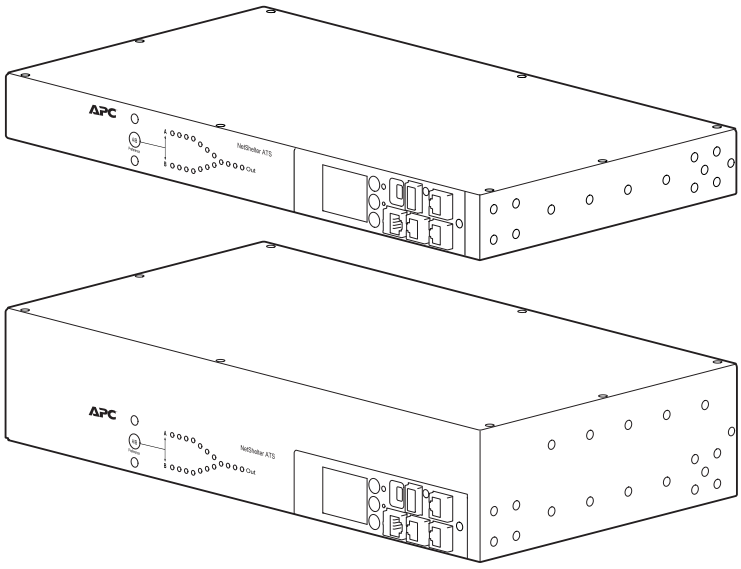
ネットワーク管理カード 3 搭載 Rack ATS

ユーザーズガイド

AP44XXA

990-91718C-018
リリース日：2025年9月



www.se.com

法律情報

本書に記載されている情報は、製品/ソリューションに関する一般的な説明、技術的特性、および推奨事項を含んでいます。

本書は、詳細な調査や運用/現場別の開発計画や概略図の代用となるものではありません。また、特定ユーザーの用途に対する製品/ソリューションの適合性または信頼性を判断するために使用すべきものではありません。関連する特定の用途または使用に関して製品/ソリューションの適切かつ包括的なリスク分析、評価、および試験を行うこと、または選択した専門家（インテグレーター、設計者等）に実施させることは、当該ユーザーの義務とします。

本書で言及されているシュナイダーエレクトリックブランドならびにシュナイダーエレクトリックSEおよびその子会社の商標は、シュナイダーエレクトリックSEまたはその子会社の所有物です。その他すべてのブランドは、各所有者の商標である場合があります。

本書およびその記載内容は、該当する著作権法で保護されており、情報提供のみを目的とし提供されています。本書のいかなる部分も、いかなる形式や手段（電子的、機械的、複写、記録、またはその他）によっても、どのような目的であっても、シュナイダーエレクトリックから書面による事前の許可を得ずに、再製または頒布することはできません。

シュナイダーエレクトリックは、「現状のまま」文書を調べる非独占な個人ライセンスを除き、本ガイドまたはその記載内容を商業的に使用する権利またはライセンスを付与することはありません。

シュナイダーエレクトリックは、本書の内容またはその形式に関して、いつでも予告なく変更または更新する権利を有します。

適用法により認められる範囲で、シュナイダーエレクトリックおよびその子会社は、本書の情報コンテンツの誤りや記入漏れまたは本書に含まれる情報の使用に起因する結果、もしくはその結果から生じる結果に関し、一切責任を負いません。

APC、APC ロゴ、Data Center Expert、EcoStruxure IT、NetShelter、および Powernet は、Schneider Electric SE またはその子会社の所有物です。その他の商標は各社に帰属します。

目次

重要な安全上の注意 —これらの指示を保存してください 9
安全に関する注意事項 10
概要 11
その他の文書 11
ユーザーのコメント 11
製品の特徴 12
内部保護対策 13
切り替え操作の仕組み 14
ユーザーアカウントの種類 15
ウォッチドッグ機能 16
ネットワークインターフェイスのウォッチドッグ機構 16
ネットワークタイマのリセット 16
ネットワークポート共有(NPS) 17
Display ID 17
NPSグループのインストール 17
ディスプレイ ID の個別割り当て 18
NPSによるファームウェアアップグレード 18
使用の開始 19
ネットワーク設定の確立 19
IPv4セットアップについて 19
IPv6設定について 20
TCP/IPの設定方法 20
.iniファイルユーティリティ 24
ファームウェアのアップデート 25
ファームウェアファイルの転送方法 25
ファームウェアアップデートユーティリティの使用 26
FTPまたはSCPを使用した単独のRack ATSのアップデート 27
XMODEMによる単独ラックATSのアップグレード 28
USBドライブを使用したファイルの転送とアップデート 28
複数のRack ATS Unitsの更新方法 29
NPSによるファームウェアアップグレード 29
アップグレードや更新の確認 30
転送結果の確認 30
前回の転送結果コード 30
インストールされたファームウェアのバージョンの確認 30
他のアプリケーションによるネットワーク管理 31
パスワードを忘れた場合 32
前面パネルの概要 33
デバイスステータスLED 34
ネットワークステータスLED 34
10/100/1000ステータスLED 34
LCDディスプレイ画面 35
デフォルト画面 36

メニュー画面 37
アラームステータスインジケータ 39
コマンドラインインターフェイス 40
CLIへのログオン 40
CLIへのローカルアクセス 40
CLIへのリモートアクセス 41
メイン画面について 42
CLIの使用方法 44
コマンド構文 45
コマンド応答コード 46
コマンド実行中のユーザー入力のプロンプト 46
コマンド編集 46
履歴 46
オートコンプリート 47
区切り文字 47
オプションと引数の入力 47
応答形式とメッセージコード 48
ネットワークマネジメントカードのコマンドの説明 49
? 49
about 51
alarmcount 51
boot 52
bye 53
cd 53
clrrst 53
console 54
date 55
delete 55
dir 56
dns 57
eapol 58
email 59
eventlog 61
exit 62
firewall 62
format 62
ftp 64
help 64
lang 64
lastrst 65
ldap 65
ledblink 69
logzip 69
netstat 70
ntp 70
ping 71
portSpeed 71

prompt 72
pwd 72
quit 72
radius 73
reboot 74
resetToDef 74
session 75
smtp 76
snmp 77
snmpv3 78
snmptrap 78
ssh 79
ssl 80
system 81
tacacs+ 83
tcpip 83
tcpip6 84
user 85
userauth 86
userdflt 86
web 87
whoami 88
wifi 88
xferINI 89
xferStatus 89
デバイスコマンドの説明 90
ネットワークポート共有コマンド 90
aboutATS 90
atsMeasure 91
atsStatus 91
bkLowLoad 92
bkNearOver 93
bkOverLoad 94
bkPeakLoad 95
bkReading 96
dispID 97
eventCounts 97
freqDeviat 98
frontPanel 99
湿度センサーの注意： 100
humAlGen 100
humHyst 101
humLow 102
humMin 103
humReading 104
humStatus 104
lcd 105
lcdBlink 105

lineVRMS 106
logToFlash 107
modbus 108
phLowLoad 109
phNearOver 109
phOverLoad 110
phPeakLoad 110
phReading 111
prodInfo 111
sensorName 112
sourceAName 112
sourceBName 113
sourcePref 113
温度センサーの注意： 114
tempAlGen 114
tempHigh 115
tempHyst 116
tempMax 117
tempPeak 118
tempReading 118
vMediumLimit 119
vNarrowLmt 120
vSensitvty 121
vWideLmt 122
vXferRange 123
Webユーザーインターフェイス 124
Web UIへのログオン 124
URLアドレスの形式 125
最初のログオン 125
Web UIの機能 126
タブ 126
Limited Status Access（限定ステータスアクセス） 126
デバイスステータスアイコン 127
クイックリンク 127
Web UI上のネットワークポート共有(NPS) 128
Homeタブ 129
Status（ステータス）タブ 130
NPSグループの表示 130
デバイスアラームの表示 131
デバイスステータスの表示 131
装置の状態の表示 132
負荷状態の表示 132
電力測定値の表示 133
環境ステータスの表示 133
ネットワークステータスの表示 134
Controlタブ 136
ユーザーセッションの管理 136

Web CLI 136
ネットワークインターフェイスのリセット 137
[Configuration]タブ 138
Rack ATSの設定 139
NPSグループの構成 139
Rack ATSの名前と場所の設定 140
優先電源の設定 140
切り替え動作の設定 141
負荷しきい値の設定 144
LCDディスプレイのオン/オフ切り替え 145
温度/湿度センサーの設定 145
セキュリティ設定の管理 147
ユーザーセッションの設定の管理 147
Ping応答の有効化 148
ローカルユーザー設定の管理 148
デフォルトのユーザー設定 150
リモートユーザー設定の管理 151
RADIUSサーバーの設定 152
ファイアウォールメニュー 153
802.1X セキュリティ設定 156
ネットワークの設定 157
プロトコル設定のまとめ 157
TCP/IPの設定およびIPv4とIPv6の通信設定 158
ネットワークポート速度の設定 160
DNSの設定 161
DNS設定のテスト 161
Webアクセスの設定 161
Webアクセス用のSSL証明書の設定 163
CLIアクセスの設定 163
SSHホストキーの設定 164
SNMPオプション 165
SNMPv1 166
SNMPv3 167
Modbus TCPの有効化 169
FTPサーバーの設定 169
AP9834でのWi-Fi設定 171
通知の設定 171
イベント別通知の設定 171
グループ別通知の設定 172
電子メール通知の設定 173
SNMPトラップ 175
全体システムの設定 177
IDの設定 177
日付、時刻、および夏時間の設定 178
設定ファイルを用いた設定の作成とインポート 179
クイックリンクの設定 179
ログの設定 180

Syslogサーバーの識別 180
システムログの設定 180
Syslogサーバーのテスト 181
[Tests]タブ 182
LCDライトの点滅設定 182
LEDライトの点滅設定 182
[Logs]タブ 183
イベントログの表示と設定 183
イベントログの表示 183
逆引き 184
ログサイズの変更 185
ネットワークポート共有のイベントログとトラップ 185
データログの表示と設定 185
Log 185
グラフ表示 186
ログ記録の間隔の設定 186
ローテーションの設定 187
データログサイズの指定 187
ファイアウォールのログ 188
FTPまたはSCPを使用したログファイルの取得 188
ログファイルをUSBフラッシュドライブにダウンロード 190
[About]タブ 191
Rack ATSについて 191
ネットワークについて 191
サポートリソース 192
環境設定値のエクスポート方法 193
手順の概要 193
.iniファイルの内容 193
.iniとネットワークポートの共有 193
詳細手順 194
.iniファイルの取得 194
.iniファイルの編集 195
1台のRack ATSにファイルを転送する 195
複数のRack ATS Unitsにファイルを転送します。 195
イベントのアップロードとエラーメッセージ 196
イベントとそのエラーメッセージ 196
Config.iniのメッセージ 196
上書きされた値によって生成されるエラー 196
関連のトピック 197
トラブルシューティング 198
アクセスに関する問題 198
SNMPの問題 199
ワールドワイドカスタマーサポート 200
ソースコードの著作権に関する注意 201

重要な安全上の注意 —これらの指示を保存してください

これらの指示を注意深く読み、機器をよく確認して、設置、操作、サービス、または保守を行う前に十分に理解してください。危険の可能性を警告するため、あるいは手順を明確にするまたは簡単にする情報に注意を促すため、次の特別メッセージが本マニュアル全体を通じ、または機器上に示されている場合があります。

「危険」または「警告」の安全ラベルにこの記号が追加されている場合、指示手順に従わないと、人体への危害につながる感電の危険が存在することを示します。

以下は安全警告記号です。これは、ユーザーに対して潜在的な人身傷害の危険を警告するために使用されます。この記号が付いたすべての安全メッセージに従い、けがや死亡の可能性を避けてください。

⚠危険

危険は危険となりうる可能性を示しており、回避措置を講じない場合は、死亡**または**重傷につながります。

上記の指示に従わないと、死亡または重傷を負うことになります。

⚠警告

警告は危険となりうる可能性を示しており、回避措置を講じない場合は、軽度**または**中度の怪我につながる恐れがあり ます。

上記の指示に従わないと、死亡、重傷、または機器の損傷を負う可能性があります。

⚠注意

注意 は危険となりうる可能性を示しており、回避措置を講じない場合は、軽度**または**中度の怪我につながる恐れがあり ます。

上記の指示に従わないと、負傷または機器の損傷を負う可能性があります。

注記

通知は、物理的な損傷に関連しない慣行に対処するために使用されます。この種類の安全メッセージには、安全警告記号を使用してはいけません。

上記の指示に従わないと、機器の損傷を負う可能性があります。

注意事項：

電気機器は、資格を持つ専門家によってのみ設置、操作、サービス、および保守を行う必要があります。この資料の使用に起因するいかなる結果についても、Schneider Electric は責任を負いません。

有資格者とは、電気機器の組立、設置、操作に関するスキルと知識を持ち、関連する危険を認識して回避するための安全訓練を受けた人のことです。

設置場所で施行されている現地の法律および規制を常に厳守してください。

安全に関する注意事項

⚠⚠危険

危険電圧

定格電圧外（ +/- 10％ ）でRack ATSを操作しないでください。電圧の制限と切り替え範囲は、切り替え動作のソフトウェアによる制御を表すものであり、使用する入力電圧を表すものではありません。

上記の指示に従わないと、死亡または重傷を負うことになります。

概要

Network Management Card 3 (NMC3)が搭載されたAPC™ Rack Automatic Transfer Switch (Rack ATS)は、サーバーなどの単一コードの設備に冗長電源を供給します。Rack ATSには2つの入力電源コードがあり、1次電源と2次電源の両方から接続された負荷機器に電力を供給します。主電源が利用できなくなったり、電源範囲外になった場合、Rack ATSは重要な負荷に影響を与えずに、二次電源から給電するように切り替えます。Rack ATSにはネットワーク接続が内蔵されており、Webユーザーインターフェース(Web UI)、コマンドラインインターフェース(CLI)、Data Center Expert™、EcoStruxure™ IT、またはSimple Network Management Protocol(SNMP)を介したリモート管理が可能です。

注記： Schneider ElectricのNetwork Management Card(NMC)を使用することで、Rack PDUをリモートで重要かつ安全に監視、管理できるようになります。

注記： 起動後にファームウェアを最新バージョンにアップデートします。Rack ATSファームウェアの最新バージョンについては、www.se.comを参照してください。ウェブサイトのホームページ(www.se.com)の検索バーに設備の型番を入力します。検索結果から目的の製品を選択して、その製品ページを開きます。製品ページのソフトウェアとファームウェアのタブを選択して、その製品で使用可能なファームウェアを表示させ、ダウンロードします。

その他の文書

このマニュアルの最新版および追加文書は、wwww.se.comから入手できます。

- 安全性に関するシート：Rack ATSの重要な安全情報が含まれます。
- 据付説明書：Rack ATSの据付および初期設定の手順について説明します。
- リリースノート：最新バージョンのファームウェアの新機能、修正済みの問題、既知の問題について説明します。
- セキュリティハンドブック：Network Management CardおよびNetwork Management Cardの内蔵コンポーネントを備えたデバイスのセキュリティ機能について説明します。

製品に関する文書をオンラインで検索するには、

1. Schneider Electricのダウンロードセンターwww.se.com/ww/en/downloadにアクセスしてください。
2. **Select location**をクリックして、リストからあなたのロケーションを選択します。

   注記： ロケーションを選択しない限り、文書をダウンロードできません。
3. 検索バーには、文書名、文書の部品番号または機器の部品番号を入力します。Enterキーを押すか、虫眼鏡アイコンをクリックして検索を開始します。
4. 検索結果から必要な文書をダウンロードします。必要な場合、ウェブページの左側にあるフィルタを選択して、検索結果を絞り込むことができます。

または、1つの製品に関するすべての文書をwww.go2se.com/ref=製品の部品番号 **> Documentation > Product Documentation**で参照できます。

ユーザーのコメント

この文書に関するご意見などをお待ちしております。www.se.comにお問合せください。

製品の特徴

Rack ATSは以下のような機能も備えています。

- 装置の前面パネルにあるLEDインジケータは、優先電源、過負荷電流、Web接続性などの動作状態を示します。これらの状態は、CLIおよびWeb UIを介して監視することもできます。
- ギガビットイーサネット接続。
- 各種のアクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー。(これらにはユーザー名とパスワードの要件があります。)
- ユーザーが最大4人同時にログインできる複数ユーザーログイン機能。
- イベントとデータロギング。イベントログには、Telnet、Secure CoPy (SCP)、ファイル転送プロトコル(FTP)、シリアル接続またはウェブブラウザ (SSL/TLSによるHTTPSアクセスまたはHTTPアクセス) によりアクセスできます。データログには、ウェブブラウザ、SCPまたはFTPによりアクセスできます。
- Rack ATSおよびNMCシステムイベントの重要度またはカテゴリに基づく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。
- WebおよびCLIインターフェイスを介した電源の監視と電源切り替えパラメータの設定機能。
- ビル管理システムがAutomatic Transfer Switch(ATS)を監視することを可能にするModbus TCPをサポートしています。
- 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
- 温度/湿度監視(APC温度/湿度センサAP9335Tおよび AP9335THが必要、付属していません)。
- 短絡に対する内部保護対策。(詳細については、内部保護対策, 13 ページを参照してください。)

  注記：各Rack ATS電源は常にダブルコンバージョンオンライン無停電電源装置(UPS)に接続することをお勧めします。
- ネットワークポート共有(NPS): Link AポートとBポートを使用して、最大32台のAP44XXAシリーズRack ATSユニットを接続することができるので、必要とされるネットワーク接続は1つのみです。
- NPSゲストファームウェアの自動更新機能を使用すると、NPSホストは接続されているゲストにファームウェアのアップデートを自動的に渡すことができます。

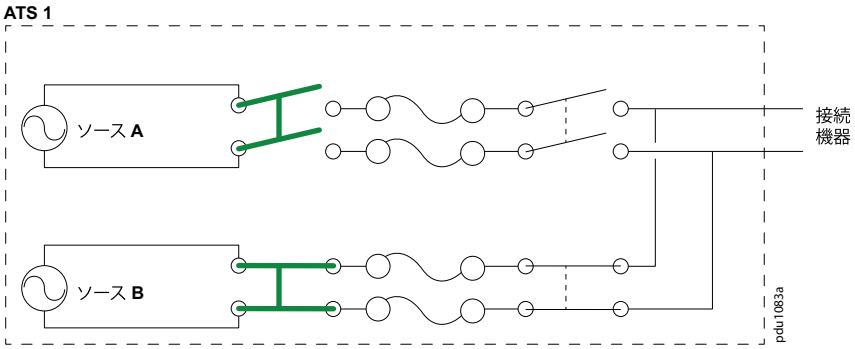
注記
ファームウェアをアップデートしてNPS機能を有効化します。

ファームウェアアップデートの手順については、ファームウェアファイルの転送方法, 25 ページを参照してください。

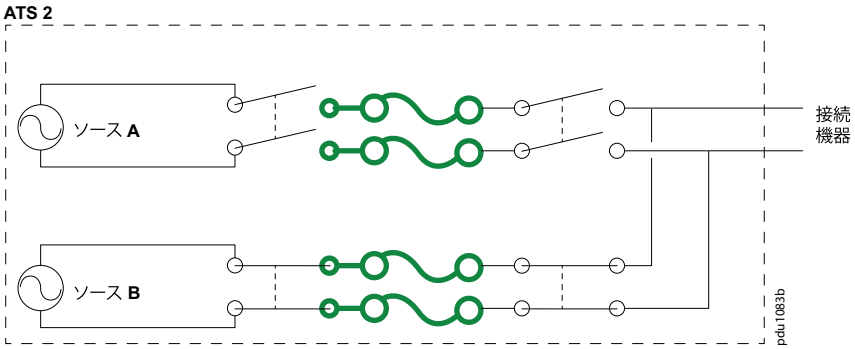
内部保護対策

Rack ATSユニットには、次の内部保護対策が含まれます。

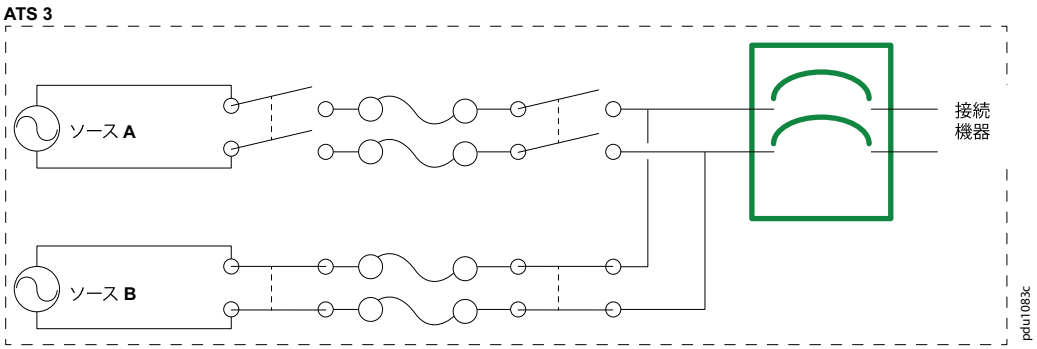
各モデルの入力リレーは、1つの入力コードから別のコードへの逆給電を防止するため、それぞれの電源の接続が切断されたときに開きます (ATS 1)。



2個または4個の交換不要のヒューズ (モデルにより異なる) がRack ATSを短絡から保護します (ATS 2)。



一部の2Uモデルには、バンクの過負荷から保護するため、単極または二極のサーキットブレーカが2個装備されています(ATS 3)。



Rack ATSでは、電源のサージ保護機能を備えていません。Rack ATSを外部の電力サージから保護するために、各Rack ATS電源を常にダブルコンバージョンオンライン無停電電源装置(UPS)に接続することをお勧めします。

切り替え操作の仕組み

切り替え動作は、複数のパフォーマンスパラメータによって決まります。これらは、ラインVRMS、切り替え電圧制限、切り替え範囲と感度です。これらのパラメータを調整して、Rack ATSが設備のニーズを満たす電力を受け入れるようにすることができます(詳細については、[Configuration]タブ, 138 ページを参照してください)。

- **ラインVRMS:** ご利用の設備に最適な電圧範囲です。許容可能なライン電圧はRack ATSモデルにより異なります(www.se.comにてご利用のRack ATSモデル用のスペックシートを参照してください)。
- **切り替え電圧制限**：Rack ATSが電源の切り替え前に許容する最大電圧と最小電圧です。切り替え電圧制限は小さくて許容可能な電力サージや電圧降下に対応する手段です。Rack ATSとご利用の設備の寿命が短くなる可能性があるため、Rack ATSを長時間、切り替え制限値付近で稼動させないでください。
- **切り替え範囲**：事前に定義された切り替え電圧制限のセットです。最大3つの切り替え範囲を設定できますが、一度に有効化できる切り替え範囲は1つのみです。
- **感度**：Rack ATSが電源を切り替えるかどうかを判断するための待機時間です。高感度は、繊細な設備のための反応性を更に高めます。低感度は、電源入力が変動しやすい場合に過剰な切り替えを防ぐのに役立ちます。

注記：切り替えプロセス全体は、高感度では最大10ミリ秒(ms)、低感度では12ミリ秒かかります。(これは、50 Hzと60 Hzの両方の電源に当てはまります。)

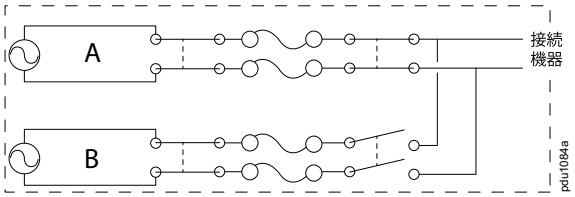
Rack ATSは電源Aと電源Bから供給される電力の電圧と周波数を継続的に監視します。どちらかの電源がパフォーマンスパラメーターの範囲外の電力を供給し始めた場合、Rack ATSはその電源を無効と見なします。次に、次の2つのいずれかが発生します。

1. 無効と見なされた電源が使用中でない場合、Rack ATSは冗長性が失われたことを示す警告を発します。
2. 無効と見なされた電源が使用中である場合、Rack ATSは他の利用可能な電源からの給電に切り替えます。

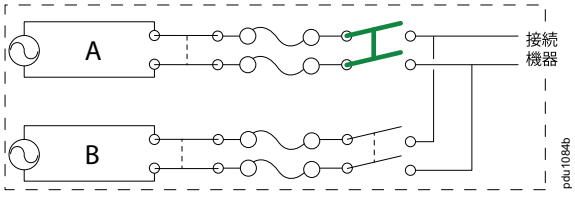
優先電源を設定した場合、Rack ATSは30秒間待機してその電源を監視します。30秒後、優先電源が再び使用可能になると、Rack ATSは優先電源に戻ります。

例：

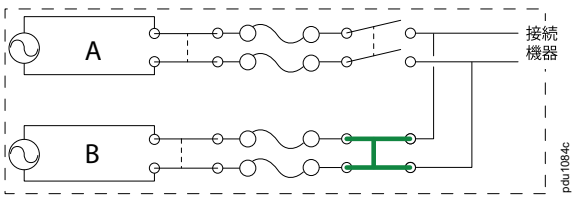
電源Aは接続設備に電力を供給し、電源Bは接続設備から分離されています。



ファームウェアは、電源Aがユーザー指定の切り替え範囲外であることを検出します。リレーを解除すると、電源Aからの電力が入力されなくなります。
これにより、異相切替が可能となり、リレー溶着の機会が大幅に減少します。
(最初のリレーは、入力電圧が低すぎる場合にのみ開きます) 。



電源Bのリレーが作動しています。電源Bは、接続されている機器に電力を供給します。



ユーザーアカウントの種類

Rack ATSにはさまざまなアクセスレベル（スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワークユーザー）があり、いずれもユーザー名とパスワードによって保護されています。最大4人のユーザーが同じRack ATSに同時にログインすることができます。

注記： 初めてスーパーユーザーのアカウントでRack ATSに接続すると、新しいパスワードを入力するように求められます。管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザーの各ユーザーアカウントはデフォルトで無効になっており、スーパーユーザーのデフォルトパスワード(**apc**)が変更されるまで有効にできません。

- 管理者またはスーパーユーザーは、Web UIの全メニューとCLIの全コマンドを使用できます。管理者ユーザータイプは削除できますが、スーパーユーザーは削除できません。スーパーユーザーと管理者のデフォルトのユーザー名とパスワードは、どちらも**apc**です。

  備考：このデバイスへ初めてアクセスするときは、スーパーユーザーアカウントのみを使用することをお勧めします。このレベルのアクセスを必要とする他の操作には、管理者アカウントを使用してください。

  備考：スーパーユーザーまたは管理者は、別の管理者のアカウントを管理できます（有効化、無効化、パスワードの変更など）。

- デバイスユーザーは、装置に関連する画面の読み取り/書き込みアクセス権を有しています。**[Security]**（セキュリティ）メニューの**[Session Management]**（セッション管理）や**[Logs]**（ログ）の**[Firewall]**（ファイアウォール）などの管理機能は使用できません。
- 読み取り専用ユーザーは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は使用できません。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。このアカウントのデフォルトのユーザー名は「**readonly**」、パスワードは「**apc**」です。
- ネットワーク専用ユーザー（リモートユーザー）は、Web UIおよびCLI（TelnetまたはSSH）を使用する場合のみログオンできます。ネットワーク専用ユーザーには、ネットワーク関連メニューへの読み取り/書き込みアクセス権しかありません。

ウォッチドッグ機能

内部の問題を検出し、予期しない入力から回復するために、Rack ATSはシステム全体をカバーするウォッチドッグ機構を内蔵しています。再起動して内部障害から復旧すると、[Network Interface Restarted]イベントがイベントログに記録されます。

ネットワークインターフェイスのウォッチドッグ機構

Rack ATSは、ネットワーク経由でのアクセスを確保できるように、内部ウォッチドッグ機構を実装しています。例えば、Rack ATSがネットワークトラフィックを受信しない状態が9.5分間続いた場合（SNMPのような直接送信、またはアドレス解決プロトコル[ARP]リクエスト）のような一斉送信のどちらの場合でも）、ネットワークインターフェイスに問題があると判断され再起動されます。ネットワークインターフェイスのウォッチドッグ機構は、起動時にアクティブなネットワークインターフェイス接続が検出されたRack ATSでのみ有効になります。

ネットワークタイマのリセット

ネットワークトラフィックが9.5分間途絶えたという理由だけでRack ATSが再起動しないように、Rack ATSは4.5分間隔でデフォルトゲートウェイへの通信を試みます。ゲートウェイが存在する場合は、Rack ATSに応答があり、9.5分間のタイマーが再起動します。ゲートウェイがない場合やアプリケーションがゲートウェイを必要としない場合は、同一サブネット上に存在しネットワークで動作しているコンピュータのIPアドレスを指定してください。このコンピュータのネットワークトラフィックにより9.5分枠のタイマが定期的にリセットされ、Rackが頻繁に再起動しないようになります。

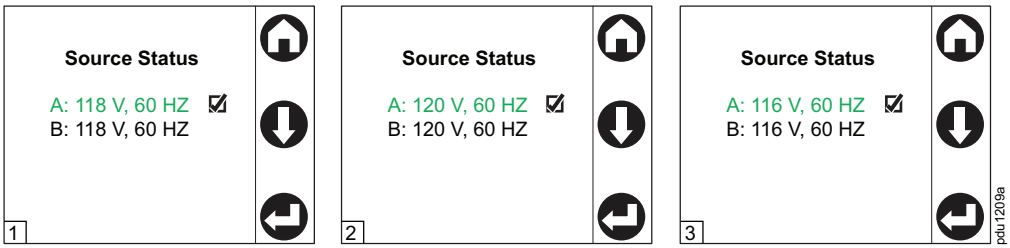
ネットワークポート共有(NPS)

ネットワークポート共有機能を使用すると、1つのネットワーク接続だけを使用して最大32台のRack ATS ユニットのステータスの表示、設定、管理ができます。これは、各ユニットの前面パネルにあるLink AとBポートを使用して、Rack ATS ユニットを接続することで可能になります。

注記： グループ内のすべてのRack ATSユニットがAP44XX**A**シリーズに含まれている必要があります。NPSホストATSは、独自のファームウェアバージョンを各ゲストで見つかったバージョンと比較します。バージョンが異なる場合、ホストはNPSチェーンを使用してファームウェアを非準拠ゲストにコピーします。

Display ID

Display IDは1 ~ 32の番号で、グループ内のRack ATSユニットを一意に識別するために使用されます。2つ以上のRack ATSユニットがNPSグループ内で相互に接続された後、これらのユニットは、この“Display ID”を使用してさまざまなインターフェイスで識別できます。このDisplay IDは、LCDディスプレイの左下隅に表示できます。



NPSグループのインストール

備考：通信に関する問題を減らすには、グループ内のATSユニットを接続するケーブルの最大合計長(Cat5e+)が10メートルを超えないようにしてください。

備考：NPSグループ内の1つのRack ATSのみをホストとして許可します。2つのホストユニットが接続されている場合、1つは自動的にNPSグループのホストに選択されます。ゲストユニットにアクティブなネットワークリンクがある場合は、そのゲストを選択してホストにすることができます。

NPSグループの詳細については、「NPSグループの構成, 139 ページ」を参照してください。

各ユニットの前面パネルにあるLink AおよびBポートを使用して、最大32台のRack ATSユニットを接続します。ユニットに任意の順序(1から32)で手動で電源を入れることで特定のDisplay IDを割り当てることができます。

1. グループに接続されたRack PDUのいずれかに電源を投入する前に、ディスプレイIDの順序を決定してください。
2. ディスプレイID 1が必要なユニットの電源を最初に入れます。
3. そのユニットが初期化され、LCD画面の表示が開始したら、ディスプレイID 2を割り当てるユニットの電源を入れます。
4. 残りのユニットも同じように設定します。
5. グループ化されたRack ATSユニットのネットワークポートをネットワークハブまたはスイッチに接続します。このユニットがRack ATSグループのホストになります。ゲストATSのデータは、ホストATSで表示できます。「ネットワーク設定の確立, 19 ページ」で指定されているように、このホストRack ATSのネットワーク機能を設定します。ホストATSは、Link AおよびBポートを介して接続されているゲストATSユニットを自動的に検出します。

これでRack ATSグループはホストユニットのIPアドレスから利用できるようになりました。必要に応じて、SNMP OID `ats5gIdentConfigModuleID`を使用してNPS IDを変更できます。ホストユニットは、**Configuration > ATS > Groups**で変更できます。

ホストRack ATSは、NPSゲストでサポートされていない多くの機能をサポートしています。以下が含まれますが、これらに限定されません。

- SNMP ats5g Group OIDs
- ゲストATSユニットのAOS/APPファームウェア更新を開始しています

- ゲストATSユニットの時間同期
- ゲストATSユニットのデータロギング

ディスプレイ ID の個別割り当て

グループ内の Rack ATS の電源を入れる前に、以下の指示に従ってください。

ディスプレイ ID を特定の順序で割り当てたい場合は、最初にユニットの電源を 1 ~ 32 の希望の順序で投入することでこれを実現できます。以下に例を示します。

1. グループに接続された Rack ATS の電源を入れる前に、希望するディスプレイ ID の順序を決定してください。
2. 最初に、ディスプレイ ID 1 にしたいユニットの電源を入れます。
3. そのユニットが初期化され、LCD が画面表示を開始した後、ディスプレイ ID 2 にしたいユニットの電源を入れます。
4. 他のユニットも、必要に応じて同じ手順で続けます。

注記： ディスプレイ ID は、CLI インターフェースから dispID コマンドを使用してのみ設定できます。

NPSによるファームウェアアップグレード

起動時および定期的な運用中に、NPSホストは独自のファームウェアバージョンを各ゲストのバージョンと比較します。バージョンが異なる場合、ホストはNPSチェーンを使用してファームウェアを非準拠ゲストにコピーします。

注記： この機能を使用するには、NPSホストとゲストの両方で常駐ファームウェアサポートが必要であるため、自動ファームウェアアップグレードはAP44XX **A** Series Rack ATSユニットでのみ使用できます。この機能を使用するには、NPSチェーンの正しい動作を維持するために、交換用Rack ATSユニットもAP44XX**A**シリーズモデルである必要があります。

使用の開始

Rack ATSの使用を開始するには、次の手順を実行します。

1. www.se.com/ww/en/downloadから入手できるインストール/クイックスタートマニュアルを使用してRack ATSを設置します。
2. 電源を投入してご利用のネットワークに接続します。据付マニュアルの指示に従ってください。
3. ネットワーク設定を行います。ネットワーク設定の確立, 19 ページを参照してください。
4. ATSのファームウェアをアップデートします。詳細については、次のを参照してください。ファームウェアのアップデート, 25 ページ.
5. 次のいずれかのインターフェイスでRack ATSの使用を開始します。
   - 表示パネル。前面パネルの概要, 33 ページを参照してください。

     注記：前面パネルではRack ATSの設定を表示できますが、設定を行うことはできません。
   - CLI。コマンドラインインターフェイス, 40 ページを参照してください。
   - Web UI。Webユーザーインターフェイス, 124 ページを参照してください。

ネットワーク設定の確立

EcoStruxure Data Center Expert™ (DCE) は、DCEプライベートネットワークで検出されたSNMPv1デバイス用のDHCP設定を提供します。Rack がDCEプライベートネットワークに接続されている場合は、このセクションを無視してDCEで[**Private (LAN2) DHCP Discovery**]タブからIPアドレスを指定できます。詳細については、DCEのマニュアルを参照してください。

注記： Rack ATSでSNMPv1を有効にする必要があります。CLIへのローカル接続を確立し(CLIへのローカルアクセス, 23 ページ)、`snmp`コマンドを使用してSNMPv1 (snmp, 77 ページ)を有効にします。

IPv4セットアップについて

ネットワークで動作させるには、Rack ATSに次の3つのTCP/IP設定を定義する必要があります。

- Rack ATSのIPアドレス
- Rack ATSのサブネットマスク
- デフォルトゲートウェイのIPアドレス (ネットワークセグメントを使用しない場合のみ必要)

  デフォルトゲートウェイがない場合は、Rack ATS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アドレスを使用してください。トラフィックが非常に少ない場合、Rack ATS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した。

  備考：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として使用しないでください。これを行うと、Rack ATSのネットワーク接続が無効になります。ネットワーク接続を再度有効にするには、シリアル接続を用いてログオンし、TCP/IPをデフォルト値にリセットする必要があります。

DHCPサーバーを使用してRack ATSのTCP/IPを設定する方法については、TCP/IPの設定およびIPv4とIPv6の通信設定, 158 ページの「**DHCP応答オプション**」を参照してください。

IPv6設定について

IPv6ネットワークでは、ユーザーの要求に適応するフレキシブルな設定が実行できます。IPv6は、このインターフェイスでIPアドレスを入力可能なところであればどこでも使用することができます。IPv6は、CLI、Web UI、またはDHCPを使用して設定できます。

TCP/IPの設定方法

次のいずれかの方法で、Rack ATSに必要なTCP/IPを設定します。

- BOOTPまたはDHCPサーバ (DHCP および BOOTP の構成, 21 ページを参照してください)。

  注記 : DHCPは、Rack のデフォルトのネットワーク設定方法です。ほとんどのネットワークはDHCPサーバーで構成されています。

- CLI (CLIへのローカルアクセス, 23 ページまたはCLIへのリモートアクセス, 23 ページを参照してください)。
- デバイスIP設定ウィザード (デバイスIP設定ユーティリティ, 20 ページを参照してください)。

  注記 : SNMPはデフォルトで無効になっており、デバイスIP設定ユーティリティを機能させるにはこれが有効になっている必要があります。CLIからSNMPを有効化することができます。

- .iniファイルを使用して、設定済みのRack から1つまたは複数の未設定のRack ATSに.iniファイルの設定をエクスポートできます。Web UIからこの操作を行うには、**[構成] > [全般] > [ユーザー構成ファイル]** に移動します。.iniファイルの編集に関する詳細なオプションおよび手順については、環境設定値のエクスポート方法, 193 ページを参照してください。

デバイスIP設定ユーティリティ

SNMPはデフォルトで無効になっており、デバイスIP設定ユーティリティを機能させるにはこれが有効になっている必要があります。CLIからSNMPを有効化することができます。(CLIへのアクセス手順については、CLIへのローカルアクセス, 23 ページを参照してください。snmpを有効化する手順については、snmp, 77 ページを参照してください。)

デバイスIP設定ユーティリティは、IPアドレスが割り当てられていないRack ATS unitsを検出することができます。検出されると、Network Management Card(NMC)のIPアドレス設定を構成できます。また、IP範囲を入力して検索を定義することで、ネットワーク上にすでに存在するデバイスを検索することもできます。このユーティリティは、指定された範囲でIPアドレスをスキャンして、すでにDHCPによって割り当てられたIPアドレスを持つRack ATS unitsを検出します。

注記 :

- このウィザードの詳細については、FAQの*How do I configure APC Network Management Card network settings?* (*APC Network Management Card*のネットワークを設定するには？) を参照してください。(FA156064)。
- DHCPオプション12の使用方法については、*Which DHCP options are used when an APC Network Management Device makes a DHCPv4 request?* (*APC*ネットワーク管理デバイスが*DHCPv4*リクエストのために使用する*DHCP*オプション) の*FAQ*記事を参照してください (FA156110)。
- FAQ記事を検索するには、www.se.comに進み、あなたのロケーションを選択します。次に、**サポート > 文書とソフトウェアのダウンロード**を選択して、検索バーにFAQ記事の番号またはタイトルを入力します。

システム要件

デバイスIP設定ユーティリティは、Microsoft® Windows® 2000、Windows Server® 2003、Windows Server 2012と、32ビットおよび64ビット版のWindows XP®、Windows Vista®、Windows 2008、Windows 7、Windows 8、およびWindows 10オペレーティングシステムで実行されます。デバイスIP設定ユーティリティは、ファームウェアバージョンが3.0.xまたはそれ以降のNetwork Management Cardをサポートしており、IPv4専用です。

デバイスIP設定ユーティリティのインストール

1. www.se.com/ww/en/downloadのダウンロードセンターにアクセスし、**Select location**をクリックして、表示されたオプションからあなたの国を選択します。
2. 検索バーに「Network Management Cardのデバイス IP設定ユーティリティ」を入力します。Network Management Cardのデバイス IP設定ユーティリティの最新バージョンをダウンロードします。
3. .zipファイルをデスクトップに展開し、実行ファイル(*DevIPSetup.exe*)を実行します。

   注記：**Start a Web browser when finished**（**終了後ウェブブラウザを起動**）オプションを有効のままにした場合、ブラウザからRack ATSにアクセスするためにユーザー名とパスワードの両方に**apc**を使用することができます。

インストールが完了すると、デバイスIP設定ユーティリティがWindowsの**スタート**メニューオプションから利用できるようになります。

DHCP および BOOTP の構成

デフォルトの TCP/IP 構成設定である **DHCP**は、適切に構成された DHCP サーバーが存在し、Rack ATSに TCP/IP 設定を提供できることを前提としています。BOOTP の設定を構成することもできます。

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。

BOOTP または DHCP サーバーを設定した後、CLI にログインして（操作手順をCLIへのローカルアクセス, 23 ページ参照）、Rack Monitor 250 に割り当てられた IP アドレスを確認できます（操作手順を手順をCLIでのTCP/IP設定の表示または設定, 24 ページ参照）。

DHCPサーバ環境設定

RFC2131/RFC2132 に準拠した DHCP サーバーを使用して、Rack ATSの TCP/IP 設定を構成することができます。

1. Rack ATS は、以下を使用して自らを識別する DHCP リクエストを送信します:
   - ベンダークラス識別子（デフォルトでは APC）
   - クライアント識別子（デフォルトでは、Rack ATSの MAC アドレス）
   - ユーザークラス識別子（デフォルトでは、Rack ATS 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情報）
   - ホスト名（デフォルトでは、Rack ATS のシリアル番号の末尾 6 桁を使用した apcXXYYZZ 形式）。これは DHCP オプション 12 として知られています。

2. 適切に構成された DHCP サーバーは、Rack ATS がネットワーク通信に必要とするすべての設定を含む DHCP オファーで応答します。DHCP オファーには、ベンダー固有情報オプション（DHCP オプション 43）も含まれます。Rack ATSは、以下の 16 進数形式で APC クッキーを DHCP オプション 43 にカプセル化していない DHCP オファーを無視するように構成することができます。（Rack ATS は、デフォルトではこのクッキーを必要としません。）

   オプション43 = 01 04 31 41 50 43

   - 最初のバイト（01）はコードです。
   - 2 番目のバイト（04）は長さです。
   - 残りのバイト（31 41 50 43）は APC クッキーです。ベンダー固有情報オプションにコードを追加する方法については、使用している DHCP サーバーのドキュメントを参照してください。

     注記：Web UI の **Require vendor specific cookie to accept DHCP Address** と、DHCP サーバーが Rack ATSに情報を提供する「APC」クッキーを必ず提供するよう要求できます。

サポートされている DHCP オプションの詳細については、TCP/IPの設定およびIPv4とIPv6の通信設定, 158 ページを参照してください。

BOOTPサーバ環境設定

Rack ATS が BOOTP サーバーを使用して TCP/IP 設定を構成するには、適切に構成された RFC951 準拠の BOOTP サーバーを検出する必要があります。

1. BOOTP サーバーの BOOTPTAB ファイルに、Rack ATS 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ブートアップ ファイル名を入力します。Rack ATSの MAC アドレスは、本体底面に記載されていますので確認してください。
2. シリアル接続を使用して CLI にアクセスし、-b <bootp>BOOTPを有効にするには。デフォルトのユーザー名とパスワードは、どちらも**apc**です。

   CLI へのアクセス方法の詳細については、CLIへのローカルアクセス, 23 ページ を参照してください。
3. Rack ATS を再起動するには、–y –Y を入力します。

   Rack ATS が再起動すると、BOOTP サーバーが TCP/IP 設定を提供します。

   - ブートアップファイル名を指定した場合、Rack ATS は BOOTP サーバーからそのファイルを TFTP または FTP を使用して転送しようとします。Rack ATSは、ブートアップファイルに指定されたすべての設定を適用します。
   - ブートアップファイル名を指定しなかった場合は、Rack ATS のその他の設定を Web UI または CLI を通じてリモートで構成できます。両方のインターフェースのデフォルトのユーザー名とパスワードは**apc**です。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。

CLIへのローカルアクセス

ローカルアクセスのために、コンソールポートを介してRack ATSに接続されているコンピュータを使用してCLIにアクセスします。

注記： この手順では、仮想COMポート(VCP)ドライバがコンピュータにインストールされていることを前提としています。必要な場合、ftdichip.comからご利用のオペレーティングシステム用のVCPドライバをダウンロードしてインストールします。

