Synergis™Softwire 統合ガイド 10.6

ドキュメントの最終更新日：2018 年 1 月 25 日

Genetec™

著作権表示

ドキュメントの情報

文書のタイトル：Synergis™Softwire 統合ガイド 10.6 文書番号：

EN.702.002-V10.6.B (2)

ドキュメント更新日：2018 年 1 月 25 日

あなたのコメント、修正、およびこのガイドについての提案を送信することができます documentation@genetec.com。

本ガイドについて

このガイドでは、Synergis™Softwire でサポートされているすべてのサードパーティ製のハードウェアの統合について説明し、あなたの Synergis™アプライアンス上でこれらのサードパーティ製デバイスを登録して設定する方法について説明します。

あなたが Synergis™Appliance コンフィギュレーションガイドを読み、Synergis™アプライアンス Portal およびセキュリティセンターで使用される用語や概念に精通しているものとします。サードパーティ製のハードウェアに関する具体的な情報については、そのメーカーの Web サイトを参照してください。

注意事項と注意事項

次の注意事項および注意事項は、このガイドで表示されることがあります。

- **先端**。トピックまたはステップの情報を適用する方法を提案しています。
- **注意**。特殊なケースを説明し、または重要なポイントに拡大。
- **重要**。トピックまたはステップに関する重要な情報を指摘します。
- **あぶない**。アクションやステップは、データ、セキュリティ上の問題、またはパフォーマンスの問題の損失を引き起こす可能性があることを示します。
- **警告**。アクションやステップは、物理的な危害が発生、またはハードウェアの損傷を引き起こす可能性があることを示します。

重要： 第三者のウェブサイト上の情報を参照し、このガイドに現れるトピックしかし、この情報はゼネテック社に予告なく変更することがあり、出版の時点で正確でした

コンテンツ

第 5 章：AutoVu SharpV カメラ

第 6 章：軸コントローラ

第 7 章：DDS コントローラ

第 8 章：HID VERTX のサブパネル

第 9 章：ハネウェルコントローラ

第 10 章：マーキュリーコントローラ

1

Synergis™Softwire による統合

このセクションでは、次のトピックについて説明します。

What is Synergis™ Softwire?

Synergis™Softwire は、IP 対応のセキュリティ・アプライアンスの様々な上で実行するゼネテック社が開発したアクセス制御ソフトウェアです。Synergis™Softwire は、これらのアプライアンスは、サードパーティのインターフェースモジュールと通信することができます。Synergis™Softwire を実行しているセキュリティアプライアンスは、セキュリティセンターでは、アクセス制御ユニットとして登録することができます。

Synergis™アプライアンスについて

Synergis™アプライアンスは、制御機能にアクセスするために専用されゼネテック社製 IP 対応のセキュリティアプライアンスです。すべての Synergis™アプライアンスは、Synergis™Softwire にプリインストールされてくるとセキュリティセンターにアクセス制御ユニットとして登録することができます。

Synergis™アプライアンスの 2 つの世代があります。

- Synergis™クラウドリンク（第 2 世代）
- Synergis™マスターコントローラ（初代）

注意： Synergis™アプライアンスは、セキュリティセンターでのアクセス制御ユニットとして登録することができますので、それらも Synergis™ユニットと呼ばれています。

Synergis™アプライアンスの詳細については、彼らは全体の Synergis™IP アクセス制御システムアーキテクチャに適合する方法には、当社のウェブサイトをご覧ください。 www.genetec.com。

インターフェイスモジュールについて

インターフェースモジュールは、IP または RS-485 を介してアクセス制御部と通信し、ユニットへの追加の入力、出力、及びリーダ接続を提供するサードパーティのセキュリティ装置です。

Synergis™Softwire 統合の文脈では、インタフェースモジュールは Synergis™アプライアンスと直接通信するハードウェアデバイスです。これらのデバイスは、マーキュリーEP コントローラなどのインテリジェントコントローラ、ことができます。このような HID VERTX 下流パネルなどのサブパネル、; あるいは、そのような STID リーダーとして読者、。」

What is Synergis™ Appliance Portal?

Synergis™アプライアンス· ポータルは、設定および Synergis™アプライアンスを管理するだけでなく、そのファームウェアをアップグレードするために使用される Web ベースの管理ツールです。

ポータルを使用すると、次のタスクを実行することができます：

- Synergis™アプライアンスにログオンするために必要なセキュリティパスワードを変更します。
- それはあなたのシステム上で動作しますので、Synergis™アプライアンスのネットワーク設定を構成します。
- 特定のアクセスマネージャからの接続を受け入れるようにアプライアンスを設定します。
- Synergis™アプライアンスに接続されたインターフェイスモジュールを登録して構成します。

  注意： ルールには例外が 1 つあります。マーキュリー· コントローラ（EP と M5-IC）が登録され、アクセス制御ユニットの周辺機器]タブで[セキュリティセンターの設定ツールから設定する必要があります。詳細については、Synergis™Softwire 統合ガイド中の水銀コントローラに関する章を参照してください。
- オンラインとオフラインの両方の操作のためのアプライアンスのアクセスコントロールの動作を設定します。
- Synergis™アプライアンスへのインタフェースモジュールの接続をテストして診断します。
- Synergis™アプライアンスのステータスおよび設定を表示およびエクスポートします。
- Synergis™アプライアンスのファームウェア（Synergis™Softwire）をアップグレードします。
- Synergis™アプライアンスのハードウェアまたはソフトウェアを再起動します。

設定ツールで行われなければならないタスク

あなたは、ポータルを介して、次のタスクを実行することはできません。代わりに、セキュリティセンター設定ツールを使用する必要があります。

- 有効/サーバ· モード動作を無効にします（このオプションはデフォルトで隠されている、それはすでに有効になった場合にのみ表示されます）。
- ドアやゾーンにデバイス（入力/出力接点、読者）を割り当てます。
- 個々のドアとゾーンのプロパティを設定します。
- カードと PIN の両方がアクセスを許可するために必要とされるようにカードと PIN の読者を設定します。
- I / O のリンクを設定します。

Synergis の展開の詳細については、™参照してください *セキュリティセンター管理者ガイド*。

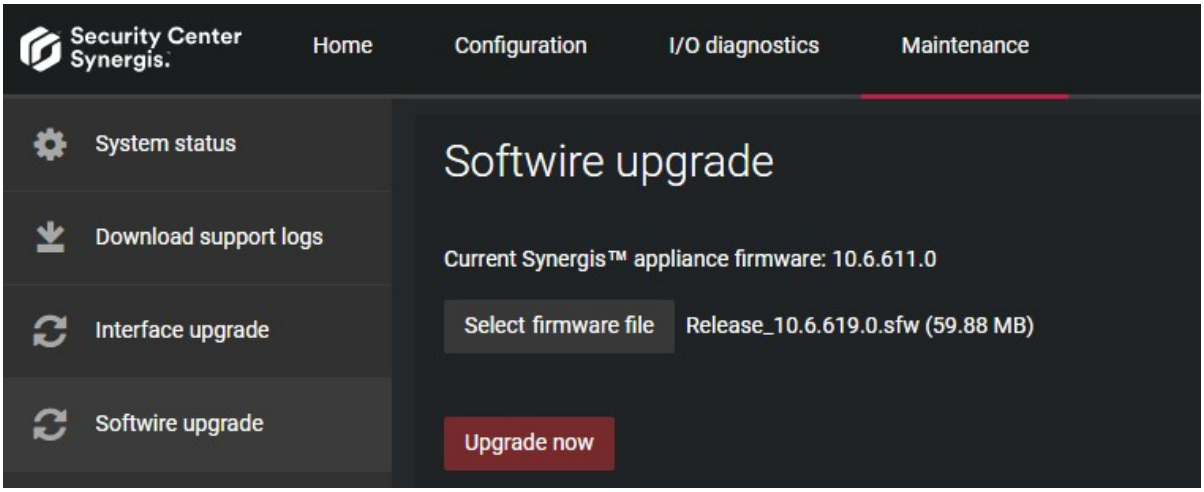
Hardening tips for interface

システムのセキュリティが組織にとって優先事項であるならば、我々はあなたがインターフェイス・モジュールのための硬化アドバイスに従うことをお勧めします。

このセクションでは、すべてのインターフェイスモジュールに適用される硬化のヒントを提示します。メーカー特有の硬化のヒントは、各メーカーのそれぞれの統合トピックに硬化でタグ付けされています。システム全体のためのガイドラインを強化するために、セキュリティセンターのセキュリティ強化ガイドを参照してください。

最新のインターフェースモジュールのファームウェアを使用します

アクセス制御ハードウェアメーカーは、頻繁に彼らの製品を更新し、新しいファームウェアを使用してセキュリティの脆弱性を修正します。我々は継続的に Synergis™Softwire とサードパーティのインターフェースモジュールメーカーが公表され、新しいファームウェアの互換性をテストします。私たちは、それぞれのサポートされている<サードパーティ製デバイス>各メーカーのトピックの推奨ファームウェアとして、Synergis™Softwire と互換性の認定を受け、最新のインターフェースモジュールのファームウェアを公開します。インタフェースモジュールの特定のモデルでは、あなたは Synergis™アプライアンスポータルからの推奨ファームウェアを適用することができます。詳細については、Synergis™Appliance コンフィギュレーションガイドを参照してください。



注意： Synergis™の-partner ファームウェアの認定追跡は現在、Synergis™Softwire 10.6 の範囲内で行われます。新たに発見された脆弱性は、私たちによって認定 1 より新しいファームウェアで固定されている場合は、メーカーのソフトウェアを使用して、それを適用します。

デフォルトのパスワードを使用しないでください

多くのアクセス制御装置は、それらのデフォルトの管理者パスワードに同梱されています。これらのパスワードは、プライベートでも、セキュアではありません。あなたの Synergis™ユニットにそれらを登録する前に、各デバイスの Web ページ上でこれらのパスワードを変更します。パスワードを変更するための最も安全な方法は、（これは理想的に HTTPS を介して行われるべきである）あなたがこれを行うことができ、その上、別のネットワークを設定することです。

お使いのハードウェア構成から未使用のインターフェイスモジュールを削除します。

あなたの Synergis™アプライアンスのハードウェア構成から未使用のインターフェイスモジュールを削除します。特定のインターフェイスモジュールは、攻撃へのアプライアンスが脆弱に開いているポートを残すことができます。あなたは Synergis™アプライアンスポータルからか、設定ツールのいずれかから未使用のインターフェイス・モジュールを削除することができます。詳しくは、各インターフェイスモジュールメーカーに対応するトピックを参照してください。

2

Allegion Schlage ロック

このセクションでは、次のトピックについて説明します。

サポートされている Allegion Schlage ロック

Allegion Schlage AD シリーズロックの統合は、Mercury EP（またはハネウェル）コントローラが必要です。この統合のために、EP コントローラはインタフェース・モジュールとして表示され、および AD シリーズのロックは、非インテリジェントデバイスとして表示されます。

のみ水銀 EP（またはハネウェル）コントローラは Synergis™ユニットと直接通信します。

注意： Allegion Schlage AD シリーズロックの統合は、セキュリティセンター5.5（またはそれ以上の最近のバージョン）と Synergis™Softwire 10.2（またはそれ以上の最近のバージョン）が必要です。Allegion Schlage NDE＆LE ロックは、セキュリティセンター5.7 SR1 と Synergis™Softwire 10.6 が必要です。

Synergis™Softwire は、次のハードウェアデバイスをサポートしています。

モデル	説明
IP コントローラ	A 水星 EP（または ハネウェル）コントローラは Synergis™ユニットと AD シリーズロックとの間のインターフェースモジュールとして作用しなければなりません。 サポートされているコントローラのモデルは以下のとおりです。 • 8 AD-300 ロックまたは 16 AD-400 ロックまでサポート拡張ボードとの水銀 EP1501 コントローラ • 16 AD-300 ロックまたは 64 AD-400 ロックまで支持水銀 EP2500 コントローラ • 16 AD-300 ロックまたは 64 AD-400 ロックまで支持ハネウェル PW6K1IC コントローラも参照します サポートされている水銀のファームウェアバージョン 126 ページ。
AD300	RS-485 インターフェースを備えた Allegion Schlage AD-300 のハードワイヤード電子ロック。EP コントローラに接続されなければならない（参照データシート）。
AD400	Allegion Schlage AD-400 無線電子ロック。EP コントローラに接続する PIM400 無線通信モジュールを必要とする（参照データシート）。
PIM400-485	Allegion Schlage PIM400-485 は、RS-485 通信モジュール、EP コントローラに 16 AD-400、ワイヤレスロックまで接続することが可能である（参照 データシート）。
PIM400-1501	Allegion Schlage PIM400-1501 が水銀 EP1501 コントローラに予め配線 PIM-485 モジュールである（参照 データシート）。
LE	Allegion Schlage LE 無線電子ロック。EP ゲートウェイに接続するために ENGAGE ゲートウェイが必要です。ロックは、Bluetooth 上ゲートウェイに接続し、その後、ゲートウェイは、RS-485 インターフェースにより直接 EP コントローラに接続されています。
NDE	Allegion Schlage NDE 無線電子ロック。EP ゲートウェイに接続するために ENGAGE ゲートウェイが必要です。ロックは、Bluetooth 上ゲートウェイに接続し、その後、ゲートウェイは、RS-485 インターフェースにより直接 EP コントローラに接続されています。

RS-485 の配線指示

AD300 ロック配線、又は PIM400 又は EP コントローラ上の RS-485 バスに、ゲートウェイモジュールと係合する場合、ワイヤコネクタは次のように

- TR +への TDA-
- TR-する TDB +

制限事項

Allegion Schlage AD、LE および NDE シリーズロックの統合は、次の制限があります。

- Allegion Schlage デバイスとマーキュリーMR パネルは同じ RS-485 バス上で混在させることはできません。
- 同じ RS-485 バスに接続されたすべての Allegion Schlage デバイスは、それぞれが異なるアドレスを持っている必要があります。
- ドアの数字は、それらが異なる PIM400 モジュールと AD300 ロックによって制御されている場合でも、同じ RS-485 バス上の異なるロック間で重複することはできません。あなたがドア/ロック 0-10 と PIM400 を持っている場合たとえば、あなたの次の PIM400 は、ドア/ロック数 11 か仕事をしたり、オンラインで来る何も始まらなければなりません。
- AD300 ロックは、RS-485 アドレスと同じであるドア番号を持っており、同じバス上の PIM400 によって使用される範囲内の任意のドアと重複することができません。たとえば、アドレス 0 の PIM400 を持っている場合 ドア/ロック 0-10 で、あなたの AD300 11 と 31 の間でアドレスを割り当てる必要があります。
- PIM400 の下にあるすべての AD400 のロックまたは ENGAGE ゲートウェイは、連続したドアの番号を持っている必要があります。
- すべての AD300 と AD400 メッセージや機能がサポートされていません。以下のロック機能はサポートされません。
  - 入る要求
  - 失速モーター
  - インテリアプッシュボタン
  - デッドボルトスイッチの位置
  - ラッチボルト
- AD300 と AD400 ロックの入力は設定できません。この機能は、ハードウェアでサポートされていません。
- 手動ロック解除と再ロックコマンドが実行されるように予想以上に時間がかかることがあります。これらのコマンドはタイミングが正確されていないラジオ（WOR）メッセージウェイクオンに依存しているためです。

サポートされている Allegion Schlage ファームウェアバージョン

この統合のすべての機能を利用するには、ファームウェアバージョンの特定の範囲を使用する必要があります。Synergis™Softwire 10.6 がサポートしている Allegion Schlage ファームウェアバージョン：

モデル	最小
AD300	AD.A.90
AD400	AD.A.90
NDE	2.10.09
LE	1.05.44

サポートされている Allegion Schlage ロック機能

Allegion Schlage AD、LE および NDE シリーズロック統合は水銀 EP（またはハネウェル）コントローラを必要とします。AD シリーズのロックは、そのコントローラから切断されている場合、ロックはアクセス権を付与またはオフラインイベントを保存することはできません。しかし、メカニカルキーだけでなく、内部のハンドルは、まだ扉を開くために使用することができます。

Synergis™Softwire 10.6 には、以下の Allegion Schlage ロック機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleElectronic	ロック
通信プロトコル [1] トゥース	RS-485、ラジオ、ブルー
暗号化されました communicationYes	[2]
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeYes	
依存 modeNo	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン MODEN / A	
劣化 modeNo	
無線 operationYes	[3]
上 Synergis™ユニットにお問い合わせください eventNDE	＆LE
ポーリング間隔（v3 のロック のみ）はい	
スケジュールのラジオ接触（ステータスレポート 間隔）で	ロック（NDE＆LE）
電池 checksYes	
電源がオン（フェイルセーフ/フェールセキュア）ロックの設定に失敗します	ロック（NDE＆LE）
ENGAGE integrationNDE	＆LE locks6
スケーラビリティ	
オフラインの最大数 eventsN / A	
自律的意思決定のための資格証明書の最大数（ メイキング）	N /
（ビットで）最大資格長	
	52

FeaturesSupported	
RS-485 チャネルごとインターフェースモジュールの最大数	32
Synergis™あたりのインターフェイスモジュールの推奨最大数 unitN / A	[5]

[1] Allegion Schlage ロックは、RS-485（AD300）、または無線（AD400）を用いて水銀 EP コントローラと通信します。水星 EP コントローラは、IP 経由 Synergis™ユニットと通信します。LE と NDE ロックは、Bluetooth 上 ENGAGE ゲートウェイに接続します。

[2] AD400（ワイヤレスロック）が AES-128 ビット暗号化を使用して 900 MHz チャネルを介して通信します。

[3] AD400 モデルはワイヤレスロックです。PIM400 通信モジュールが必要です。NDE と LE ロックは ENGAGE ゲートウェイを必要とします。

[4] 最大 8 つの異なる資格長は、スタンドアロンモードでサポートされています。以上がでサポートすることができます

依存モード。

[5] Allegion Schlage ロック統合では、とみなされる水銀 EP コントローラであります *インタフェース モジュール*、ない Allegion Schlage ロック。Synergis™単位当たりの水銀 EP コントローラの推奨数については、サポートされている水銀コントローラの機能 127 ページ。

[6] 統合は水星 EP パネルを介して行われます。EP1501 と EP2500 のみがサポートされています。マーキュリーファームウェアバージョン 1.25.6 のとおり、すべてのマーキュリー・ コントローラは、Allegion Schlage ロックをサポートしています。

個別のドアモードでは約 Allegion Schlage サポート

Allegion Schlage AD、LE、および NDE シリーズのロックによってサポートされる新しいドアモードは、アクセス制御コンテキストの広い選択に合います。

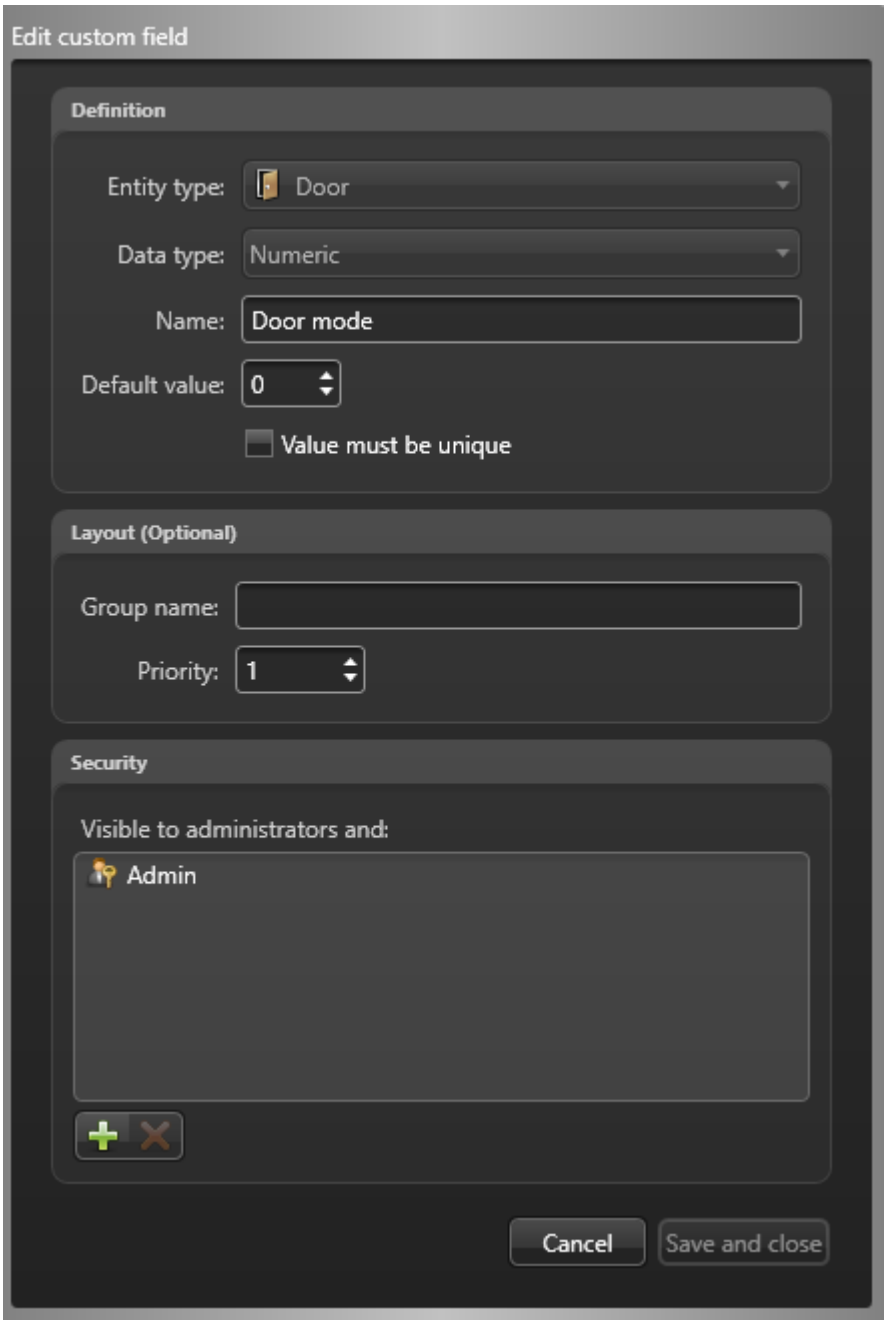
必要条件

最低限必要な Synergis™アプライアンスのファームウェアは 10.6 GA です。LE ロックは、セキュリティセンター5.7 SR1 のとしてサポートされています。アパートモードでは、水星 EP ファームウェア 1.25.6 以降は、すべての機能のために必要とされます。

モードとその機能

サポートドアモードは、設定ツールでドアにドアモード数値カスタムフィールドを使用して設定されています。モードは次のとおりです。

- 0 - 通常動作
- 1 - 教室：同じアクションが再びそれをロックされるまで（5 秒以内）2 回のスワイプ同じカードでは、ドアのロックを解除
- 2 - オフィス：ロックを解除し、再ロックする押しボタン
- 3 - プライバシー：押しボタン無効化するために、すべての外部からのアクセス、押しボタンや REX を拒否する
- 4 - アパート：押しボタンまたは REX アウトロックを解除するには、再ロックするには、ボタンを押したりスワイプするまでアンロックしたまま



制限： モード 0 に設定されていないロックの現在の制限：

- どちらもありません *カードと PIN* も *DoubleSwipe* 作業
- *スケジュールのロックを解除* そして *ロックダウン* 正常に動作しない場合があります

Allegion Schlage ロック統合のためのサポート Synergis™ アプライアンスの機能

すべての Synergis™アプライアンスの機能を Allegion Schlage ロックの統合でサポートされていません。Allegion Schlage ロックは水星 EP コントローラを介して Synergis™アプライアンスに接続されています。ために

Allegion Schlage ロックの統合によりサポート Synergis™アプライアンスの機能を参照してください サポート Synergis™

マーキュリーコントローラを統合するためのアプライアンスの機能 129 ページ。

Allegion Schlage のためのサポートされているセキュリティセンターの機能 ロック統合

すべてのセキュリティセンターのアクセス制御機能は Allegion Schlage ロックの統合でサポートされていません。

Allegion Schlage ロック統合には、以下のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeYes	[1]
	拡張助成金 timeYes	
	エントリの時間（標準/拡張）[2]	ノー
	ドアリロック - optionsLimited	[3]
	ドアはスケジュールによってロックが解除された場合 - optionsOnline	
	ドア開催します - optionsYes	
	ドアが開いて強制的に - optionsLimited	[4]
	アンロック schedulesYes	
	（REX）のオプションを終了する要求	
	REX にロックを解除（オン/オフ）はい	
	アクセスを許可した後 REX を無視する時間（中 オンライン秒）	
	ドアが開いている間 REX イベントを無視 オンライン（オン/オフ）	
	（ドアが閉じた後、REX を無視する時間 オンライン秒）	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒。）いいえ	
	ドア上の（オン/オフ）2 人のルールを強制します sideNo	
セキュリティ Desk5 ドアの手動アクション	手動でロックを解除 doorsYes	
	シャント Reader は（有効化/無効化 読者）はい	
	オーバーライドロック解除 schedulesYes	

特徴 groupSecurity	センター featureSupported	
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン、オフライン*）はい	
	交流 failYes	[6]
	バッテリーは（失敗しますローバッテリー）はい	
	ドア オープン/ closedYes	
	ドア ロック/ unlockedYes	
	ドアの強制 openYes	
	ドアはあまりにもオープン開催しました longYes	
	ドア securedN / A	
	デッドボルト（*確保し、リリース*）いいえ	
	キー overrideYes	[7]
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）	い
	いえビジター護衛ルールません（オンオフ）	ノ
	ー	
	InterlockNo	
	Antipassback	
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）いいえ	
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）いいえ	
	両方のエリアの入り口にチェックを厳格（antipassback と 終了）いいえ	
	に scheduleNo	
	グローバル antipassbackNo	
	一人称-内のルール	
	ドアアンロックに強制 scheduleNo	
	アクセスに施行 rulesNo	
エレベーター コントロール		エレベー
ター	N / A	
ゾーン管理	I / O zoneNo	
	ハードウェア zoneNo	

[1] サポートされる最大値は 255 秒です。

[2] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、入力検出イベントが発生したとき

ドアセンサーがトリガされます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[3] 開封後はタイムアウトと再ロックするように設定されたドアは、まだ助成金タイムアウト後にロック近いオプションの再ロックを備えています。

[4] のために **リーダーのブザーの動作** 、オプションの設定 *抑制* そして *ドアが閉じたときに抑制* オンラインとオフラインの動作モードの両方でサポートされています。オプション *アクセスが許可されたときに抑制* 扱われます *ドアが閉じたときに抑制*。

[5] Synergis™ユニットは、Access Manager に接続する必要があります。

[6] NDE および LE ロックの N / A。

[7] AD シリーズのロックのみ。

Synergis™ユニットに登録 Allegion Schlage ロック

Synergis™ユニットは Allegion Schlage デバイスと通信していないので、あなたは、設定ツールを使用して、水星 EP（またはハネウェル）コントローラを介してこれらのデバイスを登録する必要があります。

あなたが始める前に

- 設定 Schlage Pidion の手を使用して、各 Schlage デバイス上の異なる RS-485 アドレス（AD シリーズロックと PIM400 モジュール）（参照デバイスを保持 制限事項）、そしてあなたの水星 EP コントローラにロックして、モジュールを接続します。詳細については、Schlage ユーティリティソフトウェアのユーザガイド。
- EP コントローラに割り当てられた静的 IP アドレスを設定。

あなたは知っておくべきこと

Synergis™ユニットに登録マーキュリーコントローラは Synergis™アプライアンスポータルからは見えません

ハードウェアページ。

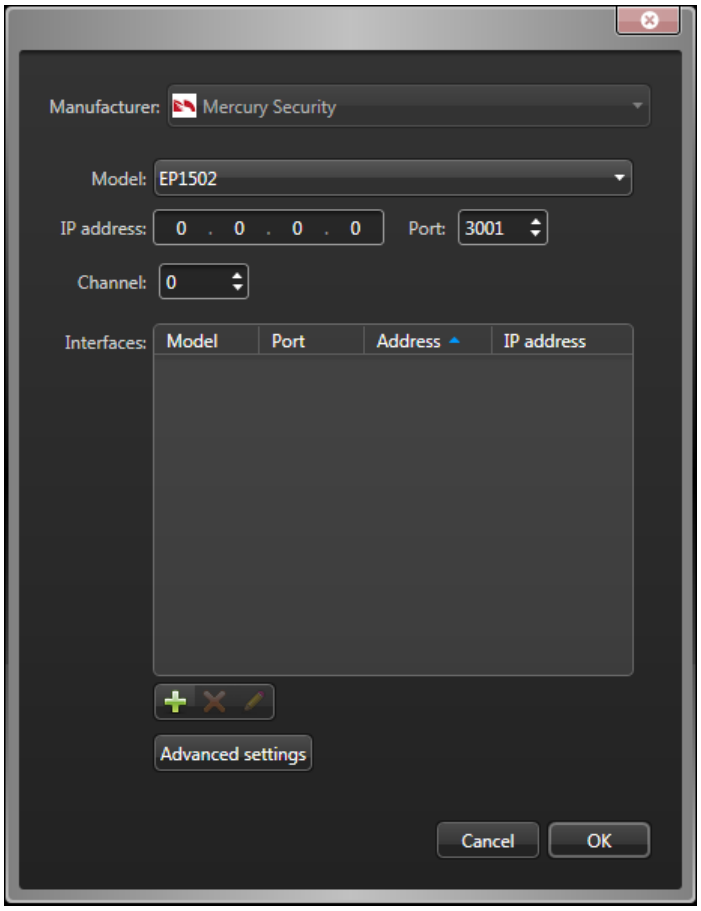
Synergis™部に、各 EP コントローラは、によってユニークなチャネル ID を割り当てなければなりません。すべての EP コントローラは Schlage デバイス（AD-300 と PIM400）が接続された RS-485 バスを持っています。同じ RS-485 バスに接続された各 Schlage デバイスは、固有の RS-485 アドレスを持っている必要があります。

Synergis™ユニットに Allegion Schlage ロックを登録するには：

1 設定ツールのホームページで、開きます *アクセス制御* 仕事。

2 クリック **役割とユニット**、その後、Synergis をクリック™ **単位**（ ）。

3 クリック **周辺機器**、[OK]をクリックします **アイテムを追加します。**（）。



4 次の情報を入力します。

- **モデル：** コントローラのモデル。
- **IP アドレス：** IT 部門によってコントローラに割り当てられた静的 IP アドレス。
- **ポート：** 通信ポート（デフォルト= 3001）。ポートは、Mercury デバイスマネージャの Web ページで構成されている値と一致する必要があります。
- **チャネル：** このコントローラに対応するチャネル ID。チャネル ID は 0 の間の任意の値とすることができますおよび 63、および Synergis™ユニット内で一意でなければなりません。割り当てられたら、それは変更してはいけません。

5 あなたの EP のコントローラに接続されている Allegion Schlage デバイスを追加します。

a) の下部には *インタフェース グループ*、クリックしてください **アイテムを追加します。** （）。

b) 表示されるダイアログボックスで、モデル（AD300 または PIM400）、ポート、およびアドレス（0〜31）を選択します。

c) （PIM400 のみ）低で、PIM400 に連結された第 1 のドア番号を入力して、カウント中に、PIM400 にリンクされているドアの数を入力します。

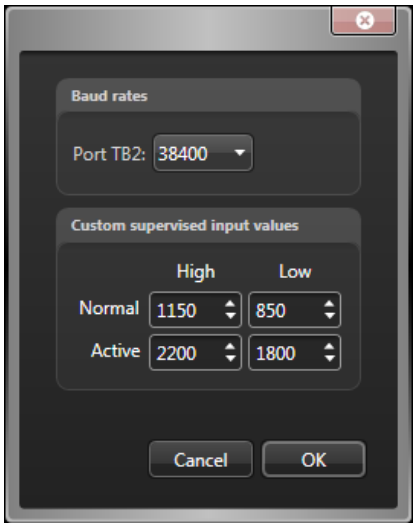
Low から低+カウントまでのすべてのドア番号は AD-400 ワイヤレスロックに対応している必要があります。

d) クリック **[OK]**。

e) 必要に応じて繰り返します。

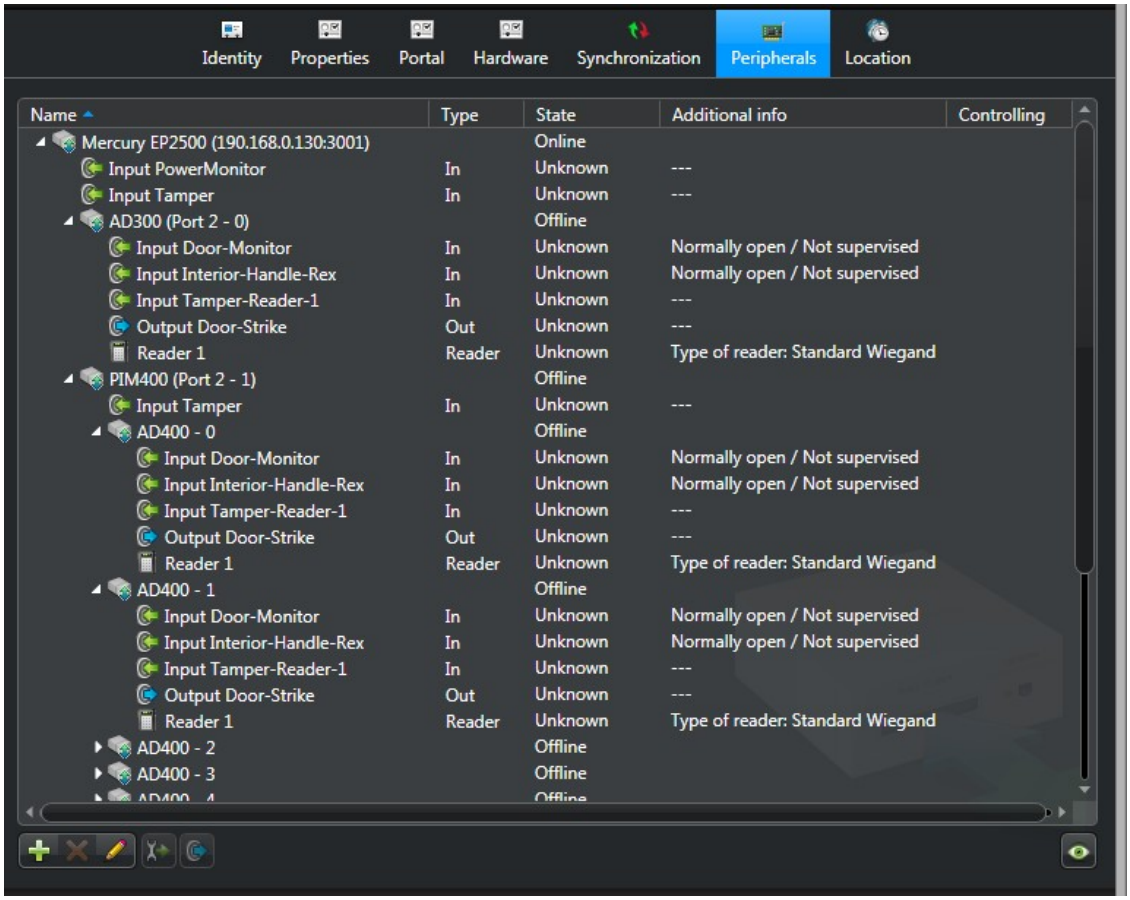
6 （オプション）をクリックして **高度な設定** 高度な設定を変更します。

使用可能な設定は、選択したコントローラのモデルによって異なります。あなたは一般的に使用可能なシリアルポートのボーレートを変更することができ、およびカスタムは、入力値を監修しました。



7 ダイアログボックスの下部にある[OK]をクリックします。

8 クリック **適用します**（✔）。
すべての添付の下流パネルと周辺機器との水銀コントローラに表示され
周辺機器 タブ。



注意： Synergis™ユニットにインターフェースモジュールを追加すると、ユニットは、ソフトウェアの再起動を実行させます。このプロセスの間に、Synergis™ユニットとそれに接続されているすべての周辺機器は、（赤）をオフラインで表示されます。

9 発見された I / O デバイスと読者のそれぞれを選択し、 そのプロパティを設定します 必要に応じて。
OSDP について（セキュアチャネル）の読者は、参照します EP コントローラに OSDP（チャネルセキュア）読者を追加 に 140 ページ。

10 入力と出力をトリガすることによって、あなたの配線と構成をテストします。
トリガーI / O は、画面上でリアルタイムに状態が変化します。
注意： リーダーの活動はに示されていません **周辺機器** タブ。

ENGAGE 統合 Allegion Schlage ロックを登録

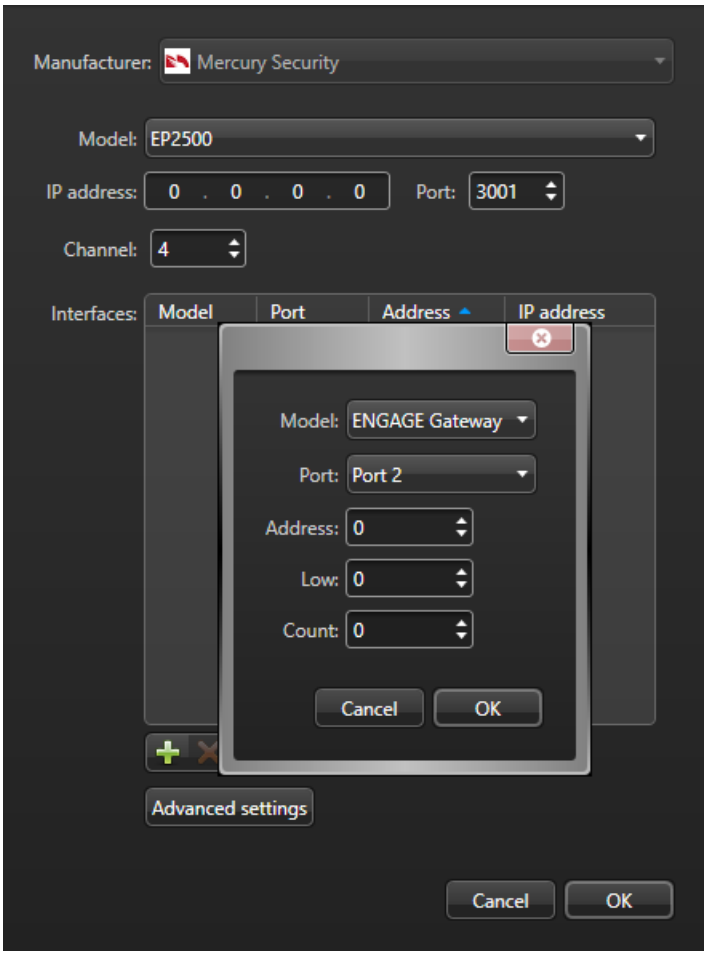
Schlage の ENGAGE プラットフォームは、資格情報がカードキーではなく、互換性のあるスマートフォンだけでなく保存することができます。統合は、水銀 EP1501 EP2500 やパネルを介して行われます。

あなたが始める前に

ENGAGE ゲートウェイへの初期設定とロックペアリングは、Android と iOS デバイスのために利用可能であるモバイルアプリを、ENGAGE Allegion を介して行われます。これは、その後、接続をタップ隅にプラス記号をタップし、手順に従って行われます。これが行われると、設定ツールでロックを登録します。

あなたは知っておくべきこと

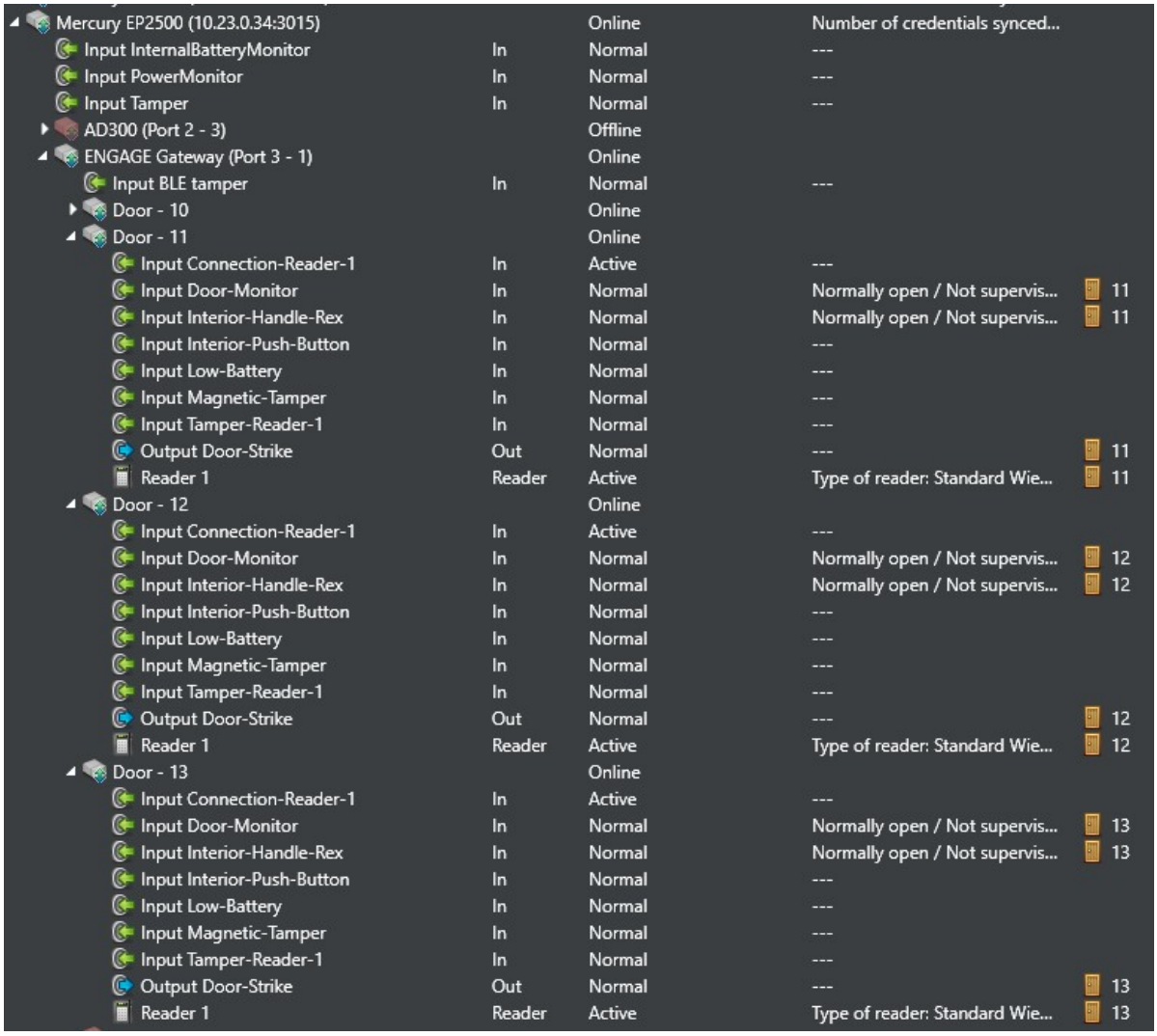
Allegion Schlage NDE と LE は、設定ツールで統合を ENGAGE とロック登録するためのプロセスでは、インターフェイスを設定するときにゲートウェイを ENGAGE 選択することを除いて、PIM400 の登録と同じです。



Synergis™ユニットに ENGAGE 対応 Allegion Schlage ロックを登録するには：

1 に記載されているように Allegion Schlage NDE または LE ロックを登録 上の登録 Allegion Schlage ロック Synergis™ユニット 15 ページ。

2 ステップ 5 で、から ENGAGE ゲートウェイを選択 **モデル** ドロップダウンメニューをクリックした後 **アイテムを追加します。** （ ） の中に *インタフェース グループ。*
に記載されているすべての接続された下流側パネルと周辺デバイスとゲートウェイと係合し
周辺機器 タブ。



