

Panduit EL2P PDU

ユーザーマニュアル

Version 1.8

目次

AI 利用に最適化されたドキュメント	12
AI 対応ユーザーマニュアル	12
セクション 1 – システム概要	13
PDU コントローラー	13
イーサネットポート経由で NMC を接続する	13
NMC をコンピュータのシリアルポートに接続する	15
セクション 2 – Web グラフィカルユーザーインターフェイス (GUI).....	16
インターネットプロトコル (IP) アドレス指定	16
Web 接続	16
Web GUI の開始	18
ダッシュボードの開始	20
システム管理情報	22
ネットワーク設定	28
ユニット情報	36
NMC の時刻と日付を設定する	39
制御と管理	42
アウトレット電力管理	43
アウトレットの制御の有効化/無効化	47
アウトレットパワーシーケンスのセットアップ	48
すべての PDU エネルギーをリセットする	51
PDU エネルギー	52
アウトレットのエネルギー	53
計測の閾値を設定する	56
Syslog セットアップ	66
メールセットアップ	69
イベントログ	72
データログ	73
Web インターフェイスアクセス	74
RADIUS 認証のシステムを設定する	76
LDAP サーバー設定でシステムを構成する	79
イベント通知	82

セクション 3 – 簡易ネットワーク管理プロトコル (SNMP).....	83
SNMP マネージメント構成	83
SNMP ユーザーを構成する	85
SNMP トラップを構成する	88
セクション 4 – ローカルディスプレイ	91
オンボードディスプレイおよびネットワークコントローラ	91
ネットワークコントローラメニューの構造	92
メインメニューの選択項目	92
[Sensors] メニュー	98
[Settings] メニュー	98
[Help] メニュー	108
検索ボックス.....	108
セクション 5 – デイジーチェーン構成.....	110
デイジーチェーンの概要	111
デイジーチェーンセットアップ	111
ブリッジモードのデイジーチェーン	112
ブリッジモードのセットアップ	113
パワーシェア	114
セクション 6 – EL2P PDU アクセサリー	115
ハードウェアの概要	115
温度スケールを構成する	118
環境センサーを構成する.....	119
セキュリティセンサーを構成する	120
センサーを削除する.....	121
セクション 7 – セキュリティハンドル	122
キャビネットアクセスコントロールを構成する.....	123
ローカルラックアクセスのユーザーを追加する.....	124
ラックアクセス設定を構成する	130
ハンドル設定を構成する	131

キーパッド設定を構成する	132
ハンドルをリモート制御する	133
ビーコンを制御する	134
ステータス LED	136
ステータス LED の状態を設定する	137
ハンドルおよび互換カードの種類	137
セクション 8 – セキュリティ	138
適合規格	138
プライマリ機能への API アクセス	138
プライマリ機能	138
安全処理機能	138
セキュア消去 – NIST SP 800-88 準拠のデータ抹消処理	139
概要	139
NIST SP 800-88 Rev. 1 の分類	139
eMMC 除去手順 (NMC)	139
SPI NOR フラッシュ消去手順 (バックプレーン)	140
トリガーおよび実行フロー	141
ログへの記録と監査	141
制限事項	142
参考文献	142
不揮発性ストレージ	142
認証データ	142
認証の優先順位	143
ネットワーク転送セキュリティ	143
無線通信	141
ネットワーク構成データ	145
ログへの記録	146
外部認証メカニズム	146
セキュアブート保護	146
ファームウェアの更新の保護	147
その他の機能	147
プロトコル	147

安全な設置	147
セキュリティに関する応答	150
保証および規制について	151
保証について	151
規制について	151
製品サポートおよび他のリソース	152
パンドウイトのサポートにアクセスする	152
導入済み製品のグローバルシステムサポート	152
展開されたソリューション向けのグローバルシステムサポート	153
頭字語と略語	154
付録 A: ファームウェアの更新手順	155
手動更新	155
自動更新	156
自動更新の構成	156
付録 B: システムリセットまたはパスワード復旧	158
付録 C: Bonjour を使用しないイーサネット経由の直接接続	161
付録 D: コマンドラインインターフェイス	164
付録 E: RADIUS サーバー構成	167
付録 F: POSIX タイムゾーン情報	169
付録 G: セキュアゼロタッチプロビジョニング (sZTP)	170
SZTP の利用開始	170
SZTP セットアップの概要	170
証明書の構成	170
バウチャーの申請	171
SZTP の操作	171
付録 H: ゼロタッチプロビジョニング (ワンタッチ ZTP)	172
ワンタッチ ZTP の利用開始	172
ワンタッチ ZTP セットアップの概要	172
付録 I: SZTP サーバー検出 (DHCP または mDNS)	174
mDNS	174
DHCP オプション	174

付録 J: SZTP ブートストラップサーバーのインストール	176
ブートストラップサーバー構成	180
SZTP のトラブルシューティング	182
付録 K: Onboard Data Collector の構成	184
要件	184
コレクター PDU のセットアップ	185
デバイス PDU のセットアップ	187
Cisco Nexus Dashboard への PDU 登録.....	189
注意.....	192
セキュリティ	192
通信図	193
付録 L: SiteCommand ユーティリティを使用した一括管理	195
付録 M: よくある質問 (FAQ)	196

図の目次

図 1: LCD 構成	13
図 2: ネットワーク接続用イーサネットポート	13
図 3: シリアル入力ポート	15
図 4: ネットワーク情報	15
図 5: 接続が拒否された例	16
図 6: 証明書の警告	17
図 7: ログインページ	17
図 8: ログイン後	18
図 9: ランディングページ/ダッシュボード	18
図 10: 電力概要ページ	20
図 11: 電源アウトレットページ	20
図 12: 環境モニタリングページ	21
図 13: セキュリティモニタリングページ	21
図 14: システム管理	22
図 15: システム情報構成	23
図 16: LCD 構成	24
図 17: PDU の位置指定	25
図 18: PDU リージョン	25
図 19: システム管理アクション	26
図 20: アップロード構成	26
図 21: デフォルト設定の警告	26
図 22: セキュア消去の警告	27
図 23: セキュア消去の完了	27
図 24: 再起動の警告	27
図 25: イーサネットインターフェイス構成	28
図 26: DNS 構成	29
図 26: Web アクセス構成	29
図 28: ネットワーク設定	30
図 28: Web アクセス構成	30
図 30: 証明書のアップロード	31
図 31: SSH 構成	31
図 32: IEEE 802.1X 構成	33
図 33: IEEE 802.1X 検証オプション	34
図 34: ユニット情報	36
図 35: ラックの場所の構成	37
図 36: 電源パネルとコアの場所	38
図 37: 日付と時刻を設定する	39
図 38: NTP 構成	40
図 39: 夏時間のタイムゾーン構成	40
図 40: NTP テストを開始する	41

図 41: NTP テストのステータス	41
図 42: 制御と管理	42
図 43: 制御と管理のデフォルトのページ表示	42
図 44: アウトレットの名前指定、時間遅延、始動時の状態、再起動	44
図 45: アウトレットの制御	45
図 46: アウトレットの制御	46
図 47: [Outlet Control] メニュー項目	47
図 48: アウトレットの制御の有効化/無効化ダイアログ	47
図 49: PDU の制御と管理	48
図 50: アウトレットの編集	48
図 51: シーケンスオン遅延時間	49
図 52: 保存されたシーケンス	50
図 53: [Reset All PDU's Energy] メニュー項目	51
図 54: [Reset All PDU's Energy] ダイアログ	51
図 55: PDU エネルギー	52
図 56: PDU エネルギー構成	52
図 57: アウトレットのエネルギー	53
図 58: 複数の [Outlet Energy Configuration] ダイアログ	54
図 59: アウトレットのエネルギー構成	55
図 60: 閾値の設定	56
図 61: 閾値の構成	56
図 62: 電力閾値	57
図 63: プライマリまたはリンク PDU を選択する	58
図 64: 相電流アラーム	59
図 65: 相電圧アラーム	60
図 66: ロードセグメントブレーカー	62
図 67: アウトレット情報	64
図 68: メールセットアップ	66
図 69: Syslog 構成	67
図 70: Syslog マッピング	68
図 71: メールセットアップ	69
図 72: SMTP アカウント設定	70
図 73: メール受信者	71
図 74: イベントログ	72
図 75: イベントログのアクションメニュー	72
図 76: データログ	73
図 77: データログ構成	73
図 78: データログ構成パネル	73
図 79: ユーザーアカウント	76
図 80: RADIUS 構成	76

図 81: ユーザーアカウント	77
図 82: TACACS+ 構成	78
図 83: LDAP 構成	80
図 84: 役割権限を有効にする	81
図 85: イベント通知	82
図 86: SNMP 構成	83
図 87: SNMP の一般情報	83
図 88: SNMP ポート	84
図 89: SNMP ポートおよびトラップポートのセットアップ	84
図 90: SNMP V1/V2c ユーザーの定義	85
図 91: V1/2c マネージャーの編集	85
図 92: SNMP v3 マネージャー	86
図 93: SNMP V3 の編集	87
図 94: SNMPv2c トラップレシーバー構成情報	88
図 95: SNMPv3 トラップサーバー構成情報	89
図 96: ネットワークコントローラ	91
図 97: ネットワークコントローラメニューの構造	92
図 98: メインメニューの選択項目	92
図 99: [Alarms] メニュー	93
図 100: [Power] メニュー	93
図 101: [Device] サブメニュー	94
図 102: [Phase] サブメニュー	95
図 103: [Breaker] サブメニュー	96
図 104: [Outlet] サブメニュー	97
図 105: センサー	98
図 106: [Setup] メニュー	98
図 107: [Network] サブメニュー	99
図 108: [Screen] サブメニュー	100
図 109: [Language] サブメニュー	101
図 110: [Units] サブメニュー	102
図 111: USB の有効化	103
図 112: [USB] サブメニュー	105
図 113: [Network] メニュー	106
図 114: 情報メニュー	107
図 115: ヘルプとサポート	108
図 116: 検索ボックスの例	109
図 117: システム管理	110
図 118: リンクされる構成	110
図 119: 6 つの PDU デイジーチェーンの接続図	111

図 120: 冗長構成およびパワーシェアを使用したブリッジモードのデ이지ーチェーン	114
図 121: センサーポート	117
図 122: ユーザーアカウント	118
図 123: 温度単位の設定	118
図 124: 環境センサー閾値構成ビュー	119
図 125: 温度センサーの編集ダイアログ	119
図 126: セキュリティセンサーアラーム構成ビュー	120
図 127: ドライ接点センサーの編集ダイアログ	121
図 128: 接続図	122
図 129: セキュリティハンドル	122
図 130: ラックアクセスコントロール	123
図 131: ラックアクセスコントロールアクション	123
図 132: イベントログ	124
図 133: カードの追加	125
図 134: カードの追加 (一時ユーザー)	126
図 135: カードアイルを指定したカードの追加	126
図 136: カードの編集	127
図 137: カードの編集 (一時ユーザー)	128
図 138: カードアイルを指定したカードの追加	129
図 139: ラックアクセス設定	130
図 140: ハンドル設定	131
図 141: キーパッド設定	132
図 142: リモート制御	133
図 143: ビーコン	134
図 144: ビーコン設定	135
図 145: ステータス LED	136
図 146: ステータス LED 設定	137
図 147: SSL 証明書のロード画面	148
図 148: アップロード	155
図 149: 自動更新	156
図 150: 自動更新の構成	157
図 151: ユーザーアイコンの [User Accounts]	159
図 152: 歯車アイコンの [User Accounts]	159
図 153: [Users] の表	160
図 154: [Edit User] 画面	160
図 155: ネットワーク接続の表示	161
図 156: プロパティ	161
図 157: イーサネットのプロパティ	162
図 158: インターネットプロトコルバージョン 4	162
図 159: CLI から読み取る	165
図 160: CLI から書き込む	166

図 161: Windows DHCP 構成.....	175
図 162: SZTP ライセンス.....	176
図 163: インストールフォルダ	177
図 164: 開始メニューの場所	177
図 165: インストールの確認.....	178
図 166: ブートストラップサーバー構成	179
図 167: インストール後のオプション.....	180
図 168: 構成のダウンロード.....	181
図 169: Windows イベントビューアー	182
図 170: SZTP イベントの例	183
図 171: コレクター PDU の Admin ユーザーの例	185
図 172: コレクター PDU での Onboard Data Collector の構成.....	186
図 173: デバイス PDU の Viewer ユーザーの例	187
図 174: デバイス PDU での Onboard Data Collector の構成.....	188
図 175: Cisco Nexus Dashboard の Integrations 画面.....	189
図 176: Cisco Nexus Dashboard と Panduit PDU の統合	189
図 177: コレクター PDU を Cisco Nexus Dashboard に登録する	189
図 178: ファブリックを選択する.....	190
図 179: 登録されたコレクター PDU	190
図 180: デバイス PDU の認証情報の例.....	191
図 181: Cisco Nexus Dashboard から Onboard Data Collector への通信.....	193
図 182: デバイス登録の通信	193
図 183: ポーリングするときの Onboard Data Collector 通信	194
図 184: SiteCommand ユーティリティ	195

AI 利用に最適化されたドキュメント

AI 対応ユーザーマニュアル

このユーザーマニュアルは、AI ツールで活用できるよう特別に作成されています。ご利用の AI ツールにそのまま入力できるよう、構成や用語、情報の整理方法を最適化しています。(例: Microsoft Co-Pilot®, Open AI ChatGPT®, Google Gemini®, Grok®)。

このマニュアルを AI ツールに読み込ませるだけで、以下を行えるようになります。

- 設定、操作、トラブルシューティングに関する質問を行う
- マニュアルに基づいた手順を確認する
- EL2P の機能や動作に応じた説明を得る

これにより、必要な情報へすばやくアクセスできるほか、検索にかかる時間を短縮でき、より対話的なサポートや学習を実現できます。

セクション1 - システム概要

PDUコントローラー

ホットスワップ可能な EL2P PDU コントローラには、タッチスクリーンと加速度計が搭載されています。加速度計によってディスプレイが自動回転し、上からの給電と下からに給電の向きに対応します。この一元型のインテリジェントハードウェアは、IP アドレスを受け取り、グラフィカル Web インターフェイスを持ち、ネットワーク経由でのアドレス指定が可能です。このユーザーマニュアルでは、PDU コントローラはネットワークマネジメントカード (NMC) とも呼ばれます。

PDU コントローラは Web GUI のシステム管理からも構成できます。

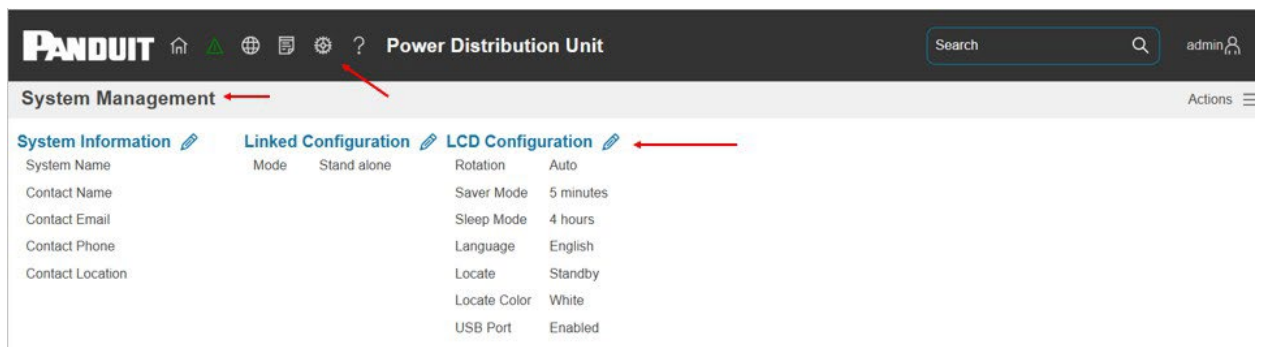


図 1: LCD 構成

イーサネットポート経由でNMCを接続する

NMC を LAN に接続することで、インターネットまたはイントラネット接続を介した通信が可能になり、インテリジェント配電ユニットからのモニタリングと制御が可能になります。

1. イーサネットケーブルを NMC のネットワークポートに接続します (図 1 参照)。
2. ケーブルの反対側の端をルーター (あるいは他の LAN デバイス) のネットワークポートに接続します。



図 2: ネットワーク接続用イーサネットポート

NMC は工場出荷時にデフォルトで DHCP および HTTPS 接続に設定されています。DHCP サーバーを使用したネットワークに接続している場合、NMC は自動的に IP アドレスを取得します。DHCP サーバーがない場合、NMC は IP を割り当てます (自動 IP)。自動 IP アドレスはリンクローカル IP アドレスになり、付録 C:Bonjour を使用しないイーサネット経由の直接接続の手順を使用して取得できます。NMC は、DHCP IP または自動 IP を検出するための mDNS をサポートしています。mDNS アドレス形式は、「pdu-<Mac アドレス>.local」です。例えば、図 1 の mDNS アドレスは、「pdu-000f9c03000b.local」に対応します。アドレスは NMC MAC アドレスに基づく固有アドレスです。

NMC をコンピュータのシリアルポートに接続する

ネットワークに接続できない場合は、シリアルインターフェイスを使用してネットワーク設定を取得できます。ネットワーク設定を検出するには、以下の手順を実行します。

1. PC を NMC のシリアルポートに接続します。図 3: シリアル入力ポートを参照してください。
2. ターミナルエミュレータプログラムを使用して、CLI コマンド「read」を送信します。
 - CLI 構成とパスワード変更については、付録 D: コマンドラインインターフェイスを参照してください。
3. 「read status.netStatus.*」と入力します。



図 3: シリアル入力ポート

```
COM21 - Tera Term VT
File Edit Setup Control Window Help

login: admin
password:
PANDUIT>read status/netStatus/*

status/netStatus/activeIPv4Address: 10.132.80.96
status/netStatus/activeIPv4Netmask: 255.255.255.0
status/netStatus/activeIPv4Gateway: 10.132.80.1
status/netStatus/linkLocalIPv6Address: fe80::20f:9cff:fe07:d78
status/netStatus/activeIPv6Address: 2001:1890:1974:3380:20f:9cff:fe07:d78
status/netStatus/ethMacAddr: 00:0f:9c:07:0d:78
PANDUIT>
```

図 4: ネットワーク情報

セクション2 - Web グラフィカルユーザーインターフェイス (GUI)

インターネットプロトコル (IP) アドレス指定

NMC が IP アドレスを受信した後、Web インターフェイスにログインして、NMC の構成や、静的 IP アドレスの割り当てを行うことができます (必要な場合)。

Web 接続

サポートされている Web ブラウザー

サポートされている Web ブラウザーは Google Chrome (モバイルおよびデスクトップ)、Mozilla Firefox、Microsoft Edge、および Apple Safari (モバイルおよびデスクトップ) です。

Web インターフェイスにログインする

- サポートされている Web ブラウザーを開いて、NMC の IP アドレスを入力します (HTTPS)。
- 「接続が拒否されました」と表示された場合、「http://」ではなく「https://」プロトコルを使用していることを再確認してください。

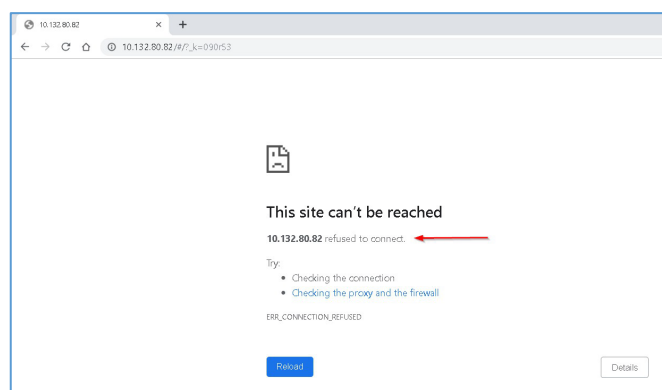


図 5: 接続が拒否された例

- デフォルトでは、Web インターフェイスで自己署名証明書が使用されています。CA 署名証明書や鍵がインストールされない限り、ブラウザーにセキュリティエラーが表示されます。Chrome ブラウザーでは、[Advanced] をクリックして、[Proceed to] リンクをクリックしてください。

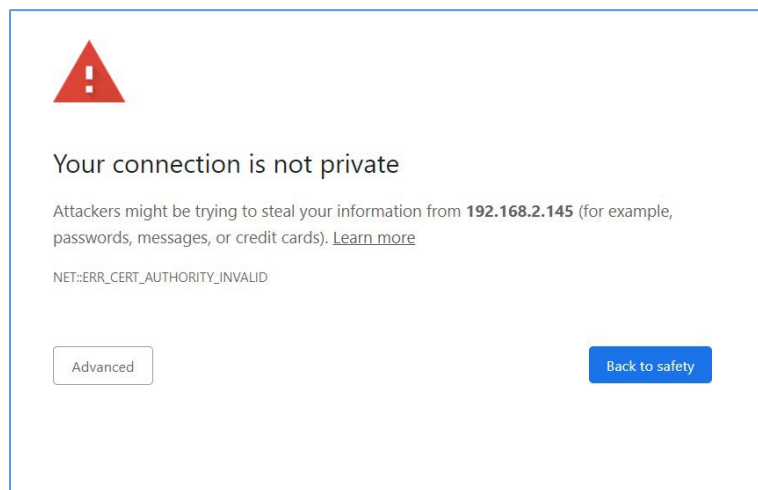


図 6: 証明書の警告

- ユーザー名とパスワードがまだ構成されていない場合、デフォルトのユーザー名 admin およびパスワード admin を使用します。セキュリティ保護のため、最初のログイン時にパスワードの変更が必要になります。
- 管理者資格が失われた場合、[付録 C](#) を使用して NMC を工場出荷時の初期設定にリセットしてください。



図 7: ログインページ

パスワードを変更する

最初のログイン時に、デフォルトのパスワードを変更する必要があります。

1. ユーザー名と現在のパスワードを入力してから、新しいパスワードを 2 度入力して確定します。パスワードは 8 ～ 40 文字にする必要があります、以下の 4 つの規則の 3 つに従う必要があります。
 - a. 小文字を 1 文字以上含む。
 - b. 大文字を 1 文字以上含む。
 - c. 数字を 1 文字以上含む。
 - d. 特殊文字を 1 文字以上含む。
2. [Log In] をクリックしてパスワードを変更します。

最初のログイン後にパスワードを変更するには、以下の手順を実行します。

1. ユーザー名をクリックし、[Change Password] を選択します。

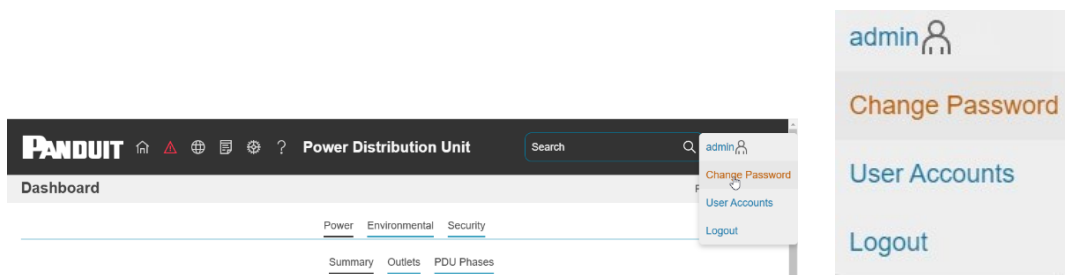


図 8: ログイン後

2. [Change Password] ウィンドウが開きます。
3. パスワードを変更するの手順に従います

Web GUI の開始

【注意】https:// を使用する必要があります (初回ログインの場合)

ランディングページ/ダッシュボード

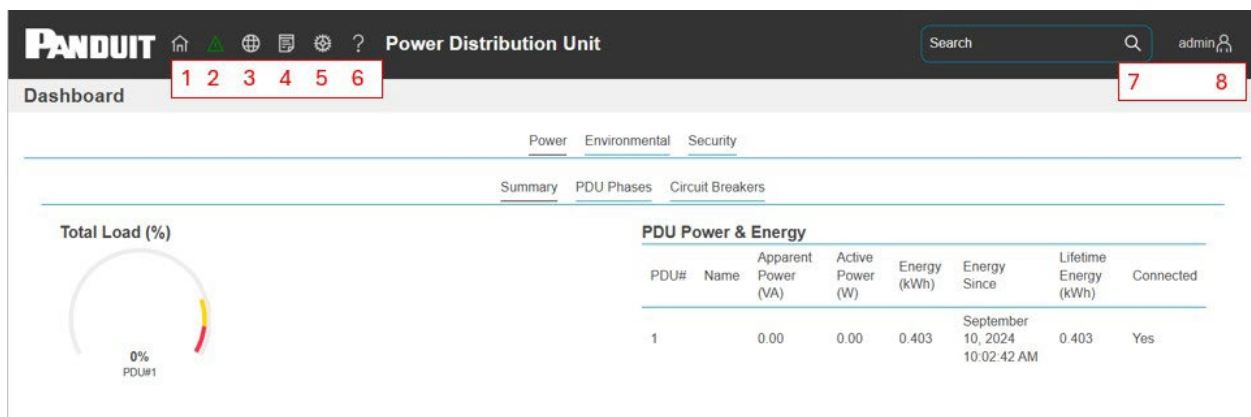


図 9: ランディングページ/ダッシュボード

番号	アイコン	説明
1		ホームアイコンは PDU の概要を示し、[Dashboard]、[Identification]、[Control & Manage]、[Rack Access Control] へのアクセスが可能です。
2		アラームアイコンは、作動しているアラームの詳細を示します。
3		このアイコンがある場合は、言語を選択できます。選択できる言語は、英語、フランス語、ドイツ語、スペイン語の 4 つです。
4		このアイコンが示す PDU のログは、表示したりダウンロードしたりできます。
5		設定アイコンは、ユーザーが「ネットワーク設定」、「システム管理」、「SNMP」、「メールセットアップ」、「トラップレシーバー」、「ユーザーアカウント」、「閾値」をセットアップできることを示します。
6		このアイコンを使用して、PDU に関するヘルプとサポートを見つけることができます。MIB とユーザーマニュアルは、このアイコンの下にあります。
7		検索アイコンは、キーワードを入力して関連する結果を検索できることを示します。
8		このアイコンはだれがログインしているか (user か admin か) を示します。アカウントのパスワードを変更できます。ユーザーアカウントをこのページから管理します。

ドロップダウンメニュー

Overview	Alarms	Language	Logs	Setting	Help	User
 Dashboard Identification Control & Manage Rack Access Control	 Active Alarms	 English Français Deutsch Español	 Event Log Data Log	 System Management Device Firmware Update Network Date & Time User Accounts Event Notifications SNMP Syslog Email Unit Information Thresholds	 Support	admin  Change Password User Accounts Logout

環境モニタリングページ

Power Environmental Security				
Internal Sensors				
Temperature (°C)				
30				
External Sensors				
Type	Sensor Name	Serial Number	Value	Status
Temperature		CN0145911B T1	23.0°C	✓OK
Temperature		CN0145911B T2	29.0°C	✓OK
Temperature		CN0145911B T3	24.0°C	✓OK
Humidity		CN0145911B RH	29.0%RH	✓OK

図 12: 環境モニタリングページ

パラメーター	説明
Type	温度、湿度、スポット、ロープ
Sensor Name	ユーザーが構成可能なセンサー名
Serial Number	センサーのシリアル番号
Value	センサーの測定値
Status	正常、閾値超過、アラーム

セキュリティモニタリングページ

Power Environmental Security				
Security Sensors				
Type	Sensor Name	Serial Number	Value	Status
Door		CN0048966C DOOR SWITCH	CLOSED	✓OK

図 13: セキュリティモニタリングページ

【注意】構成可能な PDU セキュリティ設定について詳しくは、セクション 8 を参照してください。

システム管理

システム管理には、データセンター内の PDU を特定するために使用されるシステム情報の構成や、システム構成のその他のオプションおよびアクションが含まれます。
システム管理に移動するには、歯車アイコンの下にある [System Management] を選択します。

System Management						
System Information 	Linked Configuration 		LCD Configuration 		Region Configuration 	
System Name	Mode	Daisy chain	Rotation	Auto	Region	EMEA
Contact Name	Role	Primary	Saver Mode	5 minutes		
Contact Email			Sleep Mode	4 hours		
Contact Phone			Language	English		
Contact Location			Locate	Standby		
			Locate Color	White		
			USB Port	Enabled		

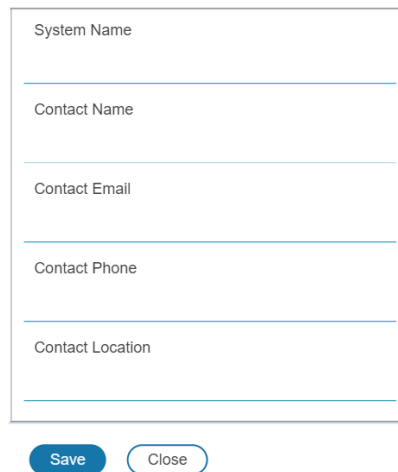
図 14: システム管理

システム情報

システム情報には、PDU システムの名前と、問題が発生した場合に連絡する担当者の情報が含まれています。システム情報を設定するには、以下の手順に従います。

1. [System Management] の横にある鉛筆アイコンを選択します。

System Information

A screenshot of the 'System Information' form. It is a vertical rectangle with a light gray border. Inside, there are five text input fields, each with a label above it: 'System Name', 'Contact Name', 'Contact Email', 'Contact Phone', and 'Contact Location'. Below the input fields, there are two buttons: a blue 'Save' button and a white 'Close' button with a blue border.

System Name
Contact Name
Contact Email
Contact Phone
Contact Location

Save Close

図 15: システム情報構成

2. [System Name] を入力します。
3. システムに問題があった場合に連絡する担当者の名前を [Contact Name] セクションに入力します。
4. 連絡する担当者のメールアドレスを [Contact Email] に入力します。
5. 連絡する担当者の電話番号を [Contact Phone] に入力します。
6. 連絡する担当者の所在地を [Contact Location] に入力します。
7. [Save] を選択します。

リンクされる構成

[Linked Configuration] サブメニューは、PDU デイジーチェーンを有効にするために使用します。詳しくは、「セクション 5 – デイジーチェーン構成」を参照してください。

LCD 構成

LCD 構成では LCD 設定のカスタマイズが可能です。

1. [System Management] → [LCD Configuration]

LCD Configuration

Rotation	
Auto	▼
Saver Mode	
5 minutes	▼
Sleep Mode	
4 hours	▼
Language	
English	▼
Locate	
Standby	▼
Locate Color	
White	▼
USB Screen	
☒ Enable	

SaveClose

図 16: LCD 構成

2. [LCD Configuration] の横にある鉛筆アイコンを選択します。
3. [Rotation] の選択: [Auto] では加速度計を使用して、回転を自動的に選択します。ほとんどの設置には [Auto] を使用しますが、それ以外の場合は画面の回転を角度で選択します。
4. [Saver Mode] の選択: LCD が、概要画面と概要画面が無効な状態との間でローテーションする時間を選択します。
5. [Sleep Mode] の選択: LCD 画面がオフになるまでの時間を選択するか、LCD がオフにならないようにするために無効にします。時間を短縮すると電力使用量が減少して LCD の寿命が延びます。
6. [Language] の選択: LCD で使用する言語を選択します。
7. [Save] を選択します。

PDU の位置指定

選択した色で LCD 画面を点滅させることによって、特定の PDU を見つける方法を指定します。

1. [LCD Configuration] の横にある鉛筆アイコンを選択します。
2. [Locate] を [Locate On] に変更します。
3. LCD 画面点滅の色を変更します。

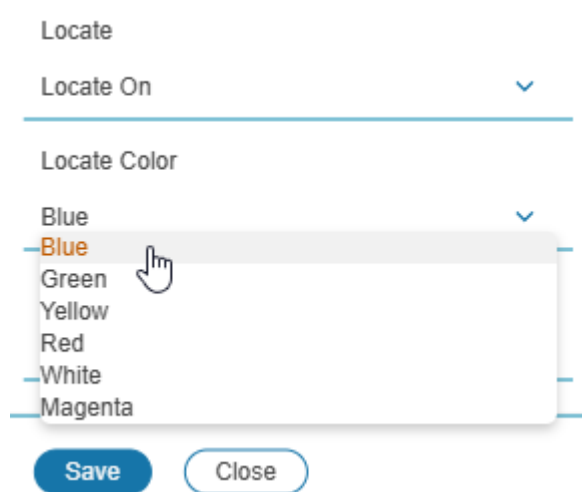


図 17: PDU の位置指定

4. [Save] を選択します。

PDU の点滅を停止するには、Web UI で [Locate] 設定を [Standby] に戻します。

リージョン構成

PDU がデュアル定格 PDU の場合、リージョンを北米と EMEA の間で切り替えることによって正しい PDU 定格を取得できます。

1. [Region Configuration] の横にある鉛筆アイコンを選択します。
2. リージョンを選択します。

Region Configuration

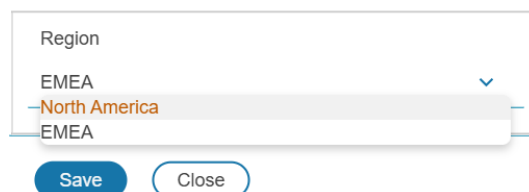


図 18: PDU リージョン

3. [Save] を選択します。

システム管理アクション

システム管理画面の右上にはアクションメニューがあります。一括設定や、PDU の初期化および再起動のオプションが用意されています。

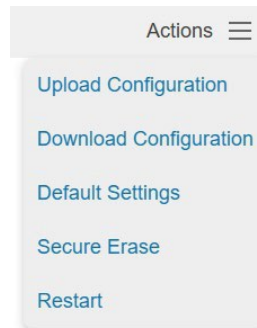


図 19: システム管理アクション

一括設定

[Download configuration] を選択して、PDU 構成をバックアップできます。クリックすると、config.json ファイルが自動的にダウンロードされます。

[Upload configuration] は、以前ダウンロードした config.json から設定を復元します。config.json をアップロードすることで、元のデバイスまたは同じ部品番号の PDU に設定を復元できます。

【注意】静的 IP などのデバイス固有のネットワーク設定は、ネットワークの競合を防ぐため config.json ファイルには含まれていません。

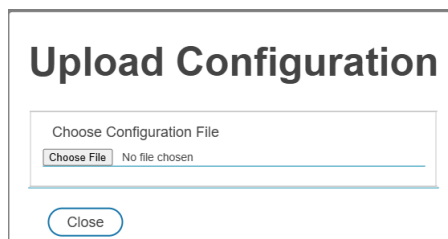


図 20: デフォルト設定の警告

デフォルト設定

[Default Settings] は、すべての設定とログを簡易消去して PDU を再起動します。エネルギーのデータは消去されません。

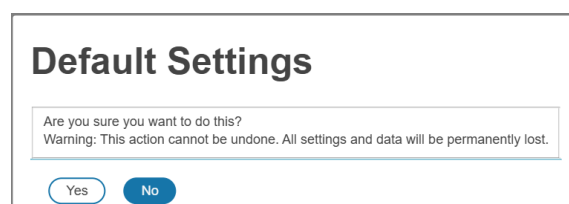


図 21: デフォルト設定の警告

セキュア消去

セキュア消去は、PDU に格納されているすべてのユーザーデータの完全かつ不可逆的な消去を実行します。デフォルトの消去設定に比べて、セキュア消去には時間がかかり、内部フラッシュメモリの条件および状態によっては数十分かかる可能性があります。

処理が完了すると、PDU は自動的に再起動し、LCD に “Secure Erase Complete” と表示されます。

セキュア消去では、すべての既存設定とユーザーデータが確実に削除されるため、PDU の安全な再設置、再販売、または再利用が可能になります。これにより、責任ある資産の再利用と製品ライフサイクルの延長 (“セカンドライフ”) の取り組みを支援します。

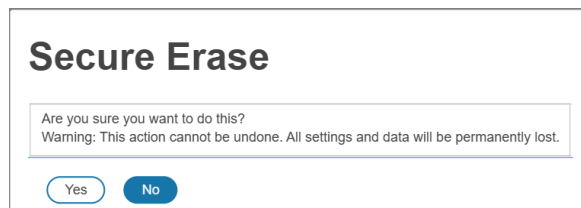


図 22: セキュア消去の警告

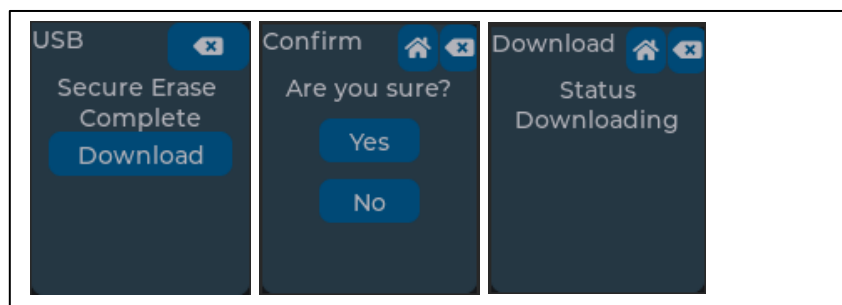


図 23: セキュア消去の完了

再起動

[Restart] は、PDU のウォームリブートを実行します。ほとんどの場合、すべてのネットワーク設定の変更は即時に反映されるため、再起動は不要です。

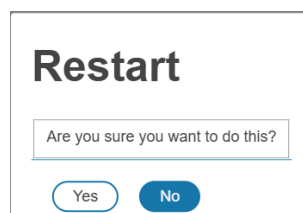


図 24: 再起動の警告

ネットワーク設定

ネットワーク設定では、IP 構成、DNS、Web アクセス、SSH 構成、およびその他のネットワーク設定を管理できます。

イーサネットインターフェイス構成

Ethernet Interface Configuration

IPv4 Enable
☒ Enable
IPv4 Configure Method
DHCP ▼
IPv4 Static Address
IPv4 Static Subnet Mask
IPv4 Static Gateway
IPv6 Enable
☒ Enable
IPv6 Configure Method
Autoconfiguration ▼
IPv6 Static Address
IPv6 Static Prefix Length
64
IPv6 Static Router

SaveClose

図 25: イーサネットインターフェイス構成

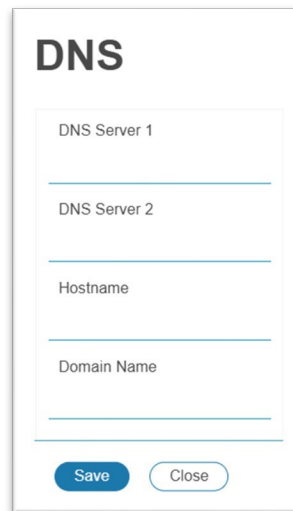
DNS 構成:

図 26: DNS 構成

Web アクセス構成

Web アクセス構成は、HTTP および HTTPS を設定するために使用します。また、このセクションは HTTPS 証明書をアップロードするためにも使用します。

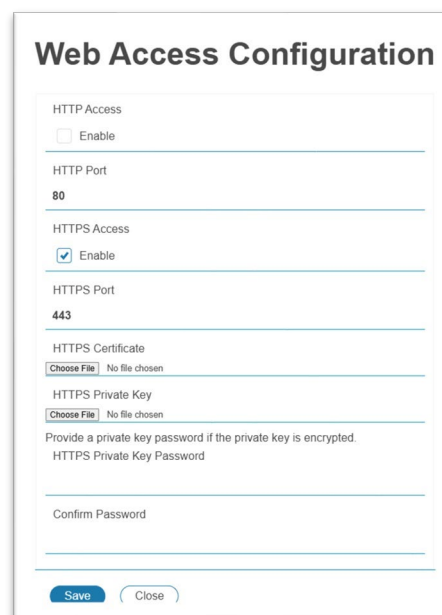


図 27: Web アクセス構成

カスタム TLS 証明書をアップロードする

製品にはデフォルトの RSA 2048 ビットのプライベートキーおよび証明書が付属しています。セキュリティを高めるために、カスタム TLS 証明書をアップロードすることをお勧めします。

1. 設定アイコンから [Network Setting] フォルダを選択します。

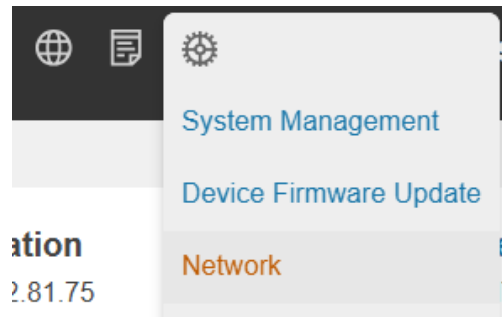


図 28: ネットワーク設定

2. [Web Access Configuration] から鉛筆アイコンを選択します。

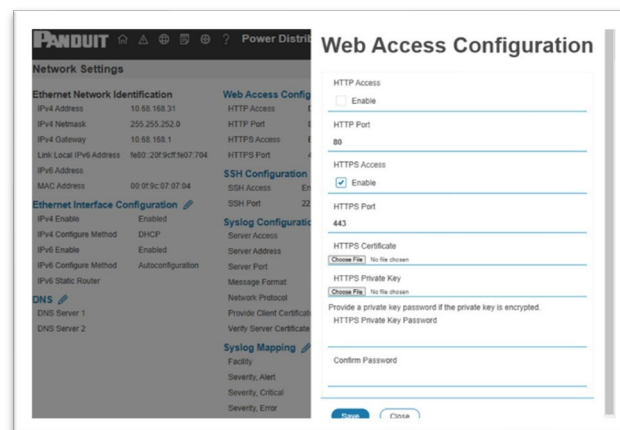
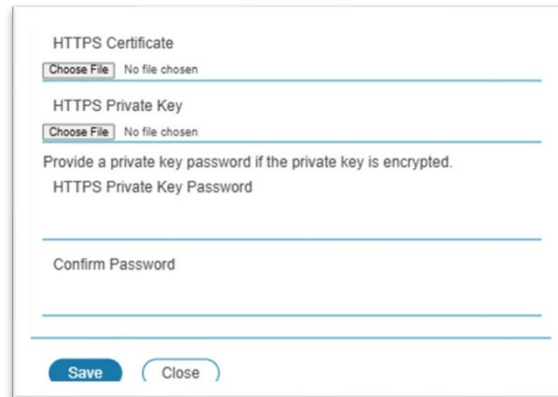


図 29: Web アクセス構成

3. [Choose File] ボタンを選択して、SSL 証明書と SSL 証明書鍵を選択します。

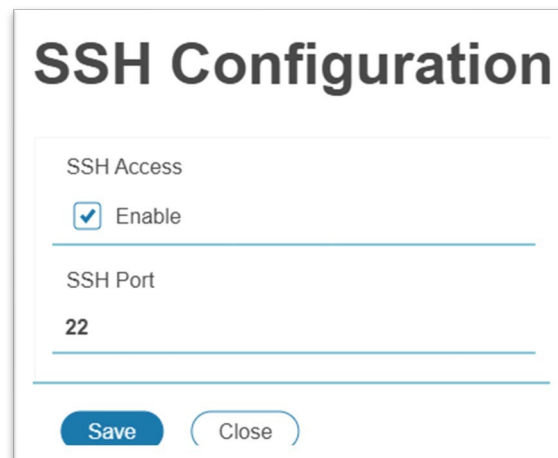


The dialog box is titled "HTTPS Certificate". It contains two "Choose File" buttons, each followed by the text "No file chosen". Below these is a section for the private key, starting with "HTTPS Private Key" and another "Choose File" button. A note states: "Provide a private key password if the private key is encrypted." Below this is a field for "HTTPS Private Key Password". At the bottom, there is a "Confirm Password" field. The dialog has "Save" and "Close" buttons at the bottom.