1. オペレーティングシステムの指示に従い、アプリケーションを開いてコンピュータのCOMポートを確認します。（Windowsオペレーティングシステムでは、ポートをデバイスマネージャで表示できます）。
2. マイクロUSBケーブルを使用して、Rack ATSのコンソールポートをコンピュータのUSBポートに接続します。

   新しく占有されたシリアルCOMポートがポート表示アプリケーションに表示されるはずです。ポート番号をメモするか、必要に応じてポートを割り当て直します。
3. ターミナルプログラム（TeraTermやPuTTYなど）を起動し、選択したシリアルCOMポートを9600bps、8データビット、パリティなし、1ストップビット、フロー制御なしに設定します。このポートでRack ATSにシリアル接続します。
4. ENTERキーを最大3回押して、ユーザー名のプロンプトを表示します。次に、ユーザー名とパスワードを入力します。

   デフォルトでは、スーパーユーザーのユーザー名とパスワードは両方とも**apc**となっています。これが初めてのログオンなら、デフォルトのパスワードを変更するように求められます。会社のパスワード要件を満たす強力なパスワードを使用することをお勧めします。

初めてネットワーク設定を行う場合は、CLIでのTCP/IP設定の表示または設定, 24 ページを参照して設定を完了してください。

CLIへのリモートアクセス

Rack ATSと同じネットワーク上にある任意のコンピュータから、ARPとPingを使用してRack ATSにIPアドレスを割り当て、SSHまたはTelnetを使用してRack ATSのCLIにアクセスし、他のTCP/IP設定を行います。デフォルトでは、はSSHを有効にし、Telnetは無効になっています。

注記： Rack ATSのIPアドレス設定後は、SSHまたはTelnetを使用してRack ATSにアクセスできます。最初にARPおよびPingを使用する必要はありませんが、CLIの初期設定にはSSHが必要です。**console**コマンドを使用して、SSHまたはTelnetを有効または無効にすることができます。必要に応じて、Web UIを使用してSSHまたはTelnetを有効または無効にすることもできます。

1. ARPを使用して、Rack ATSのIPアドレスを定義し、ARPコマンド内でRack ATSのMACアドレスを使用します。例えば、00 c0 b7 63 9f 67のMACアドレスを持つRack ATSのIPアドレスを156.205.14.141に定義するには、次のいずれかのコマンドを使用します。
   - Windowsのコマンド形式：
     `arp -s 156.205.14.141 00-c0-b7-63-9f-67`
   - LINUXのコマンド形式：`arp -s 156.205.14.141 00:c0:b7:63:9f:67`

     備考：MACアドレスは、Rack ATSの底面にあります。
2. ARPコマンドで設定したIPアドレスの割り当てには、113バイトのPingを使用します。例えば次のようになります。
   - Windowsのコマンド形式：`ping 156.205.14.141 -l 113`
   - LINUXのコマンド形式：`ping 156.205.14.141 -s 113`
3. SSHまたはTelnetを使用して、Rack ATSに新たに割り当てたIPアドレスでアクセスします。(例： `telnet 156.205.14.141`)ユーザー名とパスワードには**apc**を使用します。

設定を完了するには、CLIでのTCP/IP設定の表示または設定, 24 ページを参照してください。

CLIでのTCP/IP設定の表示または設定

DHCPまたはBOOTPを介して割り当てられたIPアドレスを表示するには、

1. CLIにログオンします。
2. IPv4アドレスを表示するには、`tcpip`を入力します。

   IPv6アドレスを表示するには、`tcpip6`を入力します。

TCP/IPv4設定を手動で割り当てるには、

1. CLIにログオンします。
2. ネットワーク管理者に連絡し、Rack ATS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. ネットワーク設定を行うために3つのコマンドを使用します。(斜体のテキストは変数を示します) 。

   `tcpip -i yourIPaddress`
   `tcpip -s yourSubnetMask`
   `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を設定するには、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`。

   注記：また、次のように3つのコマンドオプションをすべて同じ行に入力することもできます。
   `tcpip -i yourIPaddress -s yourSubnetMask tcpip -g yourDefaultGateway`
4. `Exit`を入力して、ENTERキーを押します。Rack ATSが再起動し、変更が適用されます。

TCP/IPv6設定を手動で割り当てるには、

1. CLIにログオンします。
2. ネットワーク管理者に連絡し、Rack ATS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. ネットワーク設定を行うために3つのコマンドを使用します。(斜体のテキストは変数を示します) 。

   `tcpip6 -man enable`
   `tcpip6 -i yourIPaddress`
   `tcpip -g yourDefaultGateway`

   注記： IPアドレスとデフォルトゲートウェイのために、xxxx:xxxx:xxxx:xxxx/xx形式の数値を入力します。

   `tcpip -d6 DHCPv6 mode`

   DHCPv6 modeは、`router`、`statefull`、`stateless`または`never`となることができます。
4. `Exit`を入力して、ENTERキーを押します。Rack ATSが再起動し、変更が適用されます。

tcpipコマンドの詳細については、tcpip, 83 ページまたはtcpip6, 84 ページを参照してください。

.iniファイルユーティリティ

.iniファイルユーティリティでは、設定済みのRack ATSから .iniファイル設定をエクスポートして未設定のRack ATSに適用することができます。詳細については、「**設定ファイルを用いた設定の作成とインポート**」を参照してください。

ファームウェアのアップデート

Rack ATSでファームウェアをアップデートすると、

- 最新のバグ修正とパフォーマンスの向上が得られます。
- 新機能が直ちに利用できるようになります。

また、ネットワーク上の全ファームウェアを同一バージョンにしておくことにより、すべてのRack ATS Unitsが同様の機能を同様にして対応するようになります。ここでのアップデートは、単にファームウェアファイルをRack ATSに保存することを意味します。インストールは不要です。新しいアップデートのために、www.se.com、を定期的に確認してください。

ファームウェアファイルの転送方法

最新のファームウェアは、Schneider Electricのwウェブサイトから無料で入手できます。ウェブサイトのホームページ(www.se.com)の検索バーに設備の型番を入力します。検索結果から目的の製品を選択して、その製品ページを開きます。製品ページのソフトウェアとファームウェアのタブを選択して、その製品で使用可能なファームウェアを表示させ、ダウンロードします。

1つまたは複数のNMCのファームウェアを**ファームウェアバージョン2.5.xまたはそれ以前のバージョン**にアップデートするには、次の5つの方法のいずれかを使用します。

- Windowsオペレーティングシステムの場合、www.se.comからダウンロードした**ファームウェアアップデートユーティリティ**を使用してください。ファームウェアアップデートユーティリティの使用, 26 ページを参照してください。
- サポートされているオペレーティングシステムの場合、.nmc3ファイルを転送するには、**FTP**または**SCP**を使用してください。FTPまたはSCPを使用した単独のRack ATSのアップデート, 27 ページを参照してください。
- ご利用のネットワークに接続されていないNetwork Management Cardの場合は、コンピュータからNMCにnmc3ファイルを転送するには、ブートローダーを介して**XMODEM**をUSB仮想通信ポートに接続して使用してください。を参照してください。
- ご利用のコンピュータからNMCへ.nmc3ファイルを転送するには、**USBドライブ**を使用してください。USBドライブを使用したファイルの転送とアップデート, 28 ページを参照してください。
- 複数のRack ATSユニットのアップデートについては、複数のRack ATS Unitsの更新方法, 29 ページを参照してください 。

ファームウェアアップデートユーティリティの使用

このファームウェアアップデートユーティリティは、www.se.com/ww/en/downloadから利用可能なファームウェアアップデートパッケージの一部です。(特定の製品用のアップデートユーティリティを別の製品のファームウェアのアップデートのために絶対に使用しないでください。)

このユーティリティは、Windowsベースのシステムでアップデートを行うために使用します。サポートされているWindowsオペレーティングシステムでは、ファームウェアアップデートユーティリティによりファームウェアの転送が自動的に実行されます。

ダウンロードしたファームウェアアップデートファイルを展開し、.exeファイルをダブルクリックします。次に、ダイアログボックスにIPアドレス、ユーザー名とパスワードを入力し、**Start Update Now**をクリックします。**Ping**ボタンを押して入力内容が正しいかどうかテストすることができます。

このユーティリティは、手動的なアップデートを行うために使用します（主としてLinuxシステムが対象）。Windows以外のオペレーティングシステムでは、ファームウェアアップデートユーティリティはファームウェアファイルを抽出しますが、Rack ATSのアップグレードを行いません。

ファームウェアファイルの抽出方法：

1. ダウンロードしたファームウェアアップグレードファイルからファイルを抽出してから、**ファームウェアアップデートユーティリティ**（.exeファイル）を実行します。
2. プロンプトが表示されたら、**Next>**をクリックし、ファイル抽出先のディレクトリの場所を指定します。
3. **ファイルの抽出完了**のメッセージが表示されたら、ダイアログボックスを閉じます。

抽出後の各種アップグレード方法については、「ファームウェアファイルの転送方法, 25 ページ」を参照してください。

FTPまたはSCPを使用した単独のRack ATSのアップデート

FTP

FTPを使用して、ネットワーク上にRack ATSをアップデートするには、次の手順に従ってください。

- Rack ATSは、それらのシステムIP、サブネットマスク、デフォルトゲートウェイが設定されたネットワーク上にある必要があります。
- FTPサーバーは、Rack ATSで有効になっていなければなりません。FTPサーバーは、**Configuration > Network > FTP Server**の順に選択して、有効化することができます。

ファイルを転送するには次の手順に従ってください。

1. ファームウェアファイルを抽出します。
2. 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保存されてい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 apc
   C:\apc>dir
   ```

3. FTPクライアントセッションを開始します。`C:\apc>ftp`
4. Rack ATSのIPアドレスとともに`open`を入力して、Enterキーを押します。FTPサーバー用の**ポート**の設定がデフォルトの**21番**より変更された場合、FTPコマンドに非デフォルトの値を使用する必要があります。
   - Windows FTPクライアントの場合、非デフォルトのポート番号とIPアドレスの間にスペースを入れてください。例（21000の前にスペースが入っています）：

     ```
     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の代わりにコロンが必要とされる場合があります。
5. スーパーユーザーまたは管理者としてログオンします。スーパーユーザーのデフォルトのユーザー名とパスワードは両方とも**apc**です。
6. .nmc3ファイルを送信するには、`put`コマンドを使用します。`put` *`filename.nmc3`*

   例えば、`put apc_hw21_ats5g_x-x-x-x.nmc3`

   (`x-x-x-x`はファームウェアのバージョン番号を示します)。
7. FTPにより転送が確認されたら、`quit`を入力して、セッションを終了します。

SCP

Secure CoPy(SCP)を使用して、Rack ATSのためのファームウェアをアップデートするには、次の手順に従ってください。

注記： SCPがSSHの一部であるため、SSHを有効化するとSCPも有効になります。SSHはデフォルトで有効になっています。

1. ファームウェアファイルの位置を探します。
2. SCPコマンドラインを使用して、Rack ATSにファームウェアを転送します。次の例では、`x-x-x-x`はファームウェアのバージョン番号を示します。

   ```
   scp -c <cipher> apc_hw21_ats5g_x-x-x-x.nmc3
   apc@158.205.6.185:apc_hw21_ats5g_x-x-x-x.nmc3
   ```

   注記： このSCPコマンドは、OpenSSH用のものです。このコマンドは、使用するSSHツールによって異なる場合があります。*<cipher>*はaes256-cbcまたは3des-cbcのいずれかになることができます。

XMODEMによる単独ラックATSのアップグレード

ネットワークに接続されていない単独のラックATSをXMODEMを用いてアップグレードするには、ファームウェアアップグレードユーティリティから該当のファームウェアファイルを抽出しなければなりません。(「ファームウェアファイルを抽出するには」を参照)

ファイルを転送するには次の手順に従ってください。

1. ローカルコンピュータでシリアルポートを選択し、このポートを使用しているすべてのサービスを無効にします。
2. マイクロUSBケーブルを選択したポートとラックATSにあるコンソールポートに接続します。
3. TeraTermやHyperTerminalなどのターミナルプログラムを起動し、選択したポートを115200bps、8データビット、パリティなし、1ストップビット、フロー制御なしに設定します。
4. ラックPDUにある**Reset**ボタンを押してから、すぐに**Enter**キーを2回押すか、Boot Monitorプロンプトに次の表示が出るまで押しつづけます： `BM>`
5. `XMODEM`を入力して、**ENTER**キーを押します。
6. ターミナルプログラムのメニューから**XMODEM**を選択し、次に`XMODEM`を使用して転送する.nmc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Boot Monitorプロンプトが表示されます。
7. ラックATSの管理インターフェイスを再起動するには、`reset`を入力するか、**Reset**ボタンを押します。

USBドライブを使用したファイルの転送とアップデート

転送を開始する前に、USBドライブがFAT32でフォーマットされていることを確認してください。

1. USBフラッシュドライブで**apcfirm**という名前のフォルダを作成します。
2. ファームウェアアップデートファイルをダウンロードし、必要な場合展開します。**app.nmc3**ファームウェアファイルを**apcfirm**フォルダにコピーします。

   注記：ご利用のデバイスタイプとNMC用のファームウェアアプリケーションのみ使用してください。
3. テキストエディタを使用して、ファイル名が**nmc3.rcf**となるファイルを作成し、**apcfirm**フォルダに保存します。(ファイルの拡張子は、.txtなどではなく、.rcfでなければなりません。)

   ファイルに次のテキストのみ追加します。`NMC3=`*`application_name`*`.nmc3`ここで*`application_name`*はファームウェアアップデートファイルのファイル名です。

   たとえば、ファームウェアアップデートファイルが`apc_hw21_ats5g_x-x-x-x.nmc3`となっている場合、テキストファイルには`NMC3=apc_hw21_ats5g_x-x-x-x.nmc3`と記載しなければなりません。と記載しなければなりません。

   変更をnmc3.rcfファイルに保存します。
4. フラッシュドライブをRack ATSのUSBポートに差し込みます。
5. Web UI、CLI、またはRack ATSの前面にある**Reset**ボタンを押して、管理インターフェイスを再起動します。再起動が終了するまで待ちます。

「アップグレードや更新の確認, 30 ページ」の手順を使用してアップデートが正常に完了していることを確認します。

複数のRack ATS Unitsの更新方法

次の方法のいずれかを使用します。

- **ファームウェアアップデートユーティリティ**：Windowsを利用している場合は、IPv4で複数のファームウェアアップデートのために使用します。アップデートが正常に行われたかどうか検証できるように、ユーティリティは全てのアップデート手順をログに記録します。このユーティリティはファームウェアのダウンロードに含まれています。詳細については、次のを参照してください。
  - ファームウェアアップデートユーティリティの使用, 26 ページ、または
  - FA156099のFAQの記事:「*How do I perform a mass firmware upgrade on APC network enabled products?*（APCネットワーク対応製品で一括ファームウェアアップグレードを実行するには？）」（www.se.com参照）FAQ記事を見つけるには、wwww.se.comの検索バーに記事のタイトルまたは番号を入力します。結果のページでは、**Faq**を選択して検索結果をFAQ記事のみに絞り込みます。
- **環境設定値のエクスポート**：バッチファイルを作成し、.iniファイルユーティリティを使用して、複数のRack ATSから構成設定を取得し、他のRack ATSにエクスポートすることができます。.iniファイルユーティリティのダウンロード方法の詳細については、
  - FA156117のFAQ記事:「*How can I mass configure a Network Management Card (NMC) or NMC embedded product?*（*NMC*または*NMC*埋め込み製品を一括設定するには？）」をwww.se.comで参照してください。FAQ記事を見つけるには、www.se.comの検索バーに記事のタイトルまたは番号を入力します。結果のページでは、**Faq**を選択して検索結果をFAQ記事のみに絞り込みます。
  - リリースノートをお読みください。（リリースノートはユーティリティファイルに含まれています）
- **FTPまたはSCPを使用した複数のRack ATS Unitsのアップデート:** FTPクライアントまたはSCPを使用して複数のRack ATS Unitsをアップデートするには、手順を自動的に実行するスクリプトを作成してください。

  注記：FAQ記事を見つけるには、www.se.comへ進み、あなたのロケーションを選択します。次に**サポート > 文書とソフトウェアのダウンロード**を選択して、検索バーにFAQ記事のタイトルまたは番号を入力します。

NPSによるファームウェアアップグレード

起動時および定期的な運用中に、NPSホストは独自のファームウェアバージョンを各ゲストのバージョンと比較します。バージョンが異なる場合、ホストはNPSチェーンを使用してファームウェアを非準拠ゲストにコピーします。

注記：この機能を使用するには、NPSホストとゲストの両方で常駐ファームウェアサポートが必要であるため、自動ファームウェアアップグレードはAP44XX **A** Series Rack ATSユニットでのみ使用できます。この機能を使用するには、NPSチェーンの正しい動作を維持するために、交換用Rack ATSユニットもAP44XX**A**シリーズモデルである必要があります。

アップグレードや更新の確認

転送結果の確認

ファームウェアの更新が成功したかどうかを確認するには、CLIの`xferStatus`コマンドを使用して最後の転送結果を表示するか、**mfiletransferStatusLastTransferResult** OIDにSNMP GETを実行します。

前回の転送結果コード

考えられる転送エラーには、TFTPまたはFTPサーバーが検出されない、サーバーによるアクセス拒否、サーバーが転送ファイルを検出/認識できない、転送ファイルの破損などがあります。

SNMP戻り値	コード	説明
1	`Successful`	ファイル転送は正常に完了しました。
2	`Result not available`	ファイル転送が記録されていません。
3	`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。
4	`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。
5	`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。
6	`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。
7	`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。
8	`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の確認

選択手順（パス）： About > Network

このWeb UIページを使用して、更新されたファームウェアのバージョンを確認します。MIB II sysDescr OIDに対してSNMP GETを使用することも、CLIで`aboutATS`コマンドを使用することもできます。

他のアプリケーションによるネットワーク管理

これらのアプリケーションやユーティリティは、ネットワークに接続されているRack ATSで使用できます。

- PowerNet® Management Information Base(MIB)と標準MIBブラウザ：SNMP SETとGETを実行し、SNMPトラップを使用します。
- EcoStruxure™ IT：重要なアラートや重要な情報を収集、整理、配信します。これにより、ネットワークのどこからでも、またはスマートフォンからでも、複雑な物理インフラ環境の統合ビューを提供します。
- Data Center Expert：重要なアラートや重要な情報を収集、整理、配信し、複雑な物理インフラ環境をネットワークのどこからでも複雑な物理インフラ環境の統合ビューを提供します。
- デバイスIP設定ウィザード：ネットワーク上の1台以上のRack ATS装置の基本設定を構成します。
- セキュリティウィザード：Secure Sockets Layer(SSL)/Transport Layer Security(TLS)、関連プロトコル、暗号化ルーチンを使用している場合に、Rack ATSユニットのセキュリティをサポートするのに必要なコンポーネントを作成します。

パスワードを忘れた場合

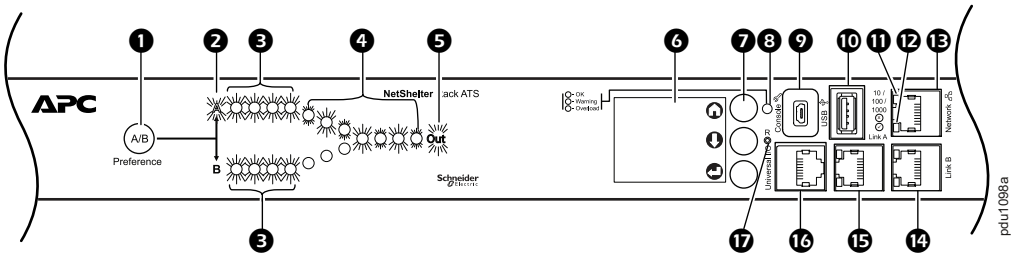
パスワードを忘れた場合、Rack ATSをそのデフォルト設定にリセットしなければなりません。Rack ATSを設定した後、.iniファイルをエクスポートして、安全な所に保存してください。このファイルを保存すれば、パスワードを忘れた場合に設定を回復することができます。

Rack ATSをリセットするには、次の手順を行います。

1. ディスプレイインターフェイスで**Reset**ボタンを20 ~ 25秒押しつづけ、その間にステータス表示LEDが緑色で点滅していることを確認します。ステータス表示LEDがオレンジ色に変わったら、**Reset**ボタンを放せば、Rack ATS の再起動が行われます。
2. デフォルトのユーザー名とパスワード(**apc**と**apc**)を使用して、保護されている接続を通じてRack ATSにアクセスします。

   保護されている接続には、シリアルケーブルによるCLIへのローカル接続、SSHによるCLIへのリモート接続、またはHTTPSによるWeb UIへの接続が含まれます。これらの保護されている各接続に関する手順は、このマニュアルに記載されています。保護されていない接続は、デフォルトで無効になっています。
3. ユーザー名とパスワードをリセットし、Rack ATSを必要な設定にします。

前面パネルの概要



Rack ATSは、操作をせずに10分後にディスプレイのバックライトがオフになるように設定されています。ディスプレイのナビゲーションボタンを押すと、バックライトが点灯します。

項目		機能
❶	Preference A/Bボタン	優先電源を設定します。1回押すとSource Aが、2回押すとSource Bが、3回の押すとno preferenceが設定されます。
❷	Source AおよびB LED	優先電源を示します。電源を使用しない場合は、両方のLEDが点灯します。LCDディスプレイに優先電源も表示されます。
❸	入力コネクタLED	各電源からの入力電圧に関する情報を提供します。RMS入力電圧と測定周波数が選択した許容範囲内にある場合、対応するLEDが点灯します。通常の動作条件（完全な電源冗長性）では、両方のLEDが点灯します。
❹	出力コネクタLED	出力にどのソースが使用されているかが示されます（点灯するのはどちらか一方のみです）。Source Preference LED、コネクタLED、および出力LEDが一緒に表示され、Rack ATSを通る電力の流れが確認されます。
❺	出力LED	Rack ATSの出力で電圧が利用可能であることを示します。
❻	LCDディスプレイ	Rack ATSのステータス、設定、製品情報を表示します。
❼	ナビゲーションボタンの表示	LCDディスプレイでは、アイコンが隣り合うボタンの目的を示します。 **ホーム**：モニター画面を移動するか、サブメニューからモニター画面に戻ります。 **Down:** モニター画面またはメニュー項目を移動します。 **選択**：メニュー項目を選択するか、モニター画面からメインメニューに移動します。
❽	デバイスステータスLED	デバイスステータスLED, 34 ページを参照してください。
❾	コンソールポート	CLIへのローカルアクセスのために、コンピュータをRack ATSに接続します。マイクロUSBケーブル（付属していません）を使用します。
❿	USBポート	ファームウェアのアップグレードにはUSBドライブを使用します。
⓫	10/100/1000ステータスLED	10/100/1000ステータスLED, 34 ページを参照してください。
⓬	ネットワークステータスLED	ネットワークステータスLED, 34 ページを参照してください。
⓭	ネットワークポート	ネットワークケーブル（付属していません）を使用してRack ATSをネットワークに接続します。
⓮ ⓯	Link AおよびLink Bポート	ネットワークポート共有機能で複数のRack ATSユニットを相互に接続するために使用します。 両方のポートを入出力ポートとして使用できます。ターミネータは必要ありません。
⓰	ユニバーサルI/O	オプションのAPC温度センサ(AP9335T)またはオプションのAPC温度/湿度センサ(AP9335TH)を接続するためのポート。
⓱	リセットスイッチ	ネットワークとシリアル通信を再起動します。

デバイスステータスLED

このLEDは、Rack ATS のアラーム状態を示します。

アラームは、ATSハードウェア (負荷しきい値違反や冗長性の損失など) や環境の監視 (温度しきい値違反やセンサ通信のアラームなど) に関連している場合があります。

条件	説明
緑色の点灯	重大または警告アラームは存在しません。
黄色の点灯	警告アラームが少なくとも1つ発生していますが、致命的アラームは発生していません。
赤が点滅	少なくとも1つの致命的アラームが発生しています。

ネットワークステータスLED

このLEDはネットワークステータスを示します。

条件	説明
オフ	Rack ATSが不明なネットワークに接続されています。
緑色の点灯	Rack ATSのTCP/IP設定は有効です。
緑色の点滅	Rack ATSのTCP/IP設定は有効ではありません。[1]
オレンジ色の点灯	Rack ATSでハードウェア障害が検出されました。
オレンジ色点滅	Rack ATSがBOOTPリクエストを作成しています。
オレンジと緑の交互点滅	Rack ATSはDHCPリクエストを作成しています。
[1]BOOTPまたはDHCPサーバーを使用していない場合、TCP/IP設定については、「CLIへのローカルアクセス, 40 ページ」または「CLIへのリモートアクセス, 23 ページ」)を参照してください。	

10/100/1000ステータスLED

このLEDは、Rack ATSのネットワークステータスを示します。

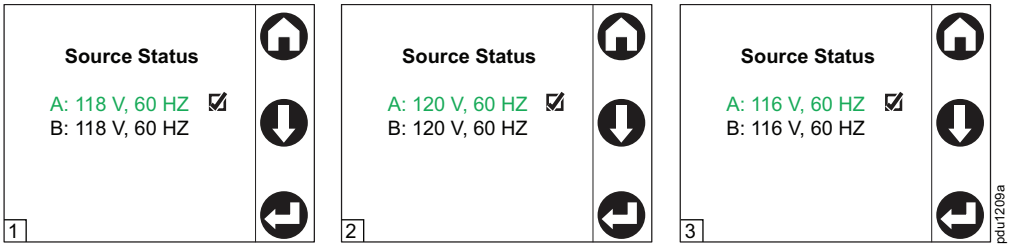
条件	説明
オフ	以下のいずれか (1つまたは複数) の状況です。 • Rack ATSは入力電源を受けていません。 • Rack ATSとネットワークを接続しているケーブルが接続されていないか、故障しています。 • Rack ATSとネットワークを接続しているデバイスの電源がオフになっています。 • Rack ATS自体が正しく動作していません。修理または交換が必要な場合があります。カスタマーサポートまでご連絡ください。
黄色の点灯	Rack ATSは、10 ~ 100メガビット/秒(Mbps)で動作するネットワークに接続されています。
緑色の点灯	Rack ATSは、1000 Mbpsで動作するネットワークに接続されています。
黄色の点滅	Rack ATSは、10 ~ 100 Mbpsの速度でデータパケットを送受信しています。
緑色の点滅	Rack ATSは、1000 Mbpsの速度でデータパケットを送受信しています。

LCDディスプレイ画面

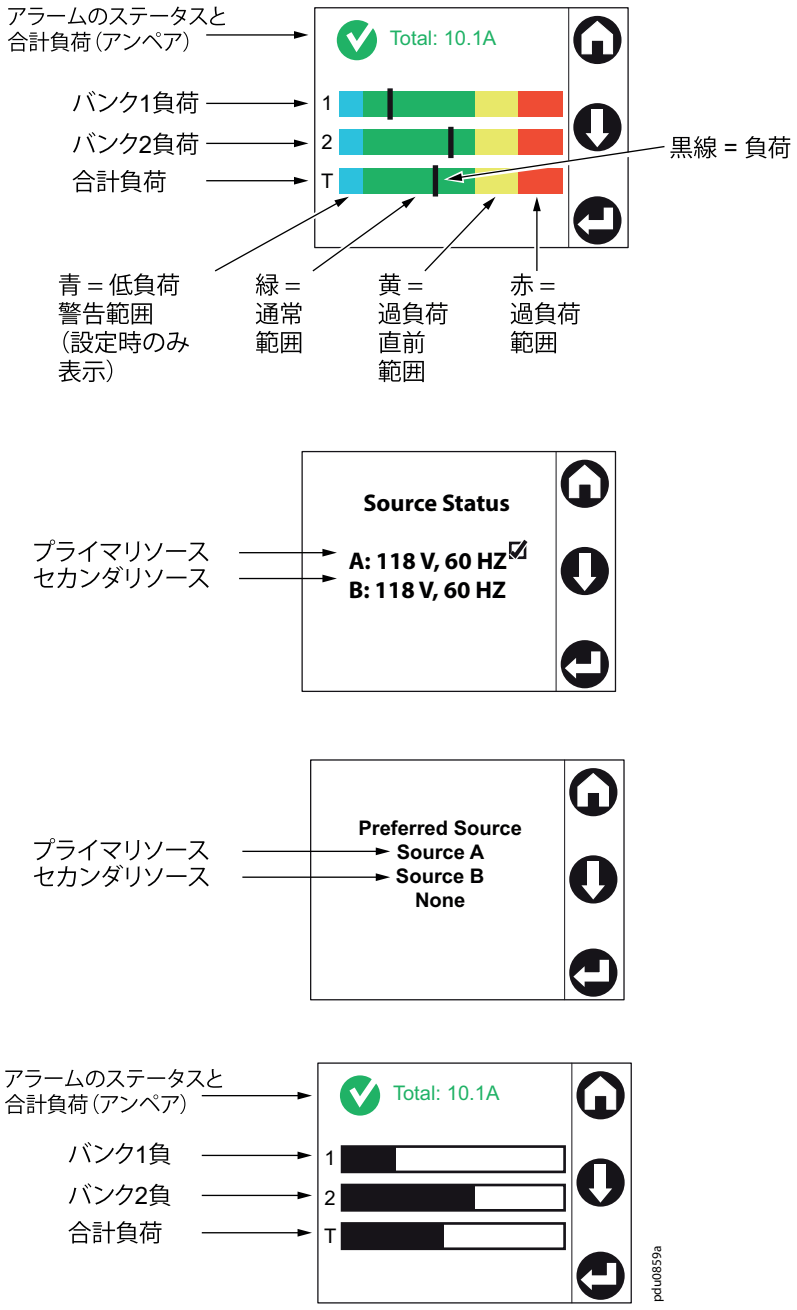
前面パネルのLCDディスプレイは、4つのデフォルト画面が自動的に交代で表示されます。[Home]または[Down]を押すと、これらの画面を手動で移動できます。[Select（選択）]を押して、メインメニューに移動するか、メニュー項目を選択できます。[Down]を使うと、メニュー項目とメニュー画面を移動できます。

30秒間何も操作しないと、LCDディスプレイがデフォルト画面に戻ります。[Home]を押してデフォルト画面に戻ることもできます。

ユニットがNPSグループの一部である場合、NPS IDはLCDディスプレイの左下隅に表示されます。

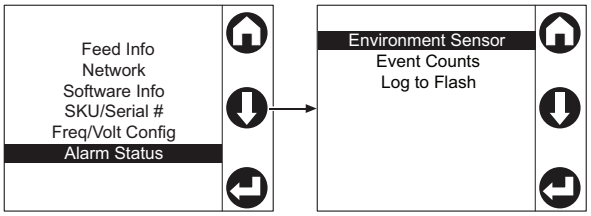


デフォルト画面



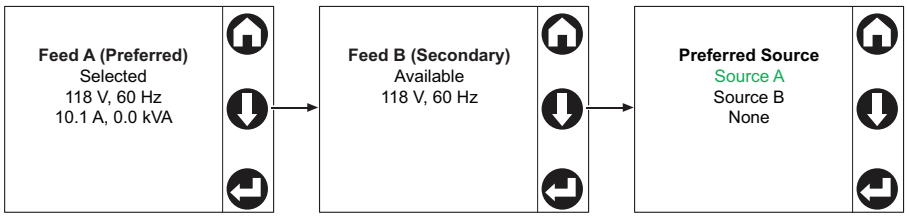
注記： バンクの数はモデルによって異なります。

メニュー画面



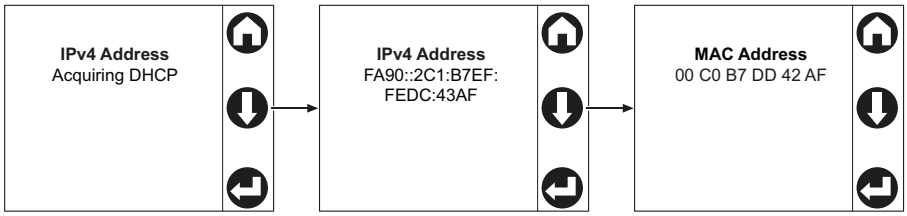
Feed Info

View information for each power source (Feed A and Feed B), or view the Preferred Source (in green text).



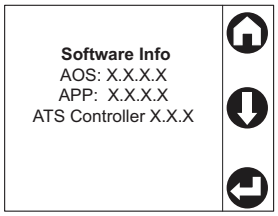
Network

View the IPv4 Address, the IPv6 Address, or the MAC Address.



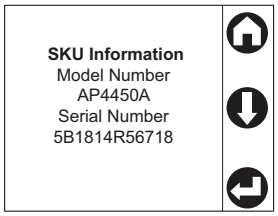
Software info

View the current software version for each firmware module.



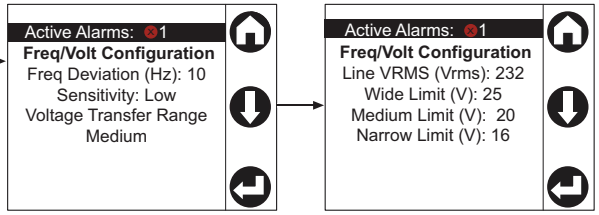
SKU/Serial#

View the model and serial number for your Rack ATS.

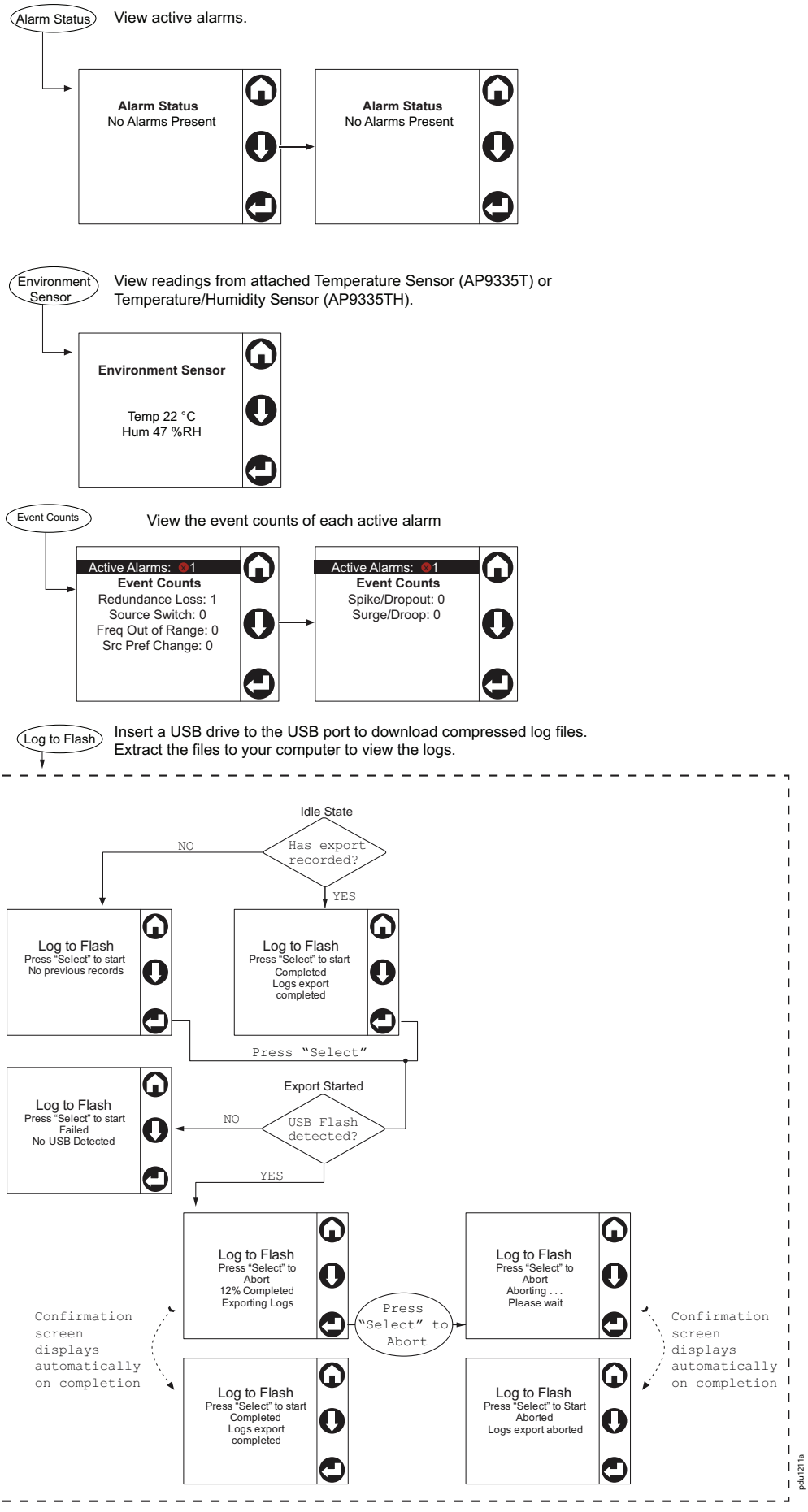


Freq/Volt Config

Configure the switching behaviour of each active alarm

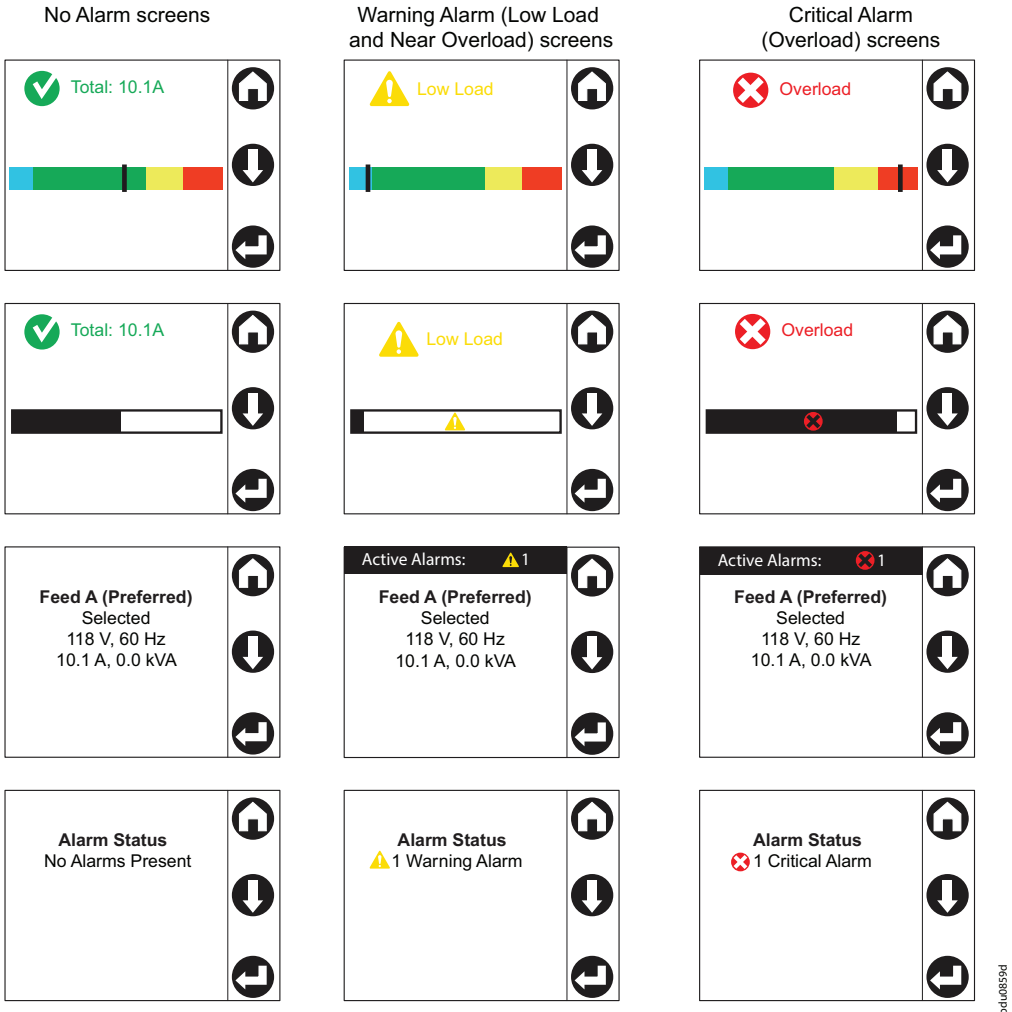


pdui210a


Alarm Status
View active alarms.
Alarm Status
No Alarms Present
Alarm Status
No Alarms Present
Environment Sensor
View readings from attached Temperature Sensor (AP9335T) or Temperature/Humidity Sensor (AP9335TH).
Environment Sensor
Temp 22 °C
Hum 47 %RH
Event Counts
View the event counts of each active alarm
Active Alarms: 1
Event Counts
Redundance Loss: 1
Source Switch: 0
Freq Out of Range: 0
Src Pref Change: 0
Active Alarms: 1
Event Counts
Spike/Dropout: 0
Surge/Droop: 0
Log to Flash
Insert a USB drive to the USB port to download compressed log files.
Extract the files to your computer to view the logs.
Idle State
Has export recorded?
NO
YES
Log to Flash
Press "Select" to start
No previous records
Log to Flash
Press "Select" to start
Completed
Logs export completed
Press "Select"
Export Started
USB Flash detected?
NO
YES
Log to Flash
Press "Select" to start
Failed
No USB Detected
Log to Flash
Press "Select" to Abort
12% Completed
Exporting Logs
Press "Select" to Abort
Log to Flash
Press "Select" to Abort
Aborting . . .
Please wait
Confirmation screen displays automatically on completion
Log to Flash
Press "Select" to start
Completed
Logs export completed
Log to Flash
Press "Select" to Start
Aborted
Logs export aborted
Confirmation screen displays automatically on completion
pdu1211a

アラームステータスインジケータ

アラームが生成されると、アラームステータスインジケータはアラームのレベル（警告または重大）を示します。



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(CLI)では、Rack ATS（およびネットワークポート共有機能を使用している場合は接続されているRack ATS装置）のステータスの設定、管理、監視を行うことができます。さらに、CLI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。CLIを使用してINIファイルをRack ATSに転送することで（特定のCLIコマンドがないパラメーターを含む）、Rack ATSのすべてのパラメーターを設定できます。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。

CLIへのログオン

CLIにアクセスするには、Rack ATS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）接続またはリモート（TelnetまたはSSH）接続のいずれかを使用できます。

CLIへのローカルアクセス

ローカルアクセスのために、コンソールポートを介してRack ATSに接続されているコンピュータを使用してCLIにアクセスします。

注記： この手順では、仮想COMポート(VCP)ドライバがコンピュータにインストールされていることを前提としています。必要な場合、ftdichip.comからご利用のオペレーティングシステム用のVCPドライバをダウンロードしてインストールします。

1. オペレーティングシステムの指示に従い、アプリケーションを開いてコンピュータのCOMポートを確認します。（Windowsオペレーティングシステムでは、ポートをデバイスマネージャで表示できます）。
2. マイクロUSBケーブルを使用して、Rack ATSのコンソールポートをコンピュータのUSBポートに接続します。

   新しく占有されたシリアルCOMポートがポート表示アプリケーションに表示されるはずです。ポート番号をメモするか、必要に応じてポートを割り当て直します。
3. ターミナルプログラム（TeraTermやPuTTYなど）を起動し、選択したシリアルCOMポートを9600bps、8データビット、パリティなし、1ストップビット、フロー制御なしに設定します。このポートでRack ATSにシリアル接続します。
4. ENTERキーを最大3回押して、ユーザー名のプロンプトを表示します。次に、ユーザー名とパスワードを入力します。

   デフォルトでは、スーパーユーザーのユーザー名とパスワードは両方とも**apc**となっています。これが初めてのログオンなら、デフォルトのパスワードを変更するように求められます。会社のパスワード要件を満たす強力なパスワードを使用することをお勧めします。

初めてネットワーク設定を行う場合は、CLIでのTCP/IP設定の表示または設定, 24 ページを参照して設定を完了してください。

CLIへのリモートアクセス

CLIへのアクセスは、TelnetまたはSSHを通して行います。デフォルトでは、SSHが有効になっています。`console`コマンドを使用して、TelnetまたはSSHを有効または無効にすることができます。必要に応じて、(**Configuration > Network > Console > Access**の順に選択し) Web UIを使用して、TelnetまたはSSHを有効または無効にすることもできます。

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は、デフォルトでは無効です。

Telnetを介してCLIにアクセスするには

1. コマンドプロンプトで、`telnet`とRack ATSのIPアドレス (たとえば、Rack ATSのIPアドレスがデフォルトのTelnetポート23を使用している場合は、`telnet 139.225.6.133`)と入力して、ENTERキーを押します。

   Rack ATSがデフォルト以外のポート番号(5000 ~ 32768)を使用している場合は、Telnetクライアントによって、IPアドレス (またはDNS名) とポート番号の間にコロンまたはスペースを含める必要があります。(これらは一般的に使用されるコマンドです。一部のクライアントではポートを引数として指定できず、Linuxのタイプによっては追加コマンドが必要になる場合があります)。
2. ユーザー名とパスワードを入力します。ユーザ名やパスワードを忘れた場合は、「パスワードを忘れた場合, 32 ページ」の手順を参照してください。

SSHによる高度なセキュリティアクセス

Web UIにSSL/TLSの高度なセキュリティを使用している場合は、SSHを使用してCLI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CLI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。SSHの設定と使用の詳細については、www.se.comの『*Security Handbook*』を参照してください。デフォルトでは、SSHが有効になっています。

メイン画面について

Rack ATSのCLIにログオンすると、次の画面が表示されます。

