Migration Guide

Migration Pathways and Priorities for Mercury Controllers and IO Modules

The pace of change in physical security continuously accelerates. Mercury has been a trusted name in security for over 30 years, helping customers navigate these shifts with our commitment to open architecture and cutting-edge solutions.

As we introduce the new Mercury MP Intelligent Controllers, we recognize that our customers are at various stages in their technology lifecycle. Some may still rely on legacy, outdated equipment, while others have adopted more recent offerings.

Much has changed since the release of our Mercury EP Controllers in 2007 and SCP Controllers in 1995. Customers operating these legacy controllers in combination with Series 2 (S2) and Series 1 (S1) IO modules expose themselves to potential security risk and supportability issues the longer they wait to upgrade.

On the other hand, those using the more recently released Mercury LP Controllers and Series 3 (S3/S3B) can modernize security capabilities and get updates to features and security through firmware updates. This guide highlights the relative urgency and critical considerations for these and other typical scenarios.
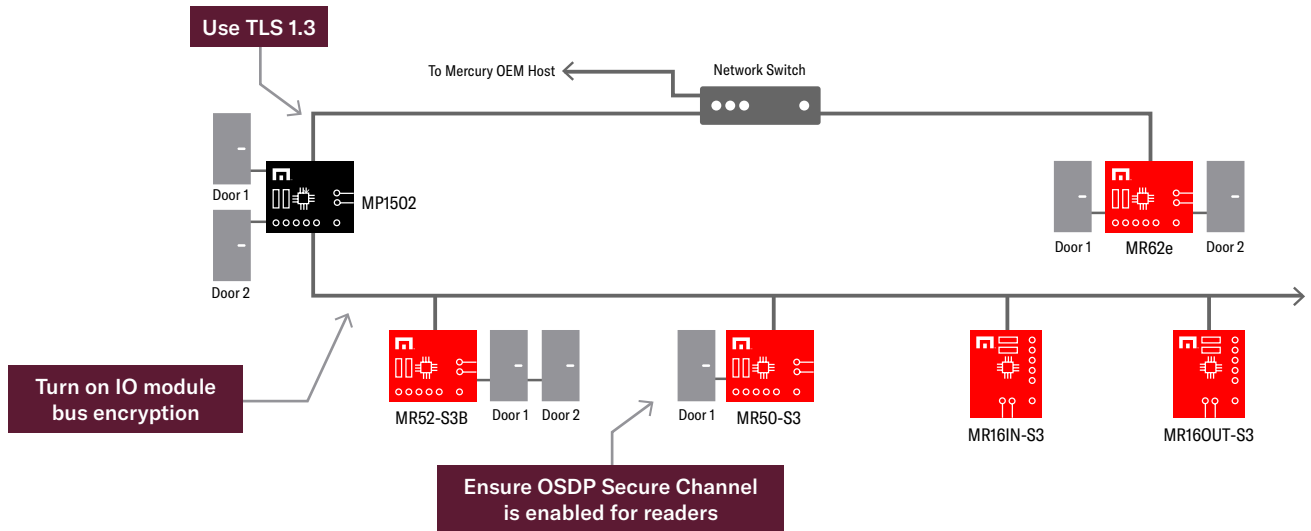
Mercury Controller Families

SCP	EP	LP	MP
1st Generation	**2nd Generation**	**3rd Generation**	**4th Generation**
1995 - 2007	2007 - 2019	2018 - 2028	2024 -
UPGRADE HARDWARE	**UPGRADE HARDWARE**	**UPGRADE FIRMWARE**	**FUTURE-PROOF**
Legacy technology no longer supportable with firmware updates.	Legacy technology no longer supportable with firmware updates.	Modern security and functional capabilities. Update to the latest applicable version of MercOS.	Future-ready app environment with early-lifecycle components and the latest features.