3

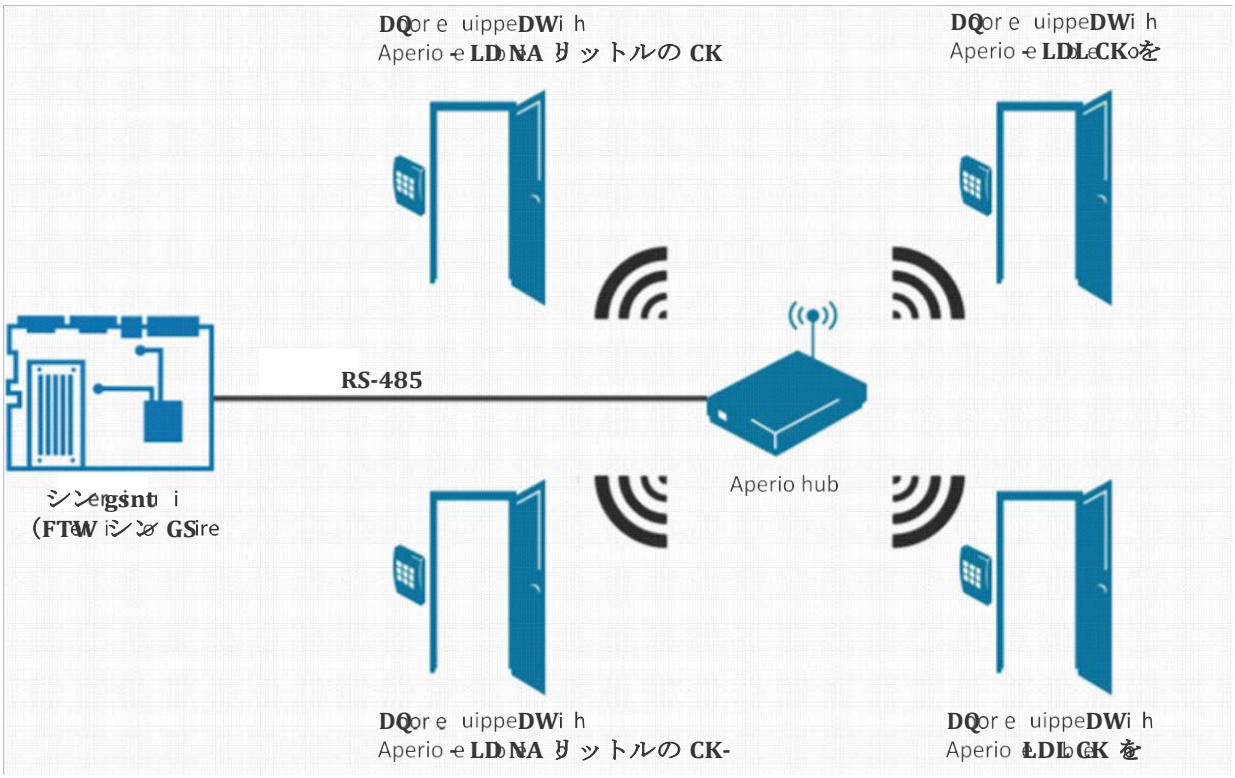
アッサ・アブロイアペリオ対応ロック

このセクションでは、次のトピックについて説明します。

Aperio integration

アペリオ対応のロックは、2.4GHz 帯のアペリオハブと通信無線ロックです。このハブは、その後順番に、RS-485 チャネル上で Synergis™ユニットと通信します。Synergis™ユニットは、すべてのアクセス制御を決定します。

次の図は、Synergis™ユニットは、アペリオ対応のロックとの通信方法を示しています。



Supported Aperio-enabled locks

アペリオの統合のために、Synergis™ユニットは、RS-485 チャネルの 1 つに接続された通信ハブを介しアペリオ対応ロックに接続します。各アペリオ対応のロックは、インタフェースモジュールと見られています。

Synergis™ Softwire は、以下のアペリオ対応デバイスをサポートしています。

モデル	説明	プラットフォーム	releaseCertification
A100	キーレスエントリー コントロール	-	デザインによってサポートされています
AH30	無線通信ハブ。各ハブは 8 つのアペリオロックまで制御します	3.4.0（V3） 1 2.6.6	認定 デザインによってサポートされています
AS100	ドア位置 センサー	-	デザインによってサポートされています
C100	シリンダーロック（ヨーロッパ モデル）	-	デザインによってサポートされています
E100	標準的な盾 RFID リーダー（欧州モデル）	- ートされています	デザインによってサポ
IN100 v3 **の IN100**	v3 の ロック -	3.5.0 -	認定 デザインによってサポートされています
K100	K100 内閣 ロック	-	デザインによってサポートされています
KS100	KS100 サーバーキャビネット ロック	-	デザインによってサポートされています
L100	電子ロックの RFID リーダー（欧州モデル）	-	デザインによってサポートされています
M100	ワイヤーフリー改修 ほぞ穴	-	デザインによってサポートされています
PR100 HF / LF	P100 高と低周波 ロック	2.6.6	デザインによってサポートされています
R100	表面実装型ワイヤレス リーダー	-	デザイン 1 によって

AH30 は、IN100 v3 のロックを操作するためのサポートされる最小バージョンをサポート 3.2.0 です

サポートされているアペリオ対応のロック機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™Softwire 10.6 には、以下のアペリオ対応のロック機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleElectronic	ロック
コミュニケーション protocolRS-485	[1]
暗号化されました communicationNo	[2]
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeYes	[3]
依存 modeNo	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン MODEN / A	
劣化 modeNo	
ワイヤレス操作	
上 Synergis™ユニットにお問い合わせください eventOn	読む
ポーリング間隔（v3 のロック のみ）はい	
スケジュールのラジオ接触（ステータスレポート インターバル）1	- 60 分。
電池 checksYes	
パワーロックの設定に失敗（フェイルセーフ/フェイル セキュア）いいえ	
スケーラビリティ	
オフラインの最大数 eventsN / A	
自律的意思決定のための資格証明書の最大数（ 作成）N / A	
（ビット単位）の最大長資格	256
RS-485 チャネルごとインターフェースモジュールの最大数	644
Synergis™単位あたりのインターフェイスモジュールの推奨最大数	64

[1] Synergis™ユニットとアペリオ無線通信ハブの間。

[2] 通信はアペリオハブとロックの間で暗号化することができます。

[3] アペリオ対応のロックはオフラインで作業 5 つの資格情報を保持することができます。

[4] 各チャネルは、8 つのハブをサポートし、各ハブは、チャネルあたり 64 のロックの最大のためには、8 つのロックをサポートします。Synergis™ユニットは、64 個のロックを制御している場合は、パフォーマンス向上のために、4 つのチャネルすべてに均等にロックを広げます。

Aperio-のためのサポート Synergis™アプライアンスの機能は、ロック統合を有効に

すべての Synergis™アプライアンスの機能は、アッサ・アブロイからアペリオ対応のロックの統合でサポートされていません。

アペリオ対応のロックの統合は、次のことをサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire* 特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）	
手動登録（*ハードウェアを追加* ダイアログ ボックス）はい	
自動登録（スキャン ボタン）はい	
プロパティ configurationLimited	[1]
コンフィギュレーション・クローニング（クローン ボタン）はい	
I / O の診断（入力、リレーのライブ監視、および 読者）はい	[2]
インタフェースモジュールのファームウェア displayHub	のみ
インタフェースモジュールのファームウェアのアップグレード（推奨適用します ファームウェア）いいえ	
アクセス制御の挙動（Synergis™ ユニット全体の設定）[2]	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）いいえ	
ドアがあるとき、「DHO」イベントを生成しません。 unrestrictedYes	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）はい	
数字の最大 PIN 長	154
デグレードモード 機能設定/ A	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）いいえ	

[1] 接続パラメータのみ。

[2] に設定された出力リレー *I / O の診断* ページによっては、すぐには反映されないことがあり **ステータスレポート間隔** そしてその **ポーリング間隔** （v3 のロックのみ）の設定。

[3] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

[4] 以下の 4 桁の PIN は受け付けておりません。

アペリオ対応のロックを統合するためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、アッサ・アブロイからアペリオ対応のロックの統合でサポートされていません。

アペリオ対応のロック統合には、以下のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeYes	
	拡張助成金 timeYes	
	入力時間（標準/拡張）なし	
	ドアリロック - optionsNo	
	ドアはスケジュールによってロックが解除された場合 - optionsYes	ドア
	開催します - optionsLimited	[1]
	ドアが開いて強制的に - optionsLimited	[1]
	アンロック schedulesYes	[2]
	（REX）のオプションを終了する要求	
	REX にロックを解除 いいえ（オン/オフ）	[3]
	アクセスを許可した後 REX を無視する時間（中 秒）はい	
	ドアが開いている間 REX イベントを無視（オン/オフ）はい	
	（ドアが閉じた後、REX を無視する時間 秒）はい	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒。）はい	
	ドア上の（オン/オフ）2 人のルールを強制します sideYes	
セキュリティ Desk4 ドアの手動アクション	手動 doorsv3 のロックを解除	ロックのみ
	シャント Reader は（有効化/無効化 読者）はい	
	オーバーライドロック解除 schedulesYes	[2]

特徴 groupSecurity	センター featureSupported
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン、オフライン*）はい
	交流 failN / A
	バッテリーは（失敗しますローバッテリー）はい
	ドア オープン/ closedYes
	ドア ロック/ unlockedYes
	ドアの強制 openYes
	ドアはあまりにもオープン開催しました longYes
	ドア securedN / A
	デッドボルト（*確保し、リリース*）はい
	キー overrideYes [5]
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理） は いビジター護衛ルール（オンオフ） は
	い
	InterlockNo
	Antipassback
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）はい [6]
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）はい
	両方のエリアの入り口にチェックを厳格（antipassback と 出口）N / A
	に scheduleYes
	グローバル antipassbackYes
	一人称-内のルール
	ドアアンロックに強制 scheduleYes
	アクセスに施行 rulesYes
エレベーター コントロール	エレベー
ター	N / A
ゾーン管理	I / O zoneNo
	ハードウェア zoneNo

[1] ザ・ **リーダーのブザーの動作** オプションがサポートされていません。

[2] アップデートが依存します **ポーリング間隔** （V3 ロック）または **ステータスレポート間隔** （V3 ロック以外）。

[3] オプション **自動的 REX を付与** 常にに設定する必要があります **オフ** 設定ツールインチ

[4] Synergis™ユニットは、Access Manager に接続する必要があります。

[5] すべてアペリオ対応の口ックは、キーオーバーライドセンサーをサポートするわけではありません。各モデルでサポートされている正確なセンサーを知るためにメーカーに確認してください。

[6] エリア内のカード所有者の存在は確認できませんので、カードイン/ REX-アウトドアにはお勧めしません

ハブとアペリオ対応のロックをペアリング

あなたは Synergis™ユニットのアペリオ対応のロックを登録する前に、アペリオ· プログラミング· アプリケーション（APA）を使用して、ハブとアペリオ対応のロックをペアリングする必要があります。

あなたが始める前に

あなたは次のことを持っていることを確認してください：

- **アペリオオンラインプログラミングアプリケーションマニュアル。** すべてのアペリオアプリケーションのインストールと使用のための取扱説明書。
- **アペリオ・プログラミング・アプリケーション（APA）。** 主な用途は、アペリオハブとロックを設定するために使用します。ハブとロックの両方が無線接続を介して構成されています。
- **USB ドングル。** APA を実行しているコンピュータに接続する必要がありますハードウェアデバイス。
- **TriBee ブートローダ。** USB ドングルドライバが含まれています。
- サポートされているファームウェア
- APA を実行するためのコンピュータ。
- （ロックペアリングを活性化するために使用）ロックのリーダーと互換性のあるカード。カード上の資格は、セキュリティセンターに登録する必要はありません。

ハブとアペリオ対応のロックをペアにするには：

1 DIP スイッチを使用してハブに -（15 1）EAC アドレスを設定します。

重要： 8 つのハブまでのデイジーチェーンの同じ RS-485 チャネルに接続することができますが、各ハブは異なる EAC アドレスを使用する必要があります。

2 ハブの電源をオンにします。
3 お使いのコンピュータに USB ドングルを差し込みます。
4 インストール *TriBee ブートローダ*（USB ドングルドライバをインストール）。
5 インストール *アペリオプログラミングアプリケーション*（APA）。
6 オープン APA（参照 *アペリオオンラインプログラミングアプリケーションマニュアル* 手順については）。利用可能な機能を示すために、通信ハブ、ロック、またはセンサーを右クリックします。
7 APA を使用して、ハブとロックのファームウェアを更新。

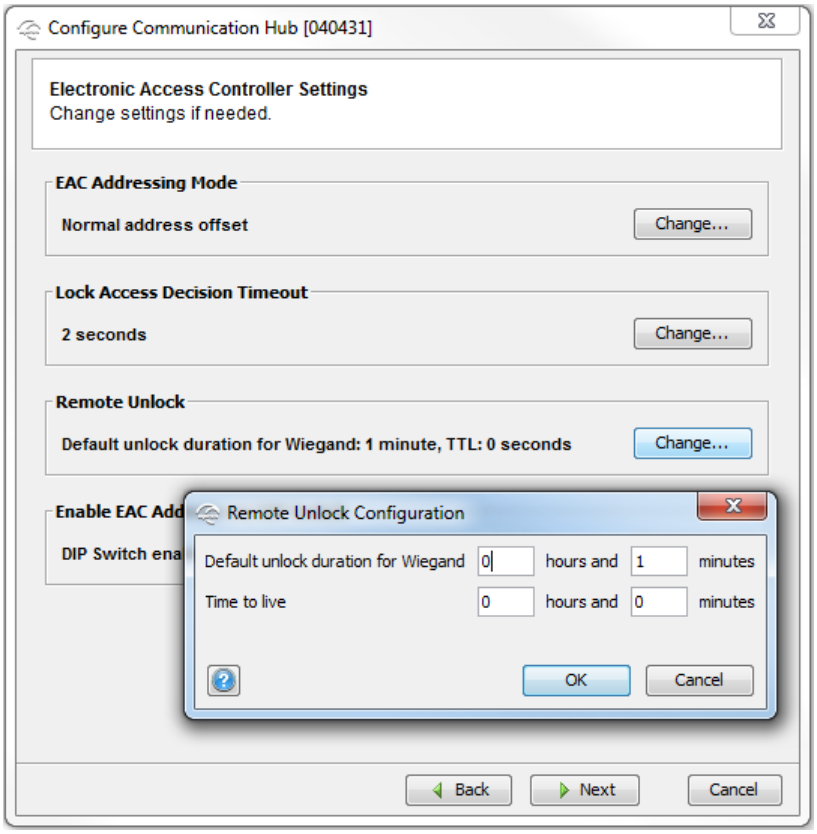
チェック サポートされるファームウェア ファームウェアを更新する前にリスト。

ベストプラクティス： 必ずロックやセンサーをアップグレードする前に、通信ハブをアップグレードします。アドレッシング EAC のための DIP スイッチを使用する AH30 通信ハブをアップグレードする場合は、必ず DIP スイッチが正しい EAC アドレスに設定されていることを確認してください。DIP 5（ペアリングモード）をアップグレード中にアクティブに設定されている場合は、通信ハブは異なる EAC アドレスを使用して開始します。

8 ハブを設定します。
9 （以前の 2.6.5 よりファームウェアとの通信ハブ）を使用してリモートロック解除オプションを有効にします セキュリティセンターは、スケジュールのロックを解除します。

ファームウェアバージョン 2.6.5 以降では、リモートロック解除オプションはデフォルトで有効になっています。

10 値を入力します **有効期間** の中に *リモートロック解除の設定* ダイアログボックスとクリック **[OK]**。



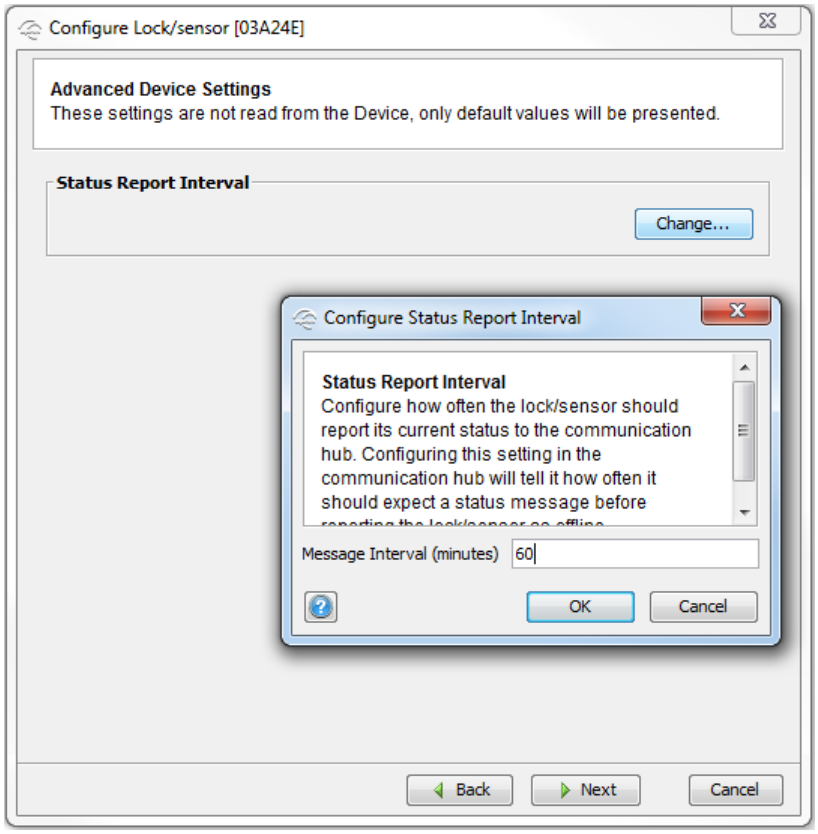
この時間は、リモートロック解除コマンド（grantAccessSequence）は、通信ハブに存在している期間を示します。この設定は、常にレポート間隔は、ロックに設定された状態よりも長くなければなりません。

あなたは、の値を無視することができます **ウィーガンドのデフォルトのロック解除期間**。

11 **15 分 - アンロックスケジュールが使用されている場合（V3 ロックを除く）、範囲 5 においてステータスレポート間隔の値を入力します。**

ザ・ **ステータスレポートの間隔** 通常は 60 分に設定されています。状況インターバル時間の減少を下げます製品のバッテリ寿命。なぜなら**ステータスレポートの間隔** 通信で使用され
ロックがオフラインになった場合には、この間隔の変更は、ロックや通信ハブの両方で行う必要がありますが検出するハブ。1 つのロックのみが通信ハブとペアリングされている場合、これは自動的に行われます。複数のロックが通信ハブとペアリングされている場合は、通信ハブを介してステータスレポートの間隔を設定する必要があります。ハブを右クリックして、同等またはペアロックの最長のステータスレポートの間隔よりも大きい値を設定してください。

注意： v3 のロックと、 **ステータスレポートの間隔** 設定はロックのオンラインステータスを報告するために使用されます。それはです**ポーリング間隔** それは、ロック解除スケジュールの開始と終了のためのタイムラグを最小限にするために使用されています。



複数のロックが通信ハブとペアリングされている場合は、ステータスレポートの間隔もロックを設定する必要があります。

12 各ワイヤレスロックについては、次の手順を実行します。

a) 右クリックし、**通信ハブ > ロックやセンサーとのペア**。ペアリングプロセスが開始されます。

b) ロック時に証明書を保持する、または通信ハブとハードウェアをペアリングするためのセンサ用磁石と係合します。

ハブは自動的にロックに EAC アドレスを割り当てます。

c) ロックに割り当てられた EAC アドレス（1〜127）を書き留めます。

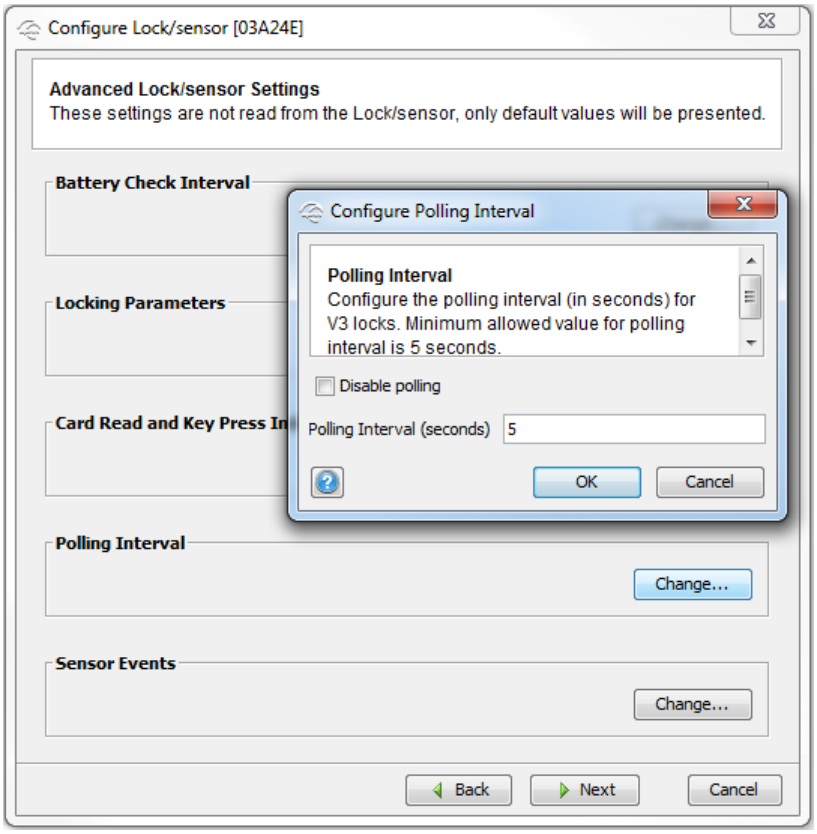
ハブの EAC アドレスがロックの EAC アドレスに組み込まれています。ロックの EAC アドレスからハブの EAC アドレスを取得するには、次の式を使用します。

ハブの EAC アドレス=ロックの EAC アドレス モジュロ 16 若しくは

ハブの EAC アドレス=（の残りの部分 *ロックの EAC アドレス*）で

割った 16 13（V3 ロックのみ）設定 ポーリング間隔 5 秒（最小時間）まで。

これは、反応を減少させる、ロック解除スケジュールを開始および終了するためのタイムラグを最小にすることです
ロックの時間。また、マニュアルは 5 秒以内に仕事にセキュリティデスクから発行されたコマンドのロックを解除することができます。コマンドのみ（ステータスレポートの間隔に応じて）1 分以上後に動作するため、v3 の以外のロックを手動でロック解除コマンドを使用することは推奨されません。



すべてのロック後 14 が対になっている、安全な無線通信（顧客モード）を使用するようにハブを設定。

あなたが完了した後、

Synergis™ユニットのロックを登録。

アペリオ対応のロックを登録

Synergis™ユニットは、アペリオ対応のロックと通信するためには、Synergis™アプライアンスポータルでそれらを登録する必要があります。

あなたが始める前に

- ハブにアペリオ対応のロックをペア。
- 次のように RS-485 のチャネル（A、B、C、又は D）のいずれかにハブを接続します。
  - チャンネルの「+」にハブの A コネクタを接続します。
  - チャンネルの「 - 」にハブの B コネクタを接続します。

アペリオ対応のロックを登録するには：

1 Synergis™ユニットにログオンします。
2 クリック **コンフィギュレーション > ハードウェア**。
3 の上部には *ハードウェア*列、クリックしてください **加えます** （）。
4 の中に *ハードウェアを追加* 選択]ダイアログボックスで、 **アペリオ** として **ハードウェアの種類**。
5 を選択 **チャネル** （A、B、C、または D）。
6 選択 **アペリオ** として **インタフェースモジュールタイプ**。
7 **あなたが登録したいのロックを指定します。**

あなたは、自動または手動でロックを登録することができます。

先端： あなたがロックの EAC アドレスを知っているし、あなただけ登録する数を持っている場合は、それらを手動で登録した場合、それはより速くなります。

次のいずれかを実行します。

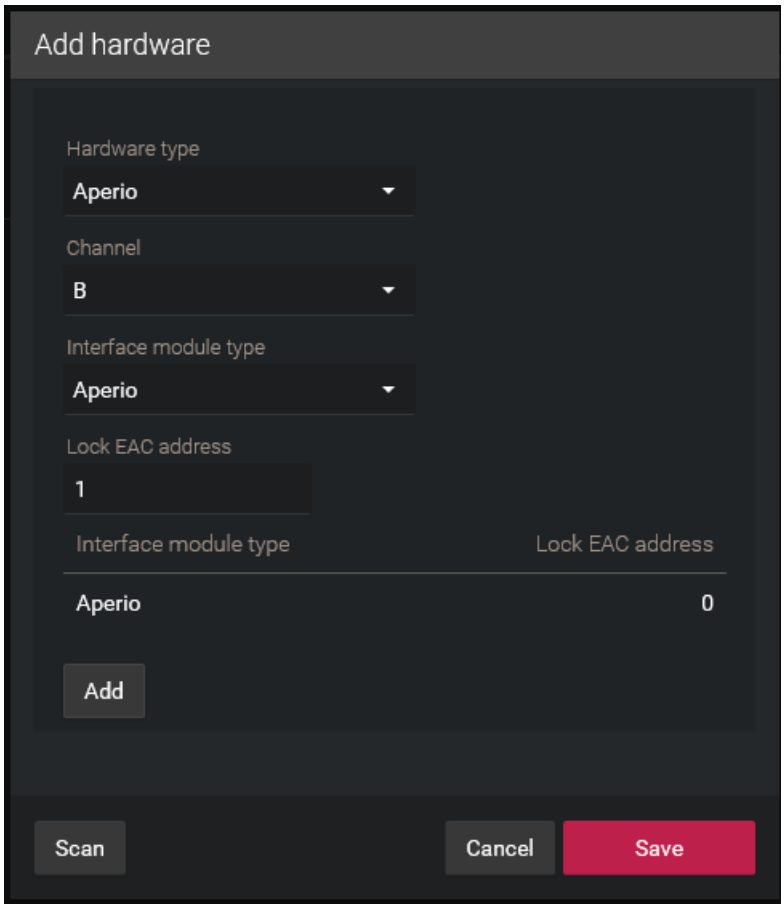
- 自動的に登録するには、[スキャン]をクリックします。

  スキャン機能は、同じチャネルに接続されている同じ製造者からのすべてのインターフェース· モジュールを検索し、登録します。

  Synergis™アプライアンスポータルが接続されているすべてのインタフェース· モジュールが見つからない場合は、手動登録をしてみてください。

- ロックの EAC アドレスを入力し、手動で登録する（1 127）、一方を書き留め にロックをペアリング ハブ、[追加]をクリックします。

同じチャネルに接続されたすべてのモジュールを構成するために、必要に応じて繰り返します。



8 クリック **セーブ**。
追加したばかりのハードウェアタイプ、チャネル、およびインタフェース・モジュールは、に表示されます *ハードウェア構成*
ページ。

9 右側のペインにそのプロパティを表示するために口ッ
クを選択します。ハブのロックの EAC アドレスの両
方が示されています。

10 ページの下部に、[保存]をクリックします。

11 I / O の診断ページからごインターフェイスモジュールの接続と設定をテストします。
インターフェイスモジュールのテストについては、以下を参照してください *Synergis™ アプライアンスの設定ガイド*。

あなたが完了した後、

- Synergis を登録™ セキュリティセンターでのユニット（参照 *Synergis™ アプライアンスの設定ガイド*）。
- アペリオ対応のロックを装備したドアを設定します。

アペリオ対応のロックを装備した構成のドア

あなたは重複を受けていないことを確認します *ドアロック*そして *ドアロック解除* セキュリティデスクでのイベントは、あなたが設定する必要があります。 **自動的 REX を付与** アペリオ対応のロックを装備したすべてのドアのために OFF にオプション。

あなたが始める前に

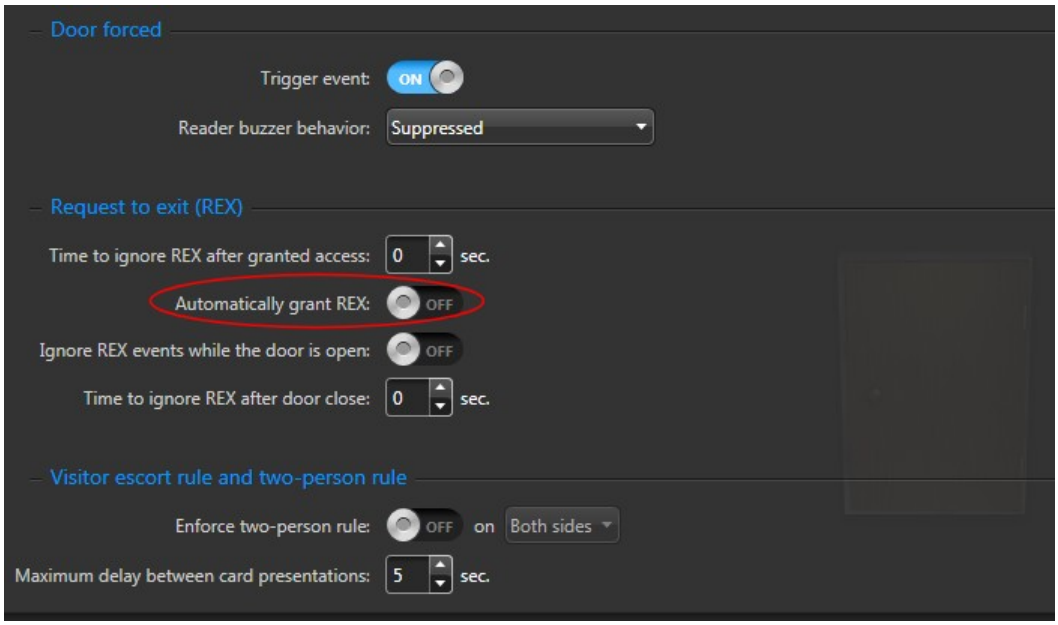
- Synergis™ユニットにアペリオ対応のロックを登録。
- Synergis を登録™ セキュリティセンターでのユニット（参照 *Synergis™ アプライアンスの設定ガイド*）。

あなたは知っておくべきこと

アペリオ対応のロックは、機械的 REX を使用しています。これは、REX がトリガされたとき、ドアの解錠を制御 Synergis™単位ではありません。ドアの設定でこのオプションを有効にすると、ドアがロックされ、ドアロック解除のイベントがセキュリティデスクで二回受けられるようになります。

アペリオ対応のロックを装備したドアを設定するには：

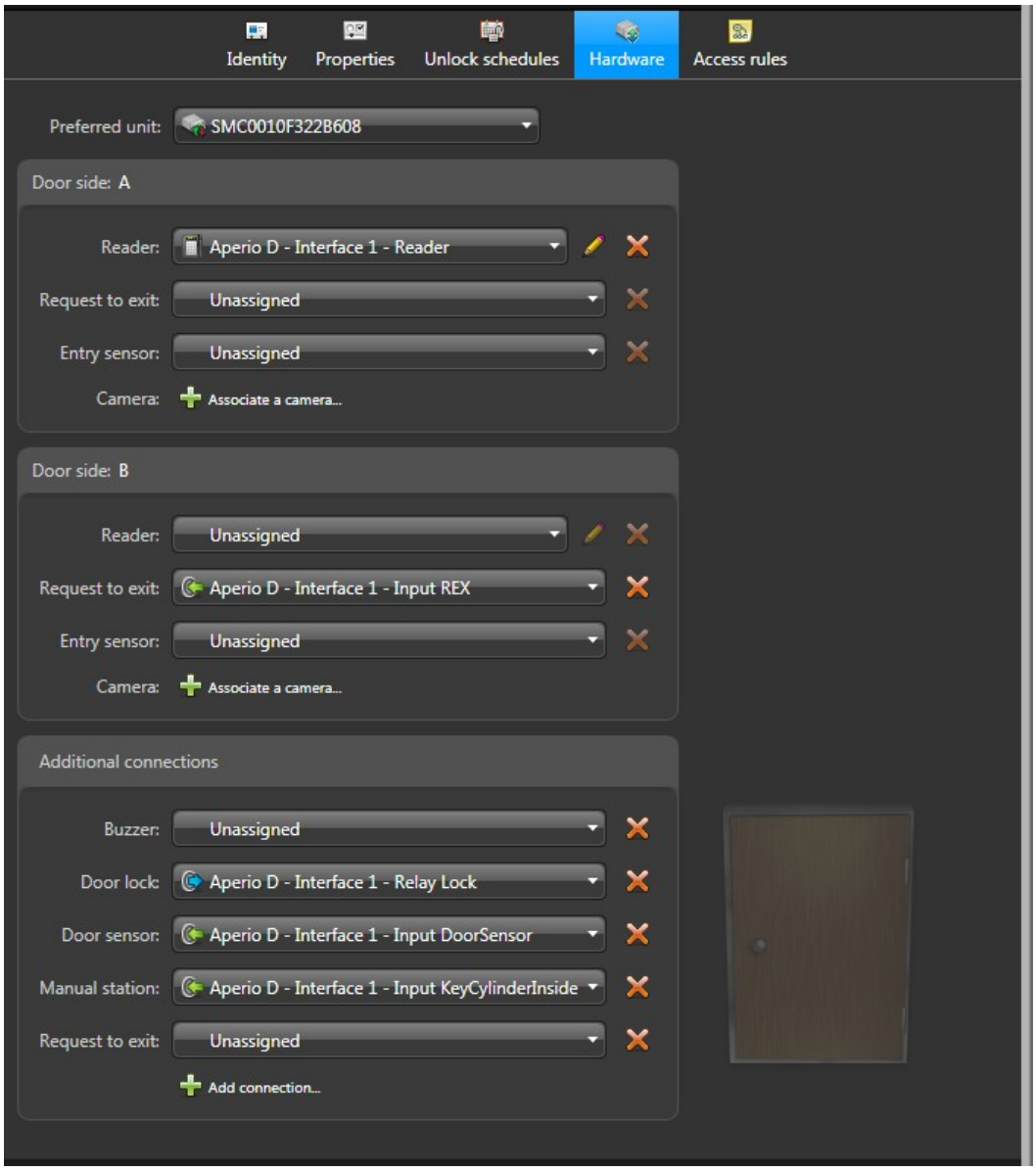
1 設定ツールでセキュリティセンターに接続します。
2 エリアビュータスクでは、アペリオ対応のロックを使用しているドアを選択します。
3 を選択 **プロパティ** タブ。
4 下 *リクエストが終了する（REX）* セクション、セット **自動的 REX を付与** に **オフ**。



5 [ハードウェア]タブを選択し、ロックを制御 Synergis™ユニットを選択します。

先端： 同じロックに対応するすべての周辺機器は、同じ接頭辞「アペリオ X - インタフェース N」と命名され、X はチャンネル名（A、B、C、または D）であり、そして n ロックの EAC アドレスです。

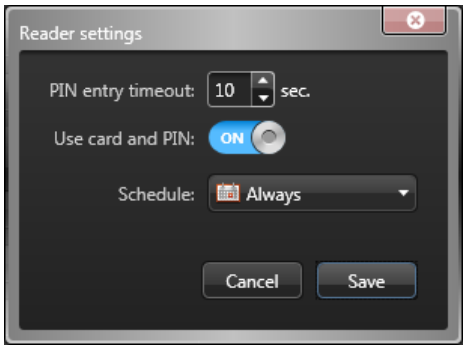
6 ドア入口側に、ドアに対応するリーダを割り当てます。
7 ドアの出口側に、ドアに対応 REX センサを割り当てます。
8 下 **追加の接続**、
   - にロックリレーを割り当てます **ドアロック**、および
   - への扉センサ入力を割り当てます **ドアセンサー**。
   - 割り当てます *KeyCylinderInside* または *KeyCylinderOutside* に **マニュアル駅**、 該当する場合。



9 読者は「カードと PIN」モードで動作するべき場合には、必ず PIN を入力するカード保有者のために十分に長いタイムアウトを設定します。

5 秒のデフォルトのアクセスのタイムアウトはアペリオ対応のロックのための十分な長さではありません。ドアに自分の証明書を提示した後、カード所有者は、LED は、PIN を入力する前に緑色に変わるまで待たなければなりません。このプロセスは、必ず 5 秒以上かかります。

1 クリック **リーダーの設定**（）の横に **リーダー**。
2 の中に *リーダーの設定* 設定ダイアログボックスで、 **カードと PIN を使用します** に に
3 をセットする **PIN 入力のタイムアウト** 所望の期間に（私たちは 10 秒をお勧めします）。



4 クリック セーブ。

10 [適用]をクリックします（ ） 変更を保存します。

4

アッサ・アブロイ IP ロック

このセクションでは、次のトピックについて説明します。

Supported Assa Abloy IP

アッサ・アブロイ IP ロック統合のために、各 IP ロックは、インターフェースモジュールと見なされます。Synergis™Softwire は以下アッサ・アブロイ IP ロックをサポートしています。

ブランド	名	タイプ	サポートされているファームウェア
コービン Russwin	アクセス 700 PIP1（ピクセル）	PoE 対応	デザインによってサポートされています
コービン Russwin	アクセス 700 PIP1（Cx の）	PoE 対応	デザインによってサポートされています
コービン Russwin	アクセス 700 PWI1（Cx の）	Wi-Fi	3_0p05_cx_v2751
コービン Russwin	アクセス 700 PWI1（ピクセル）	Wi-Fi	デザインによってサポートされています
コービン Russwin	アクセス IP1 800（SX）	PoE 対応	デザインによってサポートされています
コービン Russwin	アクセス 800 WI1（SX）	Wi-Fi	デザインによってサポートされています
コービン Russwin	IN120（Cx を） （インストール手順）	Wi-Fi	デザインによってサポートされています
コービン Russwin	IN220（Cx を）	PoE 対応	デザインによってサポートされています
SARGENT	IN120（Cx を） （インストール手順）	Wi-Fi	3_0p05_cx_v2751
SARGENT	IN220（Cx を）	PoE 対応	3_0p05_cx_v2751
SARGENT	パスポート 1000 年 P1（Cx の）	PoE 対応	3_0p05_cx_v2751
SARGENT	パスポート 1000 年 P1（ピクセル）	PoE 対応	3_0n18_px_pfm
SARGENT	パスポート千 P2（Cx を）	Wi-Fi	デザインによってサポートされています
SARGENT	パスポート千 P2（ピクセル）	Wi-Fi	3_0n18_px_pfm
SARGENT	プロフィールシリーズ v.S1（SX）	PoE 対応	3_0n18_sx_pfm、3_0n18_hx_pfm[1]
SARGENT	プロフィールシリーズ v.S2（SX）	Wi-Fi	3_0n18_sx_pfm、3_0n18_hx_pfm[1]

[1] Hx のファームウェアを実行しているの Sx コントローラはオプションが必要です **ファームウェアのタイプ** に設定します **HX** の中に *ハードウェア* **設定ツールで** Synergis™ユニットのタブ。

サポートされているアッサ・アブロイ IP ロック機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™ Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™ Softwire 10.6 には、以下のアッサ・アブロイ IP ロック機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleIntelligent	ロック
コミュニケーション protocolIP	
暗号化されました communicationYes	
参照（エスケープモードを返します 有効にする方法）はい	
通過モード（参照 有効にする方法）はい	
プライバシーモード（参照 有効にする方法）はい	
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeYes	1
依存 modeNo	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン modeYes	
劣化 MODEN / A	
ワイヤレス操作（無線 LAN のみ）	
上 Synergis™ユニットにお問い合わせください eventYes	2
スケジュールのラジオ接触（ステータスレポート インターバル）はい	3
電池 checksYes	4
電源は、はい（フェイルセーフ/フェールセキュア）ロックの設定に失敗します	5
設定可能なラジオウェイクアップイベント（参照 どのように構成する方法）はい	
スケーラビリティ	
オフラインの最大数 events10,000	6
自律的意思決定のための資格証明書の最大数（ メイキング）万	7
（ビット単位）の最大長資格	140

FeaturesSupported	
RS-485 あたりのインターフェイスモジュールの最大数 channelN / A	
Synergis™単位あたりのインターフェイスモジュールの推奨最大数	128

[1] WiFi のロックは、まだロックに同期していない未知の資格情報のロックを解除するために 15 秒かかる場合があります。二度目にバッジを付けることが必要になる場合があります。

[2] デフォルトでは、WiFi のロックは、連絡先 Synergis™ 次のイベントの単位： *アクセスが拒否されました*（何らかの理由で）、 *ドアが開いて強制的に*、および *あまりにも長いオープンドア*。

[3] デフォルトの WiFi 無線機は、スケジュールが午前 0 時 UTC 時刻に毎日です覚まします。

[4] デフォルトのバッテリーチェックのスケジュールは、午前 23 時 UTC 時刻に毎日です。

[5] デフォルトの電源は、電源がオフのとき、ドアがロックされている意味、ロック設定がセキュア失敗で失敗します。

[6] オフラインログエントリとセキュリティセンターのイベントの間に 1 対 1 のマッチが常にありません。

[7] CX のタイプのロックのみ。レガシーの Sx と Px のタイプのロックは 2400 の資格情報のままです。レガシーPx のロックはカードと PIN のために設定されている場合、容量が 1200 の資格情報に低下します。

ラジオウェイクアップイベントはアッサ・アブロイの WiFi ロックの機能について

ウェイクアップイベント あなたはロックがすぐに無線 LAN の電波を介してコントローラに報告しなければならないイベントを選択することを可能にするすべてのアッサ・アブロイの WiFi ロックに関する設定可能な機能があります。

必要条件

最低限必要なファームウェアは Synergis™Softwire 10.2 SR1 です。

使い方

デフォルトでは、ドアが開いて強制し、ドアオープンが長すぎるイベントは、彼らが発生したときに、これらのイベントを報告したロックの WiFi 無線機を覚まします。無線 LAN の電波を覚ますイベントを選択するために、個々のロックオンウェイクアップイベントのオプションを使用します。無線 LAN の電波を覚ますために選択されていないイベントは、次の WiFi ラジオウェイクアップで報告されています。

WiFi のロックのバッテリの使用量を最小限にする方法

ロックが WiFi 電波を覚ますオープンイベントを開催し、多くのドアを生成しているため、一部のインストールでは、ロックが短いバッテリ寿命を持つことができます。ドアを報告して許容できる場合、そのバッテリーの寿命を延ばすことができ、次のスケジュールや予定外のラジオ・ウェイクアップのオープンイベントを開催しました。バッテリ寿命を延長するには、開いているだけで強制的にドアにこれらのロックのためのウェイクアップイベントのオプションを設定します。ドアの強制開かれたイベントは、WiFi 無線機を覚ますと、ドアには、次の WiFi ラジオウェイクアップで報告されているオープンイベントを開催しました。

ラジオウェイクアップイベントを設定すると、アッサ・アブロイの WiFi ロックを備えています

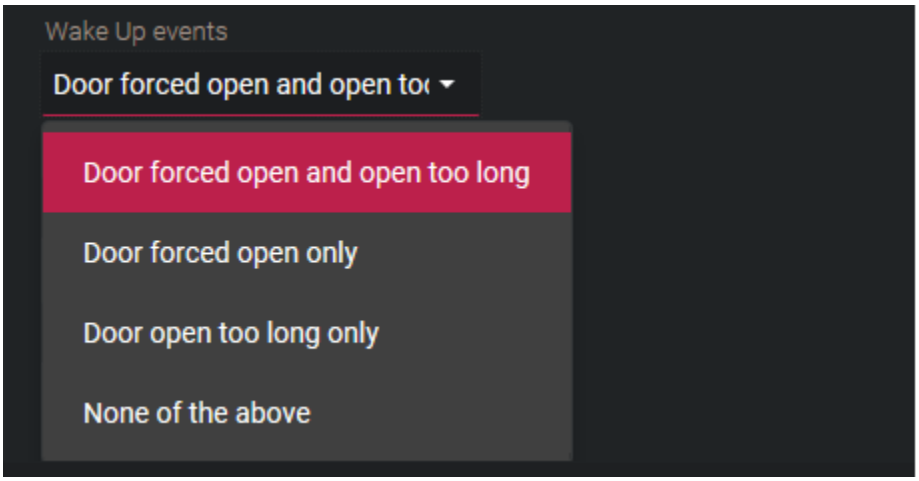
あなたは、特定のウェイクアップイベントでの Wi-Fi 電波を介してコントローラに連絡するために、個々のアッサ・アブロイの WiFi ロックを設定することができます。

あなたが始める前に

アッサ・アブロイ IP ロックを登録。

あなたは知っておくべきこと

あなたは、設定することができます ウェイクアップイベント 各アッサ・アブロイの WiFi ラジオロックのため。



ラジオウェイクアップイベントを設定するには：

1 Synergis™ユニットにログオンします。
2 クリック コンフィギュレーション > ハードウェア。
3 アッサ・アブロイ IP を選択し、アッサ・アブロイチャネルとロックを選択します。
4 をセットする ウェイクアップイベント ロックのためのオプション。
5 クリック 適用します

ボディタイプ 8200 とアッサ・アブロイ IP ロックにエスケープし、復帰モードを有効にすると、デッドボルトを監視し

アッサ・アブロイ IP ロックによって制御ドアにエスケープとリターンモードを有効にするには、ドアの脱出に戻るという名前のブール型のカスタムフィールドを作成し、あなたはこの機能が有効になっているにしたいドアを TRUE に設定する必要があります。

あなたが始める前に

この機能は、Synergis™Softwire 10.5 GA 以降が必要です。

エスケープとリターン機能をサポートアッサ・アブロイ IP ロックは、ロック本体 8200 を搭載したモデルで、デッドボルトを監視しました。

例えば：

- IN120 及び IN220 8200 デッドボルトとモティスロック。他の IN120 及び IN220 ロックは、この機能をサポートしていません。
- パスポートデッドボルト 1000 P2 のモティスロック。他のパスポート千 P2 ロックは、この機能をサポートしていません。

あなたは知っておくべきこと

カナダの火災コードは、ドアは決して「自動的に再ロック」できると述べています。エスケープとリターン機能が有効になっている場合そのため、以下の機能が無効になっています。

- スケジュールのロックを解除
- メンテナンスモード
- セキュリティデスクから手動ロック解除

- 一時的にセキュリティデスクからスケジュールを上書き

エスケープとし、カード所有者がドアを通って出て行くとき、機能が有効になって戻る、カード所有者がドアをロックするために彼らのアクセスカードを提示するまで、それが閉じた後、ドアはロック解除のまま。カード保有者は、ドアをロックするために自分のカードを提示しない場合、彼らはなくなっている一方で、ドアはロック解除のまま。カード保有者が戻ったとき、彼らはドアを開くために彼らのアクセスカードを提示する必要があります。彼らは入力した後、彼らはドアをロックするデッドボルトをスロー する必要があります。

