Dominion KX II-101

ユーザ ガイド

リリース 2.0

KX2101-0A-J
2008 年 2 月
255-62-4031-00

FCC 情報

この装置は FCC 規則のパート 15 による Class A デジタル装置の制限に準拠することが試験により証明されています。これらの制限は、商業上の設置における有害な干渉を防止するために設けられています。この装置は、無線周波数を生成、利用、放射する可能性があるので、指示に従った設置および使用をしないと、無線通信への干渉を招く恐れがあります。この装置を居住環境で操作すると、干渉を招く場合があります。

VCCI 情報 (日本)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス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。

事故、自然災害、本来の用途とは異なる使用、不正使用、Raritan 社以外による製品の変更、その他 Raritan 社が関与しない範囲での使用や、通常の運用条件以外での使用による製品の故障については、Raritan 社は一切責任を負いかねます。

CE c UL us LISTED 1F61 I.T.E.

目次

1 はじめに

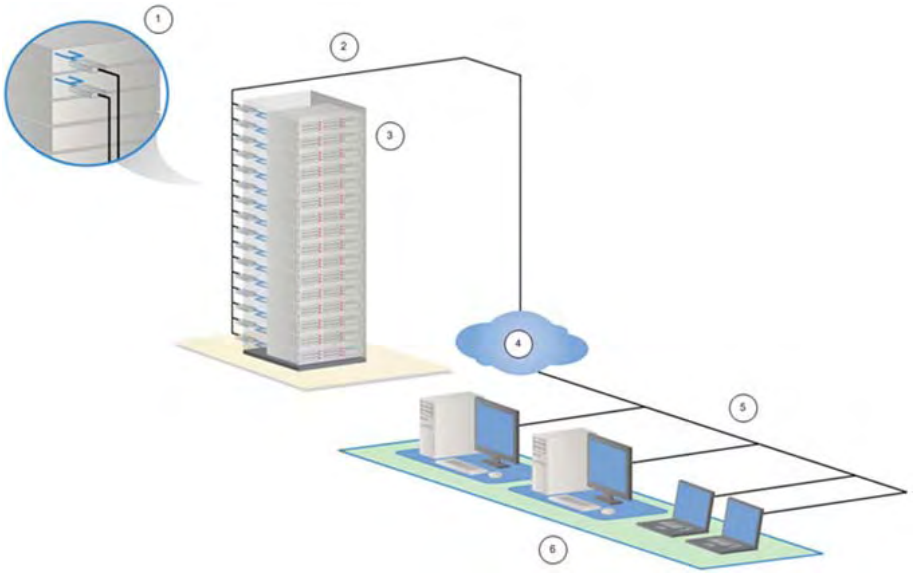
この章の内容

Dominion KX II-101 の概要

Dominion KX II-101 をご購入いただきありがとうございます。 KX II-101 は、ターゲット サーバへの接続用の 1 つのキーボード、ビデオ、およびマウス (KVM) ポートおよび IP ネットワークへの接続用の 1 つの IP ポートを提供します。 KX II-101 ユニット内では、サーバからの KVM 信号が IP 形式に変換され、IP ネットワーク経由で送信するために圧縮されます。

KX II-101 外付けで小型なサイズにより、ターゲット サーバ近くにインストールすることが容易に行え、各 KX II-101 ユニットは、独自の IP アドレスを持ちます。各ユニットは、Power-over-Ethernet (PoE) または外部の AC-DC パワー パック経由で電源が供給できます。

Dominion KX II-101 はスタンドアロン装置として操作ができ、また、Raritan の CommandCenter Secure Gateway (CC-SG) 管理アプライアンスを使用して、別の Raritan アクセス製品と併用し単一の論理ソリューション内に統合することもできます。



1 KX II-101

2 LAN

3 Windows、Linux、Sun サーバ。

4 TCP/IP

5 LAN

6 リモート (Network) アクセス

製品の写真

製品の特長

インタフェース

- 組み付けの PS/2 KVM 接続ケーブル
- 制御および仮想メディア用に選択できる USB 接続
- 初期デバイス設定、診断、外部モデム アクセス用のシリアル管理ポート
- 10/100-base-T 自動検出、全二重をサポートする Ethernet LAN ポート
- LED ネットワーク アクティビティ インジケータとステータス
- バックライト LED によるパワー ON インジケータ

ネットワーク設定

- DHCP または固定 IP デバイス アドレス

システム管理機能

- Ethernet 経由でアップグレード可能なファームウェア
- フェールセーフ ファームウェア アップグレード機能
- 管理者設定可能な時刻またはネットワーク タイム プロトコル (NTP/SNTP) サーバとの同期
- 管理者で選択可能なローカル時刻情報付き管理者操作ログ SNMP V2 エージェント
- RADIUS および LDAP 認証プロトコルをサポート

管理の特長

- Web ベース管理
- LDAP、Active Directory、RADIUS、または内部認証および認可
- DHCP または固定 IP アドレス指定
- Raritan の CommandCenter Secure Gateway (CC-SG) 管理アプライアンスとの統合

ユーザ機能

- 共通のブラウザによる Web ベースのアクセス
- わかりやすいグラフィカル ユーザ インタフェース (GUI)
- 複数のリモート ユーザを有効にする “PC Share” モード
- TCP 通信
- 英語ユーザ インタフェース
- 仮想メディア アクセス
- ずれないマウス同期
- プラグ&プレイ
- ビデオおよび仮想メディアを含む全 KVM 信号の 256 ビット暗号化

電源

- Class 2 Power-over-Ethernet (PoE) による電源供給
- 外部の AC-DC 電源アダプタによる代替電源

ビデオ解像度

- 60 Hz まで最大 1600X1200 の解像度

取り付け

- ラック マウント ブラケット

  詳細については、「*ラック マウント*『p. 190』」を参照してください。

パッケージの内容

各 KX II-101 ユニットには、次の物品が同梱されています。

- メイン ユニット KX II-101 - KVM over IP
- USB タイプ A 対タイプ B ミニ コネクタ
- AC 電源アダプタ - AC-DC 6VDC
- 海外での使用に応じた 3 つの追加の電源コンセント プラグ
- ミニ DIN - DB9 シリアル ケーブル
- マウント ブラケット キット
- Raritan ユーザ マニュアル & クイック セットアップ ガイド CD-ROM
- クイック ステップ ガイド
- アプリケーション ノート (該当する場合)
- テクニカル ノート (該当する場合)

用語

ターゲット サーバ	KX II-101 経由でリモートでアクセスされるサーバとその接続済み KVM の設定。
リモート PC	KX II-101 に接続しているターゲット サーバへのアクセスとその制御に使用する、Windows、Linux、Solaris、Apple Macintosh® コンピュータ。
管理シリアル ポート	KX II-101 は管理シリアル ポートを使用して準備されます。 付属のミニ DIN - DB9 ケーブルを使用して、PC のシリアル ポートを KX II-101 ユニットの管理シリアル ポートに接続します。 次に、標準のターミナル エミュレーション ソフトウェア (例、HyperTerminal) を使用して、管理シリアル ポートにアクセスします。管理シリアル ポートはネットワークの設定に利用されます。
ローカル ユーザ ポート	ターゲット サーバの直近にいるユーザが KX II-101 を取り外さないでサーバに接続されていたキーボードとマウスを使用できるようにするポートです。
仮想メディア	KVM ターゲット サーバがクライアント PC やネットワーク ファイル サーバからメディアにリモートでアクセスできるようにします。

オプションのアクセサリ

- DB15 から PS/2 および VGA へのローカル ユーザ ケーブル

詳細については、「*コネクタ* 『p. 189』」を参照してください。

2 重要な情報

この章の内容

ログイン

- KX II-101 のデフォルトのログイン ユーザ名は **admin** 、デフォルトのパスワードは **raritan** です。 このユーザは、管理者特権を有します。
- パスワードは大文字と小文字が区別されるため、大文字と小文字は作成したとおりに正確に入力する必要があります。
- デフォルトのパスワード raritan は、すべて小文字で入力してください。
- セキュリティを確保するために、デフォルトのパスワードはできるだけ早く変更してください。

デフォルト IP アドレス

KX II-101 は、出荷時に固定 IP アドレス (192.168.0.192) が設定されています。DHCP サーバを使用していないネットワークでは、KX II-101 シリアル管理コンソールまたは KX II-101 リモート コンソールを使用して、新しい固定 IP アドレス、ネット マスク、およびゲートウェイ アドレスを設定する必要があります。

リモート コンソールを使用して IP アドレスを KX II-101 に割り当てる詳細については、「***IP アドレスの割り当て*** 『p. 21』」を参照してください。 シリアル管理コンソールを使用して IP アドレスを設定する詳細については、「***ローカル シリアル コンソールの使用*** 『p. 25の"ターミナル エミュレーション プログラムの使用"参照先 』」を参照してください。

サービス パック

- Microsoft Internet Explorer Version 5.01 または Windows 2000 と KX II-101 を使用する場合は Service Pack 4 (SP4) 以上にアップグレードする必要があります。

3 インストールと設定

この章の内容

ターゲット サーバの設定

この章では、KX II-101 のインストールおよび設定方法について説明します。 インストールと設定は、次の手順で構成されています。

1. ***ターゲット サーバの設定***『p. 7』
2. ***ネットワーク ファイアウォールの設定***『p. 19』
3. ***KX II-101 の接続***『p. 14』
4. ***KX II-101 の設定***『p. 19』

KX II-101 をインストールする前に、次の概説のように KX II-101 を経由してアクセスするターゲット サーバを設定し、パフォーマンスを最適にします。 次の設定条件は、KX II-101 へのリモート アクセスに使用するコンピュータではなく、ターゲット サーバのみに適用されます。

サーバ ビデオ解像度の設定

最適な帯域効率とビデオ パフォーマンスを得るために、Windows、X-Windows、Solaris、および KDE などのグラフィカル ユーザ インタフェースを実行するターゲット サーバは、デスクトップの背景を無地でシンプルな明るい色の表示に設定します。 写真や複雑な階調を持つ背景は避けてください。

サーバのビデオ解像度とリフレッシュ レートが KX II-101 でサポートされていることと、信号がノンインタレースであることを確認します。 KX II-101 は次のビデオ解像度をサポートします。

テキスト モード〉

640x480、60Hz
640x480、72Hz
640x480、75Hz
640x480、85Hz
800x600、56Hz
800x600、60Hz
800x600、72Hz
800x600、75Hz
800x600、85Hz
1024x768、60Hz
1024x768、70Hz
1024x768、75Hz
1024x768、85Hz
1152x864、60Hz
1152x864、75Hz
1280x1024、60Hz
1600 x 1200、60Hz

Sun ビデオ解像度の設定

Sun システムには、コマンド ライン解像度と GUI 解像度の 2 種類の解像度設定があります。 KX II-101 でサポートされる解像度の詳細については、「***サーバ ビデオ解像度の設定*** 『p. 8』」を参照してください。

注: サポートされる解像度が機能しない場合は、モニタがマルチシンクであることを確認してください。 一部のモニタは、H and V sync では動作しません。

コマンド ライン解像度

➢ *コマンド ライン解像度を確認するには、以下の手順に従います。*

- 次のコマンドを root から実行します。

```
# eeprom output-device
```

➢ *コマンド ライン解像度を変更するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# eeprom output-device=screen:r1024x768x75
```

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

2. コンピュータを再起動します。

GUI 解像度/32 ビット

➢ *32 ビット カードの GUI 解像度を確認するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# /usr/sbin/pgxconfig –prconf
```

➢ *32 ビット カードの GUI 解像度を変更するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# /usr/sbin/pgxconfig –res1024x768x75
```

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

2. コンピュータを再起動します。

GUI 解像度/64 ビット

➢ *64 ビット カードの GUI 解像度を確認するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# /usr/sbin/m64config –prconf
```

➢ *64 ビット カードの GUI 解像度を変更するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# /usr/sbin/m64config –res1024x768x75
```

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

2. コンピュータを再起動します。

GUI 解像度/Solaris 8

➢ *32 ビットおよび 64 ビット カードの Solaris 8 の解像度を確認するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# /usr/sbin/fbconfig –prconf
```

➢ *32 ビットおよび 64 ビット カードの Solaris 8 の解像度を変更するには、以下の手順に従います。*

1. 次のコマンドを実行します。

```
# /usr/sbin/fbconfig –res1024x768x75
```

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

2. コンピュータを再起動します。

マウス モード

KX II-101 は、次のマウス モードで動作します。 ずれないマウス (Absolute Mouse Synchronization™)、インテリジェント マウス モード (アニメーション カーソルを使用しないでください)、および標準マウス モード。 ずれないマウス (Absolute Mouse Synchronization) の場合は、マウス パラメータを変更する必要はありません。 標準マウス モードとインテリジェント マウス モードの場合、このセクションの説明に従って、マウス パラメータを特定の値に設定する必要があります。

このセクションでは、さまざまなシステムで必要なマウスの設定について説明します。

Windows Vista

➢ *マウスを設定するには、以下の手順に従います。*

1. [スタート]、[設定]、[コントロール パネル]、[マウス] の順に選択します。
2. [ポインタ オプション] タブをクリックします。 [速度] グループで、以下の操作を行います。
   a. ポインタの速度設定をちょうど中間の速度に設定します。
   b. [ポインタの精度を高める] オプションをオフにします。
3. [OK] をクリックします。

➢ *アニメーション効果とフェード効果を無効にするには、以下の操作を行います。*

1. Windows の [スタート] メニューから、[コントロール パネル]、[システム] 、[システムの詳細設定] を選択します。 [システムのプロパティ] ダイアログ ボックスが表示されます。
2. [詳細設定] タブをクリックします。
3. [パフォーマンス] グループの [設定] ボタンをクリックします。 [パフォーマンス オプション] ダイアログ ボックスが表示されます。
4. [カスタム] オプションで、以下のチェックボックスをオフにします。
   - Windows 内のアニメーション コントロールと要素
   - ウィンドウを最大化や最小化するときにアニメーションで表示する
   - メニューをフェードまたはスライドして表示する
   - ヒントをフェードまたはスライドで表示する
   - メニュー項目をクリック後にフェード アウトする
5. [OK] をクリックします。

6. [コントロール パネル] を閉じます。

Windows XP の設定

Microsoft Windows XP が稼動している KVM ターゲット サーバで、[ポインタの精度を高める] オプションをオフにし、[ポインタの速度を選択する] で、速度をちょうど中速に設定します。 これらのパラメータは、[コントロール パネル]、[マウス]、[マウス ポインタ] の順に選択すると表示できます。

注: Windows 2000 または XP を実行しているターゲット サーバの場合、KX II-101 を介したリモート接続用に、専用のユーザ名を作成することが可能です。 これにより、他のユーザが高速なマウス速度を求めている場合に、ターゲット サーバのマウス ポインタの速度や加速を KX II-101 接続専用に遅く設定できます。

注: Windows XP と 2000 のログイン画面では、マウスのパラメータが、最適な KX II-101 パフォーマンス用に提案されたパラメータとは異なる、プリセットされたパラメータに戻ります。このため、これらの画面ではマウス同期は最適になりません。 Windows ターゲット サーバのレジストリを調節でき場合は、Windows レジストリ エディタを使って次の設定を変更することにより、ログイン画面で KX II-101 のマウスの同期を改善することができます。Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0

Windows 2000 の設定

Microsoft Windows 2000 が稼動しているターゲット サーバで、マウス ポインタの加速を [なし] に設定し、ポインタの速度をちょうど中速に設定します。 これらのパラメータは、[コントロール パネル]、[マウス] の順に選択すると表示できます。

Linux の設定

Linux グラフィカル インタフェースを実行しているターゲット サーバで、マウスの加速値を 1 に設定し、しきい値も 1 に設定します。

前述のように、Linux を実行しているターゲット サーバが、KX II-101 でサポートされている解像度を、標準 VESA 解像度および垂直走査周波数で使用していることを確認します。 また、ブランキング時間が VESA の標準値の +/- 40% 以内になるように Linux ターゲット サーバを設定することも必要になります。

➢ *これらのパラメータを確認するには、以下の手順に従います。*

1. Xfree86 設定ファイル XF86Config を表示します。
2. テキスト エディタを使用して、KX II-101 でサポートされてていない解像度をすべて無効にします。
3. KX II-101 でサポートされていない仮想デスクトップ機能を無効にします。
4. ブランキング時間を確認します (VESA 標準の +/- 40%)。

5. コンピュータを再起動します。

注: ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ (プラス記号) を押すと、XF86Config ファイルで有効になっているすべての解像度が順にスクロールされ、ビデオ解像度を変更できます。

Sun Solaris の設定

Solaris ターゲット サーバは、KX II-101 でサポートされているいずれかの表示解像度に設定する必要があります。 Sun マシンで一般的にサポートされる解像度を以下に示します。

1024x768@60Hz

1024x768@70Hz

1024x768@75Hz

1024x768@85Hz

1280x1024@60Hz

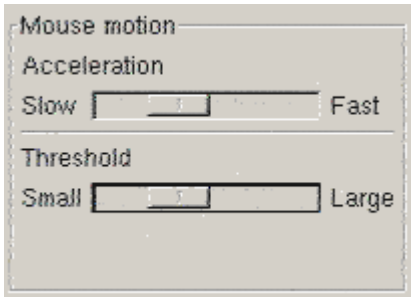
Solaris オペレーティング システムが稼動しているターゲット サーバのビデオ出力は VGA である必要があります (コンポジット Sync ではなく H-and-V Sync)。 Sun のビデオ カード出力をコンポジット Sync からデフォルト以外の VGA 出力に変更するには、最初に Stop+A コマンドを発行して bootprom モードに移行します。 次に、以下のコマンド、

```
# eeprom output-device=screen:r1024x768x75
```

を発行して出力解像度を変更します。 次に、boot コマンドを実行して、サーバを再起動します。

または、Raritan 社の代理店からビデオ出力アダプタを購入することもできます。 コンポジット Sync 出力を使用する Sun では、KX II-101 で使用するために、APSSUN II Raritan Guardian が必要です。 独立同期出力を使用する HD15 Sun では、KX II-101 で使用するために、APKMSUN Raritan Guardian が必要です。 KX II-101 は、APSUSB アダプタを使用した PS/2 バージョンのみをサポートします (コンポジット Sync はサポートされていません)。

Solaris オペレーティング システムを実行しているターゲット サーバで、マウスの加速値を正確に 1 に設定し、しきい値も正確に 1 に設定します。 これは、グラフィカル ユーザ インタフェース (下記) で設定するか、コマンド ライン "xset mouse a t" を使用して設定します。ここで、 "a" は加速値、"t" はしきい値です。



Apple® Macintosh の設定

ずれないマウス (Absolute Mouse Synchronization) を使用します。

KX II-101 の接続

KX II-101 には、下の図に示す物理接続が用意されています。

1 付属モニタおよび PS/2 ケーブル (項目 3 を参照)

2 ミニ USB ポート。 付属の USB ケーブルを使用してデバイスをターゲット サーバに接続するために使用します (付属の PS/2 ケーブルを使用しない場合)。 ずれないマウスと仮想メディア機能を使うには、USB で接続する必要があります。

3 組み付けのビデオおよび PS/2 ケーブル。 デバイスをモニタおよびターゲット サーバに接続するために使用します (USB ケーブルを使用しない場合)。

4 ローカル ユーザ ポート。 オプションのビデオおよび PS/2 ケーブルを使用して、ローカル キーボード、ビデオ、マウスをターゲット サーバに直接接続するために使用します。

5 Ethernet LAN/PoE ポート。 LAN 接続および電源 (PoE LAN 接続を使用している場合) を供給します。

6 電源コネクタ。 PoE (Power over Ethernet) LAN 接続を使用していない場合は、電源を接続します。

7 バックライト LED パワー ON および起動インジケータ。 デバイスの動作ステータス情報を表示します。

8 [Admin Port] (管理ポート)。 次のいずれかの作業を行うために使用します。

設定用の PC 上でターミナル エミュレーション プログラムを使用してデバイスを設定および管理を実行します。

パワー ストリップを設定および管理します。

デバイスにダイヤルインする外部モデムを接続します。

ターゲット サーバへの接続

KX II-101 では、組み付けの PS/2 ケーブルまたは付属の USB ケーブルを使用してターゲット サーバに接続できます。 接続する前に、「***サーバ ビデオ解像度の設定*** 『p. 8』」の説明に従って、ターゲット サーバのビデオをサポートされる解像度および垂直走査周波数に設定します。

PS/2 の設定

➢ *PS/2 ターゲット サーバで使用するように KX II-101 を設定するには、以下の手順に従います。*

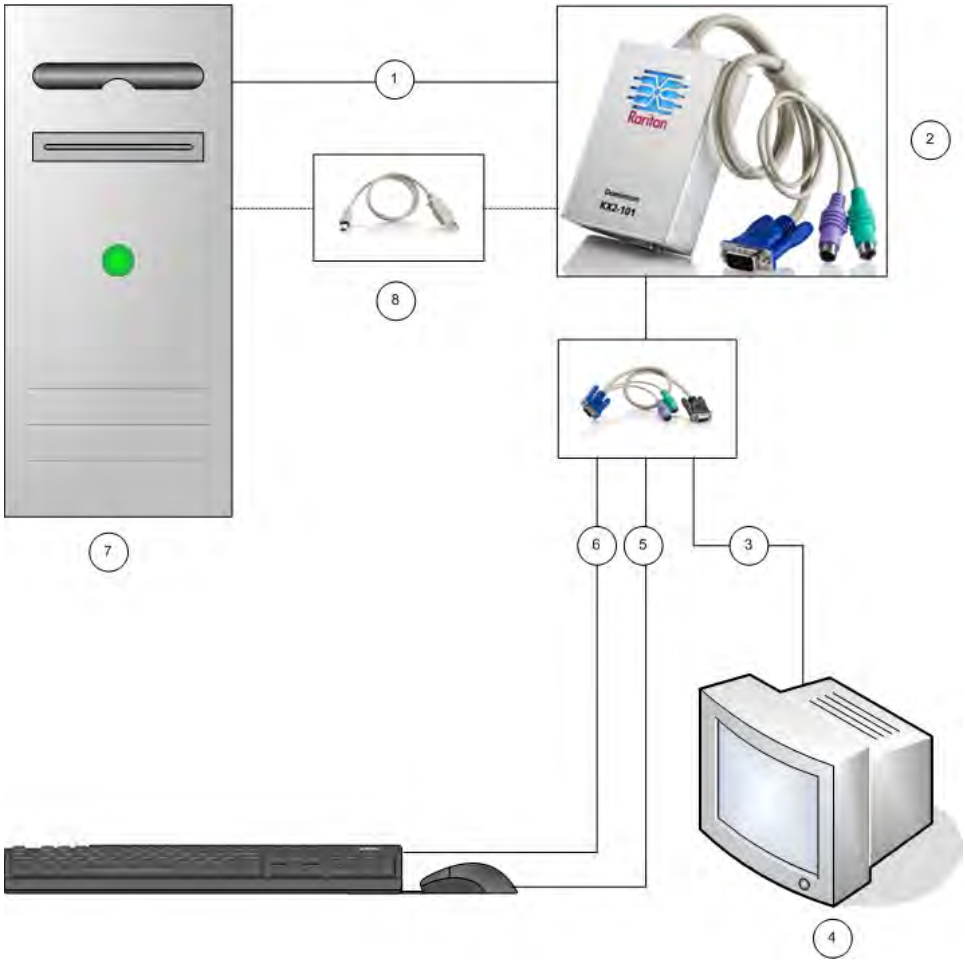
1. 組み付けのキーボード、ビデオ、マウス ケーブルを使用して KX II-101 をターゲット サーバに接続します。
2. オプションの PS/2 ケーブルを使用して、ローカルのキーボード、ビデオ、マウスを KX II-101 のローカル ユーザ ポートに接続します。

注: ローカル ユーザ ポートが機能するには、KX II-101 の電源が投入されている必要があります。

---

3. 仮想メディア (VM) 接続が必要な場合は、ミニ USB コネクタを KX II-101 に接続し、USB コネクタをターゲット サーバの USB ポートに接続します。

完了したら、下の図に示すような接続を得ることができます。



1 KX II-101 からターゲット サーバへの統合 PS/2 キーボード、ビデオ、マウスの接続

2 KX II-101

3 ローカル モニタへのビデオ接続 (オプション ケーブル)

4 ローカル モニタ

5 KX II-101 からマウスへの PS/2 接続 (オプション ケーブル)

6 KX II-101 からキーボードへの PS/2 接続 (オプション ケーブル)

7 ターゲット サーバ

8 KX II-101 からターゲット サーバへの付属のミニ USB - USB コネクタ、仮想メディア接続用

USB の設定

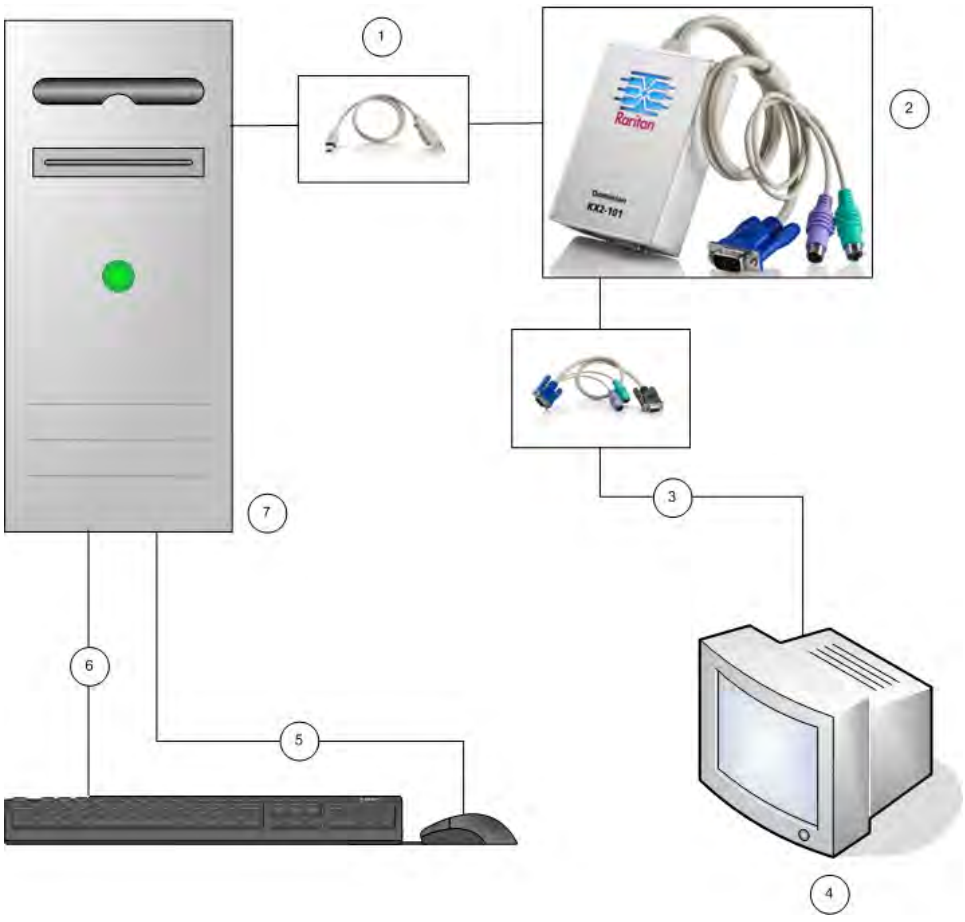
➢ *USB ターゲット サーバに KX II-101 を設定するには、以下の手順に従います。*

1. ミニ USB コネクタを KX II-101 に接続し、USB コネクタをターゲット サーバの USB ポートに接続します。
2. オプションの PS/2 DKX2-101-LPKVMC ケーブルを使用して、ローカル ビデオのみを KX II-101 のローカル ユーザ ポートに接続します。

   注: ローカル ユーザ ポートが機能するには、KX II-101 の電源が投入されている必要があります。

3. USB ケーブルを使用して、キーボードとマウスをターゲット サーバに直接接続します。

   完了したら、下の図に示すような接続を得ることができます。



1 KX II-101 からターゲット サーバへの付属のミニ USB - USB ケーブル

2 KX II-101

3 ローカル モニタへのビデオ接続 (オプション ケーブル)

4 ローカル モニタ

5 ターゲット サーバからマウスへの USB 接続

6 ターゲット サーバからキーボードへの USB 接続

7 ターゲット サーバ

ネットワークへの接続

標準 Ethernet ケーブルを、「LAN」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。 Ethernet 接続の上にある LAN LED は Ethernet のアクティビティを示します。 KX II-101 を使用中は、黄色の LED が点滅し、10Mbps の IP トラフィックを示します。 緑色のライトは 100Mbps の接続速度を示します。

KX II-101 への電源供給

KX II-101 には、標準付属の AC 電源アダプタまたは PoE (Power over Ethernet) により電源を供給できます。

- 標準の AC 電源の場合は、AC 電源アダプタ キットの片側のプラグをパワー ポートに挿し込み、もう一端を近くの電源コンセントに挿し込みます。
- PoE の場合は、10/100Mbps ケーブルを LAN ポートに指し込み、もう一端を PoE の給電された LAN に差し込みます。

KX II-101 は電源を ON にすると、起動シーケンスに進みます。この間、青色の Raritan ロゴ LED が約 45 秒間点滅します。起動が完了すると、バックライト LED が点灯したままになります。

Admin ポートの使用

Admin ポートを使用すると、HyperTerminal のようなターミナル エミュレーション プログラムを使用して、KX II-101 の設定とセットアップを実行できます。 付属のシリアル ケーブルのミニ DIN 側端部を KX II-101 の Admin ポートに指し込み、DB9 側の端部を PC またはラップトップのシリアル ポートに差し込みます。 シリアル接続の設定は、次の設定値にします。 115,200 Baud、8 データ ビット、1 ストップ ビット、パリティなし、フロー制御なし。

Admin ポートを使用して KX II-101 を設定する方法の詳細については、「ターミナル エミュレーション プログラムの使用」を参照してください。

ローカル ユーザ ポートの使用

KX II-101 では、オプションのビデオおよび PS/2 ケーブルを使用できます。これらのケーブルを使用して、LOCAL USER ポート経由でキーボードやマウスをターゲットサーバに接続できます。 LOCAL USER ポートは、KX II-101 の接続先ターゲットサーバへのパススルーとして機能し、それ以外の目的はありません。 LOCAL USER ポートが機能するには、KX II-101 の電源が投入されている必要があります。

注: ローカル ポートでは、PS/2 ホスト インタフェース接続のみがサポートされており、PS/2 コネクタを使用して KX II-101 に接続した後、ターゲット サーバを再起動する必要があります。

ネットワーク ファイアウォールの設定

ネットワーク ファイアウォールを介して KX II-101 にアクセスするには、ファイアウォールが TCP ポート 5000 での通信を許可している必要があります。または、KX II-101 の設定メニューで、指定した別の TCP ポートを使用することもできます。

KX II-101 の Web アクセス機能を活用するには、ファイアウォールが TCP ポート 443 (HTTPS 通信用の標準 TCP ポート) でのインバウンド通信を許可しておく必要があります。 HTTP 要求を HTTPS にリダイレクトする (これにより、ユーザは "https://xxx.xxx.xxx.xxx" の代わりに、より一般的な "http://xxx.xxx.xxx.xxx" を入力できます) KX II-101 の機能を活用するには、ファイアウォールが TCP ポート 80 (HTTPS 通信用の標準 TCP ポート) でのインバウンド通信も許可している必要があります。

KX II-101 の設定

KX II-101 は、次の 2 とおりの方法で設定できます。

- Web ベース KX II-101 リモート コンソールを使用する。この場合、ユニットは操作用 PC へのネットワーク接続を確立している必要があります。
- HyperTerminal のようなターミナル エミュレーション プログラムを使用する。この場合、ユニットの Admin ポートから操作用 PC への直接接続が必要です。この接続用のケーブルは KX II-101 に付属されています。

このセクションでは、両者の方法での KX II-101 の設定手順について説明します。

リモート コンソールの使用

KX II-101 リモート コンソールは、ユニットを使用および管理する前に設定できる Web ベースのアプリケーションです。 リモート コンソールを使用して KX II-101 を設定する前に、操作用 PC とユニットをネットワークに接続しておく必要があります。

KX II-101 を設定するには、以下の手順に従います。

- デフォルトのパスワードに代わる新しいパスワードを設定します。
- IP アドレスを割り当てます。
- ターゲット サーバに名前を付けます。
- ユーザおよびグループを作成します。

新しいパスワードの設定

リモート コンソールに最初にログインすると、デフォルトのパスワードに代わる新しいパスワードの設定を求めるプロンプトが表示されます。 その後、KX II-101 の設定ができます。

1. KX II-101 ユニットへのネットワーク接続可能な操作用 PC にログオンします。
2. サポートされる Web ブラウザ (Internet Explorer (IE) や Firefox など) を起動します。
3. ブラウザのアドレス フィールドに、ユニットのデフォルトの IP アドレス (下記) を入力します。

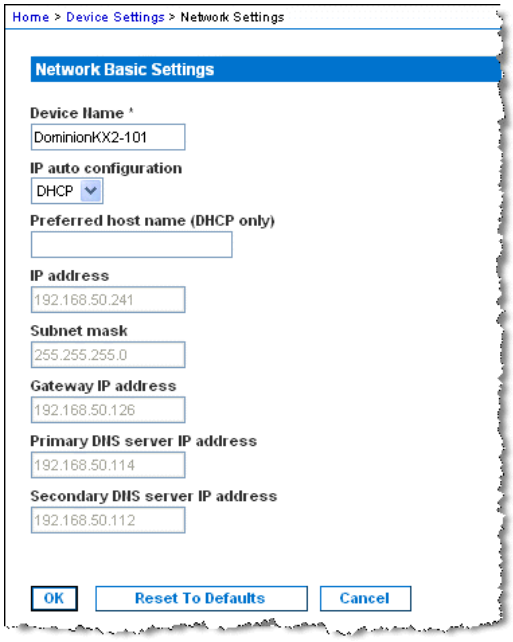
   192.168.0.192
4. Enter キーを押します。 ログイン ページが開きます。
5. ユーザ名に「admin」、パスワードに「raritan」と入力します。
6. [Login] (ログイン) をクリックします。

   [Change Password] (パスワードの変更) ページが表示されます。
7. [Old Password] (旧パスワード) フィールドに「raritan」と入力します。
8. [New Password] (新しいパスワード) フィールドに新しいパスワードを入力し、[Confirm New Password] (新しいパスワードの確認) フィールドに新しいパスワードを再入力します。 パスワードには、英数字と印刷可能な特殊文字を 64 文字まで使用できます。
9. [Apply] (適用) をクリックします。

   パスワードが正常に変更された旨のメッセージが表示されます。
10. [OK] をクリックします。 [Port Access] (ポート アクセス) ページが開きます。

IP アドレスの割り当て

1. KX II-101 リモート コンソールで、[Device Settings] (デバイス設定) の [Network Settings] (ネットワーク設定) を選択します。 [ネットワーク基本設定] (Network Basic Settings) ページが開きます。



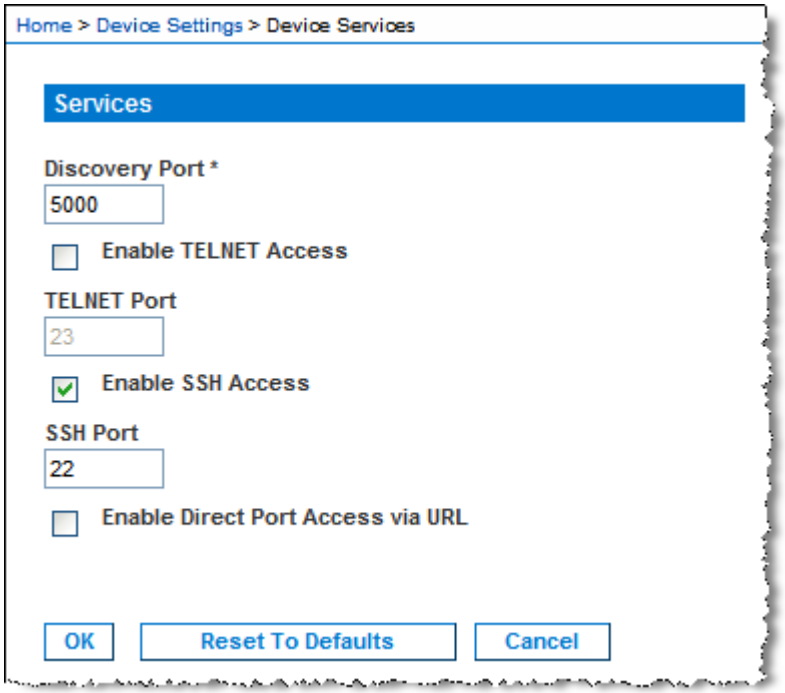
2. [Device Name] (デバイス名) フィールドで、最大 16 文字の英数字と特殊文字を組み合わせて (スペースは使用できません)、KX II-101 ユニットのわかりやすいデバイス名を指定します。
3. [IP auto configuration] (IP 自動設定) ドロップダウン リストで、IP 設定を選択します。
   - [None] (なし) (静的 IP)。 Dominion KX II-101 はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、これはデフォルトの推奨されるオプションです。 このオプションを選択した場合は、ネットワークの IP アドレスを手動で指定する必要があります。
   - [DHCP]。 このオプションを選択した場合、KX II-101 を起動するたびに、ネットワーク パラメータは DHCP サーバによって割り当てられます。

ダイレクト ポート アクセスの設定

➢ *ダイレクト ポート アクセスを設定するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。 [Device Services] (デバイス サービス) ページが開きます。

2. [Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) チェックボックスをオンにします。
3. グローバル Telnet または SSH アクセスを有効にします。
   - [Enable TELNET Access] (TELNET アクセスを有効にする) チェックボックスをオンにして、TELNET アクセスを有効にします。
   - [Enable SSH Access] (SSH アクセスを有効にする) チェックボックスをオンにして、SSH アクセスを有効にします。
4. 選択したアクセス タイプの有効な TCP ポートを指定します。 たとえば、Telnet TCP ポートを介したダイレクト ポート アクセスは 7770 として設定できます。

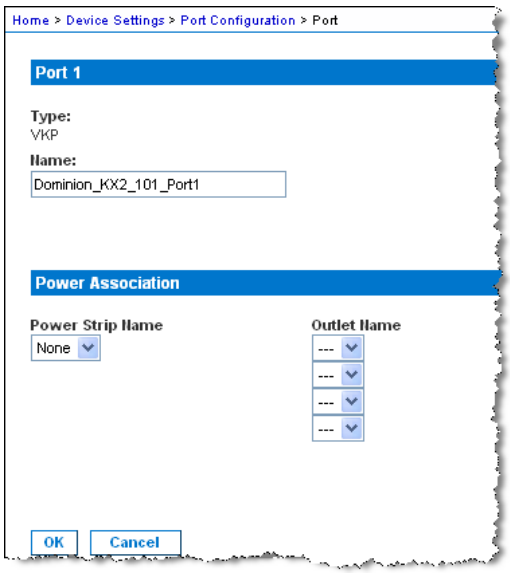


5. [OK] をクリックしてこの情報を保存します。

ターゲット サーバに名前を付ける

1. 「*KX II-101 への接続*『p. 30』」の説明に従って、KX II-101 をターゲット サーバに接続します (まだ接続していない場合)。
2. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。 [Port Configuration] (ポート設定) ページが開きます。

3. ターゲット サーバのポート名をクリックします。 [Port] (ポート) ページが開きます。



4. 名前を入力します (英数字と特殊文字を 32 文字まで入力できます)。
5. [OK] をクリックします。

ユーザとグループの作成

ユーザ グループは、ローカル認証およびリモート認証 (RADIUS または LDAP) で使用されます。 個別のユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。

➢ *ユーザ グループを作成するには、以下の手順に従います。*

1. 次の方法のいずれかを使用して、[Group] (グループ) ページを開きます。
   a. [User Management] (ユーザ管理) の [Add New User Group] (新規ユーザ グループの追加) を選択します。または、
   b. [User Group List] (ユーザ グループ リスト) ページの [Add] (追加) ボタンをクリックします。
2. [Groupname] (グループ名) フィールドに、新しいユーザ グループの名前を入力します。
3. グループの許可を設定します。 このグループに属するすべてのユーザに対して割り当てる許可について、その許可の左にあるチェックボックスをオンにします。

4. [Port Permissions] (ポート権限) ([Access] (アクセス)、[VM Access] (VM アクセス)、[Power Control] (電源管理)) を設定します。 このグループに属するユーザがアクセスできるサーバ ポートと、そのアクセスのタイプを指定します。 デフォルトでは、VM (仮想メディア) アクセスは他のポート権限と同様にオフになっています。 仮想メディアを使用するには、許可を有効にする必要があります。
5. [OK] をクリックします。

➢ *新規ユーザを作成するには、以下の手順に従います。*

1. 次の方法のいずれかを使用して、[User] (ユーザ) ページを開きます。
   a. [User Management] (ユーザ管理) の [Add New User] (新規ユーザの追加) を選択します。または、
   b. [User List] (ユーザ リスト) ページの [Add] (追加) ボタンをクリックします。
2. [Username] (ユーザ名) フィールドに、一意のユーザ名を入力します (最大 16 文字)。
3. [Full Name] (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 (最大 64 文字)。
4. [Password] (パスワード) フィールドにパスワードを入力し、[Confirm Password] (パスワードの確認) フィールドにパスワードを再入力します (最大 64 文字)。
5. [User Group] (ユーザ グループ) ドロップダウン リストからグループを選択します。 このリストには、システムによって定義されているデフォルト グループ ([Admin] (管理者)、[<Unknown>] (不明)、[Individual Group] (個別グループ)) に加えて、ユーザによって作成されたグループを含むすべてのグループが表示されます。 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。
6. [OK] をクリックします。

ターミナル エミュレーション プログラムの使用

管理シリアル コンソールを HyperTerminal のようなターミナル エミュレーション プログラムと共に使用して、KX II-101 の次の設定パラメータを設定できます。

- IP アドレス
- サブネット マスク アドレス
- ゲートウェイ アドレス
- IP アクセス制御
- LAN 速度
- LAN インタフェースモード

KX II-101 でターミナル エミュレーション プログラムを使用するには、まず付属の RS-232 シリアル ケーブルを使用して KX II-101 のAdmin ポートと PC の COM1 ポートを接続する必要があります。 詳細については、「*Admin ポートの使用* 『p. 18』」を参照してください。

手順を説明するために、このセクションではターミナル エミュレーション プログラムに HyperTerminal を使用しています。 任意のターミナル エミュレーション プログラムを使用できます。

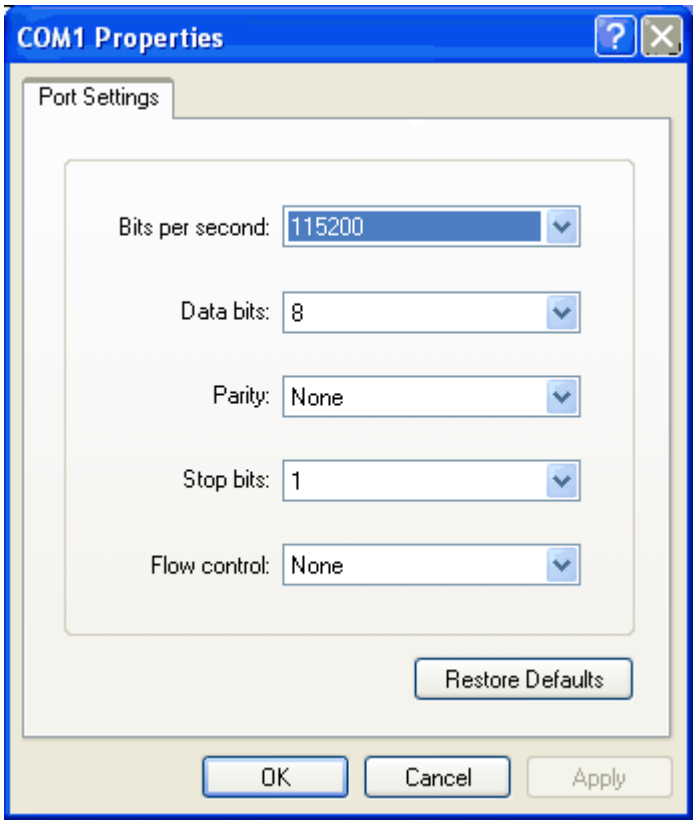
➢ *ターミナル エミュレーション プログラムを使用して KX II-101 を設定するには、以下の手順に従います。*

