

Dominion KX IV-101

取扱説明書

リリース 4.1.0

この資料には、著作権で保護されている専有情報が含まれています。全著作権所。 Raritan Inc. の書面による事前の明示的な同意なしに、本書のいかなる部分もコピー、複製、または他の言語に翻訳することはできません。

著作権 © 2020 Raritan, Inc.

KX4101-0C-v4.1.0-E

11月 2020

255-62-0023-00

©著作権 2020 Raritan, Inc. このドキュメントに記載されている、全てのサードパーティのソフトウェアとハードウェアは、それぞれの所有者の登録商標または商標であり、所有者です。

FCC(Federal Communication Commission) 情報

この機器はテスト済みであり、FCC 規則のパート 15 に準拠したクラス A デジタルデバイスの制限に準拠していることが確認済みです。これらの制限は、商用設備での有害な干渉に対する合理的な保護を提供するように設計されています。

この機器は、無線周波数エネルギーを生成、使用、及び放射する可能性があり、指示に従って設置及び使用しない場合、無線通信に有害な干渉を引き起こす可能性があります。住宅環境でこの機器を操作すると、有害な干渉を引き起こす可能性があります。

VCCI 情報 (日本)

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

Raritan は、事故、災害、誤用、乱用、製品の Raritan 以外の変更、または Raritan の合理的な制御の及ばない、または通常の動作条件下で発生しないその他のイベントに起因する、この製品の損傷について一切責任を負いません。

この製品に電源ケーブルが含まれている場合は、この製品専用で使用する必要があります。



KXIV-101 リリース 4.1.0 の新機能

- DVI、HDMI カスタム EDID、ローカルポートモニターEDID、及び新しいオーディオ設定をサポート：
 - ポート構成：KVM ポート設定（全般、ビデオ、オーディオ）（10 ページを参照）
 - **ポート構成：カスタム EDID**（18 ページ 18 ページを参照）
 - **ポート構成：ローカルポートモニターEDID**（19 ページを参照）
- DSAM のサポート：Dominion シリアル・アクセス・モジュールを使用したシリアルアクセス（21 ページを参照）
- 仮想メディア画像ファイルにアクセスする為の、新しいオプション：**仮想メディア画像ファイルにアクセスする**（64 ページを参照）
- 端子台制御用の新しいパルスオプション：**端子台の制御**（143 ページを参照）
- デバイス検出の暗号化オプション：**デバイス検出**（138 ページを参照）
- HTTP の無効設定用の新しいオプション：**HTTP/HTTPS ポート**（138 ページを参照）
- TLS1.3 のサポート：**TLS 証明書**（155 ページを参照）
- iOS で HKC を使用する為のドキュメントを更新：**Apple iOS デバイスでの HKC 使用**（98 ページを参照）
- **デュアルモニターセットアップで Dominion KX IV-101 にアクセスするための方法**（106 ページを参照）

このバージョンの Dominion KX IV-101 に適用される変更の詳細につきましては、リリースノートをご参照してください。

コンテンツ

KXIV-101 リリース 4.1.0 の新機能	iii
--------------------------	-----

CHAPTER 1 インストールと初期構成	1
-----------------------	---

サポートされているブラウザ	1
クライアントとシステムの最小推奨事項	1
パッケージの内容	2
正面図	2
背面図	3
機器の接続	4
初期設定	5
オプション 1: PC を LAN ポートに接続	5
オプション 2: ローカルポートに iOS デバイスを接続	5
オプション 3: シリアル構成	6
次のステップ	6
KVM クライアントオプション	7

CHAPTER 2 ポートへのアクセスと構成	9
------------------------	---

ポートアクセス	9
ポート構成: KVM ポート設定 一般, ビデオ, オーディオ	10
サポートされている優先ビデオ解像度	12
ポート構成: カスタム EDID	18
ポート構成: ローカルポートモニター EDID	19
ポート構成: USB 接続設定	19

CHAPTER 3 Dominion シリアルアクセスモジュールを使用したシリアルアクセス	21
---	----

DSAM 接続	22
DSAM LED の動作	22
DSAM シリアルポートの表示	23
DSAM シリアルポートの構成	24
シリアルポートキーワードリストの設定	26
DSAM ファームウェアのアップデート	28
サポートされている CLI コマンド	28
サポートされているエスケープキー文字	30

Web インターフェイスで DSAM シリアルターゲットに接続.....	30
URL ダイレクトポートアクセスで DSAM シリアルターゲットに接続	31
SSH 経由で DSAM シリアルターゲットに接続	31
HTML シリアルコンソール (HSC) のヘルプ	32
HSC 機能.....	32
HSC のブラウザのコツ	39
チャプター4 KVM クライアント	40
<hr/>	
仮想 KVM クライアント(VKCS)のヘルプ	40
Java 要件.....	41
プロキシサーバーの構成	43
接続プロパティ.....	44
接続情報	46
キーボード.....	46
ビデオ.....	50
マウスオプション	50
ツールオプション	54
オプションの表示	62
仮想メディア	63
デジタルオーディオ	66
外部機器	70
バージョン情報 - 仮想 KVM クライアント	71
アクティブ KVM クライアント (AKC) のヘルプ	71
概要	72
AKC がサポートする Microsoft.NET Framework	72
AKC がサポートするブラウザ.....	72
AKC がサポートする OS.....	72
AKC を使用する為の前提条件.....	72
プロキシサーバーの構成	73
HTML KVM クライアント (HKC)	74
接続プロパティ.....	75
接続情報	77
入力メニュー	78
ビデオメニュー.....	89
ビューメニューについて	90
ツールメニュー.....	90
仮想メディアメニュー	92
オーディオメニュー	95
外部デバイスのメニュー	97
Apple iOS デバイスでの HKC を使用	98

デュアルモニターセットアップで Dominion KX IV-101 にアクセスする為のコツ 106

CHAPTER 5 ユーザー管理 107

LDAP / Radius 情報の収集 108

認証の構成 108

 LDAP 認証 110

 Active Directory サーバーからユーザーグループ情報を返す 112

 RADIUS 認証 113

 RADIUS 経由でユーザーグループ情報を返す 114

外部認証の無効化 114

パスワード変更 114

接続ユーザー 114

ユーザーとグループ 115

 管理者グループの特別な特権 123

CHAPTER 6 デバイスの設定と情報 124

デバイス情報 124

日付と時間 127

イベント管理 128

 E メール送信 130

 SNMP 通知 130

 Syslog メッセージ 134

キーコードリスト 135

ネットワーク 136

ネットワークサービス 138

 ディスカバリーポート 139

 HTTP/HTTPS ポート 139

 SMTP サーバー設定 140

 SNMP 設定 141

 SSH 設定 142

シリアルポート 143

端子台の制御 144

 端子台をマザーボードに接続する 146

仮想メディア共有イメージ 147

CHAPTER 7 セキュリティ 148

グループベースのアクセス制御 148

IP アクセス制御 149

KVM セキュリティ 151

 直接ポートアクセス URL 152

ログインログイン設定.....	153
パスワードポリシー.....	154
TLS 証明書.....	155
役務契約.....	159
チャプター8 メンテナンス	160
バックアップと復元.....	160
イベントログ.....	162
ファームウェア履歴.....	163
ユニットのリセット.....	163
ファームウェアの更新.....	164
チャプター9 仮想メディア	167
概要.....	167
仮想メディアのパフォーマンスに関する推奨事項.....	168
メディアを使用するための前提条件.....	168
Dominion KX IV-101 仮想メディアの前提条件.....	168
クライアント PC VM の前提条件.....	168
ターゲットサーバーVM の前提条件.....	168
ローカルドライブの取り付け.....	169
仮想メディアを介してサポートされるタスク.....	169
サポートされている仮想メディアタイプ.....	169
読み取り/書き込みが利用できない場合の条件.....	170
サポートされている仮想メディアドライブ数.....	170
Linux 環境での仮想メディア.....	170
アクティブなシステムパーティション.....	170
マップされたドライブ.....	170
ドライブパーティション.....	170
ルートユーザーのアクセス許可の要件.....	171
ドライブのアクセス許可の接続 (Linux).....	171
Mac 環境での仮想メディア.....	171
アクティブシステムパーティション.....	171
ドライブパーティション.....	171
ドライブのアクセス許可を接続する (Mac).....	172

コンテンツ

仮想メディアファイルサーバーのセットアップ（ファイルサーバーISO イメージのみ） 172

CHAPTER 10 診断 173

診断のダウンロード..... 173
ネットワーク診断 174

CHAPTER 11 CLI コマンド 176

CLI: check 176
CLI: clear 176
CLI: config 177
 CLI: config authentication 178
 CLI: config device 181
 CLI: config group 182
 CLI: config keyword 183
 CLI: config network 184
 CLI: config password 186
 CLI: config port 186
 CLI: config security 187
 CLI: config serial 189
 CLI: config terminalblock 189
 CLI: config time 189
 CLI: config user 190
CLI: connect 192
CLI: diag 193
CLI: reset 194
CLI: show 195
CLI: exit 201

付録 A 仕様 202

使用される TCP と UDP ポート 203

インデックス 205

チャプター1 インストールと初期構成

内容

サポートされているブラウザ	1
クライアントとシステムの最小推奨事項	1
パッケージの内容	2
正面図	2
背面図	3
機器の接続	3
初期構成	4
オプション 1: PC を LAN ポートへ接続	5
オプション 2: ローカルポートで iOS デバイスを接続	5
オプション 3: シリアル構成	5
次のステップ	6
KVM クライアントのオプション	6

サポートされているブラウザ

- Chrome
- Edge
- Firefox
- Safari
- Internet Explorer

バージョンとの互換性の詳細については、リリースノートをご参照下さい。

クライアントとシステムの最小推奨事項

クライアントの最小要件は、使用するクライアント、及びストリーミングする予定のビデオの種類によって多少異なります。

- ▶ **ネットワーク速度の推奨事項:**
 - ギガビットイーサネットや WiFi802.11ac 等の高速ネットワーク
- ▶ **スタンドアロン仮想 KVM クライアント (VKCS) とアクティブ KVM クライアント (AKC)**
 - CPU:

- フルHD ビデオの場合: Intel Core i3 4xxx 以降などの最新の高速デュアルコア CPU、またはクアッドコア CPU。複数の KVM セッションを実行する場合は、クアッドコア CPU をお勧めします。
- 4K ビデオの場合: Intel Core i54xxx 以降などの最新の高速クアッドコア CPU。複数の 4K ストリームを実行する場合は、Intel Core i5 / i7 8xxx など、6 コア以上の CPU をお勧めします。
- 8GB RAM
- グラフィックカード: GeForce や Radeon などの最新の OpenGL 対応グラフィックカード。少なくとも 1GB。

▶ HTML KVM クライアント (HKC):

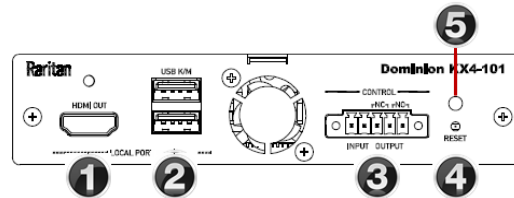
HKC では 4K ビデオは推奨されておりません。

- CPU: 最新の高速デュアルコア CPU
- 8GB RAM
- OpenGL 対応のグラフィックカード

パッケージの内容

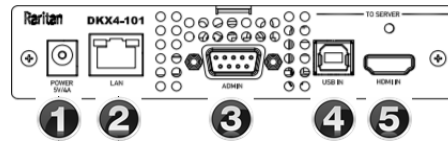
- 1 x Dominion KX IV-101
- 1 x 電源コード
- 1 x HDMI ケーブル
- 1 x USB-B to USB-A ケーブル
- 1 x 取付ブラケットキット

正面図



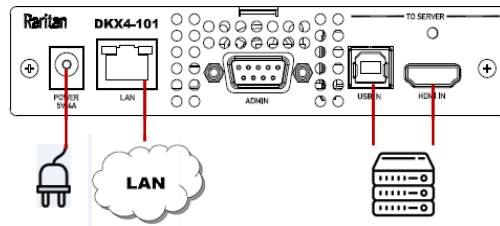
- ① ローカル HDMI 出力ポートから
モニターのローカルポート
- ② ローカルポート USB K/M:
 - ローカルポートのキーボード/マウスに使用するか、
 - 1つまたは2つの DSAM ユニートを接続。
- ③ 入出力
- ④ リセット
- ⑤ 電源ステータス LED:
 - オン (緑色): 電源オン
 - 緑色の点滅: リモートターゲット接続

背面図



- ① 電源アダプターからの電力 (5V / 4A) 供給
- ② ネットワーク速度とアクティビティ用の 2 つの LED を備えた RJ-45 LAN ネットワークポート:
 - 琥珀 OFF/緑 OFF: 非アクティブリンク
 - 琥珀 ON/緑 OFF: 1000 MBps リンク/アクティビティなし
 - 琥珀 点滅/緑 OFF: 1000 MBps リンク/アクティビティ (RX, TX)
 - 琥珀 OFF /緑 ON: 100 MBps リンク/アクティビティなし
 - 琥珀 OFF/緑 点滅: 100 MBps リンク/アクティビティ (RX, TX)
 - 琥珀 ON /緑 ON: 10 MBps リンク/アクティビティなし
 - 琥珀 点滅/緑 点滅: 10 MBps リンク/アクティビティ (RX, TX)
- ③ シリアル管理ポート
- ④ ターゲットサーバーからの USB 入力
- ⑤ ターゲットサーバーからの HDMI 入力

機器の接続



▶ **Dominion KX IV-101 をネットワークへ接続:**

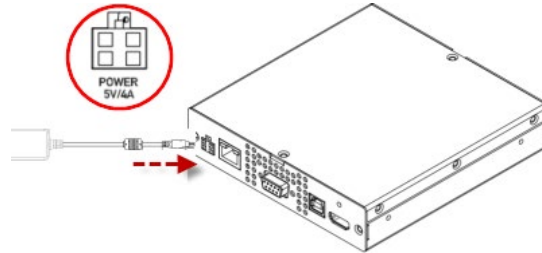
- LAN ポートを使用して、Dominion KX IV-101 をネットワークへ接続。

▶ **ターゲットサーバーを接続:**

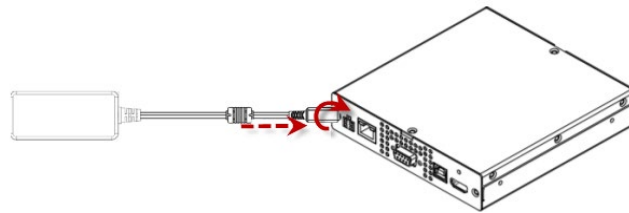
- ターゲットサーバーを HDMI ケーブルで Dominion KX IV101 HDMI IN ポートに接続。ターゲットサーバーのビデオが HDMI でない場合、Raritan ケーブル、またはビデオアダプターをご購入ください。
- 付属の USB ケーブルを使い、ターゲットサーバーを Dominion KX IV-101 USB IN ポートに接続。

▶ **電源アダプタを接続:**

- 新しいモデルには、4 ピンコネクタ付きの電源アダプターが含まれています。アダプターを押し込んでロックします。



- 下の図に示すように、元のモデルの一部にはツイストロック式アダプターが含まれています。これらは矢印でマークされています。矢印を上に向けて接続します。しっかりと押し込み、時計回りにひねってロックします。最後にロックされていることをご確認ください。

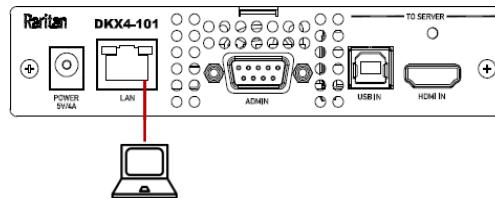


全てのデバイスの電源を入れます。

初期設定

デフォルトのログイン：
admin/raritan

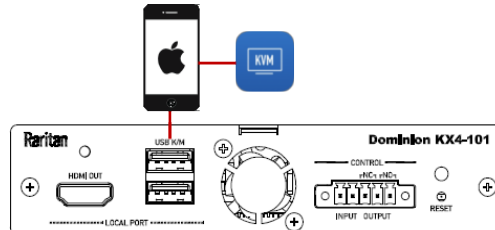
オプション1: PCをLANポートに接続



- PCのワイヤレスインターフェイスを無効にし、PCがDHCPに設定されていることを確認。ネットワークケーブルを、PCとDominion KX IV-101のLANポート間で接続します。
- ブラウザを開きます。右記のURLを入力“https://kvm.local”。
- ログインページが出てきます。
- プロンプトに従って、デフォルトのパスワードを変更して下さい。

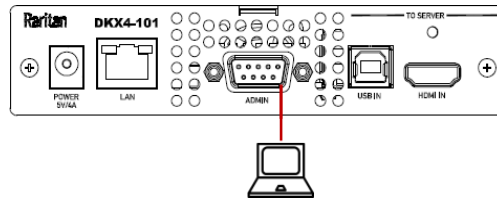
オプション2: ローカルポートにiOSデバイスを接続

必要なアプリ: Raritan 提供の「Raritan KVM」:
<https://itunes.apple.com/us/app/raritan-kvm/id1455817539?mt=8>



- iOSデバイスでRaritan KVMアプリを起動。
- Raritan KVMアプリを搭載したiOSデバイスをDominion KX IV-101のUSBポートに接続。
- アプリが接続されたDominion IV-101を検出するまで待ちます。
- プロンプトに従って、デフォルトのパスワードを変更して下さい。

オプション 3: シリアル構成



- PC と Dominion KX IV-101 シリアル管理ポートの間に、DB9 シリアルケーブルまたは USB-シリアルアダプタを接続。
- シリアルコンソール構成: (デフォルト) 115200bps / None / 8bits / 1stop
- デフォルトの DHCP IP アドレスの確認方法: 「show」コマンドを使用して「show network」を実行。
- 全てのコマンドについては、CLI コマンドをご参照ください。 (エラー! ブックマークが定義されていません。 ページを参照)

次のステップ

- ネットワーク設定の構成: [ネットワークを参照](#) (136 ページ)
- 時間設定の構成: [日時を参照](#) (127 ページ)
- 証明書のインストール: [TLS 証明書を参照](#) (155 ページ)
- ユーザーの構成: [ユーザー管理を参照](#) (107 ページ)
- ポート設定の構成: [ポート構成: KVM ポート設定 \(一般、ビデオ、オーディオ\)](#) (9 ページ)

KVM クライアントオプション

Dominion KX IV-101 は、様々な KVM クライアントを提供します。 サポートされているブラウザにて、Dominion KX IV-101 の IP アドレスを起動すると、ログインページが表示されます。HTML KVM クライアント (HKC) がデフォルトです。

- ログインページの [もっと詳しく] リンクをクリックすると、他の KVM クライアントオプションが表示されます。



- [もっと詳しく] リンクをクリックすると、クライアントオプションダイアログが起動。表示されたリンクをクリックすると、別のクライアントが起動されます。
 - https://<IP address> launches HKC
 - https://<IP address>/akc launches AKC
 - https://<IP address>/vkcs launches VKC

KX4-101 Client Options		
Three different clients are available to launch KVM sessions or administer your device, each with its own benefits. Note that you must log into each client separately.		
Client Name	How to Launch	Notes
HTML KVM Client (HKC)	On any browser, including mobile, go to https://192.168.56.27	This is what you're running now. Quickest and easiest to log into, but video performance and virtual media functionality are limited.
Active KVM Client (AKC)	On Windows, using Microsoft Edge™ Internet Explorer™ 11, or another browser with ClickOnce plug-in, go to https://192.168.56.27/akc	Recommended high-performance client for Windows. AKC will load and launch automatically when the link is clicked.
Virtual KVM Client Standalone (VKCS)	On any system with Java 1.8, go to https://192.168.56.27/vkcs	Recommended high-performance client for Mac and Linux. After clicking link, VKCS will download. If browser does not do it automatically, click the downloaded .jnlp file (or ctrl-click on Mac) to launch.

別のクライアントが選択されると、Dominion KX IV-101 はシステムを自動的チェックにて、クライアントの要件を満たしているか確認します。システムの準備が出来ている場合は、選択したクライアントがロードされます。システムが追加の要件を満たす必要がある場合は、別のメッセージが表示されます。

注意: AKC および VKCS の場合、有効な証明書をインストールするまで、ブラウザに「このサイトは安全ではありません」という警告メッセージが表示される場合があります。クリックして警告を受け入れると、サイトにアクセス可能。これらの警告メッセージを防ぐ証明書のインストールについては、TLS 証明書を参照して下さい。(155 ページ)

全てのクライアントを使用する為の詳細と手順については、KVM クライアントを参照してください(40 ページ)。

CHAPTER 2 ポートへのアクセスと構成

内容

ポートアクセス	9
ポート構成: KVM ポート設定 一般, ビデオ, オーディオ.....	9
ポート構成: カスタム EDID.....	18
ポート構成: ローカルポートモニターEDID	18
ポート構成: USB 接続設定.....	19

ポートアクセス

[Port Access]をクリックして、ポートプレビューを表示し、ターゲットに接続します。

▶ **ポートプレビュー:**

- プレビュー画像は5秒ごとに更新されます。
- プレビューを表示できるかどうかは、権限によって異なります。十分な権限がない場合は、詳細メッセージが表示されます。



▶ **ターゲットに接続:**

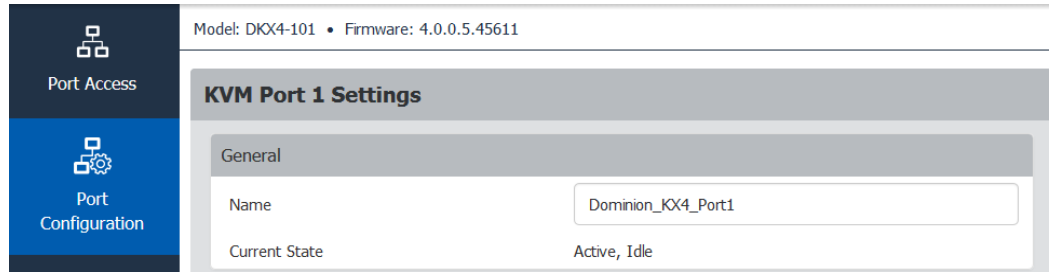
- [Connect]ボタンをクリックして、ターゲットサーバーへの接続。
- KVM クライアントの使用に関するヘルプについては、「KVM クライアント(40 ページ)」を参照してください。

ポート構成: KVM ポート設定 一般, ビデオ, オーディオ

[Port Configuration] ページには、KVM ポート名、ビデオ解像度のすべてのポート設定および USB ポートとオーディオ設定が含まれています。

▶ 全てのポート構成へのアクセス:

- [Port Configuration] をクリック



▶ KVM ポート設定:

一般設定:

- KVM ポートの名前変更: 新しい名前を入力して[保存]をクリック。
- 現在のポートステータスの表示:
 - Active, Idle : 稼働していない。
 - Active, Busy: 接続されていますが、PC 共有が無効状態。
 - 詳しくは **KVM セキュリティを参照して下さい**。(152 ページ)
 - Active, Connected : 接続済みで、PC 共有が有効状態。

ビデオ設定:

- ビデオ入力が HDMI アダプターを介して、VGA またはその他のアナログソースから発信されている場合、[Enable VGA Mode]を選択して下さい。VGA モードでは、解像度はビデオソースデバイスでのみ制御されます。
- 優先ビデオ解像度を選択します:重要! KX IV は、「EDID」データ構造を使用して、必要なビデオ解像度をターゲットサーバーに通知します。ターゲットサーバーのビデオ解像度を変更するには、[Preferred Video Resolution] を新しい解像度に変更します。ターゲットに接続時に解像度が変わります。そうでない場合は、ターゲットサーバーの解像度を変更することも可能。
 - サポートされている全ての解像度のリストについては、「サポートされている優先ビデオ解像度 (12 ページ)」を参照して下さい。
 - ロードする特定の EDID がある場合、「ポート構成: カスタム EDID (18 ページ)」を参照して下さい。

- ビデオインターフェイスを HDMI または DVI（オーディオなし）に設定します。
- ターゲットビデオが優先ビデオ解像度の変更に適切に応答しない場合は、より長いサイクルタイムを設定します。初期値は 200ms です。サイクルタイムが長くなると、ターゲットが新しい優先ビデオ解像度に、正確に応答できるようになる場合があります。
- [Enable Video Throttle] を選択して、クライアントのフレームレートを着信ビデオの半分のフレームレートに制限します。これは、クライアントのネットワーク帯域幅と CPU 負荷を減らすのに役立ちます。

Video Settings

Enable VGA Mode when the video input originates with a VGA or other analog source, through an HDMI adapter. In VGA mode, resolution is controlled on the video source device only.

Enable VGA Mode

Use these settings if necessary to help force digital video sources to desired screen resolution. Try a longer cycle time value if target does not respond properly.

Video Interface HDMI ▲▼

Preferred Video Resolution 1920x1080 @ 60Hz ▲▼

Cycle Time 200 ms ▲▼

Enable Video Throttle to cap the client frame rate at 1/2 that of the incoming video. This can be useful to reduce network bandwidth and/or CPU load on the client.

Enable Video Throttle

オーディオ設定

- 音声がなかった場合は、[Audio Compensation] を選択して有効にします。この機能を無効設定後、Dominion KX IV-101 を再起動して、別のターゲットコンピューターへの新しいオーディオ接続を許可する必要があります。

Audio Settings

If there is no audio, please enable Audio Compensation. Please reboot this KX4-101 switch if you disable this setting to connect the KX4-101 to another target computer.

Audio Compensation

- [Save] をクリックして、すべての設定を適用します。

サポートされている優先ビデオ解像度

されている各 EDID は、提供できる推奨ビデオ解像度とともに一覧表示されます。サーバーは通常、サポートできる最大の解像度とリフレッシュレートを選択します。

1024x768@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz

▶ 1152x864@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz

▶ 1280x720@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x720@60Hz

▶ 1280x960@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz

▶ 1280x1024@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz
- 1280x1024@60Hz, @75Hz

▶ 1360x768@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz
- 1360x768@60Hz

▶ 1440x900@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x960@60Hz
- 1280x1024@60Hz
- 1440x900@60Hz

▶ 1400x1050@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1400x1050@60Hz
-

▶ 1600x900@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz, @85Hz
- 1600x900@60Hz

▶ 1600x1200@60Hz

- 640x480@60Hz, @72Hz, @75Hz, @85Hz

- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz, @85Hz
- 1024x768@60Hz, @70Hz, @75Hz, @85Hz
- 1152x864@60Hz, @75Hz, @85Hz
- 1280x1024@75Hz
- 1600x1200@60Hz

▶ 1680x1050@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@60Hz, @75Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1680x1050@60Hz

▶ 1920x1080@60Hz (148.5MHz クロック)

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz

▶ 1920x1200@60Hz (Reduced Blanking 154MHz クロック)

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz

- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz

▶ 1920x2160@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x2160@60Hz

▶ 2560x1440@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz
- 2560x1440@60Hz

▶ 2560x1600@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz
- 2560x1600@60Hz

▶ 3840x1080@60Hz

- 640x480@60Hz, @72Hz, @75Hz
- 720x400@70Hz
- 720x480@60Hz
- 720x576@50Hz
- 800x600@56Hz, @60Hz, @72Hz, @75Hz
- 1024x768@60Hz, @70Hz, @75Hz
- 1152x864@75Hz
- 1280x720@50Hz, @60Hz
- 1280x800@60Hz
- 1280x1024@60Hz, @75Hz
- 1440x900@60Hz
- 1600x900@60Hz
- 1680x720@60Hz
- 1680x1050@60Hz
- 1920x1080@24Hz, @30Hz, @60Hz
- 1920x1200@60Hz
- 2560x1080@30Hz, @60Hz
- 2560x1440@60Hz

- 2560x1600@60Hz
- 3840x1080@60Hz

- ▶ **3840x1600@30Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 720x480@60Hz
 - 720x576@50Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@75Hz
 - 1280x720@60Hz
 - 1280x800@60Hz
 - 1280x1024@60Hz, @75Hz
 - 1440x900@60Hz
 - 1600x900@60Hz
 - 1680x1050@60Hz
 - 1920x1080@60Hz
 - 1920x1200@60Hz
 - 2560x1080@60Hz
 - 2560x1440@60Hz
 - 3840x1600@30Hz

- ▶ **3840x2160@30Hz**
 - 640x480@60Hz, @72Hz, @75Hz
 - 720x400@70Hz
 - 720x480@60Hz
 - 720x576@50Hz
 - 800x600@56Hz, @60Hz, @72Hz, @75Hz
 - 1024x768@60Hz, @70Hz, @75Hz
 - 1152x864@75Hz
 - 1280x720@50Hz, @60Hz
 - 1280x800@60Hz
 - 1280x1024@60Hz, @75Hz
 - 1440x900@60Hz
 - 1600x900@60Hz
 - 1680x720@60Hz
 - 1680x1050@60Hz
 - 1920x1080@24Hz, @30Hz, @60Hz
 - 1920x1200@60Hz

- 2560x1080@60Hz
- 2560x1440@60Hz
- 2560x1600@60Hz
- 3440x1440@50Hz
- 3840x2160@24Hz, @25Hz, @30Hz
- 4096x2160@30Hz

ポート構成：カスタム EDID

カスタム EDID をロードして、Dominion KX IV-101 が新しい、または異なるビデオ解像度をサポートできるようにしたり、標準でサポートされている解像度のカスタムバージョンを指定したり出来ます。追加できるカスタム EDID は、解像度ごとに1つのみ。ファイルの拡張子は「.rfp」で、要求に応じてベンダーから提供されます。

最大 20 個のカスタム EDID と、最大 10 個のカスタム HDMI EDID 及び、10 個のカスタム DVI EDID をアップロードできます。カスタム EDID はバックアップに含まれていません。

▶ カスタム EDID のアップロード方法:

1. [Port Configuration] をクリックし、[Custom EDIDs] までスクロールで下へ行きます。
2. [Browse...] をクリックして、. rfp EDID ファイルを見つけて選択します。
3. [Upload] をクリックします。これらの手順を繰り返して、ファイルを追加。
4. がアップロードされると、解像度でソートされたリストに表示されます。
 - 詳細を表示するには、[Show description] をクリックします。
 - ファイルを削除するには、[削除]アイコンをクリック。

Custom EDIDs
▲

📌 Custom EDIDs extend the capabilities of the KX4 to support new or different video resolutions. The files have a ".rfp" extension and are provided by vendor on request.

Resolution ▲	
800x600 @ 60Hz	Show Description 🗑️
1024x768 @ 70Hz	Show Description 🗑️

ポート構成：ローカルポートモニターEDID

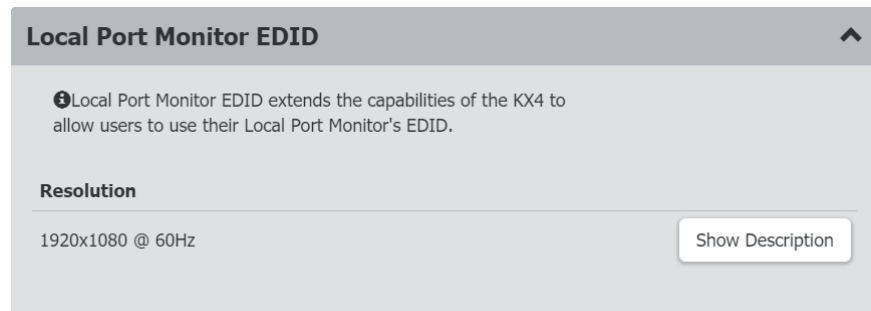
ローカルポートのモニターが Dominion KX IV-101 に接続されている場合、[Port Configuration] ページに [Local Port Monitor EDID] セクションが表示され、そのモニターの EDID が [優先ビデオ解像度] に含まれます。ローカルポートモニターの EDID は、優先ビデオ解像度として選択することで使用できます。

EDID が優先ビデオ解像度として使用されているときにローカルポートモニターを外すと、優先ビデオ解像度はデフォルトの 1920x1080 @ 60Hz 標準 EDID に戻ります。

新しいモニターが接続されると、古いローカルポートモニター EDID が上書きされます。

▶ ローカルポートモニターEDID の表示方法:

1. [Port Configuration] をクリックし、[Local Port Monitor EDID] まで下へ移動。
2. 現在接続されているローカルポートモニターの EDID が一覧表示されます。
 - 詳細を表示するには、[Show Description] をクリック。



ポート構成：USB 接続設定

ポート接続されている場合、USB 接続設定は無効になります。USB ポート設定を変更するには、KVM ターゲットから全てのユーザーが接続から離れなければなりません。

▶ ターゲットサーバーの USB 接続の設定:

- [Port Configuration] をクリックし、[USB Connection Settings] まで下へ移動。
- 使用する USB 接続設定を選択します:
 - ずれないマウスを有効 - ターゲットがずれないマウスモードをサポートしていない場合は、無効にします。
 - フルスピードの使用 - 高速 USB デバイスに対応できない BIOS に役立ちます。チェックボックスのレ点を削除すると、ターゲットの最高の USB 速度機能とのネゴシエーションが可能になります。
 - キーボードとマウスの前に、最初に仮想メディアを列挙します: ターゲットが BIOS で USB 大容量ストレージを検出できない場合、問題解決に役立ちます。

- [Save]をクリック。

USB Connection Settings

Basic

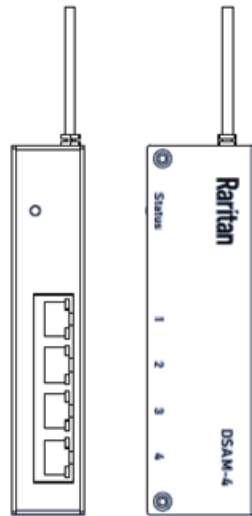
Enable Absolute Mouse	<input checked="" type="checkbox"/>
Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices	<input type="checkbox"/>
Enumerate virtual media first before keyboard and mouse	<input type="checkbox"/>

- 必要に応じて詳細オプションを設定します:
 - 仮想メディアインターフェイスのタイプ: 両方のインターフェイスを、「CDROM」または「リムーバブルディスク」に設定は出来ません。
 - 無効
 - CDROM
 - リムーバブルディスク
 - オート - CDROMまたはリムーバブルドライブのいずれかとして機能できますが、両方を同時に機能させることは出来ません。
 - 未使用の VM インターフェイスを、デバイス構成からの削除: VM が切断されたときにドライブを削除するには、このオプションを選択します。空のドライブを許可するには、このオプションをクリアします。
- [Save]をクリック。

Advanced

Virtual Media Interface #1 Type	CD-ROM
Remove Unused VM Interface #1 From Device Configuration	<input type="checkbox"/>
Virtual Media Interface #2 Type	Removable Disk
Remove Unused VM Interface #2 From Device Configuration	<input type="checkbox"/>

Chapter 3 Dominion シリアルアクセスモジュールを使用したシリアルアクセス



Dominion KX IV-101 と Dominion シリアルアクセスモジュール (DSAM) を接続すると、RS-232 シリアルポートを備えた LAN スイッチやルーター等のデバイスにアクセス可能。

DSAM は Dominion KX IV-101 から電力を得る、2 ポートまたは 4 ポートのシリアルモジュールです。

USB ケーブルを使用して、最大 2 つの DSAM モジュールを Dominion KX IV-101 に接続します。DSAM は 0U 構成でマウント出来ます。

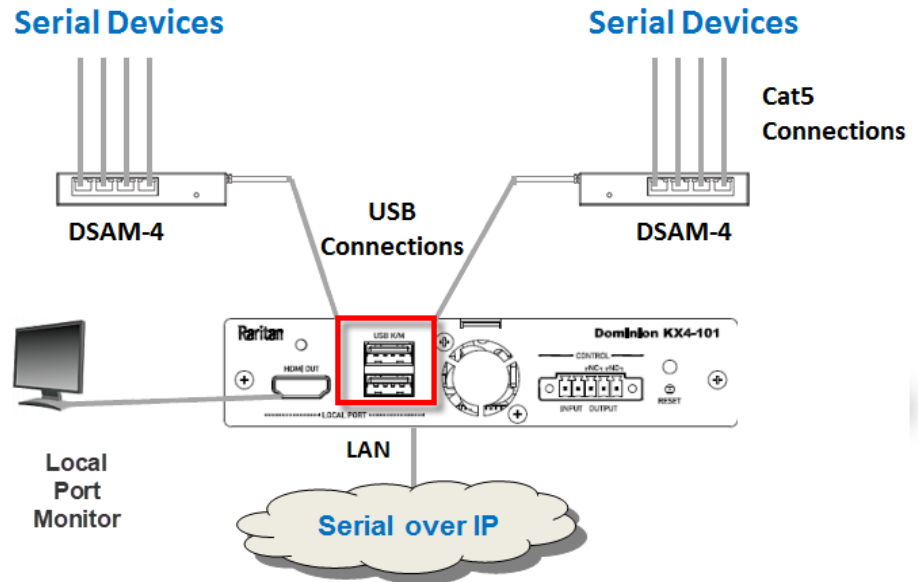
内容

DSAM を接続.....	21
DSAM シリアルポートの表示.....	23
DSAM シリアルポートの構成.....	23
シリアルポートキーワードリストの設定.....	26
DSAM ファームウェアのアップデート.....	27
サポートされている CLI コマンド.....	28
Web インターフェイスで DSAM シリアルターゲットに接続.....	30
URL ダイレクトポートアクセスで DSAM シリアルターゲットに接続.....	30
SSH 経由で DSAM シリアルターゲットに接続.....	31
HTML シリアルコンソール (HSC) のヘルプ.....	31

DSAM 接続

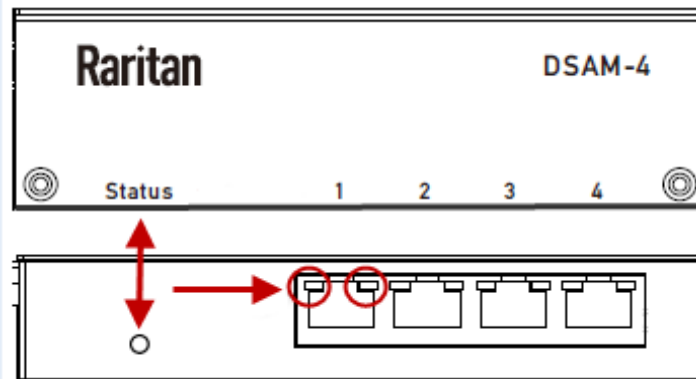
▶ DSAM を Dominion IV-101 への接続方法:

- DSAM ユニットの USB ケーブルを、Dominion IV-101 の前面にある USB K/M ポートのどちらかに接続します。
- シリアルデバイスを DSAM ユニットのシリアルポートに接続します。
- 2 台の DSAM ユニットが接続されている場合、ローカルキーボードとマウスは接続不可。
- DSAM ユニットが 1 つだけ接続されている場合は、キーボードとマウスを組み合わせ、開いている残りの USB K/M に接続出来ます。



DSAM LED の動作

DSAM ユニットには、ステータス用の 1 つの LED と、各ポートに 2 つの LED があります。



▶ ステータス LED:

ステータス LED はユニット前面にラベルが貼られています。ライトが後ろにあります。ステータス LED は、起動時とアップグレード時に情報表示します。

- グリーン LED - ゆっくり点滅: DSAM は起動しますが、Dominion KX IV-101 による制御不可。
- ブルーLED - ゆっくり点滅: Dominion KX IV-101 によって制御される DSAM。
- ブルーLED - 速い点滅: ファームウェアのアップグレードが進行中。

▶ USB ポート LED:

各 USB ポートには、左側の緑色の LED と右側の黄色の LED があります。

- グリーン LED: ポートは DCE として設定されています。
- イエローLED: ポートは DTE として設定されています。
- LED がオフ: ポートは AUTO に設定されています。

DSAM シリアルポートの表示

DSAM ユニットの Dominion KX IV-101 に接続すると、[DSAM Serial Ports] ページが表示されます。

#	Name	Type	Status	Availability	Settings
1.1	DSAM1 Port 1	DTE	Active	Idle	⚙️
1.2	DSAM1 Port 2	DTE	Active	Idle	⚙️
1.3	DSAM1 Port 3	DCE	Active	Idle	⚙️
1.4	DSAM1 Port 4	DCE	Active	Idle	⚙️

▶ DSAM シリアルポートの表示方法:

[DSAM Serial Ports] をクリック。このページからシリアルポートにアクセスして設定できます。

- ポートは、DSAM ユニットにある実際の USB の位置ごとにリストされています。
- #列は、どの Dominion KX IV-10 USB ポート DSAM が接続されているかを示します。
- Type 列は、ポートの DTE / DCE 設定を示します。
- [Status]列と [Availability]列には、現在のアクティビティが表示されます。
- [Settings]アイコンをクリックして、ポート設定を開きます。

DSAM シリアルポートの構成

シリアルポートの名前を変更し、その設定を構成できます。

▶ DSAM シリアルポートの構成方法:

1. [DSAM Serial Ports] をクリックし、構成するポートの歯車アイコンをクリックして設定画面を開きます。

Serial Port Access and Configuration					
# ▲	Name	Type	Status	Availability	Settings
1.1	DSAM1 Port 1	DTE	Active	Idle	⚙️
1.2	DSAM1 Port 2	DTE	Active	Idle	⚙️
1.3	DSAM1 Port 3	DCE	Active	Idle	⚙️
1.4	DSAM1 Port 4	DCE	Active	Idle	⚙️

2. 一般セクション:

DSAM Serial Port 1.1 Settings

General

Name

Current State Active, Idle

- ポート名を入力。
- ポートの現状を確認してください。
- ステータスと可用性が一覧表示されます。

3. [Serial Settings] セクションで、下記の設定を確認または変更します:

Serial Settings

Emulation	<input type="text" value="VT100"/>	Escape Mode	<input type="text" value="Control"/>
Encoding	<input type="text" value="Default"/>	Escape Character	<input type="text" value="]"/>
Equipment Type	<input type="text" value="Auto Detection"/>	Char Delay (ms)	<input type="text" value="0"/>
BPS	<input type="text" value="9600"/>	Line Delay (ms)	<input type="text" value="0"/>
Parity/Bits	<input type="text" value="Node/8"/>	Send Break Duration (ms)	<input type="text" value="300"/>
Flow Control	<input type="text" value="None"/>	Suppress Messages	<input type="checkbox"/>
Stop Bits	<input type="text" value="1"/>	Always Active	<input type="checkbox"/>
Multiple Writers	<input type="text" value="Single writer allowed"/>	Exit Command	<input type="text"/>
Port Keywords	<input type="text"/>		

4. エミュレーション:ポートに接続されている、シリアルターゲットの照合に使用する端末エミュレーションモードを選択します。

- VT100
- VT220
- VT320
- ANSI

チャプター3 Dominion シリアルアクセスモジュールを使用したシリアルアクセス

5. エンコーディング:必要に応じて、このポートの特定の文字エンコードを選択します。エンコーディングは、ポートのグローバル設定を設定した値に対して上書きします。
 - DEFAULT
 - US-ASCII
 - 8-BIT ASCII
 - ISO-8859-1
 - ISO-8859-15
 - UTF-8
 - Shift-JIS
 - EUC-JP
 - EUC-CN
 - EUC-KR

6. 機器のタイプ: Dominion KX IV-101 でターゲットへの物理的接続に対して、自動的に検出するかどうかを指定します。
 - デフォルトは「Auto detection」です。
 - Force DTEにより、Dominion KX IV-101 は、それに接続されているターゲットを検出する為の、データ端末検出装置として機能します。
 - DCEにより、Dominion KX IV-101 は、接続されている機器を検出する為のデータ通信機器として機能します。

注意:ターゲットに DTE または DCE のいずれかを自動検出する機能がある場合は、ポートに Force DTE または Force DCE のいずれかを選択する必要があります。 Dominion KX IV-101 は、同じポートでの DCE と DTE の両方の自動検出をサポートしておりせん。

7. ビット/秒(BPS):値を選択。
 - BPS オプション: 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
8. パリティ/ビット: 値を選択。
9. フロー制御: 値を選択。
10. ストップビット: 値を選択。
11. 複数のライター:ポートで一度に1つまたは、複数のライターを許可するオプションを選択。
12. ポートキーワード:設定すると、ポートキーワードが表示されます。
13. [Device Settings]> [Serial Port Keyword List] に移動して、ポートキーワードを追加します。エスケープモード:エスケープシーケンスは CLI にのみ影響します。エスケープモードに入ると、実行可能なコマンド (例: gethistory、view コマンド等) のメニュー、ポートセッションに戻るコマンド、及びポート接続を終了するコマンドがユーザーに表示されます。デフォルトは Control です。
 - None
 - Control

14. エスケープ文字: Dominion KX IV-101 のデフォルトは]です。(閉じ括弧).