MP
4th Generation
2024 -

MP with S3/S3B IO Modules

MP controllers with S3/S3B IO modules represent the most robust and future-proof configuration. To make the installation as secure as possible, ensure TLS 1.3 is used for connectivity between the host software and the controller. No need to worry about protecting data at rest because it is enabled by default, but be sure the system is configured for encryption on both the IO module bus and OSDP reader bus.
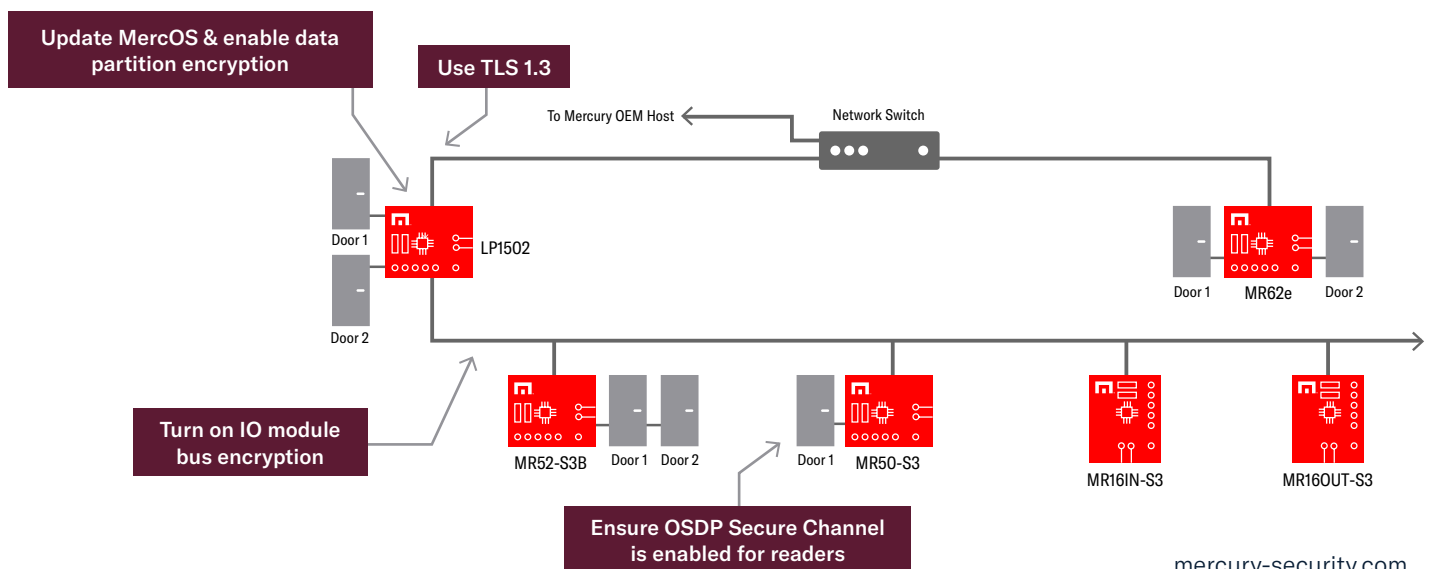
Use TLS 1.3

To Mercury OEM Host ← Network Switch

Door 1
Door 2
MP1502

Door 1 — MR62e — Door 2

Turn on IO module bus encryption

MR52-S3B   Door 1   Door 2   Door 1   MR50-S3   MR16IN-S3   MR16OUT-S3

Ensure OSDP Secure Channel is enabled for readers

LP
3rd Generation
2018 - 2028

LP with S3/S3B IO Modules

LP controllers with S3/S3B IO modules enable a secure and well-supported configuration. To make the installation as secure as possible, ensure the LPs are updated to the latest version of Mercury firmware, MercOS, and enable data partition encryption to secure data at rest. Be sure the system is configured for encryption on both the IO module bus and OSDP reader bus and that host/controller encryption is set up for TLS 1.3.

