



Synergis™ Cloud Link – Administratorhandbuch 3.1.2

Klicken Sie [hier](#) für die neueste Version dieses Dokuments.

Dokument zuletzt aktualisiert: 4. September 2024

Rechtliche Hinweise

©2024 Genetec Inc. Alle Rechte vorbehalten.

Genetec Inc. vertreibt dieses Dokument mit Software, die einen Endbenutzer-Lizenzvertrag umfasst; sie wird unter Lizenz bereitgestellt und darf nur in Übereinstimmung mit den Bedingungen der Lizenzvereinbarung verwendet werden. Die Inhalte dieses Dokuments sind urheberrechtlich geschützt.

Die Inhalte dieses Handbuchs dienen ausschließlich Informationszwecken und können ohne Vorankündigung geändert werden. Genetec Inc. übernimmt keinerlei Verantwortung oder Haftung für eventuelle inhaltliche Fehler oder Ungenauigkeiten in diesem Handbuch.

Diese Publikation darf nicht kopiert, verändert oder in irgendeiner Form oder für irgendeinen Zweck reproduziert werden, noch dürfen ohne die vorherige schriftliche Genehmigung von Genetec Inc. aus dieser Publikation abgeleitete Werke erstellt werden.

Genetec Inc. behält sich das Recht vor, nach eigenem Ermessen Änderungen und Verbesserungen an seinen Produkten vorzunehmen. Dieses Dokument beschreibt den Status eines Produkts zum Zeitpunkt der letzten Dokumentenüberarbeitung und entspricht nicht unbedingt dem neuesten Produktstand.

Genetec Inc. haftet in keinem Fall gegenüber natürlichen oder juristischen Personen für Verluste oder Schäden, die zufällig oder infolge der in diesem Dokument oder in der Computer-Software beschriebenen Anweisungen und der hier beschriebenen Hardware entstehen.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Cloudlink™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Streamvault Edge™, Synergis™, Valcri™ und ihre Logos sowie das Möbiusbandlogo sind Warenzeichen von Genetec Inc. und können in verschiedenen Gerichtsbarkeiten registriert oder zur Registrierung angemeldet sein.

Bei anderen, in diesem Dokument erwähnten Warenzeichen kann es sich um Warenzeichen oder registrierte Warenzeichen der Hersteller oder Anbieter der jeweiligen Produkte handeln.

Patent angemeldet. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™ und andere Produkte von Genetec™ wurden zum Patent angemeldet und können Gegenstand erteilter Patente sein, in den Vereinigten Staaten und in anderen Gerichtsbarkeiten weltweit.

Alle Spezifikationen können ohne vorherige Ankündigung geändert werden.

Dokumentinformationen

Dokumenttitel: Synergis™ Cloud Link – Administratorhandbuch 3.1.2

Dokumentnummer original: EN.702.043-V3.1.2(1)

Dokumentnummer: DE.702.043-V3.1.2(1)

Aktualisierungsdatum des Dokuments: 4. September 2024

Sie können Kommentare, Korrekturen und Anregungen zu diesem Handbuch an documentation@genetec.com senden.

Informationen über dieses Handbuch

Dieser Leitfaden beschreibt, wie die Synergis™ Cloud Link Appliance für die Verwendung mit Security Center konfiguriert wird, und erklärt, wie Sie alle unterstützten Geräte von Drittanbietern in Ihre Appliance integrieren. Es wird vorausgesetzt, dass Sie mit der Security Center-Plattform vertraut sind, insbesondere mit dem Synergis™-Zutrittskontrollsystem.

Dieses Handbuch ergänzt die folgende Dokumentation:

- *Security Center Administrator-Handbuch*
- *Synergis™ Cloud Link – Hardwaremontageleitfaden*
- *Synergis™ Software-Integrationshandbuch*

Weitere Informationen finden Sie im [TechDoc Hub](#).

Dieses Handbuch enthält weder Informationen, die in der Dokumentation von Drittanbietern verfügbar sind, z. B. die Details der Ein- und Ausgänge auf Ihren Schnittstellenmodulen, noch beschreibt es Software von Drittanbietern.

Terminologie

In den meisten Fällen werden *Synergis™-Einheit* (oder *Appliance*) und *Synergis™ Cloud Link-Einheit* (oder *Appliance*) synonym verwendet. Das Wort *Appliance* wird bevorzugt, wenn der Fokus auf dem Gerät selbst liegt, und das Wort *Einheit* wird bevorzugt, wenn der Fokus auf der Registrierung des Geräts in Security Center liegt.

Anmerkungen und Hinweise

Die folgenden Anmerkungen und Hinweise können in diesem Handbuch erscheinen:

- **Tipp:** Gibt Hinweise, wie die Information in einem Thema oder bei einem Arbeitsschritt angewendet werden kann.
- **Bemerkung:** Erläutert einen speziellen Fall oder vertieft einen wichtigen Punkt.
- **Wichtig:** Weist auf kritische Informationen über ein Thema oder einen Arbeitsschritt hin.
- **Achtung:** Zeigt an, dass eine Handlung oder ein Arbeitsschritt den Verlust von Daten, Sicherheitsprobleme oder Funktionsprobleme verursachen kann.
- **Warnung:** Zeigt an, dass eine Handlung oder ein Arbeitsschritt zu Verletzungen oder Schäden an der Hardware führen könnte.

WICHTIG: Inhalte in diesem Handbuch, die auf Websites von Drittanbietern verweisen, waren zum Veröffentlichungszeitpunkt korrekt. Diese Informationen können sich jedoch ohne vorherige Mitteilung von Genetec Inc. ändern.

Inhalt

Preface

Rechtliche Hinweise	ii
Informationen über dieses Handbuch	iii

Teil I: Einleitung

Kapitel 1: Einführung zu Synergis™ Cloud Link

Was ist Synergis Cloud Link?	3
Ausführen von DIP-Schalter-Befehlscodes	4
DIP-Schalter-Befehlscodes	5
Informationen zu Synergis™ Cloud Link 312	6

Kapitel 2: Erste Schritte mit dem Synergis™ Appliance Portal

Was ist Synergis Appliance Portal ?	8
Anmeldung bei der Synergis™ Cloud Link-Appliance	9
Benutzeroberfläche – Tour durch das Synergis Appliance Portal	11

Teil II: Allgemeine Konfiguration

Kapitel 3: Synergis™ Cloud Link-Konfiguration

Die Konfiguration der Synergis™Cloud Link -Einheit vorbereiten	15
Die Synergis™ Cloud Link-Einheit konfigurieren	16
Netzwerkeigenschaften konfigurieren	17
Selbstsignierte Zertifikate verwenden	21
Vertrauenswürdige Zertifikate verwenden	24
Konfigurieren von Schnittstellenmodulen, die an die Synergis™Cloud Link -Einheit angeschlossen sind	27
Standardeinstellungen von Schnittstellenmodulen ändern	29
Benutzerdefinierte Standardeinstellungen von Schnittstellenmodulen löschen	29
Einstellungen für das Schnittstellenmodul klonen	30
Angeschlossene Schnittstellenmodule testen	31
Parameter für alle Einheiten konfigurieren	33
Die Einstellungen für die Lesegerät-LED und den Pieper konfigurieren	35
Die Einstellungen für die Lesegerät-LED und den Pieper von einer Einheit zu einer anderen kopieren	38
Ausgangssteuerungen deaktivieren	39
Informationen über die Automatisierungs-Engine	40
Automatisierungs-Engine-Regeln konfigurieren	41
Entitäts-GUIDs abrufen	42
Konfigurieren der Einstellungen des nachgeschalteten Controllers	43
MIFARE DESFire konfigurieren	44
Sichere Nachrichten mit DESFire EV2 aktivieren	45
SAM-Karten entsperren	46
Schlüsselversionierung für SAM-Karten aktivieren	49
Informationen über den Synergis™ key store	50
Schlüssel-Hashes im Synergis™ key store verwenden	52
Zeitlimit für die PIN-Eingabe für Türen ändern	53

Konfigurieren der Ereignisprotokollierung auf der Synergis™Cloud Link -Einheit	54
Konfigurieren der zusätzlichen Ereignisprotokollierung in der Cloud für die Synergis™Cloud Link -Einheit	55
Die Aufbewahrungszeit von Überwachungsprotokollen für die Synergis™Cloud Link -Einheit konfigurieren	56
Synergis™ Cloud Link-Einheiten in Security Center registrieren	57
Synergis™ Cloud Link-Einheiten zu einer Access Manager-Rolle hinzufügen	57
Synergis™ Cloud Link-Einheiten zu einem gehosteten SaaS Access Manager hinzufügen	58
Die Synergis™ Cloud Link-Einheit mit dem Access Manager synchronisieren	60
Überwachungseingänge der Synergis™ Cloud Link-Appliance konfigurieren	62

Teil III: Integrationsspezifische Konfiguration

Kapitel 4: Allegion-Schlage-Funkschlösser

Allegion-Schlage-Funkschlösser in der Synergis™-Einheit registrieren:	67
Allegion-Schlage-Funkschlösser in der Synergis™-Einheit erneut registrieren:	68

Kapitel 5: Assa-Abloy-Aperio-fähige Schlösser

Koppeln von Aperio-fähigen Schlössern mit dem AH30-Hub	70
Anmeldung von Aperio-fähigen Schlössern, die an einen AH30-Hub angeschlossen sind	74
Koppeln von Aperio-fähigen Schlössern mit dem AH40 IP-Hub	77
Registrieren von Aperio-fähigen Schlössern, die an einen AH40 IP-Hub angeschlossen sind	79
Konfigurieren von Türen, die mit einem Aperio-fähigen Schloss ausgestattet sind	80

Kapitel 6: Assa-Abloy-IP-Schlösser

Konfigurationsübersicht für Assa Abloy-IP-Schlösser	84
Informationen zur Funktion Funkaktivierungsereignisse für Assa Abloy-WiFi-Schlösser	85
Konfiguration der Funktion Funkaktivierungsereignisse für Assa-Abloy-WLAN-Schlösser	86
Aktivierung des Flucht- und Rückkehrmodus bei Assa Abloy-IP-Schlössern mit Korpustyp 8200 und überwachtem Riegel	87
Konfigurieren einer Persona-Seriennummer für die Schlösser IN120 und IN220	89
Informationen zum Durchgangsmodus für Assa Abloy-IP-Schlösser	90
Aktivieren des Durchgangsmodus an Assa Abloy-IP-Schlössern	91
Aktivierung des Privatsphärenmodus bei Assa Abloy-IP-Schlössern ohne überwachten Riegel	92
Assa-Abloy-IP-Schlösser registrieren, die mit der Synergis™-Einheit verbunden sind	94
Testen der Verbindung zwischen Ihrem IP-Schloss und der Synergis™-Einheit	98
Überwachung des Batteriestatus von WiFi-Schlössern	100

Kapitel 7: AutoVu-SharpV-Kameras

Registrieren Sie die AutoVu™ SharpV-Kamera in der Synergis™-Einheit.	102
Eine SharpV-Kamera zur Steuerung einer Fahrzeugzutrittssperre konfigurieren:	105

Kapitel 8: Axis-Controller

Anmeldung von Axis-Controllern an der Synergis™-Einheit	107
Aktivieren des autonomen Modus an Axis-Controllern	109
Härtung von Axis-Controllern	110
Peripheriegeräte des Axis-Controllers konfigurieren	112
Konfigurieren der zusätzlichen E/A-Ports von AXIS A1601-Controllern	115
Lesegerätanschlüsse am Axis-A1001-Controller	117
Lesegerätanschlüsse am AXIS A1601-Controller	118
OSDP (Secure Channel)-Lesegeräte auf AXIS-A1601-Steuerungen aktivieren	119

Kapitel 9: DDS-Controller

Anmeldung von DDS RS-485-Controllern	122
Einstellung der physischen Adresse von TPL-Türcontrollern	125

Kapitel 10: HID-VertX-Sub-Panels

Registrieren der an die Synergis™-Einheit angeschlossenen HID VertX-Subpanels	127
Freischalten von Lesegerät-Überwachung für HID VertX V100	130

Kapitel 11: Mercury-Steuerungen

Einstellungen des Mercury-Lesegeräts	133
Vorbereitung für die Registrierung des Mercury-Controllers	136
Registrierung von Mercury-Controllern auf der Synergis™-Einheit	140
Konfigurieren der Mercury-Controller-Einstellungen im Synergis™ Appliance Portal	144
Unterschiede zwischen der aktivierten und deaktivierten Mercury-Host-Entscheidungsweitergabe	148
Unterstützung langer Berechtigungen auf Mercury-Controllern aktivieren	149
Beschränkungen der nativen Mercury-Bereichssteuerung	150
Konfigurieren des REX-Modus für die Erweiterte zugesicherte Zeit von Mercury pro Tür	151
Datenbank-Layouts für Mercury-Controller	152
Informationen über die Konfiguration von PINs mit führenden Nullen für Mercury-Integrationen	156
Informationen über das Gewähren von Zutritt mit Offline-Mercury-SIO-Boards	157
Offline-Mercury-SIO-Boards konfigurieren, um Zutritt über Einrichtungs-codes zu gewähren	158
Überlegungen zur Installation von OSDP-Lesegeräten mit Mercury	162
OSDP-Lesegeräte (Secure Channel) zu einem Mercury-Controller hinzufügen	164
Konfigurieren von zwei OSDP-Lesegeräten pro Mercury-Gerät	166
Konfigurieren von Mercury-Geräten für die Nutzung von zwei OSDP-Lesegeräten pro Anschluss	166
Hinzufügen von MR51e-Panels zu einem Mercury-Controller	168
Einstellung von MR51e zur Verwendung des öffentlichen DHCP-Adressierungsmodus	168
Einstellung von MR51e zur Verwendung des statischen IP-Adressierungsmodus	168
Einstellung von MR62e zur Verwendung des statischen IP-Adressierungsmodus	170
Konfiguration der Adresse des Mercury-Lesegeräts für das MR62e-Panel	170
Trennen von MR-Panels von einem Mercury-Controller	171
Informationen über Mercury-Auslöser und -Verfahren	172
Aktionstypen für Mercury-Verfahren	173
Ereignistypen für Mercury-Auslöser	175
Mercury-Auslöser im Synergis Appliance Portal konfigurieren	177
Mercury-Verfahren im Synergis Appliance Portal konfigurieren	179
Mercury-Auslöser und -Verfahren im Synergis Appliance Portal deaktivieren	181

Kapitel 12: Allegion-Schlage-Schlösser über Mercury

Anmeldung von Allegion Schlage AD-Schlössern und PIM-Modulen an der Synergis™-Einheit	183
ENGAGE-integrierte Allegion-Schlage-LE- und- NDE-Schlösser über Mercury-Controller registrieren	187

Kapitel 13: BEST-Wi-Q-Schlösser über Mercury

Das Over-Watch-Plugin für die BEST-Wi-Q-Integration konfigurieren	191
BEST-Wi-Q-Gateways auf der Synergis™-Einheit über Mercury-Controller registrieren	194
BEST-Wi-Q-Schlösser und drahtlose Zutrittssteuerungen zum Gateway hinzufügen	197
Informationen über den BEST Wi-Q-Durchgangsmodus	201

Kapitel 14: SimonsVoss-SmartIntego-Schlösser über Mercury

Vorbereitung für die Registrierung von SimonsVoss SmartIntego-Schlössern	203
Registrieren von SimonsVoss SmartIntego-Schlössern an der Synergis™-Einheit	205
Kapitel 15: SALTO-SALLIS-Funkschlösser	
Registrieren von SALTO SALLIS-Schlössern	210
Aktivieren der Verschlüsselung auf einem vorhandenen SALLIS-Router	215
Verschlüsselung auf einem SALLIS-Router deaktivieren	216
Kapitel 16: OSDP-Lesegeräte, die mit den RS-485-Ports von Synergis™ Cloud Link verbunden sind	
Erstellen eines Kanals zur Konfiguration von OSDP-Lesegeräten im Synergis™ Appliance Portal	218
Konfigurieren und Hinzufügen von OSDP-Lesegeräten im Synergis™ Appliance Portal	221
Aktivierung der sicheren Koppelung auf OSDP-Lesegeräten im Synergis™ Appliance Portal	223
MIFARE DESFire für transparente OSDP-Lesegeräte aktivieren	224
Konfigurieren von OSDP-Lesegeräten zur Verhinderung von Relaisangriffen	228
Übertragung von Dateien an OSDP-Lesegeräte im Synergis™ Appliance Portal	229
Kapitel 17: STid-Lesegeräte, die das SSCP-Protokoll verwenden	
Konfigurieren und Registrieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden	231
Aktivieren des transparenten Modus bei STid-Lesegeräten, die das SSCP-Protokoll verwenden	235
Ändern der Standardkommunikationsschlüssel RS-485 für STid-Lesegeräte, die das SSCP-Protokoll verwenden	238
Konfigurieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden, zur Verhinderung von Relaisangriffen	240
Codierung einer Berechtigung auf einer RFID-Karte in Security Desk	242
Teil IV: Wartung und Fehlerbehebung	
Kapitel 18: Wartung und Fehlersuche bei Synergis™ Cloud Link-Einheiten	
Systeminformationen auf der Synergis™ Cloud Link-Einheit anzeigen	245
Informationen zur Synergis™ Cloud Link-Einheit	245
Anmeldepasswort der Synergis™ Cloud Link-Appliance ändern	247
Synergis™Cloud Link -Benutzerprüfungen	248
Gerätekonfigurationsdatei von Ihrer Synergis Cloud Link-Einheit herunterladen	249
Konfigurationsdatei für Ihre Synergis Cloud Link-Einheit hochladen	250
Informationen über die Seite „Kapazitätsbericht“	252
Herunterladen von Supportinformationen für Ihre Synergis™Cloud Link -Einheit	254
Schnittstellenmodule über das Synergis Appliance Portal anpingen	255
Firmware der Synergis™ Cloud Link aktualisieren	256
Zurücksetzen der Synergis™Cloud Link -Einheit nach einer Firmware-Aktualisierung	257
Aktualisieren der Schnittstellenmodul-Firmware über das Synergis™ Appliance Portal	258
Nachgeschaltete Geräte, die für Upgrades über das Synergis™ Appliance Portal unterstützt werden	260
Speicher auf der Synergis™Cloud Link Appliance bereinigen	261
Peer-to-Peer-Information auf der Synergis™Cloud Link -Einheit anzeigen unit	263
Informationen zum Diagnosedienstkonto von Synergis™Cloud Link	265
Diagnosedienstkonto erstellen	265
Hardware oder Software der Synergis™ Cloud Link-Einheit neu starten	267
Glossar	268
Wo finde ich Produktinformationen?	272

Technischer Support 273

Teil I

Einleitung

Dieser Teil enthält die folgenden Kapitel:

- Kapitel 1, "[Einführung zu Synergis™ Cloud Link](#)" auf Seite 2
- Kapitel 2, "[Erste Schritte mit dem Synergis™ Appliance Portal](#)" auf Seite 7

Einführung zu Synergis™ Cloud Link

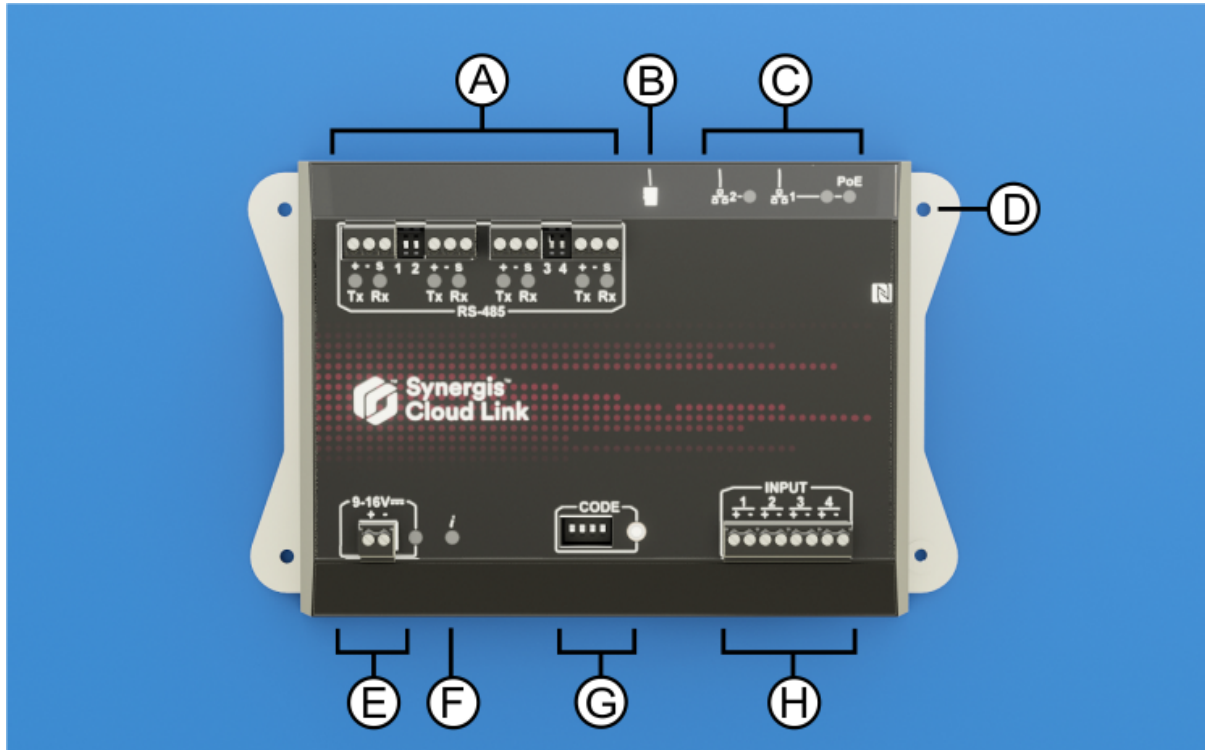
Dieser Abschnitt enthält die folgenden Themen:

- ["Was ist Synergis Cloud Link?"](#) auf Seite 3
- ["Informationen zu Synergis™ Cloud Link 312"](#) auf Seite 6

Was ist Synergis Cloud Link?

Synergis™ Cloud Link ist ein intelligentes PoE-fähiges IoT-Gateway, das als nicht proprietäre Zutrittskontrolllösung entworfen wurde.

Synergis Cloud Link bietet native Unterstützung für gängige, herstellerunabhängige Sicherheitsmodule, von intelligenten Controllern wie Mercury Security, HID Global und Axis Communications bis hin zu elektronischen Schlössern von ASSA ABLOY, Allegion und SimonVoss, die Mercury-Controller erfordern.



Hardwarefunktion	Was Sie wissen sollten
A RS-485-Ports	Synergis™ Cloud Link umfasst vier RS-485-Kommunikationskanäle. Die Anzahl der Module, die Sie an jeden RS-485-Anschluss anschließen können, hängt von der Art der Schnittstellenmodule ab, die Sie installieren.
B MicroSD-Karte	Zukünftige Verwendung
C Ethernet-Anschlüsse	Für die Verbindung mit dem IP-Netzwerk stehen zwei Ethernet-LAN-Anschlüsse zur Verfügung. BEMERKUNG: Der Ethernet-Anschluss 1 kann zur Stromversorgung der Appliance über Power over Ethernet (PoE) verwendet werden.
D Montagelöcher	Sie können das Gerät entweder an einer geeigneten Oberfläche mithilfe der Befestigungslöcher oder an einer DIN-Schiene mithilfe der optionalen DIN-Schienenhalterung befestigen.
E Stromversorgung	Schließen Sie die Appliance an ein 12 VDC-Netzteil (nominal) an.
F Informations-LED (i)	Die LED gibt Auskunft über den Systemstatus.

Hardwarefunktion	Was Sie wissen sollten
G DIP-Schalter für Befehlscode	Mit den vier CODE-DIP-Schaltern können Sie Befehle ausführen, mit denen Sie z. B. bestimmte Appliance-Konfigurationen zurücksetzen können.
H Überwachungseingänge	Die Appliance verfügt über vier Eingänge, die Sie zur Überwachung externer Ereignisse im Zutrittskontrollsystem verwenden können.

Verwandte Themen

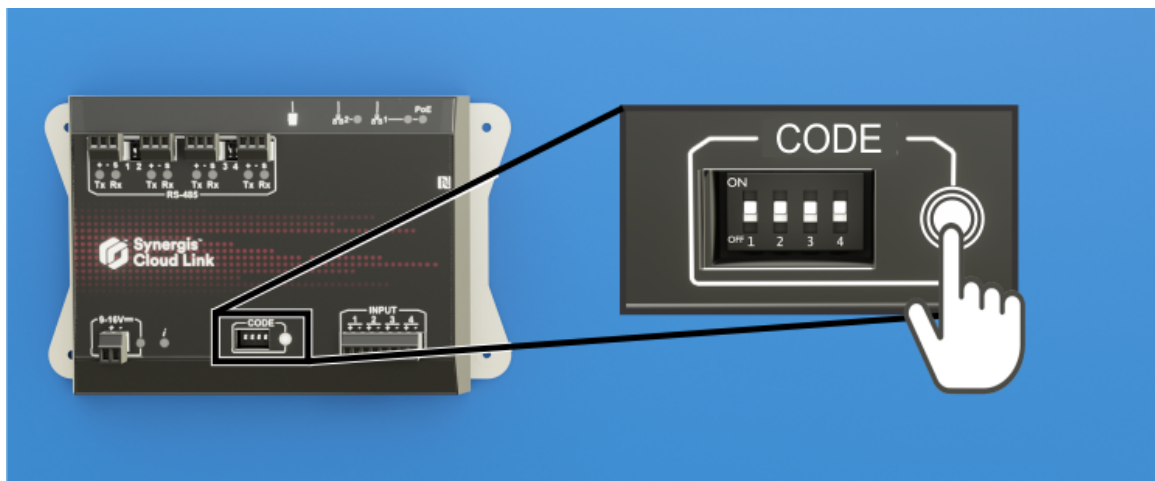
[Informationen zu Synergis™ Cloud Link 312 auf Seite 6](#)

Ausführen von DIP-Schalter-Befehlscodes

umfasst vier Code-DIP-Schalter an der Vorderseite der Appliance. Sie ermöglichen es Ihnen, Befehlscodes auszuführen, die bestimmte Konfigurationen anwenden und Einstellungen zurücksetzen können.

Prozedur

- 1 Wählen Sie einen auszuführenden Befehlscode aus. Weitere Informationen dazu finden Sie unter [DIP-Schalter-Befehlscodes](#) auf Seite 5.
- 2 Geben Sie den Code mit den DIP-Schaltern der Appliance ein.
- 3 Halten Sie die Befehlscode-Taste eine Sekunde lang gedrückt.



Die Informations-LED (i) bestätigt, dass der Code erkannt wurde.

LED-Name	LED-Farbe	Beschreibung
Information (i)	Orange: durchgehend 3 Sekunden	DIP-Schalter-Code erkannt
	Rot: 3× Blinken	DIP-Schalter-Code nicht erkannt

- 4 Um ein versehentliches Zurücksetzen der Konfiguration zu verhindern, stellen Sie die DIP-Schalter immer auf ON ON ON ON.

BEMERKUNG: Mit diesem Code ist keine Aktion verbunden, so dass es sich um einen sicheren Zustand handelt, wenn die Konfiguration abgeschlossen ist.

DIP-Schalter-Befehlscodes

Durch Ein- oder Ausschalten der vier CODE-DIP-Schalter können Sie eine Konfiguration auf die -Appliance anwenden.

DIP-Schalter-Befehle

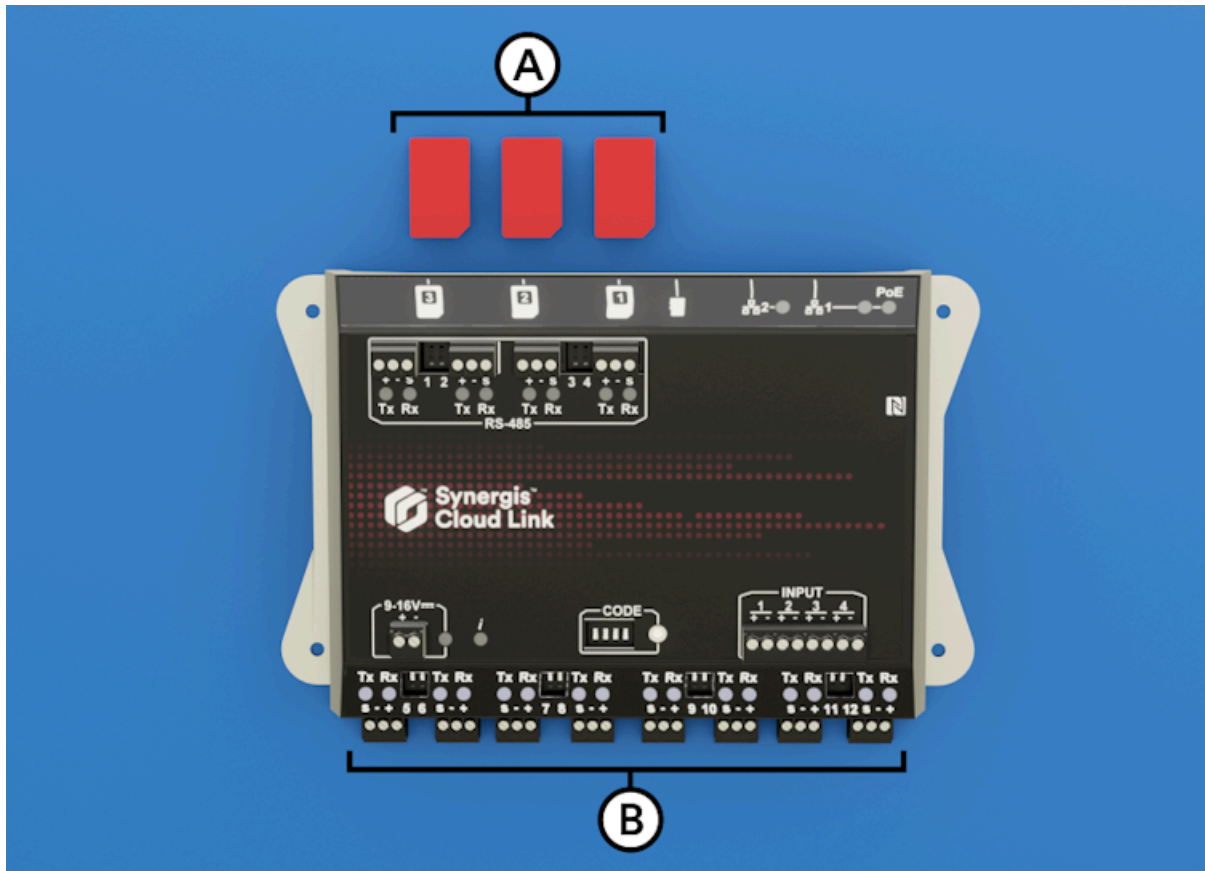
S1	S2	S3	S4	Befehlsbeschreibung
ON	ON	ON	ON	Kein Code: Um ein versehentliches Zurücksetzen der Konfiguration zu verhindern, stellen Sie die DIP-Schalter nach dem Ausführen eines Befehls auf ON ON ON ON.
ON	OFF	OFF	OFF	Teilweise Rücksetzung auf Werkseinstellungen. Dieser Befehl hat folgende Auswirkungen: <ul style="list-style-type: none"> • Setzt das Anmeldepasswort des Synergis™ Appliance Portal auf die Werkseinstellung (-Software) zurück. • Entfernt vom gehosteten SaaS Access Manager • Setzt den Netzwerkadressierungsmodus auf DHCP zurück • Setzt den Erkennungsport auf 2000 zurück • Löscht alle Hardwarekonfigurationen (angeschlossene Schnittstellenmodule) • Löscht alle Konfigurationen für Karteninhaber (Berechtigungen und Zutrittsregeln) • Setzt alle Einstellungen für die gesamte Einheit zurück • Löscht alle Protokollierungsoptionen <p>BEMERKUNG: Die Firmware der Einheit ist von diesem Befehl nicht betroffen.</p>
ON	OFF	OFF	ON	Setzt alle Einstellungen auf die Werkseinstellungen zurück und entfernt SSL-Zertifikate.
OFF	OFF	ON	OFF	Aktiviert die Möglichkeit erneut, Ausgangsstatus auf der Seite <i>E/A-Diagnostik</i> des Synergis™ Appliance Portal zu ändern.

Verwandte Themen

[Ausgangssteuerungen deaktivieren](#) auf Seite 39

Informationen zu Synergis™ Cloud Link 312

Im Vergleich zum standardmäßigen Synergis™ Cloud Link verfügt das 312-Modell der Appliance über acht zusätzliche RS-485-Ports und drei SAM-Kartensteckplätze.



Buchstabe	Hardwarefunktion	Was Sie wissen sollten
A	SAM-Kartensteckplätze	Sie können SAM-Karten zum Speichern von Verschlüsselungsschlüsseln verwenden.
B	RS-485	Der Synergis™ Cloud Link 312 stellt dem System 8 zusätzliche RS-485-Ports zur Verfügung, insgesamt also 12.

BEMERKUNG: Der Synergis™ Cloud Link 312 wurde nicht auf UL/ULC-Compliance geprüft und darf nicht in Installationen verwendet werden, bei denen eine UL/ULC-Compliance erforderlich ist.

Weitere Informationen zur Synergis Cloud Link 312 Appliance finden Sie unter [Synergis Cloud Link 312 – Spezifikatione](#).

Verwandte Themen

[Was ist Synergis Cloud Link?](#) auf Seite 3

Erste Schritte mit dem Synergis™ Appliance Portal

Dieser Abschnitt enthält die folgenden Themen:

- ["Was ist Synergis Appliance Portal ?"](#) auf Seite 8
- ["Anmeldung bei der Synergis™ Cloud Link-Appliance"](#) auf Seite 9
- ["Benutzeroberfläche – Tour durch das Synergis Appliance Portal "](#) auf Seite 11

Was ist Synergis Appliance Portal ?

Das Synergis™ Appliance Portal ist das Web-basierte Verwaltungstool für die Konfiguration und Verwaltung eines Synergis™ Gerätes und für die Aktualisierung seiner Firmware.

Sie können die folgenden Tasks über das Portal ausführen:

- Ändern des Passworts, das für die Verbindung zur Synergis™ Cloud Link Appliance erforderlich ist.
- Konfigurieren der Netzwerkeinstellungen an der Appliance, um sie Ihrem System anzupassen.
- Registrieren und Konfigurieren der Schnittstellenmodule, die mit der Appliance verbunden sind.
BEMERKUNG: Mercury- und Honeywell-Controller (PW6K1IC, PRO32IC, PW7K1IC und PRO42IC) müssen auf der Seite *Peripheriegeräte* der Zutrittskontrolleinheit im Config Tool registriert und konfiguriert werden.
- Konfigurieren des Verhaltens der Zutrittskontrolle der Appliance, für Offline- und Online-Betrieb.
- Testen und Diagnostizieren der Schnittstellenlesegeräte, E/A- und Modulverbindungen der Appliance.
- Konfigurieren von Einstellungen, die für Mercury-Steuerungen und nachgeschaltete Steuerungen spezifisch sind.
- Konfigurieren Sie die Einstellungen für die Lesegerät-LED und den Pieper mit Unterstützung von Export und Import.
- Konfigurieren von MIFARE DESFire auf OSDP- und STid-Lesegeräten.
- Aktivieren Sie SAM-Karten-basierte Kryptographie auf der Synergis™ Cloud Link 312-Appliance.
- Verwalten von X.509-Zertifikaten.
- Anzeigen und Exportieren von Status und Konfiguration der Appliance.
- Anzeigen der Funktionen und Status von Mercury-Steuerungen.
- Aktualisieren der Appliance-Firmware und Schnittstellenmodul-Firmware.
- Neustarten von Hardware oder Software der Appliance.

Tasks, die in Config Tool ausgeführt werden müssen

Sie können die folgenden Tasks nicht über das Portal ausführen. Verwenden Sie stattdessen das Security Center Config Tool.

- Zuweisen von Geräten (Ein-/Ausgangskontakte, Lesegeräte) zu Türen und Bereich.
- Konfigurieren einzelner Tür- und Bereichseigenschaften.
- Konfigurieren der E/A-Verknüpfung.
- Konfigurieren von *Karten- und PIN*-Lesegeräten, damit sowohl die Karte als auch die PIN für den Zutritt erforderlich sind.

Weitere Informationen über die Bereitstellung von Synergis finden Sie in den folgenden Kapiteln des *Security Center – Administratorhandbuchs*:

- Informationen über das Konfigurieren von Türen und *Karte-und-PIN*-Lesegeräten finden Sie unter [Bereiche, Türen und Aufzüge](#).
- Informationen über das Konfigurieren von Zonen und IO-Verknüpfungen finden Sie unter [Zonen und Einbruchserkennung](#).

Anmeldung bei der Synergis™ Cloud Link-Appliance

Um Ihre Synergis™ Cloud Link-Appliance zu konfigurieren, melden Sie sich über das Synergis™ Appliance Portal bei der Appliance an.

Bevor Sie beginnen

Die folgenden Informationen sind erforderlich, um sich das erste Mal anzumelden:

- **Hostname oder IP-Adresse der Appliance:** Der Standard-Hostname besteht aus SCL (für Synergis™ Cloud Link), gefolgt von der MAC-Adresse der Appliance. Beispielsweise SCL0010F32CF482. Die MAC-Adresse befindet sich auf dem Etikett der Appliance.

Um die IP-Adresse zu erhalten, pingen Sie die Appliance. Bei IPv6-IP-Adressen müssen Sie die letzten zwei Zeichen des Werts in der Klammer entfernen, den Sie vom Ping zurückerhalten. Die IPv6-Adresse enthält die Klammern. Beispielsweise [fe80::ebf:15ff:xxxx:xxxx].

- **Standardbenutzername und Passwort:** Der Standardbenutzername und das Standardpasswort sind *admin* und *softwire*. Bei der ersten Anmeldung werden Sie gezwungen, ein neues Passwort zu erstellen.

Was Sie noch wissen sollten

- Wenn Sie ab Synergis Cloud Link-Firmware 2.0.3 nicht DHCP verwenden, können Sie sich mithilfe einer Adresse mit lokalem Link verbinden. Vor 2.0.3 muss IPv6 eine Adresse mit lokalem Link verwenden.
- Wenn Sie kein DHCP verwenden, wird durch alternative Netzwerkverbindungen verhindert, dass das Synergis Appliance Portal geladen wird.

Prozedur

- 1 (Nur bei der ersten Anmeldung) Verbinden Sie den **LAN 1**-Port der Appliance mit Ihrem LAN.
- 2 Öffnen Sie einen Webbrowser und geben Sie `https://` gefolgt vom Hostnamen oder der IP-Adresse der Appliance ein.

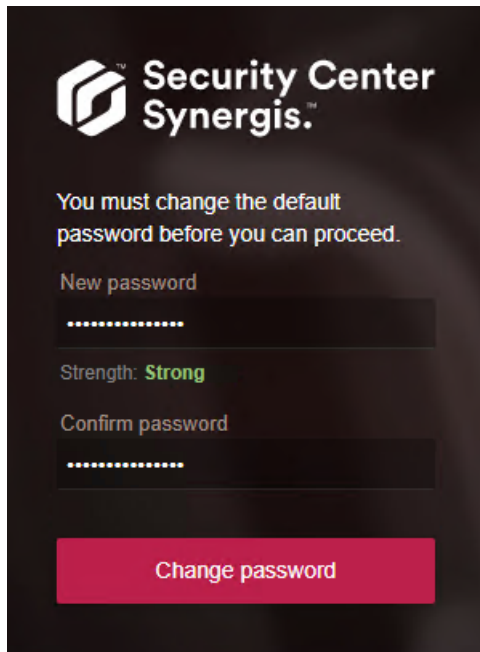
Beispiel: Die folgende ist eine Adresse, die den Hostnamen verwendet: `https://SCL0010F32CF482`

Die folgende ist eine Adresse, die das IPv6-IP-Adressformat verwendet: `https://[fe80::ebf:15ff:xxxx:xxxx]`

- 3 Wenn Sie eine neue Browsersitzung geöffnet haben, um sich bei der Appliance anzumelden, wird eine Fehlermeldung bezüglich des Zertifikats angezeigt. Befolgen Sie die Anweisungen auf dem Bildschirm Ihres Browsers, um zur Website zu gelangen.
- 4 Geben Sie den Benutzernamen und das Passwort ein und klicken Sie dann auf **Anmelden**. Wenn Sie das Standardpasswort bereits geändert haben, wird die Startseite angezeigt. Wenn Sie das Standardpasswort nicht geändert haben, müssen Sie vor der Anmeldung ein neues Passwort erstellen.

- 5 Geben Sie ein neues *starkes* oder *sehr starkes* Passwort ein, bestätigen Sie es und klicken Sie auf **Passwort ändern**.

BEMERKUNG: Das Passwort muss mindestens 15 Zeichen lang sein.



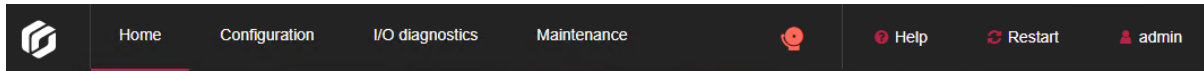
The screenshot shows the 'Security Center Synergis.' interface for changing a password. It features a dark background with white text. At the top left is the Synergis logo. Below it, a message states: 'You must change the default password before you can proceed.' There are two input fields: 'New password' and 'Confirm password', both filled with dots. A green indicator shows 'Strength: Strong'. At the bottom is a red button labeled 'Change password'.

Das Passwort wird für den Benutzer aktualisiert, und Sie müssen sich mit dem neuen Passwort anmelden.

Benutzeroberfläche – Tour durch das Synergis Appliance Portal

Die Startseite des Synergis™ Appliance Portal ist in eine obere Menüleiste und einen Schnellzugriffsbereich mit Symbolen unterteilt, die zu häufig verwendeten Tasks führen. Die Startseite ist dynamisch und die Symbole ändern sich je nach Kontext.

Das Hauptmenü besteht aus folgenden Elementen:



- **Home:** Kehrt zur Startseite zurück.
- **Konfiguration:** Öffnet die Seite *Hardware*, auf der Sie [die an die Synergis™ Cloud Link -Einheit angeschlossenen Schnittstellenmodule konfigurieren können](#). Auf die folgenden Unterseiten kann über die Seite *Konfiguration* zugegriffen werden:
 - *Geräteweite Parameter*
 - *Synergis Softwire-Protokollierung*
 - *Netzwerk*
 - *Benutzer*
 - *Einstellungen für Mercury-Controller*
 - *Mercury-Auslöser und Verfahren*
 - *Einstellungen für Lesegerät-LED und Beeper*
 - *Synergis IX-Controller-Einstellungen*
 - *Automatisierungs-Engine*
 - *Einstellungen des nachgeschalteten Controllers*
 - *Synergis™ key store*
 - *MIFARE DESFire*
 - *Erweitertes OSDP*
 - *Zertifikate*
 - *SAM-Karte* (Nur für eine [Synergis™ Cloud Link-312-Einheit](#))
 - *Cloud-Konnektivität* (für Einheiten mit dem Cloud Agent)
- **E/A-Diagnostik:** Öffnet die Seite *Kanäle*, auf der Sie die Statusänderungen der Kontakte und die auf den Lesegeräten gelesenen Berechtigungen beim Auslösen überwachen können. Auf die folgenden Unterseiten kann über die Seite *E/A-Diagnostik* zugegriffen werden:
 - *Geräte*
 - *Kanäle*
 - *Schnittstellen*
 - *Türen*
 - *Aufzüge*
 - *Hardwarezonen*
 - *E/A-Zonen*
- **Wartung:** Öffnet die Seite *Systemstatus*, auf der Sie [einen Schnappschuss Ihrer Einheit und des Netzwerkstatus anzeigen lassen können](#). Sie können auch Konfigurationsdateien von dieser Seite herunterladen. Auf die folgenden Unterseiten kann über die Seite *Wartung* zugegriffen werden:

- *Funktionsbericht*
- *Protokollanzeige*
- *Diagnoseprotokolle herunterladen*
- *Ping-Diagnostik*
- *Netzwerkerfassung* (zum Verwenden durch den Genetec Technical Support)
- *Schnittstellen-Upgrade*
- *Upgrade der Firmware*
- *Massenspeicher*
- *Peer-zu-Peer*
- *Synergis IX Backup herunterladen*
- **Benachrichtigungen:** Zeigt Systemintegritätswarnungen an.
- **Hilfe:** Öffnet ein Dropdown-Menü mit zwei Elementen:
 - *Hilfe* öffnet *Synergis™ Cloud Link – Administratorhandbuch* auf einer separaten Browserseite.
 - In *Über* werden die Firmwareversion der Synergis™ Cloud Link Appliance sowie Copyright-Informationen angezeigt.
- **Neustart:** Öffnet ein Dropdown-Menü, in dem Sie zwischen **Softwareneustart** oder **Systemneustart** wählen können, um *die Hardware oder Software der Synergis™ Cloud Link-Einheit neu zu starten* .
- **Administrator:** Öffnet ein Dropdown-Menü, in dem Sie sich vom Gerät abmelden oder *Benutzerkonfiguration* auswählen können. Hier können Sie die Sprache der Portalschnittstelle ändern.

Teil II

Allgemeine Konfiguration

Dieser Teil enthält die folgenden Kapitel:

- Kapitel 3, "[Synergis™ Cloud Link-Konfiguration](#)" auf Seite 14

Synergis™ Cloud Link-Konfiguration

Dieser Abschnitt enthält die folgenden Themen:

- ["Die Konfiguration der Synergis™ Cloud Link -Einheit vorbereiten"](#) auf Seite 15
- ["Die Synergis™ Cloud Link-Einheit konfigurieren"](#) auf Seite 16
- [" Netzwerkeigenschaften konfigurieren "](#) auf Seite 17
- [" Selbstsignierte Zertifikate verwenden "](#) auf Seite 21
- [" Vertrauenswürdige Zertifikate verwenden "](#) auf Seite 24
- ["Konfigurieren von Schnittstellenmodulen, die an die Synergis™ Cloud Link -Einheit angeschlossen sind"](#) auf Seite 27
- [" Angeschlossene Schnittstellenmodule testen "](#) auf Seite 31
- [" Parameter für alle Einheiten konfigurieren "](#) auf Seite 33
- [" Die Einstellungen für die Lesegerät-LED und den Pieper konfigurieren "](#) auf Seite 35
- [" Die Einstellungen für die Lesegerät-LED und den Pieper von einer Einheit zu einer anderen kopieren "](#) auf Seite 38
- [" Ausgangssteuerungen deaktivieren "](#) auf Seite 39
- ["Informationen über die Automatisierungs-Engine"](#) auf Seite 40
- [" Automatisierungs-Engine-Regeln konfigurieren "](#) auf Seite 41
- [" Konfigurieren der Einstellungen des nachgeschalteten Controllers "](#) auf Seite 43
- [" MIFARE DESFire konfigurieren "](#) auf Seite 44
- ["SAM-Karten entsperren"](#) auf Seite 46
- ["Schlüsselversionierung für SAM-Karten aktivieren"](#) auf Seite 49
- ["Informationen über den Synergis™ key store"](#) auf Seite 50
- ["Schlüssel-Hashes im Synergis™ key store verwenden"](#) auf Seite 52
- ["Zeitlimit für die PIN-Eingabe für Türen ändern"](#) auf Seite 53
- ["Konfigurieren der Ereignisprotokollierung auf der Synergis™ Cloud Link -Einheit"](#) auf Seite 54
- ["Konfigurieren der zusätzlichen Ereignisprotokollierung in der Cloud für die Synergis™ Cloud Link -Einheit"](#) auf Seite 55
- ["Die Aufbewahrungszeit von Überwachungsprotokollen für die Synergis™ Cloud Link -Einheit konfigurieren"](#) auf Seite 56
- ["Synergis™ Cloud Link-Einheiten in Security Center registrieren"](#) auf Seite 57
- ["Die Synergis™ Cloud Link-Einheit mit dem Access Manager synchronisieren"](#) auf Seite 60
- ["Überwachungseingänge der Synergis™ Cloud Link-Appliance konfigurieren"](#) auf Seite 62

Die Konfiguration der Synergis™ Cloud Link -Einheit vorbereiten

Bevor Sie eine Synergis™ Cloud Link -Einheit konfigurieren können, müssen Sie einige Vorkonfigurationsschritte ausführen.

- Lesen Sie die *Synergis™ Cloud Link-Versionshinweise* zu bekannten Problemen und anderen Informationen über diese Version.
- Ihnen sollte ein Computer mit einer Netzwerkkarte, einem Ethernet-Kabel und einem Webbrowser zur Verfügung stehen.
- (Optional) Weisen Sie der Synergis™ Cloud Link -Einheit eine IP-Adresse zu, welche Sie ggfs. von Ihrer IT-Abteilung bekommen.
- Konfigurieren Sie die Hardwareeinstellungen (DIP-Schalter, Adresswahlen usw.) auf ihre endgültige Position auf den Schnittstellenmodulen.
- Verbinden Sie die Schnittstellenmodule über die richtigen Kommunikationskanäle mit der Synergis™ Cloud Link-Einheit.

BEMERKUNG: Da jeder Hardwarehersteller ein anderes Kommunikationsprotokoll verwendet, müssen alle an denselben RS-485-Kanal angeschlossenen Schnittstellenmodule vom selben Hersteller stammen.

- Verbinden Sie physische Geräte (REX, Türsensoren usw.) oder verwenden Sie Testschalter und LEDs während der Konfigurationsphase.
Weitere Informationen finden Sie im *Synergis™ Cloud Link-Hardwareinstallationshandbuch*.
- Laden Sie das neueste Synergis™ Cloud Link -Paket von der Seite [Produktdownload](#) im GTAP herunter.
- Installieren und konfigurieren Sie Security Center mit mindestens einer Access Manager-Rolle.
Informationen über die Bereitstellung von Synergis™ finden Sie im *Security Center-Administratorhandbuch*.

Nach Durchführen dieser Schritte

[Ihre Synergis-Cloud-Link-Einheit konfigurieren](#) .

Die Synergis™ Cloud Link-Einheit konfigurieren

Sie können die Synergis™ Cloud Link-Einheit konfigurieren, nachdem die Schritte zur Vorkonfiguration abgeschlossen sind.

Bevor Sie beginnen

Führen Sie die vorbereitenden Schritte für die Konfiguration aus.

Prozedur

- 1 Alle Synergis™ Cloud Link-Einheiten werden mit einem werkseitig zugewiesenen Hostnamen bereitgestellt. Wenn Ihr Netzwerk DHCP nicht unterstützt, müssen Sie der [Appliance eine neue IP-Adresse zuweisen](#).
- 2 [Ändern Sie das X.509-Standardzertifikat der Einheit](#).
- 3 [Aktualisieren Sie die Firmware der Synergis™ Appliance auf die neueste Version](#).
- 4 Schließen Sie die Schnittstellenmodule physisch an die Synergis™ Cloud Link-Einheit an. Weitere Informationen finden Sie im *Synergis™ Cloud Link – Hardwareinstallationshandbuch* im [TechDoc Hub](#).
- 5 [Stellen Sie die Kommunikation zwischen der Synergis™ Cloud Link-Einheit und den angeschlossenen Schnittstellenmodulen über das Synergis™ Appliance Portal her](#).
- 6 [Testen Sie Ihre Hardwareverbindungen und Ihre Konfiguration](#) und nehmen Sie gegebenenfalls Anpassungen vor.
- 7 [Konfigurieren Sie das Zutrittskontrollverhalten der Synergis™ Cloud Link-Einheit](#).
- 8 [Fügen Sie die Synergis™ Cloud Link-Einheit einer Access Manager-Rolle hinzu](#), damit sie Teil Ihres Security Center-Systems wird.

Netzwerkeigenschaften konfigurieren

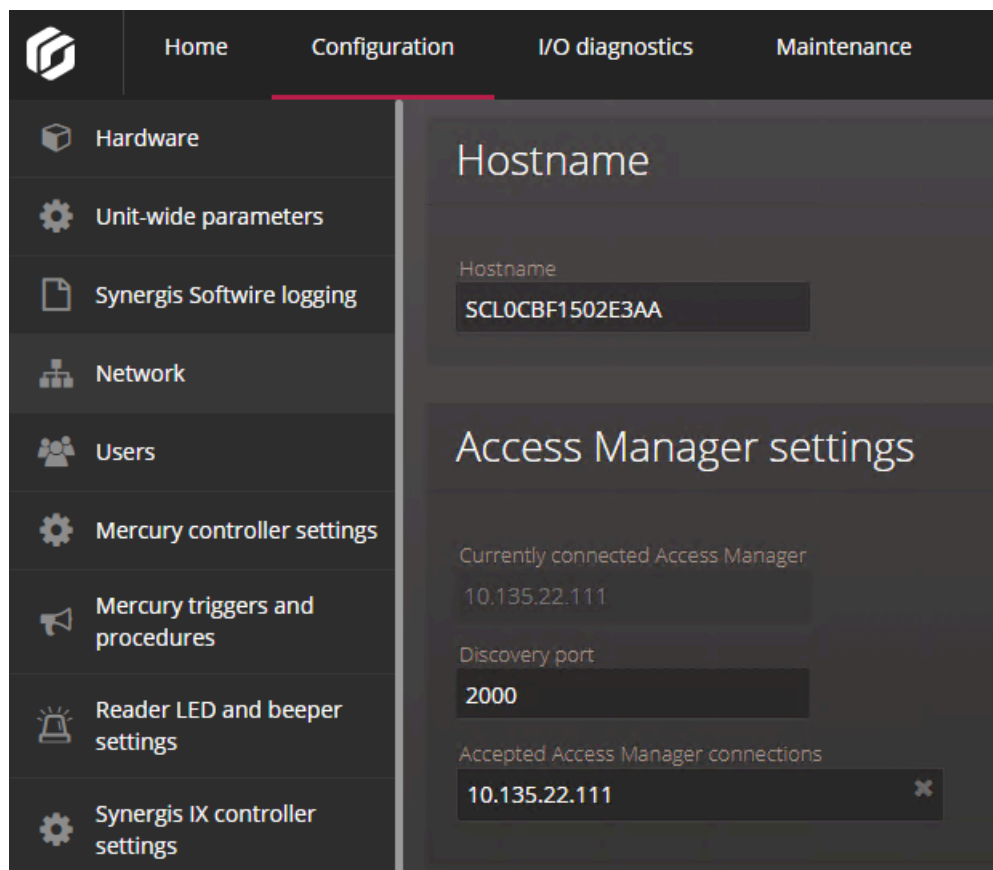
Um sicherzustellen, dass die Synergis™ Cloud Link-Einheit im Netzwerk Ihres Security Center-Systems erreichbar ist, müssen Sie die Netzwerkeigenschaften der Einheit konfigurieren.

Was Sie noch wissen sollten

Die Synergis™ Cloud Link-Einheit wird mit einem werkseitig zugewiesenen Hostnamen bereitgestellt. Wenn Ihr Netzwerk DHCP nicht unterstützt, müssen Sie der Einheit eine neue IP-Adresse zuweisen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Netzwerk**.
- 3 (Optional) Ändern Sie im Abschnitt *Hostname* bei Bedarf den **Hostnamen**.



BEST-PRACTICE: Hostnamen müssen in einem Netzwerk eindeutig sein und der Standard-Hostname muss garantiert eindeutig sein. Wir empfehlen daher, den Standard-Hostnamen beizubehalten, der sich auf dem Etikett auf der Appliance befindet.

- 4 Ändern Sie im Abschnitt *Access-Manager-Einstellungen* den **Erkennungspport**, falls notwendig.

- 5 Wählen Sie im Abschnitt *Netzwerkeinstellungen* **LAN1** oder **LAN2** als die Netzwerkschnittstelle aus, die verwendet wird, um die Synergis™ Cloud Link-Einheit mit ihrem Access Manager zu verbinden, und konfigurieren Sie dann die IP-Adresse und die Netzwerkeigenschaften der Synergis™ Cloud Link-Einheit.

WICHTIG: Um Netzwerkprobleme zu verhindern, müssen bei der Konfiguration der Netzwerkeigenschaften der Einheit strenge Regeln befolgt werden:

- Befindet sich die Einheit nicht im selben Netzwerksegment wie der Access Manager, muss die IP-Adresse der Einheit als **statische IP-Adresse** oder **DHCP mit statischer IP-Zuweisung** festgelegt werden.
- **LAN1** und **LAN2** sollten sich nicht im selben Subnetz befinden. Wenn dies der Fall ist, sollte nur einer von ihnen mit einem Default-Gateway konfiguriert werden.

The screenshot displays the configuration interface for the Synergis™ Cloud Link unit. The top navigation bar includes 'Home', 'Configuration' (highlighted), 'I/O diagnostics', and 'Maintenance'. The left sidebar lists various configuration categories, with 'Network' selected. The main content area is titled 'Network settings' and is divided into two sections: 'LAN1' (selected) and 'LAN2'. Under 'LAN1', three radio buttons are visible: 'Static IP', 'DHCP', and 'DHCP with Static IP allocation' (which is selected). Below these are input fields for 'IP address' (10.122.167.39), 'Subnet mask' (255.255.0.0), 'Default gateway' (10.122.0.1), 'Preferred DNS server', and 'Alternate DNS server'. The 'Network time' section below shows a checked checkbox for 'Use network time' and an 'NTP server' field containing 'ntp.qix.ca'.

- 6 Konfigurieren Sie im Abschnitt *Netzwerkzeit* den Network-Time-Protocol (NTP)-Server, wenn einer verfügbar ist.

a) Klicken Sie auf **Netzwerkzeit verwenden** und geben Sie den Namen des **NTP-Servers** ein.

BEST-PRACTICE: Ein NTP-Server bietet größere zeitliche Genauigkeit als das eingebaute Protokoll, das die Synergis™ Cloud Link-Einheiten mit ihrem Access Manager synchronisiert. Verwenden Sie daher die Netzwerkzeit, wenn ein NTP-Server in Ihrem Netzwerk verfügbar ist. Alle Security Center-Server und -Workstations müssen mit dem gleichen NTP-Server wie Ihre Synergis™ Cloud Link-Appliances synchronisiert sein.

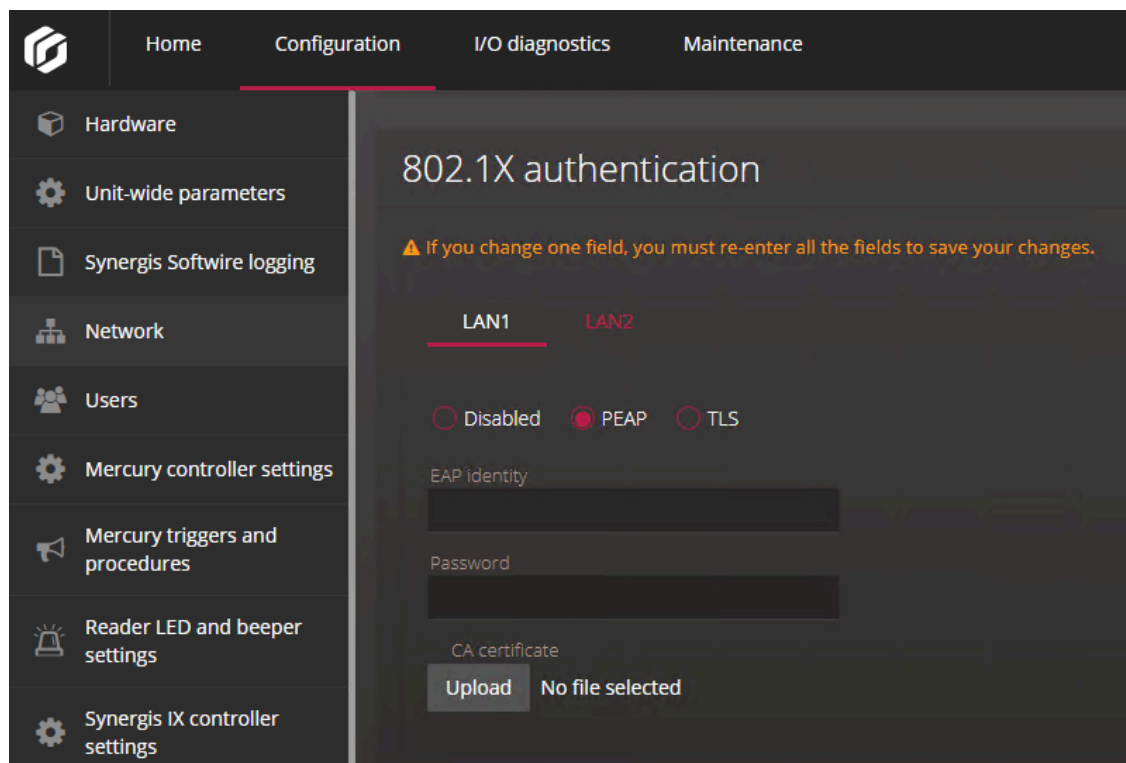
- 7 Wählen Sie im Abschnitt *802.1X-Authentifizierung* das LAN, das Sie für die 802.1X-Authentifizierung verwenden möchten, und wählen Sie den Authentifizierungsmodus aus.

BEMERKUNG: Wenn Sie diese Einstellungen einmal konfiguriert haben, werden ihre aktuellen Werte angezeigt. Wenn Sie einen Wert ändern möchten, müssen Sie alle Werte erneut eingeben. Andernfalls werden Ihre Änderungen nicht gespeichert.

- **Deaktiviert:** Die 802.1X-Authentifizierung ist standardmäßig deaktiviert.
- **PEAP:** Verwenden Sie das Protected Extensible Authentication Protocol (PEAP).

Geben Sie die **EAP-Identität** (Benutzername) und das **Passwort** ein und laden Sie das **CA-Zertifikat** hoch.

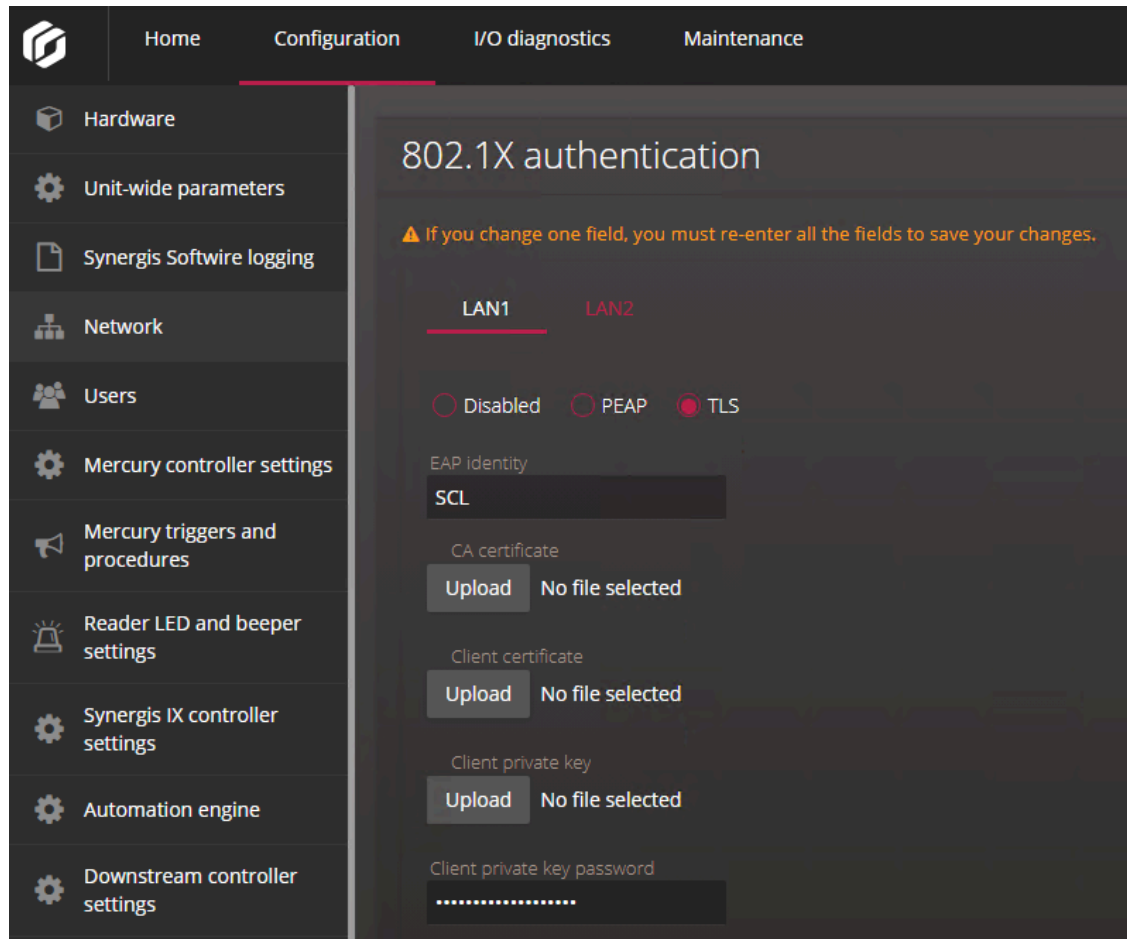
BEMERKUNG: Beim CA-Zertifikat muss es sich um eine PEM- oder DER-Datei handeln.



- **TLS:** Verwenden Sie das TLS (Transport Layer Security)-Protokoll.

Geben Sie die **EAP-Identität** (Benutzername) ein, laden Sie das **CA-Zertifikat**, das **Client-Zertifikat** und den **privaten Client-Schlüssel** hoch und geben Sie das **Passwort für den privaten Client-Schlüssel** ein.

BEMERKUNG: Beim CA-Zertifikat muss es sich um eine PEM- oder DER-Datei handeln.



8 Klicken Sie auf **Speichern**.

Die Synergis™ Cloud Link-Einheit wird neu gestartet und Sie werden automatisch zur neuen IP-Adresse der Einheit umgeleitet.

Wenn Sie die Netzwerkzeit aktiviert haben, wird die Einheit 45 Sekunden nach Aktivierung der Einstellung mit dem NTP-Server und anschließend alle 15 Minuten synchronisiert.

Verwandte Themen

[Ausführen von DIP-Schalter-Befehlscodes](#) auf Seite 4

Selbstsignierte Zertifikate verwenden

Eine Synergis™ Cloud Link-Einheit wird mit einem X.509-Zertifikat bereitgestellt, das während der Produktion generiert wurde. Ersetzen Sie das Standardzertifikat zur Erhöhung der Sicherheit, indem Sie ein neues selbstsigniertes Zertifikat erstellen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Zertifikate**.

- 3 Füllen Sie im Abschnitt *Zertifikatsverwaltung* die Identifikationsfelder aus.

BEMERKUNG: Die Felder **Allgemeiner Name**, **Alternativer Antragstellername** und **Land** sind obligatorisch.

Certificate management

⚠ Changes to the certificate settings on this page will cause the unit to appear offline in Security Center until the trusted certificate is reset in Config Tool.

Common name
SCL0CBF1500ED64

Organization
Genetec

Organization unit
Technical Writing

Locality
Montreal

State
QC

Country
CA

Subject alternative name
SCL0CBF1500ED64

Certificate type
ECDSA 384 bits

Period of
5 years

Generate new self-signed certificate

Create certificate signing request

- 4 Wählen Sie in der Liste **Zertifikatstyp** eine/n der folgenden Algorithmen und Schlüssellängen aus.
- ECDSA 256 Bits
 - ECDSA 384 Bits
 - RSA 2048 Bits
 - RSA 3072 Bits
 - RSA 4096 Bits
- 5 Klicken Sie auf **Neues selbstsigniertes Zertifikat erstellen**, starten Sie Ihren Browser dann neu und melden Sie sich wieder bei der Einheit an.
Das Zertifikat wird jetzt auf der Einheit generiert.

- 6 Installieren Sie das Zertifikat im Zertifikatspeicher des Browsers.
 - a) Klicken Sie auf **Konfiguration > Zertifikate**.
 - b) Klicken Sie im Abschnitt *Aktuelles Zertifikat* auf **Download**.
 - c) Befolgen Sie unter Windows die Anweisungen im *Zertifikatimport-Assistenten*, um das Zertifikat mit der Option **Lokaler Computer** in den Ordner *Vertrauenswürdige Stammzertifizierungsstellen* zu importieren.
Installieren Sie das Zertifikat auf allen Computern, die eine Verbindung zur aktualisierten Synergis™ Cloud Link-Einheit herstellen.

BEMERKUNG: Die Zertifikatsdatei wird mit dem Hostnamen und dem Suffix *.cer* gekennzeichnet.

- 7 Starten Sie Ihren Browser neu und melden Sie sich wieder bei der Einheit an.

Ihre Einheit zeigt keinen Sicherheitsfehler mehr in der Adressleiste an, wenn Sie eine Verbindung über den Hostnamen herstellen.

Nach Durchführen dieser Schritte

Wenn die Einheit bereits in Security Center registriert war, wird der Access Manager dem neuen Zertifikat nicht vertrauen oder sich nicht mit der Einheit verbinden und Sie müssen das vertrauenswürdige Zertifikat in Config Tool zurücksetzen.

Weitere Informationen finden Sie unter [Das vertrauenswürdige Zertifikat zurücksetzen](#) .

Vertrauenswürdige Zertifikate verwenden

Die Authentizität des selbstsignierten Zertifikats, das standardmäßig auf der Einheit ist, wird nicht wie üblich mit der Public Key Infrastructure durchgesetzt. Für mehr Sicherheit können Sie stattdessen ein vollständig vertrauenswürdiges Zertifikat verwenden, das von einer Zertifizierungsstelle signiert ist.

Was Sie noch wissen sollten

Das Verwenden eines von einer Zertifizierungsstelle signierten Zertifikats eignet sich besser für Setups, wo mehrere Computer und Browser auf die Synergis™ Cloud Link-Einheit zugreifen, da Sie dadurch nicht jeden Browser konfigurieren müssen, damit er diese vertrauenswürdigen Zertifikate erkennt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Zertifikate**.

- 3 Füllen Sie im Abschnitt *Zertifikatsverwaltung* die Identifikationsfelder aus.

Das Feld **Allgemeiner Name** enthält standardmäßig den Hostnamen der -Einheit. Das Feld **Alternativer Antragstellername** enthält standardmäßig auch den Hostnamen, kann jedoch bearbeitet werden, um eine durch Kommas getrennten DNS-Liste zu erstellen.

BEMERKUNG: Die Felder **Allgemeiner Name**, **Alternativer Antragstellername** und **Land** sind obligatorisch.

Certificate management

⚠ Changes to the certificate settings on this page will cause the unit to appear offline in Security Center until the trusted certificate is reset in Config Tool.

Common name
SCL0CBF1500ED64

Organization
Genetec

Organization unit
Technical Writing

Locality
Montreal

State
QC

Country
CA

Subject alternative name
SCL0CBF1500ED64

Certificate type
ECDSA 384 bits

Period of
5 years

Generate new self-signed certificate

Create certificate signing request

- 4 Wählen Sie in der Liste **Zertifikatstyp** eine/n der folgenden Algorithmen und Schlüssellängen aus.

- ECDSA 256 Bits
- ECDSA 384 Bits
- RSA 2048 Bits
- RSA 3072 Bits
- RSA 4096 Bits

5 Klicken Sie auf **Zertifikatsignieranforderung erstellen**.

Eine *.req*-Datei wird erstellt, die den öffentlichen Teil des Zertifikats enthält. Die Datei enthält keinen privaten Schlüssel und ist daher nicht vertraulich.

6 Navigieren Sie im Windows-Explorer zum Ordner „Downloads“ und kopieren Sie anschließend die Signaturanfragendatei *.req*. Senden Sie sie anschließend an eine Zertifizierungsstelle.

Nach der Verifizierung signiert die Zertifizierungsstelle den öffentlichen Teil des Zertifikats mit einem eigenen privaten Schlüssel.

7 Nachdem Sie die Zertifikate von der Zertifikatsstelle erhalten haben, importieren Sie das signierte Zertifikat.

a) Melden Sie sich wieder bei der Einheit an und klicken Sie auf **Konfiguration > Zertifikate**.

b) Klicken Sie im Abschnitt *Signiertes Zertifikat importieren* auf **Zertifikat auswählen** und navigieren Sie zu dem Ordner mit den Zertifikaten.

c) Wählen Sie das erste Zertifikat aus und klicken Sie auf **Hochladen**. Wiederholen Sie dies für die verbleibenden Zertifikate.

BEMERKUNG: Jedes Zertifikat in der Zertifikatkette muss einzeln oder in einem einzigen Vorgang hochgeladen werden, wenn Sie eine *.p7b*-Sammeldatei erhalten haben. Wenn Sie die Sammlungsdatei erhalten haben, müssen Sie das Stammzertifikat nicht hochladen.

