Part of HID Global

Hardening Guide

October 2018

Contents

List of Figures

This guide is for information purposes only. Mercury Security makes no warranties, expressed or implied, in this summary.

Copyright

Trademarks and Third-Party Copyrights

Revision History

Date	Description	Version
October 2018	Added ‘Protection Against Replay Attacks on IP Networks’	A.2
July 2018	Added ‘Encrypted Partition’ option	A.1
March 2018	Initial release	A.0

Contacts

2355 Mira Mar Avenue

Long Beach, CA 90815

Phone: 1.562.986.9105

Fax: 1.562.986.9205

1 Overview

This Hardening Guide covers how to maximize security with Mercury Controllers. This guide will identify critical information on features, suggest options that should be enabled, and include best practices for using the controller.

1.1 Intelligent Controllers and Interface Modules

Various generations of intelligent controllers and interface modules exist within Mercury and the OEM branded product portfolios. Product capabilities improve over time and therefore some security parameters and hardening instructions differ across products. The following intelligent controllers and interface modules are covered in this hardening guide.

LP Series Intelligent Controllers	EP4502, LP4502, LP1501, LP1502 and LP2500
EP Series Intelligent Controllers	EP1501, EP1502, EP2500, MS-ICS, M5-IC, MI-RS4, MI-XL16
Series-3 SIO Interface Modules	MR50, MR62e, MR52, MR16IN, MR16OUT
Series-2 SIO Interface Modules	MR50, MR51e, MR52, MR16IN, MR16OUT
Bridge Controllers	MS-ICS, M5-IC, MI-RS4, MI-XL16
Honeywell Controllers	PW6K1IC, PRO32IC

Note: The Bridge and Honeywell Controllers follow the EP Series functionality in this document.

1.2 Protection Levels

Depending on the system size and needs, there are different protection levels. Each level assumes the previous level's recommendation.

Table 1 Protection Levels

Protection Level	Recommendation	Procedures
Basic	Minimum protection Small businesses or office installations where the operator is also the administrator	1) Installation (section 2) – place product on private network, in secured enclosure, with updated firmware and normal DIP switch settings. 2) Web Interface (section 3) – enable HTTPS. 3) User Accounts (section 4) – remove default user login, create a unique user account with a strong password. 4) Equipment Replacement (section 8) – bulk erase controller and clear downstream module EEPROM.
Intermediate	Corporations that have a dedicated system administrator	5) Web Interface (section 3) –add authorized IP addresses. 6) Information Services (section 5) – disable discovery and SNMP services. 7) Encryption and Authentication (section 6) – enable AES or TLS encryption.

Protection Level	Recommendation	Procedures
Enterprise	Large networks with an IT/IS department. Intended for integration into an enterprise network infrastructure.	8) Information Services (section 5) – enable SNMPv3 (EP4502, LP-series). 9) Encryption and Authentication (section 6) – generate and load customized peer certificates and enable TLS. 10) Port Based Network Access Control (section 7) – enable 802.1X. 11) Enable data encryption at rest (EP4502, LP-series) (section 6.5)

2 Installation

Recommendations include private networks, securing the enclosure, ensuring the latest firmware and normal operation.

2.1 Private Network

Do not install any Ethernet products on the public Intranet.

2.2 Securing the Enclosure

Install the hardware in a secure enclosure and use a cabinet tamper to generate notifications for when the enclosure is opened.

2.3 Ensuring the latest Firmware

Check with the OEM for the latest firmware. Update all intelligent controller and SIO interface board firmware to the latest version. This ensures the latest changes and security improvements are installed.

2.4 Normal Operation

Set all dip switches to OFF for normal operation.

3 Web Interface

Modify the HTTPS, Session Timer and authorized IP addresses to reduce your risk.

3.1 HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a protocol for securing communication over a network. HTTPS is a combination of HTTP and SSL/TLS protocols. It is used to provide encrypted communication with the web server. Always enable HTTPS as the default.

Ensure DIP SW3 is in the OFF position to enable HTTPS.

