.g. /ftphome/config.txt ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password. Will prompt if missing and user name given.
`scriptrun`	Runs the autoconfiguration script.	NA

Configure Network Settings Using CLI

Note: This feature can also be managed from the SX II Remote Console. See Configure SX II Network Settings from the Remote Console.

The `network` menu commands allow you to configure SX II network settings.

Enter `admin > config > network` to access the menu.

Command	Description	Parameters
`802.1x with commands`	Enable and configure 802.1x security	▪ enable8021x <true/false> ▪ auth: 802.1x authentication type: <eap_peap/eap_tls/eap_ttls> ▪ tlsServerCert: CA certificate settings for 802.1x server certificate
`dns`	Get and configure the DNS parameters for the network.	▪ mode <auto/manual> - DNS server IP mode ▪ primary <ipaddress> - Primary DNS server IP address ▪ secondary <ipaddress> - Secondary DNS server IP address
eth	Get/set ethernet parameters	▪ if <lan1/lan1> Interface ▪ mtu <576 - 65536> - Maximum Transmission Unit
`ethernetfailover`	Used to enable and disable the ability to failover from one LAN to another.	▪ enable <true/false> - Ethernet failover enable (true), disable (false)

Command	Description	Parameters
`interface`	Configure network settings for dual-LAN failover. By default, dual LAN failover mode is disabled.	▪ ipauto <none | dhcp> - Enable DHCP as ip configuration ▪ <lan1 | lan2> - Select LAN interface you are configuring. ▪ ip <IPv4 address> - IP Address of SX II assigned for access from the IP network ▪ mask <subnetmask> - Subnet Mask obtained from the IP administrator ▪ gw ipaddress <IPv4 address> - Gateway IP Address obtained from the IP administrator ▪ mode <auto | 10hdx | 10fdx | 100hdx | 100fdx | 1000fdx> - Set Ethernet Mode to auto detect or force a specified mode.
`ipforwarding`	IP forwarding configuration.	▪ enable <true/false>
`IPv6_interface`	Set IPv6 network parameters and retrieve existing IPv6 parameters.	▪ ipauto <none | routerdisc> - Enable IPV6 auto configuration ▪ if <lan1 | lan2> - Select LAN interface you are configuring. ▪ ip ipaddress <ipaddress> - IPv6 address of SX II assigned for access from the IP network. ▪ prefixlen <prefix length> - IPV6 Address prefix length (is the number of bits in the prefix, in range of 0-128 (decimal)) ▪ gw ipaddress <IPv6 address> - Gateway IP Address obtained from the IP administrator. ▪ mode <enable or disable> - IPV6 network operational mode, enable (true), disable (false) ▪ ipforwarding: Enable <true/false>
`name`	Name the appliance.	▪ devicename <value> - name assigned to SX II ▪ hostname <value> - Preferred host name (DHCP only)
`staticroute`	Configure static routes.	▪ enable <enable> - enable (true), disable (false)
`staticrouteadd`	Add a static route.	▪ dest <dest> - Destination ▪ if <lan1 | lan2> - Interface (lan1/lan2) ▪ prefix <prefix> - IPv6 prefix length ▪ mask <mask> - IPv4 mask ▪ gateway <gateway> - Gateway ▪ mtu <mtu> - MTU (64..65536) ▪ flags <host|net> - Flags (host/net)
`staticrouteshow`	Show a list of static routes.	NA

Command	Description	Parameters
`staticroutedelete`	Used to remove a route from the kernel routing table.	▪ id <id> - id number or all

Configure 802.1X Security Settings Using CLI

Note: This feature can also be managed from the SX II Remote Console. See **802.1X Security** *(on page 113).*

The `network>802.1X` sub-menu commands allow you to configure SX II 802.1X security settings.

Enter `admin > config > network > 802.1X` to access the menu.

Command	Description	Parameters
enable8021X	Enable or disable 802.1x security	▪ Interface: <lan1/lan2> ▪ Enable: Enable feature <true/false>
auth	802.1x authentication type	▪ Interface: <lan1/lan2> ▪ type: Authentication type <eap_peap/eap_tls/eap_ttls>
eap_peap	EAP-PEAP configuration	▪ Interface <lan1 /lan2> ▪ user <username for EAP-PEAP> ▪ password <password for EAP-PEAP>
eap_tls	Display EAP-TLS settings. Configuration cannot be done with CLI.	▪ Interface <lan1/lan2> ▪ Use Key Password: <true/false> ▪ Key Password: <password for EAP-TLS>
eap_ttls	EAP-TTLS configuration	▪ Interface <lan1/lan2> ▪ Inner Authentication: <MSCHAPv2/CHAP/PAP> ▪ Username: <username for EAP-TTLS> ▪ Password: <password for EAP-TTLS>
tlsServerCert	802.1x CA Certificate settings	▪ Interface: <lan1/lan2> ▪ CA Certificate Validation: Enable or disable CA certificate validation. <true/false> . ▪ Disable Certificate Date Check: Allow expired or not yet valid certificates. <true/false>

Configure Device Settings Using CLI

Note: These functions can also be configured from the Remote Console. See **Configure Device Settings from the Remote Console** *(on page 104).*

These commands provide the ability to configure SX II server services.

Enter `admin > config > services` to access the menu.

Command	Description	Parameters
`discovery`	Configure the discovery port.	▪ port <value> - Discovery TCP listen port ▪ encryption <true/false - Discovery port encrypted
`http`	Used to control http access and define the port.	▪ port <value> - HTTP server default listen port (tcp)
`https`	Used to control https access and define the port.	▪ port <value> - HTTPS server default listen port (tcp)
`ssh`	Enable or disable SSH access and configure settings.	▪ enable <true | false> - Enable or disable SSH access, enable (true), disable (false) ▪ port <value> - SSH server tcp listen port ▪ dsa <true/false> - Use Legacy DSA ▪ authmethod <pass/cert/passcert> - Password, Certificate, or both
`telnet`	Enable or disable Telnet access. Due to the lack of security, the username, password and all traffic is in clear-text on the wire. Telnet must be enabled before it can be used; it is disabled by default. By default, the telnet port is set to 23 but can be changed by issuing the following command.	▪ enable <true | false> - Enable or disable Telnet access, enable (true), disable (false) ▪ port <value> - Telnet server tcp listen port

Configure Direct Port Access Using CLI

The permitted TCP Port Range is 1024-64510. When run without the mode parameter, the system displays the current dpa type.

Enter `admin > Config > Services >` to access this menu.

Command	Description	Parameters
`dpa`	Enable direct port access	▪ enable <true | false> - DPA access, enable (true), disable (false) ▪ url <true | false> - DPA via URL, enable (true), disable (false) ▪ loginstring <true | false> - Allow specifying DPA port in username when logging in, enable (true), disable (false) ▪ validate: <true|false> Enable Stand-alone RSC Download Server Certificate Validation
`dpaport`	Configure the IP/SSH/telnet DPA ports for specified serial ports.	▪ port <number | range | *> - Port(s) to view/modify (Single port or range of ports (1-n or 1,3,4 or * for all ports)) ▪ dpaip <ipaddress> - IP Address assigned for direct port access. 0.0.0.0 clears the setting. ▪ telnet <port number> - TCP Port assigned for direct port access via Telnet. 0 clears the setting. ▪ ssh <port number> - TCP Port assigned for direct port access via SSH. 0 clears the setting.

Anonymous Connections

You can establish an anonymous Direct Port Access connection via Telnet by typing `anonymous`, or pressing Enter at the username prompt. The anonymous connection is established without prompting for a password.

When establishing a Direct Port Access connection via SSH, entering the username `anonymous` is required. The anonymous connection is established without prompting for a password.

Use the suppress parameter to configure the following messages to display or not display the first time SX II is accessed via anonymous Direct Port Access -

```
Escape Sequence is : <escape string> <true\false>
```

"You have read-only access to this port." OR "You are now master for the port."

If suppress is true, the above messages are not displayed and connected directly to the target prompt.

If suppress is false, the above messages are displayed.

Configure SNMP Traps and Alerts Using CLI

Note: SNMP traps can also be configured from the Remote Console. See Configure SNMP Notifications from the Remote Console.

SX II supports sending SNMP alerts to a predefined SNMP server. The Raritan SNMP MIB can be found in ***Viewing the SX II MIB*** (on page 121).

Enter `admin > config > snmp` to access the menu.

Command	Description	Parameters
`add`	Add SNMPv2c trap or inform. A recipient is an IP address with an optional space- separated port number. Traps may be sent to multiple ports with the same IP address. WARNING: NON-RESPONDING DESTINATIONS MAY SIGNIFICANTLY SLOW SYSTEM RESPONSE IF INFORMS ARE CONFIGURED WITH LARGE VALUES FOR RETRIES AND/OR TIMEOUTS.	▪ dest <ipaddress | hostname> - Destination IP/hostname ▪ port <port number> - Destination port ▪ community <community> - SNMP community ▪ type: SNMP Notification Type (Trap/Inform) ▪ retries: (Number of Inform retries before quiting) <0-10> ▪ timeout: Number of seconds to wait for an Inform response <1-20>
`addv3`	Add SNMP V3 Trap or Inform. WARNING: NON-RESPONDING DESTINATIONS MAY SIGNIFICANTLY SLOW SYSTEM RESPONSE IF INFORMS ARE CONFIGURED WITH LARGE VALUES FOR RETRIES AND/OR TIMEOUTS A recipient is an IP address with an optional space- separated port number. Traps may be sent to multiple ports with the same IP address.	▪ dest <ipaddress | hostname>- Destination IP/hostname ▪ port <port number> - Destination port ▪ name <name> - Security name ▪ authproto <MD5 | SHA> - SNMP auth protocol ▪ authpass <authpass> - SNMP auth passphrase ▪ privproto <None | DES | AES> - SNMP privacy protocol ▪ privpass <privacy password> - SNMP privacy passphrase ▪ type: SNMP Notification Type (Trap/Inform) ▪ retries: (Number of Inform retries before quiting) <0-10> ▪ timeout: Number of seconds to wait for an Inform response <1-20>
`viewtraps`	Display existing SNMP traps.	NA
`del`	Delete SNMP traps.	▪ dest <ipaddress | hostname>- Destination IP/hostname ▪ port <port number> - Destination port

Command	Description	Parameters
`delv3`	Delete SNMPv3 traps.	▪ dest <ipaddress | hostname>- Destination IP/hostname ▪ port <port number> - Destination port
`snmpagent`	Configure SNMP daemon.	▪ enable <true|false> - SNMP Daemon, enable (true), disable (false) ▪ contact Contact Sunbird Professional Services and Support via the Support site at http://support.sunbirddcim.com or via email (tech@sunbirddcim.com) - SNMP contact ▪ location <location> - SNMP location ▪ community <community> - SNMP community ▪ type <read_only | read_write> - SNMP community type ▪ v2cenable <true | false> - SNMP v1/2 agent, enable (true), disable (false)
`snmptrap`	Enable or disable an SNMP trap.	▪ enable <true | false> - SNMP traps, enable (true), disable (false) ▪ v2cenable <true | false> - SNMP v1/v2c traps, enable (true), disable (false) ▪ v3enable <true | false> - SNMP v3 traps, enable (true), disable (false)
`snmpv3agent`	Configure an SNMPv3 agent.	▪ enable <true|false> - SNMP V3 Agent, enable (true), disable (false) ▪ name <security name> - Security name ▪ authproto <MD5 | SHA> - SNMP auth protocol ▪ authpass <auth password> - SNMP auth passphrase ▪ privproto <None | DES | AES> - SNMP privacy protocol ▪ privpass <privacy password> - SNMP privacy passphrase ▪ useauthforpriv <true | false> - Use auth passphrase for privacy, enable (true), disable (false)

Configure Date and Time Settings Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Date and Time Settings from the Remote Console** *(on page 116)*

Enter `admin > config > time` to access the menu.

Command	Description	Parameters
`clock`	It is important to set the date and time correctly to ensure that log entries and events contain the correct timestamp. Use this to set the time and date on the server.	▪ tz timezone - Timezone index is a number corresponding to the desired time zone. ▪ dst <true | false> - Apply DST settings, enable (true), disable (false) ▪ time - Time String <HH:MM:SS> ▪ date - Date String <YYYY-MM-DD>
`timezonelist`	Used to find the number code that corresponds to your time zone.	NA
`ntp`	Use this command if you are synchronizing SX II with an NTP server.	▪ enable <true | false> - enable or disable the use of NTP, enable (true), disable (false) ▪ primip <primaryIP> - Primary NTP server to use first. ▪ secip <secondaryip> - Secondary NTP server if the first is not available. ▪ override <true/false> - Override DHCP settings for NTP server (true/false)

Change the Default GUI Language Setting Using CLI

Note: This setting can also be configured from the Remote Console. See **Changing the Default GUI Language Setting from the Remote Console** *(on page 139).*

Enter `admin > config > language` to access the menu.

Command	Description	Parameters
`language`	Language settings only apply to the Remote Console web interface; they do not apply to the Local Console interface. The SX II GUI defaults to English, but also supports the following localized languages: • English (default) • Japanese • Simplified Chinese	▪ `set` <en | ja | zhs | zht> - GUI language code

Command	Description	Parameters
	▪ Traditional Chinese	

Configure SMTP Events and Notifications Using CLI

Note: This setting can also be configured from the Remote Console. See **Enable Email (SMTP) Notifications from the Remote Console** *(on page 124).*

Use the `log > smtp` menu to access to the options that can be used to configure the SMTP server and destination email addresses.

Enter `admin config > log > smtp` to access the menu.

Command	Description	Parameters
smtp	Configure the SMTP server.	▪ enable <true|false> - SMTP server, enable (true), disable (false) ▪ ip <ipaddress | hostname> - SMTP server IP address ▪ port <port number> - SMTP server port (1..65535) ▪ auth <true | false> - SMTP auth required, enable (true), disable (false) ▪ user <username> - SMTP user account ▪ pass <password> - SMTP user password ▪ source <source> - SMTP source address
`addemailsub`	Add a mail subscriber. Up to ten subscribers can be added.	▪ email <email> - Email address to add
`delemailsub`	Delete an email subscriber.	▪ email <email> - Email address to delete
`testsmtp`	Test email notification settings.	▪ dest <destination email> - Destination email address
`viewemailsub`	View a list of email subscribers.	NA

Configure Port Logging Settings Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Port Logging Settings from the Remote Console** *(on page 139).*

As part of its security capabilities, SX II logs data and to provide alerts based on activities between the users, SX II, and the target device.

Audit trail that allows authorities to review what has happened in the system, determine who implemented what action and when is captured as part of this function.

Event logging and SNMP traps are also available. Events can be logged locally using Syslog. Local events are maintained in a 512K per port buffer and can be stored, reviewed, cleared, or sent periodically to an FTP server.

Configuration log commands allow you to manage the logging features of the SX II server.

Enter `admin > config > Log` to access the menu.

Command	Description	Parameters
`eventlogfile`	Use this command to control and configure the logging of events to the local log.	▪ size <value> - Maximum size of local log file (in bytes). If the event log file size exceeds the available flash memory on your SX II model, the event is not saved. To avoid this, set the file size to greater than 1024 but less than 10000000. *Note: SX II model's flash memory varies.* ▪ style <wrap or flat. - Specifies what action to take when the maximum size is reached: wrap will cause the log to circle around when end is reached. flat will cause logging to stop when the end is reached.
`eventdest`	Event configuration.	▪ event <index of event> - Event Index, use 'eventlist' to see index and current configurations ▪ audit <true | false> - Audit Logging, enable (true), disable (false) ▪ snmp <true | false> - SNMP Logging, enable (true), disable (false) ▪ syslog <true | false> - Syslog Logging, enable (true), disable (false) ▪ smtp <true | false> - SMTP Logging, enable (true), disable (false)
`eventlist`	Display an indexed list of all configurable events.	NA

Command	Description	Parameters
`syslog`	Displays the list of configured syslog servers. Configure the syslog servers. Up to 8 servers can be added. Each syslog server is added and identified by a number: ip1, ip2, ip3, and so on. Configure the UDP port on the syslog server to which the syslog messages are sent. Default is 514.	▪ enable <true | false> - System event log logging, enable (true), disable (false) ▪ ip1 <ip address | hostname | delete> - syslog server address. port1 <port1number> - UDP port number for ip1. ▪ ip2 <ip address | hostname | delete> - syslog server address. port2 <port1number> - UDP port number for ip2. ▪ ip3 <ip address | hostname | delete> - syslog server address. port3 <port1number> - UDP port number for ip3. ▪ ip4 <ip address | hostname | delete> - syslog server address. port4 <port1number> - UDP port number for ip4. ▪ ip5 <ip address | hostname | delete> - syslog server address. port5 <port1number> - UDP port number for ip5. ▪ ip6 <ip address | hostname | delete> - syslog server address. port6 <port1number> - UDP port number for ip6. ▪ ip7 <ip address | hostname | delete> - syslog server address. port7 <port1number> - UDP port number for ip7. ▪ ip8 <ip address | hostname | delete> - syslog server address. port8 <port1number> - UDP port number for ip8.
`portsyslog`	Configure portsyslog server.	▪ enable <true | false> - Port logging data to a remote NFS server and also to the Syslog server, enable (true), disable (false) ▪ primaryip <primaryip> - Primary Portlog Syslog server address ▪ secondaryip <secondip> - Secondary Portlog Syslog server address ▪ category - Syslog Category local <0 - 7>

Command	Description	Parameters
`nfsportlog`	Configure the logging of port data.	▪ enable <true|false> - Logging of port data to remote NFS server, enable (true), disable (false) ▪ primaryip <primaryip> - Primary Portlog Syslog Server ▪ secondaryip <secondip> - Secondary Portlog Syslog Server ▪ primarydir <mountpath. - Primary NFS Server's mount directory. Eg., /nfslog ▪ secondarydir <mountpath> - Secondary NFS Server's mount directory. Eg., /nfslog ▪ prefix <name> - Prefix for log file name. Use " " for a blank prefix ▪ size <value> - Maximum Size (in bytes) for the log file ▪ inputlogging <true|false> - Enable/Disable logging of user input data on the port. This refers to input via keystroke from the user. ▪ indir <name> - Directory name for storing input log ▪ outdir <name> - Directory name for storing output log. Output implies data sent from target to the SX port.
`nfsencrypt`	Set the encryption key to be used for encrypting port log.	▪ enable <true|false> - SMTP Server, enable (true), disable (false) ▪ key <string> - Provide RC4 key string to be used for encryption
`portlogtime`	Use to configure the Port Log Time. Changes to the timestamp interval will go into effect after the current interval has passed and that port status timestamp has been logged."	▪ timestamp - Time interval (in seconds) between two timestamps in the log file. A value of 0 will disable timestamp logging. The default value is 20. The max value is 99999. ▪ update <update> - Update frequency (in seconds) between two updates to the remote log file. Default interval value is 30. Update Frequency range is 1 and 65535.

Enter `admin > config > log > local` to access the menu.

Command	Description	Parameters
`serialportlog`	Configure serial port log file.	▪ size <value> - Maximum File Size (bytes) ▪ enable <true|false> - Serial Port Log File, enable (true), disable (false) ▪ input <true|false> - Enable logging of all input keystrokes to file.
`serialportlogdel`	Delete serial port log file.	▪ port <number> - Ports to delete log of

Command	Description	Parameters
`serialportlogview`	View serial port log file.	▪ port Ports to view log. (Single port or range of ports (1-n or 1,3,4 or * for all ports)) ▪ type Log type <input/output> ▪ start Position in log file to start viewing <Number> ▪ length: Length of port data to read <number>
`serialportlogftp`	▪	▪ port: Port number to retrieve log <Number> ▪ type: Log type <input/output> ▪ address: FTP server address <ipaddress> ▪ ftpport: FTP server port (default 21), TCP/UDP Port, <1..65535> ▪ path: FTP server path for serial log file <String>. ▪ file: Optional destination file name. Default: portlog_[portnum] ▪ user: Optional FTP user name. <String> ▪ password Optional FTP password. Will prompt if missing and user name given. <String>

Decrypt Encrypted Log on Linux-based NFS Server

To decrypt nfs encryption on Linux® platform, follow these steps:

1. Retrieve the current nfs encryption key

```
admin > Config > Log > nfsencrypt
```

2. Cut and paste the key printed after the Key: in the command response into a file.
3. Retrieve decryption application and either place it on the Linux machine or compile its source.
4. Save the encryption key file (dsx-encrypt.key) in the same directory where the decryption application is stored.
5. Copy the encrypted portlog file to the same directory.
6. Decrypt the file using the command:

```
./decrypt -f <portlogfile> -e <keyfilename> -o  <outputfile>
```

7. The decrypted file should be saved in `<outputfile>`.

Configure Ports Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Ports from the Remote Console** *(on page 143).*

Enter `admin >` to access the menu.

Command	Description	Parameters
`listports`	List accessible ports	NA

Enter `admin > config > port` to access the menu.

Command	Description	Parameters
`keywordlist`	Display all configured keywords.	NA
keywordadd	Add a keyword to the port.	▪ port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) ▪ keyword <value> - When keyword is detected on target, notification is sent.
`keyworddelete`	Delete an existing keyword from the port.	▪ port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) ▪ keyword <value> - When keyword is detected on target, notification is sent.
`config`		▪ port <number | range | *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) ▪ name <port name> - Port name ▪ bps <1200 | 1800 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 | 230400> - Port speed in bits-per-second ▪ parity <none|even|odd> - Port parity type ▪ flowcontrol <none|hw|sw> - Port flowcontrol type hw = hardware flow control sw =X on/X off) ▪ eqtype <auto|dte|dce> - Equipment type (auto=>AUTO Detection, dte=>Force DTE, dce=>Force DCE) Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. SX II does not support autodetection of both DCE and DTE on the same port. ▪ escapemode <none|control> - Use Ctrl-key (escapemode=control) or single key (escapemode=none) as escape sequence; for

Command	Description	Parameters
		example, Ctrl- => escapemode=control ▪ escapechar= escapechar char-Escape character Raritan recommends that you do not use or Ctrl- as the Escape command. Either of these may cause unintended commands, such as opening a menu, instead of invoking the Escape Command. ▪ emulation <vt100 | vt220 | vt320 | ansi> - Target Emulation type ▪ sendbreak <duration> - Duration of the sendbreak signal in milliseconds. ▪ exitstring <cmd #delay; > - Execute exit string when port session closes, for example, config port 1 exitstring logout (execute logout on exit) config port 1 exitstring #0 (disable exit string for the port). The delay is the amount of time to wait after writing the command to the target. Number in seconds up to 60. ▪ dpaip <ipaddress> - IP Address assigned for direct port access ▪ ssh <tcp port> - TCP Port assigned for direct port access via ssh ▪ alwaysactive <true | false> - Determine whether data coming into a port is logged, for example, config port 1 alwaysactive true (always log activities coming into a port even if no user is connected) config port 1 alwaysactive false (ignore data coming into a port when no user is connected) ▪ encoding - Target Encoding type (DEFAULT|US-ASCII|ISO-8859-1|ISO-8859-15|UTF-8|Shift-JIS|EUC-JP|EUC-CN|EUC-KR) ▪ chardelay delay - Delay inserted between writing characters (0-9999ms) ▪ linedelay delay - Delay inserted between writing lines (0-9999ms) ▪ stopbits - Number of bits used to signal the end of a character (usually 1) (1/2) ▪ telnet - TCP Port assigned for direct port access via Telnet. 0 clears the setting. (TCP/UDP Port) (0..65535) ▪ ssh - TCP Port assigned for direct port access via SSH. 0 clears the setting. (TCP/UDP Port)

Command	Description	Parameters
		(0..65535) ▪ multiwrite <true/false> - Port set in multiple writer mode ▪ suppress <true/false> - Suppress SX messages when connecting to this target(true/false) ▪ portdetect <true/false> - Enable port up/down detection.

DPA Mode Port Config Command Example

The following example configures Direct Port Access. The following port command sets an IP address for DPA access to the port which is not the same as DPA by URL. The DPA IP address is just an address that goes directly to the port.

```
admin > Config > Port > config port 1 dpaip 10.0.13.1
admin > Config > Services > dpa enable true
```

- `dpa enable true` - enables IP and port DPA methods for configured ports

After entering the password, you have direct access to port 1, using the newly assigned IP specifically for port 1.

```
admin@10.0.13.1's password:
 Escape Sequence is: Control-
You are now master for the port.
```

The following example configures DPA port settings for DPAIP for range of ports.

```
admin > Config > Port > config port 1-32 dpaip 10.0.13.200
```

or

```
admin > Config > Port > config port * dpaip 10.0.13.200
```

In both cases above, port 1 will have an IP assigned as 10.0.13.200, while port 2 will have 10.0.13.201, port 3 10.0.13.203, and so on.

The following example configures DPA port settings for SSH and Telnet by TCP port.

```
admin > Config > Port > config port 1 ssh 7000 telnet 8000
```

DPA Telnet and SSH port changes are available immediately without rebooting.

```
ssh -l sx_user -p 7000 10.0.13.13 or telnet -l sx_user 10.0.13.13
8000
admin@10.0.13.13's password:
Escape Sequence is: Control-

You are now master for the port.
```

After entering the password, you have direct access to port 1, using the newly assigned TCP Ports(either ssh or telnet), specifically for port 1.

The following example configures DPA port settings for a group of ports (make sure no TCP Ports have been assigned, and a free range of TCP Ports are available for dpa TCP Port mode usage).

```
admin > Config > Port > config port 1-32 ssh 7000 telnet 8000
```

or

```
admin > Config > Port > config port * ssh 7000 telnet 8000
```

In both cases above, port 1 will have ssh port 7000 and telnet port 8000 assigned for direct port access, port 2 will have ssh port 7001 and telnet port 8001, and so on.

To configure all ports using a block of contiguous port numbers, use the <port *> command. If port_range is specified, a block of contiguous port numbers are used. The given value of base_tcpport is used as starting value. For individual port configuration, the <port number> command can be used.

Configure the Local Port Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Local Port Settings from the Remote Console** *(on page 137).*

Enter `admin > config > localport` to access the menu.

Command	Description	Parameters
`config`	Configure local ports.	▪ enable <true/false> - Standard Local Port, enable (true), disable (false) ▪ auth <common|none> - Local User Authentication: common-(Local/LDAP/RADIUS/TACACS+); none-(No authentication) (common/none) ▪ ignorecc <true/false> - Ignore CC managed mode on local port, enable (true), disable (false) ▪ kbd - Keyboard Type ▪ config baud <9600|19200|38400|57600|115200>

Configure Security Settings Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Security Settings from the Remote Console** *(on page 153).*

There are various settings configured from the `security` menu.

Enter `admin > Security` to access the menu.