Ihre Einheit zeigt keinen Sicherheitsfehler mehr in der Adressleiste an, wenn Sie eine Verbindung über den Hostnamen herstellen.

Nach Durchführen dieser Schritte

Wenn die Einheit bereits in Security Center registriert war, wird der Access Manager dem neuen Zertifikat nicht vertrauen oder sich nicht mit der Einheit verbinden und Sie müssen das vertrauenswürdige Zertifikat in Config Tool zurücksetzen.

Weitere Informationen finden Sie unter [Das vertrauenswürdige Zertifikat zurücksetzen](#) .

Konfigurieren von Schnittstellenmodulen, die an die Synergis™ Cloud Link -Einheit angeschlossen sind

Um die Kommunikation zwischen der Synergis™ Cloud Link -Einheit und den verbundenen Schnittstellenmodulen herzustellen, müssen Sie diese im Synergis™ Appliance Portal konfigurieren.

Bevor Sie beginnen

Verbinden Sie Ihre Schnittstellenmodule physisch mit der Synergis™ Cloud Link -Einheit.

Was Sie noch wissen sollten

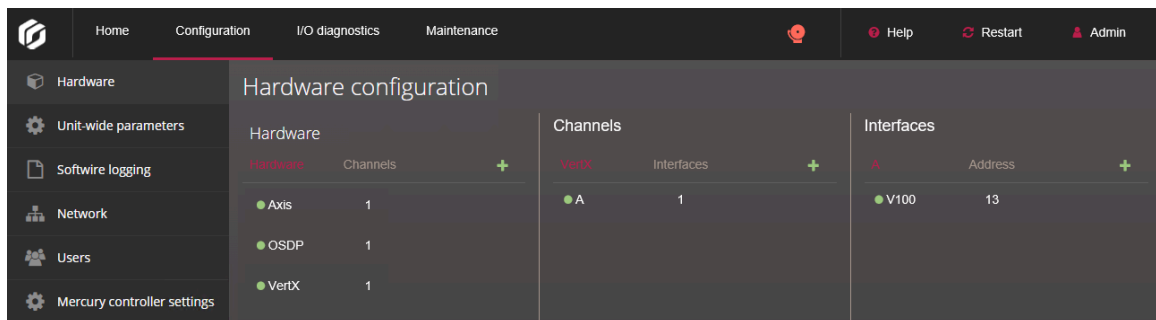
Ein Schnittstellenmodul ist eine Sicherheitsvorrichtung von einem Drittanbieter, die über IP, USB oder RS-485 mit einer Zutrittskontrollereinheit kommuniziert und für die Einheit zusätzliche Ein- und Ausgänge sowie Lesegerät-Anschlüsse bereitstellt.

BEMERKUNG: Mercury LP- und MP-Controller und Honeywell-Controller (PW6K1IC, PRO32IC, PW7K1IC und PRO42IC) müssen über das Config Tool von Security Center auf der Seite *Peripheriegeräte* der Zutrittskontrollereinheit registriert und konfiguriert werden.

Prozedur

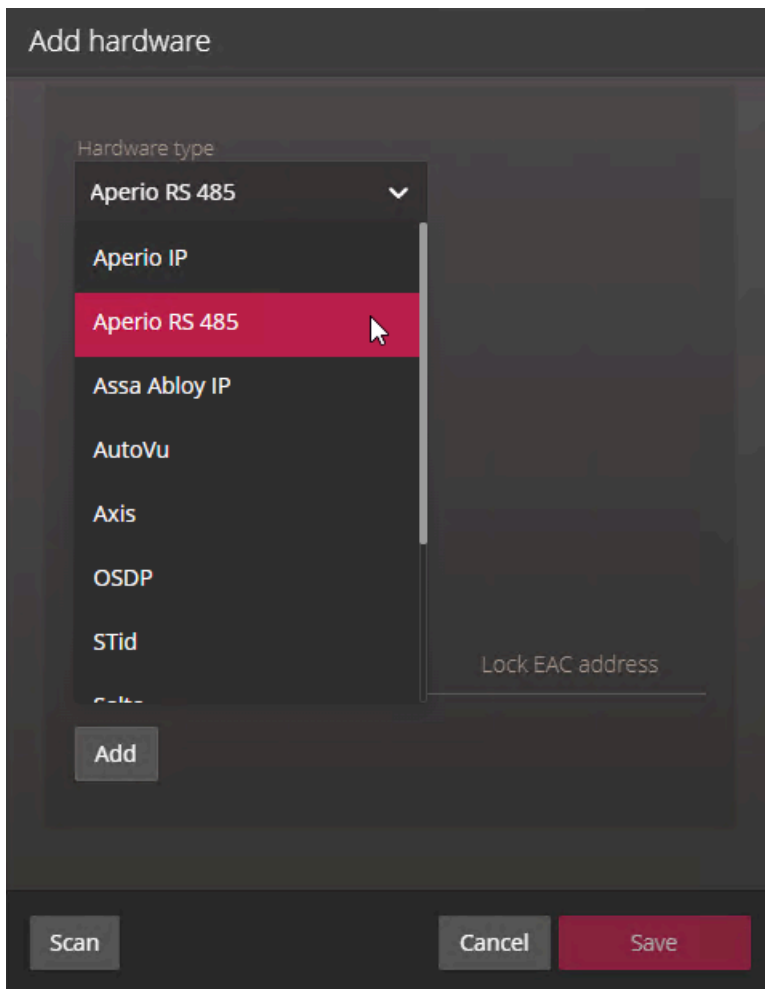
- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.


Das Portal zeigt die Hardware-Struktur als drei Spalten an. Die in jeder Spalte angezeigten Informationen hängen davon ab, was Sie in der vorherigen Spalte ausgewählt haben:



- **Hardware:** Ihre konfigurierten Hardware-Hersteller und die Anzahl die Kanäle, die Sie verwenden. Klicken auf einen Hardwarehersteller ruft dessen Kanäle in der zweiten Spalte auf.
 - **Kanäle:** Die Kanäle der Hersteller, die in der ersten Spalte ausgewählt sind. Wenn Sie den Mauszeiger über einen Kanal bewegen, werden die Optionen bearbeiten (✎), klonen (📄) und löschen (✖).
 - **Schnittstellen:** Die Schnittstellenmodule, die mit dem Kanal verbunden sind, die in der zweiten Spalte ausgewählt sind.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.

- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* den **Hardwaretyp**, den **Kanal** und die restlichen Eigenschaften des Schnittstellenmoduls aus. Diese hängen vom ausgewählten Hardwaretyp ab.



- 5 Fügen Sie im selben Dialogfeld wie folgt alle Schnittstellenmodule hinzu, die mit demselben Kanal verbunden sind:
- Um die Schnittstellenmodule manuell hinzuzufügen, klicken Sie auf **Hinzufügen**.
 - Klicken Sie auf **Scannen**, um die Schnittstellenmodule zu ermitteln.
Schnittstellenmodule desselben Herstellers, die an denselben Kanal angeschlossen sind, müssen dieselbe Baudrate verwenden und mit unterschiedlichen physischen Adressen konfiguriert sein, um in die Liste aufgenommen werden zu können.
- 6 Klicken Sie auf **Speichern**.
Die von Ihnen hinzugefügten Hardwaretypen, Kanäle und Schnittstellenmodule werden im Hardwarediagramm angezeigt.
- 7 Wählen Sie jedes hinzugefügte Schnittstellenmodul im Hardwarediagramm aus, klicken Sie auf  und konfigurieren Sie die Einstellungen im folgenden Fenster.
Eine Beschreibung dieser Einstellungen finden Sie in der Dokumentation des Herstellers.
- 8 Klicken Sie unten auf der Seite auf **Speichern**.

Nach Durchführen dieser Schritte

[Testen Sie die Schnittstellenmodule.](#)

Standardeinstellungen von Schnittstellenmodulen ändern

Wenn Sie viele Schnittstellenmodule des zu konfigurierenden Typs haben und den Konfigurationsprozess vereinfachen möchten, können Sie die werkseitigen Standardeinstellungen ändern und sie als neue Standardeinstellungen für jeden Modultyp speichern.

Was Sie noch wissen sollten

Die Synergis™ Cloud Link-Einheit ist mit den werkseitigen Standardeinstellungen für alle unterstützten Schnittstellenmodule konfiguriert.

Prozedur

- 1 Klicken Sie auf **Konfiguration > Hardware**.
- 2 Wählen Sie auf der Seite *Hardwarekonfiguration* den Hersteller, den Kanal und die Schnittstelle aus, die Sie als Modell verwenden möchten.
- 3 Nehmen Sie im Dialogfeld *Bearbeiten* alle erforderlichen Änderungen an den Einstellungen vor.
- 4 Klicken Sie auf **Als Standard festlegen** und speichern Sie die Einstellungen.

Ihre Änderungen werden als neue Standardeinstellungen gespeichert. Wenn Sie das nächste Mal ein Schnittstellenmodul desselben Typs hinzufügen, werden Ihre neuen Standardwerte zum Initialisieren der Seite *Eigenschaften* verwendet.

Benutzerdefinierte Standardeinstellungen von Schnittstellenmodulen löschen

Wenn Sie benutzerdefinierte Standardeinstellungen für Schnittstellenmodule erstellt haben und zu werkseitigen Standardeinstellungen beim Hinzufügen neuer Schnittstellenmodule zurückkehren möchten, können Sie die benutzerdefinierten Standardeinstellungen löschen.

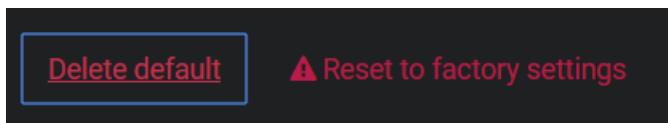
Was Sie noch wissen sollten

WICHTIG: Verwechseln Sie diese Schaltfläche (**Standard löschen**) nicht mit der Schaltfläche (**Auf Werkseinstellungen zurücksetzen**).

- Durch Klicken auf **Standard löschen** wird nur die Nutzung Ihrer benutzerdefinierten Standardeinstellungen eingestellt, sodass beim nächsten Hinzufügen eines Schnittstellenmoduls desselben Typs die werkseitigen Standardwerte verwendet werden.
- Durch Klicken auf **Auf Werkseinstellungen zurücksetzen** werden die Werte auf der aktuellen Seite beim Speichern auf die Werkseinstellungen zurückgesetzt.

Prozedur

- 1 Klicken Sie auf **Konfiguration > Hardware**.
- 2 Wählen Sie auf der Seite *Hardware* das Schnittstellenmodul aus, das Sie als Standard festgelegt haben.
- 3 Klicken Sie im Dialogfeld *Bearbeiten* auf **Standard löschen**.




Einstellungen für das Schnittstellenmodul klonen

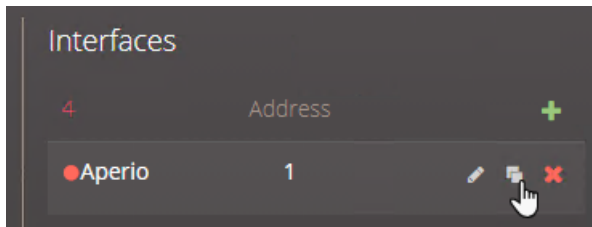
Um Zeit bei der Konfiguration zu sparen, können Sie neue Schnittstellenmodule hinzufügen, indem Sie die Einstellungen eines vorhandenen Schnittstellenmoduls duplizieren und dann Änderungen vornehmen, falls erforderlich.

Bevor Sie beginnen

Wenn Sie Ihre Schnittstellenmodule klonen möchten, die neuen jedoch bereits erstellt haben, löschen Sie die neuen.

Prozedur

- 1 Klicken Sie auf **Konfiguration > Hardware**.
- 2 Wählen Sie im Abschnitt *Hardwarekonfiguration* das Schnittstellenmodul aus, das Sie aus dem Hardwarediagramm klonen möchten.
- 3 Klicken Sie auf .



- 4 Fügen Sie im Dialogfeld *Hardware klonen* alle Schnittstellenmodule hinzu, die Sie basierend auf dem ausgewählten Modell hinzufügen möchten, und klicken Sie dann auf **Speichern**.
Sie müssen nur die physische Adresse jedes neuen Schnittstellenmoduls angeben sowie den Kanal, mit dem es verbunden ist. Alle anderen Einstellungen werden vom Modellschnittstellenmodul übernommen.

Nach Durchführen dieser Schritte

Ändern Sie die Einstellungen der geklonten Schnittstellenmodule nach Bedarf.

Angeschlossene Schnittstellenmodule testen

Sie können Ihre Hardwareverbindungen und Ihre Konfiguration testen, indem Sie ihre Reaktionen auf der Seite *E/A-Diagnose* des Synergis™ Appliance Portal in Echtzeit überwachen.

Bevor Sie beginnen

[Konfigurieren Sie die Schnittstellenmodule.](#)

Was Sie noch wissen sollten

Sie können die Seite anpassen, um die Elemente anzuzeigen, die Sie überwachen möchten.

Prozedur


- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **E/A-Diagnose** > **Schnittstellen**.

The screenshot shows the 'I/O diagnostics' page for a Mercury LP1502 device. The interface is dark-themed. On the left is a sidebar menu with categories: Devices, Channels, Interfaces, Doors, Elevators, Hardware zones, and I/O zones. The main area has a top navigation bar with 'Home', 'Configuration', 'I/O diagnostics' (selected), and 'Maintenance'. Below the navigation, there are two expandable sections for the device 'Mercury LP1502 10.23.75.138:3001' and its module 'MR52 1'. The 'Readers' section shows two entries, each with a 'Beep' button. The 'Relays' section is a table with 6 rows and 3 columns: 'Output', 'Normal', and 'Active'. The 'Inputs' section is a table with 3 rows and 6 columns: 'Input', 'Normal', 'Active', 'Trouble', 'Cut', and 'Shorted'. Each cell in the tables contains a red circle icon indicating the status.

Readers	Event
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Reader 1	Beep
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Reader 2	Beep

Relays	Normal	Active
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Output 1	●	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Output 2	●	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Output 3	●	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Output 4	●	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Output 5	●	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Output 6	●	○

Inputs	Normal	Active	Trouble	Cut	Shorted
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Input Connection-Reader-1	○	●	○	○	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Input Connection-Reader-2	○	●	○	○	○
Mercury LP1502 10.23.75.138:3001 - MR52 1 - Input Tamper- Reader-1	●	○	○	○	○

- 3 Klicken Sie auf , um die Schnittstelle zu erweitern, die Sie überwachen möchten.

- 4 Aktivieren Sie die an die Synergis™ Cloud Link -Einheit angeschlossenen Geräte (Kartenlesegeräte, Türsensoren, Türschlösser usw.) über die Schnittstellenmodule.
Wenn sich diese nicht wie erwartet verhalten, überprüfen Sie Ihre Verbindungen und die Konfigurationen Ihres Schnittstellenmoduls.

Parameter für alle Einheiten konfigurieren

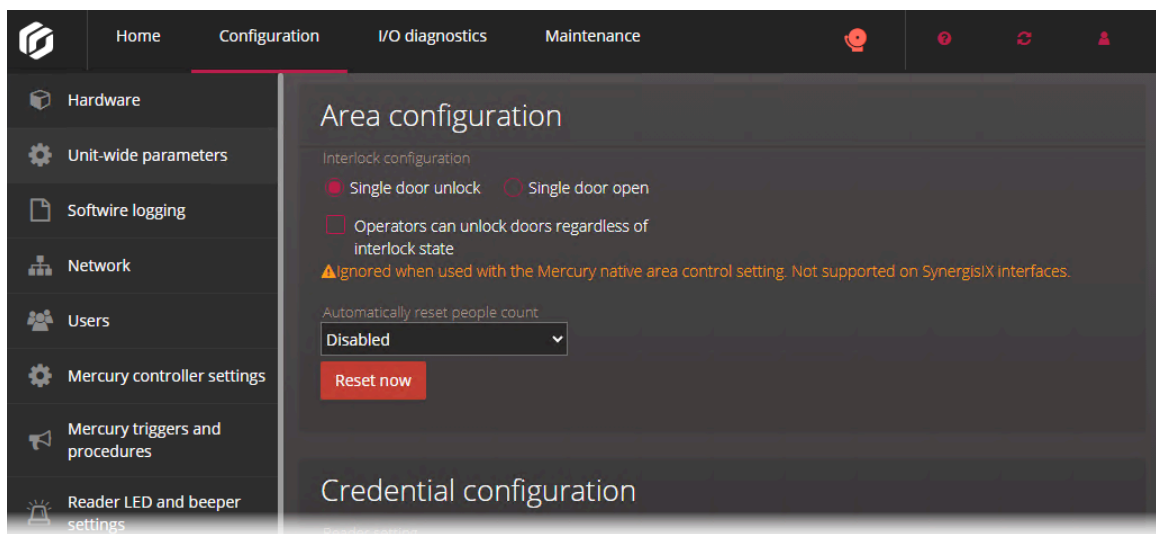
Die meisten Verhaltensweisen von Schnittstellenmodulen gelten für alle Schnittstellenmodule, die an dieselbe Synergis™ Cloud Link-Einheit angeschlossen sind. Sie können diese Einstellungen für die gesamte Einheit auf der Seite *Parameter für die gesamte Einheit* im Synergis™ Appliance Portal konfigurieren.

Was Sie noch wissen sollten

Das folgende Verfahren beschreibt alle Optionen auf der Seite *Geräteweite Parameter*. Konfigurieren Sie sie entsprechend Ihrer Systemanforderungen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Parameter für die gesamte Einheit**.



- 3 Konfigurieren Sie im Abschnitt *Bereichskonfiguration* die folgenden Optionen:
 - **Interlock (Verriegelungs)-Konfiguration:** Eine Verriegelung ist ein System mit mehreren Türen, bei dem immer nur eine Tür geöffnet werden kann. Sie haben zwei Möglichkeiten:
 - **Einzelne Tür entsperren:** Entriegeln Sie jeweils nur eine Tür.
 - **Einzelne Tür offen :** Sobald eine Tür geöffnet ist, sperren Sie sofort alle anderen Türen.
 - **Bediener können Türen unabhängig von ihrem Verriegelungsstatus entsperren:** Erlauben Sie, dass Türen manuell mithilfe der Schaltfläche **Entsperren** im Widget *Tür* entsperrt werden, selbst wenn Türen aufgrund einer Verriegelung versperrt sein sollten. Sie können diese Einstellung entweder mit den Verriegelungseinstellungen **Einzelne Tür entsperren** oder **Einzelne Tür öffnen** verwenden.
Diese Einstellung muss für jede Synergis™ Cloud Link-Einheit, die eine Verriegelung steuert, konfiguriert werden und das Ändern dieser Einstellung erfordert einen Software-Neustart.

BEMERKUNG: Diese Einstellung wird in Synergis™-IX-Integrationen nicht unterstützt und ignoriert, wenn sie mit einer der folgenden nativen Mercury-Funktionen verwendet wird:

- Anti-Passback
- Max. Belegung
- Verriegelung
- **Personenzählung automatisch zurücksetzen** : Setzen Sie die Personenzählung täglich oder wöchentlich zurück. Diese Einstellung ist standardmäßig deaktiviert.

4 Konfigurieren Sie im Abschnitt *Berechtigungsachweiskonfiguration* die folgenden Optionen:

- **Lesegeräteinstellungen:** Gilt nur für Karten- und PIN-Lesegeräte. Sie haben zwei Möglichkeiten:
 - **Karte oder PIN:** Sie können entweder die Karte oder die PIN verwenden, um den Zutritt zu gewähren.
 - **Nur Karte:** Nur die Karte wird zum Erteilen des Zutritts verwendet.

BEMERKUNG: Um den Modus *Karte und PIN* zu erzwingen, damit sowohl die Karte als auch die PIN für den Zutritt verwendet werden, müssen Sie die Einstellungen des Lesegeräts in Config Tool konfigurieren. Der Modus *Karte und PIN* funktioniert nur während des Lesegerätzeitplans. Außerhalb des Lesegerätzeitplans arbeitet das Lesegerät entweder im Modus *Nur Karte* oder im Modus *Karte oder PIN*, je nach den im Synergis Appliance Portal konfigurierten Lesegeräteinstellungen.

- **Maximale PIN-Länge:** Gilt für Schnittstellenmodule, welche die Option-00-Lesegeräte unterstützen. Die Synergis™Cloud Link -Einheit verarbeitet die eingegebene PIN in dem Moment, in dem sie die maximale Anzahl von Stellen erreicht hat, ohne auf die Taste „#“ zu warten.

BEMERKUNG: Nicht alle Integrationen unterstützen diese Funktion. Weitere Informationen finden Sie im *Synergis™ Software-Integrationshandbuch*.

5 Konfigurieren Sie im Abschnitt *Ausgangssteuerungen* die folgenden Optionen:

- **Ausgangssteuerungen deaktivieren:** Klicken Sie, um die Möglichkeit zu deaktivieren, Ausgangsstatus auf der Seite *E/A-Diagnostik* des Synergis Appliance Portals zu ändern.

6 Konfigurieren Sie im Abschnitt *Security Center SaaS-Registrierung* die folgenden Optionen:

- **Für Registrierung mit Cloud kommunizieren:** Bevor Sie Ihre Synergis™-Einheit in Security Center SaaS registrieren, vergewissern Sie sich, dass diese Option aktiviert ist. Sobald Ihre Einheit registriert ist, wird die Option automatisch deaktiviert.

7 Klicken Sie auf **Speichern**.

Alle Änderungen werden nach einem Neustart der Software wirksam.

Verwandte Themen

[DIP-Schalter-Befehlscodes](#) auf Seite 5

[Schlüsselversionierung für SAM-Karten aktivieren](#) auf Seite 49

[Ausgangssteuerungen deaktivieren](#) auf Seite 39

Die Einstellungen für die Lesegerät-LED und den Pieper konfigurieren

Sie können das Verhalten der Lesegerät-LED und des Piepers so konfigurieren, dass der Person, die vor der Tür steht, unterschiedliche Zutrittskontrollstatus kommuniziert werden. Sie können die LED beispielsweise bernsteinfarben blinken lassen, wenn das System darauf wartet, dass eine PIN eingegeben wird.

Bevor Sie beginnen

Derzeit wird diese Funktion nur von durch Mercury gesteuerte Lesegeräte unterstützt.

Was Sie noch wissen sollten

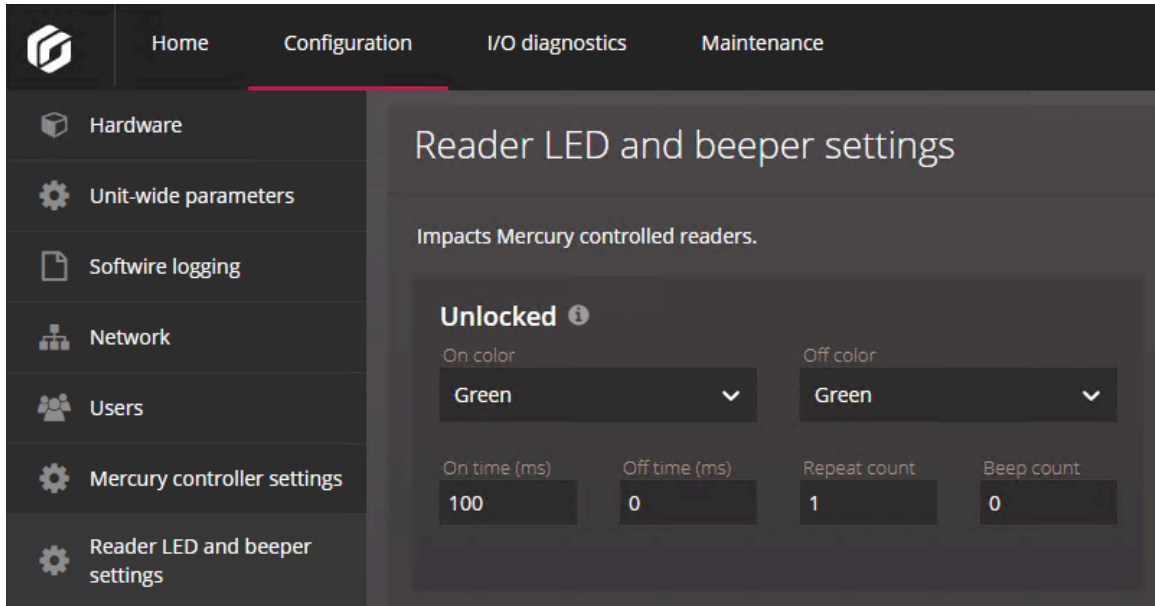
Sie können die folgenden Zutrittskontrollstatus mithilfe eines eindeutigen Verhaltens der Lesegerät-LED und des Piepers angeben:

- **Entriegelt:** Die Tür wird für Wartungszwecke, nach einem Zeitplan oder durch das vorübergehende Überschreiben eines Zeitplans entsperrt.
- **Überbrückt:** Das Lesegerät ist parallelgeschaltet (deaktiviert).
- **Nur Karte:** Die Tür ist versperrt, während das Lesegerät im Modus *Nur Karte* betrieben wird.
- **Karte und PIN:** Die Tür ist versperrt, während das Lesegerät im Modus *Karte und PIN* betrieben wird.
- **Karte oder PIN:** Die Tür ist versperrt, während das Lesegerät im Modus *Karte oder PIN* betrieben wird.
- **Zutritt verweigert:** Eine Zutrittsanforderung wird abgelehnt.
- **Zutritt erlaubt:** Eine Zutrittsanforderung wird gewährt oder die Tür wird manuell entsperrt.
- **PIN-Aufforderung:** Das System wartet darauf, dass eine PIN eingegeben wird. Dafür muss das Lesegerät im Modus *Karte und PIN* betrieben werden.
- **Aufforderung für zweiten Karteninhaber:** Das System wartet darauf, dass ein zweiter Berechtigungsnachweis vorgewiesen wird. Dies passiert, wenn eine Zwei-Personen-Regel oder eine Besucherbegleitungsregel in Kraft ist.
- **Türalarm:** Es wurde entweder der Alarm *Tür zu lange offen* oder *Öffnen der Tür erzwungen* ausgelöst.
- **Warten:** Das System wartet darauf, dass ein biometrischer Berechtigungsnachweis vorgewiesen wird oder dass ein externes System den Berechtigungsnachweid bestätigt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.

- 2 Klicken Sie auf **Konfiguration > Einstellungen für die Lesegerät-LED und den Pieper**.



- 3 Konfigurieren Sie für jeden Türstatus wie sich das Lesegerät verhalten soll:

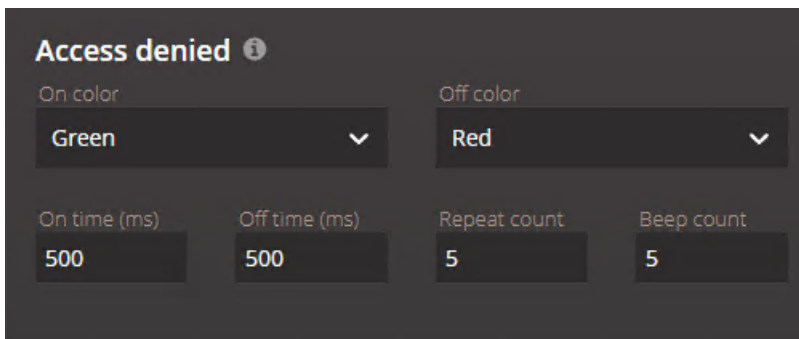
- **Farbe ein:** Die Farbe der LED, wenn die Tür zu diesem Status wechselt.
- **Zeit – ein (ms):** Die Zeit in Millisekunden, in der die LED bei der „Ein“-Farbe bleibt.
- **Farbe aus:** Die sich ändernde Farbe der LED.
- **Zeit – aus (ms):** Die Zeit in Millisekunden, in der die LED bei der „Aus“-Farbe bleibt.
- **Wiederholungsanzahl:** Wie oft die LED den Zyklus „Ein-Farbe – Aus-Farbe“ durchläuft.
- **Signaltonanzahl:** Wie oft das Lesegerät piepen sollte.

Die LED und der Pieper starten zur gleichen Zeit. Das LED-Verhalten dauert $((\text{Ein-Zeit} + \text{Aus-Zeit}) \times \text{Wiederholungsanzahl})$ Millisekunden. Dieser Verhalten wird unterbrochen, wenn die Tür zu einem anderen Status wechselt.

BEMERKUNG: Die Lautstärke und Dauer des Piepens können nicht gesteuert werden.

- 4 Klicken Sie auf **Speichern**.

- **Beispiel 1:** Damit die LED bis zu fünf Sekunden lang rot und grün blinkt und fünfmal piept, wenn der Zutritt an einer Tür verweigert wird, verwenden Sie die folgenden Einstellungen.



- **Beispiel 2:** Verwenden Sie die folgenden Einstellungen, um den Benutzer dazu aufzufordern, eine PIN einzugeben, indem Sie die LED schnell bernsteinfarben ohne Piepen blinken lassen, bis die PIN eingegeben wird.

Prompt for PIN ⓘ

On color	Off color		
Green ▼	Red ▼		
On time (ms)	Off time (ms)	Repeat count	Beep count
500	500	255	0

Die Einstellungen für die Lesegerät-LED und den Pieper von einer Einheit zu einer anderen kopieren

Sie können die LED- und Summer-Einstellungen von einer Synergis™ Cloud Link-Einheit exportieren und sie in andere Synergis™ Cloud Link-Einheiten importieren.

Bevor Sie beginnen

Konfigurieren Sie die Einstellungen für die Lesegerät-LED und den Pieper für eine erste Synergis™ Cloud Link-Einheit.

Was Sie noch wissen sollten

Die Einstellungen für die Lesegerät-LED und den Pieper sind Parameter für alle Einheiten. Derzeit werden jedoch nur von Mercury gesteuerte Lesegeräte unterstützt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an, aus der Sie kopieren möchten.
- 2 Klicken Sie auf **Konfiguration > Einstellungen für die Lesegerät-LED und den Pieper**.
- 3 Klicken Sie auf **Exportieren**.
Die Einstellungen für die LED und den Pieper werden in eine Datei namens *LedConfig<Hostname>_yyyy-mm-dd_hh_mm_ss.xml* – wobei *<Hostname>* der Hostname der Synergis™ Cloud Link-Einheit ist – in Ihrem *Downloads*-Directory gespeichert.
- 4 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an, in die Sie kopieren möchten.
- 5 Klicken Sie auf **Konfiguration > Einstellungen für die Lesegerät-LED und den Pieper**.
- 6 Klicken Sie auf **Importieren**.
Ein Dateibrowserfenster wird geöffnet.
- 7 Navigieren Sie zu Ihrem *Downloads*-Ordner, wählen Sie die gewünschte XML-Datei aus und klicken Sie auf **Öffnen**.
Die Einstellungen für die Lesegerät-LED und den Pieper werden aus der Datei gelesen und auf Ihre Synergis™ Cloud Link-Einheit angewendet.
- 8 Klicken Sie auf **Speichern**.

Ausgangssteuerungen deaktivieren

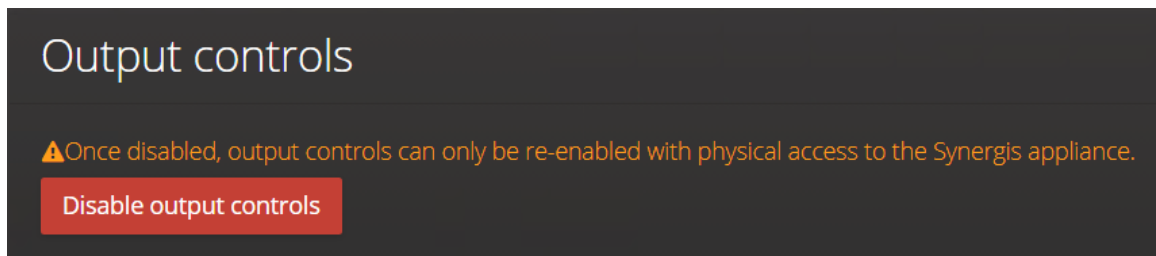
Um zu verhindern, dass Türen über das Synergis™ Appliance Portal entsperrt werden, können Sie die Steuerung von Ausgangsstatus deaktivieren.

Was Sie noch wissen sollten

- Wenn Sie Ausgangssteuerungen deaktivieren, können Sie Ausgangsstatus ansehen, sie aber nicht mehr auf der Seite *E/A-Diagnose* ändern.
- Sie können die Ausgangssteuerung nur erneut aktivieren, indem Sie einen DIP-Schalterbefehl auf der Synergis™ Cloud Link Appliance ausführen.

Prozedur

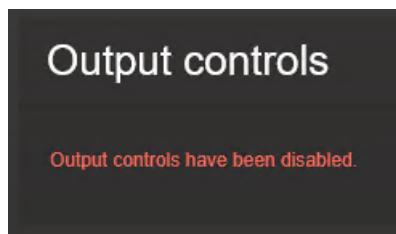
- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Parameter für die gesamte Einheit**.
- 3 Klicken Sie im Abschnitt *Ausgangssteuerungen* auf **Ausgangssteuerungen deaktivieren**.



Das Dialogfeld *Ausgangssteuerungen* erscheint und fordert Sie dazu auf, fortzufahren.

- 4 Klicken Sie auf **OK**.

Die Schaltfläche **Ausgangssteuerungen deaktivieren** verschwindet und die folgende Meldung wird angezeigt: *Ausgangssteuerungen wurden deaktiviert*.



Verwandte Themen

[DIP-Schalter-Befehlscodes](#) auf Seite 5

Informationen über die Automatisierungs-Engine

Die Automatisierungs-Engine ist eine neue Funktion in Synergis™ Software, die Regeln ausführt, ähnlich wie Event-to-Actions in Security Center. Die Automatisierungs-Engine funktioniert auch dann, wenn die Synergis™-Einheit vom Access Manager getrennt ist.

BEMERKUNG: Eine Automatisierungs-Engine-Regel generiert keine Aktion, wenn die Synergis™ Cloud Link - Einheit und ihr Downstream-Gerät nicht kommunizieren können.

Automatisierungs-Engine-Regeln sind Teil der Konfigurationsdateien der Synergis™ Cloud Link - Einheit. Es ist empfehlenswert, diese Dateien herunterzuladen, nachdem Sie die Konfiguration der Regeln abgeschlossen haben, damit Sie die Konfiguration wiederherstellen können, wenn Sie die Einheit ersetzen müssen.

Mindestanforderungen

- Synergis Cloud Link 3.0.2

BEMERKUNG: Vor Synergis Cloud Link 3.0.2 wurde die Funktion *Automatisierungs-Engine primitive Regel* genannt. Primitive Regeln, die in älteren Versionen von Synergis Cloud Link konfiguriert wurden, werden automatisch auf der Seite *Automatisierungs-Engine* im Synergis™ Appliance Portal nach einem Upgrade zu 3.0.2 oder neuer angezeigt.

Einschränkungen


Achten Sie auf die folgenden Einschränkungen der Automatisierungs-Engine-Funktion:


- Das Tool zum Kopieren der Konfiguration gilt nicht für diese Funktion.
- Das Tool zum Ersetzen von Einheiten gilt nicht für diese Funktion.
- Wenn Sie eine Tür mit aktiven Automatisierungs-Engine-Regeln löschen, werden die konfigurierten Automatisierungs-Engine-Regeln nicht gelöscht.
- Die Synergis™ Cloud Link -Einheit muss online sein, damit Sie Automatisierungs-Engine-Regeln auf der Zieleinheit konfigurieren können.
- Dezimale Werte werden für das Pulsintervall der Aktion *Ausgabe – Puls* nicht unterstützt.
- Die für einen Bereich in Security Center konfigurierte Mindestsicherheitsfreigabe überschreibt die von einer Automatisierungs-Engine-Regel aktivierte Mindestsicherheitsfreigabe.

Automatisierungs-Engine-Regeln konfigurieren

Um Aktionen auszulösen, wenn ein Zutrittskontrollereignis eintritt, konfigurieren Sie die Automatisierungs-Engine-Regeln in Synergis™ Appliance Portal . Erhöhen Sie beispielsweise die minimale Sicherheitsfreigabe für einen Bereich, wenn ein Türeingang in einen Fehlerstatus wechselt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Automatisierungs-Engine**.
- 3 Klicken Sie auf **Eine Regel hinzufügen**.
- 4 Wählen Sie im Abschnitt *Ereignis* ein auslösendes Ereignis aus der Liste aus:
 - **Lesegerät - Zutritt erlaubt**
 - **Tür - Alarm offen gehaltene Tür**
 - **Tür - Alarm erzwungene Türöffnung**
 - **Tür - Zutritt erlaubt**
 - **Tür - Zutritt verweigert**
 - **Aktualisierung des Eingangsstatus**
- 5 Geben Sie im Feld **Name** einen Namen für die Regel ein.
- 6 Abhängig vom Ereignis, das Sie ausgewählt haben, klicken Sie auf  neben dem Feld **Lesegerät, Tür** oder **Eingabe**.
- 7 Wählen Sie im Dialogfeld, das geöffnet wird, das Lesegerät, die Tür oder die Eingabe aus und klicken Sie auf **OK**.

BEMERKUNG: Wenn Sie viele Lesegeräte, Türen oder Eingänge haben, können Sie das Suchfeld oben im Dialogfeld verwenden, um mithilfe des Namens nach dem gewünschten Element zu suchen.
- 8 Wenn Sie das Ereignis *Tür - Zutritt gewährt* oder *Eingabestatus aktualisiert* ausgewählt haben, konfigurieren Sie die zusätzlichen Parameter wie folgt:
 - **Tür - Zutritt erlaubt:** (Optional) Um einer Karteninhabergruppe Zutritt zu gewähren, [rufen Sie den GUID der Karteninhabergruppe von Config Tool ab](#) und geben Sie dann den GUID im Feld **Karteninhabergruppe** ein.
 - **Aktualisierung des Eingangsstatus:** Wählen Sie einen oder mehrere Status aus, in dem sich die Eingabe befinden muss, damit die Aktion ausgelöst wird:
 - **Aktiv**
 - **Normal**
 - **Problem**
- 9 Klicken Sie im Abschnitt *Aktionen* auf **Eine Aktion hinzufügen** und wählen Sie eine der folgenden Aktionen aus der Liste aus:
 - **Ausgabe - Set**
 - **Ausgabe - gelöscht**
 - **Ausgabe - Impuls**
 - **Bereich - Sicherheitsfreigabe einrichten**
- 10 Abhängig von der Aktion, die Sie ausgewählt haben, klicken Sie auf  neben dem Feld **Ausgabe** oder **Bereich**.
- 11 Wählen Sie im Dialogfeld, das geöffnet wird, eine Ausgabe oder einen Bereich aus und klicken Sie auf **OK**.

BEMERKUNG: Wenn Sie viele Ausgänge oder Bereiche haben, können Sie das Suchfeld oben im Dialogfeld verwenden, um mithilfe des Namens nach dem gewünschten Element zu suchen.

- 12 Wenn Sie die Aktion *Ausgabe – Puls* oder *Bereich – Mindestsicherheitsfreigabe festlegen* ausgewählt haben, konfigurieren Sie die zusätzlichen Parameter wie folgt:
 - **Ausgabe – Puls:** Geben Sie im Feld **Sekunden** eine Zahl ein, um das Pulsintervall festzulegen.
 - **Bereich - Sicherheitsfreigabe einrichten:** Geben Sie im Feld **Minimum** einen Wert zwischen 1 und 7 ein, um die Mindestsicherheitsfreigabe festzulegen, die für den Zutritt zum Bereich erforderlich ist.
- 13 Konfigurieren Sie bei Bedarf weitere Aktionen.
- 14 Klicken Sie auf **Speichern**.

Nach Durchführen dieser Schritte

Laden Sie die Konfiguration Ihrer Synergis™ Cloud Link -Einheit als komprimierte Datei herunter, sodass Sie die Konfiguration der Automatisierungs-Engine-Regeln wiederherstellen können, wenn Sie die Einheit ersetzen möchten.

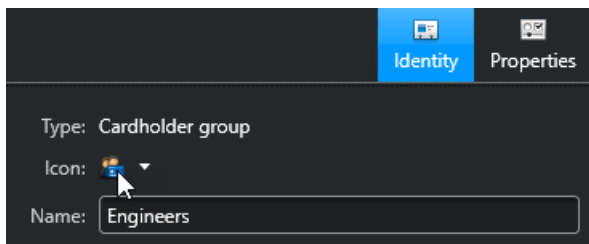
Weitere Informationen dazu finden Sie unter [Gerätekonfigurationsdatei von Ihrer Synergis Cloud Link-Einheit herunterladen](#) auf Seite 249.

Entitäts-GUIDs abrufen

Bevor Sie eine Karteninhabergruppe in einer Automatisierungs-Engine-Regel angeben können, müssen Sie den GUID (Global Unique Identifier) der Entität von Config Tool abrufen.

Prozedur

- 1 Öffnen Sie den Task *Zutrittskontrolle* auf der Startseite von Config Tool und klicken Sie auf die Ansicht **Karteninhaber und Zugangsberechtigungen**.
- 2 Wählen Sie eine Karteninhabergruppe aus der Entitätsstruktur aus.
- 3 Halten Sie auf der Seite *Identität* der Karteninhabergruppe die Steuerungstaste und führen Sie einen Doppelklick auf das Entitätssymbol aus.



Der GUID wird in Ihrer Zwischenablage gespeichert.

In diesem Video erfahren Sie mehr. Klicken Sie auf das Symbol **Untertitel (CC)**, um Videountertitel in einer der verfügbaren Sprachen einzublenden.

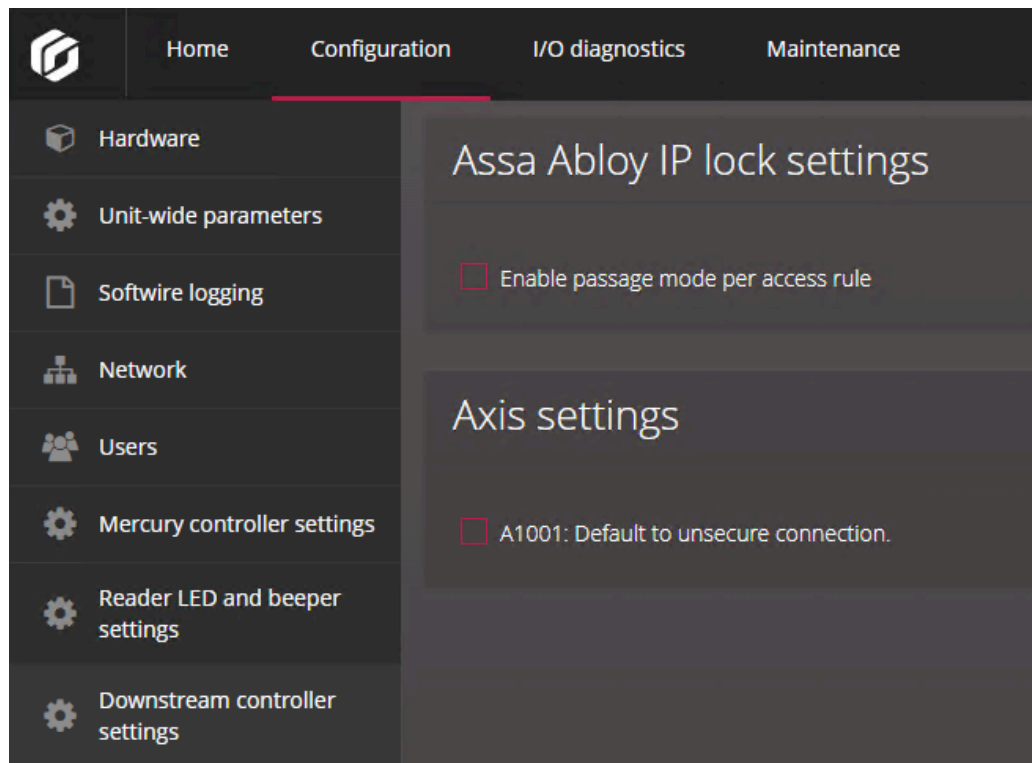


Konfigurieren der Einstellungen des nachgeschalteten Controllers

Sie können das schnittstellenmodul-spezifische Verhalten für alle an dieselbe Synergis™ Cloud Link-Einheit angeschlossenen Schnittstellenmodule auf der Seite *Einstellungen des nachgeschalteten Controllers* des Synergis™ Appliance Portals konfigurieren.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Nachgelagerte Controllereinstellungen**.



- 3 Konfigurieren Sie im Abschnitt *Assa Abloy IP-Sperreinstellungen* die folgende Option:
 - **Aktivieren des Durchgangsmodus per Zutrittsregel:** Erstellt das benutzerdefinierte Feld *PassageMode*, das für die Aktivierung der Durchgangsmodus-Funktion für Assa Abloy IP-Schlösser per Zutrittsregel erforderlich ist.
Weitere Informationen dazu finden Sie unter [Aktivieren des Durchgangsmodus an Assa Abloy-IP-Schlössern](#) auf Seite 91.
 - 4 Konfigurieren Sie im Abschnitt *Axis-Einstellungen* die folgende Option:
 - **A1001: Standard für unsichere Verbindung:** Wählen Sie diese Option aus, damit Sie mit Synergis™ Software die Firmware auf Ihrem AXIS A1001-Controller aktualisieren können, falls HTTPS nicht unterstützt wird.
 - 5 Klicken Sie auf **Speichern**.
- Alle Änderungen werden nach einem Neustart der Software wirksam.

MIFARE DESFire konfigurieren

Um MIFARE DESFire auf Ihrer Synergis™ Cloud Link-Einheit zu aktivieren, müssen Sie die Konfigurationsdatei laden und dann die Konfiguration mit Ihren transparenten STid SSCP- oder OSDP-Lesegeräten verknüpfen.

Bevor Sie beginnen

Konfigurieren Sie [STid-SSCP-Lesegeräte](#) oder [OSDP-Lesegeräte](#).

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > MIFARE DESFire**.
- 3 Klicken Sie auf **Smart-Card-Standortdatei auswählen** und navigieren Sie entweder zu Ihrer benutzerdefinierten Konfigurationsdatei (*SmartCardsSites.xml*) oder zur Standarddatei, die mit Ihrer Security Center-Installation bereitgestellt wurde.
Weitere Informationen über die Datei *SmartCardsSites.xml* finden Sie unter [MIFARE DESFire in Security Center konfigurieren](#).
- 4 Wenn Sie sichere Nachrichten mit DESFire EV2 verwenden, [aktivieren Sie diese Funktion in Ihrem System](#).
- 5 Klicken Sie auf **Hochladen**.
Die folgende Meldung wird angezeigt: *Upload erfolgreich*.
- 6 So verknüpfen Sie die Lesegeräte und MIFARE DESFire-Konfigurationen:
 - a) Wählen Sie für jedes Lesegerät einen Standort aus der Liste **Verfügbare Konfigurationen** aus.
 - b) Klicken Sie auf **Hinzufügen**.

The screenshot displays the Synergis Cloud Link configuration interface for MIFARE DESFire. The interface is divided into a sidebar and a main content area. The sidebar contains navigation options: Home, Configuration (selected), I/O diagnostics, and Maintenance. The main content area is titled "MIFARE DESFire configuration" and includes a file selection field "Select smart cards sites file" with "No file selected" and an "Upload" button. Below this is a section titled "Readers and associated MIFARE DESFire configurations" which contains a table with the following data:

Door	Reader	Available configurations	Associated configurations	Proximity Check	OSS update
Floor 1 - Main entrance	1 - 0	Site	Site	<input type="checkbox"/>	<input type="checkbox"/>
Floor 2 - Main entrance	2 - 1	Site	No configurations are associated with this reader	<input type="checkbox"/>	<input type="checkbox"/>

Below the table is a section titled "MIFARE DESFire versioning" with a checkbox for "Use key version". A note at the bottom states: "For keys stored in the Synergis key store, the latest read key version will be used."

- 7 Wenn Ihr System Schlüsselversionierung verwendet, aktivieren Sie das Kontrollkästchen **Schlüsselversionierung verwenden**.

Zwei Szenarios müssen in Betracht gezogen werden:

- **Schlüssel werden im Synergis-Schlüsselspeicher gespeichert:** Wenn das Kontrollkästchen ausgewählt ist, fragt das System die Karte, welche Schlüsselversion sie verwendet und versucht, sie im Schlüsselspeicher zu finden. Wenn das Kontrollkästchen deaktiviert ist, verwendet das System immer die letzte Version. Weitere Informationen dazu finden Sie unter [Informationen über den Synergis™ key store](#) auf Seite 50.
- **Schlüssel werden auf der SAM-Karte gespeichert:** Wenn das Kontrollkästchen ausgewählt ist, fragt das System die Karte, welche Schlüsselversion sie verwendet und versucht, sie auf der SAM-Karte zu finden. Wenn das Kontrollkästchen deaktiviert ist, verwendet das System immer die Schlüsselversion 0. Weitere Informationen finden Sie unter [Schlüsselversionierung für SAM-Karten aktivieren](#) auf Seite 49.

- 8 Klicken Sie auf **Speichern**.

Verwandte Themen

[Konfigurieren und Registrieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden](#) auf Seite 231

[Konfigurieren und Hinzufügen von OSDP-Lesegeräten im Synergis™ Appliance Portal](#) auf Seite 221

Sichere Nachrichten mit DESFire EV2 aktivieren

Um sichere Nachrichten mit DESFire EV2 zu verwenden, müssen Sie die EV2-Authentifizierung bei Ihren DESFire-Konfigurationsdateien aktivieren und sie zu Ihren Workstations und Synergis™ Cloud Link-Einheiten exportieren.

Bevor Sie beginnen

[Konfigurieren Sie MIFARE DESFire in Security Center](#) und [exportieren Sie Ihre Konfiguration als XML-Datei](#).

Was Sie noch wissen sollten

Die DESFire-Konfigurationsdatei (*SmartCardsSites.xml*) wird in Config Tool mithilfe des Tasks *Konfiguration von MIFARE DESFire* erstellt. Derzeit unterstützt dieser Task den EV2-Authentifizierungsmodus nicht. Daher müssen Sie die Einstellung in der exportierten XML-Datei manuell ändern.

Prozedur

- 1 Öffnen Sie mithilfe eines Textbearbeitungsprogramms Ihre benutzerdefinierte *SmartCardsSites.xml*-Datei.
- 2 Suchen Sie den Tag `<AuthenticationMode>` am Ende jeder Konfiguration und ersetzen Sie „EV1“ durch „EV2“.

```
<AuthenticationMode>
  <EV2 />
</AuthenticationMode>
```

- 3 Speichern Sie Ihre Änderungen und schließen Sie die Datei.
- 4 Importieren Sie mithilfe von Config Tool die bearbeitete *SmartCardsSites.xml*-Datei mit dem Task *Konfiguration von MIFARE DESFire*.
- 5 [Exportieren Sie die neue MIFARE-DESFire-Konfiguration in Ihre Workstations und Synergis™ Cloud Link-Einheiten](#).

SAM-Karten entsperren

Das Speichern kryptografischer Schlüssel auf Karten des Typs MIFARE Secure Access Module (SAM) statt auf dem Synergis™ Key Store erhöht die Sicherheit, da die Schlüssel nicht abgerufen werden können. Die SAM-Karten müssen entsperrt sein, um mit Synergis™ Cloud Link für kryptografische Vorgänge interagieren zu können.

Bevor Sie beginnen

- Konfigurieren Sie eine [Synergis™ Cloud Link 312](#)-Einheit.
BEMERKUNG: Sie benötigen eine Synergis-Cloud-Link-312-Einheit, um die SAM-Kartenschlüssel zu speichern. Weitere Informationen über die Vorbereitung von Synergis Cloud Link 312 finden Sie unter [SAM-Karten auf einem Synergis Cloud Link 312 installieren](#).
- Konfigurieren Sie SAM-Karten mit einem SAM-Produktionstool und installieren Sie bis zu drei Karten.
BEMERKUNG: Wenn Sie mehr als eine SAM-Karte installieren, müssen die Karten dieselben Schlüssel haben. Wenn mehrere SAM-Karten installiert sind, können Karten schneller gelesen und Entscheidungen betreffend den Zutritt für Einheiten mit vielen Zugriffskontrollaktivitäten schneller getroffen werden.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link 312-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Synergis™ key store**.
- 3 Klicken Sie oben in der Schlüsselliste auf **+**.
- 4 Führen Sie im Dialogfeld *Neue Version erstellen* die folgenden Schritte aus:

- a) Wählen Sie **SAM-Host-Authentifizierung** aus.
- b) Geben Sie im Feld **Komponenten** die Host-Authentifizierungsschlüssel ein, die Sie im SAM-Produktions-Tool konfiguriert haben, und klicken Sie auf **Hinzufügen**.
- c) Klicken Sie auf **OK**.

- 5 Klicken Sie auf **Konfiguration > SAM-Karte**.

The screenshot displays the Synergis™ Cloud Link Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'I/O diagnostics', and 'Maintenance'. The left sidebar lists various configuration options, with 'SAM card' selected at the bottom. The main content area is divided into two sections:

- SAM card host authentication configuration:** This section contains a warning icon and text: "Refer to the Synergis™ key store to enter the SAM host authentication." Below this are two input fields: "Key number" and "Key version", both containing the value "0".
- SAM controller status:** This section shows the "Controller version: 2.3.34" and the status of three SAM cards:
 - SAM card 1: No SAM card inserted (grey circle)
 - SAM card 2: OK (green circle)
 - SAM card 3: No SAM card inserted (grey circle)
 A "Refresh" button is located below the status list.

- 6 Geben Sie im Abschnitt *SAM-Host-Authentifizierungskonfiguration* die Schlüsselnummer und die Schlüsselversion des auf der SAM-Karte gespeicherten Host-Authentifizierungsschlüssels ein.
- 7 Überprüfen Sie im Abschnitt *SAM-Steuerungsstatus*, ob die SAM-Karten korrekt eingelegt und konfiguriert wurden.
- Es können bis zu drei SAM-Karten installiert sein. Jeder Erweiterungsslot kann einen der folgenden Status haben:
- **OK:** Eine SAM-Karte wurde eingelegt und der Host-Authentifizierungsschlüssel, die Schlüsselnummer und die Versionsnummer sind gültig.
 - **SAM-Kartenentsperrung fehlgeschlagen:** Eine SAM-Karte wurde eingelegt, aber der Host-Authentifizierungsschlüssel, die Schlüsselnummer oder die Versionsnummer stimmen nicht mit jenen auf der Karte überein.
 - **Keine SAM-Karte eingelegt:** Im Erweiterungsslot gibt es keine SAM-Karte.

Nach Durchführen dieser Schritte

Registrieren Sie STid- oder OSDP-Lesegeräte oder konfigurieren Sie registrierte Lesegeräte.

Verwandte Themen

[Schlüsselversionierung für SAM-Karten aktivieren](#) auf Seite 49

[Informationen zu Synergis™ Cloud Link 312](#) auf Seite 6

Schlüsselversionierung für SAM-Karten aktivieren

Um Versionen von Anwendungsleseschlüsseln mit Ihren MIFARE SAM-Karten zu verwenden, müssen Sie die Karten mithilfe eines SAM-Kartenkonfigurationstools mit bis zu drei Schlüsseln konfigurieren und dann die Schlüsselversionierung im Synergis™ Appliance Portal aktivieren.

Bevor Sie beginnen

- Konfigurieren Sie Ihre SAM-Karten mit bis zu drei Schlüsseln mit einem SAM-Produktionstool.
- Installieren Sie die SAM-Karten auf einer Synergis™ Cloud Link-312-Einheit. Weitere Informationen finden Sie unter [SAM-Karten auf einem Synergis Cloud Link 312 installieren](#).

Was Sie noch wissen sollten

Standardmäßig unterstützt Security Center nicht SAM-Karten mit anderen Anwendungsleseschlüsselversionen als 0. Durch Aktivieren der Schlüsselversionierung können vorcodierte Karten mit anderen Schlüsselversionen als 0 verwendet werden. Die Funktion funktioniert mit OSDP- und SSCP-Protokollen und bietet Administratoren, die ihre Schlüsselversion regelmäßig erhöhen möchten, Flexibilität bei der Schlüsselverwaltung.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link 312-Einheit an.
- 2 Klicken Sie auf **Konfiguration > MIFARE DESFire**.
- 3 Wählen Sie im Abschnitt *MIFARE-DESFire-Versionierung* das Kontrollkästchen **Schlüsselversion verwenden** aus.
Wenn das Kontrollkästchen ausgewählt ist, fragt das System die Karte, welche Schlüsselversion sie verwendet und versucht, sie auf der SAM-Karte zu finden. Wenn das Kontrollkästchen deaktiviert ist, verwendet das System immer die Schlüsselversion 0.
- 4 Klicken Sie auf **Speichern** und starten Sie die Einheit dann neu.

Verwandte Themen

[SAM-Karten entsperren](#) auf Seite 46

[Informationen zu Synergis™ Cloud Link 312](#) auf Seite 6

Informationen über den Synergis™ key store

Der Synergis™ key store wird verwendet, um kryptografische Schlüssel zu konfigurieren und zu speichern.

Schlüssel im Synergis™ key store

Jeder kryptografische Schlüssel besteht aus einer oder mehreren Komponenten. Für zusätzliche Sicherheit kann ein Schlüssel aus mehreren Komponenten bestehen, sodass der Schlüssel getrennt und an mehrere Beteiligte verteilt werden, sodass niemand den vollständigen Schlüssel hat.

Im Synergis™ key store werden für jeden Schlüssel die Version, aktuelle Anzahl von Komponenten und der Hash aufgelistet.

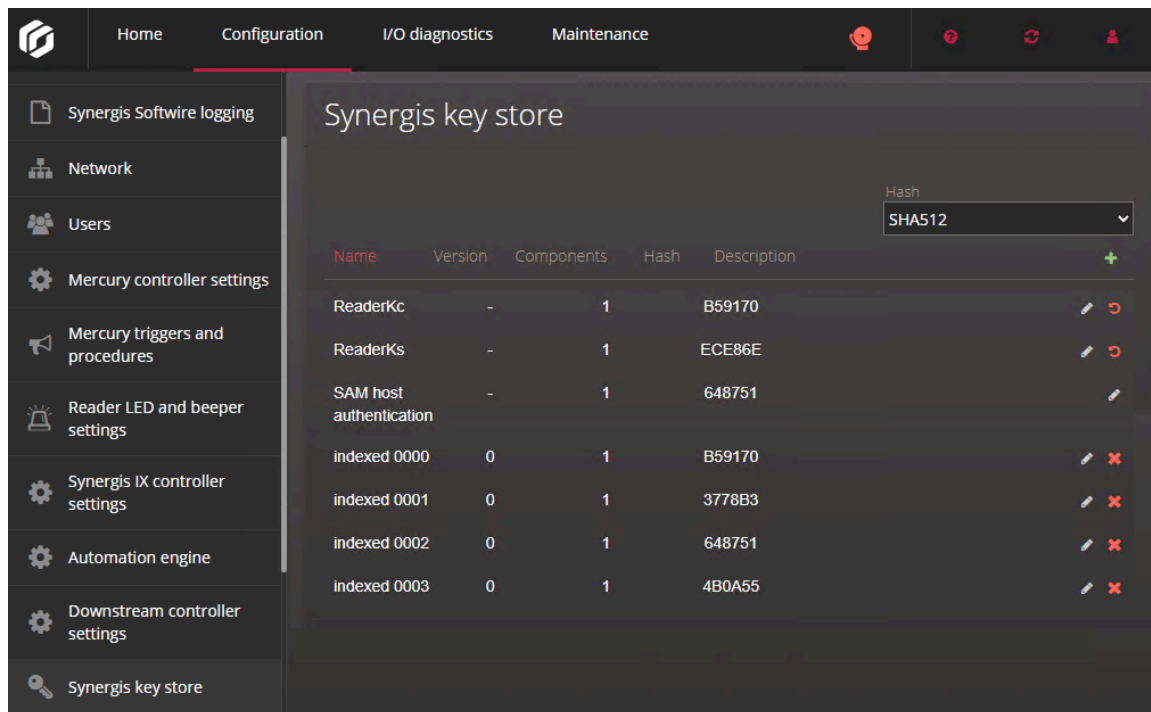
- **Version:** Die Versionsnummer des Schlüssels. Jede Version des Schlüssels, die Sie erstellen, ist ein neuer Schlüssel.

Mehrere Versionen des gleichen Schlüssels werden aufgelistet, wenn das Kontrollkästchen **Schlüsselversion verwenden** auf der [MIFARE-DESFire-Konfigurationsseite](#) aktiviert ist. Wenn das Kontrollkästchen ausgewählt ist, fragt das System die Karte, welche Schlüsselversion sie verwendet und versucht, sie im Schlüsselspeicher zu finden. Die indizierten Schlüssel 00 bis 31 können bis zu drei Versionen gleichzeitig haben. Wenn das Kontrollkästchen deaktiviert ist, verwendet das System immer die letzte Version.

Wenn Sie beispielsweise Schlüsselversionierung aktivieren und dann die Versionen 1, 2 und dann 3 für den indizierten 01-Schlüssel hinzufügen, danach das Kontrollkästchen deaktivieren, wird nur die Version 3 im Synergis-Schlüsselspeicher für diesen Schlüssel aufgelistet. Wenn Sie Version 4 erstellen und das Kontrollkästchen dann noch einmal auswählen, werden die Versionen 2, 3 und 4 aufgelistet.

BEMERKUNG: Die ReaderKc-, ReaderKs- und SAM-Host-Authentifizierungsschlüssel unterstützen keine Schlüsselversionierung. Die neuesten Änderungen werden automatisch inkrementiert.

- **Komponenten:** Die Anzahl der Komponenten, die derzeit den Schlüssel bilden. Jede Komponente ist ein hexadezimaler Wert, der aus 32 Zeichen besteht.
- **Hash:** Der Schlüssel-Hash, der verwendet wird, um zu verifizieren, ob der von Ihnen im Synergis-Schlüsselspeicher eingegebene Schlüssel gültig ist. Der Schlüssel ist gültig, wenn er dem Schlüssel-Hash von anderen Einheiten, der SAM-Karte oder dem Schlüsselkartenproduktionstool, mit dem Sie vergleichen möchten, entspricht. Weitere Informationen dazu finden Sie unter [Schlüssel-Hashes im Synergis™ key store verwenden](#) auf Seite 52.



Kryptografische MIFARE-DESFire-Schlüssel können von Security Center zu einer oder mehreren Synergis™ Cloud Link-Einheiten in Ihrem System exportiert werden. Die Schlüssel werden dann automatisch auf der Seite *Synergis-Schlüsselspeicher* vom Synergis™ Appliance Portal aktualisiert. Weitere Informationen finden Sie unter [MIFARE-DESFire-Schlüssel zu Synergis-Cloud-Link-Einheiten exportieren](#).

Anwendungsfälle für die unterschiedlichen Schlüssel

Jeder Schlüsseltyp im Synergis™ key store wird in einem bestimmten Kontext verwendet:

- **ReaderKc und ReaderKs:** Wird für die Konfiguration von Kommunikationsschlüsseln für STid-Lesegeräte verwendet. Weitere Informationen dazu finden Sie unter [Ändern der Standardkommunikationsschlüssel RS-485 für STid-Lesegeräte, die das SSCP-Protokoll verwenden](#) auf Seite 238.
- **SAM-Host-Authentifizierung:** Wird zum Entsperren von SAM-Karten verwendet, sodass Sie die darauf gespeicherten kryptografischen Schlüssel verwenden können. Weitere Informationen dazu finden Sie unter [SAM-Karten entsperren](#) auf Seite 46.
- **Indiziert 00 - 31:** Wird verwendet, um kryptografische Schlüssel zu erstellen, um auf die gesicherte Berechtigung der MIFARE-DESFire-Karte zuzugreifen. Weitere Informationen siehe [Aktivieren des transparenten Modus bei STid-Lesegeräten, die das SSCP-Protokoll verwenden](#) auf Seite 235 und [MIFARE DESFire für transparente OSDP-Lesegeräte aktivieren](#) auf Seite 224.

Schlüssel-Hashes im Synergis™ key store verwenden

Sie können Schlüssel-Hashes verwenden, um Schlüssel im Synergis™-Schlüsselspeicher und anderen Einheiten abzugleichen. Alternativ können Sie sie anhand der SAM-Karte oder des Schlüsselkarten-Produktionstools, mit dem die Schlüssel erstellt wurden, prüfen.

Was Sie noch wissen sollten

Schlüssel, die im Synergis-Schlüsselspeicher gespeichert wurden, können nicht abgerufen werden. Sie können jedoch mithilfe von Schlüssel-Hashes überprüft werden.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Synergis-Schlüsselspeicher**.
- 3 Wählen Sie aus der Liste **Hash** den Algorithmus aus, der vom Kartentool eines Drittanbieters oder der Synergis™ Cloud Link-Einheit verwendet wurde:
 - **KCV**: Schlüsselprüfsummenwert
 - **SHA1**: Secure-Hash-Algorithmus 1
 - **SHA256**: 256-Bit-Version des Secure Hash-Algorithmus 2
 - **SHA384**: 384-Bit-Version des Secure Hash-Algorithmus 2
 - **SHA512**: 512-Bit-Version des Secure Hash-Algorithmus 2

In der Spalte **Hash** wird ein Schlüssel-Hash mit 6 Zeichen (24 Bit) unabhängig vom verwendeten Algorithmus angezeigt.

- 4 Verifizieren Sie, dass der Schlüssel-Hash im Synergis™ key store der gleiche Schlüssel-Hash wie von den anderen Einheiten, der SAM-Karte oder dem Schlüsselkartenproduktionstool ist, mit dem Sie vergleichen möchten.
- 5 Verifizieren Sie, dass der Schlüssel-Hash im Synergis™ key store der gleiche Schlüssel-Hash wie von den anderen Einheiten, der SAM-Karte oder dem Schlüsselkartenproduktionstool ist, mit dem Sie vergleichen möchten.



Zeitlimit für die PIN-Eingabe für Türen ändern

Wenn lange PINs verwendet werden, können Sie das Zeitlimit für die PIN-Eingabe ändern, damit Karteninhaber mehr Zeit für die Eingabe ihrer PINs haben.

Was Sie noch wissen sollten

Das Standardzeitlimit beträgt 5 Sekunden.

Prozedur

- 1 Verbinden Sie Security Center mit Config Tool.
- 2 Wählen Sie im Task *Bereichsansicht* die Tür aus, für die ein längeres Zeitlimit für die PIN-Eingabe erforderlich ist.
- 3 Klicken Sie auf die Registerkarte **Hardware**.
- 4 Klicken Sie neben dem der Tür zugewiesenen *Karten- und PIN-Lesegerät* auf **Lesegeräteinstellungen** .
- 5 Aktivieren Sie im Dialogfeld *Lesegeräteinstellungen* die Option **Karte und PIN verwenden**, sofern diese noch nicht aktiviert ist.
- 6 Stellen Sie das **Zutrittszeitlimit** ein und klicken Sie dann auf **Speichern > OK**.
- 7 Wenn die gewünschte Einstellung *Karte oder PIN* lautet, gehen Sie wie folgt vor:
 - a) Klicken Sie auf **Lesegeräteinstellungen**  und deaktivieren Sie **Karte und PIN verwenden**.
 - b) Klicken Sie auf **Speichern**.
- 8 Klicken Sie auf **Anwenden**.

Konfigurieren der Ereignisprotokollierung auf der Synergis™ Cloud Link -Einheit

Die Synergis™ Cloud Link -Einheit kann detaillierte Protokolle für Problembehandlung und Support speichern. Diese Protokolle sind jedoch standardmäßig deaktiviert. Aktivieren Sie sie, wenn Sie die Fehlerbehebungsberichte anzeigen oder Supportprotokolle herunterladen möchten.

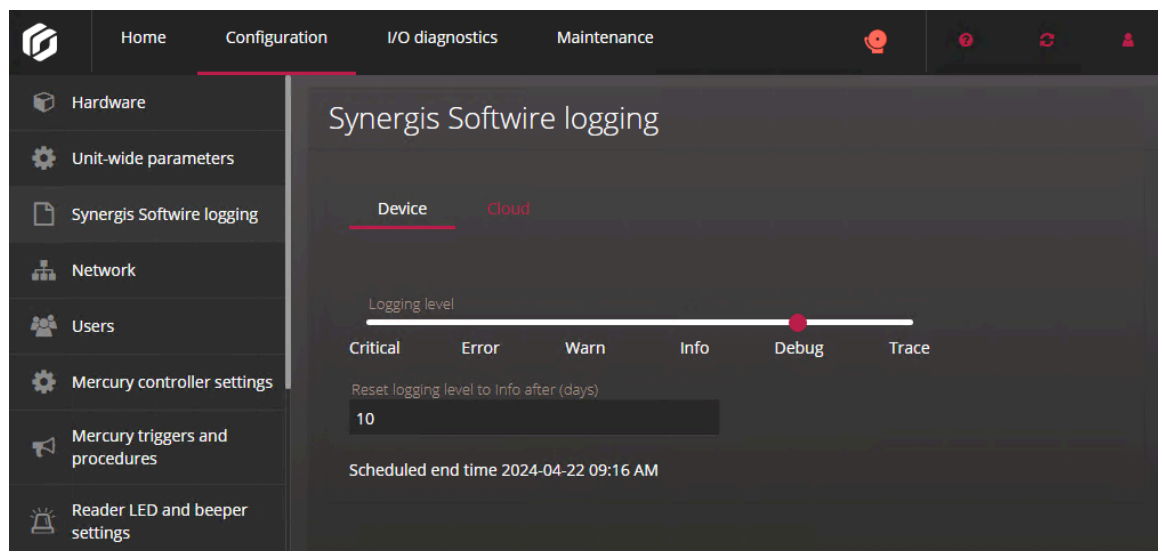
Was Sie noch wissen sollten

- Aktivieren Sie die Protokollierung nur, wenn Sie vom Genetec™ Technical Support dazu aufgefordert werden.
- *Kritische* Fehler werden unabhängig von der konfigurierten Protokollierungsstufe immer in Protokolle geschrieben.
- Sie können die Protokolle auf der Seite *Diagnoseprotokolleherunterladen* im Synergis™ Appliance Portal herunterladen.
- Sie können auch [konfigurieren, dass Protokolle über Azure Application Insights in der Cloud gespeichert werden](#).

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Konfiguration > Synergis.Softwire-Protokollierung**.
- 3 Wählen Sie im Abschnitt *Synergis-Softwire-Protokollierung* einen **Protokollierungsgrad** aus.
- 4 Wenn Sie als Protokollierungsebene **Debuggen** oder **Verfolgen** auswählen, geben Sie in das Feld **Protokollierungsebene auf Info nach (Tagen) zurücksetzen** die Anzahl der Tage ein, für die Sie Protokolle der gewählten Protokollierungsebene sammeln möchten.

Beispiel: Wenn Sie **Debug** als Protokollierungsebene auswählen und **10** in das Feld **Protokollierungsebene auf Info nach (Tagen) zurücksetzen** eingeben, werden *Kritisch*, *Fehler*, *Warnung*, *Info* und *Debug* zehn Tage lang protokolliert. Nach zehn Tagen werden nur die Protokolle *Kritisch*, *Fehler*, *Warnung* und *Info* gesammelt.



- 5 Klicken Sie auf **Speichern**.

Konfigurieren der zusätzlichen Ereignisprotokollierung in der Cloud für die Synergis™ Cloud Link -Einheit

Konfigurieren Sie Ihre Synergis™ Cloud Link -Einheit so, dass sie sich mit einer Azure Application Insights-Ressource verbindet, sodass Protokolle nicht nur auf der Einheit selbst, sondern auch in der Cloud gespeichert werden können. Dies kann die Analyse von Protokollen und die Ausführung von Überwachungstools vereinfachen.

Bevor Sie beginnen

Sie müssen eine Application Insights-Ressource erstellt und konfiguriert haben.

