DominionKX III

Handbuch für Administratoren
Version 3.0

DKX3A-v3.0.0-0B-G

Februar 2014

255-62-0002-00

Einhaltung der FCC-Anforderungen

Dieses Gerät wurde getestet und entspricht den Beschränkungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Richtlinien („Federal Communications Commission“, zuständig für die Überprüfung von Strahlungsstörungen bei elektronischen Geräten) in den USA. Diese Beschränkungen dienen dem Schutz vor schädlichen Interferenzstörungen in Heiminstallationen. Dieses Gerät erzeugt, verwendet und strahlt Energie im Radiofrequenzbereich aus. Wenn es nicht gemäß den Anweisungen installiert und verwendet wird, kann sein Betrieb schädliche Interferenzen im Funkverkehr verursachen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

Einhaltung der VCCI-Anforderungen (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan übernimmt keine Haftung für Schäden, die zufällig, durch ein Unglück, Fehler, unsachgemäße Verwendung oder eine nicht von Raritan an dem Produkt ausgeführte Änderung verursacht wurden. Des Weiteren haftet Raritan für keine Schäden, die aus sonstigen außerhalb des Einflussbereichs von Raritan liegenden Ereignissen oder nicht aus üblichen Betriebsbedingungen resultieren.

Wenn ein Netzkabel im Lieferumfang dieses Geräts enthalten ist, darf es aussschließlich für dieses Produkt verwendet werden.

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

Sicherheitsrichtlinien zur Montage im Serverschrank

Bei Raritan-Produkten, die in ein Gestell montiert werden, sind folgende Vorsichtsmaßnahmen zu beachten:

- Die Betriebstemperatur in einer geschlossenen Gestellumgebung kann höher sein als die Raumtemperatur. Sorgen Sie dafür, dass die für die Appliances angegebene, maximale Umgebungstemperatur nicht überschritten wird. Siehe **Specifications** (Technische Daten).
- Sorgen Sie für eine ausreichende Luftzirkulation in der Gestellumgebung.
- Montieren Sie Geräte im Gestell sorgfältig, um eine ungleichmäßige mechanische Belastung zu vermeiden.
- Schließen Sie die Geräte mit Vorsicht an das Stromnetz an, um eine Überlastung der Stromkreise zu vermeiden.
- Erden Sie alle Geräte ordnungsgemäß, besonders die Anschlüsse an den Netzstromkreis (z. B. Mehrfachsteckdosen statt direkter Anschlüsse).

Inhalt

Kapitel 1 Einleitung

In diesem Kapitel

Überblick

Dominion KX III ist eine Enterprise-Klasse, ein sicherer, KVM-über-IP-Switch, der 1, 2, 4 oder 8 Benutzern mit Fern BIOS-Ebenesteuerung von 8 bis 64 Server zur Verfügung stellt.

KX III kommt mit Standardeigenschaften wie DVI / HDMI / Anzeiger digitalen und analogen Video-, Audio-, virtuelle Medien, Smartcard / CAC, Blade-Server-Unterstützung und mobilem Zugriff.

Setzen Sie KX III individuell ein, oder mit den CommandCenter Secure Gateway (CC-SG) von Raritan.

Neuerungen im Hilfedokument

- KX III unterstützt DVI Video Monitore
- Auch zu dieser Version hinzugefügt:
  - Die Fähigkeit, die Reichweite des KX III durch den Anschluss an Raritan Cat5 Reach DVI zu erweitern - siehe ***Ein KX III und ein Cat5 Reach DVI verbinden - Erweiterte lokale Port Funktionalität bereitstellen*** (siehe "***Verbinden Sie KX III und Cat5 Reach DVI - Erweiterte Lokale Portfunktionalität***" auf Seite 323)
  - Änderungen zum Virtual KVM Client (VKC) und Active KVM Client (AKC) Verbindungseinheiten - siehe ***Konfigurieren von Eigenschaften für die Verbindung*** (siehe "***Konfiguration von Verbindungseigenschaften***" auf Seite 251)
  - Favoriten in dem KX III Fernklient aktivieren und deaktivieren - siehe Favoriten verwalten
  - Unterstützung für alle externen virtuellen Medientypen

Paketinhalt

KX III wird als vollständig konfiguriertes, eigenständiges Produkt in einem standardmäßigen 1U-19-Zoll-Gestellchassis (2U für DKX2-864) geliefert. Im Lieferumfang aller KX III Geräte ist Folgendes enthalten:

Enthaltene Menge	Merkmal
1	KX III Gerät
1	Kurzanleitung für die KX III Installation
1	Gestellmontagekit
2	Netzkabel
1	Vier Gummifüße (für Schreibtischaufstellung)
1	Anwendungshinweis
1	Garantiekarte

KX III Gerätbilder und Funktionen

Hardware

- Integrierter KVM-über-IP-Remotezugriff
- 1U- oder 2U-Einschub (Halterungen im Lieferumfang enthalten)
- Zwei Netzteile mit Ausfallsicherung; automatischer Wechsel des Netzteils mit Stromausfallwarnung
- Die folgenden CIMs werden unterstützt:
  - Für virtuelle Medien und Absolute Mouse Synchronization (Absolute Maussynchronisierung) verwenden Sie eines der folgenden CIMS:
    - D2CIM-VUSB
    - D2CIM-DVUSB
    - D2CIM-DVUSB-DVI
    - D2CIM-DVUSB-HDMI
    - D2CIM-DVUSB-DP
  - Erforderlich bei PS2-Verbindung:

  - DCIM-PS2
- DVI-Monitor Unterstützung von DVI Lokaler Port
  - VGA Unterstützung via DVI zu VGA Konverter
  - DVI Unterstützung via DVI Standardkabel
- Unterstützung, wenn ein KX III Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird.
- Kapazität für mehrere Benutzer (1/2/4/8 Remotebenutzer, 1 lokaler Benutzer)
- UTP-Serverkabel (Kategorie 5/5e/6)
- Zwei Ethernet-Ports (10/100/1000 LAN) mit Ausfallsicherung
- Während des Betriebs aufrüstbar
- Lokaler USB Benutzerport für den Serverschrankzugriff
  - USB Tastatur/Mausports
  - Ein USB Port an der Vorderseite und drei an der Rückseite für unterstützte USB-Geräte
  - Simultane Lokaler und Remotebenutzerzugriff
  - Lokale grafische Benutzeroberfläche (GUI) für die Verwaltung
- Zentralisierte Zugriffssicherheit
- Integrierte Stromzufuhrsteuerung
- LED-Anzeigen für den Status der beiden Netzteile, Netzwerkaktivität und Remotebenutzerstatus
- Taste zum Zurücksetzen der Hardware

Hinweis: Die KX III 3.0.0 Version bietet keine Modem-Unterstützung, aber die zukünftige Version wird solche haben.

Software

- Virtuelle Medien Unterstützung Windows®, Mac® und Linux® Umgebungen*
- Absolute Maus Synchronization

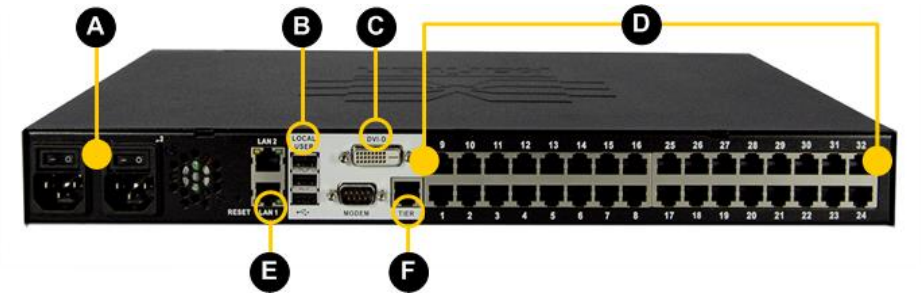
**Hinweis: Virtual media u nd Absolute Maus Synchronization erfordert die Verwendung von D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI oder D2CIM-DVUSB-DP CIM.*

- Unterstützung für digitale Audiogeräte über USB
- Port-Scanfunktion und Miniaturansicht von bis zu 32 Zielen innerhalb eines konfigurierbaren Scan-Satzes
- Webbasierte(r) Zugriff und Verwaltung
- Intuitive grafische Benutzeroberfläche (GUI)
- Unterstützung für Ausgabe über dualen Videoport
- 128-Bit-Verschlüsselung des gesamten KVM-Signals, einschließlich Video und virtueller Medien
- LDAP-, Active Directory-, RADIUS- oder interne Authentifizierung und Autorisierung
- DHCP oder feste IP-Adressen
- Smart Card-/CAC-Authentifizierung
- SNMP-, SNMP3- und Syslog-Verwaltung
- Unterstützung von IPv4 und IPv6
- Stromzufuhrsteuerung zur Vermeidung von Fehlern direkt mit Servern verknüpft
- Integration in die Verwaltungseinheit CommandCenter Secure Gateway (CC-SG) von Raritan
- Feature CC UnManage zum Entfernen eines Geräts aus der CC-SG-Steuerung
- Unterstützung für PX1- und PX2-Geräte von Raritan

Dominion KX3-832

KX3-832 Bilder

KX3-832 Funktionen



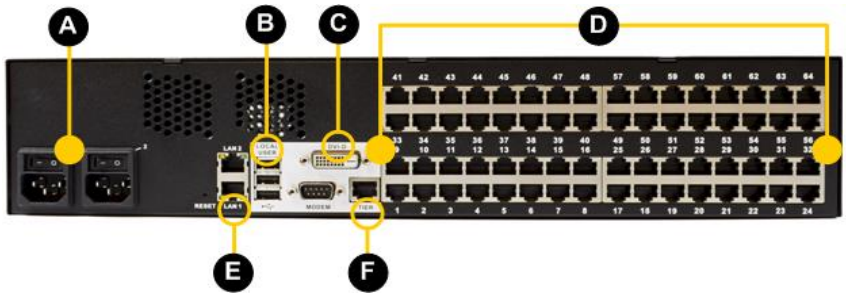
Diagrammschlüssel	
A	Zwei Netzteile AC 100V/240V
B	Lokale USB-Ports
C	DVI-D Port
D	32 KVM Ports UTP Verkabelung (Cat5/5e/6)
E	Dualer 10/100/1000-Ethernetzugriff
F	Schicht-Port

Hinweis: Die KX III 3.0.0 Version bietet keine Modem-Unterstützung, aber die zukünftige Version wird solche haben.

Dominion KX3-864

KX3-864 Bilder

KX3-864 Funktionen



Diagrammschlüssel	
A	Zwei Netzteile AC 100V/240V
B	Lokale USB-Ports
C	DVI-D Port
D	64 KVM Ports UTP Verkabelung (Cat5/5e/6)
E	Dualer 10/100/1000-Ethernetzugriff
F	Schicht-Port

Diagrammschlüssel
Hinweis: Die KX III 3.0.0 Version bietet keine Modem-Unterstützung, aber die zukünftige Version wird solche haben.

Anzahl der unterstützten Benutzer und Ports nach Modell:

Modell	Ports	Remote-Benutzer
KX3-864	64	8
KX3-832	32	8
KX3-808	8	8
KX3-464	64	4
KX3-432	32	4
KX3-416	16	4
KX3-232	32	2
KX3-216	16	2
KX3-132	32	1
KX3-116	16	1
KX3-108	8	1

Schaltfläche der KX III Fern-und Lokalkonsole

Verwenden Sie das Remote Console Interface, um KX III über eine Netzwerkverbindung zu konfigurieren und zu verwalten.

Das lokale Konsole-Interface bietet Zugriff auf KX III, wenn es ich auf dem Gestell befindet.

Siehe ***KX III Remote Console Interface*** (siehe "***Oberfläche der KX III Fernkonsole***" auf Seite 16) und ***Schaltfläche der lokalen KX III Konsole*** (auf Seite 26).

KX III KVM Client-Anwendungen

KX III funktioniert mit Virtual KVM Client (VKC) und Active KVM Client (AKC).

Für Hilfe, siehe ***Virtual KVM Client (VKC)*** (siehe "***Virtual KVM Klient (VKC) Hilfe***" auf Seite 249)und ***Active KVM Client (AKC)*** (siehe "***Aktive KVM Klient (AKC) Hilfe***" auf Seite 304)

KX III Online-Hilfe

KX III Online Hilfe wird als Ihre primäre Hilfequelle betrachtet. Die PDF-Versionen für Hilfe bieten eine sekundäre Quelle.

Siehe die KX III Versionshinweise für wichtige Informationen über die aktuelle Version, bevor Sie den KX III benutzen.

KVM-Hilfe wird als Teil der KX III Online-Hilfe bereitgestellt.

Zur KX III Installations-Hilfe gehört auch eine Kurzanleitung, die Sie auf der Firmware- und Dokumentationsseite von Raritan auf der ***Raritan-Webseite*** (***http://www.raritan.com/support/firmware-and-documentation***)finden .

Die Firmware-, Aktualisierungen- und Dokumentationen-Seite enthalten auch eine PDF-Version von Anwenderbereich für Online-Hilfe, inbegriffen KVM-Client-Hilfe, Lokale Konsole-Hilfe, Remote Konsole-Hilfe (als zutreffend), Spezifikationen und so weiter..

Hinweis: Um die Online-Hilfe zu verwenden, muss die Option "Active Content" (Aktive Inhalte) Ihres Browsers aktiviert sein.

Kapitel 2 Erste Schritte

In diesem Kapitel

Installieren und konfigurieren eines KX III

Falls dies noch nicht geschehen ist, installieren und konfigurieren Sie KX III.

Siehe die Kurzanleitung für die ***KX III Einrichtung*** ***http://www.raritan.com/support***, die Sie zusammen mit dem KX III Gerät erhalten oder laden Sie sie von der ***Raritan Support Webseite herunter*** (siehe "***KX III Installation und Konfiguration***" auf Seite 28).

Pop-Ups Zulassen

Unabhängig vom verwendeten Browser müssen Popups für die IP-Adresse des Geräts zugelassen werden, damit die KX III -Remotekonsole gestartet werden kann.

Sicherheitswarnungen und Bestätigungsmeldungen

Beim dem Anmelden bei KX III können Sicherheitswarnungen und Nachrichten für Anwendungsauthentifizierung erscheinen.

Diese beinhalten:

- Java ™ Sicherheitswarnungen und die Anträge, KX III zu validieren. Siehe ***Java Validierung und Zugangswarnung*** (auf Seite 10), und ***Installierung eines Zertifikates*** (siehe "***Installieren eines Zertifikats***" auf Seite 10)
- Je nach Browser- und Sicherheitseinstellungen werden möglicherweise verschiedene Sicherheits- und Zertifikatwarnungen angezeigt. Siehe ***Zusätzliche Sicherheitswarnungen*** (auf Seite 10)

Java Validierung und Zugangswarnung

Wenn Sie in KX III einloggen, wird Java® 1.7 Sie auffordern, KX III zu validieren und dann werden Sie den Zugriff auf die Anwendung erhalten.

Raritan empfehlt die Installation von SSL-Zertifikat in jedem KX III Gerät, um die Java-Sicherheitswarnungen zu verringern und um die Sicherheit zu verbessern. Siehe ***SSL-Zertifikate*** (auf Seite 190)

Zusätzliche Sicherheitswarnungen

Auch nachdem ein SSL-Zertifikat in dem KX III installiert wurde, je nach Browser- und Sicherheitseinstellungen werden verschiedene Sicherheitswarnungen beim Einloggen in KX III angezeigt.

Sie müssen diese Warnungen bestätigen, um die KX III Remote-Konsole zu starten.

können Sie die Zahl der Warnmeldungen zur Sicherheit und zu Zertifikaten für zukünftige Anmeldungen reduzieren, indem Sie darin die folgenden Kontrollkästchen aktivieren:

- Diese Warnung nicht mehr anzeigen
- Inhalt von diesem Herausgeber immer vertrauen

Installieren eines Zertifikats

Sie können vom Browser aufgefordert werden, das KX III SSL-Zertifikat zu akzeptieren und zu validieren.

Abhängig je nach Browser- und Sicherheitseinstellungen werden verschiedene Sicherheitswarnungen beim Einloggen in KX III angezeigt.

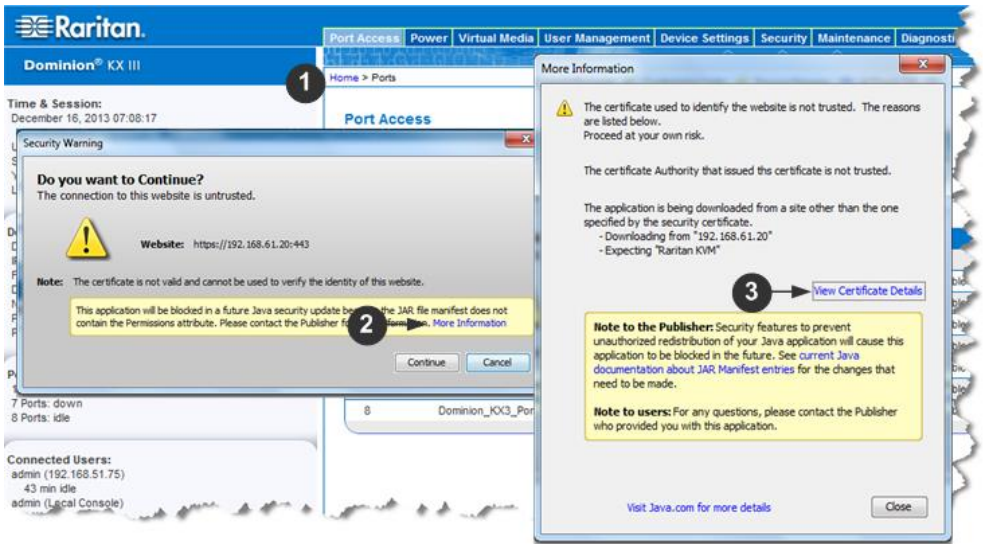
Sie müssen diese Warnungen bestätigen, um die KX III Remote-Konsole zu starten. Weitere Informationen finden Sie unter ***Sicherheitswarnungen und Bestätigungsmeldungen*** (auf Seite 9).

Hier sind zwei Beispielmethoden, wie man ein SSL-Zertifikat im Browser, sowohl mit dem Microsoft Internet Explorer 8 ® und Windows 7 ®installiert.

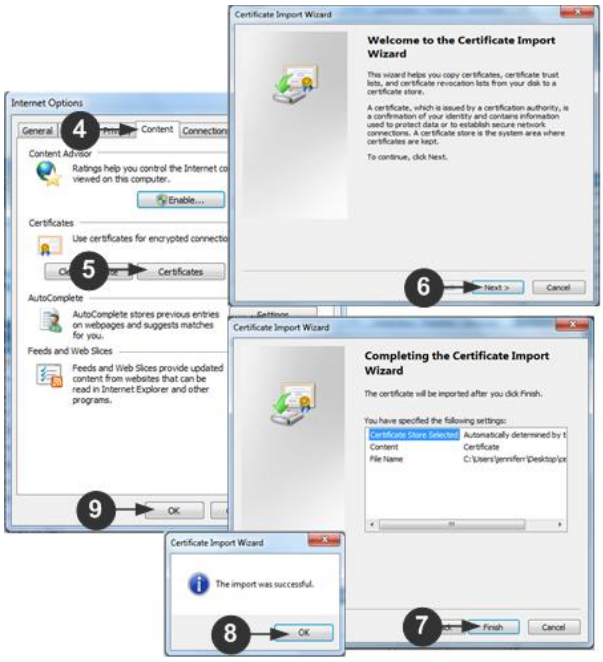
Die spezifische Methode und die Schritte hängen von Ihrem Browser und Betriebssystem ab. Siehe Ihr Browser und Betriebssystem-Handbuch für Einzelheiten.

Beispiel 1: Zertifikat in den Browser importieren

In diesem Beispiel importieren Sie das Zertifikat in den Browser.



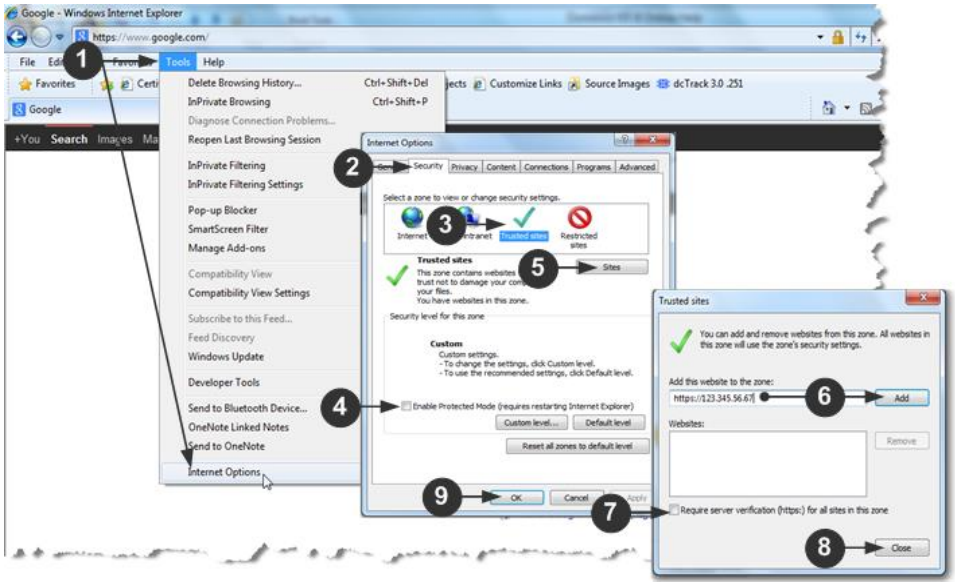
Schritte	
1	IE – Browser öffnen, dann in KX III einloggen.
2	Klicken Sie auf Weitere Information auf der ersten Java™ Sicherheitswarnung.
3	Klicken Sie „Zertifikateinzelheiten Anschauen“ in dem „Mehr Information“-Dialog. So installieren Sie das Zertifikat. Folgen Sie den Anweisungen des Wizards. *Hinweis: Wenn Sie nicht vom Browser aufgefordert werden, klicken Sie im Internet-Optionen-Dialog auf "Tools" (Extras) > "Internet Options" (Internetoptionen).*



Schritte	
4	Klicken Sie auf Inhalt-Tab
5	Auf Zertifikate klicken.
6	Der Zertikat-Importieren-Wizard öffnet und hilft Ihnen bei den Schritten. ▪ Datei importieren – Durchsuchen, um das Zertifikat zu finden ▪ Zertifikatspeicherung - Wählen Sie den Speicherort, um das Zertifikat zu speichern
7	Klicken Sie auf "Fertig stellen“ beim letzten Schritt des Wizards.
8	Das Zertifikat ist importiert. Schließen Sie die Erfolgs-Nachricht.
9	Klicken Sie auf OK in dem Internetoptionen-Dialogfeld, um die Änderungen zu aktivieren, dann schließen Sie es und öffnen Sie den Browser.

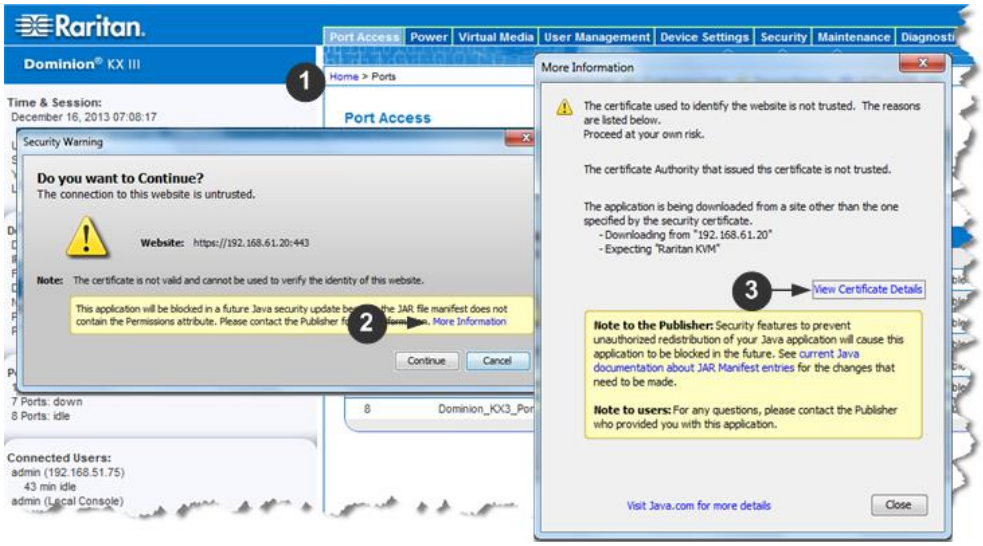
Beispiel 2: KX III zu vertrauenswürdigen Seiten hinzufügen und das Zertifikat importieren

In diesem Beispiel wird der KX-III-URL als eine vertrauenswürdige Seite hinzugefügt, und das selbssigniertes Zertifikat wird als Teil des Prozesses aufgenommen.



Schritte	
1	Klicken Sie im Internet Explorer auf "Tools" (Extras) "Internet Options" (Internetoptionen), um das Dialogfeld "Internet Options" (Internetoptionen) zu öffnen.
2	Klicken Sie auf die Registerkarte Sicherheit.
3	Klicken Sie auf "vertrauenswürdige Seite“.
4	Geschützter Mode Deaktivieren und alle Warnungen akzeptieren.
5	Klicken Sie auf die Seiten, um den vertrauenwürdigen Seiten-Dialog zu öffnen.
6	KX III URL eingeben und auf Hinzufügen klicken.
7	Deaktivieren Sie eine Serverüberprüfung für die Zone (falls zutreffend).
8	Klicken Sie auf Close (Schließen).

Schritte	
9	Klicken Sie auf OK in dem Internetoptionen-Dialogfeld, um die Änderungen zu aktivieren, dann schließen Sie es und öffnen Sie den Browser. Zertifikat zu importieren.



Schritte	
1	IE – Browser öffnen, dann bei KX III einloggen.
2	Klicken Sie auf Weitere Information auf der ersten Java™ Sicherheitswarnung.
3	Klicken Sie „Zertifikateinzelheiten Anschauen“ in dem „Mehr Information“-Dialog. So installieren Sie das Zertifikat. Folgen Sie den Anweisungen des Wizards. Weitere Informationen, siehe ***Beispiel 1: Zertifikat in den Browser importieren*** (auf Seite 11)

Anmeldung bei KX III

Melden Sie sich von einer beliebigen Workstation bei dem KX III an, die eine Netzwerkverbindung herstellen kann und auf der Microsoft .NET® bzw. Java Runtime Environment™ installiert ist.

Anmelden und KX III benutzen erfordert, dass Sie die Pop-ups erlauben.

Für Informationen über Sicherheitswarnungen und Bestätigungsmeldungen, und für Schritte, diese zu reduzieren, siehe ***Security Warnings and Validation Messages*** (siehe "***Sicherheitswarnungen und Bestätigungsmeldungen***" auf Seite 9)

So melden Sie sich bei der Webschnittstelle an:

1. Einen unterstützten Webbrowser starten.
2. Geben Sie ein:
   - Die URL - *http://IP-ADDRESS* um den virtuellen, Java-basierten KVM Client zu verwenden

     Oder

   - *http://IP-ADDRESS/akc* für den Microsoft .Net-basierten Aktiv KVM Client

   Die *IP-ADRESSE* ist die Ihrem KX III zugewiesene IP-Adresse ist.

   Sie können auch HTTPS, oder den DNS-Namen von KX III verwenden, der von Ihrem Administrator zugewiesen wurde (falls zutreffend).

   Sie werden immer auf die IP-Adresse von HTTP auf HTTPS umgeleitet.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, dann klicken Sie auf Einloggen.
4. Benutzervereinbarung annehmen (wenn zutreffend).
5. Wenn die Sicherheitswarnung erscheint, annehmen und/oder Zugang erlauben.

Kapitel 3 KX III Schaltfläche und Navigation

In diesem Kapitel

Überblick

Die KX III -Remotekonsole und die lokale KX III -Konsole bieten für die Konfiguration und Verwaltung des Geräts eine webbasierte Schaltfläche sowie eine Liste und Auswahl der Zielserver.

Oberfläche der KX III Fernkonsole

Die KX III-Remotekonsole ist eine browserbasierte grafische Benutzeroberfläche, mit der Sie sich an KVM-Zielservern und seriellen Zielgeräten, die mit KX III verbunden sind, anmelden und KX III von einem Remotestandort aus verwalten können.

Die KX III-Remotekonsole bietet eine digitale Verbindung mit den angeschlossenen KVM-Zielservern. Wenn Sie sich über die KX III-Remotekonsole bei einem KVM-Zielserver anmelden, wird ein Fenster für den Virtual KVM Client geöffnet.