Command	Description	Parameters
`banner`	SX II optionally supports a customizable welcome banner that is displayed after login. Up to 6000 characters can be entered. When you log in to SX II via a GUI, a banner with a fixed width typeface and a common dimension, such as 80x25, appears. If the banner is very large, that is, over 9000 lines, the banner displayed on the GUI does not increase the overall page size because it is contained within a scrollable text area. The banner identifies the location to which the user has logged in. You can also add a consent banner that forces the user to accept stated conditions prior to advancing into operation of the console server. The `banner` command controls the display of a security banner immediately after login.	▪ enable <true | false> - Banner display, enable (true), disable (false) ▪ audit <true | false> - Audit for the banner, enable (true), disable (false) ▪ title <value> - Title of the security banner
`bannerget`	Directs SX II to go to this site to retrieve the welcome banner. The welcome banner and the audit statement can be configured using the above command maintained on an external FTP site.	▪ address <ipaddress | hostname> - FTP Server Address ▪ port <FTP port> - FTP Server Port (default 21) ▪ path <path to file> - Path to Banner file to retrieve ▪ user <FTP username> - FTP Username ▪ password <FTP password> - FTP Password (prompted if missing)
`pcshare`	Simultaneous access to the same target by multiple users.	mode <shared/private> - Set PC-Share mode to shared or private (shared/private)

Command	Description	Parameters
`resetmode`	Configure Local Factory Reset Mode	▪ mode full <full|password|disabled> - full factory reset | password - only admin password reset | disabled - disable factory reset (full/password/disabled)
`encryption`	Sets the encryption type and FIPS mode of SX II.	▪ mode <auto | aes128 | aes256 | custom> - Set the encryption mode of the device ▪ fips <true | false> - Enable/disable FIPS 140-2 mode, enable (true), disable (false). This option requires a reboot of the device to take effect. ▪ https <true/false> - Force HTTPS for web access. ▪ customciphers <string> - Custom ciphers for HTTPs.
`hostallowlist`	Helps prevent host header attacks by limiting what a web client can send in the HOST header of an HTTP request.	▪ enable <true/false> - Enable/Disable the Host Allowlist feature.
`addhostallow`	Add a Hostname/IP to the Host Allowlist.	▪ host <Hostname/IP> - to add to the allowlist
`delhostallow`	Delete a Hostname/IP from the Host Allowlist.	▪ host <Hostname/IP> to delete from the allowlist.
`clientcertauth`	Client certificate settings.	▪ clientcert: Client certificate global settings. ▪ clientcertauth: Client certificate authentication map settings. ▪ clientcertcrl: Client certificate CRL settings. ▪ clientcertocsp: Client certificate OCSP settings.

Enter `admin > Security > firewall` to access the menu and menu options.

Command	Description	Parameters and examples
`firewall`	Enable the firewall. Rules are deleted upon disable.	enable <true | false> - Enable/Disable firewall
`viewtables`	View current iptables/ip6tables. Some rules exist by default and cannot be deleted.	NA

Command	Description	Parameters and examples

`iptables`	Administration tool for IPv4 packet filtering and NAT. SX II supports most modules.
	Firewall must be enabled.
		Example - to block icmp packets
		`iptables -A INPUT -p icmp -j DROP`
		`iptables -A OUTPUT -p icmp -j DROP`

`ip6tables`	Administration tool for IPv6 packet filtering and NAT.
	Firewall must be enabled.
		Example -
		`A INPUT -p icmpv6 --icmpv6-type 128 -j DROP`
		`ip6tables -A OUTPUT -p icmpv6 --icmpv6-type 128 -j DROP`

`iptables-save`	Save IP Tables (v4 and v6) to make firewall rules persistent.	NA

Enter `admin > Security > loginsettings` to access the menu and menu options.

Command	Description	Parameters
`idletimeout`	Specify the amount of idle time allowed before the system disconnects the user.	enable <true | false> - Enable/Disable password aging time - Idle Timeout Period in Minutes
`passwordaging`	Control when a password expires.	enable <true | false> days <value> - Number of days in Password Aging Interval
`singleloginperuser`	Restrict to a single login session per user.	enable <true/false> - Enable/Disable system wide single login session per user
`Strongpassword`	Configure strong password rules. When creating a password via CLI, it cannot begin with a space or end with a space. This does not apply to creating passwords in using the Remote Console.	enable <true|false> - Enable/Disable strong password rules for local users minlength <value> - Minimum password length maxlength <value> - Maximum password length history <value> - Number of passwords to store in password history uppercase <true|false> - true => force uppercase characters in password lowercase <true|false> - true => force lowercase characters in password numeric <true|false> - true => force numeric characters in password

Command	Description	Parameters
		other <true|false> - true => force special characters in password
`Unauthorizedportaccess`	Enable/Disable unauthorized access to a set of ports assigned to 'Anonymous' group.	enable <true/false> - Enable/Disable anonymous access to a set of ports assigned to the 'Anonymous' group
`userblocking`	Configure user lockout parameters.	mode - <disabled/timer_lockout/deactivate_userid> Set User Blocking mode (disabled/timer_lockout/deactivate_userid) timerattempts <timerattempts> - Timer Lockout Attempts lockouttime <lockouttime> - Timer Lockout Time deactivateattempts <value> - Deactivate UserID Attempts

Enter `admin > security > certificate` to access the menu and menu options.

SSL Security certificates are used in browser access to ensure that you are connecting to an authorized appliance.

Note: If SX II is not used to generate the certificate signing request and an external certificate is used instead, encryption needs to be removed from the private key before installing it on SX II. If this is the case, to remove the encryption from the key, a command such as openssl rsa -in server.key -out server2.key and server2.key should be used. Encrypted private keys are used to prevent the web server from being started by unauthorized users. Since SX II does not allow users to access the web server directly, encrypted private keys are not required and does not compromise security.

Note: When SX II is used to generate the certificate signing request, the private key is not required since SX II keeps the private key exclusive.

Command	Description	Parameters
`generatecsr`	Generate certificate signing request.	bits <1024 | 2048 | 4096> - Bit Strength of Certificate Key name <name> - Common Name (CN) country <code> - 2 Character ISO Country Code (C) state <state> - State/Province (ST) locality <locality> - Locality/City (L) org <organization> - Organization (O) unit <unit> - Organizational Unit (OU) email <email> - Email challenge <challenge> - Challenge Password selfsign <true | false> - Create a Self Signed Certificate (true/false) days <days> - Days certificate will be valid
`getcert`	Get the certificate from a specific location.	address <ipaddress | hostname> - FTP Server Address port <FTP port> - FTP Server Port (default 21) path <path to file> - Path to Certificate file to retrieve user <FTP username> - FTP Username password <FTP password> - FTP Password (prompted if missing)
`getkey`	Get certificate key.	address <ipaddress | hostname> - FTP Server Address port <FTP port> - FTP Server Port (default 21) path <path to file> - Path to Certificate Key file to retrieve user <FTP username> - FTP Username password <FTP password> - FTP Password (prompted if missing)
`viewcert`	View the current certificate.	NA
`viewcsr`	View the certificate signing request.	NA

Command	Description	Parameters
`viewcsrkey`	View the certificate signing request key.	NA
`deletecsr`	Delete the current certificate signing request.	NA

Enter `admin > Security > tls` to access the menu and menu options.

Command	Description	Parameters
`tls`	Configure TLS settings. At least one protocol must be enabled.	v1.0 Enable/Disable TLS v1.0 <true | false> v1.1 Enable/Disable TLS v1.0 <true | false> v1.2 Enable/Disable TLS v1.0 <true | false>

Addressing Security Issues

Consider doing the following in order to enhance security for console servers.

SX II supports each of these, but they must be configured prior to general use.

- Encrypt the data traffic sent between the operator console and SX II appliance.
- Provide authentication and authorization for users.
- Log data relevant to the operation for later viewing and auditing purposes. In some cases, this data is required for compliance with governmental or company regulations.
- Create a security profile.

Security Notes

Encryption of traffic between the operator console and SX II appliance is determined by the access methodology being used.

SSH and encrypted browser access (HTTPS) are enabled by default.

To accept unencrypted connections, you must manually enable the Telnet services. HTTP automatically redirects users to HTTPS, if applicable.

Configure Maintenance Settings Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Maintenance Settings from the Remote Console** *(on page 182).*

The `maintenance` commands allow you to perform maintenance-related tasks on the SX II firmware.

Enter `admin > maintenance` to access the menu.

Command	Description	Parameters
`deviceinfo`	Provides information about the SX II appliance such as build and so on.	NA
`userlist`	Displays a list of all users who are logged in, as well as their source IP addresses and any ports to which they are connected. Also found under the command root menu.	NA
`upgrade`	Upgrade device from file on FTP server.	▪ address <ipaddress | hostname> - Address of FTP Server ▪ port <FTP port> - Port of FTP server (1..65535) ▪ path <path name> - FTP server path for upgrade file. ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password. Will prompt if missing and user name given.
`upgradehistory`	Get information about the last time you upgraded the system.	NA
`backup`	Back up appliance settings and store on the FTP server.	▪ address <ipaddress | hostname> - Address of FTP Server ▪ port <FTP port> Port of FTP server (1..65535) ▪ path <path name> - FTP server path for backup file. ▪ file <file name> - Optional destination file name. Default: backup.rfp ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password. Will prompt if missing and user name given. ▪ keypass <Encryption password> - Optional encryption password.
`auditlog`	View the appliance audit log.	NA

Command	Description	Parameters
`auditlogftp`	Get the audit log and store on FTP server.	▪ address <ipaddress | hostname> - Address of FTP Server ▪ port <FTP port> - Port of FTP server (1..65535) ▪ path <path name> - FTP server path for audit log file. ▪ file <file name> - Optional destination file name. Default: audit.log ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password. Will prompt if missing and user name given.
`factoryreset`	Returns the SX II console server to its default factory settings. **Important**: If you choose to revert to the factory settings, you will erase all your custom settings and will lose your connection to SX II because, upon rebooting, the IP address of the appliance is reset to the factory default IP address of 192.168.0.192.	▪ mode <full|network> - Type of factory reset to perform
`reboot`	Reboots SX II from the CLI interface.	NA
`restore`	Restore device settings from backup file on FTP server.	▪ mode <full | protected | user | device | userdevice> - Type of restore to perform. ▪ address <ipaddress | hostname> - Address of FTP Server ▪ port <FTP port> - Port of FTP server (1..65535) ▪ path <path name> - FTP server path for backup file. ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password. Will prompt if missing and user name given. ▪ keypass <Encryption password> - Optional encryption password.

Command	Description	Parameters
logoff	Log a user off SX II (terminate their session).	▪ user <loginname> - Close all sessions for the specified user by name. ▪ session <id | all> - Close the session by identifier number or all sessions (ID/all) ▪ port <port name | port number> - Close sessions on the specified port by name or number. ▪ address <ipaddress> - Close all sessions from the specified remote address.
scriptconfigcat	List (cat) the system generated configuration script. Start line and end line are user configurable. The default values shall be as shown below. start line: "BEGIN CONFIG. SCRIPT" end line: "END CONFIG. SCRIPT"	scriptconfigcat {start startline] {end endline}
scriptget		▪ address: FTP server address <IP address> ▪ port: FTP server port (default 21), <1..65535 ▪ path: FTP server path for config file. ▪ user Optional FTP user name ▪ password Optional FTP password. Will prompt if missing and user name given.
scriptput	▪	▪ address: FTP server address <IP address> ▪ port: FTP server port (default 21), <1..65535 ▪ path: FTP server path for config file. ▪ file: Optional destination file name. Default: script.sx2 ▪ user Optional FTP user name ▪ password Optional FTP password. Will prompt if missing and user name given.

Configure Diagnostic Settings Using CLI

Note: These settings can also be configured from the Remote Console. See **Configure Diagnostic Options from the Remote Console** *(on page 191).*

The `diagnostic` commands allow you to gather information for troubleshooting.

Enter `admin > Diagnostics` to access the menu.

Command	Description	Parameters
`netif`	Network Interface Info	NA
`netstat`	Get Network Statistics	▪ type <stats | interfaces | route | ports> - stats interfaces route
`ping`	Ping a remote system to ensure it is reachable.	▪ ip <ipaddress | hostname> - IP Address/Hostname to Ping ▪ if <auto | lan1 | lan2 | usb0> - Network interface (default: auto)
`traceroute`	Trace the network route to a host.	▪ ip <ipaddress | hostname> - IP Address/Hostname to trace to ▪ maxhops <5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50> - Maximum hop limit (default: 10) ▪ if <auto | lan1 | lan2 | usb0> - Network interface (default: auto)
`diagscript`	Get and execute diagnostic script from a FTP server.	▪ address <ipaddress | hostname> - Address of FTP Server ▪ port <FTP port> - Port of FTP server (1..65535) ▪ path <path name> - FTP server path for diagnostic script file. ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password.
`diaglogput`	Take diagnostic snapshot and store on FTP server.	▪ address <ipaddress | hostname> - Address of FTP Server ▪ port <FTP port> - Port of FTP server (1..65535) ▪ path <path name> - FTP server path for diagnostic script file. ▪ user <FTP username> - Optional FTP server user name ▪ password <FTP password> - Optional FTP server password.

Command	Description	Parameters
`exportconfig`	Export a configuration file.	▪ address: FTP server address <ipaddress> ▪ port: FTP server port (default 21) <1..65535> ▪ path: FTP server path for configuration file. ▪ file: Optional destination file name. Default: exportconfig_save ▪ user: Optional FTP user name ▪ password: Optional FTP password. Will prompt if missing and user name given.

Enter `admin > diagnostics > debug` to access the menu.

Command	Description	Parameters
`setlog`	Set/get diagnostics log.	▪ module <module> - Module name ▪ level <level> - Diagnostics log level (err/warn/info/debug/trace) ▪ vflag <vflag> - Verbose flag (timestamp/module/thread/fileline) ▪ verbose <on|off> - Verbose control (on/off)
`viewstats`	View module status	▪ module <module> - Module name

Chapter 5 Connect a Rack PDU to SX II and Configure Power Control Options

SX II provides the following options when connecting a Raritan PX PDU to a SX II:

- Connect SX II to the PX PDU Serial port.

  In this configuration, access to the PX PDU is done through the PX PDU command line interface (CLI).
- Connect the SX II to the Feature port on the PX PDU.

  In this configuration, the PX PDU is managed from the SX II interface like any other power strip.

Go to https://www.raritan.com/support/product/px for support on PX PDUs.

In This Chapter

Connecting the SX II to the PX PDU Serial Port

In this configuration, after the PX is connected to the SX II, *access the PX using the PX CLI*.

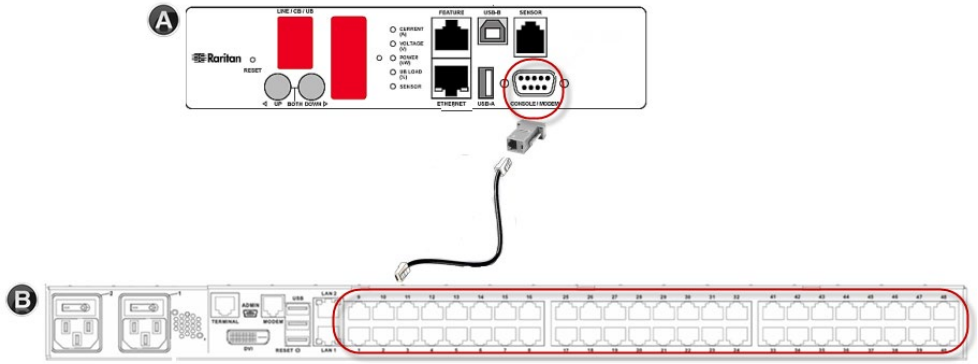
Note that the appliances used in the diagram may not match your specific models. However, the connections and ports used are the same across models.

To connect the SX II to the PX:

1. Connect an ASCSDB9F adapter to the PX2 DB9 console/modem port.

   Note: The adapter is purchased from Raritan. It does not come with PX or SX II appliances.
2. Plug a Cat5 cable into the ASCSDB9F adapter, then plug the other end of the cable in to the port on the SX II.

3. Power on the PX (if it is not already). The command line interface (CLI) interface appears.



A	PX appliance
B	SX II

Connecting the SX II to the PX PDU FEATURE Port

In this configuration, the PX is managed from the SX II interface like any other powerstrip. See Power Control.

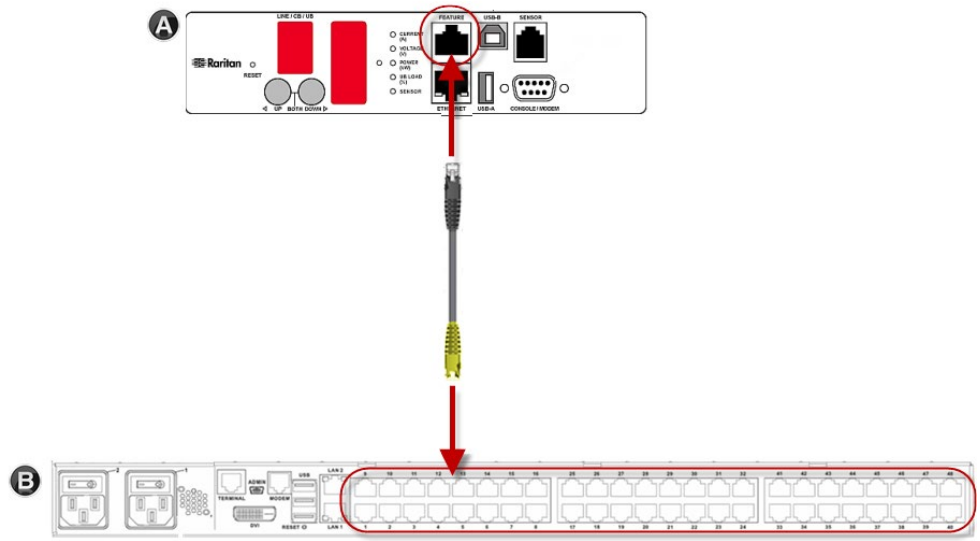
Note: Make sure that the PX PDU's Feature Port is configured to the PowerCIM setting.

Note that the appliances used in the diagram may not match your specific models. However, the connections and ports used are the same across models.

To connect the SX II to the Feature port on the PX:

1. Connect the gray end of the CSCSPCS crossover Cat5 cable into the Feature port on the PX.
2. Connect the yellow end of the CSCSPCS crossover Cat5 cable into a port on the SX II.
3. Power on the PX (if it is not already).

You can now add the PX as a managed power strip to the SX II. See ***Configure Power Strips from the Remote Console*** (on page 68)or ***Configure Power Strips Using CLI*** (on page 198)..



A	PX appliance
B	SX II

Appendix A Specifications

In This Chapter

SX II Dimensions and Physical Specifications

Form factor	1U, rack mountable
Dimensions	17.3" W x 13.15'' D x 1.73'H '; (440mm x 334mm x 44mm)
Weight	9.08 lbs; (4.12 kg)
Power	100/240VAC auto-switching: 50-60 Hz, .35A, 36-72VDC auto-switching
Max power consumption	4-Port SX: 21W | 8-port SX: 21W | 16-port SX: 22W | 32-port SX: 23W | 48-port SX: 25W
Temperatures	Operating: 0°C – 50°C. Non-Operating: 0°C – 55°C
Humidity	Operating: 20% – 85%. Non-Operating: 10% – 90%
Altitude	Operates properly at any altitude from 0 to 2,000 meters

Supported Remote Connections

Network

- 10BASE-T
- 100BASE-T
- 1000BASE-T (Gigabit) Ethernet

Protocols

- TCP/IP
- HTTP
- HTTPS
- RADIUS
- LDAP/LDAPS
- SSH
- Telnet
- TACACS+
- UDP
- SNTP

Supported Number of Ports and Remote Users per SX II Model

Model	Number of ports
SX2-04 and SX2-04M	4
SX2-08 and SX2-08M	8
SX2-16 and SX2-16M	16
SX2-32 and SX2-32M	32
SX2-48 and SX2-48M	48

Maximum Number of Users Session

A maximum of 200 users can access a single SX II at the same time.

This applies to the Remote Console access, Direct Port Access and command line interface access via SSH/Telnet.

Maximum Number of Support Users Per Port

A maximum of 10 users can access the same port and the same time.

This applies to the Remote Console access, Direct Port Access and command line interface access via SSH/Telnet.

Port Access Protocol Requirements

Protocol	Port	Communication direction
HTTP	Ports 80, 443 and 5000 must be open in the firewall for the appliance to operate. **Port 80** This port can be configured as needed. See HTTP and HTTPS Port Settings. By default, all requests received by the SX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The SX II responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the SX II, while still preserving complete security. **Port 443** This port can be configured as needed. See HTTP and HTTPS Port Settings. By default, this port is used for multiple purposes, including the web server for the HTML client, the download of client software onto the client's host, and the transfer of data streams to the client. **Port 5000** This port is used to discover other Dominion devices and for communication between Raritan devices and systems, including CC-SG for devices that CC-SG management is available. By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, see Network Settings.	Both
HTTPS SSL only	**Port 443** TCP port 443 must be open. Port 80 can be closed.	Both
SSH	**Port 22** TCP port 22 must be open. Port 22 is used for the SX II command line interface (CLI).	Both
Telnet	**Port 23** TCP port 23 must be open.	Both
TACACS+	**Port 49** Port 49 must be open.	Outgoing

Protocol	Port	Communication direction
RADIUS	**Port 1812** If SX II is configured to remotely authenticate user logins via the RADIUS protocol, port 1812 is used and must be open. However, but the system can also be configured to use any port of your designation. **Optional** **Port 1813** If the SX II is configured to remotely authenticate user logins via the RADIUS protocol, and it also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation is used to transfer log notifications.	Outgoing
LDAP	**Ports 389 and 636** Port 389 or 636 must be open. If the SX II is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. **Optional**	Outgoing
SNMP	**Ports 161 and 162** Port 161 is used for inbound/outbound read/write SNMP access. Port 162 must be open. Port 162 is used for outbound traffic for SNMP traps.	Both (Port 161) Outgoing (Port 162)
For FTP upgrades	**Port 21** Port 21 must be open.	Outgoing
SYSLOG on Configurable UDP Port	**Port 514** By default UDP port 514 is used. Configurable to a port of your choice.	Outgoing
SNTP (Time Server) on Configurable UDP	**Port 123** The SX II offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation. **Optional**	Both

You may have to open additional ports when NFS logging, using LDAP servers, and so forth.

These ports may vary from installation-to-installation depending on network topologies, virtual Local Area Networks (VLANs), and firewall configurations.

Contact your network administrator for site-specific information and settings.

SX II Port Pins

Local Terminal Port		
pin	Definition	Direction
pin 1	RTS	Output
pin 2	N/A	
pin 3	TXD	Output
pin 4	Ground	
pin 5	Ground	
pin 6	RXD	Input
pin 7	N/A	
pin 8	CTS	Input

DTE Mode on Server Port		
pin	Definition	Direction
pin 1	RTS	Output
pin 2	DTR	Output
pin 3	TXD	Output
pin 4	Ground	
pin 5	Ground	
pin 6	RXD	Input
pin 7	DSR	Input
pin 8	CTS	Input

DCE Mode on Server Port		
pin	Definition	Direction
pin 1	CTS	Input
pin 2	DSR	Input
pin 3	RXD	Input
pin 4	Ground	
pin 5	Ground	
pin 6	TXD	Output

DCE Mode on Server Port		
pin 7	DTR	Output
pin 8	RTS	Output

Port Ranges

The port range for internal port configuration - CSC, HTTP, HTTPS, SSH, Telnet, DPA SSH , DPA Telnet - is 1 to 64510. The configurable port range for socket creation is limited to 1024 to 64510.

External port configuration - LDAP, RADIUS, TACACS+ and SNMP - is not affected by a port range limitation.

Network Speed Settings

SX II network speed setting

Network switch port setting		**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
	Auto	Highest Available Speed	1000/Full	SX II: 100/Full Switch: 100/Half	100/Half	SX II: 10/Full Switch: 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
	100/Full	SX II: 100/Half Switch: 100/Full	SX II: 100/Half Switch: 100/Full	100/Full	SX II: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	100/Half	SX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	SX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	SX II: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	No Communication	SX II: 10/Full Switch: 10/Half	10/Half

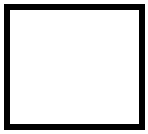
Legend:

Does not function as expected

Supported

Functions; not recommended

NOT supported by Ethernet specification; product will communicate, but collisions will occur



Per Ethernet specification, these should be “no communication,” however, note that the SX II behavior deviates from expected behavior

Note: For reliable network communication, configure the SX II and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure the SX II and LAN Switch to Autodetect (recommended), or set both to a fixed speed/duplex such as 100MB/s/Full.

Default User Session Timeouts

- SX II interface - 5 minutes (to change this, select Security > Settings and update the "Idle Timeout (minutes)" field)
- SSH - 16 minutes
- Telnet - 2 hours

SX II Supported Local Port DVI Resolutions

Following are the resolutions supported when connecting to a DVI monitor from the SX II local port.

- 1920x1080@60Hz
- 1280x720@60Hz
- 1024x768@60Hz (default)
- 1024x768@75Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1600x1200@60Hz
- 800x480@60Hz
- 1280x768@60Hz
- 1366x768@60Hz
- 1360x768@60Hz
- 1680x1050@60Hz
- 1440x900@60Hz

SX II Appliance LED Status Indicators

LEDs are used to indicate power status, appliance status and target connection status.

There are LEDs located on the front panel and rear panel of the SX II. Front Panel LED Status Indicators

- When SX II boots up, only the Power LED turns on. The power LED turns both red and blue.
- Port Channel LEDs are off the whole time SX II boots up.
- Once SX II is fully powered on, the Power LED remains on.
  - If a single power supply is plugged in, the Power LED is **Red**.
  - If both power supplies are plugged in, the Power LED is **Blue**.
- When you physically connect a powered-on target to a port on SX II via a CAT5 cable, the Port channel's LED turns on.

  The LED remains on until the target is disconnected.

Note: The target must be powered on in order for the SX II Port channel LED to turn on and the SX II to detect the target.

- When you physically disconnect a target from a port on an SX II, the port channel's LED turns off.
- When you log in to SX II and connect to a target via either Raritan Serial Console (RSC), SSH or the Local Console, the port channel's LED blinks.

  The LED blinks until you end the your connection to the target.

  If you are connected to more than one target at the same time, all LEDs blink in unison.
- When you press the SX II's Reset button to reset the appliance or when you perform a reboot from the SX II GUI, the Power LED(s) blinks as the appliance powers down and turns off.

  While the appliance powers back up, the Power LED(s) continue to blink.

  Once the appliance is powered on, the Power LED(s) stop blinking and the LED remains on.

Target Cable Connection Distances and Rates

SX II supports the following connection distances using a CAT5 cable between its Serial port and a target.

