



Synergis™ Softwire Integration Guide 10.6

Document last updated: January 25, 2018

Copyright notice

© Genetec Inc., 2017

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein. The use of this document is subject to the disclaimer of liability found in the end-user license agreement.

Genetec, Genetec Clearance, Omnicast, Synergis, AutoVu, Federation, Stratocast, Sipelia, Streamvault, Citywise, Genetec Retail Sense, Genetec Traffic Sense, Genetec Airport Sense, Genetec Motoscan, Genetec Citigraf, Genetec Mission Control, Genetec ClearID, Genetec Patroller, Community Connect, the Genetec Logo, the Mobius Strip Logo, the Genetec Clearance Logo, the Omnicast Logo, the Synergis Logo, the AutoVu Logo, and the Stratocast Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

All specifications are subject to change without notice.

Document information

Document title: Synergis™ Softwire Integration Guide 10.6

Document number: EN.702.002-V10.6.B(2)

Document update date: January 25, 2018

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide describes all third-party hardware integrations supported by Synergis™ Softwire, and explains how to enroll and configure these third-party devices on your Synergis™ appliance.

It is assumed that you have read the *Synergis™ Appliance Configuration Guide* and are familiar with the terminology and concepts used in Synergis™ Appliance Portal and Security Center. For specific information regarding the third-party hardware, refer to their manufacturer's web site.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip.** Suggests how to apply the information in a topic or step.
- **Note.** Explains a special case, or expands on an important point.
- **Important.** Points out critical information concerning a topic or step.
- **Caution.** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning.** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec Inc.

Contents

Preface

Copyright notice	ii
About this guide	iii

Chapter 1: Integration through Synergis Software

What is Synergis Software?	2
What is Synergis Appliance Portal?	3
Hardening tips for interface modules	4

Chapter 2: Allegion Schlage Locks

Supported Allegion Schlage locks	6
Supported Allegion Schlage firmware versions	7
Supported Allegion Schlage lock features	8
About Allegion Schlage support for distinct door modes	9
Supported Synergis appliance features for Allegion Schlage lock integration	11
Supported Security Center features for Allegion Schlage lock integration	12
Enrolling Allegion Schlage locks on the Synergis unit	15
Enrolling ENGAGE-integrated Allegion Schlage locks	18

Chapter 3: Assa Abloy Aperio-Enabled Locks

Aperio integration overview	21
Supported Aperio-enabled locks	22
Supported Aperio-enabled lock features	23
Supported Synergis appliance features for Aperio-enabled lock integration	25
Supported Security Center features for Aperio-enabled lock integration	26
Pairing the Aperio-enabled locks with the hub	29
Enrolling the Aperio-enabled locks	33
Configuring doors equipped with an Aperio-enabled lock	35

Chapter 4: Assa Abloy IP Locks

Supported Assa Abloy IP locks	39
Supported Assa Abloy IP lock features	40
About the Radio Wakeup events feature for Assa Abloy WiFi locks	41
Configuring the Radio Wakeup events feature for Assa Abloy WiFi locks	41
Enabling escape and return mode on Assa Abloy IP locks with body type 8200 and monitored deadbolt	42
Enabling passage mode on Assa Abloy IP locks	43
Enabling privacy mode on Assa Abloy IP locks without monitored deadbolt	44
About Assa Abloy IP Cx lock support for 10,000 credentials	45
Supported Synergis appliance features for Assa Abloy IP lock integration	47
Supported maximum PIN length for Assa Abloy IP locks	47
Supported Security Center features for Assa Abloy IP lock integration	49
Configuration overview for Assa Abloy IP locks	52
Enrolling IP locks connected to the Synergis unit	53
Testing the connection between your IP lock and the Synergis unit	56
Disabling encryption on Assa Abloy IP locks	57

Monitoring the battery status of WiFi locks	58
-------------------------------------------------------	----

Chapter 5: AutoVu SharpV Cameras

AutoVu SharpV integration overview	60
Supported AutoVu Sharp cameras	62
Supported AutoVu Sharp camera features	63
Supported Synergis appliance features for AutoVu Sharp camera integration	64
Supported Security Center features for AutoVu Sharp camera integration	65
Enrolling AutoVu SharpV cameras on the Synergis unit	68
Configuring a SharpV camera to control a vehicle access barrier	70

Chapter 6: Axis Controllers

Supported Axis controllers	72
Supported Axis controller features	73
Supported Synergis appliance features for Axis controller integration	75
Supported Security Center features for Axis controller integration	76
Enrolling the Axis controller on the Synergis unit	79
Hardening Axis controllers	81
About the tamper inputs on Axis controllers	82
Configuring the peripherals attached to Axis controllers	83
Reader connections on the Axis controller	87

Chapter 7: DDS Controllers

Supported DDS hardware	89
Supported DDS controller features	90
Supported Synergis appliance features for DDS controller integration	92
Supported Security Center features for DDS controller integration	93
Enrolling DDS RS-485 controllers	96
Preparing to enroll DDS IP controllers	98
About the RS-485 local echo switches on SMC units	102
Enrolling DDS IP controllers	103
Setting the physical address of TPL door controllers	107

Chapter 8: HID VertX Sub-Panels

Supported HID VertX sub-panels	109
Supported HID VertX sub-panel features	110
Supported Synergis appliance features for HID VertX sub-panel integration	112
Supported Security Center features for HID VertX sub-panel integration	113
Enrolling the HID VertX sub-panels connected to the Synergis unit	116
Enabling reader supervision for HID VertX V100	118

Chapter 9: Honeywell Controllers

Supported Honeywell controllers	121
Supported Honeywell firmware versions	121
Supported features for Honeywell controllers	122

Chapter 10: Mercury Controllers

Supported Mercury controllers	124
Supported Mercury firmware versions	126
Supported Mercury controller features	127
Supported Synergis appliance features for Mercury controller integration	129

Supported Security Center features for Mercury controller integration	130
Preparing to enroll the Mercury controller	133
Enrolling Mercury controllers on the Synergis unit	137
Adding OSDP (Secure Channel) readers to an EP controller	140
Adding MR51e panels to an EP controller	142
Setting MR51e to use Public DHCP addressing mode	142
Setting MR51e to use Static IP addressing mode	142
Access control unit - Synergis - Peripherals tab	144
Chapter 11: OSDP Readers	
Supported OSDP readers in Synergis Software 10.6	147
Prestaging OSDP readers connected to the Synergis unit	148
Enrolling OSDP readers connected to the Synergis unit	150
Enabling secure mode on OSDP readers	151
Chapter 12: Salto Sallis Wireless Locks	
SALTO SALLIS integration overview	154
Supported SALTO SALLIS hardware	155
Supported SALTO SALLIS features	156
Supported Synergis appliance features for SALTO SALLIS integration	158
Supported Security Center features for SALTO SALLIS integration	159
Enrolling SALLIS locks	161
Enabling encryption on an existing SALLIS router	166
Disabling encryption on a SALLIS router	167
Chapter 13: SimonsVoss SmartIntego Locks	
Supported SimonsVoss locks	169
Supported SimonsVoss lock features	170
Supported Synergis appliance features for SimonsVoss lock integration	171
Supported Security Center features for SimonsVoss lock integration	172
Preparing to enroll SimonsVoss SmartIntego locks	174
Enrolling SimonsVoss SmartIntego locks on the Synergis unit	175
Chapter 14: STid Readers	
Supported STid readers in Synergis Software 10.6	179
Configuration overview for STid readers with Synergis Software 10.6	181
Enrolling STid readers attached to the Synergis unit	182
Enabling transparent mode on STid readers	184
Changing the default communication parameters with STid readers	186
Advanced STid reader setting configuration	187
General structure SmartCardsReaders.xml for STid readers	187
Encoding a credential on an RFID card in Security Desk	188
Updating the STid configuration on your Synergis unit	189
Glossary	190
Where to find product information	195
Technical support	196

Integration through Synergis™ Software

This section includes the following topics:

- ["What is Synergis Software?"](#) on page 2
- ["What is Synergis Appliance Portal?"](#) on page 3
- ["Hardening tips for interface modules"](#) on page 4

What is Synergis™ Software?

Synergis™ Software is the access control software developed by Genetec Inc. to run on a variety of IP-ready security appliances. Synergis™ Software lets these appliances communicate with third-party interface modules. A security appliance running Synergis™ Software can be enrolled as an access control unit in Security Center.

About Synergis™ appliance

A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come preinstalled with Synergis™ Software and can be enrolled as access control units in Security Center.

There are two generations of Synergis™ appliances:

- [Synergis™ Cloud Link](#) (second generation)
- [Synergis™ Master Controller](#) (first generation)

NOTE: Because Synergis™ appliances can be enrolled as access control units in Security Center, they are also referred to as *Synergis™ units*.

To learn more about the Synergis™ appliances and how they fit into the overall Synergis™ IP access control system architecture, visit our website at www.genetec.com.

About interface modules

An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

In the context of Synergis™ Software integration, interface modules are hardware devices that communicate directly with the Synergis™ appliance. These devices can be intelligent controllers, such as the Mercury EP controllers; sub-panels, such as the HID VertX downstream panels; or readers, such as the STid readers."

What is Synergis™ Appliance Portal?

Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance, as well as upgrade its firmware.

The portal allows you to perform the following tasks:

- Change the security password required to log on to the Synergis™ appliance.
- Configure the network settings on the Synergis™ appliance so it works on your system.
- Configure the appliance to accept connections from specific Access Managers.
- Enroll and configure the interface modules attached to the Synergis™ appliance.

NOTE: There is one exception to the rule. Mercury controllers (EP and M5-IC) must be enrolled and configured from Security Center Config Tool in the access control unit's **Peripherals** tab. For more information, see the chapter on Mercury controllers in the *Synergis™ Software Integration Guide*.

- Configure the access control behavior of the appliance for both online and offline operations.
- Test and diagnose the interface module connections to the Synergis™ appliance.
- View and export the Synergis™ appliance's status and configuration.
- Upgrade the Synergis™ appliance's firmware (Synergis™ Software).
- Restart the Synergis™ appliance's hardware or software.

Tasks that must be done in Config Tool

You cannot perform the following tasks through the portal. You have to use Security Center Config Tool instead.

- Enable/disable the **Server mode** operation (This option is hidden by default; it will only appear if it was already enabled).
- Assign devices (input/output contacts, readers) to doors and zones.
- Configure individual door and zone properties.
- Configure Card and PIN readers so both the card and the PIN are required to grant access.
- Configure I/O linking.

For more information about deploying Synergis™, see the *Security Center Administrator Guide*.

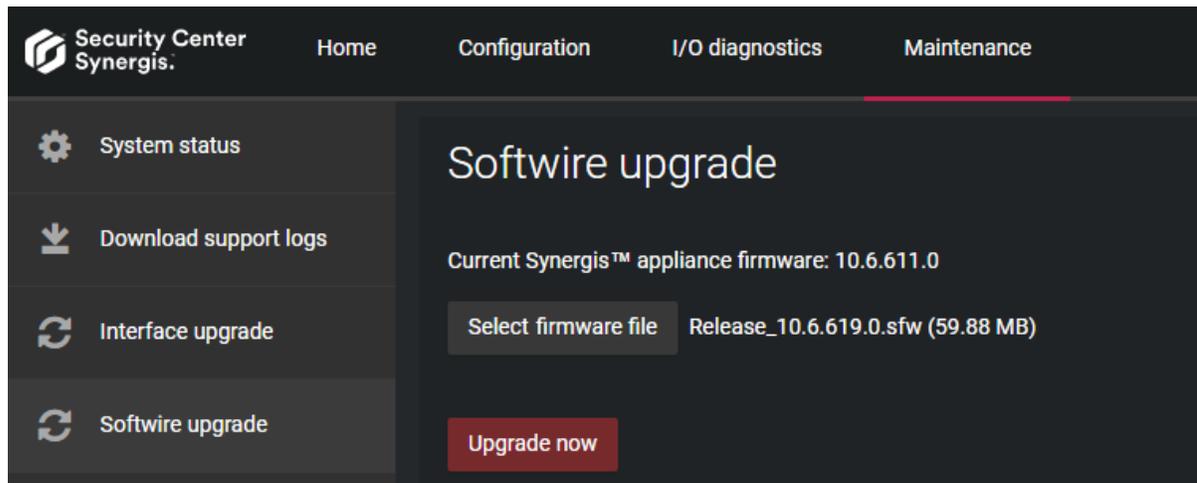
Hardening tips for interface modules

If system security is a priority for your organization, we recommend that you follow the hardening advice for interface modules.

This section only presents the hardening tips that apply to all interface modules. Manufacturer-specific hardening tips are tagged with *Hardening* in each manufacturer's respective integration topics. For hardening guidelines for the entire system, see the *Security Center Hardening Guide*.

Use the latest interface module firmware

Access control hardware manufacturers frequently update their products and fix security vulnerabilities with new firmwares. We continuously test the compatibility of the new firmwares published by third-party interface module manufacturers with Synergis™ Software. We publish the latest interface module firmwares, certified compatible with Synergis™ Software, as *recommended firmwares* in the respective *Supported <third-party devices>* topic of each manufacturer. For certain models of interface module, you can apply the recommended firmware from Synergis™ Appliance Portal. For more information, see the *Synergis™ Appliance Configuration Guide*.



NOTE: Certification tracking of Synergis™-partner firmware is now done within the scope of Synergis™ Software 10.6. If a newly-discovered vulnerability is fixed in a more recent firmware than the one certified by us, then apply it using the manufacturer's software.

Never use default passwords

Many access control devices are shipped with their default administrative passwords. These passwords are not private nor secure. Change these passwords on each device's webpage before enrolling them on your Synergis™ unit. The most secure way to change the passwords is to set up a separate network over which you can do this (this should ideally be done over HTTPS).

Delete unused interface modules from your hardware configuration

Delete any unused interface modules from your Synergis™ appliance's hardware configuration. Certain interface modules can leave open ports that make your appliance vulnerable to attacks. You can delete the unused interface modules either from Synergis™ Appliance Portal or from Config Tool. For more information, see the topics corresponding to each interface module manufacturer.

Allegion Schlage Locks

This section includes the following topics:

- ["Supported Allegion Schlage locks"](#) on page 6
- ["Supported Allegion Schlage lock features"](#) on page 8
- ["Supported Synergis appliance features for Allegion Schlage lock integration"](#) on page 11
- ["Supported Security Center features for Allegion Schlage lock integration"](#) on page 12
- ["Enrolling Allegion Schlage locks on the Synergis unit"](#) on page 15

Supported Allegion Schlage locks

Allegion Schlage AD Series lock integration requires a Mercury EP (or Honeywell) controller. For this integration, the EP controllers are viewed as interface modules, and the AD Series locks are viewed as non-intelligent devices.

Only the Mercury EP (or Honeywell) controllers communicate directly with the Synergis™ unit.

NOTE: Allegion Schlage AD Series lock integration requires Security Center 5.5 (or more recent versions) and Synergis™ Softwire 10.2 (or more recent versions). Allegion Schlage NDE & LE locks require Security Center 5.7 SR1 and Synergis™ Softwire 10.6.

Synergis™ Softwire supports the following hardware devices.

Model	Description
IP controllers	<p>A Mercury EP (or Honeywell) controller must act as an interface module between the Synergis™ unit and the AD Series locks.</p> <p>The supported controller models are:</p> <ul style="list-style-type: none"> • Mercury EP1501 controller with expansion board, supporting up to 8 AD-300 locks or 16 AD-400 locks • Mercury EP2500 controller supporting up to 16 AD-300 locks or 64 AD-400 locks • Honeywell PW6K1IC controller supporting up to 16 AD-300 locks or 64 AD-400 locks <p>See also Supported Mercury firmware versions on page 126.</p>
AD300	Allegion Schlage AD-300 hardwired electronic lock with an RS-485 interface. Must be connected to an EP controller (see datasheet).
AD400	Allegion Schlage AD-400 wireless electronic lock. Requires the PIM400 wireless communication module to connect to the EP controller (see datasheet).
PIM400-485	Allegion Schlage PIM400-485 is an RS-485 communication module, capable of connecting up to 16 AD-400 wireless locks to an EP controller (see datasheet).
PIM400-1501	Allegion Schlage PIM400-1501 is a PIM-485 module pre-wired to a Mercury EP1501 controller (see datasheet).
LE	Allegion Schlage LE wireless electronic lock. Requires an ENGAGE gateway to connect to an EP gateway. The lock connects to the gateway over Bluetooth, then the gateway connects to the EP controller directly by an RS-485 interface.
NDE	Allegion Schlage NDE wireless electronic lock. Requires an ENGAGE gateway to connect to an EP gateway. The lock connects to the gateway over Bluetooth, then the gateway connects to the EP controller directly by an RS-485 interface.

RS-485 wiring instructions

When wiring an AD300 lock, or a PIM400 or ENGAGE gateway module, to an RS-485 bus on an EP controller, wire the connectors as follows:

- TDA- to TR+
- TDB+ to TR-

Limitations

The Allegion Schlage AD, LE and NDE Series lock integration has the following limitations:

- Allegion Schlage devices and Mercury MR panels cannot be mixed on the same RS-485 bus.
- All Allegion Schlage devices connected to the same RS-485 bus must each have a different address.
- Door numbers cannot overlap between different locks on the same RS-485 bus, even if they are controlled by different PIM400 modules and AD300 locks. For example, if you have a PIM400 with doors/locks 0-10, your next PIM400 must start with door/lock number 11 or nothing will work or come online.
- An AD300 lock has a door number that is the same as its RS-485 address, and cannot overlap with any doors in the range used by a PIM400 on the same bus. For example, if you have a PIM400 at address 0 with doors/locks 0-10, you must assign your AD300 an address between 11 and 31.
- All AD400 locks under a PIM400 or an ENGAGE Gateway must have consecutive door numbers.
- Not all AD300 and AD400 messages and features are supported. The following lock features are not supported:
 - Request to enter
 - Stalled motor
 - Interior push button
 - Deadbolt switch position
 - Latch bolt
- Inputs on AD300 and AD400 locks are not configurable. This feature is not supported by the hardware.
- Manual unlock and relock commands can take more time than expected to be executed. This is because these commands rely on a Wake on Radio (WoR) message for which the timing is not precise.

Supported Allegion Schlage firmware versions

To benefit from all the features of this integration, a specific range of firmware versions must be used.

The Allegion Schlage firmware versions that Synergis™ Softwire 10.6 supports are:

Model	Minimum
AD300	AD.A.90
AD400	AD.A.90
NDE	2.10.09
LE	1.05.44

Supported Allegion Schlage lock features

Allegion Schlage AD, LE and NDE Series lock integration requires a Mercury EP (or Honeywell) controller. If the AD Series locks are disconnected from their controller, the locks cannot grant access or store offline events. However, the mechanical key, as well as the inside handle, can still be used to open the door.

Synergis™ Softwire 10.6 supports the following Allegion Schlage lock features.

Features	Supported
General characteristics	
Category of interface module	Electronic lock
Communication protocol ¹	RS-485, radio, Bluetooth
Encrypted communication	Yes ²
Online operation (connected to the Synergis™ unit)	
Supervised mode	Yes
Dependent mode	No
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	N/A
Degraded mode	No
Wireless operation	
Contact the Synergis™ unit on event	NDE & LE
Polling interval (v3 locks only)	Yes
Scheduled radio contact (Status report interval)	On Lock (NDE & LE)
Battery checks	Yes
Power fail lock settings (Fail Safe/Fail Secure)	On Lock (NDE & LE)
ENGAGE integration	NDE & LE locks ⁶
Scalability	
Maximum number of offline events	N/A
Maximum number of credentials (for autonomous decision making)	N/A
Maximum credential length (in bits)	52 ⁴

Features	Supported
Maximum number of interface modules per RS-485 channel	32
Recommended maximum number of interface modules per Synergis™ unit	N/A ⁵

¹ The Allegion Schlage lock communicates with the Mercury EP controller using RS-485 (AD300), or radio (AD400). The Mercury EP controller communicates with the Synergis™ unit over IP. LE and NDE locks connect to the ENGAGE gateway over Bluetooth.

² The AD400 (wireless lock) communicates over a 900 MHz channel using AES-128 bit encryption.

³ The AD400 model is a wireless lock. Requires the PIM400 communication module. NDE and LE locks require an ENGAGE Gateway.

⁴ Up to 8 different credential lengths are supported in *standalone mode*. More can be supported in *dependent mode*.

⁵ In the Allegion Schlage lock integration, it is the Mercury EP controller that is viewed as the *interface module*, not the Allegion Schlage lock. For the recommended number of Mercury EP controllers per Synergis™ unit, see [Supported Mercury controller features](#) on page 127.

⁶ The integration is done through Mercury EP panels. Only EP1501 and EP2500 are supported. As of Mercury Firmware version 1.25.6, all Mercury controllers support Allegion Schlage locks.

About Allegion Schlage support for distinct door modes

The new door modes supported by Allegion Schlage AD, LE, and NDE-series locks suit a wider selection of access-control contexts.

Requirements

The minimum required Synergis™ appliance firmware is 10.6 GA. LE locks are supported as of Security Center 5.7 SR1. For Apartment mode, Mercury EP firmware 1.25.6 or newer is required for full functionality.

The modes and their functions

The supported door modes are configured through the **Door mode** numeric custom field on the door in Config Tool. The modes are:

- 0 - Normal operation
- 1 - Classroom: Two swipes (within 5 seconds) by the same card unlocks the door until the same action locks it again
- 2 - Office: press button to unlock and relock
- 3 - Privacy: press button to deny all access from outside, press button or REX out to deactivate
- 4 - Apartment: press button or REX out to unlock, stays unlocked until button press or swipe to relock

Edit custom field

Definition

Entity type:  Door

Data type: Numeric

Name: Door mode

Default value: 0

Value must be unique

Layout (Optional)

Group name:

Priority: 1

Security

Visible to administrators and:

 Admin

Cancel Save and close

Limitation: Current limitations for locks that are not set to mode 0:

- Neither *Card and PIN* nor *DoubleSwipe* work
- *Unlock schedules* and *Lockdown* might not work properly

Supported Synergis™ appliance features for Allegion Schlage lock integration

Not all Synergis™ appliance features are supported with the integration of Allegion Schlage locks.

Allegion Schlage locks are connected to the Synergis™ appliance through a Mercury EP controller. For Synergis™ appliance features supported by the Allegion Schlage lock integration, see [Supported Synergis™ appliance features for Mercury controller integration](#) on page 129.

Supported Security Center features for Allegion Schlage lock integration

Not all Security Center access control features are supported with the integration of Allegion Schlage locks. The Allegion Schlage lock integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	Yes ¹	
	Extended grant time	Yes	
	Entry time (Standard/Extended) ²	No	
	Door relock - options	Limited ³	
	When door is unlocked by schedule - options	Online	
	Door held - options	Yes	
	Door forced open - options	Limited ⁴	
	Unlock schedules	Yes	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	Yes	
	Time to ignore REX after granting access (in seconds)	Online	
	Ignore REX events while door is open (On/Off)	Online	
	Time to ignore REX after door closes (in seconds)	Online	
	Visitor escort and two-person rule		
Maximum delay between card presentation (in sec.)	No		
Enforce two-person rule (On/Off) on Door side	No		
Manual actions on doors in Security Desk ⁵	Manually unlock doors	Yes	
	Reader shunting (activate/deactivate reader)	Yes	
	Override unlock schedules	Yes	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	Yes ⁶
	Battery fail (<i>Low battery</i>)	Yes
	Door open/closed	Yes
	Door locked/unlocked	Yes
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
	Deadbolt (<i>Secured, Released</i>)	No
	Key override	Yes ⁷
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	No
	Visitor escort rule (On/Off)	No
	Interlock	No
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	No
	Presence timeout (forget area presence after a certain delay)	No
	Strict (antipassback checked on both area entrance and exit)	No
	On schedule	No
	Global antipassback	No
	First-person-in rule	
	Enforce on door unlock schedule	No
	Enforce on access rules	No
	Elevator control	Elevators
Zone management	I/O zone	No
	Hardware zone	No

¹ The maximum supported value is 255 seconds.

² Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the

door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

³ A door that is configured to relock with a timeout after opening features a **Relock on close** option, which still locks after the grant timeout.

⁴ For the **Reader buzzer behavior** setting, the options *Suppressed* and *Suppressed when door closes* are supported in both online and offline operation modes. The option *Suppressed when access is granted* is treated as *Suppressed when door closes*.

⁵ The Synergis™ unit must be connected to the Access Manager.

⁶ N/A for NDE and LE locks.

⁷AD series locks only.

Enrolling Allegion Schlage locks on the Synergis™ unit

Because the Synergis™ unit does not communicate with the Allegion Schlage devices, you must enroll these devices through a Mercury EP (or Honeywell) controller, using the Config Tool.

Before you begin

- Configure a different RS-485 address on each Schlage device (AD Series lock and PIM400 module) using the Schlage Pidion hand held device (see [Limitations](#)), and connect the lock and module to your Mercury EP controller. For more information, see the [Schlage Utility Software User Guide](#).
- [Configure the assigned static IP address on the EP controller](#).

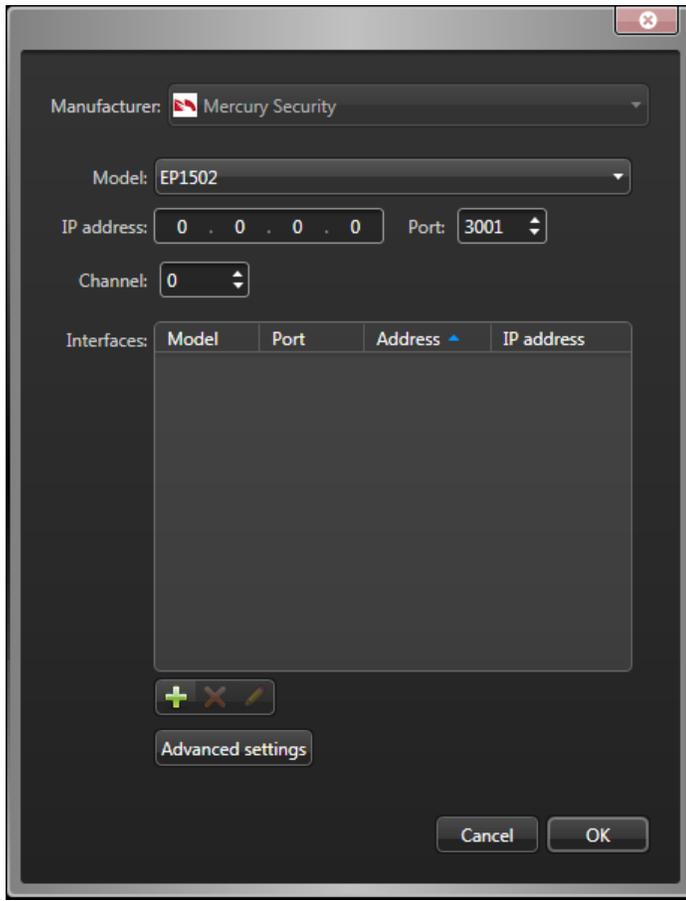
What you should know

Mercury controllers enrolled on a Synergis™ unit are not visible from the Synergis™ Appliance Portal *Hardware* page.

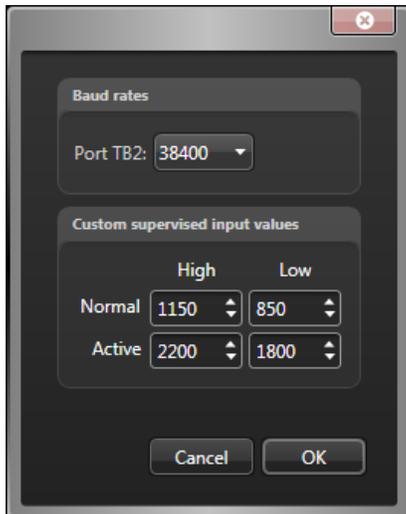
On the Synergis™ unit, each EP controller must be assigned a unique channel ID. All EP controllers have RS-485 buses to which the Schlage devices (AD-300 and PIM400) are connected. Each Schlage device connected to the same RS-485 bus must have a unique RS-485 address.

To enroll Allegion Schlage locks to the Synergis™ unit:

- 1 From the Config Tool home page, open the *Access control* task.
- 2 Click **Roles and units**, and then click the Synergis™ unit (🌐).
- 3 Click **Peripherals**, and then click **Add an item** (+).

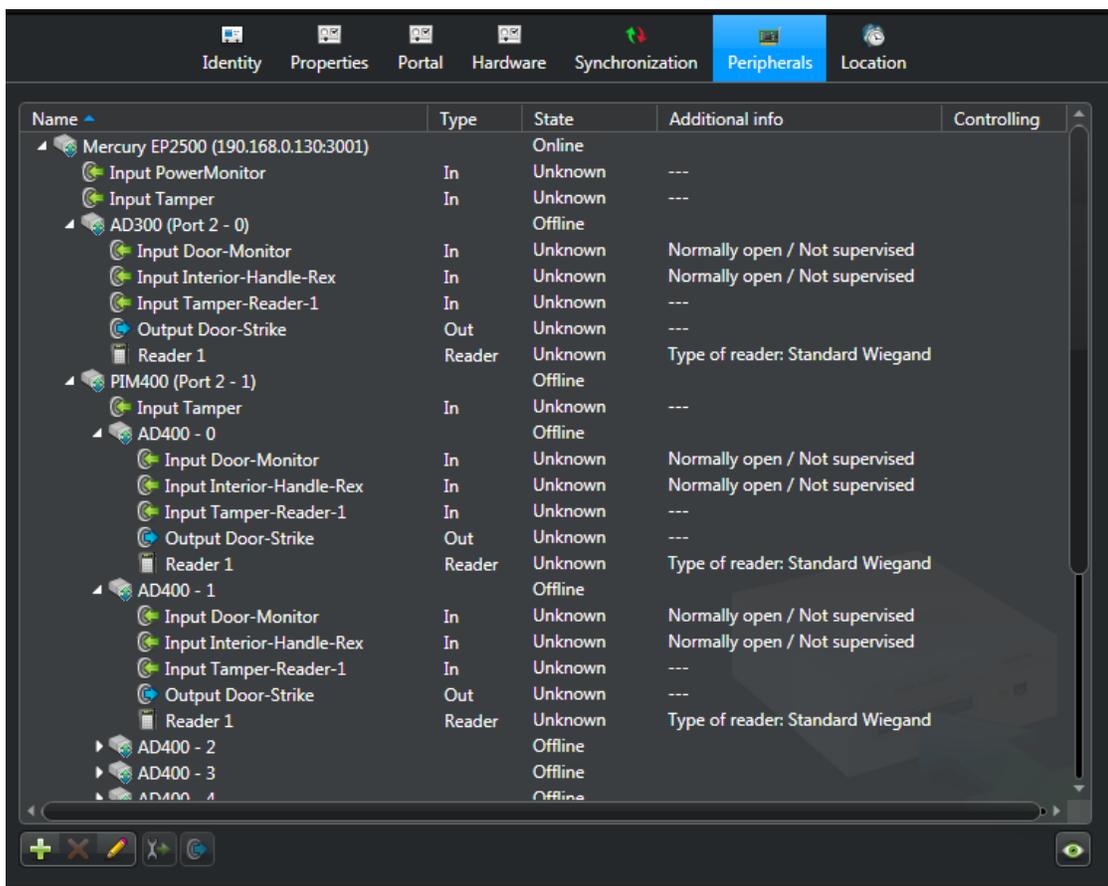


- 4 Enter the following information:
 - **Model:** Model of the controller.
 - **IP address:** Static IP address assigned to the controller by your IT department.
 - **Port:** Communication port (default=3001). The port must match the value configured on the Mercury Device Manager web page.
 - **Channel:** Channel ID corresponding to this controller. The channel ID can be any value between 0 and 63, and must be unique within the Synergis™ unit. Once assigned, it must not be changed.
- 5 Add the Allegion Schlage devices that are attached to your EP controller.
 - a) At the bottom of the *Interfaces* group, click **Add an item** (+).
 - b) In the dialog box that appears, select the **Model** (AD300 or PIM400), the **Port**, and the **Address** (0 to 31).
 - c) (PIM400 only) In **Low**, enter the first door number linked to the PIM400, and in **Count**, enter the number of doors linked to the PIM400.
All door numbers ranging from **Low** to **Low+Count** must correspond to an AD-400 wireless lock.
 - d) Click **OK**.
 - e) Repeat as necessary.
- 6 (Optional) Click **Advanced settings** to change the advanced settings.
The available settings depend on the selected controller model. You can typically change the baud rate of the available serial port, and the custom supervised input values.



- 7 Click **OK** at the bottom of the dialog box.
- 8 Click **Apply** (✓).

The Mercury controller with all its attached downstream panels and peripheral devices appear in the **Peripherals** tab.



NOTE: Adding interface modules to the Synergis™ unit causes the unit to perform a software restart. During this process, the Synergis™ unit and all peripherals attached to it appear offline (in red).

- 9 Select each of the discovered I/O devices and readers, and [configure their properties](#) as necessary. For OSDP (Secure Channel) readers, see [Adding OSDP \(Secure Channel\) readers to an EP controller](#) on page 140.

- 10 Test your wiring and configuration by triggering the inputs and outputs.
The triggered I/O changes state in real time on screen.

NOTE: Reader activities are not shown in the **Peripherals** tab.

Enrolling ENGAGE-integrated Allegion Schlage locks

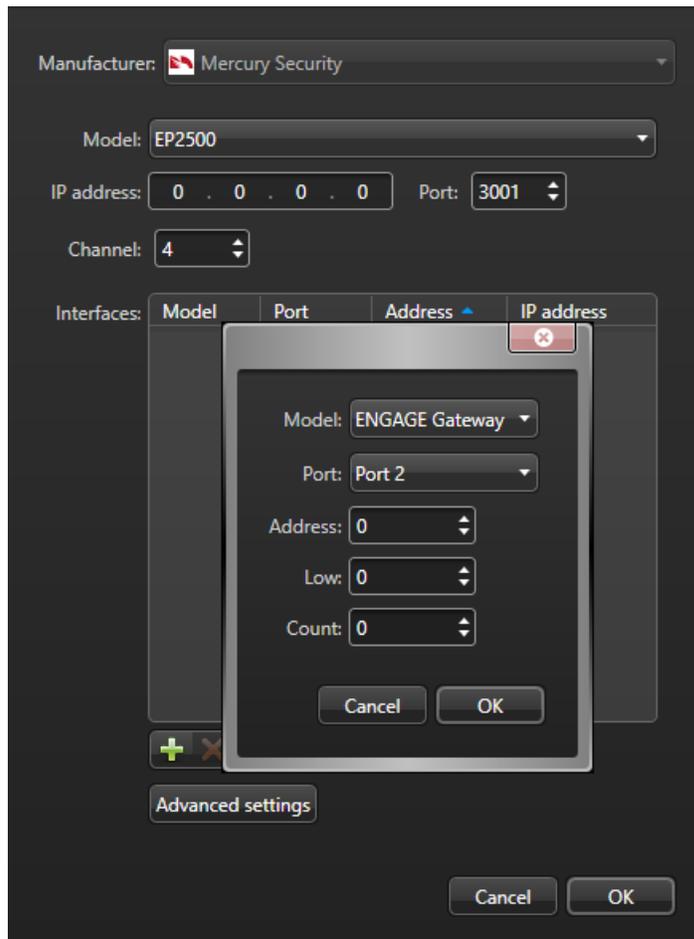
Schlage's ENGAGE platform allows credentials to be stored not only on key cards, but also on compatible smart phones. Integration is done through Mercury EP1501 or EP2500 panels.

Before you begin

Initial setup and lock pairing to the ENGAGE Gateway is done through the Allegion ENGAGE mobile app, which is available for Android and iOS devices. This is done by tapping Connect, then tapping the plus sign in the corner and following the steps. When this is done, enroll the locks in Config Tool.

What you should know

The process for enrolling Allegion Schlage NDE and LE locks with ENGAGE integration in Config Tool is the same as that for enrolling the PIM400, except that you select ENGAGE Gateway when you set the interface.