Note: HTTP is not supported on the EP4502 and LP Series controllers. Any HTTP request is redirected to HTTPS.

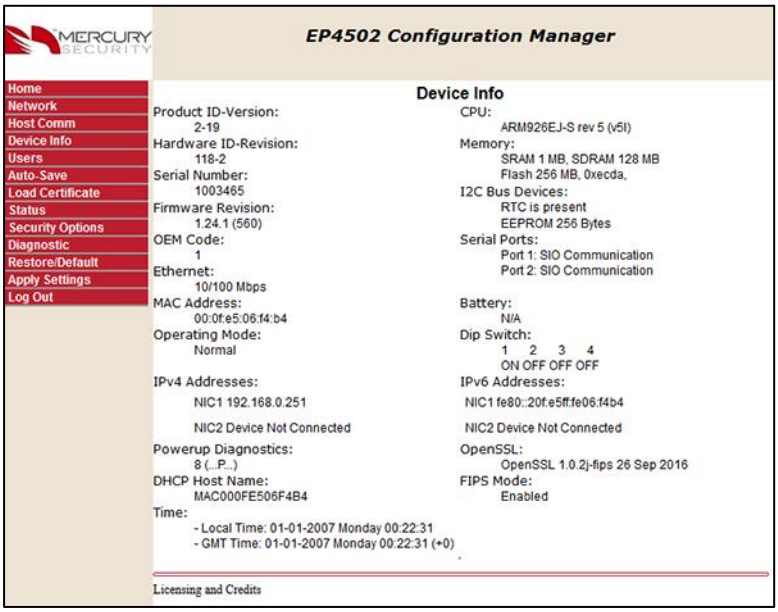


Figure 1 Device Information

3.2 Session Timer

The session timer logs off a user after a certain period of time.

A value of five (5) minutes is recommended to minimize the risk of when an attacker can access active sessions. Values from five minutes to 60 minutes in 5 minute increments are allowed.

Access the Session Timer configuration from the Users page of the web interface.

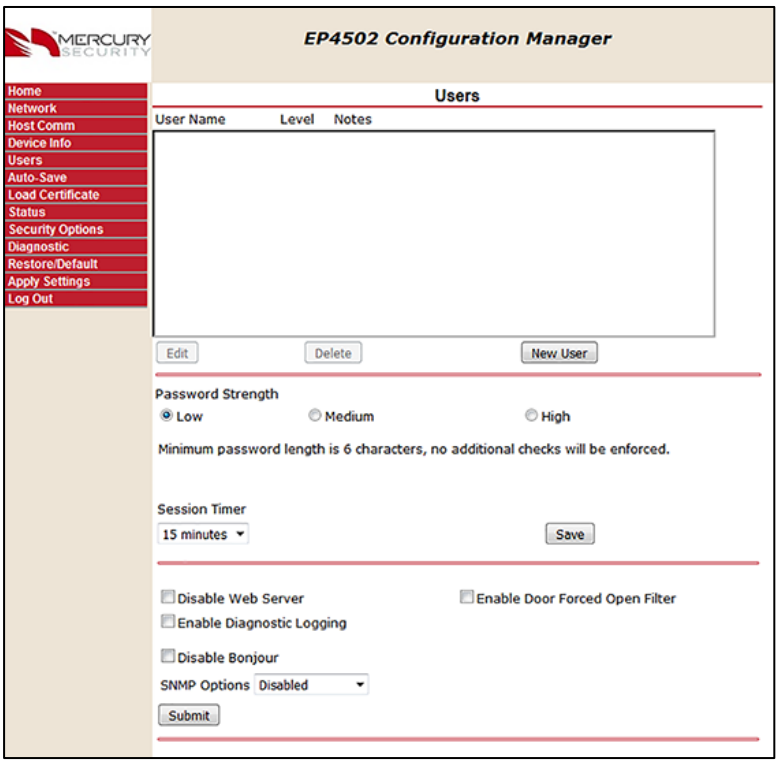


Figure 2 Users

3.3 Authorized IP Addresses

Restrict accessing the controller's host communication port.

