Dominion SX II

管理者ガイド
2.0.0

DSX2-v2.0.0.-0A-E
2015 年 8 月
255-60-0005-00

FCC 情報

この装置は、FCC 規則のパート 15 に定められたクラス A デジタル装置に関する規制要件に基づき試験が実施され、その適合が認証されています。これらの規制要件は、商業環境において機器を使用する際、有害な干渉に対する妥当な保護を提供するために設けられています。この機器は、無線周波数エネルギーを生成かつ利用すると共に、放射することもあります。取扱説明書に従って設置および使用が行われない場合は、無線通信に有害な干渉を引き起こす恐れがあります。この機器を住宅地で利用すると有害な干渉を引き起こす場合もあります。

VCCI 情報 (日本)

この装置は, クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Raritan は、事故、災害、誤用、乱用、本製品の Raritan 製品以外への改良が起因する、または Raritan が適切にコントロールできないような状況下、もしくは通常の操作以外で発生した本製品への損傷に対して一切責任を負いません。

本製品に付属されている電源ケーブルは、本製品でのみ使用してください。

目次

CS03 Certification (証明書) - DSX2-16 および DSX2-48

Raritan 社の製品を安全にご利用いただき、生死にかかわる傷害や起こりうる破損の危険性を避けるために、以下のことにご注意ください。

- 製品の構成には、2 線式の電源コードは使用しないでください。
- コンピュータやモニタの AC 電源コンセントの極性と設置が正しいことを確認してください。
- コンピュータとモニタの両方とも、接地されている電源コンセントのみを使用してください。
- バックアップ用の UPS を使用している場合、コンピュータ、モニタ、その他の装置には電源コンセントから電源を供給しないでください。

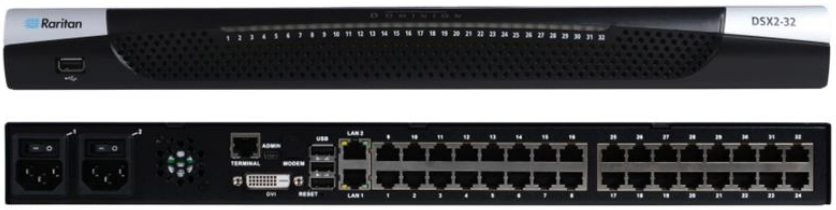
注意:この装置は適用できるカナダ産業省用端末装置技術仕様に合致しています。このことは登録番号によって確認できます。登録番号の前にある IC の略語は、登録が準拠の宣言に基づいて行われたことを意味し、カナダ産業省技術仕様に適合していることを示しています。これはカナダ産業省が認可したことを意味するものではありません。

注意:この端末装置の呼び鈴等価数(REN) は 01 です。REN は各端末装置につけられ、最大で何台の端末が電話線インタフェースに接続できるかを示しています。インタフェースの終端は種々のデバイスの組み合わせが可能ですが、ただすべてのデバイスの REN の合計が 5 を超えないという制約を守る必要があります。

AVIS:

AVIS:

Ch 1　　機能と利点



次世代コンソール サーバ

Raritan の次世代シリアル コンソール サーバ

Dominion SX II は Raritan の次世代コンソール サーバ（端末サーバとしても知られています）で、IT とネットワークの管理者にシリアルのデバイスにいつでもどこでも安全な IP アクセスと制御を提供しています。　新製品 SX II はこの市場において最も強力で、安全で、信頼性が高く、使いやすく、管理しやすい serial-over-IP （IP 経由シリアル）コンソールです。　SX II はネットワークデバイス、サーバ、PDU、電話通信とその他のシリアルデバイスに便利で生産的なアクセスを提供しています。

シリアル コンソールにおける 10 年の経験

10 年以上に亘って、何千人もの顧客が何十万代のシリアル デバイスのアクセスと制御に第 1 世代の Dominion SX に信頼を置いて使用し、総作動時間は 5 億時間を超えています。SX II はこの経験の上に広範な進歩と改革を伴って構築されています。

Dominion のプラットフォーム、ユーザインタフェースと管理

強力な Dominion ハードウエア プラットフォームで性能、信頼性と安全性を提供するのをはじめとして、SX II は事実上前のモデルの全ての Serial-over-IP の機能を含み、Dominion の共通のユーザインタフェースと管理機能に加え素晴らしい新しい能力を備えています。

全 CLI に基づく設定と自動設定

SX II は SSH、Telnet とウエブベースのユーザインタフェースを通じて完全な CLI のアクセスと管理を提供します。２つのスクリプトに基づく自動設定方法が素早いインストールとそれに引き続く設定の変更のために利用できます。

魅力ある新機能と革新

SX II の新しい機能には、軍用レベルの 256 ビット AES 暗号化と FIPS 暗号化モード、自動 DTE/DCE シリアル ポート検出、革新的なラックでのアクセス オプション、ワイヤレスモデムのサポート、IPv6 ネットワーク、スクリプトに基づく自動設定と Dominion 互換のユーザインタフェースと管理が含まれています。

Comm と Center 管理と拡張性

Raritan の Comm と Center によって、企業や組織は支店のオフィスを含む複数の場所に広がる数百あるいは数千のシリアル デバイスでさえも管理できます。

強力なハードウエア プラットフォーム

強力な新ハードウエア プラットフォーム	強力な新ハードウエア プラットフォームは 1 GHz の CPU エンジンと 8 重の RAM の増加を備えています。増加されたフラッシュ メモリは最大 8GB で、保存と記録のために使われます。前面パネルの LED はポートの接続状態を示します。
広い多様性を持つ 1U モデル	ラック搭載可能な 1U モデルは 4、8、16、32、と 48 ポートのものが利用できます。全て２重の電源供給と２重のギガビット イーサネット LAN ポートを備えています。これらのモデルはオプションの組み込みモデムがあります。ラックでのアクセスには RJ-45/シリアル、USB、と KVM コンソールが含まれます。
強力なシリアル処理エンジン	Dominion SX II はその強力なハードウエア プラットフォームで大抵の究極の使用形態に対して強力なシリアル処理を提供します。 最大で 10 人の利用者が同時に SX II に接続されたシリアル デバイスに接続できます。 最大で 200 の同時のユーザ セッションがどの SX II コンソールサーバによってもサポートされます。ポート設定時間は元の SX より最大 23 倍速くなっています。 接続時間は 50 倍早くなっています。
二重化電源	全てのモデルは２重の 100-240 ボルト AC の自動切り替え電源供給かつ自動障害切替え機能を持ち信頼性を高めています。
２重 DC 電源モデル	２重電源と２重 LAN で、8、32、と 48 ポートの DC 電源モデルが利用できます。これらのモデルは AC 電源のものと同じ機能、シリアルアクセスと性能を提供します。
全てのモデルに２重のギガビット イーサネット LAN	２重のギガビット イーサネット LAN ポートは同時作動あるいは自動切り替わりに設定できます。２重スタックの Ipv4 と Ipv6 ネットワーク機能
５つの USB ポート	Dominion SX II は４つの USB 2.0 ポートを持ち、３つは背面パネルに、１つは前面パネルにあります。これらはローカルなキーボード、マウス、3G/4G セルラーモデムに用いることができ、また USB ドライブ経由で自動設定にも使えます。USB 2.0 ミニ B ポートも１つあーカルなラップトップ接続のために使えます。
電話 モデム (オプション)	全てのモデルは内部 RJ11 接続の 56K 電話モデムのオプションを持ち、緊急時と災害復旧のために使えます。
革新的なローカルコンソール	Dominion SX II ローカル コンソールはラックでのアクセスのために複数の方法を提供しています。このコンソールは従来の RJ45 シリアルポート、USB ミニ-B ポート、そして DVI/USB KVM コンソールさえも含んでいます。
生産的なSerial-over-IP のアクセス	

Serial-over-IP (IP 経由シリアル) アクセス	Dominion SX II は最も広範な多様性のある serial-over-IP 接続を、SSH/Telnet クライアント、ウエブ ブラウザ、Comm と Center、電話モデム、セルラー モデムとラックでのアクセスを経由でサポートしています。これには CLI、GUI と複数の直接ポートアクセス方法を含んでいます。
SSH/Telnet クライアント アクセス	デスクトップ、ラップトップ、あるいは携帯デバイスからの SSH/Telnet クライアント アクセス。ユーザネーム/ポート文字列シンタックスを用いた SSH 経由の直接ポートアクセス。顧客は SSH キーをアップロードし、見、そして消去することができより安全です。
ウェブブラウザでのアクセス	Dominion SX II 経由のウエブ ブラウザでのアクセスあるいは Comm と Center ユーザ インタフェースと Raritan シリアル クライアント (RSC)。
便利なダイレクト ポート アクセス	SSH、Telnet & HTTP 経由の便利なダイレクト ポート アクセス方法。Telnet と SSHv2 のクライアントのための IP アドレスと TCP ポートに基づくアクセス。独立の IP アドレスかあるいは TCP ポート番号が各 SX II ポートへのアクセスのために割り当てられます。URL 経由の HTTPS ベースの直接アクセス。第三者の回送ソフトウエアのために Com ポートの回送がサポートできます。
携帯電話と電話モデムでのアクセス	緊急アクセス、ビジネス連続性と災害復旧のためのオプションの外部セルラー (3G/4G) モデムと内部電話モデム。
革新的なラックでのアクセス	Dominion SX II ではラックで複数のタイプのローカルアクセスを得ることができます。それには次のものが含まれます:(1) 伝統的な RJ45 シリアル ポート、(2) ラップトップ接続のためのミニ USB ポート、そして (3) ラックマウントのキーボードトレーあるいは KVM スイッチと接続するための DVI と USB ベースの KVM コンソール。
ポートのキーワード 監視と警告	ユーザはポートあたり最大 14 のキーワードを定義できます。SX II はポートから来るデータをスキャンし、キーワードの中の１つが検出されると、警報を SNMP あるいは e メール経由で送ります。シリアルのデバイスはユーザが接続されていなくても監視されるます。この結果より早い通知が行われ、修理の平均所要時間(MTTR) の短縮につながります。
ポートの Syslog、NFS とローカル ファイルへの記録撮り	シリアルデバイスとの間のポートのやり取りは Syslog サーバ、ネットワーク ファイルシステム (NFS) サーバあるいはローカルに最大 8Gb の記憶装置を持つ SX II デバイスに記録されます。
NFS ログ機能	全てのユーザーのキー入力とサーバ/デバイスの応答を NFS サーバに記録します。さらに高度な安全性のためにユーザ定義の暗号化キーで NFS サーバに記録することもできます。NFS ログにメッセージを記録しておくことは、関係しているサーバ/デバイスがダウンした時に簡単に観察することを可能にします。
SecureChat インスタント メッセ	SX II のユーザの間で、安全で即座のメッセージ交換を可能にします。分散しているユーザの共同作業を可能にし、生産性、トラブルシュー

ージ	トを増加させ、問題解決さらに訓練の時間を短訓します。
シリアル デバイスの自動ログオフ	ユーザの活動がなく時間切れとなると、ユーザが設定できる[ログオフ]命令を目標システムに送ることができます。シリアル セッションが時間切れで自動的に閉じられ、権限のないアクセスの可能性があるオープン状態を放置しません。

包括的なシリアルデバイスのアクセス

シリアルデバイス管理における 10 年の経験	第 1 世代の Dominion SX は 10 年以上に亘って顧客にサービスを提供し、50 万ポート以上が売られました。これは多様なシリアル デバイスに亘って数億時間もの動作を表しています。
自動の DTE/DCE シリアル ポート検出	この機能は Cisco 装置（とその他の互換デバイス）に対してケーブルを取り替えることなく直結の Cat5 接続を可能にします。これはまた SX II が第 1 世代の SX を既存のシリアル デバイスの接続のまま置き換えられることを意味します。
最も広範な多様性のシリアル デバイスをサポート	最も広範な多様性のシリアル デバイスをサポートし、それには、ネットワーク ルーター、イーサーネット スイッチ、ファイアウォール、UNIX/LINUX サーバ、ウィンドウズ サーバ、バーチャル ホスト、ラック PDU、UPS システム、電子通信・ワイヤレス機器が含まれます。複数のオペレーティング システムをサポートし、それには SUN® Solaris、 HP-UX、AIX、Linux®、Windows®Server 2012、そして UNIX® が含まれます。
最大 230,400 ボーのシリアル接続	シリアル接続に対して 1,200 から 230,400 bits-per-second の動作速度をサポート
フレキシブルなシリアル ポート オプション	柔軟な各シリアルポートのオプション、それには BPS、エミュレーション、エンコード、パリティ、フロー制御、ストップビット、文字とラインの遅延、常時アクティブ接続’さらにその他が含まれます。複数ユーザがオプションであるポートに同時に書き込むことができます。使用者が時間切れとなった時の終了命令を定義可能、またポート命令と電力制御に対するインライン メニューが可能
VT100/220/320/ANSI のサポート	端末エミュレーションのためのオプションの選択肢が多くなり、サポートできるデバイスの範囲が拡大します。SX II は次のコード セットをサポートしています：US-ASCII (ISO646)、 ISO8859-1(Latin-1)、ISO8859-15(Latin-9)、UTF-8 及びその他
Raritan PDU の遠隔電源制御（電源制御メニュー付き）	Raritan ラック PDU（PX、PX2、PX3、RPC)は Dominion SX II に接続でき、PDU に接続された装置の遠隔電源制御を行うことができます。遠隔電源制御は SX II GUI、SSH/Telnet クライアントあるいは Comm と Center を用いて行うことができます。出力の接続関係は複数の電源供給源を持つシリアルデバイスに対して生成でき、例えばそれらの出力端は一つの電源命令で制御することもできます。SX II は電源制御のためにシリアル セッションの間「Control P」スタイルのメニュー命令を備えています。

セキュリティ - 暗号化	
強力な 256 ビット AES 暗号化	SX II では、セキュリティを高めるために Advanced Encryption St と ard (AES) が使用されます。128 および 256 ビットの AES 暗号化が利用できます。AES は米国政府の承認した暗号アルゴリズムです。NIST (米国の国立標準技術研究所) の FIPS 標準 197 で推奨されています。
IFIPS 140-2 暗号化モジュールで認証されています。	政府、軍、その他の高度なセキュリティの応用では、Dominion SX II は強化された暗号化として認証された FIPS 140-2 暗号化モジュールを使用しています。試験され FIPS 140-2 に適合すると認証されたモジュールが米国とカナダの国家機関で機密性の高い情報の保護に受け入れられています。
強化された暗号化オプション	さらに多くの暗号化オプションがサポートされています：ウエブ-ブラウザのセキュリティに 256 および 128 ビットの SSL 暗号化、SSHv2 の接続のためには AES と 3DES がサポートされています (クライアントによります) 。
セキュリティ - 認証	

外部認証機関として LDAP、Radius、TACACS & Active Directory を利用します。	Dominion SX II は Microsoft Active Directory のような工業標準のディレクトリ サーバを組み込んで LDAP、Radius、TACACS & Active Directory を利用します。これによって Dominion SX II は既存のユーザネーム/パスワードのデータベースをセキュリティーと便利さの両面のために利用することを可能にします。SecureID はさらにセキュリティを高めるため RADIUS を通じてサポートされます。
顧客提供の SSL 認証をアップロード	顧客は強化された認証と安全な通信のために（自己サインあるいは認証権限を与えられた）ディジタル証明書を Dominion SX II にアップロードすることができます。
設定可能な強力なパスワードチェック	Dominion SX II には管理者が設定できる強力なパスワード チェック機能があります。この機能によって、ユーザーの作成したパスワードが企業または政府の標準を満たし、悪意のあるハッキング行為によって暴かれないようにします。
セキュリティ バナーの設定	政府機関や軍のようなセキュリティを重視する顧客には、ユーザがログインする前にセキュリティ メッセージを表示する必要があります。SX II では、カスタマイズ可能なバナー メッセージを表示できます。また、このメッセージへの同意を義務付けることもできます。
SSH での顧客証明書の認証	ログイン/パスワードによる認証に加えて、SSL インタフェースではユーザは SSH 証明書による認証を受けることができます。各ローカルのユーザには最大 10 個の SSH キーを割り当てることができます。このキー認証はログイン/パスワードのところで行われます。
ユーザ、グループと許可によるローカルでの認証	外部認証に加え、Dominion SX II はローカルでの認証をサポートしています。管理者はユーザとグループをカスタム化できる管理とポートアクセス許可を付けて定義できます。
ログインとパスワードのセキュリティ	SX II は複数のログインとパスワードの機能を持ち、それにはパスワードの経年処理、アイドルのタイムアウト、ユーザ封鎖とログイン制限が含まれています。ログインの失敗は締め出しとユーザを不活性化とすることができます。
SHA-2 認証のサポート	さらに安全性の高い SHA-2 の認証をサポート

セキュリティ - ネットワーク機能

２重スタックの Ipv4 と Ipv6 ネットワーク機能	Dominion SX II は Ipv4 と Ipv6 を同時にサポートする２重スタック IP ネットワーク機能を提供しています。
IPTables ファイアウォールのサポート	完全に設定可能な iptables ファイアウォールのサポートユーザが広い範囲のセキュリティのニーズに合わせて選択できカスタム化できるシステムのセキュリティレベル
選択できるスタティックルーティングのサポート	モデムと LAN1 の間、モデムと LAN2 あるいは LAN1 と LAN2 の間の接続をサポートこれによってユーザは２つの異なったネットワーク（公共と私設）と KVM あるいはイーサネット 制御のデバイスへアクセスするモデムを利用することが可能となります。ファイアウォールと共に使用する場合に、セキュアなアクセスが可能となります。
TCP/IP ポートの管理	もし希望するなら、TELNET と SSH のアクセスを無効にすることができます。これらのポートを HTTP に加えて HTTPS と discovery のポートに変えることができます。
介入者(Man In The Middle) の攻撃に備える	通信チャンネルのセキュリティ強化にクライアントとサーバに SSL 認証を使用します。
モデムの Dial-Back セキュリティ	セキュリティ強化のため、Dominion SX はモデム dial-back をサポートしています。
SSH ｖ１要求を拒否します。	SSHv1 について多く知られているセキュリティ脆弱性のため、Dominion SX は SSHv1 の接続を自動的に拒絶します。
エンドユーザの経験	
複数のユーザ側インタフェース	SX II は複数のユーザインタフェースをサポートし、ユーザが現下の仕事に最も適したインタフェースを使用する自由を与えています。これには Raritan あるいは第三者の CLI 経由のリモートアクセス、Raritan のグラフィカル ユーザ インターフェース（GUI)、ラックでの Comm と Center 経由のアクセスが含まれています。便利なダイレクト ポート アクセス方法が利用できます。
最近の CLI-GUI と完全に同等	完全な CLI の管理と設定のため、どの命令のスクリプトも可能です。
広範なブラウザをサポート	Firefox、Internet Explorer そして Chrome と広範なブラウザを提供しています。
国際的な言語のサポート	ウエブベースのユーザインタフェースは英語、日本語と中国語をサポートしています。Raritan のシリアル コンソールは４つの言語をサポートできます。英語、日本語、ハングル、と中国語
PC 共有モード	最大 10 人のユーザが接続し最大 200 のシリアル セッションで各接続されたシリアル デバイスに遠隔でアクセスできます。共有機能は共同作業、トラブルシューティングと訓練に非常に有用です。
インストールと管理は容易です。	

全 CLI に基づく設定と管理	SX II は SSH、Telnet とウエブベースのユーザインタフェースを通じて完全な CLI の管理と運用を提供します。２つのスクリプトに基づく自動設定方法が素早いインストールとそれに引き続く設定の変更のために利用できます。
USB ドライブ経由の自動構成	SX II はオプションでその USB ポートの１つに接続された USB ドライブ上の CLI スクリプトを用いて設定ができます。これは最初の設定とその後の更新に使用できます。
TFTP サーバ経由の自動構成	SX II はオプションで第２の方法、すなわち TFTP サーバに含まれた CLI スクリプトを用いて、設定ができます。これは最初の設定とその後の更新に使用できます。TFTP サーバのアドレスは DHCP で検索するかあるいは管理者によって設定されます。
Dominion 互換の管理	Dominion 互換の管理機能はウエブベースのユーザインタフェースあるいは CLI で利用できます。これには Dominion-スタイルのユーザ管理、デバイス設定、セキュリティ、保守、診断とヘルプの機能が含まれています。FTP サーバを使わずウエブ ブラウザでファームウエアの更新ができます。
インストールは容易です。	ウエブ ブラウザ、CLI あるいは自動設定で、インストレーションは数分でできます。いくつかの競合する製品では基本的なインストールにも複数のファイルの面倒な編集を必要とします。
設定可能なイベント管理と記録	SX II は膨大な種類のデバイスとユーザイベントを生成します。これにはデバイスの操作、デバイス管理の変更、セキュリティ、ユーザ作業とユーザ管理が含まれます。これらは選択的に次のものに供給されます : SNMP、syslog、email(SMTP)さらに SX II の監査用ログ SNMP v2、v3 のサポート
Raritan CommとCenter® 管理と拡張性	

Raritan Comm と Center は中央集中型の管理です。

Dominion シリーズの他の製品と同様に、Dominion SX II は完全な Comm と Center Secure Gateway の集中機能を持ち、ユーザが Dominion SX II の全てと他の Raritan デバイスを単一の IP アドレスから、そして単一の遠隔管理インタフェースの下で単一の論理システムに統合することを可能にします。

数百のシリアルデバイスを管理

Comm と Center Secure Gateway を配備すると、数百の Dominion SX II デバイス（そして数千のシリアル デバイス)を中央からアクセスし管理することが可能となります。

管理とデバイス接続に単一の IP アドレス

管理者とユーザは Comm と Center Secure Gateway によって単一の IP アドレスに接続し SX II あるいは接続されたシリアル デバイスを管理します。この接続はウエブ ブラウザからあるいは SSH を通じて行われます。CC-SG 管理の途中で、SX III のオプションとしてラックでのアクセスも可能です。

大量一括のファームウエアのアップグレード

管理者は Comm と Center から複数の SX II デバイスのファームウエアの更新（とその他の作業）をスケジュールに組むことができます。

Comm と Center Secure Gateway からの遠隔電源制御

Comm と Center は Dominion SX II のシリアル ポートに接続された Raritan PX rack PDU の遠隔電源制御をサポートしています。複数の電源供給を受けている装置では、複数の電力出力端がスイッチ装置のオンオフに相互に連携され単一のマウスクリックで操作されます。

この章の内容

パッケージの内容

SX II は、標準 1U 19 インチ ラックマウント シャーシに搭載される、完全に構成されたスタンドアロン製品として出荷されます。

SX II パッケージには次のものが含まれています –

- 1 – SX II 装置
- 1 – ラックマウント キット
- 2 – AC 電源コード
- 1 – ゴム足 1 組（4 個、デスクトップ設置用）
- 1 – 保証書
- 1 – SX II クイック セットアップ ガイド

SX II モデル

次の SX II モデルが提供できます。

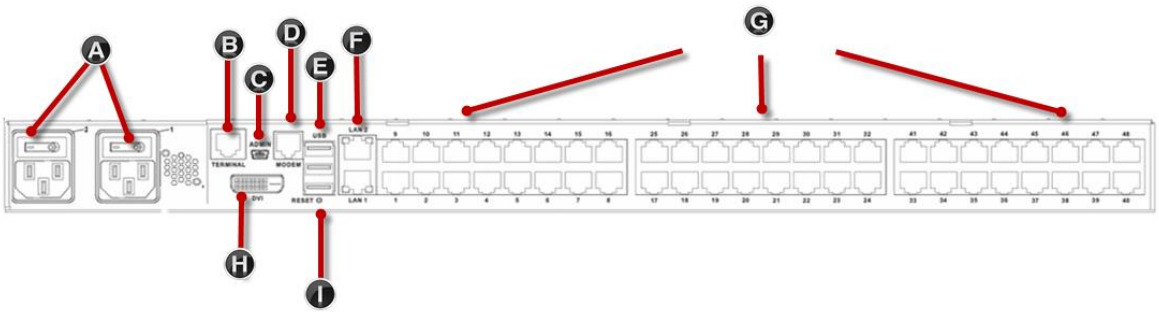
文字 M を持つモデル は全ての SX II モデルで提供される標準機能に加えて内部モデムを含んでいます。標準機能のリストは、 ***イントロダクションを参照してください。*** 『1p. の"*機能と利点*"参照 』。

- DSX2-4 と DSX-4M - 4-ポート シリアル コンソール サーバ
- DSX2-8 と DSX-8M - 8-ポート シリアル コンソール サーバ
- DSX2-16 と DSX-16M - 16-ポート シリアル コンソール サーバ
- DSX2-16 と DSX-16M - 32-ポート シリアル コンソール サーバ
- DSX2-48 と DSX-48M - 48-ポート シリアル コンソール サーバ

モデルのサイズ、重量、温度とその他の仕様は次に掲載されています ***SX II 寸法と物理的仕様*** 『244p. 』。

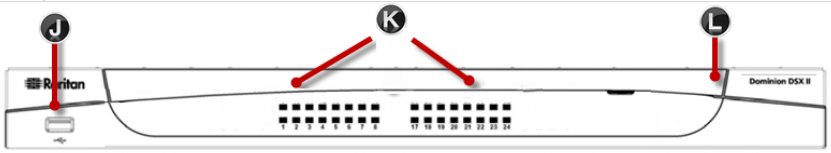
SX II 装置の図面

ここに示されている画像はあるサンプルで、モデルによって異なることにご注意ください。



装置図面の索引キー	
A	AC 電源コンセント 1 と 2、独立の電源オン/オフスイッチ付
B	端末ポート/コンソール ポート
C	管理用ミニ-USB ポート
D	モデム ポート（モデルによる）
E	3 USB ポート
F	LAN1 および LAN2 ポート

G	サーバ ポート
H	DVI-D ポート
I	リセット ボタン



装置図面の索引キー	
J	USB ポート
K	LED ポートインジケーター
L	電源状態 （注 SX II 48 ポートモデルでは電源状態は前面パネルの USB ポートの上に配置されています。）

サポートされているシリアル デバイス

- ルータ
- LAN スイッチ
- ラック PDU
- ワイアレスモデム
- Telecom モデム
- Windows サーバ
- UNIX サーバ
- Linux サーバ
- 仮想ホスト
- ファイアウォール

SX II　アクセス クライアント

Raritan Serial Console (RSC) (RSC)

遠隔コンソールからの接続によって RSC にアクセスするかあるいはスタンドアローンの RSC を用いて目標に直接アクセスします。

参照 *”Raritan Serial Console (RSC) Help”* 『48p. の*″Raritan シリアル コンソール (RSC) ヘルプ″*参照 』

ダイレクト ポート アクセス

ダイレクト ポート アクセスにより、ユーザはデバイスのログイン ダイアログ ボックスとポート アクセス ページを使用する必要がなくなります。

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

command line interface (CLI)

SSH あるいは Telnet を経由して CLI を用いて接続

参照 ”Comm と Line Interface SX2”

Ch 2 始めて SX II を設定する

SX II はリモートコンソールあるいは command line interface CLI から設定できます。

この章の内容

デフォルトのログイン情報

SX II 装置は次のデフォルトで出荷されます。最初に SX II にアクセスするときにはデフォルトを用います。

- IP アドレス – 192.168.0.192
- IP ネットマスク 255.255.255.0
- ユーザ名 – admin （全て小文字）
- パスワード – raritan （全て小文字）

重要：バックアップとビジネスの連続性の目的で、バックアップ管理者用ユーザ名とパスワードを生成することを強く勧めます。この情報は安全な場所に確保してください。

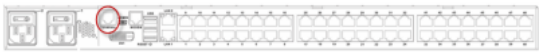
コマンドラインインタフェースを用いての最初の SX II の設定

ポートの設定（シリアル 通信パラメータ）が次のように設定されていることを確認します

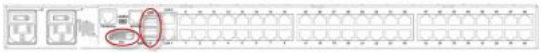
- 秒あたりビット数（BPS） = 115200
- データ ビット: 8
- パリティ: なし
- ストップ ビット = 1
- フロー制御 = なし

SX II を始めて設定するには CLI を用いて

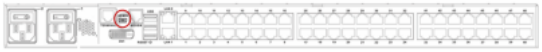
1. SX II を次の中の一つを用いて接続します –
   - コンピューターをターミナル ポートに接続しシリアルのコンソールにアクセスします。



- キーボードトレイあるいはKVMコンソールをDVI-DとUSBポートに接続します。



- ラップトップはミニUSB管理ポートに接続します。



2. SX II に接続するとエミュレータのインタフェースが開きます。キーボードのエンターキーを押してください。
3. ログイン 画面が現れると、デフォルトのユーザ名 "admin" とパスワード "raritan" を入力します。全て小文字を使用します。
4. 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。ここで、それを行い、このパスワードを今後のログインのために確実に覚えてください。 CLI を経由してパスワードを創るときには、スペースで始めたりスペースで終わることはできません。これはリモートコンソールを用いてパスワードを創る時には適用されません。

   デフォルトでは、ネットワークは静的 IP アドレスで設定されています。
5. admin から 入力になると config と入力し さらに次の入力で network を入力します。
6. admin > config > network > で入力になると次を入力します - interface if lan1 ipauto none ip <ip address> mask <mask> gw <gateway ip address>

   DHCP を使用するには、次を入力します - interface if lan1 ipauto dhcp
7. デバイスにそれを識別するための名称を与えます。

   それには次を入力します "name devicename <DSX2 name>"。

   名称には最大 32 文字までがサポートされています。スペースと特殊文字はサポートされていません。
8. admin > config > network で入力になると次を入力すると - "quit" 上位のメニューに移り admin > config となるので、次を入力します - "time"。
9. admin > config > time > で入力待ちとなり、SX II の日付および時刻を設定します。
   - 次を入力します timezonelist そして、タイムゾーンに対応するコード番号を見つけます。
   - 次を入力します clock tz <timezone code> date <date string> time <time string>

     ここで <timezone code> はタイムゾーン コード <time string> は "HH:MM:SS" のフォーマットでの現在の時刻、そして <date string> は "YYYY-MM-DD" のフォーマットでの現在の日付（引用符をふくみ、２４時間時刻を用いる）。

例: `clock tz 9 date "2015-08-15" time "09:22:33"`

10. 次を入力 `top` し、トップレベルの入力待ちに戻る。
11. 次に、次を入力 `config` し、そして入力待ちで次を入力します `-ports` 。
    ここで、目的とするデバイスが接続されている各サーバーのポートを設定できます。
12. 次を入力します `-configport` そして `?` を打ち込みポートのパラメータを見ます。
    たとえば:
    `config port 1 name cisco1700 bps 9600 parity odd flowcontrol none emulation vt100`
    ポートを範囲で指定したり、ワイルドカード アスタリスク `*` を次のように使うことができます `config port * bps 115200`
    これはすべてのポートの通信速度を 115200 bps に設定します。
    または
    `config port 3-7 bps 115200`
    これはポート 3 から 7 を 115200 bps に設定します。
    または
    `config port 1,2,7-9 bps 115200`
    これはポート 1 と 2、 7 から 9 を 115200 bps に設定します。
    このステップをデバイスが接続されている各ポートについて繰り返し行います。
13. それを終えると、次の `top` を入力し、トップレベルの入力待ちに戻ります。

Terminal Emulation を Target にセットします

SX II 上のターミナル エミュレーション設定が、特定のターゲット デバイスのポート設定と適切に関連付けられます。

Telnet や SSH などのクライアント ソフトウェアのターミナル エミュレーションの設定が、ターゲット デバイスをサポートできることを確認します。

ホスト上で使用するエンコーディングがターゲット デバイスのエンコーディング設定と一致していることを確認します。

例えば、もし Sun™ Solaris™ サーバ上の文字セットが ISO8859-1 にセットされているなら、ターゲット デバイスもまた ISO8859-1 にセットされているべきです。

SX II シリアル ポートに接続されているターゲット ホストのターミナル エミュレーションが VT100、VT220、VT320 または ANSI であることを確認します。

ほとんどの UNIX®システムでは `export TERM=vt100`（または `vt220|vt320|ansi`）が UNIX ターゲット デバイスで優先するターミナルのエミュレーションタイプをセットします。したがって、もし HP-UX® サーバ上のターミナルタイプの設定が VT100 にセットされているなら、Access Client は同様に VT100 にセットされるべきです。

CLI のエスケープ シーケンスをセット

エスケープ シーケンスはユーザが設定できるものでポートごとに設定できます。

エスケープ シーケンスがポートごとに設定できるのは、異なったターゲットのオペレーティングシステムとホストの応用ソフトが異なったエスケープ シーケンスにはまることがあるからです。

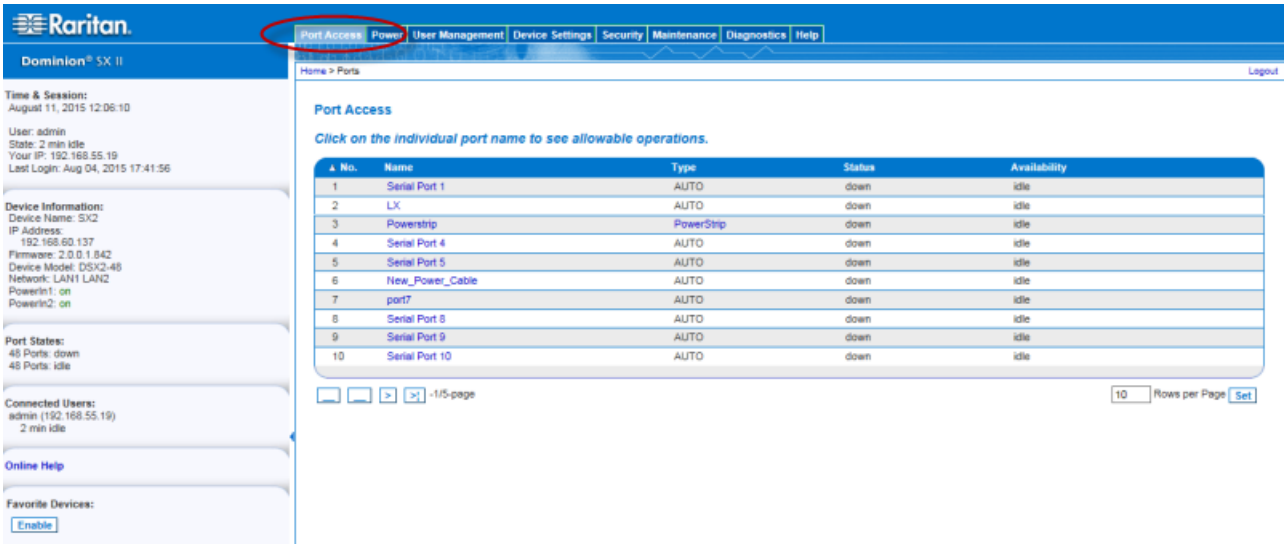
SX II サーバのデフォルトのエスケープシーケンスがアクセス応用ソフトあるいはホストのオペレーティングシステムが要求するキーシーケンスと矛盾していないことを確認してください。

コンソールのサブモードがデフォルトのエスケープシーケンス ^J が押されたときに表示されるはずです。

Raritan では [あるいは Ctrl-[を使用しないことをおすすめします。これらのいずれかは、例えばエスケープ コマンドを意図しないのに引き起こすというような、意図しないコマンドを引き起こすかもしれません。この連続キー入力はキーボードの矢印キーによっても引き起こされます。

Ch 3 リモート コンソールの機能にアクセスし使用する

リモート コンソールはネットワーク接続で SX II にログインした時にアクセスするブラウザベースのインタフェースです。



リモート コンソールの管理者用機能

管理者はリモート コンソールから SX II の設定と保守を行います、例えばネットワークのアクセスを設定したり、ユーザを追加したり管理したり、デバイスの IP アドレスを管理したり等です。

リモート コンソールのエンドユーザ向け機能

リモート コンソールから、エンドユーザはターゲットにアクセスし、お気に入りメニューを管理し、パスワードを変更したりします。

これらの機能はコマンドラインインタフェースからでも行えることを知っておいて下さい。

この章の内容

ポップアップの許可

使用するブラウザにかかわらず、SX II のリモート コンソールを立ち上げるためのポップアップを許可する必要があります。

セキュリティ警告および検証メッセージ

SX II にログインすると、セキュリティ警告およびアプリケーション検証メッセージが表示されることがあります。

それは次のようなものです：

- Java™ セキュリティ警告と SX II の検証要求

  参照 ***Java 検証およびアクセス警告*** 『19p. 』 および ***証明書のインストール*** 『22p. 』
- ブラウザおよびセキュリティの設定に基づくその他のセキュリティ警告。

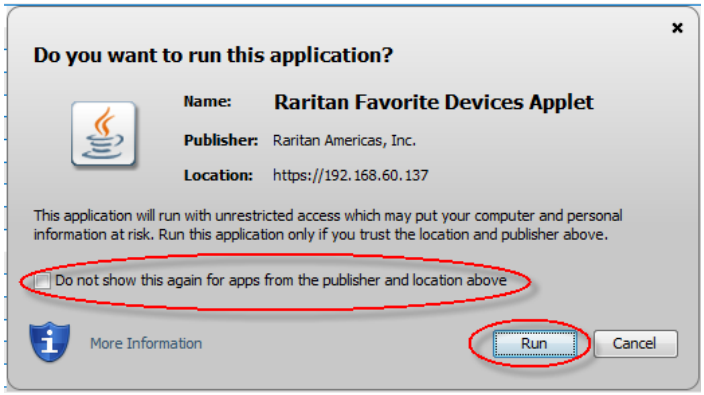
  参照 ***その他のセキュリティ警告*** 『20p. 』

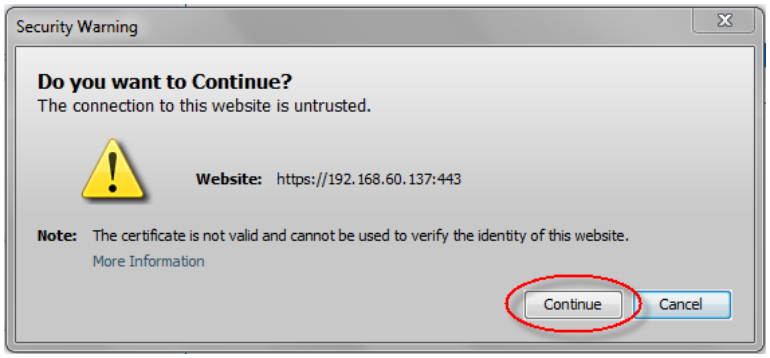
Java 検証およびアクセス警告

SX II にログインすると、Java™が SX II の有効化と、その応用ソフトへのアクセスを許可するよう促します。

Java の警告を抑制し、セキュリティを強化するために、各 SX II に SSL 証明書をインストールすることをお勧めします。

参照 *SSL 証明書* 『176p. 』

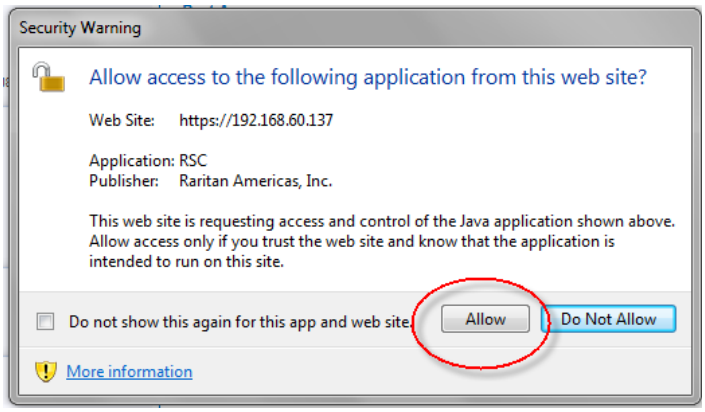




その他のセキュリティ警告

SSL 証明書が SX II にインストールされた後でも、 ブラウザおよびセキュリティの設定によっては、SX II にログインすると、さらにセキュリティ警告が表示される場合があります。

SX II リモート コンソールを起動するには、これらの警告を承諾する必要があります。



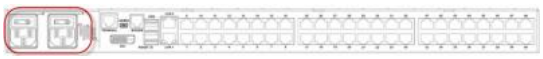
セキュリティと証明書に関する警告メッセージに対して以下のオプションをオンにすることにより、それ以降にログインしたときに表示される警告メッセージが抑制されます。

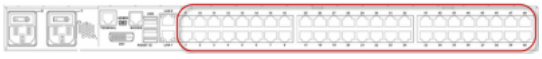
- [今後、この警告を表示しない]
- [この発行元からのコンテンツを常に信頼する]

リモートコンソールからの最初の SX II の設定

1. SX II をラックに据え付けた後、パワーコードを SX II 上の電源コネクターと外部の AC あるいは DC の電源（モデルによる）との間に接続します。
2. 第 2 の電源コネクターをバックアップ電源に接続することもできます。

   SX II とともに来る電源コードを使用してください。

   
3. 外部モデム（オプション）を接続します。参照 ***外部モデムに接続しグローバルなアクセスを可能にします。*** 『140p. の*"外部ブロードバンドモデムに接続しグローバルアクセスを有効にする"*参照 』Online Help
4. 目的のデバイスあるいはその他のシリアルで管理されているデバイスを SX II 上のサーバーポートに接続してください。

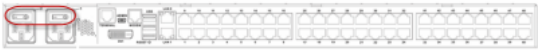
標準の Cat5 ケーブルを用い、目的のデバイスを SX II の背面で空いているポートに接続してください。

注:目的デバイスで RJ45 ポートのピン定義をチェックしてください。それは SX II 上のピン定義と合致しているはずです。

または

必要なら Raritan のゼロ化シリアルアダプターをターゲットデバイスのシリアル ポートに接続し、そして標準の Cat5 ケーブルをアダプターに差し込みます。ケーブルの他方の端を SX II の背面の空いているポートに接続します。

5. 電源スイッチで SX II の電源をオンにします。



次に、SX II をネットワークに接続し、初めてネットワーク設定を行います。

参照 ***コマンドラインインタフェースを用いての最初の SX II の設定*** 『13p. 』または リモートコンソールからの SX II ネットワーク形成の設定。

クロスオーバー ケーブル(オプション)を用いたラップトップの SX II への接続

SX II を始めて設定する際に、もしラップトップの LAN ポートから SX II の LAN1 ポートにクロスオーバーケーブルを用いて接続する場合には、次のようにしてください –

1. クロスオーバーケーブルを用いて SX II の LAN1 とラップトップの LAN ポートを接続します。
2. SX II に接続する LAN ポートの静的 IP を次に設定します `192.168.0.191` そしてネットワーク マスクを次に設定します `255.255.255.0`。
3. ブラウザーを立ち上げ、SX II に次を経由してアクセスします `192.168.0.192`。

証明書のインストール

ブラウザで、SX II の SSL 証明書を受け入れて検証するよう求められる場合があります。

依存します ブラウザおよびセキュリティの設定によっては、SX II にログインすると、さらにセキュリティ警告が表示される場合があります。

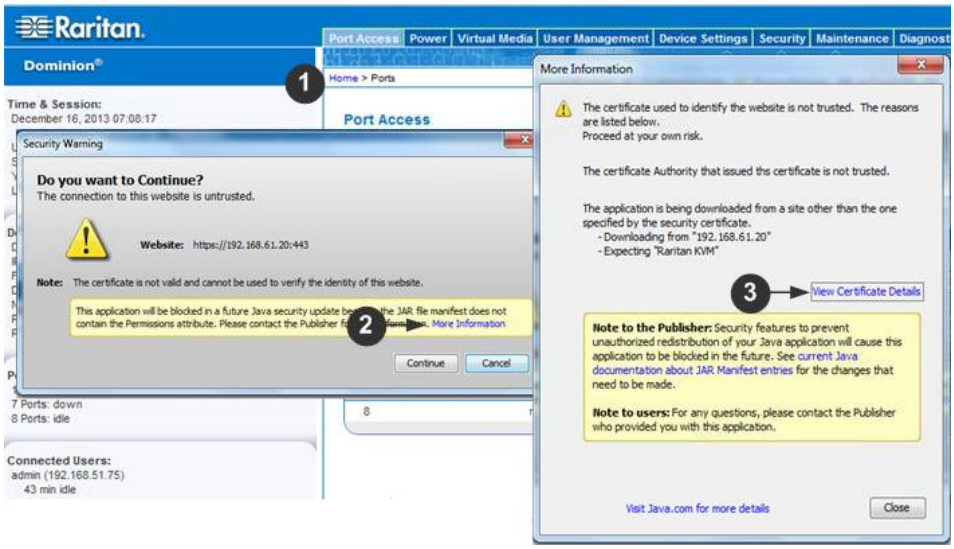
SX II リモート コンソールを起動するには、これらの警告を承諾する必要があります。 詳細については、以下を参照してください。 ***セキュリティ警告および検証メッセージ***『18p. 』。

ブラウザで SSL 証明書をインストールする方法について、例を 2 つ示します。どちらも Microsoft Internet Explorer 8® および Windows 7® を使用します。

具体的な方法および手順は、使用するブラウザおよびオペレーティング システムによって異なります。詳細については、使用するブラウザおよびオペレーティング システムのヘルプを参照してください。

例 1:ブラウザへの証明書のインポート

この例では、ブラウザに証明書をインポートします。



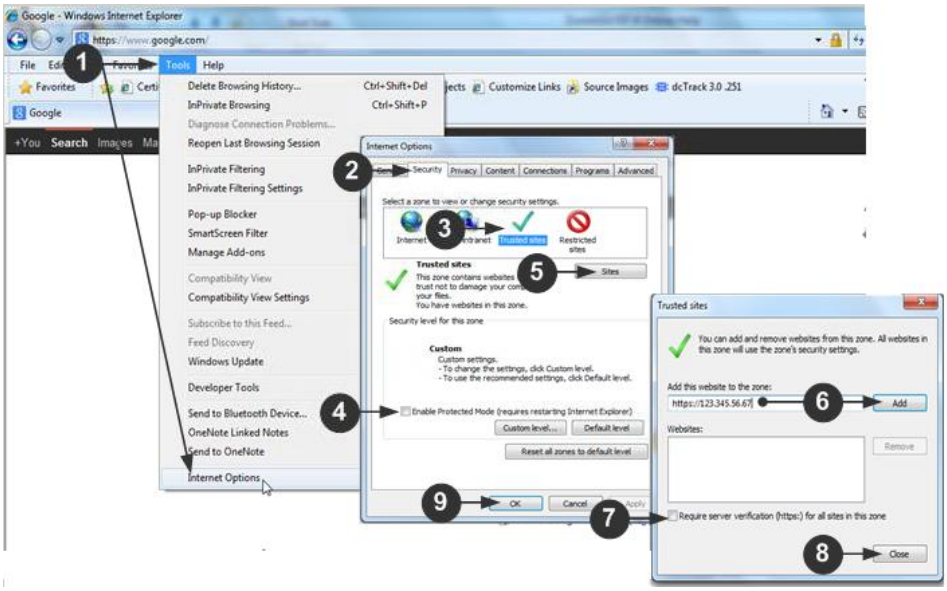
1. IE ブラウザを開き、SX II にログインします。
2. 最初の Java™ セキュリティ警告で［More Information］をクリックします。
3. More Information ダイアログ ボックスで［View Certificate Details］(証明書の詳細の表示) をクリックします。証明書をインストールするかどうかを尋ねられます。ウィザードの手順に従います。

注:ブラウザで確認が求められない場合は、手動でツールのインターネット オプションを選択して、インターネット オプション ダイアログ ボックスを開きます。

1. コンテンツ] タブをクリックします。
2. [証明書] をクリックします。
   証明書のインポート ウィザードが開くので、各手順を進めます。
   - インポートする証明書ファイル]- 参照して証明書を探す
   - [証明書ストア] - 場所を選択して証明書を保存する
3. ウィザードの最後の手順で完了をクリックします。
   証明書がインポートされます。成功メッセージを閉じます。
4. インターネット オプションダイアログ ボックスで [OK] をクリックして変更を適用し、ブラウザを閉じて再度開きます。

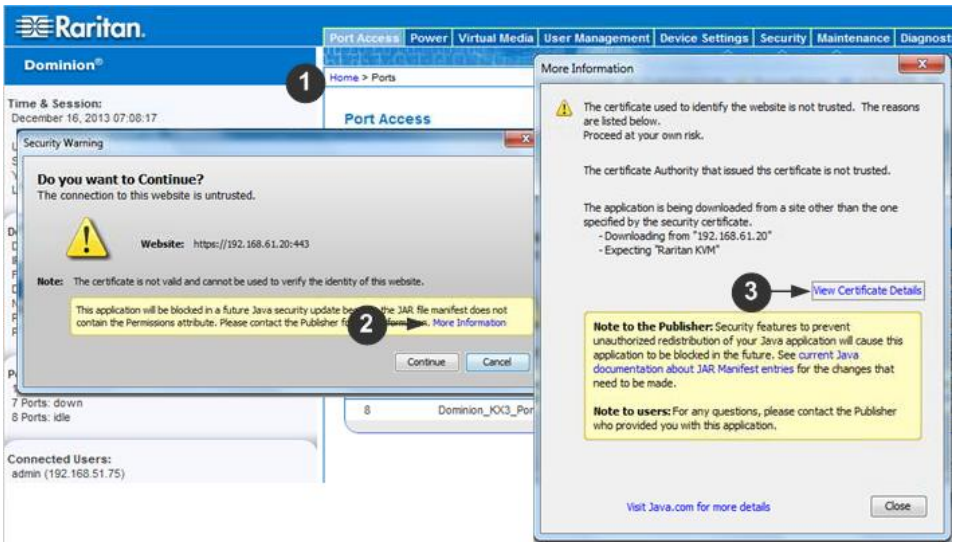
実施例 2 SX II を信頼できるサイト [Trusted Sites] に加え証明書をインポートします。

この例では、SX II の URL が信頼できるサイトとして追加され、一連の手続きの中で自己署名証明書が追加されます。



1. IE ブラウザを開き、ツールのインターネットオプション を選択して、インターネット オプション ダイアログ ボックスを開きます。
2. セキュリティタブをクリックします。
3. [Trusted Sites (信頼できるサイト)] をクリックします。
4. 保護モードを無効にして、あらゆる警告を承諾します。
5. [Sites (サイト)] をクリックして、信頼できるサイト] ダイアログ ボックスを開きます。
6. SX II の URL を入力して、追加 をクリックします。
7. このゾーンに対するサーバの確認を選択解除します (該当する場合)。
8. [Close] をクリックします。
9. インターネット オプション ダイアログ ボックスで [OK] をクリックして変更を適用し、ブラウザを閉じて再度開きます。

次に、証明書をインポートします。



1. IE ブラウザを開き、SX II にログインします。
2. 最初の Java™ セキュリティ警告で [More Information]をクリックします。
3. More Information ダイアログ ボックスで [View Certificate Details] (証明書の詳細の表示) をクリックします。証明書をインストールするかどうかを確認するダイアログ ボックスが開きます。ウィザードの手順に従います。

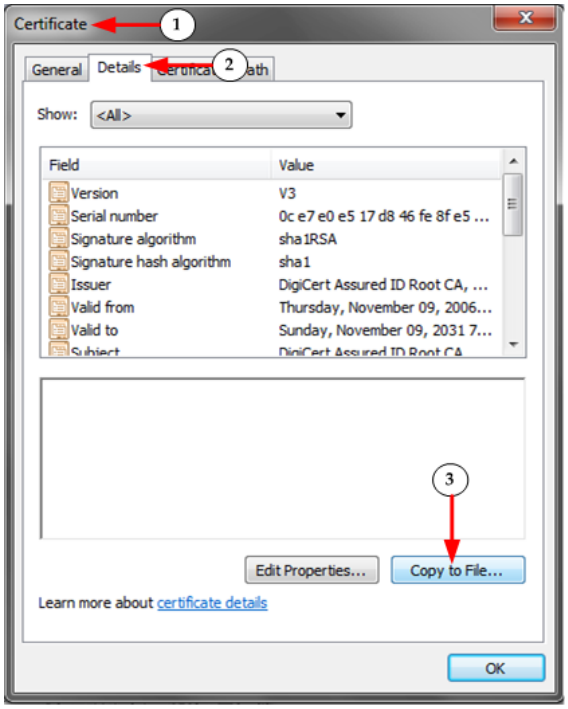
   詳細については、次を参照してください。 ***実施例 1：ブラウザへの証明書のインポート*** 『22p. の"***例 1:ブラウザへの証明書のインポート***"参照 』。

バイナリーの証明書を Base64-Encoded DER Certificate （オプション）に変換する

SX II は SSL 証明書を Base64-Encoded DER フォーマットか PEM フォーマットで要求します。

もし SSL 証明書をバイナリー フォーマットで使用していると、それをインストールすることができません。

しかし、バイナリー SSL 証明書を変換することができます。



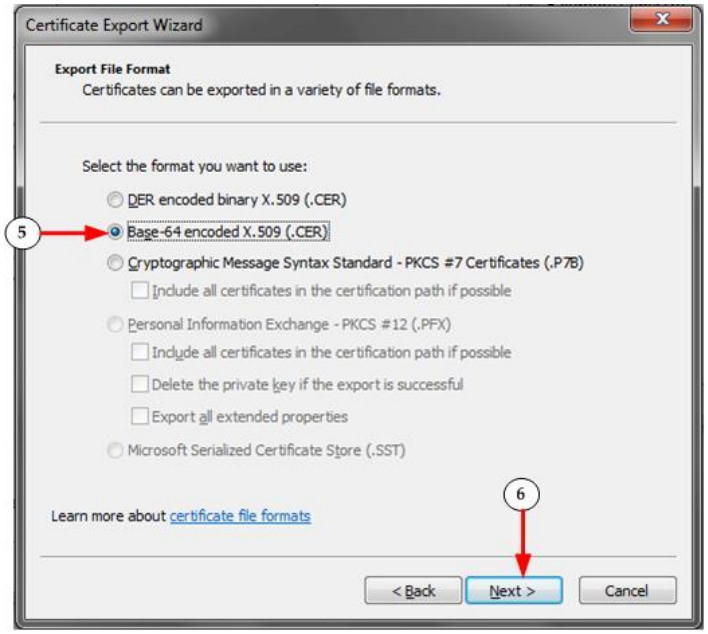
1. DEGHKVM0001.cer のバイナリー ファイルをウインドウ マシン上での位置を求めてください。

   DEGHKVM0001.cer ファイルの上でダブルクリックしてその証明書ダイアログを開けます。

2. 詳細タブをクリックします。

3. ”Copy to File...” をクリック

4. 証明書エキスポートウィザードが開きます。Next をクリックしてウイザードを開始します。



5. ウィザードの第２のダイアログで”Base-64 encoded X.509” を選択します。
6. Next をクリックしてそのファイルを Base-64 encoded X.509 として保存します。

これで、SX II で証明書のインストールができます。

SX II にログインします。

1. サポートされている ウエブ ブラウザを起動します。
2. 管理者から与えられている SX II HTTP、HTTPS あるいは DNS のアドレスを入力します。

   注:常に、HTTP の IP アドレスから HTTPS の IP アドレスにリダイレクトされます。
3. ユーザ名とパスワードを入力して、Login をクリックします。
4. ユーザ同意書に承諾します (該当する場合)。
5. セキュリティ警告が表示される場合は、アクセスの承諾または許可、あるいはその両方を行います。

リモート コンソールからパスワードを変更する

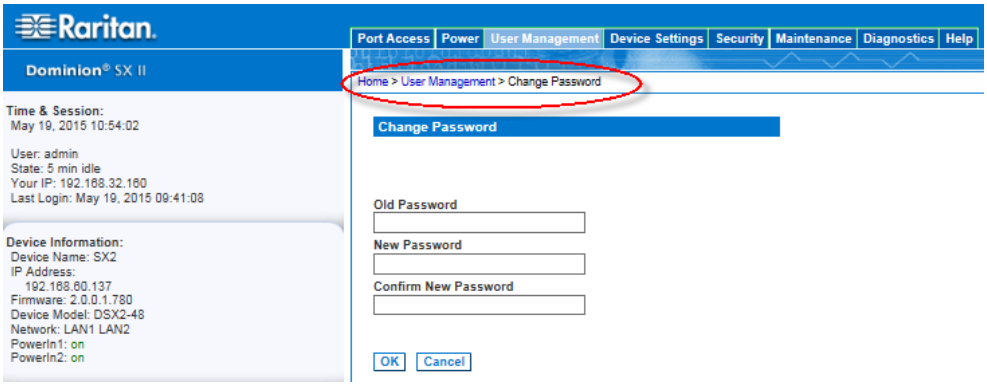
注:コマンドラインインタフェースを使ってもパスワードの変更ができます。参照 **CLI を使ってパスワードを変更する** *『199p. 』。*

- パスワードを変更するには、ユーザ管理からパスワード変更を選択してパスワード変更のページを開きます。

パスワードを変更した後にパスワードの変更に成功しましたという確認が表示されます。

強力なパスワードが使用されている場合は、パスワードに必要な形式に関する情報がこのページに表示されます。

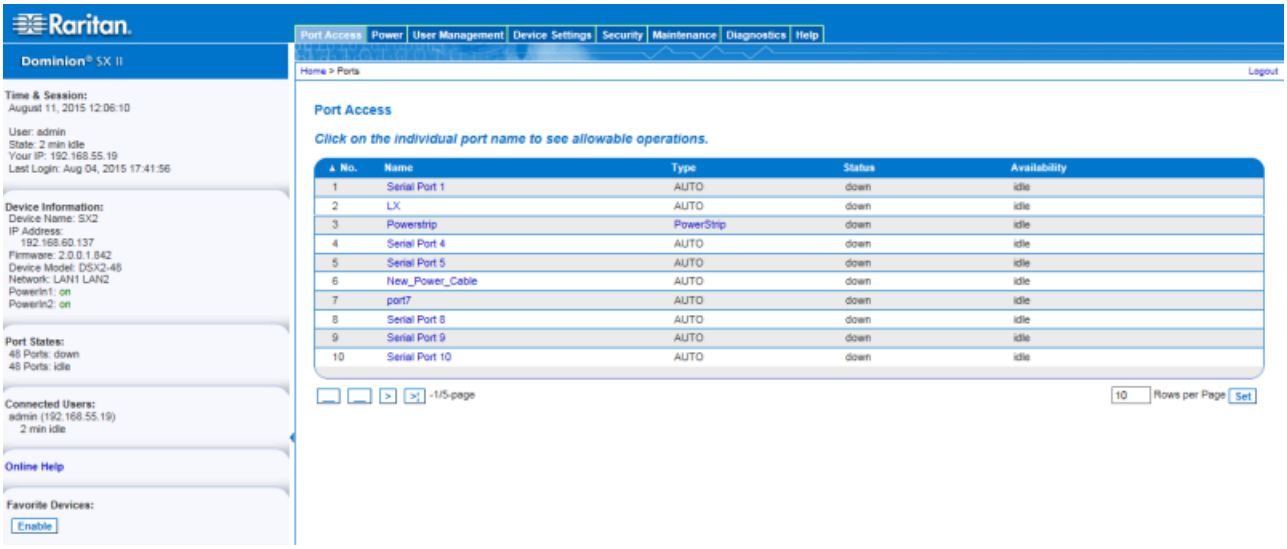
詳細については、以下を参照してください。 強力なパスワード。



重要：管理者パスワードを忘れた場合には、 SX II を後面パネルにあるリセットボタンによって出荷時デフォルトにリセットする必要があり、初期設定作業をもう一度行う必要があります。

SX II ポート アクセス ページ

正常にログインすると、ポート アクセス ページが表示され、すべてのポートについて、そのステータスと可用性が表示されます。



ポートには番号 1 から始まって SX II で使用可能ポートの総数の番号までが付いています。例えば、Port_1 – Port_64、 Port_1 – Port_32。

そのポートに名前が付けられるまでその物理ポートに"SerialPort"_"Port #"がデフォルトの名前となっています。ポートに名前が付けられると、その名前は編集されるか SX II が出荷時場設定にリセットされるまでそのポートにつけられています。

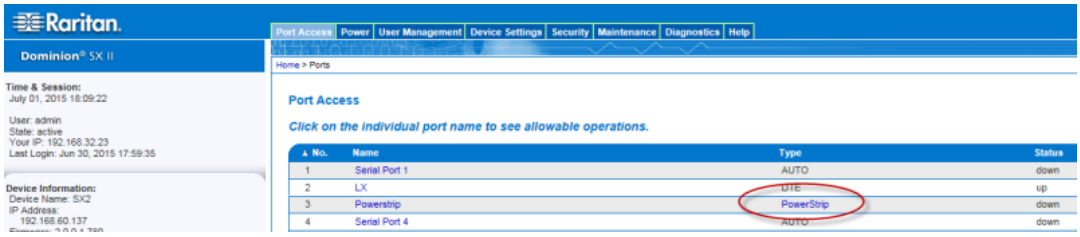
ポート タイプには、以下のものがあります。

- Auto（自動） – ターゲットが接続されていない。
- DTE – このポートに接続された DCE ターゲットは強制的に DTE の設定されます。
- DCE – このポートに接続された DTE ターゲットは強制的に DCE の設定されます。

列の見出しをクリックすることで、ポート番号、ポート名、ステータス (Up および Down)、可用性 ([Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、[Unavailable] (使用不可能)、[Connecting] (接続中)) で並べ替えを行うことができます。

リストされ使用可能とマークされたいずれかのポートの上でクリックするとそのポートの動作メニューが開きターゲットの管理ができます。詳細については、以下を参照してください ***ポートアクションメニューのオプション – ターゲットを接続、切断、電源オン、電源オフ、と電源再投入*** 『36p. 』。

リモートコンソールで、タイプ列の電源タップのリンクをクリックしポートアクセスのページから電源タップのページに素早くアクセスすることができます。



SX II 左パネル

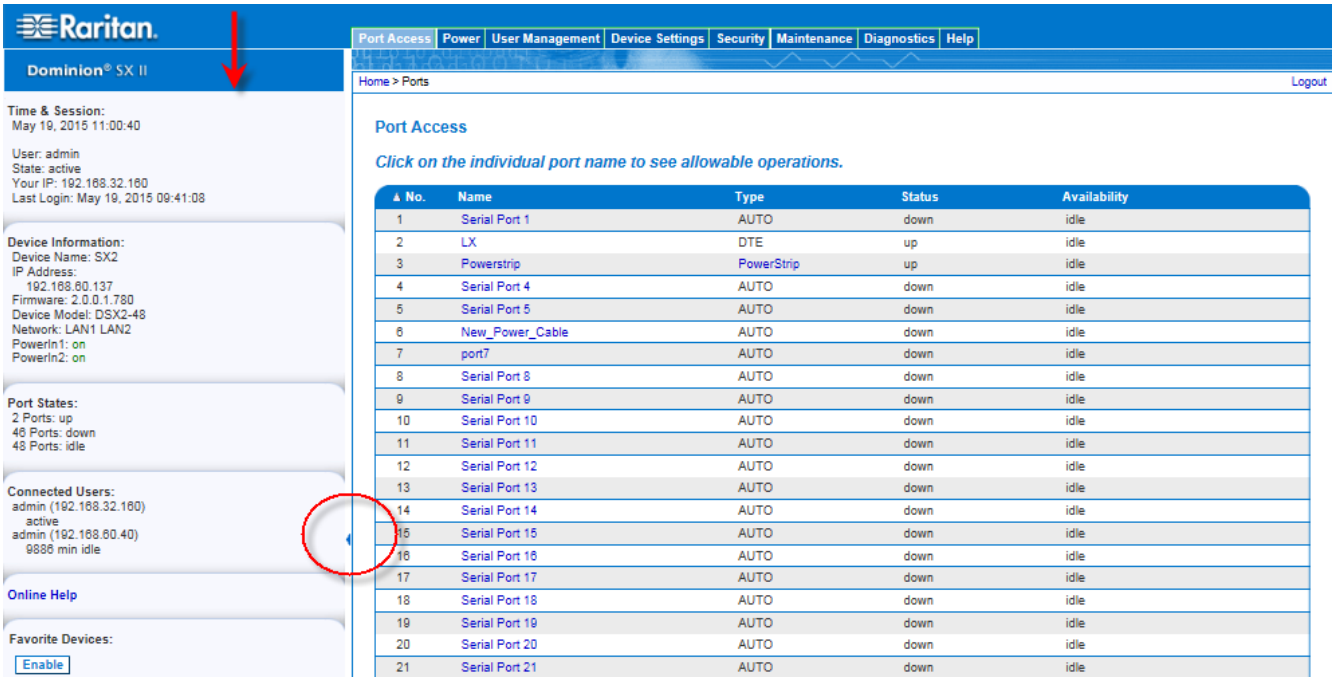
左パネルには次の情報が含まれています。

一部の情報は、特定の条件に従って、つまり役割や利用する機能などに基づいて表示されます。各情報が表示される条件もこの表に示します。

インフォメーション	記述	いつ表示されるか？
時間 と セッション	現在のセッションを開始した日時	常時
ユーザ	ユーザ名	常時

インフォメーション	記述	いつ表示されるか？
状態	アプリケーションの現在の状態（アイドルまたはアクティブ）。 アイドル状態の場合、セッションがアイドル状態になっている時間が追跡および表示されます。	常時
(あなたの IP アドレス	SX II にアクセスする際に使用された IP アドレス。	常時
最終ログイン日時	最後にログインした日時。	常時
CC-SG の管理下	SX II を管理している CC-SG デバイスの IP アドレス。	SX II が CC-SG の管理下にある場合。
デバイス情報	使用している SX II に特有の情報。	常時
デバイス名	アクセスしている SX II に付けられた名前。	常時
IP アドレス	アクセスしている SX II の IP アドレス。	常時
ファームウェア	SX II にインストールされているファームウエアの現在のバージョン	常時
デバイス モデル	アクセスしている SX II のモデル	常時
ネットワーク	LAN1 あるいは２重 LAN モードの場合 LAN1 to LAN2	常時
[PowerIn1]（電源入力 1）	電源コンセント 1 の接続状態オンまたはオフ、あるいは自動検出オフ	常時
[PowerIn2]（電源入力 2）	電源コンセント 2 の接続状態オンまたはオフ、あるいは自動検出オフ	常時
ポートの状態	SX II に使われているポートの状態 – アップ、ダウン、アイドル	常時
接続中のユーザー	現在 SX II に接続しているユーザ名と IP アドレスによって識別されるユーザ。	常時
オンライン ヘルプ	オンライン ヘルプへのリンク。	常時
FIPS モード	FIPS モード:有効、SSL 証明書:FIPS モード準拠。	FIPS が有効になっている場合

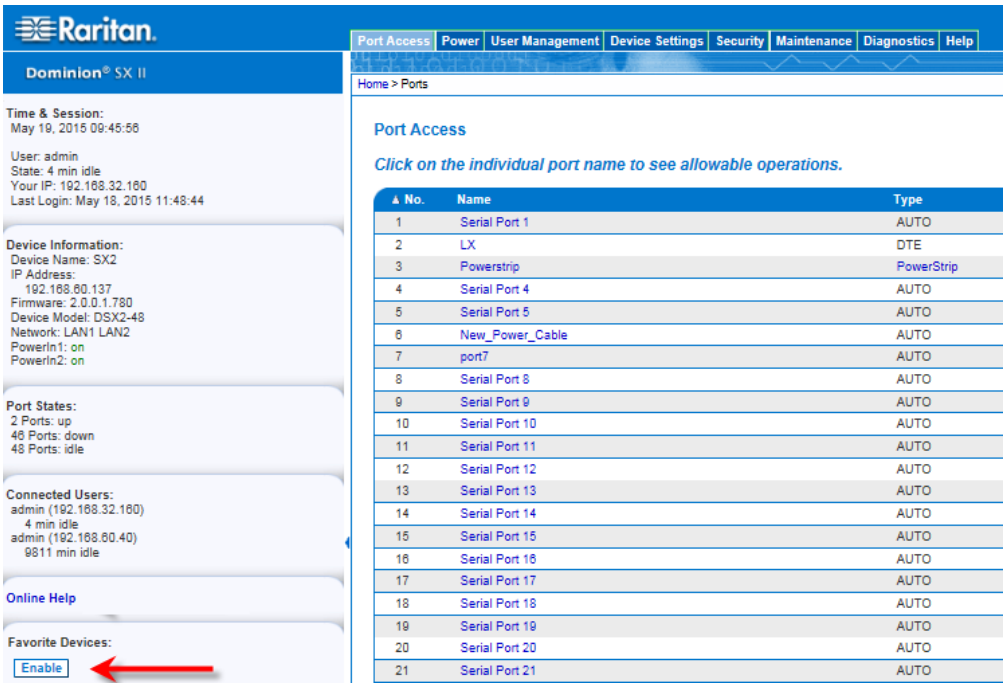
左パネルを崩しそしてパネルの右端に沿ってついている青の矢印の上でクリックして再び拡大します。



お気に入りの有効化

お気に入りの機能を有効化しそのリストを表示します、頻繁にアクセスする SX II デバイスを SX II インタフェースの左パネルのお気に入りデバイスセクションで ″Enable″ をクリックすることで行います。

セキュリティ警告が表示されたときには承諾します。

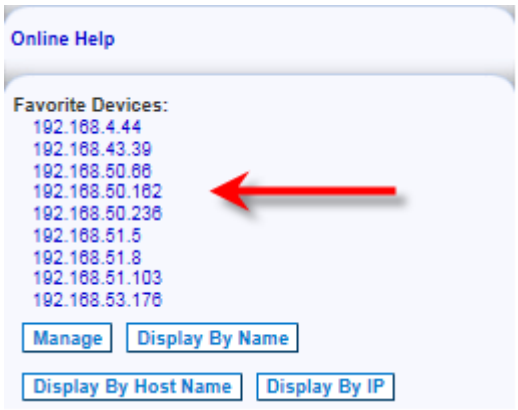


お気に入りの表示方法を変更する

SX II のお気に入りデバイスを表示する方法を対応するボタンの中の一つをクリックして変更します –

- 名前による（デフォルトの表示タイプ）

- IP アドレスによる



- ホストの名前による（もし利用可能であれば）

デバイス サブネットで見つける

このオプションではデバイス サブネット上の SX II デバイスを見つけます。これは SX II デバイスの IP アドレスのサブネットです。

このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。

この機能を使用すると、複数の SX II デバイスが相互に作用し合い、自動的に構成を拡張します。

SX II リモート コンソールは、SX II のサブネット内の SX II デバイスおよびその他の Raritan デバイスを自動的に検出します。

▶ デバイス サブネット上のデバイスを検出

1. [Manage] > [Discover Devices] – [SX II Subnet] を選択します。

デバイス探索 – SX II サブネット ページが表示されます。

2. 更新をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

デバイスを お気に入りリスト に追加

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. Add をクリックします。

見つけたデバイスにアクセスする

- デバイス名またはそのデバイスの IP アドレスをクリックします。新しいブラウザが開き、そのデバイスが表示されます。

Ch 4 ターゲットへのアクセス

ターゲット デバイスはリモート コンソールのポート アクセス ページから（RSC）を用いてアクセスできます。そしてラックでは command line interface（CLI）コマンドライン インタフェース。

ターゲットはダイレクト ポート アクセスによってもアクセスでき、その場合 SX II 経由直接ターゲットに接続し、中間の手続きを必要としません。

この章ではリモート コンソールト CLI からの接続について説明します。

この章の内容

ポートアクションメニューのオプション - ターゲットを接続、切断、電源オン、電源オフ、と電源再投入

SX II にウエブ ブラウザからログオンすると、SX II のポート アクセス ページが表示されます。詳しくは、「ポート」ページを参照してください。 *SX II ポート クセス ページ"参照* 『29p. の*"SX II ポート アクセス ページ"*参照 』。

ポート アクセス ページから、ポートアクション メニューを用いてターゲットと SX II に接続されている電源タップの接続、切断、あるいは電源の制御を行います。

いったん接続されると、ターゲットを Raritan Serial Console (RSC)をで管理できます。参照 *Raritan シリアル コンソール (RSC) ヘルプ*『48p. 』。

ターゲットあるいは電源タップにアクセスするにはその許可を持っている必要があります。

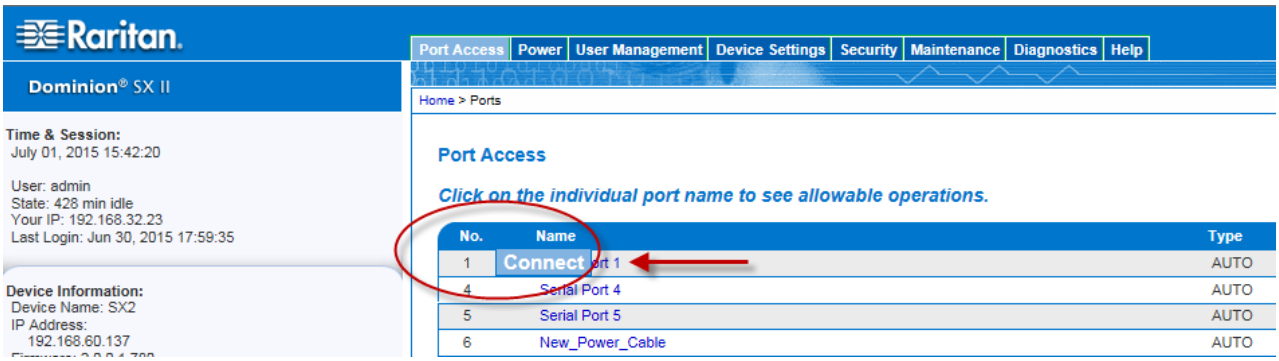
▶ ターゲットあるいは電源タップに対するポート アクション メニューにアクセスする