```
Schneider Electric                          Network Management Card AOS        vx.x.x.x
(c) Copyright 2024 All Rights Reserved      ATS5G APP                          vx.x.x.x
-------------------------------------------------------------------------------------------
Name        : Test Lab                                  Date        : 3/12/22
Contact     : Don Adams                                 Time        : 5:58:30
Location    : Building 3                                User        : Administrator
Up Time     : 0 Days 21 Hours 21 Minutes                Stat        : P+ N4+ N6+ A+
-------------------------------------------------------------------------------------------
IPv4                    : Enabled           IPv6                    : Enabled
Ping response           : Enabled
-------------------------------------------------------------------------------------------
HTTP                    : Disabled          HTTPS                   : Enabled
FTP                     : Disabled          Telnet                  : Disabled
SSH/SCP                 : Enabled           SNMPv1                  : Disabled
SNMPv3                  : Disabled
-------------------------------------------------------------------------------------------
Super User              : Enabled           RADIUS                  : Disabled
Administrator           : Disabled          Device User             : Disabled
Read-only User          : Disabled          Network-Only User       : Disabled


Type ? For command listing
Use tcpip for IP address (-i), subnet (-s), and gateway (-g)


apc >
```

- 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されているデバイスの種類を特定するために使用されます（例えば、Rack ATSなど）。

  ```
  Network Management Card AOS          vx.x.x.x
  ATS4g APP                            vx.x.x.x
  ```

- 次の3つのフィールドでは、Rack ATSのシステム名、担当者、設置場所を識別できます。

  ```
  Name                                 Test Lab
  Contact                              Don Adams
  Location                             : Building 3
  ```

- アップタイムのフィールドには、Rack ATSの管理インターフェイスが起動してから、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つのフィールドでは、日時でログインした時点を識別します。

```
Date:                                11/2/2024
Time:                                09:06:45
```

- Userフィールドでは、**スーパーユーザー**、**管理者**、**デバイスユーザー**、**読み取り専用ユーザー**または**ネットワーク専用ユーザー**のどのアカウントでログインしたかを識別します。

```
User: Administrator
```

- Stat フィールドにはRack ATSのステータスが表示されます。

  Stat: P+ N4+ N6+ A+

P+	APC Operating System(AOS)が正常に動作しています。

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-	N6-	N4- N6-	Rack ATSがネットワークへの接続に失敗しました。
N!	N6!	N4! N6!	他のデバイスがRack ATSのIPアドレスを使用しています。
* N4とN6の値は互いに異なる場合があります。例えば、N4- N6+を指定できます。			

A+	アプリケーションは正常に機能しています。
A-	アプリケーションのチェックサムが正しくありません。
A?	アプリケーションは初期化中です。
A!	アプリケーションとAOSに互換性がありません。

注記： P+が表示されない場合は、APCのカスタマーサービスセンター www.se.comにお問い合わせください。

- 上記以外のフィールドには、有効になっているプロトコルとユーザーアカウントが表示されます。

CLIの使用方法

CLIでは、コマンドを使用してRack ATSを設定できます。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。

CLIを使用すると、以下の操作も可能です。

- `help`または`?`を入力します。ENTERキーを押すと、使用しているアカウントの種類に基づいて利用可能なコマンドの一覧が表示されます。
- 指定したコマンドの目的と構文については、該当のコマンド、スペース、および`help`または`?`を入力します。例えば、RADIUS設定オプションを表示するには、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。
- 「`bye`」、「`exit`」、「`quit`」を入力すると、CLIへの接続が終了します。

コマンド構文

アイテム	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で囲まれた項目の間の垂直線は、項目が相互に排反することを示します。いずれかの項目を使用してください。

複数のオプションをサポートするコマンドの例：
`ftp [-p <ポート番号>] [-S <enable | disable>]`

この例では、`ftp`コマンドでポート番号を指定するオプション`-p`と、FTP機能を有効化/無効化するオプション`-S`を使用しています。

FTPポート番号を5010に変更してFTPを有効化するには、次の手順を実行します。

1. `ftp`コマンド、ポートオプション、および引数`5010`を入力：
   `ftp -p 5010`
2. 最初のコマンドが正常に終了したら、`ftp`コマンド、enable/disableオプション、および`enable`選択：
   `ftp -S enable`

相互に排反する引数をオプションで受け入れるコマンドの例：
`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の数を表示する場合の入力は、`enteralarmcount -p critical`

指定されていない引数を入力した場合、コマンドは成功しません。

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。

CLIでは、次の形式ですべてのコマンド操作が報告されます：
`E [0-9] [0-9] [0-9]` : エラーメッセージ

コード	メッセージ
E000	Success (成功)
E001	Successfully Issued (正常に発行)
E002	Reboot required for change to take effect (変更を有効にするには再起動が必要)
E100	Command failed (コマンド失敗)
E101	Command not found (コマンドなし)
E102	Parameter error(パラメータエラー：コマンドに指定された引数に問題がある場合に報告されます。あまりにも少なすぎる、多すぎる、間違ったタイプなど)
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)
E105	Command Prefill (コマンドプレフィル)
E106	Data Not Available (データ使用不可)
E107	Serial Communications Lost (シリアル通信が失われました)
E108	EAPoL disabled due to invalid/encrypted certificate.(無効または暗号化された証明書のため、EAPoLが無効になっている)
E200	Input error (入力エラー：コマンドの実行中にエラーが発生した場合のみ表示)
E201	No Response (応答なし：センサからの応答がない場合に報告)
E206	Invalid value(無効な値)
E213	Device busy or lost communication. (デバイスがビジーまたは通信喪失。) Please try again. (再試行してください。)

コマンド実行中のユーザー入力のプロンプト

一部のコマンドでは、追加のユーザー入力が必要です (例えば、ボーレート用に.iniプロンプトを転送するなど) 。このようなプロンプトには、1分間の固定タイムアウト時間があります。タイムアウト時間内にテキストを入力しなかった場合、コマンドは`E100`を出力します。この意味は、`Command Failed` (コマンドが失敗しました) です。コマンドプロンプトが再び表示されます。

コマンド編集

Backspaceキーは、コマンド入力中に使用できる唯一の編集機能です。Backspaceキーを押すと、現在入力しているコマンド文字列の最後の文字が削除されます。

履歴

CLIは、10個の前のコマンドを呼び出すコマンド履歴バッファを実装しています。上下矢印キーを使用して、入力したコマンドを前後に移動できます。

オートコンプリート

CLIでは、コマンド自動補完がサポートされています。部分的なコマンドを入力する場合は、[Tab]キーを押して、最初に一致したコマンドを使用してコマンドを完了させることができます。一致するものがない場合、システムはコマンドを完了しません。

Tabキーを押すと、次に使用可能なコマンドの一致が選択されます。使用可能なすべてのコマンドがスクロールされると、部分的に入力された元のコマンドが表示されます。

区切り文字

CLIでは、コマンドと引数の区切り文字として(ASCII 0x20)が使用されます。コマンドと引数の間の余分な空白は無視されます。

コマンド応答のすべてのフィールドは、効率的な解析のためにカンマで区切られています。

オプションと引数の入力

オプションなしで引数なしのコマンドを入力した場合、使用可能なすべてのオプションの現在値が返されます。

オプションを指定してコマンドを入力して引数を指定しなかった場合、そのオプションの現在値のみが返されます。

コマンドの後に疑問符(?)または`help`を入力すると、コマンドを説明するヘルプテキストが返されます。

```
<スペース> ::= (" " | multiple" ")

<有効な文字_番号> ::= (a-z | A-Z | 0-9)

<string> ::= ( 1 - 64連続する印刷可能な有効なASCII文字[hex 0x20 ~ 0x7Eの範囲]
)
```

備考：文字列に空白が含まれている場合、文字列全体を引用符(" ")で囲む必要があります。

```
<option> ::= "-"(<valid letter_number> | <valid letter_number> <valid
letter_number>)

<argument> ::= <helpArg> | <alarmcountArg> | <bootArg> | <cdArg> |
<consoleArg> | <dateArg> | <deleteArg> | <ftpArg> | <pingArg> |
<portspeedArg> | <promptArg> | <radiusArg> | <resettodefArg> |
<systemArg> | <tcpipArg> | <userArg> | <webArg> | <string>

<optionArg> ::= <option> <argument>
```

応答形式とメッセージコード

すべてのCLIコマンドで次の項目が表示されます。

<3桁の応答コード>：<応答メッセージ>

必要に応じて、このコマンドは<cr><lf>も発行し、コマンドを出力します。

成功したコマンド操作の応答コードは100未満です。100以上の応答コードは、次のような一定の形式でエラーを示します。

```
E[0-9][0-9][0-9]: Error message
```

例：

```
E000: Success
```

（該当する場合は、コマンドの出力も含まれます）。

ネットワークマネジメントカードのコマンドの説明

?

アクセス：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：ご利用のアカウントタイプで使用可能なすべての 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。

引数	説明
<マンド>	特定のコマンドのヘルプテキストを表示します。

例 1：

```
apc> ?

System Commands:

------------------------------------------------------------------------

?             about       alarmcount    boot          bye           cd
clrrst        console     date          delete        dir           dns
eapol         email       eventlog      exit          firewall      format
ftp           help        lang          lastrst       ldap          ledblink
logzip        netstat     ntp           ping          portspeed     prompt
pwd           quit        radius        reboot        resetToDef    session
smtp          snmp        snmptrap      snmpv3        ssh           ssl
system        tacacs+     tcpip         tcpip6        user          userauth
userdflt      web         whoami        wifi          xferINI       xferstatus

Device Commands:

------------------------------------------------------------------------

aboutATS      atsMeasure    atsStatus     dispID        freqDeviat    eventCounts
frontPanel    humAlGen      humLow        humMin        humHyst       humReading
humStatus     lcd           lcdBlink      lineVRMS      modbus        phLowLoad
phNearOver    phOverLoad    phPeakLoad    phReading     prodInfo      sensorName
sourceAName   sourceBNa-    sourcePref    tempAlGen     tempHigh      tempMax
              me
tempHyst      tempPeak      tempReadi-    tempAtatus    vMediumLmt    vNarrowLmt
                            ng
vSensitvty    vWideLmt      vXferRange    logToFlash
```

例 2:

```
apc> help boot
Usage: boot – Configuration Options
    boot [-b <dhcpBootp | dhcp | bootp | | manual>] (Boot Mode)
          [-a <remainDhcpBootp | gotoDhcpOrBootp>] (After IP
          Assignment)
          [-o <stop | prevSettings>] (On Retry Fail)
          [-c <enable | disable>] (Require DHCP Cookie)
          [-s <retry then stop#>] (Note: 0 = never)
          [-f <retry then fail#>] (Note: 0 = never)
          [-v <vendor class>]
          [-i <client id>]
          [-u <user class>]
```

エラーメッセージE000, E102

about

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：ハードウェアとファームウェアの情報を表示します。これらの情報は、トラブルシューティングの際にも役立ち、ウェブサイトで最新のファームウェアバージョンが用意されているかどうかを確認するときにも使用できます。

パラメータ：なし

例：

```
apc> about
     E000: Success
     Hardware
     Factory
     ---------------
     --
     Model Number:       nnnnnnnnnn
     Serial Number:      nnnnnnnnnn
     Hardware            nnnn
     Revision:
     Manufacture         mm/dd/yyyy
     Date:
     MAC Address:        00 05 A2 18 00 01
     Management          0 Days 1 Hour 42 Minutes
     Uptime:
```

エラーメッセージ：E000

alarmcount

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：システムに存在するアラームを表示します。

パラメータ：

オプション	引数	説明
-p	all	Rack ATSから報告された発生中のアラーム数を表示します。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数を表示します。
	critical	発生中の重大なアラーム数を表示します。
	informational	発生中の情報アラーム数を表示します。

例：発生中の警告アラームをすべて表示するには、次のように入力します。

```
apc> alarmcount -p warning
E000: Success
WarningAlarmCount: 0
```

エラーメッセージ：E000, E102

boot

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：Rack ATS が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含むネットワーク設定をどうやって取得するかを特定します。その後、BOOTPまたはDHCPサーバーの設定を行います。

パラメータ：

オプション	引数	説明
-b <boot mode>	dhcp | bootp | manual	Rack ATSの電源投入、リセット、再起動の際にTCP/IPの設定がどのように行われるかを定義します。
-c	[<enable | disable>] (Require DHCP Cookie)	dhcpおよびdhcpBootp 起動モードのみです。DHCPサーバーからAPC cookieを取得する要件を有効化または無効化します。
通常、これらの3つの設定のデフォールト値は変更不要です。		
-v	[<vendor class>]	APC
-i	[<client id>]	ネットワーク上で一意のものとしてRack ATSを認識可能にするMACアドレスです。
-u	[<user class>]	アプリケーションのファームウェアモジュール名です。

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、次の手順を行います。

1. boot -b dhcpを入力します。
2. DHCPサーバーからAPC Cookieを取得する要件を有効化するには、次のように入力します。

```
apc> boot -c enable
E000: Success
```

エラーメッセージ：E000, E102

bye

アクセス権：スーパーユーザー、管理者、デバイスユーザー 、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：CLIセッションを終了します。これは、`exit`または`quit`コマンドと同じように動作します。

パラメータ：なし

例：

```
apc> bye
Connection Closed - Bye
```

エラーメッセージ：なし

cd

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明：Rack PDURack ATSのディレクトリ構造内のフォルダに移動します。CLIからログアウトすると、作業ディレクトリがルートディレクトリ「/」に戻されます。

パラメータ：`<directory name>`

例1：SSHフォルダに移動して、SSHセキュリティ証明書がRack ATSにアップロードされていることを確認するには、次の手順を行います。

1. `cd ssh`を入力して、ENTERキーを押します。
2. SSHフォルダに保存されているファイル一覧を表示するには、`dir`を入力して、ENTERキーを押します。

例2：前のディレクトリフォルダに戻るには、次のように入力します。`cd . .`

エラーメッセージ：`E000, E102`

clrrst

アクセス権：スーパーユーザー、管理者

説明:ネットワークインターフェイスのリセット理由を除去します。リセット理由の詳細については、lastrst, 65 ページを参照してください。

例：なし

エラーメッセージ：なし

console

アクセス権：スーパーユーザー、管理者

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、デフォルトで無効になっているTelnetを使用するか、デフォルトで有効になっているSecure SHell(SSH)を使用するかを指定します。SSHは、ユーザー名、パスワード、データを暗号化して転送することにより保護を確保します。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。または、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します。

パラメータ：

オプション	引数	説明
-S	<enable | disable>	デバイスへのSSHアクセスを有効化または無効化します。SSHを有効にすると、SCPが有効になります。
-t	<enable | disable>	デバイスへのTelnetアクセスを有効化または無効化します。
-pt	<telnet port n>	Rack ATS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）。
-ps	<SSH port n>	Rack ATS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）。
-b	2400 | 9600 | 19200 | 38400	コンソールポート接続の通信速度を設定します（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アクセスを有効化するには、次のように入力します。

```
console -S enable
```

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
```

エラーメッセージ：E000, E102

date

アクセス権：スーパーユーザー、管理者

説明：Rack ATSにより使用される日付と時刻を設定します。

注記： Rack ATSの日付と時刻を定義するNTPサーバーを設定するには、ntp, 70 ページを参照してください。

パラメータ：

オプション	引数	説明
-d	<"datestring">	現在の日付を設定します。形式は現在の-f設定に一致する必要があります。
-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	このユーザー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。「m」（月）、「d」（日）、「y」（年）の各文字はそれぞれ 1 桁に相当します。日付または月名が 1 桁の場合、前にゼロをつけて表示されます。
-z	<time zone offset>	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、異なる時間帯の他のユーザーとの同期が可能になります。

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

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

例2：上記の形式を用いて2009年10月30日の日付を定義するには、次のように入力します。

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

例3：時刻を5:21:03 p.m.として定義するには、次のように入力します。

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

エラーメッセージ：E000, E100, E102

delete

アクセス権：スーパーユーザー、管理者

説明：ファイルシステム内のファイルを削除します。(イベントログを削除するには、eventlog, 61 ページを参照してください。)

パラメータ：

引数	説明
<file name>	削除するファイルのファイル名を入力します。

例：ファイルを削除するには、

1. ファイルを含むフォルダに移動します。たとえば、ログのフォルダに移動するには、次のように入力します。
   ```
   cd logs
   ```
2. ログのフォルダのファイルを表示するには、次のように入力します。
   ```
   dir
   ```
3. ファイルを削除するには、次のように入力します。
   ```
   delete <file name>
   ```

エラーメッセージ：E000, E102

dir

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：Rack ATSに保存されているファイルやフォルダを表示します。

パラメータ：なし

例：

```
apc> dir
E000: Success
1024 Jan 2 4:34 apc_hw21_aos_2.5.0.8.bin
6249332 Jan 2 4:34 apc_hw21_ats5g_1.1.0.15.bin
45000 Sep 30 1996 config.ini
          0    Apr    23  18:53   db/
          0    Apr    23  18:53   ssl/
          0    Apr    23  18:53   ssh/
          0    Apr    23  18:53   logs/
          0    Apr    23  18:53   sec/
          0    Apr    23  18:53   fwl/
          0    Apr    23  18:53   email/
          0    Apr    23  18:53   eapol/
          0    Apr    23  18:53   tmp/
          0    Apr    23  18:53   upsfw/
```

エラーメッセージ：E000

dns

アクセス権：スーパーユーザー、管理者

説明：ドメインネームシステム（DNS）の設定を手動で行います。

パラメータ：

オプション	引数	説明
-OM	enable | disable	DNSの手動設定をオーバーライドします。この設定が有効になっている場合、他のソース（DHCPなど）からの構成データがここで設定した手動構成よりも優先になります。
-y	<enable | disable>	システム・ホスト名の同期
-p	<primary DNS server>	プライマリDNSサーバーを設定します。
-s	<secondary DNS server>	セカンダリDNSサーバーを設定します。
-d	<domain name>	ドメイン名を設定します。
-n	<domain name IPv6>	IPv6のドメイン名を設定します。
-h	<host name>	ホスト名を設定します。

例：

```
apc > dns -OM
E000: Success
Override Manual DNS Settings: enabled
```

エラーメッセージ：E000, E102

eapol

アクセス権：スーパーユーザー、管理者

説明:EAPoL（802.1Xセキュリティ）設定をします。

パラメータ：

オプション	引数	説明
-S	enable | disable	EAPoLを有効化または無効化します。
-n	<supplicant name>	サプリカント名を設定します。
-p	<private key passphrase>	秘密キーのパスフレーズを設定します。

例1：eapolコマンド結果を表示するには：

```
apc>eapol
E000: Success
Active EAPoL Settings
----------------------------
      Status:              enabled
      Supplicant Name:     NMC-Supplicant
      Passphrase:          <hidden>
      CA file Status       Valid Certificate
      Private Key Status   Valid Certificate
      Public Key Status    Valid Certificate
```

例2：EAPoLを有効化するには：

```
apc>eapol -S enable
E000: Success
Reboot required for change to take effect.
```

email

アクセス権：スーパーユーザー、管理者

説明: Rack ATSがイベント通知を送信するために使用する電子メールのパラメータを設定します。

パラメータ：

オプション	引数	説明
-g[n]	<enable | disable>	受信者への電子メールの送信を有効化（デフォルトで）または無効化します。
-t[n]	<To Address>	受信者のユーザー名およびドメイン名です。ページングのために電子メールを使用するには、受信者のポケベルゲートウェイのアカウントのためにメールアドレス使用してください（例： myacct100@skytel.com）。ポケベルゲートウェイはメッセージを生成します。
-o[n]	<long | short> (Format)	長い形式には、名前、設置場所、連絡先、IPアドレス、デバイスのシリアル番号、日付と時刻、イベントコードおよびイベントの説明が含まれます。短い形式には、イベントの説明のみ含まれます。
-l[n]	<Language Code>	電子メール通知で使用される言語です。現時点では英語のみ使用できます。
-r [n]	<Local | recipient | custom> (Route)	SMTPサーバーのオプションを設定します。 Local（推奨）：SMTPサーバーが内部ネットワーク上にある場合、または電子メールドメイン用に設定されている場合、このオプションを選択します。遅延やネットワークの停止を制限するにはこの設定を選択します。この設定を選択した場合は、デバイスのSMTPサーバーで転送を有効にして、転送された電子メールを受信するための特別な外部電子メールアカウントを設定する必要があります。**注記**：これらの変更を行う前に、SMTPサーバーの管理者にご相談ください。 Recipient：この設定では、電子メールを受信者のSMTPサーバーに直接送信します。このサーバーは、To AddressのドメインのMXレコードのルークアップにより決定されます。デバイスは電子メールの送信を1度しか試行しません。ネットワーク故障やリモートSMTPサーバーがビジー状態により、タイムアウトが発生して電子メールが失われる可能性があります。この設定は、SMTPサーバーでの追加の管理タスクを必要としません。**注記**：この設定を使用すると、From AddressがTo Addressに一致し、認証と暗号化(TLS)が無効になり、25番のポートが使用されます。 Custom：この設定では、各電子メール受信者が独自のサーバー設定を持つことが可能になります。これらの設定は、smtpコマンドによる設定には依存しません。
Custom Route Option		
-f[n]	<From Address>	Rack ATSにより送信される電子メールメッセージのFromフィールドの内容は、電子メールメッセージの中でIPアドレスがLocal SMTP Serverとして指定されている場合には*user@[IP_address]*、DNSが構成されDNS名がLocal SMTPサーバーとして指定されている場合には*user@domain*となります。 ローカルSMTPサーバーは、この設定を行うために、サーバーでの有効なユーザーアカウントを必要とする場合もあります。サーバーの文書を参照してください。
-s{n}	<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。この定義は、-rオプションがLocalに設定されている場合にのみ必要です。
-p[n]	<Port>	SMTPポート番号はデフォルトで25番となっています。一般的なポート番号は、暗号化されていない電子メールの場合は25番、SSL/TLS暗号化された電子メールの場合は465番および587番です。ポートの設定は、1～65535のいずれかのポートに変更することができます。
-a[n]	<enable | disable> (Authentication)	SMTPサーバーが認証を必要とする場合、このオプションを有効にしてください。
-u[n]	<User Name>	SMTPサーバーが認証を必要とする場合、ここに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あり、SSL/TLSではありません。
-w[n]	<Password>	
-e[n]	<none | ifsupported | always | implicit>	暗号化をいつ使用するかを指定します。 none: SMTPサーバーは、暗号化を必要としないか、サポートしません。 ifsupported: SMTPサーバーは、STARTTLSをサポートしていることを通知しますが、接続の暗号化を必要としません。STARTTLSコマンドは、通知が与えられた後で送信されます。通常、25番のポートで使用されます。

オプション	引数	説明
		always: SMTPサーバーは、サーバーへの接続の際にSTARTTLSコマンドの送信を必要とします。通常、587番のポートで使用されます。 implicit: SMTPサーバーは、暗号化を開始した接続のみ受け入れます。STARTTLSメッセージはサーバーに送信されていません。通常、465番のポートで使用されます。
-c[n]	<enable | disable >	CAルート証明書を必要とします。所属組織のセキュリティポリシーにより、SSL/TLS接続の暗黙の信頼が許可されていない場合にのみ有効にしてください。これを有効にする場合、SMTPサーバーとのTLS接続が成功するには、証明書ローダーを使用してRack ATS unitの証明書ストアにSMTPサーバ用の有効なCA証明書をインストールする必要があります。
-i[n]	<Certificate File Name>	このフィールドは、Rack PDUにインストールされているCAルート証明書とCAルート証明書が要求されるかどうかに依存しています。
n =電子メール受信者番号（1、2、3または4）		

例：ローカルSMTPサーバを使用して、電子メール受信者1に電子メールアドレスrecipient1@apc.comで電子メールを送信できるようにするには：

```
apc> email -g1 enable -r1 local -t1 recipient1@apc.com
E000: Success
```

エラーメッセージ：E000, E102

eventlog

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明：イベントログを呼び出した日付と時刻、Rack ATSのステータスおよびRack ATSに接続されているセンサのステータスを表示します。最近のデバイスイベントおよびそれらが発生した日時を表示します。イベントログ内を移動するには以下のキーを使用します。

パラメータ：

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。このコマンドを使用して、前回イベントログを呼び出した時点以降に記録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を表示します。
B	イベントログの前のページを表示します。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旧できません。

例：

```
apc> eventlog

---- Event Log -------------------------------------------------------

  Date: 2/9/2024 Time: 13:22:26

  ----------------------------------

  Metered Rack ATS: Communication Established

  Date          Time          User        Event

  ---------------------------------------------------------------

  2/9/2024      13:17:22      System      Set Time.

  2/9/2024      13:16:57      System      Configuration change. Date format
                                          preference.
  2/9/2024      13:16:49      System      Set Date.

  2/9/2024      13:16:35      System      Configuration change. Date format
                                          preference.
  2/9/2024      13:16:08      System      Set Date.

  2/9/2024      13:15:30      System      Set Time.

  2/9/2024      13:15:00      System      Set Time.

  2/9/2024      13:13:58      System      Set Date.

  2/9/2024      13:12:22      System      Set Date.

  2/9/2024      13:12:08      System      Set Date.

  2/9/2024      13:11:41      System      Set Date.

<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

エラーメッセージ：E000, E100

exit

アクセス権：スーパーユーザー、管理者、デバイスユーザー 、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：CLIセッションを終了します。これは、byeまたはquitコマンドと同じように動作します。

パラメータ：なし

例：

```
apc> exit
Bye
```

エラーメッセージ：なし

firewall

アクセス権：スーパーユーザー、管理者

説明: Rack ATSの内部ファイアウォール機能を有効化、無効化、設定します。

パラメータ：

パラメータ	引数	説明
-S	<enable | disable>	ファイアウォールを有効化または無効化します。
-f	<file name to activate>	アクティベートするファイアウォールの名前です。
-t	<file name to test> <duration time in minutes>	テストするファイアウォールの名前と継続時間（分単位）です。
-fe		発生中のファイルエラーを表示します。
-te		テストファイルのエラーを表示します。
-c		ファイアウォールテストをキャンセルします。
-r		有効なファイアウォールルールを表示します。
-l		ファイアウォールのアクティビティログを表示します。
-Y		ファイアウォールテストプロンプトをスキップします。

例：*example.fwl*ファイアウォールポリシーファイルを有効化するには、次のように入力します。

```
apc> firewall -f example.fwl
E000: Success
```

エラーメッセージ：E000, E102

format

アクセス権：スーパーユーザー、管理者

説明: Rack ATS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、暗号化鍵、環境設定、イベントログおよびデータログをすべて消去します。このコマンドは、十分注意して使用してください。

注記： プロンプトが表示されたら、YESを入力して確定する必要があります。

注記： Rack ATSをそのデフォルトの構成にリセットするには、代わりにresetToDefコマンドを使用してください。

パラメータ：

オプション	説明
-f	設定データ、イベントログ、データログ、証明書および鍵がべて削除されます。ネットワーク設定は保持されません。
-p	設定データ、イベントログ、データログ、証明書および鍵がすべて削除されます。ネットワーク設定は保持されます。

例：

```
apc> format -p

Format FLASH file system

Warning: This will delete all configuration data,
         event and data logs, certs and keys.

All network configuration settings WILL be preserved.

Enter 'YES' to continue or <ENTER> to cancel: YES
```

エラーメッセージ：なし

ftp

アクセス権：スーパーユーザー、管理者

説明:FTPサーバーへのアクセスを有効化または無効化します。更なるオプションとして、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ポート番号に設定することができます。

注記： いかなる設定が変更されるとシステムは再起動します。

注記： FTPはデフォルトで無効になっており、SSHを介してスーパーユーザーのパスワードを設定すると、Secure CoPy(SCP)は自動的に有効になります。

パラメータ：

オプション	引数	説明
-p	<port number>（有効な範囲：21と5000~32768）	FTPサーバーがRack ATSとの通信のために使用するTCP/IPポートを定義します (デフォルトでは21番) 。FTPサーバーは、指定されたポートと、そのポートより番号が 1 つ小さいポートを両方とも使用します。
-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。

```
apc> ftp -p 5001
E000: Success
```

エラーメッセージ：E000, E102

help

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：ユーザーアカウントタイプに基づいて利用可能な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、当該コマンド名の後ろにhelpを入力します。

パラメータ：[<command>]

例1 : デバイスユーザーとしてログオンした者が利用できるコマンドの一覧を表示するには、デバイスユーザーとしてCLIにログオンし、次のように入力します。

```
help
```

例2 : alarmcountコマンドにより受け取られた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。

```
apc> alarmcount help
Usage: alarmcount -- Display Alarms
         alarmcount [-p <all | warning | critical |
         informational>]
```

lang

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明：使用中の言語を表示します。

パラメータ：なし

例：

```
apc>lang
E000: Success

Languages
enUs - English
```

エラーメッセージ：なし

lastrst

アクセス権：スーパーユーザー、管理者

説明:ネットワークインターフェイスの最後のリセットの理由を表示します。テクニカルサポートの指示に従い、このコマンドの出力を使用してネットワークインターフェイスの問題のトラブルシューティングを行います。

オプション	説明
02 NMI Reset	ネットワークインターフェイスはRack ATSの前面ディスプレイにあるリセットボタンによりリセットされました。
09 Coldstart Reset	ネットワークインターフェイスはハードウェアから電源が取り外されたためリセットされました。
12 WDT Reset	ネットワークインターフェイスはファームウェアコマンドによりリセットされました。

パラメータ：なし

例：

```
apc> lastrst
09 Coldstart Reset
E000: Success
```

エラーメッセージ：E000, E102

ldap

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：LDAP設定を表示および設定します。LDAPサーバーを使用してリモートユーザーを認証するようにデバイスを設定できます。一般的な例として、Microsoft Active DirectoryとOpenLDAPの2つがあります。認証は常に、TLS接続を介した単純なバインド要求を使用して実行されます。LDAPサーバーへのTLS接続が完了するように、LDAPサーバーのCA証明書がインストールされていることを確認します。

オプション	引数	説明
-s	<Search User URI>	最初にバインドするユーザーオブジェクトの場所を表すLDAP URIです。このユーザーオブジェクトには、ユーザーのLDAPデータベースを検索する権限が必要です。ユーザーのログイン時に、このURIのLDAPサーバーが接続され、-p (Search User Password)に指定されたパスワードを使用してDNへのバインドが実行されます。このバインドが成功すると、ログインしようとしているユーザーの検索が行われます。 このLDAP URIには、ldapまたはldapsのいずれかのスキームを含む必要があります。ldapsを使用する場合は、TLS接続は暗黙的に行われ、TCP接続はデフォルトで636番のポートを使用します。ldapを使用する場合、TLS接続はStartTLS要求を送信することにより開始し、TCP接続はデフォルトで389番のポートを使用します。ldapsの使用は標準外であり、推奨されません。 このLDAP URIには、LDAPサーバーのアドレスと、オプションとしてポート番号を含むことができます。検索ユーザーオブジェクトのDNは次のようになります。検索ユーザーDNがDCコンポーネントで終わる場合、このドメインのLDAPサービス用のSRVレコードのDNSルックアップが実行されます。SRVレコードが見つかった場合は、URIで指定されたホストの代わりにそのレコードが使用されます。SRVレコードが見つからない場合、URIで指定されたホストが使用されます。LDAP用のSRVレコードが存在することが分かっている場合、URIのホストコンポーネントを省略できます。 DNが省略された場合、ホストコンポーネントが存在する必要があり、匿名バインドが実行されます。 例： • **ldap://ldap.domain.com/ CN=searchuser,OU=users,DC=domain,DC=com** DNSが使用可能な場合は、domain.comのLDAPサービス用のSRVレコードのDNSルックアップが実行されます。見つかった場合は、接続されます。見つからない場合は、389番ポートのldap.domain.comが接続されます。TLSはStartTLS要求を送信した後で確立され、その後、-p (Search User Password)で指定したパスワードを使用して、CN=searchuser,OU=users,DC=domain,DC=comオブジェクトにバインドが実行されます。ここから、ログインしようとしているユーザーの検索が実行されます。 • **ldap:/// CN=searchuser,OU=users,DC=domain,DC=com** DNSが使用可能な場合は、domain.comのLDAPサービス用のSRVレコードのDNSルックアップが実行されます。見つかった場合は、接続されます。見つからない場合は、URIのホストコンポーネントが省略され、LDAP認証が処理できないため、接続は行われません。接続が成功すると、上記のようにStartTLS、バインドおよび検索が実行されます。 • **ldaps://ldap.domain.com**636番ポートのldap.domain.comが接続され、StartTLS要求を送信せずにTLSハンドシェイクが直ちに実行されます。これが成功すると、匿名バインドが実行されます。ここから、ログインしようとしているユーザーの検索が実行されます。 • **ldap://ldap.domain.com:42/ CN=searchuser,OU=users,DC=domain,DC=com** これは、SRVレコードが見つからない場合、42番ポートのldap.domain.comが接続される点を除いて、最初の例と同じです。 .
-p	<Search User Password>	上記のユーザー検索を実行する際に最初のバインド要求で使用するパスワードです。空白のままにすると、ユーザーDN検索が指定されているかどうかによって、匿名または認証されていないバインドが実行されます。
-t	<2 – 60>	LDAPサーバへの接続およびLDAPサーバとの通信に使用するタイムアウト（秒単位）です。最初のTCP接続はこの時間内に完了する必要があります。この場合、サーバーからの各LDAP応答は、各LDAP要求に続いて、この時間内に受信する必要があります。単一のLDAP認証が複数の要求で構成される場合があるため（紹介が追跡された場合は複数のサーバに対しても）、全体の

オプション	引数	説明
		認証時間はここで指定したタイムアウト値よりもはるかに長くなる場合があります。
-u	<Users Base DN>	これは、ログインするすべてのユーザーが存在する必要があるベースオブジェクトエントリのDNです。
-g	<Groups Base DN>	これは、次の設定で指定されたユーザーグループが存在する必要があるベースオブジェクトエントリのDNです。
-g	<Groups Base DN>	これは、次の設定で指定されたユーザーグループが存在する必要があるベースオブジェクトエントリのDNです。
-ag	<Admins Group Name>	これは、NMC管理者がメンバーとなっているLDAPグループの共通名(CN)です。ログインしようとしているユーザーがこのグループのメンバーである場合、そのユーザーには管理者のアクセス権が付与されます。
-dg	<Device Users Group Name>	これは、NMCデバイスユーザがメンバーとなっているLDAPグループの共通名(CN)です。ログインしようとしているユーザーがこのグループのメンバーである場合、そのユーザーにはデバイスユーザーのアクセス権が付与されます。
-ng	<Network Users Group Name>	これは、NMCネットワークユーザーがメンバーとなっているLDAPグループの共通名(CN)です。ログインしようとしているユーザーがこのグループのメンバーである場合、そのユーザーにはネットワークユーザーのアクセスが付与されます。
-rg	<Read Only Users Group Name>	これは、NMCの読み取り専用ユーザーがメンバーとなっているLDAPグループの共通名(CN)です。ログインしようとしているユーザーがこのグループのメンバーである場合、そのユーザーには読み取り専用ユーザーのアクセス権が付与されます。
-ad	<enable | disable>	これを有効にすると、標準のActive Directoryスキーマに従って、Userクラスのユーザーとグループクラスのグループを含むLDAPディレクトリがサポートされます。
-posix	<enable | disable>	これを有効にすると、RFC 2307で定義されたスキーマに従って、posixAccountクラスのユーザーとposixGroupクラスのグループを含むLDAPディレクトリがサポートされます。
-4519	<enable | disable>	これを有効にすると、RFC 4519で定義されたスキーマに従って、uidObjectクラスのユーザーとgroupOfNamesクラスまたはgroupOfUniqueNamesクラスのいずれかのグループを含むLDAPディレクトリがサポートされます。
-2798	<enable | disable>	これを有効にすると、RFC 2798で定義されているように、inetOrgPersonクラスのユーザーを含むLDAPディレクトリがサポートされます。
-cuser	<enable | disable>	これを有効にすると、上記で記載されているどのクラスにも適合しないクラスのユーザーを含むLDAPディレクトリをサポートできます。これを有効にすると、-ucn (Custom User Class Name)と–ucua (Custom User Username Attr)の設定が必要になります。また、-ucga (Custom User Group Number Attr)もオプションとして指定できます。
-cgroup	<enable | disable>	これを有効にすると、上記で記載されているどのクラスにも適合しないクラスのグループを含むLDAPディレクトリをサポートできます。これを有効にすると、-gcn (Custom Group Class Name)と–gcma (Custom Group Member Attr)の設定が必要になります。また、–gcga (Custom Group Group Number Attr)もオプションとして指定できます。-gcmt（Custom Group Member Type）も正しく設定する必要があります。
-ucn	<Custom User Class Name>	ユーザーエントリが属するオブジェクトクラスの名前です。-cuser（Custom User Class）が有効な場合にのみ使用されます。
-ucua	<Custom User Username Attr>	これは、-ucn (Custom User Class Name)により指定されたオブジェクトクラスのユーザーのユーザー名を含む属性の名前です。-cuser（Custom User Class）が有効な場合にのみ使用されます。
-ucga	<Custom User Group Number Attr>	これは、-ucn (Custom User Class Name)により指定されたオブジェクトクラスのユーザーのプライマリグループのグループ番号を含む

オプション	引数	説明
		属性の名前です。これはオプションで、-cuser（Custom User Class）が有効な場合にのみ使用されます。これは、posixAccountクラスのgidNumber属性と同じ方法で使用されます。
-gcn	<Custom Group Class Name>	グループエントリが属するオブジェクトクラスの名前です。-cgroup（Custom Group Class）が有効な場合にのみ使用されます。
-gcma	<Custom Group Member Attr>	これは、-gcn (Custom Group Class Name)により指定されたオブジェクトクラスのグループのメンバーを含む属性の名前です。-cgroup（Custom Group Class）が有効な場合にのみ使用されます。-gcmt（Custom Group Member Type）がDNに設定されている場合、この属性の値はDNになります。ユーザー名に設定されている場合、この属性の値はユーザー名になります。
-gcga	<Custom Group Group Number Attr>	これは、-gcn (Custom Group Class Name)により指定されたオブジェクトクラスのグループ番号を含む属性の名前です。これはオプションで、-cgroup（Custom Group Class）が有効な場合にのみ使用されます。これは、posixGroupクラスのgidNumber属性と同じ方法で使用されます。
-gcmt	<DN | user name>	これは、-gcn (Custom Group Class Name)により指定されたオブジェクトクラスのグループのメンバを指定する方法を指定します。DNまたはユーザー名のいずれかに設定できます。

例1：NMC用の既存のLDAP設定を表示するには、次のように入力します。

```
ldap
```

例2 :ldap.company.comのActive Directoryスキーマのみを使用して(または、可能な場合、company.comのldap SRVレコードを使用して)、5秒のタイムアウトでLDAPサーバーに接続し、DNのcn=admin、dc=company、dc=comの検索権限を持つ初期ユーザーとパスワードpasswordでバインドし、nmc-adminsグループのNMC管理者、nmc-ro-usersグループのNMC読み取り専用ユーザー、ネットワーク専用ユーザーとデバイスユーザーが無効になるようなLDAPを設定するには、次のように入力します。

```
ldap -s ldap://ldap.company.com/cn=admin,dc=company,dc=com -p
password -t 5 -u ou=users,dc=company,dc=com -g ou=groups,dc=
company,dc=com -ag nmc-admins -rg nmcro-users -dg "" -ng "" -ad
enable -posix disable -4519 disable -2798 disable -cuser
disable -cgroup disable
```

ledblink

アクセス権：スーパーユーザー、管理者

説明: 指定した時間点滅するようにステータス表示LEDを設定します。このコマンドを使用して、Rack ATSの位置を視覚的に確認できます。

パラメータ：

引数	説明
<time>	LEDを点滅させる時間 (分) です。

例：

```
apc> ledbllink 1
E000: Success
```

エラーメッセージ：E000, E102

logzip

アクセス権：スーパーユーザー、管理者

説明:NMCおよびRack ATSから利用できるログファイルの1つの圧縮されたアーカイブを作成します。これらのファイルは、テクニカルサポートが問題のトラブルシューティングに使用することがあります。

パラメータ：

オプション	引数	説明
-m	<電子メールの受信者> (1 ~ 4)	zipファイルの送信先となる電子メールの受信者の識別番号(1 ~ 4)です。設定された 4 つの電子メールの受信者のうち 1 つの番号を入力します。

例：

```
apc> logzip -m 1
Generating files
/dbg/debug_ZA1023006009.tar
Emailing log files to email recipient - 1
E000: Success
```

エラーメッセージ：E000, E102

netstat

アクセス権：スーパーユーザー、管理者

説明:ネットワークの状態および有効なIPv4/IPv6をすべて表示します。

パラメータ：なし

例：

```
apc> netstat
Current IP Information:
Family     mHome     Type      IPAddress                 Status
IPv6       4         auto      FE80::2CO:B7FF:FE51:      configured
                               F304/64
IPv6       0         manual    ::1/128                   configured
IPv4       0         manual    127.0.0.1/32              configured
```

エラーメッセージ：E000, E10

ntp

アクセス権：スーパーユーザー、管理者

説明:ネットワークタイムプロトコルのパラメータを表示および設定します。

パラメータ：

オプション	引数	説明
-OM	enable | disable	手動設定をオーバーライドします。
-p	<primary NTP server>	プライマリサーバーを指定します。
-s	<secondary NTP server>	セカンダリサーバーを指定します。
-e	enable | disable	NTPの使用を有効化または無効化します。
-u	<update now>	直ちにRack ATSの時刻をNTPサーバから更新します。

例1：手動設定のオーバーライドを有効化するには、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`

エラーメッセージ：E000, E102

ping

アクセス権：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用ユーザー

説明：IPアドレスまたはDNS名を指定したデバイスがネットワークに接続されているかどうかを特定します。アドレスに対して4回のクエリが行われます。

パラメータ：

オプション	引数	説明
なし	<IP address or DNS name>	*xxx.xxx.xxx.xxx*の形式でIPアドレスまたはDNSサーバーによって設定されたDNS名を入力します。
-t		停止するまでpingを続けます。

例：IPアドレスが192.168.1.50のデバイスがネットワークに接続されているかを特定するには、次のように入力します。

```
apc> ping 192.168.1.50
E000: Success
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
```

エラーメッセージ：E000, E100, E102

portSpeed

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：イーサネットポートの通信速度を定義します。

注記： ポート速度の設定は1000 Mbpsに変更できます。ただし、この変更はWeb UIを介してのみ可能です。

パラメータ：

オプション	引数	説明
-s	auto | 10H | 10F | 100H | 100F	autoイーサネットデバイスが、可能な限り速い速度で送信するようにネゴシエートできるようにします。 H =半二重（同時に一方向のみの通信） F =全二重（同時に双方向の通信） 10 = 10メガビット 100 = 100メガビット

例：半二重通信で100 Mbpsを使用して通信するようにTCP/IPポートを設定するには、次のように入力します。

```
apc> portspeed -s 100H
E000: Success
Reboot required for change to take effect.
```

エラーメッセージ：E000, E102

prompt

アクセス権：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用ユーザー

説明：現在ログオンしているユーザーのアカウントタイプを含むか除外するかを指定し、コマンドラインインターフェイスのプロンプトを設定します。この設定の変更は全ユーザーに許可されています。新しい設定が利用できるようにすべてのユーザーアカウントがアップデートされます。

パラメータ：

オプション	引数	説明
-s	long	プロンプトには現在ログオンしているユーザーのアカウントタイプが含まれます。
	short	デフォルトの設定です。プロンプトの長さは4文字です。 apc>

例：

```
apc> prompt -s long
E000: Success

Administrator@apc>prompt -s short
E000: Success
```

エラーメッセージ：E000, E102

pwd

アクセス権：スーパーユーザー、管理者、デバイスユーザー 、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：現在作業中のディレクトリへのパスを出力します。

パラメータ：なし

例：