1. 付属の RS-232 シリアル ケーブルを使用して、KX II-101 とローカル PC を接続します。

   KX II-101 の Admin ポートと PC の COM1 ポートを接続します。

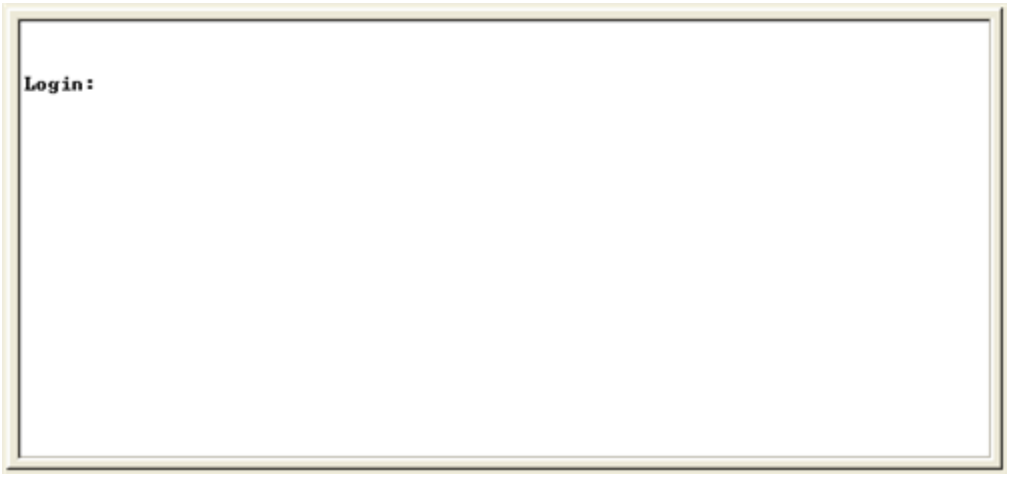
2. 使用するターミナル エミュレーション プログラムを起動し、KX II-101 を設定します。
3. ターミナル エミュレーション プログラムで次のポート構成を設定します。
   - Bits per second (ビット/秒): 115200
   - Data bits (データ ビット): 8
   - Parity (パリティ): None (なし)
   - Stop bits (ストップ ビット): 1

- Flow control (フロー コントロール): None (なし)



4. KX II-101 に接続します。

   ログイン画面が表示されます。

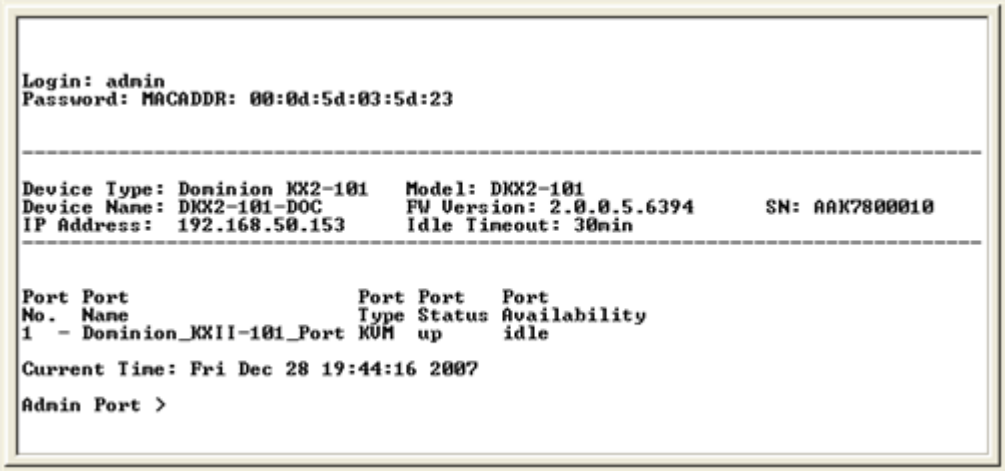


5. 管理者ユーザ名を入力して、Enter キーを押します。

パスワードの入力を確認するプロンプトが表示されます。

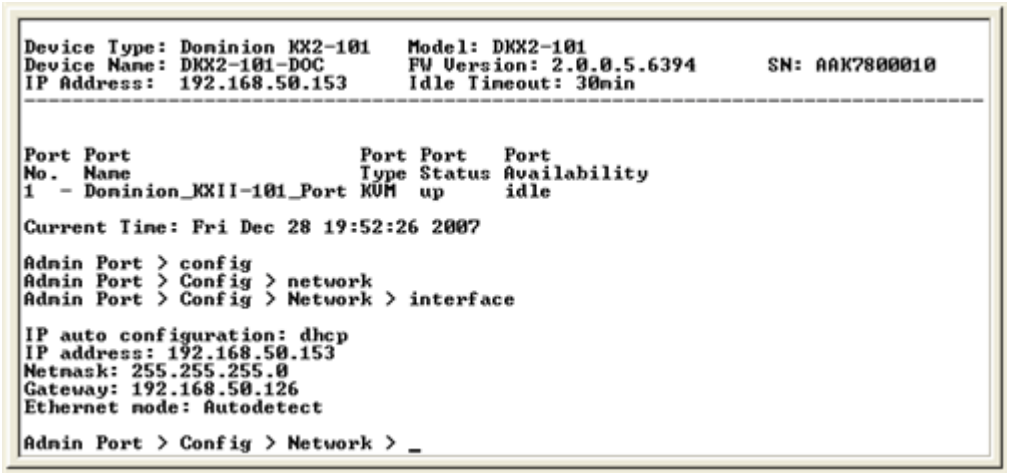
6. パスワードを入力して、Enter キーを押します。

   Admin Port (管理ポート) のプロンプトが表示されます。



7. Admin Port (管理ポート) のプロンプトで、「config」と入力し、Enter キーを押します。
8. Config (設定) のプロンプトで、「network」と入力し、Enter キーを押します。
9. 現在のインタフェース設定を確認するには、Interface (インタフェース) のプロンプトで、「interface 」と入力し、Enter キーを押します。

次のように現在のインタフェース設定が表示されます。



10. 新規ネットワーク設定を設定するには、Network (ネットワーク) のプロンプトで、「`interface` 」と入力し、その後に次のいずれかのコマンドとその適切な引数 (省略可能) を入力して Enter キーを押します。

コマンド	引数	オプション
ipauto	none|dhcp	none - デバイスの IP アドレスを手動で指定できます。 次の例に示すように、このオプションの後に ip コマンドと IP アドレスを続ける必要があります。 `interface ipauto none ip 192.168.50.12` dhcp - 起動時に、IP アドレスをデバイスに自動的に割り当てます。
ip	IP アドレス	デバイスに割り当てる IP アドレス。 初めて IP アドレスを手動で設定するときは、ipauto コマンドと none オプションと共にこのコマンドを使用する必要があります。 詳細については、「ipauto」を参照してください。 IP アドレスを手動で割り当てたら、ip コマンドを単独で使用して IP アドレスを変更できます。
mask	subnetmask	サブネット マスク IP アドレス。
gw	IP アドレス	ゲートウェイ IP アドレス
mode	mode	Ethernet モード。 次の選択肢があります。 auto - ネットワークに応じて速度とインタフェースを自動で設定します。 10hdx - 10 Mbs、半二重。 10fdx - 10 Mbs、全二重 100hdx - 100 Mbs、半二重 100fdx - 100 Mbs、全二重

設定が正常に変更されると、次のような確認メッセージが表示されます。

```
Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface ipauto none ip 192.168.50.126
Network interface configuration successful.
```

1. KX II-101 の設定を完了したら、コマンド プロンプトで「logout」と入力し、Enter キーを押します。

   コマンドライン インタフェースからログアウトされます。

4 KX II-101 への接続

この章の内容

言語サポート

KX II-101 は、次の言語のキーボード サポートを提供しています。 英語 (アメリカ)、繁体字中国語、簡体字中国語、日本語、韓国語、フランス語、ドイツ語。

注: 中国語、日本語、および韓国語のキーボードについては、表示のみに使用できます。現時点での KX II-101 リモート コンソール機能では、ローカル言語の入力はサポートされていません。

Linux での言語設定

Linux での外国語キーボードの設定方法については、『*KVM およびシリアル アクセス クライアント ユーザ ガイド*』の「**キーボードの種類**」を参照してください。

Java Runtime Environment (JRE)

重要: Java のキャッシュ機能を無効にし、**Java** キャッシュをクリアすることをお勧めします。 詳細は、**Java** のドキュメントまたは『**Raritan Multi-Platform Client / Raritan Remote Client** ユーザ ガイド』を参照してください。

KX II-101 リモート コンソールおよび MPC が動作するには、JRE が必要です。KX II-101 リモート コンソールは、Java のバージョンをチェックします。バージョンが不適切な場合または古い場合は、互換性のあるバージョンをダウンロードするように求められます。

最適なパフォーマンスを得るには、Java Runtime Environment (JRE) バージョン 1.5 を使用することを推奨しますが、KX II-101 リモート コンソールおよび MPC は JRE 1.6.x (1.6.2 を除く) など、JRE バージョン 1.4.2_05 以降 (JRE バージョン 1.5.0_02 を除く) でも動作します。

注: 多言語対応のキーボードで KX II-101 リモート コンソール (Virtual KVM Client) を使用するには、多言語バージョンの Java Runtime Environment (JRE) をインストールしてください。

KX II-101 の起動

重要: ブラウザの種類を問わず、KX II-101 リモート コンソールを起動するためには、Dominion デバイスの IP アドレスからのポップアップを許可する必要があります。

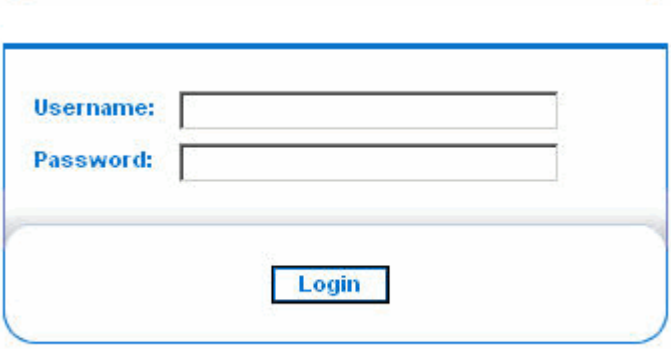
ご使用のブラウザおよびセキュリティの設定により、セキュリティと証明書に関する各種の警告が表示されることがあります。 KX II-101 リモート コンソールを起動するには、これらの警告を承諾する必要があります。

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、それ以降にログオンしたときに表示される警告メッセージを減らすことができます。

- [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]

➢ *KX II-101 リモート コンソールを起動するには、以下の手順に従います。*

1. KX II-101 ユニットにネットワークを介して接続でき、Java Runtime Environment v1.4.2_05 以降がインストールされている任意のワークステーションにログオンします (JRE は ***http://java.sun.com/*** http://java.sun.com から入手できます)。
2. サポートされる Web ブラウザ (Internet Explorer (IE) や Firefox など) を起動します。「サポートされるブラウザ」を参照してください。
3. 次の URL を入力します。 http://IP-ADDRESS。ここで、IP-ADDRESS の部分は、KX II-101 ユニットに割り当てた IP アドレスに置き換えます。 また、https を使用したり、管理者によって割り当てられた KX II-101 の DNS 名を使用することもできます (DNS サーバが設定されている場合)。単に IP アドレスをブラウザに入力してもかまいません (KX II-101 は常に IP アドレスを HTTP から HTTPS にリダイレクトします)。 ログイン ページが開きます。



4. ユーザ名とパスワードを入力します。 初めてログオンする場合は、工場出荷時のデフォルト ユーザ名とパスワード (admin および raritan (すべて小文字)) を使用してログオンします。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。詳細は、「デフォルトのパスワードの変更」を参照してください。
5. [Login] (ログイン) 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 アクセスを使用すると、通常のログイン ページに進まないで KX II-101 リモート クライアントにアクセスできます。 ダイレクト ポート アクセスを有効にすると、[Port Access] (ポート アクセス) ページに直接移動する URL を定義できます。

➢ *ダイレクト ポート アクセスを有効するには、以下の手順に従います。*

1. KX II-101 リモート コンソールを起動します。
2. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services] (デバイス サービス) ページが開きます。
3. [Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) チェックボックスをオンにします。
4. [Save] (保存) をクリックしてこの設定を保存します。

➢ *ダイレクト ポート アクセス URL を設定するには、以下の手順に従います。*

- IP アドレス、ユーザ名, パスワード、必要に応じて KX II-101 のポート番号を使用して URL を定義します。

  KVM ポートが 1 つのみある場合、ポート番号は不要です。

  ダイレクト ポート アクセス URL の形式は、次のとおりです。

  https://[**IP アドレス**]/dpa.asp?username=[**ユーザ名**]&password=[**パスワード**]&port=[**ポート番号**]

ヒント: ダイレクト ポート アクセス URL を定義し、Web ブラウザにブックマークとして保存すると、再使用が容易になります。

KX II-101 コンソールのレイアウト

KX II-101 リモート コンソール インタフェースは、設定や管理、ターゲット サーバのリストや選択用に Web 形式の HTML インタフェースを提供します。 オプションは複数のタブに配置されています。

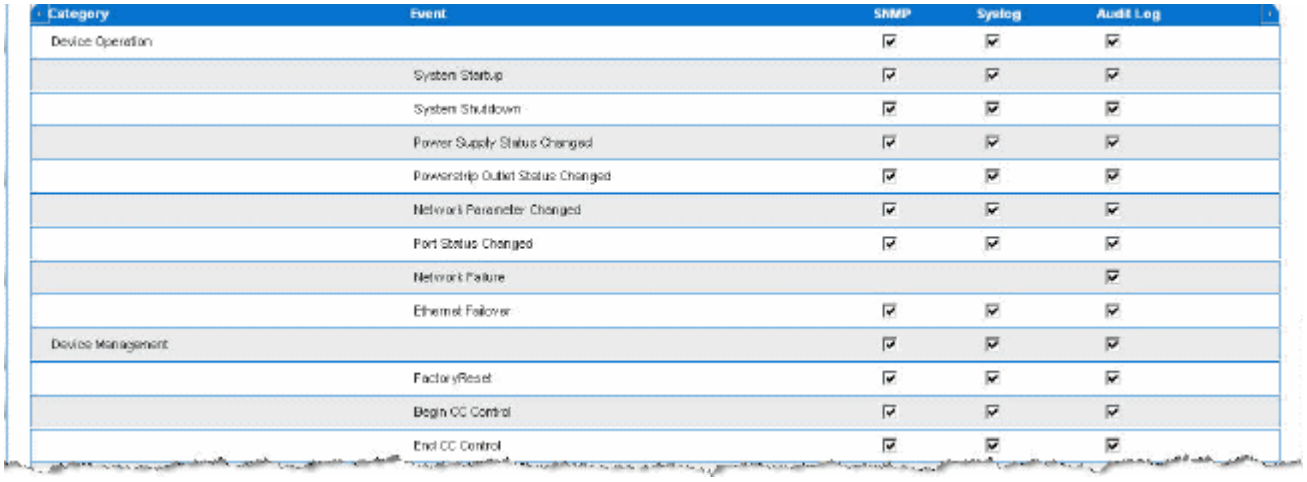
正常にログインすると、[Port Access] (ポート アクセス) ページが表示され、ポート、そのステータスと可用性が表示されます。

KX II-101 コンソールでの案内

KX II-101 リモート コンソール インタフェースは移動と選択の多くの方法を提供します。

➢ *オプションを選択するには、以下のいずれかの手順に従います。*

- タブをクリックします。使用可能なオプションのページが開きます。
- タブ上にカーソルを移動し、メニューから適切なオプションを選択します。
- 表示されるメニュー階層 (「階層リンク」) からオプションを直接クリックします。

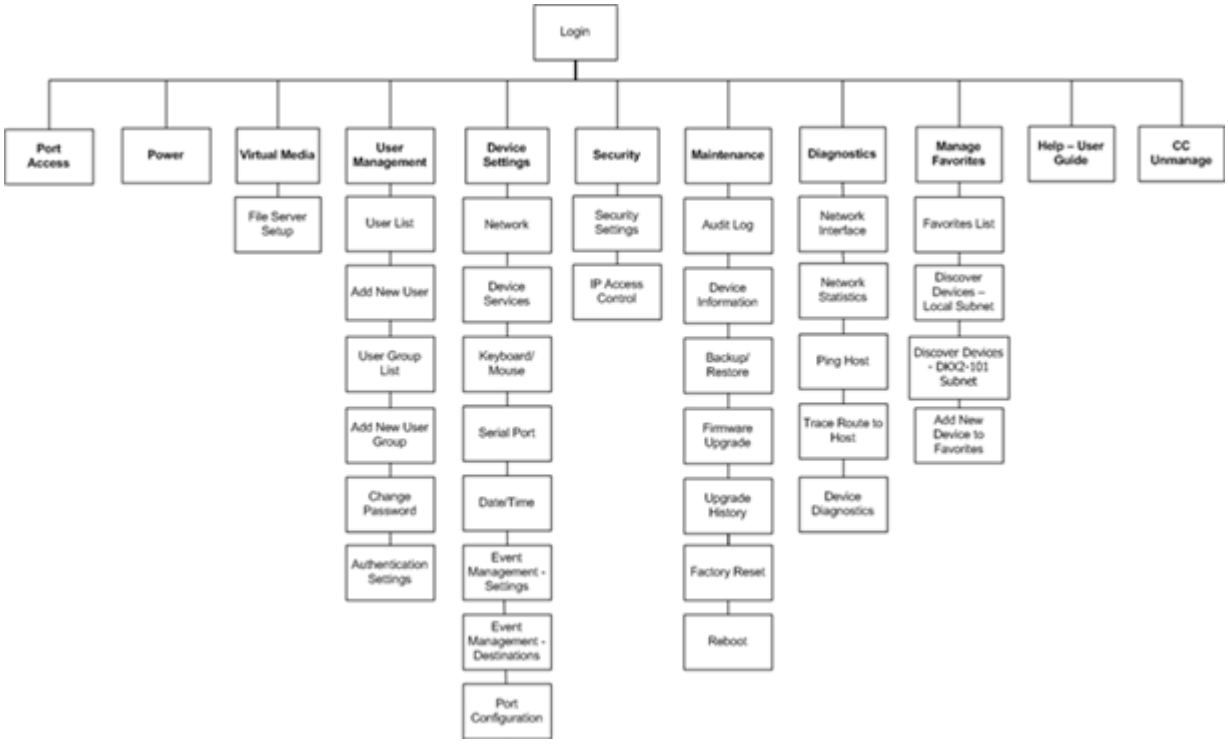


➢ *画面に収まらないページをスクロールするには、以下の手順に従います。*

- キーボードの Page Up キーと Page Down キーを使用します。または、
- 右側にあるスクロール バーを使用します。

KX II-101 リモート コンソールのメニュー マップ

以下の図に、KX II-101 リモート コンソールのすべてのメニュー オプションを示します。



ログオフ

➢ *KX II-101 リモート コンソールを終了するには、以下の手順に従います。*

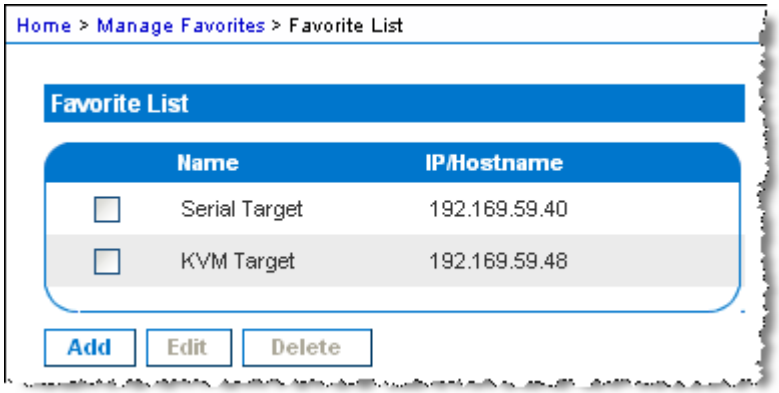
- ページの右上隅の [Logout] (ログアウト) をクリックします。

注: ログオフすると、開いているすべての Virtual KVM Client セッションとシリアル クライアント セッションが閉じられます。

お気に入りの管理

お気に入り機能を利用すると、よく使用するデバイスにすばやくアクセスできます。[Port Access] (ポート アクセス) ページの左下隅 (サイドバー) にある [Favorite Devices] (お気に入りデバイス) セクションでは、以下の操作が可能です。

- お気に入りデバイスのリストを作成および管理する。
- よく使用するデバイスにすばやくアクセスする。
- 名前または IP アドレス別にお気に入りのリストを表示する。
- サブネット上の KX II-101 デバイスを検出する (ログインの前および後)。
- 検出された KX II-101 デバイスを接続されているデバイスから取得する (ログインの後)。



➢ *お気に入りの KX II-101 デバイスにアクセスするには、以下の手順に従います。*

- ([Favorite Devices] (お気に入りデバイス) の下に表示されている) 目的のデバイスのデバイス名をクリックします。 新しいブラウザが開き、デバイスが表示されます。

➢ *[Favorite Devices] (お気に入りデバイス) リストの表示を名前順と IP アドレス順の間で切り替えるには、以下の手順に従います。*

お気に入りを IP アドレス順に表示するには、以下の手順に従います。

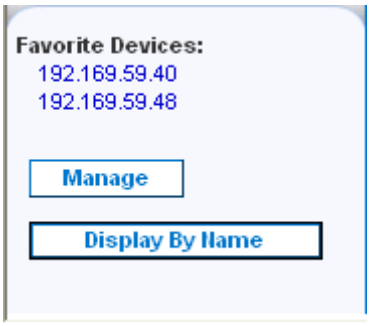
[Display by IP] (IP 順) ボタンをクリックします。

お気に入りのデバイスが名前別に表示されている場合は、[Display by IP] (IP 順) ボタンをクリックして切り替えます。

お気に入りを名前順に表示するには、以下の手順に従います。

[Display by Name] (名前順) ボタンをクリックします。

お気に入りのデバイスが IP アドレス別に表示されている場合は、[Display by Name] (名前順) ボタンをクリックして切り替えます。



[Manage Favorites] (お気に入りの管理) メニュー

➢ *[Manage Favorites] (お気に入りの管理) メニューを開くには、以下の手順に従います。*

- [Manage] (管理) ボタンをクリックします。 次の内容を含む [Manage Favorites] (お気に入りの管理) ページが開きます。

メニュー	操作
[Favorites List] (お気に入りリスト)	お気に入りデバイスのリストを管理します。
[Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット)	ローカル サブネット上のデバイスを検出します。
[Discover Devices - KX II-101 Subnet] (Discover Devices (デバイス検出)- KX II-101 サブネット)	KX II-101 デバイス サブネット上のデバイスを検出します。

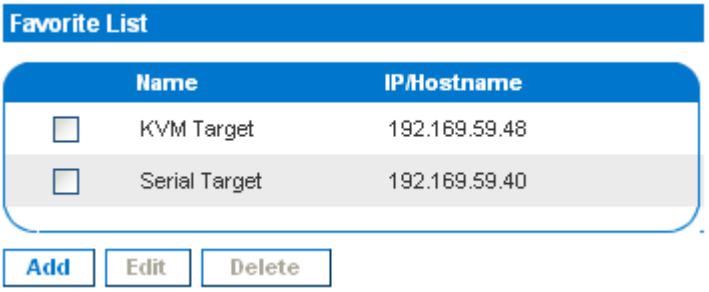
メニュー	操作
[Add New Device to Favorites] (お気に入りへの新しいデバイスの追加)	お気に入りリストのデバイスを追加、編集、および削除します。

[Favorites List] (お気に入りリスト)

[Favorites List] (お気に入りリスト) ページでは、お気に入りリストのデバイスを追加、編集、および削除できます。

➢ *[Favorites List] (お気に入りリスト) ページを開くには、以下の手順に従います。*

- [Manage] (管理) の [Favorites List] (お気に入りリスト) を選択します。 [Favorites List] (お気に入りリスト) ページが開きます。



➢ *お気に入りを追加するには、以下の手順に従います。*

- [Add] (追加) ボタンをクリックします。 [***Add New Favorite***『p. 42の"[Add New Favorite] (新しいお気に入りの追加)"参照先 』] (新しいお気に入りの追加) ページが開きます。

➢ *お気に入りを削除するには、以下の手順に従います。*

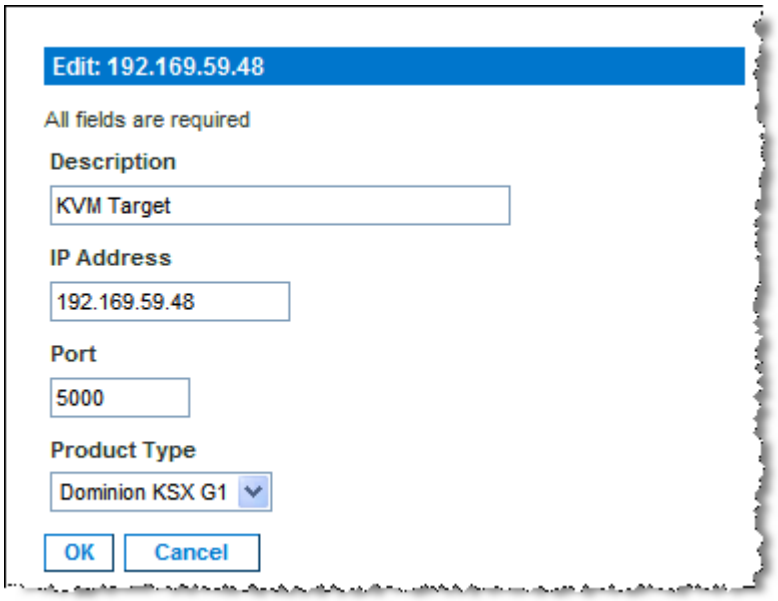
重要: お気に入りを削除する場合、確認メッセージが表示されないので注意してください。

1. 目的の KX II-101 デバイスの横にあるチェックボックスをオンにします。
2. [Delete] (削除) ボタンをクリックします。 お気に入りのリストからお気に入りが削除されます。

➢ *お気に入りを編集するには、以下の手順に従います。*

1. [Favorites List] (お気に入りリスト) ページで、目的の KX II-101 デバイスの横にあるチェックボックスをオンにします。

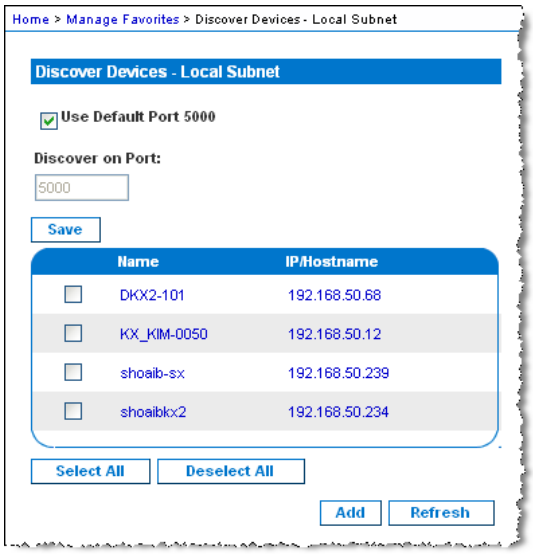
2. [Edit] (編集) ボタンをクリックします。 [Edit] (編集) ページが開きます。



3. 必要に応じてフィールドを更新します。
   - [Description] (説明)。 わかりやすい説明を入力します。
   - [IP Address] (IP アドレス)。 KX II-101 ユニットの IP アドレスを入力します。
   - [Port] (ポート)。 必要に応じて検出ポートを変更します。
   - [Product Type] (製品タイプ)。
4. [OK] をクリックします。

[Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット)

このオプションを使用すると、ローカル サブネット (KX II-101 リモート コンソールが実行されているサブネット) 上のデバイスを検出できます。また、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。



➢ *ローカル サブネット上のデバイスを検出するには、以下の手順に従います。*

1. [Favorites] (お気に入り) の [Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット) を選択します。 [Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット) ページが開きます。
2. 目的の検出ポートを選択します (検出ポートについての詳細は、「ネットワークのその他の設定」を参照してください)。
   - デフォルトの検出ポートを使用するには、[Use Default Port 5000] (デフォルト ポート 5000 を使用) オプションをオンにします。
   - 別の検出ポートを使用するには、以下の手順に従います。
   a. [Use Default Port 5000] (デフォルト ポート 5000 を使用) オプションをオフにします。
   b. [Discover on Port] (検出ポート) フィールドに、ポート番号を入力します。
   c. [Save] (保存) をクリックします。
3. [Refresh] (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 [Favorites List] (お気に入りリスト) に追加するには、以下の手順に従います。*

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] (追加) をクリックします。

ヒント: [Select All] (すべて選択) および [Deselect All] (すべての選択を解除) ボタンを使用すれば、リモート コンソール サブネット上のデバイスをすべて選択したり、すべての選択を解除したりできます。

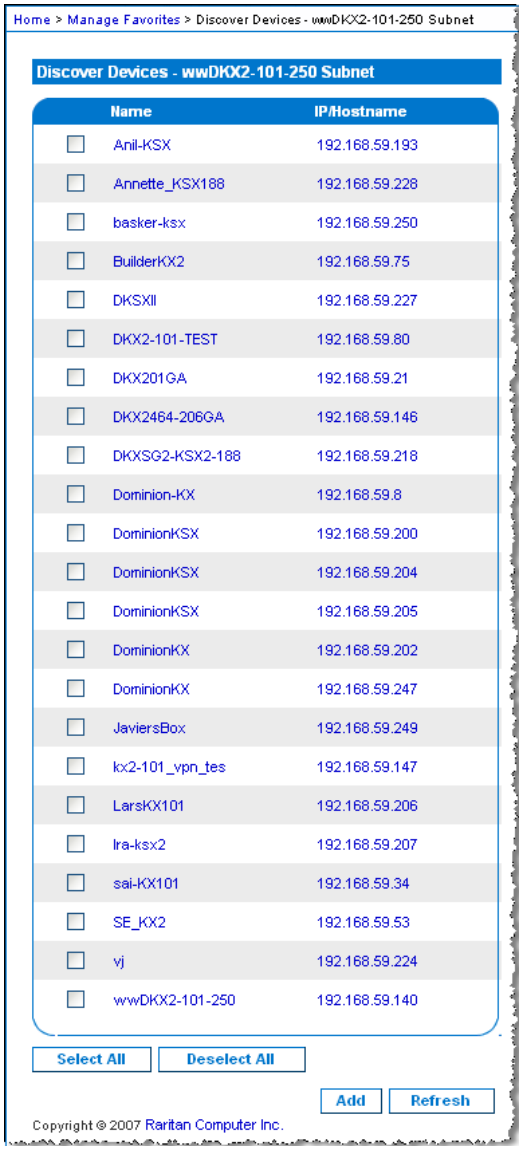
➢ *検出されたデバイスにアクセスするには、以下の手順に従います。*

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

[Discover Devices - KX II-101 Subnet] (Discover Devices (デバイス検出)- KX II-101 サブネット)

このオプションを使用すると、デバイス サブネット (KX II-101 デバイスの IP アドレスそのもののサブネット) 上のデバイスを検出できます。また、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 KX II-101 ユニットが相互に作用し合い、自動的にデバイスを検知し構成を拡張します。 KX II-101 リモート コンソールは、KX II-101 のサブネット内の KX II-101 ユニット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するには、以下の手順に従います。*

1. [Favorites] (お気に入り) の [Discover Devices - KX II-101 Subnet] (デバイス検出 - KX II-101 サブネット) を選択します。 [Discover Devices - KX II-101 Subnet] (デバイス検出 - KX II-101 サブネット) ページが開きます。
2. [Refresh] (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 [Favorites List] (お気に入りリスト) に追加するには、以下の手順に従います。*

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] (追加) をクリックします。

ヒント: [Select All] (すべて選択) および [Deselect All] (すべての選択を解除) ボタンを使用すれば、KX II-101 デバイス サブネット上のデバイスをすべて選択したり、すべての選択を解除したりできます。

➢ *検出されたデバイスにアクセスするには、以下の手順に従います。*

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

[Add New Favorite] (新しいお気に入りの追加)

➢ *デバイスを [Favorites List] (お気に入りリスト) に追加するには、以下の手順に従います。*

1. [Manage Favorites] (お気に入りの管理) の [Add New Device to Favorites] (お気に入りへの新しいデバイスの追加) を選択します。 [Add New Favorite] (新しいお気に入りの追加) ページが開きます。
2. わかりやすい説明を入力します。
3. デバイスの IP アドレスを入力します。
4. 必要に応じて検出ポートを変更します。
5. [OK] をクリックします。

このデバイスがお気に入りのリストに追加されます。

[Port Access] (ポート アクセス) ページ

KX II-101 リモート コンソールへのログインが正常に完了すると、[Port Access] (ポート アクセス) ページが開きます。 このページには、KX II-101 ポート、そのステータスおよび可用性が表示されます。 [Port Access] (ポート アクセス) ページは、KX II-101 に接続されている KVM ターゲット サーバへのアクセスを提供します。 KVM ターゲット サーバは、KX II-101 ユニットを介して制御したいサーバです。このサーバはデバイスに組み付けの PS/2 コネクタを使用して KX II-101 に接続されます。

注: KVM ターゲット サーバへの接続ごとに、新しい Virtual KVM Client ウィンドウが開きます。

➢ *[Port Access] (ポート アクセス) ページを使用するには、以下の手順に従います。*

1. KX II-101 リモート コンソールで、[**Port Access**] (ポート アクセス) タブをクリックします。 [**Port Access**] (ポート アクセス) ページが開きます。

   - [No.] (番号)。KX II-101 で使用できる 1 つのポートがあります。
   - [Name] (名前)。 KX II-101 ポートの名前です。最初は「Dominion_KX101G2_Port1」に設定されていますが、わかりやすい名前に変更できます。
   - [Availability] (可用性)。 可用性は、[Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、または [Unavailable] (使用不可能) のいずれかです。
2. ターゲット サーバに接続するには、デバイス/ターゲット サーバの名前をクリックし、[Connect] (接続) ポップアップをクリックします。[Virtual KVM Client] ウィンドウが表示され、可用性が [Busy] (ビジー) に変化します。
3. ターゲット サーバとの接続を切断するには、デバイス/ターゲット サーバの名前をクリックし、[Disconnect] (切断) ポップアップをクリックします。[Virtual KVM Client] ウィンドウが閉じて、可用性が [Idle] (アイドル) に変化します。

5 ユーザ、グループ、アクセス許可

この章の内容

ユーザ

KX II-101 は、アクセスの認可と許可を決定するためにユーザ名とグループ名の内部リストを保持しています。 この情報は、暗号化形式で内部に保存されます。 認証にはいくつかの方式があり、この方式は「ローカル認証」と呼ばれます。 すべてのユーザは認証を受ける必要があります。LDAP または RADIUS 認証を行うように KX II-101 が設定されている場合、LDAP/LDAPS または RADIUS 認証が行われた後に、ローカル認証が行われます。

KX II-101 ユニットにアクセスするには、ユーザ名とパスワードが必要です。 この情報は、KX II-101 ユニットにアクセスしようとしているユーザを認証するために使用されます。 ユーザを追加および編集する方法についての詳細は、「***ユーザ管理*** 『p. 45の "[User Management] (ユーザ管理)"参照先 』」を参照してください。

グループ

すべての KX II-101 ユニットには、3 つのデフォルト ユーザ グループが存在します。これらのグループは削除できません。

ユーザ	説明
[Admin] (管理)	このグループに所属するユーザは、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] (管理) ユーザは [Admin] (管理) グループのメンバーである必要があります。
[Unknown] (不明)	LDAP/LDAPS または RADIUS を使用して外部的に認証されるユーザまたはシステムで既知のユーザのデフォルト グループです。 外部 LDAP/LDAPS サーバまたは RADIUS サーバによって有効なユーザ グループが識別されなかった場合、[Unknown] (不明) グループが使用されます。 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。

[Individual Group] (個別グループ)	個別グループとは、基本的に個人の「グループ」です。 つまり、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。 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。 個別グループでは、グループと同じ権限をユーザ アカウントに割り当てることができます。

システムによって定義されているデフォルトのグループに加えて、グループを作成し、目的に合った適切な許可を指定できます。 ユーザ グループを作成および編集する方法についての詳細は、「ユーザ管理」を参照してください。

ユーザとグループの関係

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。 KX II-101 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、デバイスは、グループ情報を使用して、アクセスできるサーバ ポート、ユニット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。

[User Management] (ユーザ管理)

[User Management] (ユーザ管理) メニュー

[User Management] (ユーザ管理) メニューは次のように構成されています。

メニュー	操作
[User List] (ユーザ リスト)	すべてのユーザをアルファベット順に表示します。ユーザの追加、変更、または削除を行うこともできます。
[Add New User] (新規ユーザの追加)	新規ユーザを追加します。ユーザ情報の変更も行うことができます。
[User Group List] (ユーザ グループ リスト)	すべてのユーザ グループをアルファベット順に表示します。ユーザ グループの追加、変更、または削除を行うこともできます。
「Add New User Group] (新規ユーザ グループの追加)	新規ユーザ グループを追加します。ユーザ グループ情報の変更も行うことができます。
[Change Password] (パスワードの変更)	特定のユーザのパスワードを変更します。

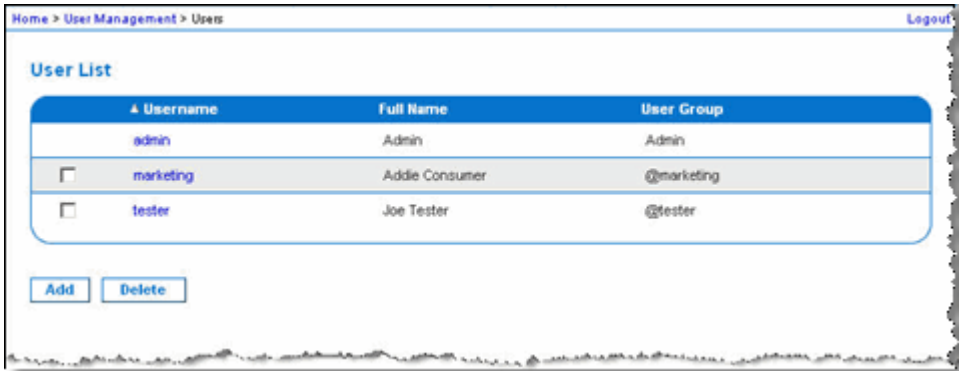
メニュー	操作
[Authentication Settings] (認証設定)	KX II-101 に対するアクセスに使用する認証の種類を設定します。

[User List] (ユーザ リスト)

[User List] (ユーザ リスト) ページには、すべてのユーザについて、ユーザ名、フル ネーム、およびユーザ グループが表示されます。 このリストは、任意の列名をクリックすることで並べ替えることができます。 [User List] (ユーザ リスト) ページでは、ユーザを追加、変更、または削除することもできます。

➢ *ユーザ リストを表示するには、以下の手順に従います。*

- [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択します。 [User List] (ユーザ リスト) ページが開きます。



➢ *新規ユーザを追加するには、以下の手順に従います。*

- [Add] (追加) ボタンをクリックします。 [User] (ユーザ) ページが開きます。 [User] (ユーザ) ページについての詳細は、「***新規ユーザの追加***『p. 47の "[Add New User] (新規ユーザの追加)"参照先 』」を参照してください。

➢ *既存のユーザを変更するには、以下の手順に従います。*

1. リストから目的のユーザを探します。
2. ユーザ名をクリックします。 [User] (ユーザ) ページが開きます。 ユーザの編集方法についての詳細は、「***既存のユーザの変更***『p. 48』」を参照してください。

➢ *ユーザを削除するには、以下の手順に従います。*

1. リストのユーザ名の左にあるチェックボックスをオンにして、目的のユーザを選択します。
2. [Delete] (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。
3. [OK] をクリックします。

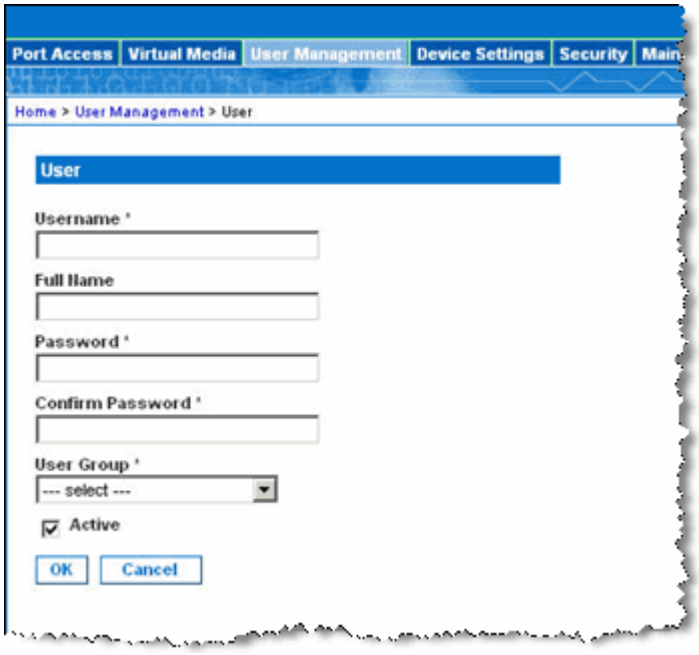
[Add New User] (新規ユーザの追加)

KX II-101 ユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。 [User] (ユーザ) ページでは、新規ユーザの追加、ユーザ情報の変更、無効化されているユーザの再有効化を行うことができます。

注: ユーザがログインに失敗した回数が [Security Settings] (セキュリティ設定) ページで設定されているログイン失敗の最大許容回数を超えた場合、そのユーザ名は無効化されます ([Active] (アクティブ) チェックボックスがオフになります)。 詳細は、「セキュリティの設定」を参照してください。

➢ *新規ユーザを追加するには、以下の手順に従います。*

1. 次の方法のいずれかを使用して、[User] (ユーザ) ページを開きます。
   - [User Management] (ユーザ管理) の [Add New User] (新規ユーザの追加) を選択します。または、
   - [User List] (ユーザ リスト) ページの [Add] (追加) ボタンをクリックします。



2. [Username] (ユーザ名) フィールドに、一意のユーザ名を入力します (最大 16 文字)。
3. [Full Name] (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 (最大 64 文字)。

4. [Password] (パスワード) フィールドにパスワードを入力し、[Confirm Password] (パスワードの確認) フィールドにパスワードを再入力します (最大 64 文字)。
5. [User Group] (ユーザ グループ) ドロップダウン リストからグループを選択します。 このリストには、システムによって定義されているデフォルト グループ ([<Unknown>] (不明) (デフォルト設定)、[Admin] (管理者)、[Individual Group] (個別グループ)) に加えて、ユーザによって作成されたグループを含むすべてのグループが表示されます。 このユーザを既存のユーザ グループに関連付けない場合は、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。

   注: [Admin] (管理) ユーザは [Admin] (管理) グループのメンバーである必要があります。

   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***『p. 52』」を参照してください。
6. このユーザを有効にするには、[Active] (アクティブ) チェックボックスをオンにします。 デフォルトはアクティブ状態 (有効) です。
7. [OK] をクリックします。

既存のユーザの変更

➢ *既存のユーザを変更するには、以下の手順に従います。*

1. [User] (ユーザ) ページで、目的のフィールドを変更します ([User] (ユーザ) ページにアクセスする方法についての詳細は、「***新規ユーザの追加***『p. 47の "[Add New User] (新規ユーザの追加)"参照先 』」を参照してください)。
2. [OK] をクリックします。

ユーザ ブロックとブロック解除

システムへのユーザのアクセスは、管理者により、またはセキュリティ設定を基に自動的にブロックできます。 詳細は、「***ユーザ ブロック***『p. 149の"[User Blocking] (ユーザ ブロック)"参照先 』」を参照してください。 ブロックされたユーザは非アクティブになり、管理者が再びアクティブにすることでブロック解除できます。

➢ *ユーザをブロックまたはブロック解除するには、以下の手順に従います。*

1. [User Management] (ユーザ管理) の [User] (ユーザ) を選択します。

   [User] (ユーザ) ページが表示されます。
2. [Active] (アクティブ) チェックボックスをオンまたはオフにします。
   - オンにした場合、ユーザはアクティブになり、KX II-101 にアクセスできます。