1. マウスをリストの中のターゲットのポートの名前の上に持っていきマウスでクリックします。

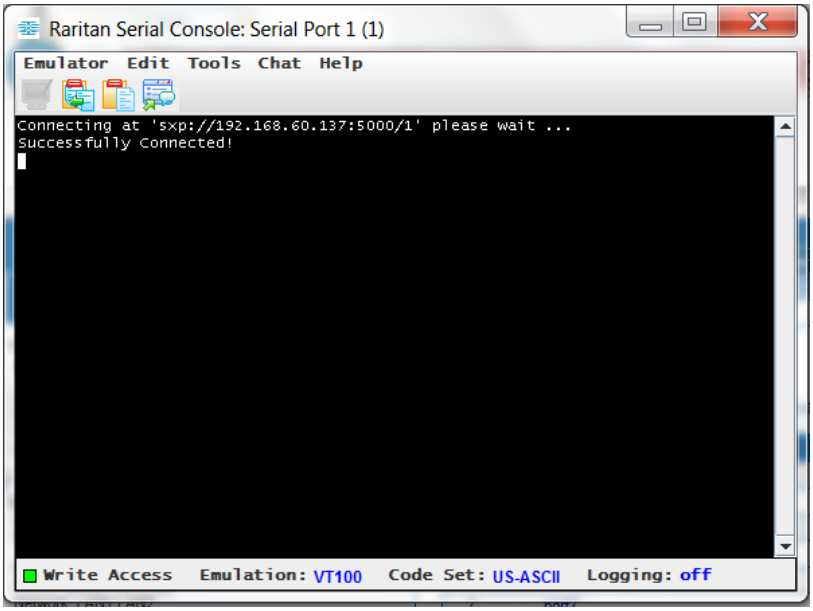
   ポート アクション メニューが表示されます。

   ポート アクション メニューには、ポートの状態と可用性に応じて、その時点で利用可能なオプションだけが表示されます。
2. 対象のポートに対して希望するメニュー オプションを選択して実行します。

- *ターゲットあるいは電源タップに接続する* 『38p. の"*ターゲットに接続する*"参照 』
- *ターゲットあるいは電源タップの切断* 『39p. 』
- *ターゲットの電源をオンにする* 『40p. の"*ターゲットあるいは電源タップのでで電源オン*"参照 』
- *ターゲットの電源をオフにする* 『41p. の"*ターゲットあるいは電源タップの電源オフ*"参照 』
- *ターゲットを電源再投入にする* 『42p. の"*ターゲットを電源再投入する*"参照 』



この後 Raritan Serial Console (RSC)を接続することができます。ターゲットに接続すると、RSC は新しいウインドウに開きます。参照『Raritan シリアル コンソール (RSC) ヘルプ』。



もし SX II にダイレクト ポート アクセスの設定がしてあると、この代わりに、ダイレクト ポート アクセスで接続することもできます。

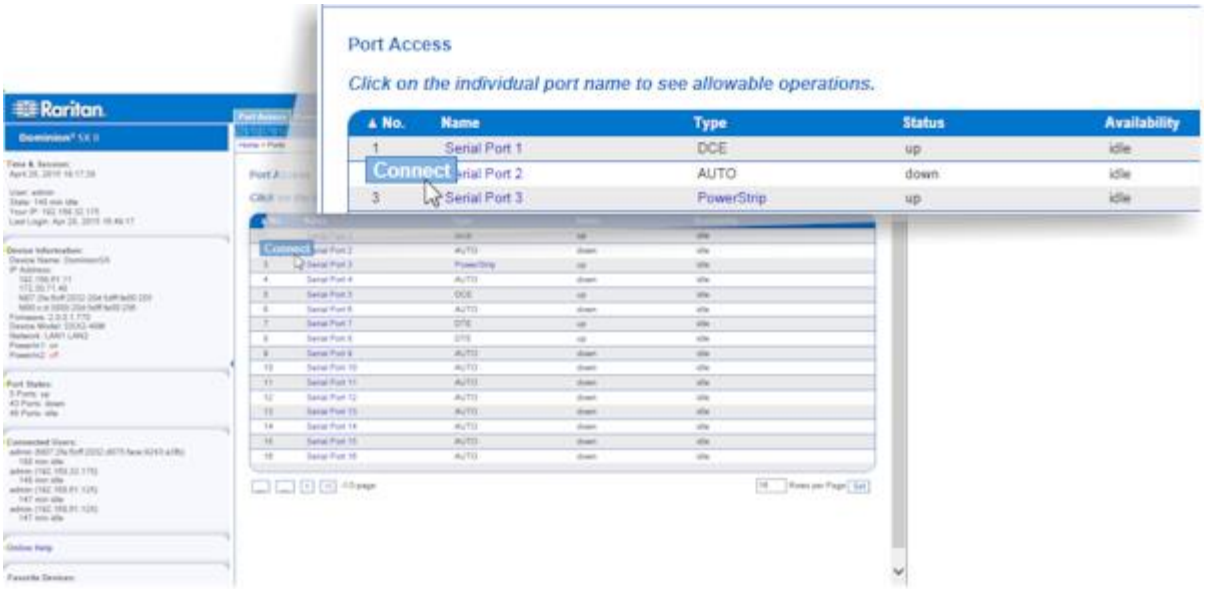
さらにコマンドラインインタフェースでターゲットに接続することもできます。参照 ***CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源再投入*** 『42p. 』。

ターゲットに接続する

ターゲット デバイスに新規の接続を作成します。

SX II リモート コンソールから、Raritan Serial Console (RSC)が新規のウインドウに開きそこからターゲットを管理します。

もしターゲットにローカルなコンソールから接続していると、ターゲットにコマンドラインインタフェースでアクセスします。参照 ***Raritan シリアル コンソール (RSC) ヘルプ*** 『48p. 』 および ***CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源再投入*** 『42p. 』。

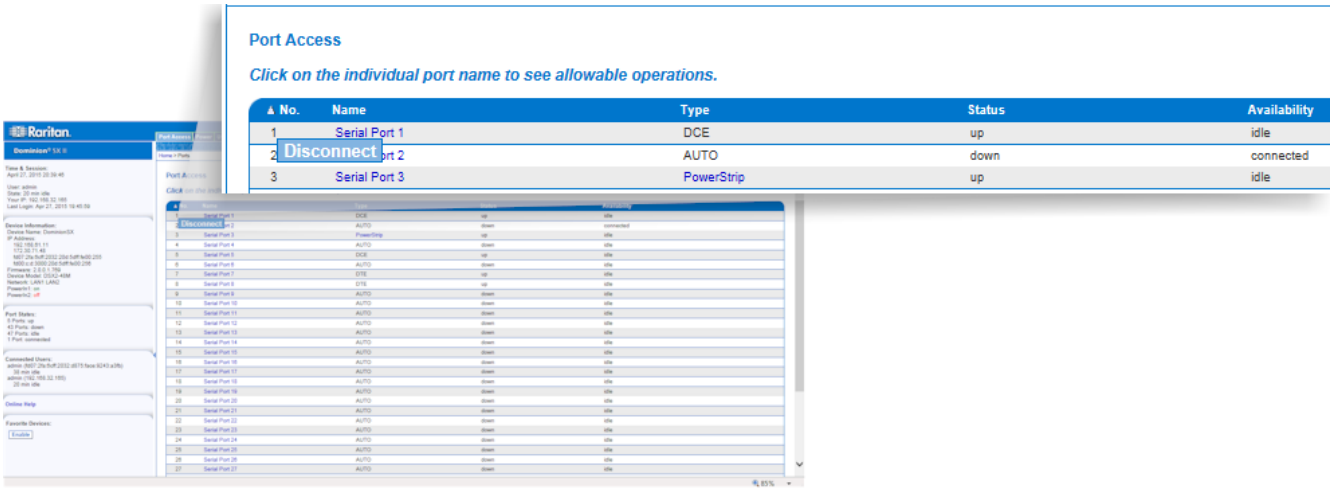


ターゲットあるいは電源タップの切断

いったんターゲットあるいは電源タップに接続しポートの状態がアップである場合、ポート アクション メニューの中のの切断メニューオプションが使用可能となっています。

切断をクリックするとターゲットあるいは電源タップを切断し Raritan Serial Console (RSC) ウインドウを閉じます。またウインドウの X アイコンをクリックするか Exit メニューオプションを用いることもできます。

参照 ***Raritan シリアル コンソール (RSC) ヘルプ*** 『48p. 』 および ***CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源電源再投入*** 『42p. の"***CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源再投入***"参照 』。

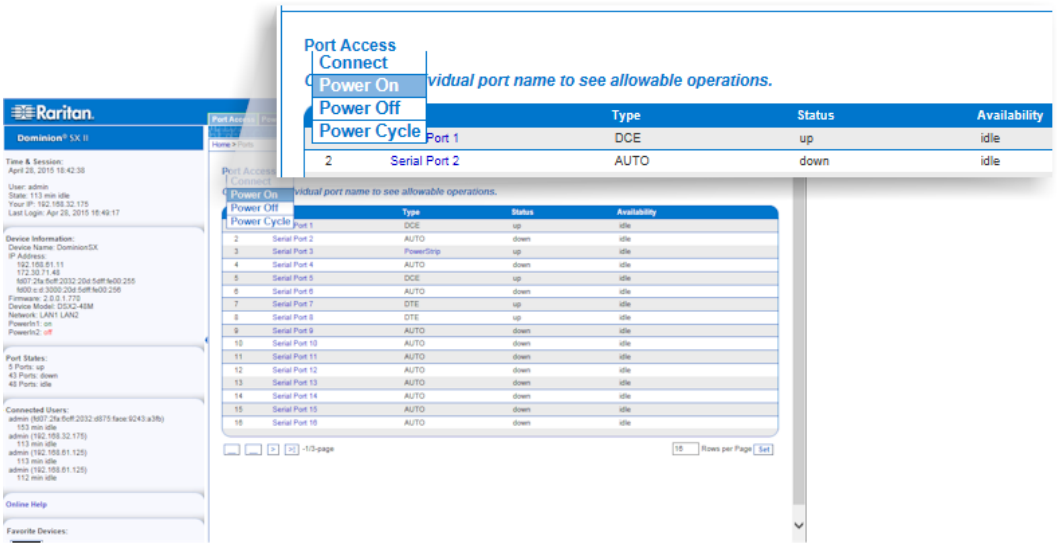


ターゲットあるいは電源タップので電源オン

リモート コンソールから関連する出力端を通じてターゲットの電源をオンにする。

このオプションはターゲットに関連した 1 つあるいはそれ以上の電源があり、かつあなたがターゲットの電源を管理する許可を持っているときに表示されます。

これらのアクションは Raritan Serial Console (RSC) あるいは コマンドラインインタフェースを通じて行うこともできます。参照 ***Raritan シリアル コンソール (RSC) ヘルプ***『48p. 』 および ***CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源再投入*** 『42p. 』。



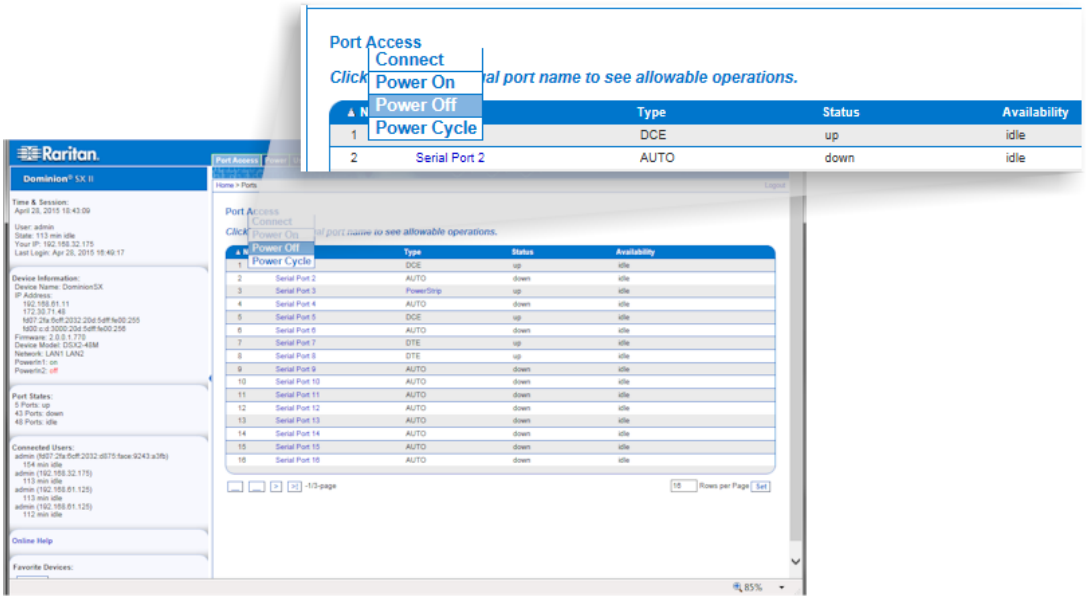
ターゲットあるいは電源タップの電源オフ

ターゲットあるいは電源タップの電源を関連する出力端を通じてオフにします。

このオプションは次の場合にのみ表示されます –

- ターゲットに関連した 1 つあるいはそれ以上の電源があり、
- かつあなたがターゲットの電源を管理する許可を持っているとき

これらのアクションは Raritan Serial Console (RSC) あるいは コマンドラインインタフェースを通じて行うこともできます。参照 ***Raritan シリアル コンソール (RSC) ヘルプ***『48p. 』 および ***CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源再投入*** 『42p. 』。



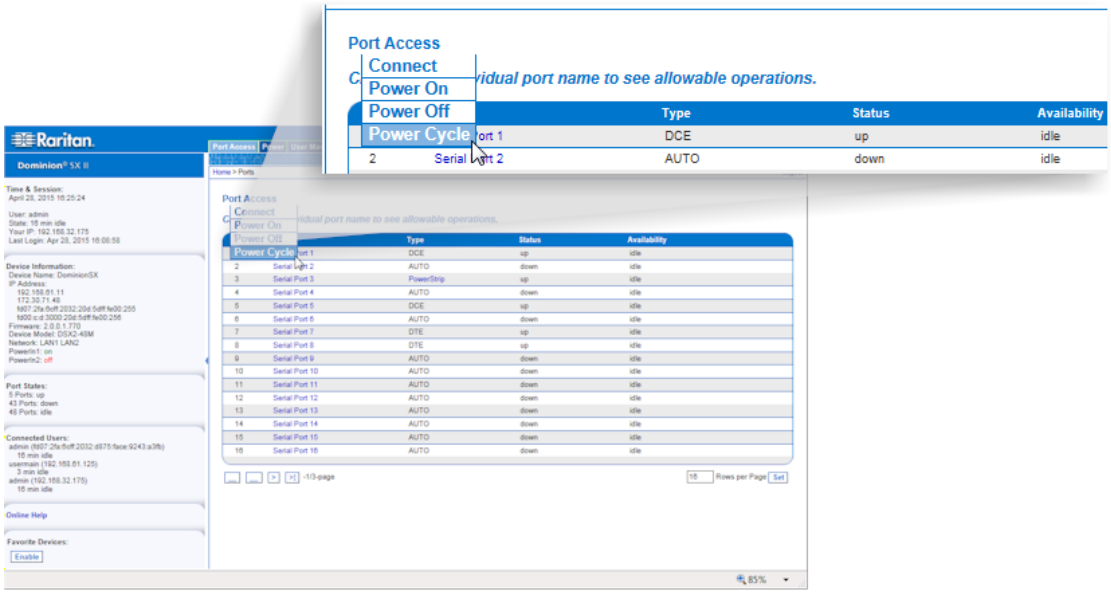
ターゲットを電源再投入する

電源再投入はターゲットあるいは電源タップをそれがプラグインしている出力端を通じてオフしそしてオンに戻すことを可能にします。

このオプションは次の場合にのみ表示されます –

- ターゲットあるいは電源タップに関連した 1 つあるいはそれ以上の電源があり、
- かつあなたが電源を管理する許可を持っているとき

これらのアクションは Raritan Serial Console (RSC) あるいは コマンドラインインタフェースを通じて行うこともできます。参照 *Raritan シリアル コンソール (RSC) ヘルプ* 『48p. 』 および *CLI を用いてターゲットに接続する – ターゲットの接続、切断、電源オン、電源オフと電源再投入* 『42p. 』。



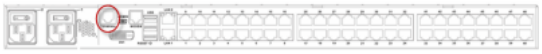
CLI を用いてターゲットに接続する - ターゲットの接続、切断、電源オン、電源オフと電源再投入

ターゲットに接続する前に、ターミナル エミュレーションとエスケープ シーケンスを設定する必要があります。参照 *ターミナル エミュレーションをターゲットにセットします* 『16p. の"*Terminal Emulation を Target にセットします*"参照 』そして *CLI のエスケープ シーケンスをセットします* 『16p. の"*CLI のエスケープ シーケンスをセット*"参照 』。

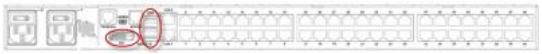
そのラックにいるときに SX II を接続

そのラックにいるときに、必要に応じて次の中から一つを行います –

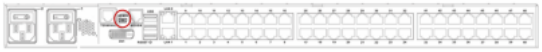
- コンピューターをターミナル ポートに接続します。



- キーボードトレイあるいはKVMコンソールをDVI-DとUSBポートに接続します。



- ラップトップはミニUSB管理ポートに接続します。



SX II ローカル コンソールにローカル ポートから接続するのは各ターゲットデバイスへのアクセスパスと独立したものであることを了解してください。

ビデオ解像度

デフォルトでは、ローカル コンソール ポートのビデオ解像度は 1024x768@60 です。

デフォルトで、モニターは通常それがサポートしている最高の解像度にセットされています。

モニターがいったん SX II ローカル ポート DVI に接続されると、SX II はモニターからその本来の好まれる解像度を含む EDID 情報を得ます。SX II はモニターの好まれる本来の解像度をそれが SX II がサポートしている解像度である限り使用します。もし、それがそうでない場合、SX II はそれがサポートする解像度に、かつモニターの解像度に最も近くに合う解像度に切り替えます。

例えば、もしモニターが本来の解像度が 2048x1600@60Hz のものが SX II に接続されると、SX II はそれが SX II がサポートする解像度ではないことを検知し、サポートしている解像度、例えば 1280x1024@60Hz を選択します。

ターゲットにリモート コンソールを用いて接続し、Raritan Serial Console (RSC)を用いて管理できることを了解しておいてください。参照 ***Raritan シリアル コンソール (RSC) ヘルプ***『48p. 』 および ***ポートアクション メニューのオプション – ターゲットを接続、切断、電源オン、電源オフ、と電源再投入*** 『36p. 』 。

接続 コマンド

ポートに接続します。

```
admin > connect <port number>
```

ポートのサブメニューコマンド

ポートのサブメニューには、エスケープ キー シーケンスで移動できます。

このポートの履歴バッファをクリアします。

```
admin > [portname] > clearhistory
```

このターゲット接続を閉じます。ターゲットが切断された場合、適切な切断メッセージが表示されます。

```
admin > [portname] > close, quit, q
```

このポートの履歴バッファを表示します。

```
admin > [portname] > gethistory
```

ポートの書き込みアクセスを取得します。

```
admin > [portname] > gethistory
```

ターゲット セッションに戻ります。

```
admin > [portname] > return
```

接続されたターゲットに切断を送信します。

```
admin > [portname] > sendbreak
```

ポートの書き込みアクセスをロックします。

```
admin > [portname] > writelock
```

ポートの書き込みアクセスのロックを解除します。

```
admin > [portname] > writeunlock
```

このポートの電源状態を尋ねます。

```
admin > [portname] > powerstatus
```

このポートの電源のオン/オフを反転します。

```
admin > [portname] > powertoggle
```

ターゲットの電源を投入します。

```
admin > [portname] > poweron
```

ターゲットの電源切断します。

```
admin > [portname] > poweroff
```

ターゲットを電源再投入にします。

```
admin > [portname] > powercycle
```

コマンド ライン インタフェースのプロトコル

- IP 接続を介した SSH (Secure Shell)
- IP 接続を介した Telnet
- ローカルポートとミニ USB ポートを経由したローカル コンソール
- ターミナル ポート

もし SX II が内蔵モデムを持ち、コンソールモードが有効化されると、モデムインタフェースもまた CLI でアクセスできます。

多くの SSH/TELNET 応用､例えば PuTTY, SSH Client と OpenSSH Client が利用可能です。これらは次のところにあり、そこからインタネットでダウンロードできます。

コマンドラインインタフェースの部分サーチ

最初の数文字を入力してキーボードのタブキーを押すと、特定のコマンドを探りあてます。

コマンドラインインタフェース（CLI）は文字列がぴったりの一致をすると入力を完成させます。

たとえば、

```
admin > Config > us
```

と入力してタブキーを押すと、次の結果を戻します `users`。

ぴったりの一致が見つからないと、CLI の階層レベルで同じレベルにあるすべてのコマンドで一致する可能性のあるものがリストされます。

たとえば、

```
admin > Config > User > add
```

と入力してタブキーを押すと、次の結果を戻します `addgroup` および `adduser`。

この場合、コマンドの続きを入力して候補が 1 つだけになるようにし、タブ キーを押してコマンドを入力を完成させます。この代わりに、リストからコマンドを使うこともできます。

コマンドラインインタフェースでのヒント

- コマンドがリストとして表示されると、それらはアルファベットの順になっています。
- コマンドでは、大文字と小文字は区別されません。
- コマンドに対してデフォルトの引数を表示しない場合、そのコマンドに対する現在の設定値が表示されます。
- コマンドのパラメータは通常パラメータ-値のペアでパラメーターの名前に続いてスペースそして値となっています。
- コマンドの後ろに疑問符（ ? ）を指定するとそのコマンドに特定のヘルプが表示されます。

コマンドラインインタフェースにおけるショートカット

- 直前のエントリを表示するには、上方向キーを押します。
- 最後に入力した文字を削除するには、バックスペース(Backspace) キーを押します。
- 誤ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、Ctrl キーを押しながら C キーを押します。
- キーボードの Enter キーを押すと、コマンドが実行されます。
- キーボードのタブを押すとコマンドを完成とします。タブはまたパラメーターと値を完成とします(もし値が列挙されたセットの部分となっていれば)。

コマンドラインインタフェースの高レベルコマンド

CLI はメニューをベースとしています。いくつかのコマンドは異なったコマンドセットのメニューに移動します。

次の共通のコマンドはコマンドラインインタフェース (CLI) のすべてのレベルで使用されます –

- `top` – CLI 階層の最上位レベル、つまり username プロンプトに戻ります。
- `history` – (履歴) SX II の CLI で入力した最後の 200 個のコマンドが表示されます。
- `logout` – (ログアウト) ユーザを現在のセッションからログアウトします。
- `quit` – (中止) ユーザを CLI 階層の 1 つ上に戻します。
- `help` CLI 構文の概要が表示されます。

Ch 5 Raritan シリアル コンソール (RSC) ヘルプ

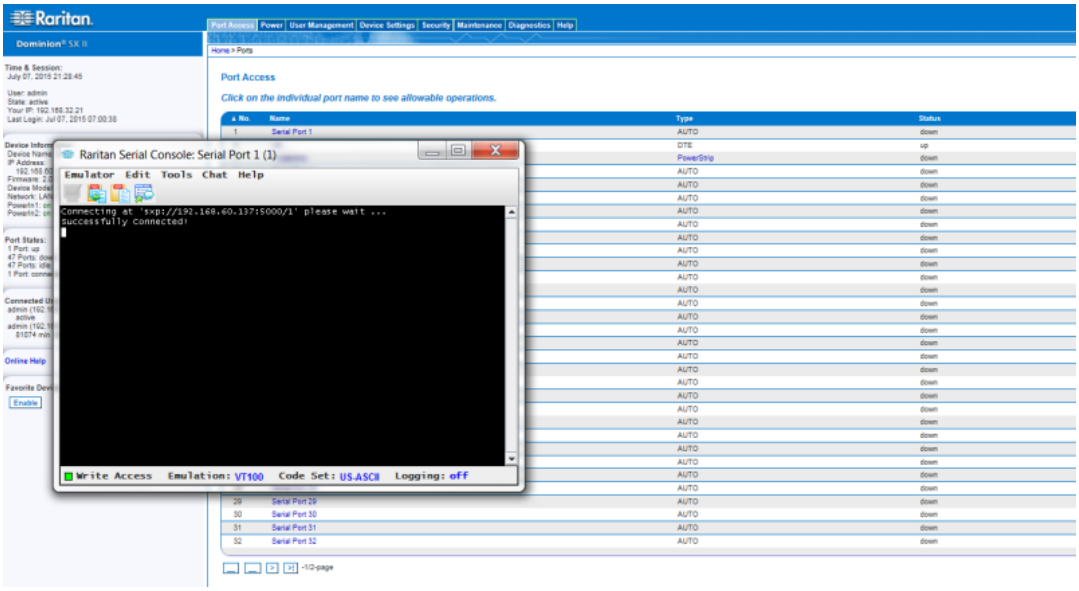
Raritan Serial Console (RSC)を SX II リモートコンソールからシリアルなターゲットに接続するのに使用します

あるいは、RSC をスタンドアローンのクライアントとしてインストールします。

RSC スタンドアローンのクライアントは SX II の IP アドレスとターゲットのポート番号を直接ターゲットに接続するのに用い、したがってリモートコンソールを接続しそしてターゲットに接続するという必要はありません。詳細については、次を参照してください。 スタンドアローン Raritan シリアル コンソールのインストール。

次の Raritan のサポートウエブサイトからスタンドアローンの RSC をダウンロードできます。 *http://www.raritan.com/support* *http://www.raritan.com/support*参照先 。

注:目標にはダイレクト ポート アクセスとコマンドラインインタフェース(CLI) からアクセスできます。



この章の内容

スタンドアローン Raritan シリアル コンソール の必要条件

Raritan Serial Console (RSC)のサポートには次の必要条件が満たされることが必要です。

- 最低 1GHz 512 MB RAM の PC
- Java™

  SX II のリリースノートで必要なバージョンを見てください。

  もし、コンパティブルなバージョンの JRE を持っていない時には、次の場所に行き *http://www.java.com* 『*http://www.java.com*参照先 』「『いまダウンロードする」のボタンをクリックしてください。

あなたのシステムはオペレーティングシステムとブラウザによっては設定の調整が必要かもしれません。JRE は JRE のダウンロードと共に設定の指示も提供しています。参照
http://www.java.com/en/download/help/testvm.xml
『*http://www.java.com/en/download/help/testvm.xml ¥o*
*http://www.java.com/en/download/help/testvm.xml*参照先 』で現在インストールされている JRE のバージョンを知ることができます。

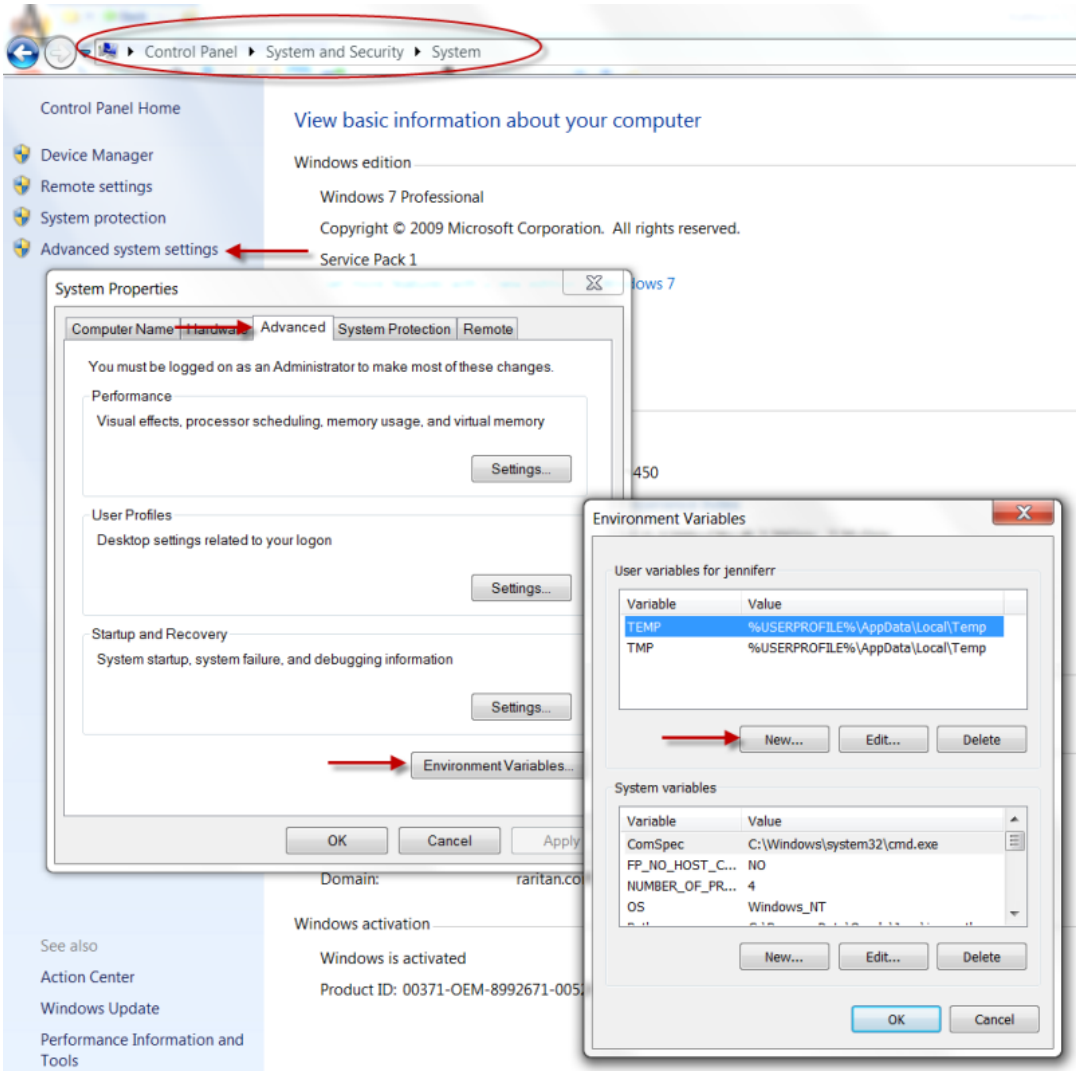
Java がコマンドラインからスタートできることを確認してください。

これを行うには、環境変数の設定が必要です。Java がインストールされたパスの正確なコピーを書き留めておきます（このパス情報は後程使います）。

ウインドウズ OS の変数をセットしスタンドアローン Raritan Serial Console (RSC)をインストールする

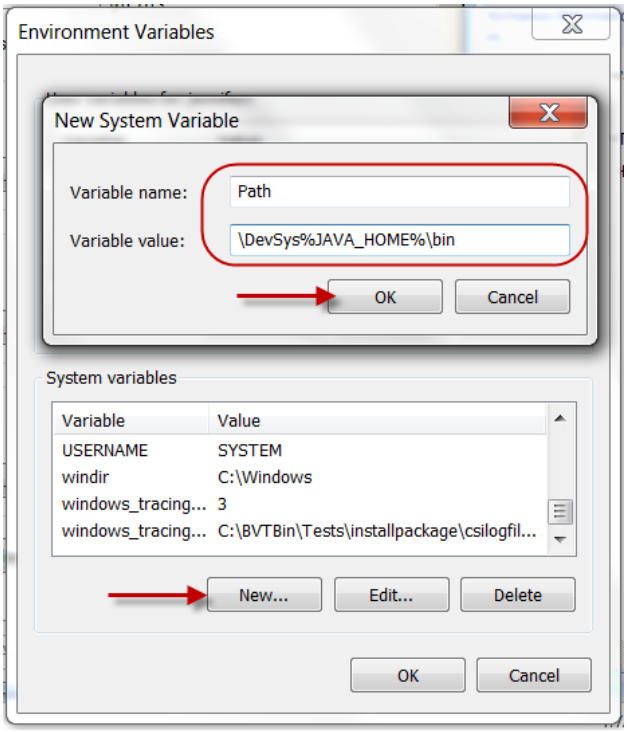
1. Start > Control Panel > System を選択します。
2. Advanced タブをクリックした後、Environment Variables をクリックします。

3. System variables のセクションで、 New をクリックします。



4. Java のインストーラされたパスを書き込みます。
5. 新システム変数ダイアログの変数値ブロックの入力欄の変数名ブロックに JAVA_HOME を加え、そして前に書き留めた Java のパスを入力します。
6. OK をクリックします。
7. PATH 変数を選択し、Edit をクリックします。
8. 現在の変数値の終わりに %JAVA_HOME%¥bin を加えます。文字列の前の値と新しい値とをセミコロン (;) で分割することを忘れないでください。

9. OK をクリックします。



10. CLASSPATH 変数を選択し、Edit をクリックします。
11. CLASSPATH 変数の値が正しく設定されたことを確認します、すなわち、その値は 1 つのピリオド(.) を持っているはずです。もし、何らかの事情で、CLASSPATH 変数の定義がない場合、1 つそれを創ります。

次に、Raritan Serial Console (RSC)をウインドウズ OS にインストールします。

RSC をインストールするには管理者特権が必要です。

1. Windows ® マシンにログインします。
2. インストール ファイル RSC-installer.jar をダウンロード (または既知の場所からコピー) します。
3. その実行可能ファイルをダブルクリックしてインストーラープログラムをスタートします。鮮やかなページが開きます。
4. Next をクリックします。インストレーションパス のページが開きます。
5. 必要なら、パスを変更します。
6. Next をクリックします。インストレーションプログラム のページが開きます。

注:RSC のスタンドアローン バージョンは Raritan のサポートウエブサイトから利用できます。
http://www.raritan.com/support/sup_upgrades.aspx
『http://www.raritan.com/support/sup_upgrades.aspx参照 』

7. Next をクリックします。ウインドウズ ショートカットのページが開きます。
8. ショートカットのためのプログラムグループを選択します。
9. Next をクリックします。インストレーション終了のページが開きます。
10. Done をクリックします。

Linux OS 変数をセッし、スタンドアローン Raritan Serial Console (RSC)を LInux にインストールする

Java™を特定のユーザのためにセットするには、 /home/Username フォルダーにある.profile ファイルを開き編集します。

Java をすべてのユーザのためにセットするには、あなたの /etc フォルダーにある .profile ファイルを開きます。

1. あなたのパスをセットする次のラインを見つけます

```
export
PATH=$PATH:/home/username/somefolder
```

2. このラインの前にあなたの JAVA_HOME をセットする必要があり、そしてあなたの PATH を変更してそれを含むようにし、次のラインを追加します

```
export
JAVA_HOME=/home/username/j2sdk1.6/
export PATH=$PATH:$JAVA_HOME/bin
```

3. ファイルを保存します。

Raritan Serial Console (RSC) をインストールするには管理者特権が必要です。

1. Linux マシンにログオンします。
2. インストール ファイル RSC-installer.jar をダウンロード (または既知の場所からコピー) します。
3. ターミナル ウィンドウを開き、インストーラが保存されているディレクトリに移動します。
4. 次をタイプします *java -jar RSC-installer.jar* Enter キーを押してインストーラーを走らせます。
5. 最初のページをロードした後 Next をクリックします。インストレーションパス 設定のページが開きます。

a. RSC をインストールするディレクトリを選択して、Next をクリックします。
b. Browse をクリックして、デフォルト以外のディレクトリに移動します。
c. インストールが完了したら、Next をクリックします。
d. もう一度 Next をクリックします。インストールは完了です。最後のページはアンインストールのプログラムのある場所と自動インストールのスクリプトを生成するオプションを提供しています。

6. Done をクリックして、インストール ウィンドウを閉じます。

UNIX OS の変数をセットする

最新の Sun Solaris™の JRE™ をチェックするには

1. Sun Solaris デスクトップのターミナル ウィンドウを起動します。
2. 次をコマンドラインにタイプします `java-version` そして Enter を押します。現在インストールされている Java Runtime Environment (JRE) のバージョンが表示されます。
   - あなたのパス変数が Java バイナリのインストールされている場所に設定されていない場合は、JRE のバージョンが表示されないことがあります。
   - JRE が「/usr/local/java」にインストールされていると仮定します。あなたの PATH 変数をセットする必要があります。
   - bash シェルのパスを設定するには:

     ```
     export
     PATH=$PATH:/usr/local/java/j2re1.6/bin
     ```

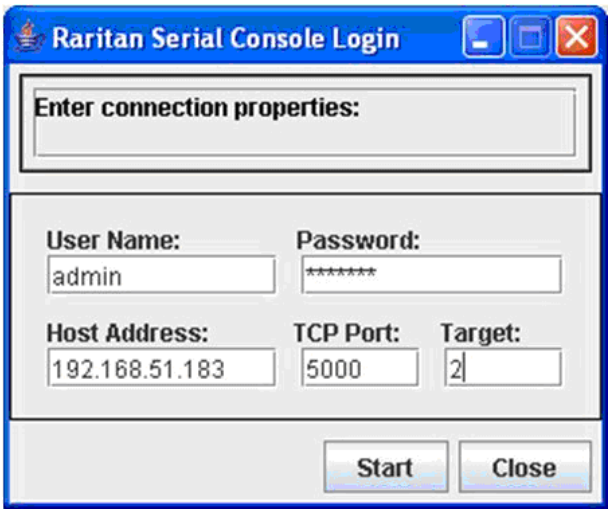
   - tcsh または csh のパスを設定するには:

     ```
     set
     PATH = ($PATH /usr/local/java/j2re1.6/bin)
     ```

   - これらのコマンドは、ログインするたびにターミナルで入力することもできますが、コマンドを .bashrc (bash シェルの場合) または .cshrc (csh または tcsh の場合) に追加するのもよいでしょう。そうすると、ログインするたびに PATH が自動的に設定されています。問題があればシェルの説明書を参照してください。
3. JRE がインストールされると、RSC のインストールに進みます。JRE がなければダウンロードし、そして RSC をインストールします。

RSC を Windows システムに立ち上げる

1. ショートカットをダブルクリックするかスタートプログラムを用いてスタンドアローン Raritan Serial Console (RSC)を立ち上げます。RSC ログイン接続の属性ダイアログが現れます。



2. Dominion SX II の IP アドレス、アカウント情報、および目的のターゲット（ポート）を入力します。
3. Start をクリックします。ポートに接続された状態で RSC が開きます。

注:ローカリゼーション サポートが原因で RSC ウィンドウに読めない文字やぼやけたページがある場合、フォントを Courier New に変更してみてください。Emulator > Settings > Display をクリックし、Terminal Font Properties または GUI Font Properties で Courier New を選択します。

Raritan Serial Console (RSC)の機能

SX II リモート コンソールから Raritan Serial Console (RSC) によってターゲットにアクセスするときそしてスタンドアローン RSC 経由でターゲットにアクセスするとき以下の機能が利用できます。

エミュレーター

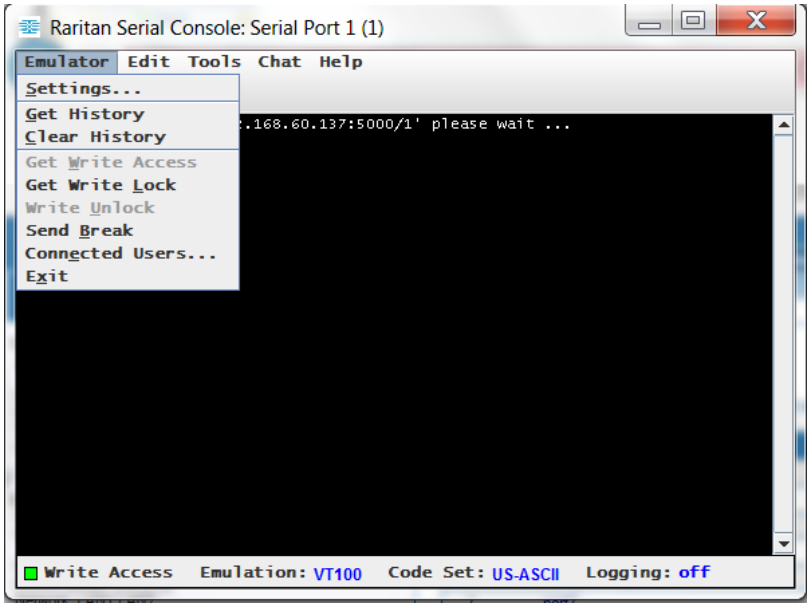
重要:Raritan Serial Console (RSC) セッションは SX II アイドル タイムアウトに影響を受けます。

もし SX II のアイドル タイムアウトの設定をデフォルトからまだ変更していない場合には、RSC セッションがアイドル タイムアウト期間を超えて自動的にクローズするかもしれません。

デフォルトのアイドル タイムアウト設定を変更し そして **RSC** を立ち上げます。 アイドル タイムアウトの設定を変更する際の詳細に関しては ログイン制限 を参照してください。

エミュレーター オプションにアクセスする

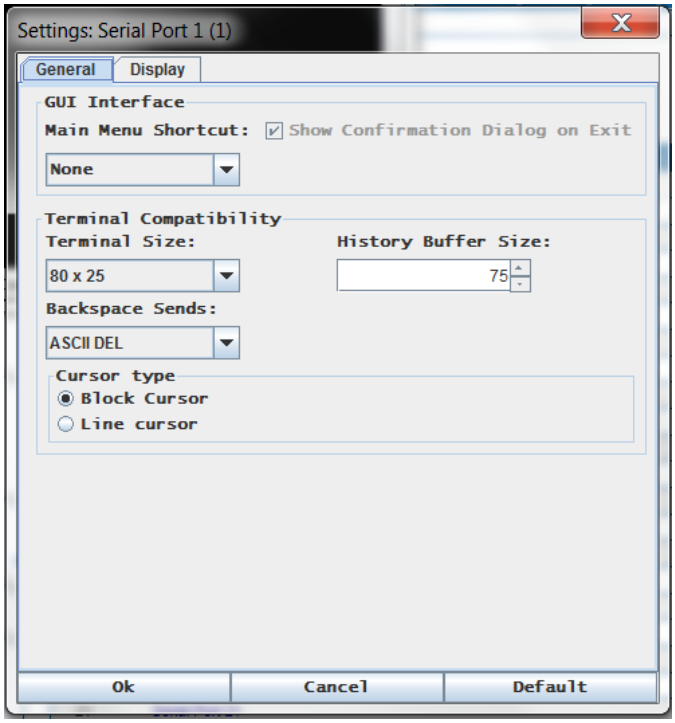
1. エミュレーターのドロップダウン メニューを選択してオプションのリストを表示します。



設定

注:管理者はターミナル エミュレーション設定を Setup > Port Configuration を用いてセットすることができます。

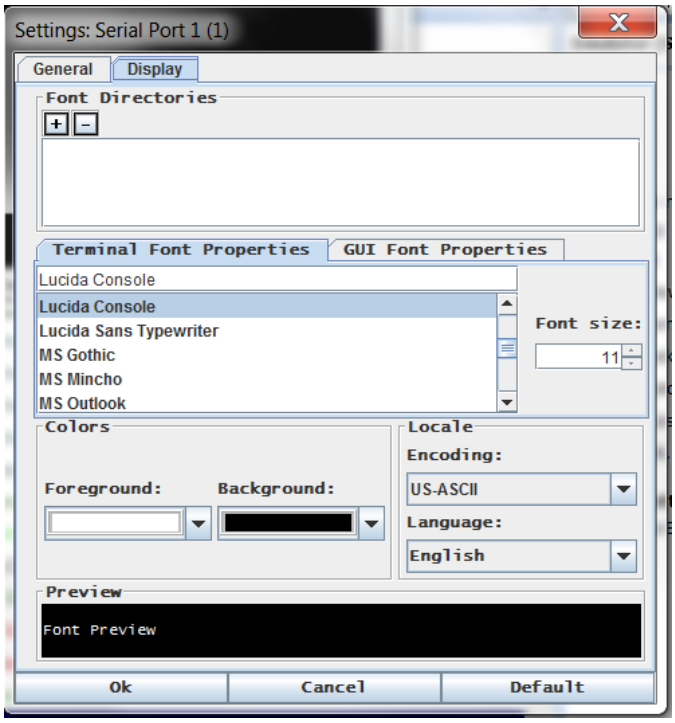
1. Emulator > Settings を選択します。設定スクリーンは General のタブにデフォルトの設定を表示します。



2. メインメニュー ショートカットのデフォルトは「なし」です。これを受け入れるか、あるいはメインメニューショートカット ドロップダウンメニューの以下の中から 1 つを選びます
   - F10
   - Alt
3. 「出るときに確認のダイアログを表示する」のチェックボックスはデフォルトで選択されていますが、好みによって外すこともできます。、
4. ターミナル サイズのデフォルトが選択されています。あるいは異なるサイズをドロップダウンから選ぶことができます。
5. バックスペースが送るものはデフォルトで ASCII DEL となっていますが、バックスペースが送るもののドロップダウンから Control-H を選ぶこともできます。
6. History Buffer (履歴バッファ) サイズのデフォルトは 75 です。値を記入するか矢印でバッファサイズを変更します。
7. カーソルタイプのデフォルトは Block (箱型) カーソルですが、ライン (下線) カーソルをラジオボタンで選択することもできます。
8. OK をクリックします。

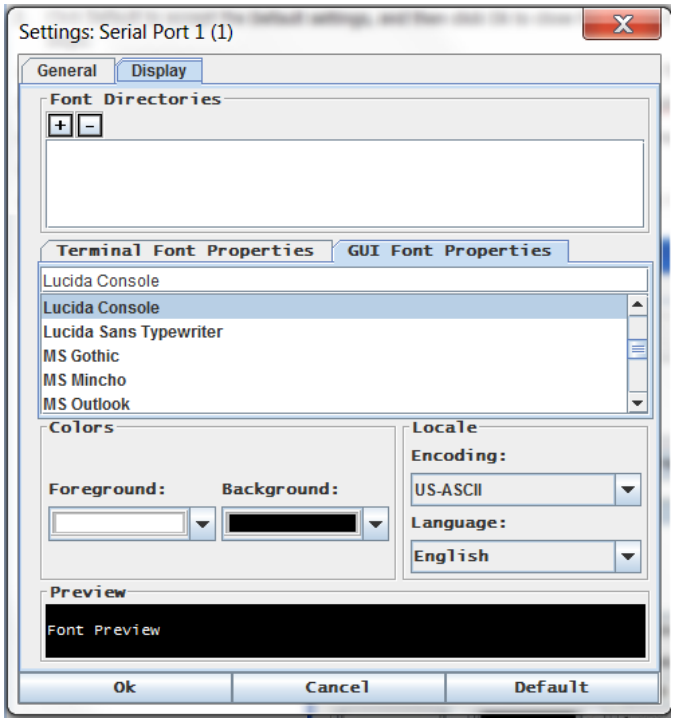
ディスプレイの設定

1. Emulator > Settings を選択し Display（表示）タブをクリックします。



2. 右下の履歴をクリックしてデフォルト設定を受け入れ、そして OK をクリックしてディスプレイの設定ウインドウを閉じます。設定を変えるには以下のステップに従ってください：
   a. ターミナル フォント属性のデフォルトは Arial ですが、ターミナル フォント属性のスクロール リストから 1 つのフォントを選択できます。
   b. GUI Font Properties（フォント属性）のタブをクリックします。

c. フォント属性のデフォルトは Monospace ですが、GUI フォント属性のスクロール リストから 1 つのフォントを選択できます。



注:簡体字のために RSC は EUC-CN のエンコーディングをサポートしています。

3. 次の選択をそれぞれのドロップダウン メニューから行います。
   - 描画色
   - 背景色
4. エンコーディングのドロップダウン リストからオプションのいずれかを選択します。
   - US-ASCII
   - ISO-8859-1
   - ISO-8859-15
   - UTF-8
   - Shift-JIS
   - EUC-CN
   - EUC-JP
   - EUC-KR
5. 言語ドロップダウン リストから以下のいずれかを選択します。
   - 英語
   - 日本語

- 韓国語
- 中国語
- ブルガリア語

6. OK をクリックしてディスプレイの設定ウインドウを閉じます。言語の設定を変更した場合には、 RSC はディスプレイ設定ウインドウが閉じるとその言語に変わります。

注:ローカリゼーション サポートが原因で RSC が立ち上がった時に読めない文字やぼやけたページがある場合、フォントを Courier New に変更してみてください。

履歴を得る

履歴情報はターゲットデバイスのデバッグ、トラブルシュート、あるいは管理上で有用です。来歴を得る機能:

- 最近のコンソールセッションの履歴をターゲットデバイスとの間で行き来したメッセージを表示することで見ることができます。
- 最大 512KB の最近のコンソール　メッセージの来歴を表示します。これによってユーザはターゲットデバイスの出来事を時を追ってみることができます。

サイズの制限値に達すると、テキスト回り込んで、最も古いデータを最も新しいデータで上書きしていきます。

注:履歴データはそれを要求したユーザにだけ表示されます。

セッションの履歴を見るには、Emulator > Get History と選択します。

履歴の消去

- 履歴を消去するには、Emulator > Clear History と選択します。

書き込みロックを得る

ポートへの許可を持つユーザの実が書き込みアクセスを取得できます。書き込み権限を持つユーザはコマンドをターゲット デバイスにコマンドを送ることができます。書き込みロックは RSC で働いているユーザの間で移動させることが可能です。

書き込みロックを可能にするには、Emulator > Get Write Access をクリックします。

- これであなたはターゲットデバイスに書き込み権限を得ます。
- 他のユーザがあなたから書き込み権限を引き取ると、
  - RSC は状態バーの書き込み権限の前に赤いブロックアイコンが表示されます。
  - 現在書き込み権限を持つユーザにメッセージが現れ、そのユーザに他のユーザがコンソールへのアクセスを取ったことを警告します。

書き込みロックを得る

書き込みロックはあなたがそれを使っている間ほかのユーザが書き込み権限を取ることを防ぎます。

1. 書き込みロックを得るには、Emulator > Get Write Lock を選択します。
2. もし書き込みロックが利用できないとき、要求が拒絶された旨のメッセージが現れます。

書き込みロック解除

書き込み閉鎖を得るには、Emulator > Get Write Lock を選択します。

ブレークの送信

Sun Solaris サーバのようなあるターゲットシステムは OK の指示を生成するために文字無し（ブレーク）の送信を要求します。これは Sun のキーボードからの STOP-A の発行と等価です。

書き込み権限を持つユーザのみがブレークを送ることができます。

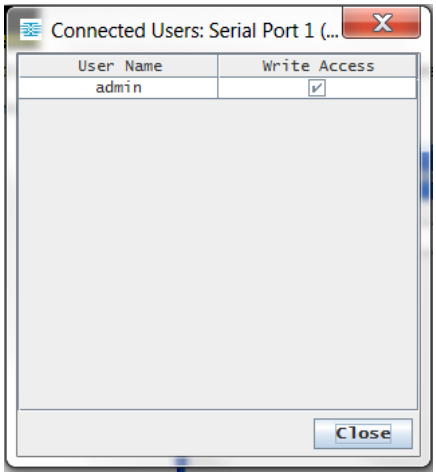
意図した「ブレーク」を Sun Solaris サーバに送るには

1. 書き込み権限を持っていることを確認します。もしそうでなければ、前のセクションの指示に従って書き込み権限を獲得します。
2. Emulator > Send Break を選択します。ブレーク送信確認（Acknowledgement）のメッセージが現れます。
3. OK をクリックします。

接続中のユーザー

接続中のユーザコマンドは現在同じポートに接続している他のユーザのリストを見れるようにするものです。

1. Emulator > Connected Users を選択します。



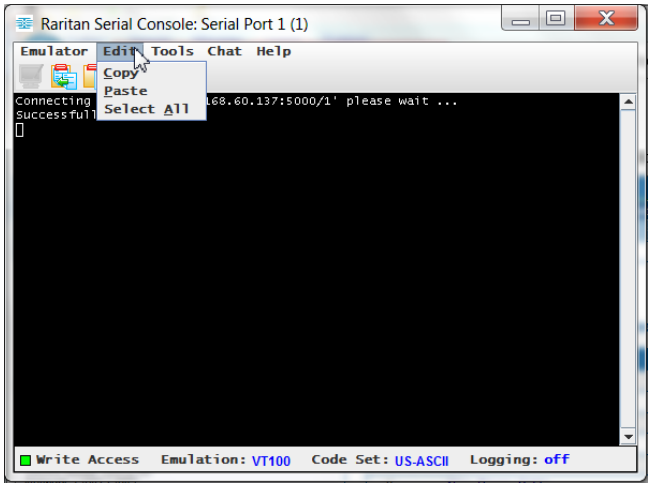
2. 書き込み権限を持つユーザの名前の次の列にチェックマークが現れます。
3. Close をクリックして接続中のユーザーのウィンドウを閉じます。

終了

1. Emulator > Exit を選択して RSC を終了します。終了の確認のメッセージが現れます。
2. Yes をクリックします。

編集

テキストの Copy、Paste と Select All コマンドを使って重要な'テキストの移動や再利用を行います。



全てのテキストをコピー アンド ペーストするには

1. Choose Edit > Select All.
2. Choose Edit > Copy と選択します。
3. カーソルをテキストを貼り付けたい箇所におきます。
4. 1回クリックしてその個所を有効にします。
5. Edit > Paste と選択します。

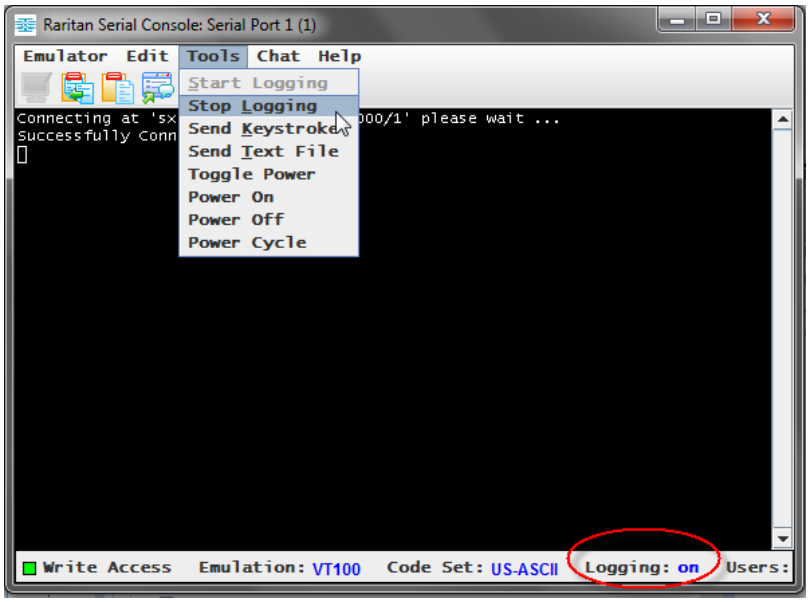
注:RSC においてはコピー アンド ペーストの制限は 9999 行です。

テキストのすべてあるいは部分の行をハイライト、コピー、貼り付けするためのショートカット

- マウスをコピーしたいテキストの上にクリックしてからドラッグします。
- Ctrl+C をテキストのコピーに使います。
- カーソルをテキストを貼り付けたい箇所に置き、その個所でクリックしてそこを有効にします。
- Ctrl+V をテキストの貼り付けに使います。

記録の開始と停止

Raritan Serial Console (RSC)をスタートすると、ステータス バーにある記録指示器が記録がオンかオフかを示します。



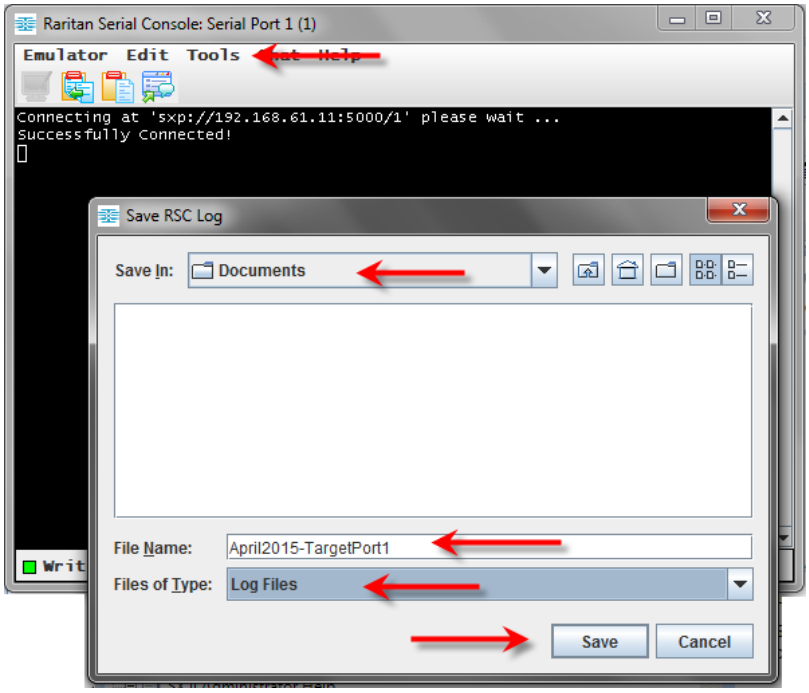
記録を開始

記録開始機能はターゲット デバイスからの生のコンソールデータを集め、あなたのコンピュータのあるファイルに保存します。

1. Tools > Start Logging を選択クリックします。
2. Save RSC Log で既存のファイルあるいは新規のファイル名を指定します。

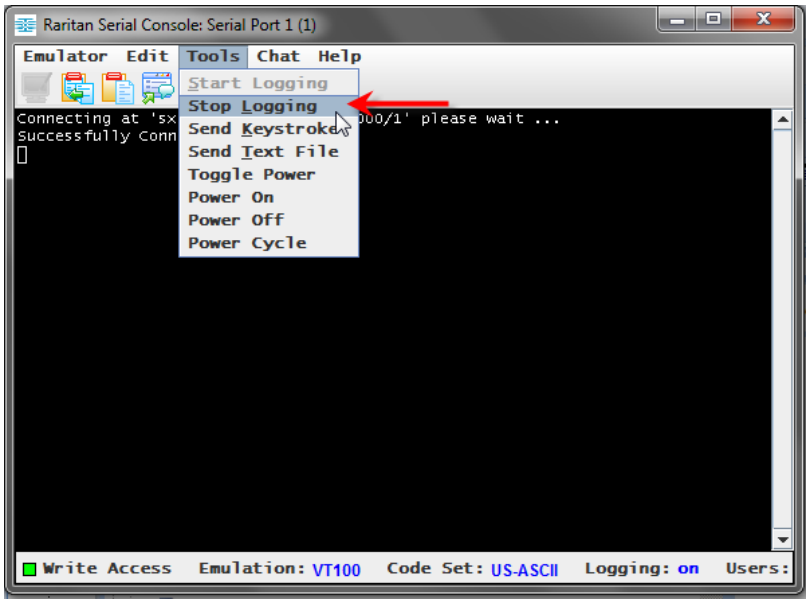
   既存のファイルを記録に選択した場合、それに上書き、追加でき、あるいは新規の名前を与えて新規なファイルとすることができます。

3. ファイルを選択あるいは生成した後 Save をクリックします。

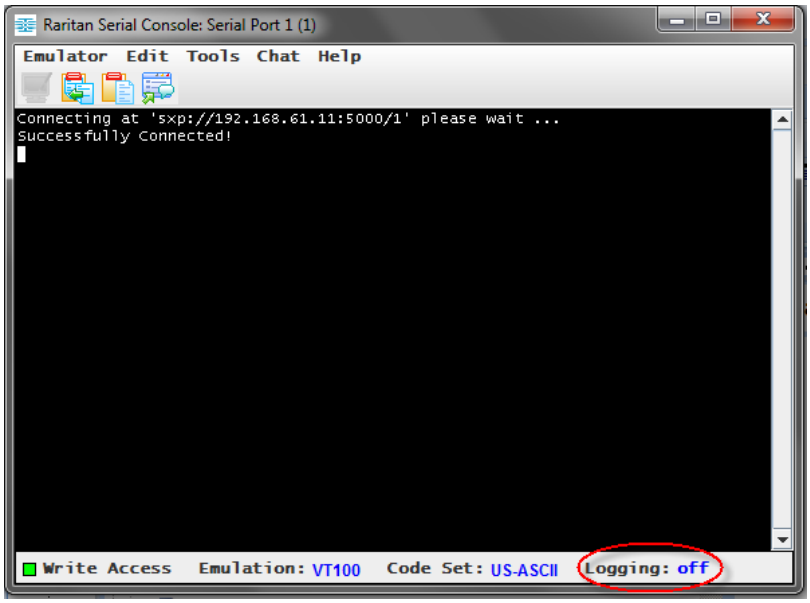


ログを停止

- Tools > Stop Logging を選択クリックします。

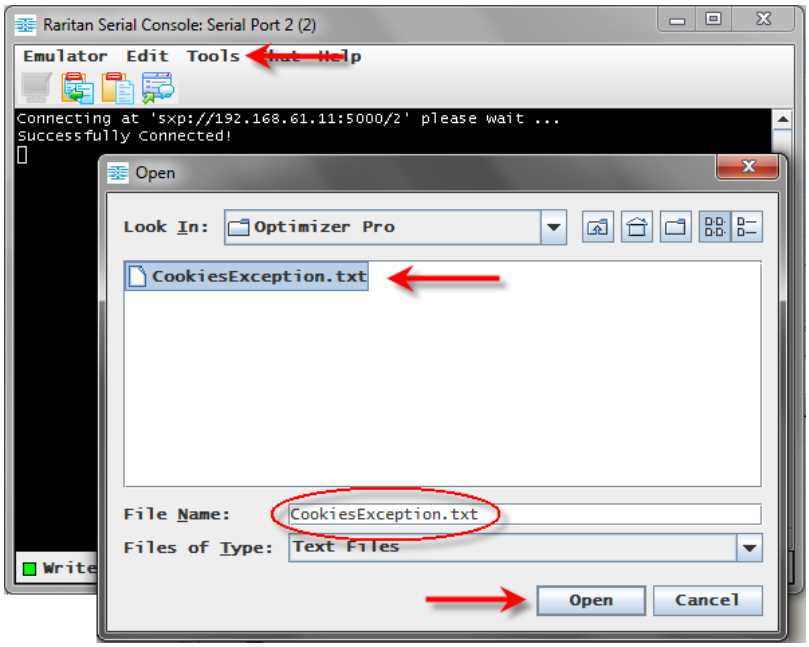


記録は停止します。



テキスト ファイルを送る

1. Tools > Send Text File を選択クリックします。テキストファイルを送る画面が現れます。
2. テキストファイルのディレクトリーを開きます。
3. テキスト ファイルをクリックするか名前を入力します。
4. Open をクリックします。



- Open をクリックすると、Raritan Serial Console (RSC)は選択したファイルがどのようなものであれそれをポートに直接送ります。
- 現在どのターゲットも接続されていない場合には、画面に何も現れません。

注：Mac® とあるいは Safari® を使用していると、この機能を使うためには次のようにします：

1. Safari で、［preferences］（環境設定）を選択します。
2. ［セキュリティ］タブで、［ウエブ サイト設定を管理］を選択します。
3. SX II ウエブサイトの上でクリックします。
4. ドロップダウン ボックスから［安全でないモードで実行］を選択します。
5. Safari を再起動します。

電源を反転

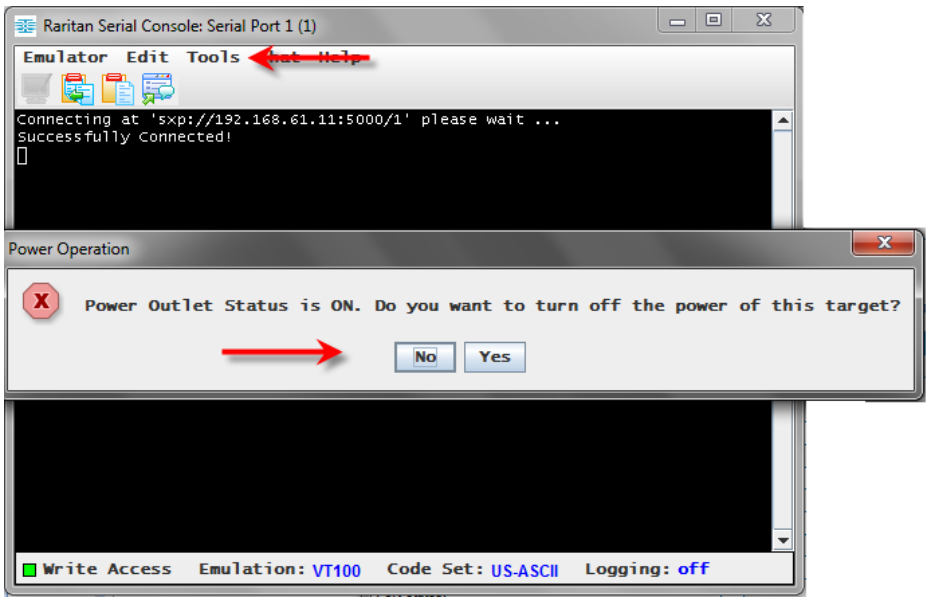
電源反転機能は電源分配ユニット(PDU）上の関連しているコンセントに接続されたデバイスの電源をオンあるいはオフします。例えば、ルーターがその PDU のコンセントの 1 つに接続している場合、ルーターの電源のオン/オフを反転させることができます。

この電源反転機能を使用する前にコンセントとデバイスのターゲットポートへの結びつきを把握していなければなりません。そのデバイスの Device Settings > Port Configuration タブで電源ポートをシリアルターゲットに割り当てます。これをまだ行っていない場合、システムはそのターゲットが電源コンセントに割り当てられていないことを述べたメッセージを表示します。

この機能を実行するにはそのポートに対する制御許可を持っていなければなりません。

1. デバイス（ルーター）のオン/オフを変えるために Toggle Power を選択します。そのコンセント（群）の状態を表示して入力待ちとなります。現在の状態に応じてデバイスのオンオフ切り替えを行えます。
2. No を選択すると、システムは RSC 画面に戻ります。

3. Yes を選択すると、システムはデバイスのターゲットポートに結び付けられたコンセントをオンあるいはオフとする電源コマンドを送ります。



もしハードウエアのエラーのメッセージを受け取った場合、その PDU コマンドは失敗したことを意味します。

ソフトウエアのエラーメッセージを受け取った場合、これはもう一人のユーザが電源コンセントを制御していることを意味し、電源制御コマンドは送ることができません。

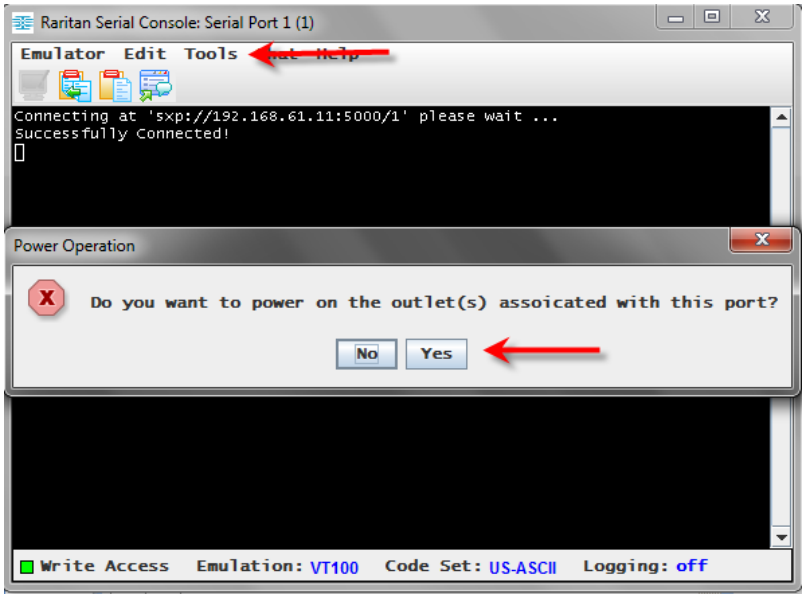
ターゲットの電源をオンにする

このオプションを Raritan Serial Console (RSC)からターゲットの電源をオンにするのに使います。

このオプションはターゲットに関連した 1 つあるいはそれ以上の電源があり、かつあなたがターゲットの電源を管理する許可を持っているときに表示されます。

1. Tools > Power On を選択クリックします。

2. 確認を求めるプロンプトが表示されたら、Yes をクリックします。

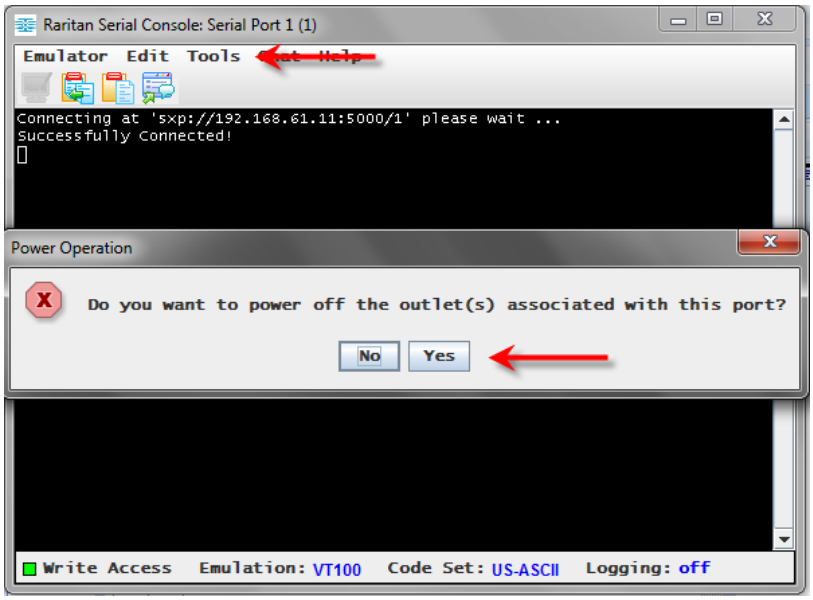


ターゲットの電源をオフにする

このオプションを Raritan Serial Console (RSC)からターゲットの電源をオフにするのに使います。

このオプションはターゲットに関連した 1 つあるいはそれ以上の電源があり、かつあなたがターゲットの電源を管理する許可を持っているときに表示されます。

1. Tools > Power Off を選択クリックします。
2. 確認を求めるプロンプトが表示されたら、Yes をクリックします。



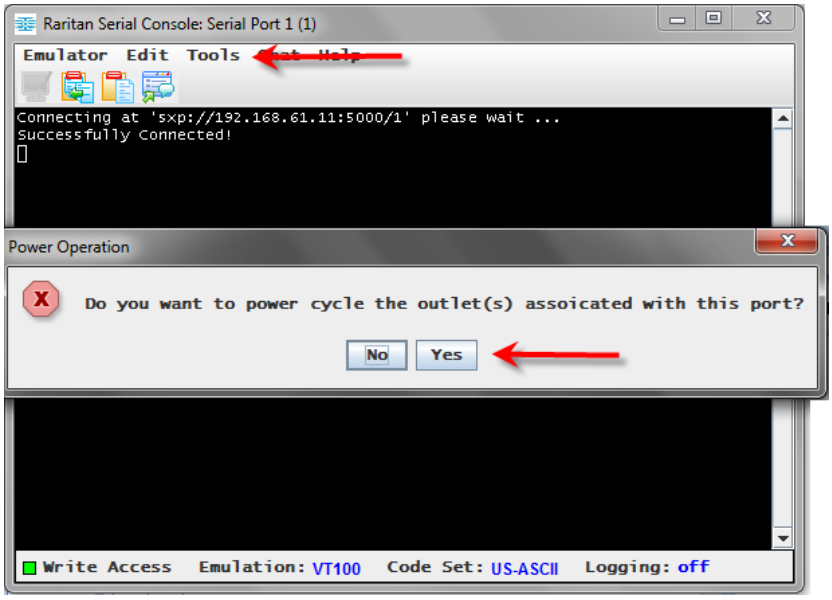
ターゲットを電源再投入する

電源再投入はターゲットをつながれているコンセントを通じてオフに変えそして再びオンに戻すものです。

このオプションは次の場合にのみ表示されます –

- ターゲットに関連した 1 つあるいはそれ以上の電源があり、
- ターゲットの電源が投入されていて（ポートの状態がアップである）
- あなたがターゲットの電源を管理するきゃかを持っている。

1. Tools > Power Cycle を選択クリックします。
2. 確認を求めるプロンプトが表示されたら、Yes をクリックします。



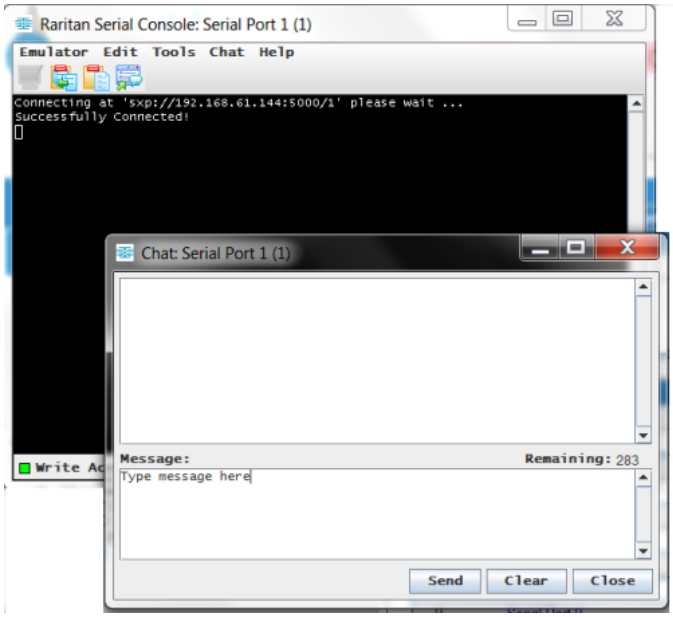
チャット

SSL 上でアクセスするブラウザを用いているとき、Chat と呼ばれる相互にチャットする機能はあなたと他のユーザを同じポートで対話することを可能にします。このチャット メッセージの最大長は 300 文字です。

注:チャットが開始されると、そのポートにログオンしている全ての SSL ユーザのモニター—にチャットウインドウが現れます。あるユーザがあるポートに複数回ログインすると、そのユーザには複数のチャットメッセージは現れません。

