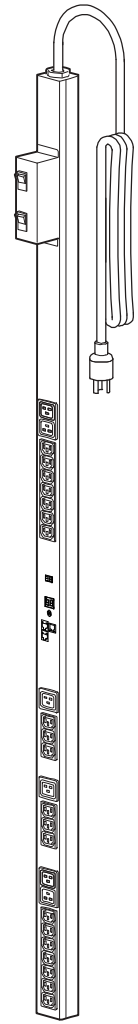
ユーザーズガイド

Managed Rack Power Distribution Unit



目次

はじめに

製品の機能

Dell® Managed Rack Power Distribution Unit (PDU) は、ネットワークで管理できるスタンドアロンの配電機器です。Rack PDU は、接続されている負荷をリアルタイムでリモート監視する機能を備えています。ユーザーが定義する警報信号により、電気回路の過負荷の可能性を警告します。リモートコマンドとユーザーインターフェイス設定を使用して、Rack PDU でコンセントのあらゆる管理を行うことができます。

Rack PDU は、Web インターフェイス、コマンドラインインターフェイス (CLI)、あるいは Simple Network Management Protocol (SNMP) を使用して管理できます。

- HTTP (HyperText Transfer Protocol) または HTTPS (HTTP over SSL (Secure Sockets Layer) を使用して、Web インターフェイスにアクセスできます。Web インターフェイスへのログオンを参照してください。
- シリアル接続、Telnet、または Secure Shell (SSH) を使用して、コマンドラインインターフェイスにアクセスできます。コマンドラインインターフェイスについてを参照してください。
- Rack PDU の管理には、SNMP ブラウザと Dell Management Information Base (MIB) を使用することができます。

Rack PDU には、次の追加機能があります。

- 接続されている全負荷のピーク負荷、電力およびエネルギーの監視
- 相の電圧、電流、電力の監視
- 各コンセントの電力の監視
- 電気回路の過負荷防止に役立つ、ネットワークと視覚に訴える警告を提供する設定が可能な警告しきい値
- 次の 4 レベルのユーザーアクセスアカウント：管理者 (Administrator)、デバイスユーザー (Device User)、読み取り専用ユーザー (Read-Only User)、コンセントユーザー (Outlet User)

- 独立したコンセント制御
- 設定可能な電源待機時間
- 最大 24 個の独立したコンセントユーザーアカウント
- イベントおよびデータの記録。イベントログには Telnet、セキュア CoPy（SCP）、ファイル転送プロトコル（FTP）、シリアル接続、または Web インターフェイス（SSL による HTTPS アクセス、または HTTP アクセス）でアクセスできます。データログには、Web ブラウザ、SCP、または FTP でアクセスできます。
- Rack PDU やシステムイベントの電子メールによる通知
- Rack PDU とシステムイベントの重要度、カテゴリに応じた SNMP トラップ、Syslog メッセージ、電子メール通知
- 認証および暗号化用セキュリティプロトコル

Rack PDU では、電源のサージ保護機能を備えていません。デバイスが電源障害や電源サージから保護されているか確認するには、Rack PDU を UPS（無停電電源装置）に接続してください。

ログオン時のアクセスの優先度

Rack PDU に同時にログオンできるのは、一人のユーザーのみです。アクセスの優先度を、高い順に示します。

- Rack PDU に直接シリアル接続されているコンピュータから、ローカルでコマンドラインインターフェイスにアクセスする場合
- リモートコンピュータから、Telnet または Secure Shell（SSH）を使用してコマンドラインインターフェイスにアクセスする場合
- Web アクセス

Rack PDU への SNMP アクセスの仕組みについては、SNMP を参照してください。

ユーザーアカウントの種類

Rack PDU には、管理者、デバイスユーザー、読み取り専用ユーザー、コンセントユーザーの 4 種類のアクセスレベルがあり、すべてがパスワードとユーザー名によって保護されています。

- 管理者は、Web インターフェイスの全メニューとコマンドラインインターフェイスの全コマンドを使用できます。デフォルトのユーザー名とパスワードはともに「admin」です。
- デバイスユーザーがアクセスできるのは以下に限られています。
  - Web インターフェイスでは [Device Manager] タブと [Environment] タブのメニュー、および [Logs] タブの左側ナビゲーションメニューの [Events] 項目と [Data] 項目からアクセスできるイベントログとデータログ イベントログとデータログではログを消去するためのボタンは表示されません。
  - コマンドラインインターフェイスの場合でも、上述と同様の機能とオプションにアクセスできます。

  デフォルトのユーザー名とパスワードはともに「device」です。
- 読み取り専用ユーザーのアクセスは以下のように制限されています。
  - Web インターフェイスを通したアクセスに限られます。
  - デバイスユーザーと同じタブとメニューへのアクセスは可能ですが、設定変更、デバイスの制御、データの削除、またはファイル転送オプションの使用はできません。環境設定オプションへのリンクは表示されますが、無効になっています。イベントログとデータログではログを消去するためのボタンは表示されません。

  デフォルトのユーザー名とパスワードはともに「readonly」です。

上記の 3 種類のユーザーアカウントの**ユーザー名**および**パスワード**の設定方法については、ユーザーアクセスの設定を参照してください。

・コンセントユーザーのアクセス権は、次のように制限されます。
  - Web インターフェイスとコマンドラインインターフェイスを使用したアクセス
  - デバイスユーザーと同じメニューへのアクセスは可能ですが、設定変更、デバイスの制御、データの削除、またはファイル転送オプションの使用は制限されます。環境設定オプションへのリンクは表示されますが、無効になっています。コンセントユーザーは、[Outlet Control]（コンセントの管理）メニューオプションにアクセスでき、これにより管理者によって割り当てられたコンセントを管理できます。コンセントユーザーは、イベントやデータログを消去することはできません。

ユーザー名とパスワードは、新規コンセントユーザーを追加する時に管理者が定義します。

はじめに

Rack PDU の使用を開始するには、次の手順を実行します。

1. ご購入の Rack PDU に同梱の「*Rack Power Distribution Unit Installation Instructions*」を使用して、Rack PDU を設置します。
2. 電源を投入してご使用のネットワークに接続します。「*Rack Power Distribution Unit Installation Instructions*」に記載の手順に従ってください。
3. ネットワーク設定を確立します。（ネットワーク設定の確立を参照）。
4. 下記の方法のいずれかを使用して、Rack PDU の使用を開始します。
   - Web インターフェイス
   - コマンドラインインターフェイス
   - Rack PDU の前面パネル

ネットワーク設定の確立

次の TCP/IP 情報を設定することにより、Rack PDU をネットワーク上で動作させることができます。

- Rack PDU の IP アドレス
- サブネットマスク
- デフォルトゲートウェイ

デフォルトゲートウェイが使用できない場合は、Rack PDU と同じサブネット上にあり、通常動作しているコンピュータの IP アドレスを指定します。トラフィックが非常に少ない場合、Rack PDU はデフォルトゲートウェイを使ってネットワークのテストを行います。

ループバックアドレス（127.0.0.1）を Rack PDU のデフォルトゲートウェイアドレスとして使用しないでください。ループバックアドレスを使用するとカードは無効になり、ローカルシリアルログオンを使用して TCP/IP 設定をデフォルトにリセットするよう要求されます。

TCP/IP の設定方法

次のいずれかの方法で、Rack PDU に必要な TCP/IP を設定します。

- BOOTP と DHCP の設定
- コマンドラインインターフェイス

BOOTP と DHCP の設定

デフォルトの TCP/IP 設定である **DHCP** は、適切に設定した DHCP サーバーにより、TCP/IP 設定を Rack PDU に提供できることを前提としています。

ユーザー設定（.ini）ファイルは、BOOTP または DHCP ブートファイルとしての機能をもつことができます。詳細については、.ini ファイルの使用を参照してください。

BOOTP Rack PDU で BOOTP サーバーを使用して TCP/IP 設定を行うには、適切に設定された RFC951-準拠の BOOTP サーバーを検出する必要があります。

BOOTP サーバーの BOOTPTAB ファイルに、Rack PDU の MAC アドレス、IP アドレス、サブネットマスク、デフォルトゲートウェイ、およびオプションで bootup ファイル名を入力してください。MAC アドレスについては、Rack PDU の下部、またはこのパッケージに付属の品質保証テスト票を参照してください。

Rack PDU を再起動すると、BOOTP サーバーが TCP/IP 設定情報を提供します。

- bootup ファイル名を指定すると、Rack PDU は、TFTP または FTP を使用して、BOOTP サーバーからこのファイルを転送しようとします。Rack PDU は、bootup ファイルにある指定されたすべての設定を利用します。
- bootup ファイル名を指定していない場合は、Web インターフェイスまたはコマンドラインインターフェイスを使用して、リモートで Rack PDU の環境設定を行うことができます。

bootup ファイルを作成するには、BOOTP サーバーのマニュアルを参照してください。

DHCP RFC2131/RFC2132 準拠の DHCP サーバーを使用して、Rack PDU の TCP/IP 値を設定できます。

ここでは、Rack PDU と DHCP サーバーの通信について簡単に説明します。DHCP サーバーで Rack PDU のネットワーク設定を行う方法については、DHCP 応答オプションを参照してください。

1. Rack PDU は、DHCP リクエストを送信しますが、このときに自らを識別するために、次のいずれかの識別子を使用します。
   - ベンダークラス識別子
   - クライアント識別子（デフォルトでは、Rack PDU の MAC アドレス）
   - ユーザークラス識別子（デフォルトでは、Rack PDU にインストールされているアプリケーションファームウェアの識別子）
2. 適切に設定された DHCP サーバーは、ネットワーク通信のために Rack PDU で必要なすべての設定を含む DHCP レスポンスを返します。また、DHCP レスポンスには、[Vendor Specific Information] オプション（DHCP オプション 43）があります。Rack PDU では、DHCP オプション 43 のベンダー cookie が次の 16 進数形式でカプセル化されていない DHCP レスポンスを無視するように設定することができます。（デフォルトでは、Rack PDU にはこの cookie は必要ありません。）

   ```
   Option 43 = 01 04 31 41 50 43
   ```

   それぞれ次の内容を表します。
   - 最初のバイト（01）はコード
   - 第 2 バイト（04）は長さ
   - 残りのバイト（31 41 50 43）はベンダー cookie

[Vendor Specific Information] オプションにコードを追加するには、DHCP サーバーのマニュアルを参照してください。

注意：Web インターフェイスの [Require vendor specific cookie to accept DHCP Address]（DHCP アドレスを有効とするにはベンダー固有の cookie が必要）チェックボックスを選択して、DHCP サーバーがベンダー固有の cookie を取得して Rack PDU に [Administration]>[Network]>[TCP/IP]>[ipv4 settings] の情報を提供するように設定できます。

コマンドラインインターフェイス

1. コマンドラインインターフェイスにログオンします。コマンドラインインターフェイスへのログオンを参照してください。
2. ネットワーク管理者に連絡し、Rack PDU の IP アドレス、サブネットマスク、デフォルトゲートウェイを取得してください。
3. ネットワーク設定には次の 3 つのコマンドを使用します （イタリック体の部分は変数です）。
   a. `tcpip -i yourIPaddress`
   b. `tcpip -s yourSubnetMask`
   c. `tcpip -g yourDefaultGateway`

   それぞれの変数に対し、*xxx.xxx.xxx.xxx* の形式で数値を入力します。
   例えば、システムの IP アドレスとして「156.205.14.141」を設定する場合、次のコマンドを入力してから ENTER キーを押します。
   `tcpip -i 156.205.14.141`
4. 「**exit**」と入力します。Rack PDU を再起動して、変更を適用します。

パスワードを忘れた場合

パスワードを忘れた場合は、Rack PDU またはその他のデバイスにシリアルポートで接続されているローカルコンピュータを使用して、コマンドラインインターフェイスにアクセスします。

1. ローカルコンピュータのシリアルポートを選択して、このポートを使用するサービスをすべて無効にします。
2. 付属のシリアルケーブルをコンピュータの選択したポートと Rack PDU にあるシリアルポートに接続します。
3. 端末プログラム（HyperTerminal® など）を起動し、選択したポートの設定を 2400bps、データビット 8、パリティなし、ストップビット 1、フロー制御なしに変更します。
4. ENTER キーを押して（必要に応じて繰り返し押してください）、[User Name] プロンプトを表示します。[User Name] プロンプトを表示できない場合は、次を確認してください。
   - このシリアルポートが他のアプリケーションによって使用されていないこと。
   - 端末の設定が手順 3 の指定通りに正しく行われていること。
   - 手順 2 で指定の適切なケーブルが使用されていること。
5. リセット ボタンを押します。ステータス LED が orange と緑の交互点滅になります。LED が点滅している間に再度リセットボタンを押して、ユーザー名とパスワードを一時的にデフォルト値に戻します。
6. ENTER キーを数回押して [User Name] プロンプトを再表示します。その後、ユーザー名とパスワードとしてデフォルト値の「dell」を入力します（[User Name] プロンプトの再表示後、ログオンに 30 秒以上かかった場合は、手順 5 を繰り返してログオンし直す必要があります）。

7. コマンドラインインターフェイスで次のコマンドを使用して、その時点では「dell」になっている [User Name] と [Password] の値を変更します。

   user -an *yourAdministratorName*

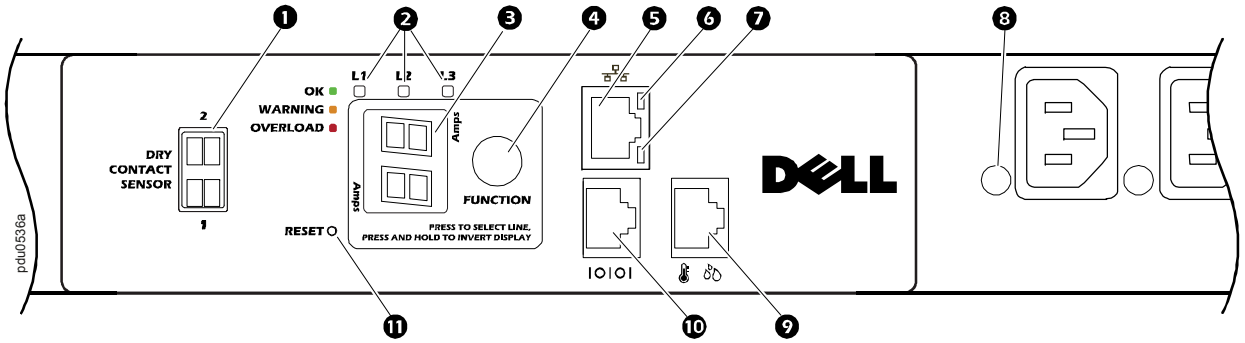
   user -ap *yourAdministratorPassword*

   例えば、管理者のユーザー名を「Don Adams」に変更したい場合は次のように入力します。

   user -an Don Adams

8. 「**quit**」または「**exit**」と入力してログオフし、シリアルケーブルの接続を外してある場合はすべて接続し直し、無効にしたサービスもすべて再起動します。

Rack PDU の前面パネル



項目		機能
❶	ドライ接点入力	2 つのドライ接点デバイスのコネクタです。
❷	相表示 LED 注意：単相 Rack PDU の場合は、LED は 1 つのみです。	アラームが発生していない時は、LED には相の電流が表示されます。いずれか一方の相表示 LED に緑が点灯します。システムは各相を自動的に循環し、相の電流を 3 秒間表示します。 一方の相にアラームが発生した場合は該当する相表示 LED が点灯し、アラーム状態が解消されるまで点灯し続けます。LED には、警告アラームの場合はオレンジが、致命的アラームの場合は赤が点灯します。複数の相でアラームが発生した場合は、システムはアラームが発生した各相を自動的に循環し、相表示 LED を 3 秒間点灯します。
❸	LED ディスプレイ	点灯中の相表示 LED の相電流を表示します。

項目		機能
❹	機能ボタン	・各相の電流を手動で表示するには、このボタンを繰り返し押します。電流は 30 秒間、またはボタンを再度押すまで表示されます。（この機能は単相 Rack PDU では使用できません。） ・IP アドレスを表示するには、IP アドレスが表示されるまで 5 秒間ボタンを押し続けます。IP が表示されたら、ボタンを離します。LED ディスプレイ上で、アドレスが 2 桁ごとに繰り返し表示されます。 ・表示を切り替えるには、「AA」と表示されるまで 10 秒間ボタンを押し続けます。「AA」と表示されるまでボタンを押し続け、表示されたらボタンを離します。
❺	10/100 base-T コネクタ	Rack PDU をネットワークに接続するポートです。
❻	10/100 LED	10/100 LED を参照してください。
❼	ネットワークステータス LED	ネットワークステータス LED を参照してください。
❽	コンセントステータス LED	コンセントに通電しているときには、緑色に点灯します。（各コンセントにコンセント LED が付いています。）
❾	温度 / 湿度センサポート	Rack PDU Temperature Sensor（温度センサ）（G853N）または Rack PDU Temperature/Humidity Sensor（温度 / 湿度センサ）（H621N）を接続するポートです。
❿	RJ-45 シリアルポート	コマンドラインインターフェイスにローカルアクセスするために、Rack PDU を端末エミュレータプログラムに接続するポートです。付属のシリアルケーブルを使用してください。
⓫	リセットボタン	電源出力に影響を及ぼさずに Rack PDU のインターフェイスを再起動するには、このリセットボタンを押して離します。

ネットワークステータス LED

状態	説明
オフ	次のいずれかの状況です。 ・Rack PDU が入力電力を受けていません。 ・Rack PDU が正常に動作していません。修理または交換が必要な可能性があります。
緑色の点灯	Rack PDU の TCP/IP 設定が有効です。
緑色の点滅	Rack PDU の TCP/IP 設定が正しくありません。
オレンジ色の点灯	Rack PDU でハードウェア障害が検出されました。
オレンジ色の点滅	Rack PDU では BOOTP リクエストを作成しています。
オレンジと緑に交互点滅	LED がゆっくり点滅している場合、Rack PDU は DHCP リクエストを作成しています。 LED が素早く点滅している場合、Rack PDU は起動中です。

1. BOOTP または DHCP サーバーを使用していない場合は、ネットワーク設定の確立を参照して Rack PDU の TCP/IP 設定を行ってください。
2. DHCP サーバーの使用方法については、TCP/IP 設定と通信設定を参照してください。

10/100 LED

状態	説明
オフ	以下のいずれか（ひとつまたは複数）の状況です。 ・Rack PDU が入力電力を受けていません。 ・Rack PDU とネットワークを接続しているケーブルが接続されていないか、あるいは故障しています。 ・Rack PDU とネットワークを接続している機器に電源が入っていません。 ・Rack PDU 自体が正常に動作していません。修理または交換が必要な可能性があります。
緑の点灯	Rack PDU は 10 メガビット / 秒（Mbps）の速度で作動するネットワークに接続されています。
オレンジ色の点灯	Rack PDU は 100 Mbps の速度で作動するネットワークに接続されています。
緑色の点滅	Rack PDU はデータパケットを 10 Mbps の速度で受信中または送信中です。
オレンジ色の点滅	Rack PDU はデータパケットを 100 Mbps の速度で受信中または送信中です。

コマンドラインインターフェイス

コマンドラインインターフェイスについて

コマンドラインインターフェイスを使用して、Rack PDU の状態を表示したり Rack PDU を管理することができます。さらに、コマンドラインインターフェイスでは操作を自動化するスクリプトを作成することができます。コマンドラインインターフェイスに対して、管理者はフルアクセス権、デバイスユーザーとコンセントユーザーは制限付きアクセス権を持ち、読み取り専用ユーザーは完全にアクセスを禁止されます。（詳細については、ユーザーアカウントの種類を参照してください。）

コマンドラインインターフェイス（CLI）を使用して INI ファイルを Rack PDU に転送することにより、Rack PDU の（CLI に固有のコマンドにはないパラメータを含む）すべてのパラメータを設定することができます。CLI では、ファイル転送に XMODEM を使用します。ただし、転送する INI ファイルを XMODEM で読み取ることはできません。

コマンドラインインターフェイスへのログオン

コマンドラインインターフェイスにアクセスするには、Rack PDU と同じネットワーク上にあるコンピュータからローカル（シリアル）接続あるいはリモート（Telnet または SSH）接続を使って行います。

Rack PDU

コマンドラインインターフェイスへのリモートアクセス

コマンドラインインターフェイスへのリモートアクセスは、Telnet または SSH を通して行います。デフォルトでは Telnet が有効になっています。SSH を有効にすると、Telnet は無効になります。

これらのアクセス手段を有効または無効にするには、Web インターフェイスを使用します。[Administration] タブ、上部メニューバーの [Network]、および左側ナビゲーションメニューの [Console] の下の [access] オプションの順に選択します。

Telnet による基本アクセス Telnet はユーザー名とパスワードによる基本的な認証セキュリティを提供しますが、暗号化による高度なセキュリティには対応していません。

Telnet を使用してコマンドラインインターフェイスにアクセスするには次の手順で行います。

1. Rack PDU と同じネットワーク上のコンピュータのコマンドプロンプトで「**telnet**」と入力し、その後 Rack PDU の IP アドレス（例えば、「**telnet 139.225.6.133**」（Rack PDU がデフォルトの Telnet ポート 23 を使用している場合））を入力して、ENTER キーを押します。
   Rack PDU がデフォルト以外のポート番号（5000 から 32768）を使用している場合、IP アドレス（または DNS 名）の後にコロンまたはスペースに続けて（Telnet クライアントによって異なります）、ポート番号を指定します。（これは一般的に使用されるコマンドの場合です。ポート番号を指定できない Telnet コマンドもあります。また、他のコマンドが必要な場合があります。）
2. ユーザー名とパスワードを入力します（デフォルトでは管理者用が「admin」と「admin」、デバイスユーザー用が「device」と「device」）。

ユーザー名やパスワードを忘れた場合については、パスワードを忘れた場合を参照してください。

SSH による高度なセキュリティのアクセス Web インターフェイスに高度な SSL セキュリティを使用している場合は、SSH によりコマンドラインインターフェイスにアクセスします。SSH は、ユーザー名、パスワード、および伝送データを暗号化します。SSH と Telnet のどちらを使用してコマンドラインインターフェイスにアクセスしても、インターフェイス、ユーザーアカウント、およびユーザーアクセス権限は同じですが、SSH を使用する場合は、まず SSH を設定し、使用するコンピュータに SSH クライアントプログラムをインストールする必要があります。

コマンドラインインターフェイスへのローカルアクセス

ローカルでアクセスする場合は、Rack PDU のシリアルポートとローカルコンピュータをシリアルケーブルで接続し、コマンドラインインターフェイスにアクセスします。

1. コンピュータのシリアルポートを選択して、このポートを使用する他のサービスを無効にします。
2. コンピュータの選択したシリアルポートから、付属のシリアルケーブルを使用して Rack PDU のシリアルポートに接続します。
3. 端末プログラム（HyperTerminal など）を起動し、選択したポートの設定を 9600 bps、データビット 8、パリティなし、ストップビット 1、フロー制御なしに変更します。
4. ENTER キーを押してプロンプト画面でユーザー名とパスワードを入力します。

メイン画面について

下記は Rack PDU のコマンドラインインターフェイスにログオンしたときに表示されるメイン画面の一例です。

```
Dell Corporation                          Network Management Card AOS  vx.x.x
(c)Copyright 2009 All Rights Reserved  RPDUD                           vx.x.x
-------------------------------------------------------------------------------
Name     : Test Lab                                    Date : 10/30/2009
Contact  : Don Adams                                   Time : 5:58:30
Location : Building 3                                  User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes                Stat : P+ N+ A+

cli>
```

メイン画面の情報フィールドは、次のとおりです。

- 次の 2 つのフィールドでは、オペレーティングシステム（AOS）とアプリケーション（APP）のファームウェアバージョンを識別できます。アプリケーションファームウェア名は、ネットワークに接続している装置の種類を確認するために使用します。前述の例では、Rack PDU のアプリケーションファームウェアが表示されています。

  ```
  Network Management Card AOS  vx.x.x

  RPDUD vx.x.x
  ```

- 次の 3 つのフィールドでは、Rack PDU のシステム名、担当者、設置場所を識別できます。(Control Console の場合は、[System] メニューを使用してこれらの値を設定します。)

  ```
  Name: Test Lab

  Contact: Don Adams

  Location: Building 3
  ```

- [Up Time] フィールドには、Rack PDU が起動してから、またはリセットされてからの動作時間が表示されます。

  ```
  Up Time: 0 Days, 21 Hours, 21 Minutes
  ```

- 次の 2 つのフィールドは、ログオン日時を表します。

  ```
  Date : 10/30/2009

  Time : 5:58:30
  ```

- [User] フィールドには、管理者としてログオンした（Administrator）か、デバイスユーザーとしてログオンした（Device ）かが表示されます。([Read Only User] アカウントではコマンドラインインターフェイスにはアクセスできません。)

  ```
  User : Administrator
  ```

・[Stat] フィールドには、Rack PDU のステータスが表示されます。

```
Stat : P+ N+ A+
```

P+	Dell オペレーティングシステムは正常に稼動しています。

IPv4 のみ	IPv6 のみ	IPv4 および IPv6*	説明
N+	**N+**	**N4+ N6+**	ネットワークは正常に機能しています。
N?	**N6?**	**N4? N6?**	BOOTP リクエストサイクルの処理中です。
N-	**N6ñ-**	**N4+ N6+**	Rack PDU はネットワークへの接続に失敗したことを示します。
N!	**N6!**	**N4! N6!**	他の機器が Rack PDU の IP アドレスを使用していることを示します。
* N4 と N6 の値は互いに異なる場合があります。例えば、N4- N6+ という値になる場合があります。			

A+	アプリケーションは正常に機能していることを示します。
A-	アプリケーションのチェックサムが間違っていることを示します。
A?	アプリケーションの初期化中であることを示します。
A!	アプリケーションと AOS に互換性がありません。

P+ が表示されない場合は、Dell サポートスタッフにお問い合わせください。

コマンドラインインターフェイスの使用

コマンドラインインターフェイスには Rack PDU の環境設定のためのコマンドを入力します。コマンドを使用するには、まず該当のコマンドを入力し、次に ENTER キーを押します。コマンドと引数は、小文字、大文字、または両方の組み合わせのいずれも有効です。オプションで大文字と小文字を区別することができます。

コマンドラインインターフェイスではまた、以下も実行できます。

- 「**?**」と入力して ENTER キーを押すと、ユーザーのアカウントタイプに基づいて利用可能なコマンドの一覧が表示されます。
- 特定のコマンドの意味とシンタックスを確認するには、該当のコマンド、スペース（英字スペース 1 つ分）の順に入力し、次に「**?**」あるいは「**help**」と入力します。例えば、RADIUS の環境設定オプションを表示する場合には次のように入力します。

  radius ?

  または

  radius help

- 上向き矢印キーを押すと、セッションで最後に使用したコマンドを表示できます。上向きと下向きの矢印キーを使用して、最近使用した 10 個までのコマンドの一覧をスクロールできます。
- コマンドラインにコマンドを 1 字以上入力し始めてから TAB キーを押すと、入力した文字列に相当する有効なコマンドの一覧をスクロールできます。
- 「**exit**」または「**quit**」と入力すると、コマンドラインインターフェイスとの接続を解除できます。

コマンド構文

項目	説明
-	オプションの前にはハイフンが必要です。
< >	オプションの定義は山括弧で囲みます。例えば次のようになります。 -dp <device password>
[ ]	コマンドで複数のオプションが受け入れられる場合、またはオプションで互いに排反する引数が受け入れられる場合、これらの値は角括弧で囲んで入力します。
|	角括弧または山括弧の中では、入力項目が相互に排反するパラータであることを表すにはこの縦線文字を使用して区切ります。括弧内に指定したパラメータのうちのどれかを使用しなければなりません。

複数のオプションをサポートするコマンドの例：

```
user [-an <admin name>] [-ap <admin password>]
```

本例のように、「user」コマンドは、管理者のユーザー名を定義する「**-an**」のオプションと管理者のパスワードを定義する「**-ap**」のオプションを受けつけます。ここで管理者のユーザー名とパスワードを「XYZ」に変更したい場合は、

1. 「user」と入力し、続いてオプション、引数「**XYZ**」の順に入力します。
   user -ap XYZ
2. 最初のコマンドが正しく実行されたら、「user」と入力し、続いて 2 番目のオプション、引数「**XYZ**」の順に入力します。
   user -an XYZ

相互に排反する引数がオプションで受け入れられるコマンドの例：

```
alarmcount -p [all | warning | critical]
```

本例のように、「-p」のオプションには、「all」、「warning」、または「critical」の 3 つの引数のみ受け入れられています。例えば、発生中の重大なアラームを表示したい場合、次のように入力します。

alarmcount -p critical

括弧内に指定されている引数以外の引数を入力すると、コマンドは正しく実行されません。

コマンド応答コード

コマンド応答コードを使用すると、エラーメッセージとの照合を行う必要なしにスクリプト動作内のエラーを確実に検出することができます。

コマンドラインインターフェイスにはすべてのコマンド動作が次の形式で表示されます。

E [0-9][0-9][0-9]: エラーメッセージ

コード	メッセージ	コード	メッセージ
E000	Success（成功）	E105	Command Prefill（コマンドプレフィル）
E001	Successfully Issued（正常に発行）	E106	Data Not Available（データ使用不可）
E002	Reboot required for change to take effect（変更を有効にするには再起動が必要）	E107	Serial communication with the Rack PDU has been lost（Rack PDU とのシリアル通信消失）
E100	Command failed（コマンドエラー）		
E101	Command not found（コマンドなし）		
E102	Parameter error（パラメータエラー）		
E103	Command line error（コマンドラインエラー）		
E104	User level denial（ユーザー権限なし）		

Network Management Card のコマンドの説明

?

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： 操作者のアカウントタイプで使用できる CLI コマンドの一覧を表示します。特定のコマンドのヘルプ情報を表示するには、該当のコマンド、疑問符の順に入力します。

例：「**alarmcount**」コマンドに使用するオプションの一覧を表示するには、次のように入力します。

```
alarmcount ?
```

about

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： ハードウェアとソフトウェアの情報を表示できます。これはトラブルシューティングの際に役立つ情報であり、この情報を元にファームウェアのアップグレードが必要か判断します。

alarmcount

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明：

オプション	引数	説明
-p	all	Rack PDU に表示されている発生中のアラームの数を参照できます。各アラームの情報はイベントログに記録されています。
	warning	発生中の警告アラームの数を参照できます。
	critical	発生中の重大なアラームの数を参照できます。

例： 発生中の警告アラームをすべて表示する場合、次のように入力します。

```
alarmcount -p warning
```

boot

アクセス： 管理者のみ

説明： Rack PDU で IP アドレス、サブネットマスク、デフォルトゲートウェイなどのネットワーク設定をどのように取得するかを定義します。その後、BOOTP または DHCP サーバーの設定を行います。

オプション	引数	説明
-b <ブートモード>	dhcp | bootp | manual	Rack PDU の電源投入、リセット、再起動の各時点での TCP/IP 設定を定義します。それぞれのブートモードについては TCP/IP 設定と通信設定を参照してください。
-c	enable | disable	dhcp と dhcpBootp のブートモードのみ。DHCP サーバーからベンダー Cookie を取得する要件を有効または無効にします。
通常、次の 3 つの設定値は変更の必要はありません。 -v <vendor class>: DELL -i <client id>: ネットワーク上で一意のものとして認識可能な、Rack PDU の MAC アドレス -u <user class>: アプリケーションファームウェアモジュールの名前です。		

例： DHCP サーバーを使用してネットワーク設定を取得するには、次の手順で行います。

1. 「**boot -b dhcp**」と入力します。
2. DHCP サーバーからベンダー Cookie を取得する要件を有効にするには、次のように入力します。

   boot -c enable

cd

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： Rack PDU のディレクトリ構造内のフォルダに移動できます。

例 1: **ssh**フォルダに移動してSSHセキュリティ証明書がRack PDUにアップロードされているかを確認するには、次の手順で行います。

1.「**cd ssh**」と入力して、ENTER キーを押します。
2.「**dir**」と入力してから ENTER キーを押すと、SSH フォルダ内のファイルが一覧表示されます。

例 2: メインディレクトリフォルダに戻るには次を入力します。

```
cd ..
```

console

アクセス： 管理者のみ

説明： ユーザーがコマンドラインインターフェイスにアクセスする際に、デフォルト設定で有効になっている Telnet を使用するか、あるいはユーザー名、パスワード、データを暗号化して保護する Secure Shell（SSH）を使用するかを指定します。セキュリティを強化するために Telnet または SSH のポート設定を変更することもできます。あるいは、コマンドラインインターフェイスへのネットワークアクセスを無効にすることも可能です。

オプション	引数	説明
-S	disable | telnet | ssh	コマンドラインインターフェイスへのアクセスを設定するか、または「disable」コマンドを使用してアクセスを防止します。SSH を有効にすると、SCP が有効に、そして Telnet が無効になります。
-pt	<telnet ポート番号>	Rack PDU との通信に使用する Telnet ポートを定義します（デフォルトでは 23 番ポート）。
-ps	<SSH ポート番号>	Rack PDU との通信に使用する SSH ポートを定義します（デフォルトでは 22 番ポート）。
-b	2400 | 9600 | 19200 | 38400	シリアルポート接続の速度を設定します（デフォルトでは 9600 bps）。

例 1: コマンドラインインターフェイスへの SSH アクセスを有効にするには、次のように入力します。

```
console -S ssh
```

例 2: Telnet ポートを 5000 番に変更するには、次のように入力します。

```
console -pt 5000
```

date

アクセス： 管理者のみ

定義： Rack PDU で使用する日付を設定します。

Rack PDU での日付と時刻を定義する NTP サーバーを設定するには、日付と時刻の設定を参照してください。

オプション	引数	説明
-d	<“日付文字列”>	現在の日付を設定します。「date -f」コマンドで指定されている日付形式から選びます。
-t	<00:00:00>	現在の時刻を、時：分：秒で設定します。24 時間形式を使用します。
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Web インターフェイスで表示されるすべての日付の形式を指定します。個々の「m」（月）、「d」（日）、「y」（年）はそれぞれ一桁に相当します。日付または月名が一桁の場合、前にゼロをつけて表示されます。
-z	<時間帯オフセット>	グリニッジ標準時 GMT との差を設定して、お住まいの地域の時間帯を指定します。これにより、異なる時間帯の地域の他のユーザーとの同期を行うことができます。

例 1: 「yyyy-mm-dd」形式で日付を表示するには、次のように入力します。

```
date -f yyyy-mm-dd
```

例 2: 上述の形式を用いて 30.10.2009 の日付を指定するには次のように入力します。

```
date -d "2009-10-30"
```

例 3: 5:21:03 p.m. の時刻を指定するには次のように入力します。

```
date -t 17:21:03
```

delete

アクセス： 管理者のみ

説明： ファイルシステム内のファイルを削除します。

引数	説明
<ファイル名>	削除するファイルの名前を入力します。

dir

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： Rack PDU に保存されているファイルやフォルダを表示できます。

dns

アクセス： 管理者のみ

定義： Domain Name System（DNS）設定を手動で実行します。

パラメータ	引数	説明
-OM	enable | disable	手動設定した DNS を上書きします。
-p	<プライマリ DNS サーバー>	プライマリ DNS サーバーを設定します。
-s	<セカンダリ DNS サーバー>	セカンダリ DNS サーバーを設定します。
-d	<ドメイン名>	ドメイン名を設定します。
-n	<IPv6 のドメイン名>	IPv6 のドメイン名を設定します。
-h	<ホスト名>	ホスト名を設定します。

eventlog

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： イベントログを呼び出した日付と時刻、Rack PDU のステータス、Rack PDU に接続されているセンサのステータスを参照できます。直近のデバイスイベントおよびそれらが発生した日付と時刻も参照できます。イベントログ内のナビゲートは以下のキー操作で行います。