図 30: 証明書のアップロード

4. 証明書がパスコードで暗号化されている場合は、パスコードを入力し、[Passcode] フィールドにもう一度パスコードを入力します
5. [Save] を選択して証明書と鍵をアップロードします。

SSH 構成:



The dialog box is titled "SSH Configuration". It has a section for "SSH Access" with a checked checkbox and the label "Enable". Below this is a section for "SSH Port" with the value "22" entered. The dialog has "Save" and "Close" buttons at the bottom.

図 31: SSH 構成

IEEE 802.1X 構成:

IEEE 802.1X は、有線または無線ネットワークへのアクセスを許可する前にデバイスの認証を行うネットワークアクセス制御規格です。

IEEE 802.1X はゲートキーパーとして機能し、認証済みのデバイスのみがネットワーク上で通信できるようにします。

IEEE 802.1X では、3 つのコンポーネントで構成されるクライアントサーバーモデルを使用します。

コンポーネント	役割
サブリカント	ネットワークアクセスを要求するデバイス (このケースでは EL2P)
オーセンティケーター	アクセスを制御するネットワークスイッチまたはアクセスポイント
認証サーバー	通常は、資格情報を検証する RADIUS サーバー

802.1X を有効にした場合、EL2P のイーサネットポートは、ユーザー名とパスワードまたは証明書による認証が完了するまで使用できません。

組織では多くの場合、次の目的で 802.1X を有効にします。

セキュリティを強化する

不正なデバイスがネットワークに接続することを防ぎます。これは官公庁、医療、金融、および規制の厳しい業界において重要な要件です。

コンプライアンス要件を満たす

PCI-DSS、ISO 27001、NIST 指針などの規格では、通常、制御されたネットワークアクセスを必要とします。

アタックサーフェスを減らす

不正なデバイス、未承認のノート PC、またはセキュリティが侵害された IoT 機器の接続を防ぎます。

デバイスの ID を確認する

各デバイスは認証され、トレーサビリティと説明責任を確保する必要があります。

802.1X が設定されたスイッチポートに接続すると、EL2P は EAPOL (EAP over LAN) リクエストを送信して認証を開始します。

スイッチは認証情報を RADIUS 認証サーバーに転送します。

認証情報が有効な場合、スイッチはポートを開放し、通常の IP 通信を許可します。

有効でない場合、デバイスはブロックされるか、制限付き VLAN に割り当てられます (構成されている場合)。

各設定項目の説明:



図 32: IEEE 802.1X 構成

[Enable]: インターフェイスの 802.1X 認証をオンに切り替えます。

[EAP Type] (拡張可能認証プロトコル):

- PEAP (Protected EAP) – セキュアな TLS トンネルでのユーザー名/パスワード (最も一般的)
- EAP-TLS – 証明書ベースの認証 (セキュリティが最も強い)
- EAP-TTLS – PEAP に似ているが柔軟性が高い

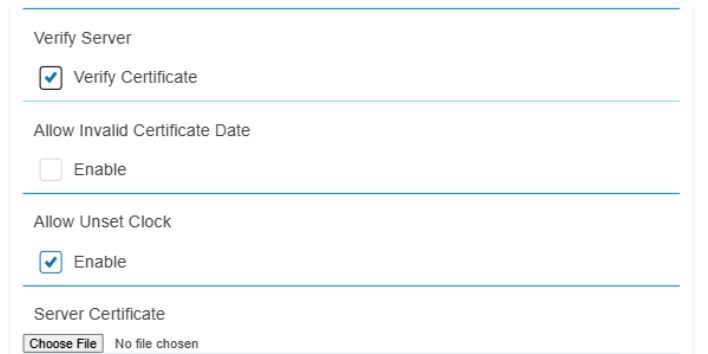
[Verify Certificate]

有効にした場合、EL2P は RADIUS サーバーの ID を、その証明書を使用して検証します。

次のときに有効にします。

- 信頼された商用の証明書、または内部の PKI 証明書を使用しているとき
- 偽装認証サーバーから最大限に保護する必要があるとき

[Verify Certificate] が有効なとき、追加の設定がダイアログに表示されます。



Verify Server

☒ Verify Certificate

Allow Invalid Certificate Date

☐ Enable

Allow Unset Clock

☒ Enable

Server Certificate

No file chosen

図 33: IEEE 802.1X 検証オプション

[Allow Invalid Certificate Date]: 期限が切れたサーバー証明書を許可します。

[Allow Unset Clock]: 時計が未設定であることによる検証エラーを防ぎます。EL2P RTC はアップタイムが短いいため、これを設定したままにすることを推奨します。

[Server Certificate]: 認証サーバー用に自己署名証明書または証明書チェーンをアップロードします。

[User Name]: RADIUS サーバーでの認証に使用される 802.1X の ID。

[Password/Confirm Password]: PEAP 認証に使用される共有シークレット。

EL2P で IEEE 802.1X を構成する

EL2P での IEEE 802.1X の実装

前提条件

EL2P で IEEE 802.1X を有効にする前に、接続されているネットワークインフラストラクチャが 802.1X 認証をサポートしていることを確認します。これには、802.1X 用に構成されたスイッチポートと、EL2P デバイス用の有効な認証情報または証明書が登録された RADIUS 認証サーバーが含まれます。

EL2P 上で認証を有効にするには:

- 適切なインターフェイスの IEEE 802.1X 構成画面を開きます
- 802.1X 機能をオンにするために [Enable] を選択します
- 必要な EAP タイプを選びます (PEAP など)
- 証明書の確認がネットワークによって必要な場合、[Verify Certificate] を有効にします
- 割り当てられたユーザー名を入力します
- 関連付けられたパスワードを入力し、[Confirm IEEE 802.1X Password] にもう一度入力します
- 設定内容を適用するには [Save] を選択します

保存後すぐにデバイスは認証を開始します。

ネットワーク側の要件

正常に動作させるには、ネットワーク側での適切な構成が必要です。スイッチポートが 802.1X モードで動作していること、および EL2P に設定された認証情報による接続を許可するよう、RADIUS サーバーに認証ポリシーが設定されていることを確認します。証明書の確認が使用される場合、必要な証明書を RADIUS サーバーと EL2P の両方に正しくインストールする必要があります。

確認

構成した後、RADIUS サーバーのログを確認するか、スイッチポートの認証ステータスを確認することによって、認証が成功したか確認します。認証されたら、EL2P は正常なネットワークアクセスが許可されます。

ユニット情報

ユニット情報を使用して、システム内の個々の PDU と、データセンター内での場所を識別できます。システム管理情報を構成するには、歯車アイコンの下にある [Unit Information] を選択します。

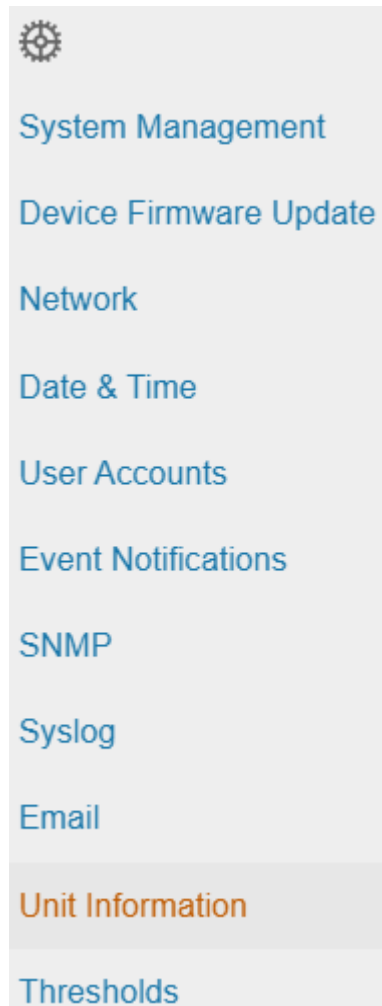


図 34: ユニット情報

画面の右側にあるドロップダウンメニューを使用して、構成するデ이지ーチェーンの中から PDU を選択します。PDU がスタンドアロンモードで構成されている場合、ドロップダウンメニューは表示されません。

Unit Information			Primary (1) ▾
Unit Information ✎	Rack Location ✎	Power Panel & Core Location ✎	
Unit Name	Room Name	Power Panel Name	
	Row Name	Core Location	
	Row Position	Core U Position	
	Rack Name		
	Rack ID		
	Rack Height		

ユニット情報

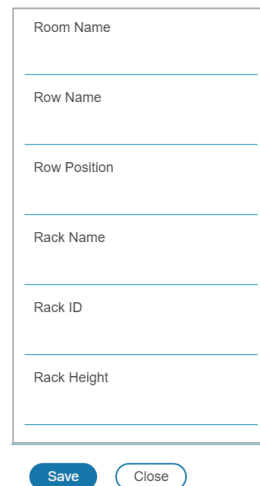
[Unit Information] タブの [Unit Name] は、特定の PDU の名前を識別します。

ラックの場所

ラックの場所は、PDU システムが存在するラックまたはキャビネットの物理的な場所を示します。システム情報を設定するには、以下の手順に従ってください。

1. [Rack Location] の横にある鉛筆アイコンを選択します。

Rack Location

A diagram of the 'Rack Location' form. It consists of a vertical container with six text input fields, each with a label above it: 'Room Name', 'Row Name', 'Row Position', 'Rack Name', 'Rack ID', and 'Rack Height'. Below the input fields are two buttons: a blue 'Save' button and a white 'Close' button with a blue border.

Room Name
Row Name
Row Position
Rack Name
Rack ID
Rack Height

Save Close

図 35: ラックの場所の構成

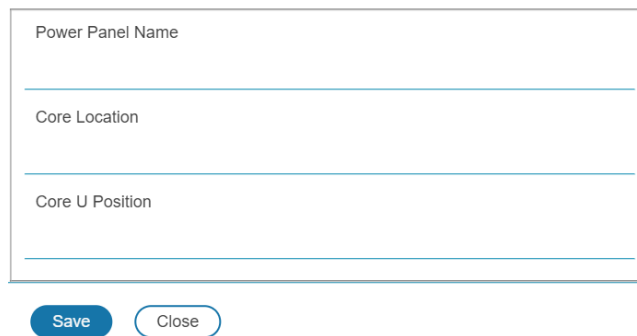
2. PDU が格納されているラックまたはキャビネットの部屋の名前を [Room Name] に入力します。
3. PDU がある列の名前を [Row Name] に入力します。
4. PDU が置かれている列の位置を [Row Position] に入力します。
5. PDU があるラックまたはキャビネットの ID を [Rack ID] に入力します。
6. PDU があるラックまたはキャビネットの高さを [Rack Height] に入力します。
7. [Save] を選択します。

電源パネルとコアの場所

[Power Panel & Core Location] には、各 PDU を接続する電源が記述されます。また、ラックまたはキャビネット内の PDU の場所も示します。構成するには、以下の手順に従ってください。

1. [Power Panel & Core Location] の横にある鉛筆アイコンを選択します。

Power Panel & Core Location



Power Panel Name

Core Location

Core U Position

Save Close

図 36: 電源パネルとコアの場所

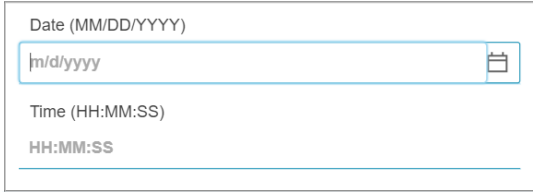
2. 電源の名前を [Power Panel Name] に入力します。
3. [Core Location] で [Front] または [Back] を選択します。[Core Location] は PDU がラックまたはキャビネットのどちら側に設置されるかを指します。縦型 PDU の場合、通常は背面 (Back) に設置されます。
4. ラックユニット (RU) の場所を [Core U Position] に入力します。縦型 PDU は、たいてい 0 RU スペースに設置されます。
5. [Save] を選択します。

NMC の時刻と日付を設定する

内部の時計は手動で設定することも、ネットワークタイムプロトコル (NTP) サーバーにリンクして日付と時刻を設定することもできます。

時刻と日付を手動で設定する

1. [Time & Date] > [Date/Time Configuration] へ進みます。



The image shows a 'Date/Time Configuration' dialog box. It has a title bar with the text 'Date/Time Configuration'. Inside the dialog, there are two main sections. The first section is labeled 'Date (MM/DD/YYYY)' and contains a text input field with the placeholder 'm/d/yyyy' and a calendar icon on the right. The second section is labeled 'Time (HH:MM:SS)' and contains a text input field with the placeholder 'HH:MM:SS'. At the bottom of the dialog, there are two buttons: 'Save' and 'Close'.

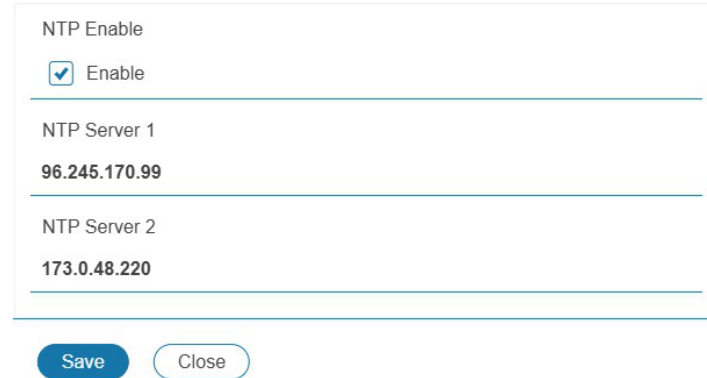
図 37: 日付と時刻を設定する

2. MM-DD-YYYY 形式を使用して日付を入力するか、カレンダーアイコンを使用して日付を選択します。
3. 表示されている 3 つのフィールドに時刻を入力します。最初のフィールドに時、次のフィールドに分、3 つ目のフィールドに秒を入力します。時間は 24 時制の形式で測定されます。例えば、1:00pm の場合は 13、2:00pm の場合は 14 です。
4. [Save] を選択します。

ネットワークタイムプロトコルを構成する

1. [Time & Date] > [Network Time Protocol (NTP)] へ進みます。

Network Time Protocol(NTP)



NTP Enable
☒ Enable

NTP Server 1
96.245.170.99

NTP Server 2
173.0.48.220

Save Close

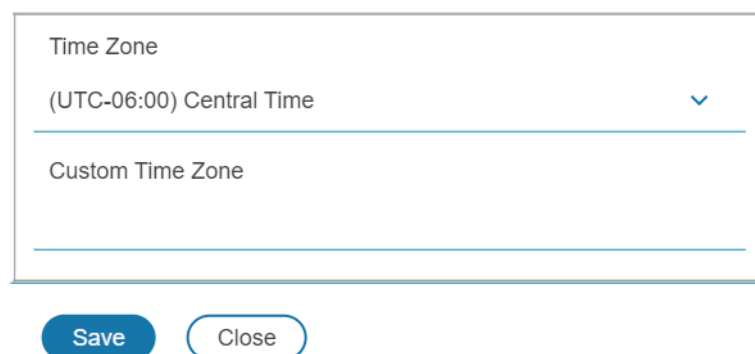
図 38: NTP 構成

2. [Enable] をクリックして NTP を有効にします。
3. プライマリ NTP サーバーのホスト名または IP アドレスを [Primary NTP Server] フィールドに入力します。
4. セカンダリ NTP サーバーのホスト名または IP アドレスを [Secondary NTP Server] フィールドに入力します。
5. [Save] を選択します。

タイムゾーン構成

1. [Time & Date] > [Time Zone Configuration] へ進みます。

Time Zone Configuration



Time Zone
(UTC-06:00) Central Time ▼

Custom Time Zone

Save Close

図 39: 夏時間のタイムゾーン構成

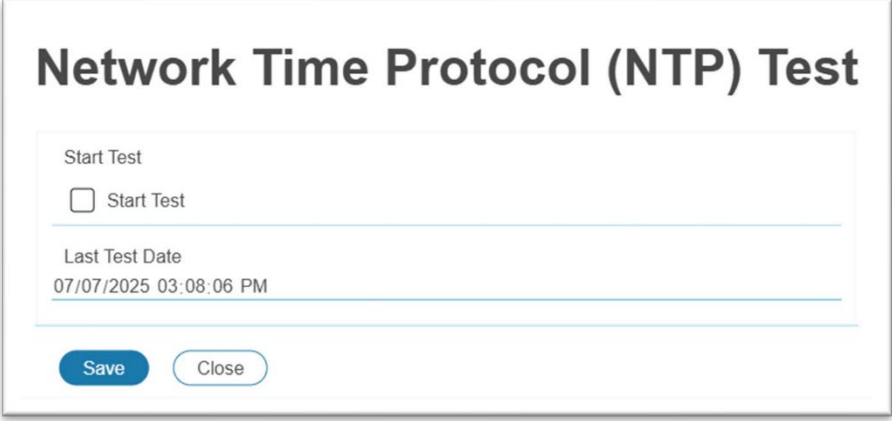
2. プルダウンメニューから事前定義されたタイムゾーンを選択します。
3. 目的のタイムゾーンがプルダウンメニューにない場合、IANA タイムゾーンデータベース (<https://www.iana.org/time-zones>) の TZ 識別子を [Custom Time Zone] に入力します。

タイムゾーンの一覧は、https://en.wikipedia.org/wiki/List_of_tz_database_time_zones にもあります。

ネットワークタイムプロトコル (NTP) テスト

ネットワークタイムプロトコルテストでは、NTP サーバーへの接続を確認できます。接続を確認するには、以下の手順に従ってください。

1. [Network Time Protocol (NTP) Test] の横にある鉛筆をクリックします。
2. [Start Test] を選択して [Save] をクリックします。



Network Time Protocol (NTP) Test

Start Test

☐ Start Test

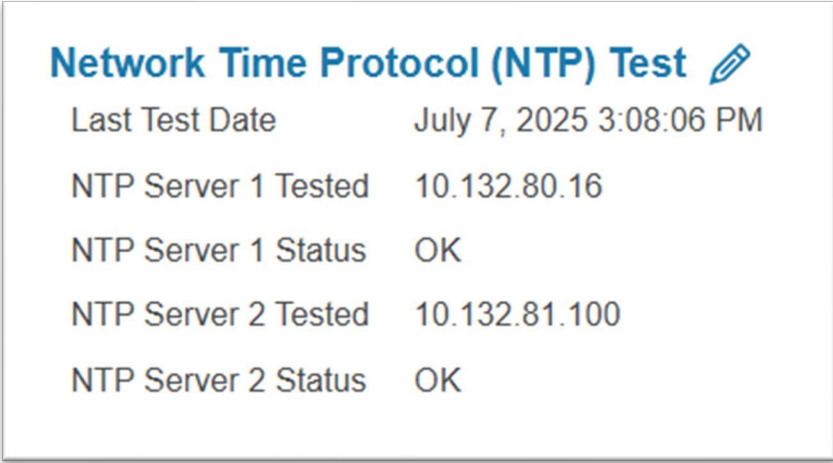
Last Test Date

07/07/2025 03:08:06 PM

Save Close

図 40: NTP テストを開始する

3. テストが完了するまで待ちます。
4. [Network Time Protocol (NTP) Test] セクションの下にステータスが表示されます。



Network Time Protocol (NTP) Test 

Last Test Date	July 7, 2025 3:08:06 PM
NTP Server 1 Tested	10.132.80.16
NTP Server 1 Status	OK
NTP Server 2 Tested	10.132.81.100
NTP Server 2 Status	OK

図 41: NTP テストのステータス

制御と管理

Web GUI の [Control and Manage] セクションでは、ユーザーは PDU の機能に基づいて操作を実行できます。アウトレットを制御したり、PDU エネルギーメーターやアウトレットごとのエネルギーメーターをリセットしたりできます。PDU の EL2P シリーズでは、アウトレットのシーケンス機能が導入されました。この機能により、ユーザーはアウトレットの電源を投入するシーケンス順序を制御できます。

制御と管理セクションにアクセスするには、ホームアイコンから [Control & Manage] を選択します。

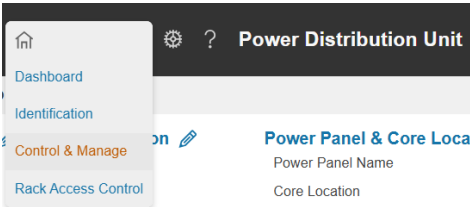


図 42: 制御と管理

Control & Manage												Actions	Primary (1)
		Outlet Control			PDU Energy			Outlet Energy					
Outlet Name	Breaker	Current (A)	Status	Power Control	On Delay (s)	Off Delay (s)	Reboot Duration (s)	State on Startup	Sequence On Delay (s)	Sequence Number			
OUTLET 1	B1	0			1	1	5		1	1			
OUTLET 2	B1	0			1	1	5		1	2			
OUTLET 3	B1	0			1	1	5		1	3			
OUTLET 4	B1	0			1	1	5		1	4			
OUTLET 5	B1	0			1	1	5		1	5			

図 43: 制御と管理のデフォルトのページ表示

アウトレット電力管理

アウトレット LED

アウトレット LED は、アウトレットに AC 電源が存在するかどうかではなく、内部 PCB でのリレーの DC コイルのステータスを示します。LED がオン (緑色) の場合、リレーコイルに通電されており、制御回路 (PDU の電源およびファームウェアの制御経路) が正常に動作し、アウトレットをオンにする制御が行われていることを示します。LED がオフの場合、リレーコイルは通電されておらず、アウトレットをオフにする制御が行われています。

【重要】サーキットブレーカーが (手動操作または過負荷が原因で) 作動した場合、リレーコイルは DC 電源によって通電されているため、アウトレット LED がオンのままになることがあります。これは、LED が下流側の線間電圧ではなく、制御経路の正常性と制御状態に基づいて点灯するためです。
この設計により、ブレーカー作動の誤検知によってファームウェアがアウトレットをオフに設定してしまうことを防ぎ、意図しないサービス停止を回避できます。

LED の意味と解説:

- 制御状態: PDU がアウトレットをオン (コイル通電)、またはオフ (コイル非通電) のどちらの状態でも制御しているか
- 制御経路の正常性: PDU の低電圧 DC 電源とリレードライバーが正常に動作しているか
- 含まれない情報: アウトレットに AC 電源が供給されているか (たとえば、ブレーカーの作動や上流側の電源喪失によりアウトレットが無電圧状態になっていても、LED はオンのままになることがある)

アウトレットステータス

アウトレットレベルの制御機能を備えた Panduit PDU では、Web インターフェイスのアウトレットの [Status] はアウトレットの状態を表します。

【注意】ユーザーは、制御する PDU をドロップダウンメニューから選択する必要があります (図 37 を参照)。



オン: アウトレットがオンです



オフ: アウトレットがオフです

アウトレットの名前指定

アウトレットレベルの制御またはモニタリング機能を備えた Panduit PDU では、各アウトレットをカスタマイズし、Web GUI を使用してすべてのサーキットブレーカーとアウトレットの関連性を表示することができます。

1. 制御と管理ページで、[Outlet Control] タブを展開します。
2. 名前を付けるアウトレットと同じ行にある鉛筆アイコンをクリックして、[Outlet Configuration] ダイアログを開きます。
3. ダイアログで、[Outlet Name] の値フィールドを選択します。
4. デフォルトの名前を削除し、新しい名前を入力します。
5. [Enter] を押します。

Outlet Configuration

Outlet Name	OUTLET 1
Breaker	B1
Current (A)	0
Status	1
On Delay (s)	1
Off Delay (s)	1
Reboot Duration (s)	5
State on Startup	On
Sequence On Delay (s)	1
Sequence Number	1

Save Close

図 44: アウトレットの名前指定、時間遅延、始動時の状態、再起動

【注意】 [Status] が 1 の場合、アウトレット遅延はオンです。 [Status] が 0 の場合、アウトレット遅延はオフです。

アウトレットのデフォルト状態を設定する

アウトレットレベルの制御を備えた Panduit PDU でアウトレットのデフォルト状態を設定すると、ユーザーは PDU 起動時の個々のアウトレットの初期電力状態を決定できます。

1. [Control & Manage] タブから [Outlet Control] タブを展開します。
2. [Outlet Configuration] ダイアログの [State on Startup] ドロップダウンメニューから選択項目を選択します。
 - [On]: 最初の始動時にアウトレットをオンにします
 - [Off]: 最初の始動時にアウトレットをオフにします
 - [Last Known]: デバイスの電源を切る前の最後の電力状態にアウトレットを戻します

アウトレットのオン/オフを切り替える

これはアウトレット切り替え式の PDU のみに該当します。

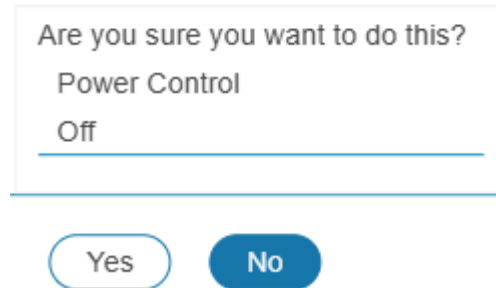
- Panduit PDU の切り替え式 PDU モデルのアウトレットでは、オン/オフの切り替えや電源の入れ直しを簡単に行えます。この操作を行うには、ユーザーが管理者権限を持っている必要があります。
 - アウトレットの PDU ブレーカーがオフになっているか、NMC がパワーシェア状態の場合、アウトレット名およびブレーカーのテキストは取り消し線付きの灰色で表示され、アウトレットがアクティブでないことを示します。
1. ホームアイコンから [Control & Manage] メニュー項目を選択します。
 2. [Power Control] 列で、オン/オフを切り替えたり再起動したりする必要のあるアウトレットのボタンをクリックします。
 3. ドロップダウンメニューから目的の電力制御を選択します。
 - a. [Cancel] は遅延された動作を停止し、現在のアウトレット状態を維持します。
 - b. [Off] はアウトレットの電源をただちにオフにします。
 - c. [Off Delayed] はアウトレットの [Off Delay (s)] 秒だけ待ってから、アウトレットの電源をオフにします。
 - d. [Reboot Delayed] はアウトレットの電源をただちにオフにし、[Reboot Delay(s)] 秒だけ待ってから、アウトレットの電源をオンにします。
 - e. [Reboot Immediately] はアウトレットの電源をただちにオフにし、約 0.5 秒待ってから、アウトレットの電源をオンにします。
 - f. [On] はアウトレットの電源をただちにオンにします。
 - g. [On Delayed] はアウトレットの [On Delay (s)] 秒だけ待ってから、アウトレットの電源をオンにします。

Outlet Name	Breaker	Current (A)	Status	Power Control	On Delay (s)
OUTLET 1	B1	0	🔌	🔌	
OUTLET 2	B1	0	🔌	🛑 Cancel	
OUTLET 3	B1	0	🔌	🛑 Off	
OUTLET 4	B1	0	🔌	🛑 Off Delayed	
OUTLET 5	B1	0	🔌	🔄 Reboot Delayed	
OUTLET 6	B1	0	🔌	🔄 Reboot Immediately	
				🔌 On	
				🔄 On Delayed	

図 45: アウトレットの制御

4. 確認ダイアログが表示されます。

Confirmation



A confirmation dialog box with a light gray border. Inside, the text 'Are you sure you want to do this?' is at the top. Below it, 'Power Control' is displayed, followed by 'Off' which is underlined. At the bottom, there are two buttons: 'Yes' (light blue) and 'No' (dark blue).

図 46: アウトレットの制御

変更内容を適用するには [Yes] を選択します。変更内容を適用しない場合は [No] を選択します。

Panduit PDU のアウトレット電源オン/オフ/再起動の遅延を設定する

これはアウトレット切り替え式の PDU のみに該当します。

1. ホームアイコンを選択し、Web UI のドロップダウンメニューから [Control & Manage] を選択します。
2. 鉛筆アイコンをクリックして、遅延を設定するアウトレットを選択します。
3. 遅延の長さを構成します。遅延設定については、アウトレットのオン/オフを切り替えるのセクションに記載されています。
【注意】遅延を 0 秒に設定すると、遅延は要求された操作をシステムが処理できる速さとほぼ同じになります。
4. [Save] を選択します。

アウトレットの制御の有効化/無効化

アウトレットの制御の有効化/無効化機能では、すべてのユーザーインターフェイスからすべてのアウトレットの電力制御状態を変更することを許可または禁止できます。注意: [Power On State] は、引き続き適切に適用されます。

1. ホームアイコンを選択し、Web UI のドロップダウンメニューから [Control & Manage] を選択します。
2. [Actions] メニューから [Outlet Control] メニューを選択します。

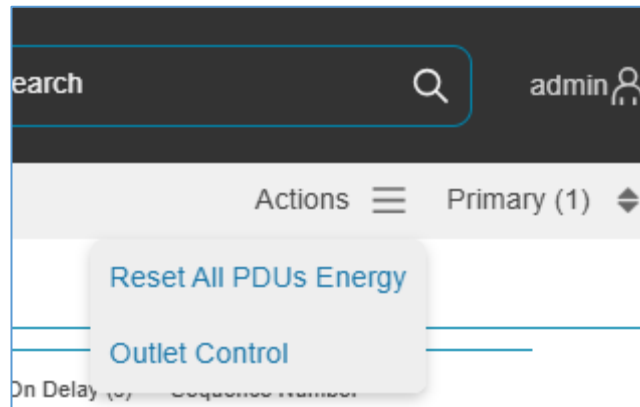


図 47: [Outlet Control] メニュー項目

3. アウトレットの制御の有効化/無効化の状態を選択します。

Outlet Control

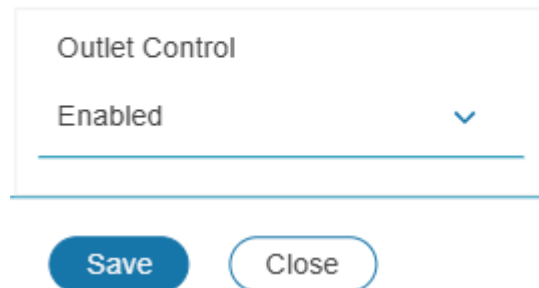
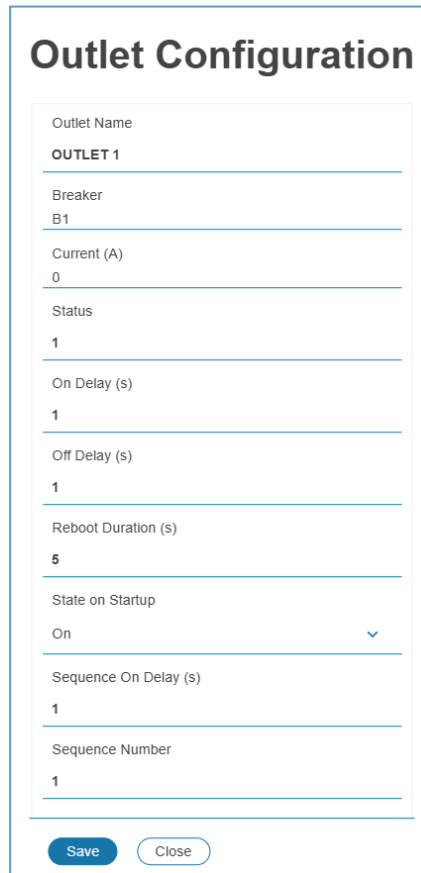


図 48: アウトレットの制御の有効化/無効化ダイアログ

4. 変更内容を適用するには [Save] を選択します。

3. アウトレットの編集ウィンドウで、[Sequence On-Delay (s)] の時間 (0~7200 秒) を入力してから、[Save] を選択します。
 - a. 【注意】遅延を 0 秒に設定すると、遅延は要求された操作をシステムが処理できる速さとほぼ同じになります。



The screenshot shows the 'Outlet Configuration' window. It contains several input fields for configuring an outlet. The 'Sequence On Delay (s)' field is highlighted, showing a value of '1'. Other fields include 'Outlet Name' (OUTLET 1), 'Breaker' (B1), 'Current (A)' (0), 'Status' (1), 'On Delay (s)' (1), 'Off Delay (s)' (1), 'Reboot Duration (s)' (5), 'State on Startup' (On), and 'Sequence Number' (1). At the bottom, there are 'Save' and 'Close' buttons.

Field	Value
Outlet Name	OUTLET 1
Breaker	B1
Current (A)	0
Status	1
On Delay (s)	1
Off Delay (s)	1
Reboot Duration (s)	5
State on Startup	On
Sequence On Delay (s)	1
Sequence Number	1

図 51: シーケンスオン遅延時間

4. アウトレットパワーシーケンスが設定されました。EL2P PDU では、単純にシーケンスオン遅延とシーケンス番号を一緒に設定することもできます。

Control & Manage

Actions

Primary (1)

Outlet Name	Breaker	Current (A)	Status	Outlet Control	PDU Energy	Outlet Energy	Sequence On Delay (s)	Sequence Number			
				Power Control	On Delay (s)	Off Delay (s)				Reboot Duration (s)	State on Startup
OUTLET 1	B1	0			1	1	5		1	1	
OUTLET 2	B1	0			1	1	5		1	2	
OUTLET 3	B1	0			1	1	5		1	3	
OUTLET 4	B1	0			1	1	5		1	4	
OUTLET 5	B1	0			1	1	5		1	1	
OUTLET 6	B1	0			1	1	5		1	1	

図 52: 保存されたシーケンス

この図では、電源が復元されるとき、アウトレットは1、5、6、2、3、4 の順に 1 秒ごとにオンになります。

すべての PDU エネルギーをリセットする

エネルギー監視機能が付いた PDU では、エネルギーメーターが最後にリセットされたときからのエネルギーの累積値を保持しています。リセット可能なすべての PDU エネルギーメーターは同時にリセットできます。これには入力およびアウトレットごとのライフタイムエネルギーメーターが含まれます。

1. ホームアイコンを選択し、Web UI のドロップダウンメニューから [Control & Manage] を選択します。
2. [Actions] メニューから [Outlet Control] メニュー項目を選択します。

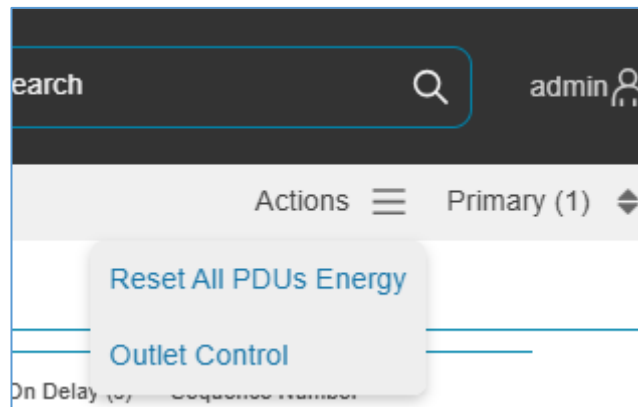


図 53: [Reset All PDUs Energy] メニュー項目

3. すべての PDU エネルギーをリセットするには [Yes] を選択します。

Reset All PDUs Energy

Are you sure you want to do this?

図 54: [Reset All PDUs Energy] ダイアログ

4. [Yes] を選択した場合、[Energy Since] は現在の日時に設定され、関連付けられたライフタイムエネルギーの測定値はゼロにリセットされます。

PDU エネルギー

入力エネルギー監視機能が付いた PDU では、[Energy Since] の日時から累積されたライフタイムエネルギーが表示されます。

1. ホームアイコンを選択し、Web UI のドロップダウンメニューから [Control & Manage] を選択します。
2. [PDU Energy] タブを選択します。

Control & Manage			Actions	Primary (1)
Outlet Control <u>PDU Energy</u> Outlet Energy				
Energy (kWh)	Energy Since	Lifetime Energy (kWh)		
0	February 2, 2025 11:55:47 AM	0		

図 55: PDU エネルギー

PDU エネルギーメーターをリセットする

個々の PDU エネルギーモニターをリセットできます。

1. エネルギーメーターの横にある鉛筆アイコンを選択して、[PDU Energy Configuration] ダイアログを表示します。

PDU Energy Configuration

Energy (kWh)

0

Reset Energy

☒

Save

Close

図 56: PDU エネルギー構成

2. [Reset Energy] の下にあるチェックボックスを選択します。
 - a. そのメーターのライフタイムエネルギー測定値をリセットするには [Save] を選択します。
 - b. 変更を適用しない場合は [Close] を選択します。

アウトレットのエネルギー

アウトレットごとのエネルギー監視機能が付いた PDU では、アウトレットごとに [Energy Since] の日時から累積されたライフタイムエネルギーが表示されます。すべてのアウトレットのエネルギーメーターをリセットできます。

- 1. ホームアイコンを選択し、Web UI のドロップダウンメニューから [Control & Manage] を選択します。
- 2. [Outlet Energy] タブを選択します。

Control & Manage							Actions	Primary (1)
		Outlet Control	PDU Energy	Outlet Energy				
Outlet Name	Breaker	Energy (kWh)	Energy Since	Lifetime Energy (kWh)				
OUTLET 1	B1	0	February 2, 2025 11:55:47 AM	0				
OUTLET 2	B1	0	February 2, 2025 11:55:47 AM	0				
OUTLET 3	B1	0	February 2, 2025 11:55:47 AM	0				
OUTLET 4	B1	0	February 2, 2025 11:55:47 AM	0				
OUTLET 5	B1	0	February 2, 2025 11:55:47 AM	0				

図 57: アウトレットのエネルギー

PDU のすべてのアウトレットのエネルギーメーターをリセットする

1. [Lifetime Energy (kWh)] の横にある鉛筆アイコンを選択して、複数の [Outlet Energy Configuration] ダイアログを表示します。

Outlet Energy Configuration

Warning: Clicking Save applies the Reset Energy option to all selected items.