チャットを開始するには

- Chat > Chat と選択クリックします。



チャットテキストボックスでテキストを消去するには

- Clear をクリックしてタイプしたテキストを消去します。

ヘルプと説明

ヘルプの話題には Raritan Serial Console (RSC)を操作するためのオンライン援助と RSC に関する公開情報が含まれます。

ヘルプの トピック

- Help > Help Topics を選択クリックします。ヘルプは第 2 のウインドウに表示されます。

Raritan シリアル コンソールについて

- Help > About Raritan Serial Console を選択クリックします。Raritan シリアル コンソールについてのメッセージが表示されます。

Ch 6 SX II 管理

このヘルプは通常管理者によって行われるタスクについての情報が含まれています。それにはユーザグループとユーザの管理、認証とセキュリティの管理、ネットワーク設定の形成等が含まれます。

同じタスクはリモート コンソールあるいは command line interface (CLI) からも行えます。したがってこのセクションはリモート コンソールと CLI セクションに分割されています。

この章の内容

リモート コンソールから SX II を管理する

このセクションは SX II リモート コンソールで実行されるタスクに特定のものです。

コマンドラインインタフェースを用いるタスクの実行についての情報は、次を参照してください。 *command line interface を用いた SX II の管理* 『199p. の″*コマンドラインインタフェース を用いて SX II を管理する*″参照 』。

リモート コンソールからの電源タップの設定

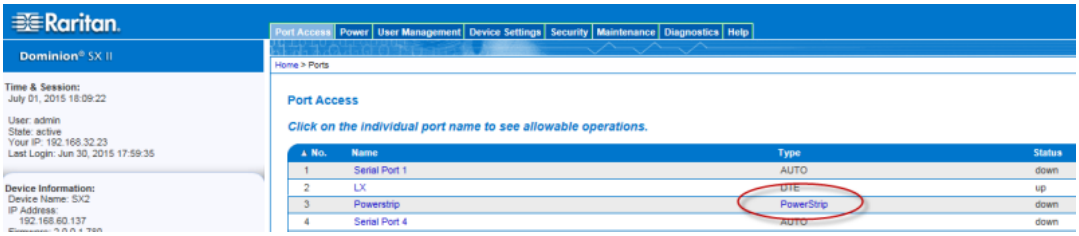
SX II に接続された Raritan PX ラック PDU コンセント（電源タップ）と Baytech のラック PDU の電源タップコンセントを制御できます。

PX を設定することについての情報は、次を参照してください **Raritan PX のオンラインヘルプ**。PX を SX II に接続する方法の詳細には、次を参照してください ***ラック PDU の接続と設定*** 『76p. の"***ラック PDU （電源タップ）の接続と設定***"参照 』。

いったん SX II に接続されると、ラック PDU とそのコンセントを設定できます。

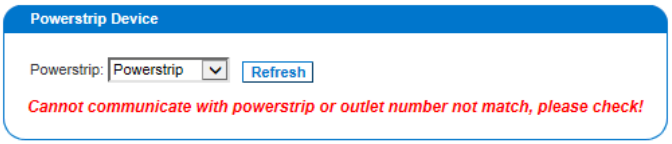
リモート コンソールからの電源タップの設定はここで示されます。あるいは コマンドラインインタフェースをいた場合の。参照 ***CLI を用いた電源タップの設定*** 『200p. 』。

リモートコンソールで、タイプ列の電源タップのリンクをクリックしポートアクセスのページから電源タップのページに素早くアクセスすることができます。



SX II に接続された電源タップがない場合、「パワーストリップが見当たりません」と述べるメッセージがページの電源タップデバイス セクションに表示されます。

電源タップがダウンしているか到達できない場合、【電源タップあるいはコンセントと通信できません、、番号が一致しませんチェックしてください」のメッセージがそのページに赤で表示されます。

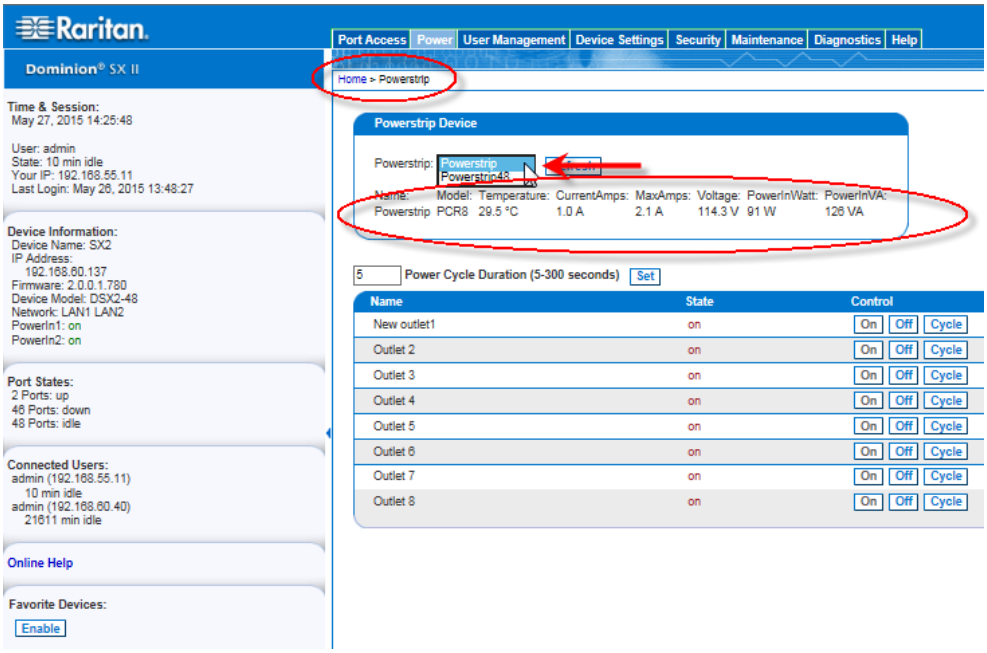


あなたがアクセスの許可を持っていて SX II に接続されている全ての電源タップが電源タップのドロップダウンにリストされています。

現在選択されている電源タップの情報はドロップダウンで表示されています –

- 名前
- モデル
- 温度

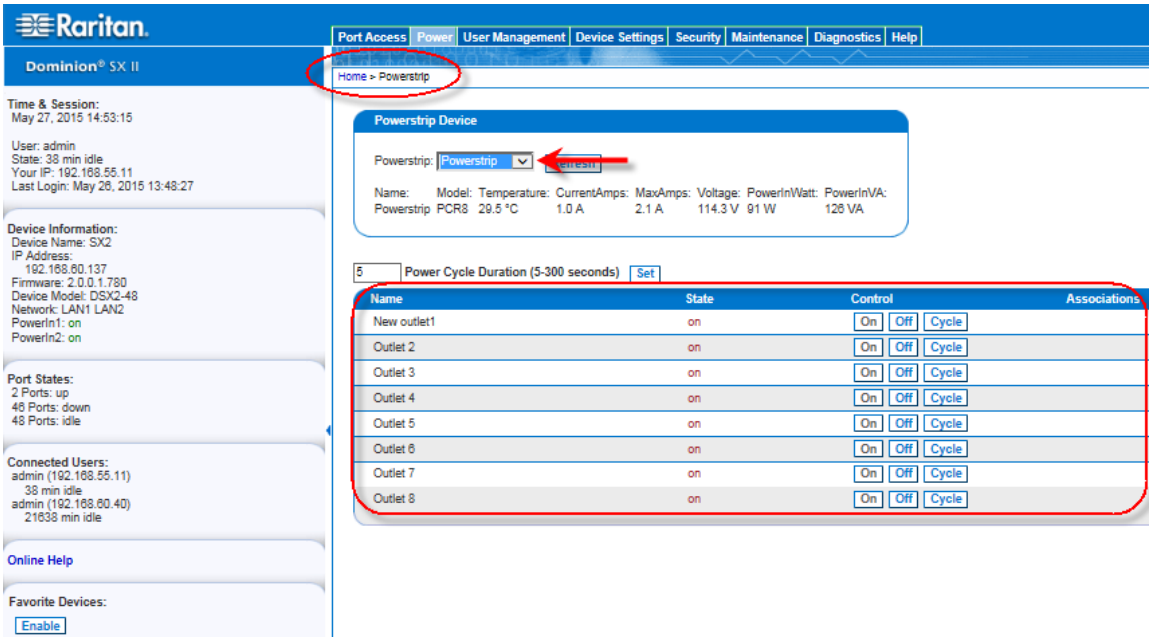
- 電流（A）
- 最大電流（A）
- 電圧
- 電力（W）
- 電力（VA）



現在選択されている電源タップの名称、その現在の状態、そしてもし有効であれば関連するポートが電源タップの情報の下に表示されます。

そのページのオン、オフ、そして電源再投入のボタンを用いて各電源タップの出力を制御します。

ドロップダウンリストから他の電源タップを選択し、その情報を見また制御します。



電源タップのコンセントの制御

コンセントの電源をオンにするには

1. 電源タップのドロップダウンから、電源をオンにしたいラック PDU (電源タップ) を選択します。
2. 電源をオンにするコンセントの横の On をクリックします。
3. 電源オン確認ダイアログ ボックスが開くので、OK をクリックして閉じます。コンセントの電源がオンになり、State 列の表示が "on" になります。

コンセントの電源をオフにするには

1. 電源をオフにするコンセントの横の Off をクリックします。
2. 電源オフ確認ダイアログ ボックスが開くので、OK をクリックして閉じます。コンセントの電源がオフになり、State 列の表示が "off" になります。

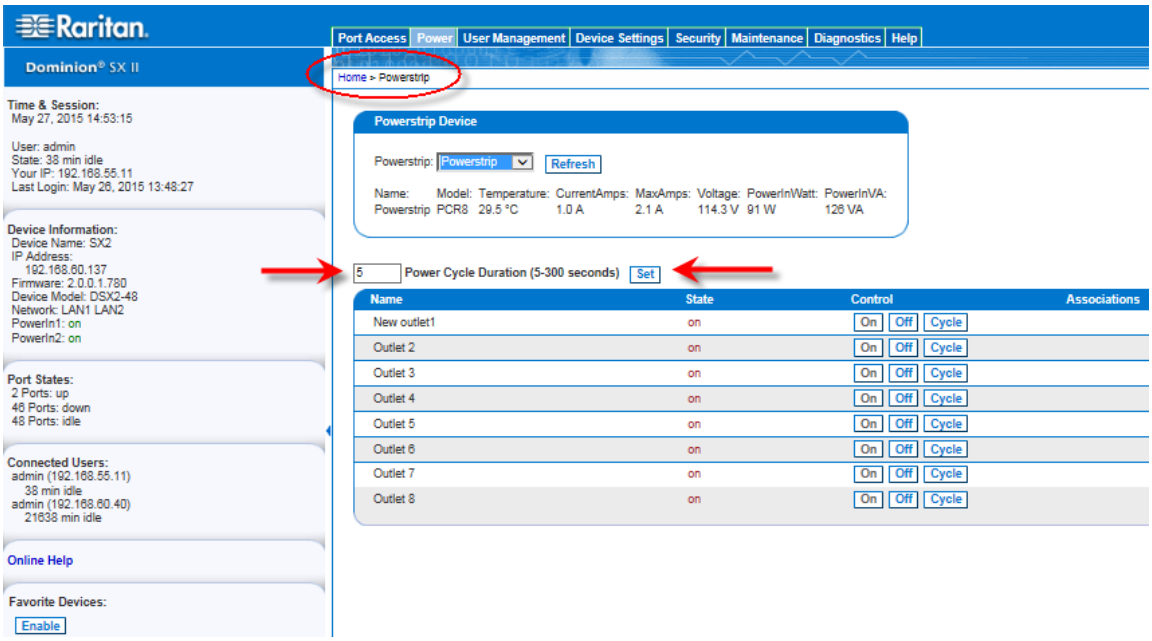
コンセントの電源を再投入するには

1. 電源を再投入するコンセントの横の Cycle をクリックします。電源再投入確認ダイアログ ボックスが開きます。
2. OK をクリックします。コンセントの電源が再投入されます。電源再投入には数秒かかることがあります。
3. 電源再投入が完了すると、電源再投入完了ダイアログ ボックスが開きます。OK をクリックしてこのダイアログ ボックスを閉じます。

デバイスを電源再投入する

電源再投入 コマンドが与えられてコンセントの出力がオフとなりオンに戻るまでの期間を指定するには、それを[電源再投入期間（5-300 秒）]の欄に入力し Set を選択します。

注:PX を SX II に接続するところであれば、パワー電源再投入を 5 秒にすることを勧めます。



ラック PDU （電源タップ）の接続と設定

SX II では、ラック PDU（電源タップ）を SX II ポートに接続できます。SX II ポート設定ページを経由してこれらのポートを電源ポートとして設定することが必要です。

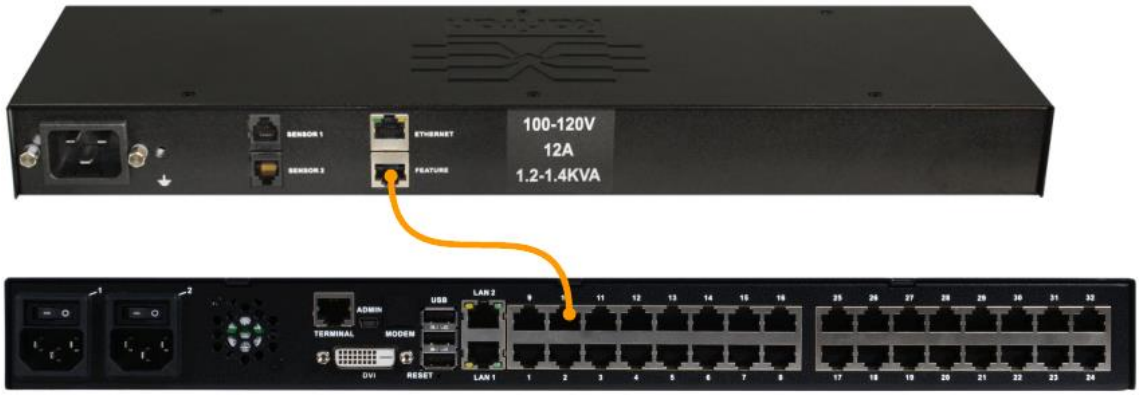
特別な Raritan のケーブルあるいは CSCSPCS -1 Rev.0C アダプター—が SX II のポートをラック PDU のその機能のポート接続するのに要求されます。

Raritan のラック PDU のみがサポートされています。

1. SX II のポートを電源ポートに設定します。
2. ポート設定ページで、電源タップに接続されているポートをクリックしてそのポート編集ページを開きます。
3. そのポートのタイプを「シリアル」から「電源タップ」に変更します。
4. 必要があればポートの名前を変更します。
5. OK をクリックします。SX II は電源タップとの通信を試みます。通信が成功すれば、ポートは電源タップとして設定されます。

   注:もし電源タップがサポートされていないモードにあれば、通信不良が起こります。電源タップの応用ソフトから電源タップをサポートされたモードに更新すると、SX II におけるポートを再度設定します。

6. いったんポートがパワーポートとして設定されると、ポート編集ページでコンセントの名前を変更できます。



電源の関連付けの削除

ターゲット サーバやラック PDU をデバイスから取り外す場合は、まずすべての電源の関連付けを削除する必要があります。ターゲットがラック PDU に関連付けられたままでターゲットをデバイスから取り外した場合、電源の関連付けは残ります。この場合、電源の関連付けを適切に削除するために [Device Settings] (デバイス設定) で切断されたターゲット サーバの [Port Configuration] (ポート設定) にアクセスすることはできません。

▶ ラック PDU の関連付けを削除するには、次の手順に従います。

1. [Power Strip Name] (電源タップ名) ドロップダウン リストから適切なラック PDU を選択します。
2. そのラック PDU に対して、[Outlet Name] (コンセント名) ドロップダウン リストから適切なコンセントを選択します。
3. [Outlet Name] (コンセント名) ドロップダウン リストから、[None] (設定なし) を選択します。
4. [OK] をクリックします。そのラック PDU/コンセントの関連付けが削除され、確認メッセージが表示されます。

▶ ラック PDU がターゲットから削除されている場合にラック PDU の関連付けを削除するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) をクリックし、アクティブなターゲットをクリックします。
2. アクティブなターゲットを、切断された電源ポートに関連付けます。これで、切断されたターゲットの電源の関連付けが破棄されます。
3. 最後に、アクティブなターゲットを、正しい電源ポートに関連付けます。

リモート コンソールからユーザとグループを設定・管理する

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてユーザとユーザグループを設定・管理する *『202p. 』。*

SX II はすべてのユーザの属性とユーザグループの内部リストを保存しています。

ユーザ諸データとグループはアクセス権限と許可を決定するのに使われます。この情報は内部に保存されています。ユーザのパスワードは暗号化された形式で保存されます。

SX II は管理者が一般の許可と属性によってグループを定義できるようにします。彼らはユーザをグループに加え、各ユーザはそのグループの属性と許可を持ちます。

グループの許可はグループ内の各個人に適用されるため、許可を各個人ごとに別々に適用する必要はありません。これでユーザの設定をする時間を削減しています。

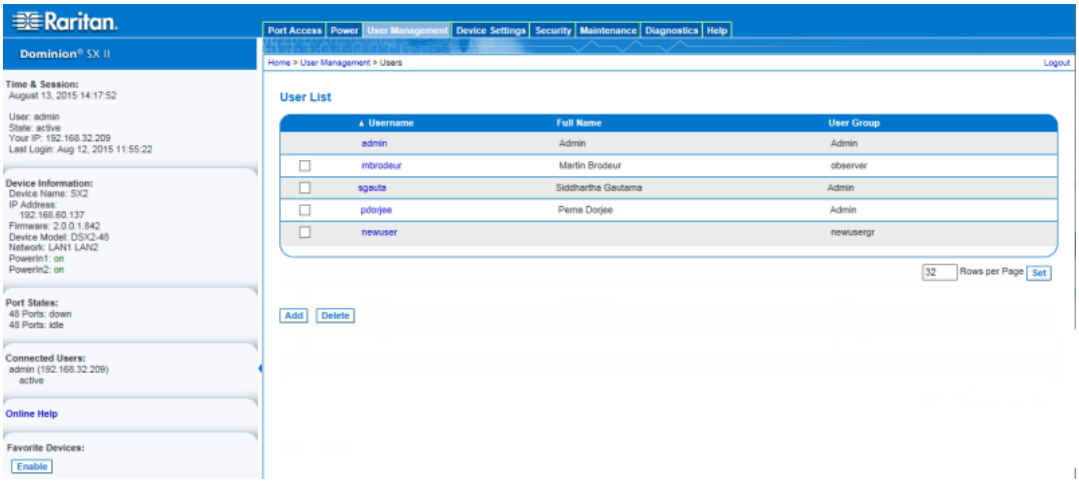
例えば、モデムアクセスと呼ばれるグループを生成し、モデムの管理の許可を持ちます。モデムアクセスグループに割り当てられた各ユーザはモデムの機能を管理できます。あなたは各ユーザに別々に許可を与える必要はありません。

ユーザーのリストを見る

- ユーザ管理 から ユーザリスト を選択します。

ユーザ リストページはその日までに生成されたすべてのユーザの属性を示していて、各人について、以下をリストしています –

- ユーザ名
- フルネーム
- ユーザ グループ



Raritan.

ユーザはグループに属し、グループには特権が割り当てられています。SX II の各種のユーザをグループに分けることにより、ユーザごとに許可を管理する必要がなくなり、あるグループ内のすべてユーザの許可を一度に管理できるようになるので、時間の節約につながります。

また、特定のユーザをグループに割り当てないようにすることも可能です。その場合は、ユーザを「個別」として分類します。

認証が成功すると、装置は、グループ情報を使用して、アクセスできるサーバ ポート、装置の再起動を許可するかどうかなど、そのユーザの許可を決定します。

注:これらの機能はコマンドラインインタフェースからでも行えます。
CLI を用いてユーザとユーザグループを設定・管理する *『202p. 』* 。

ユーザ グループ

全て SX II はデフォルトのユーザグループを付けて提供されます。これらのグループはユーザ追加ページのドロップダウンユーザグループにリストされています。

- [Admin] (管理者)

  このグループに所属するユーザは、全ての機能に完全な管理者特権を持ちます。

  元の製品出荷時のデフォルト ユーザはこのグループのメンバーであり、完全なシステム特権を持ちます。

  さらに、Admin ユーザは Admin グループのメンバーである必要があります。

- 不明

  さらに加えて、リモートサーバが有効なユーザグループを特定できない場合、不明グループが適用されます。

  これは LDAP/LDAPS RADIUS または TACACS+ を使用して外部的に認証されるユーザーのデフォルト グループです。

  さらに、新規に作成されたユーザは別のグループに割り当てられるまでこのグループに自動的に配置されます。

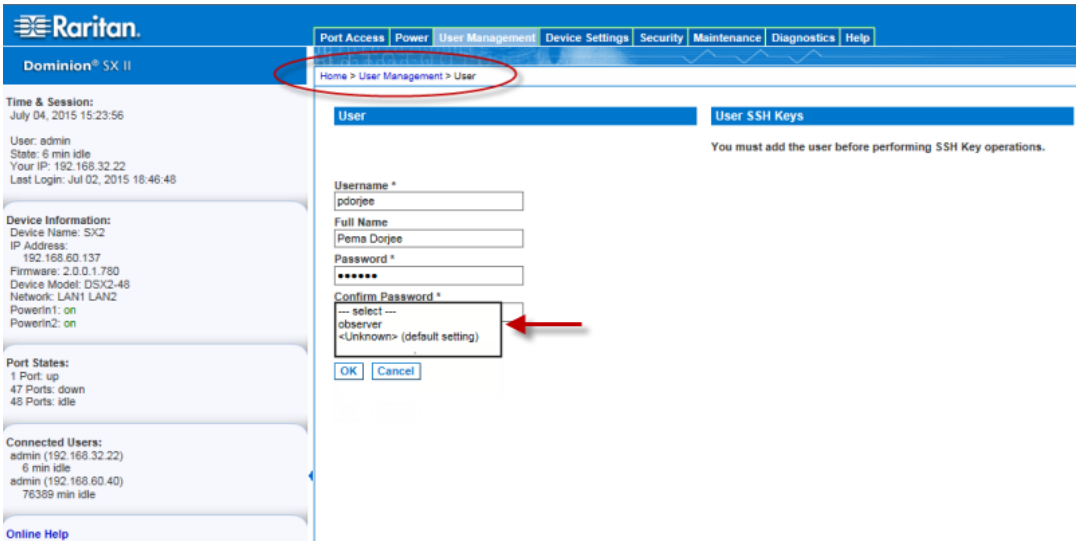
- 個別グループ

  個別グループとは、基本的に一人の「グループ」です。つまり、この特定のユーザは独自のグループに属し、他の実際のグループには属しません。

  あるユーザのアカウントがあるグループと同じ権利を持ち得るとき個人グループを用います。

  個別グループは、グループ名の先頭に @ が付けられているので区別できます。

デフォルトユーザグループは消去できませんが必要があれば追加のユーザグループを創ってニーズに合うようにし、ユーザをそれに割り当てることができます。



ユーザ プロファイル:

ユーザプロファイルは次の２つの目的に供します。

- ユーザに SX II にログインするためのユーザ名とパスワードを提供すること。
- ユーザをユーザグループに関連つけること。ユーザグループはどの機能とポートにユーザがアクセスできるかを決定します。

SX II は１人のユーザプロファイルを付けて出荷されます、それは Admin ユーザです。

このユーザプロファイルは Admin ユーザグループに割り当てられていて完全なシステムとポートの許可を持っています。このプロファイルを変更または削除することはできません。

SX II ではグループあたり最大 254 ユーザのプロファイルがサポートされています。

SX II のユーザごとにユニークなプロファイルを創ることができます。

あるいはその代わりに、プロファイルを創っておいてそれに複数のユーザを割り当てることもできます。そのプロファイルに割り当てられたユーザは同じ特権を持つことになります。これは時間の節約になりますが、ユーザに不適切な機能にアクセスする権利を与えないよう確認することが必要です。この機能は許可を制限するために使うこともできます。参照 ***SX II に限定されたアクセスを持つグループを創る***『84p. の*"SX II への限定したアクセスを持つグループの生成（IP アクセス 制御リスト）"* 参照 』。

ローカル及び遠隔認証

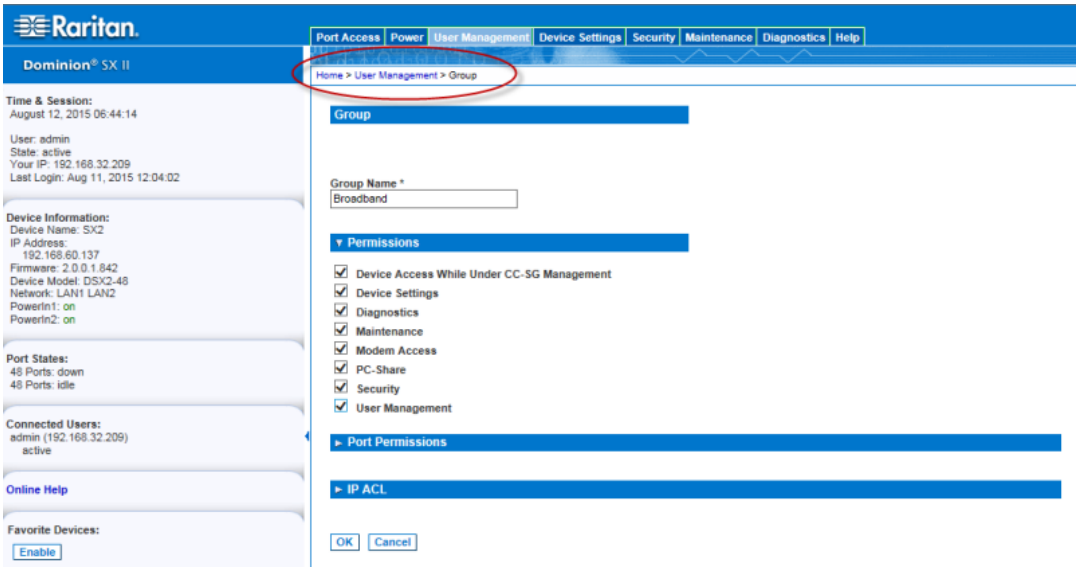
SX II にアクセスするには、全てのユーザーは認証を受けねばなりません

SX II はローカルであるいは LDAP/LDAPS, RADIUS or TACACS+ を用いて遠隔で認証できるユーザに設定できます。もし遠隔認証が可能であれば遠隔ユーザ認証はローカルな認証より先に処理されます。詳細については、次を参照してください。 ***ユーザ認証*** 『93p. の*"リモート コンソールからユーザ認証を設定する。"*参照 』。

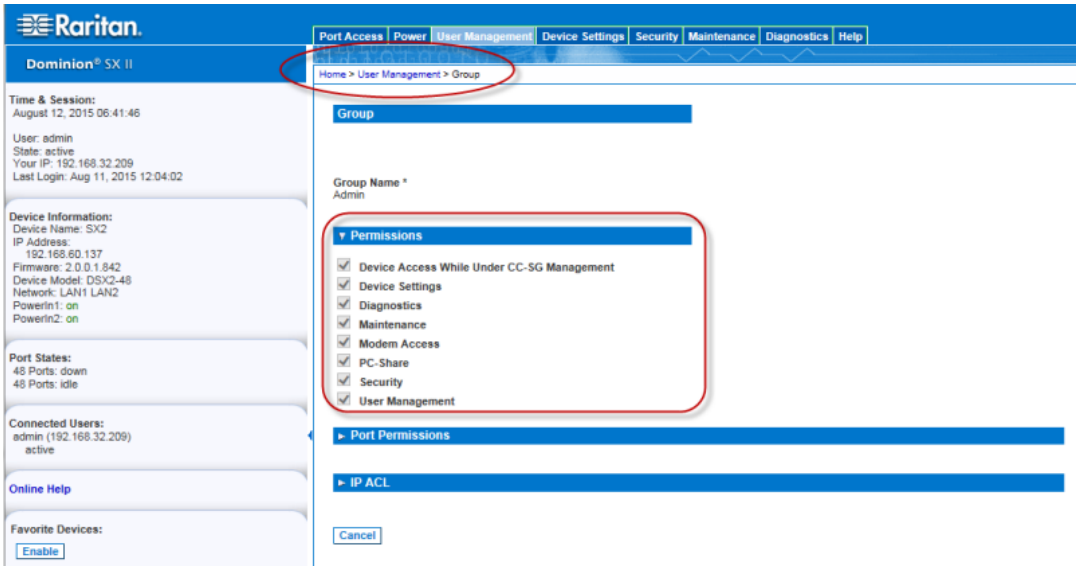
ユーザ グループの追加

1. ユーザ管理 から 新ユーザグループを追加 を選択するか、ユーザグループリスト ページで 追加 をクリックします。

2. グループ名　フィールドに、新しいユーザ グループのわかりやすい名前を入力します。



グループのアクセス許可の設定



3. そのグループに割り当てる許可を選択します。
   - CC-SG 管理下にある間のデバイスアクセス – この許可を持つユーザとユーザグループに CC-SG 管理下にある間 SX II への直接のアクセスを許可します。

     CC-SG のデバイスに対してローカルでのアクセスが可能なとき、SX II は IP アドレスを用いてアクセスされます。

     CC-SG の管理下にあるデバイスに直接アクセスすると、SX II でアクセスおよび接続アクティビティがログに記録されます。

ユーザ認証は、SX II の認証設定に基づいて実行されます。

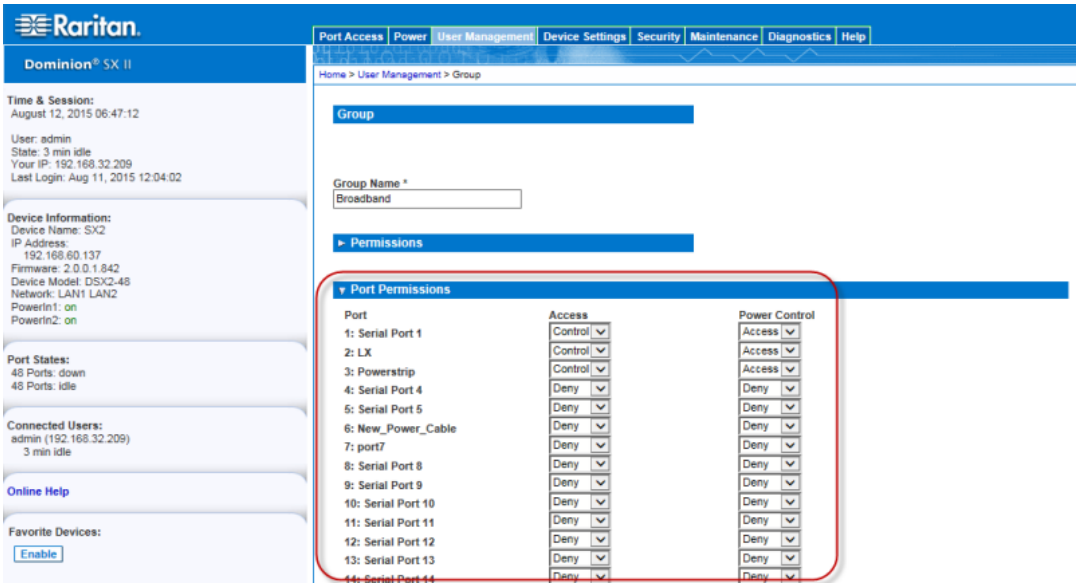
注:管理者ユーザ グループには、この許可がデフォルトで付与されます。

- デバイス設定 – ネットワーク設定、日付/時刻設定、ポートの設定、イベント管理（SNMP、Syslog）、など
- 診断 – ネットワーク インターフェース の状態、ネットワーク統計、ホストへの Ping、ホストへのトレース ルート、SX II 診断
- 保守 – データベースのバックアップと復元、ファームウェアのアップグレード、ファクトリ リセット、再起動
- PC-共有 – 複数のユーザによる同一ターゲットへの同時アクセス
- 安全- SSL 認証、安全設定、IP ACL。
- ユーザ管理 – ユーザとグループの管理、リモート、認証、ログイン設定。

***重要**:ユーザ管理 チェックボックスをオンにすると、グループのメンバーは、自身も含むすべてのユーザの許可を変更することができます。これらの許可を付与する場合は注意してください。*

- モデムアクセス – 外部モデムが SX II に接続されたときにページに表示されます。そのグループが外部モデムにアクセスすることがある場合このオプションを選択します。ブロードバンドのアクセスが GX440 モデムに対して有効化されていると、この許可がまたグループにワイアレス モデムを通じて SX II にアクセスすることを可能にします。 参照 ***外部モデムに接続しグローバルなアクセスを可能にする*** 『140p. の*"外部ブロードバンドモデムに接続しグローバルアクセスを有効にする"*参照 』。

ポートのアクセス許可の設定



4. サーバポートと電源制御に対してグループが持つアクセス許可を選択します。デフォルトは拒絶です。

   各ポートを個別に選択するか、あるいはすべてのポートに許可を与えるためページの下端にあるチェックボックスを使います。

   - 拒絶 – アクセスは完全に拒絶されます。
   - 表示 – 接続先のターゲット のビデオを表示します（操作はできません）。
   - 制御 – 接続されたターゲットを制御します。

     電源管理アクセスも付与されている場合は、そのグループに制御を割り当てる必要があります。

5. OK をクリックしてグループを生成し許可を適用します。

IP ACL の情報については、次を参照してください *SX II への限定したアクセスを持つグループの生成（IP アクセス 制御リスト）* 『84p. 』。

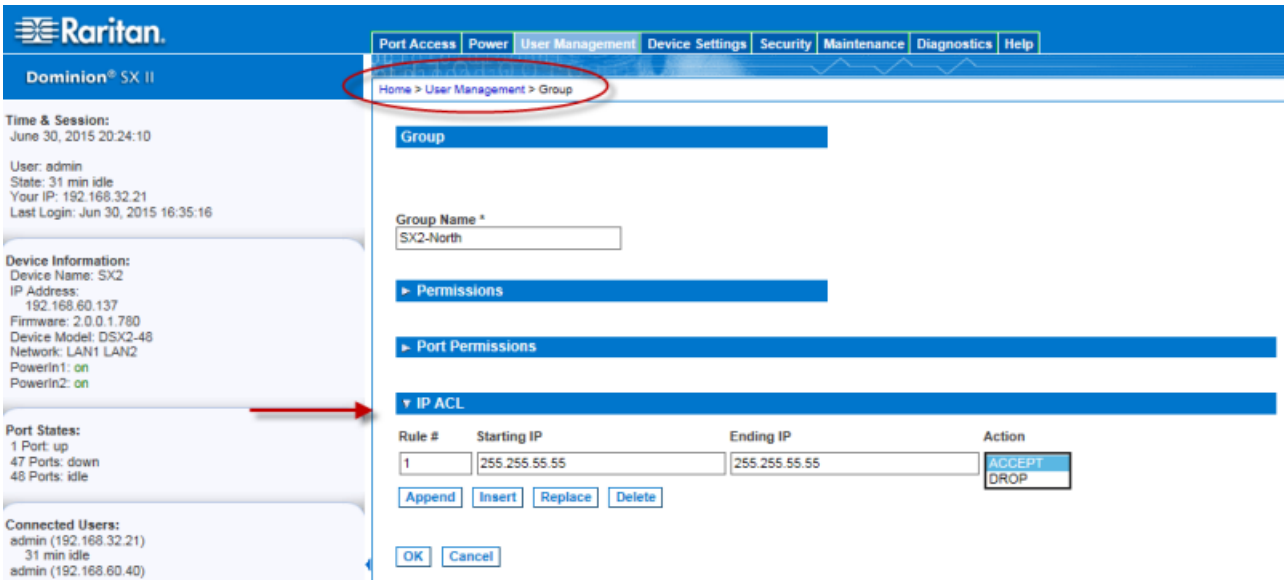
SX II への限定したアクセスを持つグループの生成（IP アクセス 制御リスト）

重要:グループベースの IP アクセス制御を使用する場合は注意が必要です。アクセスが拒否されている IP アドレスの範囲に自分の IP アドレスが含まれている場合、 SX II がロックアウトされてしまいます。

この特徴によってユーザを特定の IP アドレスのデバイスのアクセスのみを可能とするグループに割り付けることができるので SX II へのユーザのアクセスを制限します。

この機能は特定のグループに属するユーザにのみ適用されます。これはすべてのそのデバイスへのアクセスの試みに適用される IP アクセス制御リスト機能とは異なるものです。IP アクセス制御はグループベースの IP ACL に対する優先度を用い、最初に処理されます。

グループレベルをベースとする IP アクセス制御ルールの追加、挿入、置換、削除を行うには、グループ ページの［IP ACL］セクションを使用します。



ルールを末尾に追加するには

1. 開始 IP］フィールドに、開始 IP アドレスを入力します。
2. 終了 IP］ フィールドに、終了 IP アドレスを入力します。
3. 利用可能なオプションからアクションを選択します。
   - 承認 – 承認にセットされた IP アドレスは SX II デバイスへのアクセスが許可されます。
   - 拒否 – その IP アドレスによる SX II デバイスへのアクセスが拒否されます。
4. 追加、［OK］の順にクリックします。そのルールがルール一覧の末尾に追加されます。入力する各ルールについて、手順 1 ～ 4 を繰り返します。

ルールを一覧の途中に挿入するには

1. ルール番号 (#) を入力します。挿入 コマンドを使用する際にルール番号が必要です。

2. 開始 IP] (開始 IP) フィールドと 終了 IP] (終了 IP) フィールドに IP アドレスを入力します。
3. アクション ドロップダウン リストからアクションを選択します。
4. 挿入、[OK] の順にクリックします。入力したルール番号が既存のルール番号と同じである場合は、新しいルールは既存のルールの上に挿入され、リスト内のすべてのルールが下に下がります。

ルールの内容を置換するには

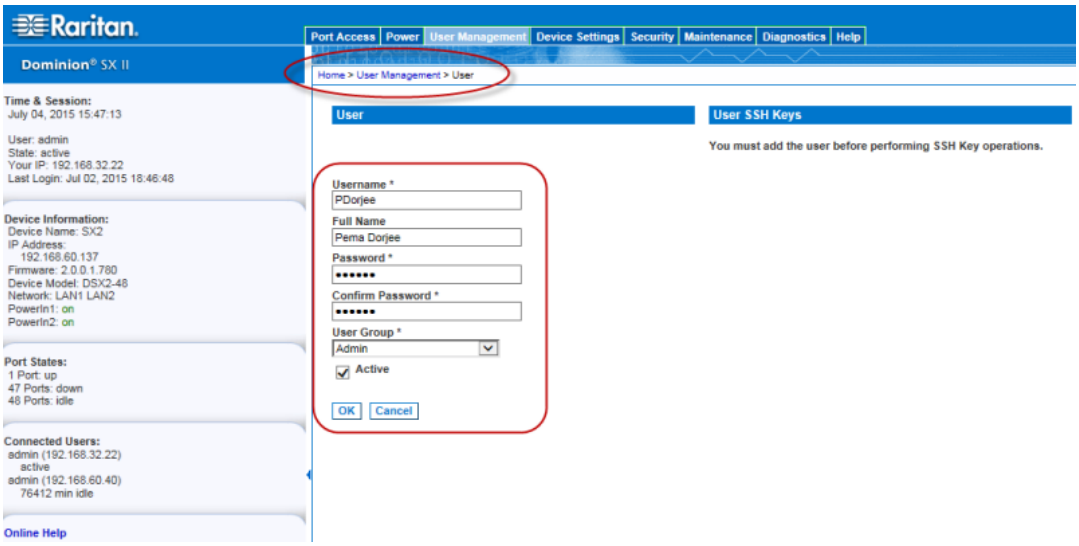
1. 置き換えるルール番号を指定します。
2. 開始 IP] フィールドと 終了 IP] フィールドに IP アドレスを入力します。
3. ドロップダウン リストからアクションを選択します。
4. 置換、[OK] の順にクリックします。同じルール番号を持つ元のルールが新しいルールに置き換わります。

ルールを削除するには

1. 削除するルール番号を指定します。
2. 削除 をクリックします。
3. 消去を確認する入力待ちとなると、OK をクリックし、ページの OK をクリックして変更を保存します。

ユーザの生成と有効化

1. ユーザ管理 の ユーザ を選択します。



2. 新しいログイン名を ユーザ名 フィールドに入力します。これはユーザが SX II にログインするために入力する名前です。必ず入力してください。

- ユーザ名は大文字小文字を区別します。

3. フルネーム フィールドに、ユーザのフル ネーム を入力します。必ず入力してください。
4. パスワード フィールドにパスワードを記入し、そして パスワードの確認 フィールドにそれをもう一度入力します。必ず入力してください。
   - パスワードは大文字小文字を区別します。

注:強力なパスワード機能が有効化となっている場合、その他にパスワードの要件があります。 強力なパスワード を参照してください。

5. ユーザをユーザグループのドロップダウンから選ぶことによってユーザグループに関連つけます。必ず入力してください。

   このユーザを既存のユーザ グループに関連付けたくない場合は、ドロップダウン リストから [Individual Group] (個別グループ) を選択します。個別グループの許可についての詳細は、「個別グループの許可の設定」を参照してください。
6. このプロファイルを直ちに有効化するかどうかを決めます。デフォルトでは、有効化のチェックボックスが選択されています。

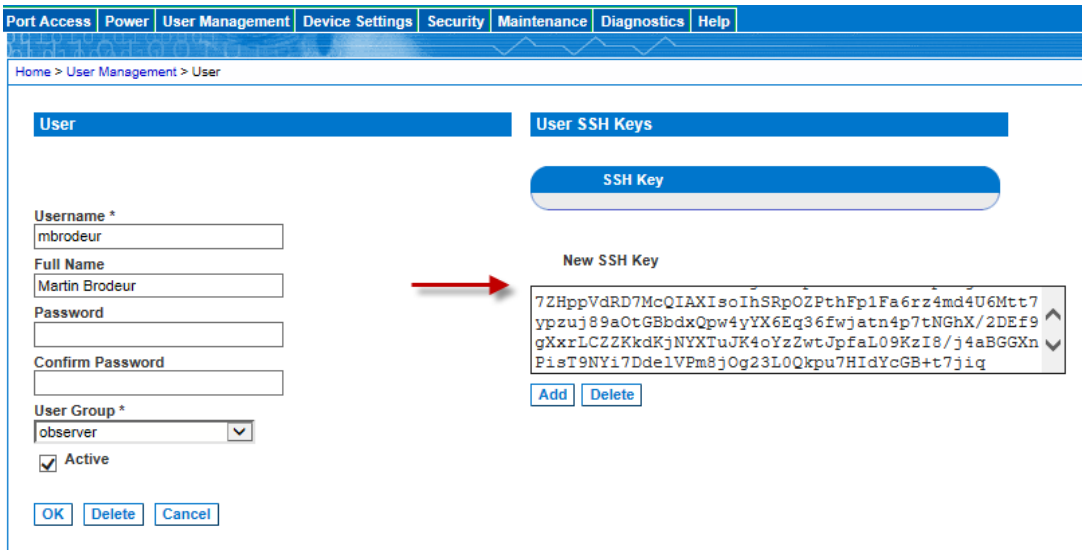
   このアカウントを無効化するには、このチェックボックスを外します。いつでも必要な時にここに戻ってユーザを有効化することができます。
7. OK をクリックします。このページが閉じます。
8. ユーザの属性が作成されユーザリストページに現れます。そのユーザのページを再度開き SSH キーセクションを有効化します。必要であれば、 SSH キーをユーザ属性に割り当てます。参照 ***ユーザのための SSH クライアント認証*** 『88p. の*"ユーザのための SSH クライアント認証を追加する"*参照 』。

ユーザのための SSH クライアント認証を追加する

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてのユーザ権限設定と認証サービス *『206p. の"*CLI を用いてのユーザ権限設定と認証サービスの設定*"参照 』*。

必要があれば、SSH（安全シェル）クライアントの認証キーがユーザーに追加されます。そのユーザはクライアント証明書が追加となる前に作成する必要があります。

1. ユーザ管理 > ユーザリスト を選択し、そして SSH クライアント認証を追加したいユーザの名前の上でクリックします。ユーザ ページが開きます。



2. SSH キーデータボックスに SSH キーデータを入力します。このデータはクライアントのために生成された rsa_id.pub キーです。

   Linux のユーザはパブリックキーを追加する際、生成されたキーの末尾に現れる "name@local host" を消去する必要があります。

   Windows のユーザは常に "name@local host" を含む必要があります。

3. 追加 をクリックします。キーデータは認証に用いられるべきで、パスワードを入力する必要はないはずです。

SSH キーを消去するには

1. 削除するキーの次にあるチェックボックスをクリックします。
2. 削除 をクリックします。
3. 確認を求めるプロンプトが表示されたら、[OK] をクリックします。

ユーザの編集あるいは非活性化

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 **CLI を用いてユーザとユーザグループを設定・管理する** *『202p. 』。*

1. ユーザ管理　の ユーザリスト を選択します。ユーザリスト ページが開きます。

   新規ユーザのページと全く同じに見えます参照 ***ユーザの生成と有効化*** 『86p. 』。
2. ユーザ名以外はどのフィールドも変更することができます。
3. セキュリティ上の理由で、パスワードは表示されません。パスワードを変更するには、パスワード フィールドと［Confirm Password ］フィールドに新しいパスワードを入力します。これらのフィールドをそのままで残せば、パスワードは変更されません。
4. 完了したら［OK］をクリックします。ユーザ プロファイルが変更されます。

ユーザの削除

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてユーザを削除する。

1. ユーザ管理　の ユーザリスト を選択します。ユーザリスト ページが開きます。
2. 削除したいユーザのユーザプロファイルの左側のチェックボックスをオンにします。（複数選択可）。
3. ［Delete ］をクリックします。削除を確認するプロンプトが表示されます。
4. ［OK］をクリックします。選択されたユーザのプロファイルは削除されます。

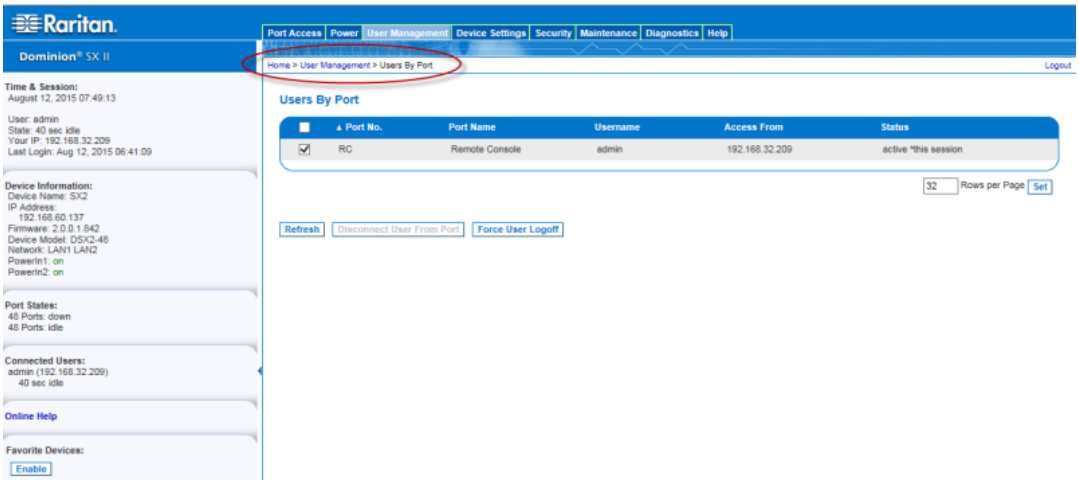
ポート別のユーザの表示

ポート別ユーザ ページには、認証済みのすべてのローカル ユーザとリモート ユーザおよび各ユーザの接続先のポートが表示されます。

- 同じユーザが複数のクライアントからログオンしている場合は、接続ごとにユーザ名がページに表示されます。たとえば、ユーザが 2 つの異なるクライアントからログオンしている場合、そのユーザ名が 2 回表示されます。
- このページには、次のユーザ情報およびポート情報が表示されます。
- ポート番号 – ユーザの接続先ポートに割り当てられているポート番号
- ポート名 – ユーザの接続先ポートに割り当てられているポート名
- 注:ユーザがターゲットに接続されていない場合は、ポート名の下にローカルコンソール または リモートコンソール が表示されます。
- ユーザ名 – ユーザ ログインやターゲット接続用のユーザ名
- からアクセス – SX II にアクセスしているクライアント PC の IP アドレス
- ステータス – 接続の現在のステータス (アクティブまたは非アクティブ)

ポート別にユーザを表示するには、以下の手順に従います。

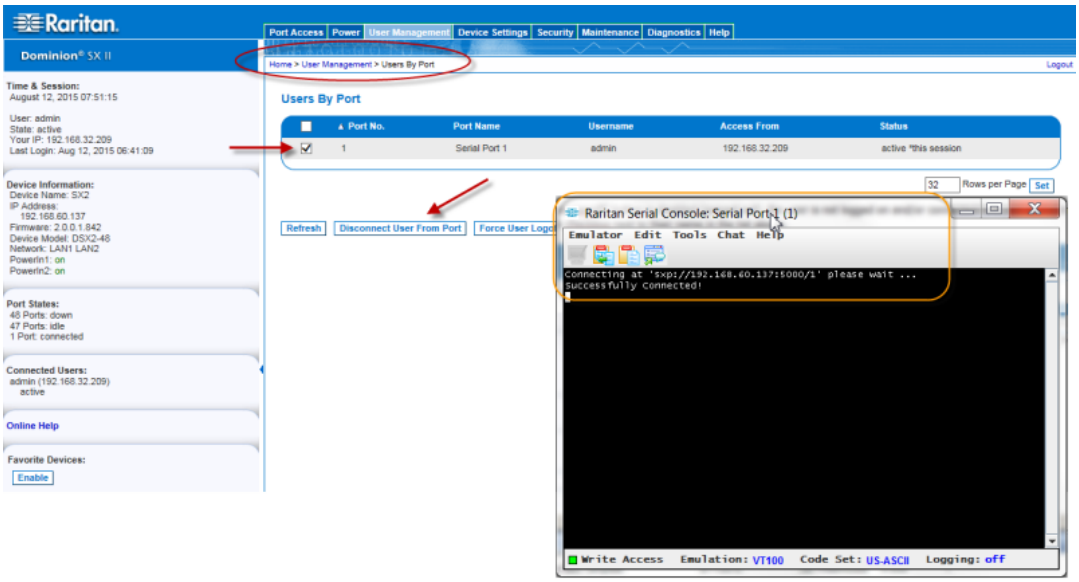
- ユーザ管理 の ポート別ユーザ を選択します。ポート別ユーザページが開きます。



Raritan.

ポートからユーザを切断する

特定のポートからユーザを　SX II からそのユーザたちをログオフさせることなく削除する。例えば、もしユーザが Raritan Serial Console (RSC) 経由でシリアルポート 1 に接続していると、あなたは彼らをポートから切断することができます。



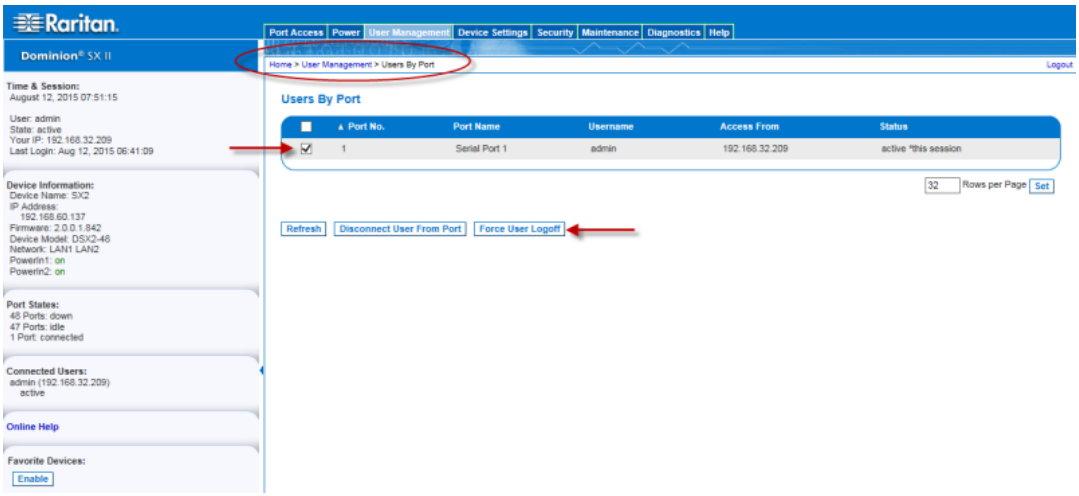
これはユーザを強制的にログオフさせるのと異なります、その時にはユーザをターゲットポートから切断し、そして SX II からもログオフさせます。参照 ユーザを SX II からログオフさせる（強制ログオフ） に情報があります

1. ユーザ管理 の ポート別ユーザ　を選択します。ポート別ユーザページが開きます。
2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。
3. ユーザをポートから切断　をクリックします。
4. 確認メッセージに対して［OK］をクリックすると、ユーザがポートから切断されます。
5. ユーザがポートから切断されたことを示す確認メッセージが表示されます。

ユーザをポートから切断 が無効となっている場合には、そのユーザは現在ポートにログオンしていないか、あるいは上記のユーザ名の隣にあるチェックボックスを選択していなかったかです。

ユーザを SX II からログオフさせる（強制ログオフ）

あなたが管理者であるかあるいはユーザ管理の許可を持っている場合、SX II にログオンしている認証されたどのユーザでもログオフすることができます。また、ユーザをポート レベルでポートから切断することもできます。参照 ポートからのユーザの切断。



1. ユーザ管理 の ポート別ユーザ を選択します。ポート別ユーザ ページが開きます。
2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。
3. ユーザ強制ログオフ をクリックします。
4. ユーザをログオフ の確認メッセージに対して［OK］をクリックします。

ユーザをポートから切断 のボタンが無効となっている場合には、そのユーザは現在ポートにログオンしてポートに接続していないか、あるいは上記のユーザ名の隣にあるチェックボックスを選択していなかったかです。

リモート コンソールからユーザ認証を設定する。

SX II は装置にアクセスするためにユーザーに認証を求めます。

認証とは、ユーザが本人であることを確認するプロセスです。ユーザが認証されると、ユーザの属するグループに基づいて、システムおよびポートに対する許可が決定されます。ユーザに割り当てられた特権により、どのようなタイプのアクセスが許可されるかが決まります。これを「認可」と呼びます。

ユーザーは SX II のローカルであるいはリモートで認証を受けることができます。

デフォルトでは、ユーザーはローカルで認証を受けます。リモート認証はそれを有効化しなければなりません。

SX II がリモート認証用に構成されている場合、外部認証サーバは主に認証を目的として使用され、認可用には使用されません。

SX II はリモート認証のユーザーのために数種類のオプションを提供しています。

- LDAP/LDAPS
- RADIUS
- TACACS+

LDAP, RADIUS と TACACS+ サーバの設定については、次を参照してください。 LDAP, RADIUS と TACACS+ サーバを設定する。

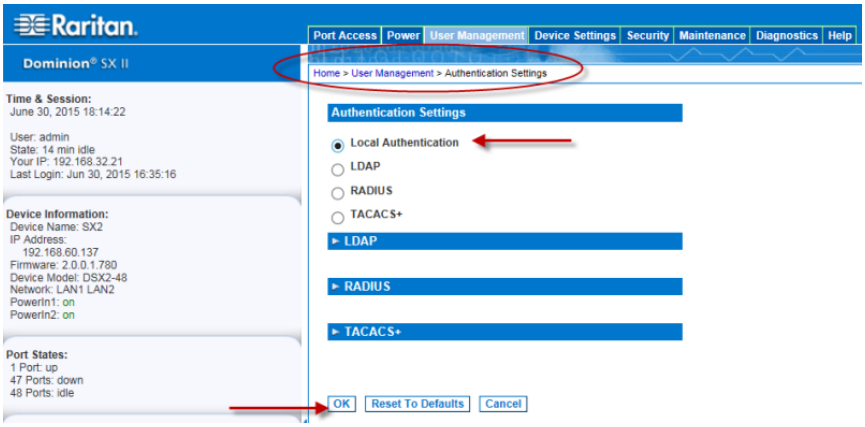
SX II において Telnet と SSH を有効化するための情報については、次を参照してください。 ***Telnet (オプション)を有効化*** 『116p. の"***Telnet を有効化 (オプション)***"参照 』 および ***SSH アクセス (オプション) を有効化*** 『115p. の"***SSH アクセスを有効化 (オプション)***"参照 』。

注:コマンドラインインタフェース経由での遠隔認証の設定ができます。参照 **CLI を用いてのユーザ権限設定と認証サービス** *『206p. の"***CLI を用いてのユーザ権限設定と認証サービスの設定***"参照 』*。

ローカルでのユーザ認証の有効化

ユーザはローカルのデータベースからのユーザ名とパスワードによって認証されます。

遠隔認証が有効化されていてそのユーザが見つからない場合は、SX II はローカルの認証データベースもチェックします。



1. ユーザ管理 の認証設定を選択します。認証設定 ページが開きます。
2. ローカルでの認証を選択します
3. [OK] をクリックして保存します。

▶ 出荷時のデフォルトに戻すには、以下の手順に従います。

- デフォルトに戻すをクリックします。

LDAP/LDAPS 認証の有効化

注:LDAP サーバを設定する際には、サーバ上のクエリー文字列のフォーマットは SX II で設定したグループの名前を含んでいるべきです。

Lightweight Directory Access Protocol (LDAP) をローカル認証の代わりに SX II ユーザの認証に使うことができます。

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル: LDAP/LDAPS) は、TCP/IP 上で動作するディレクトリ サービスを照会および変更するためのネットワーキング プロトコルです。

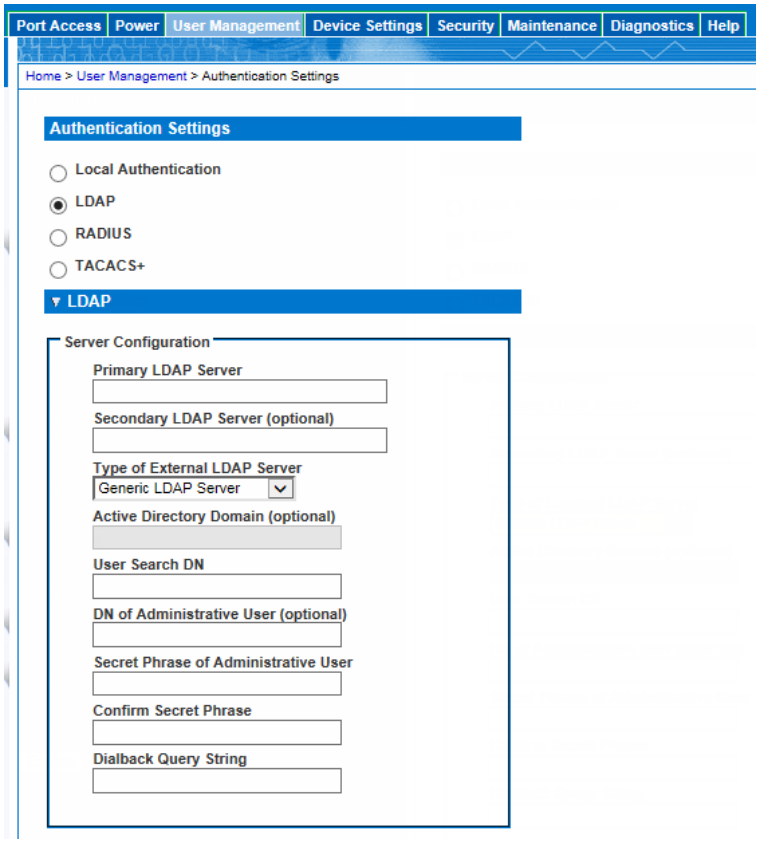
クライアントは、LDAP/LDAPS サーバ (デフォルトの TCP ポートは 389) に接続して、LDAP セッションを開始します。次に、クライアントは、オペレーション要求をサーバに送信します。サーバは、この要求に対して応答を返します。

メモ:Microsoft Active Directory は、LDAP/LDAPS 認証サーバとしてネイティブに機能します。

1. ユーザ管理 の 認証設定 をクリックして、認証設定のページを開きます。
2. [LDAP] ラジオ ボタンを選択して、ページの [LDAP] セクションを有効にします。

   LDAP のセクションが拡大します。そうならなければ、LDAP セクションのヘッダー上でクリックします。

サーバの設定



3. プライマリ LDAP サーバ のフィールドに、LDAP/LDAPS リモート認証サーバの IP アドレスまたはホスト名を入力します。
4. 〈オプション〉セカンダリ LDAP サーバ フィールドに、バックアップ LDAP/LDAPS サーバの IP アドレスまたはホスト名を入力します (最大 256 文字)。セキュア LDAP を有効にするオプションをオンにした場合は、DNS 名を使用する必要があります。残りのフィールドについては、プライマリ LDAP サーバフィールドの場合と同じ設定を使用します。
5. 外部 LDAP サーバのタイプを選択します。
   - 一般的な LDAP サーバ。
   - [Microsoft Active Directory]。Active Directory は、Windows 環境向けの Microsoft による LDAP/LDAPS ディレクトリ サービスの実装です。

- Microsoft Active Directory を選択した場合は、Active Directory ドメインの名前を入力します。例：acme.com.特定のドメインの名前については、Active Directive 管理者にお問い合わせください。〈オプション〉

6. [ユーザ検索 DN] フィールドに、LDAP データベース内でユーザ情報の検索を開始する場所の識別名を入力します。たとえば、"cn=Users,dc=raritan,dc=com" というベース検索値を設定します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。

   このフィールドは、LDAP サーバで管理者にのみユーザの役割を使用したユーザ情報の検索を許可している場合にのみ入力します。

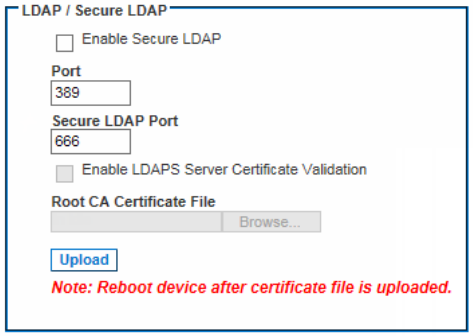
   このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。

   たとえば、管理者ユーザの DN として、"cn=Administrator,cn=Users,dc=testradius,dc=com" と設定します。オプション

7. 管理者ユーザの識別名を入力した場合は、管理者ユーザの DN をリモート認証サーバに対して認証するために使用するパスワードを入力する必要があります。

   シークレットフレーズフィールドにパスワードを入力し、[Confirm Secret Phrase] フィールドにパスワードを再入力します 。

   LDAP/LDAP Secure（保証）



8. SSL を使用する場合は、セキュア LDAP を有効にする チェックボックスをオンにします。

   これにより、LDAPS サーバ証明書の検証を有効にするチェックボックスがオンになります。

   Secure Sockets Layer (SSL) は、SX II が LDAP/LDAPS サーバと安全に通信できるようにする暗号プロトコルです。

   セキュア LDAP を有効にする（セキュア LDAP を有効にする）チェックボックスをオンにし、LDAPS サーバ証明書の検証を有効にするチェックボックスをオンにした場合は、LDAP サーバ証明書の CN に一致する DNS 名を使用する必要があります。

9. デフォルトのポートは 389 です。標準 LDAP TCP ポートを使用するか、または別のポートを指定します。
10. [Secure LDAP Port] のデフォルトは 636 です。デフォルトのポートを使用するか、または別のポートを指定します。このフィールドは、セキュア LDAP を有効にする チェックボックスがオンのときにのみ使用します。
11. 前にアップロードしたルート CA 証明書ファイルを使用してサーバから提供された証明書を検証するには、サーバ証明書の検証を有効にする チェックボックスをオンにします。

    前にアップロードしたルート CA 証明書ファイルを使用しない場合は、このチェックボックスをオフのままにします。

    この機能を無効にすることは、不明な証明機関によって署名された証明書を受け取ることと同じです。このチェックボックスは、セキュア LDAP を有効にする チェックボックスがオンのときにのみ使用できます。

    注:検証にルート CA 証明書を使用し、さらに サーバ証明書の検証を有効にする チェックボックスをオンにする場合は、サーバ ホスト名がサーバ証明書に記載された共通名と一致する必要があります。
12. 必要な場合は、ルート CA 証明書のファイルをアップロードします。

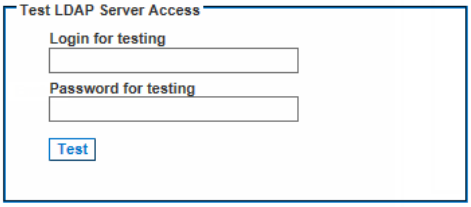
    このフィールドは、セキュア LDAP を有効にする チェックボックスがオンのときに有効になります。

    LDAP/LDAPS サーバ用の Base64 エンコードの X-509 形式の CA 証明書ファイルについては、担当の認証サーバ管理者に問い合わせてください。

    ブラウズ ボタンを使用して証明書ファイルを選択します。

    LDAP/LDAPS サーバの証明書を新しい証明書に置き換える場合は、新しい証明書を有効にするために SX II を再起動する必要があります。

    LDAP サーバ アクセスのテスト

13. LDAP の設定をテストするには、テストのためのログイン フィールドと テストのためのパスワード フィールドにそれぞれログイン名とパスワードを入力します。テスト をクリックします。

これは SX II にアクセスするために入力したユーザ名とパスワードです。 LDAP サーバがあなたを認証するために使用するユーザ名とパスワードです。

そして SX II が認証設定ページから LDAP の設定をテストします。これは LDAP と SX II をリモート認証のために設定するとき時々複雑さにしたときに助けとなります。

テストが完了すると、テストが成功したことを知らせるメッセージが表示されます。テストが失敗した場合は、詳細なエラー メッセージが表示されます。成功時には、リモート LDAP サーバから取得されたテスト ユーザのグループ情報も表示されることがあります。

RADIUS 認証の有効化

注:RADIUS サーバを設定するときには、サーバ上のユーザのための フィルターID フォーマットは次のフォーマットを取る必要があります "raritan:G{GroupOnSX}:D{DialbackNumber}"。

Remote Authentication Dial-In User Service (RADIUS) をローカル認証の代わりに SX II ユーザの認証に使うことができます。

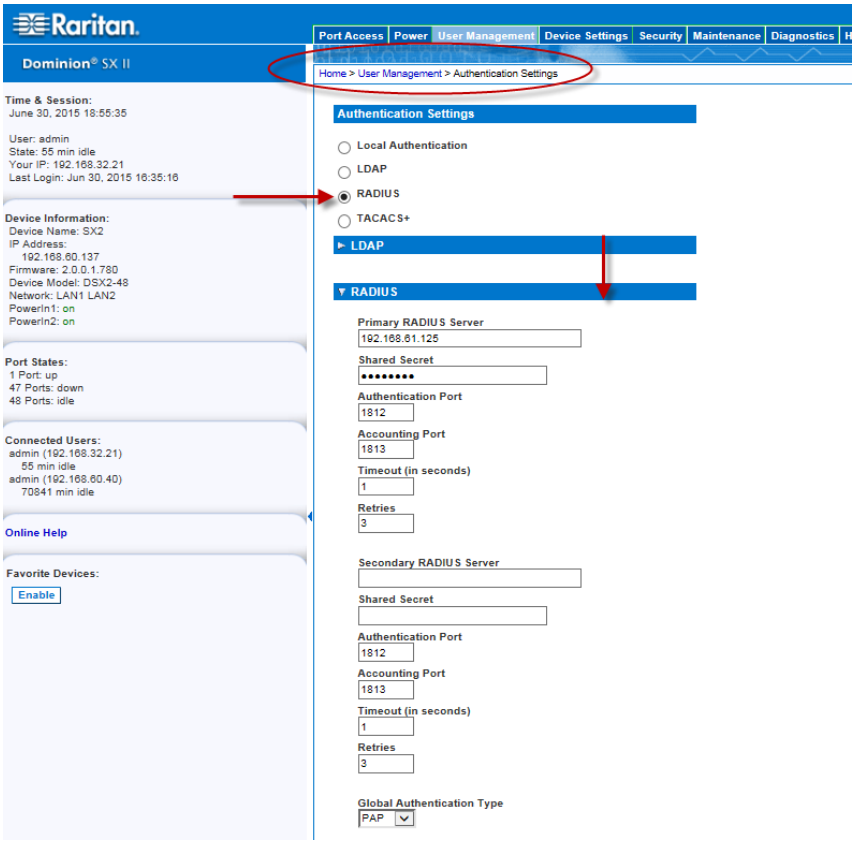
RADIUS はネットワークにアクセスする応用のための AAA (authentication, authorization, と accounting - 認証、権限付与、会計) プロトコルです。

1. ユーザ管理 の 認証設定 をクリックして、認証設定のページを開きます。
2. [RADIUS] の ラジオ ボタンをクリックして、そのページの [RADIUS] セクションを有効にします。そのセクションが拡大します。そうならなければ セクションのヘッダー上でクリックして拡大します。
3. プライマリサーバ フィールドおよび セカンダリサーバフィールドに、プライマリ認証サーバの IP アドレスおよびオプションでセカンダリ認証サーバの IP アドレスをそれぞれ入力します。
4. 共有シークレット フィールドに、認証に使用するサーバのシークレットフレーズを入力します。

   共有シークレットとは、 SX II と RADIUS サーバとの間で安全に通信を行うために両者で共有される文字列です。これは、基本的にはパスワードです。
5. 認証ポート のデフォルトは 1812 ですが、必要に応じて変更できます。
6. [Accounting Port] のデフォルトは 1813 ですが、必要に応じて変更できます。
7. 時間切れ は秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。

8. このタイムアウトは、SX II が次の認証要求を送信する前に RADIUS サーバからの応答を待つ時間です。
9. デフォルトの再試行回数は 3 回です。

   これは、SX II が RADIUS サーバに対して認証要求を送信する回数です。
10. ドロップダウン リストのオプションから、適切な グローバル認証タイプ を選択します。
    - [PAP] – PAP の場合、パスワードは平文（ひらぶん）– 暗号化されないテキストとして送信されます。PAP は対話型ではありません。サーバがログイン プロンプトを送信してその応答を待つ方式ではなく、接続が確立された時点でユーザ名とパスワードが 1 つのデータ パッケージとして送信されます。
    - [CHAP] – CHAP の場合、サーバはいつでも認証を要求できます。CHAP は、PAP よりも高いセキュリティを実現します。



RADIUS ポリシーを作成する

このセクションでは RADIUS のユーザが SX II にアクセスできるようポリシーを作成する手順を説明します。このセクションの例では２つの条件を置いています：クライアントの SX II のソース IP アドレスと UserID が SX II のユーザグループのメンバーであることです：

- NAS-IP-Address = SX II の IP アドレスのタイプ
- Windows-Group = SX II ユーザグループ

注:Dominion 製品グループの異なったモデルの SX II 装置（DKX, DKSX あるいは KX101）がある場合、（NAS-IP-Address）規則に一致する適切な条件を使用することで適切な Dominion 装置の正しいポリシーを適用する助けとなります。

---

1. インターネット認証サービスから、リモートアクセスポリシーの上で右クリックし、そして新しいリモートアクセスポリシーを選択します。
2. 新規のリモート ポリシーのウィザードがスタートします。次 をクリックします。
3. カスタムポリシーを設定するのラジオボタンを選択し、ポリシーの名前を記入します。
4. ポリシー条件のダイアログが現れます。追加... ボタンをクリックします。
5. NAS-IP-アドレス名を選択し 追加... ボタンをクリックします。SX II の IP アドレスをタイプします。
6. 第２の条件を Windows-Group の名前と SX II ユーザグループの値を用いて記入します。次 をクリックします。
7. リモートアクセス許可を与えるのラジオボタンを選択します。
8. 次 をクリックします。プロファイルのダイアログが現れます。
9. プロファイルを編集するボタンをクリックします。
10. 認証タブを選択します。暗号化なしの認証（PAP, SPAP）のチェックボックスを選択しその他のすべてのチェックボックスを外します。

    注:SX II のこのバージョンは Challenge Authentication Protocol (CHAP) をサポートしていません。

    ---

11. 詳細タブをクリックします。枠組みの決まったプロトコルを外します。

    注:各ポリシーは適合していなければなりません。もし、条件が適合していないと、IAS は次のポリシーに行きその条件を調べます。

    ---

12. 追加... ボタンをクリックします。RADIUS の属性リストが現れます。
13. フィルタ ID アドレス名を選択し 追加... ボタンをクリックします。属性値セクションで 追加 をクリックします。Attribute の値を次のようにタイプします：Raritan:G{Admin}.
14. [OK] をクリックします。

15. G{} の値は SX II のローカルにあるグループの名前で、この場合デフォルトの Admin グループです。
    - 値はダイアルバック機能を使う場合 Raritan:G{Admin}:D{1234567890} のようになります。ここで 1234567890 はダイアルバックのための電話番号です。
    - この値 Raritan:G{Admin} は SX II 上のローカルなグループと一致しなければなりません。
    - SX II は出荷の際デフォルトの Admin グループが入っています。
    - SX II の追加のユーザグループは ユーザ管理 > ユーザグループ オプションを用いて作成されます。
    - 適切なポートアクセスとユーザクラス(操作者 あるいは 監督者) を定義できます。RADIUS のユーザが SX II にアクセスするのを認可するため'グループの名前は 識別属性でそれぞれ指定しなければなりません。
16. 新規のポリシーを移動しそれがポリシーリストの最初(top) に現れるようにします。

注:要求があれば、ポリシーがダイアルアップでグループのメンバーである全てのユーザにアクセスすることを可能にします（Windows® はすでにダイアルインの可能などのユーザにもアクセスを許可するデフォルトのポリシーをすでにもっているので、この新規なポリシーはオプションとなります）。もし新しいポリシーを使用する希望であれば、それがデフォルトのポリシーより上に現れることを確認してください。

