

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



HID Mercury™

Cyber Hardening Guide

PLT-05009, A.1
January 2021

Powering
Trusted Identities

Copyright

© 2020 - 2021 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID Brick logo, the Chain Design, HID Mercury, and pivCLASS are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Contacts

For additional offices around the world, see www.hidglobal.com/contact/corporate-offices.

| Americas and Corporate | Asia Pacific |
|---|--|
| 611 Center Ridge Drive Austin, TX 78753 USA Phone: +1 866 607 7339 | 19/F 625 King's Road North Point, Island East Hong Kong Phone: +852 3160 9833 |
| Europe, Middle East and Africa (EMEA) | Brazil |
| 3 Cae Gwyrdd Green Meadow Springs Cardiff CF15 7AB United Kingdom Phone: +44 (0) 1440 711 822 | Condomínio Business Center Av. Ermano Marchetti, 1435 Galpão A2 - CEP 05038-001 Lapa - São Paulo / SP Brazil Phone: +55 11 5514-7100 |

HID Global Technical Support: www.hidglobal.com/support.

What's new

| Date | Description | Revision |
|--------------|----------------|----------|
| January 2021 | Minor changes. | A.1 |

A complete list of revisions is available in [Revision history](#).

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 01

Overview

Powering
Trusted Identities

This Hardening Guide covers how to maximize security with HID 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 HID 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-S3, MR52-S3, MR16IN-S3, MR16OUT-S3, MR62e |
| 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.

| Protection Level | Recommendation | Procedures |
|------------------|--|--|
| Basic | Minimum protection. Small businesses or office installations where the operator is also the administrator | <ol style="list-style-type: none"> 1. Installation (see Installation). Place the product on a private network, in a secured enclosure, with updated firmware and normal DIP switch settings. 2. Web Interface (see Web interface). Enable HTTPS. 3. User Accounts (see User Accounts). Remove default user login, create a unique user account with a strong password. 4. Equipment Replacement (see Equipment replacement). Bulk erase controller and clear downstream module EEPROM. |
| Intermediate | Corporations that have a dedicated system administrator | <ol style="list-style-type: none"> 5. Web Interface (see Web interface). Add authorized IP addresses. 6. Web service (see Web interface). Disable web service. 7. Information Services (see Information services). Disable discovery and SNMP services. 8. USB and SD Interfaces (see Information services). Disable USB and SD interfaces. 9. Encrypted and Authenticated Communications (see Encryption and authentication). Enable AES or TLS encryption. |

| | | |
|------------|--|--|
| Enterprise | Large networks with an IT/IS department. Intended for integration into an enterprise network infrastructure. | <ol style="list-style-type: none"> 10. Information Services (see Information services). Enable SNMPv3 (EP4502, LP-series). 11. Encrypted and Authenticated Communications (see Encryption and authentication). Generate and load customized peer certificates and enable TLS. 12. Port Based Network Access Control (see Port based networkaccess control). Enable 802.1X. 13. Enable data encryption at rest (EP4502, LP-series) (see Data at rest encryption). |
|------------|--|--|

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 02

Installation

Powering
Trusted Identities

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 when the enclosure is opened.

2.3 Firmware

Check with the systems software provider for the latest firmware. Update all intelligent controller and IO module firmware to the latest version to ensure the latest changes and security improvements are installed.

2.4 Normal operation

Set all dip switches to **OFF** for normal operation.

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 03

Web interface

Powering
Trusted Identities

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.

The screenshot shows the 'EP4502 Configuration Manager' interface. On the left is a navigation menu with options: Home, Network, Host Comm, Device Info, Users, Auto-Save, Load Certificate, Status, Security Options, Diagnostic, Restore/Default, Apply Settings, and Log Out. The 'Device Info' section is active, displaying the following information:

| Device Info | |
|-----------------------|---|
| Product ID-Version: | 2-19 |
| Hardware ID-Revision: | 118-2 |
| Serial Number: | 1003465 |
| Firmware Revision: | 1.24.1 (560) |
| OEM Code: | 1 |
| Ethernet: | 10/100 Mbps |
| MAC Address: | 00:0fe5:06:f4:b4 |
| Operating Mode: | Normal |
| IPv4 Addresses: | NIC1 192.168.0.251 NIC2 Device Not Connected |
| Powerup Diagnostics: | 8 (...) |
| DHCP Host Name: | MAC000FE506F4B4 |
| Time: | - Local Time: 01-01-2007 Monday 00:22:31 - GMT Time: 01-01-2007 Monday 00:22:31 (+0) |
| CPU: | ARM926EJ-S rev 5 (v5l) |
| Memory: | SRAM 1 MB, SDRAM 128 MB Flash 256 MB, 0xecdca, |
| I2C Bus Devices: | RTC is present EEPROM 256 Bytes |
| Serial Ports: | Port 1: SIO Communication Port 2: SIO Communication |
| Battery: | N/A |
| Dip Switch: | 1 2 3 4 ON OFF OFF OFF |
| IPv6 Addresses: | NIC1 fe80::20fe5ff:fe06:f4b4 NIC2 Device Not Connected |
| OpenSSL: | OpenSSL 1.0.2j-fips 26 Sep 2016 |
| FIPS Mode: | Enabled |

At the bottom of the interface, there is a link for 'Licensing and Credits'.

3.2 Session Timer

The session timer logs off a user after a certain period of time. A value of five minutes is recommended to minimize the risk of when an attacker can access active sessions. Values from five minutes to 60 minutes in five minute increments are allowed. Access the **Session Timer** configuration from the **Users** page of the web interface.

The screenshot shows the LP1502 Configuration Manager web interface. On the left is a navigation menu with options: Home, Network, Host Comm, Device Info, Advanced Networking, Users, Auto-Save, Load Certificate, OSDP File Transfer, Status, Security Options, Diagnostic, Restore/Default, Apply Settings, and Log Out. The main content area is titled "Users" and contains a table with columns "User Name", "Level", and "Notes". One user is listed: "UniqueUser" at level "1". Below the table are buttons for "Edit", "Delete", and "New User".

Below the Users section is the "Session Timer" configuration area, which includes a dropdown menu set to "15 minutes" and a "Save" button. Below that is the "Time Server" section with radio buttons for "Enable" and "Disable" (selected), and fields for "Server:" (set to "User Specified (Hostname)"), "Port:", "Update Interval:" (set to "Every Hour"), and "User Specified Time Server:". A note states "(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)". There is a "Save Time Server" button.

At the bottom are several checkboxes for various settings: "Disable Web Server", "Enable Diagnostic Logging", "Disable USB Interface", "Disable Zeroconf Device Discovery", "Enable Door Forced Open Filter", "Disable Default User", "Disable SD Card Interface", and "Enable Gratuitous ARP". There is also an "SNMP Options" dropdown set to "Disabled" and a "Submit" button.

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.

Select **Host Comm > Authorized IP Address Required** and specify the permitted one or two addresses.

The screenshot shows the 'EP4502 Configuration Manager' interface. On the left is a navigation menu with items: Home, Network, Host Comm, Device Info, Users, Auto-Save, Load Certificate, Status, Security Options, Diagnostic, Restore/Default, Apply Settings, and Log Out. The main content area is titled 'Host Communication' and contains the following settings:

- Communication Address:** 0 (dropdown), Use IPv6 Only
- Primary Host Port:**
 - Connection Type: IP Server (dropdown), Data Security: TLS Required (dropdown)
 - Interface: NIC1 (dropdown)
 - Port Number: 3001 (text input)
 - Radio buttons: Allow All, Authorized IP Address Required
 - Authorized IP Address: 192.168.0.250 (text input),
 - Enable Peer Certificate
- Alternate Host Port:**
 - Connection Type: Disabled (dropdown), Data Security: None (dropdown)

At the bottom, there is an 'Accept' button and a note: '* Select APPLY SETTINGS to save changes.'

3.4 Disable Web Service

The web service is used most frequently to perform initial configuration of the intelligent controller. Once the intelligent controller is configured and connected to the host, you can increase security by disabling the web service by checking the **Disable Web Service** check box at the bottom of the **Users** page. The web service can be re-enabled by the host application provided it has implemented this feature.

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 04

User Accounts

Powering
Trusted Identities

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 intelligent 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 (only if the default user was not permanently disabled):

1. Enable the default user by switching DIP SW1 from **OFF** to **ON**.
2. Log in to the web interface within five minutes.