To enroll ENGAGE-enabled Allegion Schlage locks to the Synergis™ unit:

- 1 Enroll the Allegion Schlage NDE or LE locks as described in [Enrolling Allegion Schlage locks on the Synergis™ unit](#) on page 15.

- At step 5, select the ENGAGE Gateway from the **Model** drop-down menu after clicking **Add an item** (+) in the *Interfaces* group.

The ENGAGE Gateway with all its connected downstream panels and peripheral devices is listed in the **Peripherals** tab.

Mercury EP2500 (10.23.0.34:3015)		Online	Number of credentials synced...
Input InternalBatteryMonitor	In	Normal	---
Input PowerMonitor	In	Normal	---
Input Tamper	In	Normal	---
AD300 (Port 2 - 3)		Offline	
ENGAGE Gateway (Port 3 - 1)		Online	
Input BLE tamper	In	Normal	---
Door - 10		Online	
Door - 11		Online	
Input Connection-Reader-1	In	Active	---
Input Door-Monitor	In	Normal	Normally open / Not supervis... 11
Input Interior-Handle-Rex	In	Normal	Normally open / Not supervis... 11
Input Interior-Push-Button	In	Normal	---
Input Low-Battery	In	Normal	---
Input Magnetic-Tamper	In	Normal	---
Input Tamper-Reader-1	In	Normal	---
Output Door-Strike	Out	Normal	---
Reader 1	Reader	Active	Type of reader: Standard Wie... 11
Door - 12		Online	
Input Connection-Reader-1	In	Active	---
Input Door-Monitor	In	Normal	Normally open / Not supervis... 12
Input Interior-Handle-Rex	In	Normal	Normally open / Not supervis... 12
Input Interior-Push-Button	In	Normal	---
Input Low-Battery	In	Normal	---
Input Magnetic-Tamper	In	Normal	---
Input Tamper-Reader-1	In	Normal	---
Output Door-Strike	Out	Normal	---
Reader 1	Reader	Active	Type of reader: Standard Wie... 12
Door - 13		Online	
Input Connection-Reader-1	In	Active	---
Input Door-Monitor	In	Normal	Normally open / Not supervis... 13
Input Interior-Handle-Rex	In	Normal	Normally open / Not supervis... 13
Input Interior-Push-Button	In	Normal	---
Input Low-Battery	In	Normal	---
Input Magnetic-Tamper	In	Normal	---
Input Tamper-Reader-1	In	Normal	---
Output Door-Strike	Out	Normal	---
Reader 1	Reader	Active	Type of reader: Standard Wie... 13

Assa Abloy Aperio-Enabled Locks

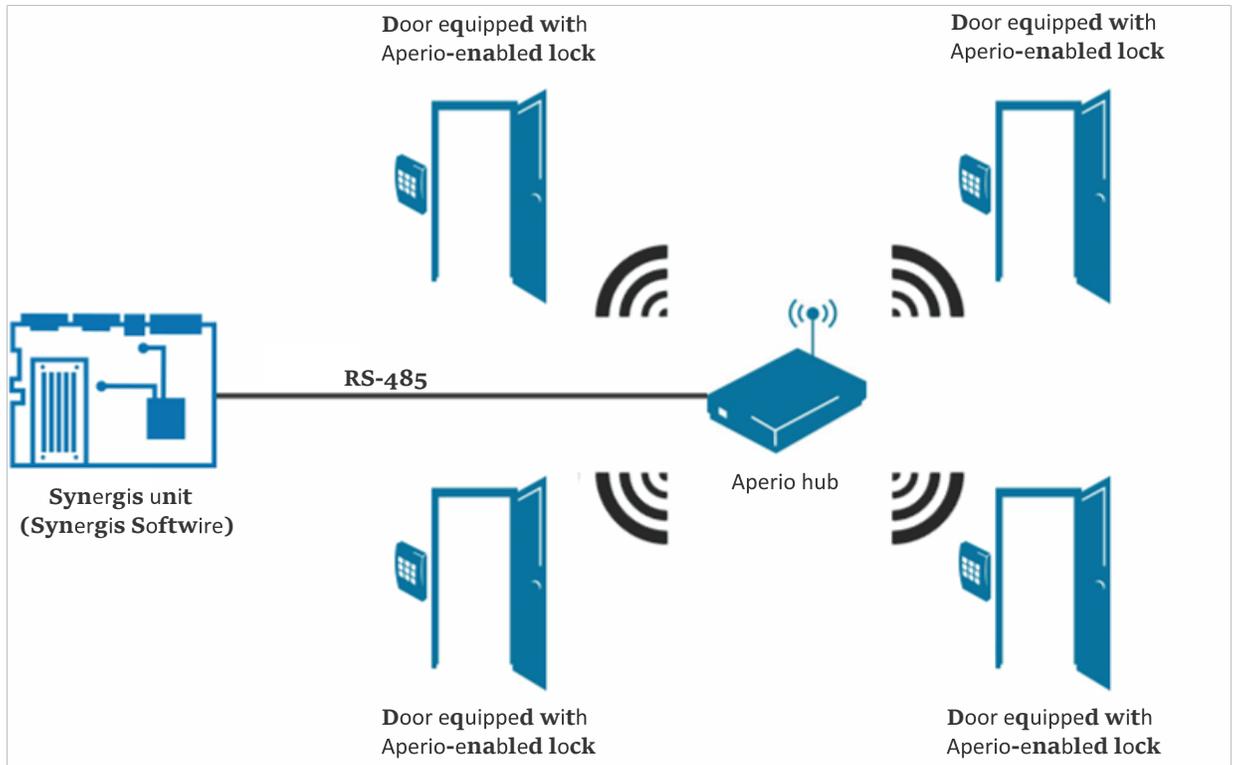
This section includes the following topics:

- ["Aperio integration overview"](#) on page 21
- ["Supported Aperio-enabled locks"](#) on page 22
- ["Supported Aperio-enabled lock features"](#) on page 23
- 25 • ["Supported Synergis appliance features for Aperio-enabled lock integration"](#) on page
- 26 • ["Supported Security Center features for Aperio-enabled lock integration"](#) on page
- ["Pairing the Aperio-enabled locks with the hub"](#) on page 29
- ["Enrolling the Aperio-enabled locks"](#) on page 33
- ["Configuring doors equipped with an Aperio-enabled lock"](#) on page 35

Aperio integration overview

Aperio-enabled locks are wireless locks that communicate with an Aperio hub on the 2.4 GHz band. This hub then in turn, communicates with the Synergis™ unit on an RS-485 channel. The Synergis™ unit makes all access control decisions.

The following diagram shows how the Synergis™ unit communicates with the Aperio-enabled locks.



Supported Aperio-enabled locks

For Aperio integration, the Synergis™ unit connects to the Aperio-enabled locks through a communication hub that is connected to one of its RS-485 channels. Each Aperio-enabled lock is viewed as an interface module.

Synergis™ Softwire supports the following Aperio-enabled devices.

Model	Description	Platform release	Certification
A100	Keyless entry control	-	Supported by design
AH30	Wireless communication hub. Each hub controls up to 8 Aperio locks	3.4.0 (v3) ¹ 2.6.6	Certified Supported by design
AS100	Door position sensor	-	Supported by design
C100	Cylinder lock (European model)	-	Supported by design
E100	Standard Escutcheon RFID-Reader (European model)	-	Supported by design
IN100 v3	v3 lock	3.5.0	Certified
IN100	-	-	Supported by design
K100	K100 Cabinet Lock	-	Supported by design
KS100	KS100 Server Cabinet Lock	-	Supported by design
L100	Electronic lock RFID-Reader (European model)	-	Supported by design
M100	Wire-free retrofit mortise	-	Supported by design
PR100 HF/LF	P100 high and low frequency locks	2.6.6	Supported by design
R100	Surface-mounted wireless reader	-	Supported by design

¹ The minimum supported version for AH30 to work with IN100 v3 locks is 3.2.0

Supported Aperio-enabled lock features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following Aperio-enabled lock features.

Features	Supported
General characteristics	
Category of interface module	Electronic lock
Communication protocol	RS-485 ¹
Encrypted communication	No ²
Online operation (connected to the Synergis™ unit)	
Supervised mode	Yes ³
Dependent mode	No
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	N/A
Degraded mode	No
Wireless operation	
Contact the Synergis™ unit on event	On read
Polling interval (v3 locks only)	Yes
Scheduled radio contact (Status report interval)	1 - 60 min.
Battery checks	Yes
Power fail lock settings (Fail Safe/Fail Secure)	No
Scalability	
Maximum number of offline events	N/A
Maximum number of credentials (for autonomous decision making)	N/A
Maximum credential length (in bits)	256
Maximum number of interface modules per RS-485 channel	64 ⁴
Recommended maximum number of interface modules per Synergis™ unit	64

¹ Between the Synergis™ unit and the Aperio wireless communication hub.

² Communication can be encrypted between the Aperio hub and the lock.

³ Aperio-enabled locks can hold five credentials that work offline.

⁴ Each channel supports eight hubs, and each hub supports eight locks, for a maximum of 64 locks per channel. If the Synergis™ unit is controlling 64 locks, spread the locks evenly on all four channels for a better performance.

Supported Synergis™ appliance features for Aperio-enabled lock integration

Not all Synergis™ appliance features are supported with the integration of Aperio-enabled locks from Assa Abloy.

The Aperio-enabled lock integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Softwire](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability)	
Manual enrollment (<i>Add hardware</i> dialog box)	Yes
Automatic enrollment (Scan button)	Yes
Property configuration	Limited ¹
Configuration cloning (Clone button)	Yes
I/O diagnostics (live monitoring of inputs, relays, and readers)	Yes ²
Interface module firmware display	Hub only
Interface module firmware upgrade (apply recommended firmware)	No
Access control behavior (Synergis™ unit-wide settings) ²	
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	No
Do not generate 'DHO' events when door is unrestricted	Yes
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	Yes
Maximum PIN length in digits	15 ⁴
Degraded mode settings	N/A
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	No

¹ Connection parameters only.

² Output relays set in the *I/O diagnostics* page may not take effect immediately, depending on the **Status report interval** and the **Polling interval** (v3 locks only) settings.

³ The door behavior settings are overwritten by the individual door settings configured in Security Center.

⁴ PINs with less than four digits are not accepted.

Supported Security Center features for Aperio-enabled lock integration

Not all Security Center access control features are supported with the integration of Aperio-enabled locks from Assa Abloy.

The Aperio-enabled lock integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	Yes	
	Extended grant time	Yes	
	Entry time (Standard/Extended)	No	
	Door relock - options	No	
	When door is unlocked by schedule - options	Yes	
	Door held - options	Limited ¹	
	Door forced open - options	Limited ¹	
	Unlock schedules	Yes ²	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	No ³	
	Time to ignore REX after granting access (in seconds)	Yes	
	Ignore REX events while door is open (On/Off)	Yes	
	Time to ignore REX after door closes (in seconds)	Yes	
Visitor escort and two-person rule			
Maximum delay between card presentation (in sec.)	Yes		
Enforce two-person rule (On/Off) on Door side	Yes		
Manual actions on doors in Security Desk ⁴	Manually unlock doors	v3 locks only	
	Reader shunting (activate/deactivate reader)	Yes	
	Override unlock schedules	Yes ²	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	N/A
	Battery fail (<i>Low battery</i>)	Yes
	Door open/closed	Yes
	Door locked/unlocked	Yes
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
	Deadbolt (<i>Secured, Released</i>)	Yes
	Key override	Yes ⁵
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	Yes
	Visitor escort rule (On/Off)	Yes
	Interlock	No
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	Yes ⁶
	Presence timeout (forget area presence after a certain delay)	Yes
	Strict (antipassback checked on both area entrance and exit)	N/A
	On schedule	Yes
	Global antipassback	Yes
	First-person-in rule	
	Enforce on door unlock schedule	Yes
	Enforce on access rules	Yes
	Elevator control	Elevators
Zone management	I/O zone	No
	Hardware zone	No

¹ The **Reader buzzer behavior** options are not supported.

² Update depends on **Polling interval** (v3 locks) or **Status report interval** (other than v3 locks).

- ³ The option **Automatically grant REX** must always be set to **OFF** in Config Tool.
- ⁴ The Synergis™ unit must be connected to the Access Manager.
- ⁵ Not all Aperio-enabled locks support the key override sensor. Confirm with the manufacturer to know the exact sensors that are supported for each model.
- ⁶ Not recommended for Card-In/REX-Out doors, because a cardholder's presence in the area cannot be verified

Pairing the Aperio-enabled locks with the hub

Before you can enroll the Aperio-enabled locks on your Synergis™ unit, you must pair the Aperio-enabled locks with the hub using the *Aperio Programming Application (APA)*.

Before you begin

Make sure you have the following:

- **Aperio Online Programming Application Manual.** Instruction manual for the installation and use of all Aperio applications.
- **Aperio Programming Application (APA).** Main application used to configure the Aperio hub and locks. Both the hub and the locks are configured through the wireless connection.
- **USB dongle.** Hardware device that must be plugged in to the computer running the APA.
- **TriBee Bootloader.** Includes the USB dongle driver.
- [Supported firmwares](#)
- A computer for running the APA.
- A card that is compatible with the lock's reader (used to activate the lock pairing).

The credential on the card does not need to be enrolled in Security Center.

To pair the Aperio-enabled lock with the hub:

- 1 Set the EAC address (1 - 15) on the hub using the DIP switches.

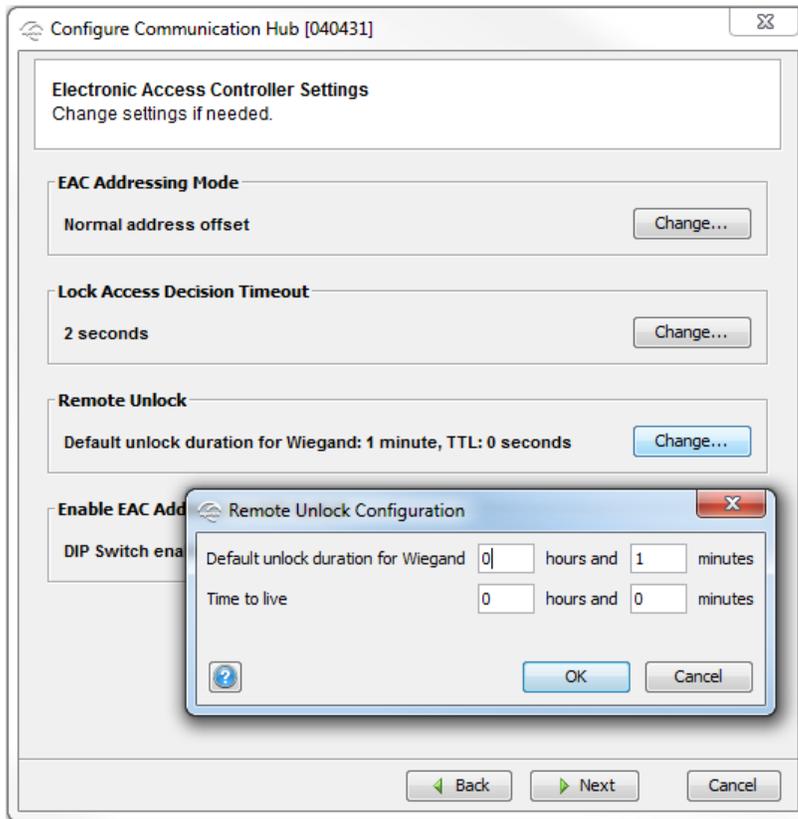
IMPORTANT: Up to eight hubs can be connected to the same RS-485 channel in a daisy chain, but each hub must use a different EAC address.

- 2 Power on the hub.
- 3 Plug in the USB dongle to your computer.
- 4 Install *TriBee Bootloader* (installs the USB dongle driver).
- 5 Install *Aperio Programming Application (APA)*.
- 6 Open APA (see the *Aperio Online Programming Application Manual* for instructions). Right-click a communication hub, a lock, or a sensor to show the available functions.
- 7 Using APA, update the firmware on the hub and the locks.

Check the [supported firmware](#) list before updating the firmware.

BEST PRACTICE: Always upgrade the communication hub before upgrading the locks or sensors. When upgrading AH30 communication hubs that use the DIP switch for EAC addressing, always check that the DIP switch is set to the correct EAC address. If DIP 5 (Pairing mode) is set to active during an upgrade, the communication hub starts using a different EAC address.

- 8 Configure the hub.
- 9 (Communication hub with a firmware earlier than 2.6.5) Enable the **Remote Unlock** option to use Security Center unlock schedules.
With firmware version 2.6.5 and later, the **Remote Unlock** option is enabled by default.
- 10 Enter a value for **Time to live** in the *Remote Unlock Configuration* dialog box and click **OK**.



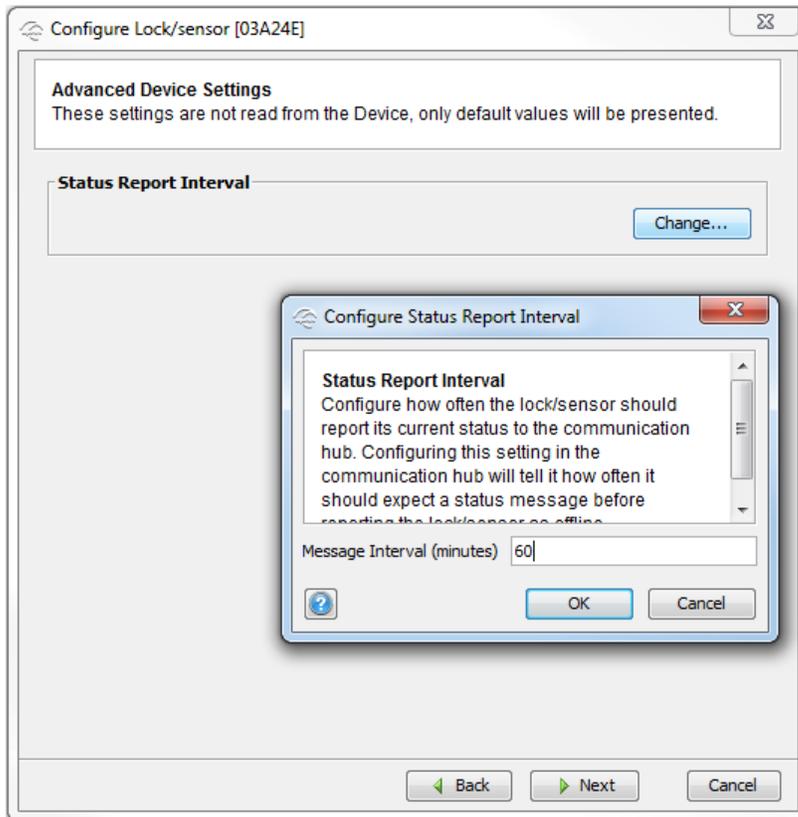
This time indicates how long the **Remote Unlock** command (grantAccessSequence) is present in the communication hub. This setting must always be longer than the **Status Report Interval** set in the lock.

You can ignore the value of **Default unlock duration for Wiegand**.

- 11 (Excluding v3 locks) If unlock schedules are used, enter a value for the **Status Report Interval** in the range 5 - 15 minutes.

The **Status Report Interval** is normally set to 60 minutes. Lowering the status interval time decreases the battery life of the product. Because the **Status Report Interval** is used by the communication hub to detect if the lock has gone offline, any changes to this interval must be made on both the lock and the communication hub. If only one lock is paired with the communication hub, then this is done automatically. If more than one lock is paired with the communication hub, then you must set the **Status Report Interval** through the communication hub. Right-click the hub and set a value that is equal or higher than the longest **Status Report Interval** for the paired locks.

NOTE: With v3 locks, the **Status Report Interval** setting is only used to report the online status of the lock. It is the **Polling Interval** that is used to minimize the time lag for starting and ending the unlock schedule.



If more than one lock is paired with the communication hub, then the **Status Report Interval** must also be set on the lock.

12 For each wireless lock, do the following:

a) Right-click and select **Communication hub > Pair with lock or sensor**.

The pairing process starts.

b) Hold the credential at the lock, or engage the magnet for the sensor to pair the hardware with the communication hub.

The hub automatically assigns an EAC address to the lock.

c) Write down the EAC address (1 to 127) assigned to the lock.

The hub's EAC address is incorporated into the lock's EAC address. To obtain the hub's EAC address from the lock's EAC address, use the following formula:

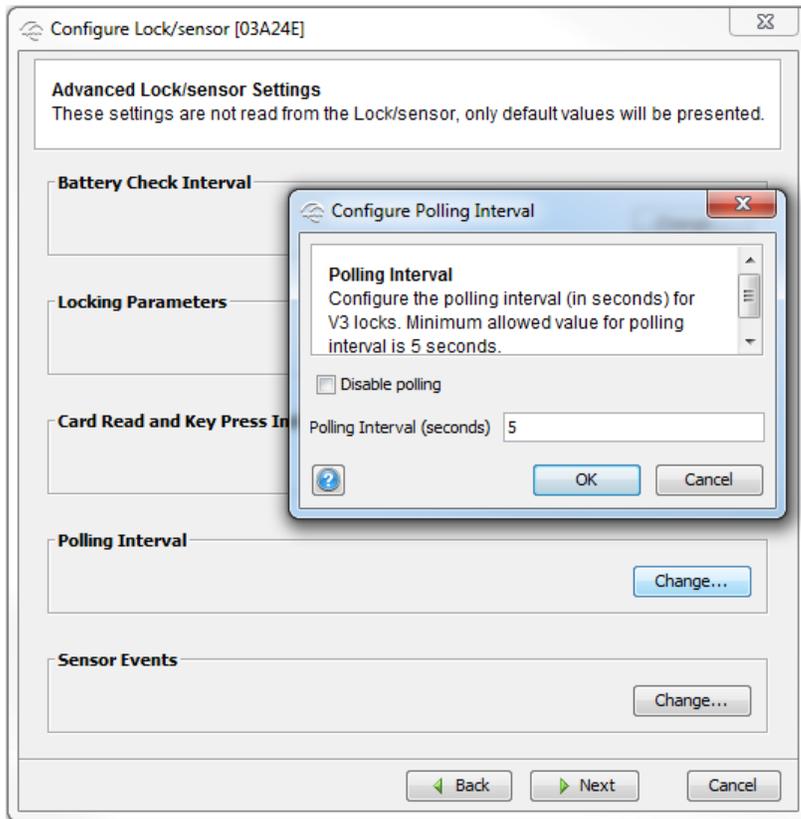
Hub's EAC address = Lock's EAC address modulo 16

or

Hub's EAC address = (Remainder of Lock's EAC address) divided by 16

13 (v3 locks only) Set the **Polling Interval** to 5 seconds (the minimum time).

This is to minimize the time lag for starting and ending the unlock schedule, which reduces the reaction time of the locks. It also allows the manual unlock commands issued from Security Desk to work within 5 seconds. It is not recommended to use manual unlock commands on locks other than v3 because the command only works after 1 minute or longer (depending on the **Status Report Interval**).



14 After all locks are paired, set the hub to use secure radio communication (**Customer mode**).

After you finish

Enroll the locks on the Synergis™ unit.

Enrolling the Aperio-enabled locks

For the Synergis™ unit to communicate with the Aperio-enabled locks, you must enroll them with Synergis™ Appliance Portal.

Before you begin

- [Pair the Aperio-enabled locks to the hub.](#)
- Connect the hub to one of the RS-485 channel (A, B, C, or D) as follows:
 - Connect the hub's A connector to the "+" of the channel.
 - Connect the hub's B connector to the "-" of the channel.

To enroll the Aperio-enabled locks:

- 1 Log on to the Synergis™ unit.
- 2 Click on **Configuration** > **Hardware**.
- 3 At the top of the *Hardware* column, click **Add** (+).
- 4 In the *Add hardware* dialog box, select **Aperio** as the **Hardware type**.
- 5 Select the **Channel** (A, B, C, or D).
- 6 Select **Aperio** as the **Interface module type**.
- 7 Specify the locks you want to enroll.

You can enroll the locks automatically or manually.

TIP: If you know the EAC addresses of the locks and you only have a few to enroll, it would be faster if you enroll them manually.

Do one of the following:

- To enroll automatically, click **Scan**.

The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

If Synergis™ Appliance Portal does not find all attached interface modules, try the manual enrollment.

- To enroll manually, enter the lock's EAC address (1 to 127) written down while [pairing the lock to the hub](#), and click **Add**.

Repeat as necessary to configure all modules connected to the same channel.

Add hardware

Hardware type
Aperio

Channel
B

Interface module type
Aperio

Lock EAC address
1

Interface module type	Lock EAC address
Aperio	0

Add

Scan Cancel Save

- 8 Click **Save**.
The hardware type, channel, and interface module you just added appear in the *Hardware configuration* page.
- 9 Select a lock to view its properties in the right pane.
Both the hub's and the lock's EAC address are indicated.
- 10 At the bottom of the page, click **Save**.
- 11 Test your interface module connection and configuration from the I/O diagnostics page.
For information about testing interface modules, see the *Synergis™ Appliance Configuration Guide*.

After you finish

- Enroll the Synergis™ unit in Security Center (see the *Synergis™ Appliance Configuration Guide*).
- [Configure the doors equipped with Aperio-enabled locks.](#)

Configuring doors equipped with an Aperio-enabled lock

To make sure that you do not receive duplicate *Door locked* and *Door unlocked* events in Security Desk, you must set the **Automatically grant REX** option to OFF for all doors equipped with an Aperio-enabled lock.

Before you begin

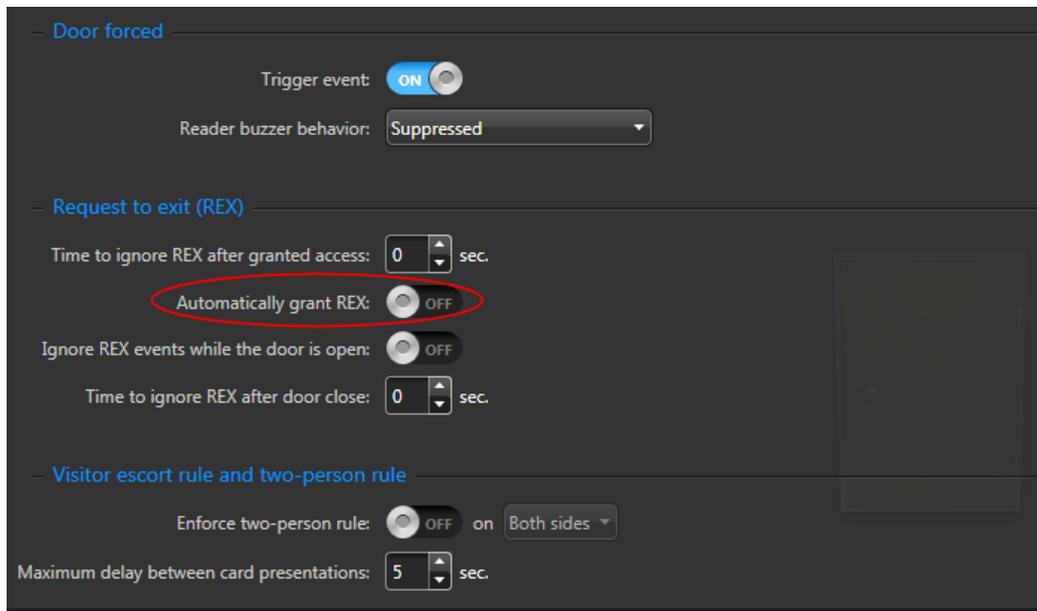
- [Enroll the Aperio-enabled locks on the Synergis™ unit.](#)
- Enroll the Synergis™ unit in Security Center (see the *Synergis™ Appliance Configuration Guide*).

What you should know

The Aperio-enabled lock uses a mechanical REX. It is not the Synergis™ unit that controls the unlocking of the door when REX is triggered. Enabling this option in the door configuration causes the *Door locked* and *Door unlocked* events to be received twice in Security Desk.

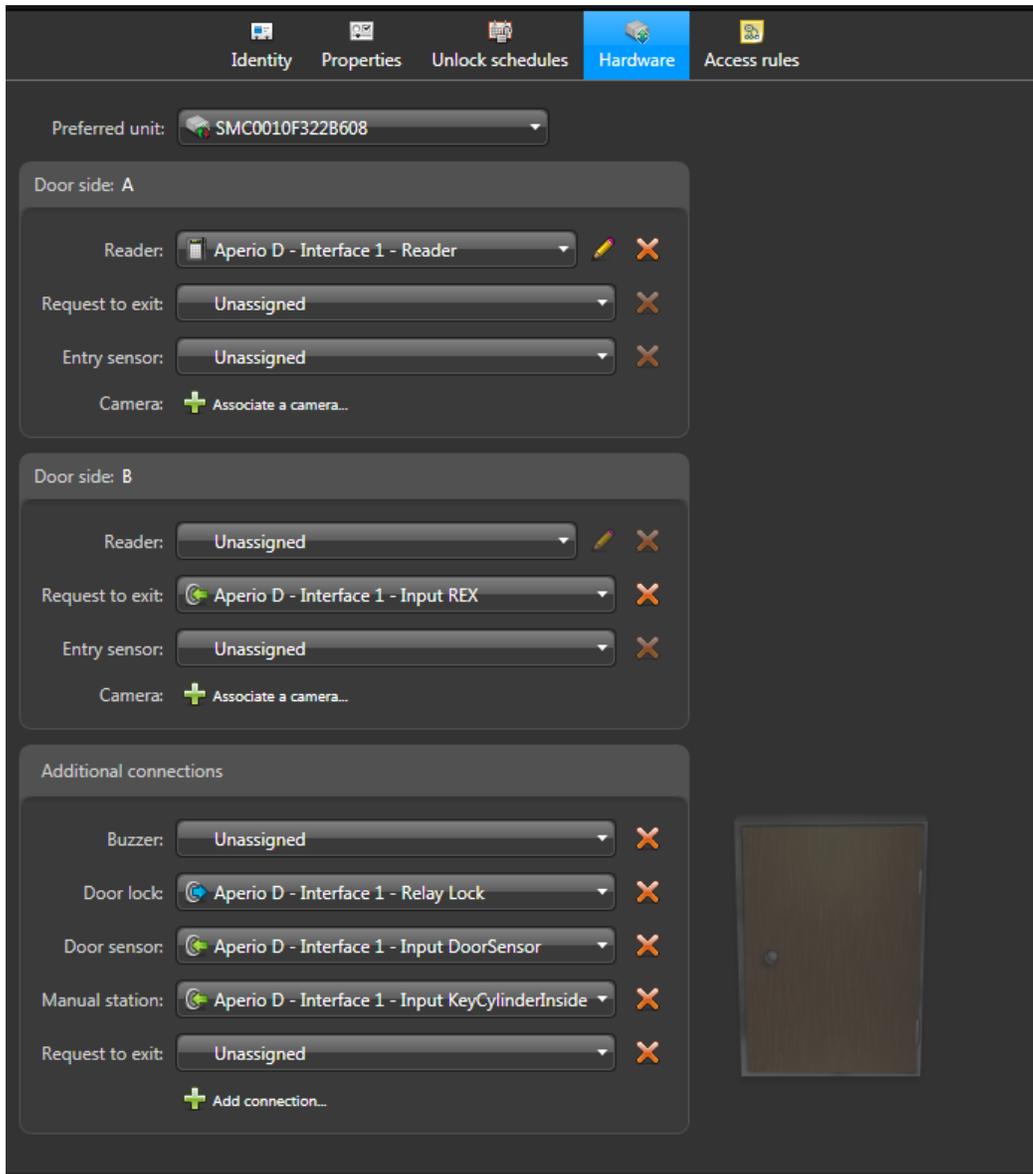
To configure a door equipped with an Aperio-enabled lock:

- 1 Connect to Security Center with Config Tool.
- 2 In the *Area view* task, select the door that is using the Aperio-enabled lock.
- 3 Select the **Properties** tab.
- 4 Under the *Request to exit (REX)* section, set **Automatically grant REX** to **OFF**.



- 5 Select the **Hardware** tab, and then select the Synergis™ unit that controls the lock.

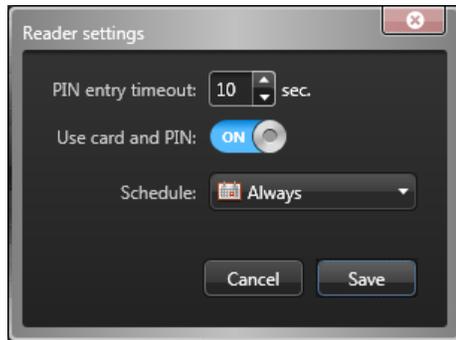
TIP: All peripherals corresponding to the same lock are named with the same prefix “Aperio X - Interface n”, where X is the channel name (A, B, C, or D), and n is the lock’s EAC address.
- 6 On the door entry side, assign the reader corresponding to the door.
- 7 On the door exit side, assign the REX sensor corresponding to the door.
- 8 Under **Additional connections**,
 - assign the lock relay to **Door lock**, and
 - assign the door sensor input to **Door sensor**.
 - assign the *KeyCylinderInside* or the *KeyCylinderOutside* to **Manual station**, if applicable.



- 9 If the reader ought to work in “Card and PIN” mode, make sure you configure a timeout long enough for the cardholder to enter the PIN.

The default access timeout of 5 seconds is not long enough for Aperio-enabled locks. After presenting their credential at the door, the cardholder has to wait until the LED turns green before entering the PIN. That process invariably takes longer than 5 seconds.

- 1 Click **Reader settings** (🔧) beside the **Reader**.
- 2 In the *Reader settings* dialog box, set **Use card and PIN** to **ON**
- 3 Set the **PIN entry timeout** to the desired duration (we recommend 10 seconds).



4 Click **Save**.

10 Click **Apply** (✓) to save your changes.

Assa Abloy IP Locks

This section includes the following topics:

- ["Supported Assa Abloy IP locks"](#) on page 39
- ["Supported Assa Abloy IP lock features"](#) on page 40
- 47 • ["Supported Synergis appliance features for Assa Abloy IP lock integration"](#) on page
- 49 • ["Supported Security Center features for Assa Abloy IP lock integration"](#) on page
- ["Configuration overview for Assa Abloy IP locks"](#) on page 52
- ["Enrolling IP locks connected to the Synergis unit"](#) on page 53
- ["Disabling encryption on Assa Abloy IP locks"](#) on page 57
- ["Monitoring the battery status of WiFi locks"](#) on page 58

Supported Assa Abloy IP locks

For Assa Abloy IP lock integration, each IP lock is viewed as an interface module.

Synergis™ Softwire supports the following Assa Abloy IP locks.

Brand	Name	Type	Supported firmware
Corbin Russwin	Access 700 PIP1 (Px)	PoE	Supported by design
Corbin Russwin	Access 700 PIP1 (Cx)	PoE	Supported by design
Corbin Russwin	Access 700 PWI1 (Cx)	WiFi	3_0p05_cx_v2751
Corbin Russwin	Access 700 PWI1 (Px)	WiFi	Supported by design
Corbin Russwin	Access 800 IP1 (Sx)	PoE	Supported by design
Corbin Russwin	Access 800 WI1 (Sx)	WiFi	Supported by design
Corbin Russwin	IN120 (Cx) (Installation instructions)	WiFi	Supported by design
Corbin Russwin	IN220 (Cx)	PoE	Supported by design
SARGENT	IN120 (Cx) (Installation instructions)	WiFi	3_0p05_cx_v2751
SARGENT	IN220 (Cx)	PoE	3_0p05_cx_v2751
SARGENT	Passport 1000 P1 (Cx)	PoE	3_0p05_cx_v2751
SARGENT	Passport 1000 P1 (Px)	PoE	3_0n18_px_pfm
SARGENT	Passport 1000 P2 (Cx)	WiFi	Supported by design
SARGENT	Passport 1000 P2 (Px)	WiFi	3_0n18_px_pfm
SARGENT	Profile Series v.S1 (Sx)	PoE	3_0n18_sx_pfm, 3_0n18_hx_pfm ¹
SARGENT	Profile Series v.S2 (Sx)	WiFi	3_0n18_sx_pfm, 3_0n18_hx_pfm ¹

¹ Sx controllers running Hx firmware require the option **Firmware type** to be set to **Hx** in the *Hardware* tab of the Synergis™ unit in Config Tool.