---

17. サービスがスタートしたことを確認します。
18. Active Directory®ユーザのためのローカルな口座が彼らのユーザプロファイルでダイアルインアクセスが可能であることを確認してください。Windows 2000® で Domain サーバがネイティブモード にあり、そして IAS が Active Directory に登録されていれば、リモートアクセスポリシーを使うためユーザプロファイル>ダイヤルイン設定をセットできます。

SX II を IAS RADIUS サーバを使用するよう設定する

SX II を IAS RADIUIS サーバを使うために設定するタスクは：

- 第１の Radius サーバ（とオプションで第２の Radius サーバ）を設定する。
- Radius のポートを設定する。
- IAS 内の IAS クライアント設定に一致したシークレット（共有シークレット）を設定する。

次の例は新規の IAS インストレーションに基づいた簡単な設定を示しています。

注:IAS の設定が既にある場合には、以下の指示は示した通りではないかもしれません。

IAS をサーバ上で有効とする。

1. IAS サーバで、コントロールパネルに行き プログラムの追加と削除を立ち上げます。
2. Windows 要素の追加あるいは削除をクリックします。
3. ネットワーキングサービスをハイライトし、そして詳細...ボタンをクリックします。
4. インターネット認証サービスのチェックボックスを選択し、[OK] をクリックします。
5. 次 をクリックしウィザードの手順に従います。

IAS アクティブ ディレクトリーのアクセス

Domain のコントローラーを使用している場合、IAS を次のステップで Active Directory®にアクセスするようセットします。

1. IAS を立ち上げ（スタート > 全プログラム > 管理ツール > インターネット認証サービス。
2. インターネット認証サービス (Local) の上で右クリックし、[Active Directory] の[Register Server] を選択します。

   注:Active Directory についての情報は次の Microsoft の URL を参照してください。
   http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

SX II をクライアントのリストに追加します。

1. インターネット認証サービスから、RADIUS クライアント の上で右クリックし、そして新しい RADIUS クライアントを選択します。
2. 呼びやすい名前と SX II の IP アドレスをタイプします。
3. Client-Vendor のドロップダウンメニューで RADIUS St と ard を選択し、 SX II の設定と一致する共有シークレットキーをタイプします。

RADIUS 認証用の Cisco ACS 5.x

Cisco Access Control Server (ACS) は SX II でサポートされているもう一つの認証解決策です。

SX II が RADIUS をサポートするには、SX II とユーザ情報の両方を RADIUS の設定に追加する必要があります。

Cisco ACS 5.x サーバを使用している場合は、SX II に RADIUS 認証を設定した後に、Cisco ACS 5.x サーバで以下の手順を完了する必要があります。

注: 以下の手順には、各ページへのアクセスに使用される Cisco のメニューおよびメニュー項目が含まれます。各手順の最新情報とその実行の詳細については、Cisco のマニュアルを参照してください。

- AAA クライアントとしての SX II の追加 (**必須**) – [Network Resources] (ネットワーク リソース)、[Network Device Group] (ネットワーク デバイス グループ)、[Network Device and AAA Clients] (ネットワーク デバイスと AAA クライアント) の順に選択
- ユーザの追加/編集 (**必須**) – [Network Resources] (ネットワーク リソース)、[Users and Identity Stores] (ユーザ ストアと ID ストア)、[Internal Identity Stores] (内部 ID ストア)、[Users] (ユーザ) の順に選択
- CHAP プロトコルを有効にするデフォルト ネットワーク アクセスの設定 (**オプション**) – [Policies] (ポリシー)、[Access Services] (アクセス サービス)、[Default Network Access] (デフォルト ネットワーク アクセス) の順に選択
- アクセスを制御する認可ポリシー ルールの作成 (**必須**) – [Policy Elements] (ポリシー要素)、[Authorization and Permissions] (認可と許可)、[Network Access] (ネットワーク アクセス)、[Authorization Profiles] (認可プロファイル) の順に選択
  - [Dictionary Type] (ディクショナリ タイプ): RADIUS-IETF
  - [RADIUS Attribute] (RADIUS 属性): Filter-ID
  - [Attribute Type] (属性タイプ): String
  - [Attribute Value] (属性値):Raritan:G{Serial_Admin} (ここで Serial_Admin は SX II にローカルで作成されたグループの名前です)。大文字と小文字が区別されます。
- セッション状況 (日時) の設定 (**必須**) – [Policy Elements] (ポリシー要素)、[Session Conditions] (セッション状況)、[Date and Time] (日時) の順に選択
- ネットワーク アクセス認可ポリシーの設定/作成 (**必須**) – [Access Policies] (アクセス ポリシー)、[Access Services] (アクセス サービス)、[Default Network Access] (デフォルト ネットワーク アクセス)、[Authorization] (認可) の順に選択

RADIUS 通信交換仕様

SX II は、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログイン	
Access-Request(1)	
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-IP-Address (4)	SX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct-Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	SX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
ログアウト	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	SX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

TACACS+ 認証を有効化する

注:TACACS+ サーバを設定する際には、サーバ上のユーザ-グループのフォーマットは SX II で設定したグループの名前を含んでいるべきです。

TACACS+ サーバを設定する際には、dominionsx service を追加するべきです。このサービスの下でのユーザ-グループの属性は SX II で設定したグループの名前を含んでいるべきです。このサービスの下でのユーザ-ダイアルバック フィールドはこのユーザのモデム ダイアルバック番号を含む。

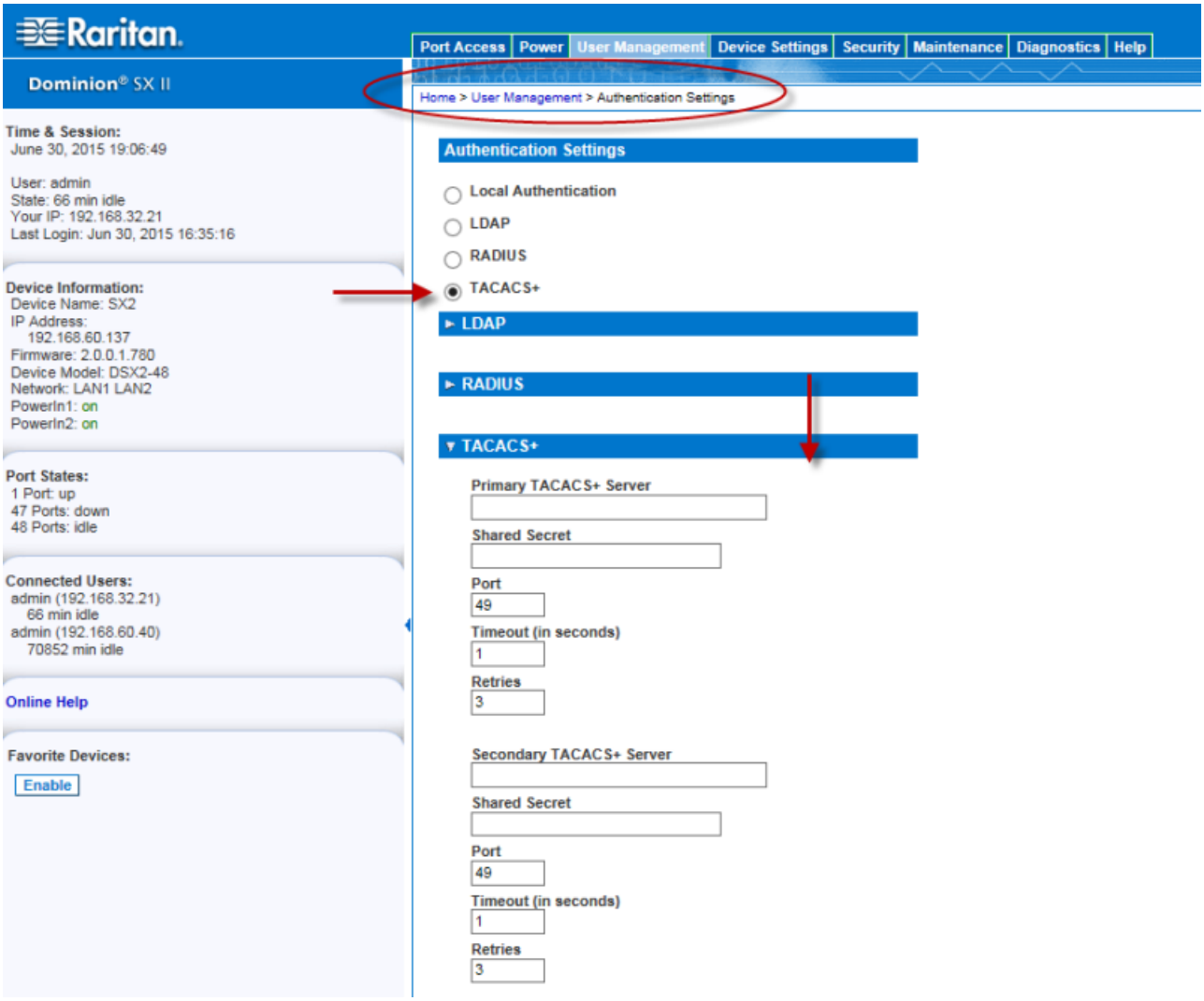
Terminal Access Controller Access-Control System Plus (TACACS+) をローカル認証の代わりに SX II ユーザの認証に使うことができます。

1. ユーザ管理 の 認証設定 をクリックして、認証設定のページを開きます。
2. [TACACS+] ラジオ ボタンをクリックして、ページの [TACACS+] セクションを有効にします。

   そのセクションが拡大します。そうならなければ セクションのヘッダー上でクリックして拡大します。
3. プライマリーの TACACS+ の下で、 TACACS+ サーバの IP アドレスそしてそれが聞き取る（入力に使う）ポート（デフォルトで 49）をそれぞれ IP アドレスとポートのフィールドにタイプします。
4. 共有シークレット フィールドに記入します。キーとしても知られるこのフィールドは暗号化と TACACS+ サーバとの共通の識別のために必要です。
5. 時間切れは秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。
6. このタイムアウトは、 SX II が次の認証要求を送信する前に TACACS+ サーバからの応答を待つ時間です。
7. デフォルトの再試行回数は 3 回です。

   これは、 SX II が TACACS+ サーバに対して認証要求を送信する回数です。
8. もしバックアップの TACACS+ サーバを持っていると、第２の TACACS+ フィールドにも同じ情報を入力します。

9. ［OK］をクリックします。TACACS+ 認証が有効になります。



ユーザ グループ情報を Active Directory サーバから返す

SX II はユーザの Active Directory ® （AD）への認証をサポートし、そのためにユーザが SX II でローカルに定義されていることを要求しません。これにより、Active Directory のユーザ アカウントとパスワードは、AD サーバ上に排他的に維持されます。認証と AD ユーザ特権は標準の SX II ポリシーと AD ユーザグループにローカルに適用される特権によって制御・管理されます。

重要:Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、SX II はこの設定をサポートします。この場合、以下に示す手順を実行する必要はありません。参照 LDAP スキーマを更新する AD LDAP/LSAPS スキーマを更新する方法についての詳細が示されています。

SX II 上で AD サーバを有効化するには

1. SX II を使用して、特殊なグループを作成し、適切な許可および特権をグループに割り当てます。

   たとえば、AD_Admin や AD_Operator というグループを作成します。
2. Active Directory サーバで、前の手順で作成したのと同じグループ名を持つ新しいグループを作成します。
3. AD サーバ上で、手順 2 で作成したグループに SX II ユーザを割り当てます。
4. SX II で、AD サーバを有効にし、適切に設定します。「LDAP/LDAPS リモート認証の実装」を参照してください。

重要な注記:

- グループ名では大文字と小文字が区別されます。
- SX II には、次のデフォルトのグループがあり、それらは変更したりし削除することはできません。Admin と<Unknown>.Active Directory サーバでこれらと同じグループ名が使用されていないことを確認してください。
- Active Directory サーバから戻ったグループの情報が SX II のグループの設定と一致しない場合、SX II は自動的に<Unknown> のグループを認証に成功したユーザに割り当てます。
- ダイアルバック番号を使用するときには、次の大小文字ケースを守った文字列 msRADIUSCallbackNumber を［Dialback Query String］に入力する必要があります。
- Microsoft からの推奨に基づいて、ドメイン ローカル グループではなく、ユーザ アカウントを含むグローバル グループを使用する必要があります。

ユーザ グループ情報を RADIUS 経由で返す

RADIUS 認証の試行が成功したら、SX II は、ユーザのグループの許可に基づいて、そのユーザの許可を決定します。

リモート RADIUS サーバは、RADIUS FILTER-ID として実装された属性を返すことによって、これらのユーザ グループ名を提供できます。FILTER-ID は、Raritan:G{*GROUP_NAME*} という形式となります。*GROUP_NAME* は、ユーザが属するグループの名前を示す文字列です。

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

GROUP_NAME は、ユーザが属するグループの名前を示す文字列です。Dial Back Number は、ユーザ アカウントに関連付けられている番号で、SX II モデムがユーザ アカウントへのダイヤルバックに使用します。

リモート コンソールから SX II のネットワーク設定を設定する

次に記述されている設定 *『リモートコンソールからの最初の SX II の設定』* 『20p. の″*リモートコンソールからの最初の SX II の設定*″参照 』 を行うのは何かの変更を行うときにも同様に適用されます。

ネットワーク設定を出荷時のデフォルトに戻す

1. デバイス管理 からネットワーク をクリックしネットワーク設定ページを開きます。
2. ページ下部にあるデフォルトにリセットをクリックします。

リモート コンソールから TFTP あるいは USB スティックを使用するためのオートスクリプトを有効化する

この機能はあなたの各 SX II に同じ設定をコピーするのに使用します。

これを行うには、SX II を設定する設定スクリプトファイルを作成します。

スクリプトの例

```
config
localport
config enable false
```

Script Result Example

```
config
Config > localport
Config > LocalPort > config enable false
Local port configuration successful.
Config > LocalPort >
```

このファイルを作成しそしてそれを各装置に配布するために次の 1 つあるいは両方を行ってください –

- そのファイルを TFTP サーバに同じ名前 DSX2_SERIAL.autoscript で保存します。新しい SX II が初めてブートアップすると、DHCP に連絡を取り、装置の IP アドレス を検索します。そして DHCP サーバは SX II に TFTP サーバの IP アドレスを送ります。

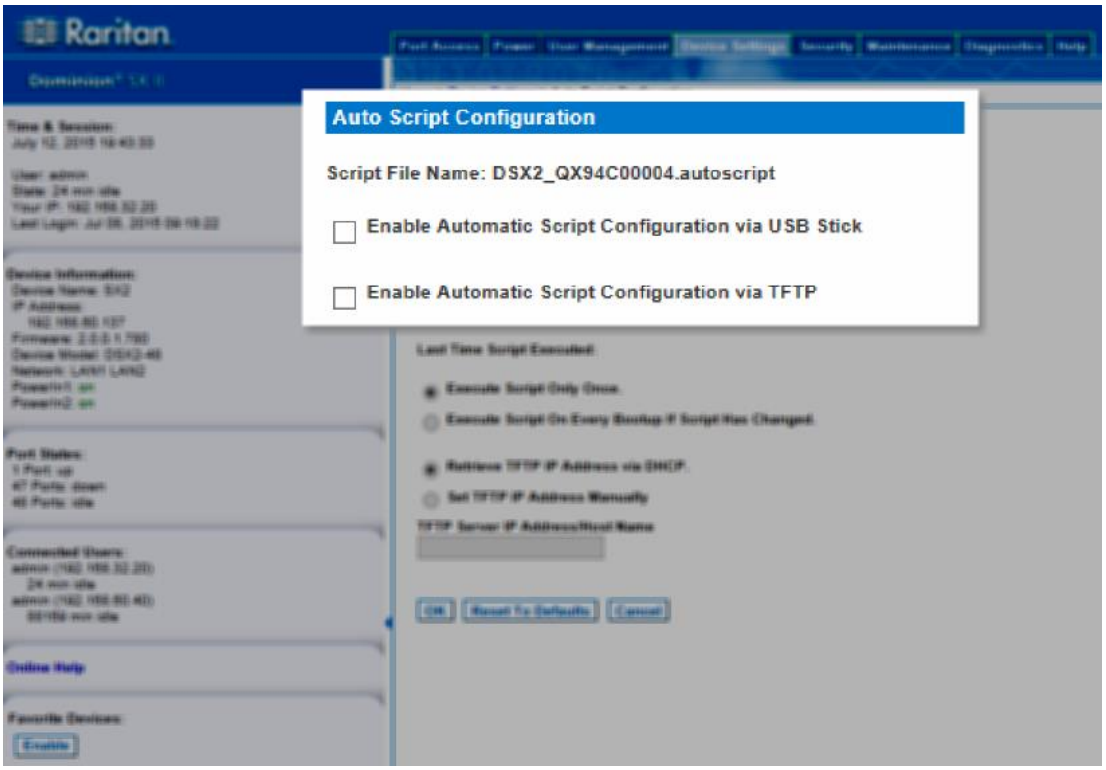
  いったん連絡が取れると、TFTP サーバから設定ファイルが送られ、その構成の設定が装置に適用され、そして装置が再起動します。

  この方法では人手による介入は一切必要ありません。

  SX II は TCTP サーバのアドレスを次の設定の 1 つから検索することを了解してください：

  - DHCP next-server (siaddr)
  - TFTP server address (option 66)。両方が指定されるとこのオプションが優先されます。

- そのファイルを USB スティックに保存します。このファイルは各装置に運びそれを設定するのに使うことができます。

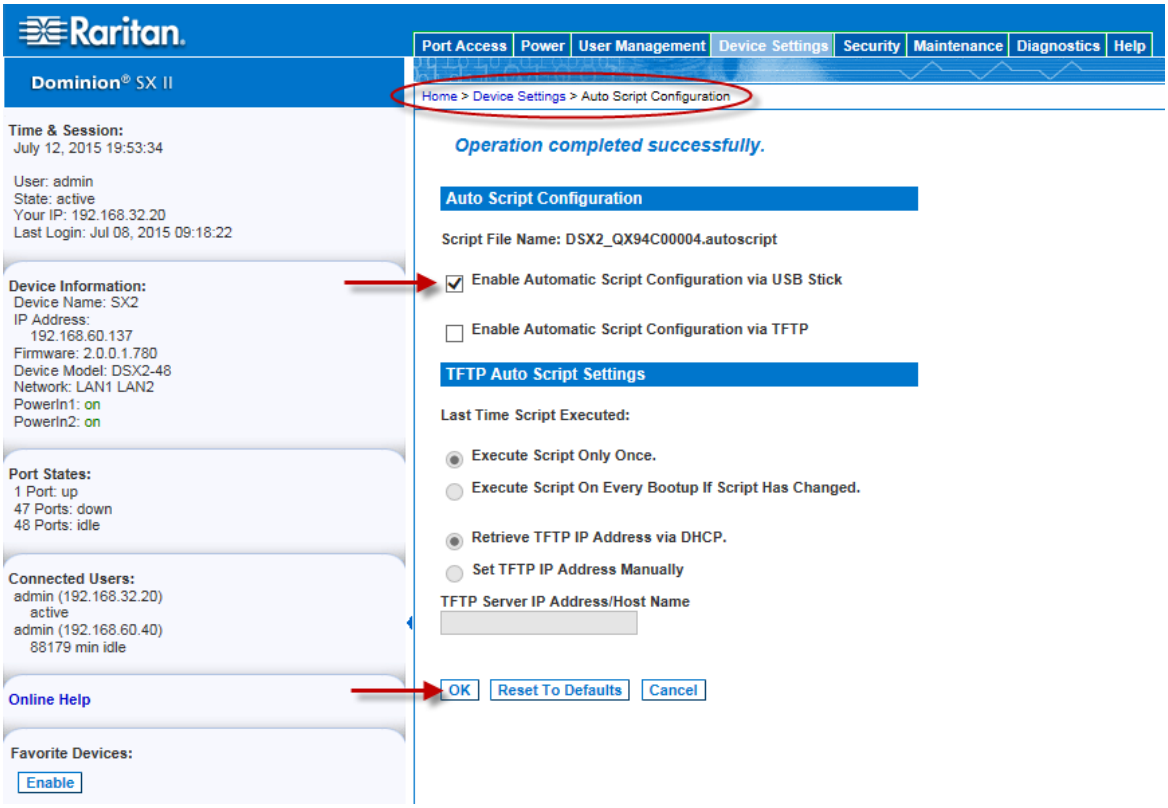


1. 設定ファイルを作成しようと思う SX II にアクセスし設定をします。
2. デバイス設定から自動設定を選択します。
3. 自動スクリプト設定セクションの先頭にこのスクリプトの名前がリストされています。読み取り専用

▶ USB スティック経由の自動スクリプト設定を有効にする：

1. USB スティックを準備し、それを SX II の前面あるいは背面の USB ポートに差し込みます。参照 *USB スティックを自動設ファイルのために準備する* 『113p. の*"USB スティックを自動設定ファイルのために準備する"*参照 』。
2. USB スティックからの自動スクリプト設定を有効にするのチェックボックスを選択します。

3. [OK] をクリックして、スクリプトを作成します。成功のメッセージがそのページに標示されます。



TFTP サーバ経由の自動スクリプト設定を有効にする：

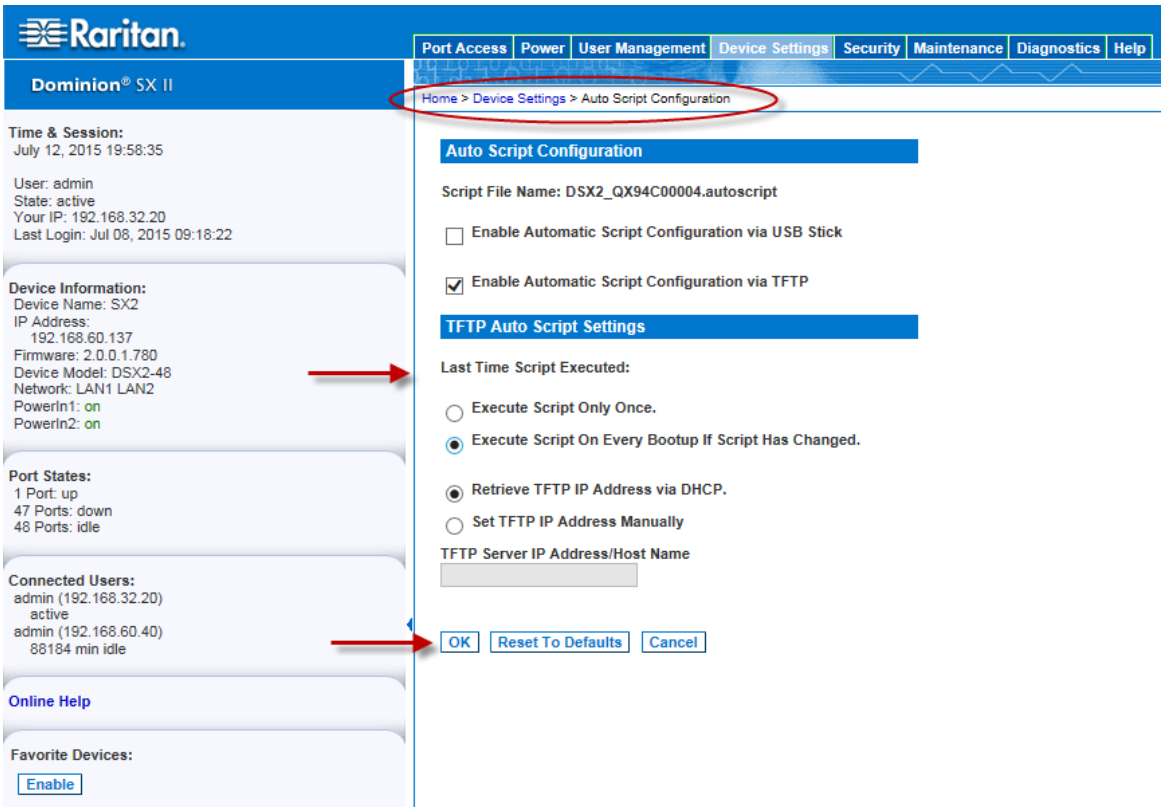
1. TFTP 経由の自動スクリプト設定を有効にするのチェックボックスを選択します。
2. TFTP の自動スクリプト設定セクションが有効になります。
3. その装置でスクリプトが走っている時を選びます。
   - スクリプトを 1 回だけ実行します – そのスクリプトは装置が初めてブートアップしたときに実行さるだけで再度実行されません。変更はその後手動で行う必要があります。
   - スクリプトが変化する毎にブートアップで実行されます – 更新はスクリプトが変化したときのブートアップで装置に適用されます。

     SX II は実行された最後のスクリプトから異なった場合にのみスクリプトを実行します。これはここで選択されたオプションに関係なく適用されます。

     SX II は最も最近に実行されたスクリプトを、それが実行された時刻を含めて覚えています。
4. いかに IP アドレスが設定されるかを選択する –

- DHCP 経由で TFTP の IP アドレスを検索します – これを行うことは、IP 自動設定は DHCP にセットし、SX II の上で有効化されることを了解して下さい。参照 DHCP を SX II で不能あるいは有効にする。
- TFTP の IP アドレスを手動でセットする – 与えられたフィールドに IP アドレスを入力します。

5. [OK] をクリックします。



USB スティックを自動設定ファイルのために準備する

USB スティックを準備するのに次を実行します –

1. USB スティックをクライアントマシンに嵌め込みます
2. からのファイルを作成し名前を `!automatic_config` とします。。
3. credential と名付けたファイルを作成します それは SX II のユーザ名とパスワードを含んでいます次のシンタックスに従います –

```
username=<user name>
password=<password>
```

注:これは管理者ユーザだけです。他のレベルのユーザはこの機能を使うことができません。

4. 次のように名付けたファイルを作成します
   <Device_Type>_<Serial_Number_Of_Device>.autoscript
   これは装置を設定するためにそこで実行されるべき全てのスクリプトを含んでいます。
5. 上記のすべてのファイルを USB スティックのトップディレクトリーにコピーします。
6. 次の名前のファイルがあれば除去します：
   <Device_Type>_<Serial_Number_Of_Device>_result.txt。
7. 以下は最終的に USB に持つべきファイル群の例です。
   ```
   !automatic_config
   credential
   DSX2_QVY4C00007.autoscript
   ```
8. 必要であれば、同じ USB スティックに他のデバイスのためのスクリプトファイルを追加します。
9. 終わればクライアントマシンから USB スティックを安全に外します。

USB スティックで自動設定を実行する

以下が USB スティックからの自動設定を用いて SX II を設定する手順です。

USB スティックを準備しそこに自動設定ファイルを入れます。参考、もしまだそうしていないなら

1. デバイスが作動できる状態にあることを確実にします。
2. 準備した USB スティックを設定しようとする SX II の前面あるいは背面の USB ポートに差し込みます。
3. ユーザ名とパスワードの認証が有効になるとスクリプトは自動的に実行されます。
4. いったんスクリプトが終了すると、SX II は２回ビープ音を発しそして
   <Device_Type>_<Serial_Number_Of_Device>_result.txt
   ファイルが生成され USB スティックのトップディレクトリーに保存されます。
5. ここで USB スティックを外すことができます。

重要 – USB をその終了前に抜くとスクリプトは実行を停止します。

リモート コンソールからデバイス設定をセットする

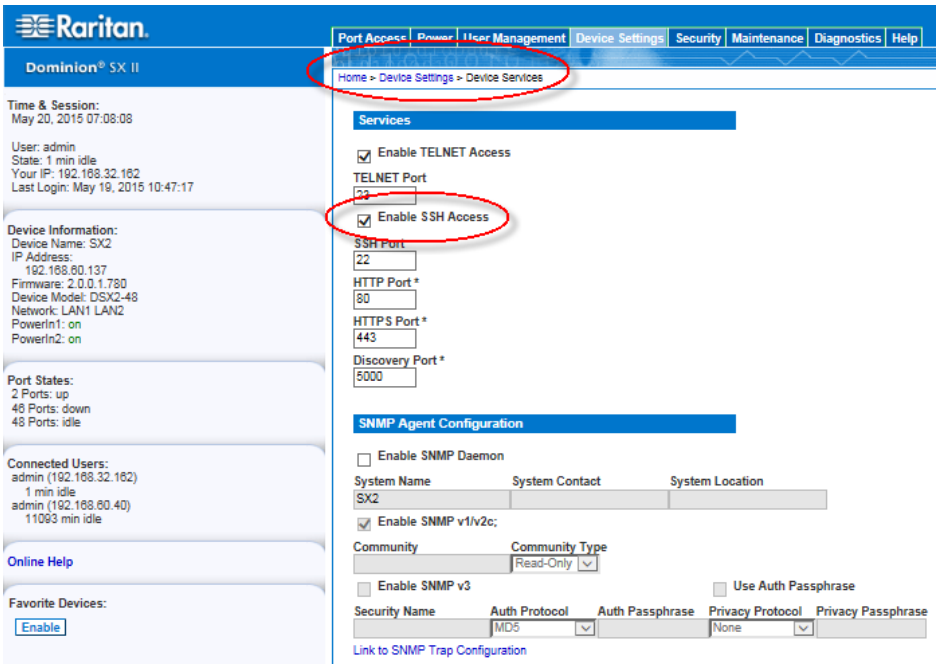
SSH アクセスを有効化（オプション）

SSH はデフォルトで有効化されています。

ポートを開けることとポートのプロトコルについては、次を参照してください。 。

SSH はリモート コンソールあるいはコマンドラインインタフェース (CLI)から無効化あるいは有効化することができます。参照 *CLI を用いたデバイス設定* 『214p. 』。

1. デバイス > デバイス設定 を選択してデバイス サービス ページを開きます。
2. SSH のアクセスを有効にするチェックボックスを選択し SSH ポートを完了します。[OK] をクリックして保存します。



Telnet を有効化 (オプション)

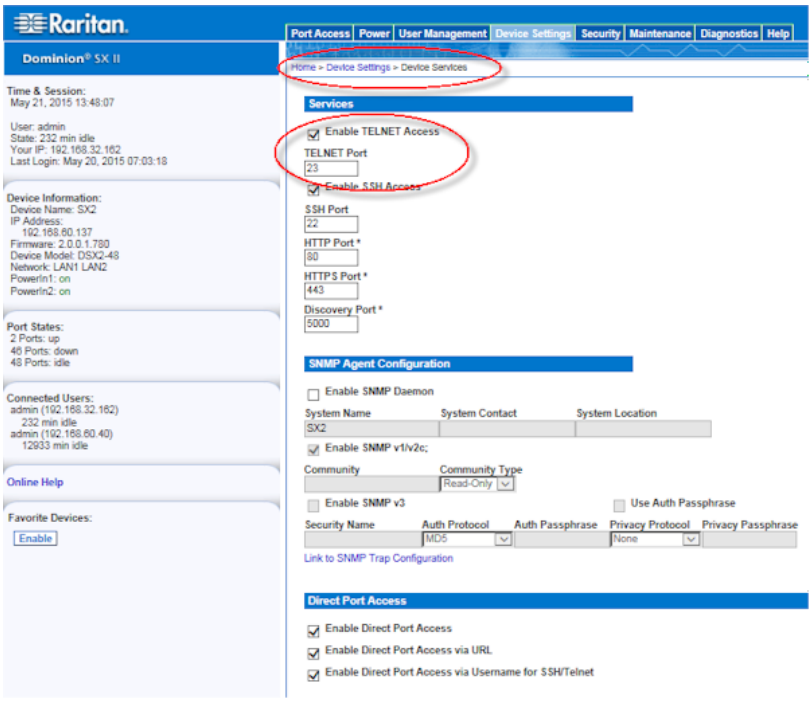
Telnet はセキュリティが低く、ユーザ名、パスワード、およびすべてのトラフィックが平文で送信されます。

Telnet は使用される前に有効化される必要があります。通常無効化されています。

Telnet はリモート コンソールあるいはコマンドラインインタフェース (CLI)から無効化あるいは有効化することができます。参照 *CLI を用いたデバイス設定* 『214p. 』。

ポートを開けることとポートのプロトコルについては、次を参照してください。 。

1. デバイス設定 からデバイスサービスサービスを選択してデバイスサービス ページを開きます。
2. 必要であれば、デフォルトのポートを変更します。
3. Telnet アクセスをを有効にするチェックボックスを選択し Telnet のポートを入力します。[OK] をクリックして保存します。



Raritan.

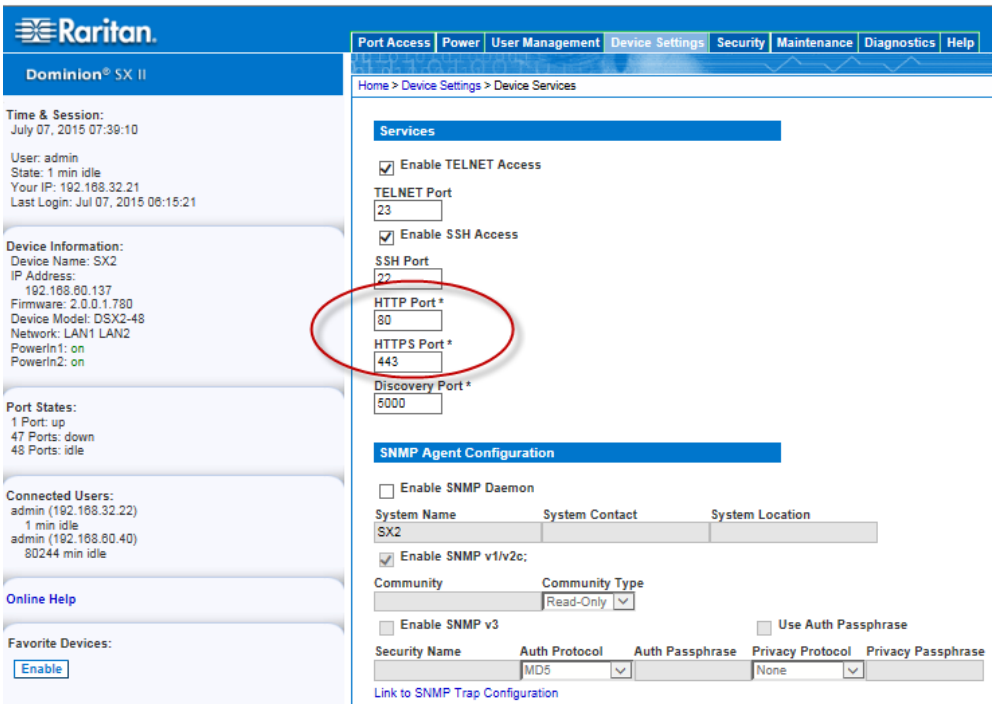
HTTP と HTTPS ポート設定の変更

必要があれば、SX II で用いる HTTP とあるいは HTTPS ポートを変更します。たとえば、デフォルトの HTTP ポートであるポート 80 を別の用途で使用している場合、HTTP 用ポートを変更すると、ポート 80 が HTTP 用として使用されなくなります。

ポートを開けることとポートのプロトコルについては、次を参照してください。 。

HTTP/HTTPS はリモート コンソールあるいはコマンドラインインタフェース (CLI)から無効化あるいは有効化することができます。参照 ***CLI を用いたデバイス設定*** 『214p. 』。

1. デバイス設定 の デバイスサービス を選択します。デバイス サービスページが開きます。
2. ポートフィールドまたはポートフィールド (あるいはその両方) に新しいポート番号を入力します。
3. [OK] をクリックします。



TCP 検出ポートを変更する

SX II の検出は、設定可能な 1 つの TCP ポートで行われます。

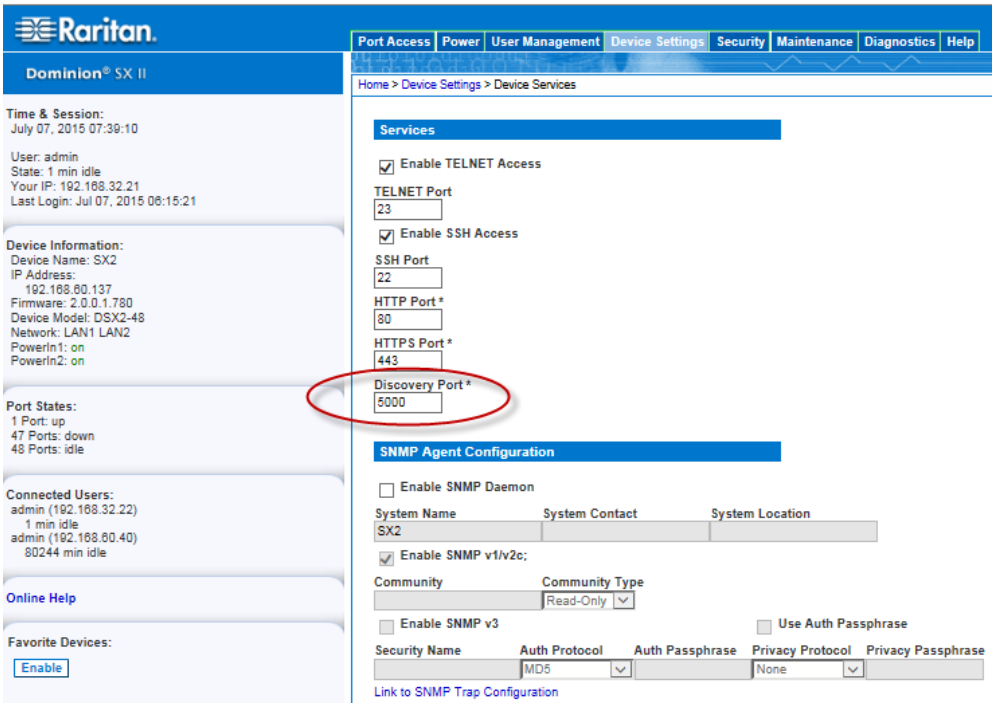
デフォルトではポート 5000 に設定されていますが、80 と 443 以外であれば、どの TCP ポートを使用するよう変更してもかまいません。

ファイアウォールの外側から SX II ユニットにアクセスするには、お使いのファイアウォールの設定で、デフォルト ポート 5000 または上記で設定したデフォルト以外のポートを使用する双方向通信を有効にする必要があります。

ポートを開けることとポートのプロトコルについては、次を参照してください。 。

TCP 検出ポート はリモート コンソールあるいはコマンドラインインタフェース (CLI)から設定することができます。参照 *CLI を用いたデバイス設定* 『214p. 』。

1. デバイス設定 の デバイスサービス を選択します。デバイス サービスページが開きます。
2. 検出ポート を入力します。
3. [OK] をクリックします。



ダイレクト ポート アクセスの有効化

ダイレクト ポート アクセスにより、ユーザはデバイスのログイン ダイアログ ボックスとポート アクセス ページを使用する必要がなくなります。

ポートに直接アクセスする方法が３通りあります。

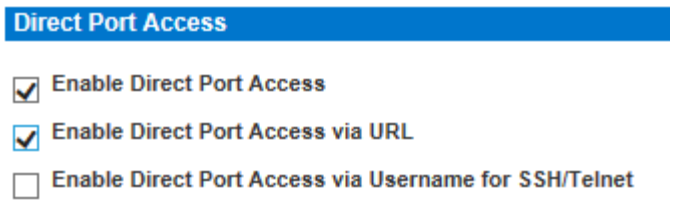
ダイレクト ポート アクセス はリモート コンソールあるいはコマンドラインインタフェース (CLI)から設定することができます。参照 ***CLI を用いて ダイレクト ポート アクセス を設定する*** 『215p. 』。

『ダイレクト ポート アクセスの有効化』と『URL 経由の直接ポートアクセスを有効化』

- URL 経由の直接ポートアクセス – この機能は以下のシンタックスの中の１つを用いて HTTP/HTTPS 経由の直接ポートアクセスの機能を提供するものです。
  - `https://IPaddress/dpa.asp?username=username&password=password&port=port number`
  - `https://IPaddress/dpa.asp?username=username&password=password&portname=port name`

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

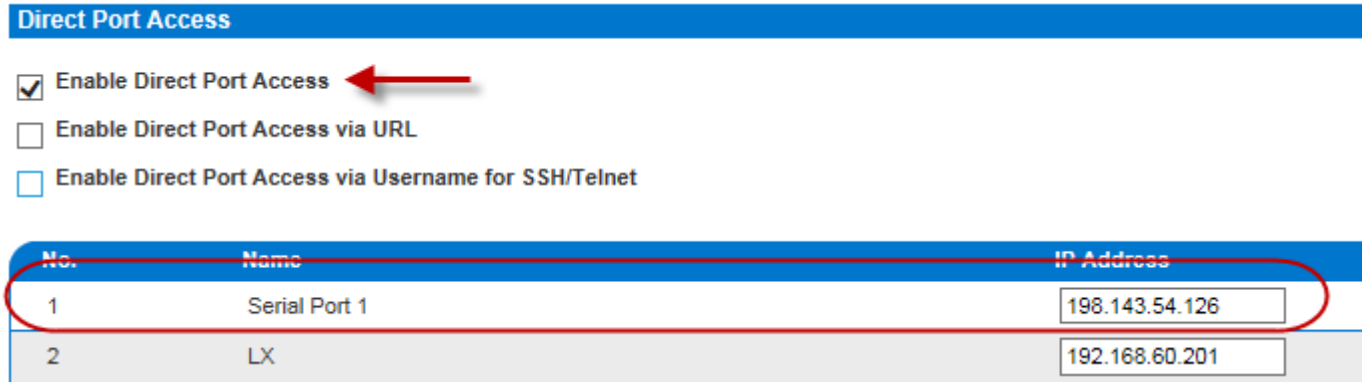
1. この機能を有効化するには デバイス設定 > デバイスサービス を選択します。、デバイス サービスページが開きます。
2. 直接ポート アクセスの有効化セクションで、直接ポート アクセスを有効にするのチェックボックスと［Enable Direct Port Access via URL］のチェックボックスを選択します。
3. ［OK］をクリックして設定を適用します。



特定した TCP ポートあるいは特定した IP アドレスを用いて SSH/Telnet 経由の ダイレクト ポート アクセス を有効にします。

この機能を使うには、SSH/Telnet が SX II にアクセスするために用いることのできる特定した IP アドレスあるいは特定した TCP ポートを設定する必要があります。そのアドレスは SX II の IP アドレス と TCP ポートとは異なるものでなければなりません。

1. デバイス設定 の デバイスサービス を選択します。
2. 直接ポート アクセスのセクションで、直接ポートアクセスを有効にする のチェックボックスを選択します。
3. このチェックボックスの下のテーブルにあるポートを求め、そしてポートに割り当てる IP アドレス を入力します。
4. [OK] をクリックして設定を適用します。



ユーザ名経由の SSH/Telnet ダイレクト ポート アクセスの有効化

この機能は特定した IP アドレスあるいは TCP ポートを要求することなくユーザ名とポートの組み合わせで DPA にアクセスする能力を提供します。

使用法とシンタックス：

- `ssh -l name[:portname/number] SXIP`

ポート-#1 に Admin としてアクセスする例：

- ssh -l admin 192.168.51.101

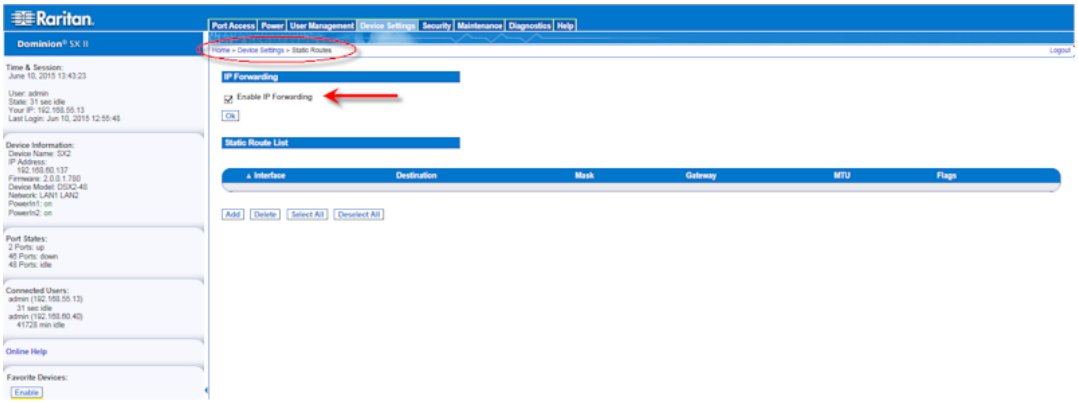
1. デバイス設定 の デバイスサービス を選択します。デバイス サービスページが開きます。
2. 直接ポート アクセスのセクションで、直接ポートアクセスを有効にする のチェックボックスと [Enable Direct Port Access via Username for SSH/Telnet] のチェックボックスを選択します。
3. [OK] をクリックして設定を適用します。

IP 転送と静的ルート

SX II が 2 つの LAN ポートを持っているかモデムアクセスように設定されている場合、IP 転送あるいは静的ルートを作ることを有効にします。

▶ **IP 転送を可能にするには：**

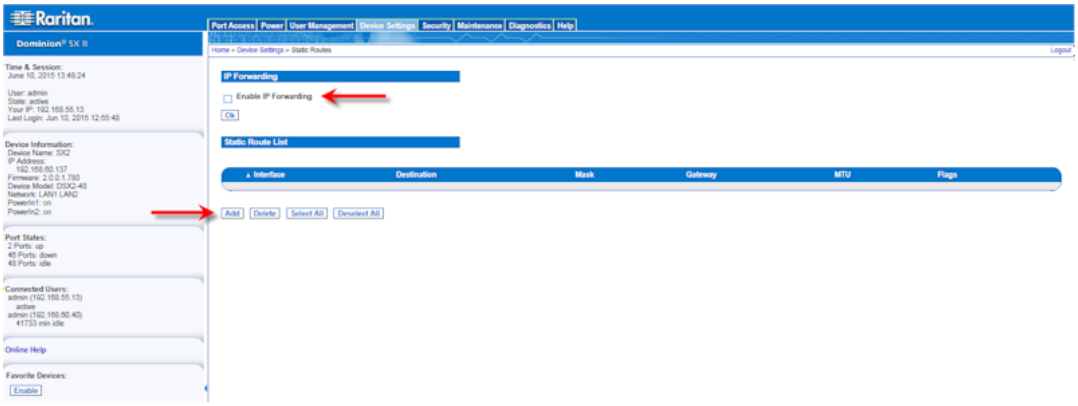
1. デバイス設定の静的ルートを選択します。静的ルートのページが開きます。
2. IP 転送のパネルに行き IP フォワーディングを有効にする チェックボックスをクリックしています。



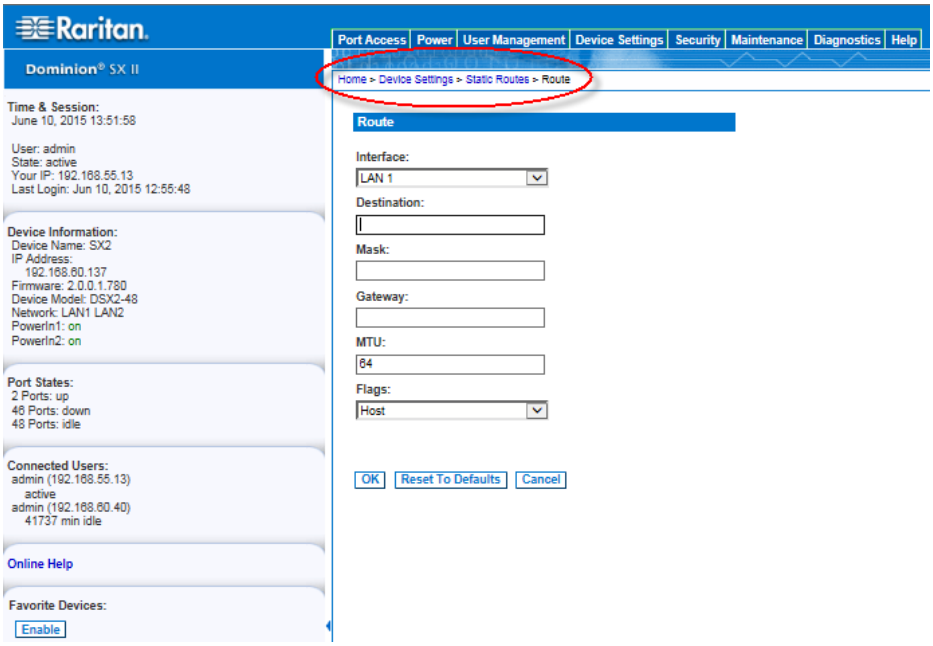
▶ **静的ルートを追加するには、以下の手順に従います。**

1. デバイス設定の静的ルートを選択します。静的ルートのページが開きます。

2. 静的ルートのリストに行き 追加 をクリックします。



ルートフィールドが表示されます。



3. インターフェースフィールドのドロップダウンメニューから設定したいものを選択します。
   - LAN1 = eth0
   - LAN2 = eth1
4. IP アドレス、サブネットマスク、と宛先における目的ホストのゲートウエイ、マスク、そしてゲートウエイ フィールドを記入します。
5. [MTU] フィールドに最大転送ユニット(MTU) をバイト数で記入します。
6. ウインドウフィールドにこのルートを通じての接続のための TCP ウインドウ サイズをバイト数で記入します。
7. フラグのドロップダウンメニューからルートのタイプを選択します。

- ホストはこのルートがホストマシンのためのものであることを意味します。
- ネットはこのルートがサブネットであることを意味します。

8. [OK] をクリックします。

静的ルートをリセットするには、以下の手順に従います。

1. デバイス設定　の 静的ルート を選択します。静的ルートのページが開きます。
2. デフォルトにリセットをクリックしてルートを工場出荷時のデフォルトにリセットします。

静的ルートを削除するには

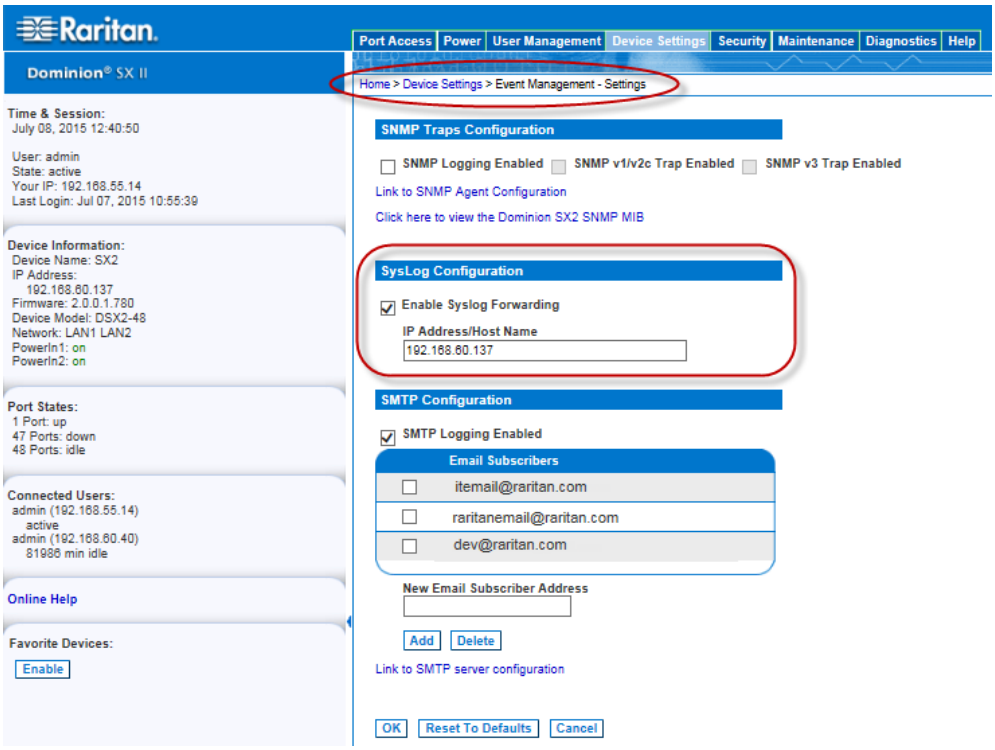
1. デバイス設定　の 静的ルート を選択します。静的ルートのページが開きます。
2. 静的ルートのリストに行き削除するルートの次にあるチェックボックスをクリックします。
3. 削除をクリックします。削除を確認するプロンプトが表示されます。
4. ［OK］をクリックします。そのルートが削除されます。

Syslog 転送を有効化する

この機能はすべてのシステムの行動を記録しそしてそれをリモートの Syslog サーバに転送するものです。

1. デバイス設定　のイベント管理を選択します。イベント管理 – 設定ページが開きます。
2. Syslog フォワーディングを有効にするを選択して、リモート Syslog サーバに装置の メッセージのログを送信します。
3. [IP Address] フィールドに Syslog サーバの IP アドレスまたはホスト名を入力します。

4. [OK] をクリックします。



注:IPv6 アドレスでは、ホスト名は最大 80 文字です。

- この設定をリセットするにはページ下部にあるデフォルトにリセットするをクリックします。

リモート コンソールから日付と時刻の設定をする

日付/時刻の設定ページを使用して、 SX II の日付と時刻を指定します。割り当て方法は 2 通りあります:

- 手動で日付と時刻を設定する。
- 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期する。

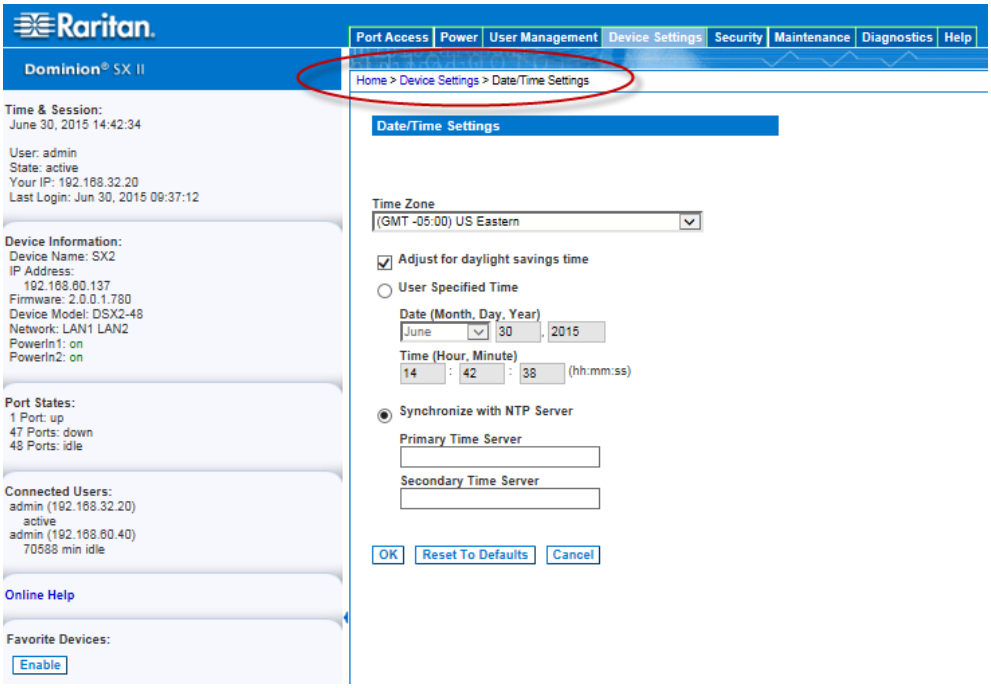
▶ 日付と時刻を設定するには、以下の手順に従います。

1. デバイス設定 の > 日付/時刻を選択します。日付/時刻の設定ページが開きます。
2. タイム ゾーンドロップダウン リストから適切なタイム ゾーンを選択します。
3. 夏時間用の調整を行うには、夏時間用の調整チェックボックスをオンにします。

4. 日付と時刻の設定に用いる方法を選択します。
   - ユーザによる時刻定義 – 日付と時刻を手動で入力する場合に、このオプションを使用します。ユーザによる時刻定義オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
   - NTP サーバと同期 – 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期するには、このオプションを選択します。
5. NTP サーバと同期オプションを選択した場合は、以下の手順に従います。
   a. プライマリ タイム サーバ)の IP アドレスを入力します。
   b. セカンダリ タイム サーバ)の IP アドレスを入力します。〈オプション〉

注:ネットワークページのネットワーク設定で [DHCP] が選択されている場合、NTP サーバ IP アドレスは、デフォルトでは DHCP サーバから自動的に取得されます。NTP サーバ IP アドレスを手動で入力するには、DHCP を無効にするチェックボックスをオンにします。

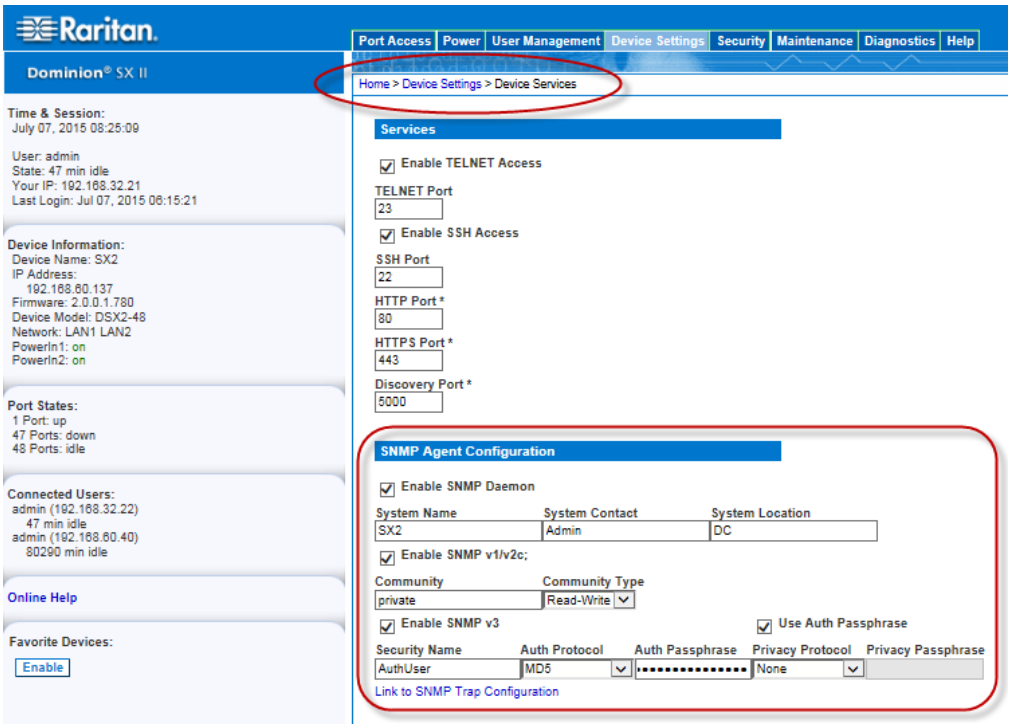
6. OK をクリックします。



リモート コンソールから SNMP エージェントの設定をする

SNMP に準拠したデバイスはエージェントと呼ばれます。それ自体のデータは Management Information Base (MIB) に格納され、デバイスはそのデータを SNMP マネージャに返します。SX II の MIB の表示方法については、「*SX II の MIB の表示*『132p. の*"Viewing the SX II MIB"*参照 』」を参照してください。

SX II は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およびプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提供します。



1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. SNMP デーモンのチェックボックスを選択し SNMP セクションを有効化します。
3. MIB-II システム グループ オブジェクトに次の SNMP エージェント識別子情報を設定します。
   - システム名 - SNMP エージェントの名前/デバイス名
   - システム コンタクト - 装置に関連する連絡先名
   - システム ロケーション - 装置の場所

4. SNMP v1/v2c を有効にするまたは SNMP v3 を有効にするを選択するか、その両方を選択します。少なくとも 1 つのオプションを選択する必要があります。必ず入力してください。
5. SNMP v1/v2c 用の次のフィールドに入力します（必要な場合）。
   - コミュニティ – 装置のコミュニティ文字列
   - Community Type – コミュニティ ユーザに読み取り専用または読み書き可能のアクセスを許可

注:SNMP コミュニティとは、SNMP を実行している装置と管理ステーションが所属するグループのことです。情報の送信先を定義するのに役立ちます。コミュニティ名はグループを特定するために使用されます。SNMP デバイスまたはエージェントは複数の SNMP コミュニティに所属している場合があります。

---

6. SNMP v3 用の次のフィールドに入力します（必要な場合）。
   - 必要な場合は、認証パスフレーズの使用を選択します。認証用のパスフレーズとプライバシーパスフレーズに同じパスフレーズを使い再入力しなくてよいようにするにはこのオプションを選択します。
   - セキュリティ名 – SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名（32 文字以内）。
   - 認証プロトコル)– SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル。
   - 認証パスフレーズ – SNMP v3 エージェントへのアクセスに必要なパスフレーズ（64 文字以内）
   - プライバシー プロトコル – 必要に応じて PDU やコンテキストデータの暗号化に使用される AES または DES アルゴリズム。
   - プライバシー パスフレーズ – プライバシー プロトコル アルゴリズムへのアクセスに使用されるパスフレーズ（64 文字以内）

次に、 SNMP トラップを設定します。これはイベント管理–設定ページで、デバイス サービスのページの一番下にある SNMP トラップ設定へのリンクをクリックすることで素早くアクセスできます。参照 SNMP トラップの設定 ここに SNMP トラップ作成の情報があります。また SX II SNMP トラップのリスト では SX II の利用できる SNMP トラップのリストがあります。

SNMP トラップを設定するとキャプチャされるイベントは、[Event Management – Destinations]（イベント管理 – 送信先）ページで選択されます。「[Event Management – Destinations]（イベント管理 – 送信先）の設定」を参照してください。

リモート コンソールから SNMP トラップを設定する

Simple Network Management Protocol (SNMP) は、ネットワーク管理を制御し、ネットワーク デバイスとその機能を監視するためのプロトコルです。SNMP は情報収集のネットワーク上でトラップあるいは通告をを送る能力を提供します。この情報は 1 つあるいは複数の条件が適合すると管理者に助言を与えるのに用いられます。

SNMP に準拠したデバイスは、エージェントと呼ばれ、そのデバイスのデータを Management Information Bases (MIB) に格納し、SNMP トラップに応答します。

SNMP エージェントは、SX II の デバイス サービス ページで設定されます。参照 *SNMP エージェントの設定*『126p. の*"リモート コンソールから SNMP エージェントの設定をする"*参照 』 ここでは SNMP エージェントの設定の情報があり、また *SX II MIB を見る* 『132p. の*"Viewing the SX II MIB"*参照 』では SX II の MIB を見るための情報があります。

ヒント:[Link to SNMP Agent Configuration] (SNMP エージェント設定へのリンク) リンクを使用すると、イベント管理 - 設定 ページから デバイス サービス ページにすばやく移動できます。

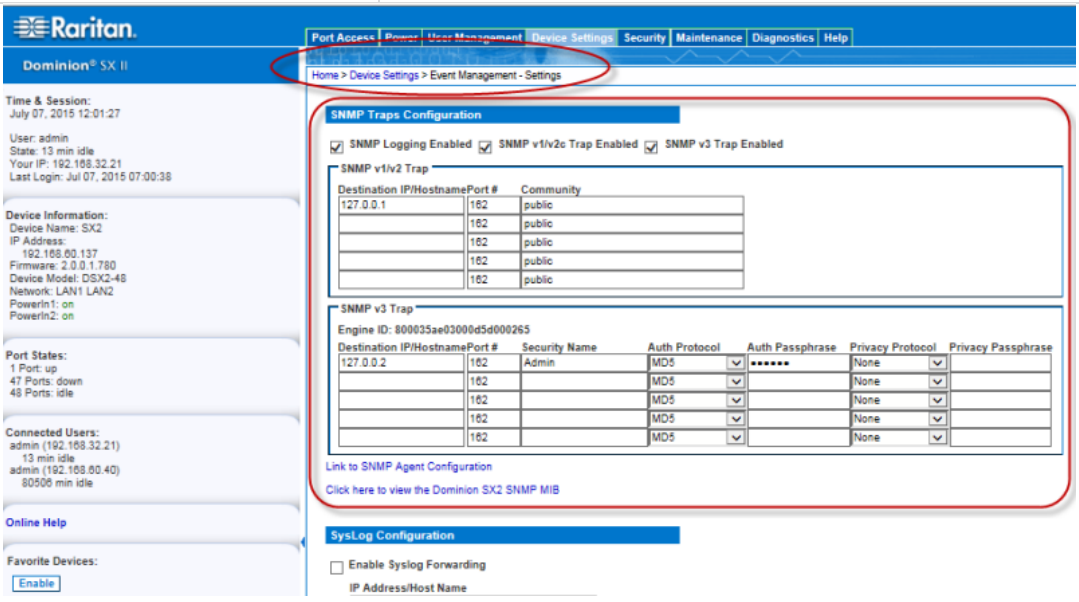
SNMP トラップは、イベント管理 - 設定 ページで設定されます。

SX II の SNMP トラップを次の表に示します。

トラップ	記述
automaticScriptConfiguration	デバイスが自動設定を試みました
configBackup	デバイス設定はバックアップされました。
configRestore	デバイス設定は復元されました。
deviceUpdateFailed	デバイスの更新に失敗しました。
deviceUpgradeCompleted	RFP ファイルを使用した SX II のアップデートが完了しました。
deviceUpgradeStarted	RFP ファイルを使用した SX II のアップデートが開始されました。
ethernetFailover	障害復旧モードで、障害が起こったことを示します。
factoryReset	デバイスが工場出荷時のデフォルトにリセットされました。
firmwareFileDiscarded	ファームウェア ファイルが破棄されました。
firmwareUpdateFailed	ファームウェアを更新できませんでした。
firmwareValidationFailed	ファームウェアの検証に失敗しました。
groupAdded	グループが SX II システムに追加されました。
groupDeleted	グループがシステムから削除されました。

トラップ	記述
groupModified	グループが変更されました。
ipConflictDetected	IP アドレスの競合が検出されました。
ipConflictResolved	IP アドレスの競合が解決されました。
networkFailure	製品の Ethernet インタフェースがネットワーク経由で通信できなくなりました。
networkParameterChanged	ネットワーク パラメータに変更が加えられました。
networkParameterChangedv2	2 重 LAN 分離モードで作動中にネットワーク パラメータに変更が加えられました。
passwordSettingsChanged	強力なパスワードの設定が変更されました。
pduConnected	電源タップが SX II に接続されました。
pduDisconnected	電源タップが SX II から切断されました。
portConnect	以前認証されたユーザがセッションを開始しました。
portConnectv2	2 重 LAN 分離モードで作動中に以前認証されたユーザが別の IP アドレスを用いてセッションを開始しました。
portConnectionDenied	ターゲット ポートへの接続が拒否されました。
portDisconnect	セッションを実行中のユーザが正常にセッションを終了しました。
portDisconnectv2	2 重 LAN 分離モードで作動中に、セッションを実行中のユーザが正常にセッションを終了しました。
portStatusChange	ポートが使用不可能な状態になっています。
powerNotification	電源の次の状態の通知です：1: アクティブ、0: 非アクティブ
powerOutletNotification	電源コンセントの状態の通知です。
rebootCompleted	SX II の再起動が完了しました。
rebootStarted	システムへの電源の入れ直しまたは OS からのウォーム起動により、SX II は再起動を開始しました。
securityBannerAction	セキュリティ バナーが承諾または拒否されました。
securityBannerChanged	セキュリティ バナーに変更が加えられました。
securityViolation	セキュリティ違反です。
setDateTime	デバイスの日付と時刻が設定されました。
setFIPSMode	FIPS モードが有効になりました。
startCCManagement	デバイスが Comm と Center の管理下におかれました。

トラップ	記述
stopCCManagement	デバイスが Comm と Center の管理下から除外されました。
sxPortAlert	そのポートにトリガーが掛けられました
userAdded	ユーザ がシステムに追加されました。
userAuthenticationFailure	不正なユーザ名または/およびパスワードでのログイン試行がありました。
userDisconnectedFromPort	ユーザがターゲットポートのリストから切断されました。
userConnectionLost	あるユーザのアクティブ セッションが、異常終了しました。
userDeleted	ユーザ アカウントが削除されました。
userForcedLogout	ユーザは管理者によって強制的にログアウトされました。
userLogin	ユーザが SX II へ正常にログインし、認証されました。
userLogout	ユーザが SX II から正常にログアウトしました。
userModified	ユーザ アカウントが変更されました。
userPasswordChanged	デバイスのいずれかのユーザのパスワードが変更されると、このイベントが発生します。
userSessionTimeout	あるユーザのアクティブ セッションが、タイムアウトにより終了しました。
userUploadedCertificate	ユーザが SSL 証明書をアップロードしました。



1. SNMP トラップの宛先を設定するには、デバイス設定 からイベント管理—設定を選択するか、デバイス サービスのページの一番下にある SNMP トラップ設定へのクイックリンクをクリックします。イベント管理 - 設定 ページが開きます。
2. ログをっ有効にするチェックボックスをオンにすると、そのセクションの残りのチェックボックスが有効になります。必ず入力してください。
3. SNMP v1/v2c トラップを有効にするまたは SNMP Trap v3 を有効にするを選択するか、その両方を選択します。

   少なくとも 1 つのオプションを選択する必要があります。

   選択すると、関連するすべてのフィールドが有効になります。必ず入力してください。
4. SNMP v1/v2c 用の次のフィールドに入力します (必要な場合)。
   - 送信先 IP/ホスト名]- SNMP 送信先の IP またはホスト名。最大 5 つの SNMP トラップの宛先を作成できます。

   注:IPv6 アドレスでは、ホスト名が最大 80 文字です。

   - ポート番号 - SNMP マネージャで使用されるポート番号
   - コミュニティ - 装置のコミュニティ文字列

   注:SNMP コミュニティとは、SNMP を実行している装置と管理ステーションが所属するグループのことです。情報の送信先を定義するのに役立ちます。コミュニティ名はグループを特定するために使用されます。SNMP デバイスまたはエージェントは複数の SNMP コミュニティに所属している場合があります。
5. SNMP v3 用の次のフィールドに入力します (必要な場合)。
   - 送信先 IP/ホスト名]- SNMP 送信先の IP またはホスト名。最大 5 つの SNMP 宛先を作成できます。

   注:IPv6 アドレスでは、ホスト名が最大 80 文字です。

   - ポート番号 - SNMP マネージャで使用されるポート番号
   - セキュリティ名 - SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名。
   - 認証プロトコル - SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル。
   - 認証パスフレーズ - SNMP v3 エージェントへのアクセスに必要なパスフレーズ。
   - プライベートプロトコル - 必要に応じて PDU やコンテキストデータの暗号化に使用される AES または DES アルゴリズム。
   - プライバシー パスフレーズ - プライバシー プロトコル アルゴリズムへのアクセスに使用されるパスフレーズ。
6. [OK] をクリックして、SNMP トラップ送信先を作成します。

次に、SNMP トラップイベントがどこに送られログされるかを設定します。送信先は、イベント管理 – 送信先 ページで設定されます。「イベント管理 – 送信先 の設定』を参照

SX II は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およびプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提供します。

▶ 既存の SNMP トラップを編集するには、以下の手順に従います。

注:どの時点で SNMP 設定 を無効にしても、SNMP 情報は保持されるので、設定を有効にし直す場合に再入力する必要はありません。

1. デバイス設定 のイベント管理 – 設定を選択します。イベント管理 – 設定 ページが開きます。
2. 必要に応じて変更し、[OK] をクリックして変更を保存します。

▶ SNMP トラップを削除するには、以下の手順に従います。

- SNMP トラップ フィールドをすべてクリアして保存します。

Viewing the SX II MIB

1. デバイス設定（デバイス設定）の [Event Management – Settings]（イベント管理 – 設定）を選択します。[Event Management – Settings]（イベント管理 – 設定）ページが開きます。
2. ここをクリックして SNMP MIB を表示する]のリンクをクリックします。ブラウザ ウィンドウで MIB ファイルが開きます。

イベント管理 - 宛先を設定

システムイベントが有効とされていると、SNMP 通知イベント（トラップ）が生成されます。このイベントは syslog あるいは監査ログに記録されることがあります。

イベントとそのイベントの情報が送られる先はイベント管理–送信先ページで設定できます。

注:SNMP、Syslog と SNMP の記録はイベント管理–設定ページで有効化されているときにのみ行われます。

▶ イベントとその送信先を選択するには、以下の手順に従います。

1. デバイス設定 の > イベント管理 – 送信先を選択します。イベント管理 – 送信先 ページが開きます。

   システム イベントは、デバイス操作、デバイス管理、セキュリティ、ユーザ アクティビティ、ユーザ グループ管理に分類されます。

2. 有効または無効にするイベントラインのアイテムと、情報の送信先のチェックボックスをオンにします。

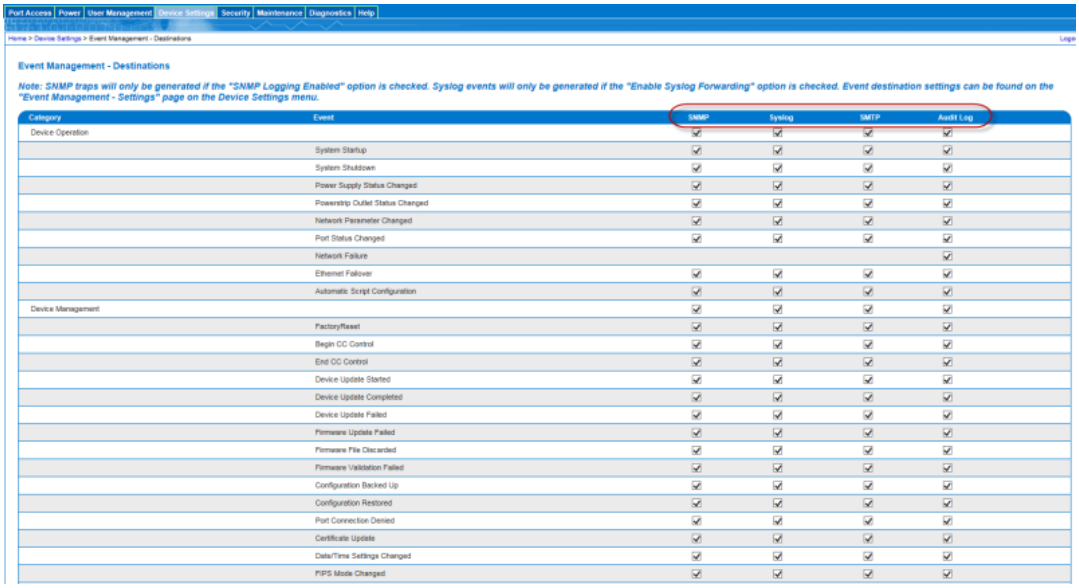
ヒント:カテゴリのチェックボックスをそれぞれオンまたはオフにすると、カテゴリ全体を有効または無効に設定できます。