```
apc> pwd
/

apc> cd logs
E000: Success

apc> pwd
/logs
```

エラーメッセージ：E000, E102

quit

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：CLIセッションを終了します。これは exit または bye コマンドと同じように動作します。

パラメータ：なし

例：

```
apc> quit
```

```
Bye
```

エラーメッセージ：なし

radius

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：既存のRADIUS設定を表示し、2つまでのRADIUSサーバーの基本的な認証パラメータを設定します。Web UIでは、追加の認証パラメータを使用できます。

RADIUSサーバーの設定方法の詳細については、Network Management Card 3 Security Handbookを参照してください。

パラメータ：

オプション	引数	説明
-a	<local | radiusLocal | radius>	RADIUS認証を設定します。 local = RADIUSは無効になっています。ローカル認証が有効になっています。 radiusLocal = RADIUS、次にローカル認証。RADIUSとローカル認証が有効になっています。最初にRADIUSサーバーからの認証が要求されます。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が有効になっています。ローカル認証が無効になっています。
-p1 -p2	<server 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。
-o1 -o2	<port>	プライマリまたはセカンダリRADIUSサーバーのポート番号です。 **注記**：RADIUSサーバーは、デフォルトで1812番ポートを使用してユーザー認証を行います。Rack ATSは1 ~ 65535のポートをサポートしています。
-s1 -s2	<server secret>	プライマリまたはセカンダリRADIUSサーバーとRack ATS間の共有秘密鍵です。
-t1 -t2	<server timeout>	Rack ATSが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時間 (秒単位) です。

例1：Rack ATSの既存のRADIUS設定を表示するには、radiusを入力して、ENTERキーを押します。

例2：セカンダリRADIUSサーバーに10秒のタイムアウトを設定するには、次のように入力します。

```
apc> radius -t2 10
E000: Success
```

エラーメッセージ：E000, E102

reboot

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：Rack ATSのみのネットワーク管理インターフェイスを再起動します。これは、Rack ATSの出力には影響しません。

オプション	説明
-Y	確認プロンプトをスキップします (大文字のYのみ) 。

例1：

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'YES' to continue or <ENTER> to cancel: YES
Rebooting...
```

例2：

```
apc> reboot -Y
E000: Success
Reboot Management Interface
Rebooting...
```

エラーメッセージ：E000, E100

resetToDef

アクセス権：スーパーユーザー、管理者

説明: 設定可能なすべてのパラメータをデフォルト値にリセットします。すべてのアカウントを削除し、イベントログとデータログを消去します。

> **注記**： 設定できない一部のパラメーターはリセットできません。resetToDefそれらは、formatコマンドを使用してファイルシステムをフォーマットすることによりRack ATSから削除するしかありません。

パラメータ：

オプション	引数	説明
-p	all | keepip	注意：すべてのパラメータをデフォルト値にリセットします。 all =イベントアクション、デバイス設定およびTCP/IP設定を含むすべての設定変更をリセットします。 keepip =TCP/IP設定を除きすべての設定変更をリセットします。

例：TCP/IP設定を除きすべての設定変更をリセットするには、次のように入力します。

```
apc> resettodef -p keepip
Reset to Defaults Except TCP/IP
Enter 'YES' to continue or <ENTER> to cancel: YES
```

エラーメッセージ：E000, E100

session

アクセス権：スーパーユーザー、管理者

説明:ログインしている者(ユーザー)、インターフェイス、アドレス、時刻とIDを記録します。

パラメータ：

オプション	引数	説明
-d	[-d <session nID>] (Delete/削除)	指定したセッションIDを持つ現在のユーザーのセッションを削除します。
-m	<enable | disable> (MultiUser Enable/複数のユーザーの有効化)	2人以上のユーザーが同時にログオンできるようにします。無効化すると、同じ時間に1人のユーザーのみログインできるようになります。
-a	<enable | disable> (Remote Authentication Override/リモート認証オーバーライド)	Rack ATSはRADIUSによるサーバーでのパスワードの保管をサポートしています。リモート認証オーバーライドを有効化すると、ローカルユーザに対して、Rack ATSに保存されているRack ATSのユーザー名とパスワードを使用してログオンするように許可します。

例：

```
apc> session
User    Interface  Address          Logged In Time      ID
-------------------------------------------------------

apc     Telnet     10.169.118.1-    00:00:03            19
                   00
E000: Success
```

エラーメッセージ：E000, E102

smtp

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：ローカル電子メールサーバーの設定を構成します。

パラメータ：

オプション	引数	説明
-f	<From Address>	Rack ATSが電子メールを送信するアドレスです。
-s	<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。
-p	<Port>	SMTPポート番号はデフォルトで25番となっています。一般的なポート番号は、暗号化されていない電子メールの場合は25番、SSL/TLS暗号化された電子メールの場合は465番および587番です。ポートの設定は、1 ~ 65535のいずれかのポートに変更することができます。
-a	<enable | disable>	SMTPサーバーが認証を必要とする場合、これを有効にしてください。
-u	<User Name>	SMTPサーバーが認証を必要とする場合、ここにユーザー名とパスワードを入力してください。
-w	<Password>	
-e	<none | ifavail | always | implicit>	暗号化のオプション： none：SMTPサーバーは、暗号化を必要としないか、サポートしません。 ifavail：SMTPサーバーは、STARTTLSをサポートしていることを通知しますが、接続の暗号化を必要としません。STARTTLSコマンドは、通知が与えられた後で送信されます。通常、25番のポートで使用されます。 always：SMTPサーバーは、サーバーへの接続の際にSTARTTLSコマンドの送信を必要とします。通常、587番のポートで使用されます。 implicit：SMTPサーバーは、暗号化を開始した接続のみ受け入れます。STARTTLSメッセージはサーバーに送信されていません。通常、465番のポートで使用されます。
-c	<enable | disable>	CAルート証明書を必要とします。 所属組織のセキュリティポリシーにより、SSL/TLS接続の暗黙の信頼が許可されていない場合にのみ有効にしてください。これを有効にする場合、SMTPサーバーとのTLS接続が成功するには、証明書ローダーを使用してRack ATS unitの証明書ストアにSMTPサーバ用の有効なCA証明書をインストールする必要があります。
-i	<証明書ファイル名>	証明書のファイル名です。

例：

```
apc> smtp
E000: Success

From:            address@example.com
Server:          mail.example.com
Port:            25
Auth:            disabled
User:            User
Password:        <not set>
Encryption:      none
Req. Cert:       disabled
Cert File:       <n/a>
```

エラーメッセージ：E000, E102

snmp

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：SNMP 1を有効化または無効化して、設定します。

注記： SNMPv1は、デフォルトで無効になっています。コミュニティ名(`-c[n]`)は、SNMPv1通信を確立する前に設定する必要があります。

パラメータ：

オプション	引数	説明
`-S`	`<enable | disable>`	SNMPv1を有効化または無効化します。
`-c [n]`	`<Community>`	コミュニティ名または文字列を指定します。
`-a [n]`	`<read | write | writeplus | disable>`	利用権限を示します。
`-n [n]`	`<IP or Domain Name>`	ネットワーク管理ステーションのIPv4/IPv6アドレスまたはドメイン名を指定します。
`[n]` =アクセス制御番号： 1、2、3または4		

例：SNMPのバージョン1を有効化するには、次のように入力します。

```
apc> snmp -S enable
E000:  Success
Reboot required for change to take effect.
```

エラーメッセージ： `E000, E102`

snmpv3

アクセス権：スーパーユーザー、管理者

説明:SNMPv3を有効化または無効化し、設定します。

注記： SNMPv3はデフォルトで無効になっています。SNMPv3通信を確立する前に、パスフレーズ（`-a[n], -c[n]`）を設定して有効なユーザープロファイルを有効化する必要があります。

パラメータ：

オプション	引数	説明
`-S`	`<enable | disable`	SNMPv3を有効化または無効化します。
`-u[n]`	`<User Name>`	ユーザー名、認証フレーズと暗号化フレーズを指定します。
`-a[n]`	`<Auth phrase>`	
`-c[n]`	`<Crypt phrase>`	
`-ap[n]`	`<sha | md5 | none>`	認証プロトコルの種類を示します。
`-pp[n]`	`<aes | des | none>`	プライバシー（暗号化）プロトコルを示します。
`-ac[n]`	`<enable | disable`	アクセスを有効化または無効化します。
`-au[n]`	`<User profile name>`	指定したユーザープロファイルにアクセス権を付与します。
`-n[n]`	`<IP or Domain Name>`	ネットワーク管理ステーションのIPv4/IPv6アドレスまたはホスト名を指定します。
`[n]` =アクセス制御番号= 1、2、3、~8		

例：「JMurphy」ユーザーにレベル2のアクセス権を付与するには、次のように入力します。

```
apc> snmpv3 -au2 "JMurphy"
E000: Success

*Reboot required for change to take effect
```

エラーメッセージ：`E000, E102`

snmptrap

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：SNMPトラップ生成を有効化または無効化します。

パラメータ：

オプション	引数	説明
`-c[n]`	`<Community>`	コミュニティ名または文字列を指定します。
`-r[n]`	`<Receiver NMS IP>`	トラップレシーバのIPv4/IPv6アドレスまたはホスト名です。
`-l[n]`	`<Language code>`	言語を指定します。現時点では、使用できる唯一のオプションは英語(`enUS`)です。
`-t[n]`	`[snmpV1 | snmpV3]`	トラップの種類を指定します。SNMPv1またはSNMPv3
`-p[n]`	`<Port>`	このトラップレシーバのためのSNMPトラップポート番号を指定します（デフォルトでは162番ポート）。範囲は1 ~ 65535です。
`-g[n]`	`[enable | disable]`	このトラップレシーバのためのトラップ生成を有効化または無効化します。デフォルトでは有効になっています。

オプション	引数	説明
-a[n]	[enable | disable]	このトラップレシーバのためのトラップ認証を有効化または無効化します（SNMPv1のみ）。
-u[n]	<profile1 | profile2 | profile3 | profile4>	このトラップレシーバのためのユーザープロファイルの識別子を選択します（SNMPv3のみ）。
n =トラップレシーバ番号 = 1、2、3、4、5または6		

例：デフォルトの英語を使用して、publicのコミュニティ名、レシーバ1のIPアドレス10.169.118.100を使用して、レシーバ1のためのSNMPv1トラップを有効化し設定するには、次のように入力します。

```
apc> snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1 snmpV1
-g1 enable
E000: Success
```

エラーメッセージ：E000, E102

ssh

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：SSHサーバーキーを表示、削除、生成します。

注記： 次のオプションを使用するには、ssh keyコマンドを使用する必要があります。

パラメータ：

オプション	引数	説明
-s		使用中のSSHサーバーキーを表示します。
-f		使用中のSSHサーバーキーのフィンガープリントを表示します。
-d		使用中のSSHサーバーキーを削除します。
-i	<filename>.p15	PKCS #15ファイルからSSHサーバーキーをインポートします。
-ecdsa	<256>（ビットサイズ）	ビット単位で指定されたサイズの楕円曲線デジタル署名アルゴリズム(ECDSA)のSSHサーバーキーを生成します。
-rsa	<1024 | 2048 | 4096>（ビットサイズ）	ビット単位で指定されたサイズのリベスト・シャミア・アドレマン(RSA)のSSHサーバーキーを生成します。

例1：SSHサーバーキーを削除するには、次のように入力します。

```
apc> ssh key -d
E000: Success
```

例2：NMCセキュリティウィザードCLIユーティリティにより生成された.p15ファイルからSSHサーバーキーをインポートするには、次のように入力します。

```
apc> ssh key -i nmc.p15
E000: Success
```

エラーメッセージ： E000, E102

ssl

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：Rack ATS Unitの公開鍵とWeb UI証明書を構成、管理し、証明書署名要求(CSR)を作成します。

注記： このコマンドには、次の3種類のオプションがあります (`key`、`csr`と`cert`)。

公開鍵の構成(`key`):

オプション	引数	説明
`-s`		使用中の公開鍵を表示します。
`-d`		使用中の公開鍵を削除します。
`-i`	`<filename>.p15`	PKCS #15ファイルから公開鍵をインポートします。
`-ecdsa`	`<256 | 384 | 521>`	ビット単位で指定されたサイズの楕円曲線デジタル署名アルゴリズム(ECDSA)の公開鍵を生成します。
`-rsa`	`<1024 | 2048 | 4096>`	ビット単位で指定されたサイズのリベスト・シャミア・アドレマン(RSA)の公開鍵を生成します。

*PKS#15ファイルはNMCセキュリティウィザードで生成できます(www.se.comで利用可能)。

例1：新しいECDSA-521公開鍵を生成するには、次のように入力します。

```
apc> ssl key –ecdsa 521
E000: Success
```

例2：NMCセキュリティウィザードCLIユーティリティにより生成された.p15ファイルから公開鍵をインポートするには、次のように入力します。

```
apc> ssl key -i nmc.p15
E000: Success
```

証明書署名要求の構成(`csr`):

オプション	引数	説明
`-s`	`<File Name>`	現在のCSRを表示します。ファイルパスが指定されていない場合、コマンドはデフォールトの場所ssl/nmc.csrをチェックします。
`-q`	`<File Name>`	アクティブな構成からCSRを作成します。ファイルパスを指定されていない場合、CSRはデフォルトの場所ssl/nmc.csrに保存されます。
`-CN`	`<Common Name>`	カスタムCSRを作成します。共通名とは、Rack ATSの完全修飾ドメイン名(FQDN)です。例えば、そのIPアドレスまたは*.nmc.local。
カスタム証明書署名要求(CSR)のオプション。**注記**：以下のオプションは、`-CN`のためにのみ使用できます。		
`-O`	`<organization>`	組織名。
`-OU`	`<organization unit>`	証明書を取り扱う組織の部門。
`-C`	`<country>`	組織が所在する2文字の国コード。
`-san`	`<Common Name | IP Address>`	Rack ATSの共通名またはIPアドレスです。

注記： 作成された証明書署名要求は、Rack ATS　Unitのsslディレクトリに保存されます。「dir, 56 ページ」を参照してください。

例3：現在の構成からクイックCSRを作成するには、次のように入力します。

```
apc> ssl csr -q
E000: Success
```

例4：最小CSRを作成するには、次のように入力します。

```
apc> ssl csr -CN 192.168.1.100 -C US
E000: Success
```

例5：カスタム証明書署名要求(CSR)を作成するには、次のように入力します。

```
apc> ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local
-san 190.0.2.0
E000: Success
```

Web UIの証明書の構成(cert):

オプション	引数	説明
-s	<File Name>	指定した証明書を表示します。**注記**：引数なしでこのオプションを実行すると、使用中の証明書が表示されます。
-f	<File Name>	指定された証明書のフィンガープリントを表示します。**注記**：引数なしでこのオプションを実行すると、使用中の証明書のフィンガープリントが表示されます。
-i	<File Name>	証明書をインポートします。
注記：この引数は、3つのオプションすべてに対して省略可能です。ファイルパスが指定されていない場合、コマンドはデフォールトの場所ssl/nmc.crtをチェックします。		

例6：有効な証明書を表示するには、次のように入力します。

```
apc> ssl cert -s
E000: Success

Certificate
-----------
  Serial Number: XXXXxXXXXXXxXXXXx
  Issuer: CN=., C=US
  Validity:
      Not Before: Mon Oct 11 16:46:44 2021 UTC
      Not After : Sat Dec 15 23:59:59 2035 UTC
  Subject: CN=., C=US
  Subject Public Key Info:
      Public Key Algorithm: ECDSA (256 bit)
      X:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
      Y:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
      Curve: P-256
  Thumbprint: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  Fingerprint:
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

例7：sslディレクトリにあるnmc.crtを表示するには、次のように入力します。

```
ssl cert -s ssl/nmc.crt
```

例8：その他の証明書(*other.crt*)をインポートするには、次のように入力します。

```
apc> ssl cert -i other.crt
```

エラーメッセージ： E000, E102

system

アクセス権：スーパーユーザー、管理者

説明:システム名、連絡先、ロケーションを表示および設定します。システムメッセージ、起動時刻、日時、ログオン中のユーザー、高レベルシステムステータスP、N、Aを設定します。(システムステータスの詳細については、メイン画面について, 42 ページを参照してください)。

パラメータ：

オプション	引数	説明
-n	<system name>	デバイス名、デバイスの責任者氏名およびデバイスの物理的な設置場所を定義します。
-c	<system contact>	

-l	<system location>	**注記**：値を複数の単語で定義する場合、当該値を引用符で囲む必要があります。これらの値は、StruxureWare Data Center Expert、EcoStruxure IT ExpertおよびRack ATS UnitのSNMPエージェントによりも使用されます。
-m	<system message>	Web UI、CLI（シリアル、Telnet、SSH）、FTPまたはSCPのログオンページに、設定可能なカスタムメッセージまたはバナーを表示します。
-s	<enable | disable>	ホスト名がシステム名と同期され、両方のフィールドが自動的に同じ値になります。 これは、dns -yを使用した場合と同じです。 **注記**：この機能を有効にすると、システム名の識別子に空白文字が使えなくなります（ホスト名フィールドに同期されるためです）。

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。

```
apc> system -l "Test Lab"
E000: Success
```

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。

```
apc> system -n "Don Adams"
E000: Success
```

エラーメッセージ：E000, E102

tacacs+

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：既存のTACACS+設定を表示し、最大2台のTACACS+サーバーのための基本的な認証パラメータを設定します。

オプション	引数	説明
-p1 -p2	<server IP>	プライマリまたはセカンダリTACACS+サーバーのサーバー名またはIPアドレスです。 .
-o1 -o2	<port>	プライマリまたはセカンダリTACACS+サーバーのポート番号です。 **注記**： TACACS+サーバーは、デフォルトではポート49を使用してユーザー認証を行います。NMCは1 ~ 65535のポートをサポートしています。
-s1 -s2	<server secret>	プライマリまたはセカンダリTACACS+サーバーとNMC間の共有秘密鍵です。
-t1 -t2	<server timeout>	NMCがプライマリまたはセカンダリTACACS+サーバーからの応答を待ちつづける時間（秒単位）です。
-d1 -d2		プライマリまたはセカンダリTACACS+サーバーの構成を削除します。
-r	<0 – 15>	読み取り専用ユーザーの権限レベルです。
-a	<0 – 15>	管理者の権限レベルです。

例1：NMCの既存のTACACS+設定を表示するには、次のように入力します。

```
tacacs+
```

例2 :セカンダリTACACS+サーバーのために10秒のタイムアウトを設定するには、次のように入力します。

```
tacacs+ -t2 10
```

tcpip

アクセス権：スーパーユーザー、管理者

説明: Rack ATSのためのIPV4 TCP/IP設定を表示し、手動で設定します。

パラメータ：

オプション	引数	説明
-S	enable | disable	TCP/IP v4を有効化または無効化します。
-l	<IPv4 address>	*xxx.xxx.xxx.xxx*の形式でRack ATSのIPアドレスを入力します。
-s	<subnet mask>	Rack ATSのサブネットマスクを入力します。
-g	<gateway>	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	<domain name>	DNSサーバーで設定したDNS名を入力します。
-h	<host name>	Rack ATSが使用するホスト名を入力します。

例1：Rack ATSのネットワーク設定を表示するには、次のように入力します。

```
apc> tcpip
E000: Success
```

```
IP Address:      192.168.1.50
MAC Address:     XX XX XX XX XX XX
Subnet Mask:     255.255.255.0
Gateway:         192.168.1.1
Domain Name:     example.com
Host Name:       HostName
```

例2：IPアドレスを手動で設定するには、192.168.1.49を入力します。

```
apc> tcpip -i 192.168.1.49
E000: Success
Reboot required for change to take effect
```

エラーメッセージ：E000, E102

tcpip6

アクセス権：スーパーユーザー、管理者

説明:IPv6を有効化します。Rack ATSのネットワーク設定を表示し、手動で設定します。

パラメータ：

オプション	引数	説明
-S	enable | disable	IPv6を有効化または無効化します。
-man	enable | disable	Rack ATSのIPv6アドレスを手動で指定できるようにします。
-auto	enable | disable	Rack ATSのIPv6アドレスを自動的に設定できるようにします。
-i	<IPv6 address>	Rack ATSのIPv6アドレスを設定します。
-g	<IPv6 gateway>	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 | stateful | stateless | never	DHCPv6モードを、stateful（アドレスおよびその他の情報用、ステータスを維持する）、stateless（アドレス以外の情報用、ステータスが維持されない）またはneverというrouter制御パラメータを選択して設定します。

例1：Rack ATSのネットワーク設定を表示するには、tcpip6を入力して、ENTERキーを押します。

```
apc> tcpip6
E000: Success

IPv6:                    enabled
Manual Settings:         disabled

IPv6 Address:            ::/64
MAC Address:             XX XX XX XX XX XX
Gateway:                 ::
IPv6 Manual Address:     disabled
IPv6 Autoconfiguration: enabled
DHCPv6 Mode:             router controlled
```

例2：2001:0:0:0:0:FFD3:0:57abのIPv6アドレス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
```

エラーメッセージ：E000, E102

user

アクセス権：スーパーユーザー、管理者

説明：各アカウントタイプのユーザー名、パスワードおよび非アクティブ時のタイムアウトを設定します。

注記： ユーザー名は編集できません。削除して新しいユーザーを作成する必要があります。

注記： スーパーユーザーのアカウント設定をリモートで変更するには、現在のパスワード(`-cp`)を入力しなければなりません。

パラメータ：

オプション	引数	説明
`-n`	`<user>`	ユーザーを表示します。
`-cp`	`<current password>`	スーパーユーザーの場合、現在のパスワードを指定する必要があります。 **注記**：`-cp`このオプションは、スーパーユーザーの設定をリモートで変更する場合にのみ必要です。
`-pw`	`<user password>`	ユーザーのために次のオプションを指定します。 **注記**：説明は引用符で囲む必要があります。
`-pe`	`<user permission>`	
`-d`	`<user description>`	
`-e`	`enable | disable`	特定のユーザアカウントのためのアクセスを有効化または無効化します。
`-te`	`enable | disable`	タッチスクリーンによるアクセスを有効化または無効化します。
`-tp`	`<touch screen access pin>`	このオプションは特定のデバイスでのみ利用できます。
`-tr`	`enable | disable`	タッチスクリーンのリモート認証オーバーライドを有効化します。このオプションは特定のデバイスでのみ利用できます。このオーバーライドを有効化すると、Rack ATSは、ローカルユーザーに対して、Rack ATSに保存されているRack ATSのパスワードを使用してログオンすることを許可します。
`-st`	`<session timeout>`	キーボードがアイドル状態のときに、ユーザーが自動的にログオフされるまでのセッションの継続時間を指定します。
`-sr`	`enable | disable`	シリアルコンソール（CLI）接続（シリアルリモート認証オーバーライドとも呼ばれる）を使用してRADIUSをバイパスします。
`-el`	`enable | disable`	イベントログの色分けを表示します。
`-lf`	`tab | csv`	ログファイルをエクスポートする際の形式を表示します。
`-ts`	`us | metric`	温度スケール（華氏または摂氏）を表示します。
`-df`	`<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>`	日付の形式を指定します。
`-lg`	`<language code (e.g. enUs)>`	ユーザーの使用言語を指定します。現在利用できる言語は英語のみです。
`-del`	`<user name>`	ユーザーを削除します。
`-l`		現在のユーザー一覧を表示します。

例1：「JMurphy」ユーザーのためにログオフ時間を10分に変更するには、次のように入力します。
`user -n "JMurphy" -st 10`

例2：「apc」のスーパーユーザーのためにログオフ時間を10分に変更するには、次のように入力します。`user -n "apc" –cp <password> –st 10`

エラーメッセージ：`E000, E102`

userauth

アクセス権：スーパーユーザー、管理者、ネットワーク専用ユーザー

説明：ユーザー認証方法を表示または構成します。ローカル認証、LDAP、RADIUS、およびTACACS+プロトコルがサポートされています。

オプション	引数	説明
-l	first | last | off	ローカルユーザーデータベースを確認するかどうか、そしていつ確認するかを指定します。 **最初**：ローカルユーザーデータベースが必ず最初に確認されます。ユーザー名が見つかった場合は、パスワードが確認され、ログインが成功するか失敗するかが決まります。ユーザー名が見つからない場合は、リモート認証が有効になっていれば使用されます。 **最後**：ローカルユーザーデータベースは、リモート認証を試行したらリモート認証サーバーへの接続でエラーが発生した場合、リモート認証の後で確認されます。リモート認証がoffになっている場合、最初と同じ動作になります。 **off**：ローカルユーザーデータベースは確認されません。 **注記**：リモート認証サーバーが停止したり、NMCの設定が間違っている場合にNMCから完全にロックアウトされる可能性があるため、この設定をoffに設定することはお勧めしません。offを使用する場合、リモート認証オーバーライド設定（セッション – a）を有効にし、スーパーユーザーまたは管理者のためにシリアルリモート認証オーバーライドオプション（ユーザー – sr）を設定することを強くお勧めします。 **注記**：ローカルユーザー認証とリモートユーザー認証の両方の設定がoffになっている場合、ローカルユーザー認証が自動的に「最初」に設定されます。 .
-r	off | radius | tacacs+ | ldap	リモート認証プロトコルを使用するか、使用する場合どれを使用するかを指定します。 **off**：リモートユーザー認証を使用せず、常にローカルユーザー認証を実行します。 **radius**：リモートユーザー認証ではRADIUSが使用されます。 **tacacs+:** リモートユーザー認証ではTACACS+が使用されます。 **ldap:** リモートユーザー認証ではLDAPが使用されます。

例：最初にローカル認証、次にTACACS+認証を設定するには、次のように入力します。

```
userauth -l first -r tacacs+
```

userdflt

アクセス権：スーパーユーザー、管理者

説明:デフォルトのユーザー設定を確立した「ユーザー」への補助機能です。デフォルトのユーザー設定には、主要な機能が2つあります。

- スーパーユーザーまたは管理者のレベルのアカウントが新しいユーザーを作成するときに、各フィールドで使用されるデフォルト値を決定します。これらの値は、設定がシステムに適用される前に変更することができます。
- リモートユーザー（RADIUSなど、リモートで認証され、システムに保存されていないユーザーアカウント）の場合、認証サーバーから提供されない値のためにこれらの値が使用されます。例えば、RADIUSサーバーがユーザーに温度設定を提供しない場合、このセクションで定義された値が使用されます。

パラメータ：

オプション	引数	説明
-e	<enable | disable>	ユーザーが作成時にデフォルトで有効または無効にされます。
-pe	<Administrator | Device | Read-Only | Network-Only>	ユーザーの権限レベルとアカウントタイプを指定します。
-d	<user description>	ユーザーの説明を提供します。説明は引用符で囲む必要があります。
-st	<session timeout> minute(s)	デフォルトのセッションタイムアウトを指定します。
-bl	<bad login attempts>	システムがアカウントを無効にするまでに許可されているユーザーが行った誤ったログイン試行回数です。この制限に達すると、アカウントがロックされたことをユーザーに知らせるメッセージが表示されます。アカウントを再度有効にしてユーザーが再度ログインできるようにするには、スーパーユーザーまたは管理者レベルのアカウント権が必要です。 **注記**：スーパーユーザーのアカウントはロックアウトされることがありませんが、必要に応じて手動で無効にすることができます。
-el	<enable | disable>（イベントログの色分け）	イベントログの色分けを有効化または無効化します。
-lf	<tab | csv>（エクスポートログの形式）	ログのエクスポート形式（タブ区切りまたはCSV）を指定します。
-ts	<us | metrics>（温度スケール）	ユーザーの温度スケールを指定します。この設定は、ユーザー設定が利用できない場合（電子メール通知など）にも使用されます。
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>（日付形式）	ユーザーが希望する日付形式を指定します。
-lg	<language code (enUs, etc)>	ユーザーの使用言語です。現時点ではenUs（米国英語）のみがサポートされています。
-sp	<enable | disable>	強力なパスワードの要件です。有効な場合： • パスワードは8～64文字でなければなりません。 • パスワードは、小文字、大文字、数字、および記号(! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ' { | } ~)を少なくとも1つずつ含む必要があります。
-pp	<interval in days>	要求されるパスワードの変更間隔です。

例：デフォルトのユーザーのセッションタイムアウトを60分に設定するには、次のように入力します。

```
apc> userdflt -st 60
E000: Success
```

エラーメッセージ：E000, E102

web

アクセス権：スーパーユーザー、管理者

説明：HTTPまたはHTTPSによるWeb UIへのアクセスを有効にします。

セキュリティを強化するために、HTTPおよびHTTPSのためのポートを、5000～32768番のいずれかの未使用のポートに変更することができます。この場合、ポート番号を指定するためにブラウザのアドレス欄にコロン（:）を入力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、次のように入力します。

```
http://152.214.12.114:5000
```

パラメータ：

オプション	引数	説明
-h	enable | disable	HTTPによるユーザーインターフェイスへのアクセスを有効化または無効化します。 デフォルトでは、HTTPが無効になっています。
-s	enable | disable	HTTPSによるユーザーインターフェイスへのアクセスを有効化または無効化します。

		デフォルトでは、HTTPSが有効になっています。 HTTPSが有効になっている場合、データは送信中に暗号化され、デジタル証明書によって認証されます。
-mp	<minimum protocol>	Webインターフェイスが使用する最小プロトコルを指定します。SSL v3.0、TLS v1.1またはTLS v1.2。
-ph	<http port #>	HTTPがRack ATSと通信するために使用するTCP/IPポートを指定します（デフォルトでは80番）。その他の使用可能な範囲は5000 ~ 32768です。
-ps	<https port #>	HTTPSがRack ATSと通信するために使用するTCP/IPポートを指定します（デフォルトでは443番）。その他の使用可能な範囲は5000 ~ 32768です。
-lsp	enable | disable	Web UIで限定ステータスページへのアクセスを有効化または無効化します。
-lsd	enable | disable	ウェブブラウザでデバイスのIPまたはホスト名にアクセスするときに、デフォルトページとして使用する限定ステータスページを有効化または無効化します。
-cs	<0 | 1 | 2 | 3 | 4>	TLS v1.2暗号化スイートのセキュリティレベルを0 ~ 4の間で選択します。ここで、4はセキュリティレベルが最も高く、0はセキュリティレベルが最も低いことを示します。デフォルト値は4です。 **注記**：-csオプションは、-mpがTLS v1.2に設定されている場合にのみ適用されます。 0 ~ 4の値を入力すると、CLIは現在許可されているSSL暗号化スイートのリストで応答します。
-hs	enable | disable	HTTP Strict Transport Security Header（HSTS)の応答ヘッダーを有効化または無効化します。

例1：Web UIへのすべてのアクセスを抑制するには、次のように入力します。

```
apc> web -h disable -s disable
```

例2：HTTPで使用するTCP/IPポートを指定するには、次のように入力します。

```
apc> web -ph 80
E000: Success
```

エラーメッセージ：E000, E102

whoami

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー

説明：現在のユーザーに関するログイン情報を提供します。

パラメータ：なし

例：

```
apc> whoami
E000: Success
admin
```

エラーメッセージ：E000, E102

wifi

将来の使用のために予約されています。

xferINI

アクセス権：スーパーユーザー、管理者

説明：シリアル接続を介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、INIファイルをアップロードするためにXMODEMを使用します。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が再起動するため、再度ログオンする必要があります。
- NMSのためのデフォルトのボーレートと違うボーレートをファイル転送に指定した場合、NMS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なおさなければなりません。

パラメータ：なし

例：

```
apc> xferINI
Enter 'YES' or 'Y' to continue or <ENTER> to cancel: <user
enters 'YES' or 'Y'>
---- File Transfer Baud Rate-----------------------
     1- 2400
     2- 9600
     3- 19200
     4- 38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.

apc>
```

エラーメッセージ：なし

xferStatus

アクセス権：スーパーユーザー、管理者

説明：前回のファイル転送の結果を表示します。

パラメータ：なし

例：

```
apc> xferStatus
E000: Success

Result of last file transfer: Successful
```

転送結果のコードについては前回の転送結果コード, 30 ページを参照してください。

エラーメッセージ：E000

デバイスコマンドの説明

ネットワークポート共有コマンド

CLIでは、ゲストRack ATSユニットにコマンドを送信できます。ユーザは、コマンドを実行するRack ATSのDisplay IDの後にコロンを最初の引数の前（またはコマンドに通常引数がない場合は最初の引数）に指定することができます。Display IDがオプションの場合（省略）、単にホストRack ATSにコマンドを送信します。

たとえば、次のようになります。`<command> [<id#>:]<arg1> <arg2>`

これにより、`<command> <arg1> <arg2>`がRack ATSに `[<id#>:]` で指定された表示IDで送信されます。Display IDの後にコロン(:)が続き、その後にスペースのない`arg1`が続きます。引数の区切りにはスペースを使用します。

aboutATS

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明ATSコントローラの情報を表示します。

パラメータ：None

例：

```
apc> aboutATS
E000: Success
Model:                          AP4450A
Firmware Rev:                   0.0.2.5
Firmware Date:                  09/23/23
Hardware Rev:                   R01
Manufacture Date:               02/04/2023
Serial Number:                  XXXXXXXXXXX
```

エラーメッセージ`E000, E102`

atsMeasure

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明電源の電力測定値およびATSの電力測定値を読み込みます。

パラメータ：なし。

例：

```
apc> atsMeasure
E000: Success
Source A Freq:                60 Hz
Source A Voltage:             121 V
Source B Freq:                60 Hz
Source B Voltage:             121 V
Total Output Power:           1.00 kVA
Source A 24V Power Supply:    24 V
Source B 24V Power Supply:    24 V
Source A Boost Voltage:       40 V
Source B Boost Voltage:       40 V
3.3 V Power Supply:           3.3 V
```

エラーメッセージE000, E102

atsStatus

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明Rack ATSのステータス情報を読み込みます。

パラメータ：なし。

例：

```
apc> atsStatus
E000: Success
Communication Status:         OK
Selected Source:              Source B
Preferred Source:             Source B
Switch Status:                OK
Front Panel:                  Unlocked
Source A:                     OK
Source B:                     Selected
Phase Synchronization:        Sync
Source A 24V Power Supply:    OK
Source B 24V Power Supply:    OK
Source A 24V Boost Voltage:   OK
Source B 24V Boost Voltage:   OK
3.3V Power Supply:            OK
```

エラーメッセージE000, E102

bkLowLoad

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明低負荷しきい値電流のバンクをアンペア単位で設定または表示します。このコマンドをサポートするのは、2つ以上のサーキットブレーカーを備えた単相SKUだけです。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<all | bank#>	all = すべてのバンク番号 Bank#（バンク#）：単一の番号かハイフン区切りの番号範囲、または単一の番号および/または番号範囲をカンマで区切って指定
<current>	新しいバンクしきい値（A）

備考：最大バンク番号は2です。Rack ATSにサーキットブレーカが2つある場合は、バンクの合計しきい値が表示されます。

例 1すべてのバンクの低負荷しきい値を表示します。

```
apc> bkLowLoad all
E000: Success
total:     0 A
1:         0 A
2:         0 A
```

例 2バンク1の低負荷しきい値を表示および設定します。

```
apc> bkLowLoad 1
E000: Success
1: 0 A

apc> bkLowLoad 1 1
E000: Success
```

例 2バンク1～2の低負荷しきい値を表示および設定します。

```
apc> bkLowLoad 1-2
E000: Success
total:     2 A
1:         1 A
2:         1 A

apc> bkLowLoad 1-2 1
E000: Success
```

エラーメッセージE000, E102

bkNearOver

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明過負荷直前しきい値電流のバンクをアンペア(A)で設定または表示します。このコマンドは、2つ以上のブレーカを備えた単相モデルでのみサポートされます。すべてのバンク、単一バンク、範囲、または単一バンクと範囲のコンマ区切りのリストを指定できます。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<all | bank#>	all = すべてのバンク番号 bank#: = 単一の番号か、ハイフンで区切られた番号の範囲、または単一のバンク番号および/または番号範囲をカンマで区切って指定。
<current>	新しいバンクしきい値（A）

備考：最大バンク番号は2です。Rack ATSにサーキットブレーカが2つある場合は、バンクの合計しきい値が表示されます。

例 1すべてのバンクの過負荷直前しきい値を表示および設定します。

```
apc> bkNearOver all
E000: Success
total:     10 A
1:         10 A
2:         10 A

apc> bkNearOver all 10
E000: Success
E000: Success
E000: Success
```

例 2バンク1の過負荷直前しきい値を表示および設定します。

```
apc> bkNearOver 1
E000: Success
1: 10 A

apc> bkNearOver 1 12
E000: Success

apc> bkNearOver all
E000: Success
total:     12 A
1:         12 A
2:         10 A
```

例 3ゲストユニット3のバンク1と2の過負荷直前しきい値設定を表示します。

```
apc> bkNearOver 3:1-2
E000: Success
1: 16 A
2: 16 A
```

エラーメッセージE000, E102

bkOverLoad

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明過負荷電流しきい値のバンクをアンペア単位で設定または表示します。このコマンドをサポートするのは、2つ以上のサーキットブレーカーを備えた単相SKUだけです。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<all | bank#>	all = すべてのバンク番号 bank#: = 単一の番号か、ハイフンで区切られた番号の範囲、または単一のバンク番号および/または番号範囲をカンマで区切って指定。
<current>	新しいバンクしきい値（A）

備考：最大バンク番号は2です。Rack ATSにサーキットブレーカが2つある場合は、バンクの合計しきい値が表示されます。

例 1すべてのバンクの過負荷しきい値を表示します。

```
apc> bkOverLoad all
E000: Success
total:     24 A
1:         14 A
2:         14 A
```

例 2バンク1の過負荷しきい値を表示します。

```
apc> bkOverLoad 1
E000: Success
1: 14 A
```

例 3バンク1と2の過負荷しきい値を設定します。

```
apc> bkOverLoad 1–2 16
E000: Success

apc> bkOverLoad all
E000: Success
total:     32 A
1:         16 A
2:         16 A
```

エラーメッセージE000, E102

bkPeakLoad

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明バンクからのピーク負荷測定値を表示します。このコマンドをサポートするのは、2つ以上のサーキットブレーカーを備えた単相SKUだけです。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<all | bank#>	all = すべてのバンク番号 bank#: = 単一の番号か、ハイフンで区切られた番号の範囲、または単一のバンク番号および/または番号範囲をカンマで区切って指定。
<current>	新しいバンクしきい値（A）

備考：最大バンク番号は2です。Rack ATSにサーキットブレーカが2つある場合は、バンクの合計しきい値が表示されます。

例：

```
apc> bkPeakLoad all
E000: Success
total:     11.0 A
1:         5.0 A
2:         5.0 A

apc> bkPeakLoad 1
E000: Success
1: 5.0 A

apc> bkPeakLoad 1-2
E000: Success
1: 5.0 A
2: 6.0 A
```

エラーメッセージE000, E102

bkReading

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明バンクの電流読取（測定値）をアンペア単位で表示します。このコマンドは、2つ以上のブレーカを備えた単相モデルでのみサポートされます。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<all | bank#>	all = すべてのバンク番号 bank#: = 単一の番号か、ハイフンで区切られた番号の範囲、または単一のバンク番号および/または番号範囲をカンマで区切って指定。
<current>	新しいバンクしきい値（A）

備考：最大バンク番号は2です。Rack ATSにサーキットブレーカが2つある場合は、バンクの合計しきい値が表示されます。

例：

```
apc> bkReading 1
E000: Success
1: 6.3 A

apc> bkReading all
E000: Success
total:     11.4 A
1:         6.3 A
2:         5.1 A

apc> bkReading 1–2
E000: Success
1: 6.3 A
2: 5.1 A
```

エラーメッセージE000, E102

dispID

アクセス：スーパーユーザー、管理者

説明: ディスプレイ ID の設定または読み取り。

パラメータ

引数	説明
<id#>:	NPS グループ内のユニットの ID (グループのサイズに応じて 1 ~ 32 の範囲)
<value>	ユニットに割り当てられる ID (1 ~ 32 の範囲)

例：

```
apc> dispID
E000: Success
ATS ID: 3*

apc> dispID 2
E000: Success

apc> dispID 2:4
E000: Success
```

Error Messages: E000, E102

eventCounts

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明：Rack ATSコントローラから報告されたイベントカウントを表示または除去します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのIDです。(グループのサイズに応じて1 ~ 32を指定できます。)
<0>	すべてのイベントカウントを0に設定します。

例：

```
apc> eventcounts
E000: Success
Event Counts
- - - - - - - - -
Redundancy Loss:              1
Source Switch:                0
Source Preference Change:     0
Spike/Dropout:                0
Surge/Droop:                  0
Frequency out of Range:       0
```

エラーメッセージ： E000, E100, E102

freqDeviat

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明許容可能な周波数変動範囲を読み込みまたは設定します（Hz）。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<3 | 5 | 10>	許容可能な周波数変動の新しい範囲：公称周波数の+/-3、5、10 Hz。

備考：周波数（atsMeasure, 91 ページを参照）が50 Hz、vSensitvty（vSensitvty, 121 ページ を参照）がHighに設定されている場合、freqDeviatは3または5となります。

例：

```
apc> freqDeviat
E000: Success
Frequency Deviation:          3 Hz
```

エラーメッセージE000, E100, E102

frontPanel

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明前面パネルの電源ボタンのコントロールを設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<locked | unlocked>	使用する前面パネルをロックまたはロック解除します。

例：

```
apc> frontPanel
E000: Success
Front Panel:unlocked

apc> frontPanel locked
E000: Success
```

エラーメッセージE000, E100, E102

湿度センサーの注意：

Humidity relatedコマンドを使用するには、オプションのAPC Temperature/Humidity Sensor (AP9335TH)をRack ATSに接続する必要があります。

humAlGen

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明湿度アラームを有効または無効に設定します。

パラメータ：

引数	説明
`<id#>:`	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）。
`<enable | disable>`	`enable` =湿度アラームを有効にします。 `disable` =湿度アラームを無効にします。

例：

```
apc> humAlGen enable
E000: Success

apc> humAlGen disable
E000: Success
```

エラーメッセージ`E000, E102`

humHyst

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明湿度しきい値のヒステリシス値を設定し、読み取ります。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<value>	新しいしきい値ヒステリシス値(% RH)

例：

```
apc> humHyst
E000: Success
6 %RH

apc> humHyst 5
E000: Success
```

エラーメッセージE000, E102

humLow

アクセス権：スーパーユーザー、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トで設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<humidity>	新しい低湿度しきい値

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。

```
apc> 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。

```
apc> humLow 12
E000: Success
```

例 3ゲストRack ATS 3の低湿度しきい値を表示するには、次のように入力します。

```
apc> humLow 3:
E000: Success
10 %RH
```

エラーメッセージE000, E102

humMin

アクセス権：スーパーユーザー、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。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<humidity>	新しい最低湿度しきい値

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。

```
apc> 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。

```
apc> humMin 8
E000: Success
```

例 3ゲストRack ATS 2の湿度値を表示するには、次のように入力します。

```
apc> humReading 2:
E000: Success
48 %RH
```

エラーメッセージE000, E102

humReading

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明センサーの湿度値を表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）

例 1湿度の値を表示するには、次のように入力します。

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

例 2ゲストRack ATS 2の湿度値を表示するには、次のように入力します。

```
apc> humReading 2:
E000: Success
48 %RH
```

エラーメッセージE000、E102、E201

humStatus

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明センサーのステータスを表示します。応答：Not Connected（接続なし）、Min Threshold Violation（最小しきい値違反）、Low Threshold Violation（低しきい値違反）、Normal（通常）。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）

例：湿度センサーのステータスを表示するには、次のように入力します。

```
apc> humStatus 1
Not Connected
```

エラーメッセージNone

lcd

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明：LCDディスプレイのステータスを設定または読み取りします。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットID（グループのサイズにより1 ~ 32からなります）
<on | off>	LCDのオン/オフを切り替えます。

例：

```
apc> lcd
E000: Success
LCD Status: On

apc> lcd off
E000: Success
```

エラーメッセージ： E000, E100, E102

lcdBlink

アクセス権：スーパーユーザー、管理者

説明ディスプレイを点滅させる分数を指定します。このコマンドは、LCD上のボタンを押すことでキャンセルできます。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1 ~ 32を指定できます）。
<time>	ディスプレイを点滅させる時間（分）。有効な範囲は[1-10]です。

例：

```
apc> lcdBlink 2
E000: Success
```

エラーメッセージE000, E102

lineVRMS

アクセス権：スーパーユーザー、管理者

説明電源の公称電源電圧（Ｖ）を読み込みまたは設定します。指定できる値は、Rack ATSモデルによって異なります。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<voltage>	電源線公称電圧(V)を設定します。

