UPS Network Management Card

Network-M2
ユーザーガイド

日本語版

2021/2/5

GFD21-201OE07-2

ダイトロン株式会社

本ユーザーマニュアルは、Eaton社発行のUser guideを機械翻訳して、部分的に文言修正しています。
画像の言語は英語となっております。あらかじめ、ご了承ください。

1 目次

2 ネットワークマネジメントモジュールのインストール

2.1 ネットワークモジュールの開梱

Network-M2には、以下の付属品が含まれます。

- QuickStart
- USB AMからマイクロUSB / M / 5Pの5フィートケーブル

梱包材は、廃棄物に関する法規制を遵守して廃棄してください。梱包材には、分別を容易にするためにリサイクルマークが印刷されています。

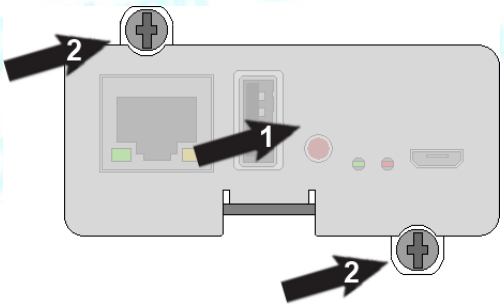
2.2 ネットワークモジュールの取り付け

ネットワークモジュールをインストールする前にデバイスの電源を落とす必要はありません。
必要なツール:プラスドライバー。

ネットワークモジュールはホットスワップ対応です。本製品の通信スロットからネットワークモジュールを抜き差ししても出力に影響はありません。.

オプションスロットのカバープレートを固定している2つのネジを外し、将来使用できるようにプレートを保管してください。.

- オプションスロットの調整チャンネルに沿ってネットワークモジュールを取り付けます.
- 2 本のネジでネットワークモジュールを固定します。



製品の電源が入っている場合、2 分後にステータスオン LED が緑色に点滅する事で、ネットワークモジュールが正しく装着され製品と通信していることを確認することができます。

2.3 RS-485 Modbus RTU 端子の配線

Modbus ネットワークモジュールは RS-485 Modbus ネットワークに EatonUPS を統合するための簡単なパスを提供し、また UPS と RS-485 Modbus ネットワーク間の通信の分離を提供します。

2線式ネットワークに配線するためにModbusネットワークモジュールのターミナルストリップを使用してください。

Modbusネットワークモジュールがネットワークチェーンに最後にインストールされたデバイスであったり、ネットワークケーブルの長さが長すぎる場合は、ターミネーションを有効にする必要があります。
ターミネーションの詳細については、ネットワークマネジメントモジュールの設置>>RS-485 Modbus RTU 端子の配線>>ターミネーションの設定を参照してください。

2.3.1 Modbus Common/GND（端子台の0Vピン）接続

ネットワークモジュールは絶縁されたデバイスです。ネットワーク上の他のすべてのデバイスが絶縁されている場合は、コモンモード電圧を制限するためにデバイス間でコモン/GND（端子台の0Vピン）を接続してください。

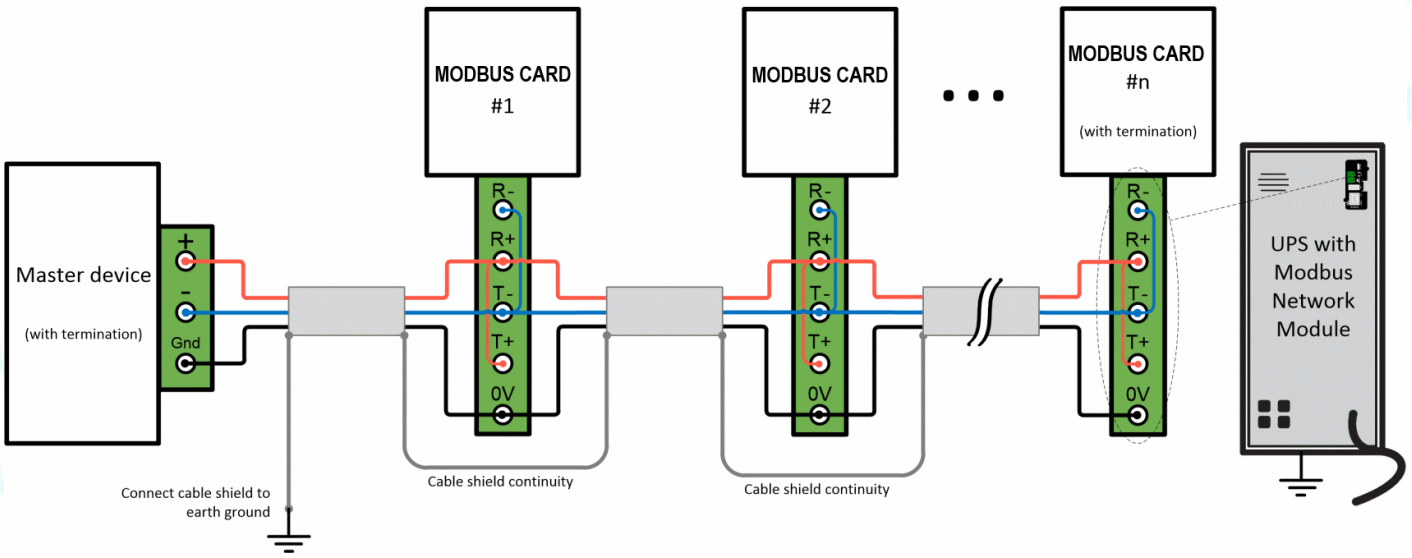
グランドループを避けるため、絶縁されていない他のデバイスにはコモン/GND(端子台の0Vピン)を接続しないでください。

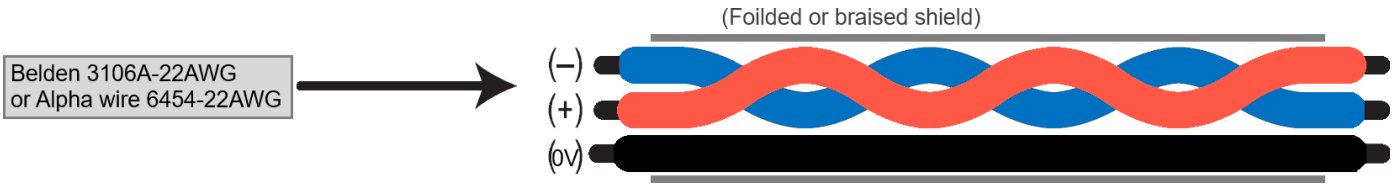
2.3.2 ケーブルシールド接続

ケーブルシールドはバスの全長にわたって連続している必要があり、接地電位差によるシールド内のグランドループ電流の流れを制限するために、一点のみ接地（アース）に接続する必要があります。

2.3.3 二線式ネットワーク

- Modbus Network Module ターミナルストリップ上で R-を T-に、R+を T+に接続します。
- RS-485 ネットワーク信号 + を Modbus Network Module 端子ストリップの R+ または T+ に接続します。
- RS-485 ネットワーク信号 – を Modbus Network Module 端子ストリップの R- または T に接続してください。

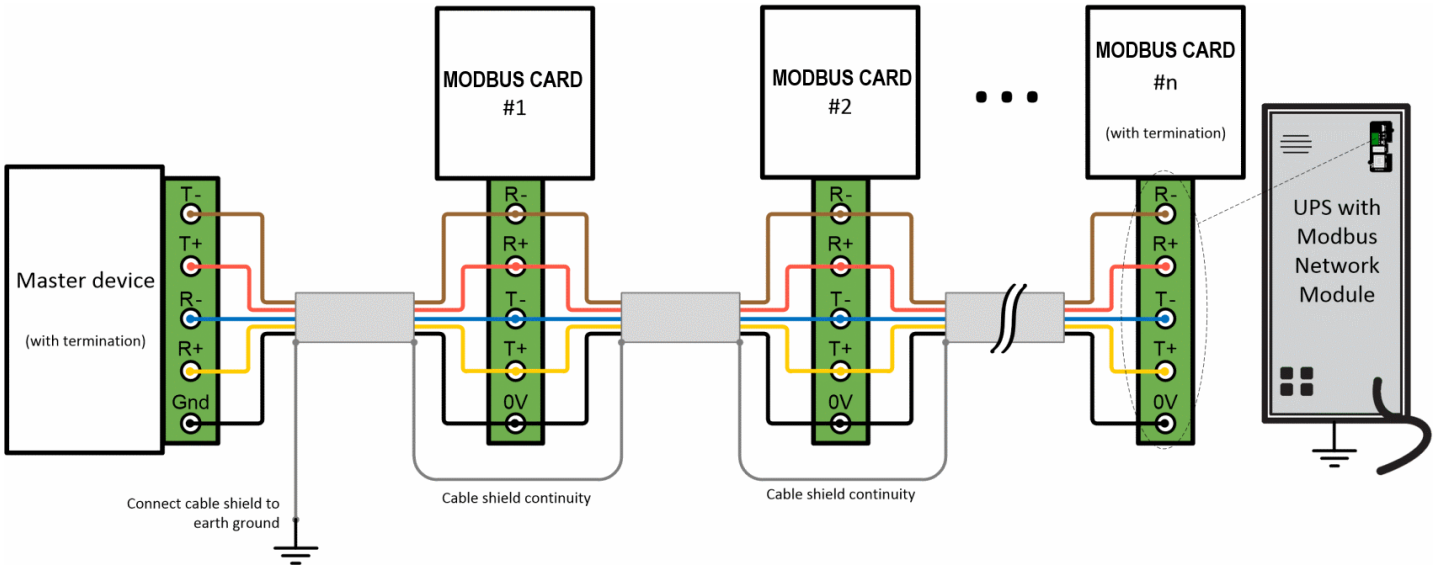


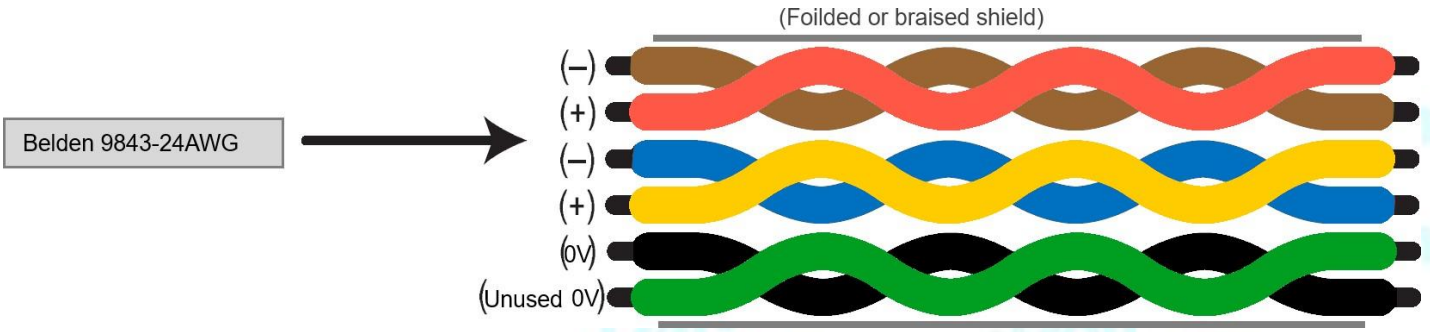


Belden 3106A-22AWG または同等のケーブル（1.5 ツイストペアシールド 120Ωケーブル、アース付き）をお勧めします。

2.3.4 四線式ネットワーク

T, T+, R-, R+を含む4つのRS-485ネットワーク信号は、それぞれ端子台R-, R+, T-, T+に接続しなければなりません。





Belden 9843-24AWG または同等のケーブル（3 ツイストペアシールド 120Ωケーブル（アース付き）を推奨します.

2.3.5 終端の設定

INDGWカードがネットワークチェーンの最後に設置されたデバイスであったり、ネットワークケーブルの長さが長すぎる場合は、ターミネーションを有効にする必要があります。

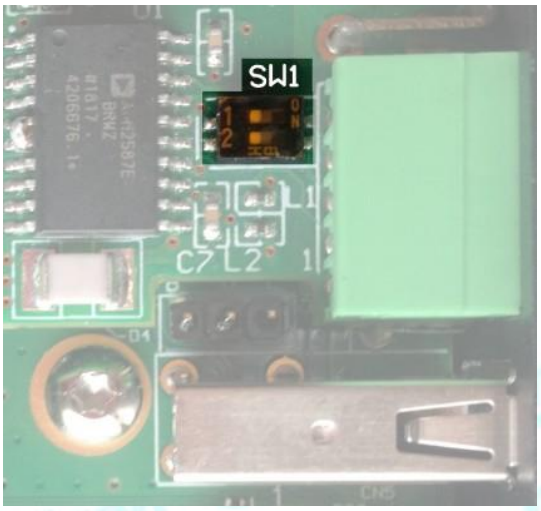
ターミネーションはノードのインピーダンスと使用されている伝送線路のインピーダンスを一致させるために使用されます。インピーダンスが不一致の場合、伝送された信号は負荷に完全に吸収されず、一部が伝送線路に反射してしまいます。

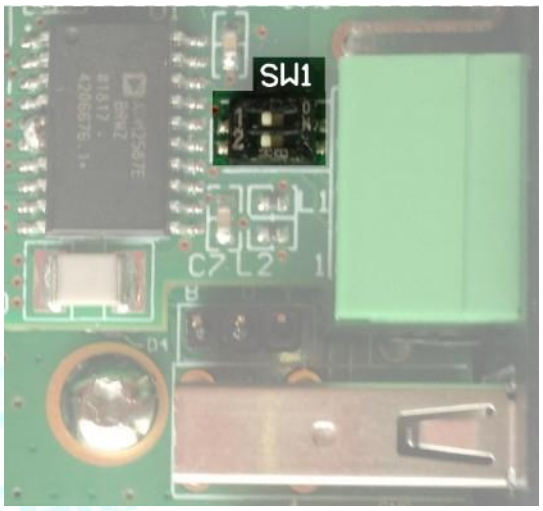
RS-485 ネットワークでは、2 つ以上の終端点を使用しないでください。

オンボード終端抵抗(120Ωを有効にするには:

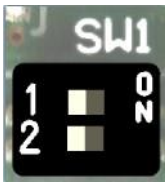
1. Modbusネットワークモジュールの上部にある終端スイッチを探します。

2. 保護をはがす:





3. 必要に応じて終端スイッチの位置を変更します。:

	スイッチの位置
終端ではない（デフォルト）	
2線式ネットワークの終端処理	以下の2つの位置のいずれかを使用することができます。:  or 

4線式ネットワークの終端処理	

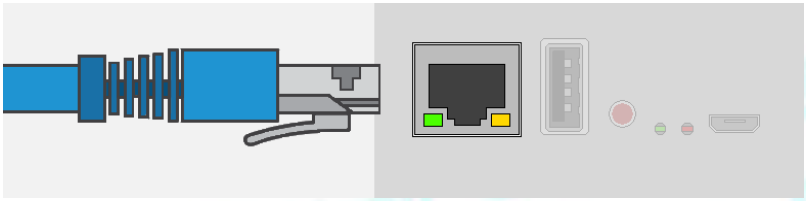
2.4 ネットワークモジュールへのアクセス

2.4.1 ネットワークを介したWebインターフェースへのアクセス

2.4.1.1 ネットワークケーブルの接続

ネットワークモジュールのセキュリティ設定は、デフォルトの状態になっている場合があります。
最大限のセキュリティを確保するにはネットワークケーブルを接続する前にUSB接続で設定して下さい。

ネットワークモジュールのネットワークコネクタとネットワークジャックの間に、標準的なギガビット互換のシールド付きイーサネットケーブル (F/UTP または F/FTP) を接続します。



2.4.1.2 ウェブインターフェースへのアクセス

ネットワークモジュールへのブラウザアクセスは、ファイアウォールまたは隔離されたネットワークを使用して外部からのアクセスから隔離することを強くお勧めします。

STEP 1 – ネットワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザのウィンドウが表示されます。

STEP 2 – Address/Location フィールドに、https://**[IP address]** とネットワークモジュールのスタティック IP アドレスを入力します。

STEP 3 – ログイン画面が表示される

STEP 4 – ユーザー名フィールドにユーザー名を入力します。デフォルトのユーザー名は **admin** です。

STEP 5 – パスワードフィールドにパスワードを入力します。デフォルトのパスワードは**admin**です。

STEP 6 – 初回ログイン時にパスワードを変更する必要があります。

STEP 7 – **[ログイン]**をクリックします。ネットワークモジュール Web インターフェースが表示されます

2.4.2 IPアドレスの検索と設定

2.4.2.1 ネットワークにはBOOTP/DHCPサーバーが装備されています(デフォルト)

2.4.2.1.1 デバイスLCDからの読み出し

注意: 古い機器では、液晶を搭載していてもIPアドレスが表示されない場合があります。機器のマニュアルを参照してください。

お使いのデバイスにLCDがある場合は、LCDのメニューから Identification>>>"COM card IPv4".
- カードのIPアドレスに注意.
- セクションに移動します。ネットワークを介して Web インターフェースにアクセスする。

2.4.2.1.2 設定ポートを介してWebブラウザを使用した場合

例えば、お使いのデバイスにLCDがない場合は、RNDISからWebインターフェースにアクセスし、次のページを参照することでIPアドレスを検出することができます。Settings>Network.

RNDIS から Web インターフェースにアクセスするには、「RNDIS からの Web インターフェースへのアクセス」のセクションを参照してください。.

- Navigate to Contextual help>>>Settings>>>Network & Protocol>>>IPV4.
- Read the IPv4 settings.

2.4.2.2 ネットワークに BOOTP/DHCP サーバーが装備されていない

2.4.2.2.1 設定ポートからの定義

アドレスは、RNDIS から Web インターフェースにアクセスすることで定義できます。

RNDIS から Web インターフェースにアクセスするには、「RNDIS から Web インターフェースにアクセスする」を参照してください

IP設定を定義する:

- Navigate to Contextual help>>>Settings>>>Network & Protocol>>>IPV4.
- Select Manual (Static IP).
- Input the following information: Address, Subnet Mask, Default Gateway
- Save the changes.

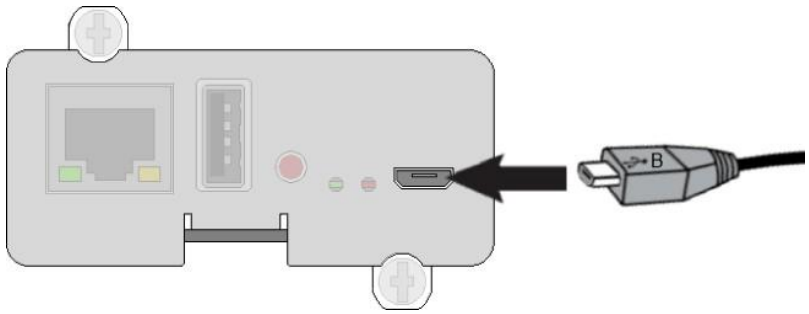
2.4.3 RNDISを介したWebインターフェースへのアクセス

この接続は、RNDIS (Ethernet over USB インターフェース) を介してネットワークモジュールのネットワーク設定にアクセスし、ローカルに設定するために使用されます。

2.4.3.1 設定ケーブルの接続

1. Micro-B to USBケーブルをホストコンピューターのUSBコネクタに接続します。

2. ケーブルをネットワークモジュールの設定コネクタに接続します。



2.4.3.2 RNDIS を通じての Web インターフェースアクセス

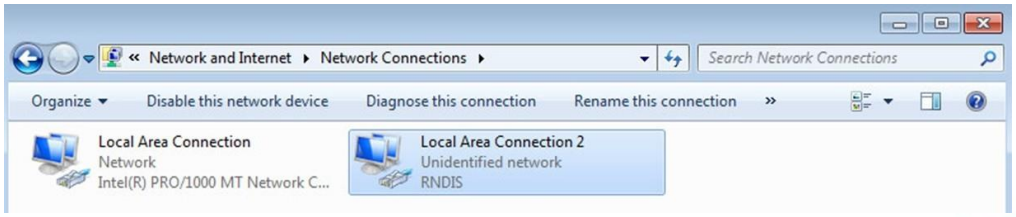
2.4.3.2.1 RNDISの設定

a 自動設定

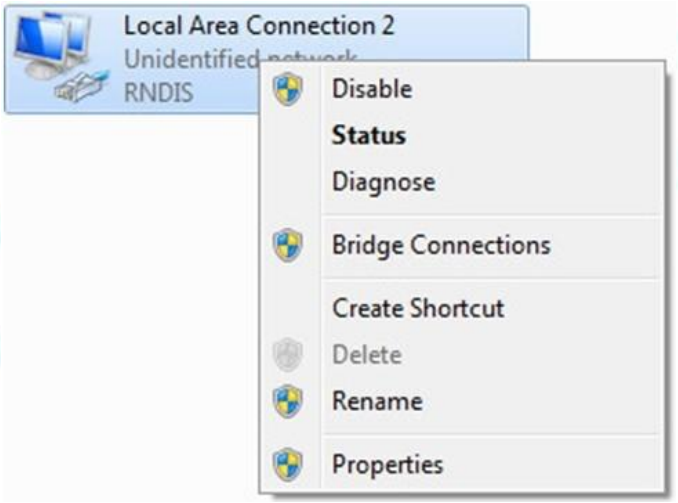
RNDISドライバは、USBからのネットワーク接続をエミュレートするために使用します。
カードをPCに接続すると、Windows® OSが自動的にRNDISドライバを検索します。
一部のコンピューターでは、OSがRNDISドライバを見つけることができ、設定が完了し、Webインターフェースへのアクセスに進むことができます。
他のいくつかのコンピューターでは、それが失敗する可能性がありますし、手動設定に進みます。

b 手動設定

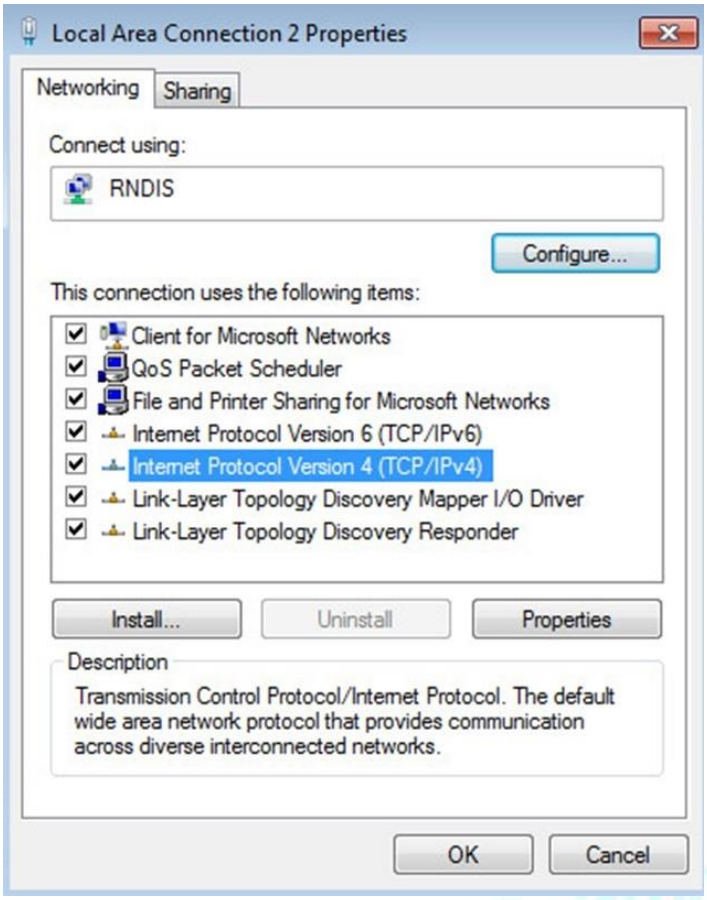
STEP 1 – Windows® OSが自動的にドライバを見つけられない場合は、Windowsのコントロールパネル>ネットワークと共有センター>ローカルエリア接続を選択してください。



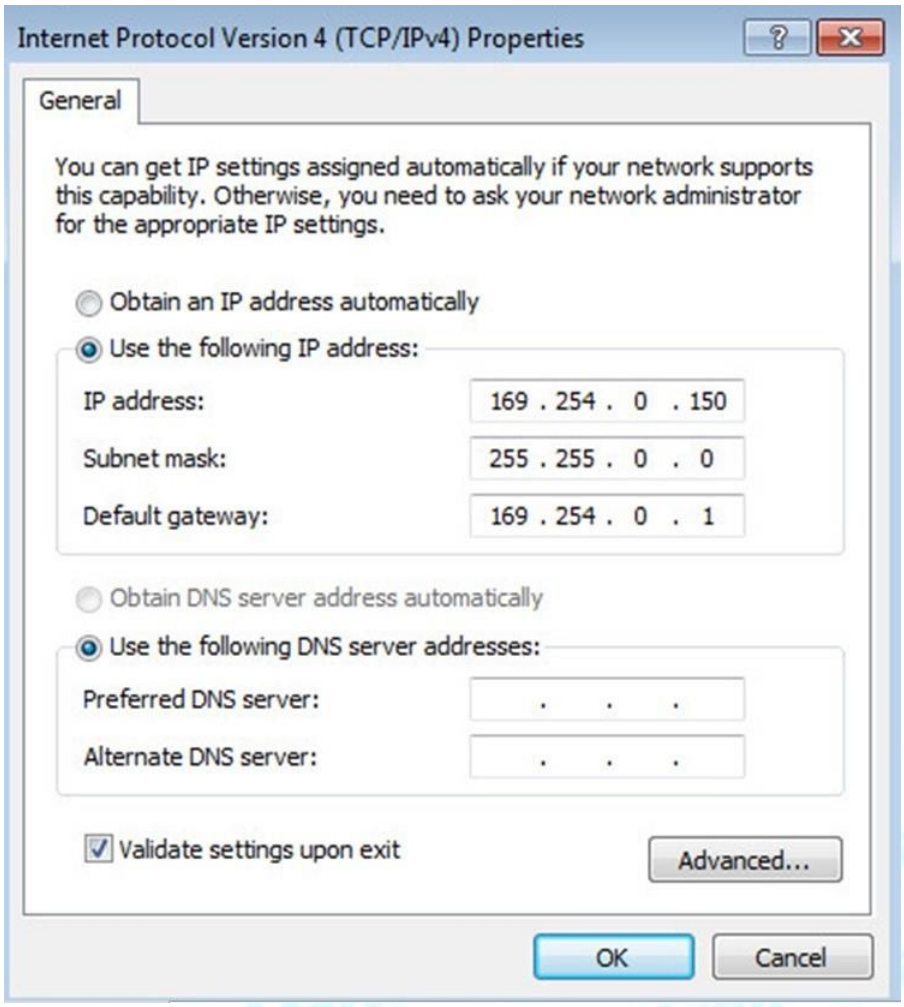
STEP 2 – RNDISローカルエリア接続を右クリックし、[プロパティ]を選択します。



STEP 3 –インターネットプロトコルバージョン4(TCP/IPv4)を選択して**[Properties(プロパティ)]**ボタンを押します。



STEP 4 –次に、以下のように設定を入力して検証（IP = 169.254.0.150、mask = 255.255.255.0.0）を行い、OKをクリックしてから[Close]をクリックします。



2.4.3.2.2 ウェブインターフェースへのアクセス

STEP 1 –デバイスの電源が入っていることを確認します。

STEP 2 –ホストコンピューターで、ウェブサイト www.eaton.com/downloads から rndis.7z ファイルをダウンロードし、解凍します。詳細については、次のセクションに移動します。Servicing the Network Management Module>>>Accessing to the latest Network Module firmware/driver

STEP 3 – setProxy.bat を起動して、必要に応じてプロキシの例外リストに 169.254.* を追加します。手動で構成するには、完全なドキュメント内のセクションに移動してください。 Installing the Network Management Module>>>Accessing the Network Module>>>Modifying the Proxy exception list

STEP 4 –サポートされているブラウザを起動すると、ブラウザウィンドウが表示されます。

STEP 5 – [Address/Location] フィールドに、**https://169.254.0.1**、RNDIS 用ネットワークモジュールのスタティック IP アドレスを入力します。ログイン画面が表示されます。

STEP 6 – [User Name] フィールドにユーザー名を入力します。デフォルトのユーザー名は **admin** です。

STEP 7 – Password(パスワード)フィールドにパスワードを入力します。デフォルトのパスワードは **admin** です。

STEP 8 – [**Login**] をクリックします。Network Module ローカル Web インターフェースが表示されます。

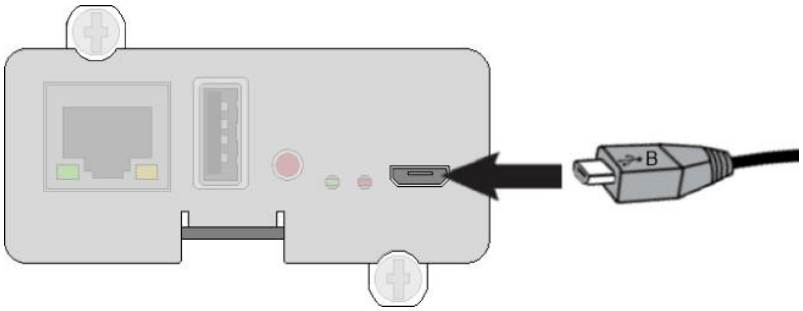
2.4.4 シリアルターミナルエミュレーションによるカードへのアクセス

この接続は、Serial (Serial over USB インターフェース) を通じて、ネットワークモジュールのネットワーク設定にローカルにアクセスして設定するために使用されます。

2.4.4.1 設定ケーブルの接続

STEP 1 – Micro-B to USBケーブルをホストコンピューターのUSBコネクタに接続します。

STEP 2 – ケーブルをネットワークモジュールの設定コネクタに接続します。



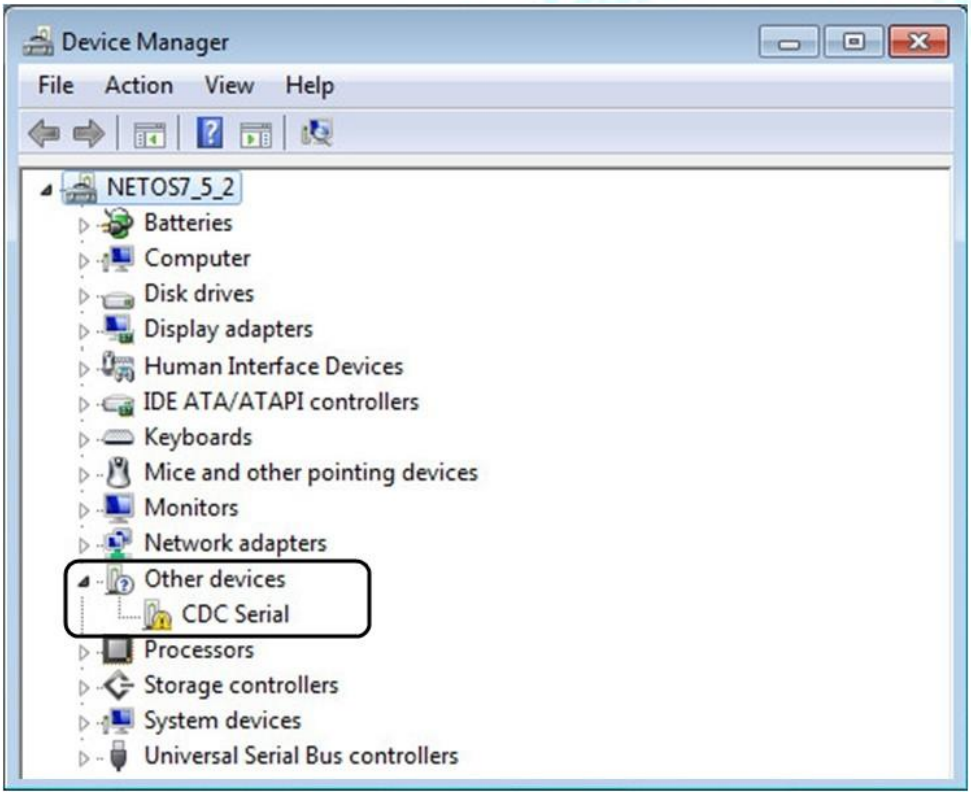
2.4.4.2 シリアル接続の手動設定

シリアルドライバは、USBからのシリアル接続をエミュレートするために使用します。
カードをPCに接続した後、Windows® OSがシリアル接続を検出するためには、ドライバの手動設定が必要です。

STEP 1 – ホストコンピューター上で、ウェブサイト www.eaton.com/downloads から rndis.7z ファイルをダウンロードし、解凍します。

STEP 2 – USBケーブルを差し込み、Windows®デバイスマネージャに移動します。

STEP 3 – リスト内のCDCシリアルをチェックし、黄色の感嘆符が付いている場合は、ドライバがインストールされていないことを意味する場合は、手順4-5-6-7に従ってくださいそれ以外の設定はOKです。

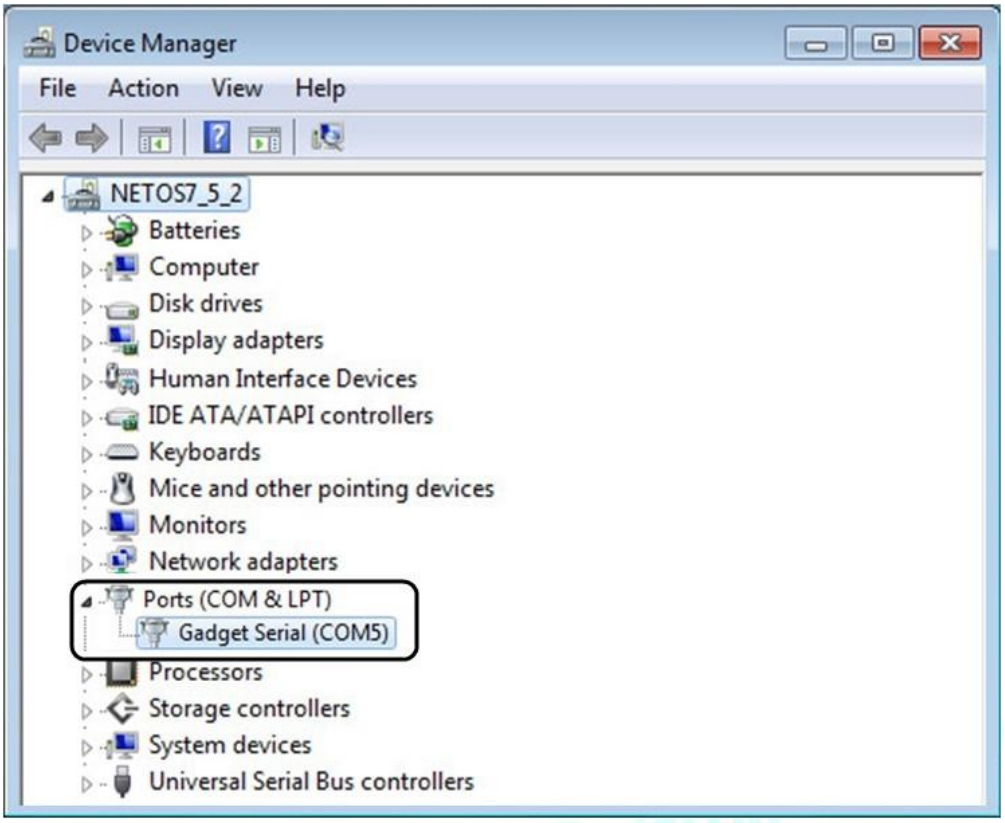


STEP 4 – 右クリックして、[ドライバソフトウェアの更新]を選択します。デバイスドライバソフトウェアの検索方法の選択を求められたら、「コンピューターでドライバソフトウェアを参照」を選択します。私のコンピューター上のデバイスドライバのリストから選択させてください」を選択します。

STEP 5 – 以前にドライバファイルをダウンロードしたフォルダを選択します。

STEP 6 – ドライバが署名されていないため警告ウィンドウが表示されます。「とにかくこのドライバソフトウェアをインストールする」を選択します。

STEP 7 – Windows®デバイスマネージャでガジェットシリアルデバイスのCOMポート番号が表示されたら、インストールは成功です。



2.4.4.3 シリアル経由でのカードへのアクセス

これは主にネットワークカードのネットワークと時間設定の自動設定を目的としています。また、ウェブ・ユーザー・インターフェースにアクセスできない場合には、ネットワークインターフェースのトラブルシューティングやリモート・リブート/リセットにも使用できます。

CLIにアクセスするには:

- SSH
- シリアルターミナルのエミュレーション。

⚠	ネットワークパラメーターを変更すると、カードがリモートで使用できなくなることがあります。このような場合は、USBを介してローカルで再構成するしかありません。
ℹ	利用可能なコマンドのこのリストは、CLIで入力することで見ることができます: *?* CLIで入力するとヘルプが表示されます:***help***

詳細については、以下を参照してください。Information>>>CLI

2.4.5 プロキシ例外リストの変更

USBケーブルを介してネットワークモジュールに接続し、システムがプロキシサーバーを使用して

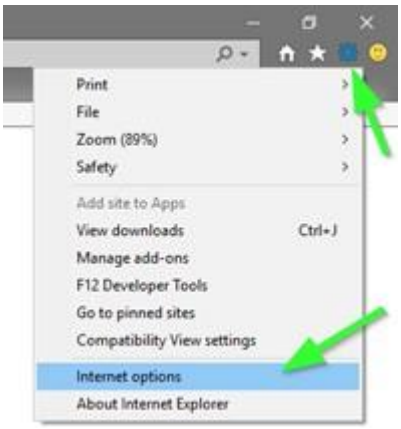
インターネットに接続するには、プロキシ設定でIPアドレス169.254.0.1を拒否することができます。

169.254.0.1 を拒否できます。* シーケンスは、物理的な接続を介してデバイスとの通信を設定す

るために使用されます。

この接続を有効にするには、プロキシ設定で例外を設定する必要があります。

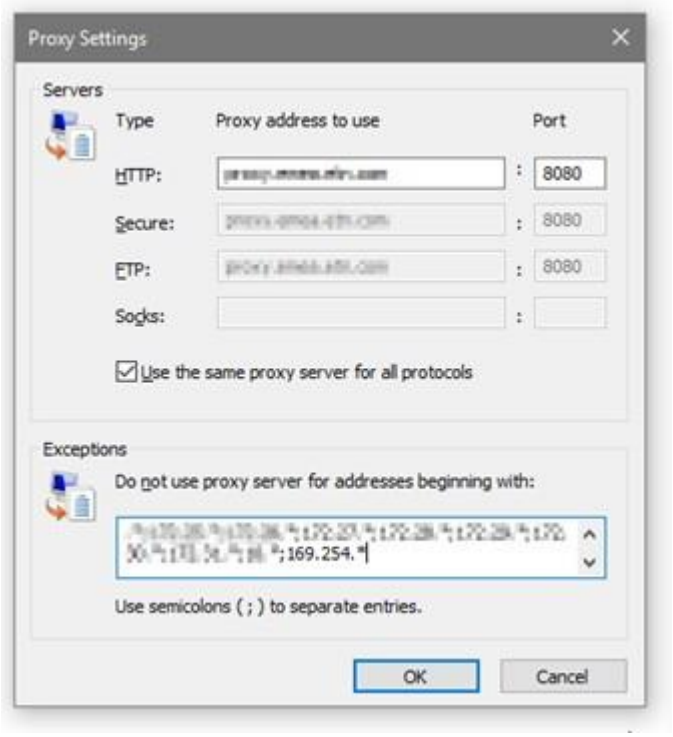
- Internet Explorerを開く
- 設定、インターネットオプションに移動



- 接続タブを選択します。
- LAN設定を押す

- ADVANCEDを押す

- 169.254のアドレスを追加します。*



- OKを押します。
- Internet Explorerを閉じて再度開きます。
- これで、Internet Explorerや他のブラウザで169.254.0.1というアドレスにアクセスできるようになりました。

2.5 Modbusの設定

2.5.1 通信パラメーターの設定

- ネットワークまたはRNDISを介してWebインターフェースにアクセスします。
- Contextual help>>Settings>>>Modbusに移動し、通信パラメーターを希望の設定に設定します。.

Modbus RTUの設定についてはContextual help>>Settings>>>Modbus>>Modbus RTUを参照してください。

Modbus TCPの設定についてはContextual help>>>Settings>>>Modbus>>Modbus TCPを参照してください。

2.5.2 利用可能なマップ

- ネットワークまたはRNDISを介してWebインターフェースにアクセスします。
- Contextual help>>Settings>>>Modbusに移動し、**[Supported MAPs（対応マップ）]**ボタンを押してMAPをダウンロードして下さい。

ファイルはリアルタイムで生成され、生成時のデバイス機能と値を考慮に入れます。
ダウンロードされたファイルの表は全てのレジスタを表示します。
Modbusマップで使用される単位は国際単位システムに属し、温度は例えばケルビンで表現されています。

2.5.2.1 テーブルコンテンツのマッピング

- address (hex): register address in hexadecimal
- address (1-base): register address in 1-base format

- Type: Register/Discrete
- Size in bytes
- Number of modbus registers
- Writable: True/False
- Representation: Int16/Uint16/String/Boolean/...
- Name
- Description
- Unit (Kelvin, A, V, W, VA, %, Hz, min, ...)
- Status to 0: status when the discrete equal 0
- Status to 1: status when the discrete equal 1
- Available: True/False – Shows if the register is available on current device
- Value: Shows current value of the register on current device

サポートされているModbusマッピングの例については下記を参照してください。
Installing the Network Management Module>>>Configuring Modbus>>>Example of supported Modbus mapping.

2.5.3 Modbus通信監視ツール

- SSHまたはシリアルターミナルエミュレーションを介してCLIにアクセスします。
- CLIで**?**と入力して利用可能なコマンドを取得します。

CLIコマンドはModbus通信の統計情報を取得するために使用することができます。詳細は下記を参照。
Information>>>CLI>>>modbus_statistics

2.5.4 サポートされているModbusマッピングの例

以下の表は、**[Supported MAPs（対応マップ）]**ボタンを押して Modbus 設定で取得できるマッピング情報の例です。.

address (hex)	address (1-base)	Type	Size in bytes	Number of modbus registers	Writable	Representation	Name	Description	Unit	Status to 0	Status to 1	Available	Value
0x100	256	Register	2	1	FALSE	Int16	Current phase 1 main 1	Input phase 1 current	A			FALSE	
0x101	257	Register	2	1	FALSE	Int16	Current phase 2 main 1	Input phase 2 current	A			FALSE	
0x103	259	Register	2	1	FALSE	Int16	Current phase 3 main 1	Input phase 3 current	A			FALSE	
0x106	262	Register	2	1	FALSE	Int16	Current phase 1 main 2	Bypass input phase 1 current	A			TRUE	0
0x107	263	Register	2	1	FALSE	Int16	Current phase 2 main 2	Bypass input phase 2 current	A			FALSE	
0x108	264	Register	2	1	FALSE	Int16	Current phase 3 main 2	Bypass input phase 3 current	A			FALSE	
0x109	265	Register	2	1	FALSE	Int16	Current phase 1 output	Output phase 1 current	A			TRUE	0
0x10a	266	Register	2	1	FALSE	Int16	Current phase 2 output	Output phase 2 current	A			FALSE	
0x10b	267	Register	2	1	FALSE	Int16	Current phase 3 output	Output phase 3 current	A			FALSE	
0x10e	270	Register	2	1	FALSE	Int16	Battery Current	Battery current	A			FALSE	
0x111	273	Register	2	1	FALSE	Uint16	Normal value active power	Normal value active power	W			TRUE	1500
0x115	277	Register	2	1	FALSE	Int16	U12 main 1	Input voltage between phases 1 and 2	V			FALSE	
0x116	278	Register	2	1	FALSE	Int16	U23 main 1	Input voltage between phases 2 and 3	V			FALSE	
0x117	279	Register	2	1	FALSE	Int16	U31 main 1	Input voltage between phases 3 and 1	V			FALSE	
0x11e	286	Register	2	1	FALSE	Int16	Voltage phase 1 main 2	Bypass input phase 1 voltage	V			TRUE	235
0x11f	287	Register	2	1	FALSE	Int16	Voltage phase 2 main 2	Bypass input phase 2 voltage	V			FALSE	
0x120	288	Register	2	1	FALSE	Int16	Voltage phase 3 main 2	Bypass input phase 3 voltage	V			FALSE	
0x120	288	Register	2	1	FALSE	Int16	Voltage phase 3 main 2	Bypass input phase 3 voltage	V			FALSE	
0x121	289	Register	2	1	FALSE	Int16	U12 main 2	Bypass input voltage between phases 1 and 2	V			FALSE	
0x122	290	Register	2	1	FALSE	Int16	U23 main 2	Bypass input voltage between phases 2 and 3	V			FALSE	
0x123	291	Register	2	1	FALSE	Int16	U31 main 2	Bypass input voltage between phases 3 and 1	V			FALSE	
0x124	292	Register	2	1	FALSE	Int16	Output voltage 1N	Output phase 1 voltage	V			TRUE	230
0x125	293	Register	2	1	FALSE	Int16	Output voltage 2N	Output phase 2 voltage	V			FALSE	
0x126	294	Register	2	1	FALSE	Int16	Output voltage 3N	Output phase 3 voltage	V			FALSE	
0x127	295	Register	2	1	FALSE	Int16	Output voltage 12	Output voltage between phases 1 and 2	V			FALSE	
0x128	296	Register	2	1	FALSE	Int16	Output voltage 23	Output voltage between phases 2 and 3	V			FALSE	
0x129	297	Register	2	1	FALSE	Int16	Output voltage 31	Output voltage between phases 3 and 1	V			FALSE	
0x12d	301	Register	2	1	FALSE	Int16	Battery Voltage	Battery voltage	V			TRUE	55
0x130	304	Register	2	1	FALSE	Int16	Output active power phase 1	Output active power phase 1	W			TRUE	0
0x131	305	Register	2	1	FALSE	Int16	Output active power phase 2	Output active power phase 2	W			FALSE	

address (hex)	address (1-base)	Type	Size in bytes	Number of modbus registers	Writable	Representation	Name	Description	Unit	Status to 0	Status to 1	Available	Value
0x132	**306**	Register	2	1	FALSE	Int16	Output active power phase 3	Output active power phase 3	W			FALSE	
0x133	**307**	Register	2	1	FALSE	Int16	Output apparent power phase 1	Output apparent power phase 1	VA			TRUE	0
0x134	**308**	Register	2	1	FALSE	Int16	Output apparent power phase 2	Output apparent power phase 2	VA			FALSE	
0x135	**309**	Register	2	1	FALSE	Int16	Output apparent power phase 3	Output apparent power phase 3	VA			FALSE	
0x136	**310**	Register	2	1	FALSE	Uint16	Output total active power	Output total active power	W			TRUE	0
0x137	**311**	Register	2	1	FALSE	Uint16	Output total apparent power	Output total apparent power	VA			TRUE	0
0x139	**313**	Register	2	1	FALSE	Uint16	% output load level	Output percent load level	%			TRUE	0
0x13a	**314**	Register	2	1	FALSE	Int16	Peak factor phase 1 x 100	Peak factor phase 1 x 100	-			FALSE	
0x13b	**315**	Register	2	1	FALSE	Int16	Peak factor phase 2 x 100	Peak factor phase 2 x 100	-			FALSE	
0x13c	**316**	Register	2	1	FALSE	Int16	Peak factor phase 3 x 100	Peak factor phase 3 x 100	-			FALSE	
0x13d	**317**	Register	2	1	FALSE	Uint16	Power factor x 100	Power factor x 100	-			TRUE	0
0x13e	**318**	Register	2	1	FALSE	Int16	Main 1 frequency	Input frequency	Hz			TRUE	50
0x140	**320**	Register	2	1	FALSE	Int16	Main 2 frequency	Bypass input frequency	Hz			TRUE	50
0x141	**321**	Register	2	1	FALSE	Int16	Output frequency	Output frequency	Hz			TRUE	50
0x149	**329**	Register	2	1	FALSE	Int16	Battery backup time	Battery backup time	Min			TRUE	0
0x14b	**331**	Register	2	1	FALSE	Uint16	Battery charging level	Battery charging level	%			TRUE	100
0x150	**336**	Register	2	1	FALSE	Int16	Voltage main 1 phase 1	Input voltage phase 1	V			TRUE	234
0x151	**337**	Register	2	1	FALSE	Int16	Voltage main 1 phase 2	Input voltage phase 2	V			FALSE	
0x152	**338**	Register	2	1	FALSE	Int16	Voltage main 1 phase 3	Input voltage phase 3	V			FALSE	
0x1a0	**416**	Register	14	7	FALSE	String	Manufacturer Name	Manufacturer name				TRUE	xxxxx
0x1a8	**424**	Register	14	7	FALSE	String	Product Name	Product name				TRUE	xxxxx
0x1b0	**432**	Register	14	7	FALSE	String	UPS Model	UPS model				TRUE	xxxxx
0x1b8	**440**	Register	14	7	FALSE	String	Serial Number	Serial number				TRUE	xxxxx
0x1c0	**448**	Register	14	7	FALSE	String	Part Number	Part number				TRUE	xxxxx
0x209	**521**	Register	2	1	FALSE	Uint16	Nominal value apparent power	Nominal value apparent power	VA			TRUE	1500
0x213	**531**	Register	2	1	FALSE	Int16	Nominal voltage of battery element	Nominal voltage of battery element	V			TRUE	48
0x400	**1024**	Discrete	1	1	FALSE	See Description	Load protected status	Load protected status		Load not protected	Load protected	TRUE	1
0x401	**1025**	Discrete	1	1	FALSE	Boolean	UPS coupled	UPS coupled status		UPS not coupled	UPS coupled	TRUE	1
0x402	**1026**	Discrete	1	1	FALSE	Boolean	Unit general alarm	Unit general alarm status		Unit no general alarm	Unit general alarm	TRUE	0
0x403	**1027**	Discrete	1	1	FALSE	Boolean	Configuration firmware fault	Configuration firmware fault status		Configuration firmware ok	Configuration firmware fault	TRUE	0
0x404	**1028**	Discrete	1	1	FALSE	See Description	UPS in backup status	UPS in backup status		UPS not in backup	UPS in backup	TRUE	0
0x405	**1029**	Discrete	1	1	FALSE	Boolean	Battery low warning	Battery low warning status		Battery ok	Battery low warning	TRUE	0
0x406	**1030**	Discrete	1	1	FALSE	Boolean	Low battery	Low battery status		Battery ok	Low battery	TRUE	0
0x407	**1031**	Discrete	1	1	FALSE	Boolean	Operation on static switch	Operation on static switch status		Operation not on static switch	Operation on static switch	FALSE	

address (hex)	address (1-base)	Type	Size in bytes	Number of modbus registers	Writable	Representation	Name	Description	Unit	Status to 0	Status to 1	Available	Value
0x409	1033	Discrete	1	1	FALSE	Boolean	Communication fault	Communication fault status		Communication ok	Communication fault	TRUE	0
0x40a	1034	Discrete	1	1	FALSE	Boolean	UPS overload	UPS overload status		UPS no overload	UPS overload	TRUE	0
0x40b	1035	Discrete	1	1	FALSE	Boolean	Emergency stop	Emergency stop status		No emergency stop	Emergency stop	TRUE	0
0x40d	1037	Discrete	1	1	FALSE	Boolean	Battery to be checked	Battery to be checked status		Battery not to be checked	Battery to be checked	TRUE	0
0x40e	1038	Discrete	1	1	FALSE	Boolean	Device verification fault	Device verification fault status		Device verification ok	Device verification fault	TRUE	0
0x411	1041	Discrete	3	3	FALSE	See Description	Ups Class	001: Off line / Line interactive 011: On line - unitary/parallel 100: On line - parallel with NS 101: On line - hot standby redundancy 000: Unknown				TRUE	11
0x415	1045	Discrete	1	1	FALSE	Boolean	Manual bypass present	Manual bypass present status		Manual bypass absent	Manual bypass present	FALSE	
0x416	1046	Discrete	1	1	FALSE	Boolean	Manual bypass switch	Manual bypass switch status		Manual bypass switch opened	Manual bypass switch closed	FALSE	
0x417	1047	Discrete	1	1	FALSE	Boolean	Mode ECO = 1	High efficiency mode		Not on high efficiency mode	On high efficiency mode	FALSE	
0x420	1056	Discrete	1	1	FALSE	Boolean	Battery present	Battery present status		Battery absent	Battery present	TRUE	1
0x421	1057	Discrete	1	1	FALSE	Boolean	Battery voltage unbalanced	Battery voltage unbalanced status		Battery voltage not unbalanced	Battery voltage unbalanced	FALSE	
0x422	1058	Discrete	1	1	FALSE	See Description	Battery test fault	Battery test result		Battery test ok	Battery test fault	TRUE	1
0x42a	1066	Discrete	1	1	FALSE	Boolean	Battery over temperature	Battery over temperature status		Battery normal temperature	Battery over temperature	FALSE	
0x42b	1067	Discrete	1	1	FALSE	Boolean	Battery fuse fault	Battery fuse fault status		Battery fuse ok	Battery fuse fault	FALSE	
0x42d	1069	Discrete	1	1	FALSE	Boolean	Battery over temperature	Battery over temperature status		Battery normal temperature	Battery over temperature	FALSE	
0x42e	1070	Discrete	1	1	FALSE	Boolean	Circuit breaker fuse fault	Circuit breaker fuse fault status		Circuit breaker fuse ok	Circuit breaker fuse fault	TRUE	0
0x42f	1071	Discrete	1	1	FALSE	Boolean	Circuit breaker QF1 status	Circuit breaker QF1 status		Circuit breaker QF1 opened	Circuit breaker QF1 closed	FALSE	
0x433	1075	Discrete	1	1	FALSE	Boolean	Time expired	Time expired status		Time not expired	Time expired	TRUE	0
0x440	1088	Discrete	1	1	FALSE	Boolean	Buck mode	Buck mode status		Not on buck mode	On buck mode	FALSE	
0x441	1089	Discrete	1	1	FALSE	Boolean	Boost mode	Boost mode status		Not on boost mode	On boost mode	FALSE	
0x442	1090	Discrete	1	1	FALSE	Boolean	Wiring fault	Wiring fault status		Wiring ok	Wiring fault	TRUE	0
0x443	1091	Discrete	1	1	FALSE	Boolean	Circuit breaker Q1 status	Circuit breaker Q1 status		Circuit breaker Q1 opened	Circuit breaker Q1 closed	FALSE	
0x448	1096	Discrete	1	1	FALSE	See Description	Main 1 voltage out of tolerance	Main 1 voltage out of tolerance		Input voltage is into the tolerance	Input voltage is out of tolerance	TRUE	0
0x449	1097	Discrete	1	1	FALSE	Boolean	Main 1 fuse fault	Main 1 fuse fault status		Main 1 fuse ok	Main 1 fuse fault	TRUE	0
0x44a	1098	Discrete	1	1	FALSE	Boolean	Charger over temperature fault	Charger over temperature status		Charger over temperature ok	Charger over temperature fault	FALSE	
0x44b	1099	Discrete	1	1	FALSE	Boolean	Main 1 frequency out of tolerance	Main 1 frequency out of tolerance status		Main 1 frequency not out of tolerance	Main 1 frequency out of tolerance	TRUE	0
0x457	1111	Discrete	1	1	FALSE	Boolean	Redundancy lost	Redundancy lost status		Redundancy not lost	Redundancy lost	FALSE	
0x461	1121	Discrete	1	1	FALSE	Boolean	Maintenance position	Maintenance position status		Not on maintenance position	On maintenance position	FALSE	
0x465	1125	Discrete	1	1	FALSE	Boolean	Main 2 overload	Main 2 overload status		Main 2 no overload	Main 2 overload	TRUE	0
0x466	1126	Discrete	1	1	FALSE	Boolean	Main 2 thermal overload	Main 2 thermal overload status		Main 2 thermal no overload	Main 2 thermal overload	FALSE	

address (hex)	address (1-base)	Type	Size in bytes	Number of modbus registers	Writable	Representation	Name	Description	Unit	Status to 0	Status to 1	Available	Value
0x467	1127	Discrete	1	1	FALSE	Boolean	Output on bypass	Output on bypass status		Output not on bypass	Output on bypass	TRUE	1
0x469	1129	Discrete	1	1	FALSE	Boolean	Main 2 frequency out of tolerance	Main 2 frequency out of tolerance status		Main 2 frequency not out of tolerance	Main 2 frequency out of tolerance	TRUE	0
0x46a	1130	Discrete	1	1	FALSE	Boolean	Main 2 voltage out of tolerance	Main 2 voltage out of tolerance status		Main 2 voltage not out of tolerance	Main 2 voltage out of tolerance	FALSE	
0x46b	1131	Discrete	1	1	FALSE	Boolean	Phase M2 out of tolerance	Phase M2 out of tolerance status		Phase M2 not out of tolerance	Phase M2 out of tolerance	TRUE	0
0x46e	1134	Discrete	1	1	FALSE	Boolean	Circuit breaker Q4S status	Circuit breaker Q4S status		Circuit breaker Q4S opened	Circuit breaker Q4S closed	FALSE	
0x470	1136	Discrete	1	1	FALSE	Boolean	Internal fault	Internal fault status		No internal fault	Internal fault	FALSE	
0x479	1145	Discrete	1	1	FALSE	Boolean	Main 2 internal fault	Main 2 internal fault status		Main 2 no internal fault	Main 2 internal fault	FALSE	
0x47b	1147	Discrete	1	1	FALSE	Boolean	Output switch status			Output switch opened	Output switch closed	FALSE	
0x490	1168	Discrete	1	1	FALSE	Boolean	Charger general fault	Charger general fault status		Charger no general fault	Charger general fault	TRUE	0
0x491	1169	Discrete	1	1	FALSE	Boolean	Battery charge	Battery charging status		Battery not charging	Battery charging	TRUE	1
0x493	1171	Discrete	1	1	FALSE	Boolean	Battery charge	Battery charging status		Battery not charging	Battery charging	TRUE	1
0x4a1	1185	Discrete	1	1	FALSE	Boolean	Chopper fault	Chopper fault status		Chopper ok	Chopper fault	TRUE	0
0x4a2	1186	Discrete	1	1	FALSE	Boolean	Rectifier short circuit	Rectifier short circuit status		Rectifier not onshort circuit	Rectifier on short circuit	TRUE	0
0x4c1	1217	Discrete	1	1	FALSE	Boolean	Inverter major fault	Inverter major fault status		Inverter ok	Inverter major fault	TRUE	0
0x4c2	1218	Discrete	1	1	FALSE	Boolean	Inverter overload	Inverter overload status		Inverter no overload	Inverter overload	TRUE	0
0x4c3	1219	Discrete	1	1	FALSE	Boolean	Inverter thermal overload	Inverter thermal overload status		Inverter no thermal overload	Inverter thermal overload	FALSE	
0x4c4	1220	Discrete	1	1	FALSE	Boolean	Inverter current limitation	Inverter current limitation status		Inverter no current limitation	Inverter current limitation	TRUE	0
0x4c5	1221	Discrete	1	1	FALSE	Boolean	UPS fuse fault	UPS fuse fault status		UPS fuse ok	UPS fuse fault	FALSE	
0x4ca	1226	Discrete	1	1	FALSE	Boolean	Inverter over temperature	Inverter over temperature status		Inverter no over temperature	Inverter over temperature	TRUE	0
0x4f1	1265	Discrete	1	1	FALSE	Boolean	Short circuit	Short circuit status		No short circuit	Short circuit	TRUE	0
0x501	1281	Discrete	1	1	FALSE	Boolean	Output voltage too high	Output voltage too high status		Output voltage not too high	Output voltage too high	FALSE	
0x502	1282	Discrete	1	1	FALSE	Boolean	Output voltage too low	Output voltage too low status		Output voltage not too low	Output voltage too low	FALSE	
0x503	1283	Discrete	1	1	FALSE	Boolean	Input voltage of bypass too high	Input voltage of bypass too high status		Input voltage of bypass not too high	Input voltage of bypass too high	FALSE	
0x504	1284	Discrete	1	1	FALSE	Boolean	Input voltage of bypass too low	Input voltage of bypass too low status		Input voltage of bypass not too low	Input voltage of bypass too low	FALSE	
0x505	1285	Discrete	1	1	FALSE	Boolean	Output frequency out of range	Output frequency out of range status		Output frequency not out of range	Output frequency out of range	FALSE	
0x506	1286	Discrete	1	1	FALSE	Boolean	Electronic power supply fault	Electronic power supply status		Electronic power supply ok	Electronic power supply fault	FALSE	
0x507	1287	Discrete	1	1	FALSE	Boolean	Bypass wiring fault	Bypass wiring fault status		Bypass wiring ok	Bypass wiring fault	FALSE	
0x508	1288	Discrete	1	1	FALSE	Boolean	Shutdown in progress	Shutdown in progress status		Shutdown not in progress	Shutdown in progress	FALSE	
0x509	1289	Discrete	1	1	FALSE	Boolean	Compatibility failure	Compatibility failure status		No compatibility failure	Compatibility failure	TRUE	0
0x50a	1290	Discrete	1	1	FALSE	Boolean	Rectifier used	Rectifier used status		Rectifier not used	Rectifier used	FALSE	

2.6 ネットワークモジュールの設定

ネットワークモジュールを設定するには、Web インターフェースを使用します。メインの Web インターフェースメニューを以下に説明します。

2.6.1 メニュー構造

	**Home:** デバイスの概要とステータス（アクティブなアラーム、コンセントのステータス、...）

	**Meters:** 電力品質のメーターとログ。
	**Controls:** デバイスやコンセントの制御。
	**Protection:** エージェント一覧、エージェントのシャットダウン順序、停電時のシャットダウン
	**Environment:** コミッショニング/ステータス、アラーム設定、情報
	**Settings:** ネットワークモジュールの設定。
	**Maintenance:** ファームウェア、サービス、リソース、システムログ
	**Legal:** 法的情報、ソースコードの利用可能性、専有要素に関する注意事項。
	**Profile:** ユーザープロファイル、パスワード変更、アカウント情報、ログアウトを表示します。
	**Help:** 別のブラウザページでドキュメントの全文を開きます。
 	**Alarms:** アラームページを開き、アクティブなアラームの数を表示します。

3 Webインターフェースのコンテキストヘルプ

3.1 ログインページ

ページの言語はデフォルトでは英語に設定されていますが、管理時にブラウザの言語に切り替えることができます。

割り当てられたIPアドレスに移動したら、ブラウザ上で信頼されていない証明書を受け入れます。

3.1.1 初めてログインする

3.1.1.1 1. デフォルトのパスワードを入力します。

初めてネットワークモジュールにログインするときは、工場出荷時に設定されているデフォルトのユーザー名とパスワードを入力する必要があります。.

- Username = admin
- Password = admin

3.1.1.2 2. デフォルトパスワードの変更

デフォルトパスワードの変更は必須で、専用ウィンドウで要求されます。最初に現在のパスワードを入力し、次に新しいパスワードを2回入力します。
安全なパスワードを定義するには、ツールチップに記載されているパスワード形式の推奨事項に従ってください。

3.1.1.3 3. ライセンス契約の承諾

次のステップでは、使用許諾契約書が表示されま

す。契約書を読み、同意して続行します。

3.1.2 トラブルシューティング

パスワードを忘れた場合のログイン方法は？

アクション

- パスワードの初期化は管理者に依頼してください。
- – あなたがメイン管理者の場合、パスワードはServicing the Network Management Module>>>Recovering main administrator password .

FWアップグレード後のWebユーザーインターフェースが最新ではない

症状

アップグレード後:
- ウェブインターフェースが最新ではない
- 新FWの新機能は表示されない

考えられる原因

ブラウザは、過去のFWデータを含むキャッシュを介してWebインターフェースを表示しています。

アクション

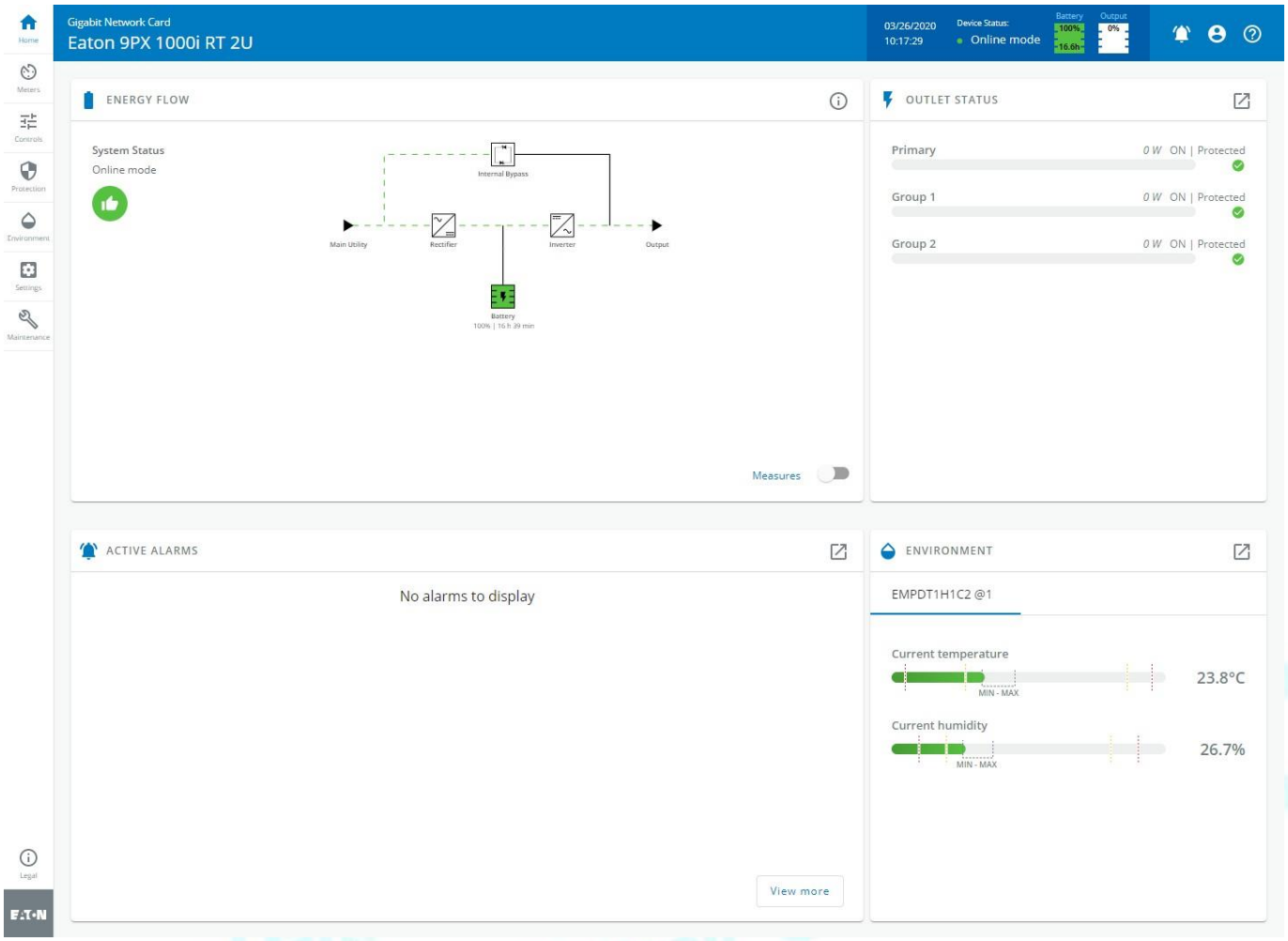
F5またはCTRL+F5を使用してブラウザのキャッシュを空にします。

3.1.2.1 その他の課題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.2 ホーム

ホーム画面では、キーメジャーやアクティブアラームを含むデバイスのステータス情報を提供します。



3.2.1 トップバーの情報/ステータス

- **Card name:** カード名を表示します。.
- **Device name:** デバイスモデルまたはシステム名をデフォルトで表示します。
  Contextual help>>>Maintenance>>>System information
- **Date and time:** ローカルタイムを表示しますが、UTCタイムは表示されません。
- **Device status:** デバイスの状態を表示します。
- **Output power:** 出力電力のステータス情報を提供します。
- **Battery status:** バッテリのステータス情報を提供します。

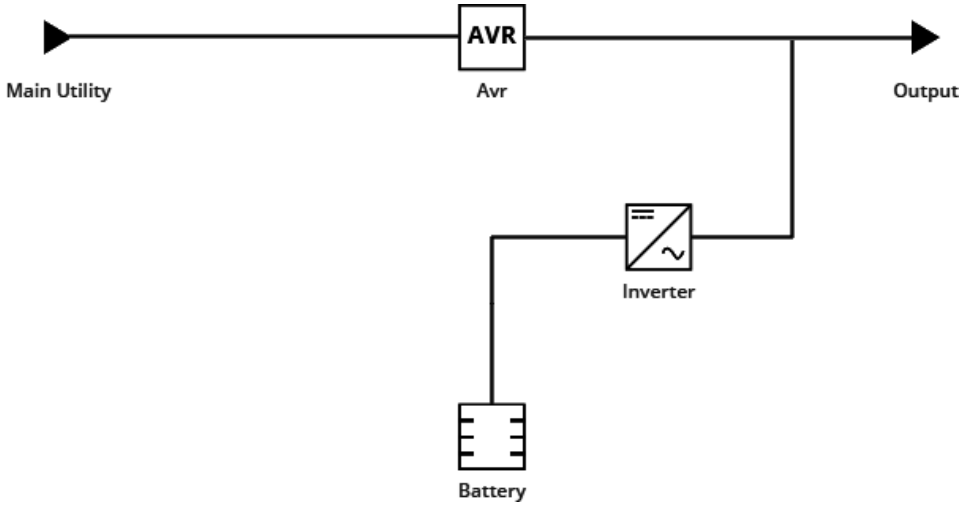
3.2.2 メニュー構造

	Home: デバイスの概要とステータス（アクティブなアラーム、コンセントのステータス、...）
	Meters: 電力品質のメーターとログ。

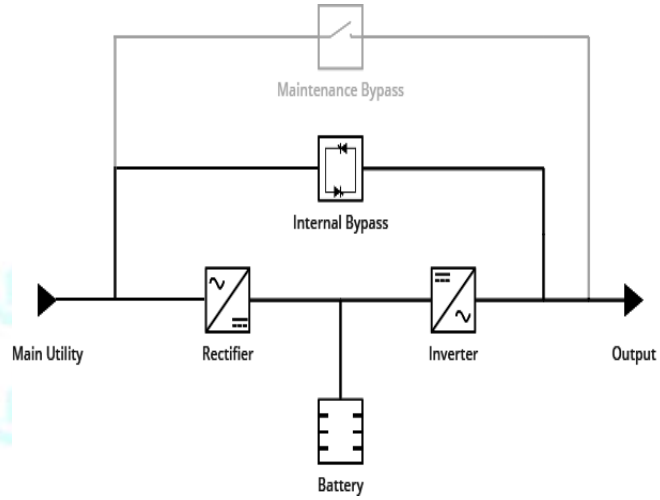
	**Controls:** デバイスやコンセントの制御。
	**Protection:** エージェント一覧、エージェントのシャットダウン順序、停電時のシャットダウン
	**Environment:** コミッショニング/ステータス、アラーム設定、情報
	**Settings:** **ネットワークモジュールの設定。**
	**Maintenance:** ファームウェア、サービス、リソース、システムログ
	**Legal:** 法的情報、ソースコードの利用可能性、専有要素に関する注意事項。
	**Profile:** **ユーザープロファイル、パスワード変更、アカウント情報、ログアウトを表示します。**
	**Help:** 別のブラウザページでドキュメントの全文を開きます。
 	**Alarms:** アラームページを開き、アクティブなアラームの数を表示します。

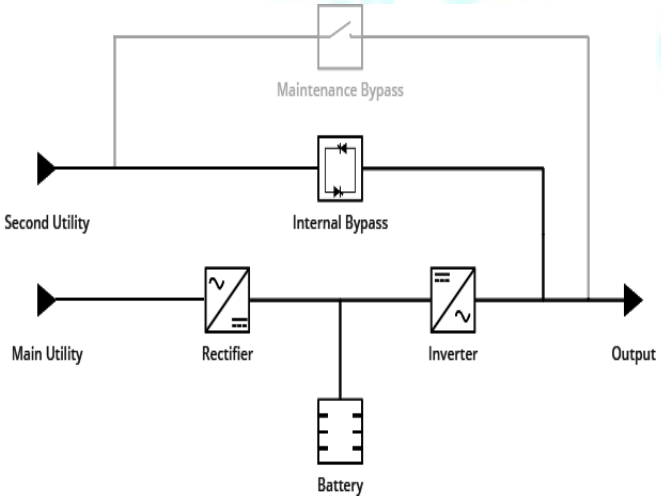
3.2.3 エネルギーフロー図

3.2.3.1 ラインインタラクティブUPS

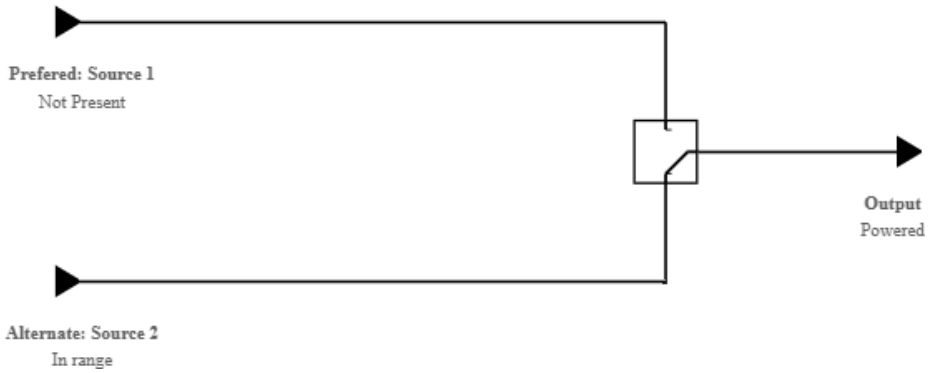


3.2.3.2 オンラインUPS

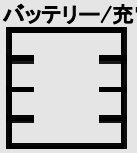
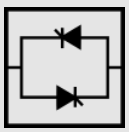




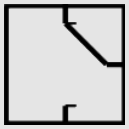
3.2.3.3 ATS



3.2.3.4 ダイアグラム要素の説明

説明とシンボル	説明	シンボルの下にある可能性のある状態		
		良好	警告	不良
入力 	主なユーティリティ入力	In range	Out of nominal range	
出力 	UPSの出力	Protected Powered	In overload Not protected	In short circuit
AVR デバイス 	装置は保護されており、AVR装置を介して電源が供給されます。	Normal mode Buck mode Boost mode	In overload	
整流器 	整流器：交流電力を直流電力に変換します。	Normal HE mode (ready) / ESS mode (ready)	In overload	In short circuit In fault
バッテリー/充電器 	バッテリーと内蔵バッテリー充電器。	Battery: OK Charger: Charging Floating Resting Off	Battery: End of life	Battery: In fault Charger: In fault Not present
インバーター 	インバーター: AC電源にDC電源を変換します。	Normal	In overload	In short circuit In fault
内部バイパス 	自動バイパス	Powered (standby, auto bypass, forced bypass, HE mode, ESS mode)	In overload	In fault

メンテナンス バイパス （オプション） 	メンテナンスバイパスを閉鎖しました。	Maintenance		

ATSデバイス 	装置はATS装置を介して電源を供給されます。			

説明とシンボル	**説明**	**可能な状態**		
		Green	**Orange**	**Black**
配線 	ブロック間の電気的接続。	Energy flow	In overload Out of nominal range	No energy Unknown

3.2.3.5 詳細

デバイスの詳細にアクセスするには、アイコンを押します。:

このビューには、デバイス識別情報と公称値の概要が表示されます。:

- Name
- Model
- P/N
- S/N
- Location
- Firmware version
- Input Voltage
- Input Frequency
- Output Voltage
- Output Frequency

[COPY TO CLIPBOARD（クリップボードにコピー）]ボタンは、情報をクリップボードにコピーします。例えば、電子メールに情報をコピーして貼り付けることができます。

3.2.3.6 対策の表示

シノプティックの入出力メジャーを提供します。

3.2.3.6.1 Example #1

1相入力、1相出力のシングル入力ソース:

入力対策	出力対策
Voltage (V) Current (A) Frequency (Hz)	Voltage (V) Current (A) Frequency (Hz)

3.2.3.6.2 例 #2

3相入力、3相出力のデュアル入力ソース

入力対策(主・副)			出力対策		
Phase #1 Voltage (V) Current (A)	Phase #2 Voltage (V) Current (A)	Phase #3 Voltage (V) Current (A)	Phase #1 Voltage (V) Current (A)	Phase #2 Voltage (V) Current (A)	Phase #3 Voltage (V) Current (A) Load (W) Load (%)
Frequency (Hz)			Frequency (Hz)		

3.2.4 コンセントの状態

負荷分割による UPS コンセントの状態(ON/OFF)を提供します。:

- ステータス(ON/OFF- 保護されている/保護されていない/電源が入っていない)
- 負荷レベル (W) - UPS モデルによる可用性

Note: ロード・セグメンテーションにより、長時間の停電時に優先度の高い機器以外の機器を自動的にパワーダウンさせて、重要な機器のバッテリーランタイムを維持することができます。
またこの機能は突入電流を制限する為のリモート再起動やシーケンシャル起動サーバーにも使用されます。

Note: コントロールメニューにアクセスするには、アイコンを押してください:

3.2.5 アクティブアラーム

アクティブなアラームのみが表示され、アラームアイコンにはアクティブなアラームの数も表示されます。アラームは、日付、アラートレベル、時間、および説明によってソートされます。

Note: アラームの履歴を表示するには、アイコンを押します。:

3.2.6 環境

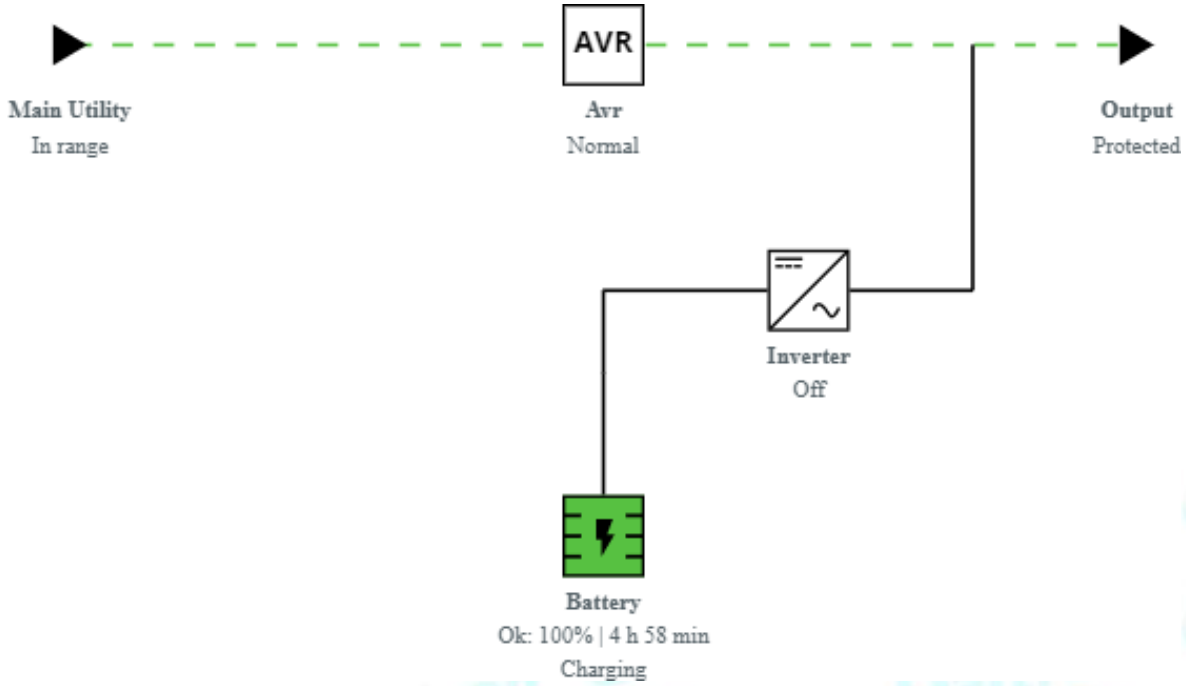
センサーの状態とデータは利用可能な場合は表示され、MIN-MAXはセンサーによって測定された最小および最大の温度または湿度を表示します。

Note: センサーデータの詳細を表示するには、アイコンを押します。:

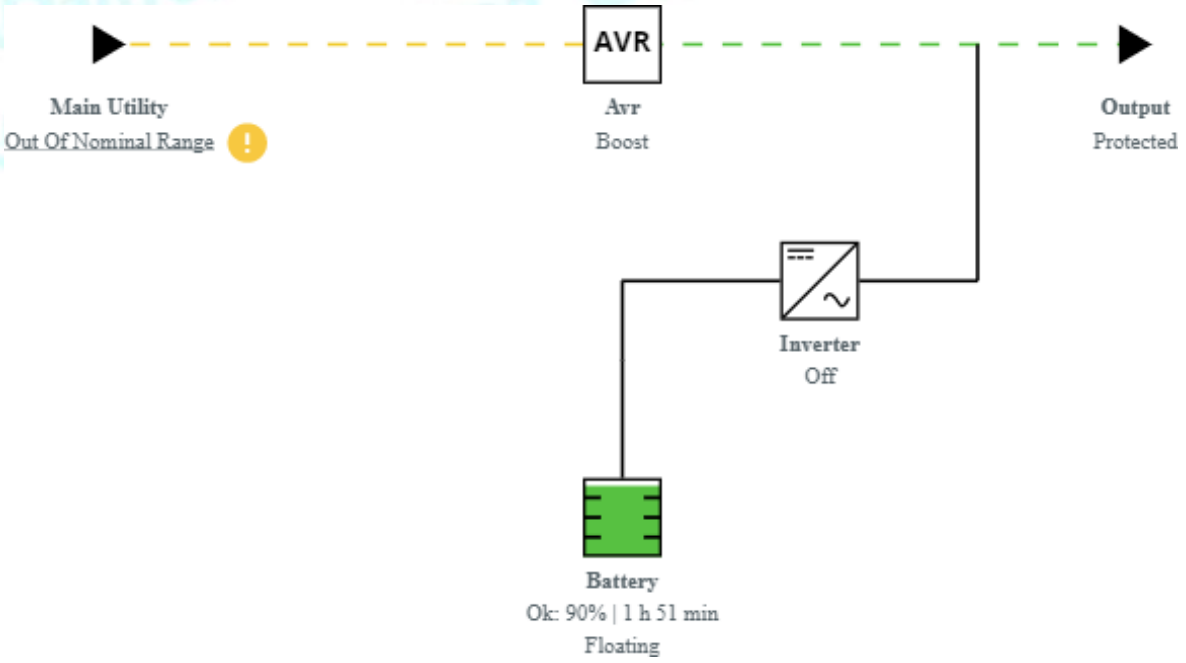
3.2.7 エネルギーフロー図の例

3.2.7.1 ラインインタラクティブUPS

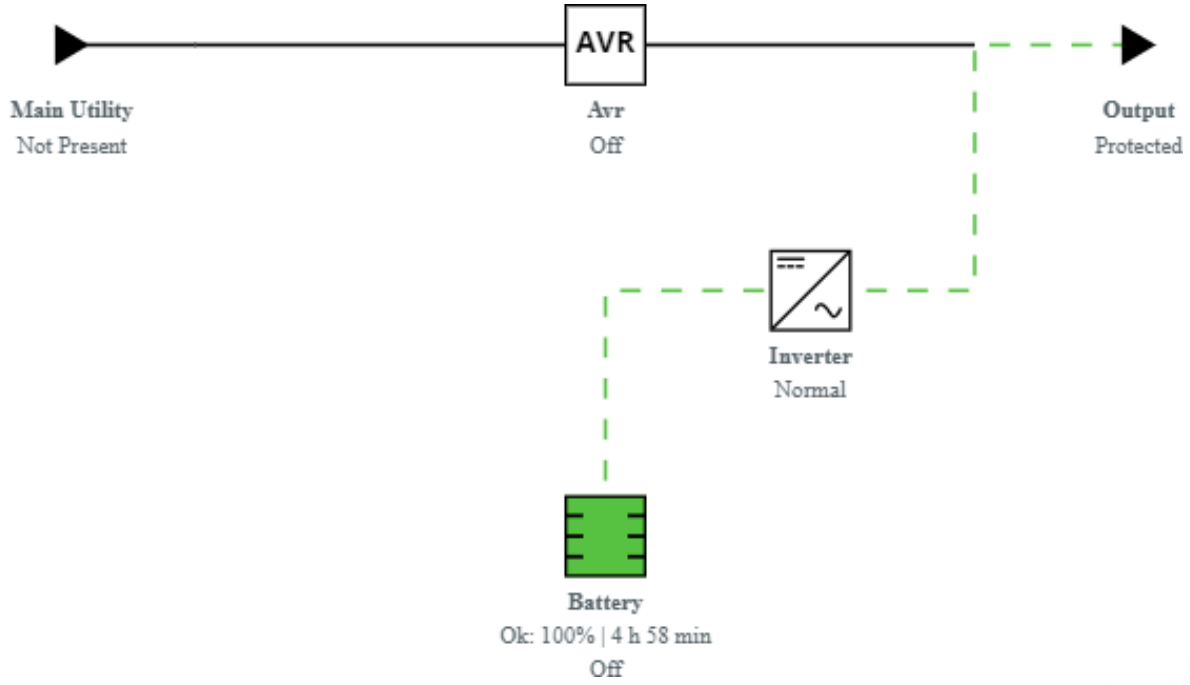
3.2.7.1.1 通常モード



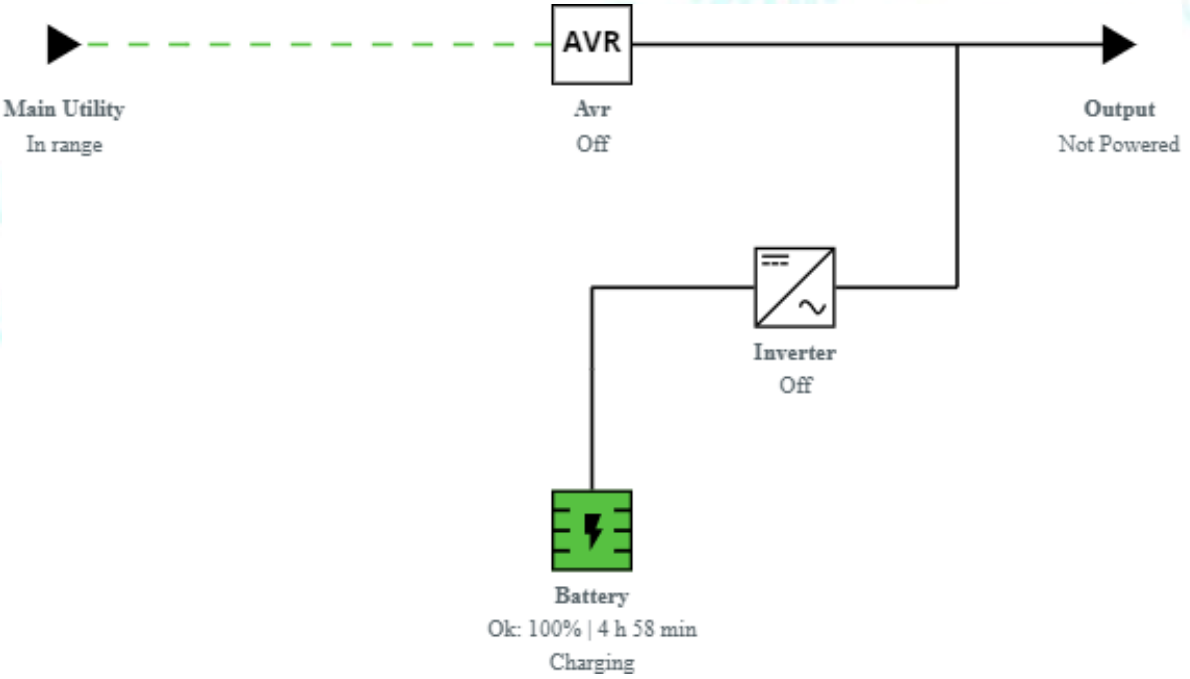
3.2.7.1.2 バック/ブーストモード



3.2.7.1.3 バッテリーモード

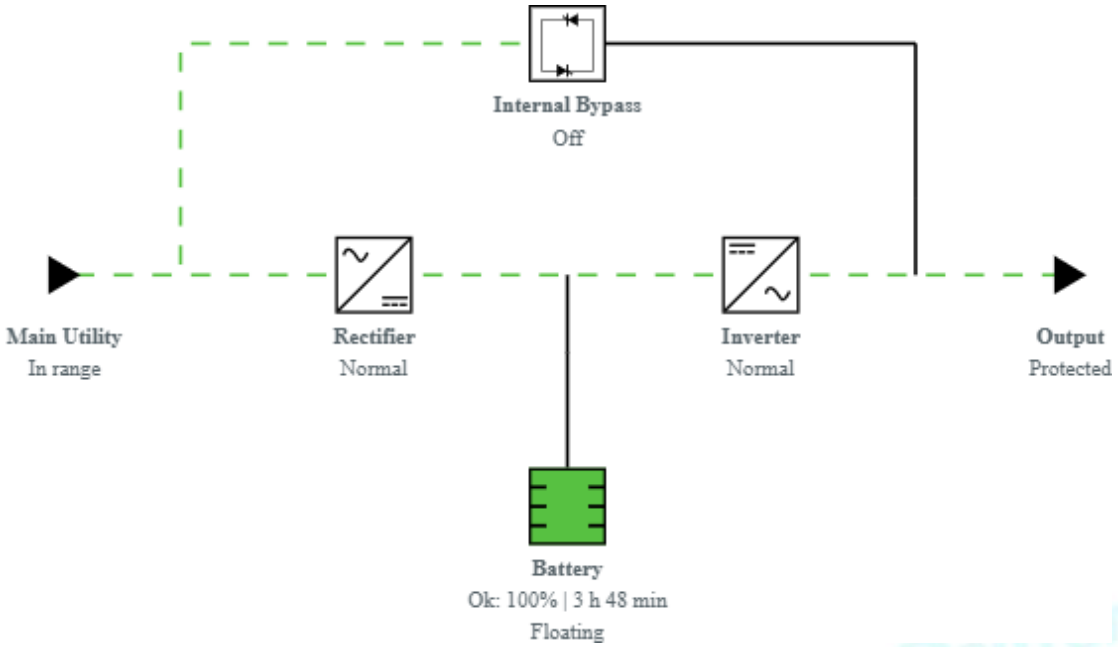


3.2.7.1.4 Off モード

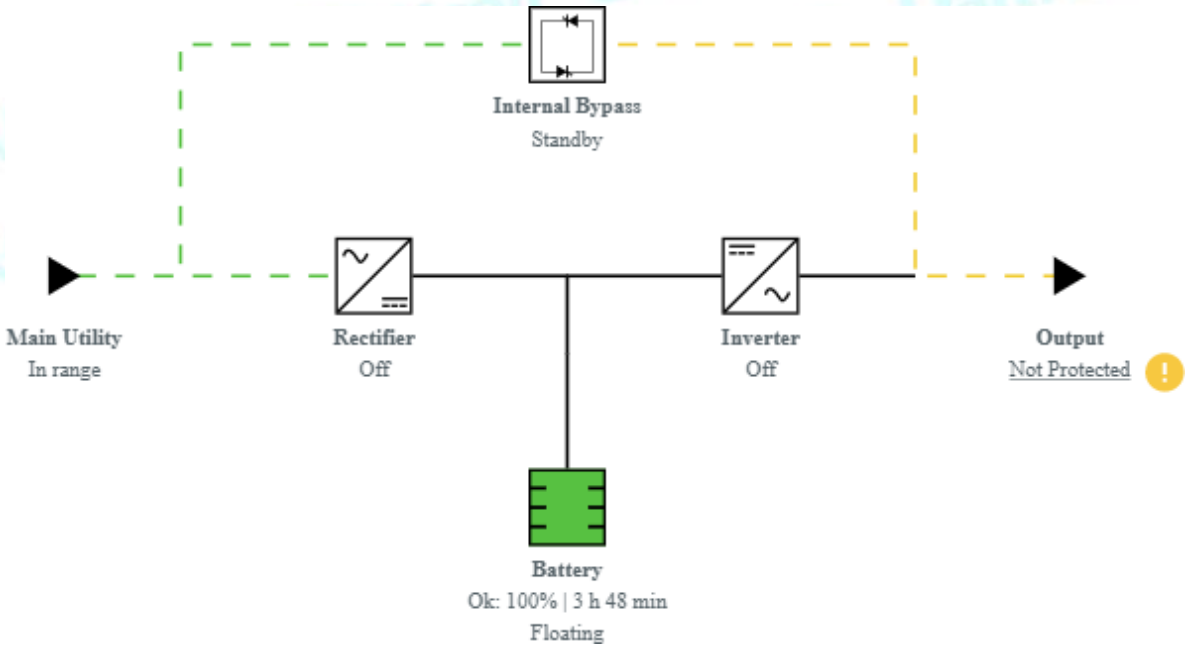


3.2.7.2 単一入力ソースのオンラインUPS

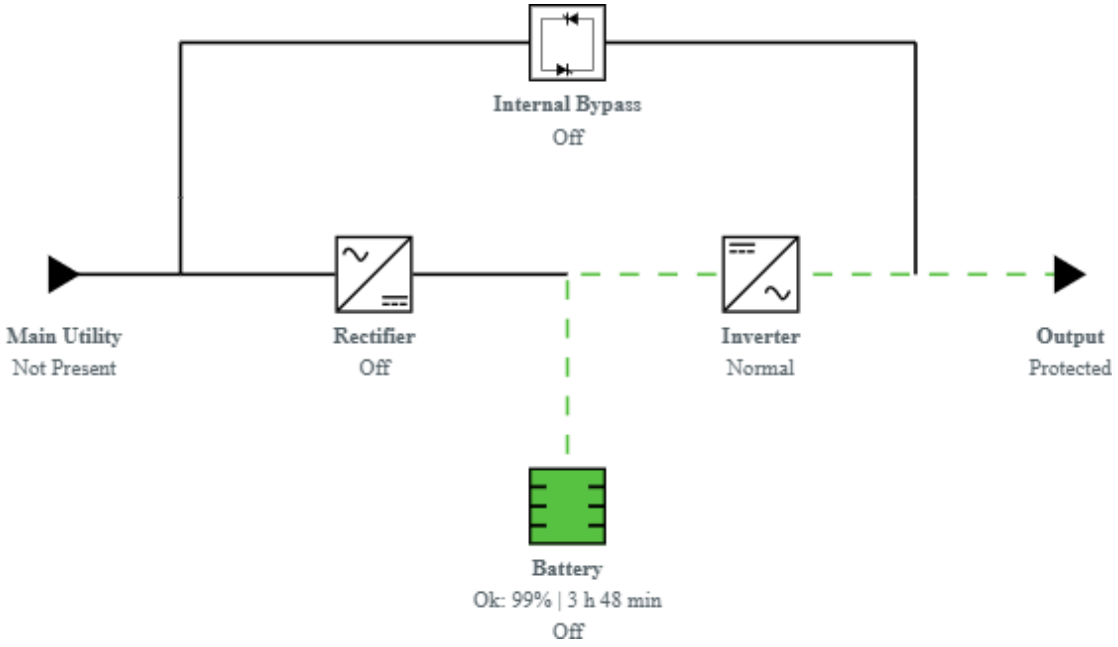
3.2.7.2.1 オンラインモード



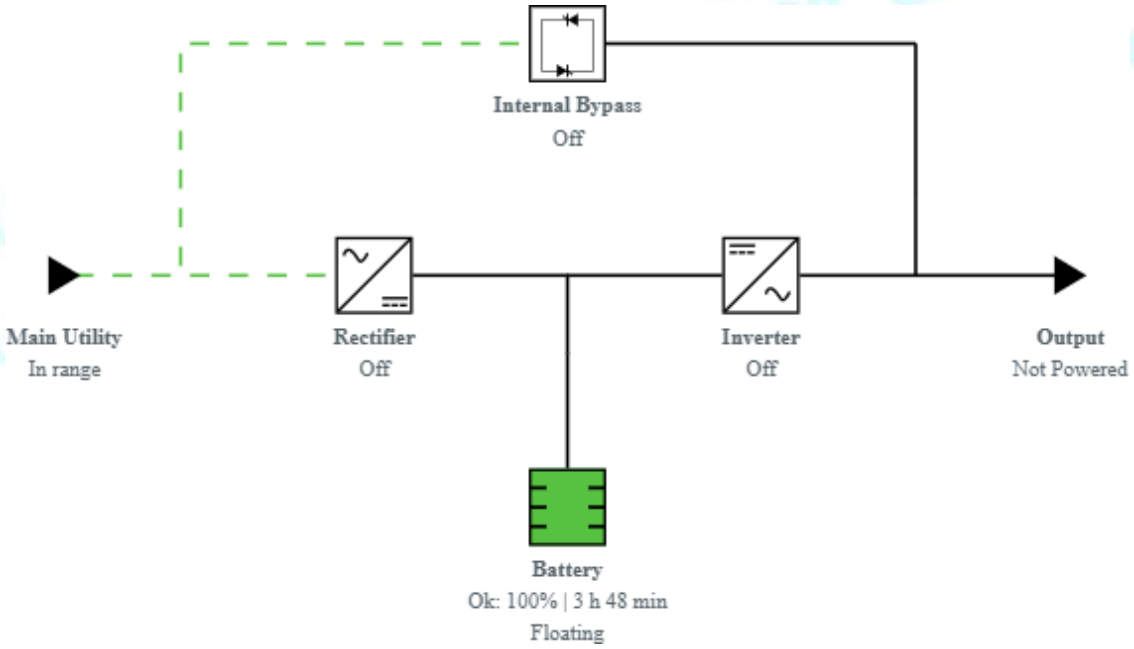
3.2.7.2.2 バイパスモード



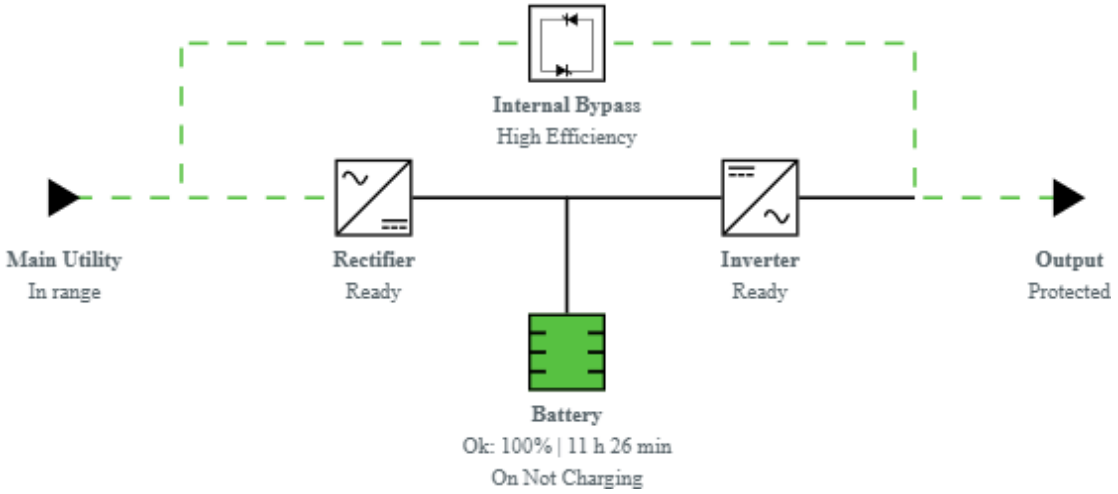
3.2.7.2.3 バッテリーモード



3.2.7.2.4 Off モード

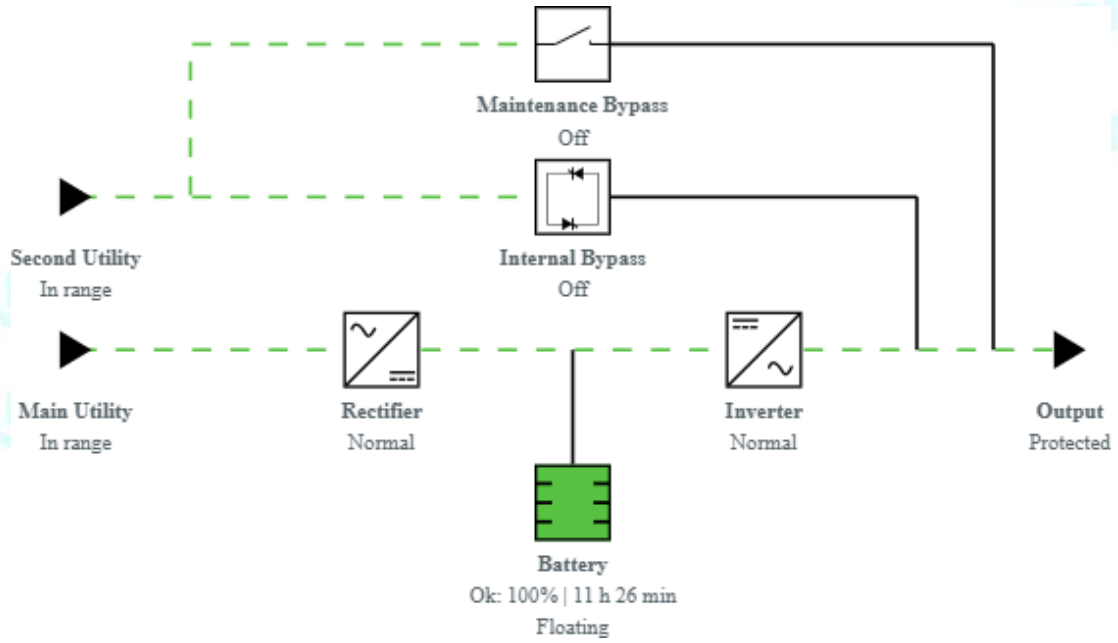


3.2.7.2.5 HE モード / ESS モード

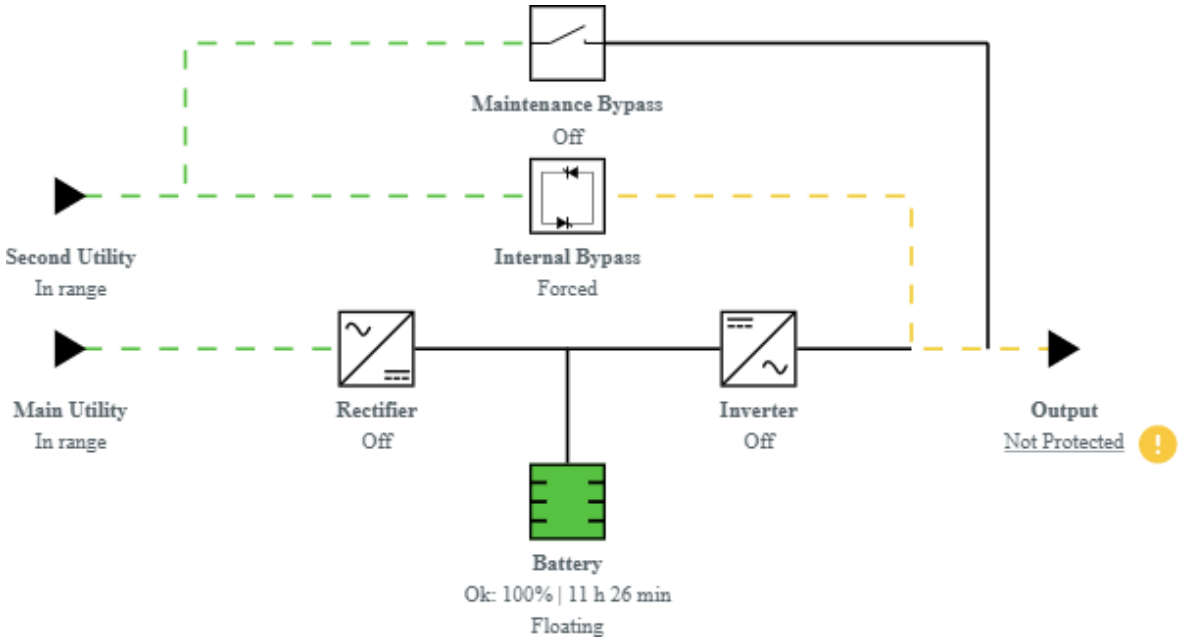


3.2.7.3 デュアル入力ソースとメンテナンスバイパスを備えたオンラインUPS

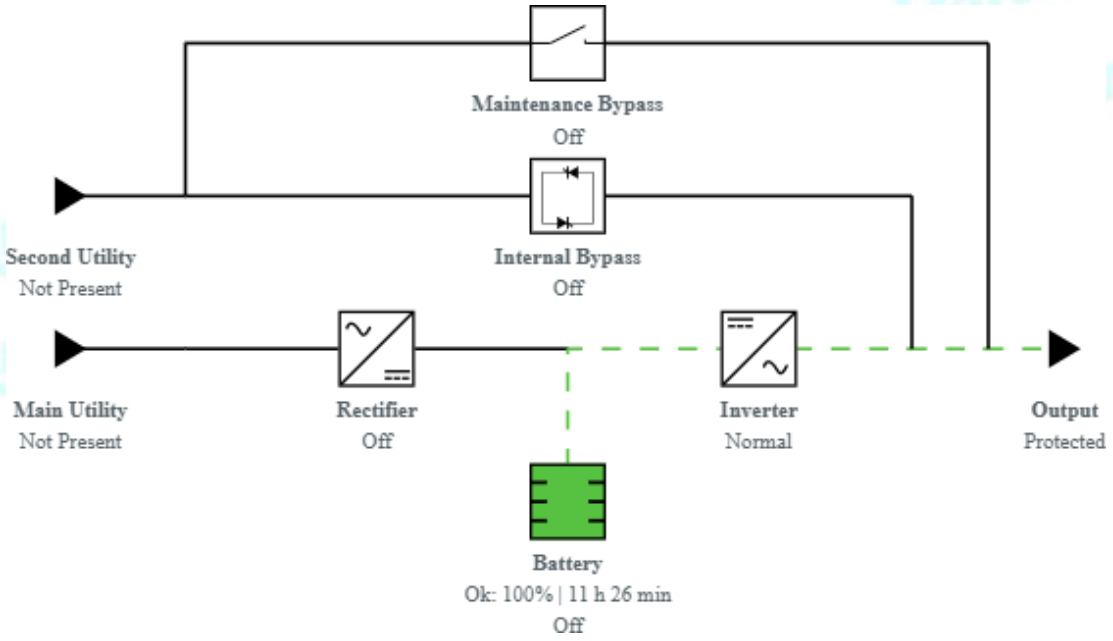
3.2.7.3.1 オンラインモード



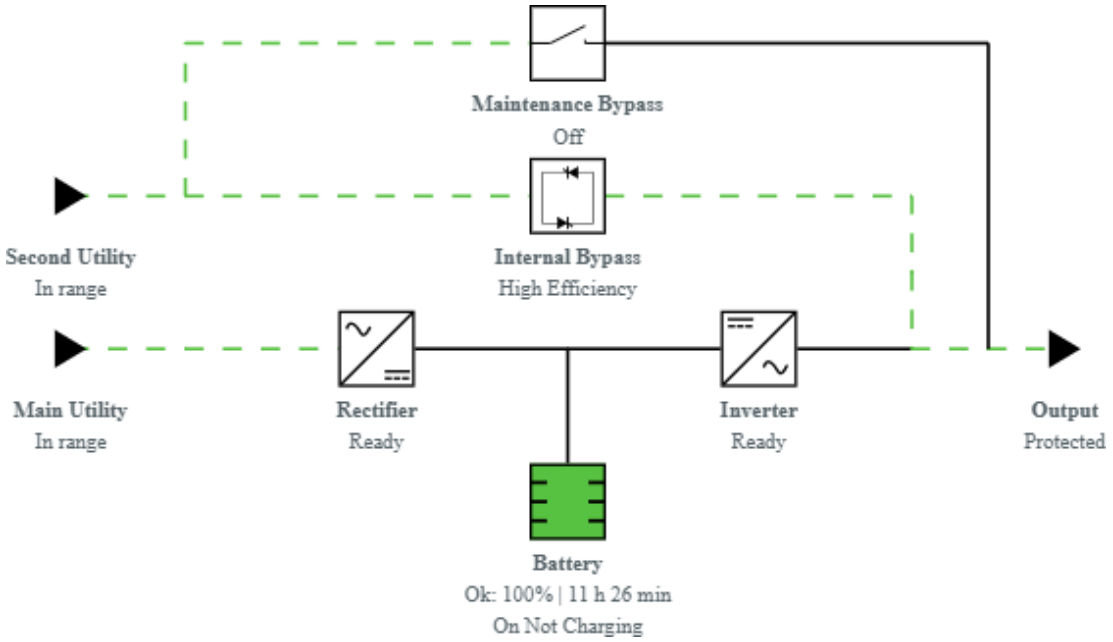
3.2.7.3.2 バイパスモード



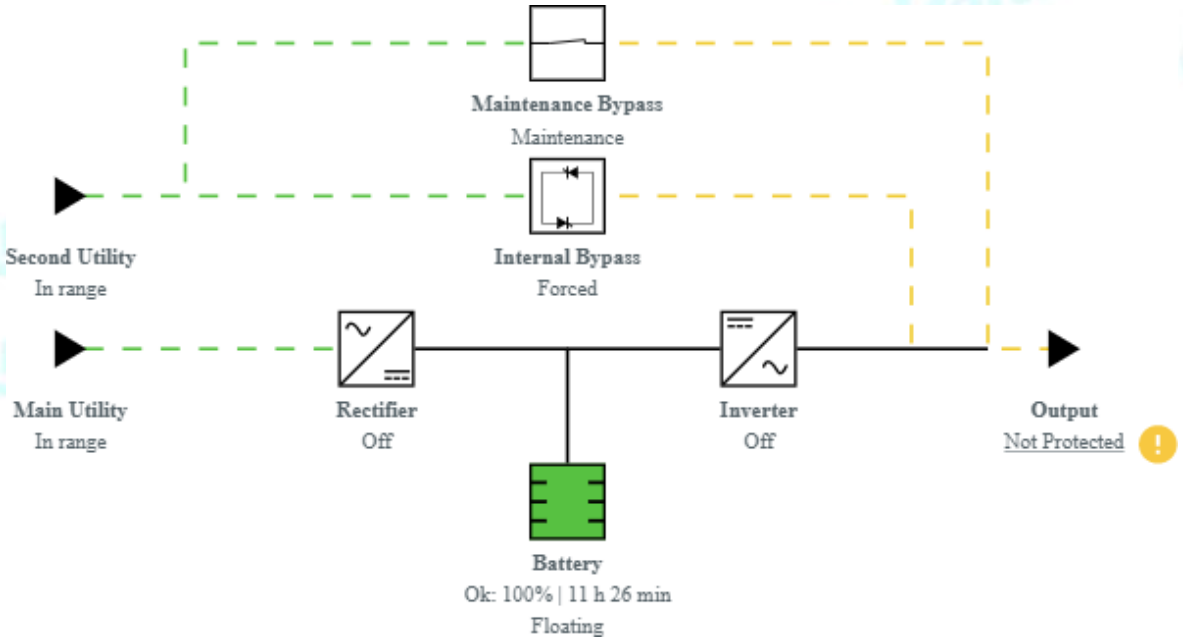
3.2.7.3.3 バッテリーモード



3.2.7.3.4 HE モード / ESS モード



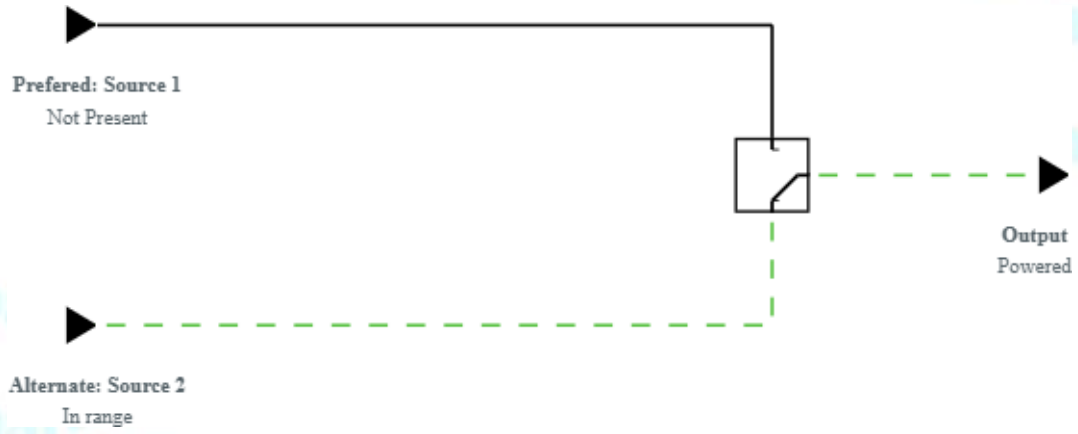
3.2.7.3.5 メンテナンスバイパスモード



3.2.7.4 ATS

3.2.7.4.1 通常モード

3.2.7.4.2 優先される電源ソースの欠落



3.2.8 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Home	✔	✔	✔

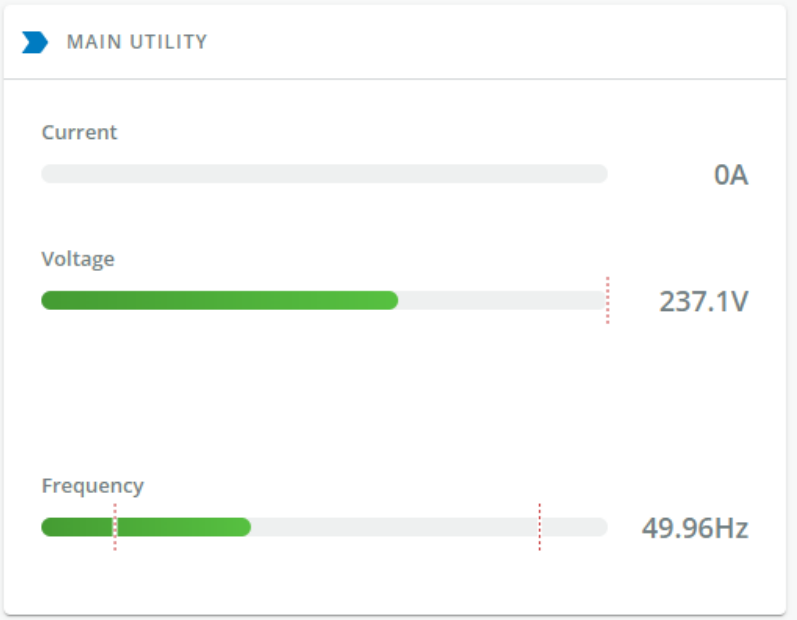
3.2.8.1 その他のアクセス権について

その他のアクセス権については下記を確認してください。
Information>>>Access rights per profiles

3.3 メーター

ゲージのカラーコード:
- Green: しきい値内の値.
- Orange/Red: しきい値の外側の値.
- Grey: デバイスが提供するしきい値はありません.

3.3.1 メインユーティリティ入力



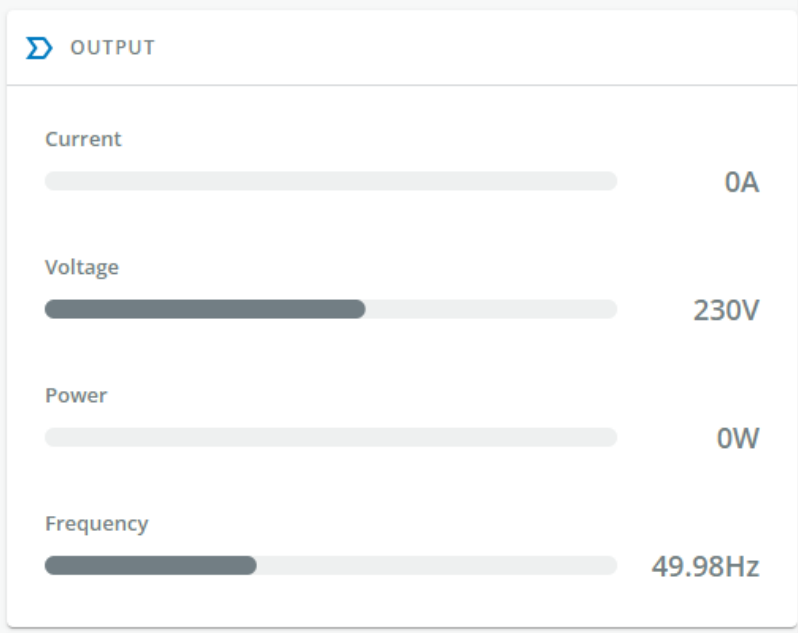
製品の主なユーティリティ対策を表示します。
- Current (A)
- Voltage (V)

3.3.2 セカンドユーティリティ入力(利用可能な場合)

提示された場合、製品の第2の効用測定値を表示します。

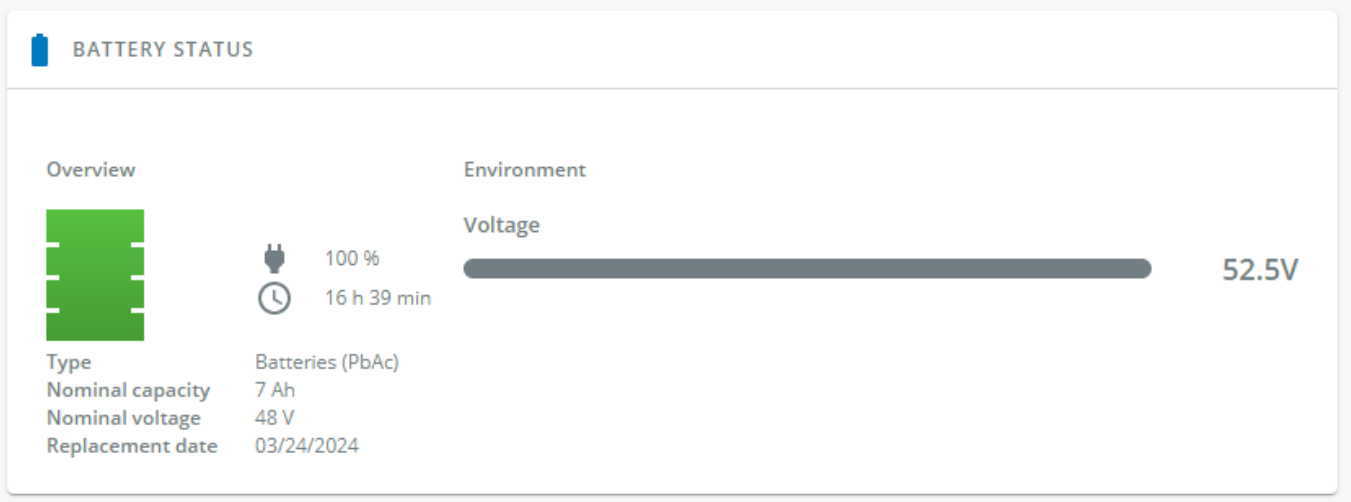
- Current (A)
- Voltage (V)

3.3.3 出力



- Voltage (V)
- Power (W)
- Current (A)

3.3.4 バッテリーの状態



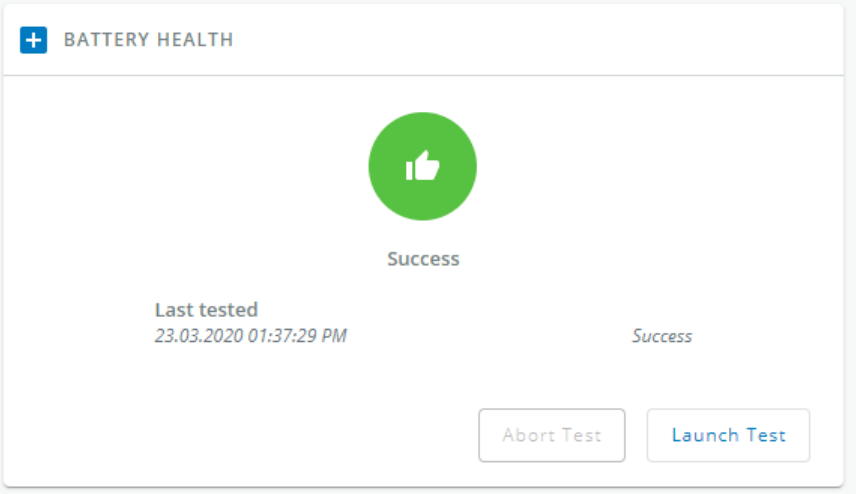
バッテリーステータスセクションは、バッテリー情報の概要です。

表示される情報は機器によって異なります。

3.3.4.1 概要・環境

- Type
- Nominal capacity
- Nominal voltage
- Capacity remaining
- Runtime
- State
- Recommended replacement date
- State of health
- Voltage
- Current
- Temperature
- Min cell voltage
- Max cell voltage
- Number of cycles
- Min temperature
- Max temperature
- BMS state

3.3.5 バッテリーヘルス



バッテリーヘルスセクションでは、バッテリーの状態を表示し、バッテリーテストを開始することができます。

ステータスは、最後に完了したバッテリーテストの結果だけでなく、その重要なステータス（色）と完了時間を反映しています。

- Pass
- Warning
- Fail
- Unknown

3.3.5.1 コマンド

[Launch test（起動テスト）]ボタンは、バッテリーテストがすでに進行中またはスケジュールされている場合には無効になります。

[Abort test（テスト中止）]ボタンは、テストが進行中またはスケジュールされている場合にのみ有効になります。

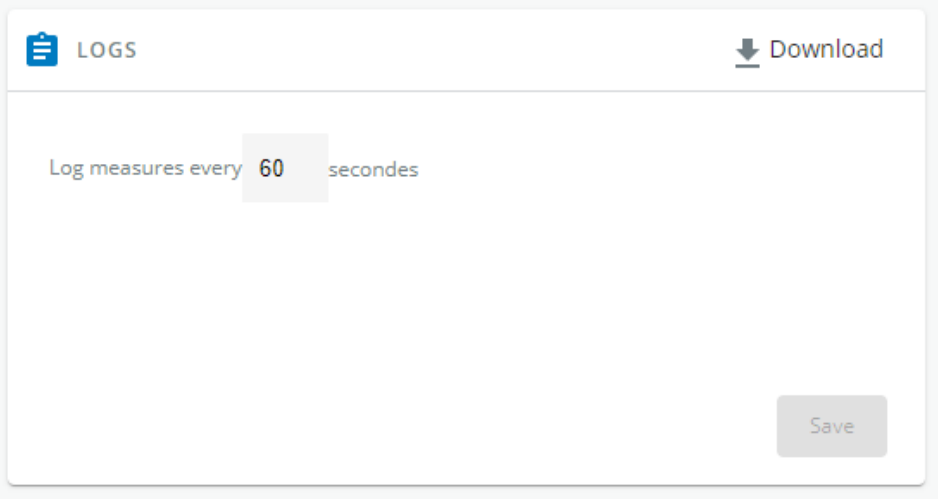
.

3.3.5.2 保留中のアクション

保留中のアクションは、バッテリーテストの状態を反映しています。

- None
- Scheduled
- In progress
- Aborted
- Done

3.3.6 ログ



このログ構成では、デバイスメジャーのログ取得頻度のみを定義することができます。

センサー計測ログの取得は設定できず、分単位で行われます。センサー計測のログは環境メニューからアクセスできます。

3.3.6.1 ダウンロード

右上のアイコンを押すと、デバイスログファイルがダウンロードされます。可能であれば、可能な対策は以下の通りです。:

- Input Voltage (V)
- Input Frequency (Hz)
- Bypass Voltage (V)
- Bypass Frequency (Hz)
- Output Voltage (V)
- Output Frequency (Hz)
- Output Current (A)
- Output Apparent Power (VA)
- Output Active Power (W)
- Output Power Factor
- Output Percent Load (%)
- Battery Voltage (V)
- Battery Capacity (%)
- Battery Remaining Time (s)

3.3.7 デフォルト設定と可能なパラメーター –メーター

	デフォルト設定	**設定可能なパラメーター**
Meters/Logs	ログの測定– 60s	ログの測定– 3600s maximum

3.3.7.1 その他の設定について

その他の設定については次を参照：Information>>>Default settings parameters

3.3.8 プロファイルごとのアクセス権

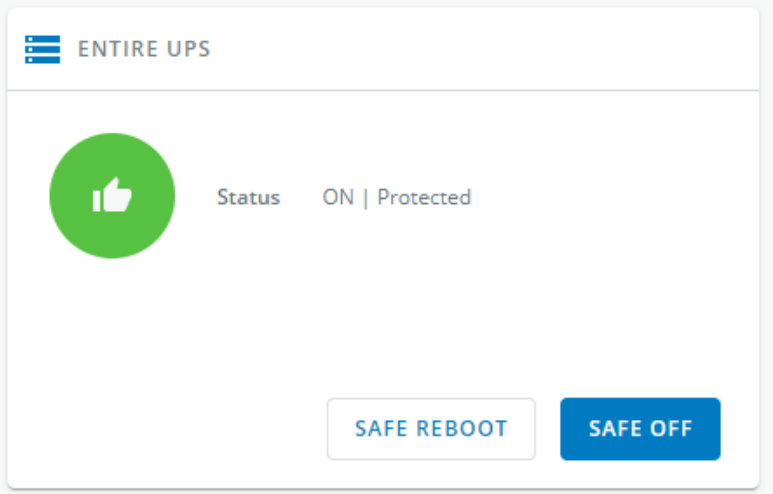
	Administrator	Operator	Viewer
Meters	✓	✓	✓
Battery health: Launch test/Abort	✓	✓	✗
Logs configuration	✓	✓	✗

3.3.8.1 その他のアクセス権について

その他の設定については次を参照： Information>>>Access rights per profiles

3.4 コントロール

3.4.1 UPS全体



コントロールは UPS 全体に対して表示され、特定のコンセントオプションに対しては表示されません。

このセクションの表には、UPS のステータス、関連するコマンド（on / off ）、および保留中のアクションが表示されます。

3.4.1.1 ステータス

UPS の現在のモードを反映します。以下は、UPS トポロジーに基づいて表示されるテーブルの潜在的な値のリストです。.

- On — Protected/Not protected
- Off — Not powered/Not protected

3.4.1.2 コマンド

以下のいずれかのボタンを押すと、一連のコマンドが使用可能になり、有効になります。確認画面が表示されます。

- **Safe OFF**

  これにより、負荷がシャットダウンされます。保護されたアプリケーションは安全にパワーダウンされます。

  この制御は、ステータスが OFF ではなく、アクティブなコマンドが実行されていない場合にのみ使用できます。

- **Safe reboot**

  これでシャットオフしてから負荷をオンにします。保護されたアプリケーションは安全にパワーダウンされます。この制御は、ステータスが OFF ではなく、アクティブなコマンドが実行されていない場合にのみ使用できます。

- **Switch ON**

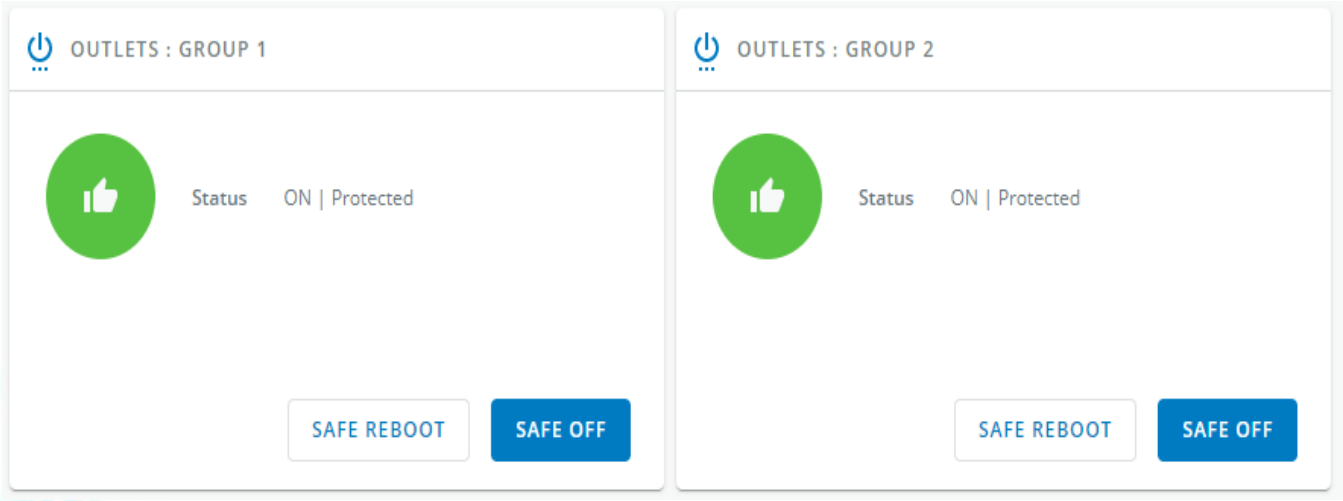
  これは、負荷をオンにするか、オンラインUPSをオンにします。

  この制御は、ステータスが OFF のとき、アクティブなコマンドが実行されていないとき、およびオンライン UPS がバイパスにあるときに利用可能です。.

3.4.1.3 保留中のアクション

シャットダウン前の待機時間と起動前の待機時間を表示します。

3.4.2 出力 – グループ1/グループ2



ロードセグメンテーションにより、バッテリーのランタイムを必要な機器に残し、長時間の停電時には優先度の低い機器を自動的にパワーダウンさせることができます。

この機能は、突入電流を制限するためのリモート再起動やサーバーの順次起動にも使用されます。

3.4.2.1 ステータス

現在のコンセントの状態を反映しています。

- On ー保護されている/保護されていない
- Off ー電源が入っていない

3.4.2.2 コマンド

以下のいずれかのボタンを押すと、一連のコマンドが使用可能になり、有効になります。確認画面が表示されます。

- **Safe OFF**

  これにより、関連する負荷セグメントに接続された負荷がシャットオフされます。保護されたアプリケーションは安全にパワーダウンされます。この制御は、ステータスが OFF ではなく、アクティブなコマンドが実行されていない場合にのみ使用できます。

- **Safe reboot**

  これにより、パワーダウンしてから、関連する負荷セグメントに接続された負荷をオンにします。保護されたアプリケーションは安全にパワーダウンします。

この制御は、ステータスが OFF ではなく、アクティブなコマンドが実行されていない場合にのみ有効です。.

- **Switch ON**

  関連する負荷セグメントに接続されている負荷をオンに切り替えます。

  この制御は、ステータスが OFF のとき、およびアクティブなコマンドが実行されていない場合に使用できます。

3.4.2.3 保留中のアクション

シャットダウン前の待機時間と起動前の待機時間を表示します。

3.4.3 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Control	✓	✓	✗

3.4.3.1 その他のアクセス権について

その他の設定については次を参照: Information>>>Access rights per profiles

3.4.4 トラブルシューティング

制御/スケジュール/停電ポリシーで許可されていないアクション

症状

以下のメッセージは、制御、スケジュール、または停電ポリシーページにアクセスしたときに表示されます。

このアクションは UPS によって許可されていません。

有効にするには、UPS のユーザーマニュアルと、UPS の設定を設定し、リモートコマンドを許可する方法についての説明書を参照してください。

考えられる原因

1- UPS の構成によりリモートコマンドが許可されていません（以下のアクションを参照してください）

2- 2- UPS はリモートコマンドをサポートしていません。

アクション

UPS の設定やリモートコマンドを許可する方法については、UPS のユーザーマニュアルとその説明書を参照してください。Example: UPS menu Settings>>>ON/OFF settings>>>Remote command>>>Enable.

3.4.4.1 その他の問題について

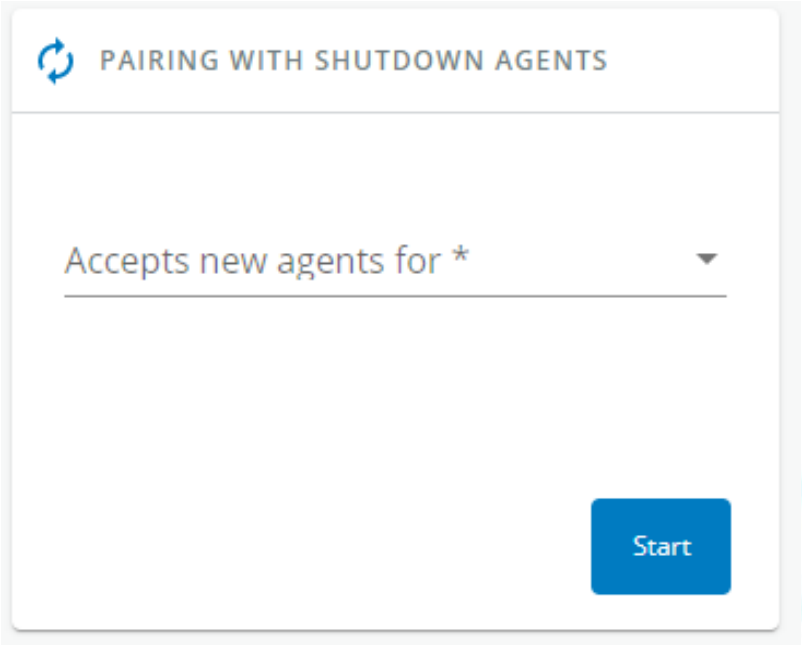
その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.5 保護

3.5.1 エージェント一覧

3.5.1.1 シャットダウンエージェントとのペアリング

ペアリング手順の詳細についてはタイル内のリンクペアリング手順に従うか次のセクションを参照してください。Servicing the Network Management Module>>>*Pairing agent to the Network Module*



UPS ネットワークモジュールとシャットダウンエージェント間の接続の認証と暗号化は、一致する証明書に基づいています。シャットダウンエージェントとUPSネットワークモジュールの自動ペアリングは、インストールが安全で信頼できるネットワークにおいて手動で行われる場合や、他の方法で証明書を作成できない場合に推奨されます。

選択した時間枠の間、ネットワークモジュールへの新しいエージェント接続は自動的に信頼され、受け入れられます。

自動受諾後、リストされたすべてのエージェントがインフラストラクチャに属していることを確認してください。そうでない場合、アクセスは**[Delete(削除)]**ボタンを使用して取り消されるかもしれません。

最大のセキュリティのために、イートンは**証明書設定**ページの2つの方法のうちの1つに従うことを推奨します。:

- クライアント証明書を手動でインポートする。
- クライアント証明書を手動でインポートする: クライアント証明書を手動でインポートする。

3.5.1.1.1 アクション

a Start

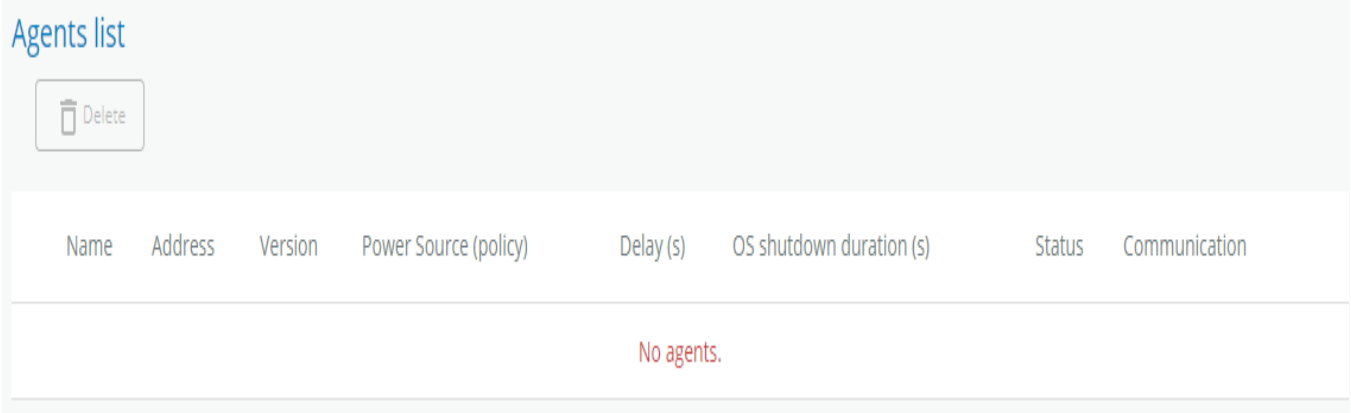
選択した時間枠、または停止するまでペアリングウィンドウを起動します。

タイムカウントダウンを表示します。

b Stop

ペアリングウィンドウを停止します。

3.5.1.2 エージェント一覧表



表には、ネットワークモジュールに接続されているIPPエージェントリストが表示され、以下の詳細が含まれています。:

- Name
- Address
- Version of the Agent
- Power source (Policy)
- Delay (in seconds)
- OS shutdown duration (in seconds)
- Status
  - In service | Protected
  - In service | Not protected
  - Stopping | Protected
  - Stopped | Protected
- Communication
  - Connected | yyyy/mm/dd hh:mm:ss
  - Lost | yyyy/mm/dd hh:mm:ss

3.5.1.3 アクション

3.5.1.3.1 削除

エージェントが接続されている場合、エージェントが再接続を試み続けるため、削除機能が正常に動作しません。そのため、ソフトウェアに接続し、ソフトウェアのノードリストからネットワークモジュールを削除してください（ノードリストでネットワークモジュールを右クリックし、**ノードの削除**をクリックしてください）。.

エージェントとの通信が途絶えた場合、**[Delete（削除）]**ボタンを使用してエージェントを削除することができます。

エージェントを選択して**[Delete（削除）]**ボタンを押すと、エージェントが削除されます。.

3.5.1.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Protection/Agent list	✓	✓	✗

3.5.1.4.1 その他のアクセス権について

その他の設定については次を参照: Information>>>Access rights per profiles

3.5.1.5 トラブルシューティング

カードのタイムスタンプが間違っていると、ソフトウェア上で「完全な取得に失敗しました」というエラーメッセージが表示されます。

症状:
IPP/IPMでは、資格情報が正しくても「完全なデータ取得に失敗しました」というエラーメッセージが表示されます。

考えられる原因:
ネットワークモジュールのタイムスタンプが正しくありません。
おそらく、MQTT証明書がネットワークモジュールの日付では有効ではありません。

アクション:

正しい日付、時刻、タイムゾーンを設定します。可能であれば、NTPサーバーを使用してください。

Contextual help>>>Settings>>>General>>>System details>>>Time & date settings

ソフトウェアがネットワークモジュールと通信できない

症状

- ネットワークモジュールで、Contextual help>>>Protection>>>Agent list>>>Agent list table エージェントのステータスが **"Lost "**と表示されます。
- ネットワークモジュールで、Contextual help>>>Settings>>>Certificate>>>Trusted remote certificates , 保護されたアプリケーション(MQTT)のステータスが**「まだ有効ではありません」**と表示されます。
- IPP/IPMでは、"認証に失敗しました"、"通知受信でエラーが発生しました "と表示されています。

考えられる原因

IPP/IPMとネットワークモジュールの証明書が一致していないため、ネットワークモジュールとシャットダウンエージェント間の接続の認証と暗号化が機能しません。

セットアップ

IPP/IPM が起動します。

ネットワークモジュールがUPSに接続され、ネットワークに接続されます。

アクション #1

ネットワークモジュールのIPP/IPM証明書の有効性を確認します。

STEP 1: ネットワークモジュールに接続する

- ネットワークコンピューターで、サポートされているWebブラウザを起動します。
- ブラウザウィンドウが表示されます。
- Address/Location フィールドに、https://xxx.xxx.xxx.xxx/ と入力します。
- xxx.xxx.xxx.xxx はネットワークモジュールのスタティック IP アドレスです。
- ログイン画面が表示されます。
- User Name(ユーザー名)フィールドにユーザー名を入力します。
- Password(パスワード)フィールドにパスワードを入力します。
- **Login** をクリックします。Network Module Web インターフェースが表示されます。

STEP 2: Settings/Certificates ページに移動

STEP 3: 信頼されたリモート証明書セクションでは、**保護されたアプリケーション(MQTT)**のステータスを

確認してください。それが **"有効 "**である場合は、Action#2 STEP 2に進み、それが **"まだ有効ではない "**場合は、

IPP/IPMと同期する必要がある時間 。

STEP 4: ネットワークモジュールの時刻をIPP/IPMと同期させ、**保護されたアプリケーション(MQTT)**のステータスが有効になったことを確認します。

通信はその後、Action#2 STEP 2に行かない場合は、回復します。

アクション #2

ネットワークモジュールにエージェントを自動受付けでペアリングします(安全で信頼できるネットワークにインストールする場合にお勧めします)。

> 手動ペアリング(最大のセキュリティ)を行う場合はServicing the Network Management Module>>>Pairing agent to the Network Module に進み、STEP 2, item 1.に進みます。

STEP 1: ネットワークモジュールに接続します。

- ワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。
- Address/Location フィールドに、https://xxx.xxx.xxx.xxx/ と入力します。
  xxx.xxx.xxx.xxx はネットワークモジュールのスタティック IP アドレスです。
- ログイン画面が表示されます。
- User Name(ユーザー名)フィールドにユーザー名を入力します。
- Password(パスワード)フィールドにパスワードを入力します。

- **ログイン**をクリックします。Network Module Web インターフェースが表示されます。

STEP 2: Protection/Agents list ページに移動してください。

STEP 3: シャットダウンエージェントとのペアリングセクションで、新しいエージェントを受け入れる時間を選択し、**[Start(スタート)]** ボタンを押して **[Continue]** を押します。選択した時間枠の間、ネットワークモジュールへの新しいエージェント接続は自動的に信頼され、受け入れられます。

STEP 4: 新しいエージェントを受け入れる時間がネットワークモジュール上で実行されている間、**エージェント(IPP/IPM)に対するアクション**フォルダ内にあるネットワークモジュール証明書ファイル*.0を削除します。
Eaton¥IntelligentPowerProtector¥configs¥tls.

クライアントサーバーが再起動しない

症状

ユーティリティの電源が復旧し、UPS とその負荷セグメントに電源が入っていますが、クライアントサーバーが再起動しません。.

考えられる原因

サーバー設定の「自動電源投入」が無効になっている場合があります。

アクション

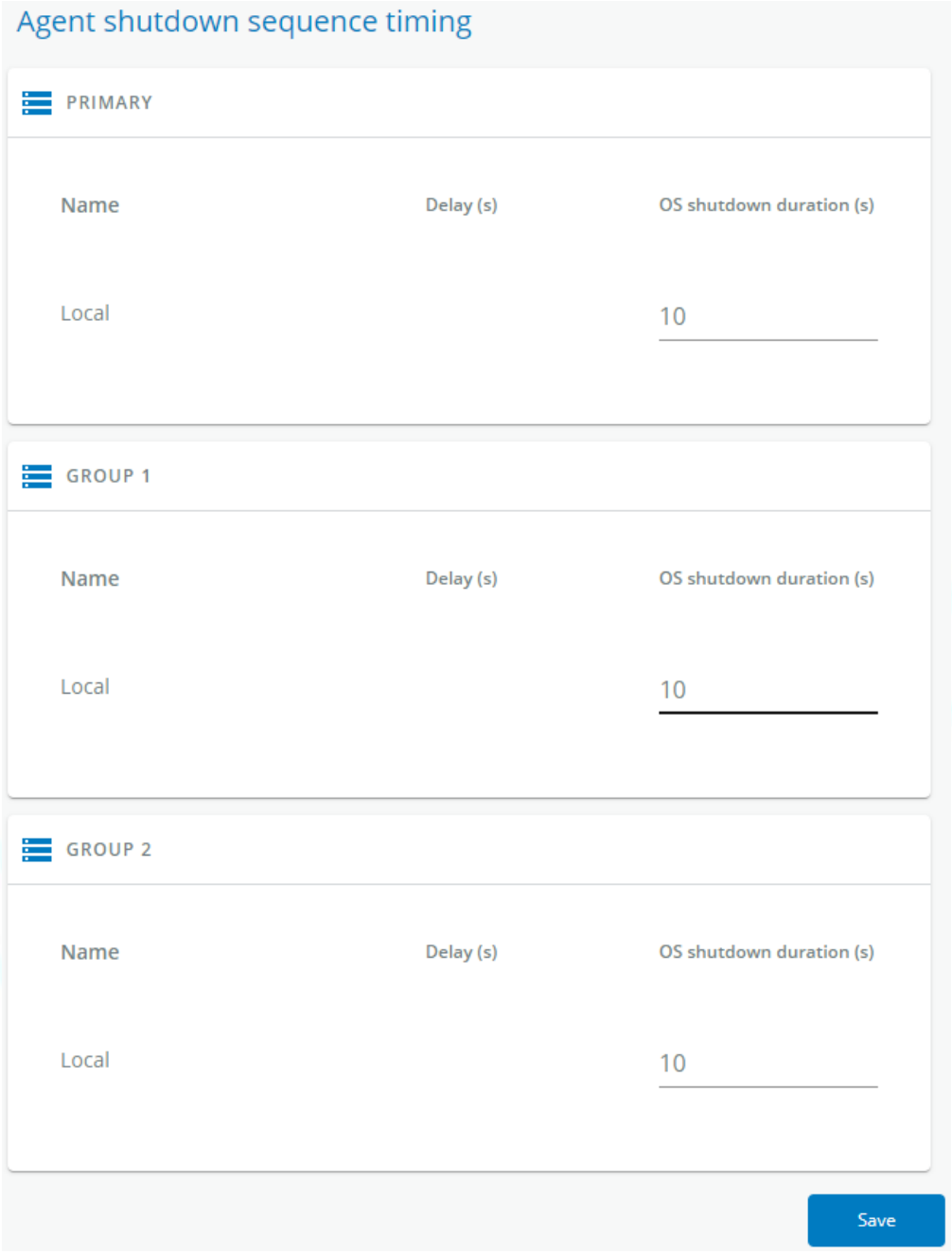
サーバーシステムのBIOSで、自動電源投入の設定を ″Enabled ″に変更します。

3.5.1.5.1 その他の問題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。.

3.5.2 エージェントのシャットダウンシーケンス

3.5.2.1 エージェントシャットダウンシーケンスタイミング



ネットワークモジュールに接続されているすべてのエージェントは、電源別の表に表示されます。..

- Primary
- Group 1
- Group 2

「ローカルエージェント」設定は、シャットダウンエージェントが登録されていない負荷セグメントの最小シャットダウン時間やパワーダウンの遅延時間などを設定するために使用されます。
たとえば、サーバーとストレージが整然とシャットダウンを実行している間、ネットワーク機器に電源を供給する負荷セグメントがあります。
表には、以下の詳細が含まれています。

- Name
- Delay (in seconds)
- OS shutdown duration (in seconds)

3.5.2.2 アクション

3.5.2.2.1 遅延設定

テーブル内の設定を選択して直接変更し、保存する.

3.5.2.2.2 OSのシャットダウン時間の設定

テーブル内の設定を選択して直接変更し、保存する

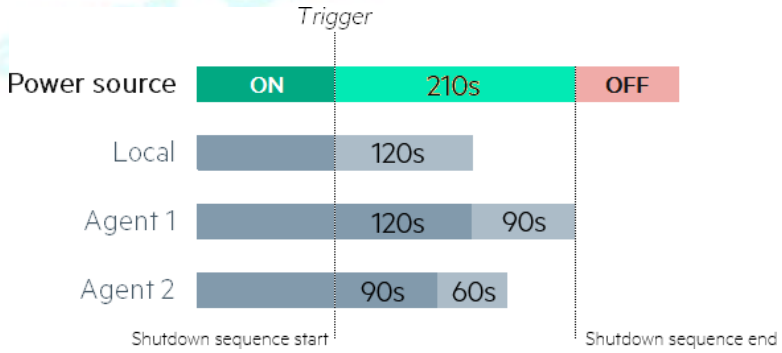
3.5.2.3 例

以下の例は、シャットダウンまたは即時シャットダウンのシャットダウンシーケンスに対するエージェント設定の影響を示しています。

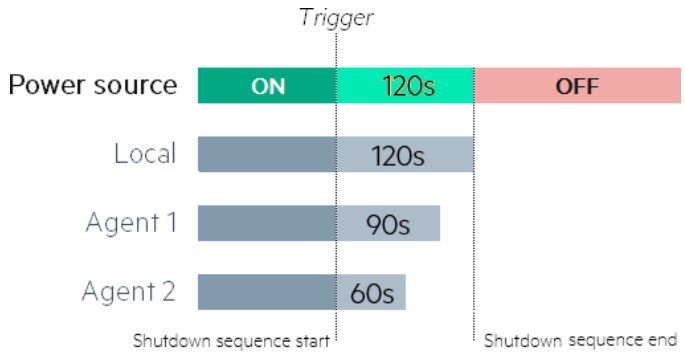
3.5.2.3.1 例 #1

Name	Delay (s)	OS shutdown duration (s)
Local		120
Agent #1	120	90
Agent #2	90	60

→ シャットダウン時間: 210s



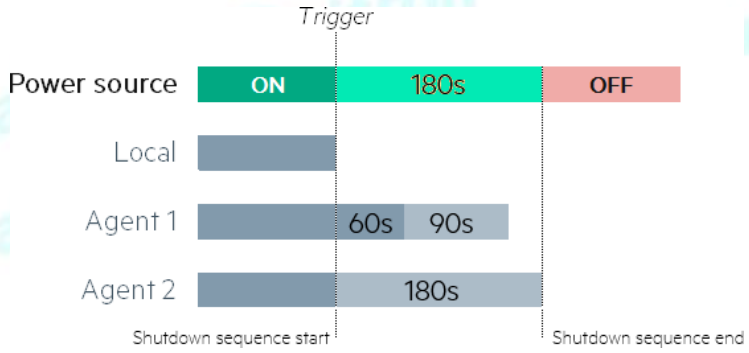
→ 即時シャットダウン時間: 120s



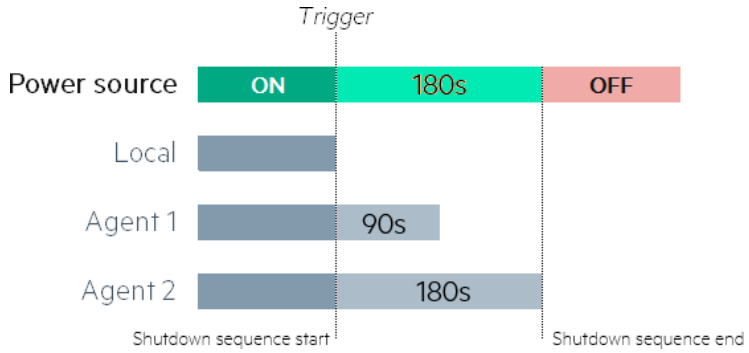
3.5.2.3.2 例 #2

Name	Delay (s)	OS shutdown duration (s)
Local		0
Agent #x	60	90
Agent #x	0	180

→ シャットダウン時間: 180s



→ 即時シャットダウン時間: 180s



図中のトリガーは、シャットダウンシーケンスが開始される瞬間であり、下記で定義されています。Contextual help>>>Protection>>>Scheduled shutdown or the Contextual help>>>Protection>>>Shutdown on power outage sections for each power source.

3.5.2.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Protection/Agent settings	✓	✓	✗

3.5.2.4.1 その他のアクセス権について

その他のアクセス権については次を参照：Information>>>Access rights per profiles

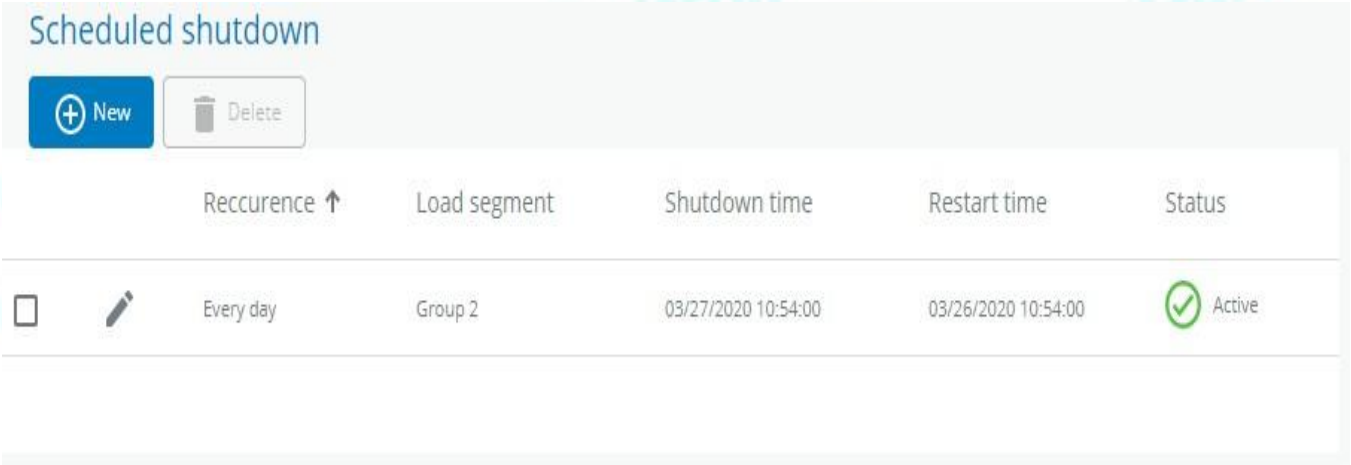
3.5.3 スケジュールされたシャットダウン

スケジュールされたシャットダウンを使用して、特定の日と時間にUPSまたは個々の負荷セグメントのいずれかをオフにします。

この機能は、営業時間外に機器の電源を切ることでエネルギーを節約したり、ネットワーク機器の電源を切ることでサイバーセキュリティを強化したりするために使用されます。

接続されているサーバーまたはアプライアンスのいずれかに対してサーバーのシャットダウンシナリオが定義されている場合、シャットダウン設定で構成されているように、対応するコンセントがオフになる前にトリガーされます。.

3.5.3.1 スケジュールされたシャットダウンテーブル



このテーブルには、スケジュールされたシャットダウンが表示され、以下の詳細が含まれています。:

- **Recurrence** – Once/Every day/Every week
- **Load segment** – Primary/Group 1/Group 2
- **Shutdown time** – Date/Time
- **Restart time** – Date/Time
- **Active** – Yes/No

3.5.3.2 アクション

3.5.3.2.1 新規

[New] ボタンを押して、スケジュールされたシャットダウンを作成します。

3.5.3.2.2 削除

スケジュールのシャットダウンを選択し、[Delete（削除）] ボタンを押して、スケジュールされたシャットダウンを削除します。.