3. OK をクリックします。

工場出荷時のデフォルトに戻すには、以下の手順に従います:

- デフォルトに戻すをクリックします。

警告: UDP 経由の SNMP トラップを使用している場合は、SX II を再起動したときに SX II と接続先のルータが同期しなくなり、再起動完了の SNMP トラップがログ記録されなくなるおそれがあります。



リモート コンソールから SNMP 通知を有効にする

イベント管理 - 設定 ページで SNMP 通知を有効化します。

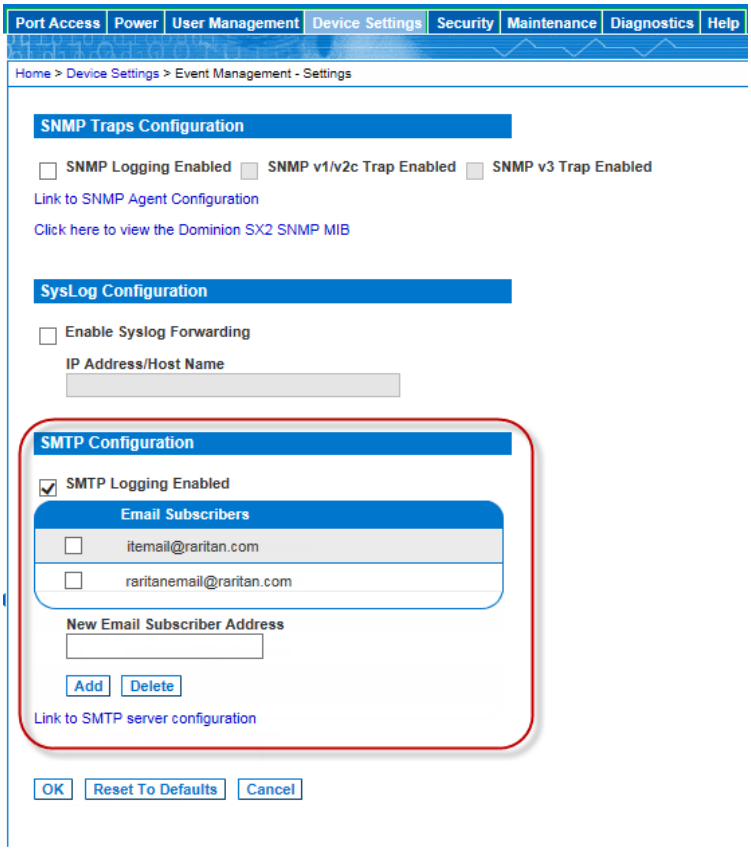
イベントが起こったとき SNMP が有効になっている各人が通知を受け取ります。最大 10 人のユーザが追加できます。

SNMP 設定ページで SNMP サーバの設定を行います。

このページはイベント管理-設定ページで、一番下にある SNMP サーバ設定へのリンクをクリックすることで素早くアクセスできます。

1. デバイス設定 の イベント管理 - 設定を選択し、イベント管理-設定ページを開きます。

2. SMTP 設定パネルに行きそして SMTP サーバを有効のチェックボックスを選択します。



3. フィールドに SMTP の読者の e-メー新 E メール読者アドレスルアドレスを記入します。
4. [OK] をクリックします。

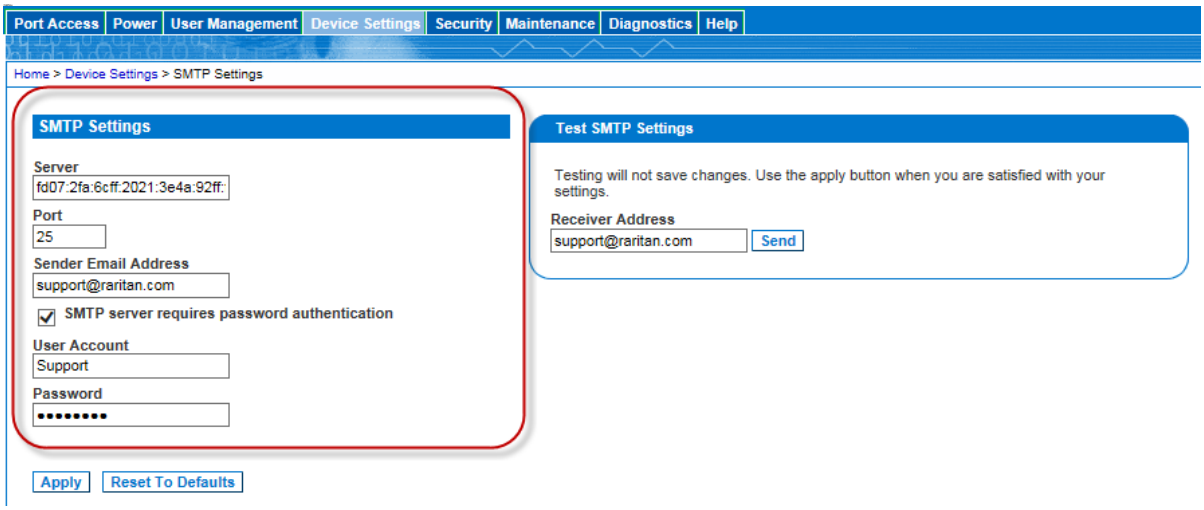
SMTP サーバ設定の形成とテスト

SMTP サーバ設定のページで SMTP サーバへの接続に必要な情報を記入します。

このサーバが STARTTLS を必要とした場合、SX II が自動的にそれを使用することを承知してください。

1. デバイス設定 > SMTP 設定 を選択します。
2. サーバのアドレス、ポートと SMTP 通知を送るのに用いられる e メールアドレスを提供します。

3. サーバが e メールを送るためにユーザ名とパスワードを要求する場合、ーザアカウントとパスワード のフィールドにそれぞれ記入します。
4. 適用 をクリックします。

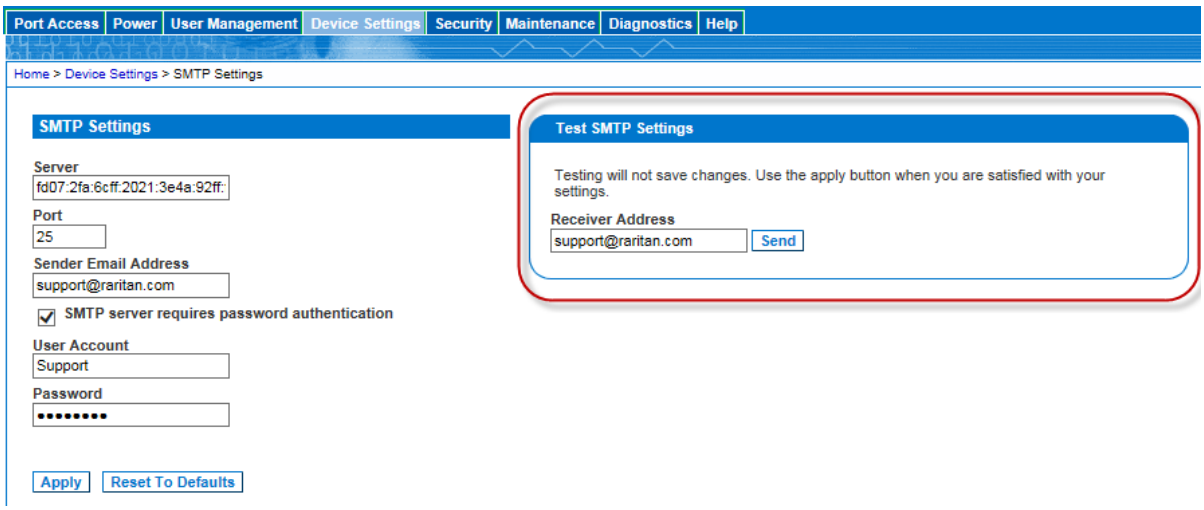


SMTP サーバの情報は正確で、SX II の装置が SMTP サーバを用いてメッセージを送れることが重要です。

このテストではそのページの SMTP 設定枠に表示された設定を用いて e メールを送ります。SX II は適用をクリックすると設定を保存します。

1. テストメッセージを受けるように宛先 e メールを記入してテスト用 e メールを送ります。

   受け取り e メールは保存されないことを了解しておいて下さい。
2. 意図したメールの送信先でメッセージが受け取られることを検証します。もし問題があれば、、SMTP 管理者に連絡を取り、SMTP サーバの IP アドレスと認証情報が正しいことを確認します。

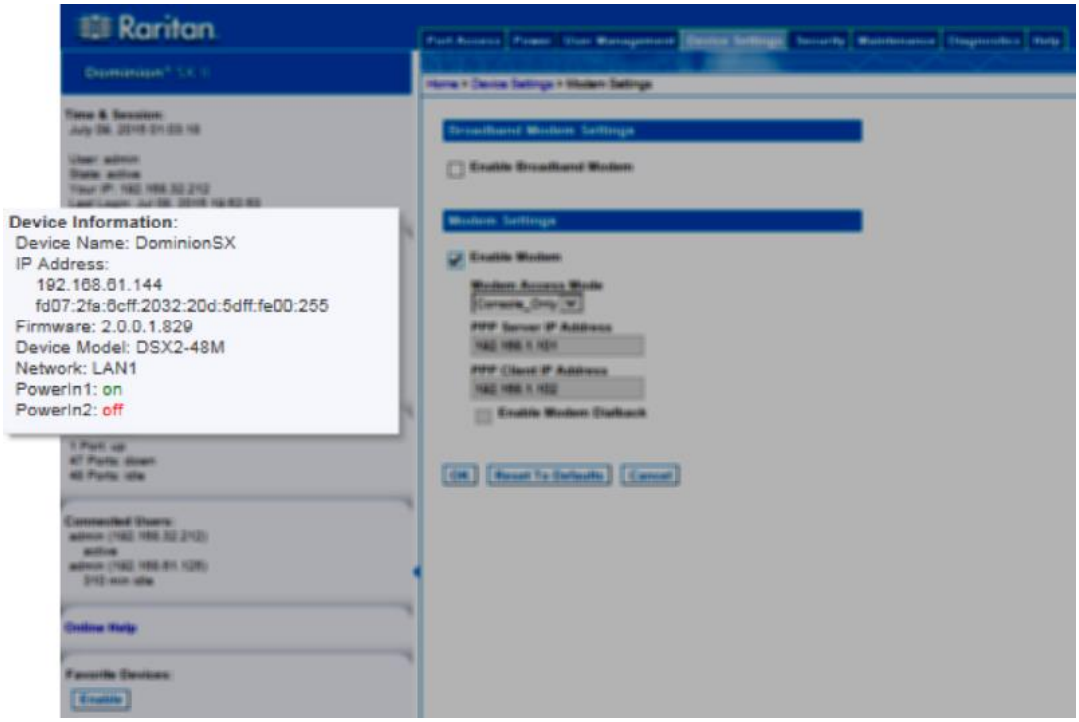


リモート コンソールからモデムを設定する

モデム設定ページで内蔵アナログモデムを持つ SX II モデルのモデムの設定を行います。コマンドラインインタフェース経由での遠隔認証の設定もできます。参照 *CLI を用いてのモデムの設定* 『210p. の*"CLI を用いたモデムの設定"*参照 』。

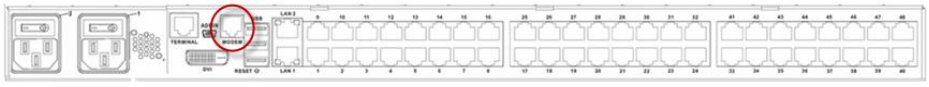
注:内蔵モデムを持たない SX II のモデルでは、モデム設定へのアクセスは持っていません。

内蔵モデムを持つ SX II のモデルはモデル名に M を持ち、例えば DSX2-4M のようになります。モデルのリストは、次を参照してください。*SX II モデル* 『10p. 』。リモート コンソールの左パネルにあるデバイス情報の下を見ればモデル名がわかります。



モデムポート経由で内蔵モデムに接続します。

- SX II 上のモデムポートに接続された電話ケーブルを使用します。



内蔵モデムの設定を構成します。

1. デバイス設定 のモデム設定をクリックし、モデム設定 ページを開きます。

注:ブロードバンドモデムの機能を有効化することは外付けワイヤレスモデムの使用に特有のものです。参照 **外付けモデムに接続しグローバルアクセスを可能にする。** *『140p. の "外部ブロードバンドモデムに接続しグローバルアクセスを有効にする" 参照 』。*

2. モデムを有効にするを選択します。
3. モデムアクセスモードを次から選択します。
   - 全て – PPP とコンソールアクセスの両方でアクセスすることができます。

     PPP 信号が検出されない場合は、コンソールアクセスを使用します。

     このモードでは、モデムのダイアルバック機能が使用できません。
   - PPP_のみ – は PPP 接続のみが可能で SX II には設定した PPP サーバの IP アドレスを通じてアクセスします。
   - コンソールのみ – ローカルのコンソール接続のみが可能で、Hyperterminal のような端末エミュレーションプログラムを通じて CLI がアクセスします。
4. モデムのアクセスモードに全てあるいは PPP_のみを選択した場合には、 IP アドレス 情報を入力します。
   - [PPP サーバ IP アドレス にアドレスを入力します。

     これは接続がダイアルアップ経由で確立されたときに SX II に割り当てられたアドレスです。必ず入力してください。
   - PPP クライアント IP アドレス にアドレスを入力します。

     ダイヤルアップ経由で接続を確立したときに、 SX II に割り当てられるインターネット アドレスです。必ず入力してください。

注:PPP サーバ IP アドレス と PPP クライアント IP アドレス は同じ値にしないでください。また、サーバやクライアントが使用するネットワーク アドレスとも競合しないようにしてください。

5. モデムのアクセスモードに PPP_のみを選択した場合には、モデムダイヤルバック機能を有効にするをそのチェックボックスを選択して有効にします。

   ダイアルバックは PPP_のみを利用した場合にのみ可能となり、それは直接モデムアクセスが PPP_のみで提供されるセキュリティ保護を迂回する理由によります。

   トーンダイアルバックがサポートされ、パルスダイアルバックはサポートされていません。

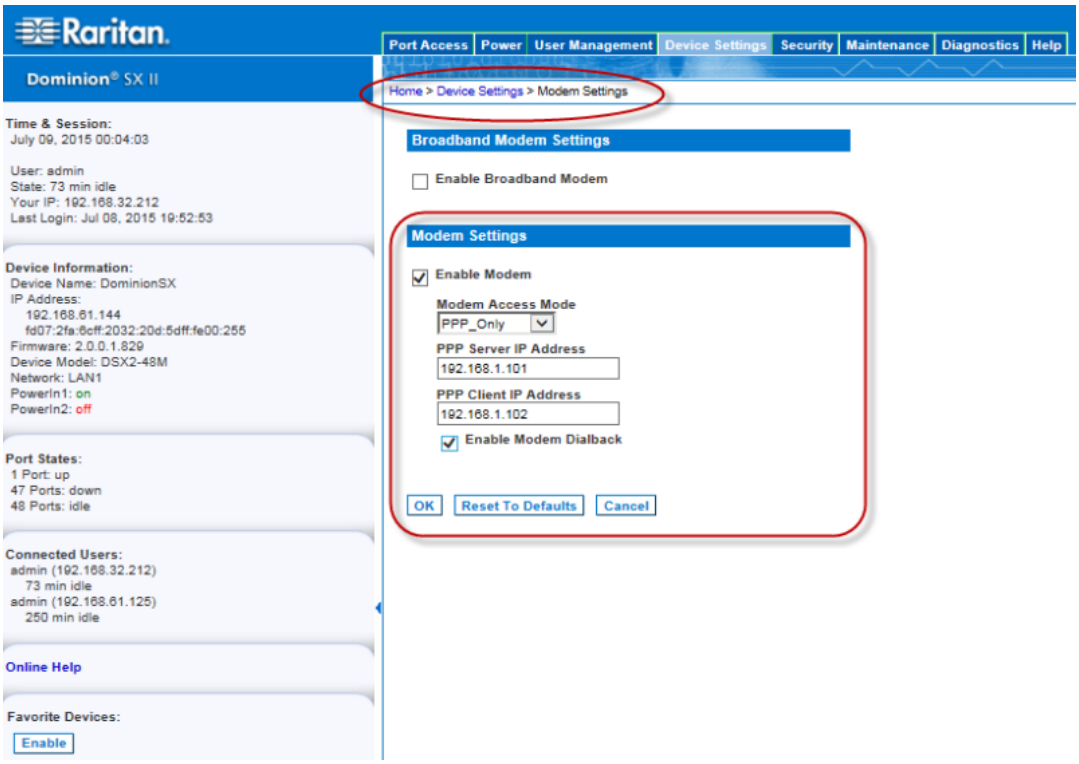
   モデムでダイアルインとダイアルバックの両方が有効となっている必要があり、ユーザのためのダイアルバック番号は認証サービス（ローカル、RADIUS、LDAP あるいは TACACS+ ）で設定されている必要があります。

モデムアクセスの許可があるユーザグループに属するが、ダイアルイン番号を持たないユーザは PPP 接続を確立することができません。

ダイヤルバックを有効にした場合、モデムを介して SX II にアクセスするユーザには、そのプロファイルでコールバック番号が定義されている必要があります。

ダイアルバックはコールの発信者が最初のダイアルインに対する応答で直ちに呼び戻されるときに起こります。

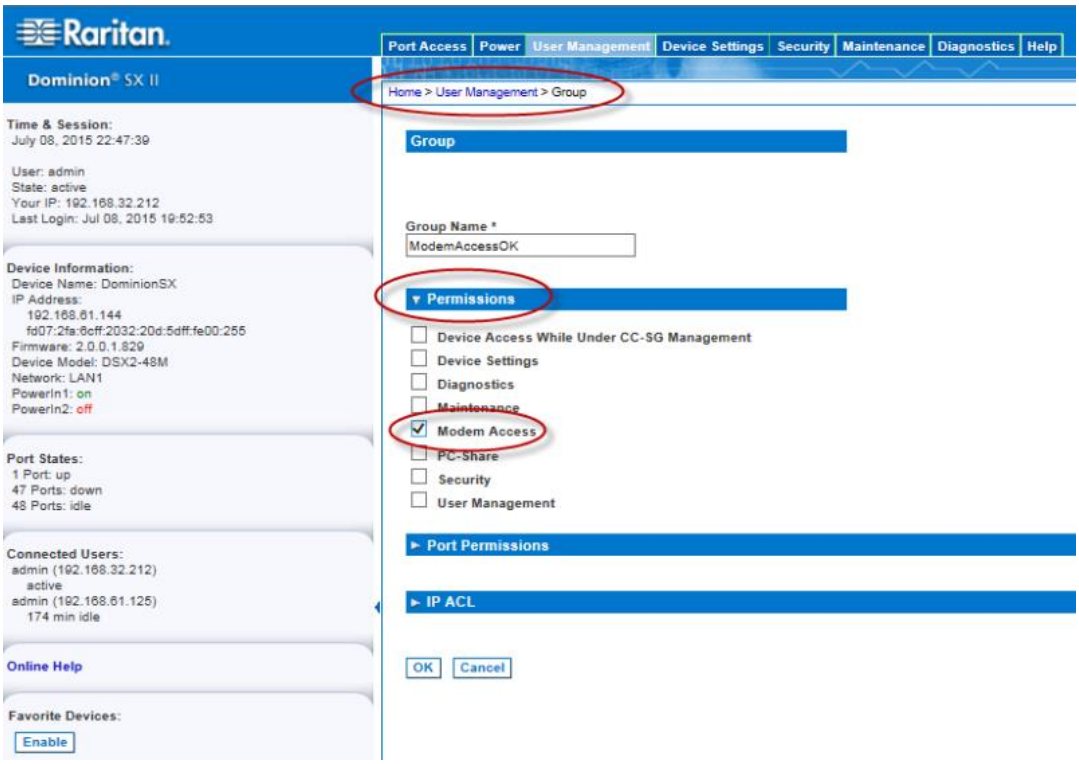
6. [OK] をクリックして変更を確認するか、デフォルトにリセットするをクリックして設定をデフォルトに戻します。



ユーザグループにモデム アクセス許可を割り当てます。

- 必要があれば、モデムアクセスの許可を持つグループにユーザを割り当てます。

  グループのページでモデムアクセスの許可をユーザグループに割り当て、それからユーザのページでユーザをそのグループに割り当てます。詳細については、以下を参照してください。 *リモート コンソールからユーザとグループを設定・管理する* 『78p. 』。



外部ブロードバンドモデムに接続しグローバルアクセスを有効にする

SX II のすべてのモデルは USB 経由で Sierra Wireless AirLink® GX440 ゲートウエイモデムを用い外部 3G/4G ワイヤレスモデムの接続をサポートしています。

GX440 モデム経由で SX II にアクセスする必要のあるユーザはモデムアクセス許可のあるユーザグループに割り当てられる必要があります。これはセキュリティ上の手段で、誰がモデム経由で SX II にアクセスできるかを制御するのに助けとなります。例えば、gx440 ユーザと呼ぶユーザグループを作成し、そのグループにモデムアクセス許可を与え、そしてモデムにアクセスする必要のあるユーザにだけそのグループに割り当てます。

さらに、ブロードバンドモデム有効化の機能は SX II で有効化されユーザが gx440 モデム経由で SX II にアクセスできるようにします。これはグローバルレベルの機能で、デフォルトでは不能とされすべてのユーザがモデム経由で SX II にアクセスできることを防いでいます。

GX440 ソフトウエアとファームウエアのバージョン

GX440 は少なくとも ALEOS ソフトウエアバージン 4.4.1.014 を持っている必要があります。

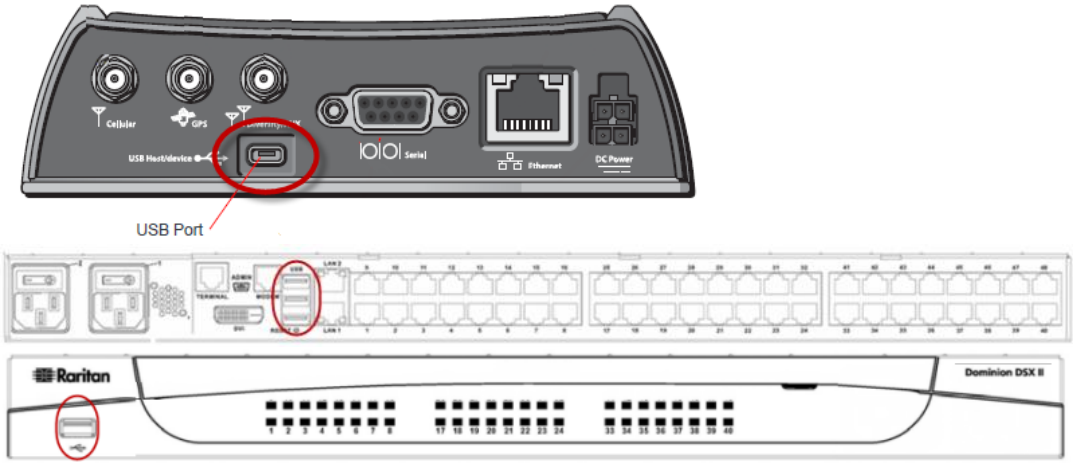
Raritan ではこの設定を Verizon Wireless MC7750 Radio Module をファームウエア バージョン 3.05.10.13 でテストを行っています。

外部、ワイヤレスモデムの接続

USB 接続

Micro A あるいは Micro B のいずれかを用いて USB タイプ A ケーブルで GX440 を SX II に接続します。

- GX440 USB ポートを SX II の背面の 3 つの USB ポートあるいは SX II の前面の USB ポートに接続します。



注:USB 接続だけがサポートされています。

GX440 を設定

以下はこれらの接続を用いて GX440 を SX II で使用するための設定手順です。

これらの設定は SX II ではなく GX440 モデムの上で行われます。

GX440 をセルラー接続ように設定する

- サービスプロバイダーから SIM カードを購入し GX440 にインストールします。
- サービスプロバイダーから静的 IP アドレスを得てそれを GX440 に割り当てます。
- GX440 はパブリックモードに設定します。
- ホスト接続モードは USB Uses Public IP にセットします。
- USB デバイスのモードは[USBNET] にセットします。

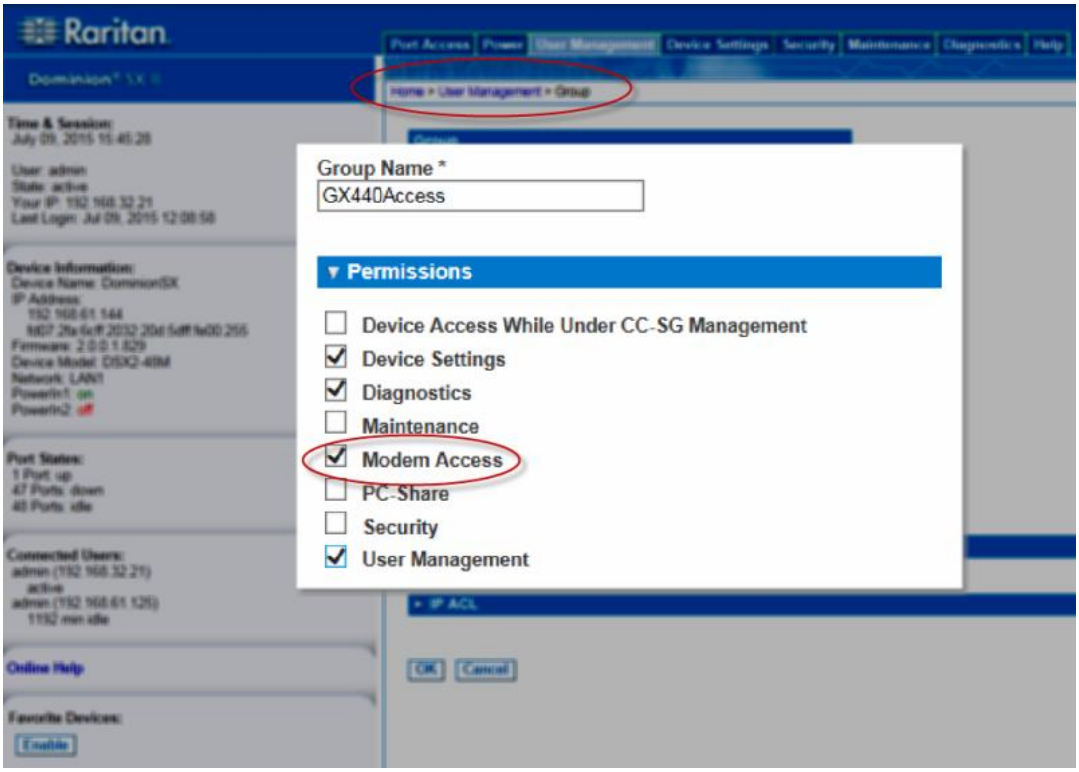
デフォルトユーザ名を変更します。

セキュリティ上の理由から、Raritan は GX440 を使用する前にあなたがデフォルトの Admin アカウントのユーザ名を新しい名前に変更されるよう勧めます。

ユーザグループにモデム アクセス許可を割り当てる

以下は SX II で適用される設定です。

- グループのページでモデムアクセスの許可をユーザグループに割り当て、それからユーザのページでユーザをそのグループに割り当てます。詳細については、以下を参照してください。 *ユーザプロファイルとグループ*『78p. の*"リモート コンソールからユーザとグループを設定・管理する"*参照 』。



ブロードバンドモデムのアクセスの有効化/無効化

この機能は外部 GX440 モデムへのアクセスを有効化/無効化するのに使います。

ブロードバンドはデフォルトでは無効になっています。これはグローバルレベルの機能であるため、すべてのユーザに対しては無効とされています。

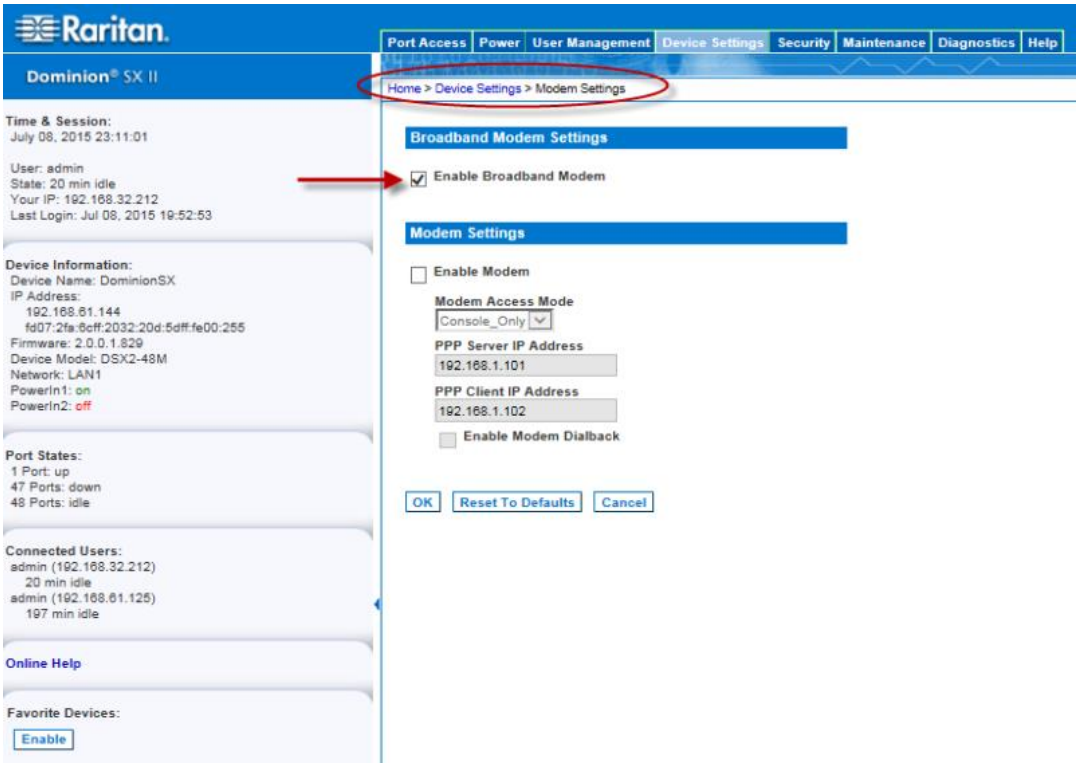
いったんこれが有効化されると、GX440 モデム経由で SX II にアクセスする必要のあるユーザはモデムアクセス許可のあるユーザグループに割り当てられる必要があります。

ブロードバンドはリモートクライアントと CLI 経由で有効化できます。

ブロードバンドをリモート コンソールから有効化するには：

1. デバイス設定 > モデム設定と選択することでブロードバンドを有効化し、ブロードバンドモデムを有効にするのチェックボックスを選択します。
2. [OK] をクリックして設定を適用します。

   これで SX II は GX440 経由でアクセス可能です。



外部モデムの接続状態とチェック

接続イベントは SX II の監査ログに記録されます。

一旦デバイスがオンとなり接続が有効となると、ゲートウエイ IP アドレス はリモート コンソールのネットワークセクションの左側パネルに表示されます。

さらに、ゲートウエイ IP アドレス はネットワーク設定ページの IPv4 section のデフォルト ゲートウエイのフィールドに表示されます。

SX II に接続されている他のターゲットと共に、SX II の診断ツールを用いて GX440 の診断を行い、ping し、追跡することができます。

電源供給の設定

SX II には二重化電源が搭載されており、これらの電源の状態を検出し、通知できます。

両方の電源が使用されている場合は、どちらも SX II で自動的に検出され、それぞれのステータスが通知されます。さらに、電源供給設定ページの Powerln1 自動検出と Powerln2 自動検出のチェックボックスがどちらも自動的にオンになります。

1 つの電源しか使用していない場合は、使用されている電源のみの自動検出を有効にすることができます。

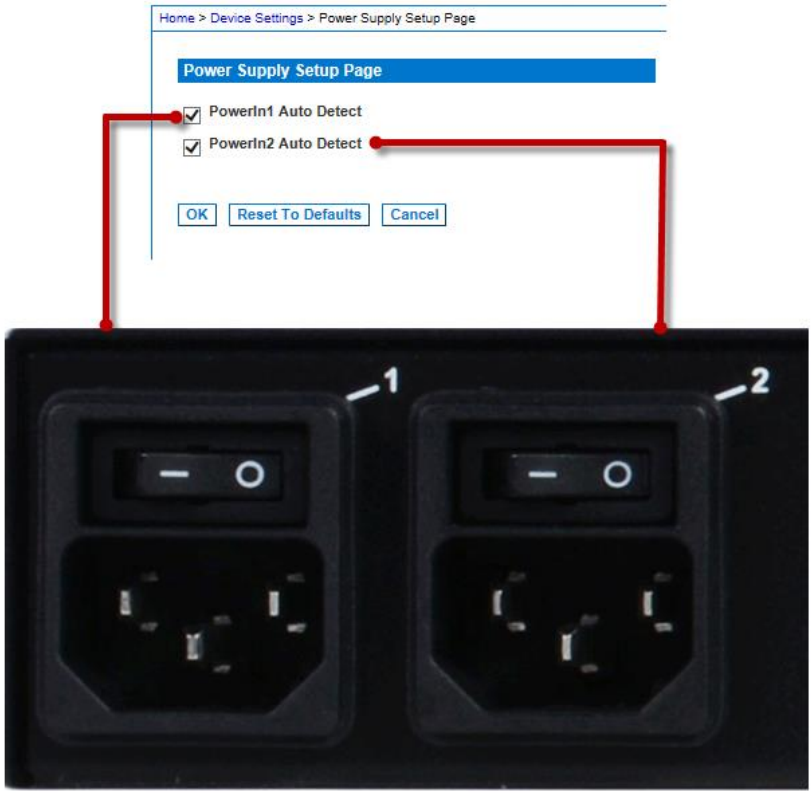
電源の正しい設定を行うと、もし電源に障害があった場合には確実に SX II が適切な通知を行うようになります。たとえば、1 番目の電源に障害が発生した場合は、ユニットの正面の電源 LED が赤色に変わります。

SX II 装置の前面にある電源 LED は上記のチェックボックスの一つあるいは両方が選択されている場合に赤となり、一方の電源入力のみが接続されます。

SX II に電源入力が接続されているときには、電源 LED は電源設定ページで行った選択にかかわらず赤となります。

▶ **使用中の電源の自動検出を有効にするには、以下の手順に従います。**

1. デバイス設定（デバイス設定）の > 電源供給設定を選択します。電源供給設定ページが開きます。



2. 電源入力を 1 番目の電源（ユニット背面の左端の電源）に接続している場合は、Powerln1 自動検出チェックボックスをオンにします。
3. 電源入力を 2 番目の電源（ユニット背面の右端の電源）に接続している場合は、Powerln2 自動検出チェックボックスをオンにします。
4. OK をクリックします。

自動検出を無効にするには、以下の手順に従います。

- 該当する電源のチェックボックスをオフにします。

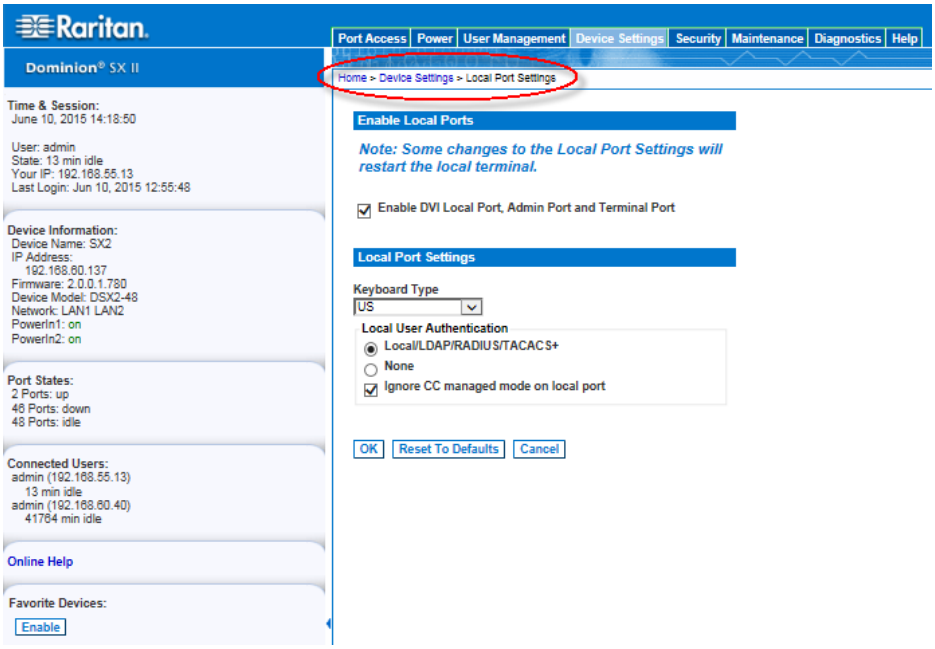
工場出荷時のデフォルトに戻すには、以下の手順に従います:

- デフォルトにリセット をクリックします。

リモート コンソールからローカルなポート設定を行う

このページでローカルなコンソールポートの設定を行います。

ローカル ポート　設定ページ上で何かの変更を行うと、ローカル端末の再起動させます。設定が変化してローカル'端末の再起動が起こるとここに記録されます。



1. DVI-D ローカルポート、Admin P ポートターミナルポートを有効にするのチェックボックスが選択されこれらのポートはデフォルトで有効化されます。そのポートを不能にするにはそのチェックボックスの選択を外します。

   この変更を行うと、端末が再起動します。

2. キーボードタイプドロップダウン リストでキーボード タイプを選択します。選択できる項目は次のとおりです。これらのキーボードのオプションはリモートコントロールだけにてきようされ、ローカルのコンソールには適用されません。

   この変更を行うと、端末が再起動します。

- アメリカ英語
- アメリカ/国際
- 英国
- [French] (フランス語)
- [German] (ドイツ語)
- [German] (ドイツ語)
- 簡体字中国語
- 繁体字中国語
- [Dubeolsik Hangul] (ハングル (韓国))
- [JIS (Japanese Industry St と ard)] (JIS (日本工業規格))
- [Portuguese] (ポルトガル語)
- ノルウェー語 (ノルウェイ)
- [Swedish] (スウェーデン語)
- [Danish] (デンマーク語)
- [Belgian] (ベルギー語)
- ハンガリー語
- スペイン語
- イタリア語
- スロベニア語

注:中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

1. ローカルユーザ認証でローカル ユーザ認証タイプを選択します。
   - ローカル/LDAP/RADIUS/TACACS+ – これは推奨オプションです。
   - なし – ローカル コンソールからのアクセスに対して認証は行われません。

     重要 – もしローカルな認証がなしにセットされていると、ユーザはキーボード上の 1 文字を押すだけで Admin ユーザとして自動的にログインされます。

     このオプションは、安全な環境でのみ選択することを推奨します。デフォルトの設定では、ユーザはユーザ名とパスワードによってローカルポートにログインします。
2. その装置が Comm と Center Secure Gateway (CC-SG) の管理下にある場合でも SX II にローカル ユーザのアクセスをするには、ローカルポートで管理モードを無視するの チェック ボックスをオンにします。または、CC-SG の管理機能下にある場合ダイレクト デバイス アクセス機能を利用します。

   いまはローカルポートで CC 管理モードを無視せず後程その装置を CC-SG 管理から外すと決めた場合、そのデバイスを CC-SG から外しこのページの戻ってこのチェックボックスを外す必要があります。

リモートコンソールからデフォルトの GUI 言語設定を変更する

SX II のウエブベースのインタフェースは、デフォルトでは英語に設定されていますが、以下のローカライズ言語もサポートされています。これらの言語はローカルコンソールには適用されません。

- 日本語
- 簡体字中国語
- 繁体字中国語

GUI 言語を変更するには、以下の手順に従います。

1. デバイス設定 の言語を選択します。言語の定 ページが開きます。
2. 言語野ドロップ ボックスの一覧から、GUI に適用する言語を選択します。
3. 適用をクリックします。英語に戻すにはデフォルトにリセットをクリックします。

注:新しい言語を適用すると、オンライン ヘルプも、選択言語に合わせてローカライズされます。

リモート コンソールからポートのログを設定する

- デバイスサービス > ポートログ設定と選択しポートログ - 設定ページにアクセスし、ローカルのログ設定します。

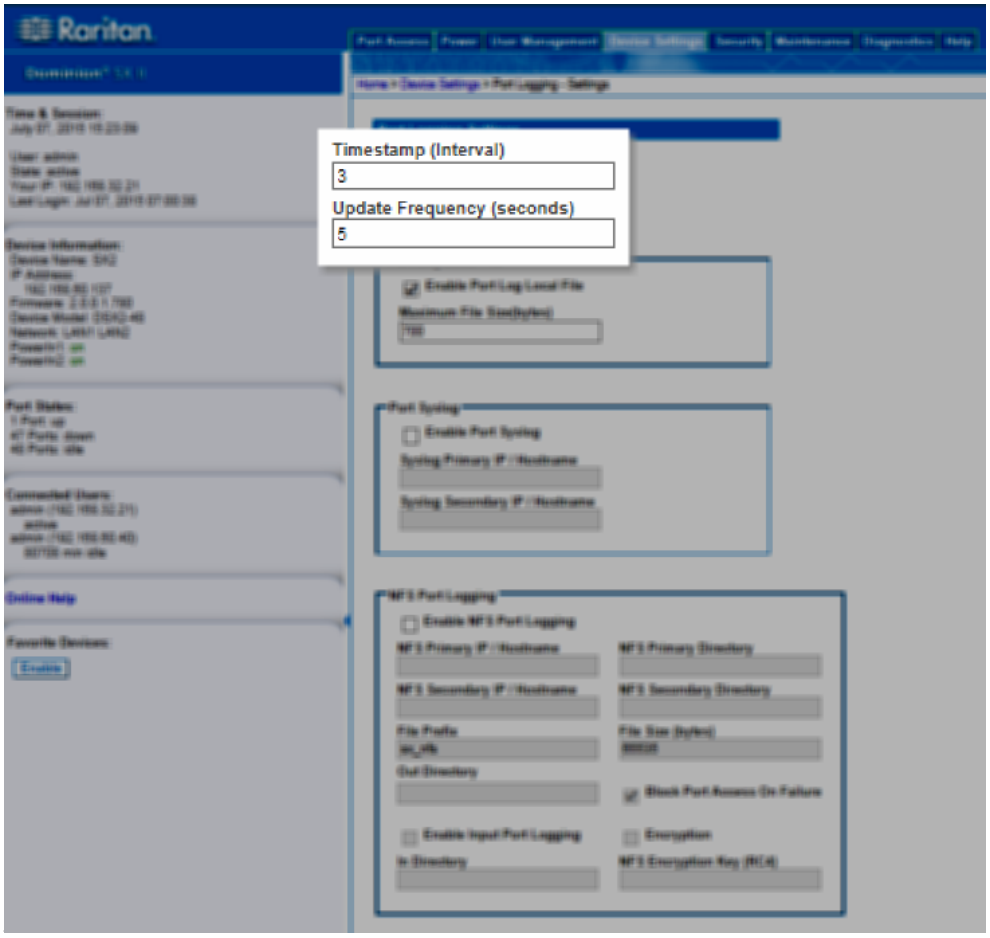
タイムスタンプと更新頻度

必要であれば、デフォルトのタイムスタンプの間隔とまたログ更新の頻度を変更します。

タイムスタンプは 2 つのタイムスタンプの間の間隔のことを指しています。時間間隔を秒の単位で 0-99999 の範囲で記入します。0 を入力するとポートログでタイムスタンプを無効にします。

更新頻度はポートのログファイル、ポートの syslog と NFS ポートログへの各データ書き込みの間の間隔です (それらが有効化されている場合)。デフォルトの間隔は 30 秒です。

データはその間隔の時間にあるいは装置のバッファが満杯になるまで SX II にバッファされます。この機能はログの輸送を管理するので、常に送り出しているわけではありません。

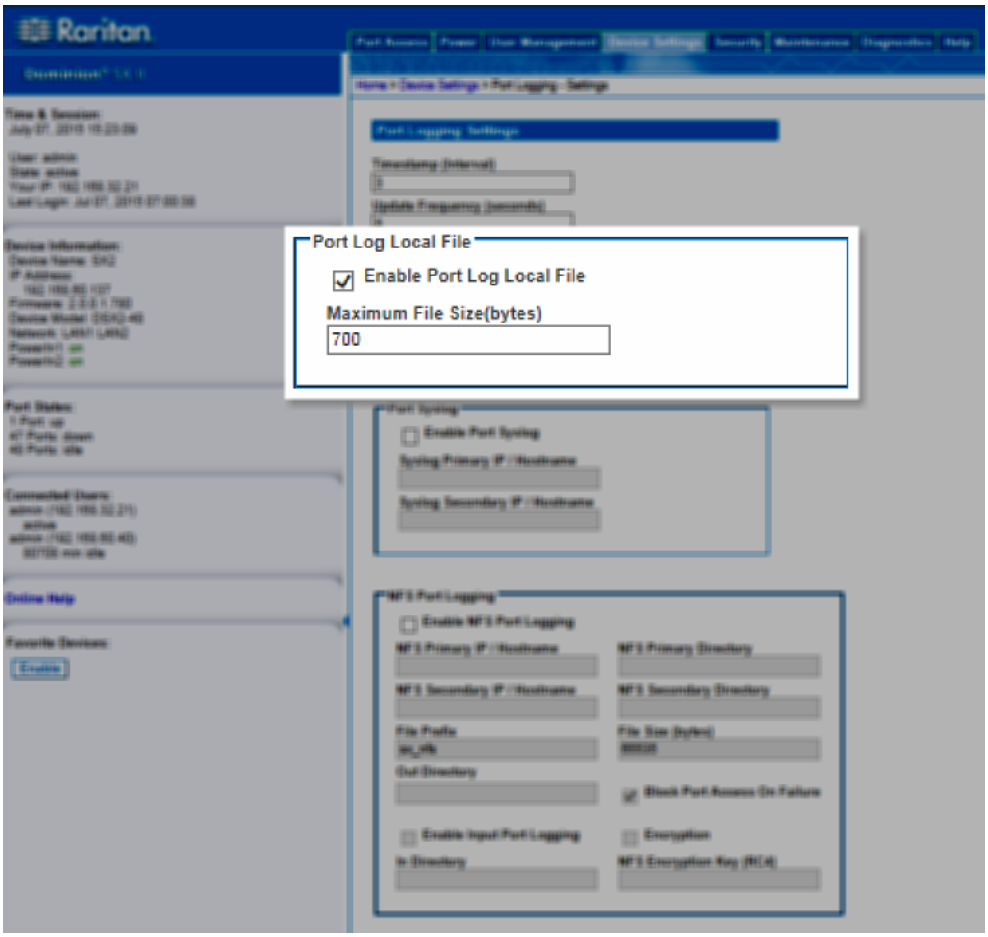


ポートログのローカルファイル

ポートログのローカルファイルを有効にして SX II 上で各ポートのデータを収集します。

ログファイルは SX II の内蔵フラッシュドライブに保存されます。8 および 16 ポートのモデルでは、2GB の内蔵フラッシュドライブがあります。その他のすべてのモデルでは 8GB のドライブとなります。

必要ならば、最大のファイルサイズを記入します。この最大量を超えたデータは保存されません。このファイルを引き出すには、次を参照してください。 *ポートのログを管理 – ローカル ファイル* 『154p. の"*ポートログを管理する – リモート コンソールからのローカルファイル*"参照 』。

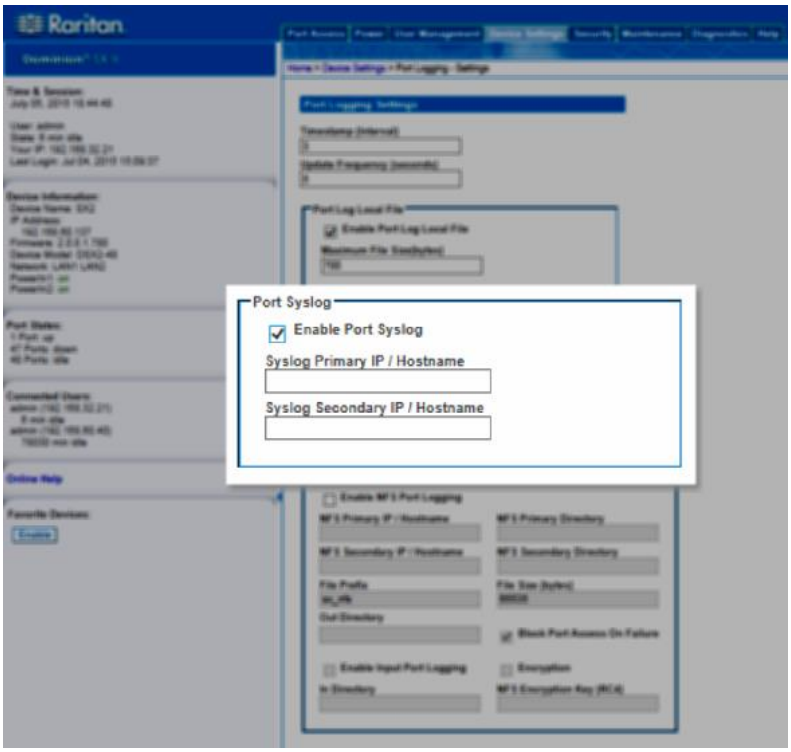


ポートの **Sys Log**

この機能はイベントのログメッセージをリモートの Syslog サーバに送ります。SX II 装置からのメッセージは Syslog サーバの LOCAL0 チャンネルに送られより効率の良い解析に備えます。

全てのメッセージが syslog サーバの LOCAL0 チャンネルから送られるので、すべてのポートの出力が同じファイルに混在します。各ポートのデータを分離することを希望するのであれば、NFS ログを使用してください。

1. [System Logging panel] に行きそして [Enable Port Syslog] のチェックボックスを選択します。



2. プライマリ IP アアドレス Syslog サーバの IP アドレスを入力します。
3. バックアップの Syslog サーバを持っている場合、その IP アドレスを セカンダリ IP アドレスフィールドに記入します。

ネットワーク ファイル システム (NFS) ロギング

ネットワークファイルシステム（NFS）のログは全てのポートの動作を NFS 共有ディレクトリーにログすることを可能にします。全てのユーザの動作とユーザのポートログインとログアウトがログに記録されます 2 種類のログがあります：

- 入力：ユーザからのすべての入力（キー入力）を記録します。

- 出力：そのサーバからコンソールサーバに来るすべてのメッセージを含みます。これは管理しているデバイス/サーバからエコーバックしてくる全てのユーザの入力を含みます。

ポートのログも有効にしなければなりません。ポートログの詳細情報については、『ポートログを有効化する』を参照してください。

注:NFS サーバはポートのログが作動するように書き込み許可を持ったエクスポートディレクトリーを持つ必要があります。

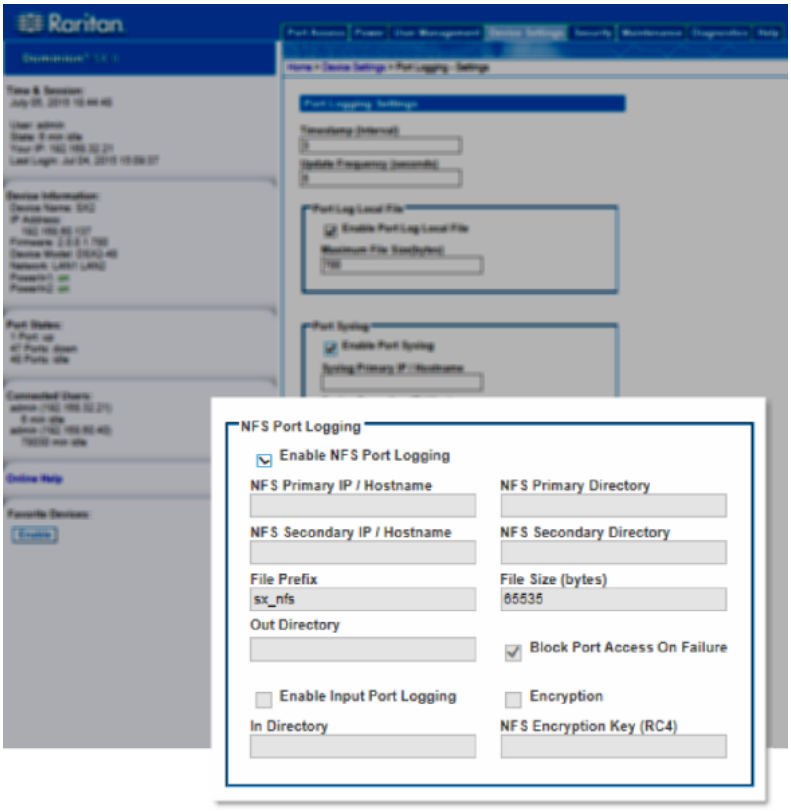
---

1. を有効にする NFS のチェックボックスを選択し NFS のログを有効にします。
2. プライマリ IP アドレスフィールドに NFS サーバの IP アドレスを入力し、それからプライマリディレクトリのフィールドにログファイルへのパスを入力します。
3. もしバックアップの NFS サーバを持っていると、このサーバの第 2 の IP フィールドと第 2 のディレクトリー フィールドにも同じ情報を入力します。第 1 のサーバが失敗すると、ポートのログは第 2 のサーバに回されます。
4. 必要であれば、ポートログ入力機能を有効化にし、入力ディレクトリフィールドに入力のためのディレクトリーを記入します。この機能を不能に変えるためには、そのチェックボックスを外します。
5. デフォルトでは失敗時ポートアクセスをブロックするが選択されています。

   この機能によって NFS マウントは作動し、NFS はソフトマウントとして作動します。

   ソフトマウントの時、ファイルシステムが不良となったとき NFS は再度マウントされます。

再マウントが成功すると、ログは続きますが、そうでなければ、以降のログイベントは禁止されます。



ポートログを管理する - リモート コンソールからのローカルファイル

ユーザを削除するには、以下の手順に従います。

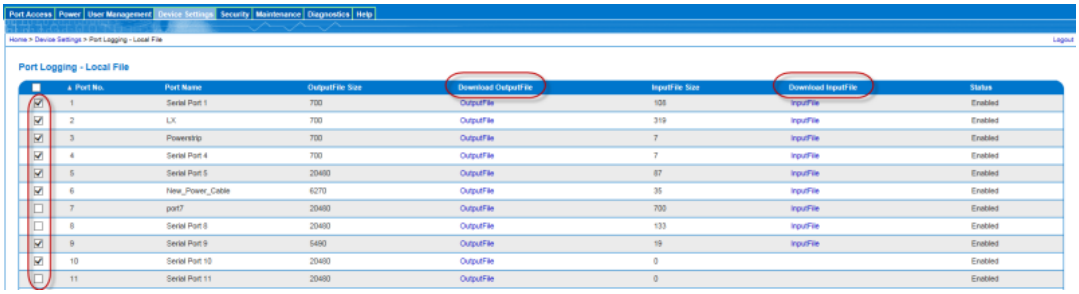
1. ログファイルのチェックボックスを選択します。
2. ログファイルを削除をクリックします。

ログファイルを取得するには、次の手順に従います。

- ログファイルの出力ファイルあるいは入力ファイルへのダウンロードのリンクをクリックします。

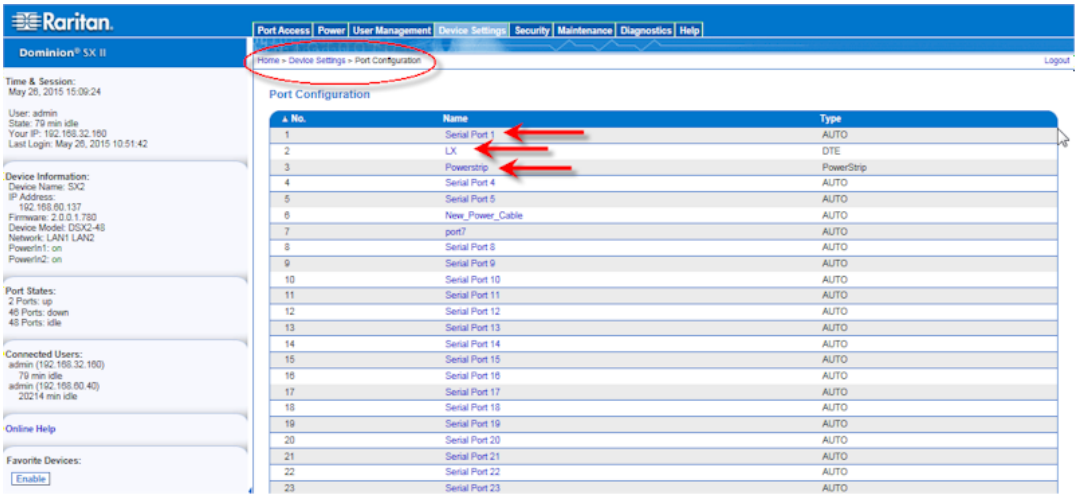
電源の文字データはポートログ ファイルには保存されないことを承知ください。

ポートのログファイルを設定するために情報については、次を参照してください。 ***ポートログの形成 – 設定*** 『149p. の"***リモート コンソールからポートのログを設定する***"参照 』。



リモート コンソールからのポートの設定

ポート設定 ページには、 SX II のポートの一覧が表示されます。



1. ポート設定ページへアクセスするには、デバイス設定 > ポート設定を選びます。

   最初このページはポートの番号順に表示されますが、列の見出しをクリックして名前あるいはタイプの順に並べ替えられます。
2. ポートのページにアクセスしてそれを設定するには、設定したいポートの名前をクリックします。
3. ターゲットのタイプ、シリアルかあるいは電源タップか、を選択します。

4. シリアルターゲットあるいは電源タップには意味のある名前を付けて下さい。

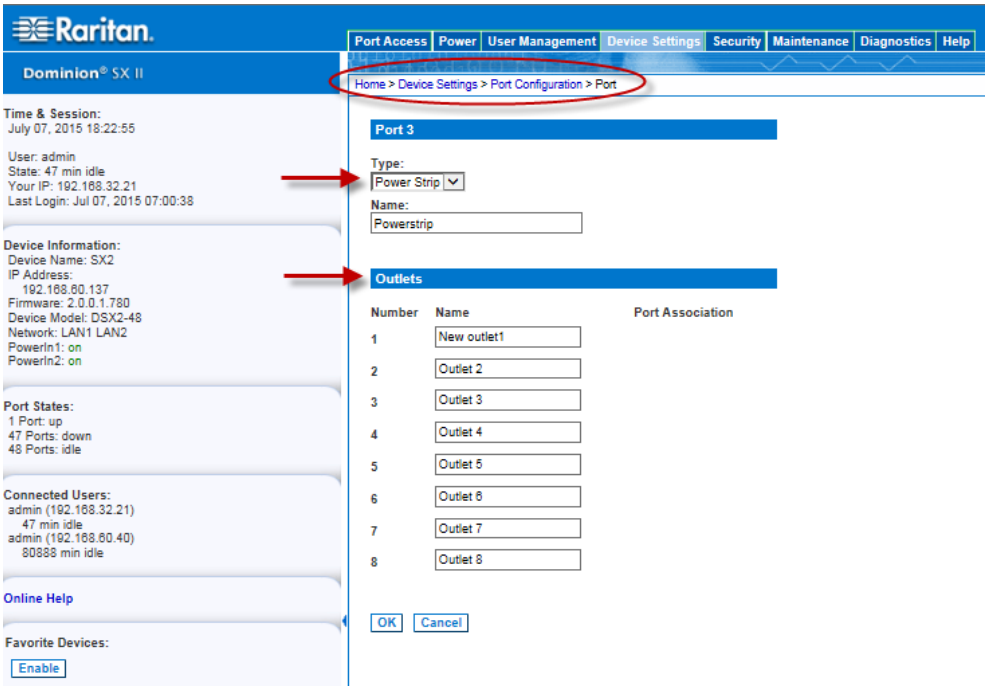
注:CommandCenter Secure Gateway では、スペースを含むラック PDU 名を認識できません。

電源タップ を設定

1. 電源タップ を選択すると、電源タップの名前を指定して OK をクリックします。電源タップが検出されると、ポート設定ページに戻ります。
2. 再度ポートを選択し希望すればそれとそのコンセント名を編集します。デフォルトのコンセント名は、です。

注:ラック PDU がターゲット デバイス（ポート）と関連付けられると、コンセント名はターゲット デバイス名に置き換えられます。コンセントに別の名前を割り当てていた場合でもそうなります。

3. [OK] をクリックします。



ターゲットデバイスを設定する

ターゲットデバイスを選択すると、あなたが形成できる多様な設定があります。

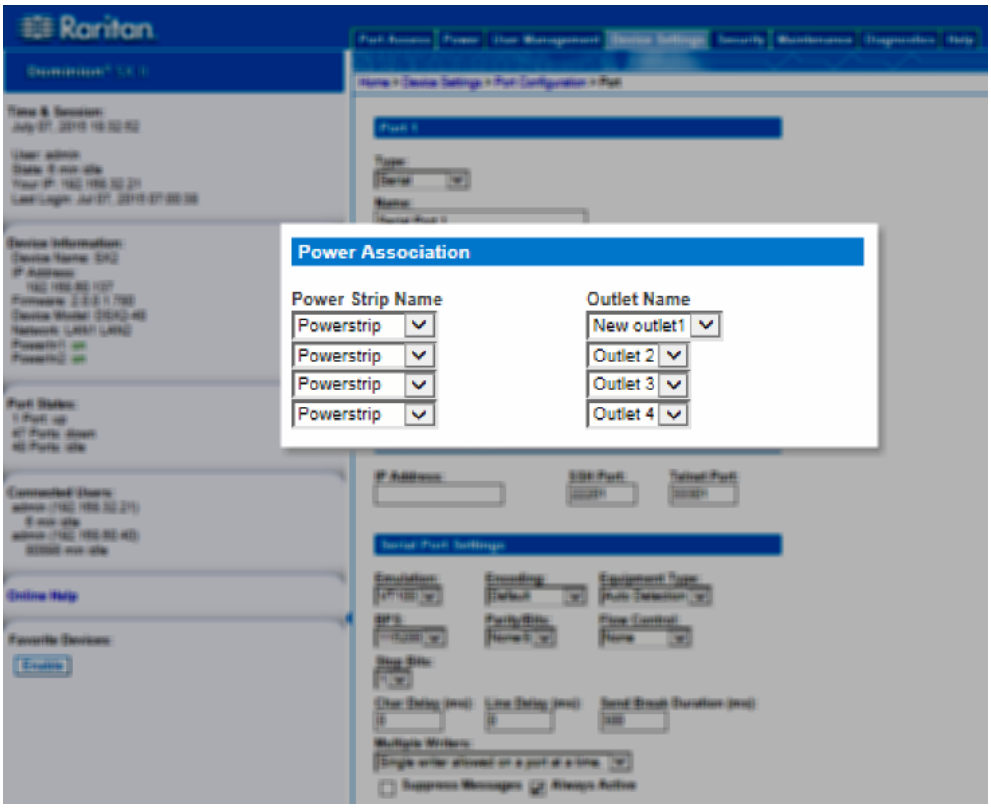
注:ラック PDU がターゲット デバイス（ポート）に関連付けられると、コンセント名はターゲット デバイス名に置き換えられます（コンセントに別の名前を割り当てていた場合でもそうなります）。

---

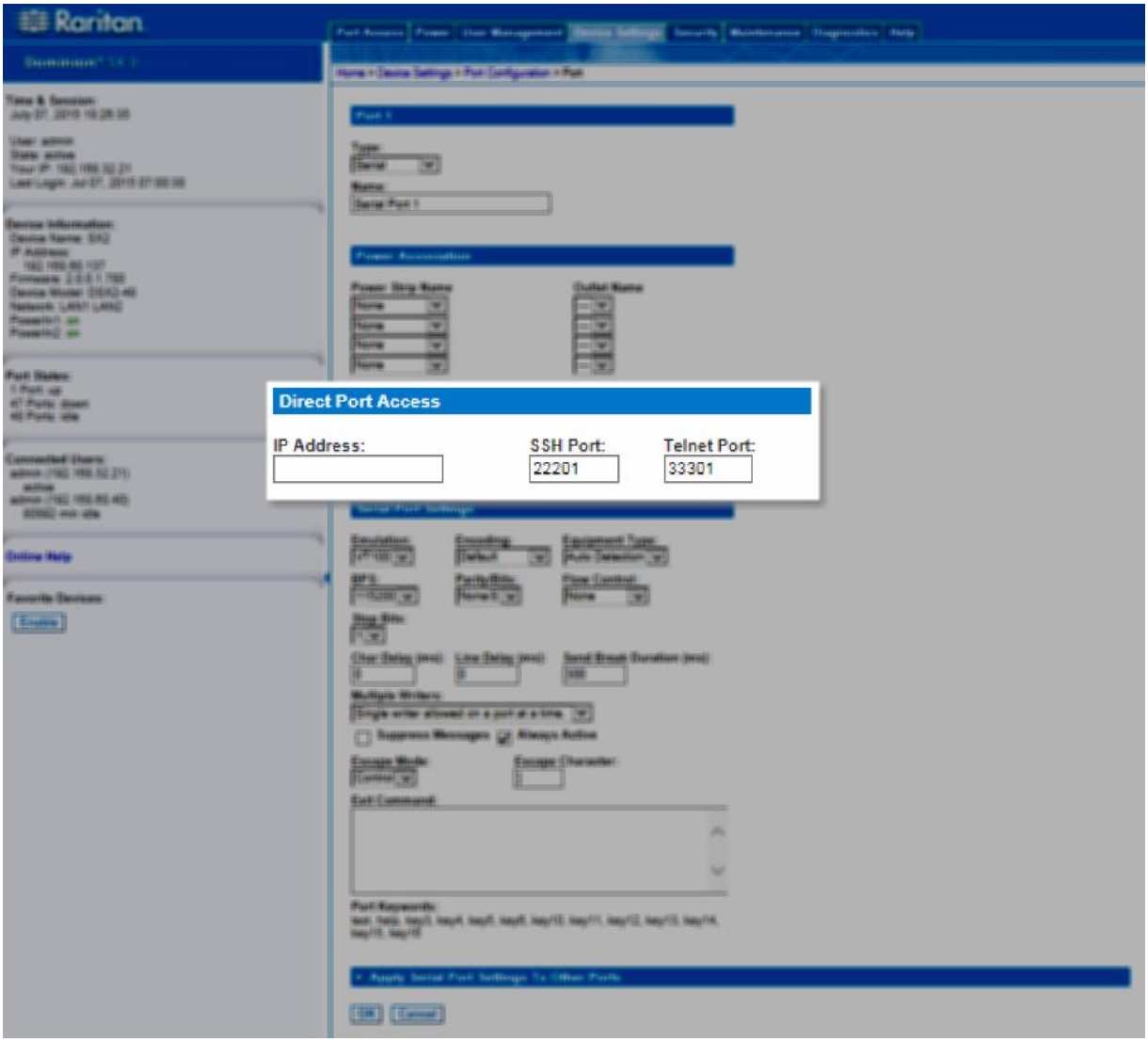
1. ターゲットの名前を記入あるいは更新
2. ポートが接続されているサーバにコンセントも接続されていると、ターゲット デバイスを電源に関連付けることができます。

   ポートには最大で 4 つの関連コンセントを接続でき、それぞれに別のラック PDU（電源タップ）を関連付けられます。このページでそれらの関連付けを定義して、ポート アクセス ページからサーバの電源オン、電源オフ、電源再投入を行えます。

   この機能を使うには、Raritan のリモート ラック PDU が必要です。
3. 電源タップの名前を選択し、名前をその各電源タップのコンセントをコンセント名のドロップダウンから選択して関連を付けます。
4. [OK] をクリックします。確認メッセージが表示されます。



5. ターゲットのポートに直接のポートアクセスを可能にするには、ポートの IP アドレス と SSH ポートと Telnet ポートを入力します。



ポート設定の構成

残りのポート設定を、必要あるいは要求によって、構成します。

1. エミュレーションフィールドのドロップダウンメニューからターミナル エミュレーションのタイプを選択します。これはポートに接続されたシリアルターゲットに合わせるために使われるターミナル エミュレーション モードです。次のものが選択できます：
   - VT100
   - VT220
   - VT320

- ANSI

2. このポートで Raritan Serial Console (RSC) が常に特定の文字エンコーディングを使うのを希望する時にはエンコ―ディングをセットします。

   エンコ―ディングはそのポートにどのようなグローバルな RSC 設定をしてもそれより優先されます。

   次のものが選択できます：DEFAULT,US-ASCII,ISO8859-1, ISO8859-15,UTF-8, Shift-JIS, EUC-JP, EUC-CN, EdUC-KR.