Note: 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.

Note: To prevent against brute force attacks, three consecutive failed login attempts will lock the user out, preventing them from logging into the web interface for a period of time.

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

1. Six character minimum

4.3.4 Password criteria

Passwords must contain three of the following categories:

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

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section **05**

Information services

Powering
Trusted Identities

Prevent discovery services by implementing the following guidelines.

5.1 Disable discovery

By default the controllers support device discovery on Windows and Linux through Zeroconf services such as Apple Bonjour and mDNSResponder. Once the controller is installed and configured it is recommended to turn-off discovery by checking the **Disable Zeroconf Device Discovery** check box at the bottom of the **Users** page. This will prevent someone with access to the same network from discovering the controllers.

5.2 Disable SNMP

By default, SNMP is disabled. If SNMP is not used, leave this setting disabled. Disable SNMP by selecting **Disabled** from the **SNMP Option** drop-down menu at the bottom of the **Users** page.

5.3 Disable USB and SD interfaces

By default, USB and SD interfaces are enabled. The SD interface can be used to collect log dumps if an intelligent controller is malfunctioning. Disable these interfaces if not used by checking the **Disable USB Interface** and **Disable SD Card Interface** check boxes toward the bottom of the **Users** page.

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 06

Encryption and authentication

Powering
Trusted Identities

Use 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 the time of manufacture. Use these certificates to encrypt communication between the host and controller. Enable TLS encryption by selecting the required level from the **Host Comm > Data Security** drop-down menu:

- **TLS Required:** Only encrypted connections are established. TLS configuration of the host software is also required. TLS Required is more secure.
- **TLS if Available:** Defaults to TLS locally at the controller (if available), with no host side changes required.

The screenshot shows the 'EP4502 Configuration Manager' web interface. On the left is a navigation menu with options: Home, Network, Host Comm, Device Info, Users, Auto-Save, Load Certificate, Status, Security Options, Diagnostic, Restore Default, Apply Settings, and Log Out. The main content area is titled 'Host Communication' and contains the following settings:

- Communication Address:** 0 (dropdown), with a checkbox for 'Use IPv6 Only'.
- Primary Host Port:**
 - Connection Type: IP Server (dropdown)
 - Data Security: TLS Required (dropdown)
 - Interface: NIC1 (dropdown)
 - Port Number: 3001 (text input)
 - Options: Allow All, Authorized IP Address Required
 - Authorized IP Address: 192.168.0.250 (text input)
 - Enable Peer Certificate
- Alternate Host Port:**
 - Connection Type: Disabled (dropdown)
 - Data Security: None (dropdown)

At the bottom, there is an 'Accept' button and a note: '* Select APPLY SETTINGS to save changes.'

HID Mercury LP Intelligent controllers support TLS 1.2. HID Mercury EP Intelligent controllers support TLS 1.1.

6.2 Host/Controller authentication

It is recommended to 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.

Note: The peer certificate of the controller must also be loaded into the host's certificate store in order to mutually authenticate the validity of the controller.

The screenshot shows the 'EP4502 Configuration Manager' web interface. On the left is a navigation menu with options: Home, Network, Host Comm, Device Info, Users, Auto-Save, Load Certificate (highlighted), Status, Security Options, Diagnostic, Restore/Default, Apply Settings, and Log Out. The main content area is titled 'Load Certificate' and contains the following sections:

- Load Certificate:** A section with two 'Please specify a certificate file (*.cert):' prompts. The first has a 'Browse...' button and the text 'certificate.crt'. The second has a 'Browse...' button and the text 'private-key.pem'. Below these is a 'Load certificate files' button.
- Certificate Information:** A table-like display showing:

| | |
|-------------|---|
| Issued to: | MAC000FE506F4B4 |
| Issued by: | Mercury Security Certificate CA 2048 |
| Valid time: | from 01/23/2018 to 07/02/2045 |
- Load Peer Certificate:** A section with a 'Please specify a peer certificate file (*.cert):' prompt, a 'Browse...' button, and the text 'peer-certificate.crt'. Below is a 'Load peer certificate' button.
- Peer Certificate Information:** A section showing:

| | |
|-------------|---------|
| Issued to: | |
| Issued by: | |
| Valid time: | from to |