Outlet Name	Energy (kWh)	Reset Energy
		☐
OUTLET 1	0	☐
OUTLET 2	0	☐
OUTLET 3	0	☐
OUTLET 4	0	☐
OUTLET 5	0	☐
OUTLET 6	0	☐

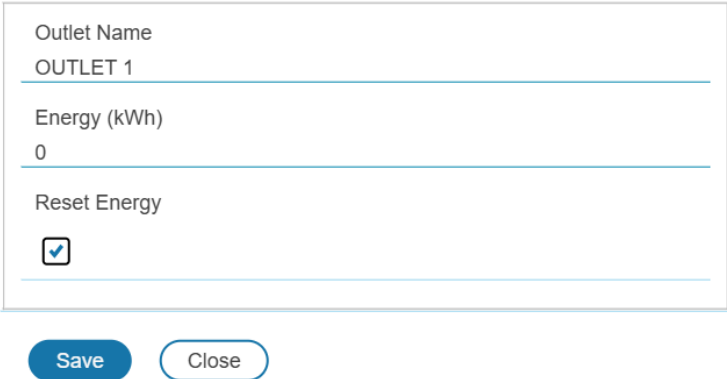
図 58: 複数の [Outlet Energy Configuration] ダイアログ

2. 同時にリセットする個々のアウトレットの横にあるチェックボックスを選択します。または、[Reset Energy] の下にある [-] チェックボックスをクリックして、すべてのアウトレットをすばやく選択したり、すべてのアウトレットが選択されている場合にその選択を解除したりすることができます。
 - a. 変更内容を適用するには [Save] を選択します。
 - b. 変更を適用しない場合は [Close] を選択します。

1 つのアウトレットのエネルギーメーターをリセットする

1. 各アウトレット行の鉛筆アイコンを選択して、アウトレットごとの [Outlet Energy Configuration] ダイアログを表示します。

Outlet Energy Configuration



Outlet Name
OUTLET 1
Energy (kWh)
0
Reset Energy
☒

Save Close

図 59: アウトレットのエネルギー構成

2. [Reset Energy] の下にあるチェックボックスを選択します。
 - a. そのアウトレットのライフタイムエネルギー測定値をリセットするには [Save] を選択します。
 - b. 変更を適用しない場合は [Close] を選択します。

計測の閾値を設定する

閾値の構成は、歯車メニューの [Thresholds] を選択して見つけることができます。

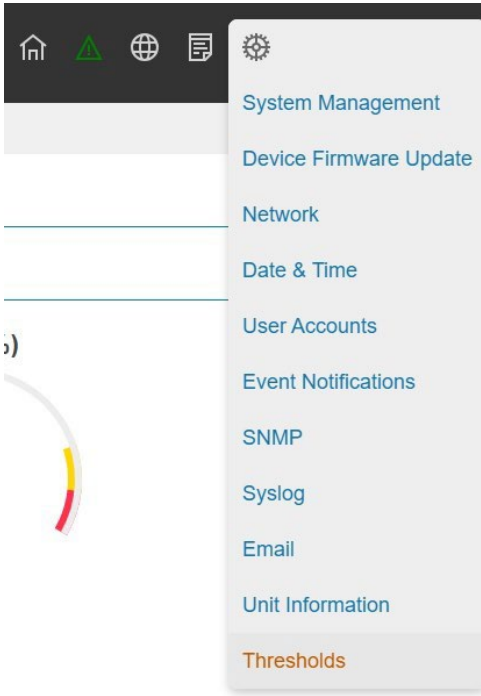


図 60: 閾値の設定

閾値は個々の PDU ごとに設定されます。初期値はその特定モデルの PDU の特性に基づいています。

閾値構成を表示したとき、無効化されている閾値はグレーで表示され、取り消し線が付いています。

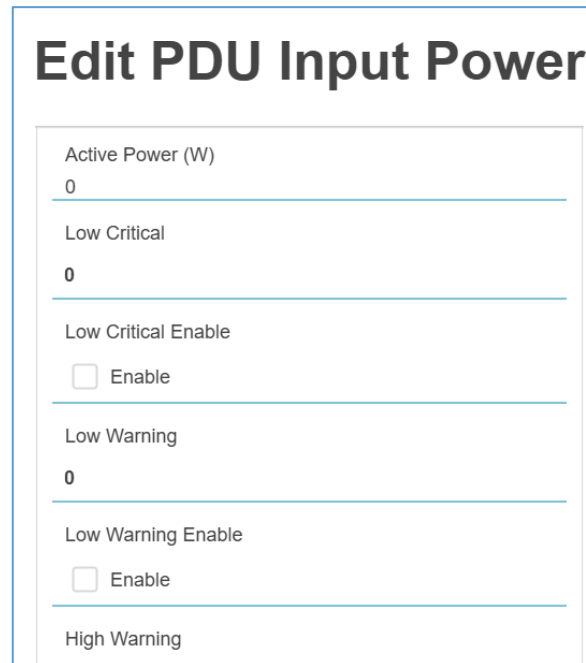
Thresholds							Primary (1) ▾
Input							
Phase							
Phase Power							
Circuit Breaker							
Outlet							
Sensors							
Current							
Phase	Current (A)	Low Critical	Low Warning	High Warning	High Critical		
1	0	0	0	21	24		
2	0	0	0	21	24		
3	0	0	0	21	24		

図 61: 閾値の構成

電力閾値

PANDUIT PDU は、電力閾値のワット数が電力閾値の構成で指定した設定を上回ったり下回ったりすると、アラート通知を送信します。

1. [Thresholds] > [Input Page] へ進みます。
2. 電力閾値の鉛筆をクリックして更新します。



Edit PDU Input Power

Active Power (W)	0
Low Critical	0
Low Critical Enable	☐ Enable
Low Warning	0
Low Warning Enable	☐ Enable
High Warning	

図 62: 電力閾値

3. 適切な閾値を選択してアンペアで入力し、[Save] をクリックします。
 - 下方臨界 (W)
 - 下方警報 (W)
 - 上方警報 (W)
 - 上方臨界 (W)

4. すべての PDU に対して手順 1 ～ 3 を繰り返します。

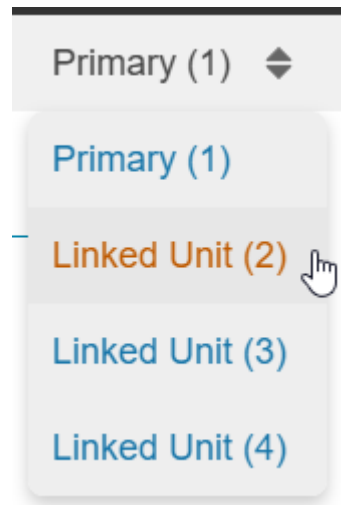


図 63: プライマリまたはリンク PDU を選択する

相電流アラーム閾値

PANDUIT PDU は、相電流アラームのアンペアが相電流アラームの構成で指定した設定を上回ったり下回ったりすると、アラート通知を送信します。

1. [Thresholds] > [Phase Page] へ進みます。
2. 相電流アラームの鉛筆をクリックして更新します。

Edit Current

Phase	1
Current (A)	0
Low Critical	0
Low Critical Enable	☐ Enable
Low Warning	0
Low Warning Enable	☐ Enable

図 64: 相電流アラーム

3. 適切な閾値を選択してアンペアで入力し、[Save] をクリックします。
 - 下方臨界 (A)
 - 下方警報 (A)
 - 上方警報 (A)
 - 上方臨界 (A)
4. すべての相およびすべての PDU に対して手順 1 ~ 3 を繰り返します。

電圧アラーム閾値

PANDUIT PDU は、相電圧が相電圧アラームの構成で指定した設定を上回ったり下回ったりすると、アラート通知を送信します。

1. [Thresholds] > [Phase Page] へ進みます。
2. 相電圧の鉛筆をクリックして更新します。

Input phases voltage alarm setting	
Low Critical (V)	180
Enable Low Critical	☒
Low Warning (V)	190
Enable Low Warning	☒
High Warning (V)	250
Enable High Warning	☒
High Critical (V)	260
Enable High Critical	☒
Reset Threshold (V)	2
Alarm State Change Delay	0
<button>Save</button>	

図 65: 相電圧アラーム

3. 適切な閾値を選択してボルト数で入力し、[Save] をクリックします。

下方臨界 (V)

下方警報 (V)

上方警報 (V)

上方臨界 (V)

リセット閾値 (V)

リセット閾値は、条件をクリアするために閾値設定を下回っていない測定値のワット数です。例えば、入力位相の電流の臨界閾値が 19 ボルト (V) に設定されているとします。電流の引き込みが 20V まで上昇すると、電流の重大アラートがトリガーされます。その後、電流は 18.1V から 20V の間で変動を続けます。リセット閾値を 1V に設定すると、PDU は入力位相の電流が臨界を上回っていることを引き続き示します。リセット閾値を指定しない (つまり、リセット閾値をゼロに設定する) と、PDU は電流が 18.9V まで下がるたびに状況をアサート停止し、19V 以上に達するたびに状況を再アサートします。電流が変動している場合は、これにより SNMP トラップ、SMTP アラート、Syslog 通知などのイベント通知が繰り返し発生することがあります。

アラーム状態変更の遅延 (サンプル)

有効にすると、PDU は、閾値を越えるサンプルが連続して指定の数まで生成された後でのみ、警報または臨界状況をアサートします。これにより、上限閾値を上回ったり下限閾値を下回ったりした直後に測定値が正常に戻る場合は、閾値アラートが生成されないことがあります。

4. すべての相に対して手順 1 ~ 3 を繰り返します。

サーキットブレーカーアラーム閾値

PANDUIT PDU は、サーキットブレーカーのアンペアがサーキットブレーカーアラームの構成で指定した設定を上回ったり下回ったりすると、アラート通知を送信します。

1. [Thresholds] > [Circuit Breaker Page] へ進みます。
2. サーキットブレーカーの鉛筆をクリックして更新します。

Load Segment Breaker

Low Critical (A)	0
Enable Low Critical	☐
Low Warning (A)	0
Enable Low Warning	☐
High Warning (A)	14
Enable High Warning	☒
High Critical (A)	16
Enable High Critical	☒
Reset Threshold (A)	1
Alarm State Change Delay	0

Save

図 66: ロードセグメントブレーカー

3. 適切な閾値を選択してアンペアで入力し、[Save] をクリックします。

下方臨界 (A)

下方警報 (A)

上方警報 (A)

上方臨界 (A)

リセット閾値 (A)

リセット閾値は、条件をクリアするために閾値設定を下回っていない測定値のワット数です。例えば、入力位相の電流の臨界閾値が 19 アンペア (A) に設定されているとします。電流の引き込みが 20A まで上昇すると、電流の重大アラートがトリガーされます。その後、電流は 18.1A から 20A の間で変動を続けます。リセット閾値を 1A に設定すると、PDU は入力位相の電流が臨界を上回っていることを引き続き示します。リセット閾値を指定しない (つまり、リセット閾値をゼロに設定する) と、PDU は電流が 18.9A まで下がるたびに状況をアサート停止し、19A 以上に達するたびに状況を再アサートします。電流が変動している場合は、これにより SNMP トラップ、SMTP アラート、Syslog 通知などのイベント通知が繰り返し発生することがあります。

アラーム状態変更の遅延 (サンプル)

有効にすると、PDU は、閾値を越えるサンプルが連続して指定の数まで生成された後でのみ、警報または臨界状況をアサートします。これにより、上限閾値を上回ったり下限閾値を下回ったりした直後に測定値が正常に戻る場合は、閾値アラートが生成されないことがあります。

すべてのサーキットブレーカーに対して手順 1 ~ 3 を繰り返します。

アウトレットアラーム閾値

PANDUIT PDU は、アウトレットのワット数がアウトレットアラームの構成で指定した設定を上回ったり下回ったりすると、アラート通知を送信します。

1. [Thresholds] > [Outlet Page] へ進みます。
2. アウトレットの鉛筆をクリックして更新します。

Outlet Information

Low Critical (W)	0
Set Lower Critical	☐
Low Warning (W)	0
Set Lower Warning	☐
High Warning (W)	30
Set High Warning	☒
High Critical (W)	45
Set High Critical	☒
Reset Threshold (W)	0
Alarm State Change Delay	0

Save

図 67: アウトレット情報

3. 適切な閾値を選択してワットで入力してから、[Save] をクリックします。

下方臨界 (W)

下方警報 (W)

上方警報 (W)

上方臨界 (W)

リセット閾値 (W)

リセット閾値は、条件をクリアするために閾値設定を下回っていない測定値のワット数です。例えば、入力位相の電流の臨界閾値が 19 ワット (W) に設定されているとします。電流の引き込みが 20W まで上昇すると、電流の重大アラートがトリガーされます。その後、電流は 18.1W から 20W の間で変動を続けます。リセット閾値を 1A に設定すると、PDU は入力位相の電流が臨界を上回っていることを引き続き示します。リセット閾値を指定しない (つまり、リセット閾値をゼロに設定する) と、PDU は電流が 18.9W まで下がるたびに状況をアサート停止し、19W 以上に達するたびに状況を再アサートします。電流が変動している場合は、これにより SNMP トラップ、SMTP アラート、Syslog 通知などのイベント通知が繰り返し発生することがあります。

アラーム状態変更の遅延 (サンプル)

有効にすると、PDU は、閾値を越えるサンプルが連続して指定の数まで生成された後でのみ、警報または臨界状況をアサートします。これにより、上限閾値を上回ったり下限閾値を下回ったりした直後に測定値が正常に戻る場合は、閾値アラートが生成されないことがあります。

すべてのアウトレットに対して手順 1 ～ 3 を繰り返します。

Syslog セットアップ

EL2P NMC は、イベントが発生したときに syslog メッセージを syslog サーバーに送信するよう構成できます。これを行うには、Syslog サーバーに関する情報を構成する必要があります。

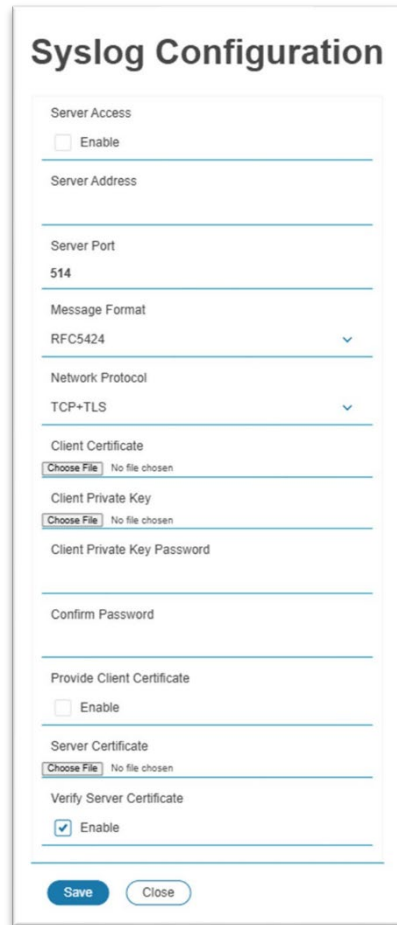
Syslog サーバー構成

1. ダッシュボードの上部リボンから、歯車設定に移動して、[Email Setup] を選択します。



図 68: メールセットアップ

2. [Syslog Configuration] の横にある鉛筆を選択して、[Edit] 画面への入力を開始します。



The image shows a 'Syslog Configuration' dialog box. It contains several fields and options: 'Server Access' with an 'Enable' checkbox; 'Server Address' text field; 'Server Port' text field with '514' entered; 'Message Format' dropdown menu with 'RFC5424' selected; 'Network Protocol' dropdown menu with 'TCP+TLS' selected; 'Client Certificate' with a 'Choose File' button and 'No file chosen' text; 'Client Private Key' with a 'Choose File' button and 'No file chosen' text; 'Client Private Key Password' text field; 'Confirm Password' text field; 'Provide Client Certificate' with an 'Enable' checkbox; 'Server Certificate' with a 'Choose File' button and 'No file chosen' text; 'Verify Server Certificate' with an 'Enable' checkbox checked. At the bottom are 'Save' and 'Close' buttons.

図 69: Syslog 構成

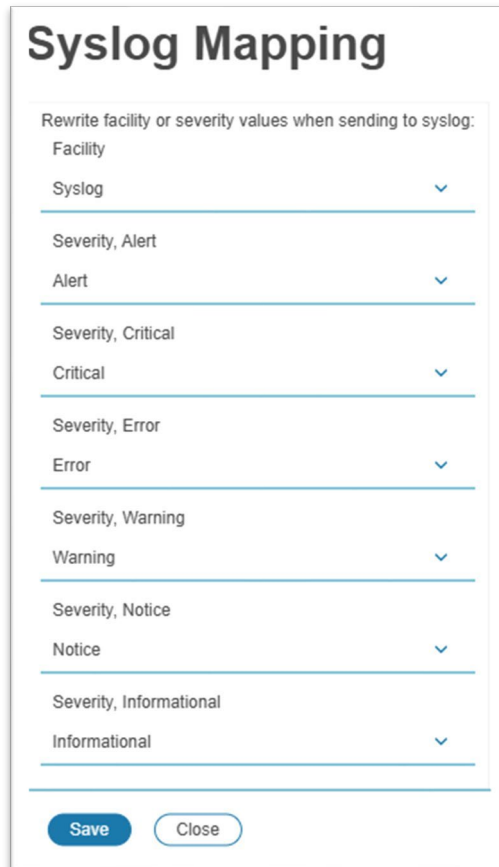
- [Server Address] を設定します。これはメッセージを受け付ける Syslog サーバーのアドレスです。
- [Message Format] を選択します。RFC3164 形式または RFC5424 形式とすることができます。
- ポート番号を構成します。ポート番号はサーバーの通信エンドポイントです。デフォルトは 514 です。そのほかの一般的な Syslog ポートは 6514 です。
- [Network Protocol] を設定します。
 - [UDP] – メッセージは UDP プロトコルを使用して送信されます。
 - [TCP] – メッセージは TCP プロトコルを使用して送信されます。
 - [TCP+TLS] メッセージは TLS で暗号化された TCP プロトコルを使用して送信されます。
- [TCP+TLS] が選択された場合、[Clients Private Key Password] または [Client Certificate] に入力できません。

3. 完了したら、[Save] を選択します。

Syslog マッピング

Syslog の [Facility] と [Severity] フィールドを別の値にマッピングして、Syslog サーバーでのトレーサビリティを容易にすることができます。フィールドを編集するには、次のようにします。

1. [Syslog Mapping] の横にある鉛筆を選択します。
2. 構成メニューのフィールドを更新します。



The image shows a 'Syslog Mapping' dialog box. At the top, it says 'Rewrite facility or severity values when sending to syslog:'. Below this, there are several rows, each with a label on the left and a dropdown menu on the right. The rows are: Facility (Syslog), Severity, Alert (Alert), Severity, Critical (Critical), Severity, Error (Error), Severity, Warning (Warning), Severity, Notice (Notice), and Severity, Informational (Informational). At the bottom of the dialog, there are two buttons: 'Save' and 'Close'.

Field	Mapping
Facility	Syslog
Severity, Alert	Alert
Severity, Critical	Critical
Severity, Error	Error
Severity, Warning	Warning
Severity, Notice	Notice
Severity, Informational	Informational

図 70: Syslog マッピング

3. 設定内容を適用するには [Save] を選択します。

メールセットアップ

Panduit NMC は、イベントが発生したときに特定のユーザーにメールを送信するように構成できます。これを行うには、SMTP (Simple Mail Transfer Protocol) サーバーに関する情報を構成する必要があります。

4. ダッシュボードの上部リボンから、歯車設定に移動して、[Email] を選択します。

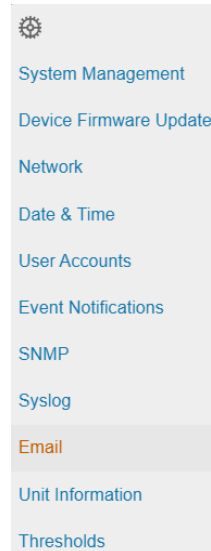


図 71: メールセットアップ

5. [SMTP Account Settings] の横にある鉛筆を選択して、[Edit] 画面への入力を開始します。

SMTP Account Settings

SMTP server

Sender email address

|

Username

Password

Confirm Password

Port

25

Number of retry attempts

3

Time interval between retry attempts (in minutes)

6

Security

None

Server requires authentication

☐ Enable

Save

Close

図 72: SMTP アカウント設定

- [SMTP server] を設定します。これはメッセージを受け付ける SMTP リレーサーバーのアドレスです。
- [Sender email address] を設定します。これはメールの送信元のメールアドレスです。PDU ごとに固有のメールアドレスを使用することも、すべての PDU について同じメールアドレスを使用することもできます。
- ポート番号を構成します。ポート番号はサーバーの通信エンドポイントです。デフォルトは 25 です。その他の一般的な SMTP ポートは 587 および 465 です。

- 送信の [Security] を設定します。
 - [None] – 接続は安全ではありません。
 - [STARTTLS] – クライアントは STARTTLS コマンドを使用して、接続を暗号化された接続にアップグレードします
 - [TLS] – クライアントはセキュア接続 (SMTPS とも言います) を確立します。
- サーバーのパスワード認証が必要かどうかを選択します。SMTP サーバーでユーザー名とパスワードが必要な場合、このオプションを選択する必要があります。
- SMTP サーバーに認証が必要な場合、ユーザー名およびパスワードを入力します。これらは SMTP サーバーの構成によって決定されます。
- 再試行回数を設定します。これは配信が失敗した場合に PDU がメッセージの再送を試行する回数です。デフォルト設定は 3 です。
- 再試行を送信する時間間隔 (分) を設定します。これは NMC が失敗したメッセージの送信を再試行する前に待機する時間 (分) です。デフォルト設定は 6 分です。

6. 完了したら、[Save] を選択します。

次に、メール受信者リストを入力します。

1. 鉛筆アイコンを選択して、メール受信者の編集画面を表示します。

Edit Email Recipient

Email Address

Enable

☐ Enable

Save Close

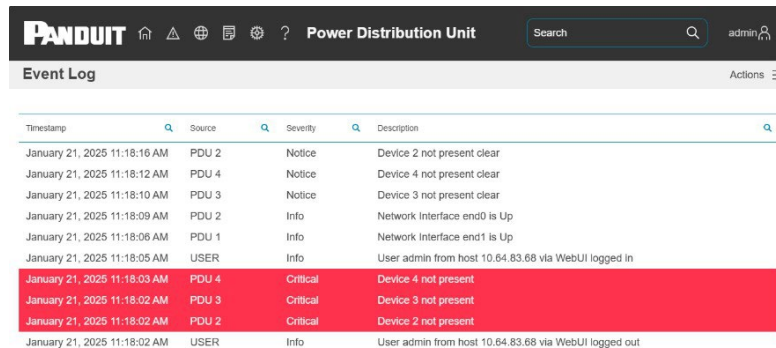
図 73: メール受信者

2. 必要なメールアドレスを入力して、[Enable] を選択します。
3. [Save] を選択します。

【注意】メールアラートを受信するユーザーは最大 5 人まで登録できます。

イベントログ

NMC イベントまたはアラームはイベントログに記録されます。これをリモートで報告するよう Syslog を構成することができます。すべての臨界イベントは赤色で強調表示されます。すべての警報イベントは黄色で強調表示されます。



Timestamp	Source	Severity	Description
January 21, 2025 11:18:16 AM	PDU 2	Notice	Device 2 not present clear
January 21, 2025 11:18:12 AM	PDU 4	Notice	Device 4 not present clear
January 21, 2025 11:18:10 AM	PDU 3	Notice	Device 3 not present clear
January 21, 2025 11:18:09 AM	PDU 2	Info	Network Interface end0 is Up
January 21, 2025 11:18:06 AM	PDU 1	Info	Network Interface end1 is Up
January 21, 2025 11:18:05 AM	USER	Info	User admin from host 10.64.83.68 via WebUI logged in
January 21, 2025 11:18:03 AM	PDU 4	Critical	Device 4 not present
January 21, 2025 11:18:02 AM	PDU 3	Critical	Device 3 not present
January 21, 2025 11:18:02 AM	PDU 2	Critical	Device 2 not present
January 21, 2025 11:18:02 AM	USER	Info	User admin from host 10.64.83.68 via WebUI logged out

図 74: イベントログ

イベントログは、[Actions] メニューからダウンロードまたはクリアできます。

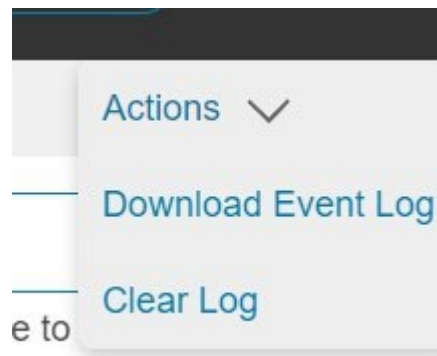


図 75: イベントログのアクションメニュー

データログ

ある時点に表示できるデータログの期間は、データログエントリ間の時間で決まります。各レコードの時間範囲は 1 ~ 1440 分に構成できます。(例として、データログが 60 分間隔の場合、データログには最大 41.67 日分のデータ 1000 レコードが格納されます。)データログが最大の 1000 レコードに到達すると、最も古いエントリは新しいエントリで上書きされます。

1. [Logs] > [Data Log] へ進みます。

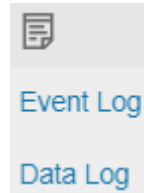


図 76: データログ

2. [Actions] ドロップダウンメニューを選択して [Data Log Configuration] を選択します。

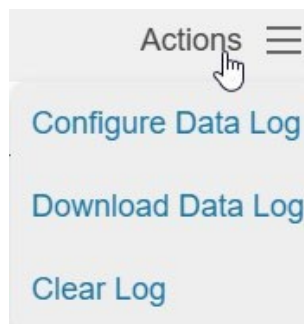


図 77: データログ構成

3. [Enable] を選択し、[Log Interval] フィールドに間隔の数値を入力します。(有効な範囲は 1 ~ 1440 分です。デフォルトの時間は 60 分です。)

Data Log Configuration

A screenshot of a web form titled 'Data Log Configuration'. The form has a light gray border and contains a single input field labeled 'Log Interval (1-1440 Minutes)'. The field contains the number '60'. Below the field are two buttons: a blue 'Save' button and a light blue 'Close' button.

図 78: データログ構成パネル

4. [Save] を選択します。

Web インターフェイスアクセス

ログアウト

ユーザーは各セッション後にログアウトして、システムが不正に変更されないようにする必要があります。

1. 画面右上のユーザー名アイコンをクリックします (「Web GUI の開始」を参照)。
2. ドロップダウンメニューで [Log Out] をクリックします。

アクセス権のタイプ

PDU には Admin、Controller、および Viewer プロファイルが付属しています。Admin 役割プロファイルは一般にはシステム管理者であり、操作上のフル権限を有する管理者権限を持っています。Viewer 役割は読み取り専用プロファイルです。他のすべてのユーザーは、管理者権限のあるユーザーが追加しなければなりません。Controller 役割は、アウトレットの制御などの PDU 機能を制御できますが、システム設定を変更することはできません。ユーザーは、それぞれ一意のログイン認証情報と、それぞれのユーザー役割により定義されます。アクセス権のレベルにより、ユーザーに何が表示されるか、そしてユーザーがどんな操作を実行できるかが決まります。アクセス権のレベルにより、どのメニュー項目にユーザーがアクセスできるか、どのフィールドに個々の設定および構成ダイアログが表示されるかが決まります。ユーザーをセットアップする前に、必要になる役割を判断します。各ユーザーに役割を指定する必要があります。これらの役割は、ユーザーに付与される権限を定義します。

役割	デフォルト権限
管理者	変更も削除もできないフル権限です。
コントローラー	PDU システムを制御できますが、構成は変更できません。
ユーザー	読み取り専用権限です。システムをモニタリングできますが、構成は変更できません。

ユーザーアカウント

ユーザーを追加するには、以下の手順を実行します。

1. [Settings] > [User Accounts] へ進みます。
2. 空のユーザー名フィールドの横にある鉛筆をクリックし、新しいユーザープロファイルを作成します。
3. [Settings] タブを使用して、以下の情報を入力します。
 - ユーザー名 (必須)
 - 役割 (必須)
 - パスワード (必須)
 - 確認パスワード (必須)
 - [Enabled] を選択してユーザーをアクティブ化します
 - ユーザーが次回ログインするときにパスワードを更新することを強制するには、[Must Change Password at next Log In] を選択します。

【注意】パスワードは 8 ～ 40 文字にする必要があり、以下の 4 つの規則の 3 つに従う必要があります。

- a. 小文字を 1 文字以上含む。
- b. 大文字を 1 文字以上含む。
- c. 数字を 1 文字以上含む。
- d. 特殊文字を 1 文字以上含む。

4. [Save] を選択して、新しいユーザープロファイルを保存します。

ユーザープロファイルを変更するには、以下の手順を実行します。

1. [Settings] > [Users] に進みます。
2. 変更するユーザーの横にある鉛筆をクリックします。
3. [Edit] を選択します。ユーザープロファイルを変更します。
4. [Save] を選択します。

ユーザープロファイルを削除するには、以下の手順を実行します。

1. [Settings] > [Users] に進みます。
2. 変更するユーザーの横にある鉛筆をクリックします。
3. ユーザー名を削除します。
4. [Save] を選択します。

RADIUS 認証のシステムを設定する

1. 設定メニューで [User Accounts] へ進みます。

User Accounts

Users		
Username	Role	Enabled
admin	Admin	Yes
Add User		

Session Management

Sign-In retries limited	Enabled
Number of Retries Allowed	3
Session Timeout Value	30 minutes
Lockout Time	10 minutes

Default Units

Temperature Units °C

RADIUS Configuration

Enable RADIUS	Disabled
Always Send Message-Authenticator Attribute	Disabled
RADIUS Server	
RADIUS Port	1812

LDAP Configuration

Enable LDAP	Disabled
LDAP Server	
Port	389
Security	None
Verify Server Certificate	Disabled
Provide Client Certificate	Disabled
Base DN	
Search User DN	
Login Name Attribute	
User Entry Object Class	

LDAP Roles

Role	Description

図 79: ユーザーアカウント

2. [Radius Configuration] へ進んで、編集鉛筆をクリックします。

RADIUS Configuration

Enable RADIUS

☐ Enable

Always Send Message-Authenticator Attribute

☐ Enable

RADIUS Server

RADIUS Port

1812

RADIUS Secret

Confirm Secret

Save Close

図 80: RADIUS 構成

- 3. [Enable] ボタンを選択します。
- 4. [Server] の IP アドレスフィールド、[Port] の番号フィールド、[Secret] フィールドを入力します。
- 5. (オプション) RADIUS メッセージをセキュリティ保護するには [Always Send Message-Authentication Attributes] を選択します。
- 6. 保存をクリックすると RADIUS 認証は完了です。

【注意】デフォルトでは、RADIUS ユーザーは役割が指定されない場合に「viewer」役割になります。RADIUS サーバーの管理者は Panduit ベンダー (19536) デクショナリを構成することがあり、「User-Role」整数属性は User (1)、Admin (2)、または Control(3) に設定されます。詳細については、付録 E: RADIUS サーバー構成を参照してください。

TACACS+ 認証のシステムを設定する

- 1. 設定メニューで [User Accounts] へ進みます。
- 2. [TACACS+ Configuration] へ進んで、編集の鉛筆をクリックします。

User Accounts

Users

Username	Role	Enabled
admin	Admin	Yes
Add User		

RADIUS Configuration

Enable RADIUS	Disabled
Always Send Message-Authenticator Attribute	Disabled
RADIUS Server	
RADIUS Port	1812

Session Management

Sign-In retries limited	Enabled
Number of Retries Allowed	3
Session Timeout Value	30 minutes
Lockout Time	10 minutes

LDAP Configuration

Enable LDAP	Disabled
LDAP Server	
Port	389
Security	None
Verify Server Certificate	Disabled
Provide Client Certificate	Disabled
Base DN	
Search User DN	
Login Name Attribute	
User Entry Object Class	

Default Units

Temperature Units	°C
-------------------	----

LDAP Roles

Role	Description
------	-------------

図 81: ユーザーアカウント

TACACS+ Configuration

Enable TACACS+

☐ Enable

TACACS+ Server

TACACS+ Port

49

TACACS+ Secret

Confirm Secret

Authentication Protocol

ASCII

Save Close

図 82: TACACS+ 構成

3. [Enable] ボタンを選択します。
4. サーバー IP アドレスフィールド、ポート番号フィールド、シークレットフィールドに入力し、認証プロトコルを選択します。
5. 保存をクリックすると、TACACS+ 認証は完了です。

【注意】TACACS+ サーバーの管理者は、次のいずれかに構成できます。

- パンドウイトベンダー固有の属性で、“panduit-user-role” を User、Control、または Admin にする
- 標準権限レベル (“priv-lvl”) を 1 (User)、7 (Control)、または 15 (Admin) に設定する

LDAP サーバー設定でシステムを構成する

LDAP をセットアップして Active Directory (AD) にアクセスし、NMC に Web インターフェイスからログインするときに認証を指定するには、以下の手順を実行します。

1. [User Accounts] ([Settings] の下) > [LDAP Configuration] へ進みます。
2. [LDAP Configuration] の横にある鉛筆アイコンを選択し、[Enable]チェックボックスをチェックします。
3. ドメインコントローラ (LDAP サーバー)/Active Directory (AD) サーバーの IP アドレスを入力します。
例: 192.168.1.101
4. ポートを入力します。
【注意】 Microsoft の場合、これは一般には 389 です。
5. セキュリティを入力します。暗号化しない送信の場合は None です。TLS 接続への接続後に接続をアップグレードする場合は StartTLS です。TLS 接続で開始する場合は TLS です。
6. [Base DN] フィールドで、AD にアクセスするために使用するアカウントを入力します。
例: CN=myuser,CN=Users,DC=EMEA,DC=mydomain,DC=com
7. [Bind Password] フィールドと [Confirm Password] フィールドにパスワードを入力します。
8. [Search User DN] フィールドで、以下を指定します。
例: DC=subdomain,DC=mydomain,DC=com
9. [Login Name Attribute] フィールドで、sAMAccountName (通常) を入力します。
10. [User Entry Object Class] フィールドで、person を入力します。

これらの LDAP 設定が構成されると、バインドは完了です。

LDAP Configuration

The image shows a web-based configuration form for LDAP. It contains the following fields and controls:

- Enable LDAP:** A checkbox labeled "Enable".
- LDAP Server:** A text input field.
- Port:** A text input field with the value "389" displayed.
- Security:** A dropdown menu currently showing "None".
- Verify Certificate:** A checkbox labeled "Verify (only valid if using TLS/startTLS)".
- Base DN:** A text input field.
- BIND Password:** A text input field.
- Confirm Password:** A text input field.
- Search User DN:** A text input field.
- Login Name Attribute:** A text input field.
- User Entry Object Class:** A text input field.

At the bottom of the form are two buttons: "Save" and "Close".

図 83: LDAP 構成

LDAP が構成されると、PDU はどのグループで認証が行われるかを検知します。役割を PDU で作成して Active Directory (AD) 内のグループを参照できるようにする必要があります。

1. Active Directory 内で、NMC 管理者になってもらいたいと考えるユーザーのグループを作成します。例: admins
【注意】 PDU によって強制される管理者の数に制限はありません。ただし、LDAP サーバーによる制限がある場合もあります。
2. PDU Web GUI で、[User Accounts] ([Settings] の下) > [LDAP Roles] をへ進みます。AD で作成した役割名 (admins など) を入力します。

3. 役割権限を必要に応じて有効にします (以下に図示)。

Edit Role

Role

Description

Privilege Level

None ▼

Enable Role

☐ enable

Save Close

図 84: 役割権限を有効にする

4. LDAP 認証を使用する準備ができました。

イベント通知

PDU の設定からイベント通知を有効にできます。

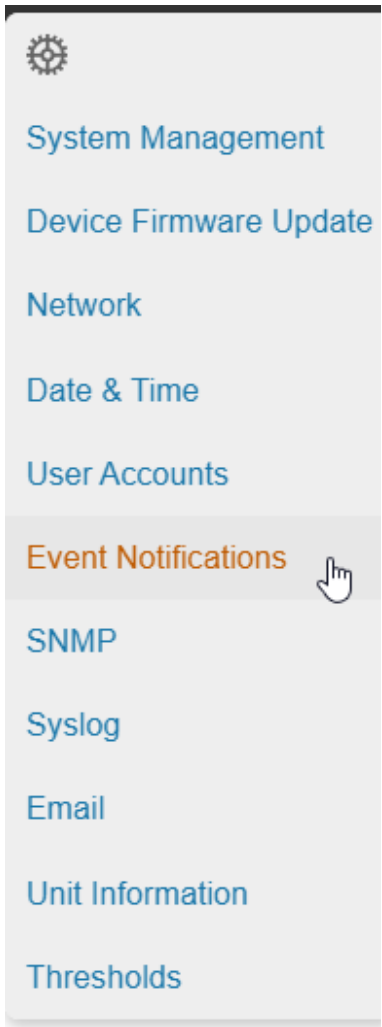


図 85: イベント通知

【注意】一部のイベント通知は、Web GUI にトグルスイッチが表示されていても、PDU タイプによっては適用されない、またはサポートされていない場合があります。それらのトグルスイッチは無視してください。
以下の表に、一部の PDU タイプでサポートされていないイベントを示します。

イベント通知	MI (Monitored Input) シリーズ	MI (Monitored Input) シリーズ、ブレーカー数が 6 個を超えるモデル	MS (Monitored Switched) シリーズ	MS (Monitored Switched) シリーズ、ブレーカー数が 6 個を超えるモデル	MPO (Monitored Per Outlet) シリーズ	MSPO (Monitored and Switched Per Outlet) シリーズ
サーキットブレーカーのステータスの変更	X	X	✓	X	✓	✓
ブレーカー電圧	X	X	✓	X	✓	✓
ブレーカー/グループの電流	✓	X	✓	X	✓	✓
アウトレット電力制御ステータスの変更	X	X	✓	✓	X	✓

セクション 3 - 簡易ネットワーク管理プロトコル (SNMP)

SNMP マネージメント構成

SNMP のセットアップ

1. Web インターフェイスにアクセスしてログインします。
2. [SNMP] の下で、[SNMP General] を選択します。(もしくは、SNMP で検索します。)SNMP General ページが表示されます。

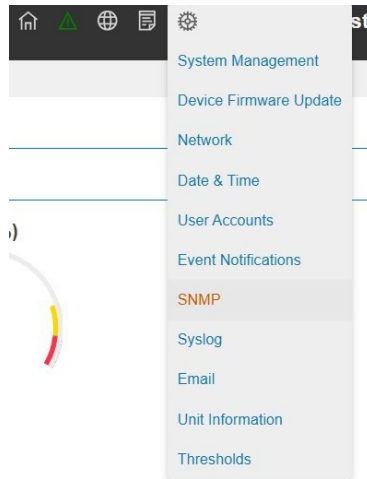


図 86: SNMP 構成

3. SNMP General ページに、SNMP のアクセスとバージョンが表示されます。

SNMP General

Enable SNMP

☒ Enable

SNMP Version

V12CV3

Save

Close

図 87: SNMP の一般情報

SNMP ポートのセットアップ

1. Web インターフェイスにアクセスしてログインします。
2. [SNMP] の下で、[SNMP Port] を選択します。SNMP Port ページが表示されます。

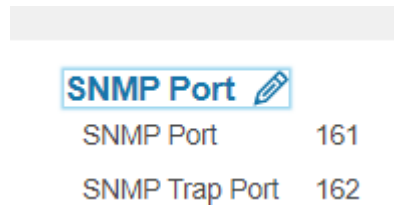


図 88: SNMP ポート

3. SNMP ポートおよび SNMP トラップポートを設定します。

SNMP Port

SNMP Port
161
SNMP Trap Port
162

Save Close

図 89: SNMP ポートおよびトラップポートのセットアップ

SNMP ユーザーを構成する

SNMP ユーザーを構成すると、ユーザーは SNMP 経由でシステムにアクセスできます。SNMP USER をセットアップするには、以下の手順に従ってください。

SNMP V1/V2c のユーザーを構成する

- 1. Web インターフェイスにアクセスしてログインします。
- 2. [SNMP] の下で、[SNMP V1/V2c] を選択します。
- 3. SNMP V1/V2c パネルで、構成する SNMP V1/V2c マネージャーを選択します。鉛筆アイコンを選択します。

SNMP v1/v2c Manager				
IP Address	Read Community	Write Community	Enabled	
0.0.0.0	public	private	Enabled	
0.0.0.0	public	private	Disabled	
0.0.0.0	public	private	Disabled	
0.0.0.0	public	private	Disabled	
0.0.0.0	public	private	Disabled	

図 90: SNMP V1/V2c ユーザーの定義

- 4. Edit パネルが表示されます。

Edit v2 User

IP Address

0.0.0.0

Read Community

public

Write Community

private

Enabled

☒ Enable

Save

Close

図 91: V1/2c マネージャーの編集

5. 以下のオプションを設定します。
- IP アドレス:この SNMP V1/V2 マネージャーのホストの IP アドレスです。このアドレスからのリクエストにのみ対応します。
- 【注意】0.0.0.0 に構成した IP アドレスはワイルドカードとして機能し、すべてのリクエストに対応します。
- 読み取りコミュニティ: SNMP V1/V2c マネージャーに SNMMP オブジェクトの読み取りを許可するための読み取り専用コミュニティの文字列です。
 - 書き込みコミュニティ: SNMP V1/V2c マネージャーに SNMMP オブジェクトの書き込みを許可するための書き込み専用コミュニティの文字列です。
6. [Enable]、[Save] をクリックします。

SNMP v3 のユーザーを構成する

1. Web インターフェイスにアクセスしてログインします。
2. [Settings] の下で、[SNMP] を選択します。
3. SNMP v3 マネージャーパネルで、構成する SNMP v3 マネージャーを選択します。最後の列の鉛筆アイコンを選択します。

SNMP v3 Manager					
Username	Security Level	Authentication Algorithm	Privacy Algorithm	Enabled	
jim	NoAuthNoPriv	SHA	AES128	Enabled	
test	AuthNoPriv	MD5	AES128	Enabled	
	AuthPriv	SHA	AES128	Disabled	
	AuthPriv	SHA	AES128	Disabled	
	AuthPriv	SHA	AES128	Disabled	

図 92: SNMP v3 マネージャー

4. Edit パネルが表示されて、構成可能なオプションが表示されます。

Edit v3 User

Username

Security Level

AuthPriv ▼

Authentication Password

Confirm Password

Authentication Algorithm

SHA ▼

Privacy Key

Confirm Password

Privacy Algorithm

AES128 ▼

Enabled

☐ Enable

Save Close

図 93: SNMP V3 の編集

5. SNMP ユーザー名を構成します。
6. セキュリティレベルをドロップダウンメニューから選択します。
- NoAuthNoPriv: 認証もプライバシーありません。これがデフォルト設定です。
 - AuthNoPriv: 認証はありますが、プライバシーがありません。
 - AuthPriv: 認証とプライバシーがあります。
7. 認証に使用する新しい一意の認証パスワードを入力します。その下にある [Confirm Password] に認証パスワードを再入力します。

8. 使用する認証アルゴリズムを選択します。
 - MD5
 - SHA
9. プライバシーアルゴリズムで使用する新しい固有の秘密鍵を入力します。その下にある [Confirm Password] に秘密鍵を再入力します。
10. 目的のプライバシーアルゴリズムを選択します。
 - AES-128
11. [Enable]、[Save] をクリックします。

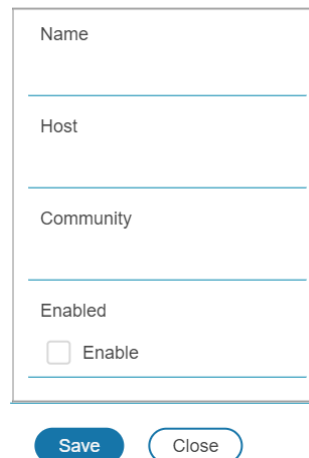
SNMPトラップを構成する

NMC は、すべてのイベントの内部ログを保持します。これらのイベントを使用すれば、SNMPトラップを第三者のマネージャーに送信できます。SNMPトラップを送信するように NMC をセットアップするには、以下の手順に従ってください。

SNMP v1 トラップ設定を構成する

1. [Settings] > [SNMP] に移動します
2. 更新する SNMPV2c トラップレシーバーの横にある鉛筆をクリックします。

Edit v2c Trap



The screenshot shows a web form titled "Edit v2c Trap". It contains four text input fields labeled "Name", "Host", "Community", and "Enabled". Below the "Enabled" field is a checkbox with the label "Enable". At the bottom of the form, there are two buttons: "Save" and "Close".