Supported Assa Abloy IP lock features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following Assa Abloy IP Lock features.

Features	Supported
General characteristics	
Category of interface module	Intelligent lock
Communication protocol	IP
Encrypted communication	Yes
Escape and return mode (see How to enable)	Yes
Passage mode (see How to enable)	Yes
Privacy mode (see How to enable)	Yes
Online operation (connected to the Synergis™ unit)	
Supervised mode	Yes ¹
Dependent mode	No
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	Yes
Degraded mode	N/A
Wireless operation (WiFi only)	
Contact the Synergis™ unit on event	Yes ²
Scheduled radio contact (Status report interval)	Yes ³
Battery checks	Yes ⁴
Power fail lock settings (Fail Safe/Fail Secure)	Yes ⁵
Configurable Radio Wakeup events (see How to configure)	Yes
Scalability	
Maximum number of offline events	10,000 ⁶
Maximum number of credentials (for autonomous decision making)	10,000 ⁷
Maximum credential length (in bits)	140

Features	Supported
Maximum number of interface modules per RS-485 channel	N/A
Recommended maximum number of interface modules per Synergis™ unit	128

¹ The WiFi lock might take up to 15 seconds to unlock for unknown credentials not yet synchronized to the lock. Badging a second time might be required.

² By default, the WiFi lock contacts the Synergis™ unit on the following events: *Access denied* (for any reason), *Door forced open*, and *Door open too long*.

³ The default WiFi radio wake up schedule is every day at 0:00 UTC time.

⁴ The default battery check schedule is every day at 23:00 UTC time.

⁵ The default Power fail lock setting is *Fail Secure*, meaning the door is locked when power is off.

⁶ There is not always a one-to-one match between an offline log entry and a Security Center event.

⁷ Cx type locks only; legacy Sx and Px type locks remain at 2,400 credentials. when legacy Px locks are configured for *Card and PIN*, the capacity drops to 1,200 credentials.

About the Radio Wakeup events feature for Assa Abloy WiFi locks

Wakeup events is a configurable feature on all Assa Abloy WiFi locks that allows you to select the events that the locks must immediately report to the controller through WiFi radio.

Requirements

The minimum required firmware is Synergis™ Softwire 10.2 SR1.

How it works

By default, the *Door forced open* and *Door open too long* events wake up the lock's WiFi radio to report these events when they occur. Use the **Wakeup events** option on each individual lock, to select the events that wake up the WiFi radio. Events that are not selected to wake up the WiFi radio are reported on the next WiFi radio wakeup.

How to help minimize battery usage on WiFi locks

In some installations, locks can have a short battery life because the locks are generating many *Door held open* events that wake up the WiFi radio. Their battery life can be extended if it is acceptable to report *Door held open* events on the next scheduled or unscheduled radio wakeup. To prolong the battery life, set the **Wakeup events** option for these locks to *Door forced open only*. The *Door forced open* events wake up the WiFi radio and the *Door held open* events are reported on the next WiFi radio wakeup.

Configuring the Radio Wakeup events feature for Assa Abloy WiFi locks

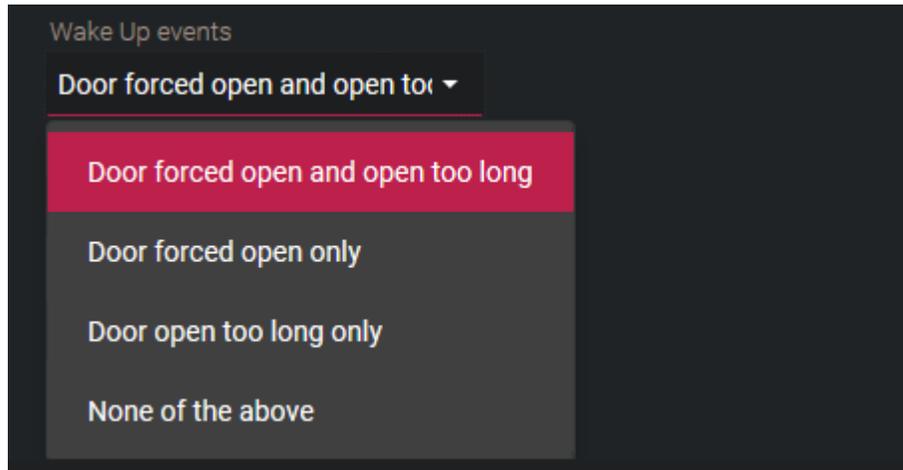
You can configure individual Assa Abloy WiFi locks to contact the controller through WiFi radio on specific Wakeup events.

Before you begin

[Enroll the Assa Abloy IP lock.](#)

What you should know

You can configure a [Wakeup event](#) for each Assa Abloy WiFi radio lock.



To configure Radio Wakeup events:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration > Hardware**.
- 3 Select **Assa Abloy IP**, then select the Assa Abloy channel and the lock.
- 4 Set the **Wakeup events** option for the lock.
- 5 Click **Apply**

Enabling escape and return mode on Assa Abloy IP locks with body type 8200 and monitored deadbolt

To enable the *escape and return mode* on doors controlled by Assa Abloy IP locks, you must create a Boolean custom field named `Escape Return` for doors, and set it to `TRUE` on the doors on which you want to have this feature enabled.

Before you begin

This feature requires Synergis™ Software 10.5 GA or later.

The Assa Abloy IP locks that support the *escape and return* feature are the models with lock body 8200 and monitored deadbolt.

For example:

- IN120 and IN220 8200 mortise lock with deadbolt. No other IN120 and IN220 locks support this feature.
- Passport 1000 P2 mortise lock with deadbolt. No other Passport 1000 P2 locks support this feature.

What you should know

The Canadian fire code states that a door can never “automatically relock”. Therefore, when the escape and return feature is enabled, the following features are disabled.

- Unlock schedules
- Maintenance mode
- Manual unlock from Security Desk
- Temporarily override schedules from Security Desk

With the escape and return feature enabled, when a cardholder exits through a door, the door remains unlocked after it closes until the cardholder presents their access card to lock the door. If the cardholder does not present their card to lock the door, the door remains unlocked while they are gone. When the cardholder returns, they must present their access card to open the door. After they have entered, they must throw the deadbolt to lock the door.

To enable the escape and return feature:

- 1 Create a Boolean type custom field for door entities, and name it `Escape Return`.
You must spell the name exactly as it is written, with capital and lowercase letters, and include the space.
- 2 Open the *Area view* task and set the **Escape Return** custom field to TRUE for all doors where this feature must be enabled.
TIP: If you need this feature enabled on many doors, we recommend using the *Copy configuration tool*.
- 3 (WiFi locks only) Trigger a radio wake up to activate the escape and return feature on the lock.
You can trigger a radio wake by removing the lock's cover and pressing the button, or by presenting a denied credential.
- 4 Go through the *escape and return mode* cycle for a first time by exiting from a door, and by presenting a valid credential after the door closes.
This causes the system to create the custom events that you can use to configure event-to-actions.

Two custom events are added to your system:

- **Escape Return Mode Start:** Door unlocked by exiting or by entry with a valid credential.
- **Escape Return Mode End:** Door locked with valid credential or by throwing deadbolt from the inner side of the door.

Enabling passage mode on Assa Abloy IP locks

To enable the *passage mode* on doors controlled by Assa Abloy IP locks, you must create a Boolean custom field named `PassageMode` for doors, and set it to TRUE on the doors on which you want to have this feature enabled.

What you should know

Passage mode is a feature available on all Assa Abloy IP locks. This feature allows any authorized cardholder to keep the lock in the unlocked state by presenting their credential. Depending on the lock controller and the lock brand, the cardholder needs to present their credential once or twice. Repeating the process returns the lock to its normal state.

To start or stop the passage mode when the reader is in *Card or PIN*, or *Card and PIN* mode, do one of the following:

- **Passage mode with single badge:** The following applies to all Sx locks and the following Cx locks: SARGENT and Corbin Russwin IN120 and IN220.
NOTE: When *privacy mode* is enabled, *passage mode* with single badge does not work for cardholders with a *security clearance* value lower than 7.
 - **Card or PIN:** Either badge once or enter the PIN to start the passage mode.
 - **Card and PIN:** Badge first, and then enter the PIN to start the passage mode.
- **Passage mode with double badge:** The following applies to all Px locks, Sx locks running Hx firmware, and the following Cx locks: SARGENT Passport 1000 P1 and P2, Corbin Russwin Access 700 PIP1 and PWI1, SARGENT and Corbin Russwin IN120 and IN220 locks with a *PERSONA* serial number. The IN120 and IN220 locks can either be ordered or configured manually. See instructions below.
 - 1 With the lock connected to a workstation, open the lock configuration file using the LCT tool.

- 2 From the **Lock Configuration** tab, click the Settings icon.
 - 3 Click the **Serial Number Setup** tab.
 - 4 Change the **Manufacturer** and **Board Type** to *Persona*.
 - 5 Apply the changes and follow the on-screen instructions. The lock now has a new serial number.
 - 6 Using LCT, re-apply the configuration to the lock.
 - 7 If the lock was already added to the Synergis™ unit, do the following in Config Tool: (1) Delete the lock and re-add it using the new serial number. (2) Re-configure the door entity hardware with the new lock.
- **Card or PIN:** Badge twice to start the passage mode. The PIN cannot be used.
 - **Card and PIN:** Badge first, and then enter the PIN. Badge again to start the passage mode.

The first time the passage mode is triggered, it creates two custom events in the system: *Passage Mode Start* and *Passage Mode End*, that you can use to configure event-to-actions.

To enable the passage mode feature:

- 1 Create a Boolean type custom field for door entities, and name it *PassageMode*.
You must spell the name exactly as it is written, with capital and lowercase letters.
 - 2 Open the *Area view* task and set the **PassageMode** custom field to TRUE for all doors where this feature must be enabled.
- TIP:** If you need this feature enabled on many doors, we recommend using the *Copy configuration tool*.

Enabling privacy mode on Assa Abloy IP locks without monitored deadbolt

To enable the *privacy mode* from Config Tool on doors controlled by Assa Abloy IP locks, you must create a Boolean custom field named *Privacy Mode* for doors, and set it to TRUE on the doors on which you want to have this feature enabled.

Before you begin

This feature requires Synergis™ Software 10.5 GA or later.

The Assa Abloy IP locks that support the privacy mode are the Cx-type PoE and WiFi locks.

NOTE: When *privacy mode* is enabled, *passage mode* with single badge does not work for cardholders with a *security clearance* value lower than 7.

What you should know

Privacy mode is an Assa Abloy IP lock feature that only grants access to supervisors (*override cardholders*). This feature is disabled as a factory default.

The following information describes how this feature works. To activate the privacy mode, press the *privacy button* found on the inner side of the door while the door is closed. The LED on the button flashes slowly for approximately 2 minutes to indicate that privacy mode is in effect. This action is equivalent to throwing the deadbolt on locks equipped with a monitored deadbolt.



All cardholders with a *security clearance* value lower than 7 function as supervisors. The privacy mode is deactivated when a cardholder opens the door from inside, or when supervisor badges in.

To enable the privacy mode from Config Tool:

- 1 Create a Boolean type custom field for door entities, and name it **Privacy Mode**.
You must spell the name exactly as it is written, with capital and lowercase letters, and include the space.
- 2 Open the *Area view* task and set the **Privacy Mode** custom field to TRUE for all doors where this feature must be enabled.

TIP: If you need this feature enabled on many doors, we recommend using the *Copy configuration tool*.

Two custom events are added to your system:

- **Deadbolt locked:** This event is triggered when privacy mode is activated on a door.
- **Deadbolt unlocked:** This event is triggered when privacy mode is deactivated on a door.

About Assa Abloy IP Cx lock support for 10,000 credentials

Cx type locks can now support up to 10,000 credentials in offline mode.

Requirements

The minimum required Synergis™ appliance firmware is 10.6 GA.

Lock online with Synergis™ Cloud Link

When a valid credential is one of the 10,000 stored on the lock:

- The *Access Granted* decision is taken by the lock;
- The reader's LED turns green and the door unlocks (default 5 seconds).

When a valid credential is not one of the 10,000 stored on the lock:

- The *Access Granted* decision is taken by the Synergis™ Cloud Link unit through reader host lookup;
- The reader's LED red for 1 second, then it turns green and the door unlocks (default 5 seconds).

Lock offline with Synergis™ Cloud Link

Only the 10 000 credentials stored on the lock will be granted access.

Lock synchronization above 10,000 credentials

Synchronization between the Synergis™ Cloud Link unit and Assa Abloy IP Cx Locks continues to work above the 10,000-credential limit has been exceeded. For example, schedule changes are still synched and credentials can be removed.

Synchronization time for 10,000 credentials:

- 1 lock per Synergis™ Cloud Link unit: 20 minutes
- 128 locks per Synergis™ Cloud Link unit: About 16 hours, 46 minutes

For wireless locks, configure the Radio wake-up schedule so that not more than 20 locks connect at the same time.

Supported Synergis™ appliance features for Assa Abloy IP lock integration

Not all Synergis™ appliance features are supported with the integration of Assa Abloy IP locks.

The Assa Abloy IP lock integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Software](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability)	
Manual enrollment (<i>Add hardware</i> dialog box)	See note ¹
Automatic enrollment (Scan button)	Yes
Property configuration	No
Configuration cloning (Clone button)	No
I/O diagnostics (live monitoring of inputs, relays, and readers)	No
Interface module firmware display	Yes
Interface module firmware upgrade (apply recommended firmware)	Yes
Access control behavior (Synergis™ unit-wide settings) ²	
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	No
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	Yes
Maximum PIN length in digits	6 ³
Degraded mode settings	N/A
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	Yes ⁴

¹ You need to [pair the IP lock with the Synergis™ unit](#).

² The door behavior settings are overwritten by the individual door settings configured in Security Center.

³ See [Supported maximum PIN length for Assa Abloy IP locks](#) on page 47.

⁴ Works, but the “Lock relay delay” is not taken into account.

Supported maximum PIN length for Assa Abloy IP locks

The supported maximum PIN length as well as the method for entering the PIN depend on the lock model and the selected reader mode.

The supported maximum PIN entry timeout is 255 seconds.

NOTE: *Card and PIN* only works with the *Always* schedule.

CAUTION: When the reader is in *Card or PIN* mode, the PIN credential works only if the cardholder also has a card credential.

Sx type locks and some Cx type locks

The following applies to all Sx locks and the following Cx locks: SARGENT and Corbin Russwin IN120 and IN220.

- **Card or PIN:** Up to 6 digits are supported. Enter the 1 to 6 digit PIN followed by '*'.
- **Card and PIN:** Present the card, then enter the 1 to 6 digit PIN followed by '*'.

Px type locks and some Cx type locks

The following applies to all Px locks, Sx locks running Hx firmware, and the following Cx locks: SARGENT Passport 1000 P1 and P2, Corbin Russwin Access 700 PIP1 and PWI1, SARGENT and Corbin Russwin IN120 and IN220 locks with a *PERSONA* serial number. The IN120 and IN220 locks can either be ordered or configured manually. See instructions below.

- **Card or PIN:** Only 6-digit PINs are supported. Enter '#' followed by the 6-digit PIN.
- **Card and PIN:** Only 4-digit PINs are supported. Present the card, then enter the 4-digit PIN.

Supported Security Center features for Assa Abloy IP lock integration

Not all Security Center access control features are supported with the integration of Assa Abloy IP locks.

The Assa Abloy IP Lock integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	PoE only	
	Standard grant time	Yes	
	Extended grant time	Yes	
	Entry time (Standard/Extended) ¹	No	
	Door relock - options	N/A	
	When door is unlocked by schedule - options	No	
	Door held - options	Yes	
	Door forced open - options	Yes	
	Unlock schedules	Yes ²	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	No	
	Time to ignore REX after granting access (in seconds)	No	
	Ignore REX events while door is open (On/Off)	No	
	Time to ignore REX after door closes (in seconds)	No	
	Visitor escort and two-person rule		
Maximum delay between card presentation (in sec.)	No		
Enforce two-person rule (On/Off) on Door side	No		
Manual actions on doors in Security Desk ³	Manually unlock doors	PoE only	
	Reader shunting (activate/deactivate reader)	No	
	Override unlock schedules	Yes ⁴	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk ⁵	Module running state (<i>Online, Offline</i>)	Yes ⁶
	AC fail	N/A
	Battery fail (<i>Low battery</i>)	Yes
	Door open/closed	Yes ⁷
	Door locked/unlocked	Yes ⁷
	Door forced open	Yes
	Door held open for too long	Yes ⁸
	Door secured	Yes ⁹
	Deadbolt (<i>Secured, Released</i>)	PoE only
	Key override	No
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	No ¹⁰
	Visitor escort rule (On/Off)	No
	Interlock	No
	Antipassback	No
	First-person-in rule	No
Elevator control	Elevators	N/A
Zone management	I/O zone	N/A
	Hardware zone	N/A

¹ Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

² IP locks accept up to a limit of 32 time intervals. If the Security Center schedules exceed this limit, only the first 32 time intervals are applied.

³ The Synergis™ unit must be connected to the Access Manager.

⁴ For WiFi locks, the command is only applied on the next radio contact.

⁵ No live event from WiFi locks. The events are only available after the next radio contact.

⁶ WiFi locks are considered offline only after the periodic radio contact + 5 min. is missed.

⁷ *Door open* and *door closed* events are generated only with PoE locks.

⁸ The timeout value set in Config Tool for triggering *Door open too long* events cannot exceed 4 minutes 15 seconds (or 255 seconds). Any value set higher than 255 seconds will be set to 255 seconds in the Synergis™ unit.

⁹A *Door secured* event is generated when the door is closed after a *Door forced* or *Door open too long* event.

¹⁰ Security clearance has no effect on the access permissions of the cardholders but it does make the locks following a Security Center unlock schedule go in locked state if security clearance is set below 7.

Configuration overview for Assa Abloy IP locks

To configure Assa Abloy IP locks to work with a Synergis™ unit, you must first configure the locks with the Lock Configuration Tool (LCT), and then pair the locks to the Synergis™ unit using the Synergis™ Appliance Portal.

The following table summarizes the IP lock configuration process.

Phase	Description	See
1	Make sure your IP lock firmware is up to date and supported by Synergis™ Software 10.6.	<ul style="list-style-type: none"> • <i>IP-Enabled Lock Installation Quick Start Guide</i> that came with your lock. • Supported Assa Abloy IP locks on page 39.
2	Configure the IP lock using the LCT. <ul style="list-style-type: none"> • Configure the Host address of the IP lock to be the same as the IP address of the Synergis™ unit. • Configure the communication port of the IP lock that the Synergis™ unit will use as a listening port when discovering the locks (Default=2571). • If encryption is required, set the AES key in the lock profile. You need this key after you pair the IP lock with the Synergis™ unit. 	<ul style="list-style-type: none"> • <i>Network & Lock Configuration Tool User Manual</i> that came with your lock.
3	Establish communication between the Synergis™ unit and its connected IP locks in Synergis™ Appliance Portal.	<ul style="list-style-type: none"> • Enrolling IP locks connected to the Synergis™ unit on page 53

Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.



Enrolling IP locks connected to the Synergis™ unit

For the Synergis™ unit to communicate with the IP locks connected to it, you must pair them together in the Synergis™ Appliance Portal using the *lock pairing mode*, and then complete the locks configuration in Config Tool.

Before you begin

Configure the IP locks using the Lock Configuration Tool (LCT). If encryption is enabled, write down the **Lock AES Key**. You need to enter this key in Config Tool.

What you should know

When the lock pairing mode is active, all the IP locks that are connected to the Synergis™ unit using the specified communication ports are discovered. After the pairing mode ends, the Synergis™ unit reconnects to the Access Manager in Security Center, and adds the paired IP locks.

NOTE: The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

To enroll the IP locks that are connected to the Synergis™ unit:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration** > **Hardware**
- 3 At the top of the *Hardware* column, click **Add (+)**.
- 4 Select **Assa Abloy IP**.
- 5 (Optional) In the **Timeout** field, select how long to activate the lock pairing mode for. New IP lock connections are only paired for the amount of time you specify.

- 6 (Optional if you're using a port other than the default, 2571) In the *ports* dialog box, type the port numbers of the communication ports you configured on the IP locks, and click **Add**.
- 7 (Optional) If you want the IP locks to be added as they are discovered, do the following:
 - a) Select the **Add locks upon discovery** option.

IMPORTANT: When this option is selected, the Synergis™ unit reconnects to the Access Manager after each group of IP locks is added. This option is only recommended if you must start configuring the IP locks before the pairing mode is complete.
 - b) From the **Delay before adding locks** option, select how many seconds must pass before the previously discovered locks are added.
- 8 Click **Start**.

IMPORTANT: For WiFi locks, press the COM or Reset button inside the back panel of the lock to trigger a connection to the Synergis™ unit.

The IP locks are detected and added to the table.

If you have problems pairing the lock to the Synergis™ unit, [test the connection between your IP lock and the unit](#).

- 9 Do one of the following:
 - To stop the lock pairing mode and add the discovered locks, click **Stop and save**.
 - To cancel the lock pairing mode, click **Cancel**.

NOTE: If the *Add locks upon discovery* option is selected, some locks might have already been added.

- Wait until the lock pairing mode times out.

The Synergis™ unit reconnects to the Access Manager, and the discovered locks are added.

10 Click **Configuration > Hardware**

The IP locks that were added appear in the hardware configuration page. Select a lock; the unit type, serial number, and lock firmware of the selected IP lock are displayed under *Properties*.

11 If no information is displayed under *Properties*, refresh the page.

For WiFi locks, it can take up to two minutes before the information is displayed under *Properties*. WiFi locks appear in red in the hardware tree because they are not in constant communication with the Synergis™ unit.

- a) For PoE locks: Under *Properties*, make sure that **Radio wakeup** is set to **Always on** so that *Access granted* events are never missed in Security Desk, and set **Battery check setting** to **Off**.
- b) For WiFi locks: Under *Properties*, make sure that **Radio wakeup** is set to **Daily**, and enter the time of day (**Hour** and **Minute**) when it should occur.

Select **Local time** if you want the radio wakeup time to follow the time zone of the Synergis™ unit. If you do not select this option, the default is UTC.

- c) Change other lock settings as you see fit.

The screenshot displays the configuration interface for an Assa Abloy IP lock. It is divided into two main sections: Properties and Configuration.

Properties Section:

- Serial number: [Redacted]
- Type: PoE (dropdown menu)
- Current Synergis™ appliance firmware: [Redacted]

Configuration Section:

- Radio wakeup: Always on (dropdown menu)
- Wake Up events: Door forced open and open to (dropdown menu)
- Fail setting: Fail secure (dropdown menu)
- Battery check setting: Off (dropdown menu)
- Disable relock settings
- Firmware type: Default (dropdown menu)

At the bottom of the interface, there are three buttons: a red button with a warning icon labeled "Reset to factory settings", a grey button labeled "Cancel", and a red button labeled "Save".

12 If encryption is enabled through LCT, select and edit the **Assa Abloy IP** channel and enter the **AESkey** (32-character hexadecimal string) configured on your lock.

13 Click **Save**.

Testing the connection between your IP lock and the Synergis™ unit

If you have trouble pairing the Synergis™ unit to your IP lock, you can test the connection between the lock and the unit using the Lock Configuration Tool (LCT).

To test the connection between your IP lock and the Synergis™ unit:

- 1 For PoE locks, refer to the **Ping Test** command in the LCT.
- 2 For WiFi locks, refer to the **Verify Connection to Host** command in the LCT.

Disabling encryption on Assa Abloy IP locks

To disable encryption on an Assa Abloy IP lock, you must clear the AES key from the Assa Abloy IP channel and remove the AES key from the lock profile with LCT.

To disable encryption on an Assa Abloy IP lock:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration > Hardware**.
- 3 Select **Assa Abloy IP**, then select the Assa Abloy channel and the lock.
- 4 Clear the field **AESkey**, and then click **Save**.
- 5 Using the Lock Configuration Tool (LCT), remove the encryption key from the lock.
 - a) Remove the AES key from the lock profile.
 - b) Click **NVRAM Reset** to reset the lock.

For instructions, see the *Network & Lock Configuration Tool User Manual* that came with your lock.

- 6 Power off the lock until the reader LED stops flashing.
- 7 Power on the lock.

Once the lock is powered-on, it comes back online.

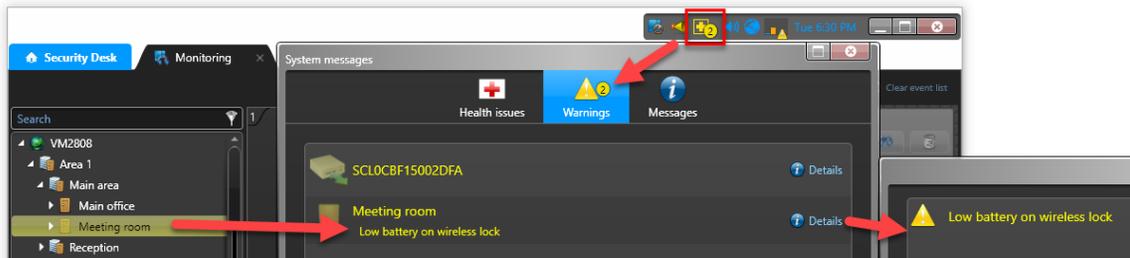
Monitoring the battery status of WiFi locks

To check the status of the battery on an Assa Abloy IP WiFi lock, you can monitor the *Battery fail* event on the Synergis™ unit that it is connected to.

What you should know

For each WiFi lock, Security Center creates a virtual input named *Input BatteryFail* that shows as *Active* in the **Monitoring** tab and yellow warning on the **System messages** icon in the **notification tray** when the battery is low.

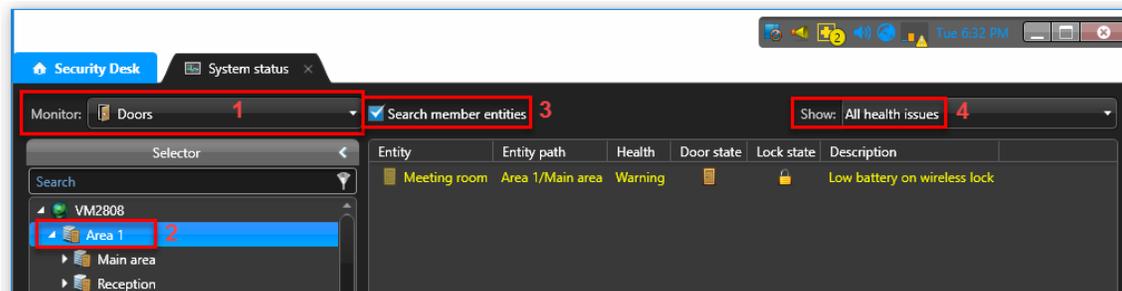
NOTE: *Input BatteryFail* is a software input created to indicate the battery status of WiFi locks. You cannot connect any physical device to this input.



To monitor the battery status of WiFi locks:

- 1 Open the *System status* task in Security Desk and select **Doors** in the **Monitor** drop-down list.
- 2 Select the parent area in the entity tree.
- 3 Click the **Search member entities** checkbox to display all the locks under the child areas.
- 4 Select **All health issues** in the **Show** drop-down list to show the doors with warnings.

NOTE: The WiFi locks that have battery problems will show an *Active* state for the **Input BatteryFailed** input



- 1 Schedule a battery replacement for those WiFi locks.

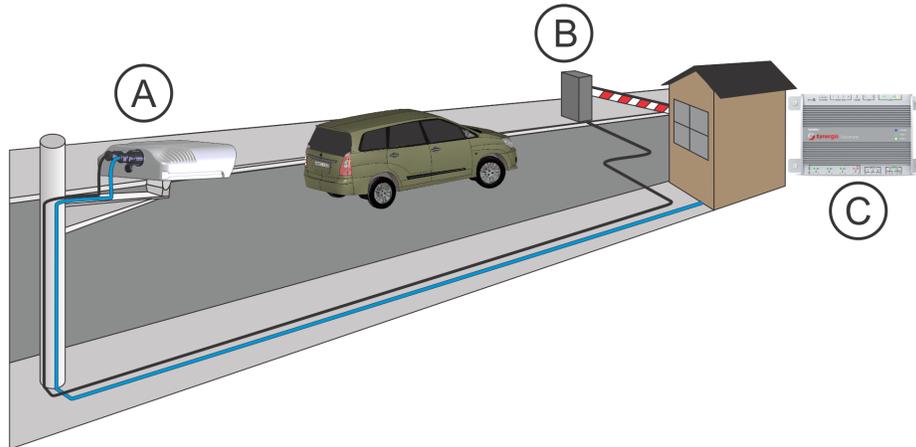
AutoVu SharpV Cameras

This section includes the following topics:

- ["AutoVu SharpV integration overview"](#) on page 60
- ["Supported AutoVu Sharp cameras"](#) on page 62
- ["Supported AutoVu Sharp camera features"](#) on page 63
- ["Supported Synergis appliance features for AutoVu Sharp camera integration"](#) on page 64
- ["Supported Security Center features for AutoVu Sharp camera integration"](#) on page 65
- ["Enrolling AutoVu SharpV cameras on the Synergis unit"](#) on page 68
- ["Configuring a SharpV camera to control a vehicle access barrier"](#) on page 70

AutoVu™ SharpV integration overview

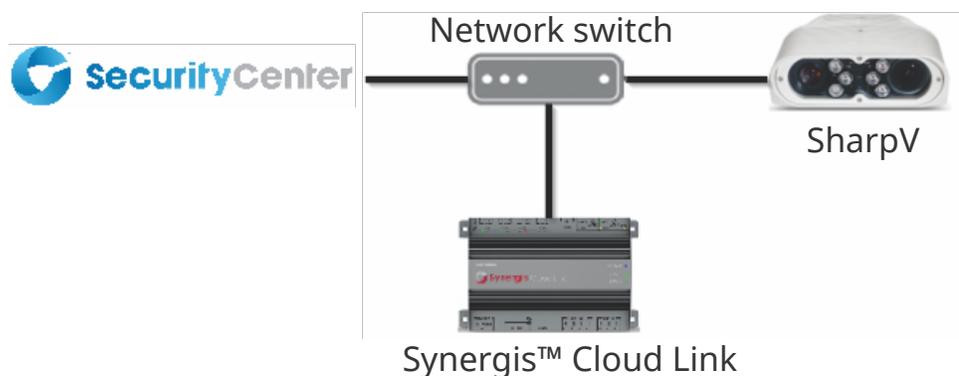
AutoVu™ SharpV cameras are capable of reading license plates from passing vehicles. When a SharpV camera is installed in a fixed location with a view of vehicle license plates as they approach a vehicle access barrier, plate reads from the camera can be used as credentials in Security Center. If the plate number matches a user's credentials, the system triggers the barrier to allow access to the vehicle.



NOTE: The ability to use license plate reads as a credential is only available in Security Center 5.6 and later.

Component	What you should know
A SharpV camera	The camera is installed in a fixed location with a view of vehicle license plates as they approach a vehicle access barrier.
B Vehicle access barrier	You can use the SharpV outputs to control a vehicle access barrier.
C Network connection	The SharpV camera communicates with Security Center and is enrolled on the Synergis™ Cloud Link.

To use license plate reads as credentials, a Synergis™ Cloud Link or a Synergis™ Master Controller must be connected through the network with the SharpV camera. The following image shows a system that includes a SharpV and a Synergis™ Cloud Link.



Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.



Supported AutoVu™ Sharp cameras

For AutoVu™ Sharp camera integration, each Sharp camera is viewed as an interface module.

Synergis™ Software supports the following Sharp cameras and corresponding firmware:

Model	Description	Supported firmware
SharpV	IP-enabled license plate recognition (LPR) camera	SharpOS 12.2 and later

NOTE: First generation Synergis™ units (Synergis™ Master Controller) do not support SharpV cameras running SharpOS 12.3 or later.

Supported AutoVu™ Sharp camera features

AutoVu™ Sharp cameras are LPR cameras. The license plate reads can be used as credentials, but not all standard access control features apply.

NOTE: The ability to use license plate reads as a credential is only available in Security Center 5.6 and later.

Synergis™ Softwire 10.6 supports the following Sharp camera features.

Features	Supported
General characteristics	
Category of interface module	Sub-panel
Communication protocol	IP
Encrypted communication	Yes (HTTPS)
Online operation (connected to the Synergis™ unit)	
Supervised mode	No
Dependent mode	Yes
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	No
Degraded mode	N/A
Scalability	
Maximum number of offline events	N/A
Maximum number of credentials (for autonomous decision making)	N/A
Maximum credential length (in bits)	N/A
Maximum number of interface modules per RS-485 channel	N/A
Recommended maximum number of interface modules per Synergis™ unit	8

Supported Synergis™ appliance features for AutoVu™ Sharp camera integration

Not all Synergis™ appliance features are supported with the integration of AutoVu™ Sharp cameras.

The Sharp camera integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Softwire](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability) ¹	
Manual enrollment (<i>Add hardware</i> dialog box)	No
Automatic enrollment (Scan button)	No
Property configuration	No
Configuration cloning (Clone button)	No
I/O diagnostics (live monitoring of inputs, relays, and readers)	No
Interface module firmware display	No
Interface module firmware upgrade (apply recommended firmware)	No
Access control behavior (Synergis™ unit-wide settings) ²	
Beep on door held open	N/A
Beep on door forced open	N/A
Beep on access denied	N/A
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	N/A
Do not generate 'DHO' events when door is unrestricted	Yes
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	N/A
Maximum PIN length in digits	N/A
Degraded mode settings	N/A
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	Yes

¹ Sharp cameras must be enrolled on the Synergis™ unit from Config Tool.

² The door behavior settings are overwritten by the individual door settings configured in Security Center.

Supported Security Center features for AutoVu™ Sharp camera integration

Not all Security Center access control features are supported with the integration of Sharp cameras.

The Sharp camera integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	Yes	
	Extended grant time	Yes	
	Entry time (Standard/Extended) ¹	Yes	
	Door relock - options	Yes	
	When door is unlocked by schedule - options	Yes	
	Door held - options	Yes	
	Door forced open - options	Yes	
	Unlock schedules	Yes	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	Yes	
	Time to ignore REX after granting access (in seconds)	Yes	
	Ignore REX events while door is open (On/Off)	Yes	
	Time to ignore REX after door closes (in seconds)	Yes	
	Visitor escort and two-person rule		
	Maximum delay between card presentation (in sec.)	N/A	
Enforce two-person rule (On/Off) on Door side	N/A		
Manual actions on doors in Security Desk ²	Manually unlock doors	Yes	
	Reader shunting (activate/deactivate reader)	Yes	
	Override unlock schedules	Yes	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	N/A
	Battery fail (<i>Low battery</i>)	N/A
	Door open/closed	Yes
	Door locked/unlocked	Yes
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	Yes
	Visitor escort rule (On/Off)	N/A
	Interlock	Yes
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	Yes
	Presence timeout (forget area presence after a certain delay)	Yes
	Strict (antipassback checked on both area entrance and exit)	Yes
	On schedule	Yes
	Global antipassback	Yes
	First-person-in rule	
	Enforce on door unlock schedule	N/A
Enforce on access rules	N/A	
Elevator control	Elevators	N/A
Zones	I/O zone	Yes
	Hardware zone	
	Zone arming input	Yes
	Zone arming schedule	Yes
	Zone arming and entry delays	No

Feature group	Security Center feature	Supported
	Zone I/O linking	Yes
	Countdown buzzer	Yes

¹ Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

² The Synergis™ unit must be connected to the Access Manager.