When there are only one or two IP addresses accessing the controller's host communication port, you can restrict where this connection originates. This filter applies to the communication port established by a host application configured in IP Server (host initiated connection) mode. In an IP Client (controller initiated connection) mode, the authorized IP addresses are programmed into the controller by the host application.

From the Host Communication page, select Authorized IP Address Required and specify the permitted one or two addresses.

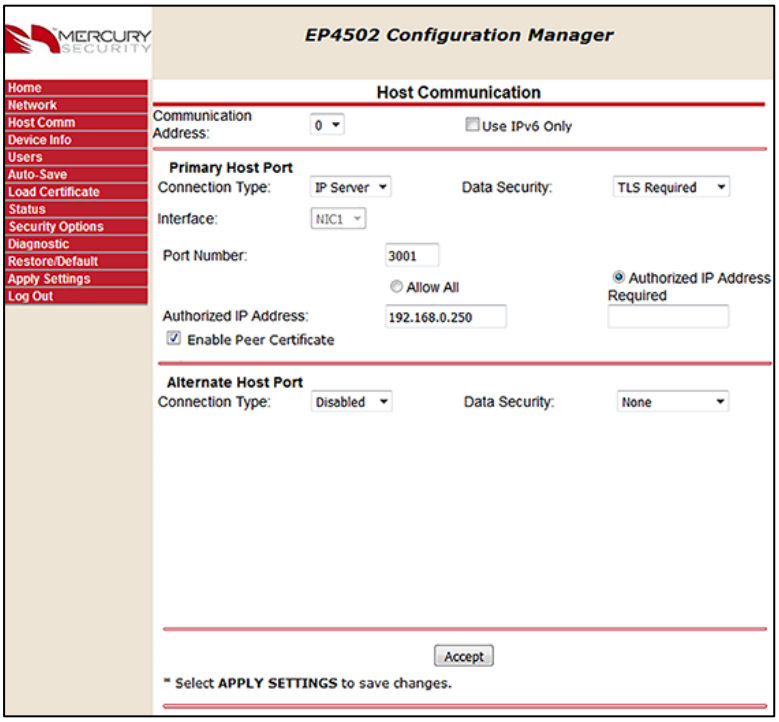


Figure 3 Authorized IP Addresses

4 User Accounts

Modifying user account information is paramount to the controller's security.

4.1 Default User Login

The following is the default user login and password for out-of-the-box controllers.

Username: admin

Password: password

The default user credentials are the same for all Mercury Security Controllers. To prevent unauthorized use, disable the default user.

For firmware 1.25.6 or later, permanently disable the default user account by clicking the Disable Default User check box from the Users page.

For firmware 1.19.4, build 0415 or later, temporarily enable the default user account with the following steps (only if the default user was not permanently disabled).

1. Enable the default user by transitioning DIP SW1 from OFF to ON. The user then has five minutes to log into the web interface.
2. A single login within the five minutes, or rebooting the board disables the ability to use the default login account until another DIP SW1 transition is performed.

For firmware before 1.19.4 build 0415, ensure DIP SW1 is OFF and at least one unique user account is created.

4.2 Unique User Accounts

Create at least one unique user the first time you login to the web interface. This user should use a unique username and password. Each person accessing the web interface should have their own unique account for audit purposes.

4.3 Password Strengths

User accounts have three levels of password strengths (Low, Medium and High).

Maximize password security by ensuring the password is a high level strength.

Note: The LP Series requires a high strength password.

4.3.1 High Strength Passwords

- Eight character minimum
- Must not contain the username
- Meets all three criteria points (see Password Criteria)

4.3.2 Medium Strength Passwords

- Six character minimum
- Meets two criteria points (see Password Criteria)

4.3.3 Low Strength Passwords

- Six character minimum

4.3.4 Password Criteria

Passwords must contain three of the four categories characters shown.