図 94: SNMPv2c トラップレシーバー構成情報

3. 表示されているフィールドに、名前、ホスト、コミュニティ名を入力します。
 - a. 名前は、異なるレシーバーを識別するためにユーザーが割り当てた名前です。
 - b. ホスト名は、SNMP システムエージェントによってトラップが送信される IP アドレスです。
 - c. コミュニティは、SNMP 管理ステーションのパスワードです。
4. [Enable] を選択して、レシーバーを有効にします。
5. [Save] を選択して保存し、終了します。

SNMP v3 トラップ設定を構成する

1. [Settings] > [SNMP] に移動します
2. 更新する SNMPV3 トラップサーバーの横にある鉛筆をクリックします。

Edit v3 Trap

Name

Host

Security Level

AuthPriv

Authentication Password

Confirm Password

Authentication Algorithm

SHA

Privacy Key

Confirm Password

Privacy Algorithm

AES128

Enabled

☐ Enable

Save Close

図 95: SNMPv3 トラップサーバー構成情報

3. 表示されているフィールドに、名前およびホスト名を入力します。
 - a. 名前は、異なるレシーバーを識別するためにユーザーが割り当てた名前です。
 - b. ホスト名は、SNMP システムエージェントによってトラップが送信される IP アドレスです。
4. セキュリティレベルをドロップダウンメニューから選択します。
 - NoAuthNoPriv: 認証もプライバシーもありません。これがデフォルト設定です。
 - AuthNoPriv: 認証はありますが、プライバシーがありません。
 - AuthPriv: 認証とプライバシーがあります。
5. 認証に使用する SNMP サーバーからの認証パスワードを入力します。その下にある [Confirm Password] に認証パスワードを再入力します。

6. 使用する認証アルゴリズムを選択します。
 - MD5
 - SHA
7. プライバシーアルゴリズム用の SNMP サーバーからの秘密鍵を入力します。その下にある [Confirm Password] に秘密鍵を再入力します。
8. 目的のプライバシーアルゴリズムを選択します。
 - AES-128
9. [Enable] を選択して、レシーバーを有効にします。
10. [Save] を選択して保存し、終了します。

セクション 4 - ローカルディスプレイ

オンボードディスプレイおよびネットワークコントローラ

オンボードディスプレイは、PDU と接続デバイスに関する情報を知らせます。PDU にはタッチ画面式のグラフィカルネットワークコントローラパネルがあります。

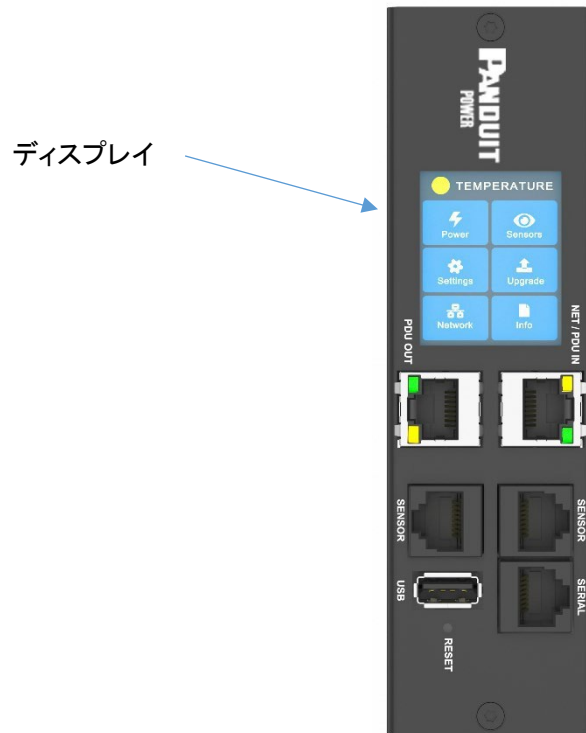


図 96: ネットワークコントローラ

ネットワークコントローラには 3 つのモードがあります。

1. メニューモード (ネットワークコントローラディスプレイのメインメニュー): PDU の電源がオンにされたか、スタンバイモードまたは節電モードで画面にタッチしたときに発生します。
2. スタンバイモード: メニューモードで PDU が 30 秒間アイドル状態になったとき (タッチ入力がないとき) に発生します。
 - スタンバイモードでは、PDU は主要な電源の値 (周波数、アンペア、ボルト、ワット、kVA) および IP アドレス (IPv4 と IPv6 の両方) をスクロール表示します。
3. 節電モード: PDU はスタンバイモードが 1 時間続いたとき、節電モードに入ります。節電モードを終了するには、画面ディスプレイにタッチします。

ネットワークコントローラメニューの構造

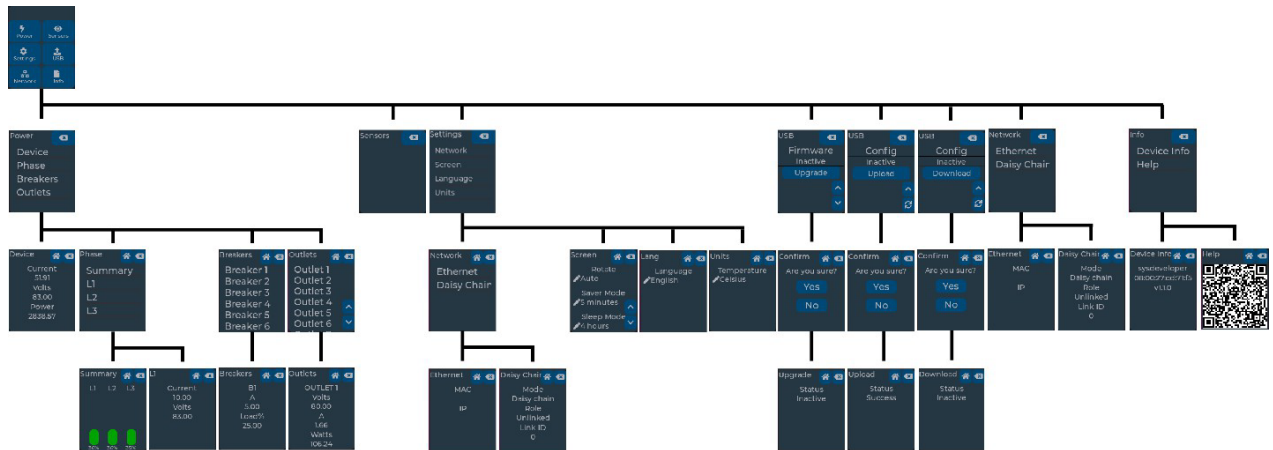


図 97: ネットワークコントローラメニューの構造

メインメニューの選択項目

PDU メニュー選択の階層構造は、[Power]、[Sensors]、[Settings]、[USB]、[Network]、および [Info] で構成されています。

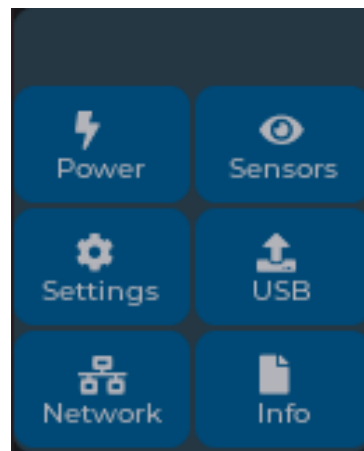


図 98: メインメニューの選択項目

[Alarms] メニュー

[Alarms] メニューには、PDU のアクティブアラームが表示されます。メインメニューでアラームヘッダーにタッチすると、アラーム画面が表示されます。確認が終わったら、[Back] を押してメインメニューに戻ります。

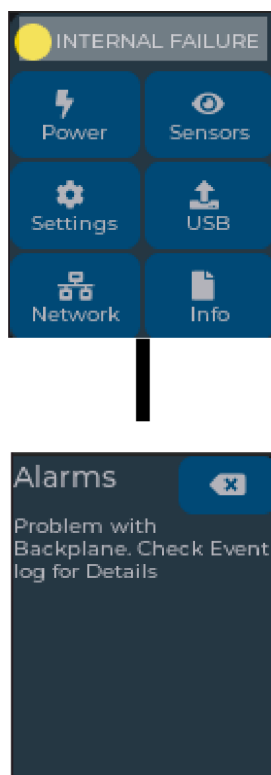


図 99: [Alarms] メニュー

[Power] メニュー

[Power] メニューではデバイス、相、ブレーカー、アウトレットを管理できます。メインメニューでメニューオプションにタッチすると、サブメニューオプションが表示されます。[Back] を押すと、直前のメニューに戻ります。[Home] を押すと、メインメニューに戻ります。

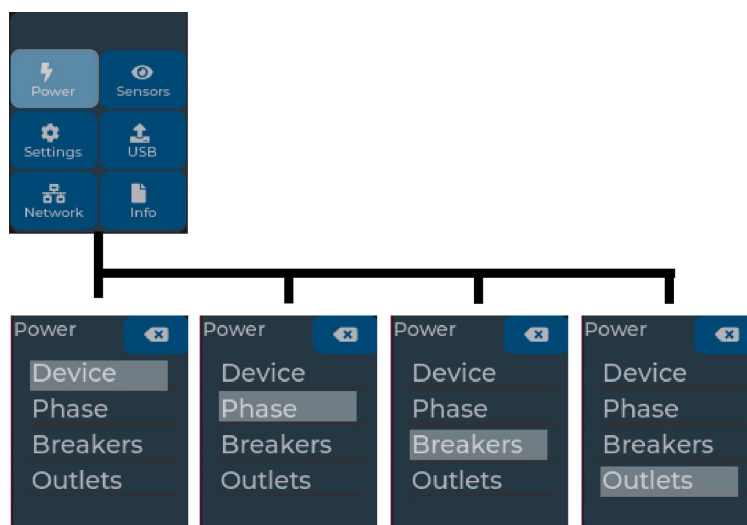


図 100: [Power] メニュー

[Device] サブメニュー

[Device] サブメニューには、電流、電圧、電力が表示されます。[Power] メニューで、[Device] にタッチすると、PDU 全体の電源の値が表示されます。[Back] を押すと、直前のメニューに戻ります。

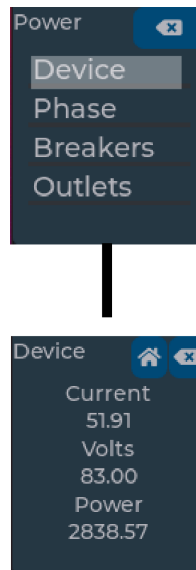


図 101: [Device] サブメニュー

[Phase] サブメニュー

[Phase] サブメニューでは、相のステータスを表示します。[Power] メニューで [Phase] にタッチすると、サブメニューの値を設定する画面が表示されます。相を選択した後で、目的の相にタッチすると、その相の値が画面に表示されます。

[Back] を押すと、直前のメニューに戻ります。

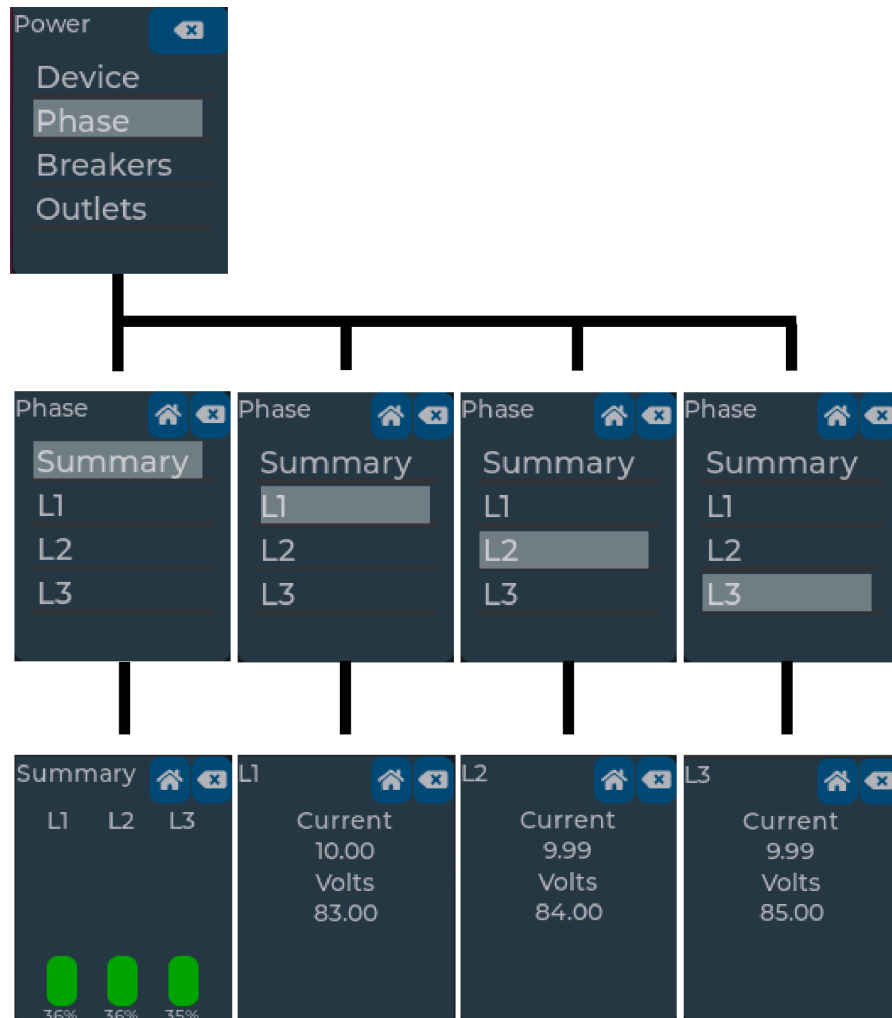


図 102: [Phase] サブメニュー

[Breaker] サブメニュー

[Breaker] サブメニューには、ブレーカーの電力値が表示されます。[Power] メニューで、[Breakers] にタッチすると、ブレーカーの一覧が表示されます。ブレーカーを表示する際、目的のブレーカー番号にタッチすると、ブレーカーの値が表示されます。[Back] を押すと、直前のメニューに戻ります。

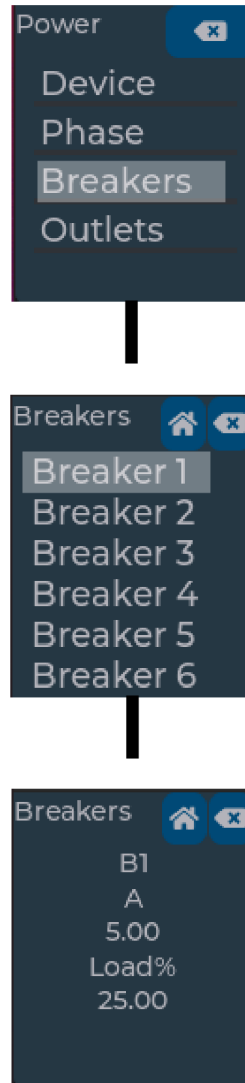


図 103: [Breaker] サブメニュー

[Outlet] サブメニュー

[Outlet] サブメニューには、シリアル番号 1 から番号 n までの電圧、電流、電力が表示されます。[Power] メニューで [Outlet] にタッチします。目的のアウトレット番号にタッチすると、アウトレットに関する値が表示されます。[Back] を押すと、直前のメニューに戻ります。

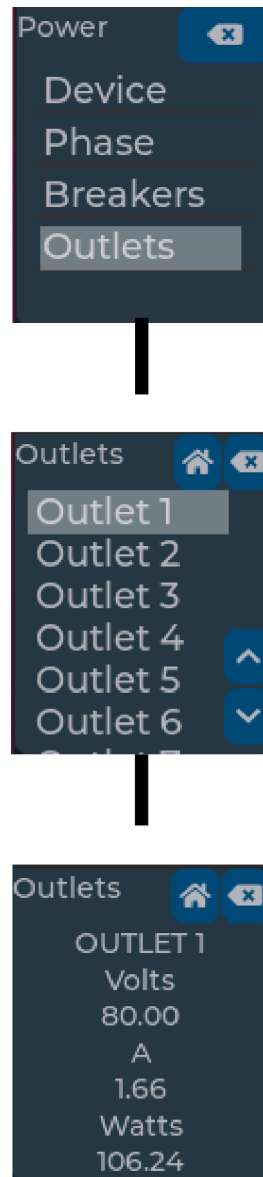


図 104: [Outlet] サブメニュー

[Sensors] メニュー

[Sensor] メニューには、温度、湿度、ドアスイッチ、漏液等が表示されます。メインメニューで、[Sensor] にタッチすると、センサーの一覧が表示されます。目的のセンサー番号にタッチすると、センサーに関する値が表示されます。[Back] を押すと、直前のメニューに戻ります。

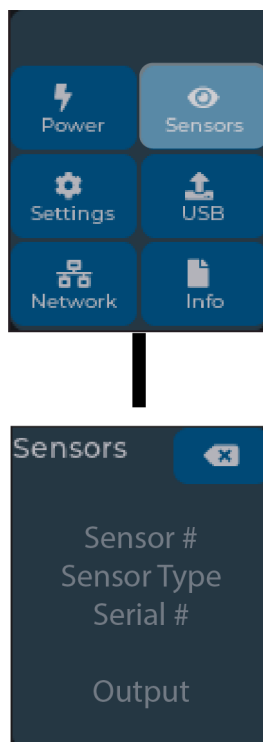


図 105: センサー

[Settings] メニュー

[Settings] メニューには、ユーザー構成オプションとして [Network]、[Screen]、[Language]、[Units] があります。[Back] を押すと、直前のメニューに戻ります。[Home] を押すと、メインメニューに戻ります。

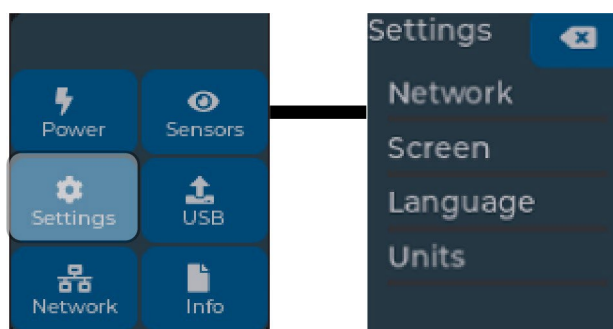


図 106: [Setup] メニュー

[Network] サブメニュー

[Network] サブメニューでは、デバイスアドレスとデ이지チェーン構成を表示できます。[Settings] メニューで [Network] にタッチすると、[Network] サブメニューに移動します。[Ethernet] にタッチすると、IP アドレスおよび MAC アドレスを表示する画面が表示されます。[Daisy Chain] にタッチすると、構成オプションが表示されます。[Back] を押すと、直前のメニューに戻ります。

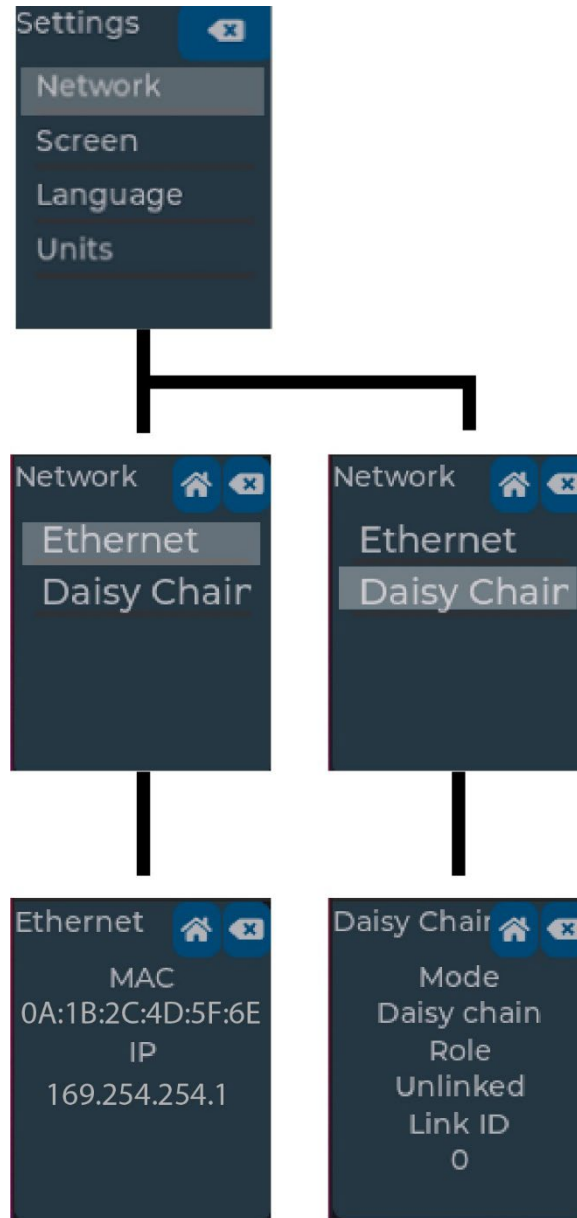


図 107: [Network] サブメニュー

[Screen] サブメニュー

[Screen] サブメニューでは、[Rotate]、[Saver Mode]、[Sleep Mode] の設定をカスタマイズできます。[Settings] メニューでサブメニューにタッチして選択します。オプションを選択した後、画面上の目的の値にタッチして設定します。[Back] を押すと、直前のメニューに戻ります。

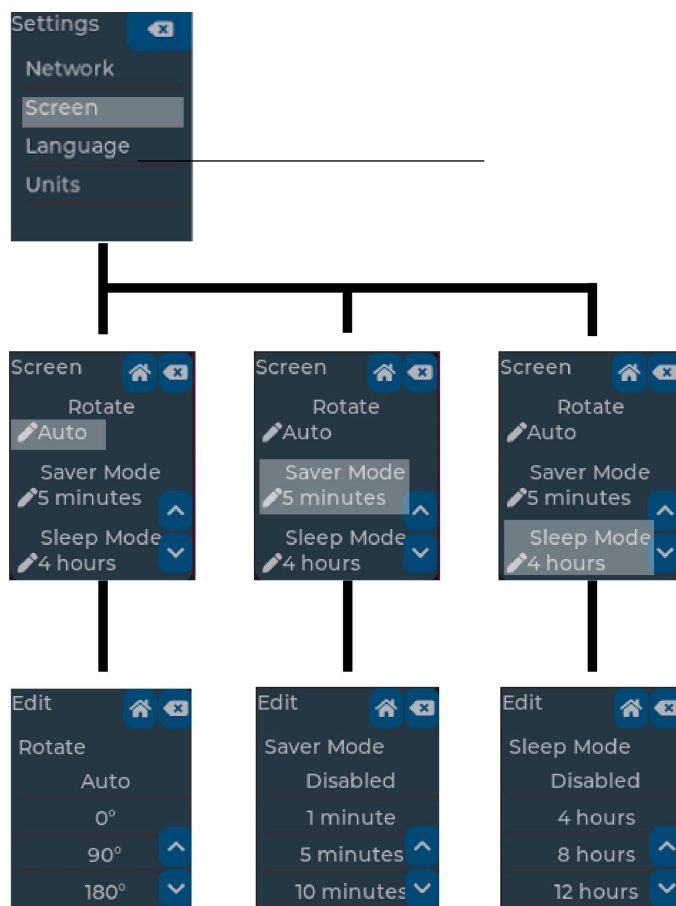


図 108: [Screen] サブメニュー

[Language] サブメニュー

[Language] サブメニューでは、使用する言語を選択できます。[Settings] メニューで、[Language] にタッチすると、サブメニューを選択する画面が表示されます。言語を選択した後、画面上の目的の値にタッチして設定します。[Back] を押すと、直前のメニューに戻ります。

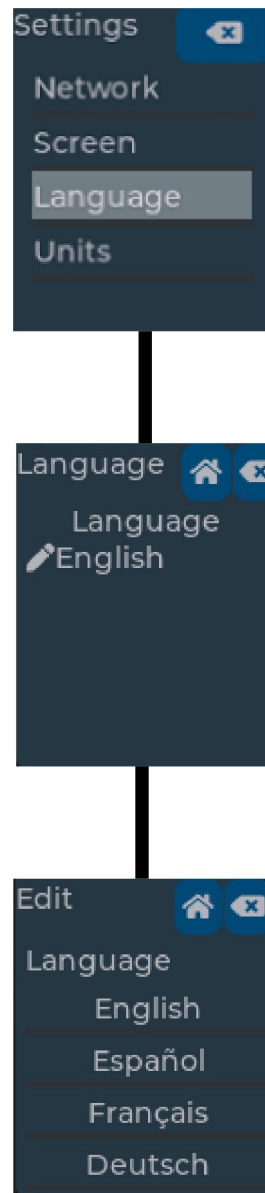


図 109: [Language] サブメニュー

[Units] サブメニュー

[Units] サブメニューには温度の単位が表示されます。[Settings] メニューで [Units] サブメニューにタッチします。
[Units] サブメニューで、目的の値にタッチして設定します。[Back] を押すと、直前のメニューに戻ります。[Home] を押すと、メインメニューに戻ります。

【注意】この操作は PDU でローカルにのみ行うことができます。

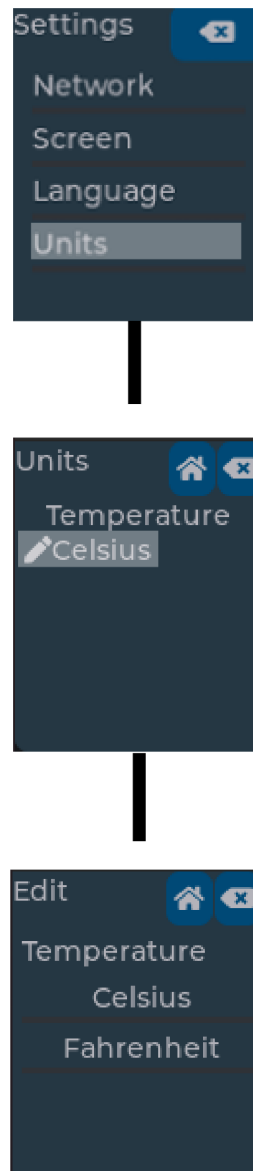


図 110: [Units] サブメニュー

USB メニュー

USB メニューは外部 USB ドライブが USB ポートに接続されたときに使用されます。ユーザーは、このメニューからファームウェアファイルをアップロードできます。デバイスによって受け入れられるのは、署名付きの正式なファームウェアファイルのみです。USB ポートは、新しい構成をアップロードしたり、接続された外部 USB ドライブに現在の構成をダウンロードしたりするために使用することもできます。

USB ポートは Web UI ([Settings] → [SystemManagement]) から有効化または無効化できます。

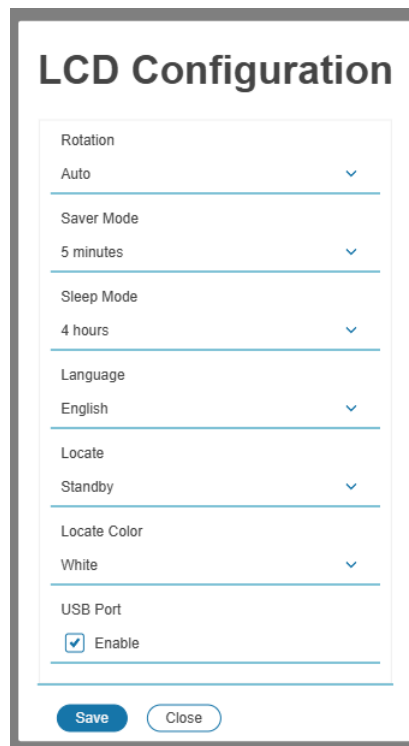


図 111: USB の有効化

USB 経由でのファームウェアの更新

【注意】USB ドライブは暗号化が解除され、FAT32 ファイルシステムとしてフォーマットされている必要があります。

ファームウェアをアップグレードまたはダウングレードするには、ファームウェアファイルが格納されている USB ストレージデバイスを挿入します。挿入すると、PDU はファームウェアファイルを自動的に検出してコピーします。ステータスは「Copying」、「Available」の順に更新されます。ステータスが「Available」になると、PDU は新しいファームウェアファイルをロードする準備が整い、USB デバイスを PDU から取り外すことができます。

ファームウェアアップグレードを開始するには、「Upgrade」、「Yes」の順にタッチして確認します。ファームウェアステータスページが表示され、ステータスは「Available」から「Uploading」に更新されます。アップロードが完了したら、ステータスは「Uploading」から「Activating」に更新されます。「Activating」フェーズ中に、PDU はファームウェアをインストールし、必要なクリーンアップを行います。

「Activating」が完了すると、デバイスは自動的に再起動します (同一のバージョンがすでにインストール済みの場合を除く)。ファームウェアのアップグレードまたはダウングレードの処理がアウトレットの状態に影響することはありません。

構成

アップロード

：新しい構成をアップロードするには、config*.json ファイルを格納している USB ストレージデバイスを挿入します。挿入すると、PDU は構成ファイルを自動的に検出してコピーします。ステータスは「Inactive」、「Copying」、「Available」の順に更新されます。ステータスが「Available」のとき、PDU は新しい構成をロードする準備が整い、USB デバイスを PDU から取り外すことができます。

構成アップロードを開始するには、「Upload」、「Yes」の順にタッチして確認します。構成アップロードステータスページが表示され、ステータスは「Available」から「Uploading」に更新されます。「Uploading」フェーズ中、PDU は構成ファイルを読み取り、デバイスについて適切な値を設定します。アップロードが完了したら、ステータスは「Success」または「Fail」を示します。いずれかのアクションに失敗した場合、ステータスは「Inactive」に戻り、プロセスを再試行することができます。

ダウンロード

：既存の構成をダウンロードするには、USB ストレージデバイスを挿入します。構成ダウンロードを開始するには、「Download」にタッチし、「Yes」で確定します。構成ダウンロードステータスページが表示され、ステータスは「Inactive」から「Downloading」に更新されます。「Downloading」フェーズ中、PDU はすべての構成データを収集し、構成ファイルを USB デバイス上に作成します。ダウンロードが完了したら、ステータスは「Success」または「Fail」を示します。いずれかのアクションに失敗した場合、ステータスは「Inactive」に戻り、プロセスを再試行することができます。

【注意】USB ドライブは暗号化が解除され、FAT32 ファイルシステムとしてフォーマットされている必要があります。

【注意】ファームウェアと構成ファイルの両方が USB デバイス上にある場合、PDU はまずファームウェアのコピーを優先させます。

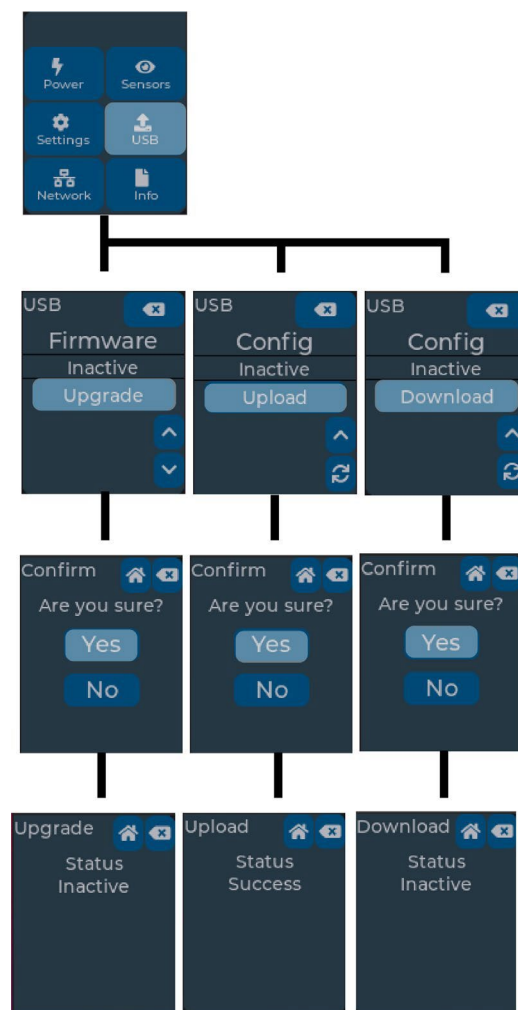


図 112: [USB] サブメニュー

[Network] メニュー

[Network] メニューには温度の単位が表示されます。[Setup] メニューで、下にスクロールして [Units] をハイライト表示します。[Select] を押して、[Units] サブメニューを入力します。値を選択した後で、[Select] を押して画面に表示される値に設定します。[Back] を押すと、直前のメニューに戻ります。[Home] を押すと、メインメニューに戻ります。

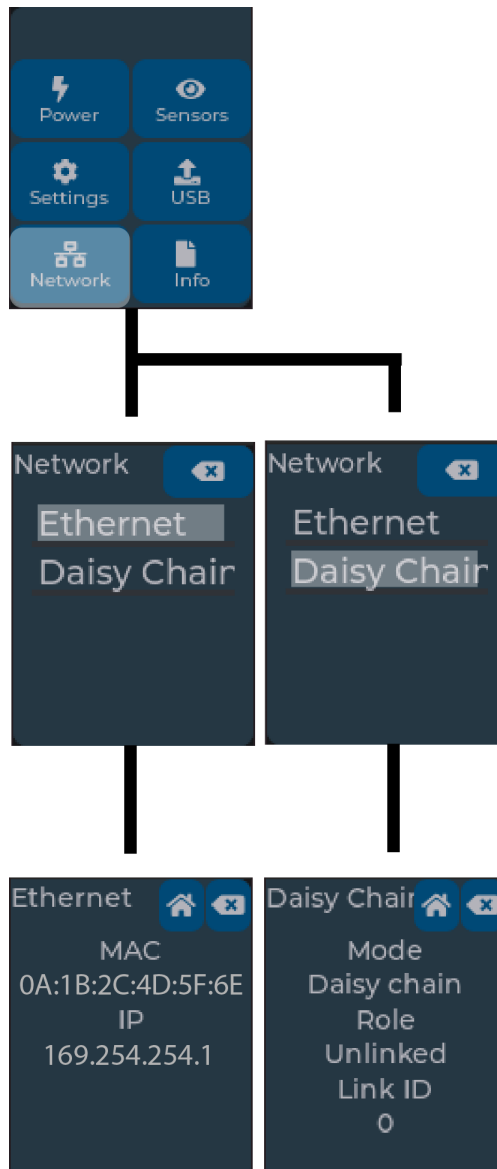


図 113: [Network] メニュー

[Info] メニュー

[Info] メニューはデバイス情報と、製品サポートページにリンクする QR コードを表示します。[Info] メニューで、[Device Info] にタッチすると、関連するすべてのデバイス情報が表示されます。[Help] をタッチすると、公開されている製品ページにリダイレクトする QR コードが表示されます。[Back] を押すと、直前のメニューに戻ります。[Home] を押すと、メインメニューに戻ります。

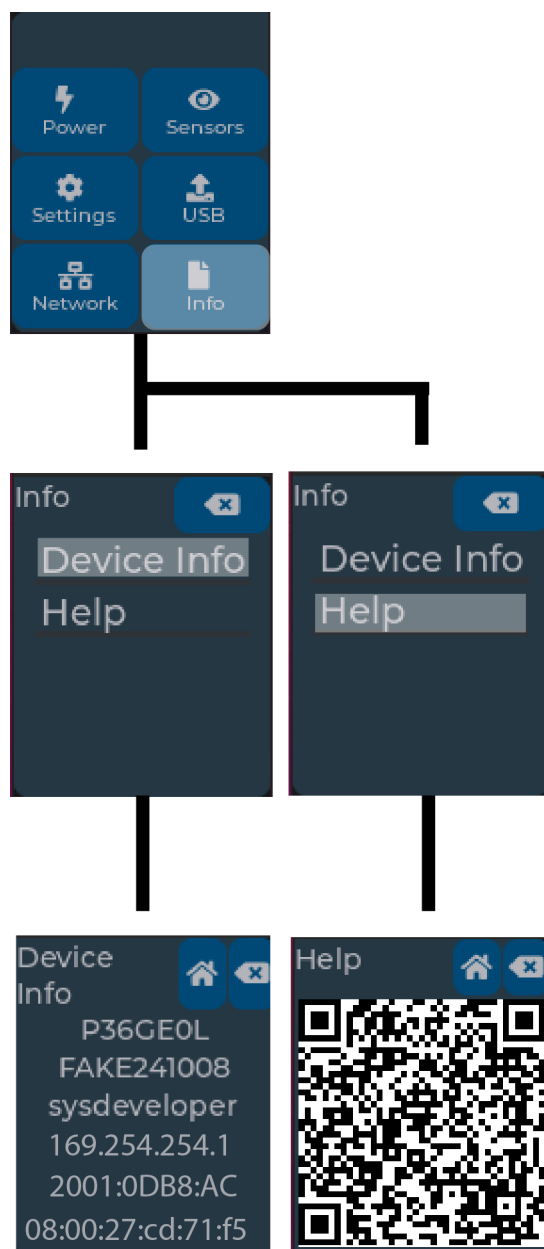


図 114: 情報メニュー

[Help] メニュー

[Help] メニューからは、ユーザーガイドやデバイスのライセンスのほか、SNMP MIB に簡単にアクセスできます。

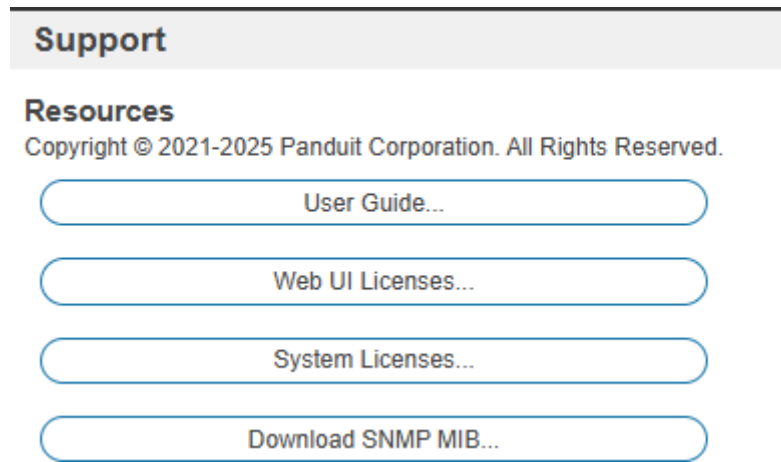


図 115: ヘルプとサポート

検索ボックス

検索ボックスでは、キーワードを入力するとキーワードの一覧が返されます。この方法により、PDU の各分野にすばやく簡単にアクセスできます。目的の分野が表示されたら、ユーザーはトピックをマウスでクリックして、その関連ページに直接移動できます。

現時点では、すべてのヘッダーがキーワードとして設定されています。検索で反応するキーワードは以下の通りです。

- 0: "Home / Dashboard"
- 1: "Home / Identification"
- 2: "Home / Control & Manage"
- 3: "Alarms / Active Alarms"
- 4: "Languages / English"
- 5: "Languages / Français"
- 6: "Languages / Deutsch"
- 7: "Languages / Español"
- 8: "Logs / Event Log"
- 9: "Logs / Data Log"
- 10: "Settings / Network Settings"
- 11: "Settings / System Management"
- 12: "Settings / Unit Information"
- 13: "Settings / Device Firmware Update"
- 14: "Settings / Event Notifications"
- 15: "Settings / SNMP Manager"

- 16: "Settings / Email Setup"
- 17: "Settings / Trap Receiver"
- 18: "Settings / User Accounts"
- 19: "Settings / Thresholds"
- 20: "Settings / Wi-Fi Settings"
- 21: "Settings / Rack Access Control"
- 22: "Settings / Link Configuration"
- 23: "Help / Support"