Raritan は、[または Ctrl-[を使用しないことをお勧めします。これらのいずれかにより、意図せずにエスケープコマンドを呼び出すなど、意図しないコマンドが発生する可能性があります。このキーシーケンスは、キーボードの矢印キーでも引き金になります。

15. 文字遅延: 個々の文字がポートを介して送信されるまでの遅延を指定するには、時間をミリ秒単位で入力します。
16. ディレイライン: テキストの行がポートを介して送信されるまでの遅延を指定するには、フィールドに入力します。
17. ブレーク時間の送信: 送信ブレーク時間をミリ秒単位で入力します。範囲は 0ms ~ 1000ms です。
18. 常時アクティブ: ユーザーが接続されていない場合でも、ポートに入ってくるアクティビティをログに記録する場合、チェックボックスを選択します。
デフォルトのオプションは、接続されたユーザーなしでポートアクセスを維持しません。つまり、ユーザーが接続されていない際にポートに入るデータを無視します。
このオプションは、ポートのデータログ用です。

注意: ポートセッションにログインしているユーザーがいない場合、デフォルトでは、ポートトラフィックは破棄されます。

19. コマンドを終了します: ログアウトなどのコマンドを入力します。それが書き込み権限を持つユーザーがポートから接続が切断した際にシステムに送信されます。
これにより、ターゲットマシンでのユーザーのセッションが確実に閉じられますが、ポートに Exit コマンドを設定する必要はありません。
20. [Save]をクリック。

シリアルポートキーワードリストの設定

ポートキーワードはフィルターとして機能。

キーワードが検出されると、メッセージは下記の宛先に送信されます。

- Event Log
- SNMP
- SMTP
- Syslog

この機能は、特定のイベントがポートで発生した場合に、管理者に通知するのに役立ちます。ポートに接続しているユーザーがいないときにキーワードを引き金するには、ポート設定で「常にアクティブ」を選択する必要があります。(詳しくは *DSAM シリアルポートの構成* を参照して下さい。(24 ページ。)) シリアルポート設定ページで既存のポートキーワードのリストを表示することも出来ます。

▶ シリアルポートキーワードの設定方法:

1. [Device Settings] をクリック > シリアルポートキーワード。[Serial Port Keyword List] ページが開きます。
2. [New] をクリック。[New Keyword Setting] ページが開きます。

3. [Keyword]フィールドにキーワードを入力し、そのキーワードに関連付けるポートを選択します。全てのポートについて、上部のチェックボックスを選択します。

New Keyword Setting

Keyword

Select Ports

<input type="checkbox"/>	Name ▲
<input checked="" type="checkbox"/>	DSAM1 Port 1
<input type="checkbox"/>	DSAM1 Port 2
<input type="checkbox"/>	DSAM1 Port 3
<input type="checkbox"/>	DSAM1 Port 4

4. [Add keyboard] をクリック。シリアルポートキーワードリストが表示されます。

Serial Port Keyword List

No.	Keyword
1	Example

- キーワードを編集または削除するには、キーワードを選択。
- 青色に変化後、[Edit]または[Delete]をクリックします。

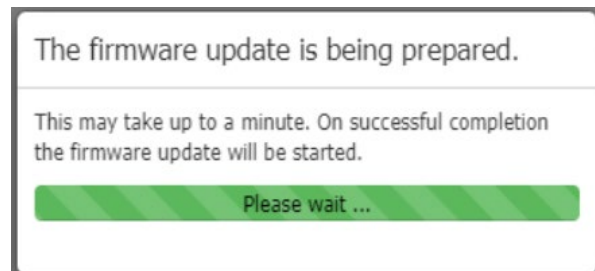
DSAM ファームウェアのアップデート

DSAM ファームウェアは、Dominion KX IV-101 ファームウェアのアップグレード中に、デバイスファームウェアで新しい DSAM パージョンが検出された際に自動的にアップグレードされます。また、DSAM ファームウェアを手動でアップグレードすることも可能。

<input checked="" type="checkbox"/>	Name	Model	Serial Number	Current DSAM Version	Update DSAM Version
<input checked="" type="checkbox"/>	DSAM1	DSAM-4	RKK6B00009	1.0	1.0

▶ **DSAM ファームウェアの手動での更新方法:**

1. [Maintenance]> [Update DSAM Firmware] を選択。
2. リストされている [Update DSAM Version] に、アップグレードしたい DSAM ユニットのチェックボックスを選択。
3. [Update Firmware] をクリックし、[OK] をクリックして確認します。
4. 進行状況のメッセージが表示されます。



5. ファームウェアのアップグレードが完了すると、成功メッセージが表示されます。

サポートされている CLI コマンド

- **show**
 - show device
DSAM が KX4-101 に接続されている場合、show device には DSAM デバイス情報が含まれます。
 - show keyword
設定されているすべてのキーワードを表示。
 - show port
DSAM シリアルポートパラメータを表示。

▪ **connect:**

DSAM シリアルポートに接続

- `connect <port index> [1.1/1.2.../2.4]`

ターゲットへの接続中に、エスケープキーシーケンスを使用して、下記のターゲットポート CLI コマンドに到達できます：

- **clearhistory**
このポートのバッファ履歴をクリア。
- **clientlist**
ポート上の全てのユーザーを表示。
- **close**
ターゲット接続を閉じます。
- **gethistory**
ポートのバッファ履歴を表示。
- **getwrite**
ポートの書き込みアクセスを取得。
- **resetport**
ポートをリセット。
- **return**
ターゲットセッションに戻る。
- **sendbreak**
接続されたターゲットにブレークを送信。
- **writelock**
ポートへの書き込みアクセスをロック。
- **writeunlock**
ポートへの書き込みアクセスのロックを解除。

▪ **config**

1. キーボード

- `keyword add [key <key>] [port <port>]`
キーワードを追加
- `keyword delete [key <key>]`
キーワードを削除
- `keyword modify [key <key>] [port <port>]`
キーワードを編集

2. ポート

DSAM シリアルポート設定の構成

- port [index <index>] [name <name>] [emulation <emulation>] [encoding <encoding>] [eqtype <eqtype>] [bps <bps>] [parity <parity>] [flowcontrol <flowcontrol>] [stopbits <stopbits>] [multiwrite <multiwrite>] [escapemode <escapemode>] [escapechar <escapechar>] [chardelay <chardelay>] [linedelay <linedelay>] [sendbreak <sendbreak>] [suppress <suppress>] [alwaysactive <alwaysactive>] [exitcommand <exitcommand>]

サポートされているエスケープキー文字

デフォルトのエスケープキーは CTRL]

カスタマイズされたエスケープキーでは、下記の文字がサポートされています。

- A-Z
- a-z
- []
- { }
- ^
- _
- ¥
- |

Web インターフェイスで DSAM シリアルターゲットに接続

The screenshot shows a web interface with a sidebar on the left containing 'DSAM Serial Ports' and 'User Management'. The main content area is titled 'Serial Port Access and Configuration' and contains a table with the following data:

# ▲	Name	Type	Status	Availability	Settings
1.1	DSAM1 Port 1	DTE	Active	Idle	⚙️
1.2	Connect	DTE	Active	Idle	⚙️
1.3	DSAM1 Port 3	DCE	Active	Idle	⚙️
1.4	DSAM1 Port 4	DCE	Active	Idle	⚙️

In the table, the 'DSAM1 Port 1' cell is highlighted with a red box, and a 'Connect' button is overlaid on it, also highlighted with a red box and a red arrow pointing to it.

▶ Web インターフェイスで、DSAM シリアルターゲットへの接続方法:

1. [DSAM シリアルターゲット] をクリックして、ポートのリストを表示
2. 接続するポートをクリックしてから、ポップアップした[接続]ボタンをクリック
HSC が新しいウィンドウで起動します。

URL 直接ポートアクセスで DSAM シリアルターゲットに接続

1. [デバイス設定]> [デバイスサービス]を選択し、[URL 経由の直接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。
2. で接続するには、下記の URL を入力します。
"https://<IP Address>/dpa.asp?port=<serial port number>&username=<username>&password=<password>"

例: https://192.168.51.101/dpa.asp?port=1.4&username=admin&password=raritan0

3. HTML シリアルクライアント (HSC) が起動し、シリアルターゲットに接続します。

SSH 経由で DSAM シリアルターゲットに接続

サポートされている CLI コマンドについて (28 ページ参照).

▶ **SSH 経由で DSAM シリアルターゲットへの接続方法:**

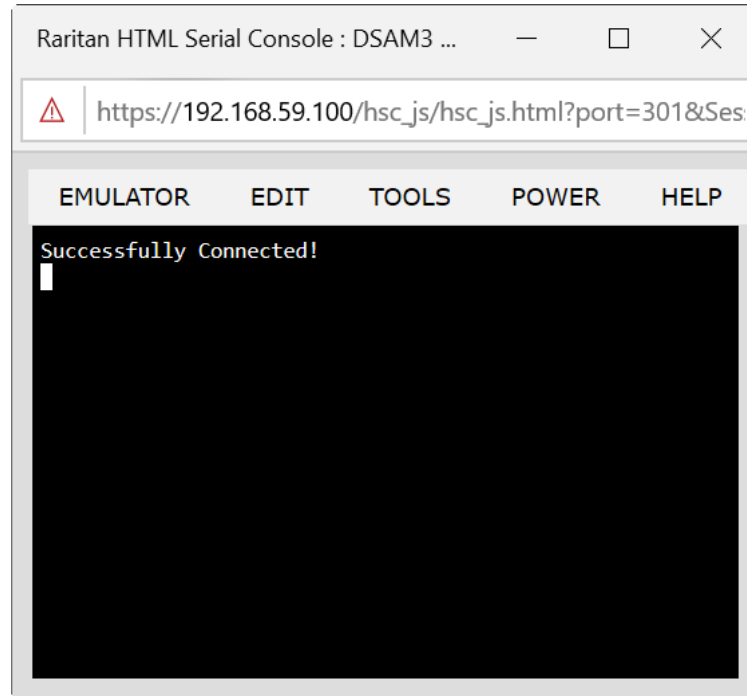
1. [Device Settings]> [Network Services]> [SSH]で SSH アクセスが有効になっていることを確認。
2. クライアント PC で SSH クライアントを起動して、Dominion KX IV-101 に接続。
3. ログイン後、ユーザーは CLI インターフェイスに入ります。
4. コマンドを入力 "connect <serial port number>"。

例: connect 1.4

5. 成功すると、シリアルターゲットにアクセス出来ます。
6. シリアルターゲットを終了するには、escape-key-sequence と入力します。デフォルトは Ctrl-] で、ポートサブメニューの CLI インターフェイスに入ります。
7. [close] と入力して、メインの CLI インターフェイスに入ります。

HTML シリアルコンソール (HSC) のヘルプ

HSC を使用してシリアルターゲットに接続。HSC は、シリアル接続を提供するいくつかの Raritan 製品をサポートしています。全ての製品が全ての HSC 機能をサポートしている訳ではありません。それらの違いについて記載されています。



HSC 機能

KX4-101 は、HSC の電源機能をサポートしていません。

エミュレータ

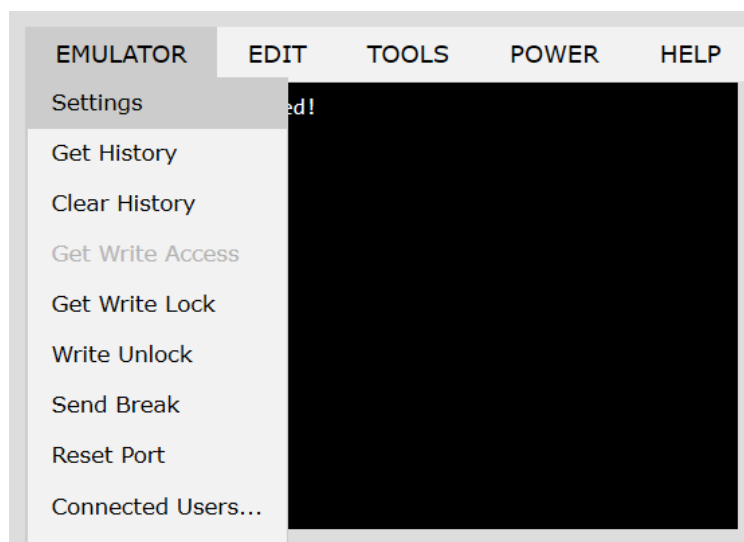
重要: HSCセッションは、Dominion KX IV-101アイドルタイムアウトの影響を受けます。

Dominion KX IV-101のアイドルタイムアウト設定をデフォルトから変更していない場合、アイドルタイムアウト期間を経過すると、セッションが自動的に閉じられる可能性があります。

デフォルトのアイドルタイムアウト設定を変更してから、HSCを起動します。アイドルタイムアウト設定の変更の詳細については、ログインの制限を参照してください。

エミュレータオプションへのアクセス

1. [EMULATOR] ドロップダウンメニューを選択して、オプションのリストを表示します。



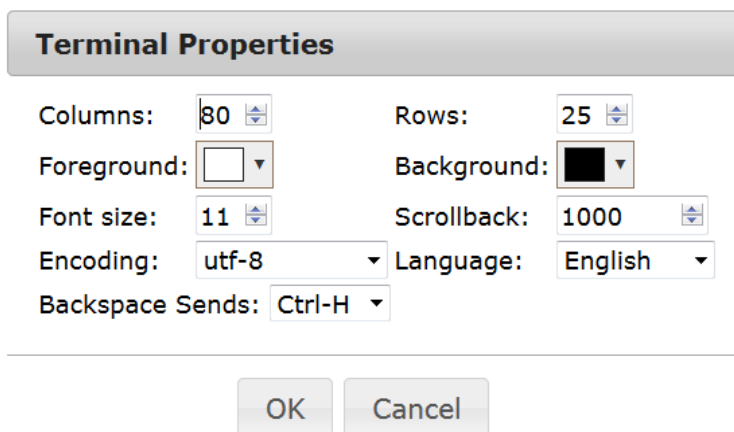
設定

注意:

KX3 の管理者は、[Settings]> [Port Configurations] でターミナルエミュレーションを設定できます。

KX4-101 の管理者は、[DSAMS Serial Ports]> [Settings]で端末エミュレーションを設定できます。

1. [EMULATOR]> [Settings]を選択します。 The Terminal Properties dialog displays the default settings. ターミナルのプロパティのダイアログには、初期設定が表示されます。



2. 端末サイズを設定します。デフォルトは 80x25 です。
3. 前景色と背景色を設定します。デフォルトは黒地に白です。
4. フォントサイズを設定します。デフォルトは 11 です。

5. スクロールバック数を設定して、スクロールに使用できる行数を示します。
6. [Encoding]のドロップダウンメニューから下記のいずれかを選択します。
 - UTF-8
 - 8-bit ascii
 - ISO-8859-1
 - ISO-8859-15
 - Shift-JIS
 - EUC-JP
 - EUC-KR
7. [Language]のドロップダウンメニューから下記のいずれかを選択します。
 - 英語
 - 日本語
 - 韓国語
 - 中国語
 - ブルガリア語
8. [Backspace Sends] のデフォルトはASCIIDELです。または [Backspace Sends]のドロップダウンメニューから Control-H を選択することも出来ます。
9. [OK]をクリックして保存。もし言語設定を変更した場合、[表示設定]ウィンドウを閉じると、HSCはその言語に変更されます。

履歴の取得

履歴情報は、ターゲットデバイスのデバッグ、トラブルシューティング、または管理の際に役立ちます。履歴の取得機能：

- ターゲットデバイスとの間のコンソールメッセージを表示することにより、コンソールセッションの最近の履歴を表示できます。
- 最大 512KB の最近のコンソールメッセージ履歴を表示します。これにより、ユーザーは時間の経過とともにターゲットデバイスのイベントを確認できます。

サイズ制限に達すると、テキストが折り返され、最も古いデータが最新のデータによって上書きされます。

注意： 履歴データは、履歴をリクエストしたユーザーにのみ表示されます。

セッション履歴を表示するには、[EMULATOR]> [Get History]を選択します。

履歴をクリア

- 履歴をクリアするには、[EMULATOR]> [Clear History]を選択します。

書き込みアクセスを取得

チャプター3 Dominion シリアルアクセスモジュールを使用したシリアルアクセス

ポートへのアクセス許可を持つユーザーのみが、書き込みアクセスを取得します。書き込みアクセス権を持つユーザーは、ターゲットデバイスにコマンドを送信出来ます。書き込みアクセスは、Get Write Access コマンドを介して、HSC で作業しているユーザー間で転送できます。

書き込みアクセスを有効にするには、[EMULATOR]を選択し、[Get Write Access]をクリック。

- これで、ターゲットデバイスへの書き込みアクセス権が付与されます。
- 別のユーザーがあなたからの書き込みアクセスを想定した場合：
 - HSC はステータスバーの書き込みアクセスの前に、赤いブロックアイコンを表示します。
 - 現在書き込みアクセス権を持っているユーザーにメッセージが表示され、別ユーザーがアクセスをコンソールへ引き継いだことをそのユーザーに警告します。

書き込みロックの取得

書き込みロックは、使用中に他ユーザーが書き込みアクセスを取得できないようにします。

1. 書き込みロックを取得するには、[EMULATOR]> [Get Write Lock]を選択。
2. もし書き込みロックの取得が使用不可の場合、要求が拒否されたというメッセージが表示されます。

書き込みロック解除の取得

ロック解除を取得するには、[EMULATOR]> [Write Unlock]を選択します。

ブレイク送信

Sun Solaris サーバーなどの一部のターゲットシステムでは、OK プロンプトを生成するためにヌル文字（ブレイク）を送信する必要があります。これは、Sun キーボードから STOP-A を発行するのと同じです。

書き込みアクセス権を持つユーザーのみが、ブレイク送信できます。

意図的な「ブレイク」を Sun Solaris サーバーに送信するには：

1. 書き込みアクセス権があることを確認します。そうでない場合は、前のセクションの手順に従って、書き込みアクセスを取得してください。
2. [EMULATOR]> [Send Break] を選択します。 Send Break Ack (Acknowledgement) メッセージが表示されます。
3. [OK]をクリック

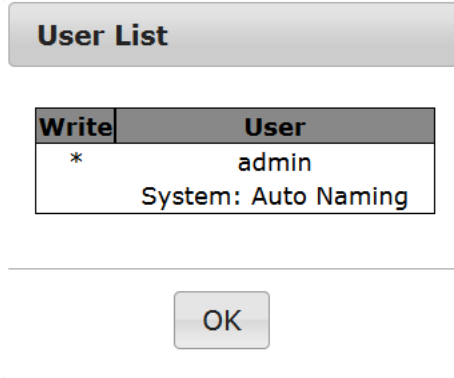
ポートをリセット

ポートのリセットは、SX2 の物理シリアルポートをリセットし、bps /ビットなどに関して設定された値に再初期化します。

接続されたユーザー

“Connected Users” コマンドを使用すると、現在同じポートに接続している他のユーザーのリストを表示できます。

1. [EMULATOR]> [Connected Users] を選択



2. コンソールへの書き込みアクセス権を持つユーザーの[Write]の列に、星印が表示されます。

終了

1. [EMULATOR]> [Exit]を選択して HSC を閉じます。

コピー&ペーストと全てのコピー

表示されているページのデータを選択してコピーできます。コピー&ペーストは、ターミナルウィンドウで右クリックすることで HSC からアクセスできます。表示されるコンテキストメニューで[コピー]または[貼り付け]を選択します。

全てのテキストをコピーするには、[Edit]メニューの[Copy All]オプションを使用します。

大量のデータを貼り付ける必要がある場合は、データをファイルに保存して、テキストファイルの送信機能を使用することをお勧めします。ブラウザウィンドウに大量のデータを貼り付けると、データ処理中にブラウザがハングする可能性があります。詳細は「テキストファイルの送信」をご参照ください。(37 ページ)

データをポートに貼り付けると、行の終わりがキャリッジ・リターンとして送信されます。

右クリックメニューの[切り取り]オプションは無効になっています。

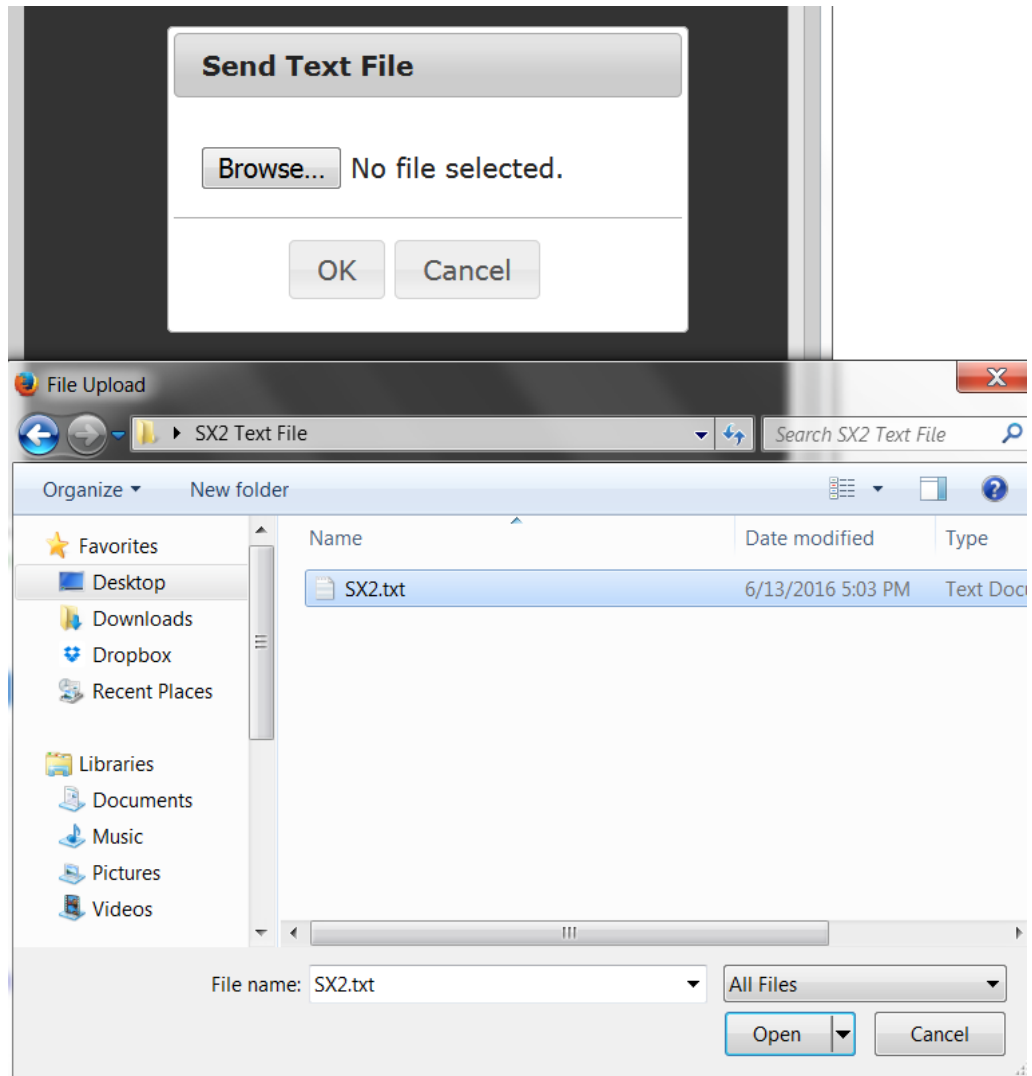
IE および一部のバージョンの Firefox の右クリックメニューに表示される[削除]オプションは使用しないでください。この削除オプションは、エミュレータウィンドウから表示されている行を完全に削除します。

▶ ブラウザ固有の動作

IE または Edge ブラウザーからコピーする場合、コピーされたデータに行末文字はありません。貼り付けられたデータはすべて 1 行に表示され、多くのスペースが含まれます。HSC ウィンドウに貼り付けると、データの位置がずれているように見える場合がありますが、データ自体は完全です。

テキストファイルの送信

1. [Edit]> [Send Text File] を選択
2. [Send Text File] ダイアログで、[参照]をクリックしてテキストファイルを見つけます。
3. [OK]をクリック
 - [OK]をクリックすると、選択したファイルがポートに送信されます。
 - 現在接続されているターゲットがない場合、画面には何も表示されません。



- ▶ Mac や Safari を使用している場合、この機能を使用する為に、下記を行ってください。

1. Safari で、[設定]を選択。
2. [セキュリティ]タブで、[Web サイト設定の管理]を選択。

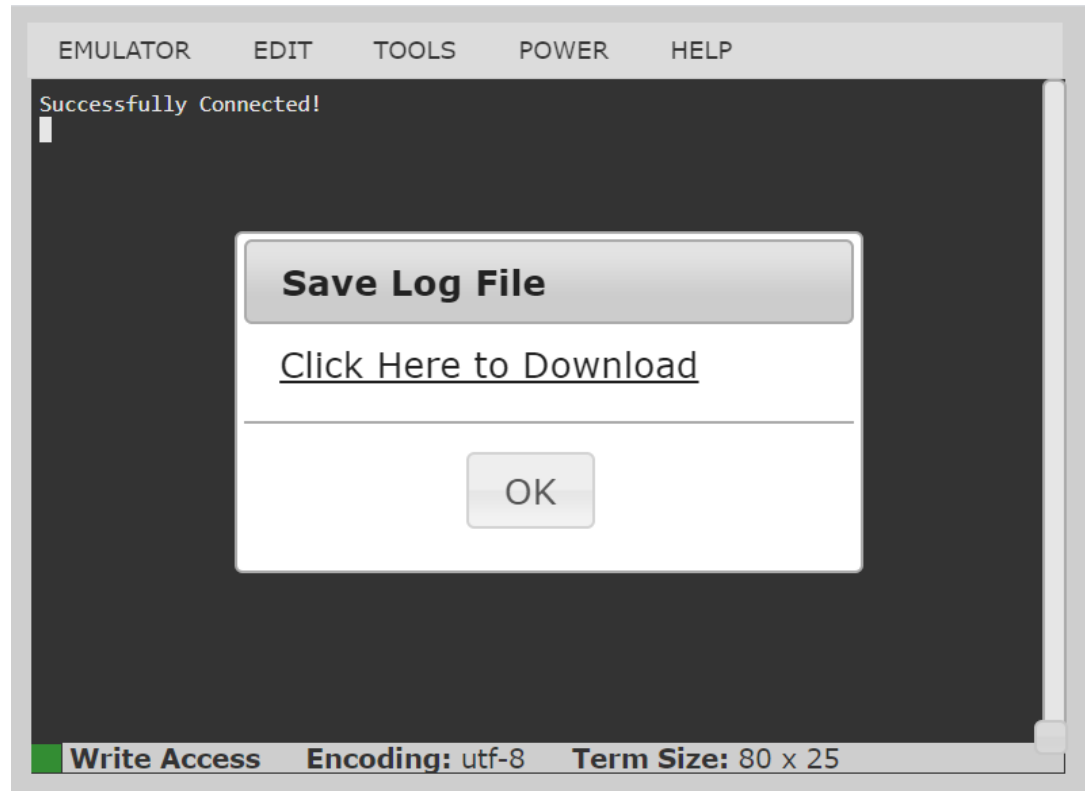
チャプター3 Dominion シリアルアクセスモジュールを使用したシリアルアクセス

3. Dominion KX IV-101 Web サイトをクリック。
4. ドロップダウンボックスから[安全でないモードで実行]を選択。
5. Safari を再起動。

ツール：ロギングの開始と停止

[Tools]メニューには、データ履歴ファイルを作成してダウンロードする為のオプションが含まれています。

1. [Tools]> [Start Logging] を選択して、メモリへのシリアルポートデータの保存を開始します。
2. [Stop Logging] をクリックして、ログファイルを保存。ダウンロードリンクを含む、ポップアップメッセージが表示されます。クリックして、メモリバッファをテキストファイルにダウンロードします。



HSC のブラウザのコツ

一部のブラウザには、HSC に影響する制限があります。

- Internet Explorer には、単一のサーバーに作成できる WebSocket の数に内部制限があります。(6) [https://msdn.microsoft.com/en-us/library/ee330736\(v=vs.85\).aspx#websocket_maxconn](https://msdn.microsoft.com/en-us/library/ee330736(v=vs.85).aspx#websocket_maxconn)
これは上記のように、レジストリ変数を変更することで変更可能です。
- Internet Explorer 11、Safari、及び Edge には、IPv6 デバイスへの接続に制限があります。WebSocket 接続を確立しようとするときに、数値 URL を使用しても機能しません。In これらのブラウザでは、デバイスのホスト名またはリテラル IPv6 を UNC として使用して、SX II に接続します。
https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names を参照。
- IOS Safari で HSC を使用する場合、「デスクトップ Web サイトの要求」設定が有効になっていると、一部のページにキーボードが表示されない場合があります。
設定を変更するには、[設定] > [Safari] > [デスクトップ Web サイトを要求] に移動し [すべての Web サイト] が選択されていないこと、及びデバイス アドレスが選択されていないことを確認します。アドレスごとに、HSC ポートに接続しているときに Safari のブラウザペインで「aA」をクリックして設定し、「Web サイト設定」を選択して「デスクトップ Web サイトの要求」が選択されていないことを確認することも出来ます。

CHAPTER 4 KVM クライアント

Dominion KX IV-101 には、個々の構成をサポートする様々な KVM クライアントを使用してアクセスできます。

- HKC は Java を使用しない Linux 及び、Mac ユーザーに最適です。
- AKC は Windows または、Edge ブラウザを使用する Windows プラットフォームに最適です。
- VKC は Java を使用する Linux 及び、Mac ユーザーに最適です。

KVM クライアント	名	プラットフォーム	特長
HTML KVM クライアント	HKC	<ul style="list-style-type: none">▪ Linux▪ Mac▪ Windows▪ HTML 及び JavaScript	<ul style="list-style-type: none">▪ Java フリー▪ ほとんどの機能をサポート▪ サポートされている機能については、HTML KVM クライアント (HKC) を参照してください。
アクティブ KVM クライアント	AKC	<ul style="list-style-type: none">▪ Windows▪ Microsoft .NET 必須	<ul style="list-style-type: none">▪ フル機能の KVM クライアント▪ Java フリー
仮想 KVM クライアント	VKC	<ul style="list-style-type: none">▪ Linux▪ Mac▪ Windows	<ul style="list-style-type: none">▪ フル機能の KVM クライアント▪ Java が必須

内容

仮想 KVM クライアント (VKCS) のヘルプ	40
アクティブ KVM クライアント (AKC) のヘルプ	71
HTML KVM クライアント (HKC)	73
デュアルモニター設定で、Dominion KX IV-101 にアクセスする為のコツ	106

仮想 KVM クライアント (VKCS) のヘルプ

VKCS を起動するには、ブラウザに “<https://<KX4-101 IP アドレス>/vkcs>” と入力。

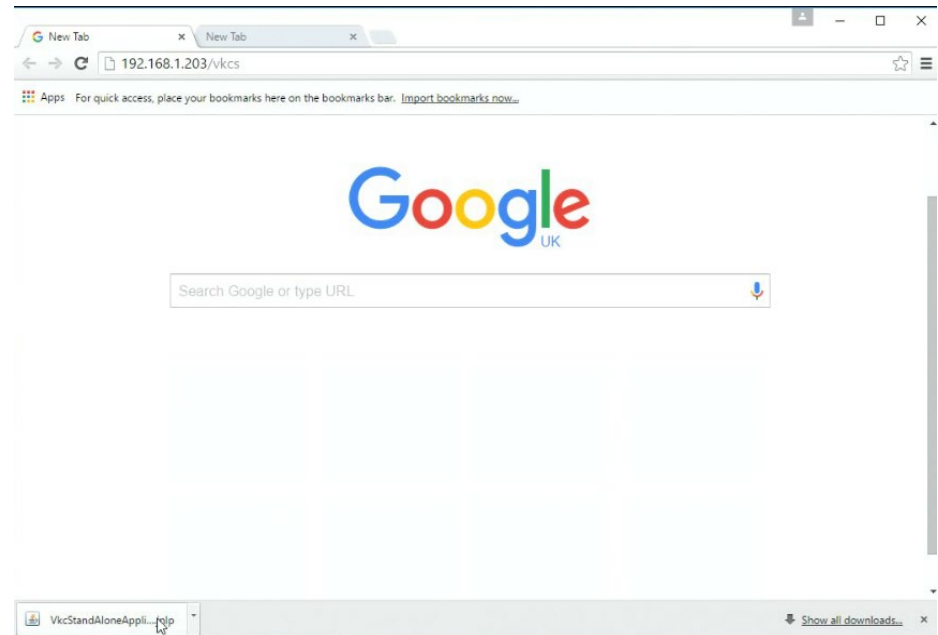
Java 要件

- サポートされている Java バージョンが必要です。サポートされている最新バージョンについては、リリースノートをご確認ください。
- Java がインストールされていない場合、「ファイルを開くことができない」というプロンプトが表示され、プログラムを検索するオプションが表示されます。

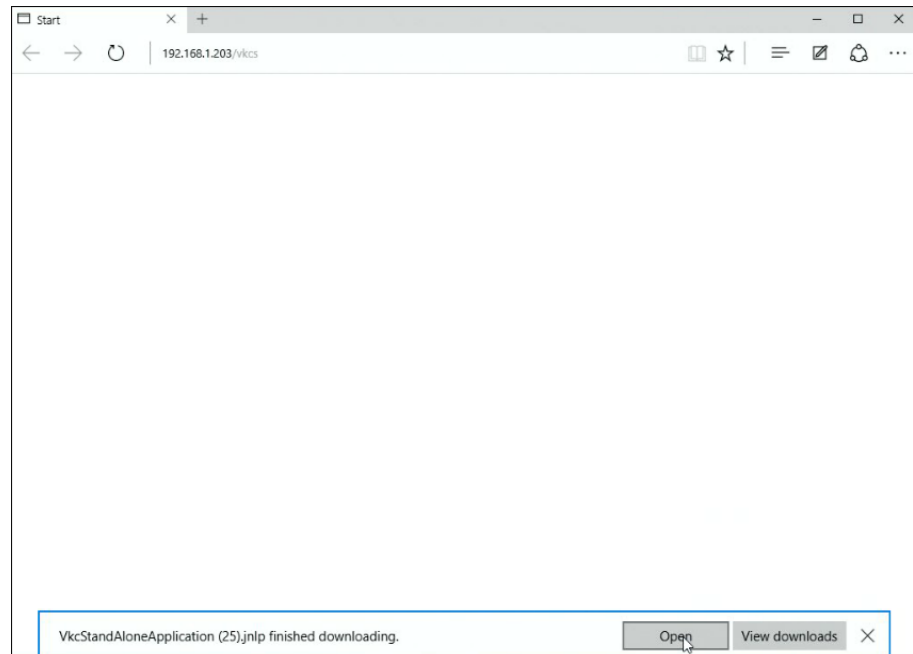
▶ VKCS の起動:

全てのブラウザで、使用するたびに VKCS スタンドアロン アプリケーションをダウンロードする必要があります。

- Chrome と Edge: ダウンロードした VKCS jnlp ファイルは、常にブラウザウィンドウの左下隅をクリックして起動する必要があります。



- Internet Explorer: 起動するには、ブラウザの下部にある [開く] をクリックする必要があります。



- Safari: jnlp ファイルをローカルに保存します。Ctrl キーを押しながら選択して開き、表示されたプロンプトで [開く] をクリックします。
- Firefox: Windows 上の Firefox の現在のデフォルト設定では、ファイルが保存され、ダウンロードから実行されます。この設定でブラウザから起動できます: [ツール] > [オプション] > [アプリケーション] の [コンテンツ タイプ] で [Jnlp ファイル] を選択し、[アクション] を [常に確認する] から [Java Web Launcher を使用する] に変更します。

Firefox ブラウザから起動すると、実行可能な警告メッセージが表示されます。これを抑制する方法は2つあります:

jnlp : // <IP アドレス> / vkcs 経由で起動。

詳細につきましては、

<https://superuser.com/questions/1441134/disable-firefoxs-open-executable-file-warning>

をご参照ください。

または

- about : config に新しい設定
- 「browser.download.skipConfirmLaunchExecutable」を追加します。
- 詳細については、
- <https://support.mozilla.org/en-US/questions/1260307> をご参照ください。

プロキシサーバーの構成

プロキシサーバーの使用が必要な場合は、リモートクライアント PC で SOCKS プロキシも提供及び、構成する必要があります。

注意：インストールされているプロキシサーバーが、HTTP プロキシプロトコルのみに対応している場合、接続できません。

▶ プロキシの設定方法:

1. リモートクライアント PC で、[コントロールパネル]> [インターネットオプション] を選択。
 - a. [接続] タブで、[LAN 設定] をクリックして、[ローカルエリアネットワーク (LAN) 設定] ダイアログが開きます。
 - b. [LAN にプロキシサーバーを使用する] を選択。
 - c. [詳細] をクリックします。 [プロキシ設定] ダイアログが開きます。
 - d. 全てのプロトコルのプロキシサーバーを構成します。

重要:「すべてのプロトコルに同じプロキシサーバーを使用する」を選択しないでください。

注意: SOCKS プロキシ (1080) のデフォルトのポートは、HTTP プロキシ (3128) とは異なります。

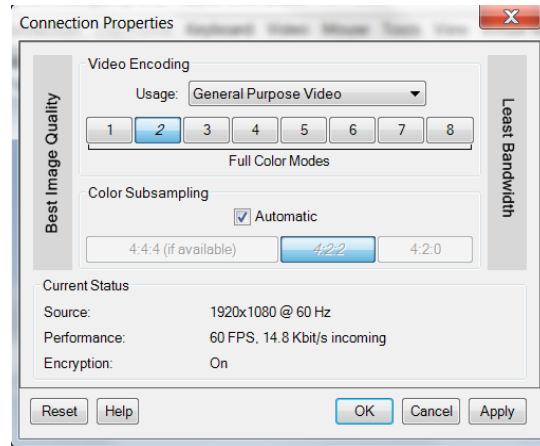
- e. 各ダイアログで [OK] をクリックして、設定を適用します。
2. 次に、Java™ アプレットの プロキシ 設定を構成します。
 - a. 「コントロールパネル」> 「Java」 を選択。
 - b. [全般] タブで、[ネットワーク設定] をクリックします。 [ネットワーク設定] ダイアログが開きます。
 - c. 「プロキシサーバーを使用する」を選択します。
 - d. [詳細] をクリックします。 [ネットワークの詳細設定] ダイアログが開きます。
 - e. 全てのプロトコルのプロキシサーバーを構成します。

重要:「すべてのプロトコルに同じプロキシサーバーを使用する」を選択しないでください。

注意: SOCKS プロキシ (1080) のデフォルトのポートは、HTTP プロキシ (3128) とは異なります。

接続プロパティ

[Connection Properties] ダイアログでは、システム機能とパフォーマンスのニーズを一致させるように、ビデオストリームパラメータを構成できます。



▶ ビデオエンコーディング

このセクションでは、ビデオエンコーディングアルゴリズムと品質設定を選択します。

- 使用法：一般的なアプリケーション領域を指定します。この選択により、このダイアログの他の場所で使用可能な選択肢が、最適化されます。
 - 汎用ビデオ: 映画、ビデオゲーム、アニメーション等のスムーズな色再現が最も重要なビデオコンテンツ。
 - コンピューターと IT アプリケーション: コンピューターのグラフィカルインターフェイス等の、テキストの鮮明さと明瞭さが重要なビデオコンテンツ。

- エンコーダモード: 8つのボタン箇所からエンコーダモードを選択します。オプションは、使用法の選択によって異なります。一般的に、ボタンバーの左側にあるモードは、より高い画質を提供しますが、より高い帯域幅を消費し、ネットワーク速度やクライアントのパフォーマンスによってはフレームレートが低下する可能性があります。右に向かうにつれて、画質の低下を犠牲にして、より低い帯域幅を消費します。ネットワークまたはクライアントに制約のある状況では、右側のモードの方が、フレームレートが向上する場合があります。

デフォルトのビデオモードは常に「フルカラー2」です。これは高品質モードであり、LAN環境での殆どの使用に適しています。必要に応じて、さらに右側のモードを試して、画質とフレームレートの適切なバランスを見つけてください。

▶ カラーサブサンプリング

カラーサブサンプリングは、エンコードされたビデオストリームの色情報を減らします。

- 自動: お勧めです。最適なカラーサブサンプリングモードは、ビデオエンコーディングセクションでの選択に基づいて有効になります。
- 4:4:4: かなりの帯域幅コストで最高品質。グラフィカルユーザーインターフェイスの一部の状況を除いて、通常は必要ありません。1920x1200を超える解像度ではサポートされていないため、これらの解像度では、カラーサブサンプリングは自動的に4:2:2にドロップダウンします。
- 4:2:2: 画質と帯域幅の適切なブレンド。
- 4:2:0: ネットワーク帯域幅とクライアント負荷の最大の節約。高解像度のラインやテキストを強調しない、殆どの汎用アプリケーションで正常に機能します。

▶ 現在のステータス

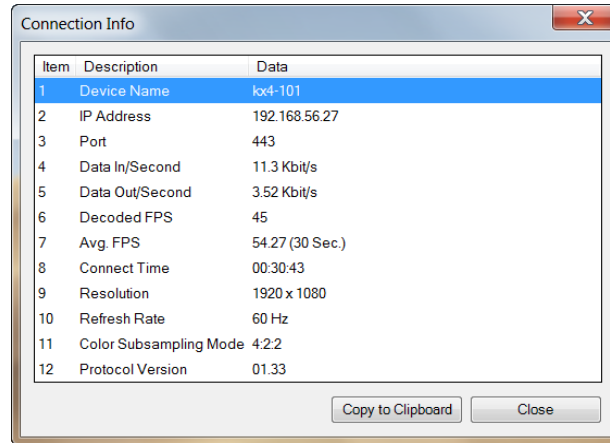
現在のステータスには、リアルタイムのビデオパフォーマンス統計が含まれます。ダイアログで設定を変更すると、パフォーマンスへの影響をすぐに確認できます。

- ソース: 着信ビデオソースの解像度とフレームレート。
- パフォーマンス: クライアントでレンダリングされる1秒あたりのフレーム数(FPS)、及び着信ビデオストリームのデータレート。これらの値は、ビデオ設定の効果を確認できる場所です。
- 暗号化: ビデオストリームが暗号化されているかどうか。暗号化されたストリームは通常、フレームレートと帯域幅が低くなります。暗号化は、セキュリティ→KVM セキュリティ→「暗号化モードを KVM 及び、仮想メディアに適用する」のグローバル設定です。

接続情報

現在の接続に関するリアルタイムの接続情報については、[Connection Info] ダイアログを開き、必要に応じてダイアログから情報をコピーします。接続プロパティを編集するには、「接続プロパティ (44 ページ)」をご参照ください。

- 接続情報を表示するには、[Connection] > [Info...] を選択します。




キーボード

Ctrl+Alt+Del マクロの送信

Ctrl+Alt+Delete マクロは頻繁に使用される為、事前にプログラムされています。

[Keyboard] > [Ctrl+Alt+Del の送信] を選択するか、ツールバーの Ctrl+Alt+Delete

ボタン  をクリックすると、このキーシーケンスがサーバーまたは、現在接続している KVM スイッチに送信されます。

対照的に、Ctrl+Alt+Del キーを物理的に押すと、Windows オペレーティング システムの構造により、意図したとおりにキー シーケンスがターゲット サーバーに送信されるのではなく、最初にご自身の PC によってコマンドがインターセプトされます。

LeftAlt+Tab を送信 (ターゲット サーバー上の開いているウィンドウを切り替える)

[Keyboard] > [LeftAlt + Tab を送信] を選択して、ターゲット サーバーで開いているウィンドウを切り替えます。

テキストをターゲットに送信

▶ テキストをターゲットに送信する方法(マクロ)