- Uppercase alphabet characters (A-Z)

- Lowercase alphabet characters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (!, $, #, or %)

5 Information Services

Prevent discovery services through implementing the following guidelines.

5.1 Disable Discovery

By default the controllers supports device discovery utilizing Zeroconf through services on Windows® and Linux like Apple® Bonjour® and mDNSResponder. Once the controller is installed and configured it is recommended to turn-off discovery. This prevents someone with access to the same network from discovering the controllers.

Disable Zeroconf Discovery through the Users page in the web interface.
See Figure 2 Users.

5.2 Disable SNMP

By default, SNMP is disabled. If SNMP is not used, leave this setting disabled.

Disable SNMP through the Users page in the web interface. See Figure 2 Users.

6 Encryption and Authentication

Utilize the following settings to improve encryption and authentication methods.

6.1 Host / Controller Encryption

The controller supports AES and TLS encryption for host communications. Use one of these methods to encrypt the data being transferred to and from the controller. TLS is recommended for data security over AES.

6.1.1 AES

Enable AES encryption by configuring both the host and controller. Load the encryption keys (128 or 256-bit) on both sides before enabling AES.

6.1.2 TLS

By default, unique certificates are loaded into each controller at production time. Use these certificates to encrypt communication between the host and controller. Enable TLS encryption through the webpage or host application, if implemented.

Provided are the options TLS Required and TLS if Available.

TLS if Available. Enable TLS if Available locally at the controller without host side changes and the default will be TLS, if possible.

TLS Required. Enable TLS Required indicates only encrypted connections are established and requires TLS configuration of the host software. TLS Required is more secure.

See Figure 4 Host Authentication for webpage configuration.

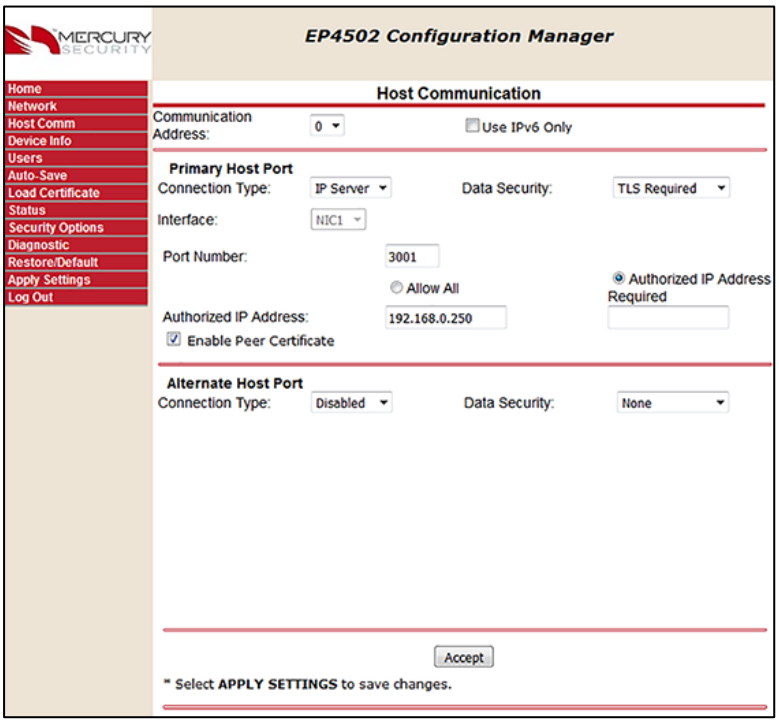


Figure 4 Host Authentication

6.2 Host / Controller Authentication

Also use certificates to authenticate the validity of the host and controller. One limitation of factory loaded certificates is they cannot be customized to the location where the controller is deployed. By loading customized peer certificates on the host and controller, a TLS connection proves the validity of host and controller.

For the controller, peer certificates are loaded through the Load Certificate page of the web interface or through the host application, if implemented. Likewise, the peer certificate of the controller must be loaded into the host's certificate store in order to mutually authenticate the validity of the controller. See Figure 5 Load Certificate for webpage configuration.