キー	説明
ESC	イベントログを閉じてコマンドラインインターフェイスに戻ります。
ENTER	ログ表示を更新します。このコマンドで、最後にイベントログを呼び出した時点以降に入力されたイベントを表示します。
スペースバー	イベントログの次のページに進みます。
B	イベントログの前のページに戻ります。このコマンドはイベントログのメインページでは利用できません。
D	イベントログを削除します。表示されるプロンプトに従って削除を確定またはキャンセルしてください。削除したイベントは復元できません。

exit

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： コマンドラインインターフェイスセッションを終了します。

format

アクセス： 管理者のみ

説明： Rack PDU のファイルシステムを再フォーマットして、セキュリティ証明書、暗号化キー、環境設定、イベントログとデータログをすべて消去します。

Rack PDU をリセットしてデフォルトの環境設定に戻すには、**resetToDef** コマンドを使用します。

FTP

アクセス： 管理者のみ

説明： FTP サーバーへのアクセスを有効または無効にします。またセキュリティを強化するために、ポート番号を 5001 ～ 32768 の間の使用していない番号に設定することができます。

オプション	引数	説明
-p	<ポート番号>	FTP サーバーが Rack PDU と通信するために使用する TCP/IP ポートを定義します（デフォルトでは 21 番ポート）。FTP サーバーは、ここで指定するポートと、それより 1 つ下の番号のポートの両方を使用します。
-S	enable | disable	FTP サーバーへのアクセスを設定します。

例： TCP/IP ポートを 5001 番ポートに変更するには、次のように入力します。

```
ftp -p 5001
```

help

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： 操作者のアカウントタイプで使用できる CLI コマンドの一覧を表示します。特定のコマンドのヘルプ情報を表示するには、該当のコマンド、「**help**」の順に入力します。

例 1: デバイスユーザーに許可されているコマンドの一覧を表示するには次のように入力します。

```
help
```

例 2:「**alarmcount**」コマンドに使用するオプションの一覧を表示するには、次のように入力します。

```
alarmcount help
```

netstat

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： ネットワークとアクティブな IPv4/IPv6 全アドレスのステータスを表示します。

ntp

アクセス： 管理者

定義： ネットワークタイムプロトコルパラメータを表示および設定します。

オプション	引数	説明
-OM	enable | disable	手動設定を上書きします。
-p	<プライマリ NTP サーバー>	プライマリサーバーを指定します。
-s	<セカンダリ NTP サーバー>	セカンダリサーバーを指定します。

例 1: 手動設定の上書きを有効にするには、次のように入力します。

```
ntp -OM enable
```

例 2: プライマリ NTP サーバーを指定するには、次のように入力します。

```
ntp -p 150.250.6.10
```

ping

アクセス： 管理者、デバイスユーザー

説明 IP アドレスまたは DNS 名で指定してあるデバイスからネットワークへの接続が確立されているかどうかを判断できます。アドレスに対して 4 回のクエリが行われます。

引数	説明
<IP アドレスまたは DNS 名>	IP アドレス（*xxx.xxx.xxx.xxx* の形式で）または DNS サーバー内で定義されている DNS 名を入力します。

例： IP アドレスが「150.250.6.10」のデバイスがネットワークに接続されているかを確認するには、次のように入力します。

```
ping 150.250.6.10
```

portSpeed

アクセス： 管理者

説明：

オプション	引数	説明
-s	auto | 10H | 10F | 100H | 100F	イーサネットポートの通信速度を定義します。「auto」コマンドでは、イーサネットデバイスができるけ速い速度を使用できるようネゴシエートすることを可能にします。ポート速度設定の詳細についてはポート速度を参照してください。

例： TCP/IP ポートでの通信を、100 Mbp での半二重通信方式（一度に一方向のみの通信）に設定するには、次のように入力します。

```
portspeed -s 100H
```

prompt

アクセス： 管理者、デバイスユーザー

説明： コマンドラインインターフェイスのプロンプトに、現在ログオンされているユーザーのアカウントの種類を含めるか除外するかを指定します。この設定の変更は、全ユーザーに許可されています。設定が変更された場合、変更内容はすべてのユーザーアカウントに反映されます。

オプション	引数	説明
-s	long	プロンプトには現在ログオンされているユーザーのアカウントの種類が含まれます。
	short	デフォルトではこの設定になっています。プロンプトは、cli>

例： 現在ログオンされているユーザーのアカウントの種類をコマンドラインインターフェイスのプロンプトに含めるには、次のように入力します。

```
prompt -s long
```

quit

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： コマンドラインインターフェイスセッションを終了します（「exit」コマンドと同様の働きをします）。

radius

アクセス： 管理者のみ

説明： このコマンドでは、既存の RADIUS 設定を表示する、RADIUS 認証を有効 / 無効に設定する、さらに 2 台までの RADIUS サーバーの基本的な認証パラメータを設定するタスクを実行できます。

RADIUS サーバーの環境設定方法の概要と、サポートされている RADIUS サーバーの一覧については、RADIUS サーバーの環境設定を参照してください。

RADIUS サーバーのこの他の認証パラメータには、Rack PDU の Web インターフェイスからアクセスできます。詳細については、RADIUS を参照してください。

RADIUS サーバーの設定については、付録 B: セキュリティハンドブックを参照してください。

オプション	引数	説明
-a	local | radiusLocal | radius	RADIUS 認証を設定します。 **local** — RADIUS は無効になり、ローカル認証が有効になります。 **radiusLocal** — RADIUS、次にローカル認証の順になります。RADIUS とローカル認証が有効になります。RADIUS サーバーからの認証が最初に要求されます。RADIUS サーバーからの応答がない場合、ローカル認証が使用されます。 **radius** — RADIUS が有効になり、ローカル認証が無効になります。

オプション	引数	説明
-p1 -p2	<サーバー IP>	プライマリまたはセカンダリ RADIUS サーバーのサーバー名または IP アドレスです。 **注意**： RADIUS サーバーは、デフォルトでは 1812 番ポートを使用してユーザー認証を行います。別のポートを使用するには、RADIUS サーバー名または IP アドレスの最後にコロンを追加し、その後に新しいポート番号を入力します。
-s1 -s2	<サーバーシークレット>	プライマリまたはセカンダリ RADIUS サーバーと Rack PDU 間の共有のシークレットです。
-t1 -t2	<サーバータイムアウト>	Rack PDU でプライマリまたはセカンダリ RADIUS サーバーからの応答を待つときの待機時間（単位は秒）です。

例 1:

Rack PDU の既存の RADIUS 設定を表示するには、「**radius**」と入力し、ENTER キーを押します。

例 2: RADIUS 認証とローカル認証を有効にするには、次のように入力します。

```
radius -a radiusLocal
```

例 3: セカンダリ RADIUS サーバーでタイムアウトになるまでの応答待ち時間を 10 秒に設定するには、次のように入力します。

```
radius -t2 10
```

reboot

アクセス： 管理者のみ

説明： Rack PDU のインターフェイスを再起動できます。

resetToDef

アクセス： 管理者のみ

説明：

オプション	引数	説明
-p	all | keepip	イベントアクション、デバイス設定を含む環境設定への全変更をリセットできます。また、TCP/IP の環境設定をリセットすることもできます。

例： TCP/IP 設定を除き、Rack PDU の環境設定への全変更をリセットするには、次のように入力します。

```
resetToDef -p keepip
```

snmp, snmpv3

アクセス： 管理者のみ

説明： SNMP 1 または SNMP 3 を有効または無効にします。

オプション	引数	説明
-S	enable | disable	SNMP の各バージョン（1 または 3）を有効にするか、表示します。

例： SNMP のバージョン 1 を有効にするには、次のように入力します。

```
snmp -S enable
```

system

アクセス： 管理者のみ

説明： システム名、連絡先、システムの設置場所、動作可能時間、日時、ログオン中のユーザー、詳細なシステムステータス P、N、A（システムステータスの詳細はメイン画面についてを参照）を表示、設定します。

オプション	引数	説明
-n	〈システム名〉	デバイス名、デバイスの責任者名、さらにデバイスの物理的な設置場所を定義します。 **注意**：（一語ではなく）複数の語を用いて値を定義する場合は、該当の値を引用符で囲んでください。
-c	〈システム担当者の連絡先〉	
-l	〈システムの設置場所〉	

例 1: デバイスの設置場所を「**Test Lab**」と設定するには、次のように入力します。

```
system -l "Test Lab"
```

例 2: システム名を「**Don Adams**」と設定するには、次のように入力します。

```
system -n "Don Adams"
```

tcpip

アクセス： 管理者のみ

説明： Rack PDU での以下のネットワーク値を表示し、手動で設定します。

オプション	引数	説明
-i	〈IP アドレス〉	Rack PDU の IP アドレスを「*xxx.xxx.xxx.xxx*」の形式で入力します。
-s	〈サブネットマスク〉	Rack PDU のサブネットマスクを入力します。
-g	〈ゲートウェイ〉	デフォルトゲートウェイの IP アドレスを入力します。ループバックアドレス（127.0.0.1）をデフォルトゲートウェイアドレスとして**使用しないでください**。
-d	〈ドメイン名〉	DNS サーバー内で設定されている DNS 名を入力します。
-h	〈ホスト名〉	Rack PDU で使用するホスト名を入力します。

例 1: Rack PDU のネットワーク設定を表示するには、「**tcpip**」と入力し、ENTER キーを押します。

例 2: Rack PDU の IP アドレスを「**150.250.6.10**」に手動で設定するには、次のように入力します。

```
tcpip -i 150.250.6.10
```

tcpip6

アクセス： 管理者のみ

説明： IPv6 を有効にし、Rack PDU での以下のネットワーク値を表示し、手動で設定します。

オプション	引数	説明
-S	enable | disable	IPv6 を有効または無効にします。
-man	enable | disable	Rack PDU の IPv6 アドレスを手動で入力できるようにします。
-auto	enable | disable	Rack PDU の IPv6 アドレスの自動設定を有効にします。
-i	<IPv6 アドレス>	Rack PDU の IPv6 アドレスを設定します。
-g	<IPv6 ゲートウェイ>	デフォルトゲートウェイの IPv6 アドレスを設定します。
-d6	router | statefull | stateless | never	DHCPv6 のモードを、「router」（ルータ制御）、「statefull」（アドレスとその他の情報のステータスを保持）、「stateless」（アドレス以外の情報のステータスは保持しない）、「never」（すべて保持しない）のパラメータを使用して設定します。

例 1: Rack PDU のネットワーク設定を表示するには、「**tcpip6**」と入力し、ENTER キーを押します。

例 2: Rack PDU に IPv6 アドレス **2001:0:0:0:0:FFD3:0:57ab** を手動で設定するには、次のように入力します。

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

user

アクセス： 管理者のみ

説明： 管理者、デバイスユーザー、読み取り専用ユーザーの各アカウントタイプに対して、ユーザー名、パスワード、そして何もアクティビティがない場合に適用するアイドルタイムアウト粋を設定します。

各アカウントタイプに許可される権限については、ユーザーアカウントの種類を参照してください。

オプション	引数	説明
-an -dn -rn	〈管理者ユーザー名〉 〈デバイスユーザー名〉 〈読み取り専用ユーザー名〉	各アカウントの種類のユーザー名を、大文字と小文字を区別して設定します。パスワードに使用できるのは 10 文字までです。
-ap -dp -rp	〈管理者ユーザーのパスワード〉 〈デバイスユーザーのパスワード〉 〈読み取り専用ユーザーのパスワード〉	各アカウントタイプのパスワードを、大文字と小文字を区別して設定します。パスワードに使用できるのは 32 文字までです。パスワード欄を空欄にする（文字を設定しない）ことはできません。
-t	〈分〉	アクティビティがない場合にそのユーザーをログオフするまでの待機時間（デフォルトでは 3 分です）を設定します。

例 1: 管理者ユーザーのユーザー名を「XYZ」に変更したい場合は、次のように入力します。

```
user -an XYZ
```

例 2: ログオフまでの待機時間を 10 分に変更するには、次のように入力します。

```
user -t 10
```

web

アクセス： 管理者のみ

説明： HTTP または HTTPS による Web インターフェイスへのアクセスを有効にします。

HTTP と HTTPS のポートを 5000 ～ 32768 の間の使用していない番号に設定すると、セキュリティを強化することができます。この場合、ブラウザのアドレス欄にコロン（:）を入力してからポート番号を指定する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合、以下のように入力します。

http://152.214.12.114:5000

オプション	引数	説明
-S	disable | http | https	Web インターフェイスへのアクセス方法を設定します。HTTPS が有効になっていると、送信データは暗号化され、デジタル証明書により認証されます。
-ph	<HTTP ポート番号>	HTTP が Rack PDU と通信するために使用する TCP/IP ポートを定義します（デフォルトでは 80 番ポート）。
-ps	<HTTPS ポート番号>	HTTPS が Rack PDU と通信するために使用する TCP/IP ポートを定義します（デフォルトでは 443 番ポート）。

例： Web インターフェイスへの全アクセスを抑制するには、次のように入力します。

web -S disable

xferINI

アクセス： 管理者のみ

説明： シリアル接続を通してコマンドラインインターフェイスにアクセスしている際に、XMODEM を使用して INI ファイルをアップロードします。アップロードが完了すると、

- システムまたはネットワークに変更があった場合、コマンドラインインターフェイスは再起動するため、ログオンし直す必要があります。
- Rack PDU のデフォルトのボーレート以外のボーレートをファイル転送に指定してあった場合、Rack PDU との通信を再確立するにはボーレートをデフォルト値に設定し直さなければなりません。

xferStatus

アクセス： 管理者のみ

説明： 前回のファイル転送の結果を表示できます。

転送結果のコードについてはアップグレードや更新の確認を参照してください。

デバイスコマンドの説明

devLowLoad

アクセス： 管理者、デバイスユーザー

説明： 機器の低負荷しきい値をキロワットで設定、または表示します。

例 1: 低負荷しきい値を表示するには、次のように入力します。

```
cli> devLowLoad
E000: Success
0.5 kW
```

例 2: 低負荷しきい値を 1 kW に設定するには、次のように入力します。

```
cli> devLowLoad 1.0
E000: Success
```

devNearOver

アクセス： 管理者、デバイスユーザー

説明： 機器の過負荷寸前しきい値をキロワットで設定、または表示します。

例 1: 過負荷寸前しきい値を表示するには、次のように入力します。

```
cli> devNearOver
E000: Success
20.5 kW
```

例 2: 過負荷寸前しきい値を 21.3 kW に設定するには、次のように入力します。

```
cli> devNearOver 21.3
E000: Success
```

devOverLoad

アクセス： 管理者、デバイスユーザー

説明： 機器の過負荷しきい値をキロワットで設定、または表示します。

例 1: 過負荷しきい値を表示するには、次のように入力します。

```
cli> devOverLoad
E000: Success
25.0 kW
```

例 2: 過負荷しきい値を 25.5 kW に設定するには、次のように入力します。

```
cli> devOverLoad 25.5
E000: Success
```

devReading

アクセス： 管理者、デバイスユーザー

説明： 機器の総電力をキロワットで、総エネルギーをキロワット時で表示します。

引数	説明
電源	総電力をキロワットで表示します。
energy	総エネルギーをキロワット時で表示します。

例 1: 総電力を表示するには、次のように入力します。

```
cli> devReading power
E000: Success
5.2 kW
```

例 2: 総エネルギーを表示するには、次のように入力します。

```
cli> devReading energy
E000: Success
200.1 kWh
```

devStartDly

アクセス： 管理者、デバイスユーザー

説明： Rack PDU に電源投入後の各コンセントの [Power on Delay]（電源投入までの待機時間）に追加される時間（秒単位）を設定または表示します。有効な値は、1 ～ 300 秒または [never]（電源オンされない）です。

例 1: コールドスタート遅延を表示するには、次のように入力します。

```
cli> devStartDly
E000: Success
5 seconds
```

例 2: コールドスタート遅延を 6 秒に設定するには、次のように入力します。

```
cli> devStartDly 6
E000: Success
```

humLow

アクセス： 管理者、デバイスユーザー

説明： 低湿度しきい値を、相対湿度のパーセンテージで設定または表示します。

例 1: 低湿度しきい値を表示するには、次のように入力します。

```
cli> humLow
E000: Success
10 %RH
```

例 2: 低湿度しきい値を設定するには、次のように入力します。

```
cli> humLow 12
E000: Success
```

humMin

アクセス： 管理者、デバイスユーザー

説明： 最低湿度しきい値を、相対湿度のパーセンテージで設定または表示します。

例 1: 最低湿度しきい値を表示するには、次のように入力します。

```
cli> humMin
E000: Success
6 %RH
```

例 2: 最低湿度しきい値を設定するには、次のように入力します。

```
cli> humMin 8
E000: Success
```

humReading

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： センサの湿度の値を表示します。

例： 湿度の値を表示するには、次のように入力します。

```
cli> humReading
E000: Success
25 %RH
```

inNormal

アクセス： 管理者、デバイスユーザー

説明： 各ドライ接点入力の通常状態を表示します。

例： 各ドライ接点入力の通常状態を表示するには、次のように入力します。

```
cli> inNormal
E000: Success
1: Open
2: Open
```

inReading

アクセス： 管理者、デバイスユーザー

説明： 各ドライ接点入力の現在の状態を表示します。

例： 各ドライ接点入力の現在の状態を表示するには、次のように入力します。

```
cli> inReading
E000: Success
1: Open
2: Open
```

olAssignUsr

アクセス： 管理者

説明： ローカルデータベースに存在するコンセントユーザーにコンセントの管理を割り当てます。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに指定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
<ユーザー>	ローカルデータベースに存在するユーザー （userAdd を参照）

例 1: ユーザー名 Bobby をコンセント 3、5 ～ 7、10 に割り当てるには、次のように入力します。

```
cli> olAssignUsr 3,5-7,10 bobby
E000: Success
```

例 2: ユーザー名 Billy をすべてのコンセントに割り当てるには、次のように入力します。

```
cli> olAssignUsr all billy
E000: Success
```

olCancelCmd

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 1 つのコンセントまたはコンセントグループに対して保留中のすべてのコマンドを取り消します。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント名〉	特定のコンセントに設定された名前 （olName を参照）
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例： コンセント 3 に対するすべてのコマンドを取り消すには、次のように入力します。

```
cli> olCancelCmd 3
E000: Success
```

olDlyOff

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： [Power Off Delay]（電源停止までの待機時間）の経過後、1 つのコンセントまたはコンセントグループの電源をオフにします（olOff を参照）。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント 3、5 ～ 7、10 の電源をオフにするには、次のように入力します。

```
cli> olDlyOff 3,5-7,10
E000: Success
```

例 2: すべてのコンセントの電源をオフにするには、次のように入力します。

```
cli> olDlyOff all
E000: Success
```

olDlyOn

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： [Power On Delay]（電源投入までの待機時間）の経過後、1 つのコンセントまたはコンセントグループの電源をオンにします（olOnDelay を参照）。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント 3、5 ～ 7、10 の電源をオンにするには、次のように入力します。

```
cli> olDlyOn 3,5-7,10
E000: Success
```

例 2: Outlet1 という名前が設定されたコンセントの電源をオンにするには、次のように入力します。

```
cli> olDlyOn outlet1
E000: Success
```

olDlyReboot

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 1 つのコンセントまたはコンセントグループの電源を入れ直します。指定したコンセントは、[Power Off Delay] の設定に基づいてオフになります（olOffDelay を参照）。選択したコンセントの最長の [Reboot Duration]（再起動待機時間）（olRbootTime を参照）の経過後に、指定したコンセントに設定された [Power On Delays]（olOnDelay を参照）に基づいてコンセントの電源オンを開始します。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント 3、5 ～ 7、10 の電源を入れ直すには、次のように入力します。

```
cli> olDlyReboot 3,5-7,10
E000: Success
```

例 2: Outlet1 という名前が設定されたコンセントの電源を入れ直すには、次のように入力します。

```
cli> olDlyReboot outlet1
E000: Success
```

olGroups

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： Rack PDU に定義されている同期したコンセントグループのリストです。（詳細については、コンセントグループの設定と制御 を参照してください。）

例： 同期したコンセントグループを一覧表示するには、次のように入力します。

```
cli> olGroups
E000: Success
Outlet Group A:
159.215.6.141 -> Outlets: 2,4,5
159.215.6.143 -> Outlets: 2,8
Outlet Group B:
159.215.6.141 -> Outlets: 1
159.215.6.166 -> Outlets: 1
```

olLowLoad

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： コンセントの低負荷警告のしきい値を設定または表示します。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
<電力>	コンセントの新規しきい値（ワット）

例 1: すべてのコンセントに対して低負荷のしきい値を 2 ワットに設定するには、次のように入力します。

```
cli> olLowLoad all 2
E000: Success
```

例 2: コンセント 3 と 5 ～ 7 の低負荷しきい値を表示するには、次のように入力します。

```
cli> olLowLoad 3,5-7
E000: Success
3: BobbysServer: 2 W
5: BillysServer: 2 W
6: JoesServer: 2 W
7: JacksServer: 2 W
```

olName

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： コンセントに指定する名前を設定または表示します。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
〈新規名前〉	特定のコンセントに設定する名前。文字と数字のみ使用できます。

例： コンセント 3 に BobbysServer という名前を設定するには、次のように入力します。

```
cli> olName 3 BobbysServer
E000: Success
3: BobbysServer
5: BillysServer
6: JoesServer
7: JacksServer
```

olNearOver

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： コンセントの過負荷直前警告のしきい値を設定または表示します。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
<電力>	コンセントの新規しきい値（ワット）

例 1: コンセント 3 と 5 ～ 7 の過負荷直前のしきい値を表示するには、次のように入力します。

```
cli> olNearOver 3,5-7
E000: Success
3: BobbysServer: 5 W
5: BillysServer: 6 W
6: JoesServer: 5 W
7: JacksServer: 4 W
```

例 2: コンセント 3 と 5 ～ 7 の過負荷直前のしきい値を設定するには、次のように入力します。

six watts, type:

```
cli> olNearOver 3,5-7 6
E000: Success
3: BobbysServer: 6 W
5: BillysServer: 6 W
6: JoesServer: 6 W
7: JacksServer: 6 W
```

olOff

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 1 つのコンセントまたはコンセントグループの電源を遅延せずにオフにします。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント名〉	特定のコンセントに設定された名前 （olName を参照）
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント 3 と 5 ～ 7 の電源をオフにするには、次のように入力します。

```
cli> olOff 3,5-7
E000: Success
```

olOffDelay

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明：「Off Delayed」コマンド（olDlyOff を参照）および「Reboot Delayed」コマンド（olDlyReboot を参照）の時間遅延を設定または表示します。

引数	説明
all	デバイスのすべてのコンセント
＜コンセント名＞	特定のコンセントに設定された名前 （olName を参照）
＜コンセント番号＞	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
＜時間＞	1 ～ 7200 秒 （2 時間）の範囲内の遅延時間

例 1: コンセント 3 と 5 ～ 7 の電源オフに 9 秒の遅延を設定するには、次のように入力します。

```
cli> olOffDelay 3,5-7 9
E000: Success
```

例 2: コンセント 3 と 5 ～ 7 に対する「Off Delayed」コマンドの遅延を表示するには、次のように入力します。

```
cli> olOffDelay 3,5-7
E000: Success
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

olOn

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 1 つのコンセントまたはコンセントグループの電源を遅延せずにオフにします。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント名〉	特定のコンセントに設定された名前 （olName を参照）
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント 3 と 5 ～ 7 の電源をオンにするには、次のように入力します。

```
cli> olOn 3,5-7
E000: Success
```

olOnDelay

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明：「On Delayed」コマンド（olDlyOn を参照）および「Reboot Delayed」コマンド（olDlyReboot を参照）の時間遅延を設定または表示します。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
<時間>	1 ～ 7200 秒 （2 時間）の範囲内の遅延時間

例 1: コンセント 3 と 5 ～ 7 の電源オンに 6 秒の遅延を設定するには、次のように入力します。

```
cli> olOnDelay 3,5-7 6
E000: Success
```

例 2: コンセント 3 と 5 ～ 7 に対する「On Delayed」コマンドの遅延を表示するには、次のように入力します。

```
cli> olOnDelay 3,5-7
E000: Success
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

olOverLoad

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： コンセントの過負荷警告のしきい値を設定または表示します。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント名〉	特定のコンセントに設定された名前 （olName を参照）
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
〈電力〉	コンセントの新規しきい値（ワット）

例 1: コンセント 3 と 5 ～ 7 の過負荷しきい値を表示するには、次のように入力します。

```
cli> olOverLoad 3,5-7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 8 W
6: JoesServer: 7 W
7: JacksServer: 6 W
```

例 2: コンセント 3 と 5 ～ 7 の過負荷しきい値を 7 ワットに設定するには、次のように入力します。

```
cli> olOverLoad 3,5-7 7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 7 W
6: JoesServer: 7 W
7: JacksServer: 7 W
```

olRbootTime

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明：「Reboot Delayed」コマンド（olDlyReboot を参照）でコンセントをオフのままにしておく時間を設定または表示します。

例 1: コンセント 3 と 5 ～ 7 に対して設定された再起動中にオフのままにする時間を表示するには、次のように入力します。

```
cli> olRbootTime 3,5-7
E000: Success
3: BobbysServer: 4 sec
5: BillysServer: 5 sec
6: JoesServer: 7 sec
7: JacksServer: 2 sec
```

例 2: コンセント 3 と 5 ～ 7 に対して再起動中にオフのままにする時間を設定するには、次のように入力します。

```
cli> olRebootTime 3,5-7 10
E000: Success
3: BobbysServer: 10 sec
5: BillysServer: 10 sec
6: JoesServer: 10 sec
7: JacksServer: 10 sec
```

olReading

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 1 つのコンセントまたはコンセントグループの電流、電力、またはエネルギーを表示します。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント名〉	特定のコンセントに設定された名前 （olName を参照）
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
current | power | energy	コンセントの新規しきい値（ワット）

例 1: コンセント 3 と 5 ～ 7 の電流を表示するには、次のように入力します。

```
cli> olReading 3,5-7 current
E000: Success
3: BobbysServer: 4 A
5: BillysServer: 5 A
6: JoesServer: 7 A
7: JacksServer: 2 A
```

例 2: コンセント 3 の電力を表示するには、次のように入力します。

```
cli> olReading 3 power
E000: Success
3: BobbysServer: 40 W
```

例 3: コンセント JoesServer のエネルギーを表示するには、次のように入力します。

```
cli> olReading joesserver energy
E000: Success
6: JoesServer: 7.3 kWh
```

olReboot

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 1 つのコンセントまたはコンセントグループの電源を遅延せずに入れ直します。複数のコンセントを指定すると、すべてのコンセントの電源を同時に入れ直します。

引数	説明
all	デバイスのすべてのコンセント
〈コンセント名〉	特定のコンセントに設定された名前 （olName を参照）
〈コンセント番号〉	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例： コンセント 3 と 5 ～ 7 を再起動するには、次のように入力します。

```
cli> olReboot 3,5-7
E000: Success
```

olStatus

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： 指定したコンセントの状態を表示します。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例： コンセント 3 と 5 ～ 7 の状態を表示するには、次のように入力します。

```
cli> olStatus 3,5-7
E000: Success
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

olUnasgnUsr

アクセス： 管理者

説明： ローカルデータベースに存在するコンセントユーザーからコンセントの管理割り当てを削除します。

引数	説明
all	デバイスのすべてのコンセント
<コンセント名>	特定のコンセントに設定された名前 （olName を参照）
<コンセント番号>	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
<ユーザー>	ローカルデータベースに存在するユーザー （userList を参照）

例 1: コンセント 3、5 ～ 7、10 の管理割り当てからユーザー名 Bobby を削除するには、次のように入力します。

```
cli> olUnasgnUsr 3,5-7,10 bobby
E000: Success
```

例 2: すべてのコンセントの管理割り当てからユーザー名 Billy を削除するには、次のように入力します。

```
cli> olUnasgnUsr all billy
E000: Success
```

phLowLoad

アクセス： 管理者、デバイスユーザー

説明： 相の低負荷しきい値をキロワットで設定または表示します。相を指定するには、次のオプションから選択します。次のように入力します。**all**、単一の相、相の範囲、または相のカンマ区切りのリスト

例 1: すべての相の低負荷しきい値を 1 kW に設定するには、次のように設定します。

```
cli> phLowLoad all 1
E000: Success
```

例 2: 相 1 から 3 までの低負荷しきい値を表示するには、次のように入力します。

```
cli> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

phNearOver

アクセス： 管理者、デバイスユーザー

説明： 相の過負荷寸前しきい値をキロワットで設定または表示します。相を指定するには、次のオプションから選択します。次のように入力します。**all**、単一の相、相の範囲、または相のカンマ区切りのリスト

例 1: すべての相の過負荷寸前しきい値を 10 kW に設定するには、次のように設定します。

```
cli> phNearOver all 10
E000: Success
```

例 2: 相 1 から 3 までの過負荷寸前しきい値を表示するには、次のように入力します。

```
cli> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

phOverLoad

アクセス： 管理者、デバイスユーザー

説明： 相の過負荷しきい値をキロワットで設定または表示します。相を指定するには、次のオプションから選択します。次のように入力します。**all**、単一の相、相の範囲、または相のカンマ区切りのリスト

例 1: すべての相の過負荷しきい値を 13 kW に設定するには、次のように設定します。

```
cli> phOverLoad all 13
E000: Success
```

例 2: 相 1 から 3 までの過負荷しきい値を表示するには、次のように入力します。

```
cli> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

phReading

アクセス： 管理者、デバイスユーザー

説明： 相の電流、電圧、電力を表示します。相の過負荷寸前しきい値をキロワットで設定または表示します。相を指定するには、次のオプションから選択します。次のように入力します。**all**、単一の相、相の範囲、または相のカンマ区切りのリスト

例 1: 相 3 の電流の測定値を表示するには、次のように入力します。

```
cli> phReading 3 current
E000: Success
3:4 A
```

例 2: 各相の電圧を表示するには、次のように入力します。

```
cli> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

例 3: 相 2 の電力を表示するには、次のように入力します。

```
cli> phReading 2 power
E000: Success
2: 40 W
```

phRestrictn

アクセス： 管理者

説明： 過負荷警告のしきい値を超えたときにコンセントに電源投入されないようにする、過負荷制限機能を設定または表示します。設定可能な引数は、「**none**」、「**near**」、「**over**」です。相を指定するには、以下のオプションから選択します。次のように入力します。**all**、単一の相、相の範囲、または相のカンマ区切りのリスト

例 1: 相 3 の過負荷制限を「none」（なし）に設定するには、次のように入力します。

```
cli> phRestrictn 3 none
E000: Success
```

例 2: すべての相の過負荷制限を表示するには、次のように入力します。

```
cli> phRestrictn all
E000: Success
1: over
2: near
3: none
```

prodInfo

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： Rack PDU についての情報を表示します。

例：

```
cli> prodInfo
E000: Success
AOS vX.X.X.X
Managed Rack PDU vX.X.X.X
Model:              DELL6xxx
Present Outlets:    12
Switched Outlets:   12
Metered Outlets:    0
Max Current:        20 A
Phases:             1
```

sensorName

アクセス： 管理者、デバイスユーザー

説明： Rack PDU の温度 / 湿度センサーポートに割り当てる名前を設定または表示します。

例 1: ポートに「Sensor1」という名前を設定するには、次のように入力します。

```
cli> sensorName Sensor1
E000: Success
```

例 2: センサーポートの名前を表示するには、次のように入力します。

```
cli> sensorName
E000: Success
Sensor1
```

tempHigh

アクセス： 管理者、デバイスユーザー

説明： 高温しきい値を、華氏または摂氏のいずれかで設定または表示します。

例 1: 高温しきい値を華氏 70 F に設定するには、次のように入力します。

```
cli> tempHigh F 70
E000: Success
```

例 2: 高温しきい値を摂氏（℃）で表示するには、次のように入力します。

```
cli> tempHigh C
E000: Success
21 C
```

例 3: 高温しきい値を華氏（° F）で表示するには、次のように入力します。

```
cli> tempHigh F
E000: Success
70 F
```

tempMax

アクセス： 管理者、デバイスユーザー

説明： 最高温度しきい値を、華氏または摂氏のいずれかで設定または表示します。

例 1: 最高温度しきい値を華氏 80 F に設定するには、次のように入力します。

```
cli> tempMax F 80
E000: Success
```

例 2: 最高温度しきい値を摂氏（℃）で表示するには、次のように入力します。

```
cli> tempMax C
E000: Success
27 C
```

例 3: 最高温度しきい値を華氏（° F）で表示するには、次のように入力します。

```
cli> tempMax F
E000: Success
80 F
```

tempReading

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： センサの温度の値を華氏または摂氏のいずれかで表示します。

例： 温度の値を華氏（° F）で表示するには、次のように入力します。

```
cli> tempReading F
E000: Success
51.1 F
```

userAdd

アクセス： 管理者

説明： コンセントユーザーをローカルユーザーデータベースに追加します。

例： ユーザー名 Bobby を追加するには、次のように入力します。

```
cli> userAdd Bobby
E000: Success
```

userDelete

アクセス： 管理者

説明： コンセントユーザーをローカルユーザーデータベースから削除します。

例： ユーザー名 Bobby を削除するには、次のように入力します。

```
cli> userDelete Bobby
E000: Success
```

userList

アクセス： 管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明： ユーザーとそのユーザーに割り当てられたコンセントを一覧表示します。

例 1: 管理者としてログインしている場合には、次のように入力します。

```
cli> userList
E000: Success
Local: admin: 1,2,3,4,5,6,7,8
Local: Bobby: 1,3
Local: Billy: 2,5
Local: Joe: 4,6
Local: Jack: 7,8
```

例 2: Billy としてログインしている場合には、次のように入力します。

```
cli> userList
E000: Success
Local: Billy: 2,5
```

userPasswd

アクセス： 管理者

説明： コンセントユーザのパスワードを設定します。

例： Bobby のパスワードを「abc123」に設定するには、次のように入力します。

```
cli> userPasswd Bobby abc123 abc123
E000: Success
```

whoami

アクセス： 管理者、デバイスユーザー、コンセントユーザー

説明： アクティブユーザーのユーザー名を表示します。

例：