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

- RSA Key Size: 3072-bit maximum (factory default is 3072-bit on LPs and 2048-bit on EP4502).
- SHA Size: SHA-384 maximum (factory default is SHA-256).
- Host and IO Module Communication TLS Ciphers: FIPS 140 cipher suite.
- Web page HTTPS/TLS Ciphers:
 - ECDH+AESGCM
 - EDH+AESGCM

EP1501, EP1502, and EP2500 controllers

- RSA Key Size: 1024-bit
- SHA Size: SHA-1
- Host, SIO Communication and Webpage HTTPS/TLS Ciphers:
 - TLS_RSA_WITH_AES_256_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA

Note: 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 *HID Mercury TLS Encryption Support Application Note (PLT-05031)*.

6.3 Controller to downstream module communications

Enable encryption between the controller and downstream devices.

| | |
|----------------------------|--|
| Series-3 IO Modules | Supports AES128 and AES256 encryption. <ul style="list-style-type: none"> For LP Series and EP4502 Intelligent Controllers, AES256 is enabled by default. For EP Series Intelligent Controllers, AES128 is available and must be configured and enabled. |
| Series-2 IO Modules | Supports AES128 encryption only. This must be configured and enabled. |
| MR51e | Supports AES128 encryption only. This is enabled by default. |
| MR62e | Supports either AES128 or TLS encryption. This is enabled by default. |

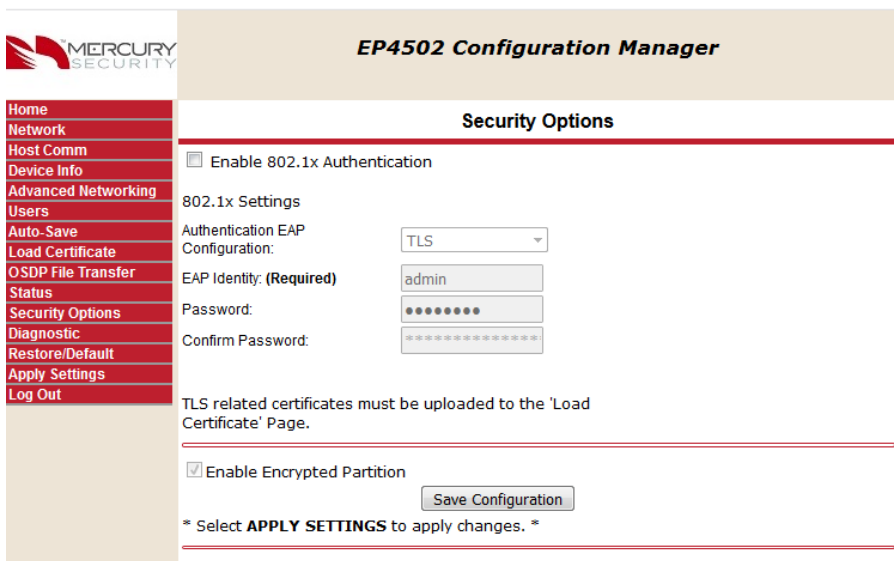
6.4 Reader communications

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

Note: OSDP secure channel encryption is not available on the Series 2 IO 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 allows the configuration and data files to be stored in an encrypted container, with the files remaining inaccessible unless the correct procedure and password are used. To enable “data at rest” encryption, select the **Security Options > Enable Encrypted Partition** check box within the web interface.



6.6 Protection against Replay attacks on IP networks

6.6.1 Host / Controller Communications

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 manufacture and are 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 the LP controller) random number generator. Additionally, only a single host connection to the controller is allowed, limiting the ability for rouge hosts to connect to the controller. Commands sent to the controller also use 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 web pages. 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 using 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.

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section **07**

Port based network access control

Powering
Trusted Identities

7.1 802.1x (EP4502 and LP Series Controllers only)

Add 802.1x authentication as an added layer of LAN security to prevent unwanted access to the 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 network. The supplicant is then 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. EAPs range from anything simple as a combination of username/password, to requiring a certificate over Transport Layer Security (TLS), or requiring both username/password and certificate over TLS. This enables the authentication server to prevent access to any supplicant that does not properly authenticate.