3. 検出フィールドには、SX II が自動的にターゲットへの物理的な接続を検出するのを希望するかどうかを示します。デフォルトは自動検出です。

   もう一つのオプションは強制 DTE の選択です、どのような場合に SX II がそれに接続したターゲットを検出するデータ通信装置として働くかを選びます。

   あるいは強制 DCE の選択です、どのような場合に SX II がそれに接続した装置を検出するデータ通信装置として働くかを選びます。

拳:目標が DTE か DCE のいずれかを自動検出する能力を持っていると、そのポートに強制 DTE あるいは強制 DCE のいずれかを選ぶことが必要となります。SX II は同一ポートに DCE と DTE の両方を自動検出することをサポートしていません。

---

4. ボー：秒あたりのビットのドロップダウン メニューから秒あたりのビットの値を選択します。
5. パリティビットのドロップダウン メニューからパリティビットを選択します。
6. フロー制御のドロップダウン メニューからフローコントロールを選択します。
7. 個別の文字がポート経由で送られる時の時間間隔’を設定する必要があれば、文字遅延ィールドにミリ秒単位で時間を記入します。
8. 何行かのテキストがポート経由で送られる時の行の時間間隔’を設定するには、行遅延フィールドにそれを記入します。
9. [sendbreak] 時間を設定するためブレーク送出時間フィールドにブレーク送出時間を記入します。ブレーク送出時間は oms - 1000ms の範囲で設定します。
10. どのユーザも接続していないときでもポートにログが来るようにするには常にアクティブを選択します。

    デフォルトは接続ユーザが居ない時にはポートアクセスを保持しない事で、これは誰も接続していないときにはポートに来るデータを無視することを意味します。

    このオプションはポートデータのログに対するものです。

注:どのユーザもポートセッションにログインしていないとき、ポートの往来は、デフォルトで、破棄されます。

---

11. もしあなたがメッセージを ダイレクト ポート アクセス経由 SX II に接続するユーザに表示されたくない場合には、メッセージを抹殺チェックボックスを選択します。
12. あるいはその代わりに、この選択と認証成功と言ったすべてのメッセージの選択を外します。これらのメッセージは直接ポートアクセス (dpa) 経由接続するユーザに表示されます。デフォルトは選択無しです。

    デフォルト無しです。
13. エスケープ モードを選択します。

    エスケープシーケンスは CLI でのみ効果があります。エスケープ モードに入るとき、ユーザは実行できるコマンドのメニュー(たとえば、履歴の取得、電源のコマンド、など) を与えられ、さらにポートセッションに戻るコマンドと、ポート接続から出るコマンドが与えられます。

    デフォルトは無しです。

    次のように変更します :

    - エスケープモードフィールドのドロップダウン メニューからコントロールを選びます。
14. エスケープ文字フィールドに文字を記入します。SX II のデフォルトは] (閉じ括弧) です。

    Raritan では [あるいは Ctrl-[を使用しないことをおすすめします。これらのいずれかは、例えばエスケープ コマンドを意図しないのに引き起こすというような、意図しないコマンドを引き起こすかもしれません。この連続キー入力はキーボードの矢印キーによっても引き起こされます。
15. 終了コマンドフィールドにコマンドをコマンドを記入します、例えば `logout`。

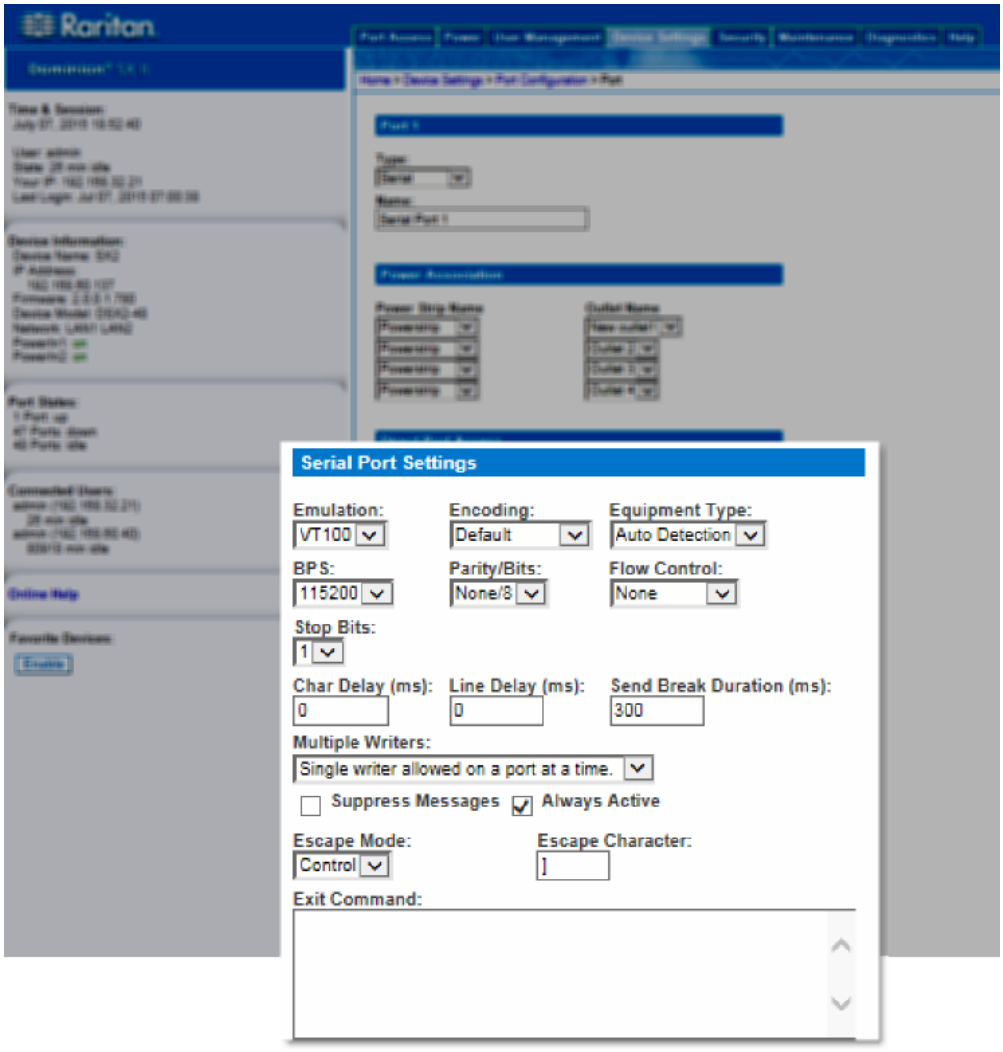
    これはユーザの書き込み許可がポートから外されたときにあなたに贈られるコマンドです。

    このコマンドの主な機能は、ターゲットマシン上のユーザのセッションが閉じたことを確認することですが、ポート上に Exit コマンドをポートで持つことは必ずしも必要ではありません。

    注:参照 ポートの設定 ここにはポート設定コマンドの詳細があります。

    ---
16. 複数のクライアントがそのポートに同時に書き込みできるよう望む場合は、複数ライターをドロップダウンで選びます。デフォルトの行動はある時点では一人のユーザの実が書き込みアクセスを持つことです。

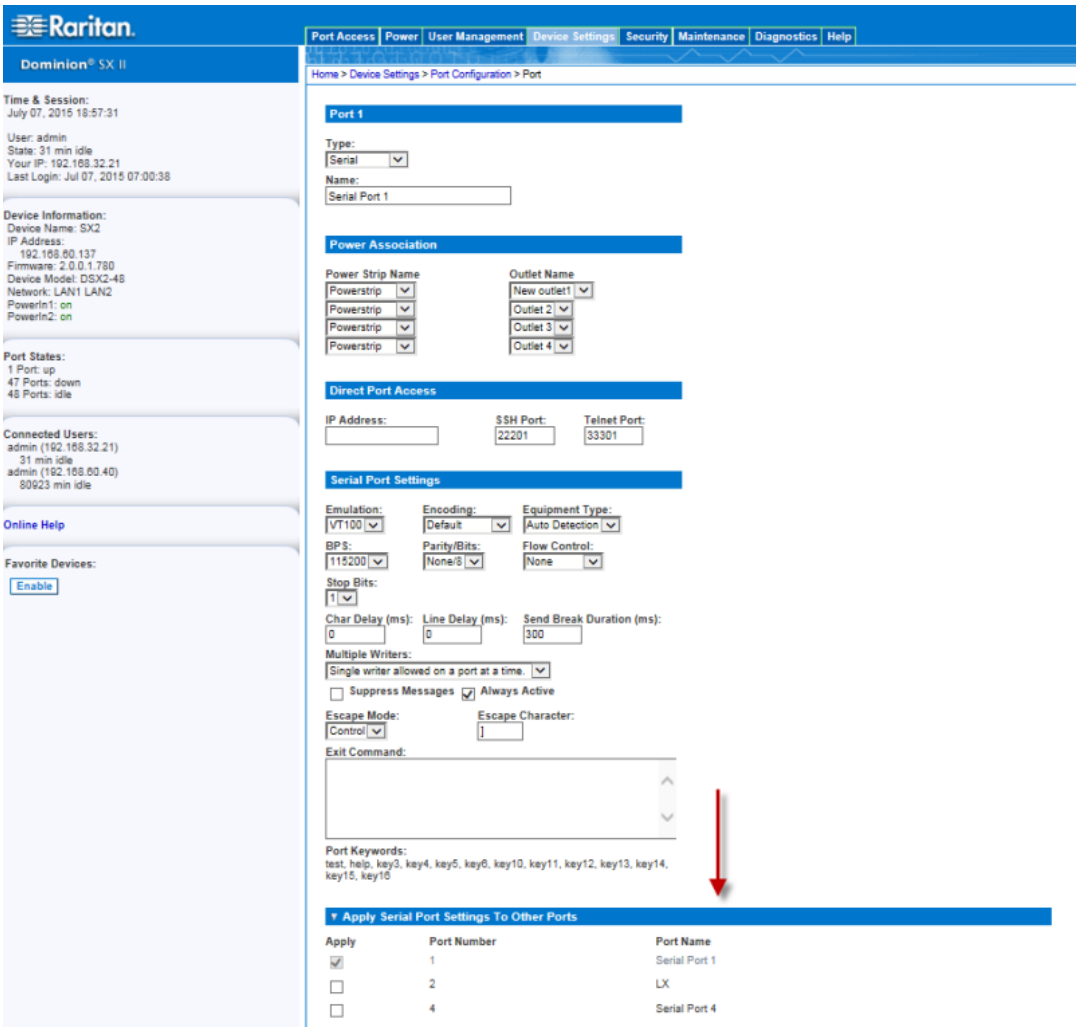
17. [OK] をクリックします。



設定を他のポートに適用する

一旦終了すると、おなじポート設定をほかのポートに適用することができます。

1. ページの[Apply Serial Port Settings To Other Ports] セクションから個別にあるいはページの下の選択ボタンを用いてポートを選びます。



2. ［OK］をクリックして LAN 設定を適用します。

ポート キーワード リスト

ポート キーワードはフィルタとして機能します。ポート キーワードを作成し、以下と関連付けることができます。

- イベント
- ローカルあるいはリモートの syslog メッセージ
- SNMP トラップ

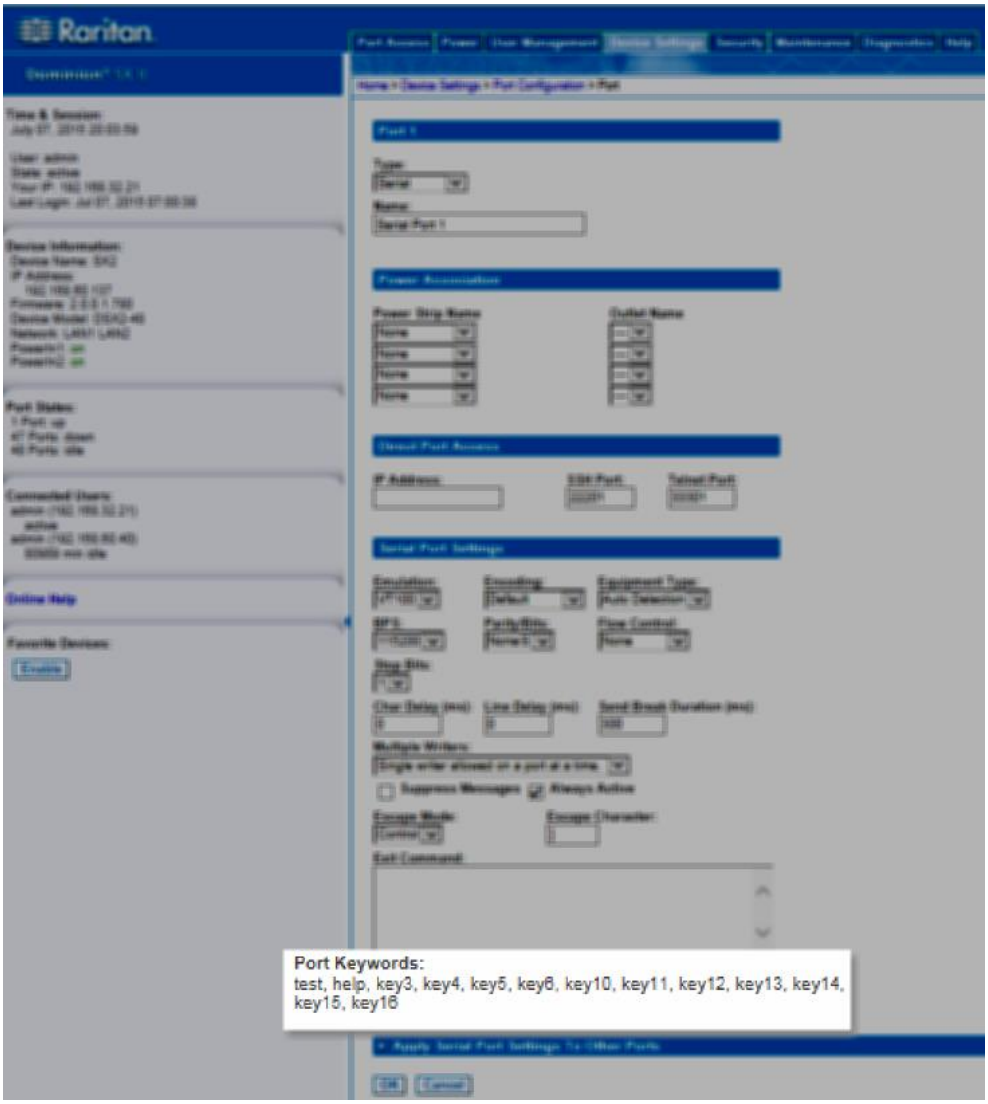
キーワードが検出されると –

- 対応するメッセージがローカルあるいは NFS ポートログにログされます。
- 対応するイベントが SMTP （もし設定されていれば）経由送られます。
- 対応するトラップが SNMP （もし設定されていれば）経由送られます。

この機能は管理者にポート上である特定のイベントが起こったかどうかを知らせるのに有用です。さらに、レポートイベントへのポートキーワードを使うことが NFS のログサイズに影響しません。

どのユーザもポートに接続されていないときキーワードが起こるためには、そのポートのポート設定ページで常にアクティブが選択されている必要があります。

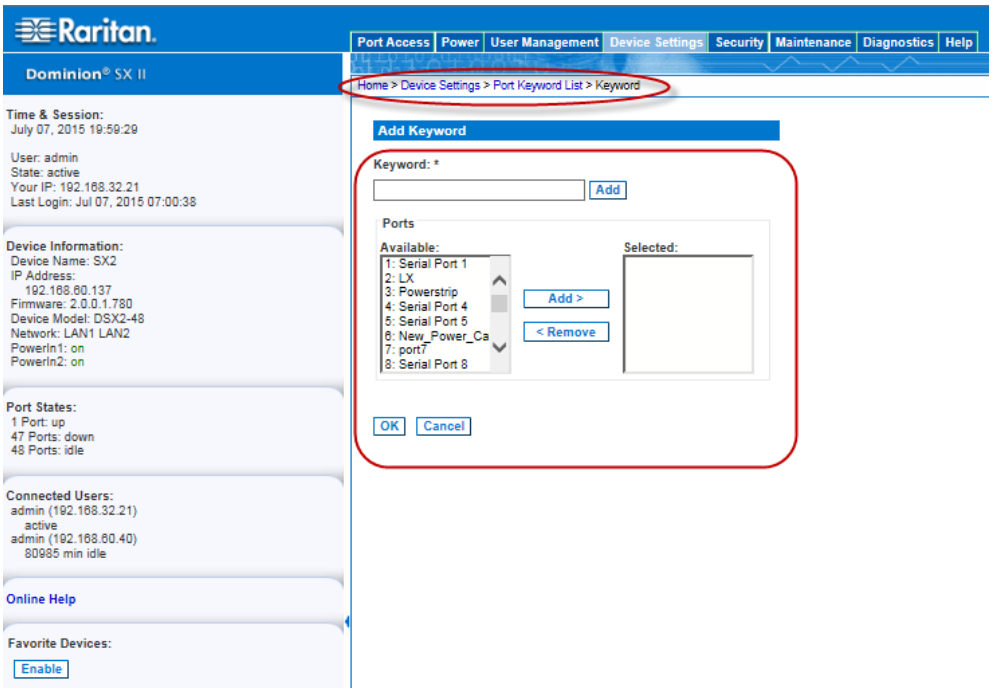
存在するポートキーワードのリストがもしあれば、ポート設定ページで表示されることを了解しておいてください。



シリアル警告イベントがイベント管理—送信先ページから選ばれます。

1. デバイス設定 のポートキーワードを選択します。ポート キーワードのリストの ページが開きます。

2. ページ下部にある　追加 をクリックします。キーワード ページが開きます。



3. キーワードのフィールドにキーワードを入力します。
4. そのキーワードに関連させたいポートを選択します。
5. 追加 をクリックしてそれらを選択されたボックスに加えます。
6. [OK] をクリックします。

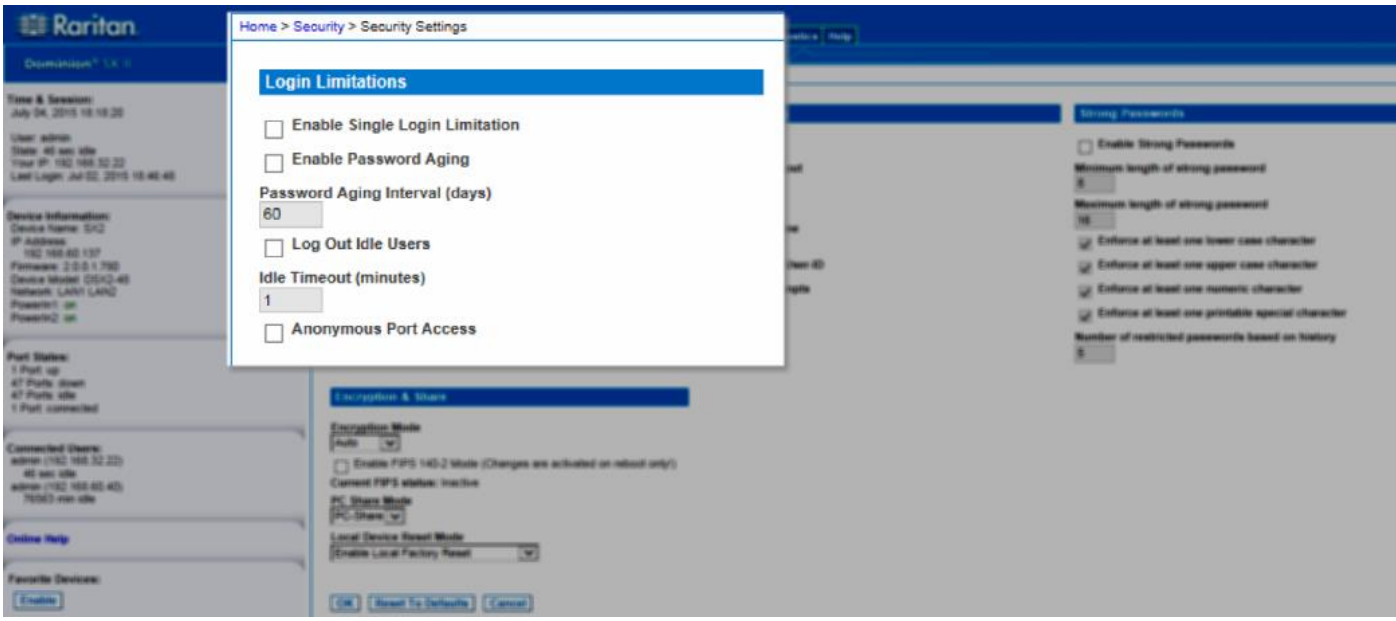
リモート コンソールからセキュリティ設定を行う

ログインの制限

ログイン制限を用いて、シングル ログイン、パスワード エージング、アイドル ユーザのログアウトに関する制限を指定できます。

ログイン制限はセキュリティ設定ページで設定できます。

- セキュリティのセキュリティ設定を選択します。



- シングル ログイン制限を有効にする

  このチェック ボックスをオンにした場合、常にユーザ名ごとに同時に 1 人しかログオンできません。このチェック ボックスをオフにした場合、所定のユーザ名とパスワードの組み合わせで、複数のクライアント ワークステーションからデバイスに同時接続できます。

- パスワード エージングを有効にする

  これを選択すると、パスワードエージング間隔フィールドで指定した日数に基づいて、すべてのユーザに対して定期的にパスワードを変更するよう要求します。

  パスワードエージングを有効にするチェックボックスをオンにするとこのフィールドが有効になるため、設定する必要があります。パスワードの変更が要求される間隔を日数で入力します。デフォルトの日数は 60 日です。

- アイドル ユーザをログアウトする、1-365 minutes 分後

  アイドルユーザをログアウトするチェック ボックスをオンにした場合、(1-365 分) 後ボックスに入力した時間が経過した後にアイドルユーザが自動ログオフされます。キーボードまたはマウスで操作が行われない場合は、すべてのセッションおよびすべてのリソースがログアウトされます。

  アイドルタイムアウトフィールドはアイドル ユーザがその後ログアウトされる時間を分でセットするために使われます。このボックスが有効になるのは、アイドルユーザをログアウトするチェック ボックスをオンにした場合です。このフィールドに入力できる値は 1 ～ 365 の範囲です。

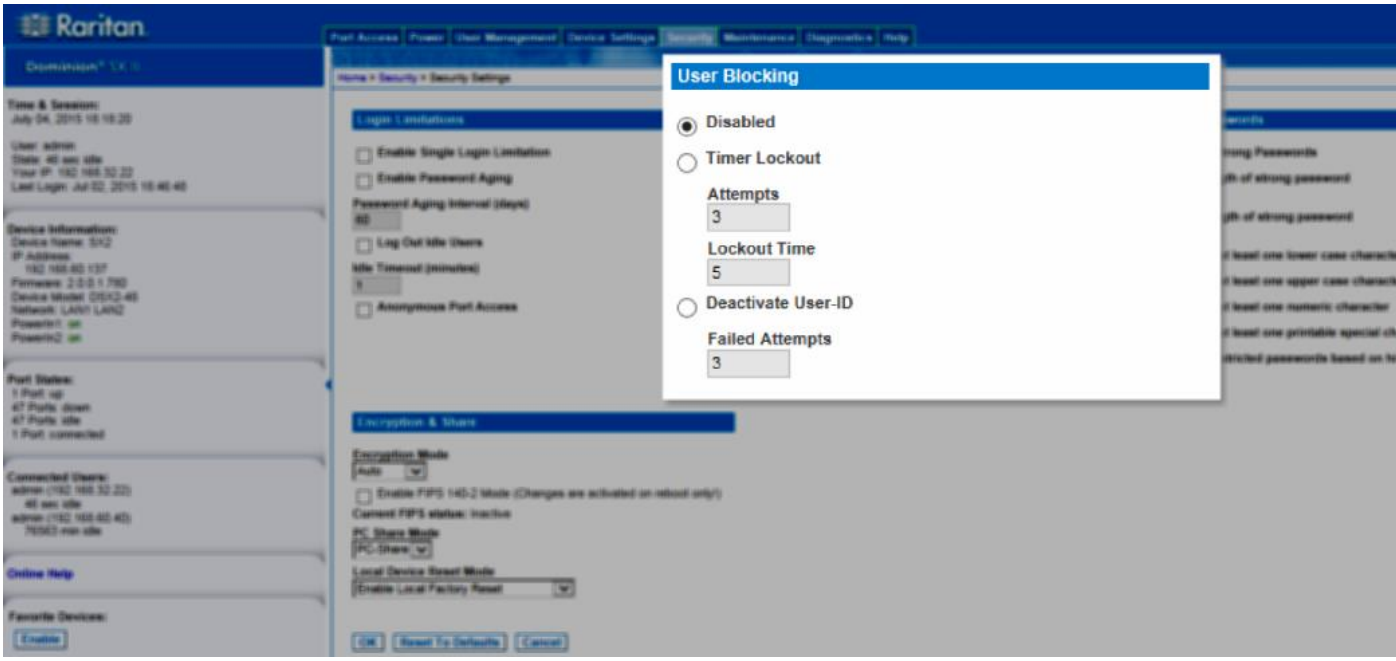
- 無記名ポートアクセス

  これが選択されると、ユーザはダイレクト ポート アクセス 経由でパスワードを入力することなくポートにアクセスできます、ただしダイレクト ポート アクセス がそのポートに有効である限りです。

ユーザのブロック

ユーザブロックオプションでは基準を指定し、ユーザがその回数ログオンに失敗するとシステムにアクセスできなくなるようにします。

- セキュリティのセキュリティ設定を選択します。



次の 3 つのオプションは、相互に排他的です。

- 無効

  デフォルトのオプションです。認証に失敗した回数に関わらず、ユーザのアクセスはブロックされません。

- タイマ ロックアウト

  ユーザが指定回数より多くログオンに失敗すると、システムへのアクセスが指定の時間拒否されます。これを選択した場合は次のフィールドが有効になります。

  - 試行回数 – この回数より多くログオンに失敗すると、ユーザはロックアウトされます。有効な範囲は 1 ～ 10 で、デフォルトの試行回数は 3 です。
  - ロックアウト時間 – ユーザがロックアウトされる時間です。有効な範囲は 1 ～ 1440 分で、デフォルトでは 5 分です。

  注:(タイマ ロックアウトでの指定は、管理者の役割が割り当てられているユーザには適用されません。

- ユーザ ID を無効化

  このオプションを選択した場合は、試行回数 フィールドで指定した回数より多くログオンに失敗すると、ユーザはシテムからロックアウトされます。

  失敗試行回数 – この回数より多くログオンに失敗すると、そのユーザのユーザ ID が無効になります。このフィールドが有効になるのは、ユーザ ID を無効化オプションを選択した場合です。有効な範囲は 1 ～ 10 です。

  指定回数より多くログオンに失敗してユーザ ID が無効になった場合、管理者はユーザ パスワードを変更し、ユーザページの [Activate] チェックボックスをオンにしてユーザ アカウントを有効化する必要があります。

強力なパスワード

セキュリティ設定ページで強力なパスワードを有効化し設定をします。

- セキュリティ の セキュリティ設定を選択して強力なパスワードを設定をします。

強力なパスワード セクションで値を指定すると、このシステムにおけるローカル認証の安全性が高まります。強力なパスワードを使用すると、最小長と最大長、必要な文字、パスワード履歴の保持など、有効な SX II ローカル パスワードの形式を設定できます。

パスワードが強力なパスワードの基準を満たしていない場合、ユーザは次回ログオンする際にパスワードを変更するよう自動的に求められます。

強力なパスワードを有効にするチェック ボックスをオフにした場合、標準の形式になっているかどうかだけが検査されます。

最低限、一般に求められる強いパスワードが可能となるための要求は次のことです –

- パスワードは 8 文字以上でなければなりません
- 最低 1 つのアルファベット文字を持っていること
- 最低 1 つのアルファベットでない区切り記号や数字のような文字を持っていること
- また、パスワードとユーザ名の最初の 4 文字には同じ文字列を使用できません。

  パスワードはスペースで始まることあるいはスペースで終わることはできません。

特殊文字使用を強制するには、最低 1 つの印刷可能な特殊文字を強制するを選択します。

[履歴によるパスワードの使用回数の制限数は以前のパスワードをこの回数以上繰り返しできないことを強制します。範囲は 1 ～ 12 で、デフォルトは 5 です。

暗号化と共有の設定

暗号化および共有)設定では、使用する暗号化のタイプ、PC　の共有モード、SX II　のリセット ボタンを押したときに実行されるリセットのタイプを指定できます。

警告:使用のブラウザでサポートされていない暗号化モードを選択した場合、そのブラウザから SX II　にアクセスできなくなります。

1. 暗号化モードボックスの一覧で暗号化モードを選択します。

   選択した暗号化モードがご使用のブラウザでサポートされていない場合 SX II に接続できない、という内容の警告が表示されます。

   この警告は、″暗号化モードを選択する際、ご使用のブラウザでその暗号化モードがサポートされていることを確認してください。サポートされていない場合、SX II に接続できません″という意味です。

   - 自動 – これは推奨オプションです。 SX II は使用可能な最高強度の暗号化モードに自動設定されます。

デバイスとクライアントが FIPS 準拠アルゴリズムの使用を正常にネゴシエートできるようにするには、自動を選択する必要があります。

- RC4 - RCA RC4　暗号化方法を使用してユーザ名、パスワード、とデータの安全保護します。これは、最初の接続認証中に SX II デバイスとリモート PC 間のプライベート通信チャンネルを提供する 128 ビットの SSL (セキュア ソケット レイヤ) プロトコルです。

  FIPS 140-2 モードを有効にして RC4　を選択すると、エラー メッセージが表示されます。RC4 は FIPS 1402 モードでは使用できません。

- AES (Advanced Encryption St と ard)　－128 は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。″128″はキーの長さを意味します。AES-256 を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。参照 ***ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する*** 『173p. 』 詳細については、以下を参照してください。

- AES (Advanced Encryption Standard)　－256 は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。″256″はキーの長さを意味します。AES-256 を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。参照 ***ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する*** 『173p. 』 詳細については、以下を参照してください。

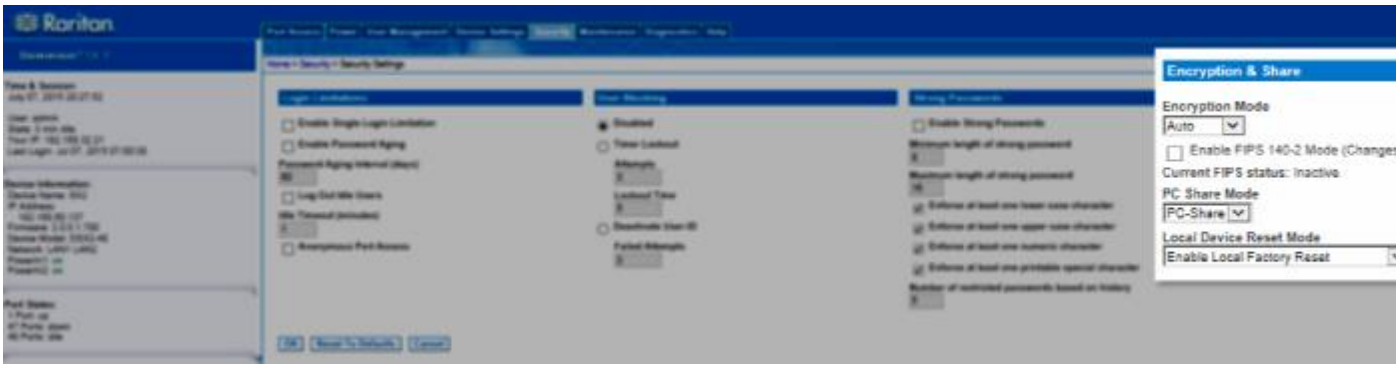
注:Windows XP® (Service Pack 2 適用) と Internet Explorer® 7 を使用している場合、AES-128 暗号化モードで SX II にリモート接続することはできません。

---

2. 政府やその他のセキュリティの高い環境では、FIPS 140-2 を有効に擦るチェックボックスをオンにして FIPS 140-2 モードを有効にします。FIPS 140-2 を有効にする方法については、FIPS 140-2 の有効化を参照してください。
3. PC 共有モード - グローバルな同時リモート アクセスを決定し、最大 8 人までのリモート ユーザが SX II に同時にログオンし、デバイスを介してターゲット デバイスを同時に表示および制御できるようにします。次のいずれかのオプションを選択します。
   - プライベート -PC を共有しません。これはデフォルトのモードです。一度に 1 人のユーザが、排他的に各ターゲット サーバにアクセスできます。

- PC-共有 – ターゲット サーバに最大 10 人のユーザ（管理者または非管理者）が同時にアクセスできます。一人のユーザがそのポートへの書き込み許可を持ちそしてほかのユーザは読み取りだけとなります、これはポートが複数書き込みモードに設定されていない場合です。

4. 必要に応じて、ローカルデバイスリセットモードボックスの一覧で値を選択します。このオプションでは、ユニットの背面にあるハードウェア リセット ボタンが押下された際に実行するアクションを指定します。さらに詳細については、 SX II をリセットボタンを用いてリセットするを参照してください。次のいずれかのオプションを選択します。
   - ローカル出荷時リセットを有効にする（デフォルト） – SX II デバイスを工場出荷時のデフォルトに戻します。
   - ローカル Admin パスワードリセットを有効にする – ローカルの管理者パスワードのみをリセットします。パスワードは次にリセットされます： *raritan*。
   - 全てのローカルリセットを無効にする – どのリセットアクションも行われません。ローカルの管理者パスワードだけをリセットします。パスワードは次にリセットされます： *raritan*。
5. ［OK］をクリックして設定を適用します。



ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する

ブラウザで AES が使用されているかどうかわからない場合は、ブラウザの製造元に問い合わせるか、暗号化方法を調べたいブラウザを使用して https://www.fortify.net/sslcheck.html Web サイトにアクセスしてください。この Web サイトでは、ブラウザの暗号化方法が検出され、レポートが表示されます。

AES 256 ビット暗号化方式は、以下のブラウザでサポートされています。

- Firefox®
- Internet Explorer®

AES 256 ビット暗号化方式を使用するには、サポート対象ブラウザを使用することに加え、Java ™Cryptography Extension ®(JCE®) 無制限強度の管轄ポリシーファイルをインストールする必要があります。

各種 JRE ™ の管轄ファイルは、Java ダウンロード ウエブサイトの [other downloads] セクションで入手できます。

FIPS 140-2 サポートの要件

SX II では、FIPS 140-2 で承認された暗号化アルゴリズムの使用がサポートされます。これにより、クライアントが FIPS 140-2 専用モードに設定されている場合に、SSL サーバとクライアントでは、暗号化されたセッションに使用されている暗号スイートを正常にネゴシエートできます。

SX II で FIPS 140-2 を使用する場合の推奨事項を以下に示します。

SX II

セキュリティ設定 ページで、暗号化と共有を自動に設定します。参照 ***暗号化と共有の設定*** 『170p. 』。

Microsoft クライアント

クライアント コンピュータと Internet Explorer® で FIPS 140-2 を有効にする必要があります。

Windows® クライアントで FIPS 140-2 を有効にするには、以下の手順に従います。

1. コントロールパネル、管理ツール、ローカルセキュリティポリシーの順に選択して、ローカル セキュリティ設定 ダイアログ ボックスを開きます。
2. ナビゲーション ツリーで、ローカルポリシー、セキュリティオプションの順に選択します。
3. 『System Cryptography:Use FIPS compliant algorithms for encryption, hashing と signing』を有効にします。
4. クライアント コンピュータを再起動します。

Internet Explorer で FIPS 140-2 を有効にするには、以下の手順に従います。

1. Internet Explorer で、ツールのインターネットオプションを選択し、[Advanced] タブをクリックします。
2. TLS 1.0 を使用チェックボックスをオンにします。
3. ブラウザを再起動します。

FIPS 140-2 の有効化

政府やその他のセキュリティの高い環境では、場合によっては、FIPS 140-2 モードを有効にする必要があります。

SX II では、『FIPS 140-2 Implementation Guidance』 の G.5 セクションのガイドラインに従って、Linux® プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。

このモードを有効にすると、SSL 証明書の生成に使用される秘密鍵を内部で生成する必要があり、ダウンロードしたりエクスポートしたりすることはできません。

FIPS 140-2 モードを有効にすると、パフォーマンスが低下する場合があります。

▶ **FIPS 140-2 を有効にするには、以下の手順に従います。**

1. セキュリティ設定(セキュリティ設定) ページを開きます。
2. セキュリティ設定 ページの暗号化および共有セクションで Enable FIPS 140-2 を有効にするチェックボックスをオンにして、FIPS 140-2 モードを有効にします。

   FIPS 140-2 モードでは、外部通信に FIPS 140-2 で承認されたアルゴリズムを利用します。

   FIPS 暗号モジュールがセッション往来の暗号化に使用されます
3. SX II を再起動します必ず実行してください。

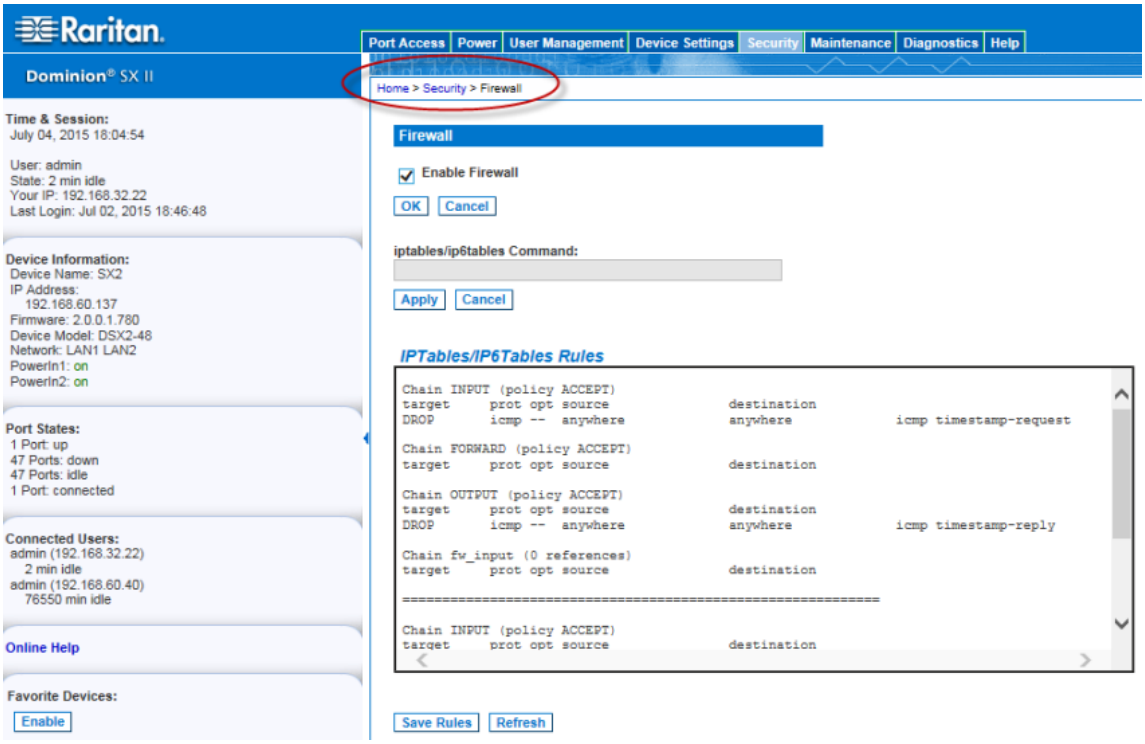
   FIPS モードが有効になると、FIPS モード: 有効というメッセージが画面の左パネルのデバイス情報セクションに表示されます。

   FIPS モードが有効になったら、セキュリティを強化するために、新しい証明書署名要求を作成することもできます。この要求は、必要な鍵暗号を使用して作成されます。署名された証明書をアップロードするか、自己署名証明書を作成します。SSL 証明書の状態は、FIPS モードに準拠せずから FIPS モードに準拠に更新されます。

   FIPS モードが有効になっている場合は、鍵ファイルをダウンロードまたはアップロードできません。最後に作成された CSR が内部で鍵ファイルに関連付けられます。さらに、CA からの SSL 証明書とその秘密鍵は、バックアップされたファイルの完全な復元に含まれません。鍵を SX II からエクスポートすることはできません。

ファイアウォール

SX II はその IP ネットワークの保護を提供し内部ルーターと LAN1、LAN2　とモデムインタフェースの間のアクセスを制御するためにファイアウォール機能をもっています。



1. セキュリティ 〉 ファイアウォールを選択します。ファイアウォールのページが開き、既存の IP テーブルルール を表示します。
2. ファイアウォールを有効にするチェックボックスをオンにします。
3. [OK] をクリックします。

注: 2 重化 LAN ユニットで IP の転送を可能にするときには、IP テーブル　ルールを用いて LAN インタフェース間で転送される通信のポリシーを生成します。

必要に応じ IP テーブル　ルールを追加します。　2 重化 LAN ユニットで IP の転送を可能にするときには、IP テーブル　ルールを用いて LAN インタフェース間で転送される通信のポリシーを生成します。

これらのルールは保存ボタンをクリックするとした後でのみ直ちに以後永久に有効になりますもしルールに誤りがあるとそのため、装置がアクセスできなくなるので、これが誤りから復旧することを可能にします。システムを再起動します。ルールを保存しないと、再起動でそれらを失います。

ルールは IPTables コマンドを用いてカーネルに追加されます。

4. IPTables Rule のフィールドにルールを記入して、適用をクリックします。必要なだけのルールを追加します。
5. 保存をクリックします。ルールがそのページに標示されます。
6. そう選択するなら一部あるいはすべてのデフォルトのルールを削除することができます。

SSL 証明書

SX II では、接続先クライアントとの間で送受信されるトラフィックを暗号化するために Secure Sockets Layer (SSL) が使用されます。

SX II とクライアントとの接続を確立する際、暗号化された証明書を使用して、SX II の正当性をクライアントに示す必要があります。

SX II 上で、証明書署名要求 (CSR) を生成し、証明機関 (CA) によって署名された証明書をインストールすることができます。SHA-1 ト SHA-2 の両方の CSR がサポートされています。

CA はまず、CSR 発行元の身元情報を検証します。

続いて、署名された証明書を発行元に返します。有名な CA によって署名されたこの証明書は、証明書発行者の身元を保証する目的で使用されます。

重要：SX II の日付と時刻が正しく設定されていることを確認します。

自己署名証明書が作成されると、SX II の日付と時刻を使用して、有効期間が計算されます。SX II の日付と時刻が正確でない場合、証明書の有効な日付範囲が正しくなくなり、証明書の検証に失敗するおそれがあります。参照 日付/時刻の設定。

葦:CSR は、SX II で生成する必要があります。

注: ファームウェアをアップグレードしても、アクティブな証明書および CSR は置き換えられません。

SSL 証明書を作成してインストールするには

1. セキュリティメニューの証明書を選択します。
2. 次の各フィールドの値を指定します。

a. 共通名 – SX II をネットワークに追加したときに指定した、SX II のネットワーク名。通常は完全にルールに則ったドメイン名です。共通名は、Web ブラウザで SX II にアクセスする際に使用する名前から、プレフィックスである「http://」を除いたものです。ここで指定した名前が実際のネットワーク名と異なる場合は、HTTPS を使用して SX II にアクセスする際に、ブラウザでセキュリティ警告が表示されます。

b. 組織内部門: SX II が属する、組織内の部門。

c. 組織: SX II が属する組織。

d. 市区町村: 組織が存在する市区町村。

e. 都道府県: 組織が存在する都道府県。

f. 国 (ISO コード): 組織が存在する国。2 文字の ISO コードを入力します。たとえば、ドイツの場合は「DE」、米国の場合は「US」と入力します。

g. チャレンジ パスワード: 一部の CA は、証明書が失効した場合などに証明書の変更を許可するための、チャレンジ パスワードを要求します。CA 証明書の CSR を生成するときに適用されます。

h. チャレンジ パスワードの確認入力: 確認のためチャレンジ パスワードを再度入力します。CA 証明書の CSR を生成するときに適用されます。

i. 電子メール: SX II とそのセキュリティを担当する人の電子メール アドレス。

j. キー長 (単位: ビット): 生成されるキーの長さ (単位: ビット)。デフォルトは 2048 です。

3. 生成するには、次のいずれかの手順に従います。

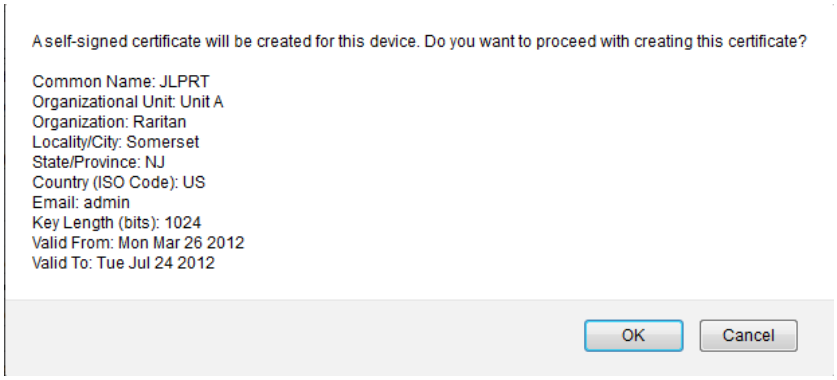
- 自己署名証明書を生成するには、以下の手順に従います。

a. 自己署名証明書を生成する必要がある場合は、自己署名証明書の作成チェックボックスをオンにします。このオプションを選択すると、入力内容に基づいて証明書が生成され、SX II が署名証明機関として機能します。CSR をエクスポートして署名入り証明書の生成に使用する必要はありません。

b. 有効期限の日数を指定します。SX II の日付と時刻が正しいことを確認してください。日付と時刻が正しくない場合、証明書の有効期間が正しく計算されない可能性があります。

c. 作成をクリックします。

d. 確認ダイアログ ボックスが表示されます。[OK] をクリックして、ダイアログ ボックスを閉じます。

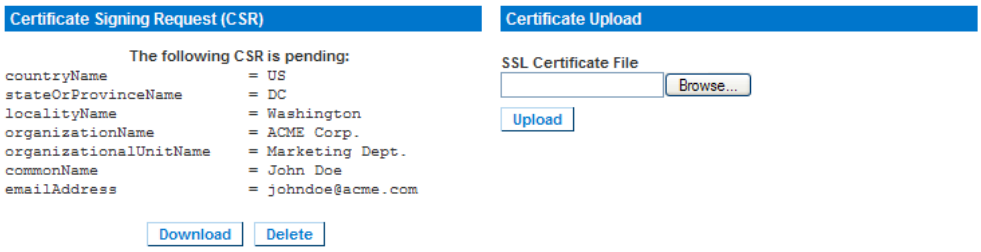


e. SX II を再起動して自己署名証明書を有効にします。

- CSR を生成して証明書の CA に送信するには、以下の手順に従います。

a. 作成をクリックします。

b. 入力したすべての情報を含むメッセージが表示されます。



c. CSR、および CSR 生成時に使用された秘密鍵を含むファイルをダウンロードするには、CSR のダウンロードをクリックします。

d. 証明書を取得するため、保存されている CSR を CA に送信します。CA から新しい証明書が届きます。

注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。

- CA から証明書を取得したら、アップロードをクリックして SX II にアップロードします。
- SX II を再起動して証明書を有効にします。

この手順が完了すると、SX II 専用の証明書が入手されます。この証明書は、 の身元をクライアントに対して示す際に使用されます。

重要：SX II 上の CSR を破棄した場合、復旧する方法はありません。誤

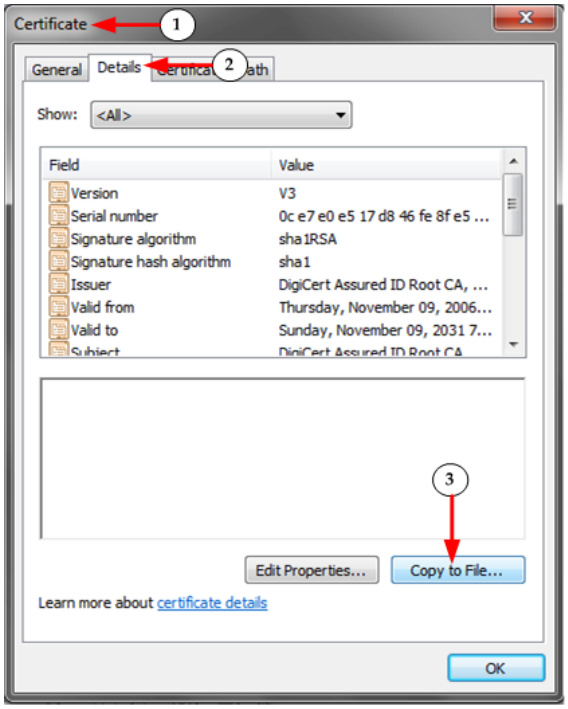
って CSR を削除してしまった場合、前述の 3 つの手順をやり直す必要があります。やり直しを回避するには、ダウンロード機能を利用し、CSR とその秘密鍵のコピーを取得しておきます。

バイナリーの証明書を Base64-Encoded DER Certificate （オプション）に変換する

SX II は SSL 証明書を Base64-Encoded DER フォーマットか PEM フォーマットで要求します。

もし SSL 証明書をバイナリー フォーマットで使用していると、それをインストールすることができません。

しかし、バイナリー SSL 証明書を変換することができます。



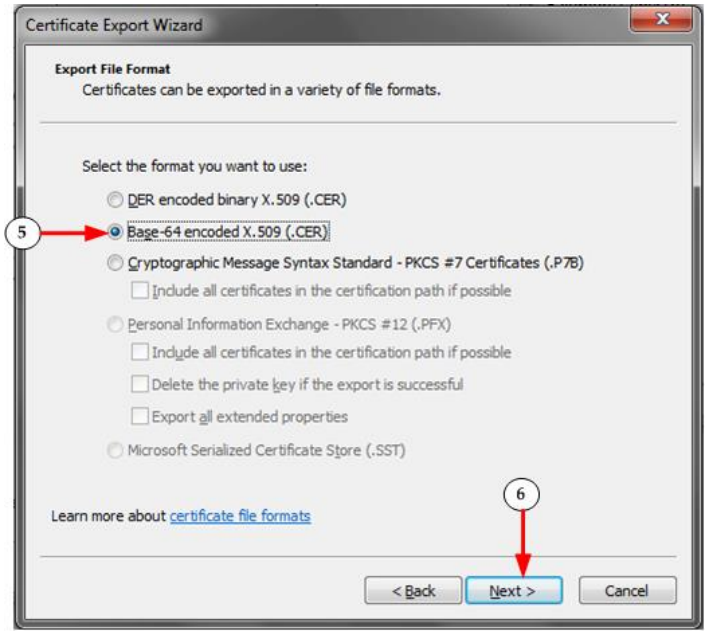
1. DEGHKVM0001.cer のバイナリー ファイルをウインドウ マシン上での位置を求めてください。

   DEGHKVM0001.cer ファイルの上でダブルクリックしてその証明書ダイアログを開けます。

2. 詳細タブをクリックします。

3. ”Copy to File...” をクリック

4. 証明書エキスポートウィザードが開きます。Next をクリックしてウイザードを開始します。



5. ウィザードの第２のダイアログで”Base-64 encoded X.509” を選択します。
6. Next をクリックしてそのファイルを Base-64 encoded X.509 として保存します。

これで、SX II で証明書のインストールができます。

セキュリティ バナー

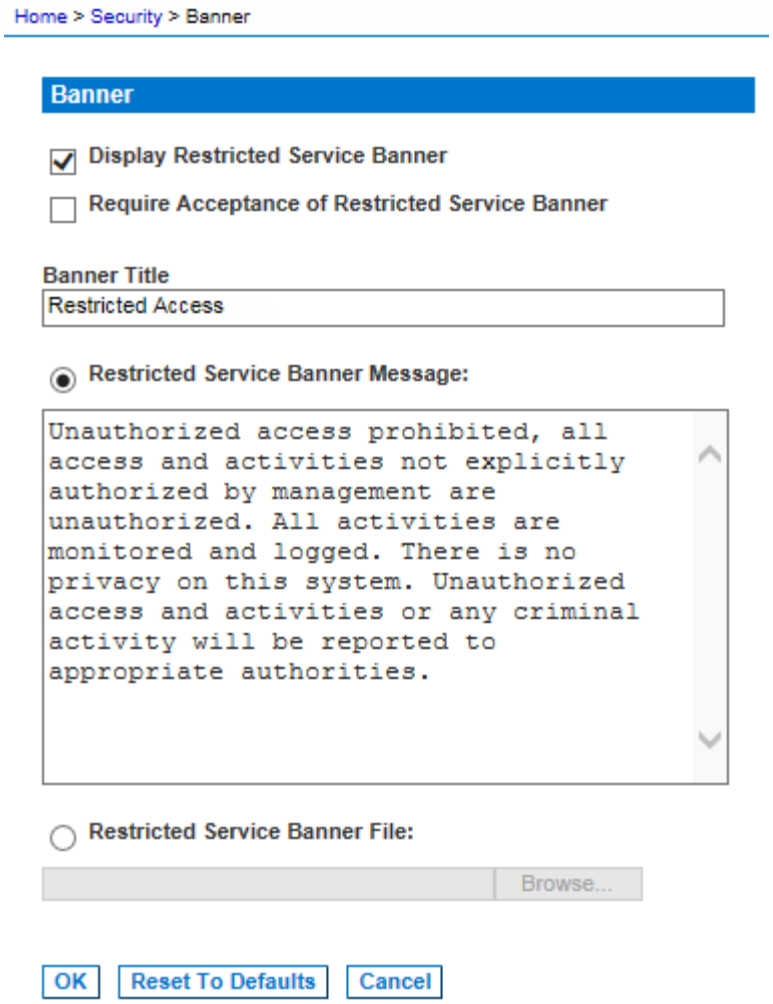
SX II ログイン プロセスにセキュリティ バナーを追加できます。この機能により、ユーザは、SX II にアクセスできるようになる前に、セキュリティ同意書に同意するかどうかの選択を求められます。セキュリティ バナーの内容は、ユーザが自分のログイン資格情報を使用して SX II にアクセスした後、[Restricted Service Agreement] (制限付きサービス同意書) ダイアログ ボックスに表示されます。

セキュリティ バナーの見出しおよび本文はカスタマイズできます。デフォルトのテキストをそのまま使用することもできます。また、セキュリティ バナーは、ユーザがセキュリティ同意書に同意してからでないと SX II にアクセスできないように設定することも、単にログイン プロセス終了後に表示することもできます。同意/不同意機能が有効になっている場合、ユーザが選択した内容が監査ログに記録されます。

セキュリティ バナーを設定するには

1. [Security] (セキュリティ) ー [Banner] (バナー) をクリックし、[Banner] (バナー) ページを開きます。
2. [Display Restricted Service Banner] (制限付きサービス バナーを表示する) チェック ボックスをオンにし、この機能を有効にします。
3. ユーザがセキュリティ バナーに同意してからでないとログイン プロセスを続行できないようにするには、[Require Acceptance of Restricted Service Banner] (制限付きサービス バナーに対する同意を義務付ける) チェック ボックスをオンにします。ユーザがセキュリティ バナーに同意するには、チェック ボックスをオンにします。この設定を有効にしない場合、ユーザがログインした後にセキュリティ バナーが表示されるだけであり、ユーザがセキュリティ バナーに同意する必要はありません。
4. 必要があれば、バナー タイトルをカスタマイズします。この情報は、バナーの一部としてユーザに対して表示されます。最大 64 文字まで使用できます。
5. [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックス内のテキストをカスタマイズします。入力できるテキストは最大 6,000 文字です。直接入力する方法と、テキスト ファイルからアップロードする方法があります。次のいずれかの手順を実行します。
   a. このボックス内のテキストを手動で編集します。[OK] をクリックします。

b. .txt ファイル内のテキストをアップロードします。具体的には、[Restricted Services Banner File] (制限付きサービス バナー ファイル) を選択し、[Browse] (参照) をクリックしてファイルを探し、アップロードします。[OK] をクリックします。ファイルがアップロードされると、そのファイル内のテキストが [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックスに表示されます。



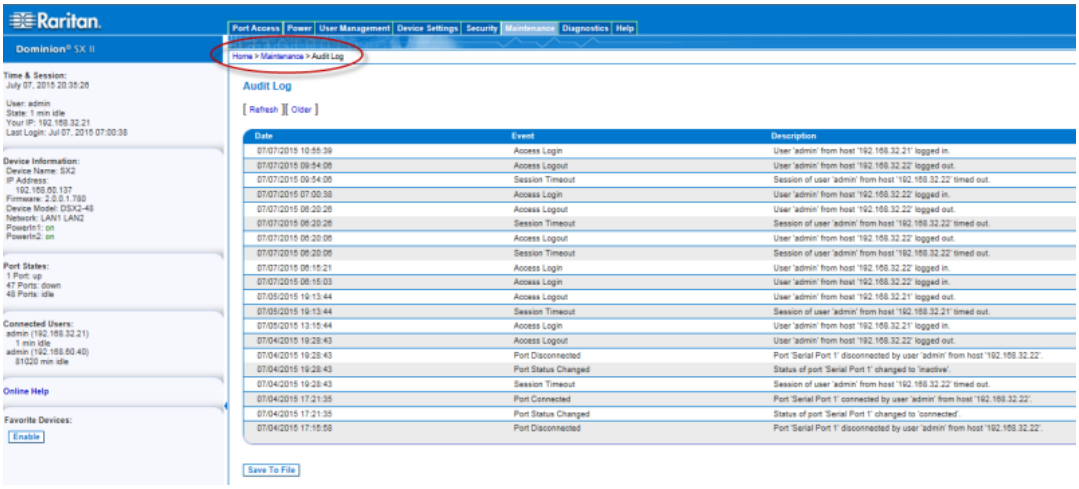
リモート コンソールから保守設定をセットする

監査ログ

SX II のシステム イベントに関するログが作成されます。

監査ログは最大で約 2K 行相当のデータを保持でき、これを超えると最も古いエントリから上書きされます。

監査ログのデータが失われないようにするには、syslog サーバまたは SNMP マネージャにデータをエクスポートします。syslog サーバまたは SNMP マネージャは、デバイス設定のイベント管理ページから設定します。



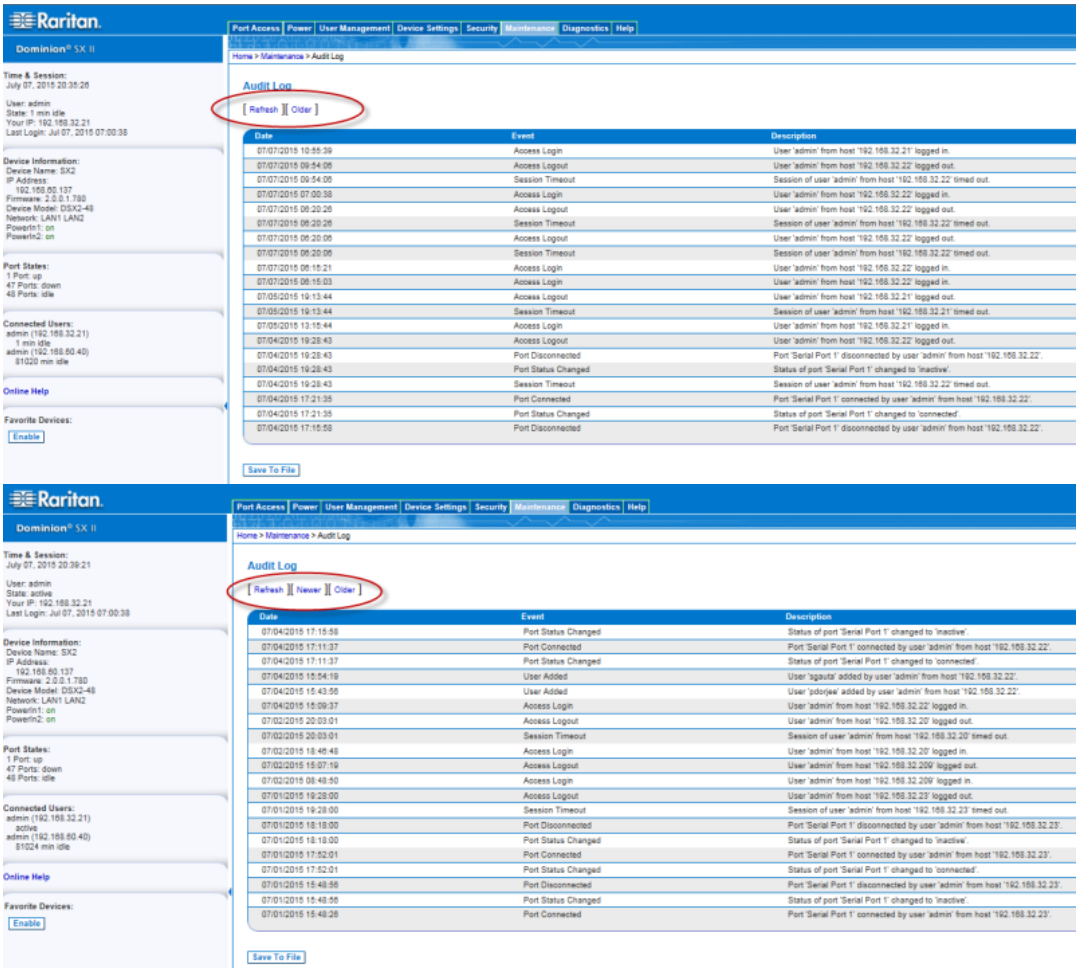
1. メンテナンスメニューの監査ログをクリックします。監査ログ ページが開きます。

   監査ログ ページでは、日時順にイベントが表示されます (最も新しいイベントが先頭に表示されます)。監査ログに含まれる情報は次のとおりです :

   - 日時: イベントが発生した日時 (24 時間形式)。
   - イベント: イベント管理ページに一覧表示されるイベント名。
   - 説明 : イベントの詳細な説明。

2. ファイルに保存をクリックしますファイルに保存ダイアログ ボックスが開きます。
3. ファイル名と保存先フォルダを選択し、保存をクリックします。監査ログが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。
4. リフレッシュをクリックしてリストをリフレッシュします。古い方をクリックして古いログ記録を見ます。

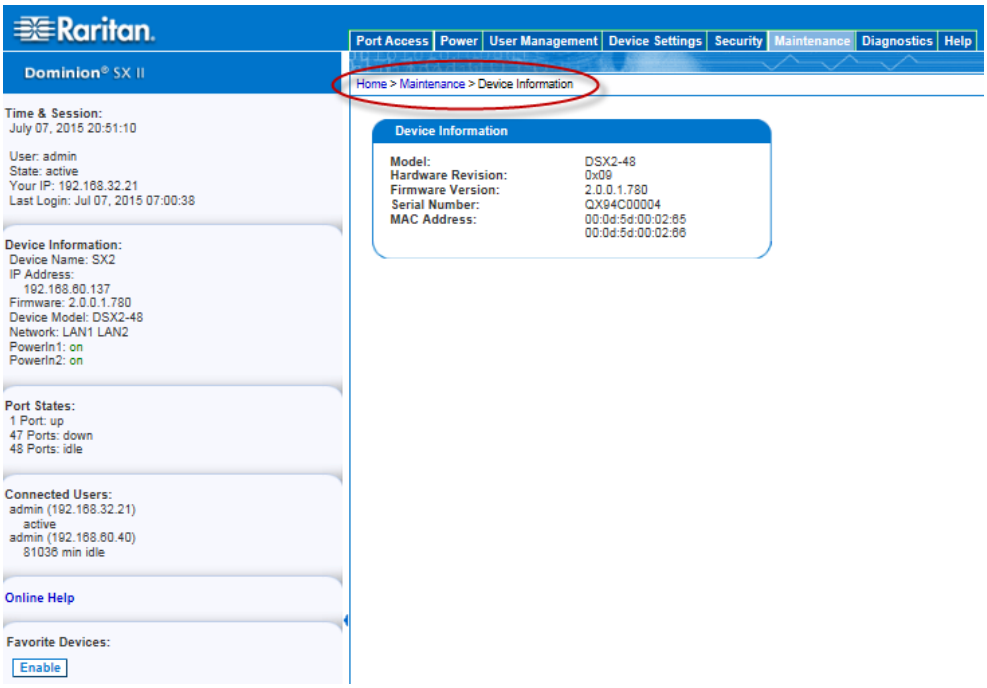
5. 監査ログをページごとにめくるには、古い方と新しい方のリンクを使います。



Raritan.

デバイス情報

メンテナンス > デバイス情報を選択しま他の SX II に特有の情報を見ます。これはサポートのために有用です。



バックアップと復元

バックアップ/復元ページでは、 SX II の設定情報をバックアップおよび復元できます。

バックアップ/復元機能には、業務継続性を確保するというメリットに加え、時間節約効果もあります。

たとえば、使用している SX II のユーザー設定をバックアップし、それらの設定を新しい SX II に復元することで、チームに対して別の SX II からのアクセス権を速やかに付与できます。

また、1 台の SX II をセットアップし、その設定情報を複数台の SX II にコピーすることもできます。

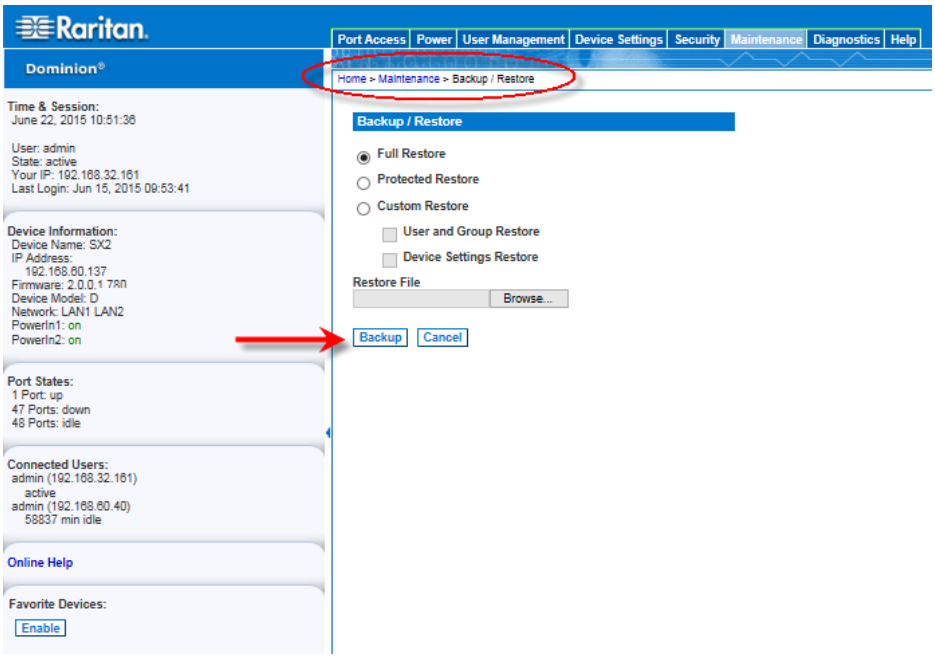
葦:バックアップ処理では、常にシステム全体がバックアップされます。復元処理では、全体を復元するか一部を復元するかをユーザが選択できます。

▶ **Internet Explorer 7 以降を使用している場合、SX II をバックアップするには、以下の手順に従います。**

1. メンテナンス メニューの > バックアップ/復元をクリックします。バックアップ/復元ページが開きます。

2. バックアップをクリックします。開くボタンを含むファイルのダウンロードダイアログ ボックスが開きます。開くをクリックしないでください。

   IE 7（以降）では、ファイルを開くデフォルトのアプリケーションとして IE が使用されるため、ファイルを開くか、または保存するように求められます。これを回避するには、ファイルを開くために使用されるデフォルトのアプリケーションをワードパッドに変更する必要があります®。



3. このためには、以下の手順に従います。
   a. バックアップ ファイルを保存します。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。
   b. 保存されたら、ファイルを探して右クリックします。[プロパティ] を選択します。
   c. [全般] タブで [変更] をクリックし、[WordPad] を選択します。

SX II を復元するには

警告:使用している SX II を旧バージョンに復元する場合、注意が必要です。バックアップ時点で設定されていたユーザ名とパスワードが復元されます。以前の管理者ユーザー名とパスワードを記憶していないと SX II からロックアウトされます。

また、バックアップ時点で現在と異なる IP アドレスを使用していた場合、その IP アドレスも同様に復元されます。IP アドレスの割り当てに DHCP を使用している場合、ローカル ポートにアクセスして復元後の IP アドレスを調べる必要があります。

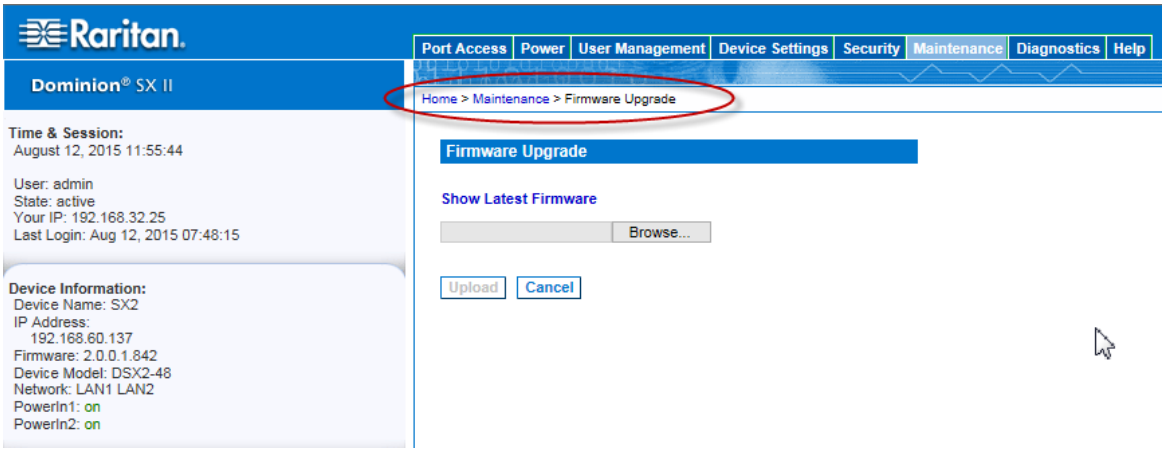
1. 実行する復元処理のタイプを選択します。
   - 完全復元: システム全体を復元します。この復元タイプの主な用途は、一般的なバックアップ/復元処理です。
   - 部分復元: デバイス固有情報 (例: IP アドレス、名前) 以外のすべての情報が復元されます。この復元タイプの用途としては、1 台の SX II をセットアップし、その設定情報を複数台の SX II にコピーするケースなどが考えられます。
   - カスタム復元: この復元タイプを選択した場合、ユーザとグループの復元チェック ボックスとデバイス設定の復元チェック ボックスのいずれか一方または両方をオンにすることができます。
   - ユーザとグループの復元: このチェック ボックスをオンにした場合、ユーザ情報とグループ情報だけが復元されます。このオプションでは認証と個人キーのファイルは復元しません。 別の SX II 上でユーザ情報をセットアップする際に便利です。
   - デバイス設定の復元: このオプションは、関連電源、、ポート グループの割り当てのような デバイス設定だけが含まれています。デバイス情報を素早くコピーする際に便利です。
2. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
3. 適切なバックアップ ファイルを探して選択し、[Open] (開く) をクリックします。選択したファイルが [Restore File] (復元ファイル) ボックスに表示されます。
4. [Restore] (復元) をクリックします。選択した復元タイプに基づいて、設定情報が復元されます。

ファームウェアのアップグレード

ファームウェアのアップグレードページで SX II のファームウエアを更新し、また SX II が CC-SG の管理のもとにある場合 CC-SG から更新します。

重要 : アップグレード処理中に、 SX II の電源を切断したり ターゲットを切断したりしないでください。装置が損傷するおそれがあります。

1. メンテナンスメニューのファームウエア更新をクリックします。ファームウェアのアップグレードページが開きます。



2. 最新のファームウエアの表示のリンクをクリックし、適切な Raritan ファームウエア配布ファイル（*.RFP）を Raritan のウエブサイトのファームウエア更新ページで見つけます。
3. そのファイルを解凍します。アップグレードを実行する前に、解凍したファイルに記載されている指示をすべてお読みください。

注:アップグレードを実行する前に、そのファームウェア配布ファイルをローカル PC にコピーしておいてください。また、そのファームウェア配布ファイルをネットワーク ドライブからロードしないでください。

---

4. ブラウズ をクリックし、ファームウェア配布ファイルを解凍したフォルダに移動します。
5. ファームウェアのアップグレードページのアップロードをクリックします。
6. アップグレードとバージョン番号に関する情報が、確認のために表示されます。（ターゲット情報を表示するよう指定した場合は、その情報も表示されます。）

注:この時点で接続していたユーザはログオフされ、新たにログオンしようとしたユーザはブロックされます。

---

7. アップグレードをクリックします。

   アップグレード処理が完了するまで待機します。アップグレード処理中は、ステータス情報および進行状況バーが表示されます。アップグレード処理が完了すると、装置が再起動します。（）再起動が完了するとビープ音が 1 回鳴ります。
8. 指示に従ってブラウザを終了し、約 5 分待ってから再度 SX II にログオンします。

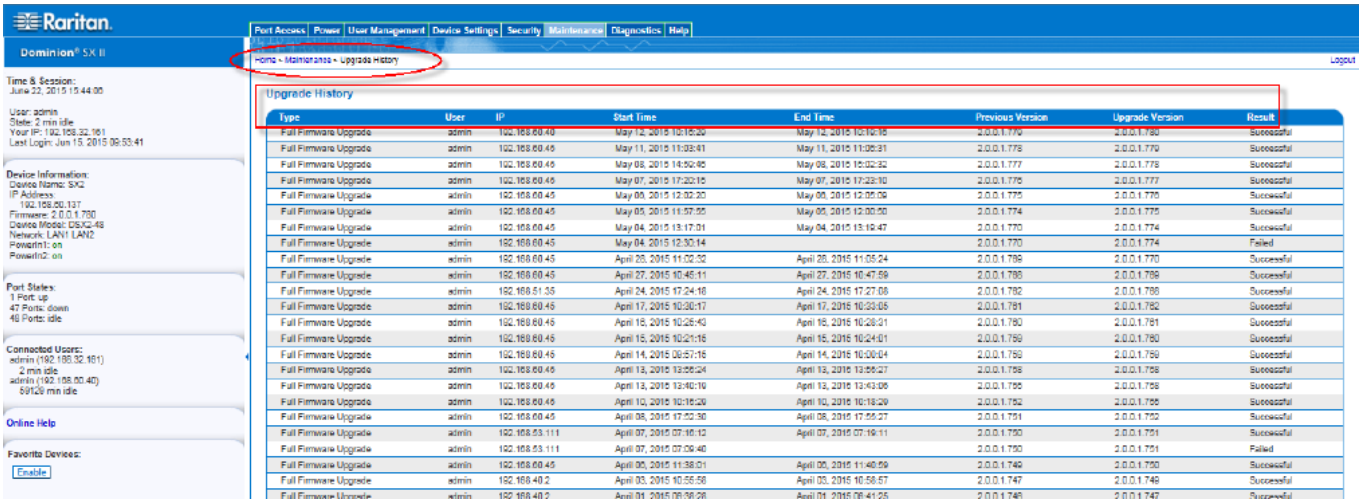
アップグレード履歴

SX II はSX II と取り付けられたデバイスに関する情報を提供します。

- メンテナンス > 更新 の履歴を選択し更新の履歴を見ます。

実行された SX II アップグレード処理に関する情報、アップグレード処理の最終ステータス、アップグレード処理の開始日時と終了日時、および、アップグレード前と現在のファームウェア バージョンが表示されます。ターゲットに関する情報も提供されます、更新へのリンクを表示をクリックして入手します。表示されターゲット情報は次のとおりです。

- タイプ : ターゲット のタイプ。
- ユーザ : アップグレード処理を実行したユーザ。
- [IP]: IP アドレス　ファームウエアの箇所。
- 開始時刻 : アップグレード処理の開始日時。
- 終了時刻 : アップグレード処理の終了日時。
- 以前のバージョン : アップグレード前のファームウェア バージョン。
- 更新後のバージョン : 現在のファームウェア バージョン。
- 結果 : アップグレード処理の結果 (成功または失敗)。



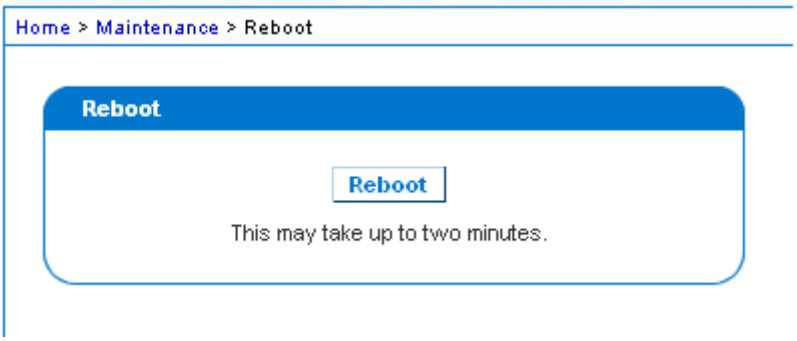
SX II　の再起動

[Reboot] (再起動) ページでは、SX II を安全に再起動できます。再起動する場合、このページから行うことを推奨します。

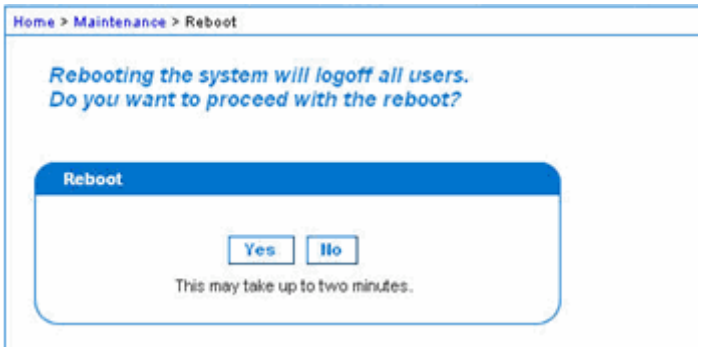
重要：すべての 接続が切断され、ユーザーもすべてログオフされます。

SX II を再起動するには

1. [Maintenance] (保守) メニューの [Reboot] (再起動) をクリックします。[Reboot] (再起動) ページが開きます。



2. [Reboot] (再起動) をクリックします。再起動してもよいかどうかを確認するダイアログ ボックスが開きます。[Yes] (はい) をクリックし、再起動処理を続行します。