モデル	許容電圧
AP4421A、AP4422A、AP4423A、AP4424A	230
AP4430A、AP4432A	200または208
AP4431A、AP4433A、AP4434A	208
AP4450A	100または120
AP4452A、AP4453A	120
AP4452AJ	100

例：

```
apc> lineVRMS
E000: Success
Nominal Line Voltage: 120

apc> lineVRMS 124
E000: Success
```

エラーメッセージE000, E100, E102

logToFlash

アクセス権：スーパーユーザー、管理者

説明ログファイルをUSBフラッシュドライブにエクスポートします。ファイルは圧縮ファイルになります。event.txt、config.ini、debug.txt、data.txtが含まれます。例外が発生すると、dump.txtも含まれます。

パラメータ：`[<filename>]` =デバッグファイルのtar名の付録。名前を入力しない場合は、デバイスのシリアル番号がファイル名として使用されます。

例 1

```
apc>logToFlash 01292018
Creating report file: /debug_01292018.tar
Press <ESC> to abort
0% completed...
Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB
flash 60% completed...
Logs export completed. You may remove USB flash now
```

例 2

```
apc>logToFlash
Creating report file:
/debug_ZA1234567890.tar Press <ESC> to abort
0% completed...Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB flash
60% completed...Logs export completed. You may remove USB flash now
```

エラーメッセージE000, E102

modbus

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明：Modbus TCPのオプションを表示および設定します。Modbus TCPによりビル管理システム（BMS）がRack ATSデバイスを監視できるようになります。

パラメータ：

オプション	引数	説明
-tE	<enable | disable>	Modbus TCPを有効化または無効化します。
-tP		Modbus TCPのポート番号を表示します。(Modbus TCPのポート番号をWeb UIで設定できます。)
-tTO	<0 – 64800>	Modbus TCP通信タイムアウトを秒単位で指定します。0は接続がタイムアウトしないことを示します。
-ka	<enable | disable>	Modbus TCPをキープアライブにします。他に通信がない場合、2時間75秒ごとにデータパケットをサーバーに送信します。通信タイムアウトを7,275秒以上に設定した場合、通信タイムアウトになるのを防ぎます。
-rDef		Modbus設定をデフォルト値にリセットします。

例1：Modbusの設定を表示するには、次のように入力します。

```
apc> modbus
E002: Success

Slave Address = 0x1
Status = DISABLED
TCP Status = DISABLED
TCP Port Number = 502
TCP Communication Timeout = 5 secs
Keep-alive = ENABLED
```

例2：Modbus TCPを有効化するには、次のように入力します。

```
apc> modbus -tE enable
E002: Success
Reboot required for change to take effect.
```

例3：Modbus TCPを有効化するには、次のように入力します。

```
apc> modbus -tE disable
E002: Success
Reboot required for change to take effect.
```

エラーメッセージ： E000, E002, E101, E102

phLowLoad

注記： このコマンドは、サーキットブレーカのないユニットのみをサポートします。

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明相の低負荷しきい値をアンペア単位で設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<current>	新しい低負荷しきい値(A)

例：

```
apc> phLowLoad
E000: Success
0 A

apc> phLowLoad 3
E000: Success
```

エラーメッセージE000, E102

phNearOver

注記： このコマンドは、サーキットブレーカのないユニットのみをサポートします。

アクセス権：スーパーユーザー、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アンペア単位で設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<current>	新しい過負荷直前しきい値（アンペア）

例：

```
apc> phNearOver
E000: Success
8 A

apc> phNearOver 9
E000: Success
```

エラーメッセージE000, E102

phOverLoad

注記： このコマンドは、サーキットブレーカのないユニットのみをサポートします。

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明相の過負荷しきい値をアンペア単位で設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<current>	新しい過負荷しきい値（アンペア）

例：過負荷しきい値を表示するには、次のように入力します。

```
apc> phOverLoad
E000: Success
10 A
```

すべての相の過負荷しきい値を10 Aに設定するには、次のように入力します。

```
apc> phOverLoad
E000: Success
10 A
```

エラーメッセージE000, E102

phPeakLoad

注記： このコマンドは、サーキットブレーカのないユニットのみをサポートします。

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明相のピーク負荷を表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）

例：

```
apc> phPeakLoad
E000: Success
4.0 A
```

エラーメッセージE000, E102

phReading

注記： このコマンドは、サーキットブレーカのないユニットでのみ使用できます。

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明相の負荷をアンペア単位で表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）

例：

```
apc> phReading
E000: Success
4.0 A
```

エラーメッセージE000, E102

prodInfo

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明Rack ATSに関する情報を表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）

例：

```
apc> prodInfo 2:
E000: Success
AOS:                    1.0.0.3
APP:                    0.0.2.5
Model:                  AP4452A
Name:                   apcRack_01
Location:               Data Center Row 3
Contact:                Don Adams
Outlets:                10
Rated Load:             16 A
Phases:                 1
Uptime:                 15 Days 1 Hours 8 Minutes
Network Link:           Link Active
NPSの種類：             Host
NPSの状態：             有効
```

エラーメッセージE000, E102

sensorName

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明Rack ATSのユニバーサルI/Oポート（温度/湿度センサーの接続ポイント）に割り当てる名前を設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<newname>	ユニバーサルI/Oポートの新しい名前

例 1ポートの名前を「Sensor1」に設定するには、次のように入力します。

```
apc> sensorName Sensor1
E000: Success
```

例 2次に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。

```
apc> sensorName
E000: Success
Sensor1
```

例 3ゲストRack ATS 2のセンサポートの名前を「Sensor1」に設定するには、次のように設定します。

```
apc> sensorName 2:Sensor1
E000: Success
```

エラーメッセージE000, E102

sourceAName

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明電源Aに割り当てられた名前を設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<sourcAName>	電源Aの名前

例：

```
apc> sourceAName
E000: Success
Wall Box Phase L1

apc> sourceAName "Wall Box N2 Phase L2"
E000: Success
```

エラーメッセージE000, E102

sourceBName

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明電源Bの名前を設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<sourcBName>	電源Bの名前

例：

```
apc> sourceBName
E000: Success
Wall Box Phase L2

apc> sourceBName "Wall Box N2 Phase L3"
E000: Success
```

エラーメッセージE000, E102

sourcePref

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明希望する優先電源を設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<A | B | None>	A =優先電源A. B =優先電源B. None =優先なし

例：

```
apc> sourcePref
E000: Success
Preferred Source: [Source A]

apc> sourcePref B
E000: Success
```

エラーメッセージE000, E102

温度センサーの注意：

温度に関するコマンドを使用するには、オプションのAPC温度/湿度センサー(AP9335T/AP9335TH)をRack ATSに接続する必要があります。

tempAlGen

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明温度アラームを有効または無効にするかどうかを設定します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<enable | disable>	enable =温度アラームを有効にします。 disable =温度アラームを無効にします。

例：

```
apc> tempAlGen enable
E000: Success

apc> tempAlGen disable
E000: Success
```

エラーメッセージE000, E102

tempHigh

アクセス権：スーパーユーザー、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。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<F | C>	華氏(F)または摂氏(C)
<temperature>	新しい高温しきい値

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。

```
apc> 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。

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

例 3ゲストRack ATS 2の高温しきい値を華氏で表示するには、次のように入力します。

```
apc> tempHigh 2:F
E000: Success
70 F
```

エラーメッセージE000, E102

tempHyst

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明温度しきい値のヒステリシスを設定して表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<F | C>	華氏(F)または摂氏(C)
<temperature>	新しい温度ヒステリシス値

例：

```
apc> tempHyst F 6
E000: Success

apc> tempHyst C
E000: Success
3 C
```

エラーメッセージE000, E102

tempMax

アクセス権：スーパーユーザー、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。id#はグループのサイズによって1 ~ 32の範囲で指定できます。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
< F | C >	華氏(F)または摂氏(C)
<temperature>	新しい最高温度しきい値

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。

```
apc> 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。

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

例 3ゲストRack PDU 3の最高温度しきい値を華氏で表示するには、次のように入力します。

```
apc> tempMax 3:F
E000: Success
95 F
```

エラーメッセージE000, E102

tempPeak

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明センサーのピーク温度読み取り値を表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<F | C>	華氏(F)または摂氏(C)

例：

```
apc> tempPeak F
E000: Success
77.5 F
```

エラーメッセージE000, E102

tempReading

アクセス権：スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明センサーの温度値を華氏または摂氏のいずれかで表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
< F | C >	華氏(F)または摂氏(C)

例 1温度値を華氏で表示するには、次のように入力します。

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

例 2ゲストRack ATS 3の温度値を摂氏で表示するには、次のように入力します。

```
apc> tempReading 3:C
E000: Success
23.5 C
```

エラーメッセージE000、E102、E201

vMediumLimit

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明電圧切り替え範囲が[Medium]に設定されている場合に使用する電圧範囲を設定または表示します。この値は[Narrow Transfer Limit]より大きく、[Wide Limit]（V）より小さくする必要があります。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
[<limit>]	中電圧切り替え範囲。指定できる値は、Rack ATSモデルによって異なります。

モデル	許容範囲の値
AP4421A、AP4422A、AP4423A、AP4424A	16-25
AP4430A、AP4432A、AP4433A、AP4434A	15～30
AP4452AJ	10-15
AP4450A、AP4452A、AP4453A	10-23

例：

```
apc> vMediumLmt
E000: Success
Voltage Medium Limit: 12 V

apc> vMediumLmt 14
E000: Success
```

エラーメッセージE000, E100, E102

vNarrowLmt

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明電圧切り替え範囲が[Narrow]に設定されている場合に使用する電圧範囲を設定または表示します。この値は[Medium Limit]より小さくする必要があります。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
[<limit>]	狭い電圧切り替え範囲。指定できる値は、Rack ATSモデルによって異なります。

モデル	許容範囲の値
AP4421A、AP4422A、AP4423A、AP4424A	16-25
AP4430A, AP4432A, AP4433A, AP4434	15～30
AP4452JA	10-15
AP4450A, AP4452A, AP4453	10-23

例：

```
apc> vNarrowLmt
E000: Success
Voltage Narrow Limit: 15 V
```

エラーメッセージE000, E100, E102

vSensitvty

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明感度を設定または表示します。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1 ~ 32を指定できます）
<High | Low>	Rack ATSの感度を設定します。 High = Rack ATSは電源障害が発生すると、2 ms後に電源を切り替えます。 Low = Rack ATSは電源障害が発生すると、4 ms後に電源を切り替えます。

備考：**周波数**が50 Hz (atsMeasure, 91 ページを参照)で**FreqDeviat** (freqDeviat, 98 ページを参照)が10に設定されている場合、**vSensitty**はLowに設定されている必要があります。

例：

```
apc> vSensitvty
E000: Success
Voltage Sensitivity: Low

apc> vSensitvty High
E000: Success
```

エラーメッセージE000, E100, E102

vWideLmt

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明電圧切り替え範囲が[Wide]に設定されている場合に使用する電圧範囲を設定または表示します。この値は[Medium Limit]より大きくする必要があります。

パラメータ：

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
[<limit>]	広い電圧切り替え範囲指定できる値は、Rack ATSモデルによって異なります。

モデル	許容範囲の値
AP4421A、AP4422A、AP4423A、AP4424A	16-25
AP4430A、AP4432A、AP4433A、AP4434A	15～30
AP4452AJ	10-15
AP4450A、AP4452A、AP4453A	10-23

例：

```
apc> vWideLmt
E000: Success
Voltage Wide Limit: 20

apc> vWideLmt 24
E000: Success
```

エラーメッセージE000, E102

vXferRange

アクセス権：スーパーユーザー、管理者、デバイスユーザー

説明電圧切り替え範囲を設定または表示します。Rack ATSの電圧が切り替え範囲を超えると、アラームが生成されます。

パラメータ：電圧切り替え範囲。

引数	説明
<id#>:	NPSグループ内のユニットのID（グループのサイズに応じて1～32を指定できます）
<Wide | Medium | Narrow>	Wide: vWideLmtの設定値に対応します Medium: vMediumLmtの設定値に対応します Narrow: vNarrowLmtの設定値に対応します

例：

```
apc> vXferRange
E000: Success
Voltage Transfer Range: Medium

apc> vXferRange Wide
E000: Success
```

エラーメッセージE000, E102

Webユーザーインターフェイス

Microsoft Internet Explorer® (IE)またはEdge®、Google Chrome®、Apple Safari®、またはMozilla Firefox®の最新バージョンを使用して、Web UIからRack ATSにアクセスできます。他の一般的に入手可能なブラウザおよびバージョンは動作するかもしれませんが、完全には検証されていません。

任意のオペレーティングシステムのWeb UIにアクセスするには、Mozilla Firefox®またはGoogle Chrome®の最新リリースを使用します。その他一般に流通しているブラウザでも動作する可能性がありますが、Schneider Electricでは充分なテストを行っていません。

Rack ATSはプロキシサーバーと連携することができません。Rack ATSのWeb UIにアクセスする前に、次のいずれかの操作を行います。

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

Web UIへのログオン

Web UIにアクセスし、ネットワーク上のRack ATSのセキュリティ設定を行うには、

1. WebブラウザのURLアドレスフィールドにRack ATSのDNS名またはIPアドレスを入力し、ENTERキーを押します。

   備考：アクセスプロトコルとしてHTTPS(SSL/TLS)を使用している場合、ログイン認証情報はサーバー証明書に記載されてい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、IPアドレスが証明書の共通名として指定されている場合は、IPアドレスを使用してRack ATSにログオン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ページが安全ではないというメッセージが表示されることがあります。これは正常であり、ウェブ UI に進むことができます。警告が表示されたのは、ウェブブラウザが HTTPS 上の暗号化に使用されるデフォルトの証明書を認識しないためです。ただし、それでも HTTPS を介して送信される情報は暗号化されています。HTTPSの詳細および警告を解決する手順については、www.se.comにある『*Security Handbook*』を参照してください。

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、スーパーユーザーと管理者ではどちらの値も「**apc**」です。スーパーユーザー、またはスーパーユーザーによって作成された管理者は、他のユーザーのユーザー名、パスワード、アカウントの詳細を定義する必要があります。)

URLアドレスの形式

WebブラウザのURLアドレスフィールドにRack ATSのDNS名またはIPアドレスを入力し、ENTERキーを押します。HTTPが有効になるまでは、URLに「`https://`」を含める必要があります。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。

ログオン時の一般的なブラウザのエラーメッセージ

エラーメッセージ	ブラウザ	エラーの原因
「ページを表示できません。」	Internet Explorer	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。
「接続できません。」	Firefox	

URL形式の例

注記： HTTPはデフォルトでは無効になっており、HTTPSはデフォルトで有効になっています。

- 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 (SSL/TLS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/TLS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/TLS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）

  `https://[2001:db8:1::2c0:b7fSf:fe00:1100]:5000`(アクセスモードがHTTPS（SSL/TLS使用のHTTP）の場合)

最初のログオン

Rack ATSに初めてログオンした場合は、デフォルトのSuper Userアカウントパスワード(**apc**)の変更を求めるメッセージが表示されます。ログインすると、**Configuration Summary**（**設定の概要**）画面に移動します。この画面は、すべてのシステムプロトコルの概要とその現在の値（例：有効/無効）です。この画面には、**Configuration > Network > Summary**と選択すれば、後からいつでもアクセスできます。

Web UIの機能

ご使用のRack ATSのWeb UIの基本的な機能については、以下の説明をお読みください。

タブ

下記のタブを使用できます。

- **Home（ホーム）:** ログオンすると表示されます。アクティブなアラーム、Rack ATSの負荷状態、およびRack ATS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, 129 ページ」を参照してください。

  備考：**Home**はログオン時に表示される既定のページです。ログインページを変更するには、希望するログインページに移動し、ブラウザウィンドウの右上にあるプッシュピンアイコンをクリックします。ログインページをホームに戻すには、ホームターゲットアイコンをクリックします。
- **Status（ステータス）**：ユーザーに**ATS**および**Network**のステータスを示します。**ATS**タブには、**アラーム**、**デバイス**、**装置**、**負荷**、**測定値**、**環境**のステータスが表示されます。**Network**タブには**ネットワーク**のみが表示されます。詳細については、「Status（ステータス）タブ, 130 ページ」を参照してください。
- **Control（制御）**：**Control**タブには、**セキュリティ**と**ネットワーク**の情報が表示されます。これらのタブの詳細については、「Controlタブ, 136 ページ」を参照してください。
- **Configuration（設定）**：**Configuration**タブには、**ATS**、**セキュリティ**、**ネットワーク**、**通知**、**一般**、および**ログ**の情報が表示されます。これらの各タブの詳細については、「[Configuration]タブ, 138 ページ」で説明します。
- **Tests（テスト）**：**Tests**タブには**ATS**と**ネットワーク**の情報が表示されます。**ATS**タブはLCDの点滅情報を表示し、**Network**タブは**LEDの点滅**情報を表示します。どちらも詳細については、「[Tests]タブ, 182 ページ」を参照してください。
- **Logs（ログ）**：**Logs**セクションには、**イベント**、**データ**、**ファイアウォール**の情報が表示されます。**Event**タブと**Data**タブには、さらに詳しい情報が表示されます。詳細については、「[Logs]タブ, 183 ページ」を参照してください。
- **About（バージョン情報）**：**About**セクションでは、**ATS**、**ネットワーク**、および**サポート**の情報が表示されます。これらの詳細については、「[About]タブ, 191 ページ」に説明があります。

Limited Status Access（限定ステータスアクセス）

有効にすると、Webブラウザの[限定ステータス]ページで、ログインを行わずにRack ATSに関する限定された情報を表示することができます。[ログイン]ページへのリンクは、[限定ステータス]ページの左上にあります。

[限定ステータス]ページを有効にするには、Web UIで**Configuration > Network > Web > Access**の順に選択します。

- **[Enable]**を選択した場合は、**Limited Status**ハイパーリンクが[ログイン]ページの左下に表示されます。このリンクをクリックすると、Rack ATSにログインせずに、[限定ステータス]ページを表示できます。
- **[Enable]**と**[Use as default]**を選択した場合、WebブラウザのURLアドレスバーにRack ATSのIPアドレスを入力すると[限定ステータス]ページがデフォルトで表示されます。

デバイスステータスアイコン

1つまたは複数のアイコンとそれに付随するテキストは、Rack ATSの現在の動作状態を示します。

アイコン	説明
	No Alarms: 現在アラームは発生していません。Rack ATSとNMCは正常に動作しています。
	Warning: 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。
	Critical: 直ちに対処を要する重大な障害が発生しています。

各ページの右上隅にあるクイックステータス領域には、Rack ATSのステータスをレポートするホームページに現在表示されているものと同じアイコンが表示されます。

- アラームが存在しない場合は、**No Alarms**アイコンが表示されます。
- アラームが存在する場合には、他のアイコン(**Critical**と**Warning**)の一方または両方が表示されます。各アイコンの後には、同じ重要度の発生中のアラームの数も表示されます。

クイックステータス領域のアイコンをクリックして、**ホーム**画面に移動できます。

クイックリンク

各Web UIページには、左下隅に設定可能な3つのリンクがあります。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。

- リンク1: APC Webサイトのホームページ
- リンク2: EcoStruxure™ ITに関する情報
- リンク3: IT配電機器の追加情報

これらのリンクは、**Configuration > General > Quick Links**から設定できます。

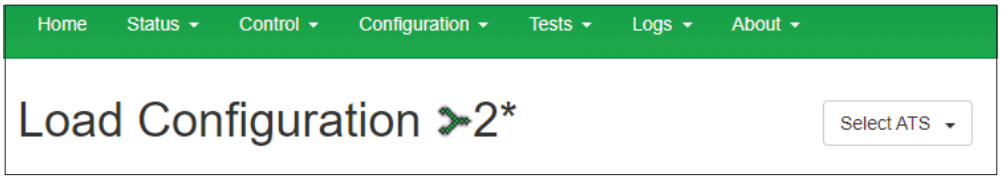
各Web UIページの右上隅には、次のリンクがあります。

- **ユーザー名**：このリンクを選択すると、ユーザーの環境設定を変更できます。
- **現在の言語**：現時点では英語のみ対応しています。
- **ログオフ**：このリンクを選択すると、現在のユーザーがWeb UIからログオフします。
- **ヘルプ**：このリンクを選択すると、状況に即した情報が表示されます。
- プッシュピンのアイコン：プッシュピンアイコンをクリックすると、現在のWebページを最初にログオンしたときに表示されるページとして設定します。ホームターゲットアイコンをクリックして、最初にログオンしたときに表示される**[Home]**ページとして設定します。

Web UI上のネットワークポート共有(NPS)

Rack ATSがNPSグループの一部である場合、Rack ATSのWeb UIには追加機能があります。これには、[NPSグループの状態]ページ(**Status > ATS > Group Status**)と[NPSグループの設定]ページ(**Configuration > ATS > Group**])が含まれます。さらに、NPS機能をサポートするWebページでは、グループ内の別のRack ATSを表示するには、そのユニットのDisplay IDを選択します。

NPSグループ内の各Rack ATSは、Rack ATSアイコン、その後のDisplay ID (1 ~ 32)で表示されます。ログインしているRack ATSは、Display IDの後にアスタリスク(*)が表示されています。



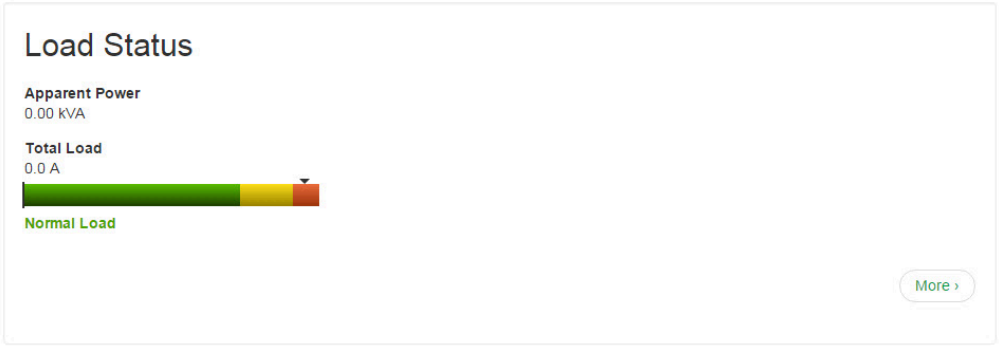
Homeタブ

アクティブなアラーム: アクティブなアラームを表示します。各ページの右上にも表示されます。アラームが発生していない場合、緑色のチェックマークとNo Alarms Presentのメッセージが表示されます。

スイッチ/電源の状態：選択した電源と、切り替えが可能かどうかを表示します。

負荷状態：デバイスの負荷をkVAで、相とバンクの負荷をAで（該当する場合）表示します。メーターは現在の負荷状態を表示します。通常（緑）、過負荷直前（黄色）または過負荷（赤）。**More**をクリックして、**Load Status**ページに移動します。(詳細については、負荷状態の表示, 132 ページを参照してください。)

注記： 低負荷しきい値が設定された場合、メーターの左側に青色の部分も表示されます。



パラメータ

- **名前**：Rack ATSの設定名です。
- **ロケーション**：Rack ATSが配置されている物理的な場所。
- **お問い合わせ先**：Rack ATSの責任者に連絡する方法。
- **型番:** SKUまたは部品番号とも呼ばれます。許容可能な電圧設定は型番によるものです。詳細については、www.se.com、にてご利用のRack ATSモデル用のスペックシートを参照してください。
- **定格**：定格は、Rack ATSの位相定格に加えて、装置で計測された相とバンクの数を示します。
- **ユーザータイプ**：Rack ATSにアクセスしているユーザーアカウントのタイプ。ユーザータイプによって権限が決まります。詳細については、ユーザーアカウントの種類, 15 ページを参照してください。
- **アップタイム**：アップタイムは、電源サイクルまたは管理インターフェイスの再起動による最後の即時再起動から数えたRack ATSの稼働時間。

最近のデバイスイベント：発生した日付や時刻を含み最新のイベントを表示します。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**タブに移動し、イベントログ全体を表示します。

Status（ステータス）タブ

[Status]タブでは、Rack ATSとネットワークの情報を表示できます。

- **ATS:** NPSグループ(**グループステータス**)アクティブアラーム(**アラーム**)、Rack ATSの一般的な構成情報(**デバイスステータス**)、電源情報とイベントカウント(**ユニットステータス**)、負荷状態(**負荷**)、および電力測定(**測定**)を表示します。
- **ネットワーク**：IPv4/IPv6の設定、ドメイン名システムのステータス、およびポート速度を表示します。

NPSグループの表示

Status > ATS > Group Status

このページでは、次の作業を実行できます。

- NPSグループの各ユニットに関する一般情報を表示します。各ユニットを選択して、そのユニットに関する特定の情報の表示/非表示を切り替え、各ユニットの設定を変更するオプションを選択します。
- **Reset/Reboot**オプションを使用して、NPSグループのネットワーク管理インターフェイスを、TCP/IP設定やEAPoL設定などの既定値に戻します。
  - TCP/IPとEAPoL（デフォルトでは、TCP/IPはDHCPに設定され、EAPoLは無効になっています）。
  - LCDオン/オフの環境設定
  - 電源AとBの名前、優先する電源の設定、前面パネルのロック
  - 周波数偏移、電圧切り替え限界、切り替え範囲、感度
  - 負荷しきい値、ピーク電流の測定値およびタイムスタンプ
  - イベントカウントとイベントカウントのタイムスタンプ
  - ワイヤード（有線）環境センサ：名前と場所、ピーク温度とタイムスタンプ、アラームステータス（無効/有効）、温度/湿度しきい値とヒステリシス値

  このオプションを選択するとNMCが再起動します。初期ログオン後にデフォルトのユーザー名とパスワード(**apc**および**apc**)を変更する必要があります。
- **ATS to defaults**オプションを使用して、NPSグループ内のネットワーク管理インターフェイスを既定に戻します。ただし、TCP/IP設定とEAPoL設定は除きます。
  - TCP/IPおよびEAPoL
  - LCDオン/オフの環境設定
  - 電源AとBの名前、優先する電源の設定、前面パネルのロック
  - 周波数偏移、電圧切り替え限界、切り替え範囲、感度
  - 負荷しきい値、ピーク電流の測定値およびタイムスタンプ
  - イベントカウントとイベントカウントのタイムスタンプ
  - ワイヤード（有線）環境センサ：名前と場所、ピーク温度とタイムスタンプ、アラームステータス（無効/有効）、温度/湿度しきい値とヒステリシス値
- 切断されたゲストをNPSグループから削除します。

  注記： ホストユニットを変更するには、**Configuration > ATS > Groups**の順に選択します。

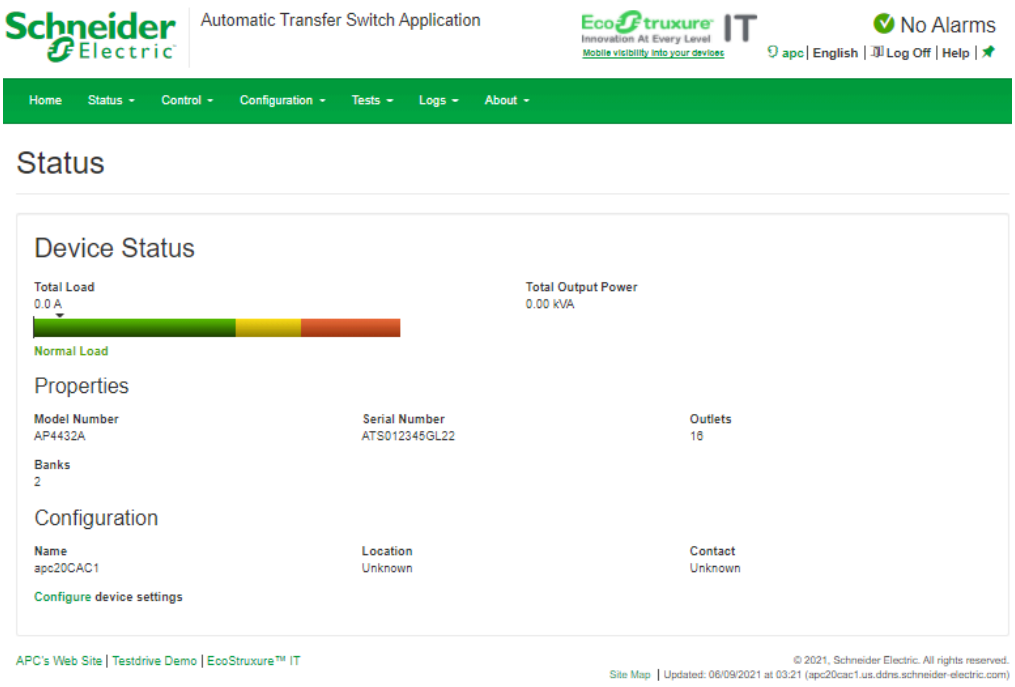
デバイスアラームの表示

選択手順 (パス) : Status > ATS > Alarms

アラームステータスアイコン (デバイスステータスアイコン, 127 ページを参照) と説明を含めて、現在のデバイスアラームを表示します。

デバイスステータスの表示

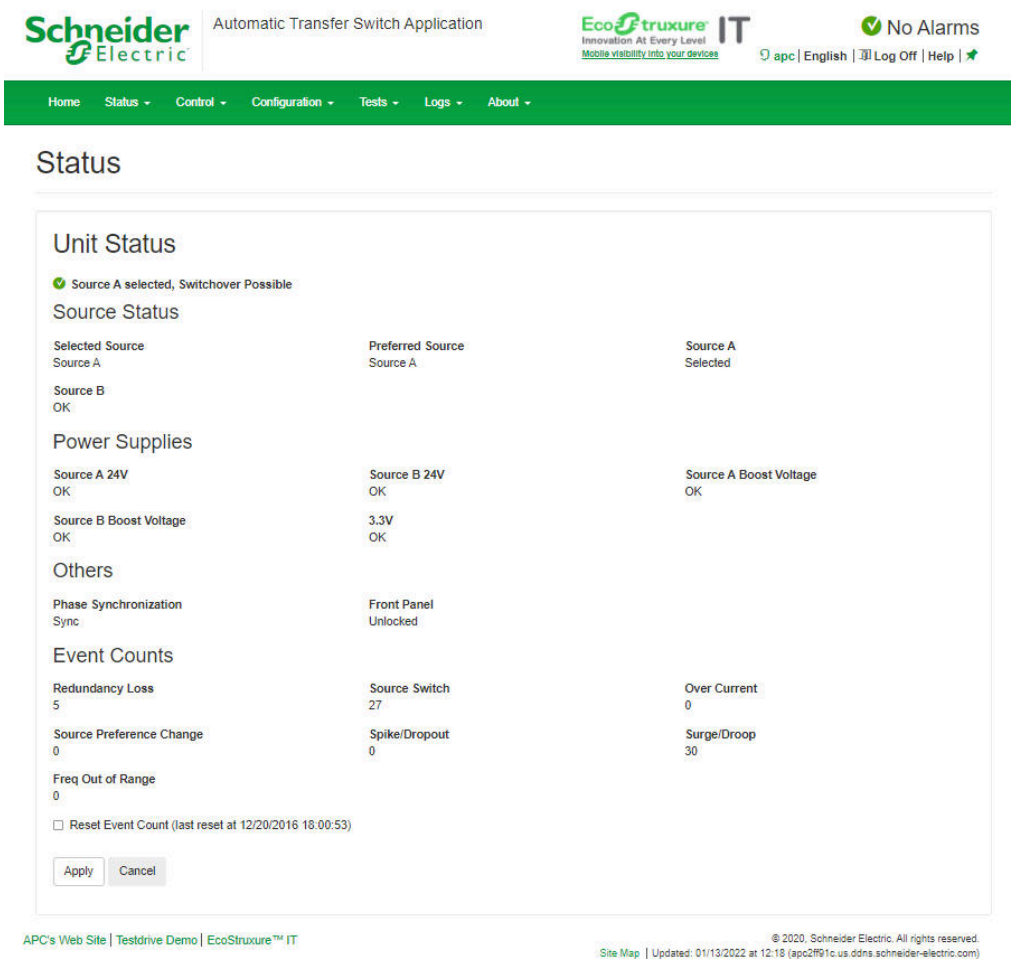
選択手順 (パス) : Status > ATS > Device



デバイスステータス、**プロパティ**、**設定**情報を表示します。**[Configure device settings (デバイス設定)]**を選択すると、**[Name]**、**[Location]**、**[Contact]**の情報を編集できます。

装置の状態の表示

選択手順（パス）： Status > ATS > Unit



1次電源と2次電源のステータス、利用可能な電源、位相同期、その他利用可能な機能を表示します。

次のイベントカウントを表示します。**冗長損失**、**電源切替**、**過電流**、**電源設定変更**、**スパイク/ドロップアウト**、**サージ電流/ドループ**、**周波数が範囲外**。これらのカウントを0にリセットするには、**[Reset Event Count]**（イベントカウントのリセット）を選択して**[Apply]**（適用）をクリックします。デバイスの電源が切断されるか、Rack ATSコントローラが更新されると、イベントカウントは自動的にゼロに設定されます。

負荷状態の表示

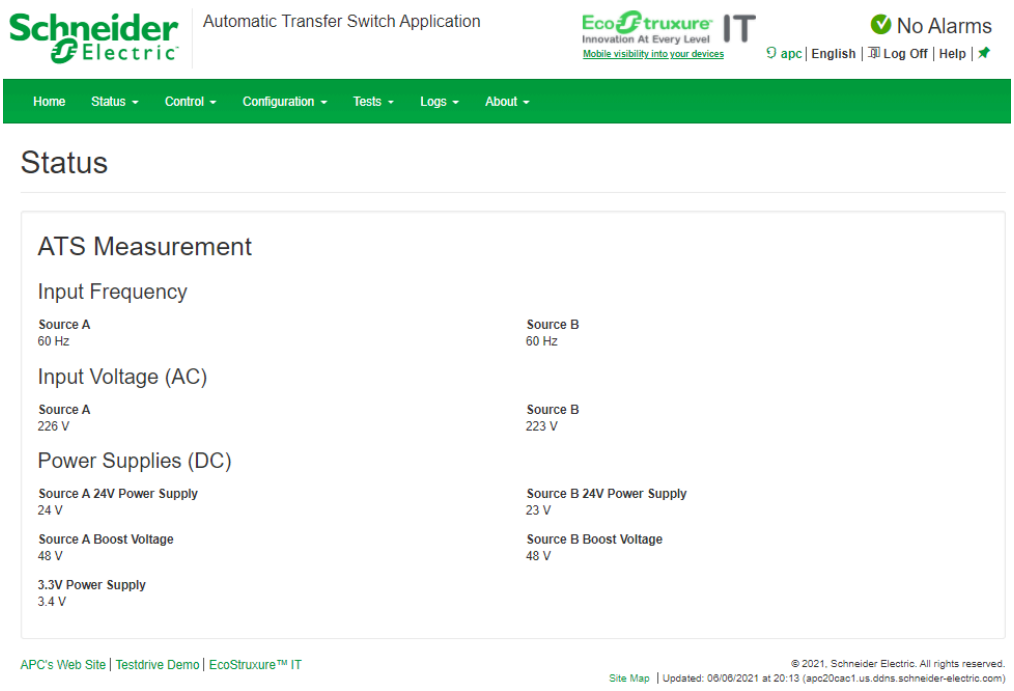
選択手順（パス）： Status > ATS > Load

緑、黄、赤に色分けされたスライドバー上のマーカーは、Rack ATSの負荷を表します。

- 緑色：通常負荷範囲
- 黄色：過負荷直前の範囲
- 赤色：過負荷範囲

電力測定値の表示

選択手順 (パス) : Status > ATS > Measurement



Input Frequency (入力周波数)、**Input Voltage (AC) (入力電圧(AC))**、および**Power Supplies (DC) (電源(DC))**の測定値を表示します。

> **注記** : **Power Supplies (DC)(電源(DC))**は、Rack ATSの内部に設置されています。接続されているハードウェアには接続されていません。カスタマサポートは、これらの読み取り値をトラブルシューティングに使用できます。

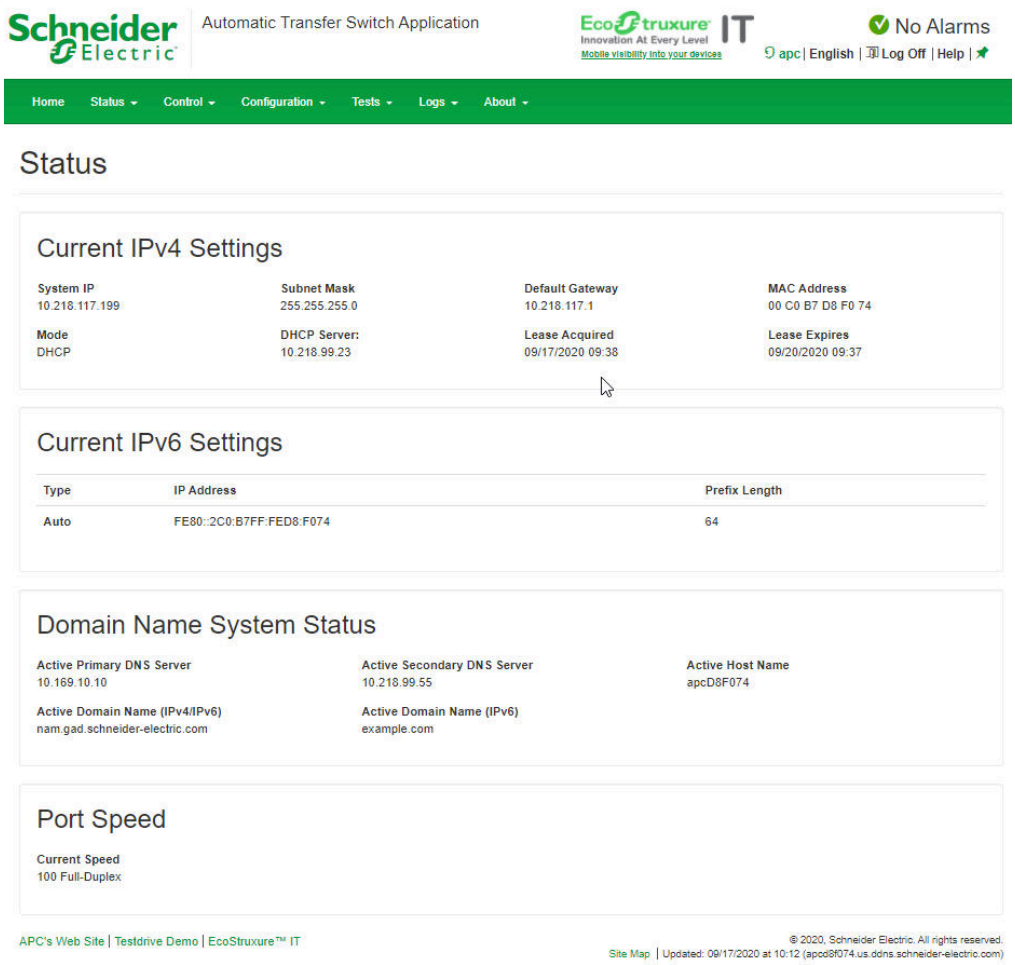
環境ステータスの表示

このページでは、接続されている温度センサー(AP9335T)または温度/湿度センサー(AP9335TH)からの次のような設定およびフィードバックを表示できます。**センサー名**、**センサーの場所**、**センサータイプ**、**アラームステータス**、**温度**、**ピーク温度**、**ピーク時間**、**リセット時間**、**湿度**、および**温度アラーム**と**湿度アラーム**が**有効**または**無効**になっているかどうか。

これらの設定は、**[Configure environment settings]**をクリックするか、**Configuration > ATS > Environment**と順に移動して設定できます。詳細については、「温度/湿度センサーの設定, 145 ページ」を参照してください。

ネットワークステータスの表示

選択手順（パス）： Status > Network > Network



現在のIPv4設定

- **System IP:** ユニットのIPアドレス。
- **Subnet Mask:** サブネットワークのIPアドレス。
- **Default Gateway:** ネットワークへの接続に使用するルーターのIPアドレス。
- **MAC Address:** ユニットのMACアドレス。
- **Mode:** IPv4設定の割り当て方式：次の3つがあります：**Manual（手動）**、**DHCP**、または**BOOTP**。
- **DHCP Server:** DHCPサーバーのIPアドレス。これは、[Mode]が[DHCP]の場合のみ表示されます。
- **Lease Acquired（リース取得日）:** IPアドレスがDHCPサーバーから受け入れられた日時。
- **Lease Expires（リース期限）:** DHCPサーバーからのIPアドレスの期限が切れて、更新が必要となる日時。

現在のIPv6設定

- **次のように入力します。**IPv6設定の割り当て方式（自動または手動）。
- **IP Address:** ユニットのIPアドレス。
- **Prefix Length（プレフィックス長さ）:** サブネットワークのアドレス範囲。

ドメイン名システムのステータス

- **Active Primary DNS Server:** プライマリDNSサーバーのIPアドレス。
- **Active Secondary DNS Server:** セカンダリDNSサーバーのIPアドレス。
- **Active Host Name:** アクティブなDNSサーバーのホスト名。
- **Active Domain Name (IPv4/IPv6):** 現在使用中のIPv4/IPv6ドメイン名。
- **Active Domain Name (IPv6):** 現在使用中のIPv6ドメイン名。

ポート速度

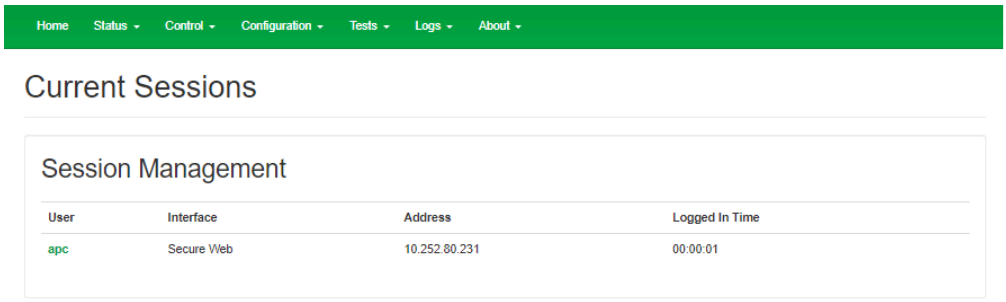
Current Speed: Ethernetポートに割り当てられている現在の通信速度(Mbps単位)、半二重（**一度に一方向のみの通信**）**または**全二重（**同じチャンネルで同時に双方向の通信**）。

Controlタブ

Controlタブのオプションを使用すると、アクティブなユーザーの管理とネットワークのセキュリティに影響するす操作をすぐに実行できます。

ユーザーセッションの管理

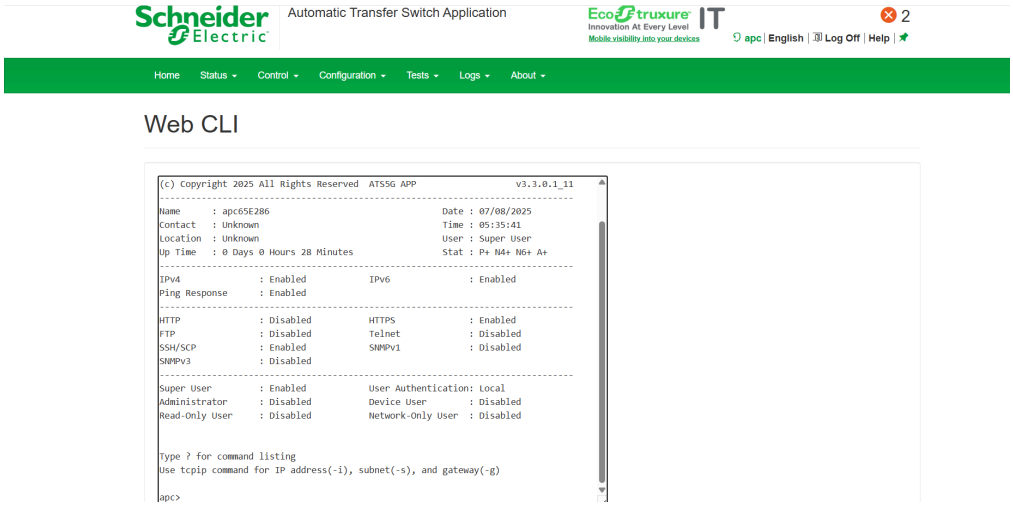
選択手順（パス）：Control > Security > Session Management



Session Management（**セッション管理**）メニューには、Rack ATSに現在接続しているすべてのアクティブユーザーが表示されます。ユーザーに関する情報を確認するには、それぞれのユーザー名を選択します。**[Session Details]**（セッション詳細）画面は、ユーザーに関する基本情報を、ユーザーがログインしているインターフェイス、そのIPアドレス、およびログイン時間を含めて表示します。**[Session Details]**ページ下部には、**[Terminate Session]**（セッション終了）ボタンがあります。管理者は別のユーザーのセッションを終了させることができます。