Distance	Bits per second
300ft/91m	1,200
300ft/91m	1,800
300ft/91m	2,400
200ft/60m	4,800
100ft/30m	9,600
50ft/15m	19,200
25ft/7.5m	38,400
16ft/5m	57,600
8ft/2.5m	115,200
4ft/1.2m	230,400

Appendix B Updating the LDAP Schema

In This Chapter

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the SX II determines the permissions for a given user based on the permissions of the user's . Your remote LDAP server can provide these user names by returning an attribute named as follows:

rciusergroup attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

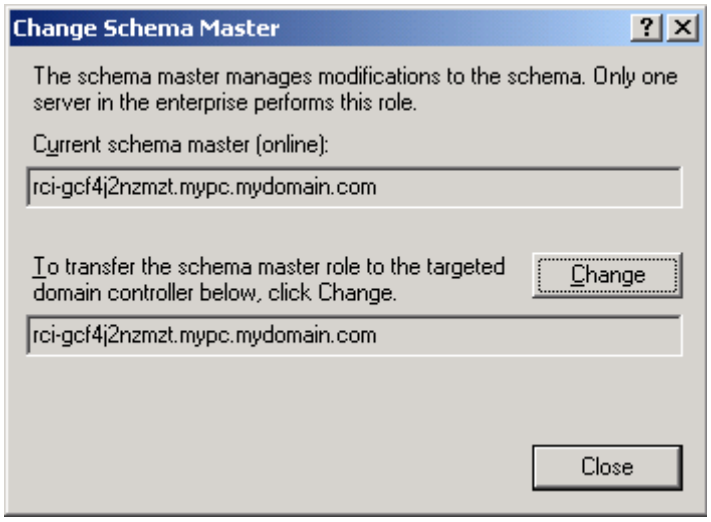
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

To permit write operations to the schema:

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



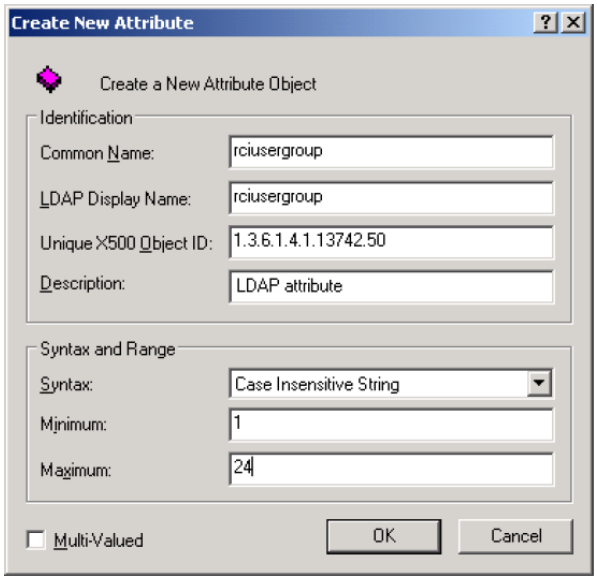
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

To create new attributes for the rciusergroup class:

1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.



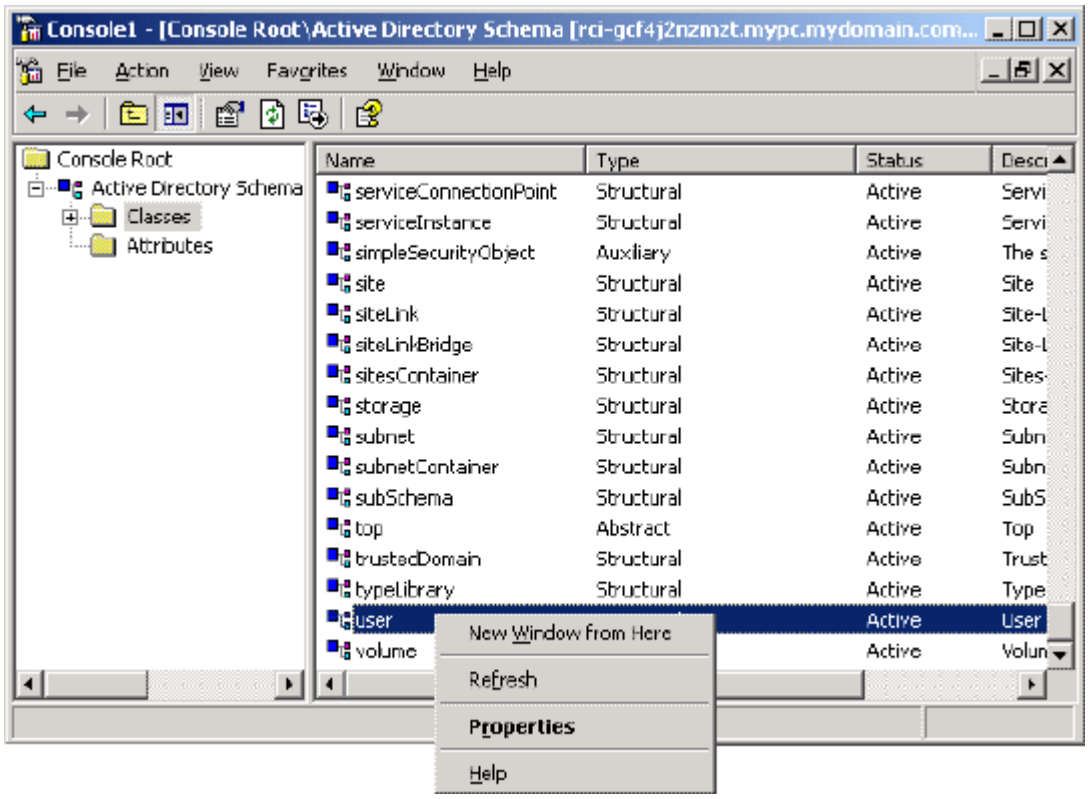
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

To add attributes to the class:

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.
6. Choose rciusergroup from the Select Schema Object list.

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

To update the schema cache:

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

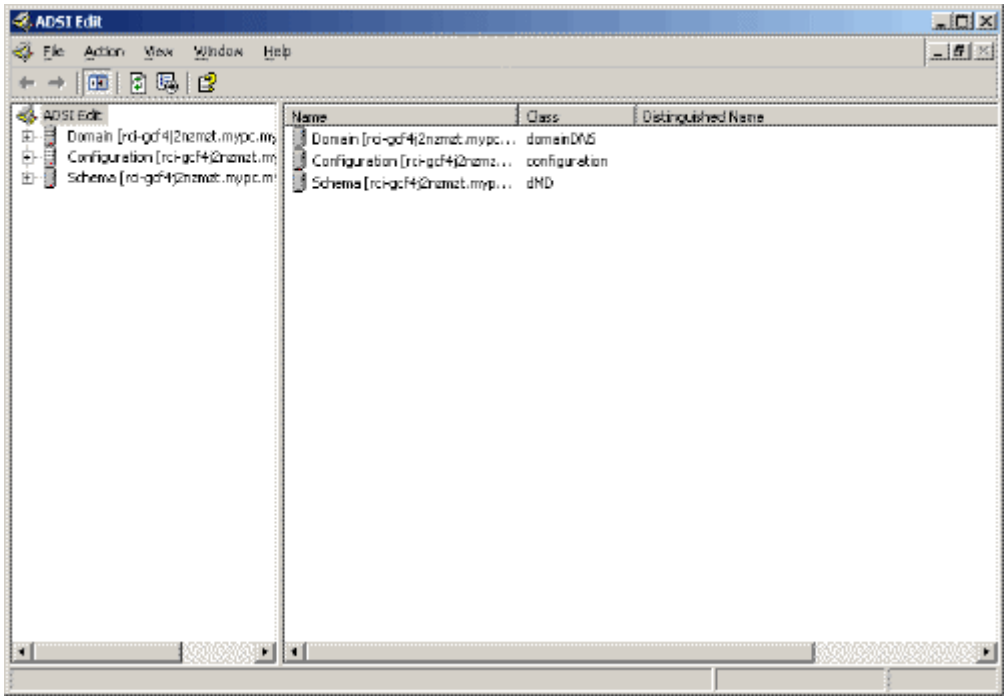
Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

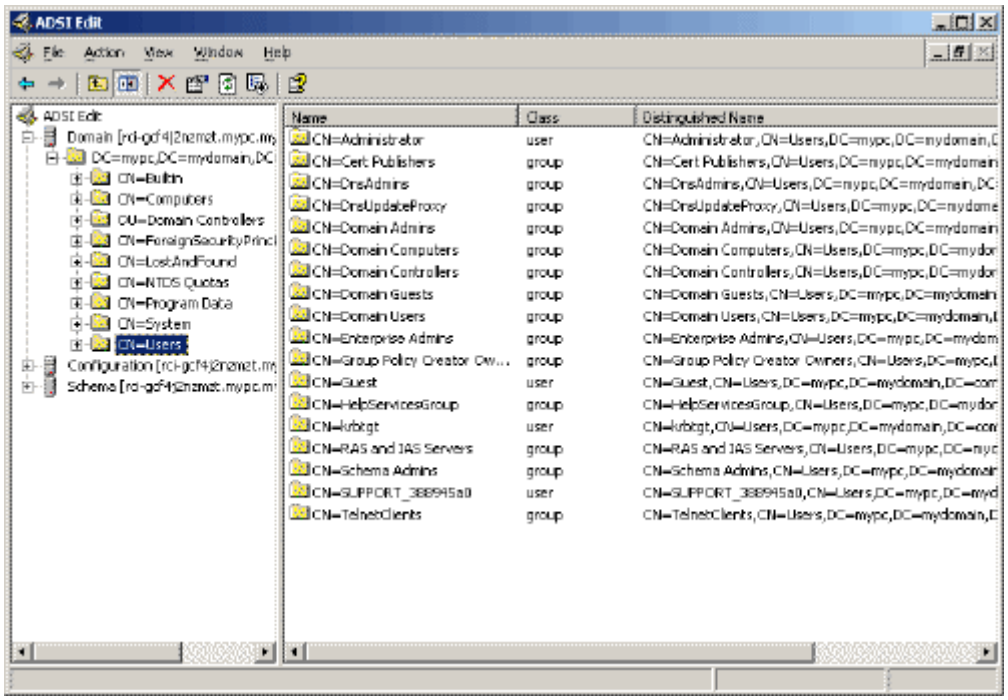
To edit the individual user attributes within the group rciusergroup:

1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

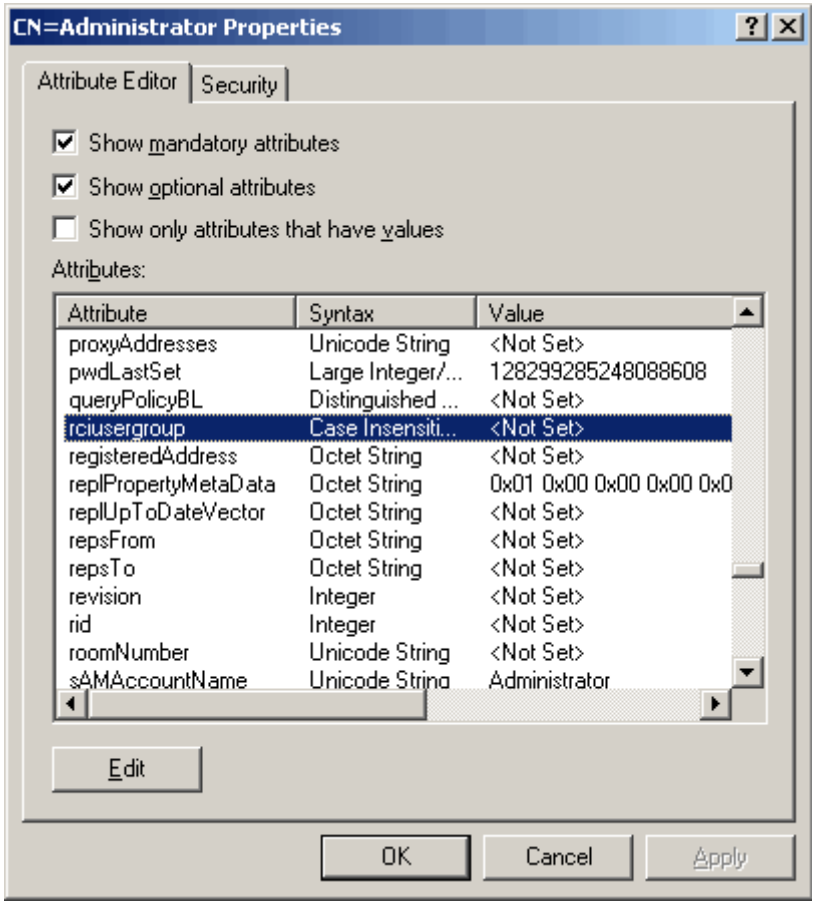
3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.



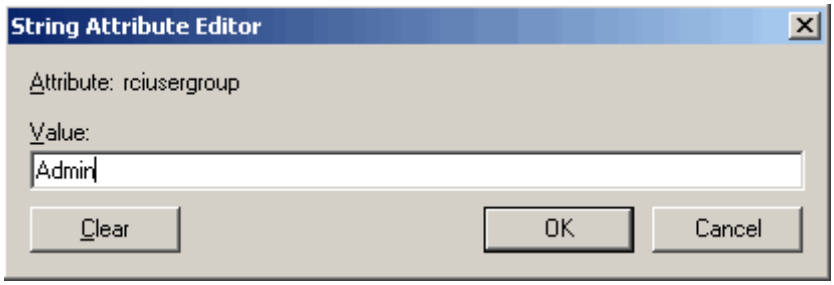
4. Open the Domain.
5. In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user (created in the SX II) in the Edit Attribute field. Click OK.



Appendix C RADIUS Configuration Examples

This appendix contains instructions and examples to help configure various RADIUS implementations.

In This Chapter

Cisco ISE 2.1.x Configurations

SX II performs authorization by means of user's membership to local User Groups. When using remote authentication, there is no user account locally on SX II, therefore there must be a way of returning user group information from the remote authentication server that SX II will then match and perform appropriate authorization. To achieve this, you must create the appropriate local group on SX II, and configure the remote authentication server to return appropriate matching group (case sensitive).

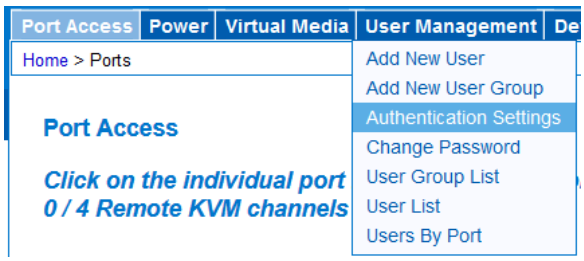
The following examples demonstrate an authorization profile called "Raritan Dominion KXIII_SXII Profile".

- See ***Cisco ISE 2.1.x for RADIUS*** (on page 256)
- See ***Cisco ISE 2.1.x for TACACS*** (on page 269)

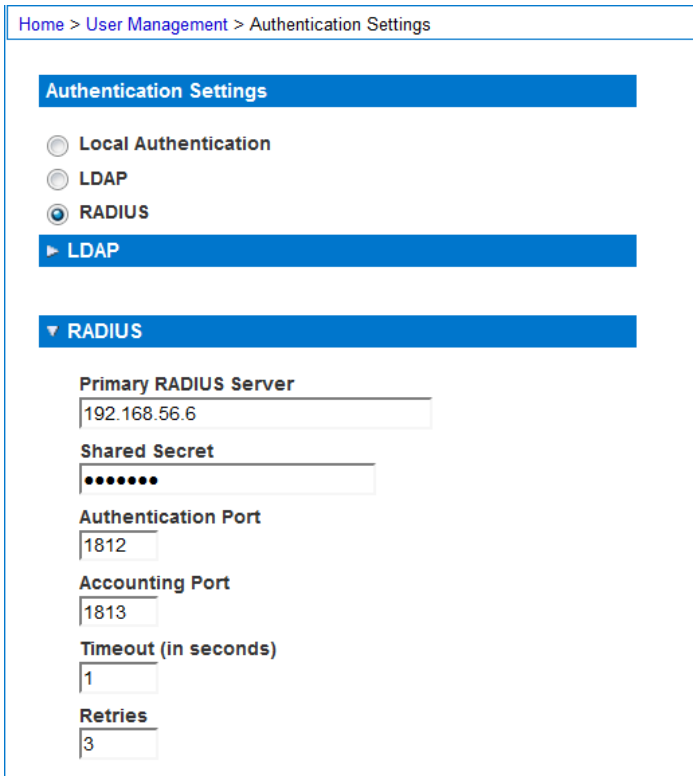
Cisco ISE 2.1.x for RADIUS

Configure SX II for RADIUS settings:

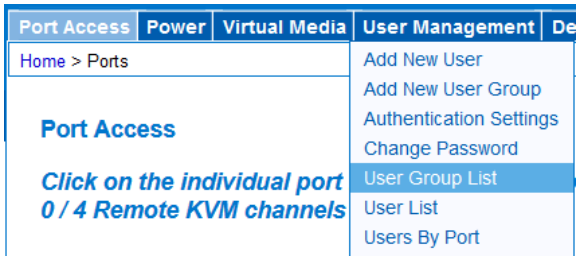
1. Login to SX II with administrative account.
2. Access User Management>Authentication>RADIUS



3. Configure RADIUS section to point to Cisco ISE 2.1.x running Radius server.



4. Create user group with appropriate permission and port permission by accessing User Management>User Group List.



Group Name *

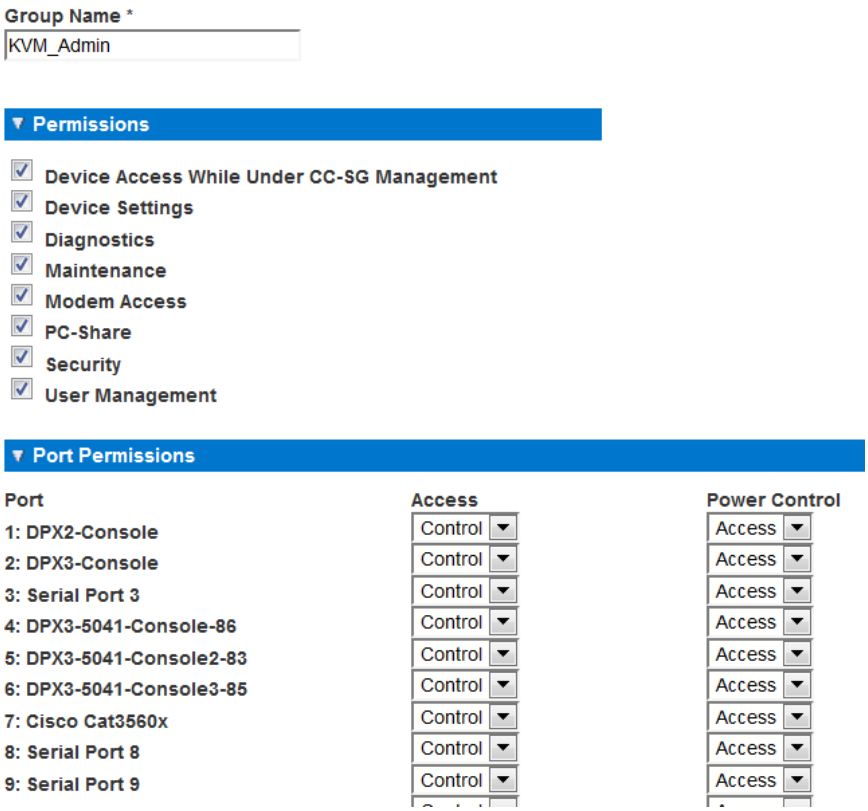
KVM_Admin

▼ Permissions

- [x] Device Access While Under CC-SG Management
- [x] Device Settings
- [x] Diagnostics
- [x] Maintenance
- [x] Modem Access
- [x] PC-Share
- [x] Security
- [x] User Management

▼ Port Permissions

Port	Access	VM Access	Power Control
1: CCSG from BMO	Control	Read-Write	Access
2: ESXi	Control	Read-Write	Access
3: Dominion_KX3_Port3	Control	Read-Write	Access
4: Dominion_KX3_Port4	Control	Read-Write	Access
5: Dominion_KX3_Port5	Control	Read-Write	Access
6: Fedora	Control	Read-Write	Access
7: Dominion_KX3_Port7	Control	Read-Write	Access
8: Dominion-KX2_Port46	Control	Read-Write	Access
9: Dominion_KX3_Port9	Control	Read-Write	Access



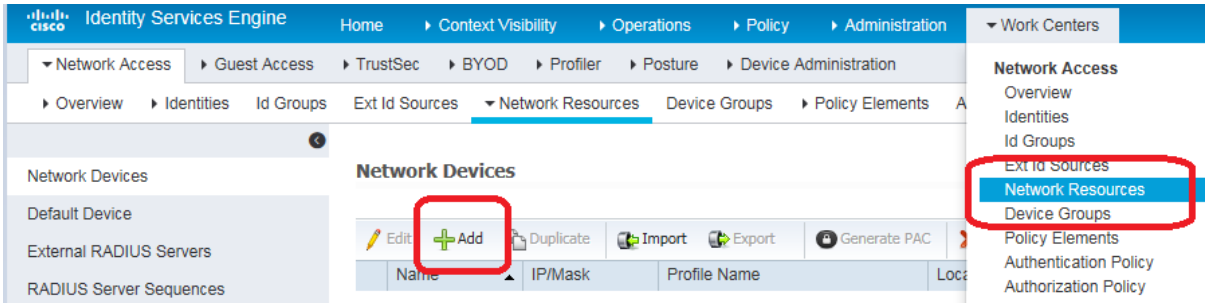
Configure Cisco ISE:

- Step 1: Add SX II Network Device
- Step 2: Add/Edit Users (Skip for external user database such as AD/LDAP)
- Step 3: Configure/Verify Allowed Authentication Protocol Service (PAP/CHAP/MS-CHAP)
- Step 4: Create Authorization Profile
- Step 5: Configure/Create Authorization Policy

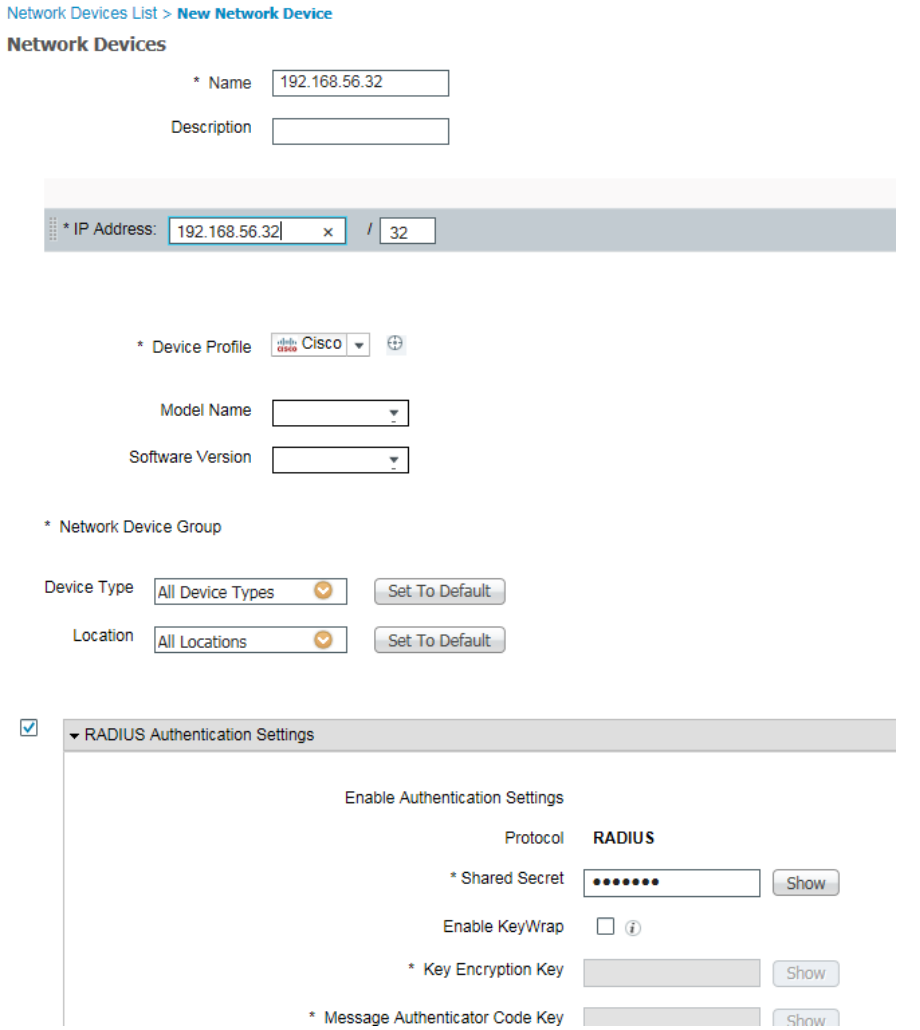
Step 1: Add SX II Network Devices:

1. Access Cisco ISE Web URL ***https://x.x.x.x/admin*** (see https://x.x.x.x/admin - ***https://x.x.x.x/admin***) and login with administrative credentials.

2. Access Work Centers>Network Resources under Network Access section to load Network Device menu and click Add



3. Configure Name, Description and IP Address/Range as well as enable Radius Authentication Settings option and set Shared secret, then click Submit to save changes. If appropriate and applicable, assign Device Type and Location.