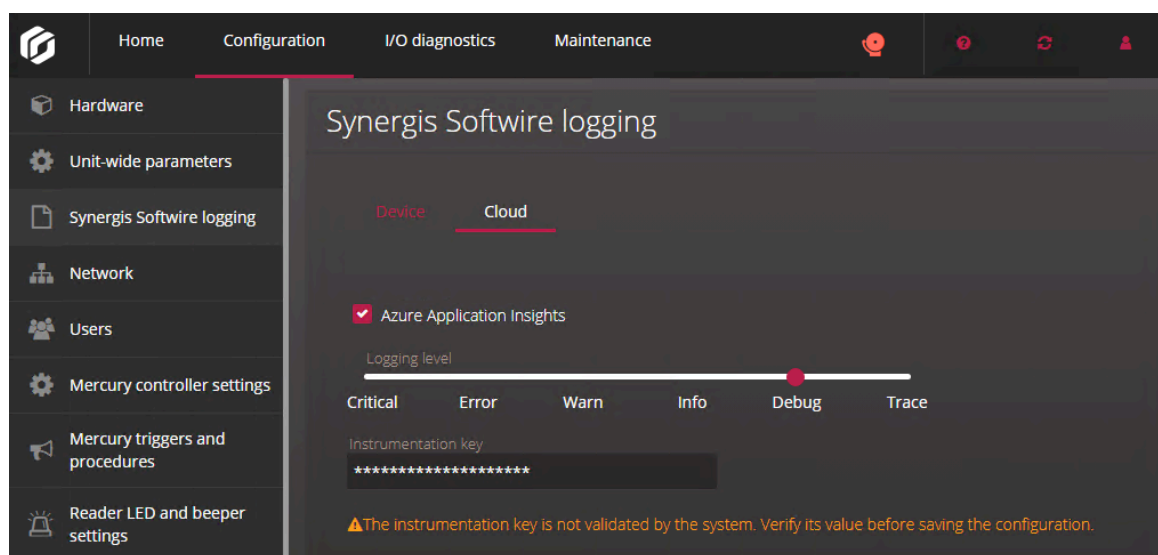
Was Sie noch wissen sollten

- Die Synergis™ Cloud Link -Einheit verbindet sich über den **Instrumentierungsschlüssel** der Application Insights-Ressource mit der Ressource.
- Sie können den Instrumentierungsschlüssel verwenden, um mehrere Synergis™ Cloud Link -Einheiten mit der gleichen Application Insights-Ressource zu verbinden.
- Sie können verschiedene Protokollierungsstufen für die auf der Synergis™ Cloud Link -Einheit und in der Cloud gespeicherten Protokolle konfigurieren.

Beispiel: Zur Platzzeinsparung auf dem Gerät können Sie das Gerät so konfigurieren, dass nur *kritische* Protokolle gespeichert werden und alle anderen Protokolle an die Cloud gesendet werden.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Synergis.Softwire-Protokollierung**.
- 3 Klicken Sie im Abschnitt *Synergis-Softwire-Protokollierung* auf die Ansicht **Cloud**, und wählen Sie dann **Azure Application Insights** aus.
- 4 Wählen Sie eine **Protokollierungsebene** aus.
- 5 Geben Sie in das Feld **Instrumentierungsschlüssel** den Instrumentierungsschlüssel der Application Insights-Ressource ein, an die Sie Protokolle senden möchten.



- 6 Klicken Sie auf **Speichern**.

Die Aufbewahrungszeit von Überwachungsprotokollen für die Synergis™ Cloud Link -Einheit konfigurieren

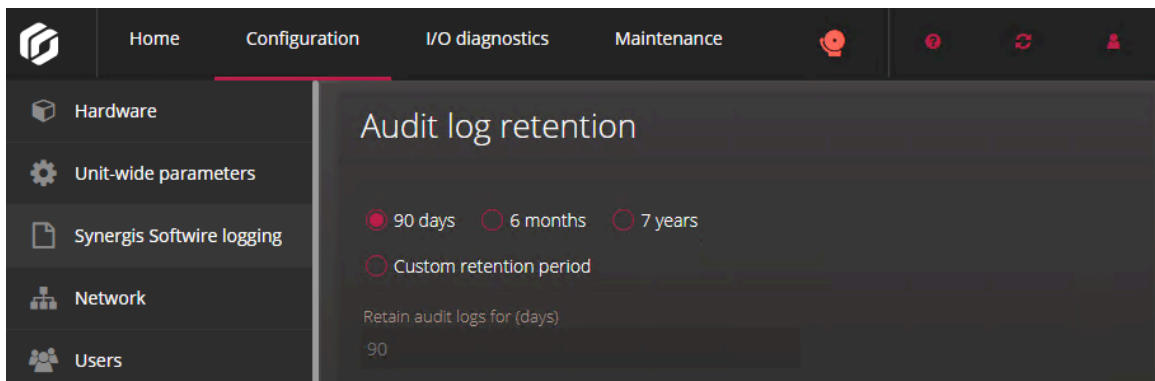
Sie können konfigurieren, wie lange die Überwachungsprotokolle für die Synergis™ Cloud Link -Einheit aufbewahrt werden sollen, bis sie automatisch gelöscht werden.

Was Sie noch wissen sollten

- Überwachungsprotokolle werden standardmäßig 90 Tage lang aufbewahrt.
- Überwachungsprotokolle können nur vom Admin-Benutzer auf der Seite *Diagnostikprotokolle herunterladen* des Portals heruntergeladen werden.
- Folgendes wird protokolliert:
 - Erfolgreiche und nicht erfolgreiche Anmeldeversuche des Benutzers, Änderungen des Benutzerpassworts und Benutzersperren, die nach drei fehlgeschlagenen Anmeldeversuchen auftreten.
 - Konfigurationsänderungen im Synergis™ Appliance Portal .
BEMERKUNG: Änderungen, die auf den Seiten *Hardware* und *Netzwerk* durchgeführt werden, werden nicht protokolliert.
 - DIP-Schalterbefehle werden auf der Synergis™ Cloud Link -Appliance ausgeführt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Konfiguration > Synergis.Softwire-Protokollierung**.
- 3 Legen Sie im Abschnitt *Aufbewahrung von Überwachungsprotokollen* eine Aufbewahrungszeit fest:



- **90 Tage**
 - **6 Monate**
 - **7 Jahre**
 - **Benutzerdefinierte Aufbewahrungsfrist:** Geben Sie einen Wert zwischen 2 und 2557 ein, um die Anzahl von Tagen für die Aufbewahrungsfrist festzulegen.
- 4 Klicken Sie auf **Speichern**.

Synergis™ Cloud Link-Einheiten in Security Center registrieren

Um eine Synergis™ Cloud Link-Einheit in Security Center zu registrieren, weisen Sie die Einheit einer Access Manager-Rolle zu.

Bevor Sie beginnen

Konfigurieren Sie die Netzwerkeigenschaften der Synergis™ Cloud Link-Einheit.

Was Sie noch wissen sollten

Wenn Sie eine Access Manager-Rolle erstellen, wird die Synergis™-Erweiterung automatisch hinzugefügt. Die Erweiterung wird mit dem Standard-Erkennungsport 2000 erstellt. Wenn Sie einen anderen Port in den Netzwerkeigenschaften der Einheit konfiguriert haben, müssen Sie ihn auch in Config Tool ändern, damit er übereinstimmt.

BEST-PRACTICE: Wenn Sie mehrere Access Manager-Rollen haben, die Synergis-Einheiten auf dem gleichen Subnetz steuern, sollten Sie dafür sorgen, dass diese verschiedene Erkennungsports nutzen. Ansonsten könnte es zu Leistungsproblemen kommen.

Prozedur

- 1 Wenn die Einheit nicht den standardmäßigen Erkennungsport verwendet, ändern Sie den Erkennungsport der Synergis™-Erweiterung, damit dieser mit dem auf Ihrer Einheit konfigurierten Port übereinstimmt:
 - a) Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
 - b) Wählen Sie den Access Manager aus und klicken Sie dann auf die Registerkarte **Erweiterungen**.
 - c) Wählen Sie die Synergis™-Erweiterung aus.
 - d) Wählen Sie den Erkennungsport aus und klicken Sie auf **Das Element bearbeiten** (✎).
 - e) Geben Sie im Dialogfeld *Erkennungsport* die Portnummer ein, die für Ihre Einheit konfiguriert ist, und klicken Sie auf **Speichern**.
- 2 [Fügen Sie die Synergis™-Einheit der Access Manager-Rolle hinzu.](#)

Synergis™ Cloud Link-Einheiten zu einer Access Manager-Rolle hinzufügen


Um in Ihrem Standort den Zutritt zu gesicherten Bereichen zu kontrollieren und in Security Center Ereignisse bei der Zutrittskontrolle zu überwachen, müssen Sie Zutrittskontrollleinheiten zu einer Access Manager-Rolle hinzufügen.

Bevor Sie beginnen

Stellen Sie sicher, dass der Erkennungsport für die Synergis™-Erweiterung der Portnummer auf Ihrer Einheit entspricht.

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Klicken Sie auf **Zutrittskontrollleinheit** (+).
- 3 Klicken Sie im Dialogfeld *Einheit erstellen* auf **Einheitentyp** und wählen Sie **Synergis** aus.

- 4 Geben Sie im Abschnitt *Netzwerkendpunkt* den Hostnamen oder die IP-Adresse der Einheit sowie den Admin-Benutzernamen und das Passwort ein.
- 5 Wenn Sie eine Portweiterleitung benötigen, klicken Sie auf **Erweiterte Einstellungen** und geben Sie die Basis-URL in das Feld **Webadresse** ein.
- 6 Klicken Sie auf **Weiter**.
- 7 Wählen Sie eine **Partition** aus, auf der die Zutrittskontrolleinheit hinzugefügt werden soll, und klicken Sie auf **Weiter**.
Partitionen bestimmen, welche Security Center-Benutzer Zugriff auf diese Einheit haben. Nur autorisierte Benutzer der Partition können die Zutrittskontrolleinheit anzeigen oder verändern.
- 8 Prüfen Sie das Fenster *Zusammenfassung des Anlegens* und klicken Sie auf **Erstellen**.
Der Access Manager versucht, sich mit der Einheit zu verbinden und registriert sie in Ihrem System. Wenn der Vorgang erfolgreich abgeschlossen wurde, wird eine Bestätigungsmeldung angezeigt.
- 9 Klicken Sie auf **Schließen** und dann auf **Aktualisieren** .
Die neu hinzugefügte Einheit wird unter dem Access Manager angezeigt, dem sie in der Ansicht **Rollen und Einheiten** zugeordnet wurde. Der Standardeinheitsname ist der Hostname der Einheit. Von nun an reagiert diese Einheit nur noch auf die von diesem Access Manager ausgegebenen Befehle.
BEMERKUNG: Wenn Sie später die Verbindungsparameter auf der Einheit ändern, müssen Sie den Access Manager darüber benachrichtigen, indem Sie die [Einheit mit dem Access Manager synchronisieren](#).
- 10 Wenn dieses Gerät als Peer mit anderen Geräten verbunden werden muss, fügen Sie es der entsprechenden Peer-Gruppe hinzu. Weitere Informationen finden Sie unter [Aktivieren von Peer-to-Peer in der Access-Manager-Rolle](#).

Synergis™ Cloud Link-Einheiten zu einem gehosteten SaaS Access Manager hinzufügen

Durch Hinzufügen einer Synergis™-Cloud-Link-Einheit zu Ihrem Access Manager kann diese Einheit sichere Verbindungen zu einer von Security Center SaaS Edition (Classic) gehosteten Bereitstellung aktivieren.

Bevor Sie beginnen

- [Stellen Sie sicher, dass der DNS und andere Netzwerkeinstellungen der Einheit konfiguriert sind.](#)
- [Ändern Sie das Standardpasswort für die Einheit.](#)
- Stellen Sie sicher, dass die Synergis™-Cloud-Link-Einheit über eine Internetverbindung verfügt.

Gehen Sie zu <https://<SCL IP address>/CloudAgent> und melden Sie sich im Synergis™-SaaS-Agent-Portal mit dem gleichen Benutzernamen und Passwort an, die Sie zum Anmelden im Synergis™ Appliance Portal verwenden. Der Verbindungsstatus ist auf der Seite *Aktivierung* der Einheit zu finden. Wenn Ihr lokales Netzwerk das Internet nur über einen Proxy-Server erreichen kann, geben Sie die Proxy-URL an und optional den Benutzernamen und das Passwort auf der Seite *Proxy*.

- Stellen Sie sicher, dass sich Ihre Config Tool-Workstation im selben Netzwerk befindet wie Ihre Synergis™ Cloud Link-Einheit.



Was Sie noch wissen sollten

Bei allen Synergis™ Cloud Link-Einheiten der nächsten Generation ist Cloud Agent vorab installiert. Cloud Agent ist ein separates Softwaremodul, das eine sichere Verbindung zur Cloud herstellt. Wenn die Einheit unter einem gehosteten SaaS Access Manager registriert ist, ist die Cloud-Verbindung aktiviert.


Prozedur

So fügen Sie eine Synergis™-Cloud-Link-Einheit zu einem gehosteten SaaS Access Manager hinzu:

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.

- 2 Klicken Sie auf **Zutrittskontrolleinheit** .
 - 3 Klicken Sie im Dialogfeld *Einheit erstellen* auf **Einheitentyp** und wählen Sie **Synergis™ SaaS** aus.
 - 4 Geben Sie im Bereich **Netzwerkendpunkt** den Hostnamen oder die IP-Adresse der Einheit ein und klicken Sie dann auf **Überprüfen**.
Das System überprüft die Synergis™ Cloud Link-Einheit und zeigt die MAC-Adresse der Einheit an.
 - 5 Geben Sie den Admin-Benutzernamen und das Passwort ein.
Der Standardbenutzername lautet `admin`. Ändern Sie das Standardpasswort, um die Einheit zu registrieren.
 - 6 Prüfen Sie das Fenster *Zusammenfassung des Anlegens* und klicken Sie auf **Erstellen**.
Config Tool sendet die Informationen der Synergis™ Cloud Link-Einheit an den Access Manager, der sie an das SaaS-Gateway weiterleitet. Wenn die Einheit mit dem SaaS-Gateway verbunden ist, wird eine Bestätigungsmeldung angezeigt.
 - 7 Klicken Sie auf **Schließen** und dann auf **Aktualisieren** .
- Die neu hinzugefügte Zutrittskontrolleinheit erscheint unter dem Access Manager, dem sie in der Ansicht **Rollen und Einheiten** zugeordnet wurde. Der Standardeinheitenname ist der Hostname der Synergis™ Cloud Link-Einheit. Diese Einheit reagiert jetzt nur noch auf die von diesem Access Manager ausgegebenen Befehle.

So löschen Sie eine Synergis™-Cloud-Link-Einheit von einem gehosteten SaaS Access Manager:

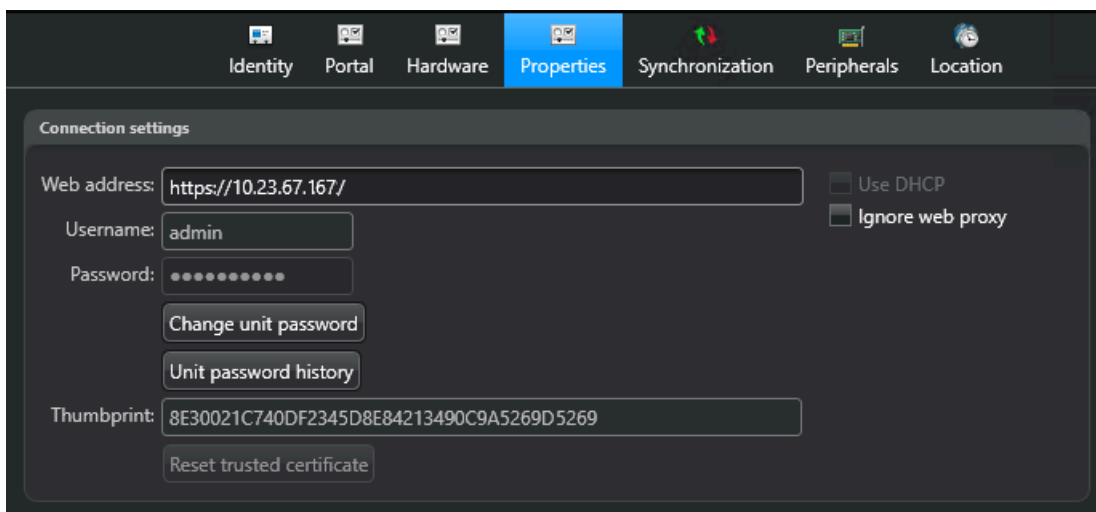
- 1 Wählen Sie in der Ansicht **Rollen und Einheiten** die Synergis™ Cloud Link-Einheit aus dem Einheitendiagramm aus.
- 2 Klicken Sie auf **Löschen** .
- 3 Klicken Sie in dem Bestätigungsdialogfeld auf **Löschen**.

Die Synergis™ Cloud Link-Einheit mit dem Access Manager synchronisieren

Einige Einstellungen auf der Synergis™ Cloud Link-Einheit werden nicht automatisch mit dem Access Manager synchronisiert. Wenn Sie über das Synergis™ Appliance Portal Einstellungen an der Einheit ändern, z. B. das Anmeldepasswort, die IP-Adresse oder die Art und Weise, wie die Einheit auf Verbindungsanfragen reagiert, müssen Sie dieselben Einstellungen im Access Manager im Config Tool ändern.

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Wählen Sie die geänderte Einheit im Einheitendiagramm aus.
- 3 Klicken Sie auf die Registerkarte **Eigenschaften**.



- 4 Ändern Sie im Abschnitt *Verbindungseinstellungen* die Parameter, damit sie den Einstellungen entsprechen, die Sie für die Einheit im Synergis™ Appliance Portal konfiguriert haben.
 - **Webadresse:** Webadresse für das Kontaktieren des Portals der Synergis™-Einheit. Wenn Sie die Webadresse ändern, damit die IP-Adresse der Einheit verwendet wird, nachdem sie mit ihrem Hostnamen registriert wurde, vergewissern Sie sich, dass Sie die IPv6-Adresse aus der Liste **Akzeptierte Access-Manager-Verbindungen** auf der Seite *Netzwerk* des Portals der Einheit löschen.

Wenn die IPV6-Adresse nicht von der Liste entfernt wird und die Verbindung der Einheit das nächste Mal getrennt wird, wird sie sich nicht erneut verbinden.

- **Benutzername und Passwort:** Login-Benutzername und Passwort.
 - **Passwort der Einheit ändern:** Klicken Sie, um das Passwort zu aktualisieren.
 - **Verlauf für Einheitenpasswort:** Zeigt die Details der letzten fünf Versuche zum Ändern des Passworts an, die über Security Center durchgeführt wurden, einschließlich Datum, vorheriges Passwort und neues Passwort.
 - **DHCP verwenden:** Ändern Sie diesen Parameter nicht, es sei denn, der Genetec Technische Support weist Sie an, dies zu tun. Dieser Parameter wird jedes Mal zurückgesetzt, wenn der Access Manager die Verbindung zur Synergis™-Einheit wiederherstellt.
 - **Webproxy ignorieren:** Wählen Sie diese Option, um den Access Manager anzuweisen, die Proxy-Server-Einstellungen des Servers zu ignorieren, der aktuell die Rolle hostet. Löschen Sie diese Option, um den Access Manager anzuweisen, den Proxy-Server-Einstellungen (Standard = gelöscht) zu folgen.
 - **Fingerabdruck:** Der Fingerabdruck des Zertifikats auf der Synergis™-Einheit. Dieses Feld wird automatisch aktualisiert, um das neue Zertifikat widerzuspiegeln, wenn Sie auf die Schaltfläche **Vertrauenswürdige Zertifikat zurücksetzen** klicken.
 - **Vertrauenswürdige Zertifikate zurücksetzen:** (Nur aktiviert, wenn das Gerät offline ist) Klicken Sie auf diese Schaltfläche, damit der Access Manager das anerkannte Zertifikat für dieses Gerät vergisst, so dass das neue Zertifikat akzeptiert werden kann. Verwenden Sie diese Funktion, wenn Sie das digitale Zertifikat des Geräts nach der Registrierung geändert haben.
- 5 Klicken Sie auf **Übernehmen**.

Überwachungseingänge der Synergis™ Cloud Link-Appliance konfigurieren

Sie können die vier Eingänge der Synergis™ Cloud Link-Appliance verwenden, um die physische Installation der Appliance zu überwachen. Sie können beispielsweise einen Eingang mit einem Sabotagetaster auf dem Gehäuse verbinden, in welchem die Appliance installiert ist.

Was Sie noch wissen sollten

- Sie können für jeden Eingang spezielles Verhalten festlegen. Jedes spezielle Verhalten entspricht einem Ereignis, das Sie im Task *Überwachung* empfangen können.

Besonderes Verhalten	Security Center-Ereignis
Stromausfall	Wechselstromfehler
Sabotagetaster	Hardwaremanipulation
Batterieausfall	Batteriefehler

- Sie können Statusänderungen der Eingänge auf der Seite *E/A-Diagnose* im Synergis™ Appliance Portal ansehen.

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Wählen Sie Ihre Synergis™ Cloud Link-Einheit aus und klicken Sie dann auf die Registerkarte **Hardware**.

- 3 Klicken Sie auf die Registerkarte **Integrierte EA** und konfigurieren Sie dann die Eingänge:
Beispiel:

The screenshot shows the 'Hardware' configuration page for 'Onboard IO'. Under the 'Inputs' section, there are four input configurations:

- Input 1:** Special behavior: Tamper switch; Input configuration: Four states; Resistance range: 1k/2k; Closed range: Lower Limit (Ohms): 800, Higher Limit (Ohms): 1200; Open range: Lower Limit (Ohms): 1800, Higher Limit (Ohms): 2200.
- Input 2:** Special behavior: Battery failure; Input configuration: Three states; Resistance range: 2.2k; Resistance range: Lower Limit (Ohms): 1900, Higher Limit (Ohms): 2500.
- Input 3:** Special behavior: AC Failure; Input configuration: Unsupervised.
- Input 4:** Special behavior: None; Input configuration: Unsupervised.

- **Besonderes Verhalten:** Das besondere Verhalten bestimmt das Ereignis, das Sie im Task *Überwachung* erhalten, wenn sich der Eingang in einem nicht normalen Status befindet. Standardmäßig ist das spezielle Verhalten auf **Keines** gesetzt. Wählen Sie eine der folgenden Optionen:
 - **Stromausfall**
 - **Sabotagetaster**
 - **Batterieausfall**
- **Eingabekonfiguration:** Wählen Sie eine der folgenden Optionen:
 - **Unbeaufsichtigt:** Eingänge werden standardmäßig nicht überwacht.
 - **Drei Zustände:** Wählen Sie eine der vorkonfigurierten Optionen, die für Sie den **Widerstandsbereich** auswählt, oder wählen Sie **Benutzerdefiniert** und geben Sie selbst **Unteres Limit (Ohms)** und **Oberes Limit (Ohms)** in Ohms ein.
 - **Vier Zustände:** Wählen Sie eine der vorkonfigurierten Optionen, die für Sie den **Geschlossenen Bereich** und **Offenen Bereich** auswählt, oder wählen Sie **Benutzerdefiniert** aus und geben Sie selbst **Unteres Limit (Ohms)** und **Oberes Limit (Ohms)** ein.

- 4 Klicken Sie auf **Anwenden**.
- 5 Klicken Sie auf die Registerkarte **Peripheriegeräte** und führen Sie einen Doppelklick auf den Eingang aus, den Sie auf der Seite *Hardware* konfiguriert haben.
- 6 (Optional) Geben Sie im Dialogfeld *Eingang bearbeiten* einen neuen Namen und eine logische ID ein.
- 7 Legen Sie den **Kontakttyp** fest:
 - a) Wählen Sie **Nicht überwacht**, **3 Status überwacht** oder **4 Status überwacht** aus, um dem Wert zu entsprechen, den Sie für die **Eingangskonfiguration** auf der Seite *Hardware* ausgewählt haben.
 - b) Wählen Sie **Normal offen** oder **Normal geschlossen**.
- 8 Klicken Sie auf **Speichern**.

Wenn sich ein Eingang in einem nicht normalen Status befindet, wird die Synergis™ Cloud Link-Einheit gelb und Sie bekommen eine Entitätswarnung. Wenn Sie die Synergis™ Cloud Link-Einheit und die Ereignisse zu besonderem Verhalten überwacht haben, erhalten Sie das Ereignis, das dem besonderen Verhalten des Ereignisses im Task *Überwachung* entspricht.

Teil III

Integrationspezifische Konfiguration

Dieser Teil enthält die folgenden Kapitel:

- Kapitel 4, "[Allegion-Schlage-Funkschlösser](#)" auf Seite 66
- Kapitel 5, "[Assa-Abloy-Aperio-fähige Schlösser](#)" auf Seite 69
- Kapitel 6, "[Assa-Abloy-IP-Schlösser](#)" auf Seite 83
- Kapitel 7, "[AutoVu-SharpV-Kameras](#)" auf Seite 101
- Kapitel 8, "[Axis-Controller](#)" auf Seite 106
- Kapitel 9, "[DDS-Controller](#)" auf Seite 121
- Kapitel 10, "[HID-VertX-Sub-Panels](#)" auf Seite 126
- Kapitel 11, "[Mercury-Steuerungen](#)" auf Seite 132
- Kapitel 12, "[Allegion-Schlage-Schlösser über Mercury](#)" auf Seite 182
- Kapitel 13, "[BEST-Wi-Q-Schlösser über Mercury](#)" auf Seite 190
- Kapitel 14, "[SimonsVoss-SmartIntego-Schlösser über Mercury](#)" auf Seite 202
- Kapitel 15, "[SALTO-SALLIS-Funkschlösser](#)" auf Seite 209
- Kapitel 16, "[OSDP-Lesegeräte, die mit den RS-485-Ports von Synergis™ Cloud Link verbunden sind](#)" auf Seite 217
- Kapitel 17, "[STid-Lesegeräte, die das SSCP-Protokoll verwenden](#)" auf Seite 230

Allegion-Schlage-Funkschlösser

Dieser Abschnitt enthält die folgenden Themen:

- "[Allegion-Schlage-Funkschlösser in der Synergis™-Einheit registrieren:](#)" auf Seite 67
- "[Allegion-Schlage-Funkschlösser in der Synergis™-Einheit erneut registrieren:](#)" auf Seite 68

Allegion-Schlage-Funkschlösser in der Synergis™-Einheit registrieren:

Allegion Schlage LE-, NDE- und Control-Schlösser (FE410 und BE467F) können ohne Mercury-Controller in die ENGAGE-Plattform integriert werden.

Was Sie noch wissen sollten

Die ENGAGE IP Integration unterstützt bis zu 10 Schlösser pro Gateway und bis zu 32 Gateways pro Synergis™-Einheit, bis zu einem Maximum von 200 Schlössern pro Einheit. Sie benötigen einen Online-Zugang, um diesen Task zu erledigen.

Prozedur

- 1 Erstellen Sie ein ENGAGE-Partnerkonto unter portal.allegionengage.com.
WICHTIG: Erstellen Sie Ihr ENGAGE-Konto nicht über die Allegion ENGAGE Mobile App.
- 2 Laden Sie die neueste Version des Genetec™ Allegion Site Configurators von der [GTAP Produkt-Download-Seite](#) herunter:
 - a) Wählen Sie in der Liste **Download Finder Synergis™ Cloud Link** aus.
 - b) Laden Sie den Genetec Allegion Site Configurator herunter.
- 3 Verwenden Sie den Genetec Allegion Site Configurator, um den Standort zu erstellen, an dem die Zutrittskontroll-Hardware installiert werden soll.
Bei diesem Vorgang wird automatisch ein Standortschlüssel erstellt. Notieren Sie den Standortschlüssel und bewahren Sie ihn an einem sicheren Ort auf.
- 4 Laden Sie die Allegion ENGAGE Mobile App aus dem App Store oder von Google Play herunter.
- 5 Öffnen Sie die Allegion ENGAGE Mobile App, um sich bei Ihrem ENGAGE-Partnerkonto anzumelden.
- 6 Verwenden Sie die Allegion ENGAGE Mobile App, um die Gateways und Schlösser dem Standort hinzuzufügen und sie zu verknüpfen.
- 7 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 8 Klicken Sie auf **Konfiguration > Hardware**.
- 9 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 10 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **Schlage IP** aus der Liste **Hardwaretyp**, und geben Sie dann die IP-Adresse des ENGAGE-Gateways und den Standortschlüssel ein, den Sie mithilfe des Genetec Allegion Site Configurator erstellt haben.
- 11 Klicken Sie auf **Speichern**.
Die Berechtigungen des Gateways werden automatisch vervollständigt, und die angeschlossenen Schlösser werden in der Hardwarestruktur aufgelistet.
WICHTIG: Vergewissern Sie sich, dass der Standortschlüssel richtig eingegeben wurde. Wenn diese nicht korrekt eingegeben wird, wird keine der Berechtigungen mit dem Schloss synchronisiert.
- 12 (Optional) Fügen Sie jedes weitere ENGAGE Gateway hinzu.
- 13 Registrieren Sie die Berechtigung im Security Center.
BEMERKUNG: Sie können keine Berechtigungen mit automatischer Eingabe über das Schloss registrieren. Sie können den Allegion Schlage MT20 Enrollment Reader im Tastendruck-Emulator-Modus verwenden.

Allegion-Schlage-Funkschlösser in der Synergis™-Einheit erneut registrieren:

Sie können Allegion-Schlage-Funkschlösser über die Seite *Hardware* der Synergis™-Einheit im Config Tool erneut registrieren, um ein Zurücksetzen des ENGAGE Gateway und dessen Schlössern zu vermeiden und die Allegion-ENGAGE-Mobilapp für das erneute Registrieren zu verwenden.

Was Sie noch wissen sollten

- Das ENGAGE Gateway muss nicht auf die Werkseinstellungen zurückgesetzt werden, bevor es über Config Tool erneut registriert wird.
- Sie können nur das Synergis™ Appliance Portal verwenden, um das ENGAGE Gateway zum ersten Mal zu registrieren oder um es nach einem Zurücksetzen auf die Werkseinstellungen zu registrieren.

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Wählen Sie in der Entitätsstruktur die Synergis™-Einheit aus, auf der Sie das ENGAGE Gateway erneut registrieren möchten.
- 3 Klicken Sie auf **Hardware > Schlage IP**.
- 4 Klicken Sie auf **Hinzufügen** (+) und geben Sie dann die folgenden Informationen ein:

- **IP-:** Die IP-Adresse des ENGAGE Gateway.
- **Benutzername:** Den Benutzernamen des ENGAGE Gateway.
- **Passwort:** Das Passwort des ENGAGE Gateway.
- **Standortschlüssel:** Der Standortschlüssel, den Sie mithilfe des Genetec™ Allegion Site Configurators erstellt haben, wenn Sie das ENGAGE Gateway erstmals registriert haben.

BEMERKUNG: Sie können die folgende URL verwenden, um den Benutzernamen und das Passwort zu finden: `https://<SCL IP>/SchlageIP/Bus/<Gateway IP>/RevealCredentials`, wobei `<SCL IP>` die IP-Adresse der Synergis™-Einheit und `<Gateway IP>` die IP-Adresse des ENGAGE Gateway ist.

- 5 Klicken Sie auf **Übernehmen**.

Die Schlösser werden zur Seite *Peripheriegeräte* der Synergis™-Einheit im Config Tool hinzugefügt. Dies kann einige Minuten dauern.

Assa-Abloy-Aperio-fähige Schlösser

Dieser Abschnitt enthält die folgenden Themen:

- ["Koppeln von Aperio-fähigen Schlössern mit dem AH30-Hub"](#) auf Seite 70
- ["Anmeldung von Aperio-fähigen Schlössern, die an einen AH30-Hub angeschlossen sind"](#) auf Seite 74
- ["Koppeln von Aperio-fähigen Schlössern mit dem AH40 IP-Hub"](#) auf Seite 77
- ["Registrieren von Aperio-fähigen Schlössern, die an einen AH40 IP-Hub angeschlossen sind"](#) auf Seite 79
- ["Konfigurieren von Türen, die mit einem Aperio-fähigen Schloss ausgestattet sind"](#) auf Seite 80

Koppeln von Aperio-fähigen Schlössern mit dem AH30-Hub

Wenn Sie Aperio-fähige Schlösser mit einem AH30-Hub verwenden, müssen Sie die Schlösser mit der Aperio Programming Application (APA) mit dem Hub koppeln, bevor Sie die Schlösser an Ihrer Synergis™-Einheit registrieren können.

Bevor Sie beginnen

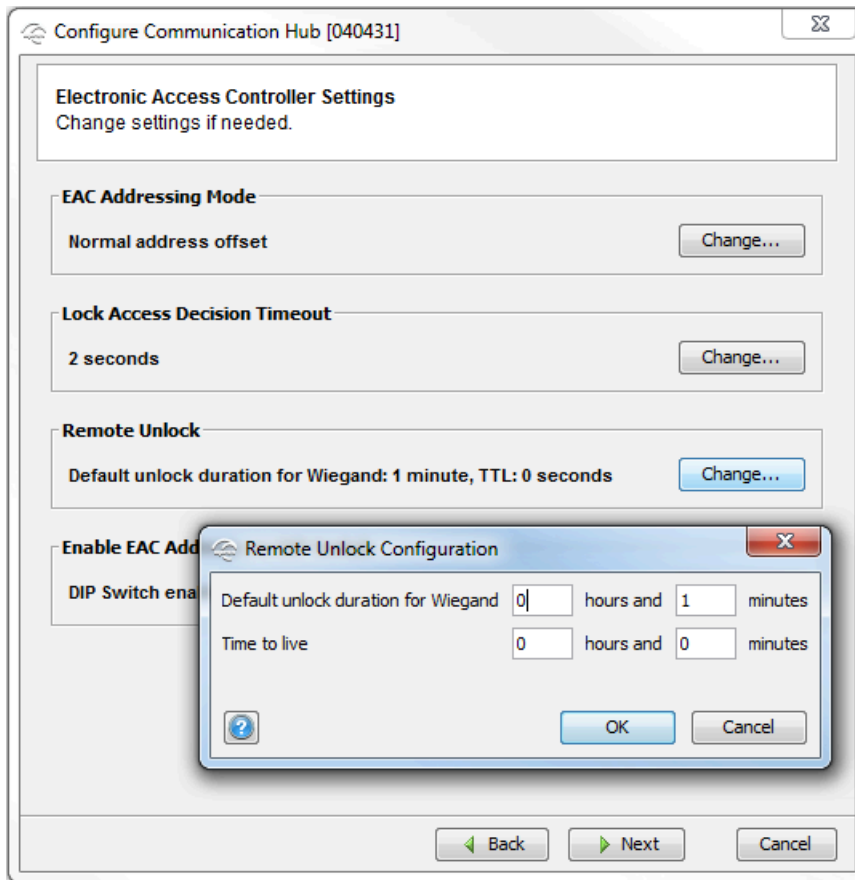
Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Aperio Online Programming Application – Handbuch
- Aperio Programming Application (APA)
- USB-Dongle
- TriBee Bootloader, was den USB-Dongle-Treiber enthält
- Unterstützte Firmware
- Computer zum Ausführen der APA.
- Karte, die mit dem Lesegerät kompatibel ist.
- Von ASSA ABLOY bereitgestellte Verschlüsselungsschlüsseldatei

Prozedur

- 1 Stellen Sie die EAC-Adresse (1 - 15) am Hub mit Hilfe der DIP-Schalter ein.
WICHTIG: Bis zu acht Hubs können an denselben RS-485-Kanal in einer Verkettung angeschlossen werden, aber jeder Hub muss eine andere EAC-Adresse verwenden.
- 2 Schalten Sie den Hub ein.
- 3 Schließen Sie den USB-Dongle an Ihren Computer an und installieren Sie Folgendes:
 - TriBee Bootloader (Treiber für den USB-Dongle)
 - Aperio Programming Application (APA)
- 4 Öffnen Sie APA und öffnen oder erstellen Sie eine Installation.
BEMERKUNG: Jede Installation ist mit einer Verschlüsselungsschlüsseldatei verknüpft. Kontaktieren Sie ASSA ABLOY wegen dieser Schlüsseldatei, um eine Installation zu erstellen.
- 5 Scannen Sie, um den Hub zu erkennen, und koppeln Sie die Schlösser mit dem Hub.
Weitere Informationen finden Sie im *Aperio Online Programming Application Manual*.
- 6 Aktualisieren Sie mithilfe der APA die Firmware auf dem Hub und den Schlössern.
Weitere Informationen finden Sie unter [Unterstützte Aperio-fähige Schlösser](#).
BEST-PRACTICE: Aktualisieren Sie immer den Kommunikations-Hub, bevor Sie die Schlösser oder Sensoren aktualisieren. Prüfen Sie, ob der DIP-Schalter auf die richtige EAC-Adresse eingestellt ist. Wenn DIP 5 (Koppelungsmodus) während einer Aktualisierung auf aktiv gesetzt wird, startet der Kommunikations-Hub mit einer anderen EAC-Adresse.
- 7 Konfigurieren Sie den Hub.
- 8 Wenn Ihre Kommunikations-Hub-Firmware älter als Version 2.6.5 ist, aktivieren Sie die Option **Fernentriegelung**, um Security Center-Entsperrungszeitpläne zu verwenden.
Ab der Firmware-Version 2.6.5 ist die Option standardmäßig aktiviert.

- 9 Geben Sie im Dialogfeld *Konfiguration für die Fernentriegelung* einen Wert für **Aktivierungsdauer** ein und klicken Sie auf **OK**.



Diese Zeit gibt an, wie lange der Befehl **Fernentriegelung** (grantAccessSequence) am Kommunikations-Hub anliegt. Diese Einstellung muss immer länger sein als das am Schloss eingestellte **Statusberichtsintervall**.

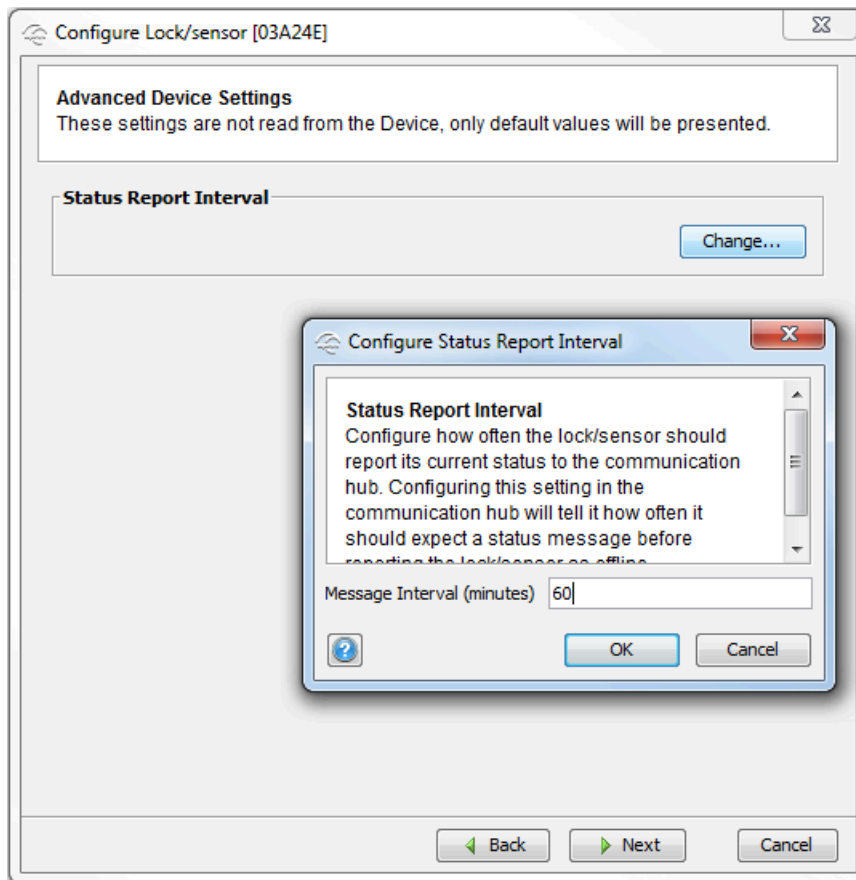
Sie können den Wert von **Default-Entriegelungsdauer für Wiegand** ignorieren.

- 10 Wenn Entsperrungszeitpläne verwendet werden, geben Sie einen Wert für das **Statusberichtsintervall** im Bereich von 5 bis 15 Minuten ein.

Wenn Sie die Statusintervallzeit verringern, verkürzt sich die Lebensdauer der Batterie des Geräts. Jede Änderung dieses Intervalls muss sowohl am Schloss als auch am Kommunikations-Hub vorgenommen werden. Wenn nur ein Schloss mit dem Kommunikations-Hub gekoppelt ist, geschieht dies

automatisch. Wenn mehr als ein Schloss mit dem Kommunikations-Hub gekoppelt ist, müssen Sie das **Statusberichtsintervall** über den Kommunikations-Hub einstellen.

BEMERKUNG: Bei v3-Schlössern wird die Einstellung **Statusberichtsintervall** nur zur Meldung des Online-Status des Schlosses verwendet. Es ist das **Abfrageintervall**, das verwendet wird, um die Zeitverzögerung für das Starten und Beenden des Entsperrungszeitplans zu minimieren.



11 Koppeln Sie jedes Funkschloss:

a) Klicken Sie mit der rechten Maustaste auf **Kommunikations-Hub** und wählen Sie **Koppeln mit Schloss oder Sensor**.

Der Kopplungsprozess beginnt.

b) Halten Sie die Berechtigung an das Schloss, oder aktivieren Sie den Magneten für den Sensor, um die Hardware mit dem Kommunikations-Hub zu koppeln.

Der Hub weist dem Schloss automatisch eine EAC-Adresse zu.

c) Notieren Sie die dem Schloss zugewiesene EAC-Adresse (1 bis 127).

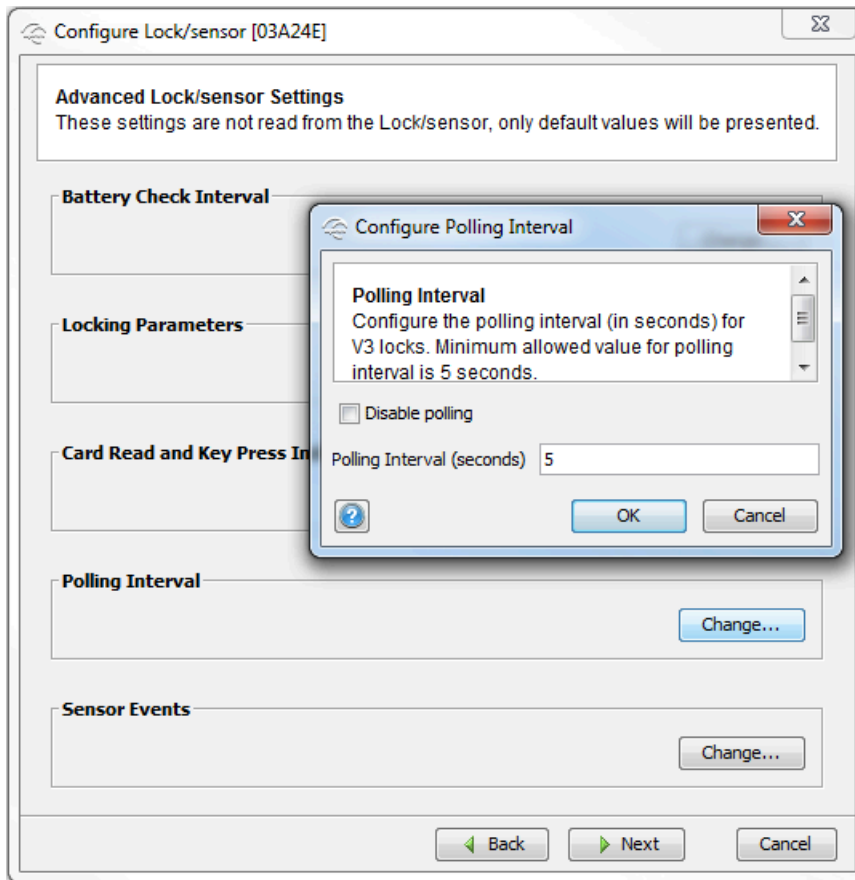
Die EAC-Adresse des Hubs wird in die EAC-Adresse des Schlosses integriert. Um die EAC-Adresse des Hubs aus der EAC-Adresse des Schlosses zu erhalten, verwenden Sie eine der folgenden Formeln:

- $EAC\text{-Adresse des Hubs} = EAC\text{-Adresse des Schlosses} \bmod 16$
- $EAC\text{-Adresse des Hubs} = (\text{Rest von } EAC\text{-Adresse des Schlosses}) \text{ geteilt durch } 16$

12 Wenn Sie v3-Schlösser verwenden, setzen Sie das **Abfrageintervall** auf 5 Sekunden.

Dadurch wird die Zeitverzögerung beim Starten und Beenden des Entsperrungszeitplans minimiert, was die Reaktionszeit der Schlösser verkürzt. Es ermöglicht auch, dass die manuellen Entsperrbefehle von Security Desk innerhalb von 5 Sekunden funktionieren. Es wird nicht empfohlen, manuelle

Entsperrbefehle für andere Schlösser als v3 zu verwenden, da der Befehl erst nach 1 Minute oder länger funktioniert, je nach **Statusberichtsintervall**.



13 Nachdem alle Schlösser gekoppelt sind, stellen Sie den Hub auf sichere Funkkommunikation ein.

Nach Durchführen dieser Schritte

Registrieren Sie die Schlösser an der Synergis™-Einheit.

Anmeldung von Aperio-fähigen Schlössern, die an einen AH30-Hub angeschlossen sind

Damit die Synergis™ Cloud Link -Einheit mit Aperio-fähigen Schlössern kommuniziert, müssen Sie diese im Synergis™ Appliance Portal registrieren.

Bevor Sie beginnen

- [Koppeln Sie die Aperio-fähigen Schlösser mit dem Hub.](#)
- Schließen Sie den Hub an einen der RS-485-Kanäle an (1 - 4) :
 - Verbinden Sie den Anschluss A des Hubs mit dem Anschluss "+" des Kanals.
 - Verbinden Sie den Anschluss B des Hubs mit dem Anschluss "-" des Kanals.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* in der Liste **Hardwaretyp** die Option **Aperio RS 485** aus.
- 5 Wählen Sie den **Kanal** aus (1 - 4) .
BEMERKUNG: Wenn Sie die Synergis™ Cloud Link 312-Einheit haben, haben Sie bis zu 12 Kanäle. Weitere Informationen finden Sie unter [Informationen über Ports in Synergis Cloud Link 312 RS-485](#).
- 6 Wählen Sie in der Liste **Schnittstellenmodultyp** die Option **Aperio**.

- 7 Geben Sie die Schlösser an, die Sie registrieren möchten, indem Sie einen der folgenden Schritte ausführen:

- Um die Anmeldung automatisch durchzuführen, klicken Sie auf **Scan**.

Die Ermittlungsfunktion sucht alle Schnittstellenmodule desselben Herstellers, die mit demselben Kanal verbunden sind, und registriert sie.

Wenn Synergis™ Appliance Portal nicht alle angeschlossenen Schnittstellenmodule findet, versuchen Sie die manuelle Anmeldung.

- Um sich manuell zu registrieren, geben Sie die EAC-Adresse (1 - 127) des Schlosses ein, die Sie beim [Koppeln des Schlosses mit dem Hub](#) notiert haben, und klicken Sie auf **Hinzufügen**.

Wiederholen Sie den Vorgang bei Bedarf, um alle an denselben Kanal angeschlossenen Module zu konfigurieren.

TIPP: Wenn Sie die EAC-Adressen der Schlösser kennen und nur einige wenige zu registrieren haben, ist es schneller, sie manuell zu registrieren.

- 8 Klicken Sie auf **Speichern**.

Der Hardwaretyp, der Kanal und das Schnittstellenmodul, das Sie gerade hinzugefügt haben, werden auf der Seite *Hardwarekonfiguration* angezeigt.

- 9 Wählen Sie ein Schloss aus, um dessen Eigenschaften im rechten Fensterbereich anzuzeigen. Die EAC-Adressen sowohl des Hubs als auch des Schlosses werden angezeigt.

- 10 Wählen Sie jedes hinzugefügte Schnittstellenmodul auf der Seite *Hardwarekonfiguration* aus und konfigurieren Sie dessen Einstellungen.

Eine Beschreibung dieser Einstellungen finden Sie in der Dokumentation des Herstellers. Nehmen Sie die Änderungen nach Bedarf vor.

11 Testen Sie die Verbindung und Konfiguration Ihres Schnittstellenmoduls auf der Seite *E/A-Diagnose* .

Nach Durchführen dieser Schritte

- Registrieren Sie die Synergis™-Einheit in Security Center.
- Konfigurieren Sie die Türen, die mit Aperio-fähigen Schlössern ausgestattet sind.

Koppeln von Aperio-fähigen Schlössern mit dem AH40 IP-Hub

Wenn Sie Aperio-fähige Schlösser mit einem AH40-Hub verwenden, müssen Sie den Hub mit der Aperio Programming Application (APA) konfigurieren, bevor Sie die Schlösser an Ihrer Synergis™-Einheit registrieren können.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Aperio Online Programming Application – Handbuch
- Aperio Programming Application (APA)
- USB-Dongle
- TriBee Bootloader, was den USB-Dongle-Treiber enthält
- Unterstützte Firmware
- Computer zum Ausführen der APA.
- Karte, die mit dem Lesegerät kompatibel ist.
- Von ASSA ABLOY bereitgestellte Verschlüsselungsschlüsseldatei

Prozedur

- 1 Schalten Sie den Hub ein.
- 2 Schließen Sie den USB-Dongle an Ihren Computer an und installieren Sie Folgendes:
 - TriBee Bootloader (Treiber für den USB-Dongle)
 - Aperio Programming Application (APA)
- 3 Öffnen Sie APA und öffnen oder erstellen Sie eine Installation.

BEMERKUNG: Jede Installation ist mit einer Verschlüsselungsschlüsseldatei verknüpft. Kontaktieren Sie ASSA ABLOY wegen dieser Schlüsseldatei, um eine Installation zu erstellen.

4 Verwenden Sie APA, um den Hub zu konfigurieren:

- a) Aktualisieren Sie die Firmware auf dem Hub und den Schlössern.

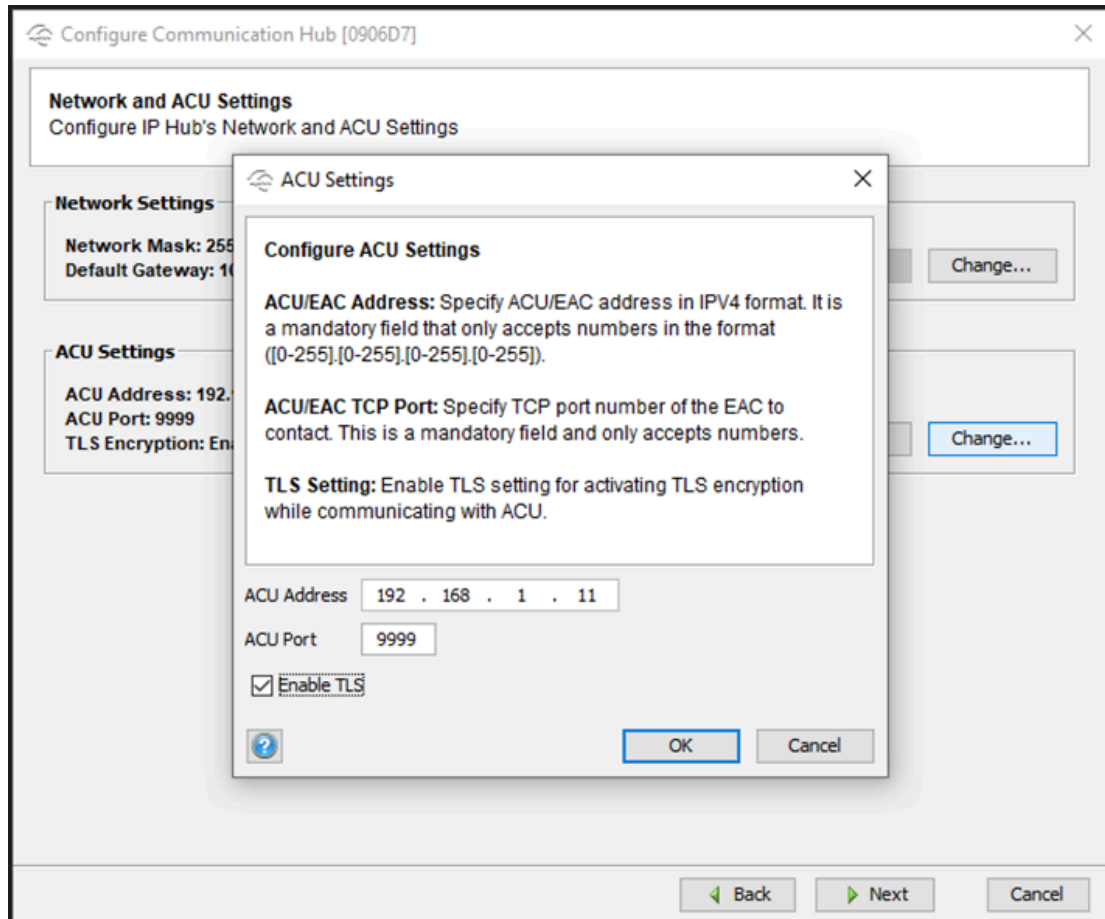
BEST-PRACTICE: Aktualisieren Sie den Kommunikations-Hub, bevor Sie die Schlösser oder Sensoren aktualisieren.

- b) Koppeln Sie den Hub mit den Lesegeräten.

Durch die Auswahl des AH40 IP-Hubs in APA wird der Hub automatisch mit den Lesegeräten gepaart.

BEMERKUNG: Notieren Sie sich die Portnummer. Sie müssen den Hub im Synergis™ Appliance Portal registrieren.

- c) Geben Sie die IP-Adresse der Synergis™-Einheit als ACU-Adresse an.



Registrieren von Aperio-fähigen Schlössern, die an einen AH40 IP-Hub angeschlossen sind

Damit die Synergis™-Einheit mit Aperio-fähigen Schlössern kommuniziert, müssen Sie diese im Synergis™ Appliance Portal registrieren.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **Aperio IP** als **Hardwaretyp**, und geben Sie die Portnummer des Hubs in das Feld **Port** ein. Der Default-Port ist 9999.
- 5 Klicken Sie auf **Speichern**.
- 6 Klicken Sie auf **Bearbeiten** (✎) an der Aperio IP-Schnittstelle.
Das Dialogfeld zur Konfiguration des Kanals wird geöffnet.
- 7 Aktivieren Sie im Konfigurationsdialogfeld das Kontrollkästchen **Registrieren** für den Hub, den Sie registrieren möchten.

BEMERKUNG: Wenn Sie mehr als einen AH40-Hub an demselben Port konfiguriert haben, werden alle angeschlossenen Hubs und ihre MAC-Adressen aufgelistet.

- 8 Klicken Sie auf **Speichern**.

Die Schlösser, die mit dem registrierten AH40-Hub verbunden sind, werden in der Hardwarestruktur aufgelistet und werden grün. Dies kann bis zu zwei Minuten dauern.

Konfigurieren von Türen, die mit einem Aperio-fähigen Schloss ausgestattet sind

Um sicherzustellen, dass Sie keine doppelten Ereignisse *Tür verriegelt* und *Tür entriegelt* in Security Desk erhalten, müssen Sie die Option **REX automatisch gewähren** für alle Türen mit einem Aperio-fähigen Schloss deaktivieren.

Bevor Sie beginnen

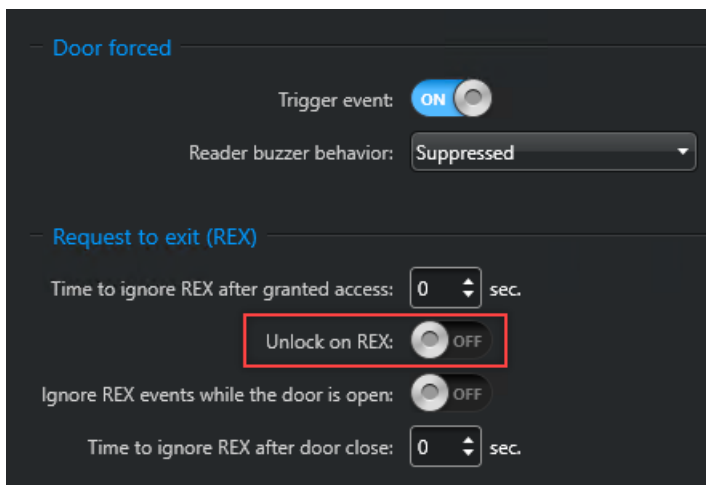
- Registrieren Sie die Synergis™ Cloud Link-Einheit in Security Center.
- Je nachdem, welchen Hub Sie verwenden, führen Sie einen der folgenden Schritte aus:
 - Bei AH30 RS-485-Hubs koppeln Sie Ihre Schlösser mit dem AH30-Hub und registrieren Sie die Aperio-fähigen Schlösser an der Synergis™-Einheit.
 - Bei AH40 IP-Hubs koppeln Sie Ihre Schlösser mit dem AH40-Hub und registrieren Sie die Aperio-fähigen Schlösser an der Synergis™-Einheit.

Was Sie noch wissen sollten

Das Aperio-fähige Schloss verwendet eine mechanische Türöffnertaste. Die Synergis™ Cloud Link -Einheit steuert die Entriegelung der Tür nicht, wenn eine Türöffnertaste ausgelöst wird. Die Aktivierung von **REX automatisch erlauben** in der Türkonfiguration bewirkt, dass die Ereignisse *Tür verriegelt* und *Tür entriegelt* zweimal im Security Desk empfangen werden.

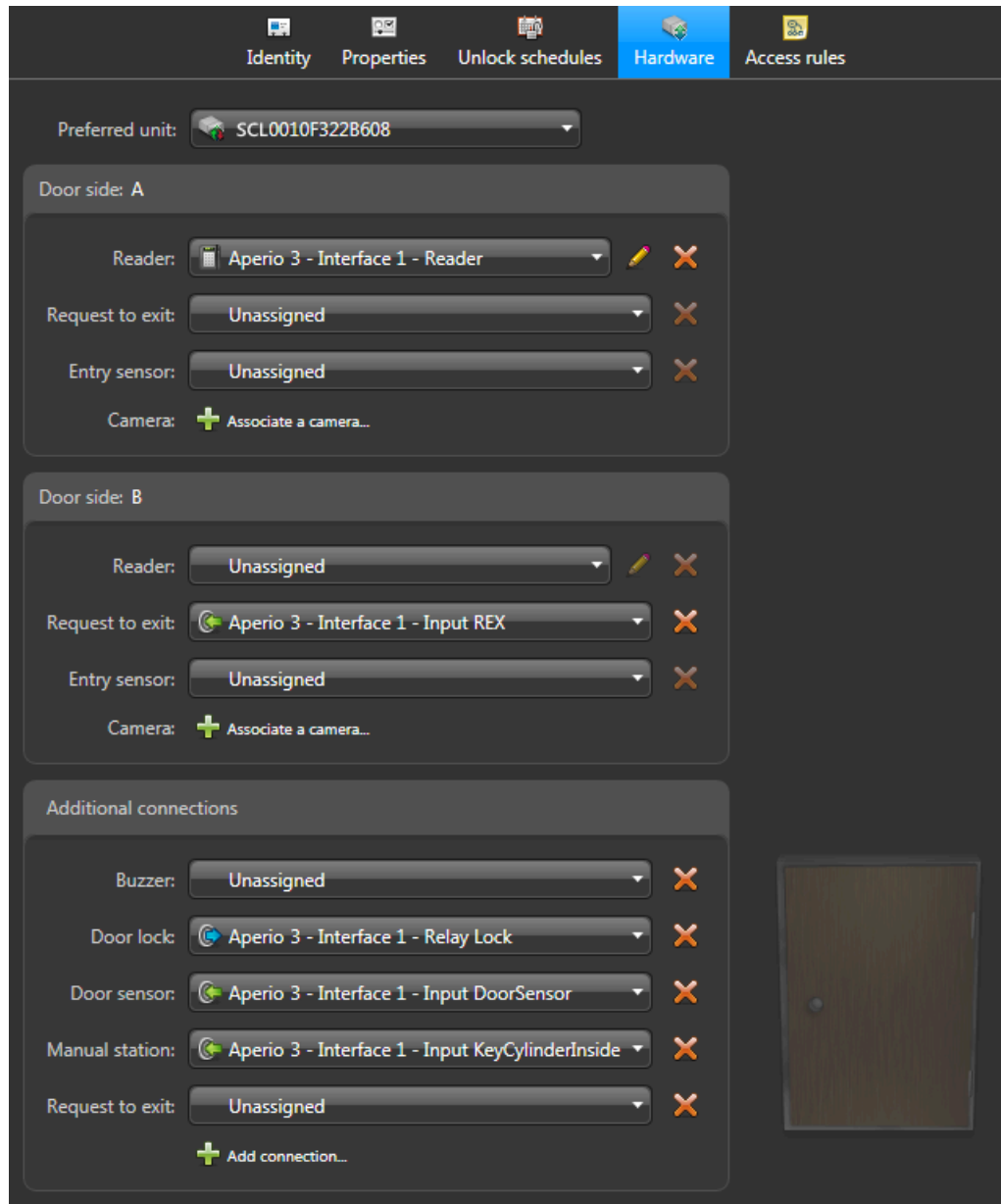
Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Bereichsansicht*.
- 2 Wählen Sie in der Objektstruktur die Tür aus, die das Aperio-fähige Schloss verwendet.
- 3 Klicken Sie auf die Registerkarte **Eigenschaften**.
- 4 Deaktivieren Sie im Abschnitt *Aufforderung zum Verlassen (REX)* die Option **Entsperren bei REX**.




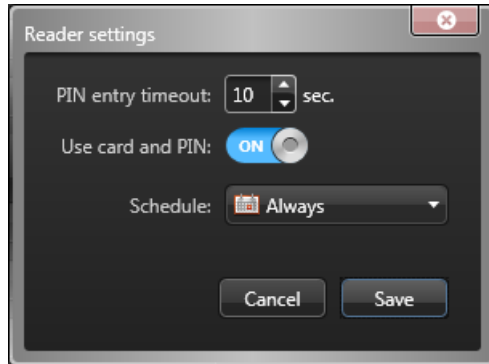
- 5 Klicken Sie auf die Registerkarte **Hardware** und wählen Sie dann die Synergis™-Einheit, die das Schloss steuert.

Alle Peripheriegeräte, die demselben Schloss entsprechen, werden mit dem gleichen Präfix „Aperio X - Interface n“ benannt, wobei X der Kanalnummer (1-4) und n die EAC-Adresse des Schlosses ist.



- 6 Weisen Sie im Abschnitt *Türseite In* das der Tür entsprechende Lesegerät zu.
- 7 Weisen Sie im Abschnitt *Türseite Out* den der Tür entsprechenden REX-Sensor zu.
- 8 Nehmen Sie im Abschnitt *Zusätzliche Verbindungen* die folgenden Einstellungen vor:
- Weisen Sie das Schlossrelais dem **Türschloss** zu.
 - Weisen Sie den Türsensoreingang dem **Türsensor** zu.
 - Weisen Sie *KeyCylinderInside* oder *KeyCylinderOutside* der **Manuellen Station** zu, falls zutreffend.

- 9 Wenn das Lesegerät im Modus *Karte und PIN* arbeiten soll, stellen Sie sicher, dass Sie eine Zeitüberschreitung konfigurieren, die lang genug ist, damit der Karteninhaber die PIN eingeben kann. Die Default-Zeitüberschreitung von 5 Sekunden für den Zutritt ist für Aperio-fähige Schlösser nicht lang genug. Nach Vorlage der Berechtigung an der Tür muss der Karteninhaber warten, bis die LED grün leuchtet, bevor er die PIN eingeben kann. Dieser Vorgang dauert in jedem Fall länger als 5 Sekunden.
- a) Klicken Sie auf **Leseeinstellungen**  neben der Liste **Lesegeräte**.
 - b) Aktivieren Sie im Dialogfeld *Lesegeräteinstellungen* die Option **Karte und PIN verwenden**.
 - c) Stellen Sie die **PIN-Eingabezeitüberschreitung** auf die gewünschte Dauer ein.
Die empfohlene Dauer beträgt 10 Sekunden.



- d) Klicken Sie auf **Speichern**.
- 10 Klicken Sie auf **Anwenden**.

Assa-Abloy-IP-Schlösser

Dieser Abschnitt enthält die folgenden Themen:

- ["Konfigurationsübersicht für Assa Abloy-IP-Schlösser" auf Seite 84](#)
- ["Informationen zur Funktion Funkaktivierungsereignisse für Assa Abloy-WiFi-Schlösser" auf Seite 85](#)
- ["Konfiguration der Funktion Funkaktivierungsereignisse für Assa-Abloy-WLAN-Schlösser" auf Seite 86](#)
- ["Aktivierung des Flucht- und Rückkehrmodus bei Assa Abloy-IP-Schlössern mit Korpustyp 8200 und überwachtem Riegel" auf Seite 87](#)
- ["Konfigurieren einer Persona-Seriennummer für die Schlösser IN120 und IN220" auf Seite 89](#)
- ["Informationen zum Durchgangsmodus für Assa Abloy-IP-Schlösser" auf Seite 90](#)
- ["Aktivieren des Durchgangsmodus an Assa Abloy-IP-Schlössern" auf Seite 91](#)
- ["Aktivierung des Privatsphärenmodus bei Assa Abloy-IP-Schlössern ohne überwachten Riegel" auf Seite 92](#)
- ["Assa-Abloy-IP-Schlösser registrieren, die mit der Synergis™-Einheit verbunden sind" auf Seite 94](#)
- ["Überwachung des Batteriestatus von WiFi-Schlössern" auf Seite 100](#)

Konfigurationsübersicht für Assa Abloy-IP-Schlösser

Um Assa Abloy-IP-Schlösser so zu konfigurieren, dass sie mit einer Synergis™-Einheit funktionieren, müssen Sie die Schlösser zunächst mit dem Lock Configuration Tool (LCT) konfigurieren und dann die Schlösser mit der Synergis™-Einheit unter Verwendung des Synergis™ Appliance Portals paaren.

Die folgende Tabelle fasst den Konfigurationsprozess der IP-Schlösser zusammen.

Phase	Beschreibung	Siehe
1	Vergewissern Sie sich, dass Ihre IP-Schloss-Firmware auf dem neuesten Stand ist und von Ihrer Version von Synergis™ Software unterstützt wird.	<ul style="list-style-type: none"> • <i>IP-fähiges Schloss Installationskurzanleitung</i>, die mit Ihrem Schloss geliefert wurde. • „Unterstützte Assa-Abloy-IP-Schlösser“ im <i>Synergis™ Software – Integrationshandbuch</i>.
2	Konfigurieren Sie das IP-Schloss mithilfe des LCT. <ul style="list-style-type: none"> • Konfigurieren Sie die Host-Adresse des IP-Schlusses so, dass sie mit der IP-Adresse der Synergis™-Einheit übereinstimmt. • Konfigurieren Sie den Kommunikationsport des IP-Schlusses, den die Synergis™ -Einheit beim Erkennen der Schlösser als Abhörport verwenden wird (Default=2571). • Wenn eine Verschlüsselung erforderlich ist, stellen Sie den AES-Schlüssel im Schlossprofil ein. Sie benötigen diesen Schlüssel, nachdem Sie das IP-Schloss mit der Synergis™-Einheit gepaart haben. 	<ul style="list-style-type: none"> • <i>Netzwerk und Lock Configuration Tool Benutzerhandbuch</i>, das mit Ihrem Schloss geliefert wurde.
3	Stellen Sie die Kommunikation zwischen der Synergis™-Einheit und den angeschlossenen IP-Schlössern im Synergis™ Appliance Portal her.	<ul style="list-style-type: none"> • Assa-Abloy-IP-Schlösser registrieren, die mit der Synergis™-Einheit verbunden sind auf Seite 94.

Informationen zur Funktion Funkaktivierungsereignisse für Assa Abloy-WiFi-Schlösser

Aktivierungsereignisse ist eine konfigurierbare Funktion bei allen Assa Abloy-WiFi-Schlössern, mit der Sie die Ereignisse auswählen können, welche die Schlösser sofort über WiFi-Funk an den Controller melden müssen.

Funktionsweise

Standardmäßig aktivieren die Ereignisse *Tür gewaltsam geöffnet* und *Tür zu lange geöffnet* den WiFi-Funk des Schlosses, um diese Ereignisse zu melden, wenn sie auftreten. Verwenden Sie die Option **Aktivierungsereignisse** für jedes einzelne Schloss, um die Ereignisse auszuwählen, die den WiFi-Funk aktivieren. Ereignisse, die nicht zum Aktivieren des WiFi-Funks ausgewählt wurden, werden bei der nächsten WiFi-Funkaktivierung gemeldet.

So minimieren Sie den Batterieverbrauch bei WiFi-Schlössern

Bei einigen Installationen kann die Lebensdauer der Batterie kurz sein, weil die Schlösser viele *Tür offen gehalten*-Ereignisse erzeugen, die den WiFi-Funk aktivieren. Deren Batterielebensdauer kann verlängert werden, wenn die Meldung von *Tür offen gehalten*-Ereignissen bei der nächsten planmäßigen oder außerplanmäßigen Funkaktivierung akzeptiert wird. Um die Lebensdauer der Batterie zu verlängern, stellen Sie die Option **Aktivierungsereignisse** für diese Schlösser auf *Nur gewaltsam geöffnete Türen*. Die *Tür gewaltsam geöffnet*-Ereignisse aktivieren den WiFi-Funk und die *Tür offen gehalten*-Ereignisse werden bei der nächsten WiFi-Funkaktivierung gemeldet.

Konfiguration der Funktion Funkaktivierungsereignisse für Assa-Abloy-WLAN-Schlösser

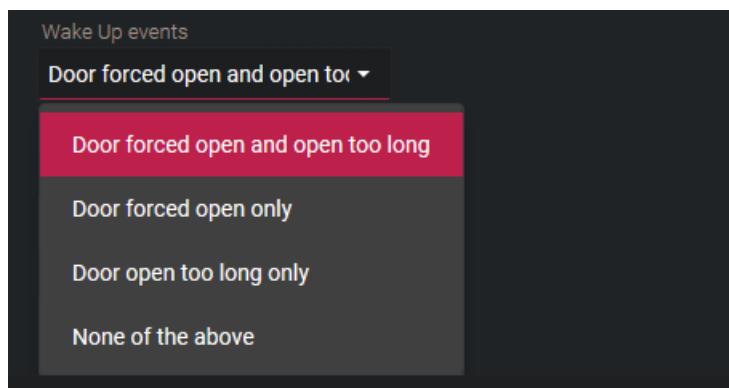
Sie können einzelne Assa-Abloy-WLAN-Schlösser so konfigurieren, dass sie bei bestimmten Aktivierungsereignissen den Controller über WLAN-Funk kontaktieren.

Bevor Sie beginnen

Registrieren Sie das Assa Abloy-IP-Schloss.

Was Sie noch wissen sollten

Sie können für jedes Assa Abloy-WLAN-Schloss ein Aktivierungsereignis konfigurieren.



Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Wählen Sie **Assa Abloy IP**, und wählen Sie dann den Assa Abloy-Kanal und das Schloss.
- 4 Stellen Sie die Option **Aktivierungsereignisse** für das Schloss ein.
- 5 Klicken Sie auf **Anwenden**.

Aktivierung des Flucht- und Rückkehrmodus bei Assa Abloy-IP-Schlössern mit Korpustyp 8200 und überwachtem Riegel

Um den *Flucht- und Rückkehrmodus* an Türen zu aktivieren, die von Assa Abloy-IP-Schlössern gesteuert werden, müssen Sie ein boolesches benutzerdefiniertes Feld mit dem Namen *Flucht- und Rückkehrmodus* für Türen erstellen und es an den Türen, an denen Sie diese Funktion aktivieren möchten, auf TRUE setzen.

Bevor Sie beginnen

Die Assa Abloy-IP-Schlösser, die die Funktion *Flucht und Rückkehr* unterstützen, sind die Modelle mit Schlosskörper 8200 und überwachtem Riegel.

Zum Beispiel:

- IN120 und IN220 8200 Einsteckschloss mit Riegel. Keine anderen IN120- und IN220-Schlösser unterstützen diese Funktion.
- Passport 1000 P2 Einsteckschloss mit Riegel. Keine anderen Passport 1000 P2-Schlösser unterstützen diese Funktion.

Was Sie noch wissen sollten

Die kanadischen Brandschutzvorschriften besagen, dass eine Tür niemals automatisch wiederverriegelt werden darf. Wenn die Flucht- und Rückkehr-Funktion aktiviert ist, sind daher die folgenden Funktionen deaktiviert.