Web CLI

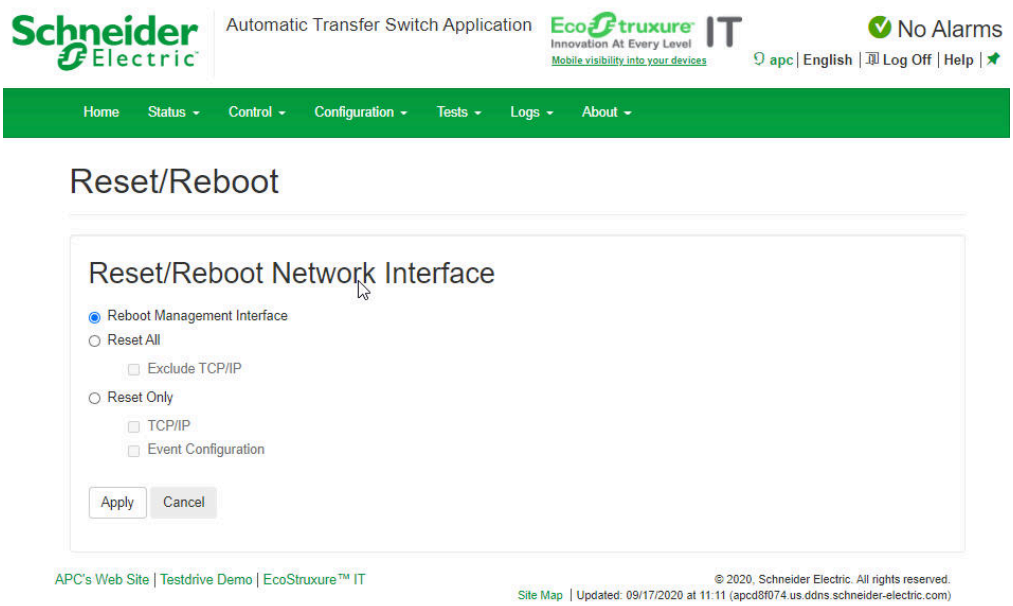
選択項目:Control > Network > Web CLI



このセクションでは、現在ログインしているユーザー向けのウェブベースのコマンドラインインターフェース（CLI）を提供します。すべての Telnet CLI コマンドは、Web CLI を通じて直接実行できます。利用可能なコマンドの詳細な説明および構文については、ネットワーク管理カード コマンドの説明, 49 ページ および デバイスコマンドの説明, 90 ページを参照してください。

ネットワークインターフェイスのリセット

選択手順（パス）：Control > Network > Reset/Reboot



このメニューでは、ネットワークインターフェイスのさまざまなコンポーネントをリセットおよび再起動できます。

設定	説明
Reboot Management Interface（管理インターフェイスの再起動）	再起動ではRack ATSユニットのネットワーク管理インターフェイスのみが再起動されます。これはRack ATSのON/OFFステータスには影響しません。
Reset All（すべてリセット）	すべてのネットワークインターフェイスをデフォルトの設定に戻します。リセット後のログオンには、デフォルトのユーザー名とパスワード(**apc**)を使用してください。その後、ユーザー名とパスワードを変更する必要があります。 **[Exclude TCP/IP]**（TCP/IPを除外）チェックボックスをオフにすると、すべての設定値がリセットされます。**[Exclude TCP/IP]**]チェックボックスをオンにすると、TCP/IPとEAPoLを除くすべての値がリセットされます。デフォルトのTCP/IP設定はDHCPです。EAPoLアクセスのデフォルトは**Disabled**です。
Reset Only（リセットのみ）	次のいずれか、または両方の設定をリセットします。 • **TCP/IP:** Rack ATSがEAPoL設定を含むTCP/IP設定値をどのように取得するかを決定する設定のみをリセットします。デフォルトのTCP/IP設定はDHCPです。EAPoLアクセスのデフォルトは**Disabled**です。 • **Event Configuration（イベントの設定）**：イベントをデフォルトの設定にリセットします。特別に設定されたイベントまたはグループもデフォルト値に戻ります。 • **Transfer Switch Configuration(切り替えスイッチ設定)**：有効なインターフェイスやログイン資格情報などのネットワーク設定を変更せずに、次の設定をリセットします。 ◦ LCDオン/オフの環境設定 ◦ 電源AとBの名前、優先する電源の設定、前面パネルのロック ◦ 周波数偏移、電圧切り替え限界、切り替え範囲、感度 ◦ 負荷しきい値、ピーク電流の測定値およびタイムスタンプ ◦ イベントカウントとイベントカウントのタイムスタンプ ◦ ワイヤード（有線）環境センサ：名前と場所、ピーク温度とタイムスタンプ、アラームステータス（無効/有効）、温度/湿度しきい値とヒステリシス値 リセットには最大1分かかります。

注記： このページでは、現在のRack ATSのみがリセットされます。NPSグループ内のユニットをリセット/再起動するオプションについては、「**Configuration > ATS > Groups**と**Status > ATS > Group Status**を参照してください。

[Configuration]タブ

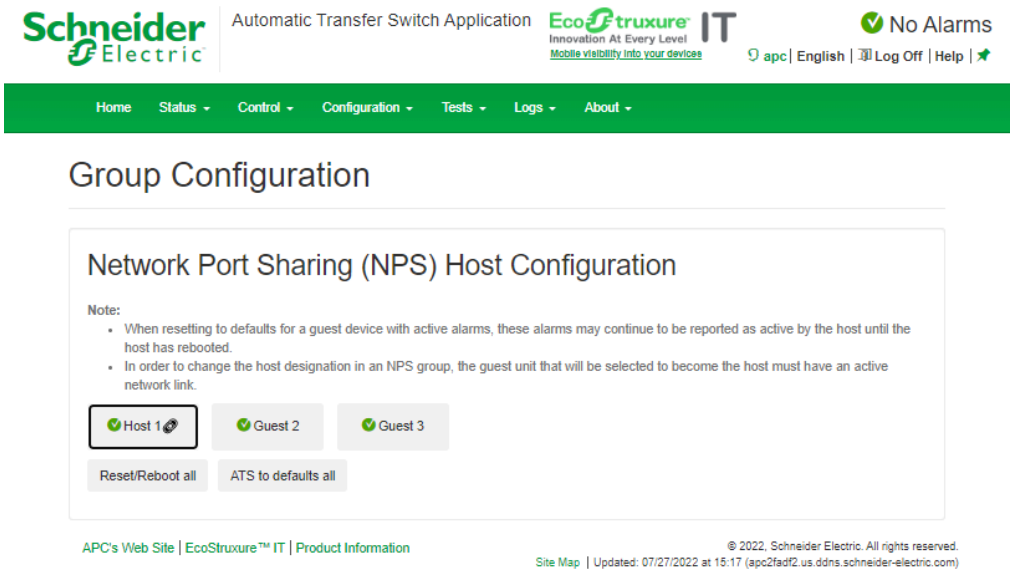
Configuration（設定）タブでは、以下の作業を実行できます。

- NPSグループ、ユニットの識別、電源設定、および切り替え動作に関連する設定を構成します(「Rack ATSの設定, 139 ページ」を参照してください)。
- セキュリティとユーザー管理に関する設定(「セキュリティ設定の管理, 147 ページ」を参照)。
- ネットワーク接続およびWeb UI/CLIへのアクセスに関する設定(「ネットワークの設定, 157 ページ」を参照)。
- 通知の設定(「通知の設定, 171 ページ」を参照)。
- ネットワーク管理インターフェイスに関する一般設定(「全体システムの設定, 177 ページ」を参照)。

Rack ATSの設定

NPSグループの構成

Configuration > ATS > Groups



このページでは、次の作業を実行できます。

- NPSグループの各ユニットに関する一般情報を表示します。各ユニットを選択して、そのユニットに関する特定の情報の表示/非表示を切り替え、各ユニットの設定を変更するオプションを選択します。
- **Reset/Reboot**オプションを使用して、NPSグループのネットワーク管理インターフェイスを、TCP/IP設定やEAPoL設定などの既定値に戻します。
  - TCP/IPとEAPoL（デフォルトでは、TCP/IPはDHCPに設定され、EAPoLは無効になっています）。
  - LCDオン/オフの環境設定
  - 電源AとBの名前、優先する電源の設定、前面パネルのロック
  - 周波数偏移、電圧切り替え限界、切り替え範囲、感度
  - 負荷しきい値、ピーク電流の測定値およびタイムスタンプ
  - イベントカウントとイベントカウントのタイムスタンプ
  - ワイヤード（有線）環境センサ：名前と場所、ピーク温度とタイムスタンプ、アラームステータス（無効/有効）、温度/湿度しきい値とヒステリシス値

  このオプションを選択するとNMCが再起動します。初期ログオン後にデフォルトのユーザー名とパスワード(**apc**および**apc**)を変更する必要があります。

- **ATS to defaults**オプションを使用して、NPSグループ内のネットワーク管理インターフェイスを既定に戻します。ただし、TCP/IP設定とEAPoL設定は除きます。
  - TCP/IPおよびEAPoL
  - LCDオン/オフの環境設定
  - 電源AとBの名前、優先する電源の設定、前面パネルのロック
  - 周波数偏移、電圧切り替え限界、切り替え範囲、感度
  - 負荷しきい値、ピーク電流の測定値およびタイムスタンプ
  - イベントカウントとイベントカウントのタイムスタンプ
  - ワイヤード（有線）環境センサ：名前と場所、ピーク温度とタイムスタンプ、アラームステータス（無効/有効）、温度/湿度しきい値とヒステリシス値
- 切断されたゲストをNPSグループから削除します。
- **Select Host**オプションを使用して、新しいホスト・ユニットを選択します。このオプションは、ターゲット・ホストにネットワーク接続がある場合（リンク・アイコン🔗で示される）のみ使用できます。

Rack ATSの名前と場所の設定

選択手順（パス）： Configuration > ATS > Device

Status（ステータス）：AのRack ATSの負荷と、kVA単位のの出力電力を表示します。

Name: Rack ATSの記述名を入力します。これは**[Home]**タブに表示されます。

Location: Rack ATSの物理的な設置場所を入力します。これは**[Home]**タブに表示されます。

Contact: Rack ATSRack PDURack Monitor 250者を入力します。これは**[Home]**タブに表示されます。

[Apply]をクリックして変更を保存するか、**[Cancel]**をクリックして変更を取り消します。

優先電源の設定

選択手順（パス）： Configuration > ATS > Source

Status（ステータス）：優先する電源の状態を表示します。

Source A Name、Source B Name: Source AとSource Bの電源に任意の名前を入力します。

Preferred Source: 両方の電源が使用可能な場合にRack ATSに優先的に電力を供給する電源を選択します。

Front Panel: 前面パネルをロックまたはロック解除します。

[Apply]をクリックして変更を保存するか、**[Cancel]**をクリックして変更を取り消します。

切り替え動作の設定

選択手順（パス）：Configuration > ATS > Frequency/Voltage

⚠⚠危険

危険電圧

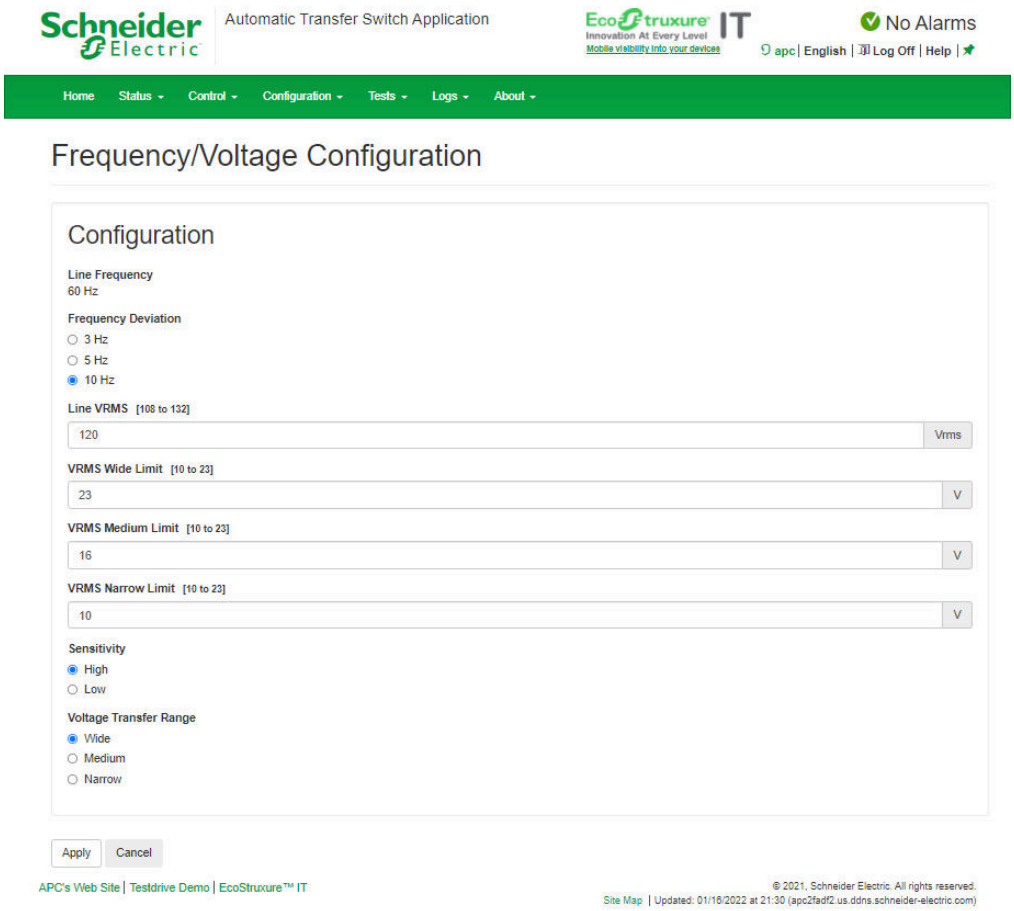
定格電圧外（+/- 10%）でRack ATSを操作しないでください。電圧の制限と切り替え範囲は、切り替え動作のソフトウェアによる制御を表すものであり、使用する入力電圧を表すものではありません。

上記の指示に従わないと、死亡または重傷を負うことになります。

モデル	定格電圧(VAC)	設定範囲(VAC)	狭いデフォルト範囲 (VAC)	中間デフォルト範囲 (VAC)	広いデフォルト範囲 (VAC)
AP4421A	230 (L-N)	± 16-25 V	± 16 V	± 20 V	± 25 V
AP4422A	230* (L-N)	± 16-25 V	± 16 V	± 20 V	± 25 V
AP4423A	230* (L-N)	± 16-25 V	± 16 V	± 20 V	± 25 V
AP4424A	230 (L-N)	± 16-25 V	± 16 V	± 20 V	± 25 V
AP4430A	200/208 (L-L)	± 15-30 V	± 15 V	± 22 V	± 30 V
AP4431A	208 (L-L)	± 15-30 V	± 15 V	± 22 V	± 30 V
AP4432A	200/208 (L-L)	± 15-30 V	± 15 V	± 22 V	± 30 V
AP4433A	208 (L-L)	± 15-30 V	± 15 V	± 22 V	± 30 V
AP4434A	208 (L-L)	± 15-30 V	± 15 V	± 22 V	± 30 V
AP4450A	100/120(L-N)	± 10-23 V	± 10 V	± 16 V	± 23 V
AP4450AJ	100 (L-N)	± 10-15 V	± 10 V	± 12 V	± 15 V
AP4452A	120 (L-N)	± 10-23 V	± 10 V	± 16 V	± 23 V
AP4452AJ	100 (L-N)	± 10-15 V	± 10 V	± 12 V	± 15 V
AP4453A	120 (L-N)	± 10-23 V	± 10 V	± 16 V	± 23 V

*220 V、韓国のみ。

電圧切り替え範囲によって、電源電圧に基づくRack ATSのスイッチ動作が決まります。電源電圧が指定された範囲外になると、Rack ATSは二次電源に切り替わります。Narrow（狭い）、Medium（中間）、Wide（広い）の各電圧を設定し、Rack ATSを目的の範囲に設定できます。使用する電源がRack ATSに適切な電力を供給していることを確認し（定格電圧の+/-10%）、電圧切り替え範囲を使用して、Rack ATSが適切な電圧外で長時間動作していないことを確認してください。



Frequency Deviation（**周波数偏移**）**:** 周波数の偏移が設定値を超えると、Rack ATSは電源を切り替えます。

> **注記**： 周波数が50 Hz（電力測定値の表示, 133 ページを参照）で**Sensitivity**（**感度**）が**High**（**高**）に設定されている場合、この値は3または5になります。

Line VRMS（**ラインVRMS**）**:** Rack ATSの定格電圧（公称入力とも呼ばれる）。VRMSの制限と切り替え範囲はこの値に基づきます。

Sensitivity（**感度**）**:** 2次電源に切り替える前に、Rack ATSがどの程度の電力変動を許容するかを管理します。感度を**[Low]**にすると、別の電源への切り替え前にRack ATSは4ミリ秒（ms）待機します（これにより、電源電圧が高すぎる、または頻繁に変動する場合に過剰な切り替えが行われないようになります）。感度を**[High]**にすると、別の電源への切り替え前にRack ATSは2ミリ秒（ms）待機します

> **注記**： 周波数が50 Hzで、［**Frequency Deviation**］が10に設定されている場合は、［**Sensitivity**］は［**Low**］に設定する必要があります。

Limits（制限）および**Transfer Range（切り替え範囲）**：**[Transfer Range]**は**[Line VRMS]**に設定した[Limit]（**[Wide]**、**[Medium]**、または**[Narrow]**をプラスまたはマイナスしたものです。**[Transfer Range]**は、電源電圧に基づいてRack ATSの切り替え動作を決定します。つまり、電源電圧が**[Transfer Range]**の範囲外に移動すると、Rack ATSは2次電源への切り替えを行います。

- **VRMSの[Wide]、[Medium]、[Narrow] Limit**：**[Transfer Range]**の設定オプションです。
- **Transfer Range:** Rack ATSで**Wide**、**Medium**、または**Narrow VRMS Limit**に基づいて電源を切り替えるかどうかを決定します。**[Transfer Range]**に設定できるのは、一度に1つの**[Limit]**に限られます。

  注記： **Voltage Transfer Range**と**Limit**は、Rack ATSの絶対最大定格の範囲内、即ち、85 ~ 265 VRMSでなければなりません。85 VRMS未満、または265 VRMSを超える電圧になると、どのような設定であってもRack ATSは電源を切り替えます。

例：Rack ATSは次のように設定されています。

Line VRMS = 208,

VRMS Wide Limit = 10,

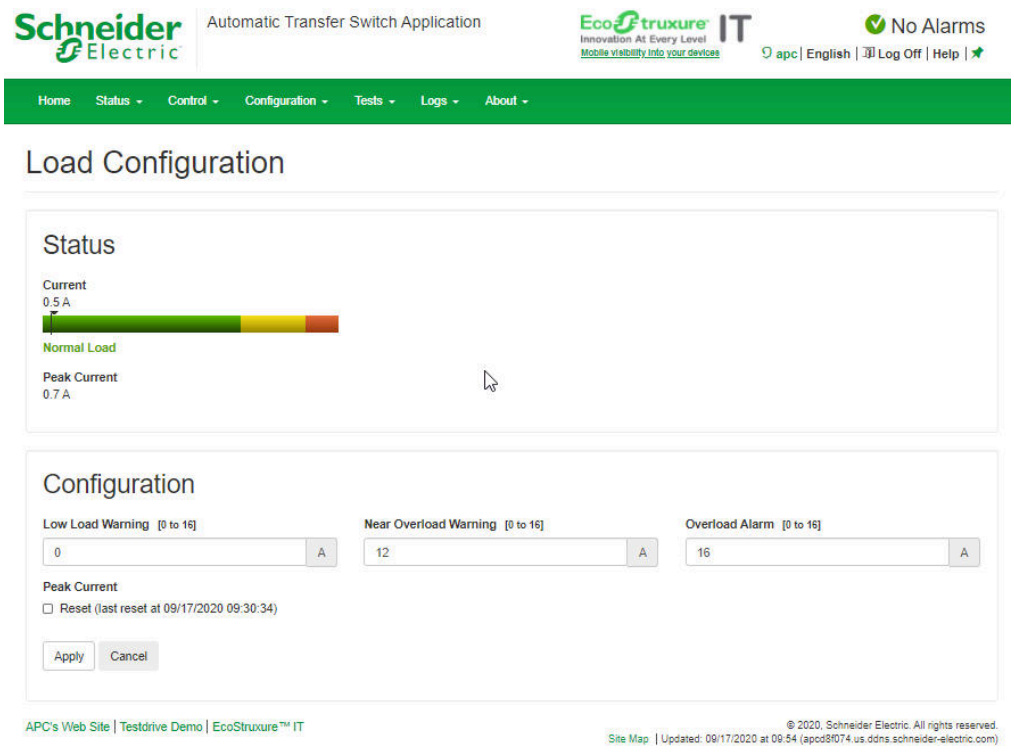
Transfer Range = Wide。

Rack ATSは、電圧が198 VRMS未満または218 VRMS以上 (208 ±10 VRMS)になると電源を切り替えます。

[Apply]をクリックして変更を保存するか、**[Cancel]**をクリックして変更を取り消します。

負荷しきい値の設定

選択手順（パス）： Configuration > ATS > Load



Status（ステータス）：デバイス、相、バンクの電流（A単位）およびピーク電流（kVA単位）を表示します。緑、黄色、赤のメーターのインジケータは、正常、過負荷寸前、過負荷のいずれかの負荷状態を示します。

Load Thresholds（負荷しきい値）：バンクが定格値を超えると、Rack ATSがアラームを発生させます。**[Low Load Warning]（低負荷警告）**、**[Near Overload Warning]（過負荷寸前警告）**、**[Overload Alarm]（過負荷アラーム）**をトリガするアンペア数を設定します。

> **注記**： サーキットブレーカが作動しても、サーキットブレーカが開いたことを示す情報は表示されません。ただし、そのバンクの電流は降下します。次の理由から、**Low Load Warning**を1 Aに設定してください。
>
> - **[Low Load Warning]**のデフォルトの設定は0 Aです。こうすると警告は実質的に無効になりますが、この設定ではWeb UIにサーキットブレーカが作動したことは表示されません。
> - ［**Low Load Warning**］に1Aの検出しきい値を設定すると、サーキットブレーカの作動が表示されます。

Peak Current（ピーク電流）：ピーク電流をリセットします。

[Apply]をクリックして変更を保存するか、**[Cancel]**をクリックして変更を取り消します。

LCDディスプレイのオン/オフ切り替え

選択手順（パス）：Configuration > ATS > LCD On/Off

LCD画面を**On**にするか**Off**にするかを選択して、[**Apply**]をクリックします。

温度/湿度センサーの設定

選択手順（パス）： Configuration > ATS > Environment

注記： この機能を使用するには、オプションのAPC温度センサー(AP9335T)またはAPC温度/湿度センサー(AP9335TH)をRack ATSに接続している必要があります。

このページの上部には、温度センサーまたは温度/湿度センサーが接続されているかどうか(**センサーの種類**)、センサーの現在の**温度**および/または**湿度**の読み取り値、およびセンサーの**アラームの状態**が表示されます。ページの右上隅にある温度計のアイコンをクリックして、華氏と摂氏を切り替えることもできます。

温度と湿度の設定について

一般設定：

- **Sensor Name:** センサーのカスタム名を入力します。
- **Sensor Location:** センサーのある場所を入力します。

温度設定：

- **High Temperature Threshold**（**高温度しきい値**）に達して**Temperature Alarms**（**温度アラーム**）が**Enabled**（**有効**）に設定されている場合は、システムがWarning（警告）アラームを生成します。
- **Maximum Temperature Threshold**（**最高温度しきい値**）に達して**Temperature Alarms**（**温度アラーム**）が**Enabled**（**有効**）に設定されている場合は、システムがCritical（重大）アラームを生成します。
- **Peak Temperature**（**ピーク温度**）は、前回の**リセット**以降に記録された最高温度です。**Peak Time**（**ピークタイム**）は、ピーク温度**が記録された**日時を示します。

湿度設定：

- **Low Humidity**（**低湿度**）しきい値に達して**Humidity Alarms**（**湿度アラーム**）が**Enabled**（**有効**）に設定されている場合は、システムがWarning（警告）アラームを生成します。
- **Minimum Humidity**（**最低湿度**）しきい値に達し、**Humidity Alarms**（**湿度アラーム**）が**Enabled**（**有効**）に設定されている場合は、システムがCritical（重大）アラームを生成します。

ヒステリシス：この値は、温度または湿度がしきい値を超えた場合に、しきい値違反をクリアするためにどれくらいの距離まで戻るかを指定します。

- [Maximum]と[High]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。
- [Minimum]と[Low]の湿度のしきい値の場合、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]または[Humidity Hysteresis]の値を大きくします。ヒステリシスの値が低すぎる場合、このような変動が原因で、しきい値違反が繰り返しクリアされる可能性があります。

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です。温度が85 °Fを超えると、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(しきい値を3 °F下回る)まで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：最低湿度しきい値は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%まで変動しながら低下する状態が繰り返し発生し、13%まで低下する状態が続きますが、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）を上回る必要があります。

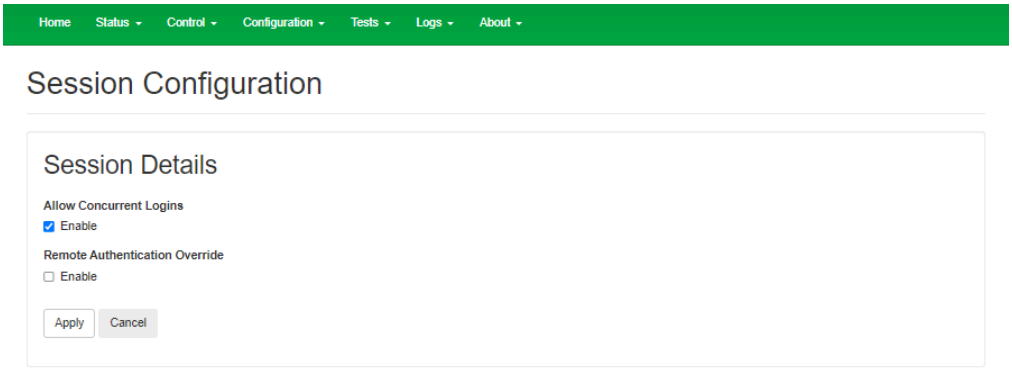
温度および湿度センサーを設定するには

1. 温度と湿度のしきい値を入力します。
2. **ヒステリシス**値を入力します。
3. 必要に応じて、アラーム生成を有効にします。
4. [**Apply**]をクリックします。

セキュリティ設定の管理

ユーザーセッションの設定の管理

選択手順（パス）：Configuration > Security > Session Management



Allow Concurrent Logins（同時ログインを許可）：2人以上のユーザーが同時にログオンできるようにするには、**[Enable]**を選択します。各ユーザーは同等のアクセス権を持ち、各インターフェイス（HTTP、FTP、Telnet、シリアル接続など）はログインユーザーとしてカウントされます。

Remote Authentication Override（リモート認証上書き）：Rack ATSは、サーバー上のパスワードのRADIUSストレージをサポートします。ただし、この上書き機能を有効にした場合、Rack ATSでは、ローカルユーザーはRack ATSにローカルに保存されているパスワードを使用してログオンできます。詳細については、「ローカルユーザー設定の管理, 148 ページ」および「リモートユーザー設定の管理, 151 ページ」を参照してください。

Ping応答の有効化

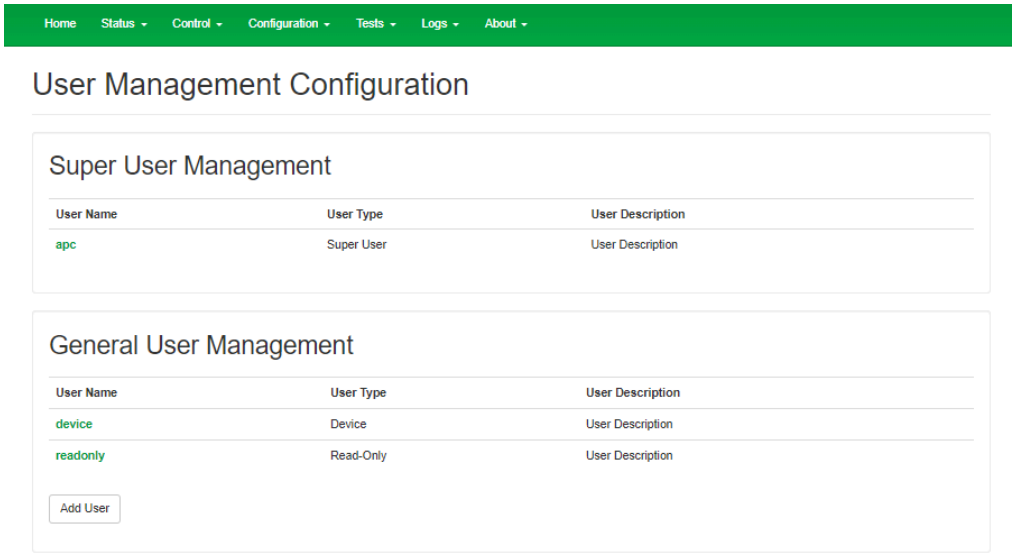
選択手順（パス）：Configuration > Security > Ping Response

IPv4のPing応答：**[Enable]**チェックボックスを選択すると、Rack ATSがネットワークpingに応答できるようになります。チェックボックスの印を外すと、Rack ATSの応答を無効にします。ping応答が有効で、Rack ATSが応答しない場合は、アクセスに関する問題, 198 ページの「 ATSに対してpingが実行できない, 198 ページ」の項を参照してください。

この設定はIPv6には適用されません。

ローカルユーザー設定の管理

選択手順（パス）：Configuration > Security > Local Users > Management



[Add User]をクリックして新規ユーザーを追加するか、**[User Name]**を選択してそのユーザーの設定を編集します。

- **Access:** [**Enable**] チェックボックスを選択すると、Rack ATSにアクセスできます。
- **User Name:** 新しいユーザー名を入力します。
- **Current Password、New Password、Confirm Password:** [New Password]フィールドと[Confirm Password]フィールドの両方に新しいパスワードを入力します。新しいユーザーのパスワードを入力する必要があります。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。

  注記：名前とパスワードの最大長は64バイトで、マルチバイト文字は64文字未満になります。64バイトより大きい**[Name]**および**[Password]**の値は切り捨てられます。管理者/スーパーユーザー設定を変更するには、3つすべてのフィールドに入力する必要があります。

- **User Type:** ドロップダウンリストからユーザータイプを選択します。

オプション	説明
Administrator	管理者は、すべてのメニューへの読み込み/書き込みアクセス権があります。
Device	デバイス関連メニューへの読み込み/書き込みアクセス権があります。管理者が有効または無効にできます。
Read-Only	読み取り専用のアクセス権。管理者が有効または無効にできます。
Network-Only	ネットワーク関連メニューへの読み取り/書き込みアクセス権があります。管理者が有効または無効にできます。

- **User Description:** ここにユーザーを識別するための詳細を入力します。
- **Session Timeout:** 非アクティブユーザーをログオフするまでのRack ATSの待ち時間を分単位で入力します（デフォルトでは3分）。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。

  注記： ユーザーがログオフせずにWeb UIを閉じた場合も、[**Session Timeout**]フィールドで指定した時間ログオン状態と見なされます。このため、Web UIを閉じたユーザーの代わりに他のユーザーが操作することができなくなる場合があります。

- **Serial Remote Authentication Override:** シリアルコンソール(CLI)接続を使用してRADIUSをバイパスするには、この[シリアルリモート認証オーバーライド]を使用します。この画面では、選択したユーザーに対して [シリアルリモート認証オーバーライド] が有効になっていますが、これが機能するには、[セッションの管理]画面を使用して一括で有効にする必要があります(ユーザーセッションの管理, 136 ページを参照)。
- **ユーザー設定**：

オプション	説明
Event Log Color Coding	この [イベントログの色分け] 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設定変更エントリの色は変わりません。 **赤**：アラームの重要度=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**：アラームの重要度=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**：アラームは解除されました。アラームの原因となった状態が改善されました。**黒**：アラームは発生していません。Rack ATSおよび接続されているすべてのデバイスは正常に動作しています。
Export Log Format	エクスポート（ダウンロード）時にイベントログを表示する形式を設定します。タブ区切り（デフォルト）ではフィールドがタブ区切りで表示され、CSVではコンマで区切られて表示されます。
Temperature scale	デフォルトの温度単位として、Fahrenheit（華氏）またはMetric（摂氏）を選択します。
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。

[Next]をクリックしてから**[Apply]**をクリックして保存するか、**[Cancel]**をクリックしてユーザー管理設定ページに戻ります。

デフォルトのユーザー設定

選択手順（パス）： Configuration > Security > Local Users > Default Settings

スーパーユーザーや管理者のレベルのアカウントで新しいユーザーを作成するときに、各フィールドで使用するデフォルト値を決定します。これらの値は、設定がシステムに適用される前に変更することができます。

リモートユーザー（RADIUSなど、リモートで認証されたシステムに保存されないユーザーアカウント）の場合は、認証サーバーから提供されない値のために、これらの値が使用されます。例えば、RADIUSサーバーがユーザーに温度設定を提供しない場合は、このセクションで定義された値が使用されます。

- **Access:** [**Enable**] チェックボックスを選択すると、Rack ATSにアクセスできます。
- **User Type:** ドロップダウンリストからユーザータイプを選択します。

オプション	説明
Administrator	管理者は、すべてのメニューへの読み込み/書き込みアクセス権があります。
Device	デバイス関連メニューへの読み込み/書き込みアクセス権があります。管理者が有効または無効にできます。
Read-Only	読み取り専用のアクセス権。管理者が有効または無効にできます。
Network-Only	ネットワーク関連メニューへの読み取り/書き込みアクセス権があります。管理者が有効または無効にできます。

- **User Description:** ここにユーザーを識別するための詳細を入力します。
- **Session Timeout:** 非アクティブユーザーをログオフするまでのRack ATSの待ち時間を分単位で入力します（デフォルトでは3分）。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。

  注記： ユーザーがログオフせずにWeb UIを閉じた場合も、[**Session Timeout**]フィールドで指定した時間ログオン状態と見なされます。このため、Web UIを閉じたユーザーの代わりに他のユーザーが操作することができなくなる場合があります。
- **Bad Login Attempts:** ユーザーがアカウントをブロックされるまでのログインの失敗回数を指定します。0 ~ 99回の範囲内で選択します。0 =無制限。
- **ユーザー設定**：

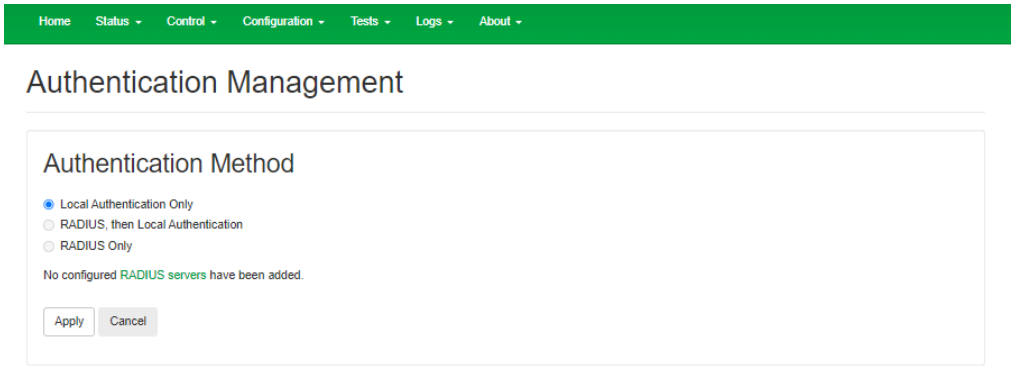
オプション	説明
Event Log Color Coding	この [イベントログの色分け] チェックボックスをオンにすると、イベントログに入力されるアラーム関連のテキストを色分けすることができます。システムイベントおよび設定変更エントリの色は変わりません。 **赤**：アラームの重要度=致命的。直ちに対処を要する重大な障害が発生しています。**オレンジ**：アラームの重要度=警告。処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。**緑**：アラームは解除されました。アラームの原因となった状態が改善されました。**黒**：アラームは発生していません。Rack ATSおよび接続されているすべてのデバイスは正常に動作しています。
Export Log Format	エクスポート（ダウンロード）時にイベントログを表示する形式を設定します。タブ区切り（デフォルト）ではフィールドがタブ区切りで表示され、CSVではコンマで区切られて表示されます。
Temperature scale	デフォルトの温度単位として、Fahrenheit（華氏）またはMetric（摂氏）を選択します。
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。

- **パスワード要件**：

オプション	説明
Strong Passwords	ユーザアカウント用に作成する新しいパスワードが、小文字と大文字、数字、記号をそれぞれ1つ以上使用しなければならない強力なものにするかどうかを設定します。
Password Policy	ユーザーにパスワードの変更が要求されるまでの日数を入力します。値を0日（デフォルト）とすると、この機能は無効になります。

リモートユーザー設定の管理

パス：**Configuration > Security > Remote Users > Authentication**



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

- ユーザーはRADIUSが有効になっているRack ATSにアクセスすると、認証要求がRADIUSサーバーに送信され、ユーザーの権限レベルが特定されます。
- Rack ATSで使用されるRADIUSユーザー名は、大文字と小文字が区別され、最大64バイトです。したがって、ASCII文字なら最大64文字まで対応します。マルチバイト言語では文字長はより小さくなります。文字のないパスワード（空白のパスワード）は許可されません。

ログオン時のリモートユーザーの認証方法を指定します。次のいずれかを選択します。

- **ローカル認証のみ**：RADIUSは無効になっています。ローカル認証が有効になっています。
- **RADIUS、次にローカル認証**：RADIUSとローカル認証が有効になっています。最初にRADIUSサーバーからの認証が要求されます。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のみ**：RADIUSが有効になっています。ローカル認証が無効になっています。

  注記： **RADIUS Only**が選択され、RADIUSサーバーが応答しない、または設定に不備がある場合、全ユーザーはリモートアクセスができなくなります。シリアル接続を介してCLIに接続し、**access**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**に変更するコマンドは、`radius -a local`になります。

ローカル認証（RADIUSサーバーの一元化された認証を使用しないもの）については、www.se.comで*Security Handbook*をご参照ください。

RADIUSサーバーの設定

選択手順（パス）：Configuration > Security > Remote Users > RADIUS

このオプションでは以下を実行できます。

- Rack ATSで使用できるRADIUSサーバー（2台まで）と各サーバーの応答タイムアウト時間を表示します。
- サーバーを選択し、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サーバーを選択すると、そのサーバーのパラメータを表示、変更できます。

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（IPv4またはIPv6）。リンクを選択してサーバーを設定します。
Port	RADIUSサーバーがユーザー認証に使用するポート（デフォルトでは1812）。Rack ATSはポート1812および5000 ~ 32768に対応しています。
Secret	RADIUSサーバーとRack ATS間の共有シークレット。
Reply Timeout	Rack ATSがRADIUSサーバーからの応答を待つ時間（秒）。
Test Settings	スーパーユーザーまたは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します。（お勧めしません）

環境設定手順の概要Rack ATSで使用するには、RADIUSサーバーの設定を行う必要があります。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、www.se.comの『Security Handbook』を参照してください。

1. Rack ATSのIPアドレスをRADIUSサーバーのクライアントリスト（ファイル）に追加します。
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 UIの場合のみ）。RADIUSユーザーファイルについての情報はRADIUSサーバーのマニュアル、その例については(www.se.comの)『*Security Handbook*』を参照してください。
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を使用する場合、辞書ファイルを構成し、RADIUSユーザーファイルを使用する必要があります。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。VSAが通常のRADIUS属性より優位になります。

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する：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を付与する場合、RADIUSの「user」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、APC-Service-Typeを`Device`（デバイス）に変更してください。

```
DEFAULTAuth-Type = System
APC-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。