エスケープとリターン機能を有効にするには：

1 ドアエンティティのためのブール型のカスタムフィールドを作成し、それはリターンをエスケープ名前を付けます。

あなたはそれが書かれているよう大文字と小文字で、まさに名前のスペル、スペースを含める必要があります。

2 エリアビューのタスクを開き、この機能を有効にする必要があり、全てのドアのために TRUE にエスケープ戻りカスタムフィールドを設定します。

先端： あなたは多くのドアを有効にこの機能が必要な場合は、我々は、使用をお勧めします *コピー設定ツール*。

3 （WiFi のロックのみ）トリガラジオは、エスケープを有効にし、ロックオン機能を返すように目を覚ます。

あなたは、ロックのカバーを外すと、ボタンを押すか、拒否された証明書を提示することで、無線ウェイクをトリガすることができます。

4 エスケープを通過し、ドアから出てくることで、ドアが閉じた後、有効な資格情報を提示することによって、初めてモードサイクルを返します。

これは、イベントとアクションを設定するために使用できるカスタムイベントを作成するためのシステムを引き起こします。

2 つのカスタムイベントは、あなたのシステムに追加されます。

- **リターンモードスタートをエスケープ：** 退出するか、有効な資格情報を持つエントリによってアンロックドア。
- **リターンモードの終了をエスケープ：** ドアは、有効な資格情報またはドアの内側からデッドボルトを投げによってロックされています。

アッサ・アブロイ IP のロックを通過モードを有効にします

アッサ・アブロイ IP ロックによって制御ドアに通過モードを有効にするには、ドアのため PassageMode という名前のブール型のカスタムフィールドを作成し、あなたは、この機能が有効になっているにしたいドアを TRUE に設定する必要があります。

あなたは知っておくべきこと

パッセージ・モードは、すべてアッサ・アブロイ IP ロックで利用できる機能です。この機能は、自分の資格情報を提示することによって、アンロック状態でロックを維持するための任意の認可カード保有者が可能になります。ロック制御部とロックブランドによっては、カード保有者は、一度か二度自分の資格情報を提示する必要があります。プロセスを繰り返すことは通常の状態にロックを返します。

読者の中にあるとき、通過モードを開始または停止するには *カードまたは PIN*、または *カードと PIN* モードは、次のいずれかを実行します。

- **単一バッジ付きの通路モード：** SARGENT とコービン Russwin IN120 及び IN220：以下は、すべての Sx ロックと、次の Cx ロックに適用されます。

  注意： いつ *プライバシーモード*有効になっています、 *通過モード*単一のバッジを持つカード保有者のために動作しません。 *安全検査* 7 より低い値。

  - **カードまたは PIN：** どちらのバッジは、一回または通過モードを開始するには PIN を入力してください。
  - **カードと PIN：** 最初のバッジ、次に通過モードを開始するには PIN を入力してください。
- **ダブルバッジ付きの通路モード：** PERSONA シリアル番号 SARGENT パスポート 1000 年 P1 と P2、コ

ービン Russwin アクセス 700 PIP1 と PWI1、サージェントとコービン Russwin IN120 及び IN220 ロック：以下はすべての PX ロック、Sx をロック Hx のファームウェアを実行し、次の Cx ロックに適用されます。IN120 及び IN220 ロックが注文したか、手動で設定することができます。以下の手順を参照してください。

1 ワークステーションに接続されたロックで、LCT ツールを使用したロック設定ファイルを開きます。

2 から **ロックの設定** タブ、[設定]アイコンをクリックしてください。
3 クリック **シリアル番号の設定** タブ。
4 変更 **メーカー** そして **基板タイプ** に *ペルソナ*。
5 **変更を適用し、画面の指示に従ってください。ロックは現在、新しいシリアル番号を持っています。**
6 LCT を使用して、ロックに設定を再適用します。
7 **ロックがすでに Synergis™ユニットに追加された場合は、設定ツールで次の手順を実行します（１）、ロックを削除し、新しいシリアル番号を使用して、それを再度追加。（２）新しいロックとドアのエンティティのハードウェアを再設定します。**

- **カードまたは PIN：** バッジは二回通過モードを開始します。PIN を使用することはできません。
- **カードと PIN：** 最初のバッジ、その後、PIN を入力してください。バッジは再び通過モードを開始します。

パッセージモードスタート：通過モードが起動される最初の時間は、それは、システム内の 2 つのカスタムイベントを作成します
そして *パッセージモード終了*あなたは、イベントとアクションを設定するために使用することができます。

通過モード機能を有効にするには：

1 **ドアエンティティのためのブール型のカスタムフィールドを作成し、それが PassageMode 名前を付けます。それが書かれているのようにして、大文字と小文字を正確に名前を綴る必要があります。**
2 **エリアビューのタスクを開き、この機能を有効にする必要があり、全てのドアのために TRUE に PassageMode カスタムフィールドを設定します。**
先端： あなたは多くのドアを有効にこの機能が必要な場合は、我々は、使用をお勧めします *コピー設定ツール*。

監視対象デッドボルトなしアッサ・アブロイ IP ロックのプライバシーモードを有効にします

アッサ・アブロイ IP ロックによって制御されるドアの設定ツールからプライバシーモードを有効にするには、ドアのプライバシーモードという名前のブール型のカスタムフィールドを作成し、あなたは、この機能が有効になっているにしたいドアを TRUE に設定する必要があります。

あなたが始める前に

この機能は、Synergis™Softwire 10.5 GA 以降が必要です。

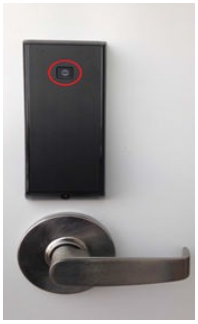
プライバシーモードをサポートしてアッサ・アブロイ IP ロックは、CX-タイプ PoE および WiFi のロックです。

注意： いつ *プライバシーモード*有効になっています、 *通過モード*単一のバッジを持つカード保有者のために動作しません。 *安全検査* 7 より低い値。

あなたは知っておくべきこと

プライバシーモードのみ（カード会員を上書き）上司へのアクセスを許可するアッサ・アブロイ IP ロック機能です。この機能は、工場出荷時の設定として無効になっています。

以下の情報は、この機能がどのように動作するかを説明します。プライバシーモードを有効にするには、ドアが閉じている間に、ドアの内側にいプライバシーボタンを押してください。プライバシーモードが有効であることを示すために、約 2 分間、ゆっくりとボタンの LED が点滅します。このアクションは、監視デッドボルトを装備したロックにデッドボルトを投げると同等です。



を持つすべてのカード会員 *安全検査* 監督としての 7 関数よりも低い値。カード保有者が内側からドアを開いたとき、またはスーパーバイザがでバッジたときに、プライバシーモードが解除されます。

設定ツールからプライバシーモードを有効にするには：

1 ドアエンティティのためのブール型のカスタムフィールドを作成し、それをプライバシーモードに名前を付けます。
あなたはそれが書かれているよう大文字と小文字で、まさに名前のスペル、スペースを含める必要があります。

2 エリアビューのタスクを開き、この機能を有効にする必要があり、全てのドアのために TRUE にプライバシーモードのカスタムフィールドを設定します。
先端： あなたは多くのドアを有効にこの機能が必要な場合は、我々は、使用をお勧めします *コピー設定ツール*。

2 つのカスタムイベントは、あなたのシステムに追加されます。

- **デッドボルトロック：** プライバシーモードは、ドアの上に起動されたとき、このイベントがトリガされます。
- **デッドボルトロックを解除します：** プライバシーモードは、ドアの上に非アクティブ化されたときに、このイベントは tiggered されます。

万の資格情報アッサ・アブロイ IP Cx のロックのサポートについて

Cx のタイプのロックは現在、オフラインモードでは、最大 10,000 の資格情報をサポートすることができます。

必要条件

最低限必要な Synergis™アプライアンスのファームウェアは 10.6 GA です。

Synergis™クラウドリンクでオンラインロック

有効な資格は、ロックに保存されている万のものである場合：

- ザ・ *アクセスを許可* 決定は、ロックによって取得されます。
- 読者の LED が緑色に点灯し、ドアロック解除（デフォルト 5 秒）。

有効な資格は、ロックに保存されている万の一つではない場合：

- アクセス許可の決定は、読者のホストルックアップで Synergis™クラウド Link ユニットによって取得されます。
- 読者のは、それが緑色に点灯し、ドアロック解除（デフォルト 5 秒）、1 秒間赤色 LED。

Synergis™クラウド・リンク付きのロックオフライン

ロックに保存されている 10 の 000 の資格情報のみがアクセスを許可されます。

万の資格情報上記のロックの同期

Synergis™クラウドリンクユニットとアッサ・アブロイ IP Cx のロックとの同期は 10,000 資格の制限を超える超過した作業を続けています。例えば、スケジュール変更がまだ同期されており、資格情報を除去することができます。

万の資格情報の同期時間：

- Synergis™クラウド Link ユニットあたり 1 錠：20 分
- Synergis™クラウド Link ユニットあたり 128 のロック：約 16 時間、46 分

ない 20 の以上のロックを同時に接続するようワイヤレスロックの場合、ラジオのウェイクアップスケジュールを設定します。

アッサ・アブロイ IP ロック統合のためのサポート Synergis™アプライアンスの機能

すべての Synergis™アプライアンスの機能は、アッサ・アブロイ IP ロックの統合でサポートされていません。

アッサ・アブロイ IP ロックの統合は、次のことをサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire*

特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）	
手動登録（*ハードウェアを追加* ダイアログ ボックス）[1]	ノートを参照してください
自動登録（スキャン ボタン）はい	
プロパティ configurationNo	
コンフィギュレーション・クローニング（クローン ボタン）いいえ	
I/O の診断（入力、リレーのライブ監視、および 読者）いいえ	
インタフェースモジュールのファームウェア displayYes	
インタフェースモジュールのファームウェアのアップグレード（推奨適用します ファームウェア）はい	
アクセス制御の挙動（Synergis™ ユニット全体の設定）[2]	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）いいえ	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）はい	
数字の最大 PIN 長	63
デグレードモード 機能設定/ A	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）はい	[4]

[1] 必要がある Synergis™ユニットと IP ロックをペアリング。

[2] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

[3] 見る アッサ・アブロイ IP ロックのサポートされている最大 PIN 長 47 ページ。

[4] 動作しますが、「ロックリレーの遅延は、」考慮されません。

アッサ・アブロイ IP ロックのサポートされている最大 PIN 長

サポートされる最大 PIN 長並びに PIN を入力するための方法は、ロックモデルと選択されたリーダモードに依存します。

サポートされる最大 PIN エントリのタイムアウトは 255 秒です。

注意： *カードと PIN のみで動作します 常に スケジュール。*

注意： 読者はカードまたは PIN モードのときは、PIN の資格は、カード保有者が、カードの資格を持っている場合にのみ機能します。

SX のタイプのロックといくつかの Cx タイプのロック

SARGENT とコービン Russwin IN120 及び IN220：以下は、すべての Sx ロックと、次の Cx ロックに適用されます。

- **カードまたは PIN：** 最大 6 桁がサポートされています。「*」が続く 1〜6 桁の PIN を入力します。
- **カードと PIN：** カードを提示し、「*」が続く 1〜6 桁の PIN を入力してください。

PX のタイプのロックといくつかの Cx タイプのロック

PERSONA シリアル番号 SARGENT パスポート 1000 年 P1 と P2、コービン Russwin アクセス 700 PIP1 と PWI1、サージェントとコービン Russwin IN120 及び IN220 ロック：以下はすべての PX ロック、Sx をロック Hx のファームウェアを実行し、次の Cx ロックに適用されます。IN120 及び IN220 ロックが注文したか、手動で設定することができます。以下の手順を参照してください。

- **カードまたは PIN：** 唯一の 6 桁の PIN はサポートされています。6 桁の PIN に続く「＃」を入力します。
- **カードと PIN：** 唯一の 4 桁の PIN はサポートされています。カードを提示し、その後、4 桁の PIN を入力してください。

アッサ・アブロイ IP ロック統合のためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、アッサ・アブロイ IP ロックの統合でサポートされていません。

アッサ・アブロイ IP ロックの統合は、次のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	PoE 対応のみ
	標準の助成金 timeYes	
	拡張助成金 timeYes	
	エントリの時間（標準/拡張）[1]	ノー
	ドアリロック - optionsN / A	
	ドアはスケジュールによってロックが解除された場合 - optionsNo	
	ドア開催します - optionsYes	
	ドアが開いて強制的に - optionsYes	
	アンロック schedulesYes	[2]
	（REX）のオプションを終了する要求	
	REX にロックを解除 いいえ（オン/オフ）	
	アクセスを許可した後 REX を無視する時間（中 秒）いいえ	
	ドアが開いている間 REX イベントを無視 いいえ（オン/オフ）	
	（ドアが閉じた後、REX を無視する時間 秒）いいえ	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒。）いいえ	
	ドア上の（オン/オフ）2 人のルールを強制します sideNo	
セキュリティ Desk3 ドアの手動アクション	手動でドアのロックを解除み	PoE 対応のみ
	シャント Reader は（有効化/無効化 読者）いいえ	
	オーバーライドロック解除 schedulesYes	[4]

特徴 groupSecurity	センター featureSupported	
セキュリティ Desk5 でのライブイベント監視	モジュールの実行状態（*オンライン*、*オフライン*）はい	6
	交流 failN / A	
	バッテリーは（失敗しますローバッテリー）はい	
	ドア オープン/ closedYes	7
	ドア ロック/ unlockedYes7	
	ドアの強制 openYes	
	ドアはあまりにもオープン開催しました longYes	8
	ドア securedYes	9
	デッドボルト（*確保し*、*リリース*）	PoE 対応のみ
	キー overrideNo	
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）	
	0 ビジター護衛ルール いいえ（オン/オフ）	NO1
	InterlockNo	
	AntipassbackNo	
	一人称イン ruleNo	
エレベーター コントロール		
ター	N / A	エレベー
ゾーン管理	I / O zoneN / A	
	ハードウェア zoneN / A	

[1] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされたときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[2] IP ロックは 32 時間間隔の限界まで受け付けます。セキュリティセンターのスケジュールは、この制限を超える場合は、最初の 32 時間間隔が適用されます。

[3] Synergis™ユニットは、Access Manager に接続する必要があります。

[4] 無線 LAN ロックの場合、コマンドは次の無線連絡先に適用されます。

[5] 無線 LAN からのライブイベントをロックしません。次回のイベントは無線連絡した後にのみ使用可能です。6 つの WiFi ロックは唯一の定期的な無線連絡+ 5 分後にオフラインと考えられています。逃しています。7 つのドアオープンドアクローズイベント

は、PoE の口ックでのみ生成されます。

[8] ドアオープンが長すぎるイベントをトリガするための設定ツールで設定したタイムアウト値は 4 分 15 を超えることはできません秒 (または 255 秒) 。任意の値がより高く 255 秒 Synergis™単位で 255 秒に設定されます設定します。

[9]A *ドアを確保* ドアが後に閉じられたときにイベントが生成されます *ドアの強制* 若しくは *あまりにも長いオープンドア*イベント。

[10] セキュリティクリアランスは、カード所有者のアクセス権には影響しませんが、それはセキュリティクリアランスが 7 未満に設定されている場合、セキュリティセンターのアンロックスケジュールがロックされた状態で行って、次のロックを行いん。

アッサ・アブロイ IP ロックの設定の概要

Synergis™ユニットで動作するようにアッサ・アブロイ IP ロックを設定するには、まずロックの設定ツール（LCT）でロックを設定し、Synergis™アプライアンスポータルを使用して Synergis™ユニットにロックをペアリングする必要があります。

次の表は、IP ロック設定プロセスをまとめたもの。

段階	DescriptionSee	
1	あなたの IP ロックのファームウェアが最新であると Synergis™Softwire 10.6 でサポートされていることを確認してください。	• *IP 対応のロックのインストールクイックスタートガイド*それはあなたのロック付属しました。 • サポートされているアッサ・アブロイ IP ロック 39 ページ。
2	LCT を使用して IP ロックを設定します。 • Synergis™ユニットの IP アドレスと同じになるように IP ロックのホストアドレスを設定します。 • ロック（デフォルト= 2571）を発見したときに Synergis™ユニットが待機ポートとして使用することを IP ロックの通信ポートを設定します。 • 暗号化が必要な場合は、ロックプロファイルの AES キーを設定します。あなたは Synergis™ユニットと IP ロックをペアリングした後、あなたは、このキーが必要です。	• *ネットワーク&ロック設定ツールユーザーズマニュアル*それはあなたのロック付属しました。
3	Synergis™ユニットと Synergis™アプライアンス Portal でその接続された IP ロックの間の通信を確立します。	• Synergis™に接続入学 IP ロック単位 53 ページ

例

より多くを学ぶためにこのビデオを見ます。クリック**キャプション**アイコン（**CC**）使用可能な言語の一つで、ビデオのキャプションをオンにします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます**互換表示設定**クリア **互換表示で表示イントラネットサイト**。

Synergis™ユニットに接続入学 IP ロック

Synergis™ユニットは、それに接続された IP ロックと通信するためには、ロックペアリングモードを使用して Synergis™アプライアンス Portal でそれらを一緒にペアリングして、構成ツールでロックの設定を完了する必要があります。

あなたが始める前に

ロックの設定ツール（LCT）を使用して、IP ロックを設定します。暗号化が有効になっている場合は、書き留め

ロック AES キー。あなたは、設定ツールで、このキーを入力する必要があります。

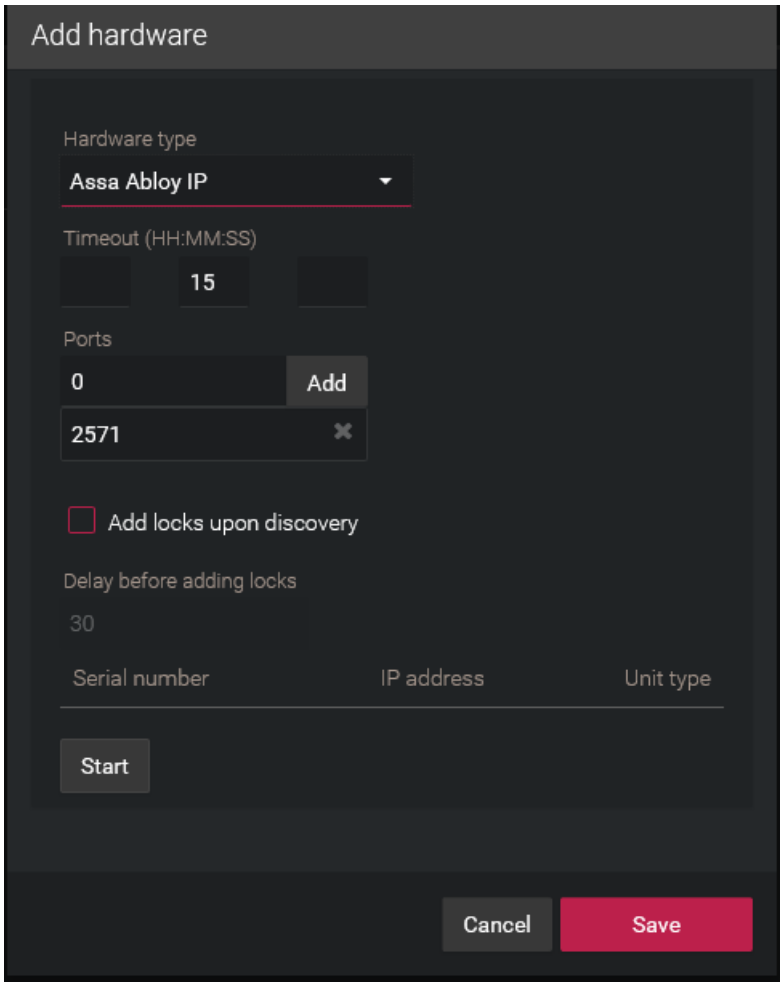
あなたは知っておくべきこと

ロックペアリングモードがアクティブである場合、指定された通信ポートを使用して Synergis™ユニットに接続されているすべての IP ロックが発見されます。ペアリングモードが終了した後、Synergis™ユニットは、セキュリティセンターでの Access Manager に再接続し、ペア IP ロックを追加します。

注意： 硬化でタグ付けされたステップや命令はオプションですが、サイバー攻撃からシステムを保護します。

Synergis™ユニットに接続されている IP ロックを登録するには：

1 Synergis™ユニットにログオンします。
2 クリック **コンフィギュレーション > ハードウェア**
3 の上部には *ハードウェア*列、クリックしてください **加えます** （）。
4 選択 **アッサ・アブロイ IP**。
5 Timeout フィールドに（オプション）、のためのロックペアリングモードを有効にするにはどのくらいの時間を選択します。新しい IP ロック接続は、唯一、指定した時間の量のためにペアリングされています。



6 （オプションのデフォルト、2571 以外のポートを使用している場合）ポート]ダイアログボックスで、IP ロックに設定された通信ポートのポート番号を入力し、[追加]をクリックします。

7 （オプション）は、それらが発見されているように、IP ロックを追加したい場合は、次の操作を行います。

a) を選択 **発見時にロックを追加します。** オプション。

重要： このオプションを選択すると IP ロックの各グループが追加された後、Synergis™ユニットは、Access Manager に再接続します。あなたがペアリングモードが完了する前に、IP ロックの設定を開始しなければならない場合のみ、このオプションが推奨されます。

b) から **ロックを追加する前に遅延** オプションは、以前に発見されたロックが追加される前に通過しなければならない秒数を選択します。

8 クリック **開始**。

重要： 無線 LAN ロックの場合、COM を押すか、Synergis™ユニットへの接続をトリガするためにロックの背面パネルの内側にボタンをリセットします。

IP ロックが検出され、テーブルに追加されます。

あなたは Synergis™ユニットにロックをペアリングに問題がある場合は、 あなたの IP ロックとの間の接続をテストします そして、ユニット。

9 次のいずれかを実行します。

- ロックペアリングモードを停止し、発見したロックを追加するには、[停止]をクリックして保存。
- ロックペアリングモードを解除するには、[キャンセル]をクリックします。

注意： もし *発見時にロックを追加します。* オプションが選択されている、いくつかのロックがすでに追加されている場合があります。

- ロックペアリングモードがタイムアウトするまで待ちます。

Synergis™ユニットは、Access Manager に再接続し、発見されたロックが追加されます。

10 クリック **コンフィギュレーション > ハードウェア**

追加された IP ロックは、ハードウェアの設定ページに表示されます。ロックを選択します。ユニットタイプ、シリアル番号、および選択された IP ロックのロックファームウェアは、プロパティの下に表示されています。

11 何も情報がプロパティの下に表示されない場合は、ページを更新します。

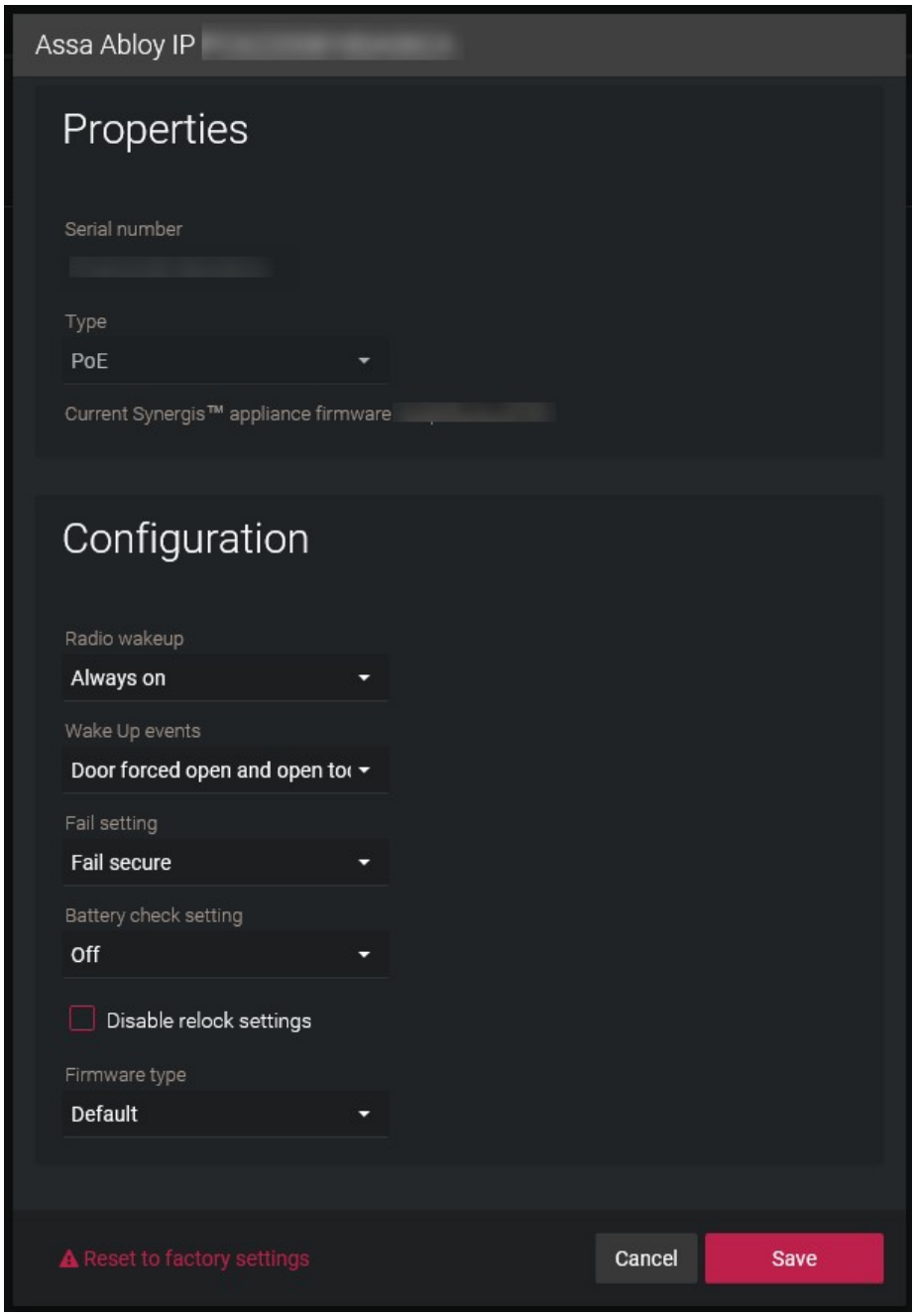
無線 LAN ロックの場合、その情報は、プロパティの下に表示される前に 2 分かかることがあります。彼らは Synergis™ユニットと常に通信していないので、無線 LAN のロックは、ハードウェアツリーに赤で表示されます。

a) PoE のロックの場合：アンダー *プロパティ*、そのことを確認してください **ラジオウェイクアップ** に設定されています **常にオン** そのため、 *アクセス許可されました*イベントは、セキュリティデスクで逃していない、と設定されている決して **バッテリーチェックの設定**に **オフ**。

b) 無線 LAN ロックの場合：アンダー *プロパティ*、そのことを確認してください **ラジオウェイクアップ** に設定されています **日々**、および時刻を入力します（**時間** そして **分**）それは起こるべきとき。

あなたは Synergis™単位の時間帯をフォローするラジオウェイクアップ時間が必要な場合は現地時間を選択します。このオプションを選択しない場合、デフォルトは UTC です。

c) **あなたが合うように、他のロック設定を変更します。**



12 暗号化が LCT を通じて有効になっている場合は、選択してアッサ・アブロイ IP チャネルを編集し、AESkey 入力してください
あなたの口ックに設定された（32 文字の 16 進文字列）。

13 クリック **セーブ**。

あなたの IP ロックと Synergis™ユニット間の接続をテストします

あなたがトラブルあなたの IP ロックに Synergis™ユニットをペアリングを持っている場合は、ロックとロックの設定ツール（LCT）を使用して、ユニット間の接続をテストすることができます。

あなたの IP ロックと Synergis™ユニットとの間の接続をテストするには：

1 PoE のロックについては、LCT に Ping テストコマンドを参照してください。

2 無線 LAN ロックの場合、を参照してください。 **ホストへの接続を確認してください** LCT でコマンド。

アッサ・アブロイ IP ロックの暗号化を無効にします

アッサ· アブロイ IP ロックの暗号化を無効にするには、アッサ· アブロイ IP チャネルから AES キーをクリアして、LCT とロックプロファイルから AES キーを削除する必要があります。

アッサ・アブロイ IP ロックの暗号化を無効にするには：

1. Synergis™ユニットにログオンします。
2. クリック **コンフィギュレーション > ハードウェア**。
3. **アッサ· アブロイ IP** を選択し、アッサ· アブロイチャネルとロックを選択します。
4. フィールドをクリア **AESkey**、[OK]をクリックします **セーブ**。
5. **ロックの設定ツール（LCT）を使用して、ロックから暗号化キーを削除します。**
   a) **ロックプロファイルから AES キーを削除します。**
   b) クリック **NVRAM のリセット** ロックをリセットします。
   手順については、 *ネットワーク&ロック設定ツールユーザーズマニュアル* それはあなたのロック付属しました。
6. **LED の点滅が停止したリーダーになるまでロックの電源をオフにします。**
7. **ロックの電源をオンにします。**
   ロックは、電源がオンになると、それがオンラインに戻ってきます。

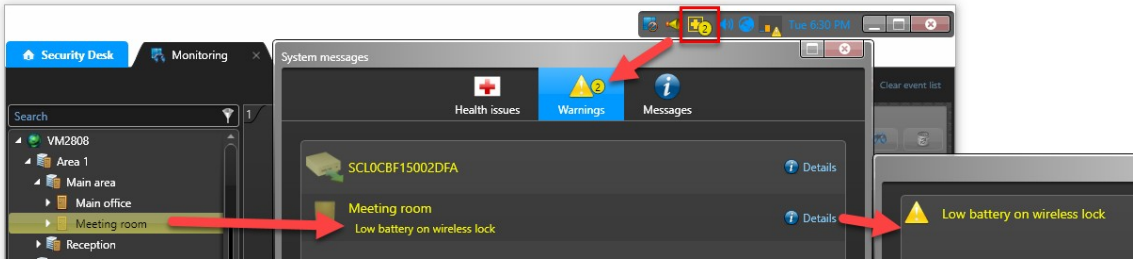
Monitoring the battery status of WiFi

アッサ・アブロイ IP の WiFi ロックのバッテリーの状態をチェックするには、バッテリーはそれが接続されている Synergis™ユニットにイベントを失敗し監視することができます。

あなたは知っておくべきこと

各無線 LAN ロックの場合は、セキュリティセンターは、指定された仮想入力を作成します *入力 BatteryFail* それはとして示し *アクティブ*の中に **モニタリング** タブ上の黄色の警告 **システムメッセージ** のアイコン **通知トレイ** バッテリーが低いとき。

注意： *入力 BatteryFail* 無線 LAN ロックのバッテリーの状態を示すために作成されたソフトウェア入力されています。あなたは、この入力に任意の物理デバイスを接続することはできません。



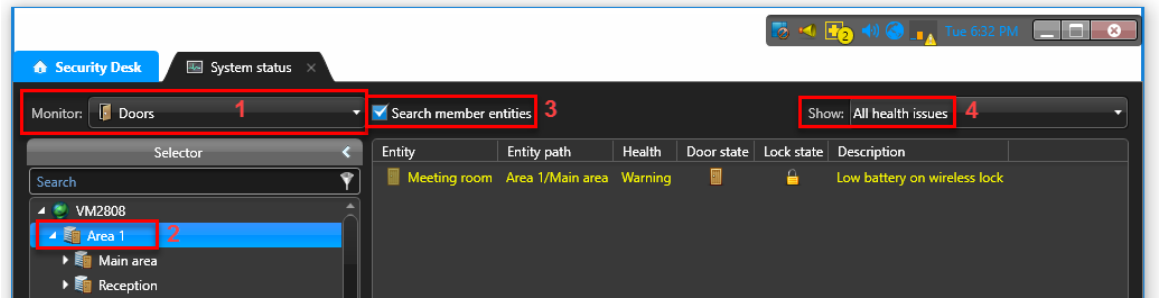
無線 LAN ロックのバッテリの状態を監視するには：

1 開きます *システムステータス* セキュリティデスクでタスクを選択 **ドア** の中に **モニター** ドロップダウンリスト。

2 **エンティティツリー内の親エリアを選択します。**

3 クリック **検索メンバーエンティティ** 子領域の下にすべてのロックを表示するためのチェックボックスをオンにします。

4 選択 **すべての健康問題** の中に **ショー** ドロップダウンリストを警告してドアを表示します。
注意： バッテリーに問題があるの WiFi ロックが表示されます *アクティブ*以下のための状態 **入力 BatteryFailed**
入力



1 これらの WiFi ロックの電池交換のスケジュールを設定します。

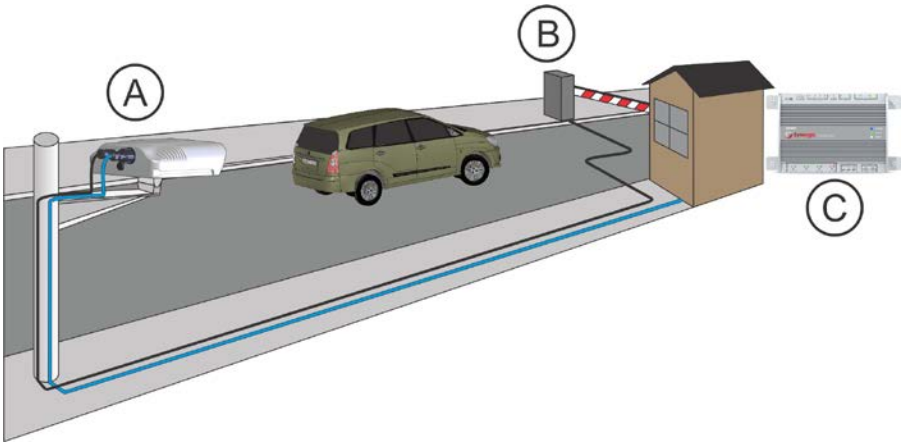
5

AutoVu SharpV カメラ

このセクションでは、次のトピックについて説明します。

AutoVu™SharpV 統合の概要

AutoVu™SharpV カメラは、通過する車両からナンバープレートを読み取ることができます。それらは、車両アクセス障壁に近づくにつれて SharpV カメラが車両のナンバープレートのビューを固定位置に設置されたときに、プレートは、カメラから読み出すセキュリティセンターに資格情報として使用することができます。プレートの番号は、ユーザーの資格情報と一致する場合、システムは、車両へのアクセスを許可するようにバリアをトリガします。



注意： ナンバープレートを使用する機能は、資格がセキュリティセンター5.6 以降でのみ利用可能であるとして読み込みます。

	成分	あなたは知っておくべきこと
A	**SharpV カメラ**	カメラは、車両ライセンスのビューを固定位置に設置されています プレートは、それらは、車両アクセスバリアに近づきます。
B	**車両アクセス障壁**	あなたは、車両へのアクセスの障壁を制御するために SharpV 出力を使用することができます
C	**ネットワーク接続**	SharpV カメラは、セキュリティセンターと通信し、Synergis に登録されます™ クラウドリンク。

ナンバープレートを使用するには Synergis™クラウドリンクまたは Synergis™マスターコントローラは SharpV カメラでネットワークを介して接続されている必要があり、資格情報として読み込みます。以下の画像は SharpV と Synergis™クラウドリンクを含むシステムを示しています。

Synergis™ クラウドリンク

より多くを学ぶためにこのビデオを見ます。クリック**キャプション** アイコン（**CC**）使用可能な言語の一つで、ビデオのキャプションをオンにします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます**互換表示設定** クリア **互換表示で表示イントラネットサイト**。

サポートされている AutoVu™シャープカメラ

AutoVu™シャープカメラの統合のために、各シャープカメラは、インターフェースモジュールと見なされます。Synergis™Softwire は、以下のシャープのカメラとそれに対応するファームウェアをサポートしています。

モデル	説明	サポートされているファームウェア
SharpV	IP 対応のナンバープレート認識（LPR）カメラ	SharpOS 12.2 以降

注意： 第一世代 Synergis™ユニット（Synergis™マスターコントローラ）SharpOS 12.3 以降を実行している SharpV カメラをサポートしていません。

サポートされている AutoVu™シャープのカメラ機能

AutoVu™シャープカメラは LPR カメラです。ナンバープレートは、資格証明書として使用することができます読み取り、すべてではなく、標準のアクセス制御機能が適用されます。

注意： ナンバープレートを使用する機能は、資格がセキュリティセンター5.6 以降でのみ利用可能であるとして読み込みます。Synergis™Softwire 10.6 には、以下のシャープのカメラ機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleSub パネル	
コミュニケーション protocolIP	
暗号化されました コミュニケーション	はい（HTTPS）
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeNo	
依存 modeYes	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン modeNo	
劣化 MODEN / A	
スケーラビリティ	
オフラインの最大数 eventsN / A	
自律的意思決定のための資格証明書の最大数（ 作成）N / A	
最大資格長（中 ビット）N / A	
RS-485 あたりのインターフェイスモジュールの最大数 channelN / A	
Synergis™単位あたりのインターフェイスモジュールの推奨最大数	8

AutoVu™シャープカメラを統合するためのサポート Synergis™アプライアンスの機能

すべての Synergis™アプライアンスの機能は AutoVu™シャープカメラの統合でサポートされていません。シャープカメラの統合は、次のことをサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire* 特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）[1]	
手動登録（*ハードウェアを追加* ダイアログ ボックス）いいえ	
自動登録 (スキャン ボタン) いいえ	
プロパティ configurationNo	
コンフィギュレーション・クローニング (クローン ボタン) いいえ	
I / O の診断 (入力、リレーのライブ監視、および 読者) いいえ	
インタフェースモジュールのファームウェア displayNo	
インタフェースモジュールのファームウェアのアップグレード (推奨適用します ファームウェア) いいえ	
アクセス制御の挙動 (Synergis™ ユニット全体の設定)[2]	
ドアに開催されたビープ音 openN / A	
ドアを強制的にビープ openN / A	
アクセスのビープ音 deniedN / A	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）N / A	
ドアがあるとき、「DHO」イベントを生成しません。 unrestrictedYes	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）N / A	
の最大 PIN 長 digitsN / A	
デグレードモード 機能設定/ A	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）はい	

[1] シャープカメラは、設定ツールから Synergis™ユニットに登録する必要があります。

[2] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

AutoVu™シャープカメラを統合するためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、シャープのカメラの統合でサポートされていません。

シャープカメラとの統合には、以下のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeYes	
	拡張助成金 timeYes	
	エントリの時間（標準/拡張）[1]	はい
	ドアリロック - optionsYes	
	ドアはスケジュールによってロックが解除された場合 - optionsYes	
	ドア開催します - optionsYes	
	ドアが開いて強制的に - optionsYes	
	アンロック schedulesYes	
	（REX）のオプションを終了する要求	
	REX にロックを解除（オン/オフ）はい	
	アクセスを許可した後 REX を無視する時間（中 秒）はい	
	ドアが開いている間 REX イベントを無視（オン/オフ）はい	
	（ドアが閉じた後、REX を無視する時間 秒）はい	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒）N / A	
	ドア上の（オン/オフ）2 人のルールを強制します sideN / A	
セキュリティ DESK2 ドアの手動アクション	手動でロックを解除 doorsYes	
	シャント Reader は（有効化/無効化 読者）はい	
	オーバーライドロック解除 schedulesYes	

Feature group	Security Center	Supported
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン*、*オフライン*）	はい
	交流 failN / A	
	バッテリーは（失敗しますローバッテリー）	N / A
	ドア オープン/ closedYes	
	ドア ロック/ unlockedYes	
	ドアの強制 openYes	
	ドアはあまりにもオープン開催しました longYes	
	ドア securedN / A	
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）	は
	いビジター護衛ルール N / A（オン/オフ）	
	InterlockYes	
	Antipassback	
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）	はい
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）はい	
	両方のエリアの入り口にチェックを厳格（antipassback と 終了）はい	
	に scheduleYes	
	グローバル antipassbackYes	
	一人称-内のルール	
	ドアアンロックに強制 scheduleN / A	
	アクセスに施行 rulesN / A	
エレベーター コントロールター	N / A	エレベー
ゾーン	I / O zoneYes	
	ハードウェアゾーン	
	ゾーンアーミング inputYes	
	ゾーンアーミング scheduleYes	
	ゾーンアーミング、エントリ delaysNo	

Feature group	Security Center	Supported
	ゾーン I / O linkingYes	
	カウントダウン buzzerYes	

[1] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされたときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[2] Synergis™ユニットは、Access Manager に接続する必要があります。

Synergis™ユニットに AutoVu™SharpV カメラを登録

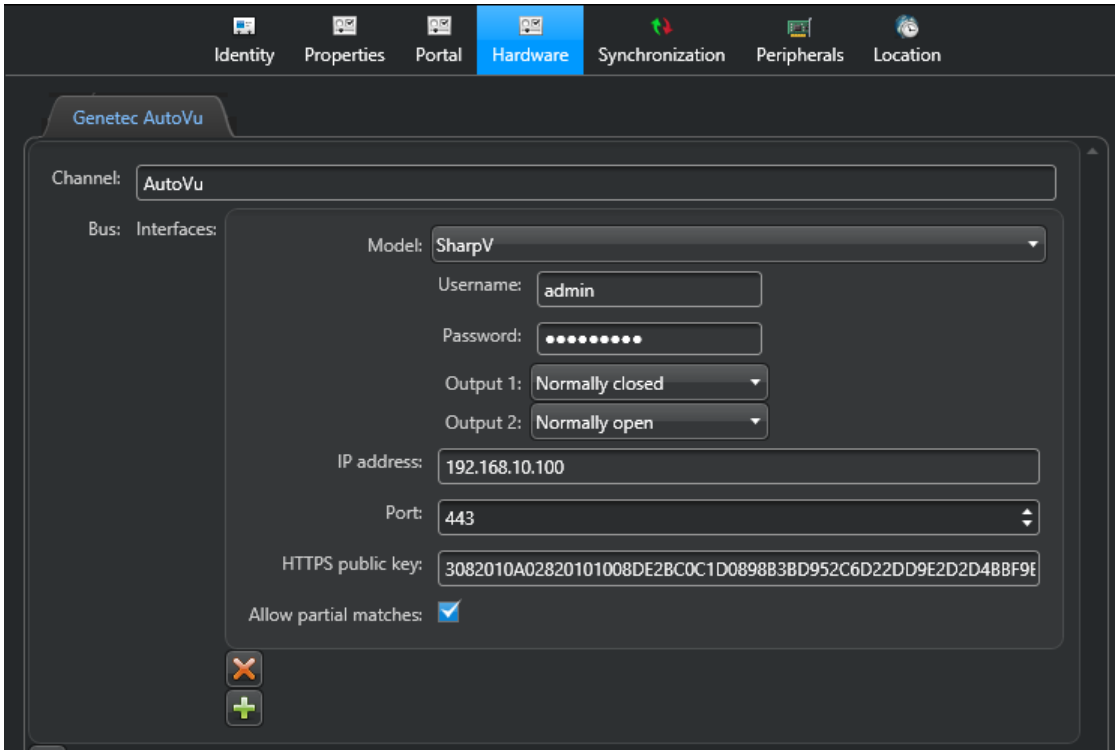
Synergis™ユニットが SharpV カメラと通信するためには、セキュリティセンターで Synergis™ユニットにカメラを登録する必要があります。

あなたが始める前に

- HTTPS 通信を使用する SharpV カメラを設定します。詳細については、インストールしているカメラの導入ガイドやハンドブックを参照してください。
- ゼネテック™の自己署名証明書または信頼できる認証局から署名付き証明書のいずれかをインストールします。
- あなたは SharpV カメラを登録している場合は、SharpV Web ポータルにログオンし、デフォルトのパスワードを変更します。

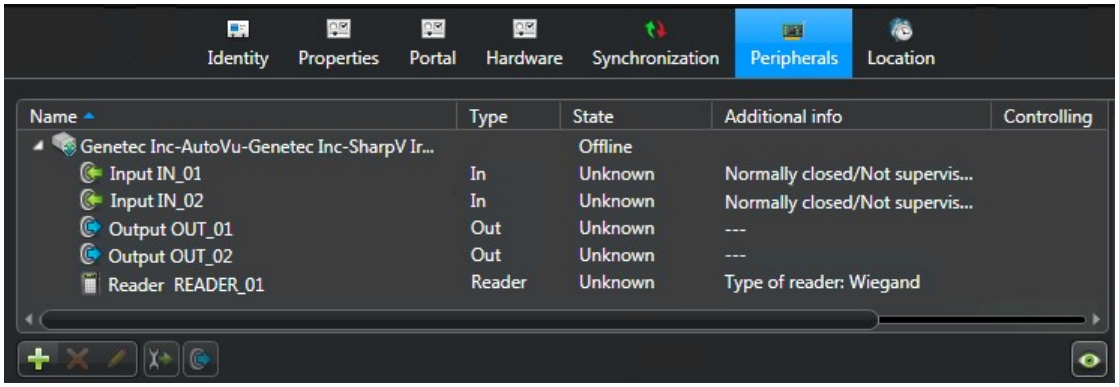
Synergis™ユニットに SharpV カメラを登録するには：

1 設定ツールのホームページで、開きます *アクセス制御* 仕事。
2 クリック 役割とユニット、その後、Synergis をクリック™ 単位 （ ）。
3 クリック ハードウェア タブ、[OK]をクリックします ゼネテック™ AutoVu™ タブ。
4 クリック 加えます （ ）。
5 入力します チャネル お好みの名前。
あなたが入力したチャンネル名は、周辺機器]タブでカメラ名に表示されます。
6 クリック インタフェース （ ）。
7 モデル]ドロップダウンリストから、SharpV を選択します。
8 を入力 ユーザー名 そして パスワード SharpV Web ポータルにアクセスするために使用されます。
注意： SharpV カメラの場合、デフォルトのパスワードを使用することはできません。
9 あなたは車のアクセス障壁を制御するために SharpV 出力を使用している場合は、出力があるかどうかを選択
ノーマルオープン 若しくは *ノーマルクローズ*。
10 を入力 IP アドレス カメラの。
11 SharpV は、セキュリティセンターとの HTTPS 通信にポート 443 を使用しています。
12 空の HTTPS 公開鍵フィールドのままにしておきます。この情報は、カメラの証明書に基づいて自動的に追加されます。
13 部分一致は、ボックスはデフォルトで選択されて確認してください許可します。この機能は、プレートが設定されたライセンスプレート資格から 1 文字の違いを持っている読み込み受け入れます。これは、プレートの数の任意の場所で、単一文字の挿入、削除、または置換を含んでいます。この機能を有効にすると、汚れや破損のナンバープレートが受け入れられる可能性が高いから、プレートを読み込みます。