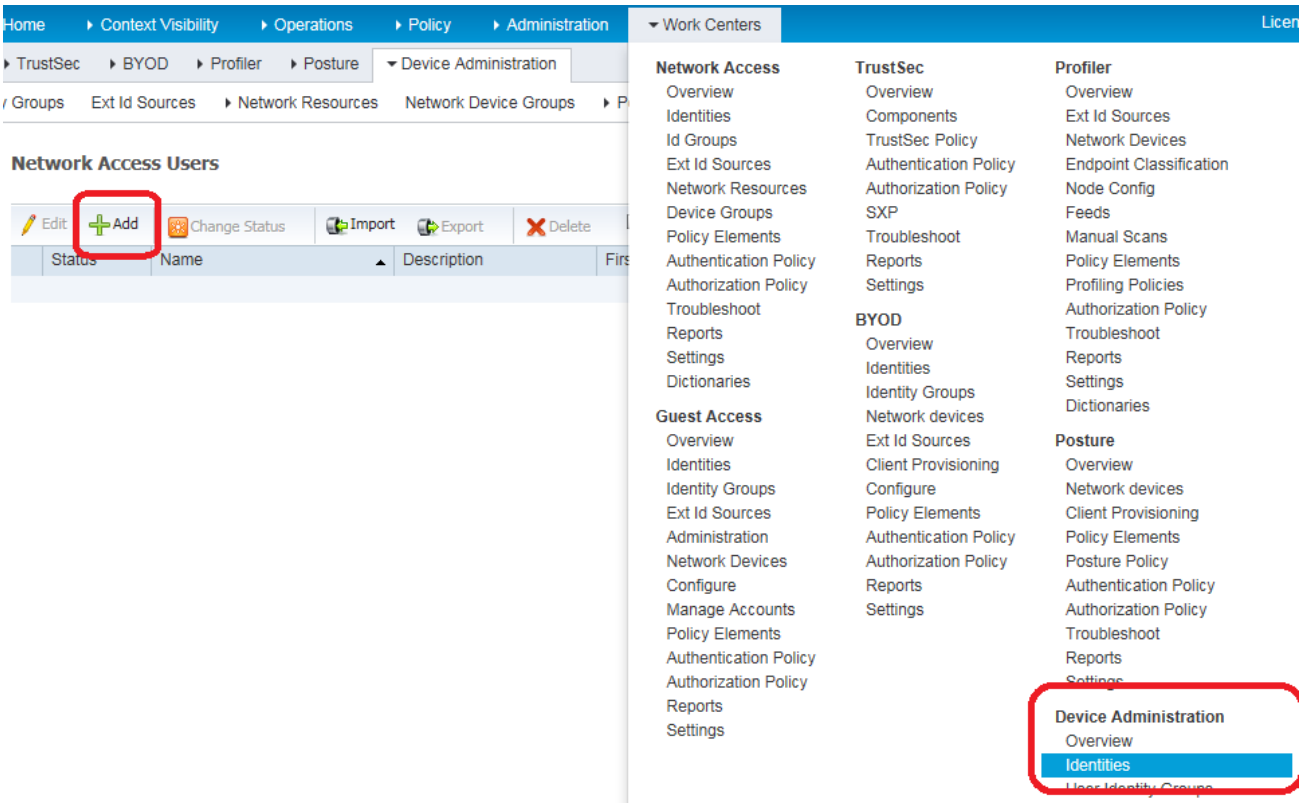


Step 2: Create/Edit User

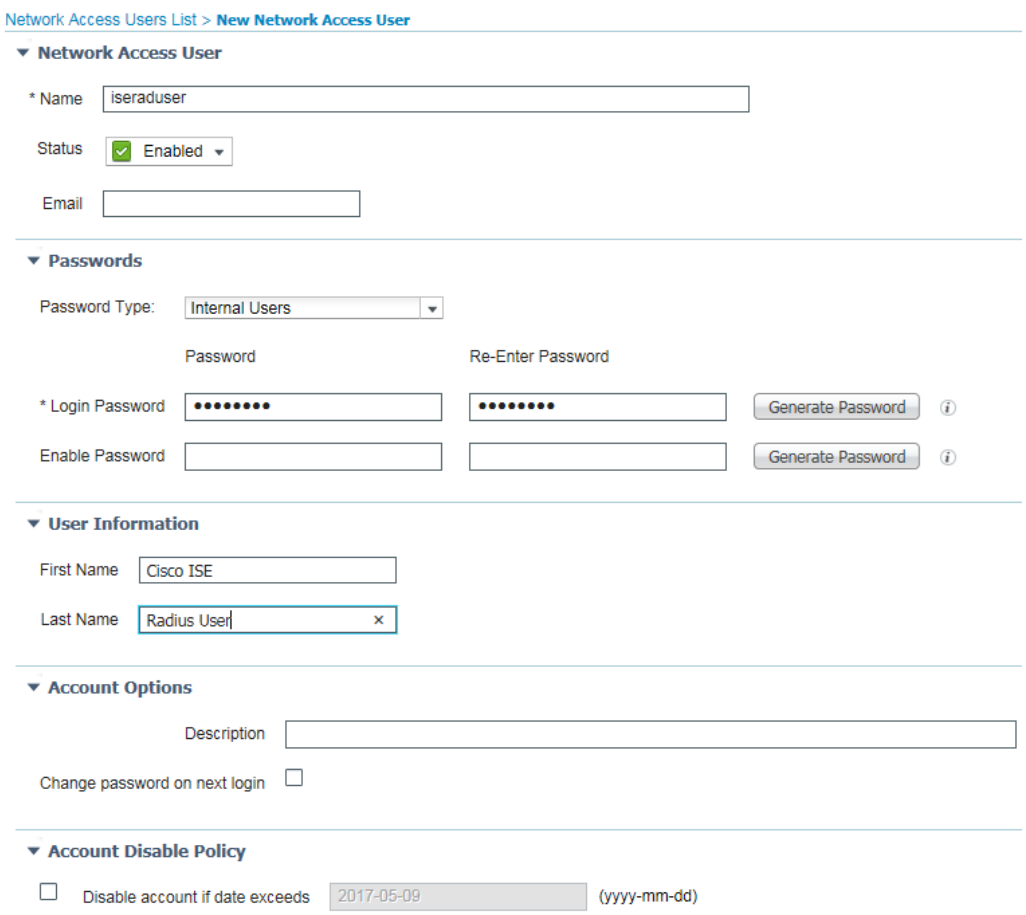
Note: Skip this step in production environments where user accounts are already created, or there is a configured external identity source (AD/LDAP).

1. Access Work Centers>Device Administration>Identities> and click 

to add a user

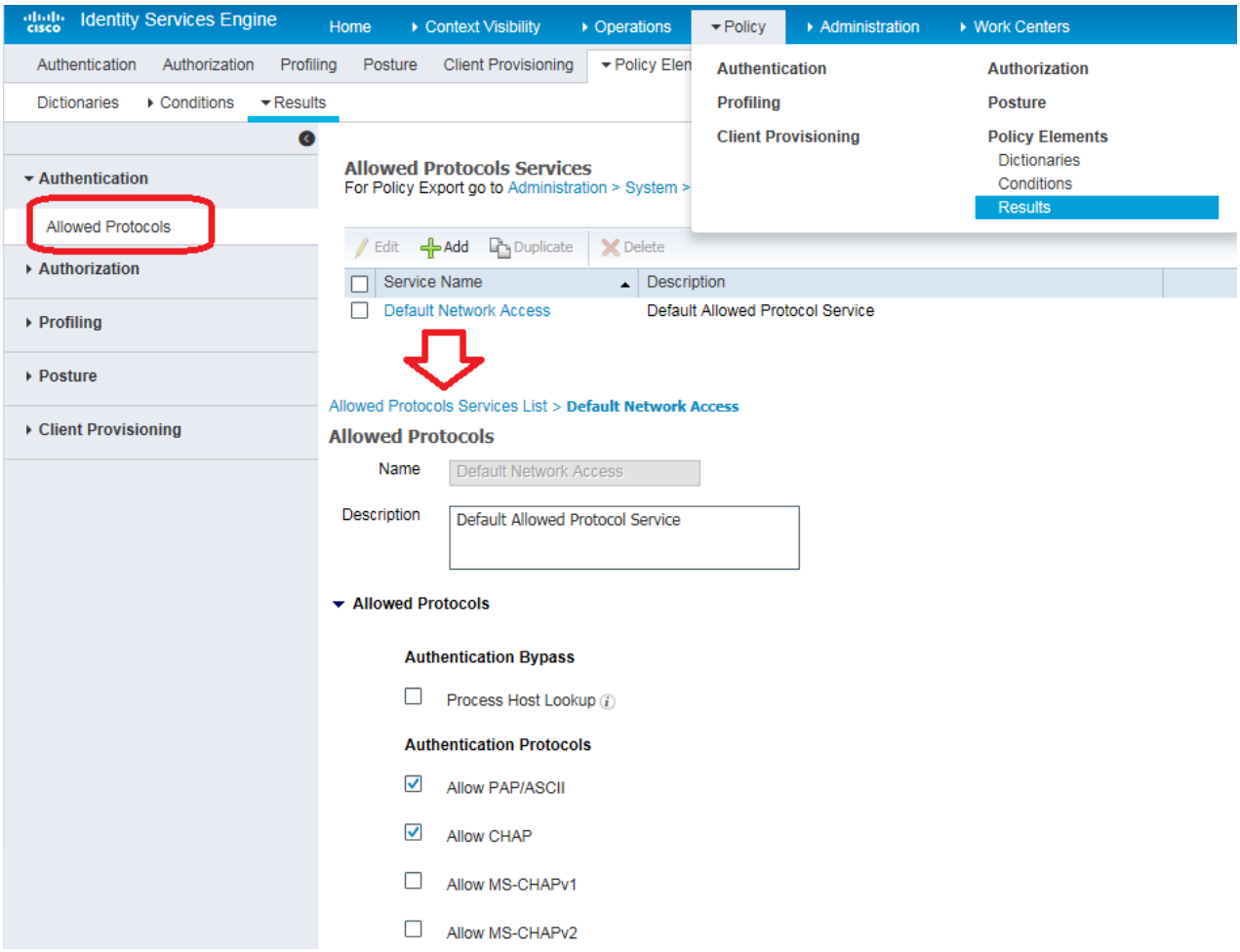


2. Configure required fields and click Submit to add user



Step 3: Configure/Verify Allowed Authentication Protocol Service (PAP/CHAP/MS-CHAP)

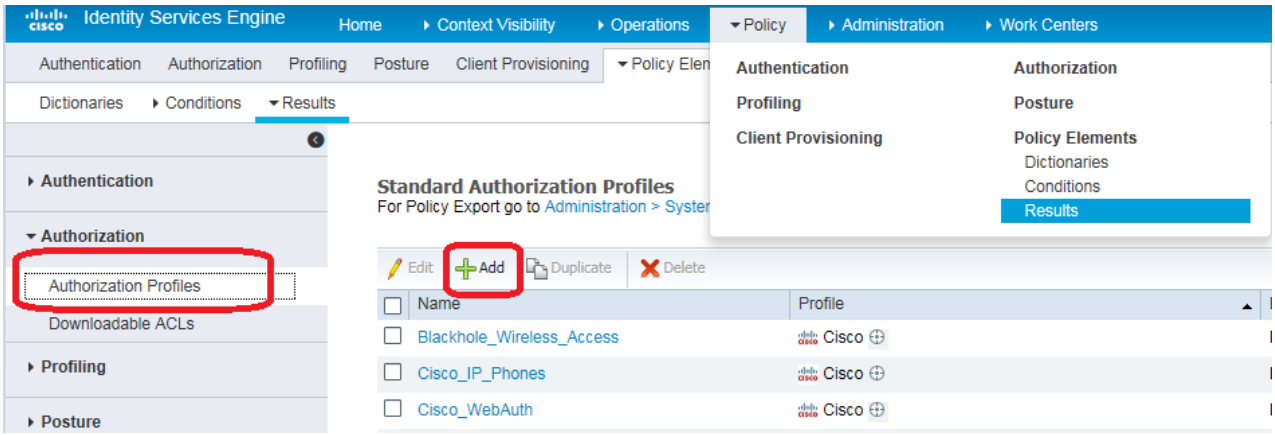
1. Access Policy>Results under Policy Elements section. Select Allowed Protocols under Authentication Dropdown from left pane. Click to Edit Default Network Access and select CHAP. SX II supports both PAP and CHAP authentication types. If CHAP authentication type is desired, verify Global Authentication Type setting on SX II RADIUS configuration is set to CHAP, and verify this step is completed on Cisco ISE 2.1.x server.



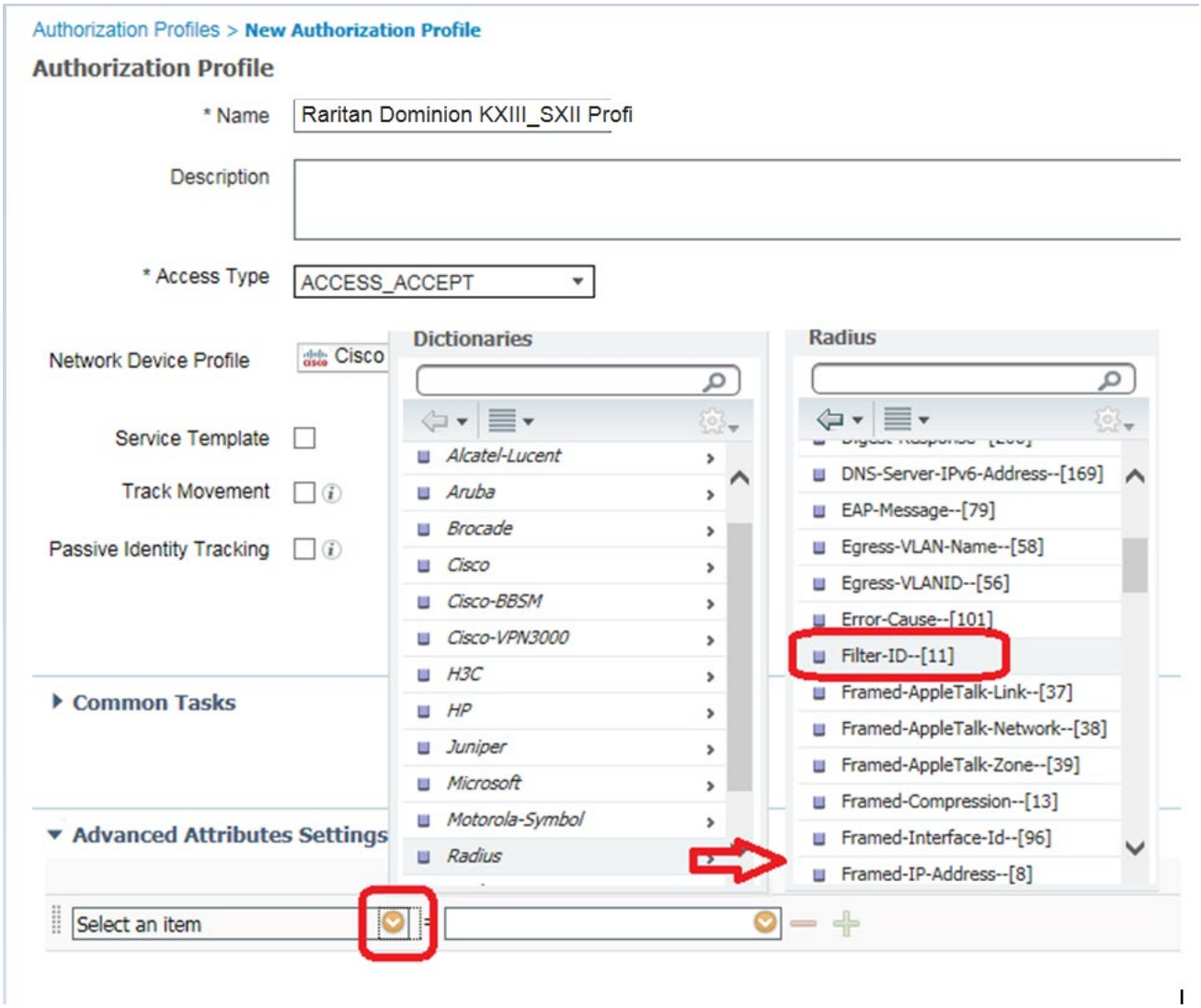
Step 4: Create Authorization Profile

1. In the Policy Elements tab, choose Policy > Results. In the left panel that displays, choose Authorization > Authorization Profiles, then Click Add

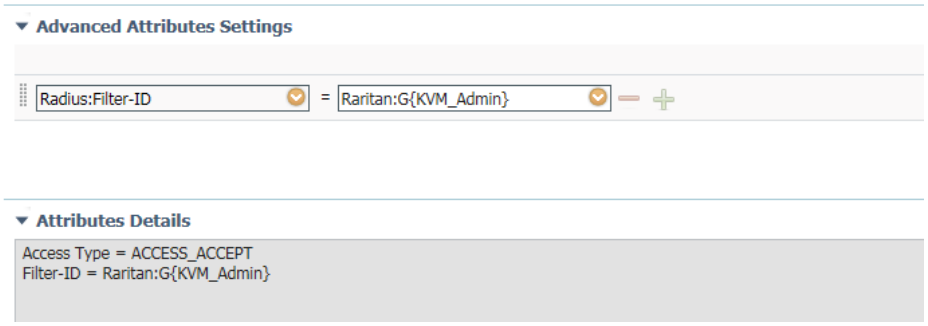
2. Under General Tab configure Policy Friendly Name



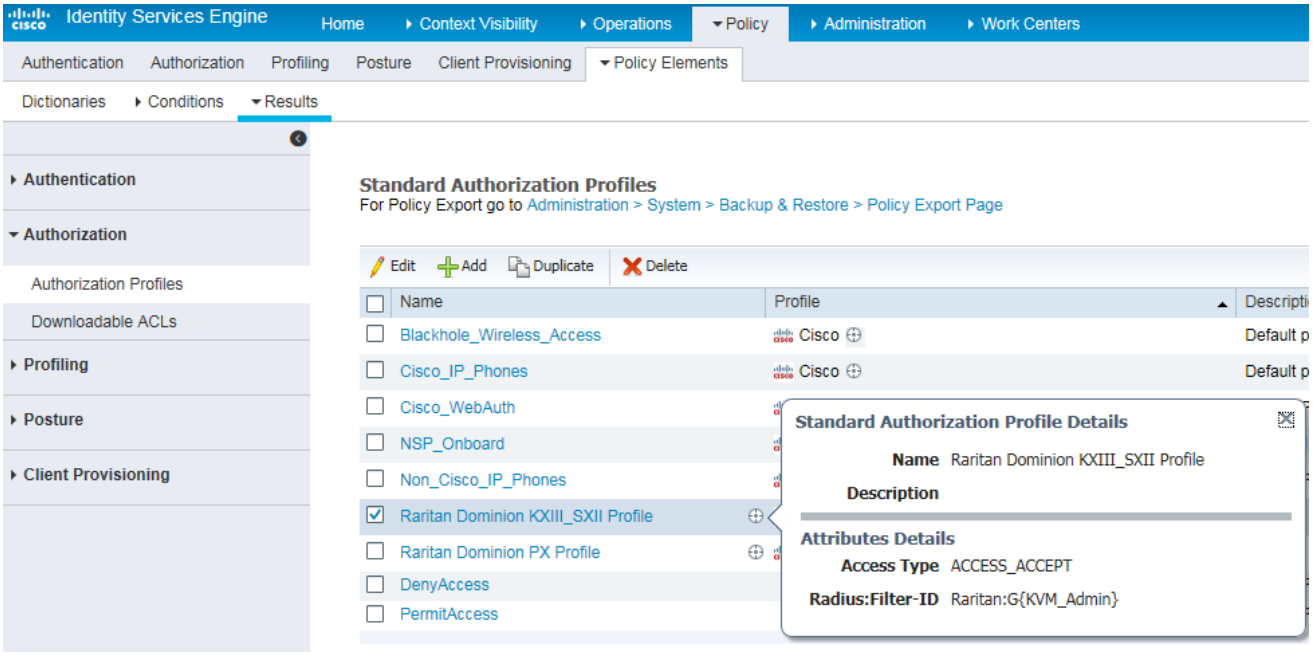
3. Specify appropriate Profile name. Scroll down to Advanced Attributes Settings section and click on drop down next to Select and Item text field. Select Radius and from Submenu select Filter-ID--[11] option.



4. Verify your selection in the text box. It must correctly display attribute name Radius:Filter-ID. In the next test field, type attribute value Raritan:G{KVM_Admin} and click anywhere on the page to set it. Confirm Attribute Details display as shown below.

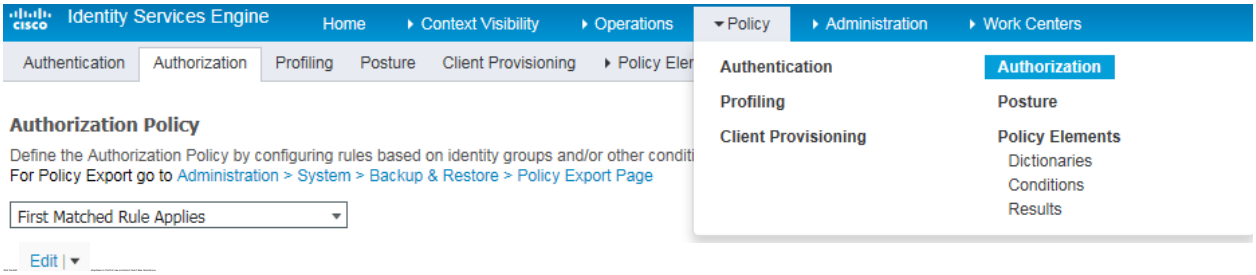


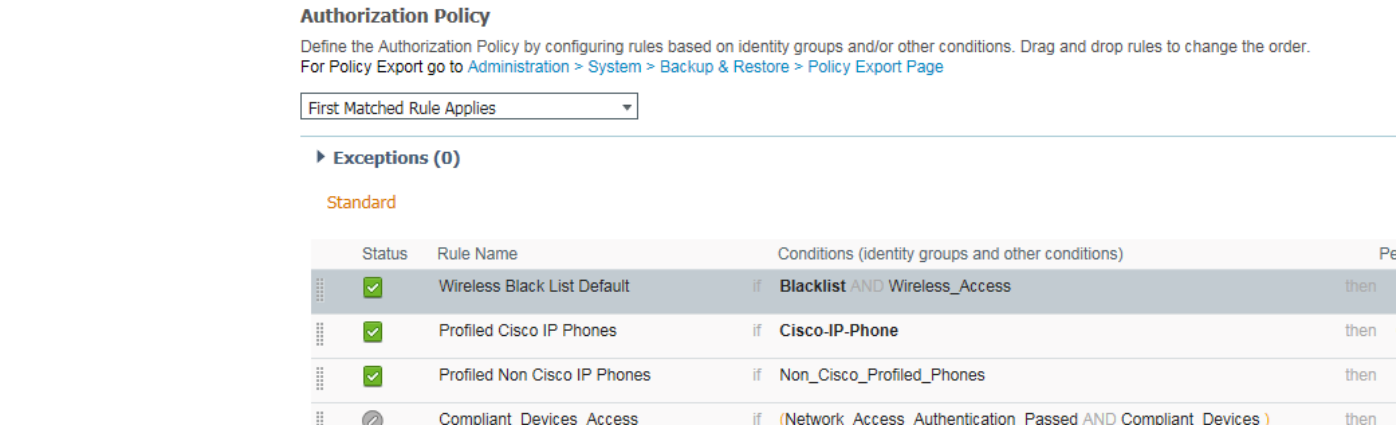
5. Click Submit to create new Authorization profile and return to the profile list summary page. Verify profile name and mouse over  icon for preview of summary.



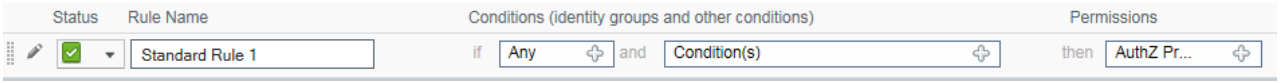
Step 5: Configure/Create Authorization Policy

1. Access Policy>Authorization to see policy listing.

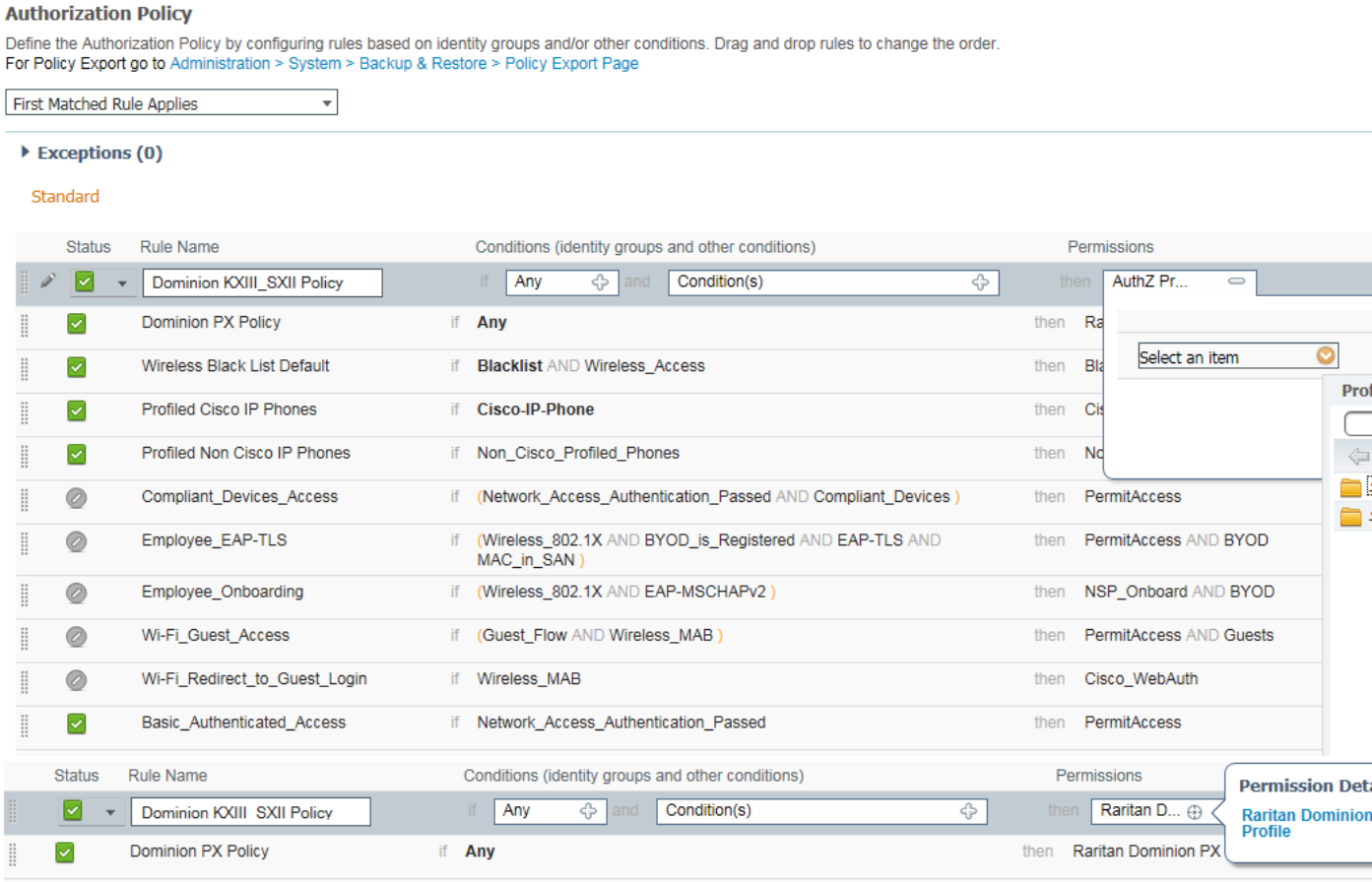




New first row is added.



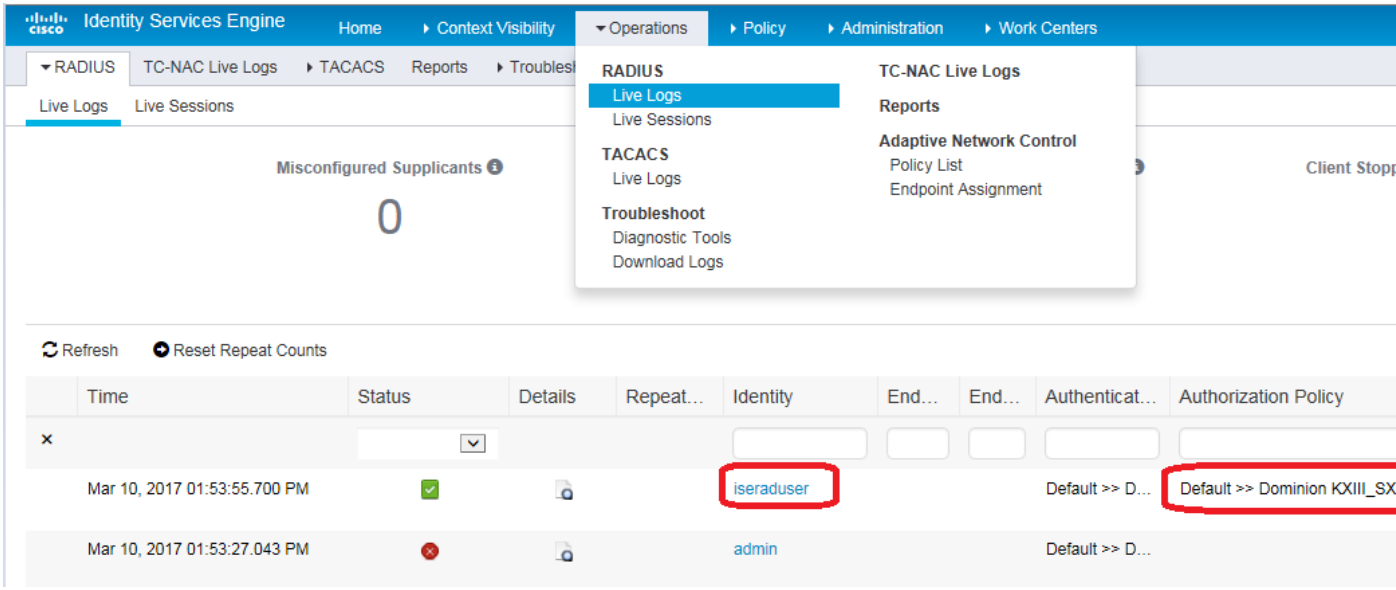
1. Specify appropriate Policy name and Click Add ( ) in the Permission text box. Select Standard to view a submenu with a list of available profiles. Select Raritan Dominion KXIII_SXII Profile and click Done complete selection.