```
bconnersAuth-Type = System
APC-Service-Type = Admin
thawkAuth-Type = System
APC-Service-Type = Device
```

サポート対象のRADIUSサーバーFreeRADIUS v1.xおよびv2.x、Microsoft Server 2008および2012 Network Policy Server (NPS)がサポートされています。その他の一般的に使用可能なRADIUSアプリケーションについては、完全には検証を行っておりません。

注記： RADIUSの使用に関する詳細については、『*Security Handbook*』を参照してください。

ファイアウォールメニュー

選択手順（パス）： **Configuration > Security > Firewall > Configuration**

ファイアウォール機能を有効または無効にします。設定したポリシーはデフォルトで一覧表示されます。**[Enable]**チェックボックスをオンにして、ファイアウォールを有効にします。チェックボックスはデフォルトで選択されていません。

- **[Apply]**をクリックして、選択したファイアウォールポリシーの有効化を確定します。**[Firewall Confirmation]**（ファイアウォールの確認）ページが開きます。
  - **[Confirmation(確認)]**ページには、有効化する前にファイアウォールをテストするための推奨事項が記載されています。必須ではありません。
  - 最初のハイパーリンクをクリックすると、**Firewall Policy**（**ファイアウォールポリシー**）ページに移動します。
  - 2番目のハイパーリンクをクリックすると、**Firewall Test**（**ファイアウォールテスト**）ページに移動します。
  - **[Apply（適用）]**をクリックするとファイアウォールが有効になり、**Configuration**（**設定**）ページに戻ります。
  - **[Cancel（キャンセル）]**をクリックすると、ファイアウォールを有効にせずに**Configuration**（**設定**）ページに戻ります。
- **[Cancel]**をクリックすると、新しい選択内容は有効になりません。**[Configuration]**（**設定**）ページに留まります。

アクティブなポリシー

選択手順（パス）： **Configuration > Security > Firewall > Active Policy**

[Available Policies]（**利用可能なポリシー**）ドロップダウンリストからアクティブなポリシーを選択し、そのポリシーの有効性を表示します。現在アクティブなポリシーがデフォルトで表示されます。別のポリシーをリストから選択できます。

- **[Apply]**をクリックして変更内容を有効にします。別のファイアウォールが選択され、有効になると、変更は直ちに有効になります。新しく設定したファイアウォールポリシーを選択する場合、有効にする前に新しいファイアウォールをテストすることが推奨されます(新しいファイアウォールは、**Configuration > Security > Firewall > Configuration**でテストできます)。
- **[Cancel]**をクリックすると元のアクティブポリシーが回復され、**Active Policy**ページに留まります。

アクティブなルール

選択手順（パス）：**Configuration > Security > Firewall > Active Rules**

ファイアウォールが有効になると、この読み取り専用ページには、現在アクティブなポリシーによって有効になった個別ルールが一覧表示されます。フィールドの説明(**Priority、Destination、Source、Protocol、Action、Log**)については、「ポリシーの作成/編集, 153 ページ」を参照してください。

ポリシーの作成/編集

選択手順（パス）：**Configuration > Security > Firewall > Create/Edit Policy**

このページを使用して、新しいポリシーを作成するか、既存のポリシーを削除または編集します。

有効なアクティブなファイアウォールポリシーは削除できません。実行中のポリシーは編集できますが、変更はすぐに適用されるため、お勧めしません。その代わりに、ファイアウォールを無効化し、ポリシーを編集し、テストしてからポリシーを再度有効にしてください。

新しいポリシーの作成

[Add Policy]（ポリシーを追加）をクリックし、新しいファイアウォールファイルのファイル名を入力します。ファイル名の拡張子は.fwlとしてください。ファイル拡張子を付けないと、自動的に.fwlが名前に付与されます。

- **[Apply]**をクリックします。ファイル名が有効な場合、空のファイアウォールポリシーファイルが作成されます。このファイルは、システム上の他のポリシーと一緒に、**/fwl**フォルダに配置されます。
- **[Cancel]**をクリックすると、新しいファイアウォールを作成せずに前のページに戻ります。

既存ポリシーの編集

[Edit Policy]（ポリシーを編集）を選択して編集ページに移動します。アクティブでないファイアウォールポリシーを編集できます。

警告ページ: アクティブな有効ポリシーを編集しようとすると、警告ページが開きます。**アクティブなファイアウォールポリシーを編集すると、すべての変更が直ちに適用されます。ファイアウォールを無効化し、ポリシーをテストしてから有効化することが推奨されます。**

- **[Apply（適用）]**をクリックすると警告ページが閉じ、**Edit Policy（ポリシーの編集）**ページに戻ります。
- **[Cancel（キャンセル）]**をクリックすると警告ページが閉じ、**Create/Edit Policy（ポリシーの作成/編集）**ページに戻ります。

1. 編集するポリシーを**[Policy Name]**（ポリシー名）ドロップダウンリストから選択し、**[Edit Policy]**をクリックします。

2. **[Add Rule（ルールを追加）]**をクリックするか、既存ルールの**[Priority（プライオリティ）]**を選択して、**[Edit Rule（ルールの編集）]**ページに移動します。このページからルール設定を変更したり、選択したルールを削除することができます。

設定	説明
Priority	2つのルールが競合する場合は、優先順位が高いルールによって処理が決まります。優先度が最も高いのは1、最も低いのは250です。
Type	**host: IP/any**フィールドに1つのIPアドレスを入力します。 **subnet: IP/any**フィールドにサブネットアドレスを入力します。 **range: IP/any**フィールドにIPアドレスの範囲を入力します。
IP/any	このルールを適用するIPアドレス、またはIPアドレスの範囲を指定します。または、次のいずれかを選択します。 - **any:** 規則はIPアドレスに関係なく適用されます。 - **anyipv4:** この規則はどのIPv4アドレスにも適用されます。 - **anyipv6:** この規則は、どのIPv6アドレスにも適用されます。
Port	規則を適用するポートを指定します： -**None:** 規則は任意のポートに適用されます。 -**Common Configured ports:** 標準ポートを選択します。 –**Other:** 非標準ポートの番号を指定してください。
Protocol	規則を適用するプロトコルを指定します。 -**any:**任意のプロトコル。 - **tcp:**アプリケーション間のより信頼性の高い情報転送に使用。 - **udp:**より高速で低帯域幅の情報を提供するためにTCPに代わって使用します。転送。遅延は少ないですが、UDPはTCPよりも信頼性に劣ります。 - **icmp:**トラブルシューティングのエラーの報告に使用されます。 - **icmpv6:**IPv6を使用するアプリケーションのトラブルシューティングのエラーの報告に使用されます。
Action	**allow:** この規則に一致するパケットを許可します。 **discard:** この規則に一致するパケットを破棄します。
Log	この規則がパケットに適用された場合、パケットがブロックされているか許可されているかにかかわらず、ファイアウォールログにエントリが追加されます(「ファイアウォールのログ、123ページ」を参照)。

ファイアウォールポリシーに、優先度の最も低いルールとして次のいずれかを追加することが推奨されます。

- ファイアウォールをホワイトリストとして使用するには、
  `250 Dest any / Source any / protocol any / discard`を追加します。
- ファイアウォールをブラックリストとして使用するには、
  `250 Dest any / Source any / protocol any / allow`を追加します。

ポリシーの削除

[Delete Policy]（ポリシーを削除）を選択してConfirm Deletion（削除確認）ページに移動します。

[Apply]をクリックして確定すると、選択したファイアウォールファイルがファイルシステムから削除されます。

ポリシーの読み込み

選択手順（パス）：Configuration > Security > Firewall > Load Policy

外部ソースから取得したポリシー（拡張子が.fwlのもの）をこのデバイスにアップロードします。

テスト

選択手順（パス）：Configuration > Security > Firewall > Test

選択したポリシーのルールを、指定した期間で一時的に強制します。

802.1X セキュリティ設定

選択手順（パス）： Configuration > Security > 802.1X Security

NMCは、IEEE 802.1Xポートベースのネットワークアクセス制御で使用されるEAPoL（Extensible Authentication Protocol over LAN）アーキテクチャでサプリカントの役割を果たします。NMCは、ユーザーに3つのクライアント側の証明書をアップロードすることを要求する認証方法としてEAP-TLSをサポートしています。秘密キーは、暗号化した形式で保管されます。802.1Xセキュリティアクセスを有効にするには、有効なパスフレーズを入力する必要があります。

注記： NMCは、EAP-TLS認証方式だけをサポートします。

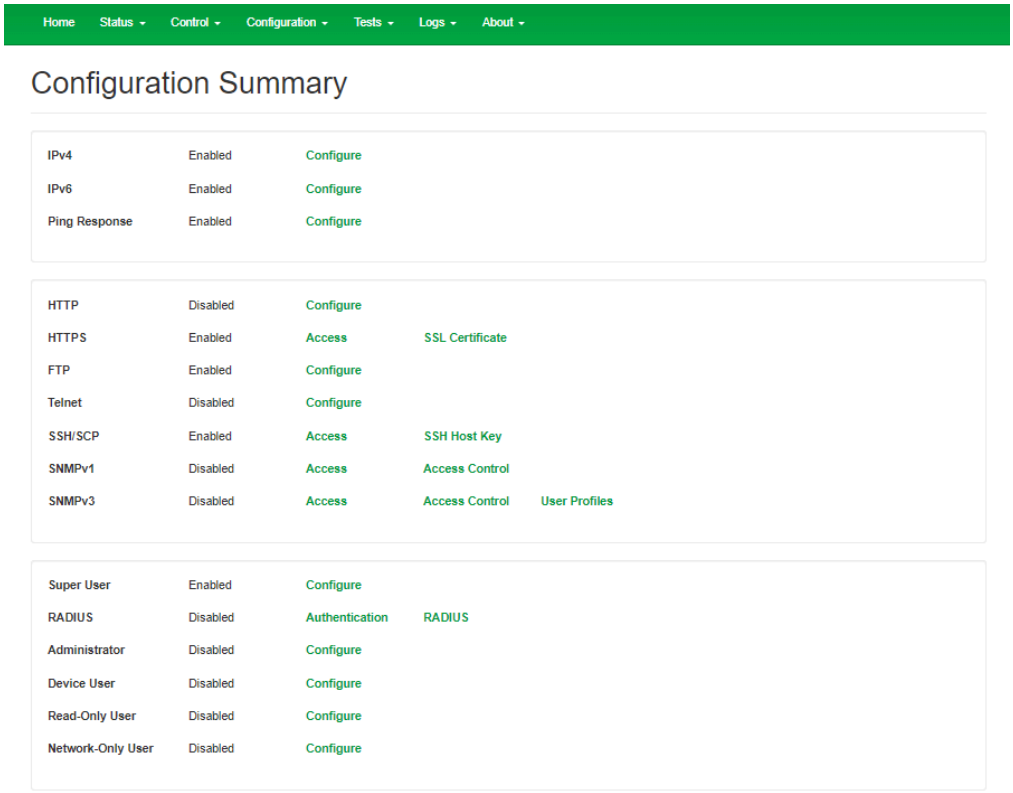
Web UIでは、EAPoL設定に以下のオプションがあります：

設定	説明
EAPoL Access（EAPoLアクセス）	802.1Xセキュリティアクセスを有効または無効にするために使用されます。 **備考**：802.1Xセキュリティアクセスは、デフォルトでは無効になっています。有効な証明書と秘密キーの有効なパスフレーズがユーザーから提供された場合にだけ、ユーザーが有効にすることができます。
Supplicant Identifier（サプリカント識別子）	ユーザが自分のサプリカント識別子を設定できるようにします（空白文字を含めて最大32文字）。 **備考**：デフォルトでは、サプリカント識別子は「NMC-Supplicantxx:xx:xx:xx:xx:xx」に設定されています。ここで、'xx'の部分の6つのオクテットがNMCのMAC IDです。
CA Certificate（CA証明書）	CAルート証明書をアップロード/交換または削除します。サポートされているファイル形式は、PEM (Privacy Enhanced Mail)形式またはDER (Distinguished Encoding Rules)形式であり、使用可能なファイル拡張子は.pem、.PEM、.der、または.DERです。
Private Key Certificate（秘密キーの証明書）	暗号化された秘密キーをアップロード/交換または削除します。サポートされているファイル形式は、PEM (Privacy Enhanced Mail)形式またはDER (Distinguished Encoding Rules)形式であり、使用可能なファイル拡張子は.keyまたは.KEYです。 **備考**：暗号化されていない秘密キーは使用できません。
Private Key Passphrase（秘密キーのパスフレーズ）	暗号化された秘密キーを復号化するためのパスフレーズを提供します。空白文字を含めて最大64文字まで可能です。
User/Public Certificate（ユーザー/公開証明書）	ユーザー/公開証明書をアップロード/交換または削除します。サポートされているファイル形式は、PEM (Privacy Enhanced Mail)形式またはDER (Distinguished Encoding Rules)形式であり、使用可能なファイル拡張子は.pem、.PEM、.der、または.DERです。

ネットワークの設定

プロトコル設定のまとめ

選択手順（パス）：Configuration > Network > Summary



このページでは、Rack ATSで有効または無効になっているすべてのプロトコルを表示することができます。該当する設定ページに移動するには、プロトコルのリンクを選択します。

TCP/IPの設定およびIPv4とIPv6の通信設定

選択手順（パス）： Configuration > Network > TCP/IP > IPv4

Rack ATSの現在の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、および起動モードを表示します。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。
BOOTP	BOOTPサーバーがTCP/IP設定を供給します。Rack ATSは、32秒間隔で、BOOTPサーバーにネットワーク割り当てを要求します。 • Rack ATSが有効な応答を受信すると、ネットワークサービスが開始されます。 • Rack ATSが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、Rack ATSは、再起動されるまでネットワーク設定要求を停止します。 • デフォルトでは、以前のネットワーク設定が存在していれば、Rack ATSは、5回のリクエスト（最初のリクエストと続く4回の再試行）で有効な応答を受信しなかった場合、以前のネットワーク設定を使用して、アクセス可能な状態を保持します。 **[Next>>]**をクリックすると[BOOTP Configuration]（BOOTPの設定）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。 • **Maximum retries（最大再試行回数）**：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（BOOTPを停止）**要求を選択します。
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 ATSは、任意のDHCPサーバーにネットワーク割り当てを要求します。 • Rack ATSが有効な応答を受信した場合、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APC cookieは（以前と同様に）必要ありません。 • Rack ATSでDHCP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や要求がタイムアウトした場合は、再起動するまでネットワーク設定の要求を停止します。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、Rack ATSに情報を提供するcookieをDHCPサーバーに提供するよう要求できます。
備考：通常、設定ページのこれらの3つの設定のデフォルト値は変更する必要はありません。 • **Vendor Class:** APC • **Client ID:** Rack ATS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) • **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	

DHCP応答オプション

有効なDHCP応答には、Rack ATSがネットワークで稼動するために必要なTCP/IP設定、およびRack ATSの動作に影響するその他の情報を提供するオプションが含まれています。

ベンダー固有の情報（オプション43）

Rack ATSは、DHCP応答でこのオプションを使用して、DHCP応答が有効かどうかを判断します。このオプションには、APC cookieと呼ばれるAPC固有のオプションがTAG/LEN/DATA形式に含まれます。これはデフォルトでは無効になっています。

- APC Cookie. Tag 1, Len 4, Data “1APC”

オプション43は、DHCPサーバーがデバイスにサービスを提供するよう設定されていることをRack ATSに通知します。

次の例では、APC cookieを含む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 ATSは、有効なDHCP応答の中にある次のオプションを使用して、自己のTCP/IPを設定します。最初のオプションを除くこれらすべてのオプションは、RFC2132で説明されています。

- **IP Address**(DHCP応答の**yiaddr**フィールド値。RFC2131で説明されています): DHCPサーバーがRack ATSにリースしているIPアドレス。
- **Subnet Mask**（オプション1）: Rack ATS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値です。
- **Router**、すなわちデフォルトゲートウェイ（オプション3）: Rack ATSがネットワークで稼動するために必要なデフォルトのゲートウェイアドレスです。
- **IP Address Lease Time**（オプション51）: Rack ATSへのIPアドレスのリース期間です。
- **Renewal Time**、T1（オプション58）: Rack ATSが、IPアドレスのリース割り当て後、このリースの更新を要求するまでの待機時間です。
- **Rebinding Time**、T2（オプション59）: Rack ATSが、IPアドレスのリース割り当て後、このリースの再バインドを要求するまでの待機時間です。

その他のオプション

Rack ATSは、有効なDHCP応答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。

- **Network Time Protocol Servers**（オプション42）：Rack ATSで使用可能な2つまでのNTPサーバー（プライマリおよびセカンダリ）。
- **Time Offset**（オプション2）: Rack ATSユニットのサブネットの、協定世界時(UTC)からの秒単位のオフセット値です。
- **Domain Name Server**（オプション6）: Rack ATSが使用できる2つまでのDomain Name System(DNS)サーバー（プライマリおよびセカンダリ）。
- **Host Name**（オプション12）: Rack ATSが使用するホスト名（最長32文字）。
- **Domain Name**（オプション15）: Rack ATSが使用するドメイン名（最長64文字）。
- **Boot File Name**(DHCP応答のファイルフィールドに表示されるブートファイル名。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ーのIPアドレスが指定されます。このサーバーからRack ATSが.iniファイルをダウンロードします。ダウンロードした後、.iniファイルはブートファイルとして使用され、設定を再設定します。

ネットワークポート速度の設定

選択手順（パス）： Configuration > Network > Port Speed

Port Speed（ポート速度）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。
- または、**10** Mbpsまたは**100** Mbpsを選択できます。どちらの場合も、半二重（**一度に一方向のみの通信**）**または**全二重（**同じチャンネルで同時に双方向の通信**）のオプションがあります。

DNSの設定

選択手順（パス）： Configuration > Network > DNS > Configuration

Configurationの下のオプションを使用して、Domain Name System(DNS)を設定します。

- **Override Manual DNS Settings:**（手動DNS設定の上書き）有効にすると、他のソース（通常はDHCP）からの設定データがここで設定した手動設定よりも優先されます。
- **Primary DNS Server or Secondary DNS Server:**（プライマリDNSサーバーまたはセカンダリDNSサーバーの）いずれかを選択して、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またはIPv6アドレスを指定します。Rack ATSで電子メールを送信するには、少なくともプライマリDNSサーバーのIPアドレスを定義する必要があります。
  - Rack ATSは、プライマリDNSサーバーまたはセカンダリDNSサーバー（指定されている場合）からの応答を最大15秒間待ちます。この時間内にRack ATS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。DNSサーバーは、Rack ATS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アドレスを定義し、ネットワーク上のコンピュータのDNS名を入力して、そのコンピュータの正しいオペレーションを検証するためにIPアドレスを探します。
- **System Name Synchronization（システム名の同期）**：システム名をホスト名と同期します。これにより、両方の入力フィールドに同じ名前が自動的に入力されます。

  注記： この機能を有効にすると、システム名の識別子に空白文字を含めることができなくなります(これは、**Host Name**フィールドと同期されるためです)。
- **Host Name:** ここでホスト名を設定し、**Domain Name**フィールドでドメイン名を設定します。その後、ドメイン名を受け入れるNMCインターフェイス（電子メールアドレスを除く）の任意のフィールドにホスト名を入力できます。
- **Domain Name (IPv4/IPv6):** ここでドメイン名のみを設定します。ドメイン名を受け入れるNMCインターフェイスのその他すべてのフィールド（電子メールアドレスを除く）にホスト名のみが入力されているときは、Rack ATS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。
  - 特定のホスト名入力の拡張子を上書きするには、最後のピリオドも含みます。NMCは、ピリオドが後続するホスト名(*mySnmpServer*.など)を完全修飾ドメイン名と同じように認識し、ドメイン名を追加しません。
- **Domain Name (IPv6):** ここでIPv6ドメイン名を指定します。

DNS設定のテスト

選択手順（パス）： Configuration > Network > DNS > Test

このオプションを使用して、IPアドレスを検索することによりDNSサーバーのセットアップをテストする、DNSクエリを送信します。テスト結果は**[Last Query Response]**（前回のクエリ応答）フィールドで確認するか、または選択したクエリタイプで使用される値を識別します。

選択されたクエリタイプ	使用するクエリ質問
by Host（ホスト）	サーバーのURL名
by FQDN	*my_server.my_domain*という書式のサーバーの完全修飾ドメイン名
by IP	サーバーのIPアドレス
by MX	サーバーのMail Exchangeアドレス

Webアクセスの設定

パス：**Configuration > Network > Web > Access**

次のいずれかの選択の変更を有効化するには、すべてのユーザーがログオフしなければなりません。

設定	説明
HTTPを有効化する：	ハイパーテキスト・トランスファー・プロトコル(HTTP)を有効化します。HTTPでは、ユーザー名とパスワードを使ってウェブアクセスができますが、送信中にユーザー名、パスワード、データの暗号化は行われません。HTTPはデフォルトで無効になっています。
HTTPSを有効化する：	セキュア・ソケッツ・レイヤー（SSL）/トランスポート・レイヤー・セキュリティ/（TLS）の上でハイパーテキスト・トランスファー・プロトコル（HTTPS）を有効化します。SSLおよびTLSは、送信中にユーザー名、パスワード、データを暗号化し、デジタル証明書を使用してRack ATSを認証します。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。HTTPSの詳細については、wwww.se.comから入手できる*Security Handbook*の「デジタル証明書の作成およびインストール」を参照してください。HTTPSはデフォルトで有効になっています。
HTTPポート：	Rack ATSとのHTTPによる通信に使用されるTCP/IPポート（デフォルトでは80番）です。

HTTPSポート：	Rack ATSとのHTTPSによる通信に使用されるTCP/IPポート（デフォルトでは443番）です。
	
	注記：またセキュリティを強化するために、いずれのポートを5000 ~ 32768番のいずれかの未使用のポートに変更することができます。この場合、ポート番号を指定するためにブラウザのアドレスフィールドにコロン（：）を入力する必要があります。例えば、ポート番号が5000、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`

最小限のプロトコル	ドロップダウンリストからHTTPSセキュリティプロトコルの最小値を選択します。
認証Cookieの要求	クッキーが有効になっている場合、装置にアクセスするユーザーは、正しいセッションID（Web URLに存在）、セッションの作成に使用されたリモートIPアドレス、およびクッキーを持っている必要があります。Cookieが無効になっているか削除されている場合、ユーザーはログインする必要なく、セッションIDの同じURLを同じウェブブラウザーの新しいタブにコピーして貼り付けることができます。 詳細については、FA235784のFAQ記事：*Network Management Card 2(NMC2)*「*Require Authentication Cookie*」を参照してください。
限定ステータスアクセス	**Enable**（**有効**）を選択すると、デバイスの基本的なステータスとともに読み取り専用の公開ウェブページが表示されます。**Use as Default Page**（**デフォルトのページとして使用**）を選択し、このステータスページをRack ATSのランディングページにします。

注記： FAQ記事を検索するには、www.se.comに進み、あなたのロケーションを選択します。次に、**サポート > 文書とソフトウェアのダウンロード**を選択して、検索バーにFAQ記事の番号またはタイトルを入力します。

Webアクセス用のSSL証明書の設定

選択手順（パス）： Configuration > Network > Web > SSL Certificate

現在の証明書ステータスを表示します。セキュリティ証明書を追加、差し替え、または削除します。

設定	説明
ステータス	• **Not installed:** 証明書がインストールされていないか、FTPまたはSCPによって誤った場所にインストールされています。**証明書ファイルの追加または交換**を使用すると、証明書がRack ATSの正しい場所(/ssl)にインストールされます。 • **Generating:** 有効な証明書が見つからなかったため、Rack ATSが証明書を生成しています。 • **Loading:** Rack ATSで証明書をアクティブ化しています。 • **Valid certificate:** 有効な証明書がインストールされたか、Rack ATSによって生成されました。証明書の内容を表示するには、このリンクを選択します。 **備考**：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/TLS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 ATS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。
証明書の操作：	• **Add or Replace（追加または交換）:** セキュリティウィザードで作成した証明書ファイルを入力するか、そのファイルの場所まで移動します。セキュリティウィザードまたはRack ATSで作成されたデジタル証明書の使用方法を選択するには、『Security Handbook』の「Creating and Installing Digital Certificates（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。このハンドブックはwww.se.comでご覧いただけます。 • **Remove（削除）**：現在の証明書を削除します。

CLIアクセスの設定

選択手順（パス）： Configuration > Network > Console > Access

Enable Telnet（Telnetを有効にする）：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。Telnetは、デフォルトでは無効です。

Enable SSH（SSHを有効にする）：SSHでは、ユーザー名、パスワード、データを暗号化して送信されます。これにより、送信中のデータの傍受、捏造、改変を防ぐことができます。デフォルトでは、SSHが有効になっています。

Telnet Port（Telnetポート）：Telnetポート（デフォルトでは23）は、Rack ATSとの通信に使用されます。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。例えば、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しなければなりません。

```
telnet 152.214.12.114:5000
```

```
telnet 152.214.12.114 5000
```

SSH Port（SSHポート）: SSHポート（デフォルトでは22）は、Rack ATSとの通信に使用されます。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。

SSHホストキーの設定

選択手順（パス）： Configuration > Network > Console > SSH Host Key

Status（ステータス）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かったため、Rack ATSがホストキーを作成しています。
- **Loading:** ホストキーが.Rack ATSで読み込み中です。
- **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 ATS上の必要な場所)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 ATSが生成した2048ビットのRSAホストキー

証明書の操作：

- **Add or Replace（追加または交換）:** 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て、ホストキーファイルをアップロードします。Security Wizardの使用方法については、www.se.comにある『*Security Handbook*』を参照してください。

  注記： SSHの有効化に要する時間を短縮するには、事前にホストキーを作成してアップロードしておきます。ホストキーが読み込まれていない状態でSSHを有効にした場合、Rack ATSはホストキーを作成します。これには1分ほどかかり、その間SSHサーバーにはアクセスできなくなります。
- **Host Key Fingerprint（ホストキーフィンガープリント）**：フィンガープリントは、サーバーの認証に役立ちます。セキュリティウィザードを使用してホストキーを生成する場合、フィンガープリントも生成されます。これは、SSHが有効になっていて、ホストキーが使用されているときに表示されます。SSHを使用して最初にデバイスに接続するとき、SSHクライアントによって提示されたフィンガープリントをセキュリティウィザードが生成したフィンガープリントと比較して、それらが一致することを確認します。(ほとんどすべてのSSHクライアントはフィンガープリントを表示します。)
- **Remove（削除）**：現在のホストキーを削除します。

  注記： 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オプション

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でネットワークに送出されます。お使いのネットワークでは暗号化による高度なセキュリティを要する場合は、SNMPv1アクセスを無効にし、替わりにSNMPv3を使用してください。

Data Center Expertを使用してパブリックネットワーク上のRack ATSを管理する場合は、Rack ATSインターフェイスとData Center Expertインターフェイスの両方で同じバージョンのSNMP（1または3）を有効にする必要があります。読み取りアクセスの場合、Data Center ExpertはRack ATSからトラップを受信できますが、Data Center Expertをトラップレシーバとして設定する間は書き込みアクセスが必要です。

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、『*Security Handbook*』を参照してください。このハンドブックはwww.se.comから入手できます。

ネットワークポートの共有

グループ内のRack ATS unitsはすべて、PowerNet-MIBで利用可能なSNMP "ats5g" OIDを介してHost Rack ATSからアクセスできます。

これらのOIDへの完全なパスは次のとおりです：iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).apc(318).products(1).hardware(1).ats5g(33)

各Rack ATSユニットは、各テーブルの対応する"Module" OIDを参照してSNMP MIBテーブルで識別できます。これらのモジュールOIDは、Rack ATSのDisplay IDを返します。

モジュールOIDの例：ats5gIdentConfigModuleID、ats5gSwitchModuleID、ats5gEnvModuleID、ats5gBankModuleID

以前のバージョンとの下位互換性を維持するため、ホストRack ATSは複数のRack ATSユニットをサポートするテーブルでは常に最初のインデックスとなります。さらに、Rack ATSグループの設定後は、Display IDが変更された場合やユニットが一時的に通信できない場合でも、ゲストRack ATSユニットのインデックス順序は変更しないでください。インデックスの順序は、Rack ATSを手動でグループから削除した場合にのみ変更する必要があります。

一時的に通信が失われたRack ATSに関連するインデックスは、MIBテーブルウォークによってスキップされます。

SNMPv1

デフォルトでは、SNMPv1は無効になっています。この設定では、SNMPv2cがSNMPv1でサポートされています。

アクセス

選択手順（パス）： Configuration > Network > SNMPv1 > 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。

アクセス制御

選択手順（パス）： Configuration > Network > SNMPv1 > 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エントリを設定できます。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選択します。

注記： 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。

注記： 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。

設定	説明
Community Name（コミュニティ名）	NMSがコミュニティにアクセスするために使用しなければならない名前。最大16文字のASCII文字を使用できます。
NMS IP/ Host Name	NMSによるアクセスを制御するIPv4または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。「255」を含むIPアドレスは、次のようにアクセスを制限します。 - 149.225.12.**255**: 149.225.12セグメントのNMSからのアクセスのみ。 - 149.225.**255.255**: 149.225セグメントのNMSからのアクセスのみ。 - 149.**255.255.255**: 149セグメントのNMSからのアクセスのみ。 - 0.0.0.0（デフォルト）または255.255.255.255: どのセグメントのNMSでもアクセス可能。
Access Type（アクセスタイプ）	NMSがコミュニティを通じて実行できるアクションです。 - **Read:** GETのみ、常時。 - **Write:** 常にGET。Web UIまたはCLIにログオンしているユーザーがいない場合はSET。 - **Write+:** 常時GETとSET。 - **Disable:** 常にGETまたはSETがない。

SNMPv3

SNMPv3は、デフォルトでは無効になっています。

SNMPのGET、SET、およ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。

注記： 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。

アクセス

選択手順（パス）： Configuration > Network > SNMPv3 > Access

SNMPv3 Access: このデバイスとの通信方式としてSNMPv3を有効にします。

ユーザープロファイル

選択手順（パス）： Configuration > Network > SNMPv3 > User Profiles

デフォルト設定では、このページには**apc snmp profile1**から**apc snmp profile4**のユーザー名で設定された4つのユーザープロファイルの設定が一覧表示されており、認証とプライバシー（暗号化）は表示されません。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。

設定	説明
User Name（ユーザー名）	ユーザープロファイルの識別子です。SNMPv3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（認証パスフレーズ）	SNMPv3を介してこのデバイスと通信するNMSが、実際にそのNMS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時間通りに通信されていること（遅延がなく、コピーされて後で不適切な時間に再送信されたものではないことを示す）を確認する15 ~ 32文字のASCII文字からなるフレーズ。
Privacy Passphrase（プライバシーパスフレーズ）	15 ~ 32文字のASCII文字からなるフレーズ(デフォルトでは`hidden crypt.phrase`)。NMSがSNMPv3でこのデバイスに送信したり、このデバイスから受信したりする（暗号化による）データのプライバシーを高めます。
Authentication Protocol（認証プロトコル）	Schneider ElectricによるSNMPv3の実装では、SHAまたはMD5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（プライバシープロトコル）	SNMPv3実装では、データの暗号化と復号にはAESまたは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、プライバシー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ーパスフレーズが含まれていなければなりません。プライバシー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ー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。 **備考**：プライバシープロトコルは、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。

アクセス制御

選択手順（パス）： Configuration > Network > SNMPv3 > 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、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。

注記： 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しているすべてのネットワーク管理システムはこのデバイスにアクセスできます。

注記： 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。

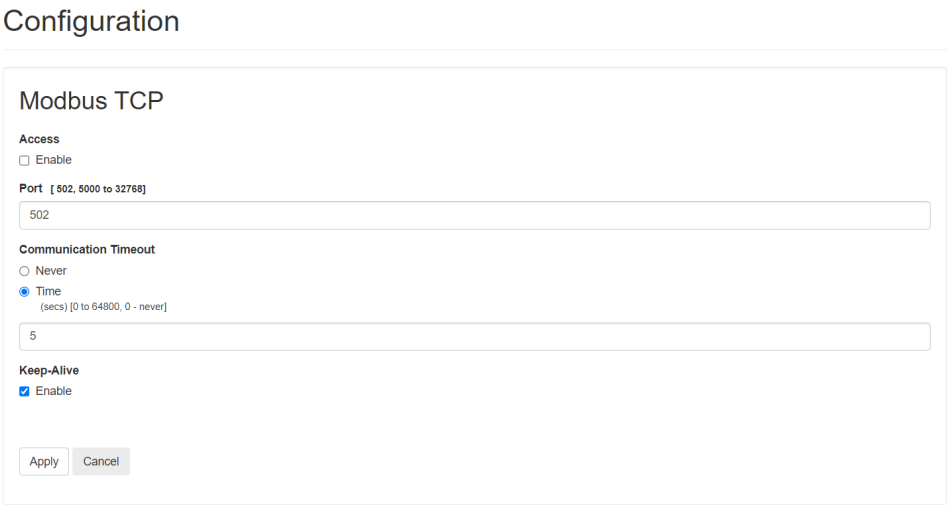
ユーザープロファイルのアクセス制御設定を変更するには、該当のユーザー名を選択します。

設定	説明
Access（アクセス）	**Enable**を選択すると、このアクセス制御エントリのパラメータで指定されたアクセス制御が有効になります。
User Name（ユーザー名）	このアクセス制御エントリを適用するユーザープロファイルを選択します。**Configuration > Network > SNMPv3 > User Profiles**で表示されたユーザープロファイルページで設定した4つのユーザー名から選択できます。
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。「255」を含むIPアドレスマスクは、次のようにアクセスを制限します。 - 149.225.12.**255**: 149.225.12セグメントのNMSからのアクセスのみ。 - 149.225.**255.255**: 149.225セグメントのNMSからのアクセスのみ。 - 149.**255.255.255**: 149セグメントのNMSからのアクセスのみ。 - 0.0.0.0（デフォルト）または255.255.255.255: どのセグメントのNMSでもアクセス可能。

Modbus TCPの有効化

パス： **Configuration > Network > TCP**

Modbusを有効化して、Building Management SystemがModbus TCPを介してRack ATSデバイスを監視できるようにします。



Modbus TCPを有効化するには、次の手順を行います。

設定	説明
Access	**Enable**を選択して、Modbus TCPを有効化します。
Port	TCP接続のポートを指定します(デフォルトでは502番ポート、または5000から32768番ポート)。
Communication Timeout:	Rack ATSデバイスがModbus Pollソフトウェアから切断されるまでの待機時間（秒単位）を入力します。
Keep-Alive	**Enable**を選択すると、他に通信が検出されない限り、Rack ATSデバイスは2時間75秒ごとにパケットをサーバーに送信します。これにより、コミュニケーションタイムアウトが7,275秒以上に設定されている場合、通信タイムアウトを防止することができます。

変更を適用にするには、Rack ATSのログオフを再起動する必要があります。

FTPサーバーの設定

選択手順（パス）： **Configuration > Network > FTP Server**

FTPサーバーの設定では、FTPサーバーへのアクセスを有効または無効にします。FTPはデフォルトでは無効になっています。

デフォルトでは、FTPサーバーは、TCP/IPポート21を介してRack ATSと通信します。FTPサーバーは指定されたポートと、そのポートより1小さい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、コマンドは`ftp 152.214.12.114:5001`となります。

注記： FTPはファイルを暗号化せずに転送します。セキュリティを強化するために、ファイルはSecure CoPy（SCP）で転送します。Secure SHell（SSH）はデフォルトで有効になっており、SCPを自動的に有効にします。ただし、SCPはスーパーユーザーのデフォルトパスワード（**apc**）が変更されるまでファイル転送を許可しません。Data Center Expertによる管理で、Rack ATSにアクセスできるようにするには、Rack ATSインターフェイスでFTPサーバーアクセスを有効にする必要があります。

注記： Rack ATSとData Center ExpertまたはEcoStruxure ITの両方で同じプロトコルが有効な場合は、FTPまたはSCPを使用して、Rack ATSとData Center ExpertまたはEcoStruxure ITの設定および更新を行うことができます。詳細については、Data Center ExpertまたはEcoStruxure ITのマニュアルを参照してください。

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、『*Security Handbook*』を参照してください。このハンドブックはwww.se.comから入手できます。

AP9834でのWi-Fi設定

選択手順（パス）：Configuration > Network > Wi-Fi

今後のバージョンアップにて使用可能。

通知の設定

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。イベントが発生した場合、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。

- 自動的な通知設定。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
- 履歴（イベントログ）
  - 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方法および使用方法については、「ログの設定, 180 ページ」を参照してください。
  - クエリ（SNMP GET）

    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。以下のアクセスタイプを設定できます

    SNMPの詳細については、「SNMPオプション, 165 ページ」を参照してください。

イベント別通知の設定

選択手順（パス）：Configuration > Notification > Event Actions > By Event

デフォルトでは、全イベントに対してログ記録が選択されています。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. イベントカテゴリまたはサブカテゴリを選択して、関連するイベントリストを表示します。
2. 既存の設定を表示するには（例：受信者に電子メールで通知する、Network Management Systems（NMS）にSNMPトラップで通知する）、イベント名をクリックしてください。Syslogサーバーを設定していないと、Syslog設定に関連する事項は表示されません。イベントログの記録またはSyslogを無効にしたり、特定の電子メール受信者やトラップレシーバの通知を無効にすることもできます。

   注記： イベント設定の詳細を表示している場合、受信者またはレシーバを追加または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または削除するには、次のセクションを参照してください。

   - Syslogサーバーの識別, 180 ページ
   - 受信者, 174 ページ
   - トラップレシーバの設定, 175 ページ

グループ別通知の設定

選択手順（パス）：Configuration > Notification > Event Actions > By Group

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. 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。
   - イベントは**[Severity]**で選択し、1つまたは複数の重要度レベルを選択できます。イベントの重要度は変更できません。
   - イベントは**Category**別に選択し、あらかじめ定義された1つまたは複数のカテゴリのイベントを選択することができます。
2. **[Next]**をクリックしてイベントアクションを選択します。

   Logging（ログへの記録）（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。
3. **[Next]**をクリックして次のいずれかを実行します。
   - 前の画面で**[Logging]**を選択し、Syslogサーバを設定していない場合は、**[Configure Event Log**(イベントログの設定)**]**を選択します。
   - 前の画面で**[Logging]**を選択し、Syslogサーバーを設定した場合は、**[Event Log]**または**[Syslog]**を選択します。
   - 前の画面で**[Email Recipients]**を選択した場合は、設定する電子メール受信者を選択します。
   - 前の画面で**Trap Receivers**（トラップレシーバ）を選択した場合は、設定するトラップレシーバを選択します。
4. **[Next]**をクリックして通知パラメータを設定します。これらの設定フィールドでは、通知を送信する電子メールのパラメータを定義します。
   - **[Logging]**を設定する場合、**[Enable Notification]**（通知を有効化）または**[Disable Notification]**（通知を無効化）を選択します。
   - **Email Recipients**または**Trap Receivers**を設定している場合は、**Enable Notification**または**Disable Notification**を選択して通知パラメータを設定します。
5. **[Next]**をクリックすると保留中のアクションが表示されますので、次のいずれかを実行します。
   - **[Apply]**をクリックして変更内容を有効にします。
   - **[Cancel]**をクリックして前の設定に戻ります。

電子メール通知パラメータ：これらの設定フィールドで、イベントの通知を送信する電子メールのパラメータを設定します。通知パラメータにアクセスするには、受信者名または受信者名を選択します。

フィールド	説明
[Delay n 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 n]	通知は指定した間隔で繰り返し送信されます（デフォルトでは、状態が解消されるまで2分おきです）。
[**Up to n times**]（最大n回）または **[Until condition clears]**	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。 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。

注記： イベントをクリアするイベントを関連付けたイベントの通知パラメータを設定することもできます。

電子メール通知の設定

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サーバーおよびセカンダリDNSサーバー（オプション）のIPアドレス
- SMTP Server（SMTPサーバ）のIPアドレスかDNS名と、From Address（送信元アドレス）
- 最高4人までの受信者の電子メールアドレス
- **Recipients**（**受信者**）オプションの**To Address**（**宛先アドレス**）設定を使用すると、テキストベースの画面に電子メールを送信できます。

サーバー

選択手順（パス）： Configuration > Notification > E-mail > Server

この画面にはご使用のプライマリ/セカンダリDNSサーバーがリストされ、次のフィールドが表示されます。

Active Primary DNS Serverまたは**Active Secondary DNS Server**ページを選択して(**Configuration > Network > DNS > Configuration**から) DNSサーバーを設定します。

設定	説明
From Address（送信元アドレス）	Rack ATS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。 • IPアドレスがローカルSMTPサーバーとして指定されている場合は、*user@ [IP_address]*の形式を使用してください。 • DNSが設定され、DNS名がローカルSMTPサーバーとして指定されている場合は、*user@domain*の形式を使用してください。 **備考**：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確認します。
SMTP Server（SMTPサーバー）	ローカルSMTPサーバーのIPv4/IPv6アドレスまたはDNS名。 **備考**：この定義が必要なのは、SMTPサーバーが**Local**に設定されている場合のみです。
Port（ポート）	SMTPポート番号（デフォルトは25）。サポートされるポートには、25、465、587、2525、および5000 ~ 32768が含まれます。
Authentication（認証）	SMTPサーバーが認証を必要とする場合は、**Enable**を選択してください。 **ユーザー名、パスワード、パスワードの確認**：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SSL/TLSではありません。
Use SSL/TLS（SSL/TLSを使用）	暗号化を使用する場合に選択します。 • **Never**（**なし**）：SMTPサーバーは暗号化を要求せず、サポートもしません。 • **If Supported**（**サポートされている場合**）**:** SMTPサーバーはSTARTTLSをサポートしていることを通知しますが、接続を暗号化する必要はありません。STARTTLSコマンドは、通知が与えられた後に送信されます。 • **Always**（**常時**）：SMTPサーバーは、接続に対してSTARTTLSコマンドの送信を要求します。 • **Implicitly**（**暗黙的**）**:** SMTPサーバーは、暗号化を開始した接続のみを受け入れます。STARTTLSメッセージはサーバーに送信されません。
Require CA Root Certificate（CAルート証明書が必要）	所属組織のセキュリティポリシーでSSL/TLS接続の暗黙の信頼が許可されていない場合にのみ有効にしてください。これを有効にすると、有効なルートCA証明書をRack ATSに読み込み、暗号化された電子メールを送信する必要があります。
File Name（ファイル名）	このフィールドは、Rack ATSにインストールされているルートCA証明書と、ルートCA証明書が必要かどうかに依存します。

受信者

選択手順（パス）： Configuration > Notification > E-mail > Recipients

4人までの電子メール受信者を指定できます。**[Add Recipient]**（受信者を追加）をクリックするか、名前を選択して設定します。

設定	説明
電子メールの受信者	
Generation（生成）	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。
To Address（宛先アドレス）	受信者のユーザー名とドメイン名。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ルックアップをバイパスするには、電子メールのドメイン名の代わりに、IPアドレスを括弧で囲んで入力します（`jsmith@company.com`の代わりに`jsmith@[xxx.xxx.x.xxx]`を使用するなど）。DNSルックアップが正常に作動しない場合に役立ちます。
Format（形式）	**Long**形式には、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。**Short**形式ではイベントの説明のみが表示されます。
Language:	送信される電子メール通知の言語。インストールされている言語パックによって異なります（該当する場合）。
Server（サーバー）	電子メールのルーティング方法を次から1つ選択します。 • **Local:** これは、サイトローカルSMTPサーバーを介して行われます。この推奨設定では、サイトローカルSMTPサーバーを使用して電子メールを送信します。この設定を選択すると遅延やネットワークの停電を抑制でき、数時間にわたって電子メールの再送信が試行されます。[Local]設定を選択すると、ご使用のデバイスのSMTPサーバーへの転送を有効にして、転送された電子メールを受信するための電子メールの特別な外部アカウントも設定する必要があります。これらの変更を行う前に、SMTPサーバーの管理者にご確認ください。 • **Recipient:** 受信者のSMTPサーバーです。Rack ATSは、受信者の電子メールアドレスにMXレコードのルックアップを行い、それをSMTPサーバーとして使用します。電子メールの送信は1回のみのため、簡単に消失するおそれがあります。 • **Custom:** この設定により、各電子メール受信者に独自のサーバー設定が適用されます。これらの設定は、ローカルSMTPサーバの設定とは独立しています(**Configuration > Notification > E-mail > Server**で設定)。
カスタム電子メールサーバー設定	
From Address（送信元アドレス）:	Rack ATSが送信した電子メールメッセージの[From]フィールドの内容。 • 「user@ IP_address」（Local SMTP Server（ローカルSMTPサーバ）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） **備考**：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。
SMTP Server:	ローカルSMTPサーバーのIPv4/IPv6アドレスまたはDNS名。 **備考**：この定義が必要なのは、SMTPサーバーが**Local**に設定されている場合のみです。
Port（ポート）	SMTPポート番号（デフォルトは25）。サポートされるポートには、25、465、587、2525、および5000 ~ 32768が含まれます。
Authentication（認証）	SMTPサーバーで認証が必要な場合は、Enableを選択してください。
User Name, Password, and Confirm Password（ユーザー名、パスワード、パスワードの確認）	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SSL/TLSではありません。
Advanced	
Use SSL/TLS（SSL/TLSを使用）	暗号化を使用する場合に選択します。 • **Never（なし）:** SMTPサーバーでは暗号化は必要ありません。 • **If Supported（サポートされている場合）:** SMTPサーバーはSTARTTLSをサポートしていることを通知しますが、接続を暗号化する必要はありません。STARTTLSコマンドは、通知が与えられた後に送信されます。 • **Always（常時）:** SMTPサーバーは、接続に対してSTARTTLSコマンドの送信を要求します。 • **Implicitly（暗黙的）:** SMTPサーバーは、暗号化を開始した接続のみを受け入れます。STARTTLSメッセージはサーバーに送信されません。

設定	説明
Require CA Root Certificate（CAルート証明書が必要）	所属組織のセキュリティポリシーでSSL/TLS接続の暗黙の信頼が許可されていない場合にのみ有効にしてください。これを有効にすると、有効なルートCA証明書をRack ATSに読み込み、暗号化された電子メールを送信する必要があります。
File Name（ファイル名）	このフィールドは、Rack ATSにインストールされているルートCA証明書と、ルートCA証明書が必要かどうかに依存します。

SSL証明書

選択手順（パス）：Configuration > Notification > E-mail > SSL Certificates

セキュリティを強化するため、Rack ATSにメールのSSL/TLS証明書をロードします。ファイルの拡張子は.crtまたは.cerです。指定した時間に5つまでのファイルをロードできます。

インストールされると、証明書の詳細も表示されます。無効な証明書は、**File Name**（ファイル名）以外のすべてのフィールドが「n/a」と表示されます。

この画面で証明書を削除できます。この証明書への参照を削除するため、証明書を使用する電子メール受信者を手動で変更してください。

テスト

選択手順（パス）：Configuration > 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

Simple Network Management Protocol (SNMP)トラップを使用すると、重要なRack ATSイベントの通知を自動的に取得できます。ネットワーク上のデバイスの監視に役立つツールです。

トラップレシーバの設定

選択手順（パス）：Configuration > Notification > SNMP Traps > Trap Receivers

トラップレシーバは**[NMS IP/Host Name]**によって表示されます（NMSはNetwork Management Systemを意味します）。最大6つのトラップレシーバを設定できます。トラップレシーバを新たに設定するには、**Add Trap Receiver**（トラップレシーバの追加）をクリックします。トラップレシーバを編集（または削除）するには、そのIPアドレス/ホスト名を選択します。

Trap Generation（トラップ生成）: このトラップレシーバのトラップ生成を有効（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。

Language: ドロップダウンリストから言語を選択します。Web UIや他のトラップレシーバと異なる言語を選択できます。

[SNMPv1]または**[SNMPv3]**を選択してトラップタイプを指定します。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）個別に設定する必要があります。

SNMPv1: SNMPv1の設定。

- **Community Name（コミュニティ名）:** SNMPv1トラップがこのトラップレシーバに送信されるときに識別子として使用される名前。
- **Authenticate Traps（認証トラップ）:** 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］設定で識別された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よって生成されるトラップ）を受信します。

SNMPv3: SNMPv3の設定。

- **User Name:** このトラップレシーバのユーザープロファイルの識別子を選択します。

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[Configuring event actions]で設定した通知設定はすべてデフォルト値に設定されます。

SNMPトラップのテスト

選択手順（パス）： Configuration > Notification > SNMP Traps > Test

Last Test Result（前回のテスト結果）: 最新のSNMPトラップテストの結果。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。
- トラップレシーバ自体が有効になっている。
- **To**（宛先）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択します。トラップレシーバが設定されていない場合は、**Trap Receiver**設定画面(**snmp receiver**)へのリンクが表示されます。

全体システムの設定

このメニューには、デバイスID、日付と時刻、使用するRack ATS設定オプションのエクスポートとインポート、クイックリンク、トラブルシューティング用のデータ統合などの設定項目が含まれています。

IDの設定

選択手順（パス）： Configuration > General > Identification

Host Name Synchronization（ホスト名の同期）: ホスト名がシステム名と同期され、両方のフィールドが自動的に同じ値になります。

> **注記**： この機能を有効にすると、システム名の識別子に空白文字を含めることができなくなります（これはホスト名フィールドと同期されるためです）。

Name, Contact, and Location（名前、連絡先、場所）: Rack ATSおよびData Center ExpertのSNMPエージェントで使用される**Name**、**Contact**（デバイスの責任者）および**Location**（物理的な場所）を定義します。

これらのフィールドは、Rack ATSのSNMPエージェント内の**sysName**、**sysContact**、および**sysLocation**オブジェクト識別子(OID)によって使用されます。MIB-II OIDの詳細については、『PowerNet® SNMP *Management Information Base (MIB)*リファレンスガイド』を参照してください。このマニュアルはwww.se.comから入手できます。

リモート監視サービスにご登録いただくと、**Name**（名前）と**Location**（ロケーション）のフィールドからもデバイスを識別できるようになります。

System Message（システムメッセージ）: 定義されると、カスタムメッセージが画面のログに表示され、すべてのユーザーが見ることができます。

日付、時刻、および夏時間の設定

選択手順（パス）： Configuration > General > Date/Time > Mode

Rack ATSが使用する時間と日付を設定します。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。

Time Zone: タイムゾーンは、グリニッジ標準時（GMT）として知られる協定世界時（UTC）とご使用の地域との時差です。

Manual Mode：手動モードでは次のいずれかの操作を行います。

- Rack ATSの日付と時刻を入力します。
- **[Apply Local Computer Time]**（ローカルコンピュータの時刻を適用します）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/時刻の設定を適用します。

Synchronize with NTP Server（NTPサーバーとの同期）：NTP(Network Time Protocol)サーバーでRack ATSの日付と時刻を定義します。デフォルトでは、Data Center Expertサーバーのプライベート側にある任意のRack ATSは、Data Center ExpertをNTPサーバーとして使用して時刻の設定を取得します。

- **Override Manual NTP Settings（手動NTP設定を上書き）:** これを選択すると、他のソース（通常はDHCP）からのデータが、ここで設定したNTP設定よりも優先されます。
- **Primary NTP Server（プライマリNTPサーバー）**：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NTPサーバー）**：セカンダリサーバーが利用可能な場合に、セカンダリNTPサーバのIPアドレスまたはドメイン名を入力します。
- **Update Interval（更新間隔）:** 更新のためにRack ATSからNTPサーバにアクセスする頻度を時間単位で設定します。最小：1、最大：8760（1年）。
- **Update Using NTP Now（今すぐNTPを使用して更新）:** 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

選択手順（パス）： Configuration > General > Date /Time > Daylight Saving

夏時間（DST）は、デフォルトでは無効になっています。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を調整する場合、**[Start]**で指定した日付と時刻に達すると、システムが時計を1時間先に進めます。そして、**[End]**で指定した日付と時刻に達すると、時計が1時間戻ります。

- 常にローカルのDSTを月の4番目の特定曜日（第4日曜日など）に開始または終了する場合は、Fourth/Last（第4/最終）を選択します。その月に5番目の日曜日がある場合も、Fourth/Last（第4/最終）を選択してください。
- 常にローカルのDSTを月の4番目の特定曜日に開始または終了する場合は、その曜日が4回あっても5回あってもFifth/Last（第4/最終）を選択します。

設定ファイルを用いた設定の作成とインポート

選択手順（パス）：Configuration > General > User Config File

1つのRack ATSの設定を使用して別の設定を行います設定したRack ATSから設定ファイル(***config.ini***)を取得し、このファイルをカスタマイズ（IPアドレスの変更など）して、カスタマイズしたファイルを新しいRack ATS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]（ステータス）	アップロードの進行状況が表示されます。 • **No configuration file uploaded（設定ファイルがアップロードされていません）**：Rack ATSが*config.ini*ファイルで設定されていません。 • **Configuration file successfully uploaded（設定ファイルが正常にアップロードされました）**：Rack ATSが*config.ini*ファイルで設定されています。このメッセージを表示するには、ページを更新する必要がある場合があります。 **備考**：アップロードは、ファイルにエラーが含まれていても成功したと見なされますが、エラーはイベントログに入力されます。
Upload（アップロード）	カスタマイズされたファイルをブラウズし、アップロードして現在のRack ATSを独自の設定で使用できるようにします。
Download（ダウンロード）	*config.ini*ファイルはWebブラウザーからコンピューターに直接ダウンロードできます。

このファイルを1台のRack ATSにアップロードする代わりに、FTPまたはSCPスクリプトを使って複数のRack ATSユニットにエクスポートすることができます。

注記： 設定したRack ATSのファイルを取得およびカスタマイズするには、「環境設定値のエクスポート方法, 193 ページ」を参照してください。

クイックリンクの設定

選択手順（パス）： Configuration > General > Quick Links

インターフェイスの各ページの左下に表示されるURLリンクを表示し、変更します。

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。

- リンク1: APC Webサイトのホームページ
- リンク2: EcoStruxure™ ITに関する情報
- リンク3: IT配電機器の追加情報

ログの設定

Syslogサーバーの識別

選択手順（パス）： Configuration > Logs > Syslog > Servers

Add Server（サーバーの追加）をクリックして、新しいシステムログサーバーを設定します。

Syslog Server: IPv4/IPv6アドレスまたはホスト名を使用して、Rack ATSから送信されるSyslogメッセージを受信するサーバーを最大4台まで識別します。

Port: Rack ATSがSyslogメッセージの送信に使用するポート。システムログに割り当てられたデフォルトのUDPポートは514です。

Language: システムログメッセージの言語を選択します。（現時点では英語のみ）。

Protocol: UDPまたはTCPを選択します。

保存するには [**Apply**] を、保存せずに終了するには [**Cancel**] をクリックします。

システムログの設定

選択手順（パス）： Configuration > Logs > Syslog > Settings

Message Generation（メッセージ生成）: システムログを通知方法として設定してあるイベントのシステムログメッセージの生成とログ記録を有効にします。

Facility Code（機能コード）：Rack ATSのシステムログメッセージに割り当てられる機能コードを選択します（デフォルトではユーザー）。

> **注記**： **ユーザー**は、Rack ATSが送信するシステムログメッセージを最も適切に定義します。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（重要度マッピング）：このセクションでは、Rack ATSの各重要度レベルまたは環境イベントをシステムログの優先度に関連付けます。ローカルオプションには、**Critical（重大）**、**Warning（警告）**、**Informational（情報）**があります。このマッピングを変更する必要はありません。

- **Emergency:** システムを使用できません
- **Alert:** 直ちに対処する必要があります
- **Critical:** 重大な障害があります
- **Error:** エラー状態
- **Warning:** 警告状態
- **Notice:** 通常の状態ですが、多少の問題があります
- **Info:** 情報メッセージ
- **Debug:** デバッグレベルのメッセージ

以下は、**Local Priority**のデフォルト設定です。

- **Critical**（重大）は**Critical**（重大）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。

Syslogサーバーのテスト

選択手順（パス）： Configuration > Logs > Syslog > Test

[Syslog servers]ページ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。結果はすべての設定済みシステムログサーバーに送信されます。

テストメッセージに割り当てる重大度を設定してから、テストメッセージを定義します。イベントタイプ（APC、システム、デバイスなど）の次にコロン、スペース、イベントテキストを配置してメッセージを形成します。メッセージは最長で50文字にすることができます。

- 優先度(PRI):メッセージイベントに割り当てられるシステムログ優先度およびRack ATSが送信するメッセージの機能コード。
- ヘッダー：タイムスタンプおよびRack ATSのIPアドレス。
- メッセージ（MSG）部分：
  - イベントタイプは、**TAG**（タグ）フィールド、コロン、スペースの形式で指定します。
  - **CONTENT**（コンテンツ）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：`APC: Test Syslog`は有効です。

[Tests]タブ

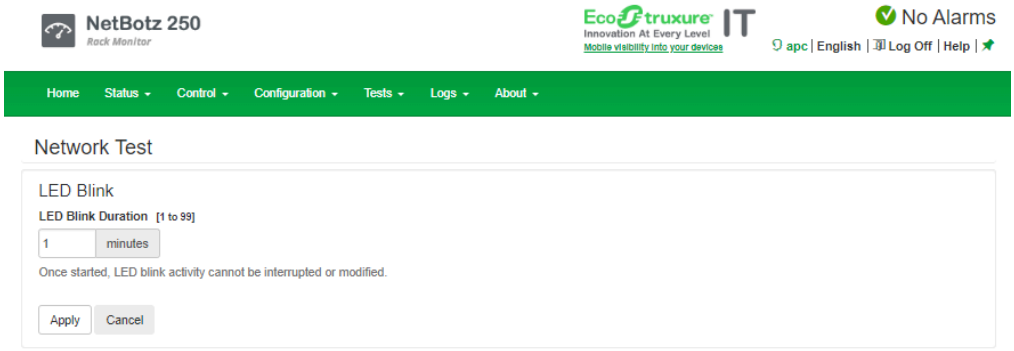
LCDライトの点滅設定

選択手順（パス）： Tests > ATS > LCD Blink

自分のRack ATSが見つからない場合は、**LCD Blink Duration**フィールドに分単位の数を入力し、[**Apply**]をクリックします。LCDディスプレイは指定した分数の間点滅します。

LEDライトの点滅設定

選択手順（パス）：Tests > Network > LED Blink



自分のRack ATSが見つからない場合は、**LED Blink Duration**フィールドに分単位の数を入力し、[**Apply**]をクリックします。ディスプレイ上の10/100/1000ステータスLEDライトが、指定された時間（分）点滅します。

[Logs]タブ

イベントログの表示と設定

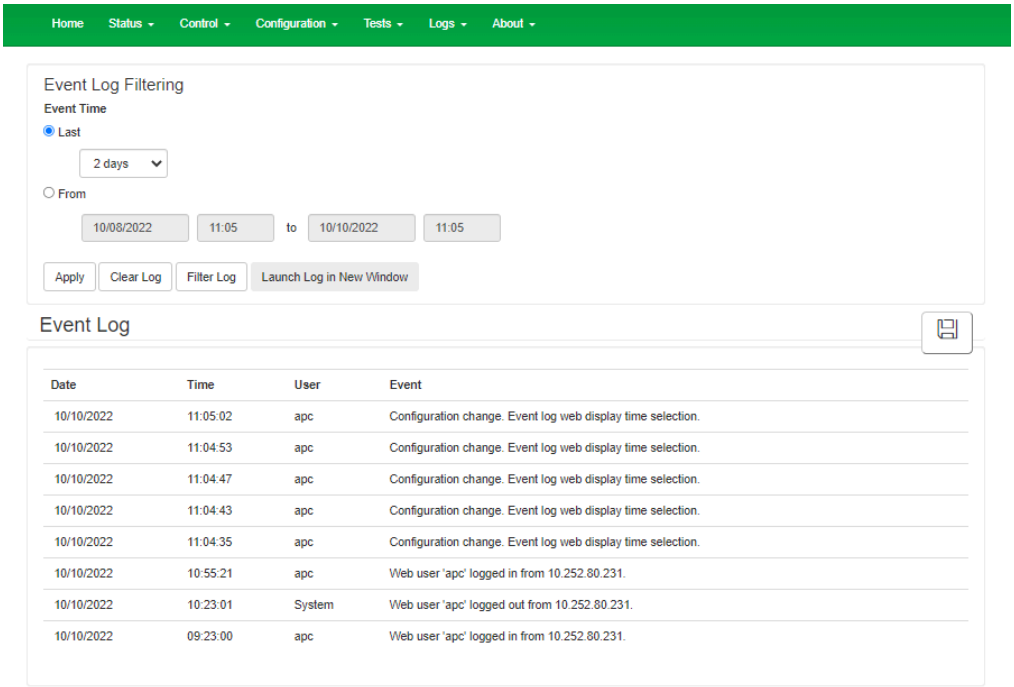
デフォルト設定では、イベントログには過去2日間に記録されたすべてのイベントが直近のものから表示されるようになっています。

さらに、ログではSNMP認証エラー以外のSNMPトラップを送信するイベントと、異常な内部システムイベントを記録します。

Local User Management画面(**Configuration > Security > Local Users > Management**で表示)では、イベントの色分けを有効にできます。

イベントログの表示

選択手順（パス）：Logs > Events > Log



ログをテキストファイルで開いたり、ログをディスクに保存するには、**[Event Log]**見出しと同じ行にあるフロッピーディスクをクリックします。

Webページでともにリストされるイベントを表示するには、**Launch Log in New Window**（新しいウィンドウでログを起動）をクリックします。

FTPまたはSecure CoPy (SCP)を使用して、イベントログを表示することもできます。「FTPまたはSCPを使用したログファイルの取得, 188 ページ」を参照してください。

Event Log Filtering: フィルタ処理を使用して、必要がない情報を除外します。

- ログを日時別にフィルタ処理するには、次の手順に従います。イベントをログに記録した時刻を指定するには、**[Last]**または**[From]**を使用します。(フィルタ設定は、Rack ATSが再起動するまで保存されます。)

- イベントの重要度またはカテゴリーでログをフィルタ処理するには：
  1. ［ **Filter Log** ］をクリックします。
  2. チェックボックスをオフにすると、表示されなくなります。
  3. ［ **Apply** ］をクリックします。**Event Log**ページの右上隅に表示されるテキストは、フィルタがアクティブであることを示します。フィルタは、クリアするか、Rack ATSが再起動するまで有効です。
  4. スーパーユーザーまたは管理者は、**[Save As Default]**をクリックして、当該のフィルタを全ユーザーに対する新しいデフォルトのログ表示として保存することができます。
- アクティブなフィルタを削除するには：
  1. **Filter Log**をクリックします。
  2. **Clear Filter (Show All)**（フィルタのクリア（すべて表示））をクリックします。

フィルタ処理の重要なポイント：

- 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。フィルタを適用すると、他のフィルタとは関係なく動作します。
- **Filter By Severity**リストで消去したイベントは、**Filter by Category**リストで選択されていても、フィルタリングされた**Event Log**には表示されません。
- 同様に、**Filter by Category**リストでクリアしたイベントは、フィルタリングされた**Event Log**には表示されません。

Clear Log: すべてのイベントを削除するには、 **Clear Log**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のを無効にするには、「通知の設定, 171 ページ」を参照してください。

逆引き

選択手順（パス）： Logs > Events > Reverse Lookup

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。

Reverse lookup（逆引き）はデフォルトでは無効です。DNSサーバーの設定が終わっていない、またはトラフィックが過大のためネットワークの機能が不良でない限り、この機能を有効にする必要はありません。

ログサイズの変更

選択手順（パス）：Logs > Events > Size

Event Log Size（イベントログのサイズ）: ログエントリの最大数を指定します(25 ~ 30000)。

注記： 最大サイズを指定するためにイベントログのサイズを変更すると、既存のログエントリはすべて削除されます。以降、ログが最大容量に達すると、データは古いものから削除されます。

ネットワークポート共有のイベントログとトラップ

ゲストユニットからのRack ATSイベントは、そのログに含めるためにホストユニットに送信されます。ログエントリには、イベントが発生したユニットのDisplay IDが含まれます。これらのイベントは、ホストユニットからのローカルイベントと同じ処理になります。従って、アラーム、SNMPトラップ、電子メール、Syslogなどは、Rack イベントとグループ内のすべてのRack ATS からのアラームをサポートします。
イベントログの例：`Rack ATS 4: Device low load.`

注記： システムイベントは、ホストRack ATSのみに関して記録されます。ゲストRack ATSユニットからのシステムイベントは、ホストRack には記録されません。

データログの表示と設定

データログを使用すると、Rack ATSの測定値、Rack ATSへの電源入力、およびRack ATSの周囲温度を表示できます。

データログの表示および容量変更の手順は、**イベント**の代わりに**データ**の下にあるメニューオプションを使用することを除き、イベントログと同じです。

注記： データログには、NPSゲストユニットからの情報は表示されません。

Log

選択手順（パス）： Logs > Data > Log

View the log by date or time（日時別にログを表示）: Lastまたは**From**を使用してデータがログに記録された時刻を定義し、［**Apply**］をクリックして変更を保存します。（このフィルタ設定はユニットが次に再起動するまで保存されます。）

Clear Data Log（データログの消去）: データログレコードをすべて削除します。削除されたデータログレコードは取得できなくなります。

Launch Log in New Window（ログを新しいウィンドウで起動）: 別のWebページでログを表示します。

［**Apply**］をクリックして変更を保存するか、［**Cancel**］をクリックして破棄します。

グラフ表示

選択手順（パス）： Logs > Data > Graphing

データログのグラフ表示は、記録されたデータのグラフ表示を提供し、既存のデータログ機能を拡張します。グラフ表示の拡張機能でデータがどのように表示され、どのように効率よく実行されるかは、ご使用のコンピュータのハードウェア、コンピュータのオペレーティングシステム、およびユニットのインターフェイスにアクセスするために使用するWebブラウザによって異なります。

> **注記**： グラフ作成機能を使用するには、ブラウザでJavaScript®を有効にする必要があります。または、FTPかSCPを使用してデータログをダウンロードし、情報をスプレッドシートアプリケーションにコピーすることもできます。

Graph Data（グラフデータ）: リストをスクロールして、グラフを作成するデータを選択します。［ **Apply** ］をクリックして変更内容を保存します。

Filter the graph by date and time（日付と時刻でグラフをフィルタ）: イベントがログに記録された日時を指定するには、**Last**または**From**を使用します。［ **Apply** ］をクリックして変更内容を保存します。(フィルタ設定は、Rack ATSが再起動するまで保存されます。)

Launch Graph in New Window（グラフを新しいウィンドウで開く）: 別のWebページでグラフを開くと、より大きく詳細なビューが表示されます。

変更を保存するには［ **Apply** ］を、破棄するには［ **Cancel** ］をクリックします。

ログ記録の間隔の設定

選択手順（パス）： Logs > Data > Interval

Log Interval（ログの間隔）設定で、データの検索とデータログへの保存を行う頻度を定義します。**[Apply]**をクリックすると、可能な保管日数が再計算され、画面上部に表示されます。ログがいっぱいになると、古いエントリから削除されます。

> **注記**： 間隔はデータの記録頻度を指定するため、間隔を小さくするとデータがより頻繁に記録され、エントリが保持される期間は短くなります。

ローテーションの設定

選択手順（パス）：Logs > Data > Rotation

ローテーション機能によって、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。このオプションで、パスワード保護やその他のパラメータを設定します。

- **FTP Server（FTPサーバー）:** ファイルが存在するサーバーのIPアドレスまたはホスト名。
- **User Name, Password（ユーザー名、パスワード）:** 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とパスワード。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。
- **File Path（ファイルパス）:** レポジトリファイルへのパス。
- **Filename（ファイル名）:** レポジトリファイルの（ASCIIテキストファイル形式の）名前。例：*datalog.txt*。新しいデータはこのファイルに追加され、上書きはされません。
- **Unique Filename（固有のファイル名）:** このチェックボックスを選択してログを*mmddyyyy_<filename>.txt*として保存します。*<filename>*は、上の**Filename**フィールドで指定したファイル名です。新しいデータはファイルに追加されますが、1日ごとに独自のファイルが生成されます。
- **hours between uploads（アップロード間隔）:** データのアップロード間隔（最大24時間）。
- **Upon failure, try uploading every *n* minutes**（失敗した場合は、n分ごとにアップロードを試す）：アップロード失敗後、次にファイルにデータをアップロードするまでの待ち時間（分単位）。
  - **Delay *n* Maximum Attempts（最大再試行回数 n）:** 最初のアップロード失敗後のアップロード試行回数の最大値です。
  - **Until upload succeeds（アップロードが成功するまで）:** 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。

［**Apply**（**適用**）］をクリックするとこれらの設定が保存されます。［**Cancel**（**キャンセル**）］をクリックする変更内容は破棄され、［**Upload Now**（**今すぐアップロード**）］をクリックすると、ログデータが切り替わります。

データログサイズの指定

選択手順（パス）：Logs > Data > Size

Data Log Size：ログエントリの最大数を指定(25-1,000)を指定します。

> **注記**： 最大ログサイズを変更すると、それまでに記録されていたエントリはすべて削除されます。以降、ログが最大容量に達すると、データは古いものから削除されます。

ファイアウォールのログ

選択手順（パス）：Logs > Firewall

ファイアウォールポリシーを作成すると、ファイアウォールイベントはこのログに記録されます。ログ記録された情報は、カスタマサービスチームが問題を解決する場合に役立ちます。ログエントリには、トラフィックおよびルールの動作（許可または廃棄）に関する情報が含まれます。ここに記録されると、これらのイベントはメインのイベントログには記録されません。

ファイアウォールログには、最近のイベントから最大50個まで記録されます。ファイアウォールログは、管理インターフェイスを再起動するとクリアされます。

ファイアウォールポリシーの詳細については、「ファイアウォールメニュー, 153 ページ」を参照してください。

FTPまたはSCPを使用したログファイルの取得

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。

- ファイルには、最近保存されたすべてのイベントが報告されます。ログが削除された、または最大サイズに達したため切り捨てられた場合、その削除または切り捨てられた情報はファイルに含まれません。
- このファイルには、イベントログまたは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 ATSRack PDURack Monitor 250**MDCの、およびの値とIPアドレス
  - 記録した各イベントのための固有の**イベントコード** (*event.txt*ファイルのみ)

    注記： Rack ATSは、ログエントリのために4桁の年表記を使用します。4桁の日付表記を表示するには、スプレッドシートのアプリケーションで4桁の日付形式を選択する必要がある場合がありますす。

ご利用の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、ログファイルを取得するためにSCPを使ってください。ご利用の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、ログファイルを取得するためにFTPを使ってください。

注記： デフォルトでは、FTPは無効で、SCP（SSH経由）は有効になっています。

必要なセキュリティタイプを設定するために利用可能なセキュリティプロトコルと方法については、www.se.com/ww/en/downloadにて*Network Management Card 3 Security Handbook* (SPD_CCON-BDYD7K_EN)を参照してください。ウェブサイトからユーザーマニュアルを表示およびダウンロードするには、あなたのロケーションを選択する必要があります。

SCPを使用したファイルの取得

*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 -c <cipher> username@hostname_or_ip_address:event.txt
./event.txt
```