Die grafischen Benutzeroberflächen der lokalen KX III-Konsole und der KX III-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Benutzerhandbuch hingewiesen. Die folgenden Optionen stehen nur für die KX III-Remotekonsole, nicht jedoch für die lokale KX III-Konsole zur Verfügung:

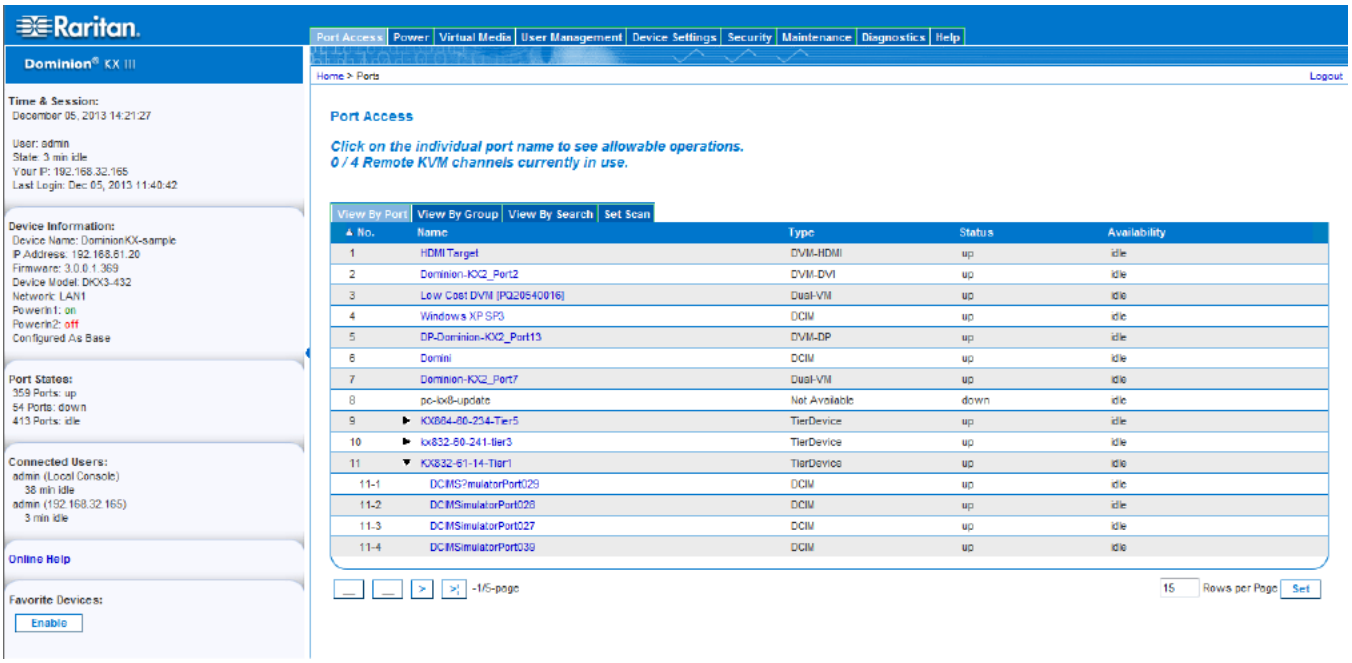
- Virtuelle Medien
- Favorites (Favoriten)
- Backup/Restore (Sicherung/Wiederherstellung)
- Firmware Upgrade (Firmware-Aktualisierung)
- SSL-Zertifikate
- Audio

Seite "Port Access" (Portzugriff) (Anzeige der Remotekonsole)

Nachdem Sie sich erfolgreich angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt, in der alle Ports mit ihrem Status und ihrer Verfügbarkeit aufgeführt sind.

Ports, die mit KVM-Zielservern (Blade- oder Standardserver) und Powerstrips verbunden sind, werden blau angezeigt und können bearbeitet werden. Rechts-Klick auf einen dieser Ports, um das Port-Aktionsmenü zu öffnen. Weitere Informationen finden Sie unter ***Port Action Menu*** (siehe "***Menü Port Action (Portaktion)***" auf Seite 20).

Für Ports, an die kein CIM angeschlossen sind oder für die kein CIM-Name angegeben ist, wird der Standardportname Dominion-KX3_Port#zugewiesen, wobei "Port#" für die Nummer des physischen KX III Ports steht.



Auf der Seite werden vier Registerkarten angezeigt (für die Ansicht nach Port, Ansicht nach Gruppe oder Ansicht nach Suche).

Klicken Sie auf eine Spaltenüberschrift, um die Ports nach Port Number (Portnummer), Port Name (Portname), Status (Up oder Down) (Ein oder Aus) und Availability (Verfügbarkeit) (Idle, Connected, Busy, Unavailable und Connecting) (Inaktiv, Verbunden, Verwendet, Nicht verfügbar und Verbindung wird hergestellt) zu sortieren.

Auf der Registerkarte "Set Scan" (Scanfunktion einstellen) können Sie außerdem nach bis zu 32 Zielen suchen, die mit dem KX III verbunden sind. Siehe Scannen von Ports - Fernkonsole

Schichtgeräte – Seite "Port Access" (Portzugriff)

Wenn Sie eine Schichtkonfiguration verwenden, in der ein KX III-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, werden die Schichtgeräte auf der Seite "Port Access" (Portzugriff) angezeigt, wenn Sie auf das Symbol "Expand Arrow" (Pfeil erweitern) ▶ links neben dem Schichtgerätenamen klicken. Weitere Informationen zu Schichten finden Sie unter Konfigurieren und Aktivieren von Schichten.

Blade-Chassis – Seite "Port Access" (Portzugriff)

Das Blade-Chassis wird in einer erweiterbaren, hierarchischen Liste auf der Seite "Port Access" (Portzugriff) angezeigt, wobei das Blade-Chassis auf Stammebene der Hierarchie angezeigt und die einzelnen Blades unterhalb der Stammebene bezeichnet und angezeigt werden. Verwenden Sie das Symbol "Expand Arrow" (Pfeil erweitern) ▶ neben dem Stamm-Chassis, um die einzelnen Blades anzuzeigen.

Hinweis: Um das Blade-Chassis in hierarchischer Reihenfolge anzuzeigen, müssen für das Bladeserver-Chassis Blade-Chassis-Subtypen konfiguriert werden.

Duale Videoportgruppen – Seite "Port Access" (Portzugriff)

Dual Video-Portgruppen werden auf der Seite für den Portzugriff als Dual Port-Typen angezeigt. Die primären und sekundären Ports, die Teil einer Portgruppe sind, werden auf der Seite für den Portzugriff jeweils als Dual Port(P) und Dual Port(S) angezeigt. Wenn der CIM-Typ beispielsweise DCIM lautet, wird "DCIM Dual Port (P)" angezeigt.

Wenn Sie auf eine Dual Port-Videogruppe über den Remote-Client zugreifen, stellen Sie eine Verbindung zum primären Port her, der das Fenster für die KVM-Verbindung für die primären und sekundären Ports der Dual Port-Gruppe öffnet.

Hinweis: Der primäre duale Videoport wird beim Erstellen der Portgruppe definiert.

Hinweis: Zwei KVM-Kanäle sind erforderlich, um remote durch Klicken auf den primären Port eine Verbindung zur Dual Video-Portgruppe herzustellen. Sollten keine zwei Kanäle verfügbar sein, wird der Verbindungslink nicht angezeigt.

Hinweis: Das Menü "Action" (Aktion) wird nicht angezeigt, wenn Sie auf einen sekundären Port in einer dualen Videoportgruppe klicken.

Hinweis: Sie können vom lokalen Port gleichzeitig eine Verbindung zum primären und sekundären Port herstellen.

Registerkarte "View by Group" (Ansicht nach Gruppe)

Auf der Registerkarte "View by Group" (Ansicht nach Gruppe) werden das Blade-Chassis, die Standardportgruppen sowie die dualen Videoportgruppen angezeigt. Klicken Sie neben einer Gruppe auf das Symbol "Expand Arrow" (Pfeil erweitern) ►, um die der Portgruppe zugewiesenen Ports anzuzeigen.

Weitere Informationen zum Erstellen der einzelnen Portgruppentypen finden Sie unter Geräteverwaltung.

Registerkarte "View by Search" (Ansicht nach Suche)

Mithilfe der Registerkarte "View by Search" (Ansicht nach Suche) können Sie nach Portnamen suchen. Die Suchfunktion unterstützt die Verwendung eines Sternchens (*) als Platzhalter sowie die Verwendung vollständiger Namen und Teile von Namen.

Registerkarte "Set Scan" (Scanfunktion einstellen)

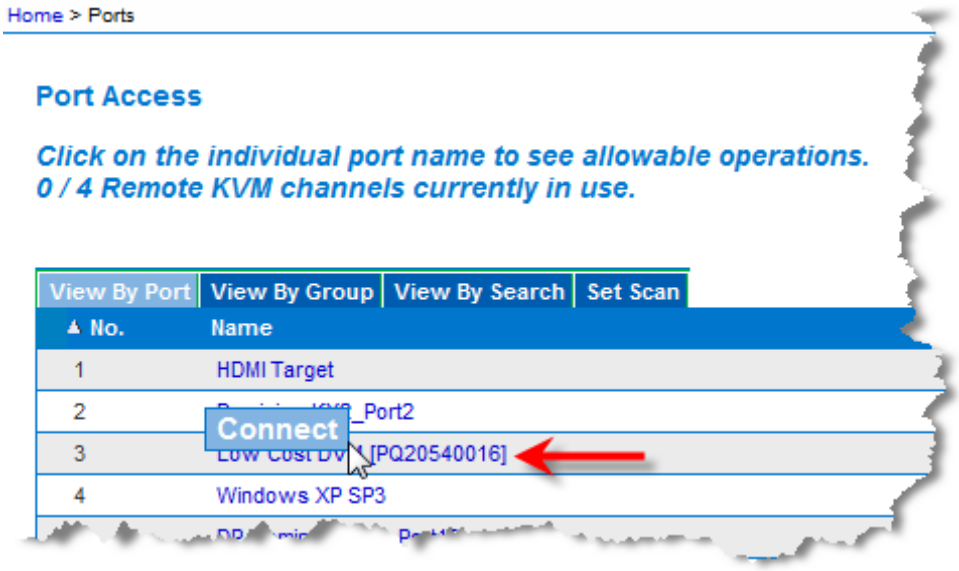
Über die Seite "Port Access" (Portzugriff) greifen Sie auf die Port-Scanfunktion zu. Mit dieser Funktion können Sie eine Reihe von zu scannenden Zielen festlegen. Die gescannten Ziele sind als Miniaturansicht verfügbar. Wählen Sie eine Miniaturansicht aus, um das entsprechende Ziel im Fenster des Virtual KVM Client zu öffnen.

Siehe - Scannen von Ports - Fernkonsole - für weitere Informationen.

Menü Port Action (Portaktion)

Wenn Sie in der Liste "Port Access" (Portzugriff) auf einen Portnamen klicken, wird das Menü "Port Action" (Portaktion) angezeigt.

Wählen Sie die gewünschte Menüoption für den Port aus. Beachten Sie, dass nur je nach dem Status und der Verfügbarkeit des Ports aktuell verfügbare Optionen im Menü "Port Action" (Portaktion) aufgelistet werden.



Verbinden

- Connect (Verbinden) – Erstellt eine neue Verbindung mit dem Zielserver.

  Für die ProductName-Remotekonsole wird eine neue Virtual KVM Client-Seite angezeigt.

  Für die lokale KX III -Konsole wechselt die Anzeige von der lokalen Benutzeroberfläche hin zum Zielserver.

  Auf dem lokalen Port muss die Oberfläche der lokalen KX III Konsole angezeigt werden, um den Wechsel durchführen zu können.

  Das Wechseln über Zugriffstasten ist vom lokalen Port auch verfügbar.

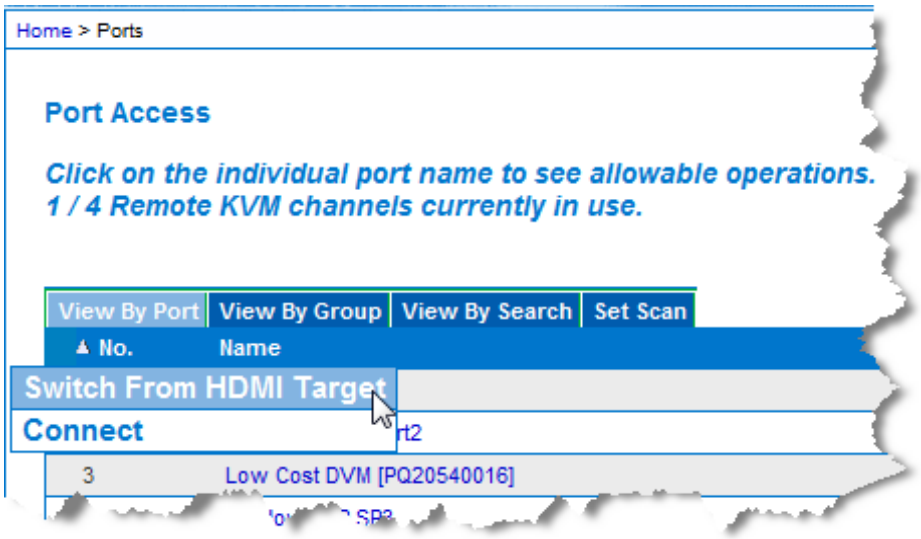
  Hinweis: Diese Option steht in der KX III-Remotekonsole für einen verfügbaren Port nicht zur Verfügung, wenn alle Verbindungen verwendet werden.

Switch From (Wechseln von)

- Switch From (Wechseln von) – Wechselt von einer bestehenden Verbindung zum gewählten Port (KVM-Zielserver).

  Diese Menüoption ist nur für KVM-Zielgeräte verfügbar und nur dann, wenn der Virtual KVM Client offen ist.

  Hinweis: Diese Menüoption steht auf der lokalen KX III-Konsole nicht zur Verfügung.

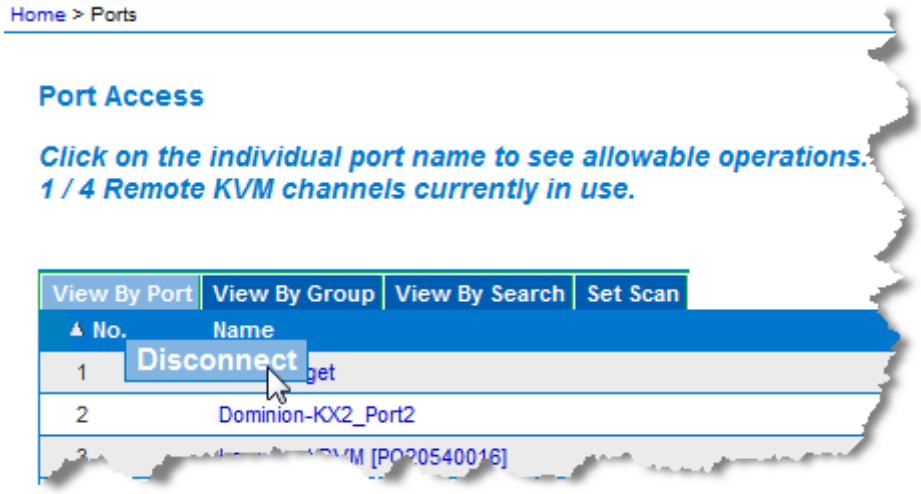


Trennen

- Disconnect (Trennen) – Trennt diese Portverbindung und schließt die Seite des Virtual KVM Client für diesen Zielserver.

  Diese Menüoption ist nur für den Portstatus Up (Ein) und die Verfügbarkeit Connected (Verbunden) bzw. Up (Ein) und Busy (Verwendet) verfügbar.

Hinweis: Diese Menüoption steht auf der lokalen KX III-Konsole nicht zur Verfügung. Sie können die Verbindung zum gewechselten Zielgerät auf der lokalen Konsole nur trennen, indem Sie die Zugriffstaste verwenden.



Einschalten

- Power On (Strom ein) – Versorgt den Zielserver über die zugeordnete Steckdose mit Strom.

  Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.

Ausschalten

- Power Off (Strom aus) – Unterbricht die Stromversorgung des Zielservers über die zugeordneten Steckdosen.

  Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht, wenn dieses eingeschaltet ist [Portstatus Up (Ein)] und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.

Aus- und einschalten

- Power Cycle (Aus- und Einschalten) – Schaltet den Zielserver über die zugeordneten Steckdosen aus und wieder ein.

  Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.

Linker Bildschirmbereich

Der linke Bildschirmbereich der KX III Schaltfläche enthält folgende Informationen.

Beachten Sie, dass einige Informationen konditional sind - was bedeutet, dass sie auf Grund Ihrer Rolle oder benutzter Funktionen, etc., angezeigt werden. Diese konditionalen Informationen werden nachfolgend aufgeführt.

Informationen	Beschreibung	Anzeige
Zeit & Sitzung	Datum und Uhrzeit, wann die aktuelle Sitzung begonnen hat.	Immer
Benutzer	Benutzername	Immer
Bundesland	Der aktuelle Status der Anwendung, entweder inaktiv oder aktiv. Bei Inaktivität zeichnet die Anwendung die Uhrzeit der inaktiven Sitzung auf und zeigt diese an.	Immer
Ihre IP	Die für den Zugriff auf KX III verwendete IP-Adresse.	Immer
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung.	Immer
Unter CC-SG-Verwaltung	Die IP-Adresse des CC-SG-Geräts, das KX III verwaltet	Wenn KX III von CC-SG verwaltet wird.
Geräteinformationen	Informationen zum verwendeten KX III	Immer
Gerätename	Dem Gerät zugewiesener Name	Immer
IP-Adresse	Die IP-Adresse des KX III	Immer
Firmware	Aktuelle Version der Firmware.	Immer
Gerätemodell	Modell des KX III	Immer
Seriennummer	Seriennummer des KX III	Immer

Informationen	Beschreibung	Anzeige
Netzwerk	Der dem aktuellen Netzwerk zugewiesene Name	Immer
Stromeingang1	Status der Stromversorgung 1. Entweder ein- oder ausgeschaltet oder automatische Erkennung ausgeschaltet.	Immer
Stromeingang2	Status der Stromversorgung 2. Entweder ein- oder ausgeschaltet oder automatische Erkennung ausgeschaltet.	Immer
Als Basis oder als Schicht konfiguriert	Wenn Sie eine Schichtkonfiguration verwenden, wird hier angezeigt, ob es sich bei KX III, auf das Sie zugreifen, um das Basis- oder Schichtgerät handelt.	Wenn KX III Teil einer Schichtkonfiguration ist
Portstatus	Die Status der Ports, die von KX III verwendet werden	Immer
Verbundene Benutzer	Die Benutzer, identifiziert durch Benutzername und IP-Adresse, die aktuell mit KX III verbunden sind	Immer
Online-Hilfe	Verknüpfung zur Online-Hilfe.	Immer
Bevorzugte Geräte	Siehe Verwalten von Favoriten.	Wenn aktiviert
FIPS-Modus	FIPS-Modus: Aktiviertes SSL-Zertifikat: Kompatibel mit FIPS-Modus	Wenn FIPS aktiviert ist

So reduzieren Sie den linken Bildschirmbereich

Der linke Bildschirmbereich kann reduziert werden, um den Anzeigebereich der Seite zu vergrößern.

So reduzieren Sie den linken Bildschirmbereich:

- Klicken Sie auf den blauen, nach links zeigenden Pfeil in der Mitte auf der linken Seite des Bildschirms. Wenn der Bildschirmbereich reduziert wurde, klicken Sie erneut auf den blauen Bereich, um den Bereich wieder zu erweitern.

Navigation in der KX III-Konsole

In den Oberflächen der KX III-Konsolen haben Sie viele Möglichkeiten für die Navigation und Auswahl.

Für die Auswahl von Optionen stehen folgende Möglichkeiten zur Verfügung:

- Klicken Sie auf eine Registerkarte. Eine Seite mit verfügbaren Optionen wird angezeigt.
- Zeigen Sie mit dem Cursor auf eine Registerkarte und wählen Sie die gewünschte Option aus dem Menü aus.
- Klicken Sie in der angezeigten Menühierarchie (den sogenannten "Breadcrumbs") direkt auf die gewünschte Option.

So blättern Sie durch Seiten, die größer als der Bildschirm sind:

- Verwenden Sie die Bild-Auf- und Bild-Ab-Tasten der Tastatur.
- Verwenden Sie die Bildlaufleiste auf der rechten Seite.

Schaltfläche der lokalen KX III Konsole

Die grafischen Benutzeroberflächen der lokalen KX III-Konsole und der KX III-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Hilfedokument hingewiesen.

Für Informationen siehe KX III Fernknsole - KX III Endbenutzer-Hilfe (siehe "***KX III Fernkonsole - KX III Anwender-Hilfe***" auf Seite 308).

Kapitel 4 KX III Administrator-Hilfe

In diesem Kapitel

Überblick

Administrator-Hilfe enthält spezifische Informationen zur KX-III-Funktionen, die in der Regel durch KX III Anwendungsadministratoren durhcgeführt werden. Solche sind: die Installation und Konfiguration von KX III, die Verwaltung von Benutzergruppen und Benutzern, Verwaltung der Sicherheit und so weiter.

Administrator-Funktionen werden in der Regel in der KX-III-Remote-Konsole und / oder von der lokalen Konsole durchgeführt.

Typisch durchgeführte Funktionen von Anwendern, mit der Verwendung von Virtual KVM Client oder Active KVM Client, und einige durchgeführten Funktionen aus der Remote-Konsole oder lokale Konsole werden in eigenen Abschnitten beschrieben.

Diese Funktionen sind virtuelle Medien, die Mauseinstellungen mit Hilfe der Scan-Port-Funktion konfigurieren, Video-Optionen konfigurieren und so weiter.

KX III Installation und Konfiguration

Siehe die Kurzanleitung für die KX III Installation, die Sie zusammen mit dem KX III Gerät erhalten oder laden Sie es von der Unterstützungsseite von Raritan herunter.

Weitere Informationen und optionale Schritte sind hier enthalten aber nicht in der QSG:

- ***Zusätzlich Unterstützte Mauseinstellungen*** (auf Seite 31)
- ***LED Status Während KX III Booten*** (auf Seite 34)
- ***Zur Verbindung mit einem VGA-Monitor (optional)*** (auf Seite 36)
- ***Schritt 6: Konfigurieren der Tastatursprache (optional)*** (auf Seite 45)

Gestellmontage

KX III passt in ein 19-Zoll-Standardgestell mit einer vertikalen Höhe von 1U (4,4 cm).

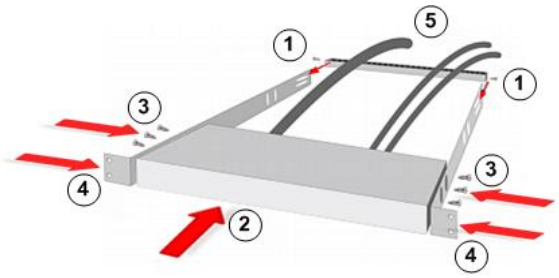
Hinweis: Das in den Abbildungen gezeigte Raritan-Gerät dient nur als Beispiel und stellt möglicherweise nicht Ihr Gerät dar. Die Montageanweisungen sind spezifisch auf Ihr Gerät zugewiesen.

Vorderseitenmontage

Die nachfolgenden Schritte entsprechen den in den Abbildungen für die Vorderseitenmontage angegebenen Nummern.

1. Befestigen Sie die Kabelhalterung mit zwei der Schrauben am hinteren Ende der seitlichen Halterungen.
2. Schieben Sie die KX III zwischen die seitlichen Halterungen, mit zur Kabelhalterung zeigender Rückseite, bis die Vorderseite mit der Hinterkante der seitlichen Halterungen abschließt.
3. Befestigen Sie KX III mit den übrigen Schrauben (drei pro Seite) an den seitlichen Halterungen.
4. Montieren Sie die gesamte Baugruppe im Gestell. Hierzu befestigen Sie die Laschen der seitlichen Halterungen an den vorderen Gestellschienen mit Ihren eigenen Schrauben und Muttern.

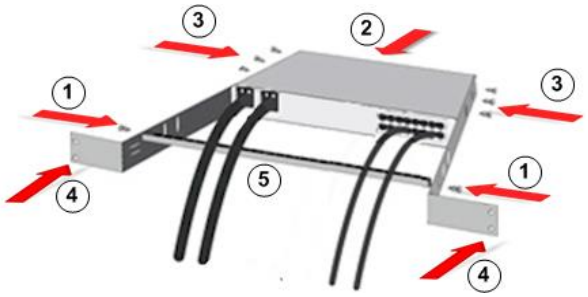
5. Führen Sie die Kabel beim Anschließen an der Rückseite der Benutzerstation oder des Switches über die Kabelhalterung.



Rückseitenmontage

Die nachfolgenden Schritte entsprechen den in den Abbildungen für die Rückseitenmontage angegebenen Nummern.

1. Befestigen Sie die Kabelhalterung mit zwei der Schrauben am vorderen Ende der seitlichen Halterung neben den Laschen der seitlichen Halterung.
2. Schieben Sie die KX III zwischen die seitlichen Halterungen, mit zur Kabelhalterung zeigender Rückseite, bis die Vorderseite mit der Hinterkante der seitlichen Halterungen abschließt.
3. Befestigen Sie KX III mit den übrigen Schrauben (drei pro Seite) an den seitlichen Halterungen.
4. Montieren Sie die gesamte Baugruppe im Gestell. Hierzu befestigen Sie mit Ihren eigenen Schrauben und Muttern die Laschen der seitlichen Halterungen an den vorderen Gestellschienen.
5. Führen Sie die Kabel beim Anschließen an der Rückseite der Benutzerstation oder des Switches über die Kabelhalterung.



Standard-Anmeldeinformationen

Standardwert	Wert
Benutzername	*admin*

Standardwert	Wert
	Dieser Benutzer besitzt Administratorrechte.
Kennwort	*raritan* Beim ersten Starten des KX III müssen Sie das Standardkennwort ändern.
IP-Adresse	192.168.0.192

Wichtig: Für die Sicherung und zur Gewährleistung der Geschäftskontinuität sollten Sie unbedingt einen Benutzernamen und ein Kennwort für den Sicherungsadministrator erstellen und diese Informationen an einem sicheren Ort aufbewahren.

Schritt 1: Konfigurieren der Einstellungen der Netzwerk-Firewall

TCP Port 5000

Lassen Sie die Netzwerk- und die Firewallkommunikation über TCP-Port 5000 zu, um den Fernzugriff zu KX III zu aktivieren.

KX III kann auch zur Verwendung eines anderen TCP-Ports konfiguriert werden. In diesem Fall muss die Kommunikation über diesen Port zugelassen werden.

TCP Port 443

Wenn Sie über einen Webbrowser auf KX III zugreifen möchten, muss der Zugriff auf den TCP-Port 443 (Standard HTTPS) zugelassen werden.

TCP-Port 80

Durch den Zugriff auf TCP-Port 80 (Standard HTTP) wird die automatische Umleitung von HTTP-Anfragen an HTTPS ermöglicht.

Schritt 2: Konfigurieren von KVM-Zielservern

Bildauflösung der Zielserver

Für eine Liste von unterstützten Ziel-Videoserverauflösungen, siehe ***KX III Supported Target Server Video Resolutions*** (siehe "***KX III Unterstützte Bildauflösung der Zielserver***" auf Seite 347) in KX III Online-Hilfe.

Mauseinstellungen

Raritan empfehlt die Verwendung von Absolute Mouse Synchronization, um die Mauseinstallungen auf dem Zielserver zu minimalisieren. Für die anderen Mausmodi, siehe ***Additional Unterstützt Mauseinstellungen*** (siehe "***Zusätzlich Unterstützte Mauseinstellungen***" auf Seite 31).

In diesem Modus werden absolute Koordinaten verwendet, um die Cursor von Client und Zielgerät synchron zu halten, auch wenn für die Maus des Zielgeräts eine andere Beschleunigung oder Geschwindigkeit eingestellt wurde.

Dieser Modus wird von Servern mit USB-Ports unterstützt und ist der Standardmodus für Virtuelle Medien CIMs.

Absolute Mouse Synchronization erfodert die Verwendung von Virtuellen Medien CIM :

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Zusätzlich Unterstützte Mauseinstellungen

Diese Einstellungen werden auf dem Zielbetriebssystem konfiguriert, sofern nicht anders angegeben ist.

Mauseinstellungen

Im Folgenden sind die Mauseinstellungen für verschiedene Betriebssysteme aufgeführt.

Diese Einstellungen werden auf dem Zielbetriebssystem konfiguriert, sofern nicht anders angegeben ist.

Siehe eine ausführliche OnlineAnleitung für KX III oder finden Sie die Einzelheiten für diesen Mauseinstellungen im Benutzerhandbuch.

Einstellungen für Microsoft Windows 7 und Windows Vista

Konfigurieren Sie diese Mauseinstellungen in Windows 7 ®und Windows Vista®:

Konfigurieren von Bewegungseinstellungen:

- Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
- Deaktivieren Sie das Kontrollkästchen "Zeigerbeschleunigung verbessern".

Deaktivieren der Animations- und Einblendeffekte:

- Steuerelemente und Elemente innerhalb von Fenstern animieren
- Animation beim Minimieren und Maximieren von Fenstern
- Menüs in Ansicht ein- oder ausblenden
- Quickinfo in Ansicht ein- oder ausblenden
- Menüelemente nach Aufruf ausblenden

Mauseinstellungen für Windows XP/Windows 2003, Windows 2008

Konfigurieren Sie diese Mauseinstellungen in Windows XP®, Windows 2003® und Windows 2008®:

Konfigurieren von Bewegungseinstellungen:

- Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
- Deaktivieren Sie die Option "Enhance pointer precision" (Zeigerbeschleunigung verbessern).
- Deaktivieren Sie die Option "Zur Standardschaltfläche springen".