If you are running a combination of LP and S2/S1 IO modules, **upgrade IO modules to S3/S3B to ensure the latest in security and functionality**.
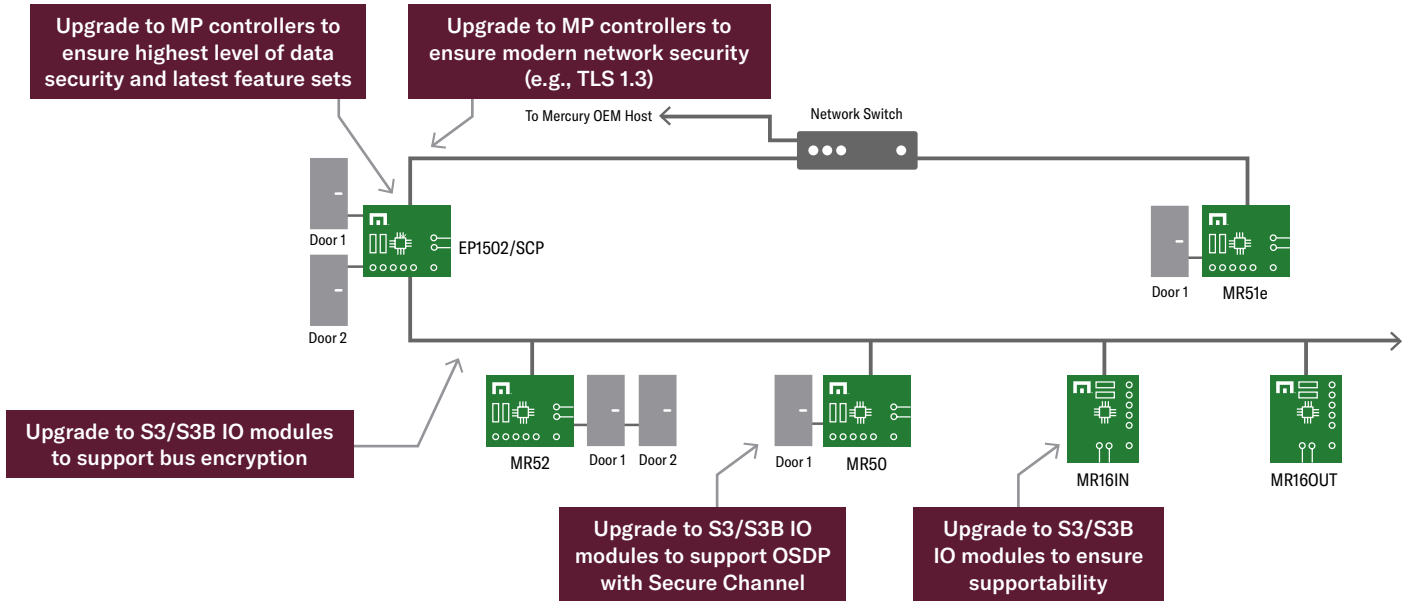
Update MercOS & enable data partition encryption

Use TLS 1.3

To Mercury OEM Host ← Network Switch

Door 1
Door 2
LP1502

Door 1 — MR62e — Door 2

Turn on IO module bus encryption

MR52-S3B   Door 1   Door 2   Door 1   MR50-S3   MR16IN-S3   MR16OUT-S3

Ensure OSDP Secure Channel is enabled for readers

mercury-security.com

EP
2nd Generation
2007 - 2019

SCP
1st Generation
1995 - 2007

EP/SCP with S2/S1 IO Modules

The importance of replacing various combinations of controllers and IO modules increases with the age of the hardware. Feasibility to implement modern security protections decreases the older the hardware gets. Customers with EP and SCP controllers using Series 2 or Series 1 IO modules should weigh the cost of replacement against the significant risks of relying on outdated hardware.