装置のリセットボタンを用いて SX II をリセットする

デバイスの背面パネルにリセット ボタンがあります。誤ってリセットされることがないように、ボタンはパネルに埋め込まれています（このボタンを使用するには、先端が尖った道具が必要です)。

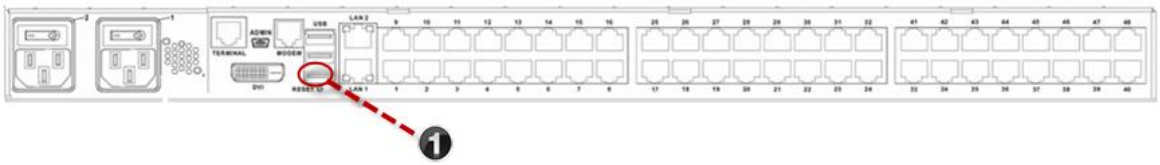
リセット ボタンを押したときに実行される処理については、暗号化および共有ページで定義します。参照 ***暗号化と共有の設定*** 『170p. 』。

注:出荷時設定にリセットする前に、監査ログを保存しておくことを推奨します。

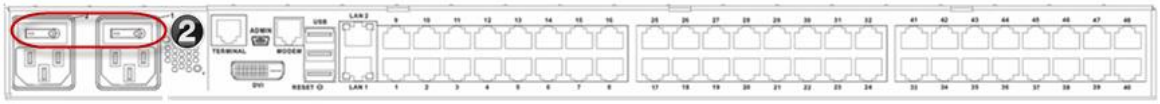
出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログを保存することについての詳細については、以下を参照してください **監査ログ** *『183p. 』。*

---

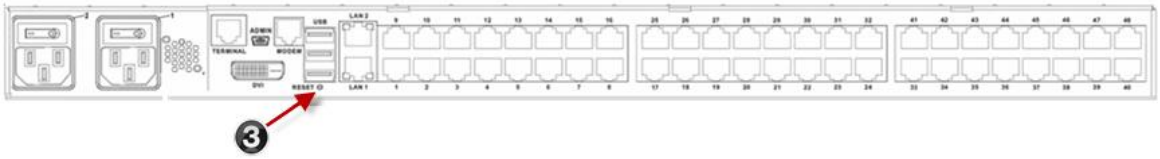
1. リセットボタンに正しくアクセスして押す野を確実にするため、リセットボタンに一番近い ボタン USB ケーブル を取り除きます。



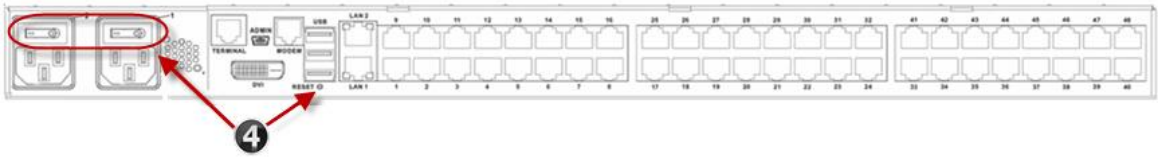
2. 電源をオフにします。



3. ペーパークリップのように先端の尖った道具を使用してリセット ボタンを押し続けます。



4. リセット ボタンを押したまま、 SX II の電源を入れ直します。約 1 秒の長さのビープ音を聞くまでリセットボタンを押し続けます。



一旦デバイスのリセットに成功すると、装置から 2 回のビープ音が装置から発せられます。

リモート コンソールから診断のオプションを設定する

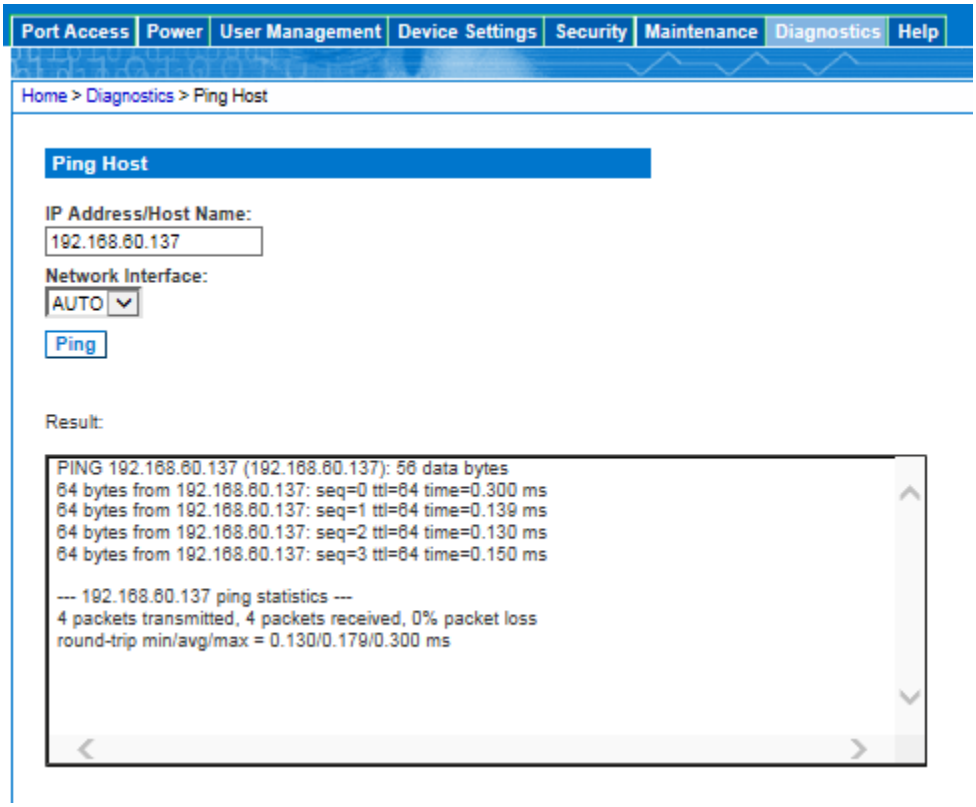
ホストに ping するページ

ping は、特定のホストまたは IP アドレスが IP ネットワーク上で接続可能であるかどうかをテストするためのネットワーク コマンドです。ホストに ping するページでは、ターゲット サーバまたは別の SX II がアクセス可能であるかどうかを調べることができます。

1. 診断メニューの > ホストに ping するをクリックします。ホストに ping するページが開きます。
2. IP アドレス/ホスト名ボックスに IP アドレスまたはホスト名を入力します。

   拳:ホスト名は 232 文字以内で指定してください。
3. アダプティブ ping。ping の実行結果が結果フィールドに表示されます。

4. ネットワークインタフェースのドロップダウンリストから特定のインタフェースに PING するためにそのインタフェースを選択します。〈オプション〉



ホストへの経路をトレースするページ

traceroute は、指定したホスト名または IP アドレスへの経路を調べるためのネットワーク コマンドです。

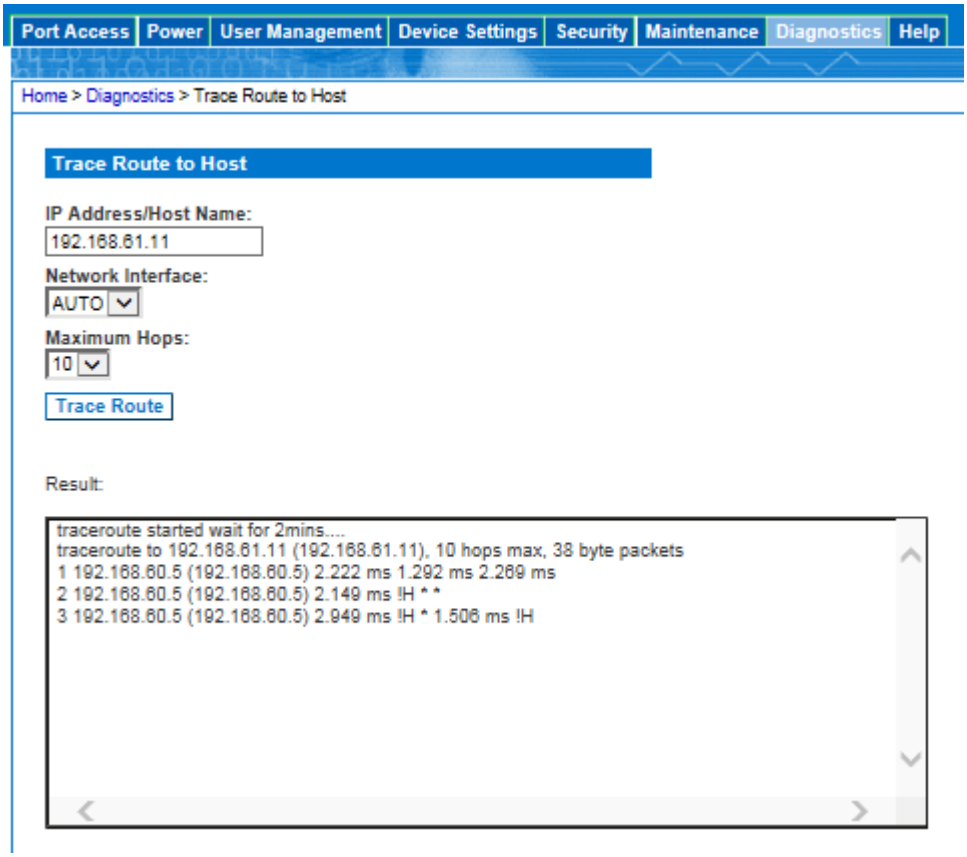
ホストまでの経路をトレースするには

1. 診断メニューのホストへの経路をトレースするをクリックします。ホストへの経路をトレースするページが開きます。
2. P アドレス/ホスト名ボックスに IP アドレスまたはホスト名を入力します。

   注:ホスト名は 232 文字以内で指定してください。

3. 最大ホップ数ボックスの一覧で最大ホップ数を選択します (5 刻みで 5 ～ 50)。
4. 経路をトレースするをクリックします。traceroute コマンドが、指定したホスト名または IP アドレスに対して、指定した最大ホップ数以内で実行されます。traceroute コマンドの実行結果が結果フィールドに表示されます。

5. ネットワークインタフェースのドロップダウンボックスから特定のインタフェースで ルート追跡するためのインタフェースを選択します。〈オプション〉



診断のスクリプトを実行し診断ファイルを作成する。

注:これは、Raritan フィールド エンジニアが使用するためのページです。Raritan のテクニカル サポート部門から指示された場合に限り、ユーザも使用できます。

この機能を用いて、 SX II からクライアントのマシンに診断情報をダウンロードします。

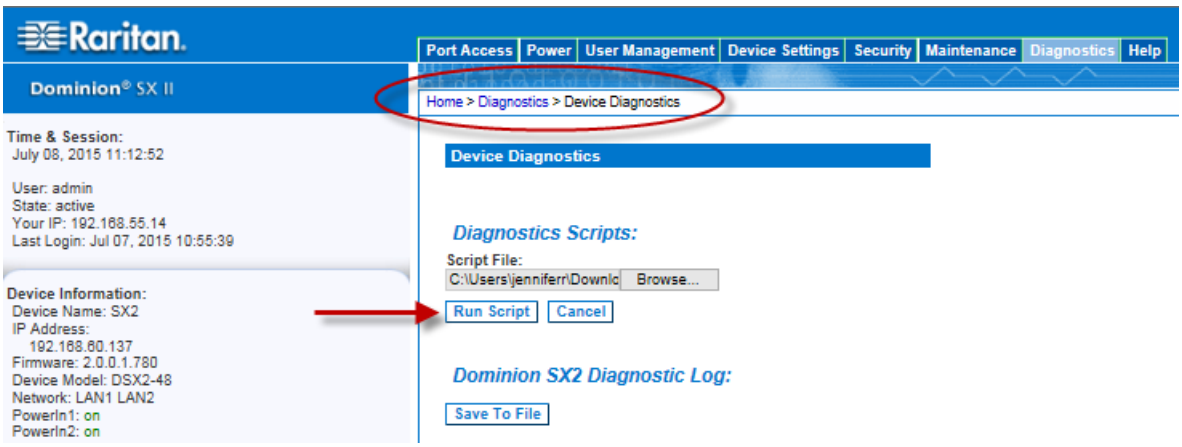
このページでは、次の 2 種類の処理を行うことができます。

- 重大エラー デバッグ セッション中に、Raritan のテクニカル サポート部門から提供された特別な診断スクリプトを実行する。このスクリプトは、SX II にアップロードされ、実行されます。このスクリプトの実行が完了した後、ファイルに保存をクリックして診断メッセージをダウンロードすることができます。
- 診断メッセージのスナップショットに対するデバイス診断ログを、SX II 装置 からクライアント コンピュータにダウンロードします。このダウンロードされた暗号化デバイス診断ログは、Raritan のテクニカル サポート部門に送信されます。このファイルを解析できるのは Raritan だけです。

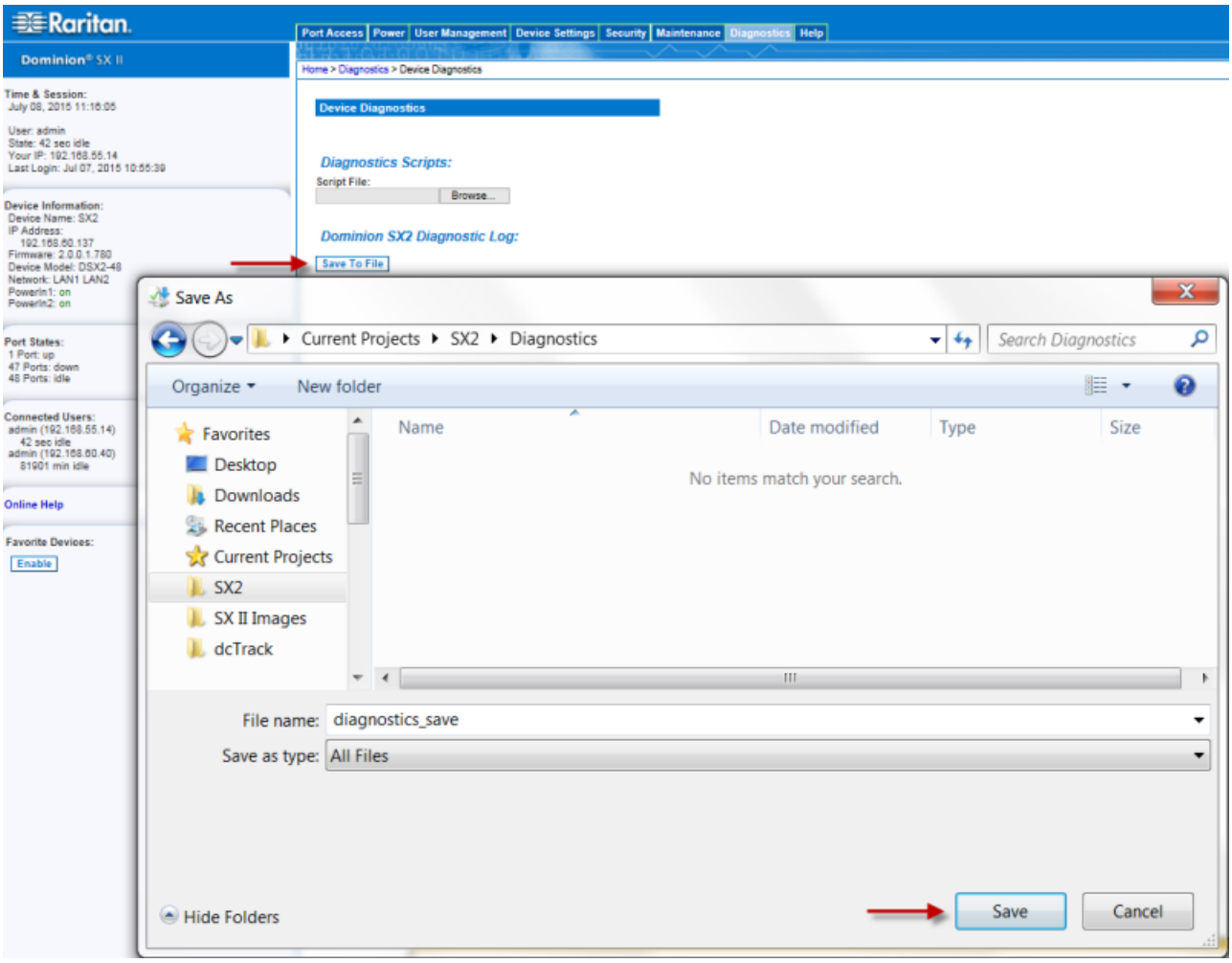
注:このページを開くことができるのは、管理者権限を持つユーザだけです。

---

1. 診断 > SX II 診断を選択します。 SX II 診断ページが開きます。
2. Raritan テクニカル サポート部門から e メールされた診断スクリプトを実行するには、Raritan から供給された診断ファイルをブラウズ機能を用いて探し当てます。
3. スクリプト実行をクリックします。この診断スクリプト ファイルを Raritan のテクニカル サポート部門に送信します。



4. Raritan テクニカル サポート部門に送る診断ファイルうを作成するには、ファイルに保存をクリックし、で保存ダイアログからファイルをローカルに保存します。



5. Raritan のテクニカル サポート部門の指示に従って、このファイルを電子メールで送信します。

ネットワーク インタフェースページ

SX II では、ネットワーク インタフェースのステータス情報を確認できます。

ネットワーク インタフェースに関する情報を表示するには

- 診断 メニューのネットワーク インタフェースをクリックします。ネットワーク インタフェースページが開きます。

表示される情報は次のとおりです。

- Ethernet インタフェースが稼動しているかどうか。
- ゲートウェイから ping できるかどうか。
- 現在アクティブな LAN ポート。

これらの情報を更新するには

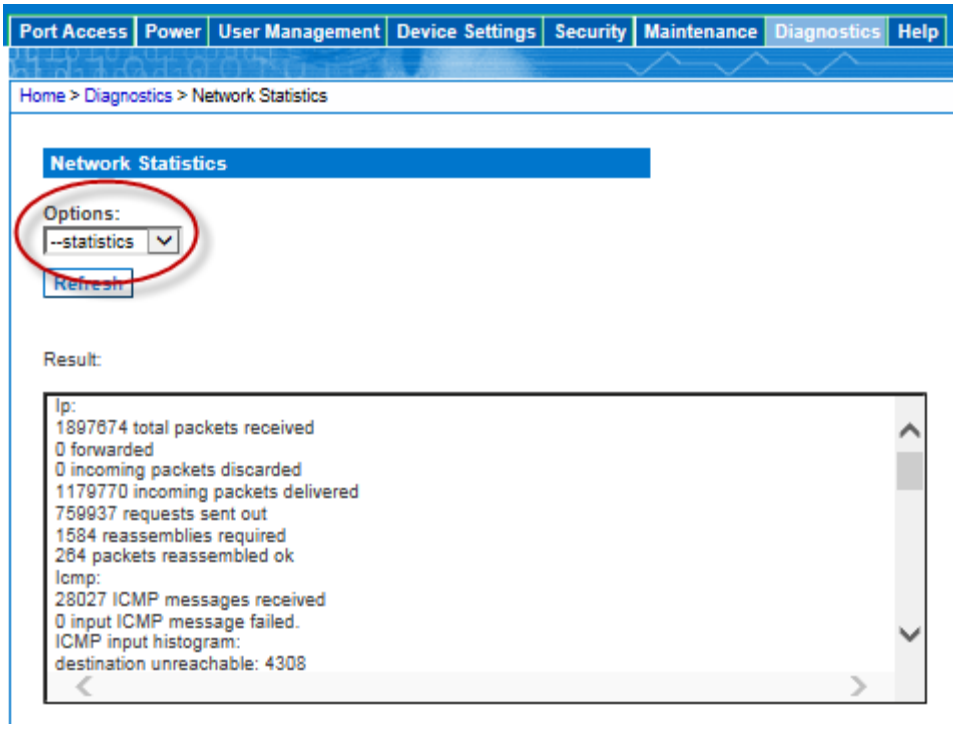
- 更新をクリックします。

ネットワーク統計) ページ

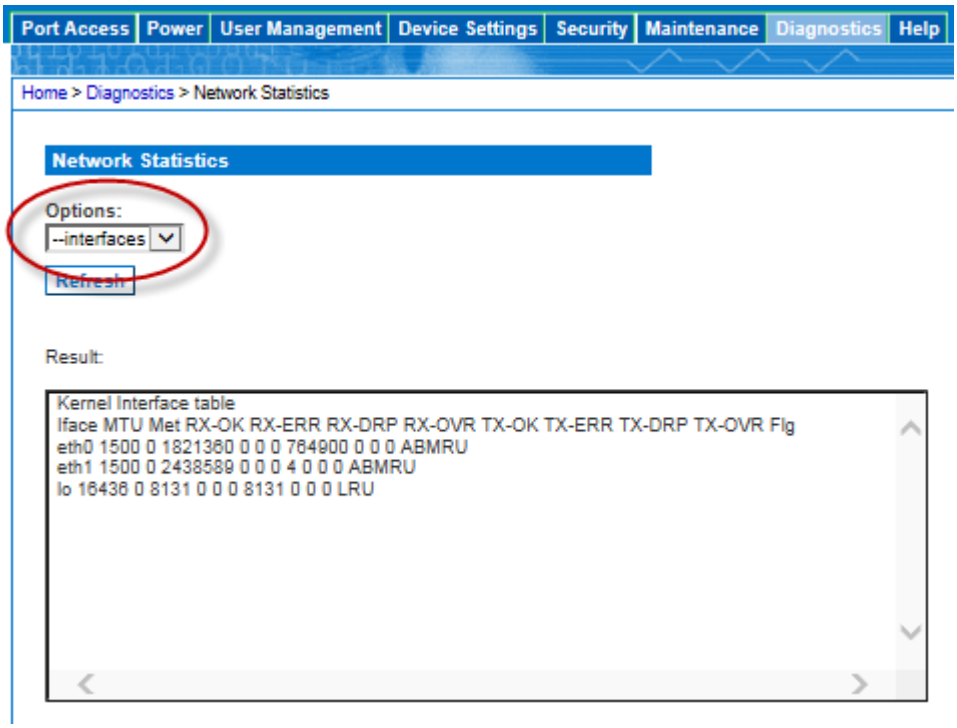
SX II では、ネットワーク インタフェースに関する統計情報を表示できます。

1. 診断メニューのネットワーク統計をクリックします。ネットワーク統計ページが開きます。
2. オプションボックスの一覧で値を選択します。
3. 更新をクリックします。オプションボックスの一覧で選択した値に応じた情報が、結果フィールドに表示されます。

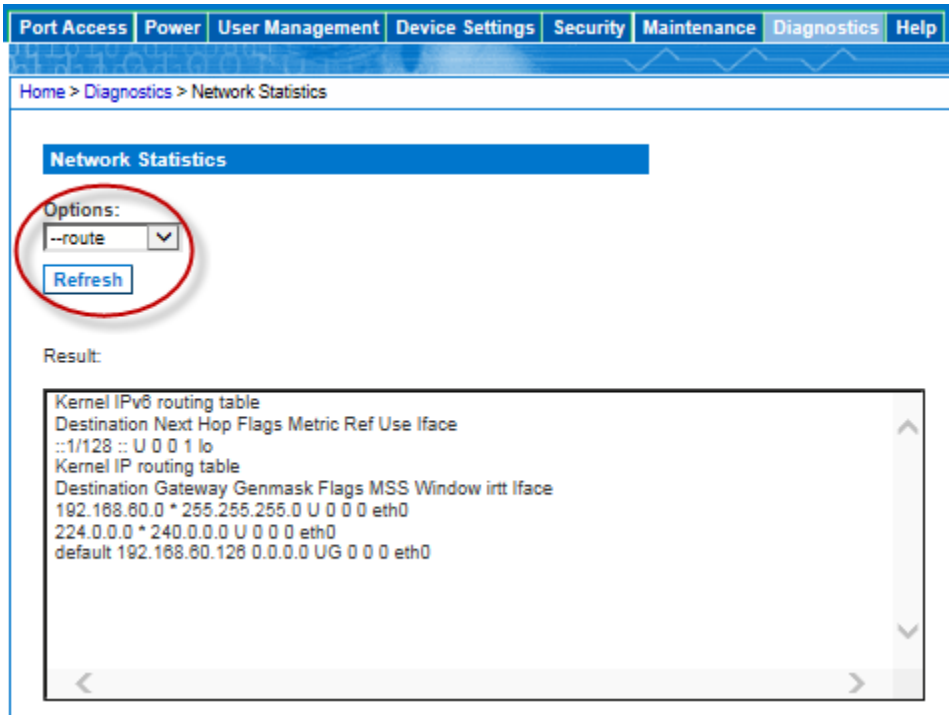
- 統計: 次に示すような情報が表示されます。



- インタフェース: 次に示すような情報が表示されます。



- 経路: 次に示すような情報が表示されます。



コマンドラインインタフェース を用いて SX II を管理する

このセクションはコマンドラインインタフェースを用いて実行されるタスクに特定のものです。

SX II リモート コンソールでのタスクの実行についての情報は、次を参照してください。 *リモート コンソールから SX II を管理する* 『71p. の *"リモート コンソールから SX II を管理する"*参照 』。

CLI を使ってパスワードを変更する

注:この機能はリモートコンソール からも設定できます。参照 **リモートコンソールからパスワードを変更する** *『28p. 』。*

重要：管理者パスワードを忘れた場合には、 SX II を後面パネルにあるリセットボタンによって出荷時デフォルトにリセットする必要があり、初期設定作業をもう一度行う必要があります。

次を入力します - admin > パスワード を選択してメニューにアクセスする。

CLI を経由してパスワードを創るときには、スペースで始めたりスペースで終わることはできません。これはリモートコンソールを用いてパスワードを創る時には適用されません。

コマンド	記述	パラメータ
パスワード	必要であれば新規のパスワードを作成します。	▪ 新規パスワード

CLI を用いた電源タップの設定

注:この機能はリモートコンソール からも設定できます。参照 **リモートコンソールからの電源タップの設定** *『72p. 』。*

以下の電源用コマンドで SX II に取り付けられた電源タップを管理できます。

次を入力します - admin > power これでメニューにアクセスします。

コマンド	記述	パラメータ
associate	電源タップのコンセントを SX II のポートに関連つけます。	▪ <port number> - 関連させる SX のポート番号 ▪ <powerstrip name> - アクセスするための電源タップの名前 ▪ <outlet number> - 電源タップ上のコンセントの番号
cycle	指定した電源タップの電源再投入 *注:PX を SX II に接続するところであれば、パワー電源再投入を 5 秒にすることを勧めます。*	▪ <port number> - 電源再投入（再投入）させる SX のポート番号 ▪ <powerstrip name> - アクセスするための電源タップの名前 ▪ <outlet number> - 電源再投入させる電源タップ上のコンセントの番号
off	指定した電源タップの電源オフ	▪ <port number> - 電源をオフさせる SX のポート番号 ▪ <powerstrip name> - アクセスするための電源タップの名前 ▪ <outlet number> - 電源をオフせる電源タップ上のコンセントの番号

コマンド	記述	パラメータ
on	指定した電源タップの電源オフ	▪ 〈port number〉 – 電源をオンさせる SX のポート番号 ▪ 〈powerstrip name〉 – アクセスするための電源タップの名前 ▪ 〈outlet number〉 – 電源をオンせる電源タップ上のコンセントの番号
powerdelay	グローバルな電源タップの遅延を設定する	▪ 〈cycle value〉 – 電源オフからオンまでの遅延
powerstatus	指定した電源タップの状態を得る	▪ 〈powerstrip name〉 – アクセスするための電源タップの名前
powerstrip	電源タップの情報を得る	▪ 〈powerstrip name〉 – アクセスするための電源タップの名前
setpowerport	SX II のポートを電源ポートを含むように設定します。	▪ 〈port number〉 –SX のポート番号
unassociate	SX II のポートから電源タップの関連つけを取り外す。	▪ 〈port number〉 – 関連を外す SX のポート番号 ▪ 〈powerstrip name〉 – アクセスするための電源タップの名前 ▪ 〈outlet number〉 – 関連を外す電源タップ上のコンセントの番号
unsetpowerport	SX II のポートから電源ポートを取り外すように設定します。	▪ 〈port number〉 –SX のポート番号

CLI を用いてユーザとユーザグループを設定・管理する

注:この機能はリモート コンソールからも実行できます。参照 **リモート コンソールからユーザとグループを設定・管理する** *『78p. 』*。

SX II はすべてのユーザの属性とユーザグループの内部リストを保存しています。

ユーザ諸データとグループはアクセス権限と許可を決定するのに使われます。この情報は内部に保存されています。ユーザのパスワードは暗号化された形式で保存されます。

SX II は管理者が一般の許可と属性によってグループを定義できるようにします。彼らはユーザをグループに加え、各ユーザはそのグループの属性と許可を持ちます。

グループの許可はグループ内の各個人に適用されるため、許可を各個人ごとに別々に適用する必要はありません。これでユーザの設定をする時間を削減しています。

例えば、モデムアクセスと呼ばれるグループを生成し、モデムの管理の許可を持ちます。モデムアクセスグループに割り当てられた各ユーザはモデムの機能を管理できます。あなたは各ユーザに別々に許可を与える必要はありません。

次を入力します - `[admin] > [Config] > [Users]` これでメニューにアクセスします。

コマンド	記述	パラメータ
`addgroup`	一般の許可を持つグループを創る	group <groupname> - グループ名 ▪ control <number | range | *> - ユーザ グループがフルの制御許可を持つポート（このグループに割り当てられたユーザはリストされたポートに対して読み書きの許可を持ちます）。電源管理アクセスも付与されている場合は、そのグループに制御を割り当てる必要があります。これは 1 つのポートあるいはある範囲のポート(1-n あるいは 1,3,4 あるいは全てのポートには *). ▪ power <number | range | *> - ユーザ グループがフルの電源制御許可を持つポート許可（true）、拒絶（false）。 ▪ pcshare <true | false> PC の共有アクセス - グループ内のユーザがあるポートにアクセスを許可されているかどうかを示し、そのポートはそのアクセスが共有であればすでにユーザが接続しているものです。許可（true）、拒絶（false）。 ▪ viewonly settings <number range *> <true or

コマンド	記述	パラメータ
		false><true | false> – ユーザグループはそのポートに読みだけの許可を持ちます。許可(true)、拒絶(false)。 ▪ cc <true | false> – CC-SG 管理コマンドの下でのアクセスが許されます。許可（true）、拒絶（false）。 ▪ diagnostics <true | false> – 診断コマンドへのアクセスの許可許可（true）、拒絶（false）。 ▪ maintenance <true | false> – 保守コマンド、データベースのバックアップと復元、ファームウェアのアップグレード、ファクトリ リセットおよび再起動への許可許可（true）、拒絶（false）。 ▪ security <true | false> – セキュリティ コマンドへのアクセスの許可 SSL 認証、セキュリティ設定、IPACL。許可（true）、拒絶（false）。 ▪ manage user <true | false> – ユーザ管理コマンドへのアクセスの許可ユーザとグループの管理、リモート、認証、ログイン設定。許可（true）、拒絶（false）。 **重要** –ユーザ管理では自身も含むすべてのユーザの許可を変更することができます。これらの許可を付与する場合は注意してください。 ▪ modem <true | false> – モデムへのアクセスの許可内蔵モデムが SX II に接続されているときにページに表示されます。そのグループが外部モデムにアクセスするのを望む場合このオプションを選択します。ブロードバンドのアクセスがあるモデムに対して有効化されていると、この許可がまたグループにワイアレス モデムを通じて SX II にアクセスすることを可能にします。許可（true）、拒絶（false）。
editgroup	既存のユーザ グループを編集するコマンド。	▪ deny <number | range | *> – リストしたポートへの許可を拒否します。 ▪ powerdeny <number | range | *> – リストしたポートへの電源許可を拒否します。
showgroup	既存のユーザグループの詳細を表示します。 グループが指定されていない場合、このコマンドはシステム中のすべてのグループを表示します。	▪ <group name> – 表示 するグループ
deletegroup	既存のユーザ グループを消去するコマンド。	▪ <group name> – 消去するグループ

コマンド	記述	パラメータ
adduser	個別のユーザを SX II に追加します。	▪ user <loginname> – ユーザのログイン名 ▪ full name <user's fullname> – ユーザのフルの名前 ▪ group <groupname > – そのユーザが関連を持つグループ ▪ password <password> – ユーザのパスワード。CLI を経由してパスワードを創るときには、スペースで始めたりスペースで終わることはできません。これはリモートコンソールを用いてパスワードを創る時には適用されません。 ▪ active <true | false> – ユーザのアカウントを有効化(true) あるいは無効化(false) します。 ▪ <dialback> – ユーザのダイアルバック用電話番号
addsshkey	この addsshkey コマンドはそのユーザに SSH キーデータを追加します。このデータはクライアントのために生成された rsa_id.pub キーです。そのユーザは SSH キーを追加する前に SX II に存在していることが必要です。 このキーデータは認証に用いられるべきで、ユーザはパスワードを入力する必要はないはずです。 Linux のユーザはデフォルトでないパブリックキーを追加する際、生成されたキーの末尾に現れる ″name@local host″ を消去する必要があります。対応する個人のキーを使用する時には必要ありません。 Windows のユーザは常に ″name@local host″ を含む必要があります。	▪ user <loginname> – ユーザのログイン名 ▪ key <value> – ユーザの SSH キー
viewsshkey	特定のユーザのための SSH キーデータを標示します。	▪ user <loginname> – ユーザのログイン名 ▪ index <index> – SSH キーのインデックスを見ます。
deletesshkey	特定のユーザの SSH キーを消去します。	▪ user <loginname> – ユーザのログイン名 ▪ index <index> – SSH キーインデックスを消去します。

コマンド	記述	パラメータ
edituser	特定のユーザの情報を更新します。	▪ Addgroup のパラメータを参照してください。
deleteuser	特定のユーザを削除します。	▪ user <loginname> - 削除するユーザ
showuser	既存のあるユーザの詳細を表示します。	▪ user <loginname> - 表示するユーザ
insertgroupacl	グループの ACL ルールを挿入します。	NA
replacegroupacl	グループの ACL ルールを置き換えます。	NA
deletegroupad	グループの ACL ルールを削除します。	NA
showgroupacl	グループの ACL ルールを表示します。	NA

CLI を用いてのユーザ権限設定と認証サービスの設定

注:この機能はリモート コンソールからも実行できます。参照 **リモート コンソールからユーザ認証を設定する。** *『93p. 』。*

SX II は装置にアクセスするためにユーザーに認証を求めます。

認証とは、ユーザが本人であることを確認するプロセスです。ユーザが認証されると、ユーザの属するグループに基づいて、システムおよびポートに対する許可が決定されます。ユーザに割り当てられた特権により、どのようなタイプのアクセスが許可されるかが決まります。これを「認可」と呼びます。

ユーザーは SX II のローカルであるいはリモートで認証を受けることができます。

デフォルトでは、ユーザーはローカルで認証を受けます。リモート認証はそれを有効化しなければなりません。

SX II がリモート認証用に構成されている場合、外部認証サーバは主に認証を目的として使用され、認可用には使用されません。

SX II はリモート認証のユーザーのために数種類のオプションを提供しています。

- LDAP/LDAPS
- RADIUS
- TACACS+

次を選択します `admin > Config > Authentication` これでメニューにアクセスします。

認証方法

コマンド	記述	パラメータ
`authmode`	認証の方法を設定します。	▪ mode <local|ldap|radius|tacacs>

LDAP の設定

この LDAP 設定メニューは LDAP と LDAPS をセットするコマンドを提供します。

次を選択します `admin > Config > Authentication > ldap` これでメニューにアクセスします。

コマンド	記述	パラメータ
ldap	セキュアーな LDAP 認証モードの設定	▪ primip <ipaddress | hostname> – 第 1 のサーバの IP アドレス ▪ secip <ipaddress | hostname> – 第 2 のサーバの IP アドレス ▪ port <value> – LDAP ポート ▪ basedn <Base DN> – Admin ユーザの DN ▪ secret <value> –Admin ユーザの認証シークレット キー ▪ search <value> – ユーザ サーチ DN ▪ dialback <value> – ダイアルバック サーチの問い合わせ ▪ domain <Active Directory Domain> – アクティブなディレクトリーのドメイン ▪ referral <true | false> – LDAP サーチの照会 ▪ server <generic | ads> – サーバのタイプ、アクティブなディレクトリーあるいは一般
ldaps	セキュアーな LDAP 認証モードの設定あるいは獲得	▪ port <value> – セキュアーな LDAP ポート ▪ enable <true | false> – セキュアーな LDAP 有効化 (true), 無効化 (false) ▪ verify <true | false> – LDAPS 認証の検証 有効化 (true), 無効化 (false)
ldapscert	LDAPS 認証の検索	▪ address <ipaddress | hostname> – FTP サーバのアドレス ▪ port <FTP port>– FTP サーバのポート(デフォルトは 21) ▪ path <path to file> – FTP 認証へのパス ▪ user <FTP username> – FTP のユーザ名 ▪ password <FTP password> – FTP パスワード (抜けているときに問われます)
testldap	LDAP 設定をテストするのに使用されます。	▪ login <LDAP user> – テストのための LDAP ログイン ▪ password <LDAP users password>

RADIUS の設定

RADIUS メニューは RADIUS サーバへのアクセスを設定するのに用いるコマンドへのアクセスを提供します。

辞書ファイルは次のロケーションで作成される必要があります。

```
/user/share/freeradius/
```

```
# -*-text ト-*-
#
# dictionary.raritan
#
# Version:  $Id$
#
VENDOR            Raritan                         8267
#
#     St と ard attribute
#
BEGIN-VENDOR      Raritan
ATTRIBUTE   Raritan-Vendor-Specific             26    string
END-VENDOR  Raritan
```

RADIUS ユーザをそのユーザ ファイルでの新しい属性を使うように更新します、 そのファイルは通常 /etc/raddb/ にあります。

```
Raritan-Vendor-Specific = "G{Administrator}"
```

注:フィルター ID とベンダーに特有の属性が存在すると、そのベンダー特有の属性が使用されます。

次を選択します admin > Config > Authentication > RADIUS これでメニューにアクセスします。

コマンド	記述	パラメータ
primaryradius	第1の RDIUS の設定を形成します。	▪ ip <ipaddress | hostname> – IP アドレス ▪ secret <value> – RADIUS 認証用秘密キー ▪ authport <value> – RADIUS 認証ポート ▪ acctport <value> – RADIUS アカウントのポート ▪ timeout <value> – RADIUS のタイムアウト(秒の単位で) ▪ retries <value> – RADIUS 再試行 ▪ chap <true | false> – CHAP 有効化/無効化(true/false)
secondaryradius	第2の RDIUS の設定を形成します。	▪ ip <ipaddress | hostname> – IP アドレス ▪ secret <value> – RADIUS 認証用シークレットキー ▪ authport <value> – RADIUS 認証ポート ▪ acctport <value> – RADIUS アカウントのポート ▪ timeout <value> – RADIUS のタイムアウト(秒の単位で) ▪ retries <value> – RADIUS 再試行 ▪ chap <true | false> – CHAP 有効化 (true), 無効化 (false)

TACACS+ の設定

TACACS+ メニューは TACACS+ へのアクセスを設定するのに用いるコマンドを提供します。

次を選択します admin > Config > Authentication > TACACS+ これでメニューにアクセスします。

コマンド	記述	パラメータ
primarytacacs	第1の TACACS+ の設定を形成するのに使用します。	▪ ip <ipaddress | hostname> – IP Address ▪ secret <value> – RADIUS 認証用シークレットキー ▪ port <value> – TACACS+ ポート ▪ timeout <value> – TACACS+ のタイムアウト (秒の単位で) ▪ 再試行<value> – TACACS+再試行
secondarytacacs	第2の TACACS+ の設定を形成	▪ ip <ipaddress | hostname> – IP Address

コマンド	記述	パラメータ
	するのに使用します。	▪ secret <value> – RADIUS 認証用秘密キー ▪ port <value> – TACACS+ ポート ▪ timeout <value> – TACACS+ のタイムアウト（秒の単位で） ▪ 再試行<value> – TACACS+再試行

CLI を用いたモデムの設定

注:モデムはリモートコンソール からも設定できます。参照 **『リモートコンソールから日付と時刻の設定をする』** *『124p. の"リモート コンソールから日付と時刻の設定をする"参照 』。このリモート コンソールの主題でさらに詳細が提供されます。*

次を選択します admin > Config > Modem これでメニューにアクセスします。

コマンド	記述	パラメータ
dialback –	ダイアルバックを有効化します。	▪ enable <true | false> – ダイアルバックのします 有効化（true)、 無効化（false)。
dialin	ダイアルインの設定を形成します。	▪ enable <true | false> – モデムを有効化/無効化します：有効化（true)，無効化（false) ▪ mode <All/PPP_Only/Console_Only> モデムのアクセスモード ▪ serverip PPP <IPv4 address> – PPP サーバの IP アドレス ▪ clientip PPP <IPv4 address> – PPP クライアントの IP アドレス
bmodem	ブロードバンドモデムの有効化/無効化	▪ enable <true | false> – ブロードバンドモデムを有効化/無効化します：有効化（true)，無効化（false)

ユーザグループにモデム アクセス許可を割り当てる

必要があれば、モデムアクセスの許可を持つグループにユーザを割り当てます。

グループのページでモデムアクセスの許可をユーザグループに割り当て、それからユーザのページでユーザをそのグループに割り当てます。

詳細については、以下を参照してください。 *『CLI を用いてユーザとユーザグループを設定・管理する』* 『202p. の*"CLI を用いてユーザとユーザグループを設定・管理する"*参照 』 または *『リモート コンソールからユーザとグループを設定・管理する』* 『78p. の*"リモート コンソールからユーザとグループを設定・管理する"*参照 』。

モデムをサポートするためのサーバの設定

第 1 の（あるいはまた第 2 の） RADIUS サーバの設定は正しく形成され SX II 上で有効化される必要があります。

- リモートの RADIUS サーバでは、ユーザの設定は以下を含んでいるべきです。

```
Filter-Id = "raritan:G{<local user group>}:D{<number for dialback>}"
```

  LDAP サーバのユーザ設定は属性にダイアルバック番号を含んでいるべきで、それは SX II 上で[Dialback search string] として設定されます。

  リモート LDAP ユーザのダイアルバック(OpenLdapv.2&v.3)

- リモート TACACS+ ユーザのダイアルバック(TACACS++v4.0.3a)

  ダイアルインとダイアルバックはモデム通信のために使用するため SX II で有効化されているべきです。第 1 の（あるいはまた第 2 の） TACACS+ サーバの設定は正しく形成され SX II 上で有効化される必要があります。

  TACACS+サーバのユーザ設定には次の行があるべきです

```
user-dialback='129'
```

CLI を用いての自動設定スクリプトの実行

注:これらの機能はリモートコンソール からも設定できます。参照 **『リモート コンソールからの自動スクリプト設定』** *『110p. の"*リモート コンソールから TFTP あるいは USB スティックを使用するためのオートスクリプトを有効化する*"参照 』。*

次を選択します [admin] > [config] これでメニューにアクセスします。

コマンド	記述	パラメータ
autoconfig	自動設定スクリプトの設定と獲得	▪ enable <true | false> – 有効化 (true), 無効化 (false) ▪ run <once/every> – スクリプトをを一度あるいはブートごとに実行 ▪ source <manual/dhcp> – DHCP あるいは自動セットで提供されるウ TFTP アドレスの使用 ▪ tftp address <ipaddress | hostname> – TFTP サーバのアドレス
autoconfig	USB 設定経由で自動スクリプトのセット/獲得	▪ enable <true | false> – 有効化 (true), 無効化 (false)

次を選択します [admin] > これでメニューにアクセスします。

コマンド	記述	パラメータ
scriptget	リモート設定スクリプトを検索する	▪ address <ipaddress | hostname> – FTP サーバのアドレス ▪ port <FTP port>– FTP サーバのポート(1 ~ 65535) ▪ path <path to file> – 設定ファイルのための FTP サーバのパス。例えば /ftphome/config.txt ▪ user <FTP username> – オプション FTP サーバのユーザ名 ▪ password <FTP password> – オプションの FTP サーバのパスワード.欠けていてユーザ名が与えられていると求められます。
scriptrun	自動設定スクリプトの実行	NA

CLI を用いたネットワーク設定の形成

注:この機能は SX II のリモートコンソール からも設定できます。参照『SX II のネットワーク設定をリモート コンソールから設定する』。

この ネットワーク メニュー コマンドは SX II のネットワーク設定をセットするのを可能にします。

次のように入力します [admin] > [config] > [network] これでメニューにアクセスします。

コマンド	記述	パラメータ
dns	ネットワークの DNS のパラメータを得て設定します。	▪ mode 〈auto/manual〉 – DNS サーバの IP モード ▪ primary 〈ipaddress〉 – 第 1 の DNS サーバの IP アドレス ▪ secondary 〈ipaddress〉 – 第 2 の DNS サーバの IP アドレス
ethernetfailover	一つの LAN から他方の LAN に障害復旧するのを有効化/無効化するのに用います。	▪ enable 〈true/false〉 – イーサネットの障害復旧： 有効化（true），無効化（false）
interface	2 重 LAN 障害復旧のためのネットワーク設定 デフォルトでは、2 重 LAN 障害復旧モードは無効化されています。	▪ ipauto 〈none | dhcp〉 – ip 設定として DHCP を有効化 ▪ 〈lan1 | lan2〉 – 設定している LAN インタフェースを選択します。 ▪ ip 〈IPv4 address〉 – IP ネットワークからのアクセスのために割り当てられた SX II の IP アドレス ▪ mask 〈subnetmask〉 – IP 管理者から得られたサブネットのマスク ▪ gw ipaddress 〈IPv4 address〉 – IP 管理者から得られたゲートウエイの IP アドレス ▪ mode 〈auto | 10hdx | 10fdx | 100hdx | 100fdx | 1000fdx〉 – イーサネットのモードを自動検出するかあるいは特定のモードに強制します。 ▪ rate 〈none | 100mb | 10mb | 5mb | 2mb | 512kb | 256kb | 128kb〉 – インタフェースのバンド幅の制限をセットします。
IPv6_interface	IPv6 ネットワーク パラメータをセットした既存の IPv6 パラメータを検索します。	▪ ipauto 〈none | routerdisc〉 – IPV6 の自動設定を有効化します。 ▪ if 〈lan1 | lan2〉 – 設定している LAN インタフェースを選択します。 ▪ ip ipaddress 〈ipaddress〉 – IP ネットワークからのアクセスのために割り当てられた SX II の Ipv6 アドレス ▪ prefixlen 〈prefix length〉 – IPV6 アドレスの接頭辞の長さ（接頭辞にあるビット数 – 0–128 (十進数)の範囲)。 ▪ gw ipaddress 〈IPv6 address〉 – IP 管理者から得られたゲートウエイの IP アドレス ▪ mode 〈enable or disable〉 – IPV6 ネットワークの動作モード，有効化（true），無効化（false）

コマンド	記述	パラメータ
name	SX II 装置の名前	▪ devicename <value> – SX II につけられた名前 ▪ hostname <value> – 好ましいホストの名前（DHCP のみ）
staticroute	静的ルートの設定。	▪ enable <true | false> – 有効化（true），無効化（false）
staticrouteadd	静的ルートを追加します。	▪ dest <dest> – 送信先 ▪ if <lan1 | lan2> – インタフェース（lan1/lan2） ▪ prefix <prefix> – IPv6 接頭辞の長さ ▪ mask <mask> – IPv4 マスク ▪ gateway <gateway> – ゲートウエイ ▪ mtu <mtu> – MTU (64 ~ 65536) ▪ flags <host|net> – フラグ（ホスト/ネット）
staticrouteshow	静的ルートのリストを見る	NA
staticroutedelete	あるルートをカーネルルーティング テーブルから削除します。	▪ id <id> – id 番号あるいはすべて

CLI を用いたデバイス設定

注:これらの機能はリモートコンソール からも設定できます。参照 **『リモート コンソールからデバイス設定をセットする』** *『115p. の"リモート コンソールからデバイス設定をセットする"参照 』。*

これらのコマンドは SX II サーバのサービスを設定する能力を提供します。

次のように入力します [admin] > [config] > [services] これでメニューにアクセスします。

コマンド	説明	パラメータ
discovery	検出ポートを設定します。	▪ port <value> – 検出用 TCP 読み取りポート
http	Http アドレスを制御しポートを定義するのに使います。	▪ port <value> – HTTP サーバのデフォルトの読み取りポート(tcp)
https	Https アクセスを制御しポートを定義するのに使います。	▪ port <value> – HTTPS サーバのデフォルトの読み取りポート(tcp)

コマンド	説明	パラメータ
ssh	SSH アクセスの有効化あるいは無効化	▪ enable <true | false> – SSH アクセスの有効化あるいは無効化：有効化（true)、 無効化（false) ▪ port <value> – SSH サーバの TCP 読み取りポート
telnet	Telnet アクセスの有効化あるいは無効化 Telnet はセキュリティが低く、ユーザ名、パスワード、およびすべてのトラフィックが平文で送信されます。 Telnet は使用される前に有効化される必要があります。通常無効化されています。 デフォルトで、telnet のポートは 23 にセットされていますが、次のコマンドを発して変更することができます。	▪ enable <true | false> – Telnet アクセスの有効化あるいは無効化：有効化（true)、無効化（false) ▪ port <value> – Telnet サーバの TCP 読み取りポート

CLI を用いて ダイレクト ポート アクセス を設定する

許可されている TCP ポートの範囲は 1024–64510 です。モード パラメータなしで実行すると、システムは現在の dpa タイプを表示します。

次のように入力します admin > Config > Services > これでこのメニューにアクセスします。

コマンド	説明	パラメータ
dpa	ダイレクト ポート アクセスの有効化	▪ enable <true | false> – DPA アクセスの有効化あるいは無効化：有効化（true)、無効化（false) ▪ url <true | false> – URL 経由の DPA： 有効化（true)、無効化（false) ▪ loginstring <true | false> – ログインした時ユーザ名で DPA ポートの指定を可能にします：有効化（true)、無効化（false)

コマンド	説明	パラメータ
dpaport	IP/SSH/telnet DPA のポートを指定したシリアルポートに設定します。	▪ port <number | range | *> -見る/変更のためのポート（これは 1 つのポートあるいはある範囲のポート（ 1-n あるいは 1,3,4 あるいは全てのポートには * ）） ▪ dpaip <ipaddress> - 直接ポートアクセスのために割り当てられた IP アドレス 0.0.0.0 は設定を消去します。 ▪ telnet <port number> - Telnet 経由で直接ポートにアクセスするために指定した TCP ポート。0 は設定を消去します。 ▪ ssh <port number> - SSH 経由で直接ポートにアクセスするために指定した TCP ポート。0 は設定を消去します。

無記名接続

Telnet 経由で無記名の ダイレクト ポート アクセス 接続を確立することができます - そのためには anonymous とタイプするか、あるいはユーザ名の入力要求に対して Enter を押します。無記名の条件はパスワードの入力要請無しで確立されます。

SSH 経由で ダイレクト ポート アクセス 接続を確立するときには、ユーザ名 anonymous を入力します。必ず実行してください。ユーザ名が入力されると パスワード の入力要請が表示されます。Enter を押します。

無記名 ダイレクト ポート アクセス で SX II が始めてアクセスされときに消去パラメータを用いて以降のメッセージを表示するかしないかを設定します。

エスケープ シーケンスは：<escape string> <true¥false>

″You have read-only access to this port.″あるいは ″You are now master for the port.″

消去機能が真の場合、上記のメッセージは表示されず、直接ターゲットの入力待ちに接続されます。

消去機能が偽の場合、上記メッセージが表示されます。

CLI を用いて SNMP のトラップと警告を設定する

注:SNMP トラップはリモートコンソール からも設定できます。参照 **『リモート コンソールから SNMP トラップを設定する』** *『128p. の"***リモート コンソールから SNMP トラップを設定する***"参照 』*。

SX II は SNMP 警告を希望する SNMP サーバに送るのをサポートします。Raritan SNMP MIB は次に見つけられます ***『SX II MIB を見る』***『132p. の*"Viewing the SX II MIB"*参照 』。

次のように入力します `[admin] > [config]` これでメニューにアクセスします。

コマンド	説明	パラメータ
`add`	トラップ受信者を追加します。 受信者は IP アドレスでオプションでスペースで分離したポート番号が付きます。 トラップは同じ IP アドレスの複数のポートに送られます。	▪ dest <ipaddress | hostname> – 送信先の IP/ホスト名 ▪ port <port number> – 送信先のポート ▪ community <community> – SNMP コミュニティ
`addv3`	トラップ受信者を追加します。 受信者は IP アドレスでオプションでスペースで分離したポート番号が付きます。 トラップは同じ IP アドレスの複数のポートに送られます。	▪ dest <ipaddress | hostname> – 送信先の IP/ホスト名 ▪ port <port number> – 送信先のポート ▪ name <name> – セキュリティ 名前 ▪ authproto <MD5 | SHA> – SNMP 認証のプロトコル ▪ authpass <authpass> – SNMP 認証のパスフレーズ ▪ privproto <None | DES | AES> – SNMP プライバシー プロトコル ▪ privpass <privacy password> – SNMP プライバシーのパスフレーズ
`viewtraps`	既存の SNMP トラップを標示します	NA
`del`	SNMP トラップを削除します。	▪ dest <ipaddress | hostname>– 送信先の IP/ホスト名 ▪ port <port number> – 送信先のポート
`delv3`	SNMPv3 トラップを削除します。	▪ dest <ipaddress | hostname>– 送信先の IP/ホスト名 ▪ port <port number> – 送信先のポート

コマンド	説明	パラメータ
snmpagent	SNMP デーモンを設定します。	▪ enable <true | false> – SNMP デーモンの有効化（true），無効化（false） ▪ contact Contact Sunbird Raritan Professional Services and Support via the Support site at http://support.sunbirddcim.com or via email (tech@sunbirddcim.com) – SNMP コンタクト ▪ location <location> – SNMP location ▪ community <community> – SNMP コミュニティ ▪ type <read_only | read_write> – SNMP コミュニティタイプ ▪ v12enable <true | false> – SNMP v1/2 エージェント：有効化（true)、無効化（false）
snmptrap	SNMP の有効化あるいは無効化	▪ enable <true | false> – SNMP トラップ： 有効化（true)、無効化（false） ▪ v12enable <true | false> – SNMP v1/v2c トラップ： 有効化（true)、無効化（false） ▪ v3enable <true | false> – SNMP v3 トラップ：有効化（true)、無効化（false）
snmpv3agent	SNMPv3 エージェントの設定	▪ enable <true | false> – SNMP v3 トラップ：有効化（true)、無効化（false） ▪ name <security name> – セキュリティ名 ▪ authproto <MD5 | SHA> – SNMP 認証のプロトコル ▪ authpass <auth password> – SNMP 認証のパスフレーズ ▪ privproto <None | DES | AES> – SNMP プライバシープロトコル ▪ privpass <privacy password> – SNMP プライバシーのパスフレーズ ▪ useauthforpriv <true | false> – プライバシーの認証パスフレーズの使用： 有効化（true)、無効化（false）

CLI を用いて日付と時刻の設定をする

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールから日付と時刻の設定をする』** *『124p. の"リモートコンソールから日付と時刻の設定をする"参照 』*

次のように入力します admin > config > time これでメニューにアクセスします。

コマンド	説明	パラメータ
クロック	日付と時刻を正しく設定することはログ入力とイベントが正しいタイムスタンプを含むために重要です。 これをサーバ上の日付と時刻をセットするのに用います。	▪ tz timezone – タイムゾーンインデックスは希望するタイムゾーンに対応する番号です ▪ dst <true | false> – DST 設定を適用します：有効化(true)、無効化（false）
timezonelist	タイムゾーンに対応するコード番号を見つけるのに用います。	NA
ntp	NTP サーバと SX II を同期するにはこのコマンドを使います。	▪ enable <true | false> – NTP の使用を有効化/無効化します：有効化（true)，無効化（false） ▪ primip <primaryIP> – 第 1 サーバを最初に使います。 ▪ secip <secondaryip> – 第 1 が利用できない場合第 2 の NTP サーバを使います。 ▪ enable <true | false> – NTP を有効化/無効化します：有効化（true)，無効化（false） ▪ override <true/false> – NTP サーバに対して DHCP の設定を上書きします（true/false）

CLI を用いてデフォルトの GUI 言語設定を変更する

注:この設定はリモート コンソールからも設定することができます。参照 **『リモートコンソールからデフォルトの GUI 言語設定を変更する』** *『149p. の"リモートコンソールからデフォルトの GUI 言語設定を変更する"参照 』。*

次のように入力します admin > [config] > [language] これでメニューにアクセスします。

コマンド	説明	パラメータ
language	言語の設定はリモートコントロールのウエブインタフェースだけに適用され、ローカルのコンソールのインタフェースには適用されません。 SX II の GUI は、デフォルトでは英語に設定されていますが、以下のローカライズ言語がサポートされています。 • 英語（デフォルト） • 日本語 • 簡体字中国語 ▪ 繁体字中国語	▪ set <en | ja | zhs | zht> – GUI 言語コード

CLI を用いた SMTP のイベントと通告の設定

注:この設定はリモート コンソールからも設定することができます。参照 **『リモート コンソールから SNMP 通知を有効にする』** *『133p. の"リモート コンソールから SNMP 通知を有効にする"参照 』。*

次のように入力します log > smtp SMTP サーバと宛先の e メールアドレスを設定するのに使うことのできるオプションにアクセスするためのメニューです。

次のように入力します admin configure > log > smtp これでメニューにアクセスします。

コマンド	説明	パラメータ
smtp	SMTP サーバの設定	▪ enable <true | false> – SMTP サーバの有効化（true)、無効化（false) ▪ ip <ipaddress | hostname> – SMTP サーバの IP アドレス ▪ port <port number> – SMTP サーバ ポート（1 ~ 65535) ▪ auth <true | false> – SMTP 認証要求： 有効化（true)、無効化（false) ▪ user <username> – SMTP ユーザ アカウント ▪ pass <password> –SMTP ユーザ パスワード ▪ source <source> – SMTP ソース アドレス

コマンド	説明	パラメータ
addemailsub	メールの読者を追加する最大 10 人のユーザを追加できます。	▪ email <email> – 追加する E メールアドレス
delemailsub	E メール読者を削除します。	▪ email <email> – 削除する E メールアドレス
testsmtp	E メール通知テストの設定	▪ dest <destination email> – 送信先 e メールアドレス
viewemailsub	E メール読者のリストを見る	NA

CLI を用いてポートログの設定を形成する

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールからポートのログを設定する』** *『149p. の"リモートコンソールからポートのログを設定する"参照 』。*

セキュリティ能力の一部として、SX II はデータをログし、ユーザ、SX II とターゲットデバイスとの間の活動に基づいて警告を与えます。

監査用軌跡がこの機能の部分として収集され、捜査担当がシステムに何が起こり、誰がどの行動をいつ行ったのかを調査するのを可能にします。、

イベントのログと SNMP トラップもまた利用可能です。イベントは Syslog を用いてローカルにログされます。ローカルなイベントはポートあたり 512K のバッファーに保管されそして保存、調査、消去あるいは FTP サーバに周期的に送られます。

ログコマンドの設定は SX II サーバのログ機能を管理することを可能とします。

次のように入力します admin > Config > Log これでメニューにアクセスします。

コマンド	説明	パラメータ
eventlogfile	このコマンドを使ってイベントをローカルなログにロギングする野を制御し設定します。	▪ eventlogfile enable<true | false> – システムイベントのログ ▪ size <value> – ローカルなログファイルの最大サイズ（バイトで） エベントログファイルのサイズが SX II モデルの利用できるフラッシュメモリの容量を越えると、イベントは保存されません。 この事態を避けるため、Raritan はファイルサイズを 1024 より大きくしかし 1 千万より小さくセットすることを勧めます。 *注:各 SX II は異なった量の利用可能フラッシュメモリ*

コマンド	説明	パラメータ
		を持っています。 ▪ style <wrap or flat> – 最大サイズに達した時に取る行動が何かを指定します。 wrap はログが最後に達すると廻りこみます。 flat は最後に達するとログを停止させます。
eventdest	ユーザの構成設定	▪ event <index of event> – イベント インデックス、インデックスを知り現在の設定を見るには [eventlist] を使います。 ▪ audit <true | false> – ログの監査： 有効化 (true)、無効化 (false) ▪ snmp <true | false> – SNMP のログ： 有効化 (true)、無効化 (false) ▪ syslog <true | false> – syslog のログ: 有効化 (true)、無効化 (false) ▪ smtp <true | false> – SMTP のログ、 有効化 (true)、無効化 (false)
eventlist	全ての設定できるインデックスのリスト	NA
syslog	Syslog サーバの設定	▪ enable <true | false> – システムイベントのログを記録する：有効化 (true)、無効化 (false) ▪ ip <ip address> – syslog サーバのアドレス
portsyslog	ポートの Syslog サーバの設定	▪ enable <true | false> – リモート NFS サーバおよび Syslog サーバへのポートロギングデータ：有効化 (true)、無効化 (false) ▪ primaryip <primaryip> – 第 1 のポートログの Syslog サーバのアドレス ▪ primaryip <primaryip> – 第 1 のポートログの Syslog サーバのアドレス

コマンド	説明	パラメータ
nfsportlog	ポートデータのログを設定します。	▪ enable <true|false> – リモート NFS サーバへのポートのデータのログ：有効化（true)、無効化（false) ▪ primaryip <primaryip> – 第 1 のポートログの Syslog サーバ ▪ secondaryip <secondip> – 第 2 のポートログの Syslog サーバ ▪ primarydir <mountpath – 第 1 NFS サーバのマウントディレクトリー例えば /nfslog ▪ secondarydir <mountpath> – 第 2 NFS サーバのマウント ディレクトリー例えば /nfslog ▪ prefix <name> – ファイル名の接頭辞 ▪ size <value> – ログファイルの最大サイズ（バイトで) ▪ inputlogging <true|false> – ポート上のユーザ入力データのログ：有効化（true)、無効化（false)ユーザのキーボードからの入力の参照です ▪ indir <name> – 入力ログを保存するためのディレクトリーの名前 ▪ outdir <name> – 出力ログを保存するためのディレクトリーの名前出力とはターゲットから SX ポートに送られるデートのことです。 ▪ block <true|false> – NFS が失敗したときにポートのアクセスを閉じます。
nfsencrypt	ポートのログを暗号化するために用いる暗号化キーをセットします。	▪ enable <true | false> – SMTP サーバの有効化（true), 無効化（false) ▪ key <string> – 暗号化のために使用する RC4 キー文字列を提供します。
portlogtime	NFS サーバのポートログ時間を設定するのに用います。	▪ timestamp – ログファイルの 2 つのタイムスタンプの間の間隔（秒で）値を 0 とするとタイムスタンプのログを無効にします。デフォルトは 20 秒です。最大値は 99999 です。 ▪ update <update> – リモートログファイルへの 2 つの更新の間の時間間隔（秒で）最大値は 99999 です。

次のように入力します admin > config > log > local これでメニューにアクセスします。

コマンド	説明	パラメータ
serialportlog	シリアル ポートのログファ	▪ size <value> – ファイルの最大サイズ（バイ

コマンド	説明	パラメータ
	イルを設定します。	トで) ▪ update <value> – 更新頻度（秒） ▪ port <name> – 変更するポート ▪ enable <true | false> – シリアル ポートのログファイル：有効化（true），無効化（false）
serialportlogdel	シリアル ポートのログファイルを削除します。	▪ port <number> – ログを削除するポート
serialportlogview	シリアル ポートのログファイルを見ます。	▪ port <number> – 変更するポート

Linux ベースの NFS サーバで暗号化されたログを復号する

Linux®のプラットフォームで nfs の暗号化を復号するには、次の手順に従います：

1. 現在の nfs 暗号化のキーを検索します

```
[admin] > [Config] > [Log] > [nfsencrypt]
```

2. キーのところにプリントされたキーを切り取り貼り付けで、コマンドの応答のファイルの中に入れます。
3. 復号ソフトを検索し、それを Linux マシンに置くか、あるいはそのソースをコンパイルします。
4. 暗号化キーファイル（dsx-encrypt.key）を復号化ソフトの保存されている同じディレクトリーに保存します。
5. 暗号化されたポートログファイルを同じディレクトリーにコピーします。
6. 次のコマンドで復号化します：

```
./decrypt -f <portlogfile> -e <keyfilename> -o  <outputfile>
```

7. 復号かされたファイルは次に保存されるはずです： <outputfile>。

CLI を用いてポートを設定する

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールからのポートの設定』** *『155p. の"*リモート コンソールからのポートの設定*"参照 』*。

次のように入力します admin > これでメニューにアクセスします。

コマンド	説明	パラメータ
listports	アクセス可能なポートを一覧表示します。	NA

次のように入力します admin > config > port これでメニューにアクセスします。

コマンド	説明	パラメータ
keywordlist	設定されたキーワードを表示します。	NA
keywordadd	キーワードをポートに追加します。	▪ port <number | range | *> –単一のあるいは範囲のポート(これは 1 つのポートあるいはある範囲のポート (1-n あるいは 1,3,4 あるいは全てのポートには *)) ▪ keyword <value> – キーワードがターゲットに検出されると、通知が送られます。
keyworddelete	ポートから既存のキーワードを削除します。	▪ port <number | range | *> – 単一のあるいは範囲のポート (1-n あるいは 1,3,4 あるいは全てのポートには *) ▪ keyword <value> – キーワードがターゲットに検出されると、通知が送られます。
config port		▪ port <number | range | *> – 単一のあるいは範囲のポート (1-n あるいは 1,3,4 あるいは全てのポートには *) ▪ name <port name> – ポートの名前 ▪ bps <1200 | 1800 | 2400 | 4800 | 9600 | 19200 | 28800 | 38400 | 57600 | 115200 | 230400> – ポートの速度を秒あたりビットで ▪ parity <none|even|odd> – ポートのパリティのタイプ ▪ flowcontrol <none|hw|sw> – ポートのフロー制御のタイプ hw = ハードウエアフロー制御 sw =X on/X off) ▪ eqtype <auto|dte|dce> – 装置のタイプ (auto=>自動検出, dte=>強制 DTE, dce=>強制 DCE) ▪ 注:ターゲットが DTE か DCE のいずれかを自動検出する能力を持っていると、そのポートに強制 DTE あるいは強制 DCE のいずれかを選ぶことが必要となります。SX II は同一ポートに DCE と DTE の両方を自動検出することをサポートしていません。

コマンド	説明	パラメータ
		▪ escapemode <none|control> – escape シーケンスとして Ctrl-key を使用 (escapemode=control) あるいは単一キー (escapemode=none); 例えば、Ctrl- => escapemode=control, escapechar= escapechar char-Escape character ▪ Raritan では使用しないまたエスケープコマンドとして Ctrl- を使用しないことを勧めます。これらのいずれかは、例えばメニューを開くというような意図しないコマンドを引き起こすかもしれません。 ▪ emulation <vt100 | vt220 | vt320 | ansi> – ターゲットのエミュレーションタイプ ▪ sendbreak <duration> – 送り戻し信号までの遅延時間をミリ秒で ▪ exitstring <cmd #delay; > – ポートセッションが閉じたときに実行する終了文字列、例えば config port 1 exitstring logout (終了でログアウトする) config port 1 exitstring #0 (そのポートの修了文字列を無効にする)。delay (遅延) はターゲットへのコマンドを書いた後の待ち時間の量 です。秒単位で最大 60 です。 ▪ dpaip <ipaddress> – 直接ポートアクセスのために割り当てられた IP アドレス ▪ ssh <port number> – SSH 経由で直接ポートにアクセスするために指定した TCP ポート。 ▪ alwaysactive <true | false> – ポートに到来するデータをログするかどうかを決定します、ポート 1 を alwaysactive true (接続しているユーザが居ない場合にポートに到来する活動を常にログする)、 config port 1 alwaysactive false (接続しているユーザが居ない場合にポートに到来するデータを無視する) ▪ suppress – DPA 接続の間、「Authentication successful』と言ったメッセージを全く表示しないか全て表示するかを決めます。 ▪ encoding – ターゲットのエンコーディングのタイプ (DEFAULT|US-ASCII|ISO-8859-1|ISO-8859-

コマンド	説明	パラメータ
		15|UTF-8|Shift-JIS|EUC-JP|EUC-CN|EUC-KR) ▪ multiwrite – 複数書き込み者でのポートの設定 ▪ chardelay delay – 書き込み文字の間に挿入される遅延時間 (0-9999ms) ▪ linedelay delay – 書き込み行の間に挿入される遅延時間 (0-9999ms) ▪ stopbits – 文字の終わりを知らせるために使われるビットの数 (通常 1) (1/2) ▪ telnet <port number> – Telnet 経由で直接ポートにアクセスするために指定した TCP ポート。0 は設定を消去します。(TCP/UDP ポート) (0 ~ 65535) ▪ ssh – SSH 経由で直接ポートにアクセスするために指定した TCP ポート。0 は設定を消去します。(TCP/UDP ポート) (0 ~ 65535) ▪ stopbits <1/2> – 文字の終わりを知らせるために使われるビットの数 ▪ chardelay – 文字の間に挿入される遅延時間 (0-9999) ミリ秒で ▪ linedelay – 行の間に挿入される遅延時間 (0-9999) ミリ秒で ▪ escapechar – エスケープ文字 ▪ encoding – (DEFAULT|US-ASCII|ISO-8859-1|ISO-8859-15|UTF-8|Shift-JIS|EUC-JP|EUC-CN|EUC-KR) – ターゲットのエンコーディングのタイプ ▪ telnet – Telnet 経由での DPA のために指定した TCP ポート(1 ~ 65535)。 ▪ multiwrite <true/false> – 複数書き込み者でのポートの設定 ▪ suppress <true/false> – このターゲットへ接続する SX メッセージを消去する (true/false) ▪ sendbreak – 送り戻し信号までの遅延時間をミリ秒で

DPA モードの Portconfig コマンドの例

以下は ダイレクト ポート アクセスを設定する例です。以下のポートコマンドは DPA 自身と同じではない DPA アクセスのための IP アドレスを URL でセットします。この DPA IP アドレスはポートに直接行くためのアドレスです。

```
[admin] > [Config] > [port] > [config port 1] dpaip 10.0.13.1
[admin] > [Config] > [Services] > [dpa enable true]
```

- dpa enable true - これはポートを設定するために IP とポートの DPA 方法を有効化します。

パスワードを入力した後、ポート 1 のために新しく特定して割り当てられた IP を用いてポート 1 に直接のアクセスを持ちます。

```
admin@10.0.13.1 のパスワード:
 エスケープ シーケンスは : Control-
これであなたはそのポートのマスターです。
```

次はある範囲のポートに対する DPAIP に DPA ポート設定を行う例です。

```
admin > Config > Port > config port 1-32 dpaip 10.0.13.200
```

または

```
admin > Config > Port > config port * dpaip 10.0.13.200
```

上記のどちらの場合も、ポート 1 は 10.0.13.200 と割り当てられた IP を持ち、ポート 2 は 10.0.13.201、ポート 3 は 10.0.13.203 などとなります。

次は TCP ポートによって SSH と Telnet に DPA ポート設定を行う例です。

```
admin > Config > Port > config port 1 ssh 7000 telnet 8000
```

DPA Telnet と SSH ポートの変更は再起動なしで直ちに有効となります。

```
ssh -l sx_user -p 7000 10.0.13.13 or telnet -l sx_user 10.0.13.13
8000
admin@10.0.13.13 のパスワード:
エスケープ シーケンスは : Control-


これであなたはそのポートのマスターです。
```

パスワードを入力した後、ポート 1 のために新しく特定して割り当てられた TCP ポート(ssh か telnet) を用いてポート 1 に直接のアクセスを持ちます。

次は一群のポートに DPA ポートの設定を行う例です（どのポートもまだ割り当てられておらず、自由な範囲の TCP ポートが dpa TCP ポートモードに使用できることを確認した下さい）。

```
admin > Config > Port > config port 1-32 ssh 7000 telnet 8000
```

または

```
admin > Config > Port > config port * ssh 7000 telnet 8000
```

上記のどちらの場合も、ポート 1 は ssh ポート 7000、telnet 8000 が直接ポートアクセスに割り当てられ、ポート 2 は ssh ポート 7001 と telnet ポート 8001、などとなります。

全てのポートを一連の連続したポート番号で設定するには、〈port *〉コマンドを用います。ポートの範囲が指定されると、連続したポート番号が使用されます。base_tcpport で与えられる値はスタートの値として使われます。個別のポートの設定には、〈port number〉コマンドが使われます。

CLI を用いたローカルなポートの設定

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールからローカルなポート設定を行う』** *『147p. の"リモート コンソールからローカルなポート設定を行う"参照 』。*

次のように入力します admin > config > network これでメニューにアクセスします。

コマンド	説明	パラメータ
config	ローカル のポートを設定する。	▪ enable 〈true/false〉 – 標準のローカルポート：有効化 (true)、無効化 (false) ▪ auth 〈common|none〉 – ローカルユーザ認証: common–(Local/LDAP/RADIUS/TACACS+); none–(No authentication) (common/none) ▪ ignorecc 〈true/false〉 – ローカルポートで CC 管理モードを無視する：有効化 (true)、無効化 (false) ▪ kbd – キーボードのタイプ

CLI を用いてセキュリティー 設定を行う

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールからセキュリティ設定を行う』** *『166p. の"リモート コンソールからセキュリティ設定を行う"参照 』。*