14 クリック **適用します**。

- SharpV カメラが中に表示されます **周辺機器** タブ。
- **入力と出力は SharpV カメラの下に表示されます。**



例

より多くを学ぶためにこのビデオを見ます。クリック**キャプション** アイコン（**CC**）使用可能な言語の一つで、ビデオのキャプションをオンにします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます**互換表示設定** クリア **互換表示で表示イントラネットサイト**。

車両へのアクセスの障壁を制御するために SharpV カメラの設定

車両へのアクセスの障壁を制御するために SharpV カメラを使用するには、障壁は、セキュリティセンターでドアとして構成する必要があります。

あなたが始める前に

- Synergis™アプライアンスへの車両アクセス障壁をワイヤー。詳細については、インストールしているアクセス制御アプライアンスのハードウェアインストレーションガイドを参照してください。
- Synergis を登録™ セキュリティセンターでのユニット（参照 *Synergis™ アプライアンスの設定ガイド*）。
- Synergis™ユニットに SharpV カメラを登録。

セキュリティセンターでの車両のアクセス障壁を設定するには：

1 設定ツールのホーム· ページから、エリアビューのタスクを開きます。
2 あなたは車のアクセス障壁を追加したいエリアを選択します。
3 クリック **エンティティを追加** > ドア。
4 ドアウィザードを作成するには、車両のアクセスバリアの名前と説明を入力します。
5 場所]ドロップダウンリストから、あなたがドアを作成されている領域を選択し、[次へ]をクリックします。
6 上の **ドア情報** ページには、バリア両側に名前を割り当てます。
例： イン/アウト、または入り口/出口。
7 それが配線され、アクセス制御部との障壁を関連付けるには：
a) から アクセス制御ユニット ドロップダウンリストを、Synergis を選択™ 単位。
b) から **インタフェースモジュール** ドロップダウンリストを、SharpV カメラを選択します。
8 クリック **次**。
9 確認 *作成の概要*、およびクリック **作ります > 閉じる。**
バリアは、エリアビューの中に表示されます *エンティティツリー*。
10 バリアを選択し、クリックしてください **プロパティ** タブ。
11 バリアの一般的なアクセス制御の動作を設定します。詳細については、*セキュリティセンター管理者ガイド*。
12 クリック **適用します**。
13 クリック **ハードウェア** タブおよびアクセス制御部と、セキュリティセンターへの扉との間の配線を説明します。詳細については、*セキュリティセンター管理者ガイド*。
14 資格証明書としてのナンバープレートを使用してカード会員を作成します。カード会員の作成の詳細については、セキュリティデスクユーザーガイドを参照してください。
カード保有者に資格証明書を割り当てる場合、ライセンスプレートのオプションを選択します。
15 ドアへのアクセス権を持つユーザーを選択します。詳細については、*セキュリティセンター管理者ガイド*。

6

軸コントローラ

このセクションでは、次のトピックについて説明します。

75

Supported Axis controllers

軸コントローラの統合のために、各 A1001 コントローラは、インターフェースモジュールと見なされます。

Synergis™Softwire は、Axis の A1001 コントローラをサポートしています。

モデル	説明	サポートされているファームウェア
A1001	2 ドアコントローラ、IP 通信をサポートする 2 つのカードイン/ REX-アウトドアまたは 1 カードイン/カードアウトドアのための 2 本の読者は、適切なをフィーチャー。	推奨：1.601

[1] このようアッサ· アブロイ IP ロック、軸、水星 EP などの特定のインテリジェントコントローラについて、あなたは Synergis™アプライアンスポータルのインタフェースのアップグレードページから推奨ファームウェアを適用することができます。他のためにメーカーは、あなたが推奨されるファームウェアを適用するために、メーカーのソフトウェアを使用する必要があります。

サポートされている軸コントローラの機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™Softwire 10.6 には、以下の軸コントローラの機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleIntelligent	コントローラ
コミュニケーション protocolIP	
暗号化されました communicationNo	
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeNo	
依存 modeYes	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン modeYes	
劣化 MODEN / A	
リーダーの通信プロトコル	
WiegandYes	
OSDP	はい
OSDP（セキュア チャンネル）いいえ	
クロックおよびデータ（磁気ストライプ）- また、ABA として知られています formatN / A	
F2F	N / A
ProprietaryN / A	
スケーラビリティ	
オフラインの最大数 イベント	30 0001
自律的意思決定のための資格証明書の最大数（ メイキング）	15
0002 最大クレデンシャル長（IN ビット）512	[3]
RS-485 あたりのインターフェイスモジュールの最大数 channelN / A	
Synergis™あたりのインターフェイスモジュールの推奨最大数 単位	664 分
の 30	

[1] オフラインログエントリとセキュリティセンターのイベントの間に 1 対 1 のマッチが常にありません。

[2] 推奨される制限は、ハード制限は 15 000 10 000 です。

[3] 我々は現在、ウィーガンド標準 26 ビット、コーポレート・ 1000 (35 ビット) 、H10306 (34 ビット) 、H10302 (37 ビット) 、および H10304 (37 ビット) ですセキュリティセンターでサポートされている標準のカードフォーマットをサポートしています。カスタムカードフォーマットは 512 ビットまで行くことができます。

[4] 以下のための最大 *Synergis™ クラウドリンク* 30.の最大であります *SV-32* 66 です。

軸コントローラを統合するためのサポート Synergis™アプライアンスの機能

すべての Synergis™アプライアンスの機能を軸コントローラの統合でサポートされていません。

軸コントローラの統合は、以下をサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire*
特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）	
手動登録（*ハードウェアを追加* ダイアログ ボックス）はい	
自動登録 (スキャン ボタン) いいえ	
プロパティ　configurationYes	
コンフィギュレーション· クローニング (クローン ボタン) はい	
I / O の診断 (入力、リレーのライブ監視、および 読者) はい	
インタフェースモジュールのファームウェア displayYes	
インタフェースモジュールのファームウェアのアップグレード (推奨適用します ファームウェア) マニュアル [2]	
アクセス制御の挙動 (Synergis™ ユニット全体の設定) [3]	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）オンライン	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）はい	
digits5 の最大 PIN 長	16
デグレードモード 機能設定/ A	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）はい	

[2] 推奨軸のファームウェアは、ファイルを適用することにより、Synergis™アプライアンスにアップロードする必要があります
Axis_10.6_xxx.y.sfx Synergis によるファームウェアのアップグレードなど™ アプライアンスのポータル。
[3] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。
[4] ビープ音は、これらのイベントに無効にすることはできません。
[5] HID モード-00 読者をサポートするインタフェースモジュールの場合。

軸コントローラを統合するためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、軸コントローラの統合でサポートされていません。

軸コントローラの統合は、次のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeYes	
	拡張助成金 timeYes	
	エントリの時間（標準/拡張）[1]	ノー
	ドアリロック - optionsLimited	[2]
	ドアはスケジュールによってロックが解除された場合 - optionsYes	ドア
	開催します - optionsLimited	[3]
	ドアが開いて強制的に - optionsLimited	[3]
	アンロック schedulesYes	
	（REX）のオプションを終了する要求	
	REX にロックを解除（オン/オフ）はい	
	アクセスを許可した後 REX を無視する時間（中 秒）N / A	
	ドアが開いている間 REX イベントを無視 N / A（オン/オフ）	
	（ドアが閉じた後、REX を無視する時間 秒）N / A	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒）オンライン	
	ドア上の（オン/オフ）2 人のルールを強制します sideOnline	
セキュリティ Desk4 ドアの手動アクション	手動 doorsOnline のロックを解除	
	シャント Reader は（有効化/無効化 読者）オンライン	
	オーバーライドロック解除 schedulesOnline	

特徴 groupSecurity	センター featureSupported
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン、オフライン*）はい
	交流 failN / A
	バッテリーは（失敗しますローバッテリー）N / A
	ドア オープン/ closedYes
	ドア ロック/ unlockedYes
	ドアの強制 openYes
	ドアはあまりにもオープン開催しました longYes
	ドア securedN / A
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）オンライン ビジ
	ター護衛ルール オンライン（オン/オフ）
	InterlockOnline
	Antipassback
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）オンライン
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）オンライン
	両方のエリアの入り口にチェックを厳格（antipassback と 終了）オンライン
	に scheduleOnline
	グローバル antipassbackOnline
	一人称-内のルール
	ドアアンロックに強制 scheduleOnline
	アクセスに施行 rulesOnline
エレベーター コントロールター	エレベーノー
ゾーン管理	I / O zoneNo
	ハードウェア zoneNo

[1] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされたときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[2] とともに **開封後は再ロック** オプションでは、遅延は常に 0 秒です。

[3] ザ・ **リーダーのブザーの動作** オプションがサポートされていません。

[4] Synergis™ユニットは、Access Manager に接続する必要があります。

Synergis™ユニットの軸コントローラを登録

Synergis™ユニットは、それに接続された軸コントローラと通信するためには、Synergis™アプライアンス Portal または設定ツールのいずれかでコントローラを登録する必要があります。

あなたが始める前に

- Axis のコントローラのシリアル番号または IP アドレスが手元にあります。その情報を検索するには、Axis のマニュアルを参照してください。

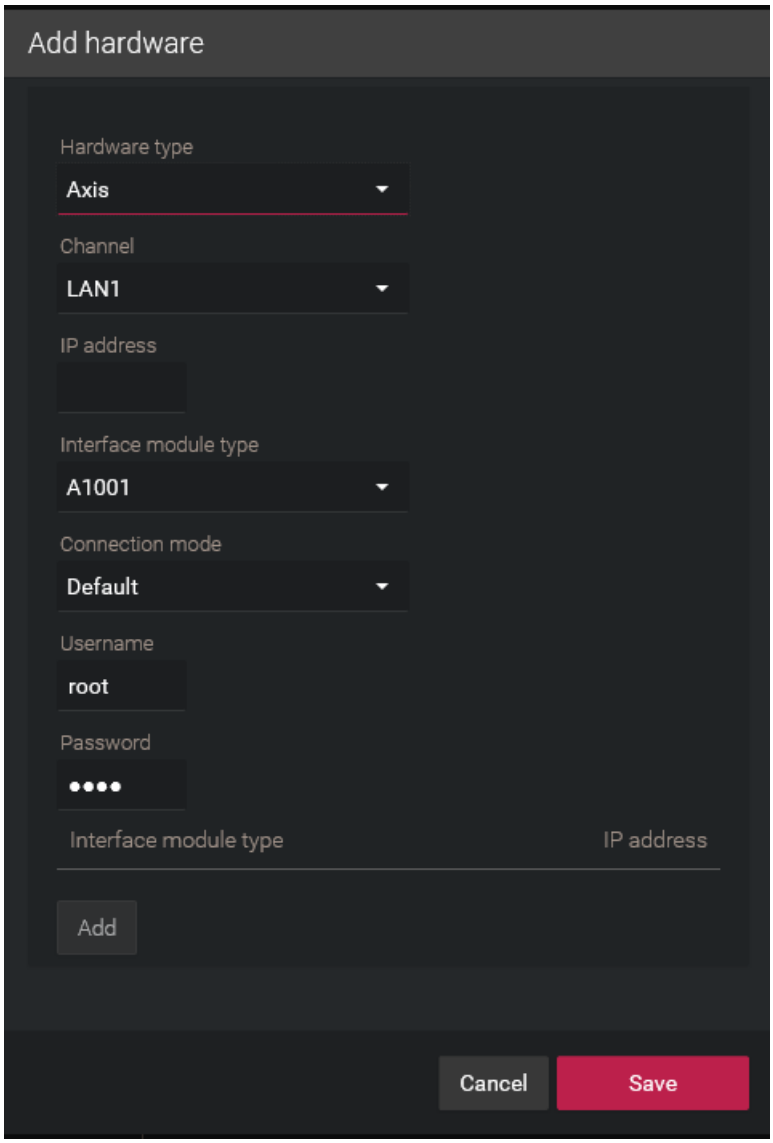
あなたは知っておくべきこと

それは、コントローラを登録するとき Synergis™ユニットは、デフォルトの設定で、すべての軸の入力接点と出力リレーを設定します。軸と Synergis™は、その設定を記述するために異なる用語を使用します。

注意： Synergis を通じてのみ登録™ アプライアンス Portal は、ここで説明されていますが、から軸コントローラを登録することができます 設定ツール > Synergis ユニット > ハードウェア タブ。

Synergis™ユニットの軸コントローラを登録するには：

1 Synergis™ユニットにログオンします。
2 クリック **コンフィギュレーション > ハードウェア**
3 の上部には *ハードウェア*列、クリックしてください **加えます** （  ）。
4 の中に *ハードウェアを追加* 選択]ダイアログボックスで、 **軸** として **ハードウェアの種類**。
5 **軸コントローラが接続されている IP チャネルを選択します。**
6 **軸コントローラに接続するために必要な接続パラメータを入力します。**
   - *シリアル番号または IP アドレス。* 軸コントローラの IP アドレスまたはシリアル番号を使用してください。
   - ***ポート。*** HTTP ポート（ デフォルト= 80 ）。
   - *ユーザー名パスワード。* 新しいユーザ名とパスワード（デフォルト= ルート/パス）。すべてのフィールドが必要です。



7 クリック **セーブ**。
追加したばかりのハードウェアタイプ、チャネル、およびインタフェース・モジュールは、に表示されます *ハードウェア構成*
ページ。軸モジュールがオンラインになるのは 1 分ほどかかる場合があります。

8 **現在のファームウェアのバージョンが最新でない場合は、それをアップグレードしてください。**
   1 **すでに軸ファームウェアパッケージをダウンロードしていない場合は、GTAP からそれをダウンロードしてください。**
   2 クリック **メンテナンス > Softwire のアップグレード**
   3 クリック **ファームウェアファイルを選択します。**

9 **ブラウザのウィンドウでは、あなたの Synergis™Softwire バージョン (Axis_10.6.xxx.y.sfw) に対応して軸のプラグインのバージョンを選択し、[開く]をクリックします。**

10 **確認メッセージボックスで、[OK]をクリックします。**

11 軸モジュールは分後にオンラインにならない場合は、クリックしてください **メンテナンス > インターフェイスのアップグレード >**
推奨ファームウェアを適用します。
これは、オンラインで、ネットワーク経由でアクセス可能なすべての登録インタフェースモジュールに推奨されるファームウェアのバージョンが適用されます。

12 **からあなたのインターフェイスモジュールの接続と構成をテスト** *I/O の診断* **ページ。詳細については、** *Synergis™ アプライアンスの設定ガイド*。

あなたが完了した後、

Synergis を追加™ Access Manager にユニットそれはあなたのセキュリティセンターのシステムの一部になるように。詳細については、*Synergis™ アプライアンスの設定ガイド*

硬化軸コントローラ

あなたが軸コントローラを登録することができます前に、Synergis™ユニット上の Axis プラグインをインストールする必要があります。

あなたが始める前に

- あなたがゼネテックのご担当者から最新の Synergis™Softwire と軸のプラグインを取得していることを確認します株式会社 Synergis™Softwire ファイルが Release_10.6.xxx.y.sfw という名前で、軸のプラグインファイルが Axis_10.6.mmm.n.sfw という名前です。軸のプラグインファイルが含まれています推奨軸ファームウェア。
- 最新のフォロー アクシスコミュニケーションズからの製品のセキュリティ勧告。
- 軸コントローラを登録。

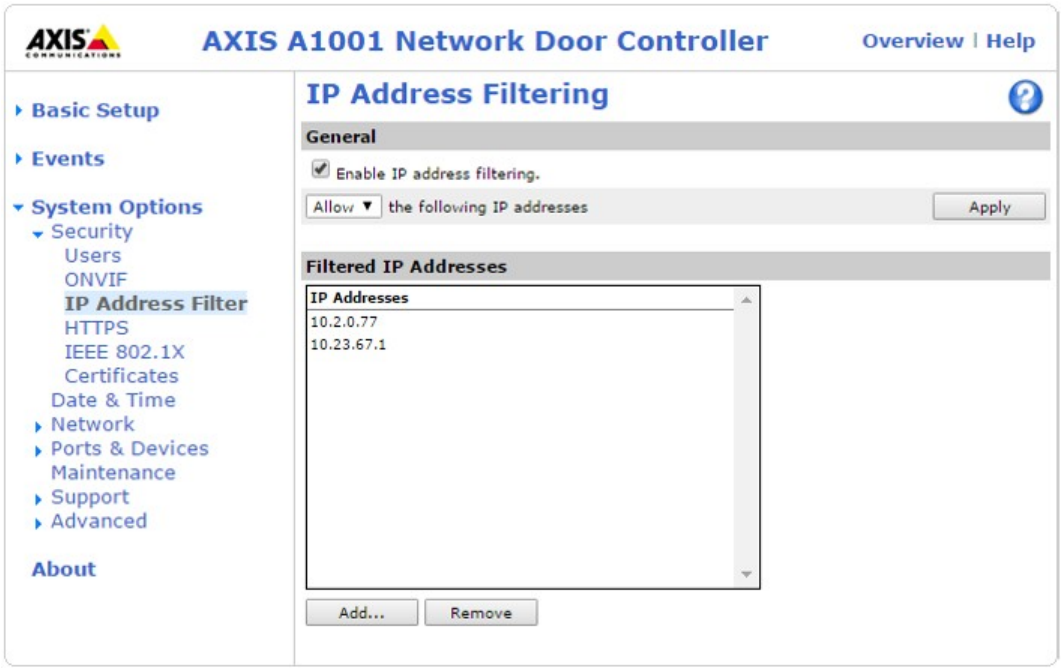
あなたは知っておくべきこと

硬化でタグ付けされたステップや命令はオプションですが、サイバー攻撃からシステムを保護します。

軸コントローラを強化するには：

1 アクシス A1001 の Web ポータルにログオンします。
詳細については、 AXIS A1001 ネットワークドアコントローラおよび AXIS エントリ Manager ユーザーマニュアル。

2 クリック セットアップ > 追加のコントロールの設定 > システムオプション > セキュリティ > IP アドレスフィルタ、とのリストに追加 フィルタリング IP アドレス Synergis の、IP アドレス™ ユニットと軸 A1001 の Web ポータルにログオンする必要があります管理ワークステーションの IP アドレス。



3 クリック セットアップ > 追加のコントロールの設定 > システムオプション > ネットワーク > TCP / IP > 高度、および両方の無効化 FTP サーバ そして RTSP サーバ。
彼らは Synergis™Softwire では使用されません。

軸コントローラの不正開封防止の入力について

軸コントローラは、セキュリティセンターで監視することができる 2 つのタンパの入力を備えています。これらの入力は、次のとおりです。

- **入力が改ざん。** この入力はアクティブのときです。
  - 2 リーダーI / O コネクタの 1 つ上の入力「IN3 は、」アクティブである、または
  - センサーが作動し、警報を改ざんフロント、または
  - 戻る改ざんアラームスイッチが作動し
- **入力 CasingOpen。** この入力はアクティブのときです。
  - センサーが作動し、警報を改ざんフロント、または
  - 戻る改ざんアラームスイッチが作動しています。

アラームを改ざん前面と背面には、アラームのピンヘッダーを改ざんそれぞれ 2 - のピンにジャンパを置くことによって無効にすることができます。

- 改ざんアラームピンヘッダー - フロント（TF）
- 改ざんアラームピンヘッダー - バック（TB）

軸コントローラに接続されている周辺機器の設定

軸コントローラに接続されている入力接点、出力リレー、および読者を設定するには、設定ツールを使用してセキュリティセンターで変更を加える必要があります。

あなたが始める前に

- Synergis™ユニットの軸コントローラを登録。
- Synergis を追加™ Access Manager にユニット。詳細については、*Synergis™ アプライアンスの設定ガイド*。

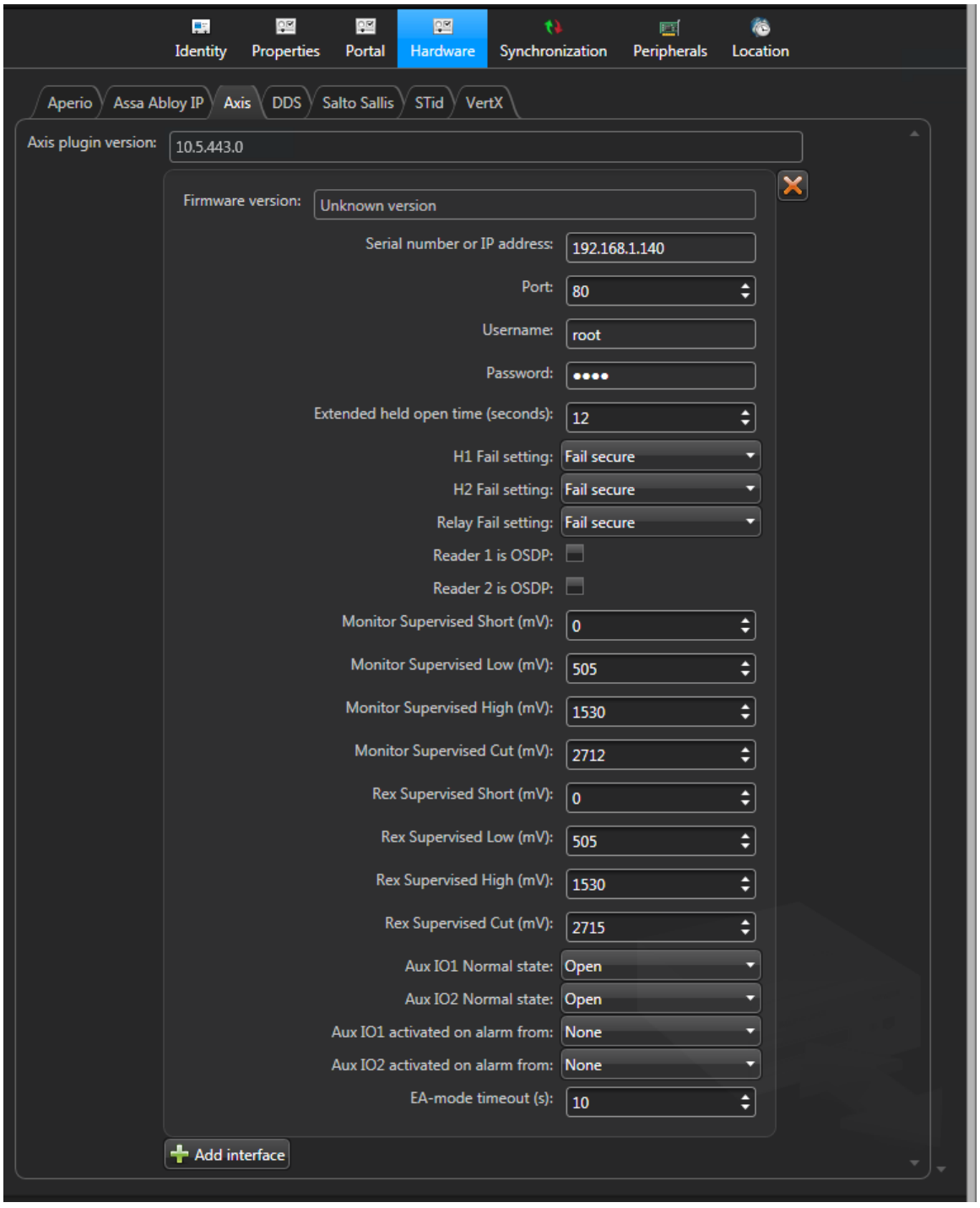
あなたは知っておくべきこと

- あなたは Synergis™ユニットのハードウェアのページから軸出力リレーと読者を設定する必要があります。
- あなたは Synergis™ユニットのハードウェアのページからからの軸の入力接点を設定する必要があります

  周辺機器 ページ。

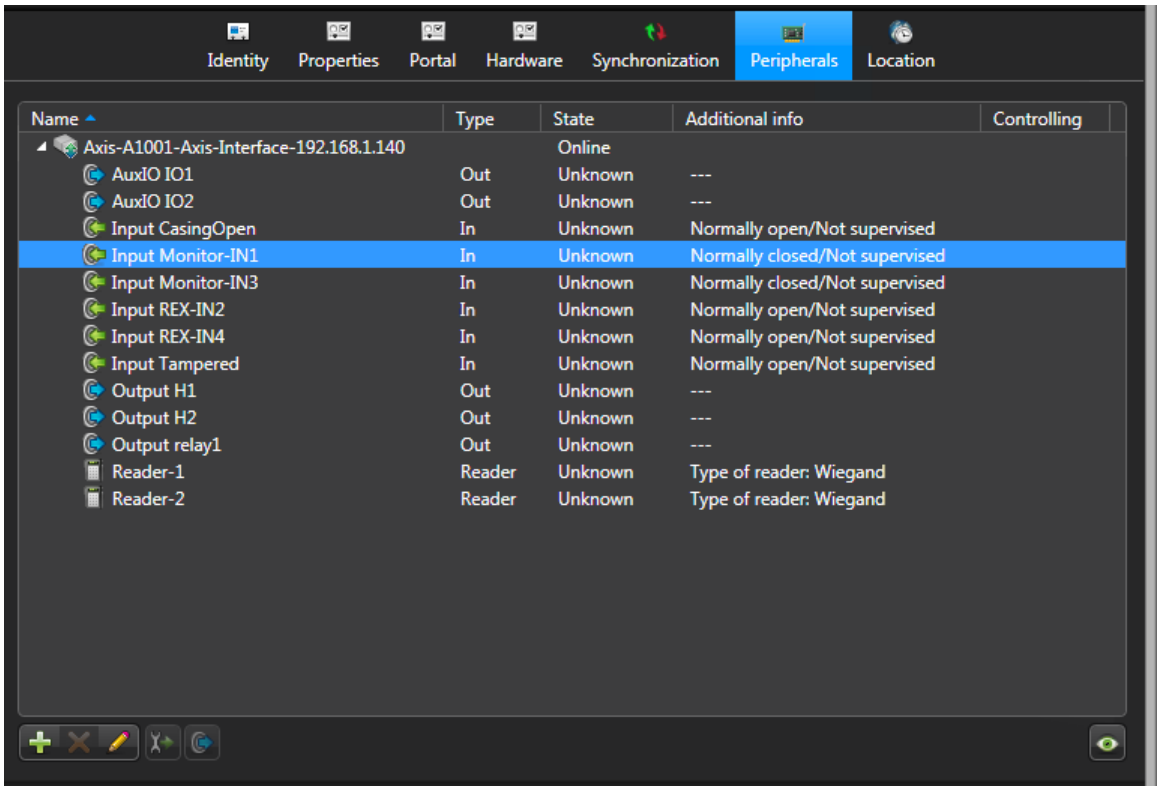
軸コントローラの周辺機器の設定を変更するには：

1 設定ツールのホームページで、開きます *アクセス制御* 仕事。
2 クリック **役割とユニット**、その後、Synergis をクリック™ **単位**（ ）。
3 クリック **ハードウェア > 軸**、必要な変更を行い、[OK]をクリックします **適用します**。

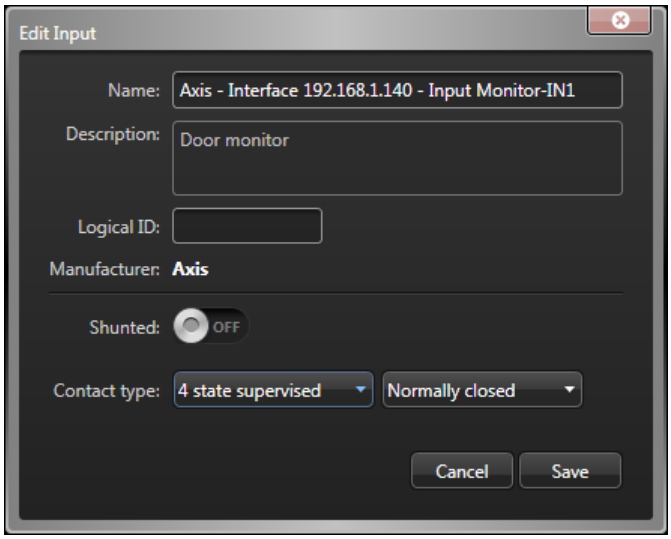


各設定の意味の詳細については、軸のマニュアルを参照してください。

4 あなたが入力接点の設定を変更する必要がある場合は、周辺機器]タブをクリックし、変更したい軸コントローラを展開します。



5 ([編集]を変更して、クリックします入力接点を選択) 。編集入力ダイアログボックスが開きます。



変更可能な設定は、選択した入力によって異なります。

- **名：** 入力デバイス名。
- **論理 ID：** 同じユニットに接続されているすべての周辺機器の中で一意でなければなりません。
- **分流さ：** 入力を無視するには、このオプションを選択します。分流されると、入力の状態のままでは、
  *ノーマル*関係なく、あなたがそれをトリガーする方法の。
- **コンタクトタイプ：** をセットする *ノーマル* 入力接点の状態とその監督モード。
  - **教師なし/ノーマルクローズ：** 入力接点の正常な状態が閉じられ、アクセス制御部は、入力がトラブル状態にあることを報告しません。

- **ないノーマルオープン/監修：** 入力接点の正常な状態が開いており、入力がトラブル状態にある場合、アクセス制御部は報告されません。
- **4 状態はノーマルクローズ/監修しました：** 入力接点の正常状態が閉じられ、アクセス制御部レポート入力は、故障状態にあるとき。
- **4 状態は、ノーマルオープン/監修しました：** 入力接点の正常な状態が開いており、入力がトラブル状態にあるとき、アクセス制御部が報じています。

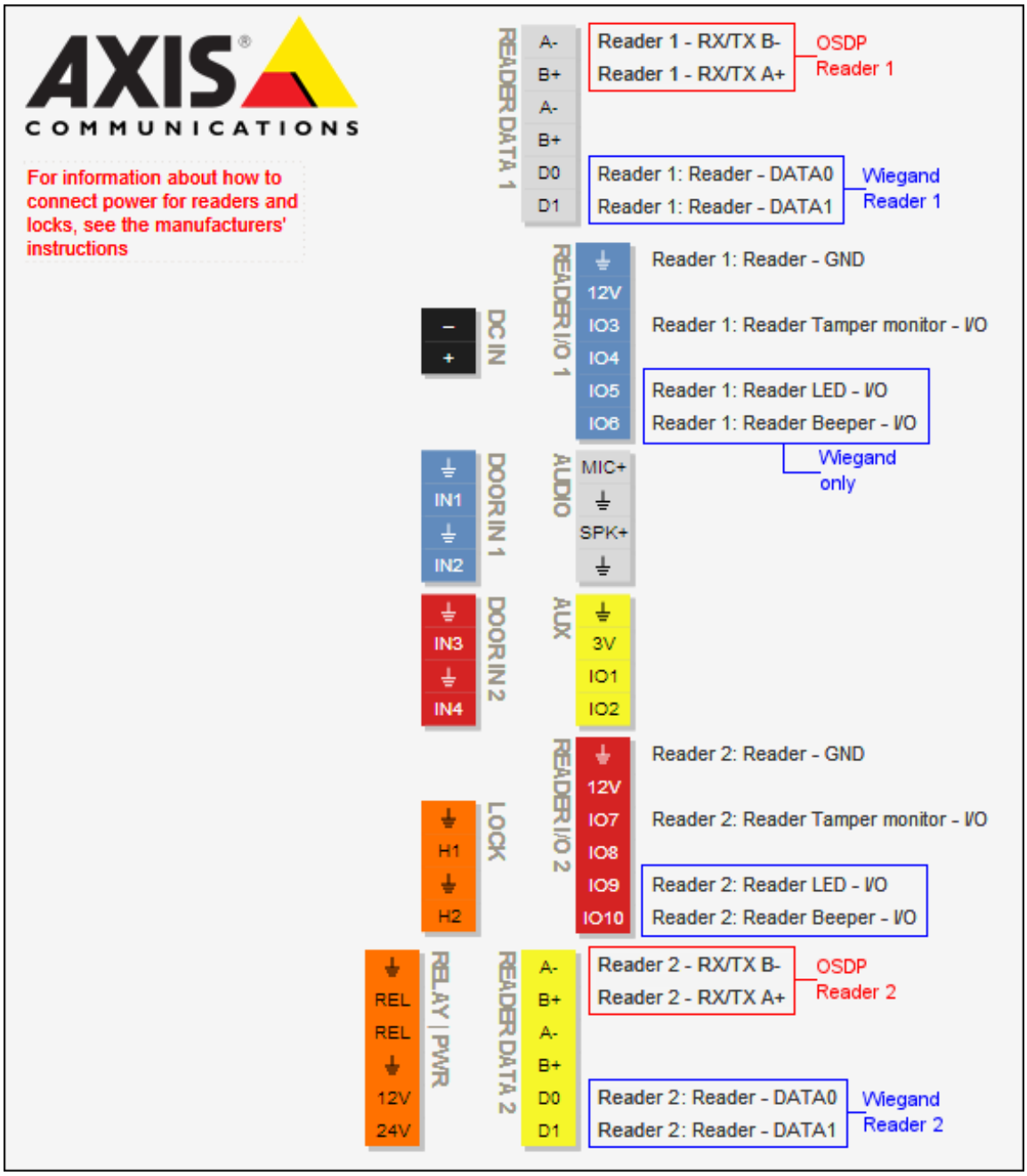
6 必要な変更を行い、[保存]をクリックし、[適用]をクリックします。

軸コントローラ上のリーダーの接続

各軸のコントローラは、セキュリティセンターConfig でリーダー1 および Reader 2 と呼ばれる、2 人の読者までサポート
ツール。読者はウィーガンド (デフォルト) または OSDP プロトコルのいずれかを使用することができます。OSDP ために、リーダは、リーダデータ A- / B の+の最初のセットに配線されなければなりません。

コネクタの設定以下のチャートが示すように軸コントローラ上のどのリーダに対応します。

注意： 軸コントローラは Synergis™ユニットに切断された場合、このピンチャートでのみ現れます。



7

DDS コントローラ

このセクションでは、次のトピックについて説明します。

Supported DDS hardware

DDS の統合のために、各 TPL ドアコントローラは、インターフェースモジュールと見なされます。

Synergis™Softwire は、次の DDS のハードウェアデバイスをサポートしています。

モデル	説明	ファームウェア
AS34 または TPL	ドアコントローラ 2 /カード内のカードアウトドアに適した 4 つのウィーガンドリーダを搭載し、RS-485 通信をサポートします。 **注意：** TPL ボードの U5 ソケットにインストールされている ROM チップは 5xxxa をラベル付けされていることを確認します。	Synergis™Softwire は、ファームウェアのカスタムバージョンが必要です。カスタムファームウェアが自動的に登録の際に TPL モジュールにプッシュされます。
AS34-P4 または TPL-P4	ドアコントローラ 4 で/ REX カードアウトドアに適した、4 人のウィーガンドリーダーを搭載し、RS-485 通信をサポートします。 **注意：** TPL ボードの U5 ソケットにインストールされている ROM チップは 6xxxa をラベル付けされていることを確認します。	
EXT-TCPT	TPL ドアのための TCP / IP 拡張ボード controller.N / A	
EXT-8E4S	TCP / IP の拡張ボードは 8 つの教師の入力を追加し、4 ROM チップ 6xxxa と TPL ドアコントローラに出力します。 この組み合わせは、TPL-P4 コントローラに TCP / IP インターフェースを追加することと同じです。	N / A

A。正確なチップの数は、ROM の記憶容量に依存します。

サポートされている DDS コントローラの機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™ Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™ Softwire 10.6 には、以下の DDS コントローラの機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleIntelligent	コントローラ
コミュニケーション プロトコル	RS-485 および IP1
暗号化されました communicationNo	
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeNo	
依存 modeYes	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン modeYes	
劣化 MODEN / A	
リーダーの通信プロトコル	
WiegandYes	
OSDP	N / A
OSDP（セキュア チャネル）N / A	
クロックおよびデータ（磁気ストライプ）- また、ABA として知られています formatYes	
F2F	N / A
ProprietaryN / A	
スケーラビリティ	
自律的意思決定のための資格証明書の最大数（ メイキング）	20 0002
（ビット単位）の最大長資格	40
RS-485 チャネルごとインターフェースモジュールの最大数	8
Synergis™ 単位あたりのインターフェイスモジュールの推奨最大数	32

[1] IP コントローラは、EXT-TCPT または EXT-8E4S 拡張ボードが必要です。

[2] Synergis™ユニットは、DDS コントローラと同期させることができる資格情報の最大数は 20,000 です。実際の制限は、AS34 モジュールにインストールされた ROM チップに応じて、低くてもよいです。

DDS コントローラを統合するためのサポート Synergis™ アプライアンスの機能

すべての Synergis™アプライアンスの機能は、DDS コントローラの統合でサポートされていません。DDS コントローラの統合は、以下をサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire* 特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）[1]	
手動登録（*ハードウェアを追加* ダイアログ ボックス）	RS-485 のみ
自動登録（スキャン ボタン）	RS-485 のみ
プロパティ コンフィギュレーション	RS-485 のみ
コンフィギュレーション・クローニング（クローン ボタン）	RS-485 のみ
I/O の診断（入力、リレーのライブ監視、および 読者）はい	
インタフェースモジュールのファームウェア displayNo	
インタフェースモジュールのファームウェアのアップグレード（推奨適用します ファームウェア）自動	
アクセス制御の挙動（Synergis™ ユニット全体の設定）[2]	
ドアに開催されたビープ音 openYes	
ドアを強制的にビープ openYes	
アクセスのビープ音 deniedYes	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）オンライン	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）オンライン	[3]
digits4 の最大 PIN 長	55
デグレードモード 機能設定/ A	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）はい	

[1] IP コントローラは、より Web ページの異なるセットを登録する必要があります *Synergis™ アプライアンスのポータル*。見る "DDS IP コントローラを登録」。

[2] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

[3] HID キーパッドモード 00 がサポートされていません。唯一のキーパッドモード 14 は、ファシリティコード 0 を生成する、です。

[4] HID ウィーガンド標準 26 ビット・カード・コードに限定されるもの（最大値= 65534）。

[5] 4 digitis 未満 PIN は受け付けておりません。

DDS コントローラを統合するためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、DDS コントローラの統合でサポートされていません。

DDS の統合は、次のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、以下を参照してください*セキュリティセンター管理者ガイド*。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	オンライン
	標準の助成金 timeYes	
	拡張助成金 timeOnline	
	エントリの時間（標準/拡張）[1]	オンライン
	ドアリロック - optionsYes	
	ドアはスケジュールによってロックが解除された場合 - optionsYes	
	ドア開催します - optionsYes	
	ドアが開いて強制的に - optionsLimited	[2]
	アンロック schedulesOnline	
	（REX）のオプションを終了する要求	
	REX にロックを解除（オン/オフ）はい	
	アクセスを許可した後 REX を無視する時間（中 秒）はい	
	ドアが開いている間 REX イベントを無視（オン/オフ）はい	
	（ドアが閉じた後、REX を無視する時間 オンライン秒）	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒。）いいえ	
	ドア上の（オン/オフ）2 人のルールを強制します sideNo	
セキュリティ Desk3 ドアの手動アクション	手動でロックを解除 doorsYes	
	シャント Reader は（有効化/無効化 読者）オンライン	
	オーバーライドロック解除 schedulesOnline	

Feature group	Security Center	Supported
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン*、*オフライン*）はい	
	交流 failNo	
	バッテリーは（失敗しますローバッテリー）いいえ	
	ドア オープン/ closedYes	
	ドア ロック/ unlockedYes	
	ドアの強制 openYes	
	ドアはあまりにもオープン開催しました longYes	
	ドア securedN / A	
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）オンライン	ビジ
	ター護衛ルール いいえ（オン/オフ）	
	InterlockOnline	
	Antipassback	
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）オンライン	[4]
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）オンライン	
	両方のエリアの入り口にチェックを厳格（antipassback と 終了）オンライン	
	に scheduleOnline	
	グローバル antipassbackOnline	
	一人称-内のルール	
	ドアアンロックに強制 scheduleNo	
	アクセスに施行 rulesNo	
エレベーター コントロール		エレベータ
ー	オンライン	
ゾーン管理	I / O zoneOnline	
	ハードウェアゾーン	
	ゾーンアーミング inputOnline	[5]
	ゾーンアーミング scheduleOnline	

Feature group	Security Center	Supported
	ゾーンアーミング、エントリ delaysOnline	

Feature group	Security Center	Supported
	ゾーン I / O linkingOnline	
	カウントダウン buzzerOnline	

[1] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされたときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[2] ザ・ リーダーのブザーの動作 オプションは、オンラインのみの操作でサポートされています。

[3] Synergis™ユニットは、Access Manager に接続する必要があります。

[4] エリア内のカード所有者の存在は確認できませんので、カードイン/ REX-アウトドアにはお勧めしません

[5] ゾーンの入力は、ドア上に設定してはいけません。

入学 DDS の RS-485 コントローラ

Synergis™ユニットはその RS-485 インタフェースに接続されている DDS コントローラと通信するためには、Synergis™アプライアンスポータルでそれらを登録する必要があります。

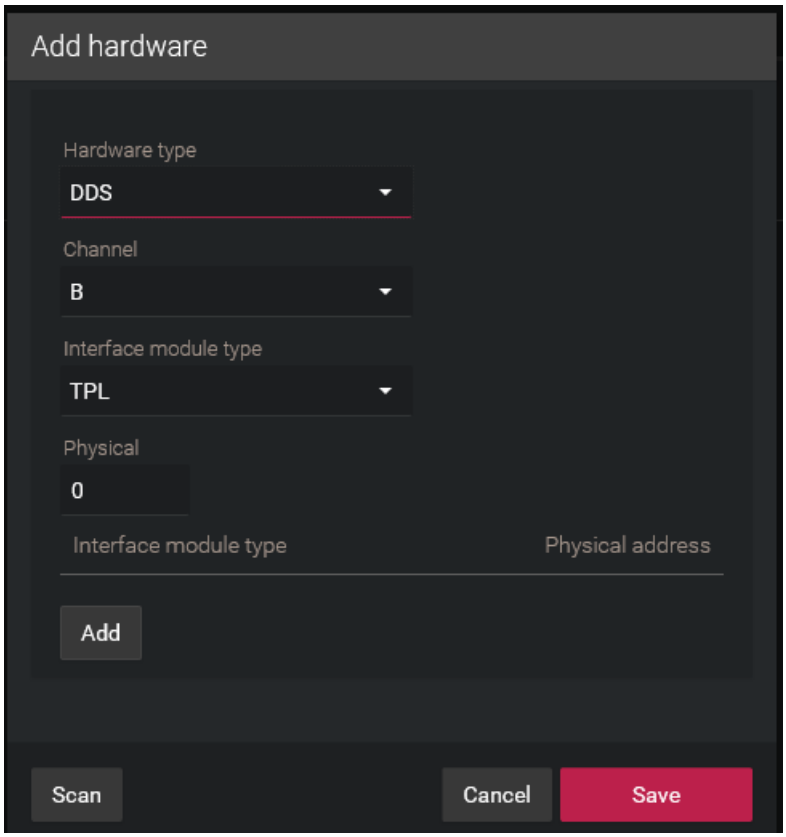
あなたが始める前に

次のように Synergis™ユニットの RS-485 チャンネル（A、B、C、または D）に DDS モジュールを接続します。

- 「-」チャンネルのに DDS モジュールの受信\ L を接続します。
- チャンネルの「+」に DDS モジュールの送信\ H を接続します。
- チャンネルの「G」への DDS モジュールの 0V に接続します。

Synergis™ユニットに接続されている DDS コントローラを登録するには：

1 Synergis™ユニットにログオンします。
2 クリック **コンフィギュレーション > ハードウェア**
3 の上部には *ハードウェア*列、クリックしてください **加えます** （）。
4 の中に *ハードウェアを追加* 選択]ダイアログボックスで、 **DDS** として **ハードウェアの種類**。
5 を選択 **チャネル** （A、B、C、または D）。
同じチャネルに接続されているすべてのインターフェースモジュールは、同じ製造業者からのものでなければなりません。
6 同じダイアログボックスでは、同じチャネルに接続されているすべてのインタフェースモジュールを追加します。次のいずれかを実行します。
- 手動で登録するには、DDS モジュールで構成されている物理アドレス（0〜31）を入力し、[追加]をクリックします
（）。その後、正確なモジュールタイプを選択します。



同じチャネルに接続されたすべてのモジュールを構成するために、必要に応じて繰り返します。

- 自動的に登録するには、[スキャン]をクリックします。

  スキャン機能は、同じチャネルに接続されている同じ製造者からのすべてのインターフェース・モジュールを検索し、登録します。

  コントローラが接続されているすべてのインタフェース・モジュールが見つからない場合は、 それらはすべて異なるがあることを確認します 物理アドレス。

7 クリック セーブ。
追加したばかりのハードウェアタイプ、チャネル、およびインタフェース・モジュールは、に表示されます *ハードウェア構成*
ページ。

8 先ほど追加した各インターフェイスモジュールの場合は、ハードウェアの設定ページから、それを選択し、その設定を行います。
これらの設定の詳細については、製造元のマニュアルを参照してください。必要に応じて変更を加えます。

9 ページの下部に、[保存]をクリックします。

10 I / O の診断ページからごインターフェイスモジュールの接続と設定をテストします。
インターフェイスモジュールのテストについては、以下を参照してください *Synergis™ アプライアンスの設定ガイド*。

あなたが完了した後、

Synergis を登録™ セキュリティセンターでのユニット (参照 *Synergis™ アプライアンスの設定ガイド*) 。

DDS IP コントローラを登録するための準備

あなたは Synergis™ユニットの DDS IP コントローラを登録する前に、シリアルポートを介してそれに接続することによって、その TCP / IP 拡張ボードに静的 IP アドレスを割り当てる必要があります。

あなたが始める前に

あなたは次のことを持っていることを確認してください：

- USB･ツー･ミニ USB ケーブル。
- 4 ポート RS-485 モジュール（お持ちでない場合はゼネテック株式会社のご担当者に尋ねます）。
- セットアッププログラム *Tibbo デバイスサーバツールキット*（どちらか *tdst-5-09-12-x64.exe* 若しくは *tdst-x86.exe 5-09-12-*）。ゼネテック株式会社のご担当者に依頼
- Synergis の最新版™ Softwire と *Tibbo.smc* プラグイン。Synergis をチェックし、アップグレードについて™ ファームウェア、参照 *Synergis™ アプライアンスの設定ガイド*。

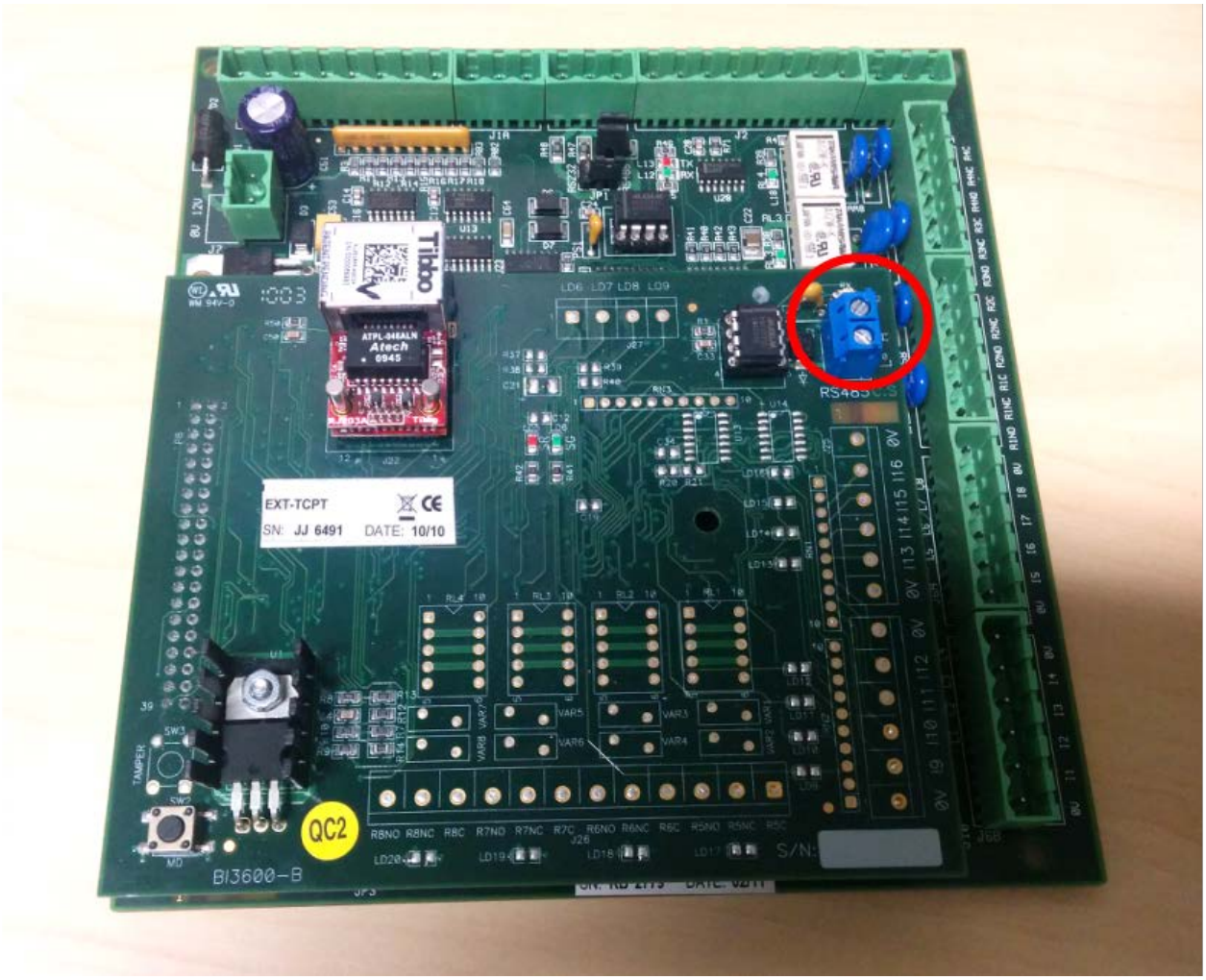
あなたは知っておくべきこと

硬化でタグ付けされたステップや命令はオプションですが、サイバー攻撃からシステムを保護します。

DDS IP コントローラを登録するために準備するには：

1 TPL コントローラに TCP / IP の拡張ボードを取り付けます。

2 4 ポート RS-485 の 1 つのモジュールチャネル（A、B、C、または D のそれぞれと「+」コネクター「 - 」に TCP / IP 拡張ボード上（赤丸）L 及び H コネクタを接続します）..