3.5.3.2.3 編集

ペンのアイコンを押してスケジュールのシャットダウンを編集し、設定にアクセスします。:

3.5.3.3 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Protection/Scheduled shutdowns	✓	✓	✗

3.5.3.3.1 その他のアクセス権について

その他のアクセス権については次を参照
Information>>>Access rights per profiles

3.5.3.4 トラブルシューティング

制御/スケジュール/停電ポリシーで許可されていないアクション

症状

以下のメッセージは、制御、スケジュール、または停電ポリシーページにアクセスしたときに表示されます。

このアクションは UPS によって許可されていません。

有効にするには、UPS のユーザーマニュアルと、UPS の設定を構成し、リモートコマンドを許可する方法についての説明書を参照してください。

考えられる原因

1- UPS の構成によりリモートコマンドが許可されていません（以下のアクションを参照してください）

2- UPS はリモートコマンドをサポートしていません。

アクション

UPS の設定やリモートコマンドを許可する方法については、UPS のユーザーマニュアルとその説明書を参照してください。例）: UPS menu Settings>>>ON/OFF settings>>>Remote command>>>Enable

3.5.3.4.1 その他の問題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

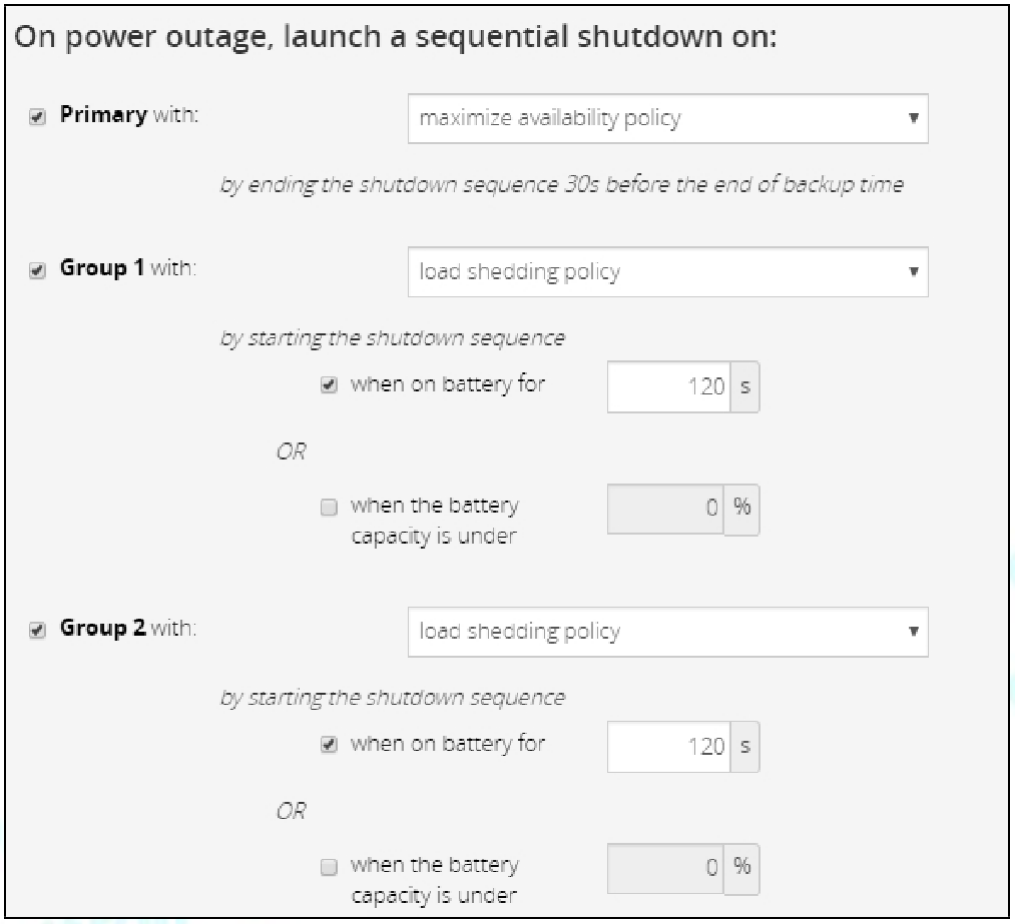
3.5.4 停電時のシャットダウン

これらの設定は、シャットダウンエージェントと連動しており、ネットワークモジュールが保護されたサーバーやアプライアンスのシャットダウンをどのように指示するかを制御します。これにより、ITシステムが正しい順序でパワーダウンするように、シャットダウンアクションに優先順位をつけてスケジュールを組むことができます。

例えば、アプリケーションを最初に、データベースサーバーを次に、ストレージを最後に、というように。また、いくつかのコンセントをオフにして消費電力を減らし、最も重要なデバイスのバッテリー駆動時間を長くすることも可能です。

アプリケーションのパワーダウンの例については、次を参照してください。
Servicing the Network Management Module>>>Powering down/up applications examples

3.5.4.1 停電基準でシャットダウン



シャットダウン基準は、UPS に存在する場合、電源（コンセントグループ）ごとに設定されます。

デフォルトでは、シャットダウンの基準は、可用性を最大化するように設定されています。

3.5.4.1.1 シャットダウン基準の選択

シャットダウンのために利用可能な基準は以下の通りです。:

a 可用性を最大にする（デフォルト）

バックアップ時間の終了30秒前にシャットダウンシーケンスを終了する。

b 即時オフ

バッテリー残量が 10 秒のときにシャットダウンシーケンスを開始します。

c カスタム

シャットダウンの基準を定義するために、いくつかの条件を設定することができます。:

- シャットダウンシーケンスを開始するには、バッテリーが10秒間使用されている場合に開始します。

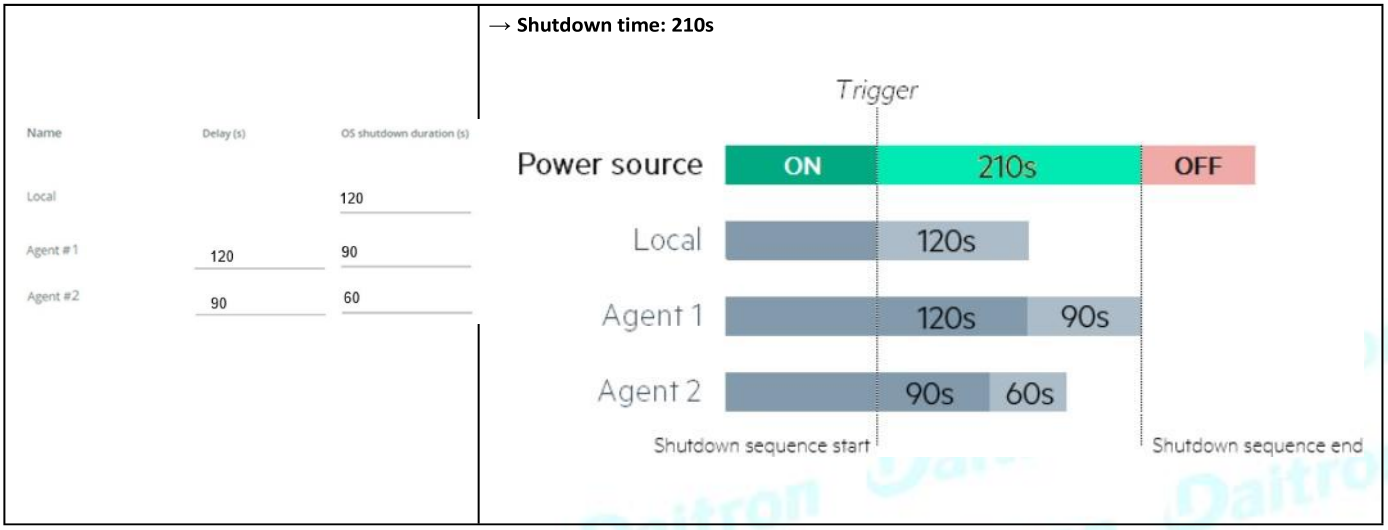
- 電池が設定容量（%）に達したときにシーケンスを開始する。
- バックアップ時間終了前の（s）で設定した時間後にシャットダウンシーケンスを開始または終了する。

シャットダウンシーケンスを開始する条件が複数ある場合、いずれかの条件に達した時点でシャットダウンシーケンスを開始します。

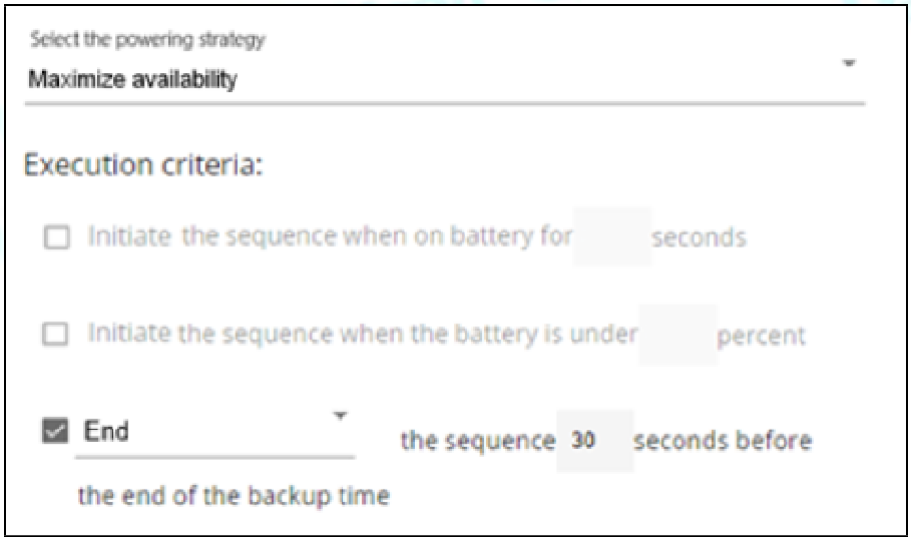
Primaryがシャットダウンすると、グループ1もグループ2もすぐにシャットダウンします。そのため、
Primaryが即時オフに設定されている場合は、グループポリシーを即時オフに制限する必要があります。

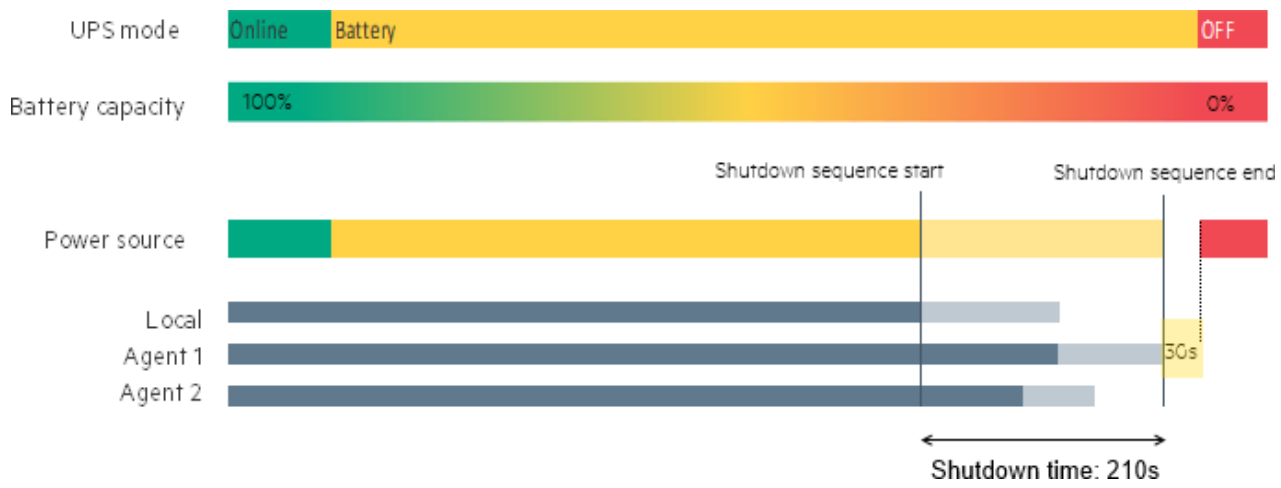
d 設定例

以下の例では、下記のエージェントの設定を使用しています。.

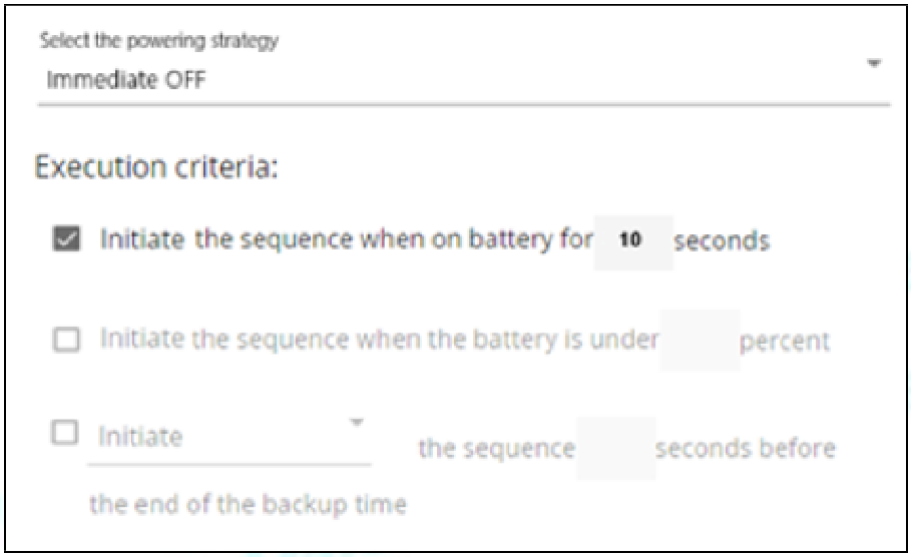


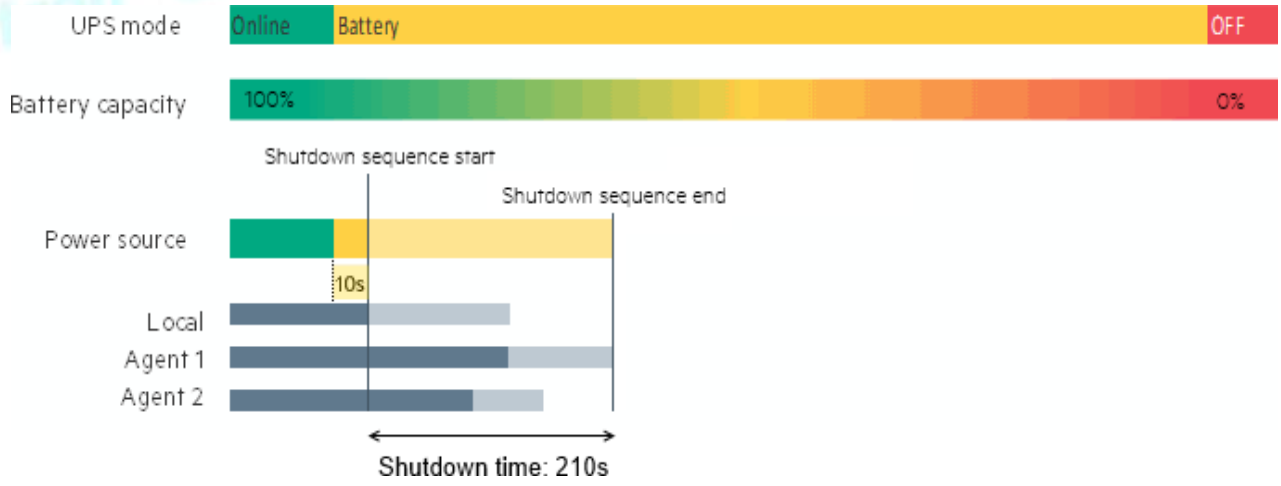
例 1: 可用性を最大にする



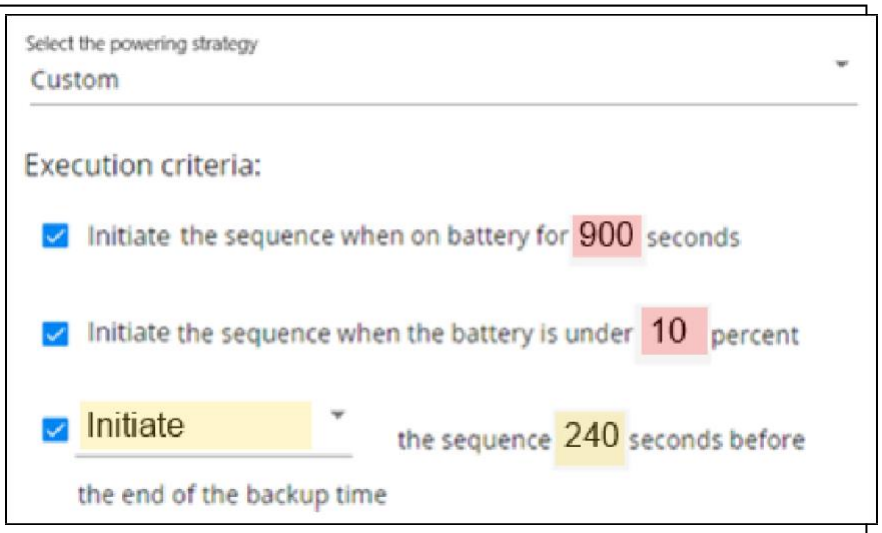
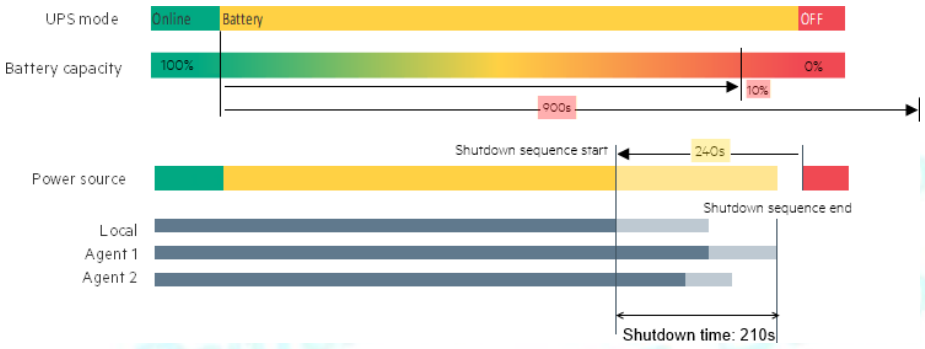


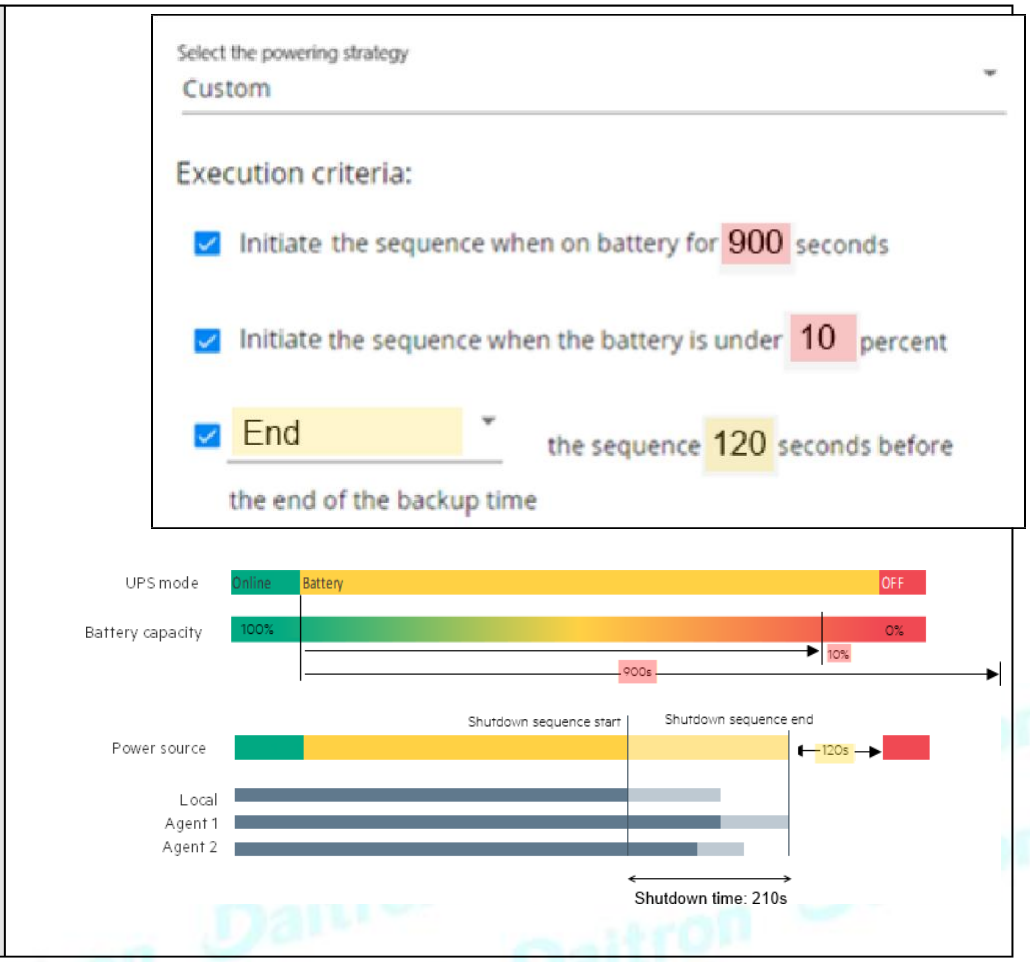
例 2:即時オフ



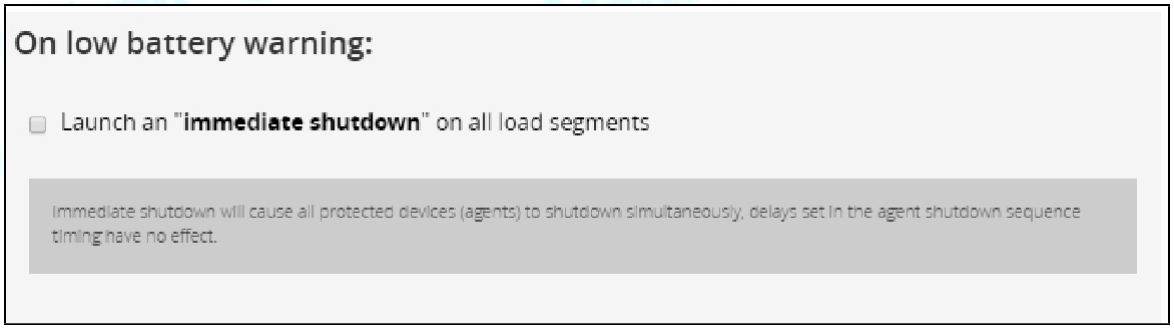


例3: カスタム

Settings #1	 

Settings #2	

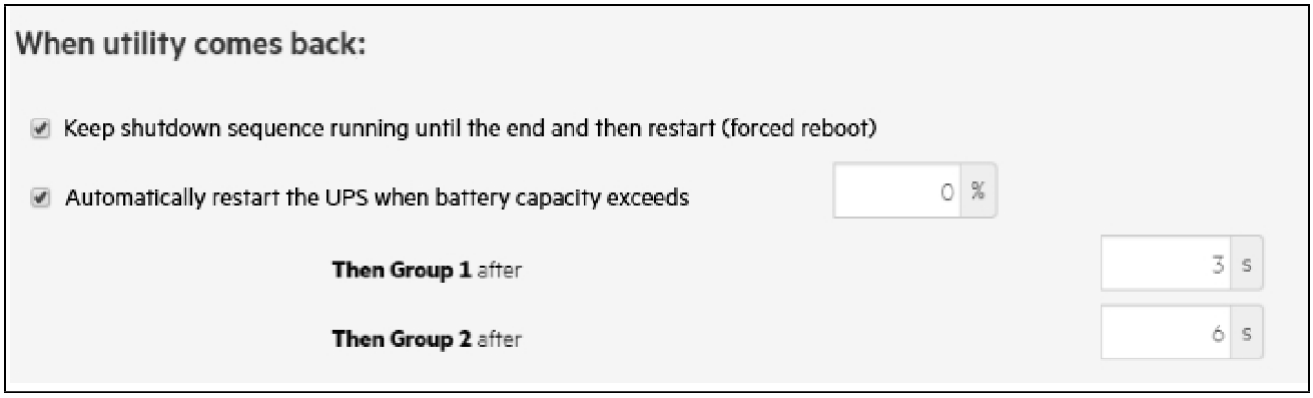
3.5.4.1.2 ローバッテリー警告で



場合によっては、更新された電源障害や故障したバッテリーのように、容量が予想よりもはるかに低いことがあります。
UPSは、UPSとその設定に応じて、推定ランタイムが2～3分残っている場合に、バッテリー低下の警告を表示します。
この時間は通常、サーバーをシャットダウンするのに十分な時間ですが、洗練されたシーケンシャル・シャットダウン・スキームを許可しません。

ローバッテリーポリシーは、このような場合を想定しています。

3.5.4.1.3 ユーティリティが戻ってくるとき



これらの設定は、ユーティリティが復帰したときの再起動シーケンスを定義します。例えば、これにより、ネットワークやストレージ機器が「プライマリ」に接続されてすぐに起動するように、ITシステムを順次起動することができます。遅延後、Group1 のデータベース サーバーがパワーアップし、Group2 のアプリケーション サーバーと Web サーバーがパワーアップします。このように起動することで、必要なサービスが必要なときに各レイヤーで利用できるようになる。順次起動することで、開始時の電力消費のピークを回避することができます。

a オプション

シャットダウンシーケンスを最後まで実行した後、再起動(強制再起動)してください。

UPS のバッテリー容量が(%)で設定したパーセンテージ値を超えるまで待ち、自動的に UPS を再起動します。

- その後、(s)で設定した時間後にグループ1を再起動します。
- その後、(s)で設定した時間後にグループ2を再起動します。

b 有効化/無効化

上記の各オプションは、チェックボックスで有効または無効にすることができ

ます。無効にすると、オプションはグレーアウトされます。

3.5.4.2 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
保護/シークエンス	✓	✓	✗

3.5.4.2.1 その他のアクセス権について

その他のアクセス権については次を確認してください。Information>>>Access rights per profiles

3.5.4.3 トラブルシューティング

制御/スケジュール/停電ポリシーで許可されていないアクション

症状

以下のメッセージは、制御、スケジュール、または停電ポリシーページにアクセスしたときに表示されます。このアクションは UPS によって許可されていません。有効にするには、UPS のユーザーマニュアルと、UPS の設定を構成し、リモートコマンドを許可する方法についての説明書を参照してください。

考えられる原因

1- UPS の構成によりリモートコマンドが許可されていません（以下のアクションを参照してください）2- UPS はリモートコマンドをサポートしていません。

アクション

UPS の設定やリモートコマンドを許可する方法については、UPS のユーザーマニュアルとその説明書を参照してください。Example: UPS menu Settings>>>ON/OFF settings>>>Remote command>>>Enable.

クライアントサーバーが再起動しない

症状

ユーティリティの電源が復旧し、UPS とその負荷セグメントの電源は入っていますが、クライアントサーバーが再起動しません。

考えられる原因

サーバー設定の「自動電源投入」が無効になっている場合があります。

アクション

サーバーシステムのBIOSで、自動電源投入の設定を「有効」に変更します。

3.5.4.3.1 その他の問題については

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。.

3.6 環境

3.6.1 試運転/ステータス

3.6.1.1 センサーの試運転/ステータステーブル

表には、センサーの試運転情報が表示され、以下の詳細が含まれています。

- **Name**
- **Location** – location-position-elevation
- **Temperature**
- **Humidity**
- **Dry contact #1** – Status and name
- **Dry contact #2** – Status and name
- **Communication** – Connected/Lost with dates

3.6.1.2 アクション

3.6.1.2.1 センサーメジャーのダウンロード

[Download sensors measures（センサー測定のダウンロード）] ボタンを押して、センサーログファイルをダウンロードします

利用可能な場合、可能な対策は以下の通りです。:

- Temperature of <sensor_1> (in K, 1 decimal digit)
- Humidity of <sensor_1> (in %, 1 decimal digit)
- Temperature of <sensor_2>> (in K, 1 decimal digit)
- Humidity of <sensor_2> (in %, 1 decimal digit)
- Temperature of <sensor_3> (in K, 1 decimal digit)
- Humidity of <sensor_3> (in %RH, 1 decimal digit)

°C = K - 273.15
°F = K x 9/5 -459.67

3.6.1.2.2 Discover

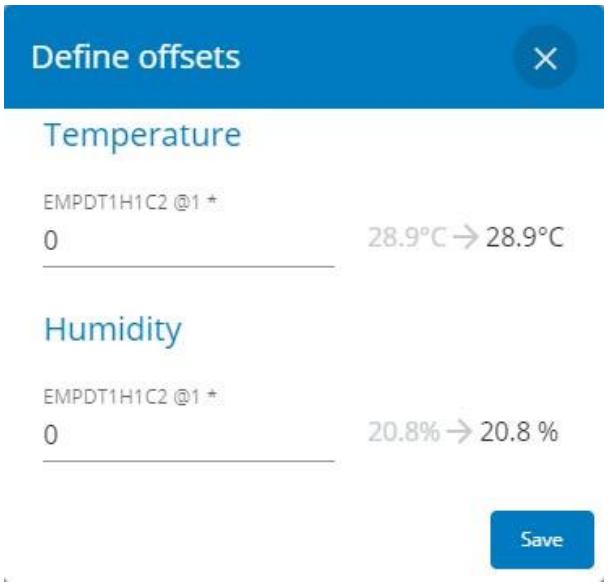
最初はテーブルが空の状態で、**[Discover（発見）]**ボタンを押してセンサー発見プロセスを開始します。センサーが発見されると、それに応じてテーブルが表示されます。

3.6.1.2.3 Delete

センサーを選択して**[Delete（削除）]**ボタンを押すとセンサーが削除されます。

センサーを削除すると、すべての試運転情報が削除されます。

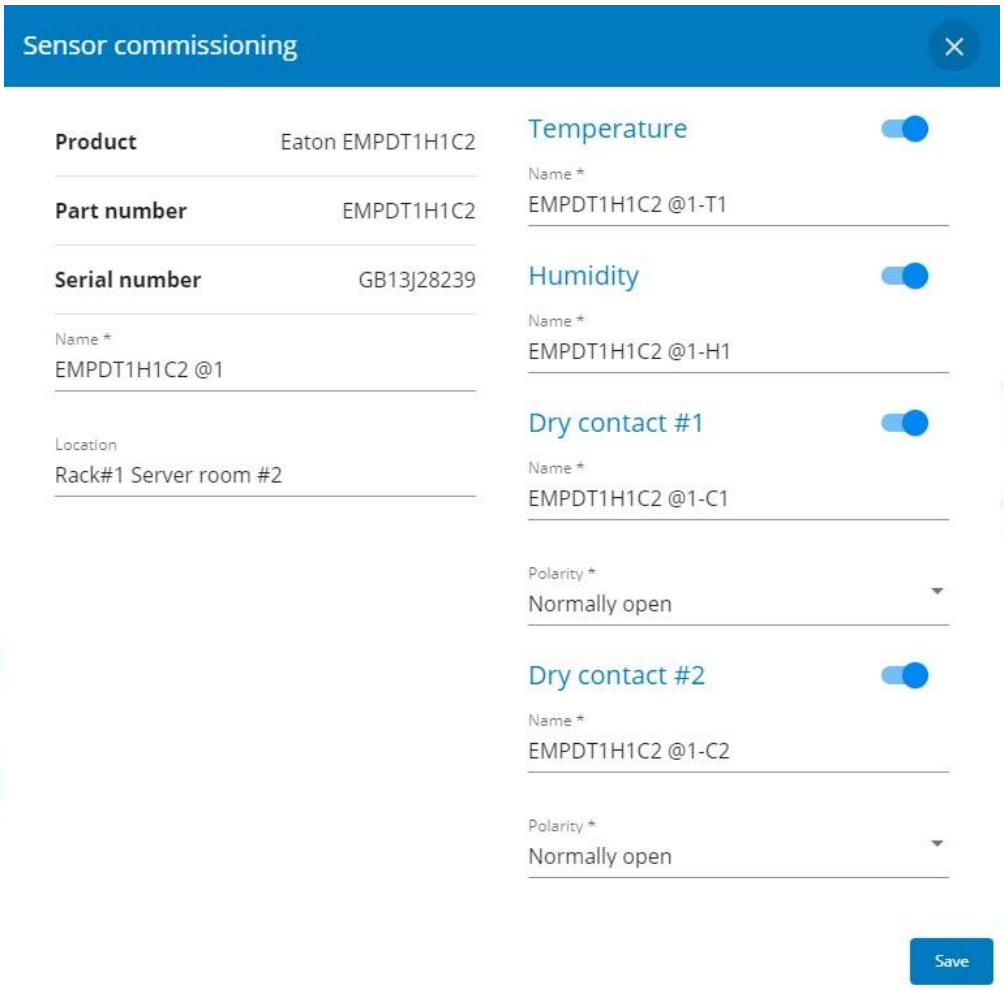
3.6.1.2.4 オフセットの定義



1. センサーを選択します。
2. **Define offset（オフセットの定義）**ボタンを押して、選択したセンサーの温度と湿度のオフセットを調整します。
3. 温度または湿度セクションを拡張します。
4. セル内のオフセットを設定すると、温度と湿度がそれに応じて更新されます。
5. 完了したら**保存**ボタンを押します。

非アクティブ化された湿度や温度は表示されず、このアイコンに置き換わります。

3.6.1.2.5 編集



ペンのロゴを押すと、センサー通信情報を編集することができます。

以下の情報と設定にアクセスすることができます。:

- Product reference
- Part number
- Serial number
- Name
- Location
- Temperature and humidity – Active (Yes, No)
- Dry contacts – Active (Yes, No)/Name/Polarity (Normally open, Normally closed)

	ドライコンタクトが閉じており、これはノーマルクローズとして構成されているため正常です。.
	ドライコンタクトは開いており、これは通常オープンとして構成されているため正常です。.
	ドライコンタクトが開いており、これは正常に閉じるように構成されているため、正常ではありません。.
	ドライコンタクトが閉じており、これはノーマルオープンとして構成されているため正常ではありません。

変更後に**保存**を押す.

非アクティブ化されたドライコンタクトは表示されず、
このアイコンに置き換えられます。:

3.6.1.3 Note:

UPS が温度補償付きバッテリー充電オプションを提供している場合は次を参照してください。
Servicing the EMP>>>Using the EMP for temperature compensated battery charging

3.6.1.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
環境/コミッショニング	✓	✓	✗
環境/ステータス	✓	✓	✓

3.6.1.4.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.6.1.5 トラブルシューティング

発見段階でEMP検出に失敗

ネットワークモジュールのContextual help>>>Environment>>>Commissioning/Statusで、センサーのコミッショニングテーブルにEMPがありません。

症状 #1

EMPsの緑のRJ45 LED(FROM DEVICE)が点灯していない。

考えられる原因

EMPはネットワークモジュールから電源が供給されていません。

アクション #1-1

それがまだOKでない場合は、アクション＃1-2に移動して、再度ディスカバリーを起動します。

アクション #1-2

1- EMPの接続とケーブルを確認してください。

セクションServicing the EMP>>>Installing the EMP>>>Cabling the first EMP to the device and Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs を参照してください。

2- USBからRS485ケーブルを取り外し、再接続します。

3- ディスカバリーを起動します。

アクション #1-3

1- ネットワーク モジュールを再起動します。2- ディスカバリーを起動します。

症状 #2

EMPのオレンジ色のRJ45 LEDが点滅しない。

考えられる原因

C#1: EMPアドレススイッチは全て0に設定されています。

C#2: EMPはデイジーチェーン接続されています。

アクション#2-1

1- 異なるアドレスを持つようにEMPのアドレスを変更し、すべてのスイッチを0にしないようにします。

Servicing the EMP>>>Defining EMPs address and termination>>>Manual addressingを参照してください。

2- USB-RS485ケーブルの接続を外し、再接続します。アドレスの変更は、EMP の電源投入後にのみ考慮されます。

3- ディスカバリーを起動します。

アクション #2-2

1- ネットワークモジュールを再起動します。

Contextual help>>>Maintenance>>>Services>>>Rebootの項を参照してください。.

2–ディスカバリーを起動する.

3.6.1.5.1 その他の問題について

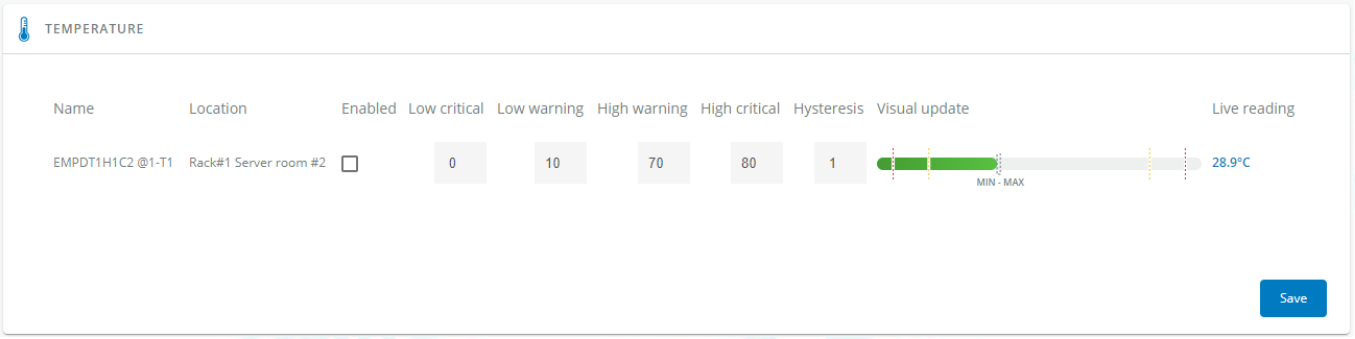
その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。.

3.6.2 アラーム設定

湿度、温度、または試運転中に無効化されたドライ接点は表示されません。
ゲージカラーコード:

- Green:しきい値内の値。
- Orange/Red:しきい値の外側の値。
- Grey:デバイスによって提供されるしきい値はありません。

3.6.2.1 温度



表は、各センサーの情報と設定を示しています。:

- Name
- Location
- Enabled – yes/no
- Low critical threshold – xx° C or xx° F
- Low warning threshold – xx° C or xx° F
- High warning threshold – xx° C or xx° F
- High critical threshold – xx° C or xx° F
- Hysteresis – x° C or x° F
- Visual update
- Live reading (MIN-MAX shows the minimal and maximal temperature measured by the sensor)

3.6.2.1.1 アクション

a 有効化する

表の設定を選択して直接変更し、**保存**します。

無効にした場合、アラームは送信されません

b アラームしきい値をセットする

最初にアラームを有効にしてから、表の設定を変更してから**保存**してください。

警告のしきい値に達すると、警告レベルでアラームが送信されます。

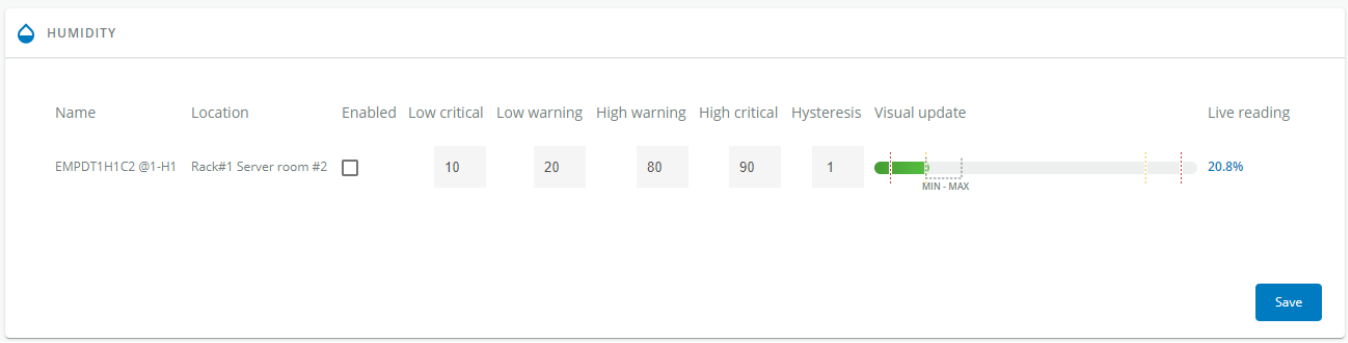
クリティカル閾値に達すると、クリティカルレベルでアラームが送信されます。

c ヒステリシスをセットする

最初にアラームを有効にして、表の設定を変更してから**保存**してください。

ヒステリシスとは、アラームがOFFになってからONになる値と、ONになってからOFFになる値の差です。

3.6.2.2 湿度



表は、各センサーの情報と設定を示しています。:

- Name
- Location
- Enabled – yes/no
- Low critical threshold – xx%
- Low warning threshold – xx%
- High warning threshold – xx%
- High critical threshold – xx%
- Hysteresis – x%
- Visual update
- Live reading (MIN–MAX shows the minimal and maximal humidity measured by the sensor)

3.6.2.2.1 アクション

a 有効化する

表の設定を選択して直接変更し、**保存**します。無効にした場合、

アラームは送信されません

b アラームしきい値をセットする

最初にアラームを有効にしてから、表の設定を変更してから**保存**してください。

警告のしきい値に達すると、警告レベルでアラームが送信されます。クリティカル

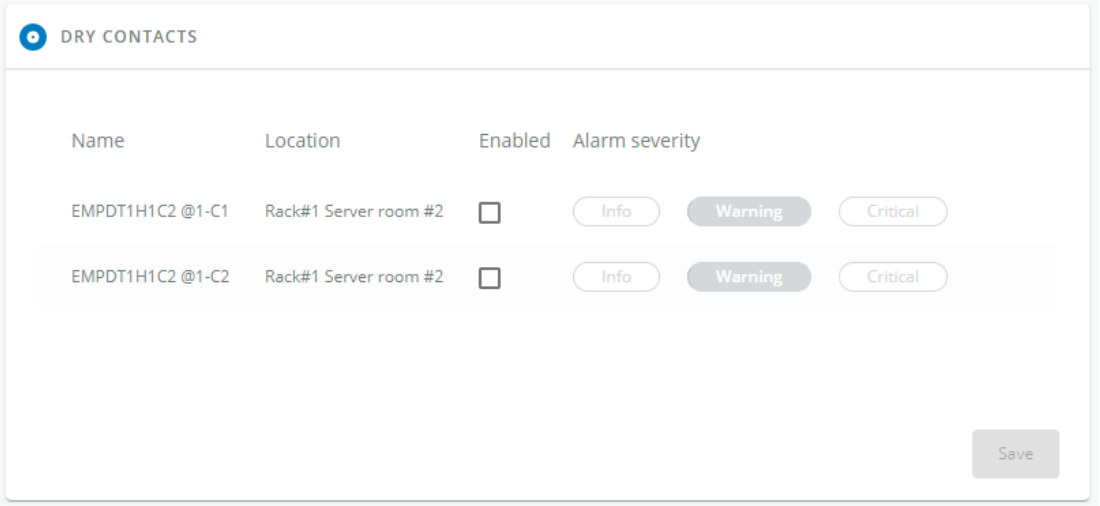
閾値に達すると、クリティカルレベルでアラームが送信されます。

c ヒステリシスをセットする

まずアラームを有効にしてから、表の設定を変更してから**保存**してください。

ヒステリシスは、アラームがOFFになってからONになる値と、ONになってからOFFになる値の差です

3.6.2.3 ドライコンタクト



表は、各ドライコンタクトの設定を示しています。:

- Name
- Location
- Enabled – yes/no
- Alarm severity – Info/Warning/Critical

3.6.2.3.1 アクション

a 有効化する

最初にアラームを有効にして、表の設定を変更してから**保存**してください。

無効にすると、アラームは送信されません。

b アラームの重要度を設定します。

最初にアラームを有効にしてから、表の設定を変更してから**保存**してください。

ドライ接点が正常な位置にない場合、選択したレベルでアラームが送信されます。

	ドライコンタクトが開いており、これは正常に閉じるように構成されているため、正常ではありません。
	ドライコンタクトが閉じており、これはノーマルオープンとして構成されているため正常ではありません。

3.6.2.4 デフォルト設定と可能なパラメーター –環境アラーム設定

	Default setting	Possible parameters

Temperature	Enabled – No Low critical – 0° C/32° F Low warning – 10° C/50° F High warning – 70° C/158° F High critical – 80° C/176° F	Enabled – No/Yes low critical<low warning<high warning<high critical
Humidity	Enabled – No Low critical – 10% Low warning – 20% High warning – 80% High critical – 90%	Enabled – No/Yes 0%<low critical<low warning<high warning<high critical<100%
Dry contacts	Enabled – No Alarm severity – Warning	Enabled – No/Yes Alarm severity – Info/Warning/Critical

3.6.2.4.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.6.2.5 プロファイルごとのアクセス権

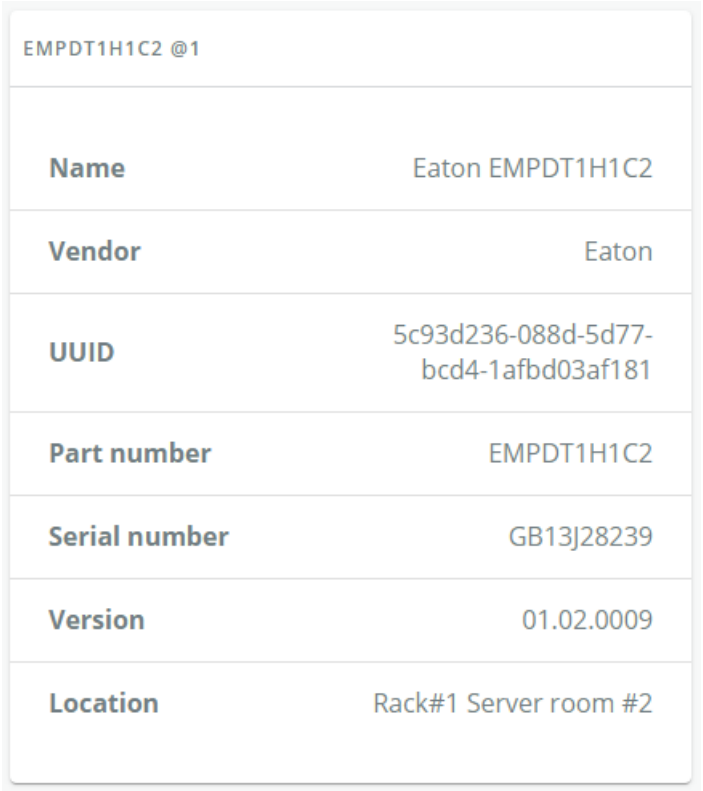
	Administrator	Operator	Viewer
Environment/Alarm configuration	✓	✓	✗

3.6.2.5.1その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.6.3 情報

センサー情報は、ネットワークモジュールに接続されている全てのセンサー情報の概要です。



- Physical name
- Vendor
- Part number
- Firmware version
- UUID
- Serial number
- Location

3.6.3.1 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Environment/Information	✓	✓	✓

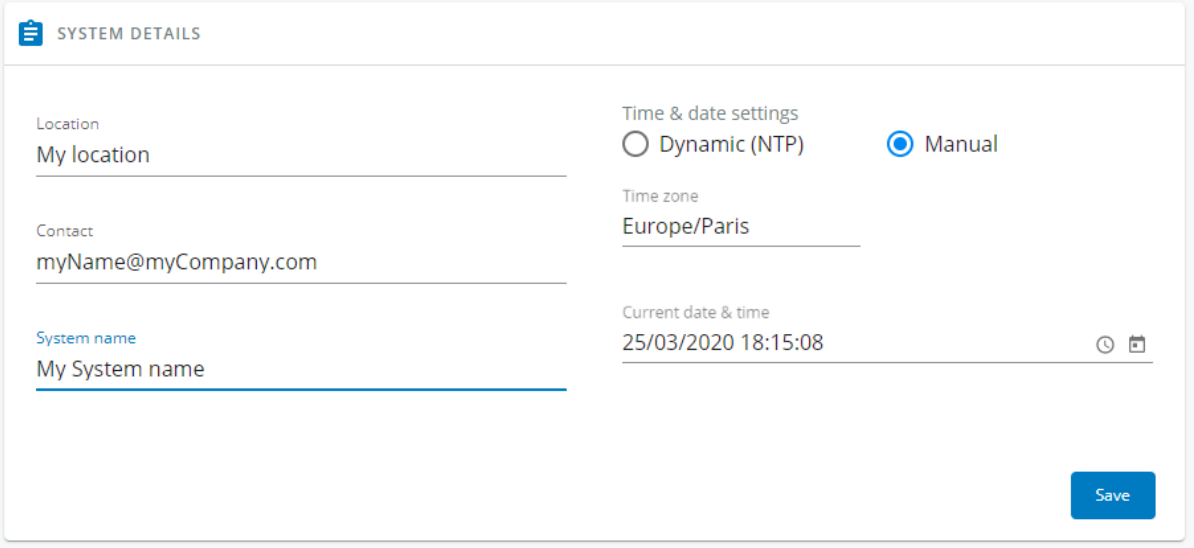
3.6.3.1.1その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7 設定

3.7.1 一般

3.7.1.1 システム詳細



3.7.1.1.1 ロケーション

カードの位置情報を提供するために使用されるテキストフィールド。カード
システム情報は、定義された場所を示すように更新される。

3.7.1.1.2 コンタクト

連絡先名の情報を提供するために使用されるテキストフィールド。カ
ードシステム情報は、連絡先名を示すように更新される。

3.7.1.1.3 システム名

システム名の情報を提供するためのテキストフィールド。カードシステ
ム情報は、システム名を表示するように更新されます。

3.7.1.1.4 日時設定

現在の日付と時刻は、画面下部のフッターに表示されます。時刻は、手動ま
たは自動で設定することができます。

a 手動：手動で日付と時刻を入力する

1. タイムゾーンのプルダウンメニューから、または地図を使って、お住まいの地域のタイムゾーンを選択します。
2. 日付と時刻を選択します。
3. 変更を保存します。

b ダイナミック（NTP）：日付と時刻を NTP サーバーと同期させます。

1. NTP サーバーの IP アドレスまたはホスト名を NTP サーバーフィールドに入力します。

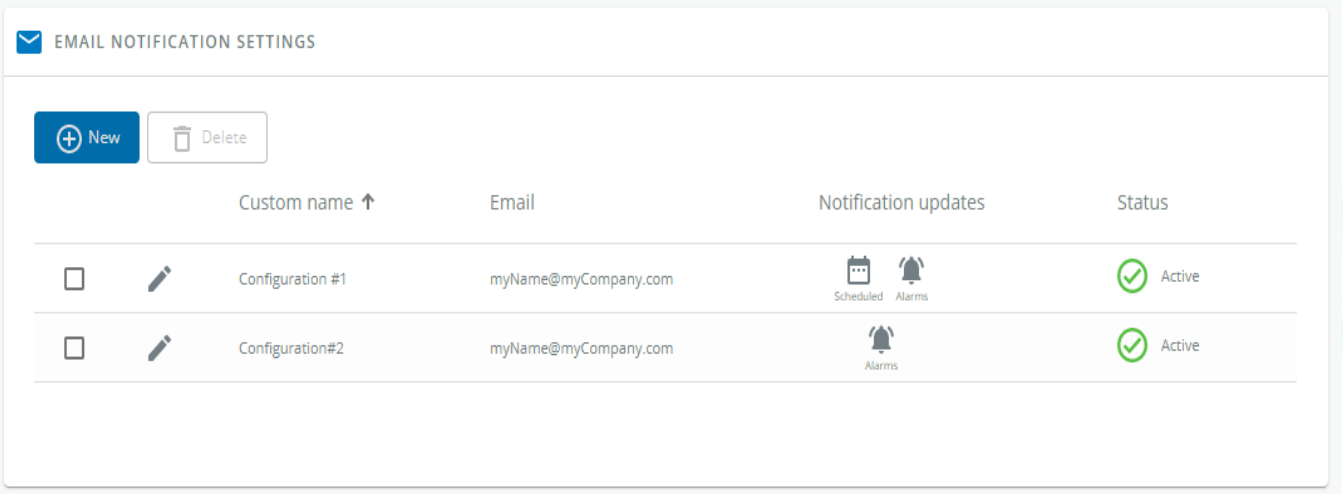
2. タイムゾーンのプルダウンメニューから、または地図を使って、お住まいの地域のタイムゾーンを選択します。

3. 変更を保存します。

DSTはタイムゾーンに基づいて管理されています。

3.7.1.2 メール通知の設定

メール送信設定の例については次を参照して下さい。
Servicing the Network Management Module>>>Subscribing to a set of alarms for email notification



3.7.1.2.1 電子メール送信設定表

この表は、すべてのメール送信設定を示しており、以下の詳細が含まれています。:

- **Configuration name**
- **Email address**
- **Notification updates** – Displays Events notification/Periodic report icons when active.
- **Status** – Active/Inactive/In delegation

3.7.1.2.2 アクション

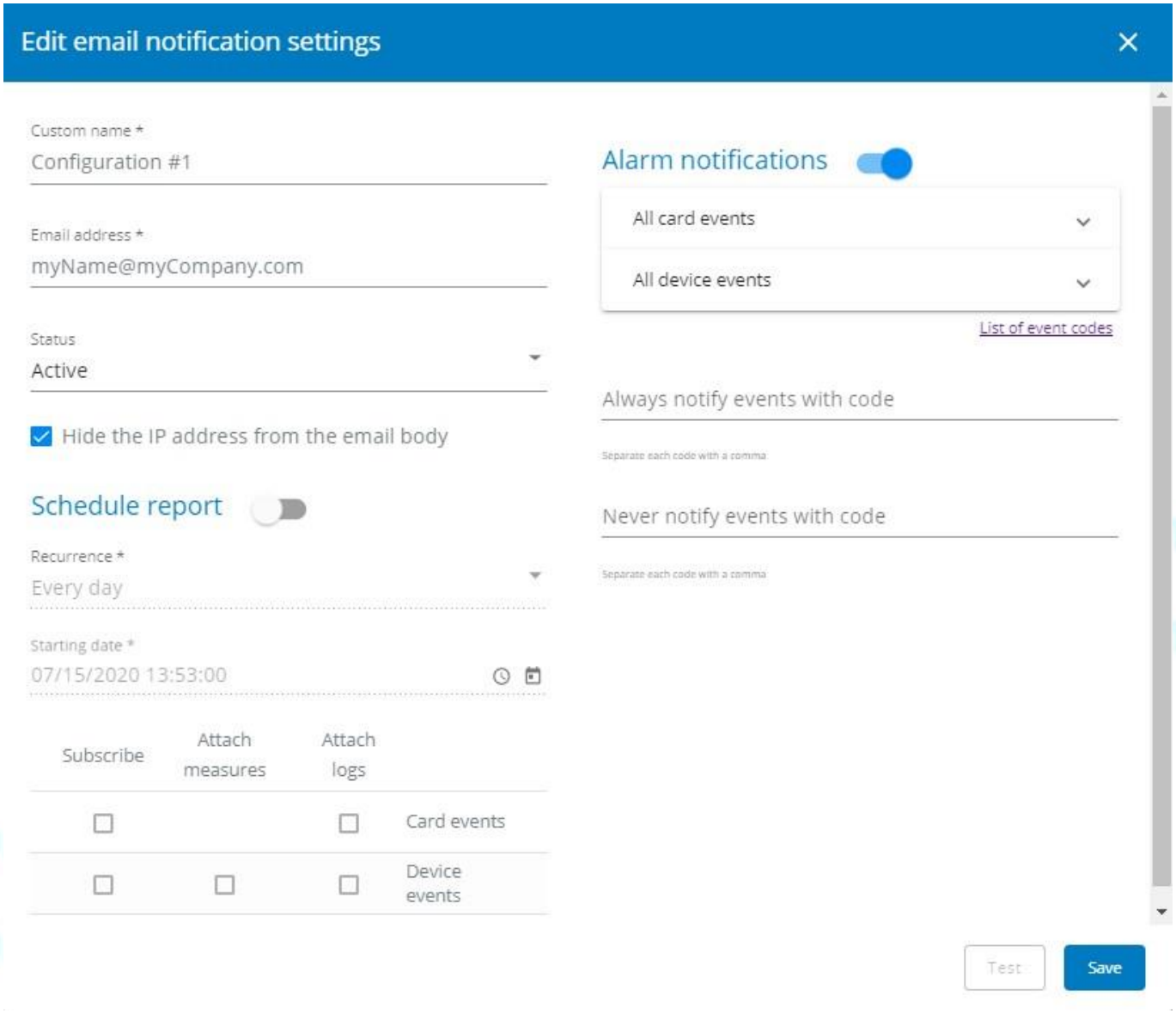
a 追加

新規作成ボタンを押して、新しいメール送信設定を作成します。.

b 削除

メール送信設定を選択し、**削除**ボタンを押して削除します。

c 編集

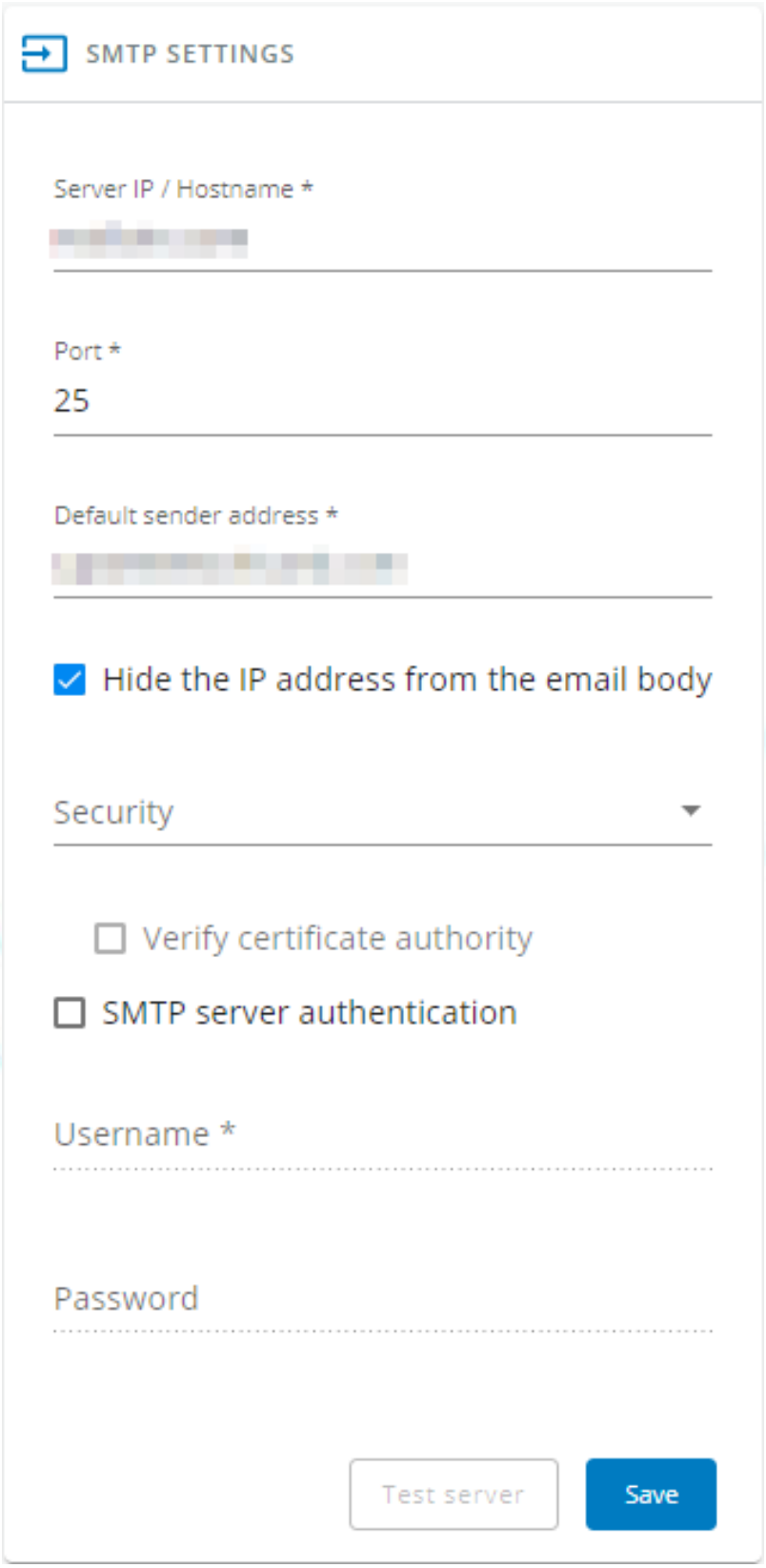


ペンのアイコンを押して、メール送信の設定を編集します。

次の設定にアクセスすることができます。:

- **Custom name**
- **Email address**
- **Status** – Active/Inactive
- **Hide the IP address from the email body** – Disabled/Enabled
  This setting will be forced to Enabled if Enabled in the SMTP settings.
- **Schedule report** – Active/Recurrence/Starting/Topic selection – Card/Devices
- **Alarm notifications** – Severity level/Attach logs/Exceptions on events notification

3.7.1.3 SMTP設定



SMTPとは、電子メールを送信するためのインターネット標準で
す。以下のSMTP設定が可能です。:

- **Server IP/Hostname** – Enter the host name or IP address of the SMTP server used to transfer email messages in the SMTP Server field.
- **Port**
- **Default sender address**
- **Hide the IP address from the email body** – Disabled/Enabled
  If Enabled, it will force this setting to Enabled in the Email notification settings.
- **Secure SMTP connection** – Verify certificate authority
- **SMTP server authentication** – Username/Password

SNMP認証にユーザー名とパスワードを必要とするSMTPサーバー認証チェックボックスを選択し、ユーザー名とパスワードを入力します。.

- Save and test server configuration

3.7.1.4 デフォルト設定と可能なパラメーター –一般

	Default setting	Possible parameters
System details	Location — empty Contact — empty System name — empty Time & date settings — Manual (Time zone: Europe/Paris)	Location — 31 characters maximum Contact — 255 characters maximum System name — 255 characters maximum Time & date settings — Manual (Time zone: selection on map/Date) / Dynamic (NTP)

Email notification settings	No email	5 configurations maximum Custom name — 128 characters maximum Email address — 128 characters maximum Hide IP address from the email body — enable/disabled Status — Active/Inactive • Alarm notifications Active — No/Yes All card events – Subscribe/Attach logs Critical alarm – Subscribe/Attach logs Warning alarm – Subscribe/Attach logs Info alarm – Subscribe/Attach logs All device events – Subscribe/Attach measures /Attach logs Critical alarm – Subscribe/Attach measures/ Attach logs Warning alarm – Subscribe/Attach measures/ Attach logs Info alarm – Subscribe/Attach measures/ Attach logs Always notify events with code Never notify events with code • Schedule report Active — No/Yes Recurrence – Every day/Every week/Every month Starting – Date and time Card events – Subscribe/Attach logs Device events – Subscribe/Attach measures/ Attach logs
SMTP settings	Server IP/Hostname — blank SMTP server authentication — disabled Port — 25 Default sender address — *device*@networkcard.com Hide IP address from the email body — disabled Secure SMTP connection — enabled Verify certificate authority — disabled SMTP server authentication — disabled	Server IP/Hostname — 128 characters maximum SMTP server authentication — disable/enable (Username/ Password — 128 characters maximum) Port — x–xxx Sender address — 128 characters maximum Hide IP address from the email body — enable/disabled Secure SMTP connection — enable/disable Verify certificate authority — disable/enable

3.7.1.4.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.1.5 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
General	✓	✗	✗

3.7.1.5.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.1.6 CLIコマンド

email-test

説明

mail-test は、SMTP の問題をトラブルシューティングするためにテストメールを送信します。

ヘルプ

```
        Usage: email-test <command> ...
Test SMTP configuration.

Commands:
  email-test -h, --help, Display help page

  email-test -r, --recipient <recipient_address> Send test
  email to the
    <recipient_address>      Email address of the recipient
```

時間

説明

時刻や日付の表示や変更に使用するコマンドです。

ヘルプ

ビューアとオペレータのプロファイルの場合:

```
time -h
  Usage: time [OPTION]... Display
  time and date.

     -h, --help              display help page
     -p, --print             display date and time in YYYYMMDDhhmmss format
```

管理者プロファイルの場合::

```
time -h
  Usage: time [OPTION]...
Display time and date, change time and date.
   -h, --help              display help page
   -p, --print             display date and time in YYYYMMDDhhmmss format
   -s, --set <mode>
         Mode values:
         - set date and time (format YYYYMMDDhhmmss) manual
              <date and time>
         - set preferred and alternate NTP servers
              ntpmanual <preferred server> <alternate server>
         - automatically set date and time ntpauto
Examples of usage:
-> Set date 2017-11-08 and time 22:00
       time --set manual 201711082200
-> Set preferred and alternate NTP servers
       time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

使用例

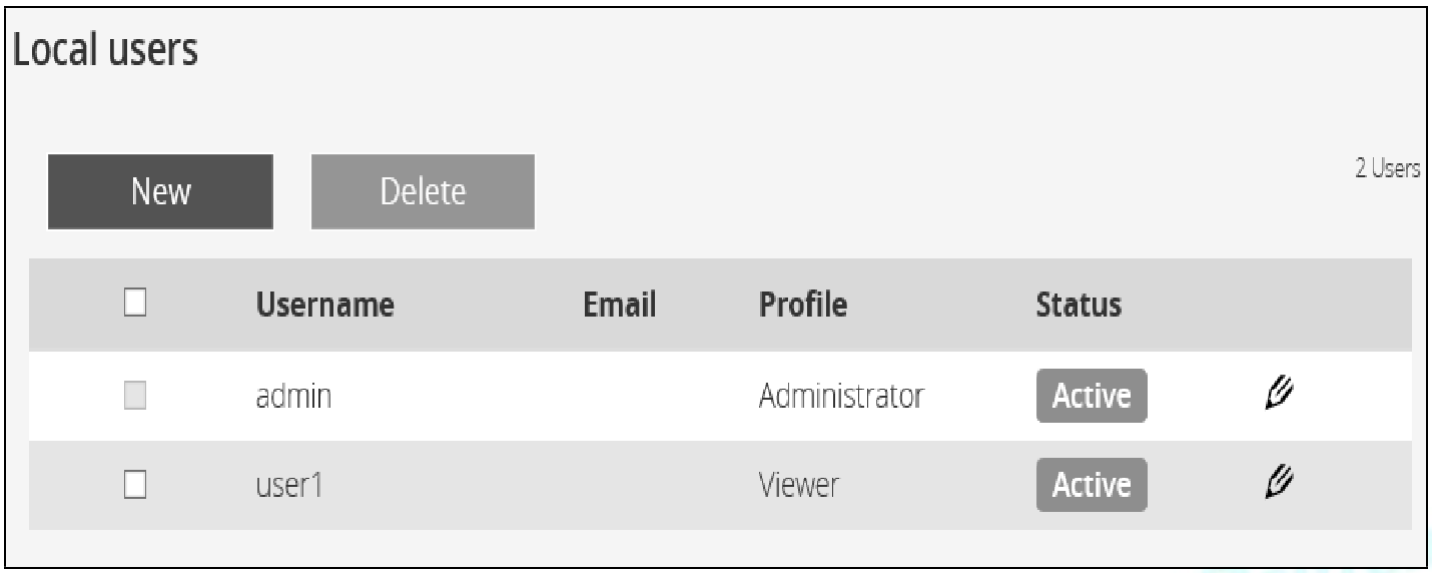
```
-> Set date 2017-11-08 and time 22:00 time --set
       manual 201711082200
-> Set preferred and alternate NTP servers
       time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

3.7.1.6.1 他のCLI コマンドの場合

CLIコマンドを参照してください。Information>>>CLI

3.7.2 ローカルユーザー

3.7.2.1 ローカルユーザーの表



この表には、サポートされているすべてのローカルユーザーアカウントが表示されており、以下の詳細が含まれています。:

- **Username**
- **Email**
- **Profile**
- **Status** – Status could take following values – Inactive/Locked/Password expired/Active

プロファイルごとのアクセス権のリストについては、以下のセクションを参照してください。
Full documentation>>>Information>>>Access rights per profiles.

3.7.2.1.1 アクション

a 追加

新規作成ボタンを押して、最大10人の新規ユーザーを作成します。.

b 削除

ユーザーを選択し、削除ボタンを押して削除します。

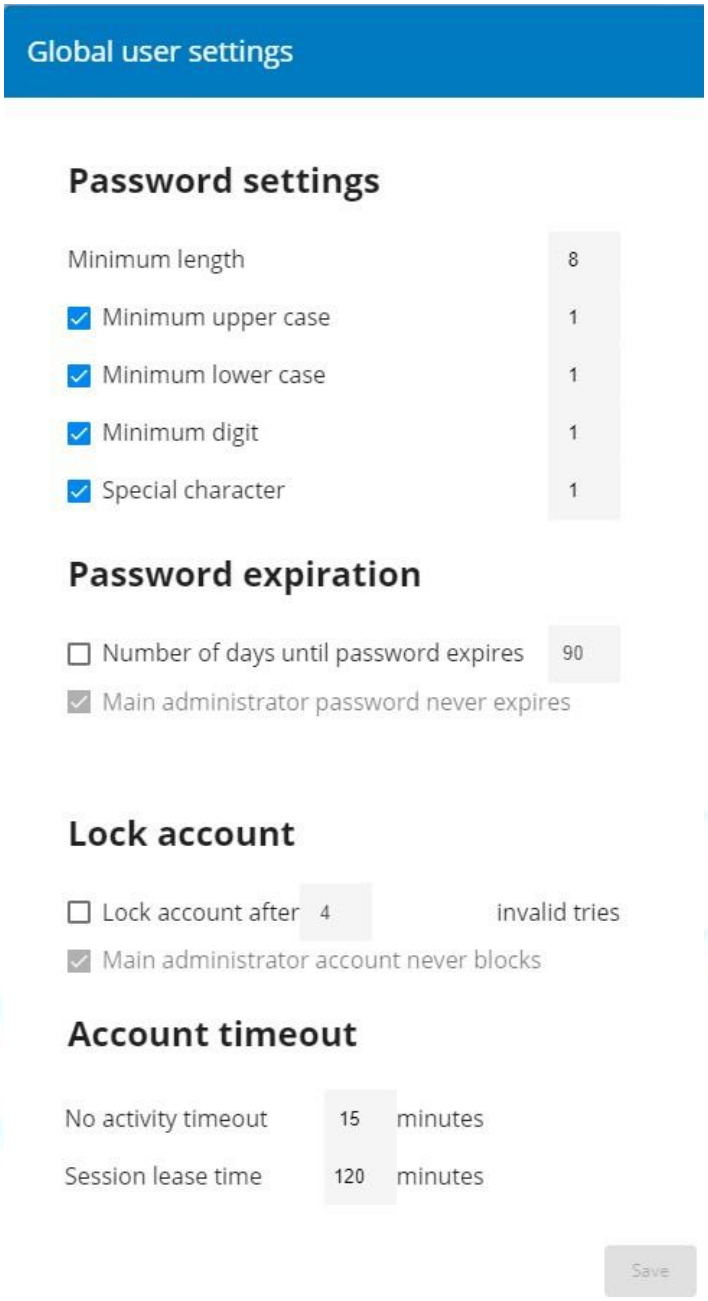
c 編集

ペンのロゴを押して、ユーザー情報を編集します。

次の設定にアクセスすることができます。:

- Active
- Profile
- Username
- Full name
- Email
- Phone
- Organization – Notify by email about account modification/Password
- Reset password
- Generate randomly
- Enter manually
- Force password to be changed on next login

d グローバル設定



変更後に**保存**を押します。
パスワードの設定
パスワードの強度ルールを設定するには、次の制限を適用します。:

- 最小長さ
- 最小大文字
- 最小小文字
- 最小桁数
- 特殊文字

パスワードの有効期限
パスワードの有効期限のルールを設定するには、次の制限を適用します。:

- パスワードの有効期限が切れるまでの日数

- 主な管理者パスワードの有効期限はありません

メイン管理者パスワードの有効期限が切れたことがない

1. この機能を無効にした場合パスワードの有効期限が切れた後に管理者アカウントをロックできます。
2. 有効にすると管理者パスワードの有効期限が切れることはありませんので定期的に変更してください。

アカウントをロックする
- 無効な試行回数の後にアカウントをロックする
- メインの管理者アカウントがブロックすることはありません

メインの管理者アカウントがブロックすることはありません

1. この機能を無効にすると、定義された失敗した接続数の後に管理者アカウントをロックすることができます。
2. 有効にすると、無制限のパスワード入力が許可されるため、管理者アカウントのセキュリティレベルが低下します。

アカウントのタイムアウト
セッションの有効期限のルールを設定するには、以下の制限を適用します。:

- アクティビティがない場合のタイムアウト時間(分単位)。

  アクティビティがない場合、指定した時間後にセッションが終了します。
- セッションのリース時間 (分単位)。

  アクティビティがある場合、指定された時間の後にセッションの有効期限が切れます。

3.7.2.2 デフォルト設定と可能なパラメーター –グローバルユーザー設定とローカルユーザー

	Default setting	Possible parameters
Password settings	Minimum length – enabled (8) Minimum upper case – enabled (1) Minimum lower case – enabled (1) Minimum digit – enabled (1) Special character – enabled (1)	Minimum length – enable (6–32)/disable Minimum upper case – enable (0–32)/disable Minimum lower case – enable (0–32)/disable Minimum digit – enable (0–32)/disable Special character – enable (0–32)/disable
Password expiration	Number of days until password expires – disabled Main administrator password never expires – disabled	Number of days until password expires – disable/enable (1–99999) Main administrator password never expires – disable/enable
Lock account	Lock account after xx invalid tries – disabled Main administrator account never blocks – disabled	Lock account after xx invalid tries – disable/enable (1–99) Main administrator account never blocks – disable/enable
Account timeout	No activity timeout – 60 minutes Session lease time – 120 minutes	No activity timeout – 1–60 minutes Session lease time – 60–720 minutes

Local users	1 user only: • Active — Yes • Profile — Administrator • Username — admin • Full Name — blank • Email — blank • Phone — blank • Organization — blank	10 users maximum: • Active — Yes/No • Profile — Administrator/Operator/Viewer • Username — 255 characters maximum • Full Name — 128 characters maximum • Email — 128 characters maximum • Phone — 64 characters maximum • Organization — 128 characters maximum

3.7.2.2.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.2.3 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Local users	✓	✗	✗

3.7.2.3.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.2.4 CLIコマンド

whoami

説明

whoami は現在のユーザー情報を表示します。:

- Username
- Profile
- Realm

ログアウト

説明

現在のユーザーをログアウトします。

ヘルプ

```
logout
  <cr> logout the user
```

3.7.2.4.1 他のCLIコマンドについて

次のCLIコマンドを参照してください。Information>>>CLI

3.7.2.5 トラブルシューティング

パスワードを忘れた場合のログイン方法を教えてください。

アクション

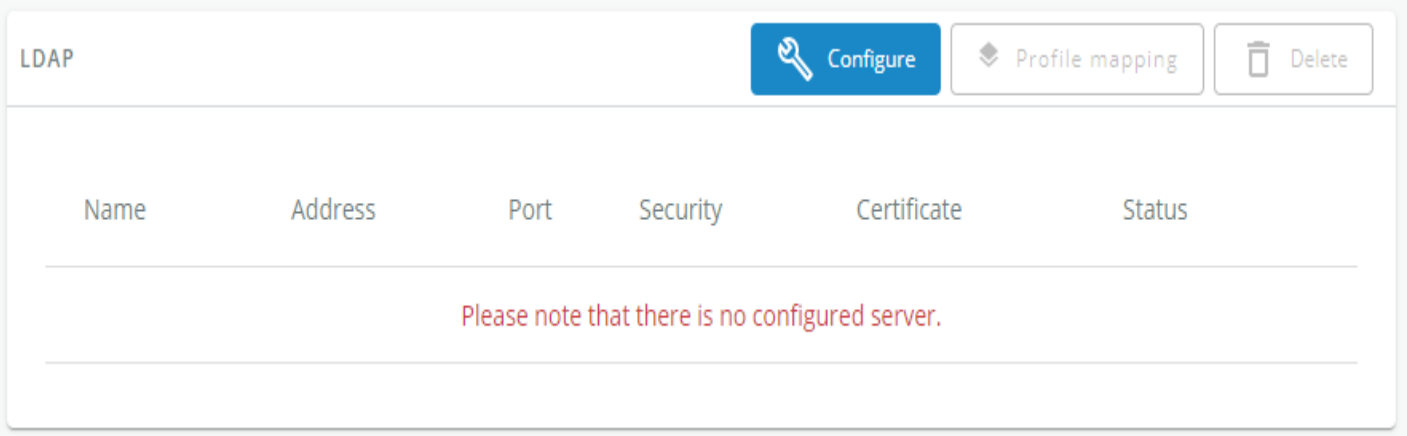
- パスワードの初期化は管理者に依頼してください。
- あなたがメイン管理者の場合、パスワードは次を参照してください。
  Servicing the Network Management Module>>>Recovering main administrator password .