2. Click Save to create policy.

Troubleshooting Tips:

1. Verify from Live Logs under Operations> TACACS that correct Authorization Policy is being applied. Click Details icon to see more information



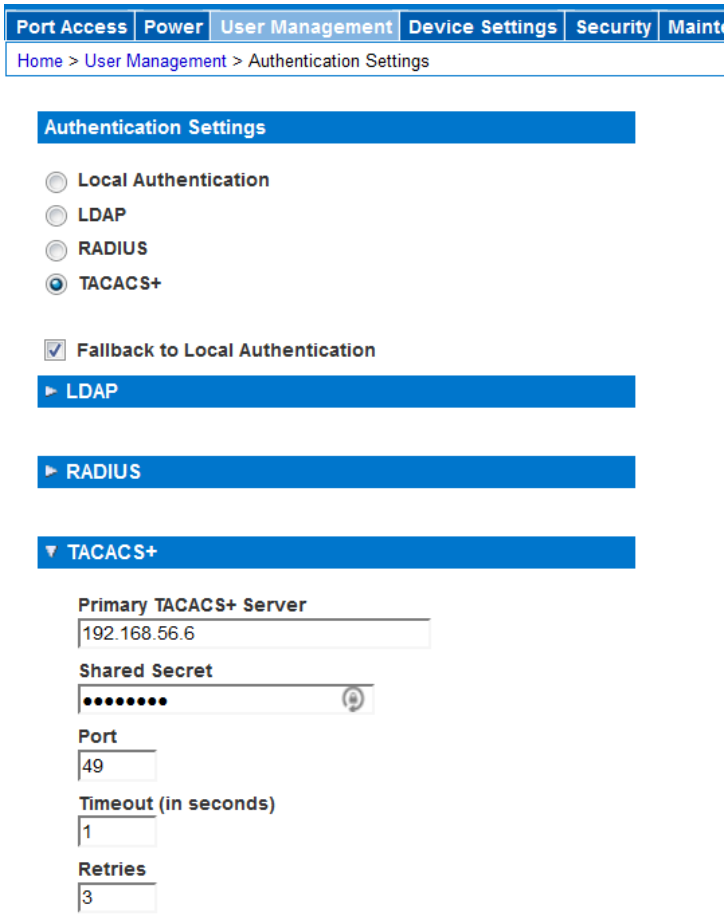
2. User authorization may fail on SX II if incorrect policy is applied. If this occurs, consider the following options:
   - Moving policy higher up in the order (in case of multiple policy sets).
   - More appropriate conditions in policy coupled with device type and location when adding SX II as a network device in Cisco ISE.

Cisco ISE 2.1.x for TACACS

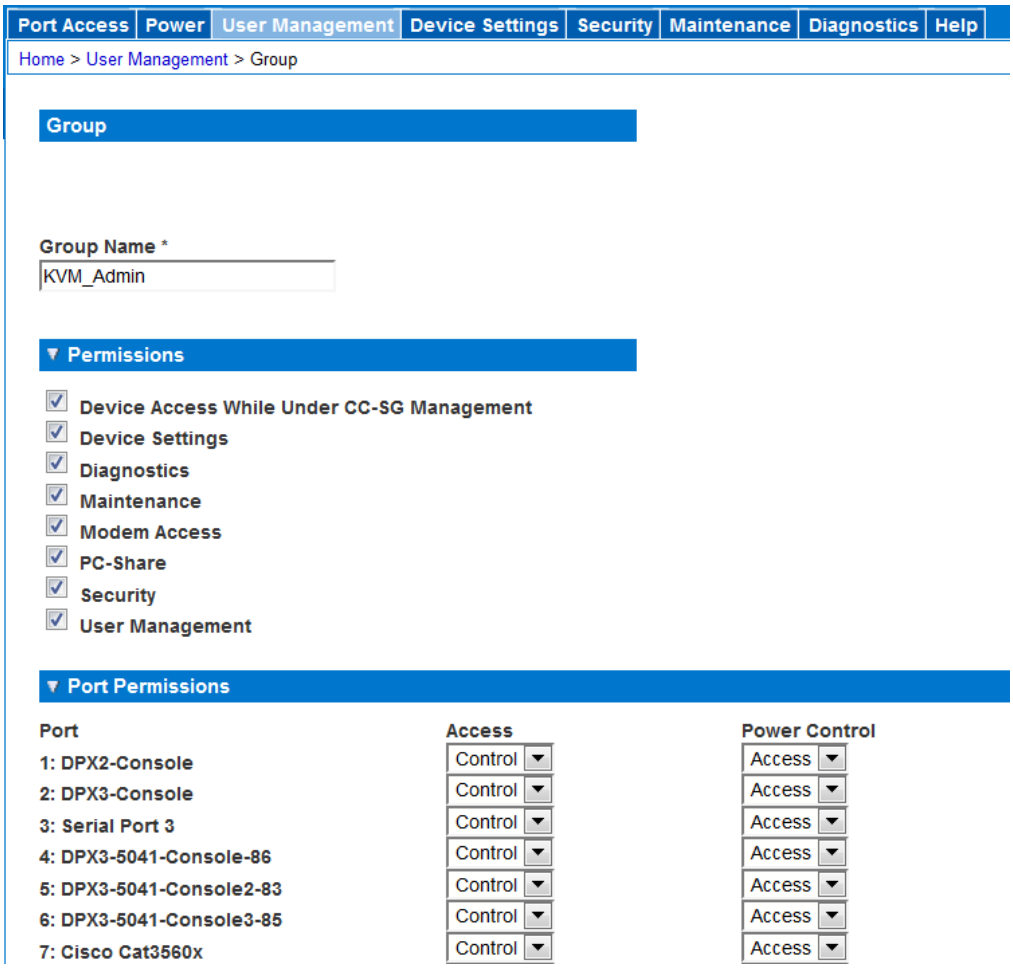
Configure SX II for TACACS+ settings:

1. Login to SX II with administrative account.

2. Access User Management>Authentication Settings and Configure it to point to Cisco ISE 2.1.x running TACACS server



3. Create user group with appropriate permissions and port permissions by accessing User Management>User Group List>Add New User Group



Configure Cisco Identity Service Engine (ISE):

Step 1: Add SX II Network Device

Step 2: Add/Edit Users (Skip if using external user database such as AD/LDAP)

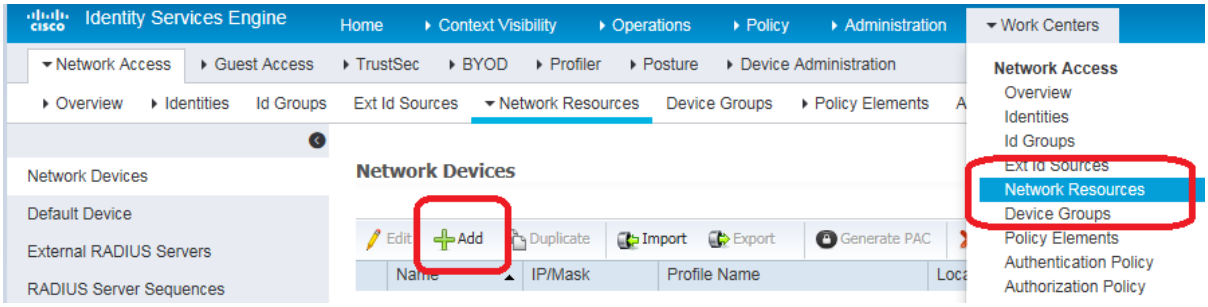
Step 3: Create TACACS profile policy element

Step 4: Configure/Create Device Admin Policy Set

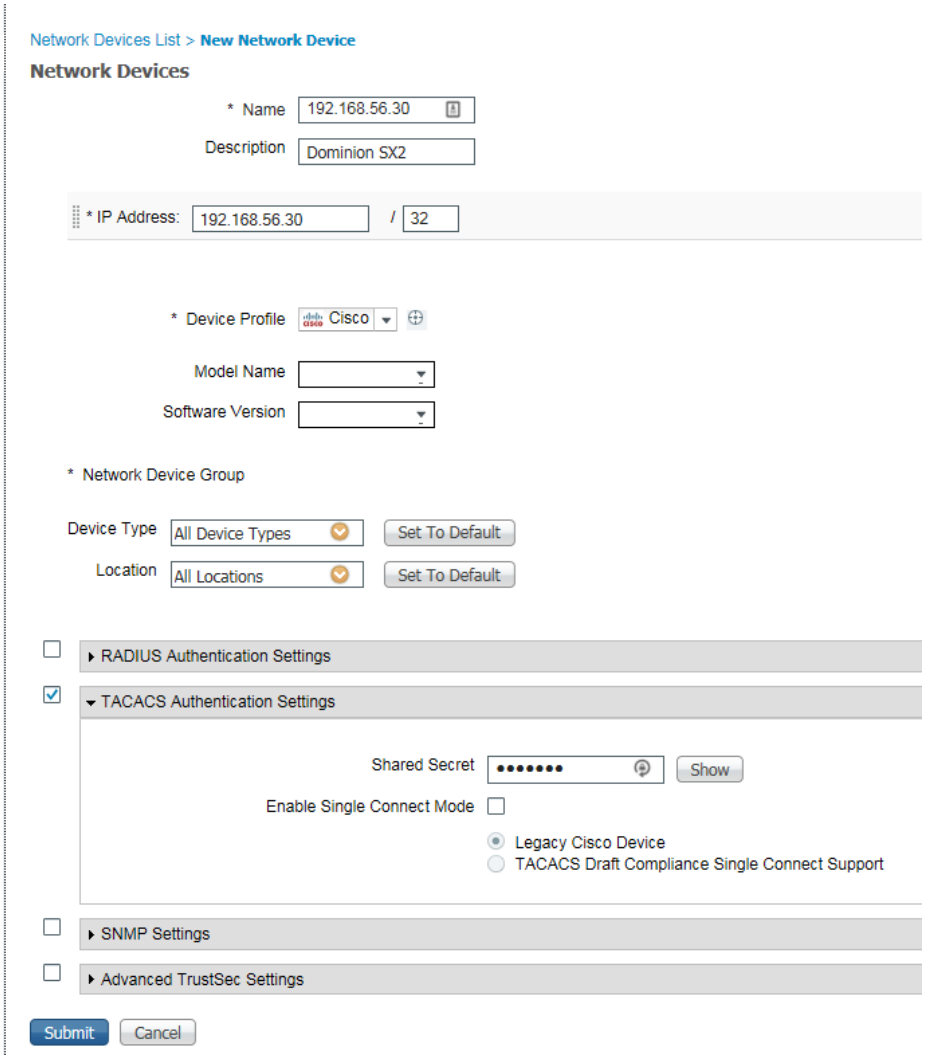
Step 1: Add SX II Network Devices:

1. Access Cisco ISE Web URL ***https://x.x.x.x/admin*** (see https://x.x.x.x/admin - ***https://x.x.x.x/admin***) and login with administrative credentials.

2. Access Work Centers>Network Access>Network Resources> to load Network Device menu and click 



3. Configure Name, Description, IP Address/Range as well as enable TACACS Authentication Settings option. Set Shared secret, then click Submit to save changes. If appropriate and applicable, assign Device Type and Location.

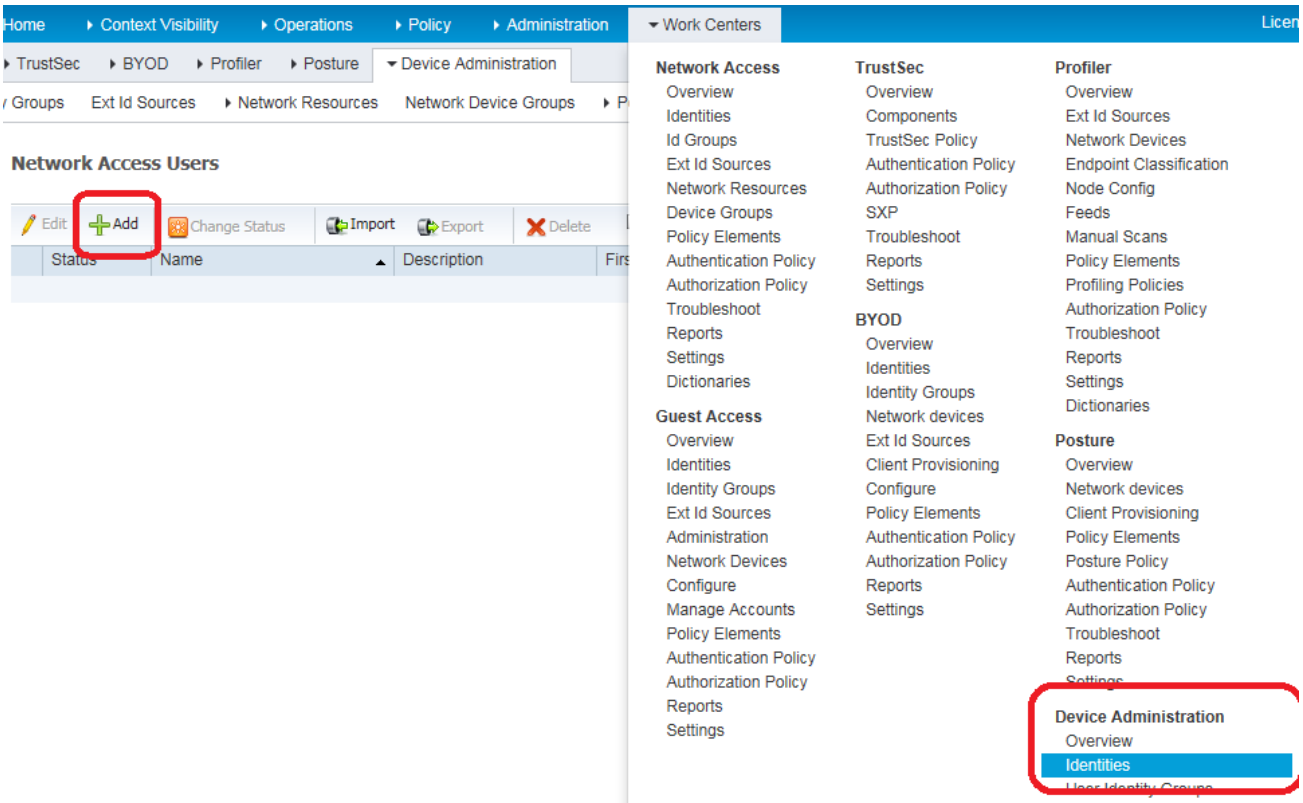


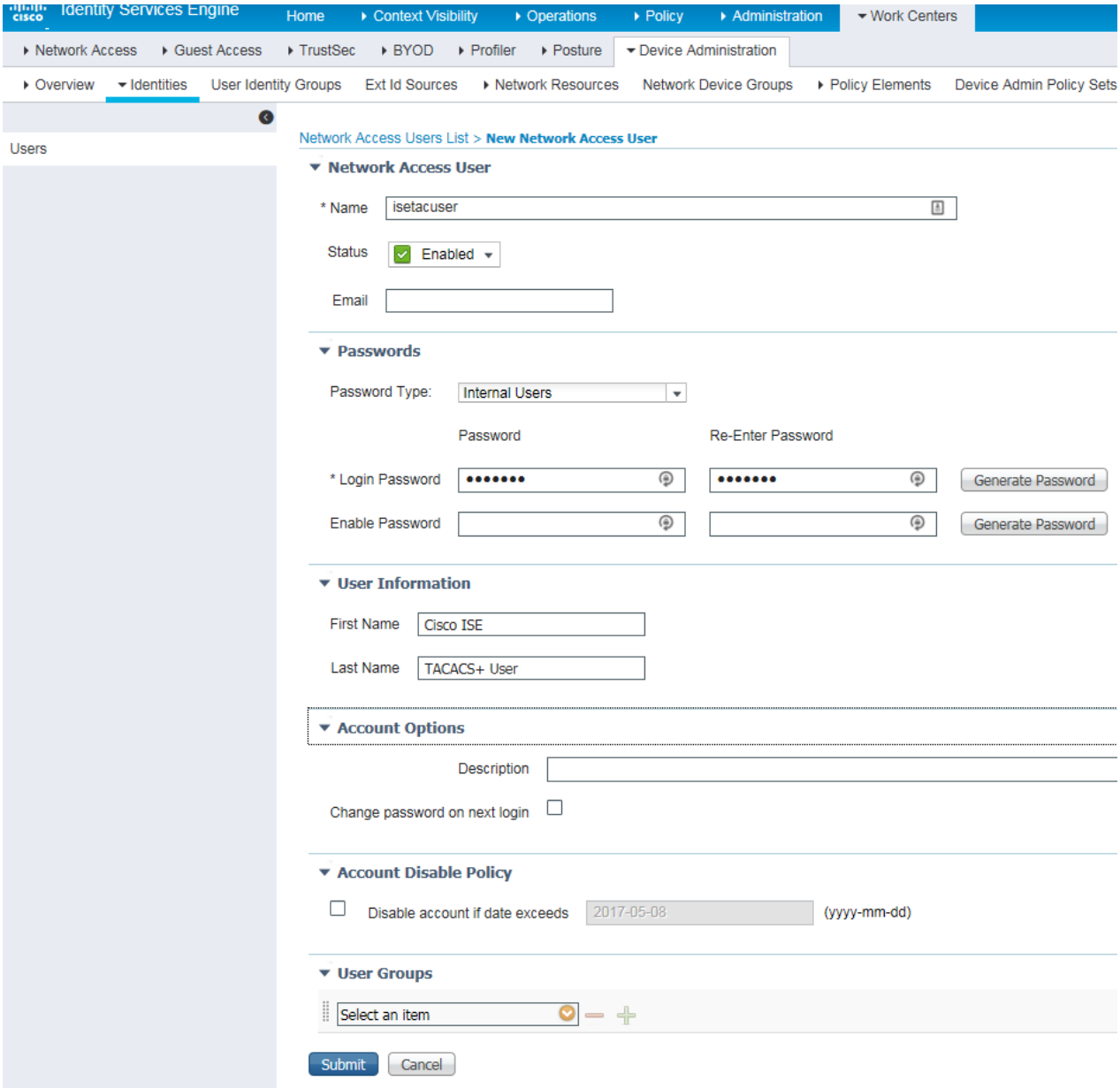
Step 2: Create/Edit User

Note: Skip this step in production environments where user accounts are already created, or there is a configured external identity source (AD/LDAP).

1. Access Work Centers>Device Administration>Identities> and click 

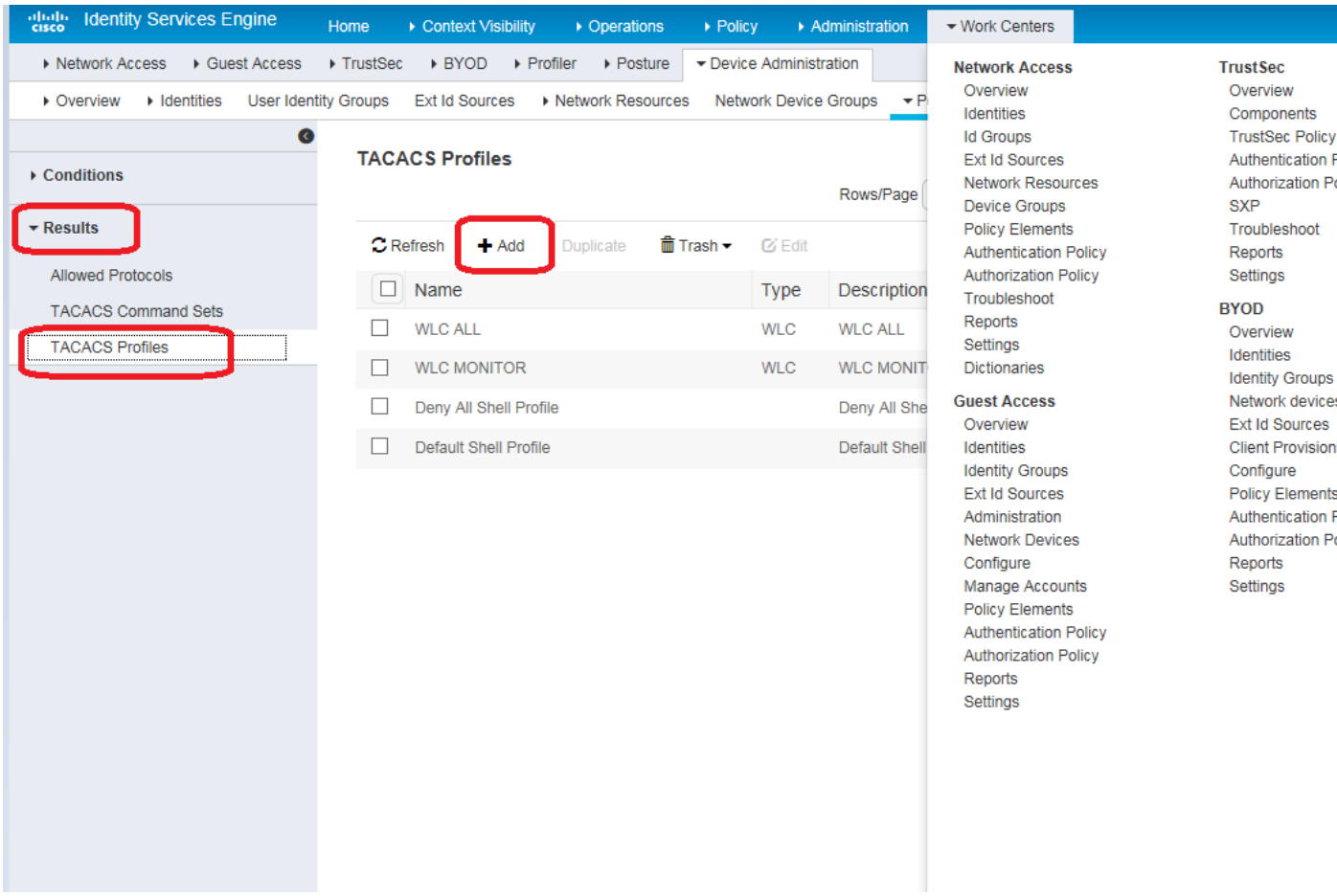
to add a user



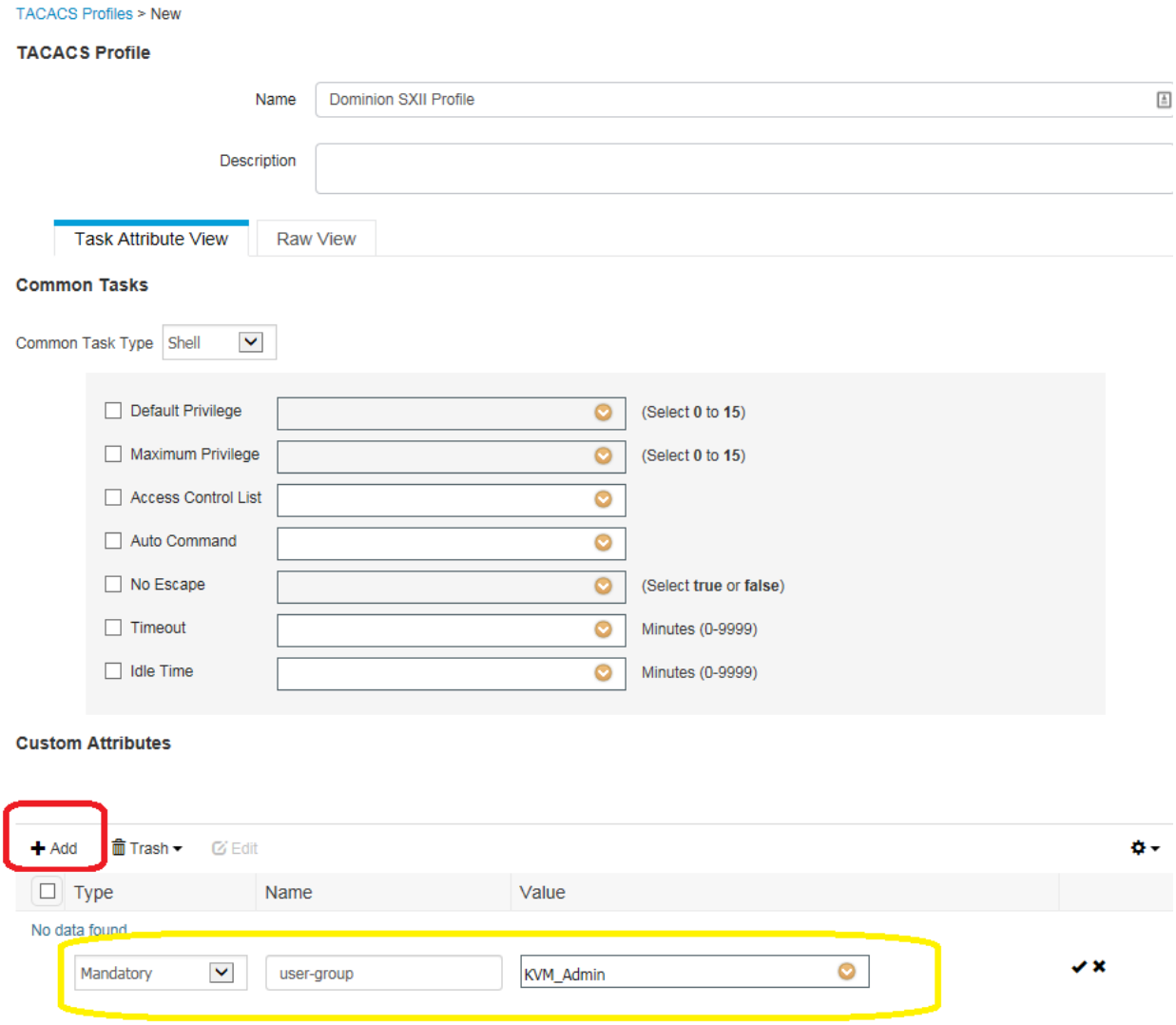


Step 3: Create TACACS Profile Policy Element:

1. Access Work Centers>Policy Elements>Results >TACACS Profiles and click + Add to add a profile.



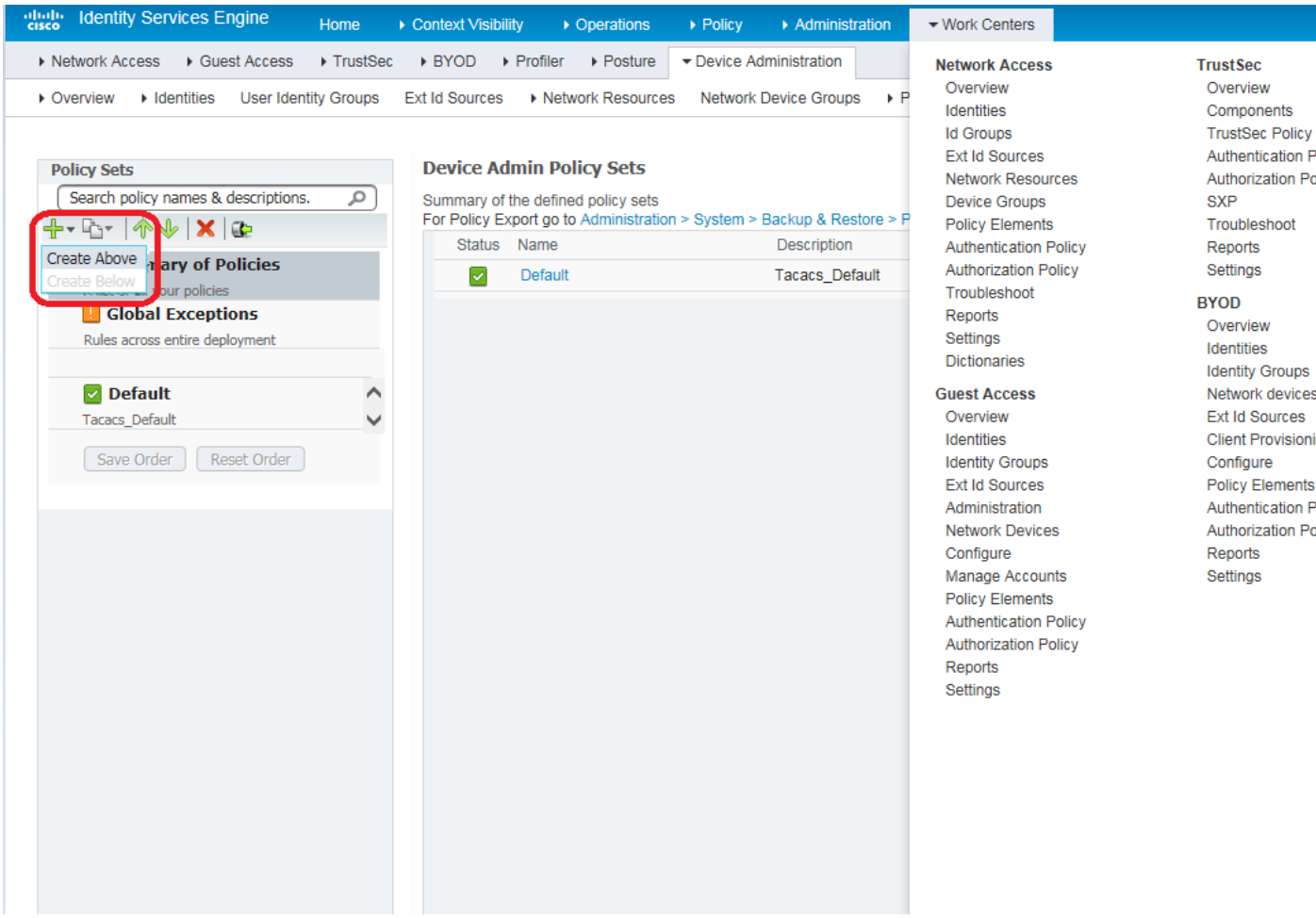
2. Configure Policy Name and click + Add under Custom Attributes section. From Type drop down, delect option Mandatory, Attribute Name as user-group and value KVM_Admin where KVM_Admin is the group name created locally on Dominion SXII (Case sensitive) then Click on ✔ to add attribute then select Submit to save changes.