Enrolling AutoVu™ SharpV cameras on the Synergis™ unit

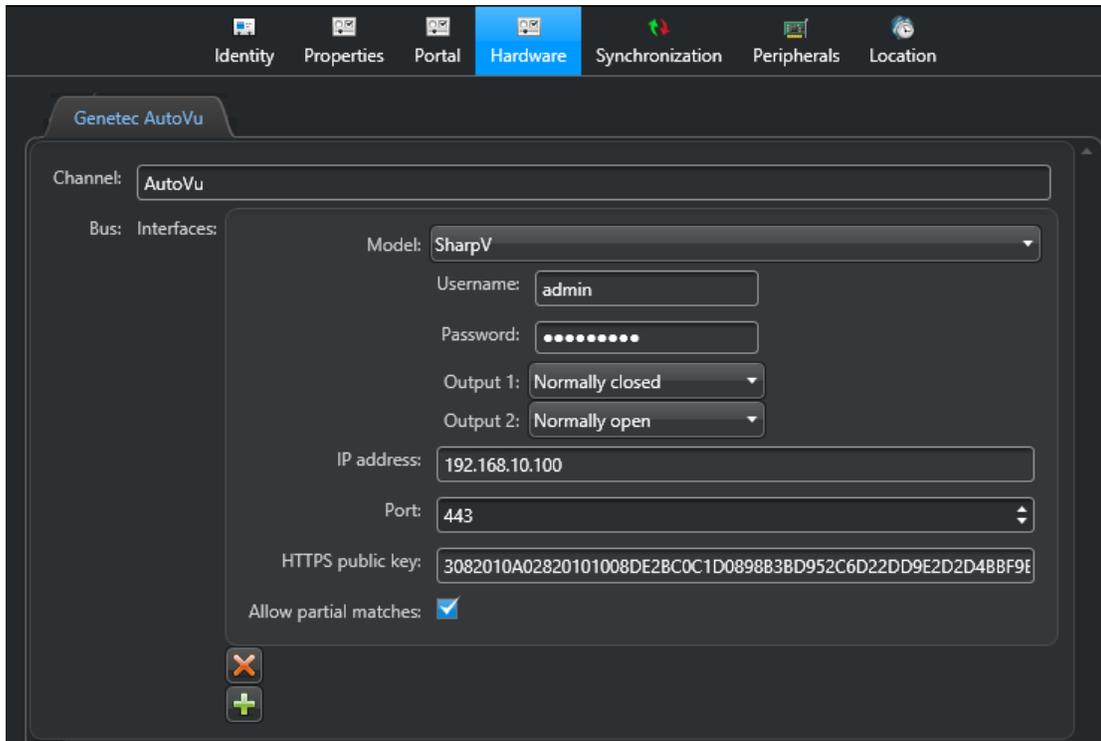
For the Synergis™ unit to communicate with the SharpV camera, you must enroll the camera on the Synergis™ unit in Security Center.

Before you begin

- Configure the SharpV camera to use HTTPS communication. For more information, see the *Deployment Guide* or *Handbook* for the camera you are installing.
- Install either the Genetec™ self-signed certificate or a signed certificate from a trusted certificate authority.
- If you are enrolling a SharpV camera, log on to the SharpV web portal and change the default password.

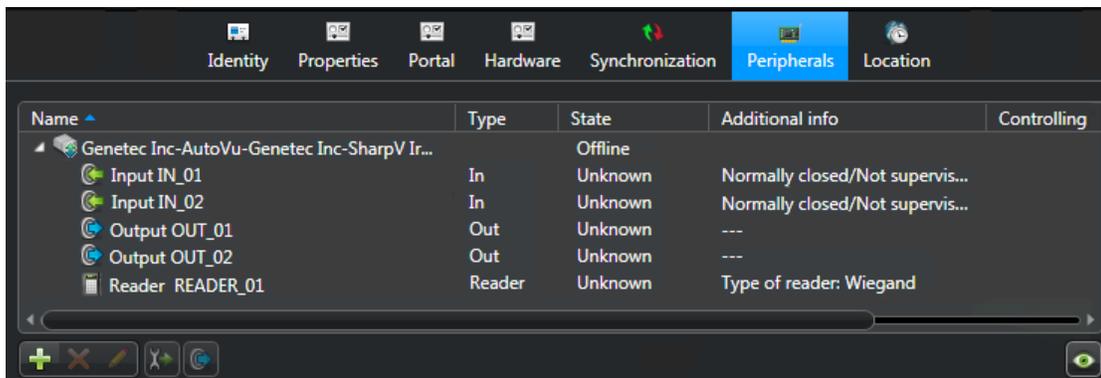
To enroll the SharpV camera on the Synergis™ unit:

- 1 From the Config Tool home page, open the *Access control* task.
- 2 Click **Roles and units**, and then click the Synergis™ unit (🌐).
- 3 Click the **Hardware** tab, and then click the **Genetec™ AutoVu™** tab.
- 4 Click **Add** (+).
- 5 Enter a **Channel** name of your choice.
The channel name you enter will appear in the camera name in the **Peripherals** tab.
- 6 Click **Interfaces** (+).
- 7 From the **Model** drop-down list, select SharpV.
- 8 Enter the **Username** and **Password** used to access the SharpV web portal.
NOTE: For SharpV cameras, you cannot use the default password.
- 9 If you are using the SharpV outputs to control a vehicle access barrier, select whether the outputs are *Normally open* or *Normally closed*.
- 10 Enter the **IP address** of the camera.
- 11 The SharpV uses **Port 443** for HTTPS communication with Security Center.
- 12 Leave the **HTTPS public key** field empty. This information is added automatically based on the camera's certificate.
- 13 The **Allow partial matches** check box is selected by default. This feature accepts plate reads that have one-character difference from a configured license plate credential; this includes a single character insertion, deletion, or substitution, at any place in the plate number. With this feature enabled, plate reads from dirty or damaged license plates are more likely to be accepted.



14 Click **Apply**.

- The SharpV camera is displayed in the **Peripherals** tab.
- The inputs and outputs are displayed under the SharpV camera.



Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.



Configuring a SharpV camera to control a vehicle access barrier

To use a SharpV camera to control a vehicle access barrier, the barrier must be configured as a door in Security Center.

Before you begin

- Wire the vehicle access barrier to the Synergis™ appliance. For more information, see the *Hardware Installation Guide* for the access control appliance you are installing.
- Enroll the Synergis™ unit in Security Center (see the *Synergis™ Appliance Configuration Guide*).
- [Enroll the SharpV camera on the Synergis™ unit.](#)

To configure a vehicle access barrier in Security Center:

- 1 From the Config Tool home page, open the *Area view* task.
- 2 Select the area where you want to add the vehicle access barrier.
- 3 Click  **Add an entity** > **Door**.
- 4 In the **Creating a door** wizard, enter the name and description of the vehicle access barrier.
- 5 From the **Location** drop-down list, select the area in which you are creating the door, and click **Next**.
- 6 On the **Door information** page, assign names to the barrier sides.
Example: In/Out, or Entrance/Exit.
- 7 To associate the barrier with the access control unit that it is wired to:
 - a) From the **Access control unit** drop-down list, select the Synergis™ unit.
 - b) From the **Interface module** drop-down list, select the SharpV camera.
- 8 Click **Next**.
- 9 Review the *Creation summary*, and click **Create** > **Close**.
The barrier appears in the area view's *entity tree*.
- 10 Select the barrier and click the **Properties** tab.
- 11 Configure the general access control behavior of the barrier. For more information, see the *Security Center Administrator Guide*.
- 12 Click **Apply**.
- 13 Click the **Hardware** tab and describe the wiring between the access control unit and the door to Security Center. For more information, see the *Security Center Administrator Guide*.
- 14 Create cardholders using their license plates as credentials. For more information on creating cardholders, see the *Security Desk User Guide*.
When assigning credentials to the cardholder, select the **License plate** option.
- 15 Select who has access to the door. For more information, see the *Security Center Administrator Guide*.

Axis Controllers

This section includes the following topics:

- ["Supported Axis controllers"](#) on page 72
- ["Supported Axis controller features"](#) on page 73
- ["Supported Synergis appliance features for Axis controller integration"](#) on page 75
- ["Supported Security Center features for Axis controller integration"](#) on page 76
- ["Enrolling the Axis controller on the Synergis unit"](#) on page 79
- ["Configuring the peripherals attached to Axis controllers"](#) on page 83
- ["Reader connections on the Axis controller"](#) on page 87

Supported Axis controllers

For Axis controller integration, each A1001 controller is viewed as an interface module.

Synergis™ Softwire supports the Axis A1001 controller.

Model	Description	Supported firmware
A1001	Two-door controller supporting IP communication, featuring two readers, suitable for two Card-in/REX-out doors or one Card-in/Card-out door.	Recommended: 1.60 ¹

¹ For certain intelligent controllers, such as Assa Abloy IP Locks, Axis, and Mercury EP, you can apply the recommended firmware from the *Interface upgrade* page of Synergis™ Appliance Portal. For other manufacturers, you might have to use the manufacturer's software to apply the recommended firmware.

Supported Axis controller features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following Axis controller features.

Features	Supported
General characteristics	
Category of interface module	Intelligent controller
Communication protocol	IP
Encrypted communication	No
Online operation (connected to the Synergis™ unit)	
Supervised mode	No
Dependent mode	Yes
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	Yes
Degraded mode	N/A
Reader communication protocols	
Wiegand	Yes
OSDP	Yes
OSDP (Secure Channel)	No
Clock and Data (Magnetic Stripe) — Also known as ABA format	N/A
F2F	N/A
Proprietary	N/A
Scalability	
Maximum number of offline events	30 000 ¹
Maximum number of credentials (for autonomous decision making)	15 000 ²
Maximum credential length (in bits)	512 ³
Maximum number of interface modules per RS-485 channel	N/A
Recommended maximum number of interface modules per Synergis™ unit	30/66 ⁴

- ¹ There is not always a one-to-one match between an offline log entry and a Security Center event.
- ² The recommended limit is 10 000. The hard limit is 15 000.
- ³ We currently support the standard card formats supported by Security Center, which are Wiegand Standard 26-bit, Corporate 1000 (35-bit), H10306 (34-bit), H10302 (37-bit), and H10304 (37-bit). Custom card formats can go up to 512 bits.
- ⁴ The maximum for a *Synergis™ Cloud Link* is 30. The maximum for an [SV-32](#) is 66.

Supported Synergis™ appliance features for Axis controller integration

Not all Synergis™ appliance features are supported with the integration of Axis controllers.

The Axis controller integration supports the following *Synergis™ Appliance Portal* and *Synergis™ Softwire* features. For a description of these features, see the *Synergis™ Appliance Configuration Guide*.

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability)	
Manual enrollment (<i>Add hardware</i> dialog box)	Yes
Automatic enrollment (Scan button)	No
Property configuration	Yes
Configuration cloning (Clone button)	Yes
I/O diagnostics (live monitoring of inputs, relays, and readers)	Yes
Interface module firmware display	Yes
Interface module firmware upgrade (apply recommended firmware)	Manual ²
Access control behavior (Synergis™ unit-wide settings) ³	
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	Online
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	Yes
Maximum PIN length in digits ⁵	16
Degraded mode settings	N/A
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	Yes

² The recommended Axis firmware must be uploaded to the Synergis™ appliance by applying the file *Axis_10.6_xxx.y.sfx* as a firmware upgrade through Synergis™ Appliance Portal.

³ The door behavior settings are overwritten by the individual door settings configured in Security Center.

⁴ The beeping cannot be disabled on these events.

⁵ For interface modules that support HID mode-00 readers.

Supported Security Center features for Axis controller integration

Not all Security Center access control features are supported with the integration of Axis controllers.

The Axis controller integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	Yes	
	Extended grant time	Yes	
	Entry time (Standard/Extended) ¹	No	
	Door relock - options	Limited ²	
	When door is unlocked by schedule - options	Yes	
	Door held - options	Limited ³	
	Door forced open - options	Limited ³	
	Unlock schedules	Yes	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	Yes	
	Time to ignore REX after granting access (in seconds)	N/A	
	Ignore REX events while door is open (On/Off)	N/A	
	Time to ignore REX after door closes (in seconds)	N/A	
	Visitor escort and two-person rule		
Maximum delay between card presentation (in sec.)	Online		
Enforce two-person rule (On/Off) on Door side	Online		
Manual actions on doors in Security Desk ⁴	Manually unlock doors	Online	
	Reader shunting (activate/deactivate reader)	Online	
	Override unlock schedules	Online	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	N/A
	Battery fail (<i>Low battery</i>)	N/A
	Door open/closed	Yes
	Door locked/unlocked	Yes
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	Online
	Visitor escort rule (On/Off)	Online
	Interlock	Online
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	Online
	Presence timeout (forget area presence after a certain delay)	Online
	Strict (antipassback checked on both area entrance and exit)	Online
	On schedule	Online
	Global antipassback	Online
	First-person-in rule	
	Enforce on door unlock schedule	Online
	Enforce on access rules	Online
Elevator control	Elevators	No
Zone management	I/O zone	No
	Hardware zone	No

¹ Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

² With the **Relock after opening** option, the delay is always 0 seconds.

³ The **Reader buzzer behavior** options are not supported.

⁴ The Synergis™ unit must be connected to the Access Manager.

Enrolling the Axis controller on the Synergis™ unit

For the Synergis™ unit to communicate with the Axis controllers connected to it, you must enroll the controllers with either Synergis™ Appliance Portal or Config Tool.

Before you begin

- Have your Axis controllers' serial number or IP address handy. To find that information, see your Axis documentation.

What you should know

The Synergis™ unit sets all Axis input contacts and output relays with a default configuration when it enrolls the controller. Axis and Synergis™ use different terminology to describe their settings.

NOTE: Only the enrollment through the Synergis™ Appliance Portal is described here, but you can also enroll an Axis controller from the **Config Tool > Synergis unit > Hardware** tab.

To enroll the Axis controller on the Synergis™ unit:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration > Hardware**
- 3 At the top of the *Hardware* column, click **Add (+)**.
- 4 In the *Add hardware* dialog box, select **Axis** as the **Hardware type**.
- 5 Select the IP channel where the Axis controller is connected.
- 6 Enter the connection parameters required to connect to the Axis controller.
 - *Serial number or IP address.* Use the IP address or serial number of the Axis controller.
 - *Port.* HTTP port (default = 80).
 - *Username/Password.* New username and password (default = root/pass).

All fields are necessary.

The screenshot shows a dark-themed 'Add hardware' dialog box. It contains the following fields and options:

- Hardware type:** A dropdown menu with 'Axis' selected.
- Channel:** A dropdown menu with 'LAN1' selected.
- IP address:** An empty text input field.
- Interface module type:** A dropdown menu with 'A1001' selected.
- Connection mode:** A dropdown menu with 'Default' selected.
- Username:** A text input field containing 'root'.
- Password:** A text input field with four dots representing a masked password.

At the bottom of the dialog, there are three buttons: 'Add' (on the left), 'Cancel' (in the center), and 'Save' (on the right, highlighted in red).

- 7 Click **Save**.
The hardware type, channel, and interface module you just added appear in the *Hardware configuration* page. It can take up to one minute for the Axis module to come online.
- 8 If the Current firmware version is not the latest, upgrade it.
 - 1 If you have not already downloaded the Axis firmware package, download it from GTAP.
 - 2 Click **Maintenance > Software upgrade**
 - 3 Click **Select firmware file**.
- 9 In the browser window, select the Axis plugin version that corresponds to your Synergis™ Software version (*Axis_10.6.xxx.y.sfw*), and click **Open**.
- 10 In the confirmation message box, click **OK**.
- 11 If the Axis module does not come online after a minute, click **Maintenance > Interface upgrade > Apply recommended firmware**.
This applies the recommended firmware versions to all enrolled interface modules that are online and accessible over the network.
- 12 Test your interface module connection and configuration from the *I/O diagnostics* page. For more information, see the *Synergis™ Appliance Configuration Guide*.

After you finish

Add the Synergis™ unit to an Access Manager so it becomes part of your Security Center system. For more information, see the *Synergis™ Appliance Configuration Guide*

Hardening Axis controllers

You need to install an Axis plugin on the Synergis™ unit before you can enroll Axis controllers.

Before you begin

- Make sure you get the latest Synergis™ Software and Axis plugin from your representative of Genetec Inc. The Synergis™ Software file is named *Release_10.6.xxx.y.sfw*, and the Axis plugin file is named *Axis_10.6.mmm.n.sfw*. The Axis plugin file contains the [recommended Axis firmware](#).
- Follow the latest [Product Security recommendations from Axis Communications](#).
- [Enroll the Axis controllers](#).

What you should know

The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

To harden Axis controllers:

- 1 Log on to the Axis A1001 web portal.
For more information, see the [AXIS A1001 Network Door Controller & AXIS Entry Manager User Manual](#).
- 2 Click **Setup > Additional Control Configuration > System Options > Security > IP Address Filter**, and add to the list of **Filtered IP Addresses**, the IP address of the Synergis™ unit and the IP address of the administrative workstation that must log on to the Axis A1001 web portal.



- 3 Click **Setup > Additional Control Configuration > System Options > Network > TCP/IP > Advanced**, and disable both **FTP server** and **RTSP server**.
They are not used by Synergis™ Software.

About the tamper inputs on Axis controllers

The Axis controller features two tamper inputs that can be monitored in Security Center.

These inputs are:

- **Input Tampered.** This input is active when:
 - Input “IN3” on one of the two reader I/O connectors is active, or
 - Front tampering alarm sensor is activated, or
 - Back tampering alarm switch is activated
- **Input CasingOpen.** This input is active when:
 - Front tampering alarm sensor is activated, or
 - Back tampering alarm switch is activated.

The front and back tampering alarms can be disabled by putting a jumper on the respective 2- pin Tampering Alarm Pin Header.

- Tampering alarm pin header – front (TF)
- Tampering alarm pin header – back (TB)

Configuring the peripherals attached to Axis controllers

To configure the input contacts, output relays, and readers attached to the Axis controller, you must make your changes in Security Center using the Config Tool.

Before you begin

- [Enroll the Axis controller on the Synergis™ unit.](#)
- Add the Synergis™ unit to an Access Manager. For more information, see the *Synergis™ Appliance Configuration Guide*.

What you should know

- You must configure the Axis output relays and readers from the Synergis™ unit's *Hardware* page.
- You must configure the Axis input contacts from the Synergis™ unit's *Hardware* page and from the *Peripherals* page.

To change the peripherals settings of the Axis controller:

- 1 From the Config Tool home page, open the *Access control* task.
- 2 Click **Roles and units**, and then click the Synergis™ unit (🌐).
- 3 Click **Hardware** > **Axis**, make the necessary changes, and click **Apply**.

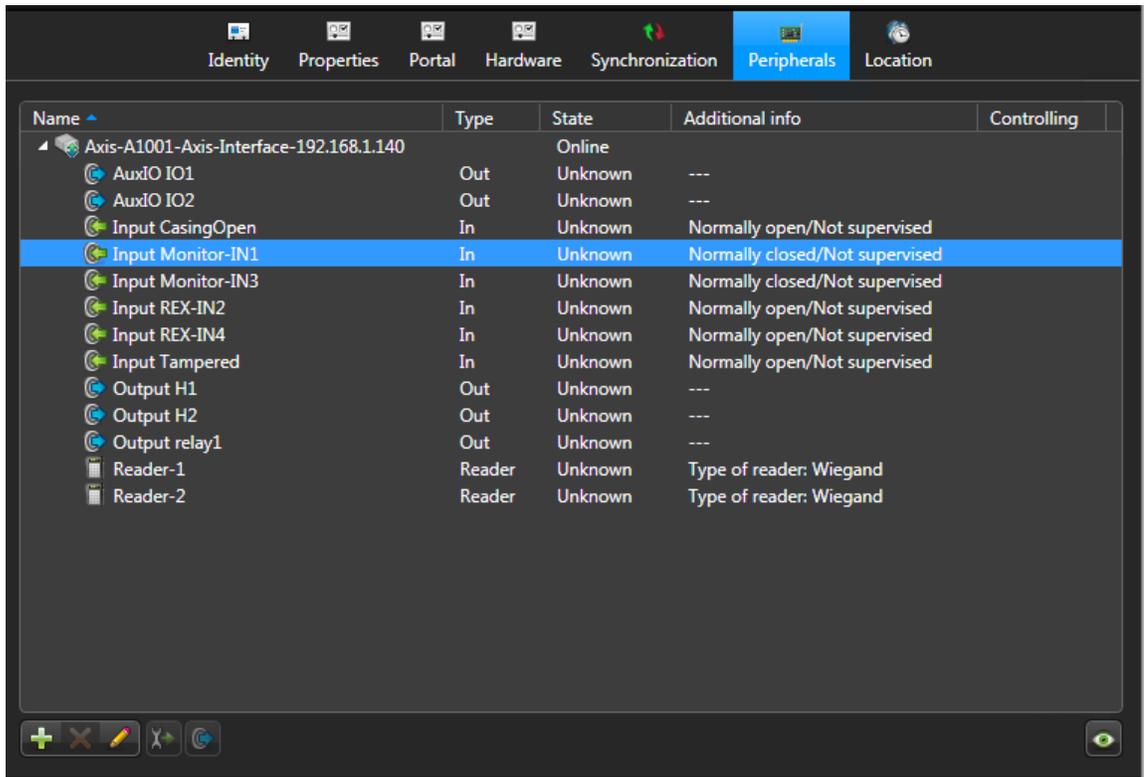
The screenshot shows the configuration interface for an Axis controller. The top navigation bar includes tabs for Identity, Properties, Portal, Hardware (selected), Synchronization, Peripherals, and Location. Below this, there are sub-tabs for AperiO, Assa Abloy IP, Axis (selected), DDS, Salto Sallis, STid, and VertX. The main configuration area is titled 'Axis plugin version: 10.5.443.0'. A modal window is open, displaying the following settings:

- Firmware version: Unknown version
- Serial number or IP address: 192.168.1.140
- Port: 80
- Username: root
- Password: [masked]
- Extended held open time (seconds): 12
- H1 Fail setting: Fail secure
- H2 Fail setting: Fail secure
- Relay Fail setting: Fail secure
- Reader 1 is OSDP: [unchecked]
- Reader 2 is OSDP: [unchecked]
- Monitor Supervised Short (mV): 0
- Monitor Supervised Low (mV): 505
- Monitor Supervised High (mV): 1530
- Monitor Supervised Cut (mV): 2712
- Rex Supervised Short (mV): 0
- Rex Supervised Low (mV): 505
- Rex Supervised High (mV): 1530
- Rex Supervised Cut (mV): 2715
- Aux IO1 Normal state: Open
- Aux IO2 Normal state: Open
- Aux IO1 activated on alarm from: None
- Aux IO2 activated on alarm from: None
- EA-mode timeout (s): 10

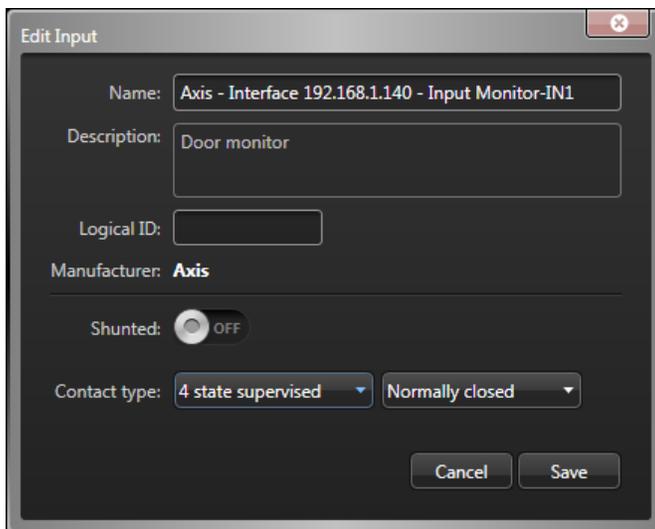
At the bottom of the modal, there is a '+ Add interface' button.

For more information on the meaning of each setting, see the Axis documentation.

- 4 If you need to change the input contact configuration, click the **Peripherals** tab and expand the Axis controller you want to modify.



- 5 Select the input contact you want to modify and click **Edit** (✎).
The *Edit input* dialog box opens.



The settings you can change depend on the selected input.

- **Name:** Input device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless of how you trigger it.
- **Contact type:** Set the *Normal* state of the input contact and its supervision mode.
 - **Not supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit does not report that the input is in the trouble state.

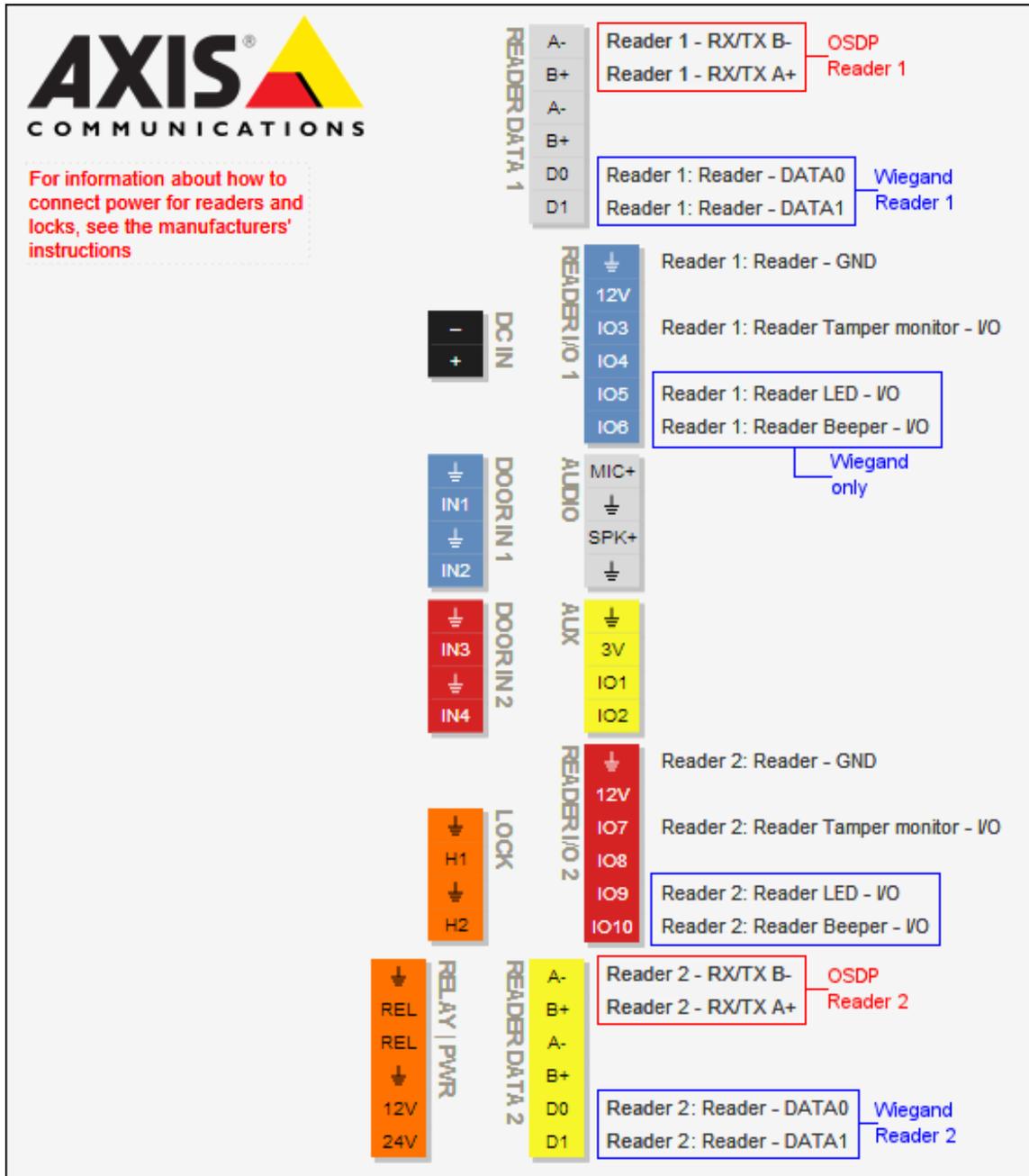
- **Not supervised / Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
 - **4-state supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
 - **4-state supervised / Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.
- 6 Make the necessary changes, click **Save**, and then click **Apply**.

Reader connections on the Axis controller

Each Axis controller supports up to two readers, called *Reader 1* and *Reader 2* in Security Center Config Tool. The readers can use either Wiegand (default) or OSDP protocol. For OSDP, the reader must be wired to the first set of reader data A-/B+.

The following chart shows which set of connectors correspond to which reader on the Axis controller.

NOTE: This pin chart only shows up if the Axis controller is disconnected to the Synergis™ unit.



DDS Controllers

This section includes the following topics:

- ["Supported DDS hardware"](#) on page 89
- ["Supported DDS controller features"](#) on page 90
- ["Supported Synergis appliance features for DDS controller integration"](#) on page 92
- ["Supported Security Center features for DDS controller integration"](#) on page 93
- ["Enrolling DDS RS-485 controllers"](#) on page 96
- ["Preparing to enroll DDS IP controllers"](#) on page 98
- ["Enrolling DDS IP controllers"](#) on page 103
- ["Setting the physical address of TPL door controllers"](#) on page 107

Supported DDS hardware

For DDS integration, each TPL door controller is viewed as an interface module.

Synergis™ Softwire supports the following DDS hardware devices.

Model	Description	Firmware
AS34 or TPL	Door controller supporting RS-485 communication, featuring four Wiegand readers, suitable for two card in/ card out doors. NOTE: Make sure the ROM chip installed on the U5 socket of the TPL board is labelled 5xxx ^a .	Synergis™ Softwire requires a custom version of the firmware. The custom firmware is automatically pushed to the TPL module during enrollment.
AS34-P4 or TPL-P4	Door controller supporting RS-485 communication, featuring four Wiegand readers, suitable for four card in/ REX out doors. NOTE: Make sure the ROM chip installed on the U5 socket of the TPL board is labelled 6xxx ^a .	
EXT-TCPT	TCP/IP extension board for the TPL door controller.	N/A
EXT-8E4S	TCP/IP extension board adding 8 supervised inputs and 4 outputs to the TPL door controller with the ROM chip 6xxx ^a . This combination is equivalent to adding TCP/IP interface to the TPL-P4 controller.	N/A

a. The exact chip number depends on the storage capacity of the ROM.

Supported DDS controller features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following DDS controller features.

Features	Supported
General characteristics	
Category of interface module	Intelligent controller
Communication protocol	RS-485 and IP ¹
Encrypted communication	No
Online operation (connected to the Synergis™ unit)	
Supervised mode	No
Dependent mode	Yes
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	Yes
Degraded mode	N/A
Reader communication protocols	
Wiegand	Yes
OSDP	N/A
OSDP (Secure Channel)	N/A
Clock and Data (Magnetic Stripe) — Also known as ABA format	Yes
F2F	N/A
Proprietary	N/A
Scalability	
Maximum number of credentials (for autonomous decision making)	20 000 ²
Maximum credential length (in bits)	40
Maximum number of interface modules per RS-485 channel	8
Recommended maximum number of interface modules per Synergis™ unit	32

¹ IP controllers require the EXT-TCPT or the EXT-8E4S extension board.

² The maximum number of credentials that the Synergis™ unit can synchronize with the DDS controller is 20,000. The actual limit may be lower, depending on the ROM chip installed on the AS34 module.

Supported Synergis™ appliance features for DDS controller integration

Not all Synergis™ appliance features are supported with the integration of DDS controllers.

The DDS controller integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Softwire](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability) ¹	
Manual enrollment (<i>Add hardware</i> dialog box)	RS-485 only
Automatic enrollment (Scan button)	RS-485 only
Property configuration	RS-485 only
Configuration cloning (Clone button)	RS-485 only
I/O diagnostics (live monitoring of inputs, relays, and readers)	Yes
Interface module firmware display	No
Interface module firmware upgrade (apply recommended firmware)	Automatic
Access control behavior (Synergis™ unit-wide settings) ²	
Beep on door held open	Yes
Beep on door forced open	Yes
Beep on access denied	Yes
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	Online
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	Online ³
Maximum PIN length in digits ⁴	5 ⁵
Degraded mode settings	N/A
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	Yes

¹ IP controllers must be enrolled through a different set of web pages than [Synergis™ Appliance Portal](#). See "[Enrolling DDS IP controllers](#)".

² The door behavior settings are overwritten by the individual door settings configured in Security Center.

³ HID keypad mode 00 is not supported. Only keypad mode 14 is, producing Facility Code 0.

⁴ Limited to HID Wiegand Standard 26-bit card code (maximum value = 65534).

⁵ PINs less than 4 digits are not accepted.

Supported Security Center features for DDS controller integration

Not all Security Center access control features are supported with the integration of DDS controllers.

DDS integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Online	
	Standard grant time	Yes	
	Extended grant time	Online	
	Entry time (Standard/Extended) ¹	Online	
	Door relock - options	Yes	
	When door is unlocked by schedule - options	Yes	
	Door held - options	Yes	
	Door forced open - options	Limited ²	
	Unlock schedules	Online	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	Yes	
	Time to ignore REX after granting access (in seconds)	Yes	
	Ignore REX events while door is open (On/Off)	Yes	
	Time to ignore REX after door closes (in seconds)	Online	
	Visitor escort and two-person rule		
Maximum delay between card presentation (in sec.)	No		
Enforce two-person rule (On/Off) on Door side	No		
Manual actions on doors in Security Desk ³	Manually unlock doors	Yes	
	Reader shunting (activate/deactivate reader)	Online	
	Override unlock schedules	Online	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	No
	Battery fail (<i>Low battery</i>)	No
	Door open/closed	Yes
	Door locked/unlocked	Yes
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	Online
	Visitor escort rule (On/Off)	No
	Interlock	Online
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	Online ⁴
	Presence timeout (forget area presence after a certain delay)	Online
	Strict (antipassback checked on both area entrance and exit)	Online
	On schedule	Online
	Global antipassback	Online
	First-person-in rule	
	Enforce on door unlock schedule	No
Enforce on access rules	No	
Elevator control	Elevators	Online
Zone management	I/O zone	Online
	Hardware zone	
	Zone arming input	Online ⁵
	Zone arming schedule	Online
	Zone arming and entry delays	Online

Feature group	Security Center feature	Supported
	Zone I/O linking	Online
	Countdown buzzer	Online

¹ Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

² The **Reader buzzer behavior** options are only supported with online operations.

³ The Synergis™ unit must be connected to the Access Manager.

⁴ Not recommended for Card-In/REX-Out doors, because a cardholder's presence in the area cannot be verified

⁵ The zone inputs must not be configured on a door.

Enrolling DDS RS-485 controllers

For the Synergis™ unit to communicate with the DDS controllers connected to its RS-485 interface, you must enroll them with Synergis™ Appliance Portal.

Before you begin

Connect the DDS modules to the Synergis™ unit's RS-485 channels (A, B, C, or D) as follows:

- Connect the Rx\L of the DDS module to the "-" of the channel.
- Connect the Tx\H of the DDS module to the "+" of the channel.
- Connect the 0v of the DDS module to the "G" of the channel.

To enroll the DDS controllers connected to the Synergis™ unit:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration** > **Hardware**
- 3 At the top of the *Hardware* column, click **Add** (+).
- 4 In the *Add hardware* dialog box, select **DDS** as the **Hardware type**.
- 5 Select the **Channel** (A, B, C, or D).
All interface modules connected to the same channel must be from the same manufacturer.
- 6 In the same dialog box, add all interface modules connected to the same channel.
Do one of the following:
 - To enroll manually, enter the physical address (0 to 31) configured on the DDS module and click **Add** (+). Then select the exact module type.

The screenshot shows the 'Add hardware' dialog box with the following configuration:

- Hardware type: DDS
- Channel: B
- Interface module type: TPL
- Physical: 0

At the bottom, there are buttons for 'Add', 'Scan', 'Cancel', and 'Save'.

Repeat as necessary to configure all modules connected to the same channel.

- To enroll automatically, click **Scan**.

The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

If the controller does not find all connected interface modules, [make sure they all have a different physical address](#).

7 Click **Save**.

The hardware type, channel, and interface module you just added appear in the *Hardware configuration* page.

8 For each interface module you just added, select it from the *Hardware configuration* page, and configure its settings.

For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.

9 At the bottom of the page, click **Save**.

10 Test your interface module connection and configuration from the I/O diagnostics page.

For information about testing interface modules, see the *Synergis™ Appliance Configuration Guide*.