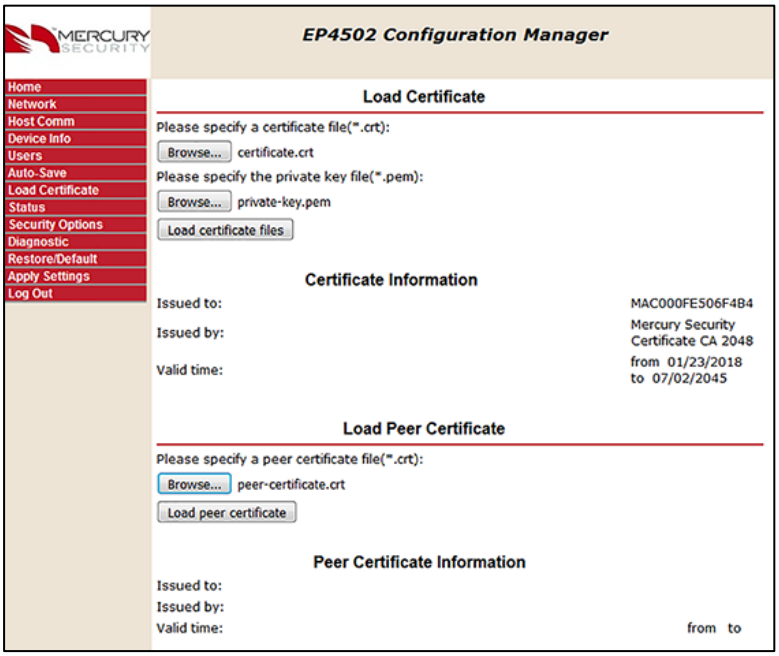


Figure 5 Load Certificate

EP4502 and LP Series controllers support larger key sizes and higher SHA size.

RSA Key Size: 4096-bit maximum – default is 2048 (EP4502) and 3072 (LP-series)

SHA Size: sha384 maximum (factory default is sha256)

Host and SIO Communication TLS Ciphers: FIPS 140 cipher suite

Webpage HTTPS/TLS Ciphers:

EECDH+AESGCM

EDH+AESGCM

EP1501, EP1502, and EP2500 controllers

RSA Key Size: 1024-bit

SHA Size: sha1

Host, SIO Communication and Webpage HTTPS/TLS Ciphers:

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

Notice: The values are recommended ONLY because these are the highest value before performance is degraded.

For more information on certificate verification (both server and controller), see the TLS Encryption Support application note.

6.3 Controller to Downstream Module Communications

Enable encryption between the controller and downstream devices.

Series 2 SIO Interface Modules	Only supports AES128 encryption. Must be configured and enabled.
Series 3 SIO Interface Modules	Supports AES128 and AES256. For LP Series and EP4502 Intelligent Controllers, AES256 encryption is enabled by default. For EP Series Intelligent Controllers, AES128 is available and must be configured, and enabled.
MR51e	Only supports AES128 encryption. Enabled by default.
MR62e	Supports either AES128 or TLS encryption. Enabled by default.

6.4 Reader Communications

Use OSDP secure channel (V2) for reader communications. This bi-directional protocol is secured using symmetric keys shared between the reader and controller, and is a more secure communication method.

Notice: OSDP secure channel encryption is not available on the Series 2 SIO modules.

6.5 Data at Rest Encryption

The ability to encrypt “data at rest” has been implemented to satisfy privacy concerns for end users in the field. The encryption will allow the configuration and data files to be stored in an encrypted container such that the files will remain inaccessible if the correct procedure and password are not used.

To enable “data at rest” encryption, select the ‘Enable Encryption Partition” on the “Security Options” property page within the installer web interface.