1. [Keyboard] > [Send text to target] をクリックします。 [テキストをターゲットに送信] ダイアログが表示されます。

2. ターゲットに送信するテキストを入力します。

注意: 英語以外の文字は、ターゲットへの送信機能はサポートされていません。

3. ターゲットが US/インターナショナル キーボード レイアウトを使用している場合は、[ターゲット システムが US/インターナショナル キーボード レイアウトに設定されている] チェックボックスを選択。
4. [OK] をクリック。

キーボードマクロ

キーボードマクロは、ターゲットサーバー向けのキーストロークの組み合わせが、ターゲットサーバーにのみ送信され、ターゲットサーバーによってのみ解釈されるようにします。そうでなければ、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、PC 固有です。別 PC を使用している場合、マクロは表示されません。

さらに、他の人があなたの PC を使用して別の名前でログインした場合、マクロはコンピューター全体規模であるため、そのユーザーはマクロを見ることになります。

新しいマクロの構築

▶ マクロの構築方法:

1. [キーボード] > [キーボード マクロ] をクリックします。[キーボード マクロ] ダイアログが表示されます。
2. [追加] をクリックします。[キーボード マクロの追加] ダイアログが表示されます。
3. [キーボード マクロ名] フィールドにマクロの名前を入力します。この名前は、作成後にキーボードメニューに表示されます。
4. [ホットキーの組み合わせ] フィールドで、ドロップダウンリストからキーボードの組み合わせを選択します。これにより、定義済みのキーストロークでマクロを実行できます。 **オプション**
5. ドロップダウンリストで、コマンドの実行に使用されるキーストロークをエミュレートするために使用する各キーを選択します。押す順番でキーを選択します。選択するたびに、[キーの追加] を選択します。各キーが選択されると、それがマクロシーケンスフィールドに表示され、選択するたびにキーを離すコマンドが自動的に追加されます。

例えば、左 Ctrl + Esc を選択してウィンドウを閉じるマクロを作成します。これは、下記のように [マクロ シーケンス] ボックスに表示されます。

左 Alt キーを押す

F4 を押す

Esc

F4 を離す

Esc

左 Alt を離す

6. [マクロ シーケンス] フィールドを確認して、マクロシーケンスが正しく定義されていることを確認します。
 - a. シーケンス内のステップを削除するには、そのステップを選択して [削除] をクリック。
 - b. シーケンス内のステップの順序を変更するには、ステップをクリックし、上下の矢印ボタンをクリックして、必要に応じて順序を変更します。

7. [OK] をクリックしてマクロを保存します。[クリア] をクリックしてすべてのフィールドをクリアし、最初からやり直します。[OK] をクリックすると [キーボード マクロ] ダイアログが表示され、新しいキーボード マクロがリストされます。
8. [閉じる] をクリックして [キーボード マクロ] ダイアログを閉じます。これで、マクロがアプリケーションのキーボード メニューに表示されます。
9. メニューで新しいマクロを選択して実行するか、マクロに割り当てたキーストロークを使用します。

マクロのインポートとエクスポート

VKC で作成されたマクロを AKC で使用することはできません。その逆も同様です。HKC で作成されたマクロは HKC とのみ互換性があり、AKC または VKC では使用できません。同様に、VKC または AKC で作成されたマクロは、HKC では使用できません。

マクロのインポート

▶ マクロのインポート方法:

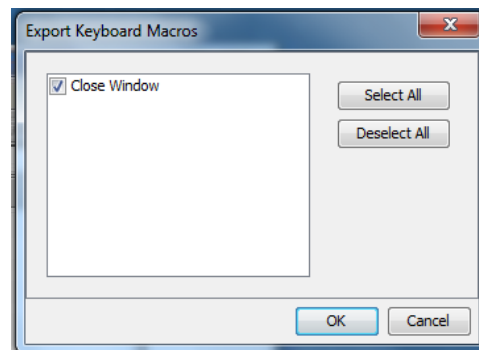
1. [キーボード] > [キーボード マクロのインポート] を選択して、[マクロのインポート] ダイアログを開きます。マクロファイルのフォルダの場所を参照します。
2. マクロファイルをクリックし、[開く] をクリックしてマクロをインポートします。
 - a. ファイル内に見つかったマクロが多すぎる場合は、エラー メッセージが表示され、[OK] を選択するとインポートが終了します。
 - b. インポートに失敗した場合、エラーダイアログが表示され、失敗した理由が表示されます。[OK] を選択して、インポートできないマクロをインポートせずに、インポートを続行します。
3. 対応するチェックボックスをオンにするか、[すべて選択] または [すべて選択解除] オプションを使用して、インポートするマクロを選択します。
4. OK をクリックしてインポートを開始。
 - a. 重複するマクロが見つかった場合は、[マクロのインポート] ダイアログが表示されます。次のいずれかを実行して下さい。

- 既存のマクロをインポートされたバージョンで置き換えるには、
[はい] をクリックします。
- [すべてはい] をクリックして、現在選択されているマクロと、見つかった他の重複するマクロを置き換えます。
- [いいえ] をクリックして元のマクロを保持し、次のマクロに進みます。
- [すべていいえ] をクリックして、元のマクロを保持し、次のマクロに進みます。見つかった他の重複もスキップされます。
- インポートを停止するには、[キャンセル] をクリック。
- または[名前の変更] をクリックしてマクロの名前を変更し、インポートします。[名前の変更] を選択すると、[マクロの名前変更] ダイアログが表示されます。フィールドにマクロの新しい名前を入力し、[OK] をクリックします。ダイアログが閉じ、プロセスが続行されます。入力された名前がマクロと重複している場合、警告が表示され、マクロに別の名前を入力する必要があります。
- b. インポートプロセス中に、許可されたインポートされたマクロ数を超えると、ダイアログが表示されます。[OK] をクリックしてマクロのインポートを続行するか、[キャンセル] をクリックしてインポートを停止します。

その後、マクロがインポートされます。既に存在するホットキーを含むマクロをインポートすると、インポートされたマクロのホットキーは破棄されます。

マクロのエクスポート

1. [ツール] > [マクロのエクスポート] を選択して、[エクスポートするキーボードマクロの選択] ダイアログを開きます。




2. 対応するチェックボックスをオンにするか、[すべて選択] または [すべて選択解除] オプションを使用して、エクスポートするマクロを選択します。
3. [OK] をクリックします。[キーボードマクロのエクスポート先] ダイアログが表示されます。マクロファイルを見つけて選択。デフォルトでは、マクロはデスクトップに存在します。
4. マクロファイルを保存するフォルダーを選択し、ファイルの名前を入力して[保存] をクリックします。マクロが既に存在する場合は、警告メッセージが表示されます。
5. [はい] を選択して既存のマクロを上書きするか、[いいえ] を選択してマクロを上書きせずにアラートを閉じます。

ビデオ

画面の更新


画面更新のコマンドは、ビデオ画面を強制的に更新します。

- [Video] > [Refresh Screen] を選択するか、ツールバーの [画面を更新] ボタン  をクリックします。

ターゲットコマンドのスクリーンショット (ターゲットスクリーンショット)

[ターゲット サーバーからのスクリーンショット] コマンドを使用して、ターゲットサーバーのスクリーンショットを撮ります。必要に応じて、このスクリーンショットを選択したファイルの場所にビットマップ、JPEG、または PNG ファイルとして保存します。

▶ ターゲットサーバーのスクリーンショット方法:

1. [Video] > [Screenshot] を選択するか、ツールバーの [ターゲット スクリーンショット] ボタン  をクリックします。
2. [保存] ダイアログで、ファイルを保存する場所を選択し、ファイル名を設定、[ファイルの種類] ドロップダウンからファイル形式を選択します。
3. [保存] をクリックして、スクリーンショットを保存。

マウスオプション

マウスモードまたは、デュアルマウスモードで操作できます。

デュアル マウス モードで、オプションが適切に構成されている場合、マウスカーソルが整列します。

ターゲット サーバーを制御する場合、リモート コンソールには 2 つのマウス カーソルが表示されます。1 つは Dominion KX IV-101 クライアント ワークステーションに属し、もう 1 つはターゲットサーバーに属します。

マウスカーソルが 2 つある場合、デバイスはいくつかのマウスモードを提供します。

- ずれないマウス (マウス同期)
- インテリジェント (マウスモード)
- スタンダード(マウスモード)

マウスポインターが KVM クライアントターゲットサーバーのウィンドウ内にある場合、マウスの動きとクリックは、接続されているターゲット サーバーに直接送信されます。

移動中は、マウスの加速設定により、クライアントのマウス ポインターがターゲットのマウスポインターよりもわずかに進みます。

シングルマウスモードでは、ターゲットサーバーのポインターのみを表示できます。他のモードが機能しない場合は、シングル マウスモードを使用できます。

2 つのモード (シングルマウスとデュアルマウス) を切り替えることができます。

デュアルマウスモード

ずれないマウスの同期

このモードでは、ターゲットマウスが異なる加速または速度に設定されている場合でも、ずれない機能を使用してクライアントカーソルとターゲットカーソルの同期を維持します。

これがデフォルトのマウスモードです。

▶ ずれないマウスの同期方法:

- KVM クライアントから [Mouse] > [Absolute] を選択します。

インテリジェントマウスモード

インテリジェントマウス モードでは、デバイスはターゲットマウスの設定を検出し、それに応じてマウス カーソルを同期して、ターゲットでのマウスのアクセラレーションを可能にします。

インテリジェントマウスモードへ設定。

▶ インテリジェントマウスモードの方法:

- [Mouse] > [Intelligent] を選択。

インテリジェントマウスの同期条件

[マウス] メニューにある [インテリジェントマウス同期] コマンドは、非アクティブな時にマウスカーソルを自動的に同期します。ただし、これが正しく機能するには、下記の条件を満たす必要があります。

- アクティブなデスクトップは、ターゲットで無効にする必要があります。
- ターゲットページの左上隅に、ウィンドウが表示されないようにしてください。
- ターゲットページの左上隅に、アニメーションの背景があってはなりません。
- ターゲットのマウスカーソルの形状は、アニメーション化されていない通常の形状である必要があります。
- ターゲットマウスの速度は、非常に遅い値または、非常に高い値に設定しないでください。
- 「ポインターの精度の向上」や「ダイアログのデフォルトボタンへのマウスのスナップ」などのターゲットの高度なマウスプロパティは、無効にする必要があります。
- ターゲット動画の端が、はっきり見える (つまり、ターゲットビデオイメージの端までスクロールすると、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、黒い境界線が表示されます)。
- インテリジェントマウス同期機能を使用する場合、デスクトップの左上隅にファイルアイコンやフォルダーアイコンがあると、機能が正常に動作しない場合があります。この機能の問題を確実に回避するには、デスクトップの左上隅にファイルアイコンやフォルダーアイコンを置かないでください。

ターゲットビデオを自動検出した後、ツールバーの [マウスの同期] ボタンをクリックして、手動でマウスの同期を開始します。これはマウスカーソルが互いに非同期化し始めた場合に、ターゲットの解像度に変更された場合にも適用されます。

インテリジェントマウス同期が失敗した場合、このモードは標準のマウス同期動作に戻ります。

マウスの構成は、ターゲットのオペレーティングシステムによって異なることにご注意ください。詳細については、該当 OS のガイドライン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。

標準マウスモード

標準マウスモードでは、標準のマウス同期アルゴリズムが使用されます。アルゴリズムは、クライアントとターゲットサーバー上の相対的なマウス位置を決定します。

クライアントとターゲットのマウスカーソルの同期を維持するには、マウスアクセラレーションを無効にする必要があります。さらに特定のマウスパラメータを、正しく設定する必要があります。

▶ 標準マウスモードの設定方法:

- [Mouse] > [Standard] を選択します。

同期のコツ

マウスの同期に問題がある場合:

1. 選択したビデオ解像度とリフレッシュレートが、デバイスでサポートされているものであることを確認します。 KVM クライアント接続情報ダイアログには、デバイスが認識している実際の値が表示されます。
2. マウスの同期が改善されない場合 (Linux、UNIX、及び Solaris KVM ターゲットサーバーの場合):
3. ターミナルウィンドウを開く。
4. 右記のコマンドを入力します: `xset mouse 1 1`
5. ターミナルウィンドウを閉じる。
6. 「KVM クライアントのマウス同期」 ボタンをクリックします。

マウスを同期

デュアルマウスモードでの[マウスの同期] コマンドは、ターゲットサーバーのマウスカーソルをクライアントのマウスカーソルに強制的に再配置します。

▶ マウスカーソルを同期するには、下記のいずれかを実行します。

- KVM クライアントツールバーの [Synchronize mouse] ボタン  をクリックするか、メニュー バーから [Mouse] > [Mouse Sync] を選択します。

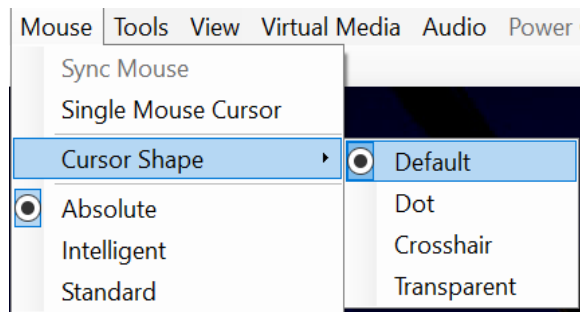
注意: このオプションは、標準及びインテリジェントマウスモードでのみ使用できます。

カーソル形状

デュアルマウスモードでは、セッションのカスタムカーソル形状を選択できます。カーソルの選択を固定するには、クライアントの起動設定をご参照ください。(58 ページ)

▶ カーソル形状の変更方法:


- マウス > カーソルの形状を選択し、リストから選択します。
 - デフォルトの矢印
 - ドット
 - クロスヘア
 - トランスペアレント

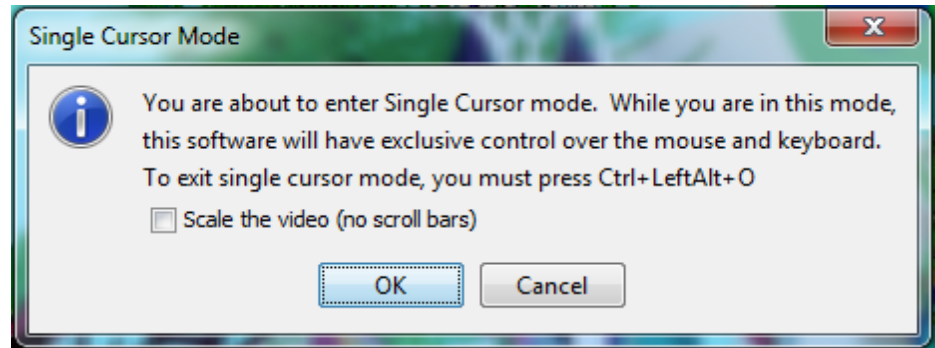


シングルマウスモード

シングルマウスモードでは、ターゲットサーバーのマウスカーソルのみが使用されます。クライアントのマウスカーソルが、画面に表示されなくなります。

注意: クライアントが仮想マシンで実行されている場合、シングルマウスモードは Windows または Linux ターゲットでは機能しません。

- ▶ シングルマウスモードに設定するには、下記のいずれかを実行します。
 - [Mouse] > [Single Mouse Cursor] を選択。
 - ツールバーにある [Single/Double Mouse Cursor] ボタン  をクリックします。



▶ シングルマウスモードの終了方法:

1. キーボードで Ctrl+Alt+O を押して、シングルマウスモードを終了します。

ツールオプション

一般的な設定

▶ ツールオプションの設定方法:

1. [Tools] > [Option] をクリックします。[オプション] ダイアログが表示されます。
2. スケーリングされた KVM イメージの OpenGL レンダリングは、デフォルトで有効になっています。パフォーマンスの問題がある場合は、[ハードウェア アクセラレータレンダリングを無効にする] チェックボックスを選択して、無効にします。AKC でのみ使用できます。

3. テクニカルサポートから指示された場合のみ、[ログを有効にする] チェックボックスを選択します。

このオプションは、ホームディレクトリにログファイルを作成します。

4. ドロップダウンリストから、キーボードタイプを選択します (必要な場合)。

オプションには、下記のものが含まれます:

- US
- フランス語 (フランス)
- ドイツ語 (ドイツ)

- 日本語
- UK
- 韓国語 (韓国)
- フランス語 (ベルギー)
- ノルウェー語 (ノルウェー)
- ポルトガル語 (ポルトガル)
- デンマーク語 (デンマーク)
- スウェーデン語 (スウェーデン)
- ドイツ語 (スイス)
- ハンガリー語 (ハンガリー)
- スペイン語 (スペイン)
- イタリア語 (イタリア)
- スロベニア語
- 翻訳: フランス語 - US

AKC では、キーボードタイプはデフォルトでローカルクライアントである為、このオプションは適用されません。

5. 必要に応じて、[フルスクリーンウィンドウサイズをクライアント解像度ではなく、ターゲット解像度に調整する] を選択します。Linux クライアントでは、オプションを使用できません。詳細と例については、「[全画面ウィンドウサイズを、ターゲット解像度に調整する \(57 ページ\)](#)」をご参照ください。
6. Mac OS/VKC の起動のみで、フルスクリーンウィンドウがメインメニューバーを覆うようにし、ドックはデフォルトで有効になっています。この設定を使用して、Mac でフルスクリーンモードで VKC を実行している時に、Java メニューバーが VKC メニューバーを非表示にしないようにします。
7. ホットキーの構成:
 - 全画面モードの切り替え - ホットキー
全画面モードに入ると、対象サーバーの表示が全画面になり、対象サーバーと同じ解像度になります。
これは、このモードの切り替えに使用されるホット キーです。
 - シングルカーソルモードの切り替え - ホットキー
シングルカーソルモードに入ると、ターゲットサーバーのマウスカーソルだけが表示されます。
これは、シングルカーソルモードのオンとオフを切り替える為に使用されるホットキーであり、クライアントのマウスカーソルを削除したり元に戻したりします。
 - スケーリング モードの切り替え - ホットキー
スケーリングモードに入ると、ターゲットサーバーはディスプレイに合わせてスケーリングされます。
これは、スケーリングモードの切り替えに使用されるホット キーです。

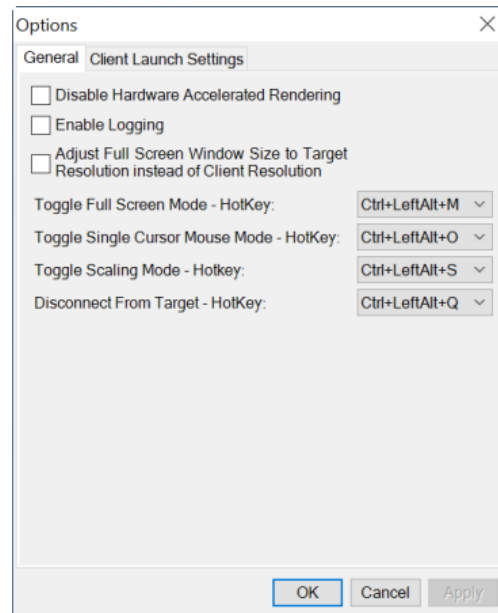
- ターゲットからの切断 - ホットキー
ユーザーがターゲットからすばやく切断できるようにするには、このホットキーを有効にします。

ホットキーの組み合わせの場合、アプリケーションでは、同じホットキーの組み合わせを複数の機能に割り当てることはできません。

例えば、Q が既にターゲットからの切断機能に適用されている場合、全画面モードの切り替え機能では使用できません。

さらにアップグレードにより、ホットキーがアプリケーションに追加され、キーのデフォルト値がすでに使用されている場合、次に使用可能な値が代わりに適用されます。

8. [OK] をクリック。



キーボードの制限事項

トルコ語キーボード

キーボードは、Active KVM Client (AKC) でのみサポートされています。

スロベニア語キーボード

キーは、JRE の制限により、スロベニア語のキーボードでは機能しません。

Linux での言語構成

Linux 上の Sun JRE では、システム環境設定を使用して構成された外国語キーボードに対して、正しいキーイベントを生成する際に問題が発生する為、下記の表で説明する方法を使用して外国語キーボードを構成します。

言語	設定方法
US	デフォルト
フランス語	キーボードインジケーター
ドイツ語	システム設定 (コントロールセンター)
日本語	システム設定 (コントロールセンター)

言語	設定方法
UK	システム設定 (コントロールセンター)
韓国語	システム設定 (コントロールセンター)
ベルギー語	キーボードインジケータ
ノルウェー語	キーボードインジケータ
デンマーク語	キーボードインジケータ
スウェーデン語	キーボードインジケータ
ハンガリー語	システム設定 (コントロールセンター)
スペイン語	システム設定 (コントロールセンター)
イタリア語	システム設定 (コントロールセンター)
スロベニア語	システム設定 (コントロールセンター)
ポルトガル語	システム設定 (コントロールセンター)

注意: キーボードインジケータは、デスクトップ環境として Gnome を使用する、Linux システムで使用する必要があります。

全画面ウィンドウサイズを、目標解像度に調整

[クライアント解像度の代わりに、フルスクリーンウィンドウサイズをターゲット解像度に調整] が有効になっている場合、クライアントは、クライアントモニターの解像度ではなく、ターゲットの解像度に等しいウィンドウでフルスクリーンで起動します。マルチモニタークライアントを使用している場合、全画面ウィンドウが複数のモニターをカバーする場合があります。設定を有効にする手順については、一般設定 (ページ 54) をご参照ください。

▶ 例:

クライアントには、8 つのモニター (それぞれ 1920 x 1080) のマルチヘッド環境があり、下記のように配置されています。

1	2	3	4
5	6	7	8

KVM セッションは、3840 x 1080 のターゲット解像度でモニター 6 で起動されます。クライアントウィンドウはモニター 6 と 7 でネイティブ解像度で開き、両方のモニターを 100%カバーします。

クライアント起動設定

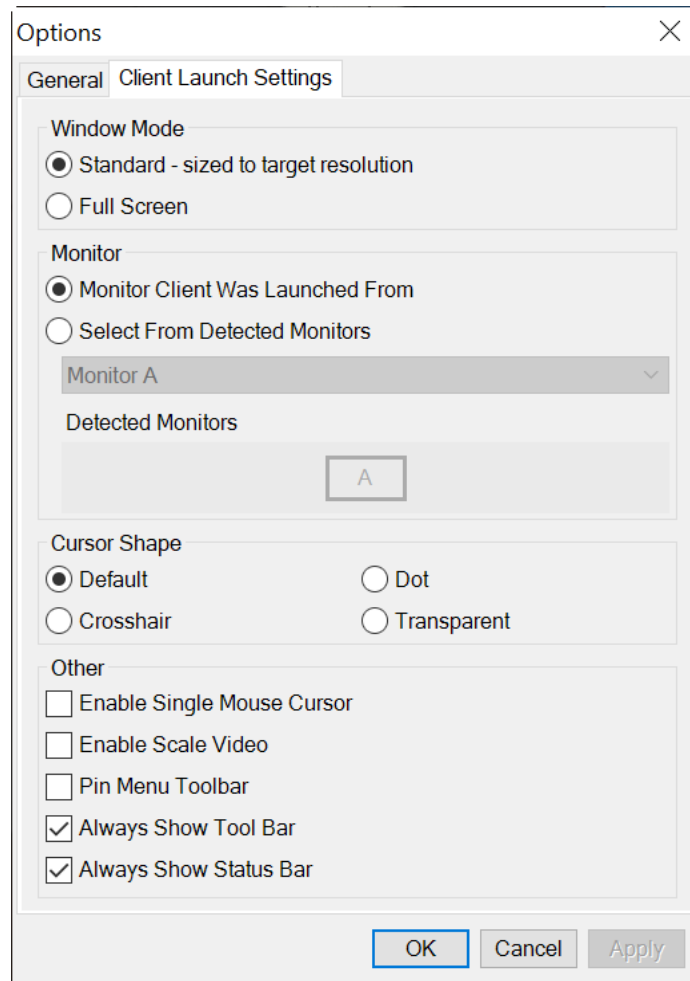
クライアント起動設定を構成すると、KVM セッションの画面設定を定義できます。

▶ クライアント起動設定の方法

1. [ツール] > [オプション] をクリック。 [オプション] ダイアログが表示されます。
 2. [クライアント起動設定] タブをクリックします。
 - ターゲットウィンドウの設定を構成するには、下記の手順を実行します：
 - ターゲットの現在の解像度を使用してウィンドウを開くには、「標準 - ターゲットの解像度に合わせたサイズ」を選択。ターゲット解像度がクライアント解像度より大きい場合、ターゲットウィンドウは可能な限り多くの画面領域をカバーし、必要に応じてスクロールバーが追加されます。
 - ターゲットウィンドウを全画面モードで開くには、「全画面」を選択。
- ターゲットビューアーを起動するモニターを構成するには、下記の手順を実行します：
- クライアントで使用されているアプリケーション（例：Web ブラウザやアプレット）と同じディスプレイを使用してターゲットビューアーを起動する場合は、[モニタークライアントの起動元] を選択。
 - 「検出されたモニターから選択」を使用して、アプリケーションによって現在検出されているモニターのリストから選択。以前に選択したモニターが検出されなくなった場合、「現在選択されているモニターが検出されませんでした」と表示されます。
 - カーソルの形状を構成方法：
 - デフォルトの矢印、ドット、クロスヘア、または透明を選択して、全てのセッションのカーソルの形状を設定します。マウスメニューを使用して、セッション中にカーソル形状を変更します。
 - 追加の起動設定の構成方法：

- サーバーへのアクセス時に、デフォルトのマウスモードとしてシングルマウスモードを有効にするには、[シングル カーソル モードを有効にする] を選択します。
- [ビデオのスケールリングを有効にする] を選択して、アクセス時にターゲットサーバーの表示を自動的にスケールリングします。
- ターゲットがフルスクリーンモードのときに、ツールバーを表示したままにする場合は[ピンメニューツールバー] を選択。デフォルトでは、ターゲットが全画面モードの場合、メニューは画面の上部にマウスを置いたときのみ表示されます。
- ツールバーを常に表示及び、ステータスバーの常に表示は、クライアントにアクセスしているコンピューターに保存されている、ユーザーごとの設定です。その為、別コンピューターを使用すると、設定が異なる場合があります。選択すると、ツールバーとステータスバーがデフォルトで表示されたままになり、選択を解除すると、ツールバーとステータスバーがデフォルトで非表示となります。

3. [OK] をクリック。



ターゲットの診断スナップショットの収集

管理者は、ターゲットの「スナップショット」を収集できます。

「スナップショット」機能は、ターゲットからログファイルとイメージファイルを生成します。

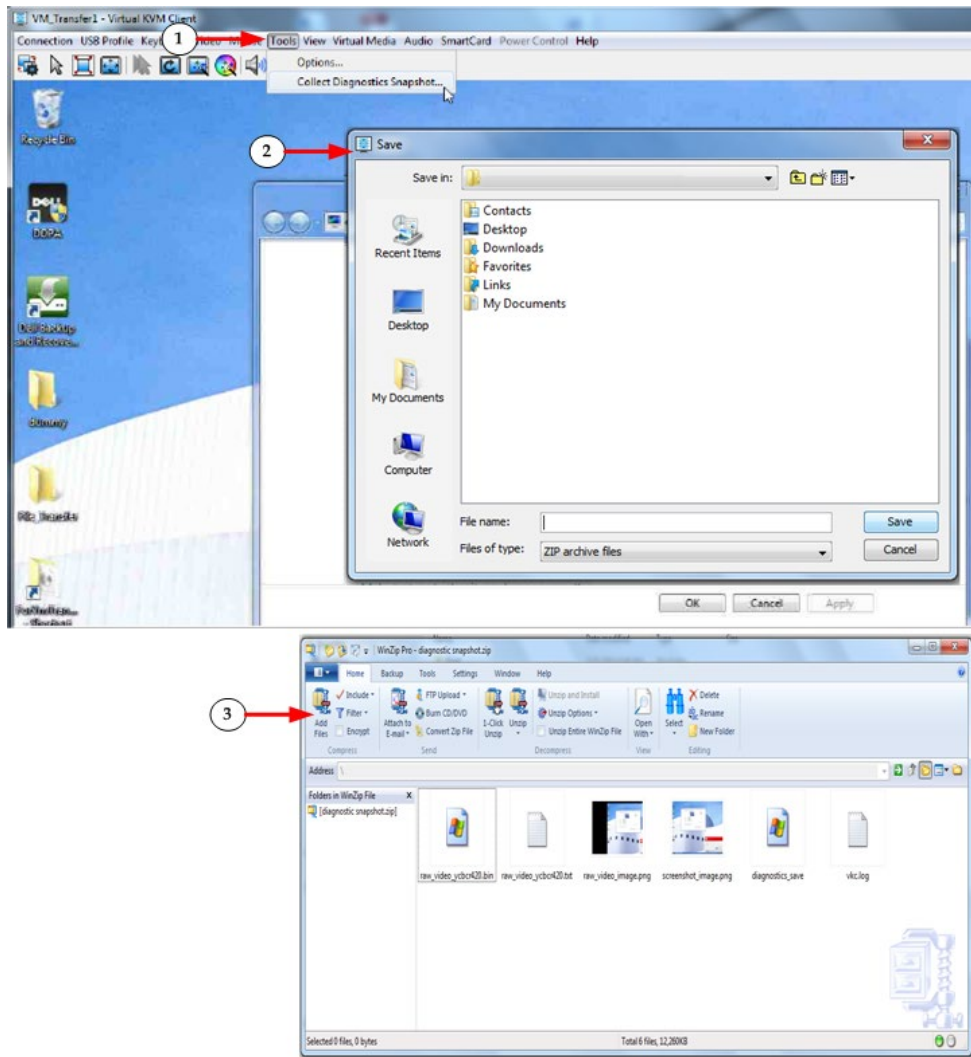
次にこれらのファイルを zip ファイルにバンドルして、テクニカルサポートチームへ送り、発生する可能性のある技術的な問題の診断に役立てることができます。

ファイルには、下記のファイルが含まれています。

- screenshot_image.png
これは発生している問題の写真を、キャプチャするターゲットのスクリーンショットです。この機能は「ターゲットからのスクリーンショット」機能と同様に動作します。
- raw_video_image.png:
生のビデオデータから作成されたスナップショット画像。あたかも「定期的な」画面更新であるかのように、クライアントの後処理が適用されることに注意してください。
- raw_video_ycber420.bin:
生のスナップショットのバイナリファイル。
- raw_video_ycber420.txt:
問題の診断に使用される、データを含むテキストファイル。
- Log.txt file:
これらはクライアントログです。
情報のキャプチャを有効にしていない場合でも、ログが含まれることに注意してください。この場合、VNC は内部メモリを使用して情報をキャプチャします。

診断スナップショットを収集する

▶ 診断スナップショットのキャプチャ方法:



Steps	
①	ターゲットにアクセスし[Tools] > [Collect Diagnostics Snapshot] をクリックします。情報が収集されると、いくつかのメッセージが表示されます。
②	診断ファイルを含む zip ファイルを保存するように求められます。
③	診断ファイルを含む zip ファイルが保存されます。

オプションの表示

ツールバーを表示

ツールバー表示の有無に関わらず、仮想 KVM クライアントを使用できます。

▶ ツールバー表示の切り替え方法 (オンとオフ):

- [表示] > [表示ツールバー] を選択。

ステータスバーを表示

デフォルトでは、ステータスバーはターゲットウィンドウの下部に表示されます。

▶ ステータスバーの非表示方法:

- [表示] > [ステータス バー] をクリックして選択を解除。

▶ ステータスバーの復元方法:

- [表示] > [ステータス バー] をクリックして選択。

スケーリング

ターゲットウィンドウを拡大縮小すると、ターゲットサーバーウィンドウの内容全体を表示できます。

この機能は、仮想 KVM クライアントのウィンドウサイズに合わせてターゲットビデオのサイズを拡大または縮小し、スクロールバーを使用せずにターゲットサーバーデスクトップ全体が表示されるように、アスペクト比を維持します。

▶ スケーリングの切り替え方法 (オンとオフ)

- [表示] > [スケーリング] を選択

フルスクリーンモード


スクリーンモードに入ると、ターゲットのフルスクリーンが表示され、ターゲットサーバーと同じ解像度が取得されます。

このモードを終了する為に使用するホットキーは、オプションダイアログで指定します。
[ツールオプション 『54 ページ』]をご参照下さい]

全画面モードでマウスを画面上部に移動すると、全画面モードメニューバーが表示されま
す。

フルスクリーンモードで、メニューバーを表示したままにする場合は[ツール オプション]、
ダイアログから [メニュー ツールバーをピン留め] オプションを有効にします。「ツール
オプション (54 ページ)」をご参照ください」

▶ フルスクリーンモードの設定方法:

- 「表示」>「全画面表示」を選択するか、「全画面表示」ボタンをクリックします 。

▶ フルスクリーンモードの終了方法:

ツールのオプションダイアログで設定されたホットキーを押します。デフォルトは
Ctrl+Alt+M です。

常にフルスクリーンモードでターゲットにアクセスしたい場合は、フルスクリーンモード
をデフォルトにすることができます。

▶ フルスクリーンモードをデフォルトモードとして設定:

1. [ツール] > [オプション] をクリックして、[オプション] ダイアログを開きます。
2. [フルスクリーンモードでの起動を有効にする] を選択し、[OK] をクリックします。


仮想メディア

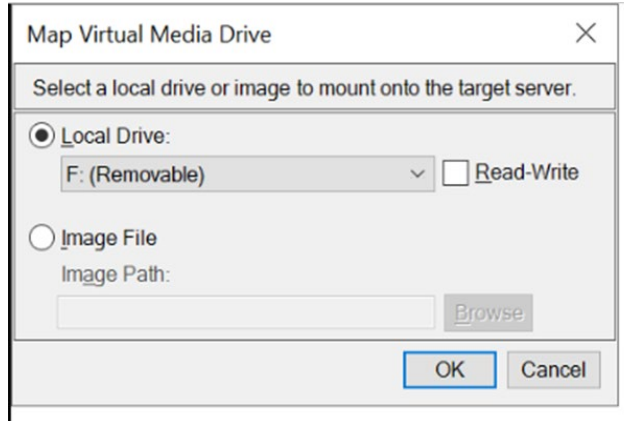
クライアントコンピュータの仮想メディアドライブへのアクセス

重要: 仮想メディアドライブに接続して、ファイル転送、アップグレード、インストール、ま
たはその他の同様のアクションを実行する場合、KVMクライアントでマウスモードを変更
しないでください。これを行うと、仮想メディアドライブでエラーが発生したり、仮想メディ
アドライブに障害が発生したりする可能性があります。

- ▶ クライアントコンピューターの仮想メディアドライブにアクセスするには、下記の手順を実行します。

1. KVM クライアントから、[仮想メディア] > [ドライブの接続] を選択するか、[ドライブの接続...]

ボタン  をクリックします。[仮想メディア ドライブのマップ] ダイアログが表示されます。



2. [ローカドライブ] ドロップダウンリストからドライブを選択します。
読み取り及び、書き込み機能が必要な場合、読み取り/書き込みチェックボックスを選択。

このオプションは、リムーバブルでないドライブでは無効になっています。詳細については、読み取り/書き込みが利用できない状態について『171 ページ』をご参照下さい。

チェックすると、接続された USB ディスクの読み取り、または書き込みが可能になります。

警告: 読み取り/書き込みアクセスの有効は危険を伴います! 複数のエンティティから同ドライブに同時アクセスすると、データが破損する恐れがあります。書き込みアクセスが必要ない場合は、このオプションを選択しないでください。

3. [OK] をクリックします。メディアはターゲットサーバーに仮想的にマウントされます。他のドライブと同じようにメディアにアクセスできます。

仮想メディアイメージファイルへのアクセス

「イメージ ファイル」オプションを使用して、リムーバブルディスクのディスクイメージにアクセスします。

▶ 画像ファイルのガイドライン:

- Linux で dd (dd if=/dev/sdb of=disk.img) を使用して作成されたイメージファイル、または Windows の Win32 Disk Imager や Mac ディスクユーティリティなどの同様のツールがサポートされています。
- Apple DMG ファイル:
 - FAT32 USB ドライブの DMG イメージ ファイルは、全ての OS で認識されます。

- Mac ドライブ上のフォルダーの DMG イメージ ファイルは、Mac OS ターゲットでのみ認識されます。
- イメージは、次の設定を使用して Mac ディスクユーティリティで作成する必要があります。→ 暗号化: なし。画像フォーマット: 読み取り/書き込み。
- サポートされていない: 暗号化または圧縮された dmg イメージ、MacOS インストールイメージ、Apple サポートサイトからダウンロードした DMG ファイル。

▶ 仮想メディアイメージファイルのアクセス方法


1. KVM クライアントから [仮想メディア] > [ドライブの接続] を選択するか [ドライブの接続...] ボタンをクリックします。[仮想メディアドライブのマップ] ダイアログが表示されます。
2. [画像ファイル] オプションを選択し、[参照] をクリックして .img または .dmg ファイルを見つけて選択します。
3. [OK] をクリックします。メディアはターゲットサーバーに仮想的にマウントされます。

CD-ROM/DVD-ROM/ISO イメージのマウント

オプションは、CD-ROM、DVD-ROM、及び ISO イメージをマウントします。

注意: ISO9660 形式がサポートされている標準です。ただし、他の CD-ROM 拡張機能も機能する場合があります。

▶ CD-ROM、DVD-ROM、または ISO イメージにアクセスする方法:

1. KVM クライアントから、[仮想メディア] > [CD-ROM/ISO イメージの接続] を選択するか  [CD ROM/ISO の接続] ボタンをクリックします。 [仮想メディア CD/ISO イメージのマッピング] ダイアログが表示されます。
2. 内蔵および外付けの CD-ROM、または DVD-ROM ドライブの場合:
 - a. [ローカル CD/DVD ドライブ] オプションを選択します。
 - b. [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と外部 CD 及び、DVD ドライブ名がドロップダウンリストに入力されます。
 - c. [OK] をクリック。
3. ISO イメージの場合:
 - a. ISO イメージオプションを選択します。 CD、DVD、またはハードドライブのディスクイメージにアクセスする場合は、このオプションを使用します。 ISO 形式がサポートされている唯一の形式です。
 - b. [参照] をクリック。
 - c. 使用するディスクイメージを含むパスに移動し、[開く] をクリックします。パスが [イメージ パス] フィールドに入力されます。
 - d. [OK] をクリック。
4. ファイルサーバー上のリモート ISO イメージの場合:
 - a. [リモートサーバーISO イメージ] オプションを選択。

- 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。使用可能なファイルサーバーとイメージパスは、仮想メディア共有イメージページを使用して構成したものです。[仮想メディア共有イメージ] ページを使用して構成したアイテムのみがドロップダウンリストに表示されます。
- c. ファイルサーバーユーザー名 - ファイルサーバーへのアクセスに必要なユーザー名。名前には、my domain/username 等のドメイン名を含めることができます。
- d. ファイルサーバー パスワード - ファイルサーバーへのアクセスに必要なパスワード (入力時にフィールドはマスクされます)。
- e. [OK] をクリック。

メディアはターゲットサーバーに仮想的にマウントされます。他のドライブと同じようにメディアにアクセスできます。

注意: Linux® ターゲットでファイル进行操作している場合、仮想メディアを使用してファイルをコピーした後で Linux Sync コマンドを使用して、コピーされたファイルを表示します。同期が実行されるまで、ファイルが表示されない場合があります。

注意: Windows 7® OS® を使用している場合、ローカル CD/DVD ドライブ、ローカル、またはリモート ISO イメージをマウントすると、リムーバブルディスクはデフォルトで Windows の [マイコンピュータ] フォルダに表示されません。

このフォルダ内のローカル CD/DVD ドライブ、ローカルまたはリモート ISO イメージを表示するには、[ツール] > [フォルダ オプション] > [表示] を選択し、[コンピュータフォルダの空のドライブを非表示にする] の選択を解除します。

仮想メディアドライブから切断

▶ 仮想メディアドライブの切断方法:

- ローカルドライブの場合は、[仮想メディア] > [ドライブの切断] を選択します。
- CD-ROM、DVD-ROM、及び ISO イメージの場合、[仮想メディア] > [CD-ROM/ISO イメージの切断] を選択。

注意: 切断コマンドを使用して仮想メディアを切断するだけでなく、KVM 接続を閉じるだけで仮想メディアも閉じられます。

デジタルオーディオ





Dominion KX IV-101 は、HDMI 経由のオーディオ再生をサポートします。

サポートされているオーディオのデバイスフォーマット

下記の再生形式がサポートされています:

- ステレオ, 16bit, 44.1K
- ステレオ, 16bit, 32K
- ステレオ, 16bit, 48K

デジタルオーディオ VKC と AKC アイコン

オーディオアイコン	アイコン名	内容
  	スピーカー	これらのアイコンはクライアント ウィンドウの下部にあるステータスバーにあります。 緑の点滅する波は、オーディオ再生セッションが現在ストリーミング中であることを示します。 セッションがミュートされると、黒いスピーカー アイコンが表示されます。 オーディオが接続されていない場合、アイコンはグレー表示されます。
	マイク	再生はサポートされていません。マイクアイコンがグレー表示されます。

オーディオ再生の推奨事項と要件

▶ オーディオレベル:

- ターゲットのオーディオレベルを中音域に設定します。
- 例: Windows® クライアントでは、オーディオを 50 以下に設定します。
- この設定は、クライアントオーディオデバイスコントロールからではなく、再生デバイスから構成する必要があります。

帯域幅の要件

下記の表は、選択した各フォーマットで音声を送信する為の、オーディオ再生帯域幅要件の詳細です。

音声フォーマット	ネットワーク帯域幅の要件
44.1 KHz, 16bit ステレオ	176 KB/s
32 KHz, 16bit ステレオ	128KB/s
48 KHz, 16bit ステレオ	192KB/s

実際には、オーディオ デバイスがターゲットに接続するとき使用される帯域幅は、ターゲットでオーディオアプリケーションを開いて使用するときキーボードとビデオデータが消費される為、より大きくなります。

一般的な推奨事項は、オーディオ/ビデオを実行する前に少なくとも、1.5MB の接続の確立。ただし、ターゲットの高い画面解像度を使用したビデオコンテンツのフルカラー接続は、はるかに多くの帯域幅を消費し、音声の品質に大きな影響を与えます。

品質の低下を軽減する為に、低帯域幅での音声品質へのビデオの影響を軽減及び、推奨されるクライアント設定がいくつかございます：

- 低品質フォーマットで音声再生を接続します。帯域幅を消費するビデオの影響は、44k よりも 11k 接続の方がはるかに目立ちません。
- [接続プロパティ] の下の接続速度を、クライアントからサーバーへの接続に対して最適な値に設定します。

[接続プロパティ] で、色深度をできるだけ低い値に設定します。色深度を 8 ビットカラーに減らすと、消費される帯域幅が大幅に削減されます。

オーディオ設定の保存

オーディオデバイス設定は、Dominion KX IV-101 デバイスごとに適用されます。

オーディオデバイスの設定を構成して Dominion KX IV-101 に保存すると、同じ設定が適用されます。

(例) Windows® オーディオ デバイスをステレオ、16 ビット、44.1K 形式として使用するように構成できます。

様々なターゲットに接続して、その Windows オーディオデバイスを使用すると、ステレオ、16 ビット、44.1K フォーマットが各ターゲットサーバーに適用されます。

全てのデバイスについて、デバイスタイプ、デバイスフォーマット、およびデバイスに適用されているバッファ設定が保存されます。

オーディオ デバイスへの接続と構成については、デジタルオーディオデバイスの接続と切断 『69 ページ』を、オーディオデバイスのバッファ設定については、バッファサイズの調整 (オーディオ設定) をご参照ください。

複数のユーザーが、ターゲット上の同じオーディオデバイスに同時にアクセスできるように、PC 共有モードと VM 共有モードの実行中にオーディオ機能を使用している場合、セッションを開始するユーザーのオーディオ デバイス設定は、セッションに参加する全てのユーザーに適用されます。

その為、ユーザーがオーディオ セッションに参加すると、ターゲット機器の設定が使用されます。

オーディオデバイスの接続と切断

オーディオデバイス設定は、Dominion KX IV-101 デバイスごとに適用されます。

オーディオデバイス設定を構成して、Dominion KX IV-101 に保存すると、同じ設定が適用されます。

詳細については、オーディオ設定の保存 『ページ 68』を参照してください。

デジタルオーディオデバイスに接続

▶ オーディオデバイスへの接続方法:

1. Dominion KX IV-101 へのブラウザ接続を開始する前に、オーディオデバイスをリモートクライアント PC に接続します。
2. ポートアクセスページからターゲットに接続。

3. 接続後、ツールバーの [Audio] ボタン  をクリック。

[オーディオ デバイスの接続] ダイアログが表示されます。リモートクライアント PC に接続されている、使用可能なオーディオデバイスのリストが表示されます。

注意: リモートクライアント PC に接続されている使用可能なオーディオ デバイスがない場合、オーディオアイコンはグレー表示されます。


4. 再生デバイスに接続している場合、[再生デバイスの接続] をオンにします。
5. ドロップダウンリストから、接続するデバイスを選択。
6. [フォーマット] ドロップダウンから再生デバイスのオーディオフォーマットを選択。

注意: 使用可能なネットワーク帯域幅に基づいて、使用する形式を選択してください。サンプリングレートが低い形式では、帯域幅の消費が少なくなり、ネットワークの輻輳を許容できる可能性があります。

7. 「ターゲットへの接続時に選択した再生デバイスを自動的にマウントする」チェックボックスを選択すると、オーディオ対応のターゲットに接続した時に、オーディオ再生デバイスが自動的に接続されます。
8. [OK] をクリック。オーディオ接続が確立されると、確認メッセージが表示されます。[OK] をクリック。


接続が確立されなかった場合、エラーメッセージが表示されます。

オーディオ接続が確立されると、[オーディオ] メニューが [オーディオの切断] に切り替わります。オーディオデバイスの設定が保存され、オーディオデバイスへの以降の接続に適用されます。

スピーカーアイコン  は、クライアントウィンドウの下部にあるステータスバーに表示されます。オーディオが使用されていない時はグレー表示されます。

オーディオデバイスから切断

▶ オーディオデバイスからの切断方法:

- ツールバーの [オーディオ] アイコンをクリック  して、切断を確認するメッセージが表示されたら [OK] を選択します。確認メッセージが表示されます。[OK] をクリックします。

キャプチャと再生のバッファサイズを調整する (オーディオ設定)

オーディオデバイスを接続すると、必要に応じてバッファサイズを調整できます。

この機能は、帯域幅の制限やネットワークスパイクの影響を受ける可能性のある、オーディオ品質を制御するのに役立ちます。

バッファサイズを増やすと音質は向上しますが、配信速度に影響する可能性があります。

使用可能な最大バッファサイズは 400 ミリ秒です。これを超えると、オーディオ品質に大きく影響する為です。

バッファサイズは、オーディオ セッション中など、必要に応じていつでも調整できます。

オーディオ設定は VVC または AKC で構成されます。

オーディオ設定について

▶ オーディオ設定の調整方法:

1. [Audio] メニューから [Audio Settings] を選択します。
2. [オーディオ設定] ダイアログが開きます。
3. 必要に応じて、キャプチャや再生バッファサイズを調整します。
4. [OK] をクリックします。



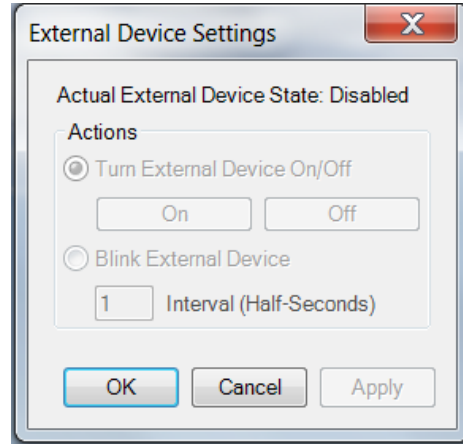
外部機器

[External Device] メニューでは、Dominion KX IV-101 の端子台に接続されているデバイスを制御できます。

▶ 外部機器の設定:

1. [External Device] > [Settings] を選択してダイアログを表示します。
2. デバイスの状態がリストされます。
3. 有効なデバイスは、アクションオプションを使用して制御できます。

- 外部デバイスのオン/オフ: 「オン」または「オフ」をクリックして、ターミナル出力リレーを制御します。
- 外部デバイスの点滅: 外部デバイスの点滅を制御する為、0.5 秒間隔と入力します。



4. [OK] または [適用] をクリックして保存。

バージョン情報 - 仮想 KVM クライアント

Raritan のテクニカルサポートが必要な場合の、クライアントのバージョン情報について :

- [ヘルプ]> [Raritan 仮想 KVM クライアントについて] を選択。

アクティブ KVM クライアント (AKC) のヘルプ

AKC を起動するには、ブラウザに `https://<IP アドレス>/akc` と入力します。

アクティブ KVM クライアント (AKC) は、Microsoft Windows .NET*テクノロジーに基づいています。

これにより、Java を使用しない Windows 環境でクライアントを実行。

AKC は、以下を除いて VKC と同じ機能を提供します :

- AKC で作成されたキーボードマクロは、他のクライアントでは使用不可。
- ダイレクトポートアクセス構成
- AKC サーバー認定検証構成 (「AKC を使用する為の前提条件 『72 ページ』」を参。)

機能の使用の詳細については、仮想 KVM クライアント (VKC) のヘルプをご参照下さい。

概要

アクティブ KVM クライアント (AKC) は、Microsoft Windows.NET®テクノロジーに基づいています。

これにより、Java を使用しない Windows 環境でクライアントを実行できます。

- AKC は、以下を除いて VKC と同じ機能を提供します：
- AKC で作成されたキーボードマクロは、他のクライアントでは使用不可。
- ダイレクトポートアクセス構成

AKC サーバー認定検証構成（「AKC を使用する為の前提条件 『72 ページ』」を参照）

機能の使用の詳細については、仮想 KVM クライアント (VKC) ヘルプをご参照下さい。

AKC がサポートする Microsoft.NET Framework

アクティブ KVM クライアント (AKC) には Windows.NET®が必要です。

サポートされているリリースノートをご参照下さい。

AKC がサポートするブラウザ

サポートされているブラウザのバージョンについては、リリースノートをご参照下さい。

AKC がサポートする OS

Internet Explorer の起動、アクティブ KVM クライアント (AKC) を使用して、Dominion KX IV-101 を介してターゲットサーバーにアクセスできます。

AKC は下記のプラットフォームと互換性があります。

- Windows7®オペレーティングシステム (最大 64 ビット)
- Windows8®オペレーティングシステム (最大 64 ビット)
- Windows10®オペレーティングシステム (最大 64 ビット)

AKC を使用する為の前提条件

クッキーの許可

アクセスされているデバイスの IP アドレスからの、クッキーが現在ブロックされていない事を確認してください。

Dominion KX IV-101 の IP アドレスを「信頼済みサイトゾーン」に含める

Windows7 ユーザーは、アクセスされているデバイスの IP アドレスが、ブラウザの信頼済みサイトゾーンに含まれていることを確認する必要があります。

「保護モード」を無効

Windows7 ユーザーは、このデバイスにアクセス時に保護モードがオンになっていないことを確認する必要があります。

最新の Edge Chromium 86.0.622.51

新しい Edge Chromium ブラウザには、AKC で有効にする必要がある実験的な Click Once サポートがあります。ブラウザは Click Once のサポートを検出しないため、AKC を手動でダウンロードする必要があります。

- Edge で Click Once を有効にするには：ブラウザに edge :// flags と入力し、Click Once サポートを検索し、有効に設定してブラウザを再起動します。
- AKC を手動でダウンロードするには：Dominion KX IV-101 URL (https :// (KX-IP-Hostname) / ake など) に移動し、Click Once サポートが検出されなかった事を示すメッセージで[ここをクリックしてください] を選択。
-

プロキシサーバーの構成

プロキシサーバーの使用が必要な場合は、リモートクライアント PC で SOCKS プロキシも提供・構成する必要があります。

注意：インストールされているプロキシサーバーが HTTP プロキシプロトコルのみに対応している場合、接続できません。

▶ SOCKS プロキシの設定方法：

1. リモートクライアント PC で、[コントロールパネル]> [インターネットオプション] を選択。
 - a. [接続] タブで、[LAN 設定] をクリックします。 [ローカルエリアネットワーク (LAN) 設定] ダイアログが開きます。
 - b. [LAN にプロキシサーバーを使用する] を選択。
 - c. [詳細] をクリックします。 [プロキシ設定] ダイアログが開きます。
 - d. 全てのプロトコルのプロキシサーバーを構成します。

重要：「すべてのプロトコルに同じプロキシサーバーを使用する」を選択しないでください。

注意：SOCKS プロキシ (1080) のデフォルトのポートは、HTTP プロキシ (3128) とは異なります。

- e. 各ダイアログで [OK] をクリックして、設定を適用します。
- f.
2. 次に、Java アプレットのプロキシ設定を構成します。
 - a. 「コントロールパネル」> 「Java」を選択。
 - b. [全般] タブで、[ネットワーク設定] をクリックします。 [ネットワーク設定] ダイアログが開きます。
 - c. 「プロキシサーバーを使用する」を選択。
 - d. [詳細] をクリック。 [ネットワークの詳細設定] ダイアログが開きます。
 - e. 全てのプロトコルのプロキシサーバーを構成。

重要：「すべてのプロトコルに同じプロキシサーバーを使用する」を選択。

注意：SOCKS プロキシ (1080) のデフォルトのポートは、HTTP プロキシ (3128) とは異なります。

HTML KVM クライアント (HKC)

HTML KVM クライアント (HKC) は、アプレットやブラウザプラグインを必要とせず、ブラウザで実行される KVM over IP アクセスを提供します。HKC は Java ではなく JavaScript を使用。

HKC は、Linux と Mac クライアントと Internet Explorer 11 (IE10 以前ではサポートされていません)、Edge、Firefox、Chrome、及び Safari ブラウザの Windows クライアントで実行されます。

・多くの KVM 機能がサポートされています。将来のリリースでは、より高度な KVM 機能が提供される予定です。

▶ サポートされている機能:

- 接続プロパティ
- 入力設定
- オーディオ再生
- 仮想メディア
- キーボードマクロ
- キーボードマクロのインポートとエクスポート
- ターゲットにテキストを送信
- キーボードとマウスの設定
- シングルマウスモード-IE ブラウザでは使用不可
- 外部機器

▶ サポートされていません:

- ビデオ設定
- クライアント起動設定、ターゲットホットキーからの切断の設定、またはツールバー表示の構成のためのツールメニュー。
- 限定的なキーボードサポート: 米国-英語、英国-英語、フランス語、およびドイツ語がサポートされています
- キーボードマクロのホットキー
- Sun ターゲット用に事前入力されたキーボードマクロ
- クライアント PC に存在するキー (米国-英語、英国-英語、フランス語、またはドイツ語) からのみマクロを作成でき、特別なファンクションキーは作成できません。
- シングルマウスモード-IE では使用不可
- 仮想メディアの書き込みはサポートされていません
- Chrome と Firefox ブラウザでのみサポートされるローカルファイル転送
- USB ドライブ接続
- オーディオキャプチャ

▶ 既知問題:

- HKC が読み込まれず、白い画面が表示される場合、ブラウザのメモリがいっぱいになっている可能性があります。全てのブラウザウィンドウを閉じて、再試行してください。

接続プロパティ

接続プロパティは、ターゲットサーバーへのリモート接続を介したストリーミングビデオのパフォーマンスを管理。

プロパティは接続にのみ適用されます。同じターゲットサーバーにアクセスする他のユーザーの接続には影響しません。

接続プロパティに変更を加えた場合、それらはクライアントによって保持されます。

▶ 接続プロパティの表示方法:

- [File]> [Connection Properties] を選択。

▶ ビデオのエンコード

このセクションでは、ビデオのエンコードアルゴリズムと品質設定を選択します。

- 使用法：一般的なアプリケーション領域を指定します。この選択により、このダイアログの他の場所で使用可能な選択肢が最適化されます。
 - 汎用ビデオ：映画、ビデオゲーム、アニメーションなど、スムーズな色再現が最も重要なビデオコンテンツ。
 - コンピューターと IT アプリケーション：コンピューターのグラフィカルインターフェイス等、テキストの鮮明さと明瞭さが重要なビデオコンテンツ。

- エンコーダモード：8つのボタンの列からエンコーダモードを選択します。オプションは、使用法の選択によって異なります。一般的に、ボタンバーの左側にあるモードは、より高い画質を提供しますが、より高い帯域幅を消費し、ネットワーク速度やクライアントのパフォーマンスによってはフレームレートが低下する可能性があります。逆に右に向かうにつれて、画質の低下を犠牲にして、より低い帯域幅を消費します。ネットワークまたはクライアントに制約のある状況では、右側のモードの方がフレームレート向上になる場合があります。

デフォルトのビデオモードは常に「フルカラー2」です。これは高品質モードであり、LAN環境での殆どの使用に適しています。必要に応じて、更に右側のモードを試行して、画質とフレームレートの適切なバランスを見つけてください。

▶ カラーサブサンプリング

カラーサブサンプリングは、エンコードされたビデオストリームの色情報を減らします。

- 自動：推奨されています。最適なカラーサブサンプリングモードは、ビデオエンコーディングセクションでの選択に基づいて、有効になります。
- 4:4:4：かなりの帯域幅コストで最高品質。グラフィカルユーザーインターフェイスの一部の状況を除いて、通常は必要ありません。1920x1200を超える解像度ではサポートされていない為、これらの解像度では、カラーサブサンプリングは自動的に4:2:2にドロップダウンします。
- 4:2:2：画質と帯域幅の適切なブレンド。
- 4:2:0：ネットワーク帯域幅とクライアント負荷の最大節約。高解像度のラインやテキストを強調しない殆どの汎用アプリケーションで、正常に機能します。

▶ 現在のステータス

現在のステータスには、リアルタイムのビデオパフォーマンス統計が含まれます。ダイアログで設定を変更すると、パフォーマンスへの影響をすぐに確認できます。

- ソース：着信ビデオソースの解像度とフレームレート。
- パフォーマンス：クライアントでレンダリングされる1秒あたりのフレーム数(FPS)、及び着信ビデオストリームのデータレート。これらの値は、ビデオ設定の効果を確認できる場所です。
- 暗号化：ビデオストリームが暗号化されているかどうか。暗号化されたストリームは通常、フレームレートと帯域幅が低くなります。暗号化は、セキュリティ→KVM セキュリティ→「暗号化モードをKVMおよび仮想メディアに適用する」のグローバル設定です。

接続情報

現在の接続に関するリアルタイムの接続情報については、[接続情報]ダイアログを開き、必要に応じてダイアログから情報をコピーします。

接続プロパティの構成については、デフォルトの接続プロパティをご参照下さい。

- デバイスの名前
- デバイスの IP アドレス
- ポート-デバイスへのアクセスに使用される KVM 通信 TCP / IP ポート
- データ入力/秒-デバイスから受信したデータレート
- データ出力/秒-デバイスに送信されるデータレート
- FPS-デバイスからの 1 秒あたりのビデオフレーム。
- 平均 FPS-1 秒あたりの平均ビデオフレーム数。
- 接続時間-現在の接続の継続時間。
- 水平解像度-ターゲットサーバーの水平解像度。
- 垂直解像度-ターゲットサーバーの垂直解像度。
- リフレッシュレート-ターゲットサーバーのリフレッシュレート。
- プロトコルバージョン-通信プロトコルバージョン。

▶ 接続情報の表示方法:

- [File]> [Connection Info] を選択。

Connection Info	
Device Name:	kx3-61-16
IP Address:	192.168.61.16
Port:	443
Data In/Second:	121 kB/s
Data Out/Second:	234 B/s
FPS:	17
Avg. FPS:	21.80
Connect Time:	00:00:25
Horizontal Resolution:	1024
Vertical Resolution:	768
Refresh Rate:	60 Hz
Protocol Version:	1.31

入力メニュー

キーボードレイアウト

▶ キーボード種類の設定方法

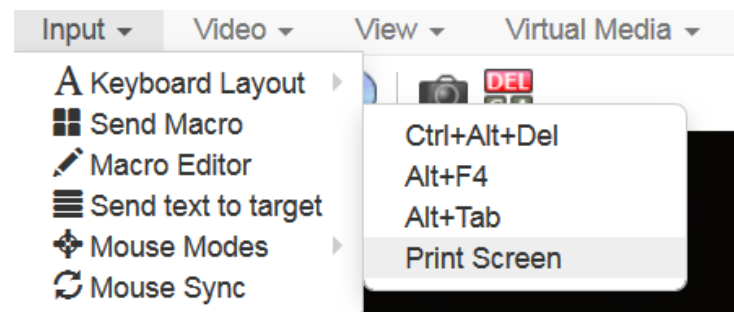
- [Input]> [Keyboard Layout] を選択してから、キーボードの種類を選択。
 - de-de
 - de-ch
 - en-gb
 - en-us
 - fr

マクロを送信

頻繁に使用する為、いくつかのキーボードマクロが事前にプログラムされています。

▶ 事前にプログラムされたマクロの送信方法:

- [Input]> [Send Macro] を選択してから、マクロを選択します。
 - Ctrl+Alt+Del: クライアントに影響を与えることなく、キーシーケンスをターゲットに送信。
 - Alt+F4: ターゲットサーバーのウィンドウを閉じます。
 - Alt+Tab: ターゲットサーバーで開いているウィンドウを切り替えます。
 - Print Screen (印刷画面) : のスクリーンショットを撮ります。



マクロの編集

キーボードマクロは、ターゲットサーバー向けのキーストロークの組み合わせがターゲットサーバーにのみ送信され、ターゲットサーバーによってのみ解釈されるようにします。そうしないと、クライアント PC によって解釈される可能性があります。

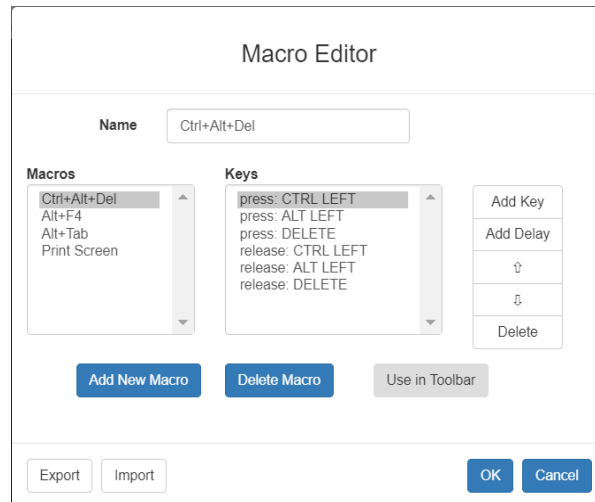
マクロはクライアント PC に保存され、PC 固有です。別 PC を使用している場合、マクロは表示されません。

さらに他の人があなたの PC を使用して、別の名前でログインした場合、マクロはコンピューター全体であるため、そのユーザーに表示されます。

HKC で作成されたマクロは、現在のブラウザと KVM デバイスでのみ使用可能。複数のブラウザまたは複数の Dominion KX IV-101 で HKC を使用する場合、マクロはブラウザとそれらが作成された Dominion KX IV-101 でのみ使用できます。マクロを別の Dominion KX IV-101 デバイスで再利用するには、マクロファイルをインポート及びエクスポートできます。「マクロのインポートとエクスポート」『p. 84』をご参照下さい。

▶ マクロエディタへのアクセス方法:

- [Input]> [Macro Editor] を選択。
- [マクロ] リストからマクロを選択して、キーの組み合わせを表示します。



新しいマクロの追加

▶ 新しいマクロの追加方法:

1. [Input]> [Macro Editor] を選択
2. [Add New Macro] をクリック

Macro Editor

Name

Macros

- Ctrl+Alt+Del
- Alt+F4
- Alt+Tab
- Print Screen
- New Macro

Keys

Add Key

Add Delay

↑

↓

Delete

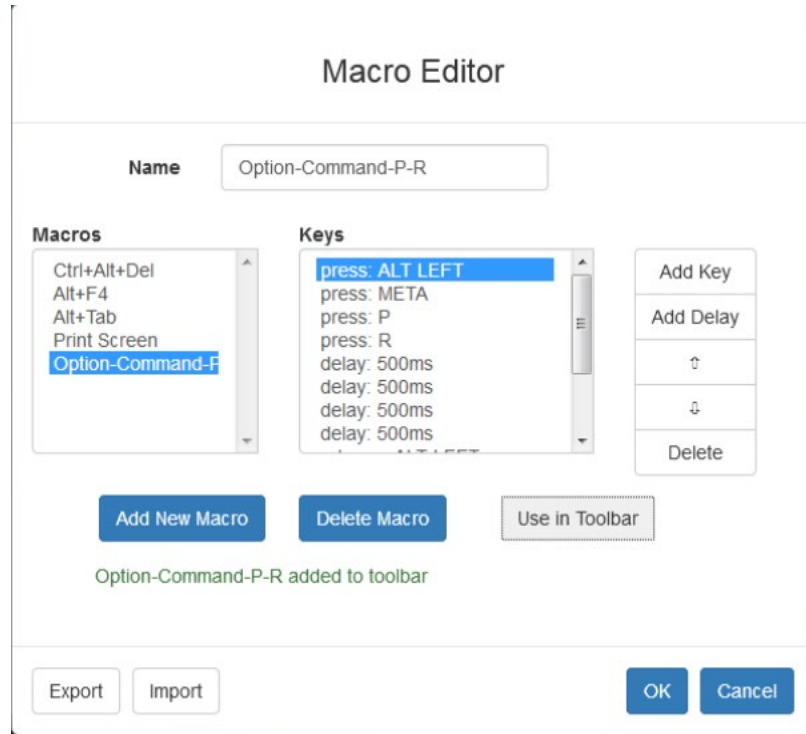
Add New Macro Delete Macro Use in Toolbar

Export

OK Cancel

3. 新しいマクロの名前を入力します。マクロが保存されると、名前が[マクロの送信]メニューに表示されます。
4. [Add New Macro] をクリックしてから、マクロに追加するキーを押します。キーを押す/キーを離すと、キーリストに表示されます。
 - 更にキーを追加するには、もう一度[キーの追加]をクリック、別のキーを押します。
 - キーを削除するには、[キー]リストでキーを選択し、[キーの削除]をクリック。
5. キーを正しい順序に配置するには、[キー]リストでキーをクリックして選択し、上下の矢印をクリックします。
6. キーシーケンスに 500 ミリ秒の遅延を追加するには、[遅延の追加]をクリックします。キーを押して放すシーケンスの途中での遅延は、キーを押し続けていることを示します。キーの長押しを示す為に、複数の遅延を追加します。上下の矢印をクリックして、遅延を正しい順序に移動します。

7. [OK]をクリックして保存します。ツールバーからこのマクロを使用するには、[ツールバーで使用]をクリックします。詳細については、「ツールバーへのマクロの追加『p. 82』」をご参照下さい。



この例は、2秒の遅延を必要とするMac起動シーケンスのマクロを示しています。

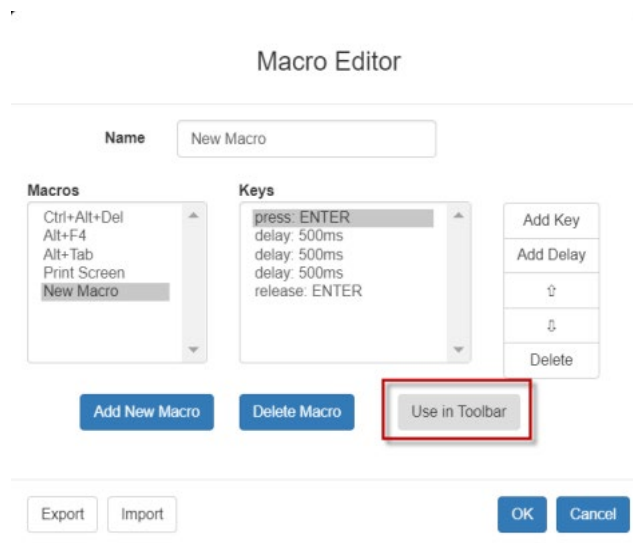
ツールバーにマクロを追加

HKC ツールバーに単一のマクロを追加して、アイコンをクリックして、マクロを使用出来るようになります。

▶ ツールバーにマクロの追加方法:

1. [Input]> [Macro Editor] を選択。
2. [マクロ]リストからマクロを選択。

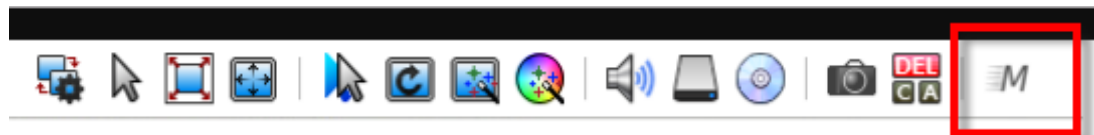
- [Use in Toolbar]をクリック。



- マクロがツールバーに追加されたことを、確認するメッセージが表示されます。
 - ツールバーからマクロを削除するには、[ツールバーから削除]をクリックするか、別のマクロを選択して[ツールバーで使用]をクリック。



- [OK]をクリックして、マクロエディタを終了します。マクロアイコンは、設定されるとツールバーに追加されます。



マクロの削除

▶ マクロの削除方法:

- [Input] > [Macro Editor] を選択。
- マクロを選択し、[Delete Macro]をクリック。
- [OK]をクリック。

Macro Editor

Name

Macros

- Ctrl+Alt+Del
- Alt+F4
- Alt+Tab
- Print Screen
- New Macro

Keys

Add Key

Add Delay

⇅

⇅

Delete

Add New Macro

Delete Macro

Use in Toolbar

Export

Import

OK

Cancel

マクロのインポートとエクスポート

HKC で作成されたマクロは、現在のブラウザと KVM デバイスでのみ使用可能。複数のブラウザまたは複数の Dominion KX IV-101 で HKC を使用する場合、マクロはブラウザとそれらが作成された、Dominion KX IV-101 でのみ使用可能。マクロを別の Dominion KX IV-101 機器で再利用するには、マクロファイルをインポート・エクスポートできます。HKC で作成されたインポート・エクスポートされたマクロファイルは、HKC とのみ互換性があり、AKC または VKC では使用できません。同様に、AKC または VKC で作成されたマクロファイルは、HKC で使用する為にインポートすることは出来ません。

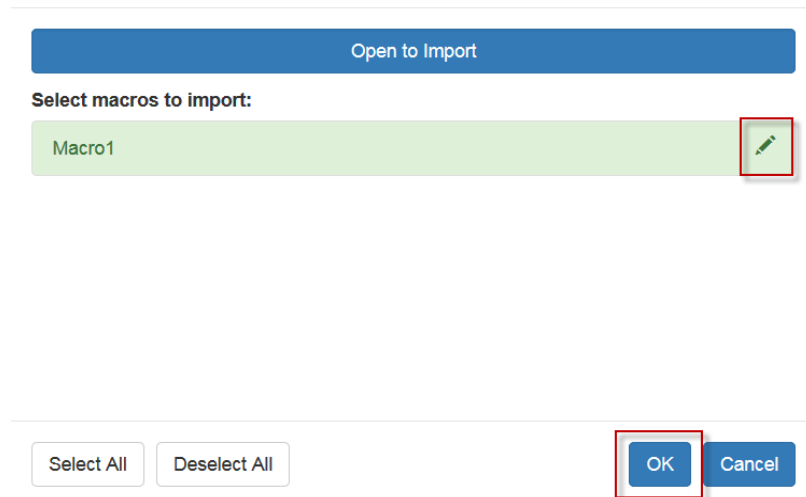
マクロは「usermacros.xml」という名前の xml ファイルにエクスポートされます。ファイルはブラウザのデフォルトのダウンロード場所に保存されます。デフォルトのマクロはエクスポートされません。

▶ マクロのインポートとエクスポート方法:

1. [Input]> [Macro Editor] を選択。ブラウザおよび Dominion KX IV-101 用に作成されたマクロのリストが[マクロエディタ]ダイアログに表示されます。
2. リストをエクスポートするには、[Export]ボタンをクリックして、ファイルを保存します。
3. マクロをインポートする Dominion KX IV-101 にログインします。
4. [Input]> [Macro Editor] を選択。
5. [Import]をクリックし、[開く] をクリックしてインポートし、usermacros.xml ファイルを選択して、[OK]をクリック。

6. ファイルで見つかったマクロがリストに表示されます。インポートするマクロを選択し、[OK]をクリック。
 - マクロ名は1つである必要があります。同じ名前のマクロが既に存在する場合、エラーメッセージが表示されます。[編集]アイコンをクリックしてマクロ名を変更し、チェックマークをクリックして名前を保存します。

Macro Import



ターゲットにテキストを送信

テキストをターゲットに直接送信するには、「テキストをターゲットに送信」機能を使用します。テキストエディタまたはコマンドプロンプトが開いていて、ターゲットで選択されている場合、テキストはそこに貼り付けられます。

▶ ターゲットへテキストを送信する方法:

1. [Input]> [Send text to target] を選択。[テキストをターゲットに送信] ダイアログが表示されます。
2. ターゲットに送信するテキストを入力。サポートされているキーボード文字のみ。
3. [OK]をクリック

マウスモード

シングルマウスモードまたは、デュアルマウスモードのいずれかで操作できます。

デュアルマウスモードで、オプションが適切に構成されている場合、マウスカーソルは整列します。

ターゲットサーバーを制御すると、リモートコンソールに 2 つのマウスカーソルが表示されます。1 つは Dominion KX IV-101 に属し、もう 1 つはターゲットサーバーに属します。

マウスカーソルが 2 つある場合、デバイスはいくつかのマウスモードを提供します。

- ずれないマウス (マウスの同期)
- インテリジェント(マウスモード)
- スタンダード (マウスモード)

マウスポインターが KVM クライアントのターゲットサーバーウィンドウ内にある場合、マウスの動きとクリックは接続されたターゲットサーバーに直接送信されます。

動作中は、マウスの加速設定により、クライアントのマウスポインターがターゲットのマウスポインターよりも僅かに進みます。

シングルマウスモードでは、ターゲットサーバーのポインターのみを表示できます。他のモードを使わない場合、シングルマウスモードを使用できます。

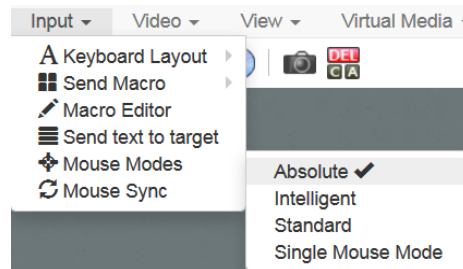
これらの 2 つのモード (シングルマウスとデュアルマウス) を切り替えることが可能。

ずれないマウス

- このモードは、ターゲットマウスが異なる加速度または速度に設定されている場合でも、ずれない特性を使用して、クライアントカーソルとターゲットカーソルの同期を維持します。

▶ ずれないマウスの設定方法:

- [Input]> [Mouse Modes]> [Absolute]を選択。

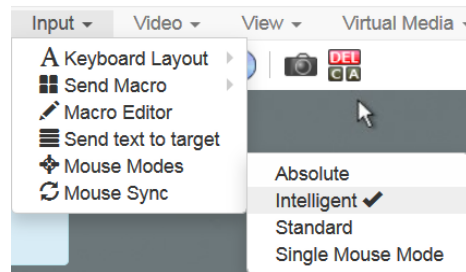


インテリジェント

インテリジェントマウスモードでは、デバイスはターゲットのマウス設定を検出し、それに応じてマウスカーソルを同期して、ターゲットでのマウスの加速を可能にします。

▶ **インテリジェントマウスモードの設定方法:**

- [Input]> [Mouse Modes]> [Intelligent]を選択します。マウスが同期します。
- 「インテリジェントマウス同期条件 『p. 52』」をご参照下さい。



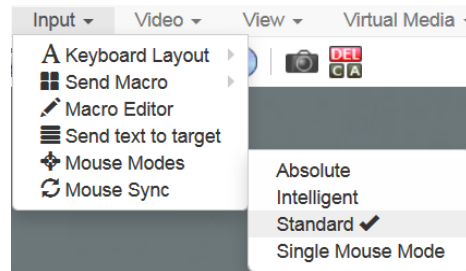
スタンダード

スタンダードマウスモードは、標準のマウス同期アルゴリズムを使用。アルゴリズムは、クライアントとターゲットサーバー上の相対的なマウスの位置を決定します。

クライアントとターゲットのマウスカーソルの同期を維持するには、マウスアクセラレーションを無効にする必要があります。更に特定のマウスパラメータを正しく設定する必要があります。

▶ **スタンダードマウスモードの設定方法:**

- [Input]> [Mouse Modes]> [Standard]を選択。



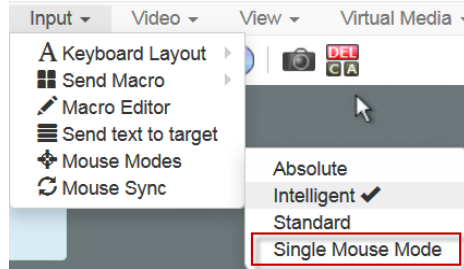
シングル

シングルマウスモードでは、ターゲットサーバーのマウスカーソルのみが使用されます。クライアントのマウスカーソルが画面から消えます。

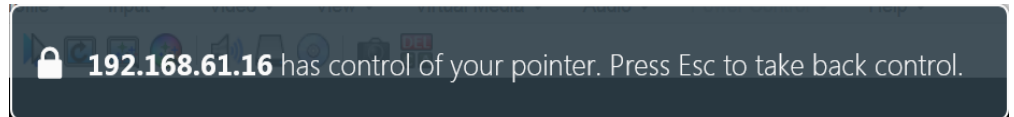
注意：クライアントが仮想マシンで実行されている場合、シングルマウスモードは Windows または Linux ターゲットでは機能しません。Internet Explorer ではシングルマウスモードは使用不可。

▶ シングルマウスモードの設定方法:

- [Input]> [Mouse Modes]> [Single Mouse Mode]を選択。



- クライアントウィンドウの上部にメッセージが表示されます。Esc キーを押してカーソルを表示します。



▶ シングルマウスモードの終了方法:

- Esc を押す。
- マウスモードがデュアルモードに戻ります。

マウスの同期

デュアルマウスモードでは、Synchronize Mouse コマンドは、ターゲットサーバーのマウスカーソルをクライアントのマウスカーソルに強制的に再配置します。

注意：このオプションは、スタンダードとインテリジェントマウスモードでのみ使用できます。

▶ マウスカーソルの同期方法:

- [Input]> [Mouse Sync] を選択。

インテリジェントマウスの同期条件

[マウス]メニューで使用できる[インテリジェントマウス同期] コマンドは、非アクティブ時にマウスカーソルを自動的に同期します。ただし、これが正しく機能するには、下記の条件を満たす必要があります。

- アクティブデスクトップは、ターゲットで無効にする必要があります。
- ターゲットページの左上隅に、ウィンドウが表示されないようにする必要があります。
- ターゲットページの左上隅に、アニメーションの背景があってはけません。
- ターゲットのマウスカーソルの形状は通常であり、アニメーション化されていない必要があります。
- ターゲットマウスの速度は、非常に遅い値/非常に高い値に設定しないでください。
- 「ポインターの精度の向上」や「ダイアログのデフォルトボタンにマウスをスナップ」等のターゲットの高度なマウスプロパティは無効にする必要があります。
- ターゲットビデオの端がはっきりと見える必要があります (=ターゲットビデオ画像の端までスクロールすると、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境界線が見えるはずです)。
- インテリジェントマウス同期機能を使用する場合、デスクトップの左上隅にファイルアイコン、またはフォルダーのアイコンがあると、機能が正常に動作しない場合があります。この機能の問題を確実に回避する為、デスクトップの左上隅にファイルアイコンや、フォルダーアイコンを置かないで下さい。

ターゲットビデオを自動検知した後、ツールバーの[マウスの同期]ボタンをクリックして、手動でマウスの同期を開始します。これはマウスカーソルが互いに非同期になり始めた場合、ターゲットの解像度に変更された場合も当てはまります。

インテリジェントマウスの同期が失敗した場合、このモードはスタンダードマウスの同期動作に戻ります。

マウスの構成は、ターゲットの OS によって異なることにご注意ください。Consult your OS 詳細については、OS のガイドラインをご参照下さい。また、インテリジェントなマウス同期は UNIX ターゲットでは機能しない事にご注意ください。

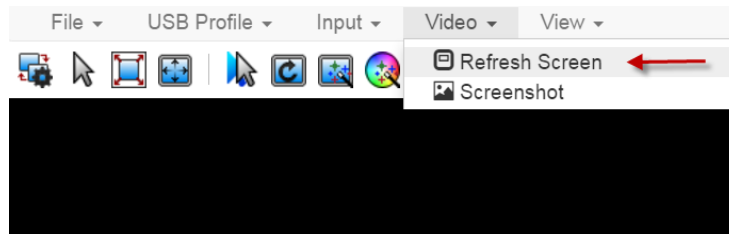
ビデオメニュー

画面の更新

[Refresh Screen] コマンドは、ビデオ画面を強制的に更新します。

▶ ビデオ画面を強制的に更新する方法:

- [Video]> [Refresh Screen] を選択。

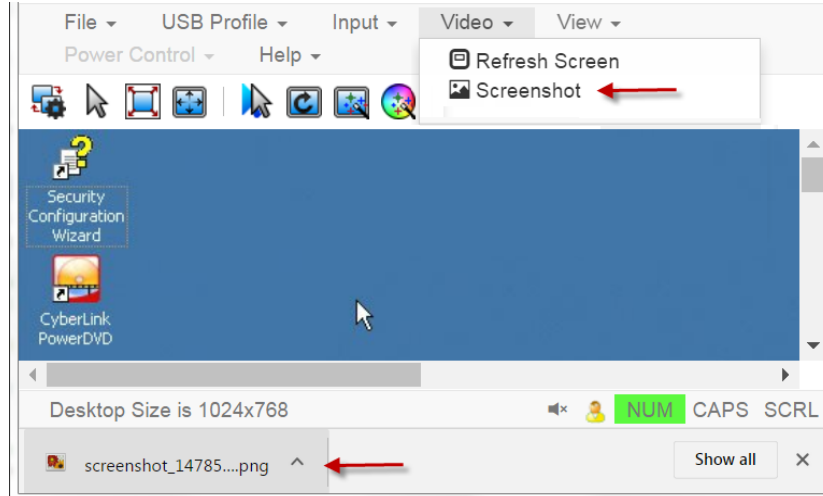


スクリーンショット

スクリーンショットコマンドを使用して、ターゲットサーバーのスクリーンショットを撮ります。

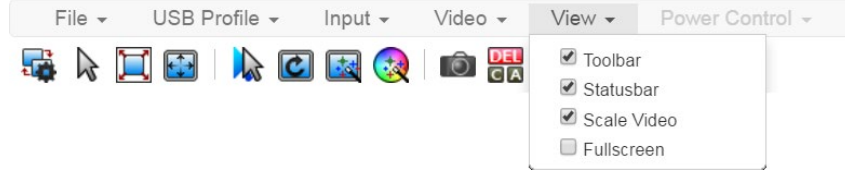
▶ ターゲットサーバーのスクリーンショットを撮る方法:

1. [Video]> [Screenshot] を選択。
2. スクリーンショットファイルは、表示または保存する為のダウンロードとして表示されます。正確なオプションは、クライアントのブラウザによって異なります。



ビューメニューについて

「View」メニューには、HKC 表示をカスタマイズする為のオプションが含まれています。



▶ ツールバーとステータスバー:

ツールバーには、いくつかのコマンドのアイコンが含まれています。ステータスバーには、クライアントウィンドウの下部に画面の解像度が表示されます。

▶ ビデオのスケール:

ビデオをスケールして、HKC ウィンドウのターゲットサーバーウィンドウのコンテンツ全体を表示します。スケールはアスペクト比を維持する為、スクロールバーを使用せずにターゲットサーバーのデスクトップ全体を表示できます。

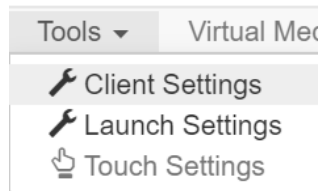
▶ 全画面表示:

フルスクリーンは、ターゲットウィンドウをフルスクリーンのサイズに設定し、クライアントをビューから削除します。

- Esc キーを押して、全画面表示を終了します。

ツールメニュー

[Tools]メニューには、HKC ターゲット接続設定のオプションが含まれています。



▶ クライアント設定:

- [Tools]> [Client Settings] を選択して、[Disable Menu in Fullscreen] オプションにアクセスします。
- 選択すると、メニューバーはフルスクリーンモードでは使用出来なくなります。この設定はクライアントに固有である為、アクセスに使用するクライアントデバイス及びブラウザごとに設定する必要があります。

Client Settings

Disable Menu in Fullscreen

OK

Cancel

▶ 起動設定:

- [Tools]> [Launch Settings] をタップして、[Enable Scale Video] オプションにアクセスします。有効にすると、ターゲットビデオは現在の KVM ウィンドウサイズに合わせて拡大縮小されます。

▶ タッチ設定-iOS クライアントで有効:

- [Tools]> [Touch Settings] をタップして、クライアントタッチ設定にアクセスします。モバイルデバイスのタッチ入力とジェスチャースクロールの設定を、カスタマイズします。

Client Touch Settings

Touch Input

Double Click Time (ms)

250 750

Mouse Click Hold Time (ms)

250 750

Use Left Hand Mouse

Gesture Scrolling

Enable Inverted Scroll x-Axis

Enable Inverted Scroll y-Axis

OK

Cancel

- ダブルクリック時間: マウスのダブルクリックに相当する、2回のタッチタップ間の時間。

- マウスクリックホールド時間：マウスの右クリックに相当する、タッチダウン後のホールド時間。
- 左マウスを使用：ターゲット OS のプライマリマウスボタンが右に設定されている場合に有効にします。
- 逆スクロールの x 軸を有効にする：選択した場合、2本の指で右に動かすと、画面がデフォルトの右ではなく左に移動します。
- 反転スクロール y 軸を有効にする：選択した場合、2本の指で上に移動すると、画面がデフォルトの上ではなく下に移動します。

仮想メディアメニュー

ブラウザの制限により、HKC は他の KVM クライアントとは異なる仮想メディア機能のセットをサポートします。

ブラウザリソースが原因で、HKC での仮想メディアファイル転送は他の KVM クライアントよりも遅くなります。

ファイルとフォルダの接続

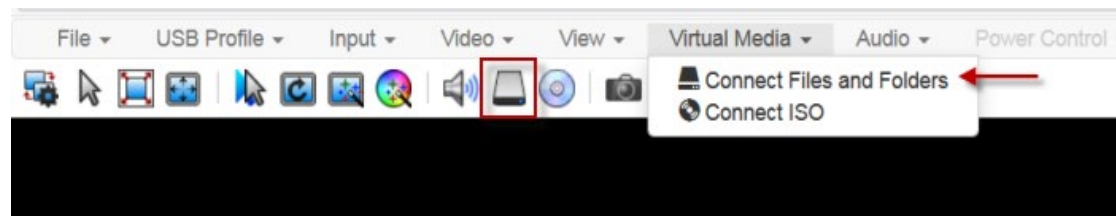
[ファイルとフォルダの接続] コマンドは、接続するファイル/フォルダを仮想メディアにドラッグアンドドロップするための領域を提供します。

サポートされているブラウザ：Chrome、Firefox、Safari

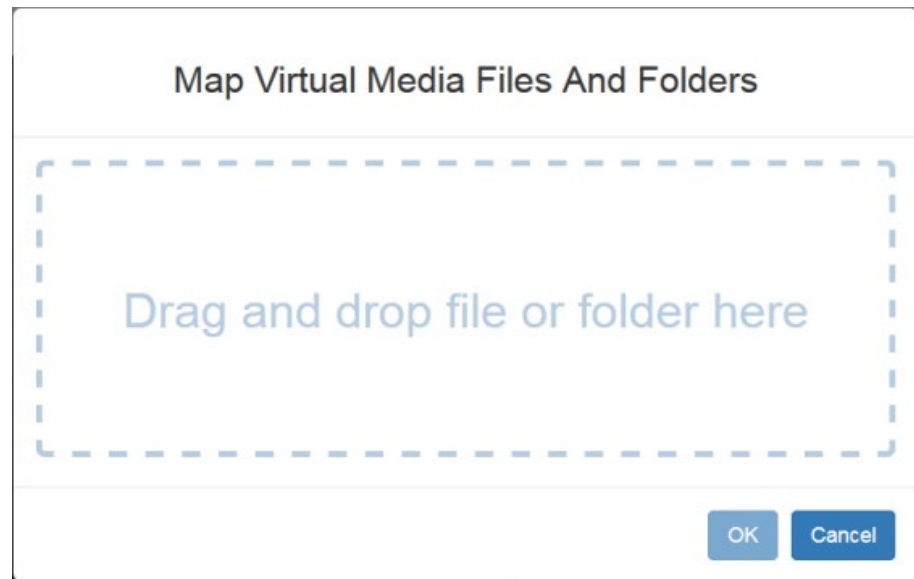
ファイルサイズの制限：ファイルあたり 4GB

▶ ファイルとフォルダの接続方法:

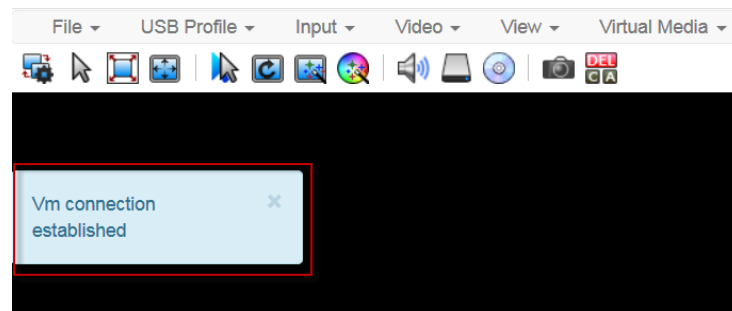
1. [Virtual Media]> [Connect Files and Folders] を選択。または、ツールバーの該当アイコンをクリックします。



2. ファイルまたはフォルダーを[Map Virtual Media Files and Folders]ダイアログにドラッグして、[OK]をクリックします。

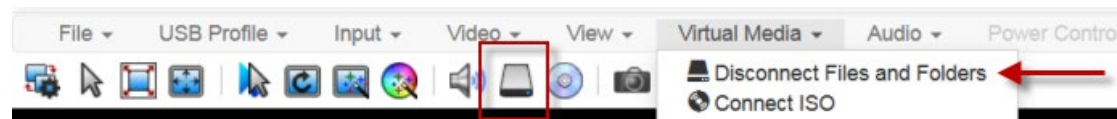


3. 仮想メディアが接続されていることを示すメッセージが表示されます。しばらくすると、選択したファイル/フォルダーを含む VM ドライブが、ターゲットサーバーにマップされます。



▶ ファイル/フォルダの切断方法:

- [Virtual Media]> [Disconnect Files and Folders] を選択。または、ツールバーの該当アイコンをクリックします。



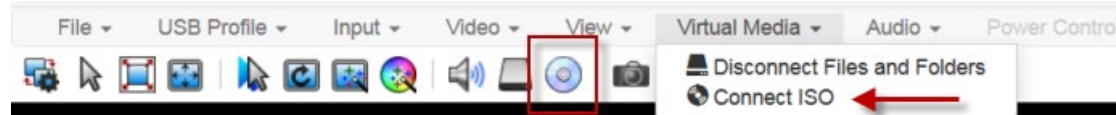
ISO の接続

Connect ISO コマンドは、仮想メディアイメージファイルをターゲットにマップします。クライアント PC から ISO、DMG、または IMG ファイルに接続するか、リモートサーバーから ISO ファイルに接続できます。

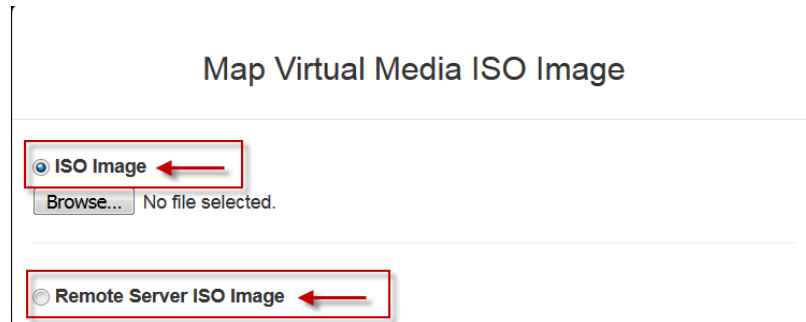
注意：画像ファイルからターゲットにファイル転送時に、SAMBA サーバーへの接続が失われると、キーボードとマウスの制御が数分間失われますが、回復します。

▶ 仮想メディアイメージファイルの配置方法:

1. [Virtual Media] > [Connect ISO] を選択。または、ツールバーの該当アイコンをクリックします。

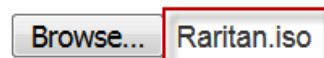


2. ファイル場所のオプションを選択。



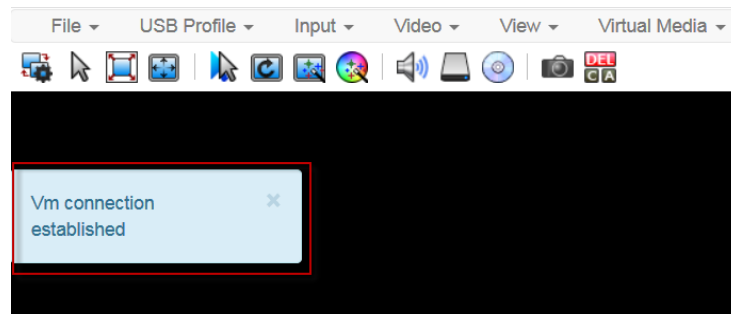
- クライアントでイメージファイルに直接アクセスできる場合、[ISO image] を選択。[Browse] をクリックし、ISO、DMG、または IMG ファイルを選択して、[OK] をクリックします。ファイル名は [Browse] ボタンの横に表示されます。

● ISO Image



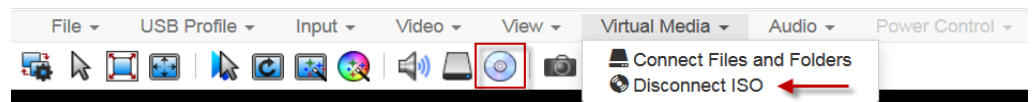
- リモートサーバー上の ISO ファイルの場合、[リモートサーバーISO イメージ] を選択。ここにマッピングを表示するには、管理者がリモート ISO ファイルを事前設定する必要があります。
- 仮想メディアファイルサーバーのセットアップ（ファイルサーバーISO イメージのみ）をご参照ください。ホスト名を選択し、イメージリストからイメージファイルを選択。ファイルサーバーのユーザー名とパスワードを入力します。

- OK をクリックして、選択したファイルをターゲットに配置します。仮想メディアが接続されていることを示すメッセージが表示されます。



▶ ISO の切断方法:

- [Virtual Media] > [Disconnect ISO] を選択。または、ツールバーの該当アイコンをクリックします。



オーディオメニュー

オーディオメニューには、オーディオ接続と設定が含まれています。

複数のターゲット接続が開いていると、音質が低下します。品質を維持するには、オーディオセッションの実行中に HKC で開くターゲット接続を 4 つまでに制限します。

注意: IE はオーディオをサポートしていません。メニューはグレーアウト表示されません。

オーディオ接続

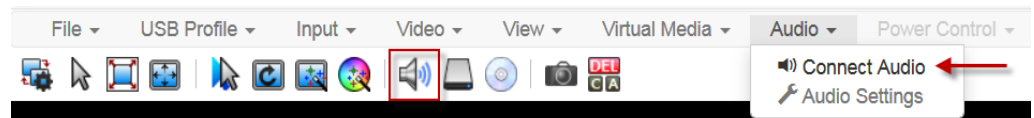
[Connect Audio] コマンドは、再生デバイスを接続し、オーディオ形式を選択。ターゲットに接続した時に選択した再生デバイスを、自動的にマウントするオプションを提供。

HKC は、クライアント PC のデフォルトのオーディオ再生デバイスを接続します。別デバイスを使用するには、クライアント OS でデフォルトとして設定する必要があります。

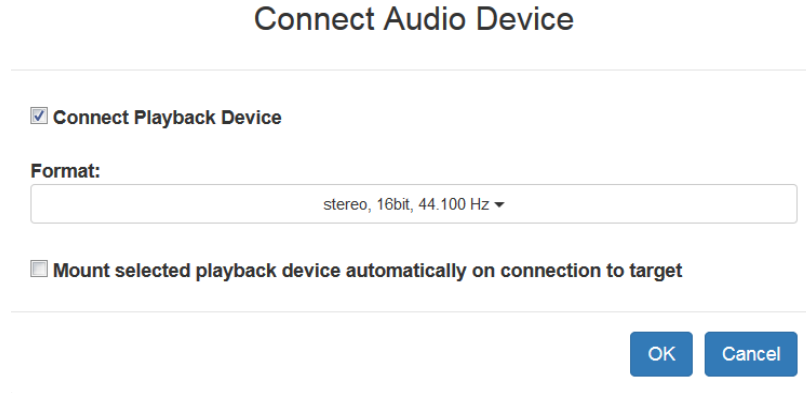
注意: 最高の品質を得るには、オーディオセッション数を最大 4 つの KVM セッションに制限してください。

▶ オーディオの接続方法:

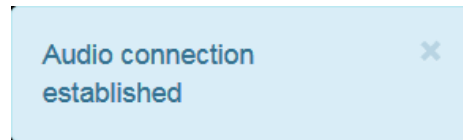
- [Audio]> [Connect Audio] を選択するか、ツールバーの該当アイコンをクリック。



2. [Connect Audio Device] ダイアログで [Connect Playback Device] チェックボックスを選択。



3. [選択した再生デバイスをターゲットへの接続時に自動的にマウントする] チェックボックスを選択して、オプションを有効にします。この設定は次にターゲット接続時に、オーディオを自動的に接続します。
4. [OK]をクリック。成功メッセージが表示されます。



▶ オーディオの切断方法:

1. [Audio]> [Disconnect Audio] を選択するか、ツールバーの該当アイコンをクリック。

オーディオ設定

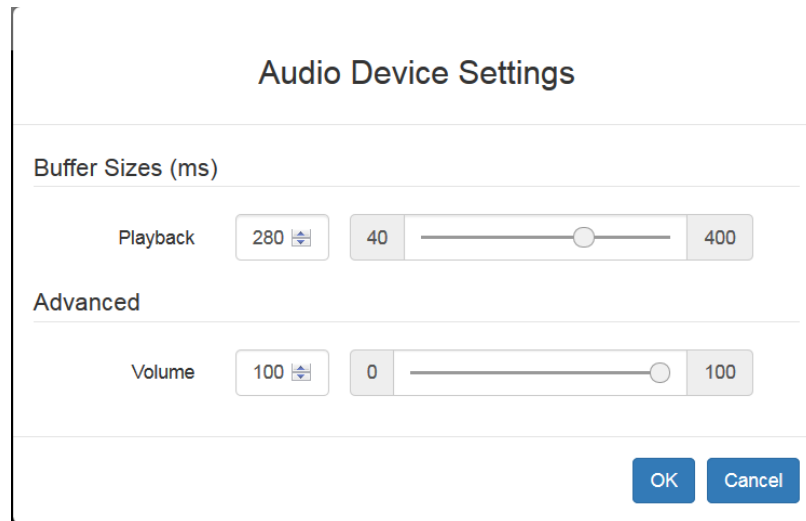
オーディオが接続されている場合、[オーディオ設定]オプションが有効になります。オーディオ設定を使用して、バッファと音量を設定します。

バッファサイズを大きくするとオーディオ品質は向上しますが、配信速度に影響を与える可能性があります。

それよりも大きいものは、オーディオ品質に大きな影響を与える為、使用可能な最大バッファサイズは400ミリ秒です。

▶ オーディオ設定の構成方法:

1. オーディオが接続されている時に、[Audio]> [Audio Device Settings]を選択。
2. 矢印またはスライダーを使用して、バッファとボリュームを設定します。



3. [OK]をクリック。

Safari での自動再生

自動マウントされた、オーディオデバイスを備えた Safari ブラウザの HKC 接続の場合、[自動再生]設定が[すべての自動再生を許可]になっていることを確認してください。

<https://support.apple.com/guide/safari/customize-settings-per-website-ibrw7f78f7fe/mac>

外部デバイスのメニュー

外部デバイスのメニューを使用すると、Dominion KX IV-101 の端子台に接続されている機器を、制御できます。

▶ 外部デバイス設定の方法:

1. [External Device]> [Settings]を選択して、ダイアログを表示します。
2. デバイスの状態が、一覧表示されます。
3. 有効なデバイスは、[アクション]オプションを使用して制御できます。
 - 外部デバイスのオン/オフを切り替える：[ON]または[OFF]をクリックして、端末出力リレーを制御します。
 - 外部デバイスの点滅：0.5 秒間隔を入力して、外部デバイスの点滅を制御します。

External Device Settings

External Device State: Disabled

Action

Turn External Device On/Off

On Off

Blink External Device

1

Interval (Half-Seconds)

OK

Cancel

Apply

4. [OK]または [Apply]をクリックして、アクションを完了します。

Apple iOS デバイスでの HKC を使用

Dominion KX IV-101 は、モバイルバージョンの HKC を使用して、iOS10.0 以降を搭載した Apple モバイルデバイスからターゲットへのリモートアクセスをサポートします。 Apple iOS 制限により、操作にいくつかの違いが見られる場合があります。「Apple iOS デバイスの制限 『p. 106』」をご参照下さい。

Apple iOS デバイスに証明書をインストール

Dominion KX IV-101 に接続する前に、Apple iOS デバイスに CA 署名付き証明書をインストールする必要があります。デフォルトの証明書のみが存在する場合、アクセスは阻止されません。ブラウザによっては、「この接続はプライベートではありません」等のエラーが表示される場合があります。

証明書を作成するとき、証明書の共通名は、デバイスへの接続に使用される IP アドレス/ホスト名と一致する必要があります。

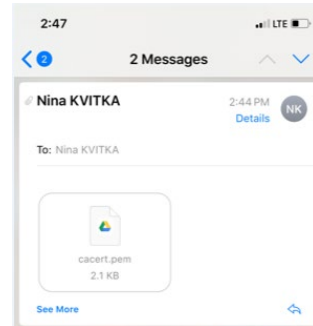
Dominion KX IV-101 証明書と Dominion KX IV-101 証明書の署名に使用する、CA 証明書の両方をインストールします。

注意：IOS デバイスからの直接接続または、CC-SG HKC 接続の起動に問題がある場合は、証明書が Apple の要件に満たしている事を確認して下さい。

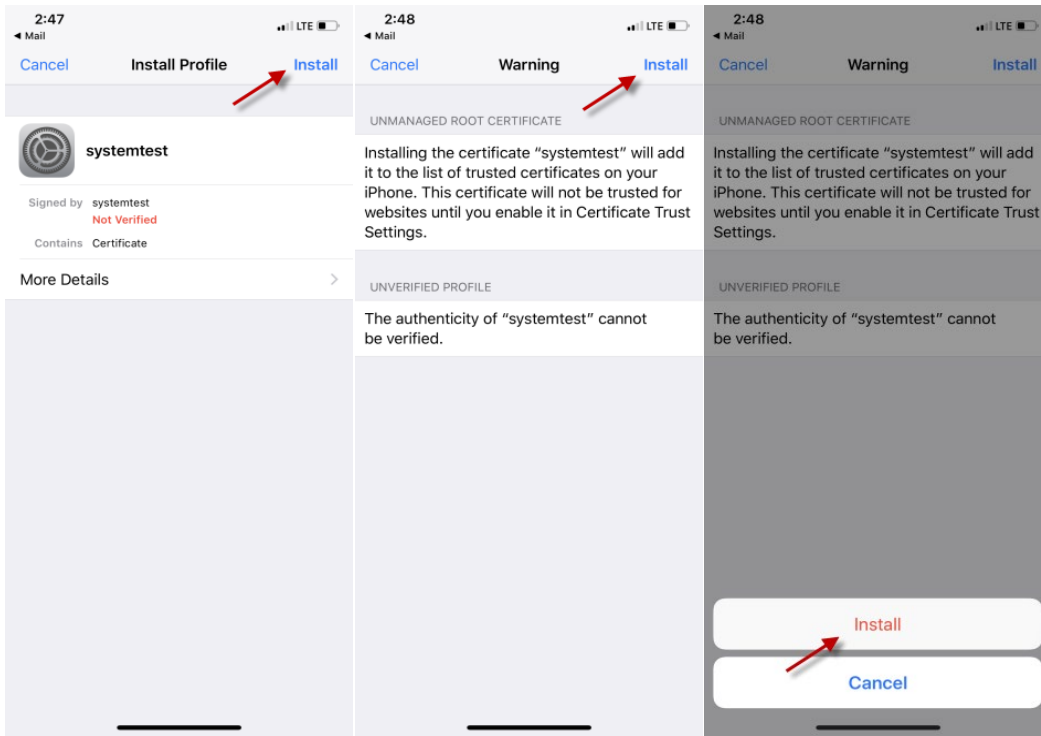
<https://support.apple.com/en-us/HT210176>

▶ IOS デバイスに証明書をインストールする方法:

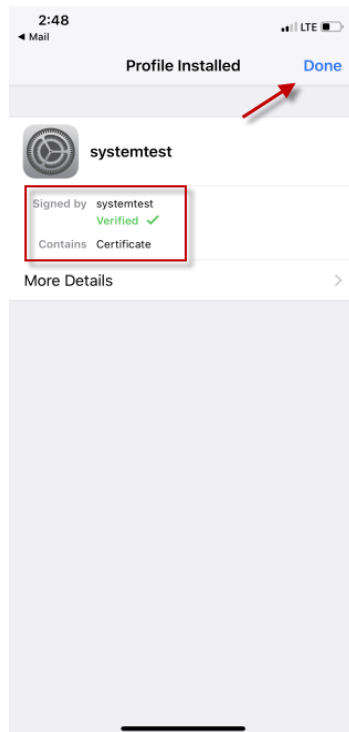
1. iOS デバイスで開くことができる電子メールアカウントに、証明書ファイルをメールで送信します。そのメールを開き、添付ファイルをタップします。



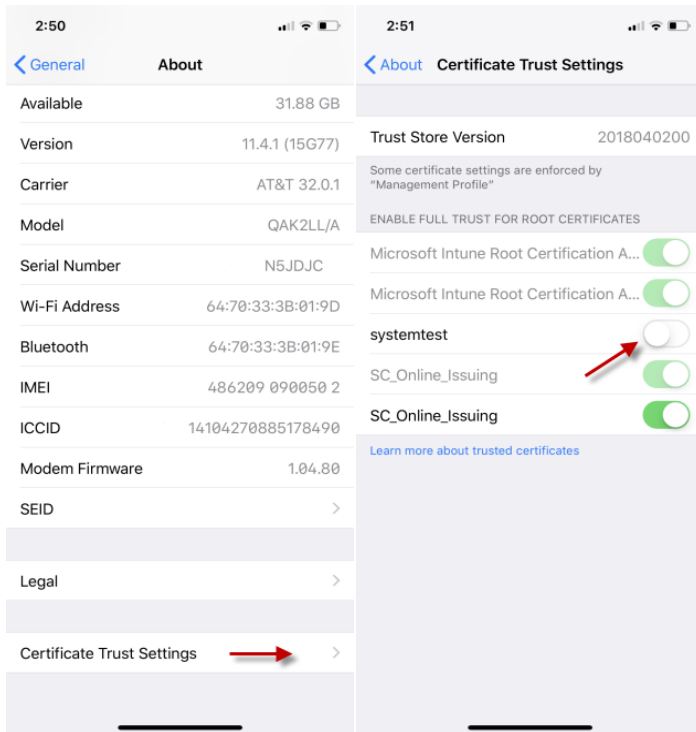
2. 証明書は、インストールする必要がある「プロファイル」としてダウンロードされます。一度にインストールできるプロファイルは 1 つのみです。例えば、プロファイルをダウンロードしてインストールせずに 2 番目のプロファイルをダウンロードした場合、2 番目のプロファイルのみをインストールできます。ダウンロードしてから 8 分以内にプロファイルがインストールされない場合、プロファイルは自動的に削除されます。
3. プロファイルをインストールするには、[設定]に移動し、[ダウンロードされたプロファイル]をタップします。
4. [インストール]をタップし、表示されるプロンプトに従って確認してインストールします。



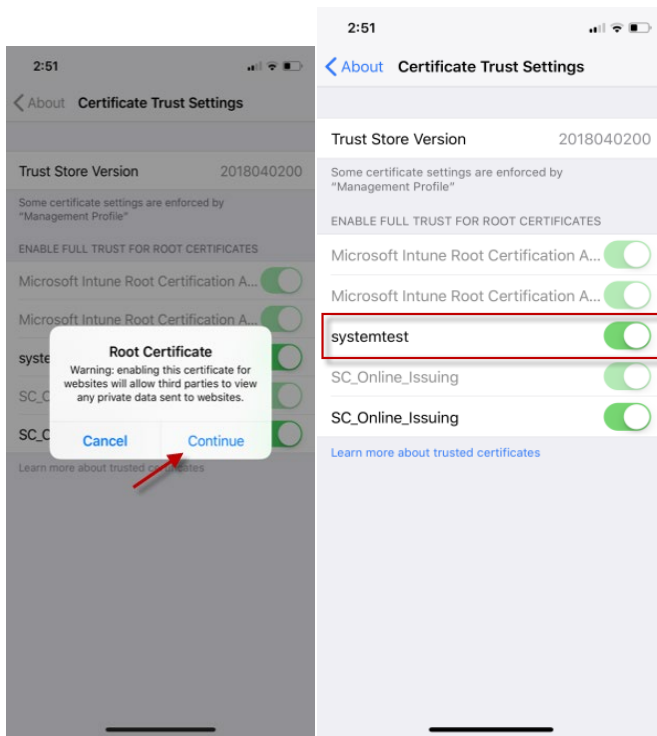
5. 完了すると、証明書に[検証済み]のマークが付けられます。 [完了]をタップします。



6. 証明書を有効にするには、[設定]> [一般]> [バージョン情報]へ移動し、一番下までスクロールします。 [証明書の信頼設定] をタップします。



7. 以前にインストールした証明書をタップして有効にします。警告が表示されます。[続行]をタップして有効にします。証明書スライダーは、有効の場合は緑色表示されます。



タッチマウス機能

各マウス機能に相当するタッチスクリーンを使用して下さい。一部のタッチ設定は構成可能です。「ツールメニュー『p. 91』」をご参照下さい。

1 本指タッチ	マウス相当
タッチダウン-移動-リリース	マウスポインターを動かす
ショートタップ	左クリック
ダブルショートタップ	左ダブルクリック
ショートタップ-タッチダウン-250ms 保持	右クリックに相当するマウス
ショートタップ-タッチダウン-移動-リリース	ドラッグアンドドロップまたは、選択のように、マウスの左ボタンを押したまま移動
2 本指タッチ	マウス相当
タッチダウン-移動-リリース	画面移動

モバイルでのキーボードアクセス

ターゲットへのキーボードアクセスは、ツールバーで使用可能な仮想キーボードを介して行われます。キーボード入力が必要とする他の全てのアクションの場合、IOS ポップアップキーボードが自動的に表示されます。

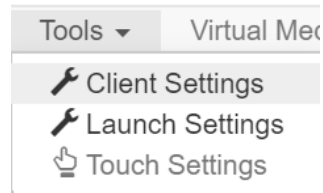
HKC iOS クライアントのキーボードマクロの管理

HKC iOS クライアントには、デフォルトのマクロのリストが含まれています。HKC マクロエディタを使用して追加のマクロを作成するか、ファイルからマクロをインポートできます。「マクロエディタ」(80 ページ) 及び「マクロのインポートとエクスポート」(84 ページ) をご参照下さい。

注意 : Apple iOS デバイスを使用している時にマクロをインポートするには、最初に PC クライアントを使用して、HKC からファイルをエクスポートします。ファイルをクラウド場所に追加して、インポートの為に IOS デバイスからアクセスします。

ツールメニュー

[ツール]メニューには、HKC ターゲット接続設定のオプションが含まれています。



▶ クライアント設定:

- [Tools]> [Client Settings] を選択して、[Disable Menu in Fullscreen] オプションにアクセスします。
- 選択すると、メニューバーはフルスクリーンモードでは使用できなくなります。この設定はクライアントに固有である為、アクセスに使用するクライアントデバイスとブラウザごとに、設定する必要があります。

Client Settings

Disable Menu in Fullscreen

OK

Cancel

▶ 起動設定:

- [ツール]> [起動設定]をタップして、[スケールビデオを有効にする] オプションにアクセスします。有効にするとターゲットビデオは、現在の KVM ウィンドウサイズに合わせて拡大縮小されます。

▶ タッチ設定-iOS クライアントで有効:

- [ツール]> [タッチ設定] をタップして、クライアントタッチ設定にアクセス。モバイルデバイスのタッチ入力と、ジェスチャースクロールの設定をカスタマイズします。

Client Touch Settings

Touch Input

Double Click Time (ms)

250 750

Mouse Click Hold Time (ms)

250 750

Use Left Hand Mouse

Gesture Scrolling

Enable Inverted Scroll x-Axis

Enable Inverted Scroll y-Axis

OK Cancel

- ダブルクリック時間：マウスのダブルクリックに相当する 2 回のタッチタップ間の時間。
- マウスクリックホールド時間：マウスの右クリックに相当する、タッチダウン後のホールド時間。
- 左マウスを使用：ターゲット OS のプライマリマウスボタンが右に設定されている場合に、有効にします。
- 逆スクロールの x 軸を有効にする：選択した場合、2 本の指で右に動かすと、画面がデフォルトの右ではなく左に移動します。
- 反転スクロール y 軸を有効にする：選択した場合、2 本の指で上に移動すると、画面がデフォルトの上ではなく下に移動します。

Apple iOS デバイスの制限

- iOS デバイスを使用したモバイルアクセスは、いくつかの Raritan 製品でサポートされています。全ての制限が全ての製品に適用されるわけではありません。違いが記載されています。ブラウザがバックグラウンドにある場合、または iOS デバイスが自動ロックモードになっている場合、ターゲット接続は約 1 分後に閉じられます。
- F1-F12、ESC、Control、Alt、OS メタキーなどの一部の特殊文字のマクロを作成できません。一般的に使用されるキーの選択は、デフォルトのマクロリストで利用できます。
- 右記のキーは編集できます。マクロインポートを使用して、F1-12 や矢印等の追加のキーを追加できます。
- iOS の Safari で、メニューオプションまたはシリアルターゲットにアクセスするには、KVM またはシリアルターゲットの起動後に、デバイスへの接続を更新する必要があります。iOS の Chrome では、不要。
- iOS は、オーディオデバイスのターゲットへの自動接続をサポートしていません。
- Ubuntu 14.04 ターゲットでは、マウスクリックにตอบสนองせず、ターゲットアイテムを押し続けて右クリックをシミュレートします。
- デュアルターゲット接続の問題：両方のターゲットウィンドウを別々に閉じる必要があります。iOS11.x デバイスの Safari から開かれたデュアルターゲットのポートは 1 つだけです。（デュアルターゲットは KX4-101 ではサポートされていません）。
- オプション「フルスクリーン」と「画面に合わせてウィンドウのサイズを変更する」は、iOS では有効/使用できません。
- クライアント仮想キーボードの KB ロケールは、デバイスの入力ロケールとターゲットの OS ロケールと一致する必要があります。
- iOS クライアントのターゲットウィンドウにはスクロールバーがありません。拡大縮小されていないビデオは、2本の指を左右または上下にスライドさせることで水平/垂直にスクロールできます。「タッチマウスの機能 『p. 103』」をご参照。
- Safari では、サーバーVM 接続のあるターゲットから、別ターゲットに切り替えるときに、ユーザーはパスワードを保存するように求められます。これらのプロンプトは、Safari > [設定] > [オートフィル] の [ユーザー名とパスワード] チェックボックスをオフにすることでオフにできます。
- Safari では、オンスクリーンキーボードに単語予測が含まれています。予測語を選択すると、最後にスペースが追加されます。(例) ログイン画面で「admin」を選択すると「admin」と入力されます。同様の動作は、VM ファイルサーバーのユーザー名とその他の領域でも発生します。
- 接続情報などのメニューオプションパネルは、移動不可。
- iOS オンスクリーンキーボードは、[保存] ボタンをタップする代わりに、キーボードの [移動] をタップして設定変更を保存すると、HTML 管理ページをマウスでクリックする度に表示されます。
- iOS クライアントから開いた DSAM ターゲットの場合、メニュー項目を選択して閉じる度に、オンスクリーンキーボードが表示されます。VNC ログインは、再起動後にログインページを更新時に発生します。これにより、ターゲット接続が失敗します。モバイル HKC ログインを復元するには、ログアウトして Dominion KX IV-101 IP またはホスト名を再入力します。この事象は、iOS クライアントと PC クライアントの両方に当てはまります。

- [仮想メディア] メニューの[VM ファイルとフォルダー] オプションは、ファイルをパネルにドラッグアンドドロップできない為、無効になっています。
- 全てのアクセント付き文字が、iOS クライアントから処理されるわけではありません。
- Safari を使用して iOS デバイスからエクスポートされたマクロファイルには、自動的に「不明」という名前が付けられ、別のクライアントにインポートするには、xml 拡張子で名前変更する必要があります。
- データのダウンロードに問題がある為、iOS デバイス上の Chrome からマクロファイルをエクスポートすることはできません。
- ターゲットでサポートされている文字のみが処理されます。 iPad のキーボードにある¥、\$、…などの iOS 文字からの応答はありません。
- オンスクリーンキーボードで、「文字」または「Return」キーを選択すると、キーボードの表示がリストの最初に戻ります。

デュアルモニターセットアップで Dominion KX IV-101 にアクセスする為のコツ

デュアルモニターセットアップで Dominion KX IV-101 にリモートアクセスする場合、Dominion KX IV-101 へのモニターが、プライマリディスプレイとして設定されている事を確認してください。 2 台のモニターを水平に配置し、モニターを左の位置にある KX4-101 に向けます。このシナリオでマウスを適切に配置するには、インテリジェントマウスモードを使用します。

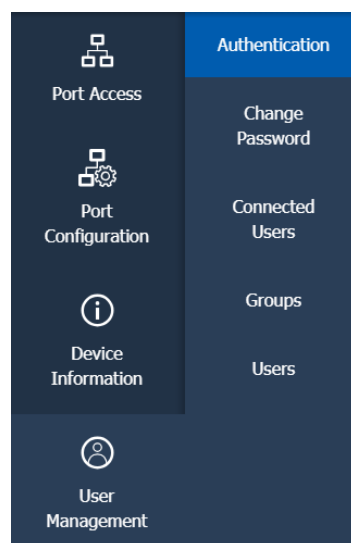
注意：Windows 10 ターゲットの場合、インテリジェントマウスモードを使用する時は、全てのアクセラレーションを無効にする必要があります。

CHAPTER 5 ユーザー管理

Dominion KX IV-101 は、ローカル認証またはリモート認証用に構成できます。外部認証を構成する準備をするには、「LDAP / RADIUS 情報の収集 『p. 109』」をご参照下さい。

Dominion KX IV-101 には、1つの組み込み管理者アカウント admin が付属しています。これは、初期ログインとシステム管理に最適です。'admin' を削除したり、その権限を変更したりすることはできませんが、ユーザー名とパスワードを変更することは出来ます。ユーザー管理に関連するその他のセキュリティ設定については、「セキュリティ 『p. 149』」をご参照下さい。

[User Management] をクリックして、サブメニューオプションを表示します。



内容

LDAP / Radius 情報の収集.....	107
認証の構成	108
外部認証の無効化	114
パスワード変更	114
接続ユーザー	114
ユーザーとグループ	115

LDAP / Radius 情報の収集

外部認証を構成するには、AA サーバーの設定に関する下記情報が必要です。これらの設定に慣れていない場合は、AA サーバー管理者にご相談ください。

▶ LDAP 認証:

- LDAP サーバーの IP アドレス、またはホスト名
- LDAP サーバーのタイプ。通常は下記のいずれかのオプションです:
 - *OpenLDAP*

Open LDAP サーバーを使用している場合、LDAP 管理者にバインド識別名 (DN) とパスワードを問い合わせてください。

- *Microsoft Active Directory (AD)*

Microsoft Active Directory サーバーを使用している場合、AD 管理者に Active Directory ドメイン名を問い合わせてください。

- 必須タイプの LDAP セキュリティ (None, TLS, SmartTLS).
 - Secure LDAP を使用している場合、LDAP 管理者に CA 証明書ファイルを問い合わせてください。
- LDAP サーバーが使用する、ネットワークポート
- バインド識別名 (DN) とパスワード (匿名バインドが使用されていない場合)
- サーバーのベース DN (ユーザーの検索に使用)
- ログイン名属性 (または AuthorizationString)
- ユーザーエントリオブジェクトクラス
- ユーザー検索サブフィルター (または BaseSearch)

▶ RADIUS 認証:

- RADIUS サーバーの IP アドレス、またはホスト名
- RADIUS サーバーで使用される、RADIUS 認証のタイプ (PAP または CHAP)
- 安全な通信のための共有秘密
- RADIUS サーバーが使用する、UDP 認証ポートとアカウントングポート

認証の構成

重要: SSL 3.0 で公開されているセキュリティの脆弱性の為、Raritan は SSL3.0 ではなく TLS を使用しています。LDAP やメールサービス等のネットワークインフラストラクチャが SSL3.0 ではなく、TLS を使用していることをご確認ください。

KX IV-101 は以下をサポート :

- Dominion KX IV-101 のローカルユーザーデータベース
- LDAP
- Radius

デフォルトでは、Dominion KX IV-101 はローカル認証用に構成されています。この方法を使用する場合、ユーザーアカウントを作成するだけで済みます。ユーザーの作成をご参照ください。

外部認証を希望する場合、Dominion KX IV-101 に外部認証と承認 (AA) サーバーに関する情報を提供する必要があります。

外部認証が利用できない時、バックアップ方法としてローカル認証を利用できるようにしたい場合、外部 AA サーバーデータを提供することに加えて、Dominion KXIV-101 でユーザーアカウントを作成します。ローカル認証と外部認証を同時に使用することは出来ません。外部認証用に構成されている場合、全ての Dominion KXIV-101 ユーザーは、外部 AA サーバーにアカウントを持っている必要があります。Dominion KX IV-101 にいつでもアクセスできる管理者を除いて、外部認証が有効になっている場合、ローカル認証のみのユーザーはアクセスできません。

▶ **認証タイプの選択方法:**

1. [User Management]> [Authentication]をクリック
2. 認証タイプを選択:
 - ローカル
 - LDAP
 - Radius
3. [Use Local Authentication if Remote Authentication is not available] チェックボックスを選択して、サーバーがダウンしている場合など、外部認証が利用できない場合のバックアップ方法としてローカル認証を許可します。
4. [Save]をクリック。認証タイプが有効になります。

外部サーバーの追加については、「LDAP 認証」(111 ページ)、「RADIUS 認証」(114 ページ)を参照、ユーザーの追加については、「ユーザーとグループ」『p. 116』をご参照下さい。

Authentication

i Local authentication is used if nothing is enabled.

Authentication Type LDAP

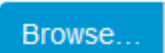
Use Local Authentication if Remote Authentication is not available

LDAP 認証

LDAP サーバーを、Dominion KX IV-101 に追加するために必要な情報を収集します。ヘルプが必要な場合、「LDAP / RADIUS 情報の収集 『p. 109』」をご参照下さい。

▶ LDAP サーバーの追加方法:

1. [User Management]> [Authentication] をクリック
2. [LDAP]セクションで、[新規]をクリックします。 LDAP の詳細を入力します。
- 3.

フィールド/設定	内容
IP アドレス / ホスト名	<ul style="list-style-type: none"> LDAP / LDAPS サーバーの IP アドレスまたはホスト名。 暗号化を有効にしない場合、このフィールドにドメイン名または IP アドレスのいずれかを入力できます。暗号化が有効になっている場合、完全修飾ドメイン名を入力する必要があります。
既存の LDAP サーバーから設定をコピー	このチェックボックスは、Dominion KX IV-101 に既存の AA サーバー設定がある場合にのみ表示されます。既存の AA サーバーの設定を複製するには、以下の複製手順を参照してください。
LDAP サーバーのタイプ	下記のいずれかのオプションを選択： <ul style="list-style-type: none"> OpenLDAP Microsoft Active Directory. .
セキュリティ	<p>Dominion KX IV-101 が LDAPS サーバーと安全に通信できるようにする TLS 暗号化を使用するかどうかを決定します。</p> <p>3つのオプションが利用可能:</p> <ul style="list-style-type: none"> StartTLS TLS None
ポート (None/StartTLS)	<ul style="list-style-type: none"> デフォルトのポートは 389 であるか、別のポートを指定。
ポート (TLS)	<p>「セキュリティ」フィールドで「TLS」が選択されている場合にのみ、構成可能。</p> <p>デフォルトのポートは 636 であるか、別のポートを指定。</p>
LDAP サーバー証明書の検証を有効にする	<p>接続前に Dominion KX IV-101 によって、LDAP サーバーの証明書を検証する必要がある場合、このチェックボックスを選択します。</p> <p>証明書の検証が失敗した場合、接続は拒否されます。</p>
CA 証明書	<p>LDAPS サーバーの CA 証明書ファイルを取得するには、AA サーバー管理者にご相談ください。</p> <p> クリックして、証明書ファイルを選択してインストールします。</p> <ul style="list-style-type: none"> [表示]をクリックして、インストールされている証明書の内容を表示します。 不適切な場合、[削除]をクリックして、インストールされている証明書を削除します。 <p><i>注意：必要な証明書ファイルが証明書のチェーンであり、証明書チェーンの要件が不明な場合、TLS 証明書チェーンをご参照ください。</i></p>

フィールド/設定	内容
期限切れでまだ有効ではない証明書を許可	<ul style="list-style-type: none"> 証明書の有効期間に関係なく、認証を成功させるには、このチェックボックスを選択します。 このチェックボックスの選択を解除すると、選択した証明書チェーン内の証明書が古くなっているか、まだ有効でないときに常に認証に失敗します。
匿名バインド	<p>このチェックボックスを使用して、匿名バインドを有効/無効にします。</p> <ul style="list-style-type: none"> 匿名バインドを使用するには、このチェックボックスを選択。 外部 LDAP / LDAPS サーバーにバインドするために、バインド DN とパスワードが必要な際は、このチェックボックスの選択を解除。
バインド DN	<p>【匿名バインド】 チェックボックスをオフにした後に必要です。 定義された検索ベースで、LDAP ディレクトリの検索を許可されているユーザーの識別名 (DN)。</p>
バインドパスワード、バインドパスワードの確認	<p>【匿名バインド】 チェックボックスをオフにした後に必要です。 バインドパスワードを入力。</p>
検索用のベース DN	<p>LDAP 検索の開始点の検索ベースの識別名 (DN)</p> <ul style="list-style-type: none"> 例: ou=dev,dc=example,dc=com
ログイン名属性	<p>ログイン名を示す LDAP ユーザークラスの属性。</p> <ul style="list-style-type: none"> 通常は uid
ユーザー入力オブジェクトクラス	<p>ユーザーエントリのオブジェクトクラス。</p> <ul style="list-style-type: none"> 通常は inetOrgPerson
ユーザー検索サブフィルター	<p>ディレクトリツリー内で、LDAP ユーザーオブジェクトを検索する為の検索条件。</p>
Active Directory ドメイン	<p>Active Directory ドメインの名。</p> <ul style="list-style-type: none"> 例: testradius.com

4. [接続のテスト] クリックして、Dominion KX IV-101 のサーバーへの接続可否を確認。
5. [サーバーの追加] をクリック。新しいLDAP サーバーが[認証]ページに表示されます。サーバーをさらに追加するには、同じ手順を繰り返します。複数のサーバーがある場合、矢印ボタンを使用してサーバーの順序を設定し、[順序を保存] をクリック。
6. これらの設定の使用を開始するには、LDAP が選択され、[認証タイプ]フィールドに保存されていることを確認してください。「認証の構成」『p. 109』をご参照下さい。

Active Directory サーバーからユーザーグループ情報を返す

Dominion KX IV-101 は、ユーザーが Dominion KX IV-101 でローカルに定義されている必要なしに、Active Directory (AD) へのユーザー認証をサポートします。これにより、Active Directory ユーザーアカウントとパスワードを AD サーバーで排他的に維持できます。承認と AD ユーザー特権は、AD ユーザーグループにローカルに適用される、標準の Dominion KX IV-101 ポリシーとユーザーグループ特権によって制御/管理されます。

重要: 既存のユーザーであり、ADスキーマを変更してActive Directoryサーバーを既に構成している場合でも、Dominion KX IV-101はこの構成をサポートしている為、次の操作を実行する必要はありません。AD LDAP / LDAPSスキーマの更新については、LDAPスキーマの更新をご参照ください。

▶ Dominion KX IV-101 で AD サーバーを有効にする方法:

1. Dominion KX IV-101 を使用して、特別なグループを作成し、これらのグループに適切なアクセス許可と特権を割り当てます。例えば、KVM_Admin や KVM_Operator 等のグループを作成します。
2. Active Directory サーバーで、前の手順と同じグループ名で新しいグループを作成します。
3. AD サーバーで Dominion KX IV-101 ユーザーを、手順 2 で作成したグループに割り当てます。
4. Dominion KX IV-101 から、AD サーバーを有効にして適切に構成します。LDAP / LDAPS リモート認証の実装を、ご参照ください。

重要な注意事項

- グループ名では、大文字と小文字が区別されます。
- Dominion KX IV-101 は、変更または削除できない下記のデフォルトグループを提供します：Admin と <Unknown>。 Active Directory サーバーが、同じグループ名を使用していない事を確認します。
- Active Directory サーバーから返されたグループ情報が、Dominion KX IV-101 グループ構成と一致しない場合、Dominion KX IV-101 は、正常に認証されたユーザーに <Unknown>のグループを自動的に割り当てます。
- ダイアルバック番号を使用する場合、大文字と小文字を区別する右記の文字列を入力する必要があります：msRADIUSCallbackNumber。
- Microsoft の推奨事項に基づいて、ドメインローカルグループではなく、ユーザーアカウントを持つグローバルグループを使用する必要があります。

RADIUS 認証

Radius サーバーを Dominion KX IV-101 に追加する為に必要な情報を収集します。ヘルプが必要な場合は、「LDAP / RADIUS 情報の収集 『p. 109』」を参照してください。

▶ **Radius サーバーの追加方法:**

1. [User Management]> [Authentication] をクリック。
2. [Radius] セクションで、[新規] をクリック。Radius の詳細を入力します。

フィールド/設定	内容
IP アドレス / ホスト名	RADIUS サーバーの IP アドレス、またはホスト名。
RADIUS 認証の種類	認証プロトコルを選択。 ・ PAP (パスワード認証プロトコル) ・ CHAP (チャレンジハンドシェイク認証プロトコル) CHAP は、ユーザー名とパスワードが暗号化されている為、一般的に安全であると見なされていますが、PAP では平文で送信されます。
認証ポート、 アカウントポート	デフォルトは標準ポート 1812 & 1813 です。 非標準のポートを使用するには、新しいポート番号を入力します。
タイムアウト	これによりタイムアウトする前に、Radius サーバーとの接続を確立する為の最大時間が設定されます。 タイムアウト期間を秒単位で入力します。
再試行	再試行回数を入力。
共有秘密、 共有秘密を確認する	共有シークレットは、Radius サーバーとの通信を保護する為に必要です。

3. [接続のテスト] をクリックして、Dominion KX IV-101 がサーバーに接続できるかどうかを確認します。

4. [サーバーの追加] をクリック。新しい Radius サーバーが[認証]ページに表示されません。サーバーをさらに追加するには、同じ手順を繰り返します。複数のサーバーがある場合、矢印ボタンを使用してサーバーの順序を設定し、[順序を保存]をクリックします。
5. これらの設定の使用を開始するには、[Radius]が選択され、[認証タイプ]フィールドに保存されている事をご確認ください。「*認証の構成*」(p. 109)をご参照ください。

RADIUS 経由でユーザーグループ情報を返す

RADIUS 認証の試行が成功すると、Dominion KX-101 は、ユーザーのグループのアクセス許可に基づいて、特定のユーザーのアクセス許可を決定します。

リモート RADIUS サーバーは、RADIUS FILTER-ID として実装された属性を返すことにより、これらのユーザーグループ名を提供できます。FILTER-ID は、次のようにフォーマットする必要があります。Raritan:G {GROUP_NAME} ここで、GROUP_NAME は、ユーザーが属するグループ名を示す文字列です。

Raritan:G{GROUP_NAME}

ここで、GROUP_NAME は、ユーザーが属するグループ名を示す文字列です。

外部認証の無効化

▶ **外部認証の無効方法:**

1. [User Management] > [Authentication] をクリック。
2. [Authentication Type] で、[Local]を選択。
3. [Save]をクリック。

パスワード変更

▶ **パスワードの変更方法:**

1. [User Management] > [Change Password] をクリック。
2. 古いパスワードを入力してから、新しいパスワードを 2 回入力します。
3. [Save]をクリック。

接続ユーザー

Dominion KX IV-101 にログインしているユーザーと、そのステータスを確認できます。管理者権限がある場合、Dominion KX IV-101 の全てのユーザーの接続を終了できます。

▶ **接続されたユーザーの表示/管理方法:**

1. [User Management] > [Connected Users] をクリック。
2. ログインしたユーザーのリストが表示されます。

3.