3.7.2.5.1 その他の問題については

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.7.3 リモートユーザー

3.7.3.1 LDAP

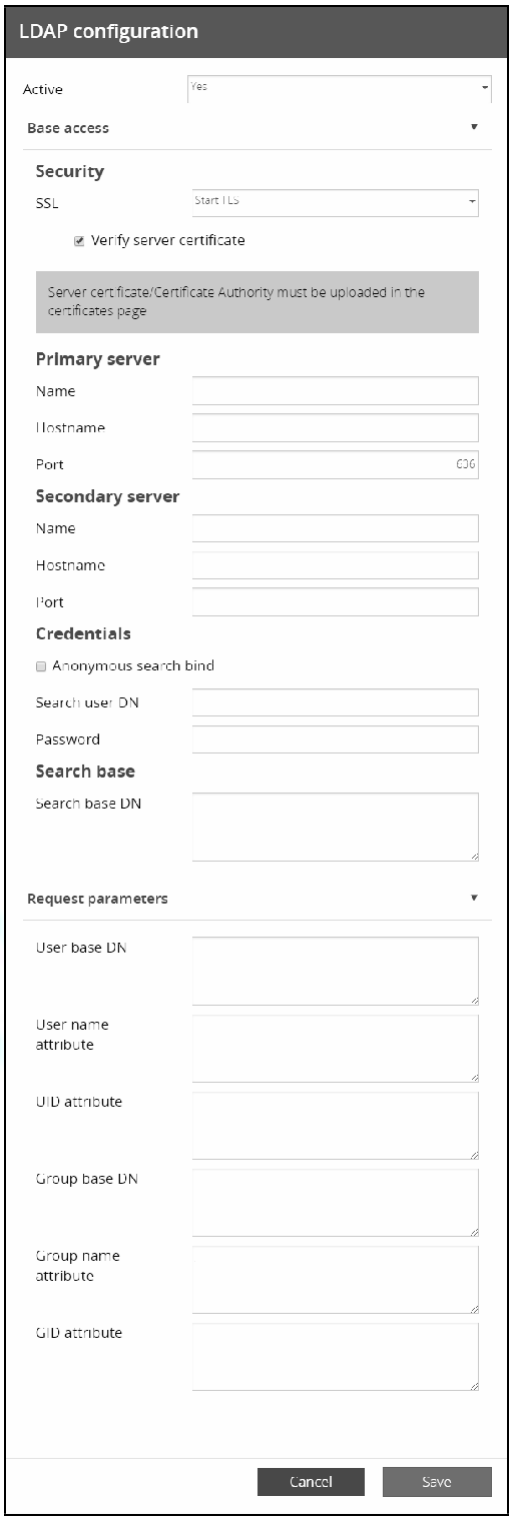


この表は、サポートされているすべてのサーバーを示しており、以下の詳細が含まれています。:

- Name
- Address
- Port
- Security
- Certificate
- Status – Status could take following values – Unreachable/Active

3.7.3.1.1 アクション

a 設定



1. **構成**を押して、次の LDAP 設定にアクセスします。:

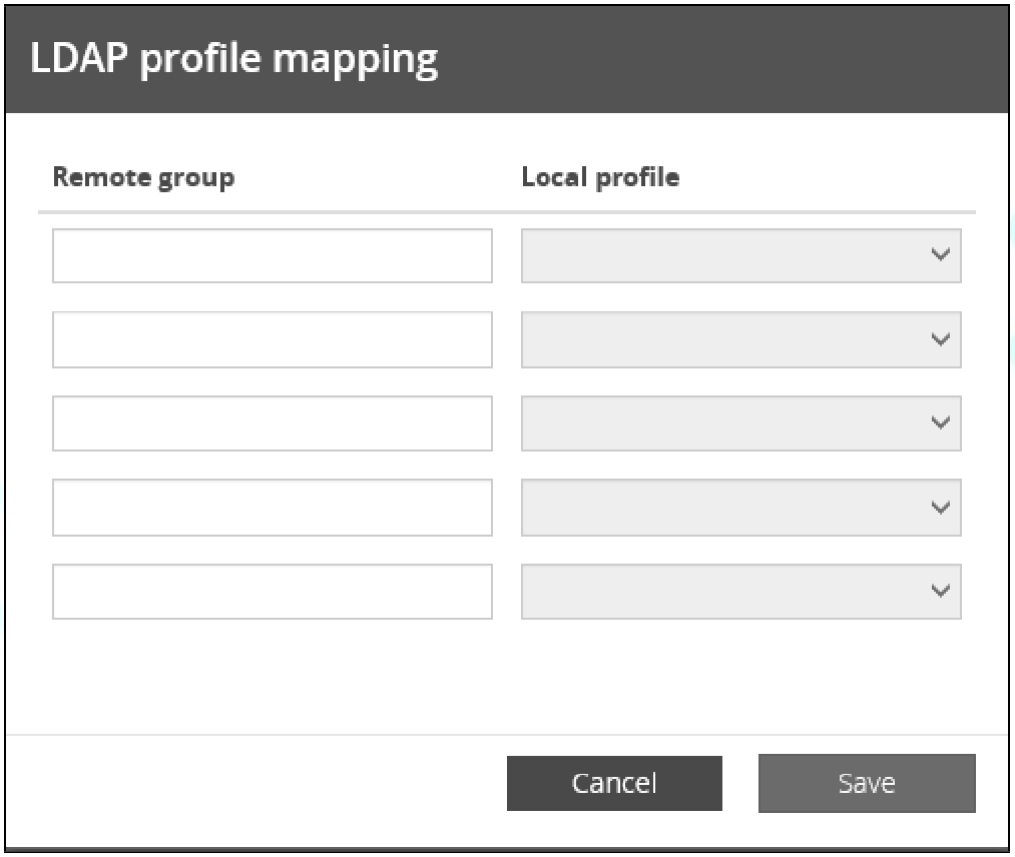
- Active
- Base access

- Security
  SSL – None/Start TLS/SSL
  Verify server certificate
- Primary server – Name/Hostname/Port
- Secondary server – Name/Hostname/Port
- Credentials – Anonymous search bind/Search user DN/Password
- Search base – Search base DN

- Request parameters
  - User base DN
  - User name attribute
  - UID attribute
  - Group base DN
  - Group name attribute
  - GID attribute

2. 保存する

b プロファイルマッピング

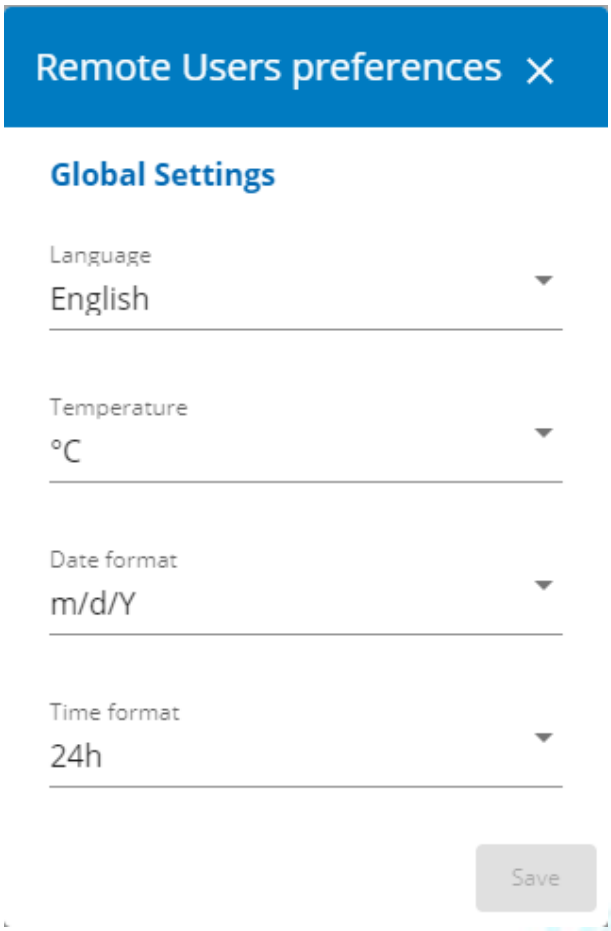


プロファイルごとのアクセス権のリストについては、以下のセクションを参照してください。Full documentation>>>Information>>>Access rights per profiles.

1. **プロファイルマッピング**を押して、リモートグループをローカルプロファイルにマッピングします。
2. **保存**する。

c ユーザー設定

すべてのユーザー設定は、すべてのリモートユーザー（LDAP、RADIUS）に適用されます。



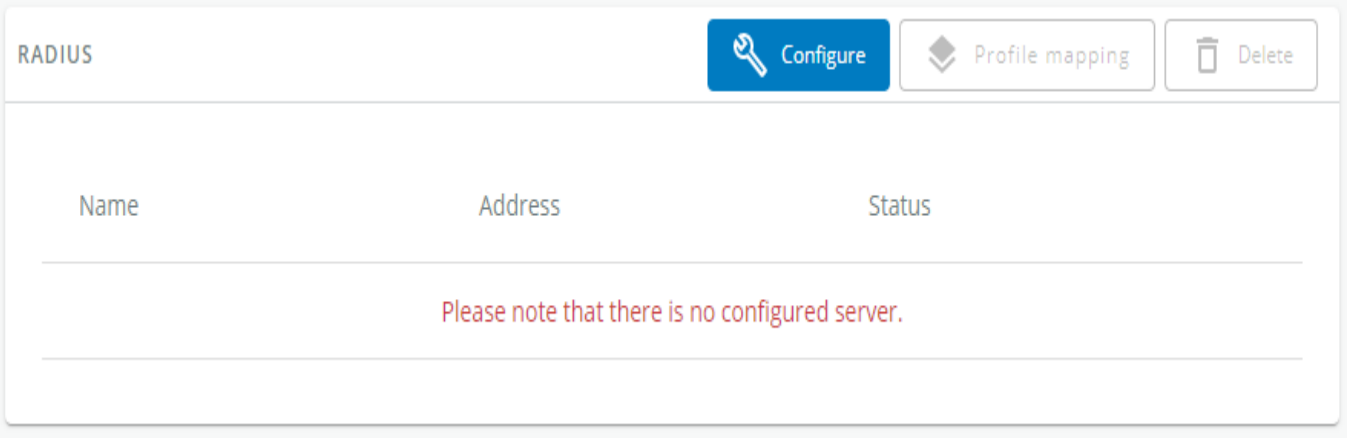
1. **[ユーザー設定]**を押して、すべての LDAP ユーザーに適用される設定を定義します。

- Language
- Temperature
- Date format
- Time format

2. **保存**する。

3.7.3.2 RADIUS

Radius は安全なプロトコルではありませんので、
最大限のセキュリティを確保するためには LDAP over TLS を使用することをお勧めします。

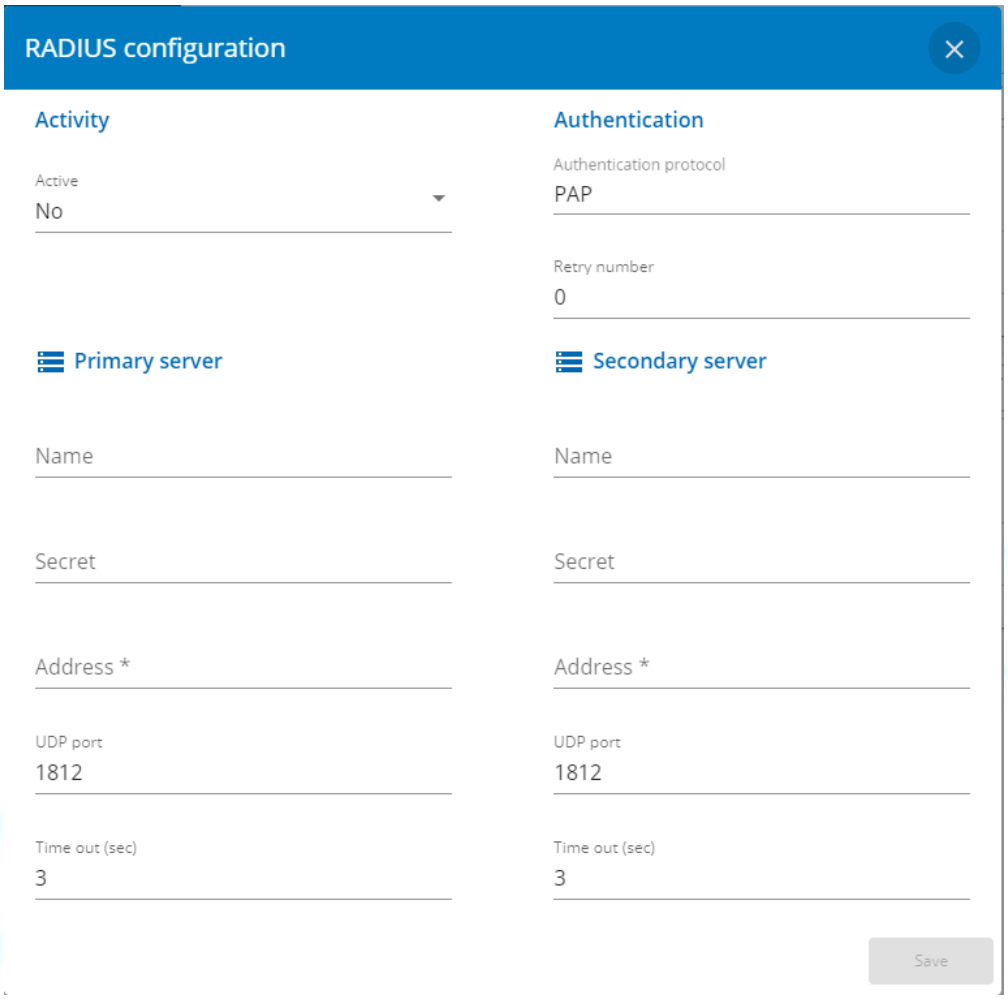


この表は、サポートされているすべてのサーバーを示しており、以下の詳細が含まれています。:

- Name – RADIUS サーバーの記述名
- Address – – RADIUS サーバーのホスト名または IP アドレス
- Status – RADIUS サーバーがアクティブか非アクティブか

3.7.3.2.1 アクション

a 設定

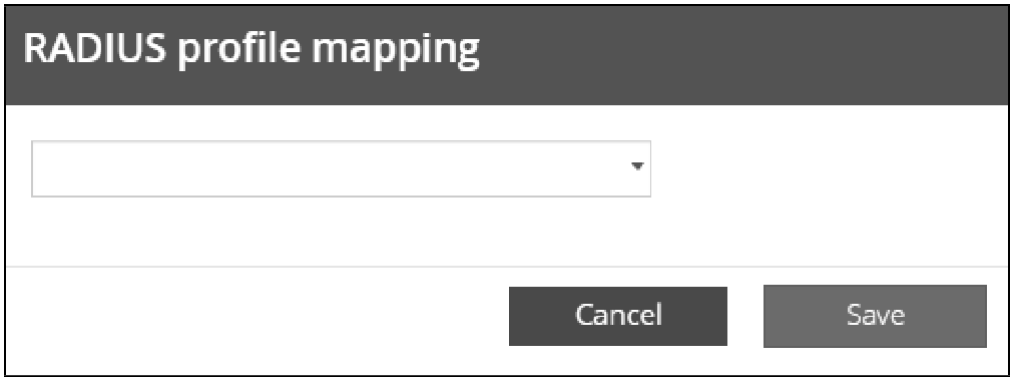


1. **[Configure]**を押して、次の RADIUS 設定にアクセスします。:

- Active
- Retry number
- Primary server
  - Name – RADIUSサーバーの記述名
  - Secret –クライアントとRADIUSサーバー間で共有される秘密。
  - Address – RADIUS サーバーのホスト名または IP アドレス
  - UDP port – RADIUS サーバーの UDP ポート (既定では 1812)
  - Time out (s) –クライアントが RADIUS サーバーからの応答を待つ時間
- Secondary server
  - Name – RADIUSサーバの記述名
  - Secret – クライアントとRADIUSサーバー間で共有される秘密。
  - Address – RADIUS サーバーのホスト名または IP アドレス
  - UDP port – RADIUS サーバーの UDP ポート (既定では 1812)
  - Time out (s) – クライアントが RADIUS サーバーからの応答を待つ時間

2. **保存**する

b プロファイルマッピング

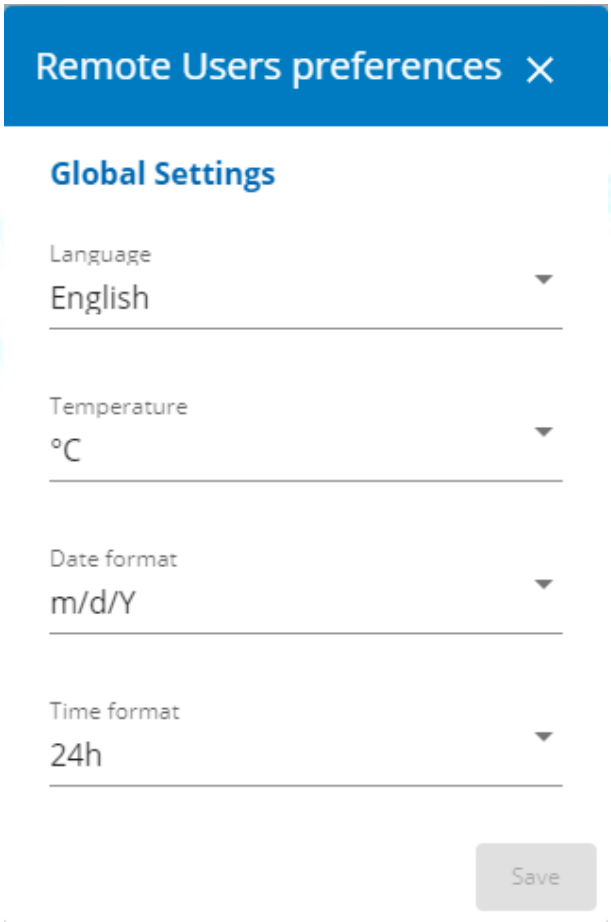


プロファイルごとのアクセス権のリストについては、以下のセクションを参照してください。
Full documentation>>>Information>>>Access rights per profiles.

1. **プロファイルマッピング**を押して、RADIUSプロファイルをローカルプロファイルにマッピングします。
2. **保存**する。

c ユーザー設定

すべてのユーザー設定は、すべてのリモートユーザー（LDAP、RADIUS）に適用されます。



1. **ユーザー設定**を押して、すべての LDAP ユーザーに適用される設定を定義します。

- Language

- Temperature
- Date format
- Time format

2. 保存する。

3.7.3.3 デフォルト設定と可能なパラメーター –リモートユーザー

	Default setting	Possible parameters
LDAP	Configure • Active – No • Security SSL – SSL Verify server certificate – enabled • Primary server Name – Primary Hostname – blank Port – 636 • Secondary server Name – blank Hostname – blank Port – blank • Credentials Anonymous search bind – disabled Search user DN – blank Password – blank • Search base Search base DN – dc=example,dc=com • Request parameters User base DN – ou=people,dc=example,dc=com User name attribute – uid UID attribute – uidNumber Group base DN – ou=group,dc=example,dc=com Group name attribute – gid GID attribute – gidNumber Profile mapping – no mapping Users preferences • Language – English • Temperature unit – ° C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)	Configure • Active – No/yes • Security SSL – None/Start TLS/SSL Verify server certificate – disabled/enabled • Primary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx • Secondary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx • Credentials Anonymous search bind – disabled/enabled Search user DN – 1024 characters maximum Password – 128 characters maximum • Search base Search base DN – 1024 characters maximum • Request parameters User base DN – 1024 characters maximum User name attribute – 1024 characters maximum UID attribute – 1024 characters maximum Group base DN – 1024 characters maximum Group name attribute – 1024 characters maximum GID attribute – 1024 characters maximum Profile mapping – up to 5 remote groups mapped to local profiles Users preferences • Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese • Temperature unit – ° C (Celsius)/° F (Fahrenheit) • Date format – MM-DD-YYYY / YYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/MM/YYY / DD MM YYYY • Time format – hh:mm:ss (24h) / hh:mm:ss (12h)

RADIUS	Configure • Active – No • Retry number – 0 • Primary server Name – blank Secret – blank Address – blank UDP port – 1812 Time out – 3 • Secondary server Name – blank Secret – blank Address – blank UDP port – 1812 Time out – 3 Users preferences • Language – English • Temperature unit – ° C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)	Configure • Active – Yes/No • Retry number – 0 to 128 • Primary server Name – 128 characters maximum Address – 128 characters maximum Secret – 128 characters maximum UDP port – 1 to 65535 Time out – 3 to 60 • Secondary server Name – 128 characters maximum Address – 128 characters maximum Secret – 128 characters maximum UDP port – 1 to 65535 Time out – 3 to 60 Users preferences • Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese • Temperature unit – ° C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)

3.7.3.3.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.3.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Remote users	✓	✗	✗

3.7.3.4.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.3.5 CLIコマンド

ldap-test

説明

Ldap-testは、LDAP構成の問題や作業の問題をトラブルシューティングするのに役立ちます。

ヘルプ

```
        Usage: ldap-test <command> [OPTION]...
Test LDAP configuration.

Commands:
   ldap-test -h, --help, Display help page

   ldap-test --checkusername <username> [--primary|--secondary] [-v] Check if the user can
   be retrieve from the LDAP server
      <username>            Remote username to test
      --primary             Force the test to use primary server (optional)
      --secondary           Force the test to use secondary server (optional)
      -v,--verbose          Print the exchanges with LDAP server (optional)

   ldap-test --checkauth <username> [--primary|--secondary] [-v] Check if remote user
   can login to the card
      <username>            Remote username to test
      -p,--primary              Force the test to use primary server (optional)
      -s,--secondary            Force the test to use secondary server (optional)
      -v,--verbose          Print the exchanges with LDAP server (optional)

   ldap-test --checkmappedgroups [--primary|--secondary] [-v] Check LDAP
   mapping
      -p,--primary              Force the test to use primary server (optional)
      -s,--secondary            Force the test to use secondary server (optional)
      -v,--verbose          Print the exchanges with LDAP server (optional) Quick guide for

testing:

In case of issue with LDAP configuration, we recommend to verify the configuration using the
commands in the following order:

   1. Check user can be retrieve on the LDAP server ldap-test --
      checkusername <username>

   2. Check that your remote group are mapped to the good profile ldap-test --
      checkmappedgroups

   3. Check that the user can connect to the card ldap-test --
      checkauth <username>
```

ログアウト

説明

現在のユーザーをログアウトする。

ヘルプ

```
logout
  <cr> logout the user
```

whoami

説明

whoamiは現在のユーザー情報を表示します。:

- Username
- Profile
- Realm

3.7.3.5.1 その他のCLIコマンド

次のCLIコマンドを参照してください。Information>>>CLI

3.7.3.6 トラブルシューティング

パスワードを忘れた場合のログイン方法を教えてください。

アクション

- パスワードの初期化は管理者に依頼してください。
- メイン管理者の場合、パスワードは下記を参照してください。

  Servicing the Network Management Module>>>Recovering main administrator password .

LDAP 設定/コミッショニングがうまくいっていない

セクションを参照してください。Servicing the Network Management Module>>>Commissioning/Testing LDAP .

3.7.3.6.1 その他の問題については

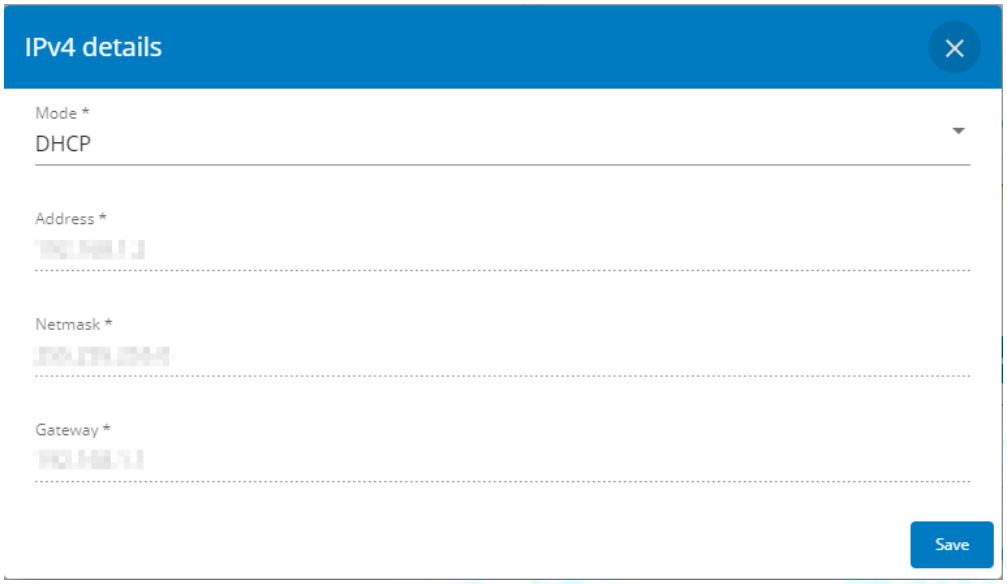
その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.7.4 ネットワーク & プロトコル

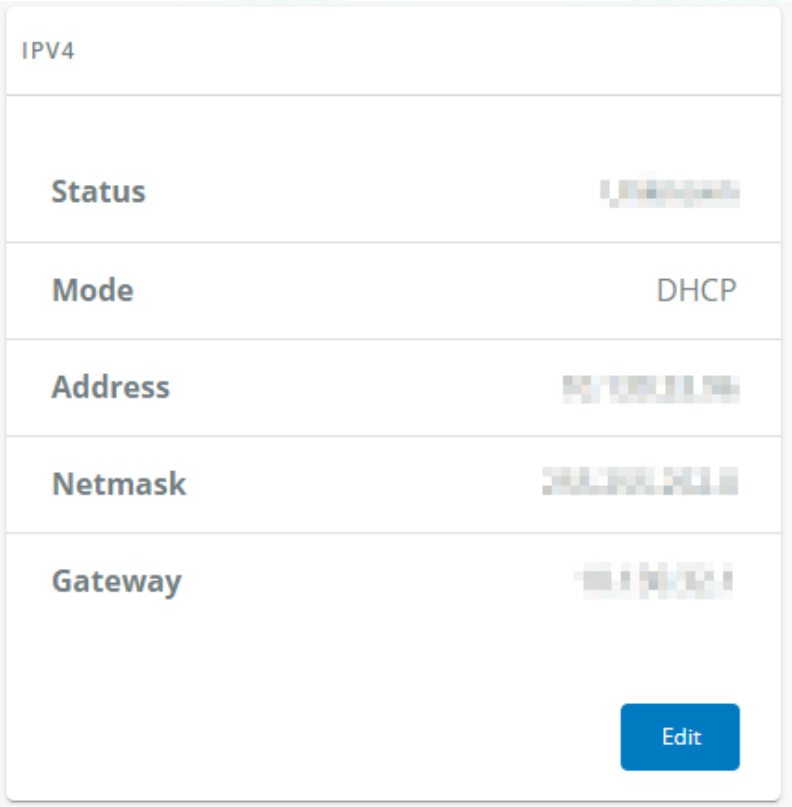
3.7.4.1 ネットワーク

3.7.4.1.1 IPv4

すべての変更は、ネットワークモジュールが再起動した後に適用されます。



編集ボタンを押してネットワーク設定を設定し、手動またはDHCP設定のどちらかを選択します。:



a 手動

Manualを選択し、ネットワークがBootPまたはDHCPサーバーで設定されていない場合は、ネットワークの設定を入力します。

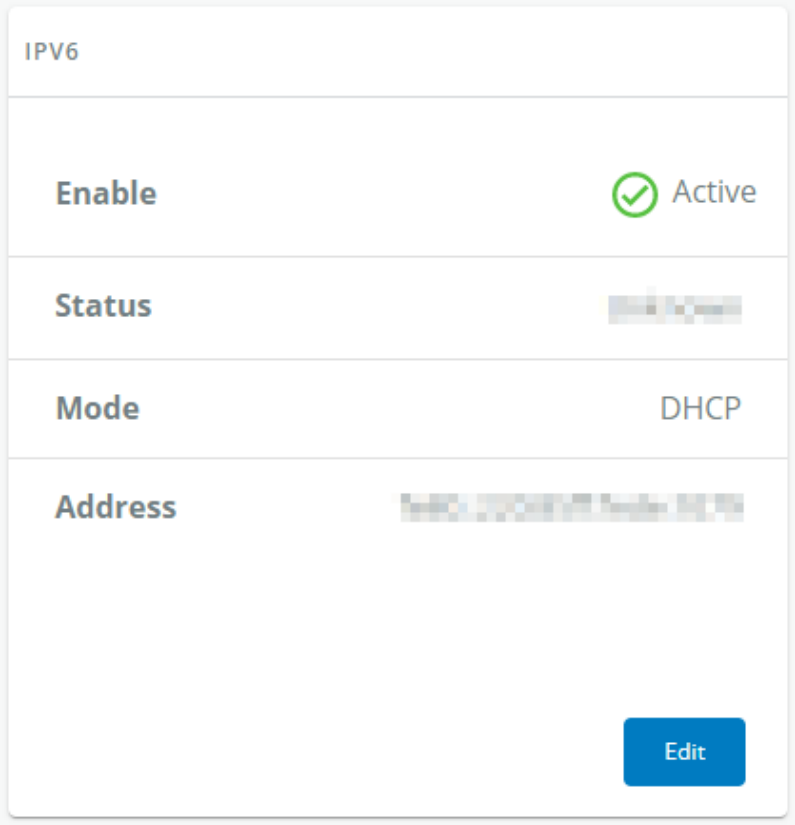
- IP アドレスを入力します。
  ネットワークモジュールには、TCP/IP ネットワークで使用するための固有の IP アドレスが必要です。
- ネットマスクを入力します。
  ネットマスクは、ネットワークモジュールが接続されているサブネットワークのクラスを識別します。
- ゲートウェイアドレスを入力します。
  ゲートウェイアドレスは異なるネットワークセグメントに接続されているデバイスやホストへの接続を可能にします。

b DHCP

ダイナミック DHCP を選択して、BootP または DHCP サーバーによるネットワークパラメーターを設定します。

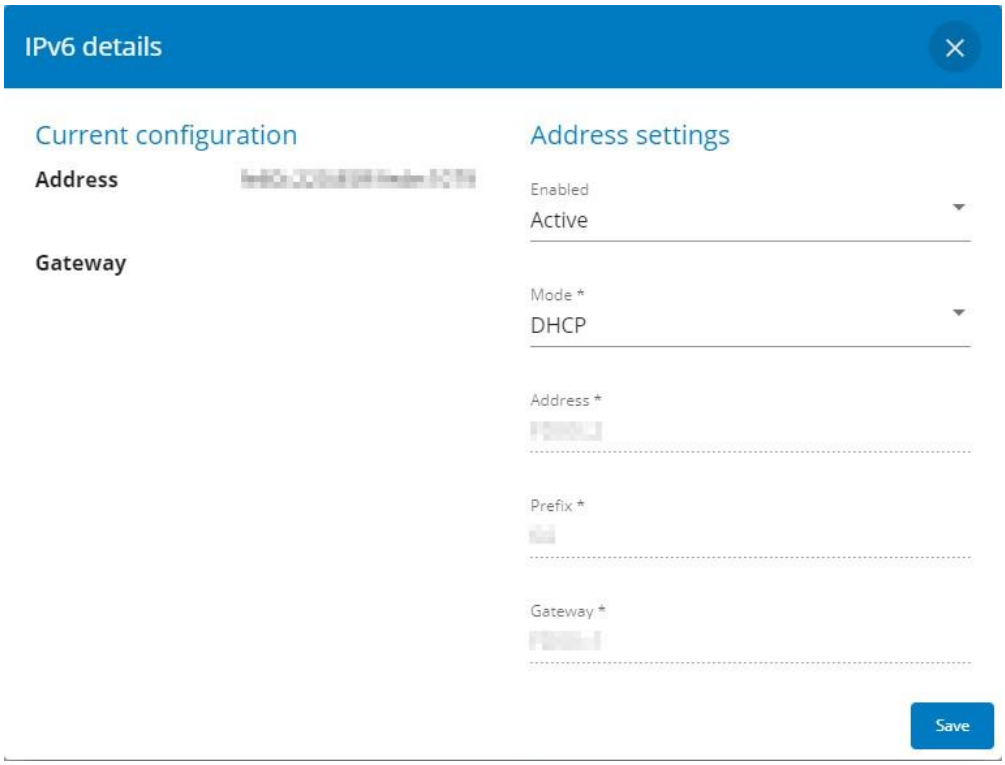
サーバーから応答を受信しない場合、ネットワークモジュールは、直近のパワーアップから最後に保存されたパラメーターで起動します。各電源投入後、ネットワークモジュールはネットワークパラメーターの回復を 5 回試行します。

3.7.4.1.2 IPv6



IPV6 ステータスと最初の 3 つのアドレスが表示されます。

編集ボタンを押してネットワーク設定を設定し、以下のIPV6の詳細情報とアクセスを取得します。



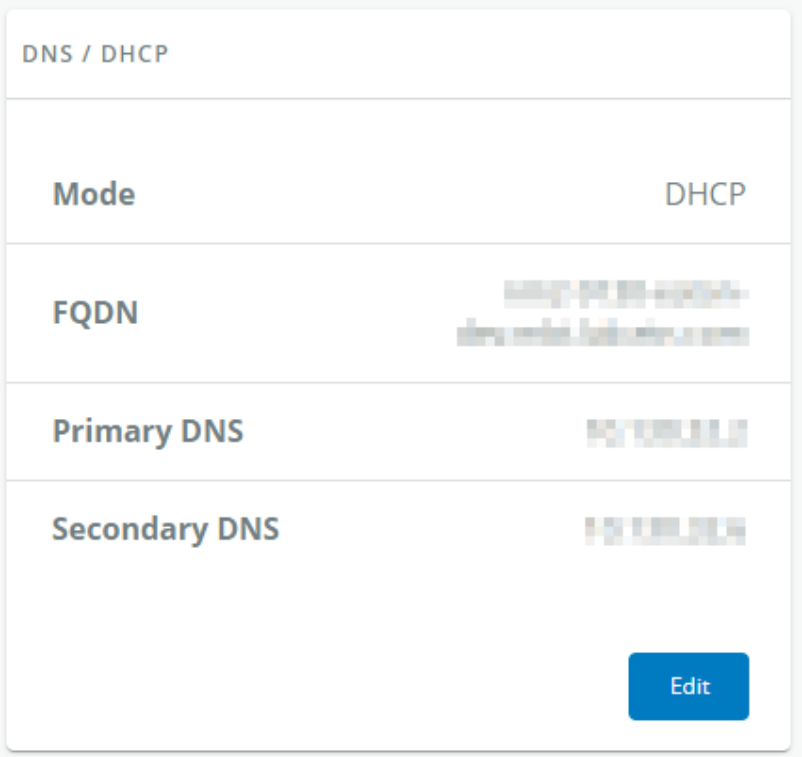
a 現在の設定

- Address
- Gateway

b アドレス設定

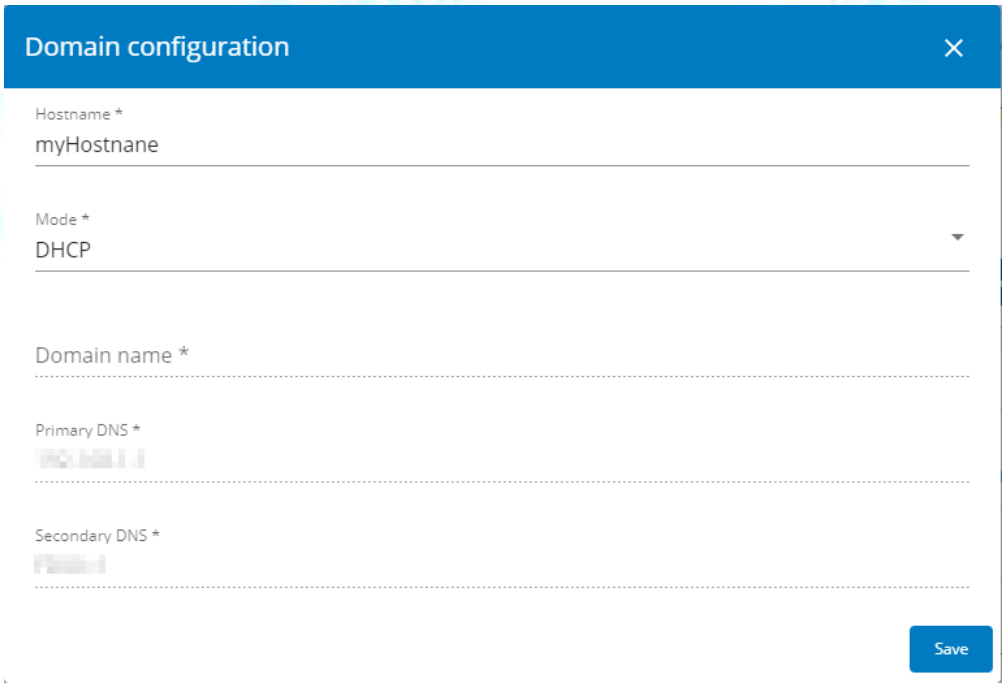
- Enabled
- Mode（Manual/DHCP）
- Address
- Prefix
- Gateway

3.7.4.1.3 DNS/DHCP



DNSは、インターネットまたはプライベートネットワークに接続されたコンピューター、サービス、またはその他のリソースのための階層分散型ネーミングシステムです。

[編集(Edit)]ボタンを押してネットワーク設定を設定し、スタティックまたはダイナミック設定を選択します。



a 手動

- ネットワークモジュールのホスト名を入力します。
- ネットワークモジュールのドメイン名を入力します。
- プライマリ DNS サーバー。
  ドメイン名の IP アドレスへの変換を提供する DNS サーバーの IP アドレスを入力します。

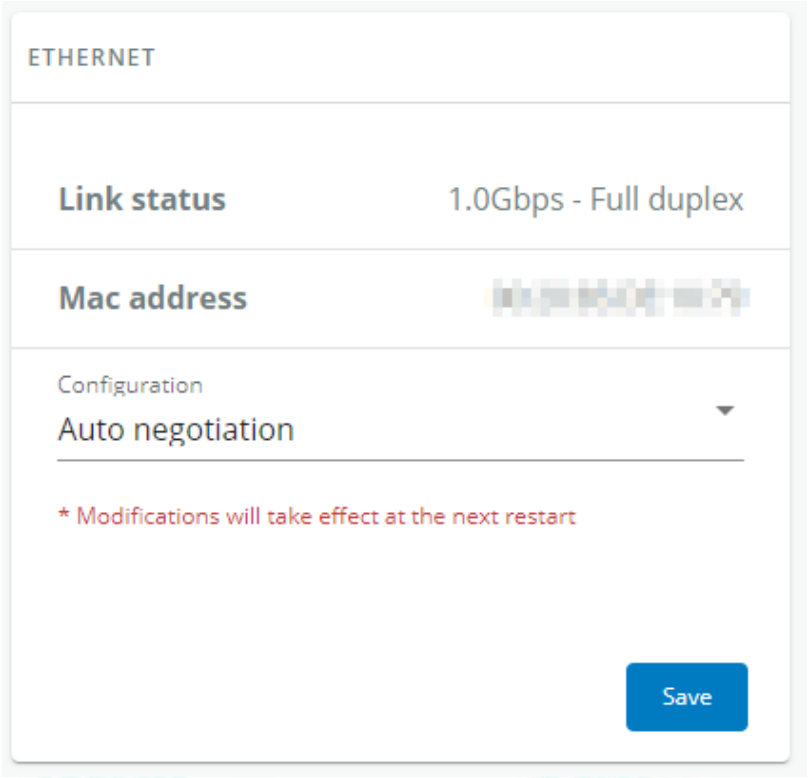
- セカンダリ DNS サーバー。

  プライマリ DNS サーバーが利用できない場合に、ドメイン名を IP アドレスに変換するセカンダリ DNS サーバーの IP アドレスを入力します。

b DHCP

- ネットワークモジュールのホスト名を入力します。

3.7.4.1.4 イーサネット



LANとは、限られたエリア内のコンピューターを相互に接続するコンピューターネットワークです。LAN設定で利用可能な値を以下に示します。:

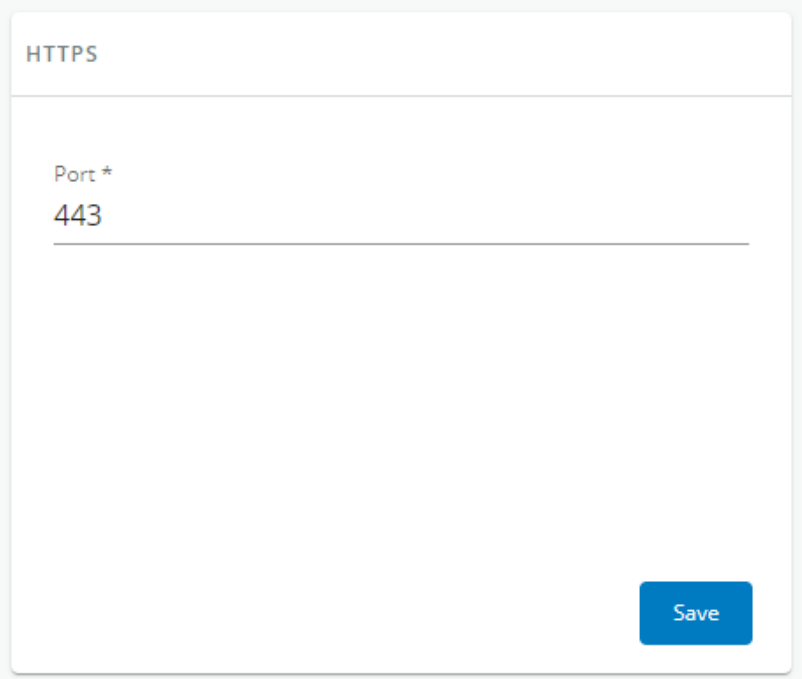
- Auto negotiation
- 10Mbps – Half duplex
- 10Mbps – Full duplex
- 100Mbps – Half duplex
- 100Mbps – Full duplex
- 1.0 Gbps – Full duplex

すべての変更は、次のネットワークモジュールの再起動後に適用されます。

3.7.4.2 プロトコル

このタブには、ネットワークを介してデバイスから情報を取得するために使用する通信プロトコルの設定が含まれています。

3.7.4.2.1 HTTPS

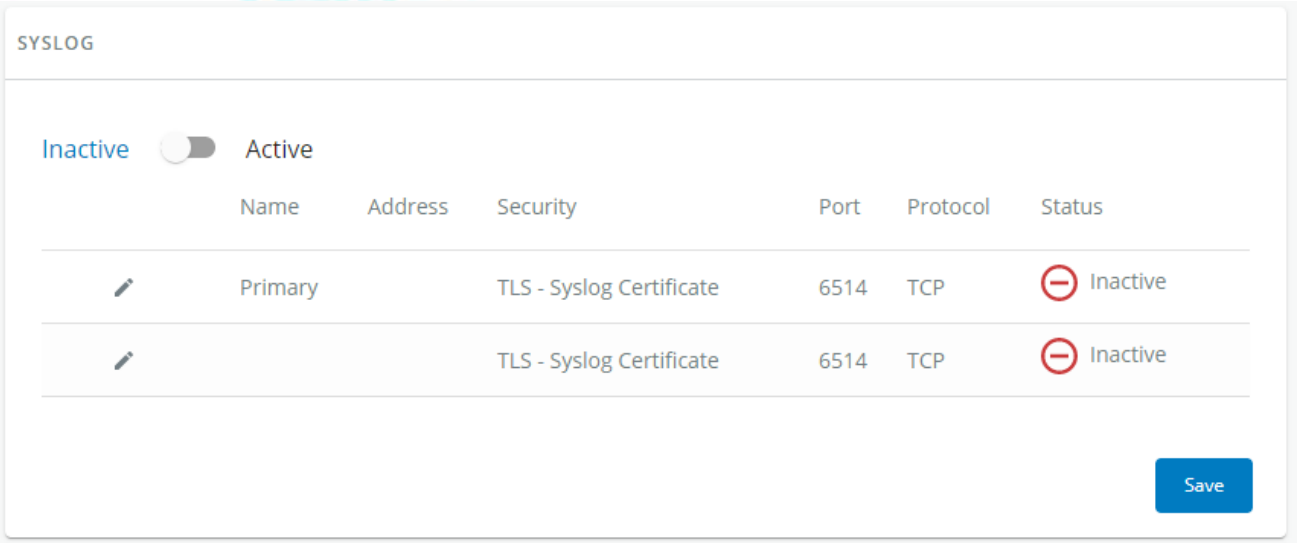


httpsのみ利用可能です。

https のデフォルトのネットワークポートは 443 です。セキュリティを強化するために、このページでポートを変更することができます。変更後、保存を押してください。

httpsしか使えないので、80番ポートはサポートされていません。

3.7.4.2.2 システムログ



a 設定

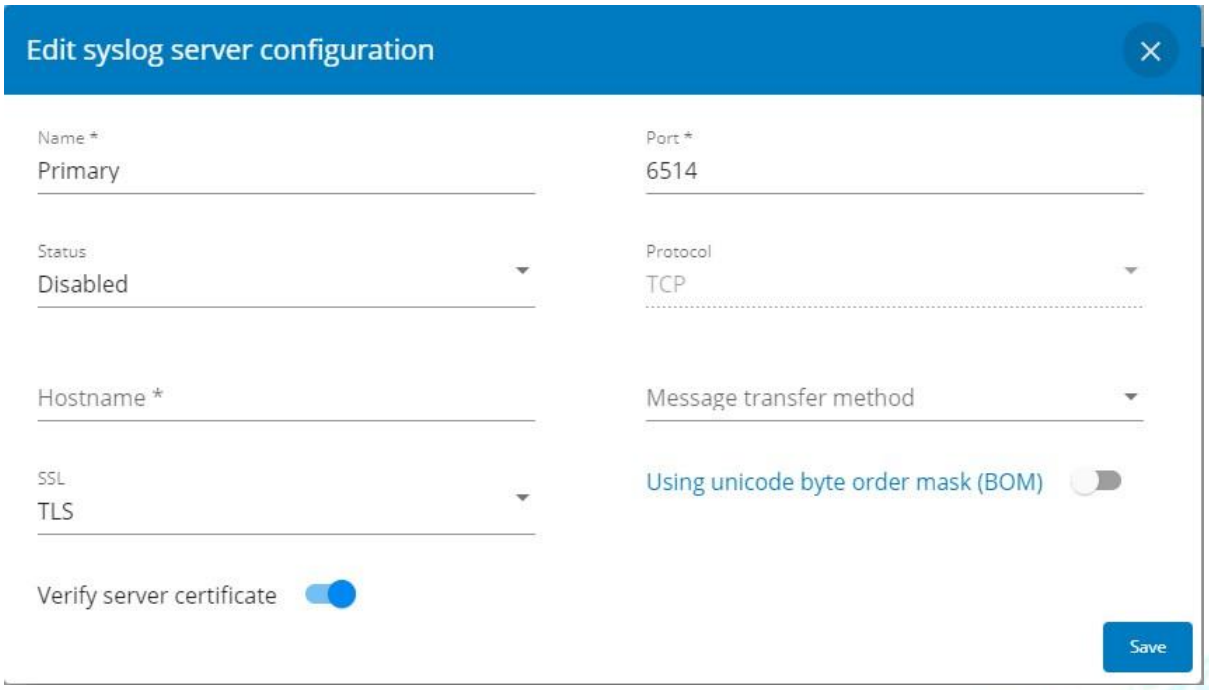
この画面では、管理者が最大 2 台の syslog サーバーを設定することが

できます。 syslogサーバーの設定を行うには:

1- Syslogを**有効**にする.

変更後に**保存**を押す.

2- syslog サーバーを**設定**する



- 編集アイコン　をクリックして設定にアクセスします。
- サーバー名を入力または変更します。
- [アクティブ] ドロップダウン リストで **[はい]** を選択して、サーバーをアクティブにします。
- ホスト名とポートを入力します。
- プロトコル – UDP/TCP を選択します。
- TCP で、メッセージ転送方法 – オクテットカウント/非透過フレームを選択します。
- 必要に応じて、オプション「Using Unicode BOM」を選択します。
- 変更後、**[保存]** を押します。

3.7.4.3 デフォルト設定と可能なパラメーター –ネットワーク & プロトコル

	Default setting	**Possible parameters**
IPV4	Mode – DHCP	Mode – DHCP/Manual (Address/Netmask/Gateway)
IPV6	Enable – checked Mode – DHCP	Enabled – Active/Inactive Mode – DHCP/Manual (Address/Prefix/Gateway)
DNS/DHCP	Hostname – *device*–[MAC address] Mode – DHCP	Hostname – 128 characters maximum Mode :DHCP/Manual (Domain name/Primary DNS/ Secondary DNS)
Ethernet	Configuration – Auto negotiation	Configuration – Auto negotiation – 10Mbps – Half duplex – 10Mbps – Full duplex – 100Mbps – Half duplex – 100Mbps – Full duplex – 1.0 Gbps – Full duplex

HTTPS	Port – 443	Port – x-xxx
Syslog	Inactive • Server#1 Name – Primary Status – Disabled Hostname – empty Port – 514 Protocol – UDP Message transfer method – Non transparent framing Using unicode byte order mask (BOM) – disabled • Server#2 Name – empty Status – Disabled Hostname – empty Port – 514 Protocol – UDP Message transfer method – DIsabled in UDP Using unicode byte order mask (BOM) – disabled	Inactive/Active • Server#1 Name – 128 characters maximum Status – Disabled/Enabled Hostname – 128 characters maximum Port – x-xxx Protocol – UDP/TCP Message transfer method – Non transparent framing Using unicode byte order mask (BOM) – disable/enable • Server#2 Name – 128 characters maximum Status – Disabled/Enabled Hostname – 128 characters maximum Port – x-xxx Protocol – UDP/TCP Message transfer method (in TCP) – Octet counting/Non transparent framing Using unicode byte order mask (BOM) – disable/enable

3.7.4.3.1 その他の設定の場合

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.4.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Network & Protocols	✓	✗	✗

3.7.4.4.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.4.5 CLIコマンド

netconf

説明

カードのネットワーク設定を表示または変更するためのツール

ヘルプ

ビューアとオペレータのプロファイルについて:

```
netconf -h
 Usage: netconf [OPTION]...
 Display network information and change configuration.

   -h, --help      display help page
   -l, --lan       display Link status and MAC address
   -4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
   -6, --ipv6      display IPv6 Mode, Addresses and Gateway
   -d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
```

管理者プロフィールの場合

```
netconf -h
 Usage: netconf [OPTION]...
 Display network information and change configuration.
  -h, --help      display help page
  -l, --lan       display Link status and MAC address
  -d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
  -4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
  -6, --ipv6      display IPv6 Mode, Addresses and Gateway
    Set commands are used to modify the settings.
  -s, --set-lan <link speed>
      Link speed values:
      auto       Auto negotiation
      10hf       10 Mbps - Half duplex
      10ff       10 Mbps - Full duplex
      100hf      100 Mbps - Half duplex
      100ff      100 Mbps - Full duplex
      1000ff     1.0 Gbps - Full duplex
  -f, --set-domain hostname <hostname>    set custom hostname
  -f, --set-domain <mode>
          Mode values:
          - set custom Network address, Netmask and Gateway:
              manual <domain name> <primary DNS> <secondary DNS>
          - automatically set Domain name, Primary and Secondary DNS
              dhcp
  -i, --set-ipv4 <mode>
          Mode values:
          - set custom Network address, Netmask and Gateway
              manual <network> <mask> <gateway>
          - automatically set Network address, Netmask and Gateway
              dhcp
  -x, --set-ipv6 <status>
          Status values:
          - enable IPv6
              enable
          - disable IPv6
              disable
  -x, --set-ipv6 <mode>
          Mode values:
          - set custom Network address, Prefix and Gateway
              manual <network> <prefix> <gateway>
          - automatically set Network address, Prefix and Gateway
              router
Examples of usage:
-> Display Link status and MAC address
     netconf -l
-> Set Auto negotiation to Link
     netconf --set-lan auto
-> Set custom hostname
     netconf --set-domain hostname ups-00-00-00-00-00-00
-> Set Adress, Netmask and Gateway
     netconf --set-ipv4 manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6
```

使用例

```
 -> Display Link status and MAC address
      netconf -l
 -> Set Auto negotiation to Link
      netconf -s auto
 -> Set custom hostname
      netconf -f hostname ups-00-00-00-00-00-00
 -> Set Adress, Netmask and Gateway
      netconf -i manual 192.168.0.1 255.255.255.0 192.168.0.2
 -> Disable IPv6
      netconf -6 disable
```

ping and ping6

説明

Ping と ping6 ユーティリティは、ネットワーク接続をテストするために使用されます。

ヘルプ

```
ping
  The ping utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
  to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST
  datagrams (``pings'') have an IP and ICMP header, followed by a ``struct
  timeval'' and then an arbitrary number of ``pad'' bytes used to fill out
  the packet.

  -c                Specify the number of echo requests to be sent
  -h                Specify maximum number of hops
  <Hostname or IP>  Host name or IP address


ping6
  The ping6 utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
  to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST
  datagrams (``pings'') have an IP and ICMP header, followed by a ``struct
  timeval'' and then an arbitrary number of ``pad'' bytes used to fill out
  the packet.

  -c                Specify the number of echo requests to be sent
  <IPv6 address>    IPv6 address
```

traceroute and traceroute6

説明

Traceroute と traceroute6 ユーティリティは、ネットワークの設定を確認するためのものです。

ヘルプ

```
traceroute
  -h                 Specify maximum number of hops
  <Hostname or IP>   Remote system to trace
```

```
traceroute6
  -h                 Specify maximum number of hops
  <IPv6 address>     IPv6 address
```

3.7.4.5.1 その他のCLIコマンドについて

次のCLIコマンドを参照してください。Information>>>CLI

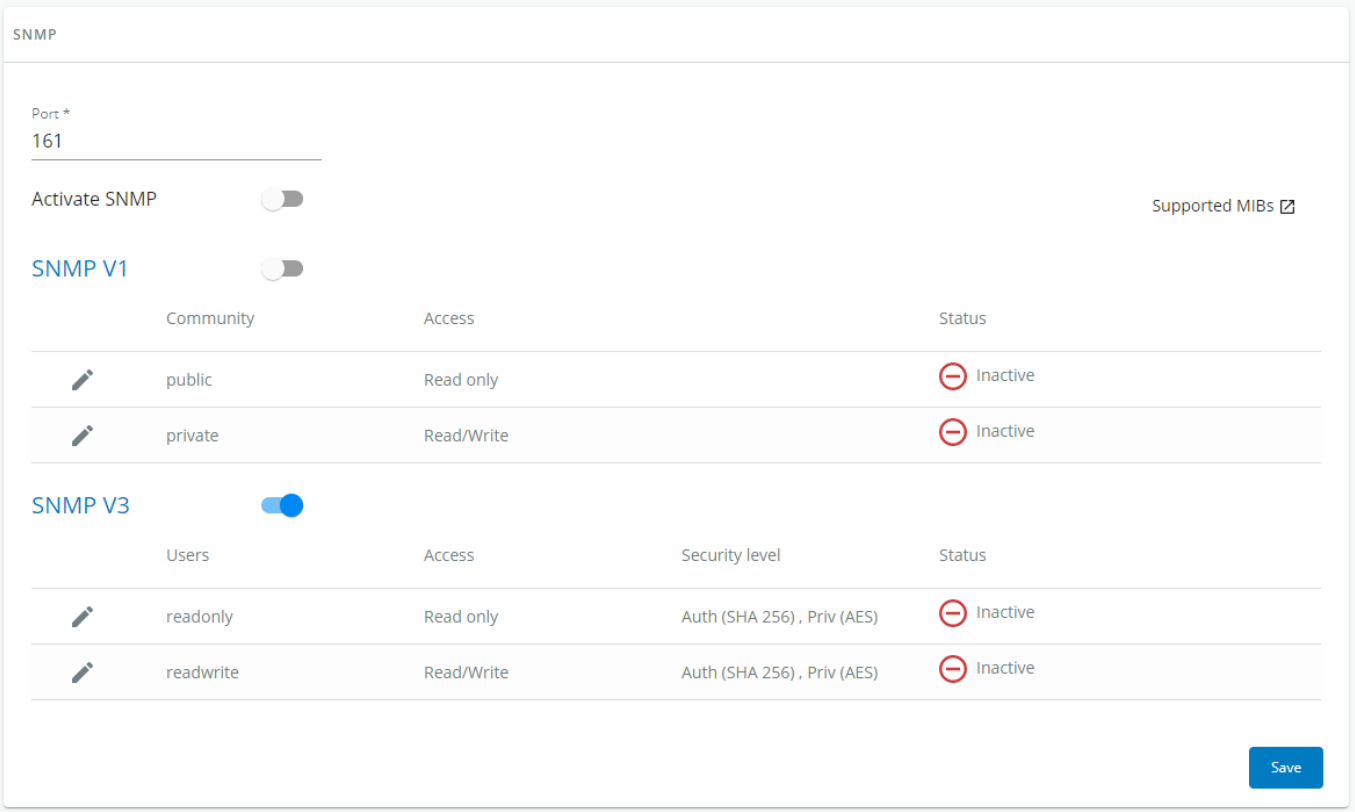
3.7.5 SNMP

このタブには、ネットワーク管理システムで使用する SNMP プロトコルの設定が含まれています。

認証設定の変更は、アクティブなユーザーアカウントの有効なパスワードを入力して確認する必要があります。

3.7.5.1 SNMP tables

SNMPのデフォルトポートは161で、通常は変更しないでください。サイバーセキュリティのために標準ポート以外のポートを使用することを好む組織もありますが、このフィールドではそれを許可します。



SNMP 監視 サードパーティの SNMP マネージャを使用して、バッテリーの状態、電源状態、イベント、およびトラップを監視します。
SNMP データを照会するには、通知アプリケーションページに SNMP マネージャを追加する必要はありません。
SNMP マネージャを設定するには:

- IP アドレスを設定します。
- SNMP v1またはv1とv3を選択します。
- SNMP マネージャが監視するために選択した MIB をコンパイルします。

サポートされているMIBのリスト: xUPS MIB | 標準IETF UPS MIB (RFC 1628) | センサーMIB

サポートされているMIBsボタンを押して、MIBsをダウンロードします。

3.7.5.1.1 設定

この画面では、管理者がネットワークモジュールに情報を要求するためにMIBを使用するコンピューターのSNMP設定を行うことができます。

SNMP のデフォルトポートは、161 (SNMP v1 および v3、set/get) および 162 (traps) です。これらのポートは、設定画面で変更してセキュリティを強化することができます。

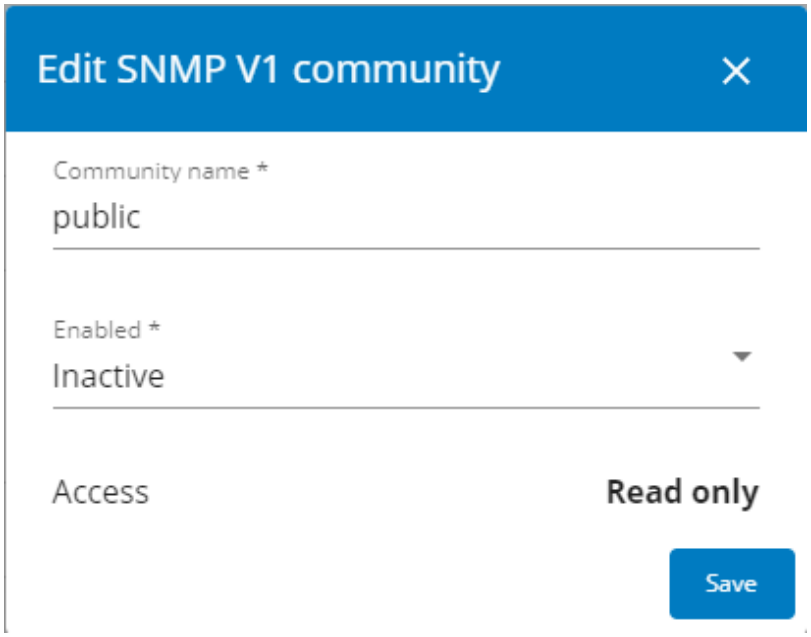
SNMP 設定を設定するには:

a SNMPエージェントを有効にする

これに加えて、v1および/またはv3を有効にし、適切なコミュニティおよびSNMP通信を可能にするための有効なユーザーアカウントを有効にする必要があります。

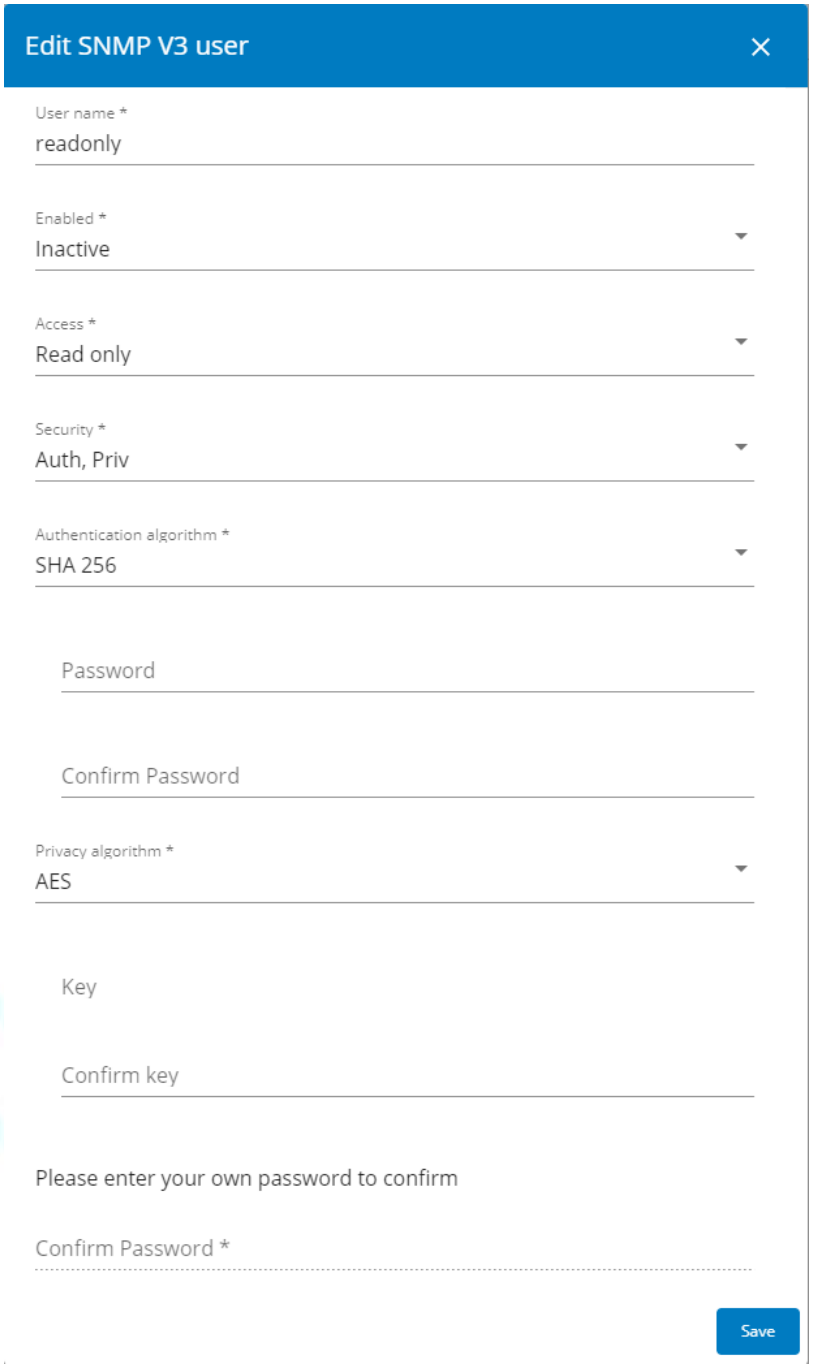
変更後に**保存**を押してください。

b SNMP V1 の設定を行う:



1. 読み取り専用または読み書きアカウントの編集アイコン をクリックして、設定にアクセスします。
2. SNMP Community Read-Only 文字列を入力します。ネットワークモジュールとクライアントは、通信するために同じコミュニティ名を共有する必要があります。
3. Enabled ドロップダウンリストで **Active** を選択して、アカウントをアクティブにします。
4. アクセスレベルは情報のみを表示するように設定されています。

c **SNMP V3 の設定を行う:**



1. 読み取り専用または読み書きアカウントの編集アイコン をクリックして、設定にアクセスします。

2. ユーザー名を編集します。

3. [有効]ドロップダウンリストで**[アクティブ]**を選択して、アカウントをアクティブにします。

4. アクセスレベルを選択します。

- **Read only**—ユーザーは認証とプライバシーを使用してSNMP変数にアクセスしません。
- **Read/Write**— SNMP 変数にアクセスするためには、認証を使用しなければなりませんが、プライバシーは使用しません。

5. Select the communication security mechanism.

- **Auth, Priv**—認証・プライバシーとの通信.
- **Auth, No Priv**—認証付きのプライバシーのない通信。
- **No Auth, No Priv**—認証やプライバシーのない通信。

6. 通信セキュリティ機構でAuthが選択されている場合は、認証アルゴリズムを選択します。

> AES192/AES256のプライバシーアルゴリズムでSHA256/SHA384/SHA512を設定することを
> お勧めします。

- **SHA**– SHA1はセキュリティが確保されていないのでお勧めできません。
- **SHA256**– パスワードとプライバシーキーを入力します。パスワードは 8 文字から 24 文字の間で，英数字と以下の特殊文字<>&@#%_=:;,./?|$*を組み合わせて使用します。
- **SHA384**– パスワードとプライバシーキーを入力します。パスワードは 8 文字から 24 文字の間で，英数字と以下の特殊文字<>&@#%_=:;,./?|$*を組み合わせて使用します。
- **SHA512**– パスワードとプライバシーキーを入力します。パスワードは 8 文字から 24 文字の間で，英数字と以下の特殊文字<>&@#%_=:;,./?|$*を組み合わせて使用します。

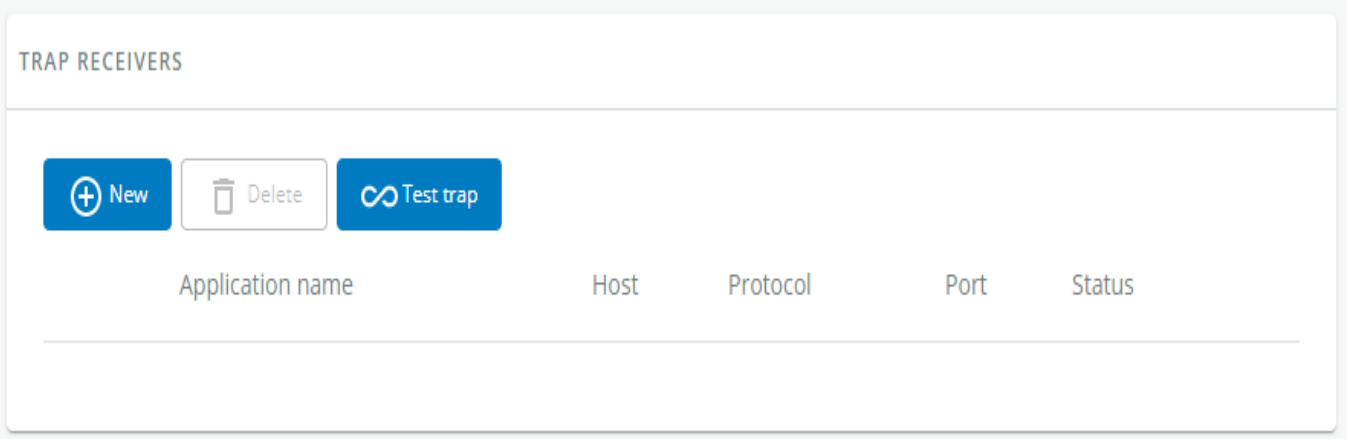
7. 通信セキュリティ機構でPrivが選択されている場合は、プライバシーアルゴリズムを選択します。

> SHA256/SHA384/SHA512認証アルゴリズムでAES192/AES256を設定することを推奨します。

- **AES**– パスワードとプライバシーキーを入力します。パスワードは 8 文字から 24 文字の間で、英数字と以下の特殊文字<>&@#%_=:;,./?|$*を組み合わせたものを使用します。
- **AES192**– パスワードとプライバシーキーを入力します。パスワードは 8 文字から 24 文字の間で，英数字と以下の特殊文字<>&@#%_=:;,./?|$*を組み合わせて使用します。
- **AES256**– パスワードとプライバシーキーを入力します。パスワードは 8 文字から 24 文字の間で，英数字と以下の特殊文字<>&@#%_=:;,./?|$*を組み合わせて使用します。

8. 自分のログインパスワードを入力し、**[保存]**をクリックします

3.7.5.2 トラップ受信機

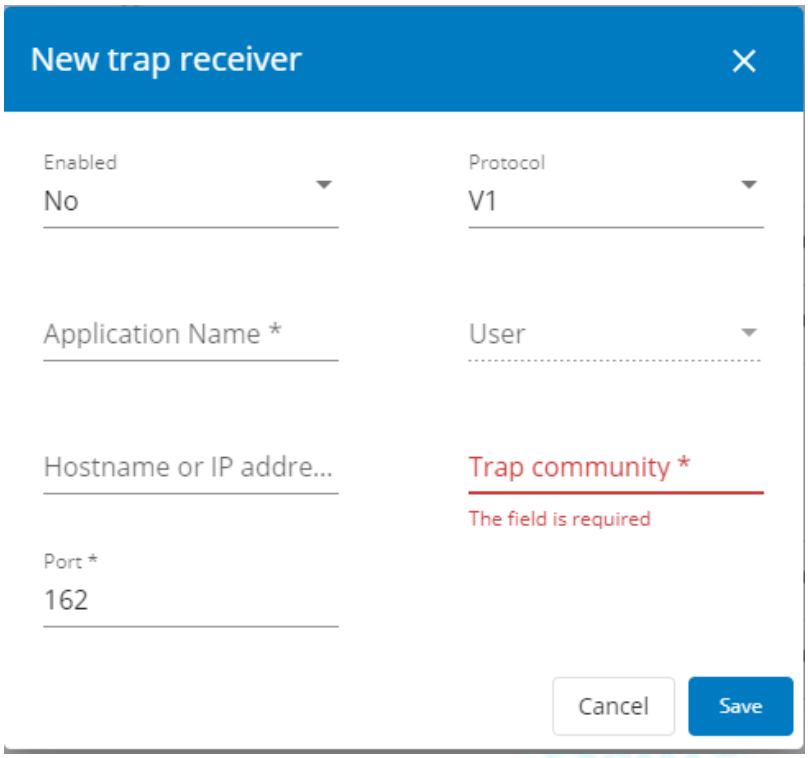


表はすべてのトラップ受信機を示しており、以下の詳細が含まれています。:

- **Application name**
- **Host**
- **Protocol**
- **Port**
- **Status:** Active/Inactive/Error(configuration error)

3.7.5.2.1 アクション

a 追加



1. **新規作成**ボタンを押して、新しいトラップ受信機を作成します。
2. 以下の設定を行ってください。:
   - Enabled – Yes/No
   - Application name
   - Hostname or IP address
   - Port
   - Protocol – V1/V3
   - Trap community (V1) / User (V3)
3. [**保存**] ボタンを押します。

b 削除

トラップ受信機を選択し、**削除**ボタンを押すと削除されます。

c 編集

ペンのアイコン✎を押して、トラップ受信機の情報を編集し、その設定にアクセスします。:

d テストトラップ

テストトラップボタンを押すと、すべてのトラップ受信機にテストトラップを送信しま

す。別ウィンドウでは、以下の値でテストの状態が表示されます。

- In progress
- Request successfully sent
- invalid type

SNMPトラップコードの詳細については次を参照してください。Information>>>SNMP traps

3.7.5.3 SNMPトラップへのリンク

- UPS Mib
- ATS Mib
- Sensor Mib

3.7.5.4 デフォルト設定と可能なパラメーター –SNMP

	Default setting	Possible parameters
SNMP	Activate SNMP – disabled Port – 161 SNMP V1 – disabled • Community #1 – public Enabled – Inactive Access – Read only • Community #2 – private Enabled – Inactive Access – Read/Write SNMP V3 – enabled • User #1 – readonly Enabled – Inactive Access – Read only Authentication – Auth (SHA-1) Password – empty Confirm password – empty Privacy – Secured – AES Key – empty Confirm key – empty • User#2 – readwrite Enabled – Inactive Access – Read/Write Authentication – Auth (SHA-1) Password – empty Confirm password – empty Privacy – Secured – AES Key – empty Confirm key – empty	Activate SNMP – disable/enable Port – x-xxx SNMP V1 – disable/enable • Community #1 – 128 characters maximum Enabled – Inactive/Active Access – Read only • Community #2 – 128 characters maximum Enabled – Inactive/Active Access – Read/Write SNMP V3 – disable/enable • User #1 – 32 characters maximum Enabled – Inactive/Active Access – Read only/Read-Write Authentication – Auth (SHA-1)/None Password – 128 characters maximum Confirm password – 128 characters maximum Privacy – Secured – AES/None Key – 128 characters maximum Confirm key – 128 characters maximum • User#2 – 32 characters maximum Enabled – Inactive/Active Access – Read only/Read-Write Authentication – Auth (SHA-1)/None Password – 128 characters maximum Confirm password – 128 characters maximum Privacy – Secured – AES/None Key – 128 characters maximum Confirm key – 128 characters maximum
Trap receivers	No trap	Enabled – No/Yes Application name – 128 characters maximum Hostname or IP address – 128 characters maximum Port – x-xxx Protocol – V1 Trap community – 128 characters maximum

3.7.5.4.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.5.5 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
SNMP	✓	✗	✗

3.7.5.5.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.5.6 トラブルシューティング

保存と復元でのSNMPv3パスワード管理の問題

影響を受けるFWのバージョン
この問題は、1.7.0以前のバージョンで行われたSNMP**設定**を1.7.0以上のバージョンで適用した場合に影響します。

症状
1.7.0以上のバージョンで設定を復元した後、SNMPv3接続が正常に動作しません。

原因
1.7.0以前のSNMPv3の**設定**を行っています。
その場合、SNMPv3の設定がSaveやRestoreの設定でうまく管理されていません。

処置方法
バージョン1.7.0以上のSNMPv3ユーザーとパスワードを**再設定**し、設定を保存します。 SNMPv3設定は、以下のようにして復元することができます。

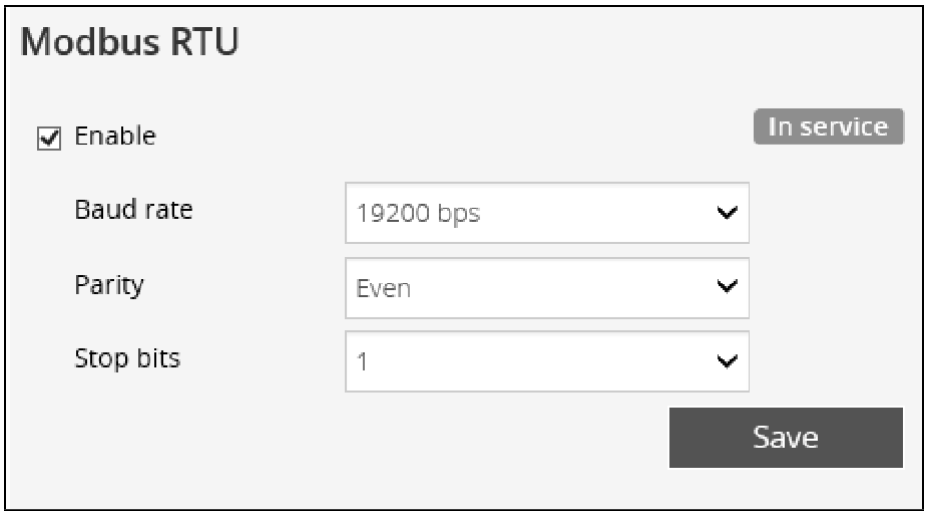
3.7.5.6.1 その他の問題については

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.7.6 Modbus

このセクションはModbusネットワークモジュールINDGWのみを対象としています。
Modbus RTUの接続方法についてはセクションを参照してください。Installing the Network Management Module>>>Wiring the RS-485 Modbus RTU terminal>>>Configuring the termination.
Modbusの設定方法については、以下のセクションを参照してください。
Installing the Network Management Module>>>Configuring Modbus
.