- Entriegelungszeitpläne
- Wartungsmodus
- Manuelle Entriegelung vom Security Desk
- Temporäres Überschreiben der Zeitpläne vom Security Desk

Wenn die Flucht- und Rückkehrfunktion aktiviert ist, bleibt die Tür nach dem Verlassen durch den Karteninhaber so lange unverschlossen, bis der Karteninhaber seine Zutrittskarte vorlegt, um die Tür zu schließen. Wenn der Karteninhaber seine Karte nicht vorlegt, um die Tür zu verriegeln, bleibt die Tür während seiner Abwesenheit unverschlossen. Wenn der Karteninhaber zurückkehrt, muss er seine Zutrittskarte vorlegen, um die Tür zu öffnen. Nach Zutritt muss er den Riegel vorschieben, um die Tür zu verriegeln.

Prozedur

- 1 Erstellen Sie ein boolesches benutzerdefiniertes Feld für Türeinheiten, und nennen Sie es *Escape Return*. Schreiben Sie den Namen genau so, wie er geschrieben wird, mit Groß- und Kleinbuchstaben und mit Leerzeichen.
- 2 Öffnen Sie den Task *Bereichsansicht* und setzen Sie das benutzerdefinierte Feld **Escape Return** auf TRUE für alle Türen, für die diese Funktion aktiviert werden muss.
TIPP: Wenn Sie diese Funktion für viele Türen aktivieren müssen, empfehlen wir die Verwendung des *Copy Configuration Tool*.
- 3 (nur bei WiFi-Schlössern) Lösen Sie einen Funkweckruf aus, um die Flucht- und Rückkehrfunktion des Schlosses zu aktivieren.
Sie können eine Funkweckung auslösen, indem Sie die Abdeckung des Schlosses entfernen und die Taste drücken oder eine verweigerte Berechtigung vorlegen.

- 4 Durchlaufen Sie den *Flucht- und Rückkehrmodus* zum ersten Mal, indem Sie eine Tür verlassen und nach dem Schließen der Tür eine gültige Berechtigung vorlegen.
Dies veranlasst das System, die benutzerdefinierten Ereignisse zu erstellen, die Sie für die Konfiguration von Event-to-Actions verwenden können.

Zwei benutzerdefinierte Ereignisse werden zu Ihrem System hinzugefügt:

- **Escape Return Modus Start:** Entriegelung der Tür durch Verlassen oder durch Betreten mit einer gültigen Berechtigung.
- **Escape Return Modus Ende:** Die Tür wird mit einer gültigen Berechtigung oder durch Verschieben des Riegels von der Innenseite der Tür verschlossen.

Konfigurieren einer Persona-Seriennummer für die Schlösser IN120 und IN220

Bevor Sie den Durchgangsmodus bei SARGENT- und Corbin Russwin Cx-Schlössern IN120 und IN220 verwenden können, müssen diese mit einer PERSONA-Seriennummer konfiguriert werden.

Prozedur

- 1 Schließen Sie das Schloss an eine Arbeitsstation an und öffnen Sie die Schlosskonfigurationsdatei mit dem LCT-Tool.
- 2 Klicken Sie auf der Seite *Schlosskonfiguration* auf das Symbol **Einstellungen**.
- 3 Klicken Sie auf die Registerkarte **Seriennummer einrichten**.
- 4 Ändern Sie **Hersteller** und **Boardtyp** in *Persona*.
- 5 Übernehmen Sie die Änderungen und folgen Sie den Anweisungen auf dem Bildschirm. Das Schloss hat jetzt eine neue Seriennummer.
- 6 Verwenden Sie LCT, um die Konfiguration erneut auf das Schloss anzuwenden.
- 7 Wenn das Schloss bereits zur Synergis™-Einheit hinzugefügt wurde, gehen Sie wie folgt vor:
 - a) Löschen Sie das Schloss und fügen Sie es mit der neuen Seriennummer wieder hinzu.
 - b) Konfigurieren Sie die Hardware der Türeinheit mit dem neuen Schloss neu.

Informationen zum Durchgangsmodus für Assa Abloy-IP-Schlösser

Der Durchgangsmodus ist eine Funktion, die für alle Assa Abloy-IP-Schlösser verfügbar ist. Diese Funktion ermöglicht es autorisierten Karteninhabern, Schlösser im entriegelten Zustand zu halten, indem sie sich je nach Schlosscontroller oder Marke einmal oder zweimal am Lesegerät ausweisen. Durch Wiederholung des Vorgangs wird das Schloss wieder in den Normalzustand versetzt.

Durchgangsmodus, ausgelöst durch einen einzelnen Ausweis

Das Folgende gilt für SARGENT Cx-Schlösser, Corbin Russwin Cx-Schlösser IN120 und IN220 und alle Sx-Schlösser. Wenn sich das Lesegerät im Modus *Karte oder PIN* oder *Karte und PIN* befindet, wird der Durchgangsmodus auf folgende Weise gestartet und beendet:

- **Karte oder PIN:** Entweder einmal ausweisen oder die PIN eingeben.
- **Karte und PIN:** Einmal ausweisen und dann die PIN eingeben.

BEMERKUNG: Karteninhaber müssen eine Sicherheitsfreigabe über 7 haben.

Durchgangsmodus ausgelöst durch doppeltes Ausweisen

Das Folgende gilt für bestimmte Schlösser:

- Alle Px-Schlösser
- Sx-Schlösser mit Hx-Firmware
- SARGENT Cx-Schloss Passport 1000 P1 und P2
- Corbin Russwin Cx-Schlösser Access 700 PIP1 und PWI1
- SARGENT- und Corbin Russwin Cx-Schlösser IN120 und IN220 mit einer PERSONA Seriennummer

BEMERKUNG: Die Schlösser IN120 und IN220 können entweder bestellt oder manuell konfiguriert werden.

- **Karte oder PIN:** Zweimal ausweisen, um den Durchgangsmodus zu starten. Die PIN kann nicht verwendet werden.
- **Karte und PIN:** Einmal ausweisen, PIN eingeben und erneut ausweisen, um den Durchgangsmodus zu starten.

Durchgangsmodus pro Tür oder pro Zutrittsregel aktiviert

Sie können die Funktion Durchgangsmodus entweder über ein benutzerdefiniertes Feld für Türen oder für Zutrittsregeln aktivieren. Die gleichzeitige Verwendung beider benutzerdefinierter Felder wird nicht empfohlen. Wenn der Durchgangsmodus über ein benutzerdefiniertes Türfeld aktiviert ist, kann jeder, der Zutritt zur Tür hat, den Durchgangsmodus verwenden. Wenn der Durchgangsmodus über ein benutzerdefiniertes Feld für eine Zutrittsregel aktiviert ist, können Sie die Funktion auf bestimmte Türen und Karteninhaber beschränken.

Aktivieren des Durchgangsmodus an Assa Abloy-IP-Schlössern

Um den Durchgangsmodus an Türen zu aktivieren, die von Assa Abloy-IP-Schlössern gesteuert werden, müssen Sie ein boolesches benutzerdefiniertes Feld mit dem Namen *PassageMode* entweder für Türen oder Zutrittsregeln erstellen.

Bevor Sie beginnen

- [Erfahren Sie mehr über die Durchgangsmodus-Funktion.](#)
- [Konfigurieren Sie eine Persona-Seriennummer für die IN120- und IN220-Schlösser.](#)

Prozedur

So aktivieren Sie die Durchgangsmodus-Funktion pro Tür:

- 1 Erstellen Sie im Config Tool ein boolesches benutzerdefiniertes Feld für Türeinheiten und nennen Sie es *PassageMode*.
BEMERKUNG: Schreiben Sie den Namen genau so, wie er geschrieben wird, mit Groß- und Kleinbuchstaben.
- 2 Öffnen Sie den Task *Bereichsansicht*.
- 3 Wählen Sie im Entitätsbrowser eine Tür und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Felder**.
- 4 Wählen Sie das benutzerdefinierte Feld **PassageMode**, und klicken Sie dann auf **Anwenden**.
- 5 Wiederholen Sie die beiden vorherigen Schritte für alle Türen, für die Sie den Durchgangsmodus aktivieren möchten.

So aktivieren Sie die Durchgangsmodus-Funktion pro Zutrittsregel:

- 1 Melden Sie sich an der Synergis™-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Nachgelagerte Controllereinstellungen**.
- 3 Wählen Sie im Abschnitt *Einstellungen für Assa Abloy IP-Schlösser* die Option **Aktivieren des Durchgangsmodus per Zutrittsregel**.
- 4 Klicken Sie auf **Speichern**.
- 5 Starten Sie Ihre Synergis™-Einheit neu.
Das benutzerdefinierte Feld *PassageMode* für Zutrittsregeln wird automatisch im Security Center erstellt.
- 6 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Zutrittsregeln**.
- 7 Wählen Sie im Entitätsbrowser eine Zutrittsregel und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Felder**.
- 8 Wählen Sie das benutzerdefinierte Feld **PassageMode**, und klicken Sie dann auf **Anwenden**.
- 9 Wiederholen Sie die beiden vorangegangenen Schritte für alle Zutrittsregeln, für die Sie den Durchgangsmodus aktivieren möchten.

Aktivierung des Privatsphärenmodus bei Assa Abloy-IP-Schlössern ohne überwachten Riegel

Um den *Privatsphärenmodus* über Config Tool an Türen zu aktivieren, die von Assa Abloy-IP-Schlössern gesteuert werden, müssen Sie ein boolesches benutzerdefiniertes Feld namens *Privacy Mode* für Türen erstellen und es an den Türen, an denen Sie diese Funktion aktivieren möchten, auf TRUE setzen.

Bevor Sie beginnen

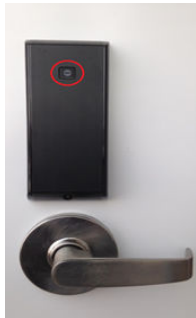
Die Assa Abloy-IP-Schlösser, die den Privatsphärenmodus unterstützen, sind die PoE- und WiFi-Schlösser vom Typ Cx.

Was Sie noch wissen sollten

Der Privatsphärenmodus ist eine Assa Abloy-IP-Schlossfunktion, die nur Supervisoren (*übergeordnete Karteninhaber*) Zutritt gewährt. Diese Funktion ist standardmäßig deaktiviert.

Die folgenden Informationen beschreiben, wie diese Funktion arbeitet. Zum Aktivieren des Privatsphärenmodus drücken Sie bei geschlossener Tür die *Privatsphärentaste* an der Innenseite der Tür. Die LED an der Taste blinkt etwa 2 Minuten lang langsam, um anzuzeigen, dass der Privatsphärenmodus aktiviert ist. Bei Schlössern, die mit einem überwachten Riegel ausgestattet sind, entspricht diese Aktion dem Verschieben des Riegels.

BEMERKUNG: Wenn das Lesegerät einen Piepton abgibt und 5 Mal lila blinkt, wenn Sie die *Privatsphärentaste* drücken, kann der Privatsphärenmodus nicht aktiviert werden, da die Tür offen ist.



Alle Karteninhaber mit einer Sicherheitsfreigabe von weniger als sieben fungieren als Supervisor. Der Privatsphärenmodus wird deaktiviert, wenn die Tür von innen geöffnet wird, oder wenn sich ein Supervisor ausweist.

Prozedur

- 1 Erstellen Sie ein boolesches benutzerdefiniertes Feld für Türeinheiten, und nennen Sie es *Privacy Mode*. Schreiben Sie den Namen genau so, wie er geschrieben wird, mit Groß- und Kleinbuchstaben und mit Leerzeichen.
- 2 Öffnen Sie den Task *Bereichsansicht* und setzen Sie das benutzerdefinierte Feld **Privacy Mode** auf TRUE für alle Türen, für die diese Funktion aktiviert werden muss.

TIPP: Wenn Sie diese Funktion für viele Türen aktivieren müssen, empfehlen wir die Verwendung des *Copy Configuration Tool*.

Zwei benutzerdefinierte Ereignisse werden zu Ihrem System hinzugefügt:

- **Türriegel geschlossen:** Dieses Ereignis wird ausgelöst, wenn der Privatsphärenmodus an einer Tür aktiviert wird.

- **Türriegel geöffnet:** Dieses Ereignis wird ausgelöst, wenn der Privatsphärenmodus an einer Tür deaktiviert wird.

Assa-Abloy-IP-Schlösser registrieren, die mit der Synergis™-Einheit verbunden sind

Damit die Synergis™-Einheit mit den angeschlossenen Assa-Abloy-IP-Schlössern kommunizieren kann, müssen Sie sie im Synergis™ Appliance Portal mit dem *Schloss-Kopplungsmodus* koppeln.

Bevor Sie beginnen

Konfigurieren Sie die IP-Schlösser mit dem Lock Configuration Tool (LCT). Wenn die Verschlüsselung aktiviert ist, notieren Sie den **Lock AES Key**.

Was Sie noch wissen sollten

Wenn der Kopplungsmodus für Schlösser aktiv ist, werden alle IP-Schlösser erkannt, die über die angegebenen Kommunikationsports mit der Synergis™-Einheit verbunden sind. Nach Beendigung des Kopplungsmodus stellt die Synergis™-Einheit die Verbindung zum Access Manager im Security Center wieder her und fügt die gekoppelten IP-Schlösser hinzu.

BEMERKUNG: Die mit *Härtung* gekennzeichneten Schritte und Anweisungen sind optional, schützen Ihr System aber vor Cyberangriffen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie in der Liste **Hardwaretyp** die Option **Assa-Abloy-IP** aus.

- 5 (Optional) Wählen Sie im Feld **Timeout**, wie lange der Kopplungsmodus des Schlosses aktiviert werden soll. Neue IP-Schlossverbindungen werden nur für die von Ihnen angegebene Zeitspanne gekoppelt.
BEMERKUNG: Sichern Sie die Konfigurationsdatei der Synergis™-Einheit für den Fall, dass Sie die Einheit irgendwann ersetzen müssen, insbesondere wenn Sie viele WLAN-Schlösser haben, da es länger dauert, sie neu zu registrieren.

- 6 Wenn Sie einen anderen Port als den Standardport 2571 verwenden, geben Sie im Feld *TCP-Port* den Kommunikationsport ein, den Sie auf den IP-Schlössern konfiguriert haben.
- 7 Wenn Sie Verschlüsselung über LCT aktiviert haben, gebe Sie im Feld *AES-Standortschlüssel* den AES-Schlüssel (32-stellige hexadezimale Zeichenfolge) ein, der auf Ihrem Schloss konfiguriert ist.
BEMERKUNG: Sie können den AES-Schlüssel auf der Seite *Hardware* der Synergis™-Einheit im Config Tool bearbeiten oder entfernen.
- 8 (Optional) Wenn Sie möchten, dass die IP-Schlösser hinzugefügt werden, sobald sie erkannt werden, gehen Sie wie folgt vor:
- Wählen Sie die Option **Schlösser bei Erkennung hinzufügen**.
WICHTIG: Wenn diese Option ausgewählt ist, stellt die Synergis™-Einheit nach dem Hinzufügen jeder Gruppe von IP-Schlössern die Verbindung zum Access Manager wieder her. Diese Option

wird nur empfohlen, wenn Sie mit der Konfiguration der IP-Schlösser beginnen müssen, bevor der Kopplungsmodus abgeschlossen ist.

- b) Wählen Sie aus der Option **Verzögerung vor dem Hinzufügen von Schlössern**, wie viele Sekunden vergehen müssen, bevor die zuvor erkannten Schlösser hinzugefügt werden.
- 9 Klicken Sie auf **Koppelung staten**.
- WICHTIG:** Bei WiFi-Schlössern drücken Sie die COM- oder Reset-Taste in der Rückseite des Schlosses, um eine Verbindung mit der Synergis™-Einheit herzustellen.
- Die IP-Schlösser werden erkannt und der Tabelle hinzugefügt.
- Wenn Sie Probleme haben, das Schloss mit der Synergis™-Einheit zu koppeln, [testen Sie die Verbindung zwischen Ihrem IP-Schloss und der Einheit](#).
- 10 Führen Sie eine der folgenden Aktionen aus:
- Um den Schlosskoppelungsmodus zu beenden und die erkannten Schlösser hinzuzufügen, klicken Sie auf **Beenden und speichern**.
 - Um den Koppelungsmodus zu beenden, klicken Sie auf **Abbrechen**.
BEMERKUNG: Wenn die Option **Schlösser bei Erkennung hinzufügen** ausgewählt ist, wurden möglicherweise bereits einige Schlösser hinzugefügt.
 - Warten Sie, bis der Schlosskopplungsmodus beendet ist.
- Die Synergis™-Einheit stellt die Verbindung zur Access Manager-Rolle wieder her und die erkannten Schlösser werden hinzugefügt.
- 11 Klicken Sie auf **Konfiguration > Hardware**.
- Die hinzugefügten IP-Schlösser werden in der Hardware-Konfigurationsstruktur angezeigt. Wenn Sie ein Schloss auswählen, werden der Gerätetyp, die Seriennummer und die Schlossfirmware des gewählten IP-Schlusses unter *Eigenschaften* angezeigt.

12 Wenn unter *Eigenschaften* keine Informationen angezeigt werden, aktualisieren Sie die Seite.

Bei WLAN-Schlössern kann es bis zu zwei Minuten dauern, bis die Informationen unter *Eigenschaften* angezeigt werden. WiFi-Schlösser erscheinen in der Hardwarestruktur in Rot, da sie nicht in ständiger Kommunikation mit der Synergis™-Einheit stehen.

- a) Für PoE-Schlösser: Stellen Sie unter *Eigenschaften* sicher, dass **Funkaktivierung** auf **Immer ein** eingestellt ist, damit *Zutritt erlaubt*-Ereignisse im Security Center nie verpasst werden, und setzen Sie **Batterieüberprüfungseinstellung** auf **Aus**.
- b) Für WiFi-Schlösser: Stellen Sie unter *Eigenschaften* sicher, dass **Funkaktivierung** auf **Täglich** eingestellt ist, und geben Sie die Tageszeit (**Stunde** und **Minute**) ein, zu der die Aktivierung erfolgen soll.
Wählen Sie **Lokalzeit**, wenn Sie möchten, dass die Funkaktivierungszeit der Zeitzone der Synergis™-Einheit folgt. Wenn Sie diese Option nicht wählen, ist die Standardeinstellung UTC.
- c) Ändern Sie die anderen Schlosseinstellungen nach Bedarf.

Assa Abloy IP

Properties

Serial number

Type
PoE

Current Synergis™ appliance firmware

Configuration

Radio wakeup
Always on

Wake Up events
Door forced open and open to

Fail setting
Fail secure

Battery check setting
Off

Disable relock settings

Firmware type
Default

⚠ Reset to factory settings

Cancel Save

13 Klicken Sie auf **Speichern**.

Testen der Verbindung zwischen Ihrem IP-Schloss und der Synergis™-Einheit

Wenn Sie Probleme haben, die Synergis™-Einheit mit Ihrem IP-Schloss zu koppeln, können Sie die Verbindung zwischen dem Schloss und der Einheit mit dem Lock Configuration Tool (LCT) testen.

Prozedur

- 1 Für PoE-Schlösser siehe den Befehl **Ping Test** im LCT.
- 2 Für WiFi-Schlösser siehe den Befehl **Verbindung zum Host prüfen** im LCT.

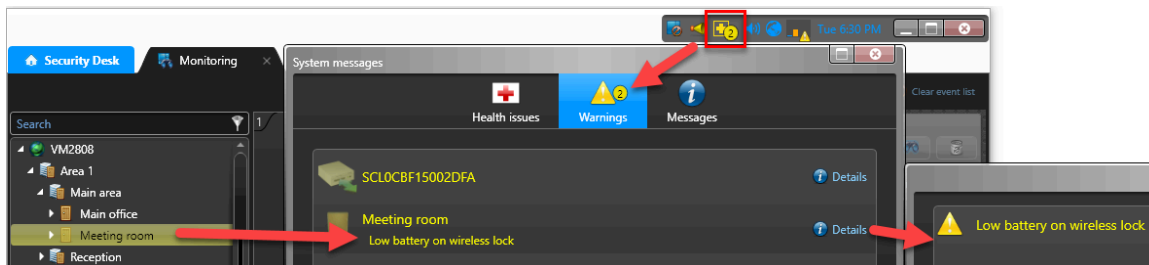
Überwachung des Batteriestatus von WiFi-Schlössern

Um den Batteriestatus eines Assa Abloy IP-WiFi-Schlusses zu überprüfen, können Sie das Ereignis *Batteriefehler* an der Synergis™-Einheit überwachen, mit dem es verbunden ist.

Was Sie noch wissen sollten

Für jedes WiFi-Schloss erstellt Security Center einen virtuellen Eingang mit dem Namen *Eingang BatteryFail*, der als *Aktiv* in der Registerkarte **Überwachung** und als gelbe Warnung auf dem Symbol **Systemmeldungen** in der Benachrichtigungsleiste angezeigt wird, wenn der Akku schwach ist.

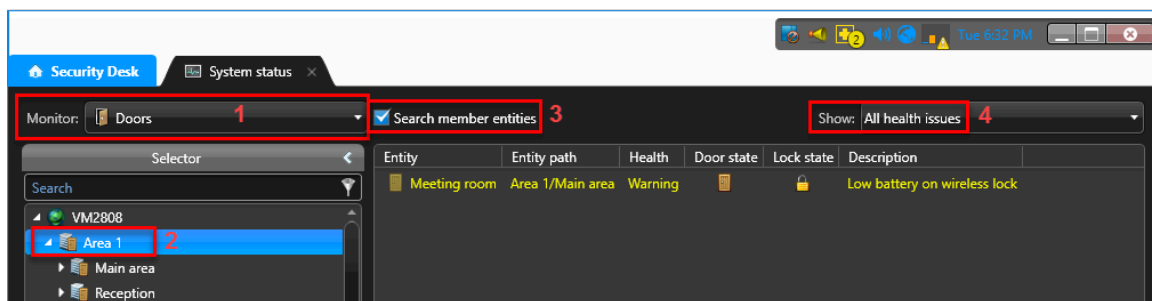
BEMERKUNG: Der *Eingang BatteryFail* ist ein Software-Eingang, der zur Anzeige des Batteriestatus von WiFi-Schlössern dient. Sie können kein physisches Gerät an diesen Eingang anschließen.



Prozedur

- 1 Öffnen Sie auf der Security Desk-Startseite den Task *Systemstatus*.
- 2 Wählen Sie in der Liste **Überwachung** den Eintrag **Türen**.
- 3 Wählen Sie im Einheitendiagramm den übergeordneten Bereich aus.
- 4 Aktivieren Sie das Kontrollkästchen **Mitgliederentitäten suchen**, um alle Schlösser unter den untergeordneten Bereichen anzuzeigen.
- 5 Wählen Sie in der Liste **Anzeigen** die Option **Alle Funktionsprobleme**, um die Türen mit Warnungen anzuzeigen.

BEMERKUNG: Die WLAN-Schlösser, die Probleme mit der Batterie haben, zeigen den Status *Aktiv* für **Eingang - Batterieausfall** an.



- 6 Planen Sie einen Batteriewechsel für die WiFi-Schlösser, die eine Warnung vor einer schwachen Batterie aufweisen.

AutoVu-SharpV-Kameras

Dieser Abschnitt enthält die folgenden Themen:

- ["Registrieren Sie die AutoVu™ SharpV-Kamera in der Synergis™-Einheit."](#) auf Seite 102
- ["Eine SharpV-Kamera zur Steuerung einer Fahrzeugzutrittssperre konfigurieren:"](#) auf Seite 105

Registrieren Sie die AutoVu™ SharpV-Kamera in der Synergis™-Einheit.

Damit die Synergis™-Einheit mit der SharpV-Kamera kommunizieren kann, müssen Sie die Kamera an der Synergis™-Einheit im Security Center registrieren.

Bevor Sie beginnen

- Konfigurieren Sie die SharpV-Kamera für die Verwendung von HTTPS-Kommunikation. Weitere Informationen finden Sie im *Bereitstellungshandbuch* oder *Handbuch* für die zu installierende Kamera.
- Installieren Sie entweder das selbstsignierte Genetec™-Zertifikat oder ein signiertes Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle.
- Wenn Sie eine SharpV-Kamera registrieren, melden Sie sich auf dem SharpV-Webportal an und ändern Sie das Standardpasswort.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **AutoVu** in der Liste **Hardwaretyp** aus.
- 5 Wählen Sie einen **Kanal** aus.
- 6 Geben Sie die **IP-Adresse** der Kamera ein.
- 7 Geben Sie den **Port** der Kamera ein.
Die SharpV verwendet **Port** 443 für die HTTPS-Kommunikation mit Security Center.
- 8 Wählen Sie in der Liste **Schnittstellentyp** die Option **SharpV**.
- 9 Geben Sie den **Benutzernamen** und das **Passwort** ein, die für den Zugriff auf das SharpV-Webportal verwendet werden.

BEMERKUNG: Für SharpV-Kameras können Sie das Standardpasswort nicht verwenden.

10 Klicken Sie auf **Hinzufügen**, dann **Speichern**.

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

- Hardware type: AutoVu
- Channel: LAN1
- IP address: 10.0.12.13
- HTTP port: 443
- Interface module type: SharpV
- Username: admin
- Password: [masked with 7 dots]

At the bottom of the dialog, there is an 'Add' button with a mouse cursor over it, a 'Cancel' button, and a 'Save' button.

- 11 Klicken Sie auf der Seite *Hardwarekonfiguration* auf die registrierte AutoVu™-Kamera und dann auf ihren Kanal und ihre Schnittstelle, um ihre Eigenschaften anzuzeigen.
- 12 Wenn Sie die SharpV-Ausgänge zur Steuerung einer Fahrzeugzutrittssperre verwenden, wählen Sie, ob die Ausgänge *Normalerweise offen* oder *Normalerweise geschlossen* sind.
- 13 Lassen Sie das Feld **Öffentlicher HTTPS-Schlüssel** leer. Diese Informationen werden auf der Grundlage des Kamerazertifikats automatisch hinzugefügt.
- 14 Das Kontrollkästchen **Teilweise Übereinstimmung erlauben** ist standardmäßig aktiviert. Diese Funktion akzeptiert Nummernschilder, die sich um ein Zeichen von einer konfigurierten Nummernschildberechtigung unterscheiden; dies umfasst das Einfügen, Löschen oder Ersetzen eines

Zeichens an einer beliebigen Stelle der Nummer. Wenn diese Funktion aktiviert ist, werden verschmutzte oder beschädigte Nummernschilder mit größerer Wahrscheinlichkeit erkannt.

AutoVu 10.0.12.13

Properties

IP address: 10.0.12.13 HTTP port: 443

Username: admin Password:

Output 1: Normal state closed

Output 2: Normal state closed

HTTPS public key: 3082010A0282

Allow partial matches

[Reset to factory settings](#) Cancel Save

15 Klicken Sie auf **Speichern**.

Im Config Tool wird die SharpV-Kamera auf der Seite *Peripheriegeräte* der Synergis™-Einheit angezeigt, und die Ein- und Ausgänge werden unter der SharpV-Kamera angezeigt.

Name	Type	State	Additional info	Controlling
Genetec Inc-AutoVu-Genetec Inc-SharpV Ir...		Offline		
Input IN_01	In	Unknown	Normally closed/Not supervis...	
Input IN_02	In	Unknown	Normally closed/Not supervis...	
Output OUT_01	Out	Unknown	---	
Output OUT_02	Out	Unknown	---	
Reader READER_01	Reader	Unknown	Type of reader: Wiegand	

Eine SharpV-Kamera zur Steuerung einer Fahrzeugzutrittssperre konfigurieren:

Um eine SharpV-Kamera zur Steuerung einer Fahrzeugzutrittssperre zu verwenden, muss die Sperre in Security Center als Tür konfiguriert sein.

Bevor Sie beginnen

- Schließen Sie die Fahrzeugzutrittssperre an die Synergis™-Appliance an. Weitere Informationen finden Sie im *Hardware-Installationshandbuch* für die zu installierende Zutrittskontroll-Appliance.
- Registrieren Sie die Synergis-Einheit in Security Center.
- [Registrieren Sie die SharpV-Kamera auf der Synergis™-Einheit.](#)

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Bereichsansicht*.
- 2 Wählen Sie den Bereich, in dem die Fahrzeugzutrittssperre hinzugefügt werden soll.
- 3 Klicken Sie auf **Eine Einheit hinzufügen** (+) und wählen Sie dann **Tür**.
- 4 Geben Sie im Assistenten für das **Erstellen einer Tür** den Namen und eine Beschreibung der Fahrzeugzutrittssperre ein.
- 5 Wählen Sie in der Liste **Standort** den Bereich aus, in dem Sie die Tür erstellen und klicken Sie auf **Weiter**.
- 6 Weisen Sie den Sperrenseiten auf der Seite *Tür-Information* Namen zu.
Beispiel: Ein/Aus oder Eingang/Ausgang.
- 7 So ordnen Sie die Sperre der Zutrittskontrolleinheit zu, mit der sie verdrahtet ist:
 - a) Wählen Sie aus der Liste **Zutrittskontrolleinheit** die Synergis™-Einheit aus.
 - b) Wählen Sie in der Liste **Schnittstellenmodul** die SharpV-Kamera.
- 8 Klicken Sie auf **Weiter**.
- 9 Prüfen Sie die Seite *Zusammenfassung des Anlegens* und klicken Sie auf **Erzeugen > Schließen**. Die Sperre wird im Einheitendiagramm angezeigt.
- 10 Wählen Sie die Sperre aus und klicken Sie dann auf die Registerkarte **Eigenschaften**.
- 11 Konfigurieren Sie das allgemeine Zutrittskontrollverhalten der Sperre. Weitere Informationen finden Sie im *Security Center – Administratorhandbuch*.
- 12 Klicken Sie auf **Übernehmen**.
- 13 .Klicken Sie auf die Registerkarte **Hardware** und beschreiben Sie die Verdrahtung zwischen der Zutrittskontrolleinheit und der Tür zu Security Center Weitere Informationen finden Sie im *Security Center – Administratorhandbuch*.
- 14 Erstellen Sie Karteninhaber, indem Sie ihre Nummernschilder als Berechtigungen verwenden. Weitere Informationen zum Erstellen von Karteninhabern finden Sie im *Security Center Benutzerhandbuch*. Wählen Sie bei der Zuweisung von Berechtigungen an den Karteninhaber die Option **Nummernschild**.
- 15 Legen Sie fest, wer Zutritt zur Tür hat. Weitere Informationen finden Sie im *Security Center – Administratorhandbuch*.

Axis-Controller

Dieser Abschnitt enthält die folgenden Themen:

- ["Anmeldung von Axis-Controllern an der Synergis™-Einheit"](#) auf Seite 107
- ["Peripheriegeräte des Axis-Controllers konfigurieren"](#) auf Seite 112
- ["Konfigurieren der zusätzlichen E/A-Ports von AXIS A1601-Controllern"](#) auf Seite 115
- ["Lesegerätanschlüsse am Axis-A1001-Controller"](#) auf Seite 117
- ["Lesegerätanschlüsse am AXIS A1601-Controller"](#) auf Seite 118
- ["OSDP \(Secure Channel\)-Lesegeräte auf AXIS-A1601-Steuerungen aktivieren"](#) auf Seite 119

Anmeldung von Axis-Controllern an der Synergis™-Einheit

Damit die Synergis™-Einheit mit Axis-Controllern kommunizieren kann, müssen Sie die Controller entweder über das Synergis™ Appliance Portal oder das Config Tool registrieren.

Bevor Sie beginnen

- Halten Sie die Seriennummern oder IP-Adressen Ihrer Axis-Controller bereit. Informationen zum Ermitteln dieser Angaben finden Sie in Ihrer Axis-Dokumentation.
- Schließen Sie Ihre Axis-Controller an die Synergis™-Einheit an.

Was Sie noch wissen sollten

Wenn an der Synergis™-Einheit ein Controller registriert wird, wird eine Standardkonfiguration für alle Axis-Eingangskontakte und Ausgangsrelais festgelegt. Axis und Synergis™ verwenden eine unterschiedliche Terminologie zur Beschreibung ihrer Einstellungen.

BEMERKUNG: Hier wird nur die Registrierung über das Synergis™ Appliance Portal beschrieben, aber Sie können einen Axis-Controller auch über **Config Tool > Zutrittskontrolle > Rollen und Einheiten** registrieren.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **Axis** als **Hardwaretyp** aus.
- 5 Wählen Sie den IP-Kanal, an den der Axis-Controller angeschlossen ist.

- 6 Geben Sie die Verbindungsparameter ein, die für die Verbindung mit dem Axis-Controller erforderlich sind.
- **IP-Adresse:** Verwenden Sie die IP-Adresse des Axis-Controllers.
 - **Schnittstellenmodultyp:** Wählen Sie den Typ der Axis-Einheit, die Sie registrieren möchten. Die Standardeinstellung ist A1001.
 - **Benutzername und Passwort:** Der Default-Benutzername und das Default-Passwort sind root bzw. pass.

The screenshot shows a dark-themed dialog box titled "Add hardware". It contains the following fields and controls:

- Hardware type:** A dropdown menu with "Axis" selected.
- Channel:** A dropdown menu with "AXIS" selected.
- IP address:** An empty text input field.
- Interface module type:** A dropdown menu with "A1001" selected.
- Username:** A text input field containing "root".
- Password:** A text input field containing four dots (masked).
- Below the fields, there are two labels: "Interface module type" and "IP address".
- At the bottom left is an "Add" button.
- At the bottom right are "Cancel" and "Save" buttons.

- 7 Klicken Sie auf **Hinzufügen**.
- 8 [Aktivieren Sie den Autonomen Modus](#) .
- 9 (Optional) Wiederholen Sie die Schritte 3 bis 8, um einen weiteren Axis-Controller hinzuzufügen.
- 10 Klicken Sie auf **Speichern**.

Der Hardwaretyp, der Kanal und das Schnittstellenmodul, das Sie gerade hinzugefügt haben, werden auf der Seite *Hardwarekonfiguration* angezeigt. Es kann bis zu einer Minute dauern, bis das Axis-Modul online geht.

- 11 Wenn die gegenwärtige Firmware-Version nicht die neueste ist, aktualisieren Sie sie, indem Sie eine der folgenden Optionen ausführen:
- Empfohlen für Security Center 5.10 oder neuer: Aktualisieren Sie die Firmware mithilfe des Tasks *Hardwareinventar* in Config Tool. Weitere Informationen finden Sie unter [Aktualisierung der Firmware und Plattform für Zutrittskontrollereinheiten und der Firmware für Schnittstellenmodule](#).
 - [Aktualisieren Sie die Firmware mit dem Synergis™ Appliance Portal](#).
- 12 Testen Sie die Verbindung und Konfiguration Ihres Schnittstellenmoduls auf der Seite *I/O-Diagnose*.
- BEMERKUNG:** Um das HTTPS-Protokoll zu verwenden, muss AXIS A1001 Firmware 1.65.2 oder neuer verwenden und A1601-Schnittstellen müssen Firmware 1.83.1.1 oder neuer verwenden.

Nach Durchführen dieser Schritte

Fügen Sie die Synergis™-Einheit einer Access Manager-Rolle hinzu, damit sie Teil Ihres Security Center-Systems wird.

Aktivieren des autonomen Modus an Axis-Controllern

Damit Ihre Axis-Einheiten unabhängig von einer Synergis™-Einheit Zugriffsentscheidungen treffen können, aktivieren Sie den *autonomen Modus* in Synergis™ Appliance Portal.

Was Sie noch wissen sollten

In Situationen mit hoher Latenz verbessert der *autonome Modus* die Verzögerung zwischen einem Kartenlese- und einem *Tür entriegelt*-Ereignis, indem die Fernautorisierung deaktiviert wird. Die Axis-Einheit sendet die Informationen an die Synergis™-Einheit, nachdem die Entscheidung getroffen wurde.

BEMERKUNG: Da der *autonome Modus* die Synergis™-Einheit nicht kontaktiert, um Zugangskontrollentscheidungen zu treffen, gibt es bestimmte Einschränkungen in Bezug auf die Aktivierung dieses Modus:

- Erweiterte Funktionen in Security Center sind deaktiviert.
- Änderungen an Berechtigungen, wie z. B. der Entzug des Zutritts einer Berechtigung, benötigen mehr Zeit, da die Änderungen während der Synchronisierung an die Axis-Einheit gesendet werden müssen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Wählen Sie in der Hardwarestruktur die Axis-Einheit aus, die Sie im *autonomen Modus* betreiben möchten. Das Konfigurationsfenster öffnet sich.

- 4 Aktivieren Sie das Kontrollkästchen **Autonomer Modus**.

The screenshot shows the 'General' settings page for an Axis controller with IP address 10.23.0.10. The settings are as follows:

- Physical address: 10.23.0.10
- Secure connection: Recommended
- HTTP port: 80
- HTTPS port: 443
- Username: root
- Password: (empty)
- HTTPS public key: 3082010A0282010100B3A1C867
- Extended held open time (seconds): 12
- Reader 1 is OSDP:
- Reader 2 is OSDP:
- Connection settings: Unencrypted
- Autonomous mode: (highlighted with a mouse cursor)

- 5 Klicken Sie auf **Speichern**.
- 6 (Optional) Wiederholen Sie die Schritte für alle Axis-Einheiten, die Sie im *autonomen Modus* betreiben möchten.

Die Axis-Einheit trifft eigenständig Entscheidungen über die Zutrittsgewährung und sendet dann Zutrittskontrollinformationen an die Synergis™-Einheit.

Härtung von Axis-Controllern

Es wird empfohlen, die IP-Adressfilterung auf dem Axis-Controller zu aktivieren, damit die IP-Adressen der Synergis™-Einheit und der Admin-Arbeitsstation eine Verbindung zum Controller herstellen können.

Bevor Sie beginnen

Prozedur

- 1 Melden Sie sich beim Webportal des Axis-Controllers an.
Weitere Informationen finden Sie in der Axis-Dokumentation.
- 2 Klicken Sie auf **Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Sicherheit > IP-Adressfilter**.
- 3 Wählen Sie die Option **IP-Adressfilterung/Produktsicherheitsempfehlungen von Axis Communications aktivieren** und dann **Erlauben** aus der Liste aus.
- 4 Klicken Sie auf **Übernehmen**.
- 5 Fügen Sie in der Liste *Gefilterte IP-Adressen* die IP-Adresse der Synergis™-Einheit und die IP-Adresse der administrativen Arbeitsstation hinzu, die sich beim Webportal des Axis-Controllers anmelden muss.

Beispiel:

- 6 Klicken Sie unter **Systemoptionen** auf **Netzwerk > TCP/IP > Erweitert**, und deaktivieren Sie die beiden Optionen **FTP-Server** und **RTSP-Server**.
Sie werden von der Synergis™ Software nicht verwendet.
- 7 Klicken Sie auf **Speichern**.

Peripheriegeräte des Axis-Controllers konfigurieren

Zum Konfigurieren der Eingangskontakte, Ausgangsrelais und Lesegeräte, die mit dem Axis-Controller verbunden sind, müssen Sie Ihre Änderungen im Config Tool und im Synergis™ Cloud Appliance Portal vornehmen.

Bevor Sie beginnen

- [Registrieren Sie den Axis-Controller auf der Synergis™-Einheit.](#)
- Fügen Sie die Synergis™-Einheit zur Access Manager-Rolle hinzu.

Was Sie noch wissen sollten

- Ausgangsrelais und Lesegeräte werden auf der Seite *Hardware* der Synergis™-Einheit im Synergis™ Appliance Portal oder im Config Tool konfiguriert.
- Eingangskontakte werden auf den Seiten *Hardware* und *Peripheriegeräte* der Synergis™-Einheit im Config Tool konfiguriert.

Prozedur

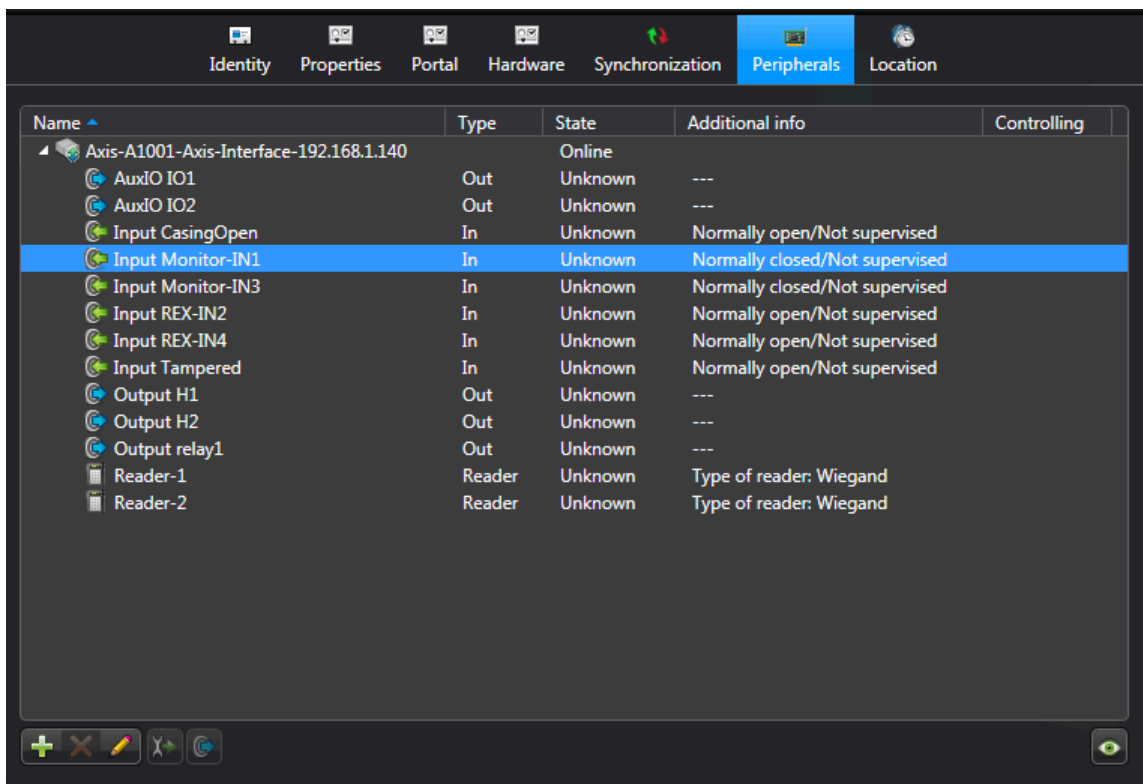
So konfigurieren Sie die Ausgangseinstellungen eines Axis-Controllers:

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 [Konfigurieren Sie bei A1601-Controllern die als Eingänge oder Ausgänge zu verwendenden Hilfs-E/A-Ports nach Bedarf.](#)
- 4 Für A1001-Controller konfigurieren Sie die Einstellungen nach Bedarf.
Weitere Informationen zu den einzelnen Einstellungen finden Sie in der Axis-Dokumentation.

So konfigurieren Sie die Eingangseinstellungen eines Axis-Controllers:

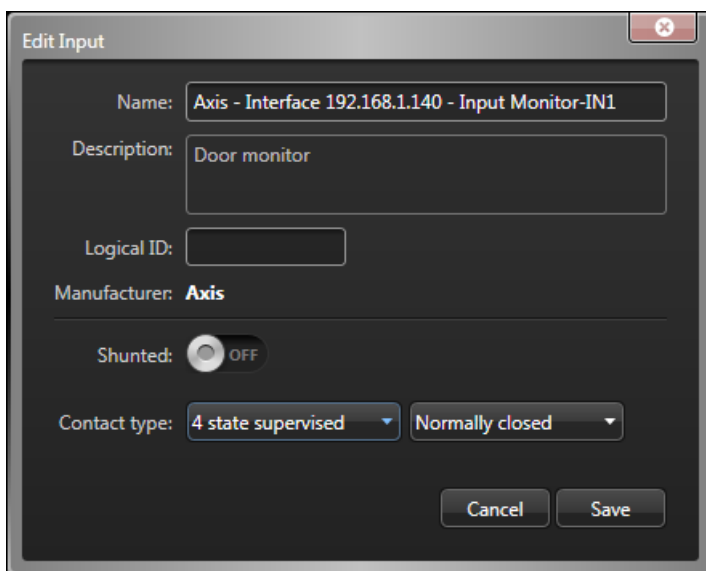
- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Wählen Sie in der Entitätsstruktur die Synergis-Einheit aus und klicken Sie auf die Registerkarte **Peripheriegeräte**.

- 3 Erweitern Sie den Achsenregler, den Sie ändern möchten, wählen Sie einen Eingang und klicken Sie dann auf **Bearbeiten** (✎).



- 4 Nehmen Sie im Dialogfeld *Eingabe bearbeiten* nach Bedarf Änderungen vor.

Beispiel:



BERMerkung: Die verfügbaren Einstellungen hängen von dem gewählten Eingang ab. Bei A1601-Geräten können E/A 1, 2, 3, 4, 13 und 14 nicht überwacht werden, wenn sie als Eingänge konfiguriert sind.

- **Name:** Name des Eingabegeräts.
- **Logische ID:** Muss für alle Peripheriegeräte eindeutig sein, die mit der gleichen Einheit verbunden sind.
- **Überbrückt:** Wählen Sie diese Option, um die Eingänge zu ignorieren. Nach der Überbrückung verbleibt der Eingangsstatus im Modus *Normal*, unabhängig davon, wie Sie ihn auslösen.

BEMERKUNG: Wenn das Öffnen der Tür erzwungen wird, wird das Ereignis *Öffnen der Tür erzwungen* weiterhin im Security Center erstellt, auch wenn der Türeingang parallel geschaltet ist.

- **Kontakttyp:** Legen Sie den Status *Normal* des Eingabekontakts und dessen Überwachungsmodus fest.
 - **Nicht überwacht/Normal geschlossen:** Der normale Status des Eingabekontakts ist geschlossen und die Zutrittskontrolleinheit berichtet nicht, ob die Eingabe einen Fehlerstatus aufweist.
 - **Nicht überwacht/Normal geöffnet:** Der normale Status des Eingabekontakts ist geschlossen und die Zutrittskontrolleinheit berichtet nicht, ob die Eingabe einen Fehlerstatus aufweist.
 - **4-fach überwacht/Normal geschlossen:** Der normale Status des Eingabekontakts ist geschlossen und die Zutrittskontrolleinheit berichtet, wenn die Eingabe einen Fehlerstatus aufweist.
 - **4-fach überwacht/Normal geöffnet:** Der normale Status des Eingabekontakts ist offen und die Zutrittskontrolleinheit berichtet, wenn die Eingabe einen Fehlerstatus aufweist.

5 Klicken Sie auf **Speichern** und dann auf **Anwenden**.

Konfigurieren der zusätzlichen E/A-Ports von AXIS A1601-Controllern

Sie können Hilfeingangsports und Hilfsausgangsports an AXIS-A1601-Controllern mithilfe des Synergis™ Appliance Portals so konfigurieren, dass sie als Eingänge oder Ausgänge fungieren.

Was Sie noch wissen sollten

- Wenn ein Hilfs-E/A bereits in einer Konfiguration verwendet wird und Sie seinen Typ ändern, wird der E/A offline geschaltet und Sie müssen diesen E/A manuell in der Konfiguration in Security Center aktualisieren.
- Standardmäßig sind die Hilfs-E/A 1 und 2 Ausgänge, und die Hilfs-E/A 3, 4, 13 und 14 sind Eingänge. Wenn sie als Eingänge konfiguriert sind, können sie nicht überwacht werden.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie auf die Axis-Einheit in der Spalte *Hardware* und dann in der Spalte *Kanäle*.
- 4 Klicken Sie in der Spalte *Schnittstellen* auf die Einheit, um deren Einstellungen zu öffnen.

- 5 Blättern Sie nach unten zum Abschnitt *Hilfs-E/As* und ändern Sie die **Hilfs-E/A-Typen**, wie erforderlich.
BEMERKUNG: Wenn Sie den Typ in einen Ausgang ändern, müssen Sie den Normalzustand als **Offen** oder **Geschlossen** konfigurieren. Der Normalzustand eines Eingangs kann nur im Config Tool konfiguriert werden.

The screenshot displays the configuration interface for an Axis-Controller, divided into three main sections: Inputs, Outputs, and Auxiliary I/Os.

- Inputs:** This section contains seven input parameters, each with a numerical value in a dark grey box:
 - 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
- Outputs:** This section contains two relay fail settings, each with a dropdown menu set to "Fail secure":
 - Relay 1 fail setting: Fail secure
 - Relay 2 fail setting: Fail secure
- Auxiliary I/Os:** This section contains eight auxiliary I/O configurations, each with a type dropdown and a normal state dropdown:
 - Aux IO 1 type: Output, Aux IO 1 normal state: Open
 - Aux IO 2 type: Output, Aux IO 2 normal state: Open
 - Aux IO 3 type: Input
 - Aux IO 4 type: Input
 - Aux IO 13 type: Input
 - Aux IO 14 type: Input

At the bottom of the interface, there are three buttons: "Set as default" (in red), "Reset to factory settings" (with a red warning triangle icon), "Cancel" (in grey), and "Save" (in red).

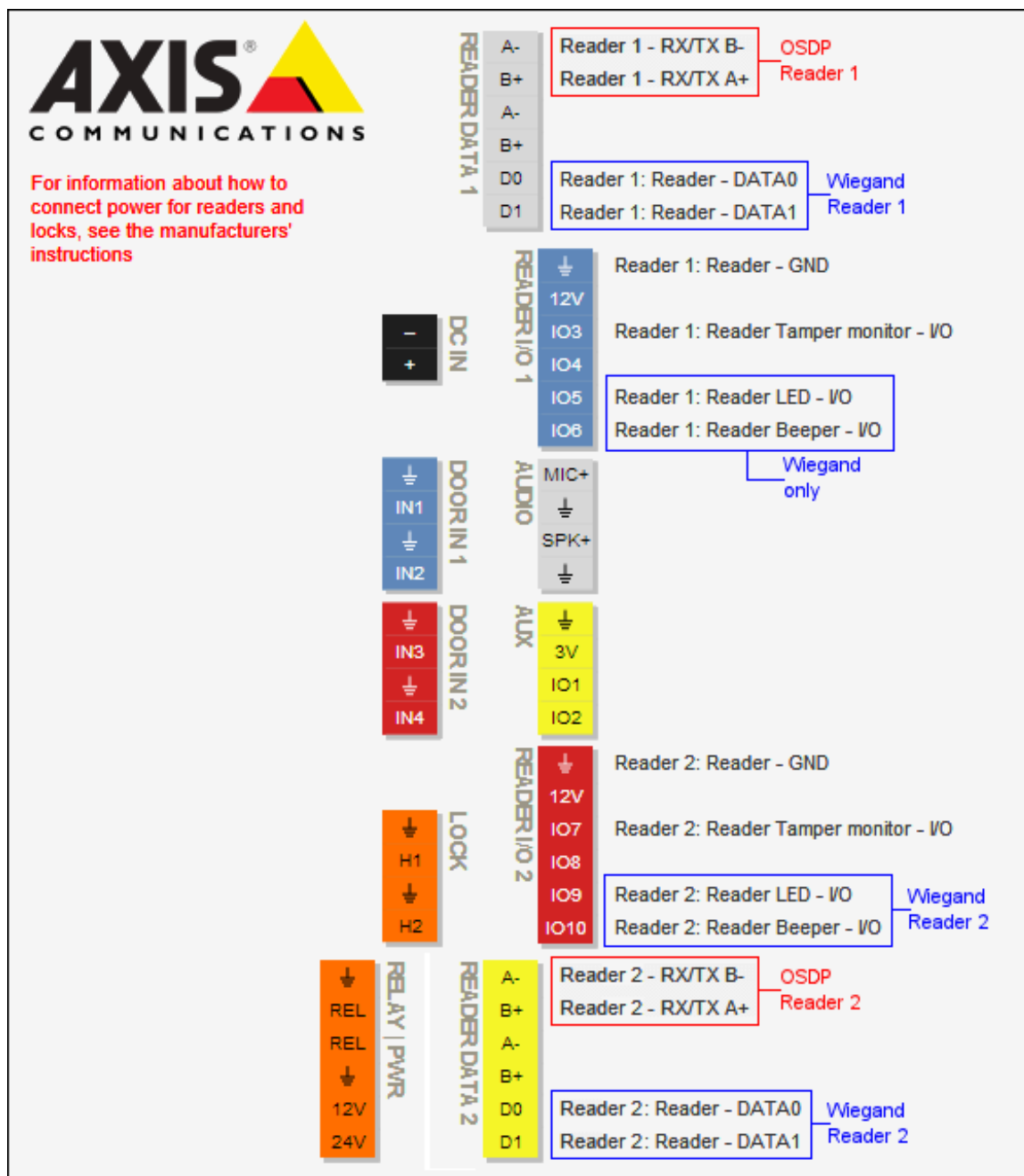
- 6 Klicken Sie auf **Speichern**.

Lesegerätanschlüsse am Axis-A1001-Controller

Jeder AXIS A1001-Controller unterstützt im Security Center Config Tool bis zu zwei Lesegeräte, die als Lesegerät 1 und Lesegerät 2 bezeichnet werden. Die Lesegeräte können entweder das Wiegand-Protokoll (Standardeinstellung) oder das OSDP-Protokoll verwenden. Für OSDP muss das Lesegerät mit dem ersten Satz von Lesegerätdaten **A-/B+** verbunden sein.

Die folgende Tabelle zeigt den Satz von Anschlüssen, die dem Lesegerät auf der Axis-Steuerung entsprechen.

BEMERKUNG: Diese Pintabelle wird nur angezeigt, wenn der Axis-Controller von der Synergis™-Einheit getrennt ist.



Lesegerätanschlüsse am AXIS A1601-Controller

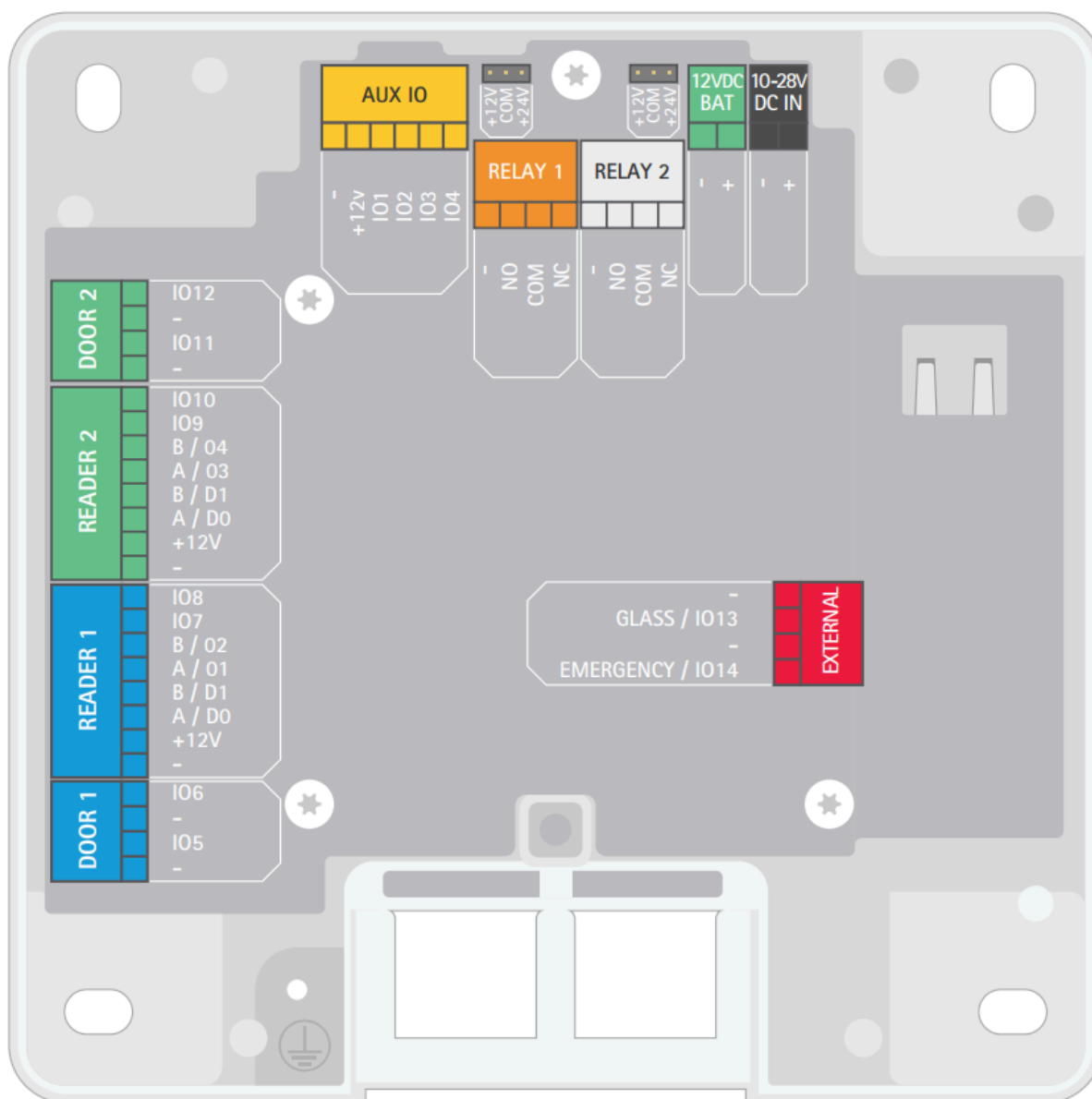
Jeder AXIS A1601-Controller unterstützt im Security Center Config Tool bis zu zwei Lesegeräte, die als *Lesegerät 1* und *Lesegerät 2* bezeichnet werden.

Die folgende Tabelle zeigt den Satz von Anschlüssen, die dem Lesegerät auf der Axis-Steuerung entsprechen.

Standardmäßig wird der A1601-Controller in Security Center wie folgt dargestellt:

- 8 Eingänge: 2 Türsensoren, 2 REX, 4 Hilfeingänge (E/A 3, 4, 13, und 14)
- 4 Ausgänge: 2 Türverriegelungsrelais, 2 Hilfsausgänge (E/A 1 und 2).

BEMERKUNG: Die Hilfs-E/As können entweder als Eingänge oder als Ausgänge konfiguriert werden.



OSDP (Secure Channel)-Lesegeräte auf AXIS-A1601-Steuerungen aktivieren

Sie können OSDP mit Secure Channel zwischen der AXIS-A1601-Steuerung und ihren OSDP-Lesegeräten verwenden, um End-to-End-Verschlüsselung sicherzustellen.

Was Sie noch wissen sollten

A1601-Steuerungen erfordern Firmware 1.84.4 oder neuer.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Wählen Sie in der Hardware-Struktur die Axis-Einheit aus, zu der Sie OSDP (Secure Channel)-Lesegeräte hinzufügen möchten.
Das Konfigurationsfenster öffnet sich.
- 4 Aktivieren Sie das Kontrollkästchen **Lesegerät ist OSDP** für das gewünschte Lesegerät.

Axis 10.23.11.28

General

Physical address	Secure connection
10.23.11.28	Recommended
HTTP port	HTTPS port
80	443
Username	Password
root	
HTTPS public key	
3082010A0282010100B3A1C867	
Extended held open time (seconds)	
12	
<input checked="" type="checkbox"/> Reader 1 is OSDP	<input type="checkbox"/> Reader 2 is OSDP
Connection settings	
Encrypted	
Specific key	

- 5 Wählen Sie in der Liste **Verbindungseinstellungen** die Option **Verschlüsselt** aus.

- 6 Geben Sie im Feld **Spezifischer Schlüssel** einen Schlüssel mit 128 Bit (32 hexadezimale Zeichen) ein.
Kopieren und fügen Sie einen bestehenden Schlüssel ein, wenn das Lesegerät zuvor für eine sichere Kommunikation konfiguriert wurde. Stellen Sie das Lesegerät andernfalls in den Installationsmodus ein (siehe Dokumentation des Lesegerätherstellers) und kopieren und fügen Sie den Schlüssel Ihrer Wahl ein.
- 7 Klicken Sie auf **Speichern**.

Der Schlüssel wird zum Axis key store hinzugefügt und wird für die Kommunikation mit dem Lesegerät verwendet.

DDS-Controller

Dieser Abschnitt enthält die folgenden Themen:

- ["Anmeldung von DDS RS-485-Controllern"](#) auf Seite 122
- ["Einstellung der physischen Adresse von TPL-Türcontrollern"](#) auf Seite 125

Anmeldung von DDS RS-485-Controllern

Damit die Synergis™-Einheit mit den an ihrer RS-485-Schnittstelle angeschlossenen DDS-Controllern kommunizieren kann, müssen Sie sie mit Synergis™ Appliance Portal registrieren.

Bevor Sie beginnen

Schließen Sie die DDS-Module wie folgt an die RS-485-Kanäle (A, B, C oder D) der Synergis™-Einheit an:

- Verbinden Sie Rx\L des DDS-Moduls mit dem "-" des Kanals.
- Verbinden Sie Tx\H des DDS-Moduls mit dem "+" des Kanals.
- Verbinden Sie 0v des DDS-Moduls mit dem "G" des Kanals.

Prozedur

- 1 Melden Sie sich bei der Synergis™Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **DDS** als **Hardwaretyp** aus.
- 5 Wählen Sie den **Kanal** (A, B, C oder D).
Alle Schnittstellenmodule, die mit demselben Kanal verbunden sind, müssen vom selben Hersteller stammen.

- 6 Fügen Sie im selben Dialogfeld alle Schnittstellenmodule hinzu, die mit demselben Kanal verbunden sind. Führen Sie eine der folgenden Aktionen aus:
- Zur manuellen Anmeldung geben Sie die am DDS-Modul konfigurierte physische Adresse (0 bis 31) ein und klicken auf **Hinzufügen (+)**. Wählen Sie dann den genauen Modultyp aus.

Add hardware

Hardware type
DDS

Channel
A3

Interface module type
TPL

Physical
2

Interface module type	Physical address
TPL	1

Add

Scan Cancel Save

Wiederholen Sie den Vorgang bei Bedarf, um alle an denselben Kanal angeschlossenen Module zu konfigurieren.

- Um die Anmeldung automatisch durchzuführen, klicken Sie auf **Scan**.

Die Ermittlungsfunktion sucht alle Schnittstellenmodule desselben Herstellers, die mit demselben Kanal verbunden sind, und registriert sie.

Wenn der Controller nicht alle angeschlossenen Schnittstellenmodule findet, [stellen Sie sicher, dass sie alle unterschiedliche physische Adressen](#) haben.

Sobald Sie auf **Hinzufügen** klicken, wechselt die Adresse im Feld **Physisch** zur nächsten verfügbaren Adresse.

- 7 Klicken Sie auf **Speichern**.
Der Hardwaretyp, der Kanal und das Schnittstellenmodul, das Sie gerade hinzugefügt haben, werden auf der Seite *Hardwarekonfiguration* angezeigt.
- 8 Wählen Sie jedes hinzugefügte Schnittstellenmodul auf der Seite *Hardwarekonfiguration* aus und konfigurieren Sie dessen Einstellungen.
Eine Beschreibung dieser Einstellungen finden Sie in der Dokumentation des Herstellers. Nehmen Sie die Änderungen nach Bedarf vor.
- 9 Klicken Sie auf **Speichern**.
- 10 Testen Sie die Verbindung und Konfiguration Ihres Schnittstellenmoduls auf der Seite *I/O-Diagnose*.

Nach Durchführen dieser Schritte

Registrieren Sie die Synergis™-Einheit in Security Center.

Einstellung der physischen Adresse von TPL-Türcontrollern

Alle TPL-Module, die an denselben RS-485-Kanal angeschlossen sind oder sich im selben LAN befinden, müssen unterschiedliche physische Adressen verwenden.

Was Sie noch wissen sollten

Die physische Adresse eines TPL-Türcontrollers wird mit zwei DIP-Schaltergruppen, DS2 und JP4, eingestellt. Wenn Sie eine TCP/IP-Erweiterungsplatine mit der TPL-Controllerplatine verbunden haben, müssen Sie diese zunächst entfernen, bevor Sie auf die DIP-Schalter zugreifen können.

Prozedur

- 1 Setzen Sie DS2/1 auf 1 oder ON.
- 2 Stellen Sie die physische Adresse an JP4 gemäß den folgenden Tabellen ein.

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

BEMERKUNG: JP4 (6, 7, 8) werden verwendet, um das Kommunikationsprotokoll des Lesegeräts einzustellen. Damit Wiegand zum Beispiel bis zu 50 Bits ohne Paritätsprüfung lesen kann, setzen Sie JP4/7 auf 1 oder ON und DS2/4 auf 1 oder ON. Weitere Informationen finden Sie in der Dokumentation von DDS für Ihr spezielles Gerät.

HID-VertX-Sub-Panels

Dieser Abschnitt enthält die folgenden Themen:

- ["Registrieren der an die Synergis™-Einheit angeschlossenen HID VertX-Subpanels"](#) auf Seite 127
- ["Freischalten von Lesegerät-Überwachung für HID VertX V100"](#) auf Seite 130

Registrieren der an die Synergis™-Einheit angeschlossenen HID VertX-Subpanels

Um eine Kommunikation zwischen der Synergis™-Einheit und den angeschlossenen Schnittstellenmodulen herzustellen, müssen Sie diese im Synergis™ Appliance Portal konfigurieren.

Bevor Sie beginnen

Schließen Sie die HID-VertX-Module an die Kanäle (1-4) Ihrer Synergis™Cloud Link -Einheit an.

BEMERKUNG: Wenn Sie die Synergis™ Cloud Link 312-Einheit haben, haben Sie bis zu 12 Kanäle. Weitere Informationen finden Sie unter [Informationen über Ports in Synergis Cloud Link 312 RS-485](#).

Prozedur

- 1 Melden Sie sich bei der Synergis™Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **VertX** als **Hardwaretyp** aus.
- 5 Wählen Sie den **Kanal** aus (1 - 4) .
Alle Schnittstellenmodule, die mit demselben Kanal verbunden sind, müssen vom selben Hersteller stammen.

- 6 Fügen Sie im selben Dialogfeld alle Schnittstellenmodule hinzu, die mit demselben Kanal verbunden sind. Sie können die Schnittstellenmodule automatisch oder manuell registrieren.

TIPP: Wenn Sie die physischen Adressen der Module kennen und nur einige wenige zu registrieren sind, wäre es schneller, sie manuell zu registrieren.

Führen Sie eine der folgenden Aktionen aus:

- Um die Anmeldung automatisch durchzuführen, klicken Sie auf **Scan**.

Die Ermittlungsfunktion sucht alle Schnittstellenmodule desselben Herstellers, die mit demselben Kanal verbunden sind, und registriert sie.

Wenn der Controller nicht alle angeschlossenen Schnittstellenmodule findet, stellen Sie sicher, dass sie alle unterschiedliche physische Adressen haben.

- Zur manuellen Registrierung geben Sie die physische Adresse (0 bis 15) ein, die auf dem HID-Schnittstellengerät konfiguriert ist, wählen Sie den Modelltyp aus und klicken Sie dann auf **+**.

Wiederholen Sie den Vorgang bei Bedarf, um alle an denselben Kanal angeschlossenen Module zu konfigurieren.

- 7 Klicken Sie auf **Speichern**.
Der Hardwaretyp, der Kanal und das Schnittstellenmodul, das Sie gerade hinzugefügt haben, werden auf der Seite *Hardwarekonfiguration* angezeigt.
- 8 Wählen Sie jedes hinzugefügte Schnittstellenmodul auf der Seite *Hardwarekonfiguration* aus und konfigurieren Sie dessen Einstellungen.
Eine Beschreibung dieser Einstellungen finden Sie in der Dokumentation des Herstellers. Nehmen Sie die Änderungen nach Bedarf vor.
- 9 Klicken Sie auf **Speichern**.
- 10 [Testen Sie die Verbindung und Konfiguration Ihres Schnittstellenmoduls auf der Seite *E/A-Diagnose*](#) .

Nach Durchführen dieser Schritte

Registrieren Sie die Synergis™-Einheit im Security Center.

Freischalten von Lesegerät-Überwachung für HID VertX V100

Um *Tür offline*-Ereignisse zu empfangen, wenn das an ein VertX V100-Panel angeschlossene Lesegerät entweder nicht angeschlossen oder ausgeschaltet ist, müssen Sie die Einstellung **I'm Alive** des Lesegeräts in Config Tool konfigurieren und das Lesegerät mit der entsprechenden Konfigurationskarte programmieren.

Bevor Sie beginnen

Registrieren Sie das VertX V100-Panel an der Synergis™-Einheit.

Was Sie noch wissen sollten

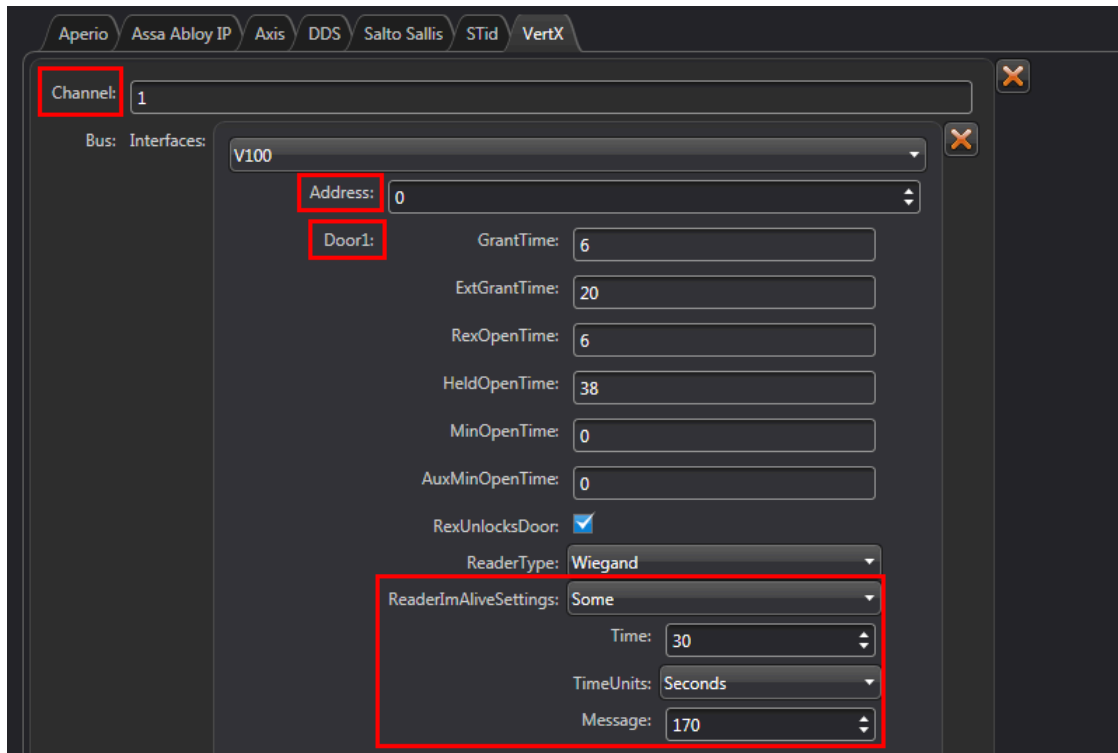
Die Lesegerätüberwachung wird nur für Lesegeräte unterstützt, die an ein VertX V100-Panel angeschlossen sind, das von einer Synergis™-Einheit gesteuert wird.

Prozedur

- 1 Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
- 2 Klicken Sie auf **Rollen und Einheiten**, und klicken Sie dann auf die Synergis™- Einheit.
- 3 Klicken Sie auf **Hardware**, und blättern Sie dann zum V100-Panel, an welches das Lesegerät angeschlossen ist.

Wenn Ihre Synergis™-Einheit mehrere V100-Panels steuert, stellen Sie sicher, dass Sie das richtige Lesegerät anhand seines **Kanals**, seiner physischen **Adresse** und seiner Türnummer (**Tür1** oder **Tür2**) identifizieren.

- 4 Klicken Sie unter der ausgewählten Tür auf **ReaderImAliveSettings**, und ändern Sie den Wert in **Some**. Die **Zeit** muss gleich oder größer sein als die **I'm Alive**-Zeit auf der Konfigurationskarte des Lesegeräts, und die **Message** muss der **I'm Alive**-Meldung entsprechen (170 ist das dezimale Äquivalent von AA in Hexadezimal).



- 5 Klicken Sie auf **Anwenden**.
- 6 Konfigurieren Sie das Lesegerät mit der entsprechenden Feldprogrammierskarte (auch als Konfigurationskarte bezeichnet).

Wenn dieses Lesegerät vom V100-Panel getrennt oder ausgeschaltet wird, erhalten Sie jetzt das Ereignis *Tür offline: Gerät ist offline* an der Tür, mit der es verbunden ist.