Deaktivieren der Übergangseffekte:

- Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".

Mauseinstellungen für Windows 2000

Konfigurieren von diesen Windows 2000® Mauseinstellungen:

Konfigurieren von Bewegungseinstellungen:

- Stellen Sie die Beschleunigung auf Keine ein.
- Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.

Deaktivieren der Übergangseffekte:

- Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".

Apple Mac Mauseinstellungen

Konfigurieren von diesen Apple Mac® Mauseinstellungen:

Die Absolute Maussynchronization ist für die ordnungsgemäße Maussynchronisation auf KVM-Zielserver mit Mac ® Betriebssystem erforderlich.

Um die Absolute Maussynchronization funktionieren zu lassen, ist eine virtuelle Medien CIM erforderlich. Für eine Liste von unterstützten CIM, siehe ***Supported Computer Interface Module (CIMs) Specifications*** (siehe "***Spezifikationen der unterstützten Computer Interface Modules (CIMs)***" auf Seite 349).

Wenn Sie Ihre KX III Installierung beendet haben, richten Sie Ihr Mac USB-Profil ein. Wenn Sie dieses Profil nicht einstellen, funktioniert die Maussynchronisierung in OS X.

Führen Sie hierfür einen der folgenden Schritte aus:

1. Mac-Ziel von dem Raritan KVM Client verbinden.
2. USB Profil > Andere Profile > Mac OS-X (10.4.9 und höher) auswählen.

   Oder

3. In KX III wählen Sie Geräteeinstellungen > Portkonfiguration aus, um die Seite Port zu öffnen.
4. Wählen Sie im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen).
5. Wählen Sie "Mac OS-X (10.4.9) und höher" aus dem „Verfügbar“-Feld, dann klicken Sie auf „Hinzufügen“, um das Feld „Ausgewählt“ hinzuzufügen.
6. Klicken Sie auf "Mac OS-X (10.4.9) und höher" in dem Feld „Ausgewählt“. Dies fügt es automatisch zu dem Bevorzugten Profil Dropdown hinzu.
7. Wählen Sie "Mac OS-X (10.4.9) und höher" aus dem „Bevorzugtes Profil“ Dropdown, dann klicken Sie das Kontrollkästchen unter "Aktives Profil Als Bevorzugtes Profil“.

- Klicken Sie auf "OK", um es zu übernehmen.

Linux Mauseinstellungen

Konfigurieren von diesen Linux® Mauseinstellungen:

- (Nur für den Mausmodus Standard) Stellen Sie die Mausbeschleunigung und den Schwellenwert genau auf 1 ein. Geben Sie den Befehl `xset mouse 1 1 ein`. Die Einstellung sollte bei der Anmeldung übernommen werden.

Sun Solaris Mauseinstellungen

Sun Solaris Mauseinstellungen konfigurieren:

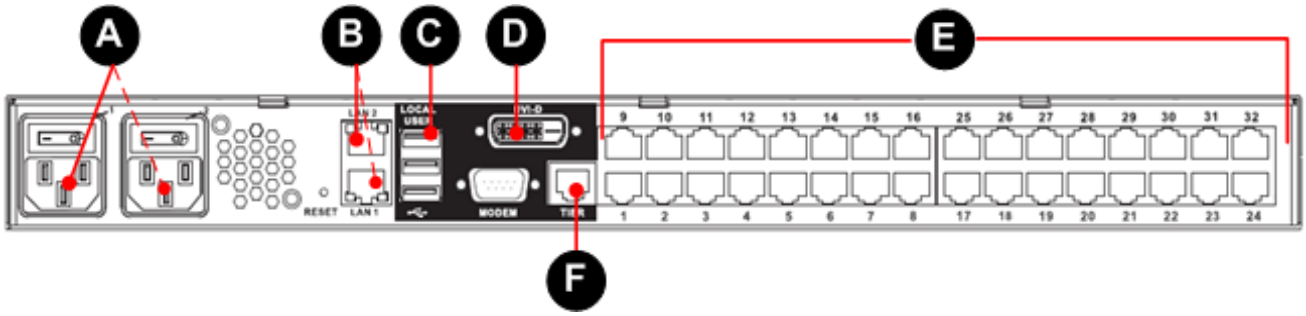
- Stellen Sie die Mausbeschleunigung und den Schwellenwert genau auf 1 ein.
- Stellen Sie sicher, dass Ihre Videokarte auf eine unterstützte Auflösung eingestellt ist und VGA ausgibt (keine Composite-Synchronisierung).

IBM AIX Mauseinstellungen

Konfigurieren von diesen IBM AIX® Mauseinstellungen:

- Navigieren Sie für Zielserver mit einem IBM AIX-Betriebssystem zum Style Manager (Stilmanager), klicken Sie auf Mouse Settings (Mauseinstellungen), und legen Sie folgende Werte fest: Mouse acceleration (Mausbeschleunigung) auf 1,0 und Threshold (Grenzbereich) auf 3,0.

Schritt 3: Anschließen der Geräte



A: Wechselstrom

So schließen Sie die Stromversorgung an:

1. Verbinden Sie das beiliegende Netzkabel mit KX III und schließen Sie es an die Wechselstromversorgung an.
2. Wenn eine Ausfallsicherung in Form zweier Netzteile gewünscht wird, verbinden Sie das zweite beiliegende Netzkabel und stecken Sie es an einer anderen Stromquelle ein als das erste Netzkabel.

LED Status Während KX III Booten

Wenn Sie KX III starten, werden sich die LED-Leuchten wie folgend verhalten:

- Beim ersten Einschalten
  - Alle Kanäle-LED sind eingeschaltet

  - Die Stromversorgung ist aus
- Auf der Boot-Phase:
  - Alle Kanäle-LED sind ausgeschaltet
  - Wenn beide Stromversorgungen eingeschaltet sind, blinkt die Betriebs-LED blau
  - Wenn eine Stromversorgung eingeschaltet ist, blinkt die Betriebs-LED rot

B: Netzwerk-Port

KX III verfügt zur Ausfallsicherung über zwei Ethernet-Ports (dienen nicht zum Lastausgleich).

Standardmäßig ist nur LAN1 aktiv und die automatische Ausfallsicherung ist deaktiviert.

Wenn die interne Netzwerkschnittstelle des KX III oder der mit diesem verbundene Netzwerkswitch nicht verfügbar sein sollte, wird der Port LAN2 unter Verwendung derselben IP-Adresse aktiviert, sofern das automatische Failover aktiviert wurde.

Herstellen einer Netzwerkverbindung:

1. Stellen Sie mit einem standardmäßigen Netzwerkkabel eine Verbindung zwischen dem Netzwerk-Port mit der Bezeichnung "LAN1" und einem Ethernet-Switch, -Hub oder -Router her.
2. Führen Sie die folgenden Schritte aus, wenn Sie die optionalen Ethernet-Failoverfunktionen des KX III nutzen möchten:
   a. Stellen Sie mit einem standardmäßigen Netzwerkkabel eine Verbindung zwischen dem Netzwerk-Port mit der Bezeichnung "LAN2" und einem Ethernet-Switch, -Hub oder -Router her.
   b. Aktivieren Sie auf der Seite KX III "Network Configuration" (Netzwerkkonfiguration) die Option "Automatic Failover" (Automatisches Failover).

C. Lokal Benutzer Port (Lokale Konsole)

Tastatur und Maus verbinden:

- Schließen Sie die USB-Tastatur und Maus an den Lokalen Benutzerport auf der Rückseite des KX III an.

Verwenden Sie den KX III Lokal-Benutzer-Port für den Zugriff auf Administrativen und Zielservers via einer graphischen Benutzer-Schnittstelle.

Der lokale Port wird für die Installation und Konfiguration benötigt, aber die weitere Verwendung dieses Ports ist optional.

Lokal DVI-D Port

Das DVI Standardkabel wird verwendet, um zu einem lokalen DVI-Monitor oder Tastatureinschub (nicht in dem KX III enthalten) zu verbinden.

Verbindung mit DVI-Port auf Raritan T1700-LED Tastaturschublade.

Verwenden Sie einen DVI-D-zu-VGA-Konverter, um das zu einem VGA-Monitor anzuschließen.

Verbindung zu einem DVI Monitor

Der lokale Monitor muss mindestens 1024x768 Auflösung unterstützen.

Verbindung zu einem DVI Monitor:

1. Schließen Sie die USB-Tastatur und Maus an den Lokalen Benutzerport auf der Rückseite des KX III an.
2. Schließen Sie das eine Ende eines DVI-Kabels am DVI-D-Port auf der Rückseite von KX III an.
3. Schließen Sie das andere Kabelende von DVI am DVI-Port auf dem DVI-Monitor an.

Zur Verbindung mit einem VGA-Monitor (optional)

Zur Verbindung mit einem VGA-Monitor.

1. Schließen Sie die USB-Tastatur und Maus an den Lokalen Benutzerport auf der Rückseite des KX III an.
2. Schließen Sie den DVI-D-auf-VGA-Konverter an dem DVI-D-Anschluss auf der Rückseite des KX III an und sichern Sie ihn, indem Sie die Schrauben auf jeder Seite im Uhrzeigersinn drehen.

3. Schließen Sie ein VGA-Kabel an dem DVI-D-auf-VGA-Konverter an, verbinden Sie das andere Ende mit dem VGA-Monitor und sichern Sie es mit den Schrauben.

Hinweis: Der DVI-D-zu-VGA-Konverter ist nicht im KX III enthalten. Kontaktieren Sie Raritan Verkaufsabteilung für Informationen.

E: Anschließen des Zielservers an KX III

So stellen Sie eine Verbindung zwischen einem Zielserver und KX III her:

1. Schließen Sie die Tastatur, Maus und Video-Stecker auf der CIM an die entsprechenden Ports auf dem Zielserver an.
2. Schließen Sie das CIM an einen freien Serverport auf der Rückseite des KX III Geräts an.

F Ebene (Optional)

Siehe ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 140, ***http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#33184***)

Schritt 4: Konfiguration von KX III

Für die folgende Schritte müssen Sie das Standardkennwort ändern und KX III zu der IP-Adresse bei der Lokalen Konsole zuweisen.

Alle anderen Schritte können entweder von der lokalen Konsole oder von der KX III Remote Console über einen unterstützten Web-Browser mit Standard-IP-Adresse von KX III durchgeführt werden.

Java® 1.7 (oder höher) oder Microsoft .NET® 3.5 (oder höher) ist für die Verwendung von KX III erfoderlich..

Ändern des Standardkennworts

Beim ersten Starten des KX III müssen Sie das Standardkennwort ändern.

So ändern Sie das Standardkennwort:

1. Sobald das Gerät gestartet ist, geben Sie den *Standard-Benutzernamen*, *Kennwort ein*. Klicken Sie auf Login (Anmelden).
2. Altes*raritan* Kennwort eingeben, dann geben Sie ein neues Kennwort ein.

   Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen.

3. Klicken Sie auf "Apply" (Übernehmen). Bestätigen Sie die Bestätigungsseite mit OK.

Zuweisen der KX III zur IP-Adresse.

So weisen Sie eine IP-Adresse zu KX III zu:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr KX III-Gerät an.

   Sie können bis zu 32 alphanumerische Zeichen und Sonderzeichen eingeben. Der Gerätename darf jedoch keine Leerzeichen enthalten.
3. Weiter, Konfigurieren der IPv4-, ipv6- und DNS-Einstellungen.

Konfiguration der IPv4-Einstellungen

1. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Geben Sie die IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
   b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
   c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
   d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
   e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
   - "None (Static IP)" \[Kein (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da KX III ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.

     Fällt der primäre Ethernet-Port (oder der Switch/Router, an dem der Ethernet-Port angeschlossen ist) aus, verwendet der Dominion KX III den sekundären Netzwerkport mit derselben IP-Adresse, wodurch sichergestellt wird, dass der Serverbetrieb nicht unterbrochen wird. Wenn es fehlschlägt, wechselt der KX III auf Sekundärnetzwerkanschluss mit der gleichen IP-Adresse, und gewährleistet, dass keine Unterbrechung stattfindet.

- DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

  Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server zugewiesen.

  Bei Verwendung von DHCP geben Sie unter "Preferred host name (DHCP only)" (Name des bevorzugten Hosts [Nur DHCP]) einen Wert ein (maximal 63 Zeichen).

2. Weiter, Konfigurieren von IPv6 und/oder DNS-Einstellungen.

Konfiguration der IPv6-Einstellungen

1. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:

   a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich und IPv6 auf dem Gerät zu aktivieren.

   b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem KX III zugeordnet ist.

   c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.

   d. Geben Sie die IP-Adresse des Gateway ein.

   e. Link-Local-IP-Adresse. Diese Adresse wird automatisch zu dem Gerät zugeordnet und sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Nur Lese-zugriff)**

   f. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Nur Lese-zugriff)**

   g. IP auto configuration (Automatische IP-Konfiguration):

   - "None (Static IP)" [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da KX III ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.

     Fällt der primäre Ethernet-Port (oder der Switch/Router, an dem der Ethernet-Port angeschlossen ist) aus, verwendet der Dominion KX III den sekundären Netzwerkport mit derselben IP-Adresse, wodurch sichergestellt wird, dass der Serverbetrieb nicht unterbrochen wird. Wenn es fehlschlägt, wechselt der KX III auf Sekundärnetzwerkanschluss mit der gleichen IP-Adresse, und gewährleistet, dass keine Unterbrechung erfolgt.

Wenn "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlange) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.

- Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.

2. Weiter, Konfigurieren von DNS-Einstellungen.

Konfigurieren von DNS-Einstellungen

1. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.
2. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

   Geben Sie die folgenden Informationen ein, wenn die Option "Following DNS Server Addresses" (Folgende DNS-Serveradressen) ausgewählt wurde. Diese Adressen sind die primären und sekundären DNS-Adressen, die verwendet werden, wenn die primäre DNS-Serververbindung aufgrund eines Ausfalls getrennt wird.

   a. "Primary DNS Server IP Address" (IP-Adresse des primären DNS-Servers)

   b. "Secondary DNS-Server IP Address" (IP-Adresse des sekundären DNS-Servers)
3. Klicken Sie abschließend auf OK.

Das KX III Gerät ist jetzt über das Netzwerk zugänglich.

Zielserver Benennen

So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist.
2. Klicken Sie auf Geräteinstellungen > Port-Konfiguration, dann klicken Sie auf den Portnamen des Zielservers, den Sie benennen möchten.

3. Geben Sie einen Namen für den Server ein.

   Geben Sie einen Namen mit bis zu 32 alphanumerische Zeichen und Sonderzeichen ein.

4. Klicken Sie auf OK.

Festlegen der automatischen Netzteilerkennung

KX III bietet doppelte Stromversorgung.

Wenn beide Netzteile verwendet werden, erkennt KX III automatisch diese und sendet Ihnen eine Benachrichtigung über den Status.

Darüber hinaus werden sowohl die Powerln1 und Powerln2 Auto Detect Checkboxen automatisch auf der Seite „Stromversorgungseinstellungen“ ausgewählt.

Wenn Sie nur ein Netzteil benutzten, aktivieren Sie die automatische Erkennung für die verwendeten Netzteile:

So aktivieren Sie die automatische Erkennung für die verwendeten Netzteile:

1. Wählen Sie "Device Settings Power Supply Setup" (Geräteeinstellungen und Netzteilkonfiguration) aus. Die Seite Power Supply Setup (Netzteilkonfiguration) wird angezeigt.
2. Wenn die Stromversorgung über das Netzteil 1 erfolgt (ganz links auf der Rückseite des Geräts), wählen Sie die Option "Powerln1 Auto Detect" (Netzteil 1 – Automatische Erkennung) aus.
3. Wenn die Stromversorgung über das Netzteil 2 erfolgt (ganz rechts auf der Rückseite des Geräts), wählen Sie die Option "Powerln2 Auto Detect" (Netzteil 2 – Automatische Erkennung) aus.
4. Klicken Sie auf OK.

Wenn eines dieser Kontrollkästchen aktiviert ist und nur das entsprechende Netzteil zurzeit angeschlossen ist, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite des Geräts rot auf.

Konfigurieren von Datum-/Uhrzeiteinstellungen (optional)

Sie können die Einstellung für Datum und Uhrzeit optional konfigurieren.

Die Einstellungen für Datum und Uhrzeit wirken sich auf die SSL-Zertifikatvalidierung aus, sofern LDAPS aktiviert ist.

So stellen Sie das Datum und die Uhrzeit ein:

1. Wählen Sie Device Settings -- Date/Time (Geräteeinstellungen -- Datum/Uhrzeit). Die Seite Date/Time Settings (Datum-/Uhrzeiteinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdown-Liste Time Zone Ihre Zeitzone aus.

3. Aktivieren Sie das Kontrollkästchen "Adjust for daylight savings time" (an Sommerzeit anpassen), um die Uhrzeit an die Sommerzeit anzupassen.
4. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:
   - User Specified Time (Benutzerdefinierte Zeit) – Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben. Falls Sie die Option "User Specified Time" (Benutzerdefinierte Zeit) ausgewählt haben, geben Sie Datum und Uhrzeit wie folgt ein: Geben Sie im Feld "Time" die Uhrzeit im Format hh:mm ein. (Verwenden Sie das 24-h-Zeitformat.)
   - Synchronize with NTP Server (Mit NTP-Server synchronisieren) – Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
5. Falls Sie die Option "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld "Primary Time Server" (Primärer Zeitserver) die IP-Adresse dieses Servers ein.
   b. Geben Sie im Feld "Secondary Time Server" (Sekundärer Zeitserver) die IP-Adresse dieses Servers ein **Optional**

Hinweis: Wenn DHCP für die Netzwerkeinstellungen auf der Netzwerk-Seite ausgewählt ist, wird die NTP-Server IP-Adresse automatisch vom DHCP-Server abgerufen werden.

Geben Sie die Adresse des NTP-Servers manuell ein, indem Sie das Override DHCP Kontrollkästchen auswählen.

---

6. Klicken Sie auf OK.

Erstellen von Benutzergruppen und Benutzern

Hinweis für CC-SG-Benutzer

Wenn KX III von CommandCenter Secure Gateway gesteuert wird, authentifiziert CC-SG Benutzer und Gruppen, mit Ausnahme von lokalen Benutzern, für die der Zugriff auf den lokalen Port erforderlich ist.

Steuert CC-SG die KX III Einheit, erfolgt die Authentifizierung von Benutzern des lokalen Ports über die lokale Benutzerdatenbank oder den für KX III konfigurierten Remote-Authentifizierungsserver (LDAP/LDAPS oder RADIUS). Sie werden nicht über die CC-SG-Benutzerdatenbank authentifiziert.

Weitere Informationen zur CC-SG-Authentifizierung finden Sie im **CommandCenter Secure Gateway-Benutzerhandbuch**, **im Administratorhandbuch** oder **im Bereitstellungshandbuch**, die im Bereich "Support" auf der ***Raritan-Website http://www.raritan.com***heruntergeladen werden können.

Unterstützte Protokolle

Zur Vereinfachung der Verwaltung von Benutzernamen und Kennwörtern bietet KX III die Möglichkeit, Authentifizierungsanforderungen an einen externen Authentifizierungsserver weiterzuleiten. Zwei externe Authentifizierungsprotokolle werden unterstützt: LDAP/LDAPS und RADIUS.

Hinweis zu Microsoft Active Directory

Microsoft® Active Directory® verwendet nativ das LDAP/LDAPS-Protokoll und kann als LDAP/LDAPS-Server und Authentifizierungsquelle für KX III fungieren. Bei Verwendung der IAS-Komponente (Internetautorisierungsserver) kann ein Microsoft Active Directory-Server auch als RADIUS-Authentifizierungsquelle dienen.

Schritt 5: Starten der KX III Remotekonsole

Melden Sie sich von einer beliebigen Workstation bei dem KX III an, der eine Netzwerkverbindung herstellen kann und auf der Microsoft .NET® bzw. Java Runtime Environment® installiert ist.

So starten Sie die KX III Remote-Konsole:

1. Einen unterstützten Webbrowser starten.
2. Geben Sie ein:
   - Die URL - *http://IP-ADDRESS* um den virtuellen, Java-basierten KVM Client zu verwenden

     Oder

   - *http://IP-ADDRESS/akc* für den Microsoft .Net-basierten Aktiv KVM Client

   Die *IP-ADRESSE* ist die Ihrem KX III zugewiesene IP-Adresse ist.

   Sie können auch HTTPS, oder den DNS-Namen von KX III verwenden, der von Ihrem Administrator zugewiesen wurde (falls zutreffend).
3. Sie werden immer auf die IP-Adresse von HTTP auf HTTPS umgeleitet.
4. Geben Sie Ihren Benutzernamen und das Kennwort ein. Klicken Sie auf Login (Anmelden).

Remotezugriff und Remotesteuerung der Zielserver

Auf der KX III Seite "Port Access" (Portzugriff) werden die KX III Ports und die verbundenen Zielserver sowie Angaben zu Status und Verfügbarkeit der Ports angezeigt.

Zugreifen auf einen Zielserver vom KX III aus

So greifen Sie auf einen Zielserver zu:

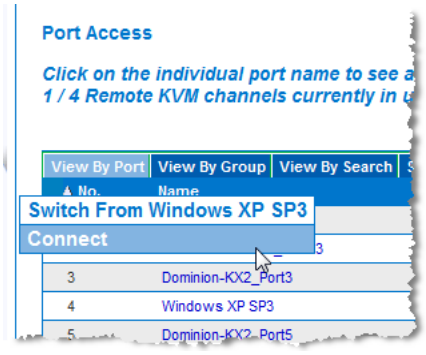
1. Klicken Sie auf der KX III Port Access Seite (Portzugriff) unter Port Name (Portname) auf den Portnamen des Ziels, auf das Sie zugreifen möchten. Das Menü Port Action (Portaktion) wird angezeigt.

2. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Connect" (Verbinden) aus. Ein KVM-Fenster wird geöffnet, das eine Verbindung zum Ziel anzeigt.

Wechseln zwischen Zielservern

So wechseln Sie zwischen KVM-Zielservern:

1. Rufen Sie die KX III-Seite "Port Access" (Portzugriff) auf, während bereits auf einen Zielserver zugegriffen wird.
2. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
3. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Switch From" (Wechseln von) aus. Der neue Zielserver, den Sie ausgewählt haben, wird angezeigt.



Trennen von einem Zielserver

So trennen Sie einen Zielserver:

- Klicken Sie auf der Seite Port Access (Portzugriff) unter Port Name (Portname) auf den Portnamen des Ziels, von dem Sie sich abmelden möchten.

  Oder

- Virtueller KVM-Client Fenster schließen.

Schritt 6: Konfigurieren der Tastatursprache (optional)

Hinweis: Dieser Schritt ist nicht erforderlich, wenn Sie eine US-/internationale Tastatur verwenden.

Wenn Sie eine andere Tastatur verwenden, muss diese für die jeweilige Sprache konfiguriert werden.

Außerdem muss die Tastatursprache für das Client-Gerät mit der der KVM-Zielserver übereinstimmen.

Weitere Informationen zum Ändern des Tastaturlayouts finden Sie in der Dokumentation Ihres Betriebssystems.

Ändern des Tastaturlayoutcodes (Sun-Zielgeräte)

Gehen Sie folgendermaßen vor, wenn Sie ein DCIM-SUSB verwenden und das Tastaturlayout auf eine andere Sprache ändern möchten.

So ändern Sie den Tastaturlayoutcode (nur DCIM-SUSB):

1. Öffnen Sie auf der Sun™-Workstation ein Texteditorfenster.
2. Vergewissern Sie sich, dass die Taste "Num Lock" aktiviert ist, und drücken Sie die linke Strg-Taste und die Taste "Entf" auf der Tastatur.

   Die LED der Feststelltaste beginnt zu blinken, was darauf hindeutet, dass sich das CIM im Modus zum Ändern des Layoutcodes befindet.

   Im Textfenster wird Folgendes angezeigt: `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX) \[Aktueller Tastaturlayoutcode = 22h (US5 UNIX)].`
3. Geben Sie den gewünschten Layoutcode ein (für eine japanische Tastatur beispielsweise *31*). Drücken Sie die Eingabetaste.
4. Schalten Sie das Gerät aus und wieder ein. Das DCIM-SUSB wird zurückgesetzt (Ein- und Ausschalten).
5. Überprüfen Sie, ob die Zeichen korrekt sind.

Schritt 7: So erstellen und installieren Sie ein SSL-Zertifikat

Raritan empfiehlt Ihnen, ein eigenes SSL-Zertifikat in jedem KX III Gerät zu installieren.

Diese bewährte Sicherheitsmethode reduziert die Anzahl der Java ® Warnmeldungen und verhindert die Man-in-the-Middle-Angriffe.

Es verhindert auch, dass zukünftige Java-Versionen und Browser-Versionen den Zugriff zu Ihrem KX III blockieren.

Für Informationen über, wie SSL Zertifikate erstellt und installiert werden, siehe ***SSL-Zertifikate*** (auf Seite 190)

Gestell-PDU-Ausgangssteuerung (Powerstrip)

Überblick

Mit KX III können Sie die Ausgänge der PX- und RPC-Gestell-PDUs (Powerstrip) von Raritan steuern. ist über ein D2CIM-PWR mit dem KX III verbunden.

Ist ein PX oder ein RPC eingerichtet und an KX III angeschlossen, können die Gestell-PDU und die Ausgänge über die Seite "Powerstrip" der KX III-Benutzeroberfläche gesteuert werden. Sie können auf diese Seite zugreifen, indem Sie auf das Menü "Power" (Strom) oben auf der Seite klicken.

Die Seite "Powerstrip" zeigt an KX III angeschlossene Gestell-PDUs an, für die der Benutzer entsprechende Portzugriffsberechtigungen erhalten hat. Bei Schichtkonfigurationen zeigt die Seite "Powerstrip" Gestell-PDUs an, die an KX III-Basis- und Schichtgeräte angeschlossen sind, für die der Benutzer entsprechende Portzugriffsberechtigungen erhalten hat.

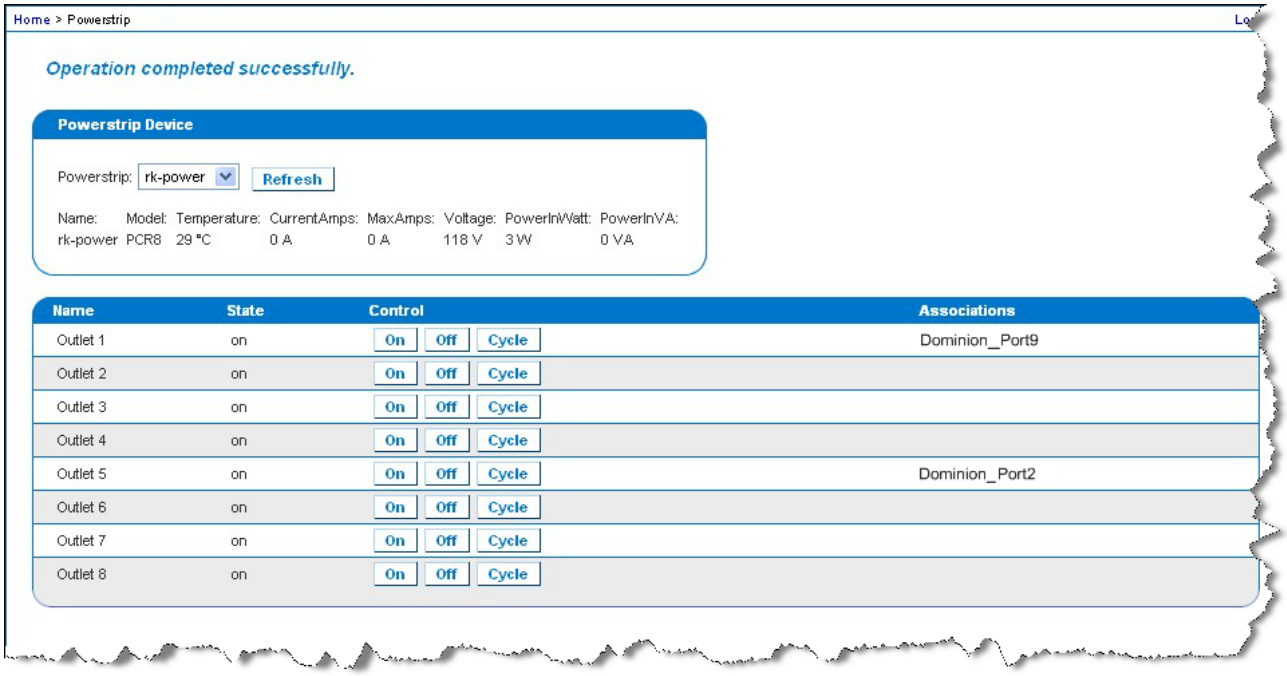
*Hinweis: Informationen zum Einrichten eines PX finden Sie im Benutzerhandbuch für **Raritan PX**.*

Auf der Seite "Powerstrip" können Sie die Ausgänge einschalten und ausschalten sowie aus- und wieder einschalten. Sie können außerdem die folgenden Informationen zu Powerstrip und Ausgang anzeigen:

- Powerstrip-Geräteinformationen:
  - Name
  - Modell
  - Temperatur
  - Current Amps (Aktuelle Stromstärke)
  - Maximum Amps (Maximale Stromstärke)
  - Voltage (Spannung)

  - Power in Watts (Strom in Watt)
  - Power in Volts Ampere (Strom in Voltampere)
- Ausgangsanzeigeinformationen:
  - Name – Der Name, der dem Ausgang bei der Konfiguration zugeordnet wurde.
  - State (Status) – Status des Ausgangs (Ein/Aus)
  - Control (Steuerung) – Ausgänge einschalten und ausschalten sowie aus- und wieder einschalten
  - Association (Zuordnung) – Die dem Ausgang zugeordneten Ports

Wenn Sie die Seite "Powerstrip" öffnen, werden die Powerstrips, die zurzeit mit KX III verbunden sind, zunächst in der Dropdown-Liste "Powerstrip" angezeigt. Außerdem werden Informationen zum aktuell ausgewählten Powerstrip angezeigt. Wenn keine Powerstrips mit KX III verbunden sind, wird die Meldung "No powerstrips found" (Keine Powerstrips gefunden) im Abschnitt "Powerstrip Device" (Powerstrip-Gerät) der Seite angezeigt.