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

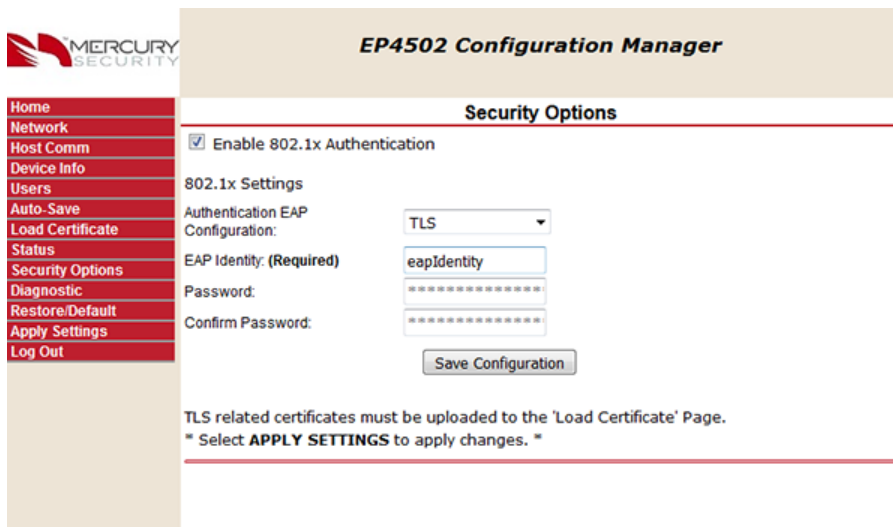
To activate, install the controller on an isolated network (or direct connect to host), configure with a static IP and connect through the web page.

If using TLS, ensure that the controller certificates are signed by the same root certificate used by the authentication server. See [Data at rest encryption](#) for details.

Once the controller is able to communicate using a browser,

1. Select **Security Options**.
2. Check the **Enable 802.1x Authentication** check box.
3. Enter the **Authentication EAP Configuration** and **EAP Identity** information, based on the authentication server configuration.
4. Enter the password in the **Password** and **Confirm Password** boxes.
5. Click **Save Configuration**.
6. Reboot the controller.
7. Connect to the desired network.

The controller is now authenticated using 802.1x.



EP4502 Configuration Manager

Security Options

Enable 802.1x Authentication

802.1x Settings

Authentication EAP Configuration:

EAP Identity: (Required)

Password:

Confirm Password:

TLS related certificates must be uploaded to the 'Load Certificate' Page.
* Select **APPLY SETTINGS** to apply changes. *

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 08

Equipment replacement

Powering
Trusted Identities

When replacing equipment it is recommended to clear all data from the board (if available).

8.1 Intelligent controller

8.1.1 Bulk erase

1. Disconnect power to the board.
2. Set S1 DIP switches 1 and 2 to **ON**.
3. Set S1 DIP switches 3 and 4 to **OFF**.
4. Reconnect power to the board. LEDs 1 and 2, and 3 and 4 should alternately flash at a 0.5 second rate.

IMPORTANT: DO NOT disconnect the power during the remainder of this procedure.

5. Within 10 seconds of powering up, change DIP switches 1 or 2 to **OFF**. Failure to do so results in the OEM default communication parameters being applied.
 - LED 2 flashes, indicating that the configuration memory is being erased. Full memory erase can take up to 60 seconds.
 - When complete, LEDs 1 and 4 will flash for eight seconds. The board will reboot eight seconds after LEDs 1 and 4 stop flashing (LEDs are off during this time).

8.2 IO modules

8.2.1 Clearing the EEPROM

Note: This procedure does not apply to the MR51e.

1. Set all DIP switches to **OFF** on the IO module.
2. Power cycle the IO module.
3. Within three seconds of reconnecting the power, set DIP switch 8 to **ON**.
4. Once the board completes the power up sequence, set the DIP switches to the required position.

8.2.2 MR62e bulk erase

1. Disconnect power to the board.
2. Set S1 DIP switches 1 and 2 to **ON**.
3. Set S1 DIP switches 3 and 4 to **OFF**.
4. Reconnect power to the board. LEDs 1 and 2, and 3 and 4 should alternately flash at a 0.5 second rate.

IMPORTANT: DO NOT disconnect the power during the remainder of this procedure.