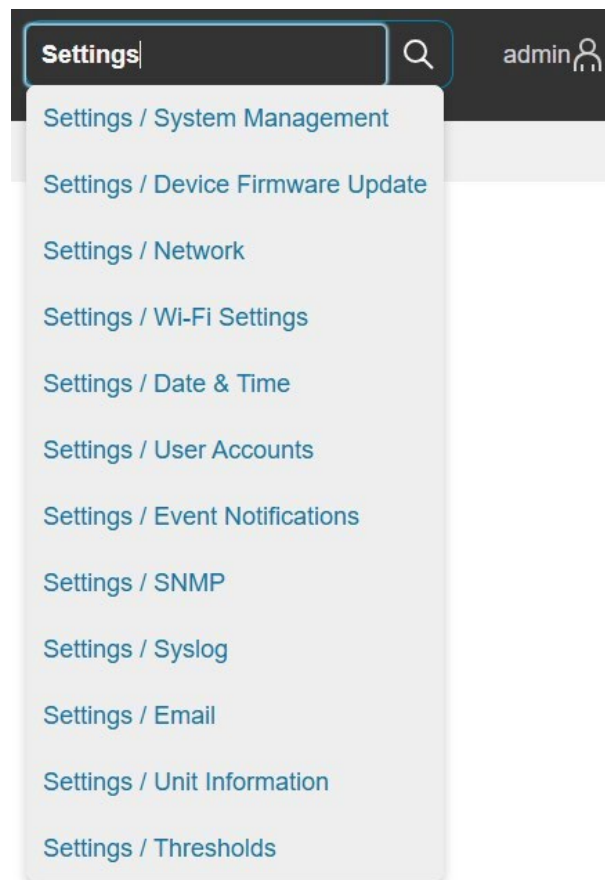


図 116: 検索ボックスの例

セクション 5 - デイジーチェーン構成

デイジーチェーン PDU 機能は工場出荷時に無効化されているため、Web GUI の [Settings] → [System Management] から有効にする必要があります。

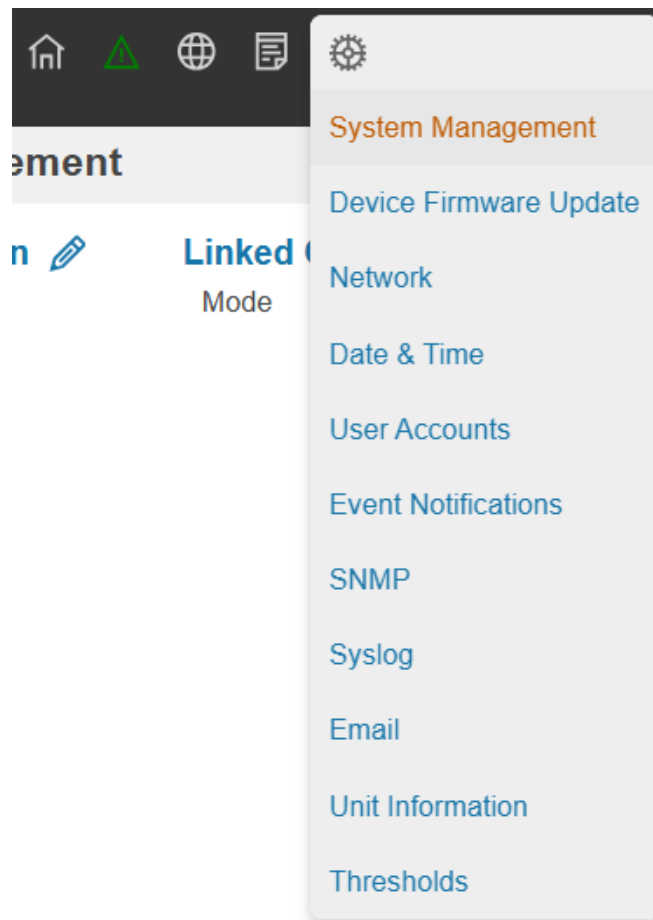


図 117: システム管理

[Linked Configuration] で、ユーザーは [Mode] を選択して、PDU の [Role] を選択する必要があります。

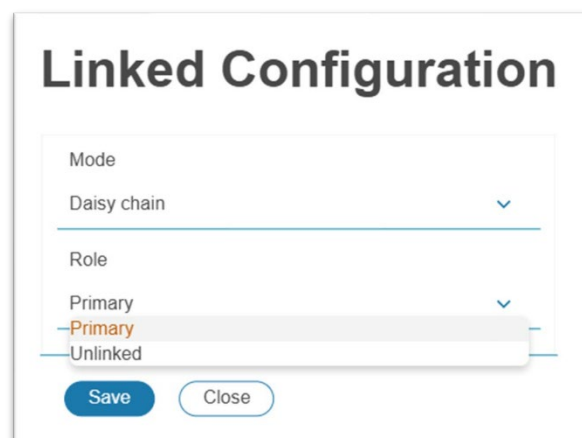


図 118: リンクされる構成

デジチェーンの概要

標準のデジチェーンモードでは、複数の EL2P PDU が直列に接続され、プライマリ PDU に割り当てられた単一の IP アドレスを通じて管理されます。下流側の PDU は個別のネットワーク ID を受け取らず、プライマリユニットの Web インターフェイスを経由して間接的にアクセスされます。

すべての通信は 1 つの管理インターフェイスを通じて集約されるため、このモードは固定のデジチェーン制限の影響を受け、同時に接続および管理できる PDU の最大数が制約を受けます。

デジチェーンモードでは、最大 64 個の EL2P PDU を 1 つの IP アドレス経由で接続できます。これにより、ユーザーはメイン PDU からデジチェーン接続されたすべての PDU の情報/データを収集し、それらの PDU を構成できます。

デジチェーンセットアップ

最初の PDU を構成した後で (プライマリ)、構成した PDU の PDU Out ポートを、デジチェーンの 2 番目の PDU の Ethernet/PDU In ポートとイーサネットケーブルで接続します。

PDU の PDU Out ポートから Ethernet/PDU In ポートへの接続を繰り返します。

Web インターフェイス (または管理ソフトウェア) に移動して、デジチェーン構成の PDU を管理および操作します。

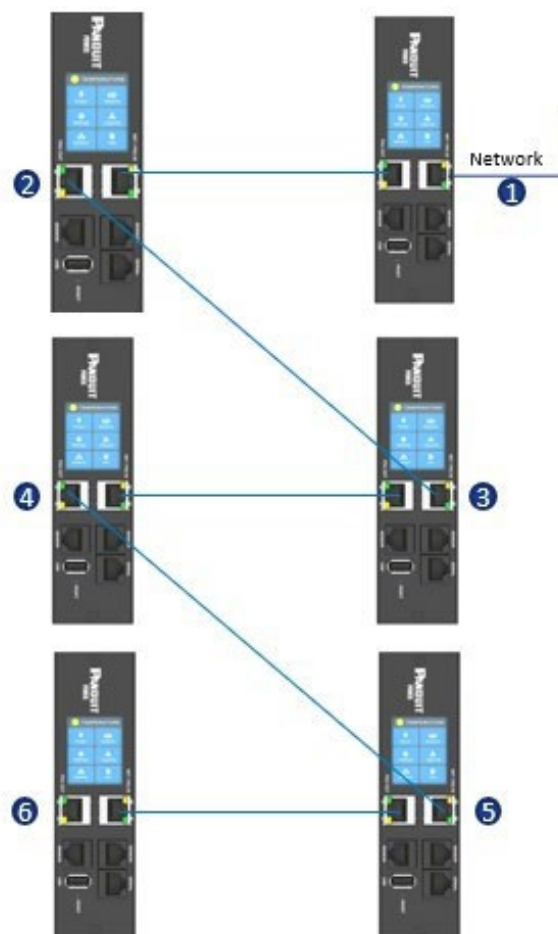


図 119: 6 つの PDU デジチェーンの接続図

ブリッジモードのデジチェーン

ブリッジモードのデジチェーンでは、標準のデジチェーンモードと同様に、複数の EL2P PDU が単一のネットワーク接続ポイントを介して物理的にデジチェーン接続されます。ただし、ネットワークレベルでは各 PDU がスタンドアロンモードで動作します。

この構成では、各 PDU には固有の IP アドレスが割り当てられるため、各ユニットは共通のネットワークアップリンクを共有しているにもかかわらず、独立してアクセス、監視、および管理できます。

そのためブリッジモードでは、標準のデジチェーンにおける制限が実質的に適用されなくなります。各 PDU は個々にアドレス指定可能で、ネットワークアクセスにおいてマスターユニットに依存しないため、拡張性はデジチェーンの上限ではなく、ネットワークの容量によって決まります。

ブリッジモードおよびネットワークの冗長性

ブリッジモードでは、デジチェーン接続された EL2P PDU グループの両端をネットワークに接続することで、ネットワークの冗長構成を実現できます。このトポロジーでは、ネットワークループを防ぐための STP (Spanning Tree Protocol) が必要です。

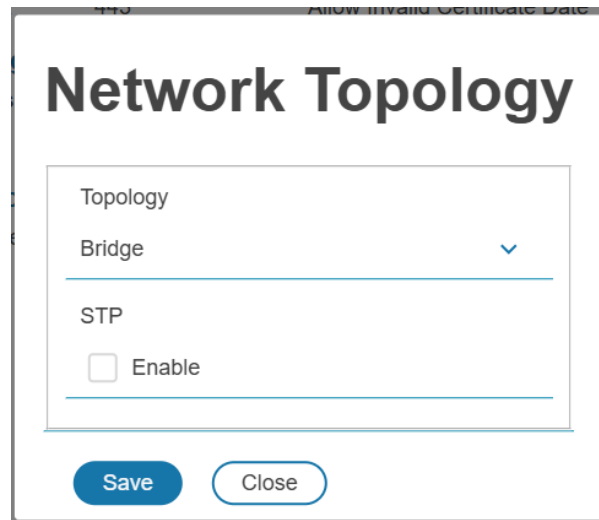
デジチェーンの両端が接続されると、STP は冗長パスを管理し、常に 1 つのアクティブな転送パスのみが使用されるようにします。STP がないと、この構成ではネットワークループが発生し、ブロードキャストストームやネットワーク性能の低下、またはネットワークの停止に至るおそれがあります。

【警告】 デジチェーンの両端をネットワークに接続する前に、必ず STP を有効にして適切に設定してください。

STP を有効にする場合は、対応する設定を接続されているネットワークスイッチにも適用する必要があります。STP が予期せず検出されたり、既存のネットワーク設定と競合したりすると、一部のネットワーク構成やスイッチポリシーでは、ポートが自動的に無効化される場合があります。設置する前に、スイッチの動作とポート構成を確認してください。

ブリッジモードのセットアップ

チェーン内の各 PDU はブリッジモード用に構成される必要があります。最初に PDU をネットワークに直接接続し、[Settings] -> [Network] で [Network Topology] を選択し、構成を [Bridge] に変更します。

A screenshot of a 'Network Topology' dialog box. The title 'Network Topology' is at the top. Below it is a 'Topology' dropdown menu with 'Bridge' selected and a blue downward arrow. Underneath is an 'STP' section with an unchecked checkbox labeled 'Enable'. At the bottom are two buttons: 'Save' (blue) and 'Close' (white with blue border).

STP を使用する場合は、ダイアログボックスの [Enabled] をチェックします。
チェーン内の次の PDU と通信可能になります。各 PDU について、この [Network Topology] 構成を繰り返してください。

パワーシェア

パワーシェアは、2つの給電のうち1つが中断した場合に継続的なセンサーモニタリングと電氣的ラックアクセスが行えるように設計されたものです。Panduit iPDU コントローラから利用できる電源が制限されているため、パワーシェアは以下の条件で設計およびテストされています。

ACF05 または AC06 Panduit セキュリティラックハンドル、ACF10 (T+D)、ACF11 (3T+D)
ACF06L Panduit セキュリティハンドル、EHH01L (T+D)、EHC01L (3T+D)

システムが不安定になったりパワーシェアが利用できなくなったりする可能性があるため、システムを過負荷状態にしないように注意する必要があります。

PDU コントローラの最大出力電力容量は $600\text{mA} @ 5\text{V} = 3 \text{ ワット}$ 、 $600\text{mA} @ 12\text{V} = 7.2 \text{ ワット}$ です。これに基づいて、パワーシェアを活用したソリューションをデプロイするときは、自動ライトバー (PN; ACD01L) を設置しないでください。

ブリッジモードのパワーシェア

冗長構成およびパワーシェアを使用したブリッジモードのデジチェーンをセットアップするには、構成中にいくつかの簡単な CLI コマンドを使用します。

UPLINK (U) PDU に対する CLI コマンド:

```
write config/powerShare/enUplink 0
write config/powerShare/enDownlink 1
```

DOWNLINK (D) PDU に対する CLI コマンド:

```
write config/powerShare/enUplink 1
write config/powerShare/enDownlink 0
```

(デジチェーン内の) 内部 PDU に対する CLI コマンド:

```
write config/powerShare/enUplink 1
write config/powerShare/enDownlink 1
```

以下の図に、冗長構成およびパワーシェアを使用したブリッジモードのデジチェーンの構成例を示します。

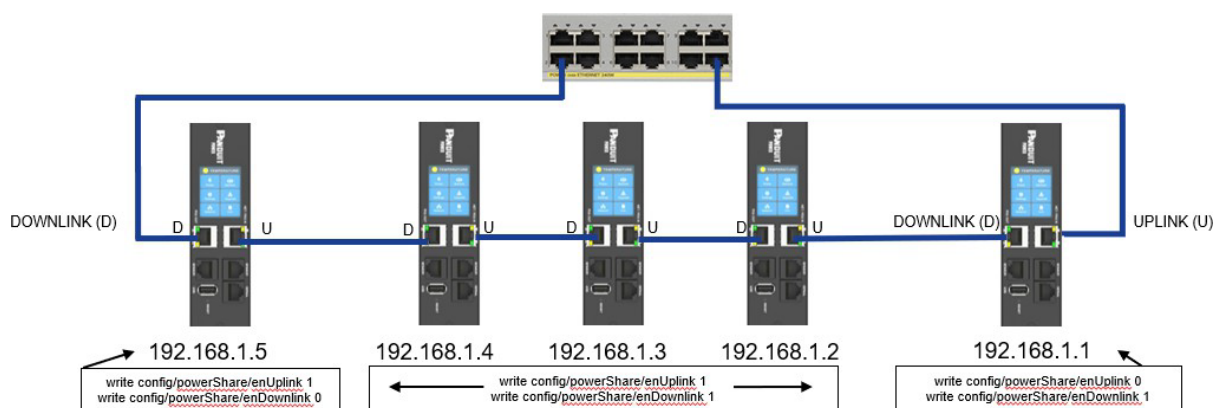


図 120: 冗長構成およびパワーシェアを使用したブリッジモードのデジチェーン

セクション 6 – EL2P PDU アクセサリー

ハードウェアの概要

重大な属性 (温度、湿度、漏れ検出、侵入など) のモニタリングは、効率良く運用されるデータセンターや IT ルームの環境を維持するための非常に重要な側面です。

EL2P PDU アクセサリーは EL2P コントローラと相互運用するように特別に設計されています。未承認のセンサーアクセサリーを NMC コントローラに接続したり、EL2P PDU センサーをサードパーティー製コントローラに接続したりすると、損傷する可能性があります。

【注意】 各 Panduit NMC コントローラでサポートされるセンサーの最大数は、接続された物理センサーアクセサリーによって提供される論理検出機能の数とタイプによって異なります。1 つの物理センサーアクセサリーが複数の論理検出機能に対応することがあります。物理センサーアクセサリーは、NMC の電源が入っているときに取り付けることができます。

論理検出機能	NMC あたりの最大論理センサー数
温度	6
湿度	4
ドア	2
ロープ	2
スポット	2
ドライ	2
自動ライトバー	2
ハンドル	2

以下の表に、利用可能な物理センサーアクセサリ製品と、アクセサリに関連した論理検出機能の一覧を示します。

物理センサーアクセサリ	説明	論理検出機能、数量
温度センサー (EA001、EA001L)	ラック内の温度をモニタリングします。	温度:1
温度&湿度センサー (EB001、EB001L)	ラック内の温度と相対湿度をモニタリングします。	温度:1 湿度:1
3 温度 + 1 湿度センサー (EC001、EC001L)	3 つの独立プローブを使用して 3 つのエリアの温度をモニタリングし、1 つのプローブを使用して相対湿度をモニタリングします。	温度:3 湿度:1
ドアセンサー (ACA01、ACA01L)	センサーを取り付けたドアが 10 mm 以上開いたときの侵入をモニタリングします。	ドア:1
漏水センサー (ロープ式)(ED00、ED001L)	抵抗率 2 メガオーム未満の液体 (蒸留水を含む) をモニタリングして漏れを検出します。	ロープ:1
漏水センサー (スポット式)(EE001、EE001L)	モニタリング領域内をモニタリングして、抵抗率 2 メガオーム未満の液体 (蒸留水を含む) の漏れを検出します。	スポット:1
センサーポートハブ (EF001、EF001L)	3 つのセンサーの追加接続が可能な受動ハブ	N/A
漏れ検出センサー延長線 (EG001、EG001L)	ロープ式の漏れ検出センサーを 6m 延長します。計 4 本の延長線を漏れ検出センサーに追加すると、合計で 30m の長さになります。	N/A
ドライ接点センサー (ACC01、ACC01L)	PDU NMC に入力され、接触状態の変化をモニタリングするように設計されています。	ドライ:1
自動ライトバー (ACD01L)	リモート制御および自動の空間照明	自動ライトバー:1
スマートラックハンドル (ACF06L)	スマートラックアクセスハンドル	ハンドル:1
3 温度 + 1 湿度、 ドアスイッチセンサー (EHC01L)	3 つの独立プローブを使用して 3 つのエリアの温度をモニタリングし、ドアの侵入をモニタリングし、1 つのプローブを使用して相対湿度をモニタリングします。	温度:3 湿度:1 ドア:1
1 温度、1 湿度ドアスイッチ センサー (EHH01L)	1 つのエリアの温度をモニタリングし、ドアの侵入をモニタリングし、1 つのプローブを使用して相対湿度をモニタリングします。	温度:1 湿度:1 ドア:1
スマートラックハンドル (ACF05、 ACF06)	湿度センサーが付いたスマートラックアクセスハンドル	ハンドル:1 湿度:1
3 温度 + ドアセンサーハーネス (ACF11 は ACF05 または ACF06 が必要)	3 つの独立プローブを使用して 3 つのエリアの温度をモニタリングし、1 つのドアをモニタリングします。	温度:3 ドア:1
1 温度 + ドアセンサーハーネス (ACF10 は ACF05 または ACF06 が必要)	ラック内の温度と 1 つのドアをモニタリングします。	温度:1 ドア:1

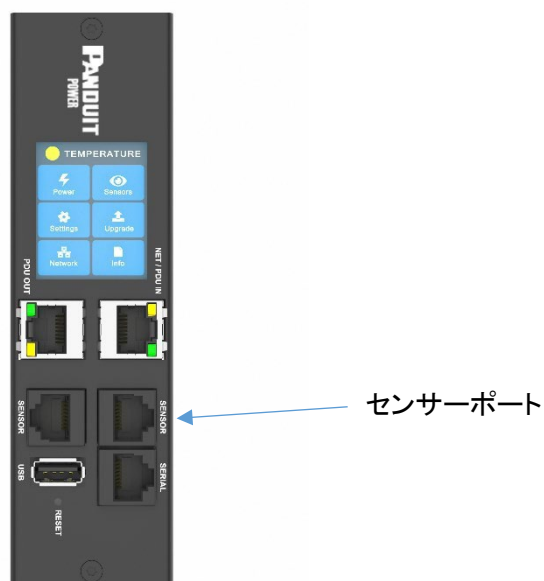


図 121: センサーポート

温度スケールを構成する

温度センサーの温度スケール (摂氏または華氏) を構成するには、以下の手順を実行します。

1. [User Accounts] へ進みます。

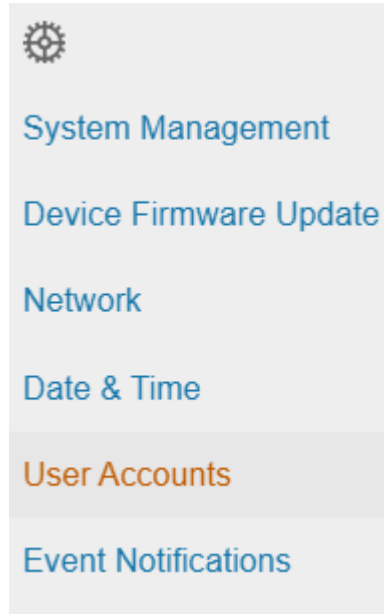


図 122: ユーザーアカウント

2. [Default Units] の横にある鉛筆を選択します。

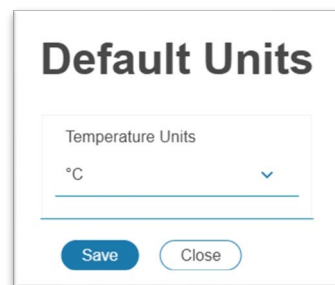


図 123: 温度単位の設定

3. 正しい単位を選択して、[Save] を選択します。

環境センサーを構成する

センサーの場所、アラーム、通知、詳細を構成するために、WEB インターフェイスを開きます。

- 1. [Settings] を開きます。
- 2. Settings ページで [Threshold] セクションを表示します。センサーを構成する閾値を選択します。

Thresholds

Environmental Sensors

Sensor Name	Type	Serial Number	Low Critical	Low Warning	High Warning	High Critical	
	Temperature	CN0111901B EB001 1B T1	18°C	15°C	27°C	32°C	
Sensor Name	Type	Serial Number	Low Critical	Low Warning	High Warning	High Critical	
	Humidity	CN0111901B EB001 1B RH	10	30	60	80	

図 124: 環境センサー閾値構成ビュー

- 3. 目的のセンサーの横にある鉛筆を選択します。
- 4. [Edit] ダイアログボックスに、センサーの名前を入力します
- 5. 上方臨界、上方警報、下方警報、および下方臨界の値を入力し、[Enable] ボックスをチェックします。
- 6. [Save] を選択してセンサーセットアップを終了します。

Edit Temperature Sensors

Sensor Name

Type

Temperature

Serial Number

CN0145911B T1

Low Critical Enable

High Critical Enable

☐ Enable

High Critical (celsius)

32

Delete

☐ Delete

Save

Close

図 125: 温度センサーの編集ダイアログ

セキュリティセンサーを構成する

センサーの場所、アラーム、通知、詳細を構成するために、WEB インターフェイスを開きます。

- 1. [Settings] を開きます。
- 2. Settings ページで [Threshold] セクションを表示します。センサーを構成する閾値を選択します。

Security Sensors					
Sensor Name	Type	Serial Number	Alarm Enable	Alarm Level	
	Door	CN0048966C DOOR SWITCH	Enabled	CRITICAL	
Sensor Name	Type	Serial Number	Alarm Enable	Alarm Level	Alarm State
	Dry	CN0140914E DRYCONTACT	Enabled	CRITICAL	Open 

図 126: セキュリティセンサーアラーム構成ビュー

- 3. 目的のセンサーの横にある鉛筆を選択します。
- 4. [Edit] ダイアログボックスに、センサーの名前を入力します
- 5. [Alarm Level] と [Alarm State] を設定します。
- 6. [Save] を選択してセンサーセットアップを終了します。

Edit Dry Contact Sensor

Sensor Name
Type
Dry
Serial Number
CN0140914E DRYCONTACT
Alarm Enable
☒ Enable
Alarm Level
CRITICAL
Alarm State
Open
Delete
☐ Delete

SaveClose

図 127: ドライ接点センサーの編集ダイアログ

センサーを削除する

1. [Settings] メニューから [Threshold] を選択します
2. 目的のセンサーの横にある鉛筆を選択します
3. [Delete] ボックスをチェックしてから保存します。

セクション 7 – セキュリティハンドル

Panduit EL2P PDU では、ユーザーがキャビネットへのアクセスを電子的に保護し、制御できます。

ハンドルの破損を防ぐために、以下の接続図を参照し、ハーネス部品番号 MA030 および ACF20 を実装するようにしてください。

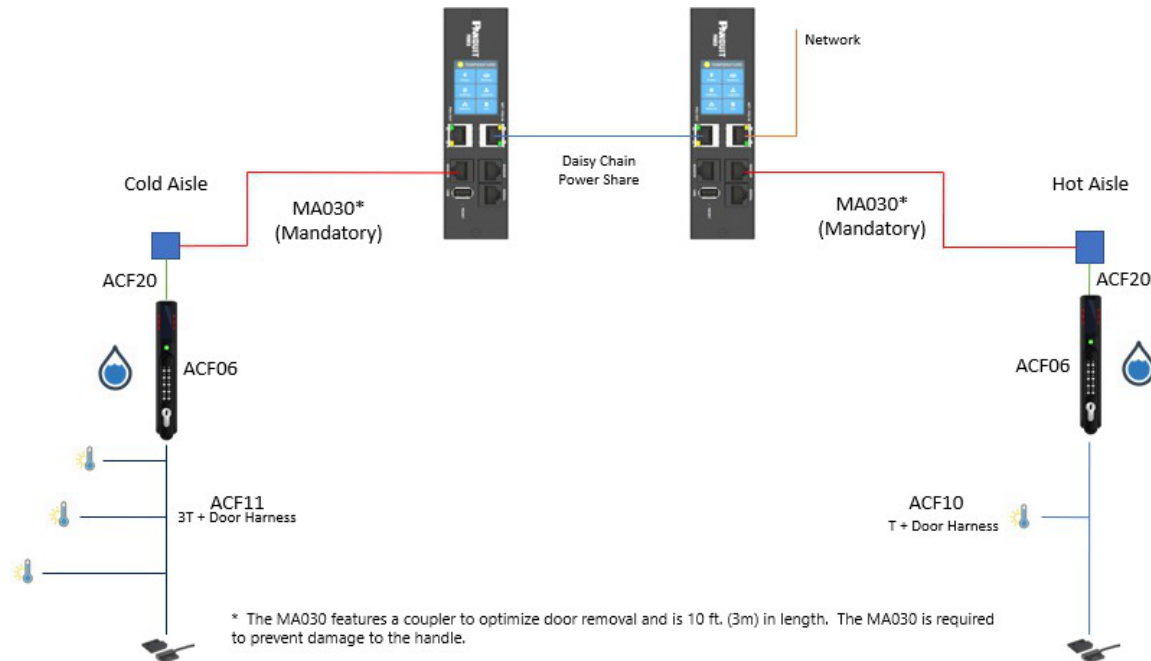


図 128: 接続図

【注意】

セキュリティを確保するため、ロック機構を利用する前にハンドルが固定されていることを確認します。ハンドルが正しく装着される前にハンドルがロックされた場合、ハンドルをロック解除し、正しく装着してから再びロックしてください。管理者権限を持つユーザーのみが、PDU への構成レベルの変更を行うことが許可されています (ラックアクセスセキュリティを含む)。



図 129: セキュリティハンドル

キャビネットアクセスコントロールを構成する

すべてのラックアクセスコントロールの構成は、Web GUI の [Rack Access Control] ページで行うことができます。Web GUI の [Rack Access Control] ページにアクセスするには、以下の手順を実行します。

【注意】

ホットアイルまたはコールドアイルは、電子ハンドルの DIP スイッチで直接選択されます。これは Web インターフェイスの構成項目ではありません。

1. NMC にログインします。
2. 家のアイコン > [Rack Access Control] へ進みます。

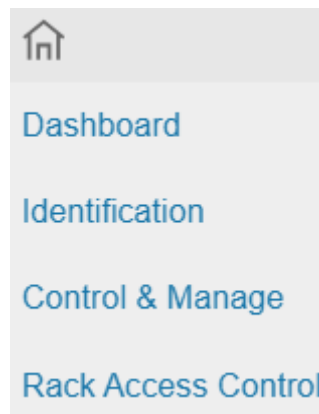


図 130: ラックアクセスコントロール

3. ページの右側にある [Actions] メニューでは、カードの追加、ラックアクセス設定、ハンドル設定、キーパッド設定、リモート制御、ビーコン設定、ステータス LED 設定を行うことができます。



図 131: ラックアクセスコントロールアクション

ローカルラックアクセスのユーザーを追加する

キャビネットへのアクセスが必要なすべてのユーザーは、自分のアクセスカードを PDU に追加する必要があります。各カード (ユーザー) には、ユーザー名と、カード ID またはキーパッド PIN コードが必要です。

【注意】

キャビネットあたり最大 200 件のカードをプログラムできます。

カード ID を調べる

カード ID を調べるには、以下の手順に従います。

1. カードをリーダーの近くに置きます (ハンドルの上部)。
2. [Logs] メニューをクリックし、NMC の [Event Logs] を選択します。

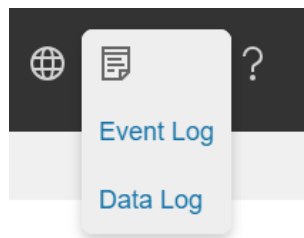


図 132: イベントログ

3. 不正なカード読み取りを示す最も新しいメッセージを探します。
例:

Warning Smart Cabinet Hot Aisle lock is swiped by non-authorized card 192292

4. メッセージの番号がカード ID です。

アクセスユーザーを追加する

1. 新しいカード (ユーザー) を追加するには、[Actions] メニューから [Add Card] を選択します。

Add Card

Card ID

16573691

Username

John

Card PIN

Card Aisle

Both ▼

Temporary User

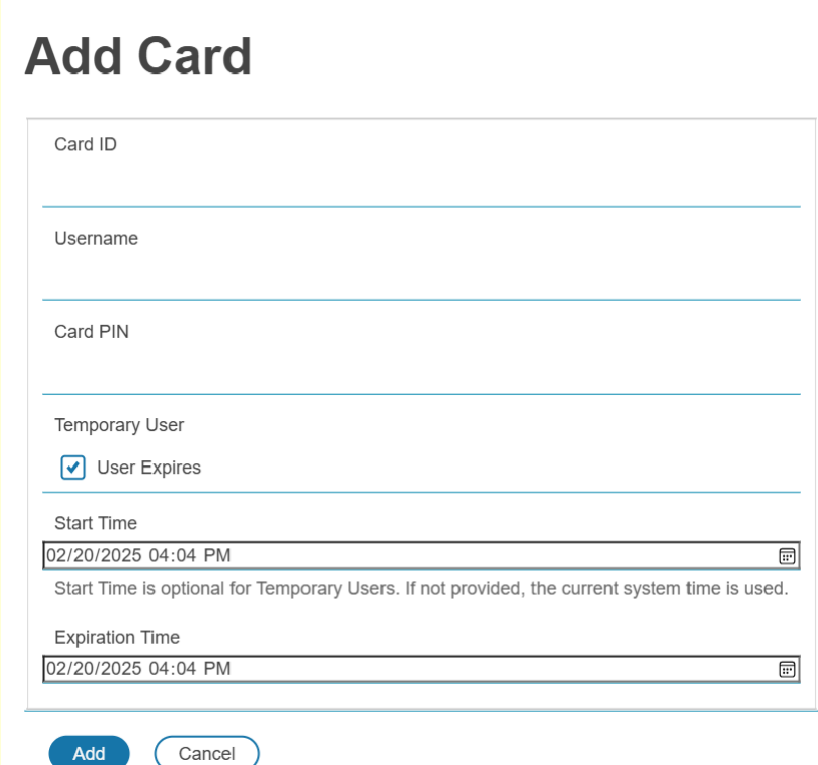
☐ User Expires

Add **Cancel**

図 133: カードの追加

2. ユーザーを特定するユーザー名を入力します。
3. システムが RFID のみまたはデュアル認証で構成されている場合、調べたカード ID を入力します。
【注意】上記の例では、カード ID は 16573691 です。
4. システムがキーパッドのみまたはデュアル認証で構成されている場合、PIN を入力します。
【注意】「キーパッドのみ」モードでは、ユーザーに一意の PIN コードを割り当てる必要があります。

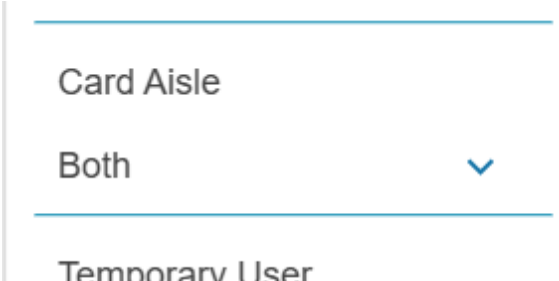
5. ユーザーが一時ユーザーの場合、アクセスは [Start Time] に始まり、[Expiration Time] に終了します。
 - a. [User Expires] を選択します。



The screenshot shows a web form titled "Add Card". It contains several input fields: "Card ID", "Username", "Card PIN", and "Temporary User". Under "Temporary User", the "User Expires" checkbox is checked. Below this are two date/time pickers: "Start Time" and "Expiration Time", both showing "02/20/2025 04:04 PM". A note states: "Start Time is optional for Temporary Users. If not provided, the current system time is used." At the bottom are "Add" and "Cancel" buttons.

図 134: カードの追加 (一時ユーザー)

- b. [Start Time] を選択します。
 - c. [Expiration Time] を選択します。
6. [Rack Access Settings] / [Aisle Control] が [Hot/Cold Standalone] に設定されている場合、[Card Aisle] フィールドを追加で設定できます。
 - a. [Both] - このユーザーは、ホットアイルまたはコールドアイル用に構成されたハンドルに対して有効です。
 - b. [Cold] - このユーザーは、コールドアイル用に構成されたハンドルに対して有効です。
 - c. [Hot] - このユーザーは、ホットアイル用に構成されたハンドルに対して有効です。



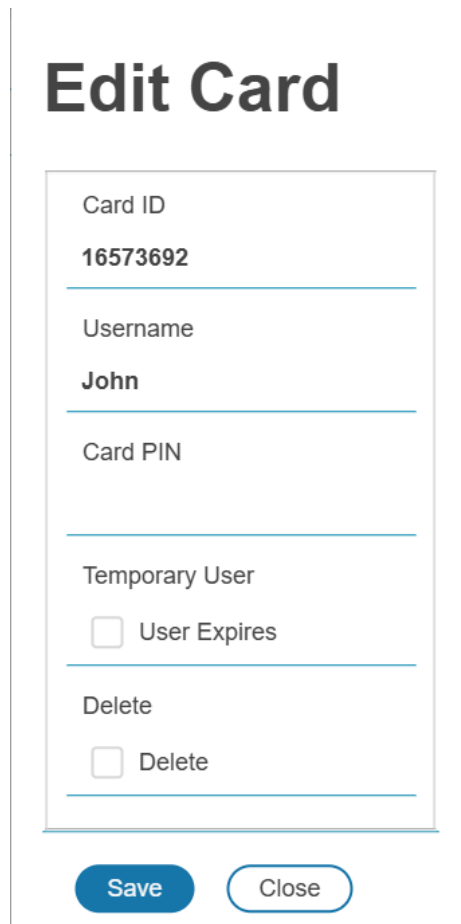
The screenshot shows a dropdown menu labeled "Card Aisle". The selected option is "Both", indicated by a blue checkmark to its right. Below the dropdown is the text "Temporary User".

図 135: カードアイルを指定したカードの追加

7. [Add] をクリックします。

アクセスユーザーを編集する

1. カード (またはユーザー) を編集するには、ユーザーの横にある鉛筆アイコンをクリックします。



The image shows a modal dialog box titled "Edit Card". It contains several input fields and checkboxes. The "Card ID" field is pre-filled with "16573692". The "Username" field is pre-filled with "John". The "Card PIN" field is empty. Below these fields is a "Temporary User" section with a checkbox labeled "User Expires". At the bottom of the form area is a "Delete" section with a checkbox labeled "Delete". At the very bottom of the dialog are two buttons: "Save" and "Close".

Card ID
16573692
Username
John
Card PIN
Temporary User
☐ User Expires
Delete
☐ Delete

Save Close

図 136: カードの編集

2. 必要に応じて [Card ID] を変更します。
3. 必要に応じて [Username] を変更します。
4. 必要に応じて [Card PIN] を入力します。
5. 上記のステップで PIN を変更した場合、[Confirm PIN] を入力します。

6. ユーザーが一時ユーザーの場合、アクセスは [Start Time] に始まり、[Expiration Time] に終了します。
 - a. [User Expires] を選択します。

Edit Card

Card ID

16573692

Username

John

Card PIN

Temporary User

☒ User Expires

Start Time

02/17/2025 05:08 PM

Start Time is optional for Temporary Users. If not provided, the current system time is used.