Mercury-Steuerungen

Dieser Abschnitt enthält die folgenden Themen:

- ["Einstellungen des Mercury-Lesegeräts"](#) auf Seite 133
- ["Vorbereitung für die Registrierung des Mercury-Controllers"](#) auf Seite 136
- ["Registrierung von Mercury-Controllern auf der Synergis™-Einheit"](#) auf Seite 140
- ["Konfigurieren der Mercury-Controller-Einstellungen im Synergis™ Appliance Portal"](#) auf Seite 144
- ["Überlegungen zur Installation von OSDP-Lesegeräten mit Mercury"](#) auf Seite 162
- ["OSDP-Lesegeräte \(Secure Channel\) zu einem Mercury-Controller hinzufügen"](#) auf Seite 164
- ["Hinzufügen von MR51e-Panels zu einem Mercury-Controller"](#) auf Seite 168
- ["Einstellung von MR62e zur Verwendung des statischen IP-Adressierungsmodus"](#) auf Seite 170
- ["Trennen von MR-Panels von einem Mercury-Controller"](#) auf Seite 171
- ["Informationen über Mercury-Auslöser und -Verfahren"](#) auf Seite 172
- ["Mercury-Auslöser im Synergis Appliance Portal konfigurieren"](#) auf Seite 177
- ["Mercury-Verfahren im Synergis Appliance Portal konfigurieren"](#) auf Seite 179
- ["Mercury-Auslöser und -Verfahren im Synergis Appliance Portal deaktivieren"](#) auf Seite 181

Einstellungen des Mercury-Lesegeräts

Dies ist eine vollständige Liste der Einstellungen des Mercury-Lesegeräts; diese Einstellungen entsprechen der spezifischen Hardware des Lesegeräts. Die meisten heute verwendeten Lesegeräte arbeiten mit dem Wiegand-Standard. Zur Verwendung von Smartcards oder zur Einrichtung von Secure OSDP2-Lesegeräten lesen Sie die technischen Hinweise zu den jeweiligen Lesegeräten.

Funktion	Beschreibung
Art des Lesegeräts	
Standard Wiegand	<ul style="list-style-type: none"> • Setzt Tastaturmodus auf HID • Setzt LED-Ansteuerungsmodus auf Bi-color • Setzt Wiegand-Impulse auf EIN
Standard Magstripe	<ul style="list-style-type: none"> • Setzt Tastaturmodus auf Keine • Setzt LED-Ansteuerungsmodus auf Bi-color • Setzt Trim Nullbits auf EIN • Setzt Halbbyte-Matrix formatieren auf EIN • Setzt Bidirektionale Mag-Decodierung zulassen auf EIN • Setzt Überwacht auf EIN • Setzt Eingänge kommen von Lesegerät auf EIN
Standard-OSDP	<ul style="list-style-type: none"> • Aktiviert OSDP-Modus • Setzt Tastaturmodus auf HID • Setzt LED-Ansteuerungsmodus auf OSDP
OSDP 2	<ul style="list-style-type: none"> • Aktiviert OSDP-Modus • Setzt Tastaturmodus auf HID • Setzt LED-Ansteuerungsmodus auf Bernutzerdefiniertes OSDP <p>Dieser Modus ermöglicht auch die Konfiguration von Bitrate des Lesegerätanschlusses, Verfolgung, Smartcard, Adresse und Verwendung der gesicherten Kommunikation.</p>
Standard F2F	<ul style="list-style-type: none"> • Setzt Tastaturmodus auf HID • Setzt LED-Ansteuerungsmodus auf Bi-color • Setzt Halbbyte-Matrix formatieren auf EIN • Setzt Casi 1-Draht F2F auf EIN
Überwachtes F2F	<ul style="list-style-type: none"> • Setzt Tastaturmodus auf HID • Setzt LED-Ansteuerungsmodus auf Bi-color • Setzt Halbbyte-Matrix formatieren auf EIN • Setzt Casi 1-Draht F2F auf EIN • Setzt Überwacht auf EIN

Funktion	Beschreibung
Überwachtes F2F mit Eingängen	<ul style="list-style-type: none"> • Setzt Tastaturmodus auf Keine • Setzt LED-Ansteuerungsmodus auf Bi-color • Setzt Halbbyte-Matrix formatieren auf EIN • Setzt Casi 1-Draht F2F auf EIN • Setzt Überwacht auf EIN • Setzt Eingänge kommen von Lesegerät auf EIN
Benutzerdefiniert	Ermöglicht dem Benutzer die Einstellung des Tastaturmodus, des LED-Ansteuerungsmodus oder anderer Einstellungen, die von der Hardware des Lesegeräts abhängen.
Tastaturmodus¹	
Keine	Es ist kein bestimmter Modus aktiv.
MR20	MR20 8-Bit-Tastaturformat mit Unterstützung gegen Manipulation.
HID	HID 4-Bit-Tastaturformat.
Indala	Acht-Bit-Motorola/Indala-Format, bestehend aus einem 4-Bit-Code und demselben Code invertiert.
MR20 keine Manipulation	MR20 8-Bit-Tastaturformat ohne Unterstützung gegen Manipulation.
4-Bit, 60 Sekunden Keep Alive	4-Bit-Tastaturformat mit HID I'm Alive-Unterstützung auf ein 60-Sekunden-Intervall eingestellt.
8-Bit, 60 Sekunden Keep Alive	8-Bit-Tastaturformat mit HID I'm Alive-Unterstützung auf ein 60-Sekunden-Intervall eingestellt.
4-Bit, 10 Sekunden Keep Alive	4-Bit-Tastaturformat mit HID I'm Alive-Unterstützung auf ein 10-Sekunden-Intervall eingestellt.
8-Bit, 10 Sekunden Keep Alive	8-Bit-Tastaturformat mit HID I'm Alive-Unterstützung auf ein 10-Sekunden-Intervall eingestellt.
LED-Ansteuerungsmodus	
Bi-color	Allgemeine 1-Draht, Tri-State-Bi-Color-Treiberschaltung.
2-Wire	Separater roter und grüner Treiber ohne Summer.
Dorado-780	Zweidraht-Treiber mit Farbkonvertierung.
LCD	Aktiviert den LCD-Anzeigetreiber auf mit LCD ausgestatteten Lesegeräten.
Bioscrypt	Aktiviert die Bioscrypt-Schnittstelle.
OSDP	Spiegelt das Verhalten der Wiegand-LED und des Summers bei OSDP-Lesegeräten wider.

Funktion	Beschreibung
SNET	Aktiviert SNET an Honeywell-Controllern.
Benutzerdefiniertes OSDP	Ermöglicht dem Benutzer, benutzerdefinierte OSDP-Einstellungen festzulegen.
Andere Steuerelemente	
Wiegand-Impulse	Aktiviert Daten 1/Daten 0 Wiegand-Impulse.
Nullbits kürzen	Entfernt führende Nullen.
Halbbyte-Matrix formatieren	Wird für die Verwendung von Magnetstreifen verwendet.
Bidirektionale Mag-Decodierung zulassen	Sendet decodierte Daten unabhängig davon, in welche Richtung die Karte gezogen wird.
Northern Mag-Decodierung zulassen	Decodiert 32-Bit-Wiegand-Daten von bestimmten Northern-Karten.
Casi 1-Draht F2F	Bei der Casi 1-Draht F2F-Kommunikationsart wird für die Kommunikation ein Draht anstelle von zwei verwendet.
Überwacht	Ermöglicht die Überwachung. Nur mit F2F-Flag verwendet.
Eingaben kommen von Lesegerät	Legt fest, dass die Eingaben vom Lesegerät kommen. Nur mit F2F-Flag verwendet.

¹ Mercury unterstützt keine Tastaturlesegeräte, die PIN im 26-Bit-Wiegand-Modus ausgeben (HID-Modus-14).

Vorbereitung für die Registrierung des Mercury-Controllers

Bevor Sie den Mercury-Controller an der Synergis™-Einheit registrieren, müssen Sie dem Controller eine statische IP-Adresse zuweisen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die folgenden Angaben haben:

- **Einrichtungs- und Konfigurationsanleitung für Mercury:** Gebrauchsanweisung für die Verbindung zum Webportal Ihres Mercury-Controllers und die Einrichtung seiner IP-Adresse (und anderer Konfigurationen).
- **Statische IP-Adresse:** Statische IP-Adresse, die dem Controller von Ihrer IT-Abteilung zugewiesen wurde.
- **Physische Adressen:** Jedes Schnittstellenpanel, das mit demselben RS-485-Port desselben Mercury-Controllers verbunden ist, muss eine eindeutige physische Adresse haben (konfiguriert über einen DIP-Schalter).

BEST-PRACTICE: Wenn Sie viele Mercury-Controller an derselben Synergis™-Einheit registrieren müssen, ist es am besten, sie alle gleichzeitig zu registrieren. Jeder Controller, den Sie der Synergis™-Einheit hinzufügen oder entfernen, führt zu einem Neustart der Einheit. Während die Einheit neu gestartet wird, ist sie für etwa 30 Sekunden offline.

Was Sie noch wissen sollten

Mercury-Controller, die an derselben Synergis™-Einheit registriert sind, können keine unterschiedlichen Partitionen im Security Center zugewiesen werden. Wenn Sie die Controller verschiedenen Partitionen zuweisen müssen, registrieren Sie sie auf verschiedenen Synergis™-Einheiten und weisen Sie dann die Synergis™-Einheiten verschiedenen Partitionen zu.

BEMERKUNG: Die mit *Härtung* gekennzeichneten Schritte und Anweisungen sind optional, schützen Ihr System aber vor Cyberangriffen.

Prozedur

- 1 Stellen Sie auf der Mercury-Controller-Platine den DIP-Schalter *S1-1* auf **EIN**. Dies gibt Ihnen ein Zeitfenster von 5 Minuten, um sich mit den Werkseinstellungen anzumelden.
- 2 Melden Sie sich am Mercury-Controller über die *Configuration Manager*-Webseite an. Verwenden Sie die Default-IP-Adresse (192.168.0.251) und -Berechtigung (admin/password) Weitere Informationen erhalten Sie in der Herstellerdokumentation.
- 3 Wählen Sie **Netzwerk** aus dem Menü, konfigurieren Sie die **IP-Adresse** des Mercury-Controllers und klicken Sie auf **Akzeptieren**.
- 4 Wählen Sie im Menü **Host Comm**.

- 5 Konfigurieren Sie auf der Seite *Host-Kommunikation* die folgenden Einstellungen, und klicken Sie auf **Akzeptieren**.

Genetec LP1502 Configuration Manager

Host Communication

Communication Address: Use IPv6 Only

Primary Host Port

Connection Type: Data Security:

Interface: 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.

- **Kommunikationsadresse:** Auf **0** setzen.
WICHTIG: Nicht zu verwechseln mit dem **Kanal**, der eindeutig sein muss, wenn Sie den Mercury-Controller an der Synergis™-Einheit registrieren.
- **Portnummer:** Die Portnummer, die von der Synergis™-Einheit für die Kommunikation mit dem Mercury-Controller verwendet wird (Standard=3001).
- **Autorisierte IP-Adresse erforderlich:** (*Härtung*) Wählen Sie diese Option, und setzen Sie **Autorisierte IP-Adresse** auf die IP-Adresse der Synergis™-Einheit.
- **Datensicherheit:** Eingestellt auf **TLS erforderlich**.
WICHTIG: Wenn TLS nicht ausgewählt ist, bleibt der Mercury-Controller offline.

- 6 Wählen Sie **Benutzer** im Menü, und klicken Sie auf **Neuer Benutzer**.

Richten Sie ein Benutzerkonto auf dem Mercury-Controller ein. Dadurch müssen Sie nicht mehr physisch auf die Einheit zugreifen und den DIP-Schalter *S1-1* auch nicht auf **EIN** schalten, wenn Sie die Konfiguration des Controllers das nächste Mal ändern.

Genetec LP1502 Configuration Manager

User Account

Select account level: (dropdown)

Username: (4-10 characters)

Change password Don't change password

Previous Password:

Password: (8-64 characters)

Password again:

Notes: (32 characters maximum)

<, >, &, =, ;, ?, +, ', -, " are illegal characters for this field.

A strong password

- Is not based on the user's account name
- Contains at least eight characters
 - Arabic numerals(0-9)
 - Nonalphanumeric characters

- 7 (Härtung) Geben Sie auf der Seite *Benutzerkonto* den **Benutzernamen** und ein starkes **Passwort** ein, bestätigen Sie das Passwort und klicken Sie dann auf **Speichern**.

- 8 Deaktivieren Sie auf der Seite *Benutzer* die Option **Time Server**.

Der Time Server ist nicht erforderlich. Synergis™ Software überwacht und stellt die Zeit an den Mercury-Einheiten automatisch ein.

Time Server

Enable Disable

Server: Port:

Update Interval:

User Specified Time Server:

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

- 9 (Härtung) Deaktivieren Sie auf der Seite *Benutzer* die **SNMP-Optionen** und klicken Sie auf **Senden**.

Disable Web Server Enable Door Forced Open Filter

Enable Diagnostic Logging Disable Default User

Disable USB Interface Disable SD Card Interface

Disable Zeroconf Device Discovery Enable Gratuitous ARP

SNMP Options (dropdown)

- 10 Wählen Sie **Einstellungen übernehmen** und klicken Sie auf **Einstellungen übernehmen, Neustart**.
- 11 Stellen Sie den DIP-Schalter *S1-1* auf der Mercury-Controller-Platine für den Normalbetrieb auf **AUS**.
Dadurch wird verhindert, dass die werkseitigen Standardeinstellungen für die Anmeldung am Controller verwendet werden.
- 12 Wenn Sie zum Fortfahren aufgefordert werden, wählen Sie **Ich verstehe und möchte fortfahren**, und klicken Sie dann auf **Ja**.

Nach Durchführen dieser Schritte

Registrieren Sie den Mercury-Controller an der Synergis™-Einheit.

Registrierung von Mercury-Controllern auf der Synergis™-Einheit

Damit die Synergis™-Einheit mit den angeschlossenen Mercury-Controllern kommunizieren kann, müssen Sie diese mit dem Security Center Config Tool registrieren.

Bevor Sie beginnen

[Bereiten Sie den Mercury-Controller für die Anmeldung vor.](#)

Was Sie noch wissen sollten

Auf der Synergis™-Einheit muss jedem Mercury-Controller eine eindeutige Kanal-ID zugewiesen werden. Alle Mercury-Controller haben RS-485-Busse, an welche die Schnittstellenpanels (MR50, MR52, MR16IN und MR16OUT) angeschlossen sind. Jedes Schnittstellenpanel, das an denselben RS-485- oder Ethernet-Bus angeschlossen ist, muss eine eindeutige physische Adresse haben.

Prozedur

- 1 Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
- 2 Klicken Sie auf **Rollen und Einheiten**, und klicken Sie dann auf die Synergis™- Einheit.

- 3 Klicken Sie auf **Peripheriegeräte** und dann auf **Einen Eintrag hinzufügen** (+).

The screenshot shows a configuration window for adding a peripheral device. The fields are as follows:

- Manufacturer:** Mercury Security (dropdown menu)
- Model:** EP1502 (dropdown menu)
- IP address:** 0 . 0 . 0 . 0 (text input) with a blue link labeled **Hostname** next to it.
- Port:** 3001 (spin box)
- Channel:** 1 (spin box)
- Interfaces:** A table with columns: Model, Port, Address (with an up arrow), and IP address. The table is currently empty.

At the bottom of the window, there are three small icons: a green plus sign (+), a red X, and a pencil. Below these icons is a button labeled **Advanced settings**. At the very bottom are **Cancel** and **OK** buttons.

- 4 Geben Sie die folgenden Informationen ein:

- **Modell:** Modell des Controllers.
- **IP-Adresse:** Statische IP-Adresse, die dem Controller von Ihrer IT-Abteilung zugewiesen wurde.
- **Hostname:** Klicken Sie auf den blauen Link, um die Steuerung ihrem Hostnamen nach zu identifizieren. Diese Option ist nur verfügbar, wenn Sie Security Center 5.12.0.0 oder höher ausführen.
BEMERKUNG: Wenn Sie eine Mercury-Steuerung mit ihrem Hostnamen registrieren, müssen Sie `.local` an den Hostnamen anhängen, wenn die Steuerung nicht bei DHCP und DNS im Netzwerk registriert ist.
- **Port:** Kommunikationsport. Der Standardwert ist 3001. Der Port muss mit dem auf der Mercury Device Manager-Webseite konfigurierten Wert übereinstimmen.
- **Kanal:** Kanal-ID für diesen Controller. Die Kanal-ID kann ein beliebiger Wert zwischen 0 und 63 sein. Sie muss innerhalb der Synergis-Einheit eindeutig sein. Nach dem Zuweisen darf sie nicht mehr geändert werden.

- 5 Wenn das ausgewählte Controller-Modell nachgelagerte Panels unterstützt, fügen Sie diese hinzu.

BEMERKUNG: Beachten Sie Folgendes:

- Für MR51e PoE-Panels fügen Sie diese nach der Anmeldung des Controllers hinzu.
 - Die von Mercury empfohlene Anzahl von acht nachgeschalteten Panels pro Controller darf für EP1501-, LP1501--Controller nicht überschritten werden.
 - Das M5-20IN-Panel belegt zwei aufeinanderfolgende Adressen auf dem Kommunikationsbus. Um die 20 Eingänge des M5-20IN-Panels nutzen zu können, müssen Sie im Config Tool zwei M5-20IN-Panels zu Ihrem M5-IC-Controller hinzufügen. Die Adresse des ersten Panels muss mit der physischen Adresse auf dem M5-20IN-Panel übereinstimmen, und die Adresse des zweiten Panels muss auf die Adresse des ersten Panels plus eins gesetzt werden.
 - MR62e-Einheiten können eine IPv6-Adresse haben, können aber nicht mit Mercury-Steuerungen über IPv6 kommunizieren.
- a) Klicken Sie in der Liste *Schnittstellen* auf **Einen Eintrag hinzufügen** (+).
 - b) Wählen Sie im Dialogfeld, das geöffnet wird, das **Modell**, den **Port**, die **Adresse** (0–31) und, wo zutreffend, die IP-Adresse des nachgeschalteten Panels aus.
Alle Panels, die an denselben Port angeschlossen sind, müssen unterschiedliche Adressen verwenden.
 - c) Klicken Sie auf **OK**.
 - d) Wiederholen Sie dies nach Bedarf.

- 6 (Optional) Klicken Sie auf **Erweiterte Einstellungen**, um die erweiterten Einstellungen zu ändern.

Die verfügbaren Einstellungen hängen vom gewählten Controller-Modell ab. Sie können in der Regel die Baudrate des verfügbaren seriellen Anschlusses, die benutzerdefinierten überwachten Eingangswerte und die Konfiguration des Stromeingangsereignisses ändern.



BEMERKUNG: Sie können bis zu vier verschiedene benutzerdefinierte Voreinstellungen für die Eingänge Ihres Mercury-Controllers festlegen. Für Benutzer, die eine Aktualisierung von früheren Security Center-Versionen durchführen und einen benutzerdefinierten Wert konfiguriert haben, wird diese Voreinstellung als **Benutzerdefiniert 1** in der Liste **AD Zeilengrenzwerte** aufgeführt.

- 7 Klicken Sie auf **OK** am unteren Rand des Dialogfelds.

8 Klicken Sie auf **Anwenden**.

Auf der Seite *Peripheriegeräte* wird der Mercury-Controller mit allen angeschlossenen nachgeschalteten Panels und Peripheriegeräten angezeigt.

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	

Das Hinzufügen von Schnittstellenmodulen zur Synergis™-Einheit führt zu einem Software-Neustart der Einheit. Während dieses Vorgangs erscheinen die Synergis™-Einheit und alle damit verbundenen Peripheriegeräte offline (in Rot).

9 Wählen Sie jedes der erkannten E/A-Geräte und Lesegeräte aus und konfigurieren Sie ihre Eigenschaften wie erforderlich.

Für OSDP-Lesegeräte (Secure Channel) siehe [OSDP-Lesegeräte \(Secure Channel\) zu einem Mercury-Controller hinzufügen](#) auf Seite 164.

10 Testen Sie Ihre Verdrahtung und Konfiguration, indem Sie die Ein- und Ausgänge auslösen.

Der ausgelöste E/A ändert seinen Zustand in Echtzeit auf dem Bildschirm.

BEMERKUNG: Lesegerätaktivitäten werden auf der Seite *Peripheriegeräte* nicht angezeigt.

Nach Durchführen dieser Schritte

Falls zutreffend, [fügen Sie die MR51e-Panels zum Mercury-Controller hinzu](#), und ordnen Sie dann die physische Verdrahtung der Schnittstellenmodule den Türen und Zonen im Security Center zu.

Konfigurieren der Mercury-Controller-Einstellungen im Synergis™ Appliance Portal

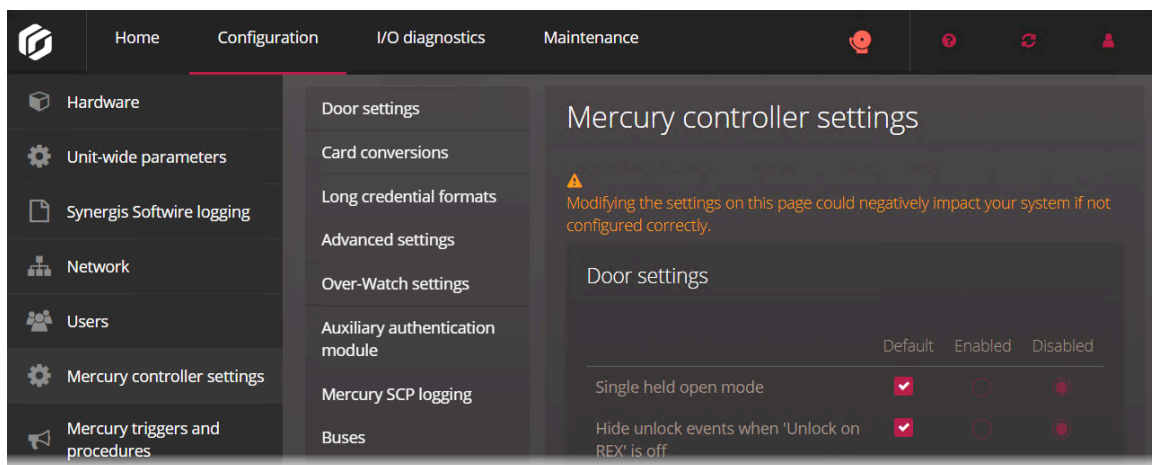
Sie können die Einstellungen für Ihre Mercury-Controller im Synergis™ Appliance Portal konfigurieren.

Was Sie noch wissen sollten

Die gesamte einer Tür oder einem Aufzug zugewiesene Hardware muss von demselben Mercury-Controller unter derselben Synergis™ Cloud Link -Einheit gesteuert werden, damit sie funktioniert, wenn die Synergis™ Cloud Link -Einheit offline ist.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Mercury-Controller-Einstellungen**.



- 3 Klicken Sie im Seitenmenü auf die Registerkarte **Türeinrichtungen**, und aktivieren Sie die folgenden Einstellungen nach Bedarf:

- **Modus zum einzelnen Offenhalten:** Ignoriert nachfolgende *Tür zu lange offen*-Ereignisse, nachdem das erste Ereignis erzeugt wurde, solange die Tür offen bleibt.

Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.

- **Entriegelungsereignisse ausblenden wenn 'Entsperren bei REX' deaktiviert ist:** Der Mercury-Controller sendet Entriegelungsereignisse bei REX-Aktivierungen, unabhängig davon, ob die Tür tatsächlich entriegelt wird oder nicht. Aktivieren Sie diese Einstellung, um diese Entriegelungsereignisse auszublenden. Die Aktivierung dieser Einstellung bewirkt eine Verzögerung bei allen empfangenen Ereignissen, sodass falsche Entriegelungsereignisse herausgefiltert werden können.

Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.

- **Übertragung durch Host deaktivieren (Offline-Modus):** Standardmäßig ist diese Einstellung deaktiviert, was bedeutet, dass die Mercury-Host-Entscheidungsweitergabe aktiviert ist und die Synergis™ Cloud Link -Einheit die Zutrittskontrollentscheidungen trifft. Wenn diese Einstellung aktiviert ist, ist die Mercury-Host-Entscheidungsweitergabe deaktiviert, was bedeutet, dass die Mercury-Controller ihre eigenen Entscheidungen treffen – und zwar so, als seien sie von der Synergis™ Cloud Link -Einheit getrennt. In diesem Fall funktionieren einige erweiterte Funktionen und Karten nicht, die noch nicht mit dem Mercury-Controller synchronisiert sind, die Tür wird jedoch reaktionsfähig.

BEST-PRACTICE: Lassen Sie die Einstellung **Host-Entscheidungsweitergabe deaktivieren (Offline-Modus)** deaktiviert. Aktivieren Sie sie nur, wenn die Netzwerkverbindung zwischen der Synergis™ Cloud

Link -Einheit und den Mercury-Controllern schlecht ist. Weitere Informationen dazu finden Sie unter [Unterschiede zwischen der aktivierten und deaktivierten Mercury-Host-Entscheidungsweitergabe](#) auf Seite 148.

- **Unbeaufsichtigter Zutritt erlaubt:** Die Lesegeräte piepen nicht, wenn der Zugang gewährt wird.
- **Unbeaufsichtigter Zutritt verwehrt:** Die Lesegeräte piepen nicht, wenn der Zugang verweigert wird.
- **Ereignis „Öffnen der Tür erzwungen“ verhindern:** *Erzwungenes Türöffnen*-Ereignisse sind deaktiviert.
Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
- **Motorfehler-Ereignisse von Schlage-Schlössern blockieren:** Ereignisse des Typs *Motorfehler* von Schlage-Schlössern werden deaktiviert.
BEMERKUNG: Diese Einstellung hat keinen Einfluss auf *Motorfehler*-Ereignisse von anderen Geräten.
Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
- **„RF-Verlust“-Ereignisse von Schlage-Schlössern blockieren:** Ereignisse des Typs *RF-Verlust* von Schlage-Schlössern werden deaktiviert.
BEMERKUNG: Diese Einstellung hat keinen Einfluss auf *RF-Verlust*-Ereignisse von anderen Geräten.
Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
- **Lesegerät-LED aus wenn verriegelt:** Die Lesegerät-LEDs an OSDP-Lesegeräten sind ausgeschaltet, wenn sich die zugehörige Tür in einem normalen Verriegelungszustand befindet.
- **Native Mercury-Bereichssteuerung:** Ermöglicht die Mercury-eigenen Antipassback-, max Belegung- und Verriegelungs-Funktionen auf der Mercury-Steuerung. Weitere Informationen dazu finden Sie unter [Beschränkungen der nativen Mercury-Bereichssteuerung](#) auf Seite 150.
Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
- **Erweiterte zugesicherte Zeit im REX-Modus:** Die Türen bleiben entriegelt, solange der REX-Eingang aktiv ist und für die normale Gewährungszeit danach. Wenn kein Türsensor vorhanden ist, bleibt die Tür entweder so lange entriegelt, wie der REX-Eingang aktiv ist, oder für die normale Gewährungszeit, je nachdem, welcher Zeitraum länger ist.

Dies ist nützlich, um zu verhindern, dass Türen, die von einem Bewegungssensor gesteuert werden, alle paar Sekunden ver- und entriegelt werden. Diese Funktion erfordert die Mercury-Firmware 1.29.1 oder höher.
BEMERKUNG: Sie können diese Einstellung auch [für jede Tür einzeln konfigurieren](#).
- **Live-Ereignisse "Aufforderung zum Verlassen":** Ändert die Art, wie Synergis™ Software Ereignisse des Typs *Aufforderung zum Verlassen* von Mercury LP- und MP-Controllern verarbeitet, damit Zeitstempel auf den Ereignissen akkurat gemeldet werden. Diese Einstellung ist standardmäßig aktiviert.
- **Türalarm-LED-Vorgänge programmieren:** Bewirkt, dass die mit Mercury-Controllern verbundenen Lesegeräte Synergis™ Software-LED- und Buzzer-Muster anstelle der Mercury-LED- und Buzzer-Muster für Türalarme befolgen.
BEMERKUNG: Ist diese Einstellung deaktiviert, blinken bei den Ereignissen *Öffnen der Tür erzwungen* und *Tür zu lange geöffnet* die LEDs der zugehörigen Lesegeräte nicht.
Wenn Sie diese Einstellung ändern, müssen Sie einen Software-Neustart durchführen und anschließend die Mercury-Controller zurücksetzen.
- **Empfang von Bedrohungscodeereignissen, wenn Bedrohungscode deaktiviert ist:** Führt dazu, dass die Ereignisse *Zutritt verweigert: Ungültige PIN* und *Bedrohungs-PIN eingegeben* beide in Security Center erstellt werden, wenn jemand eine Bedrohungs-PIN eingibt, wenn die Einstellung **Bedrohungs-PIN** in Config Tool deaktiviert ist.

- 4 Klicken Sie im Seitenmenü auf die Registerkarte **Kartenkonversionen**, und aktivieren Sie die folgenden Kartenkonversionen nach Bedarf:
Führen Sie einen Neustart der Software durch, wenn Sie eine dieser Einstellungen ändern.
- **Casi M5 56 -> 40**
 - **Mehrdeutiges HID 1441 -> 56**
 - **Verlustbehaftete Konvertierung für Berechtigungen, die länger als 52 Bits sind:** Behebt einen Fehler in Versionen von Synergis™ Software vor 10.10, bei dem Berechtigungen von 52 bis 64 Bits zu Problemen führen konnten.
 - **200 Bits FASC-N bis 128 Bits:** Alle Karten melden die 128-Bit-Version. Diese Einstellung wird mit FICAM oder Datenbanklayouts mit langern Berechtigungsnachweisen verwendet.
 - **Übersetzer für F2F zu Wiegand hinzufügen:** Andere Übersetzer hinzufügen oder konfigurieren.
- 5 Klicken Sie im Seitenmenü auf die Registerkarte **Lange Berechtigungsnachweisformate** und konfigurieren Sie die folgende Einstellung:
- **Wiegand-Formatlänge (Bits):** Lange Berechtigungsnachweisformate für Mercury-Steuerungen werden nicht automatisch in Security Center konfiguriert. Stellen Sie das Format manuell ein, indem Sie einen Wert von 64 bis 240 eingeben und dann auf **Hinzufügen** klicken. Diese Einstellung wird mit FICAM oder Datenbanklayouts mit langern Berechtigungsnachweisen verwendet.
- Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
- 6 Klicken Sie im Seitenmenü auf die Registerkarte **Erweiterte Einstellungen**, und aktivieren Sie die folgenden Einstellungen nach Bedarf:
Führen Sie einen Neustart der Software durch, wenn Sie eine dieser Einstellungen ändern.
- **SIO-Verschlüsselungssteuerung:** Ermöglicht die Verschlüsselung auf der RS-485-Übertragungsstrecke zwischen EP- oder Honeywell-Steuerungen und ihren nachgeschalteten SIO-Karten bzw. LP-Controllern und älteren SIO-Karten. LP-Controller mit S3 SIO-Karten verwenden die Verschlüsselung auf dem Kanal unabhängig von dieser Einstellung.
- BEST-PRACTICE:**
- Begrenzen Sie Bulk-Upgrades auf 10 SIO-Karten unter einem einzigen EP-Controller.
 - Bevor Sie mehrere SIO-Boards aktualisieren, deaktivieren Sie die Einstellung **SIO-Verschlüsselungssteuerung**.
 - **Kein ACR ohne Tür:** Die Lesegeräte sind nicht vorkonfiguriert, wenn SIO-Einheiten hinzugefügt werden, und die E/A-Diagnose meldet keine Kartenlesungen von nicht zugeordneten Lesegeräten. Diese Einstellung beseitigt Probleme, bei denen mehr als 64 Lesegeräteports unter einem Mercury-Controller angemeldet sind, oder Fälle, in denen Türen ohne Lesegerät verwendet werden und ebenfalls das Limit von 64 überschreiten.
 - **Zwei OSDP-Lesegeräte pro Lesegeräteport:** Damit können LP1502-, LP4502-, MP1502-, MP4502-, MR50-S3- und MR52-S3-Einheiten zwei OSDP-Lesegeräte pro Anschluss unterstützen.
 - Für LP1502, LP4502, MR50-S3 und MR52-S3 ist hierfür Security Center 5.10.4.0 oder höher erforderlich.
 - Für MP1502, MP4502 ist hierfür Security Center 5.12.1.0 oder höher erforderlich.
 - **Magstripe-Unterstützung:** Diese Einstellung ist standardmäßig aktiviert und ermöglicht die Unterstützung für bis zu acht Wiegand-Kartenformaten pro Mercury-Steuerung. Für jedes der acht Wiegand-Kartenformate werden entsprechende Magstripe-Kartenformate automatisch erstellt. Wenn die Einstellung deaktiviert ist, kann jede Mercury-Steuerung bis zu 16 Wiegand-Kartenformate unterstützen und es werden keine entsprechenden Magstripe-Kartenformate automatisch erstellt.
- 7 Klicken Sie im Seitenmenü auf die Registerkarte **Over-Watch-Einstellungen** und wählen Sie die Einstellung **LP4502-Over-Watch-Plugin** aus, um das Over-Watch-Plugin auf allen LP4502-Controllern unter der Synergis™ Cloud Link -Einheit zu aktivieren. Das Over-Watch-Plugin ist nur für die BEST-Wi-Q-Integration über Mercury erforderlich.
- Weitere Informationen dazu finden Sie unter [Das Over-Watch-Plugin für die BEST-Wi-Q-Integration konfigurieren](#) auf Seite 191.

- 8 Klicken Sie im Seitenmenü auf die Registerkarte **Hilfsauthentifizierungsmodul** und wählen Sie **Deaktiviert, PivClass** oder **TIEntryPoint** aus.
Diese Einstellung wird mit dem FICAM-Datenbanklayout und dem entsprechenden Plugin für den LP4502-Controller verwendet.
- 9 Klicken Sie im Seitenmenü auf die Registerkarte **Mercury-SCP-Protokollierung** und klicken Sie auf **Protokollierung starten** für Mercury-spezifischere Protokollierung und geben Sie die Anzahl der Tage ein, nach denen die Protokollierung enden soll.
- 10 Klicken Sie im Seitenmenü auf die Registerkarte **Busse** und klicken Sie auf **Zurücksetzen** für jeden Controller oder **Alles zurücksetzen**, um sicherzustellen, dass die neuen Einstellungen an alle Controller übertragen werden.
- 11 Klicken Sie im Seitenmenü auf die Registerkarte **Einstellungen des Datenbank-Layouts**, und konfigurieren Sie die folgenden Einstellungen:
- Wählen Sie ein Datenbanklayout aus der Liste aus.
Das Layout **Umfangreiche Funktionen (Standard)** eignet sich für die meisten Anwendungsfälle. Die anderen Datenbank-Layouts sind auf spezifische Bedürfnisse zugeschnitten. Setzen Sie nach einer Änderung des Datenbanklayouts die Controller zurück.
Weitere Informationen darüber, was die einzelnen Datenbanklayouts unterstützen, finden Sie unter [Datenbank-Layouts für Mercury-Controller](#) auf Seite 152.
 - Konfigurieren Sie die maximale PIN-Länge.
Standardmäßig maximale PIN-Länge ist standardmäßig ausgewählt. Der Default-Wert für alle Datenbanklayouts ist **6**. Um diesen Wert zu ändern, wählen Sie **Maximale benutzerdefinierte PIN-Länge** aus und geben Sie dann den neuen Wert im Feld **Maximale PIN-Länge** ein.
BEMERKUNG: Ein niedrigerer Wert wird häufig verwendet, um das Drücken der #-Taste am Ende von vierstelligen PINs zu vermeiden, wenn im System nur vierstellige PINs verwendet werden. Wenn Sie für **Maximale PIN-Länge** eine Zahl festlegen, die höher ist als die, die vom ausgewählten Datenbanklayout unterstützt wird, funktionieren Ihre Mercury-Controller nicht mehr, und PINs, die länger sind als die konfigurierte **maximale PIN-Länge**, funktionieren nicht.
Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
- 12 Klicken Sie im Seitenmenü auf die Registerkarte **PIN-Einstellungen**, und konfigurieren Sie die folgenden Einstellungen:
- Einfügen und Hinzufügen von führenden Nullen für PINs:** Um Nullen vor Ihren PINs zu verwenden, wählen Sie **Benutzerdefiniert** und geben Sie einen Wert für **PIN-Länge nach dem Hinzufügen führender Nullen** ein. Beispiel: Die maximale PIN-Länge beträgt 6 Ziffern und Sie geben **4** als **PIN-Länge nach dem Hinzufügen von führenden Nullen** ein. Wenn Ihre ursprüngliche PIN **9** war, wird die PIN zu **0009**. Wenn Ihre ursprüngliche PIN **123** war, wird die PIN zu **0123**.
Führen Sie einen Neustart der Software durch, wenn Sie diese Einstellung ändern.
Weitere Informationen dazu finden Sie unter [Informationen über die Konfiguration von PINs mit führenden Nullen für Mercury-Integrationen](#) auf Seite 156.
- 13 Klicken Sie im Seitenmenü auf die Registerkarte **Für OSDP-Lesegeräte spezifische Einstellungen**, und konfigurieren Sie folgende Einstellungen:
- Nexus- und Veridt-OSDP-LED-Korrektur:** Behebt ein LED-Problem, das bei bestimmten Nexus- und Veridt-OSDP-Lesegeräten auftritt.
 - LED-Programmierung überschreiben:** Behebt Probleme auf OSDP-Lesegeräten, bei denen die LED für einige Sekunden erlischt, wenn die Tür nach dem Öffnen wieder verriegelt wird.
- 14 Klicken Sie im Seitenmenü auf die Registerkarte **Regel zur Besucherbegleitung und Zwei-Personen-Regel** und konfigurieren Sie die folgende Einstellung:
- Maximale Verzögerung zwischen Karten-Präsentationen:** Gilt für alle Türen, die von den Mercury-Controllern gesteuert werden.
Wenn Sie diese Einstellung ändern, müssen Sie einen Software-Neustart durchführen und anschließend die Mercury-Controller zurücksetzen.

- 15 Klicken Sie im Seitenmenü auf die Registerkarte **Türverhalten bei Offline-SIO-Karten**, und wählen Sie eine der folgenden Optionen aus:

Diese Einstellung gilt nur für Türen, deren Lesegerät und Schloss sich auf derselben Mercury-SIO-Karte befinden. Türen ohne Lesegeräte sind davon nicht betroffen. Wenn die Tür aufgrund dieser Einstellung entsperrt wird, folgt das Verhalten der Lesegerät-LED nicht dem Türversperrungsstatus.

WICHTIG: Alle Ereignisse, die auftreten, während das SIO-Board nicht mit der Mercury-Steuerung verbunden ist, werden nicht aufgezeichnet.

- **Standard (gesperrt):** Wenn das SIO-Board die Verbindung mit der Mercury-Steuerung verliert, werden die Türen, die sie steuert, gesperrt, unabhängig vom Status, in dem sich die Türen befunden haben, bevor die Verbindung unterbrochen wurde.
- **Entriegelt:** Wenn das SIO-Board die Verbindung mit der Mercury-Steuerung verliert, werden die Türen, die sie steuert, entsperrt, unabhängig vom Status, in dem sich die Türen befunden haben, bevor die Verbindung unterbrochen wurde.
- **Verriegelt:** Wenn das SIO-Board die Verbindung mit der Mercury-Steuerung verliert, werden die Türen, die sie steuert, gesperrt, unabhängig vom Status, in dem sich die Türen befunden haben, bevor die Verbindung unterbrochen wurde.
- **Standortcode:** Wenn das SIO-Board die Verbindung zur Mercury-Steuerung verliert, können nur Berechtigungsnachweise mit den konfigurierten Kartenformaten und Einrichtungscodes weiterhin die Türen betreten. Wenn keine Kartenformate oder Einrichtungscodes konfiguriert sind, werden Türen, die das SIO-Board steuert, versperrt, unabhängig vom Status, in dem sich die Türen befunden haben, bevor die Verbindung unterbrochen wurde.

Weitere Informationen dazu finden Sie unter [Offline-Mercury-SIO-Boards konfigurieren, um Zutritt über Einrichtungscodes zu gewähren](#) auf Seite 158.

Führen Sie einen Software-Neustart durch, wenn Sie die Einstellung **Einrichtungscodes** auswählen.

- 16 Um alle Einstellungen auf die Standardwerte zurückzusetzen, außer die Datenbankkayouteinstellungen, klicken Sie auf **Auf Standard zurücksetzen**.

WICHTIG: Es gibt keine Möglichkeit, die vorherigen Einstellungen wiederherzustellen.

- 17 Klicken Sie auf **Speichern**.

Unterschiede zwischen der aktivierten und deaktivierten Mercury-Host-Entscheidungsweitergabe

Ihr Zutrittskontrollsystem verhält sich unterschiedlich, abhängig davon, ob die Mercury-Host-Entscheidungsweitergabe aktiviert oder deaktiviert ist.

Sie können die Mercury-Host-Entscheidungsweitergabe im Synergis™ Appliance Portal aktivieren oder deaktivieren. Navigieren Sie zu **Konfiguration > Mercury-Controller-Einstellungen > Türeinstellungen** und konfigurieren Sie dann die Einstellung **Host-Entscheidungsweitergabe deaktivieren (Offline-Modus)**. Standardmäßig ist diese Einstellung deaktiviert, was bedeutet, dass die Mercury-Host-Entscheidungsweitergabe aktiviert ist und die Synergis™-Cloud-Link-Einheit die Zutrittskontrollentscheidungen trifft.

In der folgenden Tabelle finden Sie Informationen dazu, wann sich Ihr System anders verhält, abhängig davon, ob die Mercury-Host-Entscheidungsweitergabe aktiviert oder deaktiviert ist.

	Host-Entscheidungsweitergabe aktiviert (Standard)	Host-Entscheidungsweitergabe deaktiviert
Zutrittskontrollentscheidungen getroffen von	Synergis Cloud Link	Mercury-Controller
Zeit zwischen Kartenlesung und Türentsperrung	0 bis 5 ¹ Sekunden	Weniger als 1 Sekunde

	Host-Entscheidungsweitergabe aktiviert (Standard)	Host-Entscheidungsweitergabe deaktiviert
Einen Karteninhaber oder einen Berechtigungsnachweis in Security Center löschen <ul style="list-style-type: none"> • Versionen älter als 5.11.3.5 • 5.12.0.0 	Schnell	Up to 1 hour for changes to propagatelo
Einen Karteninhaber oder einen Berechtigungsnachweis in Security Center löschen <ul style="list-style-type: none"> • 5.11.3.6 oder neuer • 5.12.1.0 oder neuer 		Kein Unterschied beim Verhalten
Einen Karteninhaber oder einen Berechtigungsnachweis manuell oder automatisch über das Ablaufdatum deaktivieren		Kein Unterschied beim Verhalten
Zutritt widerrufen, indem ein Karteninhaber von einer Karteninhabergruppe oder einer Zutrittsregel entfernt wird, indem Zeitpläne geändert werden usw. BEMERKUNG: Zutritt widerrufen, indem ein Karteninhaber gelöscht oder deaktiviert wird, ist nicht enthalten.	Schnell	Up to 1 hour for changes to propagatelo
Verriegelung, Anti-Passback und max. Belegung	Unterstützt	Die Option Native Mercury-Bereichssteuerung muss aktiviert sein.

¹ Abhängig von den Netzwerkkonditionen kann dies bis zu 5 Sekunden dauern.

Unterstützung langer Berechtigungen auf Mercury-Controllern aktivieren

Bevor Sie Berechtigungen mit bis zu 240 Bits mit Ihren Mercury-Controllern verwenden können, müssen Sie die Unterstützung für lange Berechtigungen auf Ihrer Synergis™ Cloud Link -Einheit aktivieren.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt werden:

- Auf Ihrer Synergis™ Cloud Link wird Synergis™ Software 11.0 oder höher ausgeführt und sie ist online und mit Ihrem Netzwerk verbunden.
- Die Mercury-Controller, mit denen Sie die Unterstützung für lange Berechtigungsnachweise verwenden möchten, haben die Firmware-Version 1.29.1 oder höher.

Was Sie noch wissen sollten

Da Berechtigungen mit 64 Bits oder länger nicht automatisch mit Mercury synchronisiert werden, müssen Sie sie manuell aktivieren.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
 - 2 Klicken Sie auf **Konfiguration > Mercury-Controller-Einstellungen**.
 - 3 Klicken Sie auf die Registerkarte **Datenbanklayouteinstellungen** im Seitenmenü und wählen Sie dann das Datenbanklayout **Lange Berechtigungsnachweise** aus der Liste aus.
 - 4 Klicken Sie auf die Registerkarte **Lange Berechtigungsnachweisformate** im Seitenmenü und geben Sie dann die Berechtigungsnachweislänge ein, die Sie verwenden möchten.
Der Wert muss zwischen 64 und 240 liegen.
 - 5 Klicken Sie auf **Hinzufügen**.
Sie können bis zu acht verschiedene Berechtigungsformate hinzufügen.
 - 6 Klicken Sie auf **Speichern**.
 - 7 Führen Sie einen Software-Neustart durch:
 - a) Klicken Sie im oberen Menü auf **Neustart > Software-Neustart**.
 - 8 Melden Sie sich nach dem Software-Neustart durch wieder bei der Synergis™ Cloud Link -Einheit an.
 - 9 Klicken Sie auf der Seite *Mercury-Steuerungseinstellungen* auf die Registerkarte **Busse** im Seitenmenü.
 - 10 Klicken Sie auf **Reset** für die Controller, die Unterstützung für lange Berechtigungen benötigen.
- Die neuen Berechtigungsnachweisformate, die Sie aktiviert haben, können mit Ihren Mercury-Controllern verwendet werden.

Beschränkungen der nativen Mercury-Bereichssteuerung

Die ^ nativen Mercury-Bereichssteuerung, die Interlock, max. Belegung und Antipassback umfasst, hat einige Einschränkungen.

- **Weiches Antipassback:** Das Ereignis *Antipassback-Verletzung* für weiches Antipassback wird erzeugt, wenn sich die Tür öffnet, anstatt wenn Zutritt gewährt wird.

Wenn Sie eine weiche Antipassback-Funktion für eine Tür ohne Türsensor konfigurieren, werden *Antipassback-Verletzungseignisse* nie erzeugt, da sich die Tür nie öffnet.

Weiches Antipassback auf Mercury unterstützt keine Präsenz-Zeitüberschreitung.

- **Hartes Antipassback:** Folgendes wird nicht von Mercury unterstützt:

- Hartes Antipassback, das nicht auch auf **Streng** gesetzt ist.
- Striktes und hartes Antipassback, wenn die Einstellung **Globales Antipassback aktivieren** in der Access Manager-Rolle in Config Tool aktiviert ist.

- **Antipassback-Zeitüberschreitung:** Mercury unterstützt eine Zeitüberschreitung bei hartem und strengem Antipassback. Wenn **Präsenzzeitüberschreitung** für einen Bereich konfiguriert ist, verweigert die harte Antipassback-Funktion einem Karteninhaber den Zutritt, bis die Zeitüberschreitung abgelaufen ist; danach kann dem Karteninhaber wieder Zutritt zu dem Bereich gewährt werden.

Dies löst ein *Antipassback-Verletzung*-Ereignis für weiches Antipassback aus, woraufhin hartes Antipassback erneut auf den Karteninhaber angewendet wird, bis der Timer erneut abläuft. Diese Konfiguration ist nicht kompatibel mit Bereichen, die von Synergis™ Software kontrolliert werden.

- **Das Eins-zu-eins-Modell von Mercury für Karteninhaber und Berechtigungen:** Verfügt ein Karteninhaber in Security Center über mehrere Kartenberechtigungen, so wird jede Berechtigung als zu einem separaten Karteninhaber auf der Mercury-Ebene gehörig betrachtet.

Das bedeutet, dass jede Berechtigung einmal zum Betreten desselben Bereichs verwendet werden kann, ohne dass es zu einer Antipassback-Verletzung kommt. Verwendet der Karteninhaber zwei verschiedene Berechtigungen, um einen Antipassback-Bereich mit maximaler Belegung zu betreten, wird er bei der Zählung der maximalen Belegung als zwei Personen gezählt.

- **Antipassback umgehen:** Es werden keine *Antipassback-Verletzungen* von Karteninhabern erzeugt, die die Option **Antipassback-Regeln umgehen** aktiviert haben.
- **Verriegelung und Antipassback:** Verriegelung und Antipassback funktionieren nur, wenn alle in dem diese Funktion nutzenden Bereich konfigurierten Türen vom selben Mercury-Controller gesteuert werden.

Ein Mercury-Controller kann in vielen Bereichen Türen mit einer beliebigen Kombination dieser Merkmale oder auch ohne diese Merkmale haben. In Bereichen, in denen Sie diese Funktionen nicht nutzen, können Sie die Türen von mehreren Mercury-Controllern steuern lassen.

Eine Mercury-gesteuerte Tür kann nur als Ein- und Ausgang eines Bereichs verwendet werden, indem entweder Verriegelung oder Antipassback verwendet wird, obwohl Sie in Security Center mehrere Bereiche für dieselbe Tür konfigurieren können.

- **Verriegelung:** Wenn nur ein Teil der Verriegelung aufgrund des Ausfalls einer einzelnen SIO-Karte offline ist, verhindert die Verriegelung, dass andere Türen im Verriegelungsbereich entriegelt oder geöffnet werden können.

Wenn die native Verriegelung aktiviert ist, werden die Optionen **Überschreiben** und **Sperrung** in Config Tool nicht unterstützt. Die Optionen können konfiguriert werden, ändern aber nichts.

- **Geplantes Antipassback:** Geplantes Anti-Passback wird auf Mercury-Ebene nicht unterstützt. Synergis™ Software aktiviert und deaktiviert Anti-Passback nach einem Zeitplan, solange die Mercury-Controller verbunden sind oder wenn sie sich wieder verbunden und der Zeitplan nicht auf *Immer* eingestellt ist. Mercury geht nicht in den Zeitplan selbst über, sondern bleibt in seinem Zustand zum Zeitpunkt der Unterbrechung.
- **Diskrepanzen bei der Personenzählung:** Da Mercury seine eigenen Bereiche verfolgt, kann es in einigen Fällen vorkommen, dass die Personenzählung auf dem Synergis™ Cloud Link, im Task Security Desk *Personenzählung* und auf dem Mercury-Controller nicht übereinstimmt. Um zu verhindern, dass diese Diskrepanzen zu Problemen führen, wird empfohlen, die Personenzählung regelmäßig wie folgt zurückzusetzen:
 - Navigieren Sie im Synergis™ Appliance Portal zu **Konfiguration > Parameter für die gesamte Einheit > Bereichskonfiguration**, und planen Sie dann eine tägliche oder wöchentliche Rücksetzung. Dadurch wird die Personenzählung auf dem Synergis™ Cloud Link und auf den von ihm verwalteten Mercury-Controllern zurückgesetzt.
 - Setzen Sie im Config Tool die Zählung im Task *Personenzählung* zurück, indem Sie die Aktion *Bereichs-Personenzählung zurücksetzen* in geplanten Tasks oder Event-to-Actions für jeden zu löschenden Bereich verwenden.

Konfigurieren des REX-Modus für die Erweiterte zugesicherte Zeit von Mercury pro Tür

Bevor Sie den REX-Modus für die Erweiterte zugesicherte Zeit an bestimmten Türen aktivieren können, müssen Sie ein türspezifisches Feld in Security Center erstellen.

Was Sie noch wissen sollten

- Diese Funktion erfordert die Mercury-Firmware 1.29.1 oder höher.
- Wenn der REX-Modus mit erweiterter zugesicherter Zeit aktiviert ist, bleibt die Tür so lange entriegelt, wie der REX-Eingang aktiv ist, und danach für die normale Freigabezeit. Dies ist nützlich, um zu verhindern, dass Türen, die durch einen Bewegungssensor gesteuert werden, alle paar Sekunden ver- und entriegelt werden.
- Beachten Sie die folgenden Einschränkungen dieser Funktion:
 - Wenn der Mercury-Controller neu startet, kehrt die Tür in ihren normalen Zustand zurück, bis der REX erneut ausgelöst wird.
 - Wenn kein Türsensor vorhanden ist, bleibt die Tür entweder so lange entriegelt, wie der REX-Eingang aktiv ist, oder für die normale Gewährungszeit, je nachdem, welcher Zeitraum länger ist.
 - Die Tür wird am Ende eines Entsperrungszeitplans unabhängig vom REX-Status verriegelt.
- Wenn Sie alle Mercury-gesteuerten Türen unter demselben Synergis™ Cloud Link zur gleichen Zeit steuern möchten, können Sie [die Einstellung Erweiterte zugesicherte Zeit im REX-Modus im Synergis™ Appliance Portal statt](#) konfigurieren.

BEMERKUNG: Wenn Sie das benutzerdefinierte Feld in Security Center erstellen, werden die Einstellungen für Synergis™ Cloud Link-Einheiten ignoriert, die in diesem System registriert sind.

Prozedur

- 1 Öffnen Sie den Task *System* auf der Config Tool-Startseite und klicken Sie auf die Ansicht **Allgemeine Einstellungen**.
- 2 Klicken Sie auf die Registerkarte **Benutzerdefinierte Felder** und dann auf **Einen Eintrag hinzufügen (+)**.
- 3 Legen Sie im Dialogfeld *Benutzerdefiniertes Feld hinzufügen* die folgenden Werte fest:
 - **Entitätstyp:** Wählen Sie **Tür** aus.
 - **Datentyp:** Wählen Sie **Boolesch**.
 - **Name:** Geben Sie *Erweiterte zugesicherte Zeit im REX-Modus* ein.
 - **Standardwert:** Wählen Sie diese Option, wenn Sie möchten, dass die Türen standardmäßig mit *Erweiterte zugesicherte Zeit im REX-Modus* arbeiten.

- 4 Klicken Sie auf **Speichern und schließen** und dann auf **Anwenden**.

Datenbank-Layouts für Mercury-Controller

Für Ihre Mercury-Controller stehen verschiedene Datenbanklayouts zur Auswahl.

In den folgenden Tabellen können Sie nachlesen, welches Datenbanklayout für Ihre Bedürfnisse geeignet ist.

Funktionsreiches Datenbanklayout (Default)

Modell	Maximale Anzahl der Karteninhaber
EP1501, EP1502	145.000
EP2500	370.000
M5-IC, MS-ICS	370.000
EP4502	419.000
LP1501, LP1502	200.000
LP2500	419.000
LP4502	500.000
MP1502	200.000
MP4502	500.000

Funktionsunterstützung	Unterstützt
Default-PIN-Länge	6
Maximale PIN-Länge	10
Native Bereichssteuerung (Antipassback, Verriegelung und maximale Belegung)	Ja
Zwei-Personen-Regel und Besucherbegleitung	Ja
Maximale Länge von Berechtigungen (Bit)	64
Aufzüge	Ja

Datenbanklayout mit langer Berechtigung

Modell	Maximale Anzahl der Karteninhaber
EP1501, EP1502	80.000
EP2500	210.000
M5-IC, MS-ICS	214.000
EP4502	210.000
LP1501, LP1502	111.000
LP2500	222.000
LP4502	444.000

Modell	Maximale Anzahl der Karteninhaber
MP1502	111.000
MP4502	444.000

Funktionsunterstützung	Unterstützt
Default-PIN-Länge	6
Maximale PIN-Länge	10
Native Bereichssteuerung (Antipassback, Verriegelung und maximale Belegung)	Ja
Zwei-Personen-Regel und Besucherbegleitung	Ja
Maximale Länge von Berechtigungen (Bit)	240
Aufzüge	Ja

Layout der Datenbank für lange PINs

Modell	Maximale Anzahl der Karteninhaber
EP1501, EP1502	80.000
EP2500	300.000
M5-IC, MS-ICS	300.000
EP4502	300.000
LP1501, LP1502	150.000
LP2500	350.000
LP4502	500.000
MP1502	150.000
MP4502	500.000

Funktionsunterstützung	Unterstützt
Default-PIN-Länge	15
Maximale PIN-Länge	15
Native Bereichssteuerung (Antipassback, Verriegelung und maximale Belegung)	Ja
Zwei-Personen-Regel und Besucherbegleitung	Ja

Funktionsunterstützung	Unterstützt
Maximale Länge von Berechtigungen (Bit)	64
Aufzüge	Ja

Großes Datenbanklayout

Modell	Maximale Anzahl der Karteninhaber
EP1501, EP1502	250.000
EP2500	560.000
M5-IC, MS-ICS	560.000
EP4502	600.000
LP1501, LP1502	250.000
LP2500	600.000
LP4502	600.000
MP1502	250.000
MP4502	600.000

Funktionsunterstützung	Unterstützt
Default-PIN-Länge	6
Maximale PIN-Länge	6
Native Bereichssteuerung (Antipassback, Verriegelung und maximale Belegung)	Nein
Zwei-Personen-Regel und Besucherbegleitung	Nein
Maximale Länge von Berechtigungen (Bit)	64
Aufzüge	Nein

FICAM-Datenbanklayout

Das FICAM-Datenbanklayout sollte nur dann verwendet werden, wenn Sie den Anforderungen des Federal Information Processing Standard 201 (FIPS 201) durch Berechtigungen vom Typ Personal Identity Verification (PIV), Personal Identity Verification-Interoperable (PIV-I) oder Commercial Identity Verification (CIV) entsprechen wollen. Dieses Datenbanklayout ist nur für die Verwendung mit Mercury LP4502-Controllern vorgesehen.

Weitere Informationen finden Sie im [HID-pivCLASS-Benutzerhandbuch für Security Center](#) oder [TI-EntryPoint-Authentifizierung auf Mercury LP4502 – Technote](#).

Modell	Maximale Anzahl der Karteninhaber
EP1501, EP1502	98.000
EP2500	180.000
M5-IC, MS-ICS	100.000
EP4502	180.000
LP1501, LP1502	139.000
LP2500	279.000
LP4502	500.000

Funktionsunterstützung	Unterstützt
Default-PIN-Länge	6
Maximale PIN-Länge	6
Native Bereichssteuerung (Antipassback, Verriegelung und maximale Belegung)	Online
Zwei-Personen-Regel und Besucherbegleitung	Ja
Maximale Länge von Berechtigungen (Bit)	240
Aufzüge	Ja

Informationen über die Konfiguration von PINs mit führenden Nullen für Mercury-Integrationen

Bevor Sie PINs mit führenden Nullen für Ihre Mercury-Integration im Synergis™ Appliance Portal konfigurieren, erfahren Sie mehr über die Anforderungen und wie sich die Einstellungen für die **Maximale PIN-Länge** und die **PIN-Länge nach dem Hinzufügen von führenden Nullen** auf Ihre PINs auswirken.

Voraussetzungen

Das Verwenden von PIN-Berechtigungsnachweisen in Mercury-Integrationen erfordert Folgendes:

- Security Center 5.7 SR2 oder neuer ist erforderlich, um sechsstellige PINs mit führenden Nullen zu verwenden. In 5.7 SR1 und älter funktionieren sechsstellige PINs mit führenden Nullen nicht. Der Zutritt wird dennoch gewährt, aber Sie erhalten kein *Zutritt gewährt*-Ereignis in Security Center.
- Jeder Karteninhaber muss einen Kartenberechtigungsnachweis und nur einen PIN-Berechtigungsnachweis haben.
- Wenn die Lesegeräteinstellung für alle Einheiten **Karte oder PIN** lautet, der Karteninhaber aber nur über einen PIN-Berechtigungsnachweis verfügt, wird dieser Berechtigungsnachweis nicht mit der Mercury-Steuerung synchronisiert und funktioniert nicht.
Abhilfemaßnahme: Erstellen Sie einen Dummy-Karten-Berechtigungsnachweis weisen Sie diesen dem Karteninhaber zu.
- HID-Tastaturlesegeräte müssen die Option mode-00 unterstützen.

Informationen über die maximale PIN-Länge mit führenden Nullen

Um führende Nullen für Ihre PINs zu konfigurieren, müssen Sie die Einstellung **PIN-Länge nach dem Hinzufügen von führenden Nullen** auf der Seite *Mercury-Steuerungseinstellungen* im Synergis Appliance Portal bearbeiten. Die Einstellungen **PIN-Länge nach dem Hinzufügen von führenden Nullen** und **Maximale PIN-Länge** beeinflussen einander auf folgende Weise:

- PINs funktionieren nicht mehr, wenn die **PIN-Länge nach dem Hinzufügen von führenden Nullen** größer ist als die **Maximale PIN-Länge**.
- Führende Nullen werden zu kürzeren PINs hinzugefügt, bis sie die **PIN-Länge nach dem Hinzufügen von führenden Nullen** und nicht die **Maximale PIN-Länge** erreicht haben.
- PINs, die gleich lang oder länger sind als die **PIN-Länge nach dem Hinzufügen von führenden Nullen**, sind gültig, solange sie nicht die **Maximale PIN-Länge** überschreiten.

Die **Maximale PIN-Länge** ist auf **6** festgelegt. Die **PIN-Länge nach Hinzufügen führender Nullen** ist auf **4** festgelegt.

- Wenn die ursprüngliche PIN **9** war, wird die PIN zu **0009**.
- Wenn die ursprüngliche PIN **123** war, wird die PIN zu **0123**.
- Wenn die ursprüngliche PIN **12345** war, bleibt die PIN gleich.

Informationen über das Gewähren von Zutritt mit Offline-Mercury-SIO-Boards

Erfahren Sie mehr darüber, wie Zutrittsentscheidungen beeinflusst werden, wenn Sie konfigurieren, dass Zutritt nur Berechtigungsnachweisen mit bestimmten Kartenformaten und Einrichtungscodes gewährt wird, wenn das SIO-Board die Verbindung mit der Mercury-Steuerung verliert.

- Standardmäßig unterstützt Synergis Software bis zu acht Kartenformate pro Mercury-Steuerung. Jeder Einrichtungscodes, den Sie hinzufügen, zählt als ein Kartenformat, selbst wenn die Einrichtungscodes für das gleiche Kartenformat konfiguriert werden.
BEMERKUNG: Um die Anzahl der unterstützten Kartenformate auf 16 zu erhöhen, können Sie die Option **Magstripe-Unterstützung** im Abschnitt *Erweiterte Einstellungen* auf der Seite *Mercury-Steuerungseinstellungen* deaktivieren. Magstripe wird nicht unterstützt, wenn die Option **Einrichtungscodes** als Türverhalten für Offline-SIO-Boards ausgewählt ist, auch wenn Sie die Option **Magstripe-Unterstützung** aktivieren.
- Wenn das SIO-Board die Verbindung mit der Mercury-Steuerung verliert und keine Kartenformate oder Einrichtungscodes im Synergis™ Appliance Portal hinzugefügt sind, werden die Türen, die das SIO-Board steuert, gesperrt, unabhängig vom Status, in dem sie sich befunden haben, bevor die Verbindung unterbrochen wurde.
- Folgendes passiert, wenn ein Berechtigungsnachweis in Security Center gültig ist, der Einrichtungscodes aber nicht im Synergis Appliance Portal hinzugefügt ist:
 - Wenn die Verbindung der Mercury-Steuerung von der Synergis™ Cloud Link-Einheit getrennt wird, wird Zutritt verweigert.
 - Wenn die Mercury-Steuerung mit der Synergis™ Cloud Link-Einheit verbunden ist, wird Zutritt gewährt.

Mercury – Native Bereichssteuerung, Host-Entscheidungsweitergabe und Anti-Passback

Wenn Sie das Türverhalten für Offline-SIO-Boards konfigurieren, damit Einrichtungscodes zum Gewähren von Zutritt verwendet werden, variieren Zutrittsentscheidungen basierend darauf, welche anderen Funktionen aktiviert sind und wie zusammenarbeiten.

In diesem Beispiel wird von Folgendem ausgegangen:

- Die Option **Einrichtungscodes** ist als Türverhalten für Offline-SIO-Boards im Synergis Appliance Portal ausgewählt.
- Karteninhaber 1 hat einen Berechtigungsnachweis mit einem Einrichtungscodes, der im Synergis Appliance Portal hinzugefügt ist.

- Karteninhaber 2 hat einen Berechtigungsnachweis mit einem Einrichtungscode, der *nicht* im Synergis Appliance Portal hinzugefügt ist.
- Anti-Passback wird in den Bereichen angewendet, die die Karteninhaber zu betreten versuchen.
- Die Verbindung der Mercury-Steuerung mit der Synergis™ Cloud Link-Einheit ist getrennt.

Einstellung in the Synergis Appliance Portal		
Native Mercury-Bereichssteuerung	Übertragung durch Host deaktivieren (Offline-Modus)	Zutrittsentscheidung nach dem erneuten Vorweisen eines Berechtigungsnachweises an der Tür
Deaktiviert	Deaktiviert	<ul style="list-style-type: none"> • Karteninhaber 1 erhält einen Anti-Passback-Verstoß. • Karteninhaber 2 erhält einen Anti-Passback-Verstoß.
Deaktiviert	Aktiviert	<ul style="list-style-type: none"> • Anti-Passback funktioniert nicht.
Aktiviert	Deaktiviert	<ul style="list-style-type: none"> • Karteninhaber 1 erhält einen Anti-Passback-Verstoß. • Karteninhaber 2 wird der Zutritt verweigert.
Aktiviert	Aktiviert	<ul style="list-style-type: none"> • Karteninhaber 1 erhält einen Anti-Passback-Verstoß. • Karteninhaber 2 wird der Zutritt verweigert.

Offline-Mercury-SIO-Boards konfigurieren, um Zutritt über Einrichtungscode zu gewähren

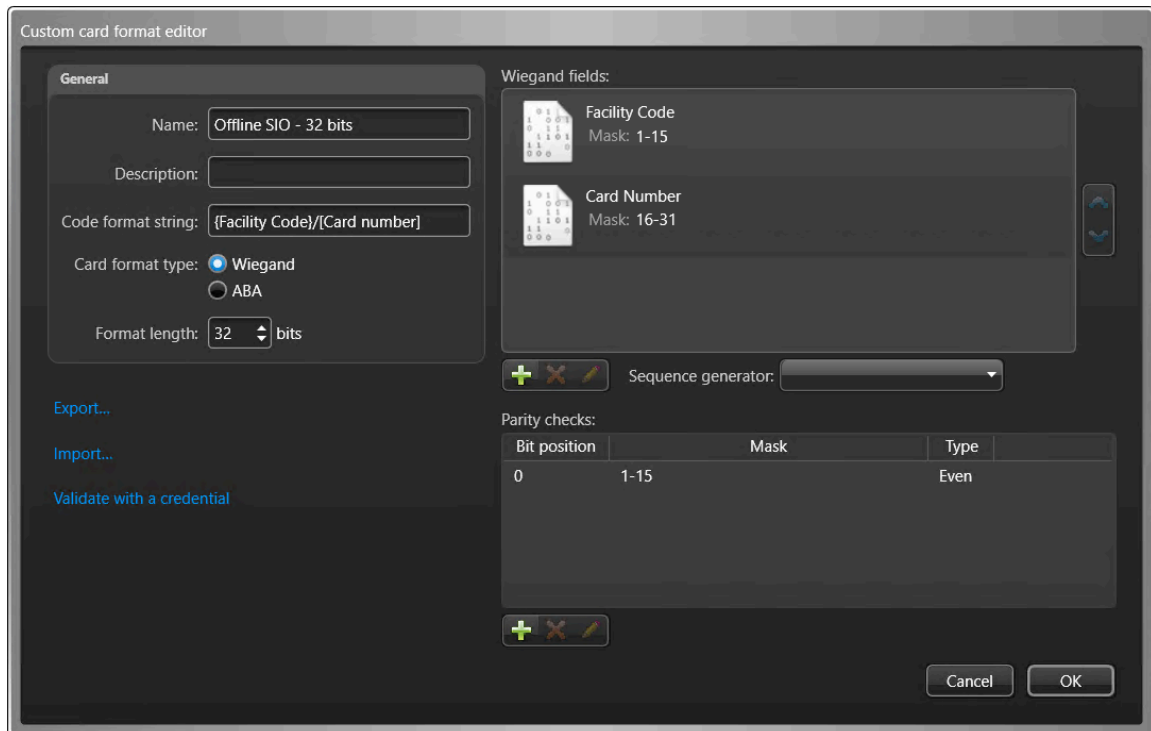
Sie können konfigurieren, dass Zutritt nur Berechtigungsnachweisen mit bestimmten Kartenformaten und Einrichtungscode oder bestimmten Raw-Kartenformaten gewährt wird, wenn die Verbindung zwischen dem SIO-Board und dem Mercury-Controller verloren geht.

Bevor Sie beginnen

- **ACHTUNG:** Wenn Sie konfigurieren, dass Zutritt über Einrichtungscode oder Kartenformate gewährt wird, wenn das SIO-Board die Verbindung mit der Mercury-Steuerung verliert, wird die Sicherheit Ihres Systems wesentlich verringert. Wenn dies konfiguriert ist, ist kein Aktivitätsverlauf verfügbar. Ereignisse, die auftreten, während das SIO-Board nicht mit dem Mercury-Controller verbunden ist, werden nicht aufgezeichnet.
- [Erfahren Sie mehr darüber, welche Auswirkungen das Gewähren von Zutritt über Kartenformate und Einrichtungscode auf Zutrittsentscheidungen hat.](#)
- Um ein benutzerdefiniertes Wiegand-Kartenformat zu verwenden, erstellen Sie es in Config Tool und exportieren Sie es als XML-Datei. Das benutzerdefinierte Kartenformat muss mit einem Wiegand-Feld

namens Einrichtungscodes konfiguriert werden. Die Maske des Wiegand-Feldes muss eine aufsteigende Folge von Bits sein, die bis zu 63 Bits lang sein kann.

Beispiel:



Weitere Informationen finden Sie unter [Benutzerdefinierte Kartenformate erstellen](#).

Prozedur

So gewähren Sie Zutritt über ein Kartenformat und einen Einrichtungscodes:

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Mercury-Controller-Einstellungen**.
- 3 Klicken Sie im Seitenmenü auf die Registerkarte **Türverhalten bei Offline-SIO-Boards** und wählen Sie **Einrichtungscodes** aus.

- 4 (Optional) Führen Sie die folgenden Schritte durch, um ein benutzerdefiniertes Kartenformat zu verwenden:
- Klicken Sie im Abschnitt *Benutzerdefinierte Wiegand-Kartenformate* auf **Datei auswählen** und wählen Sie die XML-Datei aus, die Sie aus Config Tool exportiert haben.
 - Klicken Sie auf **Kartenformat importieren**.

Das benutzerdefinierte Kartenformat wird jetzt im Abschnitt *Benutzerdefinierte Wiegand-Kartenformate* aufgelistet und kann jetzt im Drop-down-Menü **Kartenformat** im Abschnitt *Türverhalten für Offline-SIO-Boards* ausgewählt werden.

Beispiel:

Door behavior for offline SIO boards

Setting 'Facility code' as the door behavior greatly reduces the security of your system. With this behavior set, when the SIO board loses connection with the Mercury controller, access is granted based only on facility codes and without activity trails.

Facility code

Card format: Offline SIO - 32 bits

Facility code: | Add

Custom Wiegand card formats

Select file: OfflineSIO_CustomCardFormat_32.xml (1.20 KB)

Import card format

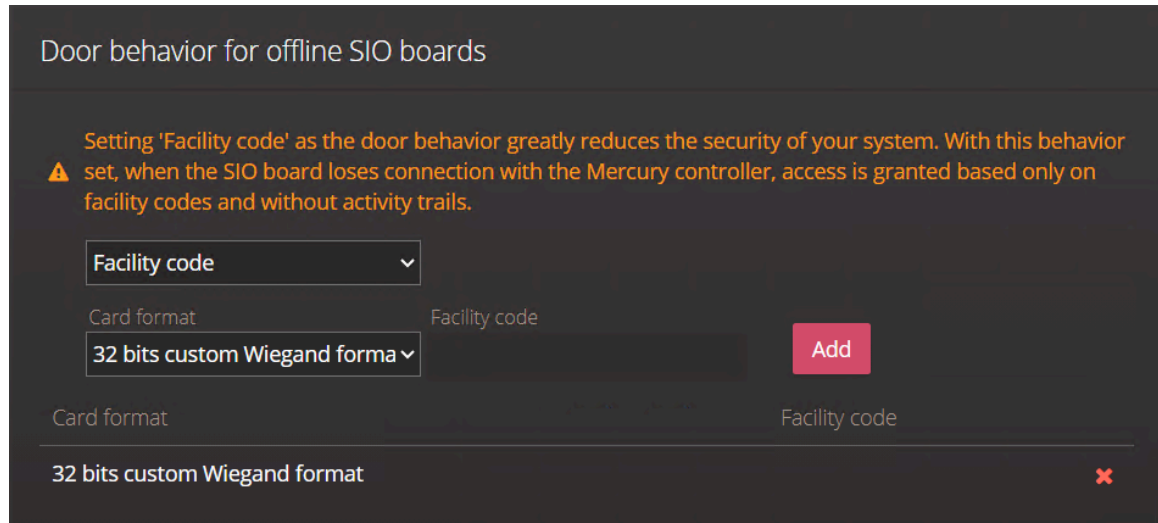
Card format	Wiegand format length (bits)
Offline SIO - 32 bits	32

- Wählen Sie in der Liste **Kartenformat** ein Kartenformat aus und geben Sie einen Wert im Feld **Einrichtungscod** ein.
- Klicken Sie auf **Hinzufügen**.
Das konfigurierte Kartenformat und der Einrichtungscod werden zur Liste hinzugefügt.
- Klicken Sie auf **Speichern** und führen Sie dann einen Software-Neustart durch.
Zurzeit wird nur Berechtigungsnachweisen gewährt, die sowohl mit dem Kartenformat als auch dem Einrichtungscod übereinstimmen.