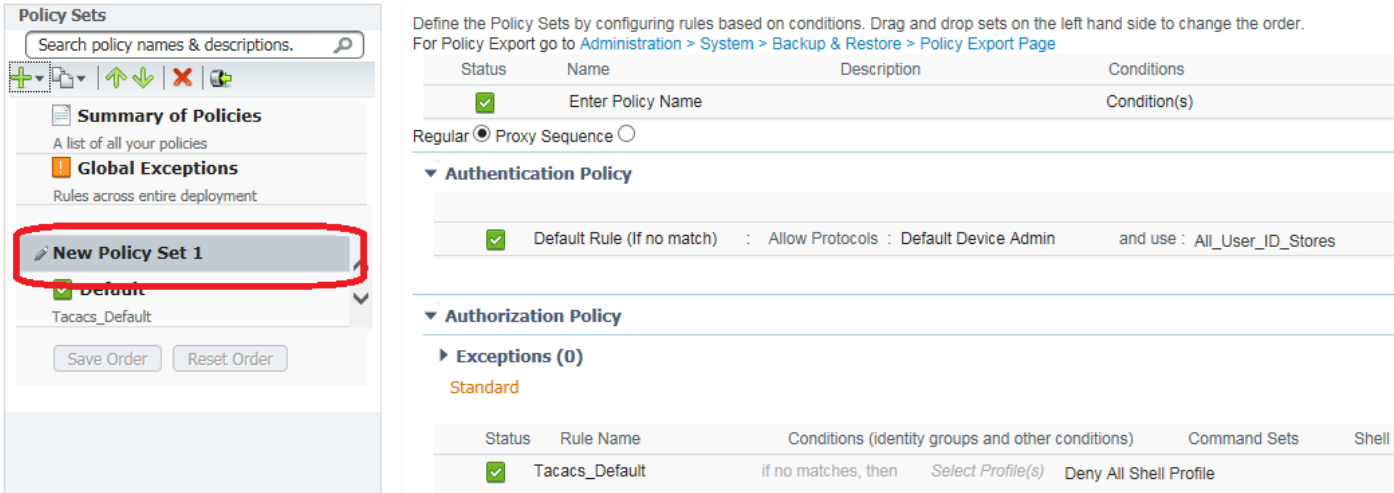
Step 4: Configure/Create Device Admin Policy Set

1. Go to Work Centers > Device Administration > Device Admin Policy Sets.

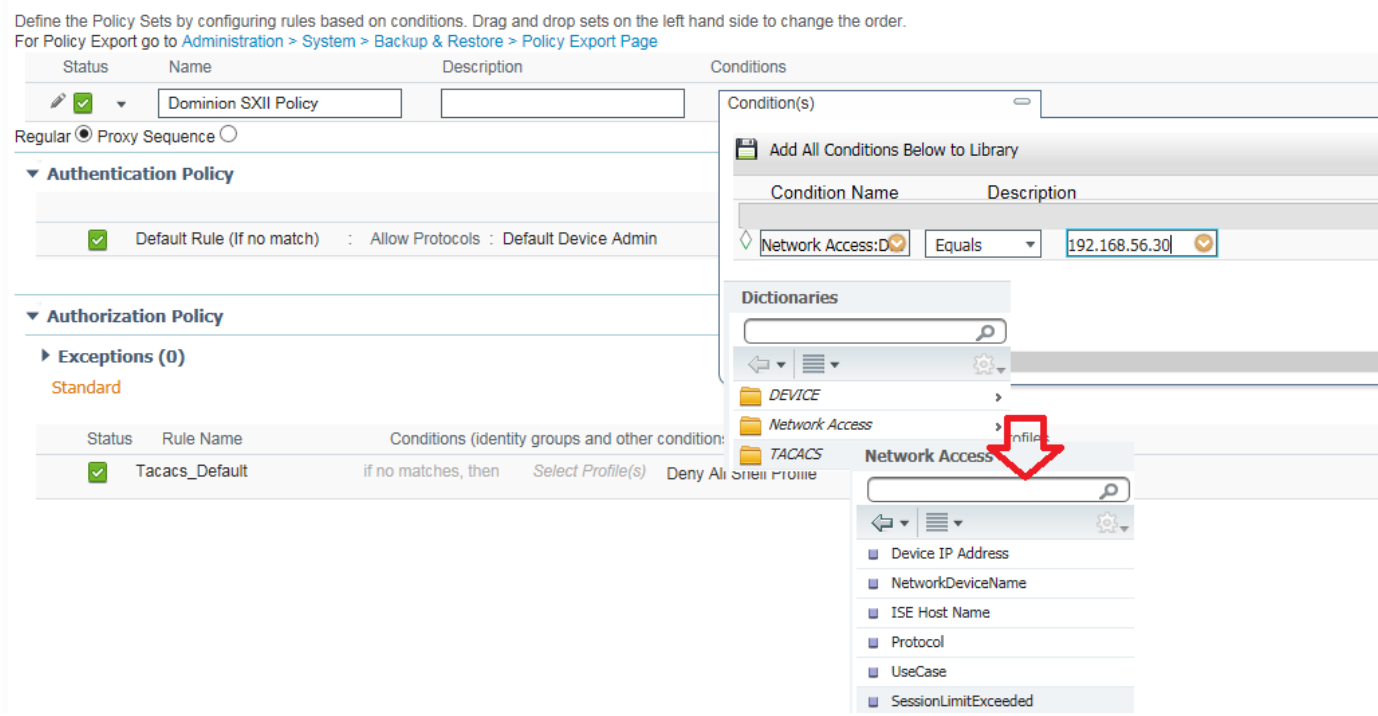
2. In the left pane, click  and Create Above to create a new policy set.



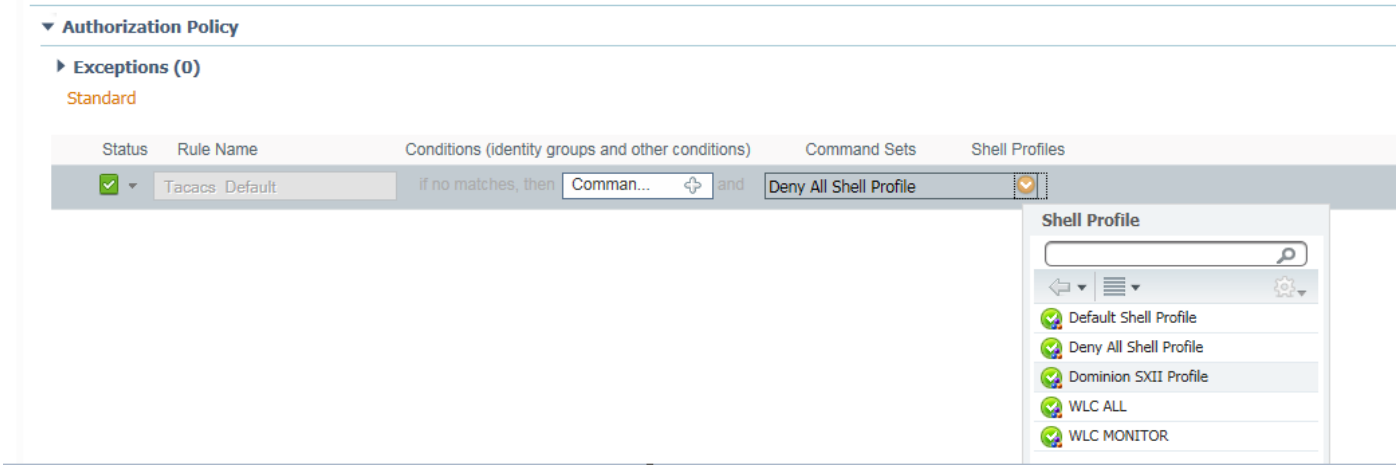
3. Above step will create New Policy Set 1



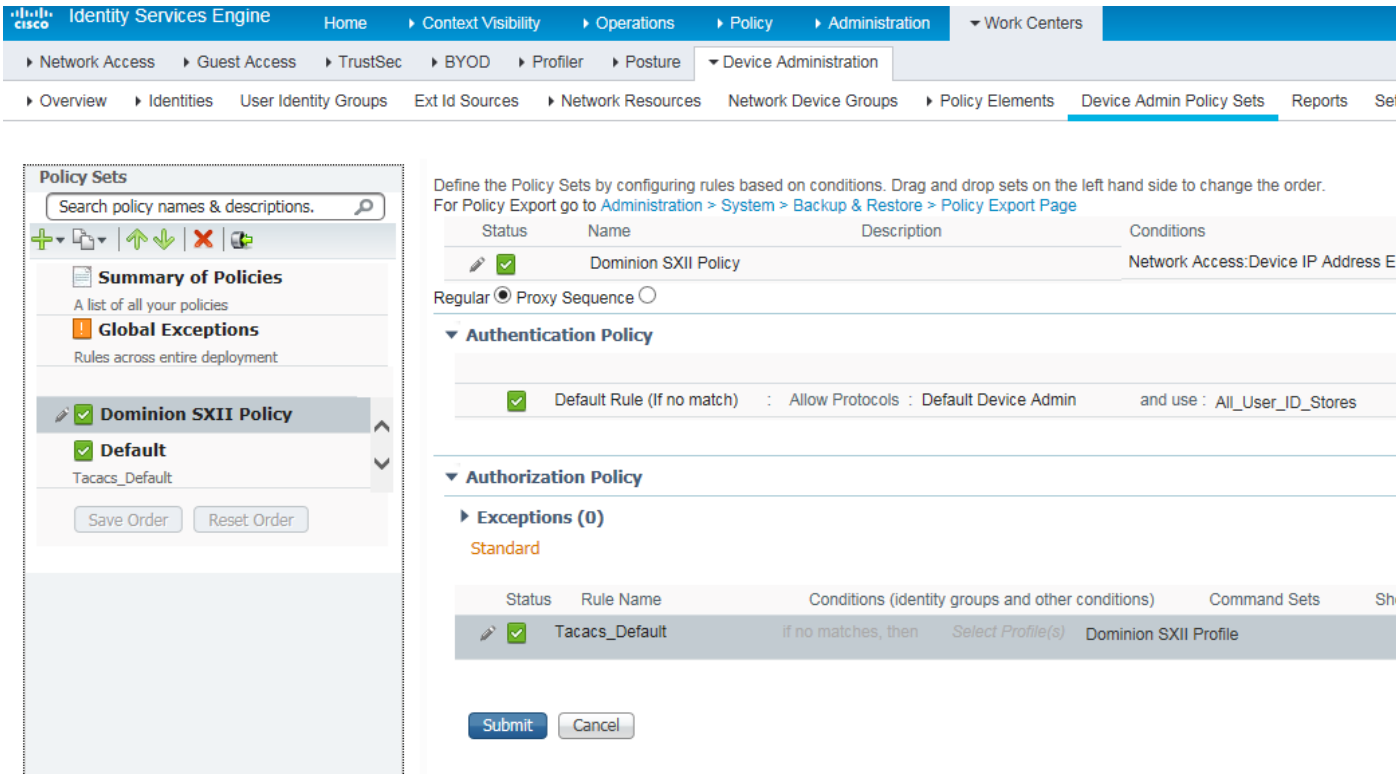
4. Click Edit and enter the Name, Description, and Condition (optional) and click Done. Authentication Policy is optional unless it is explicitly required for security guidelines and user store specific needs of your organization.



5. Create the required Authorization Policy. Click Edit and specify select drop down  under Command Sets and select profile created earlier in step 5 then click Done to save changes.

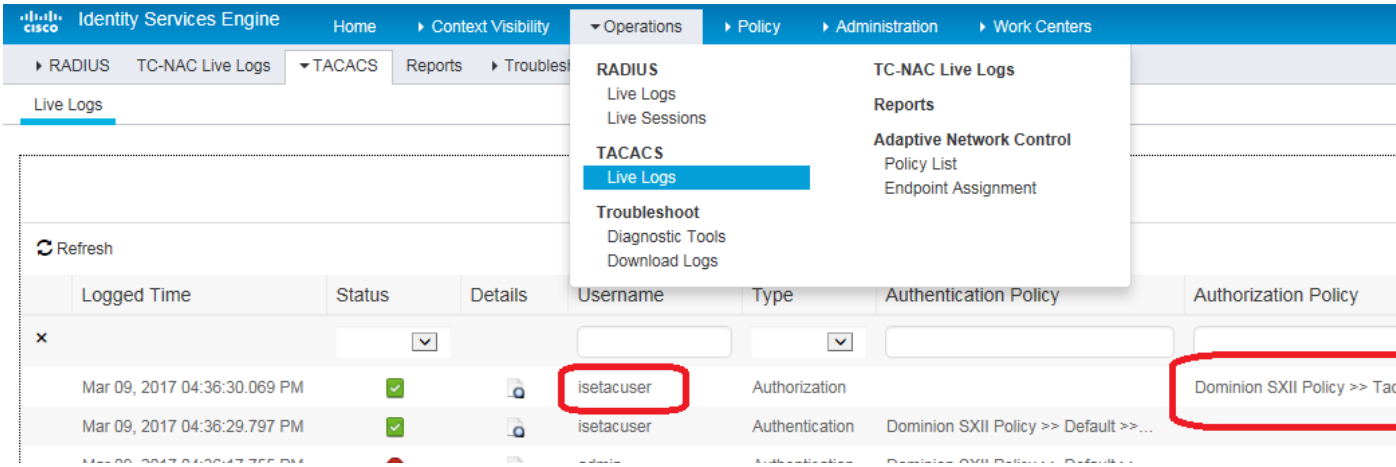


6. Click Submit to save changes. This concludes configuration on Cisco ISE pertaining to Dominion SXII TACACS authentication and authorization.

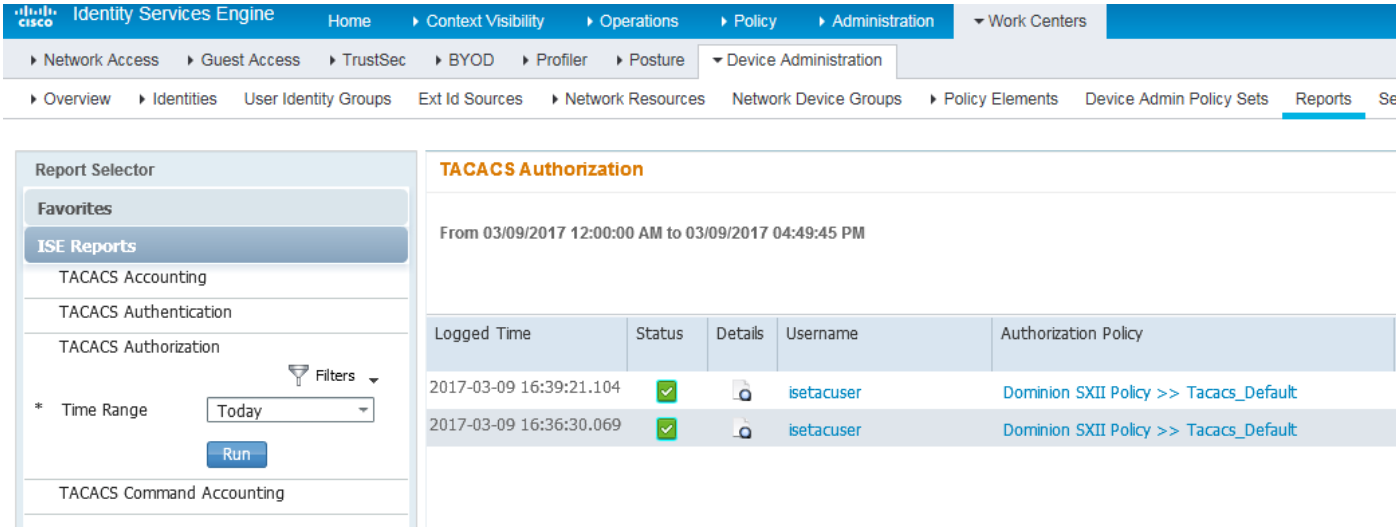


Troubleshooting Tips:

1. Verify from Live Logs under Operations> TACACS that correct Authorization Policy is being applied. Click Details icon to see more information.



2. Alternatively Choose Work Centers > Device Administration > Reports > ISE Reports



3. User authorization may fail on SX II if incorrect policy is applied. If this occurs, consider:
   - Moving policy higher up in the order (in case of multiple policy sets)
   - More appropriate conditions in policy coupled with device type and location when adding SX II as a network device in Cisco ISE

Cisco ACS 5.x for RADIUS Authentication

The Cisco Access Control Server (ACS) is another authentication solution supported by the SX II.

For the SX II to support RADIUS, both the SX II and the user information must be added into the RADIUS configuration.

If you are using a Cisco ACS 5.x server, after you have configured the SX II for RADIUS authentication, complete the following steps on the Cisco ACS 5.x server.

Note: The following steps include the Cisco menus and menu items used to access each page. Please refer to your Cisco documentation for the most up to date information on each step and more details on performing them.

- Add the SX II as a AAA Client (**Required**) - Network Resources > Network Device Group > Network Device and AAA Clients
- Add/edit users (**Required**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users
- Configure Default Network access to enable CHAP Protocol (**Optional**) - Policies > Access Services > Default Network Access
- Create authorization policy rules to control access (**Required**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
  - Dictionary Type: RADIUS-IETF
  - RADIUS Attribute: Filter-ID
  - Attribute Type: String
  - Attribute Value: Raritan:G{Serial_Admin} (where Serial_Admin is group name created locally on SX II). Case sensitive.
- Configure Session Conditions (Date and Time) (**Required**) - Policy Elements > Session Conditions > Date and Time
- Configure/create the Network Access Authorization Policy (**Required**) - Access Policies > Access Services > Default Network Access>Authorization

Configure Microsoft Network Policy Server for Dominion RADIUS Integration

The following steps show how to configure a Microsoft Network Policy Server as a RADIUS Server for integration with any Raritan Dominion product. These steps cover Windows 2012 server configurations.

Prerequisites:

Before you begin, ensure that Network Policy Access and Services as well as Active Directory are configured and available on Windows 2012 server.

This can be verified in the Server Manager snap-in Role Summary available under Administrative tools.

3 Step Process:

- Step 1 – Configure Raritan Dominion switch to use Windows 2012 NPS Radius server
- Step 2 – Add Raritan Dominion switch as Radius client on Windows 2012 NPS Radius server.
- Step 3 – Add Connection Request Policy on Windows 2012 NPS Radius server.

Step 1 – Configure Raritan Dominion switch to use Windows 2012 NPS Radius server

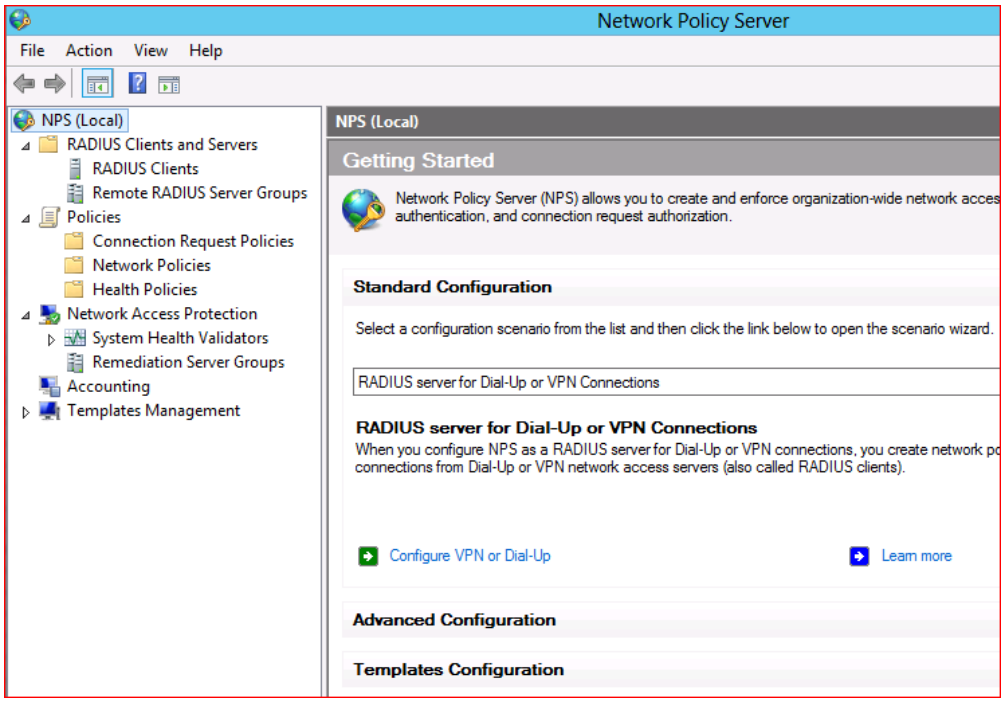
1. Login to Dominion switch and access Remote Authentication setting option and configure Radius server IP, port, secret and authentication type (CHAP/PAP) and save changes.
2. Create a user group locally on Raritan Dominion Switch with port and permission restrictions as desired.

Step 2 – Add Raritan Dominion switch as Radius client on Windows 2012 NPS Radius server.

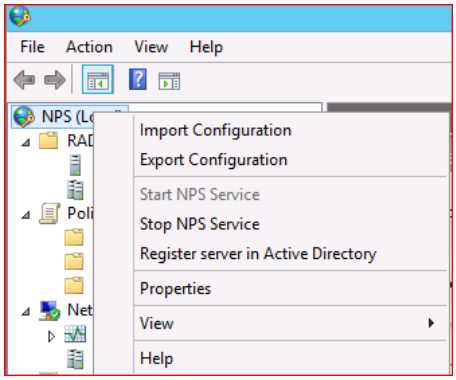
The Dominion switch is added as a client on Radius server as per Radius protocol requirements. Since Raritan Radius implementation uses Use Standard IETF Radius spec, select Radius Standard as Vendor Name.

Follow steps below in order to add Dominion as Radius client on Windows 2012 NPS Radius server.

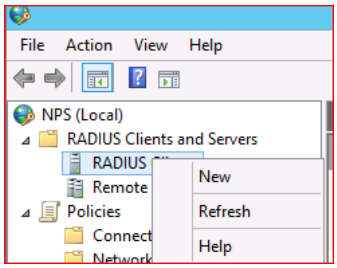
1. Launch Network Policy Server snap-in via Start>Administrative Tools>Network Policy Server.