カラム	内容
ユーザー名	接続されている各ユーザーのログイン名。
IP アドレス	各ユーザーのホストの IP アドレス。 ローカル接続 (USB) 経由のログインの場合、IP アドレスの代わりに <local>が表示されます。
クライアントタイプ	Web GUI : Web インターフェースを指します。 CLI : シリアル (USB 接続などのローカル) または SSH RDM : CC-SG またはユーザーステーション
アイドルタイム	ユーザーがアイドル状態を維持する時間の長さ。

- a. ユーザーを切断するには、[Disconnect]をクリック。
- b. 確認メッセージで[Disconnect]をクリック。ユーザーは強制的にログアウト。

ユーザーとグループ

全てのユーザーは、ログイン名とパスワードを含むユーザーアカウントを持っている必要があります。複数のユーザーが同じログイン名を使用して同時にログインが可能。 admin ユーザーはデフォルトで作成され、削除する事はできませんが、ユーザー名は変更できます。

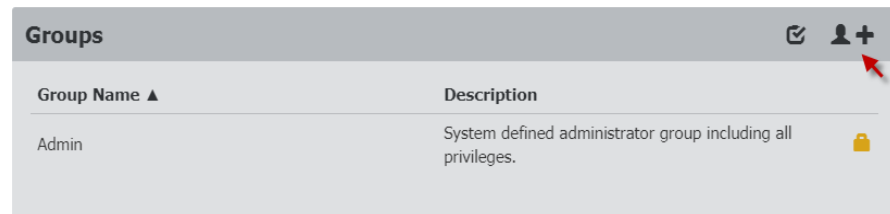
特権はグループレベルで割り当てられる為、グループも追加し、ユーザーをグループに割り当てる必要があります。管理者グループはデフォルトで作成され、排他的な特権を持っています。「管理者グループの特別な権限 『p. 124』」をご参照ください。

ユーザーが異なる特権レベルを持つ複数のグループに割り当てられている場合、指定された最高レベルのアクセスがユーザーに許可されます。

ユーザーグループの権限の変更は、次回ログイン時にグループ内のユーザーに対して、有効になります。

▶ グループの追加方法:

1. [User Management]> [Groups]をクリックし、[グループの追加] アイコンをクリック。



2. 新しいグループ情報を入 :

フィールド/設定	内容
グループ名	<ul style="list-style-type: none"> ▪ 1~32 文字 ▪ 大文字と小文字を区別 ▪ スペースは許可されています。
内容	<ul style="list-style-type: none"> ▪ グループの役割の説明を入力。 ▪ 最大 64 文字。

New Group

Settings

Group Name	<input type="text" value="Maintenance"/>
Description	<input type="text" value="Maintenance privileges"/>

3. このグループに割り当てられている特権を選択します。ここで除外として記載されているの全てのタスクは、管理者グループのみが利用できます。
4. 「管理者グループの特別な権限 『p. 124』」をご参照ください。
 - CC-SG 管理下でのデバイスアクセス : CC-SG でデバイスのローカルアクセスが有効になっている場合、ユーザーは IP アドレスを使用して Dominion KX IV-101 に直接アクセスできます。CC-SG の管理下にあるデバイスに直接アクセスすると、アクセスと接続アクティビティが Dominion KX IV-101 に記録されます。ユーザー認証は、Dominion KX IV-101 認証設定に基づいて実行されます。
 - デバイス設定 : SNMPv3 の有効化と構成を除く [デバイス設定]、メニューの全ての機能
 - メンテナンス : バックアップ/復元と工場出荷時の初期へのリセットを除く、メンテナンスメニューの全ての機能
 - PC 共有 : 複数のユーザーによる同じターゲットへの同時アクセス
 - セキュリティ : [セキュリティ]メニューの全ての機能
 - Terminal Block: All settings in Device Settings > Terminal Block, and access
 - 端子台 : [デバイス設定]> [端子台]のすべての設定、及び KVM クライアントを使用した外部接続デバイスへのアクセス
 - ユーザー管理 : [ユーザーの切断]を除く、[ユーザー管理]メニューの全ての機能

Privileges

- Device Access While Under CC-SG Management
- Device Settings
- Maintenance
- PC Share
- Security
- Terminal Block
- User Management

5. KVM ポートのアクセス権限と VM 権限を選択

KVM Port	Access	VM Access
Port 1	View	Deny

- アクセス：拒否、表示、制御
- VM アクセス：拒否、読み取り専用、読み取り/書き込み

一部の特権には、特定のアクセス許可が必要です。必要な権限を設定しないと、エラーが表示されます。

✖ Error

There is an error in port privilege section!

- To perform VM operations the user must have the Control privilege on the specific port.

Ok

6. DSAM ユニットが接続されている場合、[シリアルポート]セクションを使用して、シリアルポートのアクセス権限を選択できます。

- アクセス：拒否、表示、制御

DSAM Serial Port	Access
1.1:DSAM1 Port 1	View
1.2:DSAM1 Port 2	Control
1.3:DSAM1 Port 3	Deny
1.4:DSAM1 Port 4	Deny

- [Restrictions]セクションには、クライアントビューを制限し、キーをブロックする為のオプションがあります。

 - このグループのビューから、これらのコンポーネントを削除するには、[Hide Client Toolbar and Menu Bar]を選択。シングルマウス、フルスクリーンのスケーリングとホットキーが利用可能になります。
 - [Block Key Stroke] フィールドで、キーコードリストを選択して、このグループのユーザーがリスト内のキーを使用できないようにします。「キーコードリスト『p. 136』」をご参照ください。


Restrictions

Hide Client Toolbar and Menu Bar

Block Key Stroke

- [Save]をクリック。これらの特権と制限をユーザーに割り当てるには、ユーザーを追加または編集時にグループを選択します。

▶ ユーザーの追加方法:

- [User Management]> [Users]をクリックし、[ユーザーの追加] アイコンをクリック 。

Users ✕ +			
Enabled ▲	User Name	Full Name	Roles
✓	admin	Administrator	Admin

- ユーザー情報を入力。

フィールド/設定	内容
ユーザー名	<ul style="list-style-type: none"> ▪ Dominion KX IV-101 にログインする為に、ユーザーが入力する名前。 ▪ 4~32 文字 ▪ 大文字と小文字を区別 ▪ スペースは許可されていません。
フルネーム	<ul style="list-style-type: none"> ▪ ユーザーの姓名。 ▪ 最大 64 文字
パスワード、パスワードの認証	<ul style="list-style-type: none"> ▪ 4~64 文字 ▪ 大文字と小文字を区別 ▪ スペースは許可されています。
電話番号	ユーザーの電話番号
E-mail アドレス	<ul style="list-style-type: none"> ▪ ユーザーの E-mail アドレス ▪ 最大 128 文字 ▪ 大文字と小文字を区別
有効にする	選択すると、そのユーザーは Dominion KX IV-101 にログインできます。
次回のログイン時にパスワード変更を強制	選択すると、ユーザーが次のログイン時にパスワード変更要求が自動的に表示されます。

New User

User

Username

Full Name

Password

Confirm password

Telephone Number

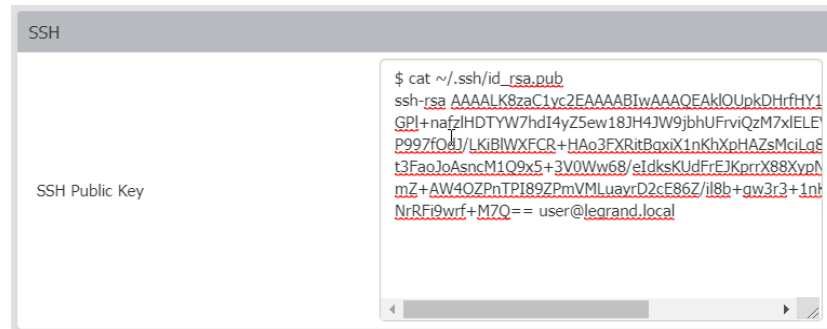
eMail Address

Enable

Force password change on next login:

3. SSH : SSH の公開鍵認証が有効になっている場合、SSH 公開鍵が必要です。
「SSH 設定 『p. 143』」をご参照ください。
4. テキストエディタで、SSH 公開鍵を開きます。

5. テキストエディタのすべてのコンテンツをコピーし、SSH 公開鍵フィールドに貼り付けます。



6. SNMPv3:SNMPv3 アクセス許可はデフォルトで無効になっています。このセクションは、SNMP 設定でアクセス許可が有効になっている場合、またはユーザーが管理者グループに属している場合に表示されます。

フィールド/設定	内容
SNMPv3 を有効にする	このユーザーによる SNMPv3 アクセスを許可する場合、このチェックボックスを選択します。 注意: SNMPv3 プロトコルは、SNMPv3 アクセスに対して有効にする必要があります。 SNMP 設定の構成をご参照ください。
セキュリティレベル	<ul style="list-style-type: none"> フィールドをクリックして、リストから優先セキュリティレベルを選択します。 なし: 認証もプライバシーもありません。これがデフォルトです。 認証: 認証であり、プライバシーはありません。 認証とプライバシー: 認証とプライバシー。

- 認証パスワード: このセクションは、「認証」、または「認証とプライバシー」が選択されている場合にのみ構成できます。

フィールド/設定	内容
ユーザーパスワードと同じ	認証パスワードがユーザーのパスワードと同じである場合、このチェックボックスを選択します。 別の認証パスワードを指定するには、チェックボックスを無効にします。
パスワード、パスワード認証	[ユーザーパスワードと同じ] チェックボックスがオフになっている場合、認証パスワードを入力します。 パスワードは、8~32 文字の ASCII 印刷可能文字で構成されている必要があります。

- プライバシーパスワード：このセクションは、[認証とプライバシー]が選択されている場合にのみ構成できます。

フィールド/設定	中身
認証パスワードと同じ	プライバシーパスワードが認証パスワードと同じである場合、このチェックボックスを選択します。 別のプライバシーパスワードを指定するには、チェックボックスを無効にします。
パスワード、パスワード認証	[認証パスワードと同じ] チェックボックスがオフになっている場合は、プライバシーパスワードを入力します。 パスワードは、8～32 文字の ASCII 印刷可能文字で構成されている必要があります。

- プロトコル：このセクションは、「認証」または「認証とプライバシー」が選択されている場合にのみ構成できます。

フィールド/設定	中身
認証	このフィールドをクリックして、目的の認証プロトコルを選択します。2つのプロトコルが利用可能です： <ul style="list-style-type: none"> ▪ MD5 ▪ SHA-1 (デフォルト)
プライバシー	<ul style="list-style-type: none"> ▪ このフィールドをクリックして、目的のプライバシープロトコルを選択します。2つのプロトコルが利用可能です： ▪ DES (デフォルト) ▪ AES-128

The image shows the SNMPv3 configuration page. It includes a header 'SNMPv3' with an expand/collapse arrow. The configuration is organized into sections:

- Enable SNMPv3:** A checked checkbox.
- Security Level:** A dropdown menu currently showing 'None', with a list of options: 'None', 'Authentication', and 'Authentication & Privacy'.
- Authentication Password:** A section containing:
 - 'Same as User Password': An unchecked checkbox.
 - 'Password': An empty text input field.
 - 'Confirm Password': An empty text input field.
- Privacy Password:** A section containing:
 - 'Same as Authentication Password': An unchecked checkbox.
 - 'Password': An empty text input field.
 - 'Confirm Password': An empty text input field.
- Protocol:** A section containing:
 - 'Authentication': A dropdown menu showing 'SHA-1'.
 - 'Privacy': A dropdown menu showing 'DES'.

1. グループ：このユーザーが属するグループを選択します。ユーザーには、グループに割り当てられた特権があります。
2. [Save]をクリック。

▶ ユーザーを編集するには;管理者のユーザー名を変更します:

1. [User Management]> [Users]をクリックし、編集するユーザーをクリックして選択。

The image shows a table titled 'Users' with the following data:

Enabled ▲	Username	Full Name	Groups	
✓	admin	Administrator	Admin	Unblock
✓	User1	User One	Admin	Unblock

2. 必要に応じてユーザー情報を変更し、[Save]をクリック。

管理者グループの特別な特権

- 下記の特別な権限は、管理者グループのみが使用できます。
-
- 復元
- 接続されたユーザーを切断
- 工場出荷時のデフォルトにリセット
- 診断
- SNMP エージェントで SNMPv3 を有効にします (SNMP の取得と設定)
- SNMPv3 ユーザーパラメーターを構成する
 - セキュリティレベル
 - 認証プロトコル
 - 認証パスワード
 - プライバシーパスワード
 - プライバシープロトコル

CHAPTER 6 デバイスの設定と情報

内容

デバイス情報	124
日付と時間	127
イベント管理	128
キーコードリスト	135
ネットワーク	136
ネットワークサービス	138
シリアルポート	143
端子台の制御	143
仮想メディア共有イメージ	146

デバイス情報

Dominion KX IV-101 の名前、システム、およびネットワークの詳細を表示するには、[デバイス情報] をクリックします。このページでは、デバイス名を変更したり、オープンソースライセンス情報を表示したりすることもできます。

▶ デバイス名の編集方法:

- [Device Information] をクリックし、[Edit] をクリックして新しい名前を入力します。
- [Save] をクリック。

The screenshot shows a dialog box titled "DKX4-101". At the top right, there is a red dashed arrow pointing to the right, followed by the text "Edit". Below this, there is a text input field labeled "Name" containing the text "DKX4-101". At the bottom right of the dialog, there are two buttons: "Cancel" with a red 'X' icon and "Save" with a checkmark icon. A mouse cursor is visible over the "Save" button.

▶ システムの詳細とステータスの表示方法:

- システムの詳細: 製品名、モデル、ファームウェアバージョン、ハードウェア ID とシリアル番号を表示します。
- システムステータス: 内部温度ステータスとローカルモニターステータスを表示します。

System	
Detail	
Product	KX4
Model	DKX4-101
Firmware Version	4.1.0.5.47190
Hardware ID	2
Serial Number	1IT8B00008
Status	
Internal Temperature Current Value	39.7°C / 103.4°F
Internal Temperature Maximum Value	40.3°C / 104.6°F
Local Monitor	Not Detected

▶ ネットワーク詳細の表示方法:

- 現在構成されているネットワークの詳細を表示します: IPv4 アドレス、MAC アドレス、リンク状態、DNS サーバー、DNS サフィックス、DNS リゾルバー設定、及び IPv4 / IPv6 ルート。

Network	
Ethernet	
IPv4 Address	192.168.56.27/24
MAC Address	00:0d:5d:00:02:da
Link State	1 GBit/s, full duplex, link OK, autonegotiation
Common	
DNS Servers	none
DNS Suffixes	none
DNS Resolver Preference	IPv6 Address
IPv4 Routes	192.168.56.0/24 dev ETHERNET default via 192.168.56.126 (ETHERNET)
IPv6 Routes	none

▶ DSAM の詳細表示方法:

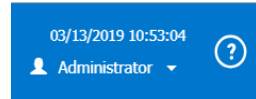
- DSAM ユニットが接続されている場合、ハードウェアの詳細 (名前、ポート番号、USB ポートの場所、モデル、ファームウェアバージョン、ハードウェア ID、シリアル番号) を表示。

DSAM	
DSAM1	
Name	DSAM1
Port Number	1
USB Port	Back Bottom
Model	DSAM-4
Firmware Version	1.0
Hardware ID	0x0
Serial Number	RKK6B00009

日付と時間

Dominion KX IV-101 の内部クロックを手動で設定するか、ネットワークタイムプロトコル (NTP) サーバーにリンクします。

Dominion KX IV-101 システムの日付と時刻は、Web インターフェイスの右上隅に表示されます。



▶ 日時の設定方法:

1. [Device Settings]> [Date/Time] をクリック。
2. タイムゾーンを選択
3. お住まいの地域が夏時間に参加している場合、[自動夏時間調整]チェックボックスが選択されていることを確認します。
4. 時間設定方法を選択します。
 - ユーザー指定時間：時間を手動で設定します。
 - NTP サーバーと同期する

ユーザー指定の時間

- カレンダーアイコンをクリックして、日付を選択します。
- 時間、分、秒で入力します。AM または PM を指定します。AM / PM をクリックして、設定を切り替えます。
- [Save] をクリック。

NTP サーバーとの同期

- DHCP によって割り当てられた NTP サーバーを使用するには: [初回と 2 回目のサーバー] フィールドを空白のままにします。DHCP によって割り当てられた NTP サーバーは、IPv4 または IPv6DHCP が有効になっている場合に使用できます。「ネットワーク 『p. 137』」をご参照ください。

NTP Settings

First Time Server

Second Time Server

Check NTP Servers

- NTP サーバーを手動で指定するには [First Time Server] フィールドにプライマリ NTP サーバーを入力。セカンダリ NTP サーバーはオプションです。[Check NTP Servers] をクリックして確認します。[Save] をクリック

NTP Settings

First Time Server

Second Time Server

Check NTP Servers

Save

イベント管理

サポートされている全てのイベントは、デフォルトでシステムログに記録されます。電子メールの送信、SNMP 通知の送信、syslog メッセージの転送等、任意のイベントに対して追加のアクションを作成することもできます。

▶ イベントとアクションの構成:

- [Device Settings]> [Event Management] をクリック
 - [Event Management] ページには、カテゴリ別にイベントが表示されます。カテゴリをクリックして、個々のイベントを表示します。この例では、「ユーザーイベント-E メール」という名前のアクションが追加され、全てのユーザーアクティビティイベントとユーザー管理イベントに割り当てられています。

Event Management + New Action

Category	Event	User events - email	System Event Log Action
> All Events	...	<input type="checkbox"/>	<input checked="" type="checkbox"/>
> Device	...	<input type="checkbox"/>	<input checked="" type="checkbox"/>
> KVM Port	...	<input type="checkbox"/>	<input checked="" type="checkbox"/>
> Serial Port	...	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▼ User Activity		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User accepted the Restricted Service Agreement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Authentication failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User logon state	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Session timeout	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
> User Administration	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save

2. イベントのチェックボックスを選択して、アクションをイベントに割り当てます。
[Save]をクリック。

▶ **アクションの追加方法:**

1. [New Action] をクリック。

Event Management + New Action

2. このアクションに名前を割り当てます。
3. 目的のアクションを選択し、構成します。
 - 電子メールアクション: 「電子メールの送信 [p. 131]」をご参照ください。
 - SNMP アクション: 「SNMP 通知 [p. 131]」をご参照ください。
 - Syslog アクション: 「Syslog メッセージ [p. 135]」をご参照ください。
4. [Create] をクリック。

E メール送信

このアクションを使用して、事前構成された SMTP 設定に従って E メールを送信するか、1 つ以上のカスタマイズされた SMTP 設定でアクションを作成します。

このアクションを、イベントに割り当てる方法については「イベント管理 『p. 129』」を、ご参照ください。

▶ メール送信アクションの作成方法:

New Action

Action Name: Email Admins

Action: Send email

Recipient Email Addresses: nina@raritan.com, steve@raritan.com

SMTP Server:

- Use default settings
 - Server Name: raritan.com
 - Sender Email Address: user@raritan.com
 - Settings can be changed in [SMTP Server settings](#).
- Use custom settings

Buttons: [Cancel] [Create]

- [Action] リストから [Send email] を選択します。
- [Recipient Email Addresses] フィールドに、受信者の E メールアドレスを入力します。複数の E メールアドレスを区切るには、コンマを使用します。
- デフォルトでは、SMTP サーバー設定がこのアクションを完了する為に使用されます。これらの設定を表示か変更するには、SMTP サーバーのハイパーリンクをクリックします。
 - 別の SMTP サーバーを使用するには、[カスタム設定を使用する] ラジオボタンをクリックします。カスタマイズされた SMTP 設定のフィールドが表示されます。「SMTP サーバーの設定 『p. 141』」をご参照ください。
- [Create] をクリック。

SNMP 通知

アクションを使用して、SNMP 通知を 1 つ以上の SNMP サーバーに送信します。

このアクションをイベントに割り当てる方法については、「イベント管理 『p. 129』」をご参照ください。

▶ SNMP 通知アクションの作成方法:

- [Action] リストから [Send SNMP notification] を選択。
- SNMP 通知のタイプを選択します。選択に基づいて、以下の手順に従ってください。

▶ SNMP v2c 通知:

New Action

Action Name

Action

Notification Type

#	Host	Port	Community
1	<input type="text" value="192.168.22.57"/>	<input type="text" value="162"/>	<input type="text" value="users"/>
2	<input type="text"/>	<input type="text" value="162"/>	<input type="text"/>
3	<input type="text"/>	<input type="text" value="162"/>	<input type="text"/>

1. [Notification Type] フィールドで [SNMPv2c Trap] を選択。
2. [Host]フィールドに、アクセスするデバイスの IP アドレスを入力。これは、SNMP システムエージェントによって、通知が送信されるアドレスです。
3. [Port]フィールドに、デバイスへのアクセスに使用するポート番号を入力。
4. [Community]フィールドに、SNMP コミュニティ文字列を入力して、デバイスにアクセスします。コミュニティは、Dominion KX IV-101 と全ての SNMP 管理ステーションを代表するグループです。
5. [Create]をクリック。

コツについて：SNMP v2c 通知アクションでは、最大 3 つの SNMP 宛先が許可されます。イベントに 3 つ以上の SNMP 宛先を割り当てる必要がある場合、すべての宛先を含む複数のアクションを作成して割り当てるのが可能です。

▶ SNMP v3 通知:

注意：複数の SNMP トラップ宛先が構成されている場合、重複した SNMP トラップ v3 secName (ユーザーID) はサポートされません。

New Action

Action Name	<input type="text" value="Syslog messages"/>
Action	<input type="text" value="Send SNMP notification"/>
Notification Type	<input type="text" value="SNMPv3 Trap"/>
Engine ID	0x800035ae8000b33777b6039fc0984c22b1bdb3017 3383275011bae2170354383
Host	<input type="text" value="192.168.22.57"/>
Port	<input type="text" value="162"/>
User ID	<input type="text" value="user"/>
Security Level	<input type="text" value="noAuthNoPriv"/>

1. [Notification Type] フィールドで、[SNMPv3 トラップ] を選択。エンジン ID は事前に入力されています。
2. 必要に応じて下記のように入力し、[OK]をクリックして設定を適用します：
 - a. ホスト：アクセスするデバイスの IP アドレスを入力。これは、SNMP システムエージェントによって通知が送信されるアドレスです。
 - b. ポート番号
 - c. ホストにアクセスする為のユーザーID。
 - d. ユーザーID に SNMPv3 権限があることをご確認ください。
 - e. ホストのセキュリティレベルを選択：

セキュリティレベル	内容
"noAuthNoPriv"	承認またはプライバシープロトコルが必要ない場合、これを選択。
"authNoPriv"	承認が必要であるがプライバシープロトコルが必要ない場合、これを選択。 認証プロトコルを選択します-MD5 または SHA 認証パスワードを入力し、認証パスワードを確認します。

セキュリティレベル	内容
"authPriv"	認証とプライバシープロトコルが必要な場合、これを選択。 認証プロトコルを選択。MD5 または SHA 認証パスワードを入力し、認証パスワードを確認。 プライバシープロトコルを選択します。DES または AES プライバシーパスワードを入力し、プライバシーパスワードを確認。

3. [Create]をクリック。

Syslog メッセージ

このアクションを使用して、イベントメッセージを指定された syslog サーバーに自動的に転送します。設定時に使用する syslog 送信メカニズムを決定します。

Dominion KX IV-101 は、syslog メッセージ送信の失敗を検出する場合と検出しない場合があります。検出された syslog の障害と理由は、イベントログに保存されます。

このアクションをイベントに割り当てる方法については、「イベント管理 『p. 129』」をご参照ください。

▶ Syslog メッセージアクションの作成方法:

New Action

Action Name

Action

Syslog Server


Transport Protocol

Legacy BSD Syslog Protocol

UDP Port

1. アクションリストから Syslog メッセージを選択。
2. [Syslog サーバー] フィールドで、syslog の転送先の IP アドレスを指定。
3. [トランスポートプロトコル] フィールドで、syslog プロトコル (UDP、TCP、または TCP + TLS) のいずれかを選択します。デフォルトは UDP です。

トランスポートプロトコル	次のステップ
UDP	<ul style="list-style-type: none"> ▪ [UDP ポート] フィールドに、適切なポート番号を入力します。デフォルトは 514 です。 ▪ 該当する場合、[レガシー-BSDSyslog プロトコル] チェックボックスを選択。
TCP	TLS 証明書は必要ありません。 [TCP ポート] フィールドに適切なポート番号を入力します。

トランスポートプロトコル	次のステップ
TCP+TLS	<p>TLS 証明書が必要です。</p> <ul style="list-style-type: none"> ▪ [TCP ポート] フィールドに適切なポート番号を入力します。デフォルトは 6514 です。 ▪ [CA 証明書] フィールドで、TLS 証明書をクリック  して選択。証明書をインポートした後、[表示]をクリックしてその内容を表示するか、[削除]をクリックして削除します。 ▪ 選択した証明書チェーン内の TLS 証明書が古くなっているか、まだ有効でない場合でもイベントメッセージを許可するには、[期限切れでまだ有効でない証明書を許可する] チェックボックスをオンにします。

4. [Create]をクリック。

キーコードリスト

キーコードリスト機能を使用して、使用をブロックするキーのリストを作成。リストをユーザーグループに割り当てて、グループがこれらのキーを使用出来ないようにします。キーコードリストは、キーボードの言語タイプごとに作成されます。キーボードタイプごとにブロックできるキーのリストが、提供されます。

F1 ユーザーに複数のブロックされたキーコードリストが割り当てられている場合、全てのキーコードリストに含まれていない場合、特定のキーを使用できます。(例) ユーザーは List1 と List2 の両方が割り当てられたグループに属しています。List1 が F1 を制限しているが、List2 が F1 を制限していない場合、ユーザーは F1 を使用できます。

▶ 新しいキーコードリストの追加方法:

1. [Device Settings]> [Keycode List] をクリック。
2. [New]をクリック。
3. キーセット名を入力して、ブロックするキーのこのリストを識別します。
キーセット名は、リストをユーザーグループに割り当てるときに使用されます。「ユーザーとグループ」『p. 116』をご参照ください。
4. 言語でキーボードタイプを選択。
5. [キー]リストからブロックする各キーを選択し [Add Key] をクリック。
追加されたキーが[選択されたキー]リストに表示されます。リストからキーを削除するには、[削除]ボタンをクリック。
6. 完了したら、[Add Keyset]をクリック。

▶ キーコードリストの編集方法:

1. [Device Settings]> [Keycode List] をクリック。
2. キーコードリストを名前をクリックして選択。選択したリストは青色で強調表示されます。
3. [Edit]をクリックしてリストを変更し、[キーセットの変更] をクリックして保存。

▶ キーコードリストの削除方法:

1. [Device Settings]> [Keycode List] をクリック。

2. キーコードリストを名前でクリックして選択。選択したリストは青色で強調表示されます。
3. [削除]をクリックして、リストを削除。

▶ キーセットからユーザーグループをブロックする方法:

[ユーザー管理]> [グループ設定] でキーセットを選択。「ユーザーとグループ『p. 116』」をご参照ください。

ネットワーク

デフォルトのネットワーク設定は、IPv4 に対して DHCP 対応です。自動的に割り当てられた IP アドレスは、[デバイス情報] ページにあります。「デバイス情報『p. 125』」をご参照ください。

注意：デバイスが CC-SG の管理下にある場合、ネットワーク設定を変更すること不可。

▶ IPv4 設定:

フィールド/設定	内容
IPv4 を有効にする	IPv4 プロトコルを有効または無効にします。
IP 自動構成	<ul style="list-style-type: none"> ▪ Select the method to configure IPv4 settings. ▪ <i>DHCP</i>: DHCP サーバーを介して IPv4 設定を自動構成します。 ▪ <i>静的</i>: IPv4 設定を手動で構成します。

-
-
- DHCP 設定：オプションで、下記の要件を満たす必要がある優先ホスト名を指定します：
 - 英数字、および/またはハイフンで構成されます
 - ハイフンで開始または終了することはできません
 - 数字で始めることはできません
 - 句読点、スペース、その他の記号を含めることはできません
 - 最大 253 文字
- 静的設定：この構文「IP アドレス/プレフィックス長」に従う静的 IPv4 アドレスを割り当てます。
(例)：192.168.84.99/24

▶ IPv6 設定:

フィールド/設定	内容
IPv6 を有効にする	IPv6 プロトコルを有効または無効にします。
IP 自動構成	IPv6 設定の構成方法を選択します。 <ul style="list-style-type: none"> ▪ <i>自動</i>: DHCPv6 を介して IPv6 設定を自動構成します。 ▪ <i>静的</i>: IPv6 設定を手動で構成します。

- 自動設定: オプションで、上記の要件を満たす必要がある優先ホスト名を指定します。
- 静的設定 : この構文「IP アドレス/プレフィックス長」に従う静的 IPv6 アドレスを割り当てます。

(例): `fd07:2fa:6cff:1111::0/128`

▶ インターフェイス設定:

フィールド	内容
スピード	<ul style="list-style-type: none"> ▪ LAN 速度を選択します。 ▪ 自動: システムは、自動ネゴシエーションを通じて最適な LAN 速度を決定します。 ▪ 10MBit/ s: 速度は常に 10Mbps です。 ▪ 100MBit/ s: 速度は常に 100Mbps です。 ▪ 1GBit/ s: 速度は常に 1 Gbps (1000 Mbps) です。
デュプレックス	<ul style="list-style-type: none"> ▪ デュプレックスモードを選択します。 ▪ 自動: Dominion KX IV-101 は、自動ネゴシエーションを通じて最適な送信モードを選択します。 ▪ フル: データは両方向に同時に送信されます。 ▪ 半分: データは一度に一方 (Dominion KX IV-101 との間で) に送信されます。
現在の状態	現在の速度やデュプレックスモード等、LAN の現在のステータスを表示します。

注意: Dominion KX IV-101 の速度とデュプレックスの両方の設定を、NON-Auto 値に設定すると、自動ネゴシエーションが無効になり、デュプレックスの不一致が発生する可能性があります。

▶ 一般的なネットワーク設定:

一般的なネットワーク設定はオプションです。特定のローカルネットワーク要件がない場合、デフォルト設定のままにします。

フィールド	内容
DNS リゾルバの比較	DNS リゾルバが、IPv4 アドレスと IPv6 アドレスの両方を返すときに使用する IP アドレスを決定します。 <ul style="list-style-type: none"> IPv4 アドレス: IPv4 アドレスを使用。 IPv6 アドレス: IPv6 アドレスを使用。
DNS サフィックス (オプション)	必要に応じて DNS サフィックス名を指定します。
1 番目/ 2 番目の DNS サーバー	静的 DNS サーバーを手動で指定。 <ul style="list-style-type: none"> これらのフィールドに静的 DNS サーバーが指定されている場合、DHCP によって割り当てられた DNS サーバーが上書きされます。 IPv4/ IPv6 設定に DHCP (または自動) が選択され、静的 DNS サーバーが指定されていない場合、Dominion KX IV-101 は DHCP によって割り当てられた、DNS サーバーを使用。

ネットワークサービス

Dominion KX IV-101 は、下記ネットワーク通信サービスをサポートしています。

- ディスカバリー
- HTTP/HTTPS
- SMTP サーバー
- SNMP
- SSH

ディスカバリーポート

Dominion KX IV-101 は、User Station や CC-SG などの他の Raritan 製品との通信にデフォルトのディスカバリーポート 5000 を使用。必要に応じてポート番号を変更できますが、デバイスが CC-SG の管理下にある間は、変更できません。

暗号化オプションが選択されていない限り、デバイスはそれ自体に関する情報（メーカー、モデル、ファームウェアバージョン、暗号化）をクリアテキストで送信します。

▶ 初期のディスカバリーポートの変更方法:

1. [Device Settings]> [Network Services]> [Discovery Port] をクリック。
2. ポート番号を入力。
3. [Encrypted] チェックボックスを選択して、デバイス情報の送信を暗号化します。
4. [保存] をクリック

The screenshot shows a configuration window titled "Network Services | Discovery". It contains a "Discovery Port" input field with the value "5000". Below it is a checked checkbox labeled "Encrypted". At the bottom right, there are two buttons: "Cancel" (with an 'X' icon) and "Save" (with a checkmark icon).

HTTP/HTTPS ポート

Dominion KX IV-101 は、デフォルトの HTTP / HTTPS ポート 80/443 を使用します。必要に応じてデフォルトを変更可能。

HTTP アクセスは HTTPS にリダイレクトされます。

▶ デフォルトの HTTP / HTTPS ポートの変更方法:

1. [デバイス設定]> [ネットワーク設定]> [HTTP / HTTPS ポート] をクリック。
2. HTTP を有効にする必要がある場合、[HTTP アクセス] チェックボックスを選択。

注意: HTTP が無効になっている場合、AKC は HTTPS 経由でダウンロードされます。Microsoft .NET は、デバイスの TLS 証明書が有効かどうかを確認します。デバイス証明書は「信頼されたルート証明機関」ゾーンに追加する必要があり、証明書の共通名はデバイスの IP アドレス、またはホスト名と一致する必要があります。

3. ポート番号を入力し、[Save] をクリック。

Network Services | HTTP/HTTPS

HTTP

HTTP Access Enable

Port

HTTPS

Port

Cancel Save

4. デバイスへの接続は、新しい HTTP / HTTPS ポート番号で更新されます。再度ログインする必要があります。

SMTP サーバー設定

イベントメールを送信するには、SMTP 設定を構成し、SMTP サーバーの IP アドレスと送信者のメールアドレスを入力する必要があります。「イベント管理 『p. 129』」をご参照ください。

電子メールメッセージが正常に送信されなかった場合、失敗イベントと理由がイベントログに記録されます。「イベントログ 『p. 163』」をご参照ください。


▶ SMTP サーバー設定の方法:

1. [Device Settings]> [Network Services]> [SMTP サーバー] をクリック。
2. 必要な情報を入力。

フィールド	内容
IP アドレス/ホスト名	メールサーバー名、または IP アドレスを入力。
ポート	ポート番号を入力。 <ul style="list-style-type: none"> ▪ デフォルトは 25
送信者のメールアドレス	送信者のメールアドレスを入力。
送信の再試行回数	Eメールの再試行回数を入力します。 <ul style="list-style-type: none"> ▪ デフォルトは 2 回です
再試行を送信する間隔	Eメールの再試行の間隔を、分単位で入力します。 <ul style="list-style-type: none"> ▪ デフォルトは 2 分です。
サーバーには認証が必要	SMTP サーバーでパスワード認証が必要な場合、このチェックボックスを選択してから、ユーザー名とパスワードを入力。
ユーザー名 パスワード	<ul style="list-style-type: none"> ▪ 4~64 文字使用できます。大文字と小文字を区別。 ▪ ユーザー名にスペースは使用できません。 ▪ パスワードにはスペースを使用可能。

フィールド	内容
SMTP over TLS を有効 (StartTLS)	SMTP サーバーが TLS をサポートしている場合、このチェックボックスを選択。

● **Settings for the CA Certificate:**

フィールド/設定	内容
	<ul style="list-style-type: none"> ▪ [Browse]をクリックして、証明書ファイルをインポートします。次に、下記が可能。 ▪ [表示]をクリックして、証明書の内容を表示します。 ▪ インストールされている証明書を削除するには、[削除]をクリック。
期限切れでまだ有効ではない証明書を許可	<ul style="list-style-type: none"> ▪ 証明書の有効期間に関係なく、認証を成功させるには、このチェックボックスを選択。

3. 設定のテスト方法：
 - a. 受信者のメールアドレスを入力します。複数のメールアドレスはカンマで区切ります。
 - b. [テストメールを送信] をクリックして、メールが受信されたことを確認します。
4. [Save]をクリック

注意：Dominion KX IV-101 デバイスの TLS ベースのプロトコルは、AES128 と 256 ビット暗号をサポートします。使用する正確な暗号は、デバイスとクライアント Web ブラウザの間でネゴシエートされます。特定の暗号を強制するには、クライアントのドキュメントで AES 設定の構成を確認してください。

SNMP 設定

SNMP マネージャーと Dominion KX-101 間の SNMP 通信を有効/無効にできます。

▶ **SNMP 通信の構成方法:**

1. [Device Settings]> [Network Services]> [SNMP]をクリック。
2. 対応するチェックボックスをクリックして、SNMP v1 / v2c および/または SNMPv3 を有効/無効にします。
 - a. SNMP v1 / v2c 読み取り専用アクセスは、デフォルトで有効になっています。デフォルトの「コミュニティ文字列の読み取り」は「public」です。
 - b. 読み取り/書き込みアクセスを有効にするには、「コミュニティ文字列の書き込み」と入力。通常、文字列は「プライベート」です。

3. 必要に応じて、MIB-II システムグループ情報を入力します。
 - a. sysContact-システムの担当者
 - b. sysName-システムに割り当てられた名前
 - c. system sysLocation-システムの場所
4. ダウンロードリンクをクリックして、SNMP マネージャーで使用する SNMPMIB を取得します。
5. [Save]をクリック。

SNMP

SNMP Agent

Enable SNMP v1 / v2c

Read Community String

Write Community String

Enable SNMP v3

MIB-II System Group

sysContact

sysName

sysLocation

Download MIBs

RADM-MIB	download
----------	--------------------------

SSH 設定

CLI への SSH アクセスを、有効/無効にしたり、TCP ポートを変更。SSH 経由でログインする為のパスワード、または公開鍵を設定したりします。

▶ SSH 設定:

1. [Device Settings]> [Network Services]> [SSH]をクリック。
2. SSH アクセスを有効/無効にするには、チェックボックスを選択/選択解除します。
3. デフォルトのポート 22 を変更するには、ポート番号を入力。
4. 認証方法の 1 つを選択します。
 - パスワード認証のみ：パスワードベースのログインのみを有効にします。
 - 公開鍵認証のみ：公開鍵ベースのログインのみを有効にします。

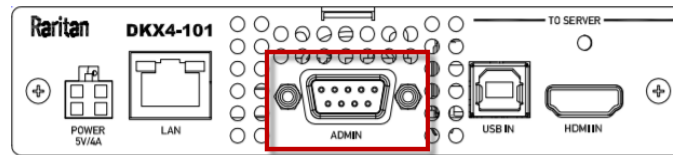
- パスワードと公開鍵認証：パスワードと公開鍵ベースのログインの両方を有効にします。これにより、どちらのログイン認証方法も使用できます。これがデフォルト設定です。

公開鍵認証が選択されている場合、SSH 接続を介してログインするには、各ユーザープロファイルに有効な SSH 公開鍵を入力する必要があります。「ユーザーとグループ『p. 116』」を参照してください。

5. [Save]をクリック。

シリアルポート

シリアルポート設定は、Dominion KX IV-101 シリアルポートのボーレートを制御します。Dominion KX IV-101 のシリアルポートは、CLI シリアルコンソールの使用のみをサポート。



▶ シリアルポートの設定方法:

1. [Device Settings]> [Serial Port] をクリック。
2. ボーレートを入力し、[Save]をクリック。

Serial Port

Baud Rate bit/s

端子台の制御

端子台制御機能を使用すると、Dominion KX IV-101 の端子台に接続されている外部デバイスを構成できます。

Dominion KX IV-101 には、1つの入力端子 + 1つの出力端子があります。

▶ 入力端子:

- 2本ピン
- 外部プッシュボタンまたはスイッチ入力をサポート
- バイナリスイッチのみ
- ユースケース：ターゲットでメンテナンスが実行されているときに、リモートアクセスをオフにする

▶ 出力端子:

- 3本ピン
- 2つのリレー。1つは常時開 (NO)、もう1つは常時閉 (NC) です。両方のリレーは同じ共通点を共有する為、1つだけを使用することをお勧めします。両方を同時に使用する場合は、コモンを正しく配線する必要があります。
- 使用例：サーバーの電源ボタンを使用して、リモート電源制御を実行する、リモートユーザーが接続されているときにライトをオンにする、ドアロックまたはカメラをオンにする。
- サポートされている出力デバイス：LED、ブザー、PC 電源ボタン。出力デバイスは、独自の電力を提供する必要があります。

▶ 権限:

端子台制御の構成と使用に関連する権限には、いくつかの種類があります。

- 端子台の設定を行うには、端子台の権限が必要です。「ユーザーとグループ『p. 116』」をご参照ください。この権限を使用すると、[デバイス設定]> [端子台制御] ページにアクセスして、入力と出力を有効/無効にしたり、リモートユーザーとローカルユーザーの入力制御を許可する権限を設定したり、出力制御のアクションを構成したりできます。以下の手順をご参照ください。
- [端子台] ページでアクセス許可を設定することに加えて、全てのリモートユーザーとローカルユーザーにポートアクセス許可を与える必要があります。KVM クライアントの外部デバイスメニューには、適切に組み合わせられた権限を持つユーザーがアクセスできます。「ユーザーとグループ『p. 116』」をご参照ください。
- ローカルポート出力を有効にする必要があります。[セキュリティ]> [KVMセキュリティ]> [ローカルポート出力を無効にする] を設定すると、他の全てのアクセス許可が上書きされます。「KVMセキュリティ『p. 152』」をご参照ください。

▶ 端子台の制御設定: 入力

1. [Device Settings]> [Terminal Block Control] をクリック。

入力構成	
外部入力スイッチを有効	入力スイッチを有効/無効にします。
現在の外部入力スイッチの状態	現在の状態が表示されます：オープンまたはクローズ。 スイッチ状態が開いているとき、デバイスは正常に機能します。
リモートコンソールユーザーに与える	リモートコンソールユーザーのアクセス許可を選択します。 <ul style="list-style-type: none"> ▪ デフォルト設定。 ▪ ビデオのみ ▪ アクセス不可：ビデオ、キーボード、及びマウスのアクティビティは許可されていません。VMセッションとKVMセッションは終了し、ターゲットへの接続は許可されていません。
ローカルコンソールユーザーに与える	ローカルコンソールユーザーのアクセス許可を選択します。 <ul style="list-style-type: none"> ▪ フルアクセス ▪ ビデオのみ ▪ アクセスなし

2. [Save]をクリック。

Terminal Block Control

Input

Enable External Input Switch

Current External Input Switch State Open

Give Remote Console User Full Access Video Only No Access

Give Local Console User Full Access Video Only No Access

▶ 端子台の制御出力の設定とアクション:

1. [Device Settings]> [Terminal Block Control] をクリック。
2. 下にスクロールして、出力設定とアクションを確認します。

3.