So gewähren Sie Zutritt über ein benutzerdefiniertes Raw-Kartenformat:

- Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- Klicken Sie auf **Konfiguration > Mercury-Controller-Einstellungen**.

- 3 Fügen Sie ein benutzerdefiniertes Kartenformat hinzu, indem Sie die folgenden Schritte ausführen:
 - a) Klicken Sie auf die Registerkarte **Lange Berechtigungsnachweisformate** im Seitenmenü und geben Sie dann die Berechtigungsnachweislänge ein, die Sie verwenden möchten.
 - b) Klicken Sie auf **Hinzufügen**.
 Das benutzerdefinierte Kartenformat kann jetzt aus der Drop-down-Liste **Kartenformat** im Abschnitt *Türverhalten für Offline-SIO-Boards* ausgewählt werden.
- 4 Klicken Sie im Seitenmenü auf die Registerkarte **Türverhalten bei Offline-SIO-Boards** und wählen Sie **Einrichtungscodes** aus.
- 5 Wählen Sie im Drop-down-Menü **Kartenformat** das benutzerdefinierte Kartenformat aus und klicken Sie auf **Hinzufügen**.

Beispiel:

- 6 Klicken Sie auf **Speichern** und führen Sie dann einen Software-Neustart durch. Zurtitt wird nur Berechtigungsnachweisen gewährt, die mit dem benutzerdefinierten Kartenformat übereinstimmen, unabhängig vom Einrichtungscodes.

Überlegungen zur Installation von OSDP-Lesegeräten mit Mercury

Vor dem Hinzufügen von OSDP-Lesegeräten zu Ihren Mercury-Controllern sind einige Punkte zu beachten.

Einschränkungen

Der Verbindungsstatus der OSDP- und OSDP 2-Lesegeräte auf Mercury-Controllern wird nicht aktualisiert, wenn das Lesegerät keiner Tür oder keinem Aufzug zugewiesen ist.

BEMERKUNG: Diese Einschränkung gilt auch für Out-Lesegeräte, wenn zwei OSDP-Lesegeräte pro Port verwendet werden.

Unterstützte Onboard-OSDP-Leser mit Mercury-Controllern

Der folgenden Tabelle können Sie entnehmen, wie viele OSDP-Lesegeräte Synergis™ Software zusammen mit Mercury unterstützt:

Modell	Onboard-Lesegerätanschlüsse	Maximale Anzahl an Onboard-OSDP-Lesegeräten pro Panel
MR50-S2 ¹	1	1
MR50-S3	1	2 (zwei auf einem Anschluss) ²
MR52-S2 ¹	2	2 (einer pro Anschluss)
MR52-S3	2	4 (zwei pro Anschluss) ²
MR51e	2	2 (nur zwei auf einem Anschluss)
MR62e	1	4 (vier an einem Anschluss)
EP1501	2	2 (nur zwei auf einem Anschluss)
EP1502	2	2 (einer pro Anschluss)
EP4502	2	2 (einer pro Anschluss)
LP1501	2	2 (nur zwei auf einem Anschluss)
LP1502	2	4 (zwei pro Anschluss) ²
LP4502	2	4 (zwei pro Anschluss) ²
MP1502	2	4 (zwei pro Anschluss) ²
MP4502	2	4 (zwei pro Anschluss) ²

BEMERKUNG: Mercury EP2500-, LP2500--Controller sind nicht aufgeführt, da sie keine integrierten Lesegerätanschlüsse haben. Sie unterstützen OSDP-Lesegeräte über die in der Tabelle aufgeführten Schnittstellenmodule.

¹ Serie 2 MR50 und Serie 2 MR52 unterstützen OSDP Secure Channel oder zwei OSDP-Lesegeräte pro Anschluss nicht.

² Zwei OSDP-Lesegeräte pro Anschluss werden über die Einstellung **Zwei OSDP-Lesegeräte pro Lesegeräteanschluss** unterstützt. Diese Einstellung wird auf der Seite *Mercury-Controller-Einstellungen* im Synergis™ Appliance Portal aktualisiert.

Verdrahtungshinweise für OSDP-Lesegeräte

Abhängig von der Baugruppen- und Leiterplattenrevision Ihres Mercury-Schnittstellenmoduls und der EP-, LP- oder MP-Controller müssen bestimmte Installationsanforderungen erfüllt werden:

- Ein 1-kOhm-Pulldown-Widerstand muss zwischen den Mercury DAT/D0- und GND-Leitungen auf Schnittstellenmodulen und EP-, LP- oder MP-Controllern eingefügt werden.
- Der Pulldown-Widerstand muss am Panel installiert werden.
- Um ordnungsgemäß zu funktionieren, dürfen in der Anlage keine Erdungsfehler vorhanden sein. Stellen Sie sicher, dass die Gleichstromerde (Rückleitung der Stromversorgung) nicht mit der Erdung verbunden ist.
- Die Verdrahtung für Wiegand kann für OSDP wiederverwendet werden. Wiegand-Standardkabel entsprechen jedoch möglicherweise nicht den RS-485-Twisted-Pair-Empfehlungen.
- Eine sternförmige Verdrahtung wird nicht empfohlen.

Um herauszufinden, ob Sie einen 1-k-Ohm-Pulldown-Widerstand zwischen D0 und GND hinzufügen müssen, sehen Sie unter [KBA-78953](#) nach.

Weitere Informationen zur Verkabelung der OSDP-Lesegeräte finden Sie unter [Anschluss der Mercury-Schnittstellenmodule in Synergis Cloud Link](#).

Abschlusswiderstände

Die folgenden Anweisungen sind besonders wichtig, wenn Sie mit einer hohen Baudrate arbeiten, beispielsweise 115.200 Baud:

- Bei OSDP-Kabeln, die länger als 200 ft. (61 m) sind oder bei Vorliegen von EMV-Störungen installieren Sie einen 120-Ohm-Widerstand an beiden Enden der RS-485-Verkettung.
- Bei Wiegand-Kabeln, die länger als 32 ft. (10 m) sind oder bei Vorliegen von EMV-Störungen installieren Sie einen 120-Ohm-Widerstand an beiden Enden der RS-485-Verkettung.

Wenn Kommunikationsfehler auftreten, können Sie die Baudrate verringern, Abschlusswiderstände hinzufügen oder beides.

OSDP-Lesegeräte (Secure Channel) zu einem Mercury-Controller hinzufügen

Um ein OSDP-Lesegerät (Secure Channel) zu einem Mercury LP- oder MP-Controller hinzuzufügen, müssen Sie zuerst das Lesegerät mit dem Config Tool auf dem Controller konfigurieren und es dann über das Synergis™ Appliance Portal mit dem Controller koppeln.



Bevor Sie beginnen

Registrieren Sie Ihren Controller mit seinen nachgeschalteten Panels auf Ihrer Synergis™-Einheit.

Was Sie noch wissen sollten

- Um ein OSDP-Lesegerät (Secure Channel) zum Mercury-Controller hinzuzufügen, müssen Sie das Lesegerät (Austausch von Tasten) mit dem Controller koppeln, mit dem es verbunden ist. Um ein Lesegerät im sicheren Modus mit einem anderen Lesegeräteanschluss zu koppeln, wenn es bereits sicher mit einem Lesegeräteport gekoppelt ist, setzen Sie das Lesegerät auf die Werkseinstellungen zurück.
- Ab Synergis™ Software 11.2 reagieren angeschlossene OSDP-Lesegeräte nicht, wenn ihnen Karten vorgelegt werden, es sei denn, sie sind für die Steuerung einer Tür oder eines Aufzugs in Security Center konfiguriert.
- Gültige Adressen für von Mercury gesteuerte OSDP-Lesegeräte sind 0 bis 3.

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Wählen Sie in der Entitätsstruktur die Synergis-Einheit aus und klicken Sie auf die Registerkarte **Peripheriegeräte**.
- 3 Erweitern Sie ggf. den Controller, um die nachgeschalteten MR-Panels und Peripheriegeräte anzuzeigen.
- 4 Klicken Sie auf das Lesegerät () , das Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten** ().

- 5 Klicken Sie im Dialogfeld *Lesegerät bearbeiten* auf die Dropdown-Liste **Lesegerättyp** und wählen Sie **OSDPv2** aus.

Beispiel:

BEMERKUNG: Die Option **Gesichert** muss aktiviert sein.

- 6 Konfigurieren Sie die anderen Einstellungen im Abschnitt *Nur OSDP (Secure Channel)* nach Bedarf und klicken Sie auf **Speichern**.
- 7 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 8 Klicken Sie auf **Konfiguration > Erweitertes OSDP**.
- 9 Suchen Sie nach der Reihe mit dem konfigurierten Port, Lesegerät sowie zugehöriger Tür und klicken Sie auf **Koppeln starten**.

Dadurch werden die Schlüssel ausgetauscht und das Lesegerät ist wieder online. Das Lesegerät ist jetzt sicher. Jedes Gerät, das den Schlüssel ablehnt, bleibt offline.

Secure OSDP Pairing			
Doors	Readers	Status	Action
-	OSDP (Port D, Address 0)	● Offline	Start pairing
Direct OSDP	OSDP (Port D, Address 1)	● Online	Paired

10 Wiederholen Sie Schritt 9 für die verbleibenden Lesegeräte.

Dadurch werden die Schlüssel ausgetauscht und die Lesegeräte sind wieder online. Die Lesegeräte sind nun sicher; jedes Lesegerät, das den Schlüssel ablehnt, bleibt offline.

Nachdem der Kopplungsvorgang abgeschlossen ist, wird das Lesegerät online im Config Tool angezeigt.

Konfigurieren von zwei OSDP-Lesegeräten pro Mercury-Gerät

Die folgenden Mercury-Geräte können jeweils zwei OSDP-Lesegeräte unterstützen: EP1501, LP1501, und MR51e. Um diese Funktion zu aktivieren, müssen Sie beide Lesegeräte so konfigurieren, dass sie den ersten Lesegerätanschluss am Mercury-Gerät verwenden.

Bevor Sie beginnen

[Konfigurieren Sie die OSDP-Lesegeräte.](#)

Was Sie noch wissen sollten

- Bei Mercury EP1501-, LP1501--Controllern ist der erste Anschluss die Klemmleiste TB2.
- Bei nachgeschalteten Mercury MR51e-Panels ist der erste Anschluss die Klemmleiste TB3.
- Wenn Sie zwei OSDP-Lesegeräte am ersten Anschluss konfigurieren, können Sie den zweiten Anschluss nicht verwenden.
- Mercury EP1501, LP1501 müssen ohne Erweiterungskarten registriert werden, damit der erste Anschluss für die beiden OSDP-Lesegeräte zur Verfügung steht.

Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
- 2 Wählen Sie in der Entitätsstruktur die Synergis-Einheit aus und klicken Sie auf die Registerkarte **Peripheriegeräte**.
- 3 Führen Sie einen Doppelklick auf **Lesegerät 1** aus und konfigurieren Sie die folgenden Einstellungen:
 - **Art des Lesegeräts:** Wählen Sie **OSDP 2** aus.
 - **Baudrate:** Wählen Sie eine Bitrate aus.
 - **Adresse:** Wählen Sie die Adresse aus, die Sie für das erste Lesegerät konfiguriert haben.
- 4 Wiederholen Sie Schritt 3 für **Lesegerät 2**, wobei Sie die für das zweite Lesegerät konfigurierte Adresse verwenden.
Wenn Sie **OSDP 2** für beide Lesegeräte auswählen, werden beide Lesegeräte automatisch dem ersten Anschluss zugewiesen.
- 5 (Optional – nur unterstützte Lesegeräte) Stellen Sie sicher, dass die Option **Gesichert** auf **EIN** gesetzt ist.

Konfigurieren von Mercury-Geräten für die Nutzung von zwei OSDP-Lesegeräten pro Anschluss

Die folgenden Mercury-Geräte unterstützen zwei OSDP-Lesegeräte an jedem ihrer integrierten Lesegerätanschlüsse: LP1502, LP4502, MP1502, MP4502, MR50-S3 und MR52-S3. Sie müssen diese Funktion im Synergis™ Appliance Portal aktivieren, bevor Sie die Lesegeräte im Config Tool konfigurieren.

Was Sie noch wissen sollten

- Damit zwei OSDP-Lesegeräte pro Anschluss auf Mercury LP1502, LP4502, MR50-S3 und MR52-S3 unterstützt werden, ist Security Center 5.10.4.0 oder höher erforderlich.

- Damit zwei OSDP-Lesegeräte pro Anschluss auf Mercury MP1502 und MP4502 unterstützt werden, ist Security Center 5.12.1.0 oder höher erforderlich.
- Wenn die Option **Zwei OSDP-Lesegeräte pro Lesegeräteanschluss** im Synergis Appliance Portal aktiviert ist und Sie nur eines der OSDP-Lesegeräte auf einer Tür konfigurieren, müssen Sie sicherstellen, dass das konfigurierte Lesegerät das primäre Lesegerät ist. Andernfalls wird sich die Tür im Warnstatus befinden, obwohl sie funktioniert.

Prozedur

- 1 Aktivieren Sie im Synergis Appliance Portal die Option **Zwei OSDP-Lesegeräte pro Lesegeräteanschluss** auf der Seite *Mercury-Controller-Einstellungen* .
BEMERKUNG: Wenn diese Option aktiviert ist, ist die Option **Smart Card** standardmäßig auf dem OSDP-Lesegerät im Config Tool aktiviert und bleibt im Hintergrund aktiviert, auch wenn Sie die Option deaktivieren.
- 2 Starten Sie Synergis Software neu.
- 3 Fügen Sie zwei OSDP-Lesegeräte zum Lesegeräteanschluss der Mercury-Steuerung hinzu:
 - a) Öffnen Sie auf der Config Tool-Startseite den Task *Zutrittskontrolle* und klicken Sie auf die Ansicht **Rollen und Einheiten**.
 - b) Wählen Sie im Einheitendiagramm die Synergis™-Einheit aus und klicken Sie auf die Registerkarte **Peripheriegeräte**.
 - c) Führen Sie einen Doppelklick auf **Lesegerät 1** aus und konfigurieren Sie die folgenden Einstellungen:
 - **Art des Lesegeräts:** Wählen Sie **OSDP 2** aus.
 - **Baudrate:** Wählen Sie eine Bitrate aus.
 - **Adresse:** Wählen Sie die Adresse aus, die Sie für das erste Lesegerät konfiguriert haben.
 - d) Klicken Sie auf **Speichern**.
 - e) Führen Sie einen Doppelklick auf **Lesegerät 1 aus** durch und wählen Sie die Adresse aus, die Sie für das zweite Lesegerät konfiguriert haben.
BEMERKUNG: Nur die Adresse muss konfiguriert werden, da *Lesegerät 1* und *Lesegerät 1 aus* bis auf die Adresse die gleiche Konfiguration verwenden.
- 4 Weisen Sie die Lesegeräte einer Tür zu.
Beispiel: *Lesegerät 1* und *Lesegerät 1 aus* müssen auf der gleichen Tür festgelegt sein und *Lesegerät 2* und *Lesegerät 2 aus* müssen auf der gleichen Tür festgelegt sein.
- 5 Wenn die Steuerung einen zweiten Lesegeräteanschluss hat, können Sie Schritt 3 wiederholen, um *Lesegerät 2* und *Lesegerät 2 aus* auf dem zweiten Anschluss zu konfigurieren.

Nach Durchführen dieser Schritte

Koppeln Sie OSDP-Lesegeräte im Synergis™ Appliance Portal. Wenn Sie OSDP 2 verwenden, müssen Sie den *Installationsmodus* möglicherweise nach der Koppelung auf dem Lesegerät deaktivieren, wenn er nach dem Koppeln nicht deaktiviert wird.

Hinzufügen von MR51e-Panels zu einem Mercury-Controller

MR51e ist ein eintüriges PoE-Panel, das über einen Mercury-Controller gesteuert werden muss. Damit das MR51e-Panel mit dem Controller kommunizieren kann, müssen Sie das MR51e-Panel so einstellen, dass es entweder den öffentlichen DHCP- (empfohlen) oder den statischen IP-Adressierungsmodus verwendet.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- Falls noch nicht geschehen, laden Sie die MR51e-Panels mit der unterstützten Firmware-Version.
- [Richten Sie den Controller in Ihrer Synergis™-Einheit ein.](#)
- Wenn die MR51e Panels den statischen IP-Adressierungsmodus verwenden, laden Sie das *MSC MR51e Address Configuration Tool* von der Mercury-Website herunter.

Was Sie noch wissen sollten

Für die Mercury-Integration über Synergis™ Software können Sie das MR51e-Panel mit nur zwei Adressierungsmodi verwenden: dem öffentlichen DHCP und der statischen IP.

BEMERKUNG: Der Lesegerätanschluss 1 am MR51e-Panel kann [bis zu zwei OSDP-Lesegeräte](#) unterstützen.

Prozedur

- 1 Führen Sie eine der folgenden Aktionen aus:
 - [Stellen Sie das MR51e-Panel auf die Verwendung von Public DHCP](#) ein (empfohlen).
 - [Stellen Sie das MR51e-Panel auf die Verwendung von Static IP](#) ein.
- 2 Öffnen Sie im Config Tool den Task *Zutrittskontrolle* und klicken Sie auf **Rollen und Einheiten**.
- 3 Wählen Sie die Synergis™-Einheit, und fügen Sie die MR51e-Platten hinzu.
Weitere Informationen finden Sie in den Schritten zum Hinzufügen nachgelagerter Panels in [Registrierung von Mercury-Controllern auf der Synergis™-Einheit](#) auf Seite 140.

Einstellung von MR51e zur Verwendung des öffentlichen DHCP-Adressierungsmodus

Wenn Ihr Netzwerk DHCP unterstützt, wird empfohlen, die MR51e-Panels so einzustellen, dass sie das öffentliche DHCP-Adressierungsmodell verwenden.

Prozedur

- 1 Stellen Sie am MR51e-Panel **S1** (Konfigurations-DIP-Schalter) **0001** ein.
Stellen Sie die DIP-Schalter 4, 3 und 2 auf OFF und den DIP-Schalter 1 auf ON.
- 2 Drücken Sie **S2** (Reset-Schalter).

Einstellung von MR51e zur Verwendung des statischen IP-Adressierungsmodus

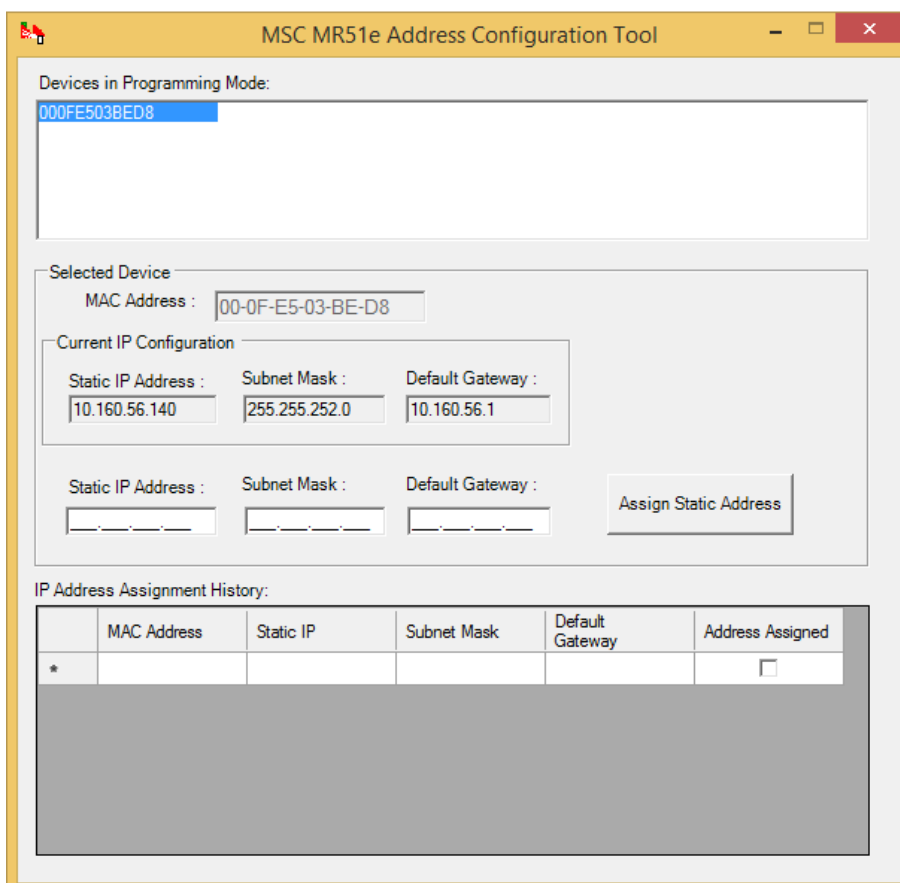
Wenn Ihr Netzwerk DHCP nicht unterstützt, stellen Sie Ihre MR51e-Panels auf das Modell der statischen IP-Adressierung ein.

Bevor Sie beginnen

Laden Sie das [MSC MR51e Address Configuration Tool](#) herunter und installieren Sie es auf Ihrem Computer. Vergewissern Sie sich, dass das MR51e-Panel mit demselben Subnetz wie Ihr Computer verbunden ist.

Prozedur

- 1 Stellen Sie am MR51e-Panel **S1** (Konfigurations-DIP-Schalter) **0011** ein.
Stellen Sie die DIP-Schalter 4 und 3 auf OFF und die DIP-Schalter 2 und 1 auf ON.
- 2 Öffnen Sie das MSC MR51e Address Configuration Tool.
- 3 Drücken Sie **S2** (Reset-Schalter).
Nach der Erkennung erscheint die MAC-Adresse des MR51e-Panels in der Liste **Geräte im Programmiermodus**.
- 4 Wählen Sie in der Liste **Geräte im Programmiermodus** das zu programmierende MR51e-Panel.
Die MAC-Adresse des ausgewählten MR51e-Panels erscheint im Feld **Ausgewähltes Gerät**.



- 5 Geben Sie die Werte für **Statische IP-Adresse**, **Subnetzmaske** und **Standardgateway** ein, und klicken Sie auf **Statische Adresse zuweisen**.
Die eingegebenen Werte erscheinen in der Gruppe **Aktuelle IP-Konfiguration** und in der Liste **Verlauf der IP-Adresszuweisung**.
- 6 Stellen Sie am MR51e-Panel **S1** (Konfigurations-DIP-Schalter) **0010** ein.
Stellen Sie die DIP-Schalter 4, 3 und 1 auf OFF und den DIP-Schalter 2 auf ON.
- 7 Drücken Sie **S2** (Reset-Schalter).

Einstellung von MR62e zur Verwendung des statischen IP-Adressierungsmodus

Bevor Sie das Mercury MR62e-Panel oder den Mercury-Controller unter der Synergis™-Einheit hinzufügen, müssen Sie der Einheit eine statische IP-Adresse zuweisen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die folgenden Angaben haben:

- **Einrichtungs- und Konfigurationsanleitung für Mercury:** Gebrauchsanweisung für die Verbindung zum Webportal Ihres Mercury-Controllers und die Einrichtung seiner IP-Adresse (und anderer Konfigurationen).
- **Statische IP-Adresse:** Statische IP-Adresse, die dem Controller von Ihrer IT-Abteilung zugewiesen wurde.

Prozedur

- 1 Melden Sie sich auf der Webseite des MR62e-Panels an.
- 2 Geben Sie in das Feld **Statische IP** eine IP-Adresse ein.
- 3 Klicken Sie auf **Speichern**.

Konfiguration der Adresse des Mercury-Lesegeräts für das MR62e-Panel

An das nachgeschaltete MR62e-Panel angeschlossene Lesegeräte werden in bestimmten Paaren verwendet und müssen auf vordefinierte, von Mercury fest programmierte Adressen konfiguriert werden, damit sie funktionieren.

Die folgende Tabelle zeigt die erforderliche Konfiguration der Lesegerätadresse:

Lesegerätnummer (Adresse)	Türeinrichtung	Mercury-Drehkreuze und -Aufzüge
0	Tür 1: Lesegerätseite IN	Ja
1	Tür 2: Lesegerätseite IN	Ja
2	Tür 1: Lesegerätseite OUT	Nein
3	Tür 2: Lesegerätseite OUT	Nein

BEMERKUNG: Um mit dem MR62e nur eine *Karteneingangs-/Kartenausgangstür* zu steuern, verwenden Sie die Adressen 0 und 2.

Um das MR62e zur Steuerung von zwei *Card In/REX Out*-Türen zu verwenden, verwenden Sie die Adressen 0 und 1.

Trennen von MR-Panels von einem Mercury-Controller

Um ein Mercury MR-Panel von einem Mercury-Controller zu trennen, das im Security Center registriert ist, können Sie das Panel im Config Tool vom Controller löschen.

Was Sie noch wissen sollten

Mercury-MR-Panels müssen in Security Center offline sein, bevor Sie sie löschen können.

Prozedur

- 1 Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
- 2 Klicken Sie auf **Rollen und Einheiten**, wählen Sie Ihre Synergis™-Einheit und klicken Sie auf die Registerkarte **Peripheriegeräte**.
- 3 Wenn das MR-Panel Türen oder Zonen steuert, trennen Sie diese.
- 4 So trennen Sie das Panel:
 - Trennen Sie das Panel von der Stromversorgung und warten Sie, bis es im Config Tool offline geht.
 - Klicken Sie auf die Registerkarte **Peripheriegeräte**, wählen Sie das Panel aus, klicken Sie auf **Bearbeiten** und ändern Sie dann die **Adresse** des Panels, sodass es die Verbindung zum Controller trennt und im Config Tool offline geht.
- 5 Klicken Sie auf die Registerkarte **Peripheriegeräte**, wählen Sie das Panel, klicken Sie auf **Löschen** und dann auf **Anwenden**.

Informationen über Mercury-Auslöser und -Verfahren

Mercury-Auslöser und -Verfahren sind mit Event-to-Actions in Security Center vergleichbar. Sie können im Synergis Appliance Portal Auslöser und Verfahren konfigurieren, um Regeln direkt auf einer Mercury-Steuerung auszuführen.

So funktionieren Mercury-Auslöser und -Verfahren im Synergis Appliance Portal

- Mercury-Auslöser und -Verfahren arbeiten zusammen, um eine Regel zu erstellen. Der Auslöser definiert das *Wann* mit einem Ereignis und das Verfahren definiert das *Was* mit einer oder mehreren Aktionen. Jeder Auslöser ist mit einem Verfahren verknüpft, aber jedes Verfahren kann in mehreren Auslösern verwendet werden.
- Wenn Entitäten, die in Auslösern und Verfahren verwendet werden, in einen unerwarteten Status kommen, können Sie sie mit der Taste **Zu Standard zurücksetzen** auf der Seite *Mercury-Auslöser und -Verfahren* zu ihrem ursprünglichen Status zurücksetzen.

BEMERKUNG: Diese Taste wird auch verwendet, um Mercury-Auslöser und -Verfahren nach dem Wiederherstellen der Konfigurationsdateien einer Synergis™ Cloud Link-Einheit wiederherzustellen.

Optimale Vorgehensweisen

Stellen Sie für die optimale Leistung von Mercury-Auslösern und -Verfahren sicher, dass die folgenden Einstellungen auf der Seite *Mercury-Steuerungseinstellungen* im Synergis™ Appliance Portal aktiviert sind:

- **Live-Ereignisse „Aufforderung zum Verlassen“:** Aktivieren Sie diese Einstellung, wenn Sie Auslöser mit REX-Ereignissen erstellen.
- **Native Mercury-Bereichssteuerung:** Aktivieren Sie diese Einstellung, wenn Sie Auslöser in Bezug auf Bereiche erstellen.

Informationen über das Überwachen von Mercury-Auslösern und -Verfahren

In Security Center 5.12 und neuer erstellen Mercury-Auslöser und -Verfahren benutzerdefinierte Ereignisse, die in Event-to-Actions verwendet werden können.

- **Ereignisse überwachen:** Sie können die benutzerdefinierten Ereignisse im Security-Desk-Task *Überwachung* überwachen, indem Sie die Synergis™ Cloud Link-Einheit zur Liste *Ereignisüberwachung* hinzufügen.
- **Ereignismeldung:** Sie können für benutzerdefinierte Ereignisse Berichte ausführen, indem Sie den Task *Zutrittskontrolleinheitsereignisse* in Security Desk und Config Tool verwenden und den Filter auf die Synergis™ Cloud Link-Einheit festlegen.
- **Funktionen:** Auf der Seite *Funktionsbericht* im Synergis Appliance Portal listen die Reihen *Benutzerdefinierte Auslöser* und *Benutzerdefinierte Verfahren* im Abschnitt *Funktionen* die Anzahl von Auslösern und Verfahren auf, die für die Mercury-Steuerung erstellt wurden.

Einschränkungen von Mercury-Auslösern und -Verfahren

Mercury-Auslöser und -Verfahren im Synergis Appliance Portal haben die folgenden bekannten Einschränkungen:

Allgemeine Einschränkungen

- Jede Mercury-Steuerung kann bis zu 3.000 Auslöser und 3.000 Verfahren haben. Auslöser und Verfahren, die diese Limits überschreiten, werden ignoriert.

Einschränkungen bei der Konfiguration

- Sie können eine Ausgabe basierend auf der Eingabeänderung aktivieren. Es gibt jedoch keine Option zum Zurücksetzen der Ausgabe zu ihrem ursprünglichen Status.

Abhilfemaßnahme: Um die Ausgabe zurückzusetzen, erstellen Sie ein separates Verfahren, um die Ausgabe auf ihren ursprünglichen Status zurückzusetzen, wobei der Auslöser auf eine Eingabeänderung festgelegt ist.

- Eingaben und Ausgaben, die Türen oder Fahrstühlen zugewiesen sind, können nicht als Überwachungspunkt- oder Kontrollpunktauslöser verwendet werden.
- Die Lesegerät-LED-Musterbefehle, die Synergis™ Software an Mercury sendet, überschreiben aktive LED-Musterverfahren. Dies umfasst das Festlegen der Lesegerät-LED auf rot beim erneuten Versperren und Festlegen der Lesegerät-LED auf grün, wenn die Tür in den Zeitplan für freien Zutritt übergeht.
- Beim Ein- und Ausschalten der Mercury-Steuerung werden die Verfahren *Lesegerätmodus*, die mit einer **Unendlichen** Dauer konfiguriert wurden, abgebrochen.
- Die temporäre Lesegerätmoduskonfiguration in *Lesegerätmodus überschreiben*-Verfahren überschreibt alle manuellen Änderungen am Lesegerätmodus.

Beispiel: Wenn Sie ein Lesegerät zum Modus *Karte und PIN* ändern, während ein *Lesegerätmodus überschreiben*-Verfahren aktiviert ist, um den Lesegerätmodus zu *gesperrt* zu ändern, bleibt die Tür versperrt. Wenn dieses Verfahren jedoch abläuft, kehrt das Lesegerät zum Modus *Karte und PIN* zurück.

- Wenn ein Karteninhaber seinen Berechtigungsnachweis an einem Lesegerät vorzeigt, das mit dem Verfahren *Lesegerätmodus überschreiben* deaktiviert war, enthält das Ereignis *Zutritt verweigert* in Security Center keinen Verweigerungsgrund.
- Bei *Kontrollpunkt festlegen*-Verfahren, die mit einem **periodischen** Befehl konfiguriert sind, sehen Sie nur die erste und letzte Änderung der Ausgabe in Config Tool.

Einschränkungen in Bezug auf Zeitpläne

- Zeitpläne werden nur dann mit der Synergis™ Cloud Link-Einheit synchronisiert, wenn sie mit einer Entität verknüpft sind, die von dieser Einheit gesteuert wird. Um für Auslöser und Verfahren exklusive Zeitpläne zu verwenden, müssen Sie eine Dummy-Tür zur Synergis™ Cloud Link-Einheit hinzufügen und die Zeitpläne bei dieser Tür anwenden.
- In Security Center können nur 255 Zeitpläne erstellt werden, einschließlich Entsperrungszeitplänen und Zeitplänen, die nur für Mercury-Auslöser und -Verfahren verwendet werden.
- Mercury hat ein Limit von 12 Zeitplanintervallen. Weitere Informationen finden Sie unter [Mercury-Einschränkungen mit Türentsperrungszeitplänen](#).

Aktionstypen für Mercury-Verfahren

Jedes Mercury-Verfahren muss eine oder mehrere der folgenden Aktionen enthalten.

Aktion	Beschreibung
Zone scharfschalten/unscharfschalten	<p>Eine Hardwarezone scharfschalten oder unscharfschalten:</p> <ul style="list-style-type: none"> • Unscharfschalten: Alle Zoneneingaben maskieren. Eingaben gehen bei Aktivierung nicht in den Alarmstatus über. • Scharfschalten: Wenn keine Eingaben aktiv sind, wird die Zone scharfgeschaltet und die Maskierung aller Eingaben aufgehoben. • Scharfschalten erzwingen: Die Zone wird scharfgeschaltet, aber die Maskierung wird nur bei inaktiven Eingaben aufgehoben. Zuvor aktive Eingaben bleiben maskiert. • Scharfschalten überschreiben: Die Zone wird scharfgeschaltet und die Maskierung aller Eingaben wird aufgehoben.

Aktion	Beschreibung
Kontrollverfahren	Steuern eines Mercury-Verfahrens: <ul style="list-style-type: none"> • Ausführen: Führen Sie die Aktionen im ausgewählten Verfahren aus. • Verzögerte abbrechen: Wenn das ausgewählte Verfahren auf eine <i>Verzögerungsaktion</i> wartet, wird das Verfahren oder Abschluss der nachfolgenden Aktionen abgebrochen. • Fortsetzung verzögert: Wenn das ausgewählte Verfahren auf eine <i>Verzögerungsaktion</i> wartet, wird die Verzögerung übersprungen, sodass nachfolgende Aktionen ausgeführt werden können.
Verzögerung	Das Verfahren wartet für die konfigurierte Anzahl von Sekunden, bevor es mit den nachfolgenden Aktionen fortfährt.
Zwangsoffnung der Tür ignorieren	„Türöffnung erzwungen“-Alarmer für die Tür deaktivieren.
Offengehaltene Tür ignorieren	„Tür offen gehalten“-Alarmer für die Tür deaktivieren.
Alarmer der Überwachungspunkte ignorieren	Maskiert die Eingabe und hält sie davon ab, bei Aktivierung in den Alarmstatus überzugehen.
Lesegerät-LED überschreiben	Ein vorübergehendes LED-Muster auf das Lesegerät anwenden. Konfigurieren Sie Folgendes: <ul style="list-style-type: none"> • Farbe ein • Farbe aus • Zeit – ein (ms) • Zeit – aus (ms) • (0-255) wiederholen • Signaltonanzahl (0-15)
Lesegerätmodus überschreiben	Den Lesegerätmodus für die konfigurierte Dauer mit einem der folgenden Lesegerätmodi überschreiben: <ul style="list-style-type: none"> • Deaktiviert: Kartenlesungen und REQ sind deaktiviert und die Tür bleibt versperrt. • Entriegelt: Die Tür ist entriegelt. • Verriegelt: Kartenerfassungen sind deaktiviert, aber REX funktionieren weiterhin. • Nur Karte: Nur Karten sind gültige Zutrittsberechtigungs-nachweise. • Karte und PIN: Karte und PIN sind für den Zutritt erforderlich. • Karte oder PIN: Karten oder PINs sind gültige Zutrittsberechtigungs-nachweise. • Nur PIN: Nur PINs sind gültige Zutrittsberechtigungs-nachweise.
Kontrollpunkt einrichten	Eine Ausgabe aktivieren, die nicht zu einem Türöffner zugewiesen ist.
Tür kurzzeitig entsperren	Die Tür für die konfigurierte Dauer entsperren.

Ereignistypen für Mercury-Auslöser

Ereignisse legen fest, wann ein Mercury-Auslöser eintritt.

Ereignis	Beschreibung
Zutritt verweigert: ungültiges Kartenformat	Zutritt wird verweigert, wenn das Kartenformat nicht mit der Mercury-Steuerung synchronisiert wurde.
Zutritt verweigert: Anfrage von Steuerung abgelehnt	Zutritt wird aus folgenden Gründen verweigert: <ul style="list-style-type: none"> • Der Lesegerätemodus ist <i>Gesperrt</i>. • Ein unbekannter Berechtigungsnachweis wird verwendet. • Die Mercury-Zutrittsbewilligungsentscheidung wird von Synergis Software überschrieben. • Eine Verriegelungsbeschränkung.
Zutritt verweigert: nicht autorisierter Karteninhaber	Zutritt wird aus folgenden Gründen verweigert: <ul style="list-style-type: none"> • Die diesem Karteninhaber zugeordnete Zutrittsregel hat für das im Zeitplan angegebene Datum bzw. die Uhrzeit keine Gültigkeit. • Eine ungültige PIN wurde eingegeben. • Ein nativer Anti-Passback-Verstoß. • Eine bekannte Karte ohne Zutritt wird am Lesegerät verwendet. • Zwei Karteninhaber müssen ihre Berechtigungen mit einer bestimmten Verzögerung nacheinander vorweisen, die Zeitspanne hierfür ist jedoch abgelaufen. • Das Belegungslimit des Bereichs wurde erreicht. • Die Besucherbegleitungsregel wird durchgesetzt, und der Besucher hat sich vor dem Gastgeber ausgewiesen. • Eine Karte und eine PIN-Nummer sind für den Zutritt zu einem Bereich erforderlich und der Karteninhaber hat innerhalb der vorgegebenen Zeit keine PIN eingegeben.
Zutritt abgelehnt: Unbekannte Berechtigung	Zutritt wird verweigert, wenn das Kartenformat erkannt wird, der Berechtigungsnachweis aber nicht mit der Mercury-Steuerung synchronisiert wurde.
Zutritt erlaubt	Der Zutritt wird gewährt, nachdem eines der Folgenden eingetreten ist: <ul style="list-style-type: none"> • Der Karteninhaber öffnet die Tür. • Die Eintrittszeit läuft ab und die Tür wird wieder versperrt. • Die Tür hat keinen Türsensor und der Eintritt wird angenommen.
Zutritt erlaubt: Eintritt erkannt	Zutritt wird gewährt, nachdem ein Eintritt erkannt wurde.
Zutritt erlaubt: entsperrt	Zutritt wird gewährt, nachdem eine Tür entsperrt wurde.
Tür geschlossen	Die Tür ist geschlossen.
Tür gewaltsam geöffnet	Das Öffnen der Tür wird erzwungen.
Tür offen gehalten	Die Tür wird offen gehalten.

Ereignis	Beschreibung
Tür geöffnet (nicht erzwungen)	Die Tür ist geöffnet, das Öffnen wurde aber nicht erzwungen.
Tür nach REX wieder zugesperrt	Die Tür wird nach einem REX wieder versperrt.
Tür nach manueller Entsperrung wieder zugesperrt	Die Tür wird nach einem manuellen Entsperren wieder versperrt.
Tür nach manueller Entsperrung oder REX wieder zugesperrt	Die Tür wird nach einem manuellen Entsperren oder einem REX wieder versperrt.
Tür durch REX entsperrt	Die Tür wird durch ein REX entsperrt.
Bedrohungscode-PIN eingegeben	Ein Bedrohungs-PIN wird am Lesegerät erkannt. Das Ereignis wird erstellt, selbst wenn die Option Bedrohungs-PIN im Bereich deaktiviert ist und der Zutritt verweigert wird.
Harte maximale Belegungszahl erreicht	Die Harte maximale Belegungszahl wurde erreicht.
Die Anzahl der schwer belegbaren Plätze hat Null erreicht	Die harte maximale Anzahl der schwer belegbaren Plätze hat Null erreicht.
Überwachungspunkt: Alarm (aktiv)	Die Eingabe mit aufgehobener Maskierung wird aktiviert. Eingaben in unscharfgeschalteten Zonen sind maskiert.
Monitor point: Fehler (Problem)	Die Eingabe geht in den Status <i>Problem</i> über.
Monitor point: sicher (inaktiv)	Die Eingabe geht in den Status <i>Inaktiv</i> über.
Lesegerätmodus: Karte und PIN	Der Lesegerätmodus wird zu <i>Karte und PIN</i> geändert.
Lesegerätmodus: nur Karte	Der Lesegerätmodus wird zu <i>Nur Karte</i> geändert.
Lesegerätmodus: Karte oder PIN	Der Lesegerätmodus wird zu <i>Karte oder PIN</i> geändert.
Lesegerätmodus: deaktiviert	Der Lesegerätmodus wird zu <i>Deaktiviert</i> geändert.
Lesegerätmodus: gesperrt	Der Lesegerätmodus ändert sich zu <i>Gesperrt</i> (Lesegerät deaktiviert).
Lesegerätmodus: nur PIN	Der Lesegerätmodus wird zu <i>Nur PIN</i> geändert.
Lesegerätmodus: entsperrt	Der Lesegerätmodus ändert sich zu <i>Entsperrt</i> (Wartungsmodus).

Mercury-Auslöser im Synergis Appliance Portal konfigurieren

Konfigurieren Sie einen Auslöser, um festzulegen, wann ein Verfahren ausgeführt wird.

Bevor Sie beginnen



[Konfigurieren Sie Mercury-Verfahren im Synergis™ Appliance Portal.](#)

Was Sie noch wissen sollten

Die Farbe des Auslösernamens gibt an, ob ein Problem bei der Konfiguration vorliegt:



- **Orange:** Die Konfiguration wurde gespeichert, aber etwas hat nicht funktioniert, wodurch sie nicht mit der Mercury-Steuerung synchronisiert wurde. Dies kann auftreten, wenn zugehörige Entitäten nicht mehr existieren oder nicht richtig mit der Steuerung synchronisiert wurden. Die Mercury-Steuerung muss online sein, damit Sie diese Farbe sehen.
- **Rot:** Für die Konfiguration erforderliche Informationen fehlen oder sind ungültig.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Mercury-Auslöser und -Verfahren.**
- 3 Wählen Sie in der Liste **Eine Steuerung auswählen** die Steuerung aus, für die Sie einen Auslöser erstellen möchten.
- 4 Klicken Sie auf **Einen Auslöser hinzufügen.**
- 5 Geben Sie im Feld **Name** einen beschreibenden Namen für den Auslöser ein.
- 6 Klicken Sie neben dem Feld **Zeitplan** auf . Wählen Sie im Dialogfeld, das geöffnet wird, einen Zeitplan aus der Liste aus und klicken Sie auf **OK.**
- 7 Klicken Sie neben dem Feld **Ereignis** auf . Wählen Sie im Dialogfeld, das geöffnet wird, ein Ereignis aus der Liste aus und klicken Sie auf **OK.**

Eine Liste der Ereignisse und ihrer Beschreibungen finden Sie unter [Ereignistypen für Mercury-Auslöser](#) auf Seite 175.

Abhängig vom Ereignis, das Sie ausgewählt haben, wird eines der folgenden Felder angezeigt:

- **Eingang:** Nur Eingaben, die zu keiner Entität in Security Center zugewiesen sind, werden aufgelistet, außer Zoneneingaben.
 - **Lesegerät:** Alle Lesegeräte, die sich unter der ausgewählten Mercury-Steuerung befinden, werden aufgelistet.
 - **Tür:** Nur Türen, die von der ausgewählten Mercury-Steuerung gesteuert werden, werden aufgelistet. Wählen Sie die Türseite aus.
 - **Bereich:** Nur Bereiche, die von der ausgewählten Mercury-Steuerung gesteuert werden, werden aufgelistet.
 - **Zone:** Nur Hardware-Zonen, die von der ausgewählten Mercury-Steuerung gesteuert werden, werden aufgelistet.
- 8 Klicken Sie neben dem Feld, das angezeigt wird, auf . Wählen Sie im Dialogfeld, das geöffnet wird, eine Entität aus der Liste aus und klicken Sie auf **OK.**
 - 9 Klicken Sie neben dem Feld **Verfahren** auf . Wählen Sie im Dialogfeld, das geöffnet wird, ein Verfahren aus der Liste aus und klicken Sie auf **OK.**

10 Wählen Sie in der Liste **Verfahrensbefehl** eine der folgenden Optionen aus:

- **Ausführen:** Führen Sie die Aktionen im ausgewählten Verfahren aus.
- **Verzögerte abbrechen:** Wenn das ausgewählte Verfahren auf eine *Verzögerungsaktion* wartet, wird das Verfahren oder Abschluss der nachfolgenden Aktionen abgebrochen.
- **Fortsetzung verzögert:** Wenn das ausgewählte Verfahren auf eine *Verzögerungsaktion* wartet, wird die Verzögerung übersprungen, sodass nachfolgende Aktionen ausgeführt werden können.

11 (Optional) Das Feld **Auslösercode (1-255)** wird angezeigt, abhängig vom von Ihnen ausgewählten Ereignis. Der Auslösercode hat einen Wert zwischen 1 und 255, den Sie für einen Karteninhaber oder Besucher in Security Center 5.12 und neuer konfigurieren können. Der gleiche Auslösercode kann für mehrere Karteninhaber und Besucher verwendet werden. Es gibt keine Hierarchie für Auslösercodes.

12 Klicken Sie auf **Speichern**.

Dieser Auslöser ist konfiguriert, um das Verfahren *Vorübergehendes Entsperren* auszuführen, wenn einem Karteninhaber mit dem Auslösercode 52 der Eintritt bei der *Haupteingangstür* verweigert wird.

The screenshot displays the Mercury configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'I/O diagnostics', and 'Maintenance'. The left sidebar lists various configuration categories, with 'Mercury triggers and procedures' selected. The main content area shows the configuration for a 'Lockdown exception' trigger. The trigger is currently disabled. The configuration details include:

- Name:** Lockdown exception
- Disabled:**
- Schedule:** Always
- Event:** Access denied: Request rejected by controller
- Door:** Main entrance
- Door side:** In (selected), Out
- Procedure:** Temporary unlock
- Procedure command:** Execute
- Trigger code (1-255):** 52

Buttons for 'Reset to default', 'Disable all', and 'Delete all' are visible at the top right of the configuration area.

Mercury-Verfahren im Synergis Appliance Portal konfigurieren

Sie müssen ein Verfahren konfigurieren, um festzulegen, welche Aktionen ausgeführt werden sollen, wenn ein auslösendes Ereignis eintritt.

Bevor Sie beginnen


Registrieren Sie eine Mercury-Steuerung auf der Synergis™ Cloud Link -Einheit.

Was Sie noch wissen sollten

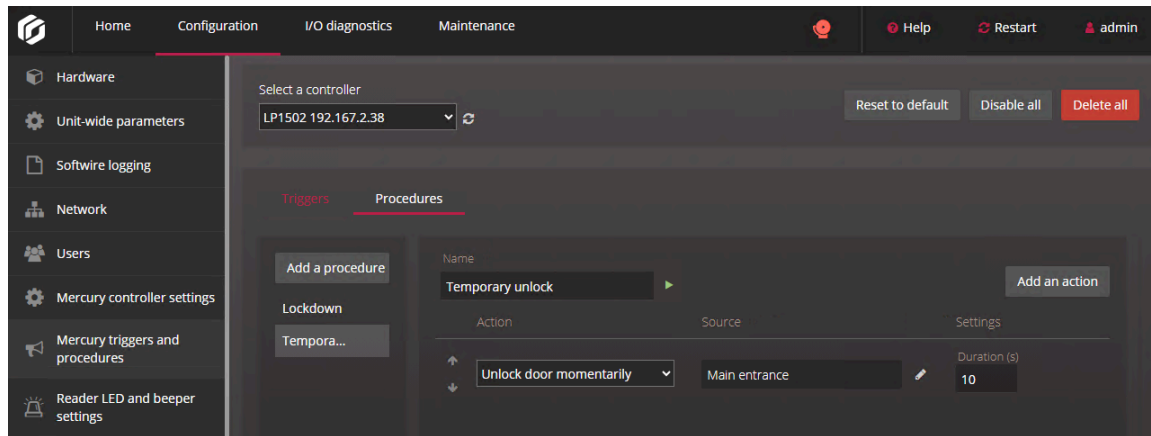
Die Farbe des Verfahrensnamens gibt an, ob ein Problem bei der Konfiguration vorliegt:

- **Orange:** Die Konfiguration wurde gespeichert, aber etwas hat nicht funktioniert, wodurch sie nicht mit der Mercury-Steuerung synchronisiert wurde. Dies kann auftreten, wenn zugehörige Entitäten nicht mehr existieren oder nicht richtig mit der Steuerung synchronisiert wurden. Wenn ein Verfahren orange ist, sind auch alle verknüpften Auslöser orange. Die Mercury-Steuerung muss online sein, damit Sie diese Farbe sehen.
- **Rot:** Für die Konfiguration erforderliche Informationen fehlen oder sind ungültig.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Mercury-Auslöser und -Verfahren**.
- 3 Wählen Sie in der Liste **Eine Steuerung auswählen** die Steuerung aus, für die Sie ein Verfahren erstellen möchten.
- 4 Klicken Sie auf die Registerkarte **Verfahren**.
- 5 Klicken Sie auf **Ein Verfahren hinzufügen**.
- 6 Geben Sie im Feld **Name** einen beschreibenden Namen für das Verfahren ein.
- 7 Klicken Sie auf **Eine Aktion hinzufügen**.
In der Spalte *Aktion* erscheint ein Drop-down-Menü.
- 8 Klicken Sie auf das Drop-down-Menü und wählen Sie eine Aktion aus.
Eine Liste der Aktionen und ihrer Beschreibungen finden Sie unter [Aktionstypen für Mercury-Verfahren](#) auf Seite 173.
In den Spalten *Quelle* und *Einstellungen* werden abhängig von der Aktion, die Sie ausgewählt haben, unterschiedliche und Tasten angezeigt.
- 9 Wenn es in der Spalte *Quelle* ein Feld gibt, klicken Sie auf  neben dem Feld und wählen Sie dann eine Quelle im Dialogfeld aus, das geöffnet wird.
- 10 Konfigurieren Sie die Einstellungen in der Spalte *Einstellungen* nach Bedarf.
- 11 (Optional) Fügen Sie nach Bedarf weitere Aktionen hinzu.
- 12 (Optional) Ordnen Sie die Aktionen mithilfe der Nach-oben- und Nach-unten-Pfeile neu an. Die Aktionen werden in der Reihenfolge ausgeführt, in der sie in der Verfahrenskonfiguration aufscheinen.
- 13 Klicken Sie auf **Speichern**.

Dieses Verfahren ist mit der Aktion *Tür vorübergehend entsperren* konfiguriert, die die *Haupteingangstür* für 10 Sekunden nach dem Auftreten des Auslösers entsperrt.



Nach Durchführen dieser Schritte

- Testen Sie das Verfahren, bevor Sie es mit einem Auslöser verknüpfen, indem Sie auf das ► neben dem Verfahrensfeld **Name** klicken. Wenn das Verfahren eine *Verzögerungsaktion* enthält, können Sie auf das ■ um das Verfahren während der Verzögerung anzuhalten und es abubrechen.
BEMERKUNG: Die Tasten werden nur angezeigt, wenn das Verfahren erfolgreich mit der Mercury-Steuerung verknüpft wurde. Die Tasten sind ausgeblendet, wenn die Steuerung offline ist oder es ungelöste Felder in der Verfahrenskonfiguration gibt. Klicken Sie auf die ↻ neben dem Steuerungsfeld, um die Seite zu aktualisieren.
- [Konfigurieren Sie Mercury-Auslöser im Synergis Appliance Portal.](#)

Mercury-Auslöser und -Verfahren im Synergis Appliance Portal deaktivieren

Um zu verhindern, dass ein Verfahren ausgeführt wird, können Sie den Auslöser deaktivieren, mit dem dieses Verfahren verknüpft ist.

Was Sie noch wissen sollten

Wenn ein Auslöser deaktiviert wird, wird die Synchronisierung mit der Mercury-Steuerung aufgehoben, ohne dass die Konfiguration verloren geht. Dies ist hilfreich, wenn Sie vorübergehend verhindern möchten, dass ein bestimmter Auslöser aktiviert wird. Sie können bei unerwartetem Verhalten eine Fehlerbehebung durchführen, indem Sie alle Auslöser deaktivieren und sie dann nacheinander wieder aktivieren, um herauszufinden, wo das Problem herkommt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Mercury-Auslöser und -Verfahren**.
- 3 Führen Sie eine der folgenden Aktionen aus:
 - Um einen einzelnen Auslöser zu deaktivieren, wählen Sie einen Auslöser aus der Liste aus und aktivieren Sie dann das Kontrollkästchen **Deaktivieren** neben dem Feld **Name**. Klicken Sie auf **Speichern**.
 - Um alle Auslöser für die ausgewählten Mercury-Steuerungen zu deaktivieren, klicken Sie oben auf der Seite *Mercury-Auslöser und -Verfahren* auf **Alle deaktivieren**. Klicken Sie im Dialogfeld, in dem Sie um die Bestätigung Ihrer Entscheidung gebeten werden, auf **Alle deaktivieren**.

Deaktivierte Auslöser sind ausgegraut.

Nach Durchführen dieser Schritte

Um einen Auslöser erneut zu aktivieren, wählen Sie den Auslöser aus und deaktivieren Sie das Kontrollkästchen **Deaktivieren** oder klicken Sie auf **Alle aktivieren**, wenn alle Auslöser deaktiviert waren. Klicken Sie auf **Speichern**.

Allegion-Schlage-Schlösser über Mercury

Dieser Abschnitt enthält die folgenden Themen:

- ["Anmeldung von Allegion Schlage AD-Schlössern und PIM-Modulen an der Synergis™-Einheit"](#) auf Seite 183
- ["ENGAGE-integrierte Allegion-Schlage-LE- und- NDE-Schlösser über Mercury-Controller registrieren"](#) auf Seite 187

Anmeldung von Allegion Schlage AD-Schlössern und PIM-Modulen an der Synergis™-Einheit

Da die Synergis™-Einheit nicht direkt mit AD-Schlössern oder PIM400-Modulen von Allegion Schlage kommuniziert, müssen Sie diese Geräte über einen Mercury EP-, LP-, MP- oder Honeywell-Controller registrieren und dafür das Config Tool verwenden.

Bevor Sie beginnen

- Konfigurieren Sie eine andere RS-485-Adresse auf jedem Schlage-Gerät (AD-Serie-Schloss und PIM400-Modul) mithilfe des Schlage-Pidion-Handgeräts und schließen Sie das Schloss und das Modul an Ihren Mercury-Controller an. Weitere Informationen finden Sie im Schlage Utility Software-Benutzerhandbuch.
- [Konfigurieren Sie die zugewiesene statische IP-Adresse auf dem Mercury-Controller.](#)

Was Sie noch wissen sollten

Auf der Synergis™-Einheit muss jedem Mercury-Controller eine eindeutige Kanal-ID zugewiesen werden. Alle Mercury-Steuerungen haben RS-485-Busse, an die die Schlage-Geräte (AD-300 und PIM400) angeschlossen sind. Jedes Schlage-Gerät, das an denselben RS-485-Bus angeschlossen ist, muss eine eindeutige RS-485-Adresse haben.

Prozedur

- 1 Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
- 2 Klicken Sie auf **Rollen und Einheiten**, und klicken Sie dann auf die Synergis™- Einheit.

- 3 Klicken Sie auf **Peripheriegeräte** und dann auf **Einen Eintrag hinzufügen** (+).

The screenshot shows a configuration window for Mercury Security. The fields are as follows:

- Manufacturer:** Mercury Security (dropdown menu)
- Model:** EP1502 (dropdown menu)
- IP address:** 0 . 0 . 0 . 0 (text input) with a blue link labeled **Hostname** next to it.
- Port:** 3001 (spin button)
- Channel:** 1 (spin button)
- Interfaces:** A table with columns: Model, Port, Address, IP address. The table is currently empty.

At the bottom of the window, there are three small icons: a green plus sign (+), a red X, and a pencil. Below these icons is a button labeled **Advanced settings**. At the very bottom are **Cancel** and **OK** buttons.

- 4 Geben Sie die folgenden Informationen ein:

- **Modell:** Modell des Controllers.
- **IP-Adresse:** Statische IP-Adresse, die dem Controller von Ihrer IT-Abteilung zugewiesen wurde.
- **Hostname:** Klicken Sie auf den blauen Link, um die Steuerung ihrem Hostnamen nach zu identifizieren. Diese Option ist nur verfügbar, wenn Sie Security Center 5.12.0.0 oder höher ausführen.
BEMERKUNG: Wenn Sie eine Mercury-Steuerung mit ihrem Hostnamen registrieren, müssen Sie `.local` an den Hostnamen anhängen, wenn die Steuerung nicht bei DHCP und DNS im Netzwerk registriert ist.
- **Port:** Kommunikationsport. Der Standardwert ist 3001. Der Port muss mit dem auf der Mercury Device Manager-Webseite konfigurierten Wert übereinstimmen.
- **Kanal:** Kanal-ID für diesen Controller. Die Kanal-ID kann ein beliebiger Wert zwischen 0 und 63 sein. Sie muss innerhalb der Synergis-Einheit eindeutig sein. Nach dem Zuweisen darf sie nicht mehr geändert werden.

- 5 Fügen Sie die Allegion Schlage-Geräte hinzu, die mit Ihrem Mercury-Controller verbunden sind.
 - a) Klicken Sie in der Liste *Schnittstellen* auf **Einen Eintrag hinzufügen** (+).
 - b) Wählen Sie im angezeigten Dialogfeld das **Modell** (AD-300 oder PIM400), den **Port** und die **Adresse** (0 bis 31) aus.
 - c) (nur PIM400) Geben Sie in **Niedrig** die erste mit dem PIM400 verbundene Türnummer und in **Anzahl** die Anzahl der mit dem PIM400 verbundenen Türen ein.
Alle Türnummern im Bereich von **Niedrig** bis **Niedrig+Zahl** müssen einem AD-400-Funkschloss entsprechen.
 - d) Klicken Sie auf **OK**.
 - e) Wiederholen Sie dies nach Bedarf.
- 6 (Optional) Klicken Sie auf **Erweiterte Einstellungen**, um die erweiterten Einstellungen zu ändern.
Die verfügbaren Einstellungen hängen vom gewählten Controller-Modell ab. Sie können in der Regel die Baudrate des verfügbaren seriellen Anschlusses, die benutzerdefinierten überwachten Eingangswerte und die Konfiguration des Stromeingangsereignisses ändern.

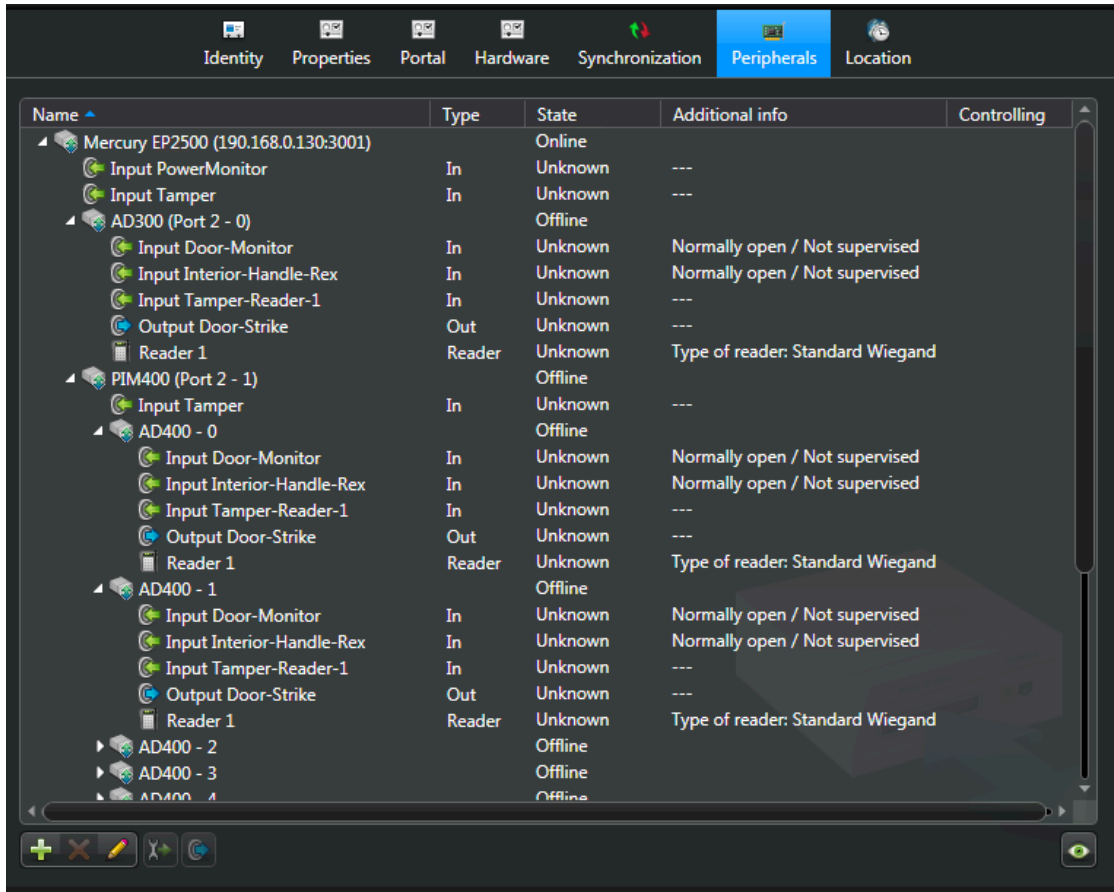


BEMERKUNG: Sie können bis zu vier verschiedene benutzerdefinierte Voreinstellungen für die Eingänge Ihres Mercury-Controllers festlegen. Für Benutzer, die eine Aktualisierung von früheren Security Center-Versionen durchführen und einen benutzerdefinierten Wert konfiguriert haben, wird diese Voreinstellung als **Benutzerdefiniert 1** in der Liste **AD Zeilengrenzwerte** aufgeführt.

- 7 Klicken Sie auf **OK** am unteren Rand des Dialogfelds.

8 Klicken Sie auf **Anwenden**.

Der Mercury-Controller mit allen angeschlossenen nachgeschalteten Panels und Peripheriegeräten ist auf der Seite *Peripheriegeräte* aufgeführt.



Das Hinzufügen von Schnittstellenmodulen zur Synergis™-Einheit führt zu einem Software-Neustart der Einheit. Während dieses Vorgangs werden die Synergis™-Einheit und alle damit verbundenen Peripheriegeräte in Rot angezeigt.

ENGAGE-integrierte Allegion-Schlage-LE- und- NDE-Schlösser über Mercury-Controller registrieren

Mit der ENGAGE-Plattform von Allegion Schlage können Sie Berechtigungsnachweise auf Schlüsselkarten und kompatiblen Mobiltelefonen speichern. Dazu müssen Sie Allegion Schlage LE- und NDE-Schlösser über die ENGAGE-Plattform integrieren, indem Sie einen Mercury EP-, LP- oder MP-Controller im Config Tool registrieren und das ENGAGE Gateway als Schnittstelle hinzufügen.

Bevor Sie beginnen

Die Ersteinrichtung und Kopplung des Schlosses mit dem ENGAGE Gateway erfolgt über die Allegion ENGAGE Mobile App, die für Android- und iOS-Geräte verfügbar ist. Tippen Sie dazu auf **Verbinden**, tippen Sie dann auf das Pluszeichen in der Ecke und folgen Sie den Schritten. Wenn dies geschehen ist, registrieren Sie die Schlösser im Config Tool.

Was Sie noch wissen sollten

Das Verfahren zur Registrierung von NDE- und LE-Schlössern von Allegion Schlage mit der ENGAGE-Integration im Config Tool ist das gleiche wie bei PIM400, mit dem Unterschied, dass Sie bei der Einstellung der Schnittstelle **ENGAGE Gateway** auswählen.

Prozedur

- 1 Registrieren Sie die Allegion Schlage NDE- oder LE-Schlösser wie in [Anmeldung von Allegion Schlage AD-Schlössern und PIM-Modulen an der Synergis™-Einheit](#) auf Seite 183 beschrieben.

- In Schritt 5 wählen Sie das ENGAGE Gateway aus dem Dropdown-Menü **Modell** aus, nachdem Sie auf **Element hinzufügen** (+) in der Liste *Schnittstellen* geklickt haben.

The screenshot shows the Mercury Security configuration interface. At the top, the 'Manufacturer' is set to 'Mercury Security' and the 'Model' is 'EP2500'. Below this, the 'IP address' is '0.0.0.0' and the 'Port' is '3001'. The 'Channel' is set to '4'. The 'Interfaces' section is visible, with a table header showing 'Model', 'Port', 'Address', and 'IP address'. A modal dialog is open, allowing the user to add a new interface. The dialog has the following fields: 'Model' (set to 'ENGAGE Gateway'), 'Port' (set to 'Port 2'), 'Address' (set to '0'), 'Low' (set to '0'), and 'Count' (set to '0'). There are 'Cancel' and 'OK' buttons at the bottom of the dialog. Below the dialog, there is a '+ x' icon and an 'Advanced settings' button. At the bottom of the main interface, there are 'Cancel' and 'OK' buttons.

Auf der Seite *Peripheriegeräte* wird das ENGAGE Gateway mit allen angeschlossenen nachgeschalteten Panels und Peripheriegeräten aufgelistet.

Beispiel:

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

BEST-Wi-Q-Schlösser über Mercury

Dieser Abschnitt enthält die folgenden Themen:

- ["Das Over-Watch-Plugin für die BEST-Wi-Q-Integration konfigurieren"](#) auf Seite 191
- ["BEST-Wi-Q-Gateways auf der Synergis™-Einheit über Mercury-Controller registrieren"](#) auf Seite 194
- ["BEST-Wi-Q-Schlösser und drahtlose Zutrittssteuerungen zum Gateway hinzufügen"](#) auf Seite 197
- ["Informationen über den BEST Wi-Q-Durchgangsmodus"](#) auf Seite 201

Das Over-Watch-Plugin für die BEST-Wi-Q-Integration konfigurieren

Bevor Sie BEST-Wi-Q-Schlösser in Security Center registrieren können, müssen Sie das Over-Watch-Plugin für Mercury-LP4502-Steuerungen konfigurieren.

Was Sie noch wissen sollten

- Alle LP4502-Steuerungen unter der gleichen Synergis™ Cloud Link-Einheit müssen mit dem gleichen Over-Watch-Benutzernamen, -Passwort und - Überwachungsport konfiguriert werden.
- Wenn Sie eine Mercury-LP4502-Einheit, die in einer BEST-Wi-Q-Integration verwendet wird, von einem Synergis™ Cloud Link zu einem anderen verschieben möchten, muss das Over-Watch-Plugin auf dem Ziel-Synergis™ Cloud Link aktiviert sein, bevor die Einheit verschoben wird.

Prozedur

- 1 Laden Sie das Over-Watch-Plugin auf die Mercury-Steuerung.
 - a) Wählen Sie auf der [GTAP-Seite Produktdownload](#) die Option **Synergis™ Cloud Link-Legacy** in der Liste **Download Finder** aus und suchen Sie dann die neueste Mercury-LP4502-Firmware.
 - b) Speichern Sie die *.sfw*-Datei auf Ihrem lokalen Datenträger.
 - c) [Aktualisieren Sie die Firmware der Mercury-Steuerung über das Synergis™ Appliance Portal](#) .
Die Mercury-Steuerung wird neu gestartet, nachdem die Firmware angewendet wurde.
 - d) Melden Sie sich bei der erweiterten Webseite der Synergis™ Cloud Link-Einheit unter <https://<IP address>/MercuryEP/FirmwareVersions> an, und klicken Sie auf die Option **Over-Watch-Paket**, die unter der Mercury-LP4502-Steuerung aufgelistet ist.
Die Mercury-Steuerung wird neu gestartet, nachdem das Plugin installiert wurde.

- 2 Konfigurieren Sie einen Over-Watch-Plugin-Benutzer auf der Mercury-Steuerung.
 - a) Melden Sie sich am Mercury-Controller über die *Configuration Manager*-Webseite an.
 - b) Klicken Sie im Seitenmenü auf **Over-Watch**.
 - c) Geben Sie auf der Seite *Over-Watch-Einstellungen* eine Portnummer im Feld **Empfangsport** ein. Der empfohlene Port ist 1883.

The screenshot shows the Genetec LP4502 Configuration Manager interface. On the left is a navigation menu with options like Home, Network, Host Comm, Device Info, Advanced Networking, Users, Auto-Save, Load Certificate, Load HID Ling Certificate, HID Origo, OSDP File Transfer, Security Options, Diagnostic, Restore/Default, Apply Settings, Over-Watch, and Log Out. The main content area is titled 'Over-Watch Settings' and is divided into three sections: 'Broker Configuration' with a 'Listening Port' field containing '1883' and a 'Save Configuration' button; 'Authorized Users' with an empty box and a 'Delete Selected User(s)' button; and 'New User' with fields for 'Username: (4-16 characters)', 'Password: (6-16 characters)', and 'Confirm Password:', along with an 'Add User' button.

- d) Geben Sie im Abschnitt *Neuer Benutzer* einen Benutzernamen und ein Passwort für den neuen Benutzer ein, bestätigen Sie das Passwort und klicken Sie auf **Benutzer hinzufügen**.
 - e) Klicken Sie im Seitenmenü auf **Einstellungen anwenden** und klicken Sie dann auf **Einstellungen anwenden, neu starten**.
- 3 Konfigurieren Sie Mercury-Einstellungen auf dem BEST-Wi-Q-Gateway.
 - a) Melden Sie sich beim BEST-Wi-Q-Gateway an.
 - b) Klicken Sie im oberen Menü auf die Registerkarte **Schnittstelle**.
 - c) Wählen Sie auf der Seite *Mercury-Schnittstellenkonfiguration* die Option **Mercury-Modus aktivieren** aus und geben Sie die IP-Adresse der Mercury-Steuerung ein.
 - d) Geben Sie in den Feldern **Port**, **Mercury-Benutzername** und **Mercury-Passwort** die Informationen ein, die Sie beim Erstellen des Over-Watch-Plugin-Benutzers auf der Mercury-Steuerung eingegeben haben.
 - e) Wählen Sie die Option **SSL aktivieren** aus und klicken Sie auf **Mercury-Zertifikat verwenden**.
 - f) Klicken Sie auf **Aktualisieren**.
Der Verbindungsstatus ist gelb.

- 4 Aktivieren Sie das Over-Watch-Plugin auf der Synergis™ Cloud Link-Einheit.
 - a) Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
 - b) Klicken Sie auf **Konfiguration > Mercury-Controller-Einstellungen**.
 - c) Klicken Sie im Seitenmenü auf die Registerkarte **Over-Watch-Einstellungen**.
 - d) Wählen Sie die Option **LP4502-Over-Watch-Plugin** aus und geben Sie den **Benutzernamen**, das **Password** und den **Port** ein, die Sie beim Erstellen des Over-Watch-Plugin-Benutzers auf der Mercury-Steuerung konfiguriert haben.
 - e) Klicken Sie auf **Speichern**.
 - f) Starten Sie Synergis™ Software neu.

Nach Durchführen dieser Schritte

Registrieren Sie ein BEST-Wi-Q-Gateway auf der Synergis™-Einheit.

BEST-Wi-Q-Gateways auf der Synergis™-Einheit über Mercury-Controller registrieren

Sie müssen BEST-Wi-Q-Gateways über Mercury-LP4502-Steuerungen in Config Tool registrieren, bevor Sie BEST-Wi-Q-Schlösser und drahtlose Zutrittskontrollsteuerungen hinzufügen können.