- オフにした場合、ユーザは非アクティブになり、KX II-101 にアクセスできません。

3. [OK] をクリックします。

   ユーザのアクティブ ステータスが更新されます。

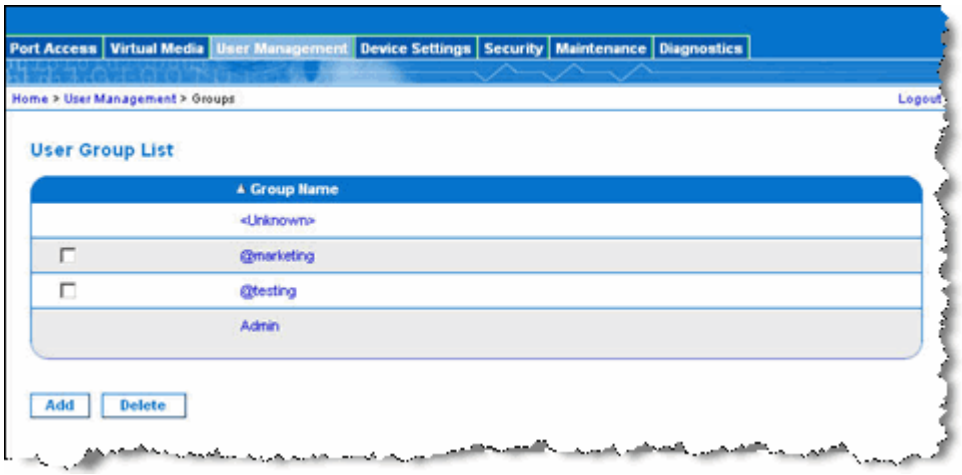
[User Group List] (ユーザ グループ リスト)

ユーザ グループは、ローカル認証とリモート認証 (RADIUS または LDAP/LDAPS) で使用されます。 個別のユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。

[User Group List] (ユーザ グループ リスト) ページには、すべてのユーザ グループのリストが表示されます。このリストは、[Group Name] (グループ名) 列見出しをクリックすることで、昇順または降順に並べ替えることができます。 [User Group List] (ユーザ グループ リスト) ページでは、ユーザ グループを追加、変更、または削除することもできます。

➢ *ユーザ グループのリストを表示するには、以下の手順に従います。*

- [User Management] (ユーザ管理) の [User Group List] (ユーザ グループ リスト) を選択します。 [User Group List] (ユーザ グループ リスト) ページが開きます。



➢ *新規ユーザ グループを追加するには、以下の手順に従います。*

- [Add] (追加) ボタンをクリックします。 [Group] (グループ) ページが開きます。[Group] (グループ) ページについての詳細は、「新規ユーザ グループの追加」を参照してください。

➢ *既存のユーザ グループを変更するには、以下の手順に従います。*

1. リストから目的のユーザ グループを探します。

2. グループ名をクリックします。 [Group] (グループ) ページが開きます。 グループを編集する方法についての詳細は、「***既存のユーザ グループの変更*** 『p. 56』」を参照してください。

➢ *ユーザ グループを削除するには、以下の手順に従います。*

重要: ユーザを含むグループを削除すると、そのユーザは <Unknown (不明)> ユーザ グループに自動的に割り当てられます。

ヒント: 特定のグループに属しているユーザを調べるには、ユーザ グループ別にユーザ リストをで並べ替えます。

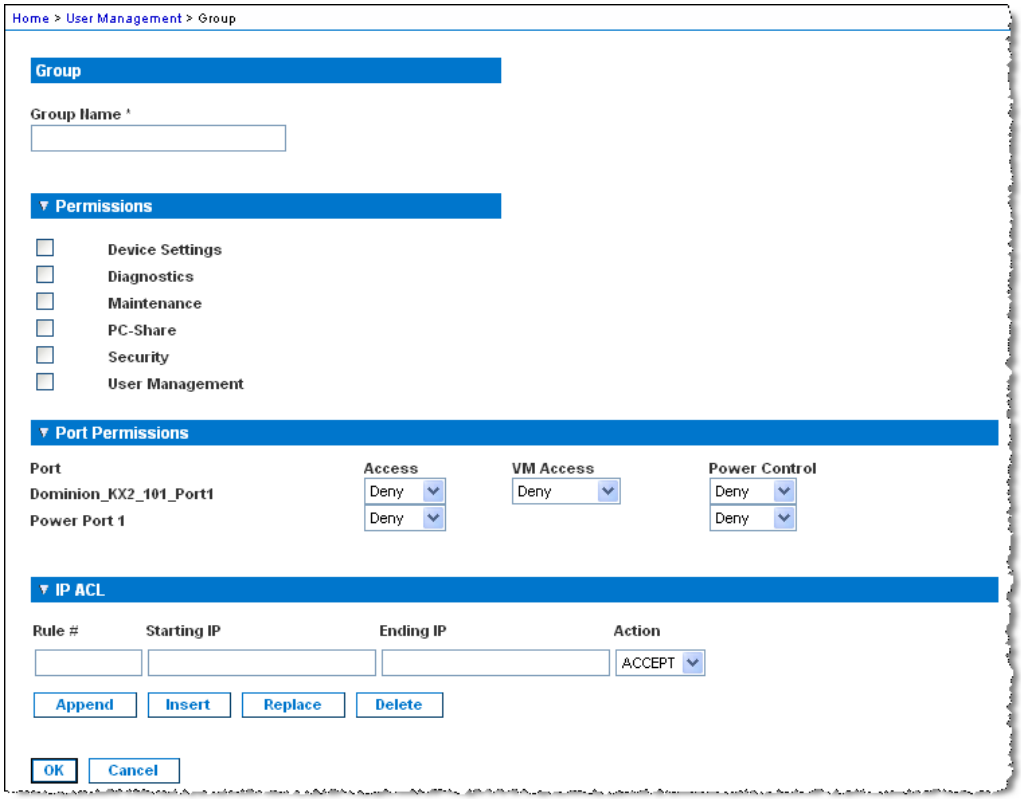
1. リストのグループ名の左にあるチェックボックスをオンにして、目的のグループを選択します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

[Add New User Group] (新規ユーザ グループの追加)

➢ *新規ユーザ グループを追加するには、以下の手順に従います。*

1. 次の方法のいずれかを使用して、[Group] (グループ) ページを開きます。
   - [User Management] (ユーザ管理) の [Add New User Group] (新規ユーザ グループの追加) を選択します。または、

- [User Group List] (ユーザ グループ リスト) ページの [Add] (追加) ボタンをクリックします。



[Group] (グループ) ページは、[Group] (グループ)、[Permissions] (許可)、[Port Permissions] (ポート権限)、および [IP ACL] (IP ACL) のカテゴリに分かれています。

2. [Group Name] (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。
3. グループの許可を設定します。 このグループに属するすべてのユーザに対して割り当てる許可の左にあるチェックボックスをオンにします。 詳細は、「***許可の設定*** 『p. 52』」を参照してください。
4. [Port Permissions] (ポート権限) を設定します。 KVM およびパワー ポートに与えるアクセスの種類を指定します。 詳細は、「ポート権限の設定」を参照してください。
5. グループベースの IP ACL (IP アクセス制御リスト) を設定します (オプション)。この機能は、IP アドレスを指定することによって、その IP アドレスから KX II-101 デバイスへのアクセスを制限します。この機能は、デバイスへのすべてのアクセスに適用される (および優先される) ***IP アクセス制御*** 『p. 153の"[IP Access Control] (IP アクセス制御)"参照先 』リスト機能とは異なり、特定のグループに属するユーザにのみ適用されます。
6. [OK] をクリックします。

注: 複数の管理機能を MPC 内で利用できます (これらの機能を利用できるのは、デフォルトの ADMIN (管理者) グループのメンバーに限られます)。

許可の設定

重要: [User Management] (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。

許可	説明
[Device Settings] (デバイス設定)	ネットワーク設定、日付/時刻設定、ポート設定 (チャンネル名、電源の関連付け)、イベント管理 (SNMP、Syslog)、仮想メディア ファイル サーバのセットアップ
Diagnostics	ネットワーク インタフェース ステータス、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、KX II-101 診断
メンテナンス	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-Share] (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
セキュリティ	SSL 証明書、セキュリティ設定 (VM 共有、PC 共有)、IP ACL
[User Management] (ユーザ管理)	ユーザおよびグループの管理、リモート認証 (LDAP/RADIUS)、ログイン設定

個別グループの許可の設定

➢ *個別ユーザ グループに許可を設定するには、以下の手順に従います。*

1. リストから目的のユーザ グループを探します。 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。
2. グループ名をクリックします。 [Group] (グループ) ページが開きます。
3. 適切な許可を選択します。
4. [OK] をクリックします。

ポート権限の設定

サーバ ポートに対して、アクセスのタイプ、仮想メディアへのアクセスのタイプ、および電源管理を指定できます。 すべての許可についてデフォルト設定はすべて無効になっていることに注意してください。

[Access] (アクセス)		[VM Access] (VM アクセス)		電源制御	
オプション	説明	オプション	説明	オプション	説明
[None] (なし)*	アクセスを完全に拒否します。	[Deny] (拒否)*	ポートに対して仮想メディア許可はすべて拒否されます。	[Deny] (拒否)*	アクセスを完全に拒否します。
[View] (表示)	接続先のターゲット サーバのビデオを表示します (操作はできません)。	[Deny] (拒否)*	ポートに対して仮想メディア許可はすべて拒否されます。	[Deny] (拒否)*	アクセスを完全に拒否します。
[Control] (制御)	接続先のターゲット サーバを制御します。	仮想メディア アクセスは、読み取りアクセスのみに制限されます。	[Read-Only] (読み取り専用) 仮想メディアに対する完全なアクセス (読み取り、書き込み)。	[Access] (アクセス)	完全なアクセス。
[Control] (制御)	接続先のターゲット サーバを制御します。	[Read-Write] (読み取り/書き込み可能)	仮想メディアに対する完全なアクセス (読み取り、書き込み)。	[Access or Deny] (アクセスまたは拒否)	完全なアクセス。またはアクセスを完全に拒否します。

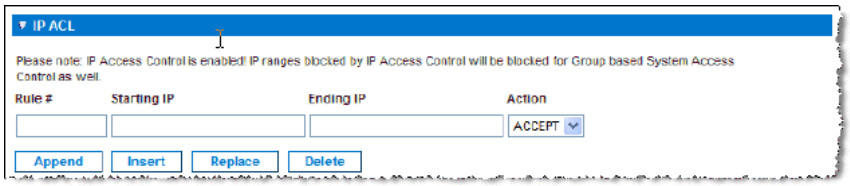
* デフォルト設定

グループベースの IP ACL (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、KX II-101 がロックアウトされてしまいます。

この機能は、選択したグループに含まれるユーザによる KX II-101 デバイスへのアクセスを特定の IP アドレスに制限します。 この機能は、デバイスへのすべてのアクセス試行に適用される (および最初に処理され、優先される) IP アクセス制御リスト機能とは異なり、特定のグループに属するユーザにのみ適用されます。 詳細は、「***IP アクセス制御*** 『p. 153の"[IP Access Control] (IP アクセス制御)"参照先 』」を参照してください。

グループレベルで IP アクセス制御ルールの追加、挿入、置換、削除を行うには、[Group] (グループ) ページの [IP ACL] (IP ACL) セクションを使用します。



➢ *新しいルールを追加するには、以下の手順に従います。*

1. [Starting IP] (開始 IP) フィールドに、開始 IP アドレスを入力します。
2. [Ending IP] (終了 IP) フィールドに、終了 IP アドレスを入力します。
3. [Action] (アクション) で、アクションを選択します。
   - [Accept] (承諾)。 その IP アドレスによる KX II-101 デバイスへのアクセスが許可されます。
   - [Drop] (拒否)。 その IP アドレスによる KX II-101 デバイスへのアクセスが拒否されます。
4. [Append] (追加) をクリックします。 ルール リストの 1 番下にルールが追加されます。
5. 入力する各ルールについて、手順 1 ～ 4 を繰り返します。

➢ *ルールを挿入するには、以下の手順に従います。*

1. [Rule] (ルール) 番号を入力します。 [Insert] (挿入) コマンドを使用するときは、ルール番号が必要です。
2. [Starting IP] (開始 IP) フィールド と [Ending IP] (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. [Insert] (挿入) をクリックします。 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。

➢ *ルールを置き換えるには、以下の手順に従います。*

1. 置き換える [Rule] (ルール) 番号を指定します。

2. [Starting IP] (開始 IP) フィールド と [Ending IP] (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. [Replace] (置き換え) を選択します。 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、以下の手順に従います。*

1. 削除する [Rule] (ルール) 番号を指定します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

重要: ACL のルールは、リスト表示されている順に評価されます。 たとえばこの例において、**2** つの **ACL** ルールの順番が逆になると、**Dominion** は通信を全く受けることができなくなります。

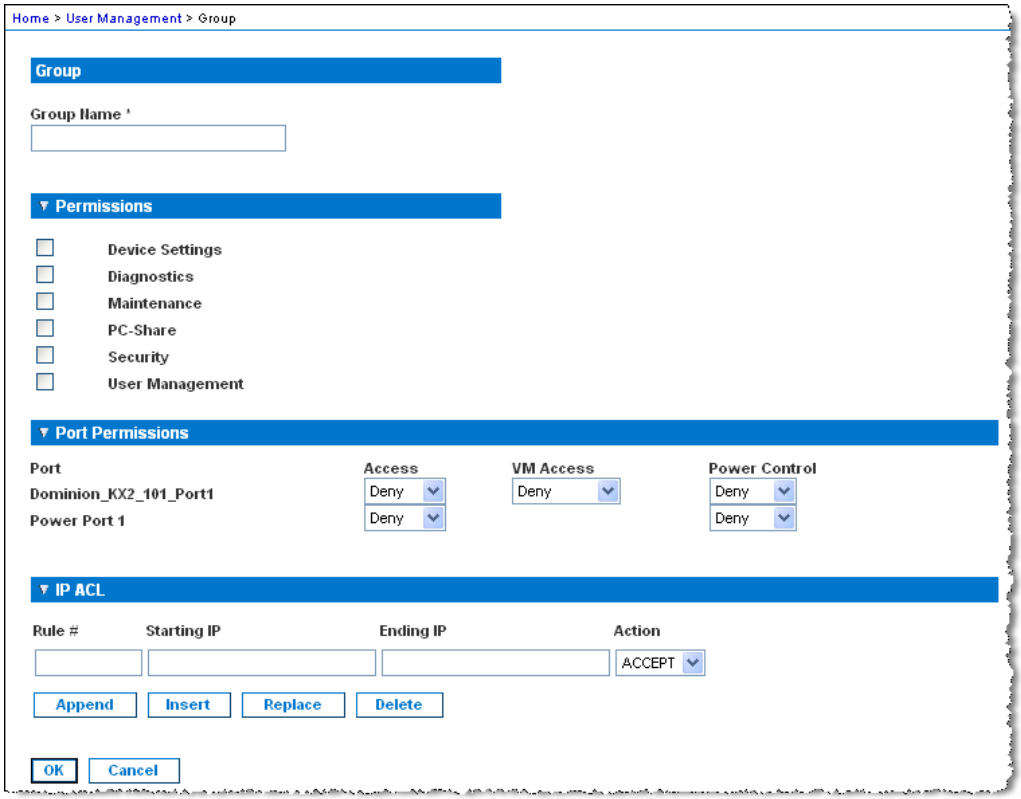
ヒント: ルール番号を使用すると、ルールが作成された順番を基により詳細に制御できます。

既存のユーザ グループの変更

注: Admin (管理者) グループに対しては、すべての許可が有効になっています (この設定は変更できません)。

➢ *既存のユーザ グループを変更するには、以下の手順に従います。*

1. [Group] (グループ) ページで、適切なフィールドを変更し、適切な許可を設定します。

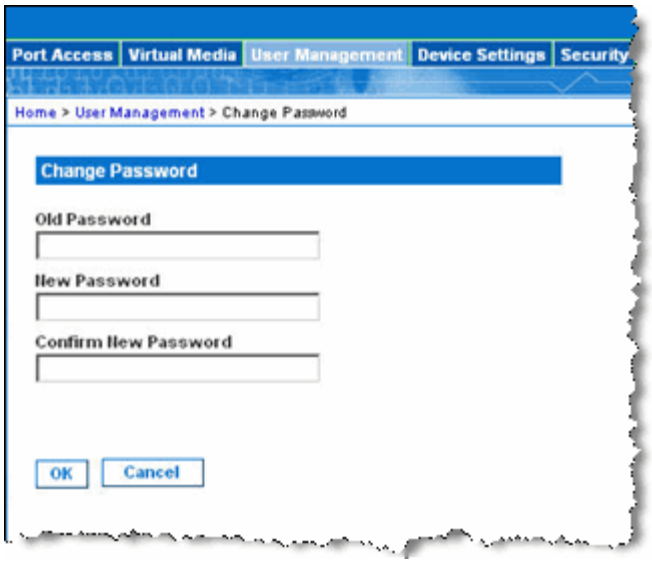


2. グループの許可を設定します。 このグループに属するすべてのユーザに対して割り当てる許可の左にあるチェックボックスをオンにします。 詳細は、「***許可の設定*** 『p. 52』」を参照してください。
3. [Port Permissions] (ポート権限) を設定します。 このグループに属するユーザがアクセスできるサーバ ポート (およびアクセスのタイプ) を指定します。 詳細は、「ポート権限の設定」を参照してください。
4. IP ACL を設定します (オプション)。 この機能は、IP アドレスを指定することで、KX II-101 デバイスへのアクセスを制限します。 詳細は、「グループベースの IP ACL (アクセス制御リスト)」を参照してください。
5. [OK] をクリックします。

[Change Password] (パスワードの変更)

➢ *パスワードを変更するには、以下の手順に従います。*

1. [User Management] (ユーザ管理) の [Change Password] (パスワードの変更) を選択します。 [Change Password] (パスワードの変更) ページが開きます。



2. [Old Password] (旧パスワード) フィールドに現在のパスワードを入力します。
3. [New Password] (新しいパスワード) フィールドに新しいパスワードを入力し、[Confirm New Password] (新しいパスワードの確認) フィールドに新しいパスワードを再入力します。 パスワードには、最大 64 文字の英数字と特殊文字を使用できます。
4. [OK] をクリックします。
5. パスワードが正常に変更された旨のメッセージが表示されます。 [OK] をクリックします。

注: 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。 パスワードと強力なパスワードについての詳細は、
*/***[Security Settings] (セキュリティ設定) - [Strong Passwords] (強力なパスワード)** *『p. 147の"[Strong Passwords] (強力なパスワード)" 参照先 』]を参照してください。*

[Authentication Settings] (認証設定)

認証設定は、この章で後述のリモート認証で説明されています。 詳細は、「認証設定」を参照してください。

リモート認証

CC-SG ユーザへの注意事項

CommandCenter Secure Gateway を使用して KX II-101 を制御している場合、(ローカル ポート アクセスを必要とする) ローカル ユーザを除き、ユーザおよびグループは CC-SG によって認証されます。 CC-SG で KX II-101 を制御している場合、ローカル ポート ユーザは、KX II-101 上で設定されているローカル ユーザ データベースまたはリモート認証サーバ (LDAP/LDAPS または RADIUS) に対して認証され、CC-SG ユーザ データベースに対して認証されません。

CC-SG 認証についての詳細は、Raritan の Web サイト (***http://www.raritan.com/support/*** http://www.raritan.com/support) から入手できる CommandCenter Secure Gateway のユーザ ガイド、管理者ガイド、またはデプロイメント ガイドを参照してください。

サポートされているプロトコル

ユーザ名とパスワードの管理を容易にするため、KX II-101 には認証要求を外部認証サーバへ転送する機能があります。 LDAP/LDAPS と RADIUS の 2 つの外部認証プロトコルがサポートされています。

Microsoft Active Directory についての注意事項

Microsoft Active Directory は、LDAP/LDAPS プロトコルをネイティブに使用し、LDAP/LDAPS サーバおよび KX II-101 の認証元として機能することが可能です。 IAS (インタフェース認証サーバ) のコンポーネントを装備している場合、Microsoft Active Directory サーバは、RADIUS 認証元としても機能します。

認証と認可

認証とは、ユーザが本物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。

KX II-101 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。

[Authentication Settings] (認証設定)

[Authentication Settings] (認証設定) ページでは、KX II-101 へのアクセスに使用する認証の種類を設定できます。 認証と認可の動作および相違点についての詳細は、「***認証と認可*** 『p. 58』」を参照してください。

注: ローカル認証はリモート認証 (LDAP または RADIUS) を選択した場合でも使用されます。

➢ *認証を設定するには、以下の手順に従います。*

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) を選択します。 [Authentication Settings] (認証設定) ページが開きます。

2. 使用する認証プロトコルのオプションを選択します ([Local Authentication] (ローカル認証)、[LDAP] (LDAP)、または [RADIUS] (RADIUS))。[LDAP] (LDAP) オプションを選択した場合、LDAP に関連するフィールドが有効になります。[RADIUS] (RADIUS) オプションを選択した場合、RADIUS に関連するフィールドが有効になります。
3. [Local Authentication] (ローカル認証) を選択した場合は、手順 6 に進みます。
4. [LDAP] (LDAP) を選択した場合は、「LDAP リモート認証の実装」を参考にして、[Authentication Settings] (認証設定) ページの [LDAP] (LDAP) セクションの各フィールドを指定してください。
5. [RADIUS] (RADIUS) を選択した場合は、「***RADIUS リモート認証の実装***『p. 64』」を参考にして、[Authentication Settings] (認証設定) ページの [RADIUS] (RADIUS) セクションの各フィールドを指定してください。
6. [OK] をクリックして保存します。

➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) 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。*

- [Reset To Defaults] (デフォルトに戻す) ボタンをクリックします。

LDAP リモート認証の実装

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) 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 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 認証サーバとしてネイティブに機能します。

➢ *LDAP 認証プロトコルを使用するには、以下の情報を入力します。*

1. [Primary LDAP Server] (プライマリ LDAP サーバ) フィールドに、LDAP リモート認証サーバの IP アドレスまたは DNS 名を入力します。 [Enable Secure LDAP] (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。
2. (オプション) [Secondary LDAP Server] (セカンダリ LDAP サーバ) フィールドに、バックアップ LDAP サーバの IP アドレスまたは DNS 名を入力します。 [Enable Secure LDAP] (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、[Primary LDAP Server] (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。
3. [Secret Phrase] (秘密フレーズ) フィールドに、リモート認証サーバへの認証に必要となるサーバの秘密フレーズ (パスワード) を入力します。次に、[Confirm Secret Phrase] (秘密フレーズの確認) フィールドに、サーバの秘密フレーズ (パスワード) を再入力します。 既存のスキーマを変更しないでください。 LDAP サーバで使用している文字列を使用します。
4. SSL を使用する場合は、[Enable Secure LDAP] (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。[Secure LDAP Port] (セキュア LDAP ポート) フィールドが有効になります。 Secure Sockets Layer (SSL) は、KX II-101 が LDAP 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。
5. [Port] (ポート) のデフォルトは 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。
6. [Secure LDAP Port] (セキュア LDAP ポート) 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、[Enable Secure LDAP] (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。
7. [Certificate File] (証明書ファイル)。 LDAP 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。 [Browse] (参照) ボタンを使用して証明書ファイルを選択します。 このフィールドは、[Enable Secure LDAP] (セキュア LDAP を有効にする) ボックスがオンのときに有効になります。
8. [DN of administrative User] (管理者ユーザの DN)。 管理者ユーザの識別名です。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,dc=Users=,dc=testradius,dc=com" と設定します。
9. [User Search DN] (ユーザ検索 DN)。 これは、LDAP に対しバインドする名前、およびデータベース内で指定されたベース DN の検索を開始する場所を示します。 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。
10. [Type of external LDAP server] (外部 LDAP サーバの種類)。 使用可能なオプションを選択します。

- [Generic LDAP Server] (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 ディレクトリ サービスの実装です。

11. [Active Directory Domain] (Active Directory ドメイン)。 Active Directory ドメインの名前を入力します。

ユーザ グループ情報を Active Directory サーバから返す

KX II-101 では、ユーザを KX II-101 でローカルに定義する必要なく、Active Directory (AD) へのユーザ認証がサポートされます。 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。 認可と AD ユーザ特権は、標準の KX II-101 ポリシーおよび (AD ユーザ グループにローカルに適用される) ユーザ グループ特権によって制御および管理されます。

---

*注: 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、KX II-101 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。 AD LDAP スキーマを更新する方法についての詳細は、**「**LDAP スキーマの更新** 『p. 66』」を参照してください。*

➢ *KX II-101 で AD サーバを有効にするには、以下の手順に従います。*

1. KX II-101 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、KVM_Admin や KVM_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 KX II-101 ユーザを割り当てます。
4. KX II-101 で、AD サーバを有効にし、適切に設定します。「LDAP 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。
- KX II-101 には、[Admin] (管理者) と [<Unknown>] (不明) のデフォルト グループが用意されています。これらのグループを変更したり削除したりすることはできません。 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 サーバから返されたグループ情報が KX II-101 のグループ設定と一致しない場合、正常に認証されたユーザに対して自動的に [<Unknown>] (不明) グループが割り当てられます。

RADIUS リモート認証の実装

Remote Authentication Dial-in User Service (RADIUS) は、ネットワーク アクセス アプリケーションのための AAA (認証 (authentication)、認可 (authorization)、アカウンティング (accounting)) プロトコルです。

➢ *RADIUS 認証プロトコルを使用するには、以下の手順に従います。*

1. 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、[Primary Radius Server] (プライマリ Radius サーバ) フィールド (および [Secondary Radius Server] (セカンダリ Radius サーバ) フィールド) に入力します。
2. (共有の秘密フィールドに) 認証に使用するサーバの秘密フレーズを入力します。共有の秘密とは、KX II-101 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。
3. [Authentication Port] (認証ポート)。 デフォルトの認証ポートは 1812 です。このポートは必要に応じて変更できます。

4. [Accounting Port] (アカウンティング ポート)。 デフォルトのアカウンティング ポートは 1813 です。このポートは必要に応じて変更できます。
5. [Timeout (in seconds)] (タイムアウト (秒))。 デフォルトのタイムアウトは 1 秒です。この値は必要に応じて変更できます。 このタイムアウトは、KX II-101 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。
6. [Retries] (再試行回数)。 デフォルトの再試行回数は 3 回です。この回数は必要に応じて変更できます。 これは、KX II-101 が RADIUS サーバに対して認証要求を送信する回数です。
7. [Global Authentication Type] (グローバル認証タイプ)。 ドロップダウン リストのオプションから選択します。
   - [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。

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、KX II-101 デバイスは、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、次の形式となります。

Raritan:G{GROUP_NAME}

GROUP_NAME は文字列で、ユーザが属するグループの名前を示します。

RADIUS 通信交換仕様

KX II-101 ユニットは、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログオン	
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)	KX II-101 ユニットの IP アドレス

属性	データ
ログオン	
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)	KX II-101 ユニットの 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
ログオフ	
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)	KX II-101 ユニットの 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

LDAP スキーマの更新

注: この章に記載されている手順は、経験豊富なユーザのみが行うようにしてください。

ユーザ グループ情報を返す

この章の情報を参考にして、認証の成功後にユーザ グループ情報を返すよう設定します (認証を補助します)。

LDAP から返す場合

LDAP/LDAPS 認証に成功すると、KX II-101 では、ユーザ 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 LDAP サーバは、以下の名前の属性を返すことで、これらのユーザ グループ名を指定できます。

rciusergroup attribute type: string

これには、LDAP/LDAPS サーバ上でスキーマの拡張が必要な場合があります。 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。

Microsoft Active Directory から返す場合

注: この操作は、経験豊富な Active Directory 管理者のみが行うようにしてください。

Windows 2000 Server の Microsoft Active Directory からユーザ グループ情報を返すには、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 の該当するマニュアルを参照してください。

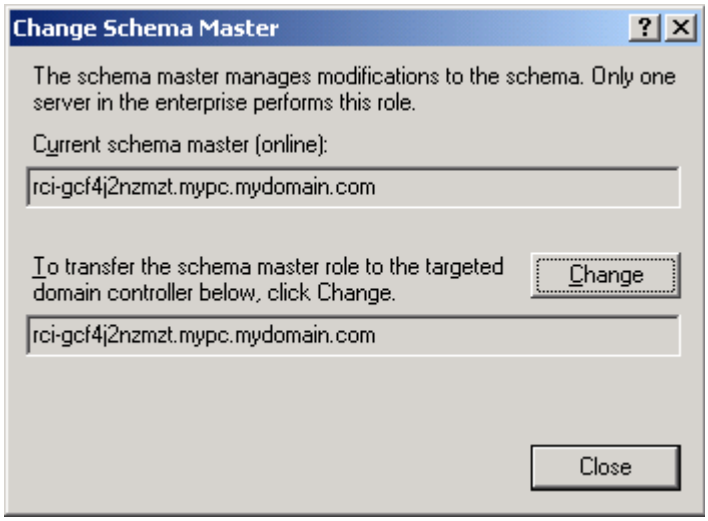
1. Active Directory のスキーマ プラグインをインストールします。手順については、Microsoft Active Directory のマニュアルを参照してください。
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するためのレジストリ設定

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には、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、以下の手順に従います。*

1. ウィンドウの左ペイン (メニューをクリックして表示される領域) の [Active Directory Schema] (Active Directory スキーマ) ルート ノードを右クリックし、次に [Operations Master] (オペレーション 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 ボックスが表示されます。



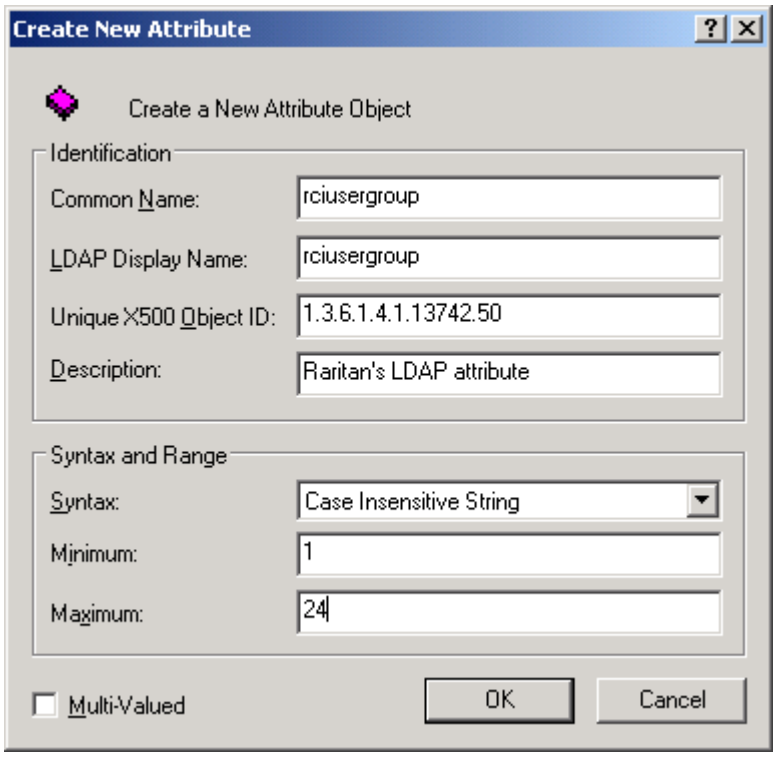
2. (オプション) [The Schema may be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正する) チェック ボックスをオンにします。
3. [OK] をクリックします。

新しい属性の作成

➢ *rciusergroup クラスの新しい属性を作成するには、以下の手順に従います。*

1. ウィンドウの左ペインの [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. 左ペインの [Attributes] (属性) を右クリックします。

3. [New] (新規) をクリックして、[Attribute] (属性) を選択します。 警告メッセージが表示されたら、[Continue] (続ける) をクリックします。[Create New Attribute] (新規属性の作成) ダイアログ ボックスが表示されます。



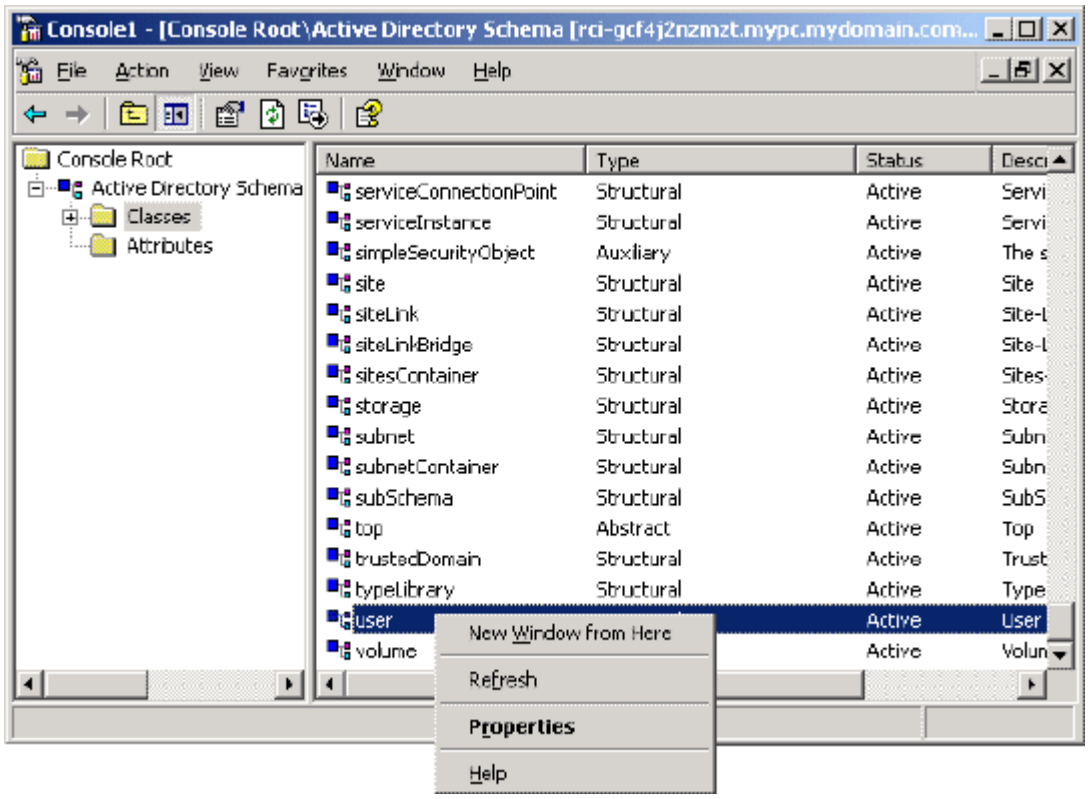
4. [Common Name] (共通名) フィールドに「*rciusergroup*」と入力します。
5. [LDAP Display Name] (LDAP 表示名) フィールドに「*rciusergroup*」と入力します。
6. [Unique x5000 Object ID] (一意の x5000 オブジェクト ID) フィールドに「*1.3.6.1.4.1.13742.50*」と入力します。
7. わかりやすい説明を [Description] (説明) フィールドに入力します。
8. [Syntax] (構文) ドロップダウン矢印をクリックし、リストから [Case Insensitive String] (大文字/小文字の区別のない文字列) を選択します。
9. [Minimum] (最小) フィールドに「*1*」を入力します。
10. [Maximum] (最大) フィールドに「*24*」を入力します。
11. [OK] をクリックして、新しい属性を作成します。

クラスへの属性の追加

➢ *属性をクラスに追加するには、以下の手順に従います。*

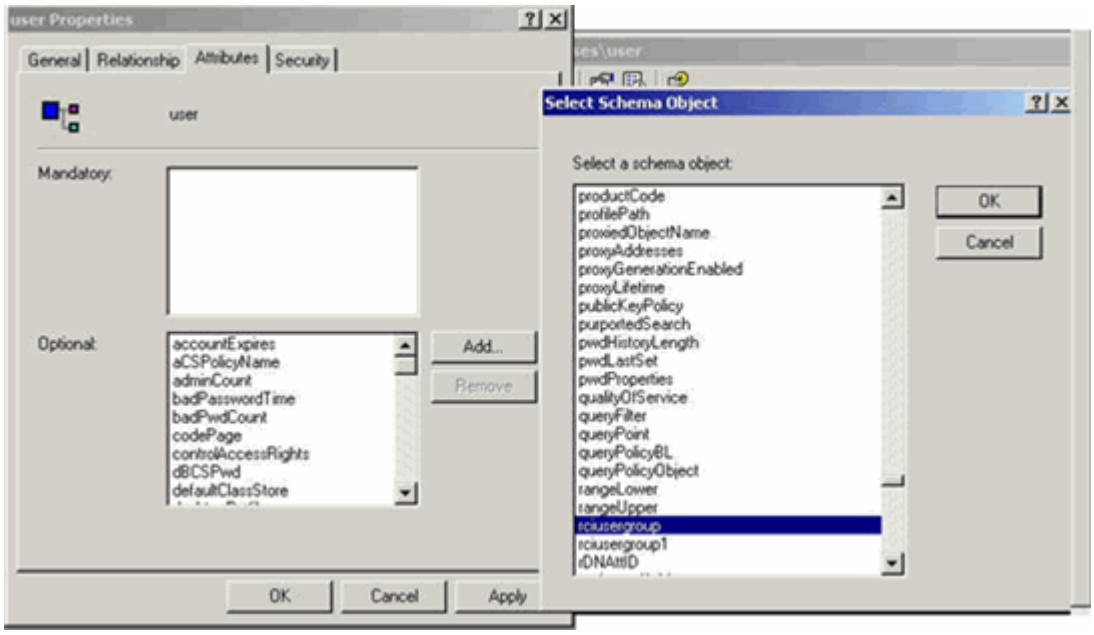
1. ウィンドウの左ペインの [Classes] (クラス) をクリックします。

2. 右ペインで [user] (ユーザ) クラスまでスクロールし、右クリックします。



3. メニューから [Properties] (プロパティ) を選択します。 [user Properties] (ユーザ プロパティ) ウィンドウが表示されます。

4. [Attributes] (属性) タブをクリックして開きます。



5. [Add] (追加) をクリックします。
6. [Select Schema Object] (スキーマ オブジェクト選択) リストから「rciusergroup」を選択します。
7. [Select Schema Object] (スキーマ オブジェクト選択) ダイアログ ボックスで [OK] をクリックします。
8. [User Properties] (ユーザ 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 キャッシュの更新

➢ *スキーマ キャッシュを更新するには、以下の手順に従います。*

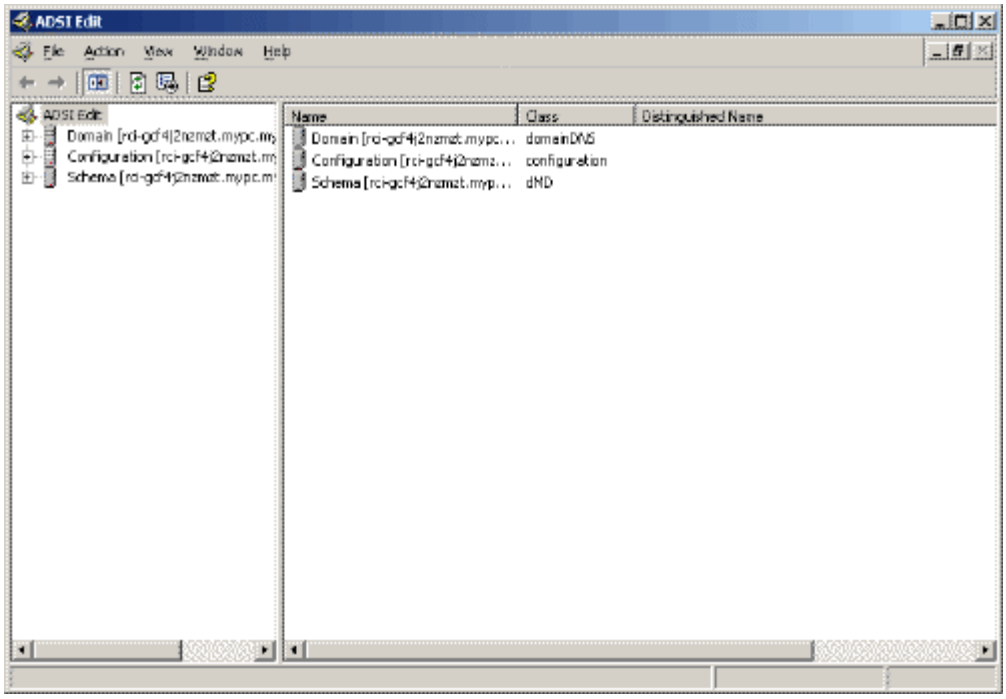
1. ウィンドウの左ペインの [Active Directory Schema] (Active Directory スキーマ) を右クリックして、ショートカット メニューから [Reload the Schema] (スキーマの再ロード) を選択します。
2. Active Directory スキーマ MMC (Microsoft Management Console) コンソールを最小化します。

ユーザ メンバの rciusergroup 属性の編集

Windows 2003 Server 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 2003 サーバ インストール CD 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読み込まれます。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、ディレクトリ サービスと共通の管理タスクを実行できます。

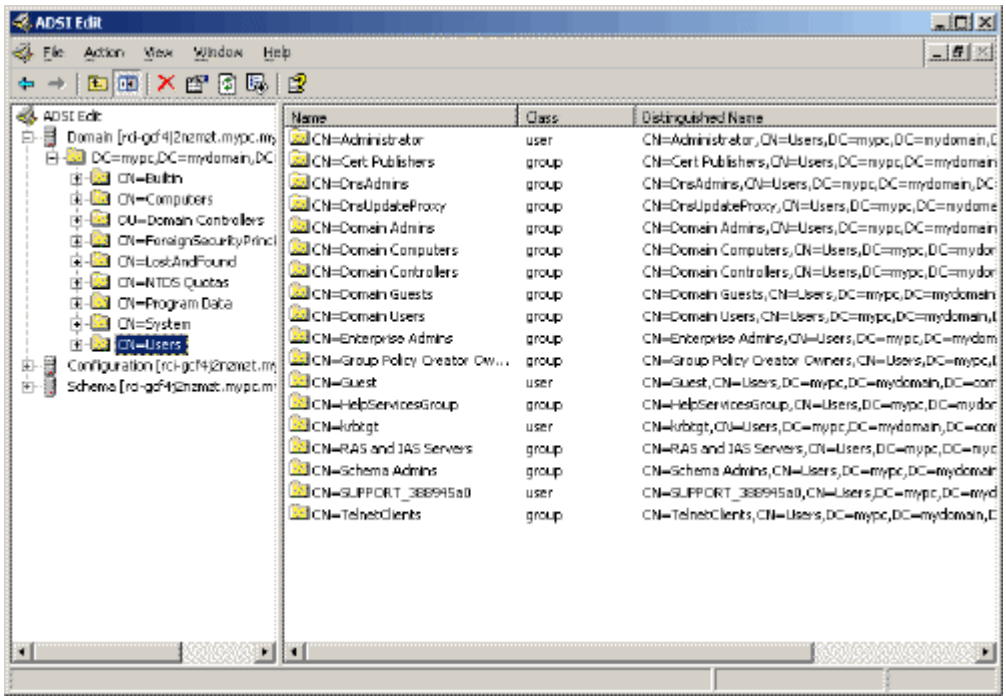
➢ *グループ rciusergroup 内の個別のユーザ属性を編集するには、以下の手順に従います。*

1. Windows 2003 サーバ インストール CD で [Support] (サポート)、[Tools] (ツール)を選択します。
2. SUPTOOLS.MSI をダブルクリックして、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ディレクトリに進みます。
4. adsiedit.msc を実行します。[ADSI Edit] (ADSI 編集) ウィンドウが開きます。