Expiration Time

02/17/2025 05:08 PM

Delete

☐ Delete

Save

Close

図 137: カードの編集 (一時ユーザー)

- b. [Start Time] を選択します。
- c. [Expiration Time] を選択します。

7. [Rack Access Settings] / [Aisle Control] が [Hot/Cold Standalone] に設定されている場合、[Card Aisle] フィールドを追加で設定できます。
 - a. [Both] - このユーザーは、ホットアイルまたはコールドアイル用に構成されたハンドルに対して有効です。
 - b. [Cold] - このユーザーは、コールドアイル用に構成されたハンドルに対して有効です。
 - c. [Hot] - このユーザーは、ホットアイル用に構成されたハンドルに対して有効です。

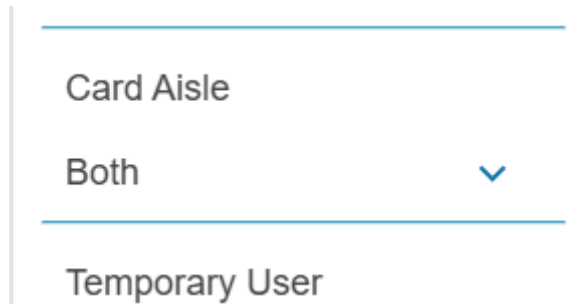


図 138: カードアイルを指定したカードの追加

8. [Save] をクリックします。

アクセスユーザーを削除する

1. カード (またはユーザー) を削除するには、ユーザーの横にある鉛筆アイコンをクリックします。
2. [Delete] ボックスをチェックします。
3. [Save] をクリックします。

ラックアクセス設定を構成する

ラックアクセス設定は、システム全体で共通です。これらには、[Aisle Control]、[Autolock Time]、[Door Open Time]、[Max Door Open Time] などがあります。

1. ラックアクセス設定を更新するには、[Actions] メニューから [Rack Access Settings] を選択します。

Rack Access Settings

Aisle Control
Hot/Cold Combined

Autolock Time (s)
10

Door Open Time (s)
20

Max. Door Open Time (s)
10

Authentication Mode
RFID & Keypad (Dual Auth)

Save Close

図 139: ラックアクセス設定

2. [Aisle Control] の 2 つのオプションから選択します。
 - a. [Hot/Cold Combined] – ホットアイルまたはコールドアイルで操作するとき、両方のハンドルが開きます。
 - b. [Hot/Cold Standalone] – ホットアイルとコールドアイル、それぞれ無関係に動作します。
3. [Autolock Time] は、ハンドルが自動的にロックされるまでの秒数です。
4. [Door Open Time] は、ドアが開いたことのアラートをハンドルが出してから秒数です。
5. [Max. Door Open Time] は、ドアが開いたことの重大アラームが通知されるまでの秒数です。
6. 目的の [Authentication Mode] を選択します。
 - a. [RFID & Keypad (Dual Auth)] – 最初に承認済みのカードを読み取り、5 秒以内に承認済みのシークレット PIN のキーパッドへの入力を開始します。
 - b. [RFID Only] – 承認済みのカードをスワイプしてキャビネットにアクセスします
 - c. [Keypad Only] – 承認済みのシークレット PIN をキーパッドに入力してキャビネットにアクセスします。
7. [Save] をクリックします。

ハンドル設定を構成する

ハンドル設定および特定のハンドルに関する情報を構成します。これらにはアクセスコントロールユニット (ACU) 名が含まれます。

1. ハンドル設定を更新するには、[Actions] メニューから [Handle Settings] を選択します。

Handle 1 Settings

Handle
UPS - Cold Aisle

ACU Name
HID

Sensor Harness Configuration
No sensor

Firmware Version
app ver 4.1

Reader Version
rfid ver 1.5

Hardware Version
hw ver 6944

Serial Number
CN014892BB HID

Delete
☐ Delete

Save Close

図 140: ハンドル設定

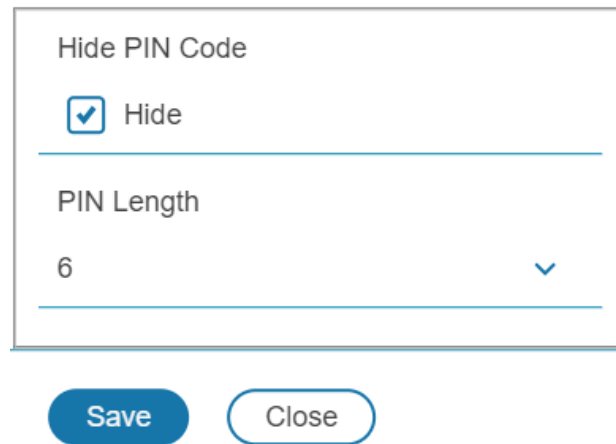
2. [ACU Name] に入力します。ACU 名は異なるハンドルを識別するための名前です。このフィールドには英数字を入力し、特殊文字も使用できます。
3. セキュリティハンドルに接続されているセンサーハーネスを選択します。
4. [Firmware Version]、[Hardware Version]、および [Serial] は、ハンドルについての読み取り専用属性です。
 - a. [Firmware Version] は、ハンドルで実行されているファームウェアバージョンです。
 - b. [Hardware Version] は、ハンドルのハードウェアのバージョンです。
 - c. [Serial Number] は、ハンドルのシリアル番号です。
5. システムからハンドルを削除するには、ハンドルを外し、[Delete]ボックスをチェックします。
6. [Save] をクリックします。

キーパッド設定を構成する

認証モードがキーパッドのみまたはデュアル認証の場合、すべてのユーザーは同じ PIN の長さに従う必要があり、「キーパッドのみ」モードではユーザーは一意の PIN コードを選択する必要があります。

1. キーパッド設定を更新するには、[Actions] メニューから [Keypad Settings] を選択します。

Keypad Settings



Hide PIN Code

☒ Hide

PIN Length

6

Save Close

図 141: キーパッド設定

2. Web UI で PIN コードを非表示にするには、[Hide Pin Code] ボックスをチェックします。
3. 必要な PIN の長さを設定します。PIN の長さは 1 桁から 16 桁まで指定できます。

ハンドルをリモート制御する

リモート制御では、ハンドルをリモートで開いたり閉じたりできます。

1. ハンドルをリモート制御するには、[Actions] メニューから [Remote Control] を設定します。

Remote Control

Handle	Name		
1 - PDU - Cold Aisle	LHID	Lock	Unlock

Close

図 142: リモート制御

2. 実行するアクションを選択します。
 - a. [Lock] を選択すると、ハンドルをリモートでロックします。
 - b. [Unlock] を選択すると、ハンドルをリモートでロック解除します。
3. 終了したら、[Close] をクリックします。

ビーコンを制御する

ビーコンは、キャビネットのステータスを一目で伝える視覚的なインジケータです。ビーコンは、システムが警報アラームのときは黄色で点滅し、重大なアラームのときは赤色で点滅します。また、ビーコンの位置指定機能を使用して、ビーコンを特定の色で点滅させて、システムの位置を簡単に見つけることもできます。ビーコン LED のデフォルト状態は緑色で点灯です。



図 143: ビーコン

ビーコン LED の表

機能	状態	色	目的
位置指定	点滅	赤、緑、青、黄、マゼンタ、アクア、白	ラックの場所を特定します(カスタマイズ可能)
重大アラーム	点滅	赤	システムの重大アラーム(カスタマイズ不可)
警報アラーム	点滅	黄	システムの警報アラーム (カスタマイズ不可)
通常状態	点灯	赤、緑、青、黄、マゼンタ、アクア、白	ハンドルの視覚的インジケータ (カスタマイズ可能)

1. ハンドルビーコンを制御するには、[Actions] メニューから [Beacon Settings] コントロールを選択します。

Beacon Settings

Function	
Standby	▼
Color	
Blue	▼

SaveClose

図 144: ビーコン設定

2. ビーコンの機能を選択します。
 - a. [Locate] – ビーコンが点滅。
 - b. [Standby] – 警報がないときのビーコンの色。
3. [Standby] または [Locate] の色を選択します。
4. [Save] をクリックします。

ステータス LED

セキュリティハンドルにはステータス LED があり、ハンドルおよびセキュリティのステータスを視覚的に表示します。すべてのステータス LED の状態を以下の表に示します。ステータス LED のデフォルト状態は緑色で点灯です。

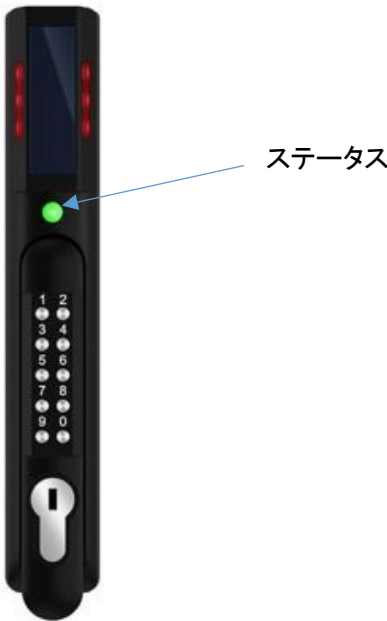


図 145: ステータス LED

ステータス LED の表 (重要度順)

ステータス LED の色	説明
スタンバイ - 点灯 (またはオフ)	スタンバイ状態でのお客様が選択可能な色。(カスタマイズ可能)
赤 - 点滅	3 回点滅して認証エラーを示す (カスタマイズ不可)
緑 - 点滅	ロックが開いている (カスタマイズ不可)
マゼンタ - 点滅	ロック解除のためにキーが使用されたか機械的ハンドルが基部から外された (カスタマイズ不可)
黄 - 点滅	ドア開放時間以内でハンドルが開いている (カスタマイズ不可)
赤 - 点灯	自動ロック時間よりも長くロックが開いている。(障害物を探す) (カスタマイズ不可)
赤 - 点灯	最大ドア開放時間よりも長くドアが開いている (ドアセンサー) (カスタマイズ不可)

- 【注意】ドア開放センサーの状態は、開いているシステムに接続されている近くのいずれかの接点センサーの状態です。ドア開放センサーの状態は、機械的ロック解除の状態とは同じではありません。ハンドルのドアセンサーにハーネスがある場合、ハーネスが構成されていることを確認してください。
- 【注意】ドアセンサーの閾値はデフォルトで [Alarm Enabled] に構成され、[Alarm Level] が [Critical] に設定して構成されています。これは [Door Open Time] および [Max Door Open Time] アラームよりも優先されます。要件を満たすように、ドアセンサーの [Alarm Level] と [Alarm Enabled] の設定をカスタマイズしてください。

ステータス LED の状態を設定する

- 1. ステータス LED の状態をスタンバイ状態に設定するには、[Actions] メニューから [Status LED Settings] を選択します。

Status LED Settings

Color

Blue

▼

Save

Close

図 146: ステータス LED 設定

- 2. ハンドルがスタンバイ状態のときのステータス LED の色を選択します。
- 3. [Save] をクリックします。

ハンドルおよび互換カードの種類

以下の表は、それぞれのスイングハンドルでサポートされるカードを示します。

	MIFARE® Classic 1k	MIFARE Plus® 2k	MIFARE® DESFire® 4k	HID® CLASS	HID® 125kHz Prox	EM 125kHz Prox	Output
ACF05							
ACF06	UID	UID	UID	UID	CSN	CSN	専用
ACF06L							

CSN = カードシリアル番号 / UID = 一意の ID

セクション 8 – セキュリティ

この製品には、ユーザーが入力したデータを格納するソフトウェアが搭載されています。ユーザーが入力したすべてのデータは、ソフトウェアを実行するシステムの不揮発性ストレージに格納されます。

適合規格

この製品は、規格「UL 2900-1: 2023 Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, ANSI/CAN/UL 2900-1, Second Edition, Dated December 13, 2023」の要件を満たすことが評価により確認されています。テスト報告番号: 4791828948-001

プライマリ機能への API アクセス

- 製品にはシステムを構成および制御するための API が提供されています。
- Web サーバーには、システムを管理するために Web GUI フロントエンドに使用されるバックエンド REST API が提供されています。
- Web サーバーには、システムを管理するための Redfish API が提供されています。
- USBポートは、LCD画面上のボタンを押すことで起動する「設定のダウンロード」、「設定のアップロード」、および「ファームウェアのアップグレード」機能へのAPIアクセスを提供します。
- USB設定アップロード機能は、管理者権限で実行されます。

プライマリ機能

API アクセスにより、承認または許可されたユーザーが、製品の操作に不可欠な製品機能を制御することができます。API によっては、一部の機能が使用できないことがあります。詳しくは、API ドキュメントを参照してください。

- API ユーザーは、制御可能なアウトレットのある製品のアウトレット電源をオンおよびオフにすることができます。
- API ユーザーは、制御可能なアウトレットのある製品のアウトレット電源をオンおよびオフにする機能を有効化および無効化することができます。

安全処理機能

- この製品には、製品の押しボタンを使用するか、Web ユーザーインターフェイス、SSH コマンドラインインターフェイス、または RJ45 シリアルインターフェイスから作動できる「デフォルト設定」機能が提供されています。
- デフォルト設定機能は、構成データを格納しているフラッシュファイルシステムから、暗号化された不揮発性ストレージファイルを削除し、構成データをデフォルト設定に再初期化します。
- NMC が PDU に接続されると、デフォルト設定機能は、PDU に格納されているフラッシュファイルシステムから、暗号化された不揮発性ストレージファイルを削除します。
- デフォルト設定機能は、イベントログおよびデータログを格納しているフラッシュファイルシステムからファイルを削除します。
- デフォルト設定機能は、ファームウェア更新アップロードを一時的に格納するためのフラッシュファイルシステムから一時ファイルを削除します。
- デフォルトへのリセット機能は、SSH RSA 3072 ビットプライベートホストキーを再生成します。
- デフォルトへのリセット機能は、SSH ED25519 256 ビットプライベートホストキーを再生成します。
- 廃棄するユニットで“デフォルト設定”機能を実行できない場合、またはデバイス上のフラッシュメモリからイベントログやデータログファイルが取り出されることを防止したい場合は、デバイスの PCBA を物理的に破壊する必要があります。

セキュア消去 — NIST SP 800-88 準拠のデータ抹消処理

概要

デバイスには、不揮発性ストレージに保存されたユーザー設定データをすべて消去する、ユーザー操作によるセキュア消去機能が実装されています。この手順は以下の 2 つのストレージデバイスを対象としています。

ストレージ	場所	内容
eMMC (マネージド NAND)	NMC カード	ユーザー構成、ログ、認証情報
SPI NOR フラッシュ	PDU バックプレーン	PDU 構成データ

NIST SP 800-88 Rev. 1 の分類

NIST Special Publication 800-88 Rev. 1「媒体のデータ消去に関するガイドライン」では、3 つのデータ抹消レベルが定義されています。

レベル	説明
消去 (Clear)	固定データパターンで上書きします。単純な非侵襲の復旧 (標準の OS ツールまたはファイル復旧ツール) から保護します。
除去 (Purge)	最先端の研究室レベルの技術を使用しても復旧が不可能になる、媒体固有のコマンドまたは技術を使用します。
破壊 (Destroy)	媒体を物理的に使用不能にします (シュレッダー処理、焼却など)。

対象	NIST レベル	理由
eMMC (NMC)	除去	表 A-8 に従って eMMC の Secure Erase および Sanitize コマンドを使用する
SPI NOR (バックプレーン)	消去	SPI NOR にはデバイス内部の Sanitize コマンドが存在せず、消去+上書きはホストレベルの技術である

それぞれの手順とその分類に関する詳細な説明を以下に示します。

eMMC 除去手順 (NMC)

eMMC の除去では、JEDEC eMMC 規格 (JESD84-B51) によって定義されたコマンドを使用します。これらのコマンドは、フラッシュ変換レイヤー (FTL) を備えたフラッシュメディアに対する Purge レベルのデータ抹消処理に適したもので、NIST SP 800-88 § 2.4 に明示的に記載されています。

手順

1. **デバイスの識別** — メーカー ID、モデル名、シリアル番号、および CID がログに記録され、NIST § 4.7 に従い監査可能なデータ抹消処記録が作成されます。
2. **セキュアな破棄** (blkdiscard -fs) — eMMC SECURE ERASE/SECURE TRIM コマンドをフラッシュコントローラに発行します。コントローラは、FTL によって再マッピングされたセルやスベアブロックとして予約されたセルも含め、NAND の物理ページを物理消去対象としてマークします。

3. **データ抹消処理** (mmc sanitize) – eMMC SANITIZE コマンドを発行します (CMD6, EXT_CSD[165])。このコマンドにより、以前にマッピング解除、破棄、または Trim されたすべてのブロックが物理的な消去対象となります。これには、ホストからの読み取りではアクセスできないオーバープロビジョニング領域も含まれます。これは、この手順を Clear (消去) から Purge (除去) レベルへ引き上げる重要なステップです。
4. **確認** – パーティション全体を親ブロックデバイス経由で再度読み出し、パーティションアライメントに依存せず、全領域がゼロ化されていることを確認します。

この手順が Purge に該当する理由

NIST SP 800-88 表 A-8 (フラッシュメモリベースのストレージデバイス) には次のことが記載されています。

除去: デバイス内部の Sanitize コマンドを使用するか (サポートされている場合)、ブロック消去の後で Sanitize コマンドを使用する。

この実装ではこのガイダンスに正確に従っています。つまり、セキュアな破棄の後に eMMC Sanitize コマンドを実行し、消去後の確認を行っています。

SPI NOR フラッシュ消去手順 (バックプレーン)

バックプレーンの SPI NOR フラッシュにはフラッシュ変換レイヤーがなく、ホストの書き込みと消去は物理セルに直接到達します。隠れたスペアブロックやウェアレベリングの再マッピング、オーバープロビジョニングされた領域は存在しません。

1. **デバイスの識別** – MTD デバイス名、JEDEC ID、製造元、部品名、タイプ、およびサイズがログに記録されます。
2. **初期消去** (flash_erase) – すべての消去ブロックが 0xFF に設定されます (NOR フラッシュの消去済み状態)。もう一度読み出すことによって確認されます。
3. **ランダムデータ上書き** – OpenSSL 経由の AES-256-CTR を使用して、/dev/random から取得したシードに基づく確定的な疑似ランダムストリームを生成します。このストリームはデバイス全体に書き込まれ、その後、同一のストリームが再生成されてデバイスの内容とバイト単位で比較されることによって検証されます。この処理により、すべてのセルが非消去状態にプログラムされるため、全セルが完全なプログラム/消去サイクルを一巡します。
4. **最終消去** (flash_erase) – すべての消去ブロックを再び 0xFF 状態に消去し、その結果を確認します。

この手順が Clear に該当する理由 (Purge ではなく)

NIST SP 800-88 表 A-8 では、フラッシュストレージの Purge (除去) をデバイス内部の Sanitize コマンドを必要とする処理として定義しており、これはホストがアクセスできない領域 (オーバープロビジョニングされたブロックや、再マッピングされたセクターなど) に到達するファームウェアレベルの処理です。一方、SPI NOR にはそのようなコマンドがなく、ホストから実行される論理的な消去手法である flash_erase および write 操作が用いられるため、その実行回数にかかわらず、NIST では Clear (消去) に分類されています。

しかし、実際のセキュリティ対策としては、以下に示すように、Clear の最小要件を超える処理が実施されます。

- **FTL がないことは隠されたデータがないことを意味します。** マネージド NAND (eMMC、SSD) に対する Purge の主な理由である、FTL が管理するスเปアブロックへのデータの隠ぺいは、SPI NOR には当てはまりません。すべての物理セルは、ホストによって直接アドレス指定可能です。
- **3 回の検証付き処理。** 消去 → ランダム上書き → 消去というサイクルにより、すべてのセルが確認を伴う完全なプログラム/消去サイクルを一巡します。これは、固定パターンによる 1 回の上書きという Clear の最小要件を上回るものです。
- **残留電荷の復元は実用的ではありません。** 現在の NOR フラッシュ技術では、研究室レベルの手法 (浮動ゲート電荷の電子顕微鏡解析など) を用いても、完全な消去サイクル後に以前のセル状態を復元することは現実的ではないと考えられています。

SPI NOR を正式に NIST の Purge に分類するためには、SPI コマンドレベルで利用可能なベンダー固有のチップ消去コマンドやセキュリティ消去コマンド (JEDEC で定義された Security Register Erase など) が必要になります。しかし、このような機能は一般的な SPI NOR デバイスには実装されていません。

トリガーおよび実行フロー

ユーザーが `/control/mgmtModuleCtrl/secureErase` を設定



`secureErase`

- ターゲットパーティションをワイプフラグファイルに書き込む
- デバイスをリブートする



`init (initramfs)`

- ワイプフラグファイルを検出する
- 構成からパーティションリストを読み取る
- パーティションごとに `erase_partition.sh` を実行する
- 結果をログに記録する

ログへの記録と監査

各消去処理では、タイムスタンプ付きのログ (`/tmp/secure-erase.log`) が生成され、これには以下が含まれます。

- デバイスの識別 (製造元、モデル、シリアル/JEDEC ID)
- 各消去ステップおよびその成功/失敗ステータス
- 確認結果

これらのフィールドにより、データ抹消処理が適切に実施されたことを確認し、その対象となった媒体を特定できるため、NIST SP 800-88 § 4.7 の推奨事項を満たすことができます。

制限事項

- **ファームウェア/ブートパーティションは消去されない** – この手順はユーザーデータのパーティションのみが対象です。デバイスをブート可能な状態に維持するため、NMC ブートパーティションとバックプレーンのファクトリ領域は意図的に保持されます。
- **ウェアレベリングされたスペアブロック (eMMC)** – eMMC Sanitize コマンドは、スペアブロックやオーバプロビジョニング領域を対象としていますが、最終的な消去範囲はコントローラの実装に依存します。

参考文献

- NIST SP 800-88 Rev. 1「*媒体のデータ抹消処理に関するガイドライン*」、2014 年 12 月。
<https://doi.org/10.6028/NIST.SP.800-88r1>
 - § 2.4 – データ抹消処理のトレンド (フラッシュ固有の考慮事項)
 - § 4.7 – 確認と文書
 - 表 A-8 – フラッシュメモリベースのストレージデバイス (Clear/Purge/Destroy)
- JEDEC JESD84-B51 – eMMC 電気規格、§ 6.6.40 (Sanitize)、§ 6.6.10 (Secure Erase/Secure Trim)

不揮発性ストレージ

- この製品では、暗号化された不揮発性ファイルを使用して構成情報を格納します。
- この製品は業界標準の暗号化アルゴリズムを使用して、不揮発性構成データを保護します。sha512 ハッシュおよび PBKDF2 鍵導出を使用した aes-256-cbc アルゴリズムが使用されます。暗号鍵は内部 HSM に格納されます。

認証データ

- ユーザー名は不揮発性メモリに格納され、システムへのアクセスの管理のために、「管理者」の役割ユーザーに使用されます。
- ソフトウェアを管理するために使用されるパスワードは、一方向の bcrypt ハッシュとして格納されます。
- ユーザーが入力するパスワードはお客様に返されません。(これらはユーザーから見て「書き込み専用」です。)
- プレーンテキストで提供する必要がある外部サービス認証資格情報 (RADIUS、LDAP、TACACS+) は、暗号化された不揮発性ストレージに格納されます。
- SNMP v1/v2c コミュニティ文字列は、暗号化された不揮発性ストレージに格納されます。
- SNMP v3 のユーザー名およびパスワードは、暗号化された不揮発性ストレージに格納されます。

認証の優先順位

認証では、有効化された認証ドメインごとに、次の順序で資格情報をチェックします。

- ユーザーアカウント
- RADIUS
- LDAP
- TACACS+

ユーザーアカウント認証ドメインは無効化できません。

ユーザーが 1 つのドメインに存在しない場合、その次の有効な認証ドメインがチェックされます。

パスワードが異なり、想定される権限レベルの異なる単一の有効なユーザー名を複数のドメインで定義しないでください。これを定義すると、予期しない権限が付与されることになる可能性があります。

ネットワーク転送セキュリティ

- この製品は、初回起動時にランダムな SSH RSA 3072 ビットのプライベートホストキーを生成します。
- この製品は、初回起動時にランダムな SSH ECDSA 256 ビットのプライベートホストキーを生成します。
- この製品には、工場出荷時に構成されたランダムに生成された RSA 2048 ビットのプライベートキーが付属しています。この鍵は、製品が最初に起動するときに HTTPS 証明書を生成するために使用されます。
- ユーザーはカスタムの HTTPS 証明書とプライベートキーをアップロードできます。
 - HTTPS 証明書では SHA-256 署名を使用する必要があります。
 - プライベートキーは RSA 2048 ビットまたは prime256v1 (SECP256R1) である必要があります。
 - 他の種類のプライベートキーが機能する場合がありますが、使用するプライベートキーのサイズが大きくなると、パフォーマンスに悪影響を及ぼすことがあります。(RSA 3072 ビット、RSA 4096 ビット。楕円曲線暗号: SECP192R1、SECP224R1、SECP256R1、SECP384R1、SECP521R1、SECP192K1、SECP224K1、SECP256K1、BP256R1、BP384R1、BP512R1、CURVE25519)
- ユーザーは、パスワードを使用して暗号化されたカスタムの HTTPS プライベートキーをアップロードできます。プライベートキーの復号は、デフォルトの openssl AES パスワード暗号化形式と互換性があります。
- プライベートキーが .pfx または .p12 ファイルに格納されている場合は、openssl を使用してパスワードで暗号化された PEM 形式に変換できます。詳しくは、openssl ドキュメントを参照してください。

例:

 - `openssl pkcs12 -in [yourfile.p12] -nocerts -nodes -passin pass:[input_password] | openssl rsa -aes256 -out [privatekey.pem] -passout pass:[new_password]`
- この製品は TLS 1.2 または TLS 1.3 を使用して HTTPS Web ブラウザクライアントと通信します。
- HTTPS クライアントとのセキュア通信暗号ネゴシエーションでは以下の暗号スイートを使用します。
 - 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - 暗号スイート: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc03c)
 - 暗号スイート: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - 暗号スイート: TLS_AES_256_GCM_SHA384 (0x1302)
 - 暗号スイート: TLS_AES_128_GCM_SHA256 (0x1301)
- この製品は TLS 1.2 または TLS 1.3 を使用して、SMTP+STARTTLS および SMTPS サーバーと通信します。

- SMTP サーバーおよび LDAP サーバーとのセキュア通信暗号ネゴシエーションでは、以下の暗号スイートを使用します。

- 暗号スイート: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- 暗号スイート: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- 暗号スイート: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- 暗号スイート: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- 暗号スイート: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- 暗号スイート: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- 暗号スイート: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
- 暗号スイート: TLS_AES_128_GCM_SHA256 (0x1301)
- 暗号スイート: TLS_AES_256_GCM_SHA384 (0x1302)
- 暗号スイート: TLS_AES_128_CCM_SHA256 (0x1304)
- 暗号スイート: TLS_AES_128_CCM_8_SHA256 (0x1305)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- 暗号スイート: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- 暗号スイート: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- 暗号スイート: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- 暗号スイート: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- 暗号スイート: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- 暗号スイート: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- 暗号スイート: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- 暗号スイート: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- 暗号スイート: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- 暗号スイート: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- 暗号スイート: TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- 暗号スイート: TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- 暗号スイート: TLS_RSA_WITH_ARIA_128_CBC_SHA256 (0xc03c)
- 暗号スイート: TLS_RSA_WITH_ARIA_256_CBC_SHA384 (0xc03d)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 (0xc048)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 (0xc049)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256 (0xc04a)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384 (0xc04b)
- 暗号スイート: TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256 (0xc04c)

- 暗号スイート: TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384 (0xc04d)
- 暗号スイート: TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256 (0xc04e)
- 暗号スイート: TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384 (0xc04f)
- 暗号スイート: TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050)
- 暗号スイート: TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05e)
- 暗号スイート: TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05f)
- 暗号スイート: TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)
- 暗号スイート: TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)
- 暗号スイート: TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256 (0xc062)
- 暗号スイート: TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384 (0xc063)
- 暗号スイート: TLS_RSA_WITH_AES_128_CCM (0xc09c)
- 暗号スイート: TLS_RSA_WITH_AES_256_CCM (0xc09d)
- 暗号スイート: TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)
- 暗号スイート: TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
- 暗号スイート: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
- この製品では、SSH クライアントと通信するために、SSH サーバーに以下のアルゴリズムを提供しています。
 - キー交換アルゴリズム:
 - curve25519-sha256
 - curve25519-sha256@libssh.org
 - ecdh-sha2-nistp521
 - ecdh-sha2-nistp384
 - ecdh-sha2-nistp256
 - diffie-hellman-group14-sha256
 - kexguess2@matt.ucc.asn.au
 - kex-strict-s-v00@openssh.com
 - ホストキーアルゴリズム:
 - rsa-sha2-256 (2048 ビット)
 - 暗号化アルゴリズム:
 - chacha20-poly1305@openssh.com
 - aes128-ctr
 - aes256-ctr
 - MAC アルゴリズム:
 - hmac-sha2-256

ネットワーク構成データ

- ネットワーク構成 (静的 IP アドレスおよび DHCP によって取得したアドレスなど) は、製品のネットワーク管理に役立つように「Identification」ページおよび Network Configuration ページに公開されています。
- この製品では内部認証メカニズムが実装されており、承認イベントが生成する「イベントログ」には、成功したログインの IP アドレスとユーザー名、および失敗したログインの IP アドレスが格納されます。

ログへの記録

- イベントログ、メール、および SNMP トラップに送信されるイベントログメッセージやアラームメッセージには、操作を実行したユーザーのユーザー名や IP アドレスが含まれる場合があります。
- データログとイベントログでは、ログの内容が変更された後に新たな閲覧者がアクセスすると、その都度 “Log is downloaded by user” というメッセージが生成されます。

外部認証メカニズム

- LDAP & RADIUS - ユーザー名およびパスワードは、暗号化された不揮発性ストレージに格納されます。
- CVE-2024-3596 BlastRADIUS: ファームウェアには BlastRADIUS の脆弱性緩和のために有効にしておく必要のある [Always send Message- Authenticator Attribute] 機能が含まれています。
- LDAP はネットワーク上で暗号化されません。
- LDAPS および LDAP with StartTLS はネットワーク上で暗号化されます。
- [Server Certificate] が構成されて、[Verify Server Certificate] が有効化された場合、リモート LDAP サーバーの真正性が検証されます。
- ユーザーは LDAP クライアントプライベートキーパスワードを使用して、暗号化されたカスタムの LDAP クライアントプライベートキーをアップロードできます。プライベートキーの復号は、デフォルトの openssl キー生成パスワード暗号化形式と互換性があります。
- RADIUS プロトコルは、ハッシュ済みおよび難読化済みのパスワードをネットワーク上で送信するためのみに設計されています。
- TACACS+ プロトコルは、ハッシュ済みおよび難読化済みのパスワードをネットワーク上で送信するためのみに設計されています。

セキュアブート保護

- この製品は、業界標準のコード署名アルゴリズムを使用して、デバイスによってブートされたファームウェアを保護します。
- 署名ブロックがブートローダーおよび内部 HSM に追加されます。
- 署名ブロックには、ブートローダーおよび RSA 3072 ビットのパブリックキーの署名が格納されています。
- RSA 3072 ビットのパブリックキーのダイジェストは 1 回限り書き込み可能な (設定後は読み書きできない) eFuse に格納され、署名ブロックを確認するために使用されます。
- パブリックキーの署名は署名ブロックおよびブートローダーのダイジェストと照らして確認され、ブートローダーの真正性と整合性が確立されます。
- ブートローダーはアプリケーションの実行ファイルの真正性と整合性を確認することによって信頼チェーンを維持します。

ファームウェアの更新の保護

- この製品では業界標準の暗号化を使用してファームウェアの更新パッケージを確認し、真正性と整合性を確立します。
- このパッケージには、パッケージペイロードに格納されている項目を説明するマニフェストが格納されています。
- 項目は、各サブ項目のチャンクサイズと SHA256 ハッシュ、およびパッケージ内のペイロードコンテナとして記載されます。
- マニフェストは SHA256 を使用してハッシュ化され、RSA 4096 ビットキーを使用して署名されます。
- このパッケージには、マニフェストのハッシュの署名が格納されます。
- パッケージには、サブ項目を保持するペイロードコンテナが格納されます。
- マニフェストまたはペイロードの内容を解釈する前に、ペイロードのシグネチャが確認されます。
- ファームウェアアプリケーションのイメージでは AES 暗号化と RSA シグネチャを使用して、秘密性、真正性、および整合性を確保します。

その他の機能

- この製品には、給電されない短い時間の間に時刻を保持するリアルタイムクロックとコンデンサが搭載されています。NTP と組み合わせることで、ログへの正確なタイムスタンプが記録されます。

プロトコル

- この製品は mDNS (UDP ポート 5353) と LLMNR (UDP ポート 5355) に対応しており、MacOS や Windows から “pdu-<Mac アドレス>.local” を使用してデバイスへ簡単に接続できます。ホスト名が構成されている場合、“pdu-<Mac アドレス>” の代わりにホスト名が使用されます。

安全な設置

パンドウイトでは、製品使用時のセキュリティの観点から、以下の事項を推奨します。

- この製品は、物理的なセキュリティが確保された場所に設置してください。可能であれば、セキュリティが確保されたデータセンター内の施錠されたキャビネットに設置することを推奨します。
- シリアルケーブル、センサーケーブル、および USB ケーブルは、これらのインターフェイスの通信が暗号化されていないため、セキュリティが確保されていないエリアに敷設しないでください。

NMC の各項目は以下のように設定してください。

NTP

イベントログや通知で正確なタイムスタンプが使用されるように、信頼できる NTP (Network Time Protocol) サーバーを設定してください。

HTTPS 証明書およびプライベートキーをアップロードする

証明書により、デバイスの HTTPS サーバーとの暗号化接続が正当なものであることを確認できます。X.509 サーバー証明書を NMC にアップロードし、証明書で RSA 2048 ビットキーを使用することをお勧めします。[HTTPS Certificate] と [HTTPS Private Key] には、**[Settings] → [Network settings] → [Web Access Configuration]** からアクセスできます。

Web Access Configuration

HTTP Access

☐ Enable

HTTP Port

80

HTTPS Access

☒ Enable

HTTPS Port

443

HTTPS Certificate

Choose File

No file chosen

HTTPS Private Key

Choose File

No file chosen

Provide a private key password if the private key is encrypted.

HTTPS Private Key Password

Confirm Password

Save

Close

図 147: SSL 証明書のロード画面

SNMPv3c を使用する

Panduit PDU NMC では、SNMPv2c および SNMPv3 の両方がサポートされています。設置のセキュリティを高めるために、SNMPv2c を無効にすることをお勧めします。さらに、すべての SNMPv3 ユーザーおよびトラップレシーバーを「Auth Priv」セキュリティレベル（認証アルゴリズム SHA-512 およびプライバシーアルゴリズム AES256）で構成することをお勧めします。

「Always send Message-Authenticator Attribute」を有効にして RADIUS を使用する

RADIUS クライアントが Message-Authenticator 属性を送信することを常に要求するように RADIUS サーバーを構成する必要があります。

使用しないインターフェイスを無効化する

デフォルトの設定は、HTTPS および SSH を有効化することです。これらのインターフェイスを使用しない場合は、無効にしておくことをお勧めします。

使用しない物理ポートは、「ロックアウト」プラグを使用して保護することができます。

USB ポートはデフォルトで有効になっています。USB ポート経由の管理操作を行うには、手動で USB フラッシュドライブを挿入し、LCD 画面のインターフェイスから実行する操作を選択する必要があります。USB 構成のアップグレード/ダウングレード機能およびファームウェアアップグレード機能は、使用しない場合は無効にできます。無効化するには、次のようにします。

- シリアル CLI または SSH: ログインして、「write config/screen/usbScreen 0」を実行します。
- Web UI: [Settings] / [System Management] / [LCD Configuration] に移動し、鉛筆アイコンをクリックし、[USB Port] の [Enable] のチェックを外し、[Save] ボタンをクリックします。

セッション管理を見直す

NMC では、お客様はセッション管理設定を柔軟に変更できます。

自動ファームウェアアップグレード

パンドUITでは製品のファームウェアをアップデートしています。「付録 A: ファームウェアの更新手順」を参照してください。ローカルサーバーを指すように自動ファームウェアアップグレードを構成し、PDU を自動で最新の状態に保つようにします。詳しくは「自動アップデート」の章を参照してください。構成されたファームウェア URI および構成 URI に格納されているリソースのアップデートは、許可された作業員のみが更新できます。

TLS サーバー証明書の確認

この製品によって実装されたプロトコルには、オプションの TLS サーバー証明書の確認が含まれる場合もあります。TLS 構成がセキュリティ要件を満たすことを確認してください。ベストプラクティスとして、[Server Certificate] (サーバー証明書または信頼された認証局の証明書) を設定し、適切な [Verify Certificate]、[Verify Server Certificate]、または [Verify Server] オプションを有効にします。サーバー証明書の確認によって、NMC は構成されたサーバーの真正性を確認できます。

TLS クライアント証明書およびクライアントのプライベートキー

製品によって実装されるプロトコルには、オプションの TLS クライアント証明書を提供する機能が含まれる場合があります。TLS 構成がセキュリティ要件を満たすことを確認してください。ベストプラクティスとして、[Client Certificate] および [Client Private Key] を設定し、関連付けられた [Provide Client Certificate] オプションを有効にします。証明書を提供することで、構成されたサーバーは、構成された NMC の真正性を確認できます。

セキュリティに関する応答

セキュリティインシデントを報告する場合は、[Product Support and Other Resources] に記載されている“テクニカルサポート”窓口までご連絡ください。

保証および規制について

保証について

<https://www.panduit.com/en/legal-information/panduit-limited-product-warranty.html>

規制について

安全性と法規制の順守

重要な安全性情報、環境情報、法規制情報については、パンドウイトの Web サイトの「Safety and Compliance Information」を参照してください。

<https://www.panduit.com/en/support/download-center/certifications.html>

製品サポートおよび他のリソース

サポートに関するほとんどのニーズは、Panduit.com にアクセスして、それぞれの製品ページに移動することで解決できます。追加の支援が必要な場合は、当社がお手伝いします。



チャットボットが 24 時間 365 日対応

バンドウィットのサポートにアクセスする

北米

カスタマーサービス

- 価格および購入の可否
- 督促

800-777-3300 または
cs@panduit.com

PDU テクニカルサポート:

- PDU の選択
- 他社製品の相互参照
- 製品ドキュメント
- 技術的な問題

メール: TechSupport@panduit.com

欧州 / 中東

カスタマーサービス

- 価格および購入の可否
- 督促

0044-(0)208-6017219 または
EMEA-CustomerServices@panduit.com

PDU テクニカルサポート:

- PDU の選択
- 他社製品の相互参照
- 製品ドキュメント
- 技術的な問題

メール: TechSupportEMEA@panduit.com

<https://www.panduit.com/en/support/contact-us.html>

導入済み製品のグローバルシステムサポート:

- ファームウェアの更新
- デバイスのセットアップ (ネットワークやアクセス制御など)
- サードパーティの DCIM、MIB Walk、SNMP セットアップ、メールセットアップ、トラップレシーバー
- 返品保証 (RMA)

メール: SystemSupport@panduit.com

展開されたソリューション向けのグローバルシステムサポート:

- ファームウェアの更新
- デバイスのセットアップ (ネットワークやアクセス制御など)
- サードパーティーの DCIM、MIB Walk、SNMP セットアップ、メールセットアップ、トラップレシーバー
- 返品保証 (RMA)

メール (推奨): SystemSupport@panduit.com

Ph (米州): 1-866-721-5302

Ph (EMEA): +44-1291-674661

グローバルポストセールサポートへお問い合わせの際は、問題の解決を円滑に進めるため、必ず以下の情報をご提供ください (お電話の場合はお手元にご用意ください)。

注文書番号:

ディストリビューター名 (該当する場合):

請求書の日付:

エンドユーザーの会社名:

サイト連絡担当者の名前:

サイト連絡担当者の電話番号:

サイト連絡担当者のメールアドレス:

サイトの配達住所:

パンドウイトの完全な部品番号:

影響を受ける総数:

不具合の説明 (出来る限り詳しく):

頭字語と略語

A アンペア (Amps/Amperes)	LDAP エルダップ (Lightweight Directory Access Protocol)
AC 交流電流 (Alternating Current)	NMC ネットワークマネージメントカード
AES 高度暗号化標準 (Advanced Encryption Standard)	PDU 配電ユニット (Power Distribution Unit)
CLI コマンドラインインターフェイス (Command Line Interface)	SHA セキュアハッシュアルゴリズム (Secure Hash Algorithms)
DHCP ダイナミックホストコンフィギュレーションプロトコル (Dynamic Host Configuration Protocol)	SNMP 簡易ネットワーク管理プロトコル (Simple Network Management Protocol)
GUI グラフィカルユーザーインターフェイス (Graphical User Interface)	TCP/IP ティーシーピーアイピー (Transmission Control Protocol/Internet Protocol)
IP インターネットプロトコル (Internet Protocol)	UPS 無停電電源装置 (Uninterruptible Power Supply)
kVA キロボルトアンペア (Kilo-Volt-Ampere) kW キロワット (Kilowatts) kWh キロワットアワー (Kilowatt Hour)	USB ユーエスビー (Universal Serial Bus)
LAN ローカルエリアネットワーク (Local Area Network)	V ボルト (Volts)
LCD 液晶ディスプレイ (Liquid-Crystal Display)	W ワット (Watts)

付録A: ファームウェアの更新手順

手動更新

ファームウェアアップグレード手順では、イメージのシグネチャを検証することによってイメージを確認します。シグネチャが一致しない場合、ファームウェアアップグレード手順ではイメージが無視され、現行バージョンを維持します。ファームウェアを更新しても、インテリジェント NMC の構成やアウトレット状態には影響しません。最新のファームウェアについては、panduit.com → Support → Download Center → PDU にアクセスしてください。

1. ファームウェアファイルを Web ページからダウンロードします。
2. ダウンロードしたファイルを圧縮解除します。
3. ユーザーインターフェイスを Web ブラウザーで開くため、NMC IP アドレスを入力します。
4. 管理者資格でログインします。
5. [Settings] > [Device Firmware Update] > [Actions] > [Upload Firmware] に移動します。
6. [Firmware Update] ダイアログボックスで、[Choose File] をクリックし、「pdu-package-*.*.bin」という名前のファームウェアファイルへ進みます。

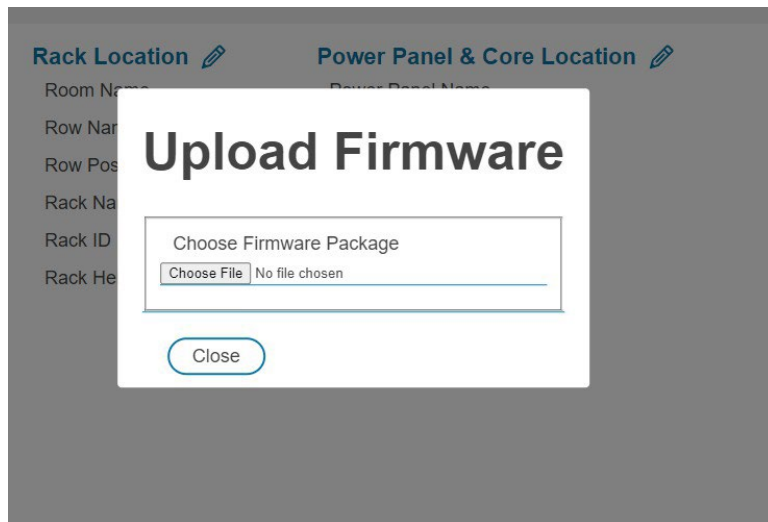


図 148: アップロード

7. ファイルを選択すると、システムが更新されます。
8. アップロードが終了すると、システムは自動的に再起動します。
9. デイジーチェーン方式では、ユーザーがプライマリ PDU でファームウェアの更新を開始すると、リンクされたすべての PDU が自動的に更新されます。

自動更新

自動更新機能は、構成ファイルとファームウェアを定期的に更新することで、現地での保守を簡素化します。SZTP は初回起動時に一度だけデバイスをプロビジョニングしますが、自動更新は運用中も継続的に動作します。

この機能は、設定済みの HTTPS URI を対象に、指定された周期でファームウェアや構成ファイルのアップデートを確認します。PDU が変更を検出できるように、HTTPS サーバーは対象ファイルに関連付けられた HTTP Last-Modified ヘッダーを更新する必要があります。このヘッダーの更新は、新しいバージョンが利用可能であることを示します。

Device Firmware Update

Actions

Network Management Card

Auto Update

Auto Update Configuration

Enable

Update Check Frequency

Interval Start Time (HH:MM:SS)

Interval End Time (HH:MM:SS)

Stagger Update

Disabled

Daily

None

None

Disabled

Auto Update Status

Firmware Update Status

Last Firmware Update

Config Update Status

Last Config Update

Waiting

December 31, 1969 6:00:00 PM

Waiting

December 31, 1969 6:00:00 PM

図 149: 自動更新

自動更新の構成

自動更新の構成には、SZTP を有効にするための設定と、ネットワークの場所、サーバーの確認、および更新パターンの設定が含まれます。自動更新を設定するには、以下の手順に従います。

1. [Auto Update Configuration] の横にある鉛筆アイコンを選択します。
2. **[Enable]** の横にあるボックスをクリックします。
3. ファームウェアファイルの HTTPS URI を **[Firmware URI]** に入力します。
4. 構成ファイルの HTTPS URI を **[Config URI]** に入力します。
5. **[Update Check Frequency]** の下にあるドロップダウンメニューをクリックし、自動更新で新しいファイルをチェックする頻度を設定します。
6. 特定のサーバーの認証を有効にするには、**[Verify Certificate]** の下にあるチェックボックスをクリックし、[Server Certificate] をクリックして、https サーバーの証明書を追加します。
7. 自動更新により更新をチェックする毎日の時間帯を構成します。期間の開始を **[Interval Start Time]** に入力します。期間の終了を **[Interval End Time]** に入力します。
8. 期間の開始時刻と終了時刻の間のランダムな時刻に更新を実行するには、**[Stagger Update]** の横にあるボックスをクリックします。これにより、多くの PDU があるときに、ネットワークトラフィックおよびサーバー負荷が大幅に増加することの対策となります。
9. 更新がないかただちに確認する場合は、**[Update Now]** ボックスをチェックします。

Auto Update Configuration

Enable

☐ Enable

Firmware URI

Config URI

Update Check Frequency

Daily

Verify Certificate

☐ Enable

Server Certificate

Interval Start Time (HH:MM:SS)

HH:MM:SS

Interval End Time (HH:MM:SS)