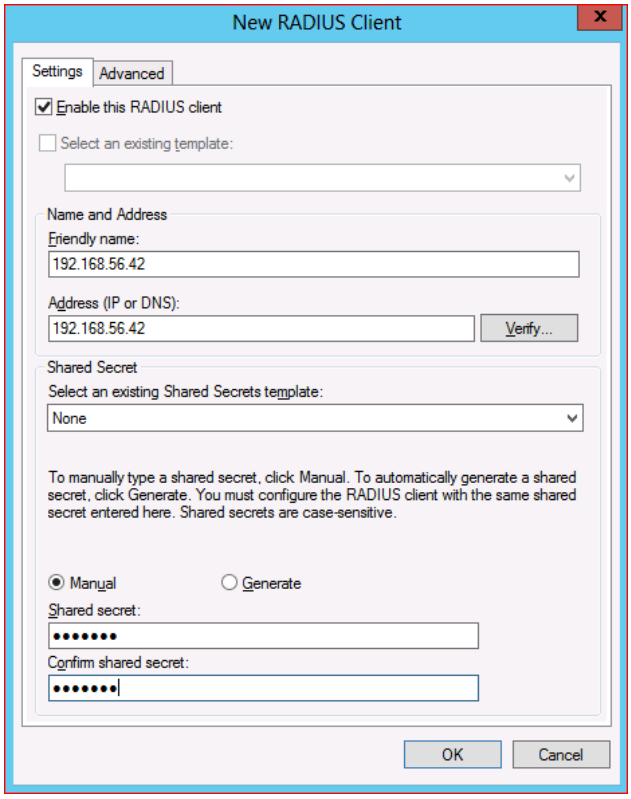
2. Right Click NPS (Local) server and select properties as show below. This step is included in order to verify Radius port number as below and confirm it Dominion switch Radius configuration port matches with this number.

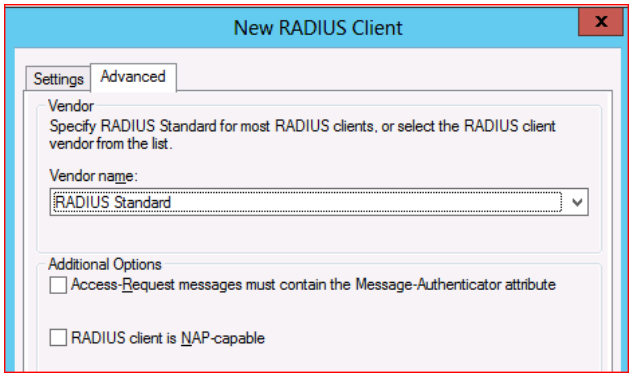


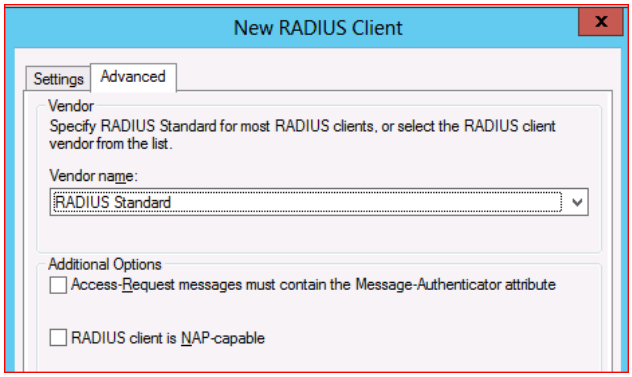
3. Right Click RADIUS Client and select New option as show below.



4. Configure Friendly name (for identification purpose), IP address of Radius client (Dominion switch IP address). Specify shared secret that will need to match with secret field of Radius configuration on dominion switch. Click on Advanced Tab to select RADIUS Vendor (Select Radius Standard)

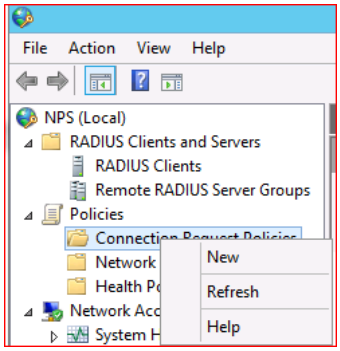




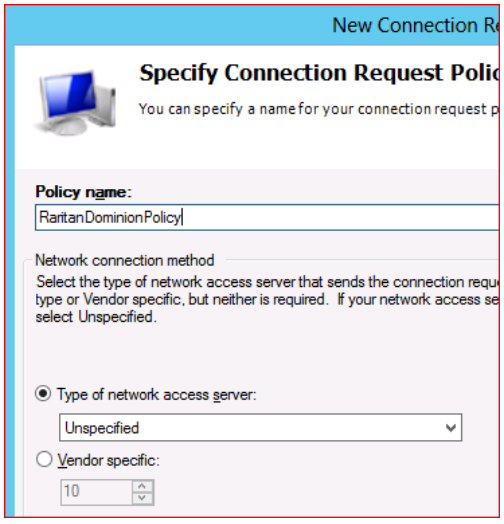


Step 3 – Add Connection Request Policy on Windows 2012 NPS Radius server.

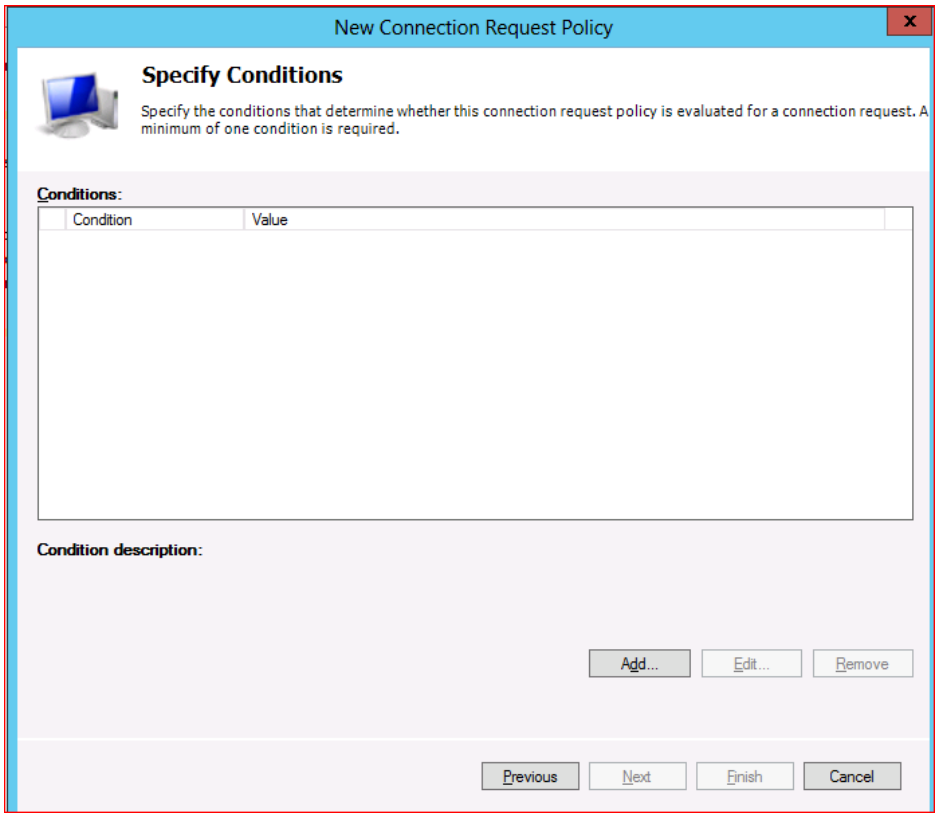
1. Expand Policies option, right click Connection Request Policies and select New to create policy.



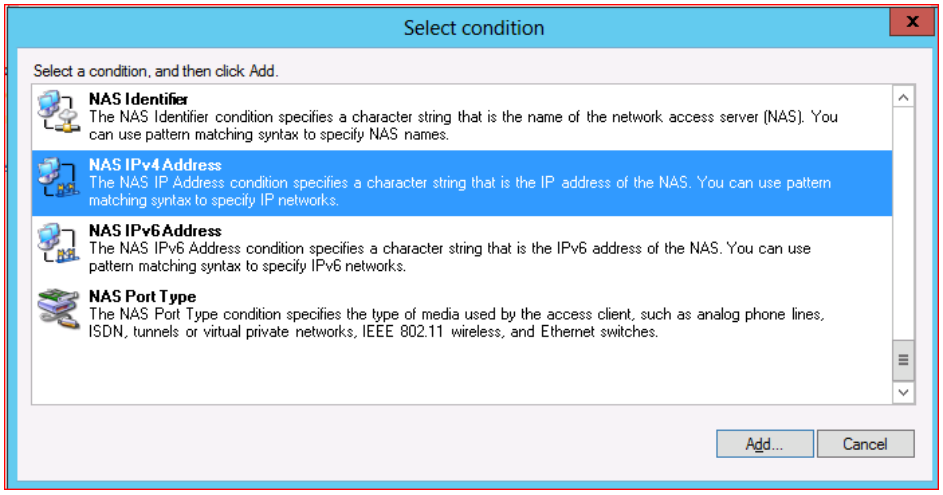
2. Specify Policy Name. Type of network access server value can be left default as Unspecified. Click Next.

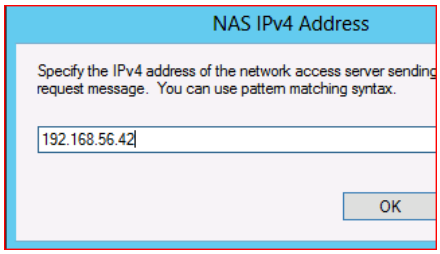


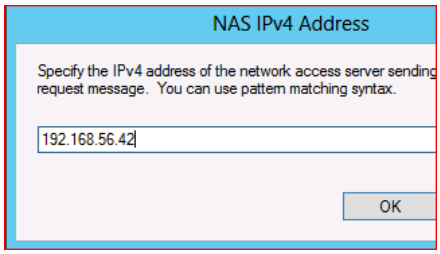
3. Depending on how many policies are configured on Radius server, how many users and groups as well as number of dominion switches in the environment, configure Specify conditions to match option in order to apply correct policy to a user request coming from Dominion switch into Radius server. Click on Add button to select list of condition before proceeding to next step.

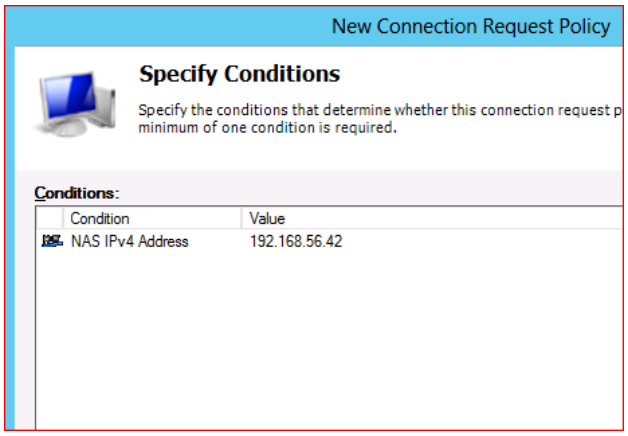


4. NAS IPv4 Address option can select and click Add to specify Dominion switch IP address.

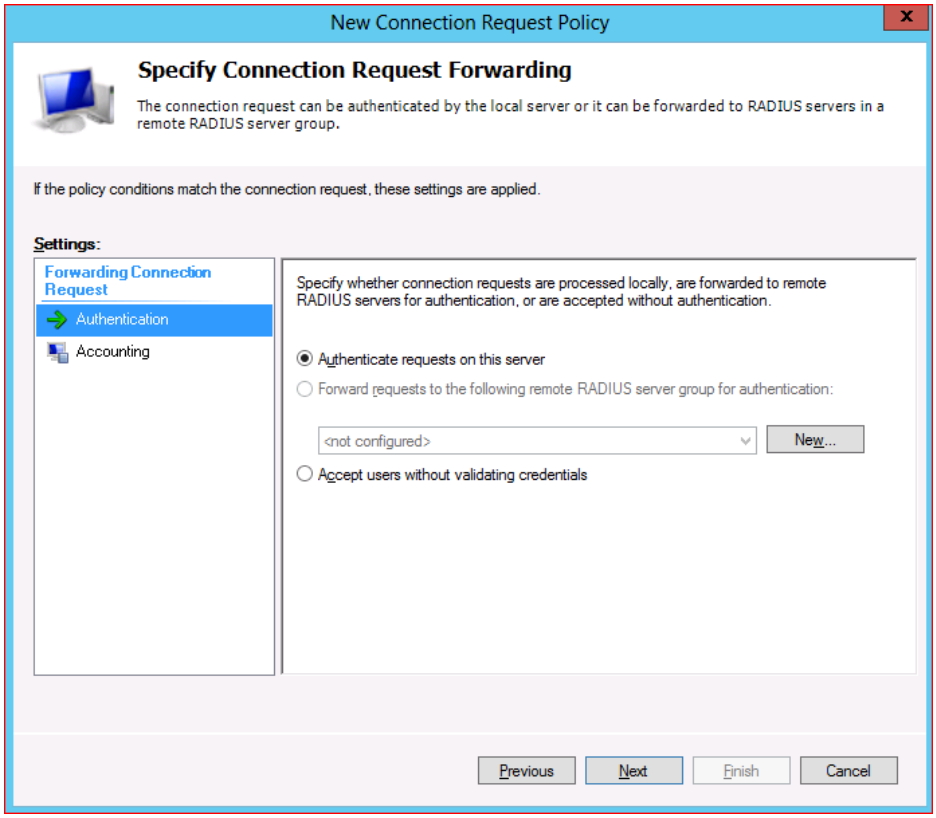




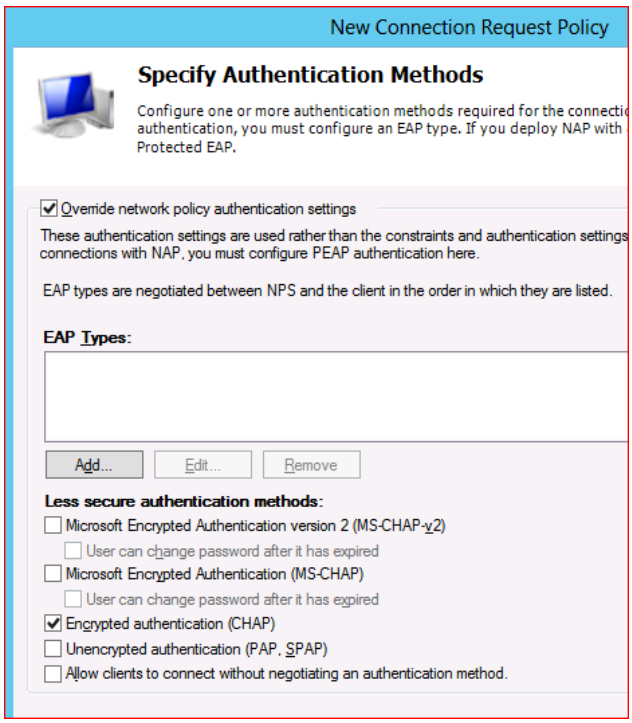




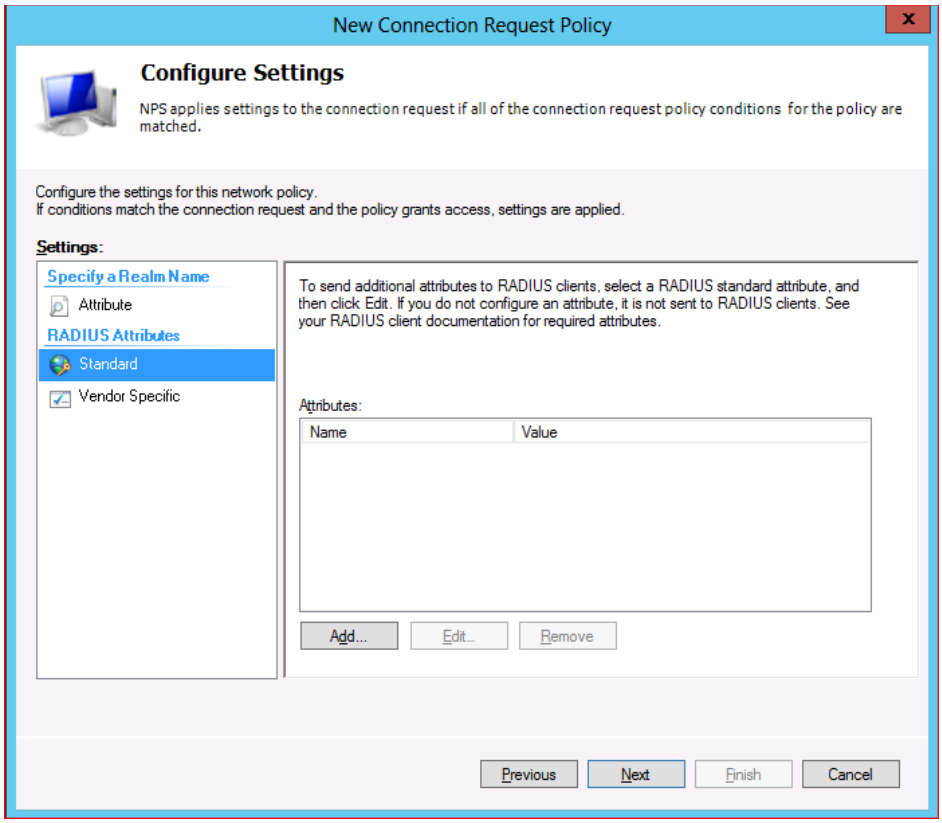
5. Click Next to specify Connection Request Forwarding option. Select appropriate option based on your environment. If you have local NPS server, select Authenticate requests on this server radius button (default) and click next to proceed further.

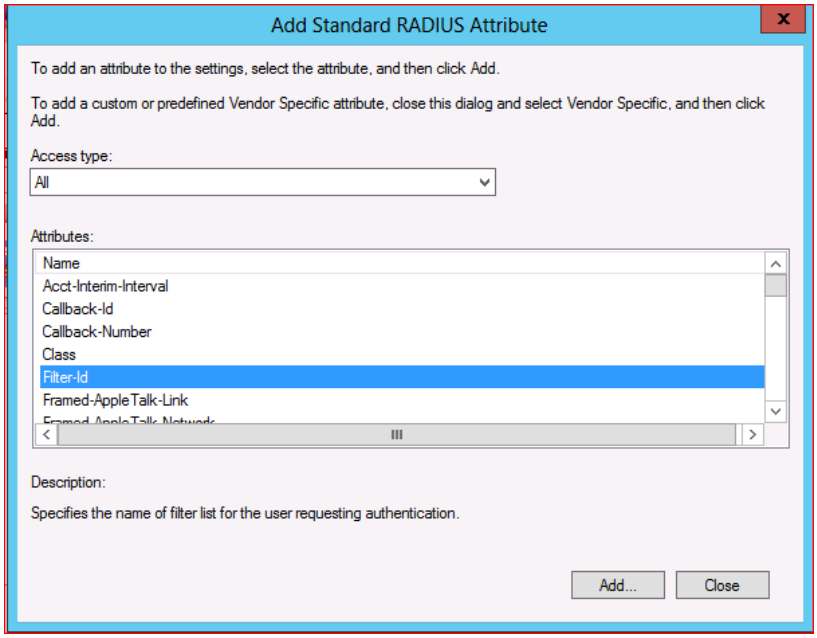


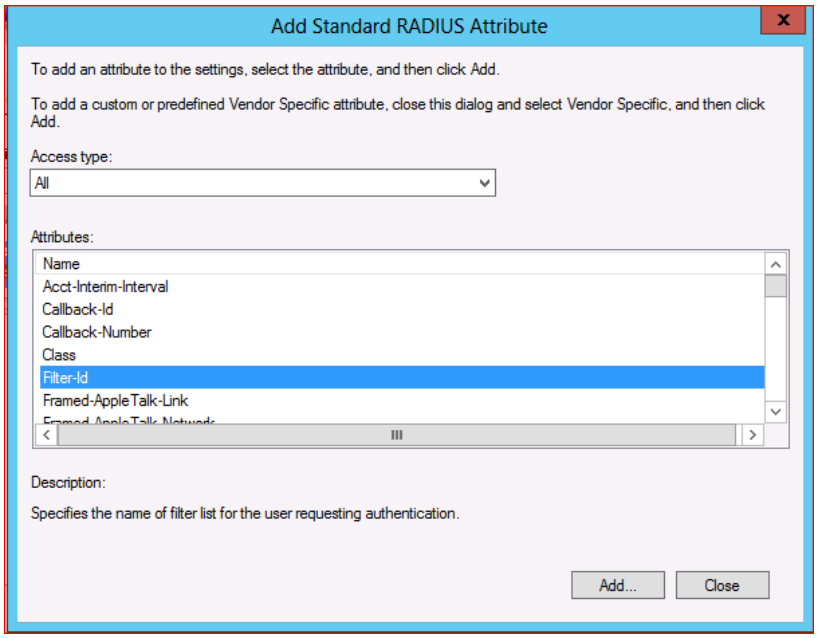
6. On Authentication Method configuration menu, enable Override network policy authentication settings option and select CHAP/PAP as applicable to match with Dominion RADIUS configuration option. Click next to proceed further.



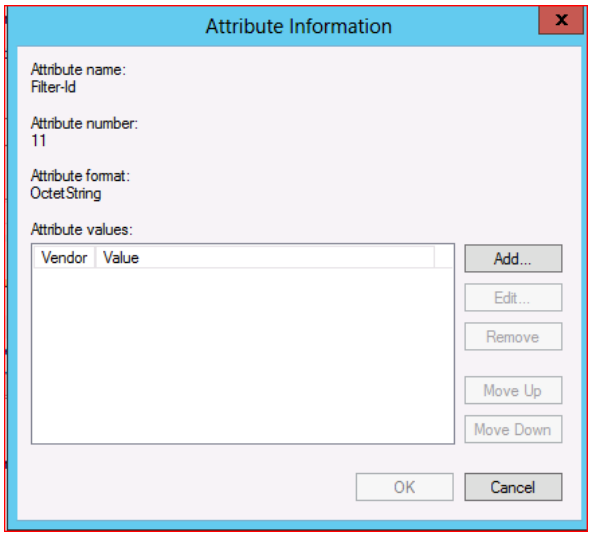
7. Select Standard under RADIUS Attributes located in settings section on next screen show below and click on Add button to see list of available attributes. As documented in Dominion switch user guide, Raritan uses Filter-Id attribute and its value for authorization. Select Filter-Id attribute from the list and click on Add.

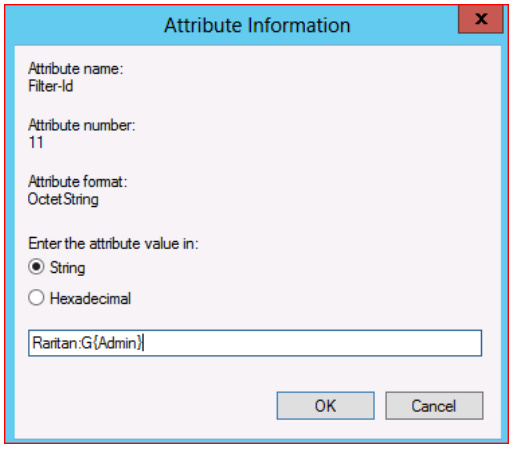


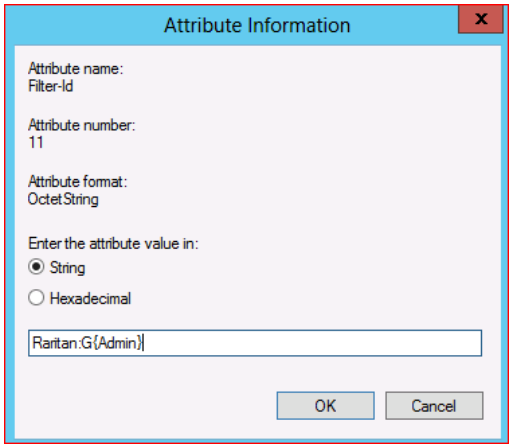


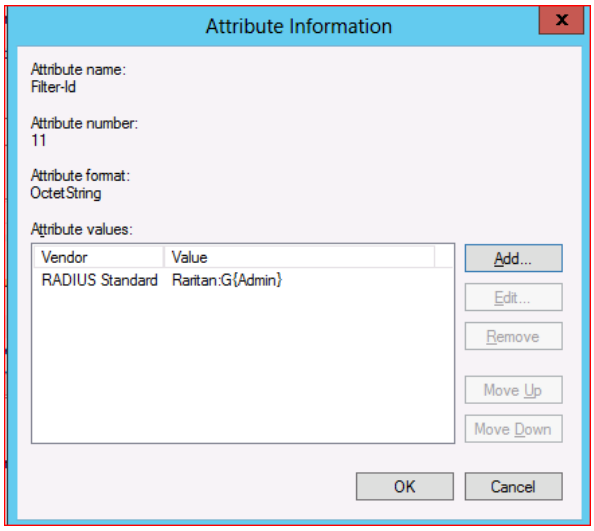


8. On Attribute Information dialogue box, click Add and configure value as string as show below. In example below value Raritan:G{Admin} is used where Admin is the group name that matches with local group (case sensitive) on Dominion switch. For configuration test purpose use of default Admin group in value is best recommended. Click OK on all dialogue boxes to close and come back to main screen.