5. [Domain] (ドメイン) を開きます。

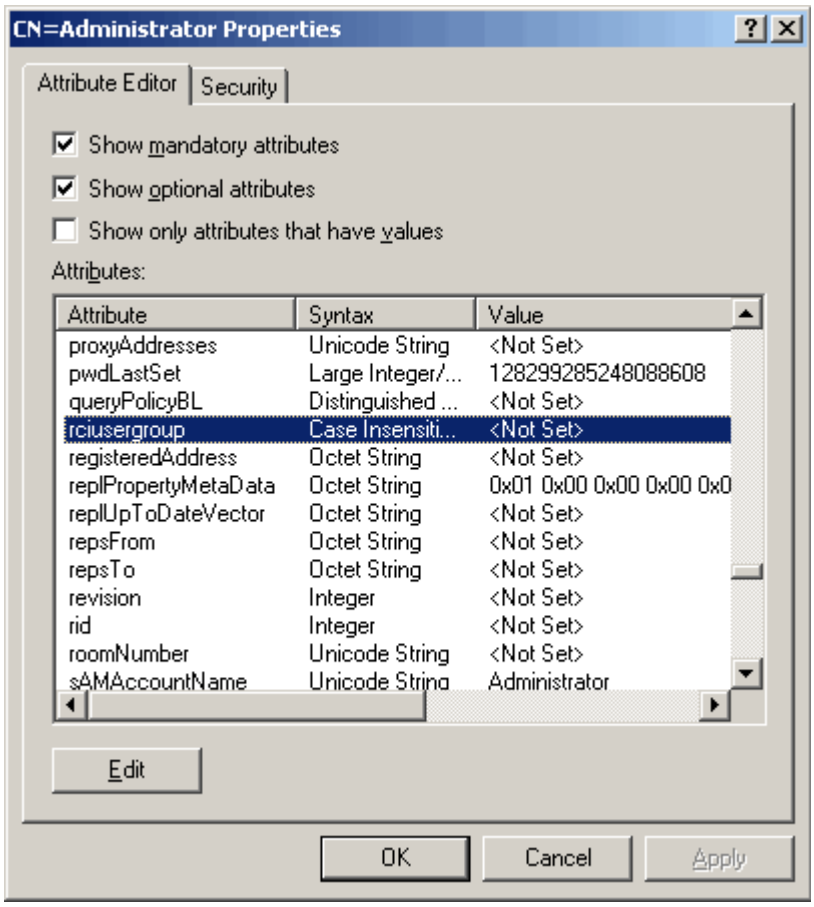
6. ウィンドウの左側のペインで「CN=Users」フォルダを選択します。



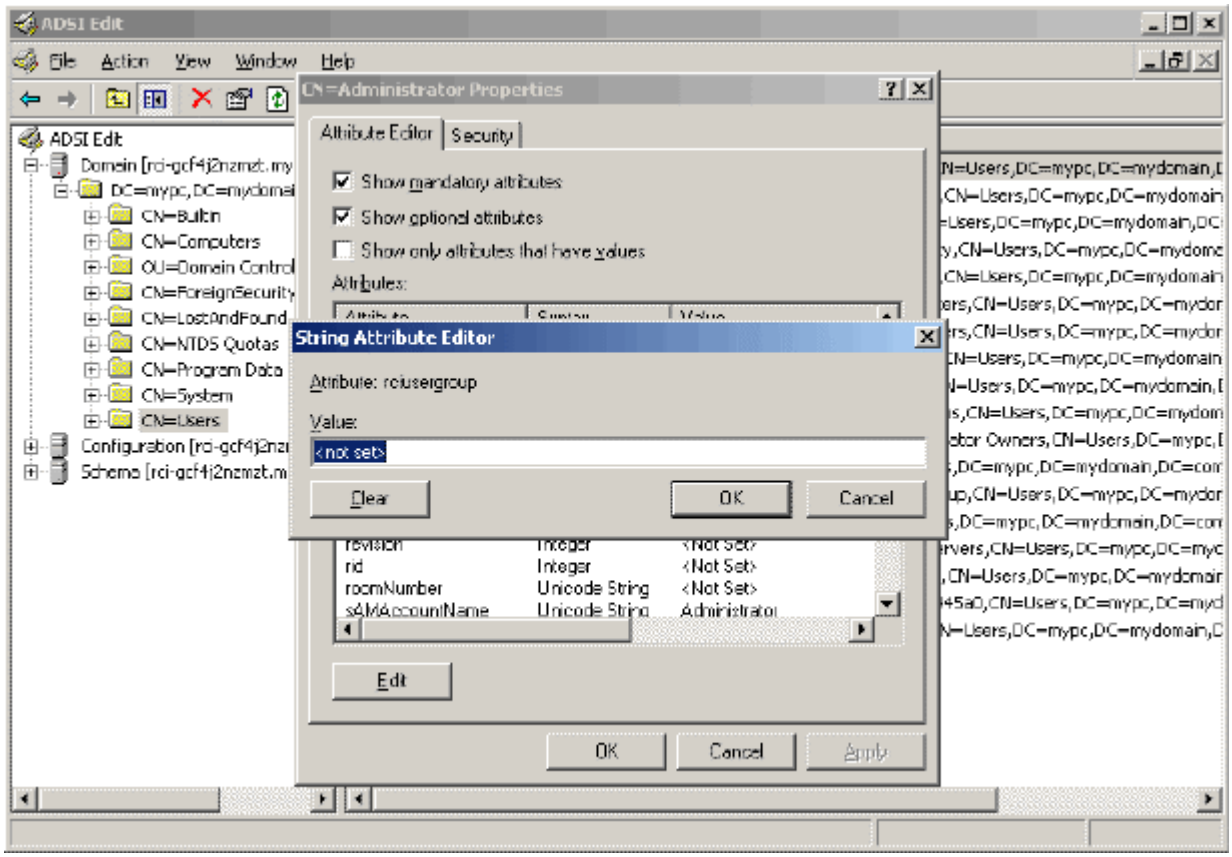
7. 右側のペインからプロパティを編集するユーザ名を選択します。 ユーザ名を右クリックして、[Properties] (プロパティ) を選択します。

8. [Attribute Editor] (属性エディタ) タブをクリックします(まだ開いていなかった場合)。

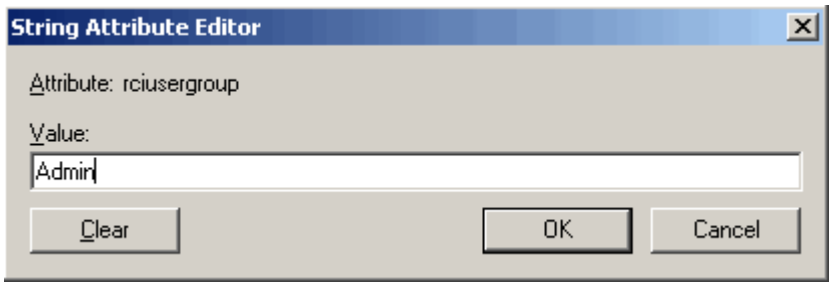
9. [Attributes] (属性) リストから「rciusergroup」を選択します。



10. [Edit] (編集) をクリックします。 [String Attribute Editor] (文字列属性エディタ) ダイアログ ボックスが表示されます。



11. ユーザ グループ (Dominion KX II-101 で作成済み) を [Edit Attribute] (属性の編集) フィールドに入力します。



12. [OK] をクリックします。

6 Virtual KVM Client

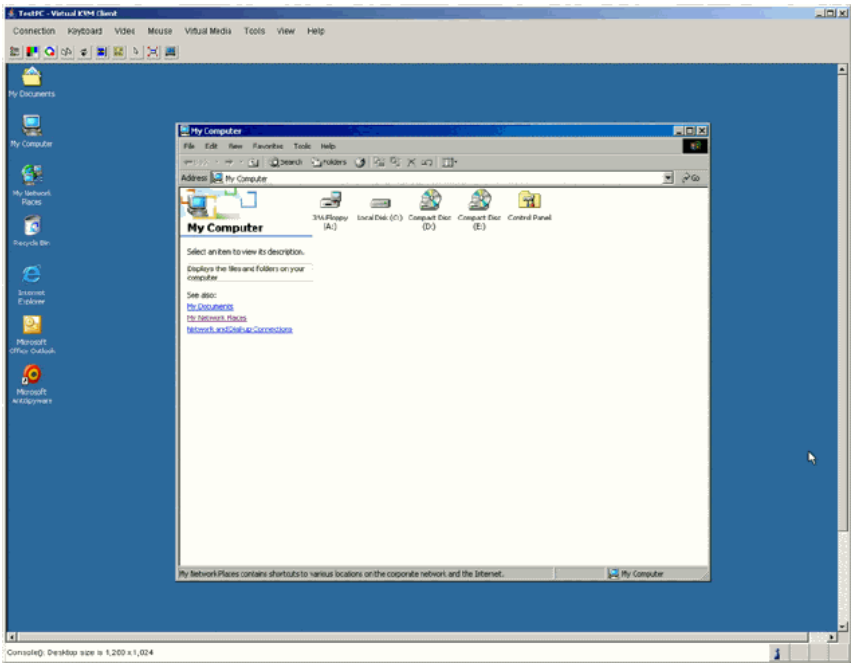
この章の内容

概要

KX II-101 リモート コンソールを使用してターゲット サーバにアクセスすると、Virtual KVM Client のウィンドウが開きます。

Virtual KVM Client ウィンドウは、お使いのコンピュータのデスクトップ上で最小化、最大化、および移動できます。

注: HTML ブラウザ表示を更新すると Virtual KVM Client 接続が切断されてしまうので注意してください。



Virtual KVM Client に用意されている機能は、メニューおよびツール バーを使用してアクセスできます。

機能	説明
メニュー バー	コマンドや設定のドロップダウン メニュー
ツール バー	よく使う機能やコマンドのショートカット ボタン
ターゲット サーバのビデオ ウィンドウ	ターゲット デバイスの表示
ステータス バー	接続パラメータ、ターゲット サーバのウィンドウ サイズ、同時接続、Caps Lock インジケータ、Num Lock インジケータに関するリアルタイム情報

オプション

メニュー ツリー

以下のリストに、Virtual KVM Client のすべてのメニューとメニュー項目を示します。

- [Connection] (接続) メニュー:
  - [Properties] (プロパティ)
  - [Connection Info] (接続情報)
  - [Exit] (終了)
- [Keyboard] (キーボード) メニュー:
  - [Send Ctrl + Alt + Delete] (Ctrl + Alt + Delete の送信)
  - [Keyboard Macros] (キーボード マクロ)
  - [Keyboard Mouse Options] (キーボード マウス オプション)
  - [User-Created Macros] (ユーザ作成マクロ) **オプション**
- [Video] (ビデオ) メニュー:
  - [Refresh Screen] (画面の更新)
  - [Auto-sense Video Settings] (ビデオ設定の自動検出)
  - [Calibrate Color] (色調整)
  - [Video Settings] (ビデオ設定)
- [Mouse] (マウス) メニュー:
  - [Synchronize Mouse] (マウスの同期)
  - [Single Mouse Cursor] (シングル マウス カーソル)
  - [Absolute] (絶対)
  - [Intelligent] (インテリジェント)
  - [Standard] (標準)
- [Virtual Media] (仮想メディア) メニュー:
  - [Connect Drive] (ドライブの接続)
  - [Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)
- [Tools] (ツール) メニュー:
  - [Options] (オプション)
- [View] (表示) メニュー:
  - [View Toolbar] (ツール バーの表示)

- [Scaling] (拡大、縮小)
- [Target Screen Resolution] (ターゲット画面解像度)

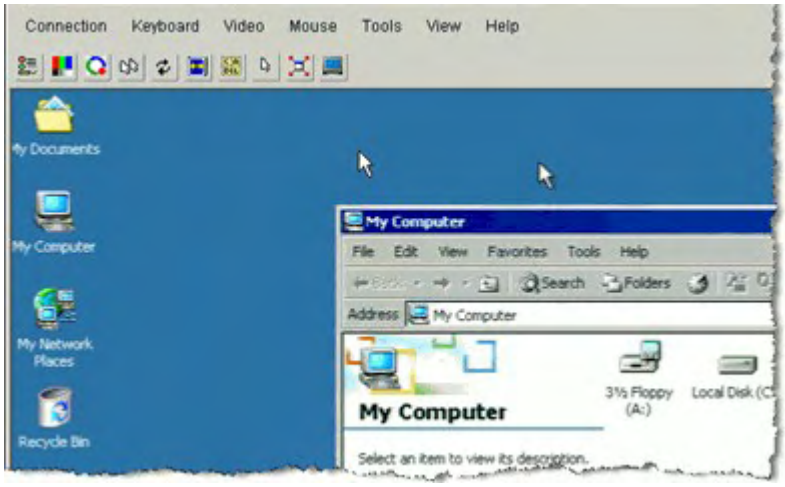
- [Help] (ヘルプ) メニュー:
  - [About Raritan Virtual KVM Client] (バージョン情報)

ツール バー

ボタン	説明
	[Properties] (プロパティ)
	[Video settings] (ビデオ設定)
	[Calibrate color] (色調整)
	[Synchronize the target mouse cursor] (ターゲット マウス カーソルの同期)
	[Refresh screen] (画面の更新)
	[Auto-sense video] (ビデオ自動検出)
	[Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信)
	[Single mouse cursor] (シングル マウス カーソル)
	[Full screen] (全画面)
	[Resize video to fit screen] (画面に合わせてビデオを調整)

マウス ポインタの同期

マウスが使用されているターゲット サーバをリモートで表示する場合、2 つのマウス ポインタが表示されます。 1 つはリモート クライアント ワークステーションのマウス ポインタで、もう 1 つはターゲット サーバのマウス ポインタです。 マウス ポインタが Virtual KVM Client ターゲット サーバ ウィンドウ内にある場合、マウスの動作やクリックは、接続されているターゲット サーバに直接送信されます。 クライアントのマウス ポインタは、マウスの加速設定により、動作がわずかにターゲット マウス ポインタより先行します。



高速 LAN 接続の場合、Virtual KVM Client のマウス ポインタを無効にしてターゲット サーバのマウス ポインタのみを表示することもできます。 この 2 つのモード (シングル マウスとデュアル マウス) は自由に切り替えることができます。 使用可能なマウス モードについての詳細は、*「[Mouse Menu] (マウス) メニュー*『p. 93の "[Mouse] (マウス) メニュー"参照先 』」を参照してください。

マウス同期のヒント

マウスを同期するには、以下の手順に従います。

1. 選択したビデオ解像度と垂直走査周波数が KX II-101 デバイスでサポートされていることを確認します。 [Virtual KVM Client Connection Info] (Virtual KVM Client 接続情報) ダイアログ ボックスには、KX II-101 デバイスの表示で使用している実際の値が表示されます。 サポートされるビデオ解像度についての詳細は、デバイスのユーザ ガイドの「サポートされるビデオ解像度」を参照してください。
2. ケーブルの長さが選択したビデオ解像度に指定されている限度内であることを確認します。 詳細は、デバイス ユーザ ガイドの「ターゲット サーバの接続距離とビデオ解像度」を参照してください。
3. インストール プロセス中にマウスとビデオが正しく構成されていることを確認します。 詳細は、デバイス ユーザ ガイドの「インストールと設定」を参照してください。

4. [Virtual KVM Client auto-sense] (Virtual KVM Client の自動検出) ボタンをクリックして自動検出を強制します。
5. 以上の手順で Linux、UNIX、Solaris KVM ターゲット サーバのマウス同期が改善しない場合は、以下の手順に従います。
   a. ターミナル ウィンドウを開きます。
   b. コマンド「*xset mouse 1 1*」を入力します。
   c. ターミナル ウィンドウを閉じます。
6. [Virtual KVM Client mouse synchronization] (Virtual KVM Client マウス同期)  ボタンをクリックします。

インテリジェント マウス モードでの追加の注意事項

- 同期ルーチンが利用する領域を空けるため、画面の左上隅にアイコンやアプリケーションがないことを確認します。
- アニメーション カーソルを使用しないでください。
- KVM ターゲット サーバでアクティブなデスクトップを無効にします。

[Connection] (接続) メニュー

[Properties] (プロパティ) ダイアログ ボックス

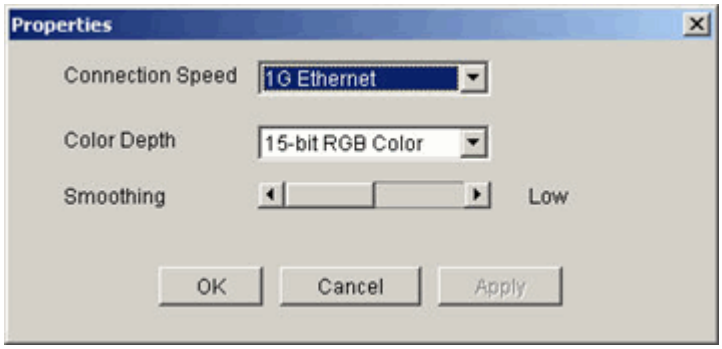
KX II-101 の動的ビデオ圧縮アルゴリズムは、さまざまな帯域幅条件で KVM コンソールの使用を可能にします。 KX II-101 ユニットの KVM 出力は、LAN 経由だけでなく WAN 経由でも使用できるように最適化されます。 さらに、色深度を制御してビデオ出力を制限できるため、さまざまな帯域幅でビデオ画質とシステム応答性のバランスを最適に維持することができます。

	[Connection Properties] (接続プロパティ)	帯域幅に関連するオプション (接続スピード、色深度など) を手動で調整します。

[Properties] (プロパティ) ダイアログ ボックスのパラメータは、さまざまな動作環境の要件に合わせて最適に設定できます。

➢ *接続プロパティを設定するには、以下の手順に従います。*

1. [Connection] (接続)、[Properties] (プロパティ) を選択します。 [Properties] (プロパティ) ダイアログ ボックスが開きます。



2. ドロップダウン リストから接続スピードを選択します。 KX II-101 では、使用可能な帯域幅を自動的に検知できるため、利用する帯域幅は制限されません。ただし、帯域幅の制限に応じて帯域幅利用を調整することもできます。

   [Auto] (自動)

   [1G Ethernet]

   [100 Mb Ethernet]

   [10 Mb Ethernet]

   [1.5 Mb (MAX DSL/T1)]

   [1 Mb (Fast DSL/T1)] (1 Mbps (高速 DSL/T1))

[512 Kb (Medium DSL/T1)]
(512 Kbps (中速 DSL/T1))

[384 Kb (Slow DSL/T1)]
(384 Kbps (低速 DSL/T1))

[256 Kb (Cable)] (256 Kbps (
ケーブル))

[128 Kb (Dual ISDN)] (128
Kbps (デュアル ISDN))

これらの設定は、実際の速度ではなく特定の条件に対して最適化されています。クライアントおよびサーバは、現在のネットワーク速度やエンコード設定に関係なく、常に最高速度でネットワークにビデオを配信しようとします。 ただし、システムの応答性が最も高くなるのは、設定が実際の環境と一致するときだけです。

3. ドロップダウン リストから色深度を選択します。 KX II-101 では、リモート ユーザに送信される色深度を動的に調整することで、さまざまな帯域幅で最適な使いやすさを実現します。

   15 ビット RGB カラー

   8 ビット RGB カラー

   4 ビット カラー

   [4-bit Gray] (2 ビット
   グレー)

   [3-bit Gray] (2 ビット
   グレー)

   [2-bit Gray] (2 ビット
   グレー)

   [Black and White] (モ
   ノクロ)

   重要: 多くの管理タスク (サーバの監視、再設定等) において、最新のビデオ グラフィック カードのほとんどで利用できる 24 ビットまたは 32 ビットのフルカラー表示は必要ありません。 このような高い色深度を送信すると、ネットワークの帯域幅を浪費することになります。

   ---

4. スライダを使用して、スムージングのレベルを指定します (15 ビット カラー モードのみ)。 ここで設定したスムージングのレベルにより、色がわずかに異なる画面領域をできるだけ滑らかな単色の組み合わせにするかが決まります。 スムージングにより、表示されるビデオ ノイズを軽減することで、対象ビデオの画質が向上します。

5. [OK] をクリックして、これらのプロパティを保存します。

➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) をクリックします。

[Connection Info] (接続情報)

➢ *Virtual KVM Client 接続に関する情報を取得するには、以下の手順に従います。*

- [Connection] (接続)、[Connection Info] (接続情報) を選択します。 [Connection Info] (接続情報) ウィンドウが開きます。

現在の接続に関する以下の情報が表示されます。

- [Device Name] (デバイス名)。 KX II-101 デバイスの名前です。
- [IP Address] (IP アドレス)。 KX II-101 の IP アドレスです。
- [Port] (ポート)。 ターゲット デバイスへのアクセスに使用される KVM 通信 TCP/IP ポートです。
- [Data In/Second] (データ入力/秒)。 入力データ レートです。
- [Data Out/Second] (データ出力/秒)。 出力データ レートです。
- [Connect Time] (接続時間)。 接続時間です。
- [FPS] ビデオで送信される毎秒フレーム数です。
- [Horizontal Resolution] (水平解像度) 水平方向の画面解像度です。
- [Vertical Resolution] (垂直解像度) 垂直方向の画面解像度です。
- [Refresh Rate] (垂直走査周波数)。 画面の更新頻度を表します。
- [Protocol Version] (プロトコル バージョン)。 RFB プロトコル バージョンです。

➢ *この情報をコピーするには、以下の手順に従います。*

- [Copy to Clipboard] (クリップボードにコピー) をクリックします。 これにより、任意のプログラムにこの情報を貼り付けることができます。

[Exit] (終了)

➢ *Virtual KVM Client (現在アクセスしているターゲット) を閉じるには、以下の手順に従います。*

- [Connection] (接続) の [Exit] (終了) を選択します。

[Keyboard] (キーボード) メニュー

[Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信)

頻繁に使用されるため、Ctrl+Alt+Delete キーボード マクロは、Virtual KVM Client にあらかじめ組み入れらています。

このキー シーケンスは、現在接続されているターゲット サーバに送信されます。 一方、Virtual KVM Client の使用中に Ctrl+Alt+Delete キーを押した場合、キー シーケンスは意図したとおりにはターゲット サーバへ送信されず、オペレーティング システムの構造により、まず使用している PC がコマンドを解釈します。

	[Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信)	ターゲット サーバに Ctrl+Alt+Delete キー シーケンスを送信します。

➢ *ターゲット サーバに Ctrl+Alt+Delete キー シーケンスを送信するには、以下の手順に従います。*

- [Keyboard] (キーボード) の [Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信) を選択します。または、
- ツール バーの [Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信) ボタンをクリックします。

[Keyboard Macros] (キーボード マクロ)

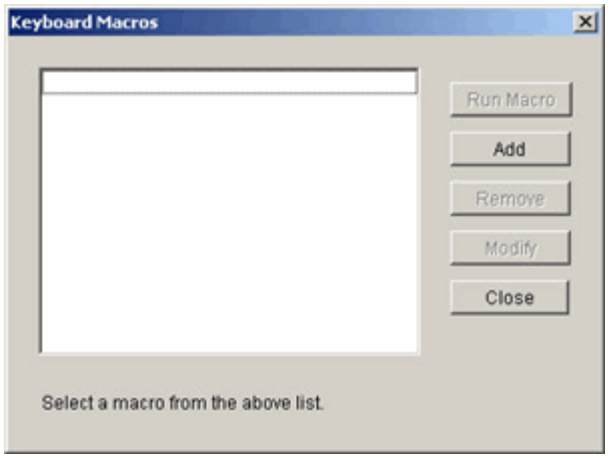
キーボード マクロを利用することで、ターゲット サーバに対するキー入力が確実にターゲット サーバに送信され、ターゲット サーバのみで解釈されます。 キーボード マクロを利用しない場合、Virtual KVM Client が実行されているコンピュータ (クライアント PC) によって解釈される可能性があります。

マクロはクライアント PC に保存され、その PC 専用になります。したがって、別の PC を使用したときは、作成したマクロを使用できません。 さらに、キーボード マクロはコンピュータ単位で管理されるので、あるユーザが使用している PC に別のユーザが自分の名前でログインした場合でも、1 人目のユーザが作成したマクロが 2 人目のユーザに対して表示されます。 Virtual KVM Client 内で作成したキーボード マクロは MPC で使用でき、またその逆も可能です。

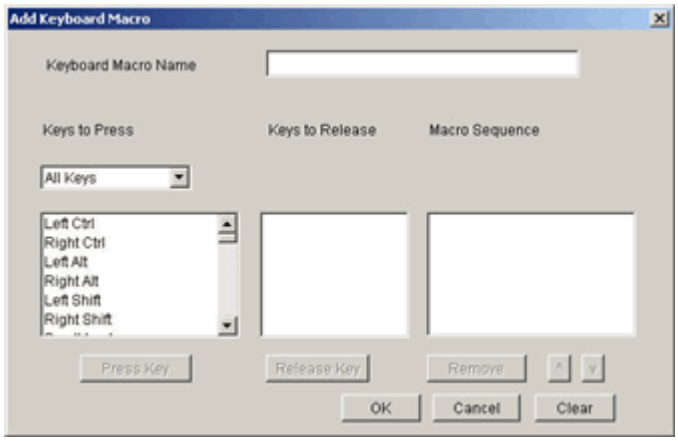
キーボード マクロの作成

➢ *キーボード マクロを作成（追加）するには、以下の手順に従います。*

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。 [Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。



2. [Add] (追加) をクリックします。 [Add Keyboard Macro] (キーボード マクロの追加) ダイアログ ボックスが表示されます。



3. [Keyboard Macro Name] (キーボード マクロ名) フィールドに名前を入力します。 この名前は、マクロが作成された後に Virtual KVM Client メニューバーに表示されます。 この例では、「Minimize All Windows」 (全ウィンドウを最小化) を使用します。

4. [Keys to Press] (押すキー) ドロップダウン リストで、以下の操作を行います。

   a. スクロールして、キー操作をエミュレートするキーを選択します (押す順番で選択してください)。

b. 1 つ選択するごとに、[Press Key] (キーを押す) ボタンをクリックします。 キーを選択するたびに、そのキーが [Keys to Release] (リリースするキー) フィールドに表示されます。

この例では、Windows キーと D キーの 2 つのキーを選択します。

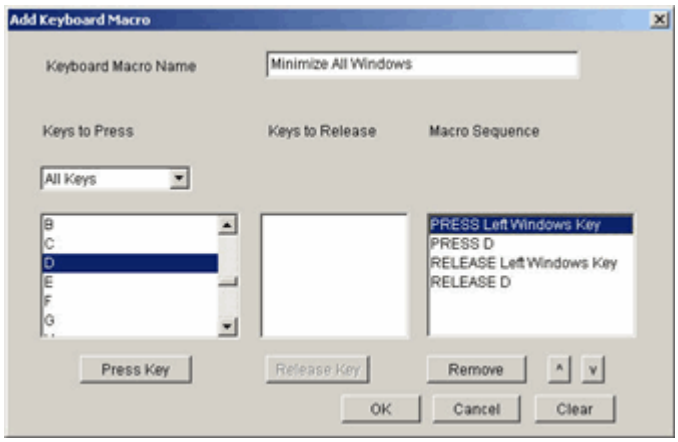
5. [Keys to Release] (リリースするキー) フィールドで、以下の操作を行います。

   a. キー リリースをエミュレートするキーを選択します (リリースする順番で選択してください)。

   b. 1 つ選択するごとに、[Release Key] (キーをリリース) をクリックします。

   この例では、押したキーが両方ともリリースされる必要があります。

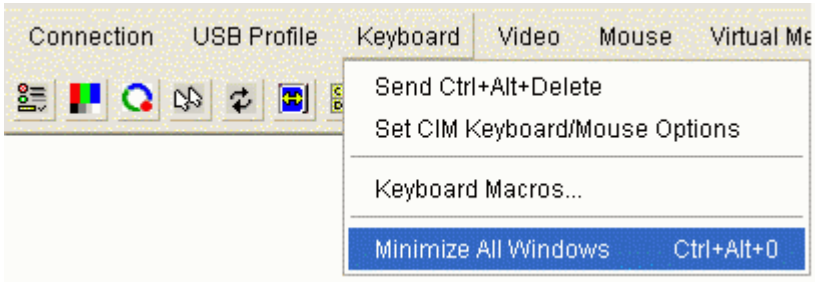
6. [Macro Sequence] (マクロ シーケンス) を確認します。この内容は、[Keys to Press] (押すキー) と [Keys to Release] (リリースするキー) の指定内容に応じて自動的に生成されます。 [Macro Sequence] (マクロ シーケンス) の内容が目的のキー シーケンスであることを確認します。 (キー操作の 1 つの手順を削除するには、手順を選択して [Remove] (削除) をクリックします。)



ヒント: [^] キー ボタンと [v] キー ボタンを使用すると、キー シーケンスを並べ替えることができます。

7. [Add Keyboard Macro] (キーボード マクロの追加) ダイアログ ボックスで [OK] をクリックしてマクロを保存します。

8. [Keyboard Macro] (キーボード マクロ) ダイアログ ボックスで [Close] (閉じる) をクリックします。 作成したキーボード マクロが [Keyboard] (キーボード) メニューのオプションとして表示されます。



➢ *すべてのフィールドをクリアして最初からやり直すには、以下の手順に従います。*

- [Clear] (クリア) ボタンをクリックします。

キーボード マクロの実行

作成したキーボード マクロは、[Keyboard] (キーボード) メニューのマクロ名をクリックすることで実行できます。

➢ *(この例を使用して) マクロを実行するには、以下の手順に従います。*

- [Keyboard] (キーボード) の [Minimize All Windows] (全ウィンドウを最小化) を選択します。

  また、[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスからマクロを選択することもできます。

➢ *マクロを実行するには、以下の手順に従います。*

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。 [Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Run Macro] (マクロの実行) をクリックします。

キーボード マクロの変更

➢ *マクロを変更するには、以下の手順に従います。*

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。 [Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。

3. [Modify] (変更) をクリックします。 [Add/Edit Keyboard Macro] (キーボード マクロの追加/編集) ダイアログ ボックスが表示されます。
4. 必要な変更を加えます。
5. [OK] をクリックします。

キーボード マクロの削除

➢ *マクロを削除するには、以下の手順に従います。*

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。 [Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Remove] (削除) をクリックします。 マクロが削除されます。

[Video] (ビデオ) メニュー

ビデオの設定を自動的に更新する方法はいくつかあります。

- [Refresh Screen] (画面の更新) オプションを使用すると、ビデオ画面が更新されます。
- [Auto-sense Video Settings] (ビデオ設定の自動検出) オプションを使用すると、ターゲット サーバのビデオ設定が自動的に検出されます。
- [Calibrate Color] (色調整) オプションを使用すると、ビデオの表示色が調整されます。

これに加え、[Video Settings] (ビデオ設定) オプションを使用すると、手動で設定を調整できます。

[Refresh Screen] (画面の更新)

[Refresh Screen] (画面の更新) オプションを使用すると、ビデオ画面が更新されます。

	[Refresh Screen] (画面の更新) ボタン

➢ *ビデオ設定を更新するには、次のいずれかの手順に従います。*

- [Video] (ビデオ) の [Refresh Screen] (画面の更新) を選択します。
- ツール バーの [Refresh Screen] (画面の更新) ボタンをクリックします。

[Auto-sense Video Settings] (ビデオ設定の自動検出)

[Auto-sense Video Settings] (ビデオ設定の自動検出) オプションを使用すると、ビデオ設定 (解像度、垂直走査周波数) が再検出され、ビデオ画面が再描画されます。

	[Auto-sense Video Settings] (ビデオ設定の自動検出) ボタン

➢ *ビデオ設定を自動的に検出するには、次のいずれかの手順に従います。*

- [Video] (ビデオ) の [Auto-sense Video Settings] (ビデオ設定の自動検出) を選択します。
- ツール バーの [Auto-sense Video Settings] (ビデオ設定の自動検出) ボタンをクリックします。

調整が行われていることを示すメッセージが表示されます。

[Calibrate Color] (色調整)

[Calibrate Color] (色調整) コマンドは、送信されたビデオ画像の色レベル (色相、輝度、彩度) を最適化するために使用します。 KX II-101 の色設定は、ターゲット サーバごとに適用されます。

	[Calibrate Color] (色調整)	色設定を調整してビデオ表示を最適化します。

注: [Calibrate Color] (色調整) オプションは、現在の接続のみに適用されます。

➢ *色を調整するには、以下の手順に従います。*

1. グラフィカル ユーザ インタフェースが動作しているターゲット サーバに対して KVM リモート接続を開きます。
2. [Video] (ビデオ) の [Calibrate Color] (色調整) を選択します (または、[Calibrate Color] (色調整) ボタンをクリックします)。 ターゲット デバイス画面の色が調整されます。

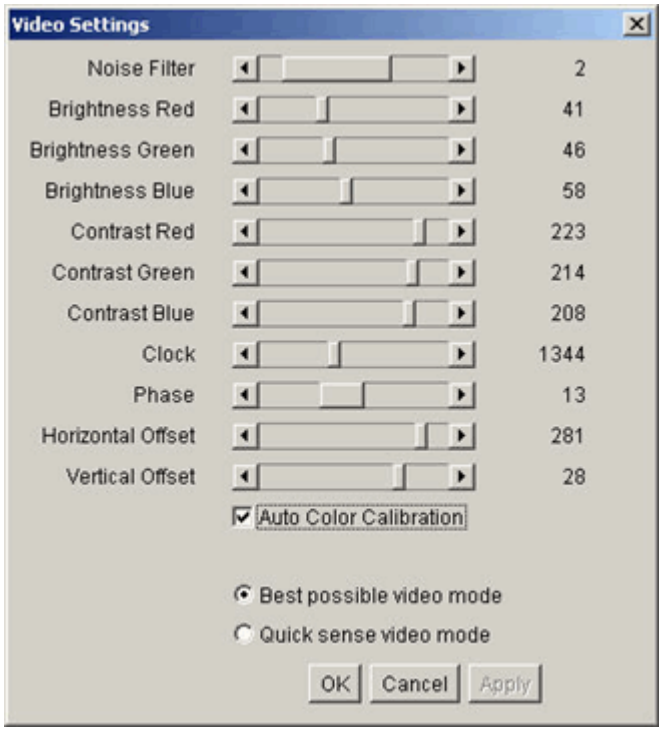
[Video Settings] (ビデオ設定)

[Video Settings] (ビデオ設定) オプションを使用すると、ビデオ設定を手動で調整できます。

	[Video Settings] (ビデオ設定)	ビデオ パラメータを手動で調整するための [Video Settings] (ビデオ設定) 画面を開きます。

➢ *ビデオ設定を変更するには、以下の手順に従います。*

1. [Video] (ビデオ) の [Video Settings] (ビデオ設定) を選択します。 [Video Settings] (ビデオ設定) ダイアログ ボックスが表示され、現在の設定が表示されます。



2. スライダを使用して、目的の結果が得られるように設定を調整します (設定を調整すると、その効果が即座に表示に反映されます)。

   - [Noise Filter] (ノイズ フィルタ): KX II-101 では、グラフィック カードからのビデオ出力の電気的干渉を除去することができます。 この機能により、画質が最適化され、消費される帯域幅が低減されます。 設定値を大きくすると、ピクセル変動は隣接するピクセルと比較して大きな色変化がある場合にのみ送信されます。 ただし、しきい値を高く設定しすぎると、正常な画面変更が意図せずフィルタリングされてしまう場合があります。
     設定値を低くすると、ほとんどのピクセル変動が送信されます。 しきい値を低く設定しすぎると、帯域幅の使用量が高くなることがあります。

   - [Brightness] (明るさ): この設定は、ターゲット サーバの画面表示の輝度を調整するために使用します。

  - [Red] (赤)。 赤信号の輝度を制御します。
  - [Green] (緑)。 緑信号の輝度を制御します。
  - [Blue] (青)。 青信号の輝度を制御します。
- [Color Contrast Settings] (色のコントラストの設定): コントラストの調節を制御します。
  - [Contrast Red] (赤コントラスト)。 赤信号を制御します。
  - [Contrast Green] (緑コントラスト)。 緑信号を制御します。
  - [Contrast Blue] (青コントラスト)。 青信号を制御します。
- ビデオ画像が大幅にぼやけている場合、設定でクロックと位相を調節することで、アクティブなターゲット サーバの画像を改善します。

警告: クロック設定と位相設定を変更する際には、注意が必要です。ビデオ画像が消えたり歪んだりする可能性があるだけでなく、元の状態に戻せなくなることがあります。 変更を加える前に、Raritan テクニカル サポートにお問い合わせください。

  - [Clock] (クロック)。 ビデオ画面上にビデオ ピクセルが表示される速度を制御します。 クロック設定に変更を加えると、ビデオ画像が水平方向に拡大または縮小されます。奇数値を設定することをお勧めします。通常は自動検出機能によって適切に設定されるため、ほとんどの環境ではこの設定を変更する必要はありません。
  - [Phase] (位相)。 位相の値の範囲は 0～31 です。これより大きな値は反復されます。 アクティブなターゲット サーバ用に最適なビデオ画像が得られる位相の位置で停止してください。
- [Offset] (オフセット): 画面上の位置を制御します。
  - [Horizontal Offset] (水平オフセット)。 ターゲット サーバの画面がモニタに表示されるときの水平位置を制御します。
  - [Vertical Offset] (垂直オフセット)。 ターゲット サーバの画面がモニタに表示されるときの垂直位置を制御します。
- [Auto Color Calibration] (自動色調整)。 色の調整を自動的に行う場合は、このオプションをオンにします。
- [Video Sensing] (ビデオ検出): ビデオ検出モードを選択します。

- [Best possible video mode] (最適ビデオ モード): ターゲットやターゲットの解像度が変更されたときに、すべての自動検出処理が実行されます。 このオプションを選択すると、最適な画像品質になるようにビデオが調整されます。
- [Quick sense video mode] (クイック検出ビデオ モード): このオプションを使用すると、クイック ビデオ自動検出が使用され、ターゲットのビデオがより早く表示されます。 このオプションは、再起動直後のターゲット サーバの BIOS 設定を入力するときに特に有効です。

3. [Apply] (適用) をクリックします。 ビデオ設定が変更されます。

注: 一部の Sun サーバでは、ある種の Sun 背景画面 (外周部が非常に暗いものなど) が中央の位置に正確に表示されない場合があります。 別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。

[Mouse] (マウス) メニュー

ターゲット サーバを制御しているとき、KX II-101 リモート コンソールには、クライアント ワークステーションとターゲット サーバの 2 つのマウス カーソルが表示されます。この場合、シングル マウス モードとデュアル マウス モードのどちらかを使用できます。デュアル マウス モードにおいて設定が適切に行われている場合、2 つのマウス カーソルは同調します。 マウスの同期に問題がある場合は、「ターゲット サーバの設定」を参照してください。

KX II-101 デバイスでは、2 つのマウス カーソルが存在するときに以下のマウス モードが提供されます。

- Absolute (ずれない) (マウス同期)
- Intelligent (インテリジェント) (マウス モード)
- Standard (標準) (マウス モード)

[Synchronize Mouse] (マウスの同期)

デュアル マウス モードで [Synchronize Mouse] (マウスの同期) オプションを使用すると、ターゲット サーバのマウス ポインタと Virtual KVM Client のマウス ポインタとの同期化が再実行されます。

	[Synchronize Mouse] (マウスの同期)

➢ *マウスを同期するには、次のいずれかの手順に従います。*

- [Mouse] (マウス) の [Synchronize Mouse] (マウスの同期) を選択します。
- ツール バーの [Synchronize Mouse] (マウスの同期) ボタンをクリックします。

[Single Mouse Cursor] (シングル マウス カーソル)

[Single Mouse Cursor] (シングル マウス カーソル) を使用すると、「シングル マウス モード」になります。このモードでは、ターゲット サーバのマウス カーソルだけが画面に表示され、ローカル PC のマウス ポインタは表示されません。 シングル マウス モードでは、[Synchronize Mouse] (マウスの同期) オプションは使用できません (単独のマウス カーソルを同期化する必要がないため)。

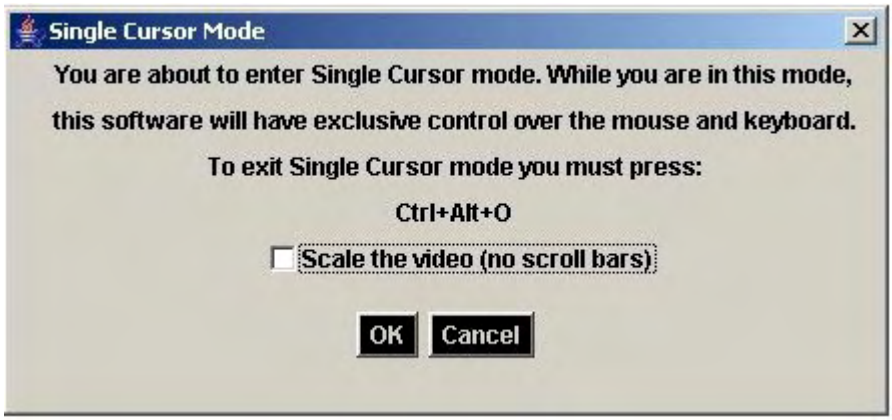
	[Single Mouse Cursor] (シングル マウス カーソル)

➢ *シングル マウス モードに入るには、次のいずれかの手順に従います。*

- [Mouse] (マウス) の [Single Mouse Cursor] (シングル マウス カーソル)を選択します。
- ツール バーの [Single/Double Mouse Cursor] (シングル/ダブル マウス カーソル) ボタンをクリックします。

➢ *シングル マウス モードを終了するには、以下の手順に従います。*

1. シングル マウス モードに切り替えるときは、次のメッセージが表示されます。[OK] をクリックします。



2. シングル マウス モードを終了するには、キーボードの Ctrl+Alt+O を押します。

[Standard] (標準)

これは、相対マウス位置を使用した標準のマウス同期アルゴリズムです。 標準マウス モードを使用する場合、クライアントとサーバのカーソルが同期するように、加速を無効にし、マウスに関連するその他のパラメータを適切に設定する必要があります。 標準マウス モードはデフォルトです。

➢ *標準マウス モードに切り替えるには、以下の手順に従います。*

- [Mouse] (マウス) の [Standard] (標準) を選択します。

[Intelligent] (インテリジェント)

KX II-101 デバイスでは、インテリジェント マウス モードにおいて、ターゲットのマウス設定を検出し、それに応じてマウス ポインタを同期できるので、ターゲットでマウスの加速を設定できます。 このモードでは、マウス カーソルが画面の左上隅で "ダンス" をし、加速を計算します。 このモードが正常に動作するには、特定の条件が満たされる必要があります。

インテリジェント マウス モードについての詳細は、『Raritan Multi-Platform Client ユーザ ガイド』(「付録 B: インテリジェント マウス同期の条件」) を参照してください。このガイドは、Raritan の Web サイト (http://www.raritan.com/support/productdocumentation) から入手可能です。または、KX II-101 に付属の Raritan ユーザ マニュアルおよびクイック セットアップ ガイド CD-ROM を参照してください。

➢ *インテリジェント マウス モードに切り替えるには、以下の手順に従います。*

- [Mouse] (マウス) の [Intelligent] (インテリジェント) を選択します。

インテリジェント マウス同期の条件

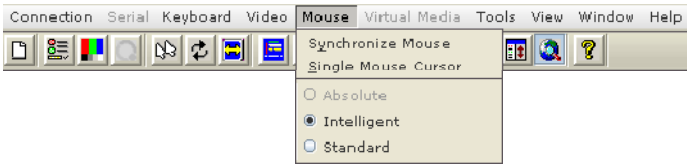
[Mouse] (マウス) メニューにある [Intelligent Mouse Synchronization] (インテリジェント マウス同期) コマンドを選択すると、マウスが動いていないときにマウス カーソルが自動的に同期されます。 この機能を適切に動作させるには、次の条件が満たされている必要があります。

- ターゲットにおいて、アクティブ デスクトップが無効であること。
- ターゲット ページの左上隅にウィンドウが表示されていないこと。
- ターゲット ページの左上隅にアニメーション背景が表示されていないこと。
- ターゲットのマウス カーソルが通常のものであり、アニメーション カーソルでないこと。
- ターゲット マウスの速度が、非常に遅い値や非常に速い値に設定されていないこと。
- [ポインタの精度を高める] や [ポインタを自動的に既定のボタン上に移動する] などの高度なマウス プロパティが無効であること。
- [ビデオ設定] ウィンドウで [最適ビデオ モード] を選択していること。
- ターゲットのビデオの外周部が明確に表示されていること (つまり、ターゲットのビデオ画像の端にスクロールしたときに、ターゲット デスクトップと [リモート KVM コンソール] ウィンドウの間に黒いボーダーが表示されている必要があります)。
- インテリジェント マウス同期機能を使用中に、デスクトップの左上隅にファイル アイコンやフォルダ アイコンがあると、この機能が正しく動作しない可能性があります。 この機能での問題を避けるために、デスクトップの左上隅にファイル アイコンやフォルダ アイコンを置かないことを推奨します。

ターゲット ビデオが自動検出された後で、ツール バーの [Synchronize Mouse] (マウス同期) ボタンをクリックして、手動でマウス同期を開始する必要があります。 ターゲットの解像度が変更された場合や、マウス カーソルが互いに同期しなくなった場合にも、この操作を行います。

インテリジェント マウス同期が失敗した場合、標準マウス同期と同じ動作になります。

マウス設定は、ターゲットのオペレーション システムよって異なります。 詳細については、使用する OS のマニュアルを参照してください。 また、インテリジェント マウス同期は UNIX ターゲットでは機能しません。



[Absolute] (絶対)

注: Absolute Mouse Synchronization は、仮想メディアに対応する USB CIM (D2CIM-VUSB) でのみ使用できます。

このモードでは、ターゲット マウスの加速または速度が異なる値に設定されている場合でも、クライアントとターゲットのポインタを同期するために絶対座標が使用されます。このモードは、USB ポートを備えたサーバでサポートされます。マウス ポインタは、ターゲット サーバ上の正確な位置に移動します。