3.7.6.1 Modbus RTU



以下のModbus RTU設定が可能です。:

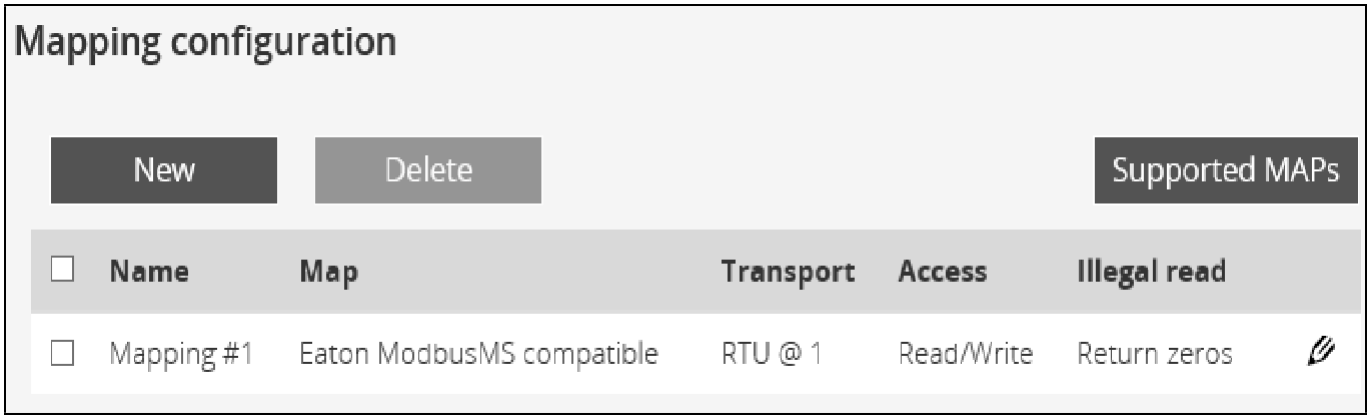
- **Enable**
- **Baud rate**
- **Parity**
- **Stop bits**

3.7.6.2 Modbus TCP

以下のModbus TCP設定が可能です:

- **Enable**
- **Port**

3.7.6.3 マッピング設定



3.7.6.3.1 マッピング設定テーブル

表は、すべてのマッピング構成を示しており、以下の詳細が含まれています。:

- **Name**
- **Map**
- **Transport**
- **Access**
- **Illegal read behaviour**
- **Coil/register base address shift**

3.7.6.3.2 アクション

a 追加

[New] ボタンを押して、新しいマッピング構成を作成します。

b 削除

マッピング構成を選択し、**[削除]**ボタンを押して削除します。

c 編集

ペンのロゴ を押して、マッピング設定を編集します。

以下の設定にアクセスできるようになります。

- Name
- Map
- Transport
- Device ID
- Access
- Illegal read behaviour
- Coil/register base address shift

d サポートされているMAP

対応MAPボタンを押すと、MAPをダウンロードすることができます。

コイル/レジスタのベースアドレスシフトが "Shift by 1 (JBUS) "に設定されている場合、生成ファイルに反映されません

ファイルはリアルタイムで生成され、生成時のデバイスの能力と値を考慮に入れます。
ダウンロードされたファイルの表は、すべての可能なレジスタを表示しますが、システムでサポートされるのは、Trueに等しいAvailableを示すものだけです。

テーブルの内容をマッピングする:

- Address (hex): 16進数レジスタアドレス
- Address (1-base): 1ベース形式のレジスタアドレス
- Type: Register/Discrete
- Size in bytes
- Number of Modbus registers
- Writable: True/False
- Representation: Int16/Uint16/String/Boolean/...
- Name
- Description
- Unit
- Status to 0: レジスタが0になったときの状態
- Status to 1: レジスタが1になったときの状態
- Available: True/False -現在のデバイスでレジスタが使用可能かどうかを表示します
- Value: 現在のデバイスのレジスタの現在の値を表示します。

3.7.6.4 デフォルト設定と可能なパラメーター -Modbus

この設定はModbusネットワークモジュールINDGWのみの設定です。

	Default setting	**Possible parameters**
Modbus RTU	Enabled — Inactive Baud rate (bps) — 19200 Parity — Even Stop bits - 1	Enabled — Inactive/Active Baud rate (bps) — 1200/2400/4800/9600/19200/38400/57600/115200 Parity — None/Even/Odd Stop bits - 1/2
Modbus TCP	Enabled — Inactive Port — 502	Enabled — Inactive/Active Port — x-xxx
Mapping configuration	No mapping	Name - 128 characters maximum Map - Eaton ModbusMS compatible Transport - RTU/TCP Device ID - from 1 to 247 Access - None/Read only/Read/Write Illegal read behaviour - Return exception/Return zeros Coil/register base address shift - No shift/Shift by 1 (JBUS)

3.7.6.4.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.6.5 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Modbus*	✓	✗	✗

**for INDGW only*

3.7.6.5.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.6.6 CLI コマンド

modbus_message_display

このセクションはModbusネットワークモジュールINDGWのみを対象としています。

説明

modbus_message_displayはサーバーを再起動してModbusメッセージを表示します。このコマンドにより、Modbusサーバーが期待通りに動作していることを確認することができます。

ヘルプ

```
modbus_message_display
  --help  Restart server and display modbus message
  -h      Restart server and display modbus message
```

modbus_statistics

このセクションはModbusネットワークモジュールINDGWのみを対象としています。

説明

modbus_statisticsはModbus RTUとTCPのステータスとサーバーの統計情報を表示します:

- Bus character overrun count
- Bus frame error count
- Bus parity error count
- Buffer overrun count

- Bus message count
- Valid message count
- CRC error count

- Incoming message count
- Discarded message count
- Processed message count
- Success returned count
- Exception returned count

ヘルプ

```
modbus_statistics
                      Display modbus server statistics

        -h, --help       Display the help page.
        -r, --reset      Reset modbus server statistics.
                         The counter from A1.1 to A1.4 are reset only at startup of the
server.
```

3.7.6.6.1 その他のCLIコマンドの場合

次のCLIコマンドを参照してください。Information>>>CLI

3.7.6.7 トラブルシューティング

Modbus通信がうまくいかない

症状

- 通信がうまくいかない

テスト情報を得るために次のModbusの設定を参照してください。
Servicing the Network Management Module>>>Configuring Modbus

考えられる原因

- 通信パラメーターが正しくありません。

通信パラメーターが目的の設定になっていることを確認してください。

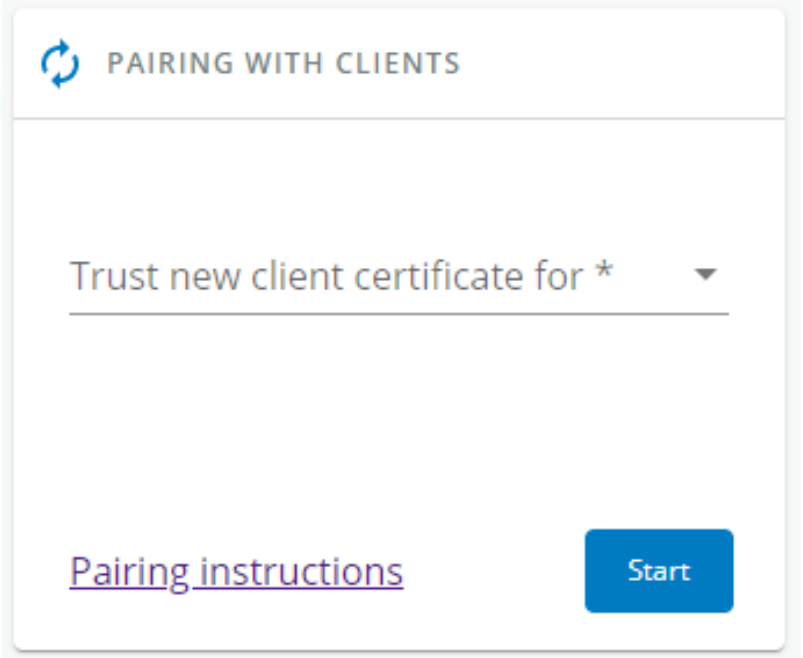
3.7.6.7.1 その他の問題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.7.7 証明書

3.7.7.1 クライアントとのペアリング

ペアリング手順の詳細については、タイル内のリンクペアリング手順に従うか、または次を参照してください。
Servicing the Network Management Module>>>*Pairing agent to the Network Module*



選択された時間枠の間、ネットワークモジュールへの新しい接続は自動的に信頼され、受け入れられます。

自動承認後、リストされたすべてのクライアントがインフラストラクチャに属していることを確認してください。そうでない場合は、[削除] ボタンを使用してアクセスを取り消すことができます。

この自動受諾の使用は、安全で信頼できるネットワークに限定してください。

最大限のセキュリティを確保するには、証明書の設定ページで以下の 2 つの方法のいずれかを実行することをお勧めします。:

- エージェントの証明書を手動でインポート
- 独自のPKIを使用してエージェントとネットワークモジュールの両方に信頼できる証明書を生成する

3.7.7.1.1 アクション

a Start

選択した時間枠の間、または停止するまでペアリングウィンドウを起動しま

す。タイムカウントダウンが表示されます。

b Stop

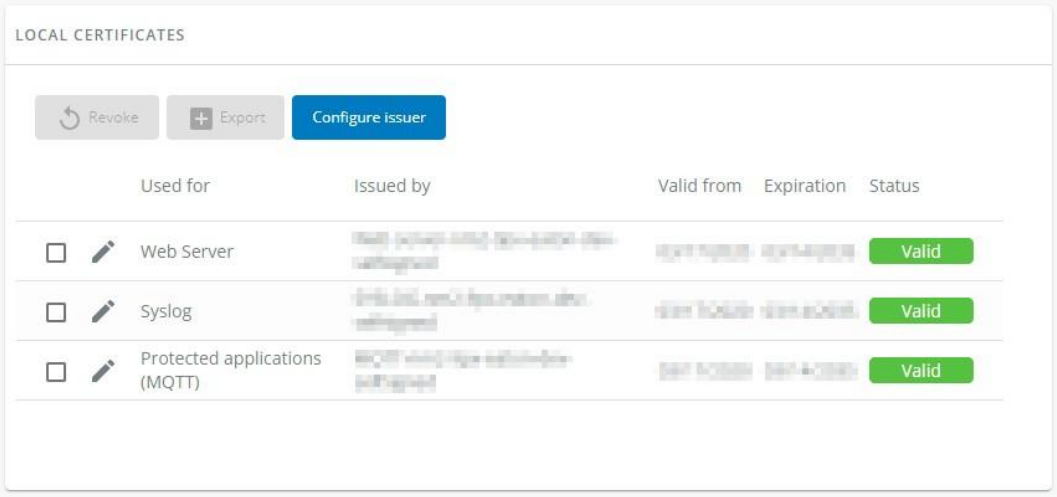
ペアリングウィンドウを停止します。

3.7.7.2 ローカル証明書

ローカル証明書の管理 :

- CA が署名した CSR およびインポート証明書を生成する。
- 新しい自己署名証明書の生成

3.7.7.2.1 ローカル証明書テーブル



表は、各ローカル証明書について以下の情報を示しています。

- Used for
- Issued by
- Valid from
- Expiration
- Status — valid, expires soon, or expired

3.7.7.2.2 アクション

a Revoke

この操作により、選択した証明書が使用されなくなります。

失効させる証明書を選択して、**[失効]**ボタンを押します。

確認画面が表示されます。「続行」を押して続行すると、この操作は復旧できません。

Revoke は、現在の証明書を新しい自己署名証明書に置き換えます。これにより、接続されているアプリケーションが切断される可能性があります。
– ウェブブラウザ
– シャットダウンアプリケーション
– モニタリングアプリケーション
リボークアクションで持ち出された証明書は回収できません。

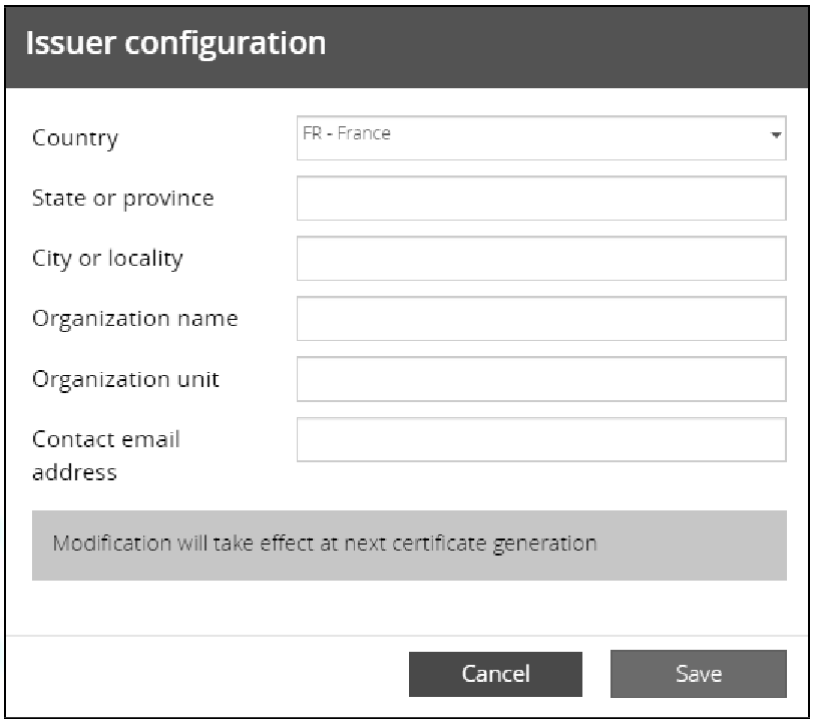
b Export

選択した証明書をOSのブラウザウィンドウにエクスポートします。

c 発行者の設定

Configure issuer**[発行者の設定]**ボタンを押します。

発行者データを編集するための設定ウィンドウが表示されます。



- Common name (CN)
- Country (C)
- State or Province (ST)
- City or Locality (L)
- Organization name (O)
- Organization unit (OU)
- Contact email address

[Save(保存)]ボタンを押す。

発行者設定は、証明書の失効後にのみ適用されます。

d 編集

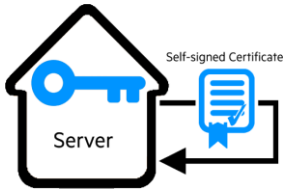
ペンのロゴ を押す:

以下のようなアクセスを得ることができます。:

- 証明書の概要

- アクション
  新しい自己署名証明書を生成します。CSRを生成します。
  証明書のインポート（CSRが生成された場合のみ利用可能
- 詳細

e 新しい自己署名証明書を生成する



選択した証明書を新しい自己署名証明書に置き換えること。

これにより、Web ブラウザ、シャットダウンアプリケーション、監視アプリケーションなどのアプリケーシ

ョンが切断されることがあります。この操作は復旧できません。

f 新しい証明書の作成:

g CSR

証明書版のGenerate Signing Request**[署名要求の生成]**ボタンを押します。CSRが自動的にダウンロードされます。
CSRは、カードの外部で管理されているCAで署名する必要があります。

h インポート証明書

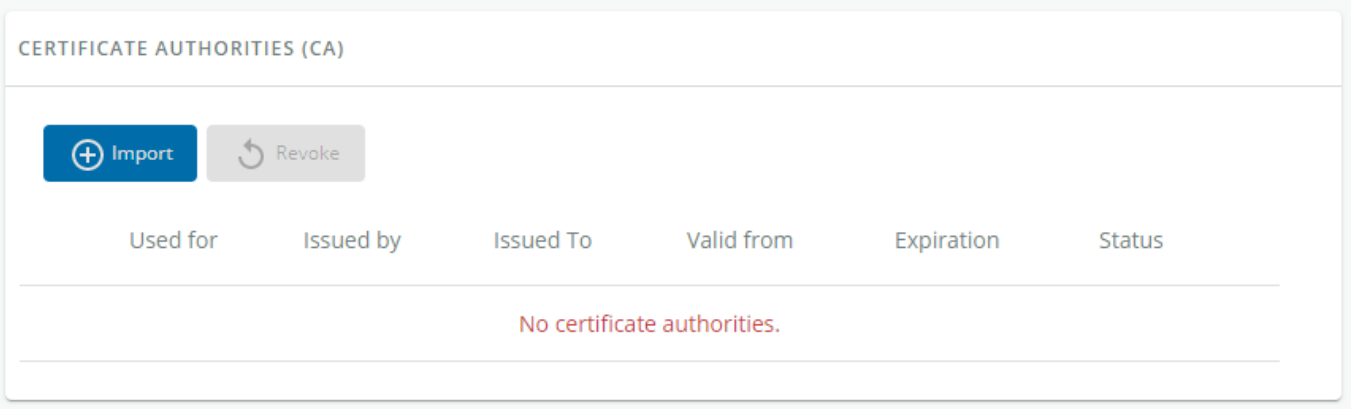
CSR が CA によって署名されると、それをネットワークモジュールにインポートできます。

インポートが完了すると、新しいローカル証明書情報がテーブルに表示されます。

3.7.7.3 認証局（CA）

CAの管理.

3.7.7.3.1 CAテーブル



この表には、以下の詳細が記載された認証局が表示されます。:

- Used for
- Issued by
- Issued to
- Valid from
- Expiration
- Status — valid, expires soon, or expired

3.7.7.3.2 アクション

a Import

CAをインポートする際には、関連するサービスを選択する必要があり、OSのブラウザ画面からアップロード処理を開始することができます。

b Revoke

取り消す証明書を選択し、**[Revoke（取り消し）]** ボタンを押します。

確認ウィンドウが表示されますので、[続行] を押して進むと、この操作は復元できません。

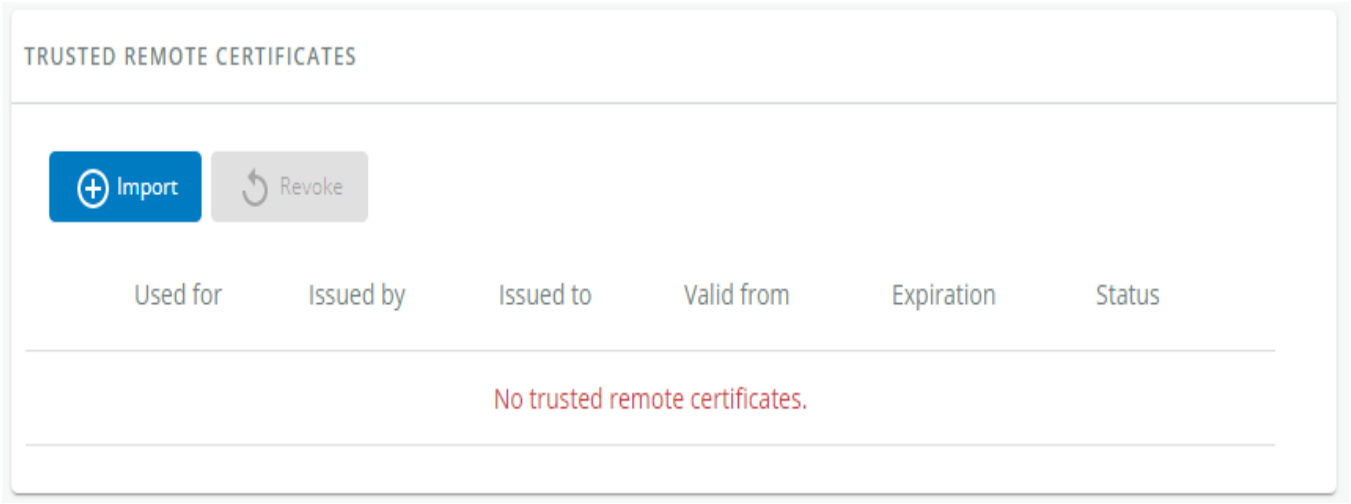
Export

選択した証明書をOSのブラウザウィンドウにエクスポートします。.

c Edit

ペンのロゴを押すと、証明書のサマリーにアクセスできます。:

3.7.7.4 信頼されたリモート証明書



表は、各信頼されたリモート証明書について以下の情報を示しています。.

- Used for
- Issued by
- Issued to
- Valid from
- Expiration
  証明書の有効期限が切れた場合、クライアントとの接続は失われます。この場合、ユーザーは接続と関連する証明書を再作成する必要があります。
- Status ―有効期限切れ

3.7.7.4.1 アクション

a Import

クライアント証明書をインポートする際には、関連するサービスを選択する必要があり、OSのブラウザウィンドウからアップロード処理を開始することができます。

b Revoke

取り消す証明書を選択し、[Revoke（取り消し）]ボタンを押します。

確認ウィンドウが表示されますので、[続行] を押して進むと、この操作は復元できません。

c Edit

ペンのロゴを押して証明書の概要を表示:

3.7.7.5 デフォルト設定と可能なパラメーター –証明書

	Default setting	Possible parameters

Local certificates	Common name — Service + Hostname + selfsigned Country — FR State or Province — 38 City or Locality — Grenoble Organization name — Eaton Organization unit — Power quality Contact email address — blank	Common name — 64 characters maximum Country — Country code State or Province — 64 characters maximum City or Locality — 64 characters maximum Organization name — 64 characters maximum Organization unit — 64 characters maximum Contact email address — 64 characters maximum

3.7.7.5.1 その他の設定について

その他の設定については次を参照してください。Information>>>Default settings parameters

3.7.7.6 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Certificate	✓	✗	✗

3.7.7.6.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.7.7.7 CLIコマンド

certificates

説明

CLI を通じて証明書を管理することができます。

ヘルプ

```
certificates <target> <action> <service_name>
  <target> :
        - local
  <action> :
        - print: provides a given certificate detailed information.
        - revoke: revokes a given certificate.
        - export: returns a given certificate contents.
        - import: upload a given certificate for the server CSR. This will replace the
CSR with the certificate given.
        - csr: get the server CSR contents. This will create the CSR if not already
existing.
  <service_name>: mqtt/syslog/webserver
```

使用例

From a linux host:

print over SSH: sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local print $SERVICE_NAME **revoke over SSH:** sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local revoke $SERVICE_NAME

export over SSH: sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local export $SERVICE_NAME
import over SSH: cat $FILE | sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local import $SERVICE_NAME

csr over SSH: sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local csr mqtt

From a Windows host: (plink tools from putty is required)

print over SSH: plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch certificates local print $SERVICE_NAME
revoke over SSH: plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch certificates local revoke $SERVICE_NAME

export over SSH: plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch certificates local export $SERVICE_NAME **import over SSH:** type $FILE | plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch certificates local import
$SERVICE_NAME

csr over SSH: plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch certificates local csr mqtt

Where:

- $USER is user name (the user shall have administrator profile)
- $PASSWORD is the user password
- $PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- $CARD_ADDRESS is IP or hostname of the card
- $FILE is a certificate file
- $SERVICE_NAME is the name one of the following services : mqtt / syslog / webserver.

3.7.7.7.1 その他のCLIコマンドの場合

次のCLIコマンドを参照してください。Information>>>CLI

3.7.7.8 トラブルシューティング

ソフトウェアがネットワークモジュールと通信できない

症状

- ネットワークモジュールで次を確認するとエージェントのステータスが ″Lost ″と表示されます。

  Contextual help>>>Protection>>>Agent list>>>Agent list table
- ネットワークモジュールで次を確認すると保護されたアプリケーション(MQTT)のステータスが「まだ有効ではありません」と表示されます。
  Contextual help>>>Settings>>>Certificate>>>Trusted remote certificates , t
- IPP/IPMでは、″認証に失敗しました″、″通知受信でエラーが発生しました ″と表示されます。.

考えられる原因

IPP/IPM 証明書がネットワークモジュールで有効でない。

IPP/IPMとネットワークモジュールの証明書が一致していないため、ネットワークモジュールとシャットダウンエージェント間の接続の認証と暗号化が機能しません。

セットアップ

IPP/IPM証明書は、セットアップではありません。IPP/IPM が起動します。

ネットワークモジュールがUPSに接続され、ネットワークに接続されます。

アクション #1

ネットワークモジュールの IPP/IPM 証明書の有効性を確認します。.

STEP 1: ネットワークモジュールへの接続

- ネットワークコンピューターでサポートされているWebブラウザを起動します。
  ブラウザウィンドウが表示されます。
- Address/Location フィールドに、https://xxx.xxx.xxx.xxx/ と入力します。xxx.xxx.xxx.xxx はネットワークモジュールのスタティック IP アドレスです。
- ログイン画面が表示されます。
- User Name(ユーザー名)フィールドにユーザー名を入力します。
- Password(パスワード)フィールドにパスワードを入力します。
- **[Login(ログイン)]** をクリックします。Network Module Web インターフェースが表示されます。

STEP 2: Settings/Certificates(設定/証明書) ページに移動します。

STEP 3: [信頼されたリモート証明書]セクションで**保護されたアプリケーション(MQTT)**のステータスを確認します。

それが **″有効 ″**である場合は、Action#2STEP2に進み、それが**″まだ有効ではない ″**場合はIPP/IPMと同期する必要があるの時間。

STEP 4: IPP/IPMとネットワークモジュールの時間を同期させ、**保護されたアプリケーション(MQTTT)**のステータスが有効になったことを確認します。

通信が回復しない場合は、Action#2STEP2に進みます。

Action #2

ネットワークモジュールにエージェントを自動受付けでペアリングします(安全で信頼できるネットワークにインストールする場合にお勧めします)。

手動ペアリング(最大のセキュリティ)を行うには下記から、STEP2の項目1に進みます。
Servicing the Network Management Module>>>*Pairing agent to the Network Module*

STEP 1: ネットワークモジュールへの接続

- ネットワークコンピューターでサポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。
- [Address/Location] フィールドにhttps://xxx.xxx.xxx.xxx/ xxx.xxx.xxx.xxxと入力します。xxx.xxx.xxx.xxx は
  ネットワークモジュールのスタティックIPアドレスです。

- ログイン画面が表示されます。
- User Name（ユーザー名）フィールドにユーザー名を入力します。
- [パスワード]フィールドにパスワードを入力します。
- Login をクリックします。Network Module Web インターフェースが表示されます。

STEP 2: 保護/エージェントのリストページに移動します。

STEP 3: シャットダウンエージェントとのペアリングセクションで、新しいエージェントを受け入れる時間を選択し、**[Start（スタート）]** ボタンを押して **[Continue]** を押します。選択した時間枠の間、ネットワークモジュールへの新しいエージェント接続は自動的に信頼され、受け入れられます

STEP 4: 新しいエージェントを受け入れる時間がネットワークモジュール上で実行されている間、**エージェント(IPP/IPM)に対するアクション** Eaton¥IntelligentPowerProtector¥configs¥tlsフォルダ内のネットワークモジュール証明書ファイル*.0を削除します。

カードのタイムスタンプが間違っていると、ソフトウェア上で「完全な取得に失敗しました」というエラーメッセージが表示されます。

症状:

IPP/IPMでは、資格情報が正しくても「完全なデータ取得に失敗しました」というエラーメッセージが表示されます。

考えられる原因:
ネットワークモジュールのタイムスタンプが正しくありません。
おそらくネットワークモジュールの日付ではMQTT証明書は有効ではありません。

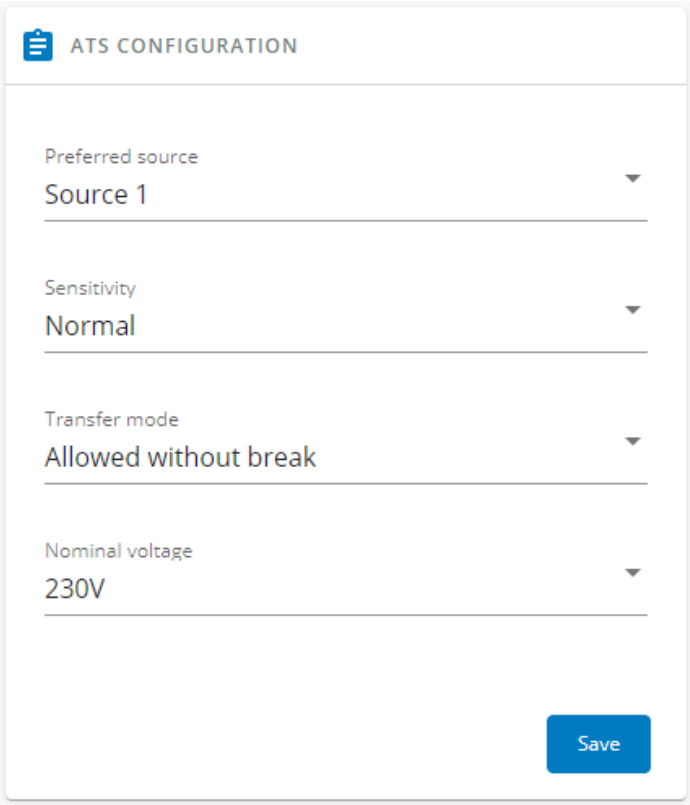
対処法:
ネットワークモジュールの日付にMQTT証明書が有効でない可能性があります。

正しい日付、時刻、タイムゾーンを設定してください。可能であれば、NTPサーバーを使用してください。Contextual help>>>Settings>>>General>>>System details>>>Time & date settings section.

3.7.7.8.1 その他の問題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.7.8 ATS



このセクションはATSデバイスのみを対象としており、すべての設定が含まれています。

- **Prefered source** –ソース1またはソース2の優先度を設定します（デフォルトではソース1）。
- **Sensitivity** –入力主電源検出の感度モードを設定します（デフォルトは通常感度、歪んだ波形に対応するために低感度）。
- **Transfer mode** –ソース間の転送モードを設定します（デフォルトでは、ソースが同期していない場合でも追加ブレークなしのStandard、ソースが同期していない場合は転送中に追加ブレークありのGap）。
- **Nominal voltage** –電圧しきい値を設定します。

3.7.8.1 特記事項

3.7.8.2 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
ATS	✓	✓	✗

3.7.8.2.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.8 メンテナンス

3.8.1 システム情報

システム情報は、主なネットワークモジュール情報の概要です。[COPY TO CLIPBOARD（クリップボードへコピー）] ボタンは、情報をクリップボードにコピーします。

3.8.1.1 識別

- System name –このフィールドを埋めると、トップバーのデバイスモデル名に置き換わります。
- Product
- Physical name
- Vendor
- UUID
- Part number
- Serial number
- Hardware version
- Location
- Contact
- MAC address

3.8.1.2 ファームウェア情報

- Version
- SHA
- Build date
- Installation date
- Activation date
- Bootloader version

3.8.1.3 プロファイルごとのアクセス権

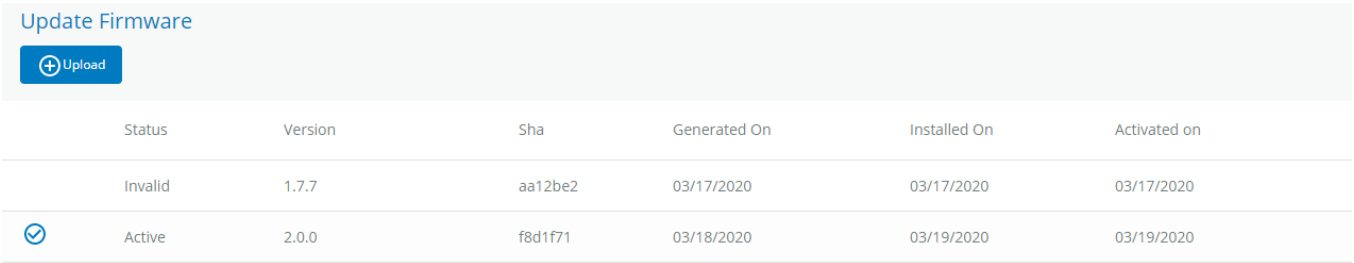
	Administrator	Operator	Viewer
System information	✓	✓	✓

3.8.1.3.1その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.8.2 ファームウェア

3.8.2.1 ファームウェアのアップデート



- 2 つの内蔵ファームウェアの情報を監視します。
- ネットワークモジュールのファームウェアをアップグレードする

3.8.2.1.1 ファームウェア情報

a Status

- Uploading
- Invalid
- Valid
- Pending reboot
- Active

b Version/Sha

関連するファームウェアのバージョンと関連する Sha.

c Generated on

ファームウェアのリリース日を表示します。

より良いパフォーマンス、セキュリティ、および最適化された機能のために、イートンはネットワークモジュールを定期的にアップグレードすることを推奨します。

d Installation on

ネットワークモジュールにファームウェアがインストールされたときに表示されます。

e Activated on

ネットワークモジュールでファームウェアがアクティベートされたときに表示されます。.

3.8.2.2 ネットワークモジュールのアップグレード

アップグレードプロセス中、ネットワークモジュールはデバイスのステータスを監視しま

せん。ファームウェアをアップグレードするには:

1. ウェブサイトから最新のファームウェアバージョンをダウンロードしてください。詳

   細については次を参照して下さい。

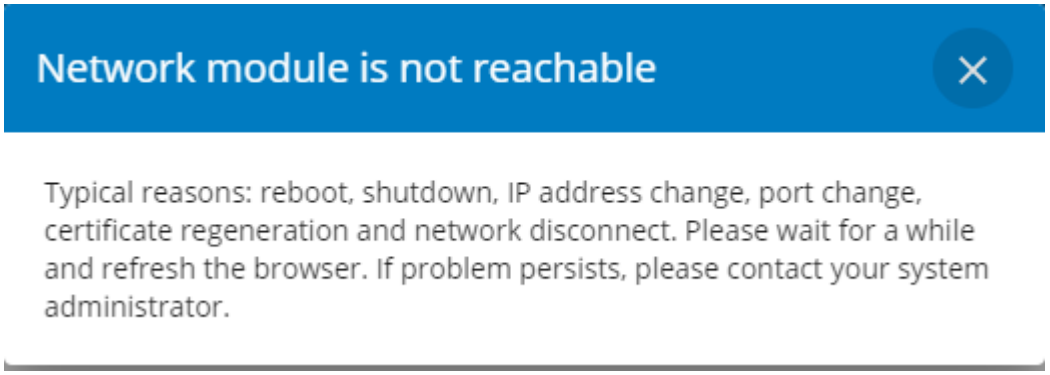
   Servicing the Network Management Module>>>Accessing to the latest Network Module firmware/driver
2. **[+Upload(アップロード)]**をクリック。
3. **[Choose file(ファイルを選択)]**をクリックし、ダウンロードしたファームウェアを保存したフォルダに移動して、ファームウェアパッケージを選択します。
4. **[Upload(アップロード)]**をクリックします。アップロードには最大5分かかります。

アクティブではなかったファームウェアは、この操作で消去されます。

アップグレードが進行中の場合、**[Upload(アップロード)]**ボタンは無効になり、進行要素は次の手順で表の下に表示されます。:

Transferring > Verifying package > Flashing > Configuring system > Rebooting

ファームウェアのアップロードが成功すると確認メッセージが表示され、ネットワークモジュールは自動的に再起動します。



Web ブラウザを閉じたり、操作を中断したりしないでください。ネットワーク構成によっては、ネットワークモジュールが異なる IP アドレスで再起動することがあります。ログインページにアクセスするには、ネットワークモジュールの再起動時間後にブラウザをリフレッシュします。F5 または CTRL+F5 を押してブラウザを空にし、Web ユーザー インターフェースに表示されるすべての新機能を取得します。「通信が失われた」と「通信が回復した」は次に表示されることがあります。Contextual help>>>Alarms

3.8.2.3 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Firmware	✓	✗	✗

3.8.2.3.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles.

3.8.2.4 CLIコマンド

get release info

説明

ファームウェアのリリースに関する基本情報を表示します。

ヘルプ

```
get_release_info
  -d  Get current release date
  -s  Get current release sha1
  -t  Get current release time
  -v  Get current release version number
```

3.8.2.4.1 その他のCLIコマンドについて

次のCLIコマンドを参照してください。Information>>>CLI

3.8.2.5 トラブルシューティング

ファームウェアのアップグレード後、ネットワークモジュールの起動に失敗する。

考えられる原因

IP アドレスが変更された.

Note: ファームウェアのフラッシュ中にアプリケーションが破損している場合、例えばファームウェアのフラッシュ中に中断が発生した場合、ブートは以前のファームウェアで行われます。

アクション

IPアドレスを回復してカードに接続します。.

次を参照して下さい。

Installing the Network Management Module>>>Accessing the Network Module>>>Finding and setting the IP address

FWアップグレード後のWebユーザーインターフェースが最新ではない

症状

アップグレード後:

- Web インターフェースが最新ではありません
- 新FWの新機能は表示されない

考えられる原因

ブラウザは、過去のFWデータを含むキャッシュを介してWebインターフェースを表示しています。

アクション

F5 または CTRL+F5 を使用してブラウザのキャッシュを空にします。

3.8.2.5.1 その他の問題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.8.3 サービス

3.8.3.1 サービスオプション

3.8.3.1.1 サニタイズ

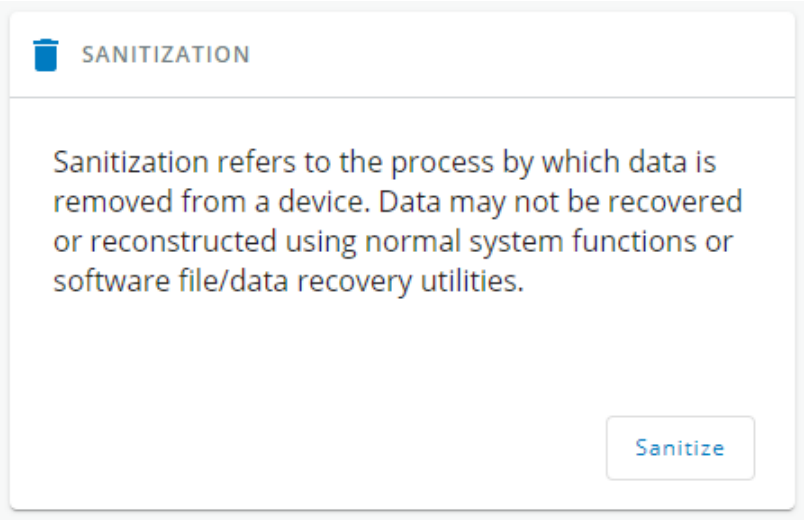
サニタイズによりすべてのデータが削除され、ネットワークモジュールは工場出荷時のデフォルト設定に戻ります。.

初期設定の詳細については次を参照してください。Information>>>Default settings parameters

ネットワークモジュールをサニタイズするには:

1. **[Sanitize（サニタイズ）]**をクリックします。.

確認メッセージが表示されますので、**[Sanitize（サニタイズ）]**をクリックして確認します。



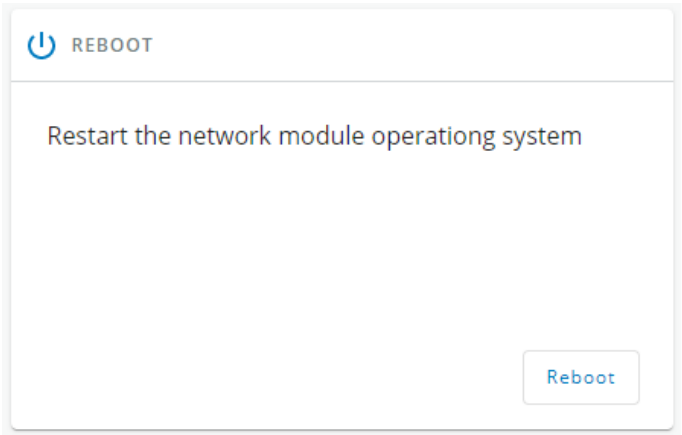
ネットワーク構成によっては、ネットワークモジュールが別の IP アドレスで再起動することがあります。メイン管理者ユーザーだけがデフォルトのログインとパスワードで残ります。ログインページにアクセスするには、ネットワークモジュールの再起動後にブラウザをリフレッシュしてください。

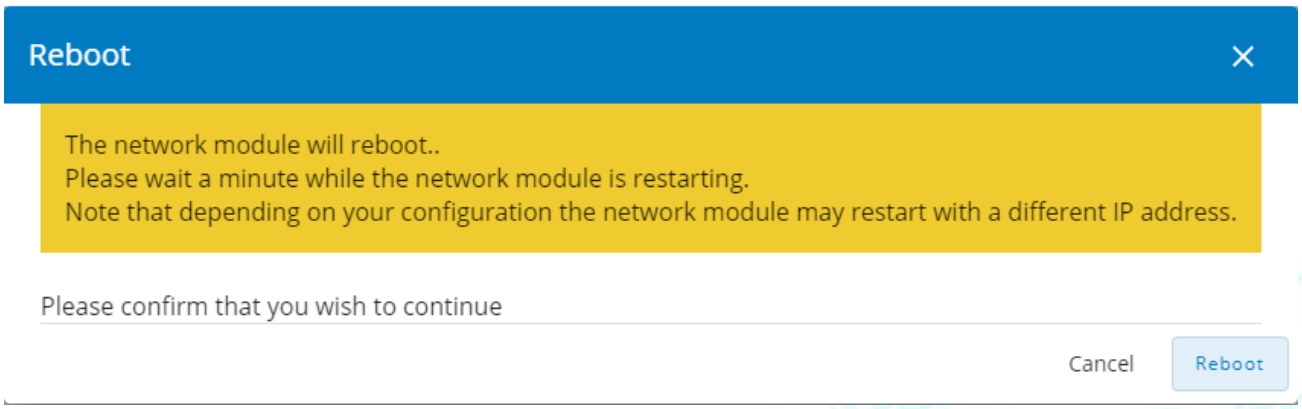
3.8.3.1.2 リブート（再起動）

リブート（再起動）とは、ネットワークモジュールのオペレーティングシステムを再起動することを意味します。ネットワークモジュールを再起動するには

[Reboot（再起動）]をクリックします。

確認メッセージが表示されますので、**[Reboot（再起動）]**をクリックして確認します。



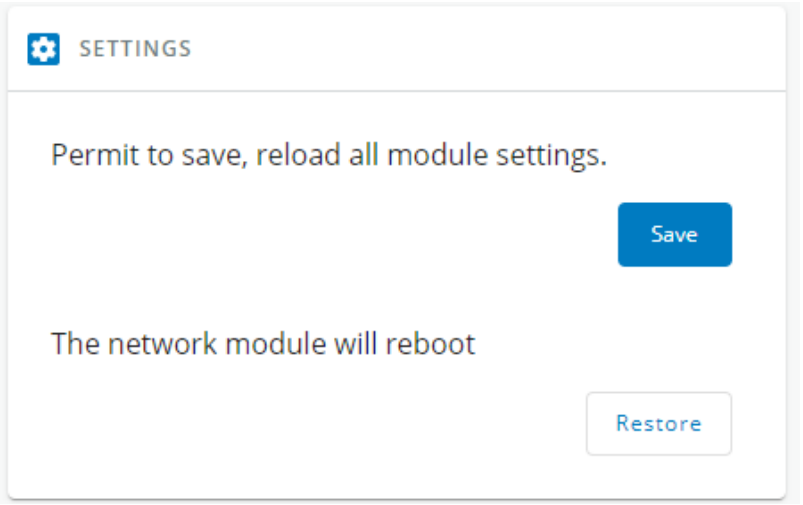


ネットワーク設定によっては、ネットワークモジュールが異なる IP アドレスで再起動することがあります。ログインページにアクセスするには、ネットワークモジュールの再起動時間後にブラウザをリフレッシュしてください。通信が失われた」と「通信が回復した」は「アラーム」セクションに表示されることがあります。

3.8.3.1.3 設定

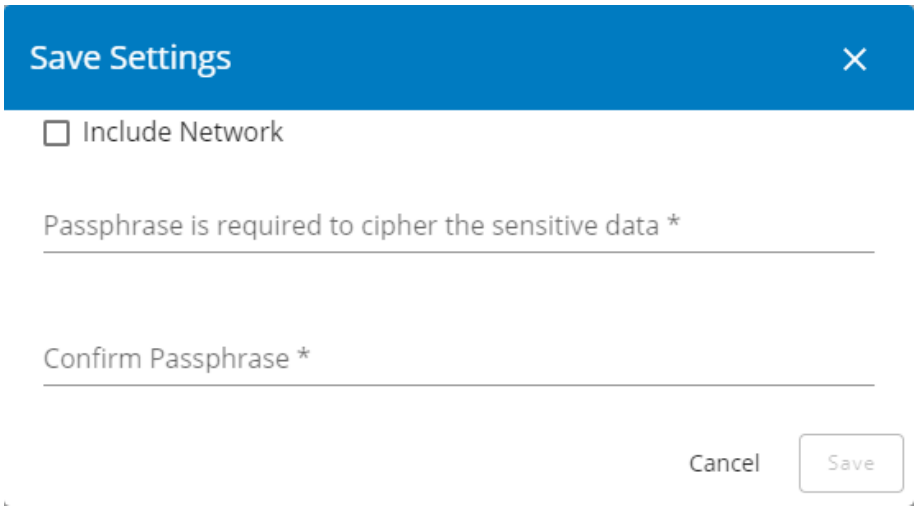
ネットワークモジュールの設定の保存と復元を許可する

詳細については、以下を参照してください。
Servicing the Network Management Module>>>Saving/Restoring/Duplicating



3.8.3.1.4 保存

以下の設定は保存されません。
メイン管理者以外のローカルユーザーセンサー設定（試運転、アラーム設定）

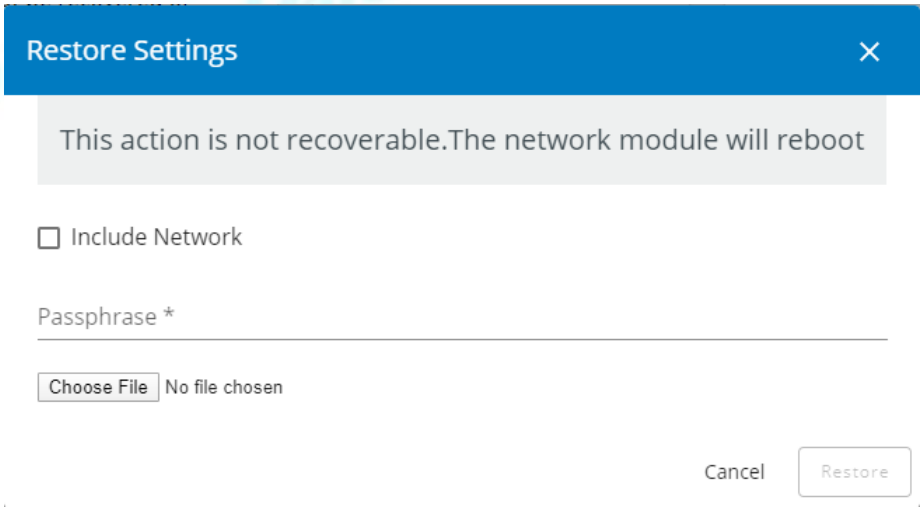


ネットワークモジュールの設定を保存するには:

1. **[Save（保存）]**をクリック。
2. 必要に応じてネットワーク設定を含めるように選択します。
   パスフレーズは、機密データを暗号化するために2回入力する必要があります。
3. **[Save（保存）]**をクリック。

3.8.3.1.5 復元

設定を復元すると、ネットワークモジュールが再起動することがあります。



ネットワーク モジュールの設定を復元するには:

1. **[Restore（復元）]**をクリック。
2. 必要に応じて、ネットワーク設定を含めるように選択します。
3. ファイル保存時に使用したパスフレーズを入力します。
4. **[Choose file（ファイルを選択）]**をクリックして、JSONファイルを選択します。

5. [Restore（復元）]をクリックして確認します。

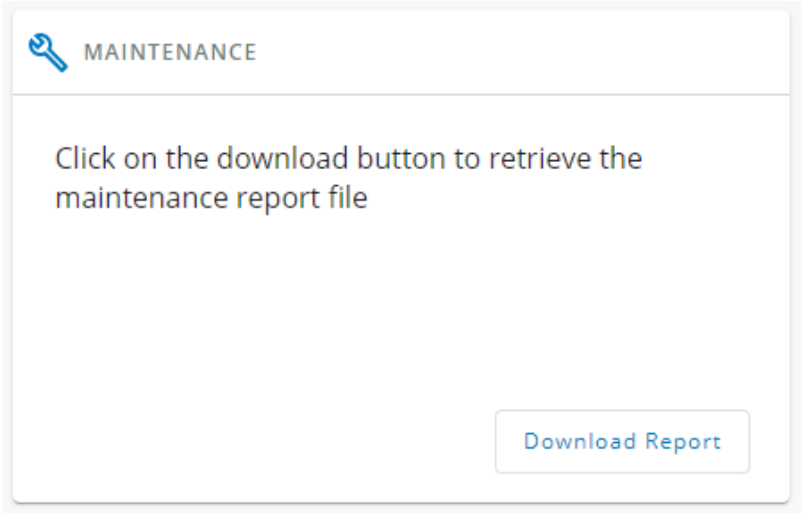
3.8.3.1.6 メンテナンス

メンテナンスレポートは、サービス担当者がネットワークモジュールの問題を診断するために使用するためのものです。それは、ファイルがパスワードで保護されている理由は、それがユーザーのために意図されていません。

メンテナンスレポートファイルをダウンロードするには、以下の手順に従います。

[Download report（レポートをダウンロード）] をクリックします。

確認メッセージが表示され、メンテナンスレポートファイルのダウンロードに成功しました。



3.8.3.2 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Services	✓	✗	✗

3.8.3.2.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.8.3.3 CLI コマンド

maintenance

説明

テクニカルサポートに渡すことができるメンテナンスレポートファイルを作成します。

ヘルプ

```
maintenance
     <cr> Create maintenance report file.
   -h, --help Display help page
```

reboot

説明

カードを復元するためのツールです。

ヘルプ

```
Usage: reboot [OPTION]
    <cr>                    Reboot the card
    --help                    Display help
    --withoutconfirmation    Reboot the card without confirmation
```

save_configuration | restore_configuration

説明

Save_configurationとrestore_configurationは、JSON形式を使用してカードの設定の一部を保存・復元します。

ヘルプ

```
save_configuration -h
  save_configuration: print the card configuration in JSON format to standard output.
```

```
restore_configuration -h
  restore_configuration: restore the card configuration from a JSON-formatted standard
input.
```

使用例

From a linux host:

Save over SSH: sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS save_configuration –p $PASSPHRASE> $FILE **Restore over SSH:** cat $FILE | sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS restore_configuration –p$PASSPHRASE

From a Windows host:

Save over SSH: plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch save_configuration –p $PASSPHRASE > $FILE **Restore over SSH:** type $FILE | plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch restore_configuration –p
$PASSPHRASE
(Require plink tools from putty)

Where:

- $USER is user name (the user shall have administrator profile)
- $PASSWORD is the user password
- $PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- $CARD_ADDRESS is IP or hostname of the card
- $FILE is a path to the JSON file (on your host computer) where the configuration is saved or restored.

sanitize

説明

カードを工場出荷時設定に戻すための Sanitize コマンド

アクセス

- Administrator

ヘルプ

```
sanitize
  -h, --help              Display help page
  --withoutconfirmation   Do factory reset of the card without confirmation
  <cr>                    Do factory reset of the card
```

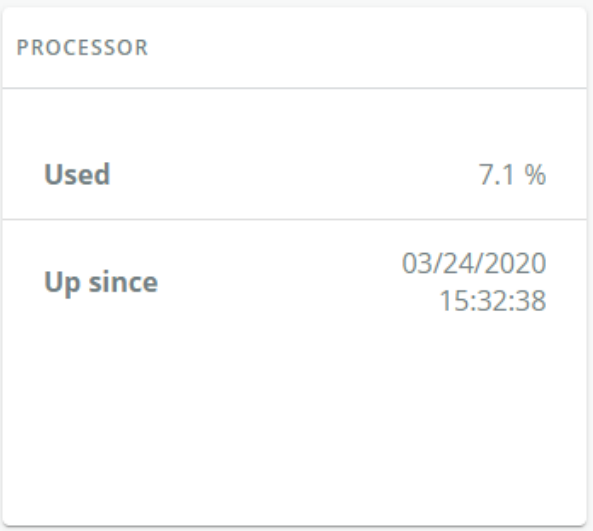
3.8.3.3.1 その他のCLIコマンドについて

その他のCLIコマンドについては次を参照してください。Information>>>CLI

3.8.4 リソース

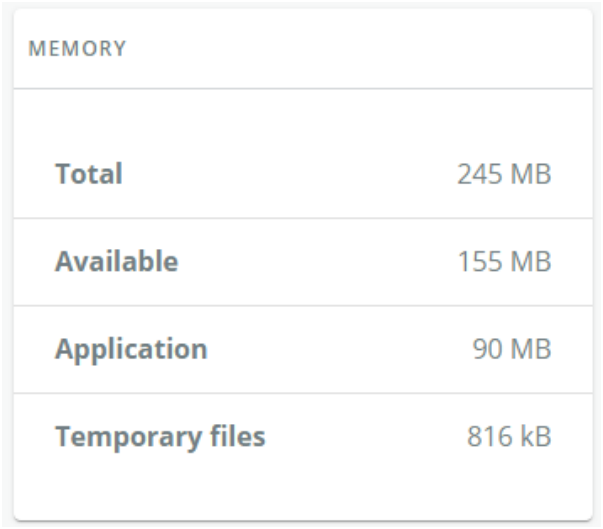
カードリソースは、ネットワークモジュールのプロセッサ、メモリ、ストレージ情報の概要です。 **[COPY TO CLIPBOARD（クリップボードへコピー）]**ボタンは、情報をクリップボードにコピーして貼り付けることができます。 例えば、電子メールに情報をコピーして貼り付けることができます。

3.8.4.1 プロセッサ



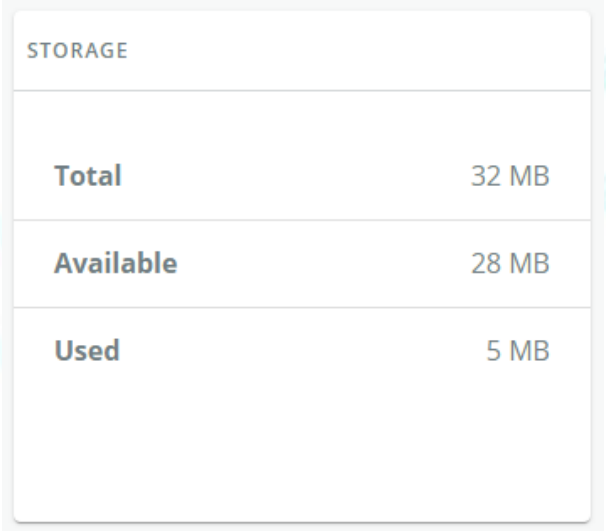
- Used in %
- Up since date

3.8.4.2 メモリ



- Total size in MB
- Available size in MB
- Application size in MB
- Temporary files size in MB

3.8.4.3 ストレージ



- Total size in MB
- Available size in MB
- Used size in MB

3.8.4.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Resources	✓	✓	✓

3.8.4.4.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.8.4.5 CLIコマンド

systeminfo_statistics

説明

以下のシステム情報の利用状況を表示します。:

1. CPU
    a. usage : %
    b. upSince : date since the system started
2. Ram
    a. total: MB
    b. free: MB
    c. used: MB
    d. tmpfs: temporary files usage (MB)
3. Flash
    a. user data
        i. total: MB
        ii. free: MB
        iii. used: MB

ヘルプ

3.8.4.5.1 その他のCLIコマンドについて

その他のCLIコマンドについては次を参照してください。Information>>>CLI

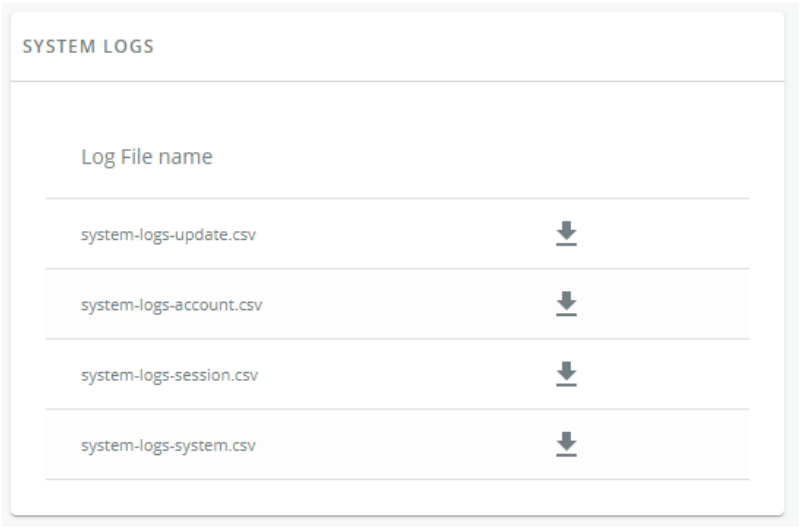
3.8.5 システムログ

3.8.5.1 システムログ

ログは4種類あります。:

- Update
- Account
- Session
- System

ダウンロードするログファイルを選択し、ダウンロードアイコンを押します。:



システムログの一覧は次を参照してください。Information>>>System Logs codes

3.8.5.2 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
System logs	✓	✗	✗

3.8.5.2.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.9 法的な情報

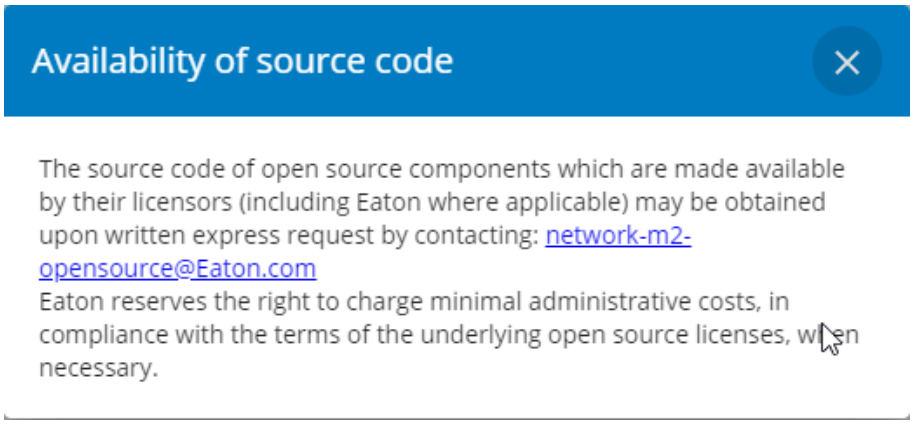
このネットワークモジュールには、様々なオープンソースライセンスまたはプロプライエタリライセンスでライセンスされているソフトウェアコンポーネントが含まれています。

3.9.1 コンポーネント

ネットワークモジュールに含まれるすべてのオープンソースコンポーネントは、ライセンスと共にリストアップされています。

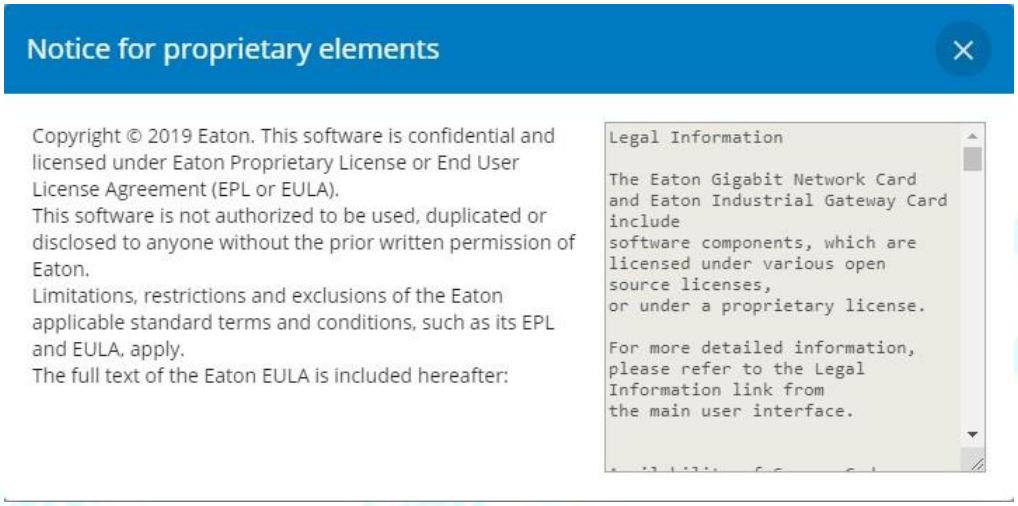
3.9.2 ソースコードの可用性

ライセンサーが利用可能なオープンソースコンポーネントのソースコードを取得する方法を提供します。



3.9.3 専有要素に関する注意事項

当社独自の（つまりオープンソースではない）要素についての通知を提供します。



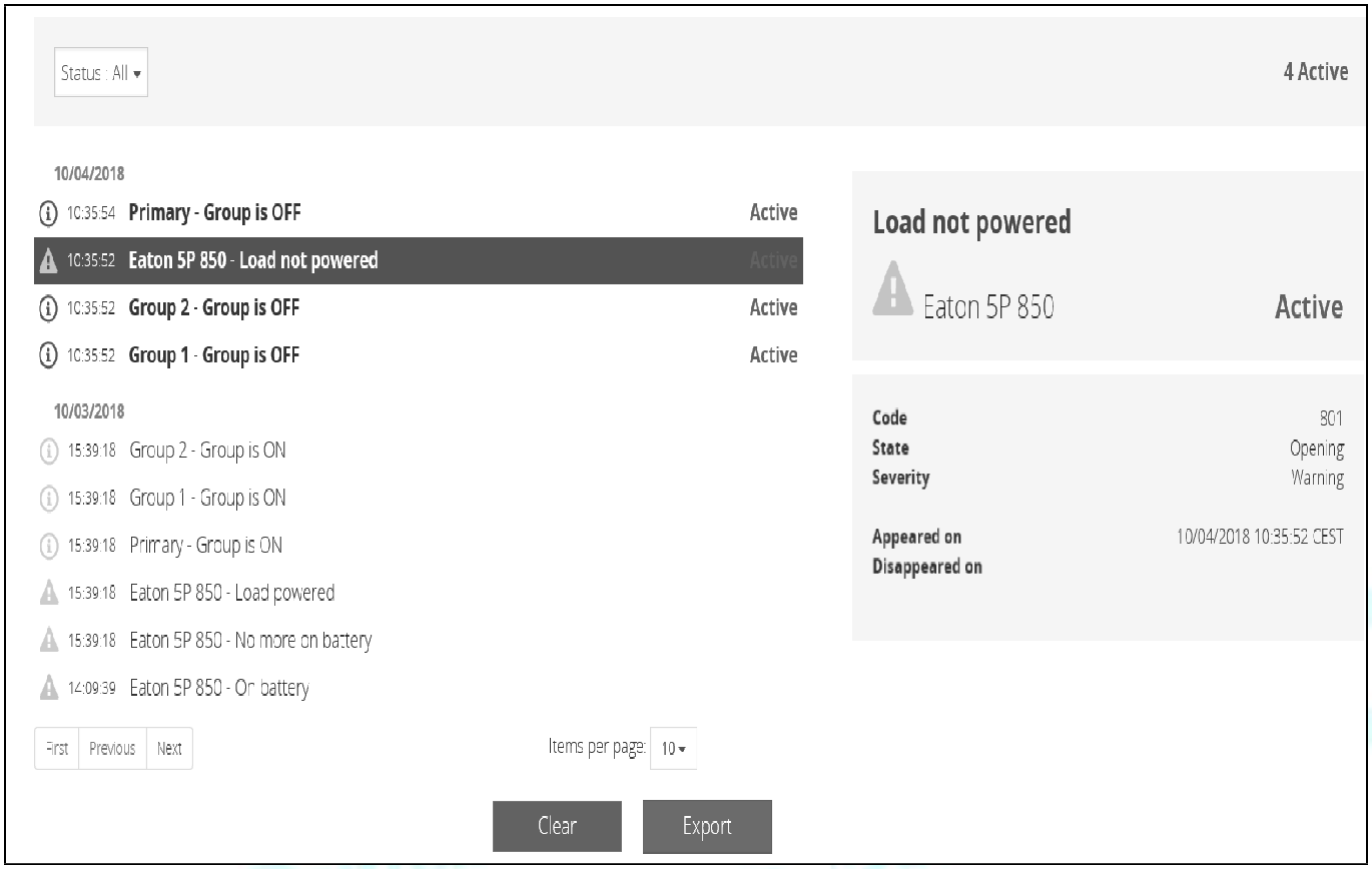
3.9.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Legal information	✓	✓	✓

3.9.4.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.10 アラーム



3.10.1 アラームの分類

下記を選択してアラームを並べ替えることができます。:

- All
- Active only

3.10.2 アクティブアラームカウンター

重大度が「良好」に設定されているアラームは、
アクティブアラームのカウンターには考慮されません。

3.10.3 アラームの詳細

すべてのアラームが表示され、アラートレベル、時間、説明、およびステータスで日付順にソートされます。

	Info/Warning/Critical logo	Alarm description text
Active	In color	In bold with "Active" label
Opened	In color	
Closed	Greyed	

3.10.4 アラームページング

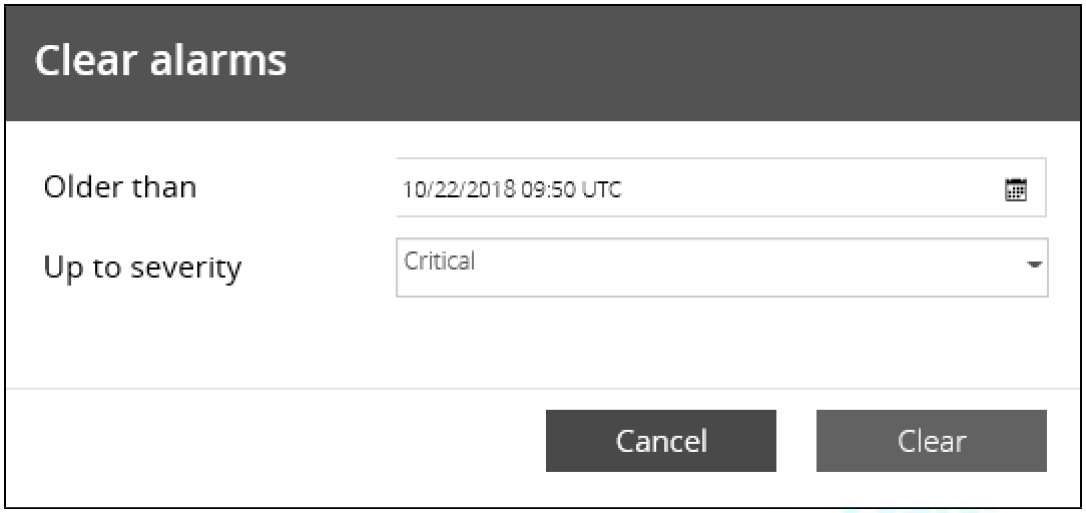
ページあたりのアラーム数を変更することができます（10–15–25–50–100）。

アラームの数が 1 ページあたりのアラーム数を超えると、最初、前、次のボタンが表示され、アラームリストのナビゲーションが可能になります。

3.10.5 エクスポート（Export）

[Export（エクスポート）]ボタンを押してファイルをダウンロードします。

3.10.6 クリア（Clear）



[Clear（クリア）]ボタンを押して、指定された日付よりも古く、定義された深刻度までのアラームをクリアします。

3.10.7 コード付きアラームリスト

アラームログコードや電子メール購読のためのシステムログコードへのアクセスを取得するには、以下のセクションを参照してください。:

- System log codes
- UPS(HID) alarm log codes
- 9130 UPS(XCP) alarm log codes
- ATS alarm log codes
- EMP alarm log codes
- Network module alarm log codes

3.10.8 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Alarm list	✓	✓	✓
Export	✓	✓	✓
Clear	✓	✓	✗

3.10.8.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

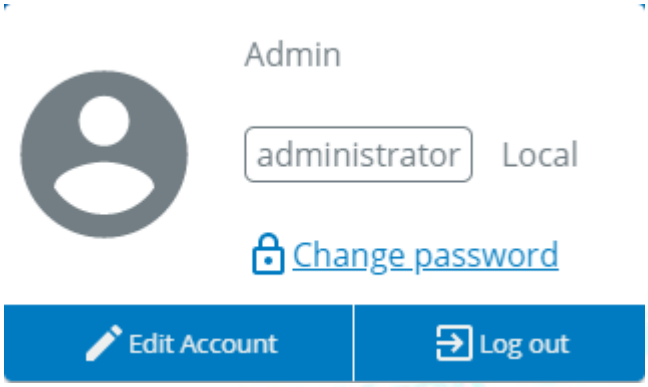
3.11 ユーザープロファイル

3.11.1 ユーザープロファイルへのアクセス

ページ右上のアイコンを押すと、ユーザープロファイルウィンドウにアクセスできます。:

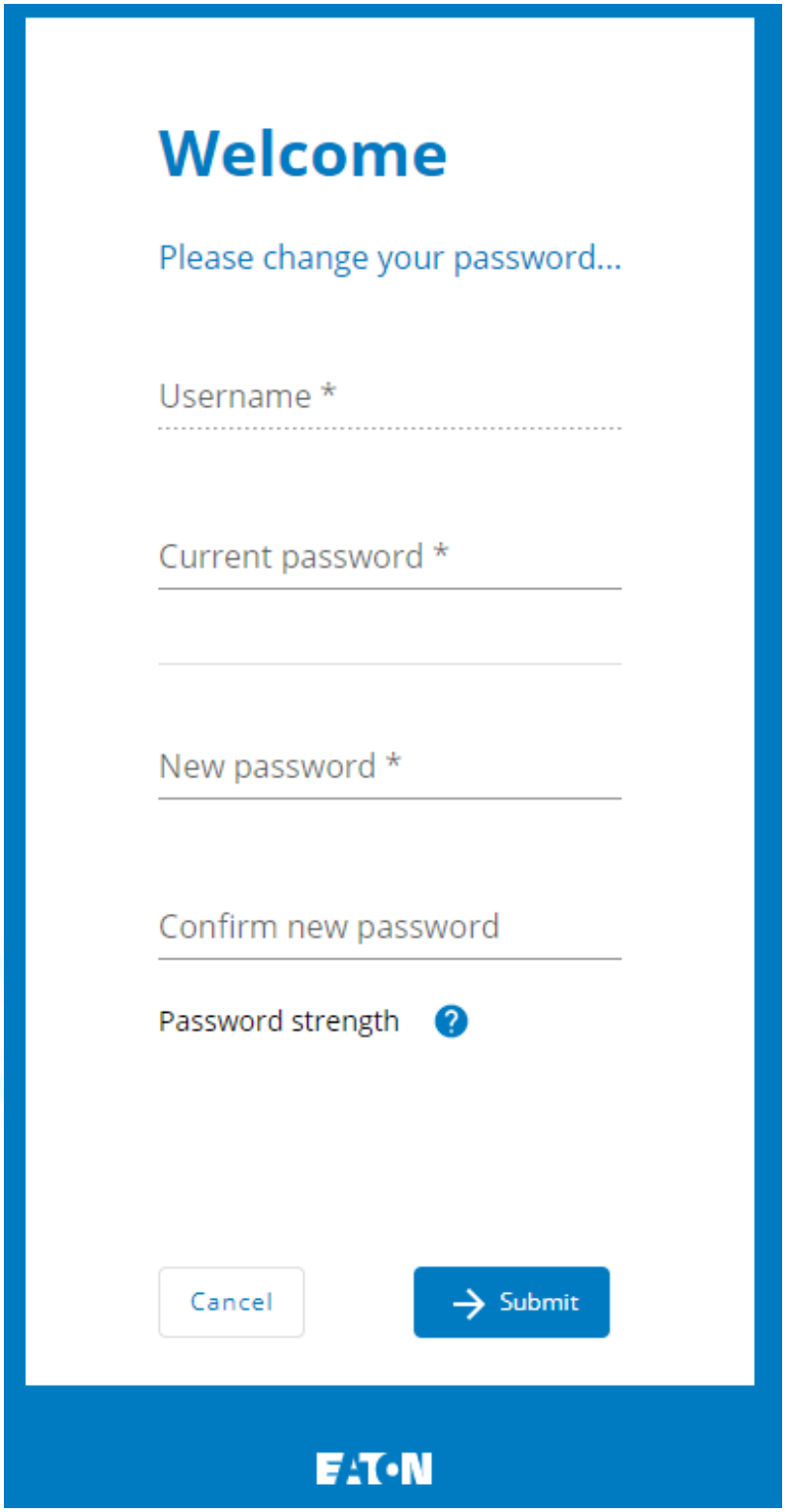
このページは、LDAP を介して接続されている場合は読み取り専用モードになっています。
Contextual help>>>Settings>>>Remote users>>>LDAP

3.11.2 ユーザープロファイル



このページでは、現在のユーザー名とその領域（ローカル、リモート）を表示し、パスワードの変更、アカウントの編集、ログアウトを行うことができます。

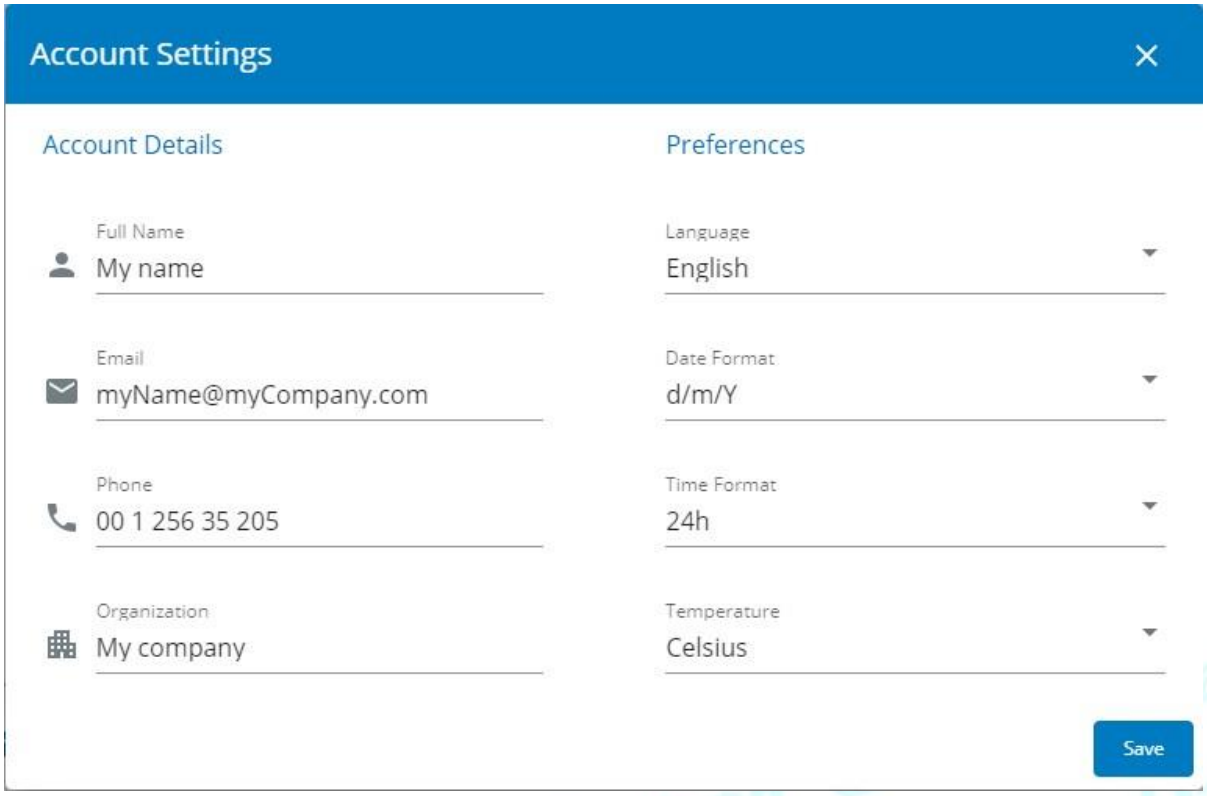
3.11.2.1 パスワード変更



[Change password（パスワードの変更）]をクリックして、パスワードを変更します。

すでにパスワードを変更している場合は、変更できない場合があります。トラブルシューティングを参照してください。

3.11.2.2 アカウントの編集



管理者権限をお持ちの方は、**[Edit account（アカウントの編集）]**をクリックして、ユーザープロファイルを編集し、以下の情報を更新することができます。:

アカウントの詳細

- Full name
- Email
- Phone
- Organization

設定

- Language
- Date format
- Time format
- Temperature

3.11.2.3 アカウントの編集

[Log out（ログアウト）]をクリックしてセッションを閉じます。

3.11.3 デフォルト設定と可能なパラメーター –ユーザープロファイル

	Default setting	Possible parameters

Profile	Account details: • Full name — Administrator • Email — blank • Phone — blank • Organization — blank Preferences: • Language — English • Date format — MM-DD-YYYY • Time format — hh:mm:ss (24h) • Temperature — ° C (Celsius)	Account details: • Full name — 128 characters maximum • Email — 128 characters maximum • Phone — 64 characters maximum • Organization — 128 characters maximum Preferences: • Language — English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese • Date format — MM-DD-YYYY / YYY-MM- DD / DD-MM-YYY / DD.MM.YYY / DD/MM/ YYY / DD MM YYYY • Time format — hh:mm:ss (24h) / hh:mm:ss (12h) • Temperature — ° C (Celsius)/° F (Fahrenheit)

3.11.3.1 その他の設定の場合

その他の設定の場合は次を参照してください。Information>>>Default settings parameters

3.11.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
User profile	✓	✓	✓

3.11.4.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

3.11.5 CLIコマンド

logout

説明

現在のユーザーをログアウトします。

ヘルプ

```
logout
  <cr> logout the user
```

whoami

説明

whoami は現在のユーザー情報を表示します。:

- Username
- Profile
- Realm

3.11.5.1 その他のCLIコマンドについて

その他のCLIコマンドについては次を参照してください Information>>>CLI

3.11.6 トラブルシューティング

プロフィールのパスワード変更がうまくいかない

症状

マイプロフィールメニューでパスワードを変更しようとすると「無効な資格情報」と表示される:

考えられる原因

パスワードは1日の期間内に1回変更済みです。

アクション

最後のパスワードの変更から再試行までの間に1日を空けてください。

3.11.6.1 その他の問題について

その他の問題の詳細については、「トラブルシューティング」のセクションを参照してください。

3.12 ドキュメント

3.12.1 組み込みドキュメントへのアクセス

ページ右上の ?アイコンを押すと、新しいウィンドウでドキュメントにアクセスできます。:

フォーカスは、コンテキストページで行われます。その後、以下のセクションに移動することができます。:

Contextual help	各ページのヘルプです。 以下のセクションからウェブページに関連するものを抜粋しています。
Servicing the Network Management Module	ネットワークモジュールのインストールと使用方法
Securing the Network Management Module	ネットワークモジュールを確保する方法。
Information	ネットワークモジュールとデバイスの一般的な情報
Troubleshooting	ネットワークモジュールのトラブルシューティング方法

検索機能はインデックス化されています。

3.12.2 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
Contextual help	✓	✓	✓
Full documentation	✓	✓	✓

3.12.2.1 その他のアクセス権について

その他のアクセス権については次を参照してください。Information>>>Access rights per profiles

4 ネットワークマネジメントモジュールのサービス

4.1 LDAPの設定/コミッショニング/テスト

4.1.1 コミッショニング

設定に関するヘルプは、Contextual help>>>Settings>>>Local users の項を参照してください。

4.1.1.1 LDAPデータベースへの接続の設定

このステップでは、ネットワークモジュールの LDAP クライアントを構成して、LDAP ベースからデータを要求します。

1.LDAP をアクティブにします。

2.LDAP サーバーの要件に応じてセキュリティ パラメーターを定義します。

3.プライマリサーバー(オプションでセカンダリサーバーも)を設定します。

4.セキュリティ設定でサーバー証明書の検証が必要な場合は、LDAP サーバー証明書をインポートします。証明書のインポートに関するヘルプは、セクションを参照してください。

a. LDAP サーバー証明書が自己署名されている場合は、***LDAP* サービス**の信頼できるリモート証明書リストに自己署名された証明書をインポートします。

b. LDAP サーバー証明書が CA によって署名されている場合は、対応する CA を ***LDAP* サービス**の証明書局 (CA) リストにインポートします。

5. LDAP サーバーにバインドする資格情報を設定するか、資格情報が必要ない場合は匿名を選択します。

6.検索ベースDNを設定します。

7.リクエストパラメーターを設定します(以下の例を参照)。

4.1.1.1.1 代表的なリクエストパラメーター

Parameter	OpenLDAP	Active Directory™ with POSIX account activated	Active Directory™
User base DN	ou=users, dc=example, dc=com	ou=users, dc=example, dc=com	ou=users, dc=example, dc=com
User name attribute	uid	uid	sAMAccountName
UID attribute	uidNumber	uidNumber	objectSid:S-1-5-xx-yy-zz (domain SID)
Group base DN	ou=groups, dc=example, dc=com	ou=groups, dc=example, dc=com	ou=groups, dc=example, dc=com
Group name attribute	gid	gid	sAMAccountName
GID attribute	gidNumber	gidNumber	objectSid:S-1-5-xx-yy-zz (domain SID)

4.1.1.2 LDAPデータベースへの接続のテスト

CLIコマンドのヘルプを参照するには、「Information」>>「CLI」>>「ldap-test」セクションを参照してください。

LDAP データベースへの接続をテストするには:

1. CLIに接続します。
2. ldap-test --checkusername コマンドを起動します。
3. ラーが発生した場合は、コマンドの冗長オプションを使用して原因を調査します。

4.1.1.3 リモートユーザーをプロファイルにマッピングする

> このステップは必須であり、LDAP ユーザーに権限を与えるようにネットワーク モジュールを設定します。プロファイルにマッピングされたグループに属していないユーザーは拒否されます。

LDAP ユーザーをプロファイルにマッピングするルールを設定します。

1. LDAP グループ名を入力します。
2. 割り当てるプロファイルを選択します。

最大 5 つのマッピング ルールを定義できます。
設定された LDAP グループに属するすべての LDAP ユーザーは、関連付けられたプロファイルによって許可された権限を持つようになります。

ユーザーが異なるプロファイルにマップされた複数のLDAPグループに属している場合、動作は未定義です。

4.1.1.4 プロファイルマッピングのテスト

CLIコマンドのヘルプを参照するには、「Information」>>「CLI」>>「ldap-test」のセクションを参照してください。

LDAPユーザープロファイルのマッピングをテストするには、以下の手順に従います。

1. CLIに接続します。
2. ldap-test --checkmappedgroupsコマンドを起動します。
3. このコマンドは、各マップされたグループが LDAP ベースに存在することを確認し、関連するローカル プロファイルを表示します。
4. エラーが発生した場合は、コマンドの verbose オプションを使用して原因を調べます。