出力構成	
外部デバイスを有効	外部デバイスを有効/無効にします
外部デバイスの状態	<ul style="list-style-type: none"> 外部デバイスの状態が表示されます。 オン オフ 点滅 無効
アクション	<p>外部デバイスで実行する出力アクションのラジオボタンを選択します。</p> <ul style="list-style-type: none"> 外部デバイスのオン/オフを切り替える：[オン]または[オフ]をクリックします。 外部デバイスのパルス：オフからオン、またはオンからオフのいずれかで、デバイスにパルスを送信します。パルスの初期状態は、ボタン「オン」と「オフ」をクリックすることで変更可能。 外部デバイスの点滅：点滅間隔が必要に応じて設定されていることを確認します。
点滅/パルス間隔	<p>点滅またはパルスの間隔を 0.5 秒で設定します。デフォルトは 1 です。</p> <ul style="list-style-type: none"> 点滅範囲：1～10 パルス範囲：1～100

4. [Save]をクリック。

端子台をマザーボードに接続する

Dominion KX IV-101 は、端子台を外部デバイスのマザーボード上のピンに接続することにより、電源 SW またはリセット SW のいずれかの 1 つの外部スイッチを制御可能。

殆どのマザーボードには、電源 SW とリセット SW ヘッダーがあります。これらは通常、ケースのフロントパネルにある押しボタンに接続されています。

- Dominion KX IV-101 の端子台の NO（ノーマルオープン）に 2 ピンヘッダーを接続。

仮想メディア共有イメージ

仮想メディアを使用して、ファイルサーバーの ISO イメージにアクセスする場合、仮想メディア共有イメージを構成します。 ISO9660 フォーマットがサポートされている標準です。ただし、他の CD-ROM 拡張機能も機能する場合があります。

Virtual Media Shared Images

No.	IP Address / Hostname	Share Name	Image Path	Enable SAMBA v1.0
1	192.168.1.211	isos	/fedora28.iso	no
2	windows2012.systemtestest2.local	isos	windows2016.iso	no
3	windows2012.systemtestest2.local	isos	/OSFiles/ubuntu18.iso	no
4	fedora.systemtestest2.local	sambaguest	/OSFiles/openSUSE.iso	no
5	192.168.1.12	isoshare	/Fedora29.iso	yes

New Edit Delete Test Connection

注意：ファイルサーバーでは、SMB / CIFS のサポートが必要です。

▶ 仮想メディアアクセス用のファイルサーバーISO イメージの指定方法:

- [Device Settings]> [Virtual Media Shared Images] をクリック。
- [新規]をクリックして、共有イメージを追加します。
- アクセスするファイルサーバーの ISO イメージに関する情報を入力します：
 - IP アドレス/ホスト名：ファイルサーバーのホスト名または IP アドレス。
 - 共有名：ISO イメージの共有名の部分。
 - イメージパス：ISO イメージの場所のフルパス名。(例) / path0 / image0.iso、 ¥ path1 ¥ image1.iso などです。
 - Dominion KX IV-101 が古いバージョンの Samba を使用できるようにするには、[Samba1.0を有効にする] チェックボックスを選択します。チェックを外すと、Samba3.0 が使用されます。
- [Test Connection] をクリックして確認します。
- [Add Shared Image] をクリック。

チャプター7 セキュリティ

内容

グループベースのアクセス制御	148
IP アクセス制御	149
KVM セキュリティ	150
ログイン設定	153
パスワードポリシー	154
TLS 証明書	155
役務契約	158

グループベースのアクセス制御

グループベースのアクセス制御ルールは、ユーザーグループのメンバーに適用される事を除いて、IP アクセス制御ルールに似ています。これにより、IP アドレスに基づいてグループにシステム権限を付与できます。

ルールは番号順に実行される為、ロールベースのアクセス制御ルールの順序は重要です。

▶ IPv4 または IPv6 グループベースのアクセス制御ルールの作成方法:

1. [Security]> [Group Based Access Control] を選択。
2. [Enable Group Based Access Control for IPv4] を選択するか、下にスクロールして [IPv6] のチェックボックスを選択。

#	Start IP	End IP	Group	Policy	
1	192.168.22.57	192.168.22.59	Admin	Deny	↑ ↓ 🗑️

3. デフォルトのポリシーを決定します。
 - 承諾: 一致するルールが存在しない場合にトラフィックを受け入れます。
 - 拒否: 一致するルールが存在しない場合、ユーザーのログイン試行を拒否します。
4. ルールを作成し、優先順位を付けます。
 - [Start IP] と [End IP]、ルールを適用する[グループ]、および[ポリシー]を入力します。
 - [Append]をクリックして、別ルールを追加します。ルールを別ルールの上に追加するには、ルールを選択して [Insert Above] をクリック。
 - ルールを順番に並べ替えるには、各ルールの矢印ボタンをクリックします。

- ルールを削除するには、ごみ箱アイコンをクリックします。
5. [Save]をクリック。IPv4 ルールと IPv6 ルールは別々に保存される事にご注意下さい。

IP アクセス制御

IP アクセス制御ルール（ファイアウォールルール）は、トラフィックを送受信するホストの IP アドレスに基づいて、Dominion KX IV-101 との間のトラフィックを受け入れるか破棄するかを決定します。ルールを作成するときは、下記の原則に留意してください。

▪ **ルールの順序は重要です。**

トラフィックが Dominion KX IV-101 に到達するか、Dominion KX IV-101 から送信されると、ルールは番号順に実行されます。IP アドレスに一致する最初のルールのみが、トラフィックを受け入れるか破棄するかを決定します。IP アドレスに一致する後続のルールはすべて無視されます。

▪ **プレフィックスの長さが重要です。**

IP アドレスを入力するときは、CIDR 表記で指定する必要があります。つまり、アドレスとプレフィックス長の両方が含まれます。(例)プレフィックス長が、24 ビットの単一のアドレスを指定するには、下記の形式を使用します：

x.x.x.x/24

/24 = プレフィックスの長さ。

▶ **IPv4 または IPv6 IP アクセス制御ルールの作成方法：**

1. [Security]> [IP Access Control] を選択。
2. [IPv4 の IP アクセス制御を有効にする] を選択するか、下にスクロールして [IPv6] のチェックボックスを選択。
3. デフォルトポリシーを選択：
 - 承諾：すべてのアドレスからのトラフィックを受け入れます。
 - ドロップ：送信元ホストに障害通知を送信せずに、全てのアドレスからのトラフィックを破棄します。
 - 拒否：全てのアドレスからのトラフィックを破棄し、ICMP メッセージを送信元ホストに送信して障害を通知します。
4. 必要に応じて、[インバウンドルール]セクション、または[アウトバウンドルール]セクションに移動します。
 - インバウンドルールは、Dominion KX IV-101 に送信されるデータを制御します。
 - アウトバウンドルールは、Dominion KX IV-101 から送信されるデータを制御。
5. ルールを作成し、優先順位を付けます。
 - アドレスとマスクを入力し、ポリシーを選択。
 - [Append]をクリックして、別ルールを追加します。ルールを別ルールの上に追加するには、ルールを選択して[上に挿入]をクリックします。
 - ルールを順番に並べ替えるには、各ルールの矢印ボタンをクリックします。選択したルールが青色で表示されます。
 - ルールを削除するには、ごみ箱アイコンをクリック。

IP Access Control

IPv4

Enable IPv4 Access Control

Inbound Rules

Default Policy: Accept

#	IP/Mask	Policy	
1	192.168.22.57/24	Drop	↑ ↓ 🗑️

Append
Insert Above

Outbound Rules

Default Policy: Accept

#	IP/Mask	Policy	
no rules defined			

Append
Insert Above

✔ Save

6. [Save]をクリック。IPv4 ルールと IPv6 ルールは別々保存される事に注意して下さい。

KVM セキュリティ

KVM セキュリティ設定ページには、暗号化モード、仮想メディア、ローカルポート、及びデバイスにローカルで影響を与える、その他の機能のオプションが含まれています。

▶ KVM セキュリティ設定の構成方法:

1. [Security]> [KVM Security] をクリック。

2. 必要に応じてオプションを選択します。

フィールド/設定	内容
KVM と仮想メディアに暗号化モードを適用	KVM だけでなく仮想メディアにも暗号化を使用するには、このチェックボックスを選択。
PC 共有	PC 共有を選択して同時リモート KVM アクセスを許可し、最大 8 人のリモートユーザーが 1 つの Dominion KX IV-101 に同時にログインし、デバイスを介して同じターゲットサーバーを同時に表示と制御できるようにします。
PC 共有アイドルタイムアウト	PC 共有モードのユーザーにアイドル時間制限を設定します。ユーザーがマウスを動かしていないか、キーボード入力を入力しておらず、タイムアウト期間が終了した場合、ユーザーは制御を放棄し、別のユーザーがターゲットのキーボードとマウスの制御にアクセス可能。
仮想メディア共有	このオプションは、PC 共有モードが有効になっている場合にのみ使用できます。選択すると、仮想メディア共有により、複数のユーザー間で仮想メディアとオーディオを共有できます。つまり、複数のユーザーが同じ仮想メディア、またはオーディオセッションにアクセスできます。デフォルトでは無効になっています。
ローカルポート出力を無効にする	端子台制御機能を使用する場合、このチェックボックスがオフになっていることを確認してください。[ローカルポート出力を無効にする] が選択されている場合、この設定は端子台制御の他の全てのアクセス許可を上書きします。「端子台の制御 『p. 145』」をご参照ください。

フィールド/設定	内容
ローカルデバイス リセットモード	<p>このオプションは、デバイスのハードウェアリセットボタンが押されたときに実行されるアクションを指定します。</p> <p>下記のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ローカルファクトリリセットを有効にする (デフォルト): Dominion KXIV-101 デバイスを、工場出荷時の初期に戻します。 ローカル管理者パスワードのリセットを有効にする: ローカル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」にリセットされます。 全てのローカルリセットを無効にする: リセットアクションは実行されません。
URL 経由の直接ポートアクセスを有効にする	<p>選択すると、ユーザーは Dominion KX IV-101 のログイン・クレデンシャルを URL に入力する事でターゲットに直接アクセスできます。「ダイレクトポートアクセス URL 『p. 153』」をご参照ください。</p>

直接ポートアクセス URL

ダイレクトポートアクセスが有効になっている場合、ブックマークできる特別な URL を使用してターゲットに直接アクセスできます。これにより、Dominion KX IV-101 へのログインをバイパスしてターゲットに接続できます。

- ユーザー名とパスワードはオプションです。ユーザー名とパスワードが指定されていない場合、ログインダイアログが表示され、認証された後、ユーザーはターゲットに直接接続されます。
- ポートは、ポート番号またはポート名場合があります。ポート名を使用している場合、名前は一意である必要があります。そうでない場合、エラーが報告されます。ポート番号は「1」です。
- ポートを完全に省略すると、エラーが報告されます。
- ユーザー名、パスワード、またはポート名の特殊文字は、エンコードされた URL コードで渡す必要があります。

▶ VKCS を使用した直接ポートアクセス:

VKCS と直接ポートアクセスを使用している場合、標準ポートに下記の構文のいずれかを使用します。

▪ <code>https://IPaddress/dpa.asp?username=username&password=password&port=1&client=vkcs</code>
▪ <code>https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=vkcs</code>

▶ AKC による直接ポートアクセス:

AKC と直接ポートアクセスを使用している場合、標準ポートに下記の構文のいずれかを使用します。

▪ <code>https://IPaddress/dpa.asp?username=username&password=password&port=1&client=akc</code>
▪ <code>https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=akc</code>

▶ HKC による直接ポートアクセス:

HKC と直接ポートアクセスを使用している場合、標準ポートに下記の構文のいずれかを使用します。

▪ <code>https://IPaddress/dpa.asp?username=username&password=password&port=1&client=hkc</code>
▪ <code>https://IPaddress/dpa.asp?username=username&password=password&portname=port name&client=hkc</code>

ログインログイン設定

[Login Settings] ページには、ユーザーのブロックとログイン制限のオプションが含まれています。

▶ ログイン設定の構成方法:

1. [Security]> [Login Settings] をクリック。
2. 失敗したログインでユーザーをブロックするには、[Block user on login failure] チェックボックスをオンにして、パラメーターを構成します。
 - ブロックタイムアウト：ログインに失敗したユーザーがログインをブロックされる期間を選択します。
 - 失敗したログインの最大数：ユーザーがブロックされる前に、実行できる失敗したログインの数を入力します。
3. アイドル期間後に、ユーザーを自動的にログアウトするには、[Idle timeout period] フィールドで時間を選択。アイドル状態のユーザーがログインしたままにできるようにするには、「Infinite」を選択します。
4. [Prevent concurrent login with same username] を選択して、同じユーザー名で複数のユーザーがログインしないようにします。この設定は、初期の管理者ユーザーには適用されません。

Login Settings

User Blocking

Block user on login failure

Block timeout

Maximum number of failed logins

Login Limitations

Idle timeout period

Prevent concurrent login with same username

5. [Save]をクリック。

パスワードポリシー

[パスワードポリシー]ページには、パスワードのエージングと強力なパスワードの設定が含まれています。

▶ パスワードポリシーの設定方法:

1. [Security]> [Password Policy] をクリック。
2. パスワードエージングを有効にするには、ユーザーが選択した間隔でパスワードを変更するように強制します。
 - パスワードエージング間隔の[Enabled]チェックボックスを選択。
 - 7日から365日までのパスワードエージング間隔を選択します。

Password Policy

Password Aging

Password Aging Interval Enabled

Password Aging Interval

3. 強力なパスワードを有効にして、それらのパラメーターを設定するには、下記のようにします。
 - 強力なパスワードの[Enabled]チェックボックスを選択。
 - パスワードの最小長と最大長を設定。最小値は8です。最大値は64です。
 - オプションを選択して、少なくとも1つの小文字、大文字、数字、および/または特殊文字を適用します。

- パスワード履歴サイズを指定します。これは、パスワードを再利用できる頻度を制御します。最大は 12 です。

Strong Passwords

Strong Passwords Enabled

Minimum Password Length

Maximum Password Length

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one special character

Password History Size

4. [Save]をクリック。

TLS 証明書

Dominion KX IV-101 は、Dominion KX IV-101 と接続されたクライアント間の暗号化されたネットワークトラフィックに TLS1. 3 を使用します。接続を確立するとき、Dominion KX IV-101 は、暗号化証明書を使用してクライアントに対して自身を識別する必要があります。Dominion KX IV-101 には、独自の証明書に置き換える必要のある、初期の証明書が含まれています。

Dominion KX IV-101 は、SHA-2 を使用して証明書署名要求 (CSR)、または自己署名証明書を生成できます。

CA は、CSR の発行者の身元を確認します。次に、CA はその署名を含む証明書を発行者に返します。有名な CA の署名が付いた証明書は、証明書の提示者の身元を保証するために使用されます。

重要: Dominion KX IV-101 の日付/時刻が正しく設定されている事をご確認下さい。

自己署名証明書が作成されると、Dominion KX IV-101 の日付/時刻が有効期間の計算に使用されます。Dominion KX IV-101 の日付/時刻が正確でない場合、証明書の有効な日付範囲が正しくない為、証明書の検証が失敗する可能性があります。「日付と時刻 『128 ページ』」をご参照ください。

注意：CSR は、Dominion KX IV-101 で生成する必要があります。

注意：ファームウェアをアップグレードする場合、アクティブな証明書と CSR は置き換えられません。

▶ **アクティブな証明書とキーを、表示及びダウンロードするには、下記手順に従います：**

1. [Security]> [TLS Certificate] をクリック。アクティブな証明書の詳細が表示されます。

Active TLS Certificate

Subject		Issuer	
Country	US	Country	US
State or province	NJ	State or province	NJ
Locality	Somerset	Locality	Somerset
Organization	Raritan Americas, Inc.	Organization	Raritan Americas, Inc.
Organizational unit	Engineering	Organizational unit	Engineering
Common name	Raritan KVM	Common name	Raritan CA
Email address	not set	Email address	not set

Miscellaneous	
Not valid before	Feb 13 21:35:57 2015 GMT
Not valid after	Feb 9 21:35:57 2030 GMT
Serial number	03
Key length	2048 bits

[Download Certificate](#)

2. [Download Key] と [Download Certificate] をクリックして、アクティブな証明書ファイルを取得します。

▶ **新しい SSL 証明書を作成してインストールする方法：**

1. [Security]> [TLS Certificate] をクリック。[New TLS Certificate] セクションまで下にスクロールします。
2. 件名フィールドに入力：
 - Country: (ISO コード) -組織が存在する国。これは 2 文字の ISO コード。例：ドイツの場合は DE、米国の場合は US
 - State or Province: -組織が存在する州、または県。
 - Locality: 組織が存在する都市。
 - Organization: Dominion KX IV-101 が属する組織名。
 - Organizational unit: このフィールドは、組織内の Dominion KX IV-101 が属する部門を指定するために使用されます。

- Common Name: ネットワークにインストールされた後の Dominion KX IV-101 のネットワーク名 (通常は完全修飾ドメイン名)。一般名は、Web ブラウザを使用して Dominion KX IV-101 にアクセスするために使用される名前と同じですが、接頭辞「http://」はありません。ここに記載されている名前と実際のネットワーク名が異なる場合、HTTPS を使用して Dominion KX IV-101 にアクセスすると、ブラウザにセキュリティ警告が表示されます。
 - Email address: Dominion KX IV-101 と、そのセキュリティを担当する連絡担当者の E メールアドレス。
3. [Add Name] ボタンをクリックして、最大 10 個のサブジェクト代替名 (SAN) を追加し、フィールドにホスト名または IP を入力。 SAN は、証明書が有効になるホスト名または IP アドレスです。
 4. 生成するには、下記のいずれかを実行します：
 - 自己署名証明書を生成するには、下記の手順を実行します。
 - a. [Key Creation Parameters] で [Self-Sign] チェックボックスを選択。このオプションを選択すると、Dominion KX IV-101 はエントリーに基づいて証明書を生成し、署名認証局として機能します。署名付き証明書を生成するために、CSR をエクスポートして使用する必要はありません。
 - b. 有効期間を日数で設定します。これは、この証明書の有効期限が切れるまでの日数を制御します。 Dominion KX IV-101 の日付/時刻が正しいことを確認してください。日付/時刻が正しくない場合、証明書の有効な日付範囲が正しく計算されない可能性があります。
 - c. [Create New TLS key] をクリック。
 - d. ページが更新されると、[新しい TLS 証明書] セクションに新しいボタンが表示され、新しく生成された自己署名証明書とキーをインストール、ダウンロード、または削除する事が可能。
 - e. 新しい証明書の使用を開始するには、[キーと証明書のインストール] をクリック。
 - f. 証明書が読み込まれると、ページが更新される場合があります。
 - 認証のために、CA に送信する CSR を生成方法：
 - a. [キー作成パラメーター] で、[Challenge] フィールドと [Confirm challenge] フィールドにパスワードを入力します。
 - b. [Create New TLS Key] をクリック。
 - c. ページが更新されると、[新しい TLS 証明書] セクションに新しいボタンが表示され、CSR のダウンロード、キーのダウンロード、または CSR の削除を行う事ができます。
 - d. [証明書署名要求のダウンロード] ボタンをクリックして、CSR をダウンロードします。 [キーのダウンロード] ボタンをクリックして、秘密キーを含むファイルをダウンロードします。
 - e. CSR を CA に送信して認証を受けます。 CA から新しい証明書を取得します。

注意: CSR と秘密鍵ファイルは一致するセットであり、それに応じて処理する必要があります。署名された証明書が元の CSR の生成に使用された秘密鍵と一致しない場合、証明書は役に立ちません。これは、CSR ファイルと秘密鍵ファイルのアップロードとダウンロードに適用されます。

- CA から証明書を取得したら、このページに戻って Dominion KX IV-101 にアップロードします。アップロード後、[インストール]をクリックして、新しい証明書の使用を開始します。証明書が読み込まれると、ページが更新される場合があります。

New TLS Certificate

Subject	Key Parameters
Country: US	Key Length: 2048
State or Province: NJ	<p>Upload Certificate</p> <p>Browse... active_cert.pem</p> <p style="text-align: center;">Upload</p>
Locality: Somerset	
Organization: not set	
Organizational Unit: not set	
Common Name: raritan	
Email Address: not set	

Download Certificate Signing Request
Download Key
Delete Certificate Signing Request

▶ キーと証明書をアップロードする方法:

1. アップロードフィールドをアクティブにするには、[セキュリティ]> [TLS 証明書]をクリックし、[新しい TLS 証明書]セクションまで下にスクロールします。
2. [キーと証明書のアップロード] チェックボックスを選択。参照とアップロードのコントロールが表示されます。

Upload key and certificate

Key File... Please choose a file to upload

Certificate file... Please choose a file to upload

Upload

役務契約

役務契約ページでは、Dominion KX IV-101 のログインページに表示される契約を有効にすることができます。ユーザーは、ログインする前に契約のチェックボックスを選択する必要があります。

▶ 役務契約の構成方法:

1. [Security]> [Service Agreement] をクリック。

2. [Enforce restricted service agreement] チェックボックスを選択。
3. フィールドに契約テキストを入力し、[Save]をクリック。ログインページにサービス契約が表示されます。ユーザーは、ログインする前にチェックボックスを選択する必要があります。

チャプター8 メンテナンス

内容

バックアップと復元	160
イベントログ	161
ファームウェア履歴	163
ユニットのリセット	163
ファームウェアの更新	164

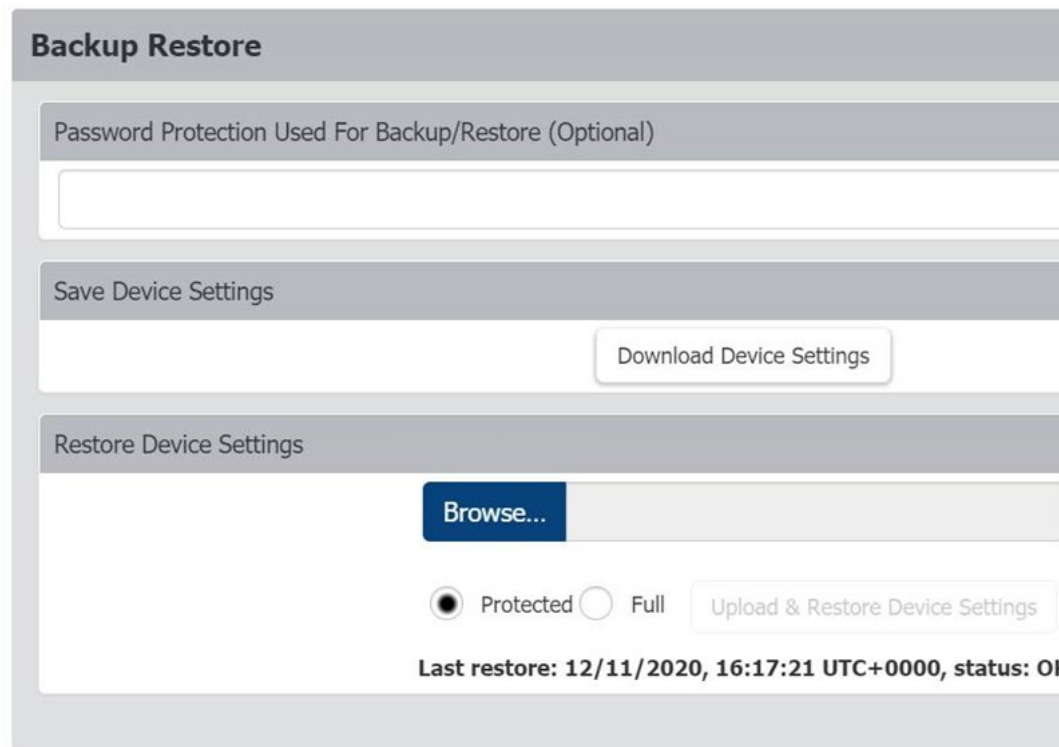
バックアップと復元

バックアップファイルをダウンロードし、バックアップファイルを使用して Dominion KX IV-101 を復元するには、admin グループのメンバーである必要があります。

パスワード保護を追加することにより、バックアップを暗号化できます。ファイルを使用して復元を実行する場合は、パスワードを入力する必要があります。


▶ デバイス設定のバックアップファイルをダウンロードする方法:

1. [Maintenance]> [Backup/Restore] をクリック。
2. バックアップファイルをパスワードで保護するには、[Password Protection Used For Backup/Restore (Optional)] フィールドにパスワードを入力。
3. [Download Device Settings] をクリックして、backup_settings.rfp ファイルを自動的にダウンロードします。



4.

▶ バックアップファイルを使用して Dominion KX IV-101 を復元する方法:

1. [Maintenance]> [Backup/Restore] ををクリック。
2. クリック  してバックアップファイルを選択。
3. [保護]または[フル]を選択します。
 - 保護: デバイス固有の設定 (ネットワーク情報、名前、優先解像度) を除く、すべての設定を復元。
 - フル: 全てを復元します。
4. ファイルがパスワードで保護されている場合、[バックアップ/復元に使用されるパスワード保護 (オプション)] フィールドにパスワードを入力します。
5. [Upload & Restore Device Settings] をクリックして、ファイルをアップロード。
6. Dominion KX IV-101 がリセットされ、ログインページが再表示され、復元が完了したことを示すまで待ちます。注意: 完全復元では、IP アドレスが変更されている可能性があります。新しい IP アドレスにログインするには、新しいブラウザセッションを開始する必要があります。

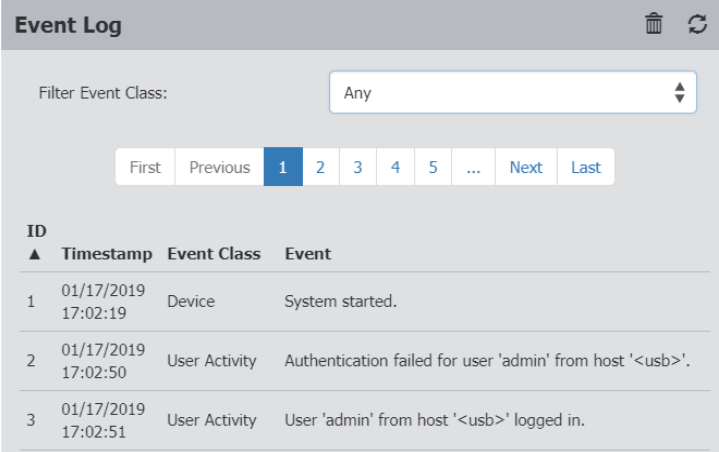
イベントログ

Dominion KX IV-101 は、特定のシステムイベントをキャプチャし、それらをローカルイベントログに保存します。

Dominion KX IV-101 で発生した 2000 を超える履歴イベントは、ローカルイベントログで確認できます。ログサイズが 256KB を超えると、新しいエントリごとに最も古いエントリが上書きされます。

▶ イベントクラス:

- デバイス
- KVM ポート
- ユーザーアクティビティ
- ユーザー管理
- シリアルポート





The screenshot shows the 'Event Log' interface. At the top, there is a 'Filter Event Class' dropdown menu set to 'Any'. Below it is a pagination bar with buttons for 'First', 'Previous', '1', '2', '3', '4', '5', '...', 'Next', and 'Last'. The main content is a table with the following data:

ID	Timestamp	Event Class	Event
1	01/17/2019 17:02:19	Device	System started.
2	01/17/2019 17:02:50	User Activity	Authentication failed for user 'admin' from host '<usb>'.
3	01/17/2019 17:02:51	User Activity	User 'admin' from host '<usb>' logged in.

▶ イベントログの表示方法:

- [Maintenance]> [Event Log] を選択。
各イベントエントリは、下記のもので構成されます：
 - イベントの ID 番号
 - イベントのタイムスタンプ：イベントログのタイムスタンプは、コンピューターのタイムゾーンに自動的に変換されます。時間の混乱を避ける為に、Dominion KX IV-101 タイムゾーン設定を、コンピュータかモバイルデバイスに適用して下さい。
 - イベントクラス
 - イベントの説明

- 右上隅の更新アイコン  をクリックして、イベントログを更新します。
- ▶ イベントカテゴリ別に表示する方法:
 - [イベントクラスのフィルター] フィールドでオプションを選択します。
- ▶ ローカルイベントログのクリア方法:
 1. 右上隅にあるゴミ箱アイコン  をクリック。
 2. 確認メッセージの[Clear Log]をクリック。

ファームウェア履歴

ファームウェアのアップグレード履歴は、デバイスの再起動またはファームウェアのアップグレード後も保持されます。工場出荷時の初期リセットが発生すると、履歴はクリアされます。

- ▶ ファームウェア更新履歴の表示方法:
 - [Maintenance]> [Firmware History] を選択。
 各ファームウェアアップデートイベントは、次のもので構成されます:
 - 日時の更新
 - 以前のファームウェアバージョン
 - ファームウェアバージョンの更新
 - 結果の更新

Firmware Update History			
Timestamp ▼	Previous Version	Update Version	Status
03/18/2019 10:05:06	4.0.0.1.45554	4.0.0.5.45611	SUCCESSFUL
03/01/2019 11:17:40	4.0.0.1.45375	4.0.0.1.45554	SUCCESSFUL

ユニットのリセット

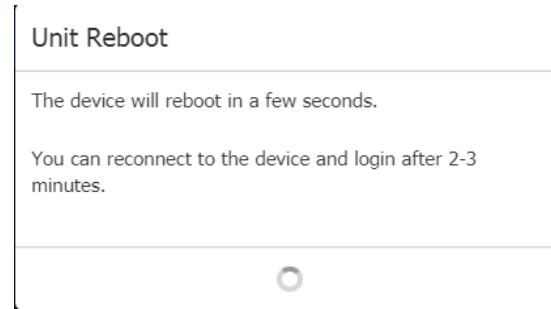
ユニットリセットセクションには、リモートで再起動するか、工場出荷時の初期にリセットするオプションがあります。

- ユニットの再起動: Dominion KX IV-101 を再起動します。
- 工場出荷時の初期にリセット: カスタマイズされた設定をすべて削除し、Dominion KX IV-101 を工場出荷時のデフォルト設定に戻します。管理者権限が必要です。

Unit Reset	
<input type="button" value="Reboot Unit"/>	<input type="button" value="Reset to Factory Defaults"/>

▶ **デバイスの再起動方法:**

1. [Maintenance]> [Unit Reset] を選択。
2. [Reboot Unit] をクリック。
3. 確認メッセージが表示されます。 [Reboot]をクリックして続行します。
カウントダウンタイマーが表示されます。



4. 再起動が完了すると、ログインページが開きます。

▶ **工場出荷時の初期状態へのリセット方法:**

1. [Maintenance]> [Unit Reset] をクリック。
2. [Reset to Factory Defaults] をクリックします。確認メッセージでクリックして、リセットを確認します。
3. カウントダウンタイマーが表示されます。完了するまでに約2分かかります。
4. リセットが完了したら、初期構成に進みます。「初期構成『p. 5』」をご参照下さい。

▶ **その他工場出荷時へのリセットのオプション:**

- Dominion KX IV-101 デバイスのリセットボタンを使用します。リセットボタンを5秒間押しします。デバイスがリセットされ、再起動します。
- CLI コマンドを実行します。CLI: リセット『p. 195』をご参照ください。

ファームウェアの更新

ファームウェアファイルは、Raritan のサポートページ (www.raritan.com/support) で入手できます。

Dominion KX IV-101 ファームウェアを更新するには、メンテナンス権限が必要です。

▶ **ファームウェアアップデートの方法:**

1. [Maintenance]> [Update Firmware] をクリック。

2. [Browse]をクリックして適切なファームウェアファイルを選択し、[Upload]をクリックします。アップロードプロセスを示すプログレスバーが表示されます。

Update Firmware

Browse...

The firmware update is being prepared.

This may take up to a minute. On successful completion the firmware update will be started.

Please wait ...

3. 完了すると、インストールされたファームウェアバージョンとアップロードされたファームウェアバージョンの両方の情報、互換性、署名チェックの結果が表示されます。

Update Firmware

A new firmware has been uploaded to your device.

Version

Installed Version	4.0.0.5.45611
New Version	4.0.0.5.45611

Compatibility

✔ The uploaded firmware file is compatible with this device.

Signature

✔ The signature of the uploaded firmware file is valid.

- キャンセルするには、[Discard Upload]をクリック。
- アップデートを続行するには、[Update Firmware]をクリック。

- 更新が開始されると、別のプログレスバーが表示されます。警告：更新中は、Dominion KX IV-101 の電源を切らないでください。更新中は、デバイスの LAN ポート LED が緑色に速く点滅します。

The firmware update is in progress

This may take some minutes. Please do not power off the device while the update is in progress! After a successful update, the device will reboot automatically.

14%

注意：アップデート中は、ユーザーは正常にログインできません。ログインしたユーザーは、操作を一時停止する必要があります。

- アップデートが完了すると、Dominion KX IV-101 が再起動し、ログインページが再表示されます。アップデートと再起動のプロセスには約 5 分かかります。更新後にデバイスに「ロード中」画面が表示され、長時間再起動した場合、ブラウザを安全に再起動し、Dominion KX IV-101 に再度ログインして、アップデート結果を確認できます。

アップデート後：Dominion KX IV-101 MIB が変更された可能性があります。SNMP マネージャーを使用している場合、MIB を再ダウンロードして更新する必要がある場合があります。「SNMP 設定 [p. 142]」をご参照ください。

▶ ファームウェアの更新は警告付きで完了しました：

iOS デバイスが Dominion KX IV-101 の USB ポートに接続されている時にアップデートを完了した場合、再起動する前に「ファームウェアのアップデートが警告付きで完了しました」というメッセージが表示されることがあります。この警告は、問題が発生した事や、更新が失敗した事を示すものではありません。

The firmware update completed with warnings

The device will now reboot. Please wait for five minutes, then follow this link to the login page to log in. If the device does not work correctly after the update, please contact Raritan support.

74%

CHAPTER 9 仮想メディア

内容

概要.....	167
仮想メディアのパフォーマンスに関する推奨事項.....	167
仮想メディアを使用するための前提条件.....	168
ローカルドライブの取り付け.....	168
仮想メディアを介してサポートされるタスク.....	169
サポートされている仮想メディアタイプ.....	169
サポートされている仮想メディアドライブ数.....	170
Linux 環境での仮想メディア.....	170
Mac 環境での仮想メディア.....	171
仮想メディアファイルサーバーのセットアップ (ファイルサーバーISO イメージのみ).....	172

概要

全ての Dominion KX IV-101 モデルは、仮想メディアをサポートしています。仮想メディアは、ターゲットサーバーがクライアント PC 及びネットワークファイルサーバーから、メディアにリモートアクセスできるようにする事で、KVM 機能を拡張します。

この機能により、クライアント PC とネットワークファイルサーバーにマウントされたメディアは、基本的にターゲットサーバーによって「仮想的にマウント」されます。ターゲットサーバーは、ターゲットサーバー自体に物理的に接続されているかの様に、そのメディアからの読み取りとメディアへの書き込みを行うことが可能。

各 Dominion KX IV-101 には、様々な CD、DVD、USB、オーディオデバイス、内蔵、リモートドライブ、及びイメージを使用したリモート管理タスクを可能にする仮想メディアが装備されています。

仮想メディアセッションは、ブラウザが提供する最も強力な暗号化(通常は 256 ビット AES)を使用して保護されます。古いブラウザは 128 ビット AES しかサポートしていない可能性があります。

HKC は全ての仮想メディア機能をサポートしているわけではありません。詳細については、HTML KVM クライアント (HKC) を参照してください。

仮想メディアのパフォーマンスに関する推奨事項

仮想メディアのパフォーマンスに関する追加の調査によると、KX4-101 の仮想メディアのパフォーマンスは最大 175Mbps の範囲である可能性があります。これは、KX3 スイッチ (8~10 Mbps) よりも、大幅に高速です。

▶ 最大パフォーマンスを引き出す方法:

- 暗号化をオフにします。暗号化はパフォーマンスに大きな影響を及ぼします。
- AKC や VKC の KVM クライアントで高速ラップトップ/ PC を利用します。
- KX IV ユーザーステーション (DKX4-UST) を利用します。
- KVM クライアントに接続された仮想メディアドライブへの書き込みは、ドライブからの読み取りよりも遅い場合があります。
- USB ドライブによってパフォーマンスが異なる場合があります。
- ネットワークパフォーマンスも要因です。

メディアを使用するための前提条件

Dominion KX IV-101 仮想メディアの前提条件

- 仮想メディアへのアクセスが必要なユーザーの場合、関連するポートへのアクセスと、ポートの仮想メディアアクセス (VM アクセスポートのアクセス許可) を許可するように Dominion KX IV-101 アクセス許可を設定する必要があります。ポートのアクセス許可はグループレベルで設定されます。
- **PC-Share を使用する場合、[セキュリティ設定] ページでも[セキュリティ設定] を有効にする必要があります。オプション**
- デバイスとターゲットサーバーの間に、USB 接続が存在する必要があります。
- 接続する KVM ターゲットサーバーの正しい USB 接続設定を選択する必要があります。

クライアント PC VM の前提条件

- 特定の仮想メディアオプションには、PC の管理者権限が必要です (例: 完全なドライブのドライブリダイレクト)。

注意: Windows を使用している場合、Internet Explorer の起動時に、ユーザーアカウント制御を無効にするか、[管理者として実行]を選択します。これを行うには、[スタート]メニューをクリックし、IE を見つけて右クリックし、[管理者として実行]を選択。

ターゲットサーバーVM の前提条件

- KVM ターゲットサーバーは、USB 接続ドライブをサポートする必要があります。

ローカルドライブの取り付け

このオプションは、ドライブ全体をマウントします。つまり、ディスクドライブ全体が仮想的にターゲットサーバーにマウントされます。

このオプションは、ハードドライブと外付け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、または DVD-ROM ドライブは含まれません。

仮想メディアを介してサポートされるタスク

- 仮想メディアは、下記のようなタスクをリモートで実行する機能を提供します。
- 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、またはパッチ適用
- オペレーティングシステムの完全なインストール

重要:仮想メディアドライブに接続した後、ファイル転送、アップグレード、インストール、またはその他の同様のアクションを実行している場合、KVMクライアントでマウスモードを変更しないでください。これを行うと、仮想メディアドライブでエラーが発生したり、仮想メディアドライブにエラーが発生したりする可能性があります。

サポートされている仮想メディアタイプ

- AKC および VKC / VKCS を使用する場合、Windows®、Mac®、Linux™クライアントで下記仮想メディアタイプがサポートされます。
- 内蔵/外付けハードドライブ
- 内蔵/USB マウントの CD/DVD ドライブ
- USB 大容量ストレージデバイス
- PC ハードドライブ
- ISO イメージ (ディスクイメージ)
- IMG ファイル
- DMG ファイル
- ISO9660 がサポートされている標準です。ただし、他の ISO 規格を使用することもできます。

注意：ブラウザの制限により、HKC は異なる仮想メディアタイプのセットをサポートしません。

読み取り/書き込みが利用できない場合の条件

仮想メディアの読み取り/書き込みは、下記の状況では使用できません：

- Linux 及び Mac クライアントの場合
- ドライブが書き込み保護されている場合
- ユーザーに読み取り/書き込み権限がない場合：
 - ポートアクセス許可が None または View に設定されている
 - ポートアクセス許可 VM アクセスが、読み取り専用または拒否に設定されている

サポートされている仮想メディアドライブ数

仮想メディア機能を使用すると、現在ターゲットに適用されている USB 接続設定でサポートされている（異なるタイプの）最大 2 つのドライブをマウントできます。これらのドライブは、KVM セッションの間アクセスできます。

例えば、特定の CD-ROM をマウントして使用し、完了したら切断することができます。ただし、CD-ROM 仮想メディアの「チャンネル」は開いたままなので、別の CD-ROM を仮想的にマウントできます。これらの仮想メディアの「チャンネル」は、USB 設定でサポートされている限り、KVM セッションが閉じられるまで、開いたままになります。

仮想メディアを使用するには、ターゲットサーバーからアクセスするクライアント、またはネットワークファイルサーバーにメディアを接続/接続します。

これは最初のステップである必要はありませんが、このメディアにアクセス前に実行する必要があります。

Linux 環境での仮想メディア

アクティブなシステムパーティション

Linux クライアントから、アクティブなシステムパーティションをマウントは不可。

Linux Ext3 / 4 ドライブパーティションは、仮想メディア接続を確立前に、umount / dev / <デバイスラベル>を介して、アンマウントする必要があります。

マップされたドライブ

Linux クライアントからマップされたドライブは、接続されたターゲットにマウントされた時にロックされません。

ドライブパーティション

- オペレーティングシステム間で、次のドライブパーティションの制限があります。
- Windows および Mac ターゲットは、Linux 形式のパーティションを読み取ることが出来ません。
- Windows と Linux は、Mac でフォーマットされたパーティションを読み取ることが出来ません。
- Linux では Windows Fat パーティションのみがサポートされています

ルートユーザーのアクセス許可の要件

Linux クライアントからターゲットに CDROM をマウントしてから、CD ROM をアンマウントすると、仮想メディア接続が閉じられます。

これらの問題を回避するには、root ユーザーである必要があります

ドライブのアクセス許可の接続 (Linux)

Linux ユーザーは、ターゲットに接続するリムーバブルデバイスに対する読み取り専用のアクセス許可を持っている必要があります。 / dev / sdb1 の場合、root ユーザーとして以下を実行：

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

これで、ドライブをターゲットに接続できるようになります。

Mac 環境での仮想メディア

アクティブシステムパーティション

仮想メディアを使用して、Mac クライアントのアクティブなシステムパーティションをマウントすることは出来ません。

ドライブパーティション

OS 間で、下記のドライブパーティションの制限があります：

- Windows と Mac ターゲットは、Linux 形式のパーティションを読み取る事ができません。
- Windows は Mac でフォーマットされた、パーティションを読み取る事ができません。
- Windows FAT 及び NTFS は Mac でサポートされています。
- Mac ユーザーは、ターゲットサーバーに接続する為に、既にマウントされているデバイスを全てアンマウントする必要があります。 > diskutil umount / dev / disk1s1 を使用してデバイスをアンマウントし、diskutil mount / dev / disk1s1 を使用して、デバイスを再マウントします。

ドライブのアクセス許可を接続する (Mac)

デバイスを Mac クライアントからターゲットに接続できるようにするには、リムーバブルデバイスへの読み取り専用のアクセス許可が必要です。また、その後にドライブをアンマウントする必要があります。

/ dev / sdb1 の場合、root ユーザーとして下記コマンドを実行します：

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
root@administrator-desktop:~# diskutil umount /dev/sdb1
```

仮想メディアファイルサーバーのセットアップ (ファイルサーバーISO イメージのみ)

この機能は、仮想メディアを使用してファイルサーバーの ISO イメージにアクセスする場合にのみ必要です。ISO9660 フォーマットがサポートされている標準です。ただし、他の CD-ROM 拡張機能も機能する場合があります。

注意：ファイルサーバーでは、SMB / CIFS のサポートが必要です。

仮想メディア共有イメージのセットアップページを使用して、仮想メディアを使用してアクセスするファイルサーバーとイメージパスを指定します。ここで指定したファイルサーバーISO イメージは、[仮想メディア CD / ISO イメージのマップ]ダイアログの[リモートサーバーISO イメージのホスト名] と [イメージ]ドロップダウンリストで選択できます。「CD-ROM / DVD-ROM / ISO イメージのマウント 『p. 65』」をご参照ください。

▶ 仮想メディアアクセス用のファイルサーバーISO イメージの指定方法:

1. リモートコンソールから[デバイス設定] / [仮想メディア共有イメージ]を選択します。仮想メディア共有イメージのセットアップページが開きます。
2. [新規]をクリックして、[共有イメージの追加] ページを開きます
3. アクセスするファイルサーバーの ISO イメージに関する情報を入力します。
 - IP アドレス/ホスト名
 - 共有名
 - 画像パス
 - 必要に応じて、[SMBv1.0 を有効にする]を選択
4. [共有イメージの追加] をクリック。
ここで指定した全てのメディアは、[仮想メディア CD / ISO イメージのマップ] ダイアログで選択できるようになりました。

チャプター10 診断

内容

診断のダウンロード	173
ネットワーク診断	173

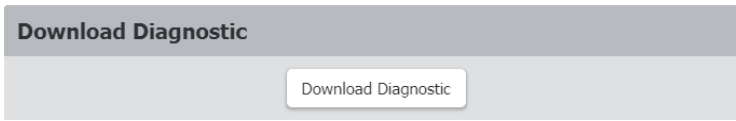
診断のダウンロード

重要:この機能は、Raritanフィールドエンジニアが使用する場合、またはRaritanテクニカルサポートから指示された場合に使用します。

Dominion KX IV-101 からクライアントマシンに、診断ファイルをダウンロードできます。ファイルは.zip ファイルに圧縮されており、Raritan テクニカルサポートに送信する必要があります。

admin グループのメンバーである必要があります。

▶ 診断ファイルのダウンロード方法:



1. [Diagnostics]> [Download Diagnostic] をクリック。
2. [Download Diagnostic] をクリックして、ファイルを保存します。
3. Raritan テクニカルサポートの指示に従って、このファイルを送信します。

エラー! 指定したスタイルは使われていません。: エラー! [ホーム] タブを使用して、ここに表示する文字列に **Heading 1** を適用してください。

ネットワーク診断

Dominion KX IV-101 は、潜在的なネットワークの問題を診断する下記ツールを提供します。

Ping

- Trace Route : 2 つのホストまたはシステム間のネットワーク上のルートを見つけます。
- TCP 接続のリスト : TCP 接続のリストを表示します。

[Diagnostics]> [Network Diagnostics] を選択し、以下の機能を実行します。

▶ Ping:

[ネットワークホスト]フィールドに IP またはホスト名を入力し、送信する要求の数を設定します。最大は 20 です。これにより、ホストに ping を送信するために送信されるパケット数が決まります。[Run] をクリックして、ホストに ping を実行します。

次に、Ping 結果が表示されます。

Ping Results