After you finish

Enroll the Synergis™ unit in Security Center (see the *Synergis™ Appliance Configuration Guide*).

Preparing to enroll DDS IP controllers

Before you can enroll a DDS IP controller on the Synergis™ unit, you must assign a static IP address to its TCP/IP extension board by connecting to it through a serial port.

Before you begin

Make sure you have the following:

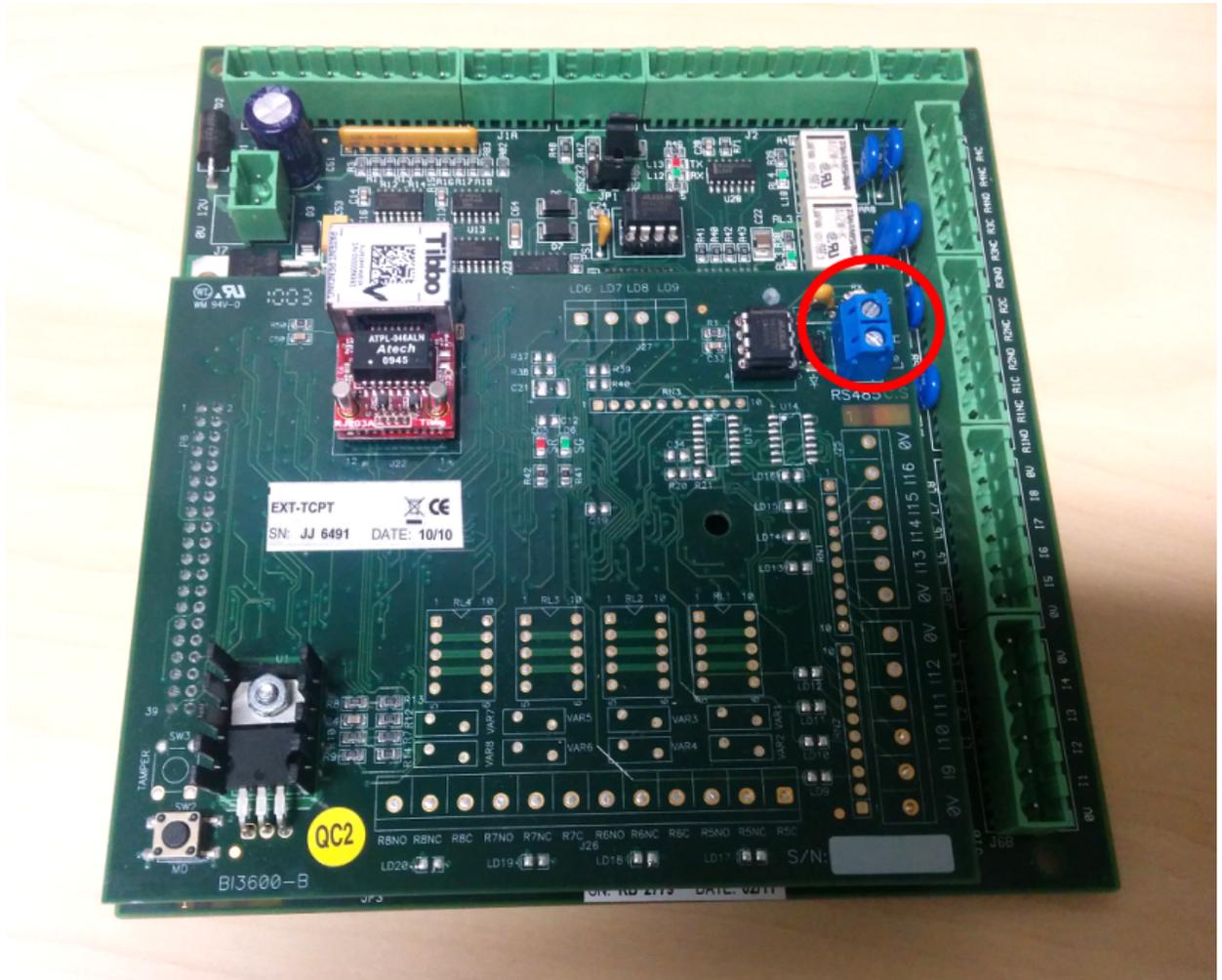
- USB-to-Mini-USB cable.
- [Four-port RS-485 module](#) (ask your representative of Genetec Inc. if you do not have one).
- Setup program for *Tibbo Device Server Toolkit* (either *tdst-5-09-12-x64.exe* or *tdst-5-09-12-x86.exe*). Ask your representative of Genetec Inc.
- Latest version of Synergis™ Software and the *Tibbo.smc* plugin. For information about checking and upgrading the Synergis™ firmware, see the *Synergis™ Appliance Configuration Guide*.

What you should know

The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

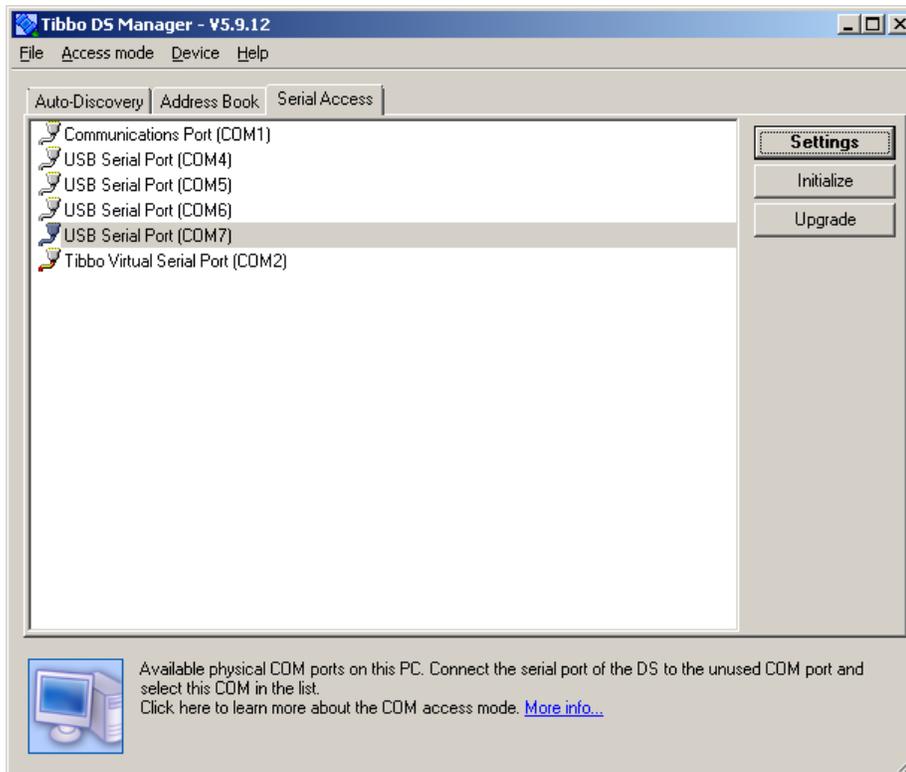
To prepare to enroll a DDS IP controller:

- 1 Attach the TCP/IP extension board to the TPL controller.
- 2 Connect the L and H connectors (circled in red) on the TCP/IP extension board to the “-” and “+” connectors respectively of one of the Four-port RS-485 module channels (A, B, C, or D)..

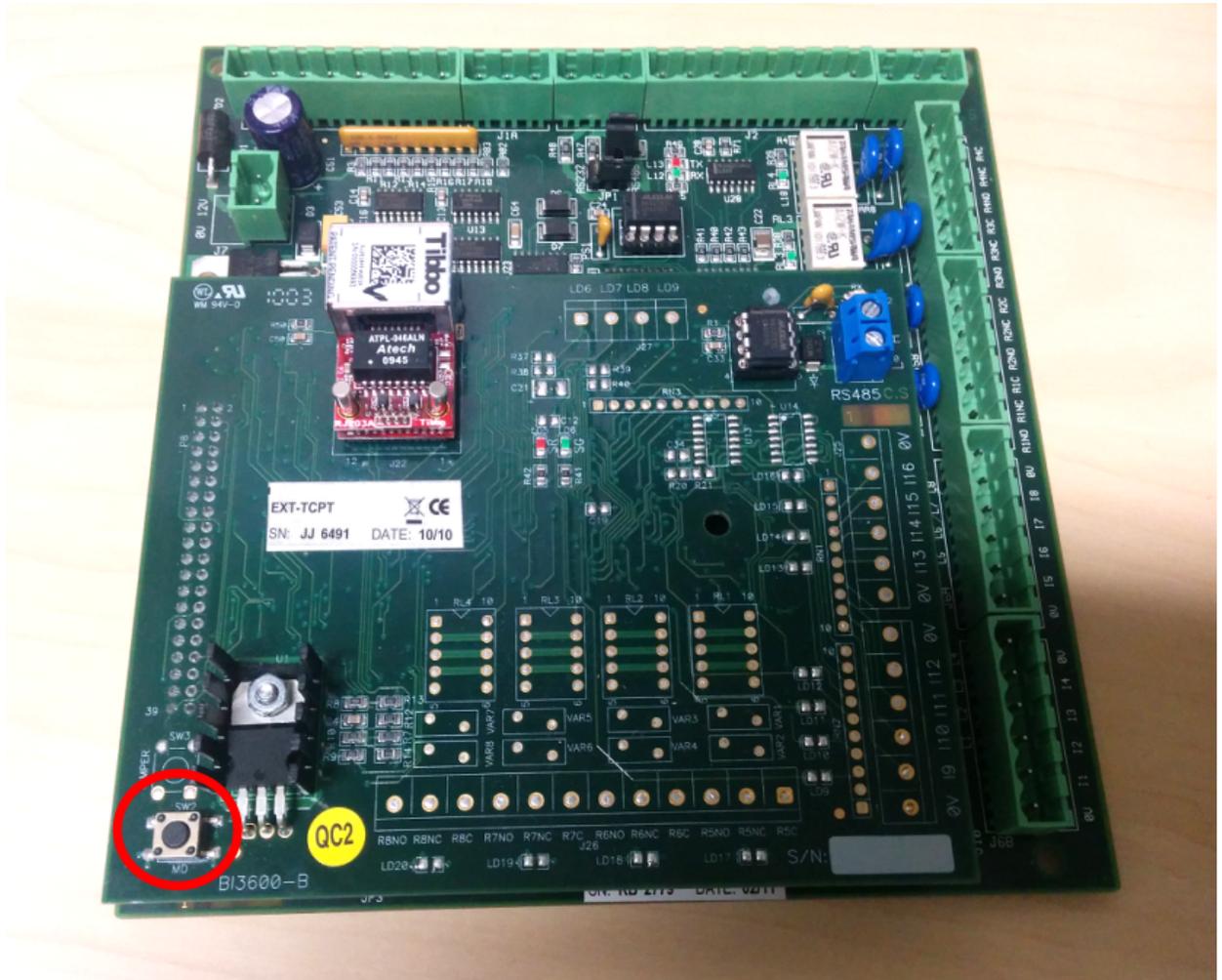


- 3 On the [Four-port RS-485 module](#), make sure that the CTS switch corresponding to the connected channel is set to ON (up) position, and the echo switch is set to the OFF (left) position.
- 4 Install *Tibbo Device Server Toolkit* on your computer.
Choose either the x86 or the x64 package based on the type of machine you have.
- 5 Connect the Four-port RS-485 module to your computer using the USB-to-mini-USB cable.
- 6 Run *Tibbo DS Manager* (`C:\Program Files\Tibbo\TDST\tdsman.exe`) as an administrator.
- 7 Click **Serial Access** and select the COM port corresponding to the channel to which the TCP/IP extension board is connected.

The four channels found on the Four-port RS-485 module are labelled “USB Serial Port (COMx)”. The first one corresponds to channel A, the second one to channel B, the third one to channel C, and the fourth one to channel D.



- 8 Click *Settings*, and do one of the following.
 - If you see the message “Press the setup button on the device”, continue with Step 9.
 - If you see the message "The device has responded with an error code. Click here to view which command failed", then make sure that the echo switch is turned OFF on the [Four-port RS-485 module](#) for the channel you are using.
 - If you see the message "Unable to open the serial port. The serial port may be in use by another program", then verify you selected the right COM port, or that no other program is using the same COM port that is connected to the TCP/IP extension board.
- 9 Press the setup button (labelled **SW2**) on the TCP/IP extension board.



10 In the *Settings* dialog box that appears, enter the following:

Network tab

- *DHCP*: 0 - Disabled
- *IP-address*: IP address assigned to the DDS controller
- *Port*: Port number (default=1001)

Connection tab

- *Transport protocol*: 1 - TCP
- (*Hardening*) *Link Service Login*: 0-Disabled
- (*Hardening*) *Inband commands*: 0-Disabled
- (*Hardening*) *Data login*: 0-Disabled
- (*Hardening*) *Routing Mode*: 0-Server (Slave)
- (*Hardening*) *Accept connection from*: 1-Current Destination IP address

Serial port tab

- *RTS/CTS flow control*: 0 - Disabled or remote
- *Baud rate*: 3 - 9600 bps

11 Click **OK**, and press the setup button on the TCP/IP extension board when prompted. For the location of the setup button, see Step 9.

12 Disconnect the TCP/IP extension board from the Four-port RS-485 module.

- 13 Set the local echo switch back to its original position on the Four-port RS-485 module, and reconnect it to the Synergis™ unit if necessary (only if you are using the Synergis™ Master Controller).
- 14 Connect the TCP/IP extension board to the same subnet where the Synergis™ unit is found.
The Ethernet connector is located under the label “Tibbo” on the TCP/IP extension board.

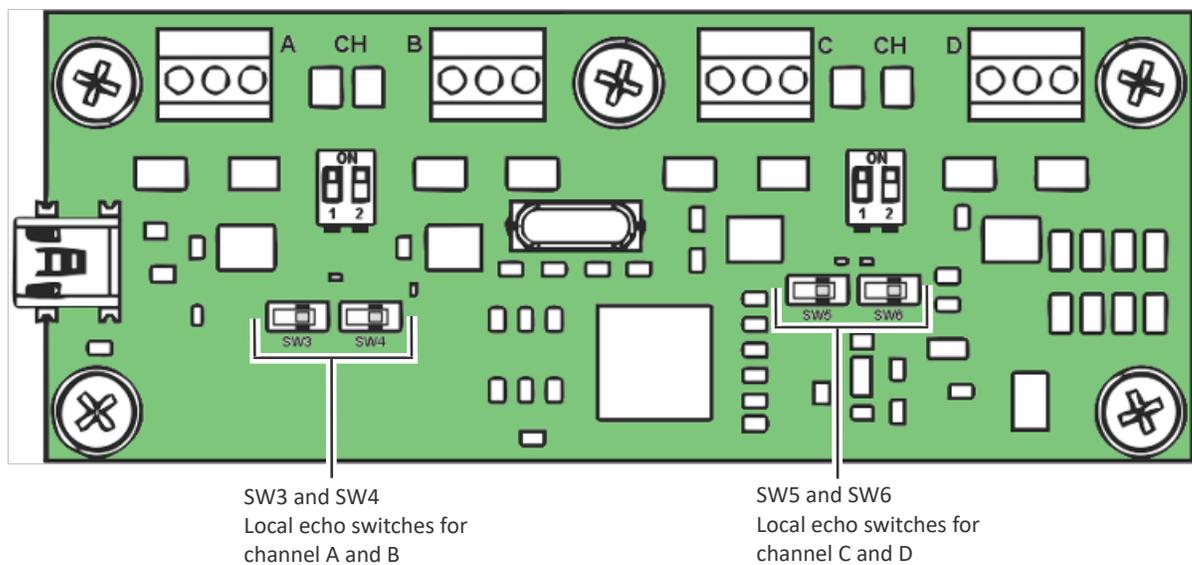
After you finish

[Enroll the DDS IP controller.](#)

About the RS-485 local echo switches on SMC units

All RS-485 channels support the local echo feature. The local echo can be turned on or off with the switches SW3 to SW6 found on the Four-port RS-485 module.

See the following diagram for the location of those switches on the board. The ON position is when the switch is aligned with its vertical marker (to the right).



IMPORTANT: When the Four-port RS-485 module is used to connect an TPL door controller to the Synergis™ unit, the local echo switch must be set to the ON position (to the right). When the Four-port RS-485 module is used to connect the TCP/IP extension board to your PC, the local echo switch must be set to the OFF position (to the left).

Enrolling DDS IP controllers

For the Synergis™ unit to communicate with the DDS controllers connected to your IP network, you must enroll them on the Synergis™ unit.

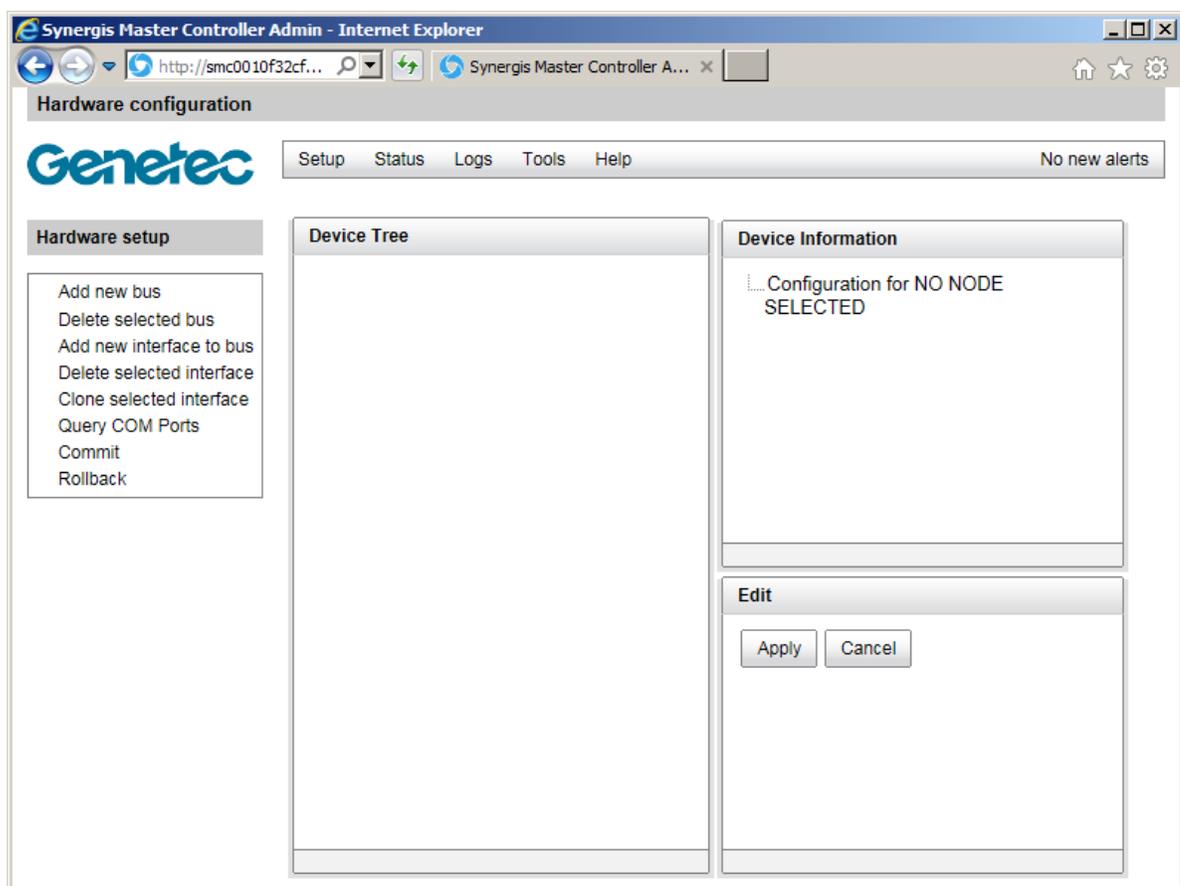
Before you begin

Make sure you have completed the following:

- [Prepare to enroll the DDS IP controller.](#)
- Latest version of Synergis™ Softwire and the *Tibbo.smc* plugin. For information about checking and upgrading the Synergis™ firmware, see the *Synergis™ Appliance Configuration Guide*.

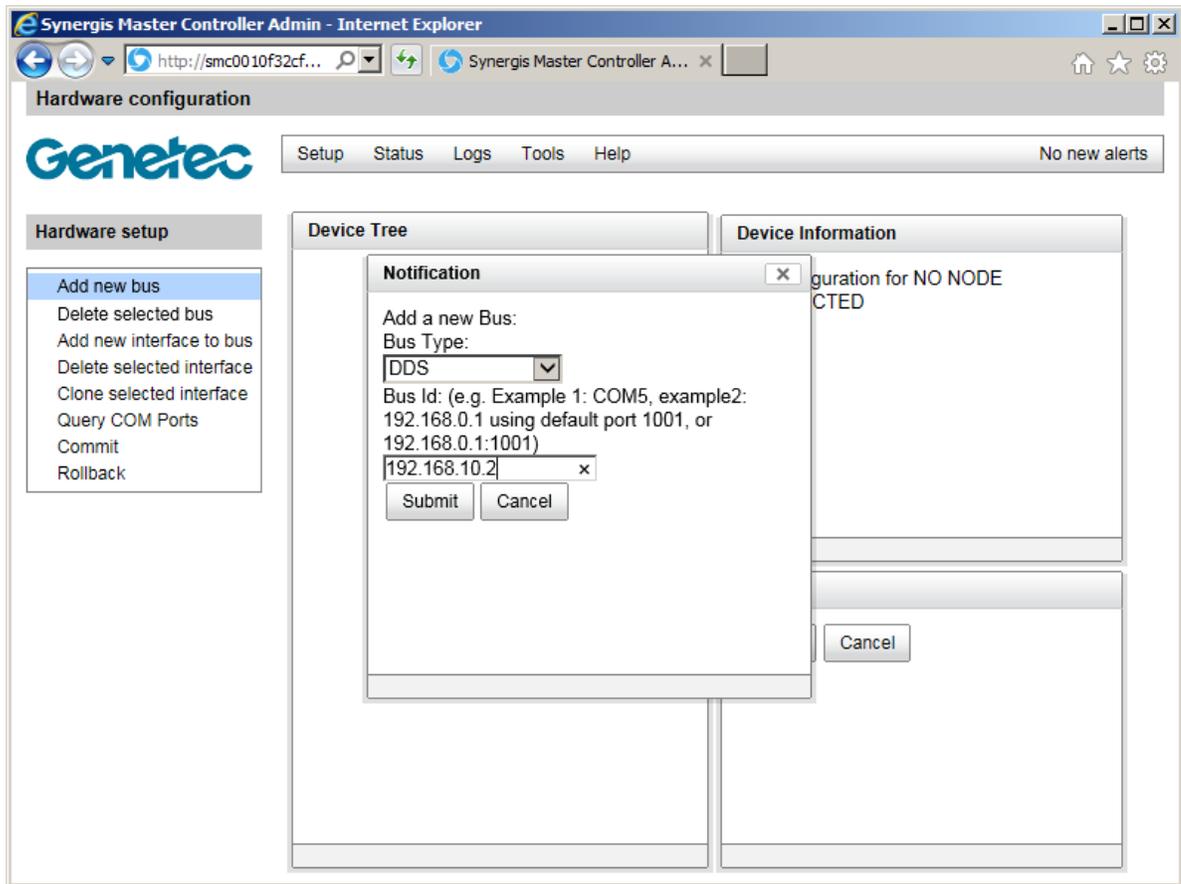
To enroll a DDS IP interface module:

- 1 Open a web browser.
- 2 In the browser's address bar, type `http://` followed by the Synergis™ unit's hostname or IP address, followed by `/smc/index.html` (for example, `http://SCL0010F32CF482/smc/index.html`).

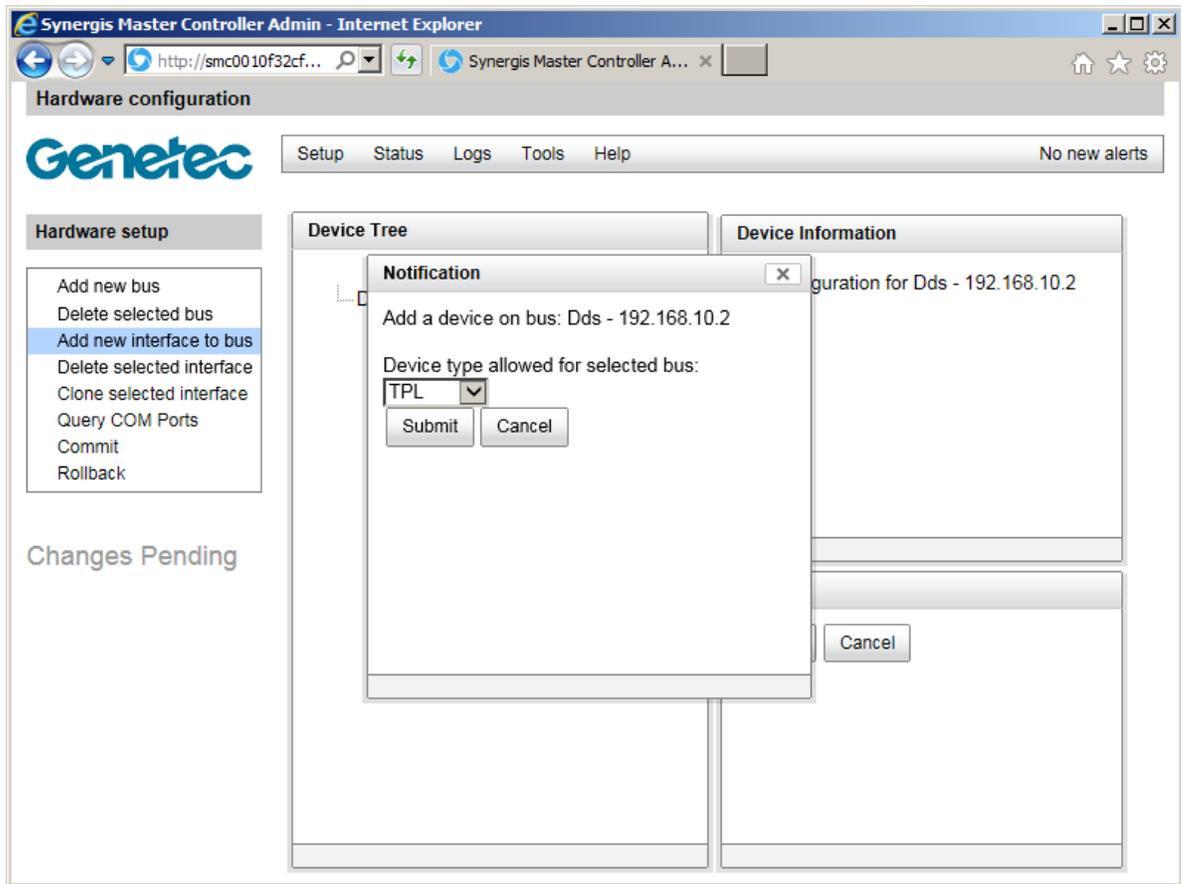


- 3 Click **Add new bus**, and select DDS as the bus type, and enter the IP address assigned to the DDS IP controller.

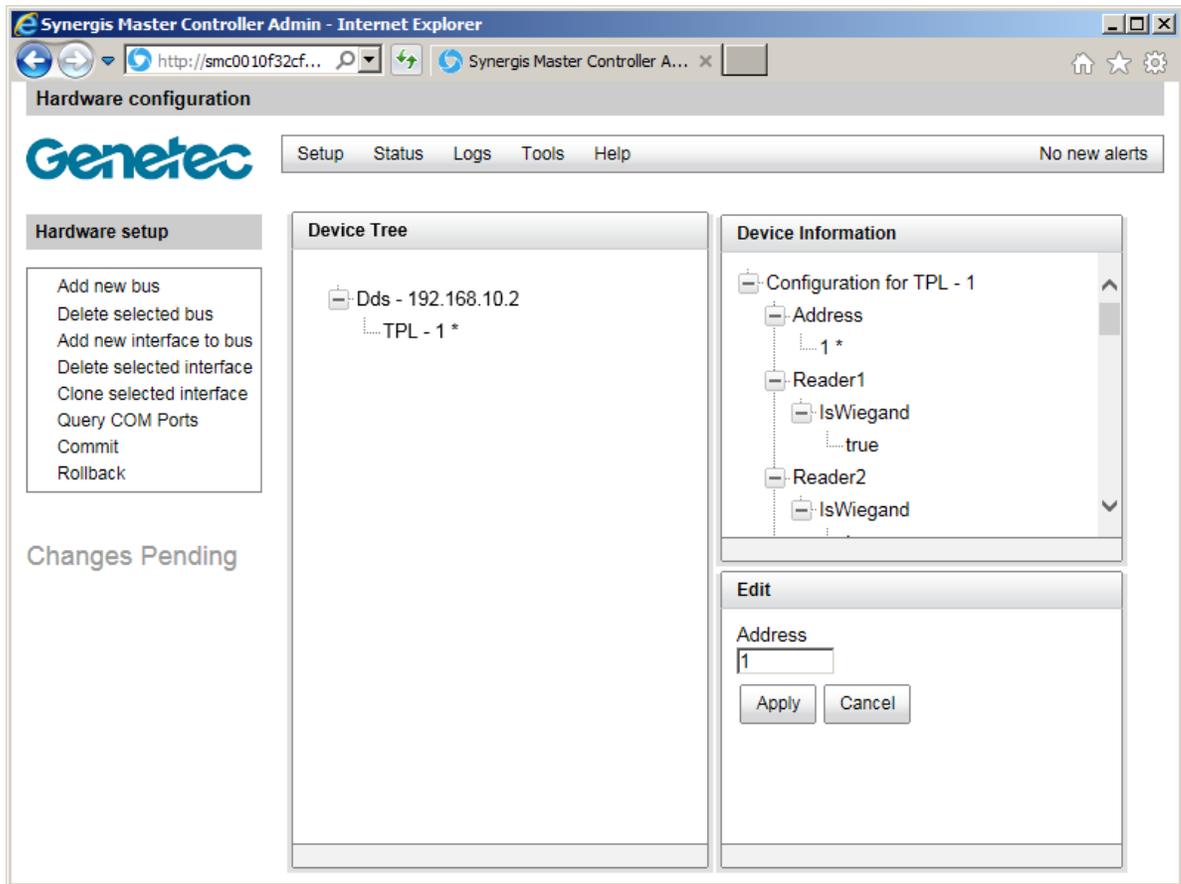
If the port number is different from the default value (1001), append it to the IP address, after a colon (“:”).



- 4 In the **Device Tree**, select the **DDS**.
An "*" appears after the bus name to indicate that it has been selected.
- 5 Click **Add new interface to bus**, select **TPL** as the device type, and then click **Submit**.



- 6 In the **Device Tree**, select the TPL device you added, and make sure that the **Address** indicated in the **Device Information** section matches to the physical address set on your DDS interface module.



- 7 Click **Commit**.

The Ethernet port on the DDS controller should start flashing.

- 8 Log on to Synergis™ Appliance Portal, click **Hardware**, click the TPL device, and test your connections with the *I/O diagnostics* page. For more information, see the *Synergis™ Appliance Configuration Guide*.

After you finish

Enroll the Synergis™ unit in Security Center (see the *Synergis™ Appliance Configuration Guide*).

Setting the physical address of TPL door controllers

All TPL modules connected to the same RS-485 channel or found on the same LAN must use different physical addresses.

What you should know

The physical address of a TPL door controller is set using two sets of DIP switches, DS2 and JP4. If you have an TCP/IP extension board attached to the TPL controller board, you must first remove it before you can access the DIP switches.

To set the physical address of a TPL door controller:

- 1 Set DS2/1 to 1 or ON.
- 2 Set the physical address on JP4 according to the following tables.

JP4/1:	0	1	0	1	0	1	0	1	0	1	0	1	0	1		
JP4/2:	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
JP4/3:	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
JP4/4:	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
JP4/5:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

JP4/1:	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
JP4/2:	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
JP4/3:	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
JP4/4:	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
JP4/5:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

NOTE: JP4 (6, 7, 8) are used to set the reader communication protocol. For example, for Wiegand to read up to 50 bits without parity check, set JP4/7 to 1 or ON, and DS2/4 to 1 or ON. For more information, see the documentation from DDS corresponding to your specific device.

HID VertX Sub-Panels

This section includes the following topics:

- ["Supported HID VertX sub-panels"](#) on page 109
- ["Supported HID VertX sub-panel features"](#) on page 110
- 112 • ["Supported Synergis appliance features for HID VertX sub-panel integration"](#) on page
- 113 • ["Supported Security Center features for HID VertX sub-panel integration"](#) on page
- ["Enrolling the HID VertX sub-panels connected to the Synergis unit"](#) on page 116
- ["Enabling reader supervision for HID VertX V100"](#) on page 118

Supported HID VertX sub-panels

For HID VertX sub-panel integration, each VertX Vnnn panel is viewed as an interface module.

Synergis™ Softwire supports the following HID VertX sub-panels.

Model	Description	Program	EPROM
V100	Door/Reader interface with two card readers, supporting Wiegand or Clock-and-Data credential formats.	113	110
V200	Input monitor interface with 16 supervised input circuits.	106	105
V300	Output control interface with 12 latching Form-C relay contacts.	107	104

Supported HID VertX sub-panel features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following HID VertX sub-panel features.

Features	Supported
General characteristics	
Category of interface module	Sub-panel
Communication protocol	RS-485
Encrypted communication	N/A
Online operation (connected to the Synergis™ unit)	
Supervised mode	N/A
Dependent mode	Yes
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	N/A
Degraded mode	Yes
Reader communication protocols	
Wiegand	Yes
OSDP	N/A
OSDP (Secure Channel)	N/A
Clock and Data (Magnetic Stripe) — Also known as ABA format	Yes
F2F	N/A
Proprietary	N/A
Scalability	
Maximum number of offline events	N/A
Maximum number of credentials (for autonomous decision making)	N/A
Maximum credential length (in bits)	136 ¹
Maximum number of interface modules per RS-485 channel	16 ²
Recommended maximum number of interface modules per Synergis™ unit	32

¹ The certified limit is 136 bits. The actual limit might be higher.

² Having many interface modules per channel decreases the polling rate per interface. This is a consideration if you have any PIN readers configured in mode 00, because you increase the chance of a digit being missed when someone enters their PIN quickly, resulting in a denied access.

Supported Synergis™ appliance features for HID VertX sub-panel integration

Not all Synergis™ appliance features are supported with the integration of HID VertX sub-panels.

The HID VertX sub-panel integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Softwire](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability)	
Manual enrollment (<i>Add hardware</i> dialog box)	Yes
Automatic enrollment (Scan button)	Yes
Property configuration	Yes
Configuration cloning (Clone button)	Yes
I/O diagnostics (live monitoring of inputs, relays, and readers)	Yes
Interface module firmware display	No
Interface module firmware upgrade (apply recommended firmware)	No
Access control behavior (Synergis™ unit-wide settings) ^{1, 2}	
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	Online
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	Online
Maximum PIN length in digits ³	15
Degraded mode settings	Yes
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	Yes

¹ The door behavior settings are overwritten by the individual door settings configured in Security Center.

² Only applies to VertX V100.

³ For interface modules that support HID mode-00 readers.