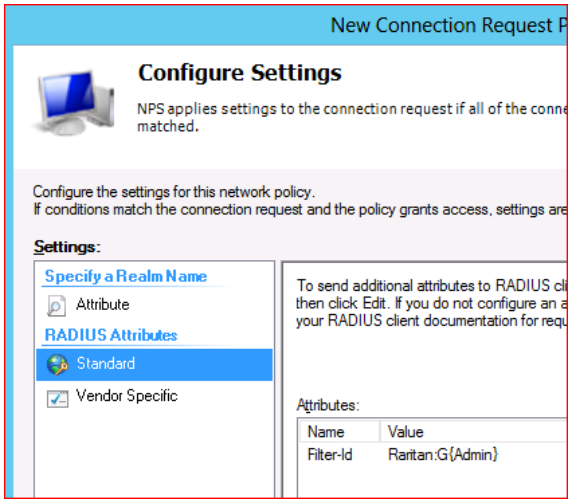


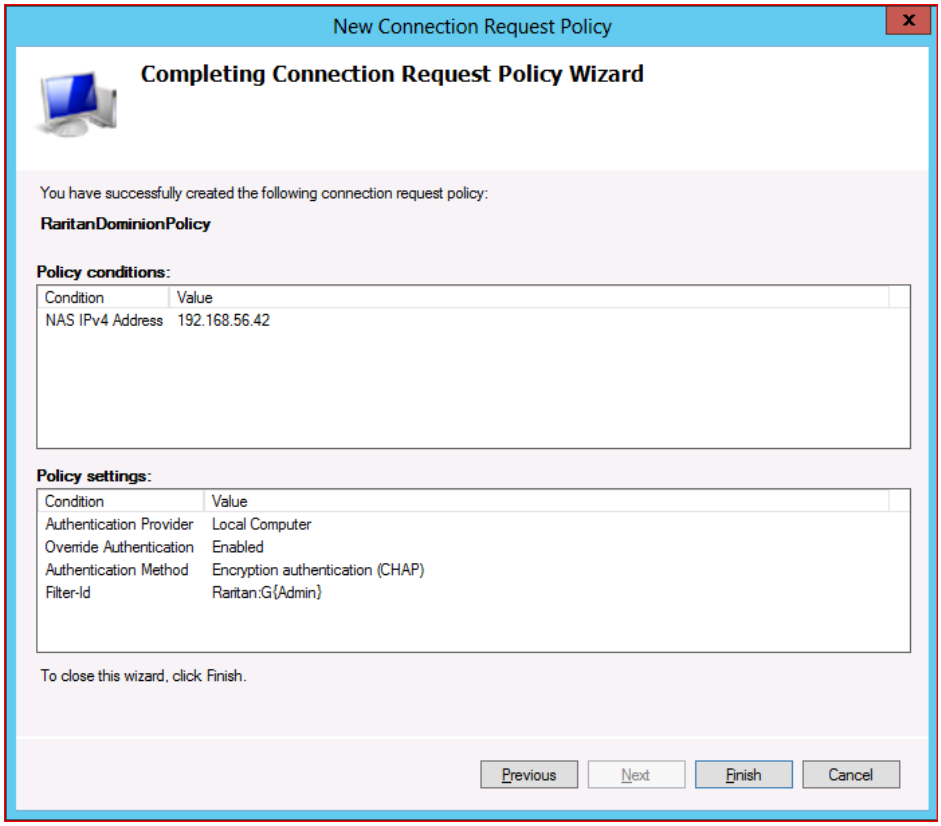


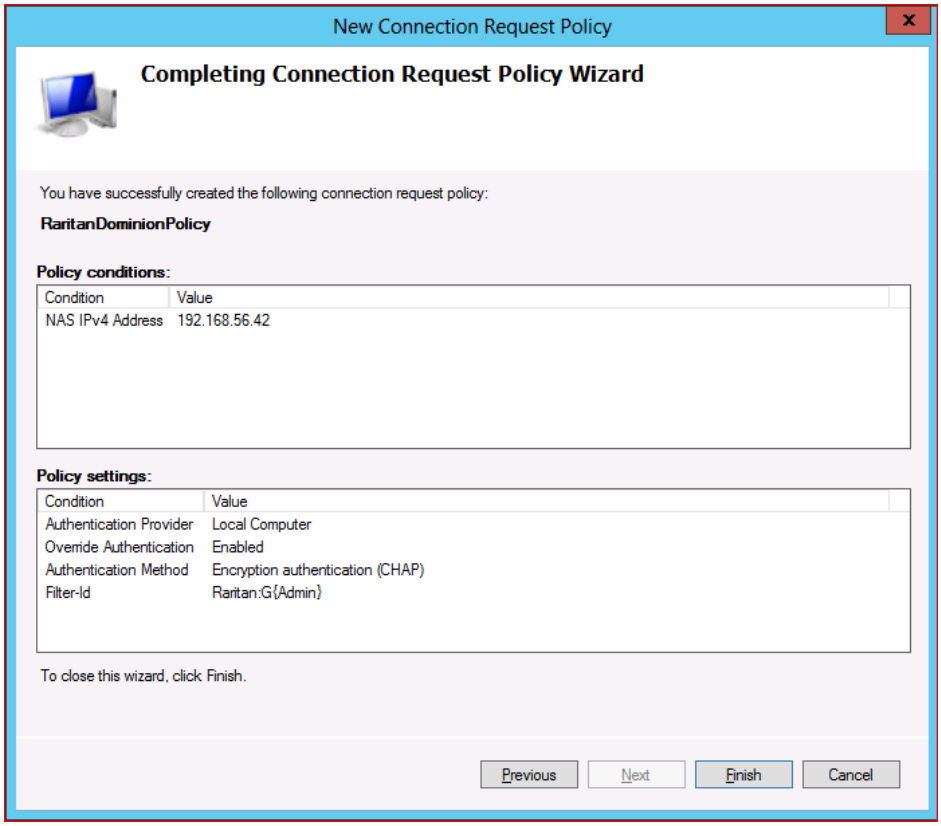

Attribute Information
Attribute name:
Filter-Id
Attribute number:
11
Attribute format:
Octet String
Enter the attribute value in:
String
Hexadecimal
Raritan:G{Admin}
OK
Cancel


Attribute Information
Attribute name:
Filter-Id
Attribute number:
11
Attribute format:
Octet String
Attribute values:
Vendor
Value
RADIUS Standard
Raritan:G{Admin}
Add...
Edit...
Remove
Move Up
Move Down
OK
Cancel

9. Click Next to view summary and Finish to complete configuration.

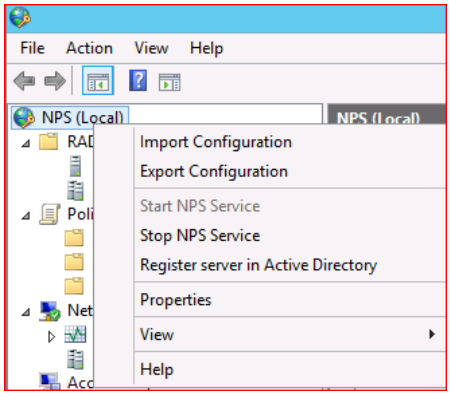


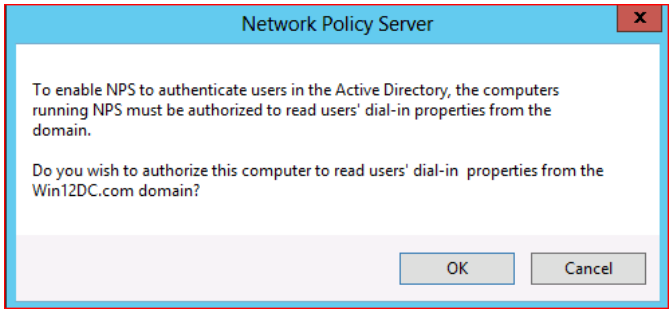


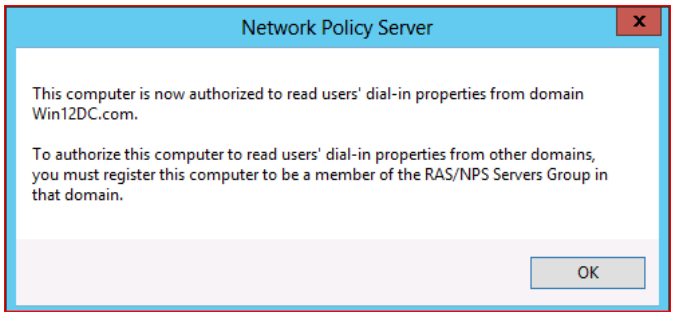

New Connection Request Policy
Completing Connection Request Policy Wizard
You have successfully created the following connection request policy:
RaritanDominionPolicy
Policy conditions:
Condition
Value
NAS IPv4 Address
192.168.56.42
Policy settings:
Condition
Value
Authentication Provider
Local Computer
Override Authentication
Enabled
Authentication Method
Encryption authentication (CHAP)
Filter-Id
Raritan:G{Admin}
To close this wizard, click Finish.
Previous
Next
Finish
Cancel

Additional Notes:

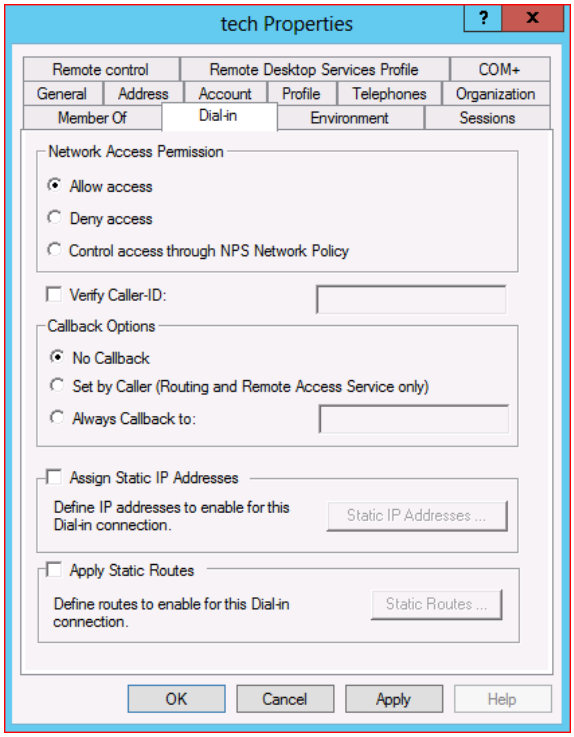
1. If this is the first time NPS/RADIUS server is being configured and user accounts are located on Active Directory, it will be required to Register NPS/RADIUS Server in Active Directory so that it can look up users in AD for password validation and return attribute values pairs back to Dominion switch.



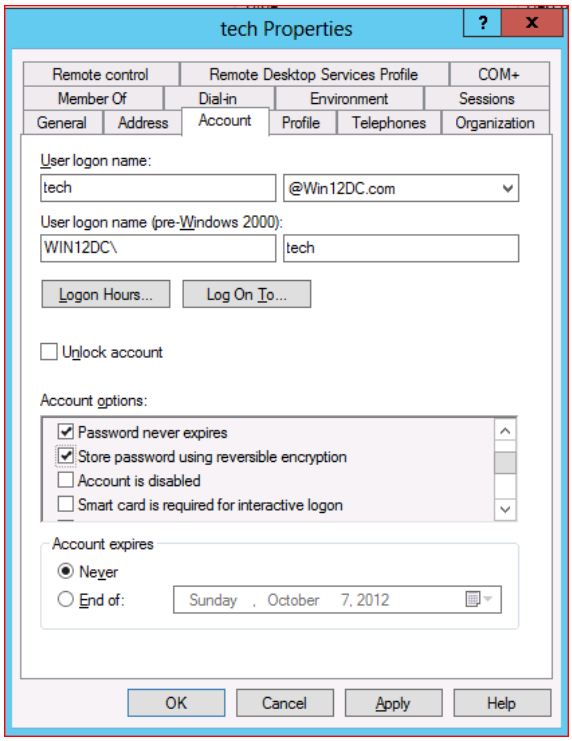




2. Ensure user on Active Directory has Dial-in Permission set to Allow access option.



3. When using CHAP, ensure that Store password using reversible encryption is enabled. User password should be reset if it is being enabled after user password is set.



RADIUS Communication Exchange Specifications

The SX II sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log in	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the SX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2)	The encrypted password.
Accounting-Request(4)	

Attribute	Data
Acct-Status (40)	Start(1) - Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the SX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Log out	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the SX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

RADIUS Using RSA SecurID Hardware Tokens

SX II supports RSA SecurID Hardware Tokens used with a RADIUS server for two factor authentication

Users will specify their RADIUS password followed by the token ID without a delimiter between.

For example:

- password = apple
- token = 1234
- User enters: apple1234

Or, configure the RADIUS server to use only hardware token and no passwords. Users will specify the token ID only.

Returning User Group Information from Active Directory Server

The SX II supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the SX II. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard SX II policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, the SX II still supports this configuration and you do not need to perform the following operations. See Updating the LDAP Schema for information about updating the AD LDAP/LDAPS schema.

To enable your AD server on SX II:

1. In SX II, create special groups and assign proper permissions and privileges to these groups.

   For example, create groups such as AD_Admin and AD_Operator.
2. On your Active Directory server, create new groups with the same group names as in the previous step.
3. On your AD server, assign the SX II users to the groups created in step 2.
4. From the SX II, enable and configure your AD server properly. See Implementing LDAP/LDAPS Remote Authentication.

Important Notes

- Group Name is case sensitive.
- The SX II provides the following default groups that cannot be changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match the SX II group configuration, the SX II automatically assigns the group of <Unknown> to users who authenticate successfully.
- If you use a dialback number, you must enter the following case-sensitive string: msRADIUSCallbackNumber in field "Dialback Query String".
- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the SX II determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows: Raritan:G{*GROUP_NAME*} where *GROUP_NAME* is a string denoting the name of the group to which the user belongs.

```
Raritan:G{GROUP_NAME}
```

where GROUP_NAME is a string denoting the name of the group to which the user belongs.

Appendix D FAQs

Dominion SX II Overview

Dominion SX II Overview	
What is the Dominion SX II?	The Dominion SX II is Raritan's next-generation Serial Console Server that provides IP access and control of serial devices, anytime, anywhere. The new SX II is the most powerful, secure, reliable, easy-to-use and manageable serial-over-IP console server on the market. SX II provides convenient and productive access to networking devices, servers, PDUs, telecommunications and other serial devices.
How is SX II different from the current SX?	The SX II is the next-generation version of the current SX. SX II has an entirely new hardware and software design that is substantially more powerful and capable than the current SX. The SX II provides virtually all of the features of the SX, plus exciting new capabilities. Unlike the current SX, all SX models come with dual power supplies, dual LAN connections and multiple local connection options. The SX II comes in 4, 8, 16, 32 and 48 models, available with and without an internal telephone modem. Many of the management features are the same as those on the Dominion KX III.
What are the SX II's new features?	New features include: Gigabit Ethernet, IPv6 networking, direct connection to Cisco devices with no rollover cables, FIPS 140-2 encryption, automatic configuration via USB stick or TFTP, 3G/4G cellular modem support, up to 8 gigabytes of flash space, multiple at the rack access options and Dominion compatible user interfaces and management.
Does the SX II have all of the current SX's features?	Virtually all of the current SX's features are included in the SX II. Several features (firmware update, fixed user groups have been replaced by more powerful Dominion style features and a few infrequently used features have been removed.
What is the pricing for SX II?	While you might expect a significant price increase for the SX II, it is priced similarly to the current SX. The exact price difference varies model by model. Some SX II models are even less expensive than the current SX models!
What are the end-of-life plans (lifecycle) for the current SX?	The Dominion SX II will replace the current Dominion SX. In the 4th quarter of 2015, Raritan will announce the end-of-sales for the current SX models, with opportunities for last-time-buys for a few months. Raritan will continue software

Dominion SX II Overview	
	support for the current SX for two years from the end-of-sales announcement date; after that there will be no more firmware releases for the current SX. CommandCenter support will likely continue past the end-of-support date. Existing hardware warrantees will be honored.
Is there a trade-in program for the SX II?	Yes, you will have the opportunity to trade in the current SX and/or competitor serial console servers.
Dominion SX II Hardware Platform	

What are some of the hardware improvements?	There are many: more powerful CPU, memory and flash space, dual power supplies (AC & DC), dual gigabit LAN ports, port status LED's, 4 USB ports, autosensing DTE/DCE ports, USB laptop access, DVI/USB access, and modem option for all models.
How does the SX II's performance compared to the current SX?	The SX II hardware platform is substantially more powerful with a 1GHz CPU, an 8-fold increase RAM, and up to 8 Gb of flash space. SX II supports up to 10 sessions per port and up to 200 total serial sessions. Port configuration is 15 to 23 times faster, with order of magnitude improvements in simultaneous connections, connection speed and serial processing.
What type of network connections does the SX II have?	The SX II has two Gigabit Ethernet LAN ports that are auto-sensing to support 10/100/1000 Megabit connections. These LAN ports can be configured for (1) single LAN connection, or (2) dual LAN connections; the latter with (a) failover or (b) simultaneous operation. Both IPv4 and IPv6 are supported.
Are all SX II models 1U? Even the 48 port model?	Yes, all models are 1U and include a rackmount kit. Like, the current SX, the 48 port model has 48 ports on the back panel; to make room for this, the dual power outlets are on the front panel.
How much flash space is available for logs?	More than you could ever possibly use!! Four and eight port SX II's have 2 Gigabits of flash space. The other models have 8 Gigabits of flash space.
Does the SX II support remote power control?	Yes, the SX II supports remote power control for serial devices via connection to Raritan PX intelligent rack PDU's.
What is the pin definition for the SX II's local admin port?	The SX II local admin port is an RJ-45 port with the following DTE pinout (Pin/ Signal): 1/RTS, 3/TXD, 4/GND, 5/GND, 6/RXD, 8/CTS. You can connect to a DB9 port on a laptop using the Raritan ASCSDB9F RJ-45(female) to DB9 (female) adapter with a Cat5 cable.
Does Dominion SX include a 19" rack mount kit?	Yes. Dominion SX II comes standard with a complete ready-to-install 19" rack mount kit.

Serial-over-IP Sessions and Access

Serial-over-IP Sessions and Access	
What types of serial access are available?	The SX II has the widest variety of serial access. This includes: SSH, Telnet and web browser serial connections. Web browser access is available via the Raritan Serial Client and through Raritan CommandCenter. Convenient Direct Port Access (DPA) methods are available. At-the-rack access is available via serial cable, USB and via a KVM console. Emergency modem access is available via optional internal modem or external 3G/4G cellular modem.
What is Direct Port Access ?	Direct Port Access provides direct and convenient access to a specific serial device connected to the SX II. Multiple Direct Port Access (DPA) methods are available via SSH, Telnet and HTTP/URL.
Does the SX II support TELNET?	TELNET is supported, but is disabled by default for security reasons as TELNET does not support encrypted sessions. We recommend that SSH is used instead of TELNET.
What about emergency access via modem?	There are two types of modem access supported. First, an internal telephone modem is optional for each SX II model (DSX2-...M models). Second, for 3G/4G cellular modem access, you can connect one of the supported Sierra Wireless modems to the SX II's USB port and access the SX II via the modem's IP address.
How can I secure the Sierra Wireless modem?	You can use the SX II's Firewall feature to create Linux-style "iptable" rules to secure the connection to the wireless modem. In addition the modem itself has a firewall capability.
How can I access the SX II when I am in the data center?	The Dominion SX II provides multiple types of at-the-rack access. To connect to a laptop or PC you can connect to its RJ45 serial port or USB mini-B port. You can connect a crash cart or rackmount keyboard tray to the SX II's DVI and USB KVM ports. To access the SX II's web-based user interface, connect a crossover Ethernet cable to the SX II's LAN port.
How can I get consolidated access to the local ports of multiple SX II's?	There are two ways to do this. First you can connect the serial admin ports of multiple SX II's to another SX II with straight Cat5 cables. Second you can connect the DVI/USB local ports of the SX II's to a KVM switch like the Dominion KX III. This can give you access to multiple SX II's in and around the

Serial-over-IP Sessions and Access	
	data center.
What baud rates are supported?	Multiple baud rates are supported: 1200, 1800, 2400, 4800, 9600 (default), 19200, 38400, 57600, 115200, and 230400 bits per second. Can set this on a per port basis from the Port Configuration page or CLI.
What code-sets does the terminal emulator in Dominion SX II support?	Dominion SX release 3.0 or higher supports VT100/VT220/VT320 and ANSI with the following code-sets: default, US-ASCII, ISO-8859-1, ISO-8859-15, UTF-8, Shift-JIS, EUC-JP, EUC-CN, and EUC-KR.
How many serial devices can be simultaneously accessed through a given SX II?	A group of users can simultaneously access all the serial devices connected to a SX II. For example, with a 48 port SX II, users can simultaneously connect to and access all 48 serial devices connected to it!
How many users can simultaneously access a single serial device connected to a SX II	Up to ten users can access a single serial device at the same time, up to a limit of two hundred simultaneous accesses per SX II. For example, on a 32 port SX II, six users could each simultaneous access each of the 32 serial devices connected to it for a total of 192 user sessions. This would not be a typical user scenario, but illustrates the powerful serial processing capacity of the SX II.
Is the Dominion SX unit SUN® "break-safe"	All Dominion SX units are SUN "break-safe" for use with SUN Solaris.
Connecting to Serial Devices	

Connecting to Serial Devices	
What type of devices can the SX II connect to?	The SX II can connect to a wide variety of serial devices including network routers, Ethernet switches, firewalls, UNIX/LINUX servers, Windows Servers, virtual hosts, rack PDU's, UPS systems and telecom/wireless gear. The SX II connects via Cat5 cable to these device's RJ-45, DB9 or DB25 serial console ports.
Are rollover cables required?	No. SX II serial connections are auto-sensing, so that they can connect to both DTE (data terminal equipment) and DCE (data communications equipment) console ports without rollover cables. The SX II can connect to Cisco and other compatible devices with RJ-45 console ports without rollover cables.
What is DTE/DCE and why is it important?	An RS-232 serial port is either DTE or DCE. DTE ports are typically used on a computer or terminal, i.e. male DB9 COM port. And DCE is used on a modem, CSU/DSU, multiplexer or peripheral. A DTE port is typically cabled to a DCE port. Connections between like ports must be connected by a specific rollover cable. Since SX II is auto-sensing, it can connect to either DTE or DCE ports.
Are adapters required?	To connect to RJ45 console ports, a regular Cat5 cable can be used with no adapter. Raritan also sells male and female DB9 and DB25 adapters for devices with these types of serial ports. Adapters are also available to connect to Raritan PX intelligent Rack PDU's.
What is the maximum distance from the SX II to a serial device?	The distance varies according to the baud rate that is used. This can range from 4 feet for 230K baud to over 300 feet for 2.4K baud.
What are some sample connections to serial devices?	The below table shows how to connect the SX II to standard networking and computer equipment. This is based on the type of serial port (RJ45, DB9 & DB25) and its gender (male or female). The required Raritan adapter is shown.

Vendor	Models	Serial Port	How to Connect
Cisco	Catalyst	RJ45	Cat5 cable
Cisco	Catalyst	DB25F	ASCSDB25M adapter and CAT5 cable
Cisco	Router	RJ45	Cat5 cable
Cisco	Router	DB25F	ASCSDB25M adapter and CAT5 cable
Cisco	UCS	RJ45	Cat5 cable
Cisco	PIX Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
HP	Servers	DB9M	ASCSDB9F adapter and CAT5 cable
Dell	Servers	DB9M	ASCSDB9F adapter and CAT5 cable
IBM	Servers	RJ45	Cat5 cable
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
Silicon Graphics	Origin	DB9M	ASCSDB9F adapter and CAT5 cable
Sun	SPARCStation	DB25F	ASCSDB25M adapter and CAT5 cable
Sun	Netra T1	RJ45	Cat5 cable
Sun	Cobalt	DB9M	ASCSDB9F adapter and CAT5 cable
Various	Windows	DB9M	ASCSDB9F adapter and CAT5 cable
Raritan	PX	RJ45	CSCSPCS-1 or CSCSPCS-10 cable

Installation, Management & Configuration

Installation, Management & Configuration	
How do I initially configure the SX II?	Initial configuration can be done manually from the SX II local console or automatically via USB stick or TFTP server. Manual configuration can be done via CLI by connecting your laptop via (1) USB , (2) serial cable, or (3) by connecting a KVM console. You can also (4) use the web GUI connecting a laptop via a crossover cable. A Quick Setup Guide (QSG) is included.
Can the SX II be completely managed by CLI? Where is the CLI defined?	Yes, the SX II can be completely managed via CLI commands. The CLI is defined in the on-line help, user guide and available from the CLI itself.
Tell me more about the automatic configuration options.	There are two ways to automatically configure the SX II. First, it can be configured by a script of CLI commands, plugged into a USB port on the SX II. Second, a script of CLI commands can be stored on a TFTP server available via DHCP Server or configured into the SX. For security, both of these automatic configuration methods must be enabled by the administrator.
Does the SX II require a FTP Server for firmware upgrades like the current SX?	No, the SX II firmware upgrade process is like that of the KX III. No FTP server is required. The user browses to an encrypted firmware file downloaded from the Raritan website. Many of the management functions are the same as with the KX III. Note that the FTP option still exists via CLI to upgrade the device in this manner.
Can I copy my current SX configuration to the new SX II?"	With the extensive software and hardware changes, the configuration backups of the current SX are unfortunately not compatible with the new SX II.
Where can I get a copy of the SNMP MIB for Dominion SX?	The SX II SNMP MIB is available from the Dominion SX II Support Page on raritan.com. It is also available from the Event Management - Settings page on the web GUI.
Does the SX II work with Raritan's Command Center?	Yes. The Dominion SX II requires CommandCenter Secure Gateway Release 6.1 and above, available in September 2015. Using CommandCenter, users can connect to thousands of serial (and KVM) devices, connected to the Dominion SX, SX II, KX III and other Raritan devices.
Security	

Security	
Is the Dominion SX II secure?	Yes, the Dominion SX II has rock-solid security with military grade security features such as 256 bit AES encryption with a FIPS 140-2 mode and encryption module. The SX II has a long list of security features and each release is tested with a vulnerability scanner. Security patches will be made available from the Raritan website.
Is the Dominion SX II FIPS 140-2 certified?	The Dominion SX II uses an embedded FIPS 140-2 validated cryptographic module running on a Linux platform per FIPS 140-2 implementation guidelines. This cryptographic module is used for encryption of serial sessions when using the Raritan Serial Client (RSC).
Is ActiveDirectory authentication supported?	Yes, ActiveDirectory, LDAP, Radius and TACACS authentication are supported. In addition the SX II administrator can create local users with their passwords.
Which ports need to be open for SX II connections?	Port 443 (for https); optionally port 80 (http) for user sessions. When using SSH, port 22 needs to be open. The TCP ports for HTTP, HTTPS, Telnet, SSH are all user configurable. These user configured ports will need to be open for access. Also, TCP port 5000.
What type of logging is available?	The SX II supports many types of events generated for user access, security events as well as administrative actions. Multiple logging methods are available including SNMP, Syslog, Email, NFS and internal log file.
Is the serial port data logged?	Yes, data from the serial devices can be logged to a local file on the SX II, Syslog or NFS server.
What is the default login and default password?	The default login is "admin" and the default password is "raritan". You are forced to change the password when you first log in to the SX II. We recommend that you also change the default "admin" name for security reasons. Also recommended is strong passwords for your local accounts, which can be enabled on the Security Settings panel.
I have lost the Admin password to the Dominion SX. What can I do?	You can restore the unit to its factory default settings. A factory reset function to restore the unit to factory default settings is provided. This reset function has several configurable options.
User Interface & Documentation	

User Interface & Documentation	
What type of web-based user interface does the Dominion SX II have?	The Dominion SX II Graphical User Interface is similar to the other Dominion products, providing a common look-and-feel across the Dominion SX II, KX, KSX and KX2-101-V2. In addition, similar management features are available including firmware update, backup and restore, security options and diagnostics.
Does the SX II require Java?	For web browser access by the Raritan Serial Console software, Java is required. Java is not required for CLI access to the SX II via SSH, Telnet or an at-the-rack connection.
Where can I get documentation (user guide, etc.) for the Dominion SX II?	The Data Sheet, available on the SX II Product Page, provides a good overview of the SX showing the available models, adapters and features. The Features and Benefits document, also available on the SX II Product Page, provides a list of the SX II features. The SX II Support Page provides detailed technical information including the Release Notes, User Manual, On-line Help, SX II MIB and firmware releases.

Appendix E SX II Support

In addition to Raritan Technical Support and Customer Support, the following resources are available.

In This Chapter

SX II Release Notes and Help

SX II Release Notes

Release notes come with the SX II appliance and are available on the Support page of ***Raritan's website*** (***http://www.raritan.com/support/firmware-and-documentation***).

Review the release notes for important information before you begin using the appliance.

SX II Quick Setup Guide

Online help is accompanied by the **SX II Quick Setup Guide**, which is included with your SX II and can be found on the Support page of ***Raritan's website*** (***http://www.raritan.com/support/firmware-and-documentation***).

SX II Online Help

SX II online help is considered your primary help resource.

Access client help is provided as part of SX II online help.

To use online help, Active Content must be enabled in your browser.

SX II Users Guide and Administrators Guide

A PDF version of help topics specific to end users is contained in the SX II User Guide and topics specific to SX II administrators are contained in the SX Administrators Guide.

Both PDFs are available on the Support page of ***Raritan's website*** (***http://www.raritan.com/support/firmware-and-documentation***).

Index

D

E

F

H

I

J

L

M

N

P

R

S

T

U

V

W