➢ *絶対マウス モードに切り替えるには、以下の手順に従います。*

- [Mouse] (マウス) の [Absolute] (絶対) を選択します。

VKC 仮想メディア

仮想メディアの設定方法および使用方法についての詳細は、「***仮想メディア*** 『p. 101』」を参照してください。

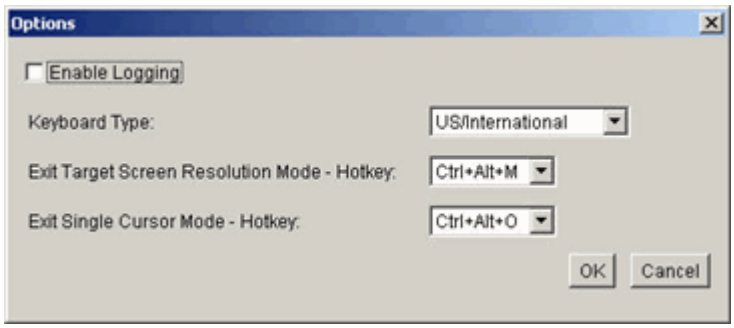
[Tools] (ツール) メニュー

[Options] (オプション)

[Tools] (ツール) メニューでは、Virtual KVM Client に関する特定のオプション (デュアル マウス モードでのマウスの同期、ログ記録の有効化、キーボードの種類、ターゲット画面解像度モードを終了するホットキー) を指定できます。

➢ *ツール オプションを設定するには、以下の手順に従います。*

1. [Tools] (ツール) の [Options] (オプション) を選択します。 [オプション] ウィンドウが表示されます。



2. テクニカル サポートから指示されたときだけ、[Enable Logging] (ログ記録を有効にする) チェックボックスをオンにします。 このオプションをオンにすると、ホーム ディレクトリにログ ファイルが作成されます。
3. 必要に応じて、ドロップダウン リストからキーボードの種類を選択します。 含まれるオプションは次のとおりです。
   - 英語 (アメリカ)/(インターナショナル)
   - フランス語 (フランス)
   - ドイツ語 (ドイツ)
   - 日本語
   - 英語 (イギリス)
   - 韓国語 (韓国)
   - ベルギー語 (ベルギー)
   - ノルウェー語 (ノルウェー)
   - デンマーク語 (デンマーク)
   - スウェーデン語 (スウェーデン)

4. [Exit Target Screen Resolution Mode - Hotkey] (ターゲット画面解像度モードの終了 - ホットキー)。 ターゲット画面解像度モードに切り替えると、ターゲット サーバの表示が全画面表示になり、ターゲット サーバと同じ解像度が取得されます。 これは、このモードを終了するためのホットキーです。ドロップダウン リストから選択します。
5. [Exit Single Cursor Mode] (シングル カーソル モードの終了) - ホットキー。 シングル カーソル モードに入ると、ターゲット サーバのマウス カーソルのみが表示されます。 これは、シングル カーソル モードを終了して、クライアント マウス カーソルに戻るために使用するホットキーで、ドロップダウン リストから選択します。
6. [OK] をクリックします。

[View] (表示) メニュー

[View Toolbar] (ツール バーの表示)

Virtual KVM Client では、ツール バーの表示/非表示を切り替えることができます。

➢ *ツール バーの表示/非表示 (オン/オフ) を切り替えるには、以下の手順に従います。*

- [View] (表示) の [View Toolbar] (ツール バーの表示) を選択します。

[Scaling] (拡大、縮小)

ターゲットのウィンドウを拡大、縮小することで、ターゲット サーバ ウィンドウ全体の内容を表示することができます。 Virtual KVM Client のウィンドウ サイズに合わせて、縦横比を維持したまま、ターゲット ビデオのサイズを拡大または縮小することができるため、スクロール バーを使用することなくターゲット サーバのデスクトップ全体を表示することができます。

➢ *拡大、縮小 (オン/オフ) を切り替えるには、以下の手順に従います。*

- [View] (表示) の [Scaling] (拡大、縮小) を選択します。

[Target Screen Resolution] (ターゲット画面解像度)

ターゲット画面解像度モードに切り替えると、ターゲット サーバの表示が全画面表示になり、ターゲット サーバと同じ解像度が取得されます。 このモードを終了するためのホットキーは、[Options] (オプション) ダイアログ ボックスで指定します (デフォルトは Ctrl+Alt+M です)。

➢ *ターゲット画面解像度モードに切り替えるには、以下の手順に従います。*

- [View] (表示) の [Target Screen Resolution] (ターゲット画面解像度) を選択します。

➢ *ターゲット画面解像度モードを終了するには、以下の手順に従います。*

- [Tools] (ツール) の [Options] (オプション) ダイアログで設定されているホットキーを押します。 デフォルトは Ctrl+Alt+M です。

CC-SG ユーザへの注意事項: [Target Screen Resolution] (ターゲット画面解像度) は無効になっています。KX II-101 デバイスが CC-SG 管理の下にない場合に利用できるのは、全画面モードのみです。

[Help] (ヘルプ) メニュー

[About Raritan Virtual KVM Client] (バージョン情報)

このメニュー オプションを選択すると、Virtual KVM Client のバージョン情報が表示されます。このバージョン情報は、Raritan テクニカル サポートを利用するときに必要になります。

➢ *バージョン情報を調べるには、以下の手順に従います。*

- [Help] (ヘルプ) の [About Raritan Virtual KVM Client] (バージョン情報) を選択します。

7 仮想メディア

この章の内容

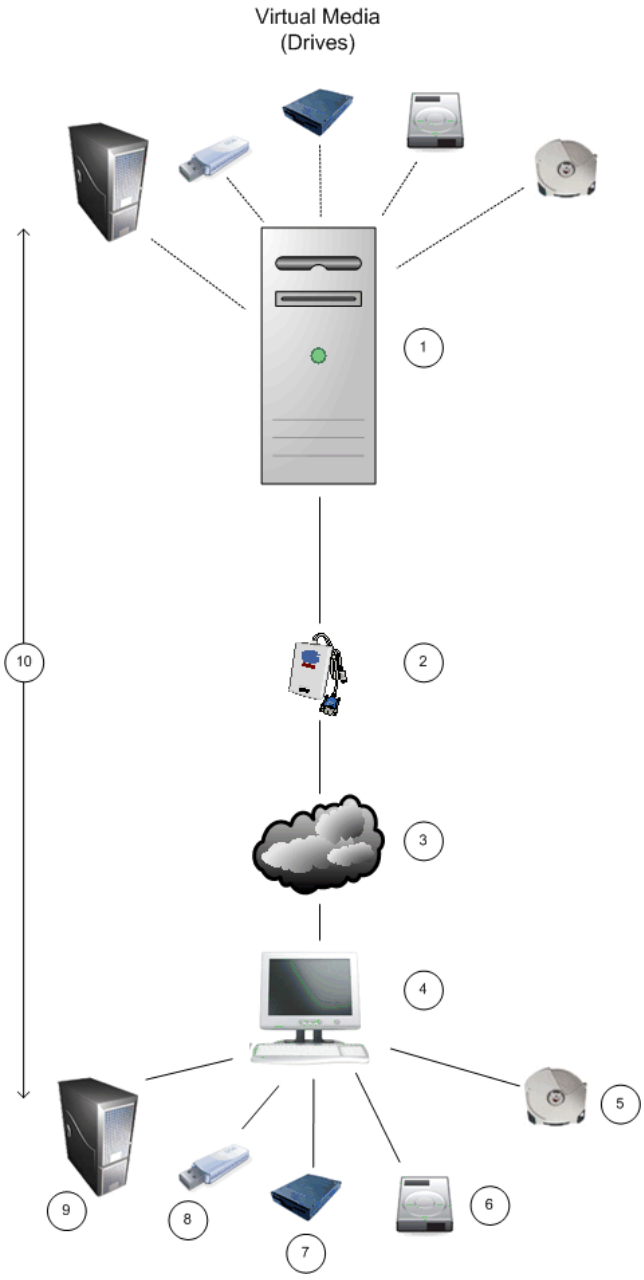
概要

KVM の機能を拡張する仮想メディアを使うことで、クライアント PC やネットワーク ファイル サーバ上のメディアに、リモートの KVM ターゲット サーバからアクセスできるようになります。 この機能を使用すると、クライアント PC やネットワーク ファイル サーバでマウントされたメディアが、ターゲット サーバでも仮想的にマウントされます。 これにより、そのメディアはターゲット サーバ自体に物理的に接続されているような形で読み書きできるようになります。 仮想メディアには、内蔵または USB マウントされた CD ドライブや DVD ドライブ、USB マス ストレージ デバイス、PC のハード ディスク、フロッピー ディスク、ISO イメージ (ディスク イメージ) などを使用できます。

仮想メディアを使用することで、以下のような作業をリモートから実行できるようになります。

- ファイルの転送
- 診断の実行
- アプリケーションのインストールと修正パッチ (patch) の適用
- オペレーティング システムの完全インストール (コンピュータの BIOS でメディアがサポートされる場合)

この拡張 KVM コントロール機能を利用することで、データ センタに出向く必要がなくなり、時間と費用が節約できます。



1 ターゲット サーバ

2 KX II-101

3 KX II-101 からローカル ワークステーションへの IP ネットワーク接続

4 ローカル ワークステーション

5 CD/DVD ドライブ

6 ハード ディスク イメージ ファイル

7 フロッピー ディスク

8 USB メモリスティック

9 リモート ファイル サーバ (ISO イメージ)

10 仮想接続

仮想メディアを使用するための前提条件

仮想メディアを使用するには、次の条件が満たされている必要があります。

KX II-101

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス (VM アクセス ポート権限) を許可するように KX II-101 を設定する必要があります。 ポート権限はグループレベルで設定されます。詳細は、ユーザ ガイドの「ポート権限の設定」を参照してください。
- KX II-101 デバイスとターゲット サーバ間に USB 接続が存在する必要があります。
- **(オプション)** PC 共有を使用する場合は、[Security Settings (セキュリティ設定)] ページで VM Share Mode (VM 共有モード) も有効にする必要があります。
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。 USB プロファイルの選択についての詳細は、ユーザ ガイドの「USB プロファイルの設定」を参照してください。

クライアント PC

- 仮想メディアの一部のオプションを使用するには、クライアント PC に対する管理者特権が必要です (ドライブ全体のドライブ リダイレクト機能など)。

  注: Microsoft Vista を使用している場合は、[ユーザ アカウント制御] をオフにする必要があります。 [コントロール パネル]、[ユーザ アカウント] の順に選択し、[ユーザ アカウント制御] をオフにします。

  Vista アカウントの許可を変更したくない場合は、Internet Explorer を管理者として実行します。 このためには、[スタート] メニューの [Internet Explorer] を右クリックし、[管理者として実行] を選択します。

- USB 2.0 の方が高速なため、推奨されます。

ターゲット サーバ

- KVM ターゲット サーバは USB 接続のドライブをサポートする必要があります。
- Windows 2000 が稼動する KVM ターゲット サーバには、最新の修正プログラムがすべてインストールされている必要があります。

仮想メディアの使用

KX II-101 仮想メディア機能を使用する場合、異なる種類のドライブを 2 台までマウントできます。 このドライブは、VM セッションが有効な間だけアクセスできます。

➢ *仮想メディアを使用するには、以下の手順に従います。*

1. ターゲット サーバからアクセスできるようにするメディアを、クライアントまたはネットワーク ファイル サーバに接続します。 この手順を最初に行う必要はありませんが、このメディアへのアクセスする前に行う必要があります。
2. 適切な***前提条件***『p. 104の"仮想メディアを使用するための前提条件"参照先 』が満たされていることを確認します。
3. (ファイル サーバ ISO イメージの場合のみ) ファイル サーバ ISO イメージにアクセスする場合は、KX II-101 リモート コンソールの ***[File Server Setup] (ファイル サーバのセットアップ) ページ***『p. 111の"ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)"参照先 』を使用して、ファイル サーバとイメージを指定してください。

   注: Raritan は ISO9660 形式を標準でサポートしています。 ただし、それ以外の CD-ROM 拡張も動作する場合があります。
4. 適切なターゲット サーバとの KVM セッションを開きます。
5. 仮想メディアに接続します。

対象メディア	この VM オプションを選択
ローカル ドライブ	***[Connect Drive] (ドライブの接続)***『p. 107の"ローカル ドライブ"参照先 』
ローカル CD/DVD ドライブ	***[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)***『p. 109の"CD-ROM/DVD-ROM/ISO イメージ"参照先 』
ISO イメージ	[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)
ファイル サーバ ISO イメージ	[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)

作業が終わったら、***仮想メディアを切断***『p. 110の"仮想メディアの切断"参照先 』します。

KVM セッションを開く

➢ *KVM セッションを開くには、以下の手順に従います。*

1. KX II-101 リモート コンソールで [Port Access] (ポート アクセス) ページを開きます。

2. [Port Access] (ポート アクセス) ページでターゲット サーバに接続します。
   a. ターゲット サーバの名前をクリックします。
   b. ポップアップ メニューから [Connect] (接続) を選択します。

Virtual KVM Client ウィンドウにターゲット サーバが表示されます。

仮想メディアへの接続

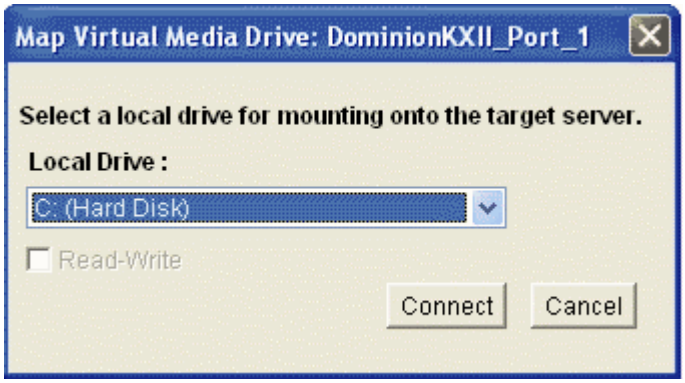
ローカル ドライブ

このオプションを使用すると、ドライブ全体がマウントされます。つまり、クライアントコンピュータのディスク ドライブ全体がターゲット サーバに仮想的にマウントされます。 このオプションは、ハード ディスク ドライブと外部ディスク ドライブにのみ使用してください。ネットワーク ドライブ、CD-ROM ドライブ、DVD-ROM ドライブは対象外です。これは、[Read-Write] (読み取り/書き込み可能) を指定できる唯一の選択肢です。

注: 特定のバージョンの Windows オペレーティング システムが動作している KVM ターゲット サーバでは、NTFS 形式のパーティション (ローカル C ドライブなど) がリダイレクトされた後で新しいマス ストレージ接続を行うことができない場合があります。 その場合には、KX II-101 リモート コンソールを閉じて再接続した後で、別の仮想メディア デバイスをリダイレクトしてください。 同じターゲット サーバに別のユーザが接続している場合、そのユーザの接続も閉じる必要があります。

➢ *クライアント コンピュータのドライブにアクセスするには、以下の手順に従います。*

1. Virtual KVM Client で、[Virtual Media] (仮想メディア) の [Connect Drive] (ドライブの接続) を選択します。 [Map Virtual Media Drive] (仮想メディア ドライブの割り当て) ダイアログ ボックスが表示されます。



2. [Local Drive] (ローカル ドライブ) ドロップダウン リストから、ドライブを選択します。
3. 読み取りと書き込みの機能が必要な場合には、[Read-Write] (読み取り/書き込み可能) チェックボックスをオンにします。 このオプションは、リムーバブル ドライブ以外では無効になっています。 詳細は、「***読み取り/書き込み可能に設定できない状況*** 『p. 108』」を参照してください。 このチェックボックスをオンにすると、接続した USB ディスクに読み取りと書き込みを実行できるようになります。

警告: 読み取り/書き込みアクセスを有効にすると危険な場合があります。 同じドライブに対して同時に複数のクライアント PC からアクセスすると、データが壊れる恐れがあります。 書き込みアクセスが不要な場合は、このオプションをオフのままにしてください。

4. [Connect] (接続) をクリックします。 メディアがターゲット サーバに仮想的にマウントされます。 このメディアには、他のドライブとまったく同じようにアクセスすることができます。

注: ターゲット サーバへの USB 接続がない場合、次のような警告メッセージが表示されます。「The virtual media capability is set up but will not be available until the USB cable is connected or the target is powered on. Please check your USB connectivity or see if the target is powered on. (仮想メディア機能が設定されましたが、USB ケーブルを接続するか、ターゲット サーバの電源をオンにするまで利用できません。USB 接続を確認するか、ターゲット サーバの電源がオンになっているかどうかを確認してください)」。 この問題を解決してからドライブに再接続してください。

読み取り/書き込み可能に設定できない状況

以下の場合、仮想メディアを読み取り/書き込み可能にすることはできません。

- 複数のハード ディスク ドライブすべてが対象の場合。
- ドライブが書き込み保護されている場合。
- ユーザに読み取り/書き込みの権限がない場合。
  - ポート権限の [Access] (アクセス) が [None] (なし) または [View] (表示) に設定されている場合。
  - ポート権限の [VM Access] (VM アクセス) が [Read-Only] (読み取り専用) または [Deny] (拒否) に設定されている場合。

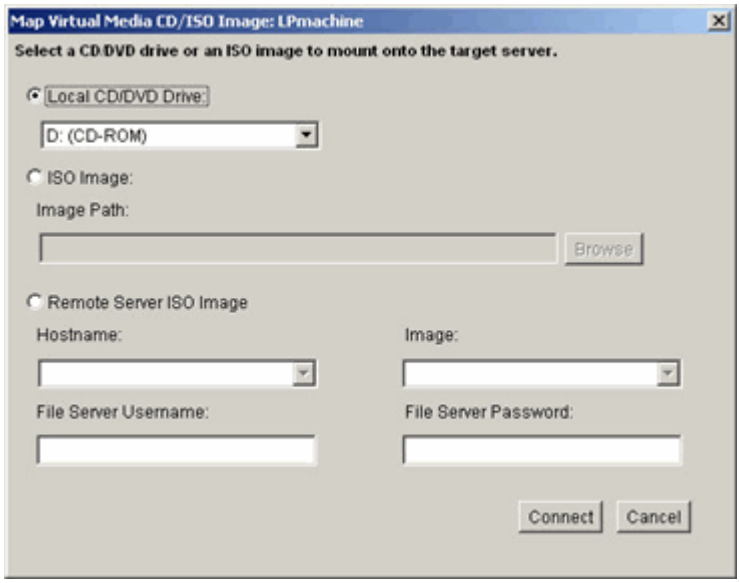
CD-ROM/DVD-ROM/ISO イメージ

このオプションを使用して、CD-ROM、DVD-ROM、ISO イメージをマウントします。

注: Raritan は ISO9660 形式を標準でサポートしています。ただし、それ以外の CD-ROM 拡張も動作する場合があります。

➢ *CD-ROM、DVD-ROM、ISO イメージにアクセスするには、以下の手順に従います。*

1. Virtual KVM Client で、[Virtual Media] (仮想メディア) の [Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続) を選択します。[Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスが表示されます。



2. 内部および外部の CD-ROM ドライブまたは DVD-ROM ドライブの場合
   a. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) を選択します。
   b. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) ドロップダウン リストから、ドライブを選択します。使用可能なすべての内部/外部の CD ドライブおよび DVD ドライブの名前が、ドロップダウン リストに表示されます。
   c. [Connect] (接続) をクリックします。
3. ISO イメージの場合
   a. [ISO Image] (ISO イメージ) オプションを選択します。CD、DVD、またはハード ディスクのディスク イメージにアクセスする場合に、このオプションを使用します。サポートされる形式は ISO 形式のみです。

b. [Browse] (参照) ボタンをクリックします。

c. 使用するディスク イメージが含まれるパスを指定して、[Open] (開く) をクリックします。 パスが [Image Path] (イメージのパス) フィールドに入力されます。

d. [Connect] (接続) をクリックします。

4. ファイル サーバ上のリモート ISO イメージの場合

a. [Remote Server ISO Image] (リモート サーバの ISO イメージ) オプションを選択します。

b. ドロップダウン リストから、ホスト名とイメージを選択します。 ファイル サーバとイメージ パスは、[File Server Setup] (ファイル サーバのセットアップ) ページを使用して設定できます。 [KX II-101 ファイル サーバ セットアップ] (KX II-101 ファイル サーバのセットアップ] ページで設定した項目がドロップダウン リストに表示されます。

c. [File Server Username] (ファイル サーバ ユーザ名)。 ファイル サーバへのアクセスに必要なユーザ名です。

d. [File Server Password] (ファイル サーバ パスワード)。 ファイル サーバへのアクセスに必要なパスワードです (入力時、フィールドはマスクされます)。

e. [Connect] (接続) をクリックします。

メディアがターゲット サーバに仮想的にマウントされます。 このメディアには、他のドライブとまったく同じようにアクセスすることができます。

仮想メディアの切断

➢ *仮想メディア ドライブを切断するには、以下の手順に従います。*

- ローカル ドライブの場合は、[Virtual Media] (仮想メディア) の [Disconnect Drive] (ドライブの切断) を選択します。
- CD-ROM、DVD-ROM、ISO イメージの場合は、[Virtual Media] (仮想メディア) の [Disconnect CD-ROM/ISO Image] (CD-ROM/ISO イメージの切断) を選択します。

注: 切断オプションを使用する方法だけでなく、KVM 接続を閉じても仮想メディアが切断されます。

ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)

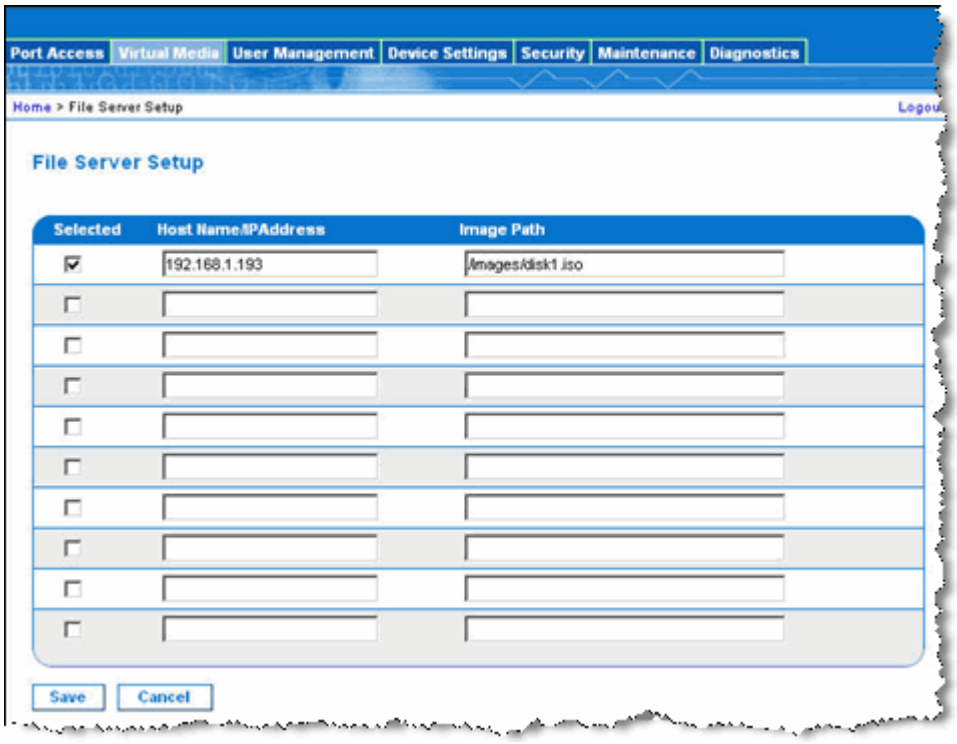
注: この機能は、仮想メディアを使用してファイル サーバ ISO イメージにアクセスする場合にのみ必要です。

注: Raritan は ISO9660 形式を標準でサポートしています。 ただし、その他の CD-ROM 拡張も動作します。

[KX II-101 File Server Setup] (KX II-101 ファイル サーバ セットアップ) ページで、KX II-101 仮想メディアを使用してアクセスするファイル サーバとイメージのパスを指定します。 ここで指定されたファイル サーバ ISO イメージは、[Remote Server ISO Image Hostname] (リモート サーバの ISO イメージ) で [Hostname] (ホスト名) および [Image] (イメージ) ドロップダウン リスト (***[Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックス***『p. 109の"CD-ROM/DVD-ROM/ISO イメージ"参照先 』) の選択肢として表示されます。

➢ *仮想メディアとしてアクセスするファイル サーバ ISO イメージを指定するには、以下の手順に従います。*

1. KX II-101 リモート コンソールから仮想メディアを選択します。 [File Server Setup] (ファイル サーバのセットアップ) ページが開きます。



2. アクセスするファイル サーバ ISO イメージに関する情報を入力します。

- [Host Name/IP Address] (ホスト名/IP アドレス)。 ファイル サーバのホスト名または IP アドレスです。
- [Image Path] (イメージのパス)。 ISO イメージの場所を表す完全パス名です。

3. 仮想メディアとしてアクセスするすべてのメディアについて、[Selected] (選択) チェックボックスをオンにします。
4. [Save] (保存) をクリックします。 これで、指定したすべてのメディアが [Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスで選択できるようになります。

8 デバイス管理

この章の内容

[Device Settings] (デバイス設定) メニュー

[Device Settings] (デバイス設定) メニューは次のように構成されています。[Network] (ネットワーク)、[Device Settings] (デバイス設定)、[Keyboard/Mouse] (キーボード/マウス)、[Serial Port] (シリアル ポート)、[Date/Time] (日付/時刻)、[Event Management - Settings] (イベント管理 - 設定)、[Event Management - Destinations] (イベント管理 - 送信先)、[Port Configuration] (ポート設定)。

メニュー	操作
[Network] (ネットワーク)	KX II-101 のネットワーク設定をカスタマイズします。
[Device Services] (デバイス サービス)	KX II-101 ネットワーク ポートを設定し、TELNET および SSH アクセスを有効にします。
[Keyboard/Mouse] (キーボード/マウス)	KX II-101 で送信されるキーボードおよびマウス信号をターゲット サーバが認識する方法を設定します。
[Serial Port] (シリアル ポート)	KX II-101 のシリアル ポートの機能を選択および設定します。
[Date/Time] (日付/時刻)	日付、時刻、タイム ゾーン、ネットワーク タイム プロトコル (NTP) を設定します。
[Event Management - Settings] (イベント管理 - 設定)	SNMP および Syslog を設定します。
[Event Management - Destinations] (イベント管理 - 送信先)	追跡するシステム イベントと、その情報の送信先を選択します。

メニュー	操作
[Port Configuration] (ポート設定)	KVM ポート、コンセントを設定します。

[Network Settings] (ネットワーク設定)

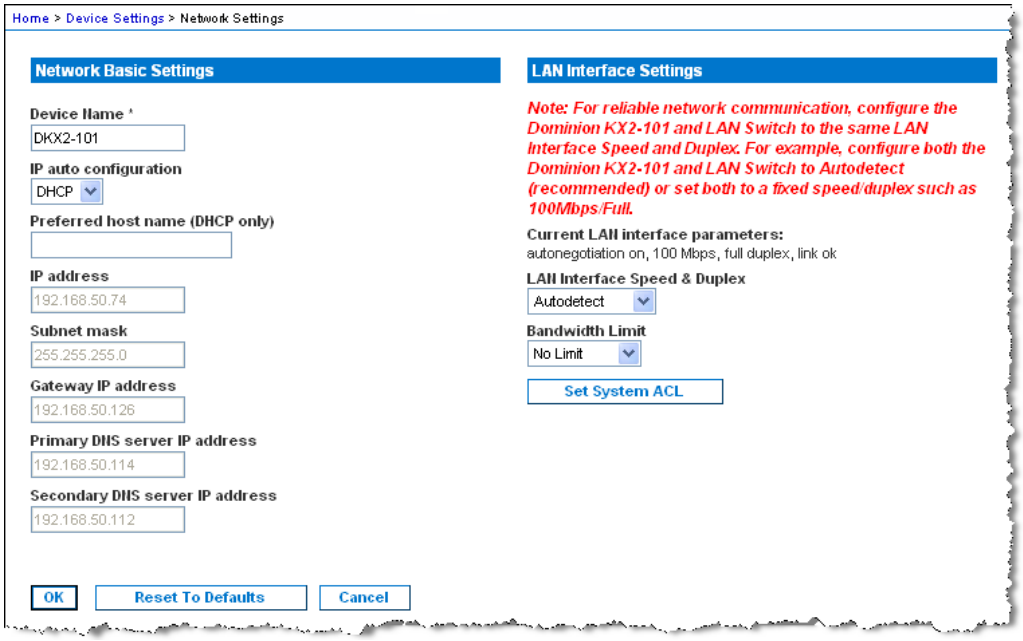
[Network Settings] (ネットワーク設定) ページを使用して、KX II-101 ユニットのネットワーク設定 (たとえば、IP アドレス、検出ポート、LAN インタフェース パラメータなど) をカスタマイズします。

基本的に、IP 設定を行うには 2 種類の方法があります。

- [None] (設定しない)。 (デフォルト) 推奨されるオプションです (静的 IP)。KX II-101 はネットワーク インフラストラクチャの一部であるため、IP アドレスを頻繁に変更されると手間がかかります。 このオプションにより、ネットワーク パラメータを固定できます。
- [DHCP]。 DHCP サーバによって IP アドレスが自動的に割り当てられます。

➢ *ネットワーク設定を変更するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。 [ネットワーク設定] (Network Settings) ページが開きます。



2. ネットワーク基本設定を更新します。 各フィールドの詳細については、「ネットワーク基本設定」を参照してください。
3. LAN インタフェースの設定を更新します。 各フィールドの詳細については、「LAN インタフェース設定」を参照してください。

4. [OK] (OK) をクリックして、これらの設定を保存します。 変更を適用するために再起動が必要な場合は、再起動メッセージが表示されます。

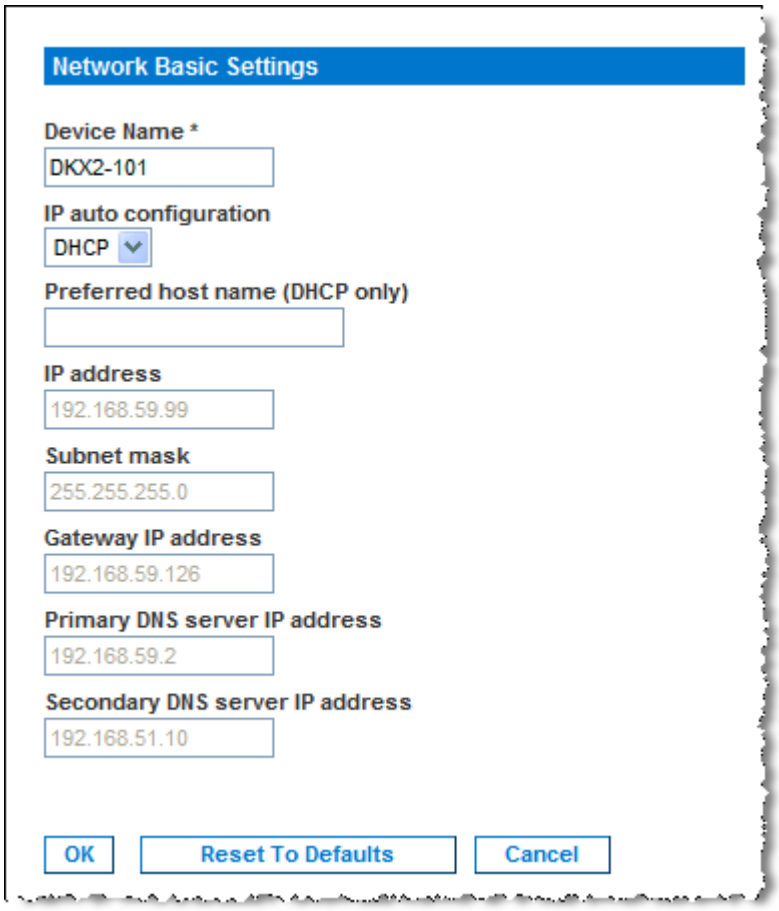
➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) 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。*

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

ネットワーク基本設定



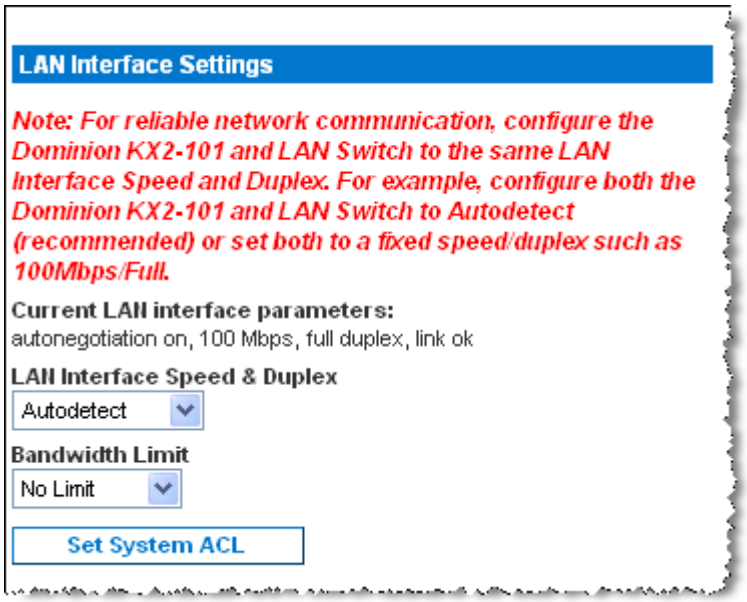
- [Device Name] (デバイス名)。 デバイスの一意の名前を入力します (最大で 16 文字です。スペースは使用できません)。 デバイスには、簡単に識別できる名前を付けてください。 KX II-101 ユニットのデフォルトの名前は「DKX2-101」です。 リモート ユーザにもこの名前が表示されます。 ただし、MPC ユーザがこのデバイスの [Connection Profile] (接続プロファイル) を作成した場合、そのユーザにはそのプロファイルの [Description] (説明) フィールドが代わりに表示されます。
- [IP auto configuration] (IP 自動設定)。 ドロップダウン リストの使用可能なオプションから選択します。
  - [None] (設定しない)。 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します (静的 IP)。 推奨されるデフォルトのオプションです。

    [IP auto configuration] (IP 自動設定) でこのオプションを選択すると、次の [Network Basic Settings] (ネットワーク基本設定) フィールドが有効になり、IP アドレスを手動で設定できるようになります。

    - [IP Address] (IP アドレス)。 デフォルトの IP アドレスは「192.168.0.192」です。
    - [Subnet Mask] (サブネット マスク)。 デフォルトのサブネット マスクは「255.255.255.0」です。
    - [Gateway IP Address] (ゲートウェイ IP アドレス)。 ゲートウェイの IP アドレスです (使用している場合)。
    - [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)。 名前を IP アドレスに変換するために使用されるプライマリ ドメイン ネーム サーバです。
    - [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)。 名前を IP アドレスに変換するために使用されるセカンダリ ドメイン ネーム サーバです (使用している場合)。
  - [DHCP]。 DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。 最大 63 文字まで使用できます。

LAN インタフェース設定



- 現在のパラメータ設定は、[Current LAN interface parameters] (現在の LAN インタフェース パラメータ) フィールドで確認します。
- [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化)。設定可能な速度と二重化の組み合わせを選択します。

自動検出	デフォルト オプション	
10 Mbps/半二重		両方の LED が点滅
10 Mbps/全二重		両方の LED が点滅
100 Mbps/半二重		黄色の LED が点滅
100 Mbps/全二重		黄色の LED が点滅
1000 Mbps/全二重	ギガビット	緑色の LED 点滅

[Half-duplex] (半二重) の場合、双方向の通信は可能ですが、一度に通信できるのは一方向だけです (同時に通信できません)。

[Full-duplex] (全二重) の場合、同時に双方向の通信が可能です。

注: 半二重または全二重で 10 Mbps で実行しているときに、問題が発生する場合があります。 問題が発生した場合は、別の速度と二重化を選択してください。

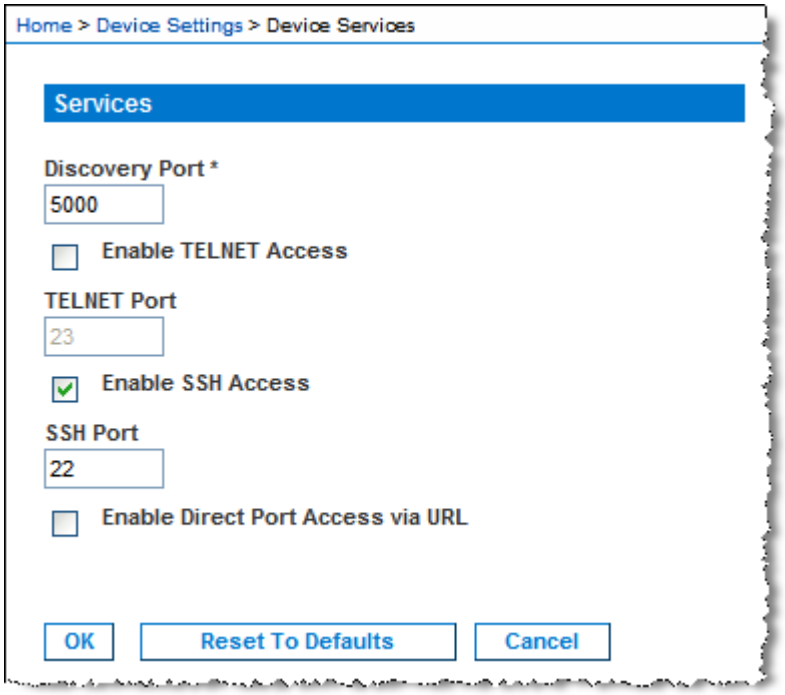
詳細は、「ネットワーク速度の設定」を参照してください。

- [Bandwidth Limit] (帯域幅の制限)。 使用可能な帯域幅の制限から選択します。
  - [128 Kilobit] (128 キロビット)
  - [256 Kilobit] (256 キロビット)
  - [512 Kilobit] (512 キロビット)
  - [2 Megabit] (2 メガビット)
  - [5 Megabit] (5 メガビット)
  - [10 Megabit] (10 メガビット)
  - [100 Megabit] (100 メガビット)
  - [No Limit] (制限なし)
- [Set System ACL] (システム ACL の設定)。 このボタンをクリックして、KX II-101 に対するグローバル レベルのアクセス制御リストの設定を行い、許可されていない IP アドレスから送信されるパケットにデバイスが応答することがないようにします。 ***[IP Access Control] (IP アクセス制御)*** 『p. 153』ページが開きます。

注: これらの ACL 値はグローバルで、KX II-101 ユニット全体に影響します。 グループレベルの ACL も作成できます。 たとえば、所定の範囲の IP アドレスからのみ KX II-101 にアクセスできる「Outsourced Vendors」というユーザ グループを作成できます (グループに固有のアクセス制御リストを作成する方法については、「グループ ベースの IP ACL (アクセス制御リスト)」を参照してください)。

[Device Services] (デバイス サービス)

[Device Services] (デバイス サービス) ページを使用して、KX II-101 の接続オプションを指定します。



➢ *検出ポートを設定するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services] (デバイス サービス) ページが開きます。
2. KX II-101 でクライアント PC との通信に使用するネットワーク ポートを入力します。
3. [Save] (保存) をクリックしてこの設定を保存します。

➢ *TELNET アクセスを有効するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services] (デバイス サービス) ページが開きます。
2. [Enable TELNET Access] (TELNET アクセスを有効する) を選択します。
3. KX II-101 への TELNET アクセスに使用するネットワーク ポートを入力します。
4. [Save] (保存) をクリックしてこの設定を保存します。

➢ *SSH アクセスを有効するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services] (デバイス サービス) ページが開きます。
2. [Enable SSH Access] (SSH アクセスを有効する) を選択します。
3. KX II-101 への SSH アクセスに使用するネットワーク ポートを入力します。
4. [Save] (保存) をクリックしてこの設定を保存します。

ダイレクト ポート アクセスの有効化

ダイレクト ポート アクセスを使用すると、通常のログイン ページに進まないで KX II-101 リモート クライアントにアクセスできます。 ダイレクト ポート アクセスを有効にすると、[Port Access] (ポート アクセス) ページに直接移動する URL を定義できます。

➢ *ダイレクト ポート アクセスを有効するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services] (デバイス サービス) ページが開きます。
2. [Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) チェックボックスをオンにします。
3. [Save] (保存) をクリックしてこの設定を保存します。

➢ *ダイレクト ポート アクセス URL を設定するには、以下の手順に従います。*

- IP アドレス、ユーザ名, パスワード、必要に応じて KX II-101 のポート番号を使用して URL を定義します。 KVM ポートが 1 つのみある場合、ポート番号は不要です。

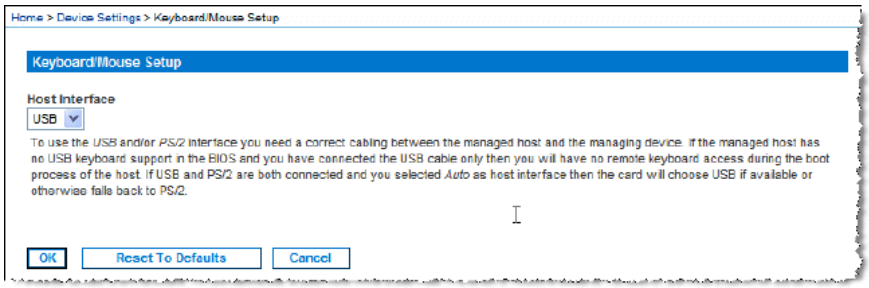
  ダイレクト ポート アクセス URL の形式は、次のとおりです。

  https://[**IP アドレス**]/dpa.asp?username=[**ユーザ名**]&password=[**パスワード**]&port=[**ポート番号**]

ヒント: ダイレクト ポート アクセス URL を定義し、Web ブラウザにブックマークとして保存すると、再使用が容易になります。

キーボード/マウスの設定

[Keyboard/Mouse Setup] (キーボード/マウス設定) ページを使用して、KX II-101 とホスト デバイス間のキーボードおよびマウス インタフェースを設定します。



- [Host Interface] (ホスト インタフェース)。 KX II-101 がキーボードおよびマウス データを PS/2 接続を介して送信するか、USB 接続を介して送信するかを選択します。
  - [Auto] (自動)。 この設定では、KX II-101 は 使用可能な場合に USB 接続を使用し、そうでない場合は代わりに PS/2 を使用します。
  - [USB]。 この設定では、KX II-101 は USB 接続を使用して、キーボードおよびマウスデータをホスト デバイスに送信します。
  - [PS/2]。 この設定では、KX II-101 は PS/2 接続を使用して、キーボードおよびマウスデータをホスト デバイスに送信します。

➢ *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。*

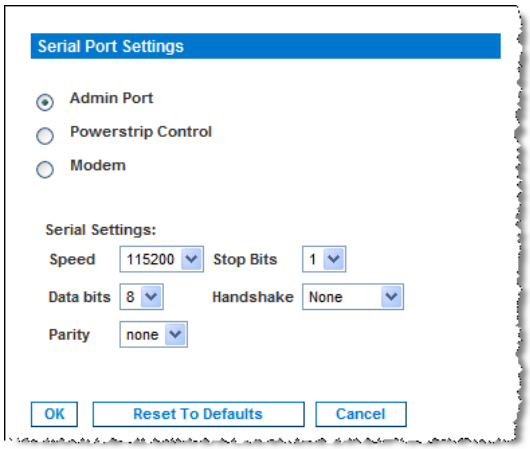
- [Reset to Defaults] (デフォルトに戻す) をクリックします。

[Serial Port Settings] (シリアル ポート設定)

[Serial Port Settings] (シリアル ポート設定) ページを使用して、KX II-101 の内蔵シリアルポートの使用方法を設定します。

➢ *シリアル ポートを設定するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Serial Port] (シリアル ポート) を選択します。 [Serial Port Settings] (シリアル ポート設定) ページが開きます。