4.1.1.5 LDAPユーザーの設定を定義する

このステップでは、すべてのLDAPユーザーに適用するユーザーの環境設定を行います。

4.1.2 LDAP認証のテスト

CLIコマンドのヘルプを得るには、Information>>>CLI>>>ldap-testのセクションを参照してください。

1. CLIに接続します。
2. ldap-test --checkauth コマンドを起動します。
3. このコマンドは、LDAP ユーザーが彼のユーザー名とパスワードを使用して認証できることを確認し、そのローカルプロファイルを表示します。
4. エラーが発生した場合は、コマンドの verbose オプションを使用して理由を調べます。

4.1.3 制限事項

- ローカルデータベースと LDAP データベースの両方に同じユーザー名が存在する場合、動作は未定義です。
- ユーザーが異なるプロファイルにマップされた複数の LDAP グループに所属している場合、動作は未定義です。
- クライアント証明書が提供されていません。サーバーがクライアントの真正性を検証することはできません。
- 2 つの異なる検索ベースで動作するように LDAP を構成することはできません。
- LDAPユーザーの設定は、すべてのLDAPユーザーに共通です。
- LDAP ユーザーは、ネットワーク モジュールを介してパスワードを変更できません。
- プロファイル マッピング設定で入力されるリモート グループ名は、英数字、アンダースコア、ハイフンのみで構成されていなければなりません (ただし、最後の 1 つを先頭にすることはできません)。

4.2 ネットワークモジュールとのペアリングエージェント

UPSネットワークモジュールとシャットダウンエージェント間の接続の認証と暗号化は、一致する証明書に基づいています。

4.2.1 エージェントの資格情報とのペアリング

STEP 1：エージェント（IPP/IPM）へのアクション。

1. エージェントのWebインターフェースに接続します。
2. アドレススキャンで UPS ネットワークモジュールを検出し、Override global authentication settings を選択して、UPS Network Module credentials を入力します。

4.2.2 自動受諾とのペアリング（安全で信頼できるネットワークで行う場合に推奨）

シャットダウンエージェントやUPSネットワークモジュールの自動受付とのペアリングは、安全で信頼できるネットワークに設置する場合や、他の方法で証明書を作成できない場合にお勧めします。

STEP1: ネットワークモジュールのアクション

1.ネットワークモジュールに接続します。

・ネットワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。

・Address/Location フィールドに、https://xxx.xxx.xxx.xxx と入力します。xxx.xxx.xxx.xxx はネットワークモジュールのスタティック IP アドレスです。

・ログイン画面が表示されます。

・User Name（ユーザー名）フィールドにユーザー名を入力します。

・Password（パスワード）フィールドにパスワードを入力します。

・**[Login（ログイン）]** をクリックします。Network Module Web インターフェースが表示されます。

2. Contextual help>>>Protection>>>Agents list ページに移動します。

3.シャットダウンエージェントとのペアリングセクションで、新しいエージェントを受け入れる時間を選択し、**[Start（スタート）]** ボタンを押し、**[Continue（続行）]** を押します。選択した時間枠の間、ネットワークモジュールへの新しいエージェント接続が自動的に信頼され、受け入れられます。

STEP2：ネットワークモジュール上で新規エージェントを受け入れる時間が実行されている間にエージェント（IPP）にアクションを実行する

1. エージェントの Web インターフェースに接続します。

2. **クイックスキャン、レンジスキャン**、または**アドレススキャン**で UPS ネットワークモジュールを検出します。

3. 検出された UPS ネットワークモジュールを右クリックし、**[Set as power source（パワーソースとして設定）]**、**[Configure（設定）]**、**[Save（保存）]**を選択します。

STEP3: ネットワークモジュールの操作

1. カードにリストされているすべてのエージェント Contextual help>>>>Protection>>>>Agent list がインフラストラクチャに属していることを確認します。見つからない場合は、**[Delete（削除）]**ボタンを使用してアクセスを取り消すことができます

2. ペアリングの時間がまだ経過している場合は、ペアリングを停止することができます。シャットダウンエージェントとのペアリングセクションで**[Stop（停止）]**を押します。

STEP1とSTEP2はどちらの方法でも構いません。

4.2.3 手動受諾とのペアリング

手動でペアリングすることで、最大のセキュリティを実現しています。

STEP1：エージェントへのアクション（IPP）

1.エージェントのWebインターフェースに接続します。

2.クイックスキャン、レンジスキャン、またはアドレススキャンで UPS ネットワークモジュールを検出します。

3.電源を定義します。

Note：このステージの後、エージェントはクライアント証明書を作成します。現在のクライアント証明書がネットワークモジュールによって信頼されていないため、電源は通信損失を示す可能性があります。

4.フォルダEaton¥IntelligentPowerProtector¥configs¥tls...にあるエージェント証明書ファイル**client.pem**をコピーします。

STEP2：ネットワークモジュールのアクション

1.ネットワークモジュールに接続します。

・ネットワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。

・Address/Location フィールドに、https://xxx.xxx.xxx.xxx と入力します。xxx.xxx.xxx.xxx はネットワークモジュールのスタティック IP アドレスです。

・ログイン画面が表示されます。

・User Name（ユーザー名）フィールドにユーザー名を入力します。

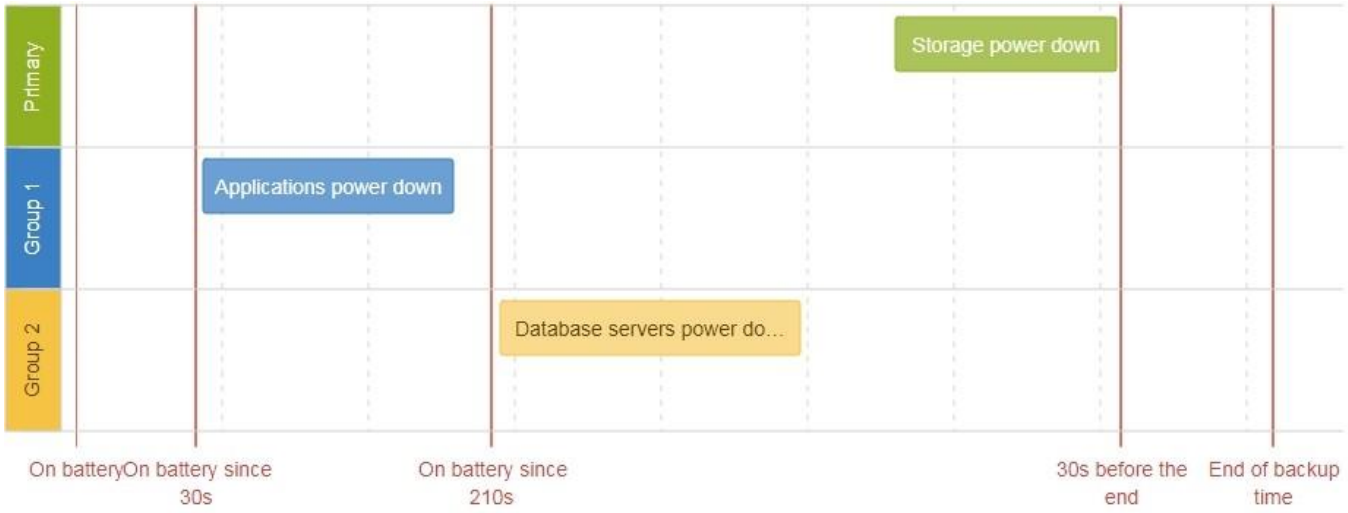
・「パスワードフィールド」にパスワードを入力します。
・**[Login（ログイン）]** をクリックします。Network Module Web インターフェースが表示されます。
2. Contextual help>>>>Settings>>>>Certificate pageに移動します。
3. 「信頼できるリモート証明書」セクションで、**[Import（インポート）]**をクリックし、**「保護されたアプリケーション（MQTT）」**を選択してから**[CONTINUE（続行）]**をクリックします。
4. 先に保存したclient.pemファイルを選択し、**[Open（開く）]**をクリックします。エージェントとの通信が復旧します。

4.3 アプリケーションの電源切断/投入（例）

4.3.1 特定の順序でITシステムの電源を落とす

4.3.1.1 ターゲット

最初にアプリケーションのパワーダウンを行い(バッテリーが30秒以上ある場合)、次にデータベースサーバーのパワーダウンを行い(アプリケーションの3分後)、最後にストレージのパワーダウンを行う(できるだけ遅く)。



4.3.1.2 Step 1:インストールの設定

4.3.1.2.1 目的

UPSが提供する負荷分割を利用して、IT機器のカテゴリ（アプリケーション、データベースサーバー、ストレージ）ごとに独立して電源を制御することができます。

また、商用電源リカバリー時にIT機器を順次再起動することができます（商用電源リカバリー時にIT機器を順次再起動）。

4.3.1.2.2 結果のセットアップ

UPSはアウトレット（グループ1とグループ2）と一次出力を提供します。

プライマリがOFFになると、グループ1もグループ2もすぐにOFFになります。

UPSへの接続は、以下のように行われます。
・グループ1: 適用
・グループ2. データベースサーバー
・プライマリ: ストレージ

4.3.1.3 Step 2: エージェントの設定

4.3.1.3.1 目的

ITソリューションが確実にシャットダウンされるようにします。

4.3.1.3.2 結果的なセットアップ

1. 各サーバー（アプリケーション、データベースサーバー、ストレージ）にIPPソフトウェアをインストールし、UPSの負荷セグメントを電源として登録します。
   ・アプリケーションの場合：グループ1
   ・データベースサーバー：グループ2
   ・ストレージ：UPS全体
2. ネットワークモジュールにエージェントをペアリングします。完了すると、エージェント一覧に各サーバーが表示されます。
3. Contextual help>>Protection>>Agent shutdown sequencingページに移動します。

エージェント設定の例については、「エージェントシャットダウンシーケンスの例」セクションを参照してください。

4. OSのシャットダウン期間を、サーバーが正常にシャットダウンするのに必要な時間に設定します。これにより、ロードセグメントの電源が切れる前に、IPPがサーバーを確実にシャットダウンします。その結果、各負荷セグメントの全体的なシャットダウンシーケンス期間が定義されます。

4.3.1.4 Step 3:停電ポリシーの設定

4.3.1.4.1 目的

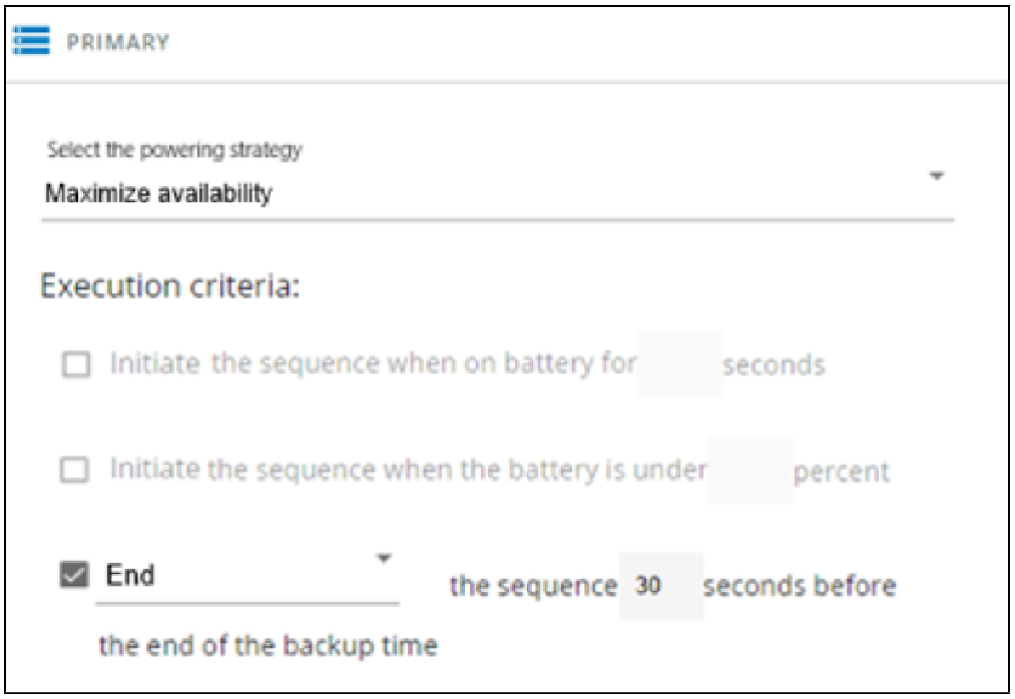
ロードセグメントポリシーを使用して、シャットダウンシーケンスを定義します。

4.3.1.4.2 結果のセットアップ

1. ネットワークモジュールの Contextual help >>> Protection >>> Shutdown on power outage ページに移動します

停電ポリシーの例については、次のセクションを参照してください。
・可用性ポリシーの例を最大化する
・即時のグレースフルシャットダウンポリシーの例
・負荷制限ポリシーの例
・カスタムポリシーの例

2. プライマリが次のように設定されていることを確認します：Maximize availability.（可用性の最大化）

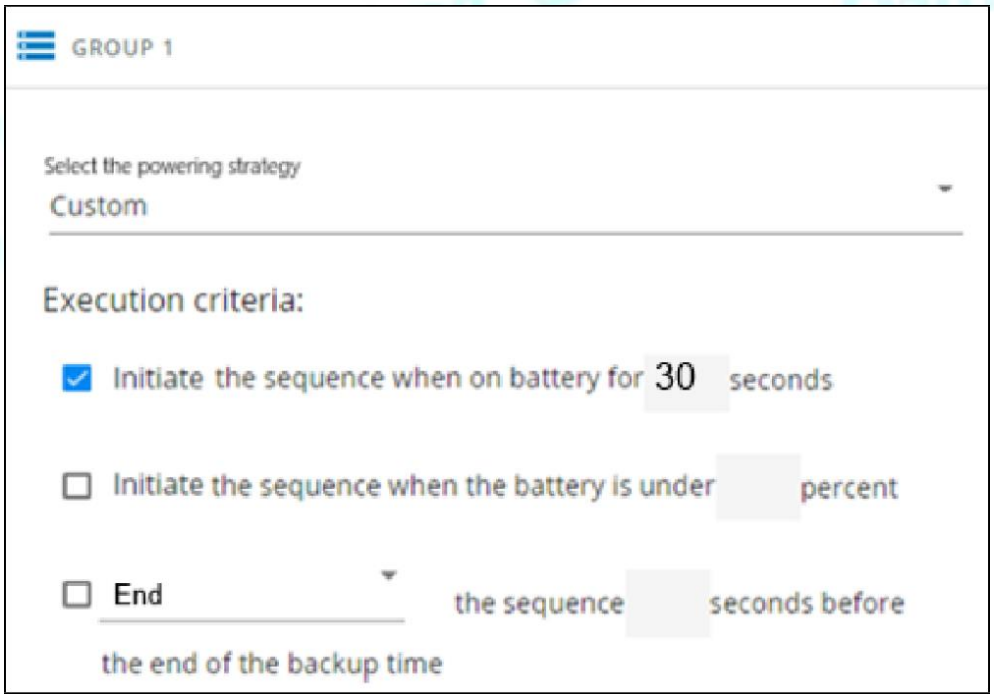


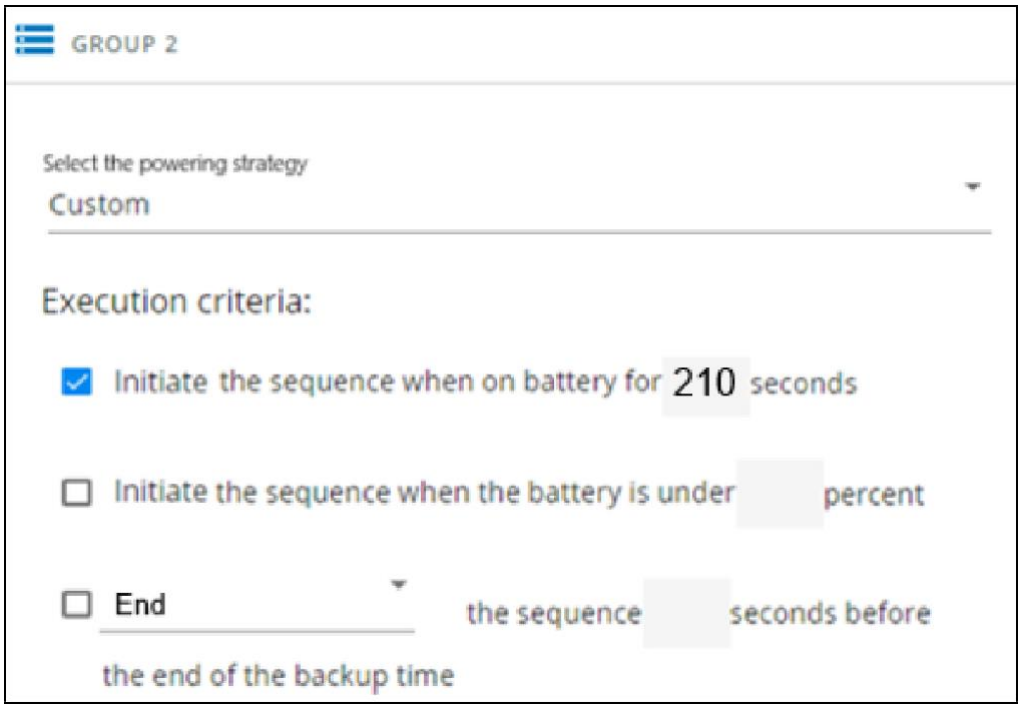
ストレージは最後に電源を切り、可用性が最大化され、バックアップ時間の終了の30秒前にシャットダウンが終了します。

3. グループ1とグループ2を[Custom(カスタム)]に設定します。

アプリケーションを最初にシャットダウンする必要があるため、グループ1は、バッテリーを30秒間オンにしたときにシャットダウンを開始するように設定されています。

サーバーは2番目にシャットダウンする必要があるため、グループ2は、210秒間バッテリーを使用しているときにシャットダウンを開始するように設定されているため、アプリケーションの3分後にシャットダウンします。

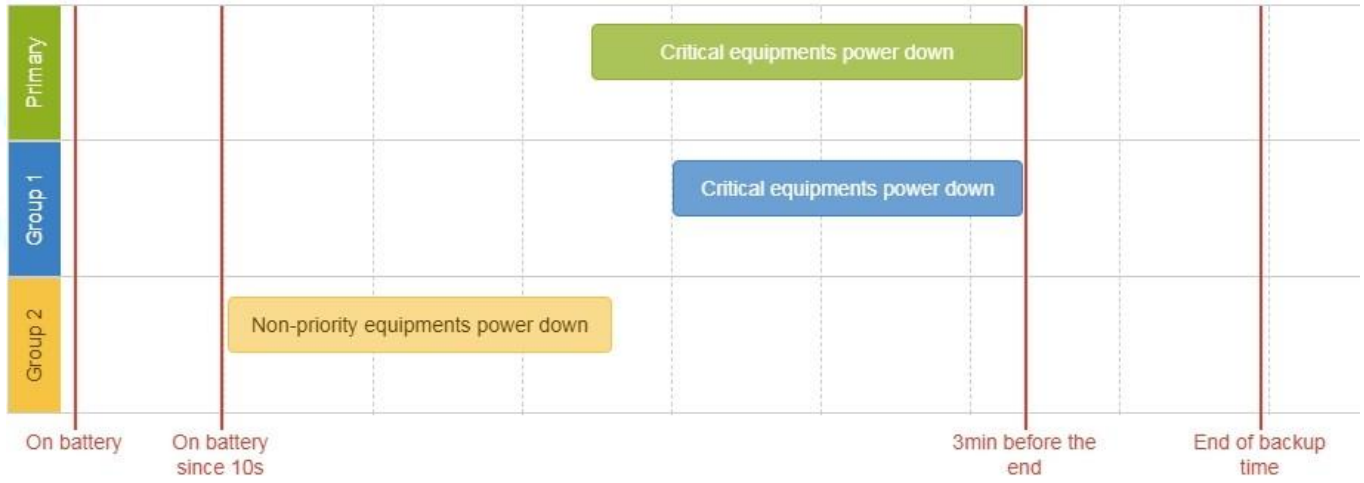




4.3.2 優先順位の低い機器から先に電源を切る

4.3.2.1 ターゲット

優先度の低い機器の電源を最初に(すぐに)オフにし、重要な機器のバッテリー電源を維持します。バックアップ時間の終了の3分前に重要な機器の電源を切ります。



4.3.2.2 Step 1:インストールのセットアップ

4.3.2.2.1 目的

UPSが提供する負荷セグメンテーションを使用して、各IT機器カテゴリ(アプリケーション、データベースサーバー、ストレージ)の電源を個別に制御します。

負荷のセグメンテーションにより、IT機器はユーティリティリカバリ時に順次再起動することもできます(ユーティリティリカバリ時にIT機器を順次再起動します)。

4.3.2.2.2 結果のセットアップ

UPSは、コンセント（グループ1およびグループ2）と一次出力を提供します。

プライマリがオフになると、グループ1とグループ2の両方がすぐにオフになります。

接続は、以下の記述に従って行うことができます。
·グループ2：非優先機器
·グループ1：重要な機器
·プライマリ：重要な機器

4.3.2.3 Step 2: エージェント設定

4.3.2.3.1 目的

ITソリューションが正常にシャットダウンされていることを確認します。

4.3.2.3.2 結果のセットアップ

1.各サーバー（アプリケーション、データベースサーバー、ストレージ）にIPPソフトウェアをインストールし、UPS負荷セグメントを電源として登録します。
·重要な機器：グループ1
·非優先機器：グループ2
·重要な機器：UPS全体
2.エージェントをネットワークモジュールにペアリングします（エージェントをネットワークモジュールにペアリングします）。完了すると、各サーバーがエージェントリストに表示されます。
3. Contextual help>>>Protection>>>Agent shutdown sequencing ページに移動します

エージェント設定の例については、「エージェントのシャットダウンシーケンス」セクションを参照してください。

4.OSのシャットダウン期間を、サーバーが正常にシャットダウンするのに必要な時間に設定します。これにより、ロードセグメントの電源が切れる前に、IPPがサーバーを確実にシャットダウンします。その結果、各負荷セグメントの全体的なシャットダウンシーケンス期間が定義されます。

4.3.2.4 Step 3:停電ポリシーの設定

4.3.2.4.1 目的

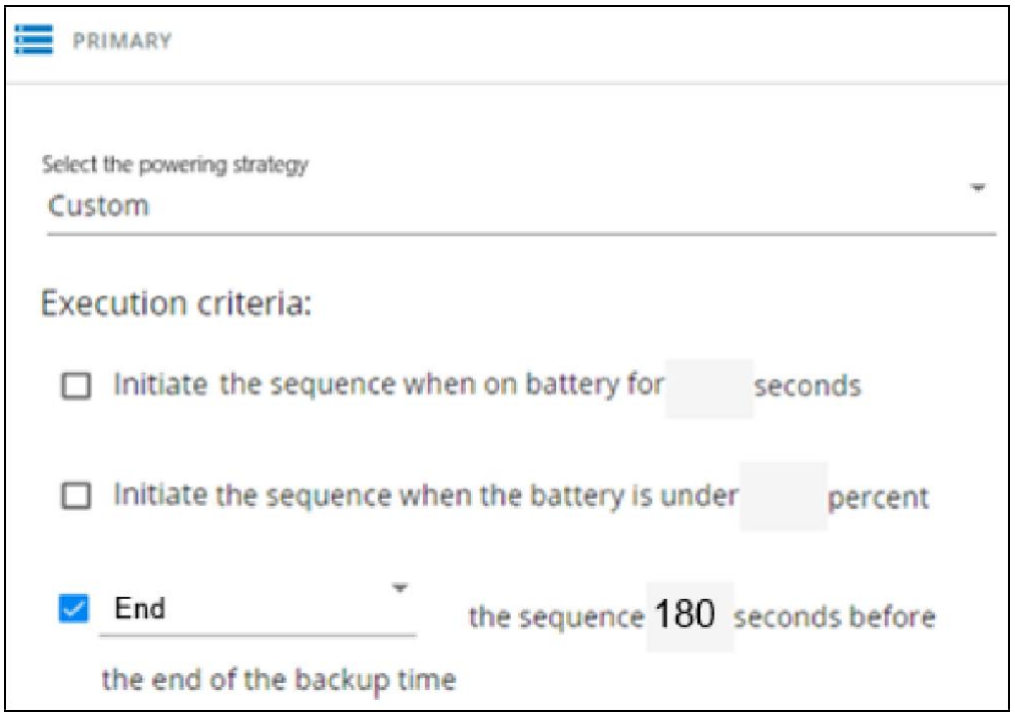
ロードセグメントポリシーを使用して、シャットダウンシーケンスを定義します。

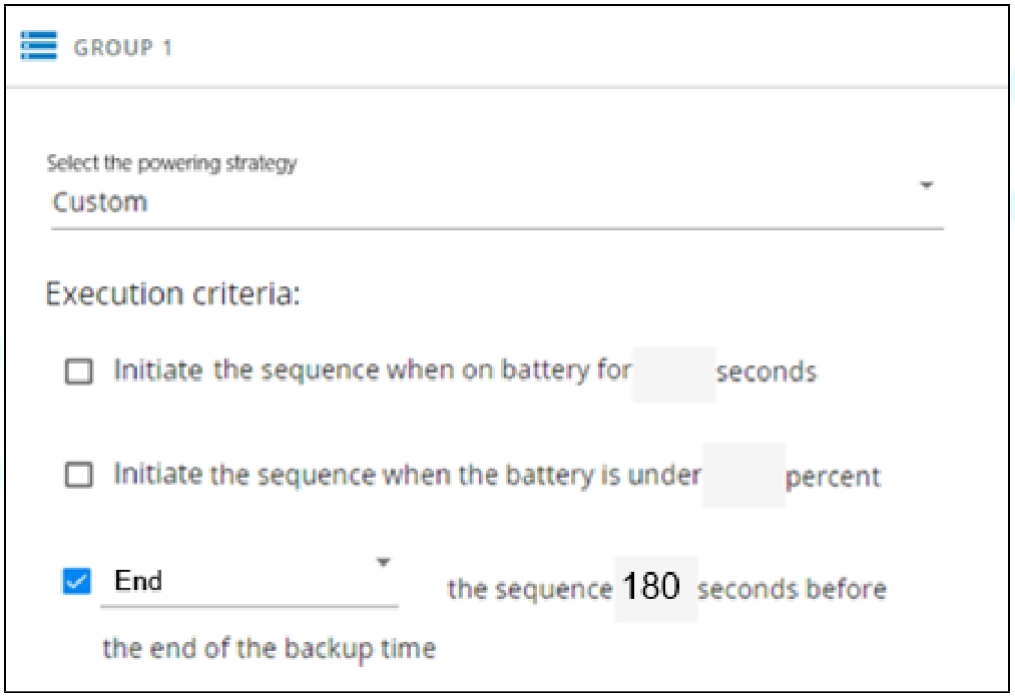
4.3.2.4.2 結果のセットアップ

1.ネットワークモジュールのContextual help>>>Protection>>>Shutdown on power outage ページのシャットダウンに移動します

停電ポリシーの例については、次のセクションを参照してください。
·可用性ポリシーの例を最大化する
·即時のグレースフルシャットダウンポリシーの例
·負荷制限ポリシーの例
·カスタムポリシーの例

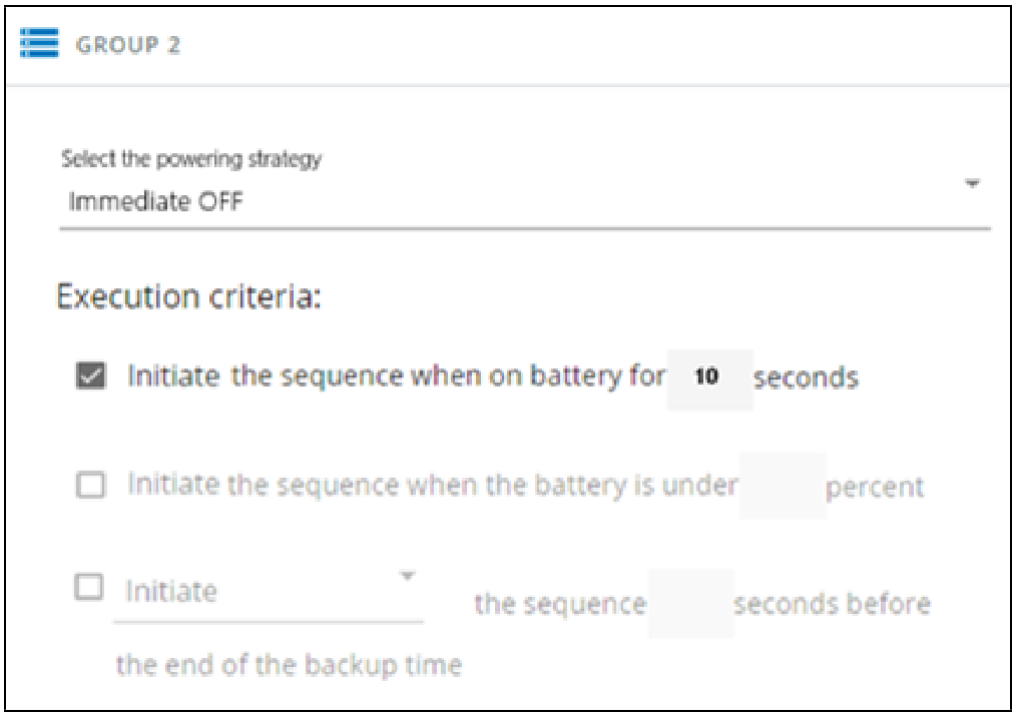
2.プライマリおよびグループ1を[Custom（カスタム）]に設定し、バックアップ時間の終了の180秒前にシャットダウンシーケンスを終了するように設定します。





重要な機器は最後に電源を切るものであり、それらの可用性は最大化され、バックアップ時間の終了前にシャットダウンが180秒で終了します。

3.グループ2を次のように設定します：**[Immediate（即時オフ）]**

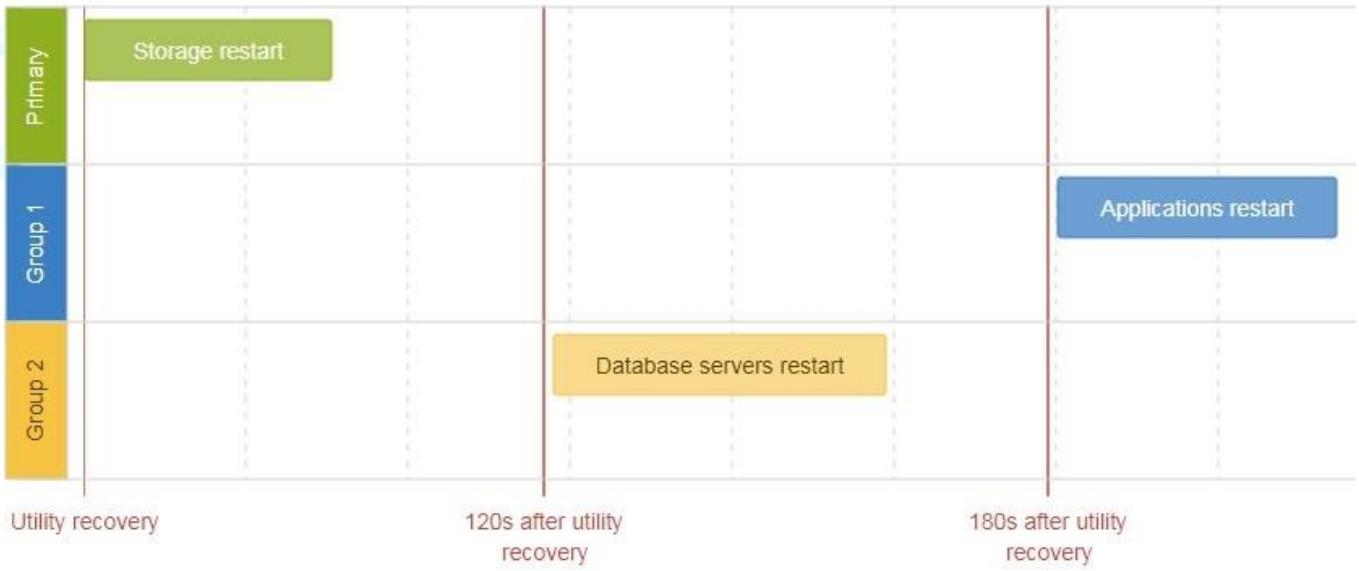


優先度の低い機器は、重要な機器のバッテリー電源を維持するために、10秒間バッテリーを使用するとすぐにシャットダウンします。

4.3.3 商用電源の回復時にIT機器を順次再起動する

4.3.3.1 目標

最初にストレージを再起動し（ユーティリティリカバリの直後）、次にデータベースサーバーを再起動し（ユーティリティリカバリの2分後）、アプリケーションを最後に再起動します（ユーティリティリカバリの3分後）。



4.3.3.2 Step 1: インストレーションセットアップ

4.3.3.2.1 目的

UPSが提供する負荷セグメンテーションを使用して、各IT機器カテゴリ（アプリケーション、データベースサーバー、ストレージ）の電源を個別に制御します。

これにより、ユーティリティの回復時にIT機器を順番に再起動できます。

4.3.3.2.2 結果のセットアップ

UPSは、コンセント（グループ1およびグループ2）と一次出力を提供します。

> ユーティリティが回復すると、プライマリはすぐに起動します。

Connections to UPS can be done as described below:

UPSへの接続は、以下のように行うことができます。

·グループ1：アプリケーション

·グループ2：データベースサーバー

·プライマリ：ストレージ

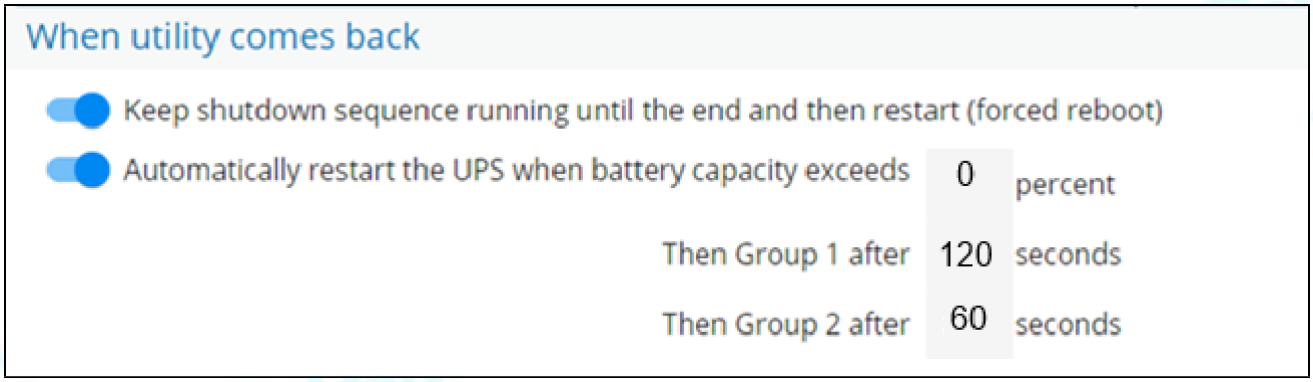
4.3.3.3 STEP2：停電ポリシーの設定

4.3.3.3.1 目的

ロードセグメントの再起動設定を使用して、再起動の順序を定義します。

4.3.3.3.2 結果のセットアップ

1. Contextual help>>>Protection>>>停電ページのShutdownおよび**元電源が戻ってきたとき**セクションに移動します。



2.「シャットダウンシーケンスを最後まで実行し続けてから再起動（強制再起動）」を有効にします。

3.「バッテリー容量を超えたときにUPSを自動的に再起動する」を有効にし、0%に設定します。

ストレージは、バッテリー容量が%制限を超えるのを待たずに、ユーティリティの回復直後に最初に再起動します。

4.次にグループ1を120秒に設定します。

データベースサーバーは、ユーティリティの回復後120秒で再起動します。

5.次にグループ2を60秒に設定します。

データベースサーバーは、ユーティリティの回復後180秒で再起動します。

4.4 ネットワークモジュールの現在のファームウェアバージョンを確認する

ネットワークモジュールの現在のファームウェアは、次の場所からアクセスできます：

- カードメニュー：Contextual help>>>Maintenance>>>System information>>>Firmware information: Firmware version x.xx.x
- カードメニュー：Contextual help>>>Maintenance>>>Firmware: Active FW version x.xx.x

4.5 最新のネットワークモジュールのファームウェア/ドライバ/スクリプトへのアクセス

最新のEatonNetwork Moduleファームウェア、ドライバ、またはスクリプトをからダウンロードします。

Eaton website www.eaton.com/downloads

4.6 カードファームウェアのアップグレード をする(Web インターフェース/シェルスクリプト)

最新のファームウェアとスクリプトにアクセスする手順については、以下を参照してください：最新のファームウェアとスクリプトへのアクセス

4.6.1 Webインターフェース

Webインターフェースを介してネットワークモジュールをアップグレードするには、次のセクションを参照してください：Webインターフェースを介したファームウェアのアップグレード

4.6.2 シェルスクリプト

4.6.2.1 前提条件

シェルスクリプトは次のツールを使用します：sshpass、scp。

Linuxホストにインストールするには、次のコマンドを使用します。

Debian/Ubuntu

```
$ sudo apt-get install sshpass scp
```

RedHat/Fedora/CentOS

```
$ sudo dnf install sshpass scp
```

シェルスクリプトを実行可能にする。:

```
$ chmod 700 install_updatePackage.sh
```

4.6.2.2 手続き

以下を使用してネットワークモジュールをアップグレードするには：

1.コンピューターでシェルターミナルを開きます（Linuxまたはcygwin。実際のまたはエミュレートされたLinuxオペレーティングシステムを意味します）。

2.シェルスクリプトinstall_updatePackage.shを使用します

```
Usage: 'install_updatePackage.sh' [options]
Upgrade tool
Mandatory arguments are -f, -i, -u and -p
-h : show help
-f <path> : path of the upgrade file
-u <username> : username of a card user allowed to start upgrade
-p <password> : user password
-i <ipaddress> : ip address of the card to upgrade
-r : reboot the card after upgrade
```

4.6.3 例

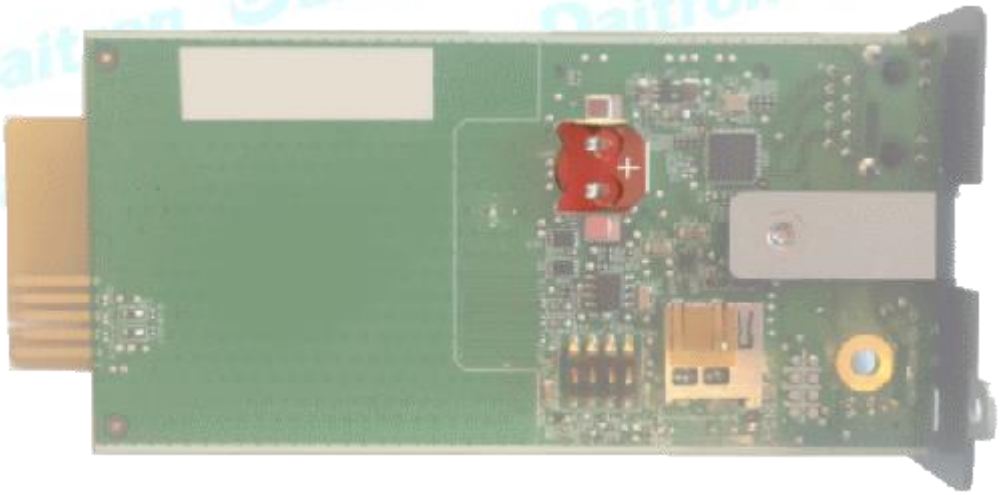
```
$ ./install_updatePackage.sh -u admin -p <mypassword> -f FW_Update.tar -i <cardIpAddress> -r
```

```
STARTING UPDATE FROM: [FW_Update.tar] to [X.X.X.X]

Transfer by scp (FW_Update.tar) to [X.X.X.X]
Warning: Permanently added 'X.X.X.X' (ECDSA) to the list of known hosts. Transfer done.
Check running upgrade status ... Check
firmware binary signature
Uncompress and flash upgrade              - inProgress(%):11
Uncompress and flash upgrade              - inProgress(%):28
Uncompress and flash upgrade              - inProgress(%):44
Uncompress and flash upgrade              - inProgress(%):61
Uncompress and flash upgrade              - inProgress(%):78
Uncompress and flash upgrade              - inProgress(%):92
Uncompress and flash upgrade              - inProgress(%):100
Uncompress and flash upgrade              - inProgress(%):100
Uncompress and flash upgrade
Executing post post_upgrade.sh script upgrade Upgrade done
Warning: Permanently added 'X.X.X.X' (ECDSA) to the list of known hosts. Rebooting...
res: Y
Update:   OK
```

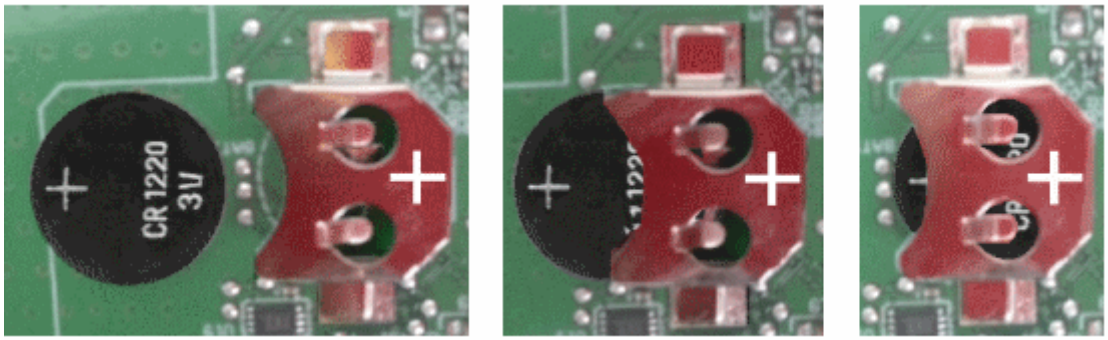
4.7 RTCバッテリーセルの交換

1. ネットワークモジュールにアクセスし、必要に応じてネットワークケーブルを外します。
2. ネットワークモジュールのネジを外し、スロットから取り外します。
3. ネットワークモジュールの背面にあるRTCバッテリーセルを見つけます。



4. 新しいバッテリーセル（CR1220タイプ）を入手します。

5. バッテリーセルを交換します。挿入するとプラスマーク(+)が表示されます。



6.ネットワークモジュールを交換してネジを固定し、操作中にネットワークケーブルが外れた場合は、ネットワークケーブルを再接続します。
7.ネットワークモジュールを接続し、日付と時刻を設定します。 詳細については、「日付と時刻」セクションを参照してください。

4.8 ネットワークモジュールの時刻を正確かつ永続的に更新する（ntpサーバー）

ネットワークモジュールのRTCを正確かつ迅速に更新するには、ネットワークモジュールのタイムソースとしてNTPサーバーを実装することをお勧めします。

LANには内部NTPサーバーがあります（ドメインコントローラー、メールサーバー、Outlookサーバーも通常はタイムサーバーです）が、pool.ntp.orgなどのパブリックntpサーバーを使用できます（関連するルールをファイアウォールシステムに追加した後）。

より詳細な情報は Contextual help>>>Settings>>>General>>>System details>>>Time & date settings セクションを参照下さい

4.9 ネットワークモジュールとUPSの時刻を同期させる

このセクションは、UPSが日付と時刻を管理できる場合にのみ有効です（確認については、UPSのユーザーマニュアルを参照してください）。

ネットワークモジュールはUTC時間を使用し、タイムゾーンとDSTを管理します。UPSは現地時間のみを管理します。

4.9.1 自動時刻同期

4.9.1.1 毎日 5 a.m.

UPS時間（現地時間）はネットワークモジュールと同期されます。

4.9.1.2 ネットワークモジュールの時間が失われた場合

ネットワークモジュールとUPSの時刻は、最後に認識されたネットワークモジュールの時刻とUPSの時刻の間の最も古い時刻と同期されます。

4.9.2 手動時刻同期

4.9.2.1 ネットワークモジュールから

ネットワークモジュールで、Contextual help>>>Settings>>>General>>>System details>>>Time & date settings セクションに移動し、時刻を更新します。

UPS時間（現地時間）は、ネットワークモジュールと直接同期されます。

4.9.2.2 UPSから

UPSで時刻が更新されると、ネットワークモジュールで時刻が同期されません。

4.10 Webページの言語を変更する

[設定]メニューでウェブページの言語を更新します。

1. Contextual help>>>User profile>>>Edit account に移動します。
2. 言語を選択し、**[Save（保存）]**ボタンを押します。

ログインページの言語は、デフォルトでは英語、またはサポートされている場合はブラウザの言語です。

4.11 ユーザー名とパスワードのリセット

4.11.1 他のユーザーの管理者として

1. Contextual help>>>Settings>>>Local users へ移動します。
2.ペンアイコンを押して、ユーザー情報を編集します。
3.ユーザー名を変更し、変更を[Save(保存)]します。
4. [Reset password(パスワードのリセット)]を選択し、次のオプションから選択します。
 ·ランダムに生成
 ·手動で入力します
 ·次回のログイン時にパスワードを強制的に変更する
5.自分のパスワードを入力して、変更を確認します。
6.変更を[Save(保存)]します。

4.11.2 自身のパスワードをリセットする

1. Contextual help>>>User profile に移動します。
2. Change password を押します。
3. 現在のパスワードと新しいパスワードを2回入力します。
4. [Submit(送信)]を押して変更を保存します。

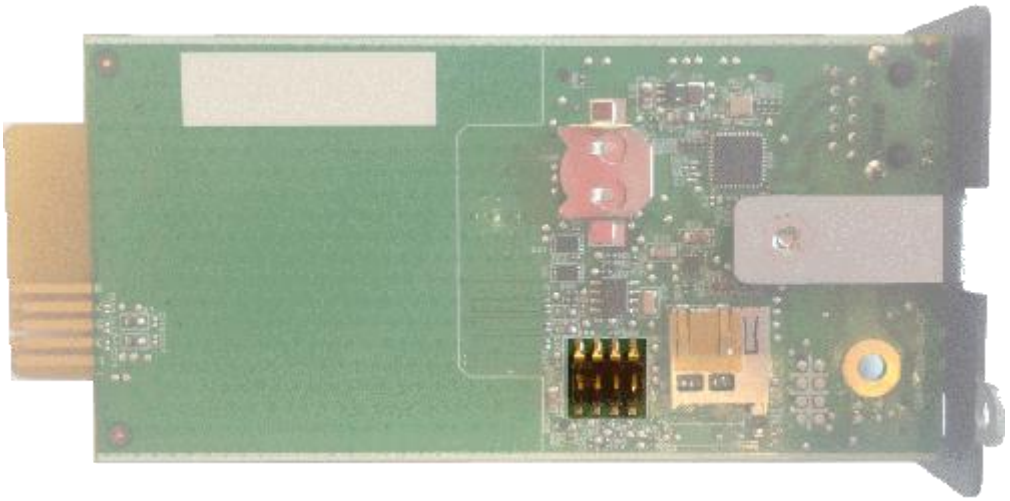
4.12 メイン管理者のパスワードを回復する

メインの管理者パスワードを回復するには、別の管理者にパスワードの初期化を依頼してください。

それが不可能な場合は、カードのサニティゼーションに進みます

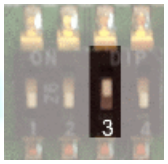
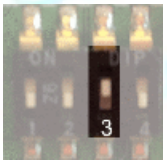
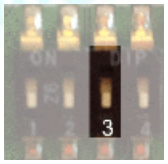
以下の手順では、カードをサニタイズし、すべてのデータを空白にします。
ネットワーク構成によっては、ネットワークモジュールが別のIPアドレスで再起動する場合があります。メインの管理者ユーザーのみがデフォルトのログインとパスワードのままになります。
ネットワークモジュールの再起動後にブラウザを更新して、ログインページにアクセスします。

1. ネットワークモジュールにアクセスし、必要に応じてネットワークケーブルを外します。
2. ネットワークモジュールのネジを外し、スロットから取り外します。
3. ネットワークモジュールの背面にあるSANITIZATIONスイッチを確認します。



4. 保護をはがします:

5. スイッチ番号3の位置を変更します。この変更は、次の電源投入時に検出され、サニタイズが適用されます。:

Case 1 :		
Case 2 :		

スイッチ1、2、または4を変更しても効果はありません。

6. ネットワークモジュールを交換してネジを固定し、必要に応じてネットワークケーブルを接続します。
7. メイン管理者のデフォルトの資格情報admin / adminを使用して、ネットワークモジュールを接続します。
8. 現在のパスワード強度ルールに従ってパスワードを変更する必要があります。

4.13 スタティックIPへの切り替え(手動)/ネットワークモジュールのIPアドレスの変更

管理者は、[設定]メニューでスタティックIPに切り替えて、ネットワークモジュールのIPアドレスを変更できます。

1. Contextual help>>>Settings>>>Network & Protocol>>>IPV4 に移動します。
2. [手動(スタティックIP)]を選択します。
3.次の情報を入力します。
   ・IPv4アドレス
   ・サブネットマスク

デバイス情報を簡単に読み取る
・デフォルトゲートウェイ

4. 変更を[Save(保存)]します。

4.14 簡単な方法でデバイス情報を読み取る

4.14.1 Webページ

製品情報は、Contextual help>>>Home>>>Energy flow diagram>>>Details にあります。具体的には、図の上部にあるボタンがあります。

4.15 電子メール通知用の一連のアラームのサブスクライブ

4.15.1 例1:1つのアラームのみをサブスクライブする(保護されていない負荷)

以下の手順に従ってください。

1.Contextual help>>>Settings>>>General>>>Email notification settings に移動します。

2. [New]ボタンを押して、新しい構成を作成します。

3.以下を選択します。

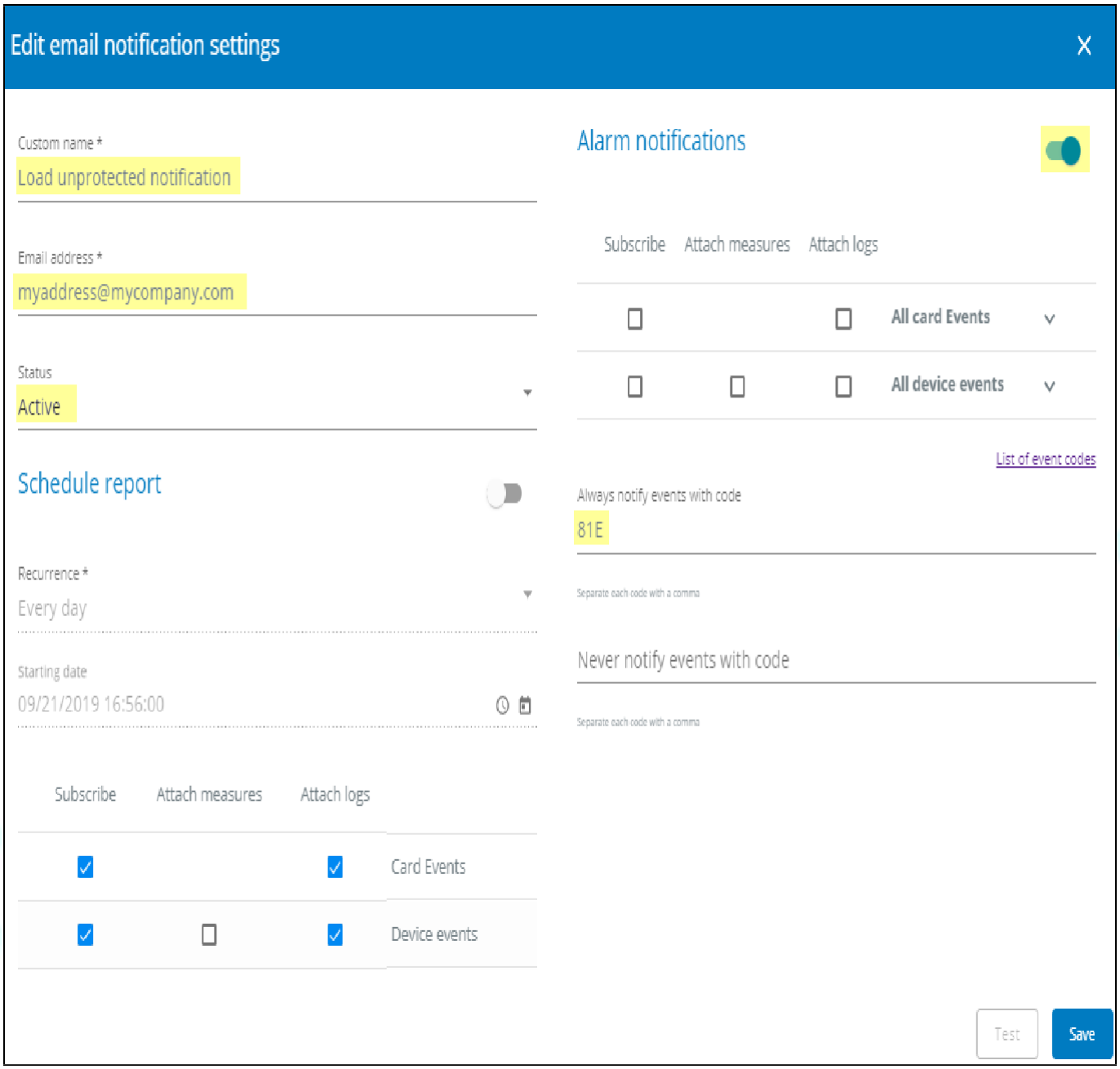
・アクティブ:YES

・構成名:保護されていない通知をロードします。

・電子メールアドレス:myaddress@mycompany.com

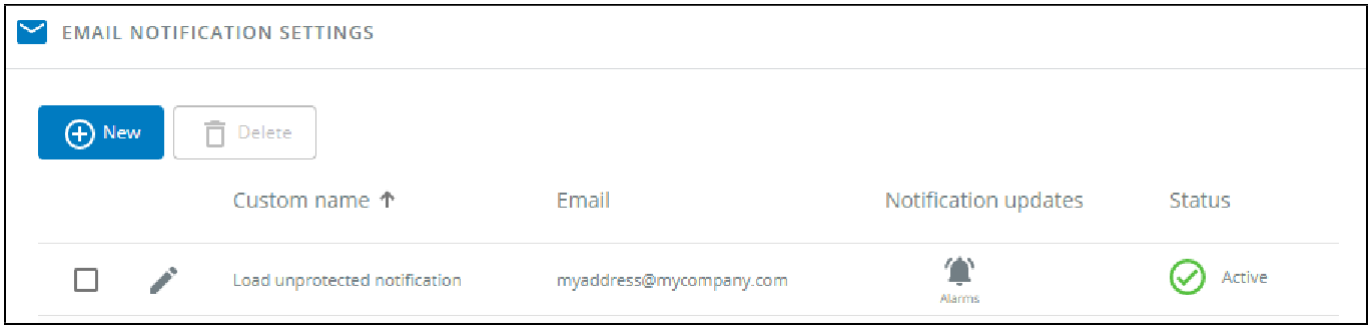
・イベントに関する通知:アクティブ

・常にコードでイベントに通知します:81E(ロードは保護されていません



この例では、カードまたはデバイスのイベントにサブスクリプションがない場合でも、デフォルトでログが添付されます。

1. **[Save（保存）]**を押すと、テーブルに新しい構成が表示されます。



4.15.2 例2：すべてのクリティカルアラームと特定の警告をサブスクライブする

以下の手順に従ってください。

1.Contextual help>>>Settings>>>General>>>Email notification settings に移動します。

2. **[New]**ボタンを押して、新しい構成を作成します。

3.以下を選択します。

・アクティブ：YES・

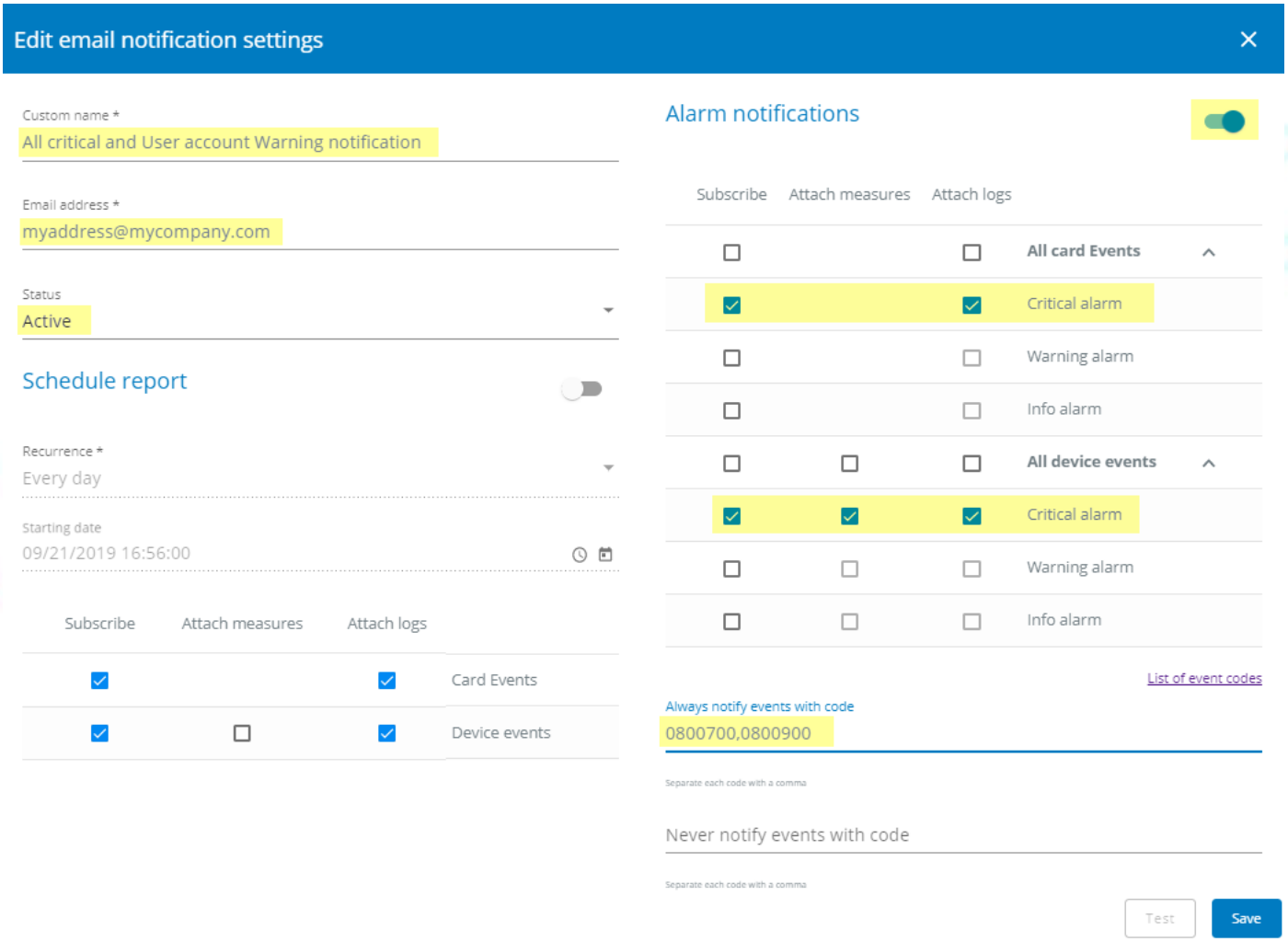
・構成名：すべてのクリティカルおよびユーザーアカウントの警告通知

・電子メールアドレス：myaddress@mycompany.com

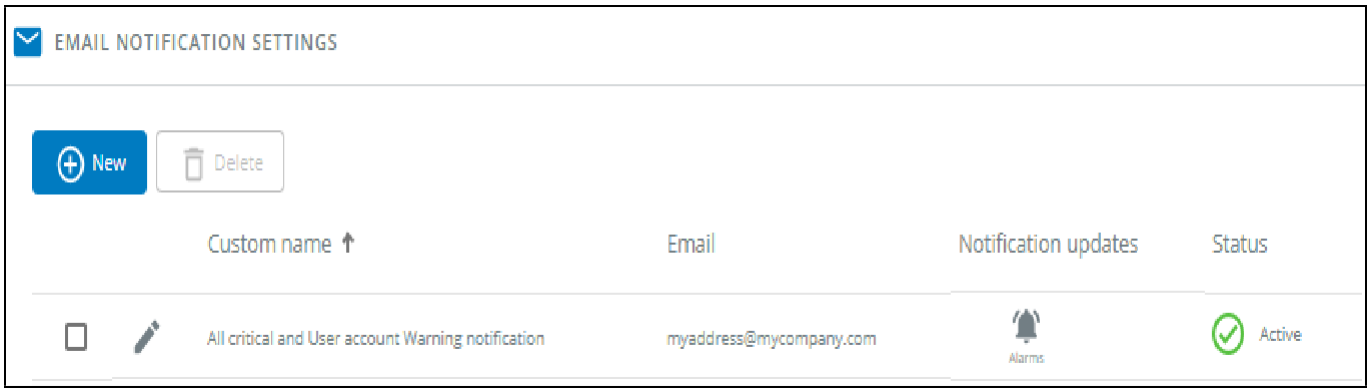
・イベントに関する通知：アクティブ

・クリティカルカードイベントとクリティカルデバイスイベントをサブスクライブする

・常にコード0800700、0800900でイベントに通知します（ユーザーアカウント–パスワードの有効期限が切れています、ユーザーアカウントはロックされています）



4. **[Save（保存）]**を押すと、テーブルに新しい構成が表示されます。

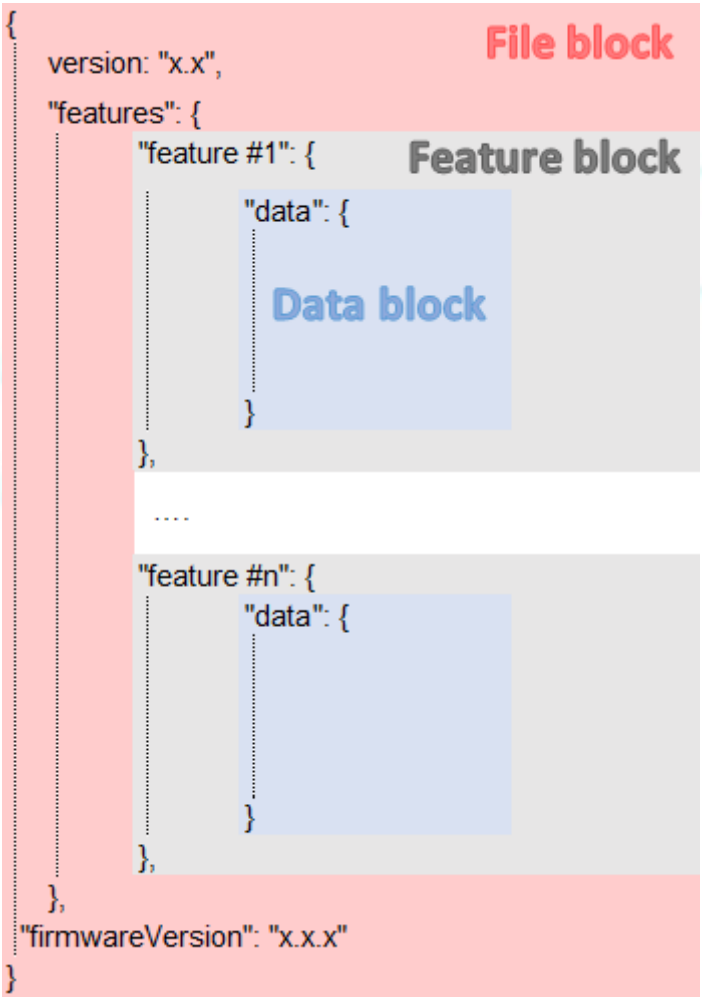


4.16 ネットワークモジュールの構成設定の保存/復元/複製

4.16.1 JSON構成ファイルを変更する

4.16.1.1 JSON ファイル構造

JSONファイルは3つのブロックで構成されています:



4.16.1.1.1 ファイルブロック

ファイルブロックは変更できません。これはJSONファイルの必須構造です。

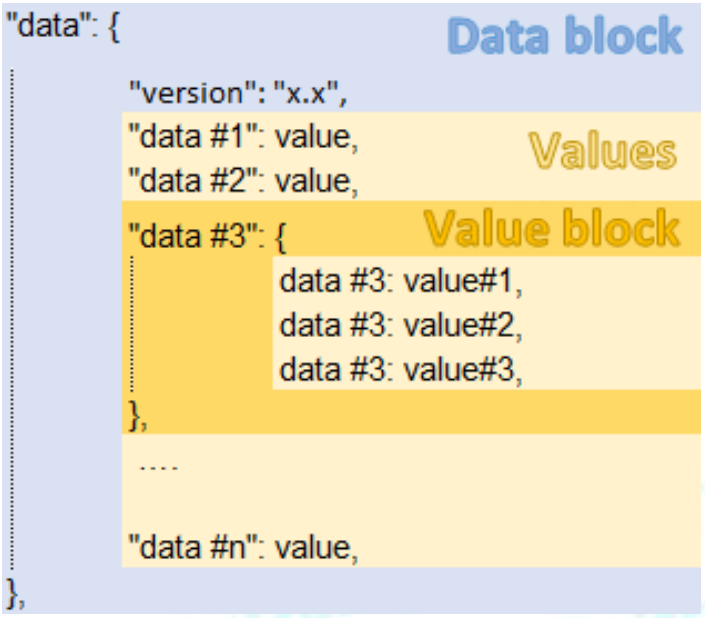
4.16.1.1.2 機能ブロック

機能ブロックには、機能の完全な定義が含まれています。

JSONファイルから削除された場合、この機能設定はカードに更新/復元されません。

4.16.1.1.3 データブロック

データブロックには、すべての機能設定値が含まれています。



a データブロック

データブロックは変更できません。これはJSONファイルの必須構造です。

b バリューブロック

Valueブロック内の一部の値を保持する必要がある場合、Valueブロック構造は変更できません。これは、JSONファイルの必須構造です。

JSONファイルから削除された場合、これらの値は更新/復元されません。

c バリュー

バリューはそのまま、変更、または削除できます。

削除されたバリューは更新/復元されません。

4.16.1.2 機密データ(パスワードなど)

機密データがパスフレーズでエクスポートされるかどうかによって、JSONファイルの構造はわずかに異なります。

4.16.1.2.1 JSONファイルはパスフレーズを使用して保存されます(推奨)

すべての機密データは以下の構造になります:

```
"password": {
        plaintext: "null",
        cyphered: "p-twlcjoV-a8FjMjkagL6w"
},
```

ファイルを復元すると、対応する設定が暗号化された値に基づいて更新されます。

4.16.1.2.2 JSONファイルはパスフレーズなしで保存されます

すべての機密データは以下の構造になります:

```
"password": {
        plaintext: "null",
},
```

ファイルを復元する場合、対応する設定はなされません。
対応する設定が以前に有効な値で設定されていなかった場合、復元の失敗につながる可能性があります。

4.16.1.3 JSONファイル例の変更

4.16.1.3.1 機密データの変更

機密データを変更するには、プレーンテキストに新しい値を入力し、暗号化されたエントリ(存在する場合)を削除する必要があります:

```
"password": {
        plaintext: "New password",
},
```

4.16.1.3.2 ローカルユーザーの追加

ローカルユーザーの追加または変更はまだ利用できません。変更できるのは事前定義されたアカウント(メイン管理者)のみです。

4.16.1.3.3 SNMP設定の変更

Original file:	Modified file:
SNMP disabled	SNMP enabled on port 161 SNMPv1 disabled SNMPv3 enabled 2 x accounts 1 x read only user (enabled) with Auth-Priv security level and passwords 1x read write user (enabled) with Auth-Priv security level and passwords 1 x active trap

Original file:

```
snmp: {
        data: {
                version: "x.x",
                dmeData: {
                        enabled: false,
                        port: xxxx,
                        v1: {
                                enabled: false,
                                communities: {
                                ..................................
                                }
                        },
                        v3: {
                                enabled: false,
                                users: [
                                        ..................................
                                ]
                        },
                        traps: {
                                receivers: [
                                ]
                        }
                }
        }
},
```

Modified file:

```
snmp: {
        data: {
                version: "x.x",
                dmeData: {
                        enabled: true,
                        port: 161,
                        v1: {
                                enabled: false,
                                communities: {
                                ..................................
                                }
                        },
                        v3: {
                                enabled: true,
                                users: [
                                        {
                                                name: "readonly",
                                                allowWrite: false,
                                                enabled: true,
                                                auth: {
                                                        enabled: true,
                                                        password: {
                                                                plaintext: xxxxxxxxxxxxxx
                                                        }
                                                },
                                                priv: {
                                                        enabled: true,
                                                        password: {
                                                                plaintext: yyyyyyyyyyyyyy
                                                        }
                                                }
                                        },
                                        {
                                                name: "readwrite",
                                                allowWrite: true,
                                                enabled: true,
                                                auth: {
                                                        enabled: true,
                                                        password: {
                                                                plaintext: zzzzzzzzzzzzzzzz
                                                        }
                                                },
                                                priv: {
                                                        enabled: true,
                                                        password: {
                                                                plaintext: wwwwwwwww
                                                        }
                                                }
                                        }
                                ]
                        },
                        traps: {
                                receivers: [
                                        {
                                                name: "xxxxxxxx",
                                                host: "xxx.xx.xxx.xx",
                                                port: xxx,
                                                community: "xxxxx",
                                                protocol: x,
                                                user: "",
                                                enabled: xxxx
                                        },
                                ]
                        }
                }
        }
},
```

4.16.1.3.4 部分的な更新/復元の作成

a 例:LDAP設定のみの更新/復元

以下のJSONコンテンツを復元すると、LDAP設定のみが更新/復元され、その他はすべて変更されません。

```
{
    "version": "x.x", "features":
    {
        "ldap": {
            "data": { "version":
            "x.x",
            "certificateData": [],
            "dmeData": {
                "enabled": true,
                "baseAccess": {
                    "security": {"ssl": 1,"verifyTlsCert": false},
                    "primary": {"name": "Primary","hostname": "xxxxxxxxx","port": xxxx},
                    "secondary": {"name": "xxxxxx","hostname": "xxxxxx","port": xxxx}, "credentials": {
                        "anonymousSearchBind": false,
                        "searchUserDN":
                        "CN=xxxx,OU=xxxx,OU=xxxx,OU=xxxx,DC=xxxx,DC=xxxx", "password":
                        {"plaintext": null}},
                    "searchBase": {"searchBaseDN": "DC=xxx,DC=xxx,DC=xxx"}
                    },
                "requestParameters": {
                    "userBaseDN": "OU=xxxx,DC=xxxx",
                    "userNameAttribute": "xxxx",
                    "uidAttribute":"objectSid:x-x-x-xx-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx", "groupBaseDN":
                    "OU=xxxx,DC=xxxx",
                    "groupNameAttribute": "xx",
                    "gidAttribute":"objectSid:x-x-x-xx-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx"
                    },
                "profileMapping": [
                    { "remoteGroup": "xxxxxxxxxxxxx","profile": 1},
                    { "remoteGroup": "xxxxxxxxxxxxx","profile": 2},
                    { "remoteGroup": "","profile": 0},
                    { "remoteGroup": "","profile": 0},
                    { "remoteGroup": "","profile": 0}
                    ]
                    }
                }
            },
        },
"firmwareVersion": "x.x.x"
}
```


4.16.1.4 JSONファイルの直感的でないデータ値

	Data	Values example

Account service	preferences>>>language	de: Deutsch en: English es: Español fr: Français it: Italiano ja: 日本語 ru: русскийzh_Hans: 简 体中文zh_Hant:繁體中文
	preferences>>>dateFormat	Y-m-d:YYYY-MM-DD d-m-Y:DD-MM-YYYY d.m.Y:DD.MM.YYYY d/m/Y:DD/MM/YYYY m/d/Y:MM/DD/YYYY d m Y: DD MM YYYY
	preferences>>>timeFormat	1: 24h 0: 12h
	preferences>>>temperatureUnit	1: ° C 2: ° F

	Data	**Values example**
Card	-	-

	Data	**Values example**
Date	timeZone	"Europe/Paris","Africa/Johannesburg","America/New_York","Asia/Shanghai" *Refer to the Web interface for the full list.*

	Data	**Values example**
email	periodicReport>>>periodicity	Every day Every week Every month
	periodicReport>>>startTime	timestamp (unix)

	Data	**Values example**

LDAP	baseAccess>>>security>>>ssl	1: None 2: Start TLS 3: SSL
	baseAccess>>>profileMapping>>>profile	administrators viewers operators

	Data	**Values example**
Measure	-	-

	Data	**Values example**
Modbus	mapping>>>configurations>>>transport	1: RTU 2: TCP
	mapping>>>configurations>>>map	network_card: Card System Information modbus_ms: Eaton ModbusMS compatible
	mapping>>>configurations>>>transportFilter	*: Access to all xx.xxx.xx.xx;yy.yyy.yy.yy;...: Access to a list of IP address
	mapping>>>configurations>>>deviceID	1 to 247
	mapping>>>configurations>>>access	0: None 1: Read only 3: Read/Write
	mapping>>>configurations>>>illegalReadBehavior	1: Return exception 2: return zeros

	rtu>>>configuration>>>baudrate	1: 1200pbs 2: 2400bps 3: 4800bps 4: 9600bps 5: 19200bps 6: 38400bps 7: 57600bps 8: 115200bps
	rtu>>>configuration>>>parity	1: None 2: Even 3: Odd
	rtu>>>configuration>>>stopBits	1: 1 Stop bit 2: 2 Stop bits

	Data	Values example
Modbus	mapping>>>configurations>>>transport	1: RTU 2: TCP
	mapping>>>configurations>>>map	network_card: Card System Information modbus_ms: Eaton ModbusMS compatible
	mapping>>>configurations>>>transportFilter	*: Access to all xx.xxx.xx.xx;yy.yyy.yy.yy;...: Access to a list of IP address
	mapping>>>configurations>>>deviceID	1 to 247
	mapping>>>configurations>>>access	0: None 1: Read only 3: Read/Write
	mapping>>>configurations>>>illegalReadBehavior	1: Return exception 2: return zeros

	Data	Values example
MQTT	-	-

	Data	Values example
Power outage policy	id	1: Primary 2: Group 1 3: Group 2

	Data	Values example
Remote user	preferences>>>language	de: Deutsch en: English es: Español fr: Français it: Italiano ja: 日本語 ru: русскийzh_Hans: 简 体中文zh_Hant:繁體中文

	preferences>>>dateFormat	Y-m-d: YYYY-MM-DD d-m-Y: DD-MM-YYYY d.m.Y: DD.MM.YYYY d/m/Y: DD/MM/YYYY m/d/Y: MM/DD/YYYY d m Y: DD MM YYYY
	preferences>>>timeFormat	1: 24h 0: 12h
	preferences>>>temperatureUnit	1: ° C 2: ° F

	Data	Values example
Schedule	scheduler	1: Primary 2: Group 1 3: Group 2
	recurrence	0: once 1: every day 2: every week
	shutdownTimeStamp	timestamp (unix)
	restartTimeStamp	timestamp (unix)

	Data	Values example
SMTP	-	-

	Data	Values example
SNMP	traps>>>receivers>>>protocol	1: SNMP v1 3: SNMP v2
	traps>>>receivers>>>user	User configuration cannot be duplicated without manual configuration through the Web interface.