```
cli> whoami
E000: Success
admin
```

Web インターフェイス

サポートされる Web ブラウザ

Microsoft® Internet Explorer®（IE）7.x 以降（Windows® OS のみ）、Mozilla® Firefox® 3.0.6 以降（全 OS）を使用して、Web インターフェイスから Rack PDU にアクセスできます。その他のブラウザについては、検証を行っておりません。

Rack PDU はプロキシサーバーと連携することができません。Web ブラウザから Rack PDU の Web インターフェイスにアクセスする前に、次のいずれかの作業を行う必要があります。

- Rack PDU でプロキシサーバーを使用しないよう Web ブラウザを設定する。
- Rack PDU の特定の IP アドレスを対象外とするようプロキシサーバーを設定する。

Web インターフェイスへのログオン

概要

Web インターフェイスの URL アドレスとして、Rack PDU の DNS 名やシステム IP アドレスを利用できます。ログオンするには、ユーザー名とパスワードの入力が必要です。これらの値には大文字と小文字の区別があります。デフォルトのユーザー名とパスワードはアカウントの種類によって次のようになっています。

- 管理者の場合は「admin/admin」
- デバイスユーザーの場合は「device/device」
- 読み取り専用ユーザーの場合は「readonly/readonly」

コンセントユーザーのアカウントには、デフォルトのユーザー名やパスワードはありません。コンセントユーザーのユーザー名とパスワード、およびアカウントのその他の詳細は、管理者が指定する必要があります。コンセントユーザーの設定を参照してください。

アクセスプロトコルとして HTTPS（SSL/TLS）を使用している場合、ログオン情報はサーバー証明書にある情報と比較されます。証明書がセキュリティウィザードで作成されており、IP アドレスが証明書でコモン名として指定されている場合は、Rack-Mount PDU にログオンするのに、IP アドレスを使用する必要があります。証明書で DNS 名がコモン名として指定されている場合は、DNS 名を使用してログオンする必要があります。

Web インターフェイスのログオン時に表示される Web ページについては、[Home] タブについてを参照してください。

URL アドレスの形式

Rack PDU の DNS 名または IP アドレスを Web ブラウザの URL アドレスフィールドに入力し、ENTER を押します。Internet Explorer にデフォルト以外の Web サーバーポートを指定する場合、URL に「**http://**」または「**https://**」を含める必要があります。

ログオン時にブラウザに表示される一般的なエラーメッセージ .

エラーメッセージ	エラーの原因	ブラウザ
「このページを表示する権限がありません」または「現在、別のユーザーがログオン中です . . . 」	別のユーザーがログオンしている	Internet Explorer、Firefox
「ページを表示できません。」	Web アクセスが無効になっているか、または URL が正しくありません。	Internet Explorer
「接続できません。」		Firefox

URL 形式の例 .

- Web1 の DNS 名 :
  - **http://Web1**（アクセスモードが HTTP の場合）
  - **https://Web1**（アクセスモードが HTTPS の場合）
- システムの IP アドレスが 139.225.6.133 で、デフォルトの Web サーバーポート（ポート番号 80）の場合 :
  - **http://139.225.6.133**（アクセスモードが HTTP の場合）
  - **https://139.225.6.133**（アクセスモードが HTTPS（SSL での HTTP）の場合）
- システムの IP アドレスが 139.225.6.133 で、デフォルト以外の Web サーバーポート（ポート番号 5000）の場合 :
  - **http://139.225.6.133:5000**（アクセスモードが HTTP の場合）
  - **https://139.225.6.133:5000**（アクセスモードが HTTPS（SSL での HTTP）の場合）
- システムの IPv6 アドレスが 2001:db8:1::2c0:b7ff:fe00:1100 で、デフォルト以外の Web サーバーポート（ポート番号 5000）の場合 :
  - **http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000**（アクセスモードが HTTP の場合）

Web インターフェイスの機能

ご使用の Rack PDU の Web インターフェイスの基本的な機能について、下記の説明をよくお読みください。

タブ

下記のタブを使用できます。

- [Home]: ログオンすると表示されます。アクティブなアラーム、Rack PDU の負荷状態、および Rack PDU で最近発生したイベントを表示します。詳細については、[Home] タブについてを参照してください。
- [Device Manager]: 接続されたすべてのデバイス、相、およびコンセント（該当する場合）の負荷状態を表示し、負荷しきい値を設定し、そしてピーク負荷の測定を表示、管理します。コンセントの管理および制御を行います。詳細については [Device Manager] タブについてを参照してください。
- [Environment]: センサが Rack PDU に接続されている場合は、温度と湿度のセンサデータを表示します。
- [Logs]: イベント、データ、およびシステムログ記録を表示します。
- [Administration]: セキュリティ、ネットワーク接続、通知、および一般設定項目を設定します。

デバイスステータスアイコン

Rack PDU の現在の動作状態は、下記のアイコンおよび各アイコンと共に表示されるテキストにより確認できます。

	[Critical]（致命的）： 直ちに対処を要する重大な障害が発生しています。
	[Warning]（警告）： 処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。
	[No Alarms]（アラームなし）： アラームは発生しておらず、Rack PDU は正常に稼動しています。

Web インターフェイスの各ページの右肩にも [Home] ページの各時点の表示と同様のアイコンが表示され、Rack PDU の状態を確認できます。

- [No Alarms] アイコンの場合、発生中のアラームはありません。
- 上記以外のアイコン（[Critical] と [Warning] アイコンのどちらかまたは両方）が表示されている場合、表示されたレベルのアラームが発生しています。アイコンのあとには当該アラームレベルの発生件数が表示されます。

[Home] タブに戻ってアクティブなアラームなど Rack PDU ステータスの概要を表示するには、インターフェイスの任意のページでクイックステータスアイコンをクリックします。

クイックリンク

インターフェイスの左下には、設定可能な 3 つのリンクがあります。デフォルト設定は次のようになります。

- Link 1: dell.com
- Link 2: dell.com/home
- Link 3: dell.com/business

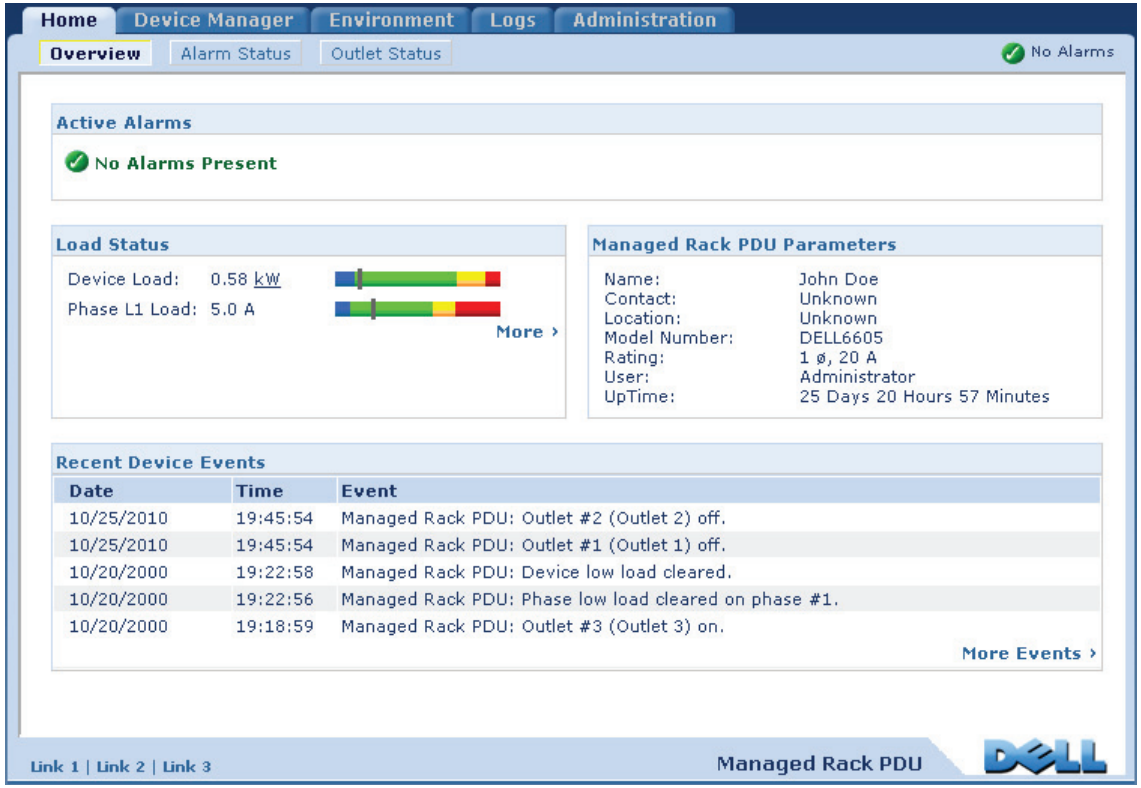
 これらのリンクを設定し直すには、リンクの設定を参照してください。

Web インターフェイスのその他の機能

- IP アドレスは左上隅に表示されます。
- [Help] リンク（内容に対応）と [Log off] リンクは右上隅に表示されます。

[Home] タブについて

アクティブなアラーム、Rack PDU の負荷状態、Rack PDU の最新イベントを表示するには、[Home] タブを使用します。

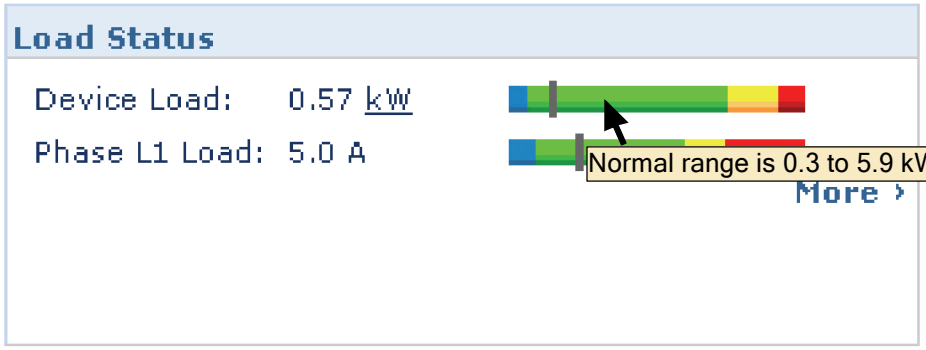


[Overview] ビュー

選択項目：[Home] > [Overview]

[Overview] の上部には、アラームのステータスが表示されます。1 つまたは複数のアラームが発生している場合は、アラームの種類と数が [Alarm Status] ビューへのリンクと共に表示されます。[Alarm Status] ビューには、各アラームの説明が表示されます。アラームが発生していない場合は、[Overview] には「No Alarms Present」と表示されます。

[Load Status] エリアには、デバイスの負荷（kW）と相の負荷（A、該当する場合）が表示されます。緑、黄、赤のメーターは、現在の負荷状態（ 正常、過負荷寸前、過負荷）を示します。低負荷しきい値を設定している場合は、メーターには緑の左側に青の部分が追加されます。設定された負荷しきい値を表示するには、カラーをマウスで選択します。



[More] をクリックして [Device Manager] タブを表示すると、しきい値の設定とピーク負荷情報の表示と管理を行うことができます。

デバイスパラメータ領域には、Rack PDU にアクセスしているユーザーアカウントの名前、連絡先、位置、定格電流、種類、そして管理インターフェイスの電源入れ直しまたは再起動のいずれかによる最後の再起動からの Rack PDU の連続稼働時間が表示されます。（詳細については、Rack PDU のリセットを参照してください。）

[Recent Device Events] に、最近発生したイベントと発生日時が新しいものから順に表示されます。最大 5 個のイベントが、同時に表示されます。[More Events] をクリックして [Logs] タブを表示すると、イベントログ記録全体を表示することができます。

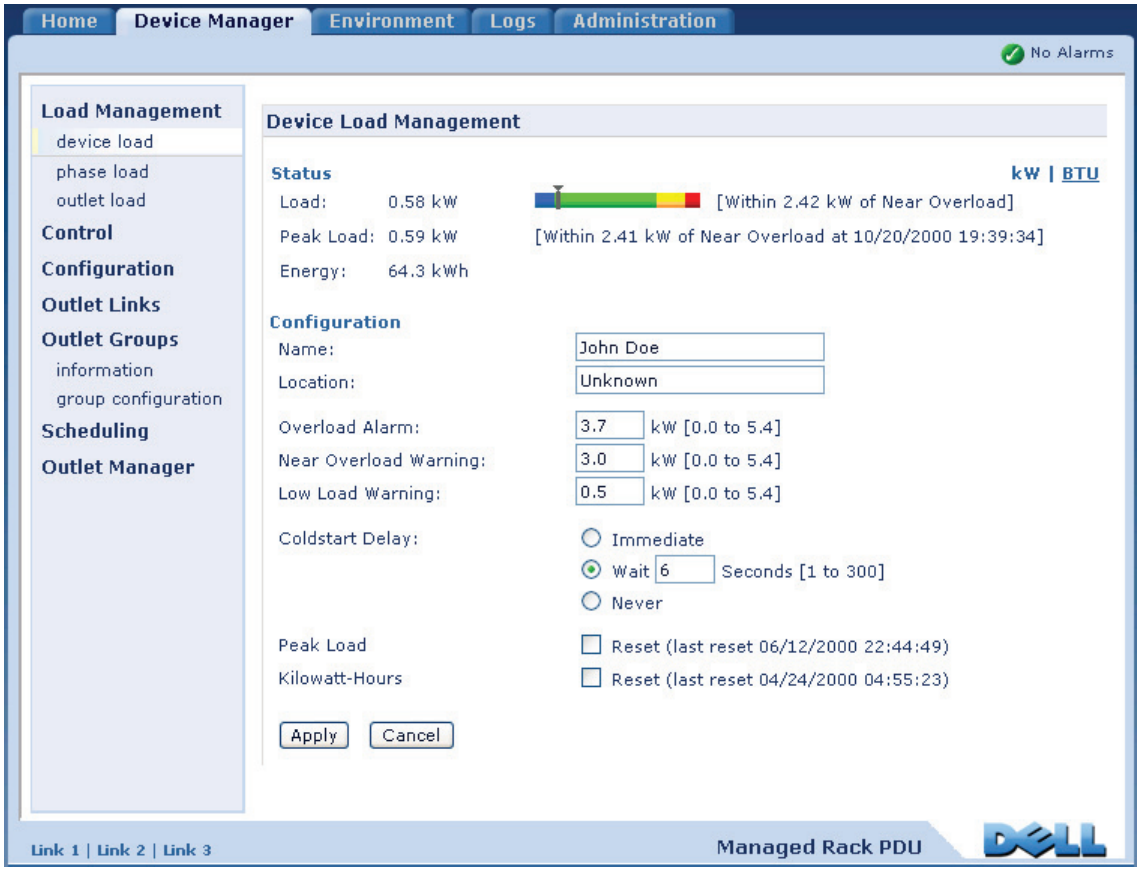
[Alarm Status] ビュー

選択項目：[Home] > [Alarm Status]

[Alarm Status] ビューでは、現在発生しているすべてのアラームの説明が表示されます。

温度または湿度しきい値違反の詳細については、[Environment] タブをクリックしてください。

デバイスの管理


Home
Device Manager
Environment
Logs
Administration
No Alarms
Load Management
device load
phase load
outlet load
Control
Configuration
Outlet Links
Outlet Groups
information
group configuration
Scheduling
Outlet Manager
Device Load Management
Status
kW | BTU
Load: 0.58 kW
[Within 2.42 kW of Near Overload]
Peak Load: 0.59 kW
[Within 2.41 kW of Near Overload at 10/20/2000 19:39:34]
Energy: 64.3 kWh
Configuration
Name: John Doe
Location: Unknown
Overload Alarm: 3.7 kW [0.0 to 5.4]
Near Overload Warning: 3.0 kW [0.0 to 5.4]
Low Load Warning: 0.5 kW [0.0 to 5.4]
Coldstart Delay:
Immediate
Wait 6 Seconds [1 to 300]
Never
Peak Load
Reset (last reset 06/12/2000 22:44:49)
Kilowatt-Hours
Reset (last reset 04/24/2000 04:55:23)
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

[Device Manager] タブについて

選択項目： [Device Manager]

[Device Manager] タブは、次の場合に使用します。

- Rack PDU の負荷状態を表示
- 接続されたすべてのデバイスと相（該当する場合）の負荷しきい値の設定
- コンセントの管理と制御
- の名前と位置の設定 Rack PDU
- ピーク負荷計測の表示と管理
- ユーザー設定可能なリンクをクリックして、Rack PDU に接続された各デバイス用の Web ページを開く

負荷状態とピーク負荷の表示

選択項目：[Device Manager] > *[Load Management] オプション*

緑、黄、赤のメーターのインジケータは、現在の負荷状態： 正常、過負荷寸前、過負荷を示します。低負荷しきい値を設定している場合は、メーターには緑の左側に青の部分が追加されます。[Device Load] を表示している場合は、メーター上部の三角形がピーク負荷を示します。

右上隅にある [kW | BTU] をクリックすると、負荷値の単位がキロワットと英国熱量単位（BTU）の間で切り替わります。

負荷しきい値の設定

選択項目： [Device Manager] > *[Load Management] オプション*

負荷しきい値を設定するには、次の手順を実行します。

1. [Device Manager] タブをクリックします。
2. デバイスや相の負荷しきい値を設定するには、[Load Management] メニューから選択を行います。
3. [Overload Alarm]、[Near Overload Warning]、および [Low Load Warning] しきい値を設定します。
4. [Apply] をクリックします。

Rack PDU の名前と位置の設定

選択項目：[Device Manager] > [Load Management] > [Device Load]

入力した名前と位置が [Home] タブに表示されます。

名前と位置は、[Device Manager] タブまたは [Administration] タブのいずれかで設定できます。一方での変更は、もう一方にも反映されます。

1. [Device Manager] タブをクリックし、[Load Management] メニューから [device load] を選択します。
2. 名前と位置を入力します。
3. [Apply] をクリックします。

[Coldstart Delay] の設定

選択項目：[Device Manager] > [Device Load]

[Coldstart Delay] は、Rack PDU に電源を投入してからコンセントの電源がオンになるまでの各コンセントの [Power On Delay] に追加する秒数です。設定できる値は、1 ～ 300 秒、[Immediate]、[Never]（電源オンされない）です。

1. [Device Manager] タブをクリックし、[Load Management] メニューから [device load] を選択します。
2. [Coldstart Delay] の選択を行います。
3. [Apply] をクリックします。

ピーク負荷と kWh のリセット

選択項目： [Device Manager] > [Device Load]

1. [Device Manager] タブをクリックし、[Load Management] メニューから [device load] を選択します。
2. 必要に応じて、[Peak Load] および [Kilowatt-Hours] チェックボックスをクリックします。
3. [Apply] をクリックします。

コンセントグループの設定と制御

コンセントグループに関する用語

*コンセントグループ*は、同一の Rack PDU 上で論理的に相互リンクされているコンセントから構成されます。1 つのコンセントグループに含まれる複数のコンセントを、同期して電源オン、電源オフ、再起動します。

- *ローカルコンセントグループ*は、1 つの Rack PDU 上の 2 つ以上のコンセントから構成されます。そのグループに含まれるコンセントのみが同期されます。
- *グローバルコンセントグループ*は、1 つの Rack PDU 上の 1 つまたは複数のコンセントから構成されます。1 つのコンセントを*グローバルコンセントとして設定し*、そのコンセントグループを最大 3 つまでの別の Rack PDU 上のコンセントグループに論理的にリンクします。リンクしたグローバルコンセントグループに含まれるすべてのコンセントが同期されます。
  - グローバルコンセントグループ内のアクションを実行したグループを*イニシエータコンセントグループ*と呼びます。
  - グローバルコンセントグループ内のイニシエータコンセントグループと同期する別のコンセントグループを*フォロアコンセントグループ*と呼びます。

コンセントグループのメンバーであるコンセントにコンセントコントロールアクションを適用すると、コンセントは次のように同期されます。

- グローバルコンセントグループでは、イニシエータコンセントグループのグローバルコンセントに設定された遅延時間と再起動待機時間が使用されます。
- ローカルコンセントグループでは、グループ内で一番小さい番号のコンセントの遅延時間と再起動待機時間が使用されます。

コンセントグループの目的と利点

Rack PDU 上で同期されたコンセントのグループを使用することで、複数のコンセントを同時にオン、オフ、再起動することができます。コンセントグループ全体でグループのアクションを同期して制御すると、次の利点があります。

- デュアルコードタイプのサーバーの電源のシャットダウンと起動を同期すると、あらかじめ決められたシステムシャットダウンまたは再起動時に、電源障害が誤って通知されることがなくなります。
- コンセントグループを利用してコンセントを同期すると、個々のコンセントの遅延時間に依存する場合と比べて、シャットダウンと再起動のタイミングがより正確になります。
- グローバルコンセントをリンク先の Rack PDU のユーザーインターフェイスに表示できます。

コンセントグループのシステム要件

同期されたコンセント制御グループをセットアップして使用するには、次の要件を満たす必要があります。

- 10/100Base-T TCP/IP ネットワークで、コンピュータやその他の同期するデバイスと電源を共有していないイーサネットハブまたはスイッチを備えている必要があります。
- コンセントグループを複数の Rack PDU 間で同期する場合は、それらの Rack PDU が次の要件を満たしている必要があります。
  - 同一サブネットに属していること。
  - オペレーティングシステム（AOS）モジュールとアプリケーションモジュールの両方が同じバージョン番号のファームウェアを使用していること。
- Rack PDU の Web インターフェイスやコマンドラインインターフェイスまたは SNMP を介して同期された制御操作を始動できるコンピュータであることが必要です。
- 同期させるコンセントグループが、同一の Multicast IP アドレスを持つ必要があります。Rack PDU を接続する各 Ethernet スイッチによって、Multicast IP アドレスの Multicast ネットワーク通信が可能になっていることを確認してください。

コンセントグループ設定のルール

コンセントグループを利用するシステムには、次のルールが適用されます。

- Rack PDU は複数のコンセントグループを持つことができますが、各コンセントが属することができるのは 1 つのコンセントブループのみです。
- ローカルコンセントグループは、グローバルコンセント以外の 2 つ以上のコンセントから構成されている必要があります。
- 1 つの Rack PDU 上のグローバルコンセントグループは、別の 3 つの各 Rack PDU 上のグローバルコンセントグループと同期することができます。
  - グローバルコンセントグループでは、グローバルコンセントに指定できるのは 1 つのコンセントのみで、同期のために別の Rack PDU 上のコンセントグループにリンクします。そのグローバルコンセントはグループ内で唯一のコンセントのこともあれば、そのグループが複数のコンセントから構成されていることもあります。
  - Rack PDU のコンセントグループを同期のためにリンクするには、これらの Rack PDU が同一の Device Multicast Name と Device Multicast Address を持ち、同じバージョンの Rack PDU ファームウェアを実行している必要があります。
  - 1 つのコンセントグループのグローバルコンセントの物理コンセント番号は、リンク先の別のコンセントグループのグローバルコンセントと同一番号である必要があります。
- コンセントグループを作成、設定するには、Web インターフェイスを使用するか、または設定済みの Rack PDU から設定ファイル（.ini file）をエクスポートする必要があります。コマンドラインインターフェイスでは、コンセントがコンセントグループのメンバーかどうかを表示し、コンセントグループに制御アクションを適用することができますが、コンセントグループのセットアップや設定は行えません。

コンセントグループの有効化

[Device Manager] タブをクリックして、左側ナビゲーションメニューの [Outlet Groups] から [Group Configuration] を選択します。次のパラメータを設定して、[Apply] をクリックします。

コンセントグループの作成の有効化

パラメータ	説明
[Device Level Outlet Group]	コンセントグループを作成するには、このパラメータを有効にする必要があります。デフォルトでは無効です。

グローバルコンセントグループ（リンクされたグループ）のサポートの有効化

パラメータ	説明
[Multicast Name]	複数の Rack PDU 上のコンセントグループをリンクするには、これらの Rack PDU のそれぞれに同一の Multicast 名と Multicast IP アドレスを指定する必要があります。 **注意：** 同一の Multicast 名と Multicast IP アドレスで最大 4 台のデバイスを設定できます。
[Multicast IP]	

コンセントグループの暗号化と認証の有効化

パラメータ	説明
[Authentication Phrase]	デバイスが他のデバイスと通信中であること、メッセージが送信中に改ざんされていないこと、そして送受信が時間通りに行われたことを確認する 15 ～ 32 文字の ASCII 文字からなるフレーズ。このフレーズは、遅延がなく、コピーされて後から時間に遅れて再送信されたものではないことを示します。
[Encryption Phrase]	暗号化によりデータのプライバシーを確認する 15 ～ 32 文字の ASCII 文字からなるフレーズ

コンセントグループのポートの設定

パラメータ	説明
[Outlet Group Port]	デバイスが他のデバイスと通信するポートの番号

他のデバイス上のコンセントグループと同期させるデバイスはすべて、Authentication Phrase、Encryption Phrase、Group Port Number を同じにする必要があります。値はユーザーには非表示になっています。

ローカルコンセントグループの作成

1. [Device Manager] タブで、左側ナビゲーションメニューの [Outlet Groups] から [Information] を選択します。
2. コンセントグループが有効になっていることを確認します。(コンセントグループの有効化を参照)。
3. [Create Local Outlet Group] をクリックします。
4. [Select Local Outlets] で、グループ化するコンセントを選択して [Outlet Group Name] フィールドにグループ名を入力します。コンセントは、2 つ以上選択する必要があります。

複数のグローバルコンセントグループの作成

別の Rack PDU 上のコンセントグループにリンクしている複数のグローバルコンセントグループのセットアップ手順

1. [Device Manager] タブで、左側ナビゲーションメニューの [Outlet Groups] から [Information] を選択します。
2. コンセントグループが有効になっていて、リンクする Rack PDU すべての Multicast パラメータ（名前と IP アドレス）が同じであることを確認します。（コンセントグループの有効化を参照。）
3. [Create Global Outlet Groups] をクリックします。
4. 作成する各グローバルコンセントグループで、チェックボックスをクリックしてコンセントを選択します。次に [Apply] をクリックします。たとえば、1 つのグローバルコンセントから構成されるコンセントグループを 5 つ作成するには、5 つのコンセントを選択します。
5. 作成したグローバルコンセントグループにコンセントを追加する方法については、コンセントグループの編集と削除を参照してください。

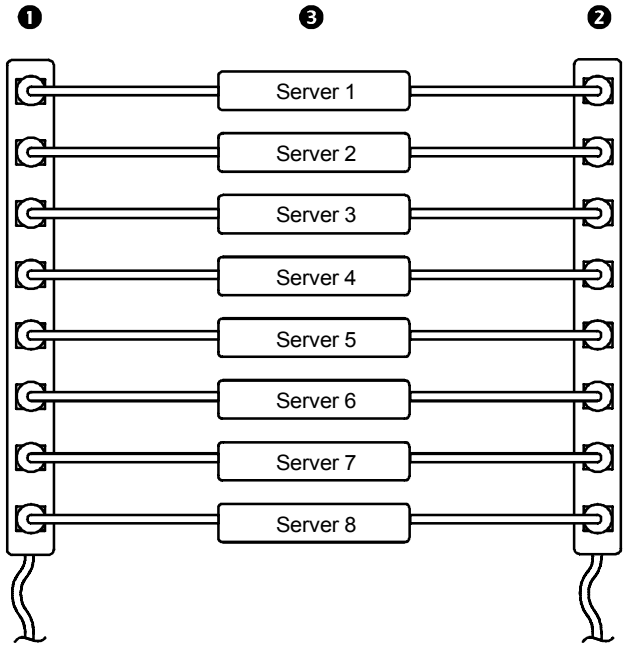
コンセントグループの編集と削除

1. [Device Manager] タブで、左側ナビゲーションメニューの [Outlet Groups] から [Information] を選択します。
2. [Configured Outlet Groups] で、編集または削除するコンセントグループの番号または名前をクリックします。
3. コンセントグループの編集では、次のいずれかを行うことができます。
   - コンセントグループの名前の変更
   - チェックボックスをクリックして選択 / 選択解除して、コンセントを追加または削除

   残っているコンセントがグローバルコンセントでない限り、コンセントが 2 つしかないコンセントグループからコンセントを削除することはできません。
4. コンセントグループを削除するには、[Delete Outlet Group] をクリックします。

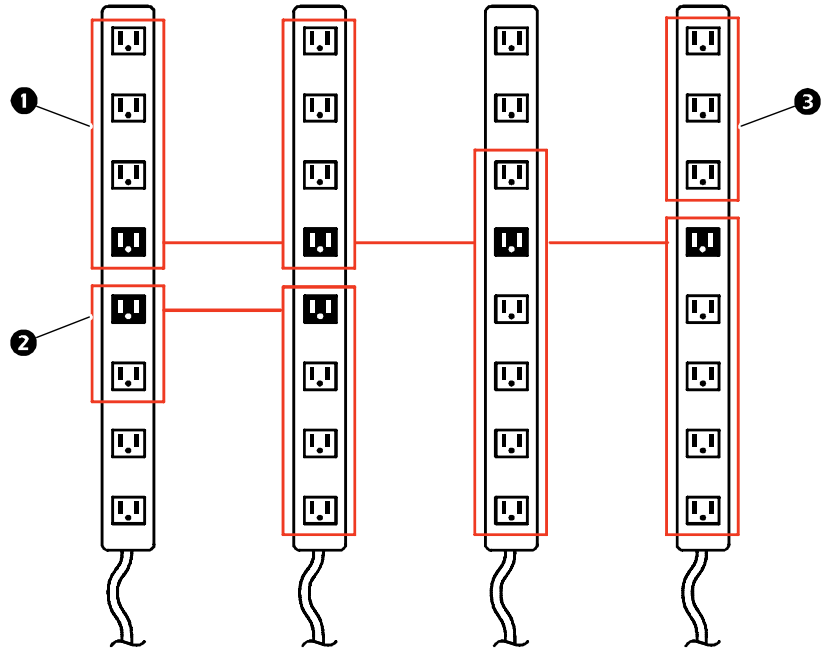
一般的なコンセントグループ設定

次の設定は、それぞれに 8 つのコンセントグループを含む 2 つの Rack PDU を示しています。各コンセントグループは 1 つのグローバルコンセントから構成されています。1 番目の Rack PDU 上の各コンセントグループ ❶ は、2 番目の Rack PDU 上の同一場所にあるコンセントグループ ❷ にリンクされています。デュアルコードタイプのサーバー ❸ の一方の電源コードは 1 番目の Rack PDU 上の各コンセントに接続され、もう一方のコードは 2 番目の Rack PDU の対応するコンセントに接続されています。電源からサーバーへの出力電力は、コンセント制御アクションに応じて同時にオン / オフに切り替わります。



次の設定は、3 セットのコンセント同期を示したものです。グローバルコンセントは黒で示されています。コンセントグループは赤い長方形で囲まれています。

❶	この 4 つのグローバルコンセントグループは、合計 19 個のコンセントを同期しています。
❷	この 2 つのグローバルコンセントグループは、6 つのコンセント（1 つのグループに 2 つ、もう 1 つのグループに 4 つ）を同期しています。
❸	このローカルコンセントグループは、1 つの Rack PDU 上の 3 つのコンセントを同期しています。



グローバルコンセントグループのセットアップと設定の確認

セットアップがコンセントグループのシステム要件すべてを満たし、コンセントグループを正しく設定したことを確認するには、Web インターフェイスの左側ナビゲーションメニュー [Outlet Groups] で [Information] を選択し、グループとその接続を表示します。

- [Configured Outlet Groups] セクションには次の内容が表示されます。
  - 現在の Rack PDU 上の設定済みコンセントグループすべて。
  - 各グループのコンセントをコンセント番号順に表示。
  - グローバルコンセントグループの同期相手になる、別の Rack PDU 上のコンセントグループ。各 Rack PDU は IP アドレスによって識別され、各グローバルコンセントは太字で表示されます。
- [Global Outlet Overview] セクションには次の内容が表示されます。
  - 現在の Rack PDU の IP アドレス。
  - 別の Rack PDU 上のコンセントグループとの同期に利用可能なグローバルコンセントが含まれた Rack PDU の IP アドレス。
  - 現在の Rack PDU 上のコンセントグループと同期されているかどうかに関わらず、Rack PDU 上で設定されたグローバルコンセントすべて。

コンセントとコンセントグループのコンセント設定

制御アクションの開始

コンセントまたはコンセントグループにコンセント制御アクションを適用すると、そのアクションに次の遅延が使用されます。

- 個々のコンセント（コンセントグループに含まれない）については、そのコンセントに設定された遅延時間と再起動待機時間がアクションに使用されます。
- グローバルコンセントグループについては、グローバルコンセントに設定された遅延時間と再起動待機時間がアクションに使用されます。
- ローカルコンセントグループについては、グループ内で一番小さい番号のコンセントに設定された遅延時間がアクションに使用されます。

Rack PDU 上でコンセントを制御する手順

1. [Device Manager] タブで左側ナビゲーションメニューから [Control] を選択します。
2. 制御するコンセントまたはコンセントグループの各チェックボックスを選択するか、または [All Outlets] チェックボックスを選択します。
3. 一覧から [Control Action] を選択し、[Next> >] をクリックします。アクションを説明する確認ページで、適用または取消を選択します。

選択可能な制御アクション

オプション	説明
[No Action]（Web インターフェイスのみ）	何も実行されません。
[On Immediate]	選択したコンセントに電力を供給します。
[On Delayed]	[Power On Delay] の値に従って、選択した各コンセントに電力を供給します。†
[Off Immediate]	選択したコンセントの電力を切断します。
[Off Delayed]	[Power Off Delay] の値に従って、選択した各コンセントの電力を切断します。†
[Reboot Immediate]	選択した各コンセントの電力を切断します。それから [Reboot Duration] の値に従って、それらの各コンセントに電力を供給します。†
[Reboot Delayed]	[Power Off Delay] の値に従って、選択した各コンセントの電力を切断します。すべてのコンセントがオフになるまで待機し（[Reboot Duration] の最大値）、それから [Power On Delay] の値に従って各コンセントに電力を供給します。†
[Cancel Pending Commands]	選択したコンセントの保留中のコマンドをすべて取り消し、現在の状態を保ちます。 **注意：** グローバルコンセントグループについては、コマンドの取り消しはイニシエータコンセントグループのインターフェイスからのみ行うことができます。このアクションにより、イニシエータコンセントグループとすべてのフォロアコンセントグループのコマンドが取り消されます。

† ローカルコンセントグループを選択した場合は、グループ内で一番小さい番号のコンセントに設定された遅延と再起動待機時間のみが使用されます。グローバルコンセントグループを選択した場合は、グローバルコンセントに設定された遅延と再起動待機時間のみが使用されます。

コンセント設定とコンセント名の設定

次の設定を使用できます。

設定	説明
[Name]	1 つまたは複数のコンセントの名前を設定します。この名前は、ステータス画面上でコンセント番号の横に表示されます。
[External Link]	Web サイトや IP アドレスへの HTTP または HTTPS リンクを指定します。 ・http://www.dell.com は、コンセントから Dell の Web サイトへのリンクです。 ・http://*pdu_ip_address*（「*pdu_ip_address*」は Rack PDU の IP アドレス）は、コンセントから Rack PDU の Web インターフェイスへの IP アドレスによるリンクであり、権限を持つユーザーはログオンできます。
[Power On Delay]	コマンドの実行からコンセントの電力供給までの Rack PDU の待機時間（秒）を設定します。 **注意：** コンセントが常時オフになるように設定するには、[Power On Delay] の横にある [Never] チェックボックスを選択します。
[Power Off Delay]	コマンドの実行からコンセントの電力切断までの Rack PDU の待機時間（秒）を設定します。 **注意：** コンセントが常時オンになるように設定するには、[Power Off Delay] の横にある [Never] チェックボックスを選択します。
[Reboot Duration]	コンセントが再度起動されるまでの待機時間（秒）を設定します。

コンセント設定またはコンセント名を設定するには、[Device Manager] タブを選択してから左側ナビゲーションメニューの [Configuration] を選択します。[Outlet Configuration] セクションの [Configure Multiple Outlets] ボタンをクリックするか、またはコンセント名をクリックします。

・複数のコンセントのコンセント設定
  - 変更するコンセント数の横にあるチェックボックスを選択するか、または [All Outlets] チェックボックスを選択します。
  - [Name] および [Link] の値を入力し、リストのすぐ下にある [Apply] ボタンをクリックします。
  - [Power On Delay]、[Power Off Delay]、または [Reboot Duration] の値を入力し、リストのすぐ下にある [Apply] ボタンをクリックします。

・単一のコンセントのコンセント設定
  - [Name] および [Link] の値を入力し、リストのすぐ下にある [Apply] ボタンをクリックします。
  - [Power On Delay]、[Power Off Delay]、または [Reboot Duration] の値を入力し、リストのすぐ下にある [Apply] ボタンをクリックします。

コンセントアクションのスケジューリング

スケジューリング可能なアクション

各コンセントの [Power On Delay]、[Power Off Delay]、[Reboot Duration] の値を設定する方法については、コンセント設定とコンセント名の設定を参照してください。コンセントアクションのスケジューリングには Web インターフェイスを使用する必要がありますが、これらの値の設定は Web インターフェイスまたはコマンドラインインターフェイスのいずれでも可能です。

コンセントグループに適用するアクションについては、スケジュールされたアクションの開始時にコンセントグループが有効になっている必要があります。例えば、[Off Delayed] が午後 4 時にスケジューリングされている場合、[Power Off Delay] は午後 4 時に開始されます。たとえコンセントのいずれも電源オフされるようスケジューリングされていないその [Power Off Delay] 期間にコンセントグループを有効にしたとしても、アクションは個々のコンセントにのみ適用され、コンセントグループには適用されません。

選択した任意のコンセントに対して、下記の表に記載されたアクションのいずれかを毎日、1、2、4、8 週間おき、または 1 度のみ行うようにスケジューリングすることができます。

オプション	説明
[No Action]	何も実行されません。
[On Immediate]	選択したコンセントに電力を供給します。
[On Delayed]	[Power On Delay] の値に従って、選択した各コンセントに電力を供給します。†
[Off Immediate]	選択したコンセントの電力を切断します。
[Off Delayed]	[Power Off Delay] の値に従って、選択した各コンセントの電力を切断します。†
[Reboot Immediate]	選択した各コンセントの電力を切断します。それから [Reboot Duration] の値に従って、これらの各コンセントに電力を供給します。†
[Reboot Delayed]	[Power Off Delay] の値に従って、選択した各コンセントの電力を切断します。すべてのコンセントがオフになるまで待機し（[Reboot Duration] の最大値）、それから [Power On Delay] の値に従って各コンセントに電力を供給します。†

† ローカルコンセントグループを選択した場合は、グループ内で一番小さい番号のコンセントに設定された遅延と再起動待機時間のみが使用されます。グローバルコンセントグループを選択した場合は、グローバルコンセントに設定された遅延と再起動待機時間のみが使用されます。

コンセントイベントのスケジューリング

1. Web インターフェイスで [Device Manager] タブを選択してから、左側ナビゲーションメニューの [Scheduling] を選択します。
2. [Outlet Scheduling] ページで [One-Time]、[Daily]、[Weekly] からイベント発生頻度を選択して、[Next] ボタンをクリックします。

   [Weekly] を選択した場合は、イベントの発生頻度を 1 週間、2 週間、4 週間、8 週間に 1 回の中から選択できます。

3. [Schedule a Daily Action] ページの [Name of event] テキストボックスで、デフォルト名「**Outlet Event**」を新規イベントを識別する名前に置き換えます。
4. ドロップダウンリストから、イベントの種類とその発生日時を選択します。

   ワンタイムイベントの日付形式は *mm/dd*、すべてのイベントの時刻形式は *hh/mm*（24 時間表示）です。

   - 毎日、または [Weekly] セクションで利用可能な間隔のいずれかでスケジューリングされているイベントは、そのイベントが削除されるか無効になるまで、スケジューリングされている間隔で発生し続けます。
   - ワンタイムイベントが発生するようにスケジューリングできるのは、スケジューリングを行う日から 12 か月以内の日付のみです。例えば、2010 年 12 月 26 日には、当日から 2011 年 12 月 26 日までの任意の日付にワンタイムイベントをスケジューリングすることができます。

5. アクションを適用するコンセントをチェックボックスで選択します。1 つまたは複数のコンセントを選択することも、また [All Outlets] を選択することも可能です。
6. [Apply] をクリックしてイベントのスケジューリングを確定するか、または [Cancel] をクリックして取り消します。

イベントを確定すると、サマリページが再表示され、スケジューリングされたイベントの一覧に新しいイベントが表示されます。

スケジュール済みコンセントイベントの編集、有効化、無効化、削除

1. Web インターフェイスで [Device Manager] タブを選択してから、左側ナビゲーションメニューの [Scheduling] を選択します。
2. [Scheduling] ページの [Scheduled Outlet Action] セクションのイベント一覧で、イベント名をクリックします。
3. [Daily/Weekly scheduled action detail] ページで、次の設定を行うことができます。

- イベントの名前、スケジューリングされている発生日時、イベントを適用されるコンセントなど、イベントの詳細事項の変更
- ページ上部の [Status of event] で、次の作業を実行できます。
  - イベントを無効にし、後からもう一度有効にできるように詳細の設定をすべて残しておきます。無効になったイベントは発生しません。イベントは、デフォルトでは作成時に有効になっています。
  - イベントを前に [Disable] に設定した場合は、イベントを有効にします。
  - イベントを削除し、システムから完全に取り除きます。削除されたイベントは復旧できません。

4. このページでの変更作業が完了したら、[Apply] をクリックして変更を確定するかまたは [Cancel] をクリックして取り消します。

[Outlet Manager] メニュー

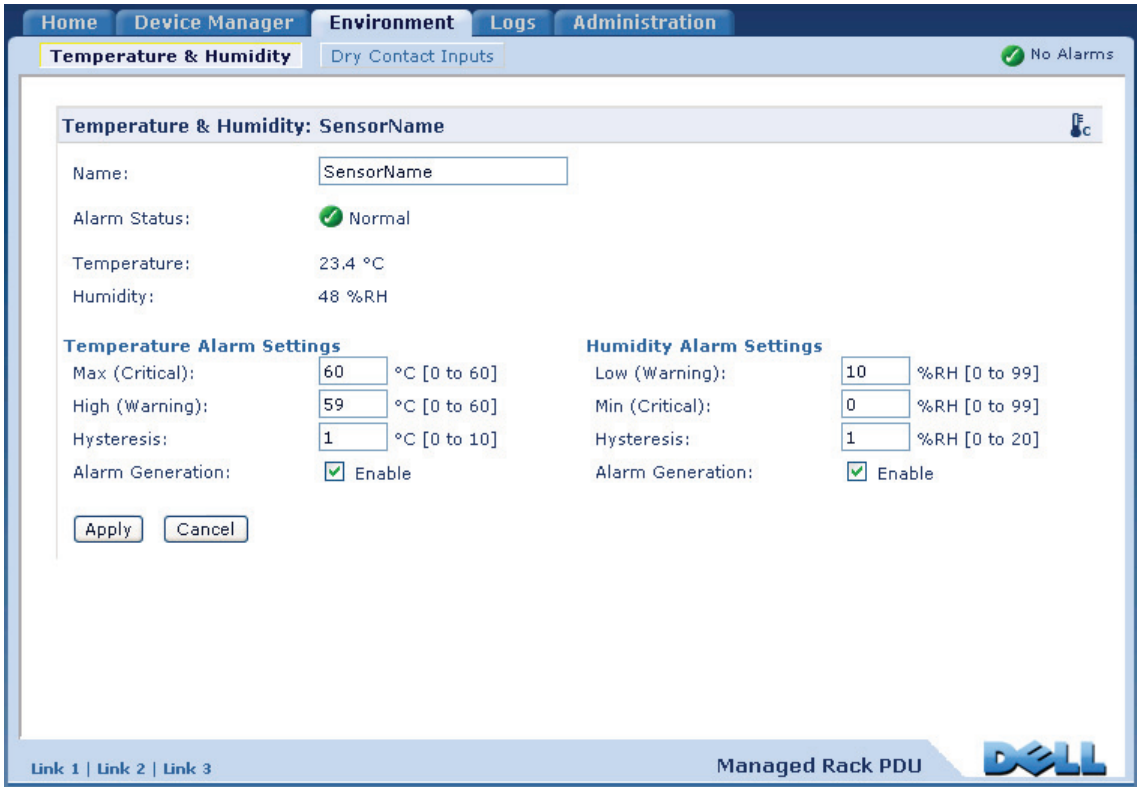
コンセントユーザーのアカウントを作成および設定します。個別のコンセントをコンセントユーザーアカウントを持つユーザに割り当てることができます。コンセントユーザーは、割り当てられたコンセントのみ制御することができます。コンセントの設定は管理者権限を持つユーザーのみ行うことができます。デバイスマネージャはコンセント設定の制限付きの権限を持ちます。

コンセントユーザーの設定

1. Web インターフェイスで [Device Manager] タブを選択してから、左側ナビゲーションメニューの [Outlet Manager] を選択します。
2. [Add New User] ボタンをクリックします。
3. 次のオプションに関する情報を入力して、[Apply] をクリックして変更を確定します。

オプション	説明
[User Name]	コンセントユーザー名を設定します。「New User」は予約語で、使用できません。 **注意：** オレンジで表示されたユーザー名は、そのユーザーアカウントが無効になっていることを示します。
[Password]	コンセントユーザーのパスワードを設定します。
[User Description]	コンセントユーザーの ID/ 説明を設定します。
[Account Status]	コンセントユーザーのアカウントを有効化、無効化、または削除します。
[Device outlet access]	ユーザーがアクセスできるコンセントを選択します。

環境


Home
Device Manager
Environment
Logs
Administration
Temperature & Humidity
Dry Contact Inputs
No Alarms
Temperature & Humidity: SensorName
Name:
SensorName
Alarm Status:
Normal
Temperature:
23.4 °C
Humidity:
48 %RH
Temperature Alarm Settings
Max (Critical):
60
°C [0 to 60]
High (Warning):
59
°C [0 to 60]
Hysteresis:
1
°C [0 to 10]
Alarm Generation:
Enable
Humidity Alarm Settings
Low (Warning):
10
%RH [0 to 99]
Min (Critical):
0
%RH [0 to 99]
Hysteresis:
1
%RH [0 to 20]
Alarm Generation:
Enable
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

温度および湿度センサの設定

選択項目： [Environment] > [Temperature & Humidity]

Rack PDU に温度センサまたは温度 / 湿度センサを接続している場合は、[Temperature & Humidity] ページから Warning および Critical アラーム（アラームの種類の詳細はデバイスステータスアイコンを参照）を生成するしきい値を設定することができます。

温度設定を実行すると、次のようになります。

- 高温しきい値に到達すると、システムが Warning アラームを発生
- 最高温度しきい値に到達すると、システムが Critical アラームを発生

同様に、湿度設定を実行すると次のようになります。

- 低湿しきい値に到達すると、システムが Warning アラームを発生
- 最低湿度しきい値に到達すると、システムが Critical アラームを発生

右上隅にある温度計記号をクリックすると、華氏と摂氏が切り替わります。

温度センサと湿度センサを設定するには、次の手順を実行します。

1. 最低、最高、高（温、湿）、低（温、湿）しきい値を入力します。
2. [Hysteresis] の値を入力します （詳細については、ヒステリシスを参照）。
3. 必要に応じて、アラームの生成を有効にします。
4. [Apply] をクリックします。

ヒステリシス この値は、温度または湿度でしきい値超過状態がクリアされる条件となる、しきい値からの差異を指定します。

- [最高] と [高温] のしきい値の場合、クリアポイントはしきい値からヒステリシスを差し引いた値です。
- [最低] と [低湿] のしきい値の場合、クリアポイントはしきい値にヒステリシスを加えた値です。

温度または湿度がわずかに上下に変動する場合に、しきい値超過アラームが何度も発生しないようにするには、[Temperature Hysteresis]（温度ヒステリシス）または[Humidity Hysteresis]（湿度ヒステリシス）の値を大きくします。ヒステリシスの値が低すぎるとこのような変動が生じることがあり、しきい値超過とクリアが繰り返し発生します。

変動しながら上昇する温度の例： 最高温度しきい値は 85° F、温度ヒステリシスは 3° F で、温度が 85° F を下回ると、しきい値超過が発生します。84° F まで変動しながら低下した後、86° F まで上昇する状態が繰り返し発生しますが、イベントがクリアされたり、新たに超過が発生したりすることはありません。既存の超過状態がクリアされるには、温度が 82° F（しきい値より 3° F 下回る）より低下しなければなりません。

変動しながら低下する湿度の例： 湿度の最低しきい値は 18%、湿度ヒステリシスは 8% です。湿度が 18% を下回ると、しきい値超過が発生します。24% まで変動しながら上昇した後、13% まで低下する状態が繰り返し発生しますが、イベントがクリアされたり新たに超過が発生したりすることはありません。既存の超過状態がクリアされるには、湿度が 26%（しきい値を 8% 超過）を超過しなければなりません。

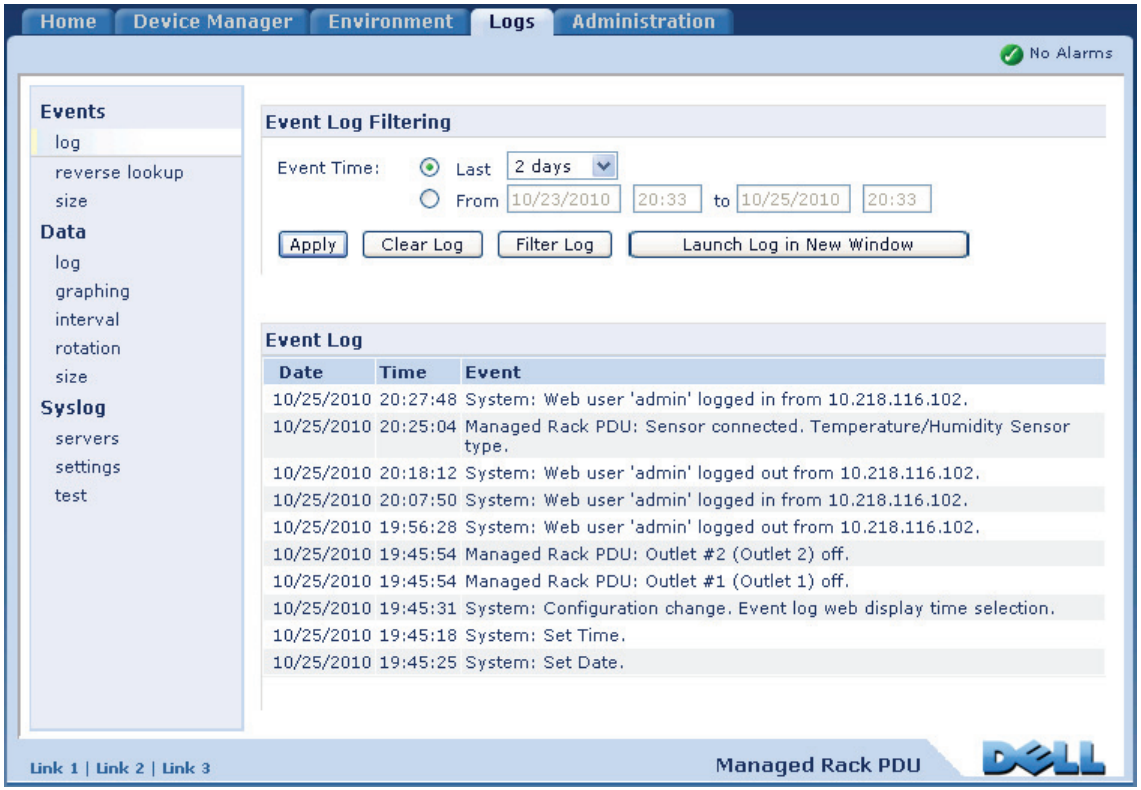
ドライ接点入力の設定

選択項目：[Environment] > [Dry Contact Inputs]

[Dry Contact Inputs] ページで、ドライ接点の現在のステータスと状態の表示と、ドライ接点の設定を行うことができます。

パラメータ	説明
[Name]	入力接点の名前。*最大* 20 文字。
[Alarm Status]	入力接点でアラームが発生していない場合は [Normal]、またはアラームが発生している場合はその重要度を表示
[State]	入力接点の現在の状態。[Closed] または [Open]。
[Alarm Generation]	入力接点の有効 / 無効を切り替えます。無効になっている場合、接点が異常な位置にあってもアラームイベントは発生しません。
[Normal State]	入力接点の通常（非アラーム）の状態。[Closed] または [Open]。

ログ


Home
Device Manager
Environment
Logs
Administration
No Alarms
Events
log
reverse lookup
size
Data
log
graphing
interval
rotation
size
Syslog
servers
settings
test
Event Log Filtering
Event Time:
Last
2 days
From
10/23/2010
20:33
to
10/25/2010
20:33
Apply
Clear Log
Filter Log
Launch Log in New Window
Event Log
Date
Time
Event
10/25/2010 20:27:48 System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010 20:25:04 Managed Rack PDU: Sensor connected. Temperature/Humidity Sensor type.
10/25/2010 20:18:12 System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010 20:07:50 System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010 19:56:28 System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010 19:45:54 Managed Rack PDU: Outlet #2 (Outlet 2) off.
10/25/2010 19:45:54 Managed Rack PDU: Outlet #1 (Outlet 1) off.
10/25/2010 19:45:31 System: Configuration change. Event log web display time selection.
10/25/2010 19:45:18 System: Set Time.
10/25/2010 19:45:25 System: Set Date.
Link 1 | Link 2 | Link 3
Managed Rack PDU

イベントログ / データログの使用方法

イベントログ

選択項目： [Logs] > [Events] > *オプション*

イベントログに対しては、表示、フィルタの設定、または削除を実行できます。デフォルト設定では、ログには過去 2 日間に記録されたすべてのイベントが直近のものから表示されるようになっています。

設定可能な全イベントとその現在の設定を一覧表示するには、[Administration] タブ、上部メニューバーの [Notification]、そして左側ナビゲーションメニューの [Event Actions]、この下の [by event] を順にクリックします。

イベントごとの設定を参照してください。

イベントログを表示するには（[Logs] > [Events] > [log]）：

- デフォルト設定により、イベントログは Web インターフェイスに 1 ページ形式で表示されます。最も新しいイベントが 1 ページ目です。ログの下のナビゲーションバーは下記のように操作します。
  - ページ番号をクリックすると、ログの該当のページが開きます。
  - [Previous] または [Next] をクリックすると、開いているページに一覧表示されている一連のイベントのすぐ前かすぐ後のイベントグループを表示できます。
  - [<<] ではログの最初のページに、[>>] ではログの最後のページに移動できます。
- ログに入力されているイベントをページ内にすべて表示させたい場合、イベントログページから [Launch Log in New Window]（ログを新しいウィンドウで開く）をクリックすると、ログ全体が全画面表示されます。

[Launch Log in New Window] ボタンを使用するには、ブラウザで JavaScript® を有効にしておく必要があります。

FTP または Secure CoPy（SCP）を使用しても、イベントログを表示することができます。FTP または SCP でログファイルを取得する方法を参照してください。

イベントログに対してフィルタを設定するには（[Logs] > [Events] > [log]）：

- **日時別にフィルタ処理するには：** イベントログの全体を表示したい場合、また「最近のイベント」に含めるイベントの数あるいは対象とする日数や月数を変更したい場合は、[Last] を選択します。ドロップダウンメニューから時間枠を選び、[Apply] をクリックします。このフィルタ設定は Rack PDU が次に再起動するまで保存されます。
  特定の時間枠に記録されたイベントを表示するには、[From] を選択します。該当の時間枠の開始と終了の時刻を（24 時間形式で）入力し、[Apply] をクリックします。このフィルタ設定は Rack PDU が次に再起動するまで保存されます。
- **イベント別にフィルタ処理するには：** ログに特定のイベントを表示させるようにするには、[Filter Log]（ログのフィルタ）をクリックします。イベントのカテゴリまたはアラームの重要度のチェックボックスのマークを外して、これらが表示されないようにします。イベントログページの右上隅に表示されている入力内容は、フィルタが有効であることを意味しています。
  管理者は、[Save As Default]（デフォルトとして保存）をクリックすることにより、このフィルタ設定を全ユーザーに対するデフォルトの表示形態に設定できます。管理者が [Save As Default] をクリックしていない場合は、そのフィルタ設定は、管理者がこの設定を解除するまで、または Rack PDU が次に再起動するまでの有効となります。
  有効になっているフィルタを削除するには、[Filter Log]、[Clear Filter (Show All)]（フィルタのクリア（すべて表示））を順にクリックします。

イベントに対するフィルタ処理は、論理 OR 演算子を使用して実行されます。

- [Filter By Severity]（重大度でフィルタ）リストで選択していないイベントは、[Filter by Category]（カテゴリでフィルタ）リストで指定してあるカテゴリでイベントが発生しても、フィルタ処理後のイベントログにはまったく表示されません。
- [Filter by Category] リストで選択していないイベントは、[Filter by Severity] リストで指定してあるカテゴリのデバイスでアラーム状況が発生しても、フィルタ処理後のイベントログにはまったく表示されません。

イベントログを削除するには（[Logs] > [Events] > [log]）：

イベントログに入力されたイベントをすべて削除するには、Web ページの [Clear Log]（ログのクリア）をクリックします。削除したイベントは復元できません。

イベントに割り当てられている重要度レベルまたはカテゴリに基づいてイベントを記録することを無効にするには、イベントごとの設定を参照してください。

逆引きを行うには（[Logs] > [Events] > [reverse lookup]）：

[Reverse lookup]（逆引き）はデフォルトでは無効です。DNS サーバーとして設定されているサーバーがないか、またはトラフィック過剰のためネットワークの機能が不良である場合を除き、この機能は有効にしてください。

[reverse lookup] を有効にすると、ネットワーク関連のイベントが発生した場合、そのイベントに関連するネットワークデバイスの IP アドレスとドメイン名が両方ともイベントログに記録されます。該当のデバイスにドメイン名がつけられていない場合、イベントには IP アドレスのみが記録されます。ドメイン名は通常、IP アドレスに比べて変更される頻度が低いことから、逆検索を有効にすると、イベントの原因となっているネットワークデバイスのアドレスを認識する機能を強化することができます。

イベントログの容量を調整するには（[Logs] > [Events] > [size]）：

デフォルト設定では、イベントログは 400 件までのイベントを収容できます。ログに含めるイベント数は変更できます。イベントログの容量を変更すると、それまでに記録されていたイベントはすべて削除されます。記録されているイベントデータを失うことを避けるため、[Event Log Size]（イベントログのサイズ）フィールドに新たな収容件数を入力する前に、FTP または SCP を使用してログ内のデータを保存してください。

 FTP または SCP でログファイルを取得する方法を参照してください。

ログが容量に達すると、データは古いものから削除されます。

データログ

選択項目：[Logs] > [Data] > *オプション*

データログには、デバイスと相（3 相 Rack PDU の場合）の電流と電力、および温度、湿度、ドライ接点のデータが指定した時間間隔で記録されます。各入力事項はデータが記録された日時別に一覧されます。

データログを表示するには（[Logs] > [Data] > [log]）：

- デフォルト設定により、データログは Web インターフェイスに 1 ページ形式で表示されます。最も新しいデータが 1 ページ目です。ログの下のナビゲーションメニューは下記のように操作します。
  - ページ番号をクリックすると、ログの該当のページが開きます。
  - [Previous] または [Next] をクリックすると、開いているページに一覧表示されている一連のデータのすぐ前かすぐ後のデータを表示できます。
  - [<<] ではログの最初のページに、[>>] ではログの最後のページに移動できます。
- ログに入力されているデータをページ内にすべて表示させたい場合、データログページから [Launch Log in New Window] をクリックすると、ログ全体が全画面表示されます。

[Launch Log in New Window] ボタンを使用するには、ブラウザのオプションの JavaScript を有効にする必要があります。

あるいは、FTP または SCP を使用しても、データログを表示することができます。FTP または SCP でログファイルを取得する方法を参照してください。

日時別にフィルタ処理するには（[Logs] > [Data] > [log]）：

データログの全体を表示したい場合、また「最近のイベント」に含めるイベントの数あるいは対象とする日数や月数を変更したい場合は、[過去] を選択します。ドロップダウンメニューから時間枠を選び、[Apply] をクリックします。このフィルタ設定はデバイスが次に再起動するまで保存されます。

特定の時間枠に記録されたデータを表示するには、[From] を選択します。該当の時間枠の開始と終了の時刻を（24 時間形式で）入力し、[Apply] をクリックします。このフィルタ設定はデバイスが次に再起動するまで保存されます。

データログを削除するには：

データログに記録されたデータをすべて削除するには、Web ページの [Clear Data Log]（データログの消去）をクリックします。削除したデータは復元できません。

データ収集の間隔を設定するには（[Logs] > [Data] > [interval]）：

[Log Interval]（ログの間隔）のオプションでは、データログに記録するデータの抽出 / 保存頻度を指定し、さらにこの設定に基づくと何日分のデータをログに保存できるかの計算を参照できます。ログが容量に達すると、データは古いものから削除されます。古いデータが自動的に削除されることを避けるため、次のセクションの手順に従ってログのローテーションを有効にし、設定してください。

データログのローテーションを設定するには（[Logs] > [Data] > [rotation]）：

FTP サーバーにデータログを保存するためのレポジトリファイルを設け、アクセス用のパスワードを設定します。ローテーション機能を有効にすると、データログのコンテンツは、FTP サーバーに設定してあるレポジトリファイルに名前およびロケーション別に付け加えられます。このファイルは、管理者が指定した更新間隔に従って更新されます。

パラメータ	説明
[Data Log Rotation]	データログのローテーションを有効または無効にします（デフォルトでは無効）。
[FTP Server Address]	データレポジトリファイルが格納されている FTP サーバーのアドレスです。
[User Name]	レポジトリファイルにデータを送信するために必要なユーザー名です。このユーザーにはまた、データレポジトリファイルに対する読み取り / 書き込みアクセスと、レポジトリファイルのディレクトリ（フォルダ）へのアクセスも許可されていなければなりません。
[Password]	レポジトリファイルにデータを送信するために必要なパスワードです。
[File Path]	レポジトリファイルへのパスです。
[Filename]	レポジトリファイル（ASCII テキストファイル形式）のファイル名です。
[Delay X hours between uploads]	レポジトリファイルのデータ更新間隔（単位：時間）です。
[Upload every X minutes]	レポジトリファイルへのデータ更新が正しく行われなかった場合に再試行を行う間隔（単位：分）です。
[Up to X times]	レポジトリファイルへのデータ更新が正しく行われなかった場合に、最初に失敗してから最大で何回再試行を行うかの値です。
[Until Upload Succeeds]	この設定の場合、ファイルの転送が完了するまで再試行が繰り返されます。

データログの容量を調整するには（[Logs] > [Data] > [size]）：

デフォルト設定では、データログは 1000 件までのレコードを格納できます。ログに格納するレコード数は変更できます。データログの容量を変更すると、それまでに記録されていたイベントはすべて削除されます。レコードが失われることがないように、FTP または SCP を使用してログを取得してから、[Data Log Size] フィールドに新しい値を入力してください。

FTP または SCP でログファイルを取得する方法を参照してください。

ログが容量に達すると、古いデータから削除されます。

FTP または SCP でログファイルを取得する方法

管理者またはデバイスユーザーは、FTP または SCP を使用して、タブ区切り形式のイベントログファイル（*event.txt*）またはデータログファイル（*data.txt*）を取得できます。これらは表計算ソフトにインポートできます。

- このファイルには、最後にログを削除した時点以降、あるいは（データログの場合には）ファイル容量に達したためファイルが切り詰められた時点以降に記録されたイベントとデータすべてが含まれます。
- このファイルには、イベントログやデータログでは表示されない次の情報も含まれています。
  - ファイル形式のバージョン（先頭行）
  - ファイルを取得した日時
  - Rack PDU の [Name]、[Contact]、[Location] の値および IP アドレス
  - 各イベント固有の [Event Code]（*event.txt* ファイルのみ）

Rack PDU は、ログエントリに 4 桁の年表記を使用します。4 桁の年表記をすべて表示するには、表計算ソフトで 4 桁の日付形式を選択する必要がある場合もあります。

システムで暗号化ベースのセキュリティプロトコルを使用している場合は、セキュアCoPy（SCP）を介してログファイルを取得します。
システムで暗号化なしの認証方法を使用している場合は、FTP を介してログファイルを取得します。

ニーズに合ったセキュリティタイプを設定するための使用可能なプロトコルと方法については、付録 B: セキュリティハンドブックを参照してください。

SCP でのファイル取得方法 SCP を介して *event. txt* ファイルを取得するには、次のコマンドを使用します。

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

SCP を介して *data. txt* ファイルを取得するには、次のコマンドを使用します。

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

FTP でのファイル取得方法 FTP を介して *event.txt* ファイルまたは *data.txt* ファイルを取得するには、次の操作を行います。

1. コマンドプロンプトから「**ftp**」の文字列と Rack PDU の IP アドレスを入力し、ENTER を押してください。

   [FTP Server] の [Port] 設定(この設定は [Administration] タブの [Network] メニューから行います）がデフォルト値（21）から変更されている場合、FTP コマンドにデフォルト以外の値を指定する必要があります。Windows FTP クライアントの場合は、パラメータをスペースで区切り、次のコマンドを入力します(一部の FTP クライアントでは、IP アドレスとポート番号の間にはスペースではなくコロンを使用する場合があります)。

   ftp>open ip_address port_number

   デフォルト以外のポート値を指定して FTP サーバーのセキュリティを強化する方法については、FTP サーバーを参照してください。5001 ～ 32768 のポートを指定することができます。

2. 管理者またはデバイスユーザーの [User Name] と [Password]（大文字 / 小文字の区別あり）の各欄に入力してログオンします。管理者の場合、**ユーザー名**と**パスワード**のデフォルトは「**admin**」です。デバイスユーザーの場合、**ユーザー名**と**パスワード**のデフォルトは「**device**」です。
3. 「**get**」コマンドを使用してログのテキストファイルをローカルドライブに転送します。

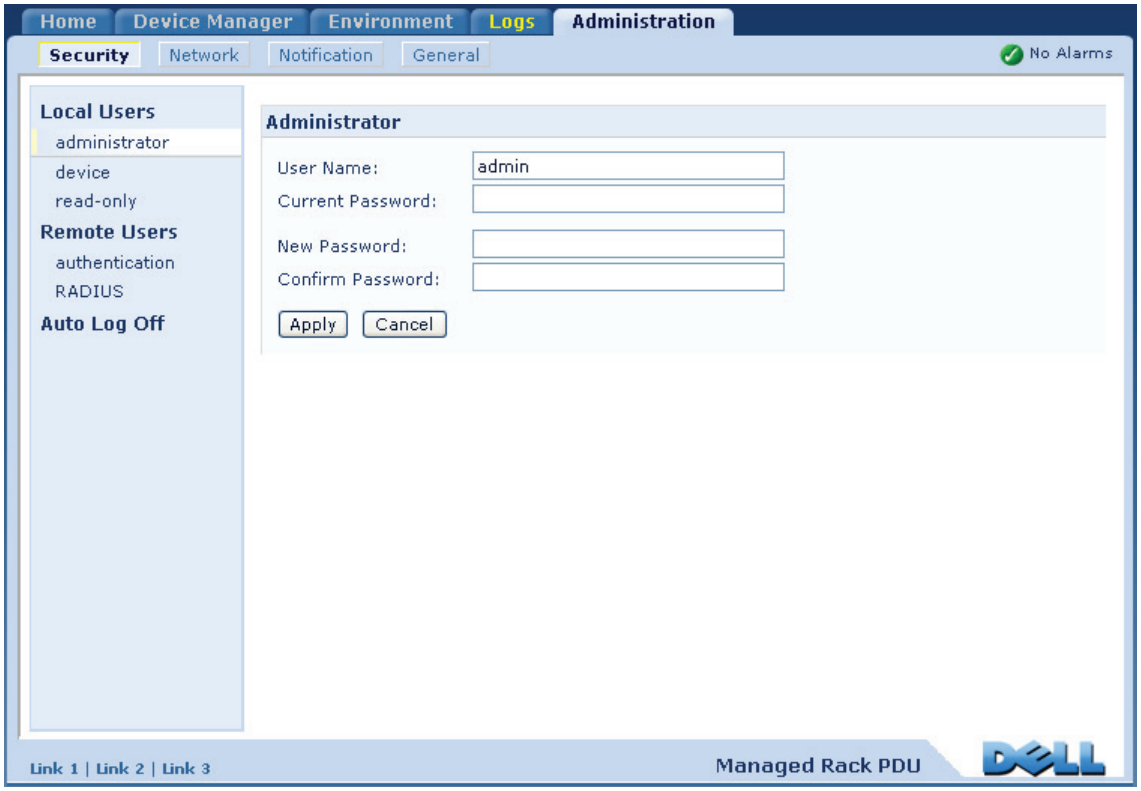
   ftp>get event.txt

   または

   ftp>get data.txt

4. FTP を終了するには、**ftp>** プロンプトで「**quit**」と入力します。

管理：セキュリティ


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
Local Users
administrator
device
read-only
Remote Users
authentication
RADIUS
Auto Log Off
Administrator
User Name:
admin
Current Password:
New Password:
Confirm Password:
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

ローカルユーザー

ユーザーアクセスの設定

選択項目： [Administration] > [Security] > [Local Users] > *オプション*

管理者は Rack PDU に常時アクセスできます。

デバイスユーザーと読み取り専用ユーザーはデフォルト設定では有効になっています。デバイスユーザーと読み取り専用ユーザーを無効にするには、左側ナビゲーションメニューから該当のユーザーアカウントを選択し、[Enable] チェックボックスのチェック印を外します。

各アカウントの種類のユーザー名を、大文字と小文字を区別して同様に設定します。最大文字数は、ユーザー名は 64 文字、パスワードは 64 文字です。パスワード欄を空欄にする（文字を設定しない）ことはできません。

各アカウントタイプに許可される権限については、ユーザーアカウントの種類を参照してください。

コンセントユーザーのアカウントには、デフォルトのユーザー名やパスワードがありません。コンセントユーザーのユーザー名とパスワード、およびアカウントのその他の詳細は、管理者が指定する必要があります。コンセントユーザーの設定を参照してください。

アカウントの種類	デフォルトのユーザー名	デフォルトのパスワード	許可されるアクセス権
管理者	admin	admin	Web インターフェイスとコマンドラインインターフェイス
デバイスユーザー	device	device	
読み取り専用ユーザー	readonly	readonly	Web インターフェイスのみ

リモートユーザー

認証

選択項目：[Administration] > [Security] > [Remote Users] > [Authentication Method]

このオプションを使用して、管理者が Rack PDU にリモートアクセスする方法を選択します。

ローカル認証（一元化された RADIUS サーバの認証を利用しない）については、付録 B: セキュリティハンドブックを参照してください。

Rack PDU は RADIUS（Remote Authentication Dial-In User Service）による認証 / 承認の機能をサポートしています。

- RADIUS が有効になった Rack PDU またはその他のネットワーク対応デバイスにアクセスする場合、認証リクエストは RADIUS サーバーに送信されてユーザーの権限レベルが判断されます。
- Rack PDU で使用される RADIUS ユーザー名は、32 文字以下に制限されています。

次のいずれかを選択します。

- [Local Authentication Only]（ローカル認証のみ）： RADIUS が無効になり、ローカル認証が有効になります。
- [RADIUS, then Local Authentication]（RADIUS、ローカル認証の順）： RADIUS とローカル認証が有効になります。RADIUS サーバーからの認証が最初に要求されます。RADIUS サーバーからの応答がない場合、ローカル認証が使用されます。
- [RADIUS Only]（RADIUS のみ）： RADIUS が有効になり、ローカル認証が無効になります。

[RADIUS Only] を指定すると、RADIUS サーバーが利用できない場合、正しく認識できないかまたは正しく設定されていないリモートアクセスは、ユーザーレベルに関わりなくアクセスできなくなります。この場合には、シリアル接続でコマンドラインインターフェイスにアクセスし、[access] の設定を [local] または [radiusLocal] に変更して再びアクセスできるようにしなければなりません。例えば、アクセス設定を [local] に変更する場合には次のコマンドを使用します。