HH:MM:SS

Stagger Update

☐ Enable

Update Now

☐ Enable

Save

Close

図 150: 自動更新の構成

付録B: システムリセットまたはパスワード復旧

EL2P コントローラは 3 つのリセットレベルに対応しており、それぞれシステム復旧の度合いが異なります。

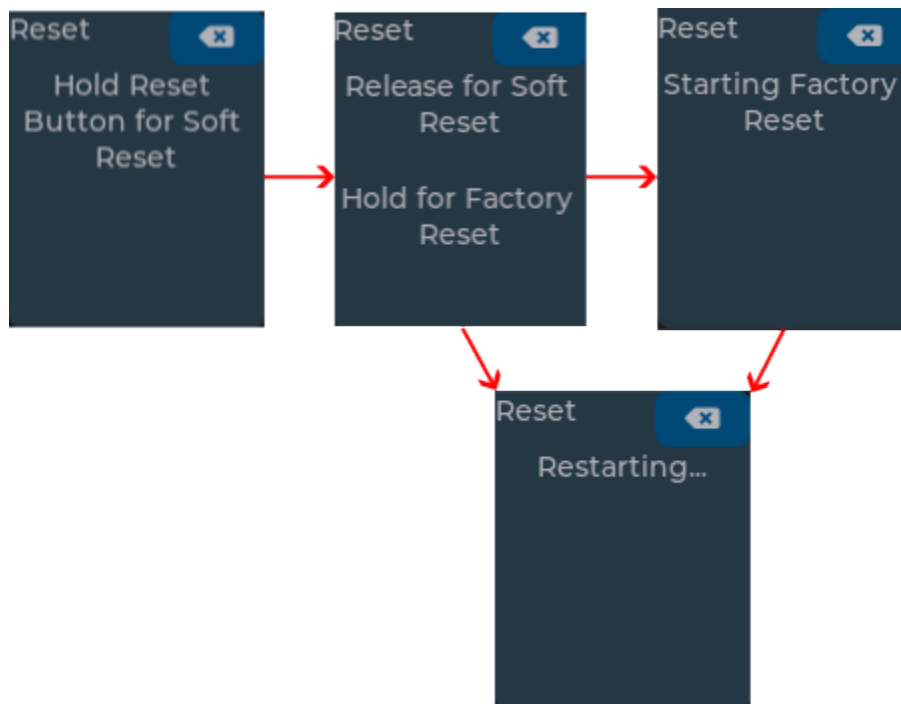
レベル 1 - ソフトリセット (NMC 再起動)

NMC の前面のリセットボタンを 2 秒押したままにします。

これにより、ボタンを放したときにソフトシステムリセットが実行され、NMC コントローラを再起動しますが、**既存のすべての構成は保持されます**。

レベル 2 - 工場出荷時の初期設定へのリセット (NMC デフォルト)

リセットボタンを 8 秒以上押したままにします (ただし 20 秒を超えないこと)。工場出荷時の初期状態へのリセットは、ボタンを放したときではなく 8 秒後に開始します。この操作では NMC コントローラは工場出荷時の初期設定に復元され、ユーザー名とパスワードを含めた**すべての構成が消去されます**。完了すると、NMC は自動的に再起動します。デフォルトの認証情報については、「[Web インターフェイスにログインする](#)」のセクションを参照してください。



レベル 3 - フルシステムリセット (NMC)

コントローラが完全にロックされている場合 (応答しない)、リセットボタンを 30 秒押したままにします。これにより、**NMC の内部マイクロコントローラへのリセットが強制され、復旧パスが提供されます**。

ユーザーパスワードの復元:

ユーザーが忘れたパスワードを復元するには、最初に管理者アカウントでログインします。画面の右上隅にあるユーザーアイコンを選択し、[User Accounts] を選択します。

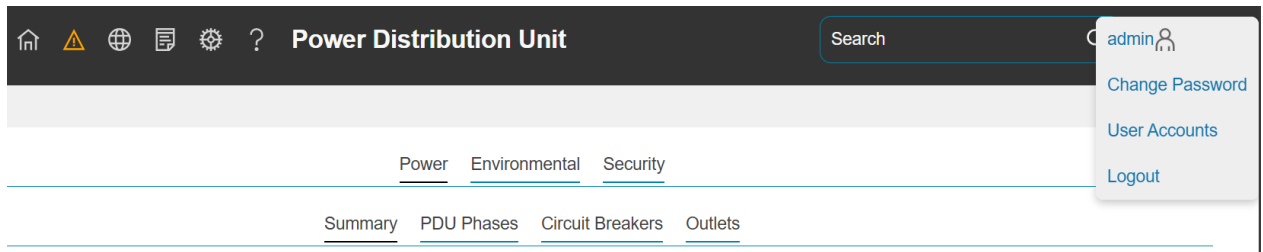


図 151: ユーザーアイコンの [User Accounts]

あるいは、歯車アイコンを選択して、[User Accounts] をクリックすることもできます。どちらの方法でも同じページに移動します。

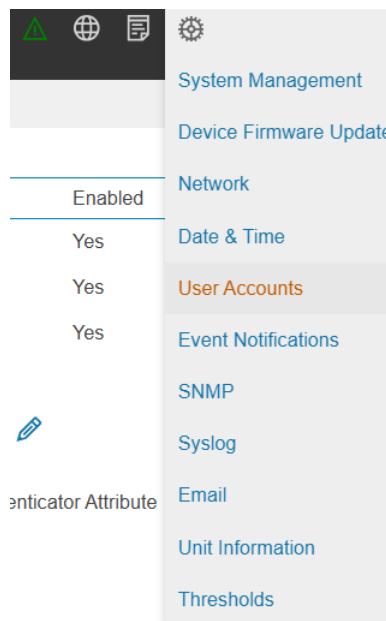


図 152: 歯車アイコンの [User Accounts]

画面の右側に [Users] の表が表示されます。パスワードを忘れたユーザーの横にある鉛筆アイコンをクリックします。

User Accounts			
Users			
Username	Role	Enabled	
admin	Admin	Yes	
user	Viewer	No	
	Viewer	No	

図 153: [Users] の表

[Edit User] 画面で新しいパスワードを [Password] フィールドに入力し、同じパスワードを [Confirm Password] フィールドに再入力してそのパスワードを割り当てることができます。また、[Must Change Password at next Log In] オプションを有効にすることを選択すると、ユーザーが次回ログインするときに新しいパスワードの作成が求められます。終了したら、[Save] をクリックしてログアウトします。これで、ユーザーは作成したパスワードでログインできます。

Edit User

Username

user

Role

Viewer

▼

Password

Confirm Password

👁

Enabled

☐ Enable

Must Change Password at next Log In

☒ Enable

Save

Close

図 154: [Edit User] 画面

付録C: Bonjour を使用しないイーサネット経由の直接接続

【注意】説明は特に Windows 10 についてのもので、Windows 10 を使用していない場合は、ご使用のオペレーティングシステムのドキュメントを参照してください。

1. Windows の検索に「network connections」と入力し、ネットワーク接続の表示を選択します。

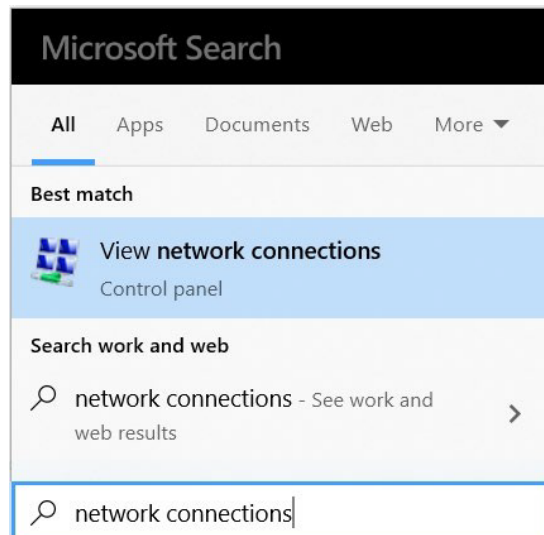


図 155: ネットワーク接続の表示

2. [イーサネット] を右クリックし、[プロパティ] を選択します。

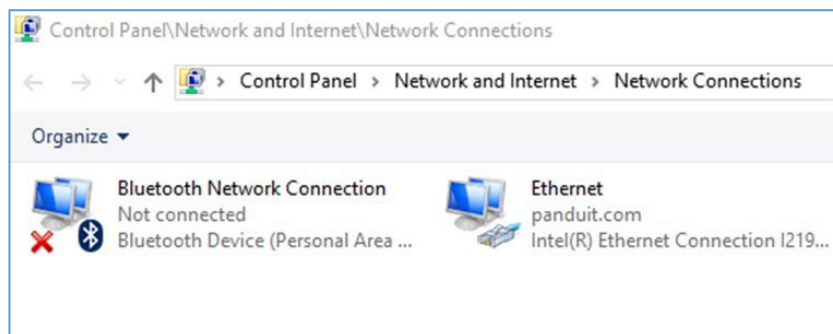


図 156: プロパティ

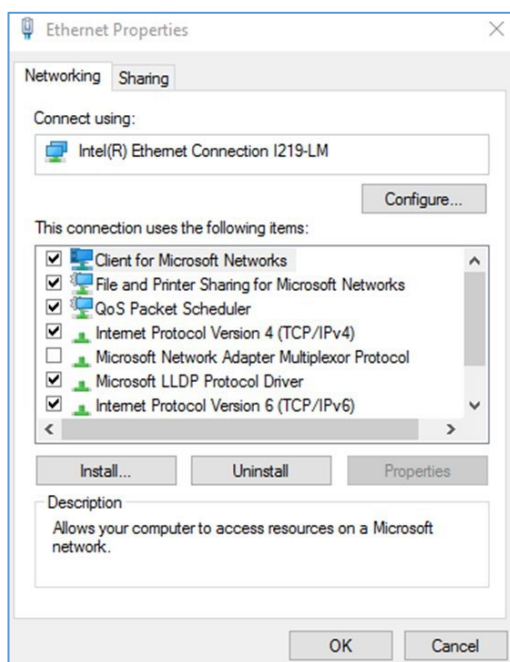


図 157: イーサネットのプロパティ

3. [インターネット プロトコル バージョン 4 (TCP/IPv4)] を選択します (下へスクロールする場合があります)。次に、[プロパティ] ボタンをクリックします。

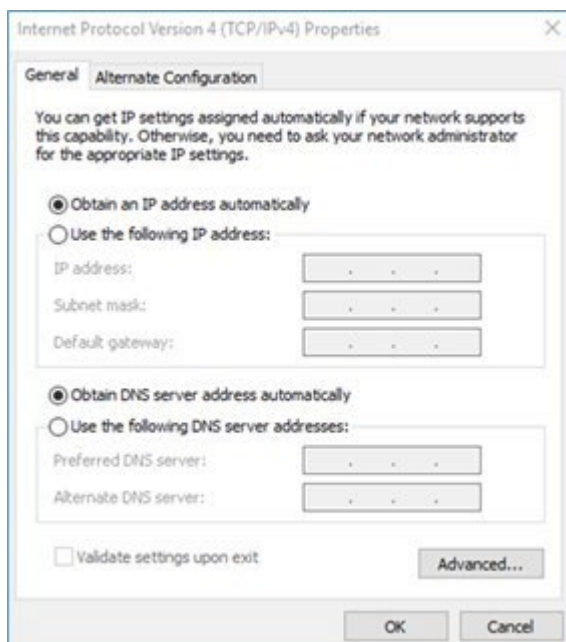


図 158: インターネットプロトコルバージョン 4

4. 選択されていない場合、[IP アドレスを自動的に取得する] ラジオボタンと [DNS サーバーのアドレスを自動的に取得する] ラジオボタンを選択します。
5. [OK] をクリックして、構成を受け入れます。
6. パッチケーブルを使用して、NMC ネットワークを PC のイーサネットポートに直接接続します。
7. NMC ユニットの電源を入れます。
8. 60 秒待機します。
9. PC で Web ブラウザーを開きます。
10. Web ブラウザーのアドレスバーに `https://169.254.254.1` と入力して Enter を押します。
プライバシーエラー (認証局が無効のエラー) が表示されることがあります。このメッセージは、最初の証明書がデバイスで使用中のときに表示されます。このエラーは想定されているものであるため続行してかまいません。

付録 D: コマンドラインインターフェイス (Command Line Interface)

NMC では、シリアルポートおよび SSH ネットワークプロトコルを使用したコマンドラインインターフェイスが提供されています。コマンドラインインターフェイスを使用して、NMC データモデルからの読み取りや書き込みを行うことができます。

シリアルポートを使用してログインする

- PC と NMC シリアル (RJ45) ポートを「USB コンソールケーブル」で接続します。業界標準の USB コンソールのサンプルを以下に示します。



- Tera Term などのターミナルエミュレータプログラムを開きます
- 通信速度 115200、8 ビットデータ、パリティなし、1 ストップビット、フロー制御なしを設定します
- 対応する COM ポートを接続します
- Web UI から同じ資格情報を使用します

SSH プロトコルを使用してログインする

- NMC の IP アドレスを特定します
- PuTTY などの SSH プログラムを開きます
- NMC への接続を開きます
- Web UI から同じ資格情報を使用します

パスワードを変更する

最初のログイン時に、変更していない場合はデフォルトのパスワードを Web UI から変更する必要があります。デフォルトのユーザー名は admin、デフォルトのパスワードは admin です。

ユーザー名と現在のパスワードを入力してから、新しいパスワードを 2 度入力して確定します。パスワードは 8 ～ 40 文字にする必要があります、以下の 4 つの規則の 3 つに従う必要があります。

- 小文字を 1 文字以上含む
- 大文字を 1 文字以上含む
- 数字を 1 文字以上含む
- 特殊文字を 1 文字以上含む

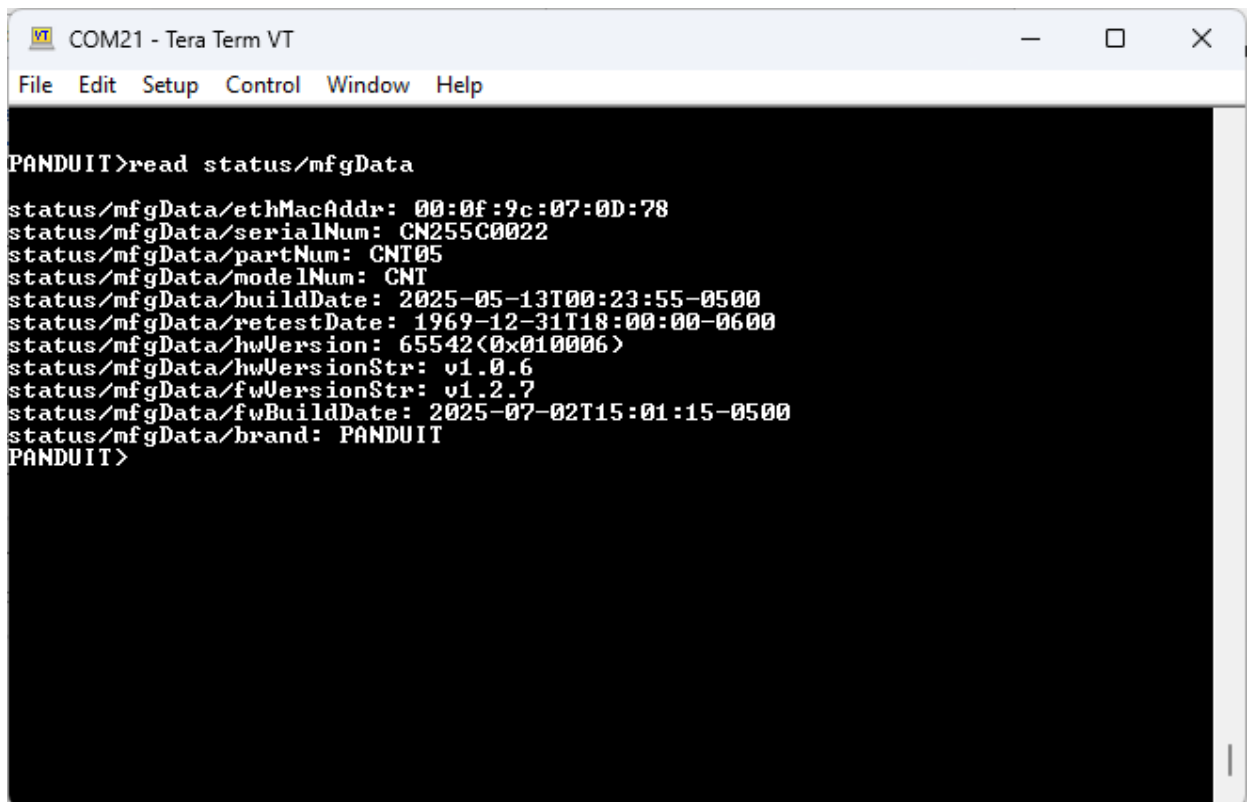
コマンド一覧

ログインすると、「PANDUIT>」プロンプトが表示されてコマンドの入力待ちの状態になります。次のコマンドのみが受け入れられます。

- Read

格納されたデータをデータモデルから読み取ります。パラメーターにはオブジェクト名または個々の項目を指定できます。オブジェクト名で問い合わせると、そのオブジェクト内のすべての項目が表示されます。

例: read status/mfgData



```
COM21 - Tera Term VT
File Edit Setup Control Window Help

PANDUIT>read status/mfgData

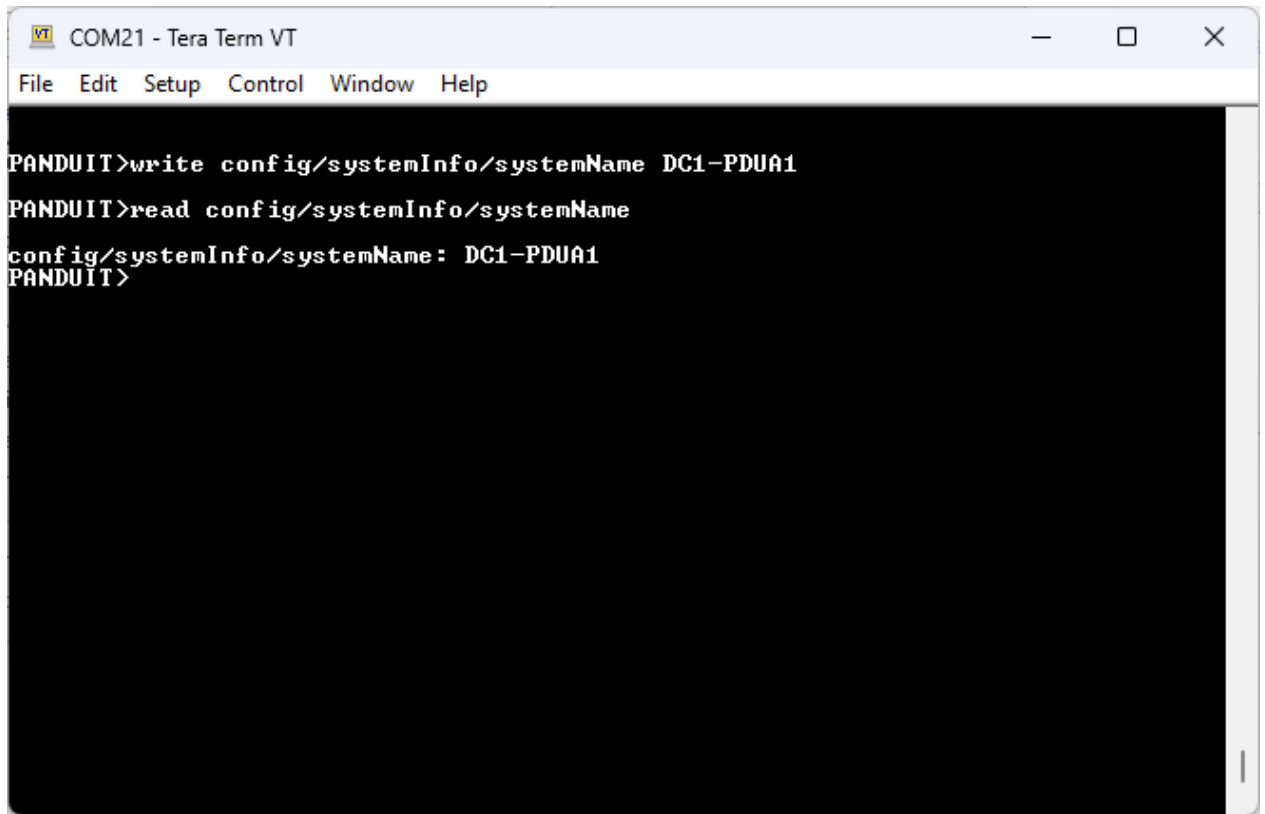
status/mfgData/ethMacAddr: 00:0f:9c:07:0d:78
status/mfgData/serialNum: CN255C0022
status/mfgData/partNum: CNT05
status/mfgData/modelNum: CNT
status/mfgData/buildDate: 2025-05-13T00:23:55-0500
status/mfgData/retestDate: 1969-12-31T18:00:00-0600
status/mfgData/hwVersion: 65542(0x010006)
status/mfgData/hwVersionStr: v1.0.6
status/mfgData/fwVersionStr: v1.2.7
status/mfgData/fwBuildDate: 2025-07-02T15:01:15-0500
status/mfgData/brand: PANDUIT
PANDUIT>
```

図 159: CLI から読み取る

- Write

データモデル内の個々の項目に値を設定します。

例: write config/systemInfo/systemName DC1-PDUA1



```
COM21 - Tera Term VT
File Edit Setup Control Window Help

PANDUIT>write config/systemInfo/systemName DC1-PDUA1
PANDUIT>read config/systemInfo/systemName
config/systemInfo/systemName: DC1-PDUA1
PANDUIT>
```

図 160: CLI から書き込む

- List

データモデル内のすべてのオブジェクトを一覧表示します

- list object

データモデル内の object のオプションを表示します

- help、?

すべてのコマンド一覧と使用方法を表示します

- logout、quit

ユーザーをログアウトします

付録 E: RADIUS サーバー構成

ユーザーが admin User-Role としてログインできるようにします。

この例では、admin User-Role としてログイン可能なユーザーに freeradius を構成する方法を示します。ここでは Ubuntu または同等のインストール環境への freeradius のクリーンインストールを想定しています。

1. freeradius をインストールするか、既存のインストール済み環境で開始します。
2. セキュリティ要件に合わせて構成された承認済みクライアント構成ステートメントを /etc/freeradius/3.0/clients.conf に作成します。
3. /usr/share/freeradius/dictionary.Panduit に、以下を含むディクショナリを作成します。

```
# *- text *-
VENDOR          Panduit          19536
BEGIN-VENDOR    Panduit
ATTRIBUTE       Panduit-User-Role 1          integer
VALUE           Panduit-User-Role User          1
VALUE           Panduit-User-Role Admin          2
VALUE           Panduit-User-Role Control         3
END-VENDOR      Panduit
```

4. 以下の行を /etc/freeradius/3.0/dictionary に追加して、dictionary.Panduit をロードします。

```
$INCLUDE /usr/share/freeradius/dictionary.Panduit
```

5. 承認済みのユーザーを、必要な役割とともに /etc/freeradius/3.0/mods-config/files/authorize に追加します。(注意: ‘users’ ファイルの場所は、独自のカスタマイズやパッケージマネージャーの種類によって異なることがあります) User-Role が指定される場合、それがユーザーの最初の属性である必要があります。パスワードはセキュリティ要件に合わせて構成されたものを使用してください。

- a. User-Role が指定されない場合(このユーザーがデフォルトの “viewer” 役割でログインする)

```
raduser          Cleartext-Password := "23456789"
                  Service-Type = 1
```

- b. User-Role が Admin に設定された場合(このユーザーが “admin” 役割でログインする)

```
radroleadmin     Cleartext-Password := "34567890"
                  Panduit-User-Role = Admin,
                  Service-Type = 1
```

- c. User-Role が User に設定された場合(このユーザーが “viewer” 役割でログインする)

```
radroleuser      Cleartext-Password := "45678901"
                  Panduit-User-Role = User,
                  Service-Type = 1
```

6. RADIUS サーバーを再起動して構成変更を有効にします。

```
systemctl stop freeradius  
systemctl start freeradius
```

7. サーバーが認証を実行することができ、構成されたユーザー役割を返すことを確認します。注意: 適用されるクライアントの制約に基づいて、この例を変更することが必要な場合があります。

```
Usage: radtest [OPTS] user passwd radius-server[:port] nas-port-number secret
```

```
# radtest 'radroleadmin' '34567890' 192.0.2.1 0 'panduit#1' "
```

```
Sending Access-Request of id 212 to 192.0.2.1 port 1812
```

```
  User-Name = "radroleadmin"
```

```
  User-Password = "34567890"
```

```
  NAS-IP-Address = 127.0.1.1
```

```
  NAS-Port = 0
```

```
  Message-Authenticator = 0x00000000000000000000000000000000
```

```
rad_recv: Access-Accept packet from host 192.0.2.1 port 1812, id=212, length=38
```

```
  Panduit-User-Role = Admin
```

```
  Service-Type = Framed-User
```

付録 F: POSIX タイムゾーン情報

カスタムのタイムゾーン形式は次のようになります。

```
STD Offset DST DstOffset,DSTStart,DSTEnd
```

(見やすくするために追加されているスペースは、以下の例に示すように除去する必要があります)

STD は、標準時間のときに使用されるタイムゾーンの略称です。

Offset は UTC からの標準時間オフセットです。

DST は、夏時間のときに使用されるタイムゾーンの略称です。

DstOffset は UTC からの夏時間オフセットです。(DST が STD より 1 時間少ない場合は省略可能)

DSTStart および DSTEnd は次の形式です。

Mm.n.d/H:MM:SS

- m (1-12): 12 カ月のうちのいずれか
- n (1-5): 1 はその月の第 1 週、5 は最後の週
- d (0-6): 0 は日曜日、6 は土曜日
- H (0-24): 時間
- MM (00-60): 分
- SS (00-60): 秒

例 1: 米国中部のタイムゾーンは次のように指定されます。

```
CST6CDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

CST は、夏時間がオフのときのタイムゾーンの略称です。

6 は UTC からの時間差です。

CDT は、夏時間がオンのときのタイムゾーンの略称です。

M3.2.0/2:00:00 は、DST が 3 月の第 2 日曜の午前 2 時に始まることを指定します。

M11.1.0/2:00:00 は、DST が 11 月の第 1 日曜の午前 2 時に終わることを指定します。

例 2: 中国標準時は次のように指定されます。