Supported Security Center features for HID VertX sub-panel integration

Not all Security Center access control features are supported with the integration of HID VertX sub-panels. The HID VertX sub-panel integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings) ¹	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	Yes	
	Extended grant time	Online	
	Entry time (Standard/Extended) ²	Online	
	Door relock - options	Online	
	When door is unlocked by schedule - options	Online	
	Door held - options	Online	
	Door forced open - options	Online	
	Unlock schedules	Online	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	Yes	
	Time to ignore REX after granting access (in seconds)	Online	
	Ignore REX events while door is open (On/Off)	Online	
	Time to ignore REX after door closes (in seconds)	Online	
	Visitor escort and two-person rule		
	Maximum delay between card presentation (in sec.)	Online	
Enforce two-person rule (On/Off) on Door side	Online		
Manual actions on doors in Security Desk ³	Manually unlock doors	Online	
	Reader shunting (activate/deactivate reader)	Online	
	Override unlock schedules	Online	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	Online
	Battery fail (<i>Low battery</i>)	Online
	Door open/closed	Online
	Door locked/unlocked	Online
	Door forced open	Online
	Door held open for too long	Online
	Door secured	N/A
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	Online
	Visitor escort rule (On/Off)	Online
	Interlock	Online
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	Online ⁴
	Presence timeout (forget area presence after a certain delay)	Online
	Strict (antipassback checked on both area entrance and exit)	Online
	On schedule	Online
	Global antipassback	Online
	First-person-in rule	
	Enforce on door unlock schedule	Online
	Enforce on access rules	Online
Elevator control	Elevators	Online
Zone management	I/O zone	Online
	Hardware zone	Online

¹ Only apply to VertX V100.

² Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

³ The Synergis™ unit must be connected to the Access Manager.

⁴ Not recommended for Card-In/REX-Out doors, because a cardholder's presence in the area cannot be verified

Enrolling the HID VertX sub-panels connected to the Synergis™ unit

To establish communication between the Synergis™ unit and the attached interface modules, you need to configure them in Synergis™ Appliance Portal.

Before you begin

Attach the HID VertX modules to the channels (A, B, C, or D) of your Synergis™ unit.

To enroll the HID VertX interface modules connected to the Synergis™ unit:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration > Hardware**
- 3 At the top of the *Hardware* column, click **Add (+)**.
- 4 In the *Add hardware* dialog box, select **HID VertX** as the **Hardware type**.
- 5 Select the **Channel** (A, B, C, or D).

All interface modules connected to the same channel must be from the same manufacturer.

- 6 In the same dialog box, add all interface modules connected to the same channel.
You can enroll the interface modules automatically or manually.

TIP: If you know the physical addresses of the modules and you only have a few to enroll, it would be faster to enroll them manually.

Do one of the following:

- To enroll automatically, click **Scan**.

The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

If the controller does not find all connected interface modules, make sure they all have a different physical address.

- To enroll manually, enter the physical address (0 to 15) configured on the HID interface device, select the model type, and then click **+**.

The screenshot shows a configuration window titled "Add hardware". It contains the following elements:

- Hardware type:** A dropdown menu with "VertX" selected.
- Channel:** A dropdown menu with "A" selected.
- Interface module type:** A dropdown menu with "V100" selected.
- Physical address:** A text input field containing "0".
- Table:** A table with two columns: "Interface module type" and "Physical address".
- Buttons:** "Add", "Scan", "Cancel", and "Save".

Repeat as necessary to configure all modules connected to the same channel.

- 7 Click **Save**.
The hardware type, channel, and interface module you just added appear in the *Hardware configuration* page.
- 8 For each interface module you just added, select it from the *Hardware configuration* page, and configure its settings.
For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.
- 9 At the bottom of the page, click **Save**.
- 10 Test your interface module connection and configuration from the I/O diagnostics page.
For information about testing interface modules, see the *Synergis™ Appliance Configuration Guide*.

After you finish

Enroll the Synergis™ unit in Security Center (see the *Synergis™ Appliance Configuration Guide*).

Enabling reader supervision for HID VertX V100

To receive *Door offline* events when the reader connected to a VertX V100 panel is either disconnected or powered off, you must configure the **I'm Alive** reader setting in Config Tool and program the reader with the appropriate configuration card.

Before you begin

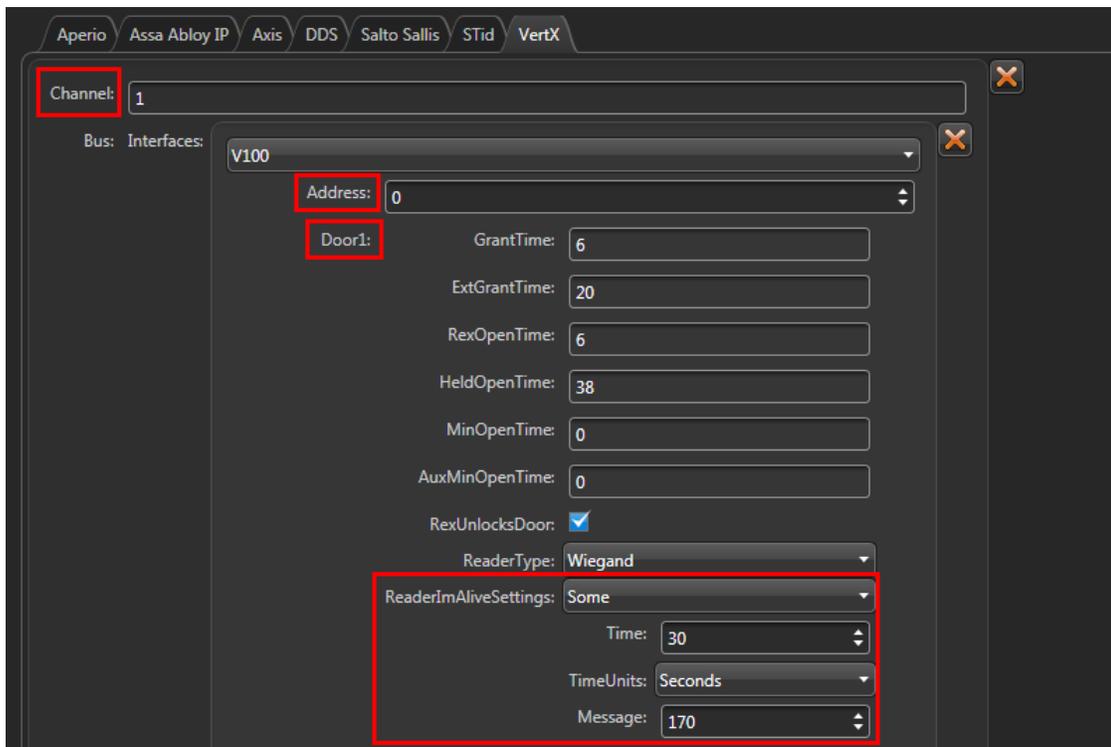
[Enroll the VertX V100 panel on the Synergis™ unit.](#)

What you should know

Reader supervision is only supported for readers connected to a VertX V100 panel that is controlled by a Synergis™ unit. To use this feature, you need Synergis™ Softwire 10.2 or later.

To enable the supervision of a reader connected to a V100 panel:

- 1 From the Config Tool home page, open the *Access control* task.
- 2 Click **Roles and units**, and then click the Synergis™ unit (🌐).
- 3 Click **Hardware**, and then scroll to the V100 panel to which the reader is connected.
If your Synergis™ unit is controlling multiple V100 panels, make sure you identify the correct reader by its **Channel**, its physical **Address**, and its door number (**Door1** or **Door2**).
- 4 Under the selected door, click **ReaderImAliveSettings**, and change its value to **Some**.
The **Time** must be equal or greater than the **I'm Alive** time found on the reader configuration card, and the **Message** must correspond to the **I'm Alive** message (170 is the decimal equivalent of AA in hexadecimal).



- 5 Click **Apply**.
- 6 Configure the reader using the appropriate field programming card (also known as a configuration card).

When this reader is disconnected from the V100 panel or powered down, you now get the event *Door offline: Device is offline* on the door that it is associated to.

Honeywell Controllers

This section includes the following topics:

- ["Supported Honeywell controllers"](#) on page 121
- ["Supported features for Honeywell controllers"](#) on page 122

Supported Honeywell controllers

For Honeywell controller integration, the Honeywell controllers are called interface modules because they serve to connect the PW6K downstream panels to the Synergis™ unit.

Only the Honeywell PW6K controllers communicate directly with the Synergis™ unit.

NOTE: Honeywell controller integration requires Security Center 5.3 SR1 (or more recent versions) and Synergis™ Softwire 10.0 (or more recent versions).

Synergis™ Softwire supports the following Honeywell devices.

Model	Description
PW6K1IC	IP controller with two supervised RS-485 buses supporting any combination of up to 32 I/O or reader sub-panels. The PW6K1IC can control up to 64 doors.
PW6K panels	PW6K downstream panels (expansion modules) used with the PW6K1IC controller: <ul style="list-style-type: none"> • PW6K1R2 – Dual reader sub-panel with eight inputs and six outputs, equivalent to Mercury MR52. • PW6K1IN – 16-input sub-panel, equivalent to Mercury MR16IN. • PW6K1OUT – 16-output sub-panel, equivalent to Mercury MR16OUT.
PW5K panels	PW5K downstream panels (expansion modules) used with the PW6K1IC controller: <ul style="list-style-type: none"> • PW5K1R1 – Single reader sub-panel with two inputs and two outputs, equivalent to Mercury MR50. • PW5K1R2 – Dual reader sub-panel with eight inputs and six outputs, equivalent to Mercury MR52. • PW5K1IN – 16-input sub-panel, equivalent to Mercury MR16IN. • PW5K1OUT – 16-output sub-panel, equivalent to Mercury MR16OUT.
Allegion Schlage locks	Honeywell PW6K1IC controller can also be used with Allegion Schlage AD Series locks. See Supported Allegion Schlage locks on page 6.
SimonsVoss SmartIntego locks	Honeywell PW6K1IC controller can also be used with SimonsVoss SmartIntego locks. See Supported SimonsVoss locks on page 169.

Supported Honeywell firmware versions

In order to benefit from all the features of this integration, a specific range of firmware versions must be used.

The Honeywell firmware versions that Synergis™ Softwire 10.6 supports are:

Model	Minimum	Recommended
PW6K1IC	2.7.5	2.8.2 ^a

^a For certain intelligent controllers, such as Assa Abloy IP Locks, Axis, and Mercury EP, you can apply the recommended firmware from the *Interface upgrade* page of Synergis™ Appliance Portal. For other manufacturers, you might have to use the manufacturer's software to apply the recommended firmware.

Supported features for Honeywell controllers

Honeywell PW6K series controllers are very similar to the Mercury EP2500 controller, and their integration supports the same feature set as for the Mercury controllers.

Supported Honeywell controller features

See [Supported Mercury controller features](#) on page 127.

Supported Synergis™ appliance features for Honeywell controller integration

See [Supported Synergis™ appliance features for Mercury controller integration](#) on page 129.

NOTE: Honeywell PW-series controllers only support up to 8-digit PINs.

Supported Security Center features for Honeywell controller integration

See [Supported Security Center features for Mercury controller integration](#) on page 130.

Enrolling Honeywell controllers on the Synergis™ unit

See [Enrolling Mercury controllers on the Synergis™ unit](#) on page 137.

Mercury Controllers

This section includes the following topics:

- ["Supported Mercury controllers"](#) on page 124
- ["Supported Mercury controller features"](#) on page 127
- 129 • ["Supported Synergis appliance features for Mercury controller integration"](#) on page
- 130 • ["Supported Security Center features for Mercury controller integration"](#) on page
- ["Preparing to enroll the Mercury controller"](#) on page 133
- ["Enrolling Mercury controllers on the Synergis unit"](#) on page 137
- ["Adding OSDP \(Secure Channel\) readers to an EP controller"](#) on page 140
- ["Adding MR51e panels to an EP controller"](#) on page 142
- ["Access control unit - Synergis - Peripherals tab"](#) on page 144

Supported Mercury controllers

For Mercury controller integration, the Mercury controllers are called interface modules because they connect the downstream panels (MR50, MR52, and so on) to the Synergis™ unit.

Only the Mercury EP and M5-IC controllers communicate directly with the Synergis™ unit.

NOTE: Mercury controller integration requires Security Center 5.3 SR1 (or more recent versions) and Synergis™ Softwire 10.0 (or more recent versions).

Synergis™ Softwire supports the following Mercury devices.

Model	Description
EP1501	IP controller with two inputs, two outputs, and two onboard reader connections. One reader connection can connect up to 8 expansion boards, allowing the EP1501 to control up to 17 doors. (datasheet)
EP1502	IP controller with eight inputs, four outputs, two reader connections, and one RS-485 bus supporting up to 32 downstream panels. The EP1502 can control up to 64 doors. (datasheet)
EP2500	IP controller with two RS-485 buses, supporting up to 64 doors. (datasheet)
EP4502	IP controller similar to the EP1502 with an extra RS-485 port. (datasheet)
MR panels	<p>Mercury downstream panels (expansion modules) supported with the EP controllers:</p> <ul style="list-style-type: none"> • MR50 – Single reader sub-panel with two inputs and two outputs (datasheet) • MR51e – Single door, network ready, PoE interface panel (datasheet) • MR52 – Dual reader sub-panel with eight inputs and six outputs (datasheet) • MR16IN – 16-input sub-panel (datasheet) • MR16OUT – 16-output sub-panel (datasheet) <p>Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the Compatibility View Settings and clear Display intranet sites in Compatibility View.</p> 
Allegion Schlage locks	EP1501 and EP2500 controllers can also be used with Allegion Schlage AD Series locks. See Supported Allegion Schlage locks on page 6.
SimonsVoss SmartIntego locks	EP1501 and EP2500 controllers can also be used with SimonsVoss SmartIntego locks. See Supported SimonsVoss locks on page 169.

Model	Description
M5 Bridge	<p>All Mercury M5 Bridge panels are designed to be plug-and-play compatible with your existing Casi Micro5 enclosure and offer one-for-one board replacement with your existing panels.¹</p> <ul style="list-style-type: none"> • M5-IC – Intelligent controller (datasheet) • M5-2K – 4-F2F reader, 10-input, 8-output control device (datasheet)² • M5-2RP – 2-reader control device (datasheet) • M5-2SRP – 2-reader control device with supervised inputs (datasheet) • M5-8RP – 8-reader control device (datasheet) • M5-20IN – 20-input control device (datasheet) • M5-16DO – 16-output control device (datasheet)³ • M5-16DOR – 16-output control device (datasheet) • M5-COM – Power and Comms controller (datasheet)⁴ <p>Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the Compatibility View Settings and clear Display intranet sites in Compatibility View.</p> 

MS Bridge	<p>All Mercury MS Bridge panels are designed to be direct retrofits of iSTAR Pro panels from Software House. The MS-I8S and MS-R8S panels can also be connected to an EP controller. This integration requires Security Center 5.6 and later.</p> <ul style="list-style-type: none"> • MS-ICS – controller panel that replaces the iSTAR Pro GCM module (datasheet) • MS-ACS – interface panel that replaces the iSTAR Pro ACM module (datasheet) • MS-I8S – 8-input panel that replaces the iSTAR Pro I8 module (datasheet) • MS-R8S – 8-output panel that replaces the iSTAR Pro R8 module (datasheet) <p>Watch this video to learn more. Click the Captions icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the Compatibility View Settings and clear Display intranet sites in Compatibility View.</p> 
------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

¹ When using inputs on the F2F reader or inputs from the interface reader ports, the odd numbered inputs shown in Config Tool are used for REX, and the even numbered inputs are used for door contacts.

² Together, the M5-IC and the M5-2K replace the Casi M2000 enclosure circuit board. There are up to eight enclosures per M5-IC: the first enclosure has one M5-IC plus one M5-2K, and the next seven enclosures have one M5-COM plus one M5-2K.

³ Digital outputs (solid state switches).

⁴ Used for downstream communication with add-on enclosures with no M5-IC.

Supported Mercury firmware versions

In order to benefit from all the features of this integration, a specific range of firmware versions must be used.

The Mercury firmware versions that Synergis™ Softwire 10.6 supports are:

Model	Minimum	Recommended
EP1501, EP1502, EP2500, M5-IC	1.19.4 ¹	1.24.4 ²
EP4502	1.20.9 ¹	1.24.4 ²
MS-ICS	1.22.9 ¹	1.24.4 ²
MR51e	1.4.2	Latest

¹ To use OSDP (Secure Channel) readers, firmware 1.22.9 or later is required if the reader is connected directly to the EP board, and firmware 1.23.6 or later is required if the reader is connected to a downstream board (red SIOv3 MR50 and MR52 boards).

² For certain intelligent controllers, such as Assa Abloy IP Locks, Axis, and Mercury EP, you can apply the recommended firmware from the *Interface upgrade* page of Synergis™ Appliance Portal. For other manufacturers, you might have to use the manufacturer's software to apply the recommended firmware.

CAUTION: Firmware version 1.19.4 has a bug that requires the F2F readers to be connected differently as a workaround. The bug is fixed in version 1.20.7. If you upgrade your controllers to the new version, make sure you also reconnect your F2F readers accordingly.

Supported Mercury controller features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following Mercury controller features.

Features	Supported
General characteristics	
Category of interface module (EP and M5-IC)	Intelligent controller
Communication protocol	IP only
Encrypted communication	Yes ¹
Online operation (connected to the Synergis™ unit)	
Supervised mode	No
Dependent mode	Yes
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	Yes
Degraded mode	N/A
Reader communication protocols	
Wiegand	Yes
OSDP	Yes
OSDP (Secure Channel)	Yes ²
Clock and Data (Magnetic Stripe) — Also known as ABA format	Yes
F2F	Yes
Proprietary	N/A
Scalability	
Maximum number of offline events	50 000 ³
Maximum number of credentials (for autonomous decision making)	250 000
Maximum credential length (in bits)	64 ⁴
Maximum number of interface modules per RS-485 channel	N/A
Recommended maximum number of interface modules per Synergis™ unit	32/256 ⁵

¹ Encryption is mandatory with Synergis™ Softwire 10.2 and later.

² The OSDP (Secure Channel) reader must be [paired to a reader port on the EP controller](#). The certified readers are: *HID multiCLASS SE RP40*, *Allegion aptiQ MT15-485*, and *Nexus Cidron SC9100-MD-MP-VG2*. Other models might also work. To use OSDP (Secure Channel) readers, firmware 1.22.9 or later is required if the reader is connected directly to the EP board, and firmware 1.23.6 or later is required if the reader is connected to a downstream board (red SIOv3 MR50 and MR52 boards).

³ There is not always a one-to-one match between an offline log entry and a Security Center event. Mercury controllers are limited to 50 000 offline log entries.

⁴ Up to 8 different credential lengths are supported in *standalone mode*. More can be supported in *dependent mode*.

⁵ There are two values that limit the number of controllers you can connect to the appliance: (1) the maximum number of controllers you can physically connect to the appliance, and (2) the maximum number of controlled readers. For both Synergis™ Cloud Link and SV32, the maximum number of EP controllers and controlled readers are 16 and 128 under Security Center 5.4 and earlier, and 32 and 256 under Security Center 5.5 and later.

Supported Synergis™ appliance features for Mercury controller integration

Not all Synergis™ appliance features are supported with the integration of Mercury controllers.

The Mercury controller integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Softwire](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability)	
Manual enrollment (<i>Add hardware</i> dialog box)	No ¹
Automatic enrollment (Scan button)	No
Property configuration	No
Configuration cloning (Clone button)	No
I/O diagnostics (live monitoring of inputs, relays, and readers)	No
Interface module firmware display	No
Interface module firmware upgrade (apply recommended firmware)	Manual
Access control behavior (Synergis™ unit-wide settings) ²	
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	N/A
Do not generate 'DHO' events when door is unrestricted	Yes
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	Yes
Maximum PIN length in digits ³	15 ⁵
Degraded mode settings	N/A

¹ Mercury controllers are [enrolled from Config Tool](#).

² The door behavior settings are overwritten by the individual door settings configured in Security Center.

³ For interface modules that support HID mode-00 readers.

⁵ A '#' must be entered after the PIN even when the PIN is 15-digits long.

Supported Security Center features for Mercury controller integration

Not all Security Center access control features are supported with the integration of Mercury controllers.

The Mercury controller integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	Yes ¹	
	Extended grant time	Yes ²	
	Entry time (Standard/Extended) ³	Online	
	Door relock - options	Limited ⁴	
	When door is unlocked by schedule - options	Online	
	Door held - options	Yes	
	Door forced open - options	Limited ⁵	
	Unlock schedules	Yes	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	Yes	
	Time to ignore REX after granting access (in seconds)	Online	
	Ignore REX events while door is open (On/Off)	Online	
	Time to ignore REX after door closes (in seconds)	Online	
	Visitor escort and two-person rule		
	Maximum delay between card presentation (in sec.)	No	
Enforce two-person rule (On/Off) on Door side	No		
Manual actions on doors in Security Desk ⁶	Manually unlock doors	Yes	
	Reader shunting (activate/deactivate reader)	Yes	
	Override unlock schedules	Yes	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	Yes
	Battery fail (<i>Low battery</i>)	Yes
	Door open/closed	Yes
	Door locked/unlocked	Yes
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	No
	Visitor escort rule (On/Off)	Yes ⁷
	Interlock	Online
	Antipassback	
	Hard (logs and denies access on <i>Antipassback violation</i>)	Online ⁸
	Presence timeout (forget area presence after a certain delay)	Online
	Strict (antipassback checked on both area entrance and exit)	Online
	On schedule	Online
	Global antipassback	Online
	First-person-in rule	
	Enforce on door unlock schedule	N/A
	Enforce on access rules	N/A
Elevator control	Elevators	Yes ⁹
Zone management	I/O zone	Online
	Hardware zone	
	Zone arming input	Offcenter ¹⁰
	Zone arming schedule	Yes
	Zone arming and entry delays	No

Feature group	Security Center feature	Supported
	Zone I/O linking	Yes
	Countdown buzzer	No

¹ The maximum supported value is 255 seconds.

² The **Extended grant time** cannot be shorter than the **Standard grant time**.

³ Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

⁴ A door that is configured to relock with a timeout after opening features a **Relock on close** option, which still locks after the grant timeout. A door that is configured to relock with a timeout after opening features a **Relock on close** option, which still locks after the grant timeout.

⁵ For the **Reader buzzer behavior** setting, the options *Suppressed* and *Suppressed when door closes* are supported in both online and offline operation modes. The option *Suppressed when access is granted* is treated as *Suppressed when door closes*.

⁶ The Synergis™ unit must be connected to the Access Manager.

⁷ Limitation: A visitor who requires an escort can be escorted by any cardholder who is someone else's escort. The escort that is assigned to the visitor in Security Center is not enforced by the EP controller.

⁸ Not recommended for Card-In/REX-Out doors, because a cardholder's presence in the area cannot be verified

⁹ Floor tracking is not supported. All floor buttons must be controlled by one EP controller. Output relays from different boards can be used, but must be assigned in consecutive blocks. This means that the last output on board A must be followed by the first output on board B if the elevator is configured across multiple boards.

¹⁰ If the zone is linked to a door through event-to-action, and the Mercury controller is operating offline (there is no connection to the Synergis™ unit), the zone does not work.

Preparing to enroll the Mercury controller

Before you enroll the Mercury controller on the Synergis™ unit, you must assign a static IP address to the controller.

Before you begin

Make sure you have the following:

- **EP Series Setup and Configuration Guide.** Instruction manual for connecting to the web portal of your Mercury controller and setting up its IP address (and other configurations).
- **Static IP address.** Static IP address assigned to the controller by your IT department.
- **Physical addresses.** Each interface panel attached to the same RS-485 port of the same Mercury controller must have a unique physical address (configured on a DIP switch).

BEST PRACTICE: If you have many Mercury controllers to enroll on the same Synergis™ unit, it is best to enroll them all at once. Each Mercury controller you add or remove from the Synergis™ unit causes the unit to restart. While the unit restarts, it is offline for about 30 seconds.

What you should know

Mercury controllers enrolled on the same Synergis™ unit cannot be assigned different partitions in Security Center. If you need to assign the Mercury controllers to different partitions, enroll them on different Synergis™ units, and then assign the Synergis™ units to different partitions.

NOTE: The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

To prepare to enroll the Mercury controller:

- 1 On the Mercury controller board, set the DIP switch S1-1 to **ON**.
This gives you a 5 minute window to log on using factory default settings.
- 2 Log on to the Mercury controller through the Mercury device's *Configuration Manager* web page. Use the default IP address (192 . 168 . 0 . 251) and credentials (admin/password). For more information, see the manufacturer's documentation.

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.



- 3 Select **Network** from the menu, configure the Mercury controller's **IP address**, and click **Accept**.
- 4 Select **Host Comm** from the menu.
- 5 In the *Host Communication* page, configure the following settings, and click **Accept**.

Genetec EP1501 Configuration Manager

Host Communication

Communication Address: Use IPv6 Only

Primary Host Port

Connection Type: Data Security:

Port Number:

Allow All Authorized IP Address Required

Authorized IP Address:

Enable Peer Certificate

Alternate Host Port

Connection Type: Data Security:

* Select **APPLY SETTINGS** to save changes.

- **Communication Address:** Set to 0. Not to be confused with the **Channel** that must be unique when you enroll the Mercury controller on the Synergis™ unit.
 - **Data Security:** Set to *TLS Required*.
IMPORTANT: This setting is mandatory for Synergis™ Softwire 10.2 and later versions to communicate with Security Center. If TLS is not selected, the Mercury EP controller stays offline.
 - **Port Number:** Port number used by the Synergis™ unit to communicate with the Mercury controller (default=3001).
 - **Authorized IP Address Required:** (*Hardening*) Select this option, and set **Authorized IP address** to the IP address of the Synergis™ unit.
- 6 Select **Users** from the menu, and click **New User**.
 Creating a user account on the Mercury controller saves you the trouble of having to physically access the unit and to set the DIP switch S1-1 to **ON** the next time you modify the controller configuration.

Genetec EP1501 Configuration Manager

Users

User Name	Level	Notes
<input type="checkbox"/> super	1	

Password Strength

Low Medium High

Minimum password length is 8 characters and three of the password strength tests must be met. Additionally, strong passwords are checked to make sure that they are not based on the user name.

Session Timer

5 minutes

- 7 (Hardening) On the *Users* page, enter the **User Name** and **Password**, and click **Save**. Set the **Password Strength** to **High**.
- 8 (Hardening) On the *Users* page, disable **Time Server**.
The Time Server is not required. Synergis™ Softwire monitors and automatically sets the time on the EP units.

Time Server

Enable Disable

time.nist.gov

User Specified Time Server:

time.nist.gov

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

- 9 (Hardening) On the *Users* page, disable **SNMP** and **Bonjour**, and click **Submit**.

Disable Web Server Enable Door Forced Open Filter

Enable Diagnostic Logging

Disable SNMP

Disable Bonjour

- 10 Select **Apply Settings** and click **Apply Settings, Reboot**.
- 11 On the Mercury controller board, set the DIP switch S1-1 to **OFF** for normal operation.
This prevents the factory default settings from being used to log on to the controller.
- 12 When prompted to proceed, select **I understand and wish to proceed**, and then click **Yes**.

After you finish

Enroll the Mercury controller on the Synergis™ unit.

Enrolling Mercury controllers on the Synergis™ unit

To have the Synergis™ unit communicate with the Mercury controllers connected to it, you must enroll them using Security Center Config Tool.

Before you begin

[Prepare the Mercury controller for enrollment.](#)

What you should know

Mercury controllers enrolled on a Synergis™ unit are not visible from the Synergis™ Appliance Portal *Hardware* page.

On the Synergis™ unit, each Mercury controller must be assigned a unique channel ID. All Mercury controllers have RS-485 buses to which the interface panels (MR50, MR52, MR16IN, and MR16OUT) are connected. Each interface panel connected to the same RS-485 bus must have a unique physical address.

To enroll a Mercury controller connected to the Synergis™ unit:

- 1 From the Config Tool home page, open the *Access control* task.
- 2 Click **Roles and units**, and then click the Synergis™ unit (🌐).
- 3 Click **Peripherals**, and then click **Add an item** (+).

Manufacturer: Mercury Security

Model: EP1502

IP address: 0 . 0 . 0 . 0 Port: 3001

Channel: 0

Model	Port	Address	IP address

+ X Pencil

Advanced settings

Cancel OK

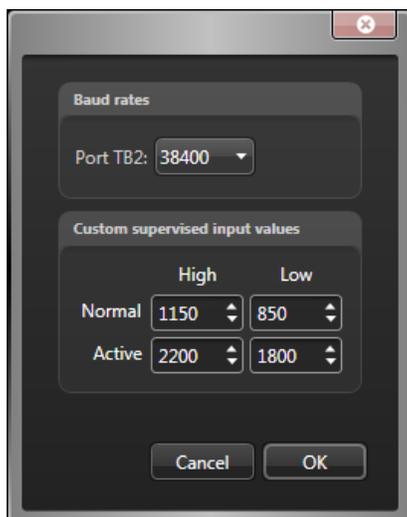
- 4 Enter the following information:
 - **Model:** Model of the controller.

- **IP address:** Static IP address assigned to the controller by your IT department.
 - **Port:** Communication port (default=3001). The port must match the value configured on the Mercury Device Manager web page.
 - **Channel:** Channel ID corresponding to this controller. The channel ID can be any value between 0 and 63, and must be unique within the Synergis™ unit. Once assigned, it must not be changed.
- 5 If the selected controller model supports downstream panels, add them.
- NOTE:** Consider the following:
- For MR51e PoE panels, add them after enrolling the EP controller.
 - Do not to exceed the limit of eight downstream panels per EP1501 controller, as recommended by Mercury.
 - The M5-20In panel occupies two consecutive addresses on the communication bus. To have the 20 inputs of the M5-20In panel, you must add two M5-20In panels in Config Tool to your M5-IC controller. The address of the first panel must match the physical address on the M5-20In board, and the address of the second panel must be set to the address of the first panel plus one.
- Below the *Interfaces* group, click **Add an item** (+).
 - In the dialog box that appears, select the **Model**, the **Port**, the **Address** (0 to 31), and the IP address (MR51e only) of the downstream panel.
All panels attached to the same port must use a different address.
 - Click **OK**.
 - Repeat as necessary.

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.



- 6 (Optional) Click **Advanced settings** to change the advanced settings.
- The available settings depend on the selected controller model. You can typically change the baud rate of the available serial port, and the custom supervised input values.



- Click **OK** at the bottom of the dialog box.
- Click **Apply** (✓).

The Mercury controller with all its attached downstream panels and peripheral devices appear in the **Peripherals** tab.

Name	Type	State	Additional info	Controlling
Mercury EP1502 (10.23.75.11:3015)		Online	Number of credentials synced: 5000	
Input 1	In	Normal	Normally open / Not supervised	
Input 2	In	Normal	Normally open / Not supervised	
Input 3	In	Normal	Normally open / Not supervised	
Input 4	In	Normal	Normally open / Not supervised	
Input 5	In	Normal	Normally open / Not supervised	
Input 6	In	Normal	Normally open / Not supervised	
Input 7	In	Normal	Normally open / Not supervised	
Input 8	In	Normal	Normally open / Not supervised	
Input PowerMonitor	In	Normal	---	
Input Tamper	In	Normal	---	
Input Tamper-Reader-1	In	Normal	---	
Input Tamper-Reader-2	In	Normal	---	
Output 1	Out	Normal	---	
Output 2	Out	Normal	---	
Output 3	Out	Normal	---	
Output 4	Out	Normal	---	
Reader 1	Reader	Active	Type of reader: OSDPv2	
Reader 2	Reader	Active	Type of reader: Standard Wiegand	
MR16In (Port TB3 - 1)		Online		
MR16Out (Port TB3 - 2)		Online		
MR50 (Port TB3 - 31)		Online		
Input 1	In	Normal	Normally open / Not supervised	
Input 2	In	Normal	Normally open / Not supervised	
Input Tamper	In	Normal	---	
Input Tamper-Reader-1	In	Normal	---	
Output 1	Out	Normal	---	
Output 2	Out	Normal	---	
Reader 1	Reader	Active	Type of reader: Standard Wiegand	

NOTE: Adding interface modules to the Synergis™ unit causes the unit to perform a software restart. During this process, the Synergis™ unit and all peripherals attached to it appear offline (in red).

- 9 Select each of the discovered I/O devices and readers, and [configure their properties](#) as necessary. For OSDP (Secure Channel) readers, see [Adding OSDP \(Secure Channel\) readers to an EP controller](#) on page 140.
- 10 Test your wiring and configuration by triggering the inputs and outputs. The triggered I/O changes state in real time on screen.

NOTE: Reader activities are not shown in the **Peripherals** tab.

After you finish

[Add the MR51e panels to the EP controller](#) (if applicable), and then map the physical wiring of the interface modules to the doors and zones in Security Center.

Adding OSDP (Secure Channel) readers to an EP controller

To add an OSDP (Secure Channel) reader to an EP controller, you must first configure the reader on the EP controller using Config Tool, and then pair the reader to the EP controller using Synergis™ Appliance Portal.

Before you begin

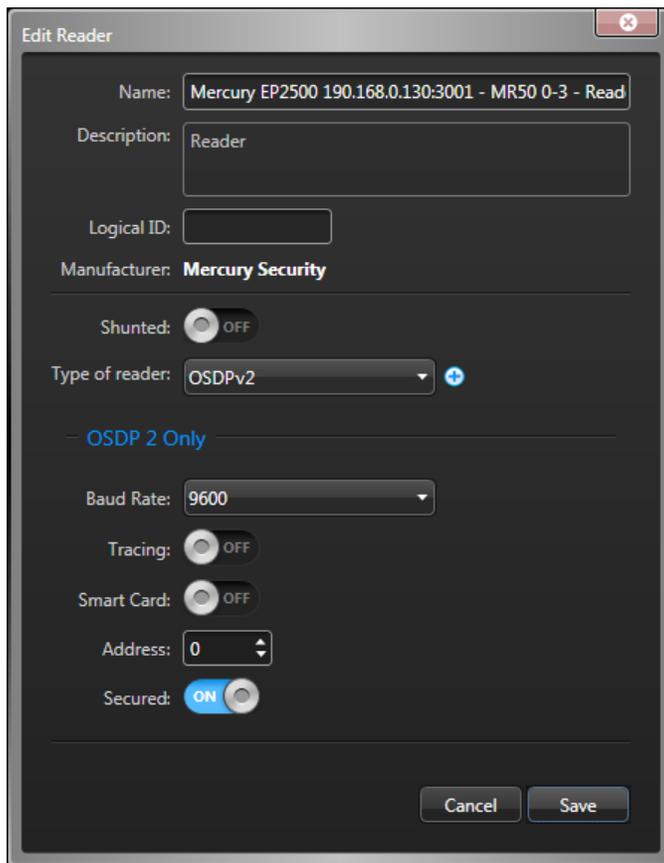
[Enroll your EP controller with its downstream panels on your Synergis™ unit.](#) This feature requires Security Center 5.6 SR2 or later.

What you should know

To add an OSDP (Secure Channel) reader to your EP controller, you must pair the reader (exchange of keys) to the board it is connected to. After the reader is securely paired to a reader port, you cannot pair it in secure mode to a different reader port without resetting the reader to factory default.

To add an OSDP (Secure Channel) reader to your EP controller:

- 1 In Config Tool, open the *Access control* task, and click **Roles and units**.
- 2 Select the Synergis™ unit (🌐) and click **Peripherals**.
- 3 If necessary, expand the EP controller to see the downstream MR panels and peripherals.
- 4 Click the reader (📄) you want to configure and click **Edit** (✎).
- 5 In the *Edit Reader* dialog box, click the **Type of reader** drop-down list, and select **OSDP (Secure Channel)**.



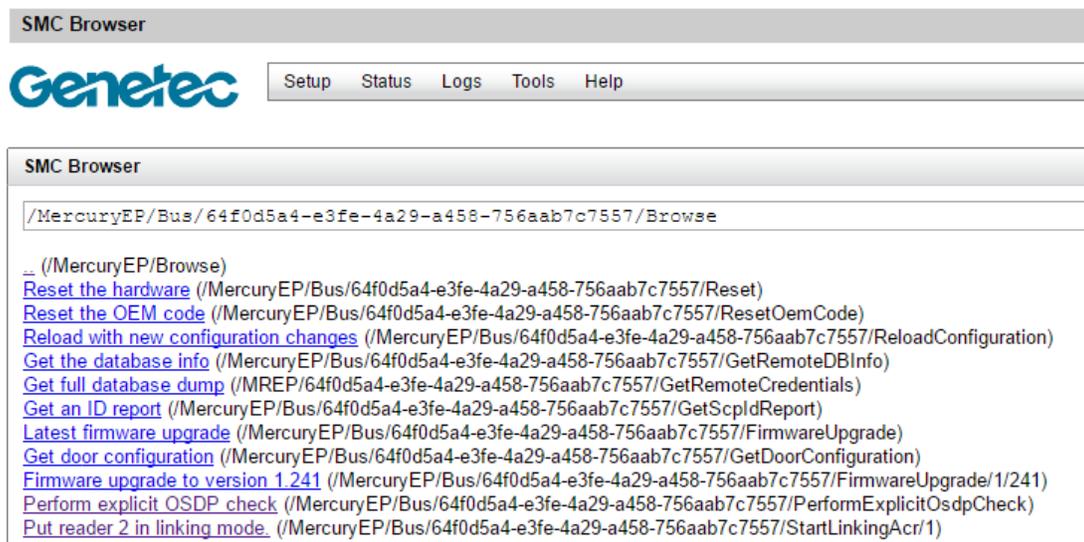
The **Secured** option must be turned on.