```
radius -a local
```

RADIUS

選択項目：[Administration] > [Security] > [Remote Users] > [RADIUS]

このオプションでは以下を実行できます。

- Rack PDU で使用できる RADIUS サーバー（2 台まで）と各サーバーのタイムアウト値を表示できます。
- リンクをクリックし、新しい RADIUS サーバーによる認証のパラメータを設定します。
- 一覧内の RADIUS サーバーをクリックすると、そのサーバーのパラメータを表示、変更できます。

RADIUS 設定	説明
[RADIUS Server]	RADIUS サーバーのサーバー名または IP アドレス（IPv4 または IPv6）リンクをクリックしてサーバーを設定します。 **注意**：RADIUS サーバーは、デフォルトでは 1812 番ポートを使用してユーザー認証を行います。別のポートを使用するには、RADIUS サーバー名または IP アドレスの最後にコロンを追加し、その後に新しいポート番号を入力します。
[Secret]	RADIUS サーバーと Rack PDU の間の共有シークレット
[Timeout]	RADIUS サーバーからの応答に対する Rack PDU の待ち時間（秒）
[Test Settings]	管理者のユーザー名とパスワードを入力して、設定した RADIUS サーバーのパスのテストを実行
[Skip Test and Apply]	RADIUS サーバーのパスのテストを省略

RADIUS サーバーの環境設定

環境設定手順の概要

Rack PDU と共に使用するには RADIUS サーバーを設定する必要があります。

Vendor Specific Attributes（VSA）で使用する RADIUS ユーザーファイルの例と、RADIUS サーバーでの辞書ファイルへの入力例に関しては、付録 B: セキュリティハンドブックを参照してください。

1. RADIUS サーバークライアントリスト（ファイル）に Rack PDU の IP アドレスを追加します。
2. Vendor Specific Attributes（VSA）が定義されている場合を除き、ユーザーには Service-Type 属性が設定されていなければなりません。Service-Type 属性が設定されていない場合、ユーザーには読み取り専用アクセスしか許可されません（Web インターフェイスの場合のみ）。

   RADIUS ユーザーファイルについては RADIUS サーバーのマニュアルを、例については付録 B: セキュリティハンドブックをそれぞれ参照してください。

3. RADIUS サーバーから供給される Service-Type 属性のかわりに VSA を使用することもできます。VSA にはディクショナリエントリと RADIUS ユーザーファイルが必要です。辞書ファイルを構成する際は、[ATTRIBUTE] と [VALUE] のキーワードに対する名前は指定しますが、数値の設定は行いません。数値を変更すると、RADIUS での認証と承認は正しく実行されなくなります。VSAs は、標準の RADIUS 属性より優先されます。

UNIX® でシャドウパスワードを使用して RADIUS サーバーを環境設定

UNIX のシャドウパスワードファイル（/etc/passwd）を RADIUS の辞書ファイルと併用する場合、ユーザー認証には下記の 2 種類の方法を使用できます。

- すべての UNIX ユーザーに管理者権限が付与する場合、RADIUS の「ユーザー」ファイルに以下を追加します。デバイスユーザーのみを許可する場合は、DELL-Service-Type を **[Device]** に変更してください。