3 上の 4 ポート RS-485 モジュール、接続されたチャンネルに対応する CTS スイッチが ON（上）位置に設定され、エコースイッチが OFF（左側）の位置に設定されていることを確認します。

4 *インストール Tibbo デバイスサーバツールキット* お使いのコンピュータ上。

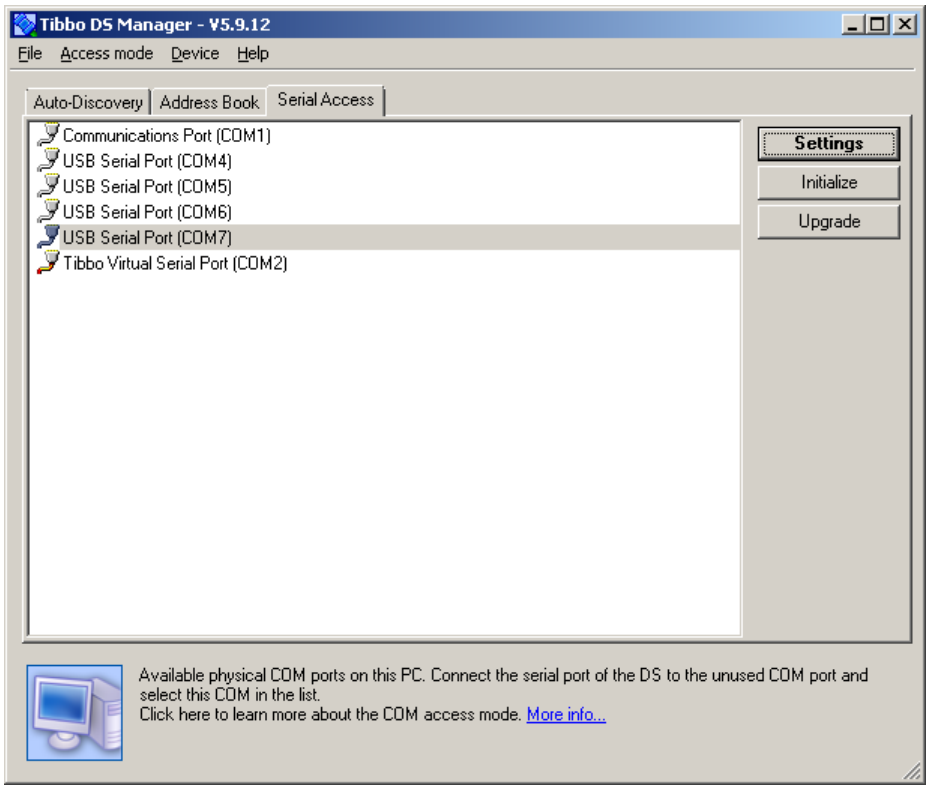
x86 またはあなたが持っているマシンの種類に基づいて、x64 のパッケージのいずれかを選択してください。

5 USB・ツー・ミニ USB ケーブルを使用してコンピュータに 4 ポート RS-485 モジュールを接続します。

6 *ラン Tibbo DS マネージャー（C：\プログラムファイル\ Tibbo \ TDST \ tdsman.exe）* 管理者として。

7 シリアルアクセスをクリックして、TCP / IP の拡張ボードが接続されているチャンネルに対応する COM ポートを選択します。

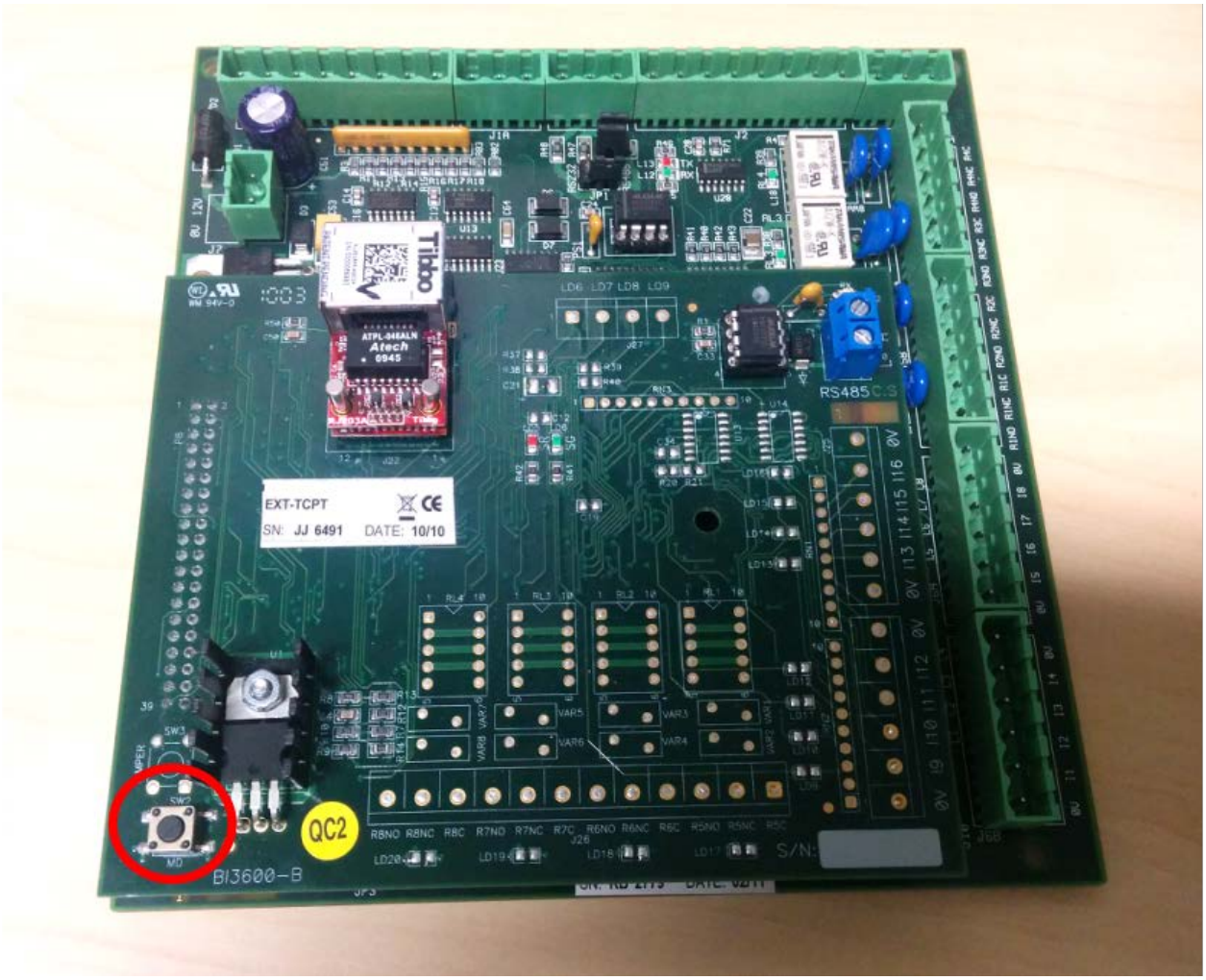
4 ポート RS-485 モジュールで見つかった 4 つのチャンネルは、「USB シリアルポート（COMx の）」ラベル付けされています。最初のものは、D.チャンネルに B、C をチャネルに第一及び第 1 チャンネルに A、第 1 のチャネルに対応します



8 [設定]をクリックし、次のいずれかを実行します。

- あなたがメッセージ「を押して、デバイス上の設定ボタン」を参照してください場合は、手順 9 に進みます。
- メッセージが表示される場合、「デバイスがエラーコードで応答しましたが。失敗したコマンドを表示するにはここをクリックしてください」、そして エコースイッチがオフになっていることを確認してください 4 ポート RS-485 モジュール チャネルのためにあなたが使用しています。
- メッセージが表示される場合、「シリアルポートを開くことができません。シリアルポートが別のプログラムによって使用中である可能性」、そして検証あなたが正しい COM ポートを選択し、または他のプログラムが接続されているのと同じ COM ポートを使用していないこと TCP / IP の拡張ボード。

9 TCP / IP 拡張ボード上（SW2 ラベル）セットアップボタンを押します。



10 表示される[設定]ダイアログボックスで、次のように入力します。

ネットワーク *タブ*

- *DHCP* : 0 - 無効
- *IP アドレス* : DDS コントローラに割り当てられた IP アドレス
- ***ポート*** : **ポート番号 (デフォルト= 1001)**

接続 *タブ*

- *トランスポートプロトコル* : 1 - TCP
- （*硬化*） *リンクサービスログイン* : 0 - 無効
- （*硬化*） *インバンドコマンド* : 0 - 無効
- （*硬化*） *データのログイン* : 0 - 無効
- （*硬化*） *ルーティングモード* : 0-サーバ（スレーブ）
- （*硬化*） *からの接続を受け入れます* : 1 - 現在の宛先 IP アドレス

シリアルポート]タブ

- *RTS / CTS フロー制御* : 0 - 無効またはリモート
- *ボーレート* : 3 から 9600 BPS

11 プロンプトが表示されたら、[OK]をクリックし、TCP / IP の拡張ボード上の設定ボタンを押してください。セットアップボタンの位置については、手順 9 を参照してください。

12 4 ポート RS-485 モジュールからの TCP / IP の拡張ボードを取り外します。

13 バック 4 ポート RS-485 モジュール上の元の位置にローカルエコースイッチを設定し、必要に応じて Synergis™ユニットに再接続（あなたは Synergis™マスターコントローラを使用している場合のみ）。

14 Synergis™ユニットが発見されているのと同じサブネットに TCP / IP の拡張ボードを接続します。イーサネットコネクタは、TCP / IP の拡張ボード上のラベル「Tibbo」の下に位置しています。

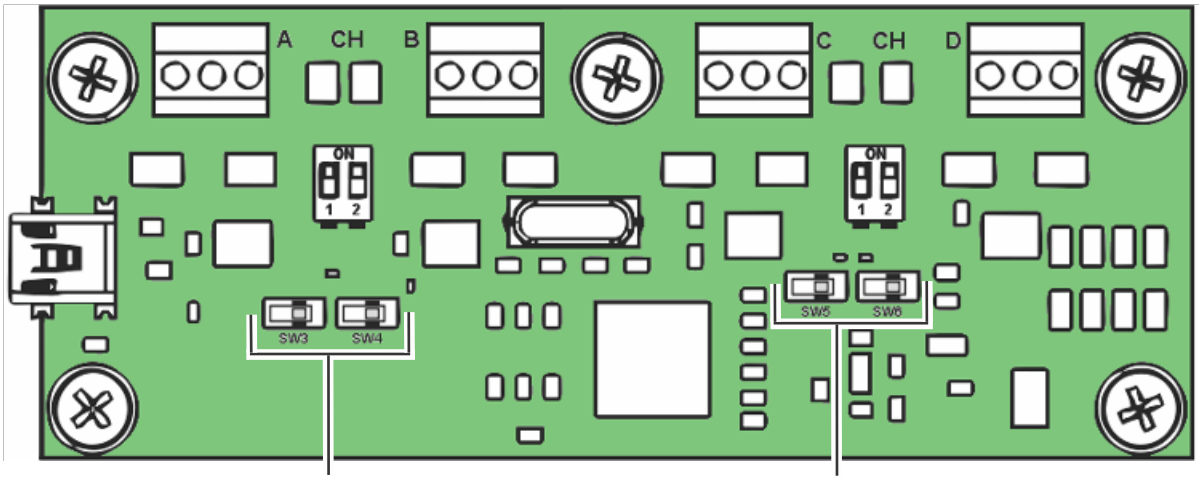
あなたが完了した後、

DDS IP コントローラを登録。

SMC ユニットの RS-485 ローカルエコースイッチについて

すべての RS-485 チャンネルは、ローカルエコー機能をサポートしています。ローカルエコーは SW6、スイッチ SW3 とオンまたはオフにすることができる 4 ポート RS-485 モジュール上に見出されます。

ボード上のこれらのスイッチの位置については、以下の図を参照してください。スイッチは、（右へ）その垂直マーカーと整列されるときにオン位置です。



SW3 そして、SW4
地元 チャネル A および B のためのエコースイッチ

SW5 そして、SW6
地元 チャネル C および D のエコースイッチ

重要： 4 ポート RS-485 モジュールは Synergis™部に TPL ドアコントローラを接続するために使用される場合、ローカルエコースイッチ（右に）ON 位置に設定されなければなりません。4 ポート RS-485 モジュールは、お使いの PC に TCP / IP の拡張ボードを接続するために使用された場合は、ローカルエコースイッチ（左）OFF 位置に設定する必要があります。

DDS IP コントローラを登録

Synergis™ユニットは、IP ネットワークに接続されている DDS コントローラと通信するためには、Synergis™ユニットにそれらを登録する必要があります。

あなたが始める前に

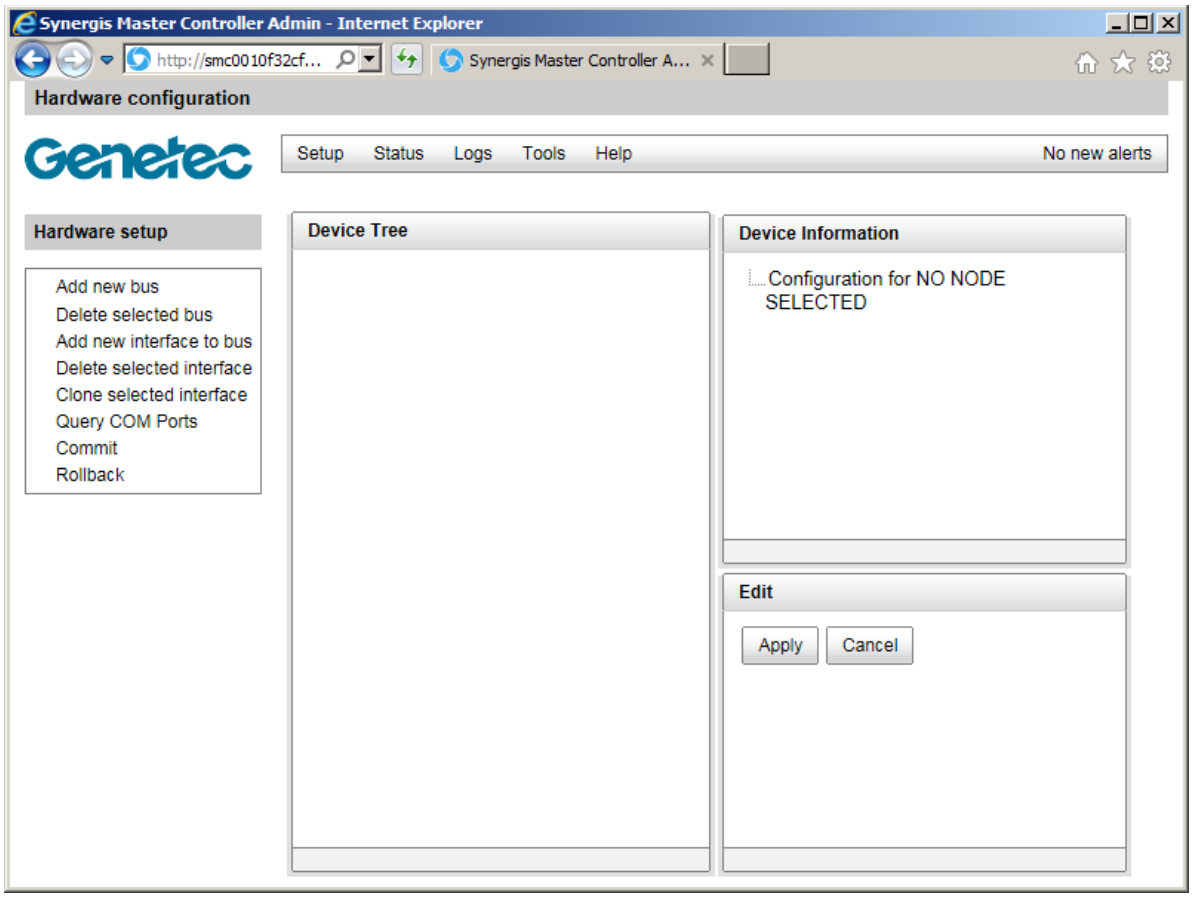
あなたは次のことを完了していることを確認します：

- DDS IP コントローラを登録するための準備。
- Synergis の最新版™ Softwire と *Tibbo.smc* プラグイン。Synergis をチェックし、アップグレードについて™ ファームウェア、参照 *Synergis™ アプライアンスの設定ガイド*。

DDS IP インタフェースモジュールを登録するには：

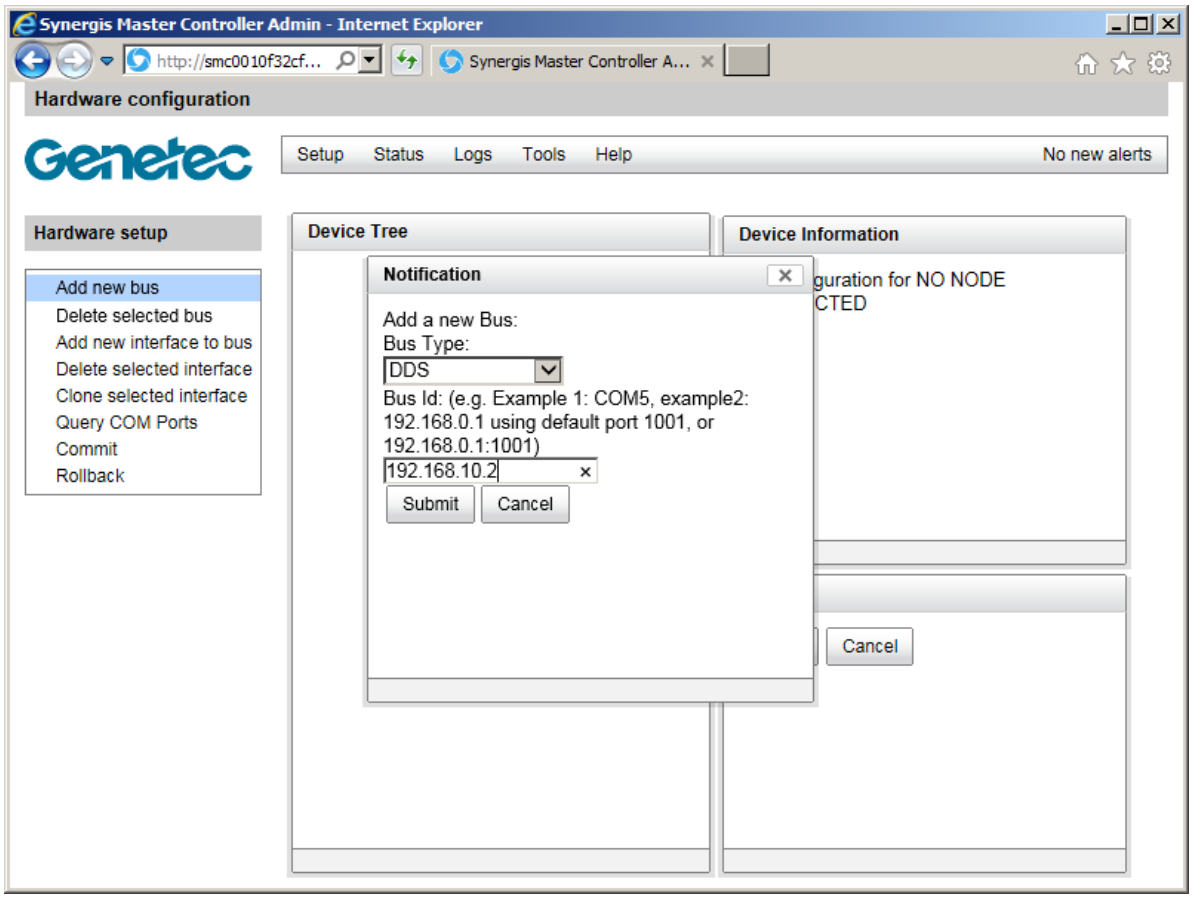
1 Web ブラウザを開きます。

2 ブラウザのアドレスバーに入力します。http：Synergis™ユニットのホスト名または IP アドレスが続い//、 例えば (/smc/index.html 続いて、 `http：//SCL0010F32CF482/smc/index.html`）。



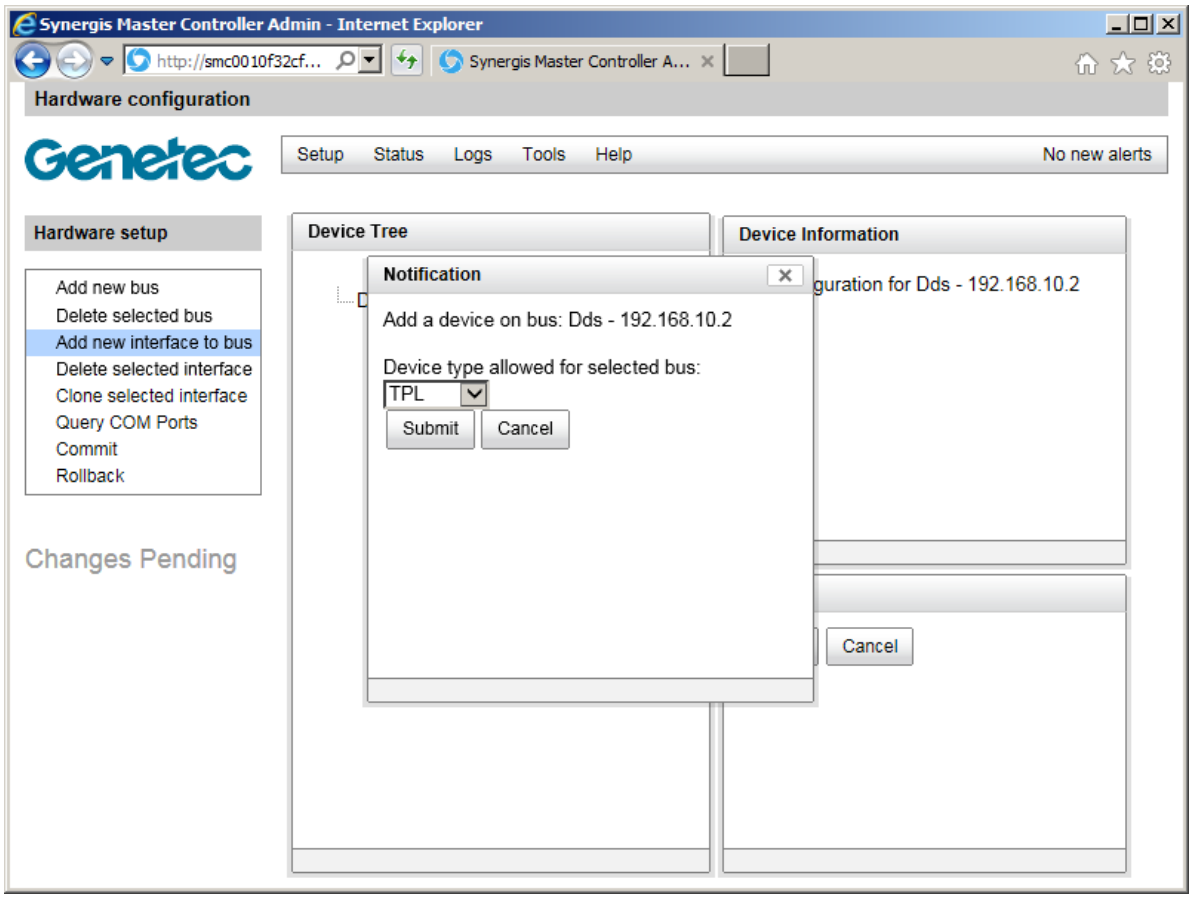
3 新しいバスを追加]をクリックし、バスタイプとして DDS を選択して、DDS IP コントローラに割り当てられた IP アドレスを入力してください。

（「：」）ポート番号はデフォルト値（1001）と異なる場合は、コロンの後に、IP アドレスに追加します。

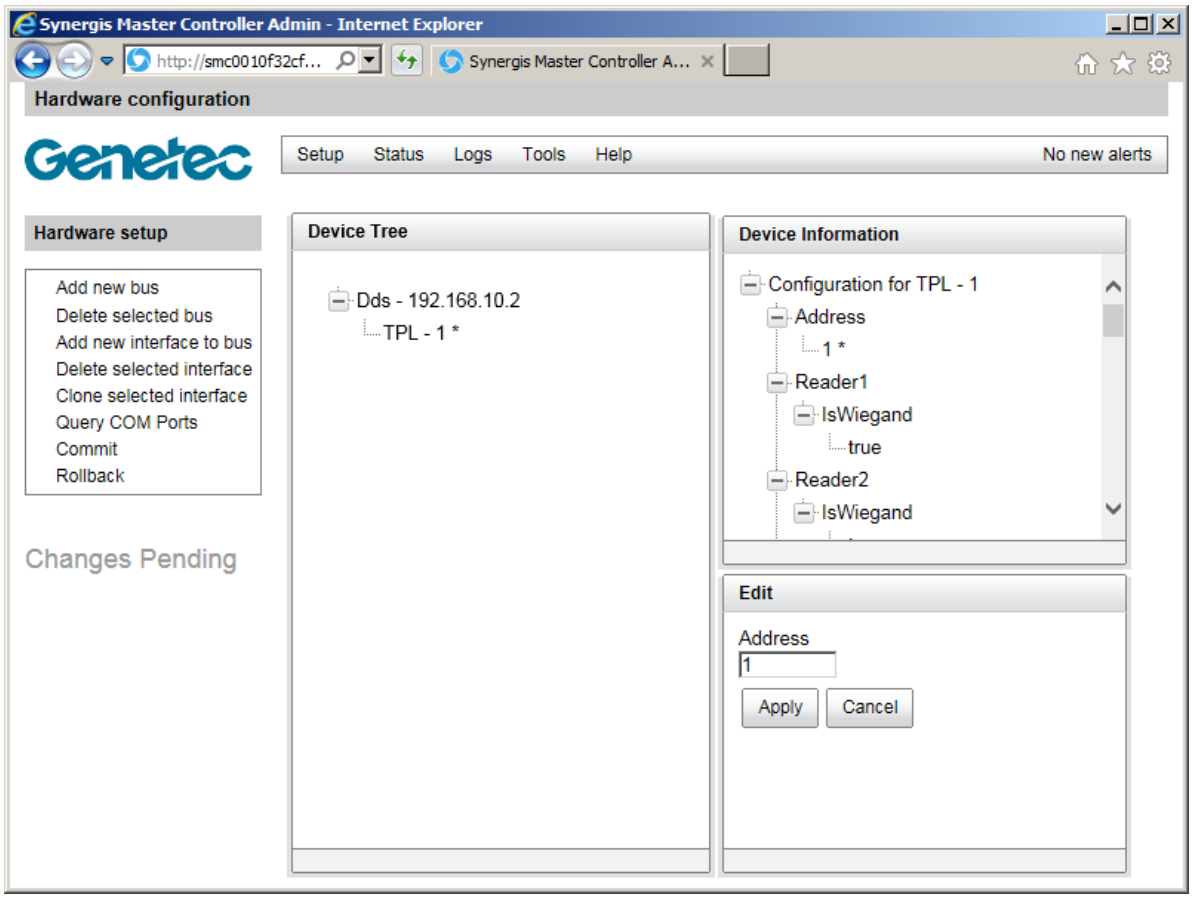


4 の中に **デバイスツリー**、 を選択 **DDS**。
「*」は、それが選択されていることを示すために、バス名の後に表示されます。

5 クリック **バスへの新しいインターフェースを追加します。**選択 **TPL** デバイスタイプとして、[OK]をクリックします **提出します**。



6 デバイスツリーで、追加した TPL デバイスを選択し、住所がで示されていることを確認します
デバイス情報 セクションでは、DDS インターフェースモジュールに設定された物理アドレスに一致します。



7 クリック コミット。

DDS コントローラの Ethernet ポートは、点滅を開始すべきです。

8 Synergis にログオンします™ アプライアンスのポータル、クリックしてください ハードウェア、TPL デバイスをクリックして、あなたとの接続をテスト *I/O の診断* ページ。詳細については、*Synergis™ アプライアンスの設定ガイド*。

あなたが完了した後、

Synergis を登録™ セキュリティセンターでのユニット (参照 *Synergis™ アプライアンスの設定ガイド*) 。

TPL ドアコントローラの物理アドレスを設定します

同じ RS-485 チャネルに接続されているか、同じ LAN 上にあるすべての TPL のモジュールは、異なる物理アドレスを使用する必要があります。

あなたは知っておくべきこと

TPL ドアコントローラの物理アドレスは、DIP スイッチ、DS2 と JP4 の二組を使用して設定されています。あなたは TPL のコントローラボードに取り付けた TCP / IP の拡張ボードを持っている場合は、DIP スイッチにアクセスする前に、あなたはそれを最初に削除する必要があります。

TPL ドアコントローラの物理アドレスを設定するには：

1 1 または ON に DS2 / 1 を設定します。

2 以下の表に従って、JP4 上の物理アドレスを設定します。

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:	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

注意： JP4 (6、7、8) は、リーダ通信プロトコルを設定するために使用されています。例えば、ウィーガンドはパリティチェックなし 50 ビットまで読み出すためには、1 又は ON に 1 または ON に JP4 / 7 を設定し、DS2 / 4。詳細については、お使いの特定のデバイスに対応した DDS からのドキュメントを参照してください。

8

HID VERTX のサブパネル

このセクションでは、次のトピックについて説明します。

Supported HID VertX sub-

HID VERTX サブパネルの統合のために、各 VERTX Vnnn パネルは、インターフェースモジュールと見なされます。

Synergis™Softwire は、次の HID VERTX サブパネルをサポートしています。

モデル	説明	プログラム	EPROM
V100	ウィーガンドまたはクロックおよびデータ資格・フォーマットをサポートする 2 人のカードリーダー付きドア/リーダーインターフェース、。	113	110
V200	16 の監視対象入力回路と入力モニタインターフェース。	106	105
V300	12 ラッチフォーム C リレー接点を有する出力制御インターフェース	107	104

サポートされている HID VERTX サブパネルの機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™Softwire 10.6 には、以下の HID VERTX サブパネルの機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleSub パネル	
コミュニケーション protocolRS-485	
暗号化されました communicationN / A	
オンライン操作（Synergis に接続されています™ 単位）	
監修 MODEN / A	
依存 modeYes	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン MODEN / A	
劣化 modeYes	
リーダーの通信プロトコル	
WiegandYes	
OSDP	N / A
OSDP（セキュア チャネル）N / A	
クロックおよびデータ（磁気ストライプ）- また、ABA として知られています formatYes	
F2F	N / A
ProprietaryN / A	
スケーラビリティ	
オフラインの最大数 eventsN / A	
自律的意思決定のための資格証明書の最大数（ 作成）N / A	
（ビット単位）の最大長資格	
	136
1	
RS-485 チャネルごとインターフェースモジュールの最大数	162

Synergis™単位あたりのインターフェイスモジュールの推奨最大数	HID VertX Sub-32

[1] 認定限度は 136 ビットです。実際の制限は高いかもしれません。

[2] チャンネルごとに多くのインタフェース・モジュールを持つことは、インターフェイスごとのポーリングレートを減少させます。あなたはモード 00 に設定された任意の PIN の読者を持っている場合は、誰かがアクセス拒否になり、すぐに自分の PIN を入力したときに逃したされている数字の可能性を高めるため、これは、考慮すべき事項です。

HID VERTX サブパネルを統合するためのサポート Synergis™アプライアンスの機能

すべての Synergis™アプライアンスの機能は、HID VERTX のサブパネルの統合でサポートされていません。

HID VERTX サブパネルの統合は、以下をサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire* 特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）	
手動登録（*ハードウェアを追加* ダイアログ ボックス）はい	
自動登録 (スキャン ボタン) はい	
プロパティ　configurationYes	
コンフィギュレーション· クローニング (クローン ボタン) はい	
I / O の診断 (入力、リレーのライブ監視、および 読者) はい	
インタフェースモジュールのファームウェア displayNo	
インタフェースモジュールのファームウェアのアップグレード (推奨適用します ファームウェア) いいえ	
アクセス制御の挙動 (Synergis™ ユニット全体の設定) [1、2]	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）オンライン	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）オンライン	
digits3 の最大 PIN 長	15
デグレードモード settingsYes	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）はい	

[1] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

[2] VERTX V100 にのみ適用されます。

[3] HID モード-00 読者をサポートするインタフェースモジュールの場合。

HID VERTX サブパネルを統合するためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、HID VERTX のサブパネルの統合でサポートされていません。

HID VERTX サブパネルの統合は、次のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）1	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeYes	
	拡張助成金 timeOnline	
	エントリの時間（標準/拡張）[2]	オンライン
	ドアリロック - optionsOnline	
	ドアはスケジュールによってロックが解除された場合 - optionsOnline	
	ドア開催します - optionsOnline	
	ドアが開いて強制的に - optionsOnline	
	アンロック schedulesOnline	
	（REX）のオプションを終了する要求	
	REX にロックを解除（オン/オフ）はい	
	アクセスを許可した後 REX を無視する時間（中 オンライン秒）	
	ドアが開いている間 REX イベントを無視 オンライン（オン/オフ）	
	（ドアが閉じた後、REX を無視する時間 オンライン秒）	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒）オンライン	
	ドア上の（オン/オフ）2 人のルールを強制します sideOnline	
セキュリティ Desk3 ドアの手動アクション	手動 doorsOnline のロックを解除	
	シャント Reader は（有効化/無効化 読者）オンライン	
	オーバーライドロック解除 schedulesOnline	

特徴 groupSecurity	センター featureSupported
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン、オフライン*）はい
	交流 failOnline
	バッテリーは（失敗しますローバッテリー）オンライン
	ドア オープン/ closedOnline
	ドア ロック/アンロック オンライン
	ドアの強制 openOnline
	ドアはあまりにもオープン開催しました longOnline
	ドア securedN / A
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）オンライン ビジ
	ター護衛ルール オンライン（オン/オフ）
	InterlockOnline
	Antipassback
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）オンライン [4]
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）オンライン
	両方のエリアの入り口にチェックを厳格（antipassback と 終了）オンライン
	に scheduleOnline
	グローバル antipassbackOnline
	一人称-内のルール
	ドアアンロックに強制 scheduleOnline
	アクセスに施行 rulesOnline
エレベーター コントロール	エレベータ
ー	オンライン
ゾーン管理	I / O zoneOnline
	ハードウェア zoneOnline

[1] VERTX V100 にのみ適用されます。

[2] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされた

ときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンター は、アクセスが許可されたときにエントリがイベントを想定し作成します。

[3] Synergis™ユニットは、Access Manager に接続する必要があります。

[4] エリア内のカード所有者の存在は確認できませんので、カードイン/ REX-アウトドアにはお勧めしません

に接続されている HID VERTX のサブパネルを登録 Synergis™ユニット

Synergis™ユニットと接続されたインターフェイスモジュール間の通信を確立するには、Synergis™アプライアンスポータルでそれらを設定する必要があります。

あなたが始める前に

あなた Synergis™ユニットのチャネル（A、B、C、または D）に HID VERTX モジュールを取り付けます。

Synergis™ユニットに接続されている HID VERTX インターフェイスモジュールを登録するには：

1 Synergis™ユニットにログオンします。
2 クリック **コンフィギュレーション > ハードウェア**
3 の上部には *ハードウェア*列、クリックしてください **加えます** （）。
4 の中に *ハードウェアを追加* 選択]ダイアログボックスで、 **HID VERTX** として **ハードウェアの種類**。
5 を選択 **チャネル**（A、B、C、または D）。
同じチャネルに接続されているすべてのインターフェースモジュールは、同じ製造業者からのものでなければなりません。
6 同じダイアログボックスでは、同じチャネルに接続されているすべてのインタフェースモジュールを追加します。あなたは、自動または手動でインターフェイスモジュールを登録することができます。
先端： あなたはモジュールの物理アドレスを知っているし、あなただけ登録する数を持っている場合、それらを手動で登録するより速くなります。

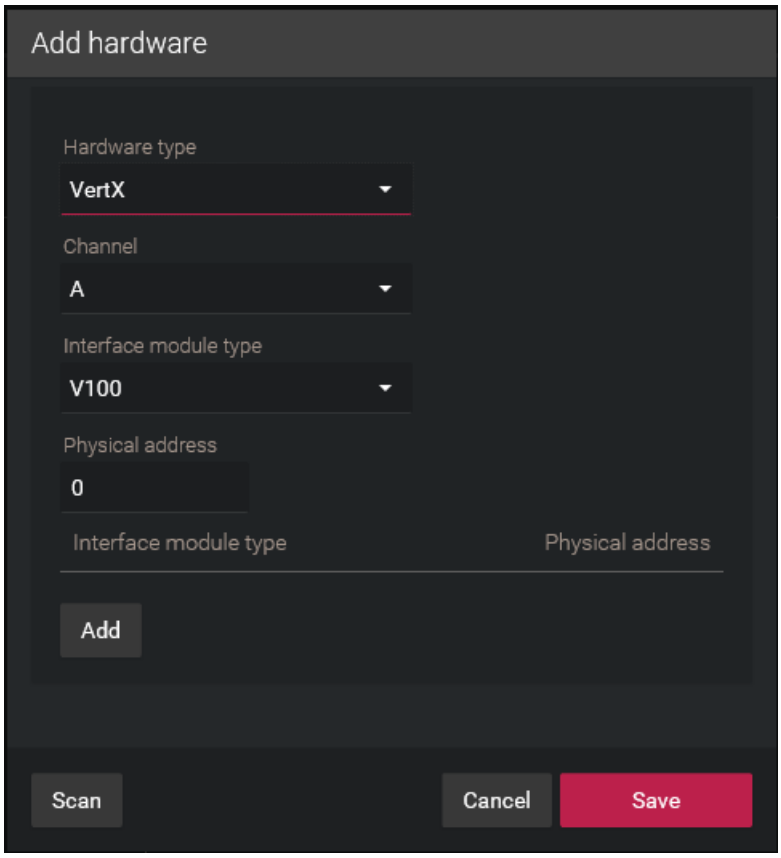
次のいずれかを実行します。

- 自動的に登録するには、[スキャン]をクリックします。

スキャン機能は、同じチャネルに接続されている同じ製造者からのすべてのインターフェース· モジュールを検索し、登録します。

コントローラが接続されているすべてのインタフェース· モジュールが見つからない場合、それらはすべてが異なる物理アドレスを持っていることを確認してください。

- 手動で登録するには、HID インタフェースデバイス上に構成された物理アドレス（0〜15）を入力し、その後、モデルタイプを選択し、そして クリック。



同じチャネルに接続されたすべてのモジュールを構成するために、必要に応じて繰り返します。

7 クリック **セーブ**。
追加したばかりのハードウェアタイプ、チャネル、およびインタフェース・モジュールは、に表示されます *ハードウェア構成*
ページ。

8 **先ほど追加した各インターフェイスモジュールの場合は、ハードウェアの設定ページから、それを選択し、その設定を行います。**
これらの設定の詳細については、製造元のマニュアルを参照してください。必要に応じて変更を加えます。

9 **ページの下部に、[保存]をクリックします。**

10 **I / O の診断ページからごインターフェイスモジュールの接続と設定をテストします。**
インターフェイスモジュールのテストについては、以下を参照してください *Synergis™ アプライアンスの設定ガイド*。

あなたが完了した後、

Synergis を登録™ セキュリティセンターでのユニット (参照 *Synergis™ アプライアンスの設定ガイド*) 。

HID VERTX V100 のための有効リーダー監督

VERTX V100 パネルに接続されたリーダが切断または電源オフのいずれかであるとき、ドアのオフラインイベントを受信するには、私は設定ツールで生きリーダーの設定だと、適切なコンフィギュレーション・カードとリーダーをプログラム設定する必要があります。