	Data	Values example
Syslog	servers>>>protocol	1: UDP 2: TCP
	servers>>>tcpframing	1: TRADITIONAL 2: OCTET_COUNTING

	Data	Values example

Web server	-	-

4.16.2 CLIによる設定の保存/復元/複製

Information>>>CLI>>>save configurationに移動します| CLIを使用して設定を保存および復元する方法の例を取得するには、構成の復元セクションを参照してください

4.16.3 Webインターフェースによる設定の保存/復元/複製

Contextual help>>>Maintenance>>>Services sectionに移動して、Webインターフェースを介して設定を保存および復元する方法に関する情報を取得します

5　ネットワークマネジメントモジュールの保護

5.1　配電システムのサイバーセキュリティに関する考慮事項

5.1.1　目的

このセクションの目的は、業界やアプリケーションを超えた顧客が、現在のサイバーセキュリティ基準に従って電気システムの電力管理にイートンソリューションを適用できるようにするための高レベルのガイダンスを提供することです。
このドキュメントは、業界が推奨する標準とベストプラクティスを満たすために考慮すべき主要なセキュリティ機能とプラクティスの概要を提供することを目的としています。

5.1.2　イントロダクション

毎日、政府や商用のコンピューターネットワークに対するサイバー攻撃は数百万にのぼります。 米国サイバー軍によると、ペンタゴンシステムは1時間に25万回プローブされています。 同様の攻撃は、建物やユーティリティシステムを操作するネットワークなど、他の種類の情報ベースのスマートネットワークでも蔓延しています。 目的が知的財産を盗むことであろうと操作を停止することであろうと、不正なネットワークアクセスに使用されるツールと技術はますます洗練されています。

5.1.3　接続性ー産業用制御システム（ICS）のサイバーセキュリティに対処する必要があるのはなぜですか？

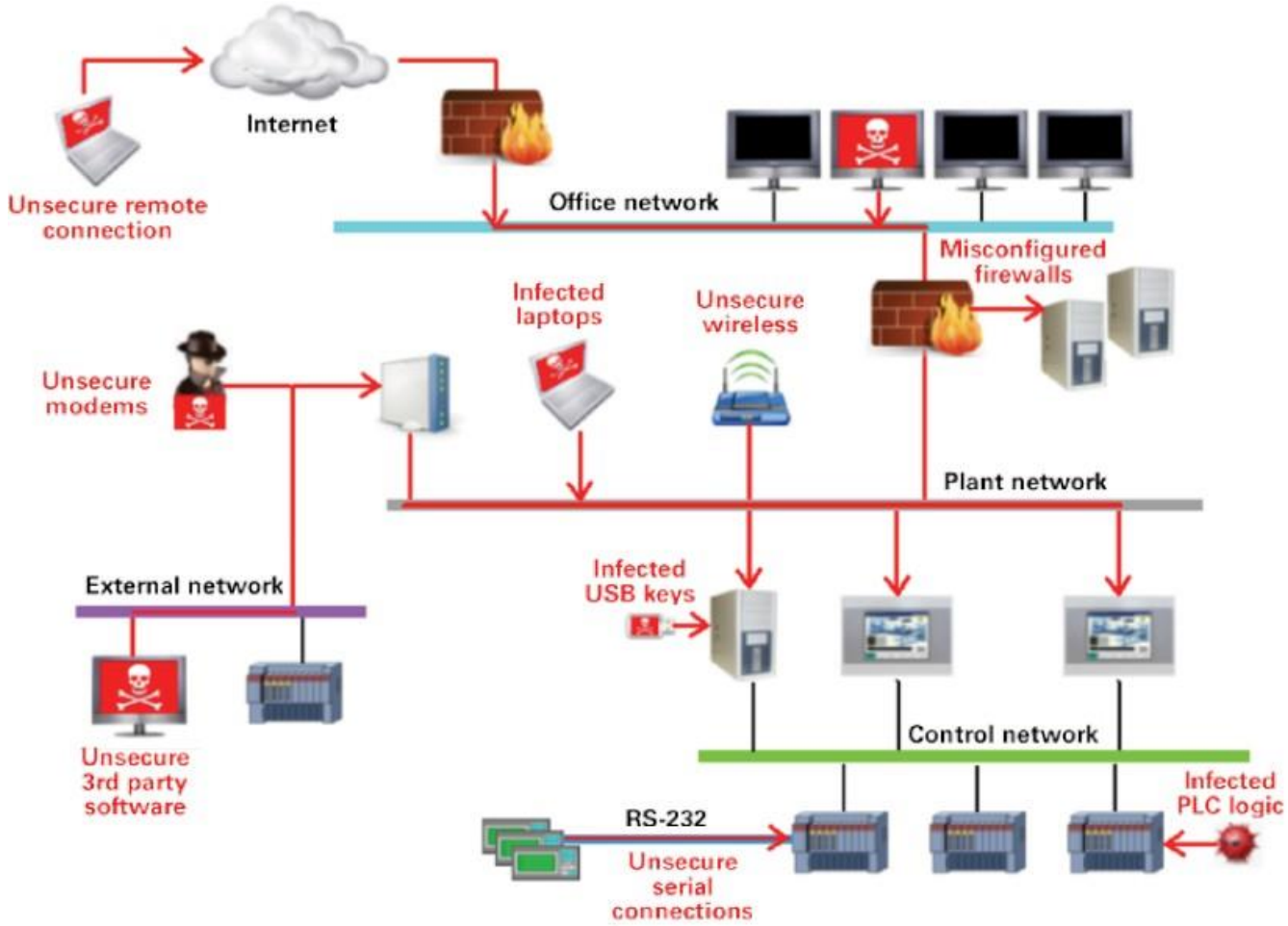
企業がフィールドデバイスを企業全体の情報システムに着実に統合している業界全体で、サイバーセキュリティに関する懸念が高まっています。 これは、個別の製造およびプロセス産業環境、さまざまな汎用および特定目的の商業ビル、さらにはユーティリティネットワークで発生します。 従来、電気システムは、独自のプロトコルを備えた専用トランシーバーを介してコンピューターに接続されたシリアルデバイスを介して制御されていました。 対照的に、今日の制御システムはますます大規模なエンタープライズネットワークに接続されており、これらのシステムは、コンピューターシステムに通常見られる同様の脆弱性にさらされる可能性があります。 情報技術（IT）とICSネットワークの違いは次のように要約できます。

- ITネットワークの主な焦点は、厳密なアクセス制御とデータ暗号化を使用して、データの機密性と整合性を確保することです。
- ICSネットワークの主な焦点は、データの安全性、可用性、および整合性です。
- エンタープライズセキュリティは、サーバーのデータを攻撃から保護します
- 制御システムのセキュリティは、ネットワークの他の部分に何が発生する可能性があるかに関係なく、施設が安全かつ確実に運用する能力を保護します

5.1.4　サイバーセキュリティの脅威ベクトル

サイバーセキュリティ脅威ベクトルは、悪意のある攻撃を仕掛けるためにエンティティがデバイスまたは制御ネットワークにアクセスするために使用できるパスまたはツールです。次の図は、他の方法では安全に見える可能性のあるネットワーク上の攻撃ベクトルの例を示しています。

5.1.4.1 制御ネットワークへのパス



上の図のパスは次のとおりです:

- インターネットを介してネットワークにアクセスする外部ユーザー
- ファイアウォールの設定ミス
- 安全でないワイヤレスルーターと有線モデム
- ファイアウォールの背後にあるネットワークにアクセスできる、他の場所にある感染したラップトップ
- 感染したUSBキーとPLCロジックプログラム
- 安全でないRS-232シリアルリンク
-

最も一般的な悪意のある攻撃は、次の形式で発生します:

・ウイルス–あるデバイスから別のデバイスに拡散し、操作に影響を与えるソフトウェアプログラム
・トロイの木馬–他のプログラムの内部に隠れてそのデバイスへのアクセスを提供する悪意のあるデバイスプログラム
・ワーム–ユーザーの操作なしで拡散し、ICSネットワークの安定性とパフォーマンスに影響を与えるデバイスプログラム
・スパイウェア–デバイスの構成を変更するデバイスプログラム

5.1.5 多層防御

従来のITシステムとICSには違いがありますが、「多層防御」の基本概念は両方に適用できます。 多層防御は、テクノロジー、人員、および運用機能を統合して、組織の複数のレイヤーにまたがるさまざまな障壁を確立する戦略です。これらの障壁には、ファイアウォール、侵入検知ソフトウェア/コンポーネント、ウイルス対策ソフトウェアなどの電子的対策と、物理的な保護ポリシーおよびトレーニングが含まれます。 基本的に、バリアはネットワークへの攻撃の可能性を減らし、「侵入者」を検出するメカニズムを提供することを目的としています。

5.1.6 脅威ベクトルの設計

5.1.6.1 ファイアウォール

ファイアウォールは、ICSネットワーク内のさまざまなネットワークセグメントおよびゾーン間の通信に、厳格で多面的なルールを追加する機能を提供します。 これらは、関連する必要なデータを通過させながら、特定のセグメントからのデータをブロックするように構成できます。 ネットワーク内にあるデバイス、アプリケーション、およびサービスを完全に理解することで、ネットワーク内のファイアウォールの適切な展開と構成をガイドできます。 ネットワークに展開できるファイアウォールの一般的なタイプは次のとおりです：

·ネットワーク層で機能するパケットフィルターまたは境界ファイアウォール
これらのファイアウォールは主にネットワーク層で動作し、ポート番号とプロトコルに基づいて事前に確立されたルールを使用して、分離されたネットワークに出入りするパケットを分析します。
これらのファイアウォールは、これらのルールに基づいて通過を許可または拒否します。

·ホストファイアウォール
これらのファイアウォールは、デバイスのポートとサービスを保護するソフトウェアファイアウォールソリューションです。 ホストファイアウォールは、デバイスの着信および発信トラフィックを追跡、許可、または拒否するルールを適用できます。これらのルールは主に、ICSに簡単に接続できるモバイルデバイス、ラップトップ、およびデスクトップにあります。

·アプリケーションレベルのプロキシファイアウォール
これらのファイアウォールは、制御ネットワーク内の個々のデバイスとコンピューターを非表示にして保護する、安全性の高いファイアウォール保護方法です。これらのファイアウォールはアプリケーション層で通信し、より優れた検査機能を提供できます。アプリケーションレベルのプロキシファイアウォールは広範なログデータを収集するため、ICSネットワークのパフォーマンスに悪影響を与**える可能性があります。**

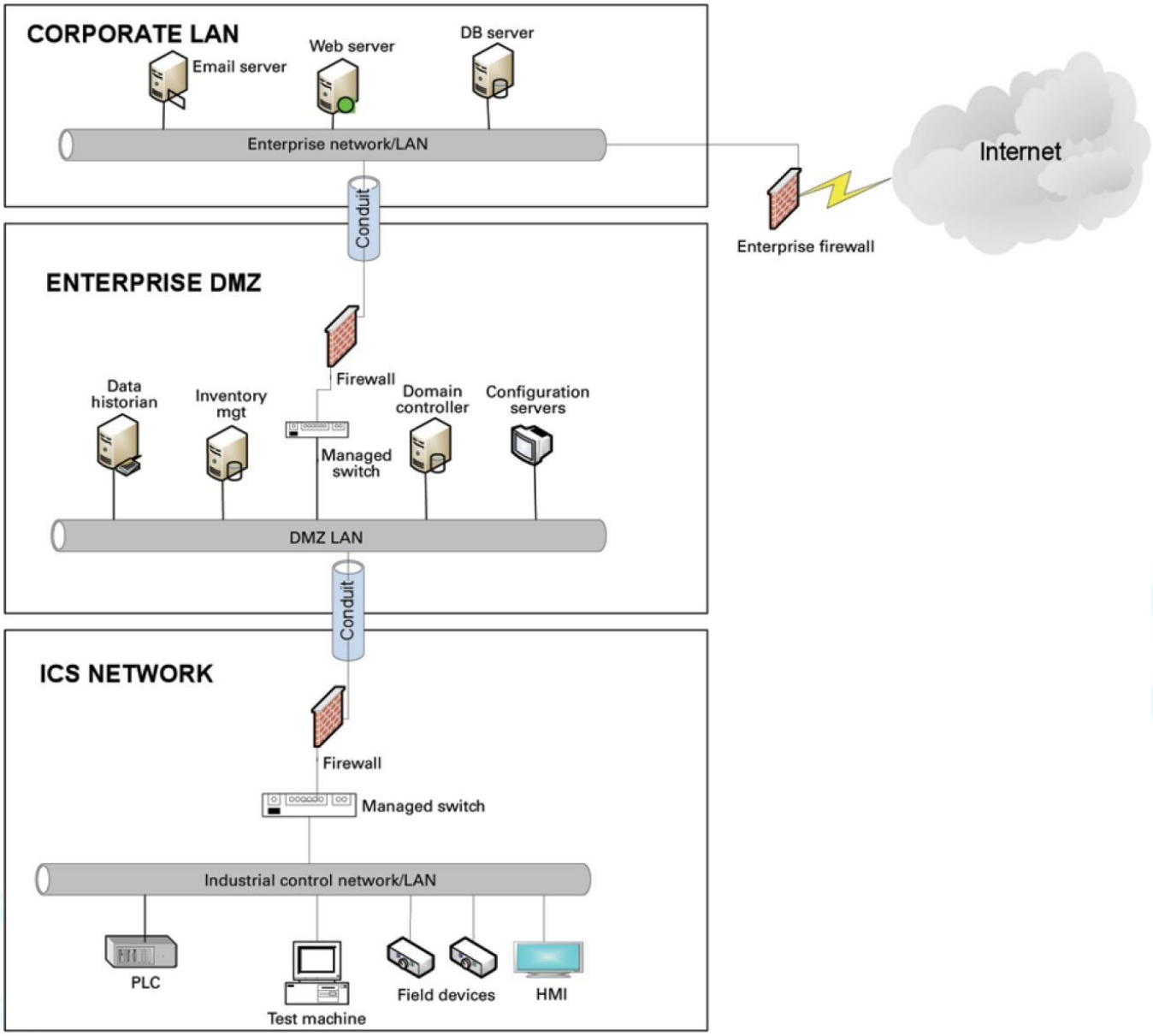
·ステートフルインスペクションファイアウォール
これらのファイアウォールは、オープンシステム相互接続（OSI）のネットワーク、セッション、およびアプリケーション層で機能します。ステートフルインスペクションファイアウォールは、許可されたセッションに属するパケットのみを許可するため、パケットフィルターファイアウォールよりも安全です。
これらのファイアウォールは、セッションの確立時にユーザーを認証し、パケットを分析して、予想されるペイロードタイプが含まれているかどうかを判断したり、アプリケーション層で制約を適用したりできます。

·SCADAハードウェアファイアウォール
これらはハードウェアベースのファイアウォールであり、制御ネットワーク内のデバイスでの異常な動作の監視に基づいてICSを防御します。たとえば、オペレータステーションのコンピューターが突然PLCをプログラムしようとすると、このアクティビティがブロックされ、システムへの重大なリスクを防ぐためにアラームが発生する可能性があります。

5.1.6.2 非武装地帯（DMZ）

ネットワークセグメンテーションは、安全な制御ネットワークを確立する上で重要な考慮事項です。 重要なコンポーネントをグループ化し、従来のビジネスITネットワークから分離することにより、ファイアウォールを使用してDMZを作成する必要があります。 次の図に示すように、組織のコアネットワークと分離された制御システムのネットワークの間にDMZを配置して、少なくとも3層アーキテクチャを採用する必要があります。

5.1.6.2.1 安全な制御ネットワークのための3層アーキテクチャ



上の図は、制御ネットワークが制御機能に基づいてレイヤーまたはゾーンに分割されていることを示しています。これらの機能は、セキュリティ制御を提供するコンジット（ゾーン間の接続）によって接続されています：

- ゾーンへのアクセスを制御する
- サービス拒否（DOS）攻撃またはマルウェアの転送に抵抗する
- 他のネットワークシステムをシールドする
- ネットワークトラフィックの整合性と機密性を保護します

ネットワークのセグメンテーションを超えて、アクセス制御（物理的および論理的の両方）を定義して実装する必要があります。

アクセス制御を設計する際の重要な考慮事項は、特定のゾーン内とゾーン間の両方で必要な相互作用を定義することです。 これらの相互作用は明確にマッピングされ、必要に応じて優先順位が付けられる必要があります。 ファイアウォールに突き刺さったすべての穴と、アクセスを提供したり、追加の接続を作成したりする重要でない機能は、攻撃にさらされる可能性を高めることを理解することが重要です。 その場合、システムは、それに接続しているデバイスと同じくらい安全になります。

正しくマッピングされていれば、制御システムの信頼性と機能への潜在的な悪影響は無視できるはずです。ただし、この要素は、追加のコスト（ファイアウォールやその他のネットワークインフラストラクチャの観点から）と環境の複雑さをもたらします。

5.1.6.3 侵入検知および防止システム（IDPS）

これらは主に、ICSネットワークで発生する可能性のあるインシデントの特定、それらに関する情報のログ記録、停止の試行、およびICSセキュリティ管理者への報告に重点を置いたシステムです。
これらのシステムはICSネットワークで重要であるため、攻撃の定期的な標的であり、それらを保護することは非常に重要です。 展開されるIDPSテクノロジーのタイプは、監視する必要のあるイベントのタイプによって異なります。
IDPSテクノロジーには4つのクラスがあります：

- ネットワークベースのIDPSは、特定のICSネットワークセグメントまたはデバイスのネットワークトラフィックを監視し、ネットワークおよびアプリケーションプロトコルのアクティビティを分析して、疑わしいアクティビティを特定します。
- ワイヤレスIDPSは、ワイヤレスネットワークトラフィックを監視および分析して、ICSワイヤレスネットワークプロトコルに関連する疑わしいアクティビティを特定します。
- ネットワーク動作分析IDPSは、ICSネットワークトラフィックを調べて、DOS攻撃などの異常なトラフィックフローを生成する脅威を特定します。
- ホストベースのIDPSは、疑わしいアクティビティがないか、単一のICSネットワークホスト内で発生する特性とイベントを監視します。

5.1.7 ポリシー、手順、基準およびガイドライン

多層防御戦略を成功させるには、十分に文書化され、継続的にレビューされているポリシー、手順、基準、およびガイドラインが必要です。

- ポリシーは、目的を達成し、誰が、何を、そしてなぜに対処するために実行しなければならない手順またはアクションを提供します
- 手順は、操作のために従うべき詳細な手順を提供し、方法、場所、および時期に対処します
- 基準は通常、特定のハードウェアとソフトウェアを参照し、特定のテクノロジーまたはパラメーターの均一な使用と実装を指定します
- ガイドラインは、ポリシー、手順、および基準を実装する方法に関する推奨事項を提供します

5.1.7.1 ICSネットワークを理解する

ネットワークでホストされているすべてのデバイス、アプリケーション、およびサービスのインベントリを作成すると、監視対象の初期ベースラインを確立できます。 これらのコンポーネントが識別および理解されると、制御、所有権、および運用上の考慮事項を作成できます。

5.1.7.2 ログとイベントの管理

パフォーマンスとセキュリティの両方の観点から、ネットワーク内で何が起こっているかを理解することが重要です。これは、制御システム環境で特に当てはまります。

ログとイベントの管理には、ルーター、ファイアウォール、IDS / IPSなどのインフラストラクチャコンポーネント、およびホスト資産の監視が含まれます。セキュリティ情報およびイベント管理（SIEM）システムは、さまざまなソースからイベントを収集し、相関関係とアラートを提供できます。

イベントの生成と収集、またはSIEMの実装でさえ、それだけでは十分ではありません。多くの組織にはSIEMソリューションがありますが、アラートは監視されていないか、見過ごされています。

監視には、環境を監視する機能と監視を実行する機能の両方が含まれます。機能に関連しています

環境の設計とアーキテクチャ。監視機能を考慮した方法で構築されていますか？キャパシティは、情報の意味のある解釈を実行し、タイムリーで適切なアクションを開始するために必要なリソース（人員、ツール、専門知識）に話しかけます。

監視を通じて、組織は疑わしいアクティビティや悪意のあるアクティビティなどの問題を特定できます。新しい（許可されていない可能性のある）デバイスが環境に出現すると、認識を高めることができます。ログとイベントの管理が制御システムデバイスの機能や信頼性に悪影響を与えないように、慎重に検討する必要があります。

5.1.7.3 セキュリティポリシーと手順

「資産の所有者」を特定し、サイバーセキュリティプログラムのポリシーと手順を開発することが重要です。これらのポリシーは、効果的であるために実用的で強制力がある必要があります。 ポリシーは、物理的なアクセス、請負業者、ベンダーなどのアクセス関連の問題にも対処する必要があります。

既存の（従来の）IT標準およびポリシーは、制御システムに適用されない（または考慮されていない）場合があります。 ギャップ分析を実行して、既存のポリシーでカバーされていない（または適切にカバーされていない）コンポーネントを特定する必要があります。 既存のポリシーおよび標準との関係を明示的に特定し、新しいポリシーまたはサポートポリシーを開発する必要があります。 産業用制御システムの管理者は、ICSネットワークの保護に役立つポリシーを実装するために、適切な承認と管理の完全なサポートを持っていることが重要です。

5.1.7.4 ICS の強化

システム強化の目標は、ICSネットワークを安全に構成することにより、できるだけ多くのセキュリティリスクを軽減することです。アイデアは、必要なものに基づいて構成を確立し、侵入者に別の可能性のあるエントリポイントを提供する可能性のある不要なサービスやアプリケーションを排除することです。

展開されているさまざまなプラットフォームと製品（オペレーティングシステム、アプリケーション、およびドライブ、メーター、HMIデバイスなどのインフラストラクチャ要素）に対して、最小限のセキュリティベースラインを確立する必要があります。 該当する場合は、次のアクションを実装する必要があります：

- 不要なサービスを無効にする
- 匿名FTPを無効にする
- クリアテキストプロトコルを使用しないでください（たとえば、Telnetの代わりにSSH v2を使用してください）
- 必要なパッケージ/アプリケーション/機能のみをインストールする
- ウイルス対策ソリューションを展開する（可能な場合）
- USBデバイスの使用を無効にするか制御する
- 警告バナーを作成します
- デフォルトのパスワードを変更する（例：SNMP）

基本オペレーティングシステムプラットフォームを制御するデバイスにこれらのアクションを実装する方が簡単な場合があります。ただし、いくつか上記の項目のうち、製品固有の構成オプションから構成できます。

このような変更は、制御システムデバイスの機能に影響を与える可能性があります。この影響を最小限に抑えるために、展開前に広範なテストを実施する必要があります。

5.1.7.5 継続的な評価とセキュリティトレーニング

ICSのセキュリティと、ICSを操作し、それに依存する人々の安全を確保するために、ICSネットワーク管理者と通常のユーザーを適切にトレーニングすることが重要です。

問題を特定し、他の防御可能なネットワーク要素の有効性を理解するには、継続的な脆弱性評価が重要です。

評価には、以下のテストと検証を含める必要があります：

- 監視機能とアラートがトリガーされ、期待どおりに応答されます
- サービスとアプリケーションのデバイス構成
- ゾーン内およびゾーン間の予想される接続
- 環境内にこれまで知られていなかった脆弱性が存在する
- パッチの有効性

評価を実施するためのプログラムを確立する必要があります。

実際の評価は、社内またはサードパーティの組織である資格のあるリソースによって実行される必要があります。 誰が評価を実行するかに関係なく、社内リソースは評価アクティビティの計画、スコーピング、およびサポートに関与する必要があり、そのように適切にトレーニングする必要があります。

評価は、以下に対処するために明確に定義された方法論に従って実施する必要があります：

- 物理的セキュリティ
- 人とプロセス
- ネットワークセキュリティー
- ホストのセキュリティ
- アプリケーションのセキュリティ（社内で開発されたものと市販されているもの（COTS）の両方）

5.1.7.6 パッチ管理の計画と手順

問題のタイムリーな認識と適切なアクションに基づいて、パッチ適用と脆弱性管理のプロセスを確立する必要があります。このプロセスでは、制御システム環境を構成するすべての要素を考慮に入れる必要があります。
環境内のさまざまなコンポーネントの脆弱性および助言情報について、情報リソースを特定する必要があります。これらには、ベンダー固有のソース、および脆弱性アドバイザリ情報を提供するその他のパブリックサービスまたは商用サービスを含める必要があります。たとえば、National Vulnerability Database（NVD）は、で特定された脆弱性に関連する情報を提供します。

一般的なITコンポーネント、産業用制御システムのサイバー緊急対応チーム（ICS-CERT）は、制御システムに固有のアドバイザリを公開しています。
環境内のコンポーネントごとに、定期的なパッチ展開スケジュールを確立する必要があります。コンポーネントに応じて、これは、コンポーネン

トまたはベンダーのパッチまたは脆弱性に関連する問題の過去の頻度に応じて、月次スケジュールから必要に応じた展開までさまざまです。
さらに、帯域外または緊急パッチ管理は考慮され、資格を定義する必要があります。
脆弱性情報とアドバイザリを定期的に確認し、問題の相対的な重大度と緊急性を判断するために評価を実行する必要があります。
プロセスの要素には、準備、スケジューリング、および変更の管理も含める必要があります。テストとロールバックの手順。
範囲、期待、およびレポートを含む、利害関係者への展開前の通知。テストは重要な要素です。
パッチ適用の効果を明確に理解する必要があります。制御システムコンポーネントへの意図しないまたは予期しない影響は、パッチを展開する決定に影響を与えます。パッチを安全に展開できないと判断されたが、問題の重大度が重大な懸念事項であると判断された場合は、補償管理を調査する必要があります。

5.1.8 結論

重要な資産を保護するために、すべての組織はサイバーセキュリティの脅威を真剣に受け止め、組織のニーズに固有のシステム全体の防御的アプローチで積極的に対応する必要があります。

完全に安全な保護方法はありません。 今日有効な防御メカニズムは明日は有効ではない可能性があります。サイバー攻撃の方法と手段は常に変化しています。 ICS管理者は、サイバーセキュリティの変化を認識し続け、管理するシステムの潜在的な脆弱性を防ぐために引き続き取り組むことが重要です。

5.1.9 用語と定義

DMZ	非武装ゾーンは、組織の外部とのインターフェースとなる論理的または物理的なサブネットワークです。サービスをより大きな信頼されないネットワークに提供し、セキュリティの追加レイヤーを提供しています。
Encryption	アルゴリズムを使って平文や明文を変換し、特別な知識を持っている人以外には読めないようにするプロセス。
ICS	他の装置またはシステムの動作を管理、命令、指示、または規制する装置または装置のセット。
Protocol	通信チャネルを介して情報を送信するために必要なデータ表現、シグナリング、認証、エラー検出のための標準的なルールのセット。

5.1.10 頭字語

COTS	Commercially Off-the-Shelf
DMZ	Demilitarized Zone
DOS	Denial of Service
FTP	File Transfer Protocol
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems – Cyber Emergency Response Team
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IT	Information Technology
NVD	National Vulnerability Database
OSI	Open System Interconnection
PLC	Programmable Logic Controller

SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SIEM	Security Information and Event Management
USB	Universal Serial Bus

5.1.11 参照

[1]推奨プラクティス：多層防御戦略による産業用制御システムのサイバーセキュリティの改善、2009年10月
https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf
[2] NIST.SP.800-82産業用制御システム（ICS）セキュリティガイド、2011年6月
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
[3] NIST.SP.800-94侵入検出および防止システムガイド（IDPS）、2007年2月
http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[4]産業用制御システムにおける一般的なサイバーセキュリティの脆弱性、2011年5月
http://ics-cert.uscert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
[5]ネットワークセキュリティモニタリングのタオ、2005年リチャードベイトリ

5.2 サイバーセキュリティが推奨するセキュリティ強化のガイドライン

5.2.1 イントロダクション

このネットワークモジュールは、サイバーセキュリティを重要な考慮事項として設計されています。 このセクションの推奨事項に従って実装すると、ネットワークモジュールに対するサイバーセキュリティのリスクを最小限に抑えることができる、多数のサイバーセキュリティ機能が製品で提供されるようになりました。 このセクションの「安全な構成」または「強化」のガイドラインは、システムに対するサイバーセキュリティのリスクを適切に最小限に抑えるために、製品を安全に展開および保守するための情報をユーザーに提供します。

Eatonは、製品のサイバーセキュリティリスクを最小限に抑えることに取り組んでおり、製品とソリューションにサイバーセキュリティのベストプラクティスと最新のサイバーセキュリティテクノロジーを導入しています。 お客様にとって、より安全で信頼性が高く、競争力のあるものになります。 イートンはまた、www.eaton.com ／ cybersecurityで参照できるサイバーセキュリティのベストプラクティスホワイトペーパーを顧客に提供しています。

5.2.2 安全な構成に関するガイドライン

5.2.2.1 資産の識別とインベントリ

システム内のすべてのデバイスを追跡することは、システムのサイバーセキュリティを効果的に管理するための前提条件です。 各コンポーネントを一意に識別する方法で、システム内のすべてのコンポーネントのインベントリを維持するようにしてください。このネットワークモジュールを容易にするために、次の識別情報をサポートします–製造元、タイプ、シリアル番号、ファームウェアバージョン番号、および場所。

5.2.2.1.1 ネットワークモジュールの識別とそのファームウェア情報

Contextual help>>>Maintenance>>>System information に移動して取得できます。

定義

- システム名
- 製品
- 物理的な名前
- ベンダー
- UUID
- 部品番号
- シリアルナンバー
- ハードウェアバージョン
- 場所
- 連絡先

ファームウェアバージョン

- ファームウェアバージョン
- ファームウェアSHA
- ファームウェアの日付
- ファームウェアのインストール日
- ファームウェアのアクティベーション日
- ブートローダーバージョン

COPY TO CLIPBOARDボタンは、情報をクリップボードにコピーします。

5.2.2.1.2 通信の設定

Contextual help>>>Settings>>>Network & Protocol に移動して取得できます。

LAN

- Link status
- MAC address
- Configuration

IPV4

- Status
- Mode
- Address
- Netmask
- Gateway

Domain

- Mode
- FQDN
- Primary DNS
- Secondary DNS

IPV 6

- Status
- Mode
- Addresse
-
-

5.2.2.1.3 デバイス詳細

Contextual help>>>Home>>>Energy flow diagram>>>Details に移動して取得できますDetails

- Name
- Model
- P/N
- S/N
- Location
- FW version

COPY TO CLIPBOARDボタンは、情報をクリップボードにコピーします。

5.2.2.2 物理的保護

産業用制御プロトコルは、プロトコルレベル、物理ポート、およびコントローラーモードスイッチで暗号化保護を提供しないため、サイバーセキュリティリスクにさらされます。このような場合、物理的なセキュリティは重要な防御層です。ネットワークモジュールは、物理的に安全な場所に配置および運用されることを考慮して設計されています。

- ネットワークモジュールおよび関連システムを含むキャビネットおよび/またはエンクロージャへの物理的アクセスは、常に制限、監視、およびログに記録する必要があります。
- 盗聴や妨害行為を防ぐために、通信回線への物理的なアクセスを制限する必要があります。あるキャビネットから別のキャビネット間を走る通信回線には、金属製のコンジットを使用することをお勧めします。
- デバイスへの不正な物理的アクセスを持つ攻撃者は、デバイスの機能に重大な混乱を引き起こす可能性があります。ロック、カードリーダー、ガードなど、その場所への物理的なアクセス制御を組み合わせて使用する必要があります。
- ネットワークモジュールは、次の物理アクセスポート、コントローラーモードスイッチ、およびUSBポートをサポートします：RJ45、USB A、USBMicro-B。それらへのアクセスを制限する必要があります。
- 操作（ファームウェアのアップグレード、構成の変更、ブートアプリケーションの変更など）のために、許可されていないUSBデバイスまたはSDカードを接続しないでください。
- USBまたはSDカードスロットを介してポータブルデバイスを接続する前に、マルウェアやウイルスがないかデバイスをスキャンしてください。

5.2.2.3 承認とアクセス制御

ネットワークモジュールで提供される論理アクセスメカニズムを安全に構成して、デバイスを不正アクセスから保護することが非常に重要です。 イートンは、システムへのアクセスが正当なユーザーのみに制限されるように、利用可能なアクセス制御メカニズムを適切に使用することをお勧めします。 また、そのようなユーザーは、職務/職務を完了するために必要な特権レベルのみに制限されています。

- 最初のログイン時にデフォルトの資格情報が変更されていることを確認します。ネットワークモジュールは、デフォルトの資格情報を使用して本番環境に委託しないでください。デフォルトの資格情報がマニュアルに公開されているため、これは重大なサイバーセキュリティの欠陥です。
- パスワード共有なし-各ユーザーが、パスワードを共有するのではなく、目的の機能のために自分のパスワードを取得するようにします。ネットワークモジュールのセキュリティ監視機能は、各ユーザーが独自のパスワードを持っていることを確認して作成されます。ユーザーがパスワードの共有を開始するとすぐに、セキュリティ制御が弱まります。
- 管理者権限の制限-脅威アクターは、正当な資格情報、特に特権の高いアカウントに関連付けられた資格情報の制御を取得することにますます焦点を合わせています。特権をユーザーの職務に必要なものだけに制限します。
- 定期的なアカウントのメンテナンスを実行します（未使用のアカウントを削除します）。
- 人事異動があるたびに、パスワードやその他のシステムアクセス資格情報を変更します。
- 追加のセキュリティ対策として、ユーザー名とパスワードとともにクライアント証明書を使用します。

ネットワークモジュールのユーザー管理の説明：

- ユーザーとプロファイルの管理: Contextual help>>>Settings>>>Local users に移動します。

  Add users
  Remove users
  Edit users

- パスワード/アカウント/セッション管理: (Contextual help>>>Settings>>>Local users に移動します)

  パスワード強度ルール-最小長/最小大文字/最小小文字/最小桁/特殊文字アカウントの有効期限-アカウントの有効期限が切れるまでの日数/アカウントをブロックするまでの試行回数セッションの有効期限-アクティビティタイムアウトなし/セッションリース時間

  （推奨される）デフォルト値については、埋め込みヘルプの「デフォルト設定パラメーター」を参照してください。 さらに、アカウントの有効期限を有効にして、ユーザーにパスワードを定期的に更新させることができます。

- デフォルトの資格情報：admin / admin

  デフォルトの「admin」パスワードの変更は、最初の接続時に適用されます。また、Contextual help>>>Settings>>>Local users

pageからデフォルトの「admin」ユーザー名を変更することをお勧めします。ユーザーアカウントを編集する方法については、埋め込まれたヘルプに従ってください。

- サーバーおよびクライアント証明書の構成:(Contextual help>>>Settings>>>Certificateに移動します）構成方法については、埋め込まれたヘルプに従ってください。

5.2.2.4 未使用の機能を無効にする

ネットワークモジュールは、ファームウェアのアップグレード、構成の変更、電源スケジュールの設定などの複数のオプションを提供します。デバイスは、SSH、SNMP、SMTP、HTTPSなどのデバイスに接続するための複数のオプションも提供します。SNMPv1などのサービスは安全でないと見なされ、イートンはすべてを無効にすることをお勧めします そのような安全でないサービス。

- USBやSDカードなどの未使用の物理ポートを無効にすることをお勧めします。
- SNMPv1などの安全でないサービスを無効にする。

ネットワークセキュリティー

「umac」ベースのMACアルゴリズムの使用は避け、カードのSSHインターフェースへの接続中は安全なアルゴリズムのみを使用してください
イートンは、次の安全なアルゴリズムの使用を推奨しています。

- キー交換アルゴリズム
  - curve25519-sha256@libssh.org
  - diffie-hellman-group14-sha256
  - diffie-hellman-group18-sha512
- 暗号化アルゴリズム
  - aes256-ctr
  - aes256-gcm@openssh.com
  - aes128-gcm@openssh.com
- メッセージ認証コード(MAC) アルゴリズム
  - hmac-sha2-512-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com

ネットワークモジュールは、システムおよび構成内の他のデバイスとの通信を容易にするネットワークアクセスを提供します。 ただし、この機能は、安全に構成されていない場合、大きなセキュリティホールを開く可能性があります。

Eatonは、ネットワークを論理エンクレーブに分割し、通信をホスト間パスに制限することを推奨しています。 これにより、機密情報と重要なサービスを保護し、ネットワーク境界の侵害による被害を制限できます。 少なくとも、ユーティリティ産業用制御システムネットワークは、セキュリティ制御を向上させるために3層アーキテクチャ(NIST SP800-82 [R3]で推奨）にセグメント化する必要があります。

ファイアウォール、侵入検知/保護デバイスなどの適切なネットワーク保護デバイスを展開します。

配電システムに関するイートンサイバーセキュリティの考慮事項[R1]で、さまざまなネットワークレベルの保護戦略に関する詳細情報を見つけてください。 ネットワークモジュールがスムーズに動作するために必要なアクセスを許可するようにファイアウォールを構成するには、以下の情報を使用してください。

- デバイスで実行されているすべてのポートとサービスのリストを取得するために下記に移動します。
  Information>>>Specifications/Technical characteristics

- SNMPV1 / SNMP V3は、Contextual help>>>Settingsコ>>> SNMPに移動して無効化または構成できます。 手順は、Contextual help>>>Settings>>> SNMPで利用できます。

5.2.2.5 ロギングとイベント管理

ベストプラクティス

- Eatonは、すべての管理および保守アクティビティを含め、すべてのリモートインタラクティブセッションを暗号化、ログ記録、および監視することをお勧めします。
- ログがバックアップされていることを確認し、バックアップを最低3か月間、または組織のセキュリティポリシーに従って保持します。
- 少なくとも15日ごとにログレビューを実行します。
- [情報] >>> [イベントコードのリスト]に移動して、ログ情報とそのエクスポート方法を取得します。

5.2.2.6 *安全なメンテナンス*

ベストプラクティス

5.2.2.6.1 ファームウェアのアップデートとパッチを定期的に適用する

産業用制御システムに対するサイバー攻撃が増加しているため、イートンは自社製品に包括的なパッチおよび更新プロセスを実装しています。 ユーザーは、一貫したプロセスを維持して、新しいファームウェアの更新を迅速に監視し、必要に応じて、またはリリースされたときにパッチと更新を実装することをお勧めします。

- ヘルプで次の場所に移動します
  Contextual help>>>Maintenance>>>Services

  ネットワークモジュールをアップグレードする方法に関する情報を取得します。
- ·イートンには、堅牢な脆弱性対応プロセスもあります。 製品にセキュリティの脆弱性が発見された場合、イートンは脆弱性にパッチを適用し、サイバーセキュリティWebサイト（http://eaton.com/cybersecurity）から情報速報をリリースし、www.eaton.com / downloadsからパッチを適用します。

組織/システムの定期的なサイバーセキュリティリスク分析を実施します。

Eatonは、特定の顧客の展開の一部として、およびEaton独自の開発サイクルプロセス内の両方で、サードパーティのセキュリティ会社と協力してシステム監査を実行してきました。 Eatonは、定期的なサイバーセキュリティ監査または評価を実行するための組織の取り組みにガイダンスとサポートを提供できます。

5.2.2.6.2 事業継続/サイバーセキュリティディザスタリカバリの計画

組織がビジネス継続性を計画することは、サイバーセキュリティのベストプラクティスです。 OT事業継続計画を確立し、定期的にレビューし、可能であれば、確立された継続計画を実行します。 オフサイトバックアップに次のものが含まれていることを確認してください

- ネットワークモジュールの最新のファームウェアコピーのバックアップ。ネットワークモジュールで最新のファームウェアが更新されたらすぐに、バックアップコピーを更新することをSOPの一部にします。
- 最新の構成のバックアップ。
- 最新のユーザーリストのドキュメント。
- デバイスの現在の構成を安全に保存および保存します。

5.2.3 参考文献

[R1] *Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):*

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] *Cybersecurity Best Practices Checklist Reminder (WP910003EN):*

http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] *NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:*

https://ics-cert.us-cert.gov/Standards-and-References

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

5.3 プロファイルを介したユーザー権限の構成

ユーザープロファイルは、新しいユーザーを作成するときに定義したり、既存のユーザーを変更するときに変更したりできます。 設定の「Contextual help>>>Settings>>>Local users」セクションを参照してください。

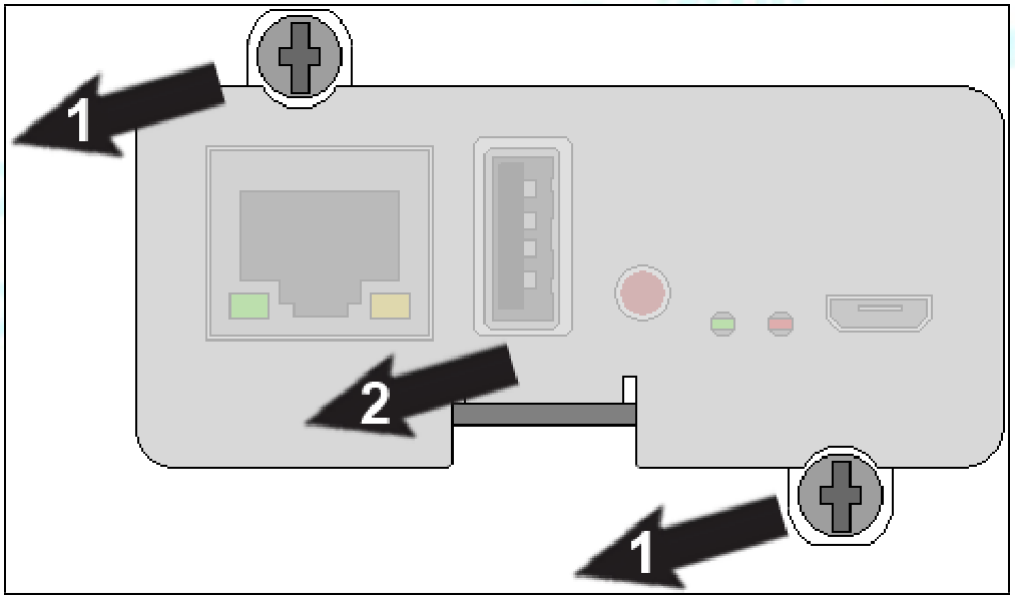
5.4 ネットワークマネジメントモジュールの廃止

報告されるデータ侵害の頻度が増えるにつれ、企業は効果的で信頼性の高い廃止措置のポリシーと手順を実装することがますます必要になっています。

廃止されたIT機器に保存されているデータが悪意のある人の手に渡ったり、データが侵害されたりしないように保護するために、以下の廃止措置手順に従うことをお勧めします：

1- ネットワークモジュールをサニタイズするサニタイズにより、すべてのデータ（ユーザー名とパスワード、証明書、キー、設定、ログなど）が消去されます。ネットワークモジュールをサニタイズするには、Contextual help>>>Maintenance>>>Services>>>Sanitization sectionを参照してください。

2- デバイスからネットワークモジュールをアンマウントします。ネットワークモジュールのネジを外し、スロットから取り外します。



6 EMPの保守

6.1 説明と機能

オプションの環境モニタリングプローブEMPDT1H1C2を使用すると、温度と湿度の読み取り値を収集し、環境データをリモートでモニタリングできます。
1つまたは2つのドライコンタクトデバイス（含まれていません）のステータスを収集および取得することもできます。 最大3つの環境モニタリングプローブを1つのデバイスにデイジーチェーン接続できます。
ネットワークモジュールを介してSNMPまたは標準のWebブラウザを使用してリモートで測定値を監視できます。これにより、より優れた電源管理制御と柔軟な監視オプションが提供されます。
EMPデバイスには、ネジとネジアンカー、ナイロンファスナー、タイラップ、および磁石が付属しています。 デバイスは、ラックのどこにでも、またはラックの近くの壁に取り付けることができます。

詳細については、デバイスのマニュアルを参照してください。

EMPには次の機能があります：

·ホットスワップ機能を使用すると、デバイスまたはデバイスに接続されている負荷の電源をオフにすることなく、プローブを安全に取り付けることができるため、取り付けが簡単になります。

·EMPは、温度と湿度の情報を監視して、重要な機器を保護するのに役立ちます。

·EMPは、0° Cから70° Cまでの温度を±2° Cの精度で測定します。

·EMPは、±5%の精度で10%から90%の相対湿度を測定します。

·EMPは、最大50m（165フィート）の長さのCAT5ネットワークケーブルを使用して、デバイスからある程度離れた場所に配置できます。

·EMPは、ユーザーが提供した2つの連絡先デバイスのステータスを監視します。

·温度、湿度、および接点の閉鎖ステータスは、ネットワークモジュールまたはLCDインターフェース（使用可能な場合）を介してWebブラウザから表示できます。

·温度と湿度のオフセットを設定できます。

6.2 EMPの開梱

EMPDT1H1C2センサーには次のものが含まれます：

·ドライコンタクト端子台

·クイックスタート

·USBからRS485へのコンバーター

·RJ45メス−メスコネクタ

·壁取り付けネジとアンカー

·ラック取り付けネジナットとワッシャー

·タイラップ（x2）

·ナイロンファスナー

梱包材は、廃棄物に関するすべての地域の規制に従って廃棄する必要があります。梱包材にはリサイクルシンボルが印刷されており、仕分けが容易です。

6.3 EMPのインストール

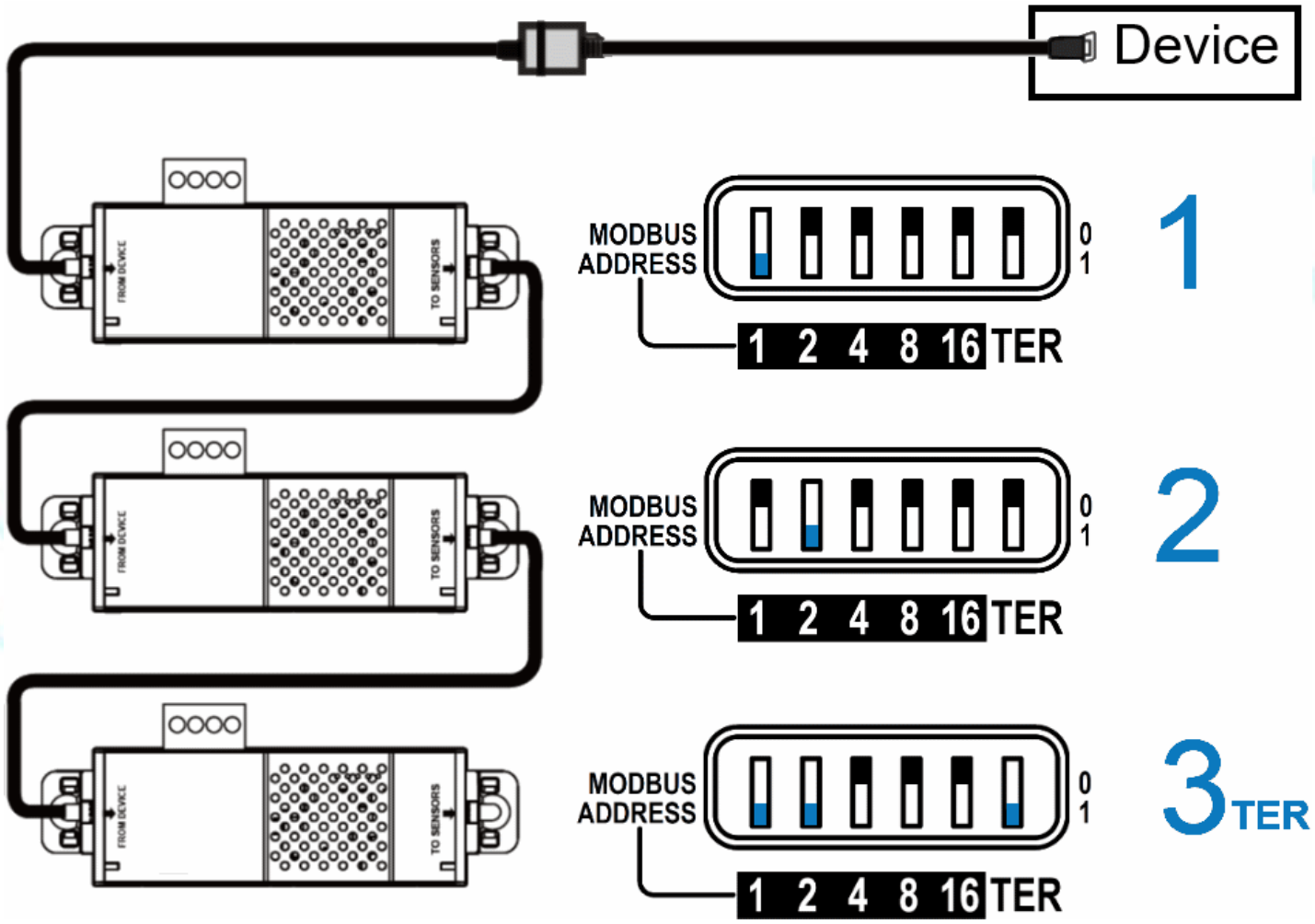
6.3.1 EMPのアドレスとターミネーションの定義

6.3.1.1 手動アドレス指定

EMPの電源を入れる前にアドレスを定義する必要があります。そうしないと、変更が考慮されません。Modbusアドレスを0に設定しないでください。設定しないと、EMPが検出されません。

デイジーチェーン内のすべてのEMPに**異なるアドレス**を定義します。
デイジーチェーンの最後のEMPでRS485終端（TER）を1に設定し、他のすべてのEMPで0に設定します。

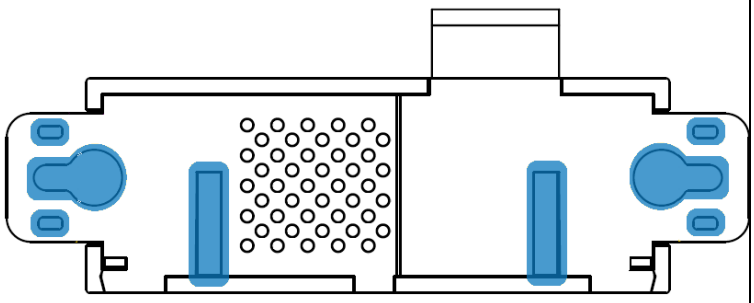
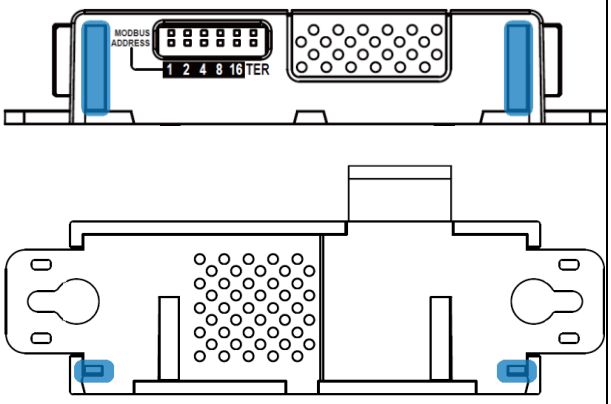
6.3.1.1.1 例：デバイスに接続された3つのEMPの手動アドレス指定



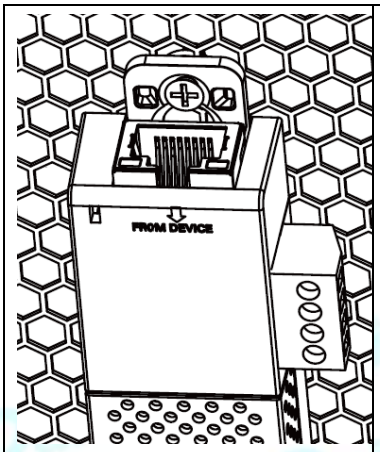
TO DEVICE RJ45コネクタの緑色のLEDは、EMPがネットワークモジュールから電力を供給されているかどうかを示します。

6.3.2 EMPの取り付け

EMPには、磁石、ケーブルタイスロット、および鍵穴が含まれており、複数の方法でEMPを設置に取り付けることができます。

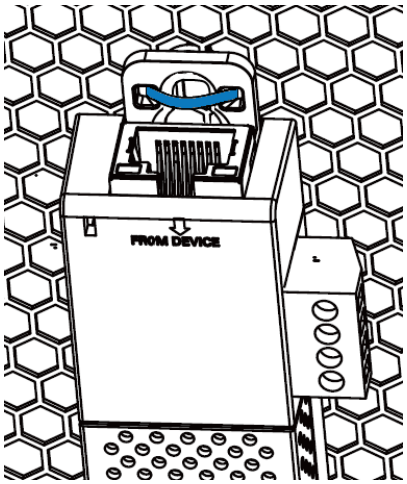
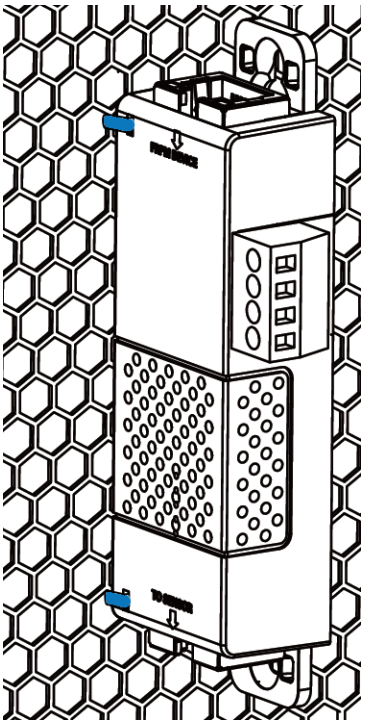
Bottom mounting capabilities: • magnets • keyholes • tie wraps • nylon fastener	Side mounting: • magnets • tie wraps
	

6.3.2.1 鍵穴の例を使用したラック取り付け

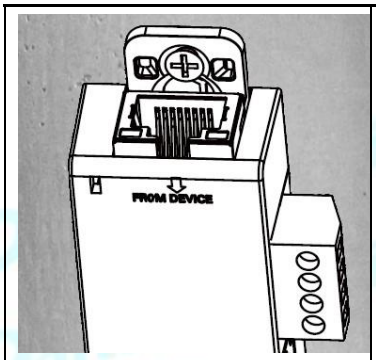
	EMPをラックに取り付けるには、付属のネジ、ワッシャー、ナットを使用します。次に、EMPをネジに取り付けて締めます。

6.3.2.2 タイラップを使用したラックマウントの例

EMPをラックのドアに取り付けるには、付属のケーブルタイを使用します。

Bottom mounting	Side mounting
	

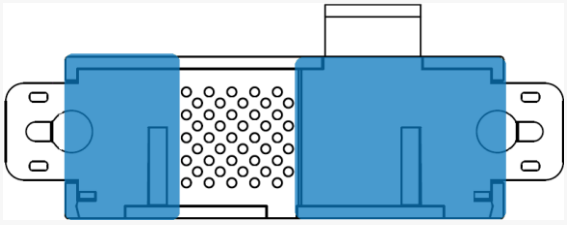
6.3.2.3 ネジによる壁取り付けの例

	ラックに近い壁にEMPを取り付けるには、付属のネジとネジアンカーを使用します。次にEMPをネジに取り付けて締めます。

6.3.2.4 ナイロンファスナーを使用した壁取り付けの例

EMPをエンクロージャ環境内に取り付けるには、一方のナイロンファスナーをEMPに取り付け、もう一方のナイロンファスナーをエンクロージャのレールポストに取り付けます。 次に、2つのナイロンストリップを一緒に押して、EMPをレールポストに固定します。

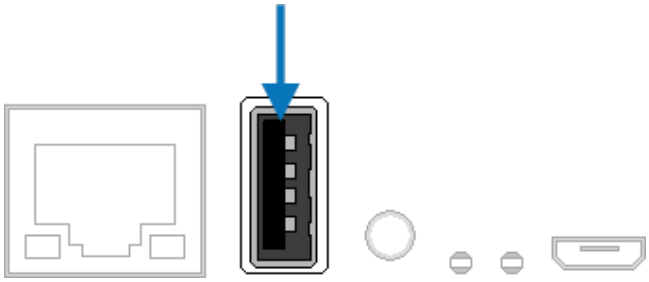
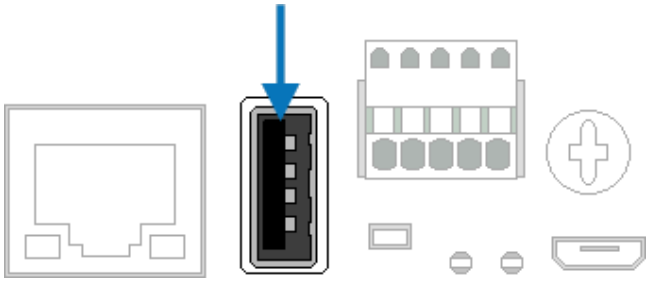
ナイロンファスナーをカットし、下で強調表示されている場所のEMP下部に貼り付けます。これにより、EMPデータ収集パーツとの干渉を防ぐことができます。



6.3.3 最初のEMPからデバイスへのケーブル接続

6.3.3.1 利用可能なデバイス

6.3.3.1.1 Network-M2/INDGW

Network-M2	INDGW
	

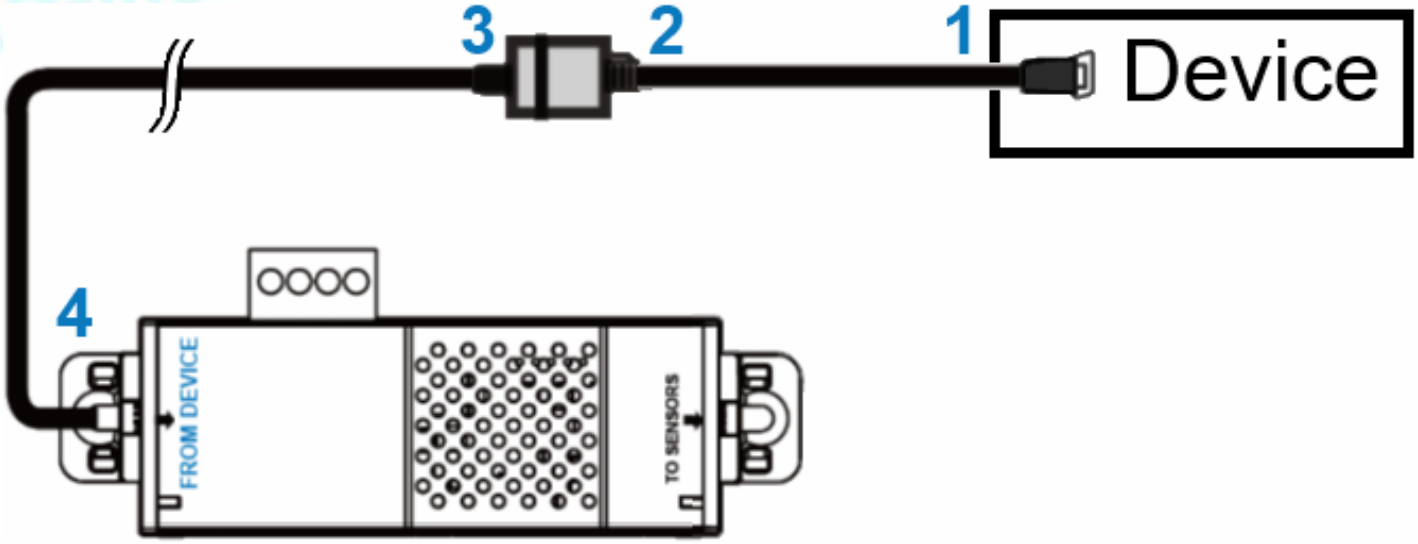
6.3.3.2 EMPをデバイスに接続する

EMPの電源を入れる前にアドレスを定義する必要があります。そうしないと、変更が考慮されません。Modbusアドレスを0に設定しないでください。設定しないとEMPが検出されません。

6.3.3.2.1 必要なもの:

- EMP
- RJ45 female/female connector (EMPアクセサリで提供)
- USB to RS485 converter cable (EMPアクセサリで提供)
- Ethernet cable (**付属していません**).
- デバイス

6.3.3.2.2 接続手順



STEP 1 – 「USB-RS485コンバータケーブル」をデバイスのUSBポートに接続します。

STEP2–「USB–RS485コンバータケーブル」をRJ45メス/メスコネクタに接続します。

STEP3–イーサネットケーブルをRJ45メス/メスコネクタのもう一方の端に接続します。

STEP4–イーサネットケーブルのもう一方の端をEMP（FROM DEVICE）のRJ–45ポートに接続します。

付属のタイラップを使用して、「RS485–USBケーブル」をネットワークケーブルに固定します。

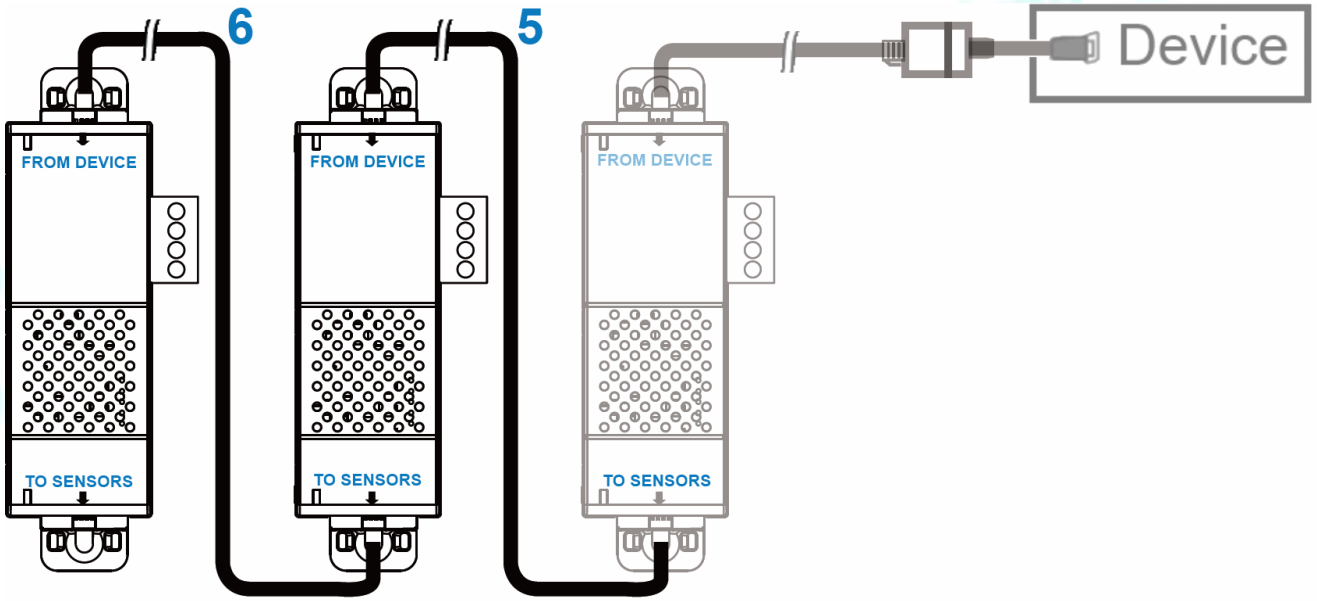
6.3.4 デイジーチェーンEMP

EMPの電源を入れる前にアドレスを定義する必要があります。それ以外の場合、変更は適用されません。
Modbusアドレスを0に設定しないでください。そうしないと、EMPは検出されません。

6.3.4.1 必要なもの:

- デバイスに接続された最初のEMP（前のセクションを参照）
- 追加のEMP
- 2 x Ethernet cable（付属していません）
- デバイス

6.3.4.2 手順

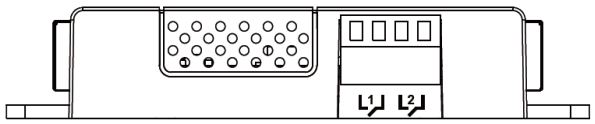


1つのデバイスで最大3つのEMPをデイジーチェーン接続できます。

STEP5–イーサネットケーブルを最初のEMPの「TOSENSORS」ポートと2番目のEMPの「FROMDEVICE」ポートに接続します。

STEP6–イーサネットケーブルを2番目のEMPの「TOSENSORS」ポートと3番目のEMPの「FROMDEVICE」ポートに接続します。

6.3.5 外部接点デバイスの接続



外部デバイスをEMPに接続するには：

STEP1–外部接点閉鎖入力をEMPの端子台に接続します（下の表と図を参照）。

·外部接点デバイス1.デバイス1からのリターンおよび信号入力ワイヤをネジ留め式端子1に接続します。

·外部接点デバイス2。デバイス2からのリターンおよび信号入力ワイヤをネジ留め式端子2に接続します。

STEP2– EMPの上部にある対応する締め付けネジを締めて、ワイヤを固定します。

6.4 EMPの試運転

6.4.1 ネットワークモジュールデバイス上

STEP1– ネットワークモジュールに接続する：

·ネットワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。

·[アドレス/場所]フィールドに、次のように入力します。https：//xxx.xxx.xxx.xxx/ここで、xxx.xxx.xxx.xxxはネットワークモジュールのIPアドレスです。

·ログイン画面が表示されます。

·[User Name]フィールドにユーザー名を入力します。

·[Password]フィールドにパスワードを入力します。

·**[Login（ログイン）]**をクリックします。ネットワークモジュールのWebインターフェースが表示されます。

STEP2– **[Environment(環境)]**メニューに移動します：

STEP3– 試運転に進みます：詳細については、コンテキストヘルプを参照してください。
：Contextual help>>>Environment>>>Commissioning/Status

- **[Discover（発見）]**をクリックします。ネットワークモジュールに接続されているEMPがテーブルに表示されます。

検出されると、EMPRJ45コネクタのオレンジ色のLEDがデータトラフィックを示します。検出プロセスが失敗した場合は、トラブルシューティングのセクションを参照してください。

- ペンのロゴを押してEMP情報を編集し、その設定にアクセスします。
- 必要に応じて、[**Define offsets（オフセットの定義）**]をクリックして、温度または湿度のオフセットを定義します。

STEP 4 –アラーム設定を定義します。詳細については、コンテキストヘルプを参照してください ：Contextual help>>>Environment>>>Alarm configuration

- アラーム設定ページを選択します。
- アラームを有効または無効にします。
- 温度、湿度、およびドライ接点アラームのしきい値、ヒステリシス、および重大度を定義します。

.

6.5 温度補償されたバッテリー充電にEMPを使用する

このセクションは、温度補償されたバッテリー充電オプションを提供するUPSにのみ適用されます。

EMPの電源を入れる前にアドレスを定義する必要があります。それ以外の場合、変更は適用されません。Modbusアドレスを0に設定しないでください。そうしないと、EMPは検出されません。
デイジーチェーン内のすべてのEMPに**ユニークなアドレス**を定義します。
デイジーチェーンの最後のEMPでRS485終端（TER）を1に設定します。他のEMPでは、これを0に設定する必要があります。

6.5.1 EMPへの対応

アドレス31をバッテリーの室温専用のセンサーに設定します。

·次の図に示すように、すべてのModbusアドレススイッチを1に設定して、EMPをアドレス31に設定します。

6.5.2 EMPの試運転

参照セクション Contextual help>>>Environment>>>Commissioning/Status.

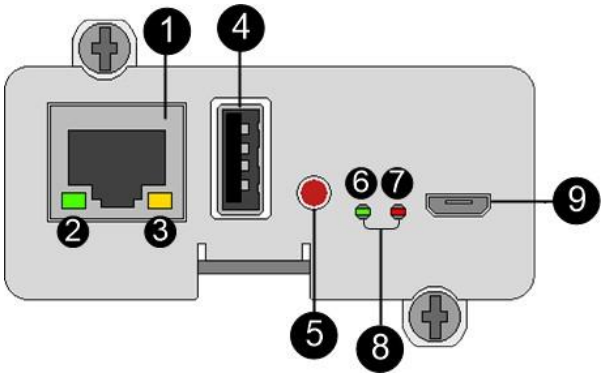
6.5.3 UPSで温度補償されたバッテリー充電を有効にする

UPSで温度補償されたバッテリー充電機能を有効にする必要があります。

温度補償されたバッテリー充電を有効にするには、UPSユーザーマニュアルを参照してください。

7 インフォメーション

7.1 フロントパネルコネクターと LED インジケーター



Nbr	ネーム	詳細
1	Network connector	Ethernet port
2	Network speed LED	Flashing green sequences: • 1 flash — Port operating at 10Mbps • 2 flashes — Port operating at 100Mbps • 3 flashes — Port operating at 1Gbps
3	Network link/activity LED	• Off — UPS Network Module is not connected to the network. • Solid yellow — UPS Network Module is connected to the network, but no activity detected. • Flashing yellow — UPS Network Module is connected to the network and sending or receiving data.
4	AUX connector	For Network Module accessories only. ***一般的な電源やUSB充電器には使用しないでください。.***
5	Restart button	Ball point pen or equivalent will be needed to restart: • Short press (<6s) — Safe software restart (firmware safely shutdown before restart). • Long press (>9s) — Forced hardware restart.
6	ON LED	Flashing green — Network Module is operating normally.
7	Warning LED	Solid red — Network Module is in error state.

8	Boot LEDs	Solid green and flashing red — Network Module is starting boot sequence.
9	Settings/UPS data connector	Configuration port. Access to Network Module's web interface through RNDIS (Emulated Network port). Access to the Network Module console through Serial (Emulated Serial port).