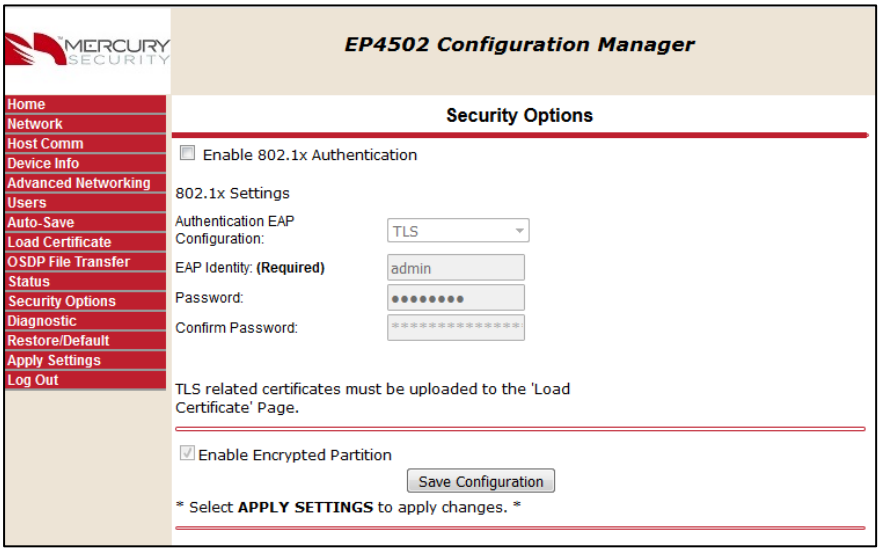


Figure 6 Encrypted Partition

6.6 Protection Against Replay Attacks on IP Networks

6.6.1 Host / Controller Communications

As stated in prior sections, the LP/EP intelligent controllers support AES and TLS encryption for host communications. These mechanisms are used to encrypt the data transferred to and from the controller. When using AES encryption (128 or 256-bit), both the host and controller are loaded with encryption keys set by the host software system. When using TLS encryption, unique certificates are installed on every controller at the time of production and used to encrypt communication between the host and controller. Additionally, the host software system or Mercury installer web pages may be used to load customized peer certificates to the controller. Encryption and network specific mutual authentication can then be realized by loading controller peer certificates on the host software system. Different controller models support different key lengths and ciphers. When utilizing AES or TLS each session is protected using session keys that are generated using a FIPS 140-2 approved (and certified on LP controller) random number generator. Additionally, only a single host connection to the controller is allowed, thus limiting the ability for rogue hosts to connect to the controller. Commands sent to the controller also utilize sequence numbers that reduce the ability to replay commands that are out of sequence.

6.6.2 Controller / IP-Based Downstream Module Communications

The MR62e and MR51e IP-enabled input/output modules support AES encryption (128-bit) between the controller and downstream module by default. Additionally, the newer MR62e supports TLS specifically for the installer webpages. The AES encryption on the MR62e and MR51e is synchronized using a combination of random seed and RSA1024 private/public key pairs generated every time after reboot. When utilizing AES or TLS, each session is protected using session keys that are generated using an FIPS 140-2 approved random number generator. These security mechanisms help protect against replay command attacks.