あなたが始める前に

Synergis™ユニットの VERTX V100 パネルを登録。

あなたは知っておくべきこと

リーダ監督のみ Synergis™ユニットによって制御される VERTX V100 パネルに接続された読者のために支持されています。この機能を使用するには、Synergis™Softwire 10.2 以降が必要です。

V100 パネルに接続されたリーダの監視を有効にします：

1 設定ツールのホームページで、開きます *アクセス制御* 仕事。

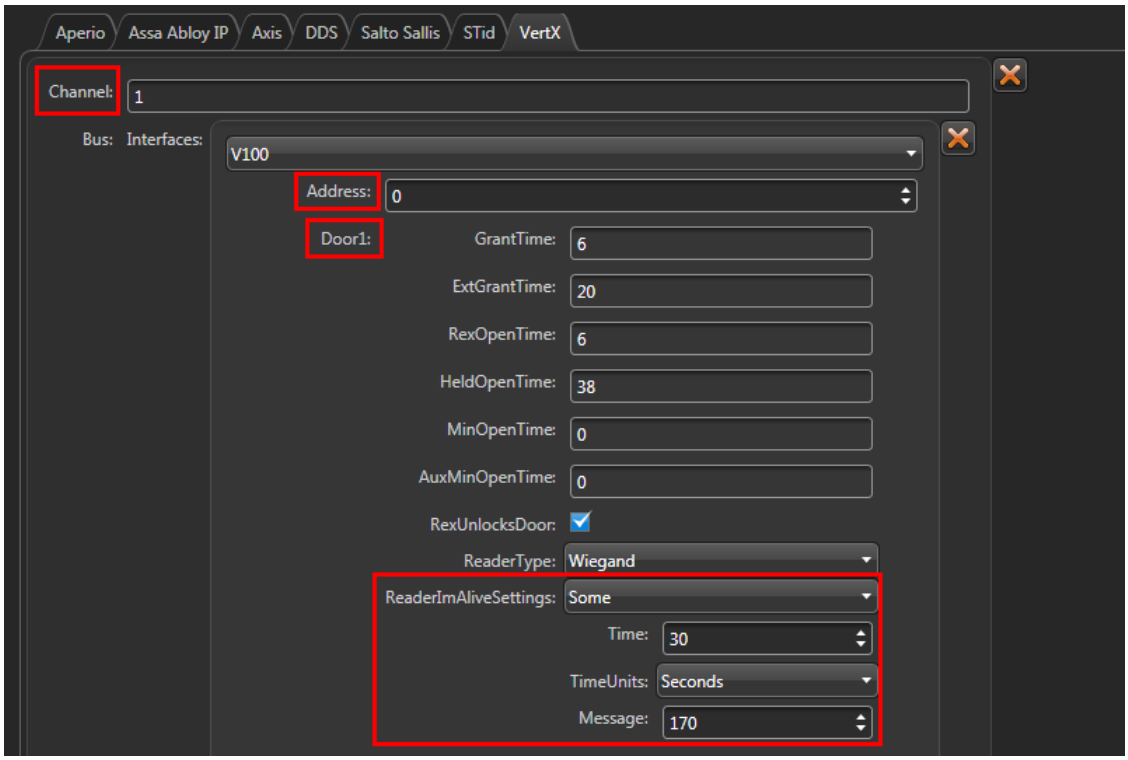
2 クリック 役割とユニット、その後、Synergis をクリック™ 単位 （ ）。

3 ハードウェアをクリックして、読者が接続されている V100 パネルにスクロールします。

あなたの Synergis™ユニットは、複数の V100 パネルを制御している場合は、そのチャンネル、その物理アドレス、およびそのドア数（Door1 または Door2）で正しいリーダーを識別してください。

4 選択されたドアの下に、クリック **ReaderImAliveSettings**、およびその値を変更します 一部。

時間は、私は、リーダ構成カード上に見出さアライブ時間だ等しいかまたはより大きくなければならない、そしてメッセージは、私は ALIVE メッセージ（170 は 16 進数で AA の 10 進数である）よに対応しなければなりません。



5 クリック 適用します。

6 （また、構成カードとしても知られる）は、適切なフィールド・プログラミング・カードを使用して、リーダーを設定します。

この読者は、V100 パネルから切断またはパワーダウンされると、あなたは今イベントのドアをオフラインで取得：デバイスは、それが関連付けられている扉にオフラインになっています。

9

ハネウェルコントローラ

このセクションでは、次のトピックについて説明します。

Supported Honeywell controllers

彼らは Synergis™ユニットに PW6K 下流のパネルを接続するのに役立つので、ハネウェルコントローラの統合については、ハネウェル・コントローラは、インタフェース・モジュールと呼ばれています。

唯一のハネウェル PW6K コントローラは Synergis™ユニットと直接通信します。

注意： ハネウェルコントローラの統合は、セキュリティセンター5.3 SR1（または最新バージョン）と Synergis™Softwire 10.0（またはそれ以上の最近のバージョン）が必要です。

Synergis™Softwire は、次のハネウェル・デバイスをサポートしています。

モデル	説明
PW6K1IC	2 つの教師 RS-485 バスは最大 32 までのいずれかの組み合わせを支持するとともに IP コントローラ I / O 又はリーダサブパネル。PW6K1IC は 64 戸まで制御することができます。
PW6K パネル	PW6K1IC コントローラと共に使用 PW6K 下流パネル（拡張モジュール）： • PW6K1R2 - マーキュリーMR52 に相当する 8 つの入力と 6 つの出力、デュアルリーダサブパネル。 • PW6K1IN - 16 入力サブパネル、水銀 MR16IN に相当します。 • PW6K1OUT - 16 出力サブパネル、水銀 MR16OUT に相当します。
PW5K パネル	PW6K1IC コントローラと共に使用 PW5K 下流パネル（拡張モジュール）： • PW5K1R1 - 2 つの入力と 2 つの出力を有する単一のリーダサブパネル、水銀 MR50 に相当します。 • PW5K1R2 - マーキュリーMR52 に相当する 8 つの入力と 6 つの出力、デュアルリーダサブパネル。 • PW5K1IN - 16 入力サブパネル、水銀 MR16IN に相当します。 • PW5K1OUT - 16 出力サブパネル、水銀 MR16OUT に相当します。
Allegion Schlage ロック	ハネウェル PW6K1IC コントローラも Allegion Schlage AD シリーズのロックを使用することができます。見るサポートされている Allegion Schlage ロック 6 ページ。
SimonsVoss SmartIntego ロック	ハネウェル PW6K1IC コントローラは SimonsVoss SmartIntego ロックとともに使用することもできます。見るサポートされている SimonsVoss ロック 169 ページ。

サポートされているハネウェルのファームウェアバージョン

この統合のすべての機能を利用するためには、ファームウェアバージョンの特定の範囲を使用する必要があります。

Synergis™Softwire 10.6 がサポートしているハネウェルのファームウェアのバージョン：

モデル	最小	推奨
PW6K1IC	2.7.5	2.8.2[A]

[A] このようアッサ・アブロイ IP ロック、軸、水星 EP などの特定のインテリジェントコントローラについて、あなたは Synergis™アプライアンスポータルのインタフェースのアップグレードページから推奨ファームウェアを適用することができます。他のために
メーカーは、あなたが推奨されるファームウェアを適用するために、メーカーのソフトウェアを使用する

Supported Honeywell controllers

必要があります。

Supported features for Honeywell

ハネウェル PW6K シリーズコントローラは、Mercury EP2500 コントローラに非常に似ている、との統合は、Mercury コントローラのと同じ機能セットをサポートしています。

サポートされているハネウェルコントローラの機能

見る サポートされている水銀コントローラの機能 127 ページ。

ハネウェルコントローラを統合するためのサポート **Synergis™**アプライアンスの機能

見る マーキュリーコントローラを統合するためのサポート Synergis™アプライアンスの機能 129 ページ。

注意： ハネウェル PW-シリーズコントローラは、最大 8 桁の PIN をサポートしています。

ハネウェルコントローラを統合するためのサポートされているセキュリティセンターの機能

見る マーキュリーコントローラを統合するためのサポートされているセキュリティセンターの機能 130 ページ。

Synergis™ユニットにハネウェル・コントローラを登録

見る Synergis™ユニットに登録マーキュリー・ コントローラ 137 ページ。

10

マーキュリーコントローラ

このセクションでは、次のトピックについて説明します。

サポートされているマーキュリー・コントローラ

それらは Synergis™ユニットに下流パネル（MR50、MR52 など）を接続するための水銀制御の統合のために、水銀コントローラは、インターフェースモジュールと呼ばれます。

唯一の水星 EP と M5-IC コントローラは Synergis™ユニットと直接通信します。

注意： マーキュリーコントローラの統合は、セキュリティセンター5.3 SR1（または最新バージョン）と Synergis™Softwire 10.0（またはそれ以上の最近のバージョン）が必要です。

Synergis™Softwire は、次の Mercury デバイスをサポートしています。

モデル	説明
EP1501	二つの入力、二つの出力、および 2 つのオンボードリーダー接続の IP コントローラ。一のリーダー接続は EP1501 17 のドアまで制御することができ、8 枚の拡張ボードまで接続することができます。（データシート）
EP1502	8 つの入力、4 つの出力二つリーダ接続、および 32 枚の下流パネルまでサポート 1 RS-485 バスと IP コントローラ。EP1502 は 64 戸まで制御することができます。（データシート）
EP2500	2 つの RS-485 バスと IP コントローラ、64 戸までサポート。（データシート）
EP4502	余分な RS-485 ポートを備えた EP1502 に似た IP コントローラ。（データシート）
氏パネル	EP コントローラでサポートマーキュリー下流パネル（拡張モジュール）： • MR50 - 2 つの入力と 2 つの出力を有する単一のリーダサブパネル（データシート） • MR51e - シングルドア、ネットワーク対応、PoE インタフェースパネル（データシート） • MR52 - 8 つの入力と 6 つの出力を有するデュアル・リーダサブパネル（データシート） • MR16IN - 16 入力サブパネル（データシート） • MR16OUT - 16 出力サブパネル（データシート） より多くを学ぶためにこのビデオを見ます。使用可能な言語の一つで、ビデオのキャプションをオンにするキャプションのアイコン（CC）をクリックします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます **互換表示設定** クリア **互換表示で表示イントラネットサイト**。
Allegion Schlage ロック	EP1501 と EP2500 コントローラは Allegion Schlage AD シリーズロックでも使用することができます。見るサポートされている Allegion Schlage ロック 6 ページ。
SimonsVoss SmartIntego ロック	EP1501 と EP2500 コントローラは SimonsVoss SmartIntego ロックでも使用することができます。見るサポートされている SimonsVoss ロック 169 ページ。

モデル	説明
M5 ブリッジ	すべてのマーキュリーM5 ブリッジパネルは、プラグアンドプレイ、既存の CASI Micro5 エンクロージャと互換性があるように設計されており、既存の panels.1 と 1 対 1 ボードの交換を提供しています • M5-IC - インテリジェントコントローラ (データシート) • M5-2K - 4- F2F リーダ、10 入力 8 出力制御装置 (データシート) 2 • M5-2RP - 2-リーダ制御装置 (データシート) • M5-2SRP - 教師入力を有する 2 リーダ制御装置 (データシート) • M5-8RP - 8-リーダ制御装置 (データシート) • M5-20IN - 20 入力制御装置 (データシート) • M5-16DO - 16 出力制御装置 (データシート) 3 • M5-16DOR - 16 出力制御装置 (データシート) • M5-COM - パワーと途切れコントローラ (データシート) 4 より多くを学ぶためにこのビデオを見ます。使用可能な言語の一つで、ビデオのキャプションをオンにするキャプションのアイコン (CC) をクリックします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます **互換表示設定** クリア **互換表示で表示イントラネットサイト**。
ミズ ブリッジ	すべてのマーキュリーMS ブリッジパネルは、ソフトウェアハウスから ISTAR の Pro パネルの直接の換装できるように設計されています。MS-I8S および MS-R8S パネルはまた、EP コントローラに接続することができます。この統合は、セキュリティセンター5.6 以降が必要です。 • ISTAR プロ GCM モジュールを置き換えるコントローラパネル (- MS-ICS データシート) • ISTAR プロ ACM モジュールを置き換えインタフェースパネル (- MS-ACS データシート) • ISTAR プロ I8 モジュールを置き換える 8 入力パネル (- MS-I8S データシート) • MS-R8S - ISTAR プロ R8 モジュールを置き換え、8 出力パネル (データシート) より多くを学ぶためにこのビデオを見ます。使用可能な言語の一つで、ビデオのキャプションをオンにするキャプションのアイコン (CC) をクリックします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます **互換表示設定** クリア **互換表示で表示イントラネットサイト**。

[1] インタフェースリーダポートから F2F リーダーまたは入力の入力を使用する場合は、設定ツールに示す奇数番目の入力が REX のために使用され、偶数番号の入力は、ドア接点のために使用されます。

[2] 一緒に、M5-IC と M5-2K は CASI M2000 エンクロージャの回路基板を交換してください。M5-IC あたり 8 台のエンクロージャまであります：最初のエンクロージャは 1 M5-IC プラスワン M5-2K を持っており、次の 7 つのエンクロージャは 1 M5-COM プラスワン M5-2K を持っています。

[3] デジタル出力 (ソリッドステートスイッチ)。

[4] アドオンなし M5-IC とエンクロージャとの下り通信に使用されます。

サポートされている水銀のファームウェアバージョン

この統合のすべての機能を利用するためには、ファームウェアバージョンの特定の範囲を使用する必要があります。

Synergis™Softwire 10.6 がサポートしているマーキュリーのファームウェアのバージョン：

モデル	最小	推奨
EP1501、EP1502、EP2500、M5-IC	1.19.4[1]	1.24.4[2]
EP4502	1.20.9[1]	1.24.4[2]
MS-ICS	1.22.9[1]	1.24.4[2]
MR51e	1.4.2	最新

[1] OSDP（セキュアチャネル）リーダーを使用するために、読者は、EP ボードに直接接続されている場合、後でファームウェア 1.22.9 またはが必要であり、読者は下流ボード（赤 SIOv3 MR50 に接続されている場合、ファームウェア 1.23.6 以降が必要とされますそして、MR52 ボード）。

[2] このようアッサ· アブロイ IP ロック、軸、水星 EP などの特定のインテリジェントコントローラについて、あなたは Synergis™アプライアンスポータルのインタフェースのアップグレードページから推奨ファームウェアを適用することができます。他のためにメーカーは、あなたが推奨されるファームウェアを適用するために、メーカーのソフトウェアを使用する必要があります。

注意： ファームウェアバージョン 1.19.4 は、回避策として別々に接続することが F2F リーダーを必要とバグがあります。バグはバージョン 1.20.7 で修正されています。あなたが新しいバージョンにコントローラをアップグレードする場合は、あなたもそれに応じて F2F の読者を再接続してください。

サポートされている水銀コントローラの機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™Softwire 10.6 には、以下のマーキュリーコントローラの機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースモジュールのカテゴリー（EP と インテリジェント M5-IC）	コントローラ
コミュニケーション protocolIP	のみ
暗号化されました communicationYes	[1]
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeNo	
依存 modeYes	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン modeYes	
劣化 MODEN / A	
リーダーの通信プロトコル	
WiegandYes	
OSDP	はい
OSDP（セキュア チャネル）はい	[2]
クロックおよびデータ（磁気ストライプ）- また、ABA として知られています formatYes	
F2F	はい
ProprietaryN / A	
スケーラビリティ	
オフラインの最大数 イベント	50 0003
自律的意思決定のための資格証明書の最大数（ メイキング）	250
000（ビット単位）の最大長資格	644
RS-485 あたりのインターフェイスモジュールの最大数 channelN / A	
Synergis™あたりのインターフェイスモジュールの推奨最大数 単位	2565 分

の 32

[1] 暗号化は Synergis™Softwire 10.2 以降では必須です。

[2] OSDP（セキュアチャネル）リーダーでなければなりません EP コントローラ上のリーダーポートにペア。認定の読者は、次のとおりです。HID マルチクラス SE RP40、Allegion aptiQ MT15-485、およびネクサス Cidron SC9100-MD-MP-VG2。他のモデルでも動作するかもしれません。OSDP（セキュアチャネル）リーダーを使用するために、読者は、EP ボードに直接接続されている場合、後でファームウェア 1.22.9 またはが必要であり、読者は下流ボード（赤 SIOv3 MR50 に接続されている場合、ファームウェア 1.23.6 以降が必要とされますそして、MR52 ボード）。

[3] オフラインログエントリとセキュリティセンターのイベントの間に 1 対 1 のマッチが常にありません。マーキュリーコントローラは 50 の 000 オフライン・ログ・エントリに制限されています。

[4] 最大 8 つの異なる資格長は、スタンドアロンモードでサポートされています。以上がでサポートすることができます

依存モード。

[5] （1）コントローラの最大数は、あなたが物理的にアプライアンスに接続することができ、かつ制御読者の（2）の最大数：2 つのアプライアンスに接続できるコントローラの数を制限値があります。Synergis™クラウドリンクと SV32 の両方のために、EP コントローラおよび制御読者の最大数は 16 と 128 5.4 セキュリティセンターの下で以前のバージョンでは、32 と 256 です セキュリティセンターの下で 5.5 以降。

マーキュリーコントローラを統合するためのサポート Synergis™アプライアンスの機能

すべての Synergis™アプライアンスの機能は、マーキュリー・コントローラの統合でサポートされていません。

マーキュリーコントローラの統合は、以下をサポートしています *Synergis™ アプライアンスのポータル* そして *Synergis™ Softwire* 特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）	
手動登録（*ハードウェアを追加* ダイアログ ボックス）いいえ	[1]
自動登録（スキャン ボタン）いいえ	
プロパティ configurationNo	
コンフィギュレーション・クローニング（クローン ボタン）いいえ	
I/O の診断（入力、リレーのライブ監視、および 読者）いいえ	
インタフェースモジュールのファームウェア displayNo	
インタフェースモジュールのファームウェアのアップグレード（推奨適用します ファームウェア）マニュアル	
アクセス制御の挙動（Synergis™ ユニット全体の設定）[2]	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）N/A	
ドアがあるとき、「DHO」イベントを生成しません。 unrestrictedYes	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）はい	
digits3 の最大 PIN 長	155
デグレードモード 機能設定/ A	

[1] マーキュリー・コントローラは、 設定ツールから登録。

[2] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

[3] HID モード-00 読者をサポートするインタフェースモジュールの場合。

[5] 「＃」は PIN は、15 桁の長さであっても、PIN の後に入力する必要があります。

マーキュリーコントローラを統合するためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は、マーキュリー・コントローラの統合でサポートされていません。

マーキュリーコントローラの統合は、次のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeYes	[1]
	拡張助成金 timeYes	[2]
	エントリの時間（標準/拡張）[3]	オンライン
	ドアリロック - optionsLimited	[4]
	ドアはスケジュールによってロックが解除された場合 - optionsOnline	
	ドア開催します - optionsYes	
	ドアが開いて強制的に - optionsLimited	[5]
	アンロック schedulesYes	
	（REX）のオプションを終了する要求	
	REX にロックを解除（オン/オフ）はい	
	アクセスを許可した後 REX を無視する時間（中 オンライン秒）	
	ドアが開いている間 REX イベントを無視 オンライン（オン/オフ）	
	（ドアが閉じた後、REX を無視する時間 オンライン秒）	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒。）いいえ	
	ドア上の（オン/オフ）2 人のルールを強制します sideNo	
セキュリティ Desk6 ドアの手動アクション	手動でロックを解除 doorsYes	
	シャント Reader は（有効化/無効化 読者）はい	
	オーバーライドロック解除 schedulesYes	

Feature group	Security Center	Supported
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン、オフライン*）はい	
	交流 failYes	
	バッテリーは（失敗しますローバッテリー）はい	
	ドア オープン/ closedYes	
	ドア ロック/ unlockedYes	
	ドアの強制 openYes	
	ドアはあまりにもオープン開催しました longYes	
	ドア securedN / A	
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル管理）いいえ	ビ
	ジター護衛ルール（オンオフ）	Yes
	7	
	InterlockOnline	
	Antipassback	
	ハード（ログとのアクセスを拒否します *Antipassback 違反*）オンライン	[8]
	プレゼンスタイムアウトは（特定の後に地域の存在を忘れます 遅延）オンライン	
	両方のエリアの入り口にチェックを厳格（antipassback と 終了）オンライン	
	に scheduleOnline	
	グローバル antipassbackOnline	
	一人称-内のルール	
	ドアアンロックに強制 scheduleN / A	
	アクセスに施行 rulesN / A	
エレベーター controlElevatorsYes		[9]
ゾーン管理	I / O zoneOnline	
	ハードウェアゾーン	
	ゾーンアーミング inputOffcenter	[10]
	ゾーンアーミング scheduleYes	

Feature group	Security Center	Supported
	ゾーンアーミング、エントリ delaysNo	

Feature group	Security Center	Supported
	ゾーン I / O linkingYes	
	カウントダウン buzzerNo	

[1] サポートされる最大値は 255 秒です。

[2] ザ・ **拡張許可時間** より短くすることはできません **標準許可時間**。

[3] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされたときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[4] 開口がまだ依然として後ロック開口部が閉じるオプションを再ロックを特徴とした後、タイムアウトと再ロックするように構成されたグラント timeout.A ドア、後ロック近いオプションの再ロックを特徴とした後にタイムアウトと再ロックするように構成されたドア助成金のタイムアウト。

[5] のために **リーダーのブザーの動作** 、オプションの設定 *抑制* そして *ドアが閉じたときに抑制* オンラインとオフラインの動作モードの両方でサポートされています。*オプション アクセスが許可されたときに抑制* 扱われます *ドアが閉じたときに抑制*。

[6] Synergis™ユニットは、Access Manager に接続する必要があります。

[7] 制限：護衛を必要と訪問者が誰か他の人の護衛である任意のカード保有者に護衛することができます。セキュリティセンターでは、訪問者に割り当てられている護衛は EP コントローラによって強制されていません。

[8] エリア内のカード所有者の存在は確認できませんので、カードイン/ REX-アウトドアにはお勧めしません

[9] フロアの追跡がサポートされていません。すべての階のボタンが 1 つの EP コントローラによって制御されなければなりません。異なるボードからの出力リレーを使用することができるが、連続ブロックに割り当てる必要があります。これは、エレベータは複数のボード間で設定されている場合、ボード A の最後の出力は、ボード B 上の第一の出力が続かなければならないということを意味します。

[10] ゾーンは、イベント・ツー・作用を介してドアにリンクされている、とマーキュリーコントローラがオフラインで動作している場合は、ゾーンが動作しません（Synergis™ユニットに接続されていません）。

マーキュリーコントローラを登録するための準備

あなたは Synergis™ユニットのマーキュリーコントローラを登録する前に、コントローラに静的 IP アドレスを割り当てる必要があります。

あなたが始める前に

あなたは次のことを持っていることを確認してください：

- **EP シリーズのセットアップおよび構成ガイド。** あなたの水星コントローラの Web ポータルに接続し、その IP アドレス（および他の構成）を設定するための取扱説明書。
- **静的 IP アドレス。** IT 部門によってコントローラに割り当てられた静的 IP アドレス。
- **物理アドレス。** 同じ水銀コントローラの同じ RS-485 ポートに接続されている各インタフェースパネルは、（DIP スイッチで構成された）固有の物理アドレスを持っていなければなりません。

ベストプラクティス： あなたは同じ Synergis™ユニットに登録する多くのマーキュリー・コントローラを持っている場合、それは、一度にすべてを登録するのが最善です。追加または Synergis™ユニットから取り外した各マーキュリー・コントローラは、ユニットを再起動するようになります。ユニットが再起動しますが、それは、約 30 秒間オフラインになっています。

あなたは知っておくべきこと

同じ Synergis™ユニットに登録マーキュリー・コントローラは、セキュリティセンター内の異なるパーティションを割り当てることはできません。あなたは、別のパーティションにマーキュリー・コントローラを割り当てる異なる Synergis™単位でそれらを登録し、別のパーティションに Synergis™ユニットを割り当てる必要がある場合。

注意： 硬化でタグ付けされたステップや命令はオプションですが、サイバー攻撃からシステムを保護します。

水銀コントローラを登録するために準備するには

1 水銀コントローラボード上、ON に DIP スイッチ S1-1 を設定します。
これはあなたの工場出荷時のデフォルト設定を使用してログオンするために 5 分間のウィンドウを提供します。

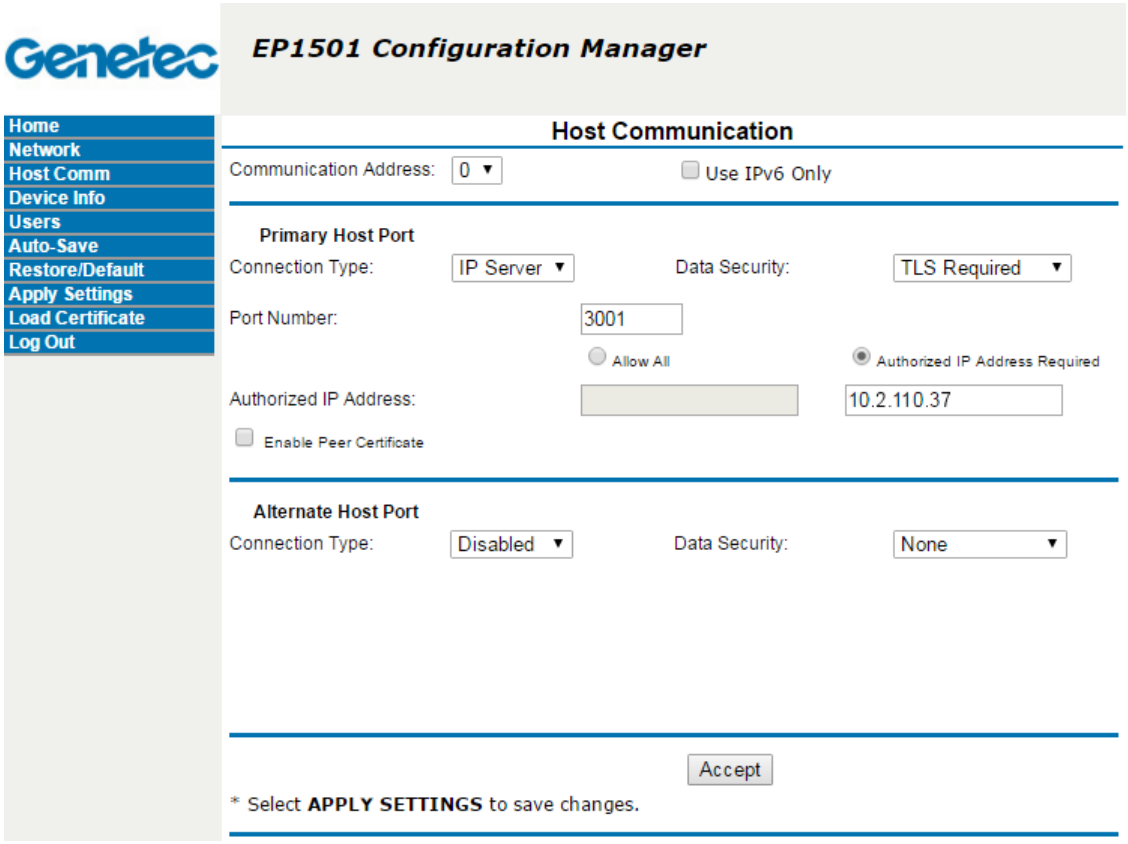
2 Mercury デバイスの構成マネージャの Web ページを介しマーキュリーコントローラにログオンします。デフォルトの IP アドレス（192.168.0.251）と証明（管理者/パスワード）を使用します。詳細については、製造元のマニュアルを参照してください。

より多くを学ぶためにこのビデオを見ます。クリック**キャプション**アイコン（**CC**）使用可能な言語の一つで、ビデオのキャプションをオンにします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます**互換表示設定**クリア **互換表示で表示イントラネットサイト**。

3 **選択 ネットワーク メニューから、水星、コントローラの設定 IP アドレス、およびクリック 受け入れます。**

4 選択 **ホストコム** メニューから。

5 の中に *ホスト通信* ページには、以下の設定を行い、[OK]をクリックします **受け入れます。**

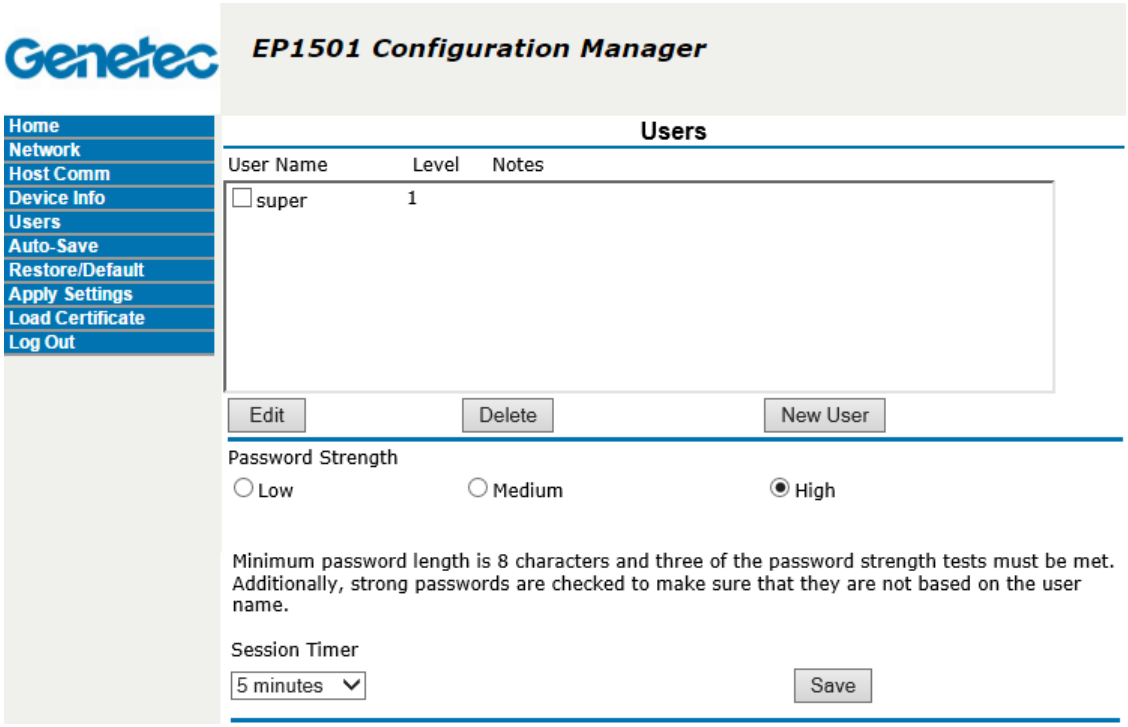


- 通信アドレス： 0 に設定すると混同しないように チャネル あなたは Synergis のマーキュリーコントローラを登録するときには、一意である必要があります™ 単位。
- データセキュリティ： に設定 *TLS 必須*。

  重要： この設定は、セキュリティセンターと通信 Synergis™Softwire 10.2 以降のバージョンでは必須です。TLS が選択されていない場合は、水星 EP コントローラがオフラインのままです。
- ポート番号： 水銀コントローラ (デフォルト= 3001) と通信するために Synergis™ユニットによって使用されるポート番号。
- 必要な認可 IP アドレス： (*硬化*) は、このオプションを選択し、設定 承認された IP アドレス Synergis の IP アドレスに™ 単位。

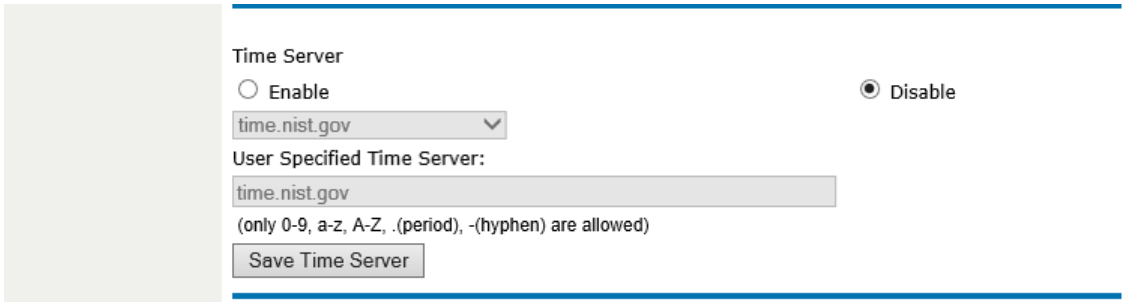
6 選択 **ユーザー** メニュー、およびクリックから **新しいユーザー**。

マーキュリーコントローラ上でユーザーアカウントを作成すると、あなたの物理的なユニットにアクセスするために、あなたは、コントローラの設定を変更し、次回オンに DIP スイッチ S1-1 を設定する手間を省くことができます。

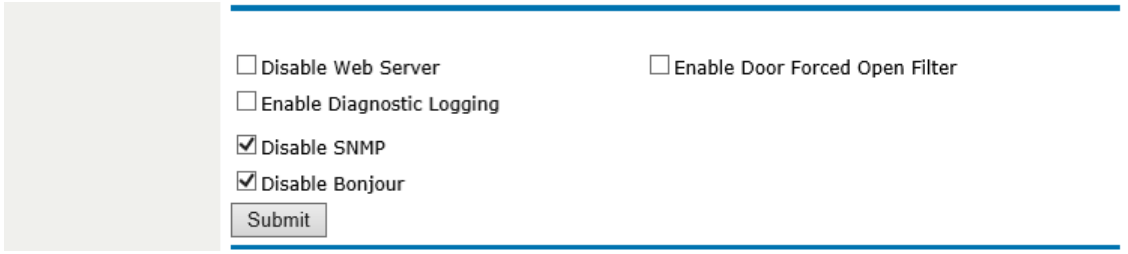


7 （*硬化*）オン ユーザー ページ、入力します。 **ユーザー名** そして **パスワード**、お よびクリック **セーブ**。をセットする**パスワードの強度** に **高い**。

8 （*硬化*）オン ユーザー ページ、無効 **タイムサーバ**。
タイムサーバは必要ありません。Synergis™Softwire **は監視し、自動的に** EP **単位で時間を設定しま す。**



9 （*硬化*）オン ユーザー ページ、無効 **SNMP** そして **ボンジュール**、およびクリック **提出します**。



10 選択 **設定を適用** クリックします **設定の適用、再起動します。**

11 **水銀コントローラボード上に、通常の動作のために** OFF **に** DIP **スイッチ** S1-1 **を 設定します。これは、コントローラにログオンするために使用されているから、工 場出荷時の設定を防ぎます。**

12 続行するプロンプトが表示されたら、選択 **私は理解して続行したいです**、[OK]をクリックします **はい**。

あなたが完了した後、

Synergis™ユニットのマーキュリーコントローラを登録。

Synergis™ユニットに登録マーキュリー・コントローラ

Synergis™ユニットは、それに接続された水銀コントローラと通信させるには、[セキュリティセンターの設定ツールを使用してそれらを登録する必要があります。

あなたが始める前に

入学のためのマーキュリーのコントローラを準備。

あなたは知っておくべきこと

Synergis™ユニットに登録マーキュリーコントローラは Synergis™アプライアンスポータルからは見えません

ハードウェアページ。

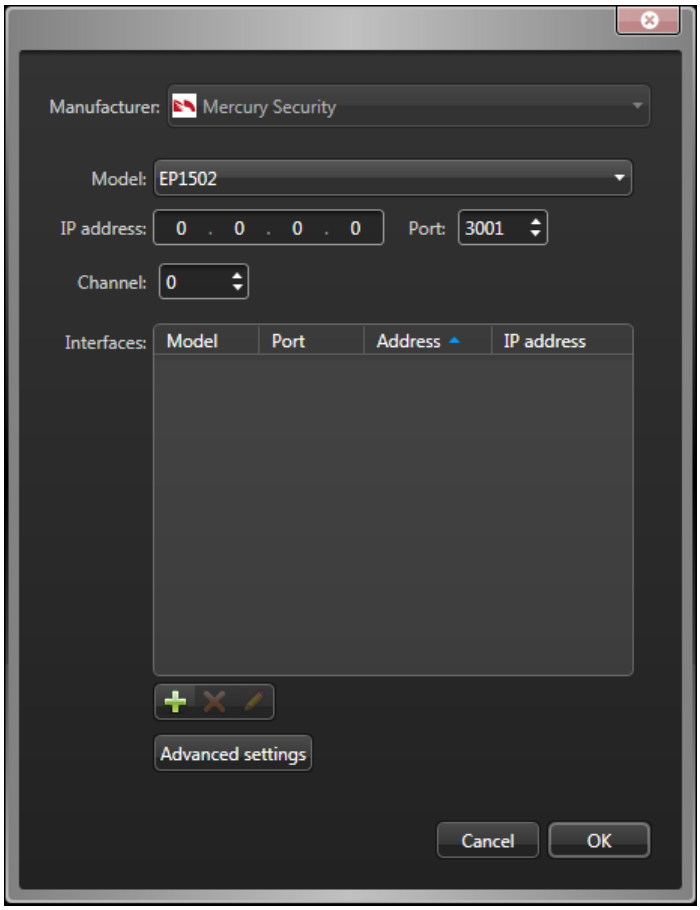
Synergis™部に、各水銀コントローラによって一意のチャネル ID を割り当てなければなりません。すべてのマーキュリー・コントローラは、インタフェースパネル (MR50、MR52、MR16IN、および MR16OUT) が接続された RS-485 バスを持っています。同じ RS-485 バスに接続された各インタフェースパネルは、固有の物理アドレスを持っている必要があります。

Synergis™ユニットに接続された水銀のコントローラを登録します。

1 設定ツールのホームページで、開きます *アクセス制御* 仕事。

2 **クリック 役割とユニット、その後、Synergis をクリック™ 単位** ( ) 。

3 クリック **周辺機器**、[OK]をクリックします **アイテムを追加します。** ( ) 。



4 **次の情報を入力します。**

- **モデル：** コントローラのモデル。

- **IP アドレス：** IT 部門によってコントローラに割り当てられた静的 IP アドレス。
- **ポート：** 通信ポート（デフォルト= 3001）。ポートは、Mercury デバイスマネージャの Web ページで構成されている値と一致する必要があります。
- **チャネル：** このコントローラに対応するチャネル ID。チャネル ID は 0 の間の任意の値とすることができますおよび 63、および Synergis™ユニット内で一意でなければなりません。割り当てられたら、それは変更してはいけません。

5 選択したコントローラモデルが下流のパネルをサポートしている場合は、それらを追加します。

注意： 次のことを考えてみます。

- MR51e の PoE パネルの場合、EP コントローラを登録した後、それらを追加。
- 水星によって推奨されているように、EP1501 コントローラあたり 8 枚の下流パネルの限度を超えないようにしてください。
- M5-20In パネルは、通信バス上の 2 つの連続したアドレスを占めています。M5-20In パネルの 20 個の入力を持つために、あなたはあなたの M5-IC への設定ツールで 2 枚の M5-20In パネルを追加する必要があります
コントローラ。第一のパネルのアドレスが M5-20In ボード上の物理アドレスと一致している必要があり、及び第二のパネルのアドレスは、最初のパネルに加えていずれかのアドレスに設定されなければなりません。

a) 以下 *インタフェースグループ*、クリックしてください **アイテムを追加します。** （）。

b) 表示されるダイアログボックスで、モデル、ポート、アドレス（0〜31）、及び下流パネルの IP アドレスを（MR51e のみ）を選択します。
同じポートに接続されているすべてのパネルは、異なるアドレスを使用する必要があります。

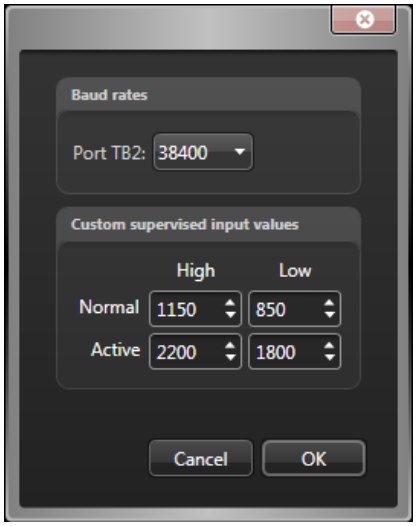
c) クリック **[OK]**。

d) 必要に応じて繰り返します。

より多くを学ぶためにこのビデオを見ます。クリック**キャプション** アイコン（**CC**）使用可能な言語の一つで、ビデオのキャプションをオンにします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます**互換表示設定** クリア **互換表示で表示イントラネットサイト**。

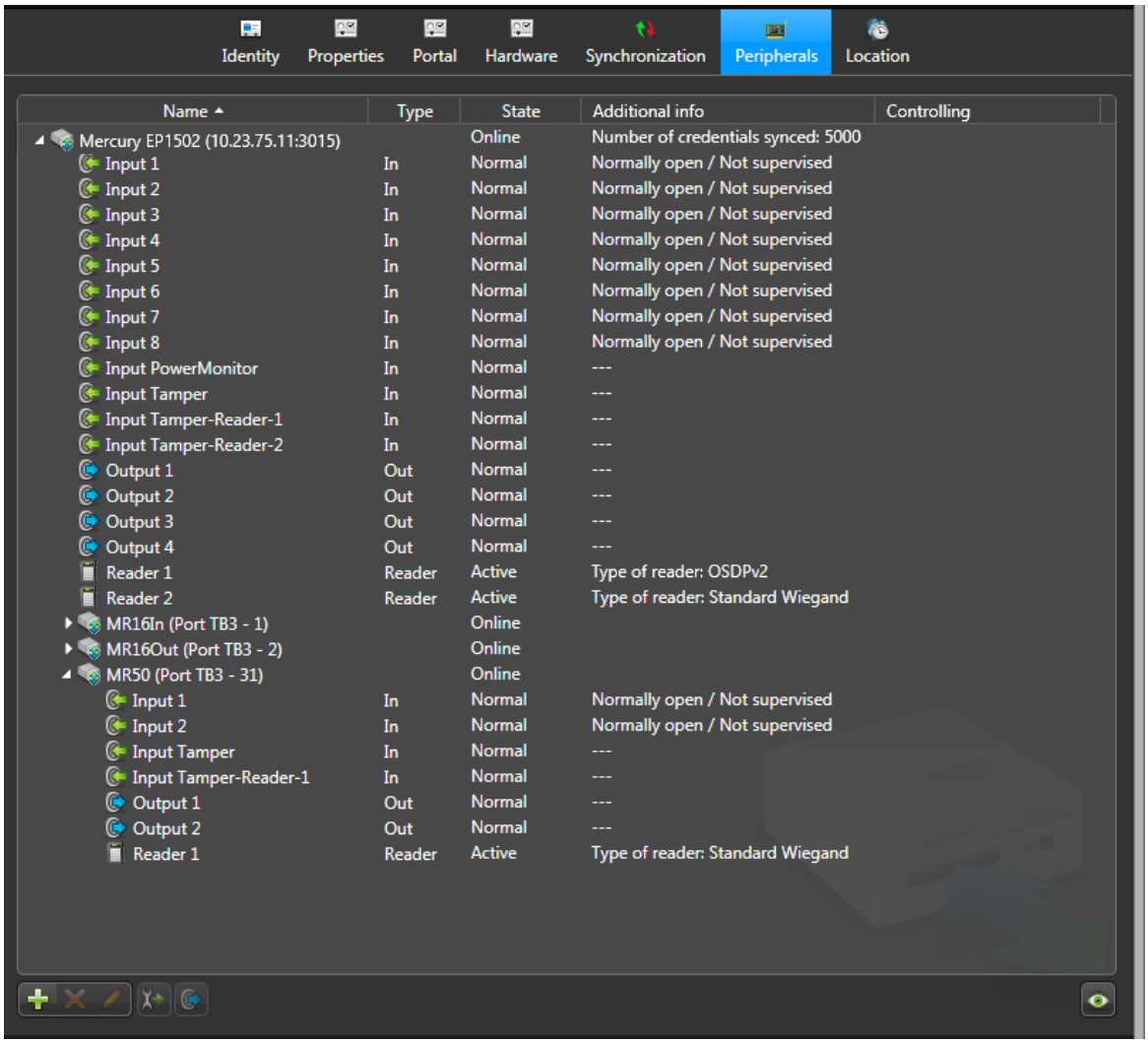
6 （オプション）をクリックして **高度な設定** 高度な設定を変更します。

使用可能な設定は、選択したコントローラのモデルによって異なります。あなたは一般的に使用可能なシリアルポートのボーレートを変更することができ、およびカスタムは、入力値を監修しました。



7 ダイアログボックスの下部にある[OK]をクリックします。

8 クリック **適用します** （）。
すべての添付の下流パネルと周辺機器との水銀コントローラに表示され
周辺機器 タブ。



注意： Synergis™ユニットにインターフェースモジュールを追加すると、ユニットは、ソフトウェアの再起動を実行させます。このプロセスの間に、Synergis™ユニットとそれに接続されているすべての周辺機器は、（赤）をオフラインで表示されます。