- 6 Configure other OSDP (Secure Channel)-specific settings as necessary and click **Save**.

- 7 Connect to the Synergis™ unit through a web browser.

NOTE: You are not using Synergis™ Appliance Portal for this operation.

- a) In the URL field of the browser, type `https://<unit>/smc/index.html`, where `<unit>` is the domain name or the IP address of the Synergis™ unit.
Examples: `https://scl0cbf15003cd8/smc/index.html` or `https://10.160.18.15/smc/index.html`
 - b) In the *Login* page, enter the **User Name** and **Password**, and click **Login**.
Use the same username and password you would use when logging on through Synergis™ Appliance Portal.
- 8 In the *Hardware configuration* page, click **Tools > Advanced**.
- 9 In the *SMC Browser* page, click **Mercury EP device tools**.
- 10 In the refreshed page, click **Bus "n.n.n.n"**, where *n.n.n.n* is the IP address of the EP controller.
- 11 In the refreshed page, click **Put reader x in linking mode**, where *reader x* is the reader you configured as OSDP (Secure Channel) and secure in Config Tool.



After the pairing process is completed, the reader appears online in Config Tool.

Adding MR51e panels to an EP controller

MR51e is a single door PoE panel that must be controlled through an EP controller. For the MR51e panel to communicate with an EP controller, you must set the MR51e panel to use either the Public DHCP (recommended) or the Static IP addressing mode.

Before you begin

Make sure of the following:

- If not already done, load the MR51e panels with the [supported firmware version](#).
- [Enroll the EP controller on your Synergis™ unit](#).
- If the MR51e panels are using the Static IP addressing mode, download the *MSC MR51e Address Configuration Tool* from the Mercury website.

What you should know

For Mercury integration through Synergis™ Softwire, you can use the MR51e panel with only two addressing modes: the Public DHCP, and Static IP.

To add a MR51e module to your EP controller:

- 1 Do one of the following:
 - [Set the MR51e panel to use Public DHCP](#) (recommended).
 - [Set the MR51e panel to use Static IP](#).
- 2 In Config Tool, open the *Access control* task, and click **Roles and units**.
- 3 Select the Synergis™ unit (🌐), and add the MR51e panels.
For more information, see the steps for adding downstream panels in [Enrolling Mercury controllers on the Synergis™ unit](#) on page 137.

Setting MR51e to use Public DHCP addressing mode

If your network supports DHCP, it is recommended to set your MR51e panels to use Public DCHP addressing model.

To set the MR51e panel to use Public DCHP:

- 1 On the MR51e panel, set **S1** (Configuration DIP switches) to '0001'.
Set DIP Switch 4, 3, and 2 to OFF, and DIP Switch 1 to ON.
- 2 Press **S2** (Reset Switch).

Setting MR51e to use Static IP addressing mode

If your network does not support DHCP, set your MR51e panels to use Static IP addressing model.

Before you begin

Download the [MSC MR51e Address Configuration Tool](#) and install it on your computer. Make sure the MR51e panel is connected to the same subnet as your computer.

To set the MR51e panel to use Static IP:

- 1 On the MR51e panel, set **S1** (Configuration DIP switches) to '0011'.

- Set DIP Switch 4 and 3 to OFF, and DIP Switch 2 and 1 to ON.
- Open the [MSC MR51e Address Configuration Tool](#).
 - Press **S2** (Reset Switch).
Once detected, the MAC address of the MR51e panel appears in the **Devices in Programming Mode** list.
 - In the **Devices in Programming Mode** list, select the MR51e panel to be programmed.
The MAC address of the selected MR51e panel appears in the **Selected Device** field.

Devices in Programming Mode:

000FE503BED8

Selected Device

MAC Address : 00-0F-E5-03-BE-D8

Current IP Configuration

Static IP Address : 10.160.56.140 Subnet Mask : 255.255.252.0 Default Gateway : 10.160.56.1

Static IP Address : Subnet Mask : Default Gateway : Assign Static Address

IP Address Assignment History:

	MAC Address	Static IP	Subnet Mask	Default Gateway	Address Assigned
*					<input type="checkbox"/>

- Enter the values for **Static IP Address**, **Subnet Mask**, and **Default Gateway**, and click **Assign Static Address**.
The entered values appear in the **Current IP Configuration** group and in the **IP Address Assignment History** list.
- On the MR51e panel, set **S1** (Configuration DIP switches) to '0010'.
Set DIP Switch 4, 3, and 1 to OFF, and DIP Switch 2 to ON.
- Press **S2** (Reset Switch).

Access control unit - Synergis™ - Peripherals tab

This section lists the settings found in the Synergis™ access control unit **Peripherals** tab, in the *Access control* task. This tab displays in a hierarchical view, all the interface modules attached to the unit, along with any downstream panels attached to them.

From the **Peripherals** tab, you can add and delete interface modules, and change the name and settings of the peripherals (readers and I/O devices) attached to the unit.

The informations displayed on this page are:

- **Name:** Name of the interface module or peripheral. The peripherals are displayed in a hierarchical view by default.

Click **Viewing mode** () to select the *Flat view* if it is your preference.

- **Type:** Peripheral type: *In* (Input), *Out* (Output), *Reader*. Blank if it is not a peripheral.

(Output relays only) Click **Trigger output** () at the bottom of the list to send an output behavior (*Active*, *Normal*, or *Pulse*) to the selected device.

- **State:** Live peripheral state: *Active*, *Normal*, *Shunted* (inputs and readers only), *Trouble* (inputs only), or *Unknown*.

Use this column to test the connected interface modules and validate the wiring configuration of the I/O devices.

- **Additional info:** Settings specific to the type of peripheral.

Double-click a peripheral, or click **Edit** () at the bottom of the list to edit the settings of the selected peripheral.

- **Controlling:** Entity (door, elevator, zone) controlled by this peripheral.

Click **Jump to** () at the bottom of the list to view the configuration tabs of the entity controlled by the selected peripheral.

- **Logical ID:** (Hidden by default) Logical ID assigned to this peripheral for ease of reference in macros and SDK programs.
- **Physical name:** (Hidden by default) Static name assigned to this peripheral by the system.

TIP: Information on this page is also available to Security Desk users through the *System status* task, when monitoring peripherals.

Interface modules you can add and delete

You can only add and delete Mercury controllers (EP and M5-IC) attached to your Synergis™ unit from the **Peripherals** tab. For all other types of interface modules, you must add them either through the **Hardware** tab, or through the *Hardware* page of the Synergis™ Appliance Portal.

Editable reader settings

The editable reader settings are:

- **Name:** Reader name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the reads.

This action can also be issued from Security Desk.

- **Type of reader:** Select the type corresponding to your reader. The list of available reader types depends on the type of interface module you have. Selecting the *Custom* reader type allows you to configure all the reader options manually.

Editable input settings

The editable input settings are:

- **Name:** Input device name.
- **Description:** (Read only) Input description.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless how you trigger it.
- **Debounce:** The amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. This option filters out signals that are unstable.
- **Contact type:** Set the normal state of the input contact and its supervision mode.
 - **Not supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit does not report that the input is in the trouble state.
 - **Not supervised / Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
 - **4-state supervised / Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
 - **4-state supervised / Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.
 - **Custom:** Allows you to set your custom range of values for *Active* and *Normal* input states. The actual values are set in the Mercury controller Advanced settings.

Editable output settings

The editable reader settings are:

- **Name:** Output device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.

OSDP Readers

This section includes the following topics:

- ["Supported OSDP readers in Synergis Softwire 10.6"](#) on page 147
- ["Prestaging OSDP readers connected to the Synergis unit"](#) on page 148
- ["Enrolling OSDP readers connected to the Synergis unit"](#) on page 150
- ["Enabling secure mode on OSDP readers"](#) on page 151

Supported OSDP readers in Synergis™ Softwire 10.6

With Secure Open Supervised Device Protocol (OSDP), you can move away from Wiegand readers without making a large infrastructure investment, since only the readers need to be replaced.

The following OSDP readers were certified and are supported by Synergis™ Softwire 10.6. Other OSDP readers might also work correctly.

Manufacturer	Model	Certified firmware
Allegion	aptiQ MT14-485 X14_14 reader	FW1212
HID	Multiclass SE RPK40EKTB readers	00312-F, 00316-F
STid	ARCR31BPH52B1	ARC-R3x- XSZ235A03_04InitMem.hex

Supported Synergis™ appliances

OSDP readers connect directly to the RS-485 ports on a Synergis™ Cloud Link or a Synergis™ Master Controller equipped with an RS-485 board.

Streamvault™ appliances are not equipped with RS-485 ports, and are therefore not compatible with direct OSDP readers.

Prestaging OSDP readers connected to the Synergis™ unit

Before you can enroll OSDP readers on the Synergis™ unit, they must first be prestaged through programming mode.

Before you begin

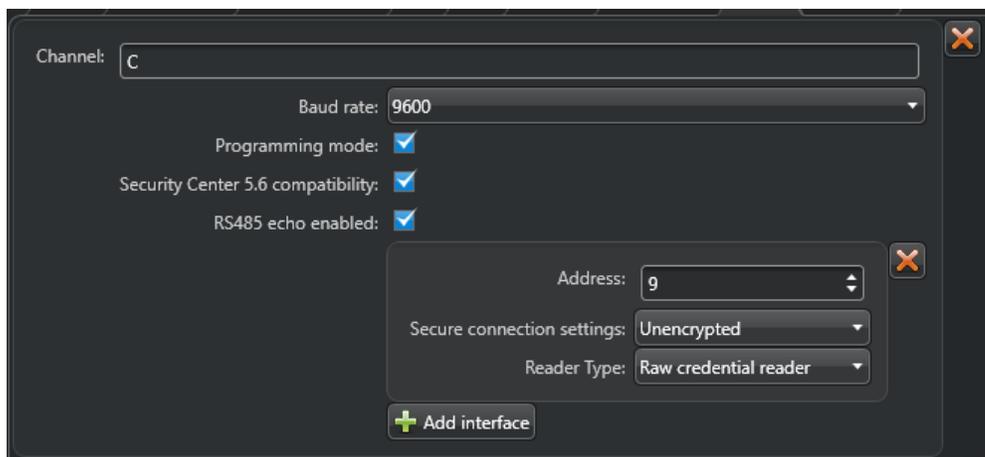
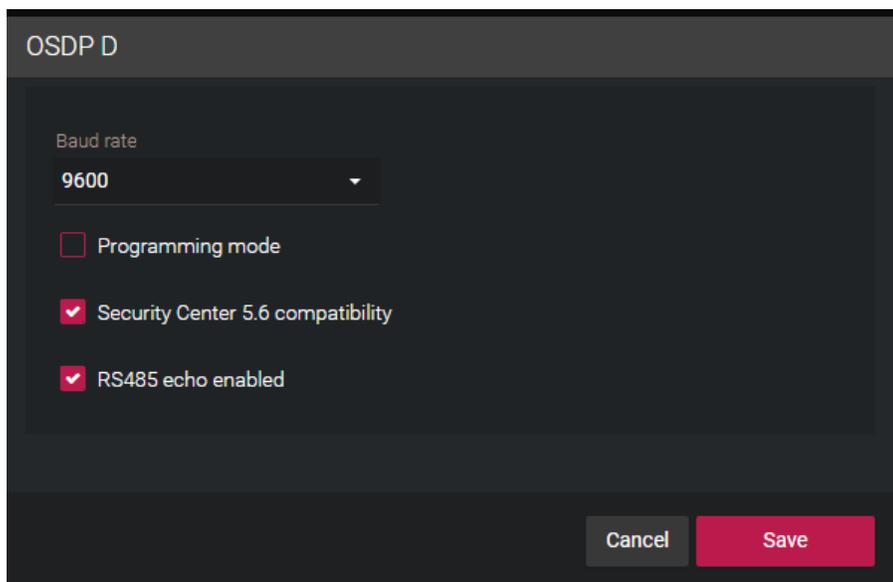
- Make sure that your readers are wired or rewired for the native OSDP solution.
- Make sure that all readers are powered down.

What you should know

It is not recommended to connect more than eight OSDP (regular or secure channel) readers to the same RS-485 channel, as it increases the controller's response time.

To prestage the OSDP readers connected to the Synergis™ unit:

- 1 From the Config Tool home page, open the *Hardware* task.
- 2 Select **OSDP**, and then click **Add channel** and set the channel to A, B, C, or D, depending on context.
- 3 Click the **Enable programming mode** checkbox.



- 4 Click **Add interface**, then set the desired RS-485 address.

- 5 Power up one reader from the RS-485 bus. It will receive the address and appear online.
- 6 Power down the reader.
- 7 Enter a new RS-485 address and apply the change.
- 8 Power on the next reader; it will receive the address
- 9 Repeat steps 4 to 8 until all readers have been prestaged.
- 10 Disable programming mode

After you finish

[Enroll the readers.](#)

Enrolling OSDP readers connected to the Synergis™ unit

For the Synergis™ unit to communicate with the OSDP readers connected to it, you must enroll them with Synergis™ Appliance Portal.

Before you begin

- [Prestage the OSDP readers.](#)
- Make sure your reader firmware is up to date and [supported by Synergis™ Software.](#)

What you should know

After prestaging the OSDP readers, you can enroll them on the Synergis™ unit.

To enroll the OSDP readers connected to the unit:

- 1 In Config Tool, click **Access control** > **Roles and units**. Then, select your Synergis™ Cloud Link or Synergis™ Master Controller and open its **OSDP** tab.
- 2 Select one of the prestaged OSDP channels, then click **Add interface** and add the address corresponding to the first reader.
- 3 Repeat for the remaining readers.

After you finish

[Enable security on the enrolled readers.](#)

Enabling secure mode on OSDP readers

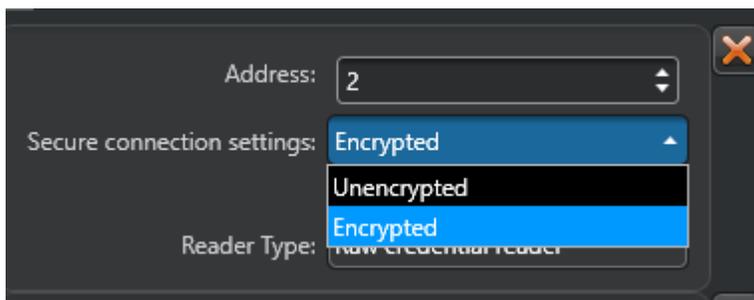
By default, OSDP readers are enrolled in an unencrypted state. Enabling encryption increases access-point security.

Before you begin

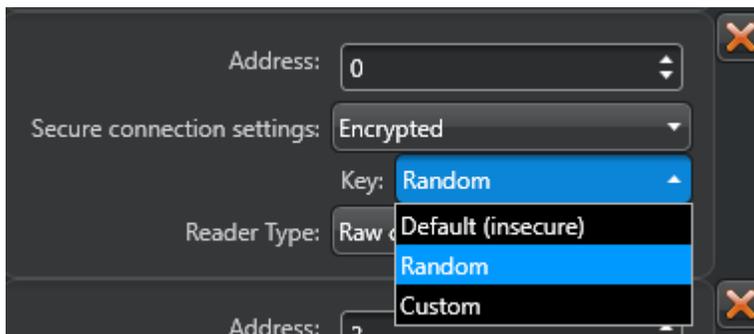
[Enroll the OSDP readers.](#)

To enable encryption on your OSDP readers:

- 1 In Config Tool, click **Access control** > **Roles and units**. Then, select your Synergis™ unit and open its **OSDP** tab and select one of the OSDP readers you [enrolled](#).
- 2 Set the **Secure connection settings** drop-down to *Encrypted*.



- 3 Set the **Key** drop-down to **Random**. Alternately, if you prefer to specify your own 128-bit (32 hexadecimal characters) key, then select **Custom**.



- 4 Repeat steps 1 to 3 for the remaining readers.
At this point, the readers will go offline, as you have told Synergis™ Software to use certain keys, but the readers have not yet been configured with those keys.
- 5 Connect to the Synergis™ unit through a web browser.

NOTE: You will not be using Synergis™ Appliance Portal for this operation.

Navigate to `https://<unit>/smc/index.html#page=/OSDP/Browse`, where <unit> is the domain name or the IP address of the Synergis™ unit.

Examples:

`https://scl0cbf15003cd8/smc/index.html#page=/OSDP/Browse`

or

`https://10.160.18.15/smc/index.html#page=/OSDP/Browse`

- 6 Click on the port you specified for the first reader in Config Tool, then click on a **Linking mode** on the next page to send the key to the reader.

The image shows two screenshots of the Genetec SMC Browser interface. The top screenshot shows the main menu with 'Setup', 'Status', and 'Logs' buttons. Below the Genetec logo, the address bar contains '/OSDP/Browse'. A link for 'Port "D" (/OSDP/Bus/D/Browse)' is visible. The bottom screenshot shows the same interface with an additional 'Tools' button. The address bar now contains '/OSDP/Bus/D/Browse'. Below the address bar, a list of links is displayed: '.. (/OSDP/Browse)', 'Linking mode: 2 (/OSDP/Bus/D/StartLinkingReader/2)', 'Linking mode: 0 (/OSDP/Bus/D/StartLinkingReader/0)', 'Linking mode: 3 (/OSDP/Bus/D/StartLinkingReader/3)', 'Linking mode: 4 (/OSDP/Bus/D/StartLinkingReader/4)', 'Linking mode: 5 (/OSDP/Bus/D/StartLinkingReader/5)', 'Linking mode: 6 (/OSDP/Bus/D/StartLinkingReader/6)', 'Linking mode: 7 (/OSDP/Bus/D/StartLinkingReader/7)', and 'Linking mode: 8 (/OSDP/Bus/D/StartLinkingReader/8)'.

- 7 Repeat steps 5 and 6 for the remaining readers.

This will exchange the keys, and the readers will come back online in Config Tool. They will then be secure; no reader that rejects the key will come back online if encryption is enabled on the Synergis™ Softwire side.

Salto Sallis Wireless Locks

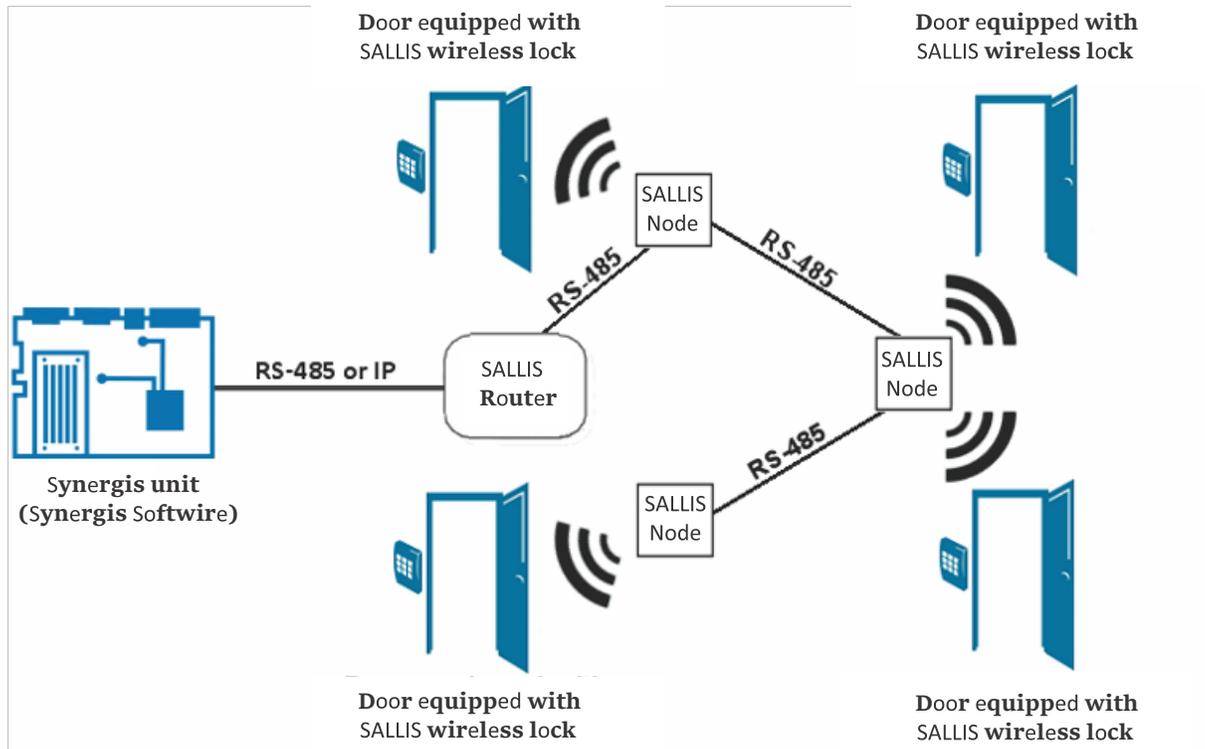
This section includes the following topics:

- ["SALTO SALLIS integration overview"](#) on page 154
- ["Supported SALTO SALLIS hardware"](#) on page 155
- ["Supported SALTO SALLIS features"](#) on page 156
- ["Supported Synergis appliance features for SALTO SALLIS integration"](#) on page 158
- ["Supported Security Center features for SALTO SALLIS integration"](#) on page 159
- ["Enrolling SALLIS locks"](#) on page 161
- ["Enabling encryption on an existing SALLIS router"](#) on page 166
- ["Disabling encryption on a SALLIS router"](#) on page 167

SALTO SALLIS integration overview

SALTO SALLIS wireless locks communicate with SALLIS nodes connected through an RS-485 bus to the SALLIS router. The SALLIS router then, communicates with the Synergis™ unit, either through an RS-485 channel or the IP channel.

The following diagram shows how the Synergis™ unit communicates with the SALTO SALLIS wireless locks through the SALLIS (Salto Lock Link System) system.



NOTE: The SALTO SALLIS wireless lock is a non-intelligent lock. It relies on the Synergis™ unit to make all access control decisions.

Supported SALTO SALLIS hardware

For SALTO SALLIS integration, the Synergis™ unit connects to the SALLIS locks through a wireless router that is connected to its IP channel or one of its RS-485 channels. Each SALLIS lock is viewed as an interface module.

Synergis™ Softwire supports the following SALTO SALLIS devices:

Model	Description	Supported firmware
SALLIS 00-59 RS485 router	SALLIS RS-485 router connecting the Synergis™ unit to the wireless (RF) communication nodes.	01.11
SALLIS 00-72 PoE router	SALLIS PoE router connecting the Synergis™ unit to the wireless (RF) communication nodes.	01.06
SALLIS 00-71 mini-node	SALLIS RF communication mini-node attached to the SALLIS PoE router board. Only one mini-node can be added per router.	02.00
SALLIS 00-60 node	SALLIS RF communication node between the SALLIS router and the SALLIS lock system. It works with both the RS-485 and the PoE routers.	02.00
SALLIS 00-38 XS4 lock	SALLIS lock system used to control the physical access to a premise.	02.00

IMPORTANT: After changing the battery on the lock, always re-initialize it and restart the router.

Supported SALTO SALLIS features

Interface modules come in all shapes and sizes and offer a wide range of features. Synergis™ Softwire supports most of the common features found on the market.

Synergis™ Softwire 10.6 supports the following SALTO SALLIS features.

Features	Supported
General characteristics	
Category of interface module	Electronic lock
Communication protocol	(IP or RS-485) ¹
Encrypted communication	IP and RS-485
Online operation (connected to the Synergis™ unit)	
Supervised mode	No
Dependent mode	Yes
Offline operation (no connection to the Synergis™ unit)	
Standalone mode	No
Degraded mode	No
Wireless operation	
Contact the Synergis™ unit on event	On read
Scheduled radio contact	Every 8 sec.
Battery checks	Every 10 min.
Power fail lock settings (Fail Safe/Fail Secure)	N/A
Scalability	
Maximum number of offline events	N/A
Maximum number of credentials (for autonomous decision making)	N/A
Maximum credential length (in bits)	56 ²
Maximum number of interface modules per RS-485 channel	16 ³
Recommended maximum number of interface modules per Synergis™ unit	64 ⁴

¹ Protocol between the Synergis™ unit and the SALLIS router.

² The maximum credential length must be set from the SALLIS application, under Installation Data, IDCode Size.

³ One RS-485 router per channel, and up to 16 locks per router.

⁴ Either four RS-485 routers with 16 locks each, or one PoE router with 64 locks.

Supported Synergis™ appliance features for SALTO SALLIS integration

Not all Synergis™ appliance features are supported with the integration of SALTO SALLIS wireless locks. The SALTO SALLIS wireless lock integration supports the following [Synergis™ Appliance Portal](#) and [Synergis™ Softwire](#) features. For a description of these features, see the [Synergis™ Appliance Configuration Guide](#).

Synergis™ Appliance Portal and firmware features	Supported
Hardware configuration (pre-staging capability)	
Manual enrollment (<i>Add hardware</i> dialog box)	Yes
Automatic enrollment (Scan button)	Yes
Property configuration	Yes
Configuration cloning (Clone button)	Yes
I/O diagnostics (live monitoring of inputs, relays, and readers)	Partial ¹
Interface module firmware display	Router only
Interface module firmware upgrade (apply recommended firmware)	No
Access control behavior (Synergis™ unit-wide settings) ²	
Beep on door held open	No
Beep on door forced open	No
Beep on access denied	No
Interlock setting (<i>Single door unlock</i> or <i>Single door open</i>)	No
Do not generate 'DHO' events when door is unrestricted	Yes
Reader setting (<i>Card or PIN</i> or <i>Card only</i>)	No
Maximum PIN length in digits	N/A
Degraded mode settings	N/A
Lock relay (<i>After door opens</i> or <i>When door closes</i>)	No

¹ Inputs without a sensor attached are not monitored on the I/O diagnostic page.

² The door behavior settings are overwritten by the individual door settings configured in Security Center.

Supported Security Center features for SALTO SALLIS integration

Not all Security Center access control features are supported with the integration of SALTO SALLIS wireless locks.

The SALTO SALLIS wireless lock integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	Yes	
	Standard grant time	No ¹	
	Extended grant time	No	
	Entry time (Standard/Extended) ²	No	
	Door relock - options	No	
	When door is unlocked by schedule - options	See note ³	
	Door held - options	Limited ⁴	
	Door forced open - options	Limited ⁴	
	Unlock schedules	Yes	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	N/A	
	Time to ignore REX after granting access (in seconds)	Yes	
	Ignore REX events while door is open (On/Off)	Yes	
	Time to ignore REX after door closes (in seconds)	Yes	
Visitor escort and two-person rule			
Maximum delay between card presentation (in sec.)	Yes		
Enforce two-person rule (On/Off) on Door side	Yes		
Manual actions on doors in Security Desk ⁵	Manually unlock doors	Yes	
	Reader shunting (activate/deactivate reader)	Yes	
	Override unlock schedules	Yes	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	N/A
	Battery fail (<i>Low battery</i>)	Yes
	Door open/closed	No
	Door locked/unlocked	No
	Door forced open	Yes
	Door held open for too long	Yes
	Door secured	N/A
	Deadbolt (<i>Secured, Released</i>)	N/A
	Key override	Yes
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	Yes
	Visitor escort rule (On/Off)	Yes
	Interlock	No ⁶
	Antipassback	No
	First-person-in rule	
	Enforce on door unlock schedule	Yes
	Enforce on access rules	Yes
Elevator control	Elevators	N/A
Zone management	I/O zone	No
	Hardware zone	No ⁷

¹ Must be configured in the SALLIS application. The default value is 6 sec.

² Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

³ All events are ignored when the door is unlocked.

⁴ The **Reader buzzer behavior** options are not supported.

⁵ The Synergis™ unit must be connected to the Access Manager.

⁶ Because there is no door sensor, there is no *Door opened* event to guide the interlock.

⁷ It is possible to create a hardware zone entity in Config Tool using inputs from SALLIS, but there would be a significant trigger delay.

Enrolling SALLIS locks

For the Synergis™ unit to communicate with the SALLIS locks, you must enroll them with Synergis™ Appliance Portal.

Before you begin

Set up your SALTO SALLIS infrastructure (routers, nodes, and wireless locks) according to the instructions found in the *SALLIS Installation & Maintenance Guide*. You must first define the nodes and the doors using the SALLIS application, then update the routers and initialize the locks using the PPD (Portable Programmer Device). As you do this, write down the following information:

- **IP router:** IP address and port number.
- **RS-485 router:** Synergis™ unit channel the router is connected to (A, B, C, or D).
- **Lock:** Router, lock ID, and the door where it is installed.

Use descriptive door names, for example “4th floor storage room”. If you have already created the door entities in Security Center, use the same names for ease of reference.

What you should know

The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

To enroll a SALTO SALLIS wireless lock:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration > Hardware**
- 3 At the top of the *Hardware* column, click **Add (+)**.
- 4 In the *Add hardware* dialog box, select **Salto** as the **Hardware type**.
- 5 Identify the channel where the SALLIS router is connected, and do one of the following:
 - Select the IP channel, and enter the IP address and port number used by the router.

Add hardware

Hardware type
Salto

Channel
NEW (IP)

NEW (IP)
Example: 192.168.0.1 or 192.168.0.1:80 to specify a port.

Interface module type
Salto Sallis

Physical address
1

Enable encryption

Interface module type Physical address

Add

Scan Cancel Save

- Select an RS-485 channel (A, B, C, or D). All interface modules connected to the same RS-485 channel must be from the same manufacturer.

Add hardware

Hardware type
Salto

Channel
B

Interface module type
Salto Sallis

Physical address
1

Enable encryption

Interface module type Physical address

Add

Scan Cancel Save

- 6 (Hardening) If you want encryption, select **Enable encryption** and enter the **AES site key**.

NOTE: You cannot change the encryption settings through the *Add hardware* dialog box on an existing channel. To enable encryption after the channel has been created, you will have to [change the channel configuration on Synergis™ Appliance Portal](#).

The screenshot shows the 'Add hardware' dialog box with the following configuration:

- Hardware type: Salto
- Channel: B
- Interface module type: Salto Sallis
- Physical address: 1
- Enable encryption:
- AES site key: [Redacted]
- Buttons: Add, Scan, Save

- 7 In the same dialog box, add all interface modules connected to the same channel. You can enroll the interface modules automatically or manually.

TIP: If you know your lock IDs (physical addresses) and you only have a few to enroll, it would be faster to enroll them manually.

Do one of the following:

- To enroll automatically, click **Scan**

The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

If the controller does not find all connected interface modules, make sure they all have a different physical address.

- To enroll manually, enter the lock ID as the Physical address, and click **Add (+)**.

NOTE: Valid lock IDs are 1-16 for RS-485 routers, and 1-64 for PoE routers.

Repeat as necessary to configure all wireless locks connected to the same channel.

- 8 Click **Save**.

The hardware type, channel, and interface module you just added appear in the *Hardware configuration* page.

After you finish

- Test your interface module connection and configuration from the I/O diagnostics page. For information about testing interface modules, see the *Synergis™ Appliance Configuration Guide*.
- Associate your doors to the SALLIS locks in Security Center.

Enabling encryption on an existing SALLIS router

Encryption is a channel property in Synergis™ Appliance Portal. You can enable the encryption or change the encryption password on a SALLIS router by changing the channel configuration on Synergis™ Appliance Portal.

What you should know

You cannot change the channel settings while adding a lock to an existing channel. After the channel is created, all changes to the channel properties must be made from the channel property page. Once encryption is enabled, you cannot disable it simply by disabling it in Synergis™ Appliance Portal. You'll also need to [disable the encryption by connecting directly to the router](#).

To enable encryption on an existing SALLIS router:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration** > **Hardware** and select the SALTO channel
- 3 Select the **Enable encryption** option, and enter the **AES site key**.
- 4 Click **Save**.

Disabling encryption on a SALLIS router

To disable encryption on a SALLIS router, you need to disable it in both Synergis™ Appliance Portal and on the router itself.

To disable encryption on a SALLIS router:

- 1 Log on to the Synergis™ unit.
- 2 At the top of the *Hardware* column, click **Add** (+).
- 3 Select the SALTO channel, and then clear the **Enable encryption** option.
- 4 Click **Save**.
In the device tree, all SALLIS locks under the selected channel appear in red (inactive).
- 5 For a RS-485 router, do the following:
 - 1 Using the SALLIS application, download the router configuration to the PPD.
 - 2 On the PPD, select **Update router**.
 - 3 Connect the PPD to the router.

- 6 For a PoE router, do the following:

NOTE: If you have many routers to update, update them one at a time.

- 1 Open the PoE router cover, and click and hold the CLR button for 5 seconds.

The LED on the PoE router board turns orange.

- 2 Using a web browser, connect to the web portal of the router.

Type `http://192.168.0.234` in the browser URL field.

NOTE: Your workstation must be on the same subnet as the router for you to connect to its web portal.

- 3 In the browser page, under **Router encryption > Return to Plain mode?**, select **Yes**.
- 4 Click **Send**.

The message **Configuration successfully sent** appears in the browser.

In the device tree, all SALLIS locks under the selected channel appear in black (active).

SimonsVoss SmartIntego Locks

This section includes the following topics:

- ["Supported SimonsVoss locks"](#) on page 169
- ["Supported SimonsVoss lock features"](#) on page 170
- ["Supported Synergis appliance features for SimonsVoss lock integration"](#) on page 171
- ["Supported Security Center features for SimonsVoss lock integration"](#) on page 172
- ["Preparing to enroll SimonsVoss SmartIntego locks"](#) on page 174
- ["Enrolling SimonsVoss SmartIntego locks on the Synergis unit"](#) on page 175

Supported SimonsVoss locks

SimonsVoss SmartIntego lock integration requires a Mercury EP (or Honeywell) controller. For this integration, the EP controllers are viewed as interface modules, and the SmartIntego locks are viewed as non-intelligent devices. All SmartIntego locks are wireless.

Only the Mercury EP (or Honeywell) controllers communicate directly with the Synergis™ unit.

NOTE: SimonsVoss SmartIntego lock integration requires Security Center 5.6 (or more recent versions) and Synergis™ Softwire 10.4 (or more recent versions).

Synergis™ Softwire supports all SmartIntego models that work with Mercury IP controllers.

Model	Description
IP controllers	<p>A Mercury EP (or Honeywell) controller must act as an interface module between the Synergis™ unit and the SmartIntego locks.</p> <p>The supported controller models are:</p> <ul style="list-style-type: none"> • Mercury EP1501 controller with expansion board, supporting up to 16 SmartIntego locks • Mercury EP1502 or EP2500 controller, supporting up to 64 SmartIntego locks • Honeywell PW6K1IC controller supporting up to 64 SmartIntego locks <p>See also Supported Mercury firmware versions on page 126.</p>
Gateway node	Handles the communication between the Mercury IP controller and SmartIntego locks (Up to 16 locking devices per node through a 868 MHz wireless connection, with a range up to 30 meters.).
Programming dongle	Required to pair the locks to the Gateway node.
Smart Handle	Door handle/reader combo. Includes a manual REX out which cannot be monitored. May come with or without inputs.
Digital Locking Cylinder	Different wireless models; some of them have two readers, but only one reader is detected by the Mercury IP controller. May come with or without inputs.
Padlock	Padlock with no keyhole, only a card reader.