Bevor Sie beginnen

Konfigurieren Sie das Over-Watch-Plugin auf der Mercury-Steuerung und aktivieren Sie es auf der Synergis™-Einheit.

Was Sie noch wissen sollten

Prozedur

- 1 Registrieren Sie den Mercury-LP4502-Controller in Config Tool.
 - a) Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
 - b) Klicken Sie auf **Rollen und Einheiten**, und klicken Sie dann auf die Synergis™- Einheit.
 - c) Klicken Sie auf **Peripheriegeräte** und dann auf **Einen Eintrag hinzufügen** (+).

Manufacturer: Mercury Security

Model: LP4502

IP address: 0 . 0 . 0 . 0 [Hostname](#)

Port: 3001

Channel: 1

Interfaces:

Model	Port	Address	IP address

+ x pencil

Advanced settings

Cancel OK

- d) Geben Sie die folgenden Informationen ein:
 - **Modell:** Wählen Sie „LP4502“ aus.
 - **IP-Adresse:** Statische IP-Adresse, die dem Controller von Ihrer IT-Abteilung zugewiesen wurde.
 - **Hostname:** Klicken Sie auf den blauen Link, um die Steuerung ihrem Hostnamen nach zu identifizieren. Diese Option ist nur verfügbar, wenn Sie Security Center 5.12.0.0 oder neuer ausführen.
 - **Port:** Kommunikationsport (Default=3001). Der Port muss mit dem auf der Mercury Device Manager-Webseite konfigurierten Wert übereinstimmen.
 - **Kanal:** Kanal-ID für diesen Controller. Die Kanal-ID kann ein beliebiger Wert zwischen 0 und 63 sein und muss innerhalb der Synergis™-Einheit eindeutig sein. Nach dem Zuweisen darf sie nicht mehr geändert werden.

- 2 Fügen Sie das BEST-Wi-Q-Gateway als Schnittstelle zur Mercury-Steuerung hinzu.
 - a) Klicken Sie in der Liste *Schnittstellen* auf **Einen Eintrag hinzufügen** (+).
 - b) Wählen Sie im Dialogfeld, das geöffnet wird, **BEST-Wi-Q-Gateway** als **Modell** aus und geben Sie die **MAC-Adresse** ein.
BEMERKUNG: Stellen Sie sicher, dass die MAC-Adresse in Großbuchstaben eingegeben wird, 12 Zeichen lang ist und keine Punkte, Doppelpunkte oder Bindestriche enthält. Beispielsweise *A1B2C3D4E5F6*.

Der Mercury-Controller und das BEST-Wi-Q-Gateway sind auf der Seite **Peripheriegeräte** der Synergis™ Cloud Link-Einheit im Config Tool online und die Verbindung wird auf der Webseite des BEST-Wi-Q-Gateways hergestellt.

Nach Durchführen dieser Schritte

Koppeln Sie BEST-Wi-Q-Schlösser oder drahtlose Zutrittssteuerungen mit dem BEST-Wi-Q-Gateway und weisen Sie ihnen ACR (Zutrittskontrolllesegerät, Access Control Reader)-IDs über die Webseite des BEST-Wi-Q-Gateways zu, sodass sie im Config Tool später hinzugefügt werden können. Weitere Informationen über das Koppeln von Geräten mit dem Gateway finden Sie in der BEST-Wi-Q-Dokumentation.

BEST-Wi-Q-Schlösser und drahtlose Zutrittssteuerungen zum Gateway hinzufügen

Sie müssen BEST-Wi-Q-Schlösser und drahtlose Zutrittssteuerungen zum Gateway im Config Tool hinzufügen.

Bevor Sie beginnen

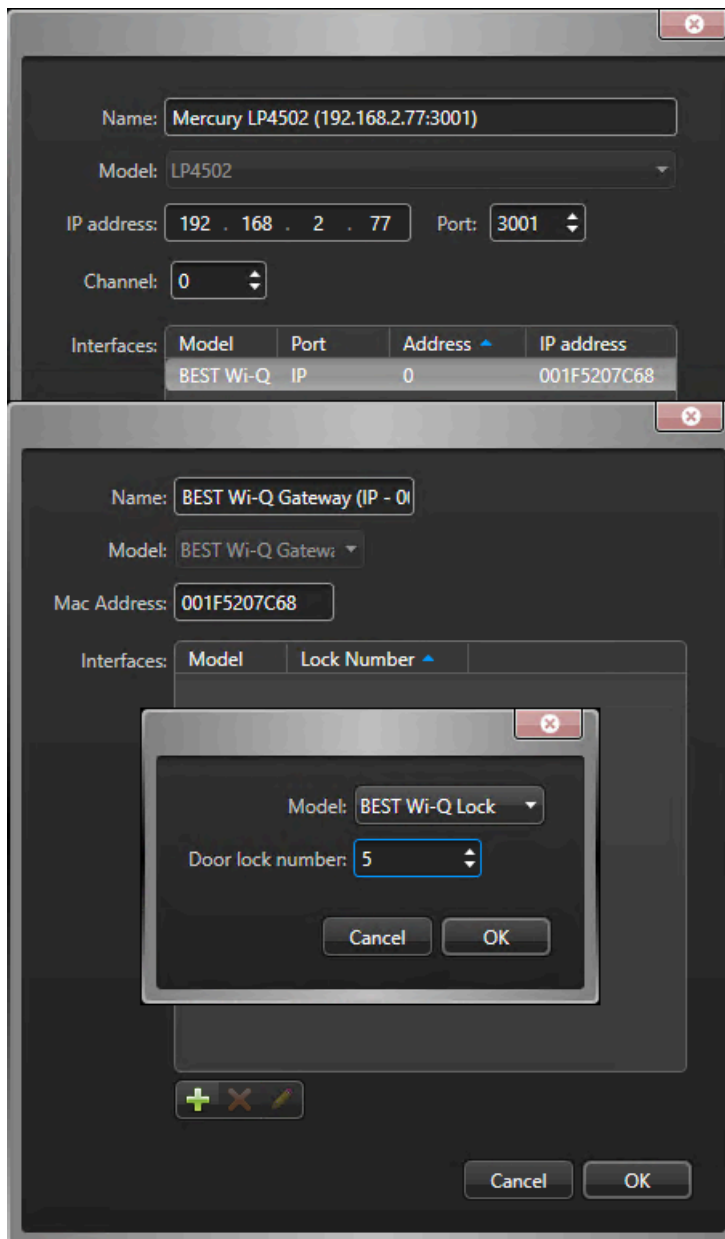
Koppeln Sie BEST-Wi-Q-Schlösser oder drahtlose Zutrittssteuerungen mit dem BEST-Wi-Q-Gateway und weisen Sie ihnen ACR (Zutrittskontrolllesegerät, Access Control Reader)-IDs über die Webseite des BEST-Wi-Q-Gateways zu, sodass sie im Config Tool hinzugefügt werden können. Weitere Informationen über das Koppeln von Geräten mit dem Gateway finden Sie in der BEST-Wi-Q-Dokumentation.

Prozedur

- 1 Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
- 2 Klicken Sie auf **Rollen und Einheiten**, und klicken Sie dann auf die Synergis™- Einheit.
- 3 Klicken Sie auf die Registerkarte **Peripheriegeräte** und führen Sie dann einen Doppelklick auf die Mercury-LP4502-Steuerung aus.
- 4 Führen Sie im Dialogfeld, das geöffnet wird, einen Doppelklick auf das BEST-Wi-Q Gateway in der Liste *Schnittstellen* aus.
- 5 Klicken Sie im Dialogfeld, das geöffnet wird, auf **Ein Element hinzufügen** (+) unter der Liste *Schnittstellen*.

Ein Dialogfeld wird geöffnet, bei dem **BEST-Wi-Q-Schloss** als **Modell** ausgewählt ist. Diese Option wird für Schlösser und drahtlose Zutrittssteuerungen verwendet.

- 6 Geben Sie die **Türschlossnummer** für das Schloss oder die drahtlose Zutrittssteuerung ein und klicken Sie dann auf **OK**.



BEMERKUNG: Die Türschlossnummer muss der Zutrittskontrollesegeräte-ID entsprechen, die dem Schloss oder der drahtlosen Zutrittssteuerung an der Webseite des BEST-Wi-Q-Gateways zugewiesen wurde.

Status	ACR ID	Description	MAC Address	Firmware	Actions
●	5	WACS	0014F540ED7E	3.02.004	EDIT [X] [↺] [DEEP ↻]
●	10	Lock10	0014F540EEF7	3.02.005	EDIT [X] [↺] [DEEP ↻]

Showing 1 to 2 of 2 entries

7 Klicken Sie auf **OK** > **OK**.

8 Klicken Sie auf **Anwenden**.

Die Mercury-Steuerung, das BEST-Wi-Q-Gateway und Schlösser werden auf der Seite *Peripheriegeräte* angezeigt.

Name	Type	State	Additional info	Controlling
Mercury LP4502 (192.168.2.77:3001)		Online	Number of credentials synced...	
Input 1	In	Normal	Normally open / Not supervis...	LP Door 1
Input 2	In	Normal	Normally open / Not supervis...	LP Door 1
Input 3	In	Normal	Normally open / Not supervis...	LP Door 2
Input 4	In	Normal	Normally open / Not supervis...	LP Door 2
Input 5	In	Normal	Normally open / Not supervis...	LP REX door
Input 6	In	Normal	Normally open / Not supervis...	LP REX door
Input 7	In	Normal	Normally open / Not supervis...	
Input 8	In	Normal	Normally open / Not supervis...	
Input Connection-Reader-1	In	Active	---	
Input Connection-Reader-2	In	Active	---	
Input InternalBatteryMonitor	In	Active	---	
Input PowerMonitor	In	Normal	---	
Input Tamper	In	Normal	---	
Input Tamper-Reader-1	In	Active	---	
Input Tamper-Reader-2	In	Normal	---	
Output 1	Out	Normal	---	LP Door 1
Output 2	Out	Normal	---	LP Door 2
Output 3	Out	Normal	---	LP REX door
Output 4	Out	Normal	---	
Reader 1	Reader	Active	Standard OSDP	LP Door 1
Reader 2	Reader	Active	Standard Wiegand	LP Door 2
BEST Wi-Q Gateway (IP - ADDRESS0014F5208...		Online		
Input Tamper	In	Normal	---	
BEST Wi-Q Lock - 5		Online		
BEST Wi-Q Lock - 10		Online		
Sim - SIM (Sim 1)		Online		
Sim - SIM (Sim 2)		Online		
Synergis - OnboardIO (1 - Onboard IO)		Online		

Auf der Webseite des BEST-Wi-Q-Gateways wird der Status des Schlosses oder der drahtlosen Zutrittssteuerung grün, das/die Sie im Config Tool hinzugefügt haben.

Nach Durchführen dieser Schritte

Weisen Sie im Config Tool die Schloss- oder WAC-E/A zu Türen zu. Sie können die Türvorlage *Karte hinein*, *REX hinaus* verwenden, um die Konfiguration zu beschleunigen.

Beispiel: Die folgende Abbildung zeigt eine typische Konfiguration auf der Seite *Hardware* einer Tür.

Preferred unit:

Preferred interface:

Door side In ✎

Reader: ✎ ✕

Request to exit: ✕

Entry sensor: ✕

Camera:

Door side Out ✎

Reader: ✎ ✕

Request to exit: ✕

Entry sensor: ✕

Camera:

Additional connections

Door lock: ✕

Door sensor: ✕

Informationen über den BEST Wi-Q-Durchgangsmodus

BEST-Wi-Q-Geräte haben einen nativen Durchgangsmodus, auch bekannt als *Klassenraummodus* oder *doppeltes Ausweisen*, wobei der Benutzer eine Tür entsperrt, indem er einen Ausweis doppelt am Lesegerät vorweist, und sie wieder versperrt, indem er sich wieder doppelt ausweist.

So aktivieren und konfigurieren Sie die Funktion

Der BEST-Wi-Q-Durchgangsmodus wird über das benutzerdefinierte Türfeld *DoubleSwipe* aktiviert, so wie die Funktion zur Aktivierung des doppelten Ausweisens im Security Center aktiviert wird.

Weitere Informationen finden Sie unter den folgenden Themen im *Security Center – Administratorhandbuch*:

- Informationen über Doppelausweisaktivierung
- Doppelausweisaktivierung
- Eine Tür für Doppelausweisaktivierung konfigurieren

Damit ein Karteninhaber den Durchgangsmodus benutzen kann, muss er Teil von allen Karteninhabergruppen sein, die zum Verwenden des benutzerdefinierten Felds *DoubleSwipe* auf allen BEST-Wi-Q-Türen unter der gleichen Mercury-LP4502-Steuerung konfiguriert sind. Um die Konfiguration zu vereinfachen ist es daher empfehlenswert, nur eine Karteninhabergruppe zum Verwenden der Funktion auf diesen Türen zuzuweisen.

Nachdem diese Funktion konfiguriert wurde, wird beim doppelten Ausweisen am Lesegerät das Ereignis *Doppeltes Ausweisen an* erstellt und die Tür wird entsperrt. Doppeltes Ausweisen beim gleichen Lesegerät erstellt wieder ein Ereignis des Typs *Doppeltes Ausweisen aus* und die Tür wird wieder versperrt.

Einschränkungen

Türen mit BEST-Wi-Q-Schlössern unterstützen Mercury-Summerfunktionen nicht.

SimonsVoss-SmartIntego-Schlösser über Mercury

Dieser Abschnitt enthält die folgenden Themen:

- ["Vorbereitung für die Registrierung von SimonsVoss SmartIntego-Schlössern"](#) auf Seite 203
- ["Registrieren von SimonsVoss SmartIntego-Schlössern an der Synergis™-Einheit"](#) auf Seite 205

Vorbereitung für die Registrierung von SimonsVoss SmartIntego-Schlössern

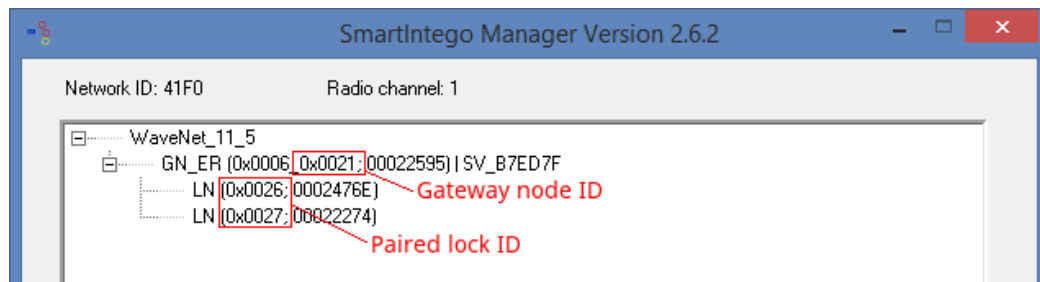
Bevor Sie die SmartIntego-Schlösser an der Synergis™-Einheit registrieren können, müssen Sie den Gateway-Knoten mit Ihren SmartIntego-Schlössern koppeln.

Was Sie noch wissen sollten

Die mit *Härtung* gekennzeichneten Schritte und Anweisungen sind optional, schützen Ihr System aber vor Cyberangriffen.

Prozedur

- 1 Folgen Sie der Dokumentation, die mit Ihren SmartIntego-Geräten geliefert wurde, und koppeln Sie den Gateway-Knoten mit Ihren SmartIntego-Schlössern.
- 2 Schreiben Sie die folgenden Informationen auf:
 - IP-Adresse des Gateway-Knotens.
 - Die Geräte-IDs aus dem Fenster *SmartIntego Manager*.



Die Gateway-Knoten-ID ist die zweite hexadezimale Zahl nach GN_ER.

Die Schloss-ID ist die erste hexadezimale Zahl nach LN.

- 3 (*Härtung*) Folgen Sie der Dokumentation, die mit Ihren SmartIntego-Geräten geliefert wurde, und konfigurieren Sie den Kommunikationsverschlüsselungsschlüssel für Ihre Schlösser.
Die SmartIntego-Software erlaubt es nicht, ein Schloss ohne Passwort mit dem Hub zu koppeln.
Verwenden Sie ein sicheres Passwort für das Schließsystem.

New Project - SmartIntego

Project:

Name: SmartIntego for Systemintegration

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

Locking system:

Password: ●●●●●●

Confirm password: ●●●●●●

Attention! Please store your passwords in safe place!
When you lost passwords, you will not able to program your locking system.

Launch SmartIntego Manager

Open this project as default

Create Cancel

Registrieren von SimonsVoss SmartIntego-Schlössern an der Synergis™-Einheit

Da die Synergis™-Einheit nicht mit den SimonsVoss SmartIntego-Geräten kommuniziert, müssen Sie diese Geräte über einen Mercury EP-, LP-, MP- oder Honeywell-Controller registrieren und dafür das Config Tool verwenden.

Bevor Sie beginnen

[Koppeln Sie Ihren Gateway-Knoten mit Ihren SmartIntego-Schlössern.](#)

Was Sie noch wissen sollten

Mercury-Controller, die auf einer Synergis-Einheit registriert sind, sind auf der Seite *Hardware* des Synergis™ Appliance Portal nicht sichtbar.

Auf der Synergis™-Einheit muss jedem Mercury-Controller eine eindeutige Kanal-ID zugewiesen werden. Der Controller kommuniziert mit den SmartIntego Gateway-Knoten über IP. IP-Adressen können sich innerhalb desselben Netzes nicht überschneiden.

Prozedur

- 1 Öffnen Sie auf der Config-Tool-Startseite den Task *Zutrittskontrolle*.
- 2 Klicken Sie auf **Rollen und Einheiten**, und klicken Sie dann auf die Synergis™- Einheit.

- 3 Klicken Sie auf **Peripheriegeräte** und dann auf **Einen Eintrag hinzufügen (+)**.

- 4 Geben Sie die folgenden Informationen ein:

- **Modell:** Modell des Controllers.
- **IP-Adresse:** Statische IP-Adresse, die dem Controller von Ihrer IT-Abteilung zugewiesen wurde.
- **Hostname:** Klicken Sie auf den blauen Link, um die Steuerung ihrem Hostnamen nach zu identifizieren. Diese Option ist nur verfügbar, wenn Sie Security Center 5.12.0.0 oder höher ausführen.
BEMERKUNG: Wenn Sie eine Mercury-Steuerung mit ihrem Hostnamen registrieren, müssen Sie `.local` an den Hostnamen anhängen, wenn die Steuerung nicht bei DHCP und DNS im Netzwerk registriert ist.
- **Port:** Kommunikationsport. Der Standardwert ist 3001. Der Port muss mit dem auf der Mercury Device Manager-Webseite konfigurierten Wert übereinstimmen.
- **Kanal:** Kanal-ID für diesen Controller. Die Kanal-ID kann ein beliebiger Wert zwischen 0 und 63 sein. Sie muss innerhalb der Synergis-Einheit eindeutig sein. Nach dem Zuweisen darf sie nicht mehr geändert werden.

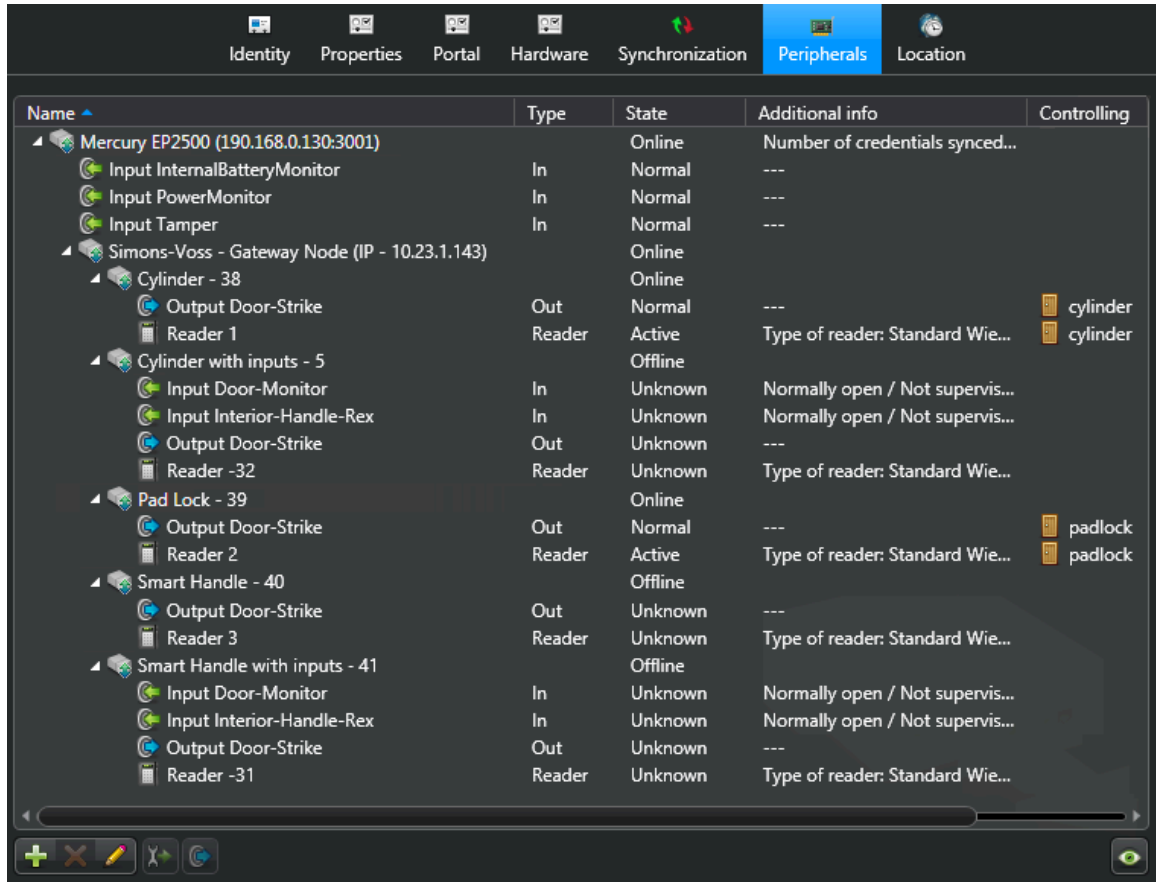
- 5 Klicken Sie unten in der Gruppe *Schnittstellen* auf **Einen Eintrag hinzufügen** (+), um den SmartIntego-Gateway-Knoten hinzuzufügen, mit dem der Controller kommunizieren soll.
 - a) Klicken Sie im angezeigten Dialogfeld auf **Modell** und wählen Sie dann den Knoten **SimonsVoss Gateway** aus.
 - b) Geben Sie in **IP-Adresse** die IP-Adresse des Gateway-Knotens ein.
 - c) Geben Sie in **Router** den Dezimalwert der Gateway-Knoten-ID ein.
Wenn die Gateway-Knoten-ID zum Beispiel 0x0021 lautet, geben Sie 33 ein ($= 2 \times 16 + 1$).

- 6 Klicken Sie unten in der Liste *Schnittstellen* auf **Einen Eintrag hinzufügen** (+), um die Schlösser hinzuzufügen, die mit dem Gateway-Knoten gekoppelt sind.
 - a) Klicken Sie in dem angezeigten Dialogfeld auf **Modell** und wählen Sie dann das Schlossmodell (Smart Handle, Vorhängeschloss, Zylinder usw.) aus.
 - b) Geben Sie in **Türverriegelungsnummer** den Dezimalwert der Schloss-ID ein.
Wenn die Schloss-ID zum Beispiel 0x0026 lautet, geben Sie 38 ein ($= 2 \times 16 + 6$).

- c) Klicken Sie auf **OK**.
- d) Wiederholen Sie den Vorgang, wenn Sie weitere Schlösser hinzufügen möchten.
- e) Klicken Sie auf **OK**.

7 Klicken Sie auf **OK > Anwenden**.

Der Mercury-Controller mit allen angeschlossenen nachgeschalteten Panels und Peripheriegeräten ist auf der Seite *Peripheriegeräte* aufgeführt.



BEMERKUNG: Das Hinzufügen von Schnittstellenmodulen zur Synergis™-Einheit führt zu einem Software-Neustart der Einheit. Während dieses Vorgangs werden die Synergis™-Einheit und alle damit verbundenen Peripheriegeräte in Rot angezeigt.

8 Testen Sie Ihre Konfiguration, indem Sie die Ausgänge auslösen.

Der ausgelöste Ausgang ändert seinen Zustand in Echtzeit auf dem Bildschirm.

BEMERKUNG: Lesegerätaktivitäten werden auf der Seite *Peripheriegeräte* nicht angezeigt.

SALTO-SALLIS-Funkschlösser

Dieser Abschnitt enthält die folgenden Themen:

- ["Registrieren von SALTO SALLIS-Schlössern"](#) auf Seite 210
- ["Aktivieren der Verschlüsselung auf einem vorhandenen SALLIS-Router"](#) auf Seite 215
- ["Verschlüsselung auf einem SALLIS-Router deaktivieren"](#) auf Seite 216

Registrieren von SALTO SALLIS-Schlössern

Damit die Synergis™-Einheit mit SALTO SALLIS-Schlössern kommuniziert, müssen Sie diese im Security Center mithilfe des Synergis™ Appliance Portals registrieren.

Bevor Sie beginnen

Richten Sie Ihre SALTO SALLIS-Infrastruktur (Router, Knoten und Funkschlösser) gemäß den Anweisungen in der *SALLIS-Installations- und Wartungsanleitung* ein.

Definieren Sie zunächst die Knoten und die Türen mit der SALLIS-Anwendung und aktualisieren Sie dann die Router und initialisieren Sie die Schlösser mit dem PPD (Portable Programmer Device). Notieren Sie dabei die folgenden Informationen:

- **IP-Router:** IP-Adresse und Portnummer.
- **RS-485-Router:** Der Synergis™-Einheitenkanal, an den der Router angeschlossen ist (1 - 4) .
- **Schloss:** Router, Schloss-ID und die Tür, an der es installiert ist.

Verwenden Sie aussagekräftige Türnamen, z. B. *1. Stock, Lagerraum*. Wenn Sie die Türeinheiten bereits in Security Center erstellt haben, verwenden Sie der Einfachheit halber dieselben Namen.

Was Sie noch wissen sollten

Die mit *Härtung* gekennzeichneten Schritte und Anweisungen sind optional, schützen Ihr System aber vor Cyberangriffen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **Salto** als **Hardwaretyp** aus.

- 5 Identifizieren Sie den Kanal, an den der SALLIS-Router angeschlossen ist, und führen Sie dann einen der folgenden Schritte aus:
 - Wählen Sie den IP-Kanal aus, und geben Sie die vom Router verwendete IP-Adresse und Portnummer ein.

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

- Wählen Sie einen RS-485-Kanal aus (1 - 4) . Alle Schnittstellenmodule, die mit demselben RS-485-Kanal verbunden sind, müssen vom selben Hersteller stammen.

Add hardware

Hardware type
Salto

Channel
2

Interface module type
Salto Sallis

Physical address
1

Enable encryption

Interface module type Physical address

Add

Scan **Cancel** **Save**

- 6 (Härtung) Wenn Sie Verschlüsselung wünschen, wählen Sie **Verschlüsselung aktivieren** und geben Sie den **AES-Standortschlüssel** ein.

BEMERKUNG: Sie können die Verschlüsselungseinstellungen nicht über das Dialogfeld *Hardware hinzufügen* für einen vorhandenen Kanal ändern. Um die Verschlüsselung zu aktivieren, wenn der Kanal bereits erstellt wurde, [ändern Sie die Kanalkonfiguration im Synergis™ Appliance Portal](#).

The screenshot shows a dark-themed dialog box titled "Add hardware". It contains several configuration fields:

- Hardware type:** A dropdown menu with "Salto" selected.
- Channel:** A dropdown menu with "2" selected.
- Interface module type:** A dropdown menu with "Salto Sallis" selected.
- Physical address:** A text input field containing the number "1".
- Enable encryption:** A checkbox that is checked, with a red checkmark icon.
- AES site key:** A text input field with a red underline and a cursor, containing several dots representing a key.

At the bottom of the dialog, there are three buttons: "Scan" (grey), "Cancel" (grey), and "Save" (red).

- 7 Fügen Sie im selben Dialogfeld alle Schnittstellenmodule hinzu, die mit demselben Kanal verbunden sind. Sie können die Schnittstellenmodule automatisch oder manuell registrieren.

TIPP: Wenn Sie Ihre Schloss-IDs (physische Adressen) kennen und nur einige wenige zu registrieren haben, ist es schneller, diese manuell zu registrieren.

- Um die Registrieren automatisch durchzuführen, klicken Sie auf **Scannen**.

Die Ermittlungsfunktion sucht alle Schnittstellenmodule desselben Herstellers, die mit demselben Kanal verbunden sind, und registriert sie.

Wenn der Controller nicht alle angeschlossenen Schnittstellenmodule findet, stellen Sie sicher, dass sie alle unterschiedliche physische Adressen haben.

- Zur manuellen Anmeldung geben Sie die Schloss-ID als **physische Adresse** ein und klicken auf **Hinzufügen (+)**.

BEMERKUNG: Gültige Schloss-IDs sind 1 bis 16 für RS-485-Router und 1 bis 64 für PoE-Router.

Wiederholen Sie den Vorgang nach Bedarf, um alle Funkschlösser zu konfigurieren, die mit demselben Kanal verbunden sind.

- 8 Klicken Sie auf **Speichern**.

Der Hardwaretyp, der Kanal und das Schnittstellenmodul, das Sie gerade hinzugefügt haben, werden auf der Seite *Hardwarekonfiguration* angezeigt.

- 9 [Testen Sie die Verbindung und Konfiguration Ihres Schnittstellenmoduls auf der Seite *E/A-Diagnose*](#) .

Nach Durchführen dieser Schritte

Verknüpfen Sie Ihre Türen mit den SALLIS-Schlössern im Security Center.

Aktivieren der Verschlüsselung auf einem vorhandenen SALLIS-Router

Verschlüsselung ist eine Kanaleigenschaft in Synergis™ Appliance Portal. Sie können die Verschlüsselung aktivieren oder das Verschlüsselungskennwort auf einem SALLIS-Router ändern, indem Sie die Kanalkonfiguration im Synergis™ Appliance Portal ändern.

Was Sie noch wissen sollten

Sie können die Kanaleinstellungen nicht ändern, während Sie ein Schloss zu einem bestehenden Kanal hinzufügen. Nachdem der Kanal erstellt wurde, müssen alle Änderungen an den Kanaleigenschaften über die Kanaleigenschaftsseite vorgenommen werden. Nachdem die Verschlüsselung aktiviert wurde, können Sie sie nicht mehr deaktivieren, indem Sie sie im Synergis™ Appliance Portal deaktivieren. Sie müssen [die Verschlüsselung auch deaktivieren, indem Sie sich direkt mit dem Router verbinden](#).

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Wählen Sie den SALTO-Kanal.
- 4 Wählen Sie die Option **Verschlüsselung aktivieren**, und geben Sie den **AES-Standortschlüssel** ein.
- 5 Klicken Sie auf **Speichern**.

Verschlüsselung auf einem SALLIS-Router deaktivieren

Um die Verschlüsselung auf einem SALLIS-Router zu deaktivieren, müssen Sie sie sowohl in Synergis™ Appliance Portal als auch auf dem Router selbst deaktivieren.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie den SALTO-Kanal, und deaktivieren Sie dann die Option **Verschlüsselung aktivieren**.
- 5 Klicken Sie auf **Speichern**.
In der Gerätestruktur erscheinen alle SALLIS-Schlösser unter dem ausgewählten Kanal in rot (inaktiv).
- 6 Gehen Sie für einen RS-485-Router wie folgt vor:
 - a) Laden Sie mit der SALLIS-Anwendung die Routerkonfiguration in das PPD herunter.
 - b) Wählen Sie im PPD die Option **Router aktualisieren**.
 - c) Verbinden Sie das PPD mit dem Router.
- 7 Bei einem PoE-Router gehen Sie wie folgt vor:

BEMERKUNG: Wenn Sie viele Router zu aktualisieren haben, aktualisieren Sie sie nacheinander.

 - a) Öffnen Sie die Abdeckung des PoE-Routers, und halten Sie die Taste **CLR** fünf Sekunden lang gedrückt. Die LED auf der PoE-Router-Platine leuchtet orange.
 - b) Verbinden Sie sich mit einem Webbrowser mit dem Webportal des Routers.
Geben Sie <http://192.168.0.234> in das URL-Feld des Browsers ein.
BEMERKUNG: Ihre Workstation muss sich im selben Subnetz wie der Router befinden, damit Sie eine Verbindung zum Webportal herstellen können.
 - c) Wählen Sie auf der Browserseite unter **Router-Verschlüsselung > Zurück zum einfachen Modus?** die Option **Ja**.
 - d) Klicken Sie auf **Senden**.

Die Meldung *Konfiguration erfolgreich gesendet* wird im Browser angezeigt. In der Gerätestruktur werden alle SALLIS-Schlösser unter dem ausgewählten Kanal in schwarzer Farbe (aktiv) angezeigt.

OSDP-Lesegeräte, die mit den RS-485-Ports von Synergis™ Cloud Link verbunden sind

Dieser Abschnitt enthält die folgenden Themen:

- "[Erstellen eines Kanals zur Konfiguration von OSDP-Lesegeräten im Synergis™ Appliance Portal](#) " auf Seite 218
- "[Konfigurieren und Hinzufügen von OSDP-Lesegeräten im Synergis™ Appliance Portal](#)" auf Seite 221
- "[Aktivierung der sicheren Koppelung auf OSDP-Lesegeräten im Synergis™ Appliance Portal](#)" auf Seite 223
- "[MIFARE DESFire für transparente OSDP-Lesegeräte aktivieren](#)" auf Seite 224
- "[Konfigurieren von OSDP-Lesegeräten zur Verhinderung von Relaisangriffen](#)" auf Seite 228
- "[Übertragung von Dateien an OSDP-Lesegeräte im Synergis™ Appliance Portal](#)" auf Seite 229

Erstellen eines Kanals zur Konfiguration von OSDP-Lesegeräten im Synergis™ Appliance Portal

Bei OSDP-Lesegeräten müssen die RS-485-Bitrate und Adresse konfiguriert sein, bevor sie verwendet werden können. Sie können Ihre Lesegeräte direkt über das Synergis™ Appliance Portal konfigurieren, indem Sie einen OSDP-Kanal mit aktiviertem Programmiermodus erstellen.

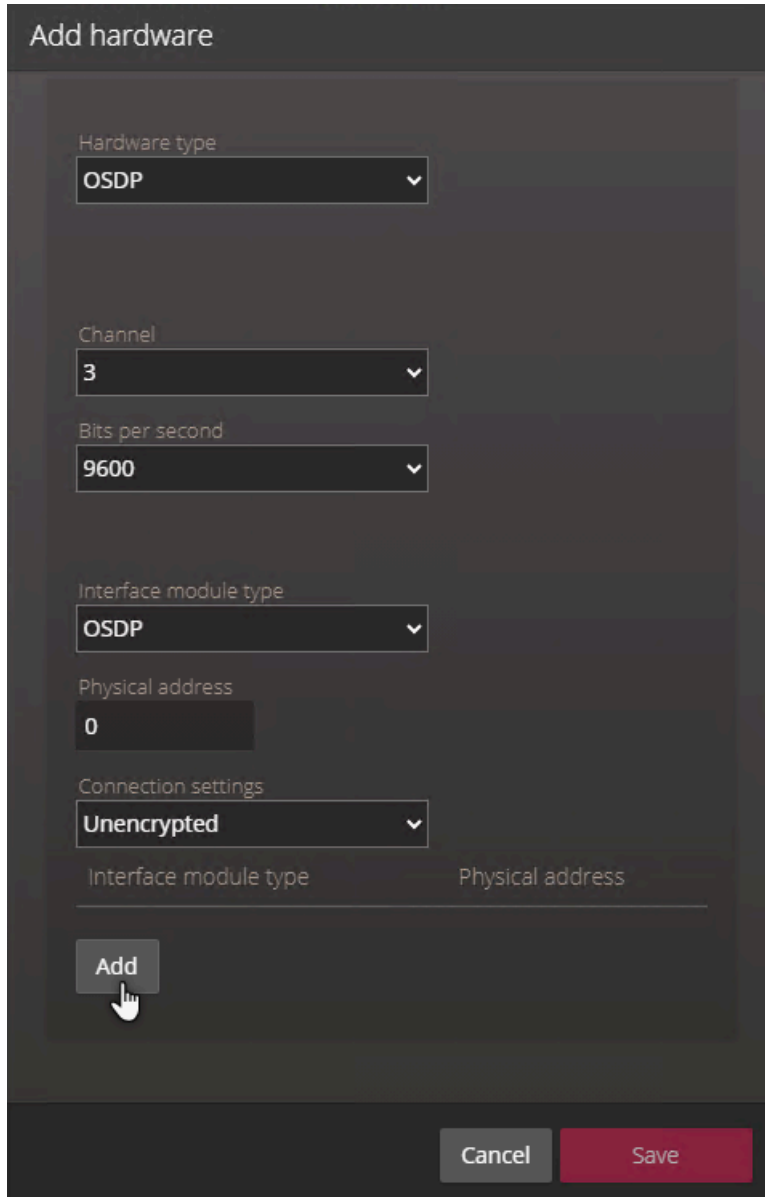
Was Sie noch wissen sollten

- Bei OSDP-Lesegeräten, die mit einer Mercury-Einheit verbunden werden sollen, wird mithilfe dieses Verfahrens gefolgt von dem [Festlegen der physischen Adresse des Lesegeräts](#) im Synergis™ Appliance Portal die Verwendung einer Konfigurationskarte zum Festlegen der Baudrate und der physischen Adresse des Lesegeräts abgelöst.
- Wenn der Programmiermodus aktiviert ist, kann jeweils nur ein Online-Lesegerät an den RS-485-Kanal angeschlossen werden.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **OSDP** als **Hardwaretyp** aus.
- 5 Wählen Sie den **Kanal** aus (1 - 4) .
BEMERKUNG: Wenn Sie die Synergis™ Cloud Link 312-Einheit haben, haben Sie bis zu 12 Kanäle. Weitere Informationen finden Sie unter [Informationen über Ports in Synergis Cloud Link 312 RS-485](#).
- 6 Wählen Sie aus der Liste **Bits pro Sekunde** die Bitrate aus, die Sie für Ihr Gerät konfigurieren möchten.
BEMERKUNG: Wählen Sie in der Liste **Andere** aus, um eine benutzerdefinierte Bitrate einzugeben.

- 7 Klicken Sie unter **Typ des Schnittstellenmoduls** auf **Hinzufügen**.



Add hardware

Hardware type
OSDP

Channel
3

Bits per second
9600

Interface module type
OSDP

Physical address
0

Connection settings
Unencrypted

Interface module type Physical address

Add

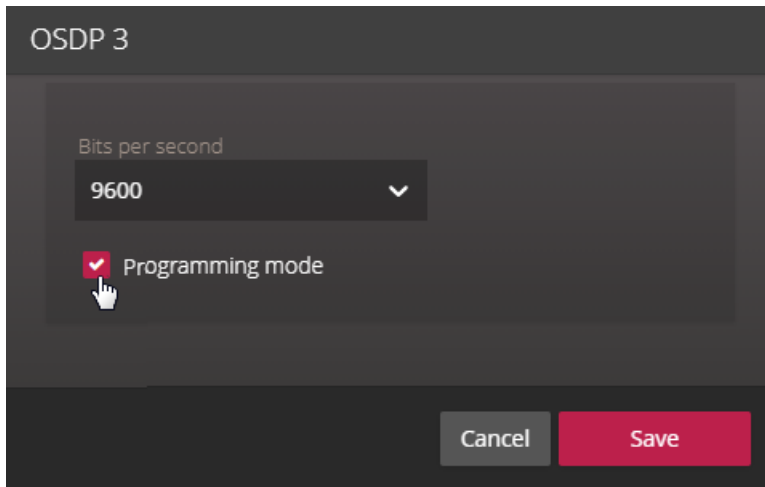
Cancel Save

- 8 Klicken Sie auf **Speichern**.
Der Kanal und die Schnittstelle werden erstellt.
- 9 Wählen Sie in der Hardwarestruktur den OSDP-Kanal aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** (✎).

OSDP-Lesegeräte, die mit den RS-485-Ports von Synergis™ Cloud Link verbunden sind

- 10 Wenn Sie ein Lesegerät hinzufügen, aktivieren Sie das Kontrollkästchen **Programmierungsmodi** checkbox.

Wenn Sie über eine Konfigurationskarte verfügen, können Sie diese anstatt des **Programmiermodus** verwenden. Sehen Sie in der Dokumentation nach, die mit Ihrer Karte geliefert wurde.



- 11 Klicken Sie auf **Speichern**.

Nach Durchführen dieser Schritte

[Konfigurieren Sie die OSDP-Lesegeräte](#)

Konfigurieren und Hinzufügen von OSDP-Lesegeräten im Synergis™ Appliance Portal

Um OSDP-Lesegeräte zu einer Mercury- oder Synergis™-Einheit hinzuzufügen, konfigurieren Sie die Lesegeräte mithilfe von Synergis™ Appliance Portal.

Bevor Sie beginnen

Erstellen Sie einen OSDP-Kanal mit aktiviertem Programmiermodus.

Was Sie noch wissen sollten

- Alle Lesegeräte, die an denselben RS-485-Kanal angeschlossen sind, müssen mit unterschiedlichen Adressen versehen werden.
- Bevor Sie OSDP-Lesegeräte an eine Mercury-Einheit anschließen, müssen Sie möglicherweise die Baudrate und die Adresse des Lesegeräts einstellen. Durch die Einstellung der Baudrate im Synergis™ Appliance Portal und die anschließende Durchführung dieses Verfahrens wird die Verwendung einer Konfigurationskarte ersetzt.
- Wenn der Programmiermodus aktiviert ist, kann jeweils nur ein Lesegerät an den RS-485-Kanal angeschlossen werden.

BEST-PRACTICE: Wenn Sie OSDP-Lesegeräte an benachbarten Drehkreuzen installieren, ist es nicht empfehlenswert, mehr als zwei Lesegeräte an denselben RS-485-Kanal anzuschließen, da sich dadurch die Reaktionszeit des Controllers erhöht und die Wahrscheinlichkeit hoch ist, dass zwei oder mehr Karten gleichzeitig vorgelegt werden. Bei herkömmlichen Türen können Sie bis zu vier Lesegeräte pro Bus installieren.

Prozedur

- 1 Wählen Sie in der Hardwarestruktur das OSDP-Lesegerät aus, das Sie beim Erstellen des OSDP-Kanals hinzugefügt haben, und klicken Sie auf **Bearbeiten** (✎).

- 2 Geben Sie im Dialogfeld *Eigenschaften* die physische Adresse ein, die Sie für das Lesegerät festlegen möchten, und konfigurieren Sie die Optionen **Signalton bei Kartenlesen** und **LED bei Abwesenheit ausschalten** wie gewünscht.

OSDP 0

Properties

Physical address
0

Connection settings
Unencrypted

Reader type
Non-transparent reader (reader configuration)

Beep on card read

Turn off LED when idle

Cancel Save

- 3 Klicken Sie auf **Speichern**.
- 4 Verbinden und starten Sie das Lesegerät.
Die konfigurierte Bitrate und physische Adresse werden an das Lesegerät gesendet, welches den Betrieb startet, nachdem es diese akzeptiert hat.
- 5 Trennen Sie das Lesegerät oder schalten Sie es aus.
- 6 Wiederholen Sie die Schritte 1 bis 5 für die verbleibenden Lesegeräte.
- 7 Wählen Sie in der Hardwarestruktur den OSDP-Kanal aus und klicken Sie auf **Bearbeiten** (✎).
Deaktivieren Sie dann das Kontrollkästchen **Programmiermodus**, welches Sie beim Erstellen des Kanals ausgewählt haben.
- 8 Fügen Sie die konfigurierten Lesegeräte hinzu:
 - a. Klicken Sie oben in der Spalte *Adresse* auf **Hinzufügen** (+).
 - b. Klicken Sie im Dialogfeld *Hardware hinzufügen* auf **Hinzufügen**, um die Lesegeräte an den von Ihnen programmierten Adressen hinzuzufügen.
- 9 Klicken Sie auf **Speichern**.

Nach Durchführen dieser Schritte

Aktivieren Sie den sicheren Modus auf den Lesegeräten.

Aktivierung der sicheren Koppelung auf OSDP-Lesegeräten im Synergis™ Appliance Portal

Standardmäßig sind OSDP-Lesegeräte unverschlüsselt registriert. Durch Aktivieren der sicheren Koppelung wird die Sicherheit von Zutrittspunkten erhöht.

Bevor Sie beginnen

[Konfigurieren Sie die OSDP-Lesegeräte.](#)

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Wählen Sie in der Hardwarestruktur das OSDP-Lesegerät aus und klicken Sie auf **Bearbeiten** (✎).
- 4 Wählen Sie in der Liste **Verbindungseinstellungen** die Option **Verschlüsselt** aus.
- 5 From the **OSDP Secure Channel key** list, select one of the following:
 - **Random key:** Generates a random 128-bit (32 hexadecimal characters) key.
 - **Default key:** Uses the unit's default key. This choice is less secure.
 - **Specific key:** This choice lets you specify your own 128-bit (32 hexadecimal characters) key.
- 6 Klicken Sie auf **Speichern**.
- 7 Klicken Sie auf **Konfiguration > Erweitertes OSDP**.
- 8 Suchen Sie nach der Reihe mit dem konfigurierten Port, Lesegerät sowie zugehöriger Tür und klicken Sie auf **Koppeln starten**.

Dadurch werden die Schlüssel ausgetauscht und das Lesegerät ist wieder online. Das Lesegerät ist jetzt sicher. Jedes Gerät, das den Schlüssel ablehnt, bleibt offline.

Doors	Readers	Status	Action
-	OSDP (Port D, Address 0)	● Offline	Start pairing
Direct OSDP	OSDP (Port D, Address 1)	● Online	Paired

MIFARE DESFire für transparente OSDP-Lesegeräte aktivieren

Bei OSDP-Lesegeräten im transparenten Modus müssen Sie die Schlüssel auf Ihrer Synergis™ Cloud Link-Einheit oder auf SAM (Secure Access Modules)-Karten speichern, wenn Sie das Synergis™ Cloud Link-312-Modell haben.

Bevor Sie beginnen

Konfigurieren Sie die MIFARE-DESFire-Schlüssel auf Ihrer Synergis™ Cloud Link-Einheit.

Was Sie noch wissen sollten

Der Modus *Karte oder PIN* wird bei OSDP-Lesegeräten, die im DESFire-Modus (transparenter Modus) konfiguriert wurden, nicht unterstützt.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Hardware** und wählen Sie dann ein registriertes OSDP-Lesegerät aus.
- 3 Klicken Sie auf **Bearbeiten** (✎) für die Schnittstelle des ausgewählten Lesegeräts.

OSDP-Lesegeräte, die mit den RS-485-Ports von Synergis™ Cloud Link verbunden sind

- 4 Wählen Sie in der Liste **Lesegerätetyp** die Option **Transparentes Lesegerät (MIFARE DESFire)** aus.

OSDP 0

Properties

Physical address
0

Connection settings
Unencrypted

Reader type
Transparent reader (MIFARE DESFire)

MIFARE DESFire key location
Synergis key store

Beep on card read

Turn off LED when idle

Cancel Save

- 5 Wählen Sie in der Liste **MIFARE DESFire-Schlüsselort** eine der folgenden Optionen aus:

The screenshot shows a configuration window titled "OSDP 0" with a "Properties" section. It contains several dropdown menus and a checkbox. The "Physical address" is set to "0". "Connection settings" is set to "Unencrypted". "Reader type" is set to "Transparent reader (MIFARE DESFire)". The "MIFARE DESFire key location" dropdown is open, showing three options: "Synergis key store" (highlighted in blue), "SAM (Software crypto)", and "SAM (Hardware crypto)". At the bottom, there is a checkbox labeled "Turn off LED when idle" which is unchecked. Two buttons, "Cancel" and "Save", are located at the bottom right of the window.

- **Synergis key store:** The key for decrypting credentials is stored on the Synergis unit. This option does not require a SAM card.
- **SAM (Software crypto):** This is the faster of the SAM options, but requires the **SessionDumpKey** option to be enabled during the SAM configuration process. For more information, see the documentation that came with your SAM card configuration software.
- **SAM (Hardware crypto):** This option does not require **SessionDumpKey** to be enabled during the SAM configuration process.

BERMerkung: Die SAM-Optionen sind nur verfügbar, wenn Sie das Synergis™ Cloud Link-312-Modell haben.

- 6 Klicken Sie auf **Speichern**.
- 7 Wenn Sie die Option **Synergis-Schlüsselspeicher** wählen, verwenden Sie das Synergis™ Appliance Portal, um auf den *Synergis-Schlüsselspeicher* zuzugreifen und die Schlüssel einzugeben:
- a. Wählen Sie einen Index aus.
 - b. Klicken Sie auf **Neue Version erstellen** und geben Sie einen 32-stelligen hexadezimalen Schlüssel in das Textfeld ein.
 - c. Klicken Sie auf **Hinzufügen**.

Die MIFARE-DESFire-Konfigurationsdatei, die für indizierte Schlüssel verwendet wird, ist mit softwaretransparenten und nicht transparenten Lesegeräten kompatibel.

Einschränkungen: Es gibt zwei Einschränkungen bei softwaretransparenten Lesegeräten:

- Transparente Lesegeräte können derzeit keine Karten codieren.
- Karten mit aktiviertem transparenten Modus benötigen ca.100 ms länger, um gelesen zu werden.

Nach Durchführen dieser Schritte

[Konfigurieren Sie MIFARE DESFire.](#)

OSDP-Lesegeräte, die mit den RS-485-Ports von Synergis™ Cloud Link verbunden sind

Verwandte Themen

[Informationen zu Synergis™ Cloud Link 312](#) auf Seite 6

Konfigurieren von OSDP-Lesegeräten zur Verhinderung von Relaisangriffen

Verhindern Sie Relaisangriffe auf unterstützten OSDP-Lesegeräten, indem Sie eine maximale Verzögerung für die Kartenauthentifizierung konfigurieren.

Was Sie noch wissen sollten

Während eines Relaisangriffs dauert die Authentifizierung einer Karte länger als gewöhnlich, da die Angreifer dazwischen Nachrichten aneinander übermitteln müssen. Daher können Relaisangriffe effektiv verhindert werden, indem Sie eine maximale Verzögerung für die Kartenauthentifizierung festlegen. Wenn die maximale Verzögerung beim Lesen einer Karte überschritten wird, trifft die Synergis™ Cloud Link-Einheit keine Entscheidung bezüglich des Zutritts und die Tür bleibt gesperrt.

BEMERKUNG: Beim Überschreiten der maximalen Verzögerung wird das Ereignis *Zutritt verweigert* nicht generiert.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > MIFARE DESFire**.
- 3 Wählen Sie im Abschnitt *Lesegeräte und verknüpfte MIFARE-DESFire-Konfigurationen* die Option **Näheprüfung** neben einem oder mehreren OSDP-Lesegeräten aus.
- 4 Geben Sie für jedes Lesegerät mit aktivierter **Näheprüfung** einen Wert in Millisekunden in das Feld **ms** ein, um die maximale Verzögerung für die Kartenauthentifizierung zu definieren.

TIPP: Die Verhinderung von Relaisangriffen wird für jedes Lesegerät einzeln aktiviert. Da sich das Timing jedes Lesegeräts unterscheidet, bestimmen Sie die durchschnittliche Zeit, die ein Lesegerät benötigt, um einen legitimen Ausweis zu authentifizieren, und addieren Sie eine geringe Fehlertoleranz hinzu, um die maximale Verzögerung zu berechnen. Als Fehlertoleranz wird ein Wert von 40 Millisekunden empfohlen.

Um die Authentifizierungsdauer einer Karte zu bestimmen, gehen Sie zu **Wartung > Protokollanzeige**. Wählen Sie im Dropdown-Menü **Logger** die Option **Syslog** aus und geben Sie im Feld **Nach regex filtern** *SmartCard* ein. Prüfen Sie die Authentifizierungszeit in den Protokollen mit dem Präfix *SmartCard*.

- 5 Klicken Sie auf **Speichern**.

Übertragung von Dateien an OSDP-Lesegeräte im Synergis™ Appliance Portal

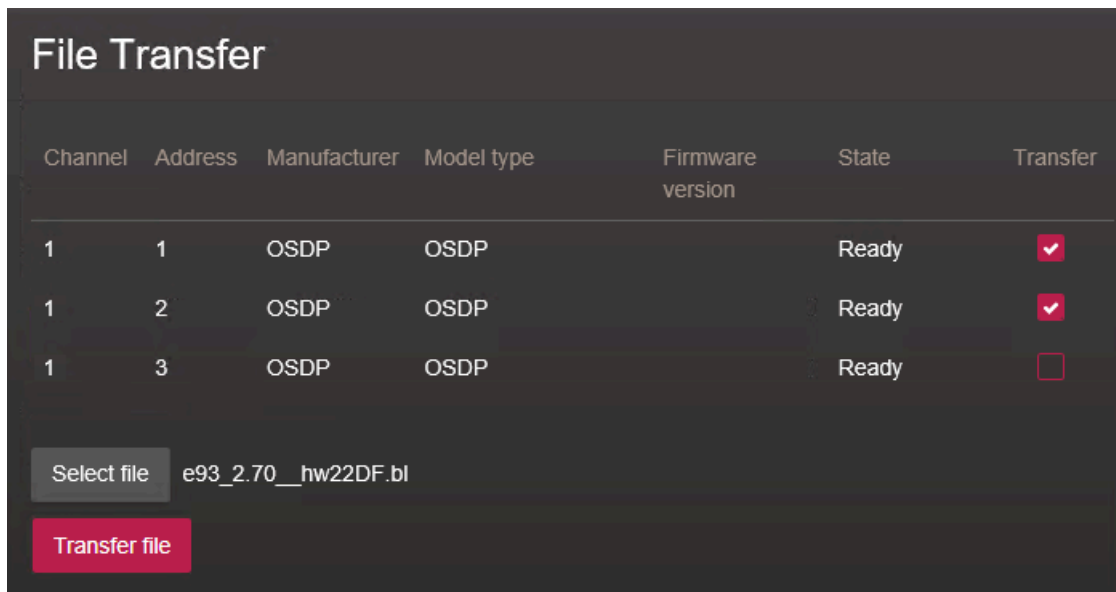
Sie können die Firmware oder Konfiguration von OSDP-Lesegeräten aktualisieren, indem Sie Dateien im Synergis™ Appliance Portal auf die Lesegeräte übertragen.

Was Sie noch wissen sollten

- Das folgende Vorgehen bezieht sich nur auf OSDP-Lesegeräte, die sich direkt mit der Synergis™ Cloud Link-Einheit verbinden.
- Verwenden Sie die Firmware und Konfigurationsdateien, die von Ihrem Hersteller bereitgestellt werden.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Erweitertes OSDP**.
- 3 Wählen Sie im Abschnitt *Dateiübertragung* das Kontrollkästchen in der Spalte **Übertragung** von jenen Lesegeräten aus, zu denen Sie die Datei übertragen möchten.
- 4 Klicken Sie auf **Datei auswählen**.
- 5 Wählen Sie im Dateibrowser die Firmware- oder Konfigurationsdatei aus und klicken Sie auf **Öffnen**.
- 6 Klicken Sie auf **Datei übertragen**.



Die Firmware oder Konfiguration werden angewendet, nachdem die ausgewählten Lesegeräte neu gestartet wurden.

STid-Lesegeräte, die das SSCP-Protokoll verwenden

Dieser Abschnitt enthält die folgenden Themen:

- ["Konfigurieren und Registrieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden"](#) auf Seite 231
- ["Aktivieren des transparenten Modus bei STid-Lesegeräten, die das SSCP-Protokoll verwenden"](#) auf Seite 235
- ["Ändern der Standardkommunikationsschlüssel RS-485 für STid-Lesegeräte, die das SSCP-Protokoll verwenden"](#) auf Seite 238
- ["Konfigurieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden, zur Verhinderung von Relaisangriffen"](#) auf Seite 240
- ["Codierung einer Berechtigung auf einer RFID-Karte in Security Desk"](#) auf Seite 242

Konfigurieren und Registrieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden

Damit die Synergis™-Einheit mit den angeschlossenen STid-Lesegeräten kommunizieren kann, müssen Sie die Lesegeräte im Synergis™ Appliance Portal konfigurieren und registrieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihre STid-Lesegerät-Firmware auf dem neuesten Stand ist und von Synergis™ Software unterstützt wird.

Was Sie noch wissen sollten

Wenn Sie STid-Lesegeräte an benachbarten Drehkreuzen installieren, ist es nicht empfehlenswert, mehr als zwei Lesegeräte an denselben RS-485-Kanal anzuschließen, da sich dadurch die Reaktionszeit des Controllers erhöht und die Wahrscheinlichkeit hoch ist, dass zwei oder mehr Karten gleichzeitig vorgelegt werden. Bei herkömmlichen Türen können Sie bis zu vier Lesegeräte pro Bus installieren.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Hardware**.
- 3 Klicken Sie oben in der Spalte **Hardware** auf **Hinzufügen (+)**.
- 4 Wählen Sie im Dialogfeld *Hardware hinzufügen* die Option **SSCP** als **Hardwaretyp** aus.
- 5 Wählen Sie den **Kanal** aus (1 - 4) .
BEMERKUNG: Wenn Sie die Synergis™ Cloud Link 312-Einheit haben, haben Sie bis zu 12 Kanäle. Weitere Informationen finden Sie unter [Informationen über Ports in Synergis Cloud Link 312 RS-485](#).
- 6 Wählen Sie unter **SSCP-Protokollversion** entweder **V1** oder **V2**, je nachdem, welches Protokoll das Lesegerät unterstützt.

- 7 Stellen Sie **Bits pro Sekunde** und **Physische Adresse** (1 bis 127) ein.

Die Rate **Bits pro Sekunde** ist eine Kanaleigenschaft und folgt der Bitrate des letzten Schnittstellenmoduls, das dem Kanal hinzugefügt wurde. Die Default-Bitrate ist 38.400 bps. Höhere Bitraten verbessern die Lesezeit der Karte auf Kosten der maximalen Kabellänge.

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

- Hardware type: SSCP
- Channel: 2
- Interface module type: W33/W35B
- Bits per second: 38400
- SSCP protocol version: V1
- Physical address: 1

At the bottom of the dialog, there are three buttons: "Scan", "Cancel", and "Save".

- 8 Klicken Sie auf **Hinzufügen**.

Der Anschluss, die Bitrate und die physische Adresse für das Lesegerät werden in Synergis™ Software konfiguriert.

- 9 (Optional) Wenn Sie die Protokollversion **V1** verwenden, wählen Sie einen Kommunikationsmodus aus:
- Wählen Sie das Lesegerät an der von Ihnen konfigurierten Adresse und klicken Sie auf **Bearbeiten** (✎).
 - Wählen Sie in der Liste **Kommunikationsmodus** einen Modus aus:
 - Klartext* (Standardmodus)
 - Verschlüsselt* (verschlüsselte Kommunikation)
 - Signiert* (authentifizierte Kommunikation)
 - Verschlüsselt und signiert* (sowohl private als auch authentifizierte Kommunikation)

BEMERKUNG: Wenn Sie **V2** verwenden, ist nur die Option **Verschlüsselt und signiert** verfügbar.

The screenshot shows a configuration window titled 'SSCP 0' with a 'Configuration' section. It contains three main settings: 'Physical address' set to '0', 'Communication mode' set to 'Encrypted and signed', and 'MIFARE DESFire key location' set to 'Non-transparent reader'. There is a checked checkbox for 'Tamper erases keys'. At the bottom, there are four buttons: 'Set as default', 'Reset to factory settings', 'Cancel', and 'Save'.

Die Option **Manipulation löscht Schlüssel** ist standardmäßig aktiviert und löscht alle integrierten Schlüssel, wenn die Einheit manipuliert wird.

- Klicken Sie auf **Speichern**.
- Wählen Sie in der Hardwarestruktur die von Ihnen konfigurierte Schnittstelle aus und klicken Sie auf **Bearbeiten** (✎).
 - Aktivieren Sie in dem sich öffnenden Dialogfeld das Kontrollkästchen **Programmiermodus** und klicken Sie auf **Speichern**.
Das System programmiert das Lesegerät mit Ihrer physischen Adresse und Bitratenkonfiguration.
 - Wählen Sie die Schnittstelle aus und klicken Sie auf **Bearbeiten** (✎).
 - Deaktivieren Sie das Kontrollkästchen **Programmiermodus** und klicken Sie auf **Speichern**.
 - Wiederholen Sie den Vorgang, um die verbleibenden Lesegeräte nacheinander hinzuzufügen, und zwar ein Lesegerät pro Anschluss.
BEMERKUNG: Wenn Sie mehrere Lesegeräte zu einem Anschluss hinzufügen, verwenden Sie einen freien Anschluss, um sie einzeln zu konfigurieren, bevor Sie sie mit ihrem Zielanschluss verbinden.
 - Testen Sie die Verbindung und Konfiguration Ihres Schnittstellenmoduls auf der Seite [E/A-Diagnose](#).

Nach Durchführen dieser Schritte

BEST-PRACTICE: *(Härtung)* Die Änderung der vom Hersteller bereitgestellten Standardverschlüsselungsschlüssel erhöht die Sicherheit.

Aktivieren des transparenten Modus bei STid-Lesegeräten, die das SSCP-Protokoll verwenden

MIFARE-DESFire-Lesegeräte erfordern kryptografische Schlüssel, um auf die gesicherte Berechtigung einer Karte zuzugreifen. Wenn die Lesegeräte für den transparenten Modus konfiguriert sind, werden diese Schlüssel in den Synergis™ key store oder eine SAM-Karte (Secure Access Module) geladen.

Bevor Sie beginnen

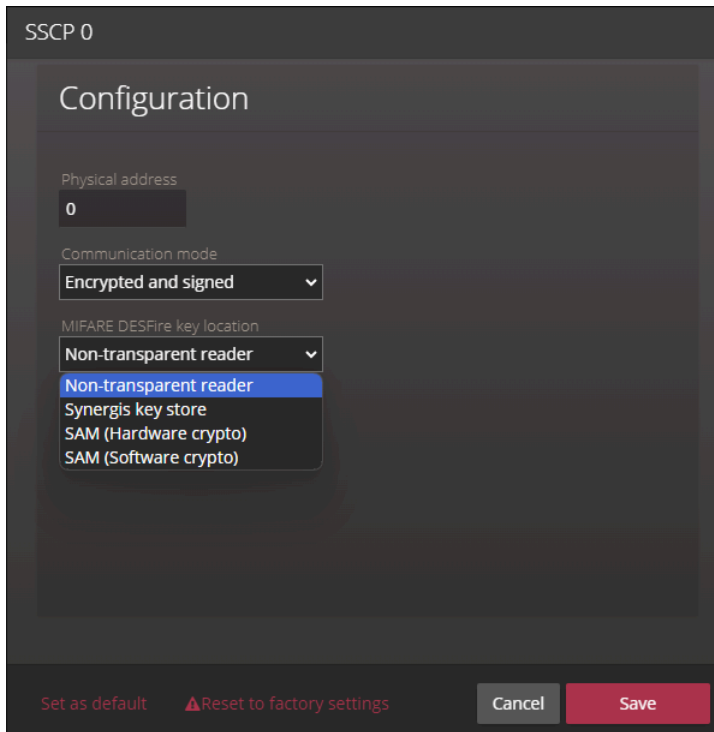
Die Tür muss mit einem STid-Lesegerät ausgestattet sein, dessen Teilenummer auf AA oder AD endet.

BEMERKUNG: Transparente STid-Lesegeräte mit Teilenummern, die auf BB enden, können in diesem Szenario nicht verwendet werden. Eine Liste der Lesegeräte, die als transparente Lesegeräte verwendet werden können, finden Sie unter [Unterstützte STid-Lesegeräte, die das SSCP-Protokoll verwenden](#).

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Konfiguration** > **Hardware** und wählen dann **SSCP** aus.
- 3 Klicken Sie auf **Bearbeiten** (✎) für die Schnittstelle des Lesegeräts.

- 4 Wählen Sie im Dialogfeld für die Lesegerätkonfiguration in der Liste **MIFARE DESFire-Schlüsselort** eine der folgenden Optionen aus:



- **Synergis key store:** The key for decrypting credentials is stored on the Synergis unit. This option does not require a SAM card.
- **SAM (Software crypto):** This is the faster of the SAM options, but requires the **SessionDumpKey** option to be enabled during the SAM configuration process. For more information, see the documentation that came with your SAM card configuration software.
- **SAM (Hardware crypto):** This option does not require **SessionDumpKey** to be enabled during the SAM configuration process.

BEMERKUNG: Die SAM-Optionen sind nur verfügbar, wenn Sie das Synergis™ Cloud Link-312-Modell haben.

- 5 Wenn Sie die Option **Synergis™-Schlüsselspeicher** wählen, verwenden Sie das Synergis™ Appliance Portal, um auf den Synergis™-Schlüsselspeicher zuzugreifen und die Schlüssel einzugeben:
- Wählen Sie einen Index aus.
 - Klicken Sie auf **Neue Version erstellen** und geben Sie einen 32-stelligen hexadezimalen Schlüssel in das Textfeld ein.
 - Klicken Sie auf **Hinzufügen**.

Die MIFARE-DESFire-Konfigurationsdatei, die für indizierte Schlüssel verwendet wird, ist mit softwaretransparenten und nicht transparenten STid-Lesegeräten kompatibel.

Einschränkungen: Es gibt zwei Einschränkungen bei softwaretransparenten Lesegeräten:

- Transparente Lesegeräte können derzeit keine Karten codieren.
- Karten mit aktiviertem transparenten Modus benötigen ca.100 ms länger, um gelesen zu werden.

Nach Durchführen dieser Schritte

Die 32 verfügbaren indizierten Schlüssel im Synergis™ key store erhöhen die Sicherheit, indem sie die Eingabe von Schlüsseln in Komponenten ermöglichen. Durch Klicken auf **Hinzufügen** zwischen den Komponenten ist es möglich, dass mehrere Beteiligte jeweils nur einen Teil des erforderlichen Schlüssels kennen.

Verwandte Themen

[Informationen zu Synergis™ Cloud Link 312 auf Seite 6](#)

Ändern der Standardkommunikationsschlüssel RS-485 für STid-Lesegeräte, die das SSCP-Protokoll verwenden

Sie können die standardmäßigen Signatur- und Verschlüsselungsschlüssel ändern, die für die verschlüsselte und signierte Kommunikation mit den STid-Lesegeräten verwendet werden.

Bevor Sie beginnen

Ändern Sie die werkseitig installierten *Signatur-* und *Verschlüsselungsschlüssel* für mehr Sicherheit.

Was Sie noch wissen sollten

Das Ändern der Default-Signatur- und Verschlüsselungsschlüssel beinhaltet das Ändern der Werte für die RS-485-Schlüssel *ReaderKs* und *ReaderKc* auf dem Lesegerät und auf der Seite *Synergis™-Schlüsselspeicher* im Synergis™ Appliance Portal. Das STid-Lesegerät bietet auch die Möglichkeit, die Schlüssel in einem der integrierten Schlüsselverzeichnisse zu speichern.

SSCP V2-Lesegeräte verwenden nur den Schlüssel *ReaderKc*.

BEMERKUNG: Wird bei der Verwendung von indizierten Schlüsseln ein STid-Lesegerät manipuliert, geht die Tür im Config Tool offline, und die LED des Lesegeräts blinkt orange. In diesem Fall legen Sie die SKB-Karte vor, um die RS-485-Schlüssel in das Lesegerät zu laden. Wenn die Schlüssel geladen sind, geht das Lesegerät wieder online (die LED leuchtet rot).

Prozedur

- 1 Melden Sie sich an der Synergis-Einheit an.
- 2 Klicken Sie auf **Konfiguration > Synergis-Schlüsselspeicher**.
- 3 Wenden Sie die neuen Verschlüsselungswerte an, *ReaderKc* für den Verschlüsselungsschlüssel und *ReaderKs* für den Signaturschlüssel.
- 4 Konfigurieren Sie die Schlüssel:
 - a) Klicken Sie auf **Konfiguration > Hardware** und wählen dann **SSCP** aus.
 - b) Klicken Sie auf **Bearbeiten** (✎) auf dem Kanal des Lesegeräts.
 - c) Wenn die Schlüssel *ReaderKc* und *ReaderKs* am Lesegerät konfiguriert wurden, lassen Sie die Kontrollkästchen **Verwenden Sie indizierte Verschlüsselungsschlüssel (Kc) auf allen Lesegeräten** und **Verwenden Sie indizierte Signaturschlüssel (Ks) auf allen Lesegeräten** deaktiviert. Wenn das Lesegerät indizierte Signatur- und Verschlüsselungsschlüssel verwendet, aktivieren Sie die Kontrollkästchen **Verwenden Sie indizierte Verschlüsselungsschlüssel (Kc) auf allen Lesegeräten**

und **Verwenden Sie indizierte Signaturschlüssel (Ks) auf allen Lesegeräten** und geben Sie dann die richtigen Werte für die Schlüsselindizes ein.

SSCP 1

SSCP protocol version
V1

Bits per second
38400

Programming mode

Use indexed encryption key (Kc) on all readers

Reader key index
0

Use indexed signature key (Ks) on all readers

Reader key index
0

Cancel Save

- 5 Bei Lesegeräten, die indizierte Schlüssel verwenden, legen Sie die SKB-Karte vor, um die RS-485-Schlüssel in das Lesegerät zu laden.

Konfigurieren von STid-Lesegeräten, die das SSCP-Protokoll verwenden, zur Verhinderung von Relaisangriffen

Verhindern Sie Relaisangriffe auf unterstützten STid-Lesegeräten, indem Sie das System Verzögerungen bei der HF-Kommunikation zwischen Karten und Lesegeräten erkennen lassen und Zutrittsanforderungen von Karten zurückweisen, bei denen die Kommunikation zu lange dauert.

Bevor Sie beginnen

- Dieses Verfahren gilt nur für STid-Lesegeräte, die das SSCP- oder SSCP V2-Protokoll und Firmware v21 oder höher verwenden.
- [Aktivieren Sie sichere Nachrichten mit DESFire EV2.](#)

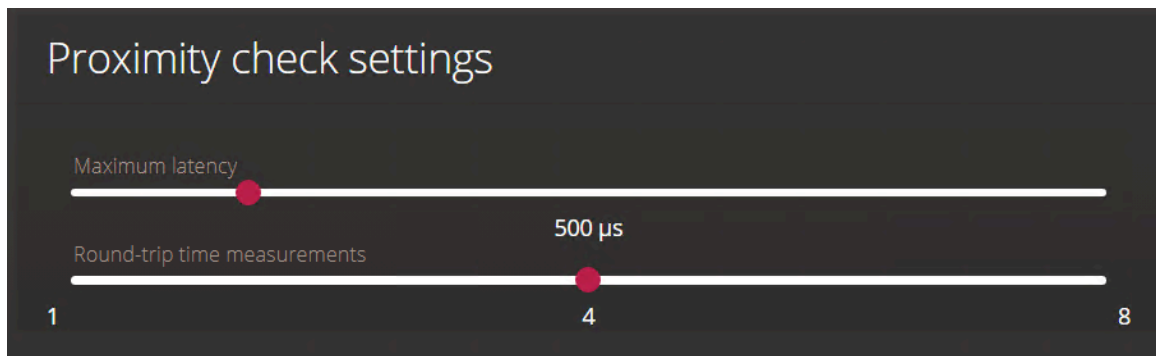
Was Sie noch wissen sollten

Bei einem Relaisangriff werden anhand von zwei schädlichen Geräten Nachrichten zwischen einem Lesegerät und einer Karte übermittelt. So können Angreifer Türen öffnen, ohne dass die Karte physisch an die Nähe des Lesegeräts gehalten werden muss. In solchen Fällen dauert die Authentifizierung einer Karte länger als gewöhnlich, da die Angreifer dazwischen Nachrichten aneinander übermitteln müssen.

Eine Näheprüfung für STid-Lesegeräte sorgt dafür, dass nur Zutrittsanforderungen von Karten erlaubt werden, die innerhalb einer konfigurierten Zeitspanne erfolgen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Konfiguration > MIFARE DESFire.**
- 3 Wählen Sie im Abschnitt *Lesegeräte und verknüpfte MIFARE-DESFire-Konfigurationen* die Option **Näheprüfung** neben einem oder mehreren STid-Lesegeräten aus.
- 4 (Optional) Konfigurieren Sie im Abschnitt *Einstellungen der Näheprüfung* Folgendes:
BERMerkung: Es wird empfohlen, die Standardeinstellungen beizubehalten. Wenn Sie die maximale Latenz verringern, kann es passieren, dass bestimmte Karten die Näheprüfung nicht bestehen. Eine Erhöhung der maximalen Latenz kann eventuell einen Relaisangriff erleichtern.