2. シリアル ポートで利用する機能を選択するには、以下の手順に従います。
   - [Admin Port] (管理ポート)。 クライアント PC から KX II-101 に直接接続して詳細な設定にアクセスするには、このオプションを選択します。
   - [PowerStrip Control] (パワー ストリップ制御)。 シリアル インターフェースで制御されるパワー ストリップに KX II-101 を接続する場合は、このオプションを選択します。
   - [Modem] (モデム)。 ダイヤルイン アクセスを提供するために外部モデムを KX II-101 に接続する場合は、このオプションを選択します。
3. For the [Modem] (モデム) オプションでは、モデムの使用設定を次のように入力して設定します。
   a. KX II-101 とモデム間のデータ速度を [Serial line speed] (シリアル ライン速度) ドロップダウン リストから選択します。
   b. モデム init 文字列を入力します。
   c. モデム サーバ IP アドレスを入力します。 これは、ユーザがモデムを介して接続した後、KX II-101 Web インタフェースにアクセスするために入力するアドレスです。
   d. モデム クライアント IP アドレスを入力します。 これは、ユーザがモデムを介して接続した後、ユーザに割り当てられるアドレスです。

4. [OK] をクリックします。

[Date/Time Settings] (日付/時刻の設定)

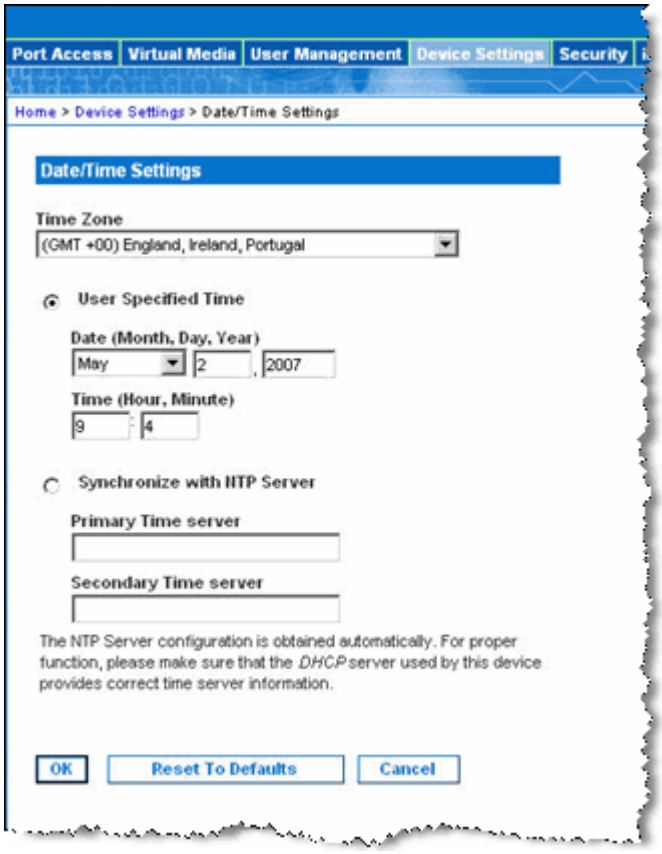
[Date/Time Settings] (日付/時刻の設定) ページを使用して、KX II-101 の日付と時刻を指定します。 これには 2 とおりの方法があります。

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

注: KX II-101 は夏時間をサポートしません。

➢ *日付と時刻を設定するには、以下の手順に従います。*

1. [Device Settings] (デバイス設定) の [Date/Time] (日付/時刻) を選択します。 [Date/Time Settings] (日付/時刻の設定) ページが開きます。



2. [Time Zone] (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. 日付と時刻の設定で用いる方法を選択します。

- [User Specified Time] (ユーザによる時刻定義)。 日付と時刻を手動で入力するには、このオプションを選択します。
- [Synchronize with NTP Server] (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。

4. [User Specified Time] (ユーザによる時刻定義) オプションを選択した場合は、以下の手順に従って日付と時刻を入力します。
   a. ドロップダウン リストから [Month] (月) を選択します。
   b. その月の [Day] (日)を入力します。
   c. yyyy の形式で [Year] (年) を入力します。
   d. hh:mm の形式で [Time] (時刻) を入力します (24 時間制で入力します)。
5. [Synchronize with NTP Server] (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. [Primary Time server] (プライマリ タイム サーバ) の IP アドレスを入力します。
   b. [Secondary Time server] (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)。
6. [OK] をクリックします。

イベント管理

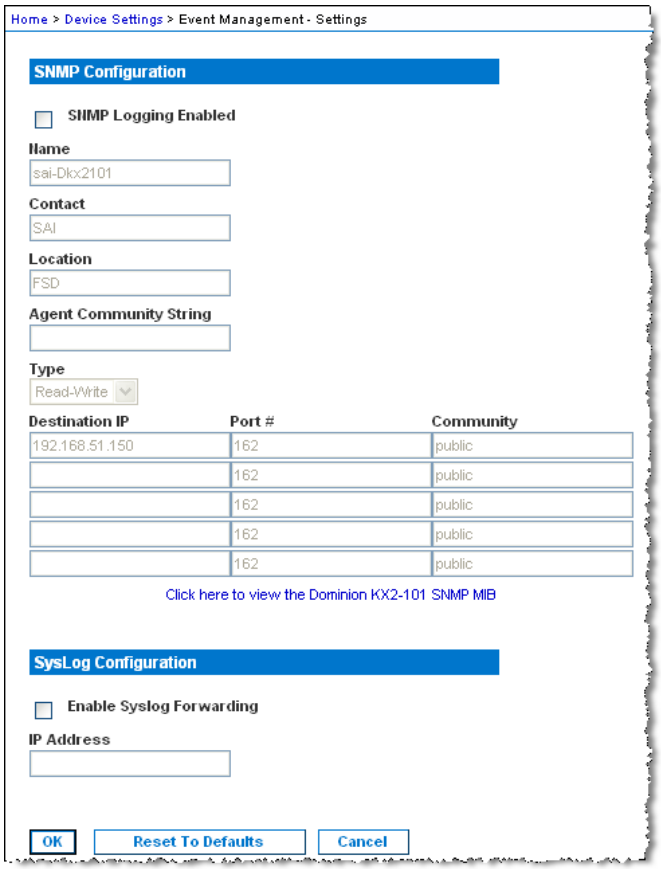
KX II-101 イベント管理機能によって、一連の画面から、SNMP マネージャ、Syslog、監査ログへのシステム イベントの送信を有効または無効にできます。 これらのイベントはカテゴリ分けされるため、イベントごとに 1 つまたは複数の宛先に送信するかどうかを指定できます。

SNMP の設定

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。 KX II-101 では、イベント管理を通じて SNMP エージェントがサポートされます。 SNMP エージェントとトラップの詳細については、「***SNMP エージェント設定*** 『p. 130』」および「***SNMP トラップ設定*** 『p. 130』」を参照してください。

➢ *SNMP を設定する（SNMP のログ作成を有効にする）には、以下の手順に従います。*

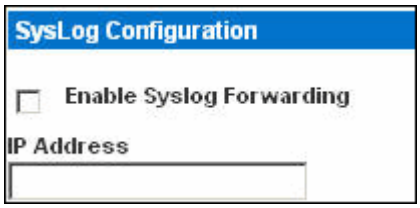
1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。 [Event Management - Settings] (イベント管理 - 設定) ページが開きます。



2. [Enable SNMP Logging] (SNMP ログを有効にする) オプションを選択します。これによって残りの SNMP フィールドが有効になります。

3. [Name] (名前) フィールドには、KX II-101 コンソール インタフェースに表示されているとおりに、SNMP エージェント (使用している Dominion ユニット) の名前を、[Contact] (連絡先) フィールドには、そのユニットに関連する連絡先を、[Location] (所在地) フィールドには、Dominion ユニットが物理的に設置されている場所を入力します。
4. [Agent Community String] (エージェント コミュニティの文字列) (Dominion ユニットの文字列) を入力します。 SNMP コミュニティとは、SNMP を実行しているデバイス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。これは、SNMP デバイスまたはエージェントが複数の SNMP コミュニティに所属している場合があるためです。
5. [Type] (タイプ) ドロップダウン リストを使用して、コミュニティに読み取り専用と読み書き可能のいずれかを指定します。
6. [Destination IP] (送信先 IP)、[Port #] (ポート番号)、[Community] (コミュニティ) を指定して、最大で 5 つの SNMP マネージャを設定します。
7. [Click here to view the KX II-101 SNMP MIB] (KX II-101 SNMP MIB を表示するにはここをクリックします) というリンクをクリックして、SNMP Management Information Base にアクセスします。
8. [OK] をクリックします。

Syslog の設定



➢ *Syslog を設定する (Syslog の送信を有効にする) には、以下の手順に従います。*

1. [Enable Syslog Forwarding] (Syslog 送信有効) オプションを選択して、リモート Syslog サーバにデバイス メッセージのログを送信します。
2. [IP Address] (IP アドレス) フィールドに Syslog サーバの IP アドレスを入力します。
3. [OK] をクリックします。

➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) 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。*

- [Reset To Defaults] (デフォルトに戻す) ボタンをクリックします。

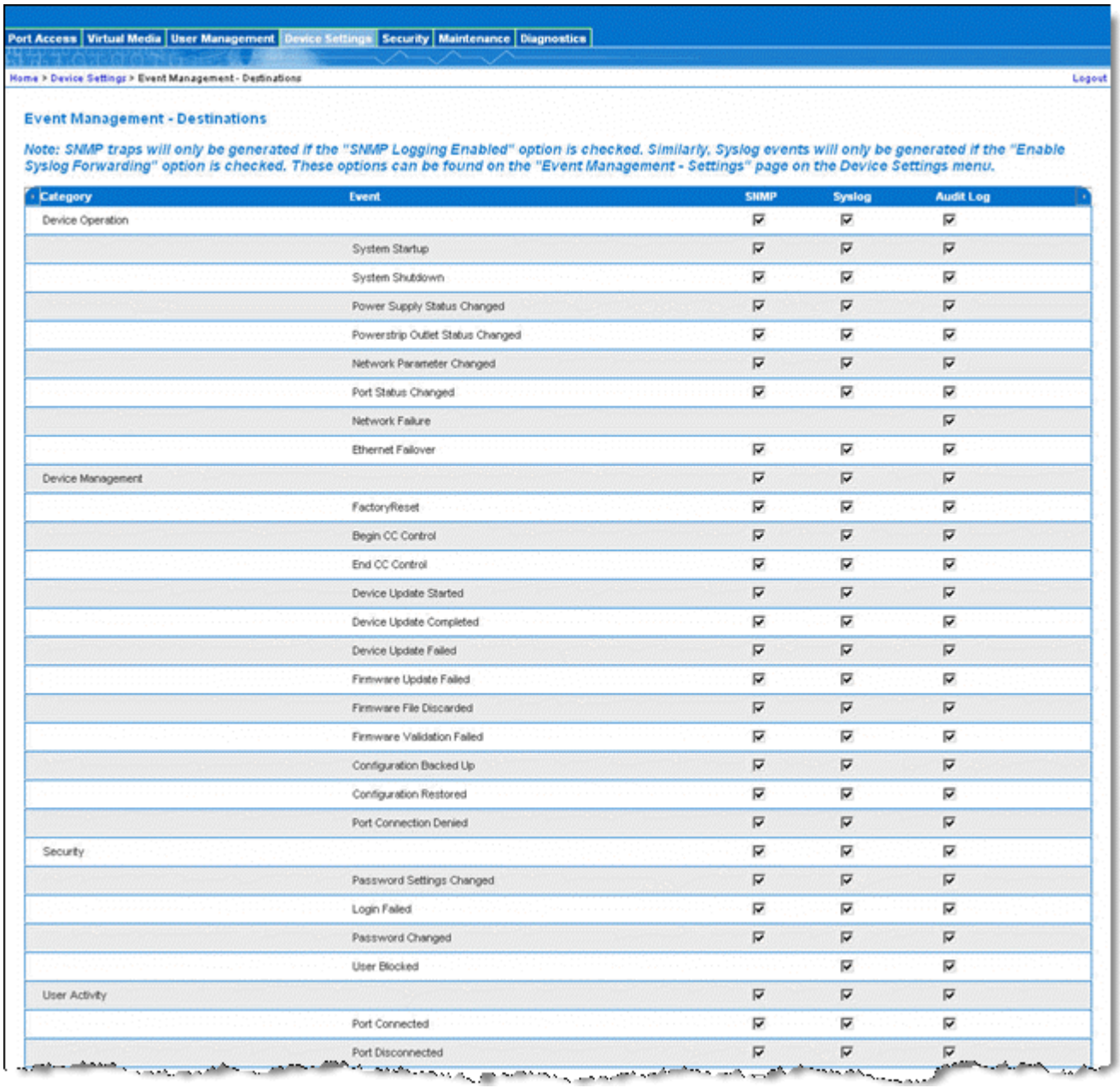
[Event Management - Destinations] (イベント管理 - 送信先)

システム イベントを有効にすると、SNMP 通知イベント (トラップ) を生成できます。また、システム イベントを Syslog または監査ログにログ記録できます。 [Event Management - Destinations] (イベント管理 - 送信先) ページを使用して、追跡するイベントと、その情報の送信先を選択します。

注: SNMP トラップは、[SNMP Logging Enabled] (SNMP ログを有効にする) オプションが選択されている場合にのみ生成されます。一方、Syslog イベントは、[Enable Syslog Forwarding] (Syslog 送信有効) オプションが選択されている場合にのみ生成されます。これらのオプションは、いずれも [Event Management - Settings] (イベント管理 - 設定) ページで設定します。「[Event Management - Settings] (イベント管理 - 設定)」を参照してください。

➢ *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. [Device Settings] (デバイス設定) の [Event Management - Destinations] (イベント管理 - 送信先) を選択します。 [Event Management - Destinations] (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 [Event] (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: [Category] (カテゴリ) ライン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。

➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) 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。*

- [Reset To Defaults] (デフォルトに戻す) ボタンをクリックします。

警告: UDP 経由の SNMP トラップを使用している場合、KX II-101 を再起動したときに、KX II-101 と接続先のルータが同調できなくなり、SNMP トラップ「reboot completed (再起動の完了)」がログ記録されない可能性があります。

SNMP エージェント設定

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。 KX II-101 (SNMP エージェント) と SNMP マネージャとの間の SNMP 接続を設定するには、イベント ログ ページを使用します。

SNMP トラップ設定

SNMP によって、トラップまたは通知を送信する機能と、1 つ以上の条件が満たされた場合に管理者に忠告する機能が提供されます。 KX II-101 のトラップを次の表に示します。

トラップ名	説明
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 KX II-101 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 KX II-101 のアップデートが開始されました。
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 KX II-101 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。

トラップ名	説明
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。
passwordSettingsChanged	強力なパスワードの設定が変更されました。
portConnect	以前認証されたユーザが KVM 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	KVM 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	電源コンセントの状態の通知です。 1: アクティブ、0: 非アクティブ
powerOutletNotification	パワー ストリップ デバイスのコンセントの状態の通知です。
rebootCompleted	KX II-101 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、KX II-101 は再起動を開始しました。
securityViolation	セキュリティ違反です。
startCCManagement	デバイスが CommandCenter の管理下におかれました。
stopCCManagement	デバイスが CommandCenter の管理下から除外されました。
userAdded	ユーザ アカウント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。
userConnectionLost	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。
userLogin	ユーザが KX II-101 へ正常にログインし、認証されました。
userLogout	ユーザが KX II-101 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。

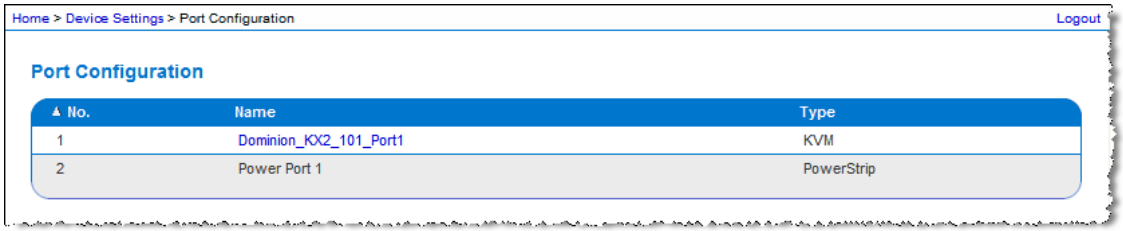
トラップ名	説明
userPasswordChanged	デバイスのいずれかのユーザのパスワードが変更されると、このイベントが発生します。
userSessionTimeout	あるユーザのアクティブ セッションが、タイムアウトにより終了しました。
vmImageConnected	ユーザが仮想メディアを使用してターゲットにデバイスまたはイメージのマウントを試みました。 デバイスまたはイメージのマッピング (マウント) が試行されるたびに、このイベントが生成されます。
vmImageDisconnected	ユーザが仮想メディアを使用してターゲットからデバイスまたはイメージのマウント解除を試みました。

[Port Configuration] (ポート設定)

[Port Configuration] (ポート設定) ページには、KX II-101 のポートの一覧が表示されます。 KVM ターゲット サーバまたはパワー ストリップに接続されているポートは青色で表示され、編集できます。

➢ *ポート設定を変更するには、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) を選択します。 [Port Configuration] (ポート設定) ページが開きます。



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フィールドごとに並べ替えられます。

- [Port Number] (ポート番号)。 1 から KX II-101 ユニットで使用できるポートの合計数までの番号が振られています。
- [Port Name] (ポート名)。 ポートに割り当てられている名前です。 ポート名が黒色で表示されている場合は、名前の変更およびポートの編集はできません。ポートが青色で表示されている場合は、編集できます。

注: ポート名にアポストロフィ (" ' ") を使用することはできません。

- [Port Type] (ポート タイプ)。 ポートに接続されているターゲットのタイプです。

ポート タイプ	説明
PowerStrip	パワー ストリップ
KVM	KVM ターゲット

2. 編集するポートの [Port Name] (ポート名) をクリックします。
   - KVM ポートの場合は、[Port] (ポート) ページが開きます。 このページで、ポートに名前を付け、電源を関連付けて、ターゲット サーバ設定を設定します。
   - パワー ストリップの場合は、パワー ストリップ の [Port] (ポート) ページが開きます。 このページで、パワー ストリップとそのコンセントに名前を付けます。

注: [Power Port 1] (パワー ポート 1) リンクは、Raritan 電源タップを KX II-101 に接続し、設定している場合にのみ有効です。 そうでない場合、このリンクは無効です。

9 電源制御

この章の内容

概要

KX II-101 では、ターゲット サーバの電源をリモートで制御できます。 この機能を使用するには、Raritan リモート パワー ストリップが必要です。

➢ *KX II-101 の電源制御機能を使用するには、以下の手順に従います。*

1. ターゲット サーバにパワー ストリップを接続します。
2. パワー ストリップに名前を付けます。
3. パワー ストリップのコンセントをターゲット サーバに関連付けます。
4. ***[Powerstrip Device] (パワーストリップ デバイス)***『p. 142の"電源タップ デバイスの制御"参照先 』ページで、パワー ストリップのコンセントをオン、オフします。

パワー ストリップの接続

1 KX II-101 から Raritan パワー ストリップまでの DKX2-101-SPDUC コネクタ (別売り)

2 Raritan パワー ストリップ。

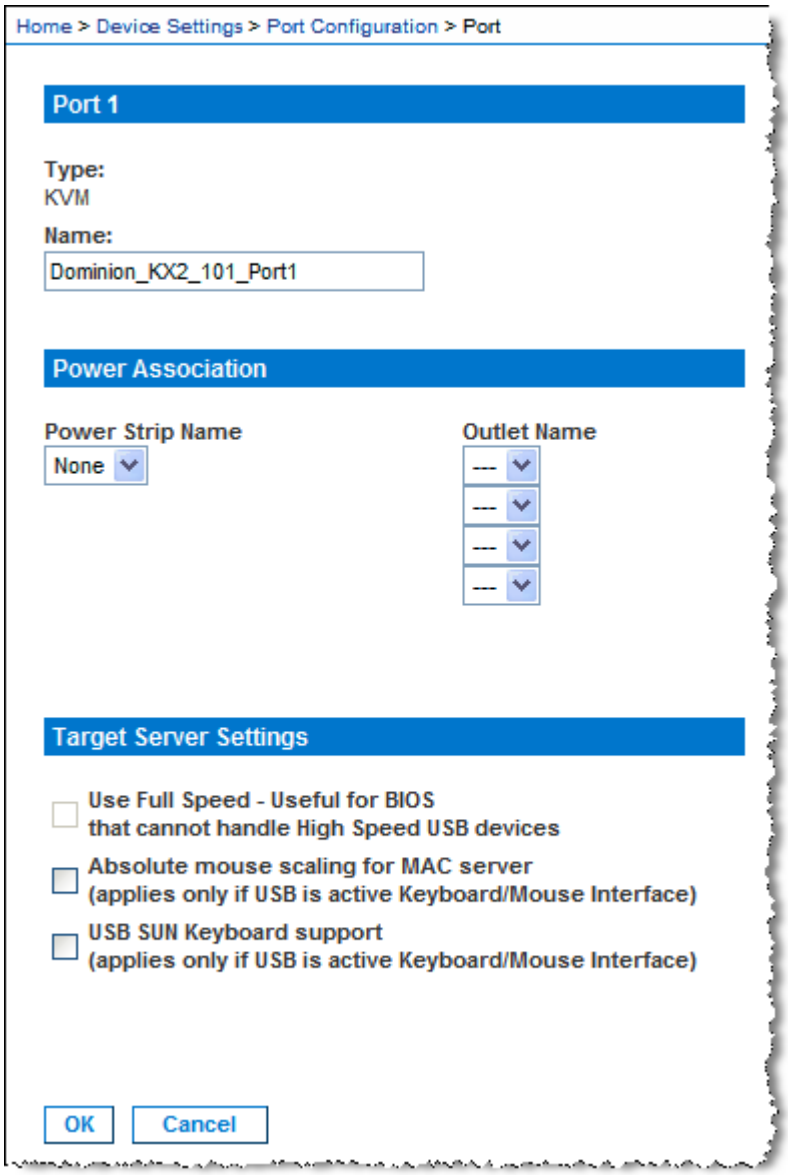
➢ *KX II-101 を Raritan パワー ストリップを接続するには、以下の手順に従います。*

1. DKX2-101-SPDUC ケーブルのミニ DIN9M コネクタを KX II-101 の Admin ポートに接続します。
2. DKX2-101-SPDUC ケーブルの RJ45M コネクタを Raritan パワー ストリップのシリアル ポート コネクタに接続します。
3. AC 電源コードをターゲット サーバと、パワー ストリップの空いているパワー ストリップ コンセントに接続します。
4. パワー ストリップを AC 電源に接続します。
5. Raritan パワー ストリップの電源をオンにします。

パワー ストリップの名前の指定 (パワー ストリップの [Port] (ポート) ページ)

[Port Configuration] (ポート設定) ページで、Raritan リモート パワー ストリップに接続しているポートを選択すると、この [Port] (ポート) ページが開きます。[Type] (タイプ) フィールドと [Name] (名前) フィールドには、あらかじめ入力されています。 パワー ストリップの各コンセントに関する次の情報が表示されます。 コンセントの [Number] (番号)、[Name] (名前)、[Port Association] (ポートの関連付け)。

このページを使用してパワー ストリップとそのコンセントに名前を付けます。いずれの名前にも最大 32 文字の英数字を使用でき、特殊文字を含めることができます。



注: パワー ストリップがターゲット サーバ (ポート) に関連付けられると、コンセント名はターゲット サーバ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る場合も同様です)。

➢ *パワー ストリップ (およびコンセント) に名前を付けるには、以下の手順に従います。*

注: CommandCenter Service Gateway では、スペースを含むパワー ストリップ名を認識できません。

1. パワー ストリップの [Name] (名前) を覚えやすい名前に変更します。
2. 必要に応じて、([Outlet] (コンセント)) [Name] (名前) を変更します (デフォルトのコンセント名は、「Outlet #」です)。
3. [OK] をクリックします。

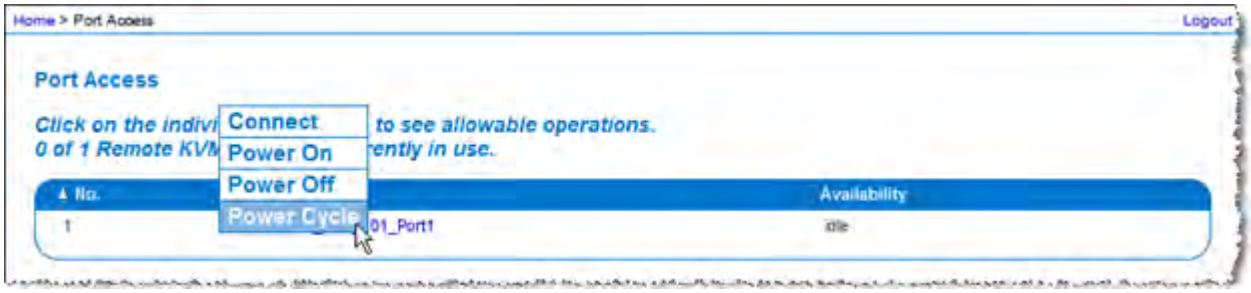
➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) をクリックします。

コンセントへの KVM ターゲット サーバの関連付け ([Port] (ポート) ページ)

[Port Configuration] (ポート設定) ページで、ターゲット サーバに接続しているポートを選択すると、この [Port] (ポート) ページが開きます。 このページで、電源の関連付けを実行したり、ポートの名前をわかりやすい名前に変更したりすることができます。

サーバには、パワー ストリップと関連付けることができる、最大で 4 つの電源プラグを接続できます。 このページで、これらの関連付けを定義して、以下に示すように [Port Access] (ポート アクセス) ページからサーバの電源の投入、切断、再投入を行えます。



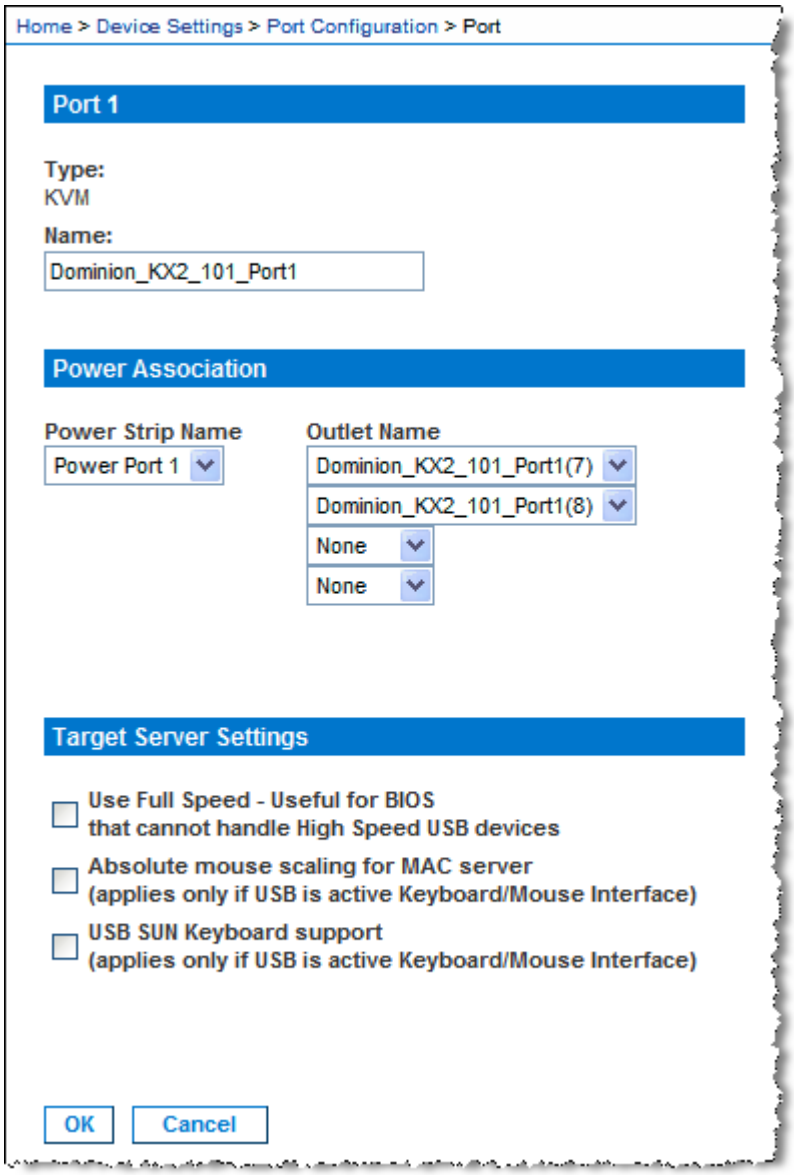
*注: この機能を使用するには、Raritan Dominion PX パワー ストリップをデバイスに接続しておく必要があります。 詳細は、「**パワー ストリップの接続** 『p. 135』」を参照してください。*

➢ *電源の関連付けを行う (パワー ストリップ コンセントを KVM ターゲット サーバに関連付ける) には、以下の手順に従います。*

注: パワー ストリップがターゲット サーバ (ポート) に関連付けられると、コンセント名はポート名に置き換えられます。 この名前は、[Port 2] (ポート 2) ページで変更できます。

1. [Power Strip Name] (パワー ストリップ名) ドロップダウン リストからパワー ストリップを選択します。
2. [Outlet Name] (コンセント名) ドロップダウン リストからコンセントを選択します。
3. 必要な電源の関連付けごとに、手順 1 と 2 を繰り返します。
4. [OK] をクリックします。 確認メッセージが表示されます。

2 つのコンセントが関連付けられたパワー ストリップを以下に示します。



➢ *ポート名を変更するには、以下の手順に従います。*

1. ターゲット サーバの名前など、わかりやすい名前を入力します。 名前には最大 32 文字の英数字が使用でき、 特殊文字を含めることができます。
2. [OK] をクリックします。

➢ *変更を保存せずに終了するには、以下の手順に従います。*

- [Cancel] (キャンセル) をクリックします。

➢ *パワー ストリップの関連付けを削除するには、以下の手順に従います。*

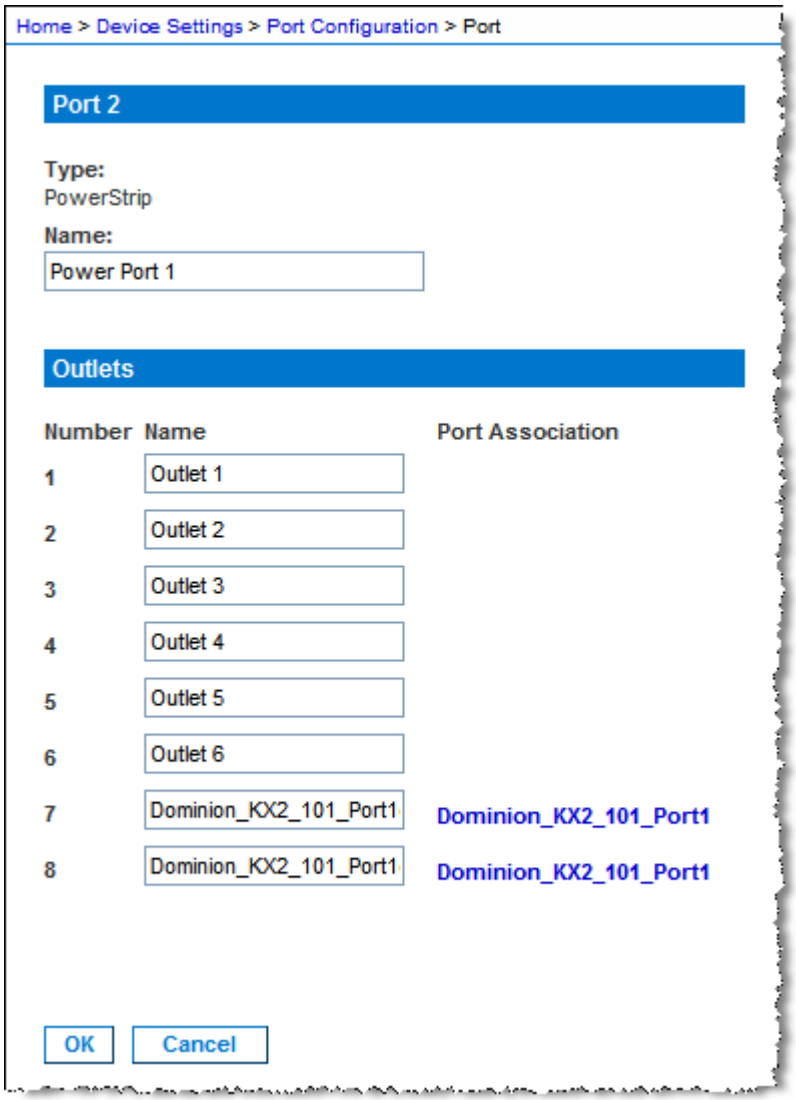
1. [Power Strip Name] (パワー ストリップ名) ドロップダウン リストから該当するパワー ストリップを選択します。
2. そのパワー ストリップに対して、[Outlet Name] (コンセント名) ドロップダウン リストから該当するコンセントを選択します。
3. [Outlet Name] (コンセント名) ドロップダウン リストから、[None] (設定なし) を選択します。
4. [OK] をクリックします。 そのパワー ストリップとコンセントの関連付けが削除されます。 確認メッセージが表示されます。

コンセントの関連付けの表示

➢ *パワー ポートの設定を表示するには、以下の手順に従います。*

- [Home] (ホーム)、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定) [power port name] (パワー ポート名) の順に選択します。

  [Outlets] (コンセント) の下に、パワー ストリップに対するコンセントの関連付けが表示されます。

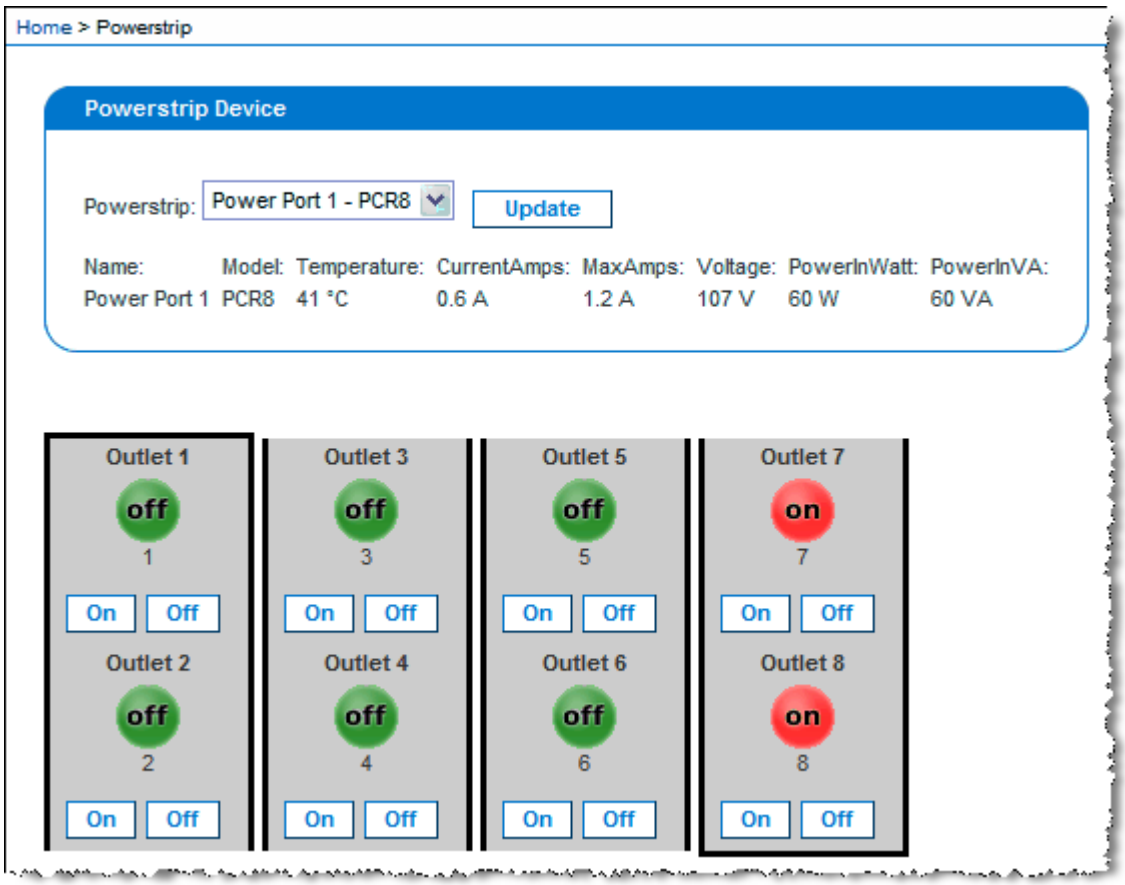


➢ *パワー ポートの設定を編集するには、以下の手順に従います。*

- [Port 2] (ポート 2) の [Name] (名前) フィールドを編集して、パワーポート名を変更します。
- [Outlets] (コンセント) の [Name] (名前) フィールドを編集して、コンセント名を変更します。コンセント名は [Powerstrip Device] (パワーストリップ デバイス) ページに表示されます。詳細は、「***パワーストリップ デバイスの制御***『p. 142の"電源タップ デバイスの制御"参照先 』」を参照してください。
- コンセント名の横にある [Port Association] (ポートの関連付け) リンクをクリックし、[Port 1] (ポート 1) ページで編集して、コンセントの関連付けを変更します。詳細は、***コンセントへの KVM ターゲット サーバの関連付け ([Port] (ポート) ページ)***『p. 137』を参照してください。

電源タップ デバイスの制御

[Powerstrip Device] (パワーストリップ デバイス) ページを使用して電源タップ デバイスを制御できます。このページで、電源タップの各コンセントをオン、オフできます。



➢ *ＫＸ II-101 に接続されている電源タップを制御するには、以下の手順に従います。*

1. [Home] (ホーム) の [Powerstrip] (パワーストリップ) を選択します。

   [Powerstrip Device] (パワーストリップ デバイス) ページが開きます。

2. コンセントごとに [On] (オン) または [Off] (オフ) をクリックして、オンまたはオフにします。

3. 確認のプロンプトが表示されたら、[OK] をクリックします。

   電源コンセントがオンまたはオフに切り替わります。

注: KX II-101 で制御できるのは、1 つの電源タップのみです。[Powerstrip] (パワーストリップ) メニューで別の電源タップを選択することはできません。

---

10 [Security Settings] (セキュリティ設定)

この章の内容

[Security Settings] (セキュリティ設定) メニュー

[Security] (セキュリティ) メニューは次のように構成されています。 [Security Settings] (セキュリティ設定) および [IP Access Control] (IP アクセス制御)。

メニュー	操作
[Security Settings] (セキュリティ設定)	ログイン制限、強力なパスワード、ユーザ ブロック、暗号化および共有に関するセキュリティを設定します。
[IP Access Control] (IP アクセス制御)	KX II-101 ユニットへのアクセスを制御します。 グローバル アクセス制御リストの設定を行い、許可されていない IP アドレスから送信されるパケットにデバイスが応答することのないようにします。

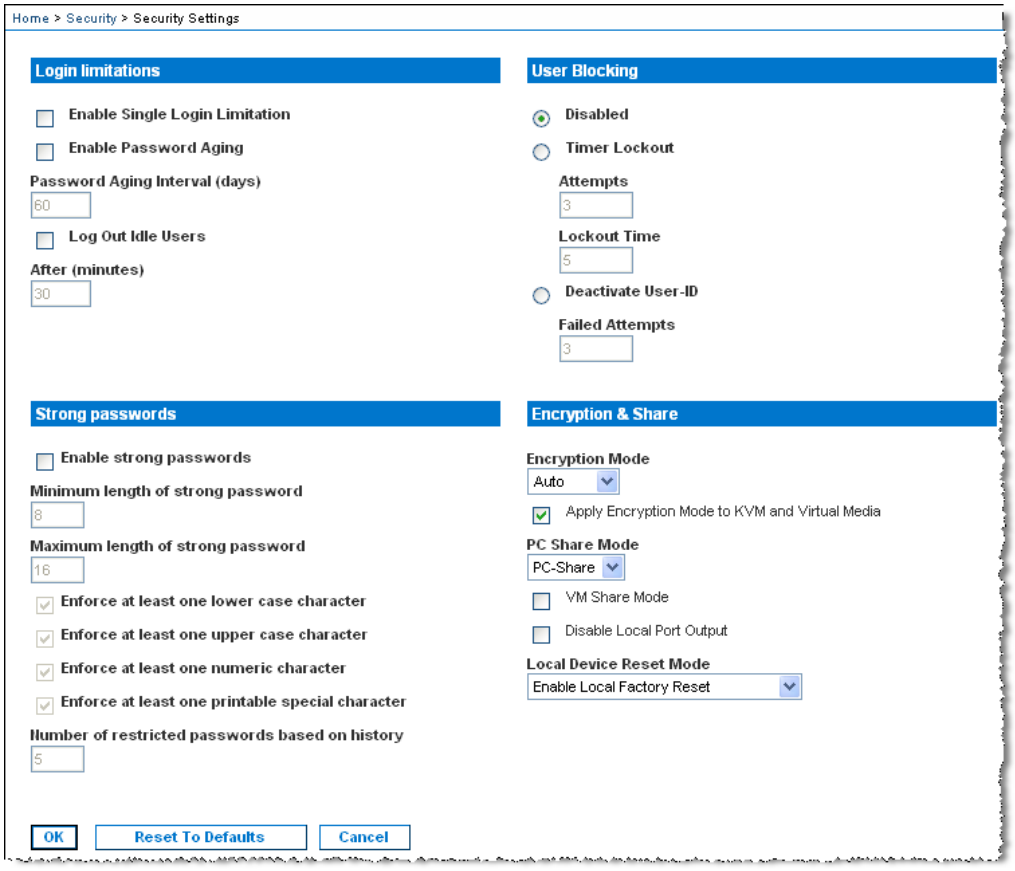
[Security Settings] (セキュリティ設定)

[Security Settings] (セキュリティ設定) ページで、ログイン制限、ユーザ ブロック、パスワード ルール、暗号化および共有に関するセキュリティを指定できます。

パブリック キーとプライベート キーの交換には Raritan SSL 証明書が使用され、セキュリティのレベルを高めます。 Raritan Web サーバ証明書は自己署名され、Java アプレット証明書は VeriSign 証明書によって署名されます。 暗号化を行うと、情報が漏洩しないよう保護されていることを保証できます。またこれらの証明書によって、事業体の身元が Raritan, Inc であることが証明されます。

➢ *セキュリティ設定を行うには、以下の手順に従います。*

1. [Security] (セキュリティ) の [Security Settings] (セキュリティ設定) を選択します。 [Security Settings] (セキュリティ設定) ページが開きます。



フィールドの構成は次のグループに分けられます。 ログイン制限、強力なパスワード、ユーザ ブロック、暗号化および共有。

2. 必要に応じて、 ***[Login Limitations] (ログイン制限)*** 『p. 146の"[Logon Limitations] (ログオン制限)"参照先 』の設定を更新します。

3. 必要に応じて、***[Strong Passwords] (強力なパスワード)*** 『p. 147』の設定を更新します。
4. 必要に応じて、***[User Blocking] (ユーザ ブロック)***『p. 149』の設定を更新します。
5. 必要に応じて、 [Encryption & Share] (暗号化および共有) の設定を更新します。
6. [OK] をクリックします。

➢ *変更を保存せずにページを閉じるには、以下の手順に従います。*

- [Cancel] (キャンセル) をクリックします。

➢ *デフォルトに戻すには、以下の手順に従います。*

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

[Logon Limitations] (ログオン制限)

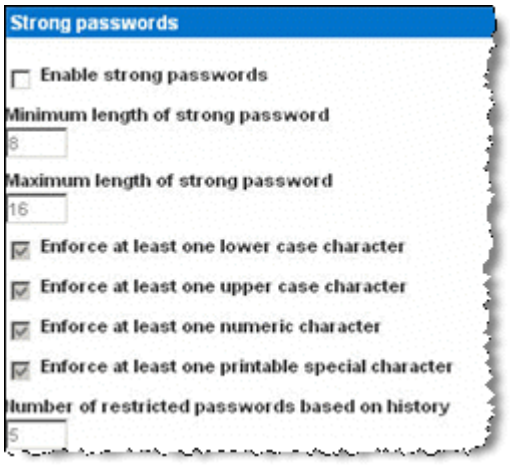
ログオン制限を使用して、シングル ログオン、パスワード エージング、アイドル ユーザのログオフに関する制限を指定できます。

制限	説明
[Enable Single Login Limitation] (シングル ログオン制限を有効にする)	これを選択すると、ユーザ名ごとに同時には 1 人のログインしか許可されません。 この選択を解除すると、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。
[Enable password aging] (パスワード エージングを有効にする)。	これを選択すると、[Password Aging Interval] (パスワード エージング間隔) 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。 [Password Aging Interval (days)] (パスワード エージング間隔 (日))。 [Enable Password Aging] (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。