Einschalten und Ausschalten sowie Ein- und Ausschalten von Ausgängen

So schalten Sie einen Ausgang ein:

1. Klicken Sie auf das Menü "Power" (Strom), um die Seite "Powerstrip" zu öffnen.

2. Wählen Sie aus der Dropdown-Liste "Powerstrip" die PX-Gestell-PDU (Powerstrip) aus, die Sie einschalten möchten.
3. Klicken Sie auf "Refresh" (Aktualisieren), um die Stromzufuhrsteuerung anzuzeigen.
4. Klicken Sie auf den Ausgang (Outlet), den Sie einschalten möchten.
5. Klicken Sie auf OK, um das Bestätigungsdialogfeld "Power On" (Strom ein) zu schließen. Der Ausgang schaltet sich ein und der Status wird als "On" (Ein) angezeigt.

So schalten Sie einen Ausgang aus:

1. Klicken Sie auf Off (Aus) - neben dem Outlet - den Sie einschalten möchten.
2. Klicken Sie im Dialogfeld "Power Off" (Strom aus) auf OK.
3. Klicken Sie im Bestätigungsdialogfeld "Power Off" (Strom aus) auf OK. Der Ausgang schaltet sich aus und der Status wird als "Off" (Aus) angezeigt.

So schalten Sie einen Ausgang aus und wieder ein:

1. Klicken Sie auf Zyklus neben dem Ausgang, den Sie verwalten möchten. Das Dialogfeld "Power Cycle Port" (Port aus- und wieder einschalten) wird geöffnet.
2. Klicken Sie auf OK. Der Ausgang wird nun aus- und wieder eingeschaltet (dies kann einige Sekunden dauern).
3. Wenn der Vorgang abgeschlossen ist, öffnet sich ein Dialogfenster. Klicken Sie zum Schließen des Dialogfensters auf OK.

USB-Profile

Überblick

Um die Kompatibilität des KX III auf verschiedene KVM-Zielserver auszuweiten, bietet Raritan eine Standardauswahl an USB-Konfigurationsprofilen für die Implementierung auf vielen Betriebssystemen und Servern auf BIOS-Ebene an.

Das generische USB-Profil (Standard) erfüllt die Anforderungen der großen Mehrheit der bereitgestellten KVM-Zielserverkonfigurationen.

Weitere Profile stehen zur Verfügung, um die speziellen Anforderungen anderer häufig bereitgestellten Serverkonfigurationen (z. B. Linux® und Mac OS X®) zu erfüllen.

Außerdem stehen einige Profile (festgelegt nach Plattformname und BIOS-Revision) zur Verfügung, um die Kompatibilität der Funktion der virtuellen Medien mit dem Zielserver zu verbessern (wenn z. B. auf BIOS-Ebene gearbeitet wird).

USB-Profile werden unter "Device Settings“ "Port Configuration" "Port" (Geräteeinstellungen > Portkonfiguration > Port) auf den lokalen und Remotekonsolen des KX III konfiguriert.

Ein Geräteadministrator kann den Port mit den Profilen konfigurieren, die den Anforderungen des Benutzers und der Zielserverkonfiguration am besten entsprechen.

Ein Benutzer, der eine Verbindung mit einem KVM-Zielserver herstellt, kann unter diesen vordefinierten Profilen im Virtual KVM Client wählen, je nach Betriebsstatus des KVM-Zielservers.

Wenn beispielsweise der Server ausgeführt wird und der Benutzer das Windows®-Betriebssystem verwenden möchte, ist es sinnvoll, das generische Profil zu verwenden.

Wenn der Benutzer jedoch die Einstellungen im BIOS-Menü ändern oder von einem virtuellen Medienlaufwerk einen Neustart ausführen möchte, kann, je nach Zielservermodell, ein BIOS-Profil eher geeignet sein.

Sollte keines der von Raritan bereitgestellten Standard-USB-Profile mit dem betreffenden KVM-Zielgerät funktionieren, wenden Sie sich an den technischen Kundendienst von Raritan.

CIM-Kompatibilität

Um USB-Profile nutzen zu können, müssen Sie einen Virtuellen Medien CIM mit aktualisierter Firmware verwenden. Für eine Liste von virtuellen Medien CIM, siehe ***Unterstützt Computer Schnittstellen module (CIMs) Technische Daten*** (siehe "***Spezifikationen der unterstützten Computer Interface Modules (CIMs)***" auf Seite 349).

Verfügbare USB-Profile

Die aktuelle Version des KX III verfügt über eine Auswahl an USB-Profilen, die in der folgenden Tabelle beschrieben werden. Neue Profile sind in jeder von Raritan zur Verfügung gestellten Firmwareaktualisierung enthalten. Wenn neue Profile hinzugefügt werden, werden diese in der Hilfe dokumentiert.

USB-Profil	Beschreibung
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200-BIOS Verwenden Sie entweder dieses oder das generische Profil für das Dell PowerEdge 1950/2950/2970/6950/R200-BIOS. Einschränkungen: ▪ Keine
BIOS Dell OptiPlex ™ Nur Tastatur und Maus	Dell OptiPlex BIOS Zugriff (Nur Tastatur und Maus) Verwenden Sie dieses Profil, um Tastaturfunktionalität für das Dell OptiPlex-BIOS zu erhalten, wenn D2CIM-VUSB verwendet wird. Verwenden Sie bei Nutzung des neuen D2CIM-DVUSB das generische Profil. Hinweis: ▪ Optiplex 210L/280/745/GX620 benötigt das D2CIM-DVUSB mit generischem Profil, um virtuelle Medien zu unterstützen. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Keine Unterstützung für virtuelle Medien
BIOS Dell Optiplex 790	Verwenden Sie dieses Profil für Dell Optiplex 790 während BIOS-Vorgängen. Warnhinweis: ▪ Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.

USB-Profil	Beschreibung
	Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Absolute Mouse Synchronization (Absolute Maussynchronisierung) nicht unterstützt ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS Dell Optiplex 790 Nur Tastatur	Verwenden Sie dieses Profil für Dell Optiplex 790, wenn Sie Tastaturmakros während BIOS-Vorgängen verwenden. Nur die Tastatur ist mit diesem Profil aktiviert. Einschränkungen: ▪ Maus ist deaktiviert. ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke sind deaktiviert.
BIOS DellPowerEdge Nur Tastatur und Maus	Dell PowerEdge BIOS Zugriff (Nur Tastatur und Maus) Verwenden Sie dieses Profil, um Tastaturfunktionalität für das Dell PowerEdge-BIOS zu erhalten, wenn das D2CIM-VUSB verwendet wird. Verwenden Sie bei Nutzung des neuen D2CIM-DVUSB das generische Profil. Hinweis: ▪ PowerEdge 650/1650/1750/2600/2650 BIOS unterstützen keine USB-, CD-ROM-Laufwerke und Festplatten als startbares Gerät. ▪ PowerEdge 750/850/860/1850/2850/SC1425-BIOS benötigt das D2CIM-DVUSB mit generischem Profil, um virtuelle Medien zu unterstützen. ▪ Verwenden Sie das Profil "BIOS Dell PowerEdge 1950/2950/2970/6950/R200" oder das generische Profil für PowerEdge 1950/2950/2970/6950/R200, wenn im BIOS gearbeitet wird. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt ▪ Keine Unterstützung für virtuelle Medien
BIOS ASUS P4C800-Hauptplatine	Verwenden Sie dieses Profil, um auf das BIOS zuzugreifen und über "Virtual Media" (Virtuelle Medien) auf Asus P4C800-basierten Systemen zu starten. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle

USB-Profil	Beschreibung
	Geschwindigkeit (12 Mbit/s) ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS Generic	BIOS Generic Verwenden Sie dieses Profil, wenn das generische Profil des Betriebssystems auf dem BIOS nicht funktioniert. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Verwenden Sie dieses Profil für HP Proliant DL145 PhoenixBIOS während der Installation des Betriebssystems. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Verwenden Sie dieses Profil zum Hochfahren von Desktops der Serie "HP Compaq DC7100/DC7600" über virtuelle Medien. Einschränkungen: ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS Verwenden Sie dieses Profil für die IBM® Thinkcentre Lenovo-Hauptplatine (Modell 828841U) bei BIOS-Vorgängen. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
IBM BladeCenter H mit Advanced Management	Verwenden Sie dieses Profil, um die virtuellen Medien zu aktivieren, wenn D2CIM-VUSB oder D2CIM-DVUSB an das

USB-Profil	Beschreibung
Module	Advanced Management Module angeschlossen sind. Einschränkungen: ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 und X61 (Hochfahren über virtuelle Medien) Verwenden Sie dieses Profil zum Hochfahren von Laptops der Serie T61 und X61 über virtuelle Medien. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Generisch	Das generische USB-Profil entspricht in etwa dem Verhalten der ursprünglichen KX3 Version. Verwenden Sie dies für die Betriebssysteme Windows 2000®, Windows XP®, Windows Vista® und höher. Einschränkungen: ▪ Keine
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Verwenden Sie dieses Profil für den Server der Serie "HP Proliant DL360/DL380 G4" bei der Installation des Betriebssystems unter Verwendung der HP SmartStart CD. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) wird nicht unterstützt
HP Proliant DL360/DL380 G4 (Windows 2003® Server-Installation)	HP Proliant DL360/DL380 G4 (Windows 2003 Server-Installation) Verwenden Sie dieses Profil für den Server der Serie "HP Proliant DL360/DL380 G4" bei der Installation von Windows 2003 Server ohne Verwendung der HP SmartStart CD. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Linux®	Generisches Linux-Profil Dies ist das generische Linux-Profil. Verwenden Sie es für Redhat Enterprise Linux, SuSE Linux Enterprise Desktop und ähnliche Distributionen. Einschränkungen: ▪ Absolute Mouse Synchronization™ (Absolute

USB-Profil	Beschreibung
	Maussynchronisierung) wird nicht unterstützt
BIOS Mac®	BIOS Mac Verwenden Sie dieses Profil für Mac-BIOS. Einschränkungen: ▪ Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) wird nicht unterstützt ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. Wenn Sie dieses USB Profil benutzen, sehen Sie Information über ***Mausmodi bei Verwendung des Mac Boot Menü*** (auf Seite 56)
MAC OS X® 10.4.9 (und höher)	Mac OS X Version 10.4.9 (und höher) Dieses Profil kompensiert die Skalierung von Mauskoordination, die in den neueren Versionen von Mac OS X eingeführt wurden. Wählen Sie dieses Profil aus, wenn die lokalen und Remote-Mauspositionen an den Desktop-Rändern nicht mehr synchronisiert sind. Einschränkungen: ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) Verwenden Sie dieses Profil für die Industriemainboards der Serie "RUBY-9715VG2A" mit Phoenix/AwardBIOS v6.00PG. Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS Verwenden Sie diese Profil für Hauptplatinen der Serie "Supermicro" mit Phoenix AwardBIOS. Einschränkungen: ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
Suse 9.2	SuSE Linux 9.2 Verwenden Sie dieses Profil für die SuSE Linux 9.2-Distribution. Einschränkungen: ▪ Absolute Mouse Synchronization™ (Absolute

USB-Profil	Beschreibung
	Maussynchronisierung) wird nicht unterstützt ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Troubleshooting 1	Fehlerbehebungsprofil 1 ▪ Massenspeicher vorrangig ▪ Tastatur und Maus (Typ 1) ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.
Fehlerbehebung 2	Fehlerbehebungsprofil 2 ▪ Tastatur und Maus (Typ 2) vorrangig ▪ Massenspeicher ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.
Fehlerbehebung 3	Fehlerbehebungsprofil 3 ▪ Massenspeicher vorrangig ▪ Tastatur und Maus (Typ 2) ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) ▪ Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.
Use Full Speed for Virtual Media CIM (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden)	Use Full Speed for Virtual Media CIM (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) Dieses Profil entspricht in etwa dem Verhalten der ursprünglichen KX3 Version, wenn die Option "Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM) aktiviert ist. Hilfreich bei einem BIOS, das nicht mit Hochgeschwindigkeits-USB-Geräten funktioniert.

USB-Profil	Beschreibung
	Einschränkungen: ▪ USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Use Full Speed for Keyboard and Mouse USB (Volle Geschwindigkeit für Tastatur- und Maus-USB)	Dieses Profil aktiviert die volle Geschwindigkeit der USB-Schnittstelle für Tastatur und Maus auf dem Dual-VM-CIM. Dieses Profil eignet sich für Geräte, die mit den Einstellungen für niedrige USB-Geschwindigkeiten nicht ordnungsgemäß funktionieren. Einschränkungen: ▪ USB-Bus-Geschwindigkeit auf volle Geschwindigkeit (12 MBit/s) für USB-Schnittstelle der Tastatur und Maus eingestellt

Mausmodi bei Verwendung des Mac Boot Menü

Bei der Arbeit mit USB-Profile und wenn Sie die Maus im Mac-Boot-Menü verwenden möchten, müssen Sie den Single Mausmodus verwenden, da der Absolute Mausmodus im BIOS nicht unterstützt ist.

So konfigurieren Sie die Maus für das Arbeiten im Menü "Boot":

1. Starten Sie Ihren Mac-Computer, und drücken Sie die Alt-Taste, um das Menü "Boot" zu öffnen. Zu diesem Zeitpunkt reagiert die Maus noch nicht.
2. Ein-Cursor-Modus Wählen Maus antwortet jetzt.

   Hinweis: Im Modus "Single Mouse" (Ein Cursor) ist die Geschwindigkeit des Mauszeigers möglicherweise gering.

3. Sobald Sie das Menü "Boot" verlassen haben und das Betriebssystem hochgefahren ist, beenden Sie den Modus "Single Mouse" (Ein Cursor), und schalten Sie zurück in den Mausmodus "Absolute Mouse" (Absolut), um eine bessere Leistung der Maus zu erhalten.

Auswählen von Profilen für einen KVM-Port

KX III enthält eine Reihe von USB-Profilen, die Sie einem KVM-Port zuweisen können, basierend auf den Eigenschaften des KVM-Zielservers, mit dem das Profil verbunden wird. Sie können USB-Profile unter "Device Settings" "Port Configuration" "Port" (Geräteeinstellungen > Portkonfiguration > Port) auf der lokalen oder der Remotekonsole des KX III einem KVM-Port zuweisen.

Der Administrator legt die Profile fest, die am wahrscheinlichsten für ein spezielles Zielgerät benötigt werden. Diese Profile stehen anschließend über Virtual KVM Client (VKC) zur Auswahl bereit. Wenn ein Profil nicht zur Verwendung freigegeben wurde, können sie auf alle verfügbaren Profile zugreifen, indem Sie "USB Profile" "Other Profiles" (USB-Profil > Weitere Profile) auswählen.

Durch die Zuordnung von USB-Profilen zu einem KVM-Port sind diese Profile für Benutzer, die mit einem KVM-Zielserver verbunden sind, verfügbar. Wenn erforderlich, kann der Benutzer ein USB-Profil aus dem USB-Profilmenü im Virtual KVM Client (VKC) auswählen.

Informationen zur Zuordnung von USB-Profilen zu einem KVM-Port finden Sie unter ***Konfigurieren von USB-Profilen (Seite "Port")*** (auf Seite 131).

User Management (Benutzerverwaltung)

Benutzergruppen

KX III speichert eine interne Liste aller Benutzer- und Gruppennamen, um die Zugriffsautorisierung und die Berechtigungen festzulegen. Diese Informationen werden intern in einem verschlüsselten Format gespeichert. Es gibt verschiedene Arten der Authentifizierung. Diese wird als lokale Authentifizierung bezeichnet. Alle Benutzer müssen authentifiziert werden. Wenn KX III für LDAP/LDAPS oder RADIUS konfiguriert wurde, wird erst deren entsprechende Authentifizierung durchgeführt und anschließend die lokale Authentifizierung.

Jedes KX III enthält standardmäßig drei Benutzergruppen. Diese Gruppen können nicht gelöscht werden:

Benutzer	Beschreibung
Admin	Benutzer dieser Gruppe verfügen über vollständige Administratorrechte. Der ursprüngliche werkseitige Standardbenutzer ist Mitglied dieser Gruppe und verfügt über sämtliche Systemrechte. Außerdem muss der Benutzer Admin der Gruppe Admin angehören.
Unbekannt	Dies ist die Standardgruppe für Benutzer, die extern über LDAP/LDAPS oder RADIUS authentifiziert werden oder die im System unbekannt sind. Wenn der

Benutzer	Beschreibung
	externe LDAP/LDAPS- oder RADIUS-Server keine gültige Benutzergruppe erkennt, wird die Gruppe Unknown (Unbekannt) verwendet. Außerdem wird jeder neu erstellte Benutzer automatisch in diese Gruppe aufgenommen, bis der Benutzer einer anderen Gruppe zugewiesen wird.
Individual Gruppe	Eine individuelle Gruppe ist im Prinzip eine aus einer Person bestehende „Gruppe“. Dies bedeutet, dass sich der Benutzer in seiner eigenen Gruppe befindet und nicht mit anderen echten Gruppen verknüpft ist. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen. In individuellen Gruppen können Benutzerkonten dieselben Rechte wie eine Gruppe aufweisen.

In ProductName können bis zu 254 Benutzergruppen erstellt werden. In KX III können bis zu 254 Benutzergruppen erstellt werden.

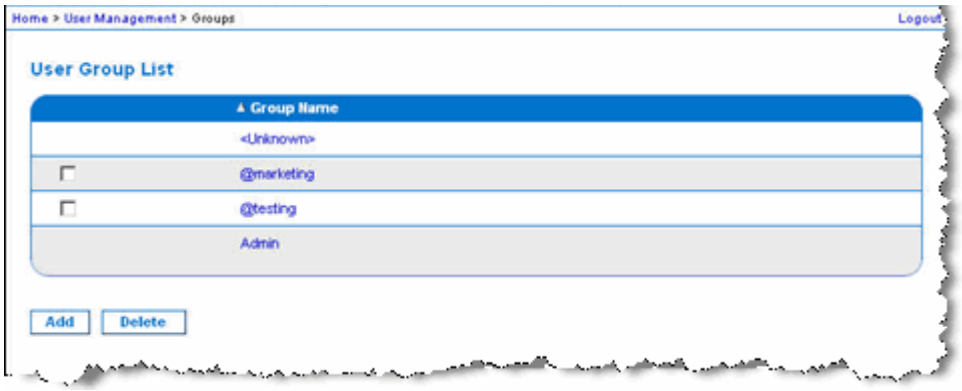
User Group List (Liste der Benutzergruppen)

Benutzergruppen werden bei der lokalen und der Remoteauthentifizierung (über RADIUS oder LDAP/LDAPS) verwendet. Es ist empfehlenswert, Benutzergruppen vor dem Erstellen einzelner Benutzer zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe hinzugefügt werden muss.

Die Seite "User Group List" (Liste der Benutzergruppen) enthält eine Liste aller Benutzergruppen, die in auf- oder absteigender Reihenfolge sortiert werden kann, indem Sie auf die Spaltenüberschrift "Group Name" (Gruppenname) klicken. Auf der Seite "User Group List" (Liste der Benutzergruppen) können Sie außerdem Benutzergruppen hinzufügen, ändern oder löschen.

So zeigen Sie eine Liste der Benutzergruppen an:

- Wählen Sie "User Management > User Group List" (Benutzerverwaltung > Liste der Benutzergruppen). Die Seite "User Group List" (Liste der Benutzergruppen) wird angezeigt.



Beziehung zwischen Benutzern und Gruppen

Benutzer sind Mitglied in einer Gruppe, und Gruppen verfügen über bestimmte Berechtigungen. Sie können Zeit sparen, indem Sie die verschiedenen Benutzer Ihrer KX III-Einheit in Gruppen organisieren. So können Sie die Berechtigungen aller Benutzer in einer Gruppe auf einmal verwalten anstatt für jeden Benutzer einzeln.

Sie können bei Bedarf auch darauf verzichten, bestimmte Benutzer Gruppen zuzuordnen. In diesem Fall können Sie den Benutzer als "Individuell" klassifizieren.

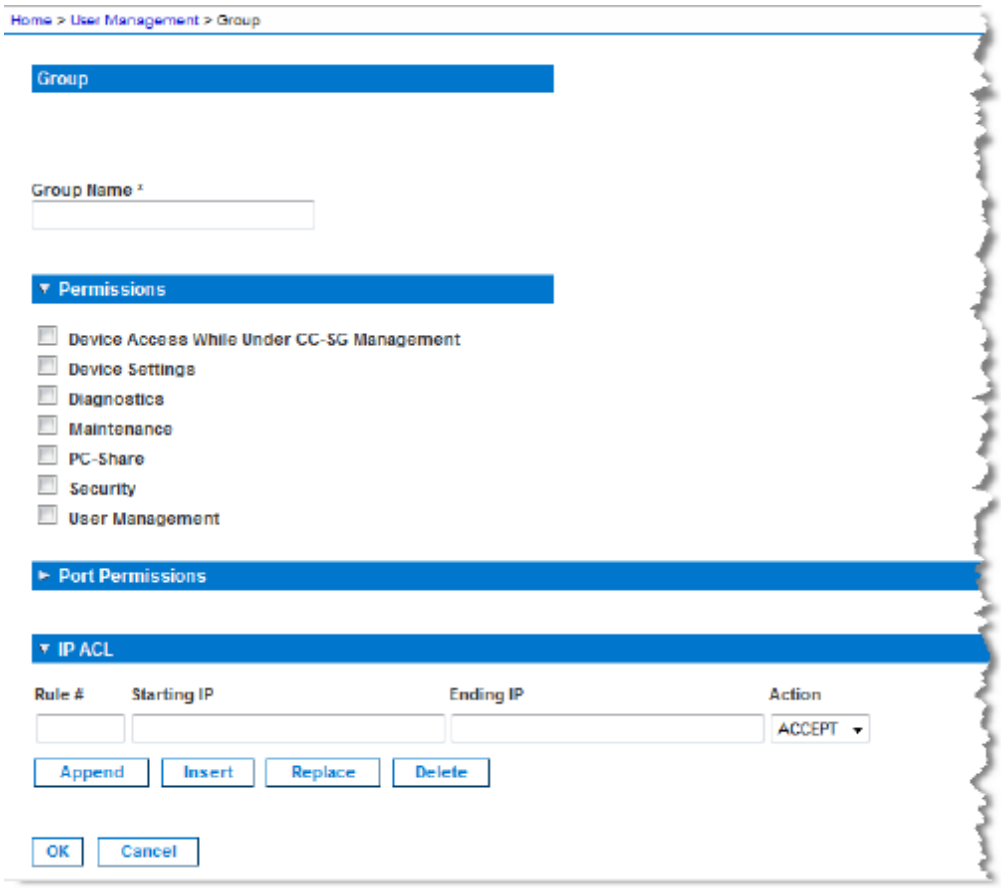
Nach der erfolgreichen Authentifizierung verwendet das Gerät Gruppeninformationen, um die Berechtigungen des Benutzers zu bestimmen, z. B. die Zugriffsberechtigungen für verschiedene Server-Ports, ob ein Neustart des Geräts zulässig ist und weitere Funktionen.

Hinzufügen einer neuen Benutzergruppe

So fügen Sie eine neue Benutzergruppe hinzu:

1. Wählen Sie "User Management > Add New User Group" (Benutzerverwaltung > Neue Benutzergruppe hinzufügen) oder klicken Sie auf der Seite "User Group List" (Liste der Benutzergruppen) auf die Schaltfläche "Add" (Hinzufügen).
2. Geben Sie im Feld "Group Name" (Gruppenname) einen aussagekräftigen Namen für die neue Benutzergruppe ein (bis zu 64 Zeichen).
3. Aktivieren Sie die Kontrollkästchen neben den Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. See Festlegen von Berechtigungen
4. Legen Sie für jeden Benutzer in dieser Gruppe die Server-Ports und den Zugriffstyp fest. Siehe ***Festlegen von Port-Berechtigungen*** (auf Seite 63)
5. Legen Sie die IP-ACL fest. Diese Funktion beschränkt den Zugriff auf das KX III Gerät, indem Sie IP-Adressen angeben. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für alle Zugriffsversuche auf das Gerät gilt und Priorität hat. Siehe ***Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)*** (auf Seite 64). **Optional**

6. Klicken Sie auf OK.



Festlegen von Berechtigungen

Berechtigung	Beschreibung
Gerätezugriff unter CC-SG-Verwaltung	Ermöglicht Benutzern und Benutzergruppen mit dieser Berechtigung den direkten Zugriff auf KX III unter Verwendung einer IP-Adresse, wenn die Option "Lokal Access" (Lokaler Zugriff) für das Gerät in CC-SG aktiviert ist. Es kann von der lokalen und der Remotekonsole aus sowie vom zugegriffen werden. Wird unter CC-SG-Verwaltung direkt auf ein Gerät zugegriffen, werden Zugriff und Verbindungsaktivitäten auf KX III protokolliert. Die Benutzerauthentifizierung erfolgt gemäß den KX III Authentifizierungseinstellungen. *Hinweis: Die Benutzer der Gruppe "Admin" verfügen standardmäßig über diese*

Berechtigung	Beschreibung
	Berechtigung.
Geräteeinstellungen	Netzwerkeinstellungen, Einstellungen für Datum und Uhrzeit, Portkonfiguration (Kanalnamen, Stromzuordnungen), Ereignisverwaltung (SNMP, Syslog), Dateiserver-Setups für virtuelle Medien
Diagnose	Status der Netzwerkschnittstelle, Netzwerkstatistik, Ping an den Host, Verfolgen der Route zum Host, KX III Diagnose
Wartung	Sichern und Wiederherstellen von Datenbanken, Firmware-Aktualisierung, Wiederherstellen der Standardeinstellungen, Neustart.
PC-Share (PC-Freigabe)	Gleichzeitiger Zugriff auf ein Zielgerät durch mehrere Benutzer. Wenn Sie eine Schichtkonfiguration verwenden, in der ein KX III Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen alle Geräte dieselben PC-Freigabeeinstellung verwenden. Weitere Informationen zu Schichten finden Sie unter Konfigurieren und Aktivieren von Schichten.
Sicherheit	SSL-Zertifikat, Sicherheitseinstellungen (VM-Freigabe, PC-Freigabe), IP-ACL.
User Management (Benutzerverwaltung)	Benutzer- und Gruppenverwaltung, Remoteauthentifizierung (LDAP/LDAPS/RADIUS), Anmeldeeinstellungen. Wenn Sie eine Schichtkonfiguration verwenden, in der ein KX III Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen auf allen Geräten dieselben Einstellungen für Benutzer, Benutzergruppe und Remote-Authentifizierung verwendet werden. Weitere Informationen zu Schichten finden Sie unter Konfigurieren und Aktivieren von Schichten.

Festlegen von Port-Berechtigungen

Sie können für jeden Serverport den Zugriffstyp der Gruppe sowie den Portzugriffstyp auf virtuelle Medien und die Stromzufuhrsteuerung festlegen. Die Standardeinstellung für alle Berechtigungen ist "Deny" (Ablehnen).

Portzugriff	
Option	**Beschreibung**
Deny (Ablehnen)	Zugriff vollständig verweigert
View (Anzeigen)	Anzeigen des Videobildes, aber keine Interaktion mit dem angeschlossenen Zielserver
Control (Steuern)	Steuerung des angeschlossenen Zielservers Die Option "Control" (Steuern) muss der Gruppe zugeordnet sein, wenn der Zugriff auf virtuelle Medien und Stromzufuhrsteuerung ebenso gewährt wird. Damit alle Benutzer in einer Benutzergruppe hinzugefügte KVM-Switches erkennen können, muss jedem Benutzer Steuerzugriff gewährt werden. Benutzer ohne diese Berechtigung können einen KVM-Switch, der später hinzugefügt wird, nicht anzeigen. Der Steuerzugriff muss für Audio- oder Smart Card-Steuerelemente gewährt werden, damit er aktiv ist.