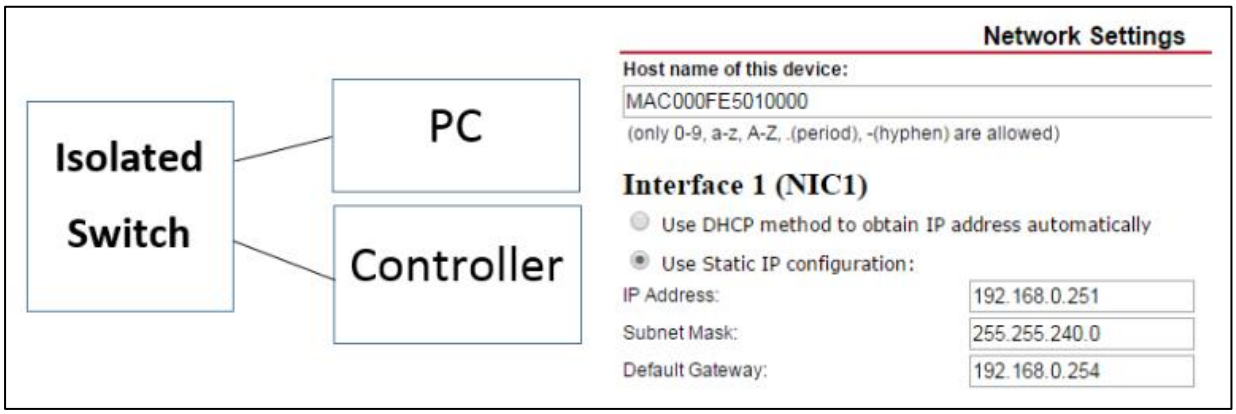
7 Port Based Network Access Control

7.1 802.1x - EP4502 and LP Series Controllers Only

As an added layer of local area network security, add 802.1x authentication to prevent unwanted access to a given network. A supplicant, or device intending to connect to the network, must first agree on a type of Extensible Authentication Protocol (EAP) with the authentication server that is linked to the desired network. Afterwards, the supplicant is required to pass a series of challenges passed from the middle-man, authenticator in order to communicate with the network connected to the authentication server. EAP's range from anything simple as a combination of username/password, to requiring a certificate over Transport Layer Security (TLS), and requiring both username/password, and certificate over TLS. By doing so, the authentication server can prevent access to any supplicant who does not properly authenticate.

This feature is only supported on the EP4502 (firmware 1.24.1) and the LP Series controllers.

To activate, install the controller on an isolated network (or direct connect to host), configure with a static IP and connect through the web page.



If you are using TLS, you must also ensure that the controller certificates are signed by the same root certificate used by the authentication server. See Figure 7 Security Options for webpage configuration on loading certificates.

Once the controller is able to communicate using a browser,

1. Select Security Options.
2. Check Enable 802.1x Authentication.
3. Enter the EAP login and password (based on the authentication server configuration).
4. Reboot the controller.
5. Connect to the desired network.

The controller is now authenticated using 802.1x.

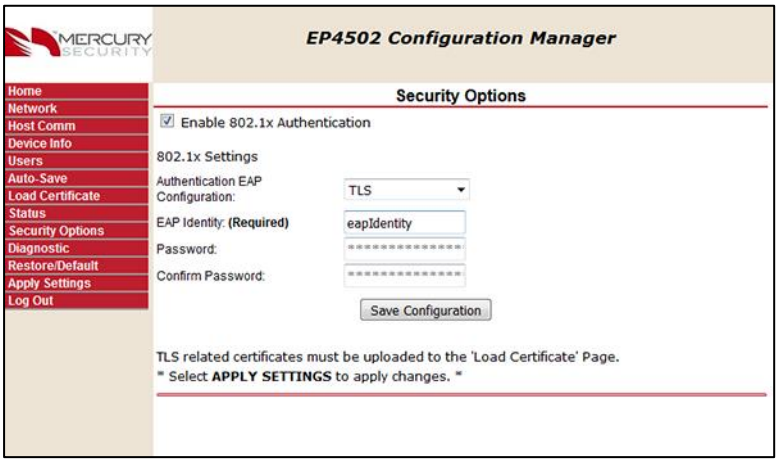


Figure 7 Security Options

8 Equipment Replacement

When replacing a board, clear data if the hardware is capable.

8.1 Controller

Perform the bulk erase procedure to sanitize the board.

8.1.1 Bulk Erase Procedure

CAUTION: Do not remove power during steps 1-8.

1. Set S1 DIP switches.

   1 & 2 ON

   3 & 4 OFF
2. Apply power to the board.
3. Watch for LEDs 1 & 2 and 3 & 4 to alternately flash at a 0.5 second rate.
4. Within 10 seconds of powering up, change switches 1 or 2 to OFF.

   If these switches are not changed, the board powers up using the OEM default communication parameters.
5. LED 2 flashes, indicating that the configuration memory is being erased.
6. Full memory erase takes up to 60 seconds.
7. When complete, only LEDs 1 & 4 flash for eight seconds.
8. The board reboots eight seconds after LEDs 1 & 4 stop flashing (LEDs are off during this time).