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages. If using Internet Explorer, the video might not display. To fix this, open the **Compatibility View Settings** and clear **Display intranet sites in Compatibility View**.



Limitations

- Manual unlock and relock commands can take more time than expected to be executed. This is because these commands rely on a wireless communication that may take a few seconds to respond.
- Only MIFARE DESFire®, and MIFARE Plus card formats are supported.

Supported SimonsVoss lock features

SimonsVoss SmartIntego lock integration requires a Mercury EP (or Honeywell) controller. If the SmartIntego locks are disconnected from their controller, the locks cannot grant access or store offline events.

Synergis™ Softwire 10.6 supports the following SimonsVoss lock features.

Features	Supported
Category of interface module	Electronic lock
Communication protocol ¹	IP, radio
Encrypted communication	Yes ²
Online operation (connected to the Synergis™ unit)	N/A
Offline operation (no connection to the Synergis™ unit)	N/A
Wireless operation	Yes ³
Reader communication protocols	N/A
Maximum credential length (in bits)	52 ⁴
Recommended maximum number of interface modules per Synergis™ unit	N/A ⁵

¹ The Gateway node communicates with the Synergis™ unit over IP. The Gateway node communicates with the wireless locks over radio.

² All SmartIntego wireless locks communicate over a 868 MHz channel using AES-128 bit encryption.

³ Requires the Gateway node (communication module).

⁴ Up to 8 different credential lengths are supported in *standalone mode*. More can be supported in *dependent mode*.

⁵ In the SimonsVoss lock integration, it is the Mercury EP controller that is viewed as the *interface module*, not the SimonsVoss lock. For the recommended number of Mercury EP controllers per Synergis™ unit, see [Supported Mercury controller features](#) on page 127.

Supported Synergis™ appliance features for SimonsVoss lock integration

Not all Synergis™ appliance features are supported with the integration of SimonsVoss locks.

SimonsVoss locks are connected to the Synergis™ appliance through a Mercury EP controller. For Synergis™ appliance features supported by the SimonsVoss lock integration, see [Supported Synergis™ appliance features for Mercury controller integration](#) on page 129.

Supported Security Center features for SimonsVoss lock integration

Not all Security Center access control features are supported with the integration of SimonsVoss locks. The SimonsVoss lock integration supports the following Security Center access control features. For more information on these features, see the *Security Center Administrator Guide*.

Feature group	Security Center feature	Supported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	No	
	Standard grant time	Yes ¹	
	Extended grant time	N/A	
	Entry time (Standard/Extended) ²	N/A	
	Door relock - options	No	
	When door is unlocked by schedule - options	Yes	
	Door held - options	No	
	Door forced open - options	N/A	
	Unlock schedules	Yes	
	Request to exit (REX) options		
	Unlock on REX (On/Off)	N/A	
	Time to ignore REX after granting access (in seconds)	N/A	
	Ignore REX events while door is open (On/Off)	N/A	
	Time to ignore REX after door closes (in seconds)	N/A	
	Visitor escort and two-person rule		
Maximum delay between card presentation (in sec.)	No		
Enforce two-person rule (On/Off) on Door side	No		
Manual actions on doors in Security Desk ³	Manually unlock doors	Yes	
	Reader shunting (activate/deactivate reader)	No	
	Override unlock schedules	Yes	

Feature group	Security Center feature	Supported
Live event monitoring in Security Desk	Module running state (<i>Online, Offline</i>)	Yes
	AC fail	No
	Battery fail (<i>Low battery</i>)	Yes
	Door open/closed	No
	Door locked/unlocked	No
	Door forced open	No
	Door held open for too long	No
	Door secured	N/A
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	N/A
	Visitor escort rule (On/Off)	N/A
	Interlock	N/A
	Antipassback	N/A
	First-person-in rule	N/A
Elevator control	Elevators	N/A
Zone management	I/O zone	N/A
	Hardware zone	N/A

¹ The maximum supported value is 255 seconds. Values between 26 and 59 seconds are rounded to 1 minute. Values above 60 seconds are rounded to the next minute. For example, 121 seconds is rounded to 3 minutes.

² Security Center requires an entry sensor in order to accurately detect entry into an area. In the absence of the entry sensor, Security Center uses the door sensor, and the *Entry detected* event is generated when the door sensor is triggered. In the absence of both sensors, Security Center generates the *Entry assumed* event when access is granted.

³ The Synergis™ unit must be connected to the Access Manager.

Preparing to enroll SimonsVoss SmartIntego locks

Before you can enroll the SmartIntego locks on the Synergis™ unit, you must pair the Gateway node to your SmartIntego locks.

What you should know

The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

To prepare to enroll the SmartIntego locks:

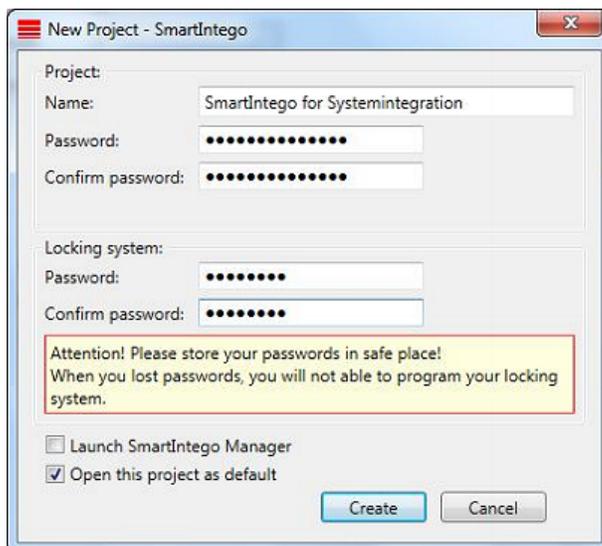
- 1 Follow the documentation that came with your SmartIntego devices and pair the Gateway node to your SmartIntego locks.
- 2 Write down the following information:
 - The IP address of the Gateway node.
 - The device IDs taken from the *SmartIntego Manager* window.



The Gateway node ID is the second hexadecimal number following GN_ER.

The lock ID is the first hexadecimal number following LN.

- 3 (*Hardening*) Follow the documentation that came with your SmartIntego devices and configure the communication encryption key for your locks. SmartIntego software does not allow a lock to be paired to the hub without a password. Use a strong password for the locking system.



Enrolling SimonsVoss SmartIntego locks on the Synergis™ unit

Because the Synergis™ unit does not communicate with the SimonsVoss SmartIntego devices, you must enroll these devices through a Mercury EP (or Honeywell) controller, using the Config Tool.

Before you begin

Pair your the Gateway node to your SmartIntego locks.

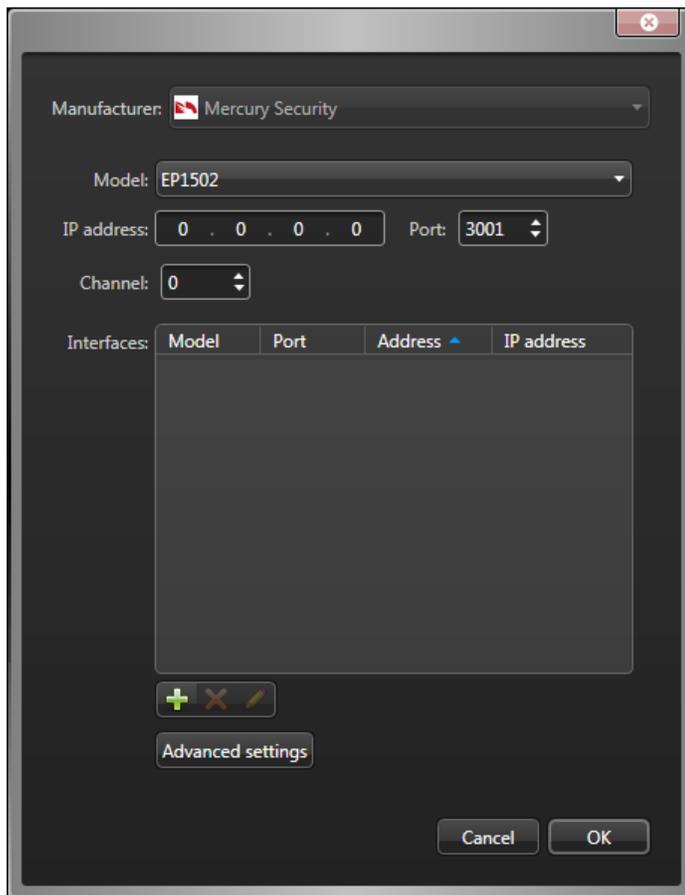
What you should know

Mercury controllers enrolled on a Synergis™ unit are not visible from the Synergis™ Appliance Portal *Hardware* page.

On the Synergis™ unit, each EP controller must be assigned a unique channel ID. The EP controller communicates with the SmartIntego Gateway nodes through IP. IP addresses cannot overlap within the same network.

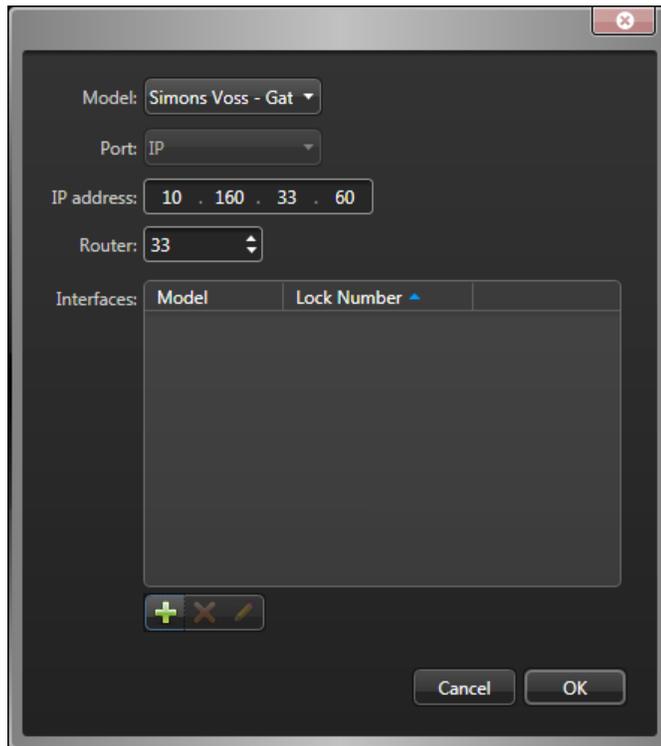
To enroll SimonsVoss SmartIntego locks to the Synergis™ unit:

- 1 From the Config Tool home page, open the *Access control* task.
- 2 Click **Roles and units**, and then click the Synergis™ unit (🌐).
- 3 Click **Peripherals**, and then click **Add an item** (+).

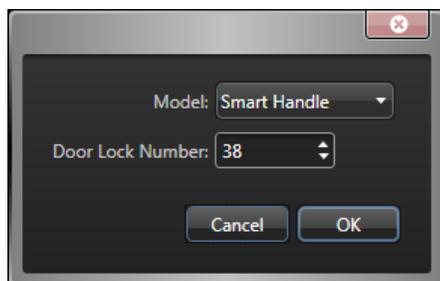


- 4 Enter the following information:

- **Model:** Model of the controller.
 - **IP address:** Static IP address assigned to the controller by your IT department.
 - **Port:** Communication port (default=3001). The port must match the value configured on the Mercury Device Manager web page.
 - **Channel:** Channel ID corresponding to this controller. The channel ID can be any value between 0 and 63, and must be unique within the Synergis™ unit. Once assigned, it must not be changed.
- 5 Add the SmartIntego Gateway node that you want the EP controller to talk to.
- a) At the bottom of the *Interfaces* group, click **Add an item** (+).
 - b) In the dialog box that appears, click **Model** and select **SimonsVoss Gateway node**.
 - c) In **IP address**, enter the IP address of the Gateway node.
 - d) In **Router**, enter the decimal value of the Gateway node ID.
For example, if the Gateway node ID is 0x0021, enter 33 (= 2 x 16 + 1).



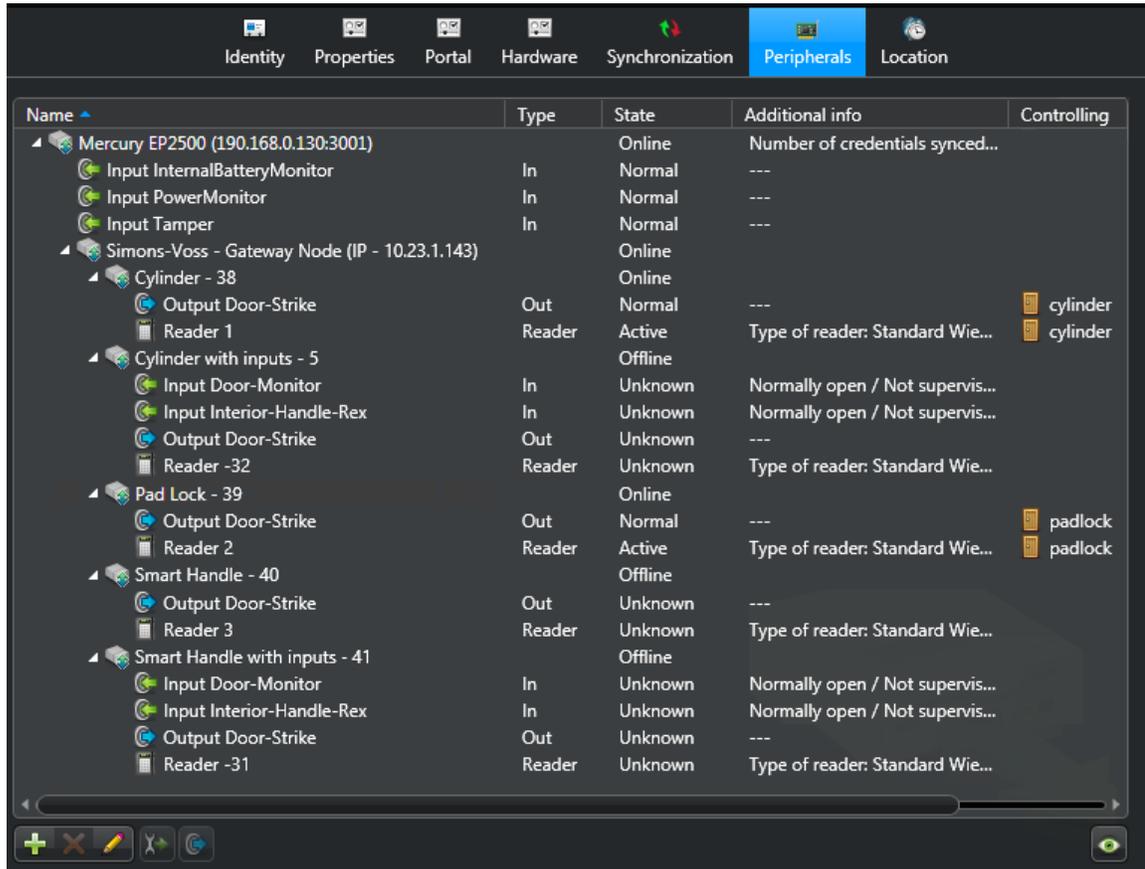
- 6 Add the locks paired to the Gateway node.
- a) In the dialog box that appears, click **Model** and select the lock model (Smart Handle, Padlock, Cylinder).
 - b) In **Door Lock Number**, enter the decimal value of the lock ID.
For example, if the lock ID is 0x0026, enter 38 (= 2 x 16 + 6).



- c) Click **OK**.
- d) Repeat if you have more locks to add.

- e) Click **OK**.
- 7 Click **Apply** (✓).

The Mercury controller with all its attached downstream panels and peripheral devices appear in the **Peripherals** tab.



NOTE: Adding interface modules to the Synergis™ unit causes the unit to perform a software restart. During this process, the Synergis™ unit and all peripherals attached to it appear offline (in red).

- 8 Test your configuration by triggering the outputs.
The triggered output changes state in real time on screen.

NOTE: Reader activities are not shown in the **Peripherals** tab.

STid Readers

This section includes the following topics:

- ["Supported STid readers in Synergis Software 10.6"](#) on page 179
- ["Configuration overview for STid readers with Synergis Software 10.6 "](#) on page 181
- ["Enrolling STid readers attached to the Synergis unit"](#) on page 182
- ["Changing the default communication parameters with STid readers"](#) on page 186
- ["Advanced STid reader setting configuration"](#) on page 187
- ["Encoding a credential on an RFID card in Security Desk"](#) on page 188
- ["Updating the STid configuration on your Synergis unit"](#) on page 189

Supported STid readers in Synergis™ Softwire 10.6

For STid reader integration, each reader is viewed as an interface module.

Synergis™ Softwire supports the following STid readers.

Model	Description	Supported firmware
ARC1-W33-X/PH5-7AA/1 (SSCP/RS-485)	ARC-One - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® One mini mullion readers - RS-485 SSCP	Supported by design
ARC1-W33-X/PH5-7AD/1 (SSCP2/RS-485)	ARC-One - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® One mini mullion readers - RS485 SSCP2	Supported by design
ARC1-W33-X/PH5-7BB/1 (RemoteSecure)	ARC-One - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® One mini mullion readers - RS-485 compliant with RemoteSecure	Supported by design
ARC-W33-A/PH5-7AA/y (SSCP/RS-485)	ARC-A - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard Upgradable readers - RS-485 SSCP	Supported by design
ARC-W33-A/PH5-7AD/y (SSCP2/RS-485)	ARC-A - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard Upgradable readers - RS485 SSCP2	Certified (v6)
ARC-W33-A/PH5-7BB/y (RemoteSecure)	ARC-A - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard Upgradable readers - RS-485 compliant with RemoteSecure	Certified (v17)
ARC-W33-B/PH5-7AA/y (SSCP/RS-485)	ARC-B - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Keypad upgradable readers with keypad - RS485 SSCP. <i>Can operate in Card or PIN, Card and PIN, and Card and PIN on schedule modes.</i>	Certified (v5)
ARC-W33-B/PH5-7AD/y (SSCP2/RS-485)	ARC-B - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard Upgradable readers - RS485 SSCP2	Supported by design
ARC-W33-B/PH5-7BB/y (RemoteSecure)	ARC-B - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard Upgradable readers with keypad - RS-485 compliant with RemoteSecure	Supported by design
ARC-W33-G/PH5-5AA/y (USB)	ARC-G - 13.56 MHz Architect® DESFire® EV1 Secure Read/Write Desktop readers/encoders -USB	Supported by design
ARC-W35-G/PH5-5AA/y (USB)	ARC-G - 13.56 MHz Architect® DESFire® EV1 Secure Read/Write Desktop readers/encoders - USB	Certified
INT-E-7AA/7BB (SSCP/ RS-485)	RemoteSecure - "Transparent" Read/Write reader interface - RS485 & RS485 Host	Certified

Model	Description	Supported firmware
LXS-W33-E/PH5-7AA/y (SSCP/RS-485)	LXS - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard readers - RS-485 SSCP	Certified (U9, U11)
LXS-W33-E/PH5-7AD/y (SSCP2/RS-485)	LXS - CSPN 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard readers - RS-485 SSCP2	Supported by design
LXS-W33-E/PH5-7BB/y (RemoteSecure)	LXS - 13.56 MHz DESFire® EV1 Secure Read/Write Architect® Standard readers - RS-485 compliant with RemoteSecure	Supported by design
STR-W35-E/PH5-5AA/y (USB)	MIFARE Plus/DESFire EV1 reader/encoder - USB	Certified (U9)

Configuration overview for STid readers with Synergis™ Softwire 10.6

The following table summarizes the reader configuration process.

NOTE: STid USB encoding readers are controlled by Security Desk in Security Center 5.6 and later. For more information, see the *Security Desk User Guide*.

Phase	Description	See
1	Make sure your STid reader firmware is up to date and supported by Synergis™ Softwire. Contact your STid representative for the latest firmware.	<ul style="list-style-type: none"> STid-SESPRO documentation that came with your reader. Supported STid readers in Synergis™ Softwire 10.6 on page 179.
2	Configure the reader firmware settings, such as the device address, baud rate, encryption keys, and so on.	STid-SESPRO documentation that came with your reader.
3	Establish communication between the Synergis™ unit and its attached STid readers by configuring them in Synergis™ Appliance Portal ¹ .	Enrolling STid readers attached to the Synergis™ unit on page 182.
4	<p>The Synergis™ unit is pre-configured to communicate with the STid readers using their factory-installed signature and encipherment keys.</p> <p>We recommend changing these encryption keys for better security.</p>	Changing the default communication parameters with STid readers on page 186.
5	If you want your readers to do more than simply returning the CSN (card serial number), then configure the advanced reader settings in <i>SmartCardsReaders.xml</i> .	Advanced STid reader setting configuration on page 187.
6	Apply the settings configured in XML files to the Synergis™ unit.	Updating the STid configuration on your Synergis™ unit on page 189.

¹The reader LED turns OFF in maintenance mode. The door is unlocked, and the reader and all the inputs associated to the door are shunted.

Enrolling STid readers attached to the Synergis™ unit

For the Synergis™ unit to communicate with the STid readers connected to it, you must enroll them with Synergis™ Appliance Portal.

Before you begin

- Configure the STid readers' firmware with STid-SESPRO and attach them the Synergis™ unit.
- Make sure your STid reader firmware is up to date and [supported by Synergis™ Software](#).

What you should know

It is not recommended to connect more than two readers to the same RS-485 channel, as it increases the controller's response time.

NOTE: The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

To enroll the STid readers connected to the Synergis™ unit:

- 1 Log on to the Synergis™ unit.
- 2 Click **Configuration** > **Hardware**
- 3 At the top of the *Hardware* column, click **Add (+)**.
- 4 In the *Add hardware* dialog box, select **STid** as the **Hardware type**.
- 5 Select the **Channel** (A, B, C, or D) and its baud rate (**Bits per second**).

All interface modules connected to the same channel must be from the same manufacturer.

NOTE: The baud rate is a channel property. The channel follows the baud rate of the last reader added to the channel. We strongly suggest to set the baud rate to 38400 bps.

Later, if you want to change the baud rate on a channel, select the channel in the hardware tree and change its value in the configuration page.

- 6 Select the **SSCP protocol version** (either **V1** or **V2**).
The SSCP protocol is a channel property. The channel follows the SSCP protocol of the first reader added to the channel.

(Hardening) The SSCP protocol V2 enforce encrypted and signed communication. Make sure you change the factory default signature and encryption key.

- 7 In the same dialog box, add all STid readers connected to the same channel.
Do one of the following:
 - To add manually, enter the physical address (1 to 127) of the reader and click Add.

The screenshot shows a configuration window titled "Add hardware". It contains the following fields and options:

- Hardware type: STid
- Channel: B
- Interface module type: W33/W35B
- Bits per second: 9600
- SSCP protocol version: V1
- Physical address: 0

Below the fields, there are two labels: "Interface module type" and "Physical address". At the bottom left is an "Add" button. At the bottom right are three buttons: "Scan", "Cancel", and "Save".

Repeat for the second reader if necessary.

- To enroll automatically, click **Scan**.

The discover feature finds and adds all interface modules from the same manufacturer that are connected to the same channel. For this to work, all of the interface modules must use the same baud rate and be configured with a different physical address.

If the controller does not find all connected interface modules, verify their baud rate and physical address.

8 Click **Save**.

The hardware type, channel, and interface module you just added appear in the *Hardware configuration* page.

9 For each interface module you just added, select it from the *Hardware configuration* page, and configure its settings.

For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.

10 Select the **Communication mode**.

The choices are:

- *Plain* (default mode)
- *Encrypted* (private communications)
- *Signed* (authenticated communications)

- *Encrypted and signed* (both private and authenticated communications)

NOTE: If you selected **V2** as the **SSCP protocol**, then only the **Encrypted and signed** option is available.

While the encryption keys are common for all readers connected to the same Synergis™ unit, the communication mode between the unit and each STid reader can be configured separately.

BEST PRACTICE: (*Hardening*) We recommend [changing the default encryption](#) keys provided by the manufacturer for added security.

11 At the bottom of the page, click **Save**.

After you finish

Test your interface module connection and configuration from the I/O diagnostics page. For information about testing interface modules, see the *Synergis™ Appliance Configuration Guide*.

Related Topics

[Advanced STid reader setting configuration](#) on page 187

Enabling transparent mode on STid readers

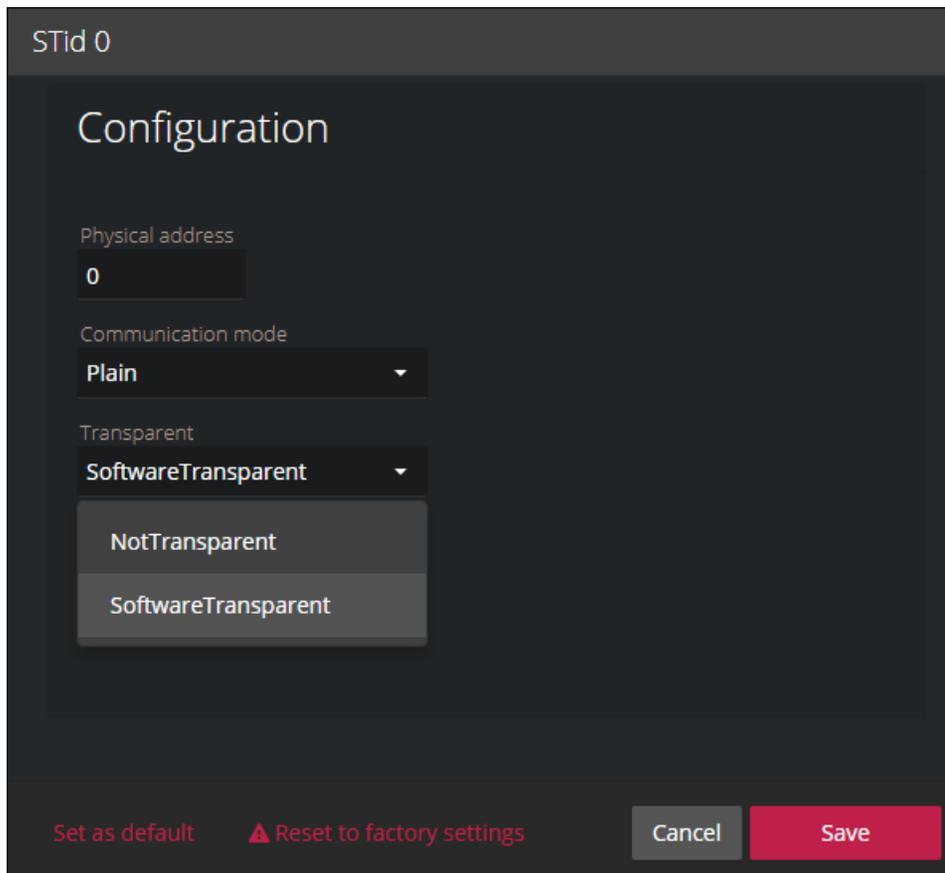
DESFire EV1 readers require cryptographic keys to access a card's secured credential. When keys are loaded into a reader or a Synergis™ unit, then the reader acts as a transparent reader.

Before you begin

- The door must be controlled by a Synergis™ unit running Synergis™ Softwire 10.6 GA or later.
- The door must have an STid reader with a part number ending in AA or AD.
- **NOTE:** Transparent STid readers with part numbers ending in BB cannot be used in this scenario. See [Supported STid readers in Synergis™ Softwire 10.6](#) on page 179 for a list of readers that can be used as transparent readers.

To set up transparent STid readers:

- 1 Open Config Tool.
- 2 Under **STid > Interfaces**, set the **Transparent** option to SoftwareTransparent.



3 Store the cryptographic keys on the Synergis™ Cloud Link.

When you configure the cyptographic keys on the Synergis™ Cloud Link:

- You enter the keys into the 32 available indexed keys in the *primitive key store* through the Synergis™ Softwire 10.6 portal.
- The *SmartCardsSites.xml* file used for the indexed keys is compatible with both software-transparent and non-transparent STid readers.

Limitation: There are two limitations with software transparent readers:

- Transparent readers currently cannot encode cards.
- Cards with transparent mode enabled take about 100 ms longer to read.

Changing the default communication parameters with STid readers

You can change the default signature and encipherment keys used for encrypted and signed communication with the STid readers.

Before you begin

Best practice: The Synergis™ unit is pre-configured to communicate with the STid readers using their factory-installed *Signature* and *Encipherment* keys. We recommend that you use your own key values for better security.

What you should know

Changing the default signature and encipherment keys involves changing a configuration file *STidConfig.xml* on the Synergis™ unit, and a three-step input of the new encryption values by three separate individuals, using the *Primitive key store* page on the Synergis™ Appliance Portal.

To change the encryption keys:

To change the signature and encipherment keys used for encrypted and signed communication with the STid readers, you must apply the new encryption values, *ReaderKc* for the encipherment key and *ReaderKs* for the signature key, to the Synergis™ unit.

For the exact procedure, contact your representative of Genetec Inc.

See also "[Updating the STid configuration on the Synergis™ unit](#)".

Advanced STid reader setting configuration

If you want your readers to do more than just returning the CSN (Card Serial Number) of the cards read (default behavior), you must modify the advanced reader settings stored in the *SmartCardsReaders.xml* file.

Contact your representative of Genetec Inc. for a copy of this XML file so you can modify it to match your actual reader settings. Once it is updated, you must [apply this configuration to your Synergis™ unit](#).

General structure SmartCardsReaders.xml for STid readers

The general structure of SmartCardsReaders.xml is as follows:

```
<SmartCards>
<Readers>
<ReaderParameters ...>
Parameters for 1st reader...
</ReaderParameters>
<ReaderParameters ...>
Parameters for 2nd reader...
</ReaderParameters>
...
<ReaderParameters ...>
Parameters for nth reader...
</ReaderParameters>
</Readers>
</SmartCards>
```

NOTE: The XML file must contain one <ReaderParameters> tag for every STid reader connected to your Synergis™ unit. The above is a generic structure. For any specific card configuration, contact your representative of Genetec Inc.

Sample XML code for a simple reader

The following sample code describes a simple reader.

```
<ReaderParameters Encode="false">
<Reader Pointer="/Devices/Bus/STid/A/Reader/2" />
<Source> <None/> </Source>
<Sites>
<Site Name="INT" />
<Site Name="EXT" />
</Sites>
</ReaderParameters>
```

The tag descriptions are as follows.

- The <Reader> tag identifies the reader. The Pointer parameter must match the reader settings configured in both STid-SESPro and Synergis™ Appliance Portal. Our example refers to the reader connected to Channel A at the address 2.
- The <Site> tag lists the contexts for which the reader is configured to read from the card. In our example, the reader returns the credential associated to the first context successfully found, named either "INT" or "EXT".

Encoding a credential on an RFID card in Security Desk

You can encode a credential on an RFID card using Security Desk.

What you should know

STid USB encoding readers are controlled by Security Desk in Security Center 5.6 and later. For more information, see the *Security Desk User Guide*.

Updating the STid configuration on your Synergis™ unit

To update the STid configuration on your Synergis™ unit, you need to apply the STid configuration XML files to your unit using the Synergis™ Appliance Portal.

To update the STid configuration:

- 1 Zip your XML files (*SmartCardsReaders.xml*, *SmartCardSites.xml*, and *STidConfig.xml*) into a single zip file and rename it to *NewConfig.smc*.

The *NewConfig.smc* file must be located on your local drive.

The *SmartCardSites.xml* file contains predefined format template settings and is found in the Security Center Client installation folder.

- 2 Contact your Genetec Inc.. representative for the exact procedure to apply the *NewConfig* file to your unit using the Synergis™ Appliance Portal.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

- access control unit** An access control unit is a type of entity that represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.
- Access Manager** Access Manager is the role that manages and monitors access control units on the system.
- access point** An access point is any entry (or exit) point to a physical area where access can be monitored and governed by access rules. An access point is typically a door side.
- access rule** An access rule is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point.
- antipassback** Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

C

- cardholder** A cardholder is a type of entity that represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.
- credential** A credential is a type of entity that represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

D

- degraded mode** Degraded mode is an offline operation mode of the interface module when the connection to the Synergis™ unit is lost. The interface module grants access to all credentials matching a specified facility code. Only Mercury and HID VertX interface modules can operate in degraded mode.
- dependent mode** Dependent mode is an online operation mode of the interface module where the Synergis™ unit makes all access control

decisions. Not all interface modules can operate in dependent mode.

E

Engage

Schlage's Engage platform allows credentials to be stored not only on key cards, but also on compatible smart phones. Integration is done through Mercyry EP1501 or EP2500 panels.

F

first-person-in rule

The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

G

global antipassback

Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple Synergis™ units.

H

hardware zone

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

I

interface module

An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

interlock

An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one door to be open at any given time.

I/O linking

I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).

I/O zone

An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis™ units, while one unit acts as the master unit. All Synergis™ units involved in an I/O zone

must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

M

mobile credential

A mobile credential is a credential on a smartphone that uses Bluetooth or Near Field Communication (NFC) technology to access secured areas.

S

secured area

A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

security clearance

A security clearance is a numerical value used to further restrict the access to an area when a threat level is in effect. Cardholders can only enter an area if their security clearance is equal or higher than the minimum security clearance set on the area.

server mode

The server mode is a special online operation mode restricted to Synergis™ units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode.

standalone mode

Standalone mode is an offline operation mode of the interface module where it operates autonomously, making decisions based on the access control settings previously downloaded from the Synergis™ unit. Activity reporting occurs on schedule, or when the connection to the unit is available. Not all interface modules can operate in standalone mode.

strict antipassback

A strict antipassback is an antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.

supervised mode

Supervised mode is an online operation mode of the interface module where the interface module makes decisions based on the access control settings previously downloaded from the Synergis™ unit. The interface module reports its activities in real time to the unit, and allows the unit to override a decision if it contradicts the current settings in the unit. Not all interface modules can operate in supervised mode.

SV-32	The SV-32 is a compact-sized network security appliance that comes pre-installed with Microsoft® Windows, Genetec™ Security Center, and the SV Control Panel. With built-in analog encoder capture cards, the SV-32 is a turnkey appliance that enables you to quickly deploy a standalone system (video surveillance OR access control) or unified system (video surveillance AND access control).
Synergis™ appliance	A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come preinstalled with Synergis™ Software and can be enrolled as access control units in Security Center.
Synergis™ Appliance Portal	Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance, as well as upgrade its firmware.
Synergis™ Cloud Link	Synergis™ Cloud Link is an intelligent and PoE-enabled access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. Synergis™ Cloud Link is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.
Synergis™ Master Controller	Synergis™ Master Controller (SMC) is an access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.
Synergis™ Software	Synergis™ Software is the access control software developed by Genetec Inc. to run on a variety of IP-ready security appliances. Synergis™ Software lets these appliances communicate with third-party interface modules. A security appliance running Synergis™ Software can be enrolled as an access control unit in Security Center.
Synergis™ unit	A Synergis™ unit is a Synergis™ appliance that is enrolled as an access control unit in Security Center.

T

threat level	Threat level is an emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.
timed antipassback	Timed antipassback is an antipassback option. When Security Center considers a cardholder to be already in an area, a passback event is generated when the cardholder attempts to access the same area again during the time delay defined by <i>Presence timeout</i> . When the time delay has expired,

the cardholder can once again pass into the area without generating a passback event.

two-person rule

The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

U**unit synchronization**

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

unlock schedule

An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).

V**visitor escort rule**

The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay.

Z**zone**

A zone is a type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to [Genetec™ Portal](#) and click [Technical Information](#). Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Genetec Patroller™ and the Sharp Portal also include context-sensitive help for each screen. To access the help, click **Help**, press F1, or tap the ? (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

Before contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues.

To access the Technical Information Site, log on to [Genetec™ Portal](#) and click [Technical Information](#). Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: [EN_GLM_ASSURANCE](#) and [EN_GLM_ADVANTAGE](#).

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log in or sign up at <https://gtapforum.genetec.com>.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to <http://www.genetec.com/support/training/training-calendar>.

Licensing

- For license activations or resets, please contact GTAC at <https://gtap.genetec.com>.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at <https://gtap.genetec.com> to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.