SCPを使用して*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 -c <cipher> username@hostname_or_ip_address:data.txt ./data.
txt
```

注記：

- このSCPコマンドは、OpenSSH用のものです。使用されるSSHツールによってはコマンドが異なる場合があります。
- OpenSSHを使用する場合、<*cipher*>はaes256-cbcまたは3des-cbcのいずれかになることができます。

FTPを使用したevent.txtまたはdata.txtファイルの取得

1. コマンドプロンプトで`ftp`とRack ATSのIPアドレスを入力して、ENTERキーを押します。**FTPサーバー**オプション(**管理**タブの**ネットワーク**メニューで設定されるオプション)のための**ポート**の設定がデフォルト値（**21番**）より変更された場合、FTPコマンドに非デフォルト値を使用する必要があります。Windows FTPクライアントの場合は、スペースを含む次のコマンドを使用します。（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スペースではなくコロンを使用する必要があります。）

   ```
   ftp>open ip_address port_number
   ```

   Configuration > Network > Port > FTP Serverの下でデフォルト値以外のポートを設定して、FTPサーバーのセキュリティを強化できます。5001 ~ 32768のいずれか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**（ユーザー名）と**Password**（パスワード）（大文字/小文字の区別あり）入力してログオンします。管理者の場合、**User Name**（ユーザー名）と**Password**（パスワード）のデフォルト値はそれぞれ**apc**です。デバイスユーザーの場合、User Name（ユーザー名）は**device**、**Password**（パスワード）は**apc**がそれぞれデフォルト値になっています。

3. `get`コマンドを使用して、ログのテキスト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`を入力します。

ログファイルをUSBフラッシュドライブにダウンロード

1. USBフラッシュドライブをRack ATSのディスプレイインターフェイスのUSBポートに挿入します。転送を開始する前に、USBドライブがFAT32でフォーマットされているか確認してください。
2. ディスプレイ画面で**Log to Flash**までスクロールし、**Select**ボタンを押します。
3. **Select**ボタンをもう一度押して、ログファイルをフラッシュドライブにエクスポートします。

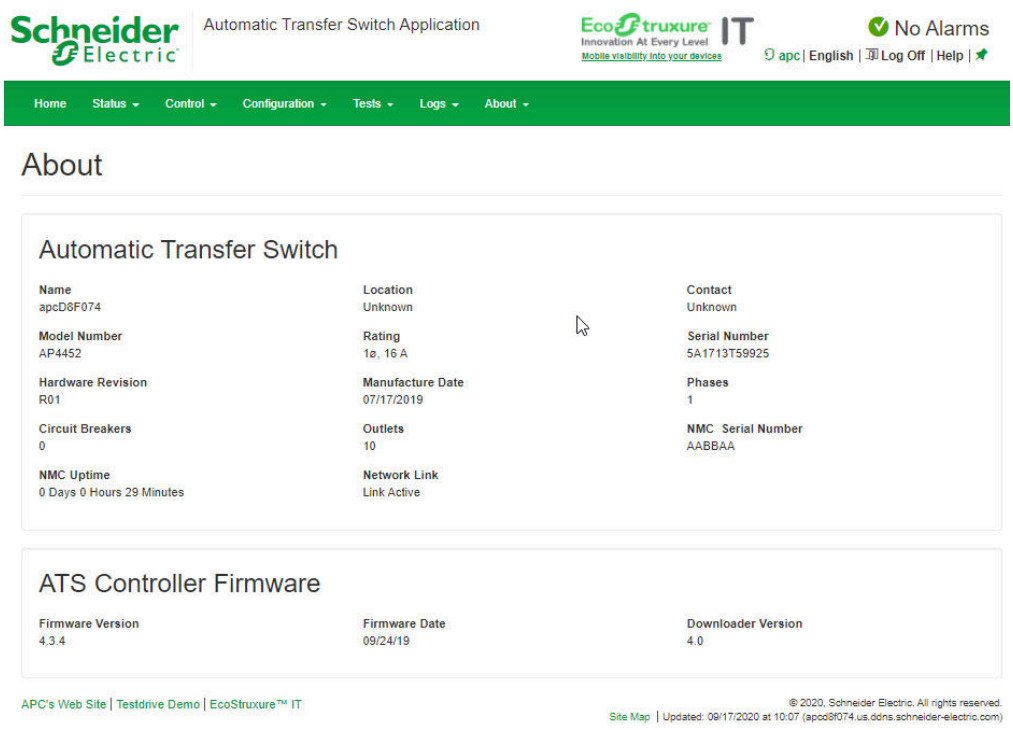
ダウンロード処理中はいつでも**Select**ボタンを押して、ダウンロードを中止することができます。

注記： Rack ATSにdebug.txtファイルまたはdump.txtファイルが存在しない場合、USBフラッシュドライブにダウンロードできません。これらのファイルは、予期しないシステムクラッシュまたはNetwork Management Card(NMC)のリセット後にのみ作成されます。debug.txtおよびdump.txtファイルは、テクニカルサポートの目的でのみ使用されます。

[About]タブ

Rack ATSについて

パス：**About > ATS**



ハードウェアの情報は、Rac ATSで問題が生じた場合、APCのカスタマーサポートがトラブルシューティングする際に役立ちます。シリアル番号およびMACアドレスは、ラックPDU本体にも表記されています。

Management Uptimeとは、ネットワーク管理インターフェイスの連続稼動時間です。

ネットワークについて

選択手順（パス）： About > Network

アプリケーションモジュール、APC OS（AOS）、APCブートモニタの情報には、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。これらの情報はトラブルシューティングに役立ちます。また、Webサイト(www.se.com)からアップデートをダウンロードする必要があるかどうかもチェックできます。

サポートリソース

選択手順（パス）： About > Support

このページには、複数のサポートリソースへのリンクが記載されています。

- **Knowledge Base（ナレッジベース）:** Schneider Electric WebサイトのFAQへの直接リンクです。
- **会社連絡先情報**：Schneider Electricが提供する複数のサポートサービスへの電話番号を提供します。
- **ソフトウェアおよびファームウェアのダウンロード**：ご使用の製品のソフトウェアアップグレードをダウンロードできます。

テクニカルサポートのデバッグ情報のダウンロード：このオプションを使用すると、このインターフェイスのさまざまなデータを、トラブルシューティング目的やカスタマサポート用に単一のZIPファイルにまとめることができます。このようなデータには、イベントログとデータログ、設定ファイル、複雑なデバッグ情報が含まれます。[**Generate Logs**]（ログの生成）をクリックしてファイルを作成し、[**Download**]をクリックしてダウンロードします。ZIPファイルを表示するか保存するかを尋ねられます。

環境設定値のエクスポート方法

手順の概要

スーパーユーザー/管理者は、Rack ATSの.iniファイルを取得し、別のRack ATSまたは複数のRack ATS Unitsにエクスポートできます。次の手順に従ってください。詳細に関しては、後続セクションを参照してください。

1. 必要な設定でRack ATSの設定を行い、そのRack ATSから.iniファイルを取得します。
2. 必要に応じて.iniファイルを他のデバイスにアップロードする前に、任意のテキストエディタを使って編集することができます。セクション間でデータ項目を移動することはできません。セミコロン(;)で始まる行は処理されません。
3. Rack ATSでサポートされているファイル転送プロトコルを使用して、コピーを他の（1つまたは複数）のデバイスに転送します。複数のRack ATS Unitsへの転送には、FTPまたはSCPスクリプトを使用するか、.iniファイルユーティリティを使用します。各受信ユニットは、このファイルを使用して独自の設定を再構成してから、このファイルを削除します。

   注記： FTPはデフォルトでは無効になっています。必要な場合は、**Configuration > Network > FTP Server**の順に選択して、FTPを有効化します。

   注記： config.iniを使用したユーザーの管理：config.iniを使用してユーザーを管理することはできなくなりました。ユーザーは、別の.csfファイルを使用して管理できるようになりました。詳細な情報については、FA156117のFAQ記事を参照してください。「How can I mass configure a Network Management Card (NMC) or NMC embedded product?（NMCまたはNMC埋め込み製品を一括設定するには？）」を参照してください。FAQ記事を見つけるには、www.se.comへ進み、あなたのロケーションを選択してください。次に**サポート > 文書とソフトウェアのダウンロード**を選択して、検索バーに記事のタイトルまたは番号を入力します。

.iniファイルの内容

Rack ATSから取得したconfig.iniファイルに含まれる内容は次のとおりです。

- セクション見出しとキーワード（ファイル取得元の特定のデバイスでサポートされているもののみ）：**セクション見出し**は、括弧([ ])で囲まれたカテゴリ名です。各セクション見出しの下の**キーワード**は、特定のRack ATS設定を記述するラベルです。各キーワードの後には、等記号（ = ）と値（デフォルト値または設定した値）が続きます。
- `Override`キーワード：このキーワードは、デフォルト値を使用して、1つまたは複数のキーワードとそのデバイス固有の値のエクスポートを防ぎます。例えば、`[NetworkTCP/IP]`セクションでは、`Override`のデフォルト値 (Rack ATSのMACアドレス)により、`SystemIP`、`SubnetMask`、`DefaultGateway`および`BootMode`の値のエクスポートがブロックされます。

.iniとネットワークポートの共有

.ini環境設定ユーティリティでは、グループ内のすべてのデバイスの値を取得および設定できます。下位互換性を維持するため、ホストRack ATSは常に"ATS_A"として指定されています。ゲストRack ATSユニットは、ディスプレイIDに基づいて、ATS_Zまで昇順で"ATS_B"、"ATS_C"、"ATS_D"と指定されます。その後、さらにPDUをATS_AA、最大ATS_FFに指定します。従って、"ATS_A"は必ずしもディスプレイID 1と相関するわけではありません。

注記： Rack ATSグループ内には可能な多数の設定値があるため、INIファイルの処理には非常に時間がかかる場合があります。たとえば、すべての値が変更された4台のRack ATSグループの処理は、30分かかることがあります。

詳細手順

.iniファイルの取得

可能であれば、Rack ATSのインターフェイスを使用して、エクスポートする設定で構成してください。(直接に.iniファイルを編集する場合、エラーが発生する恐れがあります。)

次に、FTP、SCP、またはWeb UIを介して、設定済みのRack ATSから*config.ini*を取得します。

FTPを使用するには：

1. IPアドレスを使って、Rack ATSへの接続を確立します。

   ```
   ftp> open ip_address
   ```

2. スーパーユーザー/管理者のユーザー名とパスワードを使用してログオンします。
3. *Rack ATS*Rack PDUの設定値を含むファイルを取得します。

   ```
   ftp> get config.ini
   ```

   このファイルは、FTPを起動したフォルダに書き込まれます。

   環境設定値を複数のRack ATS Unitsにエクスポートする方法については、FA156117のFAQ記事：「*How can I mass configure a Network Management Card (NMC) or NMC embedded product?* (*NMC*または*NMC*埋め込み製品を一括設定するには？) を参照してください。FAQ記事を見つけるには、www.se.comの検索バーに記事のタイトルまたは番号を入力します。結果のページで、**Faq**を選択して、検索結果をFAQ記事のみに絞り込みます。

SCPを使用するには：

次のコマンドを使用します。

```
scp -c <ciper> username@hostname_or_ip_address:config.ini
./config.ini
```

次に正しいパスワードを入力します。

注記：

- このSCPコマンドはOpenSSH用のものです。使用されるSSHツールによってはコマンドが異なる場合があります。
- OpenSSHを使用する場合、*<cipher>*はaes256-cbcまたは3des-cbcのいずれかになることができます。Aes256の方が安全です。

Web UIを使用するには：

Configuration > General > User Config Fileに移動し、**Download**を選択します。

.iniファイルの編集

他のRack ATS ユニットに転送する前に、ファイルを慎重に編集してください。

1. 変更にはテキストエディタを使用します。
   - 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。
   - 受け入れ側のRack ATS ユニットがNetwork Time Protocolサーバーにアクセスできる場合は、システム時刻を最も正確にエクスポートできるように、`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、各コメント行をセミコロン (;) で開始します。
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。**

1台のRack ATSにファイルを転送する

.iniファイルを別のRack ATSに転送するには、次のいずれかの操作を行います。

- 受け入れ側のRack ATSのWeb UIから、**[Configuration] > [General] > [User Config File]**を選択します。ファイルへの完全なパスを入力するか、または [参照] ボタンを押してご使用のローカルPCのファイルを指定します。
- Rack ATS ユニットでサポートされているいずれかのファイル転送プロトコル(FTP、FTP Client、SCP、TFTP)を使用します。以下にFTPを使用する例を示します。
  1. 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 ATSにログインします。

     ```
     ftp> open ip_address
     ```
  2. カスタマイズした.iniファイルのコピーを、受け手側のRack ATS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 ATS Unitsにファイルを転送します。

.iniファイルを複数のRack ATS Unitsに転送するには、次のいずれかの操作を行います。

- FTPまたはSCPを使用しますが、ファイルを単一のRack ATSにエクスポートする手順を繰り返すスクリプトを作成します。

- バッチ処理ファイルと.iniファイルユーティリティを使用します。

  バッチファイルを作成してユーティリティを使用するには、FA156117のFAQ記事を参照してください。「*How can I mass configure a Network Management Card (NMC) or NMC embedded product?*（*NMC*または*NMC*埋め込み製品を一括設定するには？）」を参照してください。FAQ記事を見つけるには、www.se.comの検索バーに記事のタイトルまたは番号を入力します。結果のページでは、**Faq**を選択して検索結果をFAQ記事のみに絞り込みます。

イベントのアップロードとエラーメッセージ

イベントとそのエラーメッセージ

受け入れ側のRack ATSが.iniファイルを使用して設定の更新を完了すると、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、受信側のRack ATSによるアップロードは成功し、追加のイベントテキストでエラーが示されます。

イベントテキスト	説明
`Configuration file warning: Invalid keyword on line number. Configuration file warning: Invalid value on line` *number.*	無効なキーワードまたは値を持つ行は無視されます。
`Configuration file warning: 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。
`Configuration file warning: Keyword found outside of a section on line` *number.*	ファイルの先頭に入力されたキーワード(つまり、セクション見出しの前)は無視されます。
`Configuration file warning: 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ファイルは、そのダウンロード元のRack ATSの設定を含めるために正しく検出されていなければなりません。Rack ATS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、キーワードと値の代わりにメッセージが含まれます。例えば次のようになります。

`Rack ATS not discovered`

.iniファイルのインポートでRack ATSの設定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を無視してください。

上書き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値のエクスポート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。どの値がオーバーライドされるかについては、「.iniファイルの内容, 193 ページ」を参照してください。

上書きされた値はデバイス固有であり、他のRack ATS units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。

関連のトピック

Windowsオペレーティングシステムでは、.iniファイルを転送するかわりに、デバイスIP設定ウィザードを使用して、Rack ATSの基本的なTCP/IP設定を更新し、そのユーザーインターフェイスを介して他の設定を行うことができます。デバイスIP設定ウィザードのダウンロードとインストール方法については、「デバイスIP設定ユーティリティ, 20 ページ」を参照してください。

トラブルシューティング

アクセスに関する問題

問題が解決されない場合、または本章に説明が記載されていない場合、カスタマケアwww.se.comにお問い合わせください。

問題	対処方法
ネットワークポートシェアリングホストが新しいファームウェアにアップデートされた後、ゲストのRack ATSユニットで「ファームウェアバージョンが一致しません」というアラームが表示されます。	これは、指定された時間にホストユニットによって自動的に解決されます。イベントは以下の順で記録されます。「Remote RATS 2 (SN: xxxxxxxxxxx) firmware version does not match. (リモートRATS 2 (SN: xxxxxxxxxxx) のファームウェアバージョンが一致しません。)」 > 「Guest RATS firmware download started. (ゲストRATSファームウェアのダウンロードが開始されました。)」 > 「Guest RATS firmware download completed. (ゲストRATSファームウェアのダウンロードが完了しました。)」 > 「Remote RATS 2 (SN: xxxxxxxxxxx) firmware version alarm has been cleared. (リモートRATS 2 (SN: xxxxxxxxxxx)もファームウェアバージョンアラームが解除されました。)」 > 「Remote RATS 2 (SN: xxxxxxxxxxx) communication established. (リモートRATS 2 (SN: xxxxxxxxxxx)の通信が確立されました。)」
Rack ATSに対してpingが実行できません。	Rack ATSユニットのステータスLEDが緑色の場合は、Rack ATSと同じネットワークセグメントにある別のノードに対してpingを試行します。これが失敗した場合、Rack ATSに問題はありません。ステータスLEDが緑色以外の場合、またはpingテストが成功した場合、次の事項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 ATSとNMSのIPアドレスを確認します。 • NMSがRack ATS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 ATS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。
通信ポートをターミナルプログラムを通して指定できません。	ターミナルプログラムを使用してRack ATSを設定する前に、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。
シリアル接続を介してCLIにアクセスできません。	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を試します。
CLIにリモートアクセスができません。	• 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。スーパーユーザーまたは管理者がこれらのアクセス方法を有効かすることができます。デフォルトでは、FTPは無効、SSHは有効になっています。SSHとTelnetは、個別に有効かまたは無効化することができます。 • SSHの場合、Rack ATSがホストキーを作成中である可能性があります。ラックPDUはこのホストキーを作成するのに1分ほどかかることがあります。その間SSHにはアクセスできません。
Web UIにアクセスできません。	• HTTPまたはHTTPSアクセスが有効になっていることを確認します。 • 正しいURLを指定していることを確認します。これはRack ATS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。これには、URLの先頭に**http**ではなく**https**が必要です。 • Rack ATSにpingを実行して応答があるかどうかを確認します。 • Rack ATSでサポートされているウェブブラウザを使用していることを確認します。Webユーザーインターフェイス, 124 ページを参照してください。 • Rack ATSが再起動したばかりでSSL/TLSセキュリティが設定中である場合は、Rack ATSがサーバー証明書を生成中である可能性があります。Rack ATSはこの証明書を作成するのに1分ほどかかることがあります。その間SSL/TLSサーバーにはアクセスできません。
ネットワークポートシェアリング (NPS) を使用して通信できません。	• ネットワークポートシェアリングに通信問題がある場合、最大32台のユニット間のネットワークケーブルの全長が10メートル以下であることを確認してください。 • ネットワークポートシェアリングを使用していて、グループ内で1つまたは複数のユニットを見ることができない場合、グループ内のすべてのユニットが同じファームウェアリビジョンを使用していることを確認します。ゲストRack ATSユニットはホストからファームウェアのアップデートを受け取る必要がありますが、ホストのファームウェアリビジョンにまったく応答しないと思われるユニットを手動でアップデートすると、問題が解決します。適切なファームウェアリビジョンは、Schneider Electricのウェブサイト**www.se.com**からダウンロードできます。

SNMPの問題

問題	対処方法
GETを実行できない	• 読み取りアクセス（GET）のコミュニティ名（SNMPv1）またはユーザープロファイル設定（SNMPv3）を確認します。 • CLIまたはWeb UIからNMSにアクセスできることを確認します。 「SNMPオプション, 165 ページ」を参照してください。
SETを実行できない	• SNMPが有効になっているか確認します。SNMPv1とSNMPv3は、デフォルトでは無効になっています。 • 読み取り/書き込み権（SET）のコミュニティ名（SNMPv1）またはユーザプロファイル設定（SNMPv3）を確認します。 • CLIまたはWeb UIを使用して、NMSに書き込み(SET)アクセス権があること(SNMPv1)、またはNMSがアクセス制御リストを通してターゲットIPアドレスへのアクセス権が許可されていること(SNMPv3)を確認します。「SNMPオプション, 165 ページ」を参照してください。
NMSでトラップを受信できない	• NMSに対するトラップの種類（SNMPv1もしくはSNMPv3）がトラップレシーバとして正しく設定されているかを確認します。 • SNMP v1の場合、**mconfigTrapReceiverTable**のMIB OIDに対するクエリを行い、NMSのIPアドレスが一覧に正しく入力されているかと、このNMSに指定されているコミュニティ名が一覧内のコミュニティ名と一致しているかを確認します。いずれかが正しくない場合は、**mconfigTrapReceiverTable** OIDにSETを実行するか、またはCLIやWeb UIを使用してトラップレシーバの設定を修正します。 • SNMPv3の場合、NMSのユーザープロファイル設定を確認し、トラップテストを実行します。プロファイルおよびトラップテストの詳細については、「SNMPオプション, 165 ページ」、「通知の設定, 171 ページ」、「SNMPトラップ, 175 ページ」を参照してください。
NMSが受信したトラップを識別できない	トラップがアラーム/トラップデータベースと正しく統合されているかどうかについてはNMSのマニュアルを参照してください。

ワールドワイドカスタマーサポート

この製品のサポートは、www.se.comからご利用いただけます。

ソースコードの著作権に関する注意

cryptlibはDigital Data Security New Zealand Ltdの著作物です（1998年）。

Copyright © 1990, 1993, 1994 The Regents of the University of California. 版権所有

このコードはマイク・オルソン氏によってカリフォルニア州立大学バークレー校に寄贈されたソフトウェアに由来しています。

以下の条件を満たせば、プログラム修正の有無にかかわらず、ソース形式またはバイナリ形式での再配布と使用が許されます。

1. ソースコードを再配布する場合、上記の著作権表記、この条件リスト、下記の否認文をファイルに含める必要があります。
2. バイナリ形式で再配布する場合は、上記の著作権表記、この条件リスト、下記の否認文を、配布するマニュアルおよび / または他の資料などに転記する必要があります。
3. バイナリ形式で再配布する場合は、上記の著作権表記、この条件リスト、下記の否認文を、配布するマニュアルおよび / または他の資料などに転記する必要があります。
4. この大学の名称またはその寄贈者の名前のいずれも、事前の書面で特定の許可を得ることなく、このソフトウェアに由来する製品の支持または販売促進のために使用することはできません。

このソフトウェアは著作権者および寄贈者により「現状のまま」提供されており、商品価値や目的への適合性に関する黙示的な保証も含め、またこれに限定されず、いかなる明示的または黙示的な保証も否認されています。契約の解釈、厳密な責任の解釈、または不法行為（不注意またはその他の理由を含め）の解釈など、責任のあらゆる解釈を含めて、また損害の可能性を示唆された場合も含めて、あらゆる状況において、著作権者またはその配布者は、このソフトウェアの利用によって生じた直接的な損害、間接的な損害、偶発的な損害、特殊な損害、典型的な損害、付帯的な損害（代替品またはサービスの調達費、設備の使用不能による損失、データ喪失、利益の損失、業務の停止を含めて、またこれに制限されず）に対して責任を負いません。

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+33 (0) 1 41 29 70 00

www.se.com

規格、仕様、設計はその時々で変更されるため、この出版物に含まれる情報は必ず確認を取ってください。

© 2025 Schneider Electric. 著作権保有。

990-91718C-018