VM-Zugriff	
Option	**Beschreibung**
Ablehnen	Berechtigung für virtuelle Medien wird für diesen Port vollständig verweigert
Read-Only (Lese-zugriff)	Zugriff auf virtuelle Medien ist auf das Lesen beschränkt
Lese/Schreibzugriff	Vollständiger Zugriff (Lesen und Schreiben) auf virtuelle Medien

VM-Zugriff Zugriff auf Stromzufuhrsteuerung	
Option	**Beschreibung**
Deny (Ablehnen)	Keine Berechtigung für die Stromzufuhrsteuerung auf dem Zielserver
Access (Zugriff)	Volle Berechtigung für die Stromzufuhrsteuerung auf einem Zielserver

Bei Blade-Chassis wird über die Zugriffsberechtigungen auf den Port der Zugriff auf die URLs, die für dieses Blade-Chassis konfiguriert wurden, gesteuert. Die verfügbaren Optionen lauten "Deny" (Ablehnen) oder "Control" (Steuern). Außerdem besitzt jedes Blade im Chassis eine eigene unabhängige Port-Berechtigungseinstellung.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein KX III-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, erzwingt das Schichtgerät individuelle Portsteuerungsebenen. Weitere Informationen zu Schichten finden Sie unter Konfigurieren und Aktivieren von Schichten.

Festlegen von Berechtigungen für eine individuelle Gruppe

So legen Sie Berechtigungen für eine individuelle Benutzergruppe fest:

1. Wählen Sie die gewünschte Gruppe aus der Liste der Gruppen aus. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen.
2. Klicken Sie auf den Gruppennamen. Die Seite "Group" (Gruppe) wird angezeigt.
3. Wählen Sie die gewünschten Berechtigungen aus.
4. Klicken Sie auf "OK".

Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)

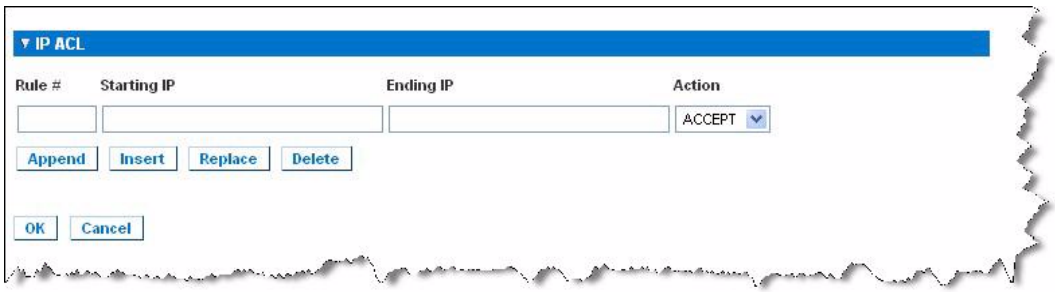
Wichtig: Gehen Sie bei der Verwendung der gruppenbasierten IP-Zugriffssteuerung bedachtsam vor. Der Zugriff auf KX III kann Ihnen verweigert werden, wenn sich Ihre IP-Adresse in einem Bereich befindet, der keine Zugriffsberechtigung hat.

Mit diesem Feature beschränken Sie den Zugriff auf das KX III-Gerät durch Benutzer in der ausgewählten Gruppe auf bestimmte IP-Adressen. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für alle Zugriffsversuche auf das Gerät gilt, zuerst verarbeitet wird und Priorität hat.

Wichtig: Die IP-Adresse 127.0.0.1 wird vom lokalen KX III-Port

verwendet und kann nicht gesperrt werden.

Verwenden Sie den Abschnitt "IP ACL" (IP-ACL) auf der Seite "Group" (Gruppe), um Regeln für die IP-Zugriffssteuerung auf Gruppenebene hinzuzufügen, einzufügen, zu ersetzen und zu löschen.



So fügen Sie Regeln hinzu:

1. Geben Sie im Feld "Starting IP" (IP-Startadresse) die IP-Startadresse ein.
2. Geben Sie im Feld "Ending IP" (IP-Endadresse) die IP-Endadresse ein.
3. Wählen Sie unter "Action" (Aktion) eine der folgenden Optionen:
   - Accept (Akzeptieren) – Diese IP-Adressen können auf das KX III-Gerät zugreifen.
   - Drop (Ablehnen) – Diesen IP-Adressen wird der Zugriff auf das KX III-Gerät verweigert.
4. Klicken Sie auf "Append" (Anfügen). Die Regel wird unten in der Liste hinzugefügt. Wiederholen Sie die Schritte 1 bis 4, um weitere Regeln hinzuzufügen.

So fügen Sie eine Regel ein:

1. Geben Sie eine Regelnummer ein (#). Diese ist für den Befehl "Insert" (Einfügen) erforderlich.
2. Geben Sie Werte in die Felder "Starting IP" (IP-Startadresse) und "Ending IP" (IP-Endadresse) ein.
3. Wählen Sie in der Dropdownliste "Action" (Aktion) eine Option aus.
4. Klicken Sie auf "Insert" (Einfügen). Wenn die eingegebene Regelnummer einer bereits vorhandenen entspricht, wird die neue Regel vor der vorhandenen Regel eingefügt, und alle Regeln werden um eine Position nach unten verschoben.

So ersetzen Sie eine Regel:

1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie Werte in die Felder "Starting IP" (IP-Startadresse) und "Ending IP" (IP-Endadresse) ein.

3. Wählen Sie in der Dropdownliste "Action" (Aktion) eine Option aus.
4. Klicken Sie auf "Replace" (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

So löschen Sie eine Regel:

1. Geben Sie die zu löschende Regelnummer an.
2. Klicken Sie auf "Delete" (Löschen).
3. Klicken Sie zum Bestätigen des Löschvorgangs auf OK.

Wichtig: ACL-Regeln werden in der Reihenfolge ausgewertet, in der sie aufgeführt sind. Werden die beiden ACL-Regeln in diesem Beispiel vertauscht, akzeptiert Dominion z. B. gar keine Kommunikation.

Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP

Tipp: Mithilfe der Regelnummern können Sie die Reihenfolge, in der die Regeln erstellt werden, besser steuern.

Ändern einer vorhandenen Benutzergruppe

Hinweis: Für die Gruppe Admin sind alle Berechtigungen aktiviert (dies kann nicht geändert werden).

So ändern Sie eine vorhandene Benutzergruppe:

1. Bearbeiten Sie auf der Seite Group (Gruppe) die entsprechenden Felder, und legen Sie die gewünschten Berechtigungen fest.
2. Legen Sie unter "Permissions" (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe Festlegen von Berechtigungen.
3. Legen Sie unter Port Permissions (Portberechtigungen) die Portberechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Server-Ports fest, und geben Sie die Zugriffsart an. Siehe ***Festlegen von Portberechtigungen*** (siehe "***Festlegen von Port-Berechtigungen***" auf Seite 63).
4. Legen Sie die IP-ACL fest (optional). Mit diesem Feature beschränken Sie den Zugriff auf das KX III-Gerät, indem Sie IP-Adressen angeben. Siehe ***Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)*** (auf Seite 64).
5. Klicken Sie auf "OK".

So löschen Sie eine Benutzergruppe:

Wichtig: Wenn Sie eine Gruppe mit Benutzern löschen, werden die Benutzer automatisch der Benutzergruppe <unknown> (unbekannt) zugewiesen.

Tipp: Um herauszufinden, welche Benutzer einer bestimmten Gruppe angehören, sortieren Sie die Benutzerliste nach Benutzergruppe.

1. Wählen Sie eine Gruppe aus der Liste aus, indem Sie das Kontrollkästchen links vom Gruppennamen aktivieren.
2. Klicken Sie auf Löschen.
3. Klicken Sie zum Bestätigen des Löschvorgangs auf OK.

Benutzer

Benutzern müssen Benutzernamen und Kennwörter zugeordnet werden, damit sie auf KX III zugreifen können. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf KX III zuzugreifen.

Für jede Benutzergruppe können bis zu 254 Benutzer erstellt werden.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein KX III-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, Benutzer benötigen die Zugriffsberechtigung für das Basisgerät sowie auf das individuelle Schichtgerät (bei Bedarf).

Wenn sich Benutzer am Basisgerät anmelden, wird jedes Schichtgerät abgefragt und der Benutzer kann auf jeden Zielserver zugreifen, für den er Berechtigungen aufweist. Weitere Informationen zu Schichten finden Sie unter Konfigurieren und Aktivieren von Schichten.

Hinzufügen eines neuen Benutzers

Es ist empfehlenswert, Benutzergruppen vor dem Erstellen von KX III-Benutzern zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe zugewiesen werden muss. Siehe **Hinzufügen einer neuen Benutzergruppe**.

Auf der Seite "User" (Benutzer) können Sie neue Benutzer hinzufügen, Benutzerinformationen ändern und deaktivierte Benutzer erneut aktivieren.

Hinweis: Ein Benutzername kann deaktiviert werden, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche die auf der Seite "Security Settings" (Sicherheitseinstellungen) festgelegte maximale Anzahl der Anmeldeversuche überschritten hat. Siehe **Sicherheitseinstellungen** *(siehe "***Security Settings (Sicherheitseinstellungen)***" auf Seite 175).*

So fügen Sie einen neuen Benutzer hinzu:

1. Wählen Sie User Management > Add New User (Benutzerverwaltung > Neuen Benutzer hinzufügen) auf der Benutzerlistenseite.
2. Geben Sie im Feld "Username" (Benutzername) einen eindeutigen Namen ein (bis zu 16 Zeichen).
3. Geben Sie im Feld "Full Name" (Vollständiger Name) den vollständigen Namen des Benutzers ein (bis zu 64 Zeichen).
4. Geben Sie im Feld "Password" (Kennwort) ein Kennwort ein, und anschließend im Feld "Confirm Password" (Kennwort bestätigen) erneut (bis zu 64 Zeichen).
5. Wählen Sie in der Dropdownliste User Group (Benutzergruppe) die Gruppe aus.

   Wenn Sie diesen Benutzer keiner vorhandenen Benutzergruppe zuordnen möchten, wählen Sie in der Dropdownliste die Option "Individual Group" (Individuelle Gruppe) aus. Weitere Informationen zu den Berechtigungen einer individuellen Gruppe finden Sie unter ***Festlegen von Berechtigungen für eine individuelle Gruppe*** (auf Seite 64).
6. Lassen Sie das Kontrollkästchen "Active" (Aktiv) aktiviert, um den neuen Benutzer zu aktivieren. Klicken Sie auf "OK".

Anzeigen der KX III Benutzerliste

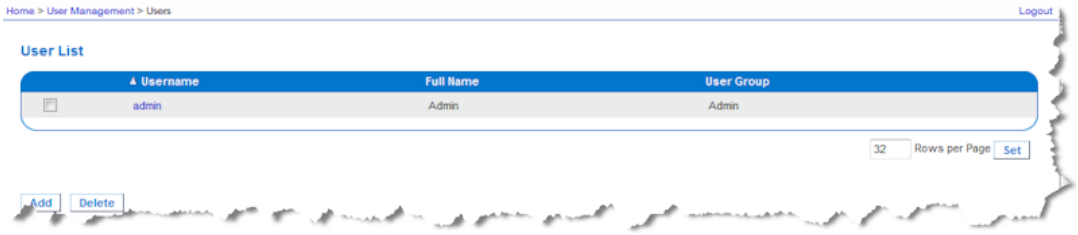
Die Seite User List (Benutzerliste) enthält eine Liste aller Benutzer einschließlich des Benutzernamens, des vollständigen Namens und der Benutzergruppe. Klicken Sie auf einen Spaltennamen, um die Liste nach einer der Spalten zu sortieren. Auf der Seite "User List" (Benutzerliste) können Sie Benutzer hinzufügen, ändern oder löschen.

KX III Benutzer mit Berechtigungen für die Benutzerverwaltung können bei Bedarf Benutzer von den Ports trennen oder Benutzer abmelden (Abmelden erzwingen). Siehe ***Trennen der Benutzer von Ports bzw.*** (siehe "***Trennen der Benutzer von Ports***" auf Seite ***70)Abmelden der Benutzer bei KX III (Erzwungene Abmeldung)***. (siehe "Abmelden der Benutzer bei KX III (Erzwungene Abmeldung)" auf Seite 71)

Informationen zum Anzeigen der Zielports, mit denen jeder Benutzer verbunden ist, finden Sie unter ***Anzeigen der Benutzer nach Port*** (auf Seite 70).

So zeigen Sie die Benutzerliste an:

- Wählen Sie "User Management User List" (Benutzerverwaltung Benutzerliste). Die Seite "User List" (Benutzerliste) wird angezeigt.



Anzeigen der Benutzer nach Port

Die Seite "User By Ports" (Benutzer nach Ports) enthält alle authentifizierten lokalen und Remote-Benutzer sowie die Ports, mit denen die Benutzer verbunden sind. Es werden nur permanente Verbindungen zu Ports aufgeführt. Ports, auf die beim Scannen nach Ports zugegriffen wird, werden nicht aufgeführt.

Wenn derselbe Benutzer über mehrere Clients angemeldet ist, wird dessen Benutzername für jede hergestellte Verbindung angezeigt. Wenn sich ein Benutzer z. B. über zwei (2) verschiedene Clients angemeldet hat, wird dessen Name zweimal aufgeführt.

Diese Seite enthält die folgenden Benutzer- und Portinformationen:

- Port Number (Portnummer) – Nummer des Ports, mit dem der Benutzer verbunden ist
- Port Name (Portname) – Name des Ports, mit dem der Benutzer verbunden ist

  Hinweis: Wenn ein Benutzer nicht mit einem Ziel verbunden ist, wird "Local Console" (Lokale Konsole) oder "Remote Console" (Remotekonsole) unter dem Portnamen angezeigt.

- Username (Benutzername) – Benutzername für Benutzeranmeldungen und Zielverbindungen
- Zugriff Von – IP-Adresse von Client PC auf den KX III zugreifen
- Status – aktueller aktiver oder inaktiver Status der Verbindung

So zeigen Sie die Benutzer nach Port an:

- Wählen Sie "User Management User by Port" (Benutzerverwaltung > Benutzer nach Port). Die Seite "Users by Port" (Benutzer nach Port) wird angezeigt.

Trennen der Benutzer von Ports

Wenn Benutzer getrennt werden, werden sie vom Zielport getrennt, ohne dass sie bei KX III abgemeldet werden.

Hinweis: Beim Abmelden der Benutzer werden sie vom Zielport getrennt und bei KX III abgemeldet. Weitere Informationen zur erzwungenen Abmeldung von Benutzern finden Sie unter **Abmelden der Benutzer bei KX III (Erzwungene Abmeldung)** *(auf Seite 71).*

So trennen Sie Benutzer vom Port:

1. Wählen Sie "User Management > Users by Port" (Benutzerverwaltung > Benutzer nach Port). Die Seite "Users by Port" (Benutzer nach Port) wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen der Person, die Sie vom Ziel trennen möchten.
3. Klicken Sie auf "Disconnect User from Port" (Benutzer von Port trennen).
4. Klicken Sie in der Bestätigungsmeldung auf "OK", um den Benutzer zu trennen.
5. Eine Bestätigungsmeldung über die erfolgreiche Trennung des Benutzers wird angezeigt.

Abmelden der Benutzer bei KX III (Erzwungene Abmeldung)

Wenn Sie Administrator sind, können Sie alle lokal authentifizierte Benutzer, die auf KX III angemeldet sind, abmelden. Benutzer können auch auf Portebene getrennt werden. Siehe ***Trennen der Benutzer von Ports*** (auf Seite 70).

So melden Sie einen Benutzer bei KX III ab:

1. Wählen Sie "User Management > Users by Port" (Benutzerverwaltung > Benutzer nach Port). Die Seite "Users by Port" (Benutzer nach Port) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen der Person, die Sie vom Ziel trennen möchten.
3. Klicken Sie auf "Force User Logoff" (Benutzerabmeldung erzwingen).
4. Klicken Sie in der Bestätigungsmeldung "Logoff User" (Benutzer abmelden) auf "OK".

Ändern eines vorhandenen Benutzers

So ändern Sie einen vorhandenen Benutzer:

1. Öffnen Sie die Seite "User List" (Benutzerliste) unter "User Management" > "User List" (Benutzerverwaltung > Benutzerliste).
2. Wählen Sie den Benutzer aus der Liste auf der Seite "User List" (Benutzerliste) aus.
3. Klicken Sie auf den Benutzernamen. Die Seite "User" (Benutzer) wird angezeigt.
4. Bearbeiten Sie auf der Seite "User" (Benutzer) die entsprechenden Felder. Informationen zum Zugriff auf die Seite "User" (Benutzer) finden Sie unter ***Hinzufügen eines neuen Benutzers*** (auf Seite 68).
5. Klicken Sie auf "Delete" (Löschen), um einen Benutzer zu löschen. Sie werden aufgefordert, den Löschvorgang zu bestätigen.
6. Klicken Sie auf OK.

Authentication Settings (Authentifizierungseinstellungen)

Bei der Authentifizierung geht es darum, die Identität des Benutzers zu überprüfen. Nach der Authentifizierung dient die Benutzergruppe dazu, die jeweiligen System- und Port-Berechtigungen zu ermitteln. Die dem Benutzer zugewiesenen Berechtigungen legen fest, welche Art des Zugriffs zulässig ist. Dies nennt man Autorisierung.

Wenn KX III zur Remote-Authentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein KX III-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen das Basisgerät und die Schichtgeräte dieselben Authentifizierungseinstellungen verwenden.

Auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) können Sie die Art der Authentifizierung für den Zugriff auf KX III konfigurieren.

Hinweis: Wird der Benutzer bei aktivierter Remoteauthentifizierung (LDAP/LDAPS oder RADIUS) nicht gefunden, wird zusätzlich die Authentifizierungsdatenbank geprüft.

So konfigurieren Sie die Authentifizierung:

1. Wählen Sie "User Management > Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen). Die Seite "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie die Option für das gewünschte Authentifizierungsprotokoll aus. Zur Verfügung stehen "Local Authentication" (Lokale Authentifizierung), "LDAP/LDAPS" oder "RADIUS". Bei Auswahl der Option "LDAP" werden die restlichen LDAP-Felder aktiviert, bei Auswahl der Option "RADIUS" die restlichen RADIUS-Felder.
3. Wenn Sie "Local Authentication" (Lokale Authentifizierung) auswählen, fahren Sie mit Schritt 6 fort.
4. Wenn Sie sich für "LDAP/LDAPS" entscheiden, lesen Sie den Abschnitt Implementierung der LDAP-Remoteauthentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Abschnitt "LDAP" der Seite "Authentication Settings" (Authentifizierungseinstellungen).
5. Wenn Sie sich für "RADIUS" entscheiden, lesen Sie den Abschnitt Implementierung der RADIUS-Remote-Authentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Bereich "RADIUS" der Seite "Authentication Settings" (Authentifizierungseinstellungen).
6. Klicken Sie zum Speichern auf "OK".

So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Implementierung der LDAP/LDAPS-Remoteauthentifizierung

Lightweight Directory Access Protocol (LDAP/LDAPS) ist ein Netzwerkprotokoll für die Abfrage und Änderung von Verzeichnisdiensten, die über TCP/IP ausgeführt werden. Ein Client startet eine LDAP-Sitzung, indem er eine Verbindung mit einem LDAP/LDAPS-Server herstellt (Standard-TCP-Port: 389). Anschließend sendet der Client Anfragen an den Server, und der Server sendet Antworten zurück.

Erinnerung: Microsoft Active Directory fungiert als LDAP/LDAPS-Authentifizierungsserver.

So verwenden Sie das LDAP-Authentifizierungsprotokoll:

1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Wählen Sie das Optionsfeld "LDAP" aus, um den Abschnitt "LDAP" der Seite zu aktivieren.
3. Klicken Sie auf das 

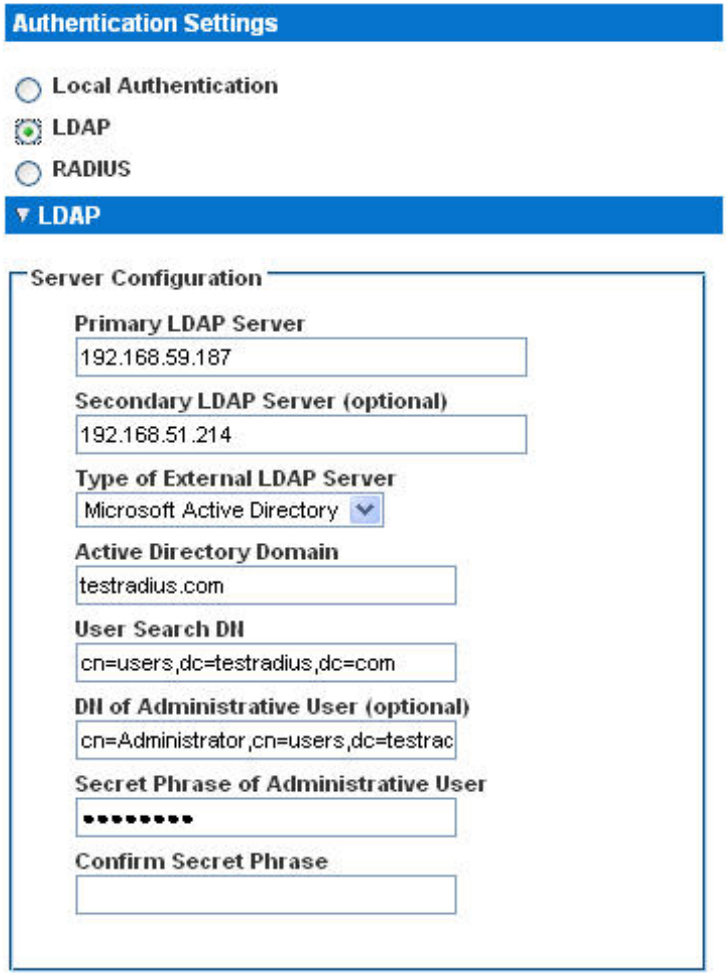
-Symbol, um den Abschnitt "LDAP" zu erweitern.

   Serverkonfiguration

4. Geben Sie im Feld "Primary LDAP Server" (Primärer LDAP-Server) die IP-Adresse oder den DNS-Namen des LDAP/LDAPS-Remote-Authentifizierungsservers ein (bis zu 256 Zeichen). Sind die Optionen "Enable Secure LDAP" (Secure LDAP aktivieren) und "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) ausgewählt, muss der DNS-Name verwendet werden, um dem CN des LDAP-Serverzertifikats zu entsprechen.
5. Geben Sie im Feld "Secondary LDAP Server" (Sekundärer LDAP-Server) die IP-Adresse oder den DNS-Namen des LDAP/LDAPS-Sicherungsservers ein (bis zu 256 Zeichen). Wenn die Option "Enable Secure LDAP" (Secure LDAP aktivieren) ausgewählt ist, muss der DNS-Name verwendet werden. Für die restlichen Felder gelten die gleichen Einstellungen wie für "Primary LDAP Server" (Primärer LDAP-Server). **Optional**
6. "Type of external LDAP Server" (Typ des externen LDAP-Servers)

7. Wählen Sie den externen LDAP/LDAPS-Server aus. Wählen Sie eine der folgenden Optionen:
   - "Generic LDAP Server" (Generischer LDAP-Server)
   - Microsoft Active Directory. Microsoft hat die LDAP/LDAPS-Verzeichnisdienste in Active Directory für die Verwendung in Windows-Umgebungen implementiert.
8. Geben Sie den Namen der Active Directory-Domäne ein, wenn Sie Microsoft Active Directory ausgewählt haben. Zum Beispiel *acme.com*. Fragen Sie Ihren leitenden Administrator nach einem speziellen Dömanennamen.
9. Geben Sie in das Feld "User Search DN" (DN für Benutzersuche) den Distinguished Name ein, bei dem Sie die Suche nach Benutzerinformationen in der LDAP-Datenbank beginnen möchten. Es können bis zu 64 Zeichen verwendet werden. Ein Beispiel für einen Basissuchwert ist: `cn=Benutzer,dc=raritan,dc=com`. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für diese Felder.
10. Geben Sie den Distinguished Name (DN) des Administratorbenutzers in das Feld "DN of Administrative User" (DN des Administratorbenutzers) ein (maximal 64 Zeichen). Füllen Sie dieses Feld aus, wenn Ihr LDAP-Server nur Administratoren die Suche nach Benutzerinformationen mithilfe der Funktion "Administrative User" (Administratorbenutzer) gestattet. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für dieses Feld. Ein Wert für "DN of administrative User" (DN des Administratorbenutzers) könnte wie folgt aussehen: `cn=Administrator,cn=Benutzer,dc=testradius,dc=com`. **Optional**

11. Wenn Sie einen "Distinguished Name" (DN) für den Administratorbenutzer eingeben, müssen Sie das Kennwort eingeben, um den DN des Administratorbenutzers am Remote-Authentifizierungsserver zu authentifizieren. Geben Sie das Kennwort in das Feld "Secret Phrase" (Geheimer Schlüssel) und ein weiteres Mal in das Feld "Confirm Secret Phrase" (Geheimen Schlüssel bestätigen) ein (maximal 128 Zeichen).



LDAP/LDAP Secure

12. Aktivieren Sie das Kontrollkästchen "Enable Secure LDA" (Secure LDAP aktivieren), wenn Sie SSL verwenden möchten. Dadurch wird das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, über das KX III sicher mit dem LDAP/LDAPS-Server kommunizieren kann.
13. Der Standardport lautet 389. Verwenden Sie entweder den Standard-TCP-Port für LDAP oder legen Sie einen anderen Port fest.

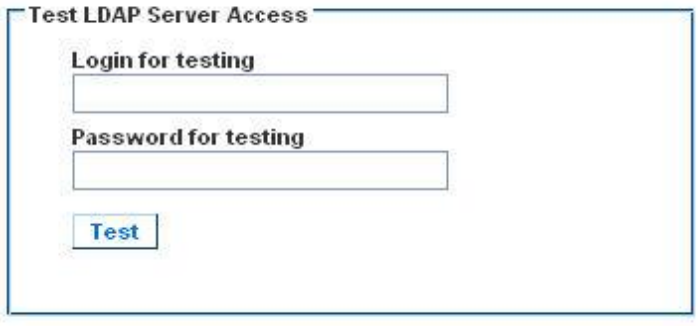
14. Der standardmäßige Secure LDAP-Port lautet 636. Verwenden Sie entweder den Standardport oder legen Sie einen anderen Port fest. Dieses Feld wird nur verwendet, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist.
15. Aktivieren Sie das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren), und verwenden Sie die zuvor hochgeladene CA-Stammzertifikatdatei zur Validierung des vom Server bereitgestellten Zertifikats. Wenn Sie die zuvor hochgeladene CA-Stammzertifikatdatei nicht verwenden möchten, lassen Sie das Kontrollkästchen deaktiviert. Die Deaktivierung dieser Funktion entspricht der Annahme des Zertifikats einer unbekannten Zertifizierungsstelle. Dieses Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert wurde.

   Hinweis: Ist zusätzlich zur CA-Stammzertifikat-Validierung die Option "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert, muss der Hostname des Servers mit dem bereitgestellten allgemeinen Namen im Serverzertifikat übereinstimmen.
16. Laden Sie die CA-Stammzertifikatdatei hoch, falls dies erforderlich ist. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist. Fragen Sie den Administrator des Authentifizierungsservers nach der CA-Zertifikatdatei im Base64-codierten X-509-Format für den LDAP-/LDAPS-Server. Navigieren Sie über die Schaltfläche "Browse" (Durchsuchen) zur entsprechenden Zertifikatdatei. Wenn Sie ein Zertifikat für den LDAP-/LDAPS-Server durch ein neues Zertifikat ersetzen, müssen Sie KX III neu starten, damit das neue Zertifikat wirksam wird.

Testen des LDAP-Serverzugriffs

17. KX III bietet Ihnen aufgrund der Komplexität einer erfolgreichen Konfigurierung von LDAP-Server und KX III zur Remoteauthentifizierung die Möglichkeit, die LDAP-Konfigurierung auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) zu testen. Um die Authentifizierungseinstellungen zu testen, geben Sie den Anmeldenamen in das das Feld "Login for testing" (Anmeldung für Test) und das Kennwort in das Feld "Password for testing" (Kennwort für Test) ein. Das sind der Benutzername und das Kennwort, die Sie für den Zugriff auf KX III eingegeben haben und die vom LDAP-Server für Ihre Authentifizierung verwendet werden. Klicken Sie auf "Test".

    Ist der Test abgeschlossen, wird Ihnen in einer Meldung angezeigt, ob der Test erfolgreich war oder nicht. Ist der Test fehlgeschlagen, wird Ihnen eine detaillierte Fehlermeldung angezeigt. Es wird das Ergebnis des erfolgreich durchgeführten Tests oder, falls der Test nicht erfolgreich war, eine detaillierte Fehlermeldung angezeigt. Außerdem können Gruppeninformationen angezeigt werden, die im Falle eines erfolgreichen Tests für den Testbenutzer vom LDAP-Remoteserver abgerufen werden.