```
DEFAULT      Auth-Type = System
             DELL-Service-Type = Admin
```

- RADIUS の「user」ファイルにユーザー名と属性を加え、「/etc/passwd」に対してこのパスワードを確認します。以下はユーザー名「**bconners**」と「**thawk**」での例です。

```
bconners     Auth-Type = System
             DELL-Service-Type = Admin
thawk        Auth-Type = System
             DELL-Service-Type = Device
```

サポート対象の RADIUS サーバー

FreeRADIUS および Microsoft IAS 2003 をサポートしています。その他の RADIUS アプリケーションについては、検証を行っておりません。

操作がない場合のタイムアウト

選択項目：[Administration] > [Security] > [Auto Log Off]

このオプションでは、アクティビティがない場合にそのユーザーをログオフするまでの待機時間（デフォルトでは 3 分です）を設定します。この値を変更した場合、変更内容を適用するにはログオフする必要があります。

ブラウザウィンドウの右上部にある [Log Off] をクリックしてログオフせずにブラウザを閉じると、ブラウザは閉じてもタイマは作動したままの状態になります。そのためユーザーがまだログオンしているものと見なされ、[Minutes of Inactivity] に指定された時間が経過するまでは誰もログオンできなくなります。たとえば、[Minutes of Inactivity] がデフォルト値のままの場合、ユーザーが適切にログオフせずにブラウザウィンドウを閉じると、その後 3 分間はいずれのユーザーもログオンできません。

管理： 通知


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
Event Actions
by event
by group
E-mail
server
recipients
test
SNMP Traps
trap receivers
test
Event Actions for Individual Events
To list all events in a main category by severity level, click the main category name. To list all events in a sub-category by severity level, click the sub-category name.
Device
Communications
Device
Phase Load
Outlet Load
Outlet Control
Sensor
System
Mass Configuration
Security
Link 1 | Link 2 | Link 3
Managed Rack PDU

イベントアクション

選択項目：[Administration] > [Notification] > [Event Actions] > *オプション*

通知の種類

イベントアクションは、単独のイベントまたはイベントグループに対して発生するよう設定できます。これらのイベントアクションが発生した場合、当該イベントのユーザーには次の任意の方法で通知できます。

- 能動的な自動通知。通知は、事前設定されたユーザーまたは監視デバイスに直接送信されます。
  - 電子メール通知
  - SNMP トラップ
  - システムログ通知
- 間接的な通知
  - イベントログ。直接の通知方法を設定しない場合は、発生したイベントを識別できるよう、必ずログを有効にしなければなりません。

    また、システム性能データをログ記録してデバイス監視に使用することもできます。このデータログオプションの設定と使用については、データログを参照してください。
  - クエリ（SNMP GET）

    詳細については SNMP を参照してください。SNMP では、NMS が有効になり情報のクエリが実行されるようになります。データ送信の前に暗号化を行わない SNMPv1 を使用する場合、制限度が最も高い SNMP アクセスタイプ（READ）を選択することにより、リモート設定が改変されるリスクを負わずに情報クエリを実行できるようになります。

イベントアクションの設定

通知に関するパラメータ イベントを消去できるオプションのあるイベントの場合、イベントを単独であるいはグループで設定する際に、これからの 2 つのセクションの記載に従って下記のパラメータも設定できます。パラメータにアクセスするには、該当のレシーバまたは受信者名をクリックします。

パラメータ	説明
[Delay *x* time before sending]	イベントが発生し、ここで指定する期間を過ぎてもその状態が続いている場合、通知が送信されます。指定した期間内にイベントが収まった場合、通知は行われません。
[Repeat at an interval of *x* time]	通知はここで指定する間隔で（例：2 分おき）送信されます。
[Up to *x* times]	発生中のイベントがある間、通知はここで指定する回数だけ繰り返されます。
[Until condition clears]	通知は、イベント状態が収まるかまたは解消されるまで繰り返し送信されます。

イベントごとの設定 イベントアクションをイベントごとに設定する場合、下記の手順で行います。

1. [Administration] タブ、上部メニューバーの [Notification]、および左側ナビゲーションメニューの [Event Actions] の下の [by event] の順に選択します。
2. イベントの一覧で印のついているコラムを点検し、設定しようとしているアクションがすでに設定済みかを確認してください。（デフォルトでは全イベントに対してログ記録が設定されています。）

3. 既存の設定を表示または変更するには（例：受信者に電子メールまたはポケットベルで通知する、Network Management Systems（NMS）に SNMP トラップで通知する）、該当のイベント名をクリックしてください。

システムログサーバーを設定していないと、システムログ設定に関連する事項は表示されません。

イベント設定の詳細を参照しているときには、設定の変更、イベントログやシステムログの有効 / 無効、特定の電子メール受信者やトラップレシーバへの通知の無効は実行できますが、受信者またはレシーバを追加 / 削除することはできません。受信者またはレシーバを追加 / 削除したい場合は下記を参照してください。

- システムログサーバーの識別
- 電子メールの受信者
- トラップレシーバ

グループ別の設定 イベントグループを同時に設定する場合、下記の手順で行います。

1. [Administration] タブ、上部メニューバーの [Notification]、左側ナビゲーションメニューの [Event Actions]、その下の [by group] を順に選択します。
2. 設定を適用するイベントをどのグループに分類するかを選びます。
   - [Grouped by severity] を選択し、いくつかの重要度レベルの中の該当する（1つまたは複数の）レベルのイベントをすべて選択します。イベントの重要度は変更できません。
   - [Grouped by category] を選択し、事前に定義されたカテゴリのうち該当する（単独または複数の）カテゴリのイベントをすべて選択します。

3. [Next >>] をクリックし、ページ間を移動して以下を設定します。
   a. イベントグループに対するイベントアクションを選択します。
   - [Logging]（デフォルト）以外のアクションを選ぶには、関連する受信者またはレシーバが少なくとも 1 人（1 つ）事前に設定されていなければなりません。
   - システムログサーバーを設定してあり [Logging] を選んだ場合は、次のページで [Event Log] または [Syslog]（あるいは両方）を選択してください。

   b. 新しく設定したイベントアクションをこのイベントグループに対して有効にするか、それともアクションを無効にするかを選択します。

能動的、自動、直接の通知

電子メール通知

セットアップの概要 イベント発生時に SMTP を使用して電子メールを最大 4 人の受信者に送信することができます。

電子メール機能を使用するには、次の項目を設定する必要があります。

- プライマリ DNS サーバー（ドメイン名システムサーバー）の、また必要であればセカンダリ DNS サーバーの IP アドレス

DNS を参照してください。

- [SMTP Server] と [From Address] の IP アドレスまたは DNS 名

SMTP を参照してください。

- 最高 4 人までの受信者の電子メールアドレス

電子メールの受信者を参照してください。

[recipients] オプションの [To Address] 設定を使用すると、テキストベースのポケットベルに電子メールを送信できます。

SMTP

選択項目: [Administration] > [Notification] > [Notification] > [server]

設定	説明
[Local SMTP Server]	ローカル SMTP サーバーの IPv4/IPv6 アドレスまたは DNS 名です。 **注意：** この設定は、**[SMTP Server]** に **[Local]** を指定している場合にのみ必要です。電子メールの受信者を参照してください。
[From Address]	Rack PDU が送信する電子メールメッセージの **[From]** フィールドの内容です。 ・「*user@ IP_address*」（**[Local SMTP Server]** に IP アドレスが指定されている場合） ・「*user@domain*（DNS サーバーが指定されており、**[Local SMTP Server]** に DNS 名が設定されている場合） **注意：** ローカル SMTP サーバー上に有効なユーザーアカウントを所有していないと、サーバーの環境設定を行えない場合もあります。サーバーのマニュアルを参照してください。

電子メールの受信者

選択項目：[Administration] > [Notification] > [E-mail] >[recipients]

4 人までの電子メール受信者を設定できます。

設定	説明
[To Address]	受信者のユーザー名およびドメイン名です。ポケットベルに電子メールを送信するには、その受信者のポケットベル用ゲートウェイのアカウントアドレスを指定してください（例：**myacct100@skytel.com**）。ポケットベル用ゲートウェイがメッセージを生成します。 メールサーバーの IP アドレスの DNS 参照を回避するには、角括弧内に電子メールドメイン名ではなく、IP アドレスを指定します。たとえば、jsmith@company.com の代わりに、jsmith@[xxx.xxx.x.xxx] と指定します。これは DNS を正しく参照できない場合に便利です。 **注意：** 受信者のポケットベルは文字ベースのメッセージ交換に対応している必要があります。

設定	説明
[E-mail Generation]	受信者への電子メール送信を有効（デフォルト）または無効にします。
[SMTP Server]	電子メールのルーティングを行うために、次のいずれかの方法を選択します。 ·[Local]: Rack PDU の SMTP サーバーを使用します（推奨）。この設定では、電子メールは Rack PDU の 20 秒のタイムアウト前に送信され、必要な場合は何度か送信を再試行します。また次のいずれかも設定してください。 ·電子メールを外部の SMTP サーバーにルーティングできるように、Rack PDU の SMTP サーバで転送機能を有効にします。通常、SMTP サーバーは電子メールを転送するようには設定されていません。転送機能を有効にする前に、SMTP サーバーの管理者に相談してください。 ·外部メールアカウントに電子メールを転送するために、Rack PDU 用の電子メールアカウントを設定します。 ·[Recipient]: 電子メールを受信者の SMTP サーバーに直接送信します。この設定では、Rack PDU は電子メールの送信を 1 度しか試行しません。トラフィックの多いリモートの SMTP サーバーの場合、タイムアウトのために一部の電子メールが一度も発信されない結果となることがあります。 受信者が Rack PDU の SMTP サーバーを使用している場合、この設定を行っても何も影響はありません。
[Format]	長い形式では、名前、場所、連絡先、IP アドレス、デバイスのシリアル番号、日付と時刻、イベントコード、イベントの説明が含まれます。短い形式の場合はイベントの説明のみです。
[User Name Password Confirm Password]	ご使用のメールサーバーで認証が必要な場合は、ユーザー名とパスワードを入力してください。これは単純な認証で SSI ではありません。

電子メールテスト

選択項目：[Administration] > [Notification] > [E-mail] > [test]

設定した受信者にテストメールを送信します。

SNMP トラップ

トラップレシーバ

選択項目：[Administration] > [Notification] > [SNMP Traps] > [trap receivers]

NMS IP/ホスト名別にトラップレシーバを表示できます。トラップレシーバは 6 つまで設定できます。

- トラップレシーバを新たに設定するには、[Add Trap Receiver] をクリックします。
- トラップレシーバを変更または削除するには、まず IP アドレスまたはホスト名をクリックして設定にアクセスします。（トラップレシーバを削除すると、削除したトラップレシーバのイベントアクション下で設定されていた通知設定はすべてデフォルト設定に戻ります。）
- トラップレシーバにトラップの種類を指定するには、SNMPv1 または SNMPv3 のオプションボタンを選択します。NMS で両方のトラップを受信できるようにするには、2 つのトラップレシーバをこの NMS 用に（トラップのそれぞれの種類ごとに）設定する必要があります。

項目	説明
[Trap Generation]	このトラップレシーバに対するトラップの生成を有効（デフォルト）または無効にします。
[NMS IP/Host Name]	このトラップレシーバの IPv4/IPv6 アドレスまたはホスト名です。デフォルト値は 0.0.0.0 で、この場合トラップレシーバは未定義のままです。

SNMPv1 オプション

項目	説明
Community Name	SNMPv1 トラップの場合、識別子として名前（デフォルトでは「**public**」）がこのトラップレシーバに送信されます。
Authenticate Traps	このオプションが有効（デフォルト）になっていると、[NMS IP/Host Name] により識別された NMS は認証トラップ（このデバイスへの不正なログオンの試みに対して生成されるトラップ）を受信します。この機能を無効にする場合は、チェックボックスのチェック印を外してください。

SNMPv3 オプション このトラップレシーバに対するユーザープロファイルの識別子を選択します。（ここで指定するユーザー名で識別されるユーザープロファイルの設定を表示するには、上部メニューバーの [Network]、左側ナビゲーションメニューの [SNMPv3]、その下の [user profiles] を順に選択します。）

ユーザープロファイルの作成および認証 / 暗号化方式の選択については、SNMPv3 を参照してください。

SNMP トラップテスト

選択項目：[Administration] > [Notification] > [SNMP Traps] > [test]

[Last Test Result] もっとも最近に行われた SNMP トラップテストの結果です。SNMP トラップテストが正しく実行されても、確認できるのはトラップが送信されたことのみで、指定されたトラップレシーバが受信したかどうかは確認できません。トラップテストが成功するには、以下のすべての条件が満たされなければなりません。

- 指定されたトラップレシーバに対し設定されている SNMP バージョン（SNMPv1 または SNMPv3）がこのデバイスで有効になっている。
- トラップレシーバが有効になっている。
- [To] アドレス欄にホスト名が指定されている場合、そのホスト名は有効な IP アドレスにマッピング可能である。

[To] テスト用の SNMP トラップの送信先となる IP アドレスまたはホスト名を選びます。トラップレシーバが何も設定されていない場合、[Trap Receiver] 設定ページへのリンクが表示されます。

システムログ

選択項目：[Logs] > [Syslog] > *オプション*

Rack PDU では、イベントが発生したときに最大 4 大のシステムログサーバーにメッセージを送信できます。システムログサーバーはネットワークデバイスで発生したイベントをログ記録し、イベントの統合的な記録を提供します。

このユーザーガイドでは、システムログまたはシステムログの設定について詳細説明を行っていません。システムログの詳細については、「RFC3164」を参照してください。

システムログサーバーの識別

選択項目：[Logs] > [Syslog] > [servers]

設定	説明
Syslog Server	IPv4/IPv6 アドレスまたはホスト名を使用して、Rack PDU から送信される Syslog メッセージを受信する 4 つまでのサーバーを識別します。
Port	Rack PDU がシステムログメッセージの送信に使用する User Datagram Protocol (UDP) ポートです。デフォルト値は 514 です。これはシステムログに割り当てられた UDP ポート番号です。
Protocol	システムログメッセージを表示する言語を選択します。

システムログ設定

選択項目：[Logs] > [Syslog] > [settings]

設定	説明
Message Generation	システムログ機能を有効（デフォルト）または無効にします。
Facility Code	Rack PDU のシステムログメッセージに割り当てる機能コード（デフォルトは「User」）を選択します。 **注意**：Rack PDU が送信したシステムログメッセージを定義するには、「User」を選択することをお勧めします。システムログネットワークまたはシステム管理者からの指示がある場合を除き、この設定は**変更しないでください**。
Severity Mapping	システムログの優先度を有効にして、Rack PDU または環境イベントのそれぞれの重要度をマッピングします。このマッピングを変更する必要はありません。 RFC3164 では、次のように定義されています。 ・[Emergency]（緊急）：システムを利用できません。 ・[Alert]（警告）：即座に対処する必要があります。 ・[Critical]（致命的）：重大な障害があります。 ・[Error]（エラー）：エラーが発生しています。 ・[Warning]（警告）：警告状態が発生しています。 ・[Notice]（注）：通常の状態ですが、多少の問題があります。 ・[Informational]（情報）：情報メッセージです。 ・[Debug]（デバッグ）：デバッグレベルのメッセージです。 以下は、[Local Priority] 設定に割り当てられるデフォルト値です。 ・[Severe]（致命的）は [Critical]（致命的）に関連付けられます。 ・[Warning]（警告）は [Warning]（警告）に関連付けられます。 ・[Informational]（情報）は [Info]（情報）に関連付けられます。 **注意**：システムログメッセージを無効にする場合は、イベントアクションの設定を参照してください。

システムログのテストと形式の例

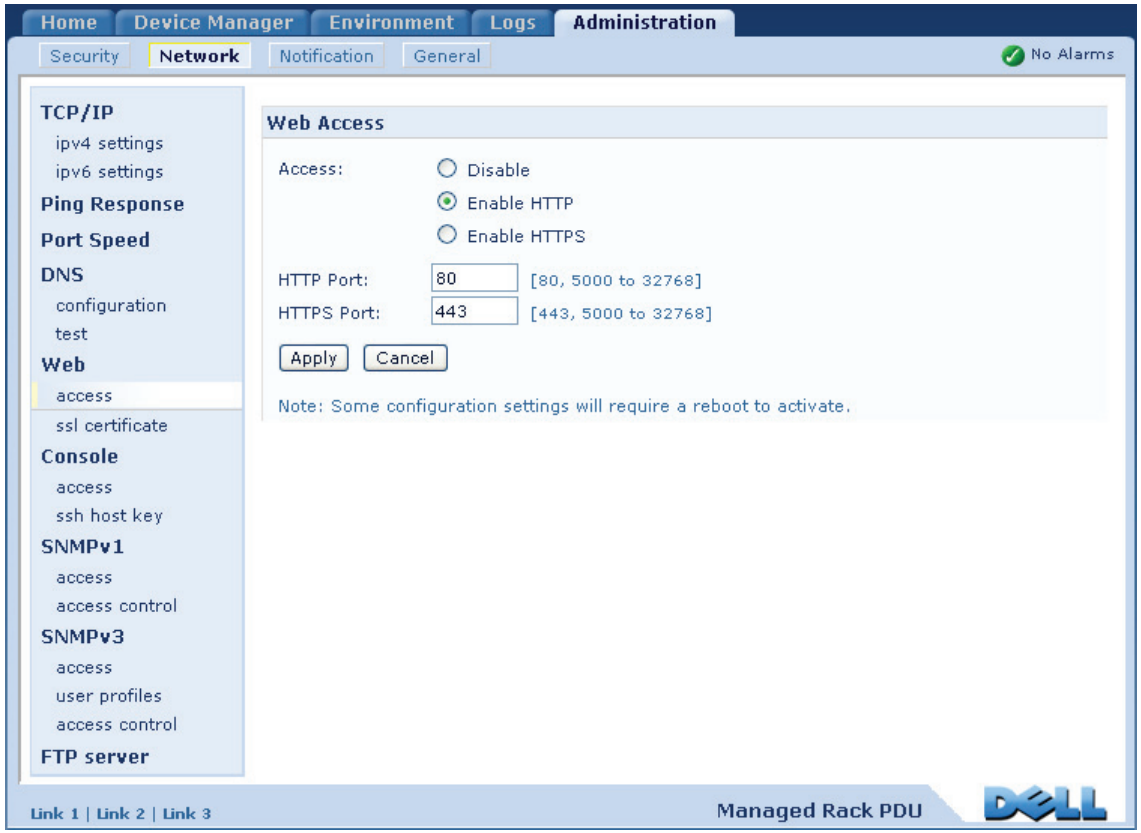
選択項目：[Logs] > [Syslog] > [test]

[servers] オプションで設定したシステムログサーバーにテストメッセージを送信します。

1. テストメッセージに指定する重大度を選択します。
2. 必要なメッセージフィールドに応じて、テストメッセージを定義します。
   - 優先度（PRI）：メッセージのイベントと、Rack PDU が送信するメッセージの機能コードに割り当てるシステムログ優先度。
   - ヘッダ：タイムスタンプと Rack PDU の IP アドレス。
   - メッセージ（MSG）部分：
     - イベントタイプは、[TAG] フィールド、コロン、スペースの形式で指定します。
     - [CONTENT] フィールドは、イベントテキスト、（任意で）1 スペース、イベントコードの形式で指定します。

       例えば、**Dell: Test Syslog** は有効な形式です。

管理：ネットワーク機能


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
TCP/IP
ipv4 settings
ipv6 settings
Ping Response
Port Speed
DNS
configuration
test
Web
access
ssl certificate
Console
access
ssh host key
SNMPv1
access
access control
SNMPv3
access
user profiles
access control
FTP server
Web Access
Access:
Disable
Enable HTTP
Enable HTTPS
HTTP Port:
80
[80, 5000 to 32768]
HTTPS Port:
443
[443, 5000 to 32768]
Apply
Cancel
Note: Some configuration settings will require a reboot to activate.
Link 1 | Link 2 | Link 3
Managed Rack PDU

TCP/IP 設定と通信設定

TCP/IP 設定

選択項目：[Administration] > [Network] > [TCP/IP]

上部メニューバーの [Network] を選択すると、左側ナビゲーションメニューで [TCP/IP] オプションがデフォルトで選択され、Rack PDU のその時点での IPv4 アドレス、サブネットマスク、デフォルトゲートウェイ、MAC アドレス、ブートモードが表示されます。

DHCP と DHCP のオプションについては、「RFC2131」および「RFC2132」を参照してください。

設定	説明
Enable	このチェックボックスで、IPv4 を有効または無効にします。
Manual	IP アドレス、サブネットマスク、デフォルトゲートウェイを入力して IPv4 を手動で設定します。

1. 通常、これらの設定ページでは次の 3 つの設定値は変更不要です。
   - [Vendor Class]（ベンダークラス）：DELL
   - [Client ID]（クライアント ID）：Rack PDU の MAC アドレス（ローカルエリアネットワーク（LAN）上での固有の ID）です。
   - [User Class]（ユーザークラス）：アプリケーションファームウェアモジュールの名前です。

設定	説明
BOOTP	BOOTP サーバーが TCP/IP 設定を供給します。32 秒間隔で、Rack PDU は BOOTP サーバーからのネットワーク割り当てを要求します。 ・有効なレスポンスを受信すると、Rack PDU はネットワークサービスを開始します。 ・Rack PDU で BOOTP サーバーを検出したがそのサーバーへの要求に失敗した場合、または要求がタイムアウトになった場合は、Rack PDU はネットワーク設定要求を停止し、再起動されるまで停止したままとなります。 ・デフォルトでは、以前のネットワーク設定が存在しており、5 回の要求（最初の要求とその 4 回の再試行）に対して Rack PDU が有効なレスポンスを受信しなかった場合は、以前のネットワーク設定が使用され、アクセス可能な状態が保たれます。 [Next >>] をクリックすると [BOOTP Configuration] ページにアクセスでき、ここから再試行回数および再試行が失敗した場合の措置を設定できます[1]。 ・[Maximum retries]（最大試行回数）：有効な応答が得られない場合の再試行の回数を指定します。無制限に試行を繰り返すようにするにはゼロ（0）を入力します。 ・[If retries fail]（再試行に失敗した場合）：[Use prior settings]（前回の設定を適用）（デフォルト）または [Stop BOOTP request]（BOOTP リクエストを停止）のいずれかを指定します。
DHCP	デフォルトではこの設定になっています。32 秒間隔で、Rack PDU は DHCP サーバーからのネットワーク割り当てを要求します。 ・有効な応答が得られた場合、Rack PDU ではリースを受け入れてネットワークサービスを開始するために DHCP サーバーからのベンダー cookie は必要ありません。 ・Rack PDU で DHCP サーバーを検出できてもこのサーバーへのリクエストに対して応答が得られないかまたはタイムアウトとなった場合は、再起動するまでネットワーク設定のリクエストを行わなくなります。[1] ・[Require vendor specific cookie to accept DHCP Address]（DHCP アドレスを有効とするにはベンダー固有の cookie が必要）：このチェックボックスを選択すると、DHCP サーバーに cookie を提供するよう要求して Rack PDU に情報を供給することができます。

1. 通常、これらの設定ページでは次の 3 つの設定値は変更不要です。
   ・[Vendor Class]（ベンダークラス）：DELL
   ・[Client ID]（クライアント ID）：Rack PDU の MAC アドレス（ローカルエリアネットワーク（LAN）上での固有の ID）です。
   ・[User Class]（ユーザークラス）：アプリケーションファームウェアモジュールの名前です。

DHCP 応答オプション

それぞれの有効な DHCP レスポンスのオプションは、ネットワークで稼動するために Rack PDU が必要とする TCP/IP 値を提供したり、Rack PDU の動作に影響する情報を提供します。

ベンダー固有の情報（オプション 43） Rack PDU では、DHCP からの応答が有効であるかを判断するために、DHCP からの応答にあるこのオプション（オプション 43）を使用します。このオプションには、TAG/LEN/DATA 形式でベンダー Cookie に挿入される固有のオプションが含まれます。これはデフォルトでは無効になっています。

- **Vendor Cookie. Tag 1, Len 4, Data “1APC”**
  オプション 43 は、DHCP サーバーが Dell Rack PDU にサービスを提供するよう設定されていることを Rack PDU に通知します。
  次の例では、Vendor Cookie を含んだベンダー固有の情報オプションを 16 進数の形式で指定しています。

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

TCP/IP オプション Rack PDU は、有効な DHCP レスポンスの中にある次のオプションを使用して TCP/IP を設定します。これらのオプションは、最初のオプション以外はすべて「RFC2132」で説明されています。

- **IP アドレス**（DHCP 応答の [yiaddr] フィールド値。「RFC2131」で説明されています）：DHCP サーバが Rack PDU にリースしている IP アドレスです。
- **サブネットマスク**（オプション 1）：Rack PDU がネットワークで稼動するために必要なサブネットマスクの値です。
- **ルーター**、すなわちデフォルトゲートウェイ（オプション 3）：Rack PDU がネットワークで稼動するために必要なデフォルトゲートウェイアドレスです。
- **IP アドレスのリース期間**（オプション 51）：Rack PDU への IP アドレスのリース期間です。
- **更新時間、T1**（オプション 58）：IP アドレスリースの割り当て後、このリースの更新を要求するまでの Rack PDU の待ち時間です。
- **再バインド時間、T2**（オプション 59）：IP アドレスリースの割り当て後、このリースの再バインドを要求するまでの Rack PDU の待ち時間です。

その他のオプション Rack PDU は、有効な DHCP レスポンス内でもこれらのオプションを使用します。これらのオプションは、最後のオプション以外はすべて「RFC2132」で説明されています。

- **ネットワーク時間プロトコルサーバー**（オプション 42）：Rack PDU で使用される 2 つまでの NTP サーバ（プライマリサーバとセカンダリサーバ）です。
- **時間オフセット**（オプション 2）：Rack PDU サブネットの、協定世界時（UTC）からのオフセット値です。
- **ドメイン名サーバー**（オプション 6）：Rack PDU が使用できる 2 個までのドメイン名システム（DNS）サーバー（プライマリおよびセカンダリ）です。
- **ホスト名**（オプション 12）：Rack PDU が使用するホスト名（最長 32 文字）です。
- **ドメイン名**（オプション 15）：Rack PDU が使用するドメイン名（最長 64 文字）です。
- **ブートファイル名**（DHCP 応答の [file] フィールド値、「RFC2131」で説明されています）：ダウンロード用のユーザー環境設定ファイル（.ini file）への完全なディレクトリパスです。DHCP 応答の [siaddr] フィールドによりサーバの IP アドレスが指定されます。Rack PDU はこのサーバから .ini ファイルをダウンロードします。ダウンロードが完了すると、Rack PDU は .ini ファイルをブートファイルとして使用し、再設定を行います。

選択項目：[Administration] > [Network] > [TCP/IP] > [IPv6 settings]

設定	説明
Enable	このチェックボックスで、IPv6 を有効または無効にします。
Manual	IP アドレスとデフォルトゲートウェイを入力して IPv6 を手動で設定します。
Auto Configuration	[Auto Configuration] チェックボックスを選択すると、システムはルーター（使用できる場合）からアドレスプリフィックスを取得します。このプリフィックスを使用して、IPv6 のアドレスを自動的に設定します。

設定	説明
DHCPv6 Mode	[Router Controlled]: このオプションを選択すると、受信した IPv6 ルーター広告に含まれる M フラグ（Managed Flag）と O フラグ（Other Flag）で DHCPv6 を制御します。ルーター広告を受信すると、NMC で M フラグと O フラグのどちらが設定されているかを確認します。NMC では、M（管理アドレス設定フラグ）と O（その他のステートフル設定フラグ）の「ビット」の状態を次のように解釈します。 ・*どちらも設定されていない*: ローカルネットワークには DHCPv6 インフラストラクチャがないことを示します。NMC はルーター広告と手動設定を使用して、ローカルや他の設定にリンクしていないアドレスを取得します。 ・*M、または M と O が設定されている*: この場合は、完全な DHCPv6 アドレス設定が行われます。DHCPv6 を使用して、アドレスおよび他の設定を取得します。これは DHCPv6 がステートフルであると呼ばれます。M フラグを受信すると、問題のインターフェイスが閉じるまで DHCPv6 アドレスの設定が効果をもち続けます。M フラグが設定されていないルーター広告パケットを連続で受信した場合も同様です。 最初に O フラグを受信し続いて M フラグを受信した場合は、NMC は M フラグを受信してから完全アドレス設定を実行します。 ・*O のみ設定されている*: この場合は、NMC が DHCPv6 情報要求パケットを送信しています。DHCPv6 を使用して、「他の」設定（DNS サーバーの場所など）が実行されますが、アドレスは提供されません。これは DHCPv6 がステートレスであると呼ばれます。 [Address and Other Information]: このラジオボタンを選択すると、DHCPv6 を使用してアドレスおよびその他の設定が取得されます。これは DHCPv6 がステートフルであると呼ばれます。 [Non-Address Information Only]: このラジオボタンを選択すると、DHCPv6 を使用して、「他の」設定（DNS サーバーの場所など）が実行されますが、アドレスは提供されません。これは DHCPv6 がステートレスであると呼ばれます。 [Never]: これを選択すると、DHCPv6 は無効になります。

Ping 応答

選択項目：[Administration] > [Network] > [Ping Response]

[IPv4 Ping Response] で [Enable] チェックボックスを選択すると、Network Management Card でネットワークの Ping に応答できます。このチェックボックスを選択解除すると、NMC の応答は無効になります。この設定は IPv6 には適用されません。

ポート速度

選択項目：[Administration] > [Network] > [Port Speed]

[Port Speed] 設定では TCP/IP ポートの通信速度を設定します。

- [Auto-negotiation]（オートネゴシエーション）（デフォルト）の場合、イーサネットデバイスは可能なかぎり速い速度で通信するようネゴシエートしますが、2 台のデバイスのサポート速度が一致しない場合は遅い方の速度が使用されます。
- また 10 Mbps または 100 Mbps を選択することもできます。どちらの場合でも、半二重（一度に一方向のみの通信）または全二重（同じチャンネルで一度に双方向の通信）のオプションを利用できます。

DNS

選択項目：[Administration] > [Network] > [DNS] > *オプション*

[DNS] オプションを使用して、Domain Name System（DNS）の設定とテストを行います。

- [Primary DNS Server] または [Secondary DNS Server] を選択して、プライマリおよびオプションのセカンダリ DNS サーバーの IPv4/IPv6 アドレスを指定します。Rack PDU で電子メールを送信できるようにするには、少なくともプライマリ DNS サーバーの IP アドレスを指定する必要があります。
  - Rack PDU は最大 15 秒間、プライマリ DNS サーバーまたはセカンダリ DNS サーバー（セカンダリ DNS サーバーを指定した場合）の応答を待ちます。この時間内に Rack PDU が応答を受信できなかった場合、電子メールを送信することができません。したがって、DNS サーバーは Rack PDU と同じセグメント内または最寄りのセグメントに配置してください（WAN は経由できません）。
  - DNS サーバーの IP アドレスを指定したら、そのサーバーの IP アドレスを調べるために、ネットワーク上のコンピュータに DNS 名を入力して該当の DNS が稼動していることを確認します。
- [Host Name]：管理者がこのフィールドにホスト名を、そして [Domain Name] フィールドにドメイン名を指定してある場合、ユーザーは、ドメイン名を受け入れる Rack PDU インターフェイスのいずれのフィールド（電子メールアドレスを除く）にもホスト名を入力することができます。
- [Domain Name (IPv4)]：管理者がドメイン名を設定する必要があるのはここのみです。ドメイン名を受け入れる Rack PDU インターフェイス（電子メールアドレスを除く）の他の全部のフィールドに、ホスト名のみが入力されているときは、Rack PDU によってドメイン名が追加されます。
  - 特定のホスト名を入力した場合にドメイン名が追加されるのを無効にしたい場合は、ドメイン名フィールドをデフォルトの「somedomain.com」か、または「0.0.0.0」に設定します。

- 特定のホスト名を入力した場合（トラップレシーバの設定時など）の拡張を無効にする場合は、後に続くピリオドを含めて指定します。Rack PDU はピリオドが後続するホスト名（例：「*mySnmpServer.*」）を完全修飾ドメイン名と同じように認識しますのドメイン名を追加しません。

・[Domain Name (IPv6)]: ここで IPv6 のドメイン名を指定します。

・[test] を選択すると、DNS サーバーの設定をテストする DNS クエリを送信します。

- [Query Type] では、DNS クエリに使用する方式を選択します。
  - ・[by Host]: サーバーの URL 名
  - ・[by FQDN]: 完全修飾ドメイン名
  - ・[by IP]: サーバーの IP アドレス
  - ・[by MX]: サーバーが使用する Mail Exchange
- [Query Question]（クエリ質問）設定を使用して、選択したクエリの種類に使用する値を指定します。

選択されたクエリタイプ	使用するクエリ質問
[by Host]	URL
[by FQDN]	完全修飾ドメイン名（*my_server.my_domain*）
[by IP]	IP アドレス
[by MX]	Mail Exchange アドレス

- DNS リクエストのテストの結果は [Last Query Response]（前回のクエリ応答）に表示されます。

Web

選択項目： [Administration] > [Network] > [Web] > *オプション*

オプション	説明

[access]	下記のいずれかのオプションに対する変更を有効にするには Rack PDU からログオフする必要があります。
	・[Disable]: Web インターフェイスへのアクセスを無効にします。（アクセスを再び有効にするには、コマンドラインインターフェイスにログオンし、「**http -S enable**」のコマンドをタイプします。HTTPS へのアクセスの場合、「**https -S enable**」とタイプしてください。）
	・[Enable HTTP]（デフォルト）: Hypertext Transfer Protocol（HTTP）を有効にします。HTTP はユーザー名とパスワードを使用したアクセスを提供しますが、通信中にはユーザー名、パスワード、データの暗号化を行いません。
	・[Enable HTTPS]: Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）を有効にします。SSL により、送信中にユーザ名、パスワード、データが暗号化され、デジタル証明書を使用して Rack PDU が認証されます。HTTPS が有効になっている間は、ブラウザに小さな錠前のアイコンが表示されます。
	
	デジタル証明書を使用する際に複数の種類から選択する方法については、付録 B: セキュリティハンドブックの「デジタル証明書の作成とインストール」を参照してください。
	
	[HTTP Port]: Rack PDU との HTTP による通信に使用される TCP/IP ポート（デフォルト値は 80）です。
	
	[HTTPS Port]: Rack PDU との HTTPS による通信に使用される TCP/IP ポート（デフォルト値は 443）です。
	
	HTTP または HTTPS のいずれの場合でも、5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。この場合、ブラウザのアドレス欄にコロン（:）を入力してからポート番号を指定する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合は次のように入力します。
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

オプション	説明
[ssl certificate]	セキュリティ証明書を追加、差し替え、または削除します。 [Status]: ・[Not installed]: 証明書はインストールされていません、または FTP か SCP によって間違った場所にインストールされています。[Add or Replace Certificate File] を使用することで、証明書を Rack PDU の正しい場所（/ssl ）にインストールできます。 ・[Generating]: 有効な証明書が検出されなかったため、Rack PDU は証明書を生成中です。 ・[Loading] : Rack PDU で証明書を有効にする処理が進行中です。 ・[Valid certificate]: Rack PDU で有効な証明書がインストール、または生成されました。証明書の内容を表示するには、このリンクをクリックします。 **無効な証明書をインストールしてしまった場合、または SSL を有効にした時点で証明書がインストールされていなかった場合は、Rack PDU はデフォルトの証明書を生成します。このプロセスにより、インターフェイスにアクセスできるまでに 1 分ほどの遅延が生じます。**デフォルトの証明書では基本的な暗号化ベースのセキュリティレベルになります。この証明書を使用してログオンできますが、ログオン時にセキュリティアラートメッセージが表示されます。 [Add or Replace Certificate File]: Security Wizard で作成した証明書ファイルを入力するか、またはそのファイルの場所まで移動します。 Security Wizard で作成したデジタル証明書、または Rack PDU で生成されたデジタル証明書の使用方法の選択については、付録 B: セキュリティハンドブックの「デジタル証明書の作成とインストール」を参照してください。 [Remove]: 既存の証明書を削除します。

コンソール

選択項目：[Administration] > [Network] > [Console] > *オプション*

オプション	説明

[access]	Telnet または Secure Shell（SSH）へのアクセス方法を下記の中から 1 つ選びます。
	・[Disable]：コマンドラインインターフェイスへのアクセスをすべて無効にします。
	・[Enable Telnet]（デフォルト）：Telnet ではユーザー名、パスワード、データは暗号化せずに送信されます。
	・[Enable SSH]：SSH ではユーザー名、パスワード、データは暗号化して送信され、送信中のデータの傍受、偽造、改変の試みから保護されます。
	
	次のプロトコルで使用するようポートを設定します。
	・[Telnet Port]：Rack PDU との通信に使用される Telnet ポート（デフォルトでは 23）です。5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。ユーザーは、デフォルト以外のポートを指定する場合、コロンまたはスペース（Telnet クライアントにより異なります）を次に入力する必要があります。たとえば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合、Telnet クライアントでは次のいずれかのコマンドを入力する必要があります。
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	・[SSH Port]：Rack PDU との通信に使用される SSH ポート（デフォルトでは 23）です。5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。デフォルト以外のポート番号を指定する場合に必要となるコマンドライン形式の詳細については、SSH クライアントのマニュアルを参照してください。

オプション	説明
ssh host key	[Status] はホストキー（秘密キー）のステータスを表します。 ・[SSH Disabled: No host key in use] ： 無効になっている場合、SSH ではホストキーを使用できません。 ・[Generating]: 有効なホストキーが見つからないため、Rack PDU が、ホストキーを作成中です。 ・[Loading] ： Rack PDU. でホストキーを有効にする処理が進行中です。 ・[Valid]: 以下の有効なホストキーのいずれかが、/ssh ディレクトリ（Rack PDU 上の指定の場所）にあります。 ・Security Wizard で作成した 1024 ビットまたは 2048 ビットのホストキー ・Rack PDU により生成された 2048 ビットの RSA ホストキー [Add or Replace]: Security Wizard で作成したホストキーファイルの保存場所まで移動しホストキーをアップロードします。 Security Wizard の使用方法については、付録 B: セキュリティハンドブックを参照してください。 **注意**：SSH を有効にするためにかかる時間を減らすには、事前にホストキーを作成しアップロードしておきます。**ホストキーがインストールされていない状態で SSH を有効にした場合、Rack PDU はホストキーを作成します。これには 1 分ほどかかり、この間 SSH サーバーにはアクセスできなくなります。** [Remove]: 既存のホストキーを削除します。

SSH を使用するには、SSH クライアントがインストールされている必要があります。大部分の Linux およびその他の UNIX プラットフォームには、SSH クライアントが含まれていますが、Microsoft Windows オペレーティング システムには含まれていません。クライアント提供ベンダーから入手してください。

SNMP

SNMP のユーザー名、パスワード、コミュニティ名はすべてプレーンテキスト形式でネットワークに送信されます。お使いのネットワークでセキュリティレベルの高い暗号化が必要な場合、SNMP アクセスを無効にするか、または各コミュニティのアクセスを [Read] に設定してください。(読み取りアクセスのコミュニティはステータス情報の受信と SNMP トラップの使用が許可されています。)

お使いのシステムでのセキュリティ強化と管理の詳しい手順については、付録 B: セキュリティハンドブックを参照してください。

SNMPv1

選択項目：[Administration] > [Network] > [SNMPv1] > *オプション*

オプション	説明
[access]	[Enable SNMPv1 Access]: このデバイスとの通信方法として SNMP version 1 を有効にします。
access control	どの Network Management Systems（NMS）がこのデバイスにアクセスできるかを指定するために、4 つまでのアクセス制御を設定できます。アクセス制御の最初のページでは、デフォルト設定により、利用できる 4 つの SNMPv1 コミュニティのそれぞれにアクセス制御が 1 つずつ割り当てられていますが、この設定を編集して任意のコミュニティに複数のアクセス制御を適用し、特定のいくつかの IPv4/IPv6 アドレス、ホスト名、または ＩＰアドレスマスクによりアクセスできるように設定することができます。コミュニティのアクセス制御設定を変更するには、該当のコミュニティ名をクリックします。 ・コミュニティのアクセス制御をデフォルト設定のまま変更せずにおいた場合、そのコミュニティはネットワーク上のどの場所からでもこのデバイスにアクセスできます。 ・1 つのコミュニティ名に対して複数のアクセス制御を設定した場合、アクセス制御設定が 4 つまでに制限される要件のため、他のコミュニティ（1 つまたは複数）ではアクセス制御をまったく設定できないことになります。あるコミュニティでアクセス制御が何も設定されていない場合、そのコミュニティはこのデバイスにアクセスできません。 [Community Name] : コミュニティにアクセスするために NMS が使用しなければならない名前です。ASCII 文字 15 字以内で設定します。これら 4 つのコミュニティのデフォルト名は、**[public]**、**[private]**、**[public2]**、**[private2]** です。 [NMS IP/Host Name]: NMS によりアクセスを制御する IPv4/IPv6 アドレス、IP アドレスマスク、またはホスト名です。ホスト名または特定の IP アドレス（例 :149.225.12.1）を使用することで、特定の場所の NMS のみにアクセスを許可することができます。IP アドレスに「255」が含まれる場合、アクセスは次のように制限されます。 ・149.225.12.**255**: 149.225.12 セグメント上の NMS のみにアクセスを許可。 ・149.225.**255.255**: 149.225 セグメント上の NMS のみにアクセスを許可。 ・149.**255,255,255**: 149 セグメント上の NMS のみにアクセスを許可。 ・0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）: どのセグメントの NMS でもアクセス可能。 [Access Type]: NMS がコミュニティを通して実行できる操作です。 ・[Read]: 常に GET のみ。 ・[Write]: 常に GET。さらに、Web インターフェイスまたはコマンドラインインターフェイスにログオンされているユーザーがいない場合には SET。 ・[Write+]: 常に GET と SET。 ・[Disable]: 常に、GET と SET は不可。

SNMPv3

選択項目：[Administration] > [Network] > [SNMPv3] > *オプション*

SNMP の GET、SET、及びトラップレシーバの場合、SNMPv3 はユーザープロファイルのシステムを使用してユーザーを識別します。SNMPv3 ユーザーが GET や SET の実行、MIB の表示、トラップの受信を行うには、MIB ソフトウェアプログラムにより割り当てられたユーザープロファイルが必要です。

SNMPv3 を使用するには、SNMPv3 をサポートする MIB プログラムが必要です。

Rack PDU は、SHA または MD5 認証、および AES または DES の暗号化をサポートしています。

オプション	説明
[access]	[SNMPv3 Access]: このデバイスとの通信方法として SNMPv3 を有効にします。

オプション	説明
[user profiles]	デフォルト設定では [dell snmp profile1] から [dell snmp profile4] のユーザー名で 4 つのユーザープロファイルが設定されており、認証とプライバシー（暗号化）は何も設定されていません。ユーザープロファイルの以下の設定を変更したい場合、一覧内の該当のユーザー名をクリックします。 [User Name]: ユーザープロファイルの識別子です。SNMP バージョン 3 では、送信中のデータパケットのユーザー名をこのユーザー名と照合してユーザープロファイルに GET、SET、およびトラップをマッピングします。ユーザー名には 32 文字までの ASCII 文字を使用できます。 [Authentication Passphrase]: 15 から 32 文字の ASCII 文字からなるフレーズ（デフォルトでは「**dell auth passphrase**」）により、SNMPv3 を通してこのデバイスと通信している NMS が表明どおりの NMS であること、メッセージが通信中に改変されていないこと、メッセージが妥当な時間枠内に送信されている（すなわち遅延なく送信されている）こと、さらにメッセージのコピーが後の不適切な時点に再送信されていないことが証明されます。 [Privacy Passphrase]: 15 から 32 文字の ASCII 文字からなるフレーズ（デフォルトでは「**dell crypt passphrase**」）により、NMS が SNMPv3 を通してこのデバイス間で送受信するデータのプライバシー（暗号化によるプライバシー）が確実になります。 [Authentication Protocol]: Dell による SNMPv3 実装では、SHA と MD5 の認証がサポートされています。認証プロトコルを選択しないと認証は行われません。 [Privacy Protocol]: Dell による SNMPv3 実装では、データの暗号化と復号には AES と DES のプロトコルがサポートされています。送信データのプライバシーに関しては、プライバシプロトコルが選択されており、かつ NMS からのリクエストにプライバシパスフレーズが含まれていなければなりません。プライバシプロトコルが有効になっていても NMS からのリクエストにプライバシパスフレーズが含まれていないと、SNMP リクエストは暗号化されません。 **注意**: プライバシプロトコルは、認証プロトコルが選択されていない場合は選択できません。

オプション	説明
[access control]	どの Network Management Systems（NMS）がこのデバイスにアクセスできるかを指定するために、4 つまでのアクセス制御を設定できます。アクセス制御の最初のページでは、デフォルト設定により、利用できる 4 つのユーザープロファイルのそれぞれにアクセス制御が 1 つずつ割り当てられていますが、これは変更可能で、任意のユーザープロファイルに複数のアクセス制御を適用して、特定のいくつかの IP アドレス、ホスト名、または IP アドレスマスクによりアクセスできるように設定することができます。 ・ユーザープロファイルのアクセス制御をデフォルト設定のまま変更せずにおいた場合、そのプロファイルを使用する NMS はすべてこのデバイスにアクセスできます。 ・1 つのユーザープロファイルに対して複数のアクセス制御を設定した場合、アクセス制御設定が 4 つまでに制限される要件のため、他のユーザープロファイル（1 つまたは複数）ではアクセス制御をまったく設定できないことになります。あるユーザープロファイルに対しアクセス制御が何も設定されていない場合、そのプロファイルを使用する NMS はこのデバイスにまったくアクセスできなくなります。 ユーザープロファイルのアクセス制御設定を変更するには、該当のユーザー名をクリックします。 [Access]: [Enable] チェックボックスをオンにすると、そのアクセス制御設定のパラメータで指定されているアクセス制御が有効になります。 [User Name]: このアクセス制御を適用するユーザープロファイルをドロップダウンリストから選びます。左側ナビゲーションメニューの [user profiles] オプションで設定してある 4 つのユーザー名が、この場合に利用できるオプションとして一覧表示されます。 [NMS IP/Host Name]: NMS によるアクセスを制御する ＩＰ アドレス、ＩＰ アドレスマスク、またはホスト名です。ホスト名または特定の IP アドレス（例 :149.225.12.1）を使用することで、特定の場所の NMS のみにアクセスを許可することができます。IP アドレスマスクに「255」が含まれる場合、アクセスは次のように制限されます。 ・149.225.12.255: 149.225.12 セグメント上の NMS のみにアクセスを許可。 ・149.225.255.255: 149.225 セグメント上の NMS のみにアクセスを許可。 ・149.255.255.255: 149 セグメント上の NMS のみにアクセスを許可。 ・0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）: どのセグメントの NMS でもアクセス可能。

FTP サーバー

選択項目：[Administration] > [Network] > [FTP Server]

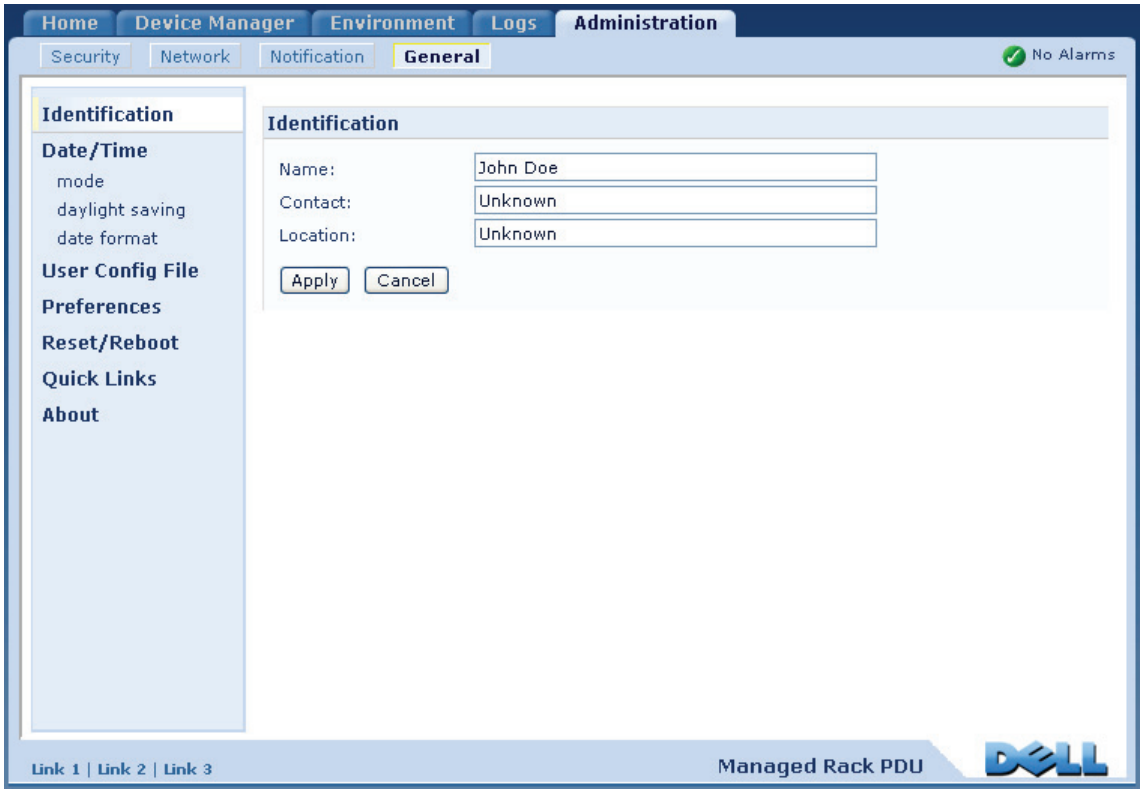
[FTP Server] では、FTP サーバーへのアクセスを有効（デフォルト）または無効にできます。また FTP サーバーが Rack PDU との通信に使用する TCP/IP ポート（デフォルトでは 21 番ポート）も指定できます。FTP サーバーは、ここで指定するポートと、それより 1 つ下の番号のポートの両方を使用します。

またセキュリティを強化するために、**ポート**番号を 5001 ～ 32768 の間の使用していない番号に設定することができます。この場合、ユーザーはコロン（:）を使用してデフォルト以外のポート番号を指定する必要があります。例えば、ポート番号が 5001 で IP アドレスが 152.214.12.114 の場合、「**`ftp 152.214.12.114:5001`**」のコマンドを使用します。

FTP は暗号化を使用しないでファイルを転送します。セキュリティを強化するには、FTP サーバーを無効にし、ファイルを SCP で送信してください。Secure Shell（SSH）を選択して設定すると、自動的に SCP が有効になります。

お使いのシステムでのセキュリティ強化と管理の詳しい手順については、付録 B: セキュリティハンドブックを参照してください。

管理：全般オプション


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
Identification
Date/Time
mode
daylight saving
date format
User Config File
Preferences
Reset/Reboot
Quick Links
About
Identification
Name:
John Doe
Contact:
Unknown
Location:
Unknown
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

ID

選択項目：[Administration] > [General] > [ID]

Rack PDU の SNMP エージェントで使用される [Name]（デバイス名）、[Location]（物理的なロケーション）、[Contact]（デバイスの責任者）を定義します。これらの設定は、MIB-II が使用する [sysName]、[sysContact]、[sysLocation] の各 Object Identifier（OID）の値として使用されます。

MIB-II OID の詳細については、「Dell Management Information Base（MIB）」を参照してください。

日付と時刻の設定

方法

選択項目：[Administration] > [General] > [Date & Time] > [mode]

Rack PDU で使用する日付と時刻を設定します。既存の設定の変更は、手動で、またはネットワーク時間プロトコル（NTP）サーバーを介して行います。

- [Manual Mode]：次のいずれかを実行します。
  - Rack PDU の日付と時刻を入力します。
  - [Apply Local Computer Time] のチェックボックスをオンにして、使用しているコンピュータの日付 / 時刻の設定と一致するようにします。
- [Synchronize with NTP Server]：Rack PDU の日付と時刻が NTP サーバーにより定義されるようにします。

設定	説明
[Primary NTP Server]	プライマリ NTP サーバーの IP アドレスまたはドメイン名を入力します。
[Secondary NTP Server]	セカンダリサーバーが利用可能な場合に、セカンダリ NTP サーバーの IP アドレスまたはドメイン名を入力します。
[Time Zone]	タイムゾーンを選択します。一覧表の各タイムゾーンの前に表示されている数字は、Coordinated Universal Time（UTC：協定世界時間、旧グリニッジ標準時）との時差を表します。
[Update Interval]	更新のために Rack PDU から NTP サーバーにアクセスする頻度を時間で設定します。*最小* 1；*最大* 8760（1 年）。
[Update Using NTP Now]	NTP サーバーに直ちにアクセスして日付と時刻を更新します。

夏時間

選択項目：[Administration] > [General] > [Date & Time] > [daylight saving]

米国方式の夏時間（DST）を有効にするか、または地域の夏時間に合わせて DST を調整してください。DST はデフォルトでは無効になっています。

[Daylight Savings Time]（DST）をカスタマイズする場合：

- 夏時間が、必ず月の 4 番目の特定の曜日（例：第 4 日曜日）に開始または終了する場合、[Fourth/Last] を選択します。次の年の同月には第 5 日曜日がある場合でも、第 4 日曜日に時間設定が変更されます。
- 夏時間が、必ず月の最後の特定の曜日（第 4 でも第 5 でも）に開始または終了する場合は、[Fifth/Last] を選択します。

形式

選択項目：[Administration] > [General] > [Date & Time] > [date format]

Web インターフェイスで表示されるすべての日付の形式を指定します。個々の「m」（月）、「d」（日）、「y」（年）はそれぞれ数字 1 文字に相当します。日付または月名が一桁の場合、前にゼロをつけて表示されます。

.ini ファイルの使用

選択項目：[Administration] > [Administration] > [User Config File]

いずれかの Rack PDU の設定を使用して他の Rack PDU を設定することができます。設定した Rack PDU から config.ini ファイルを読み出して、そのファイルをカスタマイズし（IP アドレスの変更など）、そのファイルを新しい Rack PDU にアップロードします。このファイルは、ファイル名が 64 文字以内で拡張子が「.ini」でなければなりません。

[Status]	アップロードの進行状況が表示されます。ファルにエラーがある場合でもアップロードできますが、その場合、システムイベントからイベントログにエラーが報告されます。
[Upload]	現在の Rack PDU にもこの設定を適用できるようカスタマイズしたファイルをアップロードします。

設定済みの Rack PDU の環境設定ファイルを取得およびカスタマイズする手順については、環境設定値のエクスポート方法を参照してください。

環境設定ファイルを 1 台の Rack PDU にアップロードする代わりに、FTP または SCP スクリプトを使用して複数の Rack PDU にファイルをエクスポートすることができます。

イベントログおよび温度単位

選択項目：[Administration] > [General] > [Preferences]

イベントログテキストの色分け

デフォルトではこの選択は無効になっています。[Event Log Color Coding] チェックボックスをオンにすると、イベントログに入力されるアラーム関連のテキストを色分けすることができます。システムイベントおよび環境設定への変更に関しては色分けは適用されません。

テキストの色	アラームの重要度
赤	[Critical]（致命的）：直ちに対処を要する重大な障害が発生しています。
オレンジ	[Warning]（警告）：処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。
緑	[Alarm Cleared]（アラーム状態クリア）：アラームの原因となっていた状況が好転しました。
黒	[Normal]（正常）：現在アラームは何も発生していません。Rack PDU および接続下のすべてのデバイスは正常に機能しています。

デフォルトの温度単位を変更

このユーザーインターフェイスで表示されるすべての温度測定値に適用する温度の単位（華氏または摂氏）を選択します。

Rack PDU のリセット

選択項目：[Administration] > [General] > [Reset/Reboot]

操作	説明
[Reboot Management Interface]	Rack PDU のインターフェイスを再起動します。
[Reset All][1]	[Exclude TCP/IP] チェックボックスをオフにすると、すべての設定構成値を消去できます。[Exclude TCP/IP] チェックボックスをオンにすると、TCP/IP 値を除く他のすべての値をリセットできます。
[Reset Only][1]	[TCP/IP settings]：TCP/IP 設定が [DHCP & BOOTP]（デフォルト設定）になっていると、Rack PDU では要件として DHCP サーバーまたは BOOTP サーバーから TCP/IP 設定を取得しなければならなくなります。TCP/IP 設定と通信設定を参照してください。
	[Event configuration]：イベント環境設定に加えられたこれまでのイベント別およびグループ別の変更内容を、すべてデフォルト値に戻します。
	[RPDU to Defaults]：ネットワーク設定を除く Rack PDU 設定のみを、デフォルト値に戻します。
1. リセットには最大 1 分かかります。	

リンクの設定

選択項目：[Administration] > [General] > [Quick Links]

[Administration] タブ、上部メニューバーの [General]、左側ナビゲーションメニューの [Quick Links] を順に選択すると、インターフェイスの各ページ左下に表示される URL のリンク先を表示または変更できます。

デフォルト設定では、これらのリンクをクリックすると下記の Web ページに移動します。

- Link 1：dell.com
- Link 2：dell.com/home
- Link 3：dell.com/business

次のいずれかの項目を再設定する場合は、[Display] 列のリンク名をクリックします。

- [Display]：インターフェイス各ページに表示される短い形式のリンク名です。
- [Name]：リンク先や目的を表わす名称です。
- [Address]：別のデバイスまたはサーバーの URL など、任意の URL です。

Rack PDU について

選択項目：[Administration] > [General] > [About]

ハードウェア情報は、Rack PDU に関する問題のトラブルシューティングに役立ちます。シリアル番号および MAC アドレスは、Rack PDU 本体に表記されています。

アプリケーションモジュール、Dell OS (AOS)、ブートモニタのファームウェア情報には、ファームウェア名、ファームウェアバージョン、および各ファームウェアモジュールの作成日が表示されます。トラブルシューティングの際には、この情報も有用です。

[Management Uptime] はインターフェイスのこれまでの継続稼動時間です。

環境設定値のエクスポート方法

.ini ファイルの取得とエクスポート

手順の概要

管理者は Rack PDU の .ini ファイルを取得して、ほかの Rack PDU（複数の Rack PDU を含む）にエクスポートすることができます。

1. Rack PDU をエクスポートする値に設定します。
2. Rack PDU から .ini ファイルを取得します。
3. 少なくとも TCP/IP 設定を変更してこのファイルをカスタマイズします。
4. Rack PDU でサポートされるファイル転送プロトコルを使用して、ファイルのコピーをほか（1 台または複数）の Rack PDU に転送します。複数の Rack PDU に転送する場合は、FTP または SCP スクリプトを使用します。

ファイルを受信した各 Rack PDU で、このファイルによって各自の設定を行い、設定後はファイルを削除します。

.ini ファイルの内容

Rack PDU から取得した config.ini ファイルには次の内容が含まれます。

- *セクションヘディング* と *キーワード*（ファイルの取得元のデバイスでサポートされているもののみ）：セクションヘディングはカテゴリ名に相当し、角括弧（[ ]）で囲まれています。各セクションヘディングの下のキーワードは、Rack PDU の特定の設定について記述するラベルです。各キーワードの後には、イコールサイン、そして値（デフォルト値または設定されている値）が続きます。

- **[Override]** キーワード： このキーワードがデフォルト値の場合、デバイス固有の値が設定されたひとつまたは複数のキーワードの値はエクスポートされません。例えば、**[NetworkTCP/IP]** セクションでは「**Override**」がデフォルト値（Rack PDU の MAC アドレス）になっており、**[SystemIP]**、**[SubnetMask]**、**[DefaultGateway]**、**[BootMode]** の値がエクスポートされないようになっています。

詳細手順

取得 .ini ファイルをエクスポート用にセットアップして取得するには次の作業を行います。

1. 可能であれば、Rack PDU のインターフェイスを使用して、このファイルにエクスポート用の設定を適用します。直接 .ini ファイルを編集すると、エラーを招く危険があります。
2. FTP を使用して設定済み Rack PDU から config.ini ファイルを取得するには：
   a. IP アドレスにより、Rack PDU への接続を確立します。
      ftp> open *ip_address*
   b. 管理者のユーザー名とパスワードを入力してログオンします。
   c. Rack PDU の設定が保存された config.ini ファイルを取得します。
      ftp> get *config.ini*

      ファイルが起動した FTP からフォルダに書き込まれます。

カスタマイズ ファイルをエクスポートする前にカスタマイズする必要があります。

1. テキストエディタを使ってファイルをカスタマイズします。
   - セクションヘディング、キーワード、事前に定義された値については大文字と小文字の区別はありませんが、ユーザーが定義したストリング値には区別があります。
   - 値がないことを表すには、連続するクォーテーションマークを使用します。例えば、**LinkURL1=""** は URL が意図的に指定されていないことを示します。
   - スペースから始まる値、スペースで終わる値は、クォーテーションマークで囲みます。またすでにクォーテーションマークで囲まれている値も、さらにクォーテーションマークで囲みます。
   - スケジュールされているイベントをエクスポートする場合、値は ini ファイル内で直接設定します。
   - システム時刻を更に正確にエクスポートできるよう、Rack PDU がネットワーク時間プロトコルサーバーにアクセスできる場合には、**[NTPEnable]** を **[enabled]** に設定します。

     NTPEnable=enabled

     また、**[SystemDate/Time]** セクションを別個の .ini ファイルとしてエクスポートすることで転送時間を短くすることもできます。
   - コメントを追加するには、コメントの各行をセミコロン（;）で始めます。
2. カスタマイズしたファイルを同じフォルダ内で別名ファイルとしてコピーします。
   - このファイルは、ファイル名が 64 文字以内で拡張子が「.ini」でなければなりません。
   - 後日の使用のためにカスタマイズした元のファイルを保持します。**コメント行へ内容を追加した場合、この保存ファイルにのみ、追加内容が記録されています。**

単独の Rack PDU へのファイル転送 .ini ファイルを別の Rack PDU に転送するには次のいずれかの手順を実行します。

- ファイルの受け手側の Rack PDU の Web インターフェイスで、[Administration] タブ、上部メニューバーの [General]、左側ナビゲーションメニューの [User Config File] を順に選択します。ファイルへの完全なパスを入力するか、または [Browse] ボタンを押してファイルを指定します。
- Rack PDU でサポートされているファイル転送プロトコル（FTP、FTP Client、SCP、TFTP）のいずれも使用できます。以下に FTP を使用する例を示します。
  a. カスタマイズした .ini ファイルのコピーを保存してあるフォルダから、FTP を介して、.ini ファイルのエクスポート先の Rack PDU にログオンします。
  ftp> open *ip_address*
  b. カスタマイズした .ini ファイルのコピーを、受信側 Rack PDU のルートディレクトリにエクスポートします。
  ftp> put *filename.ini*

複数の Rack PDU へのファイルのエクスポート .ini ファイルを複数の Rack PDU にエクスポートするには FTP または SCP を使用しますが、単独の Rack PDU にファイルをエクスポートする手順を組み込んでおり、それを繰り返すスクリプトを記述する必要があります。

アップロード関連のイベントとエラーメッセージ

イベントとエラーメッセージ

受け入れ側の Rack PDU で .ini を使用した設定のアップデートが完了すると次のイベントが起こります。

`Configuration file upload complete, with` *`number`* `valid values`

キーワード、セクション名、または値が無効な場合、受信側 Rack PDU によるアップロードは継続して追加のイベントテキストがエラーを記述します。

イベントテキスト	説明
設定ファイル警告 : Invalid keyword on line *number*. 設定ファイル警告 : Invalid value on line *number*.	無効なキーワードまたは値を持つラインは無視されます。
設定ファイル警告 : Invalid section on line *number*.	セクション名が無効だと、そのセクションに含まれるキーワード / 値の対は無視されます。
設定ファイル警告 : Keyword found outside of a section on line *number*.	ファイルの始めに入力されたキーワード（セクションヘディングの前）は無視されます。
設定ファイル警告 : Configuration file exceeds maximum size.	ファイルサイズが大きすぎる場合、アップロードは完了しません。ファイルのサイズを減らすか 2 つのファイルに分割するかして、もう一度アップロードを試みます。

config.ini のメッセージ

config.ini ファイルのダウンロード元の Rack PDU が正しく検出されないと、ファイルには環境設定が含まれなくなります。Rack PDU が存在しないか検出されなかった場合、config.ini ファイルの該当セクション名の下には、キーワードと値のかわりにメッセージが入力されます。例えば次のようになります。