5. Within 10 seconds of powering up, change DIP switches 1 or 2 to **OFF**. Failure to do so results in the OEM default communication parameters being applied.
 - LED 2 flashes, indicating that the configuration memory is being erased. Full memory erase can take up to 60 seconds.
 - When complete, LED 1 illuminates for three seconds. The board will then reboot.

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Section 09

Network ports

Powering
Trusted Identities

9.1 EP controllers

| Port | Port Type | Usage | Disable |
|------|-----------|------------------------------|--|
| 67 | UDP | DHCPS | No. |
| 68 | UDP | DHCPC | No. |
| 80 | TCP | HTTP | Yes (Home > Users > Disable Web Server). |
| 161 | UDP | SNMP | Yes (Home > Users > Disable SNMP). |
| 443 | TCP | HTTPS | Yes (Home > Users > Disable Web Server). |
| 3001 | TCP | Mercury Host Protocol (MSP2) | Yes (Home > Host Comm > Connection Type). |
| 4001 | TCP | PSIA | |
| 5353 | UDP | Zeroconf (discovery) | Yes (Home > Users > Disable Zeroconf Device Discovery). |

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

9.2 LP controllers

| Port | Port Type | Usage | Disable |
|-------|-----------|------------------------------|--|
| 67 | UDP | DHCPS | No. |
| 68 | UDP | DHCPC | No. |
| 161 | UDP | SNMP | Yes (Home > Users > Disable SNMP). |
| 443 | TCP | HTTPS | Yes (Home > Users > Disable Web Server). |
| 3001 | TCP | Mercury Host Protocol (MSP2) | Yes (Home > Host Comm > Connection Type). |
| 4001 | TCP | PSIA | |
| 5353 | UDP | Zeroconf (discovery) | Yes (Home > Users > Disable Zeroconf Device Discovery). |
| 47808 | TCP | BACnet | Yes. BACnet is disabled by default. |
| 47307 | UDP | OTIS | Yes (only when OTIS integration is enabled). |
| 45303 | UDP | OTIS | Yes (only when OTIS integration is enabled). |
| 46303 | UDP | OTIS | Yes (only when OTIS integration is enabled). |
| 46308 | UDP | OTIS | Yes (only when OTIS integration is enabled). |
| 45308 | UDP | OTIS | Yes (only when OTIS integration is enabled). |
| 10200 | TCP | pivCLASS® Embedded | Yes (configure through the pivCLASS embedded web page). |

9.3 MR51e

| Port | Port Type | Usage | Disable |
|------|-----------|---|---------|
| 3001 | TCP | Mercury SIO Communication Protocol (MSPI) | No. |

9.4 MR62e

| Port | Port Type | Usage | Disable |
|------|-----------|---|--|
| 161 | UDP | SNMP | Yes, off by default (Home > Users > Disable SNMP). |
| 443 | TCP | HTTPS | Yes (Home > Users > Disable Web Server). |
| 3001 | TCP | Mercury SIO Communication Protocol (MSP1) | No. |
| 5353 | UDP | Zeroconf (discovery) | Yes (Home > Users > Disable Zeroconf Device Discovery). |

Revision history

| Date | Description | Revision |
|--------------|---|-----------------|
| January 2021 | Minor changes. | A.1 |
| April 2020 | Updated to latest HID corporate template and assigned new document part number. | A.0 |
| October 2018 | Added Protection Against Replay Attacks on IP Networks. | N/A |
| July 2018 | Added 'Encrypted Partition' option. | N/A |
| March 2018 | Initial release (under Mercury branding). | N/A |

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION.

Use and disclosure of this information is strictly restricted by the terms of a nondisclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 611 Center Ridge Dr. Austin, TX 78753.



Powering Trusted Identities

Americas & Corporate

611 Center Ridge Drive
Austin, TX 78758
USA

Support: 866-607-7339

Asia Pacific

19/F 625 King's Road
North Point
Island East
Hong Kong

Support: 852-3160-9833

Europe, Middle East & Africa

3 Cae Gwyrdd
Green Meadow Springs
Cardiff, CF15 7AB
United Kingdom

Support: +44 (0) 1440 711 822

Brazil

Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP, Brazil

Phone: +55 11 5514-7100

PLT-05009, A.1