Rückgabe von Benutzergruppeninformationen vom Active Directory-Server

KX III unterstützt die Benutzerauthentifizierung zu Active Directory® (AD), ohne dass Benutzer lokal in KX III definiert sein müssen. Dadurch können Active Directory-Benutzerkonten und -Kennwörter ausschließlich auf dem Active Directory-Server verwaltet werden. Die Autorisierungs- und Active Directory-Benutzerrechte werden mit standardmäßigen KX III-Richtlinien und Benutzergruppenrechten, die lokal auf Active Directory-Benutzergruppen angewendet werden, gesteuert und verwaltet.

WICHTIG: Wenn Sie bereits Kunde von Raritan, Inc. sind und den Active Directory-Server bereits durch Ändern des Active Directory-Schemas konfiguriert haben, unterstützt KX III diese Konfiguration nach wie vor, und Sie müssen den folgenden Vorgang nicht durchführen. Informationen zur Aktualisierung des

Active Directory-LDAP/LDAPS-Schemas finden Sie unter Aktualisieren des LDAP-Schemas.

So aktivieren Sie den AD-Server auf der KX III-Einheit:

1. Erstellen Sie auf der KX III-Einheit besondere Gruppen und weisen Sie ihnen geeignete Berechtigungen zu. Erstellen Sie z. B. Gruppen wie "KVM_Admin" und "KVM_Operator".
2. Erstellen Sie auf dem Active Directory-Server neue Gruppen mit denselben Gruppennamen wie die im vorherigen Schritt erstellten Gruppen.
3. Weisen Sie die KX III-Benutzer auf dem AD-Server den Gruppen zu, die Sie in Schritt 2 erstellt haben.
4. Aktivieren und konfigurieren Sie den AD-Server auf der KX III-Einheit. Siehe ***Implementierung der LDAP/LDAPS-Remoteauthentifizierung*** (auf Seite 73).

Wichtige Hinweise:

- Bei der Eingabe des Gruppennamens muss die Groß-/Kleinschreibung beachtet werden.
- KX III bietet folgende Standardgruppen, die nicht geändert oder gelöscht werden können: "Admin" und "<Unknown>" (Unbekannt). Stellen Sie sicher, dass diese Gruppennamen nicht auch vom Active Directory-Server verwendet werden.
- Wenn die vom Active Directory-Server zurückgegebenen Gruppeninformationen nicht mit der KX III-Gruppenkonfiguration übereinstimmen, weist KX III den Benutzern, die sich erfolgreich authentifizieren, automatisch die Gruppe "<Unknown>" (Unbekannt) zu.
- Wenn Sie eine Rückrufnummer verwenden, müssen Sie die folgende Zeichenfolge unter Beachtung der Groß-/Kleinschreibung eingeben:*msRADIUSCallbackNumber.*
- Auf Empfehlung von Microsoft sollten "Global Groups" (globale Gruppen) mit Benutzerkonten verwendet werden, keine "Domain Local Groups" (lokale Domaingruppen).

Implementierung der RADIUS-Remote-Authentifizierung

Remote Authentication Dial-in User Service (RADIUS) ist ein AAA-Protokoll [Authentication, Authorization Accounting (Authentifizierung, Autorisierung und Kontoführung)] für Anwendungen für den Netzwerkzugriff.

So verwenden Sie das RADIUS-Authentifizierungsprotokoll:

1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Klicken Sie auf das Optionsfeld "RADIUS", um den Abschnitt "RADIUS" der Seite zu aktivieren.
3. Klicken Sie auf das 

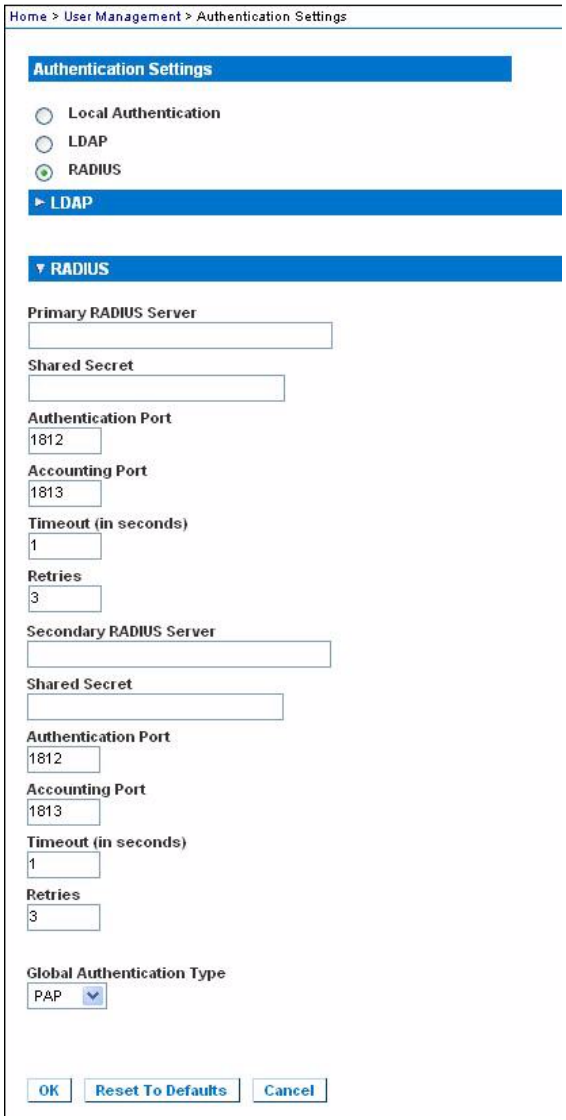
-Symbol, um den Abschnitt "RADIUS" zu erweitern.
4. Geben Sie in den Feldern "Primary Radius Server" (Primärer RADIUS-Server) und "Secondary Radius Server" (Sekundärer RADIUS-Server) die jeweiligen IP-Adressen des primären und optionalen sekundären Remote-Authentifizierungsservers ein (bis zu 256 Zeichen).
5. Geben Sie im Feld "Shared Secret" (Gemeinsamer geheimer Schlüssel) den geheimen Schlüssel für die Authentifizierung ein (bis zu 128 Zeichen).

   Der gemeinsame geheime Schlüssel ist eine Zeichenfolge, die KX III und dem RADIUS-Server bekannt sein muss, damit diese sicher kommunizieren können. Es handelt sich dabei praktisch um ein Kennwort.
6. Der Standardport für "Authentication Port" (Authentifizierungsport) lautet 1812, kann jedoch nach Bedarf geändert werden.
7. Der Standardport für "Accounting Port" (Kontoführungsport) lautet 1813, kann jedoch nach Bedarf geändert werden.
8. Das "Timeout" (Zeitlimit) wird in Sekunden aufgezeichnet. Der Standardwert beträgt 1 Sekunde, kann jedoch bei Bedarf geändert werden.

   Das Zeitlimit bezeichnet die Zeitspanne, während der KX III auf eine Antwort vom RADIUS-Server wartet, ehe eine weitere Authentifizierungsanforderung gesendet wird.
9. Die standardmäßige Anzahl an Neuversuchen beträgt 3.

   Dieser Wert gibt an, wie oft KX III eine Authentifizierungsanforderung an den RADIUS-Server sendet.
10. Wählen Sie in der Dropdownliste den "Global Authentication Type" (Globaler Authentfizierungstyp) aus:

- PAP – Mit PAP werden Kennwörter als unformatierter Text gesendet. PAP ist nicht interaktiv. Benutzername und Kennwort werden als ein Datenpaket gesendet, sobald eine Verbindung hergestellt wurde. Der Server sendet nicht zuerst eine Anmeldeaufforderung und wartet auf eine Antwort.
- CHAP – Mit CHAP kann der Server jederzeit eine Authentifizierung anfordern. CHAP bietet mehr Sicherheit als PAP.



Cisco ACS 5.x für RADIUS-Authentifizierung

Bei Verwendung eines Cisco ACS 5.x Servers führen Sie nach dem Konfigurieren von KX III für die RADIUS-Authentifizierung die folgenden Schritte auf dem Cisco ACS 5.x Server aus.

Hinweis: Die folgenden Schritte umfassen die Cisco Menüs und Menüelemente, die für den Zugriff auf die einzelnen Seiten verwendet werden. Aktuelle Informationen und weitere Einzelheiten zum Ausführen der einzelnen Schritte finden Sie in der Cisco Dokumentation.

- KX III als AAA-Client hinzufügen (**Erforderlich**) – "Network Resources" (Netzwerkressourcen) > "Network Device Group" (Netzwerkgeräte-Gruppe)> "Network Device and AAA Clients" (Netzwerkgerät und AAA-Clients)
- Benutzer hinzufügen/bearbeiten (**Erforderlich**) – "Network Resources" (Netzwerkressourcen) > "Users and Identity Stores" (Benutzer und Identitätsspeicher) > "Internal Identity Stores" (Interne Identitätsspeicher) > "Users" (Benutzer)
- Standardnetzwerkzugriff zur Aktivierung des CHAP-Protokolls konfigurieren (**Optional**) – "Policies" (Richtlinien) > "Access Services" (Zugriffsdienste) > "Default Network Access" (Standardnetzwerkzugriff)
- Autorisierungsregeln zur Zugriffskontrolle erstellen (**Erforderlich**) – "Policy Elements" (Richtlinienelemente) > "Authorization and Permissions" (Autorisierung und Berechtigungen) > "Network Access" (Netzwerkzugriff) > "Authorization Profiles" (Autorisierungsprofile)
  - Wörterbuchtyp: RADIUS-IETF
  - RADIUS-Attribut: Filter-ID
  - Attributtyp: Zeichenfolge
  - Attributwert: Raritan:G{KVM_Admin} (wobei KVM_Admin der Gruppenname ist, der lokal auf dem Dominion KVM-Switch erstellt wird). Die Groß-/Kleinschreibung muss beachtet werden.
- Sitzungsbedingungen konfigurieren (Datum und Uhrzeit) (**Erforderlich**) – "Policy Elements" (Richtlinienelemente) > "Session Conditions" (Sitzungsbedingungen) > "Date and Time" (Datum und Uhrzeit)
- Die Autorisierungsrichtlinie für den Netzwerkzugriff konfigurieren/erstellen (**Erforderlich**) – "Access Policies" (Zugriffsrichtlinien) > "Access Services" (Zugriffsdienste) > "Default Network Access" (Standardnetzwerkzugriff) > "Authorization" (Autorisierung)

Zurückgeben von Benutzergruppeninformationen über RADIUS

Wenn ein RADIUS-Authentifizierungsversuch erfolgreich ist, bestimmt KX III die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers.

Ihr Remote-RADIUS-Server kann diese Benutzergruppennamen bereitstellen, indem er ein als RADIUS FILTER-ID implementiertes Attribut zurückgibt. Die FILTER-ID sollte folgendermaßen formatiert sein: Raritan:G{*GROUP_NAME*}. Dabei ist *GROUP_NAME* eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört.

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

Dabei ist "GROUP_NAME" eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört, und "Dial Back Number" die dem Benutzerkonto zugeordnete Nummer, die das KX III-Modem für den Rückruf des Benutzerkontos verwendet.

Spezifikationen für den RADIUS-Kommunikationsaustausch

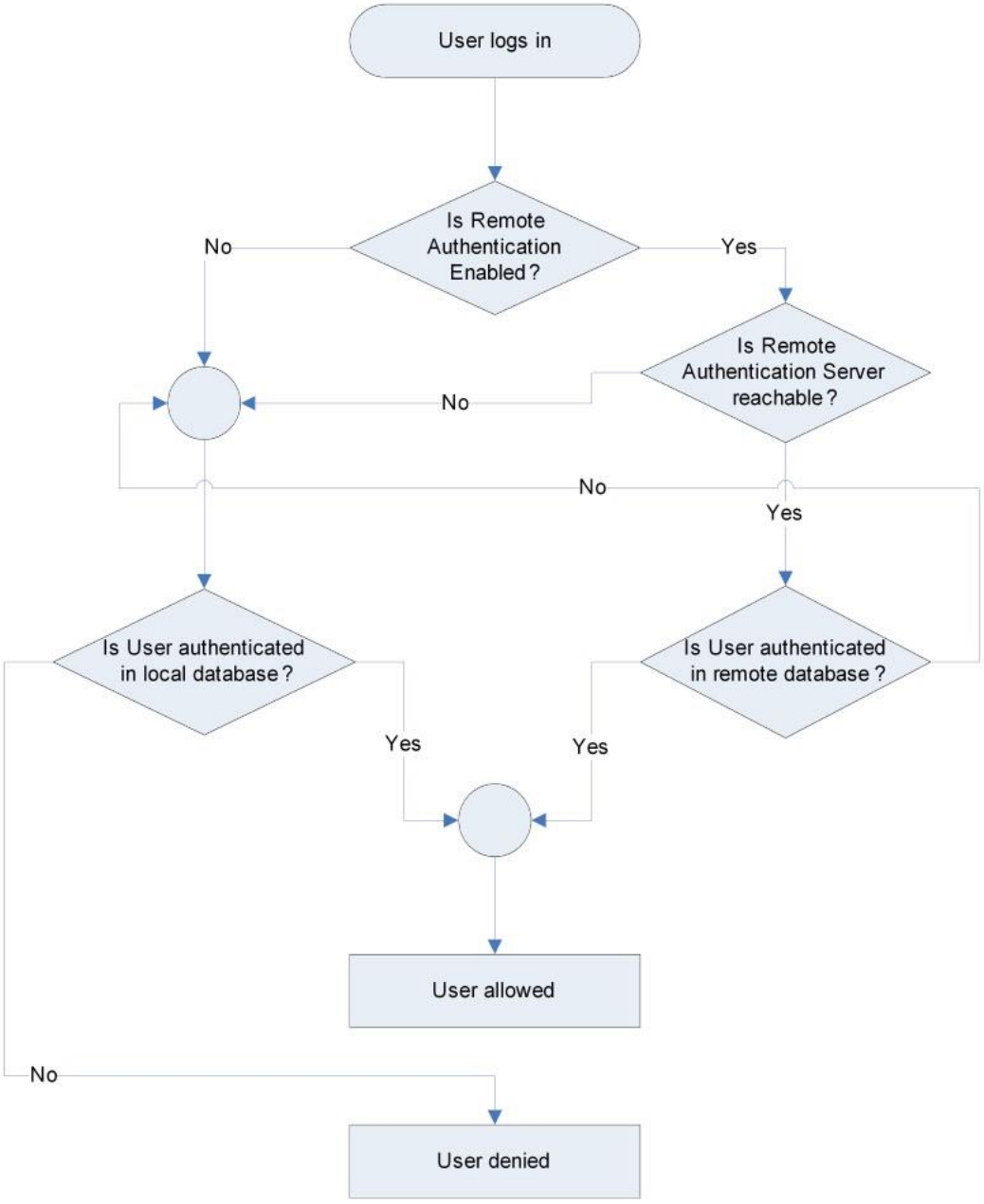
KX III sendet die folgenden RADIUS-Attribute an Ihren RADIUS-Server:

Attribut	**Daten**
Anmelden	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-IP-Address (4)	Die IP-Adresse des KX III.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.
User-Password(2)	Das verschlüsselte Kennwort.
Accounting-Request(4)	
Acct-Status (40)	Start(1) – Kontoführung wird gestartet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des KX III.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.

Attribut Abmelden	Daten
Accounting-Request(4)	
Acct-Status (40)	Stop(2) – Kontoführung wird beendet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des KX III.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.

Benutzerauthentifizierungsprozess

Die Remoteauthentifizierung wird über den im folgenden Diagramm angegebenen Vorgang durchgeführt:

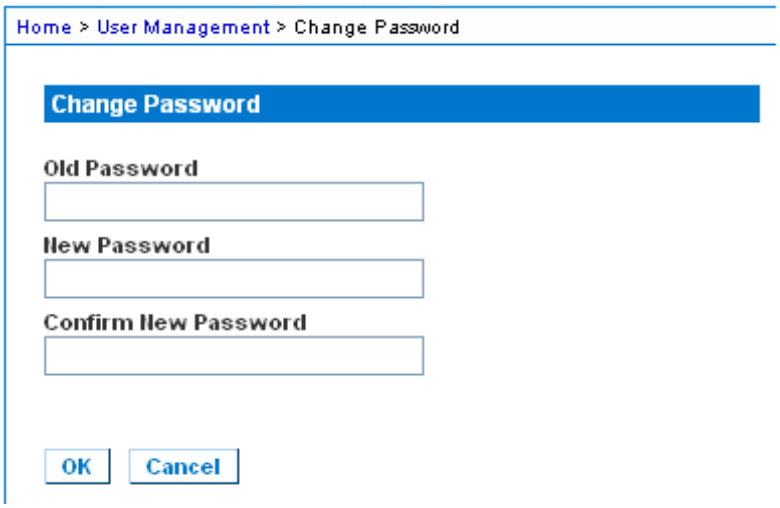


Ändern von Kennwörtern

So ändern Sie Ihr KX III-Kennwort:

1. Wählen Sie User Management Change Password (Benutzerverwaltung Kennwort ändern). Die Seite Change Password (Kennwort ändern) wird angezeigt.
2. Geben Sie das aktuelle Kennwort in das Feld Altes Kennwort ein.
3. Geben Sie in das Feld "New Password" (Neues Kennwort) ein neues Kennwort ein. Geben Sie das Kennwort im Feld "Confirm New Password" (Neues Kennwort bestätigen) erneut ein. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen.
4. Klicken Sie auf OK.
5. Sie erhalten eine Bestätigung, dass das Kennwort erfolgreich geändert wurde. Klicken Sie auf OK.

Hinweis: Wenn sichere Kennwörter verwendet werden müssen, enthält diese Seite Informationen zum erforderlichen Format. Weitere Informationen zu Kennwörtern und **sicheren Kennwörtern** *(siehe "***Strong Passwords (Sichere Kennwörter)***" auf Seite 178) finden Sie unter Sichere Kennwörter in der Online-Hilfe.*



Geräteverwaltung

Network Settings (Netzwerkeinstellungen)

Auf der Seite "Network Settings" (Netzwerkeinstellungen) können Sie die Netzwerkkonfiguration (z. B. IP-Adresse, Erkennungsport und LAN-Schnittstellenparameter) für Ihre KX III-Einheit anpassen.

Es stehen Ihnen zwei Optionen zum Festlegen der IP-Konfiguration zur Verfügung:

- None (default) [Keine (Standard)] – Dies ist die empfohlene Option (statisches IP). Da die KX III-Einheit Teil Ihrer Netzwerkinfrastruktur ist, möchten Sie wahrscheinlich, dass die Adresse möglichst konstant bleibt. Bei dieser Option können Sie die Netzwerkparameter selbst einrichten.
- DHCP – Mit dieser Option wird die IP-Adresse automatisch durch einen DHCP-Server zugewiesen.

So ändern Sie die Netzwerkkonfiguration:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Aktualisieren der Basisnetzwerkeinstellungen. Siehe ***Basisnetzwerkeinstellungen*** (siehe "***Network Basis Settings (Basisnetzwerkeinstellungen)***" auf Seite 87).
3. Aktualisieren der LAN-Schnittstelleneinstellungen. Siehe ***LAN-Schnittstelleneinstellungen*** (siehe "***LAN Interface Settings (LAN-Schnittstelleneinstellungen)***" auf Seite 91).
4. Klicken Sie auf OK, um die Konfiguration festzulegen. Ist für die vorgenommenen Änderungen ein Neustart des Geräts erforderlich, wird eine entsprechende Meldung angezeigt.

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Network Basis Settings (Basisnetzwerkeinstellungen)

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter ***Netzwerkeinstellungen*** (siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 86).

So weisen Sie eine IP-Adresse zu:

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen > Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr KX III-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.
3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
   b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
   c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
   d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
   e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

   - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da KX III ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.

   - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

     Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server zugewiesen. Bei Verwendung von DHCP geben Sie unter "Preferred host name (DHCP only)" (Name des bevorzugten Hosts [Nur DHCP]) einen Wert ein (maximal 63 Zeichen).

4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.
   b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem KX III zugeordnet ist.
   c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.
   d. Geben Sie die IP-Adresse des Gateway ein.
   e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lese-zugriff)**
   f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lese-zugriff)**
   g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

   - None (Keine) – Wählen Sie diese Option aus, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

     Wenn für "IP auto configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlange) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.

   - Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.

5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.
6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

Geben Sie die folgenden Informationen ein, wenn die Option "Following DNS Server Addresses" (Folgende DNS-Serveradressen) ausgewählt wurde. Diese Adressen sind die primären und sekundären DNS-Adressen, die verwendet werden, wenn die primäre DNS-Serververbindung aufgrund eines Ausfalls getrennt wird.

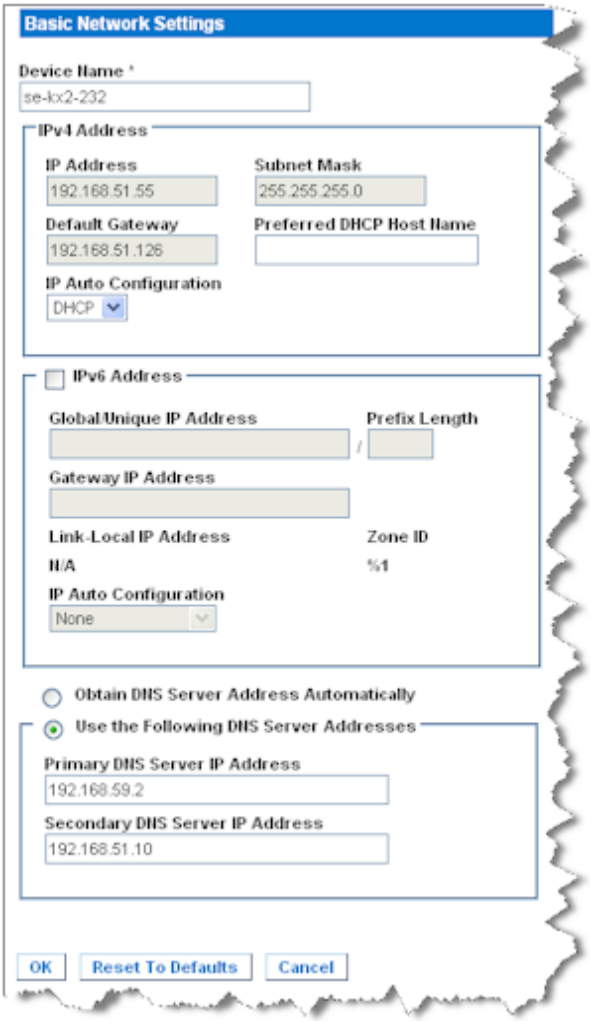
a. "Primary DNS Server IP Address" (IP-Adresse des primären DNS-Servers)

b. "Secondary DNS-Server IP Address" (IP-Adresse des sekundären DNS-Servers)

7. Klicken Sie abschließend auf "OK".

Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter ***LAN-Schnittstelleneinstellungen*** (siehe "***LAN Interface Settings (LAN-Schnittstelleneinstellungen)***" auf Seite 91).

Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des KX III den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben.Weitere Informationen finden Sie auf der Seite **Network Settings** *(siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 86) (Netzwerkeinstellungen).*



Raritan.

LAN Interface Settings (LAN-Schnittstelleneinstellungen)

Die aktuellen Parametereinstellungen werden im Feld "Current LAN interface parameters" (Aktuelle LAN-Schnittstellenparameter) angezeigt.

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen - Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Wählen Sie aus folgenden Optionen die LAN-Schnittstellengeschwindigkeit und Duplex aus:
   - "Autodetect (default option)" [Automatische Aushandlung (Standardoption)]
   - 10 Mbit/s/Halb – Beide LEDs blinken
   - 10 Mbit/s/Voll – Beide LEDs blinken
   - 100 Mbps/Half (10 Mbit/s/Halb) – Gelbe LED blinkt
   - 100 Mbps/Full (10 Mbit/s/Voll) – Gelbe LED blinkt
   - 1000 Mbit/s/Voll (Gigabit) – grüne LED blinkt
   - "Half-duplex" (Halbduplex) sorgt für Kommunikation in beide Richtungen, jedoch nicht gleichzeitig.
   - "Full-duplex" (Vollduplex) ermöglicht die gleichzeitige Kommunikation in beide Richtungen.

   Hinweis: Bei 10 Mbit/s und Halb- oder Vollduplex kann es gelegentlich zu Problemen kommen. Verwenden Sie in einem solchen Fall eine andere Geschwindigkeit und Duplexeinstellung.

   Weitere Informationen finden Sie unter ***Netzwerk-Geschwindigkeitseinstellungen*** (auf Seite 354).
3. Aktivieren Sie das Kontrollkästchen "Enable Automatic Failover" (Automatisches Failover aktivieren), um zu veranlassen, dass KX III die Netzwerkverbindung automatisch mithilfe eines zweiten Netzwerkports wiederherstellt, wenn der aktive Netzwerkport ausfällt.

   Hinweis: Da ein Failoverport erst aktiviert wird, wenn tatsächlich ein Ausfall stattgefunden hat, empfiehlt Raritan, den Port nicht zu überwachen oder ihn erst zu überwachen, nachdem ein Ausfall stattgefunden hat.

   Wenn dieses Kontrollkästchen aktiviert ist, stehen die folgenden beiden Felder zur Verfügung:
   - Ping Interval (seconds) (Pingintervall [Sekunden]) – Mit dem Pingintervall wird festgelegt, wie häufig KX III den Status des Netzwerkpfads zum festgelegten Gateway prüft. Das Standardpingintervall beträgt 30 Sekunden.

- Timeout (seconds) (Zeitlimit [Sekunden]) – Das Zeitlimit bestimmt, wie lange ein festgelegtes Gateway über die Netzwerkverbindung nicht erreichbar sein darf, bevor ein Fehler auftritt.

Hinweis: Pingintervall und Zeitlimit können durch Konfiguration optimal an die Bedingungen des Netzwerks angepasst werden. Die Einstellung für das Zeitlimit sollte so gewählt werden, dass mindestens 2 oder mehr Pinganforderungen übertragen und beantwortet werden können. Wird beispielsweise eine hohe Failover-Rate aufgrund von starker Netzwerkauslastung beobachtet, sollte das Zeitlimit auf das 3- bis 4-fache des Pingintervalls erhöht werden.

4. Wählen Sie die Bandbreite aus.
5. Klicken Sie auf OK, um die LAN-Einstellungen zu übernehmen.

Ports konfigurieren

Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.

So greifen Sie auf eine Portkonfiguration zu:

1. Wählen Sie "Geräteeinstellungen Portkonfiguration". Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.

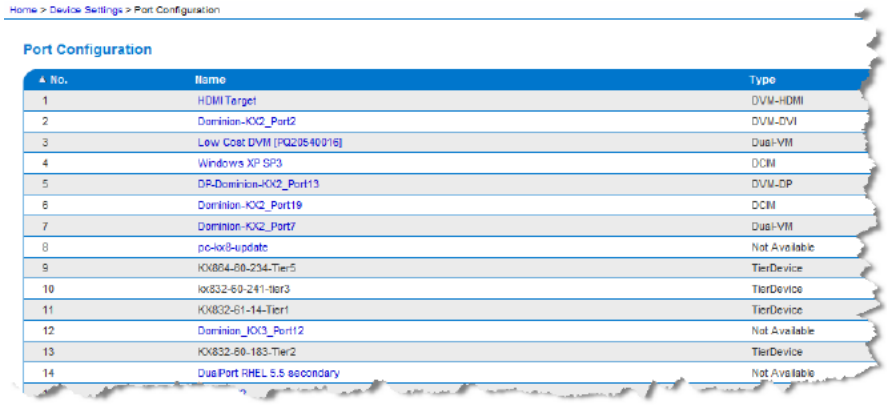
   Der Inhalt der Seite wird zunächst in der Reihenfolge der Port-Nummern angezeigt. Sie können für eine andere Sortierung jedoch auf eine der Spaltenüberschriften klicken.
2. Klicken Sie auf den Portnamen des Ports, den Sie bearbeiten möchten.
   - Für KVM-Ports wird die Seite "Port" für KVM und Blade-Chassis-Ports angezeigt.
   - Für Gestell-PDUs wird die Seite "Port" für Gestell-PDUs (Powerstrips) angezeigt. Auf dieser Seite können Sie die Gestell-PDUs und ihre Ausgänge benennen.

Seite Port Configuration (Portkonfiguration)

Die Seite "Port Configuration" (Port-Konfiguration) enthält eine Liste der KX III Ports.

Wenn der Status eines Ports ausgeschaltet ist, wird dafür "Not Available" (Nicht verfügbar) angezeigt. Ein Port kann ausgeschaltet sein, wenn das CIM des Ports entfernt oder ausgeschaltet wurde.

Hinweis: Bei Blade-Chassis kann zwar der Name des Blade-Chassis, nicht aber die Namen des Bladeslots geändert werden.



Portnummer

Die für das KX III Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert.

Portname

Für Ports, an die kein CIM angeschlossen sind oder für die kein CIM-Name angegeben ist, wird der Standardportname zugewiesen, wobei "Port#" für die Nummer des physischen KX III Ports steht.

Sie können Ports auch umbenennen, die aktuell nicht über ein CIM mit KX III verbunden sind und daher den Status "Not Available" (Nicht verfügbar) haben.