```
Rack PDU not discovered
```

インポートした .ini ファイルで設定されていた Rack PDU をエクスポートしようとしていなかった場合は、これらのメッセージは無視してください。

無効にされた値によって生成されるエラー

「**Override**」キーワードとその値によってエクスポート値のグループがブロックされた場合には、イベントログにエラーメッセージが生成されます。

どの値が無効にされるかについての詳細は、.ini ファイルの内容を参照してください。

上書きされた値はデバイス固有でほかの Rack PDU へのエクスポートには適していないため、これらのエラーメッセージは無視してください。これらのエラーメッセージが出されるのを避けるため、「**Override**」キーワードを含む行と無視されるべき値を含む行を削除することができます。セクションヘディングを含む行は削除、変更しないでください。

ファイルの転送

ファームウェアのアップグレード方法

ファームウェアアップグレードの利点

Rack PDU のファームウェアのアップグレードには、次のような利点があります。

- 新しいファームウェアには最新版のバグ修正が反映されており、性能も改善されています。
- アップグレードすることで新機能が直ちに利用できるようになります。

またネットワーク上のすべてのファームウェアを同一バージョンにしておくことで、すべての Rack PDU が新機能に均一に対応するようになります。

ファームウェアのファイル

ファームウェアバージョンには、オペレーティングシステム（AOS）モジュール、アプリケーションモジュール、ブートモニタ（bootmon）モジュールの 3 つモジュールが含まれています。各モジュールには、転送中にデータを破損から保護するための巡回冗長検査（CRC）がいくつか含まれています。

Rack PDU で使用されるオペレーティングシステム（AOS）ファイル、アプリケーションファイル、およびブートモニタモジュールファイルは、下記の基本形式を共有しています。

dell_*hardware-version*_*type*_*firmware-version*.bin

- **dell**：Dell ファイルであることを表します。
- ***hardware-version***：**hw0***x* は、このバイナリファイルを使用できるハードウェアバージョンを表します。
- ***type***：このファイルが、Rack PDU のオペレーティングシステム（AOS）モジュール用なのか、それともブートモニタモジュール用なのかを示します。
- ***version***：ファイルのバージョン番号です。
- **bin**：バイナリファイルであることを表します。

Rack PDU の各ファームウェアモジュールのバージョン番号を確認するには、Rack PDU について を参照してください。

ファームウェアファイルの転送方式

Rack PDU のファームウェアアップグレードは下記のいずれかの方法で行ってください。

- ネットワークに接続されているサポート対象オペレーティングシステム稼動のコンピュータから、FTP または SCP を使用して個々の AOS とアプリケーションファームウェアモジュールを転送してアップグレードします。
- ネットワークに接続されていない Rack PDU の場合は、シリアル接続で XMODEM を使用して個々のファームウェアモジュールをコンピュータから Rack PDU に転送することができます。

個々のファームウェアモジュールを転送する場合は、このファームウェアモジュールの転送に入る前に、まずオペレーティングシステム（AOS）モジュールを Rack PDU に**送信しておかなければなりません**。

FTP または SCP を使用した単独の Rack PDU のアップグレード

FTP ネットワーク上にある単独の Rack PDU を FTP を介してアップグレードするには、下記の条件を満たしている必要があります。

- Rack PDU がネットワークに接続されており、カードのシステム IP、サブネットマスク、デフォルトゲートウェイが設定済みである。
- Rack PDU で FTP サーバーが有効である。
- ファームウェアファイルを Dell.com よりダウンロードしている。

ファイルを転送するには：

1. ネットワーク上のコンピュータで、[コマンド プロンプト] ウィンドウを開きます。ファームウェアファイルがあるディレクトリに移動し、ファイル一覧を表示します。

   ```
   C:\>cd\dell
   C:\dell>dir
   ```

   一覧内のファイルの「*xxx*」の部分はそれぞれ相当するファームウェアバージョン番号です。

   - **dell_hw05_aos_*xxx*.bin**
   - **dell_hw05_application_*xxx*.bin**

2. FTP クライアントセッションを開始します。
   C:\dell>ftp
3. 「**open**」とタイプし、Rack PDU の IP アドレスを入力して ENTER キーを押します。FTP サーバーのポートの値がデフォルトの 21 ではない場合、FTP コマンドにデフォルト以外の値を指定する必要があります。
   - Windows FTP クライアントの場合、デフォルト以外のポート番号と IP アドレスの間にはスペースを入れて区切ります。例えば次のようになります。
     ftp> open 150.250.6.10 21000
   - 一部の FTP クライアントでは、ポート番号の前にスペースではなくコロンが必要です。
4. 管理者権限でログオンします。デフォルトのユーザー名とパスワードはそれぞれ「admin」です。
5. AOS をアップグレードします。（下記の例の「*xxx*」の部分は相当するファームウェアバージョン番号です。）
   ftp> bin
   ftp> put dell_hw05_aos_*xxx*.bin
6. FTP により転送が確認されたら、「quit」と入力してセッションを終了します。
7. 20 秒経過したら、手順 2 から手順 5 までを繰り返します。手順 5 では、アプリケーションモジュールのファイル名を使用してください。

SCP Secure CoPy（SCP）を使用して Rack PDU のファームウェアをアップグレードするには次の手順に従ってください。

1. 前述の FTP の手順で説明したファームウェアモジュールを検索して保存場所を確認します。
2. SCP コマンドラインを使用して、AOS ファームウェアモジュールを Rack PDU に転送します。下記の例の「*xxx*」の部分は相当する AOS モジュールバージョン番号です。
   scp dell_hw05_aos_xxx.bin
   dell@158.205.6.185:dell_hw05_aos_xxx.bin
3. 同様の SCP コマンドラインを使用し、該当のアプリケーションモジュール名で、アプリケーションファームウェアモジュールを Rack PDU に転送します。

複数の Rack PDU のアップグレード方法

FTP または SCP による複数の Rack PDU のアップグレード FTP クライアントを使って複数の Rack PDU をアップグレードするには、手順を自動実行するスクリプトを作成してください。

XMODEM による単独の Rack PDU のアップグレード

XMODEM を使用してネットワーク上にない単独の Rack PDU をアップグレードするには、まず Dell.com からファームウェアファイルをダウンロードする必要があります。

ファイルを転送するには：

1. ローカルコンピュータでアップグレードに使用するシリアルポートを選択し、このポートを使用しているサービスを無効にします。
2. 付属のシリアル設定ケーブルを、選択したポートと Rack PDU にあるシリアルポートに接続します。
3. 端末プログラム（ハイパーターミナルなど）を起動し、選択したポートの設定を 57600 bps、データビット 8、パリティなし、ストップビット 1、フロー制御なしに設定します。
4. Rack PDU の [RESET] ボタンを押し、続けてすぐに ENTER キーを 2 度押すか、あるいは [Boot Monitor] プロンプトに **BM>** が表示されるまで Enter キーを押します。
5. 「**xmodem**」と入力して ENTER キーを押します。
6. 端末プログラムのメニューから XMODEM を選び、XMODEM を用いて転送するバイナリ AOS ファームウェアファイルを選択します。XMODEM を介した転送が完了すると、画面には再び [Boot Monitor] プロンプトが表示されます。
7. アプリケーションモジュールをインストールするには、手順 5 ～ 6 を繰り返します。手順 6 では該当のアプリケーションモジュールファイル名を使用します。
8. 「**reset**」と入力するかまたは [Reset] ボタンを押して、Rack PDU を再起動させます。

ファームウェアモジュールに使用する形式については、ファームウェアのファイルを参照してください。

アップグレードや更新の確認

転送結果の確認

ファームウェアアップグレードが成功したかどうかを確認するには、コマンドラインインターフェイスに **xferStatus** コマンドを入力して直近の転送結果を表示するか、または mfiletransferStatusLastTransferResult OID に対して SNMP GET クエリを実行します。

直近の転送結果コード

コード	説明
Successful	ファイル転送は正常に完了しました。
Result not available	ファイル転送が記録されていません。
Failure unknown	先ほどのファイル転送は、何らかの理由で失敗しました。
Server inaccessible	ネットワークで TFTP または FTP サーバーが見つかりませんでした。
Server access denied	TFTP または FTP サーバーへのアクセスが拒否されました。
File not found	TFTP または FTP サーバーは指定のファイルを見つけられませんでした。
File type unknown	ファイルをダウンロードしましたが、内容が認識されませんでした。
File corrupt	ファイルをダウンロードしましたが、ファイル内に巡回冗長検査（CRC）で誤りとなったものがあります。

インストールされたファームウェアのバージョン番号の確認

Web インターフェイスからアップグレードしたファームウェアモジュールのバージョンを確認するには、[Administration] タブ、上部メニューバーの [General]、左側ナビゲーションメニューの [About] を順に選択するか、または MIB II sysDescr OID に SNMP GET を実行します。コマンドラインインターフェイスでは、「**about**」コマンドを使用してください。

トラブルシューティング

Rack PDU のアクセスに関するトラブル

問題	対処方法
Rack PDU に対して ping が実行できない	Rack PDU のステータス LED が緑の場合、Rack PDU と同じネットワークセグメントの別のノードに対して ping を試行します。これが失敗する場合、問題は Rack PDU に起因するものではありません。ステータス LED が緑でない場合、または ping テストが成功した場合は、次の事柄を確認してください。 ・すべてのネットワーク接続を確認します。 ・Rack PDU と NMS の IP アドレスを確認します。 ・NMS が Rack PDU と異なる物理ネットワーク（またはサブネットワーク）上にある場合は、デフォルトゲートウェイ（またはルーター）の IP アドレスを確認します。 ・Rack PDU のサブネットマスクのサブネットビット数を確認します。
通信ポートを端末プログラムを通して指定できない	端末プログラムを使用して Rack PDU を設定するには、その前にその通信ポートを使用しているすべてのアプリケーション、サービス、プログラムを終了する必要があります。
コマンドラインインターフェイスにシリアル接続でアクセスできない	ボーレートを変更していないことを確認してください。2400、9600、19200 または 38400 で試します。
コマンドラインインターフェイスにリモートアクセスできない	・正しいアクセス方法（Telnet または Secure Shell（SSH））を使用していることを確認してください。これらのアクセス方法を有効にするには管理者の権限が必要です。デフォルトでは、Telnet が有効です。SSH を有効にすると、自動的に Telnet が無効になります。 ・SSH の場合、Rack PDU がホストキーを作成中である可能性があります。Rack PDU はこのホストキーの作成に最高で 1 分かかります。この間 SSH にはアクセスできません。

問題	対処方法
Web インターフェイスにアクセスできない	・HTTP または HTTPS アクセスが有効になっているかどうかを確認します。 ・正しい URL を指定していることを確認します。これは Rack PDU で使用されているセキュリティシステムと同一である必要があります。SSL では、URL の始めの部分が「https」（「http」ではなく）になっていなければなりません。 ・Rack PDU に ping を実行して応答があるかどうかを確認してください。 ・Rack PDU でサポートされている Web ブラウザを使用しているかどうかを確認します。サポートされる Web ブラウザを参照してください。 ・Rack PDU が再起動したばかりで SSL セキュリティの設定中である場合は、Rack PDU がサーバー証明書を生成中の可能性があります。Rack PDU はこの証明書を作成するのに最高で 1 分かかります。この間 SSL サーバーは利用できません。

付録 A：サポートされているコマンドの一覧

Network Management Card のコマンドの説明