7.2 仕様/技術的特徴

仕様	
Dimensions (wxdxh)	132 x 66 x 42 mm | 5.2 x 2.6 x 1.65 in
Weight	70 g | 0.15 lb
RoHS	100% compatible
Storage	
Storage temperature	-25° C to 70° C (14° F to 158° F)
Ambient conditions	
Operating temperature	0° C to 70° C (32° F to 158° F)
Relative humidity	5%-95%, noncondensing
Module performance	
Module input power	5V-12V ±5% | 1A
AUX output power	5V ±5% | 200mA
Date/Time backup	CR1220 battery coin cell | The RTC is able to keep the date and the time when Network Module is OFF
Functions	
Languages	English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese
Alarms/Log	Email, SNMP trap, web interface / Log on events
Network	Gigabit ETHERNET, 10/100/1000Mb/s, auto negotiation, HTTP 1.1, SNMP V1, SNMP V3, NTP, SMTP, DHCP
Security	Restricted to TLS 1.2
Supported MIBs	*xUPS MIB | Standard IETF UPS MIB (RFC 1628) | Sensor MIB*
Browsers	Internet Explorer, Google Chrome, Firefox, Safari
Settings (default values)	
IP network	DHCP enabled | NTP server: pool.ntp.org
Port	443 (https), 22 (ssh), 161 (snmp), 162 (snmp trap), 25 (smtp), 8883 (mqtts), 123 (ntp), 5353 (mdns-sd), 80 (http), 514 (syslog),636 (LDAP), 1812 (RADIUS)
Web interface access control	User name: admin | Password: admin
Settings/Device data connector	USB RNDIS Apipa compatible | IP address: 169.254.0.1 | Subnet mask: 255.255.0.0

7.3 デフォルト設定と設定可能なパラメーター

7.3.1 設定

デフォルト設定と可能なパラメーター –一般

	デフォルト設定	可能なパラメーター
System details	Location — empty Contact — empty System name — empty Time & date settings — Manual (Time zone: Europe/Paris)	Location — 31 characters maximum Contact — 255 characters maximum System name — 255 characters maximum Time & date settings — Manual (Time zone: selection on map/Date) / Dynamic (NTP)
Email notification settings	No email	5 configurations maximum Custom name — 128 characters maximum Email address — 128 characters maximum Hide IP address from the email body — enable/disabled Status — Active/Inactive • Alarm notifications Active — No/Yes All card events – Subscribe/Attach logs Critical alarm – Subscribe/Attach logs Warning alarm – Subscribe/Attach logs Info alarm – Subscribe/Attach logs All device events – Subscribe/Attach measures/Attach logs Critical alarm – Subscribe/Attach measures/ Attach logs Warning alarm – Subscribe/Attach measures /Attach logs Info alarm – Subscribe/Attach measures/ Attach logs Always notify events with code Never notify events with code • Schedule report Active — No/Yes Recurrence – Every day/Every week/Every month Starting – Date and time Card events – Subscribe/Attach logs Device events – Subscribe/Attach measures/ Attach logs
SMTP settings	Server IP/Hostname — blank	Server IP/Hostname — 128 characters maximum

	SMTP server authentication — disabled Port — 25 Default sender address — *device*@networkcard.com Hide IP address from the email body — disabled Secure SMTP connection — enabled Verify certificate authority — disabled SMTP server authentication — disabled	SMTP server authentication — disable/enable (Username/Password — 128 characters maximum) Port — x-xxx Sender address — 128 characters maximum Hide IP address from the email body — enable/disabled Secure SMTP connection — enable/disable Verify certificate authority — disable/enable

デフォルト設定と可能なパラメーター –グローバルユーザー設定とローカルユーザー

	デフォルト設定	可能なパラメーター
Password settings	Minimum length — enabled (8) Minimum upper case — enabled (1) Minimum lower case — enabled (1) Minimum digit — enabled (1) Special character — enabled (1)	Minimum length — enable (6–32)/disable Minimum upper case — enable (0–32)/disable Minimum lower case — enable (0–32)/disable Minimum digit — enable (0–32)/disable Special character — enable (0–32)/disable
Password expiration	Number of days until password expires — disabled Main administrator password never expires — disabled	Number of days until password expires — disable/enable (1–99999) Main administrator password never expires — disable/enable
Lock account	Lock account after xx invalid tries — disabled Main administrator account never blocks — disabled	Lock account after xx invalid tries — disable/enable (1–99) Main administrator account never blocks — disable/enable
Account timeout	No activity timeout — 60 minutes Session lease time — 120 minutes	No activity timeout — 1–60 minutes Session lease time — 60–720 minutes
Local users	1 user only: • Active — Yes • Profile — Administrator • Username — admin • Full Name — blank • Email — blank • Phone — blank • Organization — blank	10 users maximum: • Active — Yes/No • Profile — Administrator/Operator/Viewer • Username — 255 characters maximum • Full Name — 128 characters maximum • Email — 128 characters maximum • Phone — 64 characters maximum • Organization — 128 characters maximum

デフォルト設定と可能なパラメーター –リモートユーザー

	デフォルト設定	可能なパラメーター
LDAP	Configure • Active – No • Security SSL – SSL Verify server certificate – enabled • Primary server Name – Primary Hostname – blank Port – 636 • Secondary server Name – blank Hostname – blank Port – blank • Credentials Anonymous search bind – disabled Search user DN – blank Password – blank • Search base Search base DN – dc=example,dc=com • Request parameters User base DN – ou=people,dc=example,dc=com User name attribute – uid UID attribute – uidNumber Group base DN – ou=group,dc=example,dc=com Group name attribute – gid GID attribute – gidNumber Profile mapping – no mapping Users preferences • Language – English • Temperature unit – ° C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)	Configure • Active – No/yes • Security SSL – None/Start TLS/SSL Verify server certificate – disabled/enabled • Primary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx • Secondary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx • Credentials Anonymous search bind – disabled/ enabled Search user DN – 1024 characters maximum Password – 128 characters maximum • Search base Search base DN – 1024 characters maximum • Request parameters User base DN – 1024 characters maximum User name attribute – 1024 characters maximum UID attribute – 1024 characters maximum Group base DN – 1024 characters maximum Group name attribute – 1024 characters maximum GID attribute – 1024 characters maximum Profile mapping – up to 5 remote groups mapped to local profiles Users preferences • Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese • Temperature unit – ° C (Celsius)/° F (Fahrenheit) • Date format – MM-DD-YYYY / YYY-MM- DD / DD-MM-YYY / DD.MM.YYY / DD/ MM/YYY / DD MM YYYY • Time format – hh:mm:ss (24h) / hh:mm:ss (12h)

RADIUS	Configure • Active – No • Retry number – 0 • Primary server Name – blank Secret – blank Address – blank UDP port – 1812 Time out – 3 • Secondary server Name – blank Secret – blank Address – blank UDP port – 1812 Time out – 3 Users preferences • Language – English • Temperature unit – ° C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)	Configure • Active – Yes/No • Retry number – 0 to 128 • Primary server Name – 128 characters maximum Address – 128 characters maximum Secret – 128 characters maximum UDP port – 1 to 65535 Time out – 3 to 60 • Secondary server Name – 128 characters maximum Address – 128 characters maximum Secret – 128 characters maximum UDP port – 1 to 65535 Time out – 3 to 60 Users preferences • Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese • Temperature unit – ° C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)

デフォルト設定と可能なパラメーター –ネットワーク & プロトコル

	デフォルト設定	可能なパラメーター
IPV4	Mode – DHCP	Mode – DHCP/Manual (Address/Netmask/Gateway)
IPV6	Enable – checked Mode – DHCP	Enabled – Active/Inactive Mode – DHCP/Manual (Address/Prefix/Gateway)
DNS/DHCP	Hostname – *device*–[MAC address] Mode – DHCP	Hostname – 128 characters maximum Mode :DHCP/Manual (Domain name/Primary DNS/ Secondary DNS)
Ethernet	Configuration – Auto negotiation	Configuration – Auto negotiation – 10Mbps – Half duplex – 10Mbps – Full duplex – 100Mbps – Half duplex – 100Mbps – Full duplex – 1.0 Gbps – Full duplex
HTTPS	Port – 443	Port – x–xxx
Syslog	Inactive • Server#1 Name – Primary Status – Disabled Hostname – empty Port – 514 Protocol – UDP Message transfer method – Non transparent framing Using unicode byte order mask (BOM) – disabled • Server#2 Name – empty Status – Disabled Hostname – empty Port – 514 Protocol – UDP Message transfer method – DIsabled in UDP Using unicode byte order mask (BOM) – disabled	Inactive/Active • Server#1 Name – 128 characters maximum Status – Disabled/Enabled Hostname – 128 characters maximum Port – x–xxx Protocol – UDP/TCP Message transfer method – Non transparent framing Using unicode byte order mask (BOM) – disable/ enable • Server#2 Name – 128 characters maximum Status – Disabled/Enabled Hostname – 128 characters maximum Port – x–xxx Protocol – UDP/TCP Message transfer method (in TCP) – Octet counting/ Non transparent framing

		Using unicode byte order mask (BOM) – disable/ enable

デフォルト設定と可能なパラメーター –SNMP

	デフォルト設定	可能なパラメーター
SNMP	Activate SNMP — disabled Port — 161 SNMP V1 — disabled • Community #1 — public Enabled — Inactive Access — Read only • Community #2 — private Enabled — Inactive Access — Read/Write SNMP V3 — enabled • User #1 — readonly Enabled — Inactive Access — Read only Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured – AES Key — empty Confirm key — empty • User#2 — readwrite Enabled — Inactive Access — Read/Write Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured – AES Key — empty Confirm key — empty	Activate SNMP — disable/enable Port — x-xxx SNMP V1 — disable/enable • Community #1 — 128 characters maximum Enabled — Inactive/Active Access — Read only • Community #2 — 128 characters maximum Enabled — Inactive/Active Access — Read/Write SNMP V3 — disable/enable • User #1 — 32 characters maximum Enabled — Inactive/Active Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured – AES/None Key — 128 characters maximum Confirm key — 128 characters maximum • User#2 — 32 characters maximum Enabled — Inactive/Active Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured – AES/None Key — 128 characters maximum Confirm key — 128 characters maximum
Trap receivers	No trap	Enabled — No/Yes Application name — 128 characters maximum Hostname or IP address — 128 characters maximum Port — x-xxx Protocol — V1 Trap community — 128 characters maximum

デフォルト設定と可能なパラメーター –Modbus

	デフォルト設定	可能なパラメーター
Modbus RTU	Enabled — Inactive Baud rate (bps) — 19200 Parity — Even Stop bits – 1	Enabled — Inactive/Active Baud rate (bps) — 1200/2400/4800/9600/19200/38400/57600/115200 Parity — None/Even/Odd Stop bits – 1/2
Modbus TCP	Enabled — Inactive Port — 502	Enabled — Inactive/Active Port — x–xxx
Mapping configuration	No mapping	Name – 128 characters maximum Map – Eaton ModbusMS compatible Transport – RTU/TCP Device ID – from 1 to 247 Access – None/Read only/Read/Write Illegal read behaviour – Return exception/Return zeros Coil/register base address shift – No shift/Shift by 1 (JBUS)

デフォルト設定と可能なパラメーター –証明書

	デフォルト設定	可能なパラメーター
Local certificates	Common name — Service + Hostname + selfsigned Country — FR State or Province — 38 City or Locality — Grenoble Organization name — Eaton Organization unit — Power quality Contact email address — blank	Common name — 64 characters maximum Country — Country code State or Province — 64 characters maximum City or Locality — 64 characters maximum Organization name — 64 characters maximum Organization unit — 64 characters maximum Contact email address — 64 characters maximum

7.3.2 メーター

デフォルト設定と可能なパラメーター –メーター

	デフォルト設定	可能なパラメーター
Meters/Logs	Log measures every — 60s	Log measures every — 3600s maximum

7.3.3 センサーのアラーム設定

デフォルト設定と可能なパラメーター –環境アラーム設定

	デフォルト設定	可能なパラメーター
Temperature	Enabled — No Low critical – 0° C/32° F Low warning – 10° C/50° F High warning – 70° C/158° F High critical – 80° C/176° F	Enabled — No/Yes low critical<low warning<high warning<high critical
Humidity	Enabled — No Low critical – 10% Low warning – 20% High warning – 80% High critical – 90%	Enabled — No/Yes 0%<low critical<low warning<high warning<high critical<100%
Dry contacts	Enabled — No Alarm severity – Warning	Enabled — No/Yes Alarm severity – Info/Warning/Critical

7.3.4 ユーザープロファイル

デフォルト設定と可能なパラメーター –ユーザープロファイル

	デフォルト設定	可能なパラメーター
Profile	Account details: • Full name — Administrator • Email — blank • Phone — blank • Organization — blank Preferences: • Language — English • Date format — MM-DD-YYYY • Time format — hh:mm:ss (24h) • Temperature — ° C (Celsius)	Account details: • Full name — 128 characters maximum • Email — 128 characters maximum • Phone — 64 characters maximum • Organization — 128 characters maximum Preferences: • Language — English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese • Date format — MM-DD-YYYY / YYY-MM- DD / DD-MM-YYY / DD.MM.YYY / DD/ MM/YYY / DD MM YYYY • Time format — hh:mm:ss (24h) / hh:mm:ss (12h) • Temperature — ° C (Celsius)/° F (Fahrenheit)

7.4 プロファイルごとのアクセス権

7.4.1 ホーム

	Administrator	Operator	Viewer
Home	✓	✓	✓

7.4.2 メーター

	Administrator	Operator	Viewer
Meters	✓	✓	✓
Battery health: Launch test/Abort	✓	✓	✗
Logs configuration	✓	✓	✗

7.4.3 コントロール

	Administrator	Operator	Viewer
Control	✓	✓	✗

7.4.4 保護

	Administrator	Operator	Viewer
Protection/Scheduled shutdowns	✓	✓	✗

	Administrator	Operator	Viewer
Protection/Agent list	✓	✓	✗

	Administrator	Operator	Viewer
Protection/Agent settings	✓	✓	✗

	Administrator	Operator	Viewer
Protection/Sequence	✓	✓	✗

7.4.5 環境

	Administrator	Operator	Viewer
Environment/Commissioning	✓	✓	✗
Environment/Status	✓	✓	✓

	Administrator	Operator	Viewer
Environment/Alarm configuration	✓	✓	✗

	Administrator	Operator	Viewer

Environment/Information	✓	✓	✓

7.4.6 設定

	Administrator	Operator	Viewer
General	✓	✗	✗

	Administrator	Operator	Viewer
Local users	✓	✗	✗

	Administrator	Operator	Viewer
Remote users	✓	✗	✗

	Administrator	Operator	Viewer
Network & Protocols	✓	✗	✗

	Administrator	Operator	Viewer
SNMP	✓	✗	✗

	Administrator	Operator	Viewer
Modbus*	✓	✗	✗

**for INDGW only*

	Administrator	Operator	Viewer
Certificate	✓	✗	✗

	Administrator	Operator	Viewer
ATS	✓	✓	✗

7.4.7 メンテナンス

	Administrator	Operator	Viewer
System information	✓	✓	✓

	Administrator	Operator	Viewer
Firmware	✓	✗	✗

	Administrator	Operator	Viewer
Services	✓	✗	✗

	Administrator	Operator	Viewer
Resources	✓	✓	✓

	Administrator	Operator	Viewer
System logs	✓	✗	✗

7.4.8 法的情報

	Administrator	Operator	Viewer
Legal information	✓	✓	✓

7.4.9 アラーム

	Administrator	Operator	Viewer
Alarm list	✓	✓	✓
Export	✓	✓	✓
Clear	✓	✓	✗

7.4.10 ユーザープロファイル

	Administrator	Operator	Viewer
User profile	✓	✓	✓

7.4.11 コンテキストヘルプ

	Administrator	Operator	Viewer
Contextual help	✓	✓	✓
Full documentation	✓	✓	✓

7.4.12 CLI コマンド

	Administrator	Operator	Viewer
get release info	✓	✓	✓

	Administrator	Operator	Viewer
history	✓	✓	✓

	Administrator	Operator	Viewer
ldap-test	✓	✗	✗

	Administrator	Operator	Viewer
logout	✓	✓	✓

	Administrator	Operator	Viewer
maintenance	✓	✗	✗

	Administrator	Operator	Viewer
modbus_message_display*	✓	✗	✗

**for INDGW only*

	Administrator	Operator	Viewer

modbus_statistics*	✓	✗	✗

for INDGW only

	Administrator	Operator	Viewer
netconf	✓	✓ (read-only)	✓ (read-only)

	Administrator	Operator	Viewer
ping	✓	✗	✗
ping6	✓	✗	✗

	Administrator	Operator	Viewer
reboot	✓	✗	✗

	Administrator	Operator	Viewer
save_configuration	✓	✗	✗
restore_configuration	✓	✗	✗

	Administrator	Operator	Viewer
sanitize	✓	✗	✗

	Administrator	Operator	Viewer
ssh-keygen	✓	✗	✗

	Administrator	Operator	Viewer
time	✓	✓ (read-only)	✓ (read-only)

	Administrator	Operator	Viewer
traceroute	✓	✗	✗
traceroute6	✓	✗	✗

	Administrator	Operator	Viewer
whoami	✓	✓	✓

	Administrator	Operator	Viewer
email-test	✓	✗	✗

	Administrator	Operator	Viewer
systeminfo_statistics	✓	✓	✓

	Administrator	Operator	Viewer
certificates	✓	✗	✗

7.5 イベントコードのリスト

電子メールサブスクリプションのアラームログコードまたはシステムログコードにアクセスするには、以下のセクションを参照してください：

7.5.1 システムログコード

システムログを取得するには、Contextual help>>>Maintenance>>>System logsセクションに移動し、[**システムログのダウンロード]ボタン**を押します。

以下のコードは、電子メール送信構成に「イベント通知の例外」を追加するために使用されるコードです。電子メールまたはログに表示されるときに、コードの前にゼロが追加される場合があります。

7.5.1.1 クリティカル

Code	Severity	Log message	File
0801000	Alert	User account – admin password reset to default	logAccount.csv
0E00400	Critical	The [selfsign/PKI] signed certificate of the <service> server is not valid	logSystem.csv
0A00700	Error	Network module file system integrity corrupted <f/w: xx.yy.zzzz>	logUpdate.csv
0000D00	Error	Card reboot due to database error	logSystem.csv
0700200	Error	Failed to start execution of script "<script description>". Client not registered. (<script uuid>)	logSystem.csv
0700400	Error	Execution of script "<script description>" failed with return code: <script return code>. (<script uuid>)	logSystem.csv
0700500	Error	Execution of script "<script description>" timeout! (<script uuid>)	logSystem.csv
0700700	Alert	Failed to prepare isolated environment for script execution. Protection service startup is aborted.	logSystem.csv

7.5.1.2 警告

Code	Severity	Log message	File
0A00200	Warning	Network module upgrade failed <f/w: xx.yy.zzzz>	logUpdate.csv
0A00A00	Warning	Network module bootloader upgrade failed <f/w: xx.yy.zzzz>	logUpdate.csv
0B00500	Warning	RTC battery cell low	logSystem.csv
0E00200	Warning	New [self/PKI] signed certificate [generated/imported] for <service> server	logSystem.csv
0E00300	Warning	The [self/PKI] signed certificate of the <service> server will expires in <X> days	logSystem.csv
0800700	Warning	User account – password expired	logAccount.csv
0800900	Warning	User account– locked	logAccount.csv
0C00100	Warning	Unable to send email: Smtp server is unknown	logSystem.csv
0C00200	Warning	Unable to send email: Authentication method is not supported	logSystem.csv
0C00300	Warning	Unable to send email: Authentication error	logSystem.csv
0C00500	Warning	Unable to send email: Certificate Authority not recognized	logSystem.csv
0C00600	Warning	Unable to send email: Secure connection required	logSystem.csv
0C00800	Warning	Unable to send email: Unknown error	logSystem.csv
0C00B00	Warning	Unable to send email: Recipient not specified	logSystem.csv
0F01300	Warning	Card reboot due to Device FW upgrade	logSystem.csv
1000F00	Warning	<*feature*> settings partial restoration	logSystem.csv
1001000	Warning	<*feature*> settings restoration error	logSystem.csv
1000C00	Warning	Settings partial restoration	logSystem.csv

1000D00	Warning	Settings restoration error	logSystem.csv

7.5.1.3 情報

Code	Severity	Log message	File
0300D00	Notice	User action – sanitization launched	logSystem.csv
0A00500	Notice	Network module sanitized	logUpdate.csv
0A00900	Notice	Network module bootloader upgrade success <f/w: xx.yy.zzzz>	logUpdate.csv
0A00B00	Notice	Network module bootloader upgrade started <f/w: xx.yy.zzzz>	logUpdate.csv
0A00C00	Notice	Periodic system integrity check started	logUpdate.csv
0B00100	Notice	Time manually changed	logSystem.csv
0B00700	Notice	NTP sever not available <NTP server address>	logSystem.csv
0900100	Notice	Session – opened	logSession.csv
0900200	Notice	Session – closed	logSession.csv
0900300	Notice	Session – invalid token	logSession.csv
0900400	Notice	Session – authentication failed	logSession.csv
0300F00	Notice	User action – network module admin password reset switch activated	logSystem.csv
0E00500	Notice	[Certificate authority/ Client certificate] <id> is added for <service>	logSystem.csv
0E00600	Notice	[Certificate authority/ Client certificate] <id> is revoked for <service>	logSystem.csv
0700100	Info	Start execution of script "<script description>". (<script uuid>)	logSystem.csv
0700300	Info	Execution of script "<script description>" succeeded. (<script uuid>)	logSystem.csv
0700600	Info/Notice / Error/Debug	<Script execution log message>	logSystem.csv
0800100	Notice	User account – created <user account id>	logAccount.csv
0800200	Notice	User account – deleted <user account id>	logAccount.csv
0800400	Notice	User account – name changed <user account id>	logAccount.csv
0800600	Notice	User account – password changed	logAccount.csv
0800800	Notice	User account– password reset <user account id>	logAccount.csv
0800A00	Notice	User account– unlocked	logAccount.csv
0800B00	Notice	User account – activated <user account id>	logAccount.csv
0800C00	Notice	User account – deactivated <user account id>	logAccount.csv
0900D00	Notice	<user> connected into interactive CLI with session id XXXXXX	logSession.csv
0900E00	Notice	<user> disconnected from interactive CLI with session id XXXXXX	logSession.csv
0900F00	Notice	<user> doesn't have access to CLI – CLI session id XXXXXX	logSession.csv
0901000	Notice	<user> connected and executes remote command <command> into the CLI – CLI session id XXXXXX	logSession.csv
0901100	Notice	<user> finished executing remote command <command> into the CLI – CLI session id XXXXXX	logSession.csv
0901200	Notice	<user> connection rejected – CLI session id XXXXXX	logSession.csv
0901300	Notice	<user> disconnected from interactive CLI with session id XXXXXX due to session timeout	logSession.csv
0901400	Notice	<user> disconnected from interactive CLI with session id XXXXXX due to concurrent connection with session id XXXXXX	logSession.csv
0100C00	Notice	Syslog is started	logSystem.csv

0100B00	Notice	Syslog is stopping	logSystem.csv
0100D00	Notice	Network module is booting	logSystem.csv
0100E00	Notice	Network module is operating	logSystem.csv
0100F00	Notice	Network module is starting shutdown sequence	logSystem.csv
0101000	Notice	Network module is ending shutdown sequence	logSystem.csv
0101400	Notice	Network module shutdown requested	logSystem.csv
0101500	Notice	Network module reboot requested	logSystem.csv
0100200	Notice	<nb alarms> alarms exported and flushed	logSystem.csv
0A00100	Info	Network module upgrade success <f/w: xx.yy.zzzz>	logUpdate.csv
0A00300	Info	Network module upgrade started	logUpdate.csv
0A00600	Info	Network module file system integrity OK <f/w: xx.yy.zzzz>	logUpdate.csv
0B00300	Info	Time with NTP synchronized	logSystem.csv
0B00600	Info	Time settings changed	logSystem.csv
0B01100	Info	Time reset to last known date: "date"	logSystem.csv
0C00F00	Info	Test email	
1000100	Info	Settings saving requested	logSystem.csv
1000200	Info	<*feature*> settings saved	logSystem.csv
1000A00	Info	Settings restoration requested	logSystem.csv
1000E00	Info	<*feature*> settings restoration success	logSystem.csv
1000B00	Info	Settings restoration success	logSystem.csv
0301500	Notice	Sanitization switch changed	logSystem.csv
0A01600	Notice	Major version downgrade	logUpdate.csv
0D00800	Notice	DHCP client script called with <script parameters>	logSystem.csv
0D00900	Notice	IPv4 configuration changed to <ipsv4_address>	logSystem.csv
0D01000	Notice	IPv6 configuration changed to <ipsv6_address>	logSystem.csv

コード0700600のイベントは、シャットダウンスクリプト内で使用されます。重大度は、イベントのコンテキストによって異なる場合があります。

7.5.2 UPS(HID) アラームログコード

この表は、9130UPSを除くすべてのUPSに適用されます。

アラームログを取得するには、Contextual help>>>Alarms sectionセクションに移動し、**[アラームのダウンロード]**ボタンを押します。

以下のコードは、電子メール送信構成に「イベント通知の例外」を追加するために使用されるコードです。電子メールまたはログに表示されるときに、コードの前にゼロが追加される場合があります。

7.5.2.1 クリティカル

Code	Severity	Active message	Non-active message	Advice
002	Critical	Internal failure	End of internal failure	Service required
004	Critical	Temperature alarm	Temperature OK	Check air conditioner
100	Critical	Rectifier fuse fault	Rectifier fuse OK	Service required
105	Critical	Input AC module failure	Input AC module OK	Service required
207	Critical	Bypass AC module failure	Bypass AC module OK	-
208	Critical	Bypass overload	No bypass overload	-
305	Critical	Rectifier failure	Rectifier OK	Service required
306	Critical	Rectifier overload	Rectifier OK	Reduce output load
308	Critical	Rectifier short circuit	Rectifier OK	Reduce output load
400	Critical	DCDC converter failure	DCDC converter OK	Service required
500	Critical	Battery charger fault	Battery charger OK	Service required
607	Critical	Battery test failed	Battery test OK	Check battery
60D	Critical	No battery	Battery present	Check battery
61B	Critical	Battery BMS fault	Battery BMS OK	Check battery
629	Critical	Battery voltage low critical	Battery voltage OK	Check battery
62B	Critical	Battery voltage high critical	Battery voltage OK	Check battery
62D	Critical	Battery charge current low critical	Battery charge current OK	Check battery
62F	Critical	Battery charge current high critical	Battery charge current OK	Check battery
631	Critical	Battery discharge current low critical	Battery discharge current OK	Check battery
633	Critical	Battery discharge current high critical	Battery discharge current OK	Check battery
635	Critical	Battery temperature low critical	Battery temperature OK	Check battery
637	Critical	Battery temperature high critical	Battery temperature OK	Check battery
63E	Critical	Battery fault	Battery OK	Check battery
704	Critical	Inverter internal failure	UPS OK	Service required
705	Critical	Inverter overload	No power overload	Reduce output load
706	Critical	Temperature alarm	Temperature OK	Check air conditioner
70B	Critical	Inverter short circuit	End of inverter short circuit	Service required
805	Critical	Output short circuit	Output OK	Reduce output load

811	Critical	Parallel negative power	Parallel power OK	Reduce output load
815	Critical	Calibration fault	Calibration OK	Service required
81E	Critical	Load unprotected	Load protected	-

7.5.2.2 警告

Code	Severity	Active message	Non-active message	Advice
001	Warning	On battery	No more on battery	-
007	Warning	Fan fault	Fan OK	Service required
00B	Warning	Parallel UPS redundancy lost	Parallel UPS redundancy OK	Reduce output load
00E	Warning	Parallel UPS communication lost	Parallel UPS communication OK	Service required
00F	Warning	Parallel UPS not compatible	Parallel UPS compatibility OK	Service required
010	Warning	UPS power supply fault	UPS power supply OK	Service required
011	Warning	Parallel UPS protection lost	Parallel UPS protection OK	Reduce output load
012	Warning	Parallel UPS measure inconsistent	Parallel UPS measure OK	Service required
103	Warning	Utility breaker open	Utility breaker closed	-
104	Warning	Input AC frequency out of range	Input AC frequency in range	-
106	Warning	Input AC not present	Input AC present	-
107	Warning	Input bad wiring	Input wiring OK	Check input wiring
108	Warning	Input AC voltage out of range (-)	Input AC voltage in range	-
109	Warning	Input AC voltage out of range (+)	Input AC voltage in range	-
110	Warning	Building alarm (through dry contact)	Building alarm OK	-
11F	Warning	Building alarm (through Network module)	Building alarm OK	-
10A	Warning	Input AC unbalanced	End of input AC unbalanced	-
200	Warning	Bypass phase out range	Bypass phase in range	-
201	Warning	Bypass not available	Bypass available	Service required
202	Warning	Bypass thermal overload	Bypass thermal OK	Reduce output load
203	Warning	Bypass temperature alarm	Bypass temperature OK	Check air conditioner
204	Warning	Bypass breaker open	Bypass breaker closed	-
205	Warning	Bypass mode	No more on bypass	-
206	Warning	Bypass frequency out of range	Bypass frequency in range	-
209	Warning	Bypass voltage out of range	Bypass voltage in range	-
20A	Warning	Bypass AC over voltage	End of bypass AC over voltage	-
20B	Warning	Bypass AC under voltage	End of bypass AC under voltage	-
20C	Warning	Bypass bad wiring	Bypass wiring OK	Check bypass wiring
300	Warning	DC bus + too high	DC bus + voltage OK	Service required
301	Warning	DC bus - too high	DC bus - voltage OK	Service required
302	Warning	DC bus + too low	DC bus + voltage OK	Service required
303	Warning	DC bus - too low	DC bus - voltage OK	Service required
304	Warning	DC bus unbalanced	DC bus OK	Service required
501	Warning	Charger temperature alarm	Charger temperature OK	Service required

502	Warning	Max charger voltage	Charger voltage OK	Service required
503	Warning	Min charger voltage	Charger voltage OK	Service required
600	Warning	Battery fuse fault	Battery fuse OK	Service required
602	Warning	Battery fuse fault	Battery fuse OK	Service required
604	Warning	Battery low state of charge	Battery state of charge OK	-
605	Warning	Battery temperature alarm	Battery temperature OK	Service required
606	Warning	Battery breaker open	Battery breaker closed	Service required
610	Warning	Battery low voltage	Battery voltage OK	Check battery
613	Warning	Battery voltage too high	Battery voltage OK	Check battery
616	Warning	Battery voltage unbalanced	Battery voltage OK	Check battery
61C	Warning	Communication with battery lost	Communication with battery recovered	Check battery
61E	Warning	At least one breaker in battery is open	All battery breakers are closed	Check battery
61F	Warning	Battery State Of Charge below limit	Battery State Of Charge OK	-
620	Warning	Battery State Of Health below limit	Battery State Of Health OK	Check battery
628	Warning	Battery voltage low warning	Battery voltage OK	Check battery
62A	Warning	Battery voltage high warning	Battery voltage OK	Check battery
62C	Warning	Battery charge current low warning	Battery charge current OK	Check battery
62E	Warning	Battery charge current high warning	Battery charge current OK	Check battery
630	Warning	Battery discharge current low warning	Battery discharge current OK	Check battery
632	Warning	Battery discharge current high warning	Battery discharge current OK	Check battery
634	Warning	Battery temperature low warning	Battery temperature OK	Check battery
636	Warning	Battery temperature high warning	Battery temperature OK	Check battery
638	Warning	Battery BMS failure	Battery BMS OK	Check battery
639	Warning	Battery temperature unbalanced	Battery temperature OK	Check battery
63D	Warning	Battery warning	Battery OK	Check battery
700	Warning	Inverter limitation	No current limitation	Reduce output load
701	Warning	Inverter fuse fault	Inverter fuse OK	Service required
70A	Warning	Inverter thermal overload	No power overload	Reduce output load
70C	Warning	Inverter voltage too low	Inverter voltage OK	Service required
70D	Warning	Inverter voltage too high	Inverter voltage OK	Service required
801	Warning	Load not powered	Load powered	-
803	Warning	Output breaker open	Output breaker closed	-
806	Warning	Emergency power OFF	No emergency OFF	-
808	Warning	Power overload	No power overload	Reduce output load
80D	Warning	Internal configuration failure	Internal configuration OK	Service required
80E	Warning	Overload pre-alarm	No overload pre-alarm	Reduce output load
810	Warning	Overload alarm	No overload	Reduce output load
814	Warning	Firmware watchdog reset	Firmware watchdog OK	Service required

816	Warning	Compatibility failure	Compatibility OK	Service required
817	Warning	Output over current	No output over current	Reduce output load
818	Warning	Output frequency out of range	Output frequency in range	Service required
819	Warning	Output voltage too high	Output voltage OK	Service required
81A	Warning	Output voltage too low	Output voltage OK	Service required
81B	Warning	UPS Shutoff requested	End of UPS shutoff requested	Service required
81D	Warning	Load not powered	Load protected	-
900	Warning	Maintenance bypass	Not on maintenance bypass	-
901	Warning	Maintenance bypass breaker closed	Maintenance bypass breaker open	-
B01	Warning	Batteries are aging. Consider replacement*	Batteries aging condition cleared	-

*「Batteries are aging.Consider replacement」は、ご利用開始から4年経過をお知らせ致します。

7.5.2.3 情報

Code	Severity	Active message	Non-active message	Advice
005	Info	Communication lost (with UPS)	Communication recovered (with UPS)	Service required
009	Info	On high efficiency / On ESS mode	High efficiency disabled / ESS disabled	-
013	Info	Upgrading: limited communication	End of upgrade mode	-
101	Info	On AVR (Boost)	End of AVR (Boost)	-
102	Info	On AVR (Buck)	End of AVR (Buck)	-
603	Info	Battery discharging	End of UPS battery discharge	-
63C	Info	Battery information	Battery OK	-
A00	Info	Group 1 is OFF	Group 1 is ON	-
A01	Info	Group 2 is OFF	Group 2 is ON	-
A0F	Info	Group is OFF	Group is ON	-

7.5.2.4 グッド

重大度が「良好」に設定されているアラームは、アクティブアラームのカウンターには考慮されません。

Code	Severity	Active message
60E	Good	UPS external battery set as “No battery”
826	Good	Load powered

7.5.3 9130 UPS(XCP) アラームログコード

この表は9130UPSに使用してください。

アラームログを取得するには、Contextual help>>>Alarms sectionセクションに移動し、**[アラームのダウンロード]ボタン**を押します。

以下のコードは、電子メール送信構成に「イベント通知の例外」を追加するために使用されるコードです。電子メールまたはログに表示されるときに、コードの前にゼロが追加される場合があります。

7.5.3.1 クリティカル

Code	Severity	Active message	Non-active message	Advice
2012	Critical	Emergency power OFF	No emergency OFF	-
2019	Critical	Building alarm	No building alarm	-
2020	Critical	Bypass temperature alarm	Bypass temperature OK	-
2024	Critical	Temperature alarm	Temperature OK	-
2026	Critical	Rectifier overload	Rectifier OK	-
2030	Critical	Rectifier failure	Rectifier OK	-
2031	Critical	Inverter internal failure	UPS OK	-
2034	Critical	Battery charger fault	Battery charger OK	-
2056	Critical	Battery low state of charge	Battery state of charge OK	-
2058	Critical	Output short circuit	Output OK	-
2070	Critical	UPS power supply fault	UPS power supply OK	-
2075	Critical	Rectifier overload	Rectifier OK	-
2077	Critical	Input AC module failure	Input AC module OK	-
2102	Critical	Inverter limitation	No current limitation	-
2111	Critical	Inverter thermal overload	No power overload	-
2112	Critical	DCDC converter failure	DCDC converter OK	-
2132	Critical	Parallel UPS protection lost	Parallel UPS protection OK	-
2143	Critical	Maintenance bypass	Not on maintenance bypass	-
2188	Critical	Bypass AC module failure	Bypass AC module OK	-
2191	Critical	Battery fault	Battery OK	Check battery
2192	Critical	Fuse fault	Fuse OK	-
2193	Critical	Fan fault	Fan OK	-
2199	Critical	No battery	Battery present	Check battery
2200	Critical	Temperature out of range	Temperature in range	-
2259	Critical	Rectifier short circuit	Rectifier OK	-
2260	Critical	Rectifier short circuit	Rectifier OK	-
2261	Critical	Rectifier short circuit	Rectifier OK	-
2323	Critical	Inverter overload	No power overload	-
2324	Critical	Inverter short circuit	End of inverter short circuit	-

2325	Critical	Bypass overload	No bypass overload	-
2328	Critical	Bypass thermal overload	Bypass thermal OK	-
2364	Critical	Internal failure	End of internal failure	-
2402	Critical	Parallel UPS not compatible	Parallel UPS compatibility OK	-
281E	Critical	Load unprotected	-	-

7.5.3.2 警告

Code	Severity	Active message	Non-active message	Advice
2000	Warning	Inverter voltage too high	Inverter voltage OK	-
2001	Warning	Inverter voltage too low	Inverter voltage OK	-
2003	Warning	Bypass AC over voltage	End of bypass AC over voltage	-
2004	Warning	Bypass AC under voltage	No Bypass AC under voltage	-
2005	Warning	Bypass frequency out of range	Bypass frequency in range	-
2006	Warning	Input AC voltage out of range (+)	Input AC voltage in range	-
2007	Warning	Input AC voltage out of range (-)	Input AC voltage in range	-
2008	Warning	Input AC frequency out of range	Input AC frequency in range	-
2009	Warning	Output voltage too high	Output voltage OK	-
2010	Warning	Output voltage too low	Output voltage OK	-
2011	Warning	Output frequency out of range	Output frequency in range	-
2021	Warning	Charger temperature alarm	Charger temperature OK	-
2023	Warning	Max charger voltage	Charger voltage OK	-
2025	Warning	Power overload	No power overload	-
2027	Warning	Output over current	No output over current	-
2028	Warning	DC bus + too high	DC bus + voltage OK	-
2029	Warning	DC bus + too low	DC bus + voltage OK	-
2032	Warning	Battery breaker closed	Battery breaker open	-
2057	Warning	On battery	No more on battery	-
2063	Warning	Parallel UPS communication lost	Parallel UPS communication OK	-
2067	Warning	Input AC not present	Input AC present	-
2105	Warning	Bypass available	Bypass not available	-
2106	Warning	Utility breaker closed	Utility breaker open	-
2159	Warning	Overload pre-alarm	No overload pre-alarm	-
2162	Warning	Overload alarm	No overload	-
2168	Warning	Battery discharging	End of UPS battery discharge	-
2169	Warning	Bypass mode	No more on bypass	-
2170	Warning	Load not powered	-	-
2176	Warning	Compatibility failure	Compatibility OK	-
2189	Warning	Load not powered	-	-
2194	Warning	Input bad wiring	Input wiring OK	-
2206	Warning	UPS Shutdown requested	End of UPS shutdown requested	-
2224	Warning	Internal configuration failure	Internal configuration OK	-

2225	Warning	Parallel UPS redundancy lost	Parallel UPS redundancy OK	-
2231	Warning	DC bus unbalanced	DC bus OK	-
2240	Warning	Parallel UPS communication lost	Parallel UPS communication OK	-
2306	Warning	Bypass breaker open	Bypass breaker closed	-
2326	Warning	Bypass phase out range	Bypass phase in range	-
2327	Warning	Bypass voltage out of range	Bypass voltage in range	-
2366	Warning	Bypass bad wiring	Bypass wiring OK	-

7.5.3.3 情報

Code	Severity	Active message	Non-active message	Advice
2063	Info	Communication lost	Communication recovered	-
2196	Info	On AVR (Buck)	End of AVR (Buck)	-
2197	Info	On AVR (Boost)	End of AVR (Boost)	-
2227	Info	On high efficiency	High efficiency disabled	-
2A0F	Info	Group is OFF	Group is ON	-

7.5.4 ATS アラームログコード

アラームログを取得するには、Contextual help>>>Alarms sectionセクションに移動し、**[アラームのダウンロード]ボタン**を押します。

以下のコードは、電子メール送信構成に「イベント通知の例外」を追加するために使用されるコードです。電子メールまたはログに表示されるときに、コードの前にゼロが追加される場合があります。

7.5.4.1 クリティカル

Code	Severity	Active message	Non-active message	Advice
F03	Critical	Internal failure	End of internal failure	-
F08	Critical	Internal failure	End of internal failure	-
F0B	Critical	Internal failure	End of internal failure	-
F0D	Critical	In short circuit	Not in short circuit	-
F10	Critical	Load not powered	Load powered with no continuity	-
F11	Critical	Internal failure	End of internal failure	-
F13	Critical	Temperature out of range	Temperature in range	-
F1B	Critical	Off	On preferred source	-

7.5.4.2 警告

Code	Severity	Active message	Non-active message	Advice
F00	Warning	Unsynchronized sources	Synchronized sources	-
F01	Warning	Frequency out of range	Frequency in range	-
F02	Warning	Out of range	In range	-
F04	Warning	Voltage in derated range	Voltage in normal range	-
F06	Warning	Frequency out of range	Frequency in range	-
F07	Warning	Not in range	In range	-
F09	Warning	Voltage in derated range	Voltage in normal range	-
F0C	Warning	In overload	Not in overload	-
F0F	Warning	Internal configuration failure	Internal configuration OK	-
F12	Warning	Overload Fault	No overload fault	-
F15	Warning	Input waveform is not OK	Input waveform is OK	-
F16	Warning	Voltage out of range	Voltage in range	-
F17	Warning	Input waveform is not OK	Input waveform is OK	-
F18	Warning	Voltage out of range	Voltage in range	-
F1A	Warning	On alternate source	-	-

7.5.4.3 グッド

重大度がGoodに設定されているアラームは、アクティブなアラームのカウンターには考慮されません。

Code	Severity	Active message	Non-active message	Advice
F05	Good	Source 1 used to power the load	Source 1 not used to power the load	-
F0A	Good	Source 2 used to power the load	Source 2 not used to power the load	-
F19	Good	On preferred source	-	-

7.5.5 EMP アラームログコード

アラームログを取得するには、Contextual help>>>Alarms sectionに移動し、**[アラームのダウンロード]**ボタンを押します。

以下のコードは、電子メール送信構成に「イベント通知の例外」を追加するために使用されるコードです。電子メールまたはログに表示されるときに、コードの前にゼロが追加される場合があります。

7.5.5.1 クリティカル

Code	Severity	Active message	Non-active message	Advice
1201	Critical	Temperature is critically low	Temperature is back to low	-
1204	Critical	Temperature is critically high	Temperature is back to high	-
1211	Critical	Humidity is critically low	Humidity is back to low	-
1214	Critical	Humidity is critically high	Humidity is back to high	-

7.5.5.2 警告

Code	Severity	Active message	Non-active message	Advice
1200	Warning	Communication lost	Communication recovered	-
1202	Warning	Temperature is low	Temperature is back to normal	-
1203	Warning	Temperature is high	Temperature is back to normal	-
1212	Warning	Humidity is low	Humidity is back to normal	-
1213	Warning	Humidity is high	Humidity is back to normal	-

7.5.5.3 重大度を設定可能

Code	Severity	Active message	Non-active message	Advice
1221	Settable	Contact is active	Contact is back to normal	-

7.5.6 ネットワークモジュールアラームログコード

アラームログを取得するには、Contextual help>>>Alarms sectionに移動し、**[アラームのダウンロード]**ボタンを押します。

以下のコードは、電子メール送信構成に「イベント通知の例外」を追加するために使用されるコードです。電子メールまたはログに表示されるときに、コードの前にゼロが追加される場合があります。

7.5.6.1 警告

7.5.6.1.1 保護

Code	Severity	Active message	Non-active message	Advice
1032	Warning	Protection: immediate shutdown in progress	Protection: immediate shutdown completed	-
1053	Warning	Protection: communication lost with agent	Protection: communication recovered with agent	-

7.5.6.1.2 アラーム

Code	Severity	Active message	Non-active message	Advice
1303	Warning	Alarms: the number of alarms is too high and above 6 000	Alarms: the number of alarms is back to normal	2 000 alarms have been erased and saved in a backup file.

7.5.6.2 情報

7.5.6.2.1 保護

Code	Severity	Active message	Non-active message	Advice
1016	Info	Protection: sequential shutdown scheduled	Protection: sequential shutdown canceled	-
1017	Info	Protection: sequential shutdown in progress	Protection: sequential shutdown completed	-
1054	Info	Protection: agent is in unknown state	Protection: agent is in service	-
1055	Info	Protection: agent is starting	Protection: agent is in service	-
1056	Info	Protection: agent is stopping	Protection: agent is in service	-
1057	Info	Protection: agent is stopped	Protection: agent is in service	-
1100	Info	Schedule: shutdown date reached	Schedule: shutdown initiated	-

7.5.6.2.2 通信

Code	Severity	Active message	Non-active message	Advice
1300	Info	Communication: No device connected	Communication: Communication with the device is back	-
1301	Info	Communication: Device not supported	Communication: Communication with the device is back	-

7.5.6.2.3 アラーム

Code	Severity	Active message	Non-active message	Advice
1302	Info	Alarms: the number of alarms is high and above 5 000	Alarms: the number of alarms is back to normal	It is recommended to Export and Clear the alarm log.

7.6 SNMP トラップ

7.6.1 UPS Mib

7.6.1.1 IETF Mib-2 Ups トラップ

この情報は参照用です。

Trap oid : **.1.3.6.1.2.1.33.2.0.x**	**Description :**
.1.3.6.1.2.1.33.2.0.**1**	Sent whenever the UPS transfers on battery, then sent every minutes until the UPS Comes back to AC Input.
.1.3.6.1.2.1.33.2.0.**3**	Sent whenever an alarm appears. The matching alarm oid is added as bound variables in the table below.
.1.3.6.1.2.1.33.2.0.4	Sent whenever an alarm disappears. The matching alarm oid is added as bound variables in the table below.

Alarm oid at : **.1.3.6.1.2.1.33.1.6.3.x**	**Description when trap 3**	**Description when trap 4**
.1.3.6.1.2.1.33.1.6.3.**1**	Battery test failed	Battery test OK
.1.3.6.1.2.1.33.1.6.3.**2**	Battery discharging	End of UPS battery discharge
.1.3.6.1.2.1.33.1.6.3.**3**	Low battery	Battery OK
.1.3.6.1.2.1.33.1.6.3.**5**	Temperature alarm	Temperature OK
.1.3.6.1.2.1.33.1.6.3.**6**	Input AC not present	Input AC present
.1.3.6.1.2.1.33.1.6.3.**8**	Power overload	No power overload
.1.3.6.1.2.1.33.1.6.3.**9**	Bypass mode	No more on bypass
.1.3.6.1.2.1.33.1.6.3.**10**	Bypass not available	Bypass available
.1.3.6.1.2.1.33.1.6.3.**13**	Battery charger fault	Battery charger OK
.1.3.6.1.2.1.33.1.6.3.**14**	Not powered	Powered (Protected or Not protected)
.1.3.6.1.2.1.33.1.6.3.**16**	Fan fault	Fan OK
.1.3.6.1.2.1.33.1.6.3.**17**	Battery fuse fault Rectifier fuse fault Inverter fuse fault	Battery fuse OK Rectifier fuse OK Inverter fuse OK
.1.3.6.1.2.1.33.1.6.3.**18**	Internal failure	End of internal failure

Alarm oid at : .1.3.6.1.2.1.33.1.6.3.x	Description when trap 3	Description when trap 4
.1.3.6.1.2.1.33.1.6.3.**20**	Communication lost	Communication recovered
.1.3.6.1.2.1.33.1.6.3.**23**	Shutdown imminent	Shutdown canceled

7.6.1.2 Xups Mib トラップ

この情報は参照用です。

Trap oid : .1.3.6.1.4.1.534.1.11.4.1.0.x	Trap message at oid : .1.3.6.1.4.1.534.1.11.3.0
.1.3.6.1.4.1.534.1.11.4.1.0.**3**	Battery discharging
.1.3.6.1.4.1.534.1.11.4.1.0.**4**	Battery low
.1.3.6.1.4.1.534.1.11.4.1.0.**5**	No more on battery
.1.3.6.1.4.1.534.1.11.4.1.0.**6**	Battery OK
.1.3.6.1.4.1.534.1.11.4.1.0.**7**	Power overload
.1.3.6.1.4.1.534.1.11.4.1.0.**8**	Internal failure
.1.3.6.1.4.1.534.1.11.4.1.0.**10**	Inverter internal failure
.1.3.6.1.4.1.534.1.11.4.1.0.**11**	Bypass mode
.1.3.6.1.4.1.534.1.11.4.1.0.**12**	Bypass not available
.1.3.6.1.4.1.534.1.11.4.1.0.**13**	Load not powered
.1.3.6.1.4.1.534.1.11.4.1.0.**14**	On battery
.1.3.6.1.4.1.534.1.11.4.1.0.**15**	Building alarm through input dry contact
.1.3.6.1.4.1.534.1.11.4.1.0.**16**	Shutdown imminent
.1.3.6.1.4.1.534.1.11.4.1.0.**17**	No more on bypass
.1.3.6.1.4.1.534.1.11.4.1.0.**20**	Breaker open
.1.3.6.1.4.1.534.1.11.4.1.0.**23**	Battery test failed
.1.3.6.1.4.1.534.1.11.4.1.0.**26**	Communication lost
.1.3.6.1.4.1.534.1.11.4.1.0.**30**	Sensor contact is active
.1.3.6.1.4.1.534.1.11.4.1.0.**31**	Sensor contact back to normal
.1.3.6.1.4.1.534.1.11.4.1.0.**32**	Parallel UPS redundancy lost
.1.3.6.1.4.1.534.1.11.4.1.0.**33**	Temperature alarm
.1.3.6.1.4.1.534.1.11.4.1.0.**34**	Battery charger fault
.1.3.6.1.4.1.534.1.11.4.1.0.**35**	Fan fault
.1.3.6.1.4.1.534.1.11.4.1.0.**36**	Fuse fault
.1.3.6.1.4.1.534.1.11.4.1.0.**42**	Sensor temperature is below/above critical threshold
.1.3.6.1.4.1.534.1.11.4.1.0.**43**	Sensor humidity is below/above critical threshold
.1.3.6.1.4.1.534.1.11.4.1.0.**48**	Maintenance bypass

7.6.2 ATS Mib

この情報は参照用です。

Trap oid : .1.3.6.1.4.1.534.10.2.10.x	Trap description
.1.3.6.1.4.1.534.10.2.10.**1**	Communication lost
.1.3.6.1.4.1.534.10.2.10.**2**	Communication recovered
.1.3.6.1.4.1.534.10.2.10.**3**	Output powered
.1.3.6.1.4.1.534.10.2.10.**4**	Output not powered
.1.3.6.1.4.1.534.10.2.10.**5**	Overload
.1.3.6.1.4.1.534.10.2.10.**6**	No overload
.1.3.6.1.4.1.534.10.2.10.**7**	Internal failure
.1.3.6.1.4.1.534.10.2.10.**8**	No internal failure
.1.3.6.1.4.1.534.10.2.10.**9**	Source 1 normal
.1.3.6.1.4.1.534.10.2.10.**10**	Source 1 out of range
.1.3.6.1.4.1.534.10.2.10.**11**	Source 2 normal
.1.3.6.1.4.1.534.10.2.10.**12**	Source 2 out of range
.1.3.6.1.4.1.534.10.2.10.**13**	Sources desynchronized
.1.3.6.1.4.1.534.10.2.10.**14**	Sources synchronized
.1.3.6.1.4.1.534.10.2.10.**15**	Output powered by source 1
.1.3.6.1.4.1.534.10.2.10.**16**	Output powered by source 2
.1.3.6.1.4.1.534.10.2.10.**20**	Remote temperature low
.1.3.6.1.4.1.534.10.2.10.**21**	Remote temperature high
.1.3.6.1.4.1.534.10.2.10.**22**	Remote temperature normal
.1.3.6.1.4.1.534.10.2.10.**23**	Remote humidity low
.1.3.6.1.4.1.534.10.2.10.**24**	Remote humidity high
.1.3.6.1.4.1.534.10.2.10.**25**	Remote humidity normal
.1.3.6.1.4.1.534.10.2.10.**26**	Contact 1 active
.1.3.6.1.4.1.534.10.2.10.**27**	Contact 1 inactive
.1.3.6.1.4.1.534.10.2.10.**28**	Contact 2 active
.1.3.6.1.4.1.534.10.2.10.**29**	Contact 2 inactive

7.6.3 Sensor Mib

7.6.3.1 Sensor Mib トラップ

この情報は参照用です。

Trap oid : .1.3.6.1.4.1.534.6.8.1.x.x.x	Trap description
.1.3.6.1.4.1.534.6.8.1.**1.0.1**	Sent whenever the sensor count changes after a discovery or removing from the UI.
.1.3.6.1.4.1.534.6.8.1.**1.0.2**	Sent whenever one status of each sensor connected changes.
.1.3.6.1.4.1.534.6.8.1.**2.0.1**	Sent whenever one status of each temperature changes.
.1.3.6.1.4.1.534.6.8.1.**3.0.1**	Sent whenever one status of each humidity changes.
.1.3.6.1.4.1.534.6.8.1.**4.0.1**	Sent whenever one status of each digital input alarm changes.

7.7 CLI

CLIには、次の方法でアクセスできます。

·SSH

·シリアル端末エミュレーション（Servicing the Network Management Module>>>Installing the Network Module>>>Accessing the card through serial terminal emulation のセクションを参照）

これは主に、ネットワークの自動構成とネットワークカードの時間設定を目的としています。また、Webユーザーインターフェースにアクセスできない場合のトラブルシューティングやネットワークインターフェースのリモート再起動/リセットにも使用できます。

警告：ネットワークパラメーターを変更すると、カードがリモートで使用できなくなる可能性があります。これが発生した場合は、USBを介してローカルでのみ再構成できます。

7.7.1 使用可能なコマンド

CLIで入力すると、いつでもこのリストを表示できます：

```
?
```

7.7.2 コンテキストヘルプ

CLIで入力すると、いつでもこのリストを表示できます：

```
help
```

```
CONTEXT SENSITIVE HELP
[?] - Display context sensitive help. This is either a list of possible command completions with
          summaries, or the full syntax of the current command. A subsequent repeat of this key, when
          a command has been resolved, will display a detailed reference.

AUTO-COMPLETION
The following keys both perform auto-completion for the current command line. If the command prefix is not
unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending
                part of the command line will be highlighted and explained.

[space] - Auto-completes, or if the command is already resolved inserts a space. MOVEMENT KEYS
[CTRL-A] - Move to the start of the line [CTRL-E] -
Move to the end of the line.
[up]          - Move to the previous command line held in history. [down]          -
Move to the next command line held in history. [left] - Move the insertion point left
one character. [right]    - Move the insertion point right one character.

DELETION KEYS
[CTRL-C]        - Delete and abort the current line
[CTRL-D]        - Delete the character to the right on the insertion point. [CTRL-K]        - Delete all the
characters to the right of the insertion point. [CTRL-U]        - Delete the whole line.
[backspace] - Delete the character to the left of the insertion point.

ESCAPE SEQUENCES
!!      - Substitute the last command line.
!N      - Substitute the Nth command line (absolute as per 'history' command)
!-N - Substitute the command line entered N lines before (relative)
```

7.7.3 リリース情報を取得する

7.7.3.1 説明

ファームウェアリリースに関連する特定の基本情報を表示します。

7.7.3.2 ヘルプ

```
get_release_info
  -d  Get current release date
  -s  Get current release sha1
  -t  Get current release time
  -v  Get current release version number
```

7.7.3.3 詳細

7.7.3.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
get release info	✅	✅	✅

7.7.4 ヒストリー

7.7.4.1 説明

カードで実行された最近のコマンドを表示します。

7.7.4.2 ヘルプ

```
history
  <cr>                Display the current session's command line history(by default display
last 10 commands)
  <Unsigned integer>  Set the size of history list (zero means unbounded). Example 'history
6' display the 6 last command
```

7.7.4.3 詳細

7.7.4.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
history	✅	✅	✅

7.7.5 ldap-テスト

7.7.5.1 説明

LDAP構成の問題または作業上の問題をトラブルシューティングするためのLdapテストヘルプ

7.7.5.2 ヘルプ

```
        Usage: ldap-test <command> [OPTION]...
Test LDAP configuration.

Commands:
   ldap-test -h, --help, Display help page

   ldap-test --checkusername <username> [--primary|--secondary] [-v] Check if the user can
   be retrieve from the LDAP server
      <username>            Remote username to test
      --primary             Force the test to use primary server (optional)
      --secondary           Force the test to use secondary server (optional)
      -v,--verbose          Print the exchanges with LDAP server (optional)

   ldap-test --checkauth <username> [--primary|--secondary] [-v] Check if remote user
   can login to the card
      <username>            Remote username to test
      -p,--primary              Force the test to use primary server (optional)
      -s,--secondary            Force the test to use secondary server (optional)
      -v,--verbose          Print the exchanges with LDAP server (optional)

   ldap-test --checkmappedgroups [--primary|--secondary] [-v] Check LDAP
   mapping
      -p,--primary              Force the test to use primary server (optional)
      -s,--secondary            Force the test to use secondary server (optional)
      -v,--verbose          Print the exchanges with LDAP server (optional) Quick guide for

testing:

In case of issue with LDAP configuration, we recommend to verify the configuration using the
commands in the following order:

   1. Check user can be retrieve on the LDAP server ldap-test --
      checkusername <username>

   2. Check that your remote group are mapped to the good profile ldap-test --
      checkmappedgroups

   3. Check that the user can connect to the card
      ldap-test --checkauth <username>
```

7.7.5.3 詳細

7.7.5.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
ldap-test	✓	✗	✗

7.7.6 ログアウト

7.7.6.1 詳細

現在のユーザーをログアウトします。

7.7.6.2 ヘルプ

```
logout
  <cr> logout the user
```

7.7.6.3 詳細

7.7.6.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
logout	✓	✓	✓

7.7.7 メンテナンス

7.7.7.1 説明

テクニカルサポートに渡すことができるメンテナンスレポートファイルを作成します。

7.7.7.2 ヘルプ

```
maintenance
   <cr> Create maintenance report file.
   -h, --help Display help page
```

7.7.7.3 詳細

7.7.7.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
maintenance	✓	✗	✗

7.7.8 modbusメッセージの表示

このセクションは、Modbusネットワークモジュール INDGW専用です

7.7.8.1 説明

modbus_message_displayはサーバーを再起動し、Modbusメッセージを表示します。このコマンドを使用すると、Modbusサーバーが期待どおりに機能していることを確認できます。

7.7.8.2 ヘルプ

```
modbus_message_display
  --help  Restart server and display modbus message
  -h      Restart server and display modbus message
```

7.7.8.3 詳細

7.7.8.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
modbus_message_display*	✓	✗	✗

**for INDGW only*

7.7.9 modbus分析

> このセクションは、ModbusネットワークモジュールINDGW専用です

7.7.9.1 説明

modbus_statisticsは、ModbusRTUとTCPのステータスおよびサーバー統計を表示します：

·バスキャラクターのオーバーランカウント

·バスフレームエラーカウント

·バスパリティエラーカウント

·バッファオーバーランカウント

·バスメッセージ数

·有効なメッセージ数

·CRCエラーカウント

·受信メッセージ数

·破棄されたメッセージ数

·処理されたメッセージ数

·成功はカウントを返しました

·例外がカウントを返しました

7.7.9.2 ヘルプ

```
modbus_statistics
                      Display modbus server statistics

        -h, --help       Display the help page.
        -r, --reset      Reset modbus server statistics.
                         The counter from A1.1 to A1.4 are reset only at startup of the
server.
```

7.7.9.3 詳細

7.7.9.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
modbus_statistics*	✓	✗	✗

**for INDGW only*

7.7.10 netconf

7.7.10.1 説明

カードのネットワーク構成を表示または変更するためのツール。

7.7.10.2 ヘルプ

ビューアおよびオペレータプロファイルの場合：

```
netconf -h
 Usage: netconf [OPTION]...
 Display network information and change configuration.

   -h, --help      display help page
   -l, --lan       display Link status and MAC address
   -4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
   -6, --ipv6      display IPv6 Mode, Addresses and Gateway
   -d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
```

管理者のためのプロファイル:

```
netconf -h
  Usage: netconf [OPTION]...
  Display network information and change configuration.
    -h, --help              display help page
    -l, --lan               display Link status and MAC address
    -d, --domain            display Domain mode, FQDN, Primary and Secondary DNS
    -4, --ipv4              display IPv4 Mode, Address, Netmask and Gateway
    -6, --ipv6              display IPv6 Mode, Addresses and Gateway Set
        commands are used to modify the settings.
    -s, --set-lan <link speed> Link speed
          values:
          auto              Auto negotiation
          10hf              10 Mbps - Half duplex
          10ff              10 Mbps - Full duplex 100hf
                            100 Mbps - Half duplex 100ff
                            100 Mbps - Full duplex 1000ff
                            1.0 Gbps - Full duplex
    -f, --set-domain hostname <hostname>                    set custom hostname
    -f, --set-domain <mode>
                Mode values:
                - set custom Network address, Netmask and Gateway: manual <domain
                    name> <primary DNS> <secondary DNS>
                - automatically set Domain name, Primary and Secondary DNS dhcp
    -i, --set-ipv4 <mode>
                Mode values:
                - set custom Network address, Netmask and Gateway manual
                    <network> <mask> <gateway>
                - automatically set Network address, Netmask and Gateway dhcp
    -x, --set-ipv6 <status>
                Status values:
                - enable IPv6
                    enable
                - disable IPv6
                    disable
    -x, --set-ipv6 <mode>
                Mode values:
                - set custom Network address, Prefix and Gateway manual
                    <network> <prefix> <gateway>
                - automatically set Network address, Prefix and Gateway router
Examples of usage:
-> Display Link status and MAC address
        netconf -l
-> Set Auto negotiation to Link
        netconf --set-lan auto
-> Set custom hostname
        netconf --set-domain hostname ups-00-00-00-00-00-00
-> Set Adress, Netmask and Gateway
        netconf --set-ipv4 manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6
```

7.7.10.3 使用例

```
 -> Display Link status and MAC address
      netconf -l
 -> Set Auto negotiation to Link
      netconf -s auto
 -> Set custom hostname
      netconf -f hostname ups-00-00-00-00-00-00
 -> Set Adress, Netmask and Gateway
      netconf -i manual 192.168.0.1 255.255.255.0 192.168.0.2
 -> Disable IPv6
      netconf -6 disable
```

7.7.10.4 詳細

7.7.10.5 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
netconf	✓	✓ (read-only)	✓ (read-only)

7.7.11 ping と ping6

7.7.11.1 説明

PingおよびPing6ユーティリティは、ネットワーク接続をテストするために使用されます。

7.7.11.2 ヘルプ

```
ping
  The ping utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
  to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST
  datagrams (``pings'') have an IP and ICMP header, followed by a ``struct
  timeval'' and then an arbitrary number of ``pad'' bytes used to fill out
  the packet.

  -c               Specify the number of echo requests to be sent
  -h               Specify maximum number of hops
  <Hostname or IP>  Host name or IP address
```

```
ping6
  The ping6 utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
  to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST
  datagrams (``pings'') have an IP and ICMP header, followed by a ``struct
  timeval'' and then an arbitrary number of ``pad'' bytes used to fill out
  the packet.

  -c               Specify the number of echo requests to be sent
  <IPv6 address>    IPv6 address
```

7.7.11.3 詳細

7.7.11.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
ping	✅	❌	❌
ping6	✅	❌	❌

7.7.12 reboot

7.7.12.1 説明

カードを再起動するためのツール。

7.7.12.2 ヘルプ

```
Usage: reboot [OPTION]
    <cr>                    Reboot the card
    --help                  Display help
    --withoutconfirmation   Reboot the card without confirmation
```

7.7.12.3 詳細

7.7.12.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
reboot	✅	❌	❌

7.7.13 save_configuration | restore_configuration

7.7.13.1 説明

. Save_configurationとrestore_configurationは、JSON形式を使用して、カードの構成の特定の部分を保存および復元しています。

7.7.13.2 ヘルプ

```
save_configuration -h
  save configuration: print the card configuration in JSON format to standard output.
```

```
restore_configuration -h
  restore_configuration: restore the card configuration from a JSON-formatted standard input.
```

7.7.13.3 使用例

7.7.13.3.1 linux ホストから:

Save over SSH: sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS save_configuration –p $PASSPHRASE> $FILE
Restore over SSH: cat $FILE | sshpass –p $PASSWORD ssh $USER@$CARD_ADDRESS restore_configuration –p $PASSPHRASE

7.7.13.3.2 Windows ホストから:

Save over SSH: plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch save_configuration –p $PASSPHRASE > $FILE
Restore over SSH: type $FILE | plink $USER@$CARD_ADDRESS –pw $PASSWORD –batch restore_configuration –p $PASSPHRASE (Require plink tools from putty)

Where:

・$ USERはユーザー名です(ユーザーは管理者プロファイルを持っている必要があります)

・$ PASSWORDはユーザーパスワードです

・$ PASSPHRASEは、適切なデータを暗号化/復号化するためのパスフレーズです。

・$ CARD_ADDRESSは、カードのIPまたはホスト名です。

・$ FILEは、構成が保存または復元されるJSONファイル(ホストコンピューター上)へのパスです。

7.7.13.4 詳細

7.7.13.5 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
save_configuration	✓	✗	✗
restore_configuration	✓	✗	✗

7.7.14 sanitize

7.7.14.1 説明

カードを出荷時設定にリセットする構成に戻すためのサニタイズコマンド。

7.7.14.2 アクセス

- 管理者

7.7.14.3 ヘルプ

```
sanitize
  -h, --help             Display help page
  --withoutconfirmation  Do factory reset of the card without confirmation
  <cr>                   Do factory reset of the card
```

7.7.14.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
sanitize	✓	✗	✗

7.7.15 ssh-keygen

7.7.15.1 説明

sshキーの生成に使用されるコマンド

7.7.15.2 ヘルプ

```
ssh-keygen
  -h, --help  Display help
  <cr>        Renew SSH keys
```

7.7.15.3 詳細

7.7.15.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
ssh-keygen	✓	✗	✗

7.7.16 time

7.7.16.1 説明

時刻と日付を表示または変更するために使用されるコマンド

7.7.16.2 ヘルプ

ビューアおよびオペレータプロファイルの場合:

```
time -h
 Usage: time [OPTION]...
 Display time and date.

   -h, --help      display help page
   -p, --print     display date and time in YYYYMMDDhhmmss format
```

管理者のためのプロファイル:

```
time -h
 Usage: time [OPTION]...
Display time and date, change time and date.
  -h, --help      display help page
  -p, --print     display date and time in YYYYMMDDhhmmss format
  -s, --set <mode>
      Mode values:
      - set date and time (format YYYYMMDDhhmmss)
          manual <date and time>
      - set preferred and alternate NTP servers
          ntpmanual <preferred server> <alternate server>
      - automatically set date and time
          ntpauto
Examples of usage:
-> Set date 2017-11-08 and time 22:00
     time --set manual 201711082200
-> Set preferred and alternate NTP servers
     time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

7.7.16.3 使用例

```
 -> Set date 2017-11-08 and time 22:00
      time --set manual 201711082200
 -> Set preferred and alternate NTP servers
      time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

7.7.16.4 詳細

7.7.16.5プロファイルごとのアクセス権

	Administrator	Operator	Viewer
time	✓	✓ (read-only)	✓ (read-only)

7.7.17 tracerouteおよび traceroute6

7.7.17.1 説明

TracerouteおよびTraceroute6ユーティリティは、ネットワークの構成を確認するためのものです。

7.7.17.2 ヘルプ

```
traceroute
  -h                Specify maximum number of hops
  <Hostname or IP>  Remote system to trace
```

```
traceroute6
  -h                Specify maximum number of hops
  <IPv6 address>    IPv6 address
```

7.7.17.3 詳細

7.7.17.4プロファイルごとのアクセス権

	Administrator	Operator	Viewer
traceroute	✓	✗	✗
traceroute6	✓	✗	✗

7.7.18 whoami

7.7.18.1 説明

whoamiは現在のユーザー情報を表示します:

- Username
- Profile
- Realm

7.7.18.2 詳細

7.7.18.3 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
whoami	✓	✓	✓

7.7.19 email-テスト

7.7.19.1 説明

mail-testは、SMTPの問題をトラブルシューティングするためのテストメールを送信します。

7.7.19.2 ヘルプ

```
        Usage: email-test <command> ...
Test SMTP configuration.

Commands:
  email-test -h, --help, Display help page

  email-test -r, --recipient <recipient_address>
  Send test email to the
    <recipient_address>      Email address of the recipient
```

7.7.19.3 詳細

7.7.19.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
email-test	✓	✗	✗

7.7.20 systeminfo_statistics

7.7.20.1 説明

以下のシステム情報の使用法を表示します:

1. CPU
   a. usage : %
   b. upSince : date since the system started
2. Ram
   a. total: MB
   b. free: MB
   c. used: MB
   d. tmpfs: temporary files usage (MB)
3. Flash
   a. user data
      i. total: MB
      ii. free: MB
      iii. used: MB

7.7.20.2 Help

```
systeminfo statistics
                      Display systeminfo statistics

        -h, --help       Display the help page.
```

7.7.20.3 詳細

7.7.20.4 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
systeminfo_statistics	✓	✓	✓

7.7.21 証明書

7.7.21.1 説明

CLIを介して証明書を管理できます。

7.7.21.2 ヘルプ

```
certificates <target> <action> <service_name>
  <target> :
        - local
  <action> :
        - print: provides a given certificate detailed information.
        - revoke: revokes a given certificate.
        - export: returns a given certificate contents.
        - import: upload a given certificate for the server CSR. This will replace the CSR
with the certificate given.
        - csr: get the server CSR contents. This will create the CSR if not already existing.
  <service_name>: mqtt/syslog/webserver
```

7.7.21.3 使用例

7.7.21.3.1 linux ホストから:

print over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local print $SERVICE_NAME revoke over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local revoke $SERVICE_NAME

export over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local export $SERVICE_NAME
import over SSH: cat $FILE | sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local import

$SERVICE_NAME csr over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local csr mqtt

7.7.21.3.2 Windows ホストから: (puttyからのplinkツールが必要です)

print over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local print $SERVICE_NAME
revoke over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local revoke $SERVICE_NAME

export over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local export $SERVICE_NAME
import over SSH: type $FILE | plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local import
$SERVICE_NAME

csr over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local csr mqtt

7.7.21.3.3 Where:

- $ USERはユーザー名です(ユーザーは管理者プロファイルを持っている必要があります)
- $ PASSWORDはユーザーパスワードです
- $ PASSPHRASEは、適切なデータを暗号化/復号化するためのパスフレーズです。
- $ CARD_ADDRESSは、カードのIPまたはホスト名です。
- $ FILEは証明書ファイルです
- $ SERVICE_NAMEは、mqtt / syslog / webserverのいずれかの名前です。

7.7.21.4 詳細

7.7.21.5 プロファイルごとのアクセス権

	Administrator	Operator	Viewer
certificates	✓	✗	✗

7.8 法的情報

このネットワークモジュールには、さまざまなオープンソースライセンスまたはプロプライエタリライセンスのいずれかでライセンスされているソフトウェアコンポーネントが含まれています。

詳細については、フッターのメインユーザーインターフェースからの法的情報リンクを参照してください。

7.8.1 ソースコードの可用性

ライセンサーが提供するオープンソースコンポーネントのソースコードは、書面による明示的な要求に応じて、network-m2-opensource @ Eaton.comに連絡して入手できます。 イートンは、状況に応じて、基盤となるオープンソースライセンスの条件に従って、最小限の管理コストを請求する権利を留保します。

7.8.2 オープンソース要素の注意事項

この製品には、BSDまたはApache v2ライセンスの下でリリースされ、次のようなさまざまなプロジェクト、人々、およびエンティティによって開発されたソフトウェアが含まれていますが、これらに限定されません。

- * the Regents of the University of California, Berkeley and its contributors,
- * the OpenEvidence Project,
- * Oracle and/or its affiliates,
- * Mike Bostock,
- * JS Foundation and other contributors,
- * 2011-2014 Novus Partners, Inc.

この製品には、OpenSSLToolkitで使用するためにOpenSSLProjectによって開発されたソフトウェアが含まれています。（www.openssl.org/）。
この製品には、Eric Young（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれています。
この製品には、MITライセンスの下でリリースされ、次のようなさまざまなプロジェクト、人々、およびエンティティによって開発されたソフトウェアが含まれていますが、これらに限定されません：

- * Google, Inc.,
- * the AngularUI Team
- * Lucas Galfasó
- * nerv
- * Angular
- * Konstantin Skipor
- * Filippo Oretti, Dario Andrei
- * The angular-translate team and Pascal Precht,
- * Twitter, Inc.
- * Zeno Rocha
- * Kristopher Michael Kowal and contributors
- * JS Foundation and other contributors
- * Jonathan Hieb
- * Mike Grabski
- * Sachin N.

この製品には、Creative Commons Attribution 4.0、Creative Commons Attribution-ShareAlike 3.0UnportedおよびSILOpen Font Licenseライセンスの下でリリースされ、以下によって作成されたコンテンツが含まれています：

- * IcoMoon
- * Dave Gandy
- * Stephen Hutchings and the Typicons team.

完全で最新の著作権情報、ライセンス、および免責事項にアクセスするには、本製品のHTMLユーザーインターフェースから入手できる「法的情報」ページを参照してください。

7.8.3 当社独自の（オープンソースではない）要素についての注意事項

7.9 頭字語と略語

AC：交流。
ATS：自動転送スイッチは、2つのソース間で負荷を切り替える電気スイッチです。

AVR：自動電圧調整は、機器を最適な範囲で稼働させ続けるための安定した電圧を提供します。BMS：バッテリー管理システムは、リチウムイオンバッテリーを管理する電子システムです。
bps：ビット/秒
BOM：Syslogでは、テキストストリームの先頭にエンコードされたバイト順マークを配置すると、テキストがUnicodeであることを示し、使用されているエンコードスキームを識別できます。
CA：認証局
CLI：コマンドラインインターフェース。
目的は、連続するテキスト行（コマンドライン）の形式のコマンドを使用して、ネットワークモジュールと対話することです。CSR：証明書署名要求
DC：直流。
DN：識別名（LDAP）。
DHCPv6：ダイナミックホスト構成プロトコルバージョン6は、IPv6ネットワークでの動作に必要なIPアドレス、IPプレフィックス、およびその他の構成データを使用してインターネットプロトコルバージョン6（IPv6）ホストを構成するためのネットワークプロトコルです。
これは、IPv4のダイナミックホスト構成プロトコルに相当するIPv6です。
DNS：ドメインネームシステムは、インターネットまたはプライベートネットワークに接続されたコンピューター、サービス、またはその他のリソース用の階層型分散型ネーミングシステムです。
DST：夏時間。
EMP：環境モニタリングプローブ

GID：グループ識別子は、特定のグループ（LDAP）を表すために使用される数値です。

HTTPS：HTTPSは、トランスポート層セキュリティ（TLS）によって暗号化された接続内のハイパーテキスト転送プロトコル（HTTP）を介した通信で構成されます。
IPP：Intelligent Power Protectorは、管理者がブラウザベースの管理コンソールからデバイスを管理できるようにするWebベースのアプリケーションです。管理者は、単一のデバイス（UPS、ATS、ePDU）をローカルおよびリモートで監視、管理、および制御できます。使い慣れたブラウザインターフェースにより、ネットワーク上のどこからでもデバイス管理者ソフトウェアとデバイスクライアントソフトウェアに安全にアクセスできます。管理者は、電源障害設定を構成し、重要なサーバーの最大稼働時間のためにUPS負荷セグメントを定義できます。UPSは、ユーティリティ電源障害時に重要なデバイスのランタイムを延長するように構成することもできます。ほとんどのUPSの場合、背面パネルのレセプタクルは、負荷セグメントと呼ばれる1つ以上のグループに分割されており、個別に制御できます。重要度の低い機器に接続されている負荷セグメントをシャットダウンすることにより、重要度の高い機器の実行時間が延長され、保護が強化されます。
IPv4：インターネットプロトコルバージョン4は、インターネットプロトコル（IP）の4番目のバージョンです。
IPv6：インターネットプロトコルバージョン6は、インターネットプロトコル（IP）の最新バージョンです。
JSON：JavaScript Object Notationは、人間が読める形式のテキストを使用して、属性と値のペアと配列データ型で構成されるデータオブジェクトを送信するオープンスタンダードのファイル形式です。
kVA：キロボルトアンペア。
LAN：LANは、ローカルエリアネットワークであり、自宅やオフィスなどの小さなローカルエリアをカバーするコンピューターネットワークです。
LDAP：ライトウェイトディレクトリアクセスプロトコルは、インターネットプロトコルを介して分散ディレクトリ情報サービスにアクセスして維持するための業界標準のアプリケーションプロトコルです。

MAC：コンピューターのメディアアクセス制御アドレスは、ネットワークセグメントのデータリンク層で通信するためにネットワークインターフェースに割り当てられた一意の識別子です。
MIB：管理情報ベースは、通信ネットワーク内のエンティティを管理するために使用されるデータベースです。ほとんどの場合、SNMP（Simple Network Management Protocol）に関連付けられています。
NTP：ネットワークタイムプロトコルは、コンピューターシステム間のクロック同期のためのネットワークプロトコルです。
PDU / ePDU：配電ユニット（PDU）は、特にデータセンター内にあるコンピューターやネットワーク機器のラックに電力を分配するように設計された複数の出力を備えたデバイスです。
P / N：部品番号。
RTC：リアルタイムクロック。
RTU：リモートターミナルユニットS / N：シリアル番号。
SMTP：Simple Mail Transfer Protocolは、電子メール（Eメール）送信のインターネット標準です。
SNMP：Simple Network Management Protocolは、IPネットワーク上の管理対象デバイスに関する情報を収集および整理し、その情報を変更してデバイスの動作を変更するためのインターネット標準プロトコルです。
SSH：Secure Shellは、セキュリティで保護されていないネットワーク上でネットワークサービスを安全に運用するための暗号化ネットワークプロトコルです。 SSL：Secure Sockets Layerは、ネットワークトラフィックに使用される暗号化プロトコルです。
TCP：伝送制御プロトコル
TLS：トランスポート層セキュリティは、コンピューターネットワークを介した通信セキュリティを提供する暗号化プロトコルです。
TFTP：Trivial File Transfer Protocolは、クライアントがリモートホストからファイルを取得したり、リモートホストにファイルを配置したりできるようにする単純なロックステップファイル転送プロトコルです。
UID：ユーザー識別子（LDAP）。
UTC：協定世界時は、世界が時計と時間を規制する主要な時間基準です。

UPS：無停電電源装置は、入力電源または主電源に障害が発生したときに負荷に緊急電力を供給する電気装置です。
UPSは通常、コンピューター、データセンター、通信機器、その他の電気機器など、予期しない停電によって怪我、死亡、重大なビジネスの中断、またはデータ損失が発生する可能性のあるハードウェアを保護するために使用されます。

8 トラブルシューティング

8.1 制御/スケジュール/停電ポリシーで許可されていないアクション

8.1.1 現象

以下のメッセージは、制御、スケジュール、または停電ポリシーページにアクセスすると表示されます。

このアクションはUPSでは許可されていません。

これを有効にするには、UPSのユーザーマニュアルと、UPS設定を構成してリモートコマンドを許可する方法についての説明を参照してください。

8.1.2 考えられる原因

1- UPS構成のため、リモートコマンドは許可されていません（以下のアクションを参照）

2- UPSはリモートコマンドをサポートしていません。

8.1.3 アクション

UPS の設定やリモートコマンドを許可する方法については、UPS のユーザーマニュアルとその説明書を参照してください。例: UPS menu Settings>>>ON/OFF settings>>>Remote command>>>Enable.

8.2 カードのタイムスタンプが間違っていると、ソフトウェアに「完全な取得に失敗しました」というエラーメッセージが表示されます

8.2.1 現象

IPP / IPMは、資格情報が正しい場合でも、「完全なデータ収集に失敗しました」というエラーメッセージを表示します。

8.2.2 考えられる原因

ネットワークモジュールのタイムスタンプが正しくありません。
おそらく、MQTT証明書はネットワークモジュールの日付では無効です。

8.2.3 アクション

適切な日付、時刻、タイムゾーンを設定します。 可能であれば、NTPサーバーを使用してください。

Contextual help>>>Settings>>>General>>>System details>>>Time & date settingを参照してください。

8.3 クライアントサーバーが再起動しない

8.3.1 現象

ユーティリティ電源が復旧し、UPSとその負荷セグメントの電源がオンになりましたが、クライアントサーバーは再起動しません。

8.3.2 考えられる原因

「自動電源オン」サーバー設定が無効になっている可能性があります。

8.3.3 アクション

.サーバーシステムBIOSで、自動電源オンの設定を「有効」に変更します

8.4 EMP検出が発見段階で失敗する

ネットワークモジュールのContextual help>>>Environment>>>Commissioning/Statusで、センサーコミッショニングテーブルにEMPがありません。

8.4.1 現象 #1

EMPの緑色のRJ45LED（FROM DEVICE）がオンになっていません。

8.4.1.1 考えられる原因

EMPは、ネットワークモジュールから電力を供給されていません。

8.4.1.2 アクション #1-1

ディスカバリーを再度起動します。それでも問題が解決しない場合は、アクション＃1-2に進みます。

8.4.1.3 現象 #1-2

1- EMPの接続とケーブルを確認します。EMP>>>Installing the EMP>>>Cabling the first EMP to the device and Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs.のEMPのセクションを参照してください。

2- USB-RS485ケーブルを取り外して再接続します。

3- ディスカバリーを起動します。それでも問題が解決しない場合は、アクション＃1-3に進みます。

8.4.1.4 アクション #1-3

1- ネットワークモジュールを再起動します。

2- ディスカバリーを起動します。

8.4.2 現象 #2

EMPのオレンジ色のRJ45LEDが点滅していない.

8.4.2.1 考えられる原因

C＃1：EMPアドレススイッチはすべて0に設定されています。

C＃2：EMPはデイジーチェーン接続されており、Modbusアドレスは欠落しているEMPで同じです。

8.4.2.2 アクション #2-1

1- EMPのアドレスを別のアドレスに変更し、すべてのスイッチが0にならないようにします。EMP>>>Defining EMPs address and termination>>>Manual addressing.のセクションを参照してください。

2- USB-RS485ケーブルを取り外して再接続します。 アドレスの変更は、EMPの電源投入後にのみ考慮されます。

3- ディスカバリーを起動します。それでも問題がない場合は、アクション＃2-2に進みます。

8.4.2.3 アクション #2-2

1- ネットワークモジュールを再起動します。

Contextual help>>>Maintenance>>>Services>>>Rebootを参照してください。

2-ディスカバリーを起動します。

8.5 パスワードを忘れた場合、どうすればログインできますか？

8.5.1 アクション

- 管理者にパスワードの初期化を依頼してください。
- メイン管理者の場合は、Network Management Module>>>Recovering main administrator passwordで説明されている手順に従って、パスワードを手動でリセットできます。

8.6 ソフトウェアがネットワークモジュールと通信できない

8.6.1 現象

- ·ネットワークモジュールのContextual help>>>Protection>>>Agent list>>>Agent list tableで、エージェントはステータスとして「Lost」を表示しています。
- ネットワークモジュールの Contextual help>>>Settings>>>Certificate>>>Trusted remote certificatesで、保護されたアプリケーション（MQTT）のステータスが「Not valid yet」と表示されます。
- IPP / IPMは、「The authentication has failed」、「The notifications reception encountered error」と表示します。

8.6.2 考えられる原因

IPP / IPM証明書は、ネットワークモジュールではまだ有効ではありません。

IPP / IPMとネットワークモジュールの証明書が一致していないため、ネットワークモジュールとシャットダウンエージェント間の接続の認証と暗号化が機能していません。

8.6.3 セットアップ

IPP / IPMが開始されます。

ネットワークモジュールはUPSとネットワークに接続されています。

8.6.4 アクション #1

ネットワークモジュールのIPP / IPM証明書の有効性を確認してください。

STEP1：ネットワークモジュールに接続する
·ネットワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。
·[Address/Location]フィールドに、次のように入力します。https：//xxx.xxx.xxx.xxx/ここで、xxx.xxx.xxx.xxxはネットワークモジュールのスタティックIPアドレスです。
·ログイン画面が表示されます。
·[User Name]フィールドにユーザー名を入力します。
·[Password]フィールドにパスワードを入力します。
·[Login]をクリックします。ネットワークモジュールのWebインターフェースが表示されます。

STEP2：[**Settings/Certificates**]ページに移動します

STEP3：[**Trusted remote certificates**]セクションで、保護されたアプリケーション（MQTT）のステータスを確認します。
「有効」の場合は、アクション＃2のSTEP2に進みます。「**Not yet valid**」の場合は、IPP / IPMと同期する必要があります。

STEP4：ネットワークモジュールの時刻をIPP / IPMと同期し、**保護されたアプリケーション（MQTT）**のステータスが有効になったことを確認します。

アクション＃2 STEP2に進まない場合、通信は回復します。

8.6.5 アクション #2

エージェントをネットワークモジュールにペアリングし、自動受け入れします（インストールが安全で信頼できるネットワークで行われる場合に推奨されます）

> 手動ペアリング（最大のセキュリティ）については、Network Management Module>>>Pairing agent to the Network Module]セクションに移動してから、STEP2の項目1に移動します。

STEP1：ネットワークモジュールに接続します。

·ネットワークコンピューターで、サポートされているWebブラウザを起動します。ブラウザウィンドウが表示されます。

·[アドレス/場所]フィールドに、次のように入力します。https：//xxx.xxx.xxx.xxx/ここで、xxx.xxx.xxx.xxxはネットワークモジュールのスタティックIPアドレスです。

·ログイン画面が表示されます。

·[User Name]フィールドにユーザー名を入力します。

·[Password]フィールドにパスワードを入力します。

·**[Login（ログイン）]**をクリックします。ネットワークモジュールのWebインターフェースが表示されます。

STEP2：**Protection/Agents list**ページに移動します。

STEP3：[**Pairing with shutdown agent**]セクションで、新しいエージェントを受け入れる時間を選択し、**[Start]**ボタンを押して**[Continue]**を押します。選択した時間枠の間に、ネットワークモジュールへの新しいエージェント接続が自動的に信頼され、受け入れられます。

STEP4：新しいエージェントを受け入れる時間がネットワークモジュールで実行されている間の**エージェントに対するアクション（IPP / IPM）**

Eaton ¥ IntelligentPowerProtector ¥ configs ¥ tlsフォルダーにあるネットワークモジュール証明書ファイル* .0を削除します。

8.7 LDAP設定/コミッショニングが機能しない

Servicing the Network Management Module>>>Commissioning/Testing LDAP.を参照。

8.8 プロファイルのパスワード変更が機能しない

8.8.1 現象

プロファイルメニューでパスワードを変更しようとすると、パスワードの変更に「Invalid credentials」と表示されます:

8.8.2 考えられる原因

パスワードは、1日のうちに1回変更されています。

8.8.3 アクション

最後のパスワード変更と再試行の間に1日かかります。

8.9 保存と復元に関するSNMPv3パスワード管理の問題

8.9.1 影響を受けるFWバージョン

この問題は、バージョン1.7.0以降に適用された場合、1.7.0より前のバージョンで行われたSNMP構成に影響します。

8.9.2 現象

1.7.0バージョン以降で設定を復元した後、SNMPv3接続が正しく機能しない

8.9.3 原因

SNMPv3は、1.7.0より前に**構成**されていました。

その場合、SNMPv3構成は、保存および復元設定によって適切に管理されません。

8.9.4 アクション

. バージョン1.7.0以降でSNMPv3ユーザーとパスワードを**再構成**し、設定を保存します。その後、SNMPv3構成を復元できます。

8.10 アップグレード後にアラームリストがクリアされた

8.10.1 現象

FWのアップグレード後、アラームリストはクリアされ、空になりました。

8.10.2 アクション

アラームリストはcsvファイルに保存されており、RestAPI呼び出しを使用して取得できます。

8.10.2.1 認証する:

```
curl --location --request POST 'https://{{domain}}/rest/mbdetnrs/1.0/oauth2/token' \
--header 'Content-Type: application/json' \
--data-raw '{ "username":"admin", "password":"supersecretpassword", "grant_type":"password",
"scope":"GUIAccess" }'
```

8.10.2.2 アラームログバックアップの取得:

```
curl --location --request GET 'https://{{domain}}/rest/mbdetnrs/1.0/alarmService/actions/
downloadBackup' \
--header 'Authorization: Bearer {{access_token}}'
```

8.11 ファームウェアのアップグレード後、ネットワークモジュールの起動に失敗する

8.11.1 考えられる原因

IPアドレスが変更されました。
注:ファームウェアのフラッシュ中の中断などによりアプリケーションが破損している場合、起動は以前のファームウェアで実行されます。

8.11.2 アクション

IPアドレスを回復し、カードに接続します。

Installing the Network Management Module>>>Accessing the Network Module>>>Finding and setting the IP address セクションを参照。

8.12 FWアップグレード後のWebユーザーインターフェースが最新ではない

8.12.1 現象

アップグレード後:

- Webインターフェースが最新ではありません。
- 新しいFWの新機能は表示されません。

8.12.1.1 考えられる原因

ブラウザは、以前のFWデータを含むキャッシュを介してWebインターフェースを表示しています。

8.12.1.2 アクション

F5またはCTRL + F5を使用してブラウザのキャッシュを空にします。