```
CST-8
```

CST は、中国標準時のタイムゾーンの略称です。

-8 は UTC からの時間差です。

(中国には夏時間がないため、残りのフィールドは省略されています)

付録 G: セキュアゼロタッチプロビジョニング (sZTP)

通信事業者の基本的なビジネス要件は、セキュリティを危険にさらすことなく可能な限りコストを削減することです。

通信事業者にとって、デバイスの設置は莫大なコストがかかるだけでなく、訓練を受けた専門家によっては設置方法が異なるため多様性がもたらされます。これを改善するため、PDU ではセキュアゼロタッチプロビジョニング (SZTP) をサポートしています。これは、物理的な配置とネットワークケーブルおよび電源ケーブルの接続以外の設置に関して何のアクションも起こさず、デバイスがブートストラップデータを安全に取得できるようにするブートストラップ戦略です。

パンドウイトのセキュアゼロタッチプロビジョニングは [RFC 8572](#) に従っています。

SZTP の利用開始

SZTP では以下のものがが必要です。

- 1) ブートストラップソフトウェアを実行する Windows サーバー
- 2) ローカルでないネットワーク使用のための DHCP および DNS のネットワーク構成の変更
- 3) SZTP の証明書
- 4) パンドウイトからの SZTP バウチャー
- 5) EL2P ファームウェアバージョン 1.4.1 以上

SZTP セットアップの概要

- 手順 1: CA 証明書とサーバー証明書/プライベートキーを作成または取得します。サーバー証明書には、DNS を使用して Windows サーバーに解決可能な名前が含まれていることを確認します。
- 手順 2: 署名付きバウチャーを systemsupport@panduit.com に要求します。
- 手順 3: Panduit SZTP ブートストラップソフトウェアを Windows サーバーにインストールします。
- 手順 4: SZTP DHCP オプションを提供するようにネットワーク DHCP サーバーを構成します。
- 手順 5: 各 PDU のための構成ファイルを作成します。
- 手順 6: 新しい PDU をネットワークに接続します。SZTP は、サーバー上にバウチャーがある各 PDU を自動的に更新して構成します。PDU が以前接続またはログインされていた場合、SZTP を初期化するようデフォルトに設定します。

証明書の作成とネットワークの構成には、ネットワーク管理者の支援が必要になります。SZTP の構成手順の詳細については、以下のセクションを参照し、「付録 J: SZTP ブートストラップサーバーのインストール」および「付録 I: SZTP サーバー検出 (DHCP または mDNS)」を参照してください。

証明書の構成

SZTP では、ブートストラップサーバーの認証のためのトラストアンカーとして機能する少なくとも 1 つの CA 証明書の構成が必要です。バウチャー申請の一部としてトラストアンカー証明書をパンドウイトに送信する必要があります。

- トラストアンカーは、ブートストラップサーバー証明書自体でなく、ルート CA 証明書または中間 CA 証明書である場合があります。
- 既存の会社のルートオプトラスト、または中間 CA が使用される場合もあります。
- ブートストラップサーバー証明書には、トラストアンカーに戻るチェーンが含まれている必要があります。
- “トラストアンカー” は、バウチャーに組み込まれると、“pinned-domain-cert” と呼ばれます。

バウチャーの申請

ブートストラップサーバーによって Panduit PDU に提供されるバウチャーは、PDU の所有権を証明します。パンドゥイットにバウチャーを申請するときは、以下の項目を提供します。

- PDU のシリアル番号
- PDU の所有権の証明
- トラストアンカー証明書

SZTP 所有権バウチャーを systemsupport@panduit.com に申請します。

SZTP の操作

工場出荷状態の Panduit PDU は、SZTP ブートストラップサーバーにバウチャーおよび構成情報が登録されていれば、電源投入後にネットワークへ接続するだけで自動的にプロビジョニングされます。

SZTP は各 PDU で一回実行されるように設計されており、以下のいずれかが発生した場合に自動で無効化されます。

- 正常なブートストラップが (SZTP 経由で) 実行された
- ログインアクティビティがない。
- PDU がダイジェチェーンのリンク済みユニットになった。

PDU が SZTP を無効にした後、SZTP を使用したい場合、PDU を工場出荷時の初期設定にリセットする必要があります。定期的にファームウェアをアップデートするには、自動更新機能を使用してください。

付録 H: ゼロタッチプロビジョニング (ワンタッチ ZTP)

通信事業者の基本的なビジネス要件は、セキュリティを危険にさらすことなく可能な限りコストを削減することです。

通信事業者にとって、デバイスの設置は莫大なコストがかかるだけでなく、訓練を受けた専門家によっては設置方法が異なるため多様性がもたらされます。これを改善するため、PDU ではゼロタッチプロビジョニング (ZTP) をサポートしています。これは、機器の設置とネットワークおよび電源ケーブルの接続以外に作業を必要とせず、デバイスがブートストラップデータを取得できるようにするプロビジョニング方式です。

最高レベルのセキュリティを維持するため、パンドウイトのゼロタッチプロビジョニング (ZTP) はワンタッチプロビジョニング方式に変更されました。サーバーを信頼できるセキュリティ保護されたネットワークでは、ワンタッチプロビジョニングを使用できます。これは、パンドウイトが提供するバウチャーを必要としない自動プロビジョニング方式です。ZTP を有効にするには、ディスプレイ上で手動による確認操作を行う必要があります。

パンドウイトのワンタッチプロビジョニングは、メーカーのバウチャー要件を除いて [RFC 8572](#) に従っています。

ワンタッチ ZTP の利用開始

ZTP では以下のものがが必要です。

- 1) ブートストラップソフトウェアを実行する Windows サーバー。
- 2) ローカルでないネットワーク使用のための DHCP および DNS のネットワーク構成の変更。
- 3) EL2P ファームウェアバージョン 1.5.3 以上

ワンタッチ ZTP セットアップの概要

手順 1: Panduit SZTP ブートストラップソフトウェアを Windows サーバーにインストールします。

構成でワンタッチを有効にしてください。詳しくは、「付録 J: SZTP ブートストラップサーバーのインストール」を参照してください。

手順 2: SZTP DHCP オプションを提供するようにネットワーク DHCP サーバーを構成します。

詳しくは、「付録 I: SZTP サーバー検出 (DHCP または mDNS)」を参照してください。

手順 3: 各 PDU のための構成ファイルを作成します。

詳しくは、「付録 J: SZTP ブートストラップサーバーのインストール」を参照してください。

手順 4: 新しい PDU をネットワークに接続します。PDU が以前接続またはログインされていた場合、SZTP を初期化するようデフォルトに設定します。

手順 5: 各 PDU の ZTP を有効にします。

- 1) LCD の設定アイコンにタッチします。
- 2) [Enable ZTP] ボタンをタッチします。

PDU は自動でプロビジョニングします。

付録 I: SZTP サーバー検出 (DHCP または mDNS)

PDU は DHCP オプションを使用するか mDNS を (ローカルで) 使用するかのいずれかの方法で SZTP ブートストラップサーバーを検出します。

mDNS

PDU および SZTP ブートストラップサーバーが同じローカルネットワークにある場合、mDNS サービスを使用して PDU に自分自身をアドバタイズするようブートストラップサーバーを構成することができ、DHCP 構成を変更する必要はありません。これを行うには、ブートストラップサーバーのインストール中に、[Enable mDNS] をチェックし、サーバーのホスト名を入力します。

この方法では EL2P ファームウェアバージョン 1.6.x 以上が必要です。
PDU が mDNS 経由でブートストラップサーバーを検出してこれに接続するには、最大 6 分必要な場合があることに注意してください。

DHCP オプション

それ以外の場合はすべて、DHCP を使用して、ブートストラップサーバーへのリダイレクト URI を提供します。リダイレクト情報は、DHCPv4 (オプション 143) または DHCPv6 (オプション 136) のいずれかを使用して提供できます。ブートストラップ情報は、RFC8572 セクション 8.2 および 8.3 に従って、“URI” 構造として提供する必要があります。

uri-length	URI
------------	-----

- uri-length: 2 オクテット長、URI データの長さを指定します。
- URI: SZTP ブートストラップサーバーの URI。

DHCP によって提供される URI は、“https://<ブートストラップホスト名>[:<ポート>]” の形式である必要があります。

DHCP サーバーソフトウェアによっては、正しい形式を使用して SZTP URI オプションをセットアップするとき、オプション値を 16 進数で書くことが必要な場合もあります。たとえば、sztpbootstrap.panduitlabs.com でデフォルトの HTTPS ポート 443 を使用するブートストラップサーバーの場合、URI は次のようになります。

<https://sztpbootstrap.panduitlabs.com>

これを ASCII コードの 16 進表記で表すと次のようになります。
68 74 74 70 73 3A 2F 2F 73 7A 74 70 62 6F 6F 74 73 74 72
61 70 2E 70 61 6E 64 75 69 74 6C 61 62 73 2E 63 6F 6D

37 バイト存在し、これは 16 進数では 0x0025 であるため、オプション値は次のようになります。
00 25 68 74 74 70 73 3A 2F 2F 73 7A 74 70 62 6F 6F 74 73 74
72 61 70 2E 70 61 6E 64 75 69 74 6C 61 62 73 2E 63 6F 6D

Windows DHCP サーバー上で、以下の手順に従います。

- 1) DHCP コンソールを開きます。
- 2) IPv4 を右クリックし、[既定のオプションの設定] を選択します。
- 3) [追加] をクリックして、構成情報を入力します。
 - a. 名前: SZTP
 - b. データ型: バイナリ
 - c. コード: 143
 - d. 説明: SZTP リダイレクト URI
- 4) [OK] をクリックして新しいオプションを保存します。
- 5) IPv4 ツリーの下にある目的のスコープに移動します。
- 6) [スコープオプション] を右クリックし、[オプションの構成] を選択します。
- 7) [143 SZTP] オプションのボックスにチェックを付けます。
- 8) Panduit ブートストラップソフトウェアを実行するサーバーの URI の 16 進数データを入力します。

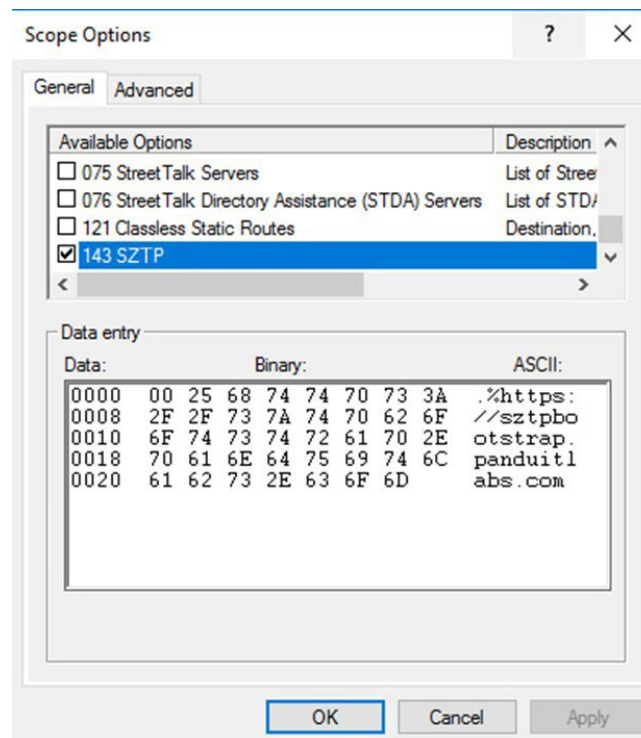


図 161: Windows DHCP 構成

付録 J: SZTP ブートストラップサーバーのインストール

Panduit ブートストラップソフトウェアは Windows コンピューター上で動作します。これは SZTP を使用する Panduit PDU のためのブートストラップ情報とファームウェアイメージを提供します。

- 1) Panduit ブートストラップソフトウェアを、<https://www.panduit.com/pdu-support> のサポートにある PDU ファームウェアパッケージから取得します。
- 2) インストーラーをダブルクリックします。
- 3) パンドウイトの EULA を読んで同意します。

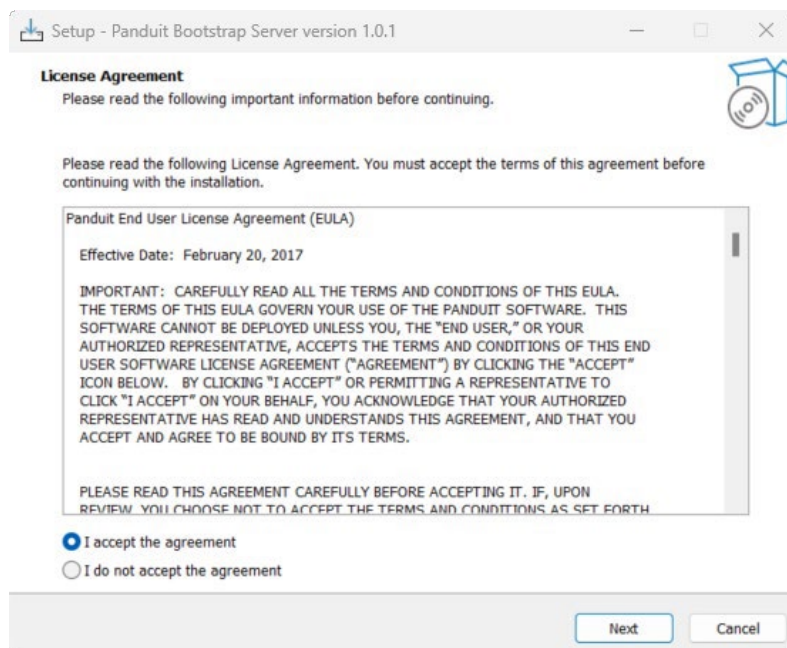


図 162: SZTP ライセンス

- 4) ソフトウェアのインストールフォルダを選択します。デフォルトが推奨されます。

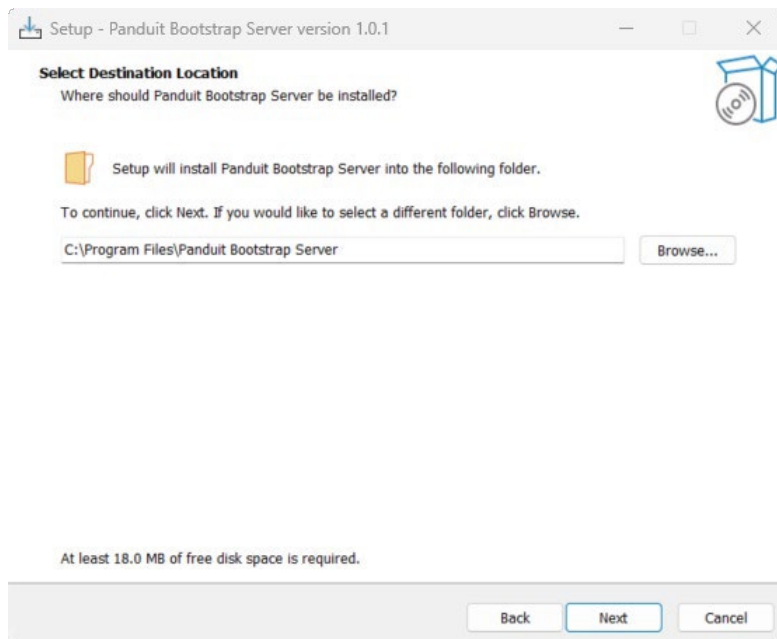


図 163: インストールフォルダ

- 5) 開始メニューフォルダを選択します。

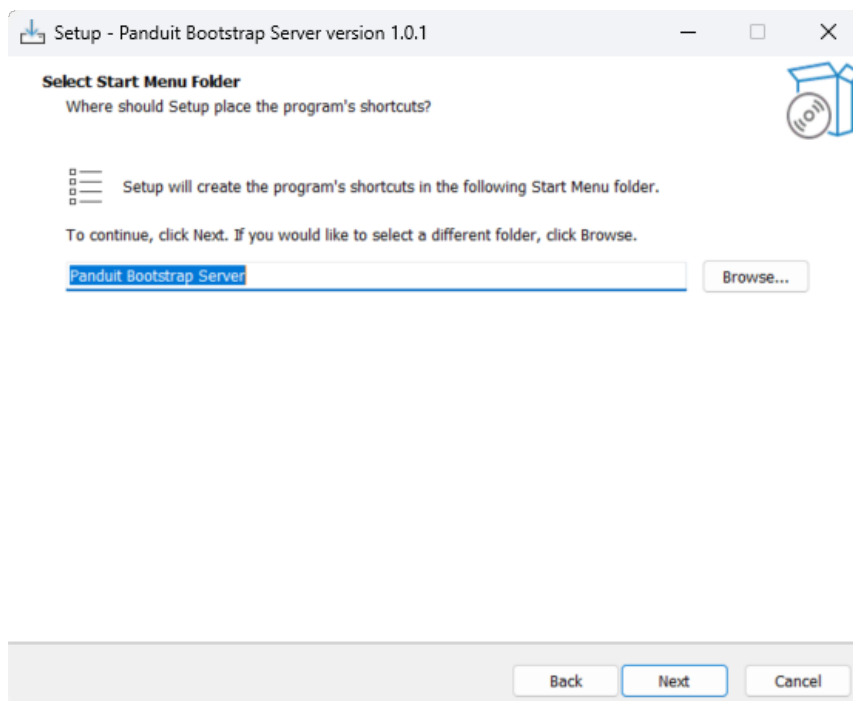


図 164: 開始メニューの場所

6) [Install] をクリックして、ソフトウェアのインストールを開始します。

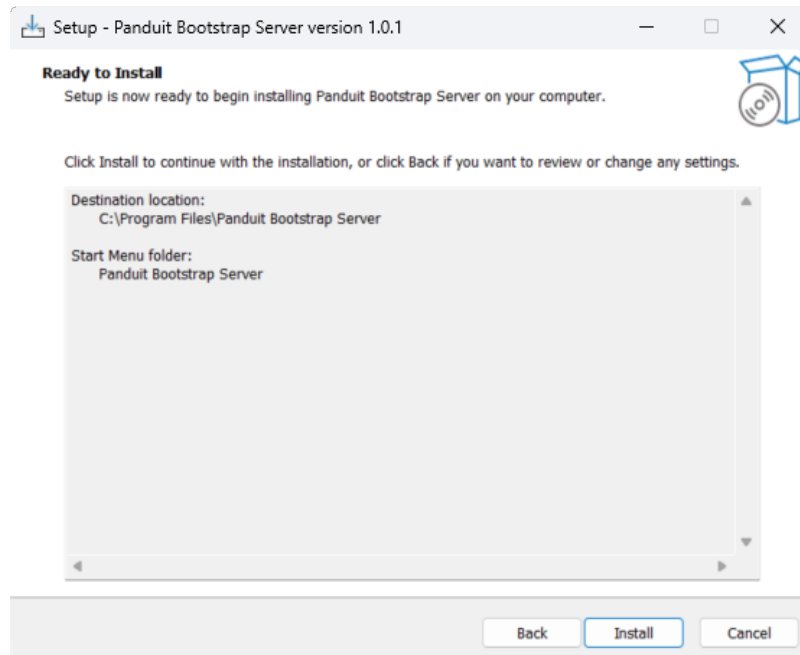
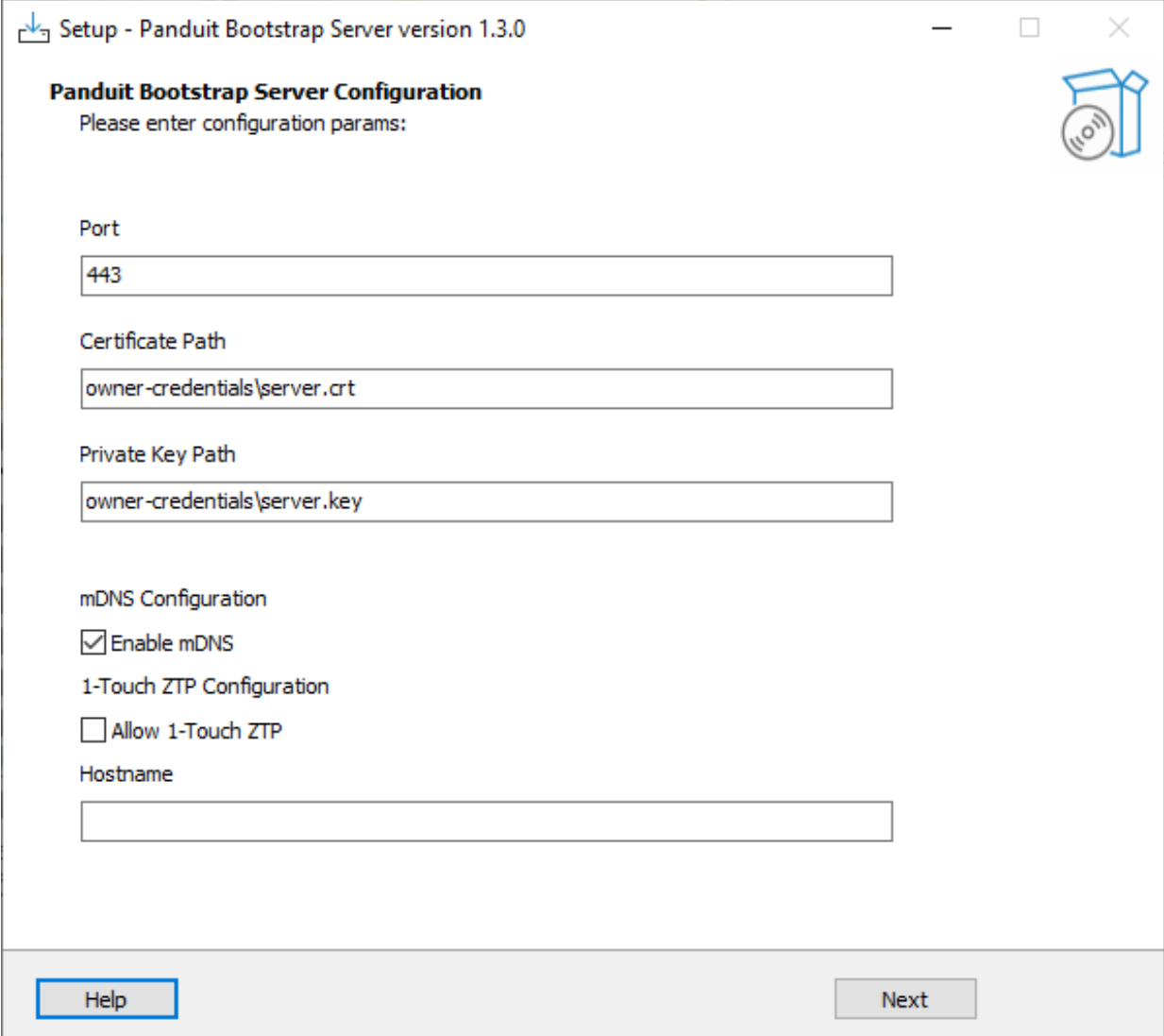


図 165: インストールの確認

- 7) ブートストラップサーバー構成オプションを設定します。SZTP の場合はデフォルトが推奨されます。これらのオプションは、インストール後に `server.cfg` を編集して変更できます。

ワンタッチプロビジョニングの場合:

- [Allow 1-Touch ZTP] をチェックします。
- ブートストラップサーバーの自己署名証明書を自動生成するために、[Certificate/Key Path] のテキストを削除し、ZTP の [Hostname] を指定します。



Setup - Panduit Bootstrap Server version 1.3.0

Panduit Bootstrap Server Configuration
Please enter configuration params:

Port
443

Certificate Path
owner-credentials\server.crt

Private Key Path
owner-credentials\server.key

mDNS Configuration
☒ Enable mDNS

1-Touch ZTP Configuration
☐ Allow 1-Touch ZTP

Hostname

Help Next

図 166: ブートストラップサーバー構成

- 8) インストール後のオプションを選択します。

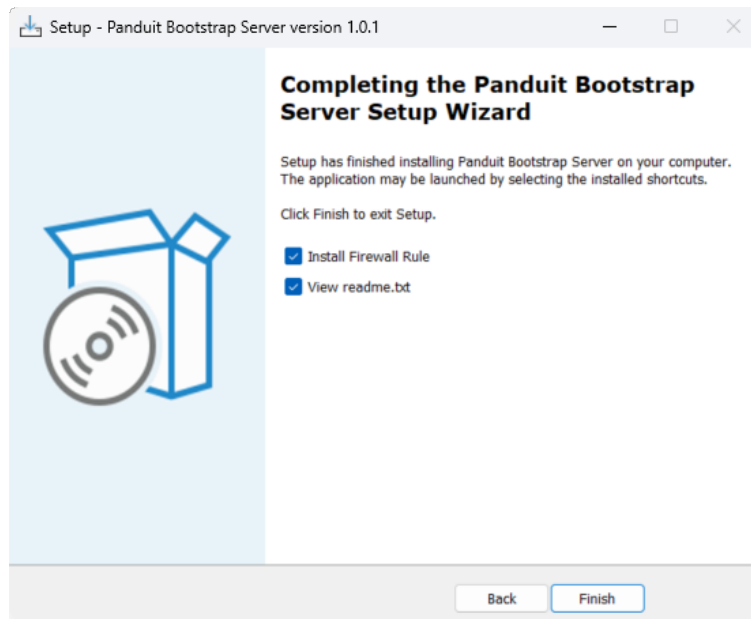


図 167: インストール後のオプション

【注意】サーバー上のファイアウォールが、インストールプロセスの最初の方で選択したポートをブロックする場合、SZTP は機能しません。ネットワーク上のデバイスがブートストラップサーバーと通信できるようにする Windows ファイアウォール規則をインストーラーによって追加するには、[Install Firewall Rule] をチェックしたままにします。Windows ファイアウォールを実行しないか、規則を手動で構成する場合、このオプションのチェックを外すことができます。

ブートストラップサーバー構成

- 1) パンドウイトからのバウチャーを、インストールフォルダの “ownership-vouchers” フォルダにコピーします。PDU ごとに 1 つのバウチャーファイルがあります。PDU のシリアル番号が ABC123 の場合、バウチャーファイルに「ABC123.vcj」という名前を付けます。
(ワンタッチの場合はこの手順をスキップします)
- 2) ブートストラップサーバー証明書およびキーを owner-credentials フォルダにコピーし、server.cfg に指定したとおりに名前を付けます。
 - サーバー証明書の [commonName] フィールド (または [subjectAltName] DNS フィールド) は、ブートストラップサーバーのアドレスに一致する必要があります。
 - commonName と subjectAltName の両方が存在する必要があります。
 - サーバー証明書は pinned-domain-cert と同じであってはなりません。サーバー証明書は、pinned-domain-cert によって署名されているか、pinned-domain-cert までたどることができる任意の数の中間エンティティによって署名される必要があります。
 - サーバー証明書は PEM 形式でなければならず、pinned-domain-cert までたどることができるすべての中間エンティティの証明書を含む必要があります。順番は、先頭がサーバー証明書で、次に中間エンティティがあり、最後に pinned-domain-cert となります。

- 3) 最新の EL2P ファームウェアパッケージをダウンロードし、“boot-image” フォルダにコピーします。
- 4) 各 PDU のための構成ファイルを作成します。
 - 構成ファイルは Web UI を使用して、同じタイプの Panduit PDU 上に作成できます。
 - 構成ファイルは [Settings] -> [System Management] -> [Actions] -> [Download Configuration] からダウンロードします。

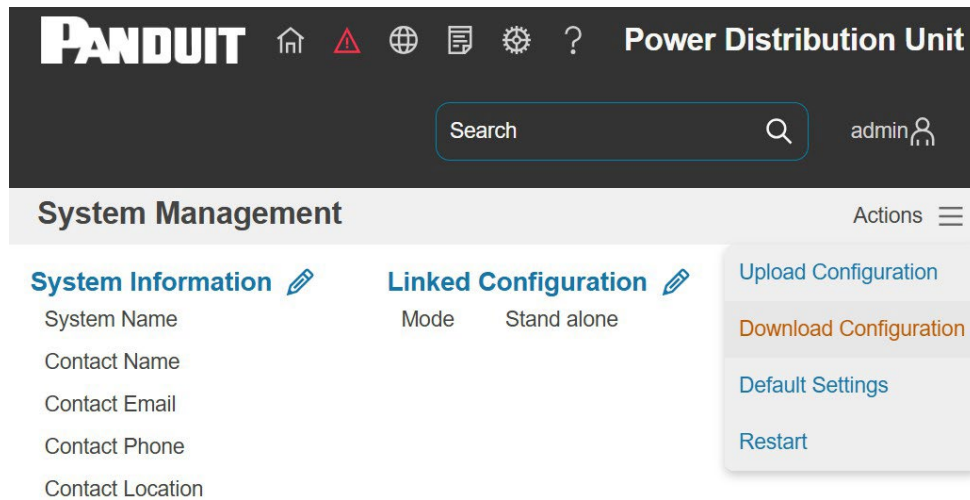


図 168: 構成のダウンロード

- 5) 各 PDU のための構成ファイルを“configurations”フォルダにコピーします。

構成ファイルは PDU ごとに 1 つ存在し、PDU のシリアル番号を使用して名前が付けられます。PDU のシリアル番号が ABC123 の場合、構成ファイルに「ABC123.json」という名前を付けます。

- 6) services.msc を実行し、[Panduit SZTP Bootstrap Service] を開始します。

デフォルトでは、サーバーは再起動すると自動的に開始されます。この動作はservices.msc を使用して変更できます。

SZTP のトラブルシューティング

- 1) Windows イベントビューアーを開きます。
- 2) [イベントビューアー] -> [Windows ログ] -> [Application] の下で、[PanBootstrapService] のすべてのイベントを確認します。

次のようにフィルターできます。

[現在のログをフィルター...] -> [イベントソース:] -> [PanBootstrapService] を選択します。

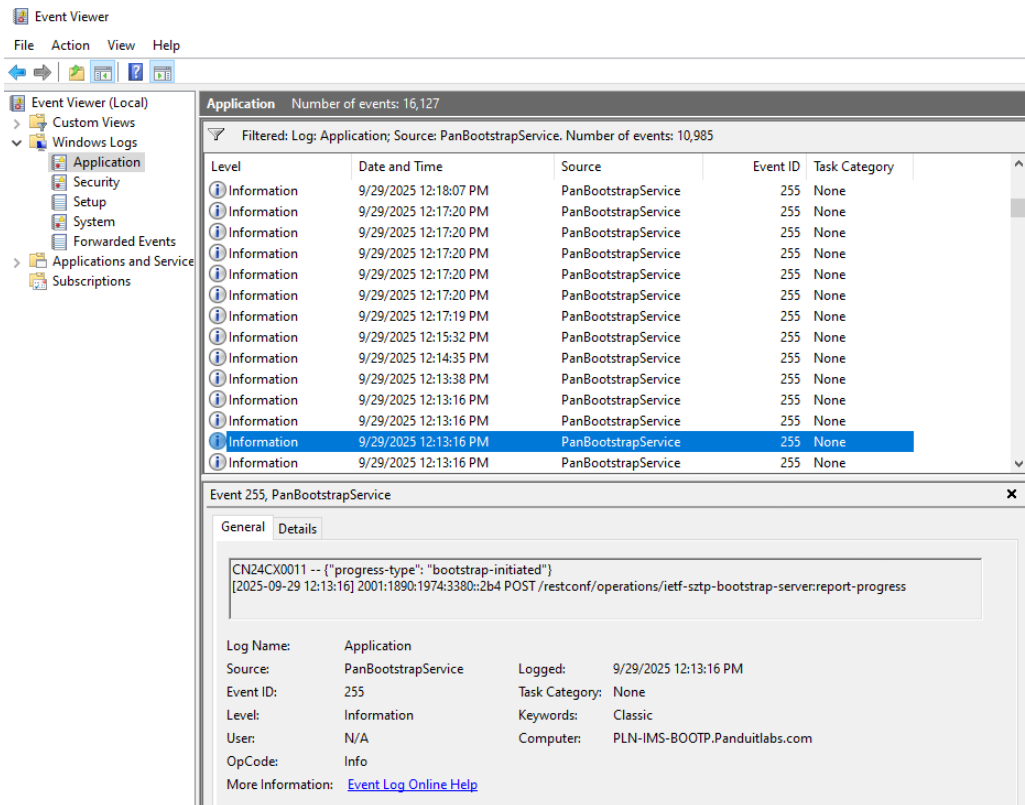


図 169: Windows イベントビューアー

- 3) 起動時にすべてのバウチャーが確認され、問題が発生した場合はログに記録されます。

- 4) 接続したすべての SZTP クライアントについて、SZTP の進捗状況がログに記録されています。

General	Details
CN24CX0011 -- {"progress-type": "bootstrap-initiated"} [2025-09-29 12:13:16] 2001:1890:1974:3380::2b4 POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress	
General	Details
CN24CX0011 -- {"progress-type": "informational", "message": "Boot image: Updating to version 8.8.8 from 6.6.6"} [2025-09-29 12:13:16] 2001:1890:1974:3380::2b4 POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress	
General	Details
CN24CX0011 -- {"progress-type": "boot-image-installed-rebooting"} [2025-09-29 12:14:35] 2001:1890:1974:3380::2b4 POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress	
General	Details
CN24CX0011 -- {"progress-type": "informational", "message": "Boot image: Already running version 8.8.8"} [2025-09-29 12:17:20] 2001:1890:1974:3380::2b4 POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress	
General	Details
CN24CX0011 -- {"progress-type": "informational", "message": "Configuration: Applied"} [2025-09-29 12:17:20] 2001:1890:1974:3380::2b4 POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress	
General	Details
CN24CX0011 -- {"progress-type": "bootstrap-complete"} [2025-09-29 12:17:20] 2001:1890:1974:3380::2b4 POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress	

図 170: SZTP イベントの例

付録 K: Onboard Data Collector の構成

Onboard Data Collector を使用すると、パンドウイト製の EL2P PDU を Cisco Nexus Dashboard から監視することができます。Onboard Data Collector は、EL2P PDU ファームウェア上に Panduit Data Collector の機能を提供します。“コレクター” PDU は、構成されたデバイスから 15 分ごとにポーリングすることによって、“デバイス” PDU からメトリクスを収集します。コレクター PDU はそれ自身のメトリクスを収集することもできます。

要件

Onboard Data Collector を利用するための要件は以下の通りです。

- 1) EL2P ファームウェアバージョン 1.6.4 以上。
- 2) 収集プロセスに関与する PDU に静的 IP または固定の DHCP リースが付与されている。
- 3) Cisco Nexus Dashboard バージョン 4.1.1 以上。

コレクター PDU のセットアップ

Onboard Data Collector をセットアップするには、“コレクター” に指定する PDU 上に admin ユーザーアカウントを構成する必要があります。このアカウントはローカルアカウントである必要があります。このユーザーアカウントをセットアップするには、以下の手順に従ってください。

- 1) コレクター PDU として構成する PDU に WebUI 経由でログインします。
- 2) WebUI で、[Settings] -> [User Accounts] に移動します。

Edit User

Username
collector

Role
Admin

Password
.....

Confirm Password
.....

Enabled
☒ Enable

Must Change Password at next Log In
☐ Enable

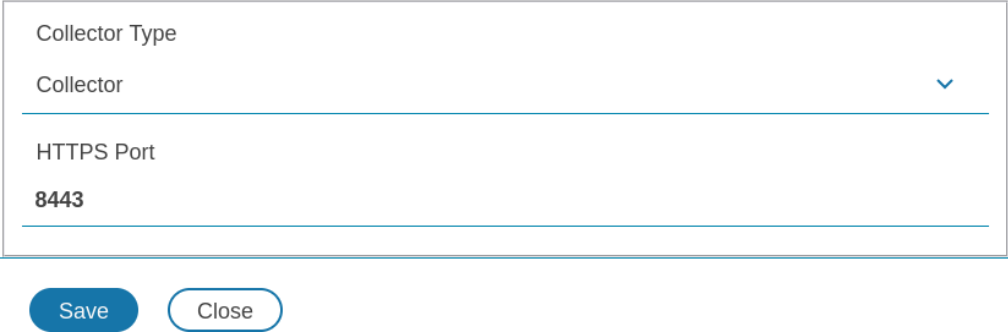
Save Close

図 171: コレクター PDU の Admin ユーザーの例

- 3) [Users] で、リストの一番下にある [Add User] 項目の右側にある鉛筆アイコンをクリックして、ユーザーアカウントを作成します。このユーザーは、“Admin” 役割を持つ必要があり、[Enabled] をチェックし、[Must Change Password at next Log In] のチェックを外す必要があります。

今度は、Onboard Data Collector を WebUI 上で構成する必要があります。

Onboard Data Collector Configuration



Collector Type

Collector

HTTPS Port

8443

Save Close

図 172: コレクター PDU での Onboard Data Collector の構成

- 1) WebUI で、[Settings] -> [Network] -> [Onboard Data Collector Configuration] に移動します。
- 2) [Collector Type] を [Collector] に設定します。これにより、Onboard Data Collector HTTPS Web サーバーが有効になります。このサーバーは、その HTTPS 証明書とプライベートキーを HTTPS Web サーバーと共有します。
 - a. [HTTPS Port] は、Cisco Nexus Dashboard と通信するために 8443 に設定する必要があります。このポート番号は別のポート番号と競合しないようにしてください。
 - b. この操作により、WebUI がホスティングされている HTTPS サーバー上のデバイス REST API が有効になるため、コレクター PDU のメトリクスをポーリングできるようになります。

デバイス PDU のセットアップ

コレクター PDU をセットアップしたら、今度はメトリクスを収集する対象のデバイス PDU をセットアップできます。コレクター PDU は、それ自身に登録したり、別のコレクター PDU に登録したりできることに注意してください。

コレクター PDU のセットアップと同じように、ユーザーはユーザーアカウントを作成する必要があります。

- 1) デバイス PDU として構成する PDU に WebUI 経由でログインします。
- 2) WebUI で、[Settings] -> [User Accounts] に移動します。

Edit User

Username

device

Role

Viewer

Password

.....

Confirm Password

.....

Enabled

☒ Enable

Must Change Password at next Log In

☐ Enable

Save

Close

図 173: デバイス PDU の Viewer ユーザーの例

- 3) [Users] で、リストの一番下にある [Add User] 項目の右側にある鉛筆アイコンをクリックして、ユーザーアカウントを作成します。このユーザーには“Viewer”役割を持たせることを推奨します。[Enabled] をチェックし、[Must Change Password at next Log In] のチェックを外す必要があります。
 - a. このアカウントは、データ収集アカウントとシステム管理アカウントを分離するために、“Viewer”役割で構成する必要があります。デバイスアカウントは Controller や Administrator とすることができますが、これらの追加の権限から受けるメリットはありません。

次に、PDU をデバイスとして構成することができます (注意: ユーザーがコレクター PDU を構成していて、コレクター PDU をそれ自身に登録したり、別のコレクター PDU に登録したりすることを希望している場合、この手順はスキップできます)。

Onboard Data Collector Configuration

Collector Type
Device
HTTPS Port
8443

Save Close

図 174: デバイス PDU での Onboard Data Collector の構成

- 1) WebUI で、[Settings] -> [Network] -> [Onboard Data Collector Configuration] に移動します。
- 2) [Collector Type] を [Device] に設定します。これにより、HTTPS Web サーバー上のデバイス REST API が有効になります。
 - a. この操作では、Onboard Data Collector HTTPS Web サーバーは有効にならないため、[HTTPS Port] は無視してもかまいません。
 - b. [Settings] -> [Network] -> [Web Access Configuration] の [HTTPS Port] の値は“443”である必要があります。つまり、WebUI がホスティングされている HTTPS ポートはポート 443 である必要があります。これにより、コレクター PDU がデバイス PDU と通信できます。

Cisco Nexus Dashboard への PDU 登録

ここで、ユーザーはコレクター PDU とデバイス PDU をセットアップする必要があります。ユーザーはここでコレクター PDU を Cisco Nexus Dashboard に登録することができます。Cisco Nexus Dashboard WebUI で、以下の手順に従ってください。

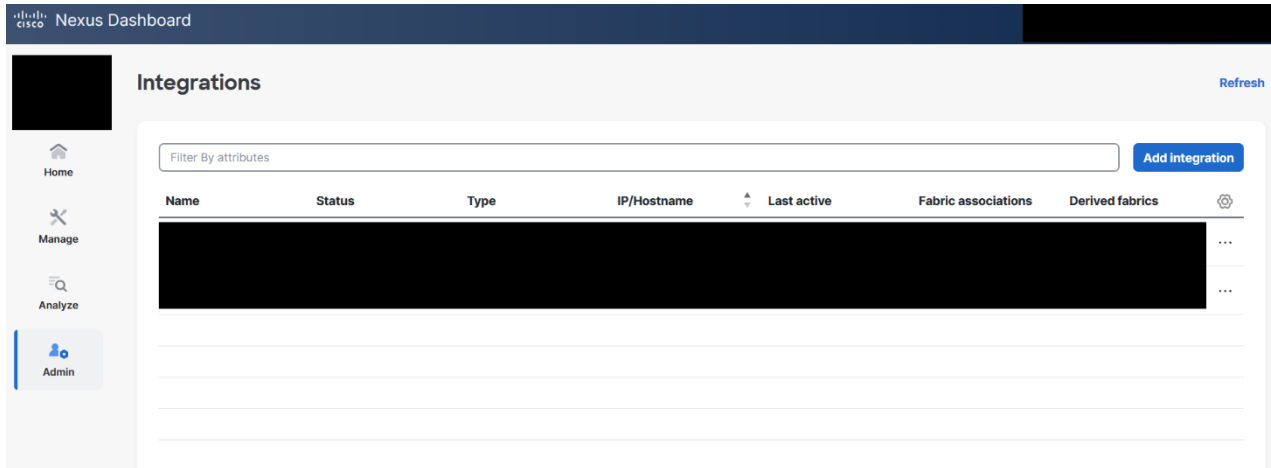


図 175: Cisco Nexus Dashboard の Integrations 画面

- 1) [Home] ページから、[Admin] -> [Integrations] に移動し、[Add integration] をクリックします。

Energy management



Panduit PDU

Monitor energy usage and unlock energy management insights for fabrics and individual devices connected to a Panduit PDU

図 176: Cisco Nexus Dashboard と Panduit PDU の統合

- 2) スクロールダウンして、[Panduit PDU] を選択します。

PDU Collector

Claim a Panduit PDU collector

Provide the IP and credentials for your Panduit PDU Collector, select a fabric to associate it with, and give it a name to identify it on Nexus Dashboard Insights. [What's a collector?](#)



You'll need to make sure your Panduit PDU Collector and PDUs are installed before continuing. [Learn more](#)

Collector name *

IP address *

Username *

Password *

[Show](#)

図 177: コレクター PDU を Cisco Nexus Dashboard に登録する

- 3) コレクター PDU のセットアップ中に作成された “Admin” 役割の資格情報を [Username] および [Password] フィールドに入力します。コレクター PDU の [IP address] を入力し、その [Collector name] を入力します。

Association

Fabric name	Type
Select...	-

図 178: ファブリックを選択する

- 4) PDU をファブリックと関連付け、[Save] をクリックします。

Add PDUs

Your Panduit PDU Collector is ready to be added—now, let's onboard your PDUs. How would you like to add PDUs to your collector?
You can add and remove additional PDUs later.

PDU Collector ✓ Added

 Collector version Vendor
PANDUIT

PDU Collector

Add the PDU at the address to the collector.

PDUs added to the collector

Add one or more IP addresses above

図 179: 登録されたコレクター PDU

- 5) コレクター PDU が正しく登録されます。ユーザーはここでデバイス PDU をコレクターに追加できます。登録するデバイス PDU の IP アドレスを入力し、[Add to collector] をクリックします。認証情報の入力を求めるプロンプトがユーザーに表示されます。
- a. コレクター PDU の IP アドレスを入力して自分自身のメトリクスを収集することができることに注意してください。

Add to collector

Please provide the credentials for 1 PDU.

SNMP protocol

Username *

Authentication type *

Authentication protocol *

Authentication password *

Priv protocol *

Priv password *

☐ Save as default

図 180: デバイス PDU の認証情報の例

- 6) [SNMP protocol] を選択し、[V3] を選択します。
- a. Onboard Data Collector では SNMP の代わりに HTTPS を使用するため、これらの設定をこのように構成する必要があることに注意してください。

- 7) [Username] を選択し、デバイス PDU のセットアップ中に作成された “Viewer” 役割のユーザーのデバイスユーザー名を入力します。
- 8) [Authentication type] を選択し、[authPriv] に設定します。
- 9) [Authentication protocol] を選択し、[SHA] に設定します。
- 10) [Authentication password] を選択し、“Viewer” 役割のユーザーのデバイスパスワードを入力します。
- 11) [Priv protocol] を選択し、[AES-256] を選択します。
- 12) [Priv password] を選択し、“Viewer” 役割のユーザーのデバイスパスワードを入力します。

各コレクター PDU に対して手順 1～4 を繰り返し、各デバイス PDU に対して手順 5～12 を繰り返すことで、ユーザーは監視する PDU を正しく登録できます。一部のデータは登録してから Cisco Nexus Dashboard に表示されるまで 15 分以上かかります。

注意

- コレクター PDU の “Admin” 役割のアカウントのパスワードを Cisco Nexus Dashboard UI 経由で変更した場合、新しいパスワードは NMC の強いパスワードの要件を満たす必要があります。

セキュリティ

ログインイベントを削減するため、Onboard Data Collector のリフレッシュエンドポイントでは、有効なリフレッシュトークンを与えたときに新しいリフレッシュトークンが生成されます。ユーザーが初めてログインしたとき、ユーザーは最初にログインエンドポイントを使用して、アクセストークンを取得する必要があります。

- NMC を再起動すると、すべてのアクセストークンとリフレッシュトークンがただちに期限切れとなります。
- ユーザーのアクセストークン期間 (5 分) を無効にすると、そのユーザーはログインできなくなり、そのユーザーに対して発行されたすべてのアクセストークンが期限切れとなります。
- ユーザーのリフレッシュトークン期間 (30 分) を無効にすると、そのユーザーはログインできなくなり、そのユーザーに対して発行されたすべてのアクセストークンおよびリフレッシュトークンが期限切れとなります。

通信図

以下の図は、Cisco Nexus Dashboard、コレクター PDU、およびポーリングされるデバイス PDU の間の通信を示しています。

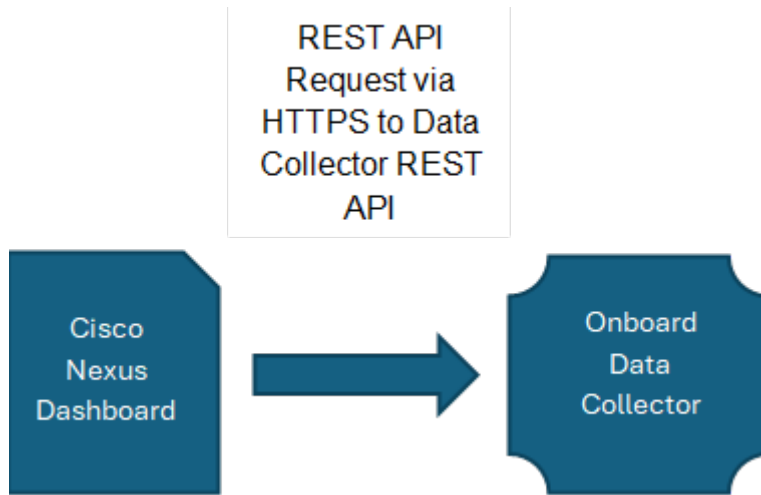


図 181: Cisco Nexus Dashboard から Onboard Data Collector への通信

上の図は、Onboard Data Collector と Cisco Nexus Dashboard の間の通常の通信を示しています。

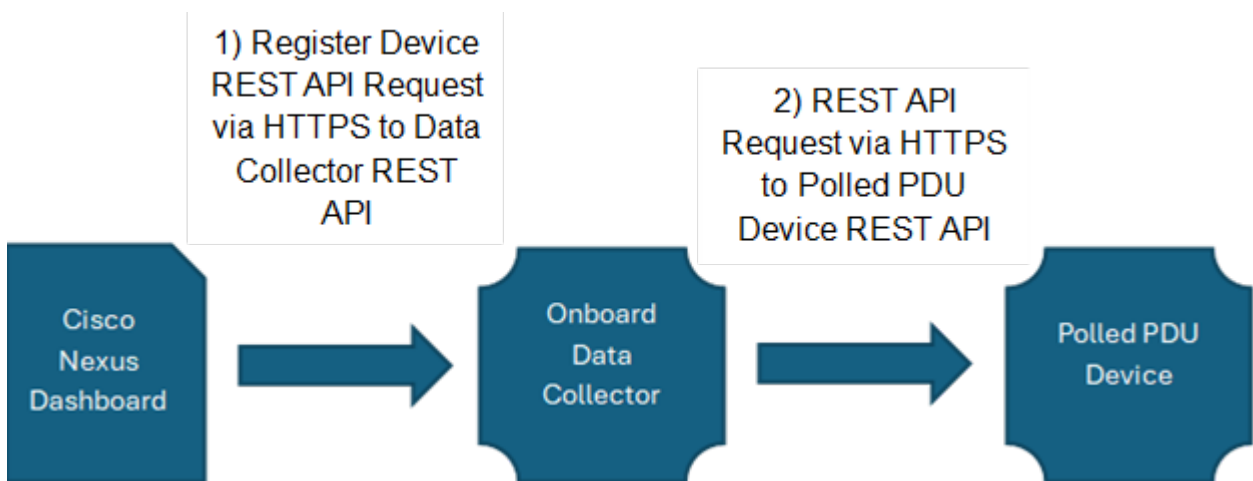


図 182: デバイス登録の通信

上の図は、Cisco Nexus Dashboard がデバイス PDU を登録するときの通信の例を示しています。

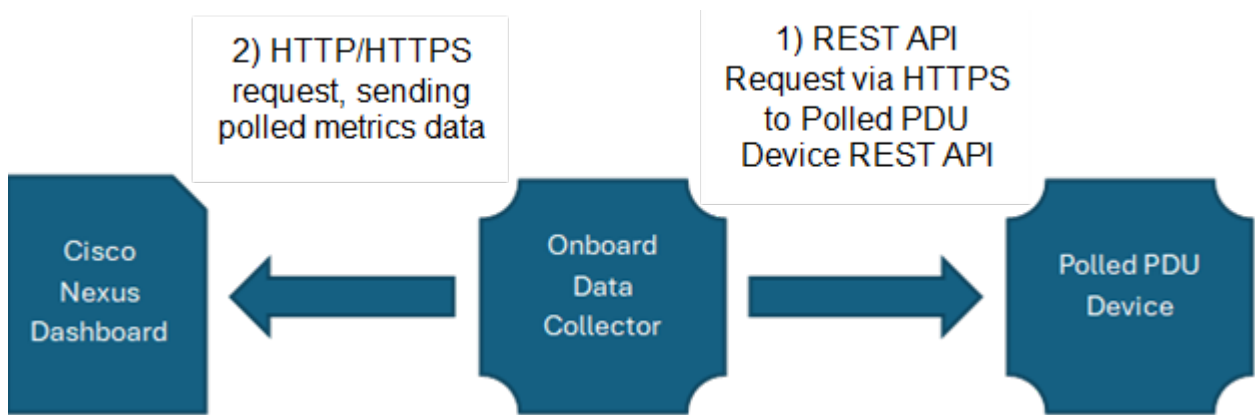


図 183: ポーリングするときの Onboard Data Collector 通信

上の図は、コレクター PDU がデバイス PDU をポーリングし、ポーリングされたデータを Cisco Nexus Dashboard に送信するときの通信の例を示しています。

付録 L: SiteCommand ユーティリティを使用した一括管理

SiteCommand ユーティリティは、複数の Panduit EL2P PDU にわたる一括構成およびファームウェア管理を簡素化するために、パンドウイットによって提供されている無料の軽量ソフトウェアツールです。

SiteCommand ユーティリティは、複数の Panduit EL2P PDU の管理を最適化する設置、試運転、および保守の活動用に設計されています。

SiteCommand ユーティリティの最新バージョンについては、panduit.com → Support → Download Center → PDU にアクセスしてください。

1. SiteCommand ユーティリティを Web ページからダウンロードします。
2. ダウンロードしたファイルを圧縮解除します。
3. SiteCommand ユーティリティのインストーラーファイルをダブルクリックして実行します。
4. 指示に従ってインストールプロセスを完了します。
5. ソフトウェアをインストールした後、デスクトップに追加された起動アイコンをクリックするか、Web ブラウザーに「<https://localhost:8557/>」と入力します。

【注意】詳細については、SiteCommand ユーティリティユーザーマニュアルを panduit.com → Support → Download Center → PDU からダウンロードしてください。

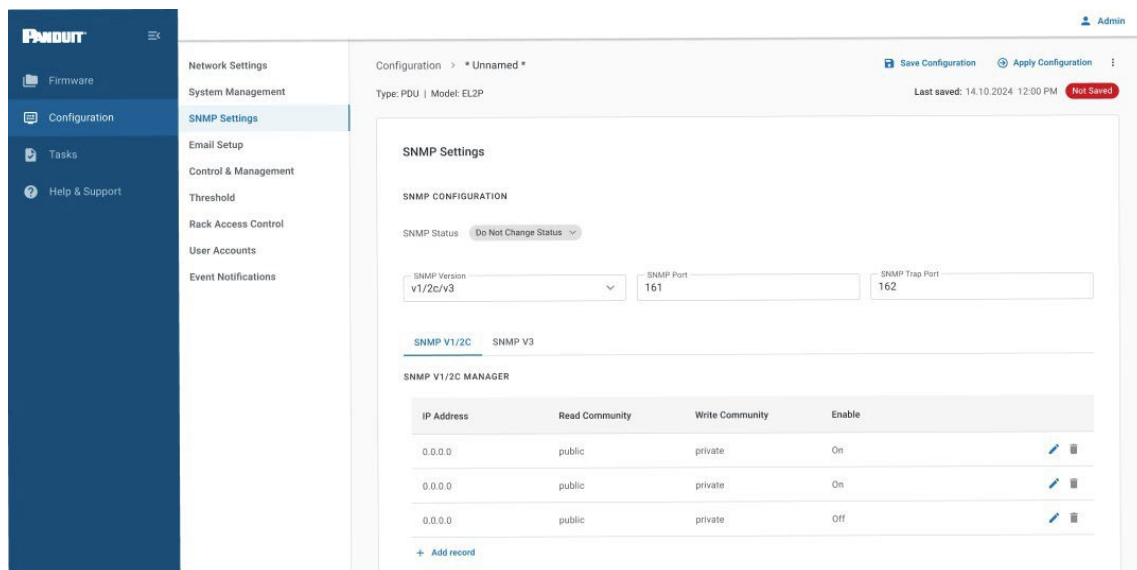


図 184: SiteCommand ユーティリティ

付録 M: よくある質問 (FAQ)

質問:

ブリッジモードで動作している PDU は、STP が有効なときに同じスイッチに接続できますか？ またはネットワークループを防ぐために別々のスイッチに接続すべきですか？

回答:

STP はネットワークループを防ぐように設計されているため、PDU は同じスイッチに接続することも、複数のスイッチに接続することもできますが、それらのスイッチが STP をサポートしていて同じサブネット内で動作していることが条件となります。STP が有効になっていて正しく機能しているとき、複数の PDU を同じスイッチに接続しても、ループは発生しません。

質問:

ブリッジモードは、STP が許可されない特定のスパインリーフアーキテクチャなどのネットワーク環境で使用できますか？

回答:

はい。ブリッジモードは STP が許容されない環境で動作できます。これらの場合は STP を無効にする必要があり、チェーンの最後のデバイスをネットワークに再び接続しないようにしてください。この接続によりループが発生します。

質問:

ネットワークに接続されたとき、PDU はスイッチによって別のスイッチングデバイスとして特定されますか？

回答:

STP が有効なとき、PDU は STP プロセスに参加しますが、LLDP を使用しないため、標準のネットワークスイッチとして完全には認識されません。基本的なループ防止動作は行いますが、スイッチとしての情報をアドバタイズしたり交換したりすることはありません。

質問:

パワーシェアはブリッジモードでも動作しますか？

回答:

はい。パワーシェアはブリッジモードで動作しますが、CLI 構成が必要です。これが必要となるのは、カスタマー機器に接続されているリンク上でパワーシェアを有効にすると、ネゴシエーションの問題が発生することがあるためです。

理想を言えば、パワーシェアは PDU 間でのみ有効にするべきで、エンドポイントでは有効にするべきではありません。スタンドアロンモードでは、パワーシェアはデフォルトで無効になっていますが、これは通常 PDU がカスタマー機器に直接接続されているためです。

質問:

ブリッジモードでは、WebGUI は隣接する PDU を表示しますか？ またはスタンドアロン装置として動作しますか？

回答:

スタンドアロンモードの PDU は隣接する PDU を認識しません。

質問:

チェーン内の 1 番目と 3 番目の PDU のみブリッジモードが有効になっている場合、WebGUI はどのように動作しますか？

回答:

ベストプラクティスとして、1 つのトポロジーを選び、すべての PDU にわたって一貫して適用します。同じチェーン内でモードを混用することは推奨されません。