9 発見された I / O デバイスと読者のそれぞれを選択し、 そのプロパティを設定します 必要に応じて。

OSDP について（セキュアチャネル）の読者は、参照します EP コントローラに OSDP（チャネルセキュア）読者を追加 に 140 ページ。

10 入力と出力をトリガすることによって、あなたの配線と構成をテストします。

トリガーI / O は、画面上でリアルタイムに状態が変化します。

注意： リーダーの活動はに示されていません **周辺機器** タブ。

あなたが完了した後、

EP コントローラに MR51e パネルを追加します。（該当する場合）、[セキュリティセンターのドアやゾーンへのインターフェイス· モジュールの物理的な配線をマップします。

EP コントローラに OSDP（チャネルセキュア）読者を追加

EP コントローラに OSDP（セキュアチャネル）リーダーを追加するには、まず設定ツールを使用して EP コントローラ上のリーダーを構成し、Synergis™アプライアンスポータルを使用して EP コントローラにリーダーをペアリングする必要があります。

あなたが始める前に

あなたの Synergis™ユニットにその下流のパネルを使用して EP コントローラを登録。この機能は、セキュリティセンター5.6 SR2 以降が必要です。

あなたは知っておくべきこと

あなたの EP コントローラに OSDP（セキュアチャネル）リーダーを追加するには、それが接続されているボードを読者（鍵の exhange）をペアリングする必要があります。リーダーがしっかりリーダーポートにペアリングされた後は、工場出荷時にリーダーをリセットせずに別のリーダーポートにセキュアモードでそれをペアリングすることはできません。

OSDP を追加するには、あなたの EP のコントローラにリーダー（チャネルを保護）：

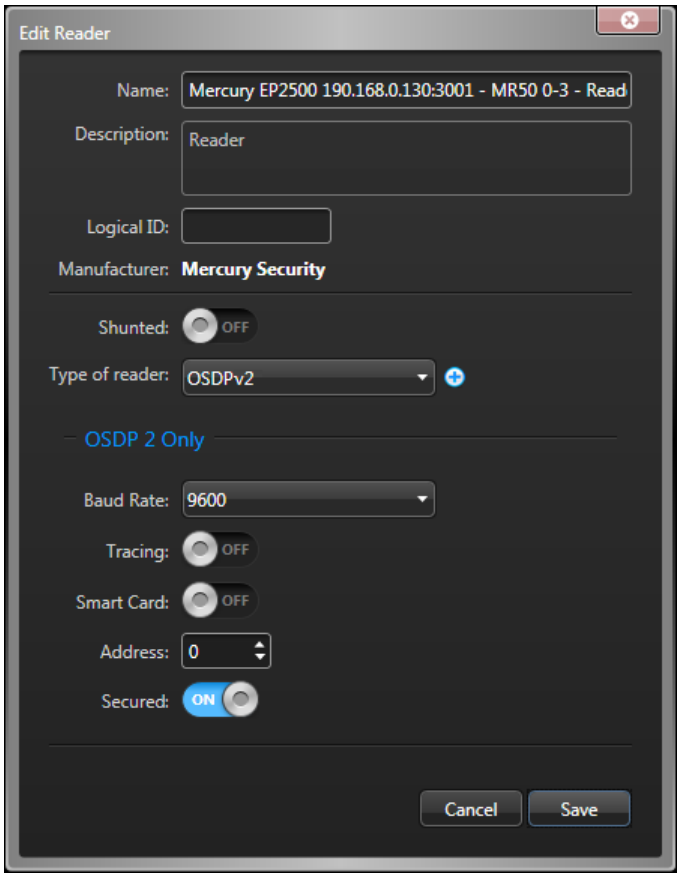
1 設定ツールでは、開きます *アクセス制御* タスク、およびクリック **役割とユニット**。

2 Synergis を選択™ 単位（ ）をクリックします **周辺機器**。

3 必要に応じて、下流の MR パネルと周辺機器を参照するために EP コントローラを展開します。

4 （読者をクリックします ）あなたは（[編集]を設定し、クリックします ）。

5 の中に *編集リーダー* ダイアログボックス、クリックしてください **リーダーのタイプ** リストドロップダウン、および選択 **OSDP（セキュアチャネル）**。



ザ・ **確保** オプションをオンにする必要があります。

6 他の OSDP（セキュアチャネル）必要に応じて固有の設定を行い、[保存]をクリックします。

7 Web ブラウザを介して Synergis™ユニットに接続します。

注意： この操作のために Synergis™アプライアンスポータルを使用していません。

a) ブラウザタイプの https の URL フィールドに：// <ユニット> /smc/index.html、<単位>ドメイン名または Synergis™ユニットの IP アドレスです。

例：HTTPS：//scl0cbf15003cd8/smc/index.html または https://10.160.18.15/smc/index.html を

b) の中に *ログイン* ページ、入力します。 **ユーザー名** そして **パスワード**、およびクリック **ログイン**。

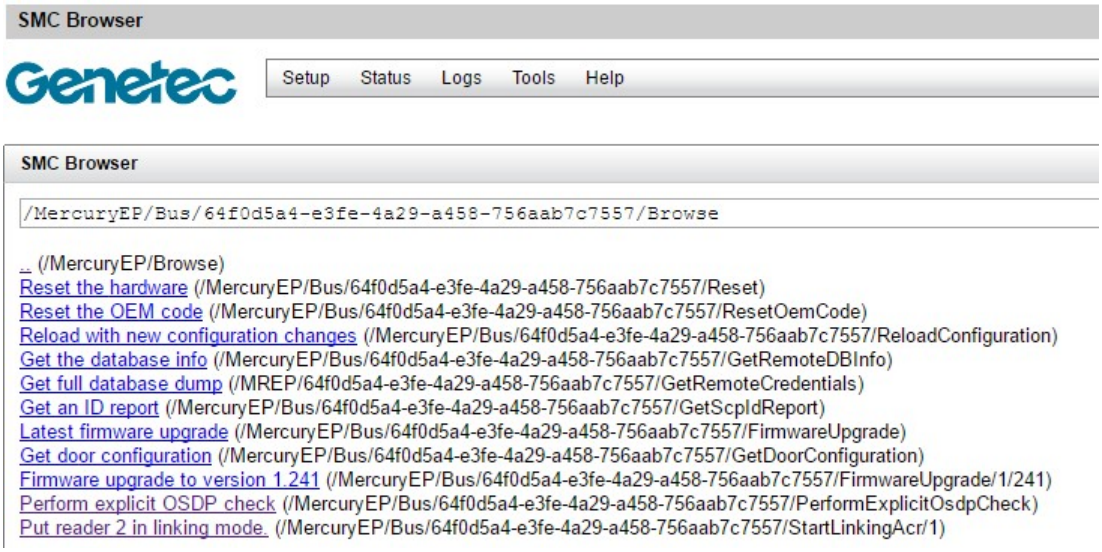
Synergis™アプライアンスポータルを通じてログオンするときに使用するのと同じユーザ名とパスワードを使用してください。

8 の中に *ハードウェア構成* ページ、クリックしてください **ツール > 高度**。

9 の中に *SMC Broswer* ページ、クリックしてください **水星 EP デバイスツール**。

10 リフレッシュページで、クリックしてください **バス「NNNN」** ここで、 *NNNN* EP コントローラの IP アドレスです。

11 リフレッシュページで、クリックしてください **リンクモードにリーダーX** ここで、 *リーダーの x* あなたが設定ツールで OSDP（セキュアチャネル）とセキュアとして設定リーダーです。



ペアリングプロセスが完了したら、読者は設定ツールでオンライン表示されます。

EP コントローラに MR51e パネルを追加

MR51e は EP コントローラを介して制御されなければならない単一のドアの PoE パネルです。MR51e パネルは EP コントローラと通信するために、あなたはどちらか（推奨）パブリック DHCP または静的 IP アドレッシングモードを使用する MR51e パネルを設定する必要があります。

あなたが始める前に

次のことを確認してください：

- まだ行っていない場合は、と MR51e パネルをロード サポートされるファームウェアバージョン。
- あなたの Synergis™ユニットに EP コントローラを登録。
- MR51e パネルは静的 IP アドレッシングモードを使用している場合は、ダウンロードしてください *MSC MR51e アドレス設定ツール* マーキュリーのウェブサイトから。

あなたは知っておくべきこと

公共 DHCP、および静的 IP：Synergis™Softwire を通じて Mercury インテグレーションのために、あなたは 2 つだけのアドレッシング・モードで MR51e パネルを使用することができます。

あなたの EP コントローラに MR51e モジュールを追加するには：

1 次のいずれかを実行します。
   - 公共 DHCP を使用するように MR51e パネルを設定します（推奨）。
   - 静的 IP を使用するように MR51e パネルを設定します。
2 設定ツールでは、開きます *アクセス制御* タスク、およびクリック **役割とユニット**。
3 （Synergis™ユニットを選択）、および MR51e パネルを追加します。
   詳細については、下流側にパネルを追加するための手順を参照してください 上の登録マーキュリー・コントローラ Synergis™ユニット 137 ページ。

MR51e を設定すると、公共 DHCP アドレッシング・モードを使用するには

お使いのネットワークが DHCP をサポートしている場合、公共の DCHP のアドレッシングモデルを使用するように MR51e パネルを設定することをお勧めします。

公共 DCHP を使用するように MR51e パネルを設定するには：

1 MR51e パネルに、S1（構成 DIP スイッチ）を '0001' に設定。ON に設定された DIP スイッチ 4、3、及び OFF の 2、及び DIP スイッチ 1。
2 プレス S2（リセットスイッチ）。

MR51e を設定すると、静的 IP アドレッシングモードを使用するには

お使いのネットワークが DHCP をサポートしていない場合は、静的 IP アドレス指定のモデルを使用するように MR51e パネルを設定します。

あなたが始める前に

ダウンロード MSC MR51e アドレス設定ツール お使いのコンピュータにインストールします。MR51e パネルは、コンピュータと同じサブネットに接続されていることを確認します。

静的 IP を使用するように MR51e パネルを設定するには：

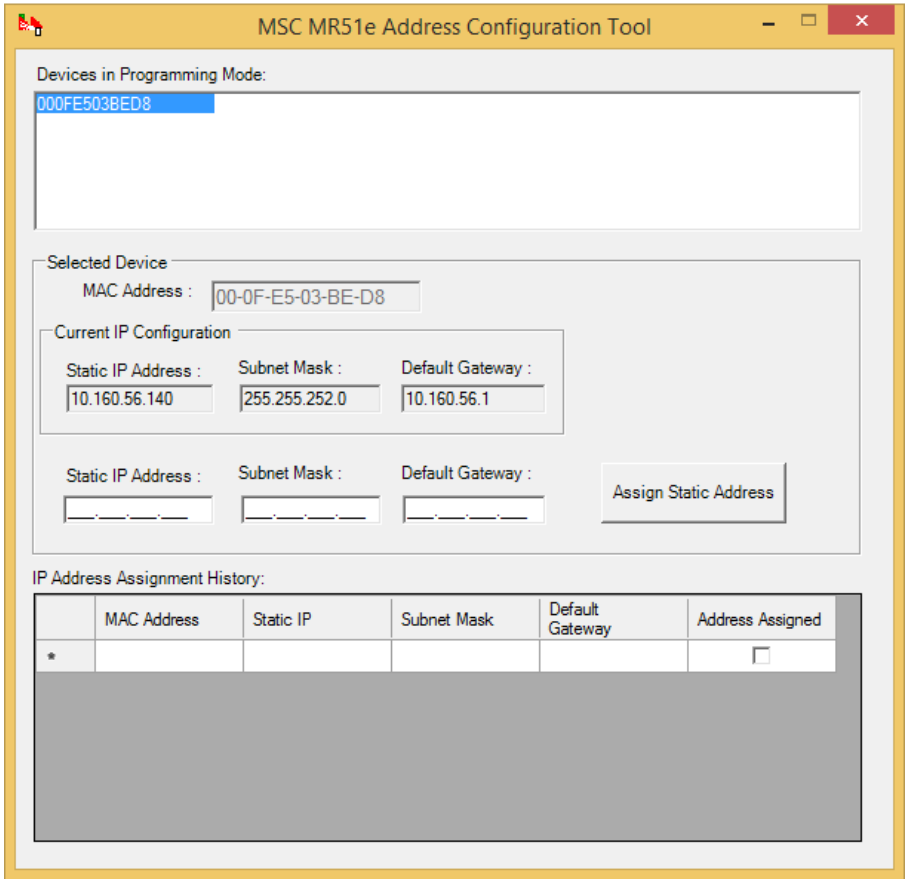
1 MR51e パネルに、S1（構成 DIP スイッチ）を '0011' に設定。

ON と OFF に設定 DIP スイッチ 4 と 3 を、および DIP スイッチ 2 及び 1。

2 開きます MSC MR51e アドレス設定ツール。

3 プレス S2 (リセットスイッチ) 。
検出されたら、MR51e パネルの MAC アドレスがに表示されます **プログラミングモードのデバイス** リスト。

4 の中に **プログラミングモードのデバイス** リスト、プログラムすることが MR51e パネルを選択します。選択 MR51e パネルの MAC アドレスがに表示されます**選択したデバイス** フィールド。



5 値を入力します。**静的 IP アドレス**、**サブネットマスク**、および **デフォルトゲートウェイ**、および クリック **静的アドレスを割り当てます**。
入力された値は、で表示されます **現在の IP 設定** グループとで **IP アドレスの割り当ての歴史** リスト。

6 MR51e パネルに、S1 (構成 DIP スイッチ) を '0010' に設定。ON に設定された DIP スイッチ 4、3、及び OFF 1、及び DIP スイッチ 2。

7 プレス S2 (リセットスイッチ) 。

アクセス制御部 - Synergis™ - 周辺機器]タブ

このセクションでは、アクセス制御タスクで、Synergis™アクセス制御ユニット周辺機器]タブにある設定を示しています。それらに接続されているすべての下流パネルと共に階層ビューには、このタブが表示され、ユニットに接続されているすべてのインターフェースモジュール。

周辺機器]タブでは、追加のインタフェース･モジュールを削除し、ユニットに接続されている周辺機器（リーダおよびI/Oデバイス）の名前と設定を変更することができます。

このページに表示される情報は以下のとおりです。

- **名：** インタフェースモジュールまたは周辺機器の名前。周辺機器は、デフォルトでは、階層ビューに表示されます。

  クリック **表示モード**（）を選択します *フラット表示* あれば、それはあなたの好みです。
- **タイプ：** ペリフェラルタイプ： *に*（入力）、 *でる*（出力）、 *リーダー*。それは、周辺でない場合は、ブランク。

  （出力リレーのみ）をクリックして **トリガ出力**（）リストの一番下にある（出力動作を送信しますアクティブ、*ノーマル*、または *パルス*）選択されたデバイスに関する。
- **状態：** 周辺状態を生きます： *アクティブ*、 *ノーマル*、 *分流さ*（入力とリーダのみ）、 *トラブル*（入力のみ）、または

  未知の。

  接続インターフェイスモジュールをテストし、I/Oデバイスの配線構成を検証するには、この列を使用。
- **追加情報：** 周辺のタイプに固有の設定。

  （周辺機器をダブルクリックするか、[編集]をクリックします）リストの一番下に選択された周辺の設定を編集します。
- **制御：** この周辺で制御エンティティ（ドア、エレベーター、ゾーン）。

  （ヘジャンプクリック）選択された周辺機器によって制御されるエンティティの設定タブを表示するリストの下部にあります。
- **論理ID：** マクロとSDKプログラムでの参照を容易にするために、この周辺に割り当てられた論理IDを（デフォルトでは非表示）。
- **物理名：** システムにより、この周辺に割り当てられた静的な名前を（デフォルトでは非表示）。

先端： 周辺機器を監視する場合、このページの情報は、システムステータスタスクからもセキュリティデスクのユーザーに利用可能です。

追加および削除することができますインターフェイスモジュール

あなただけの周辺機器]タブからあなたSynergis™ユニットに取り付けマーキュリー･コントローラ（EPとM5-IC）を追加および削除することができます。インターフェイスモジュールの他のすべてのタイプのために、あなたは、ハードウェアタブで、またはSynergis™アプライアンスポータルのハードウェアのページのいずれかを介してそれらを追加する必要があります。

編集可能なリーダーの設定

編集可能なリーダーの設定は次のとおりです。

- **名：** リーダーの名前。
- **論理ID：** 同じユニットに接続されているすべての周辺機器の中で一意でなければなりません。
- **分流さ：** 読み込みを無視するには、このオプション

  ョンを選択します。このアクションは、また、

  セキュリティデスクから発行することができます。

- **リーダーのタイプ：** お使いのリーダーに対応するタイプを選択します。可能なリーダータイプのリストは、あなたが持っているインターフェースモジュールの種類によって異なります。カスタムリーダーのタイプを選択すると、手動ですべての読者のオプションを設定することができます。

編集可能な入力設定

編集可能な入力の設定は次のとおりです。

- **名：** 入力デバイス名。
- **説明：** 入力の説明を（読み取り専用）。
- **論理 ID：** 同じユニットに接続されているすべての周辺機器の中で一意でなければなりません。
- **分流さ：** 入力を無視するには、このオプションを選択します。分流されると、入力の状態は、あなたがそれをトリガーに関係なく、どのように、ノーマルのままです。
- **デバウンス：** 入力が変化した状態にすることができる時間の量は、（例えば、にアクティブから変更しました
  *ノーマル*状態変化が報告されている）の前に。このオプションは、不安定な信号をフィルタリングします。
- **コンタクトタイプ：** 通常の入力接点の状態とその監督モードを設定します。
  - **教師なし/ノーマルクローズ：** 入力接点の正常な状態が閉じられ、アクセス制御部は、入力がトラブル状態にあることを報告しません。
  - **ないノーマルオープン/監修：** 入力接点の正常な状態が開いており、入力がトラブル状態にある場合、アクセス制御部は報告されません。
  - **4 状態はノーマルクローズ/監修しました：** 入力接点の正常状態が閉じられ、アクセス制御部レポート入力は、故障状態にあるとき。
  - **4 状態は、ノーマルオープン/監修しました：** 入力接点の正常な状態が開いており、入力がトラブル状態にあるとき、アクセス制御部が報じています。
  - **カスタム：** あなたは、アクティブおよび通常の入力状態の値のカスタム範囲を設定することができます。実際の値は、マーキュリー・コントローラの詳細設定で設定されています。

編集可能な出力設定

編集可能なリーダーの設定は次のとおりです。

- **名：** 出力デバイス名。
- **論理 ID：** 同じユニットに接続されているすべての周辺機器の中で一意でなければなりません。

11

OSDP リーダー

このセクションでは、次のトピックについて説明します。

Supported OSDP readers in Synergis™ Softwire

唯一の読者は交換する必要があるためセキュアなオープン教師付きデバイスプロトコル（OSDP）を使用すると、大規模なインフラ投資をせずにウィーガンド読者から離れて移動することができます。

次 OSDP の読者は、認定されたと Synergis™Softwire 10.6 でサポートされています。その他 OSDP 読者も正常に動作する可能性があります。

メーカー	モデル	認定ファームウェア
Allegion	aptiQ MT14-485 X14_14 リーダー	FW1212
HID	マルチクラス SE RPK40EKTB リーダー	00312-F、00316-F
STID	ARCR31BPH52B1	ARC-R3x-XSZ235A03_04InitMem.hex

サポート **Synergis™**アプライアンス

OSDP の読者は、RS-485 ボードを搭載した Synergis™クラウドリンクまたは Synergis™マスターコントローラ上の RS-485 ポートに直接接続します。

Streamvault™アプライアンスは、RS-485 ポートが装備されていないので、直接の互換性がありませんされています OSDP リーダー。

Synergis™ユニットに接続され OSDP リーダーを事前登録

あなたは Synergis™ユニットに OSDP リーダーを登録するには、まずプログラミングモードを通じて事前登録する必要があります。

あなたが始める前に

- あなたの読者は、有線またはネイティブ OSDP ソリューションのために再配線されていることを確認します。
- すべての読者がパワーダウンしていることを確認します。

あなたは知っておくべきこと

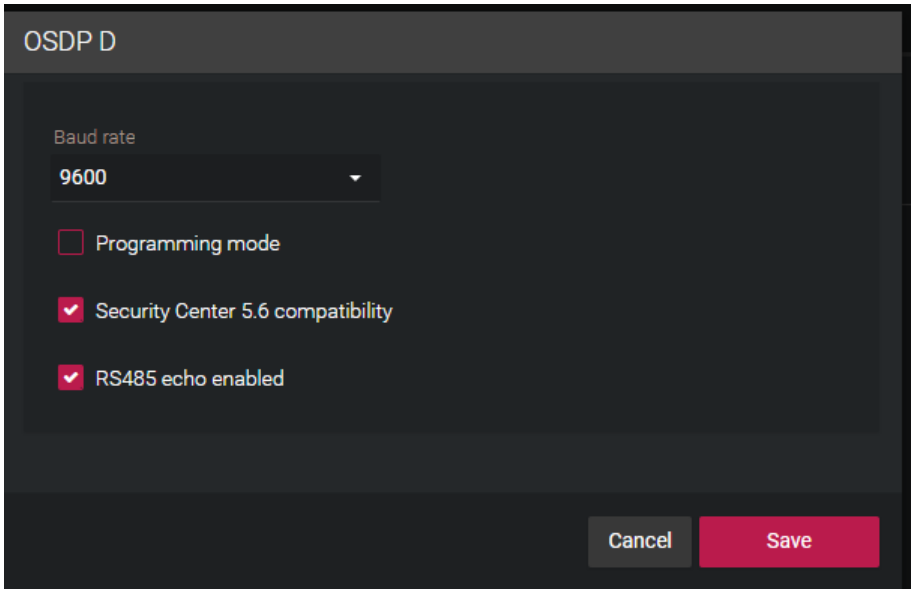
コントローラの応答時間を増加させるように、同じ RS-485 チャネルに個以上の OSDP (規則的またはセキュアチャネル) リーダを接続することは推奨されません。

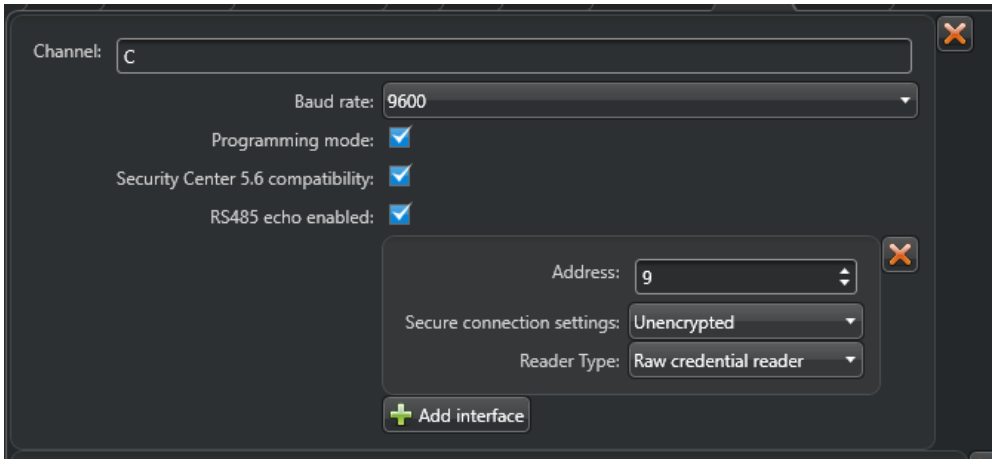
Synergis™ユニットに接続され OSDP リーダーを事前登録するには：

1 設定ツールのホーム· ページから、ハードウェアのタスクを開きます。

2 OSDP を選択し、[チャンネルを追加]をクリックし、コンテキストに応じて、A、B、C、または D のチャンネルを設定します。

3 クリック **プログラミングモードを有効にします** チェックボックスをオンにします。





4 クリック **インタフェースを追加**、その後、目的の RS-485 のアドレスを設定します。

5 RS-485 バスから 1 人のリーダーにパワーアップ。これは、アドレスを受信し、オンライン表示されます。
6 読者の電源を切ります。
7 新しい RS-485 アドレスを入力して、変更を適用します。
8 次のリーダーの電源をオンにします。それは、アドレスを受信します
9 すべての読者は、事前登録されるまで、8〜ステップ 4 を
繰り返します。10 無効化プログラミングモード

あなたが完了した後、

読者を登録。

Synergis™ユニットに接続入学 OSDP リーダー

Synergis™ユニットは、それに接続され OSDP リーダーと通信するためには、Synergis™アプライアンスポータルでそれらを登録する必要があります。

あなたが始める前に

- プレステージ OSDP の読者は、。
- お使いのリーダーのファームウェアが最新であることを確認して、 Synergis™ Softwire でサポートされています。

あなたは知っておくべきこと

OSDP の読者を事前登録した後、あなたは Synergis™ユニットにそれらを登録することができます。

ユニットに接続された **OSDP** リーダーを登録します。

1 設定ツールでは、クリックしてください アクセス制御 > 役割とユニット。次に、あなたの Synergis を選択™ クラウドリンクまたは Synergis™ マスターコントローラとそのを開きます **OSDP** タブ。
2 事前登録 OSDP チャネルの一つを選択し、インタフェースを追加]をクリックし、最初のリーダーに対応したアドレスを追加します。
3 残りの読者のために繰り返します。

あなたが完了した後、

登録読者のセキュリティを有効にします。

OSDP リーダーにセキュアモードを有効にします

デフォルトでは、OSDP の読者は、暗号化されていない状態で登録されています。暗号化を有効にすると、アクセス・ポイントのセキュリティを向上させます。

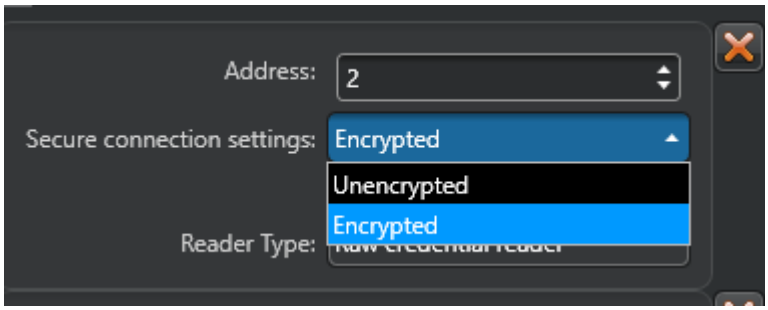
あなたが始める前に

OSDP リーダーを登録。

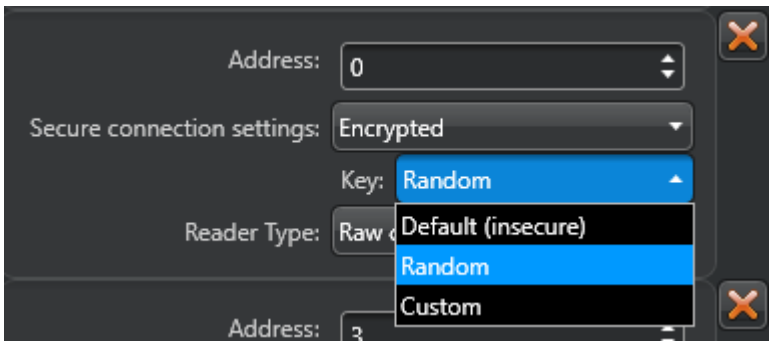
あなたの **OSDP** の読者に暗号化を有効にするには：

1 設定ツールでは、クリックしてください アクセス制御 > 役割とユニット。次に、あなたの Synergis を選択 ™ ユニットとそのを開きます
OSDP タブと OSDP リーダーのいずれかを選択します 在籍。

2 をセットする **セキュアな接続設定** ドロップダウンに *暗号化されました。*



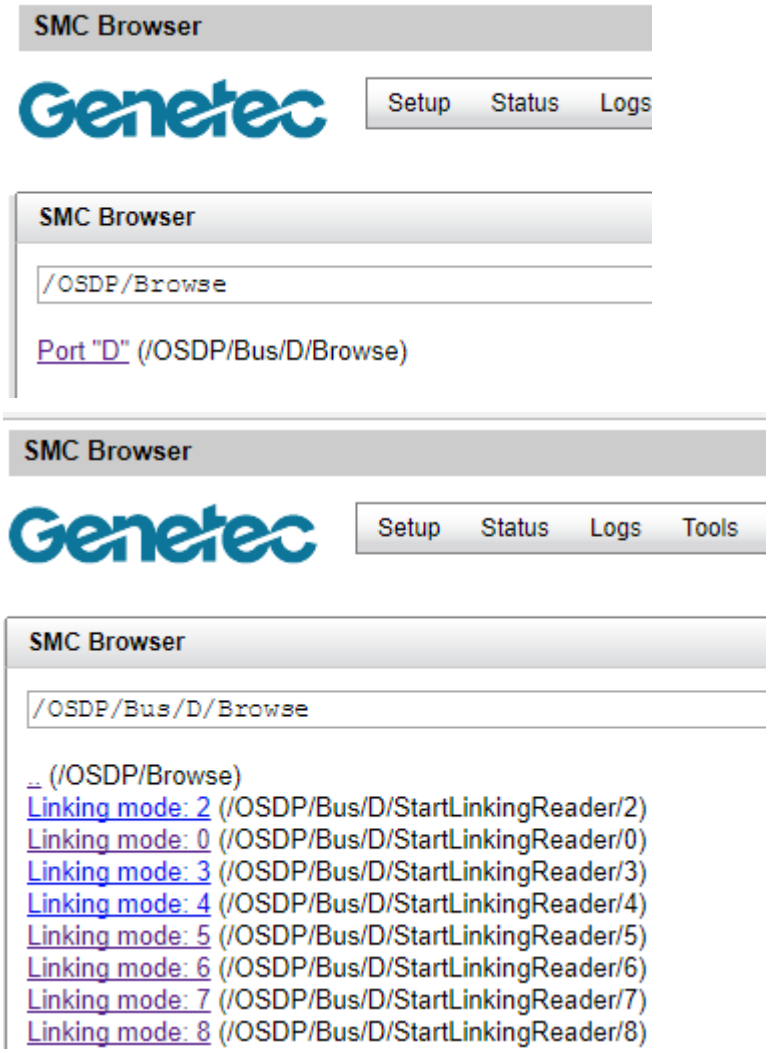
3 主なドロップダウンランダムに設定します。代わりに、あなたはあなた自身の 128 ビット（32 進数文字）を指定したい場合キー、[カスタム]を選択。



4 繰り返しは、残りの読者のため 1—3 ステップ。
あなたが特定のキーを使用するように Synergis™Softwire に語っているが、読者はまだそれらのキーを使用して構成されていないとして、この時点で、読者は、オフラインになります。

5 Web ブラウザを介して Synergis™ユニットに接続します。
注意： この操作のために Synergis™アプライアンス・ポータルを使用していません。
https に移動します。<単位>はドメイン名または Synergis™ユニットの IP アドレスです// <ユニット> /smc/index.html#page=/OSDP/Browse、。
例： HTTPS：
`//scl0cbf15003cd8/smc/index.html#page=/OSDP/Browse` か
`https://10.160.18.15/smc/index.html#page=/OSDP/Browse`

6 あなたが設定ツールでの最初の読者のために指定したポートをクリックし、読者への鍵を送信するには、次のページにリンクするモードをクリックしてください。



7 繰り返しは、残りの読者のために、手順 5 と 6。

これは、鍵を交換し、読者は、設定ツールでオンラインに戻ってくるだろう。そして、彼らは、セキュアになります。暗号化は Synergis™Softwire 側で有効になっている場合は、キーを拒否何読者がオンラインに戻って来ないだろう。

12

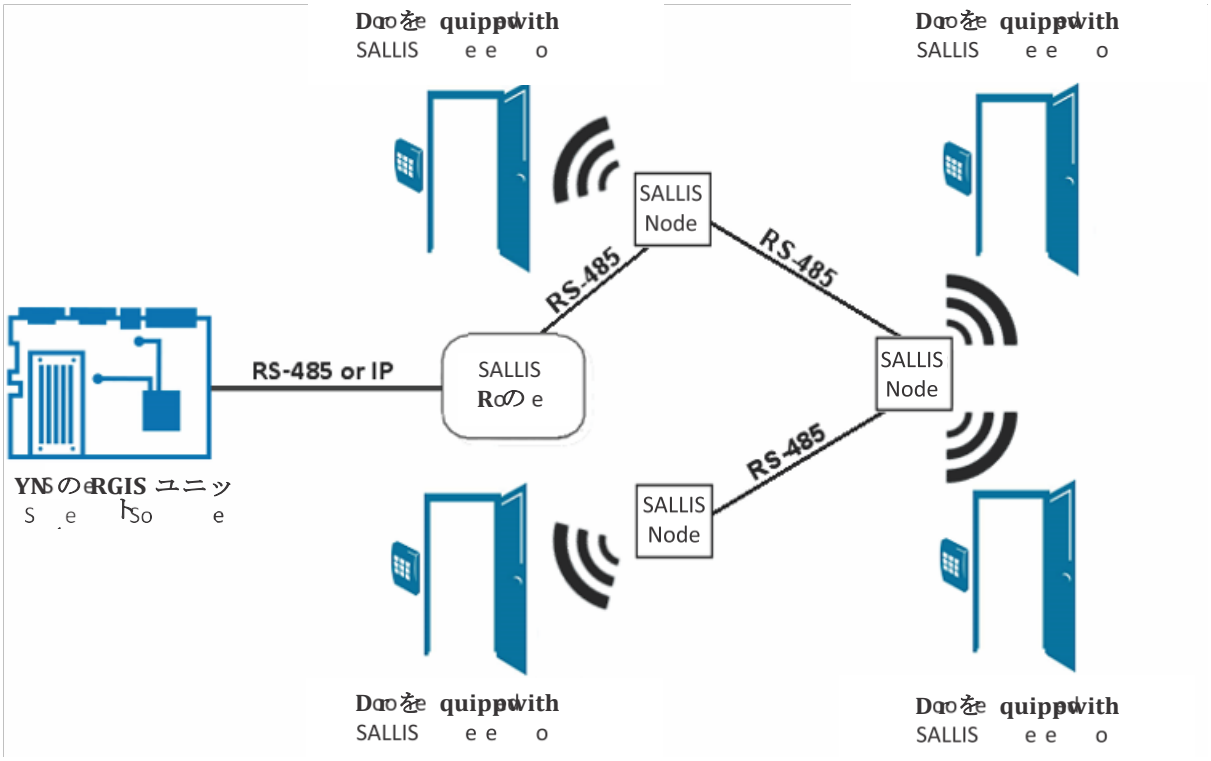
サルト Sallis ワイヤレスロック

このセクションでは、次のトピックについて説明します。

SALTO SALLIS integration overview

サルト SALLIS ワイヤレスロックは SALLIS と通信 SALLIS ルータに RS-485 バスを介して接続されたノード。SALLIS ルータは、その後、いずれかの RS-485 チャネルまたは IP チャネルを介して、Synergis™ユニットと通信します。

以下の図は Synergis™ユニットが SALLIS (サルトロックリンクシステム) システムを介して SALTO SALLIS ワイヤレスロックと通信する方法を示しています。



注意： SALTO SALLIS ワイヤレスロックは、非インテリジェントなロックです。これは、すべてのアクセス制御の決定を行うために Synergis™ユニットに依存しています。

Supported SALTO SALLIS hardware

SALTO SALLIS 統合のため、Synergis™ユニットは、その IP チャネル又はその RS-485 チャネルの 1 つに接続されている無線ルータを介して SALLIS ロックに接続します。各 SALLIS ロックは、インターフェースモジュールと見なされます。

Synergis™ Softwire は、次の SALTO SALLIS デバイスをサポートしています。

モデル ファームウェア	説明	サポートされている
SALLIS 00-59 RS485 ルータ	Synergis を接続 SALLIS RS-485 ルータ™ 無線（RF）通信ノードのユニット。	01.11
SALLIS 00 から 72 の PoE ルータ	Synergis を接続 SALLIS PoE 対応ルータ™ 単位 無線（RF）通信ノードへ。	01.06
SALLIS 00 から 71 ミニノード	に取り付けられた SALLIS RF 通信ミニノード SALLIS の PoE ルータボード。一つだけのミニノードは、ルータごとに追加することができます。	02.00
SALLIS 00-60 ノード	間 SALLIS RF 通信ノード SALLIS ルータと SALLIS ロックシステム。これは、RS-485 および PoE ルータの両方で動作します。	02.00
SALLIS 00 から 38 XS4 ロック	物理的に制御するために使用 SALLIS ロックシステム 前提へのアクセス。	02.00

重要：ロックにバッテリーを変更した後、常にそれを再初期化し、ルータを再起動します。

サポートされている SALTO SALLIS 機能

インタフェースモジュールは、すべての形や大きさに来て、機能の広い範囲を提供しています。Synergis™Softwire が市場に見られる共通の機能のほとんどをサポートしています。

Synergis™Softwire 10.6 には、以下の SALTO SALLIS の機能をサポートしています。

特徴	サポートさ
一般的な特性	
インタフェースのカテゴリー moduleElectronic	ロック
コミュニケーション プロトコル	（IP または RS-485）1
暗号化されました コミュニケーション	IP と RS-485
オンライン操作（Synergis に接続されています™ 単位）	
監修 modeNo	
依存 modeYes	
オフライン操作（Synergis への接続なし™ 単位）	
スタンドアロン modeNo	
劣化 modeNo	
ワイヤレス操作	
上 Synergis™ユニットにお問い合わせください eventOn	読む
スケジュールラジオ contactEvery	8 秒。
電池 チェック	10 分ごと。
パワーロックの設定に失敗（フェイルセーフ/フェイル セキュア）N / A	
スケーラビリティ	
オフラインの最大数 eventsN / A	
自律的意思決定のための資格証明書の最大数（ メイキング）	N /
（ビットで）最大資格長	
	56
2	
RS-485 チャネルごとインターフェースモジュールの最大数	163
Synergis™単位あたりのインターフェイスモジュールの推奨最大数	644

[1] Synergis™ユニットと SALLIS ルータ間のプロトコル。

[2] 最大資格長は、インストールデータ、IDCODE サイズの下で、SALLIS アプリケーションから設定する必要があります。

[3] 一つの RS-485 チャネルあたりルータ、およびルータあたり最大 16 個の口ック。

[4] 4 つの RS-485 のいずれかで 16 の口ック毎、又は 64 個の口ックを有するものの PoE ルータとルータ。

SALTO SALLIS 統合のためのサポート Synergis™アプライアンスの機能

すべての Synergis™アプライアンスの機能を SALTO SALLIS ワイヤレスロックの統合でサポートされていません。SALTO SALLIS ワイヤレスロックの統合は、次のことをサポートしています *Synergis™ アプライアンスポータル* そして *Synergis™ Softwire* 特徴。これらの機能の詳細については、*Synergis™ アプライアンスの設定ガイド*。

Synergis™ アプライアンス Portal およびファーム	サポートさ
ハードウェア構成（事前ステージング機能）	
手動登録（*ハードウェアを追加* ダイアログ ボックス）はい	
自動登録（スキャン ボタン）はい	
プロパティ configurationYes	
コンフィギュレーション・クローニング（クローン ボタン）はい	
I / O の診断（入力、リレーのライブ監視、および 一部の読者）	[1]
インタフェースモジュールのファームウェア displayRouter	のみ
インタフェースモジュールのファームウェアのアップグレード（推奨適用します ファームウェア）いいえ	
アクセス制御の挙動（Synergis™ ユニット全体の設定）[2]	
ドアに開催されたビープ音 openNo	
ドアを強制的にビープ openNo	
アクセスのビープ音 deniedNo	
インターロックの設定（*シングルドアアンロック* 若しくは *シングルドアオープン*）いいえ	
ドアがあるとき、「DHO」イベントを生成しません。 unrestrictedYes	
リーダーの設定（*カードまたは PIN* 若しくは *カードのみ*）いいえ	
の最大 PIN 長 digitsN / A	
デグレードモード 機能設定/ A	
ロックリレー（*ドアが開いた後* 若しくは *ときにドアが閉じます*）いいえ	

[1] 取り付けたセンサなしの入力は I / O 診断ページで監視されていません。

[2] ドアの動作設定は、セキュリティセンターで構成され、個々のドアの設定によって上書きされます。

SALTO SALLIS 統合のためのサポートされているセキュリティセンターの機能

すべてのセキュリティセンターのアクセス制御機能は SALTO SALLIS ワイヤレスロックの統合でサポートされていません。

SALTO SALLIS ワイヤレスロック統合には、以下のセキュリティセンターのアクセス制御機能をサポートしています。これらの機能の詳細については、セキュリティセンターの管理者ガイドを参照してください。

特徴 groupSecurity	センター featureSupported	
ドア動作設定（Synergis™ユニット全体の設定を上書きします）	メンテナンスモード（ドアに鍵を維持し、すべてのアクセスイベントを無視）	はい
	標準の助成金 timeNo	[1]
	拡張助成金 timeNo	
	エントリの時間（標準/拡張）[2]	ノー
	ドアリロック - optionsNo	
	ドアはスケジュールによってロックが解除された場合 - オプション注 3 を参照してください	
	ドア開催します - optionsLimited	[4]
	ドアが開いて強制的に - optionsLimited	[4]
	アンロック schedulesYes	
	（REX）のオプションを終了する要求	
	REX にロックを解除 N / A（オン/オフ）	
	アクセスを許可した後 REX を無視する時間（中 秒）はい	
	ドアが開いている間 REX イベントを無視 （オン/オフ）はい	
	（ドアが閉じた後、REX を無視する時間 秒）はい	
	ビジター護衛と 2 人のルール	
	カード提示の間の最大遅延時間（中 秒。）はい	
	ドア上の（オン/オフ）2 人のルールを強制します sideYes	
セキュリティ Desk5 ドアの手動アクション	手動でロックを解除 doorsYes	
	シャント Reader は（有効化/無効化 読者）はい	
	オーバーライドロック解除 schedulesYes	

特徴 groupSecurity	センター featureSupported	
セキュリティデスクでのライブイベント監視	モジュールの実行状態（*オンライン、オフライン*）はい	
	交流 failN / A	
	バッテリーは（失敗しますローバッテリー）はい	
	ドア オープン/ closedNo	
	ドア ロック/ unlockedNo	
	ドアの強制 openYes	
	ドアはあまりにもオープン開催しました longYes	
	ドア securedN / A	
	デッドボルト（*確保し、リリース*）N / A	
	キー overrideYes	
（セキュリティで保護された領域のための）エリアの制限	最低限のセキュリティクリアランス（脅威レベル 管理）	は
	いビジター護衛ルール（オンオフ）	は
	い	
	InterlockNo	[6]
	AntipassbackNo	
	一人称-内のルール	
	ドアアンロックに強制 scheduleYes	
	アクセスに施行 rulesYes	
エレベーター コントロールター	N / A	エレベー
ゾーン管理	I / O zoneNo	
	ハードウェア zoneNo	[7]

[1] SALLIS アプリケーションで設定する必要があります。デフォルト値は 6 秒です。

[2] セキュリティセンターは、正確に領域への侵入を検出するために、入口センサが必要です。入口センサがない場合には、セキュリティセンターは、ドアセンサーを使用し、ドアセンサーがトリガーされたときにエントリが検出イベントが生成されます。両方のセンサーがない場合には、セキュリティセンターは、アクセスが許可されたときにエントリがイベントを想定し作成します。

[3] ドアのロックが解除されたときにすべてのイベントが無視されます。

[4] ザ・ リーダーのブザーの動作 オプションがサポートされていません。

[5] Synergis™ユニットは、Access Manager に接続する必要があります。

[6] 何のドアセンサーがないため、インターロックを導くために何のドア開いたイベントはありません。

[7] SALLIS からの入力を使用して設定ツールでハードウェアゾーンエンティティを作成することは可能ですが、重要なトリガー遅延が存在することになります。

入学 SALLIS ロック

Synergis™ユニットは SALLIS ロックと通信するためには、Synergis™アプライアンスポータルでそれらを登録する必要があります。

あなたが始める前に

SALLIS インストール & メンテナンスガイドで見つかった指示に従って、お使いのサルト SALLIS インフラストラクチャ（ルータ、ノード、およびワイヤレスロック）を設定します。あなたは最初のルーターを更新し、PPD（ポータブルプログラマーデバイス）を使用してロックを初期化し、その後、ノードと SALLIS アプリケーションを使用してドアを定義する必要があります。あなたがこれを行うと、以下の情報を書き留め：

- **IP ルータ：** IP アドレスとポート番号。
- **RS-485 ルータ：** Synergis™ 単位チャネルは、ルータは（A、B、C、または D）に接続されています。
- **ロック：** ルータ、ロック ID、およびそれがインストールされているドア。