Upgrade to MP controllers to ensure highest level of data security and latest feature sets

Upgrade to MP controllers to ensure modern network security (e.g., TLS 1.3)

To Mercury OEM Host

Network Switch

Door 1

Door 2

EP1502/SCP

Door 1

MR51e

Upgrade to S3/S3B IO modules to support bus encryption

MR52

Door 1   Door 2

Door 1

MR50

MR16IN

MR16OUT

Upgrade to S3/S3B IO modules to support OSDP with Secure Channel

Upgrade to S3/S3B IO modules to ensure supportability

Controllers	Mercury SCP	Mercury EP	Mercury LP	Mercury MP
Upgrade Recommendation	**Most Urgent**	**Urgent**	**Supported through 2028**	**Future-ready**
	• No longer serviceable • Outdated network security • Limited memory • Insecure reader and I/O communications • No smart card/biometric support	• Lacks updated IP security standards (e.g., TLS 1.3) • No FIPS compliance • No modern reader update capabilities • Lacks crypto chip	• Upgrade to the latest applicable* MercOS • Local or cloud-based host connectivity • FIPS 140-3 (pending) • Remote firmware update • Latest network security (mTLS, TLS 1.3)	• Build with new components early in their lifecycle • Modern, hardware-based security (ARM TrustZone, Secure Boot) • App-ready • Remote power cycling • FIPS 140-3 (pending)

* Always consult your OEM software provider for firmware updates. Feature compatibility of MercOS and OEM software vary based on use cases and OEM software provider feature consumption.

| IO Modules	Mercury S1 (MR)	Mercury S2 (MR)	Mercury S3 & S3B (MR)
Upgrade Recommendation	**Most Urgent**	**Urgent**	**Future-ready**
	• No longer serviceable • No RS485 bus encryption • Insecure reader communication • No smart card/biometric support	• No OSDP Secure Channel • No RS485 bus encryption • Lacks crypto chip • No support for FICAM profiles • Not HSPD-12/FIPS 201 Compliant	• Secure crypto engine (S3B) • Embedded crypto chip • OSDP Secure Channel • AES 256 Data Encryption • Support for biometrics, F/2F and clock and data

Secure Your Future Today

Mercury is dedicated to helping customers adapt and protect against the latest security threats and industry changes. For organizations with older hardware, now is the perfect time to upgrade. EP and SCP boards, which are now severely outdated, cannot comply with modern standards due to their age. Customers using LP controllers should always ensure controllers are running the latest applicable version of Mercury firmware, MercOS, and plan for future MP controller purchases and transitions to ensure extensibility and supportability beyond 2028.

By opting for MP controllers and S3/S3B IO modules, your infrastructure is positioned as future-proof, agile and secure. MP controllers will be available later in 2024. Please get in touch with your Mercury representative or OEM partner for details on availability and questions regarding compatibility and upgrade pathways.

Controllers	Mercury SCP	Mercury EP	Mercury LP	Mercury MP
Hardware Availability	No longer manufactured		Ending in 2024	Starting in 2024
Key Security Elements	Limited	Limited	Secure Crypto Chip	Secure Crypto Chip ARM TrustZone Secure Boot Processor
Apps and Integrations	No	Minimal and unsupported	Limited (locks, elevators, strong authentication, power supplies)	Future-ready scalable embedded app environment
Network Security			TLS 1.3, mTLS Requires MercOS 2.x	TLS 1.3, mTLS Requires MercOS 2.x
Firmware Support	No	No	Through 2028	Yes
New Feature Support	No	No	Through 2028	Yes
FIPS Certified	No	No	140-3 (pending) Requires MercOS 2.x	140-3 (pending)
Remote Reader Reboot	No	No	No	Yes
Designed for Cloud API	No	No	Yes Update to MercOS 2.x*	Yes Update to MercOS 2.x*
OSDP Secure Channel	No	No	Yes	Yes
Biometric Reader Support	No	No	Yes	Yes

* For any features, consult your OEM software provider. Many new features of MP and/or MercOS require consumption by the software system.

mercury-security.com
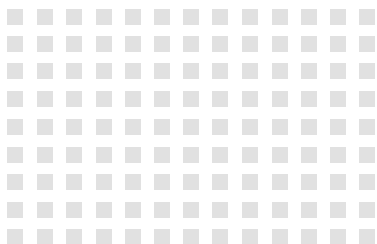
Mercury Security
11165 Knott Avenue, Suite AB
Cypress, CA 90630
mercury-security.com