8.2 Downstream Modules

On the downstream module, clear the EEPROM.

8.2.1 Clearing EEPROM Procedure

Perform the following steps to clear the configuration stored in EEPROM.

1. Set all DIP switches to OFF on the SIO.
2. Cycle power.
3. Within three seconds of applying power, set DIP switch 8 to the ON position.
4. After the board completes its power up sequence, set the DIP switches to the correct state.

Notice: This procedure does not work on the MR51e.

8.2.2 MR62e Bulk Erase

NOTICE: Do not remove power during steps 4-6.

1. Set S1 DIP switches to: 1 & 2 ON, 3 & 4 OFF.
2. Apply power to the MR62e.
3. Watch for LEDs 1 & 2 and 3 & 4 to alternately flash at a 0.5 second rate.
4. Within 10 seconds from applying power, change switches 1 or 2 to OFF.
   If these switches are not changed, the MR62e will power up using the OEM default communication parameters.
5. LEDs 1 and 2 alternately flash at a 0.5 second rate while the memory is erased.
6. Once the memory is erased, LED 1 will be on for about 3 seconds and then the MR62e will reboot.

9 Network Ports

Network ports used by intelligent controllers, MR51e and MR62e.

9.1 EP Controllers

The following ports are used by the EP Controllers.

Port	Port Type	Usage	Disable
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes – Use Disable Web Server from the Users web confirmation page.
161	UDP	SNMP	Yes – Use Disable SNMP from the Users web configuration page.
443	TCP	HTTPS	Yes - Use Disable Web Server from the Users web configuration page.
3001	TCP	Mercury Host Protocol (MSP2)	Yes – Set the Connection Type from the Host Comm page to an option other than IP.
4001	TCP	PSIA	
5353	UDP	Zeroconf (Discovery)	Yes – Use the Disable Bonjour option from the Users web configuration page.

Note: Configure the Mercury Host Protocol (MSP2) to use a different port. The default port is 3001.

9.2 LP Controllers

The following ports are used by the LP Controllers.

Port	Port Type	Usage	Disable
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes – Use Disable Web Server from the Users web confirmation page.
161	UDP	SNMP	Yes – Use Disable SNMP from the Users web configuration page.
443	TCP	HTTPS	Yes - Use Disable Web Server from the Users web configuration page.
3001	TCP	Mercury Host Protocol (MSP2)	Yes – Set the Connection Type from the Host Comm page to an option other than IP.
4001	TCP	PSIA	
5353	UDP	Zeroconf (Discovery)	Yes – Use the Disable Bonjour option from the Users web configuration page.
47808	TCP	BACnet	Yes – BACnet is disabled by default.
47307	UDP	OTIS	Yes – Only used when OTIS integration is enabled.
48307	UDP	OTIS	Yes – Only used when OTIS integration is

Port	Port Type	Usage	Disable
			enabled.
45303	UDP	OTIS	Yes – Only used when OTIS integration is enabled.
46303	UDP	OTIS	Yes – Only used when OTIS integration is enabled.
46308	UDP	OTIS	Yes – Only used when OTIS integration is enabled.
45308	UDP	OTIS	Yes – Only used when OTIS integration is enabled.
10200	TCP	pivCLASS Embedded	Yes – Configure through the pivCLASS embedded web configuration page.

9.3 MR51e

The following are ports used by the MR51e.

Port	Port Type	Usage	Disable
3001	TCP	Mercury SIO Communication Protocol (MSP1)	No

9.4 MR62e

The following are ports used by the MR62e.

Port	Port Type	Usage	Disable
161	UDP	SNMP	Yes – Off by default. Configure through the web configuration page.
443	TCP	HTTPS	Yes - Use Disable Web Server from the Users web configuration page.
3001	TCP	Mercury SIO Communication Protocol (MSP1)	No
5353	UDP	Zeroconf (Discovery)	Yes – Use the Disable Bonjour option from the Users web configuration page.