```
?
about
alarmcount
   [-p [all | warning | critical]]
boot
   [-b <dhcpBootp | dhcp | bootp | manual>]
   [-a <remainDhcpBootp | gotoDhcpOrBootp>]
   [-o <stop | prevSettings>]
   [-f <retry then fail #>]
   [-c <dhcp cookie> [enable | disable]]
   [-s <retry then stop #>]
   [-v <vendor class>]
   [-i <client id>]
   [-u <user class>]
cd
console
   [-S<disable | telnet | ssh>]
   [-pt <telnet port n>]
   [-ps <SSH port n>]
   [-b <2400 | 9600 | 19200 | 38400>]
date
   [-d < “datestring” >]
   [-t <00:00:00>]
   [-f [mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd]]
delete
dir
dns
   [-OM <enable | disable>]
   [-p <primary DNS server>]
   [-s <secondary DNS server>]
   [-d <domain name>]
   [-n <domain name IPv6>]
   [-h <host name>]
eventlog
exit
format
```

```
ftp
   [-p <port number>]
   [-S <enable | disable>]
help
netstat
ntp
   [-OM <enable | disable>]
   [-p <primary NTP server>]
   [-s <secondary NTP server>]
ping
   [<IP address or DNS name>]
portspeed
   [-s [auto | 10H | 10F | 100H | 100F]]
prompt
   [-s [long | short]]
quit
radius
   [-a <access> [local | radiusLocal | radius]]
   [-p# <server IP>]
   [-s# <server secret>]
   [-t# <server timeout>]
reboot
resetToDef
   [-p <all | keepip>]
snmp, snmpv3
   [-S <enable | disable>]
system
   [-n <system name>]
   [-c <system contact>]
   [-l <system location>]
tcpip
   [-i <IP address>]
   [-s <subnet mask>]
   [-g <gateway>]
   [-d <domain name>]
   [-h <host name>]
tcpip6
   [-S <enable | disable>]
   [-man <enable | disable>]
   [-auto <enable | disable>]
   [-i <IPv6 address>]
   [-g <IPv6 gateway>]
   [-d6 <router | stateful | stateless | never>]
```

```
user
   [-an <Administrator name>]
   [-dn <Device User name>]
   [-rn <Read-Only User name>]
   [-ap <Administrator password>]
   [-dp <Device User password>]
   [-rp <Read-Only User password>]
   [-t <inactivity timeout in minutes>]
web
   [-S <disable | http | https>]
   [-ph <http port #>]
   [-ps <https port #>]
xferINI
xferStatus
```

デバイスコマンドの説明

```
devLowLoad
   [<power>]
devNearOver
   [<power>]
devOverLoad
   [<power>]
devReading
   [< “power” | “energy” >]
devStartDly
humLow
   [<humidity>]
humMin
   [<humidity>]
humReading
inNormal
inReading
olAssignUsr
   [< “all” | outlet name | outlet# > <user>]
olCancelCmd
   [< “all” | outlet name | outlet#>]
olDlyOff
   [< “all” | outlet name | outlet#>]
olDlyOn
   [< “all” | outlet name | outlet#>]
olDlyReboot
   [< “all” | outlet name | outlet#>]
olGroups
```

olLowLoad
[< “all” | outlet name | outlet#> <power>]
olName
[< “all” | outlet# > <new name>]
olNearOver
[< “all” | outlet name | outlet#> <power>]
olOff
[< “all” | outlet name | outlet# >]
olOffDelay
[< “all” | outlet name | outlet#> <time>]
olOn
[< “all” | outlet name | outlet#>]
olOnDelay
[< “all” | outlet name | outlet#> <time>]
olOverLoad
[< “all” | outlet name | outlet#> <power>]
olRbootTime
[< “all” | outlet name | outlet#> <time>]
olReading
[< “all” | outlet name | outlet# > <current | power | energy>]
olReboot
[< “all” | outlet name | outlet# >]
olStatus
[< “all” | outlet name | outlet# >]
olUnasgnUsr
[< “all” | outlet name | outlet# > <user>]
phLowLoad
[< “all” | phase#> <current>]
phNearOver
[< “all” | phase#> <current>]
phOverLoad
[< “all” | phase#> <current>]
phReading
[< “all” | phase#> < “current” | “voltage” | “power” >]
phRestrictn
[< “all” | phase#> <none | near | over>]
prodInfo
tempHigh
[< “F” | “C” > <temperature>]
tempMax
[< “F” | “C” > <temperature>]
tempReading
[< “F” | “C” >]

```
userAdd
   [<new user>]
userDelete
   [<user>]
userList
userPasswd
   [<user> <new password> <new password>]
whoami
```

付録 B: セキュリティハンドブック

本付録の内容と目的

本付録では、Dell® Rack PDU のファームウェアバージョン 5.*x.x* のセキュリティ機能について記載しています。このファームウェアバージョンでは、ネットワーク上で Rack PDU のリモート操作を実行できます。

本付録は、また、次のプロトコルや機能、状況に応じたプロトコルの選択方法、セキュリティシステム全体におけるプロトコルや機能の設定および使用方法についても触れています。

- Telnet および Secure Shell (SSH)
- Secure Sockets Layer (SSL)
- RADIUS
- SNMPv1 および SNMPv3

さらに本付録では、SSL と SSH を使用した高度なセキュリティに必要なコンポーネントを Rack PDU Security Wizard を使用して作成する方法についても説明しています。

セキュリティ機能

パスワードとパスフレーズの保護

パスワードとパスフレーズは、Rack PDU 内に通常のテキスト形式では保存されていません。

- パスワードは、一方向ハッシュアルゴリズムを使用してハッシュ化されています。
- 認証と暗号化に使用されるパスフレーズは、暗号化されてから Rack PDU に保存されます。

アクセス手法のサマリ

コマンドラインインターフェイスへのシリアルアクセス

セキュリティアクセス	説明
ユーザー名とパスワードでアクセス	常に有効です。

コマンドラインインターフェイスへのリモートアクセス

セキュリティアクセス	説明
使用可能な手段： ・ユーザー名とパスワード ・サーバーポートの選択 ・有効化または無効化が可能なアクセスプロトコル ・Secure Shell (SSH)	高度なセキュリティのためには、SSH を使用します。 ・Telnet の場合は、ユーザー名とパスワードはプレーンテキスト形式で送信されます。 ・SSH を有効化すると Telnet は無効となり、コマンドラインインターフェイスへ暗号化されたアクセスが可能となります。これにより、送信中のデータの傍受、捏造、改変を防ぐ機能が追加されます。

セキュリティアクセス	説明
使用可能な手段（SNMPv1）： ・コミュニティ名 ・ホスト名 ・NMS IP フィルタ ・有効化または無効化が可能なエージェント ・読み込み / 書き込み / 無効化機能による 4 つのアクセスコミュニティ	SNMPv1 および SNMPv3 のいずれも、ホスト名を指定することにより、特定の Network Management System（NMS）からのアクセスに制限されます。さらに NMS IP フィルタにより、次の例に示すように、IP アドレスフォーマットのいずれかで指定される NMS へのアクセスのみが許可されます。 ・159.215.12.1: IP アドレスが 159.215.12.1 の NMS のみ。 ・159.215.12.255: 159.215.12 セグメントのあらゆる NMS。 ・159.215.255.255: 159.215 セグメントのあらゆる NMS。 ・159.255.255.255: 159 セグメントのあらゆる NMS。 ・0.0.0.0 または 255.255.255.255: あらゆる NMS。 SNMPv3 には追加セキュリティ機能があり、次の機能も含まれます。 ・認証パスフレーズにより、Rack PDU またはネットワーク対応デバイスにアクセスしようとする NMS が、実際にその NMS 自身であることが裏付けられます。 ・送信中のデータ暗号化です。この暗号化と復号化にはプライバシーパスフレーズが必要です。
使用可能な手段（SNMPv3）： ・4 つのユーザープロファイル ・認証パスフレーズによる認証 ・プライバシーパスフレーズによる暗号化 ・SHA または MD5 認証 ・AES または DES 暗号化アルゴリズム ・NMS IP フィルタ	

ファイル転送プロトコル

セキュリティアクセス	説明
使用可能な手段： ・ユーザー名とパスワード ・サーバーポートの選択 ・有効化または無効化が可能な FTP サーバーおよびアクセスプロトコル ・SCP（Secure CoPy）	FTP を使用した場合、ユーザー名とパスワードはプレーンテキスト形式で送信されます。また、ファイルは暗号化なしで転送されます。 SCP を使用すると、ユーザー名とパスードが暗号化されます。また、ファームウェアの更新、環境設定ファイル、ログファイル、Secure Sockets Layer（SSL）証明書、Secure Shell（SSH）ホストキーなどの転送されるファイルが暗号化されます。ファイル転送プロトコルとして SCP を選択する場合は、SSH を有効にし、FTP を無効にします。

Web サーバー

セキュリティアクセス	説明
使用可能な手段： ・ユーザー名とパスワード ・サーバーポートの選択 ・有効化または無効化が可能な Web インターフェイスアクセス ・Secure Sockets Layer（SSL）	基本的な HTTP 認証モードでは、ユーザー名とパスワードが Base64 で符号化され、暗号化されずに送信されます。 SSL は、Network Management Card またはネットワーク対応デバイスの使用がサポートされている Web ブラウザ、およびほとんどの Web サーバーで使用可能です。Web プロトコルの HyperText Transfer Protocol over Secure Socket Layer（HTTPS）は、Web サーバーへのページリクエストおよび Web サーバーによってユーザーに返されるページを暗号化 / 復号化します。

RADIUS

セキュリティアクセス	説明
使用可能な手段： ・アクセス権の集中認証 ・RADIUS サーバーと、Rack PDU またはデバイスの間で共有されているサーバーシークレット	RADIUS（Remote Authentication Dial-In User Service）は、各 Rack PDU のリモートアクセスを集中管理するために使用される、認証、許可、アカウンティングサービスです。（Rack PDU は認証機能と許可機能をサポートしています。）

アクセスの優先度

アクセスの優先度を、高い順に示します。

- Rack PDU に直接シリアル接続されているコンピュータから、ローカルでコマンドラインインターフェイスにアクセスする場合
- リモートコンピュータから、Telnet または Secure Shell（SSH）を使用してコマンドラインインターフェイスにアクセスする場合
- Web アクセス

デフォルトのユーザー名とパスワードの迅速な変更

Rack PDU のインストールと初期設定の後で、ユーザー名とパスワードをデフォルト値から固有の値に直ちに変更して、基本的なセキュリティを確立します。

ポートの割り当て

Telnet、FTP サーバー、SSH/SCP、または Web サーバーで非標準ポートを使用する場合は、ユーザーが Rack PDU へのアクセスに使用するコマンドラインまたは Web アドレスでポートを指定する必要があります。非標準のポート番号を使用すれば、セキュリティレベルを高めることができます。ポートは初期状態では、プロトコルの標準である″よく知られたポート″に設定されています。セキュリティを強化するには、FTP サーバーの場合は 5001 ～ 32768 の範囲で、その他のプロトコルおよびサーバーの場合は 5000 ～ 32768 の範囲で未使用のポート番号のいずれかにリセットします。(FTP サーバーでは、指定されたポートとその番号より 1 つ小さい番号のポートの両方が使用されます。)

SNMPv1 によるユーザー名、パスワード、およびコミュニティ名

SNMPv1 のユーザー名、パスワード、およびコミュニティ名はすべてプレーンテキスト形式でネットワークに転送されます。ネットワークトラフィックを参照できるユーザーなら、ユーザー名やパスワードを傍受して Rack PDU のコマンドラインインターフェイスや Web インターフェイスのアカウントにログオンできます。コマンドラインインターフェイスおよび Web インターフェイスで使用可能な暗号化ベースのオプションによりネットワークのセキュリティを高める必要がある場合は、SNMPv1 アクセスを無効にするか、またはアクセスを [Read] に設定する処置を必ず行ってください。([Read] アクセスにより、ステータス情報の受信と SNMPv1 トラップの使用が可能となります。)

SNMPv1 アクセスを無効にするには、[Administration] タブで上部メニューバーの [Network] を選択し、左側ナビゲーションメニューの [SNMPv1] 項目下の [access] を選択します。[Enable SNMPv1 access] のチェックを外し、[Apply] をクリックします。

[Read] への SNMPv1 アクセスを設定するには、[Administration] タブで上部メニューバーの [Network]、および左側ナビゲーションメニューの [SNMPv1] 項目下の [access control] を選択します。そして、設定した Network Management System (NMS) ごとに、コミュニティ名をクリックしてアクセスの種類を [Read] に設定します。

認証

Rack PDU 用のセキュリティ機能を使用するよう選択できます。このセキュリティ機能は、暗号化を使用せずに、ユーザー名、パスワード、IT アドレスを使用して基本的な認証を提供することでアクセスをコントロールします。重要なデータが転送されることのない環境では、これらの基本的なセキュリティ機能で十分です。

SNMP GETS、SETS、およびトラップ

SNMP を使用して Rack PDU を監視または設定する場合にセキュリティ機能を強化するには、SNMPv3 を選択します。SNMPv3 ユーザープロファイルで使用される認証パスフレーズにより、Rack PDU と通信しようとする Network Management System（NMS）が実際にその NMS 自身であること、送信中にメッセージが変更されていないこと、およびメッセージが遅延、コピー、不適切な時間が経過した後の再送によるものでないことが裏付けられます。デフォルトでは、SNMPv3 が無効になっています。

Dell が実装している SNMPv3 では、SHA-1 または MD5 プロトコルを使用して認証を行うことができます。

Web インターフェイスとコマンドラインインターフェイス

Rack PDU とクライアントインターフェイス（コマンドラインインターフェイスや Web インターフェイス）間のデータや通信が傍受されないようにするには、次の暗号化ベースの手段を使用すれば、より高度なセキュリティが確保できます。

- Web インターフェイスの場合は、Secure Sockets Layer（SSL）プロトコルを使用します。
- コマンドラインインターフェイスアクセスの場合にユーザー名とパスワードを暗号化するには、Secure Shell（SSH）プロトコルを使用します。
- ファイルを高いセキュリティで転送するためにユーザー名、パスワード、データを暗号化するには、Secure CoPy（SCP）プロトコルを使用します。

暗号化に基づくセキュリティの詳細については、暗号化を参照してください。

暗号化

SNMP GETS、SETS、およびトラップ

SNMP を使用して Rack PDU を監視または設定する場合に通信を暗号化するには、SNMPv3 を選択します。SNMPv3 ユーザープロファイルのプライバシーパスフレーズにより、NMS と Rack PDU またはネットワーク対応デバイスとの間で送受信されるデータのプライバシー（AES または DES 暗号化アルゴリズムを使用した暗号化による）が確保されます。

コマンドラインインターフェイスの Secure Shell（SSH）と Secure CoPy（SCP）

Secure Shell プロトコル SSH は、コンピュータコンソールまたは*シェル*にリモートでアクセスするためのセキュアなメカニズムを提供します。このプロトコルはサーバー（この場合 Rack PDU）の認証を行い、SSH クライアントとサーバー間のすべての通信を暗号化します。

- SSH は、Telnet を使用する場合の高度なセキュリティです。Telnet 自体には暗号化機能はありません。
- SSH は、認証の証明書であるユーザー名とパスワードが、ネットワークトラフィックを傍受する人物によって使用されることのないように保護します。
- SSH サーバー（Rack PDU）を SSH クライアントに対して認証するには、SSH サーバーに固有なホストキーが使用されます。ホストキーは偽造不可能な ID で、ネットワーク上の無効なサーバーが有効なサーバーであるかのように振る舞ってユーザー名やパスワードを取得するのを防ぎます。

  サポートされる SSH クライアントアプリケーションについては、Telnet および Secure Shell（SSH）を参照してください。ホストキーを作成するには、SSH ホストキーの作成を参照してください。

- Rack PDU では SSH バージョン 2 をサポートしており、データ転送中の傍受、偽造、または改ざんの試行からデータを保護します。
- SSH を有効にすると、Telnet は自動的に無効になります。

・インターフェイス、ユーザーアカウント、ユーザーアクセス権は、コマンドラインインターフェイスへのアクセスに SSH を使用する場合も Telnet を使用する場合も同じです。

Secure CoPy SCP は安全なファイル転送を実行するアプリケーションで、FTP の代わりに使用できます。SCP では、ユーザー名、パスワード、ファイルの暗号化に使用される転送プロトコルの基盤として SSH プロトコルが使用されます。

・SSH を有効化して設定を行うと、SCP も自動的に有効化されて設定されます。その後の SCP の設定は不要です。

・FTP は確実に無効にする必要があります。SSH を有効にするだけでは、FTP は無効になりません。FTP を無効にするには、[Administration] タブで上部メニューバーの [Network] を選択し、左側ナビゲーションメニューの [FTP Server] を選択する必要があります。[Enable] チェックボックスのチェックを外し、[Apply] をクリックします。

Web インターフェイスの Secure Sockets Layer (SSL)

安全な Web 通信を行うためには、Rack PDU の Web インターフェイスへのアクセスに使用するプロトコルモードとして HTTPS (SSL/TLS) を選択して、Secure Sockets Layer (SSL) を有効にします。HyperText Transfer Protocol over Secure Socket Layer (HTTPS) は、ユーザーからのページリクエストと Web サーバーからユーザーに返されるページの暗号化および復号化を行う Web プロトコルです。

Rack PDU では、SSL バージョン 3.0 と関連する TLS (Transport Layer Security) バージョン 1.0 をサポートしています。ほとんどのブラウザでは有効にする SSL のバージョンが選択できます。

SSL が有効な場合は、ブラウザに小さな鍵のアイコンが表示されます。 

SSL では、ブラウザでサーバー（この場合は Rack PDU）の認証が行えるよう、デジタル証明書が使用されます。ブラウザにより以下が確認されます。

- サーバー証明書のフォーマットが適切である。
- サーバー証明書の有効期限日時が有効期間内である。
- ユーザーがログオン時に指定した DNS 名または IP アドレスが、サーバー証明書の「Common Name」に一致する。
- サーバー証明書が信用のある証明機関によって署名されている。

大手のブラウザ製造元はそれぞれ、商用認証機関の CA ルート証明書をブラウザの証明書ストア（キャッシュ）に配信します。これによってサーバー証明書の署名と CA ルート証明書の署名を比較できます。

Rack PDU Security Wizard を使用すると、外部認証機関に送信する証明書署名リクエストを作成したり、また既存の認証機関を利用したくない場合にはブラウザの証明書ストア（キャッシュ）にアップロードする Dell ルート証明書を作成できます。また、このウィザードを使用すると、Rack PDU にアップロードするサーバー証明書を作成することもできます。

これらの証明書の使用方法についての要約は、デジタル証明書の作成とインストールを参照してください。
証明書および証明書リクエストの作成については、ルート証明書とサーバー証明書の作成とサーバー証明書と署名リクエストの作成を参照してください。

SSL では、多種のアルゴリズムや暗号化暗号も使用され、サーバーの認証、データの暗号化が行われ、データの保全性が確保されます。つまり、データは傍受されたり、別のサーバーによって送信されたりしません。

最近アクセスした Web ページは Web ブラウザのキャッシュに保存され、ユーザー名とパスワードを再入力せずに再度そのページにアクセスできます。コンピュータから離れるときは、必ずブラウザのセッションを終了してください。

デジタル証明書の作成とインストール

目的

パスワードの暗号化よりも高度なセキュリティが必要なネットワーク通信のために、Rack PDU の Web インターフェイスによってセキュアソケットレイヤー（SSL）プロトコルによるデジタル証明書の使用がサポートされています。デジタル証明書は、Rack PDU（サーバー）を Web ブラウザ（SSL クライアント）に対して認証することができます。

1024 ビットキーまたは 2048-ビットキーを生成できます。2048 ビットキーでは、より複雑な暗号化と高度なセキュリティが得られます。

次のセクションはデジタル証明書の作成、実装、使用の方法を要約したもので、ご使用のシステムにもっとも適切な手法を決定するための参考にしてください。

- 方法 1: Rack PDU によって自動生成されるデフォルト証明書を使用
- 方法 2: Rack PDU Security Wizard を使用して CA 証明書とサーバー証明書を作成
- 方法 3: Rack PDU Security Wizard を使用して、外部認証機関のルート証明書によって署名される証明書署名リクエストおよびサーバー証明書を作成

所属企業または組織が専用の認証機関を運営している場合は、方法 3 を選択することもできます。Rack PDU Security Wizard を同じように使用しますが、商用認証機関ではなく専用の認証機関を使用します。

システムに適した方法の選択

Secure Sockets Layer（SSL）プロトコルを使用している場合、次のデジタル証明書の使用方法から任意の方法を選択できます。

方法 1: Rack PDU によって自動生成されるデフォルト証明書を使用 SSL を有効にした場合は Rack PDU を再起動する必要があります。サーバー証明書が存在しない場合、Rack PDU は、自己署名されたデフォルトのサーバー証明書を再起動中に生成します。ただし、この証明書をユーザーが設定することはできません。

方法 1 には次の利点と欠点があります。

- **利点：**
  - この証明書が送信される前に、ユーザー名とパスワードおよび Rack PDU との間で送受信される全データが暗号化されます。
  - このデフォルトのサーバー証明書は、他の 2 つのデジタル証明書オプションのどちらかを設定するまでの間の暗号化ベースのセキュリティを提供するために使用できます。または、SSL による暗号化の利点を活用できることから、そのまま使用を続けることもできます。
- **欠点：**
  - Rack PDU はこの証明書を作成するのに最高で 1 分かかります。この間 Web インターフェイスは利用できません。（この待機時間は、SSL を有効にした後に初めてログオンする際に発生します。）
  - この方法には、CA 証明書（認証機関によって署名された証明書）によって提供される認証は含まれません。方法 2 および方法 3 には含まれます。ブラウザにはキャッシュされた CA 証明書は存在しません。したがって、Rack PDU にログインするときにブラウザでセキュリティアラートが生成されます。アラートでは、信用のある機関によって署名された証明書が利用できないということが示され、続行するかどうかの確認を要求されます。このメッセージを回避するには、Rack PDU へのアクセスが必要な各ユーザーのブラウザの証明書ストア（キャッシュ）にデフォルトサーバー証明書をインストールする必要があります。さらにユーザーは、Rack PDU にログオンするときは常に、サーバーの完全修飾ドメイン名を使用する必要があります。
  - デフォルトのサーバー証明書には、有効な「*Common Name*」（Rack PDU の DNS 名または IP アドレス）の代わりに Rack PDU のシリアル番号が記されています。そのため、Rack PDU はユーザー名、パスワード、アカウントの種類（例：**管理者**、**デバイスユーザー**、**読み取り専用ユーザー**）を使用して Web インターフェイスへのアクセスを制御できるものの、ブラウザはどの Rack PDU がデータを送信または受信しているのかを認証できません。
  - SSL セッションを開始するとき暗号化に使用される*公開キー*（RSA キー）の長さは、デフォルトでは 2048 ビットです。

方法 2: Rack PDU Security Wizard を使用して CA 証明書とサーバー証明書を作成

Rack PDU Security Wizard により次の 2 つのデジタル証明書を作成します。

- *CA ルート証明書*（証明機関のルート証明書）。この証明書は、Rack PDU Security Wizard で全サーバー証明書に署名するために使用されます。その後、Rack PDU へのアクセスを必要とする各ユーザーのブラウザの証明書ストア（キャッシュ）にインストールできます。
- Rack PDU にアップロードする *サーバー証明書*。Rack PDU Security Wizard でサーバー証明書が作成されると、CA ルート証明書を使用してそのサーバー証明書に署名が入れられます。

Web ブラウザは Rack PDU のデータ送信やデータ要求を次のように認証します。

- Rack PDU を特定するために、ブラウザは証明書作成時にサーバー証明書の「*distinguished name*」で指定された「*common name*」（Rack PDU の IP アドレスまたは DNS 名）を使用します。
- サーバー証明書が「信用のある」認証機関によって署名されていることを確認するため、ブラウザはサーバー証明書の署名とブラウザにキャッシュされているルート証明書の署名を比較します。有効期限日により、サーバー証明書が有効なものかどうかが確認されます。

方法 2 には次の利点と欠点があります。

- **利点：**
  - 証明書が送信される前に、ユーザー名とパスワード、および Rack PDU との間で送受信される全データが暗号化されます。
  - SSL セッションの設定時に、暗号化に使用される *公開キー*（RSA キー）の長さを選択します（デフォルト設定の 1024 ビット、または複雑な暗号でセキュリティレベルをより高度にするには 2048 ビットを使用します）。
  - Rack PDU にアップロードしたサーバー証明書により、データが正しい Rack PDU で送受信されていることが SSL で認証できます。これにより、ユーザー名、パスワード、送信データの暗号化を超える高いレベルのセキュリティが得られます。

- ブラウザにインストールしたルート証明書により、ブラウザでの Rack PDU のサーバー証明書の認証が可能になり、無許可アクセスからの保護が強化されます。

・**欠点：**
証明書には商用認証機関のデジタル署名が付けられていないため、各ユーザーのブラウザの証明書ストア（キャッシュ）に個別にルート証明書をロードする必要があります。（商用認証機関用のルート証明書は、方法 3 で説明されているように、ブラウザメーカーによりすでにブラウザの証明書ストア内に収納されています。）

方法 3: Rack PDU Security Wizard を使用して、外部認証機関のルート証明書によって署名される証明書署名リクエストおよびサーバー証明書を作成 Rack PDU Security Wizard により、認証機関に送信するリクエスト（.csr ファイル）を作成します。認証機関からは、リクエストで送信した情報に基づいて、署名入りの証明書（.crt ファイル）が返信されます。その後、Rack PDU Security Wizard によりサーバー証明書（.p15 ファイル）が作成されます。この証明書には、認証機関から返信されたルート証明書の署名が含まれます。サーバー証明書を Rack PDU にアップロードします。

所属企業または組織が専用の認証機関を運営している場合は、方法 3 を選択することもできます。Rack PDU Security Wizard を同じように使用しますが、商用認証機関ではなく専用の認証機関を使用します。

方法 3 には次の利点と欠点があります。

・**利点：**
- 証明書が送信される前に、ユーザー名とパスワード、および Rack PDU との間で送受信される全データが暗号化されます。
- ブラウザの証明書キャッシュにあるルート証明書にすでに署名した証明機関による認証であるという利点があります。（商用認証機関の CA 証明書は、ブラウザソフトウェアの一部として配布されます。自分の会社または機関の専用の認証機関は、各ユーザーのブラウザのブラウザストアに CA 証明書がすでにロードされているケースが多いでしょう）。したがって、Rack PDU へのアクセスを必要とする各ユーザーのブラウザにルート証明書をアップロードする必要はありません。

- SSL セッションの設定に使用される*公開キー*（RSA キー）の長さを選択します（デフォルト設定の 1024 ビット、または複雑な暗号でセキュリティレベルをより高度にするには 2048 ビットを使用します）。
- Rack PDU にアップロードしたサーバー証明書により、データが正しい Rack PDU で送受信されていることが SSL で認証できます。これにより、ユーザー名、パスワード、送信データの暗号化を超える高いレベルのセキュリティが得られます。
- ブラウザは、Rack PDU にアップロードしたサーバー証明書のデジタル署名を、ブラウザの証明書キャッシュに既存の CA ルート証明書の署名と比較します。これにより、無許可アクセスからの保護が強化されます。

・**欠点**：

- セットアップ時に、認証機関からの署名済みのルート証明書をリクエストするという追加の手順を実行する必要があります。
- 署名済み証明書の提供にあたり、外部認証機関から課金される場合があります。

ファイアウォール

一部の認証方式は他の方式に比べてはるかに強力なセキュリティを実現していますが、完全に安全なセキュリティ方式とは言い切れません。セキュリティの弱点を保護するためにも、適切に設定したファイアウォールを配置することが重要になります。

Rack PDU Security Wizard の使用

Rack PDU Security Wizard は、セキュアソケットレイヤー（SSL）と関連するプロトコル、暗号化ルーチンを使用している場合にネットワーク上の Rack PDU 用の高度なセキュリティのために必要とするコンポーネントを作成します。

証明書およびホストキーによる認証

*認証*機能は、ユーザーまたはネットワークデバイス（Rack PDU など）の ID を確認するものです。通常、コンピュータユーザーの識別はパスワードにより行われますが、ただし、ネット上でのより厳格なセキュリティ方式が要求されるトランザクションや通信の場合には、Rack PDU でも、さらに安全な認証方法をサポートしています。

- 安全な Web アクセスを行うための Secure Sockets Layer（SSL）では、認証にデジタル証明書を使用しています。デジタル *CA ルート*証明書は認証機関（CA）から公開キー基盤の一部として発行されるので、そのデジタル署名は Rack PDU のサーバー証明書のデジタル署名と一致しなれければなりません。
- Secure Shell（SSH）は、Rack PDU のコマンドラインインターフェイスへのリモートターミナルアクセスに使用されますが、認証には公開*ホストキー*を使用します。

証明書の使用方法 Rack PDU がサポートする全ブラウザを含め、大部分の Web ブラウザには、商用認証機関すべてからの CA ルート証明書のセットが含まれています。

サーバーの認証（この場合 Rack PDU）は、ブラウザからサーバーへの接続がなされるたびに行われます。ブラウザはサーバーの証明書に対して、ブラウザが既に認める認証機関による署名が確実に行われているかをチェックします。

認証は次の場合に行われます。

- SSL が有効な各サーバー（Rack PDU）で、サーバー自体にサーバー証明書が存在する場合。
- Rack PDU の Web インターフェイスへのアクセスに使用されるブラウザが、いずれもサーバー証明書を署名した CA ルート証明書を含んでいる場合。

認証に失敗すると、サーバー認証が失敗したが処理を続行するかどうかを尋ねるメッセージがブラウザに表示されます。

使用ネットワークでデジタル証明書からの認証が不要の場合、Rack PDU が自動生成するデフォルトの認証を使用することができます。デフォルト証明書のデジタル署名はブラウザでは認識されませんが、デフォルト証明書を使用することで、送信するユーザー名、パスワード、データ暗号化用に SSL が使用できるようになります。（デフォルトの証明書を使用する場合は、Rack PDU の Web インターフェイスにログオンする前に、認証を受けないアクセスに同意するかどうかのプロンプトが表示されます。

SSH ホストキーの使用方法 SSH *ホストキー*の認証機能は、SSH クライアントがサーバーと交信するたびに、サーバー（Rack PDU）の ID 認証を行います。SSH を有効にした各サーバーには、サーバー自体に SSH ホストキーが必要です。

SSL および SSH セキュリティのために作成するファイル

SSL および SSH セキュリティシステムのコンポーネントを作成するには、Rack PDU Security Wizard を使用します。

- Rack PDU のサーバー証明書（証明書から得られる認証の利点を利用したい場合）。作成できるサーバー証明書の種類は下記のとおりです。
  - Rack PDU Security Wizard で作成したカスタム CA ルート証明書からの署名付きサーバー証明書。所属企業や機関で専用の認証機関が確立されておらず、商用の認証機関を使用したサーバー証明書の署名を希望しない場合には、この方法を使用してください。
  - 外部認証機関からの署名付きサーバー証明書。この認証機関は、所属企業や機関の管理下の機関の場合と、商用の認証機関の場合（CA ルート証明書はブラウザソフトウェアの一部として配付されている）とがあります。
- サーバー証明書に必要な全情報（デジタル署名を除く）を含む証明書署名リクエスト。外部認証機関を使用している場合はこのリクエストが必要になります。
- CA ルート証明書。
- コマンドラインインターフェイスへのログオンの際に、Rack PDU の認証のために SSH クライアントプログラムが使用する SSH ホストキー。

Rack PDU Security Wizard で作成する SSL 認証の公開キーと SSH のホストキーを、1024 ビットの RSA キー（デフォルト設定）にするか、または複雑な暗号でセキュリティレベルがより高度な 2048 ビットの RSA キーにするかを定義します。

SSL サーバー証明書と SSH ホストキーを Rack PDU Security Wizard で作成せず、また使用もしない場合、Rack PDU は 2048 ビットの RSA キーを生成します。

Rack PDU セキュリティウィザードで作成したサーバー証明書、ホストキー、CA ルート証明書を使用できるのは、DellRack PDU 製品のみとなります。これらのファイルは、OpenSSL® や Microsoft® Internet Information Services（IIS）などの製品では作動しません。

ルート証明書とサーバー証明書の作成

サマリ

所属企業や機関で専用の認証機関が確立されておらず、商用の認証機関によるサーバー証明書の署名を希望しない場合は、この手順を使用してください。

Rack PDU Security Wizard で生成された証明書の一部である公開 RSA キーのサイズを定義します。1024 ビットのキーと、複雑な暗号でセキュリティレベルがより高度な 2048 ビットのキーを生成できます。（ウィザードを使っていない場合に Rack PDU により生成されるデフォルトキーは 2048 ビットです。）

- Rack PDU に使用されるすべてのサーバー証明書に署名する CA ルート証明書を作成します。このプロセス中には次 2 つのファイルが作成されます。
  - 拡張子が .p15 のファイル。これは暗号化ファイルで、認証機関の秘密キーと公開ルート証明書が含まれます。サーバー証明書の署名はこのファイルにより行われます。
  - ファイル拡張子が .crt のファイルには、認証機関の公開ルート証明書のみが含まれます。このファイルは、Rack PDU にアクセスする際使用する Web ブラウザにロードできます。ブラウザが行う Rack PDU のサーバー証明書確認がこれで可能になります。
- サーバー証明書を作成します。この証明書は、拡張子 .p15 のファイルに保存されます。このプロセス中、サーバー証明書に署名をする CA ルート証明書を求めるプロンプトが表示されます。
- サーバー証明書を Rack PDU にロードします。
- サーバー証明書が必要となる各 Rack PDU に対し、サーバー証明書を作成、ロードする作業を繰り返します。

作成手順

CA ルート証明書の作成

1. Rack PDU Security Wizard をご使用のコンピュータにインストールしていない場合は、インストールプログラム（Rack PDU Security Wizard.exe）を取得して実行します。
2. Windows の［スタート］メニューで、［プログラム］→ [Rack PDU Security Wizard] の順に選択します。
3. [Step 1] 画面で、作成するファイルの種類として [CA Root Certificate] を選択し、次に生成するキーの長さを選択します （デフォルト設定の 1024 ビットを使用するか、またはより複雑な暗号化と高度なセキュリティレベルを得るには 2048 ビットを使用してください）。
4. 認証機関の公開ルート証明書と秘密キーを格納するファイルの名称を入力します。このファイルの拡張子は .p15 となり、デフォルトでは、インストールフォルダである **C:\Program Files\Dell\Rack PDU Security Wizard** に作成されます。
5. [Step 2] 画面で、CA ルート証明書の設定に必要な情報を入力します。[Country] と [Common Name] のフィールドは必須です。他は任意で入力してください。[Common Name] フィールドには、会社または代理店を識別できる名前を入力します。英数字のみを使用し、スペースは入れないでください。

   デフォルトでは CA ルート証明書は作成の日付 / 時刻から 10 年間有効ですが、[Validity Period Start] と [Validity Period End] のフィールドは編集できます。

6. 次の画面では証明書のサマリを確認します。下向きにスクロールし、証明書の固有のシリアル番号とフィンガープリントを表示します。設定した情報に変更を加える場合は、[Back] をクリックして 情報を訂正します。

   証明書のサブジェクト情報と証明書の発行者情報は同一でなければなりません。

7. 最後の画面で、証明書が作成され、次の作業に必要な情報が表示されるか確認します。
   - サーバー証明書に署名する際に使用する .p15 ファイルの場所と名前。
   - .crt ファイルの場所と名前。このファイルは、Rack PDU またはデバイスへのアクセスが必要な各ユーザーのブラウザにロードする CA ルート証明書です。

ブラウザへの CA ルート証明書のロード Rack PDU にアクセスする必要のある各ユーザーのブラウザに .crt ファイルをロードします。

.crt ファイルをブウザの証明書ストア（キャッシュ）へロードする方法については、ブラウザのヘルプを参照してください。以下は Microsoft Internet Explorer での手順の要約です。

1. [ツール] を選択し、メニューバーから [インターネット オプション] を選びます。
2. ダイアログボックスの [コンテンツ] タブで、[証明書] をクリックしてから [インポート] をクリックします。
3. この後は、証明書インポートウィザードに表示される説明に従ってください。X.509 のファイルタイプを選択します。また CA 公開ルート証明書は、ルート証明書とサーバー証明書の作成の手順で作成した .crt の拡張子のファイルです。

SSL サーバーユーザー証明書の作成

1. Windows の [スタート] メニューで、[プログラム] → [Rack PDU Security Wizard] の順に選択します。
2. [Step 1] 画面で、作成するファイルの種類に [SSL Server Certificate]（SSL サーバー証明書）を選択してから、生成するキーの長さを選択します（デフォルト設定の 1024 ビット、または複雑な暗号でセキュリティレベルがより高度な 2048 ビットのいずれかを使用します）。
3. サーバー証明書と秘密キーを格納するこのファイルの名称を入力します。このファイルの拡張子は .p15 となり、デフォルトでは、フォルダ **C:\Program Files\Dell\Rack PDU Security Wizard** に作成されます。

4. [Browse] をクリックし、ルート証明書とサーバー証明書の作成の手順で作成した CA ルート証明書を選択します。CA ルート証明書により、生成中のサーバーユーザー証明書の署名が行われます。
5. [Step 2] 画面で、サーバー証明書の設定に必要な情報を入力します。[Country] と [Common Name] のフィールドは必須です。他は任意で入力してください。[Common Name] フィールドには、サーバー（Rack PDU）の IP アドレスまたは DNS 名を入力します。デフォルトでは、サーバー証明書は 10 年間有効ですが、[Validity Period Start] と [Validity Period End] のフィールドは編集することができます。

   構成情報も署名の一部になるため、構成情報が証明書ごとに一意である必要があります。サーバー証明書の設定を CA ルート証明書の設定と同一にすることはできません。（ただし、有効期限は一意の構成情報とはみなされません。その他の構成情報は異なっている必要があります。）

6. 次の画面では証明書のサマリを確認します。下向きにスクロールし、証明書の固有のシリアル番号とフィンガープリントを表示します。設定した情報に変更を加える場合は、[Back] をクリックして 情報を訂正します。
7. 最後の画面で証明書が作成されたことが確認できます。また、サーバー証明書を Rack PDU にロードするよう指示されます。サーバー証明書の場所と名前が表示されます。証明書にはファイル拡張子 .p15 が付き、Rack PDU の公開鍵と公開ルート証明書が含まれます。

サーバー証明書を Rack PDU にロードします。

1. [Administration] タブで、上部に表示されるメニューバーの [Network] オプションと左側ナビゲーションメニューの [Web] 項目下の [ssl certificate] オプションを選択します。

2. [Add or Replace Certificate File] を選択し、サーバー証明書、手順ルート証明書とサーバー証明書の作成で作成した .p15 ファイルを参照します。（デフォルトロケーションは **C:\Program Files\Dell\Rack PDU Security Wizard** です。）

サーバー証明書を転送する代わりに、FTP または Secure CoPy（SCP）を使用することができます。SCP の場合は、cert.p15 の名称の証明書を 156.205.6.185 の IP アドレスを使って Rack PDU に送信するコマンドは次のようになります。