制限	説明
[Log out idle users] (アイドル ユーザのログアウト)	このチェック ボックスをオンにすると、非アクティブの状態で一定の時間が経過した場合、ユーザ セッションを自動的に切断します。 [After] (経過時間) フィールドに時間を入力します。 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オフされます。 ただし、実行中の仮想メディア セッションはタイムアウトしません。 [After (minutes)] (経過時間 (分))。 アイドル ユーザがログオフされるまでの時間です (分)。 [Log out idle users] (アイドル ユーザのログアウト) オプションをオンにすると、このフィールドが有効になります。

[Strong Passwords] (強力なパスワード)

[Strong Passwords] (強力なパスワード) によってシステムの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 KX II-101 ローカル パスワードの形式を定義する判別の基準を設定できます。



- [Enable strong passwords] (強力なパスワードを有効にする)。 強力なパスワードには、アルファベットとアルファベット以外の文字 (句読点または数字) をそれぞれ 1 文字以上含むパスワードを指定する必要があります。 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。
  これを選択すると、強力なパスワードの規則が適用されます。 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、ユーザは次回ログイ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。 この選択を解除すると、標準の形式での検証だけが適用されます。 これを選択した場合は次のフィールドが有効になるため、設定する必要があります。
  - [Minimum length of strong password] (強力なパスワードの最小長)。 パスワードは 8 文字以上でなければなりません。 デフォルトでは 8 文字ですが、最大 63 文字まで拡張できます。
  - [Maximum length of strong password] (強力なパスワードの最大長)。 デフォルトでは 16 文字ですが、最大 64 文字まで拡張できます。
  - [Enforce at least one lower case character] (1 文字以上の小文字の使用を強制する)。 これを選択すると、パスワードに 1 文字以上の小文字が必要になります。
  - [Enforce at least one upper case character] (1 文字以上の大文字の使用を強制する)。 これを選択すると、パスワードに 1 文字以上の大文字が必要になります。
  - [Enforce at least one numeric character] (1 文字以上の数字の使用を強制する)。 これを選択すると、パスワードに 1 文字以上の数字が必要になります。
  - [Enforce at least one printable special character] (1 文字以上の印刷可能な特殊文字の使用を強制する)。 これを選択すると、パスワードに 1 文字以上の (印刷可能な) 特殊文字が必要になります。
  - [Number of restricted passwords based on history] (履歴を参照する制限パスワードの数)。 このフィールドは、パスワード履歴の幅を表します。つまり、繰り返し使用できない以前のパスワードの数を表します。 範囲は 1 ～ 12 で、デフォルトは 5 です。

[User Blocking] (ユーザ ブロック)

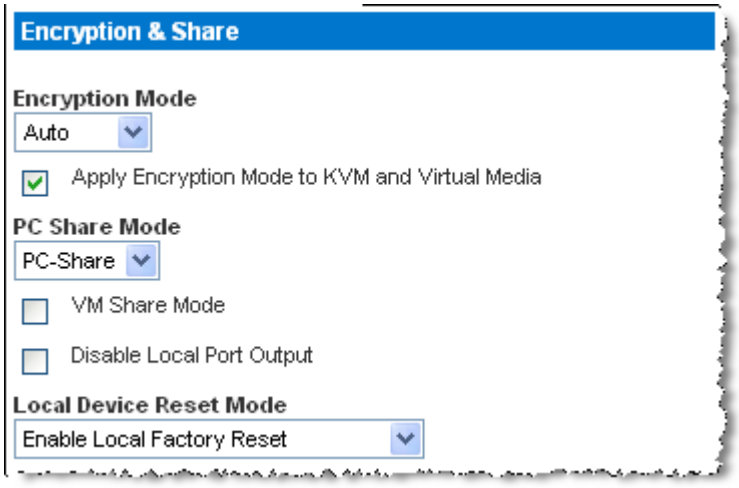
ユーザ ブロック オプションでは基準を指定し、ユーザが指定回数ログインに失敗するとシステムにアクセスできなくなるようにします。 次の 3 つのオプションは、相互に排他的です。

- [Disabled] (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。
- [Timer Lockout] (タイマー ロックアウト)。 ユーザが指定回数より多くログインに失敗すると、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。
  - [Attempts] (試行回数)。 失敗できるログインした回数を示し、この回数より多くログインに失敗すると、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。
  - [Lockout Time] (ロックアウト タイム)。 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。
- [Deactivate User-ID] (ユーザ ID の無効化)。 このオプションを選択した場合は、[Failed Attempts] (失敗した回数) フィールドで指定した回数より多くログインに失敗すると、ユーザはシステムからロックアウトされます。
  - [Failed Attempts] (失敗できる試行回数)。 失敗できるログインの試行回数を示し、この回数より多くログインに失敗すると、そのユーザのユーザ ID が無効になります。 [Deactivate User-ID] (ユーザ ID の無効化) オプションを選択すると、このフィールドが有効になります。 有効な範囲は 1 ～ 10 です。

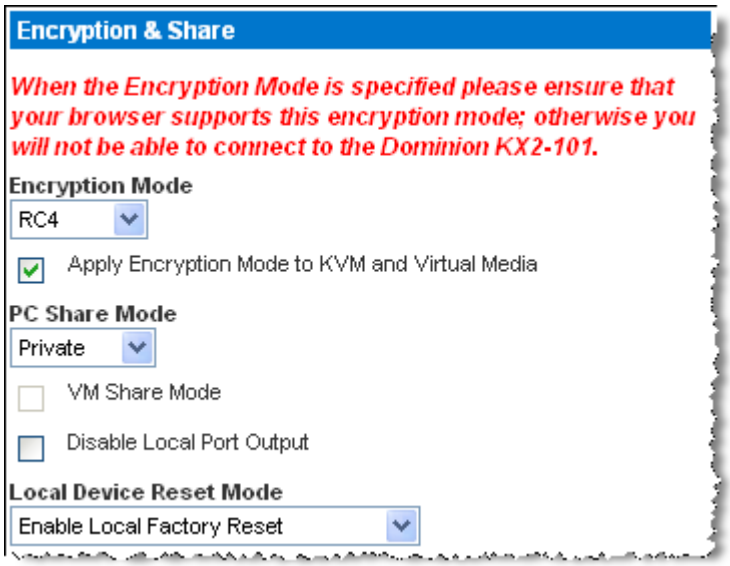
指定回数より多くログインに失敗してユーザ ID が無効になった場合、管理者はユーザ パスワードを変更し、***[User] (ユーザ)***『p. 47の"[Add New User] (新規ユーザの追加)"参照先 』ページの [Active] (有効化) チェックボックスをオンにしてユーザ アカウントを有効化する必要があります。

[Encryption and Share] (暗号化および共有)

[Encryption & Share] (暗号化および共有) の設定を使用して、使用する暗号化のタイプ、PC と VM の共有モード、KX II-101 のリセット ボタンが押下された場合に実行されるリセットのタイプを指定できます。



- [Encryption Mode] (暗号化モード)。 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。 暗号化モードを選択した場合、使用しているブラウザが選択したモードをサポートしていないと、KX II-101 に接続できないという警告が表示されます。



  - [Auto] (自動)。 推奨されるオプションです。KX II-101 はオート ネゴシエーションを行い、最も高い暗号化レベルに設定されます。

  - [RC4]。 RSA RC4 暗号方式を使用して、ユーザ名、パスワード、ビデオ送信を含む KVM データが保護されます。 これは、最初の接続認証中に KX II-101 ユニットとリモート 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。
  - [AES-128]。 AES (Advanced Encryption Standard) 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 はキーの長さを表します。 [AES-128] 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。 詳細については、「***使用しているブラウザの AES 暗号化の確認*** 『p. 152』」を参照してください。
  - [AES-256]。 AES (Advanced Encryption Standard) 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 はキーの長さを表します。 [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。 詳細については、「***使用しているブラウザの AES 暗号化の確認*** 『p. 152』」を参照してください。
- [Apply Encryption Mode to KVM and Virtual Media] (暗号化モードを KVM および仮想メディアに適用する)。 このオプションを選択すると、選択された暗号化モードが KVM と仮想メディアの両方に適用されます。 認証後、KVM データと仮想メディア データにも 128 ビットの暗号化が適用され、転送されます。
- [PC Share Mode] (PC 共有モード)。 グローバルな同時リモート KVM アクセスを特定し、最大 8 人までのリモート ユーザが KX II-101 に同時にログオンし、デバイスを介してターゲット サーバを同時に表示および制御できるようにします。 ドロップダウン リストをクリックして、次のオプションのいずれかを選択します。
  - [Private] (プライベート)。 PC を共有しません。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-Share] (PC 共有)。 KVM ターゲット サーバに最大 8 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。 ただし、リモート ユーザはキーボートやマウスで全く同じ操作を行えるため、文字の入力やマウスの操作を止めないユーザがいると、正しく操作できない場合があることに注意してください。

- [VM Share Mode] (VM 共有モード)。 このオプションは [PC-Share Mode] (PC 共有モード) が有効な場合にのみ有効になります。 このオプションを選択すると、複数のユーザで仮想メディアを共有できるようになります。つまり、複数のユーザが同じ仮想メディア セッションにアクセスできます。 デフォルトでは無効に設定されています。
- [Local Device Reset Mode] (ローカル デバイス リセット モード)。 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されるアクションを指定します。 詳細については、「リセット ボタン」を参照してください。 次のオプションのいずれかを選択します。
  - [Enable Local Factory Reset] (ローカルでのファクトリ リセットを有効にする)(デフォルト)。 KX II-101 ユニットを工場出荷時のデフォルトに戻します。
  - [Enable Local Admin Password Reset] (ローカルでの管理者パスワードの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「raritan」に戻ります。
  - [Disable All Local Resets] (ローカルでのすべてのリセットを無効にする)。 リセットは一切実行されません。

使用しているブラウザの AES 暗号化の確認

使用しているブラウザで AES がサポートされているかどうかが不明な場合は、ブラウザ メーカーに問い合わせるか、暗号化方式を確認するブラウザを使用して次の Web サイトにアクセスしてください。 https://www.fortify.net/sslcheck.html。 この Web サイトでは、使用しているブラウザの暗号化方式を検出し、レポートを表示できます。

注: IE6 は AES 128 または 256 ビット暗号化をサポートしません。

AES 256 の前提条件とサポートされる設定

AES 256 ビット暗号化は、次の Web ブラウザでのみサポートされます。

- Firefox 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

ブラウザによるサポートに加え、AES 256 ビット暗号化では、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、次のリンクの [その他のダウンロード] セクションで入手できます。

- JRE1.4.2 - http://java.sun.com/j2se/1.4.2/download.html
- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

[IP Access Control] (IP アクセス制御)

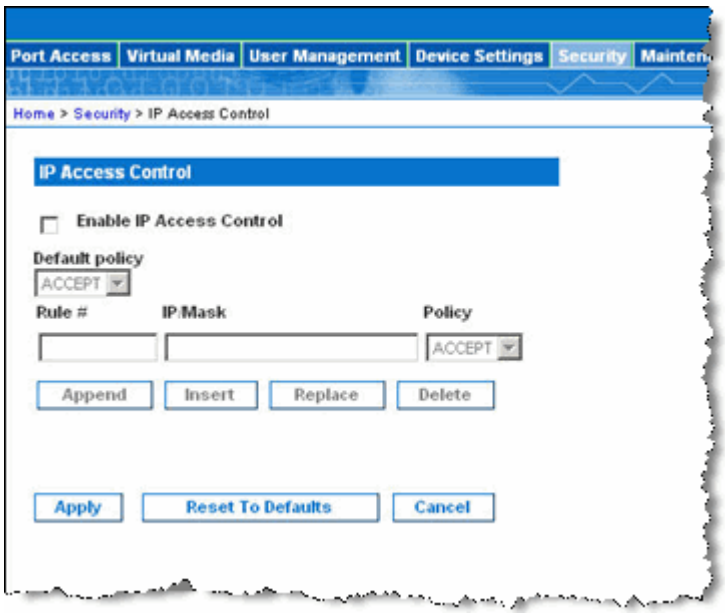
IP アクセス制御を使用して、KX II-101 ユニットへのアクセスを制御できます。 グローバル アクセス制御リスト (ACL) の設定を行い、許可されていない IP アドレスから送信されるパケットにデバイスが応答することのないようにします。 IP アクセス制御はグローバルに作用し、KX II-101 ユニット全体に影響しますが、グループレベルでユニットへのアクセスを制御することもできます。 グループレベルの制御の詳細については、「グループ ベースの IP ACL (アクセス制御リスト)」を参照してください。

重要: KX II-101 ローカル ポートでは、IP アドレス 127.0.0.1 が使用されます。 IP アクセス制御リストを作成する際に、ブロックされる IP アドレス範囲に 127.0.0.1 が含まれていると、KX II-101 ローカル ポートにアクセスできなくなります。

➢ *IP アクセス制御を使用するには、以下の手順に従います。*

1. 次のいずれかの方法を使用して、[IP Access Control] (IP アクセス制御) ページを開きます。
   - [Security] (セキュリティ) の [IP Access Control] (IP アクセス制御) を選択します。または、
   - [Network Settings] (ネットワーク設定) ページで [Set System ACL] (システム ACL の設定) ボタンをクリックします。

   [IP Access Control] (IP アクセス制御) ページが開きます。



2. [Enable IP Access Control] (IP アクセス制御を有効にする) チェックボックスをオンにし、IP アクセス制御とページの残りのフィールドを有効にします。

3. [Default Policy] (デフォルト ポリシー) を選択します。 これは、指定した範囲内にない IP アドレスに対して実行されるアクションを表します。
   - [Accept] (承諾)。 その IP アドレスによる KX II-101 デバイスへのアクセスが許可されます。
   - [Drop] (拒否)。 その IP アドレスによる KX II-101 デバイスへのアクセスが拒否されます。

➢ *新しいルールを追加するには、以下の手順に従います。*

1. [IP/Mask] (IP/マスク) フィールドに IP アドレスとサブネット マスクを入力します。
2. ドロップダウン リストからポリシーを選択します。
3. [Append] (追加) をクリックします。 ルール リストの 1 番下にルールが追加されます。
4. 入力する各ルールについて、手順 1 ～ 3 を繰り返します。

➢ *ルールを挿入するには、以下の手順に従います。*

1. [Rule] (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. [IP/Mask] (IP/マスク) フィールドに IP アドレスとサブネット マスクを入力します。
3. ドロップダウン リストからポリシーを選択します。
4. [Insert] (挿入) をクリックします。 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。

➢ *ルールを置き換えるには、以下の手順に従います。*

1. 置き換える [Rule] (ルール) 番号を指定します。
2. [IP/Mask] (IP/マスク) フィールドに IP アドレスとサブネット マスクを入力します。
3. ドロップダウン リストからポリシーを選択します。
4. [Replace] (置き換え) を選択します。 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、以下の手順に従います。*

1. 削除する [Rule] (ルール) 番号を指定します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されます。 [OK] をクリックします。

ヒント: ルール番号を使用すると、ルールが作成された順番を基により詳細に制御できます。

11 メンテナンス

この章の内容

[Maintenance] (メンテナンス) メニュー

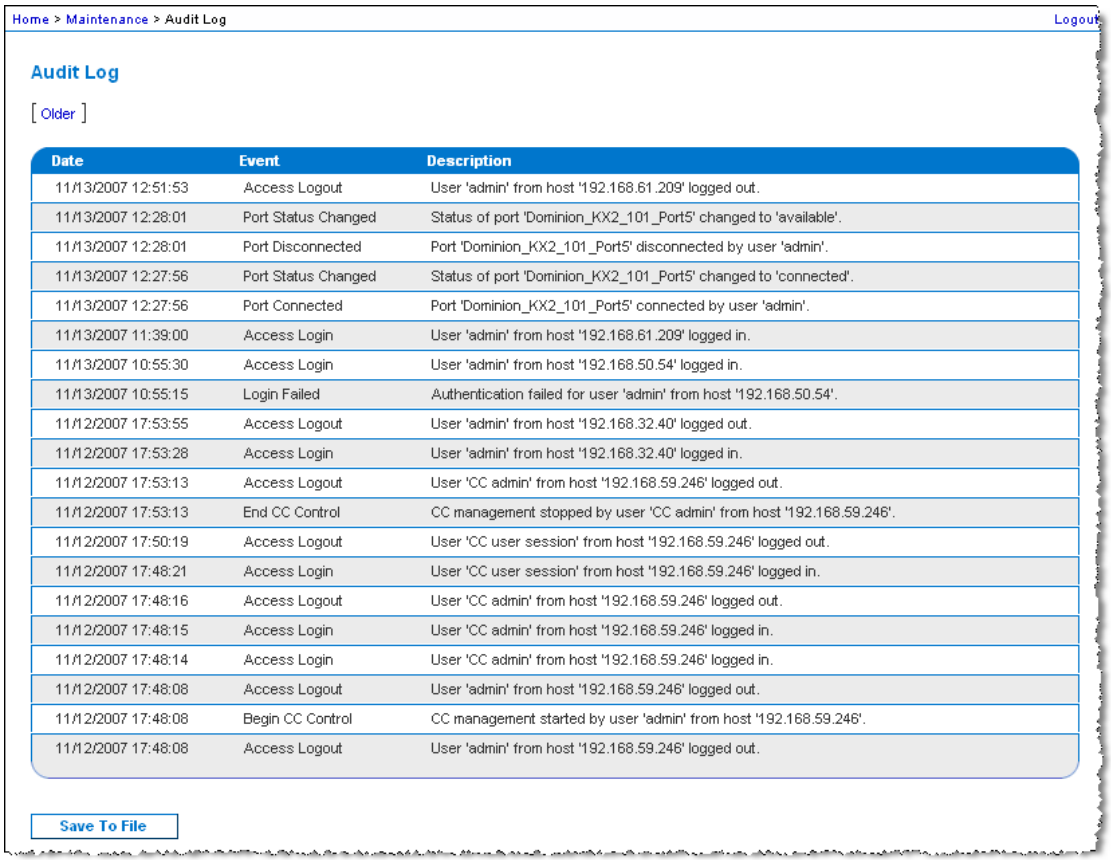
[Maintenance] (メンテナンス) メニューには次のオプションが含まれます。 [Audit Log] (監査ログ)、[Device Information] (デバイス情報)、[Backup/Restore] (バックアップと復元)、[Firmware Upgrade] (ファームウェアのアップグレード)、[Factory Reset] (ファクトリ リセット)、[Upgrade History] (アップグレード履歴)、[Reboot] (再起動)。

[Audit Log] (監査ログ)

KX II-101 のシステム イベントに関するログが作成されます。

➢ *KX II-101 ユニットの監査ログを表示するには、以下の手順に従います。*

1. [Maintenance] (メンテナンス) の [Audit Log] (監査ログ) を選択します。[Audit Log] (監査ログ) ページが開きます。



Date	Event	Description
11/13/2007 12:51:53	Access Logout	User 'admin' from host '192.168.61.209' logged out.
11/13/2007 12:28:01	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'available'.
11/13/2007 12:28:01	Port Disconnected	Port 'Dominion_KX2_101_Port5' disconnected by user 'admin'.
11/13/2007 12:27:56	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'connected'.
11/13/2007 12:27:56	Port Connected	Port 'Dominion_KX2_101_Port5' connected by user 'admin'.
11/13/2007 11:39:00	Access Login	User 'admin' from host '192.168.61.209' logged in.
11/13/2007 10:55:30	Access Login	User 'admin' from host '192.168.50.54' logged in.
11/13/2007 10:55:15	Login Failed	Authentication failed for user 'admin' from host '192.168.50.54'.
11/12/2007 17:53:55	Access Logout	User 'admin' from host '192.168.32.40' logged out.
11/12/2007 17:53:28	Access Login	User 'admin' from host '192.168.32.40' logged in.
11/12/2007 17:53:13	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:53:13	End CC Control	CC management stopped by user 'CC admin' from host '192.168.59.246'.
11/12/2007 17:50:19	Access Logout	User 'CC user session' from host '192.168.59.246' logged out.
11/12/2007 17:48:21	Access Login	User 'CC user session' from host '192.168.59.246' logged in.
11/12/2007 17:48:16	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:15	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:14	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:08	Begin CC Control	CC management started by user 'admin' from host '192.168.59.246'.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.

[Audit Log] (監査ログ) ページには、日付と時刻順にイベントが表示されます (最も新しいイベントが 1 番上に表示されます)。 監査ログには次の情報が含まれます。

- [Date] (日付)。 イベントの発生した日付と時刻です。24 時間制で表示されます。
- [Event] (イベント)。 [Event Management] (イベント管理) ページに表示されるイベント名です。
- [Description] (説明)。 イベントの詳細な説明です。

➢ *監査ログを保存するには、以下の手順に従います。*

注: 監査ログの保存は KX II-101 リモート コンソールでのみ実行できます。ローカル コンソールでは実行できません。

---

1. [Save to File] (ファイルに保存) ボタンをクリックします。 [Save File] (ファイルの保存) ダイアログ ボックスが開きます。
2. 対象のファイル名と保存先を選択し、[Save] (保存) をクリックします。 監査ログは、クライアント マシン上で指定した場所に指定した名前でローカルに保存されます。

➢ *監査ログのページを移動するには、以下の手順に従います。*

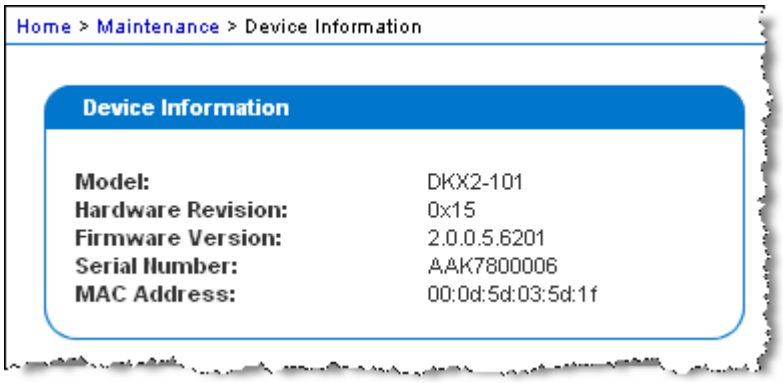
- [Older] (古いログへ) リンクおよび [Newer] (新しいログへ) リンクを使用します。

[Device Information] (デバイス情報)

[Device Information] (デバイス情報) ページでは、使用している KX II-101 デバイスに関する詳細な情報を確認できます。 この情報は、Raritan のテクニカル サポートにご連絡いただく際に役立ちます。

➢ *KX II-101 に関する情報を表示するには、以下の手順に従います。*

- [Maintenance] (メンテナンス) の [Device Information] (デバイス情報) を選択します。 [Device Information] (デバイス情報) ページが開きます。



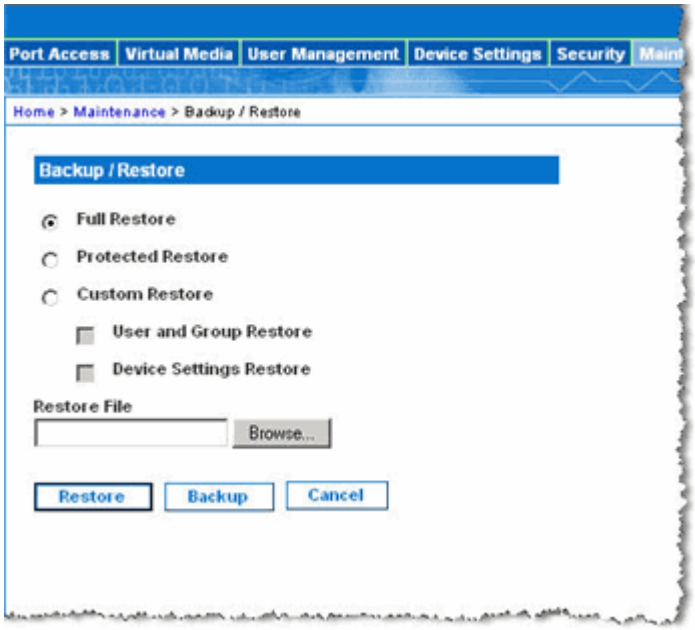
使用している KX II-101 に関する以下の情報が提供されます。 [Model] (モデル)、[Hardware Revision] (ハードウェア リビジョン)、[Firmware Version] (ファームウェア バージョン)、[Serial Number] (シリアル番号)、[MAC Address] (MAC アドレス)。

[Backup and Restore] (バックアップと復元)

[Backup/Restore] (バックアップ/復元) ページでは、Dominion KX II の設定と構成をバックアップおよび復元できます。 バックアップと復元は、業務の継続性に貢献するだけではありません。この機能は、時間を節約するためのメカニズムとしても役立ちます。 たとえば、使用中の KX II-101 のユーザ設定をバックアップして、それを新しい KX II-101 に復元することで、別の KX II-101 から自分のチームにすばやくアクセスできます。 また、1 台の KX II-101 でセットアップを行い、その設定を複数の KX II-101 デバイスにコピーすることもできます。

➢ *[Backup/Restore] (バックアップ/復元) ページを表示するには、以下の手順に従います。*

- [Maintenance] (メンテナンス)の [Backup/Restore] (バックアップ/復元) を選択します。 [Backup/Restore] (バックアップ/復元) ページが開きます。



注: バックアップを行うと、常にシステム全体がバックアップされます。 復元については、全体の復元と部分的な復元のどちらかを選択できます。

➢ *KX II-101 をバックアップするには、以下の手順に従います。*

1. [Backup] (バックアップ) をクリックします。 [File Download] (ファイルのダウンロード) ダイアログ ボックスが表示されます。
2. [Save] (保存) をクリックします。 [Save As] (名前を付けて保存) ダイアログ ボックスが表示されます。

3. 保存先を選択し、ファイル名を指定してから、[Save] (保存) をクリックします。 [Download Complete] (ダウンロードの完了) ダイアログ ボックスが表示されます。
4. [Close] (閉じる) をクリックします。 バックアップ ファイルは、使用しているクライアント マシン上で指定した場所に指定した名前で、ローカルに保存されます。

➢ *KX II-101 を復元するには、以下の手順に従います。*

警告: 使用している KX II-101 を以前のバージョンに復元する際には、注意が必要です。 バックアップ時点に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名とパスワードを記憶していないと、KX II-101 からロックアウトされます。

また、バックアップの時点で現在とは異なる IP アドレスを使用していた場合は、その IP アドレスも同様に復元されます。 設定で DHCP を使用している場合は、更新後にローカル ポートにアクセスし、IP アドレスを確認する際にのみこの操作を行うことが考えられます。

1. 実行する復元のタイプを選択します。
   - [Full Restore] (完全な復元)。 システム全体の完全な復元を行います。 一般に、従来のバックアップと復元の目的で使用します。
   - [Protected Restore] (保護された復元)。 シリアル番号、MAC アドレス、IP アドレス、名前などのデバイスに固有な情報を除き、システム全体が復元されます。 このオプションを使用すると、1 台の KX II-101 でセットアップを行い、その設定を複数の KX II-101 デバイスにコピーすることもできます。
   - [Custom Restore] (カスタム復元)。 このオプションでは、[User and Group Restore] (ユーザとグループの復元)、[Device Settings Restore] (デバイス設定の復元) のどちらか一方または両方を選択できます。 該当するチェックボックスをオンにします。
     - [User and Group Restore] (ユーザとグループの復元)。 このオプションに含まれるのは、ユーザとグループの情報だけです。 このオプションを使用すると、別の KX II-101 にすばやくユーザを設定できます。
     - [Device Settings Restore] (デバイス設定の復元)。 このオプションに含まれるのは、デバイス設定だけです。 このオプションを使用すると、デバイス情報をすばやくコピーできます。
2. [Browse] (参照) ボタンをクリックします。 [Choose file] (ファイルの選択) ダイアログ ボックスが表示されます。
3. 適切なバックアップ ファイルに移動して選択し、[Open] (開く) をクリックします。 選択したファイルは、[Restore File] (復元ファイル) フィールドにリスト表示されます。

4. [Restore] (復元) を選択します。 選択した復元のタイプに基づいて、設定が復元されます。

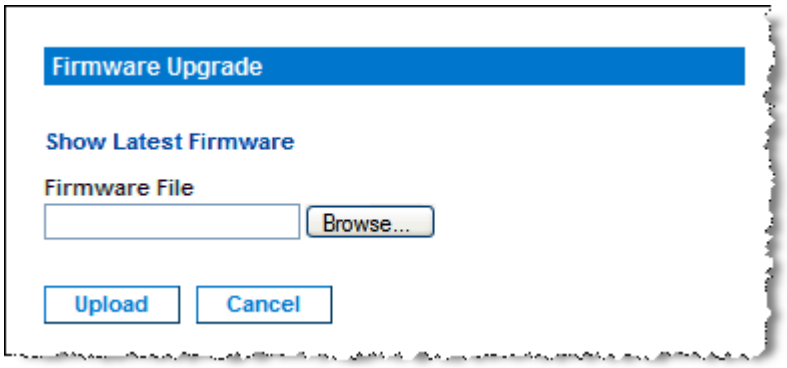
[Firmware Upgrade] (ファームウェアのアップグレード)

[Firmware Upgrade] (ファームウェアのアップグレード) ページを使用して、KX II-101 ユニットのファームウェアをアップグレードします。 このページは、KX II-101 リモート コンソールでのみ使用できます。

重要: アップグレードの実行中は、使用している KX II-101 ユニットの電源を切断しないでください。ユニットが損傷する可能性があります。

➢ *KX II-101 ユニットをアップグレードするには、以下の手順に従います。*

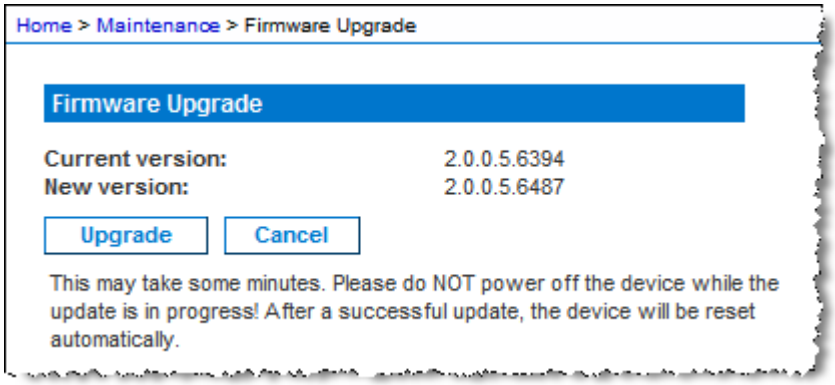
1. [Maintenance] (メンテナンス) の [Firmware Upgrade] (ファームウェアのアップグレード) を選択します。 [Firmware Upgrade] (ファームウェアのアップグレード) ページが開きます。



2. [Show Latest Firmware] (最新のファームウェアの表示) リンクをクリックし、[Firmware Upgrades] (ファームウェア アップグレード) の [KX II-101] ページで適切な Raritan ファームウェアの配布ファイル (*.RFP) を確認し、ダウンロードします。
3. ファイルを解凍して、アップグレードを実行する前に、ファームウェアの ZIP ファイルに含まれる手順をすべてお読みください。

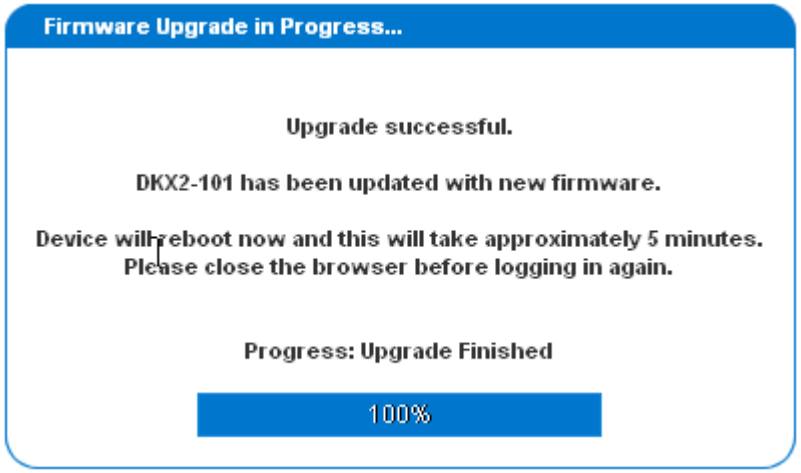
注: アップロードの前に、ファームウェア更新ファイルをローカル PC にコピーしてください。 ファイルをネットワーク ドライブからロードしないでください。 [Browse] (参照) ボタンをクリックして、アップグレード ファイルを解凍したディレクトリに移動します。

4. [Firmware Upgrade] (ファームウェアのアップグレード) ページで [Upload] (アップロード) をクリックします。 アップグレードに関する情報とバージョン番号が確認のために表示されます。



注: この時点で接続していたユーザはログアウトされ、新たなログインの試行はブロックされます。

5. [Upgrade] (アップグレード) をクリックします。 アップグレードが完了するまで待機します。 アップグレード中は、ステータス情報と進捗状況を示すバーが表示されます。 アップグレードが完了すると、ユニットが再起動します。



6. 表示に従ってブラウザを閉じ、約 5 分待ってから、再度 KX II-101 にログインします。

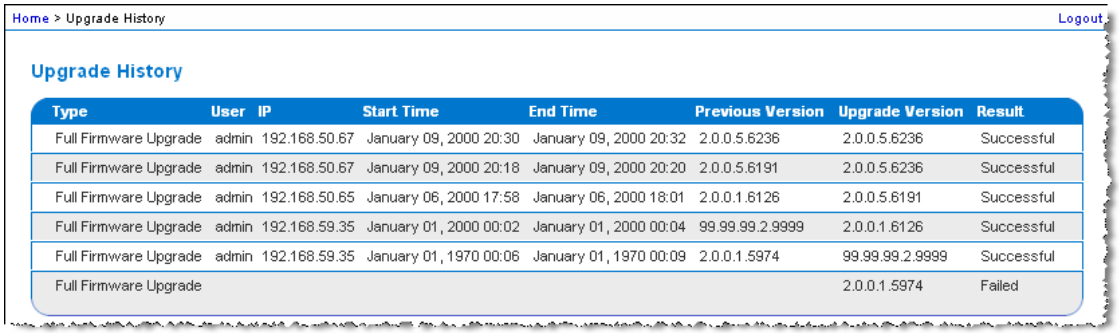
   Multi-Platform Client を使用してデバイス ファームウェアのアップグレードを行う方法については、『Raritan Multi-Platform Client (MPC) ユーザ ガイド』を参照してください。

アップグレード履歴

KX II-101 では、KX II-101 ユニットと接続されている CIM で実行したアップグレードに関する情報を確認できます。

➢ *アップグレード履歴を表示するには、以下の手順に従います。*

- [Maintenance] (メンテナンス)の [Upgrade History] (アップグレード履歴)を選択します。 [Upgrade History] (アップグレード履歴) ページが開きます。



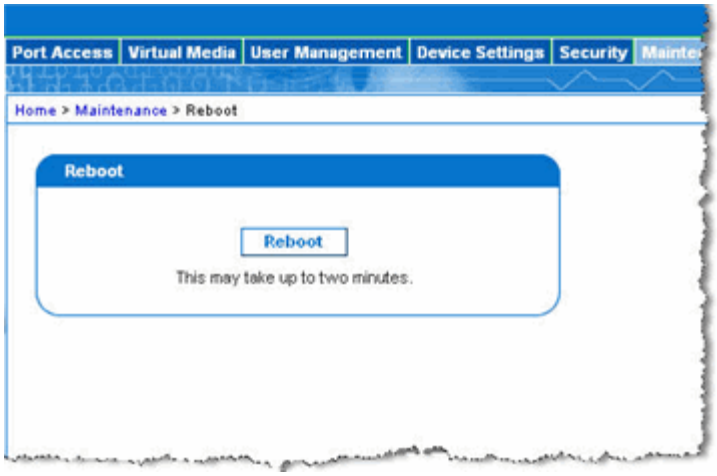
[Reboot] (再起動)

[Reboot] (再起動) ページを使用すると、安全かつ制御された順序で KX II-101 ユニットを再起動できます。そのため、この方法で再起動を行うことをお勧めします。

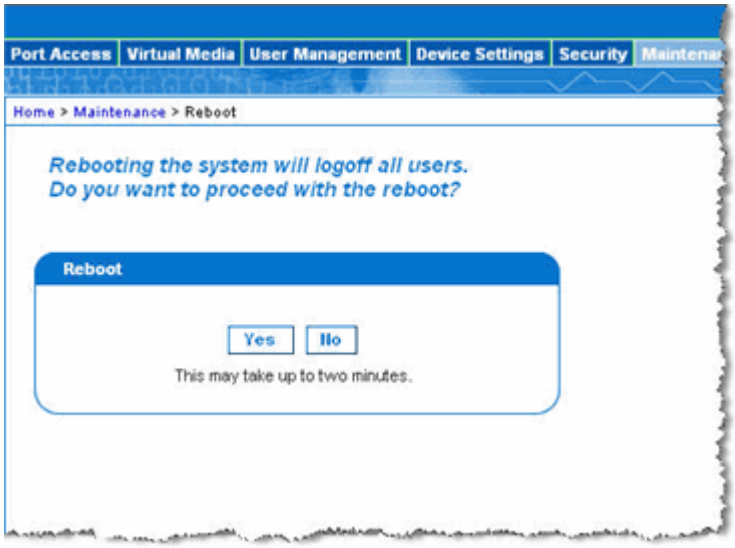
重要: すべての KVM およびシリアル接続が切断され、ユーザもすべてログオフされます。

➢ *KX II-101 を再起動するには、以下の手順に従います。*

1. [Maintenance] (メンテナンス)の [Reboot] (再起動) を選択します。 [Reboot] (再起動) ページが開きます。



2. [Reboot] (再起動) ボタンをクリックします。 操作を確認するプロンプトが表示されます。



3. [Yes] (はい) をクリックして、再起動を続行します。

➢ *再起動せずに終了するには、以下の手順に従います。*

- [No] (いいえ) をクリックします。

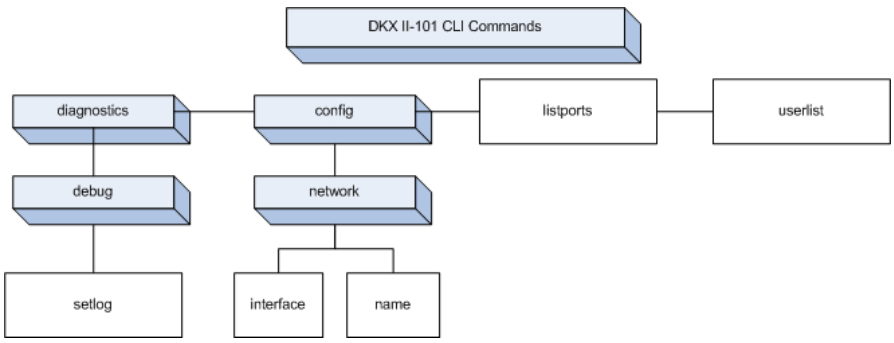
12 コマンド ライン インタフェース（CLI）

この章の内容

概要

この章では、KX II-101 で使用できる CLI コマンドの概要について説明します。コマンドの一覧および定義、コマンドの例が示されているこの章のセクションへのリンクについては、*「CLI コマンド」*『p. 170の"CLI コマンド"参照先 』」を参照してください。

以下の図は CLI コマンドの概要です。



注: 次のコマンドは、前の図の CLI のすべてのレベルから使用できます。top、history、logout、quit、help。

CLI を使用しての KX II-101 へのアクセス

次の方法のいずれかを使用して、KX II-101 にアクセスします。

- IP 接続を介した TELNET
- IP 接続を介した SSH (Secure Shell)
- 付属のケーブルと HyperTerminal のようなターミナル エミュレーション プログラムを使用しての RS-232 シリアル インタフェースを介した多機能管理シリアル ポート

複数の SSH/TELNET クライアントを使用可能で、次の場所から取得できます。

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/*** http://www.chiark.greenend.org.uk/~sgtatham/putty/
- ssh.com の SSH クライアント - ***www.ssh.com*** http://www.ssh.com
- Applet SSH Client - ***www.netspace.org/ssh*** http://www.netspace.org/ssh
- OpenSSH Client - ***www.openssh.org*** http://www.openssh.org

*注: Accessing the CLI by SSH または TELNET へのアクセスには、KX II-101 Remote Client の [Device Services] (デバイス サービス) ページでアクセスを設定する必要があります。 詳細については、「**デバイス サービス** 『p. 119の"[Device Services] (デバイス サービス)" 参照先 』」を参照してください。*

KX II-101 への SSH 接続

SSHv2 をサポートする SSH クライアントを使用して接続します。 [Devices Services] (デバイス サービス) ページで SSH アクセスを有効にする必要があります。詳細については、「***デバイス サービス*** 『p. 119の"[Device Services] (デバイス サービス)"参照先 』」を参照してください。

注: セキュリティ上の理由から、SSH V1 は KX II-101 でサポートされていません。

Windows PC からの SSH アクセス

➢ *Windows PC から SSH セッションを開くには、以下の手順に従います。*

1. PuTTY などの SSH クライアント ソフトウェアを起動します。
2. KX II-101 サーバの IP アドレス「192.168.0.192」を入力します。
3. デフォルトの設定ポート 22 を使用する [SSH] を選択します。
4. [Open] (開く) ボタンをクリックします。

5. 次のプロンプトが表示されます。
   `login as:`

ログイン情報の詳細は、「ログオン」セクションを参照してください。

UNIX ワークステーションからの SSH アクセス

- *UNIX/Linux ワークステーションから SSH セッションを開き、ユーザ admin としてログオンするには、次のコマンドを入力します。*

```
ssh -l admin 192.168.30.222
```

パスワードのプロンプトが表示されます。

ログイン情報の詳細は、「ログオン」セクションを参照してください。

ログイン

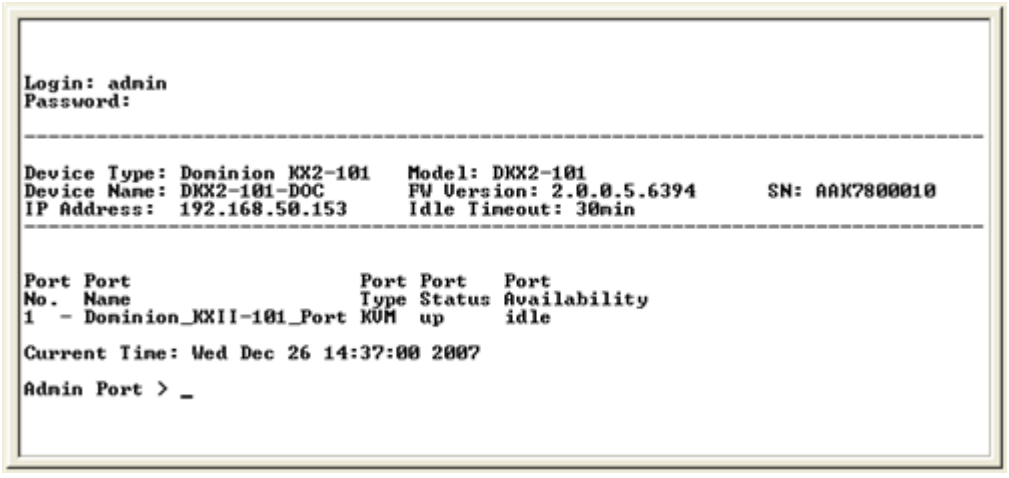
- *ログインするには、次のように ユーザ名 admin を入力します。*

  `Login: admin`

  パスワードのプロンプトが表示されます。 デフォルト パスワード raritan を入力します。

  `Password:`

  ようこそメッセージが表示されます。 以上で、管理者としてログインしています。



次の「*CLI のナビゲーション* 『p. 169』」セクションを確認したら、「***管理シリアル コンソールの使用*** 『p. 25の"ターミナル エミュレーション プログラムの使用"参照先 』」で説明されている初期設定タスクを実行できます。

CLI のナビゲーション

CLI を使用する前に、CLI のナビゲーションと構文を理解しておくことが重要です。さらに、CLI の使用を簡素化するキーの組み合わせがあります。

CLI プロンプト

コマンド ライン インタフェースのプロンプトは、現在のコマンド レベルを示します。 プロンプトのルート部分はログイン名です。ターミナル エミュレーション アプリケーションを使用する管理シリアル ポートへの直接接続の場合、Admin Port がコマンドのルート プロンプトです。

```
Admin Port > Config > Network >
```