セキュリティ メニューから多様な設定を行えます。

次のように入力します admin > Security これでメニューにアクセスします。

コマンド	説明	パラメータ
banner	SX II はオプションでカストマイズできる歓迎バナーをサポートしています。これはログインの後に表示されます。最大 6000 文字まで使用できます。 ある GUI を通じてログインすると、固定幅の文字配列で一般的な大きさの 80x25 を持ったバナーが現れます。バナーが非常に大きくて、すなわち 9000 行以上、とするとその GUI に表示されるバナーは全体のページサイズを増やしません、それはスクロール可能なテキスト領域に入っている必要があるからです。 バナーはユーザがログインした場所を識別するものです。また同意バナーを追加することができ、コンソールサーバの操作に入る前にそこに述べられた条件を強制的に承諾するようにします。 「ソフトウェア banner コマンドはログイン後直ちにセキュリティバナーを表示するよう制御'します。	▪ enable <true | false> – バナー表示： 有効化（true)、無効化（false) ▪ audit <true | false> – バナーの監査：有効化（true)、無効化（false) ▪ title <value> –セキュリティ バナーの表題
bannerget	SX II をこのサイトに行き歓迎バナーを検索するように導きます。歓迎バナーと監査宣言は外部 FTP サイトに保持されている上記コマンドを用いて設定できます。	▪ address <ipaddress | hostname> – FTP サーバのアドレス ▪ port <FTP port>– FTP サーバのポート(デフォルトは 21) ▪ path <path to file> – バナーファイルを検索するパス ▪ user <FTP username> – FTP のユーザ名 ▪ password <FTP password> – FTP パス

コマンド	説明	パラメータ
		ワード（もしなければ入力を要請します)
pcshare	複数のユーザによる同一ターゲットへの同時アクセス	mode <shared/private> – PC-Share mode モードを共有あるいは個人とします(共有/個人)
resetmode	ローカルを工場出荷時のリセット状態に設定します	▪ mode full <full|password|disabled> – 完全な工場出荷時にリセット | password – admin のパスワードのみリセット | disabled – 工場出荷時リセットを無効にする(full/password/disabled)
encryption	暗号化のタイプと FIPS のモードをセットします。	▪ mode <auto | aes128 | aes256 | rc4> – デバイスの暗号化モードをセットします ▪ fips <true | false> – FIPS 140-2 モードを有効化/無効化します： 有効化 (true), 無効化 (false).このオプションは効果を発するにはデバイスの再起動を必要とします。

次のように入力します admin > Security > firewall これでメニューとメニューオプションにアクセスします。

コマンド	説明	パラメータと説明
firewall	ファイアウォールを有効にします。	enable <true | false> – ファイアウオールを有効化/無効化： 有効化 (true)、無効化 (false)
viewtables	現在の iptables/ip6tables を見ます。	NA
iptables	Ipv4 パケットフィルタリングと NAT の管理ツール	例 – icmp パケットを閉鎖するには iptables -A INPUT -p icmp -j DROP iptables -A OUTPUT -p icmp -j DROP
ip6tables	IPv6 パケットフィルタリングと NAT の管理ツール	例： iptables -A INPUT -p icmp -j DROP ip6tables -A OUTPUT -p icmpv6 --icmpv6-type 128 -j DROP
iptables-save	ファイアウォールルールを 継続的なものにするため IP テーブル（v4 と v6）を保存します。	NA

次のように入力します admin > Security > loginsettings これでメニューとメニューオプションにアクセスします。

コマンド	説明	パラメータ
idletimeout	システムがユーザを切り離す前に許されるアイドル時間を指定します。	enable <true | false> – パスワードのエージングを有効化/無効化します。 time – アイドルのタイムアウト期間を分で
passwordaging	パスワードがいつ期限切れとなるかを制御します。	enable <true | false> days <value> – パスワード エージングの期間を日数で
singleloginperuser	ユーザを単一のログインセッションだけに制限します。	enable <true/false> – システムに亘ってユーザあたり単一のログインセッションとするのを有効化/無効化
Strongpassword	強力なパスワードルールを設定します。 CLI を経由してパスワードを創るときには、スペースで始めたりスペースで終わることはできません。これはリモートコンソールを用いてパスワードを創る時には適用されません。	enable <true|false> – ローカルユーザのために強力なパスワードルールを有効化/無効化します。 minlength <value> – 最小のパスワードの長さ maxlength <value> – 最大のパスワードの長さ history <value> – パスワード履歴に保存するパスワードの数 uppercase <true|false> – true => パスワードに大文字を必要とします。 lowercase <true|false> – true => パスワードに小文字を必要とします。 numeric <true|false> – true =>パスワードに数字を必要とします。 numeric <true|false> – true =>パスワードに特殊文字を必要とします。
Unauthorizedportaccess	「無記名」グループに割り当てられた一連のポートへの無許可のアクセスを有効化/無効化します。	enable <true/false> – 「無記名」グループに割り当てられた一連のポートへの無記名のアクセスを有効化/無効化します。

コマンド	説明	パラメータ
userblocking	ユーザロックアウトのパラメータを設定します。	mode – <disabled/timer_lockout/deactivate_userid> ユーザ締め出しモードをセットします (disabled/timer_lockout/deactivate_userid) timerattempts <timerattempts> – 試行に時間切れでロックアウトします。 lockouttime <lockouttime> – 時間切れロックアウトの時間 deactivateattempts <value> – ユーザ ID に試行を再有効化します。

次のように入力します admin > security > certificate これでメニューとメニューオプションにアクセスします。

SSL セキュリティ認証がブラウズのアクセスのために使われ、権限のある装置に接続していることを確実にします。

注:もし SX II が証明書署名依頼を生成せずその代わり外部の認証を用いていた場合、それを SX II にインストールする前に人キーから暗号化を取り除くことが必要です。この場合には、キーから暗号を取り除くため、openssl rsa -in server.key -out server2.key と server2.key のようなコマンドを用いる必要があります。個人キーの暗号化がウエブサーバを無許可のユーザで開始されるのを防ぐために使われます。SX II はユーザがウエブサーバに直接アクセスすることを許可していないので、個人キーの暗号化は要求されずセキュリティに妥協もしません。

注:SX II が証明書署名依頼を生成するのに用いられると、 SX II が個人キーを排他的に守るため個人キーは要求されません。

コマンド	説明	パラメータ
generatecsr	証明書署名依頼（CSR）の生成	bits 〈1024 | 2048〉 – 証明書キーのビット強度 name 〈name〉 – 共通名（CN） country 〈code〉 – ISO の 2 文字の国コード（C） state 〈state〉 – 州/県（ST） locality 〈locality〉 – 地方/市（L） org 〈organization〉 – 組織（O） unit 〈unit〉 – 組織の部門（OU） email 〈email〉 – E メール challenge 〈challenge〉 – 挑戦パスワード selfsign 〈true | false〉 – 本人署名証明書（true/false） days 〈days〉 – 証明書が有効となるまでの日数
getcert	特定の場所から証明書を得ます。	address 〈ipaddress | hostname〉 – FTP サーバのアドレス port 〈FTP port〉– FTP サーバのポート(デフォルトは 21) path 〈path to file〉 – 証明書ファイルを検索するパス user 〈FTP username〉 – FTP のユーザ名 password 〈FTP password〉 – FTP パスワード（もしなければ入力を要請します）
getkey	証明書のキーを得ます。	address 〈ipaddress | hostname〉 – FTP サーバのアドレス port 〈FTP port〉– FTP サーバのポート(デフォルトは 21) path 〈path to file〉 – 証明書キーファイルを検索するパス user 〈FTP username〉 – FTP のユーザ名 password 〈FTP password〉 – FTP パスワード（もしなければ入力を要請します）
viewcert	現在の証明書を見ます。	NA
viewcsr	証明書署名依頼（CSR）の生成	NA

コマンド	説明	パラメータ
viewcsrkey	証明書署名依頼キーを見る	NA
deletecsr	現在の証明書署名依頼を削除します。	NA

セキュリティ問題に注目する

コンソールサーバのセキュリティを強化するために以下を行うことを考えます。

SX II はこれらの各々をサポートしていますが、一般的な使用を開始する前に設定しておく必要があります。

- 運用担当者用コンソールと SX II との間で送受信されるデータ トラフィックを暗号化する。
- ユーザに対して認証を行い、また、ユーザに付与する権限を制限する。
- 後程見て監査するために操作に対して適切なデータをログする。あるケースでは、このデータは政府と会社の規制に準拠するために必要とされます。
- セキュリティプロファイルの作成

セキュリティ ノート

運用担当者用コンソールと SX II との間で送受信されるデータ トラフィックの暗号化は使用されるアクセス方法によって決定されます。

デフォルトでは SSH と暗号化されたブラウザーへのアクセスが有効とされています。

暗号化されていない接続を受け入れるためには、Telnet サービスを手動で有効化しなければなりません。HTTP は自動的にユーザを可能であれば HTTPS に振り替えます。

CLI を用いた保守の設定を設定する

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールから保守設定をセットする』** *『183p. の"リモート コンソールから保守設定をセットする"参照 』。*

この maintenance コマンドは SX II のファームウエアの保守に関係したタスクを実行することを可能にします。

次を入力します admin > maintenance これでメニューにアクセスします。

コマンド	説明	パラメータ
deviceinfo	SX II の装置について構造等の情報を提供します。	NA
userlist	ルグインしている全てのユーザのリストを表示し、彼らのソース IP アドレスと接続しているポートを表示します。 同様にコマンドのルートメニューにあるものとして：	NA
upgrade	デバイスを FTP サーバ上のファイルからアップグレードします。	▪ address 〈ipaddress | hostname〉 – FTP サーバのアドレス ▪ port 〈FTP port〉 – FTP サーバのポート（1 ~ 65535） ▪ path 〈path name〉 – FTP サーバのアップグレードアップグレード ファイルへのパス ▪ user 〈FTP username〉 – オプションの FTP サーバのユーザ名 ▪ password 〈FTP password〉 – オプションの FTP サーバのパスワード欠けていてユーザ名が与えられていると求められます。
upgradehistory	最後にシステムをアップグレードした時の情報を得ます。	NA
backup	装置の設定をバックアップし、FTP サーバに保存します。	▪ address 〈ipaddress | hostname〉 – FTP サーバのアドレス ▪ port 〈FTP port〉 – FTP サーバのポート（1 ~ 65535） ▪ path 〈path name〉 – FTP サーバのバックアップファイルへのパス ▪ file 〈file name〉 – オプションの宛先ファイル名デフォルトは backup.rfp です。 ▪ user 〈FTP username〉 – オプションの FTP サーバのユーザ名 ▪ password 〈FTP password〉 – オプションの FTP サーバのパスワード欠けていてユーザ名が与えられていると求められます。
auditlog	装置の監査ログを見ます。	NA

コマンド	説明	パラメータ
auditlogftp	監査ログを得て FTP サーバに保存します。	▪ address <ipaddress | hostname> – FTP サーバのアドレス ▪ port <FTP port> – FTP サーバのポート（1 ~ 65535） ▪ path <path name> – FTP サーバの監査ログファイルへのパス ▪ file <file name> – オプションの宛先ファイル名デフォルトは audit.log です。 ▪ user <FTP username> – オプションの FTP サーバのユーザ名 ▪ password <FTP password> – オプションの FTP サーバのパスワード欠けていてユーザ名が与えられていると求められます。
factoryReset	SX II コンソールサーバをその工場出荷時のデフォルト設定に戻します。 **重要** –:工場出荷時の設定に戻すことを選ぶと、すべてのカスタム設定を消去し、SX II への接続を失います、それは再立ち上げの際、装置の IP アドレスは工場出荷時のデフォルト JP アドレス 192.168.0.192 にリセットされるからです。	▪ mode <full|network> – 実行する工場出荷時リセットのタイプ
Reboot	CLI インタフェースから SX II を再立ち上げします。	NA
restore	デバイスを FTP サーバ上のバックアップ ファイルからリストアします。	▪ mode <full | protected | user | device | userdevice> – 実行するリストアのタイプ ▪ address <ipaddress | hostname> – FTP サーバのアドレス ▪ port <FTP port> – FTP サーバのポート（1 ~ 65535） ▪ path <path name> – FTP サーバのバックアップファイルへのパス ▪ user <FTP username> – オプションの FTP サーバのユーザ名 ▪ password <FTP password> – オプションの FTP サーバのパスワード欠けていてユーザ名が与えられていると求められます。

コマンド	説明	パラメータ
logoff	ユーザを SX II からログオフさせる（強制ログオフ）	▪ user <loginname> – 名前で指定したユーザのすべてのセッションを閉じます。 ▪ session <id | all> – 識別番号によるか全てのセッションを閉じます (ID/all)。 ▪ port <port name | port number> – 名前あるいは番号で指定したポート上のセッションを閉じます。 ▪ address <ipaddress> – 指定したリモートアドレスからのセッションをすべて閉じます。

CLI を用いて、診断の設定を形成する

注:これらの設定はリモートコンソール からも設定できます。参照 **『リモート コンソールから診断のオプションを設定する』** *『192p. の"リモート コンソールから診断のオプションを設定する"参照 』。*

この diagnostic コマンドはトラブルシュートのための情報を集めるのを可能にします。

次を入力します admin > Diagnostics これでメニューにアクセスします。

コマンド	説明	パラメータ
netif	ネットワーク インタフェースの情報	NA
netstat	ネットワークの統計を得ます。	▪ type <stats | interfaces | route> - 統計インタフェースルート
ping	リモートシステムを ping してそれが到達できることを確実にします。	▪ ip <ipaddress | hostname> - ping する IP アドレス/ホスト名 ▪ if <auto | lan1 | lan2 | usb0> - ネットワークインタフェース(デフォルト: auto)
traceroute	ネットワークのホストへのルートを追跡します。	▪ ip <ipaddress | hostname> - トレースする IP アドレス/ホスト名 ▪ maxhops <5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50> - 最大ホップの制限 (デフォルト:10) ▪ if <auto | lan1 | lan2 | usb0> - ネットワークインタフェース(デフォルト: auto)
diagscript	FTP サーバから診断スクリプトを得て実行します。	▪ address <ipaddress | hostname> - FTP サーバのアドレス ▪ port <FTP port> - FTP サーバのポート (1 ~ 65535) ▪ path <path name> - FTP サーバのバックアップファイルへのパス ▪ user <FTP username> - オプションの FTP サーバのユーザ名 ▪ password <FTP password> - オプションの FTP サーバのパスワード
diaglogput	監査スナップショットを得て FTP サーバに保存します。	▪ address <ipaddress | hostname> - FTP サーバのアドレス ▪ port <FTP port>- FTP サーバのポート(1 ~ 65535) ▪ path <path name> - FTP サーバの診断スクリプトファイルへのパス ▪ user <FTP username> - オプションの FTP サーバのユーザ名 ▪ password <FTP password> - オプションの FTP サーバのパスワード

次を入力します admin > diagnostics > debug これでメニューにアクセスします。

コマンド	説明	パラメータ
setlog	診断ログをセット/得ます	▪ module 〈module〉 – モジュール名 ▪ level 〈level〉 – 診断ログのレベル (err/warn/info/debug/trace) ▪ vflag 〈vflag〉 – 冗長なフラグ (timestamp/module/thread/fileline) ▪ verbose 〈on|off〉 – 冗長制御 (on/off)
viewstats	モジュールの状態を見ます。	▪ module 〈module〉 – モジュールの名前

Ch 7 ラック PDU を SX II に接続し電力制御のオプションを設定する。

SX II は PX2 を SX II に接続するとき次のオプションを提供します。

- SX II を PX2 シリアルポートに接続します。
  この構成で、PX2 へのアクセスが PX2 コマンドラインインタフェース（CLI）を通じた行われます。
- SX II を PX2 の機能ポートに接続します。
  この構成で、PX2 は他の電源タップと同様に SX II インタフェースから管理されます。

次を参照してください。 **PX2 ヘルプ** ここに PX2 装置を用いることに関する情報があります。

この章の内容

SX II を PX2 シリアルポート - SX に接続する

この構成で、 PX が SX II に接続された後、 CLI を用いて PX にアクセスします 。

この図面に用いられた装置はあなたの特定のモデルとは一致しないかもしれないことを承知してください。しかし、使われている接続はどのモデルでも同じです。

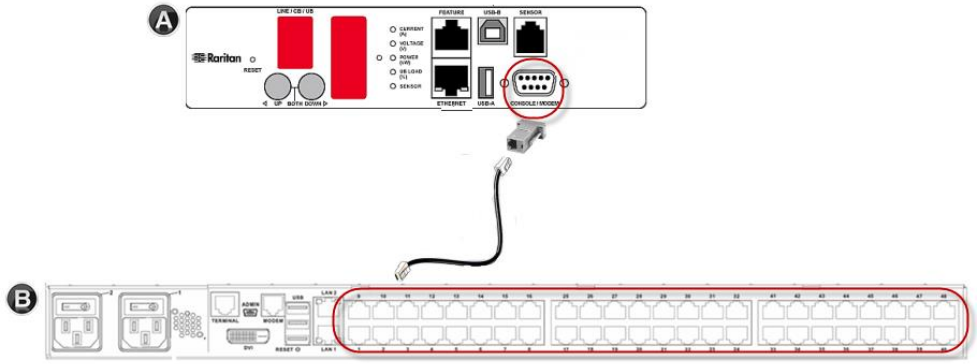
SX II を PX に接続するには：

1. ASCSDB9F アダプターを PX2 DB9 コンソール/モデム ポートに接続します。

   注:このアダプターは Raritan から購入できます。それは PX あるいは SX II に付いて来ません。

2. Cat5 ケーブルを ASCSDB9F アダプタに差し込み、ケーブルの他方の端を SX II のポートに差し込みます。

3. PX2 の電源を入れます（まだ入っていなければ）。コマンドライン インタフェース（CLI）インタフェースが現れます。



A	PX 装置
B	SX II

SX II を PX2 フィーチャーに接続する

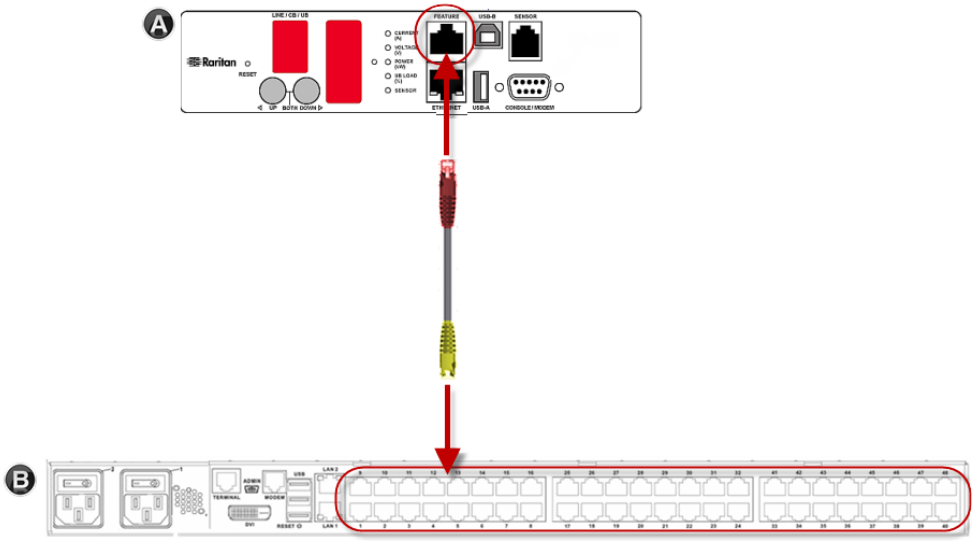
この構成で、PX は他の電源タップと同様に SX II インタフェースから管理されます。参照 『電源制御』。

この図面に用いられた装置はあなたの特定のモデルとは一致しないかもしれないことを承知してください。しかし、使われている接続はどのモデルでも同じです。

SX II を PX のフィーチャー ポートに接続するには：

1. CSCSPCS クロスオーバ Cat5 ケーブルの赤色の端を PX 上の機能ポートに接続します。
2. CSCSPCS クロスオーバ Cat5 ケーブルの黄色の端を SX II のポートに接続します。
3. PX の電源を入れます（まだ入っていなければ）。

これで PX を SX II への管理された電源タップとして追加できます。参照 *リモート コンソールからの電源タップの設定* 『72p. 』 または *CLI を用いた電源タップの設定* 『200p. 』。



A	PX 装置
B	SX II

Ap A 仕様

この章の内容

SX II 寸法と物理的仕様

形状要素	1U ラックマウント可能
電源	100/240VAC 自動スイッチ:50-60 Hz, .35A, 36-72VDC 自動スイッチ
最大使用電力	4-ポート SX:21W ｜ 8-ポート SX:21W ｜ 16-ポート SX:22W ｜ 32-ポート SX:23W ｜ 48-ポート SX:25W
温度	動作時:0° C - 50° C. 非動作時:0° C - 55° C
湿度	動作時:20% - 85%非動作時：10% - 90%
海抜高度	0 から 2,000 m の高度で成城に動作

サポートされているリモート接続

ネットワーク

- 10BASE-T
- 100BASE-T
- 1000BASE-T（ギガビット）イーサネット

プロトコル

- TCP/IP
- HTTP
- HTTPS
- RADIUS
- LDAP/LDAPS
- SSH
- Telnet
- TACACS+
- UDP
- SNTP

SX II モデル１台当たりサポートされるポートの数

モデル	ポート数
SX2-04 と SX2-04M	4
SX2-08 と SX2-08M	8
SX2-16 と SX2-16M	16
SX2-32 と SX2-32M	32
SX2-48 と SX2-48M	48

ユーザセッションの最大数：

同時に最大で 200 のユーザが単一の SX II にアクセス可能。

これはリモートアクセス、SSH/Telnet 経由のダイレクト ポート アクセス および コマンドラインインタフェース に適用されます。

ポートあたりの最大サポートユーザ数

同時に最大で 200 のユーザが単一の SX II にアクセス可能。

これはリモートアクセス、SSH/Telnet 経由のダイレクト ポート アクセス および コマンドラインインタフェース に適用されます。

ポートアクセスのプロトコルの必要条件

プロトコル	ポート	通信方向
HTTP	装置が動作するためにポート 80, 443 と 5000 がファイアウォールで開かれることが必要	両方

プロトコル	ポート	通信方向
	ポート 80 このポートは、必要に応じて設定できます。参照 HTTP ポートおよび HTTPS ポートの設定。 完全なセキュリティを確保するため、デフォルトでは、SX II によって HTTP (ポート 80) で受信された要求は、すべて HTTPS に自動転送されます。 要求はポート 80 で受け付けられるので、SX II にアクセスするためにユーザはブラウザのアドレス ボックスに明示的に「https://」と入力する必要はありません。また、セキュリティも完全に確保されます。 **ポート 443** このポートは、必要に応じて設定できます。参照 『HTTP ポートおよび HTTPS ポートの設定』。 デフォルトでは、このポートはさまざまな目的で使用されます。たとえば、クライアントから HTML で Web サーバにアクセスする場合、クライアント ソフトウェアをクライアントのホストにダウンロードする場合、 データをクライアントに転送する場合などです。 **ポート 5000** このポートは、他の Dominion デバイスの検出、および Raritan デバイスと各種システム (CC-SG 管理で利用可能なデバイス向けの CC-SG など) との間の通信に使用されます。 このポートはデフォルトで 5000 に設定されていますが、現在使われていない別の TCP ポートに変更することもできます。この設定方法については、次をを参照してください。『ディスプレイの設定』。	
HTTPS SSL のみ	**ポート 443** TCP ポート 443 はオープンでなければなりません。 ポート 80 は閉じられます。	両方
SSH	**ポート 22** TCP ポート 22 はオープンでなければなりません。 ポート 22 は SX II コマンドラインインタフェース (CLI) のために使用されます。	両方
Telnet	**ポート 23** TCP ポート 22 はオープンでなければなりません。	両方
TACACS+	**ポート 49**	外向け

プロトコル	ポート	通信方向
	ポート 49 はオープンでなければなりません。	
RADIUS	**ポート 1812** SX II が RADIUS プロトコルを用いてリモートで認証されるユーザログインで設定されていると、ポート 1812 は使用されオープンでなければなりません。 しかし、このシステムはまたあなたが指定するどのポートを使用しても設定できます。 **これはオプションです** **ポート 1813** RADIUS プロトコルを使用してユーザをリモート認証するように SX II が設定されており、かつ、イベントのログ記録に RADIUS アカウンティングが使用されている場合、ログ通知の転送にデフォルトでポート 1813 が使用されます。ただし、別のポートに変更することもできます。	送信
LDAP	**ポート 389 と 636** ポート 389 と 636 はオープンでなければなりません。 LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように SX II が設定されている場合、デフォルトでポート 389 または 636 が使用されます。ただし、あなたの指定する別のポートに変更することもできます。 **これはオプションです**	送信
SNMP	**ポート 161 と 162** ポート 161 は 内向け/外向け、 読み/書きの、SNMP アクセスのために使用されます。 ポート 162 はオープンでなければなりません。ポート 162 は 外向け SNMP トラップのために使用されます。	両方（ポート 161） 送信 （ポート 182）
FTP アップグレード用	**ポート 21** ポート 21 はオープンでなければなりません。	送信
SYSLOG、設定可能 UDP ポート	**ポート 514** UDP ポート 514 はオープンでなければなりません。 SX II が sylog サーバにメッセージを送るように設定されていると、UDP ポート 514 は通信用に使われます。	送信

プロトコル	ポート	通信方向
SNTP (時刻サーバ)、設定可能 UDP	**ポート 123 にあります。** SX II の内部クロックをオプションで中央の時刻サーバと同期させることができます。 この機能を利用するには UDP ポート 123 (SNTP 用の標準ポート) を使用する必要がありますが、あなたの指定する別のポートに変更することもできます。 **これはオプションです**	両方

NFS ログを取るとき LDAP サーバを使うなどして追加のポートを開く必要があります。

これらのポートはインストールするごとに、ネットワークのトポロジー、バーチャル ローカル エリア ネットワーク (VLAN) 、それにファイアウォールの設定によって変わります。、

ネットワークの管理者に連絡を取って、サイトに特有の情報と設定を尋ねてください。

SX II ポート ピン設定

ローカル ターミナル ポート		
pin	定義	方向
pin 1	RTS	出力
pin 2	使用せず	
pin 3	TXD	出力
pin 4	接地	
pin 5	接地	
pin 6	RXD	入力
pin 7	使用せず	
pin 8	CTS	入力

サーバポートの DTE モード		
pin	定義	方向
pin 1	RTS	出力
pin 2	DTR	出力

サーバポートの DTE モード		
pin 3	TXD	出力
pin 4	接地	
pin 5	接地	
pin 6	RXD	入力
pin 7	DSR	入力
pin 8	CTS	入力

サーバポートの DCE モード		
pin	定義	方向
pin 1	CTS	入力
pin 2	DSR	入力
pin 3	RXD	入力
pin 4	接地	
pin 5	接地	
pin 6	TXD	出力
pin 7	DTR	出力
pin 8	RTS	出力

SX2 ポート範囲

内部のポート設定のためのポートの範囲 – CSC, HTTP, HTTPS, SSH, Telnet, DPA SSH , DPA Telnet – は 1 to 64510 ソケット作成のためのポート範囲は 1024 から 64510 に限定されています。

外部のポート設定 – LDAP, RADIUS, TACACS+ と SNMP – はポート範囲の制限に影響を受けません。

ネットワーク速度の設定

SX II における ネットワーク速度の設定

ネットワーク スイッチ	自動	1000/全二重	100/全二重	100/半二重	10/全二重	10/半二重
自動	使用可能な	1000/全二重	SX II :100/	100/半二重	SX II :10/全	10/半二重

SX II　におけるネットワーク速度の設定

におけるポートの設定	最高速度		全二重 スイッチ:100/半二重		二重 スイッチ:10/半二重	
	1000/全二重	1000/全二重	通信不可	通信不可	通信不可	通信不可
1000/全二重						
100/全二重	SX II :100/半二重 スイッチ:100/全二重	SX II :100/半二重 スイッチ:100/全二重	100/全二重	SX II :100/半二重 スイッチ:100/全二重	通信不可	通信不可
100/半二重	100/半二重	100/半二重	SX II :100/全二重 スイッチ:100/半二重	100/半二重	通信不可	通信不可
10/全二重	SX II :10/半二重 スイッチ:10/全二重	通信不可	通信不可	通信不可	10/全二重	SX II :10/半二重 スイッチ:10/全二重
10/半二重	10/半二重	通信不可	通信不可	通信不可	SX II :10/全二重 スイッチ:10/半二重	10/半二重

凡例:

通信できません。

サポート

通信は行えますが、推奨できません。

Ethernet 仕様でサポートされていません。通信は行えます

が、衝突が発生します。

Ethernet 仕様では通信できないことになっています。SX II は期待どおりに動作しません。

注:ネットワーク通信の信頼性を高めるため、SX II とネットワーク スイッチの双方で、通信速度と通信方式を同じ設定にしてください。たとえば、SX II とネットワーク スイッチで "自動検出" に設定するか (推奨)、または、双方の通信速度と通信方式を同じ設定にします (例: 100 Mbps/全二重)。

ユーザ セッションのタイムアウトのデフォルト値

- SX II インタフェースー 5 分（これを変更するには、セキュリティを選び [Settings Idle Timeout] (minutes)] のフィールドに記入します。
- SSH – 16 分
- Telnet – 2 時間

SX II でサポートするﾛｰｶﾙ ポート DVI の解像度

以下は DVI モニターを SX II のローカルポートから接続するときの解像度です。

- 1920x1080@60Hz
- 1280x720@60Hz
- 1024x768@60Hz (デフォルト)
- 1024x768@75Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1600x1200@60Hz
- 800x480@60Hz
- 1280x768@60Hz
- 1366x768@60Hz
- 1360x768@60Hz
- 1680x1050@60Hz
- 1440x900@60Hz

SX II 装置の LED 状態表示

LED は電源状態、装置の状態、とターゲット接続状態を表示しています。

SX IIの前面パネルと後面パネルに LED があります。前面パネルの LED 状態表示

- SX II が立ち上がると、電源 LED のみが点灯します。電源 LED は赤と青の両方になります。
- ポートチャンネル LED は SX II が立ち上がる間消えています。
- SX II が完全に電源オンとなると、電源 LED はそのままオンになっています。
  - 単一の電源供給が差し込まれていると、電元 LED は **赤**。
  - 両方の電源がオンの場合、電源 LED は **青**。
- 電元オンのターゲットを CAT5 ケーブルで SX II に物理的に接続すると、ポートチャンネルの LED は点灯します。

  LED はターゲットが切り離されるまで点灯しています。

注:SX II ポートチャンネル LED が点灯し、SX II がターゲットを検出するためにはターゲットは電源がオンでなければなりません。

- ターゲットを SX II のポートから物理的に切り離すと、ポートチャンネルの LED は消灯します。
- SX II にログインし Raritan Serial Console (RSC), SSH あるいはローカルコンソール経由でターゲットに接続すると、ポートチャンネル LED は点滅します。

  その LED はターゲットへの接続が終了するまで点滅します。

  同時に１つ以上のターゲットに接続すると、すべての LED がそろって点滅します。
- SX II のリセットボタンを押して装置をリセットするときあるいは SX II GUI からリブートを行ったとき、電源 LED は装置の電源が切れオフとなるとき点滅します。

  装置の電源が戻る間、電源 LED は点滅を続けます。

  装置が復電すると、電源 LED は点滅を止め点灯となります。

ターゲットのケーブル接続の距離とレート

SX II はそのシリアルポートとターゲットを CAT5 ケーブルで接続するとき次の距離までをサポートします。

距離	秒あたりビット (最大転送速度)
300ft/91m	1,200

300ft/91m	1,800
300ft/91m	2,400
200ft/60m	4,800
100ft/30m	9,600
50ft/15m	19,200
25ft/7.5m	28,800
25ft/7.5m	38,400
16ft/5m	57,600
8ft/2.5m	115,200
4ft/1.2m	230,400

Ap B LDAP スキーマを更新する

この章の内容

ユーザ グループ情報を返す

この章で説明する内容に従って、ユーザ認証の成功後にユーザ グループ情報を返すように設定してください。ユーザ グループ情報は、ユーザへの権限付与に役立ちます。

LDAP/LDAPS から返す場合

LDAP/LDAPS 認証に成功すると、 SX II では、そのユーザのに付与されている権限に基づいて、そのユーザに付与する権限が決まります。リモート LDAP サーバから次のような名称の属性が返されるので、ユーザ名がわかります。

rciusergroup 属性のタイプ：文字列

このように属性を返すには、LDAP/LDAPS サーバ上でスキーマを拡張しなければならないことがあります。認証サーバ管理者に連絡し、この属性を有効にしてください。

また、Microsoft® Active Directory® の場合、標準 LDAP memberOf が使用されます。

Microsoft Active Directory から返す場合

警:この手順は、経験豊富な Active Directory® 管理者だけが行ってください。

Windows 2000 Server 上の Microsoft Active Directory からユーザ 情報を返すには、LDAP/LDAPS スキーマを更新する必要があります。詳細については、Microsoft 発行のドキュメントを参照してください。

1. Active Directory 用のスキーマ プラグインをインストールします。インストール手順については、Active Directory のドキュメントを参照してください。

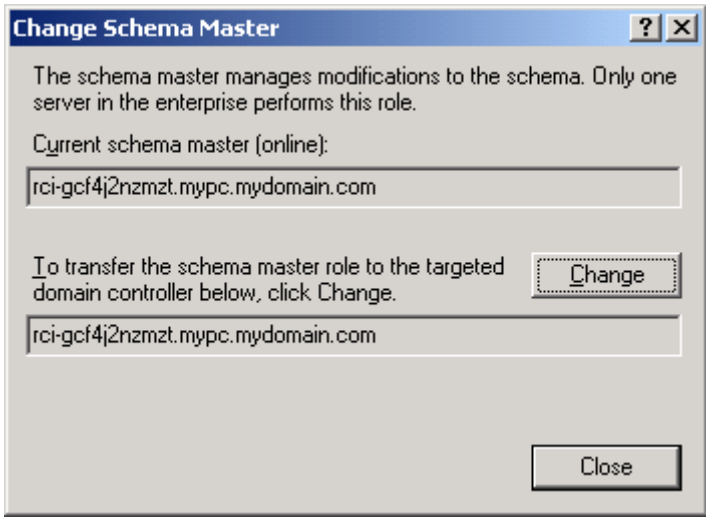
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するようにレジストリを設定する

ドメイン コントローラによるスキーマへの書き込みを許可するため、スキーマの更新を許可するレジストリ エントリを設定する必要があります。

スキーマへの書き込みを許可するには

1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) ルート ノードを右クリックし、コンテキスト メニューの [Operations Master] (操作マスタ) をクリックします。[Change Schema Master] (スキーマ マスタの変更) ダイアログ ボックスが開きます。



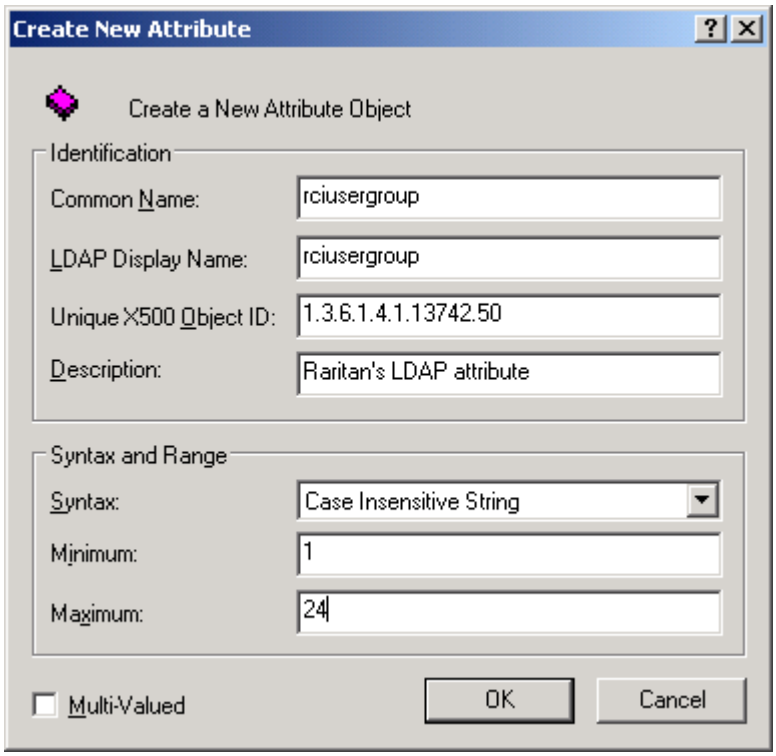
2. [Schema can be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正できるようにする) チェック ボックスをオンにします。**(オプション)**
3. [OK] をクリックします。

新しい属性を作成する

rciusergroup クラスに対する新しい属性を作成するには

1. ウィンドウの左ペインで、[Active Directory Schema] (Active Directory® スキーマ) の前に表示されている [+] (+) 記号をクリックします。
2. 左ペインで [Attributes] (属性) を右クリックします。

3. コンテキスト メニューの [New] (新規) をクリックし、続いて [Attribute] (属性) をクリックします。警告メッセージが表示されたら、[Continue] (続行) をクリックします。[Create New Attribute] (属性の新規作成) ダイアログ ボックスが開きます。



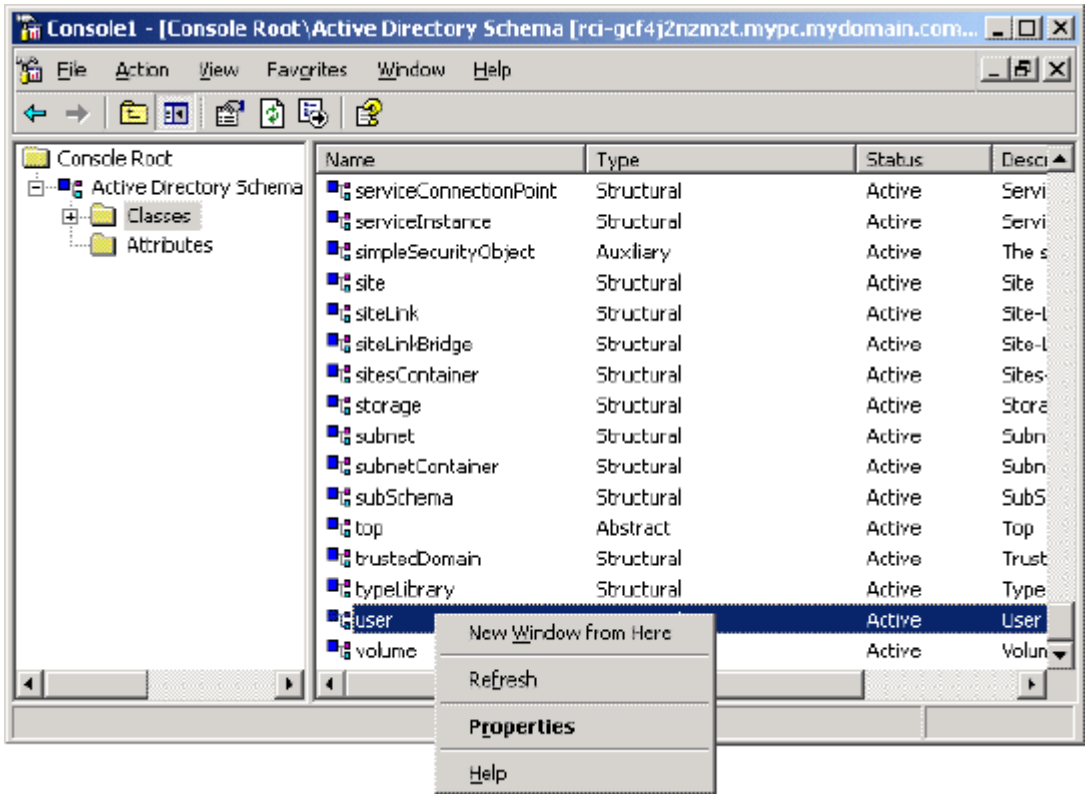
4. [Common Name] (共通名) ボックスに「rciusergroup」と入力します。
5. [LDAP Display Name] (LDAP 表示名) ボックスに「rciusergroup」と入力します。
6. [Unique X500 Object ID] (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
7. [Description] (説明) ボックスにわかりやすい説明を入力します。
8. [Syntax] (構文) ボックスの一覧で [Case Insensitive String] (大文字/小文字の区別がない文字列) を選択します。
9. [Minimum] (最小) ボックスに「1」と入力します。
10. [Maximum] (最大) ボックスに「24」と入力します。
11. [OK] をクリックし、新しい属性を作成します。

属性をクラスに追加する

▶ 属性をクラスに追加するには

1. ウィンドウの左ペインで [Classes] (クラス) をクリックします。

2. 右ペインをスクロールして [user] (user) を表示し、右クリックします。



3. コンテキスト メニューの [Properties] (プロパティ) をクリックします。[user Properties] (user のプロパティ) ダイアログ ボックスが開きます。
4. [Attributes] (属性) タブをクリックしてそのプロパティ ページを開きます。
5. [Add] (追加) をクリックします。

6. [Select a schema object] (スキーマ オブジェクトを選択) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。

7. [Select Schema Object] (スキーマ オブジェクトを選択) ダイアログ ボックスで [OK] をクリックします。
8. [user Properties] (user のプロパティ) ダイアログ ボックスで [OK] をクリックします。

スキーマ キャッシュを更新する

スキーマ キャッシュを更新するには

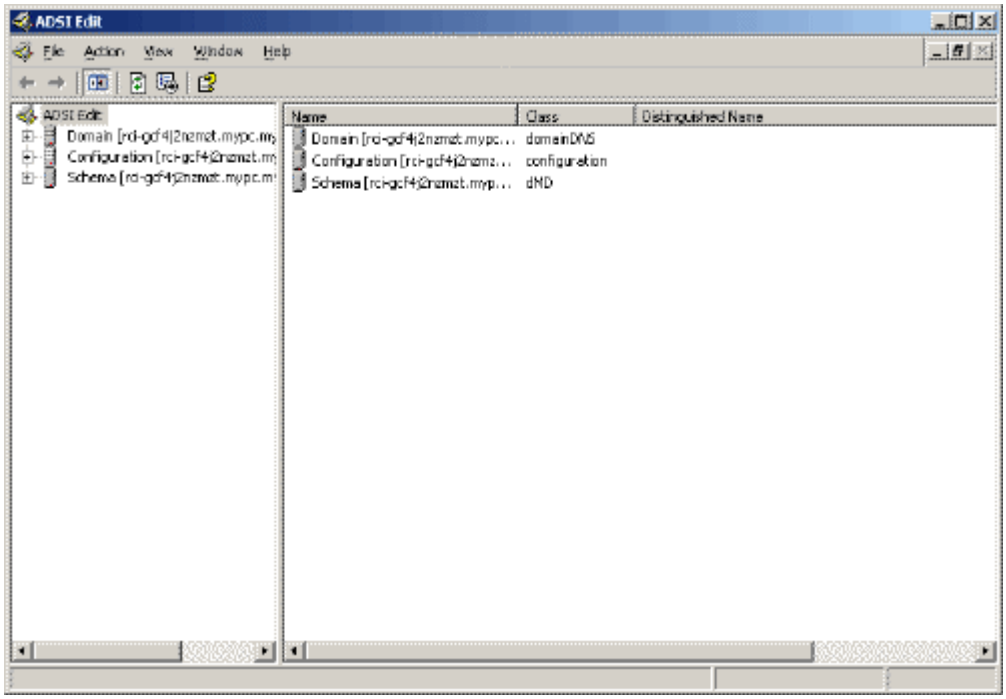
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

ユーザ メンバの rciusergroup 属性を編集する

Windows Server 2003 上で Active Directory スクリプトを実行するには、Microsoft から提供されるスクリプトを使用します (Windows Server 2003 のインストール用 CD-ROM に収録されています)。これらのスクリプトは、Microsoft® Windows 2003 のインストール時にシステムにロードされます。Active Directory Service Interface (ADSI) は、Active Directory の下位レベルのエディタとして動作します。これにより、オブジェクトの追加、削除、移動などの一般的な管理作業を、ディレクトリ サービスを使用して行うことができます。

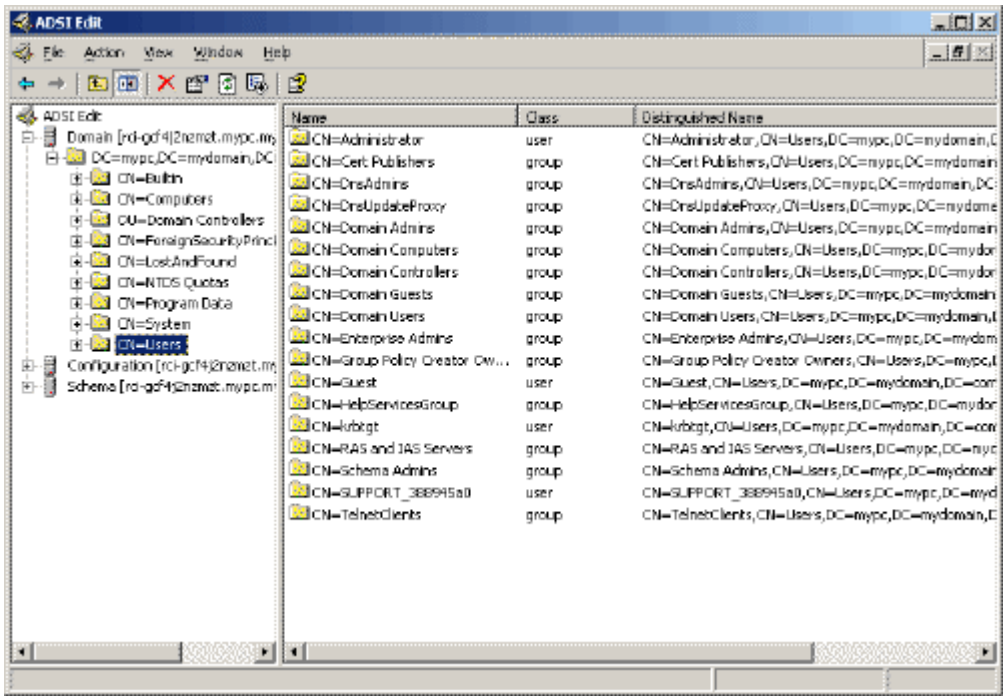
rciusergroup グループ内の個別のユーザ属性を編集するには

1. Windows Server 2003 のインストール用 CD-ROM を挿入し、エクスプローラで Support フォルダの下の Tools フォルダを開きます。
2. SUPTOOLS.MSI をダブルクリックし、サポート ツールをインストールします。
3. サポート ツールがインストールされたフォルダを開きます。adsiedit.msc を実行します。ADSI Edit ウィンドウが表示されます。



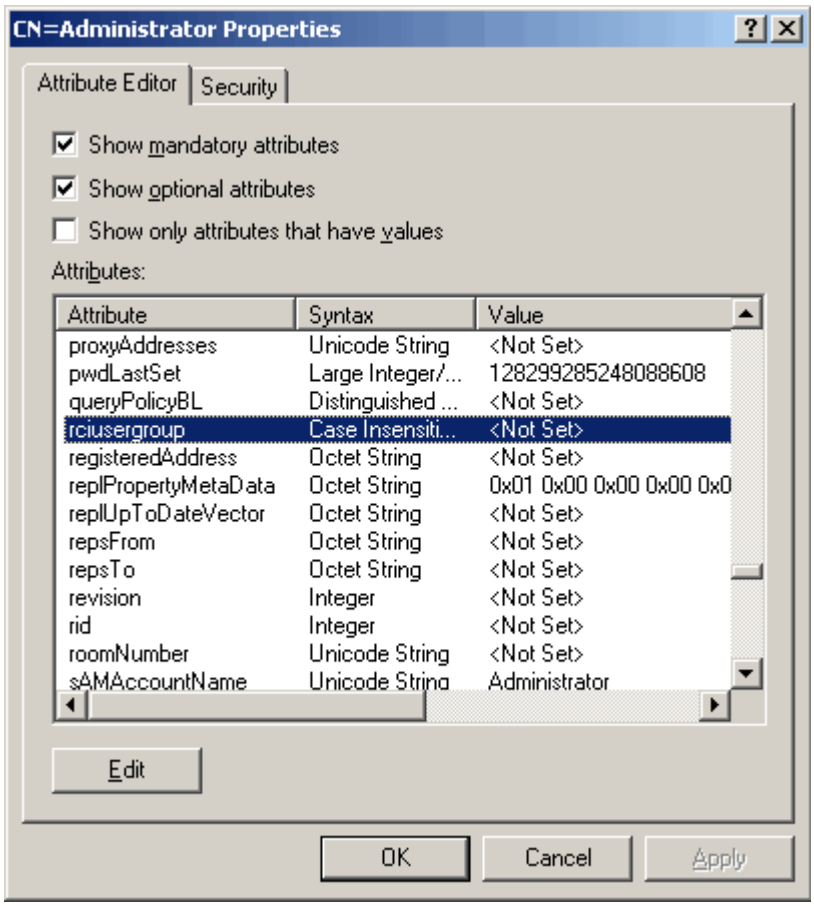
4. ドメインを開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。

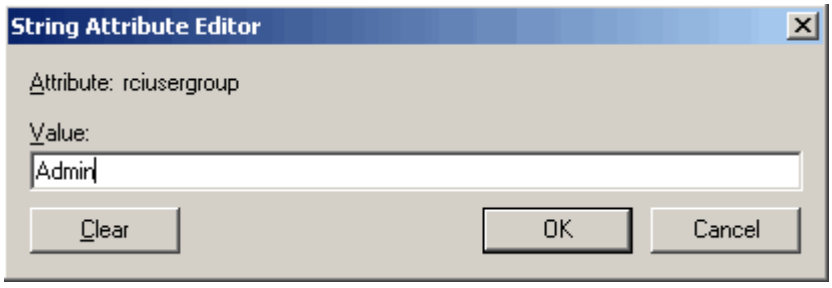


6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキスト メニューのプロパティをクリックします。

7. 属性エディタ)タブをクリックします。属性ボックスの一覧で rciusergroup を選択します。



8. 編集 をクリックします。文字列属性エディタダイアログ ボックスが開きます。
9. [Edit Attribute] フィールドに、 SX II で作成したユーザ を入力します。OK をクリックします。



Ap C よくある質問

Dominion SX II の概要

Dominion SX II の概要

Dominion SX II とは何ですか？	Dominion SX II は Raritan の次世代シリアル コンソール サーバで、は従来のデバイスにいつでもどこでも安全なIP アクセスと制御を提供しています。 新製品 SX II はこの市場において最も強力で、安全で、信頼性が高く、使いやすく、管理しやすい IP 上のシリアル コンソールです。 SX II はネットワークデバイス、サーバ、PDU、電話通信とその他のは従来のデバイスに便利で生産的なアクセスを提供しています。
SX II は従来の SX とどのように違うのですか？	SX II 従来の SX の次世代バージョンです。SX II は全面的に新しいハードウエアとソフトウエアの設計となり抜本的に従来の SX より以上に強力で多機能となっています。SX II は事実上 SX の全ての機能に加えて素晴らしい新機能を提供します。従来の SX とは違って、全ての SX モデルは２重電源供給、２重 LAN 接続と複数のローカル接続を備えています。SX II はモデルは 4、8、16、32、と 48 のモデルが、内蔵モデム有または無で利用できます。多くの管理機能は Dominion SX III にあるものと同じです。
SX II の新機能は何ですか？	新機能には以下のものが含まれます：ギガビット イーサネット、IPv6 ネットワーク、Cisco のデバイスとロールオーバ ケーブルなしでの直接接続、FIPS 140-2 暗号化、USB スティックあるいは TFTP 経由の自動設定、3G/4G セルラーモデムのサポート、最大 8 ギガバイトのフラッシュ スペース、複数のラックでのアクセス方法と Dominion と共通のユーザ インタフェースと管理。
SX II は従来 SX の機能のすべてを持っていますか？	事実上従来の SX の機能は SX II に含まれています。いくつかの機能（ファームウエアの更新、固定ユーザグループ）はより強力な Dominion スタイルの機能で置き換えられ少数のあまり使われない機能は削除されました。
SX II の価格はいくらですか？	SX II に相当の価格上昇を予想されるかもしれませんが、それは従来の SX と同様です。正確な価格の違いはモデルごとに異なります。いくつかの SX II モデルは従来の SX モデルより低価格にさえなっています！
従来の SX 製品の最後プランはあ	Dominion SX II が従来の Dominion SX に置き換わります。2015 年第 4 四半期に、Raritan は従

Dominion SX II の概要	
るのでしょうか？	来の SX モデルの最終セールを数か月売り切りセールスの機会があります。Raritan は従来の SX に対するソフトウエア サポートをセールス終了のアナウンスの日付から２年間続けます：それ以降は従来の SX へのファームウエアの発行はなくなります。Comm と Center のサポートはサポート終了を超えても続けられます。既存のハードウエアの補償は有効です。
SX II のための下取りプログラムはありますか？	はい、従来の SX とあるいは他社のシリアル コンソール サーバの下取りの機会があります。

Dominion SX II ハードウエア プラットフォーム

ハードウエアの改良のいくつかを教えてください。	たくさんあります：より強力な CPU、メモリーとフラッシュのスペース、２重電源供給（AC と DC）、２重ギガバイト LAN ポート、ポート状態 LED、4 USB ポート、自動センシング DTE/DCE ポート、USB ラップトップアクセス、DVI/USB アクセス、と全モデルでモデムのオプション。
SX II の性能は従来の SX に比べてどうですか？	SX II ハードウエア プラットフォームは抜本的により強力で、 1GHz CPU、8-重に増加した RAM、最大 8Gb のフラッシュスペース。SX II はポートあたり 10 のセッションと 200 のトータル シリアル セッションをサポートします。ポートの設定は 15 から 23 倍速く、同時接続、接続速度とシリアルの処理で桁違いの改良となっています。
SX II はどのようなネットワーク接続のタイプを持っていますか？	SX II は２つのギガビット イーサネット LAN のポートを持っていて 10/100/1000 Megabit 接続を自動検出でサポートします。LAN ポートの設定として（1）シングル LAN 接続、あるいは（2）２重 LAN 接続が可能で、後者は(a) 障害復旧あるいは(b) 同時動作で作動します。 IPv4 と IPv6 の両方のアドレスがサポートされています。
SX II モデルのすべては 1U ですか？48 ポートモデルでもそうでしょうか？	はい、全てのモデルは 1U でラックマウントキットが含まれています。現 SX と同様に、48 ポートモデルは 48 のポートを背面パネルに持っています：この空間を作るため、２重電源コンセントは前面にあります。
ログのために利用できるフラッシュのスペースはどのくらいですか？	あなたが過去に使ったかもしれないどれよりも大きいです。4 と 8 ポートの SX II は２つの 2 ギガバイトのフラッシュスペースを持っています。他のモデルでははは２つの 8 ギガバイトのフラッシュスペースを持っています。
SX II はリモート電源制御をサポートしていますか？	はい、SX II はシリアル デバイスのために Raritan PX インテリジェント ラック PDU への接続を用いてリモート電源制御をサポートしています。
SX II のローカル admin ポートのためのピン割り当てはどうなっていますか？	SX II のローカル admin ポートは RJ-45 ポートで次の DTE ピン割り当てとなっています（ピン/信号：1/RTS, 3/TXD, 4/GND, 5/GND, 6/RXD, 8/CTS。ラップトップの DB9 ポートに Raritan ASCSDB9F RJ-45(メス) から DB9（メス）へのア

	ダプターに Cat5 ケーブルで接続できます。
Dominion SX は 19" のラックマウント キットを含んでいますか？	はい。Dominion SX II は標準ですぐにインストールできる 19″ のラックマウント キットがついて来ます。

Serial-over-IP セッションとアクセス

Serial-over-IP セッションとアクセス

どのようなタイプのシリアルアクセスが可能ですか？	SX II は最も広範な多様性のシリアル アクセスをサポートし、それは次のものを含みます：SSH、Telnet とウエブブラウザーのシリアル接続ウエブ ブラウザ アクセスは Raritan シリアル クライアントを用い、 Raritan Comm と Center を通じて可能です。 便利な Direct Port Access (DPA)方法が利用できます。At-the-rack （ラックでの）アクセスはシリアルケーブル、USB と KVM コンソール経由で利用できます。緊急時のモデムアクセスがオプションの内蔵モデムあるいは外部の 3G/4G セルラー モデム経由で可能です。
ダイレクト ポート アクセスとは何ですか？	ダイレクト ポート アクセスは SX に接続されたシリアルデバイスへの直接で便利なアクセスを提供します。複数の Direct Port Access (DPA) 方法が SSH、Telnet と HTTP/URL 経由で利用できます。
SX II は Telnet をサポートしていますか？	Telnet はサポートされていますが、しかし Telnet が暗号化セッションをサポートしていないのでセキュリティ上の理由でデフォルトで無効とされています。Telnet の代わりに SSH を使う事を勧めます。
緊急時のモデム経由のアクセスとは何ですか？	２種類のタイプのモデムアクセスがサポートされています。第一に、内臓電話モデムは各 SX II のモデルにオプションとなっています（DSX２－...M モデル）。第二に、3G/4G セルラーモデムアクセスのために、 Sierra Wireless Airlink GX440 ワイヤレスモデムを SX II の USB ポートに接続でき、モデムの IP アドレス経由で SX II にアクセスできます。
いかにして Sierra のワイヤレスモデムの安全を確保できますか？	SX II のファイアウォール機能を用いて Linux スタイルの ″iptable″ ルールを作成しワイヤレスモデムへの接続を安全なものにします。さらにモデム自身もファイアウォール機能を持っています。
データセンタにいるとき いかにして SX II にアクセスできますか？	Dominion SX II ではラックでの複数のタイプのローカルアクセスを得ることができます。ラップトップあるいは PC を接続するため RJ45 シリアルポートあるいは USB ミニ B ポートに接続できます。移動台あるいはラックマウントのキーボード台を使ってキーボードを SX II

Serial-over-IP セッションとアクセス	
	の DVI と USB KVM ポートに接続できます。SX II のウエブベースのユーザインタフェースにアクセスするには、クロスオーバーのイーサネットケーブルを SX II の LAN ポートに接続します。
複数の SX II のローカルなポートに統合したアクセスを得ることができますか？	割り当て方法は 2 通りあります。第 1 に、複数の SX II のシリアル admin ポートをもう 1 台の SX II にストレート Cat5 ケーブルで接続できます。第 2 に、SX II の DVII/USB ローカルポートを Dominion SX III のような KVM スイッチに接続することができます。これでデータセンター内と周辺の複数の SX II へのアクセスを与えます。
どのボーレートがサポートされていますか？	1200, 1800, 2400, 4800, 9600 (デフォルト), 19200, 28800, 38400, 57600, 115200, と 230400 ボーこれをポート設定ページあるいは CLI からポートごとに設定できます。
Dominion SX II のターミナルエミュレータはどのコードセットをサポートしていますか？	Dominion SX リリース 3.0 或いはそれ以降は VT100/VT220/VT320 と ANSI を次のコードセットでサポートしています：規定値：225 スレド,US-ASCII,ISO-8859-1,ISO-8859-15,UTF-8,Shift-JIS,EUC-JP,EUC-CN, と EUC-KR。
ある SX II を通じて同時にアクセスできるアシリアルデバイスはいくつですか？	一群のユーザが SX II に接続された全てのシリアルデバイスに同時にアクセスできます。例えば、48 ポートの SX II で、ユーザは同時にそれに接続された 48 のシリアルデバイスの全てに接続しアクセスすることができます。
一群のユーザが SX II に接続された全てのシリアルデバイスに同時にアクセスできます。	10 人までのユーザが単一のシリアルデバイスに同時にアクセスでき、SX II あたり 200 までの同時アクセスが可能です。例えば、32 ポートの SX II で、6 人のユーザが同時にそれに接続された 32 のシリアルデバイスの全てにアクセスし、トータルで 192 ユーザセッションを持てます。これは典型的なユーザのシナリオではないかも知れませんが、SX II の強力なシリアル処理能力を示すものです。
Dominion SX は SUN® "break-safe"のユニットですか？	全ての Dominion SX ユニットは SUN Solaris を使用するに当たって SUN ″break-safe″ です。
シリアルデバイスへの接続	

シリアルデバイスへの接続

SX II はどのようなタイプのデバイスが接続できますか？	SX II は最も広範な多様性のシリアル デバイスをサポートし、それには、ネットワーク ルーター、イーサーネット スイッチ、ファイアウォール、UNIX/LINUX サーバ、ウィンドウズ サーバ、バーチャル ホスト、ラック PDU、UPS システム、電子通信・ワイヤレス機器が含まれます。SX II は Cat5 ケーブルでこれらのデバイスの RJ-45, DB9 あるいは DB25 シリアルコンソールのポートに接続します。
ロールオーバケーブルが必要ですか？	いいえ、SX II のシリアル接続は自動センシングですから、DTE （データ ターミナル装置)と DCE （データ通信装置）のコンソール ポートにロールオーバーケーブルなしで接続できます。SX II は Cisco とその他のコンパティブルなデバイスに RJ-45 コンソールポートにロールオーバケーブルなしで接続できます。
DTE/DCE というのは何でしょう、なぜそれが重要なのでしょうか？	RS-232 シリアルポートは DTE あるいは DCE です。DTE ポートは典型的にはコンピュータあるいはターミナル、すなわちオスの DB9 COM ポートです。DCE はモデム、CSU/DSU、マルチプレックサ あるいは周辺機器に使われます。DTE ポートは典型的に DCE ポートにケーブル接続します。ポート間の接続は特別なロールオーバーケーブルで接続される必要があります。SX II は自動センシングなので、DTE あるいは DCE ポートのどちらでも接続できます。
アダプターが必要ですか？	RJ45 のコンソールポートに接続するには、通常の Cat5 ケーブルがアダプターなしで使えます。Raritan はこれらのタイプのシリアルポートを持つデバイスのためにオスとメスの DB9 と DB25 アダプターを販売しています。アダプターはまた Raritan PX インテリジェント ラック PDU に接続するためにも使用されます。アダプターとピン割り当ての情報については SX II ユーザガイド あるいはオンライン ヘルプを参照してください。
SX II からシリアルデバイスまでの最大距離はいくらですか？	その距離は使用されるボー レートに従って変わります。これは 230K ボーでの 4 フィートから 2.4K ボーでの 300 フィートまでの範囲があります。

シリアルデバイスへの接続

シリアルデバイスへの接続の例は何ですか？

以下の表はどのようにして SX II を標準のネットワークとコンピュータに接続するかを示しています。これはシリアルポートのタイプ（RJ45, DB9 と DB25）とその（オスかメス）によります。必要なアダプターも示します。

Vendor	Models	Serial Port	How to Connect
Cisco	Catalyst	RJ45	Cat5 cable
Cisco	Catalyst	DB25F	ASCSDB25M adapter and CAT5 cable
Cisco	Router	RJ45	Cat5 cable
Cisco	Router	DB25F	ASCSDB25M adapter and CAT5 cable
Cisco	UCS	RJ45	Cat5 cable
Cisco	PIX Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
HP	Servers	DB9M	ASCSDB9F adapter and CAT5 cable
Dell	Servers	DB9M	ASCSDB9F adapter and CAT5 cable
IBM	Servers	RJ45	Cat5 cable
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
Silicon Graphics	Origin	DB9M	ASCSDB9F adapter and CAT5 cable
Sun	SPARCStation	DB25F	ASCSDB25M adapter and CAT5 cable
Sun	Netra T1	RJ45	Cat5 cable
Sun	Cobalt	DB9M	ASCSDB9F adapter and CAT5 cable
Various	Windows	DB9M	ASCSDB9F adapter and CAT5 cable
Raritan	PX	RJ45	CSCSPCS-1 or CSCSPCS-10 cable

インストール、管理、と設定

インストール、管理、と設定

どのようにして最初に SX II をせ設定しますか？	最初の設定は手動で SX II ﾛｰｶﾙコンソールからあるいは自動で USB スティックあるいは TFTP サーバから行えます。手動の設定は CLI 経由でラップトップを(1) USB、(2) シリアルケーブルで接続する、あるいは(3)KVM コンソールを接続する事によって行えます。また(4)ウエブ GUI を使ってラップトップをクロスオーバケーブルで接続して行えます。クイック セットアップ ガイド（QSG）が含まれています。
SX II は CLI によって完全に管理できますか？どこに CLI が定義されていますか？	はい、SX II は CLI コマンドによって完全に管理できます。CLI はオンラインヘルプ、ユーザガイドと CLI それ自身から定義されます。
自動設定のオプションについてもう少し教えてください。	SX II の自動設定方法は 2 通りあります。第 1 に、それは SX II の USB ポートに差し込んだ CLI コマンドのスクリプトによって設定できます。第 2 に、CLI コマンドのスクリプトは DHCP サーバあるいは SX に設定された TFTP サーバ上に保存することができます。セキュリティのため、これらの自動設定方法は管理者によって有効化される必要があります。
SX II はファームウエアのアップグレードに従来の SX と同様に FTP サーバを必要としますか？	いいえ、SX II ファームウエアの更新の手順は KX III と同様です。FTP サーバは必要としません。ユーザは Raritan のウエブサイトからブラウズして暗号化されたファームウエアをダウンロードします。多くの管理機能は Dominion SX III にあるものと同じです。デバイスをこの方法でアップグレードするため CLI 経由で FTP オプションもあることは承知してください。
従来の SX の設定を新しい SX II のコピーできますか？	かなりのハードウエアとソフトウエアの変化があるため、従来の SX の設定バックアップは残念ながら新しい SX II とはコンパティブルではありません。
Dominion SX のための SNMP MIB のコピーはどこで得られますか？	SX II SNMP MIB は raritan.com ポートページの Dominion SX II サポートページにあります。 またウエブ GUI 上のイベント管理 – 設定 ページで得られます。
SX II は Raritan のコマンドセンタで使えますか？	はい。Dominion SX II は Comm と Center Secure Gateway Release 6.1 とそれ以上を必要とし、2015 年 9 月に入手可能となります。Comm と Center を使い、ユーザは Dominion SX、SX II、KXIII に接続

インストール、管理、と設定	
	された何千ものシリアル（と KVM）デバイス、そしてそのほかの Raritan のデバイスに接続できます。
セキュリティ	

セキュリティ

Dominion SX II は安全ですか？	はい、Dominion SX II は軍用グレードの強固なセキュリティ機能を持ち、それには FIPS 140-2 モードと暗号化モジュール付きの AES 暗号化を備えています。SX II はいくつものセキュリティ機能を持ち、各製品は脆弱性走査でテストされています。 セキュリティ パッチは Raritan から入手可能になります。
Dominion SX II は FIPS 140-2 の認証を受けていますか。	Dominion SX II では、FIPS 140-2 実装ガイダンスに従って、Linux プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。この暗号モジュールが Raritan シリアルクライアント (RSC)を用いる際シリアルセッションの暗号化に使用されます。
ActiveDirectory 認証はサポートされていますか？	はい、ActiveDirectory、LDAP、 RADIUS と TACACS+ 認証がサポートされています。さらに SX II の管理者はパスワードを付けてローカルのユーザを作成できます。
どのポートを SX II の接続の際開けておく必要がありますか？	ユーザセッションのためにはポート 443(https 用); オプションでポート 80(http 用) 。SSH を用いるときは、ポート 22 を開けておく必要があります。HTTP, HTTPS, Telnet, SSH のための TCP ポートはすべてユーザが設定できます。これらユーザが設定したポートはアクセスのために開けておく必要があります。 また、TCP ポート 5000 も。
どのようなタイプのログが利用できますか？	SX II は管理的操作とともにユーザアクセス、セキュリティイベントなどのために作成された多くのタイプのイベントをサポートしています。SNMP, Syslog, Email, NFS を含む複数のログ方法と内部ログファイルが利用できます。
シリアルポートのデータはログされますか？	はい、シリアルデバイスからのデータは SX II、Syslog あるいは NFS サーバ上のローカルファイルにログされます。
デフォルトのログインとデフォルトのパスワードは何ですか？	デフォルトのログインは ″admin″ デフォルトのパスワードは ″raritan″ です。SX II に始めてログインした時、パスワードの変更を強制されます。セキュリティの理由からデフォルトのユーザ名 ″admin″ も変更する事をすすめます。ローカルのアカウントのために強力なパスワードを勧めます、それはセキュリティ設定パネルで有効化され

セキュリティ	
	ます。
Dominion SX への admin パスワードを失いました。どうすればよいですか。	そのユニットを出荷時のデフォルトに復元することができます。工場リセット機能はそのユニットを工場出荷時のデフォルト設定に復元することができます。リセット機能にはいくつかの設定可能なオプションがあります。
ユーザインタフェースと説明書	
Dominion SX II はどのようなタイプのウエブベースのユーザインタフェースを持っていますか？	Dominion SX II のグラフィカル ユーザインタフェースはほかの Dominion 製品に類似していて、Dominion SX II, KX, KSX と KX2-101-V2 を通じて共通の使用感覚を提供しています。さらに、ファームウエアの更新、バックアップと復元、セキュリティオプションと診断を含んで類似した管理機能が利用できます。
SX II は Java を必要としますか？	Raritan シリアルコンソールソフトウエアのウェブブラウザでのアクセスのため、Java が必要です。SSH, Telnet あるいはラックでの接続経由の SX II への CLI アクセスには Java は必要ようありません。
どこで Dominion SX II の説明書（ユーザガイドなど）を入手できますか？	SX II の製品ページにあるデータシートは、SX の良い概要を提供していて入手可能なモデル、アダプターと機能を示しています。SX II の製品ページはまた、機能と利点の記述も提供しています。SX II のサポートページはリリースノート、ユーザマニュアル、オンラインヘルプ、 SX II MIB とファームウエア リリースを含む詳細な技術的情報を提供しています。

Ap D SX II のサポート

Raritan のテクニカル サポートとお客様サポートに加え、次の情報も利用可能です。

この章の内容

SX II リリース ノートとヘルプ

SX II リリース ノート

リリースノートが SX II 装置とともに配達されまた Raritan ウエブサイトのサポートページにもあります 。

装置を使用する前に、リリースノートに重要な情報をチェックしてください。

SX II クイック セットアップ ガイド

オンラインヘルプが使えます。また **SX II クイック セットアップ ガイド**が SX II に含まれていますし、Raritan のウエブサイトのサイトページのサポートページにも見つけられます。 。

SX II オンライン ヘルプ

SX II オンライン ヘルプは、プライマリ ヘルプ ソースと見なされます。

Raritan Serial Console (RSC) ヘルプは SX II オンラインヘルプの一部として提供されます。

オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。

SX II ユーザガイドと管理者ガイド

最終ユーザに特定した内容の PDF バージョンが SX II のユーザガイドに含まれていて、SX II 管理者に特定した内容は SX 管理者ガイドに含まれています。

どちらの PDF も Raritan ウエブサイトのサポートページにあります。 。

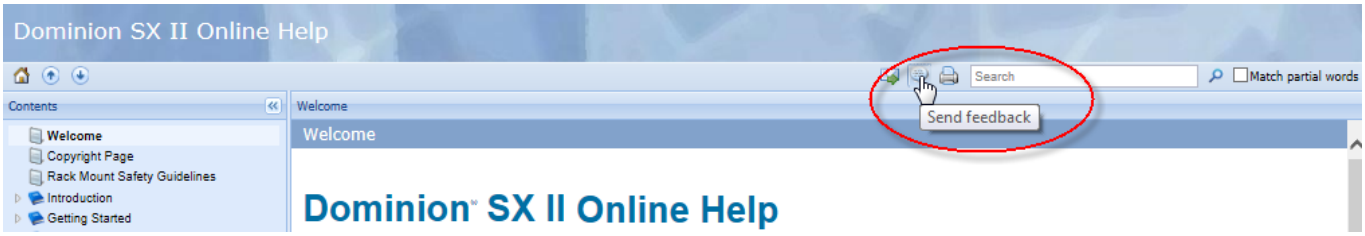
文書チームにフィードバックを届ける

文書係にオンラインヘルプあるいはユーザガイドに関連した質問やフィードバックを直接届けてください。

次にＥ メール下さい： documentation@raritan.com, あるいはオンラインヘルプから直接に次の一つを使ってください：

オンラインヘルプにある「フィードバックを送る」機能を用います：

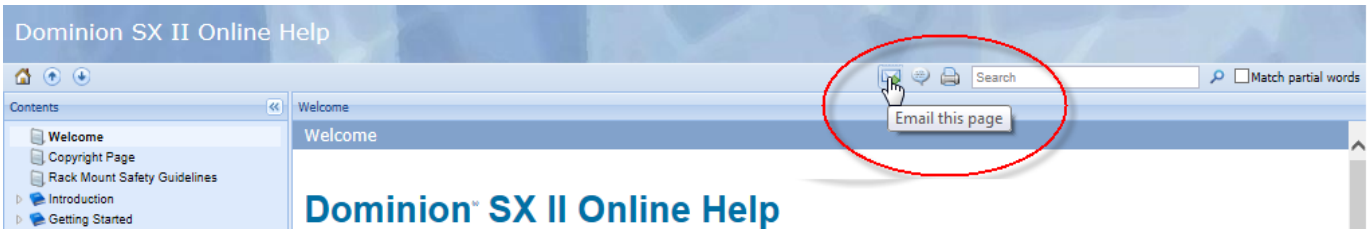
- オンライン ヘルプを開き、ツールバーにある「フィードバックを送る」のアイコンをクリックします。デフォルトのｅメールクライアントにあるチーム宛のｅメールアドレスが開きます。



文書係にオンラインヘルプの特定の内容についてｅメールします。

- オンラインヘルプのその内容のを開け、オンラインヘルプのツールバーから「このページをｅメールする」のアイコンをクリックします。

  デフォルトのｅメールクライアントにあるチーム宛のｅメールアドレスが開きます。



注:この方法によるフィードバックは オンラインヘルプの内容だけに限られ、 技術サポート、販売、ウエブサイト、あるいは製品情報に関するものではありません。Raritan のウエブサイトのご連絡のページでその他の連絡情報について参照してください。