Führen Sie zum Umbenennen eines Ports mit dem Status "Not Available" (Nicht verfügbar) einen der folgenden Schritte aus:

- Benennen Sie den Port um. Beim Anhängen eines CIM wird der CIM-Name verwendet.
- Benennen Sie den Port um, und wählen Sie "Persist name on Next CIM Insertion" (Name bei nächster CIM-Installation beibehalten). Beim Anhängen eines CIM wird der zugewiesene Name in das CIM kopiert.
- Setzen Sie den Port durch Auswählen der Option "Reset to Defaults" (Auf werksseitige Standardeinstellungen zurücksetzen) auf die werksseitigen Standardeinstellungen zurück. Beim Anhängen eines CIM wird der CIM-Name verwendet.

Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).

Nachdem Sie den Port umbenannt haben, können Sie mit der Funktion „Reset to Default“ (Standardwerte wiederherstellen) den Standardportnamen jederzeit wieder herstellen.

Wenn Sie einen Portnamen auf die Standardeinstellung zurücksetzen, werden alle vorhandenen Stromzuordnungen entfernt. Gehört der Port einer Portgruppe an, wird er außerdem aus der Gruppe entfernt.

Porttyp

Porttyp beinhaltet:

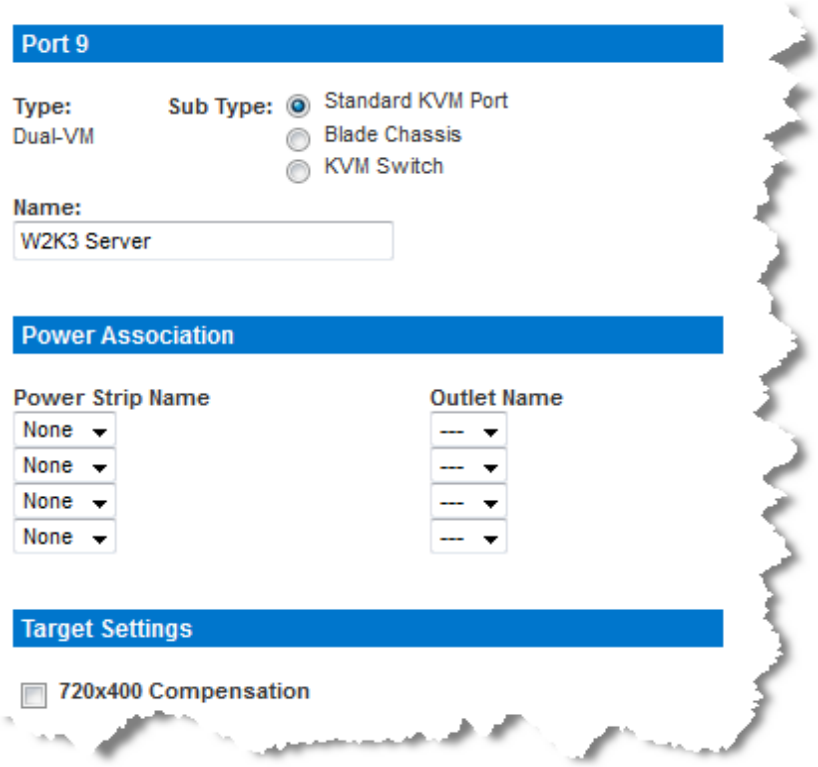
- DCIM – Dominion-CIM
- TierDevice-Schichtgerät
- "Not Available" (Nicht verfügbar) – Kein CIM angeschlossen
- DVM-DP – Display-Port CIM
- DVM-HDMI - HDMI CIMsws'
- DVM-DVI – DVI CIM
- PowerStrip (Gestell-PDU) – Powerstrip angeschlossen
- VM - D2CIM - VUSB CIM
- Dual - VM - D2CIM-DVUSB CIM
- Blade-Chassis – Blade-Chassis und die dem Chassis zugeordneten Blades (in hierarchischer Reihenfolge angezeigt)
- KVM-Switch – Generische KVM-Switch-Verbindung
- PCIM – Paragon-CIM

Konfigurieren von Standardzielservern

So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist. Weitere Einzelheiten finden Sie unter Schritt 3: Anschließen der Geräte für eine Beschreibung zum Anschließen der Geräte.
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
3. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite "Port" wird angezeigt.
4. Wählen Sie "Standard KVM Port" als Subtyp für den Port aus.
5. Weisen Sie dem mit diesem Port verbundenen Server einen Namen zu. Der Name darf maximal 32 alphanumerische Zeichen oder Sonderzeichen umfassen.

6. Klicken Sie auf OK.



Konfigurieren von KVM-Switches

KX III unterstützt außerdem die Verwendung von Tastenfolgen, um zwischen Zielen zu wechseln. Außer der Verwendung von Tastenfolgen mit Standardservern wird KVM-Switching auch von Blade-Chassis und Schichtkonfigurationen unterstützt.

Wichtig: Damit die Benutzergruppen den von Ihnen erstellten KVM-Switch sehen können, müssen Sie zuerst den Switch und dann die Gruppe erstellen. Wenn eine vorhandene Benutzergruppe den von Ihnen erstellten KVM-Switch sehen muss, müssen Sie die Benutzergruppe neu erstellen.

So konfigurieren Sie KVM-Switches:

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite **Port** wird angezeigt.
3. Wählen Sie den KVM-Switch aus.

4. Wählen Sie das KVM-Switch-Modell aus.

   Hinweis: Es wird nur ein Switch in der Dropdown-Liste angezeigt.

5. Wählen Sie "KVM Switch Hot Key Sequence" (KVM-Switch-Tastenfolge) aus.
6. Geben Sie die maximale Anzahl der Zielports (2-32) ein.
7. Geben Sie im Feld "KVM Switch Name" den gewünschten Namen für diese Portkonfiguration ein.
8. Aktivieren Sie die Ziele für die KVM-Switch-Tastenfolge. Geben Sie die KVM-Switch-Ports mit angeschlossenen Zielen an, indem Sie für jeden Port die Option "Active" (Aktiv) auswählen.
9. Im Abschnitt "KVM Managed Links" (Verwaltete KVM-Verknüpfungen) der Seite können Sie die Verbindung zu einer Webbrowseroberfläche konfigurieren, wenn verfügbar.
   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL Name – Geben Sie die URL zur Benutzeroberfläche ein.
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.
   e. Feld "Username" (Benutzername) - Geben Sie den Parameter des Benutzernamens ein, der in der URL verwendet wird. Beispielsweise *username*=admin, wobei *username* das Feld "username" (Benutzername) ist.
   f. Feld "Password" (Kennwort) - Geben Sie den Parameter des Kennworts ein, der in der URL verwendet wird. Beispielsweise *password*=raritan, wobei *password* das Feld "password " (Kennwort) ist.
10. Klicken Sie auf "OK".

So ändern Sie den aktiven Status eines KVM-Switch-Ports oder einer URL:

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite **Port** wird angezeigt.
3. Deaktivieren Sie das Kontrollkästchen "Active" (Aktiv) neben dem KVM-Switch-Zielport oder neben der URL, um den aktiven Status zu ändern.
4. Klicken Sie auf "OK".

Konfigurieren von CIM-Ports

KX III unterstützt die Verwendung von standardmäßigen und virtuellen Medien CIMs, um einen Server mit KX III zu verbinden.

So konfigurieren Sie ein CIM:

1. Wählen Sie "Geräteeinstellungen Portkonfiguration". Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite Port wird angezeigt.
3. Wählen Sie "Standard KVM Port" als Subtyp für den Port aus.
4. Weisen Sie dem mit diesem Port verbundenen Server einen Namen zu. Der Name darf maximal 32 alphanumerische Zeichen oder Sonderzeichen umfassen.
5. Ordnen Sie im Abschnitt "Power Association" (Stromzuordnung) bei Bedarf einem Port ein Powerstrip zu.
6. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
7. Legen Sie für digitale CIMs die Auflösung des Ziels so fest, dass Sie mit der systemeigenen Anzeigeauflösung des Monitors übereinstimmt. Wählen Sie hierfür die Auflösung aus der Dropdownliste "Display Native Resolution" (Systemeigene Auflösung) aus.

   Wenn Sie ein HDMI CIM verwenden, bieten einige Betriebssystem-/Videokartenkombinationen möglicherweise nur eine beschränkte Auswahl an RGG-Werten. Verbessern Sie die Farben, indem Sie das Kontrollkästchen "DVI Compatibility Mode" (DVI-Kompatibilitätsmodus) auswählen.
8. Klicken Sie auf OK.

Konfiguration von Gestell-PDU-Zielen (Powerstrip)

Mit dem KX III können Sie Gestell-PDUs (Powerstrips) mit KX III-Ports verbinden.

Die Konfiguration der KX III-Gestell-PDUs erfolgt auf der Seite "KX III Port Configuration" (KX II-Port-Konfiguration).

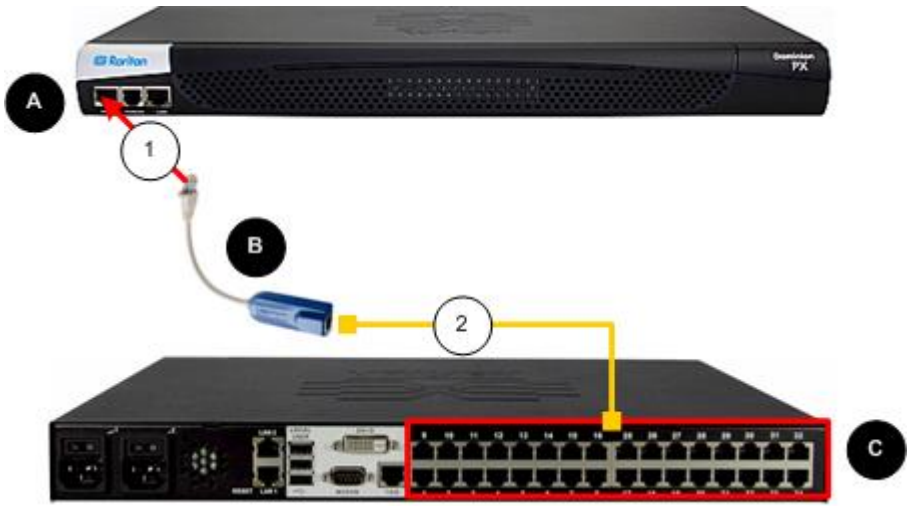
Hinweis: Raritan empfiehlt, nicht mehr als acht (8) Rack-PDUs (Power-Streifen) zu einem KX III auf einmal zu verbinden, da die Leistung beeinträchtigt werden kann.

Verbinden einer Gestell-PDU

Die Gestell-PDUs (Powerstrips) der Serien Raritan PX werden über das D2CIM-PWR CIM mit dem Dominion-Gerät verbunden.

So schließen Sie die Gestell-PDU an:

1. Verbinden Sie den RJ-45-Stecker des D2CIM-PWR mit der RJ-45-Buchse des seriellen Ports der Gestell-PDU.
2. Verbinden Sie die RJ-45-Buchse des D2CIM-PWR mit einer der freien Systemport-Buchsen des KX III mittels eines direkten Kabels der Kategorie 5.
3. Schließen Sie ein Netzkabel am Zielserver und einem verfügbaren Gestell-PDU-Ausgang an.
4. Schließen Sie die Gestell-PDU an eine Netzsteckdose an.
5. Schalten Sie das Gerät ein.



Diagrammschlüssel	
A	PX Rack PDU mit Seriellem Port

B	D2CIM-PWR
C	KX III
1	D2CIM-PWR zu PDU Serieller Port Verbindung
2	D2CIM-PWR zu KX III Zielserver-Port via Cat5 Kabel

Benennen der Gestell-PDU (Seite "Port" für Powerstrips)

Hinweis: PX-Gestell-PDUs (Powerstrips) können im PX-Gerät und im KX III benannt werden.

Sobald eine Remote-Gestell-PDU von Raritan an KX III angeschlossen ist, wird diese auf der Seite "Port Configuration" (Port-Konfiguration) angezeigt. Klicken Sie auf dieser Seite auf den Namen des Stromzufuhr-Ports, um darauf zuzugreifen. Die Felder "Type" (Typ) und "Name" sind bereits ausgefüllt.

Hinweis: Der (CIM-)Typ kann nicht geändert werden.

Die folgenden Informationen werden für jeden Ausgang der Gestell-PDU angezeigt: [Outlet] Nummer, Name, und Portzuordnung.

Auf dieser Seite können Sie die Gestell-PDU und deren Ausgänge benennen. Die Namen können bis zu 32 alphanumerische Zeichen umfassen und dürfen Sonderzeichen enthalten.

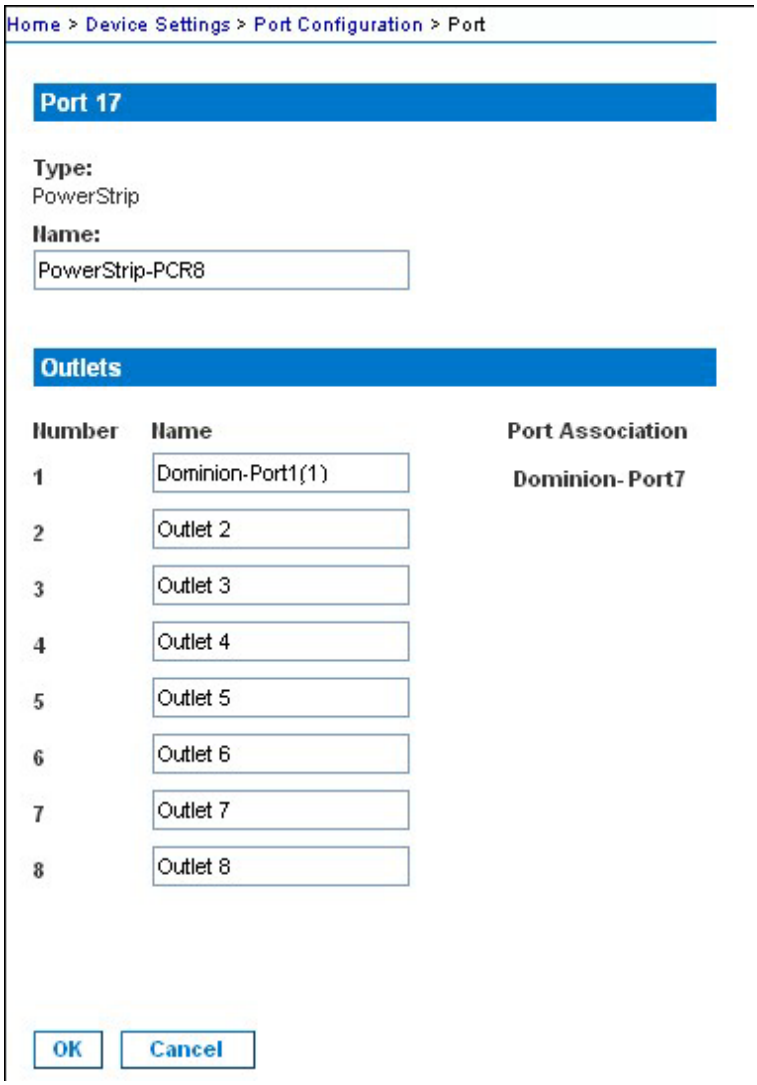
Hinweis: Wenn eine Rack-Stromverteilungseinheit einem Zielserver (Port) zugeordnet ist, wird der Name des Ausgangs durch den Namen des Zielservers ersetzt, auch wenn Sie dem Ausgang einen anderen Namen zugewiesen haben.

So weisen Sie der Rack-Stromverteilungseinheit und den Ausgängen einen Namen zu:

Hinweis: CommandCenter Secure Gateway erkennt keine Namen von Rack-Stromverteilungseinheiten, die Leerzeichen enthalten.

1. Geben Sie den Namen der Gestell-PDU ein (falls erforderlich).
2. Ändern Sie ggf. den [Ausgangs-]namen. (Der Standardname entspricht der Ausgangsnummer.)

3. Klicken Sie auf OK.



Zuordnen der Ausgänge zu Zielservern

Die Seite "Port" wird geöffnet, wenn Sie auf der Seite "Port Configuration" (Portkonfiguration) auf einen Port klicken.

Wenn ein Ausgang mit dem gleichen Server verbunden ist, kann eine Leistungsverbindung mit dem Ziel-Server hergestellt werden.

Ein Server kann maximal vier Netzschalter haben, und Sie können jedem eine andere Gestell-PDU (Powerstrip) zuordnen. Auf dieser Seite können Sie diese Zuordnungen definieren, damit Sie auf der Seite Port Access (Portzugriff) den Server einschalten, ausschalten sowie ein- und ausschalten können.

Für dieses Feature benötigen Sie Folgendes:

- Remotegestell-PDU(s) von Raritan
- Power CIMs (D2CIM-PWR)

Eine Power-Zuordnung Erstellen

So stellen Sie Stromzuordnungen her (ordnen Gestell-PDU-Ausgänge den KVM-Zielservern zu):

Hinweis: Wenn eine Gestell-PDU einem Zielserver (Port) zugeordnet ist, wird der Ausgangsname durch den Namen des Zielservers ersetzt (auch wenn Sie dem Ausgang einen anderen Namen zugeordnet haben).

1. Auf der Port-Konfiguration Seite, wählen Sie den Zielserver, womit Sie den PDU verknüpfen möchten.
2. Wählen Sie eine Gestell-PDU in der Dropdownliste "Power Strip Name" (Powerstripname) aus.
3. Wählen Sie einen Ausgang für diese Gestell-PDU in der Dropdownliste "Outlet Name" (Ausgangsname) aus.
4. Wiederholen Sie die Schritte 1 und 2 für alle gewünschten Stromzuordnungen.
5. Klicken Sie auf OK. Eine Bestätigungsmeldung wird angezeigt.

Entfernen Sie eine Power-Zuordnung

Wenn Sie Zielserver und/oder Rack-Stromverteilungseinheiten vom Gerät trennen, müssen Sie zunächst die Zuordnungen der Stromausgänge löschen. Wenn ein Ziel einer Rack-Stromverteilungseinheit zugewiesen wurde und das Ziel vom Gerät entfernt wird, bleibt die Zuordnung des Stromausgangs erhalten. In diesem Fall können Sie nicht auf die Portkonfiguration des getrennten Zielservers unter "Device Settings" (Geräteeinstellungen) zugreifen, um die Stromzuordnung ordnungsgemäß zu löschen.

So entfernen Sie eine Gestell-PDU-Zuordnung:

1. Wählen Sie die entsprechende Gestell-PDU in der Dropdownliste "Power Strip Name" (Powerstripname) aus.
2. Wählen Sie den entsprechenden Ausgang für diese Gestell-PDU in der Dropdownliste "Outlet Name" (Ausgangsname) aus.
3. Wählen Sie in der Dropdown-Liste "Outlet Name" (Ausgangsname) die Option "None" (Kein).
4. Klicken Sie auf OK. Die Gestell-PDU-/Ausgangszuordnung wird entfernt und eine Bestätigungsmeldung wird angezeigt.

So entfernen Sie eine Gestell-PDU-Zuordnung, wenn die Gestell-PDU vom Zielgerät entfernt wurde:

1. Klicken Sie auf "Device Settings“ "Port Configuration" (Geräteeinstellungen > Portkonfiguration) und anschließend auf das aktive Zielgerät.
2. Ordnen Sie das aktive Zielgerät dem getrennten Stromversorgungsport zu. Dadurch wird die Stromzuordnung des getrennten Zielgeräts aufgehoben.
3. Ordnen Sie anschließend das aktive Zielgerät dem richtigen Stromversorgungsport zu.

Konfigurieren von Blade-Chassis

Zusätzlich zu Standardservern und Gestell-PDUs (Powerstrips) können Sie Blade-Chassis steuern, die an einen KX III Geräteport angeschlossen sind. Bis zu acht Blade-Chassis können gleichzeitig verwaltet werden.

Wenn der Blade-Chassis-Typ unterstützt wird, wird das Blade-Chassis automatisch nach dem Anschließen erkannt.

Wenn Ein Bladeserver-Chassis erkannt wurde, wird diesem ein Standardname zugewiesen und es wird auf der Seite "Port Access" (Portzugriff) zusammen mit Standardzielservern und Gestell-PDUs angezeigt.

Wenn der Typ nicht unterstützt wird, muss das Blade manuell konfiguriert werden. Das Blade-Chassis muss als Blade-Chassis-Subtyp konfiguriert sein.

Für weitere Informationen darüber, wie Schichten angezeigt werden, siehe ***Port Access Page (Remote Console Display)*** (siehe "***Seite "Port Access" (Portzugriff) (Anzeige der Remotekonsole)***" auf Seite 17).

Konfigurieren von Blade-Chassis-Optionen

Mit Ausnahme von Blade-Chassis von HP und der UCS-Blade-Chassis von Cisco® werden generische Blade-Chassis und Blade-Chassis von IBM® und Dell® auf der Seite "Port" konfiguriert.

Der mit dem Blade-Chassis verbundene Port muss mit dem Blade-Chassis-Modell konfiguriert werden.

Die speziellen Konfigurationsmöglichkeiten für einen Bladeserver hängen von der Marke des Bladeservers ab, den Sie verwenden. Spezielle Informationen zu allen unterstützten Blade-Chassis finden Sie in den jeweiligen Themenbereichen in diesem Abschnitt des Hilfedokuments.

Dell

- Dell PowerEdgeR 1855, 1955 und M1000e

  Die Dell PowerEdge 1855/1955-Blades bieten außerdem die Möglichkeit, von jedem individuellen Blade aus eine Verbindung zu einem Port des Dominion-Geräts herzustellen. Wenn auf diese Weise eine Verbindung hergestellt wurde, können die Blades auch gruppiert werden und somit Bladeservergruppen bilden.

IBM

- IBM BladeCenter Modelle E und H

Generisch

- Eine generische Option ermöglicht Ihnen, einen Blade-Chassis zu konfigurieren, der nicht der folgende Server ist: einDell PowerEdge® 1855, 1955 und M1000e; HP BladeSystem c3000 und c7000; IBM BladeCenter® H, E und S; Cisco UCS B-Serie.

HP

- HP BladeSystem c3000 und c7000 sowie UCS-Blade-Server von Cisco werden über individuelle Verbindungen zwischen dem Dominion-Gerät und dem einzelnen Blade unterstützt.

  Die Ports werden mithilfe des Features "Port Group Management" (Portgruppenverwaltung) in einer Chassis-Darstellung gruppiert.

Manuelle und Auto-Discovery Konfigurierung von Blade-Chassis

Zwei Betriebsarten werden für Blade-Chassis zur Verfügung gestellt: Manuelle Konfiguration und automatische Erkennung.

Wenn ein Blade-Chassis für die automatische Erkennung konfiguriert wird, werden Zustandsänderungen in den folgenden Fällen vom Dominion-Gerät nachverfolgt und aktualisiert:

- Wenn ein neuer Bladeserver zum Chassis hinzugefügt wird.
- Wenn ein bestehender Bladeserver vom Chassis entfernt wird.

Hinweis: Bei den IBM-Blade-Center-Modellen E und H unterstützt der KX III nur die automatische Erkennung für AMM[1] als aktives primäres Verwaltungsmodul.

Kurzbefehl-Sequenzen zum Zugang Blade-Chassis

Außerdem wird die Verwendung von Tastenfolgen, um den KVM-Zugriff auf ein Blade-Chassis zu übertragen, unterstützt.

Die Optionen für Blade-Chassis, bei denen Benutzer eine Tastenkombination auswählen können, sind auf der Seite "Port Configuration" (Portkonfiguration) verfügbar.

Die Tastenfolgen für Blade-Chassis, bei denen diese vordefiniert sind, sind auf der Seite "Port Configuration" (Portkonfiguration) bereits in den entsprechenden Feldern eingegeben, wenn das Blade-Chassis ausgewählt wird.

Wenn die Standardtastenfolge für die Übertragung des KVM-Zugriffs auf ein IBM BladeCenter H beispielsweise "NumLock + NumLock + SlotNummer" lautet, wird diese Tastenfolge standardmäßig angewendet, wenn das IBM BladeCenter H während der Konfiguration ausgewählt wird. Weitere Informationen zu den Tastenfolgen finden Sie in der Dokumentation Ihres Blade-Chassis.

Blade-Chassis-Interface mit eine, anderen Port verbinden

Sie können die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Auf Chassis-Ebene können bis zu vier Verknüpfungen definiert werden.

Die erste Verknüpfung ist für die Verbindung zur Administrativmodul-GUI für Blade-Chassis reserviert.

Diese Verknüpfung kann beispielsweise vom technischen Kundendienst verwendet werden, um eine Chassis-Konfiguration schnell zu überprüfen.

Blade-Chassis Verwalten

Blade-Chassis können vom Virtual KVM Client (VKC), vom Active KVM Client (AKC) und von CC-SG verwaltet werden.

Das Verwalten von Bladeservern über den VKC und den AKC entspricht der Verwaltung von Standard-Zielservern.

Siehe Weitere Informationen finden Sie unter Arbeiten mit Zielservern **und im Administratorhandbuch** CC-SG Administrators Guide.

Hinweis: Alle Änderungen der Blade-Chassis-Konfiguration werden auf diese Client-Anwendungen übertragen.

Wichtig: Wenn das CIM, das das Blade-Chassis mit dem Dominion-Gerät verbindet, ausgeschaltet ist oder die Verbindung vom Dominion-Gerät getrennt wurde, werden alle bestehenden Verbindungen zum Blade-Chassis beendet. Wenn die Verbindung über das CIM wieder hergestellt ist oder dieses eingeschaltet wurde, müssen Sie die Verbindung(en) erneut herstellen.

Konfigurieren von generischen Blade-Chassis

Bei Auswahl der Option "Generic Blade Chassis" (generische Blade-Chassis) steht Ihnen nur die manuelle Konfiguration zur Verfügung. Weitere wichtige Informationen zur Konfiguration von Blade-Chassis finden Sie unter ***Unterstützte Blade-Chassis-Modelle*** (auf Seite 123), ***Unterstützte CIMs für Blade-Chassis*** (auf Seite 124) und ***Erforderliche und empfohlene Blade-Chassis-Konfigurationen*** (auf Seite 127). Informationen zu Kabellänge und Videoauflösungen bei der Verwendung des Dell®-Chassis mit KX III finden Sie unter ***Kabellängen und Videoauflösungen für Dell-Chassis*** (auf Seite 355).

So konfigurieren Sie ein Chassis:

1. Verbinden Sie das Blade-Chassis mit KX III. Weitere Einzelheiten finden Sie unter Schritt 3: Anschließen der Geräte.
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus, um die Seite "Port Configuration" (Portkonfiguration) zu öffnen.

3. Klicken Sie auf der Seite "Port Configuration" (Portkonfiguration) auf den Namen des Blade-Chassis, das Sie konfigurieren möchten. Die Seite "Port" wird angezeigt.
4. Aktivieren Sie das Optionsfeld "Blade Chassis" (Blade-Chassis). Auf der Seite werden nun die für die Konfiguration eines Blade-Chassis erforderlichen Felder angezeigt.
5. Wählen Sie aus der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) die Option "Generic" (Generisch) aus.
6. Konfigurieren Sie das Blade-Chassis wie gewünscht.
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Definieren Sie die Tastenfolge, die Sie verwenden möchten, um vom KVM zum Blade-Chassis zu wechseln. Die Tastenfolge zum Wechseln muss der Tastenfolge entsprechen, die im Blade-Chassis vom KVM-Modul verwendet wird.
   b. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Nicht zutreffend.
   c. Maximum Number of Slots (Maximale Anzahl an Slots) – Geben Sie die standardmäßige maximale Anzahl an Slots ein, die auf dem Blade-Chassis verfügbar sind.
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Nicht zutreffend.
   e. Username (Benutzername) – Nicht zutreffend.
   f. Password (Kennwort) – Nicht zutreffend.
7. Ändern Sie ggf. den Namen des Blade-Chassis.
8. Geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.
9. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen 

, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).

b. URL – Geben Sie die URL zur Benutzeroberfläche ein. **Erforderlich**

c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird. **Optional**

d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird. **Optional**

Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.

---

e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 119). **Optional**

10. USB-Profilinformationen sind für eine generische Konfiguration nicht verfügbar.
11. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
12. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.

Wählen Sie die systemeigene Anzeigeauflösung des CIMs aus der Dropdownliste "Display Native Resolution" (Systemeigene Auflösung) aus. Dies ist der bevorzugte Auflösungs- und Zeitabstimmungsmodus des digitalen CIM. Sobald Sie eine Auflösung ausgewählt haben, wird sie für das CIM übernommen.

1. Wenn keine Auflösung ausgewählt wird, wird die Standardauflösung 1024x1280@60Hz verwendet.
2. Klicken Sie zum Speichern der Konfiguration auf OK.

Konfigurieren von Dell-Blade-Chassis

Weitere wichtige Informationen zur Konfiguration von Blade-Chassis finden Sie unter ***Unterstützte Blade-Chassis-Modelle*** (auf Seite 123), ***Unterstützte CIMs für Blade-Chassis*** (auf Seite 124) und ***Erforderliche und empfohlene Blade-Chassis-Konfigurationen*** (auf Seite 127). Informationen zu Kabellänge und Videoauflösungen bei der Verwendung des Dell®-Chassis mit KX III finden Sie unter ***Kabellängen und Videoauflösungen für Dell-Chassis*** (auf Seite 355).