- **Maximale Latenz:** Der Schwellenwert für den Austausch zwischen der Karte und dem Lesegerät in Mikrosekunden. Der Standardwert beträgt 500 Mikrosekunden.
- **Messungen der Roundtrip-Zeit:** Gibt an, wie oft die Austauschaktivitäten zwischen dem Lesegerät und der Karte gemessen werden, um zu berechnen, ob die gelesene Karte gültig ist. Jeder Austausch muss unter dem konfigurierten Wert für **Maximale Latenz** liegen.

5 Klicken Sie auf **Speichern**.

Wenn der Wert für **Messungen der Roundtrip-Zeit** auf 4 gesetzt ist und ein Lesegerät mit aktivierter **Näheprüfung** eine Zutrittsanforderung erhält, wird eine Näheprüfung ausgeführt, entsprechend der Konfiguration im Abschnitt *Einstellungen der Näheprüfung*. Die Näheprüfung berechnet die Dauer eines Austauschs zwischen der Karte und dem Lesegerät viermal.

Die Näheprüfung hat eines der folgenden Ergebnisse:

- Wenn die berechnete Zeit für jeden der vier Austauschaktivitäten unter dem Wert für **Maximale Latenz** liegt, besteht die Karte die Näheprüfung. Die Synergis™ Cloud Link -Einheit gewährt oder verweigert den Zutritt basierend auf den Zutrittsrechten der Karte und die Tür wird entsprechend entsperrt oder nicht.
- Wenn mindestens eine der Austauschaktivitäten den Wert für **Maximale Latenz** übersteigt, besteht die Karte die Näheprüfung nicht. Die Synergis™ Cloud Link -Einheit trifft keine Entscheidung bezüglich des Zutritts und die Tür bleibt gesperrt.

BEMERKUNG: Wenn eine Näheprüfung nicht erfolgreich verläuft, wird das Ereignis *Zutritt verweigert* nicht generiert.

Codierung einer Berechtigung auf einer RFID-Karte in Security Desk

Sie können eine Berechtigung auf einer RFID-Karte mit Security Desk codieren.

Was Sie noch wissen sollten

STid-USB-Codierlesegeräte werden von Security Desk gesteuert. Weitere Informationen finden Sie unter [Externe Zutrittskontrollgeräte aktivieren](#).

Teil IV

Wartung und Fehlerbehebung

Dieser Teil enthält die folgenden Kapitel:

- Kapitel 18, "[Wartung und Fehlersuche bei Synergis™ Cloud Link-Einheiten](#)" auf Seite 244

Wartung und Fehlersuche bei Synergis™ Cloud Link-Einheiten

Dieser Abschnitt enthält die folgenden Themen:

- ["Systeminformationen auf der Synergis™ Cloud Link-Einheit anzeigen"](#) auf Seite 245
- ["Anmeldepasswort der Synergis™ Cloud Link-Appliance ändern"](#) auf Seite 247
- ["Synergis™ Cloud Link -Benutzerprüfungen"](#) auf Seite 248
- ["Gerätekonfigurationsdatei von Ihrer Synergis Cloud Link-Einheit herunterladen"](#) auf Seite 249
- ["Konfigurationsdatei für Ihre Synergis Cloud Link-Einheit hochladen"](#) auf Seite 250
- [" Informationen über die Seite „Kapazitätsbericht“ "](#) auf Seite 252
- ["Herunterladen von Supportinformationen für Ihre Synergis™ Cloud Link -Einheit"](#) auf Seite 254
- ["Schnittstellenmodule über das Synergis Appliance Portal anpingen"](#) auf Seite 255
- ["Firmware der Synergis™ Cloud Link aktualisieren"](#) auf Seite 256
- ["Zurücksetzen der Synergis™ Cloud Link -Einheit nach einer Firmware-Aktualisierung"](#) auf Seite 257
- ["Aktualisieren der Schnittstellenmodul-Firmware über das Synergis™ Appliance Portal"](#) auf Seite 258
- ["Nachgeschaltete Geräte, die für Upgrades über das Synergis™ Appliance Portal unterstützt werden"](#) auf Seite 260
- ["Speicher auf der Synergis™ Cloud Link Appliance bereinigen"](#) auf Seite 261
- ["Peer-to-Peer-Information auf der Synergis™ Cloud Link -Einheit anzeigen unit"](#) auf Seite 263
- ["Informationen zum Diagnosedienstkonto von Synergis™ Cloud Link "](#) auf Seite 265
- ["Hardware oder Software der Synergis™ Cloud Link-Einheit neu starten"](#) auf Seite 267

Systeminformationen auf der Synergis™ Cloud Link-Einheit anzeigen

Sie können den Status und die Konfigurationsdateien der Synergis™ Cloud Link-Einheit zur Fehlerbehebung anzeigen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Wartung** > **Systemstatus**.
- 3 Klicken Sie auf **Einheit**, um die Hardware- und Firmwareinformationen der Einheit anzuzeigen.
- 4 Klicken Sie auf **Netzwerk**, um die Netzwerkkonfiguration und den Status der Einheit anzuzeigen.

Nach Durchführen dieser Schritte

Laden Sie die Konfigurationsdateien der Einheit herunter.

Informationen zur Synergis™ Cloud Link-Einheit

Auf der Registerkarte *Einheit* auf der Seite *Systemstatus* des Synergis™ Appliance Portals werden Informationen zur Hardware und Firmware der Synergis™-Cloud-Link-Einheit angezeigt.

Eigenschaftsname	Eigenschaftswert
Hostname	Hostname der Synergis™ Cloud Link-Einheit. Den Standardhostnamen bilden die Buchstaben „SCL“ (Synergis™ Cloud Link), gefolgt von der MAC-Adresse der Einheit. Die MAC-Adresse ist die erste Adresse auf dem Etikettenaufkleber auf der Einheit. Wenn auf dem Etikett beispielsweise 0010F32CF482 steht, lautet der Standardhostname SCL0010F32CF482.
Hardwaretyp	Genetec Synergis Appliance.
Produkttyp	Synergis™ Cloud Link G2
Firmwareversion	Die Version der auf der Einheit ausgeführten Synergis™ Cloud Link-Firmware.
Synergis-Software-Version	Die Version von Synergis™ Software, die mit der Synergis™ Cloud Link-Firmware gebündelt ist.
Build-Datum	Das Datum, an dem die Firmware hergestellt wurde.
Upgrade-Datum	Das Datum, an dem die Firmware auf die aktuelle Version aktualisiert wurde.
RAM	Der verwendete RAM und der gesamte RAM.
Massenspeicher	Der verwendete Massenspeicher und der Gesamtmassenspeicher.
Interne Temperatur	Die interne Temperatur der Einheit. Wenn die oberen und unteren Temperaturgrenzwerte überschritten werden, wird dieser Wert rot und in den Portalbenachrichtigungen wird eine Warnung angezeigt. Weitere Informationen finden Sie unter Synergis Cloud Link – Spezifikatione .

Eigenschaftsname	Eigenschaftswert
RTC-Batteriespannung	Der RTC-Batteriestand in Volt. Wenn der untere Grenzwert unterschritten wird, wird eine Warnung in den Portalbenachrichtigungen und im Security Center angezeigt.
Stromquelle	Die Stromquelle der Einheit.
Laufzeitumgebung	Frameworkversion der installierten Software.
Erkennungspport	Der Erkennungspport, der von den Access Manager-Rollen für die Kommunikation mit dieser Synergis™ Cloud Link-Einheit verwendet wird. BEMERKUNG: Die IP-Adresse des Access Manager muss auch der Synergis™-Einheit bekannt sein, damit eine Kommunikation zwischen beiden stattfinden kann.
Systembetriebszeit	Seit dem letzten Neustart der Hardware verstrichene Zeit.
Servicebetriebszeit	Seit dem letzten Neustart der Software verstrichene Zeit.
Aktuell verbundener Access Manager	IP-Adresse des Access Manager, der dieses Gerät verwaltet.
Offline-Protokollanzahl	Anzahl der protokollierten Ereignisse, die noch nicht mit der Access Manager-Rolle synchronisiert wurden, wenn die Einheit offline ist. Zeigt Null an, wenn die Einheit online ist. BEMERKUNG: Dies sind allgemeine Ereignisse, die dem Access Manager gemeldet werden. Sie sollten nicht mit den Fehlerbehebungsprotokollen der Synergis™ Cloud Link-Einheit verwechselt werden.
Anzahl von konfigurierten Kanälen	Anzahl der Kommunikationskanäle, die mit angeschlossenen Schnittstellenmodulen konfiguriert wurden. Die Synergis™ Cloud Link-Einheit verfügt über zwei Arten von Kanälen: IP und RS-485.
Seriennummer	Die Seriennummer der Einheit.
Die Anzahl von Peers, die mit dieser Einheit verbunden sind	Die Anzahl von Synergis™ Cloud Link-Einheiten, die mit der Einheit als Peers verbunden sind.

Anmeldepasswort der Synergis™ Cloud Link-Appliance ändern

Als bewährtes Sicherheitsverfahren sollte das Anmeldepasswort für die Synergis™ Cloud Link-Appliance regelmäßig geändert werden.

Was Sie noch wissen sollten

- Das neue Passwort muss mindestens 15 Zeichen lang, eindeutig und zufällig sein. Die Schaltfläche **Speichern** wird erst angezeigt, wenn das System die Stärke des Passworts als *Stark* oder *Sehr stark* erachtet.
- Wenn die Synergis Cloud Link-Appliance bereits in Security Center registriert wurde, wird empfohlen, das Passwort mithilfe des Tasks *Hardwareinventar* in Config Tool und nicht im Synergis™ Appliance Portal zu ändern. Security Center 5.10.1 ist die erforderliche Mindestversion dafür.

Weitere Informationen finden Sie unter [Passwörter für Zutrittskontrollereinheiten in Config Tool ändern](#).

Prozedur

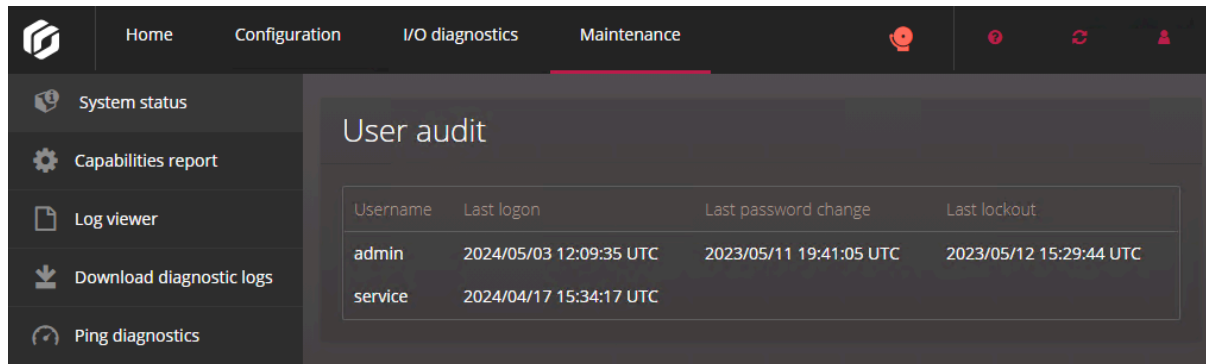
- 1 Melden Sie sich bei der Synergis Cloud Link-Appliance an.
- 2 Klicken Sie auf **Konfiguration > Benutzer**.
- 3 Wählen Sie auf der Seite *Benutzerkonfiguration* einen Benutzer aus.
- 4 Geben Sie das alte Passwort ein, geben Sie dann das neue Passwort ein und bestätigen Sie es.
- 5 Klicken Sie auf **Speichern**.
- 6 Bei Appliances, die bereits in Security Center registriert wurden, ändern Sie das Passwort in Config Tool, um [die Appliance mit der verbundenen Access Manager-Rolle zu synchronisieren](#).

Das neue Passwort wird sofort angewendet.

Synergis™ Cloud Link -Benutzerprüfungen

Um die Aktivität von Benutzern im Synergis™ Appliance Portal zu untersuchen, können Sie anzeigen lassen, wann sich Benutzer zuletzt bei der Synergis™ Cloud Link -Einheit angemeldet haben, wann zuletzt ihr Passwort geändert wurde und wann sie zuletzt nach drei fehlgeschlagenen Anmeldeversuchen gesperrt wurden.

Navigieren Sie zu **Wartung > Systemstatus**, um den Abschnitt *Benutzerprüfung* aufzurufen. Alle Zeitstempel für Benutzeraktivität werden in UTC angegeben.



Username	Last logon	Last password change	Last lockout
admin	2024/05/03 12:09:35 UTC	2023/05/11 19:41:05 UTC	2023/05/12 15:29:44 UTC
service	2024/04/17 15:34:17 UTC		

Gerätekonfigurationsdatei von Ihrer Synergis Cloud Link-Einheit herunterladen

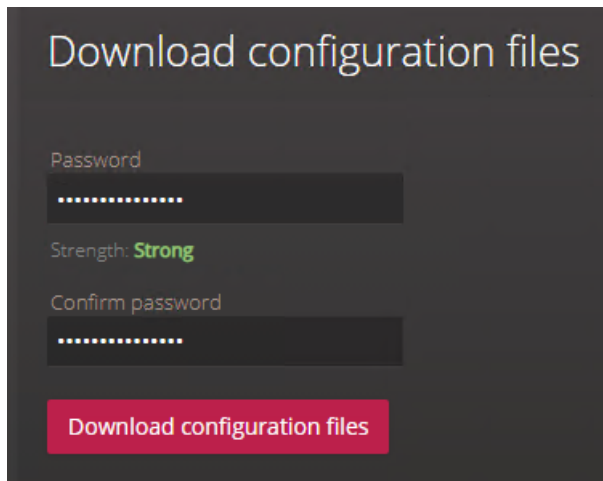
Sie können die Konfiguration Ihrer Synergis™ Cloud Link-Einheit als komprimierte Datei herunterladen, um die Konfiguration während des Austauschs einer Einheit auf der anderen Einheit wiederherzustellen.

Was Sie noch wissen sollten

Die Konfigurationsdatei enthält Hardware-Einstellungen, einschließlich überwachter Eingangswerte und RIO, sowie Automatisierungs-Engine-Regeln. Die Datei enthält nicht das Administratorpasswort der Einheit und keine Synergis-Schlüsselspeicherdaten.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Wartung > Systemstatus**.
- 3 Geben Sie im Abschnitt *Konfigurationsdateien herunterladen* ein starkes Passwort ein und bestätigen Sie es.
BEMERKUNG: Das Passwort muss mindestens 15 Zeichen lang sein.



The screenshot shows a dark-themed dialog box titled "Download configuration files". It contains two password input fields, both filled with dots. The first field is labeled "Password" and has a strength indicator below it that says "Strength: Strong" in green text. The second field is labeled "Confirm password". At the bottom of the dialog is a red button with the text "Download configuration files".

- 4 Klicken Sie auf **Konfigurationsdateien herunterladen**.
BEMERKUNG: Diese Taste bleibt deaktiviert, wenn das Passwort nicht stark genug ist oder wenn die Passwortbestätigung nicht übereinstimmt.
- 5 Klicken Sie auf **Speichern**.

Konfigurationsdatei für Ihre Synergis Cloud Link-Einheit hochladen

Wenn Sie eine Synergis™ Cloud Link-Einheit austauschen, können Sie die Konfigurationsdatei der alten Einheit herunterladen und dann auf die Ersatzeinheit hochladen, um die Konfiguration wiederherzustellen.

Bevor Sie beginnen

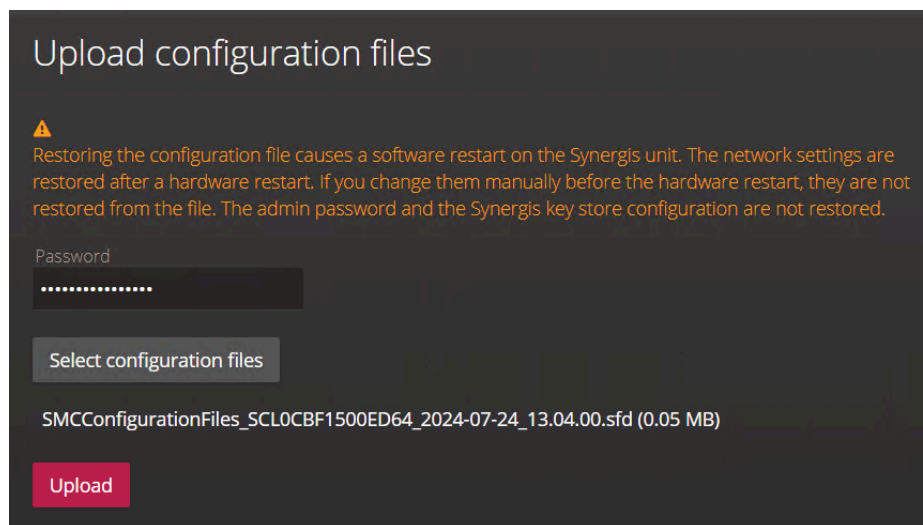
Laden Sie die Konfigurationsdateien der Synergis-Cloud-Link-Einheit herunter.

Was Sie noch wissen sollten

Die Konfigurationsdatei enthält Hardware-Einstellungen, einschließlich überwachter Eingangswerte und RIO, sowie Automatisierungs-Engine-Regeln. Die Datei enthält nicht das Administratorpasswort der Einheit und keine Synergis-Schlüsselspeicherdaten.

Prozedur

- 1 Melden Sie sich an der Synergis Cloud Link-Einheit an.
- 2 Klicken Sie auf **Wartung** > **Systemstatus**.
- 3 Klicken Sie im Abschnitt *Konfigurationsdateien hochladen* auf **Konfigurationsdateien auswählen**.
- 4 Navigieren Sie zu dem heruntergeladenen Konfigurationspaket auf Ihrem lokalen Laufwerk und klicken Sie auf **Öffnen**.
- 5 Wenn Sie beim Herunterladen der Konfigurationsdatei ein Passwort festgelegt haben, geben Sie es in das Feld **Passwort** ein.
- 6 Klicken Sie auf **Hochladen**.



Das Konfigurationspaket wird hochgeladen und die Synergis Cloud Link-Einheit wird neu gestartet.

Nach Durchführen dieser Schritte

- Konfigurieren Sie das Administratorpasswort und die Synergis-Schlüsselspeicherkonfiguration manuell neu, da sie nicht in der Konfigurationsdatei enthalten sind.

- Um die Netzwerkeinstellungen aus der Konfigurationsdatei wiederherzustellen, starten Sie die Hardware neu.

Informationen über die Seite „Kapazitätsbericht“

Zur Erleichterung der Fehlersuche bei Problemen mit den in Ihrem System registrierten Mercury -Controllern können Sie die Seite *Fähigkeitsbericht* im Synergis™ Appliance Portal hinzuziehen. Auf dieser Seite erhalten Sie einen Überblick über den Status, die Nutzung der Funktionen und die Ereignisprotokolle für jeden Ihrer Controller.

The screenshot shows the 'Units' page for a Mercury LP1502 controller. The page is divided into several sections:

- Units Summary:** Shows 'Over capacity (0)' and 'Offline (0)'. A list of units is shown under 'All units (1)', with one unit 'Mercury LP1502 10.23.75.51:3018' listed. A 'Refresh' button is at the top right, and a 'Download' button is at the bottom right.
- Controller Details:** Shows the controller name 'Mercury LP1502 10.23.75.51:3018', 'Last refresh time: 2022/02/01 17:09:13 UTC', and 'Firmware version: 1.30.1'.
- Usage Statistics Table:**

Field	Usage
Access control readers	4/64
Access levels	0/16000
Areas	0/127
Card formats	8/8
Control points	10/2048
Credentials	0/200000
Elevator access levels	0/255
Monitor point groups	0/128
Monitor points	16/2048
Procedures	0/7000
SIO port 1	1/32
Timezones	0/255
Triggers	0/7000
Zones	0/42
- Event logs:** Shows a log entry for 'Card formats' with a timestamp of '2022/02/01 17:06:36 UTC' and a status of 'Limit reached (8/8)'.

Auf die Seite *Fähigkeitenbericht* können nur Benutzer mit Administratorrechten zugreifen. Die Seite ist in die folgenden Abschnitte unterteilt:

- **Einheiten:** Listet alle Mercury-Controller auf, die an der Synergis™ Cloud Link-Einheit angemeldet sind. Dieser Bereich muss manuell aufgefrischt werden. Sie können die Controller in drei verschiedenen Ansichten betrachten:
 - Kapazitätsüberschreitung
 - Offline
 - Alle Einheiten

Wenn Sie eine Einheit auswählen, werden der Abschnitt „Funktionen“ und der Abschnitt *Ereignisprotokolle* für diese Einheit angezeigt. Durch Anklicken von **Download** wird eine CSV-Datei erzeugt, welche die aufgelisteten Einheiten mit ihrer aktuellen Kapazitätsnutzung enthält.

- **Abschnitt Funktionen für die ausgewählte Einheit:** Dieser Abschnitt wird nach der im Abschnitt *Einheiten* ausgewählten Einheit benannt. Er zeigt die folgenden Informationen an:
 - **Letzte Aktualisierungszeit:** Der Zeitstempel, wann die Daten zuletzt abgerufen wurden.
 - **Firmwareversion:** Die Firmwareversion der Einheit.
 - **Funktionen:** Eine Tabelle, in der alle unterstützten Fähigkeiten des Geräts und die aktuelle Verwendung für jede Fähigkeit aufgeführt sind. Zum Beispiel bedeutet 2/64 in der Zeile *Zutrittskontrolllesegeräte*, dass das Gerät bis zu 62 weitere Lesegeräte unterstützen kann. Wenn Sie den Mauszeiger über das Symbol ⓘ neben jeder Funktion bewegen, werden die entsprechende Security Center-Konzepte angezeigt.
Die Verwendungswerte sind wie folgt farblich codiert:
 - Rot bedeutet Kapazitätsüberschreitung.
BEMERKUNG: Wenn Hardware zurückgesetzt wird, während die Kapazitäten überschritten werden, funktionieren die Offline-Türfunktionen und OSDP-Lesevorgänge nicht, solange die Kapazitäten überschritten werden.
 - Orange bedeutet, dass die Kapazität erreicht ist.
 - Grün bedeutet, dass die Kapazität unterschritten wird.
- **Ereignisprotokolle:** Listet die 10 jüngsten kritischen Ereignisse für die ausgewählte Einheit seit dem letzten Start der Firmware auf, z. B. wenn das Limit einer Fähigkeit erreicht oder überschritten wird.

Herunterladen von Supportinformationen für Ihre Synergis™ Cloud Link -Einheit

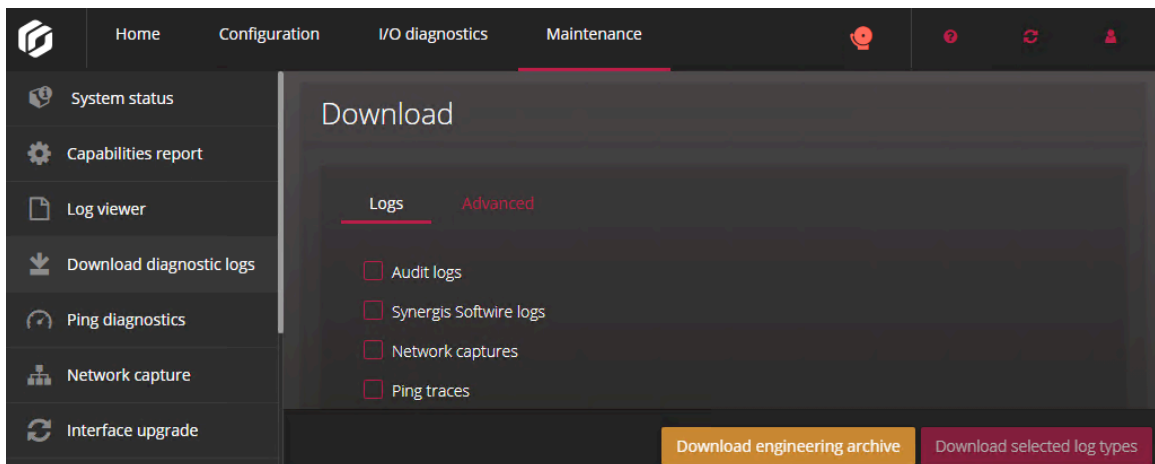
Um die Fehlersuche an Ihrer Synergis™ Cloud Link -Einheit zu vereinfachen, können Sie eine einzige Datei mit allen Informationen, die Sie für den technischen Support von Genetec™ benötigen, vom Synergis™ Appliance Portal herunterladen.

Was Sie noch wissen sollten

Bei der Engineering-Archivdatei handelt es sich um eine verschlüsselte .gen-Datei, die nur der Genetec Technical Support entschlüsseln kann. Die Archivdatei enthält alle Protokolle und eine Sicherung der Konfiguration der Einheit.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Wartung > Diagnostikprotokolle herunterladen**.
- 3 Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie auf **Engineering-Archiv herunterladen**.
 - Wählen Sie im Abschnitt *Protokolle* bestimmte Protokollkategorien zum Herunterladen aus und klicken Sie dann auf **Ausgewählte Protokolltypen herunterladen**.
 - Klicken Sie auf die Registerkarte **Erweitert**, klappen Sie die Kategorien aus und wählen Sie bestimmte Protokolle zum Herunterladen aus. Klicken Sie dann auf **Ausgewählte Protokolldateien herunterladen**.



Die Datei wird heruntergeladen.

- 4 Speichern Sie die Datei, um sie dem Genetec Technical Support zu übermitteln.

Schnittstellenmodule über das Synergis Appliance Portal anpingen

Sie können Schnittstellenmodule und ihre nachgeschalteten Schnittstellen über das Synergis™ Appliance Portal anpingen, um zu überprüfen, ob die Installation Ihrer Einheit erfolgreich war, oder um Netzwerk- oder Paketverlustprobleme zu beheben.

Was Sie noch wissen sollten

- Sie können zwei Arten von Pings über das Portal ausführen:
 - **Kurzer Ping:** Dauert weniger als 10 Sekunden. Die Ergebnisse werden unter der ausgewählten Einheit angezeigt.
 - **Langzeit-Ping:** Pingt jede Sekunde für eine ausgewählte Dauer. Es können mehrere Schnittstellenmodule gleichzeitig angepingt werden. Eine tar.gz-Datei mit den Ergebnissen des Pingvorgangs kann von der Seite *Diagnostikprotokolle herunterladen* des Portals heruntergeladen werden.
- ASSA-ABLOY- und RIO-Einheiten können nicht angepingt werden.
- Synergis™ IX-Geräte benötigen Firmware 4.00_1143_M036 oder höher, um pingfähig zu sein.
- Je nach Firewall-Einstellungen funktioniert das Pinggen möglicherweise nicht.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Klicken Sie auf **Wartung > Ping-Diagnostik**.
Eine Liste aller Schnittstellenmodule und nachgeschalteten Schnittstellen, die an Ihre Synergis™ Cloud Link-Einheit angeschlossen sind, wird angezeigt.
- 3 So starten Sie einen Ping:
 - Für einen kurzen Ping: Wählen Sie ein Schnittstellenmodul aus und klicken Sie dann auf **Ping**.
 - Für einen langen Ping: Wählen Sie ein oder mehrere Schnittstellenmodule aus, wählen Sie eine **Ping-Langzeitdauer** aus und klicken Sie dann auf **Ping starten**.

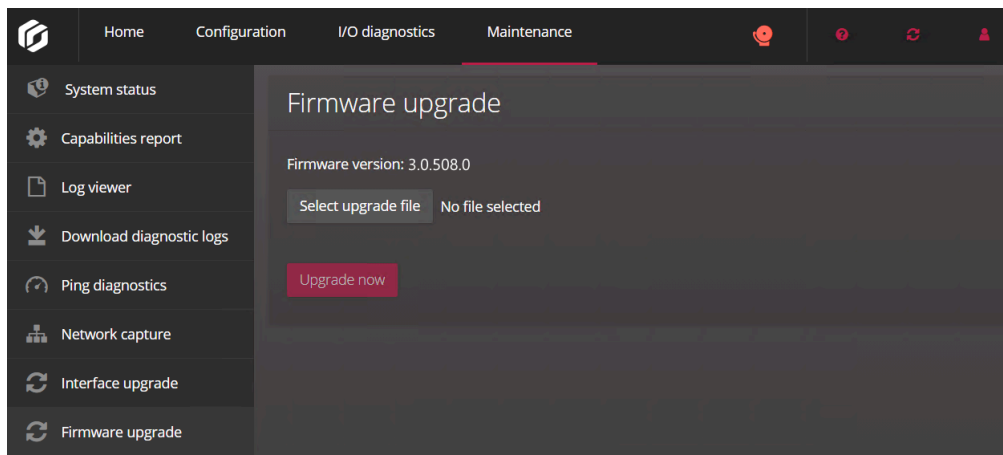
Die Ergebnisse des kurzen Pingvorgangs werden unter dem von Ihnen angepingten Schnittstellenmodul aufgelistet. Die Langzeit-Ping-Ergebnisse sind auf der Seite *Diagnostikprotokolle herunterladen* verfügbar.

Firmware der Synergis™ Cloud Link aktualisieren

Um sicherzustellen, dass Sie über die neuesten Sicherheits-Patches und Verbesserungen verfügen, halten Sie Ihre Synergis™-Cloud-Link-Einheit mit der neuesten Firmwareversion auf dem neuesten Stand.

Prozedur

- 1 Laden Sie die neueste Firmware auf der [GTAP-Seite Produktdownload](#) herunter:
 - a) Wählen Sie in der Liste **Download Finder** die Option **Synergis™ Cloud Link** aus, und suchen Sie dann nach Ihrer Firmware.
 - b) Speichern Sie die *.sfw*-Datei auf Ihrem lokalen Datenträger.
- 2 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 3 Klicken Sie auf **Wartung > Firmware-Upgrade**.



- 4 Klicken Sie auf **Upgrade-Datei auswählen**.
- 5 Wählen Sie im folgenden Dateibrowser die *.sfw*-Firmwaredatei aus und klicken Sie auf **Öffnen**.
- 6 Klicken Sie auf **Jetzt aktualisieren**.

Das Upgrade kann einige Minuten in Anspruch nehmen – danach wird die Einheit neu gestartet.

Zurücksetzen der Synergis™ Cloud Link -Einheit nach einer Firmware-Aktualisierung

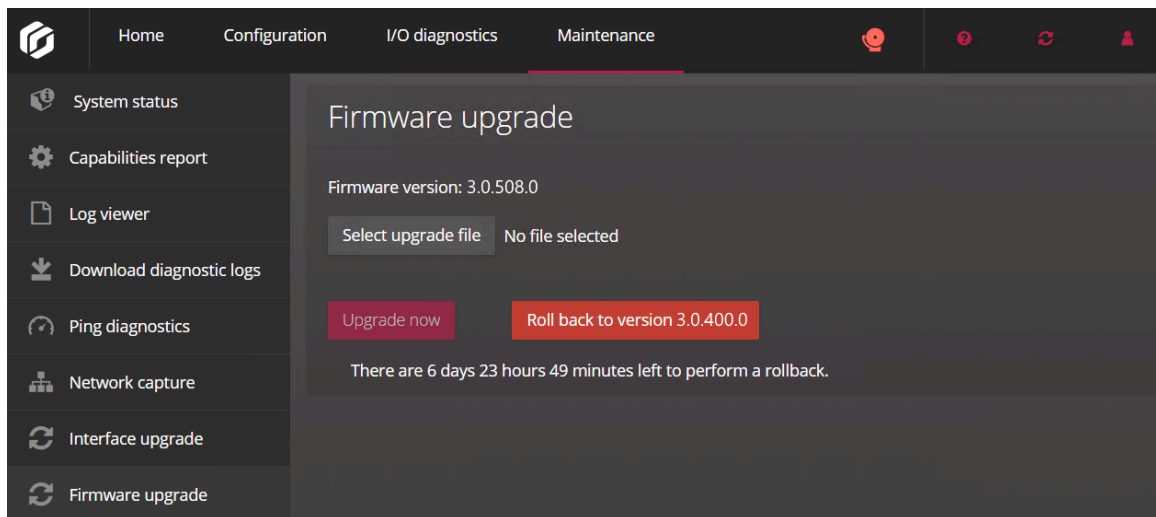
Nach einer Synergis™ Cloud Link -Firmware-Aktualisierung haben Sie sieben Tage Zeit, die Aktualisierung im Synergis™ Appliance Portal rückgängig zu machen.

Was Sie noch wissen sollten

- Durch das Zurücksetzen wird die Einheit wieder in den Zustand vor der Aktualisierung versetzt. Die Firmware und alle Konfigurationsänderungen, die nach der Aktualisierung vorgenommen wurden, werden rückgängig gemacht.
- Die Schaltfläche **Zurück zu Version X.Y.Z** wird in den folgenden Fällen nicht angezeigt:
 - Sieben Tage nach der Aktualisierung sind vergangen.
 - Der Speicherplatz auf dem Gerät reichte nicht aus, um die temporäre Sicherung nach der Aktualisierung zu speichern.
 - Sie haben die Aktualisierung bereits rückgängig gemacht.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Wartung > Firmware-Upgrade**.



- 3 Klicken Sie auf **Zurück zu Version X.Y.Z**.

Es öffnet sich ein Warndialogfeld mit der folgenden Meldung: *Die Konfiguration wird auf den Stand vor der letzten Aktualisierung zurückgesetzt.*

- 4 Klicken Sie auf **OK**.

Die Einheit wird neu gestartet. Nach Abschluss des Zurücksetzens wird die folgende Meldung angezeigt: *Zurücksetzen erfolgreich abgeschlossen. Die Seite wird automatisch aktualisiert, sobald die Einheit verfügbar ist.*

Aktualisieren der Schnittstellenmodul-Firmware über das Synergis™ Appliance Portal

Die Synergis™ Cloud Link-Einheiten funktionieren am besten, wenn auf allen angeschlossenen Schnittstellenmodulen die empfohlene Firmware ausgeführt wird. Empfohlene Firmwareversionen sind durch Genetec Inc. zertifiziert.

Bevor Sie beginnen

- Es ist empfehlenswert, die Firmware des Schnittstellenmoduls mithilfe des Tasks *Hardwarebestand* im Config Tool statt im Synergis™ Appliance Portal zu aktualisieren, da Sie im Task *Hardwareinventar* Folgendes durchführen können:

- Schnittstellenmodule stapelweise und einzeln aktualisieren.
- Upgrades planen und E-Mail-Benachrichtigungen für fehlgeschlagene Upgrades konfigurieren.
- Den Upgrade-Prozess und die aktuelle Firmware für jedes Schnittstellenmodul ansehen.
- Mercury-SIO-Module und -Schnittstellen aktualisieren.

Weitere Informationen finden Sie unter [Aktualisierung der Firmware und Plattform für Zutrittskontrollleinheiten und der Firmware für Schnittstellenmodule](#).

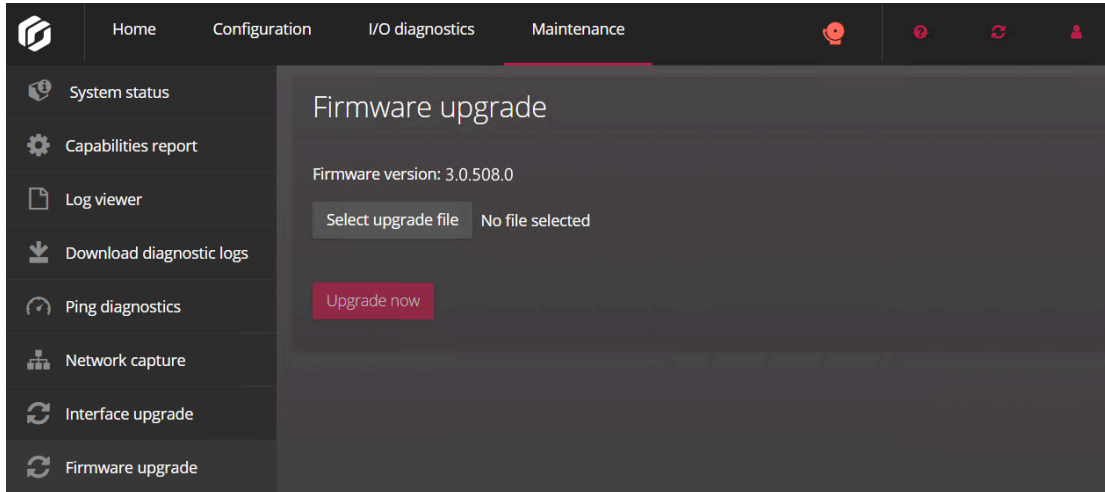
- [Wenn Sie das Upgrade über das Synergis™ Appliance Portal durchführen möchten, stellen Sie sicher, dass Ihr Schnittstellenmodul auf diese Weise aktualisiert werden kann.](#)

Was Sie noch wissen sollten

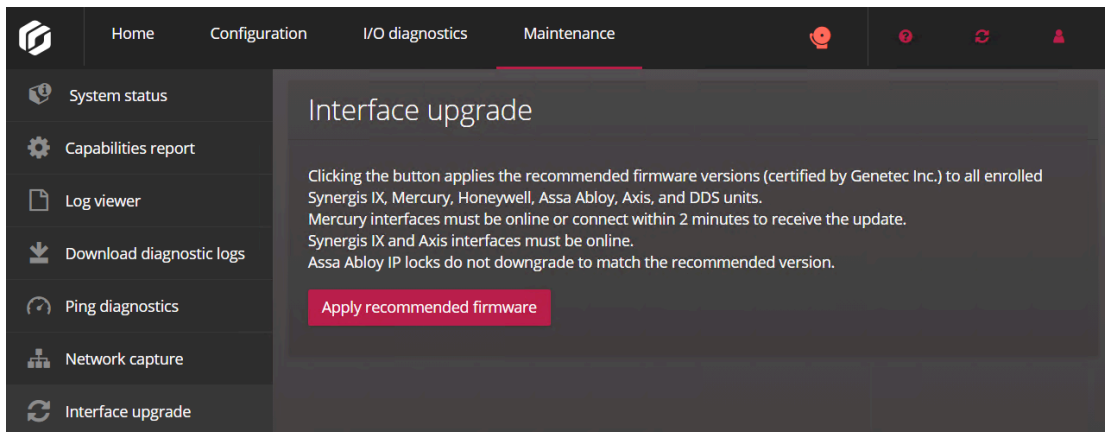
Wenn Ihre Schnittstellenmodule mit einer neueren als den empfohlenen Firmwareversionen geladen werden, werden sie herabgestuft, mit Ausnahme von ASSA-ABLOY-IP-Schlössern.

Prozedur

- 1 Laden Sie die Firmware auf die Synergis™ Cloud Link-Einheit hoch:
 - a) Wählen Sie auf der [GTAP-Seite Produktdownload](#) die Option **Synergis™ Cloud Link** in der Liste **Download Finder** aus und suchen Sie dann nach der Firmware Ihres Schnittstellenmoduls.
 - b) Speichern Sie die *.sfw*-Datei auf Ihrem lokalen Datenträger.
 - c) Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
 - d) Klicken Sie auf **Wartung > Firmware-Upgrade**.



- e) Klicken Sie auf **Upgrade-Datei auswählen**.
 - f) Wählen Sie im folgenden Dateibrowser die *.sfw*-Firmwaredatei aus und klicken Sie auf **Öffnen**.
 - g) Klicken Sie auf **Jetzt aktualisieren**.
- Die Firmware wird auf die Synergis™ Cloud Link-Einheit hochgeladen.
- 2 Übertragen Sie die Firmware per Push an die Schnittstellenmodule:
 - a) Klicken Sie auf **Wartung > Schnittstellen-Upgrade**.



- b) Klicken Sie auf **Empfohlene Firmware anwenden**.

Die folgende Bestätigungsmeldung wird angezeigt: *Upgrade erfolgreich abgeschlossen*.

Nachgeschaltete Geräte, die für Upgrades über das Synergis™ Appliance Portal unterstützt werden

Sie können die Firmware von bestimmten Geräten im Synergis™ Appliance Portal aktualisieren. Bei Herstellern, die nicht unterstützt werden, müssen Sie möglicherweise die Software des Herstellers verwenden, um die empfohlene Firmware anzuwenden.

Die folgenden Geräte können über das Synergis™ Appliance Portal aktualisiert werden:

- **Mercury:**
 - EP1501, EP1502, EP2500, EP4502
 - LP1501, LP1502, LP2500, LP4502
 - MP1502, MP4502
 - M5-IC
 - MS-ICS
- **Honeywell:**
 - PRO32IC
 - PRO42IC
 - PW6K1IC
 - PW7K1IC
- **ASSA ABLOY:**
 - Corbin-Russwin- und SARGENT-IP-Schlosssets (CX-Controller, PoE und WLAN)
- **Axis:**
 - A1001
 - A1601
- **DDS:**
 - TPL
 - JET
- **OSDP-Lesegeräte:**
 - Deister
 - WaveLynx
- **Synergis™ IX Controller:**
 - SY-SIX-CTRL-DIN
 - SY-SIX-CTRL-DIN-1D

Speicher auf der Synergis™ Cloud Link Appliance bereinigen

Stellen Sie sicher, dass Sie auf Ihrer Synergis™ Cloud Link Appliance über genügend Speicherplatz verfügen, bevor Sie Updates oder neue Firmware installieren. Sie können auf der Seite *Speicher* von Synergis™ Appliance Portal überprüfen, wie viel freier Speicher vorhanden ist und Speicherbereinigungen auf Ihrer Appliance durchführen.

Was Sie noch wissen sollten

WICHTIG: Während die Bereinigung durchgeführt wird, werden Firmware-Updates und Systemneustarts auf der Synergis™ Cloud Link Appliance blockiert.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Wartung > Speicher**.

The screenshot displays the Synergis™ Cloud Link Appliance web interface. The top navigation bar includes 'Home', 'Configuration', 'I/O diagnostics', and 'Maintenance'. The left sidebar contains various system management options, with 'Storage' selected. The main content area is divided into two sections: 'Storage' and 'Cleanup'.

Storage Section:

- Used space: 1.16 GiB
- Free space: 12.25 GiB

A pie chart visualizes the storage usage, showing a small red slice for used space and a large grey slice for free space.

Cleanup Section:

- Delete archived and obsolete SCL logs
 ⚠ SCL logging will continue. The cleanup operation only affects archived and obsolete logs.
- Delete Mercury SCP logs
 ⚠ Mercury SCP logging has stopped and will remain disabled after the cleanup.

A 'Start cleanup' button is located at the bottom of the Cleanup section.

3 Wählen Sie Folgendes aus:

- **Archivierte und veraltete SCL-Protokolle löschen:** Wenn Sie diese Bereinigung starten, werden archivierte und veraltete Synergis-Software-Protokolle gelöscht.
- **Mercury SCP-Protokolle löschen:** Wenn Sie diese Bereinigung starten, werden alle Mercury-SCP-Protokolle gelöscht.

4 Klicken Sie auf **Bereinigung starten**.

Peer-to-Peer-Information auf der Synergis™ Cloud Link - Einheit anzeigen unit

Um Probleme in Bezug auf Einheiten zu beheben, die als Peers mit der Synergis™ Cloud Link- Einheit verbunden sind, und um zu verifizieren, dass alle Einheiten miteinander kommunizieren können, können Sie deren Status sowie weitere Informationen über das ansehen Synergis™ Appliance Portal .

Was Sie noch wissen sollten

- Wenn die Option **Peer-to-Peer** auf der Seite *Eigenschaften* der Access Manager-Rolle im Config Tool deaktiviert ist, werden die Zeile *Anzahl von verbundenen Peers* und die Seite *Peer-to-Peer* nicht im Synergis Appliance Portal angezeigt.
- Damit zwei Einheiten als Peers verbunden werden können, müssen sie der gleichen Peer-Gruppe angehören. Bis zu 15 Einheiten können der gleichen Gruppe angehören. Weitere Informationen finden Sie unter [Aktivieren von Peer-to-Peer in der Access-Manager-Rolle](#).
- Damit die Informationen zum globalen Antipassback korrekt bleiben (welcher Karteninhaber welchen Bereich betreten darf), muss immer mindestens ein Gerät eingeschaltet sein. Diese Informationen werden nirgendwo gespeichert, wenn alle Geräte ausgeschaltet werden, gehen sie verloren.
- Einheiten, die unter einer gehosteten Access-Manager-Rolle registriert sind, müssen **DHCP** oder **DHCP mit statischer IP** verwenden, damit Peer-to-Peer funktioniert. Wenn die Einheiten **Statische IP** verwenden, können sie nicht miteinander kommunizieren. Sie können die Netzwerkeinstellungen konfigurieren, indem Sie zu **Konfiguration > Netzwerk** im Synergis Appliance Portal navigieren.

Prozedur

So können Sie die Anzahl der Peers anzeigen lassen, die mit der Synergis™ Cloud Link -Einheit verbunden sind:

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Wartung > Systemstatus**.
- 3 Klicken Sie auf **Einheit**.

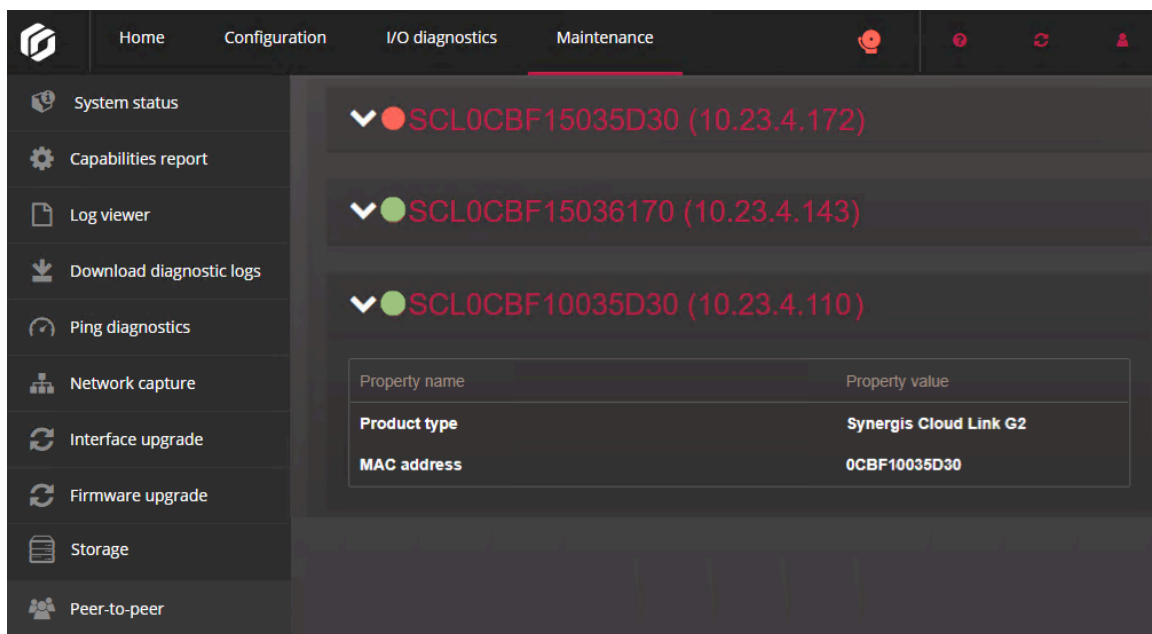
In der Zeile *Anzahl von verbundenen Peers* wird die Anzahl der Online-Peers über der Gesamtzahl der Peers angezeigt. Beispielsweise gibt *10/12* an, dass es 12 Einheiten außer Ihrer unter der gleichen Access-Manager-Rolle gibt, aber nur 10 davon sind mit Ihrer Einheit verbunden.

So können Sie die Details über Peers anzeigen lassen, die mit der Synergis™ Cloud Link -Einheit verbunden sind:

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit an.
- 2 Klicken Sie auf **Wartung > Peer-to-Peer**.
Die Liste von Peers wird angezeigt.

- 3 Klicken Sie auf eine Einheit, um den Produkttyp und MAC-Adresse anzuzeigen.

Beispiel:



Informationen zum Diagnosedienstkonto von Synergis™ Cloud Link

Das Diagnosedienstkonto gewährt einem Kontoinhaber, der kein Administrator ist, grundlegende Diagnose- und Fehlerbehebungsrechte.

Mit dem Diagnosedienstkonto kann sich eine Person ohne Administratorrechte bei der Synergis™ Cloud Link - Einheit anmelden und grundlegende Diagnose- und Fehlerbehebungstasks ausführen.

Der Diagnosedienstbenutzer hat Zugriff auf eine kleinere Anzahl an Funktionen als der Administrator. Dienstbenutzer können auf die folgenden Seiten im Synergis™ Appliance Portal zugreifen:

- **Hardware:** Die Hardwarekonfiguration anzeigen.
- **Synergis Software-Protokollierung:** Die Protokollierungsebenen und Überwachungsprotokollaufbewahrung konfigurieren.
- **Netzwerk:** Lassen Sie den Hostnamen der Einheit, Access-Manager-Einstellungen sowie Netzwerkeinstellungen anzeigen.
- **Benutzer:** Das Passwort für den Dienstbenutzer aktualisieren.
- **E/A-Diagnostik:** Von der Einheit gesteuerte Entitäten anzeigen lassen. Ausgänge steuern, wenn die Ausgangssteuerung aktiviert ist.

Weitere Informationen dazu finden Sie unter [Ausgangssteuerungen deaktivieren](#) auf Seite 39.

- **Systemstatus:** Die Einheiten- und Netzwerkeigenschaften sowie die Benutzerüberwachungsprotokolle anzeigen lassen.
- **Diagnoseprotokolle herunterladen:** Protokolle und das verschlüsselte Engineering-Archiv herunterladen, um sie an den Genetec™ Technical Support zu übermitteln.
BEMERKUNG: Servicebenutzer können keine Überwachungsprotokolle herunterladen.
- **Ping-Diagnostik:** Pingen Sie Schnittstellenmodule und ihre nachgeschalteten Schnittstellen an.

Diagnosedienstkonto erstellen

Durch das Erstellen eines Dienstkontos über Synergis™ Appliance Portal können Sie jemandem, der keine Administratorrechte besitzt, grundlegenden Zugriff auf die Diagnose und Fehlerbehebung gewähren.

Was Sie noch wissen sollten

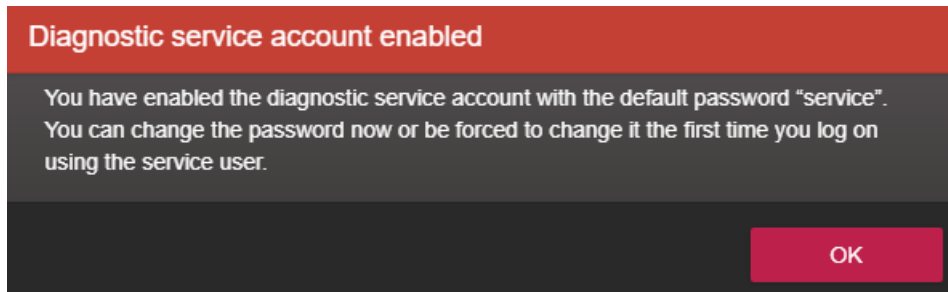
Der Benutzername und das Standardpasswort für das Diagnoseservicekonto lauten beide *service*. Sie können das Standardpasswort sofort zurücksetzen, nachdem Sie das Konto aktiviert haben, oder Sie werden bei der ersten Anmeldung über das Konto dazu gezwungen.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link -Einheit als Administrator an.
- 2 Klicken Sie auf **Konfiguration > Benutzer**.

3 Klicken Sie auf **Diagnosedienstkonto aktivieren**.

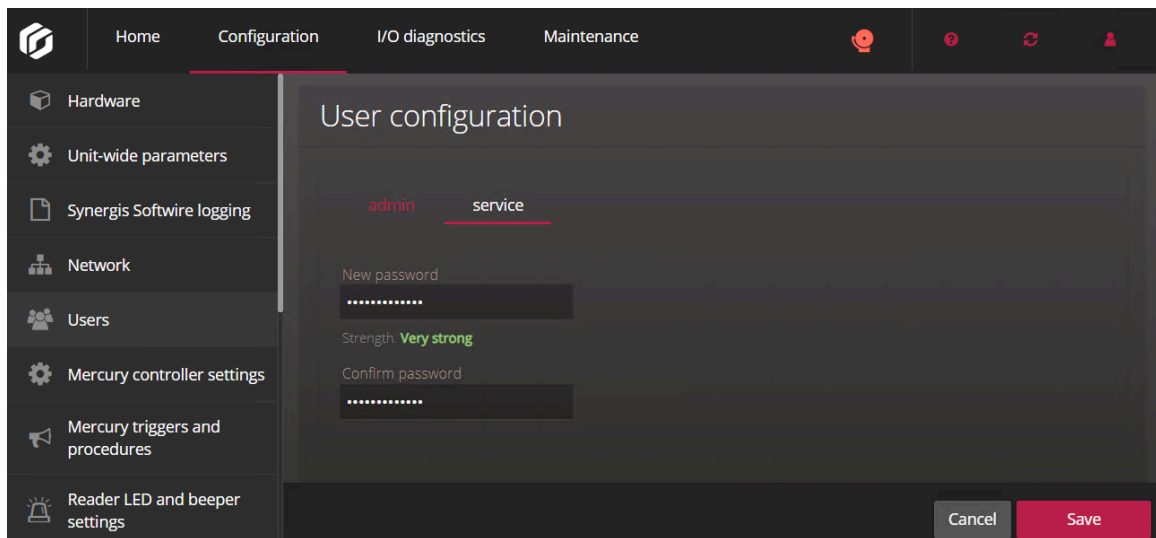
Ein Dialogfeld wird geöffnet, welches bestätigt, dass das Servicekonto aktiviert wurde.



4 Klicken Sie auf **OK**.

5 Klicken Sie auf die Registerkarte **Service** und ändern Sie das Standardpasswort zu einem starken oder sehr starken Passwort.

BEMERKUNG: Das Passwort muss mindestens 15 Zeichen lang sein.



6 Klicken Sie auf **Speichern**.

Hardware oder Software der Synergis™ Cloud Link-Einheit neu starten

Während einer Fehlerbehebungssitzung fordert Sie der Support-Mitarbeiter möglicherweise auf, einen harten oder weichen Neustart auf der Synergis™ Cloud Link-Einheit durchzuführen.

Was Sie noch wissen sollten

- Ein erzwungener Neustart oder *Systemneustart* ist erforderlich, wenn Sie Hardwareprobleme haben.
- Ein weicher Neustart bzw. ein *Softwareneustart* ist nur in seltenen Fällen erforderlich. Die Synergis™ Cloud Link-Einheit startet die eigene Firmware automatisch neu, nachdem Sie die Firmwareversion geändert haben. Manuelle Softwareneustarts werden nur zu Debugging- oder Supportzwecken verwendet.

Prozedur

- 1 Melden Sie sich bei der Synergis™ Cloud Link-Einheit an.
- 2 Wählen Sie im Menü **Neustart** die gewünschte Neustartmethode aus.
 - Klicken Sie auf **Systemneustart**, um die Hardware der Einheit neu zu starten.
 - Klicken Sie auf **Softwareneustart**, um die Software der Einheit neu zu starten.

Glossar

Abhängigkeitsmodus

Der Abhängigkeitsmodus ist ein Online-Betriebsmodus des Schnittstellenmoduls, in dem die Synergis™ Einheit alle Zutrittskontrollentscheidungen trifft. Nicht alle Schnittstellenmodule können im Abhängigkeitsmodus arbeiten.

Access Manager

Die Access Manager-Rolle verwaltet und überwacht Zutrittskontrollgeräte im System.

Antipassback

Ein Anti-Passback ist eine Zutrittseinschränkung zu einem gesicherten Bereich, die einen Karteninhaber daran hindert, einen Bereich zu betreten, den er noch nicht verlassen hat, und umgekehrt.

Automatisierungs-Engine

Die Automatisierungs-Engine ist eine neue Funktion in Synergis™ Software, die Regeln ausführt, ähnlich wie Event-to-Actions in Security Center. Die Automatisierungs-Engine funktioniert auch dann, wenn die Synergis™-Einheit vom Access Manager getrennt ist.

Beaufsichtigter Betrieb

Der beaufsichtigte Betrieb ist ein Online-Betriebsmodus des Schnittstellenmoduls, bei dem das Schnittstellenmodul Entscheidungen auf Basis der Zutrittskontrollentscheidungen trifft, die zuvor aus der Synergis™ Einheit heruntergeladen wurden. Das Schnittstellenmodul berichtet seine Aktivitäten in Echtzeit an die Einheit und ermöglicht der Einheit, eine Entscheidung zu überschreiben, wenn sie den aktuellen Einstellungen in der Einheit widerspricht. Nicht alle Schnittstellenmodule können im beaufsichtigten Modus arbeiten.

Bedrohungsstufe

Eine Bedrohungsstufe warnt Systembenutzer vor sich ändernden Sicherheitsbedingungen, wie z. B. einem Brand oder einer Schießerei, in einem bestimmten Bereich oder im gesamten System. Bestimmte Handhabungsverfahren können automatisch angewendet werden, wenn eine Bedrohungsstufe erhöht oder aufgehoben wird.

Berechtigung

Eine Berechtigung stellt eine berührungslose Karte, Biometrievorlage oder PIN dar, die für den Zutritt zu einem gesicherten Bereich erforderlich ist. Eine Berechtigung kann jeweils nur einem Karteninhaber zugeordnet werden.

Double-Badge-Aktivierung

Mit der Double-Badge-Aktivierung, die auch als Doppelausweisaktivierung bezeichnet wird, kann ein autorisierter Karteninhaber eine Tür entsperren und Aktionen auslösen, indem er seine Berechtigung zweimal vorweist. Bis zum nächsten Doppelausweis-Ereignis bleiben die Tür entsperrt und die Ereignisse aktiv.

E/A-Verknüpfung

E/A (Eingabe/Ausgabe)-Verknüpfung, ist die Steuerung eines Ausgangsrelais auf Basis des kombinierten Zustands (normal, aktiv, fehlerhaft) einer Gruppe überwachter Eingänge. Eine Standardanwendung ist ein Summer (über ein Ausgangsrelais), der meldet, wenn eines der Fenster im Erdgeschoss eines Gebäudes zerbrochen ist (vorausgesetzt, dass jedes Fenster mit einem „Glasbruch“-Sensor überwacht wird, der an einen Eingang angeschlossen ist).

E/A-Zone

Eine E/A-Zone ist eine Zoneneinheit, in der die E/A-Verknüpfung auf mehrere Synergis™-Einheiten verteilt werden kann, wobei eine Einheit als Master-Einheit fungiert. Alle Synergis™-Einheiten einer E/A-Zone müssen vom gleichen Access Manager verwaltet werden. Die E/A-Zone arbeitet unabhängig vom Access Manager, stellt aber ihre Funktion ein, wenn die Master-Einheit ausfällt. Eine E/A-Zone kann von Security Desk aktiviert und deaktiviert werden, solange die Master-Einheit online ist.

Eingeschränkter Modus

Der eingeschränkte Modus ist ein Betriebsmodus des Schnittstellenmoduls, bei dem die Verbindung Synergis™ Einheit unterbrochen ist. Das Schnittstellenmodul gewährt den Zugriff auf alle Berechtigungen, die einem bestimmten Standortcode entsprechen.

Entriegelungszeitpläne

Entriegelungszeitpläne legen fest, wann bei einem Zutrittspunkt (Türseite oder Aufzugflure) freier Zugang gewährt wird.

F2F-Protokoll

Das F2F-Protokoll ist ein proprietäres Protokoll für Casi Rusco-Lesegeräte. F2F ist ein Ein-Draht-Protokoll, im Gegensatz zu zwei Drähten in den Fällen von Wiegand oder OSDP.

Geschützter Bereich

Ein *geschützter Bereich* ist eine Bereichsentität, die für einen zutrittskontrollierten, realen Ort steht. Ein geschützter Bereich besteht aus Türen an den Außengrenzen (für das Betreten und Verlassen des Bereichs) und Zutrittsbeschränkungen (die den Zutritt zu diesem Bereich regeln).

Globales Anti-Passback

Globales Anti-Passback ist eine Funktion, die Anti-Passback-Einschränkungen auf Bereiche erweitert, die von mehreren Synergis™-Einheiten gesteuert werden.

Hardware-Zone

Eine Hardwarezone ist eine Einheit, bei der die E/A-Verknüpfung von einer einzigen Einheit ausgeführt wird. Eine Hardwarezone arbeitet unabhängig vom Access Manager und kann daher nicht von Security Desk aktiviert oder deaktiviert werden.

Interface-Modul

Ein Schnittstellenmodul ist eine Sicherheitsvorrichtung von einem Drittanbieter, die über IP, USB oder RS-485 mit einer Zutrittskontrollereinheit kommuniziert und für die Einheit zusätzliche Ein- und Ausgänge sowie Lesegerät-Anschlüsse bereitstellt.

Karteninhaber

Ein Karteninhaber stellt eine Person dar, die gesicherte Bereiche aufgrund ihrer Berechtigungen (in der Regel sind dies Zutrittskarten) betreten und verlassen kann, und deren Aktivitäten nachverfolgt werden können.

Mobile Berechtigung mobiler Berechtigungsnachweis

Eine mobile Berechtigung ist eine Berechtigung, die sich auf einem Smartphone befindet, das Bluetooth oder Near Field Communication (NFC)-Technologie verwendet, und die es ermöglicht, auf geschützte Bereiche zuzugreifen.

Regel "Alles offen"

Bei der Anwendung auf Bereiche, Türen und Aufzüge gewährt die Regel "Alles offen" allen Karteninhabern jederzeit Zutritt.

Regel für den Zutritt der ersten Person

Die Regel für den Zutritt der ersten Person ist eine zusätzliche Zutrittsbeschränkung für einen gesicherten Bereich. Sie erlaubt den Zutritt einer Person erst dann, wenn bereits ein Aufsichtskarteninhaber den Zugangspunkt passiert hat. Die Beschränkung kann Geltung erhalten, wenn es freien Zugang gibt (bei Entriegelungszeitplänen für Türen) und wenn der Zutritt kontrolliert wird (bei Zutrittsregeln).

Regel zur Besucherbegleitung

Die Regel zur Besucherbegleitung ist eine zusätzliche Zutrittsbeschränkung für einen gesicherten Bereich. Sie verlangt, dass Besucher während ihres Aufenthalts von einem Karteninhaber begleitet werden. Besucher erhalten ohne Begleitperson keinen Zutritt an Zutrittspunkten, sofern sie nicht mit dem als Begleitperson agierenden Karteninhaber ihre Berechtigung in definiertem zeitlichen Abstand vorlegen.

Sicherheitsüberprüfung

Eine Sicherheitsüberprüfung ist ein numerischer Wert, der den Zutritt zu einem Bereich weiter einschränkt, wenn eine Bedrohungsstufe ausgerufen wurde. Karteninhaber können nur dann einen Bereich betreten,

wenn die Werte ihrer Sicherheitsüberprüfung gleich oder höher als die Werte sind, die für diesen Bereich festgelegt wurden.

Sperrregel

Die Sperrregel ist eine permanente Zutrittsregel, die allen Karteninhabern jederzeit den Zugang verweigert und als Ausnahme zu den Regeln, die den Zutritt gewähren, verwendet werden kann.

Sperrung

Eine Verriegelung ist eine Zugangseinschränkung zu einem gesicherten Bereich. Sie bewirkt, dass immer nur eine von mehreren aufeinanderfolgenden Perimetertüren zu einem bestimmten Zeitpunkt geöffnet sein darf.

Standalone-Modus

Der Standalone-Modus ist ein Betriebsmodus, bei dem das Schnittstellenmodul autonome Entscheidungen auf Basis der Zutrittskontrollereinstellungen trifft, die zuvor aus der Synergis™-Einheit heruntergeladen wurden. Wenn das Modul online ist, erfolgt die Aktivitätsmeldung live. Wenn das Modul offline ist, erfolgen Berichte über Aktivitäten zeitgeplant oder wenn die Verbindung zur Einheit verfügbar ist. Nicht alle Schnittstellenmodule können im Standalone-Modus arbeiten.

Strenger Antipassback

Ein strenger Antipassback ist eine Antipassback-Option. Ist die Option aktiviert, wird ein Passback-Ereignis generiert, wenn ein Karteninhaber versucht, einen Bereich zu verlassen, zu dem er noch niemals Zutritt hatte. Bei Deaktivierung generiert Security Center nur dann Passback-Ereignisse, wenn Karteninhaber einen Bereich betreten, den Sie noch niemals verlassen haben.

Synchronisierung von Einheiten

Synchronisierung von Einheiten ist der Prozess, bei dem die neuesten Security Center-Einstellungen auf eine Zutrittskontrollereinheit heruntergeladen werden. Diese Einstellungen, wie Zutrittsregeln, Karteninhaber, Berechtigungen, Entriegelungszeitpläne usw., sind erforderlich, damit die Einheit zutreffende und eigenständige Entscheidungen treffen kann, wenn keine Verbindung zum Access Manager besteht.

Synergis™ Appliance Portal

Das Synergis™ Appliance Portal ist das Web-basierte Verwaltungstool für die Konfiguration und Verwaltung eines Synergis™ Gerätes und für die Aktualisierung seiner Firmware.

Synergis™ Cloud Link

Synergis™ Cloud Link ist ein intelligentes PoE-fähiges IoT-Gateway, das als nicht proprietäre Zutrittskontrolllösung entworfen wurde. Synergis™ Cloud Link bietet nativen Support für eine Vielzahl von intelligenten Steuerungen und elektronischen Schlössern.

Synergis™-Einheit

Eine Synergis™-Einheit ist eine Synergis™ Appliance, die als Zutrittskontrollereinheit in Security Center eingesetzt wird.

Synergis™ Gerät

Eine Synergis™ Appliance ist eine IP-fähige Sicherheitslösung von Genetec, die speziell für Zutrittskontrollfunktionen entwickelt wurde. Alle Synergis™ Appliances werden mit vorinstalliertem Synergis™ Software geliefert und werden als Zutrittskontrollereinheiten in Security Center eingesetzt.

Synergis™ key store

Der Synergis™ key store ist eine Datenbank, die transparente Lesegerätschlüssel, die Schlüssel *ReaderKc* und *ReaderKs* für STid-Lesegeräte und den SAM LockUnlock-Schlüssel für Synergis™-Einheiten mit dem optionalen Erweiterungsmodul enthält. Die Schlüssel in der Datenbank können nicht eingesehen oder gelesen, jedoch mit Hilfe von Schlüsselhashes überprüft werden.

Synergis™ Software

Synergis™ Software ist eine von Genetec entwickelte Zutrittskontrollsoftware, die auf unterschiedlichen IP-fähigen Sicherheitslösungen ausgeführt werden kann. Synergis™ Software ermöglicht diesen Einheiten die Kommunikation mit Schnittstellenmodulen von Drittanbietern. Eine Sicherheitslösung, die auf Synergis™ Software läuft, wird als Zutrittskontrollereinheit in Security Center eingesetzt.

X.509-Zertifikat

X.509-Zertifikat und *digitales Zertifikat* sind Synonyme. In Security Center werden diese beiden Begriffe austauschbar verwendet.

Zone

Eine Zone ist eine Einheit, die eine Auswahl an Eingängen überwacht und Ereignisse auf Grundlage kombinierter Zustände auslöst. Diese Ereignisse können für die Steuerung von Ausgangsrelais verwendet werden.

Zutrittskontrolleinheit

Eine Zutrittskontrolleinheit stellt ein intelligentes Gerät für die Zutrittskontrolle dar (zum Beispiel eine Synergis™ Appliance, ein Axis Powered by Genetec-Türcontroller oder ein HID-Netzwerkcontroller). Dieses kommuniziert direkt mit Access Manager über ein IP-Netzwerk. Eine Zutrittskontrolleinheit arbeitet eigenständig, wenn sie vom Access Manager getrennt wird.

Zutrittsregel

Eine Zutrittsregelentität definiert eine Liste der Karteninhaber, denen der Zutritt auf der Grundlage eines Zeitplans erlaubt oder verweigert wird. Zutrittsregeln können auf gesicherte Bereiche und Türen zum Eingang und Ausgang oder Einbruchserkennungsbereiche für Aktivierung und Deaktivierung angewendet werden.

Zwei-Personen-Regel

Das Vier-Augen-Prinzip ist eine Zutrittsbeschränkung für eine Tür. Sie verlangt, dass zwei Karteninhaber (einschließlich Besucher) ihre Berechtigungsträger in definiertem zeitlichem Abstand vorlegen, um Zutritt zu erhalten.

Wo finde ich Produktinformationen?

Unsere Produktdokumentation steht in folgenden Bereichen zur Verfügung:

- **Genetec™ TechDoc Hub:** Die aktuelle Dokumentation ist im [TechDoc Hub](#) verfügbar.
Sie finden die gesuchte Information nicht? Nehmen Sie Kontakt mit documentation@genetec.com auf.
- **Installationspaket:** Das Installationshandbuch und die Versionshinweise stehen im Ordner Dokumentation zur Verfügung, der sich im Installationspaket befindet. Einige Dokumente beinhalten auch einen direkten Link zum Herunterladen der aktuellen Version des Dokuments.
- **Hilfe:** Security Center-Clientanwendungen und webbasierte Anwendungen beinhalten eine Hilfe, in der die Funktionsweise des Produkts und die Nutzung der Produktfunktionen erläutert werden. Um auf die Hilfe zuzugreifen, klicken Sie auf **Hilfe**, drücken Sie F1, oder tippen Sie auf das ? (Fragezeichen) in den jeweiligen Client-Anwendungen.

Technischer Support

Das Genetec™ Technical Assistance Center (GTAC) möchte seinen Kunden weltweit den bestmöglichen technischen Supportservice bieten. Als Kunde von Genetec Inc. haben Sie Zugriff auf den TechDoc Hub, wo Sie Informationen und Antworten auf produktbezogene Fragen finden können.

- **Genetec TechDoc Hub:** Hier finden Sie Artikel, Handbücher und Videos, die Ihnen bei Fragen oder technischen Problemen weiterhelfen.

Bevor Sie sich an GTAC wenden oder einen Support-Fall öffnen, durchsuchen Sie bitte zunächst den TechDoc Hub nach potenziellen Fehlerbehebungen, Umgehungslösungen oder bekannten Problemen.

Melden Sie sich im [Genetec Portal](#) an und klicken Sie auf [TechDoc Hub](#), um auf den TechDoc Hub zuzugreifen. Sie finden die gesuchte Information nicht? Nehmen Sie Kontakt mit documentation@genetec.com auf.

- **Genetec Technical Assistance Center (GTAC):** Die Kontaktaufnahme mit dem GTAC ist in den folgenden [Produktbeschreibung: Genetec™ Advantage](#) beschrieben.

Technische Schulungen

Unsere qualifizierten Trainer können Sie – in einer professionellen Lernumgebung oder aus der Annehmlichkeit Ihres Büros heraus – bei Systemdesign, Installation, Betrieb und Fehlerbehebung anleiten. Technische Schulungen werden für alle Produkte sowie für Kunden mit unterschiedlichstem technischen Hintergrund angeboten und können an spezifische Anforderungen und Ziele angepasst werden. Weitere Informationen finden Sie unter <http://www.genetec.com/support/training/training-calendar>.

Lizenzierung

- Für die Aktivierung oder Zurücksetzung von Lizenzen wenden Sie sich bitte an GTAC unter <https://portal.genetec.com/support>.
- Bei Fragen zu Lizenzumfang, Teilenummern oder einer Bestellung wenden Sie sich bitte an den Genetec Kundenservice unter: customerservice@genetec.com, oder rufen Sie an unter: +1-866-684-8006 (Option #3).
- Wünschen Sie eine Demolizenz oder haben Sie Fragen zur Preisgestaltung, wenden Sie sich bitte an den Genetec Vertrieb unter: sales@genetec.com, oder rufen Sie an unter: +1-866-684-8006 (Option #2).

Probleme mit Hardwareprodukten und Defekte

Bitte wenden Sie sich an GTAC unter <https://portal.genetec.com/support>, um Probleme mit Genetec™-Geräten oder anderer Hardware zu melden, die über Genetec Inc. bezogen wurde.