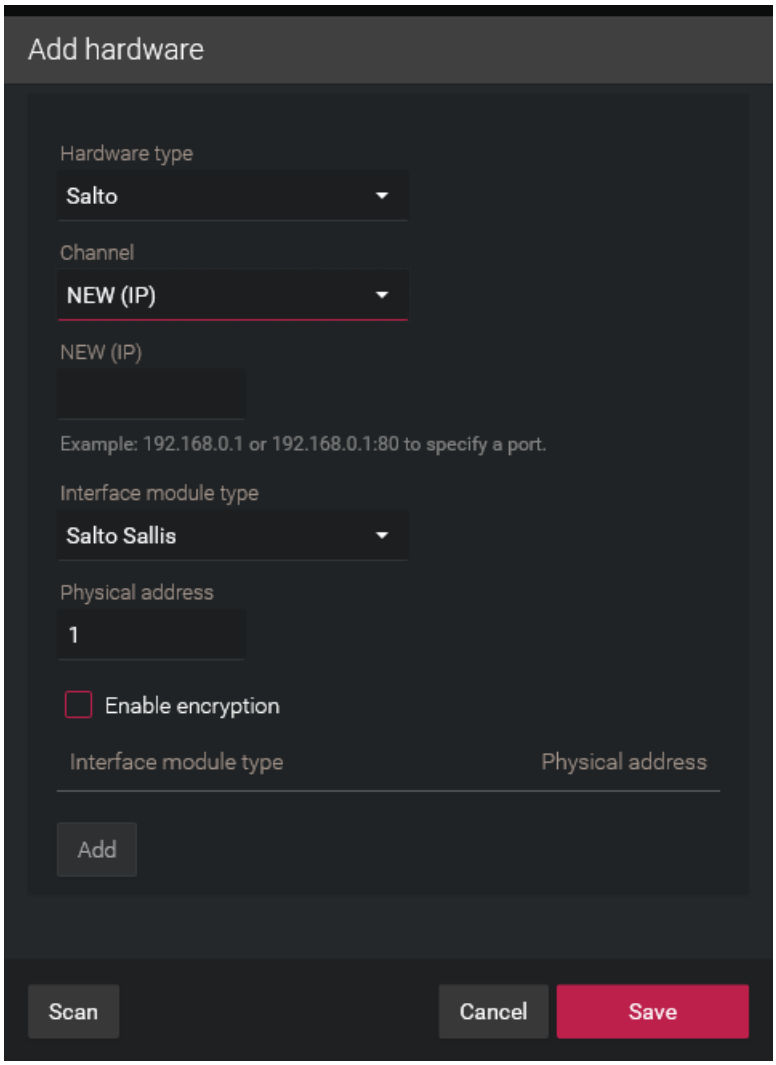
  たとえば、「4 階保管室」のために、わかりやすいドアの名前を使用します。すでにセキュリティセンターでは、ドアのエンティティを作成している場合は、参照を容易にするために同じ名前を使用します。

あなたは知っておくべきこと

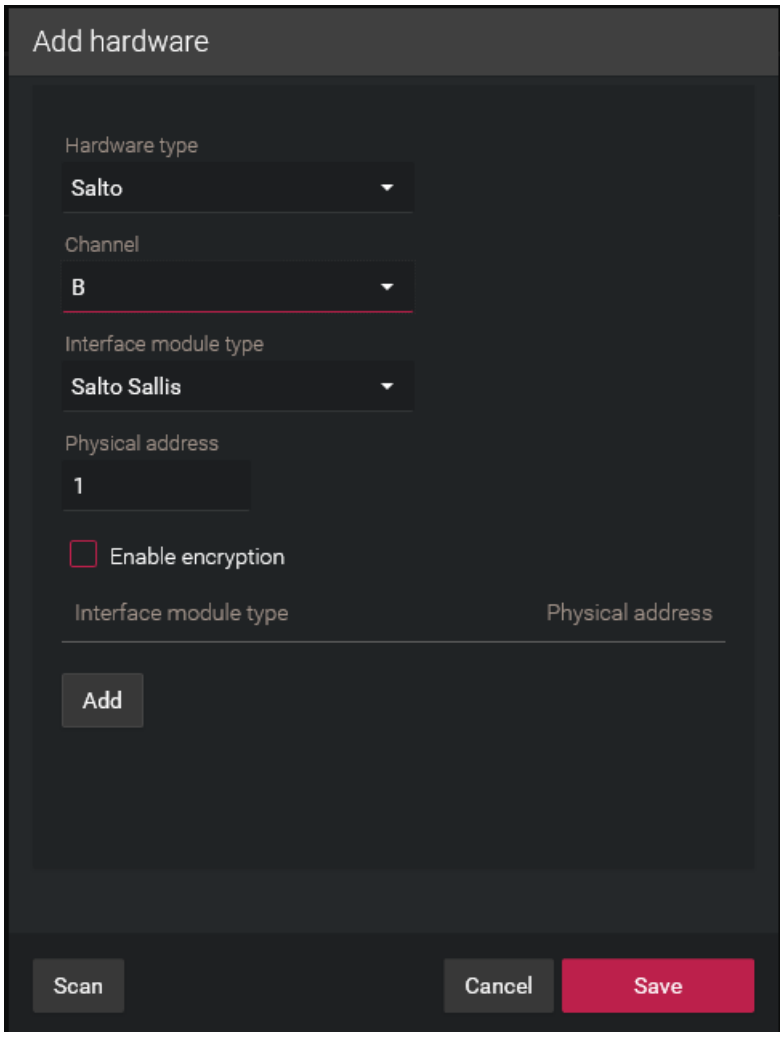
硬化でタグ付けされたステップや命令はオプションですが、サイバー攻撃からシステムを保護します。

SALTO SALLIS ワイヤレスロックを登録するには：

1 Synergis™ユニットにログオンします。
2 クリック **コンフィギュレーション > ハードウェア**
3 の上部には *ハードウェア*列、クリックしてください **加えます**（  ）。
4 の中に *ハードウェアを追加*選択]ダイアログボックスで、 **サルト** として **ハードウェアの種類**。
5 SALLIS ルータが接続されているチャンネルを特定し、次のいずれかを実行します。
   - IP チャネルを選択して、ルータが使用する IP アドレスとポート番号を入力してください。

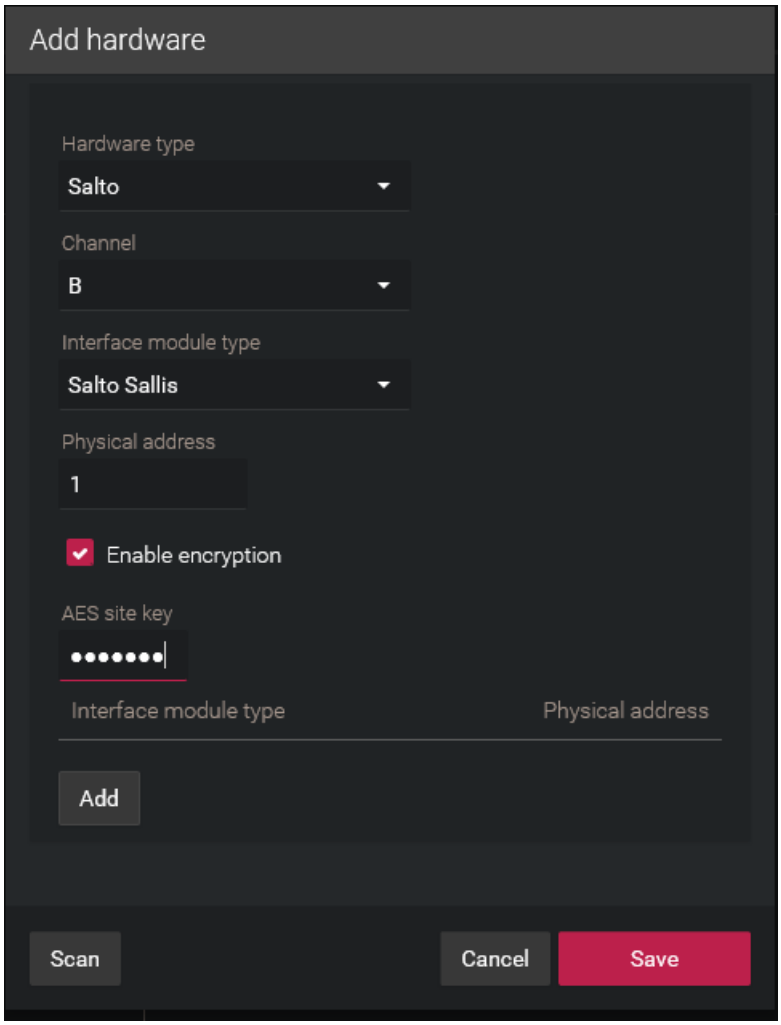


- RS-485 のチャネル（A、B、C、または D）を選択します。同じ RS-485 チャネルに接続されているすべてのインターフェースモジュールは、同じ製造業者からのものでなければなりません。



6 （*硬化*あなたが暗号化をしたい場合）、を選択 **暗号化を有効にします** そして、入力します。 **AES サイトキー**。

注意： あなたは、既存のチャネル上のハードウェアの追加]ダイアログボックスを使用して暗号化設定を変更 cannnot。チャネルが作成された後に暗号化を有効にするには、する必要がありますチャンネルを変更 Synergis™アプライアンスポータルの設定。



7 同じダイアログボックスでは、同じチャネルに接続されているすべてのインタフェースモジュールを追加します。あなたは、自動または手動でインターフェイスモジュールを登録することができます。

先端： あなたはロックの ID (物理アドレス) を知っているし、あなただけ登録する数を持っている場合、それらを手動で登録するより速くなります。

次のいずれかを実行します。

- 自動的に登録するには、[スキャン]をクリックします

  スキャン機能は、同じチャネルに接続されている同じ製造者からのすべてのインターフェース･モジュールを検索し、登録します。

  コントローラが接続されているすべてのインタフェース･ モジュールが見つからない場合、それらはすべてが異なる物理アドレスを持っていることを確認してください。

- (手動で登録物理アドレスとしてロック ID を入力し、[追加]をクリックします)。

注意： 有効なロック ID は、RS-485 ルータの 1-16、および PoE ルータの 1-64 です。

同じチャネルに接続されているすべてのワイヤレスロックを設定するために、必要に応じて繰り返します。

8 クリック **セーブ**。
追加したばかりのハードウェアタイプ、チャネル、およびインタフェース・モジュールは、に表示されます *ハードウェア構成* ページ。

あなたが完了した後、

- I / O の診断ページからごインターフェイスモジュールの接続と設定をテストします。インターフェイスモジュールのテストについては、以下を参照してください *Synergis™ アプライアンスの設定ガイド*。
- セキュリティセンターで SALLIS 口ックへのあなたのドアを関連付けます。

既存の SALLIS ルータ上での暗号化を有効にします

暗号化は Synergis™アプライアンス Portal のチャネルプロパティです。あなたは、暗号化を有効または Synergis™アプライアンスポータル上のチャネル構成を変更することにより、SALLIS ルータ上の暗号化パスワードを変更することができます。

あなたは知っておくべきこと

既存のチャネルにロックを追加しているときは、チャンネルの設定を変更することはできません。チャネルが作成された後、チャネルのプロパティに対するすべての変更は、チャネルのプロパティページから行う必要があります。一度
暗号化が有効になっている、あなたは Synergis™アプライアンスポータルでそれを無効にするだけで、それを無効にすることはできません。また、する必要がありますルータに直接接続することにより、暗号化を無効にします。

既存の SALLIS ルータ上で暗号化を有効にするには：

1 Synergis™ユニットにログオンします。
2 クリック**コンフィギュレーション > ハードウェア** そして、SALTO チャンネルを選択
3 を選択 **暗号化を有効にします** オプション、および入力します。 **AES サイトキー**。
4 クリック **セーブ**。

Disabling encryption on a SALLIS

SALLIS ルータの暗号化を無効にするには、両方の Synergis™アプライアンスポータルで、ルータ自身にそれを無効にする必要があります。

SALLIS ルータの暗号化を無効にするには：

1 Synergis™ユニットにログオンします。

2 の上部には *ハードウェア*列、クリックしてください **加えます** （）。

3 SALTO チャンネルを選択し、[クリア **暗号化を有効にします** オプション。

4 クリック **セーブ**。

デバイスツリーで、選択されたチャネルの下のすべての SALLIS ロックが赤（非アクティブ）に現れます。

5 RS-485 ルータの場合は、次の手順を実行します。

1 SALLIS アプリケーションを使用して、PPD にルータの設定をダウンロードしてください。

2 PPD で、選択 **アップデートルータ**。

3 ルータに PPD を接続します。

6 PoE 対応ルータの場合は、次の手順を実行します。

注意： あなたが更新する多くのルータを持っている場合は、それらを一つずつ更新します。

1 PoE 対応ルータのカバーを開き、5 秒間 CLR]ボタンをクリックして保持します。 PoE 対応ルータ· ボード上の LED がオレンジ色に点灯します。

2 Web ブラウザを使用して、ルータの Web ポータルに接続します。

タイプ `http://192.168.0.234` ブラウザの URL フィールドに入力します。

注意： あなたのワークステーションを使用すると、その Web ポータルに接続するためのルータと同じサブネット上にある必要があります。

3 ブラウザのページで、下 **ルータの暗号化 > プレーンモードに戻りますか？**選択 **はい**。

4 クリック **送ります**。

メッセージ **設定が正常に送信され** ブラウザに表示されます。

デバイスツリーで、選択されたチャネルの下のすべての SALLIS ロックが黒（アクティブ）に現れます。

13

SimonsVoss SmartIntego ロック

このセクションでは、次のトピックについて説明します。

Supported SimonsVoss

SimonsVoss SmartIntego ロック統合は、Mercury EP（またはハネウェル）コントローラを必要とします。この統合のために、EP コントローラはインタフェース・モジュールとして表示され、そして SmartIntego ロックは非インテリジェントデバイスとして表示されます。すべての SmartIntego ロックはワイヤレスです。

のみ水銀 EP（またはハネウェル）コントローラは Synergis™ユニットと直接通信します。

注意： SimonsVoss SmartIntego ロックの統合は、セキュリティセンター5.6（またはそれ以上の最近のバージョン）と Synergis™Softwire 10.4（またはそれ以上の最近のバージョン）が必要です。

Synergis™Softwire は、Mercury IP コントローラで動作するすべての SmartIntego モデルをサポートしています。

モデル	説明
IP コントローラ	A 水星 EP（または ハネウェル）コントローラは Synergis™ユニットと SmartIntego ロックとの間のインターフェースモジュールとして作用しなければなりません。 サポートされているコントローラのモデルは以下のとおりです。 • 16 までサポート拡張ボードとの水銀 EP1501 コントローラ SmartIntego ロック • 64 の SmartIntego ロックまでサポート水銀 EP1502 又は EP2500 コントローラ • 64 の SmartIntego ロックまでサポートハネウェル PW6K1IC コントローラも参照してください。 サポートされている水銀のファームウェアバージョン 126 ページ。
ゲートウェイ ノード	（30 メートルまでの範囲で、868 MHz の無線接続を介してノードごとに 16 台のロック装置まで。）水銀 IP コントローラと SmartIntego ロックとの間の通信を処理します。
プログラミング ドングル	ゲートウェイノードにロックをペアリングするために必要です。
スマート ハンドル	ドアハンドル/リーダーコンボ。監視することができないマニュアル REX アウトが含まれています。または入力なしで来るかもしれません。
デジタルロック シリンダー	異なる無線モデル。それらのいくつかは、二つの読者を持っているが、唯一のリーダーは、水銀 IP コントローラによって検出されます。または入力なしで来るかもしれません。
南京錠	無鍵穴、唯一のカードリーダーと南京錠。

より多くを学ぶためにこのビデオを見ます。クリック**キャプション**アイコン（**CC**）使用可能な言語の一つで、ビデオのキャプションをオンにします。Internet Explorer を使用している場合、ビデオが表示されないことがあります。この問題を解決するには、開きます**互換表示設定**クリア **互換表示で表示イントラネットサイト**。

制限事項

- 手動ロック解除と再ロックコマンドが実行されるように予想以上に時間がかかることがあります。これらのコマンドが応答するのに数秒かかる場合があります無線通信に依存しているためです。

Supported SimonsVoss

- MIFAREDESFire®、および MIFARE Plus のカード形式のみがサポートされています。

Supported SimonsVoss lock features

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

Synergis™ Softwire 10.6 supports the following SimonsVoss lock features.

FeaturesSupported	
Category of interface moduleElectronic	lock
Communication protocol[1]	IP, radio
Encrypted communicationYes	[2]
Online operation (connected to the Synergis™ unit)N/A	
Offline operation (no connection to the Synergis™ unit)N/A	
Wireless operationYes	[3]
Reader communication protocolsN/A	
Maximum credential length (in bits)	524
Recommended maximum number of interface modules per Synergis™ unitN/A	[5]

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

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

[3] Requires the Gateway node (communication module).

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

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

Supported Synergis™ appliance features for SimonsVoss lock integration

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

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

Supported Security Center features for SimonsVoss lock integration

Not all Security Center access control features are supported with the integration of SimonsVoss locks.

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

Feature groupSecurity	Center featureSupported	
Door behavior settings (overrides the Synergis™ unit-wide settings)	Maintenance mode (keep door unlocked and ignore all access events)	No
	Standard grant timeYes	[1]
	Extended grant timeN/A	
	Entry time (Standard/Extended)[2]	N/A
	Door relock - optionsNo	
	When door is unlocked by schedule - optionsYes	
	Door held - optionsNo	
	Door forced open - optionsN/A	
	Unlock schedulesYes	
	Request to exit (REX) options	
	Unlock on REX (On/Off)N/A	
	Time to ignore REX after granting access (in seconds)N/A	
	Ignore REX events while door is open (On/Off)N/A	
	Time to ignore REX after door closes (in seconds)N/A	
	Visitor escort and two-person rule	
	Maximum delay between card presentation (in sec.)No	
	Enforce two-person rule (On/Off) on Door sideNo	
Manual actions on doors in Security Desk3	Manually unlock doorsYes	
	Reader shunting (activate/deactivate reader)No	
	Override unlock schedulesYes	

Feature groupSecurity	Center featureSupported	
Live event monitoring in Security Desk	Module running state (*Online, Offline*)Yes	
	AC failNo	
	Battery fail (*Low battery*)Yes	
	Door open/closedNo	
	Door locked/unlockedNo	
	Door forced openNo	
	Door held open for too longNo	
	Door securedN/A	
Area restrictions (for secured areas)	Minimum security clearance (threat level management)	N/A
	Visitor escort rule (On/Off)	N/A
	InterlockN/A	
	AntipassbackN/A	
	First-person-in ruleN/A	
Elevator control	Elevators	N/A
Zone management	I/O zoneN/A	
	Hardware zoneN/A	

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

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

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

Preparing to enroll SimonsVoss SmartIntego locks

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

What you should know

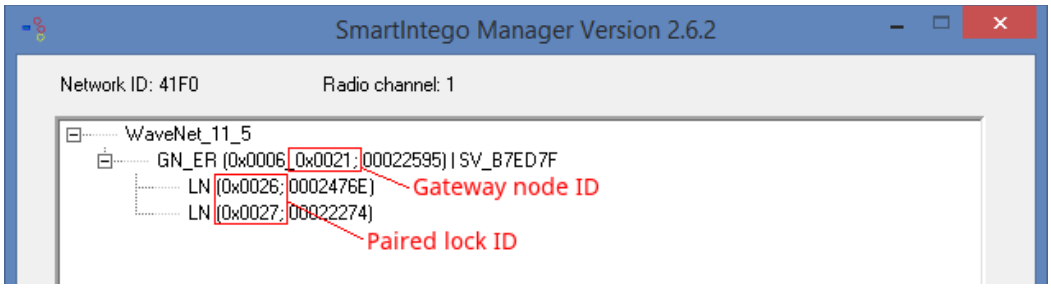
The steps and instructions tagged with Hardening are optional, but will protect your system against cyberattacks.

To prepare to enroll the SmartIntego locks:

1 Follow the documentation that came with your SmartIntego devices and pair the Gateway node to your SmartIntego locks.

2 Write down the following information:

- The IP address of the Gateway node.
- The device IDs taken from the *SmartIntego Manager* window.



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

The lock ID is the first hexadecimal number following LN.

3 (Hardening) Follow the documentation that came with your SmartIntego devices and configure the communication encryption key for your locks.

SmartIntego software does not allow a lock to be paired to the hub without a password. Use a strong password for the locking system.

Enrolling SimonsVoss SmartIntego locks on the Synergis™ unit

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

Before you begin

Pair your the Gateway node to your SmartIntego locks.

What you should know

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

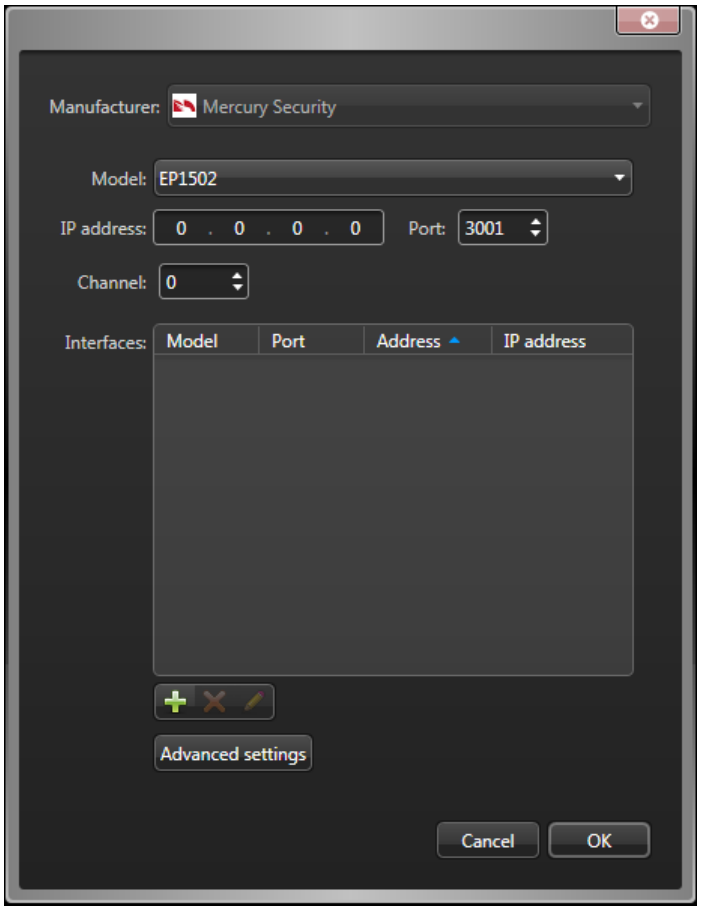
On the Synergis™ unit, each EP controller must by assigned a unique channel ID. The EP controller communicates with the SmartIntego Gateway nodes through IP. IP addresses cannot overlap within the same network.

To enroll SimonsVoss SmartIntego locks to the Synergis™ unit:

1 From the Config Tool home page, open the *Access control* task.

2 Click **Roles and units**, and then click the Synergis™ unit ( ).

3 Click **Peripherals**, and then click **Add an item** ( ).



4 Enter the following information:

- **Model:** Model of the controller.
- **IP address:** Static IP address assigned to the controller by your IT department.
- **Port:** Communication port (default=3001). The port must match the value configured on the Mercury Device Manager web page.
- **Channel:** Channel ID corresponding to this controller. The channel ID can be any value between 0 and 63, and must be unique within the Synergis™ unit. Once assigned, it must not be changed.

5 Add the SmartIntego Gateway node that you want the EP controller to talk to.

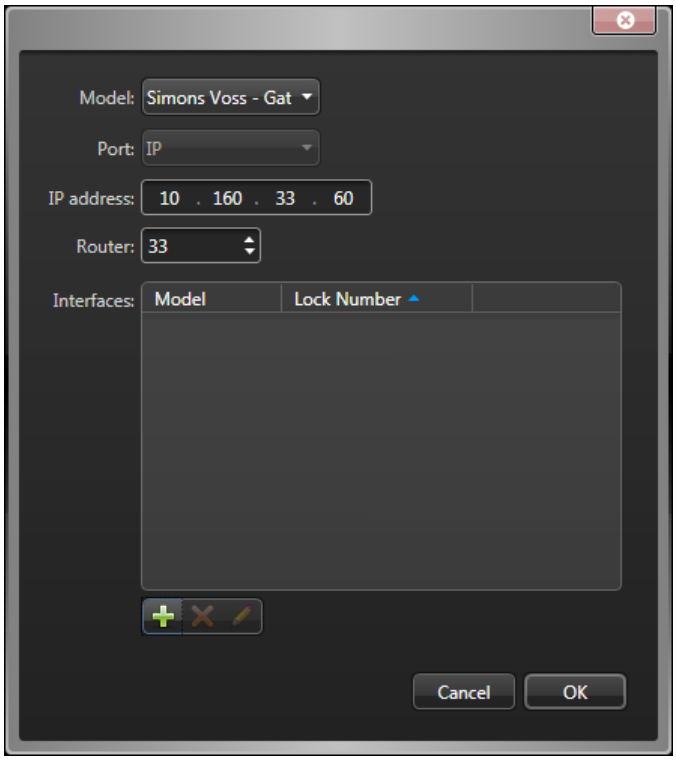
a) At the bottom of the *Interfaces* group, click **Add an item** ( ).

b) In the dialog box that appears, click **Model** and select **SimonsVoss Gateway node**.

c) In IP address, enter the IP address of the Gateway node.

d) In Router, enter the decimal value of the Gateway node ID.

For examle, if the Gateway node ID is 0x0021, enter 33 (= 2 x 16 + 1).

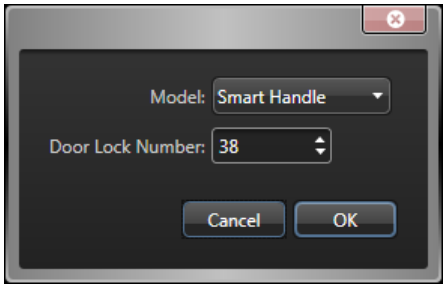


6 Add the locks paired to the Gateway node.

a) In the dialog box that appears, click Model and select the lock model (Smart Handle, Padlock, Cylinder).

b) In **Door Lock Number**, enter the decimal value of the lock ID.

For examle, if the lock ID is 0x0026, enter 38 (= 2 x 16 + 6).



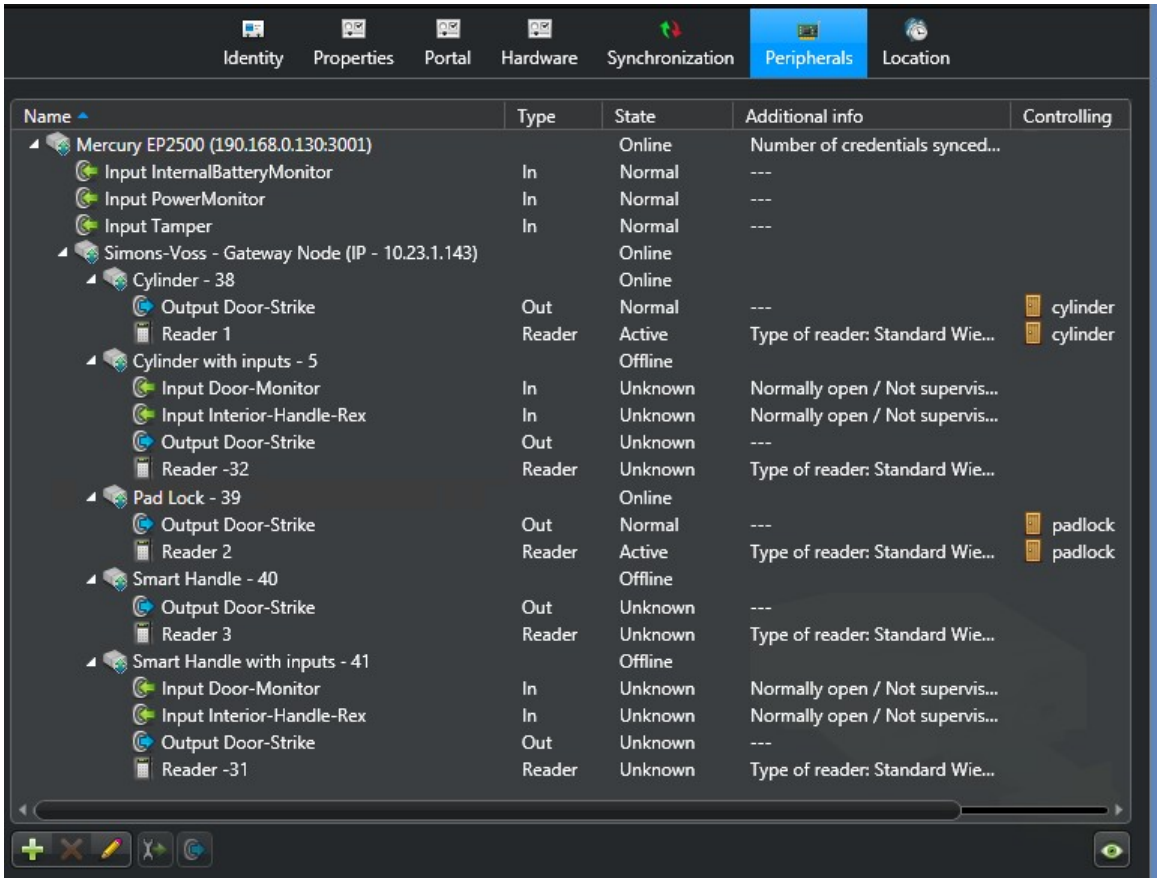
c) Click **OK**.

d) Repeat if you have more locks to add.

e) Click **OK**.

7 Click **Apply** ( ).

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



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

8 Test your configuration by triggering the outputs.

The triggered output changes state in real time on screen.

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

14

STid Readers

This section includes the following topics:

Supported STid readers in Synergis™ Softwire 10.6

For STid reader integration, each reader is viewed as an interface module. Synergis™ Softwire supports the following STid readers.

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

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

Configuration overview for STid readers with Synergis™ Softwire 10.6

The following table summarizes the reader configuration process.

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

Phase	Description	See
1	Make sure your STid reader firmware is up to date and supported by Synergis™ Softwire. Contact your STid representative for the latest firmware.	• STid-SESPro documentation that came with your reader. • Supported STid readers in Synergis™ Softwire 10.6 on page 179.
2	Configure the reader firmware settings, such as the device address, baud rate, encryption keys, and so on.	STid-SESPro documentation that came with your reader.
3	Establish communication between the Synergis™ unit and its attached STid readers by configuring them in Synergis™ Appliance Portal1.	Enrolling STid readers attached to the Synergis™ unit on page 182.
4	The Synergis™ unit is pre-configured to communicate with the STid readers using their factory-installed signature and encipherment keys. We recommend changing these encryption keys for better security.	Changing the default communication parameters with STid readers on page 186.
5	If you want your readers to do more than simply returning the CSN (card serial number), then configure the advanced reader settings in *SmartCardsReaders.xml*.	Advanced STid reader setting configuration on page 187.
6	Apply the settings configured in XML files to the Synergis™ unit.	Updating the STid configuration on your Synergis™ unit on page 189.

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

Enrolling STid readers attached to the Synergis™ unit

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

Before you begin

- Configure the STid readers' firmware with STid-SESPro and attach them the Synergis™ unit.
- Make sure your STid reader firmware is up to date and supported by Synergis™ Softwire.

What you should know

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

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

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

1 Log on to the Synergis™ unit.

2 Click **Configuration > Hardware**

3 At the top of the *Hardware* column, click **Add** ( ).

4 In the *Add hardware* dialog box, select **STid** as the **Hardware type**.

5 Select the **Channel** (A, B, C, or D) and its baud rate (**Bits per second**).

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

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

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

6 Select the **SSCP protocol version** (either **V1** or **V2**).

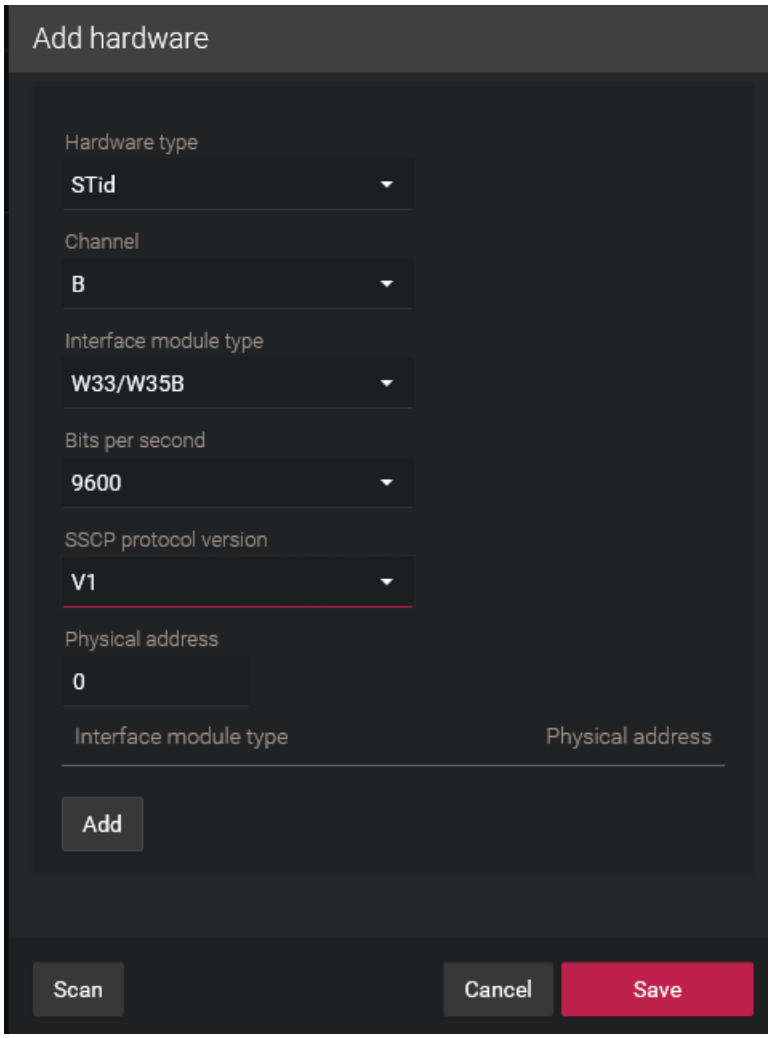
The SSCP protocol is a channel property. The channel follows the SSCP protocol of the first reader added to the channel.

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

7 In the same dialog box, add all STid readers connected to the same channel.

Do one of the following:

- To add manually, enter the physical address (1 to 127) of the reader and click Add.



Repeat for the second reader if necessary.

- To enroll automatically, click Scan.

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

If the controller does not find all connected interface modules, verify their baud rate and physical address.

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

9 For each interface module you just added, select it from the Hardware configuration page, and configure its settings.
For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.

10 Select the **Communication mode**.
The choices are:

- *Plain* (default mode)
- *Encrypted* (private communications)
- *Signed* (authenticated communications)

- *Encrypted and signed* (both private and authenticated communications)

NOTE: If you selected **V2** as the **SSCP protocol**, then only the **Encrypted and signed** option is available.

While the encryption keys are common for all readers connected to the same Synergis™ unit, the communication mode between the unit and each STid reader can be configured separately.

BEST PRACTICE: (Hardening) We recommend changing the default encryption keys provided by the manufacturer for added security.

11 At the bottom of the page, click Save.

After you finish

Test your interface module connection and configuration from the I/O diagnostics page. For information about testing interface modules, see the *Synergis™ Appliance Configuration Guide*.

Related Topics

Advanced STid reader setting configuration on page 187

Enabling transparent mode on STid readers

DESFire EV1 readers require cryptographic keys to access a card's secured credential. When keys are loaded into a reader or a Synergis™ unit, then the reader acts as a transparent reader.

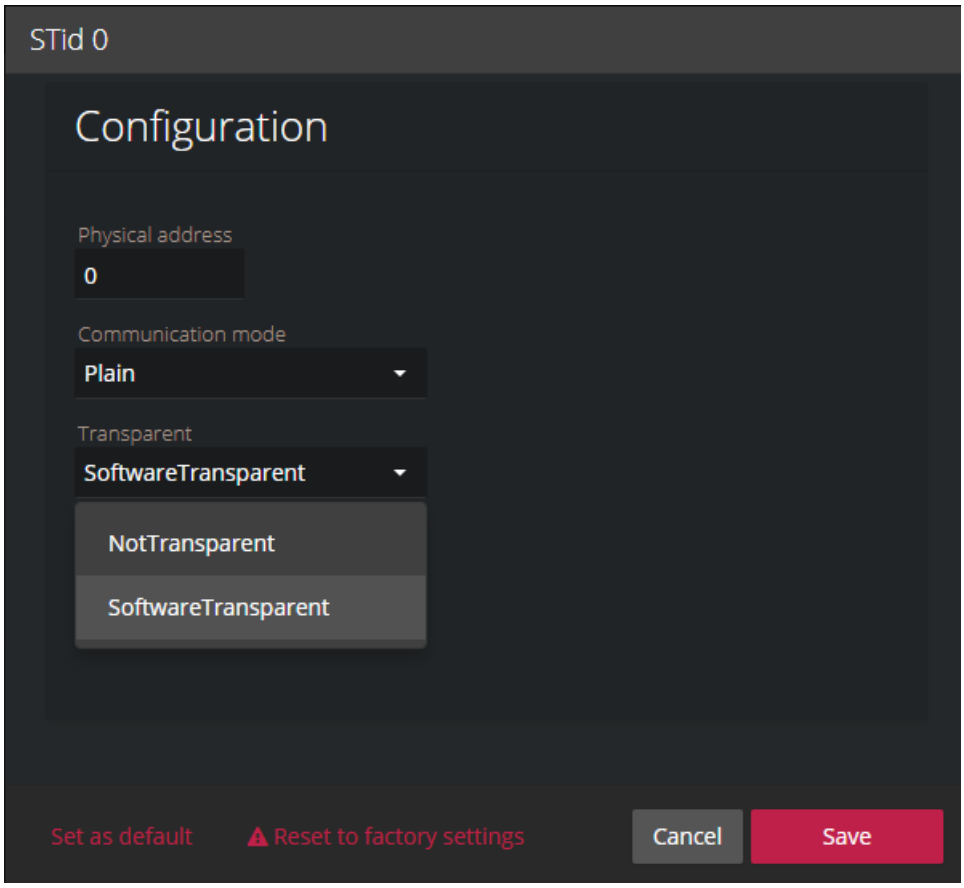
Before you begin

- The door must be controlled by a Synergis™ unit running Synergis™ Softwire 10.6 GA or later.
- The door must have an STid reader with a part number ending in AA or AD.
- **NOTE:** Transparent STid readers with part numbers ending in BB cannot be used in this scenario. See Supported STid readers in Synergis™ Softwire 10.6 on page 179 for a list of readers that can be used as transparent readers.

To set up transparent STid readers:

1 Open Config Tool.

2 Under **STid > Interfaces**, set the **Transparent** option to SoftwareTransparent.



3 Store the cryptographic keys on the Synergis™ Cloud Link.

When you configure the cyptographic keys on the Synergis™ Cloud Link:

- You enter the keys into the 32 available indexed keys in the primitive key store through the Synergis™ Softwire 10.6 portal.
- The SmartCardsSites.xml file used for the indexed keys is compatible with both software-transparent and non-transparent STid readers.

Limitation: There are two limitations with software transparent readers:

- Transparent readers currently cannot encode cards.
- Cards with transparent mode enabled take about 100 ms longer to read.

Changing the default communication parameters with STid readers

You can change the default signature and encipherment keys used for encrypted and signed communication with the STid readers.

Before you begin

Best practice: The Synergis™ unit is pre-configured to communicate with the STid readers using their factory-installed Signature and Encipherment keys. We recommend that you use your own key values for better security.

What you should know

Changing the default signature and encipherment keys involves changing a configuration file STidConfig.xml on the Synergis™ unit, and a three-step input of the new encryption values by three separate individuals, using the Primitive key store page on the Synergis™ Appliance Portal.

To change the encryption keys:

To change the signature and encipherment keys used for encrypted and signed communication with the STid readers, you must apply the new encryption values, ReaderKc for the encipherment key and ReaderKs for the signature key, to the Synergis™ unit.

For the exact procedure, contact your representative of Genetec

Inc. See also "Updating the STid configuration on the Synergis™

unit".

Advanced STid reader setting configuration

If you want your readers to do more than just returning the CSN (Card Serial Number) of the cards read (default behavior), you must modify the advanced reader settings stored in the SmartCardsReaders.xml file.

Contact your representative of Genetec Inc. for a copy of this XML file so you can modify it to match your actual reader settings. Once it is updated, you must apply this configuration to your Synergis™ unit.

General structure SmartCardsReaders.xml for STid readers

The general structure of SmartCardsReaders.xml is as follows:

```
<SmartCards>
<Readers>
<ReaderParameters ...>
Parameters for 1st reader...
</ReaderParameters>
<ReaderParameters ...>
Parameters for 2nd reader...
</ReaderParameters>
...
<ReaderParameters ...>
Parameters for nth reader...
</ReaderParameters>
</Readers>
</SmartCards>
```

NOTE: The XML file must contain one <ReaderParameters> tag for every STid reader connected to your Synergis™ unit. The above is a generic structure. For any specific card configuration, contact your representative of Genetec Inc.

Sample XML code for a simple reader

The following sample code describes a simple reader.

```
<ReaderParameters Encode="false">
<Reader Pointer="/Devices/Bus/STid/A/Reader/2" />
<Source> <None/> </Source>
<Sites>
<Site Name="INT" />
<Site Name="EXT" />
</Sites>
</ReaderParameters>
```

The tag descriptions are as follows.

- The <Reader> tag identifies the reader. The Pointer parameter must match the reader settings configured in both STid-SESPro and Synergis™ Appliance Portal. Our example refers to the reader connected to Channel A at the address 2.
- The <Site> tag lists the contexts for which the reader is configured to read from the card. In our example, the reader returns the credential associated to the first context successfully found, named either "INT" or "EXT".

Encoding a credential on an RFID card in Security

You can encode a credential on an RFID card using Security Desk.

What you should know

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

Updating the STid configuration on your Synergis™

To update the STid configuration on your Synergis™ unit, you need to apply the STid configuration XML files to your unit using the Synergis™ Appliance Portal.

To update the STid configuration:

1 Zip your XML files (*SmartCardsReaders.xml*, *SmartCardSites.xml*, and *STidConfig.xml*) into a single zip file and rename it to *NewConfig.smc*.

The *NewConfig.smc* file must be located on your local drive.

The SmartCardSites.xml file contains predefined format template settings and is found in the Security Center Client installation folder.

2 Contact your Genetec Inc.. representative for the exact procedure to apply the NewConfig file to your unit using the Synergis™ Appliance Portal.

Glossary

A B C D E F G H I J K L M NO P Q R S T U V WXY Z A

access control unit — An access control unit is a type of entity that represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Access Manager — Access Manager is the role that manages and monitors access control units on the system.

access point — An access point is any entry (or exit) point to a physical area where access can be monitored and governed by access rules. An access point is typically a door side.

access rule — An access rule is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point.

antipassback — Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

C

cardholder — A cardholder is a type of entity that represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.

credential — A credential is a type of entity that represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

D

degraded mode — Degraded mode is an offline operation mode of the interface module when the connection to the Synergis™ unit is lost. The interface module grants access to all credentials matching a specified facility code. Only Mercury and HID VertX interface modules can operate in degraded mode.

dependent mode — Dependent mode is an online operation mode of the interface module where the Synergis™ unit makes all access control

	decisions. Not all interface modules can operate in dependent mode.

E

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

F

first-person-in rule	The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

G

global antipassback	Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple Synergis™ units.

H

hardware zone	A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

I

interface module	An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.
interlock	An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one door to be open at any given time.
I/O linking	I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).
I/O zone	An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis™ units, while one unit acts as

the master unit. All Synergis™ units involved in an I/O zone

must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

M

mobile credential

A mobile credential is a credential on a smartphone that uses Bluetooth or Near Field Communication (NFC) technology to access secured areas.

S

secured area

A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

security clearance

A security clearance is a numerical value used to further restrict the access to an area when a threat level is in effect. Cardholders can only enter an area if their security clearance is equal or higher than the minimum security clearance set on the area.

server mode

The server mode is a special online operation mode restricted to Synergis™ units, in which the unit allows the Access Manager (the server) to make all access control decisions. The unit must stay connected to the Access Manager at all times to operate in this mode.

standalone mode

Standalone mode is an offline operation mode of the interface module where it operates autonomously, making decisions based on the access control settings previously downloaded from the Synergis™ unit. Activity reporting occurs on schedule, or when the connection to the unit is available. Not all interface modules can operate in standalone mode.

strict antipassback

A strict antipassback is an antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.

supervised mode

Supervised mode is an online operation mode of the interface module where the interface module makes decisions based on the access control settings previously downloaded from the Synergis™ unit. The interface module reports its activities in real time to the unit, and allows the unit to override a decision if it contradicts the current settings in the unit. Not all interface modules can operate in supervised mode.

SV-32
The SV-32 is a compact-sized network security appliance that comes pre-installed with Microsoft® Windows, Genetec™ Security Center, and the SV Control Panel. With built-in analog encoder capture cards, the SV-32 is a turnkey appliance that enables you to quickly deploy a standalone system (video surveillance OR access control) or unified system (video surveillance AND access control).

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

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

Synergis™ Cloud Link
Synergis™ Cloud Link is an intelligent and PoE-enabled access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. Synergis™ Cloud Link is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

Synergis™ Master Controller
Synergis™ Master Controller (SMC) is an access control appliance of Genetec Inc. that supports a variety of third- party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

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

Synergis™ unit
A Synergis™ unit is a Synergis™ appliance that is enrolled as an access control unit in Security Center.

T

threat level
Threat level is an emergency handling procedure that a Security Desk operator can enact on one area or the entire system to deal promptly with a potentially dangerous situation, such as a fire or a shooting.

timed antipassback
Timed antipassback is an antipassback option. When Security Center considers a cardholder to be already in an area, a passback event is generated when the cardholder attempts to access the same area again during the time delay defined by Presence timeout. When the time delay

has expired,

	the cardholder can once again pass into the area without generating a passback event.
two-person rule	The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

U

unit synchronization	Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.
unlock schedule	An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).

V

visitor escort rule	The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay.

Z

zone	A zone is a type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Genetec Patroller™ and the Sharp Portal also include context-sensitive help for each screen. To access the help, click Help, press F1, or tap the ? (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues.

  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log in or sign up at https://gtapforum.genetec.com.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and
  troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, please contact GTAC at https://gtap.genetec.com.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.