```
PING 192.168.56.27 (192.168.56.27): 56 data bytes
64 bytes from 192.168.56.27: seq=0 ttl=64 time=0.219 ms
64 bytes from 192.168.56.27: seq=1 ttl=64 time=0.183 ms
64 bytes from 192.168.56.27: seq=2 ttl=64 time=0.179 ms
64 bytes from 192.168.56.27: seq=3 ttl=64 time=0.196 ms
64 bytes from 192.168.56.27: seq=4 ttl=64 time=0.171 ms
--- 192.168.56.27 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.171/0.189/0.219 ms
```

Close

▶ Trace Route:

1. 次のフィールドに値を入力します。

フィールド/設定	内容
ホスト名	ルートを確認するホストの IP アドレスまたは名前。
タイムアウト	トレーズルート操作を終了する為の秒単位のタイムアウト値。最大 900 秒。
ICMP パケットの使用	インターネット制御メッセージプロトコル (ICMP) パケットを使用して、trace route コマンドを実行するには、このチェックボックスを選択。

2. [Run] をクリックします。Trace Route の結果が表示されます。

▶ TCP 接続のリスト:

1. [List TCP Connections] タイトルバーをクリックして、アクティブな接続のリストを表示。

List TCP Connections ^						
Active Internet connections (w/o servers)						
#	Proto	Recv- Q	Send- Q	Local Address	Foreign Address	State
1	tcp	0	0	::ffff:192.168.56.27: 443	::ffff:192.168.55.78:62 654	TIME_WAIT
2	tcp	0	0	::ffff:192.168.56.27: 443	::ffff:192.168.55.78:62 644	TIME_WAIT

チャプター11 CLI コマンド

Dominion KX IV-101 は、CLI で下記カテゴリのコマンドをサポートします。

check	サービスの確認
clear	ログのクリア
config	構成ビューに入る
connect	ターゲットへ接続
diag	診断ビューに入る
exit	セッションを終了
reset	デバイスをリセット
show	様々なデバイス情報を表示

内容

CLI: check	176
CLI: clear	176
CLI: config	176
CLI: connect	191
CLI: diag	192
CLI: reset	193
CLI: show	194
CLI: exit	200

CLI: check

```
check
# check ntp
```

CLI: clear

```
clear
# clear eventlog
Do you really want to clear the event log? [y/n]
```


CLI: config

```
config
# config
config:#
```

▶ 使用可能なコマンド:

apply	変更した設定を保存し、構成モードを終了
authentication	認証の設定
cancel	変更した設定を破棄し、構成モードを終了
check	サービスを確認
device	デバイスの構成
group	ユーザーグループの構成
keyword	DSAM シリアルポートのキーワードを設定
network	ネットワークの設定
password	現在ログインしているユーザーのパスワードを変更
port	DSAM シリアルポートの設定
security	セキュリティの設定
serial	シリアルポートの設定
terminalblock	端子台の設定
time	日付/時刻設定
user	ユーザーの設定

CLI: config authentication

authentication

config # authentication

使用可能なコマンド:

- ldap LDAP サーバー設定の構成
- radius RADIUS サーバー設定の構成
- type 認証タイプの構成 (local/ldap/radius)

▶ LDAP:

add 新しい LDAP サーバーを追加

addClone 新しい LDAP サーバーを追加し、別のサーバーのクローンを作成

delete LDAP サーバーを削除

modify 既存の LDAP サーバーを変更

- config # authentication ldap add

```
authentication ldap add <host> <port> <security> <bindtype> <basedn>
<loginnameattr> <userentryclass> [userSearchSubfilter <usersearchfilter>]
[adDomain <addomain>] [verifyServerCertificate <certverify>]
[allowExpiredCertificate <allowexpiredcert>] [bindDN <binddn>]
```

新しい LDAP サーバーを追加

host	IP アドレス/ホスト名
port	ポート番号 (0..4294967295)
type	LDAP サーバータイプ (openldap/activeDirectory)
security	セキュリティタイプ (none/startTls/tls)
bindtype	バインドタイプ (anonymousBind/authenticatedBind)
basedn	検索用のベース DN
loginnameattr	ログイン名属性
userentryclass	ユーザーエントリ オブジェクト・クラス
userSearchSubfilter	ユーザー検索サブフィルター
adDomain	Active Directory ドメイン
verifyServerCertificate	LDAP サーバー証明書の検証を有効にする (true/false)
allowExpiredCertificate	期限切れでまだ有効ではないサーバー証明書を許可する (true/false)
bindDN	バインド DN

- config # authentication ldap addClone

```
authentication ldap addClone <index> <host>
```

新しい LDAP サーバーを追加し、別のサーバーのクローンを作成

index ソースサーバー・インデックス

host IP アドレス/ホスト名

- config # authentication ldap delete

```
authentication ldap delete <index>
```

Delete LDAP server

index Server index

- config # authentication ldap modify

```
authentication ldap modify <index> [host <host>] [port <port>] [serverType ]
[securityType <security>] [bindType <bindtype>] [searchBaseDN <basedn>]
[loginNameAttribute <loginnameattr>] [userEntryObjectClass <userentryclass>]
[userSearchSubfilter <usersearchfilter>] [adDomain <addomain>]
[verifyServerCertificate <certverify>] [certificate] [allowExpiredCertificate
<allowexpiredcert>] [bindDN <binddn>] [bindPassword] [sortPosition <position>]
```

既存の LDAP サーバーを変更

index	インデックス
host	IP アドレス/ホスト名
port	ポート番号 (0..4294967295)
serverType	LDAP サーバータイプ (openldap/activeDirectory)
securityType	セキュリティタイプ (none/startTls/tls)
bindType	バインドタイプ (anonymousBind/authenticatedBind)
searchBaseDN	検索用のベース DN
loginNameAttribute	ログイン名属性
userEntryObjectClass	ユーザーエントリ オブジェクト・クラス
userSearchSubfilter	ユーザー検索サブフィルター
adDomain	Active directory ドメイン
verifyServerCertificate	LDAP サーバー証明書の検証を有効にする
(true/false)	
certificate	証明書 CA チェーン
allowExpiredCertificate	期限切れでまだ有効ではないサーバー証明書を許可する
(true/false)	
bindDN	バインド DN
bindPassword	バインド・パスワード
sortPosition	サーバーリストの新しいポジション

▶ RADIUS:

- config # authentication radius

使用可能コマンド:

- 追加

新しい Radius サーバーの追加

host	IP アドレス/ホスト名
type	認証タイプ (pap/chap/msChapV2)
authport	認証ポート番号 (0..4294967295)
acctport	アカウントポート番号 (0..4294967295)
timeout	タイムアウト (1..60)
retries	再試行回数 (0..5)

- 削除

Radius サーバーの削除

index	サーバー・インデックス
-------	-------------

- 変更

新しいRadius サーバーの変更

```
config:# authentication radius modify
```

```
authentication radius modify <index> [host <host>] [authType ] [authPort
<authport>] [accountPort <acctport>] [timeout <timeout>] [retries <retries>]
[secret] [sortPosition <position>]
```

index	インデックス
host	IP アドレス/ホスト名
authType	認証タイプ (pap/chap/msChapV2)
authPort	認証ポート番号 (0..4294967295)
accountPort	アカウントポート番号 (0..4294967295)
timeout	タイムアウト (1..60)
retries	再試行回数 (0..5)
secret	共有秘密
sortPosition	サーバーリストの新しいポジション

▶ タイプ:

- config # authentication type

```
authentication type [useLocalIfRemoteUnavailable <localfallback>]
```

認証タイプを構成

type	認証タイプ (local/ldap/radius)
useLocalIfRemoteUnavailable	リモート認証が利用できない場合、ローカル認証を使用 (true/false)

CLI: config device

device

config:# device name

device [name <name>]

デバイスの構成

name Device name

(例) デバイスに「KX4newname」という名前を付けるには、設定メニューで「device name KX4newname」と入力し、「apply」と入力して保存。

CLI: config group

グループ

```
config:# group create
```

```
group create [name <name>] [privileges <privs>]
```

新しいグループの作成

name Group name

privileges Group privileges (one or more (separated by '/') of
changeTerminalBlockSettings/deviceAccessUnderCcsG/deviceSettings/maintenance/pcS
hare/portControl:1/portControl:all/portViewOnly:1/portViewOnly:all/portVmROnly:1
/portVmROnly:all/portVmRW:1/portVmRW:all/securitySettings/userManagement)

```
config:# group delete [name <name>]
```

グループを削除

name Group name (Admin)

```
config:# group modify [name <name>] [description <desc>] [addPrivileges  
<addprivs>] [removePrivileges <removeprivs>]
```

グループの編集

name グループ名 (アドミン)

description グループの説明

addPrivileges Add group privileges (one or more (separated by '/') of
changeTerminalBlockSettings/deviceAccessUnderCcsG/deviceSettings/maintenance/pcS
hare/portControl:1/portControl:all/portViewOnly:1/portViewOnly:all/portVmROnly:1
/portVmROnly:all/portVmRW:1/portVmRW:all/securitySettings/userManagement)

removePrivileges Remove group privileges (one or more (separated by '/') of
changeTerminalBlockSettings/deviceAccessUnderCcsG/deviceSettings/maintenance/pcS
hare/portControl:1/portControl:all/portViewOnly:1/portViewOnly:all/portVmROnly:1
/portVmROnly:all/portVmRW:1/portVmRW:all/securitySettings/userManagement)

CLI: config keyword

キーワード

```
config:# keyword add
```

```
keyword add [key <key>] [port <port>]
```

キーワードの追加

```
keyword delete [key <key>]
```

キーワードの削除

```
keyword modify [key <key>] [port <port>]
```

キーワードを編集

CLI: config network

ネットワーク

```
config:# network dns [firstServer <server1>] [secondServer <server2>]
[searchSuffixes <searchSuffixes>] [resolverPreference <resolverPreference>]
```

Configure DNS settings

firstServer	最初の DNS サーバー
secondServer	2 番目の DNS サーバー
searchSuffixes	接尾辞を検索
resolverPreference	DNS リゾルバー設定 (preferV4 / preferV6)

```
config:# network ethernet [speed <speed>] [duplexMode <duplexMode>]
```

イーサネット・インターフェイス設定

speed	スピード (1000Mbps/100Mbps/10Mbps/オート)
duplexMode	デュプレックスモード (ハーフ/フル/オート)

```
config:# network ipv4 gateway
```

```
network ipv4 gateway <gateway>
```

デフォルトの IPv4 ゲートウェイを構成

gateway	Default IPv4 gateway
---------	----------------------

```
config:# network ipv4 interface [enabled <enabled>] [configMethod <configMethod>]
[preferredHostName <prefHostname>] [address <addrCidr>]
```

Configure interface IPv4 設定

enabled	IPv4 プロトコルを有効/無効にする (true/false)
configMethod	IPv4 構成方法 (dhcp/static)
preferredHostName	優先ホスト名
address	IPv4 アドレス/プレフィックス長

```
config:# network ipv6 gateway
```

```
network ipv6 gateway <gateway>
```

デフォルトの IPv6 ゲートウェイを構成

gateway	Default IPv6 gateway
---------	----------------------

```
config:# network ipv6 interface [enabled <enabled>] [configMethod <configMethod>]
[preferredHostName <prefHostname>] [address <addrCidr>]
```

インターフェイスの IPv6 設定

enabled	IPv6 プロトコルを有効/無効にする (true/false)
configMethod	IPv6 の構成方法 (automatic/static)
preferredHostName	優先ホスト名
address	IPv6 アドレス/プレフィックス長


```

config:# network services discovery
network services discovery [port <port>]
検出ポートを構成
port    RDM 検出ポート (1..65535)

config:# network services http [enabled <enabled>] [port <port>] [enforceHttps
<enforcehttps>]
HTTP アクセスを構成

enabled    HTTP アクセスを有効/無効にします (true/false)
port      HTTP アクセス TCP ポート (1..65535)
enforceHttps  Web アクセスの HTTPS エンフォースメントを有効にする (true/false)

config:# network services https [enabled <enabled>] [port <port>]
HTTPS アクセスを構成する
enabled    HTTPS アクセスを有効/無効にする (true/false)
port      HTTPS アクセス TCP ポート (1..65535)

config:# network services snmp [v1/v2c <v12enabled>] [v3 <v3enabled>]
[readCommunity <readcommunity>] [writeCommunity <writecommunity>] [sysContact
<syscontact>] [sysName <sysname>] [sysLocation <syslocation>]
SNMP 設定を構成
v1/v2c    SNMP v1 / v2c アクセスを有効 (有効化/無効化)
v3        SNMPv3 アクセスを有効 (有効化/無効化)
readCommunity  SNMP 読み取りコミュニティ文字列
writeCommunity  SNMP コミュニティ文字列を書く
sysContact    MIB-II sysContact
sysName       MIB-II sysName
sysLocation   MIB-II sysLocation

config:# network services ssh [enabled <enabled>] [port <port>] [authentication
<authmode>]
SSH アクセスを構成
enabled    SSH アクセスを有効/無効にする (true/false)
port      SSH アクセス TCP ポート (1..65535)
authentication    Authentication    type
(passwordOnly/publicKeyOnly/passwordOrPublicKey)

```

CLI: config password

```
config:# password
```

次に[Enter]を押します。システムは、現在のパスワードと新しいパスワードの入力を求め、新しいパスワードを確認します。

```
config:# apply
```

確認パスワードが正しければ、パスワードが変更されます。

CLI: config port

ポート: DSAM シリアルポート設定を構成

```
port [index <index>] [name <name>] [emulation <emulation>] [encoding <encoding>]
[eqtype <eqtype>] [bps <bps>] [parity <parity>] [flowcontrol <flowcontrol>]
[stopbits <stopbits>] [multiwrite <multiwrite>] [escapemode <escapemode>]
[escapechar <escapechar>] [chardelay <chardelay>] [linedelay <linedelay>]
[sendbreak <sendbreak>] [suppress <suppress>] [alwaysactive <alwaysactive>]
[exitcommand <exitcommand>]
```

CLI: config security

```
config:# security groupBasedAccessControl ipv4
security groupBasedAccessControl ipv4 [enabled <enable>] [defaultPolicy
<defpolicy>]
```

IPv4 のグループベースのアクセス制御設定を構成

enabled グループベースのアクセス制御を有効にする (true/false)
 defaultPolicy 初期のポリシー (許可/拒否)

```
config:# security groupBasedAccessControl ipv6 [enabled <enable>] [defaultPolicy
<defpolicy>]
```

IPv6 IPv6 のグループベースのアクセス制御設定を構成します

enabled グループベースのアクセス制御を有効にする (true/false)
 defaultPolicy 初期のポリシー (許可/拒否)

```
config:# security ipAccessControl ipv4
```

```
security ipAccessControl ipv4 [enabled <enable>] [defaultPolicyIn <defpolicyin>]
[defaultPolicyOut <defpolicyout>]
```

IPv4 アクセス制御設定を構成する

enabled アクセス制御を有効にする (true/false)
 defaultPolicyIn インバウンドトラフィックのデフォルトポリシー
 (accept/drop/reject)
 defaultPolicyOut アウトバウンドトラフィックのデフォルトポリシー
 (accept/drop/reject)

```
config:# security ipAccessControl ipv6 [enabled <enable>] [defaultPolicyIn
<defpolicyin>] [defaultPolicyOut <defpolicyout>]
```

IPv6 アクセス制御設定を構成する

enabled IP アクセス制御を有効にする (true/false)
 defaultPolicyIn インバウンドトラフィックのデフォルトポリシー
 (accept/drop/reject)
 defaultPolicyOut アウトバウンドトラフィックのデフォルトポリシー
 (accept/drop/reject)

```
config:# security loginLimits [singleLogin <singlelogin>] [passwordAging
<pwaging>] [passwordAgingInterval <pwaginginterval>] [idleTimeout <idletimeout>]
```

ログイン制限を構成

singleLogin 同時ユーザーログインを防止 (有効化/無効化)
 passwordAging パスワードのエージングを有効にする (有効化/無効化)
 passwordAgingInterval パスワードのエージング間隔を設定 (日数) (7..365)
 idleTimeout ユーザーのアイドルタイムアウトを設定 (分数) (1..1440 か
 無限)

```
config:# security restrictedServiceAgreement [enabled <enabled>] [bannerContent]
```

制限付きサービス契約バナーを構成

enabled 制限付きサービス契約の実行を有効にする (true/false)
 bannerContent 制限付きサービス契約バナー

```
config:# security strongPasswords [enabled <enable>] [minimumLength <minlength>]
[maximumLength <maxlength>] [enforceAtLeastOneLowerCaseCharacter <forcelower>]
[enforceAtLeastOneUpperCaseCharacter <forceupper>]
[enforceAtLeastOneNumericCharacter <forcenumeric>]
[enforceAtLeastOneSpecialCharacter <forcespecial>] [passwordHistoryDepth
<historydepth>]
```

強力なパスワード要件を構成

enabled 強力なパスワードを有効にする (true/false)
 minimumLength パスワードの最小長 (8..32)
 maximumLength パスワードの最大長 (16..64)
 enforceAtLeastOneLowerCaseCharacter 少なくとも1つの小文字を使用
 (有効化/無効化)
 enforceAtLeastOneUpperCaseCharacter 少なくとも1つの大文字を強制
 (有効化/無効化)
 enforceAtLeastOneNumericCharacter 少なくとも1つの数字を強制
 (有効化/無効化)
 enforceAtLeastOneSpecialCharacter 少なくとも1つの特殊文字を適用
 (有効化/無効化)
 passwordHistoryDepth パスワードの履歴数 (1..12)

```
config:# security userBlocking [maximumNumberOfFailedLogins <maxfails>] [blockTime
<blocktime>]
```

ユーザーブロッキングを構成

maximumNumberOfFailedLogins ユーザーをブロックする前にログイン失敗の最大数を設定
 (3..10 か 無制限)
 blockTime ユーザーのブロック時間を設定 (分数) (1..1440 か無限)

CLI: config serial

```
config:# serial [consoleBaudRate <consolebps>] [modemBaudRate <modembps>]
[deviceDetectionType <detecttype>]
```

シリアルポート設定を構成

```
consoleBaudRate    シリアルコンソールのボーレート
(1200/2400/4800/9600/19200/38400/57600/115200)

modemBaudRate      モデムのボーレート
(1200/2400/4800/9600/19200/38400/57600/115200)

deviceDetectionType デバイス検出モード
(automatic/forceConsole/forceAnalogModem/forceGsmModem)
```

CLI: config terminalblock

```
config:# terminalblock [inputEnable <inputEnable>] [inputRemote <inputRemote>]
[inputLocal <inputLocal>] [outputEnable <outputEnable>] [outputAction
<outputAction>] [blinkInterval <blinkInterval>]
```

端子台設定を構成

```
inputEnable    スイッチの有効化/無効化 (enable/disable)
inputRemote    入力リモートコンソールのセットアップ
(fullAccess/videoOnly/noAccess)
inputLocal     入力ローカルコンソールのセットアップ
(fullAccess/videoOnly/noAccess)
outputEnable   出力デバイスの有効化/無効化 (enable/disable)
outputAction   アクションの設定 (deviceOff/deviceOn/blinkDevice)
blinkInterval  セットアップデバイスの点滅間隔 (0.5 秒で) (1..10)
```

CLI: config time

```
config:# time [method <method>] [zone] [autoDST <autodst>]
```

日付/時刻設定を構成

```
method    時間設定方法 (manual/ntp)
zone      タイムゾーンを選択
autoDST   自動夏時間の調整 (enable/disable)
```

CLI: config user

```
config:# user create
```

```
user create [name <name>] [enabled <enabled>] [groups <groups>]
```

新ユーザーの作成

name ユーザー名

enabled ユーザーが有効な状態(true/false)

groups グループ (comma separated list of group names) (Admin)

- ユーザーが新しいユーザー「cccc」をグループ「aaa」と「bbbbbb」に作成する場合、グループ名のスペースを受け入れることができない為、グループ名を引用符で囲む必要があります。
- コマンド例:
 - user create name cccc enabled true groups "aaa/bbb bbb"

```
config:# user delete [name <name>]
```

ユーザー削除

name ユーザー名 (管理者)

```
config:# user modify [name <name>] [password] [fullName <fullname>]
[telephoneNumber <telephone>] [eMailAddress <email>] [enabled <enabled>]
[forcePasswordChangeOnNextLogin <forcepwchange>] [snmpV3Access <snmpv3>]
[securityLevel <seclvl>] [userPasswordAsAuthenticationPassphrase
<pwasauthpass>] [authenticationPassPhrase
<authpassasprivpass>]
[useAuthenticationPassPhraseAsPrivacyPassPhrase <authpassasprivpass>]
[privacyPassPhrase] [authenticationProtocol <authproto>] [privacyProtocol
<privproto>] [groups <groups>] [sshPublicKey]
```

ユーザーの作成または編集

name	ユーザー名 (admin)
password	アカウントパスワード
fullName	フルネーム
telephoneNumber	電話番号
eMailAddress	E メールアドレス
enabled (true/false)	ユーザーが有効な状態
forcePasswordChangeOnNextLogin	ユーザーが次のログイン時にパ
スワードを変更する必要があるかどうかを選択 (true/false)	
snmpV3Access (enable/disable)	SNMPv3 アクセスを有効/無効
securityLevel (noAuthNoPriv/authNoPriv/authPriv)	SNMPv3 セキュリティレベル
userPasswordAsAuthenticationPassphrase authentication passphrase (true/false)	SNMPv3 としてパスワードを使用
authenticationPassPhrase	認証パスフレーズ
useAuthenticationPassPhraseAsPrivacyPassPhrase パスフレーズとして使用 (true/false)	認証パスフレーズをプライバシー
privacyPassPhrase	プライバシーパスフレーズ
authenticationProtocol	認証プロトコル (MD5/SHA-1)
privacyProtocol (DES/AES-128)	プライバシープロトコル
groups りリスト) (管理者)	グループ (グループ名のコンマ区切
sshPublicKey	SSH 公開鍵を設定

CLI: connect

connect <port index> (1.1/1.2.../2.4)

サポートされている CLI コマンド 『p. 28』 をご参照ください。

CLI: diag

diag

diag:# netstat

netstat <mode>

Netstat

mode netstat モードを指定 (ports/connections)

diag:# nslookup <host>

ネームサーバークエリ

host DNS 情報を照会するためのホスト名または IP アドレス

diag:# ping <dest> [count <num_echos>] [size <packet_size>] [timeout <timeout>]

Ping

dest ターゲットホスト名または IP アドレス

count 送信するエコー要求数を指定 (1..100) [5]

size 1つの要求パケットのバイト数を指定 (1..65468) [56]

timeout 応答を待機する最大時間 (秒単位) を指定 (1..600)

diag:# traceroute <dest> [useICMP]

Trace route

dest ターゲットホスト名または IP アドレス

useICMP UDP パケットの代わりに ICMP パケットを使用

CLI: reset

リセット

```
# reset
reset <command> [arguments...]
```

▶ 使用可能コマンド:

factorydefaults	デバイスを工場出荷時のデフォルトにリセット
unit	デバイスをリセットして再起動

```
# reset factorydefaults
reset factorydefaults /y ...
デバイスを工場出荷時のデフォルトにリセット
```

```
/y ... Assume 'yes' as answer to questions
```

```
# reset unit /y ...
デバイスをリセットして再起動
```

```
/y ... Assume 'yes' as answer to questions
```

CLI: show

表示

show <command> [arguments...]

▶ 使用可能コマンド:

authentication	認証設定に関する情報を表示
connectedusers	接続されているユーザー情報を表示
device	デバイス情報を表示、接続されている場合、DSAM 情報も
eventlog	イベントログを表示
groups	グループ情報を表示
history	セッションコマンド履歴を表示
keyword	設定されたシリアルポートキーワードを表示
network	全てのネットワーク情報を表示
port	DSAM シリアルポートパラメータを表示
security	セキュリティ設定を表示
serial	シリアルポートパラメータを表示
terminalblock	端子台の設定を表示
time	日付/時刻情報を表示
user	ユーザー情報を表示

```
# show authentication
認証タイプ : ローカル

構成済みの LDAP サーバー :

# IP address Server type
-----
No servers are currently configured.

構成済みの Radius サーバー:

# IP address Authentication type Ports (auth./acc.)
-----
No servers are currently configured.
#
# show connectedusers
-----
User Name      IP Address  Client Type  Idle Time
-----
admin          192.168.55.11  CLI (SSH)    0m
#
# show device
Device 'SteveKX4-101'
Product:      KX4
Model:        DKX4-101
Firmware Version: 4.0.0.1.45557
Hardware ID:   1
Serial Number: 1IT8400006
Internal Temperature Current Value: 38.7 C / 101.6 F
Internal Temperature Maximum Value: 39.6 C / 103.3 F

# show eventLog
Event Time      Event Class  Event Message
```

```

-----
-----
2019-03-01 09:17:34 EST    User Activity  User 'admin' from host '192.168.32.187'
logged out.
2019-03-01 09:17:34 EST    User Activity  Session of user 'admin' from host
'192.168.32.187' timed out.
2019-03-01 09:44:54 EST    User Activity  User 'admin' from host '192.168.32.206'
logged in.
2019-03-01 09:55:00 EST    User Activity  User 'admin' from host '192.168.32.206'
logged out.
2019-03-01 09:55:00 EST    User Activity  Session of user 'admin' from host
'192.168.32.206' timed out.
2019-03-01 16:03:52 EST    User Activity  Authentication failed for user 'admin'
from host '192.168.32.187'.
2019-03-01 16:03:56 EST    User Activity  User 'admin' from host '192.168.32.187'
logged in.
2019-03-01 16:15:00 EST    User Activity  User 'admin' from host '192.168.32.187'
logged out.
2019-03-01 16:15:00 EST    User Activity  Session of user 'admin' from host
'192.168.32.187' timed out.
2019-03-04 06:32:19 EST    User Activity  User 'admin' from host '192.168.32.184'
logged in.
2019-03-04 06:33:17 EST    Device        Firmware upgrade started from version
'4.0.0.1.45553' to version '4.0.0.1.45557' by user 'admin' from host
'192.168.32.184'.
2019-03-04 06:35:52 EST    Device        The ETHERNET network interface link is
now up.
2019-03-04 06:35:54 EST    Device        Firmware upgraded successfully from
version '4.0.0.1.45553' to version '4.0.0.1.45557' by user 'admin' from host
'192.168.32.184'.
2019-03-04 06:35:54 EST    Device        System started.
2019-03-04 06:36:34 EST    User Activity  Authentication failed for user 'admin'
from host '192.168.32.184'.
2019-03-04 06:36:39 EST    User Activity  User 'admin' from host '192.168.32.184'
logged in.
2019-03-04 06:45:00 EST    User Activity  User 'admin' from host '192.168.32.184'
logged out.
2019-03-04 06:45:00 EST    User Activity  Session of user 'admin' from host
'192.168.32.184' timed out.
2019-03-06 07:43:24 EST    User Activity  User 'admin' from host '192.168.55.11'
logged in.
2019-03-06 07:55:10 EST    User Activity  User 'admin' from host '192.168.55.11'
logged out.
2019-03-06 07:55:10 EST    User Activity  Session of user 'admin' from host
'192.168.55.11' timed out.
2019-03-07 09:39:44 EST    User Activity  User 'admin' from host '192.168.55.11'
logged in.

```

```

2019-03-07 09:53:22 EST    User Activity  User 'admin' from host '192.168.55.11'
logged out.
2019-03-07 09:53:22 EST    User Activity  Session of user 'admin' from host
'192.168.55.11' timed out.
2019-03-11 13:14:34 EDT    User Activity  User 'admin' from host '192.168.55.11'
logged in.
2019-03-11 13:16:39 EDT    User Activity  User 'admin' from host '192.168.55.11'
logged in.
2019-03-11 13:24:46 EDT    User Activity  User 'admin' from host '192.168.55.11'
logged out.
2019-03-11 13:24:46 EDT    User Activity  Session of user 'admin' from host
'192.168.55.11' timed out.
2019-03-11 13:29:13 EDT    User Activity  User 'admin' from host '192.168.55.11'
logged out.
2019-03-11 13:30:32 EDT    User Activity  User 'admin' from host '192.168.55.11'
logged in.

```

```
# show groups
```

```
Group 'Admin' :
```

```
Description: System defined administrator group including all privileges.
```

```
Privileges:  adminPrivilege
```

```
# show keyword
```

```
Keyword: Example
```

```
Port: 1.1
```

```
# show network
```

```
DNS resolver
```

```
Servers:          192.168.50.115
                  192.168.50.116
```

```
Search suffix:   raritan.com.
```

```
Resolver preference: Prefer IPv6 addresses
```

```
Routing
```

```
IPv4
```

```
Default gateway: 192.168.50.126
```

```
Static routes:   None
```

```
IPv6
```

```
Default gateway: None
```

```
Static routes:   None
```

```

Interface 'ETHERNET'
  Link
    Configured speed: Automatic
    Configured duplex: Automatic
    Link state: Autonegotiation On, 1 Gbit/s, Full Duplex, Link OK
    MAC address: 00:0d:5d:00:02:d5
  IPv4
    Config method: DHCP
    Address: 192.168.50.35/24
    Preferred hostname: Not configured
    DHCP server: 192.168.50.115
  IPv6
    Disabled

# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Group based access control for IPv4: Disabled

Group based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login: No

Strong passwords: Disabled

Restricted Service Agreement: disabled
# show serial
Configured console baud rate: 115200 bit/s
Configured modem baud rate: 115200 bit/s

Device detection type: Force console
Detected device: Console

# show terminalblock
External input switch: Disabled
Current external switch state: Open

```

```
Give remote console user:    Full Access
Give local console user:    Full Access
External output device:    Disabled
External device state:    Disabled
Output action:              Turn Device Off
Device blink interval:     1 (half-seconds)
```

```
# show time
Device Time:    2019-03-11 13:50:26 EDT
Time Zone:     (UTC-05:00) Eastern Time (US & Canada)
Setup Method:  NTP synchronized
```

```
# show user
User 'admin':
Enabled: Yes
Groups:  Admin
```

```
SNMP v3 Access: Disabled
```

CLI: exit

出口
exit

付録 A 仕様

ケースの寸法:	<ul style="list-style-type: none"> 140mm (W) x 144mm (D) x 30mm (H), 5.51" (W) x 5.67" (D) x 1.18" (H)
重さ [電源アダプターを除く]:	<ul style="list-style-type: none"> 0.65kg (1.421lb)
動作温度:	<ul style="list-style-type: none"> 0 ° C -- 55 ° C (32 ° F --131 ° F)
保管温度:	<ul style="list-style-type: none"> 20 ° C -- 80 ° C (-4 ° F --176 ° F)
動作湿度:	<ul style="list-style-type: none"> 20%-80% RH
保管湿度:	<ul style="list-style-type: none"> 10%-90% RH
最大消費電力:	<ul style="list-style-type: none"> 4K@ 30 ビデオストリームでローカル USB デバイスなしの 12.5W。DKX4-101 は、それぞれ最大 500mA の 2 つの USB デバイスをサポートできます。
電源アダプター:	<ul style="list-style-type: none"> 異なるプラグを備えた ATS024T-W050V : 入力: ユニバーサル 100VAC-240VAC 50/60Hz 出力: 5VDC/4A C14 ソケット 安全認証: UL / CUL / PSE / BSMI / RCM / GS EMI: FCC / CE Class B ; Conduction and Radiation Met.
追加の電源アダプター:	<ul style="list-style-type: none"> C14 ソケット入力を備えた ATS24T-P050 入力: ユニバーサル 100VAC-240VAC 50/60Hz 出力: 5VDC/4A プラグ: US, EU, AU, UK, CN, Korea 安全認証: UL / CUL / PSE / BSMI / RCM / GS EMI: FCC / CE Class B ; Conduction and Radiation Met.
端子台出力:	<ul style="list-style-type: none"> ドライ接点出力は、最大 2A / 30VDC、0.5A / 60VDC、または 0.3A / 125VAC の負荷をサポート。
端子台入力:	<ul style="list-style-type: none"> ドライ接点入力のみ。電源入力はサポートしていません。
追加のインターフェースサポート用のケーブル:	<ul style="list-style-type: none"> D4CBL-DP-HDMI D4CBL-MDP-HDMI D4CBL-DVI-HDMI D4CBL-USBC-HDMI D4CBL-VGA-HDMI
取付けブラケット:	<ul style="list-style-type: none"> ブラケット「L」 KX101 (部品番号 250-62-3011-00) が含まれています。
オプションの取り付けハードウェア:	<ul style="list-style-type: none"> メタルフック DSAM-4 3 つの DKX4-101 ユニットを取り付ける為の 1U ブラケット RACK-KIT-DKX4-101-3 ユニバーサル HDMI ケーブルロック P / N : 254-01-0055-00

エラー! 指定したスタイルは使われていません。: エラー! [ホーム] タブを使用して、ここに表示する文字列に **Heading 1** を適用してください。

内容

使用される TCP と UDP ポート 203

使用される TCP と UDP ポート

▶ TCP ポートのリスニング:

- * 80: http アクセス (構成可能)
- * 443: https アクセス (構成可能)
- * 5000: CC-SG & KXUS アクセス (構成可能)
- * 22: SSH アクセス (有効な場合、構成可能)
- * 68: DHCP アクセス (DHCP が有効の場合)

▶ UDP ポートのリスニング:

- * 162: SNMP アクセス (SNMP エージェントが有効になっている場合)
- * 5001: CC_SG イベント通知 (CC-SG 管理下にある場合)

▶ TCP Ports Outgoing:

- * 389: LDAP 認証 (LDAP が有効になっている場合、構成可能)
- * 636: LDAPS/StartTLS (LDAPS / StartTLS が有効になっている場合、構成可能)
- * 25: SMTP (E メール) (有効になっている場合)
- * 445: SMB (Windows ファイルシステム) アクセス (リモート ISO イメージアクセス).

▶ UDP Ports Outgoing:

- * 514: Syslog (有効な場合、構成可能)
- * 5001: CC_SG イベント通知 (CC-SG 管理下にある場合、構成可能)
- * 1812: RADIUS 認証 (有効な場合、構成可能)
- * 1813: RADIUS 認証 (有効な場合、構成可能)

インデックス

A

- Absolute • 86
- Absolute Mouse Synchronization • 51
- Access a Virtual Media Drive on a Client Computer • 63
- Access a Virtual Media Image File • iii, 64
- Active KVM Client (AKC) Help • 71
- Active System Partition • 172
- Active System Partitions • 171
- Add a Macro to the Toolbar • 82
- Add New Macro • 80
- Adjust Audio Settings • 70
- Adjust Full Screen Window Size to Target Resolution • 55, 57
- Adjusting Capture and Playback Buffer Size (Audio Settings) • 70
- Admin Group Special Privileges • 116, 117, 124
- AKC Supported Browsers • 72
- AKC Supported Microsoft .NET Framework • 72
- AKC Supported Operating Systems • 72
- Allow Cookies • 72
- Audio Menu • 96
- Audio Playback Recommendations and Requirements • 67
- Audio Settings • 97
- Auto Play in Safari • 98

B

- Backup and Restore • 161
- Bandwidth Requirements • 67
- Browser Tips for HSC • 39
- Build a New Macro • 47

C

- Change Your Password • 115
- CLI
 - check • 177
 - clear • 177
 - config • 178
 - config authentication • 179
 - config device • 182
 - config group • 183
 - config keyword • 184

- config network • 185
- config password • 187
- config port • 187
- config security • 188
- config serial • 190
- config terminalblock • 190
- config time • 190
- config user • 191
- connect • 193
- diag • 194
- exit • 202
- reset • 165, 195
- show • 196

- CLI Commands • 6, 177
- Client Launch Settings • 53, 58
- Client PC VM Prerequisites • 169
- Collect a Diagnostic Snapshot • 60
- Collecting a Diagnostic Snapshot of the Target • 60
- Conditions when Read/Write is Not Available • 64, 171
- Configure DSAM Serial Ports • 24, 26
- Configure Serial Port Keyword List • 26
- Configuring Authentication • 109, 113, 115
- Connect Audio • 96
- Connect Drive Permissions (Linux) • 172
- Connect Drive Permissions (Mac) • 173
- Connect DSAM • 22
- Connect Files and Folders • 93
- Connect ISO • 95
- Connect to a Digital Audio Device • 69
- Connect to DSAM Serial Target with URL Direct Port Access • 31
- Connect to DSAM Serial Targets in the Web Interface • 30
- Connect to DSAM Serial Targets via SSH • 31
- Connected Users • 115
- Connecting and Disconnecting from a Digital Audio Device • 68, 69
- Connecting the Equipment • 4
- Connecting the Terminal Block to a Motherboard • 147
- Connection Info • 46, 78
- Connection Properties • 44, 46, 76

Copy and Paste and Copy All • 36
 Cursor Shape • 53

D

Date and Time • 6, 128, 157
 Delete a Macro • 83
 Device Information • 125, 137
 Device Settings and Information • 125
 Diagnostics • 174
 Digital Audio • 66
 Digital Audio VKC and AKC Icons • 67
 Direct Port Access URL • 153
 Disable 'Protected Mode' • 72
 Disabling External Authentication • 115
 Disconnect from an Audio Device • 70
 Disconnect from Virtual Media Drives • 66
 Discovery Port • iii, 140
 Dominion KX IV-101 Virtual Media
 Prerequisites • 169
 Download Diagnostic • 174
 Drive Partitions • 171, 172
 DSAM LED Operation • 22
 Dual Mouse Modes • 51

E

Emulator • 32
 Enter Intelligent Mouse Mode • 51
 Event Log • 141, 163
 Event Management • 129, 131, 135, 141
 Export Macros • 49
 External Device • 70
 External Device Menu • 98

F

Firmware History • 164
 Front View • 2
 Full Screen Mode • 63

G

Gathering LDAP/Radius Information • 108, 109,
 111, 114
 General Settings • 54, 57
 Group Based Access Control • 149

H

HSC Functions • 32

HTML KVM Client (HKC) • 75
 HTML Serial Console (HSC) Help • 32
 HTTP/HTTPS Ports • iii, 140

I

Import and Export Macros • 80, 84, 104
 Import Macros • 48
 Importing and Exporting Macros • 48
 Include Dominion KX IV-101 IP Address in
 'Trusted Sites Zone' • 72
 Initial Configuration • 5, 165
 Input Menu • 79
 Install Certificate on Apple iOS Device • 100
 Installation and Initial Configuration • 1
 Intelligent • 87
 Intelligent Mouse Mode • 51
 Intelligent Mouse Synchronization Conditions •
 52, 87, 89
 IP Access Control • 150

J

Java Requirements • 41

K

Keyboard • 46
 Keyboard Access on Mobile • 104
 Keyboard Layout • 79
 Keyboard Limitations • 56
 Keyboard Macros • 47
 Keycode List • 119, 136
 KVM Client Options • 7
 KVM Clients • 8, 9, 40
 KVM Security • 10, 145, 152

L

Latest Edge Chromium 86.0.622.51 • 73
 LDAP Authentication • 110, 111
 Limitations on Apple iOS Devices • 99, 106
 Login Settings • 154

M

Macro Editor • 80, 104
 Maintenance • 161
 Manage HKC iOS Client Keyboard Macros • 104
 Mapped Drives • 171
 Minimum Client and System

- Recommendations • 1
- Mounting CD-ROM/DVD-ROM/ISO Images • 65, 173
- Mounting Local Drives • 170
- Mouse Modes • 86
- Mouse Options • 50
- Mouse Sync • 88
- Mouse Synchronization Tips • 53

N

- Network • 6, 129, 137
- Network Diagnostics • 175
- Network Services • 139
- Next Steps • 6
- Number of Supported Virtual Media Drives • 171

O

- Option 1
 - Connect a PC to the LAN Port • 5
- Option 2
 - Connect an iOS device at the Local Port • 5
- Option 3
 - Serial configuration • 6
- Overview • 72, 168

P

- Package Contents • 2
- Password Policy • 155
- Port Access • 9
- Port Access and Configuration • 9
- Port Configuration
 - Custom EDIDs • iii, 10, 18
 - KVM Port Settings - General, Video, Audio • iii, 6, 10
 - Local Port Monitor EDID • iii, 19
 - USB Connection Settings • 19
- Prerequisites for Using AKC • 71, 72
- Prerequisites for Using Virtual Media • 169
- Proxy Server Configuration • 43, 73

R

- Radius Authentication • 110, 114
- Rear View • 3
- Refresh Screen • 90
- Refreshing the Screen • 50

- Returning User Group Information from Active Directory Server • 113
- Returning User Group Information via RADIUS • 115
- Root User Permission Requirement • 172

S

- Saving Audio Settings • 68, 69
- Scaling • 62
- Screenshot • 90
- Screenshot from Target Command (Target Screenshot) • 50
- Security • 108, 149
- Send Ctrl+Alt+Del Macro • 46
- Send Email • 130, 131
- Send LeftAlt+Tab (Switch Between Open Windows on a Target Server) • 46
- Send Macro • 79
- Send Text File • 36, 37
- Send Text to Target • 46, 85
- Serial Access With Dominion Serial Access Module • iii, 21
- Serial Port • 144
- Service Agreement • 160
- Single • 88
- Single Mouse Mode • 54
- SMTP Server Settings • 131, 141
- SNMP Notifications • 130, 131
- SNMP Settings • 142, 167
- Specifications • 203
- SSH Settings • 120, 143
- Standard • 87
- Standard Mouse Mode • 52
- Supported Audio Device Formats • 66
- Supported Browsers • 1
- Supported CLI Commands • 28, 31, 193
- Supported Escape Key Characters • 30
- Supported Preferred Video Resolutions • 10, 12
- Supported Tasks Via Virtual Media • 170
- Supported Virtual Media Types • 170
- Synchronize Your Mouse • 53
- Syslog Messages • 130, 135

T

- Target Server VM Prerequisites • 169
- TCP and UDP Ports Used • 204

Terminal Block Control • iii, 145, 153
 Tips for Accessing Dominion KX IV-101 With
 Dual Monitor Setups • iii, 107
 TLS Certificate • iii, 6, 8, 156
 Tool Options • 54, 63
 Tools
 Start and Stop Logging • 38
 Tools Menu • 91, 103, 104
 Touch Mouse Functions • 103, 106

U

Unit Reset • 164
 Update DSAM Firmware • 28
 Update Firmware • 165
 User Management • 6, 108
 Users and Groups • 110, 116, 136, 137, 144, 145
 Using HKC on Apple iOS Devices • iii, 99

V

Version Information - Virtual KVM Client • 71
 Video • 50
 Video Menu • 90
 View DSAM Serial Ports • 23
 View Menu • 91
 View Options • 62
 View Status Bar • 62
 View Toolbar • 62
 Virtual KVM Client (VKCS) Help • 40
 Virtual Media • 63, 168
 Virtual Media File Server Setup (File Server ISO
 Images Only) • 173
 Virtual Media in a Linux Environment • 171
 Virtual Media in a Mac Environment • 172
 Virtual Media Menu • 93
 Virtual Media Performance Recommendations
 • 169
 Virtual Media Shared Images • 148

W

What's New in KX IV-101 Release 4.1.0 • iii