```
scp cert.p15 dell@156.205.6.185
```

サーバー証明書と署名リクエストの作成

サマリ

所属企業・機関で専用の認証機関が確立されている、または商用の認証機関によるサーバー証明書の署名が必要な場合には、この手順を使用してください。

- 証明書署名リクエスト（CSR）を作成します。CSR には、デジタル署名を除くサーバー証明書の全情報が含まれます。このプロセスでは次の 2 つの出力ファイルが作成されます。
  - .p15 の拡張子のファイル（Rack PDU の秘密キーを格納）
  - 拡張子が .csr のファイル（外部認証機関に送信する証明書への署名リクエストを格納）
- 認証機関から署名付きの証明書を受信したら、この証明書をインポートします。証明書をインポートすると、秘密キーを含む .p15 ファイルと外部認証機関からの署名付き証明書を含むファイルが結合されます。この出力ファイルは暗号化された新規のサーバー証明書で、ファイル拡張子は .p15 になります。
- サーバー証明書を Rack PDU にロードします。
- サーバー証明書が必要となる各 Rack PDU に対し、サーバー証明書を作成、ロードする作業を繰り返します。

作成手順

証明書署名リクエスト（CSR）の作成

1. Rack PDU Security Wizard をご使用のコンピュータにインストールしていない場合は、インストールプログラム（Rack PDU Security Wizard.exe）を取得して実行します。
2. Windows の［スタート］メニューで、［プログラム］→［Rack PDU Security Wizard］の順に選択します。

3. [Step 1] 画面で、作成するファイルの種類に [Certificate Request] を選択してから、生成するキーの長さを選択します（デフォルト設定の 1024 ビット、または複雑な暗号でセキュリティレベルがより高度な 2048 ビットのいずれかを使用します）。
4. Rack PDU の秘密キーを格納するファイルの名称を入力します。このファイルの拡張子は .p15 となり、デフォルトでは、フォルダ C:¥Program Files¥Dell¥Rack PDU Security Wizard に作成されます。
5. [Step 2] 画面では、証明書署名リクエスト（CSR）の設定に必要な情報、すなわち署名付きのサーバー証明書に含めるべき情報を入力します。[Country] と [Common Name] のフィールドは必須です。他は任意で入力してください。[Common Name] フィールドには Rack PDU の IP アドレスまたは DNS 名を入力します。

   デフォルトではサーバー証明書は作成の日付 / 時刻から 10 年間有効ですが、[Validity Period Start] と [Validity Period End] のフィールドは編集することができます。

6. 次の画面では証明書のサマリを確認します。下向きにスクロールし、証明書の固有のシリアル番号とフィンガープリントを表示します。設定した情報に変更を加える場合は、[Back] をクリックして 情報を訂正します。

   証明書のサブジェクト情報と証明書の発行者情報は同一でなければなりません。

7. 最後の画面で証明書署名リクエストが作成されたことが確認できます。またファイルの場所と名前も表示されます（ファイルの拡張子は .csr です）。
8. 証明書署名リクエストを外部認証機関に送信します。認証機関は、商用認証機関、あるいは該当する場合には所属企業や機関が管理する認証機関のいずれかとします。

   サーバー証明書の署名および発行に関しては、認証機関からの説明を参照してください。

署名付き証明書のインポート 外部認証機関から署名付き証明書が返されたら、証明書をインポートします。署名付き証明書と秘密キーは、この手順により SSL サーバー証明書に統合されます。SSL サーバー証明書は後に Rack PDU にアップロードすることになります。

1. Windows の［スタート］メニューで、［プログラム］→ [Rack PDU Security Wizard] の順に選択します。
2. [Step 1] 画面で、作成するファイルの種類として [Import Signed Certificate] を選択します。
3. 外部認証機関から受信した署名付きサーバー証明書まで移動し、このファイルを選択します。このファイルの拡張子は .cer または .crt です。
4. 証明書署名リクエスト（CSR）の作成の作業の step 4 で作成したファイルに移動し、このファイルを選択します。このファイルには Rack PDU の秘密キーが含まれおり、拡張子は .p15 となっています。デフォルトでは、ファイルはインストールフォルダである **C:\Program Files\Dell\Rack PDU Security Wizard** に保存されます。
5. Rack PDU へアップロードする署名付きサーバー証明書となる出力ファイルの名称を指定します。このファイルのファイル拡張子は .p15 でなければなりません。
6. [Next] をクリックし、サーバー証明書を生成します。サマリ画面上の証明書の [Issuer Information] で、外部認証機関が証明書に署名したことが確認できます。
7. 最後の画面で証明書が作成されたことが確認できます。また、サーバー証明書を Rack PDU にロードするよう指示されます。サーバー証明書の場所と名前が表示されます。この証明書ファイルの拡張子は .p15 で、.cer または .crt ファイルから得た Rack PDU の秘密キーと公開キーが格納されています。

サーバー証明書を Rack PDU にロードします。

1. [Administration] タブで、上部に表示されるメニューバーの [Network] オプションと左側ナビゲーションメニューの [Web] 項目下の [ssl certificate] オプションを選択します。
2. [Add or Replace Certificate File] を選択し、サーバー証明書、手順ルート証明書とサーバー証明書の作成で作成した .p15 ファイルを参照します。（デフォルトロケーションは **C:\Program Files\Dell\Rack PDU Security Wizard** です。）

上記の代わりに、FTP または Secure CoPy（SCP）を介して Rack PDU にサーバー証明書を送信することもできます。SCP の場合は、cert.p15 の名称の証明書を 156.205.6.185 の IP アドレスを使って Rack PDU に送信するコマンドは次のようになります。

```
scp cert.p15 dell@156.205.6.185
```

SSH ホストキーの作成

サマリ

これは任意手順のため、省略できます。SSH 暗号化を選択してホストキーを作成しなかった場合は、再起動した時点で Rack PDU により 2048 ビットの RSA キーが生成されます。Rack PDU Security Wizard で作成する SSH のホストキーを、1024 ビットまたは 2048 ビットの RSA キーのどちらにするか定義します。

1024 ビットキーを生成することができます。または、複雑な暗号でセキュリティレベルがより高度な 2048 ビットキーを作成することができます。

- Rack PDU Security Wizard でホストキーを作成します。このキーは暗号化され、拡張子 .p15 のファイルに保存されます。
- ホストキーを Rack PDU にロードします。

作成手順

ホストキーの作成

1. Rack PDU Security Wizard をご使用のコンピュータにインストールしていない場合は、インストールプログラム（Rack PDU Security Wizard.exe）を取得して実行します。
2. Windows の［スタート］メニューで、［プログラム］→［Rack PDU Security Wizard］の順に選択します。
3. [Step 1] 画面で、作成するファイルの種類に [SSH Server Host Key] を選択してから、生成するキーの長さを選択します（デフォルト設定の 1024 ビット、または複雑な暗号でセキュリティレベルがより高度な 2048 ビットのいずれかを使用します）。
4. ホストキーを格納するファイルの名前を入力します。このファイルのファイル拡張子は .p15 でなければなりません。デフォルトの場合、ファイルはインストールフォルダである **C:\Program Files\Dell\Rack PDU Security Wizard** に作成されます。
5. [Next] をクリックし、ホストキーを生成します。
6. サマリ画面に、SSH バージョン 2 のフィンガープリントが表示されます。これらのフィンガープリントは各ホストキーに固有で、ホストキーを識別します。ホストキーを Rack PDU にロードした後、アップロードの合否は、SSH クライアントプログラムにより表示される Rack PDU の SSH のフィンガープリントがここで表示されたフィンガープリントと一致するかをチェックすることで確認できます。
7. 最後の画面で証明書署名リクエストが作成されたことが確認できます。また、Rack PDU ホストキーをロードするよう求められ、ファイル拡張子 .p15 であるホストキーのファイルの場所と名前が表示されます。

ホストキーを Rack PDU にロードします。

1. [Administration] タブで、上部に表示されるメニューバーの [Network] オプションと左側ナビゲーションメニューの [Console] 項目下の [ssh host key] オプションを選択します。
2. [Add or Replace Host Key] を選択し、ホストキー、手順ホストキーの作成で作成した .p15 ファイルを参照します。（デフォルトロケーションは **C:\Program Files\Dell\Rack PDU Security Wizard** です。）
3. [User Host Key] ページの下部に SSH フィンガープリントがあります。SSH クライアントプログラムにより Rack PDU にログオンし、これらのフィンガープリントがクライアントプログラムで表示されるフィンガープリントと一致することを確認して正しいホストキーのアップロードを確認します。

上記の代わりに、FTP または Secure CoPy（SCP）を介してホストキーファイルを Rack PDU に送信することもできます。SCP の場合は、hostkey.p15 の名称のホストキーを 156.205.6.185 の IP アドレスを使って Rack PDU に送信するコマンドは次のようになります。

```
scp hostkey.p15 dell@156.205.6.185
```

コマンドラインインターフェイスのアクセスとセキュリティ

管理者アカウントまたはデバイスユーザーアカウントを持つユーザーは、Telnet または Secure Shell（SSH）で（2 つのうちで有効になっている方で）コマンドラインインターフェイスにアクセスできます。（管理者は、Web インターフェイスから、[Administration] タブの上部メニューバーの [Network]、および左側ナビゲーションメニューの [Console] 項目下の [access] オプションを選択して、これらのアクセス方法のいずれかを有効にできます。）デフォルトでは、Telnet が有効です。SSH を有効にすると、自動的に Telnet が無効になります。

Telnet による基本アクセス Telnet はユーザー名とパスワードによる基本的な認証セキュリティを提供しますが、暗号化による高度なセキュリティには対応していません。

SSH による高度なセキュリティアクセス Web インターフェイスに SSL セキュリティを使用している場合、コマンドラインインターフェイスへのアクセスには Secure Shell（SSH）を使用します。SSH は、ユーザー名、パスワード、および伝送データを暗号化します。

SSH と Telnet のどちらを使用してコマンドラインインターフェイスにアクセスしても、インターフェイス、ユーザーアカウント、およびユーザーアクセス権限は同じですが、SSH を使用する場合は、まず SSH を設定し、使用するコンピュータに SSH クライアントプログラムをインストールする必要があります。

Telnet および Secure Shell（SSH）

SSH 有効中は、Telnet を使ってコマンドラインインターフェイスにアクセスすることはできません。SSH を有効にすると、SCP は自動的に有効になります。

SSH が有効で、そのポートが設定されている場合は、Secure CoPy（SCP）を使用するために必要な設定はほかにはありません。SCP では SSH と同じ環境設定が使用されます。

SSH を使用するには、SSH クライアントがインストールされている必要があります。Linux や他の UNIX® プラットフォームには SSH クライアントが含まれていますが、Microsoft Windows のオペレーティングシステムには含まれていません。SSH クライアントはさまざまなベンダーから入手可能です。

Telnet および Secure Shell（SSH）のオプションの設定：

1. Web インターフェイスの [Administration] タブ、上側メニューバーの [Network] メニューを選択して、左側のナビゲーションメニューの [Console] 項目下にある [access] オプションを使用します。
2. Telnet と SSH のポートを設定します。

   非標準ポートで提供される特別なセキュリティに関しては、ポートの割り当てを参照してください。

3. 左側ナビゲーションメニューの [Console] で [ssh host key] を選択し、あらかじめ Rack PDU Security Wizard で作成されたホストキーファイルを指定して Rack PDU にロードします。

   ここでホストキーファイルを指定しない場合、無効なホストキーをインストールした場合、またはホストキーをインストールしないで SSH を有効にした場合は、Rack PDU で RSA ホストキーが 2048 ビットで生成されます。Rack PDU でホストキーを作成するには、Rack PDU を再起動する必要があります。Rack PDU では、

このホストキーの作成に最長で 1 分かかります。この間 SSH にはアクセスできません。

代わりに、Windows オペレーティングシステムのコマンドフロンプトなどのコマンドラインインターフェイスから、FTP または Secure CoPy（SCP）を介してホストキーファイルを送信することができます。

4. SSH バージョン 2 の SSH ホストキーのための *フィンガープリント*を表示します。ほとんどの SSH クラアントでは、セッション開始時にフィンガープリントが表示されます。クライアントが表示した指紋は Web インターフェイスまたは Rack PDU. のコマンドラインインターフェイスで記録された指紋と比較されます。

Web インタ－フェイスからのアクセスとセキュリティ HTTP と HTTPS（SSL）

Hypertext Transfer Protocol（HTTP）ではユーザー名とパスワードでアクセスを指定しますが、通信中にはユーザー名、パスワード、データの暗号化を行いません。HTTPS（HyperText Transfer Protocol over Secure Sockets Layer）では、通信中にユーザー名、パスワード、データが暗号化され、デジタル証明書により Rack PDU の認証が行われます。

デジタル証明書を使用する際の複数の方法からの選択については、デジタル証明書の作成とインストールを参照してください。

HTTP および HTTPS の設定：

1. [Administration] タブ、上部メニューバーの [Network]、および左側ナビゲーションメニューの [Web] の下の [access] の順に選択します。
2. HTTP または HTTPS を有効にして、この 2 つのプロトコルがそれぞれ使用するポートを設定します。変更内容は次回のログオン以降に反映されます。SSL が有効になっていれば、ブラウザに小さな鍵のアイコンが表示されます。

非標準ポートで提供される特別なセキュリティに関しては、ポートの割り当てを参照してください。

3. 左側に表示されるナビゲーションメニューの [Web] の下にある [ssl certificate] を選択し、Rack PDU にサーバー証明書をインストールするかどうかを定義します。Rack PDU Security Wizard で証明書を作成したけれども、インストールしていない場合は、次のようになります。
   - Web インターフェイスで証明書ファイルが検索され、Rack PDU にアップロードされます。
   - 代わりに Secure CoPy（SCP）プロトコルまたは FTP を使用して、そのファイルを Rack PDU 上の場所に送信することができます。

   前もってサーバー証明書を作成またはアップロードしておくと、HTTPS の有効化に要する時間を削減できます。サーバー証明書をロードせずに HTTPS を有効にすると、再起動時に Rack PDU によって証明書が作成されます。**Rack PDU はこの証明書を作成するのに最長で 1 分かかります。この間 SSL サーバーは利用できなくなります。**

   Rack PDU が作成した証明書には一部制限があります。方法 1: Rack PDU によって自動生成されるデフォルト証明書を使用を参照してください。

4. 有効なデジタルサーバー証明書がロードされていれば、[Status] フィールドにリンクが表示されます。[Valid Certificate] このリンクをクリックすると、証明書のパラメータが表示されます。

パラメータ	説明
[Issued To]:	[Common Name (CN)]: Rack PDU. の IP アドレスまたは DNS 名。このフィールドは、Web インターフェイスへのログオン方法を制御します。 ・証明書が作成されたときにこのフィールドに IP アドレスが指定されていれば、IP アドレスを使用してログオンします。 ・証明書が作成されたときにこのフィールドに DNS 名が指定されていれば、DNS 名を使用してログオンします。 証明書用に指定してある IP アドレスまたは DNS 名をログオンの際に指定しないと認証は受けられません。この場合エラーメッセージが表示され、継続するかどうか確認されます。 デフォルトで Rack PDU によって生成されたサーバー証明書の場合、このフィールドには Rack PDU のシリアル番号が表示されます。 [Organization (O)]、[Organizational Unit (OU)]、および [Locality]、[Country]: サーバー証明書を使用する組織の名前、組織単位、ロケーションです。デフォルトで Rack PDU によって生成されたサーバー証明書の場合、[Organizational Unit (OU)] フィールドには、「Internally Generated Certificate (内部的に生成された証明書)」と表示されます。 [Serial Number]: サーバー証明書のシリアル番号です。
[Issued By]:	[Common Name (CN)]: CA ルート証明書に指定されたコモン名です。デフォルトで Rack PDU によって生成されたサーバー証明書の場合、このフィールドには Rack PDU のシリアル番号が表示されます。 [Organization (O)] および [Organizational Unit (OU)]: サーバー証明書を発行した組織の名前、組織単位です。デフォルトで Rack PDU またはデバイスによって生成されたサーバー証明書の場合、このフィールドには、「Internally Generated Certificate (内部的に生成された証明書)」と表示されます。
[Validity]:	[Issued on]: 証明書が発行された日時です。 [Expires on]: 証明書の有効期限終了日時です。

パラメータ	説明
[Fingerprints]:	2 つのフィンガープリントは双方とも長い英数文字のストリングで、コロン（:）で区切られています。このフィンガープリントは固有の識別子で、サーバーをさらに正確に認証するために使用されます。ブラウザで表示するときに証明書に含まれているフィンガープリントと比較するため、フィンガープリントを記録しておきます。 [SHA1 Fingerprint]: このフィンガープリントはセキュアハッシュアルゴリズム（Secure Hash Algorithm、SHA-1）により作成されます。 [MD5 Fingerprint]: このフィンガープリントは Message Digest 5（MD5）アルゴリズムにより作成されます。

サポートされている RADIUS の機能およびサーバー

サポートされている機能

サポート対象の認証と認証の機能： RADIUS（Remote Authentication Dial-In User Service）がサポートされています。RADIUS を使用して、それぞれの Rack PDU をリモートで集中的に管理します。ユーザーが Rack PDU にアクセスすると、認証リクエストが RADIUS サーバーに送信され、ユーザーのアクセス権レベルが判断されます。

アクセス権レベルの詳細については、ユーザーアカウントの種類を参照してください。

サポートされている RADIUS サーバー

サポート対象の RADIUS サーバー： FreeRADIUS と Microsoft IAS 2003 がサポートされています。その他の RADIUS アプリケーションについては、検証は行われていません。

Rack PDU の設定

認証

Rack PDU で使用される RADIUS ユーザー名は、32 文字以下に制限されています。

[Administration] タブで、一番上に表示されたメニューバーの [Security] を選択します。次に、左側ナビゲーションメニューの [Remote Users] で、[authentication] を選択して認証方法を決定します。

- [Local Authentication Only]: RADIUS が無効になり、ローカル認証が有効になります。
- [RADIUS, then Local Authentication]（RADIUS、ローカル認証の順）: RADIUS 認証とローカル認証の両方が有効になります。まず、RADIUS サーバーから認証が要求されます。ローカル認証は、RADIUS サーバーからの応答がない場合のみ使用されます。
- [RADIUS Only]（RADIUS のみ）: RADIUS が有効になり、ローカル認証が無効になります。

[RADIUS Only] が選択されているのに RADIUS サーバーを使用できない、正しく認識できない、または設定に不備があるといった場合、全ユーザーに対してリモートアクセスを利用できなくなります。この場合には、シリアル接続でコマンドラインインターフェイスにアクセスし、RADIUS のアクセス設定を **[local]** または **[radiusLocal]** に変更して再びアクセスできるようにしなければなりません。例えば、アクセス設定を **[local]** に変更する場合には次のコマンドを使用します。

```
radius -a local
```

RADIUS

RADIUS を設定するには、[Administration] タブの一番上に表示されるメニューバーで [Security] を選択します。次に、左側に表示されるナビゲーションメニューの [Remote Users] で、[RADIUS] を選択します。

設定	説明
[RADIUS Server]	RADIUS サーバーのサーバー名または IP アドレス **注意：** RADIUS サーバーは、デフォルトでは 1812 番ポートを使用してユーザー認証を行います。別のポートを使用するには、RADIUS サーバー名または IP アドレスの最後にコロンを追加し、その後に新しいポート番号を入力します。
[Secret]	RADIUS サーバーと Rack PDU の間の共有シークレット。
[Reply Timeout]	RADIUS サーバからの応答に対する Rack PDU の待ち時間（秒）
[Test Settings]	管理者のユーザー名とパスワードを入力して、設定した RADIUS サーバーのパスのテストを実行
[Skip Test and Apply]	RADIUS サーバーのパスのテストを省略

2 つの設定済みサーバーがリストされ [RADIUS, then Local Authentication] または [RADIUS Only] のいずれかの認証方法が有効な場合は、[Switch Server Priority] ボタンをクリックしてユーザーを認証する RADIUS サーバーを変更することができます。

RADIUS サーバーの設定

Rack PDU と共に使用するには RADIUS サーバーを設定する必要があります。このセクションの例は、お使いの RADIUS サーバーで必要な内容やフォーマットとは異なる場合があります。ここに挙げた例でアウトレットユーザーについて触れている場合は、アウトレットユーザーをサポートする Rack PDU デバイスにのみ該当します。

1. RADIUS サーバークライアントリスト（ファイル）に Rack PDU の IP アドレスを追加します。
2. 代わりに [Vendor Specific Attributes (VSAs)] が定義されていない限り、[Service-Type] 属性を設定する必要があります。[Service-Type] 属性を設定しなければ、リードオンリーのアクセスしかできません（Web インターフェイスのみ）。[Service-Type] の値は、管理者権限を設定する Administrative-User (6) と、デバイス権限を設定する Login-User (1) の 2 つです。

RADIUS ユーザーファイルについては、RADIUS サーバーのマニュアルを参照してください。

[Service-Type Attributes] の使用例

この RADIUS ユーザーファイルの例では、次のようになります。

- **RPDUAdmin** は **Service-Type Administrative-User, (6)** に対応
- **RPDUDevice** は **Service-Type: Login-User, (1)** に対応
- **RPDUReadOnly** は **Service-Type: null** に対応

```
RPDUAdmin       Auth-Type = Local, Password = "admin"
   Service-Type = Administrative-User

RPDUDevice      Auth-Type = Local, Password = "device"
   Service-Type = Login-User

RPDUReadOnly    Auth-Type = Local, Password = "readonly"
```

[Vendor Specific Attributes] の使用例

RADIUS サーバーから提供される [Service-Type] 属性に代わって、[Vendor Specific Attributes (VSAs)] を使用することができます。この手法には、辞書の項目と RADIUS ユーザーファイルが必要です。辞書ファイルでは、数値ではなく、キーワード ATTRIBUTE と VALUE の名前を定義することができます。この数値を変更すると、RADIUS の認証と権限付与が適切に機能しなくなります。VSAs は、標準の RADIUS 属性より優先されます。

辞書ファイル RADIUS 辞書ファイル（dictionary.dell）の例を次に示します。

```
#
# dictionary.dell
#
#
VENDOR    DELL 318
#
# Attributes
#
ATTRIBUTE DELL-Service-Type 1 integer DELL
ATTRIBUTE DELL-Outlets      2 string DELL

VALUE DELL-Service-Type Admin    1
VALUE DELL-Service-Type Device   2
VALUE DELL-Service-Type ReadOnly 3
#
# For devices with outlet users only
#
VALUE DELL-Service-Type Outlet   4
```

VSA を設定した RADIUS ユーザーファイル VSA を設定した RADIUS ユーザーファイルの例を次に示します。

```
VSAAdmin     Auth-Type = Local, Password = "admin"
             DELL-Service-Type = Admin

VSADevice    Auth-Type = Local, Password = "device"
             DELL-Service-Type = Device

VSAReadOnly Auth-Type = Local, Password = "readonly"
             DELL-Service-Type = ReadOnly

# Give user access to device outlets 1, 2 and 3.
VSAOutlet    Auth-Type = Local, Password = "outlet"
             DELL-Service-Type = Outlet,
             DELL-Outlets = "1,2,3"
```

次の関連トピックを参照してください。

- ユーザーアカウントの種類： ユーザー権限の 3 つの基本的なレベル（[Administrator]、[Device User]、[Read-Only User]）に関する情報
- サポートされている RADIUS サーバー： テストを行いサポートが確認されている RADIUS サーバーに関する情報

UNIX シャドウパスワードを設定した例 UNIX シャドウパスワードファイル（/etc/passwd）を RADIUS 辞書ファイルと共に使用した場合、ユーザーの認証には次の 2 つの認証方法が使用されます。

- すべての UNIX ユーザーに管理者権限が付与する場合、RADIUS の「ユーザー」ファイルに以下を追加します。デバイスユーザーのみを許可する場合は、Dell-Service-Type を **[Device]** に変更してください。

```
DEFAULT    Auth-Type = System
           DELL-Service-Type = Admin
```

- RADIUS の「user」ファイルにユーザー名と属性を加え、「/etc/passwd」に対してこのパスワードを確認します。以下はユーザー名「**bconners**」と「**thawk**」での例です。

```
bconners          Auth-Type = System
                  DELL-Service-Type = Admin
thawk             Auth-Type = System
                  DELL-Service-Type = Outlet
                  DELL-Outlets = "1,2,3"
```

索引

Numerics

あ

い

え

き

く

こ

さ

し

す

せ

た

て

と

ね

は

ひ

ふ

ほ

め

ゆ

り

る

ろ

B

C

D

E

F

H

I

J

L

N

O

P

R

S

T

U

W

X

Z

ユーザーズガイド

Managed Rack PDU

11/2010 パーツ番号 990-3926-018

www.dell.com | support.dell.com