TELNET/SSH の場合、admin がコマンドのルート プロンプトです。

```
admin > config > network >
```

コマンドの完成

CLI は、部分的に入力されたコマンドの完成をサポートします。 入力の最初の数文字を入力して Tab キーを押します。文字例が一意に一致する場合、CLI は入力を完成させます。

- 一致が見つからない場合、CLI はそのレベルの有効なエントリを表示します。
- 複数の可能性のある一致が見つかった場合、CLI は有効なエントリも表示します。
- エントリを一意にするために追加のテキストを入力し、Tab キーを押して入力を完成させます。

CLI 構文 - ヒントとショートカット

ヒント

- コマンドはアルファベット順に一覧表示されます。
- コマンドでは大文字と小文字を区別しません。
- パラメータ名は下線を含まない 1 つの単語で表されます。
- 引数のないコマンドはデフォルトでコマンドの現在の設定を示します。
- コマンドの後に疑問符 (?) を入力すると、そのコマンドのヘルプが表示されます。
- 縦線 (|) はオプションまたは必須のキーワードまたは引数内の選択肢を示します。

ショートカット

- 最後のエントリを表示するには、上向きの矢印を押します。
- 入力した最後の文字を削除するには、Backspace キーを押します。
- 間違ったパラメータを入力した場合は、Ctrl/C キーを使用してコマンドを終了またはキャンセルします。
- コマンドを実行するには、Enter キーを使用します。
- コマンドを完成するには、Tab キーを押します。 例、`Admin Port > Conf` 。 次に、システムは、`Admin Port > Config >` プロンプトを表示します。

すべてのコマンド ライン インタフェース レベルに共通のコマンド

「CLI コマンド」には、すべての CLI レベルで使用できるコマンドが一覧で表示されています。 これらのコマンドは CLI 内での移動にも役立ちます。

コマンド	説明
top	CLI 階層の最上位または「username」プロンプトに戻ります。
history	KX II-101 CLI で入力された最新の 200 個のコマンドが表示されます。
help	CLI 構文の概要を表示します。
quit	1 レベルだけ戻ります。
logout	ユーザ セッションをログアウトします。

CLI コマンド

下の表は、使用可能なすべての CLI コマンドの一覧とその説明です。

コマンド	説明
config	[Configuration] (設定) メニューに切り替えます。
diagnostics『p. 172』	[diagnostics] (診断) メニューに切り替えます。.
debug『p. 172の "[Debug] (デバッグ)" 参照先 』	[debug] (デバッグ) メニューに切り替えます。
help	CLI 構文の概要を表示します。
history	現在のセッションのコマンド ラインの履歴を表示します。
interface	KX II-101 のネットワーク インタフェースを設定します。
listports『p. 175の "Listports コマンド"参照先 』	ポート、ポート名、ポート タイプ、ポート ステータス、およびポートの可用性を一覧表示します。
logout	現在の CLI セッションをログアウトします。
name『p. 174の "[Name] (名前) コマンド"参照先 』	デバイス名を設定します。
network『p. 173の "[Network] (ネットワーク)"参照先 』	ネットワーク設定を表示し、設定できます。
quit	前のコマンドに戻ります。
setlog『p. 172の "Setlog コマンド"参照先 』	デバイスのログ記録オプションを設定します。
top	[root] (ルート) メニューに戻ります。
userlist『p. 175の "Userlist コマンド"参照先 』	アクティブなユーザ数、ユーザ名、ポート、およびステータスを一覧表示します。

Diagnostics

[Diagnostics] (診断) メニューでは、KX II-101 の各種モジュールのログ記録オプションを設定できます。 Raritan テクニカル サポートのエンジニアに指示された場合のみ、ログ記録オプションを設定する必要があります。 サポート エンジニアは、これらのログ記録オプションを使用して、デバッグおよびトラブルシューティングに関する正しい情報を取得できます。 サポート エンジニアが指示した場合、ログ記録オプションの設定方法とログ ファイルを生成して Raritan テクニカル サポートに送信する方法が指示されます。

重要: Raritan テクニカル サポート エンジニアの監督下でのみログ記録オプションを設定してください。

[Debug] (デバッグ)

[Diagnostics] (診断) の [Debug] (デバッグ) メニューでは、Setlog コマンドを使用して KX II-101 のログ記録オプションを設定できます。

Setlog コマンド

Setlog コマンドを使用すると、KX II-101 の各種モジュールのログ記録レベルを設定し、モジュールごとに現在のログ記録レベルを表示できます。 setlog コマンドの構文は、次のとおりです。

```
setlog [module <module>] [level <level>] [vflag <vflag>]
[verbose <on|off>]

 Set/Get diag log level
```

次の表で、Setlog コマンドのオプションを説明します。 Raritan テクニカル サポートから、これらの設定の指定方法をお伝えします。

コマンドのオプション	説明
module	モジュール名。
level	診断レベル: err warn info debug trace

コマンドのオプション	説明
vflag	verbose flag のタイプ: timestamp module thread fileline
verbose [on|off]	ログ記録をオンまたはオフにします。

Setlog コマンドの例

次の Setlog コマンドは、libpp_serial モジュールの verbose ログ記録をオンにしたデバッグのログ記録レベルを設定しています。

```
Setlog module libpp_serial level debug verbose on
```

[Configuration] (設定)

[Configuration] (設定) メニューでは、ネットワーク インタフェースの設定とデバイス名の設定に使用する network コマンドにアクセスできます。

[Network] (ネットワーク)

[Configuration] (設定) の [Network] (ネットワーク) コマンドを使用して、KX II-101 のネットワーク接続とデバイス名を設定します。

コマンド	説明
interface	KX II-101 のネットワーク インタフェースを設定します。
name	デバイス名を設定します。

[Name] (名前) コマンド

name コマンドを使用して、デバイス名とホスト名を設定します。

デバイス名の構文は、次のとおりです。

```
name devicename <>
```

ホスト名の構文は、次のとおりです。

```
name hostname <>
```

`name` コマンドの例

次のコマンドは、デバイス名を設定します。

```
Admin Port > Config > Network > name devicename <device
name>
```

次のコマンドは、ホスト名を設定します。

```
Admin Port > Config > Network > name hostname <host name>
```

[Interface] (インタフェース) コマンド

interface コマンドを使用して、KX II-101 のネットワーク インタフェースを設定します。 コマンドが受け入れられると、ユニットは HTTP/HTTPS 接続を切断して新しいネットワーク接続を初期化します。 すべての HTTP/HTTPS ユーザは、新しい IP アドレスと正しいユーザ名およびパスワードを使用してデバイスに再接続する必要があります。 詳細は、「***インストールと設定*** 『p. 7』」を参照してください。

interface コマンドの構文は、次のとおりです。

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode
<auto/10hdx/10fdx/100hdx/100fdx]
```

次の表で、network コマンドのオプションを説明します。

コマンドのオプション	説明
ipauto	固定または動的 IP アドレス。
ip ipaddress	IP ネットワークからのアクセスに割り当てられる KX II-101 の IP アドレス
mask subnetmask	IP 管理者から取得したサブネット マスク
gw ipaddress	IP 管理者から取得したゲートウェイ IP アドレス
mode <auto | 100fdx>	[Ethernet Mode] (Ethernet モード) を auto に設定します。または、100Mbps 全二重 (100fdx) を指定します。

Interface コマンドの例

次のコマンドは、IP アドレス、マスク、ゲートウェイ アドレスを設定し、モードを自動検出に設定します。

```
Admin Port > Config > Network > interface ipauto none ip 192.168.50.12 mask 255.255.255.0 gw 192.168.51.12 mode auto
```

Listports コマンド

Listports コマンドは、アクティブなユーザ数、ユーザ名、ポート、およびステータスを一覧表示します。

Listports コマンドの例

```
Admin Port > listports

Port Port                 Port Port   Port
No.  Name                 Type Status Availability
1  - Dominion_KXII-101_Port KVM  up     idle
```

Userlist コマンド

Userlist コマンドは、ポート、ポート名、ポート タイプ、ポート ステータス、およびポートの可用性を一覧表示します。

Userlist コマンドの例

```
Admin Port > Userlist

Active user number: 1

User Name | From      | Status

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

admin     | Admin Port | active
```

13 Diagnostics

この章の内容

[Diagnostics] (診断) メニュー

[Diagnostics] (診断) ページはトラブルシューティングの目的で使用されるページであり、主に KX II-101 デバイスの管理者を対象としています。 すべての [Diagnostics] (診断) ページで ([Diagnostics] (診断) を除く)、標準的なネットワーク コマンドが実行されます。表示される情報は、それらのコマンドの出力結果です。 [Diagnostics] (診断) メニュー オプションは、ネットワーク設定のデバッグと変更に役立ちます。

[Diagnostics] (診断) は、Raritan テクニカル サポートの指示に従って使用するオプションです。

次のオプションを使用できます。

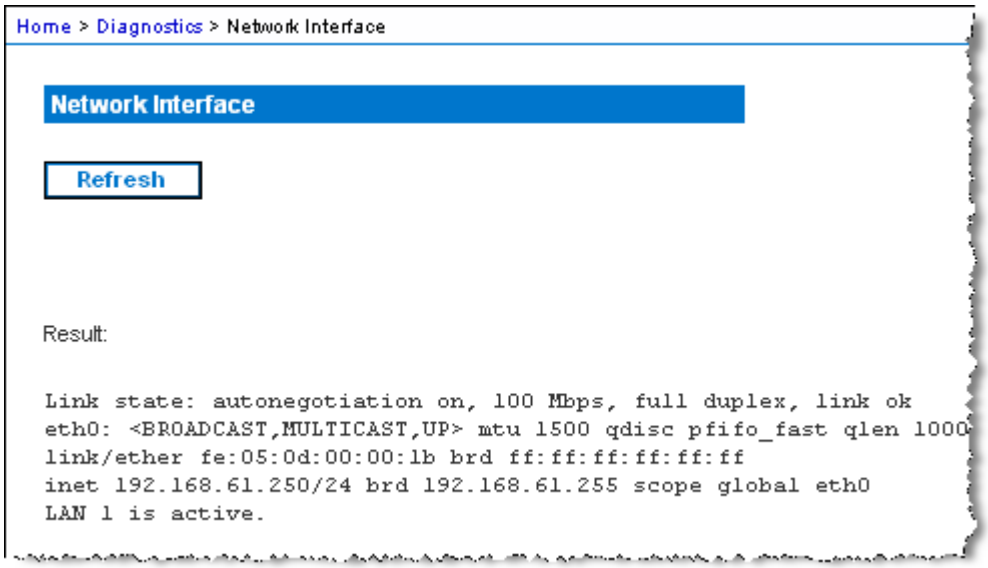
メニュー	操作
[Network Interface] (ネットワーク インタフェース)	ネットワーク インタフェースの状態を取得します。
[Network Statistics] (ネットワーク統計)	ネットワークについての統計を取得します。
[Ping Host] (ホストへの Ping)	特定のホストが IP ネットワーク上でアクセス可能かどうかを特定します。
[Trace Route to Host] (ホストへのトレース ルート)	選択したホストまでのすべてのルートを特定します。
[Device Diagnostics] (デバイス診断)	Raritan テクニカル サポートの指示があった場合に使用します (リモート コンソールのみ)。

[Network Interface] (ネットワーク インタフェース) ページ

KX II-101 では、ネットワーク インタフェースの状態に関する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、以下の手順に従います。*

- [Diagnostics] (診断) の [Network Interface] (ネットワーク インタフェース) を選択します。 [Network Interface] (ネットワーク インタフェース) ページが開きます。



次の情報が表示されます。

- Ethernet インタフェースが稼動しているか、ダウンしているか。
- ゲートウェイが Ping 可能か否か。
- 現在アクティブな LAN ポート。

➢ *この情報を更新するには、以下の手順に従います。*

- [Refresh] (更新) ボタンをクリックします。

[Network Statistics] (ネットワーク統計) ページ

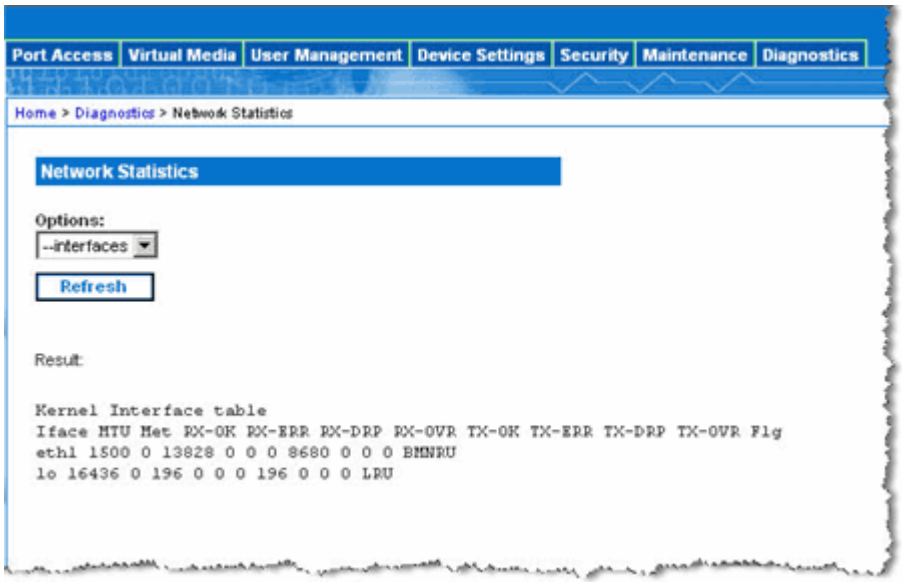
KX II-101 では、ネットワーク インタフェースに関する統計を確認できます。

➢ *ネットワーク インタフェースの統計を表示するには、以下の手順に従います。*

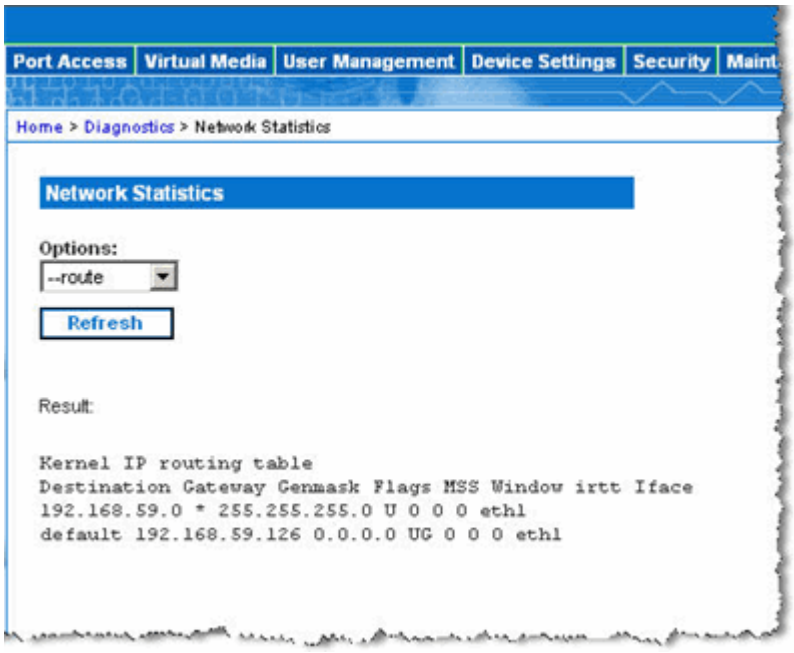
1. [Diagnostics] (診断) の [Network Statistics] (ネットワーク統計) を選択します。 [Network Statistics] (ネットワーク統計) ページが開きます。

2. [Option] (オプション) ドロップダウン リストから適切なオプションを選択します。
   - [Statistics] (統計)。 次に示すようなページが生成されます。

- [Interfaces] (インタフェース)。 次に示すようなページが生成されます。



- [Route] (ルート)。 次に示すようなページが生成されます。



3. [Refresh] (更新) ボタンをクリックします。

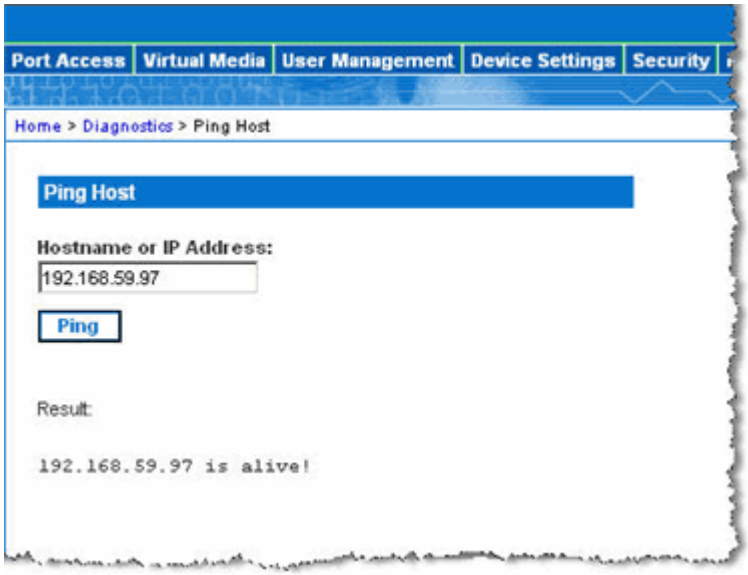
   [Result] (結果) フィールドに該当する情報が表示されます。

[Ping Host] (ホストへの Ping) ページ

Ping は、特定のホストまたは IP アドレスが IP ネットワーク上でアクセス可能であるかどうかをテストするために使用される、ネットワーク ツールです。 [Ping Host] (ホストへの Ping) ページを使用すると、ターゲット サーバまたは別の KX II-101 ユニット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。

➢ *ホストに Ping を実行するには、以下の手順に従います。*

1. [Diagnostics] (診断) の [Ping Host] (ホストへの Ping) を選択します。 [Ping Host] (ホストへの Ping) ページが開きます。



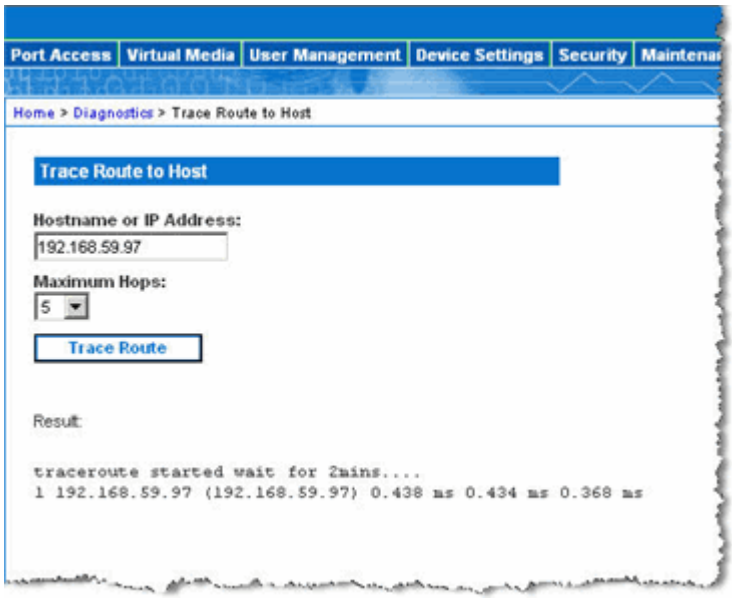
2. [Hostname or IP Address] (ホスト名または IP アドレス) フィールドにホスト名または IP アドレスを入力します。
3. [Ping] をクリックします。 [Result] (結果) フィールドに Ping の結果が表示されます。

[Trace Route to Host] (ホストへのトレース ルート) ページ

トレース ルートは、特定のホスト名または IP アドレスまでに辿るすべてのルートを特定するために使用されるネットワーク ツールです。

➢ *ホストまでのルートをトレースするには、以下の手順に従います。*

1. [Diagnostics] (診断) の [Trace Route to Host] (ホストへのトレース ルート) を選択します。 [Trace Route to Host] (ホストへのトレース ルート) ページが開きます。



2. [Hostname or IP Address] (ホスト名または IP アドレス) フィールドにホスト名または IP アドレスを入力します。
3. ドロップダウン リストから [Maximum Hops] (最大ホップ数) を選択します (5 刻みで 5 ～ 50、)。
4. [Trace Route] (トレース ルート) ボタンをクリックします。 トレース ルート コマンドは、所定のホスト名、IP アドレス、最大ホップ数で実行されます。 [Result] (結果) フィールドにトレース ルートの出力結果が表示されます。

[Device Diagnostics] (デバイス診断)

注: このページは、Raritan フィールド エンジニアによる使用を目的としたページです。Raritan テクニカル サポートに指示された場合に限り、ユーザも使用できます。

[Device Diagnostics] (デバイス診断) ページでは、診断情報を KX II-101 からクライアント マシンにダウンロードします。 Raritan テクニカル サポートが提供するオプションの診断スクリプトと共にまたは単独で、デバイス診断ログを生成できます。 診断スクリプトを使用すると、問題を診断するための多くの情報が得られます。

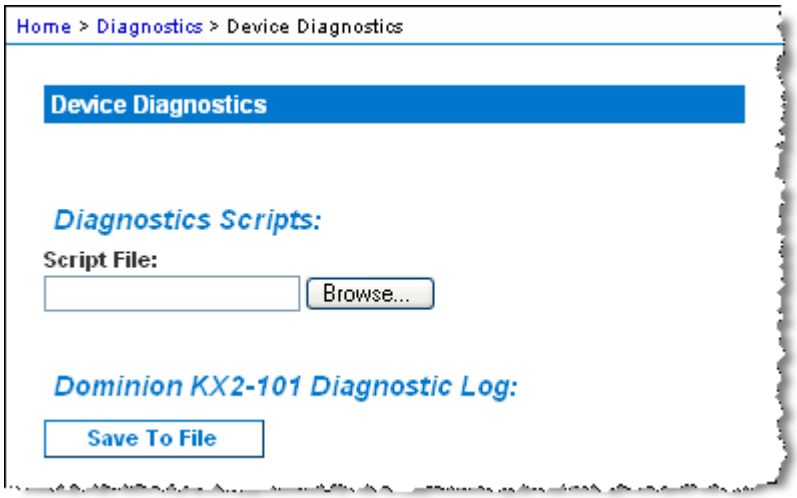
次の設定を使用します。

- 診断スクリプト (オプション) 重大なエラーのデバッグ セッション中に Raritan テクニカル サポートの提供する特別なスクリプトを読み込みます。 スクリプトはユニットにアップロードされ、実行されます。
- デバイス診断ログ。 診断メッセージのスナップショットを KX II-101 ユニットからクライアントにダウンロードします。 この暗号化されたファイルは、その後 Raritan テクニカル サポートに送信されます。このファイルは、Raritan でのみ解析できます。

注: このページにアクセスできるのは管理者特権を持つユーザだけです。

➢ *KX II-101 システム診断を実行するには、以下の手順に従います。*

1. [Diagnostics] (診断) の [Device Diagnostics] (デバイス診断) を選択します。 [Device Diagnostics] (デバイス診断) ページが開きます。

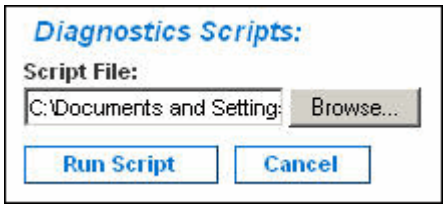


2. (オプション) Raritan テクニカル サポートから診断スクリプトを入手した場合は、以下の手順を実行します。 そうでない場合は、手順 3 に進みます。
   a. Raritan から提供される診断ファイルを取得し、必要に応じて解凍します。

b. [Browse] (参照) ボタンを使用します。 [Choose File] (ファイルの選択) ダイアログ ボックスが開きます。

c. その診断ファイルに移動し、選択します。

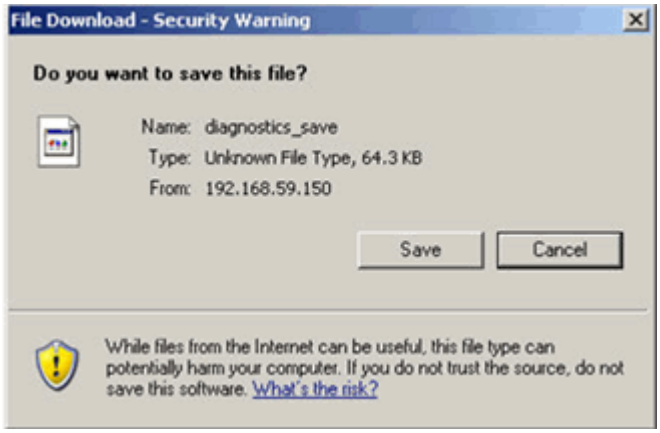
d. [Open] (開く) をクリックします。 [Script File] (スクリプト ファイル) フィールドにファイルが表示されます。



e. [Run Script] (スクリプトを実行する) をクリックします。

3. 診断ファイルを作成して Raritan テクニカル サポートに送信するには、以下の手順に従います。

a. [Save to File] (ファイルに保存) ボタンをクリックします。 [File Download] (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。



b. [Save] (保存) をクリックします。 [Save As] (名前を付けて保存) ダイアログ ボックスが開きます。

c. 適切なディレクトリに移動し、[Save] (保存) をクリックします。

4. Raritan テクニカル サポート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。

14 CC Unmanage

この章の内容

概要

KX II-101 デバイスが CommandCenter Secure Gateway の管理下にあるとき、KX II-101 リモート コンソールを使用してデバイスに直接アクセスを試みると、次のメッセージが表示されます (有効なユーザ名とパスワードの入力後)。

CC-SG 管理からの KX II-101 の除外

CC-SG の制御対象から KX II-101 を除外しない限り、デバイスには直接アクセスできません。 ただし、CommandCenter からのハートビート メッセージを KX II-101 で受信しない場合 (CommandCenter がネットワーク上に存在しない場合など) は、CC-SG の制御対象から KX II-101 を除外してデバイスにアクセスできます。 これは、CC Unmanage 機能を使用することで行えます。

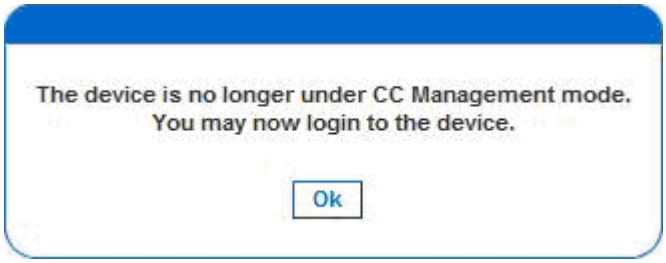
注: この機能を使用するには、メンテナンス権限が必要です。

ハートビート メッセージを受信していない場合にデバイスに直接アクセスを試みると、次のメッセージが表示されます。

➢ *CC-SG 管理からデバイスを除外する（CC Unmanage を使用する）には、以下の手順に従います。*

1. [Yes] (はい) ボタンをクリックします。 操作を確認するプロンプトが表示されます。

2. [Yes] (はい) ボタンをクリックします。 CC の管理対象からのデバイスの除外を確認するメッセージが表示されます。



3. [Yes] (はい) をクリックします。 KX II-101 ログイン ページが開きます。

プロキシ モードでの CC-SG の使用

Virtual KVM Client バージョンが CC-SG プロキシ モードで認識されない

Virtual KVM Client を CommandCenter Secure Gateway (CC-SG) からプロキシ モードで起動すると、Virtual KVM Client バージョンが認識されません。[About Raritan Virtual KVM Client] (バージョン情報) ダイアログ ボックスに、バージョンは「Version Unknown (不明なバージョン)」と表示されます。

プロキシ モードと MPC

KX II-101 を CC-SG 管理下で使用していて、Multi-Platform Client (MPC) の使用を計画している場合は、CC-SG プロキシ モードを使用しないでください。

A 仕様

この章の内容

KX II-101

フォーム ファクタ	Zero U フォーム ファクタ。ラックに縦または横に取り付け可能 (ブラケット キットを付属)
寸法 (DxWxH)	4.055"x 2.913"x 1.063"、103 x 74 x 27mm
重量	0.6292lbs、0.286kg
電源	AC/DC (100-240V~/ 6VDC) 電源アダプタ または Power over Ethernet (PoE) ミッドスパン給電方式 シグナルペア給電方式
使用温度	0° ～ 40°C (32° ～ 104°F)
湿度	20% ～ 85% RH
インジケータ: 青 RARITAN バックライト ロゴ ネットワーク ポート	起動および電力レベル インジケータ ネットワーク アクティビティおよび接続速度インジケータ
ローカル接続	1- USB ポート、USB キーボード / マウス、およびターゲットへの仮想メディア接続用 1- ミニ DIN9 ポート、フル RS-232 機能、モデム接続、および Dominion PX 接続の多機能シリアル ポート用

リモート接続: ネットワーク プロトコル	10/100 Ethernet (RJ45) ポート x 1 TCP/IP、HTTP、HTTPS、UDP、RADIUS、LDAP、SNTP、DHCP
画面解像度: PC グラフィック モード SUN® ビデオ モード	720x400 (DOS) 640 X 480 @ 60/72/75/85Hz、 800 X 600 @ 56/60/72/75/85Hz、 1024 X 768 @ 60/70/75/85Hz、 1152 X 864 @ 60/75Hz、 1280 X 1024 @ 60Hz、 1600 X 1200 @ 60Hz
認定:	UL/CUL、FCC Class A、CB、CE Class A、VCCI Class A

コネクタ

インタフェース タイプ	長さ (インチ、cm)	説明
ビデオ	15″、38 cm	統合ケーブル
PS/2	15″、38 cm	統合ケーブル
ミニ USB - USB(M)	17.7″、45 cm	USB 用ケーブル
ミニ Din9(M) - DB9(F)	72″、182 cm	シリアル用ケーブル
DKX2-101-LPKVMC	3.9"、10 cm	ローカル ポート統合用ケーブル
DKX2-101-SPDUC	70.86"、180 cm	Dominion PX への接続用ケーブル

Raritan Remote Client ソフトウェア

オペレーティング システムの要件: Windows XP / NT / ME / 2000

B ラック マウント

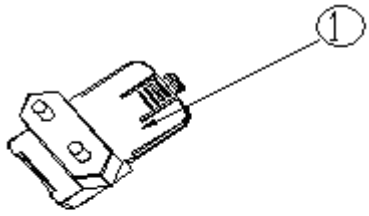
KX II-101 ユニットは、サーバ ラックのいずれの側にも縦または横、前向きまたは後ろ向きに取り付けることができます。 KX II-101 キットに付属のブラケットとネジを使用します。

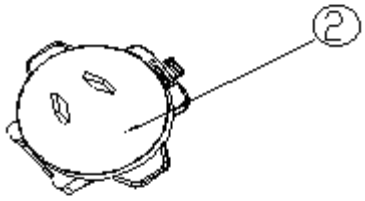
この章の内容

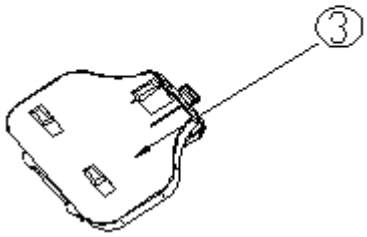
AC-DC アダプタ クリップ取り付け具

クリップ タイプの識別

1. EU クリップ
2. オーストラリア クリップ
3. UK クリップ

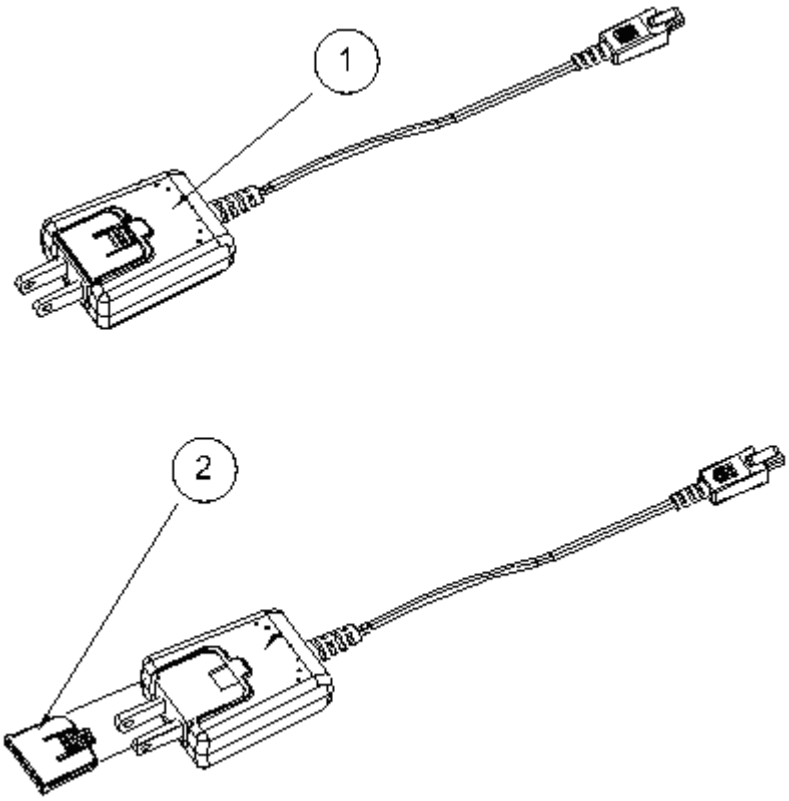






AC-DC 電源アダプタからのアタッチメント カバーの取り外し

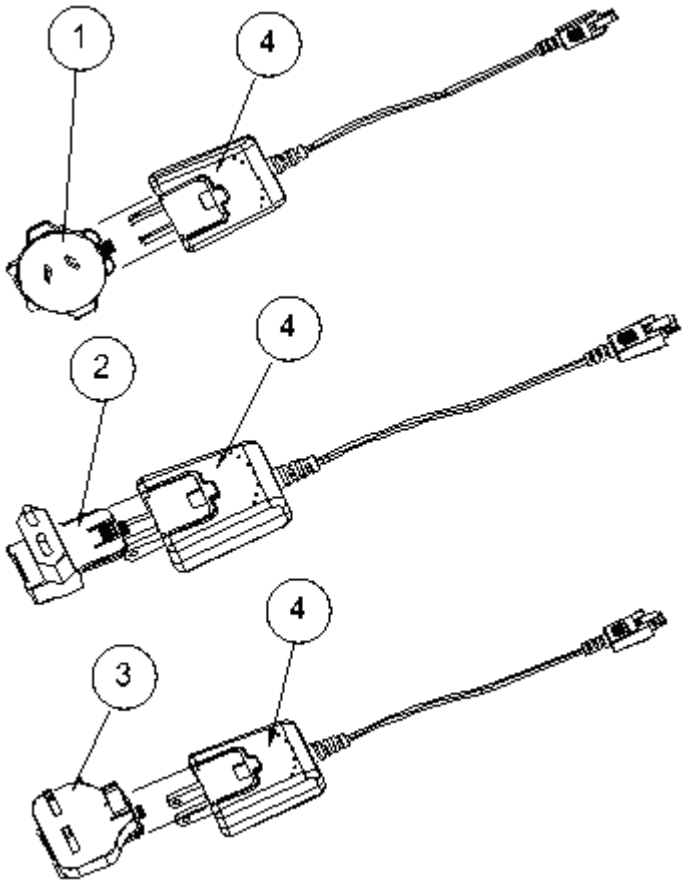
1. AC/DC 電源アダプタ
2. アタッチメント カバー。 押して取り外します。



AC-DC 電源アダプタへのクリップの取り付け

1. オーストラリア クリップ
2. EU クリップ
3. UK クリップ

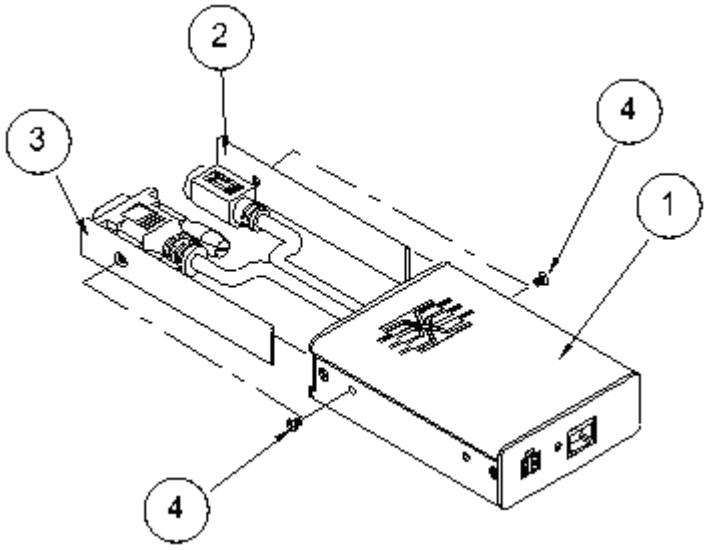
4. 電源アダプタ



ブラケットの取り付け

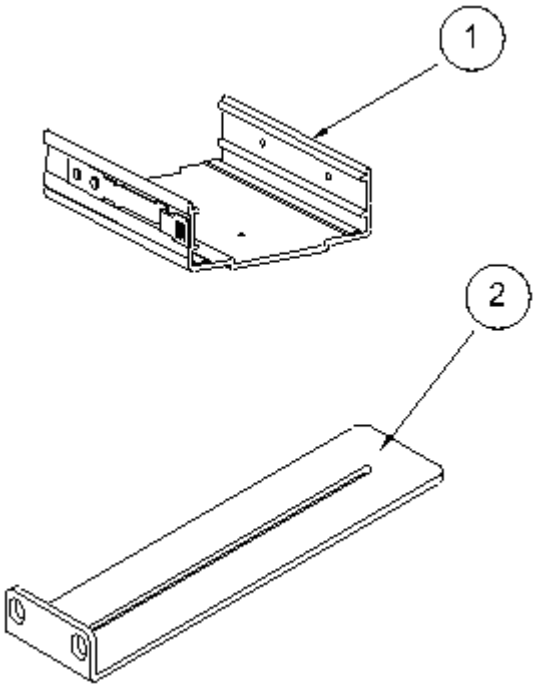
1. KX II-101 ユニット
2. 右パネル
3. 左パネル
4. ネジ

- KX II-101 ユニットからネジを取り外します。
- KX II-101 ユニットの左パネルおよび右パネルをスライドさせて外します。



KX II-101 ブラケット部品

1. U ブラケット
2. L ブラケット

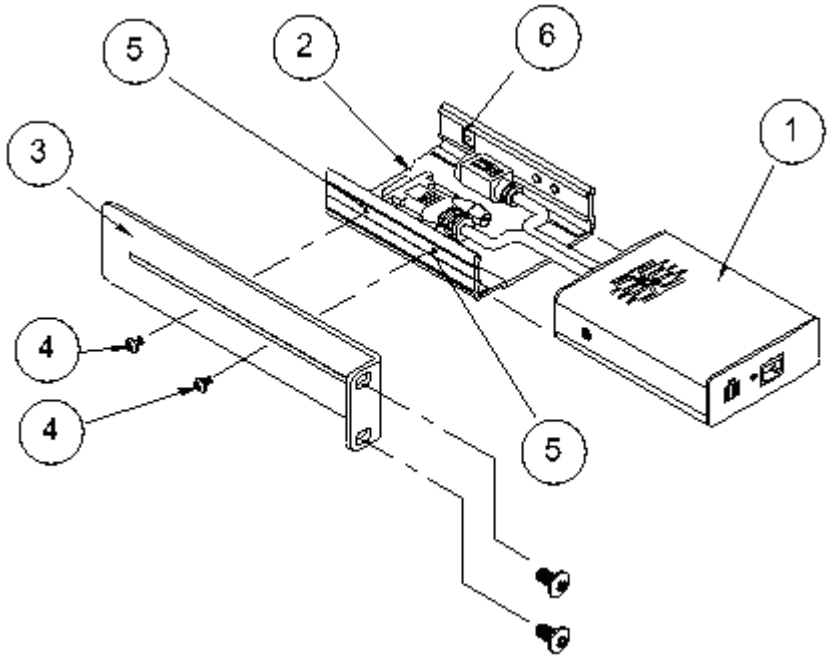


横に取り付ける KX II-101 にブラケットを取り付けます

1. KX II-101 ユニット
2. U ブラケット
3. L ブラケット
4. ネジ
5. 取り付け穴
6. ラッチ レバー

- 付属のネジを使用して U ブラケットを L ブラケットに取り付けます。 ネジを締め付ける前にブラケットの位置を調整します。
- ラック取り付けネジ (ラック メーカー提供品) を使用して U ブラケットと L ブラケットのアセンブリをラックに取り付けます。
- KVM ハーネスをターゲット側に向けて、KX II-101 ユニットを U ブラケット内にスライドさせます。 ラッチ レバーを引っ張って解放し、KX II-101 ユニットを U ブラケットに固定します。.

下の図は、KX II-101 を左側に取り付けています。 KX II-101 を右側に取り付けるには、ブラケットを KX II-101 ユニットの右側に取り付けることを除き、上記の指示に従います。



縦に取り付ける KX II-101 にブラケットを取り付けます

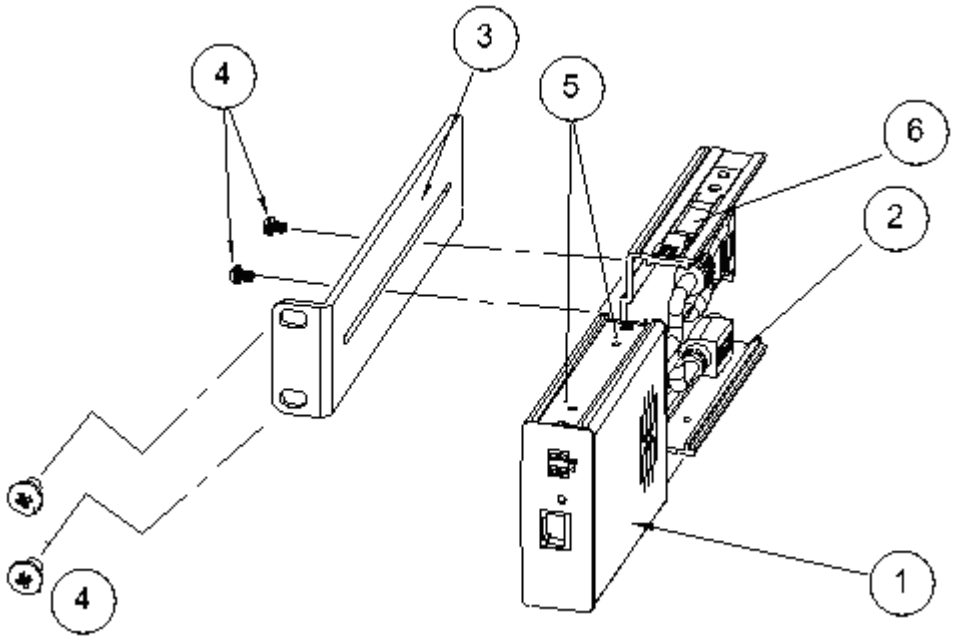
1. KX II-101 ユニット

2. U ブラケット
3. L ブラケット
4. ネジ
5. 取り付け穴
6. ラッチ レバー

付属のネジを使用して U ブラケットを L ブラケットに取り付けます。 ネジを締め付ける前にブラケットの位置を調整します。

ラック取り付けネジ (ラック メーカー提供品) を使用して U ブラケットと L ブラケットのアセンブリをラックに取り付けます。

KVM ハーネスをターゲット側に向けて、KX II-101 ユニットを U ブラケット内にスライドさせます。 ラッチ レバーを引っ張って解放し、KX II-101 ユニットを U ブラケットに固定します。



索引

A

C

D

I

J

K

L

M

P

R

S

U

V

W

あ

か

さ

た

な

は

ま

や

ら

漢字

➢ *米国/カナダ/ラテン アメリカ*

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 : 800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ : 6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ : 6 を押してから 2 を押してください。
Fax : 732-764-8887
CommandCenter NOC に関する電子メール : tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール : tech@raritan.com

➢ *中国*

北京
月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 : +86-10-88091890

上海
月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 : +86-21-5425-2499

広州
月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 : +86-20-8755-5561

➢ *インド*

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 : +91-124-410-7881

➢ *日本*

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : +81-3-3523-5994
電子メール : support.japan@raritan.com

➢ *ヨーロッパ*

ヨーロッパ
月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 : +31-10-2844040
電子メール : tech.europe@raritan.com

英国
月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 : +44-20-7614-77-00
フランス
月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 : +33-1-47-56-20-39

ドイツ
月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 : +49-20-17-47-98-0

➢ *韓国*

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 : +82-2-5578730

➢ *メルボルン (オーストラリア)*

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 : +61-3-9866-6887

➢ *台湾*

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 : +886-2-8919-1333
電子メール : tech.rap@raritan.com