So fügen Sie ein Blade-Chassis hinzu:

1. Verbinden Sie das Blade-Chassis mit KX III. Weitere Einzelheiten finden Sie unter Schritt 3: Anschließen der Geräte.
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus, um die Seite "Port Configuration" (Portkonfiguration) zu öffnen.
3. Klicken Sie auf der Seite "Port Configuration" (Portkonfiguration) auf den Namen des Blade-Chassis, das Sie konfigurieren möchten. Die Seite "Port" wird angezeigt.
4. Aktivieren Sie das Optionsfeld "Blade Chassis" (Blade-Chassis). Auf der Seite werden nun die für die Konfiguration eines Blade-Chassis erforderlichen Felder angezeigt.
5. Wählen Sie aus der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) das Blade-Chassis-Modell von Dell aus.

So konfigurieren Sie ein Dell PowerEdge M1000e:

1. Wenn Sie das Dell PowerEdge M1000e ausgewählt haben, ist die automatische Erkennung verfügbar. Konfigurieren Sie das Blade-Chassis wie gewünscht. Vor der Konfiguration eines Blade-Chassis, das automatisch erkannt werden kann, muss dieses so konfiguriert werden, dass SSH-Verbindungen für die festgelegte Portnummer ermöglicht werden (siehe Device Services (Gerätedienste)). Außerdem muss zuvor auf dem Blade-Chassis ein Benutzerkonto mit den entsprechenden Authentifizierungsdaten erstellt werden.

a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Wählen Sie die Tastenfolge aus, die Sie verwenden möchten, um vom KVM zum Bladeserver zu wechseln. Die Tastenfolge zum Wechseln muss der Tastenfolge entsprechen, die im Blade-Chassis vom KVM-Modul verwendet wird.

b. Maximum Number of Slots (Maximale Anzahl an Slots) – Die standardmäßige maximale Anzahl an Slots, die auf dem Blade-Chassis verfügbar sind, wird automatisch eingegeben.

c. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Geben Sie die primäre IP-Adresse für das Blade-Chassis ein. **Erforderlich für den Auto-Discovery-Modus**

d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Ändern Sie ggf. die Portnummer. **Erforderlich für den Auto-Discovery-Modus**

e. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf das Blade-Chassis verwendet wird. **Erforderlich für den Auto-Discovery-Modus**

f. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf das Blade-Chassis verwendet wird. **Erforderlich für den Auto-Discovery-Modus**

2. Wenn Sie möchten, dass KX III Chassis-Blades automatisch erkennt, aktivieren Sie das Kontrollkästchen "Blade Auto-Discovery" (Automatische Blade-Erkennung) und klicken anschließend auf die Schaltfläche "Discover Blades on Chassis Now" (Blades auf Chassis jetzt suchen). Wenn die Blades erkannt wurden, werden sie auf der Seite angezeigt.

3. Ändern Sie ggf. den Namen des Blade-Chassis. Wenn das Chassis bereits benannt wurde, erscheint der Name automatisch in diesem Feld. Wenn es noch nicht benannt wurde, wird dem Chassis von KX III ein Name zugewiesen. Die Standard-Namenskonvention für Blade-Chassis durch KX III lautet "Blade_Chassis_Port#".

4. Wenn Sie sich im Modus "Manual" (Manuell) befinden, geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.

   Wenn Sie sich im Modus "Auto-discovery" (Automatische Erkennung) befinden, werden im Feld "Installed" (Installiert) die Slots angezeigt, die bei der Erkennung Blades enthalten.

5. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen 

, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).

   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für Dell M1000e finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis*** (auf Seite 130).

   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.

   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.

   ---

   e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 119).

6. USB-Profile sind für Dell-Chassis nicht verfügbar.
7. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
8. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.

Wählen Sie die systemeigene Anzeigeauflösung des CIMs aus der Dropdownliste "Display Native Resolution" (Systemeigene Auflösung) aus. Dies ist der bevorzugte Auflösungs- und Zeitabstimmungsmodus des digitalen CIM. Sobald Sie eine Auflösung ausgewählt haben, wird sie für das CIM übernommen.

1. Wenn keine Auflösung ausgewählt wird, wird die Standardauflösung 1024x1280@60Hz verwendet.
2. Klicken Sie zum Speichern der Konfiguration auf OK.

So konfigurieren Sie ein Dell PowerEdge 1855/1955:

1. Wenn Sie das Dell 1855/1955 ausgewählt haben, ist die automatische Erkennung *nicht verfügbar*. Konfigurieren Sie das Blade-Chassis wie gewünscht.
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Wählen Sie die Tastenfolge aus, die Sie verwenden möchten, um vom KVM zum Bladeserver zu wechseln. Bei den Modellen Dell 1855/1955 blockiert der KX III alle vorhandenen Tastenfolgen. Wenn Sie eine generische Konfiguration auf das Modell Dell 1855 anwenden, wird nur eine vorhandene Zugriffstaste blockiert.
   b. Maximum Number of Slots (Maximale Anzahl an Slots) – Die standardmäßige maximale Anzahl an Slots, die auf dem Blade-Chassis verfügbar sind, wird automatisch eingegeben.
   c. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Nicht zutreffend.
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Nicht zutreffend.
   e. Username (Benutzername) – Nicht zutreffend.
   f. Password (Kennwort) – Nicht zutreffend.
2. Ändern Sie ggf. den Namen des Blade-Chassis.

3. Geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.
4. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen 

, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für Dell PowerEdge 1855/1955 finden Sie unter Beispiel-URL-Formate für Blade-Chassis.
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.

   ---

e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 119).

5. USB-Profile sind für Dell-Chassis nicht verfügbar.
6. Klicken Sie zum Speichern der Konfiguration auf OK.

Konfigurieren von IBM-Blade-Chassis

Weitere wichtige Informationen zur Konfiguration von Blade-Chassis finden Sie unter ***Unterstützte Blade-Chassis-Modelle*** (auf Seite 123), ***Unterstützte CIMs für Blade-Chassis*** (auf Seite 124) und ***Erforderliche und empfohlene Blade-Chassis-Konfigurationen*** (auf Seite 127). Informationen zu Kabellänge und Videoauflösungen bei der Verwendung des Dell®-Chassis mit KX III finden Sie unter ***Kabellängen und Videoauflösungen für Dell-Chassis*** (auf Seite 355).

So fügen Sie ein Blade-Chassis hinzu:

1. Verbinden Sie das Blade-Chassis mit KX III. Weitere Einzelheiten finden Sie unter Schritt 3: Anschließen der Geräte.
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus, um die Seite "Port Configuration" (Portkonfiguration) zu öffnen.
3. Klicken Sie auf der Seite "Port Configuration" (Portkonfiguration) auf den Namen des Blade-Chassis, das Sie konfigurieren möchten. Die Seite "Port" wird angezeigt.
4. Aktivieren Sie das Optionsfeld "Blade Chassis" (Blade-Chassis). Auf der Seite werden nun die für die Konfiguration eines Blade-Chassis erforderlichen Felder angezeigt.
5. Wählen Sie aus der Dropdownliste „IBM®Blade Server Chassis Model" (Bladeserver-Chassis-Modell) das Blade-Chassis-Modell von Dell aus.

So konfigurieren Sie ein IBM BladeCenter H oder E:

1. Wenn Sie das IBM BladeCenter H oder E ausgewählt haben, ist die automatische Erkennung verfügbar. Konfigurieren Sie das Blade-Chassis wie gewünscht. Vor der Konfiguration eines Blade-Chassis, das automatisch erkannt werden kann, muss dieses so konfiguriert werden, dass SSH-Verbindungen für die festgelegte Portnummer ermöglicht werden (siehe Device Services (Gerätedienste)). Außerdem muss zuvor auf dem Blade-Chassis ein Benutzerkonto mit den entsprechenden Authentifizierungsdaten erstellt werden. KX III unterstützt nur die automatische Erkennung für AMM\[1].
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Vordefiniert
   b. Maximum Number of Slots (Maximale Anzahl an Slots) – Die standardmäßige maximale Anzahl an Slots, die auf dem Blade-Chassis verfügbar sind, wird automatisch eingegeben.
   c. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Geben Sie die primäre IP-Adresse für das Blade-Chassis ein. **Erforderlich für den Auto-Discovery-Modus**
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Ändern Sie ggf. die Portnummer. **Erforderlich für den Auto-Discovery-Modus**
   e. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf das Blade-Chassis verwendet wird. **Erforderlich für den Auto-Discovery-Modus**
   f. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf das Blade-Chassis verwendet wird. **Erforderlich für den Auto-Discovery-Modus**
2. Wenn Sie möchten, dass KX III Chassis-Blades automatisch erkennt, aktivieren Sie das Kontrollkästchen "Blade Auto-Discovery" (Automatische Blade-Erkennung) und klicken anschließend auf die Schaltfläche "Discover Blades on Chassis Now" (Blades auf Chassis jetzt suchen). Wenn die Blades erkannt wurden, werden sie auf der Seite angezeigt.
3. Ändern Sie ggf. den Namen des Blade-Chassis. Wenn das Chassis bereits benannt wurde, erscheint der Name automatisch in diesem Feld. Wenn es noch nicht benannt wurde, wird dem Chassis von KX III ein Name zugewiesen. Die Standard-Namenskonvention für Blade-Chassis durch KX III lautet "Blade_Chassis_Port#".
4. Wenn Sie sich im Modus "Manual" (Manuell) befinden, geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.

Wenn Sie sich im Modus "Auto-discovery" (Automatische Erkennung) befinden, werden im Feld "Installed" (Installiert) die Slots angezeigt, die bei der Erkennung Blades enthalten.

5. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen 

, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).

   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für IBM BladeCenter finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis.*** (siehe "***Beispiel-URL-Formate für Blade-Chassis***" auf Seite 130)

   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.

   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.

   ---

e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 119).

6. Definieren Sie ggf. das USB-Profil für das Blade-Chassis oder wählen Sie ein bestehendes USB-Profil aus. Klicken Sie auf das Symbol zum Auswählen des USB-Profils für einen Port 

oder das Symbol zum Übernehmen von ausgewählten Profilen für sonstige Ports 

, um die entsprechenden Abschnitte der Seite zu erweitern. Siehe ***Konfigurieren von USB-Profilen (Seite "Port")*** (auf Seite 131).

7. Klicken Sie zum Speichern der Konfiguration auf OK.

So konfigurieren Sie ein IBM BladeCenter (Sonstige):

1. Wenn Sie "IBM BladeCenter (Other)" [IBM BladeCenter (Sonstige)] ausgewählt haben, ist die automatische Erkennung *nicht* verfügbar. Konfigurieren Sie das Blade-Chassis wie gewünscht.

   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Wählen Sie die Tastenfolge aus, die Sie verwenden möchten, um vom KVM zum Bladeserver zu wechseln.

   b. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Geben Sie die primäre IP-Adresse für das Blade-Chassis ein. Nicht zutreffend.

   c. Maximum Number of Slots (Maximale Anzahl an Slots) – Geben Sie die standardmäßige maximale Anzahl an Slots ein, die auf dem Blade-Chassis verfügbar sind.

   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Nicht zutreffend.

   e. Username (Benutzername) – Nicht zutreffend.

   f. Password (Kennwort) – Nicht zutreffend.

2. Ändern Sie ggf. den Namen des Blade-Chassis.

3. Geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen. Wenn er noch nicht benannt wurde, wird dem Bladeserver von KX III ein Name zugewiesen. Die Standard-Namenskonvention für Bladeserver lautet "Blade_Chassis_Port#_Slot#".
4. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen 

, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für IBM BladeCenter finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis.*** (siehe "***Beispiel-URL-Formate für Blade-Chassis***" auf Seite 130)
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.

e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 119).

5. USB-Profile werden für Konfigurationen von IBM (Sonstige) nicht verwendet.
6. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
7. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.

Wählen Sie die systemeigene Anzeigeauflösung des CIMs aus der Dropdownliste "Display Native Resolution" (Systemeigene Auflösung) aus. Dies ist der bevorzugte Auflösungs- und Zeitabstimmungsmodus des digitalen CIM. Sobald Sie eine Auflösung ausgewählt haben, wird sie für das CIM übernommen.

1. Wenn keine Auflösung ausgewählt wird, wird die Standardauflösung 1024x1280@60Hz verwendet.
2. Klicken Sie zum Speichern der Konfiguration auf OK.

Tipps zum Hinzufügen einer Webbrowseroberfläche

Sie können eine Webbrowseroberfläche hinzufügen, um eine Verbindung zu einem Gerät mit einem eingebetteten Webserver herzustellen. Eine Webbrowseroberfäche kann außerdem verwendet werden, um eine Verbindung mit einer beliebigen Webanwendung herzustellen (z. B. die Webanwendung, die einer RSA-, DRAC- oder ILO-Prozessorkarte zugeordnet ist).

Dazu müssen Sie DNS konfigurieren, ansonsten werden URLs nicht umgewandelt. Für IP-Adressen müssen Sie DNS nicht konfigurieren.

So fügen Sie eine Webbrowseroberfläche hinzu:

1. Der Standardname für eine Webbrowseroberfläche wird bereitgestellt. Ändern Sie den Namen ggf. im Feld "Name".

2. Geben Sie die URL oder den Domainnamen der Webanwendung in das URL-Feld ein. Sie müssen die URL eingeben, bei der die Webanwendung normalerweise den Benutzernamen und das Kennwort ablesen kann.

   Folgen Sie unten angegebenen Beispielen, um korrekte Formate zu erhalten:

   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html

3. Geben Sie den Benutzernamen und das Kennwort ein, mit denen Sie auf diese Benutzeroberfläche zugreifen können. **///Optional**
4. Wenn Sie den Benutzernamen und das Kennwort eingegebne haben, geben Sie in die Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, die auf der Anmeldeseite der Webanwendung verwendet werden. Sie müssen die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feldnamen zu suchen (nicht die Feldbezeichnungen).

Tipp zum Suchen von Feldnamen:

- Suchen Sie im HTML-Quellcode der Anmeldeseite der Webanwendung nach der Bezeichnung des Feldes [z. B. "Username" (Benutzername) oder "Password" (Kennwort)].
- Wenn Sie die Feldbezeichnung gefunden haben, suchen Sie im nebenstehenden Code nach einem Tag, der folgendermaßen aussieht: name="user". Das Wort in Anführungszeichen ist der Feldname.

Konfigurieren von HP- und Cisco UCS-Blade-Chassis (Portgruppenverwaltung)

KX III unterstützt den Zusammenschluss von Ports, die mit verschiedenen Bladetypen verbunden sind, zu einer Gruppe, die das Blade-Chassis repräsentiert. Speziell Cisco® UCS, HP®BladeServer-Blades und Dell® PowerEdge™ 1855/1955-Blades, wenn das DellPowerEdge 1855/1955 von jedem individuellen Blade aus mit einem Port auf KX III verbunden ist.

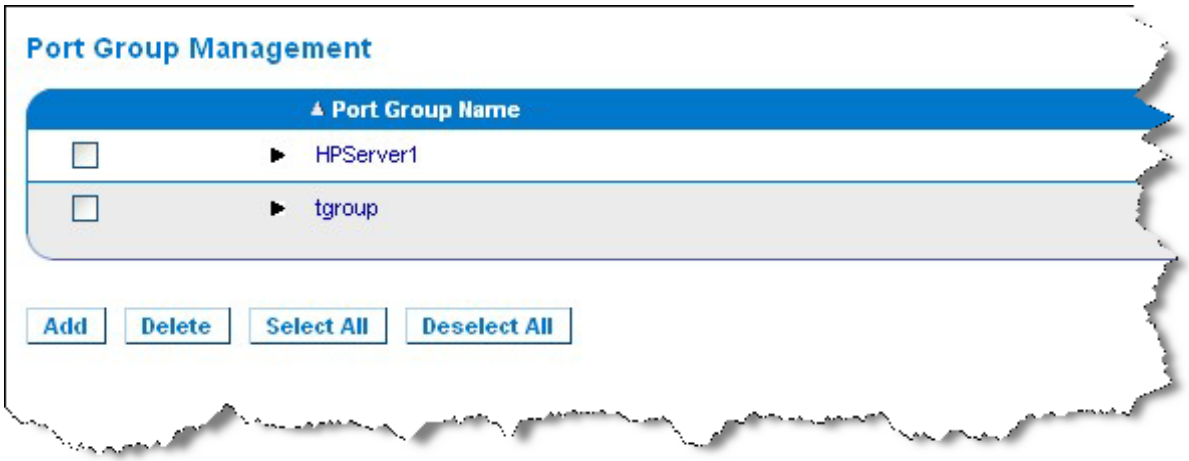
Das Chassis wird durch einen Portgruppennamen identifiziert, und die Gruppe wird als Bladeservergruppe auf der Seite "Port Group Management" (Portgruppenverwaltung) festgelegt. Portgruppen bestehen nur aus Ports, die als Standard-KVM-Ports konfiguriert wurden, nicht aus Ports, die als Blade-Chassis konfiguriert wurden. Ein Port kann nur einer einzigen Gruppe angehören.

Ports, die mit integrierten KVM-Modulen in einem Blade-Chassis verbunden sind, werden als Blade-Chassis-Untertypen konfiguriert. Diese Ports können in Portgruppen aufgenommen werden.

Wenn KX III Ports mit integrierten KVM-Modulen in einem Blade-Chassis, nicht mit einzelnen Blades, verbunden sind, werden die Ports als Blade-Chassis-Untertypen konfiguriert. Diese Ports können nicht in Portgruppen aufgenommen werden und werden nicht in der Liste "Select Port for Group, Available" (Port für Gruppe auswählen, Verfügbar) angezeigt.

Wenn ein Standard-KVM-Port in eine Portgruppe aufgenommen wurde und somit im Folgenden als Blade-Chassis-Subtyp verwendet wird, muss dieser Port zunächst aus der Portgruppe entfernt werden.

Portgruppen werden mithilfe der Option "Backup and Restore" (Sicherung und Wiederherstellung) wiederhergestellt (siehe ***Backup and Restore*** (siehe "***Backup/Restore (Sicherung/Wiederherstellung)***" auf Seite 199) (Sicherung und Wiederherstellung)).



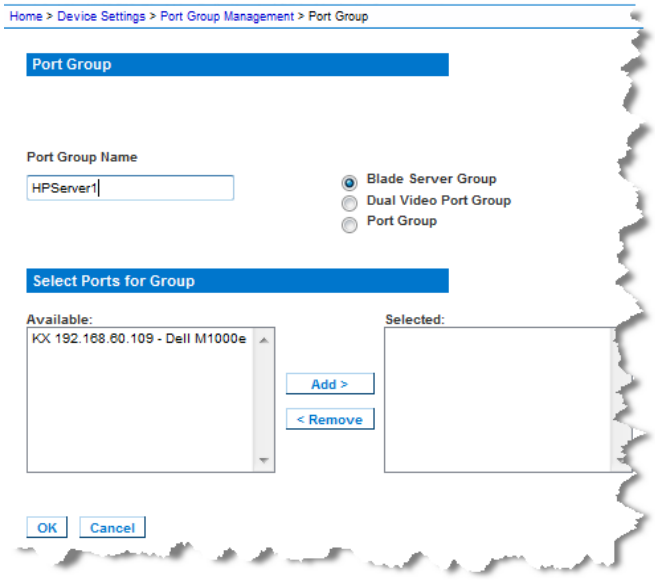
So fügen Sie eine Portgruppe hinzu:

1. Klicken Sie auf "Device Settings" "Port Group Management" (Geräteeinstellungen > Portgruppenverwaltung), um die Seite "Port Group Management" (Portgruppenverwaltung) zu öffnen.
2. Klicken Sie auf die Schaltfläche "Add" (Hinzufügen), um die Seite "Port Group" (Portgruppe) zu öffnen.
3. Geben Sie unter "Port Group Name" (Portgruppenname) einen Portgruppennamen ein. Dabei müssen Sie die Groß-/Kleinschreibung nicht beachten. Der Portgruppenname kann bis zu 32 Zeichen umfassen.
4. Aktivieren Sie das Kontrollkästchen "Blade Server Group" (Bladeservergruppe).

   Wenn Sie festlegen möchten, dass diese Ports zu Blades in einem Blade-Chassis zugeordnet werden (z. B. HP c3000 oder Dell PowerEdge 1855), aktivieren Sie das Kontrollkästchen "Blade Server Group" (Bladeservergruppe).

   Hinweis: Dies ist besonders wichtig für CC-SG-Benutzer, die HP-Blades auf Chassis-Basis organisieren möchten; jedes Blade verfügt jedoch über eine eigene Verbindung zu einem Port auf KX III.

5. Klicken Sie im Abschnitt "Select Ports for Group" (Port für Gruppe auswählen) im Feld "Available" (Verfügbar) auf einen Port. Klicken Sie auf "Add" (Hinzufügen), um den Port zur Gruppe hinzuzufügen. Der Port wird in das Feld "Selected" (Ausgewählt) verschoben.
6. Klicken Sie auf OK, um die Portgruppe hinzuzufügen.



So bearbeiten Sie Portgruppeninformationen:

1. Klicken Sie auf der Seite "Port Group Management" (Portgruppenverwaltung) auf die Verknüpfung der Portgruppe, die Sie bearbeiten möchten. Die Seite "Port Group" (Portgruppe) wird angezeigt.
2. Bearbeiten Sie die Informationen wie gewünscht.
3. Klicken Sie zum Speichern der Änderungen auf OK.

So löschen Sie eine Portgruppe:

1. Klicken Sie auf die Seite "Port Group Management" (Portgruppenverwaltung) und aktivieren Sie das Kontrollkästchen der Portgruppe, die Sie löschen möchten.
2. Klicken Sie auf Löschen.
3. Bestätigen Sie die Warnungsmeldung mit OK.

Unterstützte Blade-Chassis-Modelle

Die Tabelle enthält die Blade-Chassis-Modelle, die von KX III unterstützt werden, sowie die entsprechenden Profile, die pro Chassis-Modell ausgewählt werden sollten, wenn sie in der KX III Anwendung konfiguriert werden. Eine Liste dieser Modelle kann auf der Seite "Port Configuration"(Portkonfiguration) in der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) ausgewählt werden. Diese Liste wird angezeigt, wenn das Optionsfeld "Blade Chassis" (Blade-Chassis) ausgewählt wurde. Weitere Informationen zur Konfiguration der einzelnen Blade-Chassis-Modelle finden Sie in den jeweiligen Themenbereichen in diesem Abschnitt des Hilfedokuments.

Blade-Chassis-Modell	KX III Profil
Cisco® UCS	Konfiguration mithilfe der Funktionen der Portgruppenverwaltung Siehe ***Konfigurieren von HP- und Cisco UCS-Blade-Chassis (Portgruppenverwaltung)*** (auf Seite 121)
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E

Blade-Chassis-Modell	KX III Profil
HP®	Konfiguration mithilfe der Funktionen der Portgruppenverwaltung Siehe ***Konfigurieren von HP- und Cisco UCS-Blade-Chassis (Portgruppenverwaltung)*** (auf Seite 121)

Unterstützte CIMs für Blade-Chassis

Die folgenden CIMs werden für Blade-Chassis, die über KX III verwaltet werden, unterstützt:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Die folgende Tabelle enthält unterstützte CIMs für alle Blade-Chassis-Modelle, die von KX III unterstützt werden.

Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
Generisch	Wenn bei der Verbindungsherstellung zu einem als generisch konfigurierten Blade-Chassis ein D2CIM-VUSB oder D2CIM-DVUSB verwendet wird, können Sie die USB-Profile von der Seite "Port Configuration" (Portkonfiguration) und dem USB-Profilmenü des Client auswählen. Virtuelle Medien werden jedoch für generische Blade-Chassis nicht unterstützt, und das Menü "Virtual Media" (Virtuelle Medien) ist im Client deaktiviert.	• DCIM-PS2 • DCIM-USBG2
Cisco® UCS Server-Chassis	Mit dem KVM-Kabel (N20-BKVM) von Cisco können Sie die Verfahren zur Verwaltung, Konfiguration und Diagnose von Serverblades durchführen, indem Sie Grafik- und USB-Geräte direkt mit dem Serverblade verbinden. Quelle: *Cisco UCS 5108 Server Chassis Installation Guide (Installationshandbuch für Server-Chassis)*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB

Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
Dell® PowerEdge™ 1855	Beinhaltet eines der drei KVM-Module: • Analog KVM Ethernet switch module (Analoges KVM-Ethernet-Switchmodul) – Standard • Digital Access KVM switch module (KVM-Switchmodul für digitalen Zugriff) – Optional • KVM switch module (KVM-Switchmodul) – Standard auf Systemen, die vor April 2005 verkauft wurden Diese Switches bieten einen benutzerdefinierten Anschluss, mit dem Sie zwei PS/2 und ein Grafikgerät am System anschließen können. Quelle: *Benutzerhandbuch Dell Poweredge 1855*	• DCIM-PS2
Dell PowerEdge 1955	Einer dieser beiden KVM-Modultypen kann installiert werden: • Analog KVM switch module (Analoges KVM-Switchmodul) • Digital Access KVM switch module (KVM-Switchmodul für digitalen Zugriff) Beide Module ermöglichen es Ihnen, ein(e) PS/2-kompatible Tastatur, Maus und Videomonitor am System anzuschließen (mithilfe eines benutzerdefinierten Kabels, das mit dem System bereitgestellt wird). Quelle: *Betriebsanleitung Dell Poweredge 1955*	• DCIM-PS2
Dell PowerEdge M1000e	Das KVM-Switchmodul (iKVM) ist in diesem Chassis integriert. Das iKVM ist kompatibel mit folgenden Peripheriegeräten: • USB-Tastaturen, USB-Zeigegeräte • VGA-Monitore mit DDC-Unterstützung Quelle: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide (Benutzerhandbuch Dell Chassis Management Controller, Firmware-Version 1.0)*	• DCIM-USBG2
HP® BladeSystem c3000	Mit dem c-Class Blade SUV-Kabel von HP können Sie die Verfahren zur Verwaltung, Konfiguration und Diagnose von Blade-Chassis	• DCIM-USBG2 • D2CIM-VUSB

Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
	durchführen, indem Sie Grafik- und USB-Geräte direkt mit dem Serverblade verbinden. Quelle: *HP Proliant™ BL480c Server Blade Maintenance and Service Guide (Instandhaltungs- und Servicehandbuch HP Proliant BL480c-Serverblade)*	• D2CIM-DVUSB (für Standard-KVM-Port betrieb ohne KVM-Option)
HP BladeSystem c7000	Mit dem c-Class Blade SUV-Kabel von HP können Sie die Verfahren zur Verwaltung, Konfiguration und Diagnose von Serverblades durchführen, indem Sie Grafik- und USB-Geräte direkt mit dem Serverblade verbinden. Quelle: *HP ProLiant BL480c Server Blade Maintenance and Service Guide (Instandhaltungs- und Servicehandbuch HP ProLiant BL480c-Serverblade)*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (für Standard-KVM-Port betrieb)
IBM® BladeCenter® S	Das Advanced Management Module (AMM) bietet Systemverwaltungsfunktionen und (KVM-)Multiplexverfahren (Tastatur/Video/Maus) für alle Blade-Chassis. Zu den AMM-Anschlüssen zählen: serieller Port, Videoverbindung, Remoteverwaltungsport (Ethernet) sowie zwei USB v2.0-Ports für Tastatur und Maus Quelle: *Implementing the IBM BladeCenter S Chassis (Implementierungsanleitung IBM BladeCenter S Chassis)*	• DCIM-USBG2
IBM BladeCenter H	Im Lieferumfang des BladeCenter H-Chassis ist standardmäßig ein Advanced Management Module enthalten. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	Im Lieferumfang des aktuellen Chassis-Modells "BladeCenter E" (8677-3Rx) ist standardmäßig ein Advanced Management Module enthalten. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	Im Lieferumfang des BladeCenter T-Chassis ist standardmäßig ein Advanced Management	• DCIM-PS2

Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
	Module enthalten. Im Gegensatz zum Standard-BladeCenter-Chassis bestehen das KVM-Modul und das Management Module im BladeCenter T-Chassis aus separaten Komponenten. Auf der Vorderseite des Verwaltungsmoduls sind nur die LEDs zur Anzeige des Status vorhanden. Alle Ethernet- und KVM-Verbindungen werden von der Rückseite aus mit den LAN- und KVM-Modulen verbunden. Das KVM-Modul ist ein Hot-Swap-Modul auf der Rückseite des Chassis und verfügt über zwei PS/2-Anschlüsse für Tastatur und Maus, ein Systemstatuspanel sowie einen HD-15-Videoanschluss. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	
IBM BladeCenter HT	Im Lieferumfang des BladeCenter HT-Chassis ist standardmäßig ein Advanced Management Module enthalten. Mit diesem Modul können Sie das Chassis verwalten sowie die lokale KVM-Funktion übernehmen. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	• DCIM-USBG2

Hinweis: Die IBM BladeCenter-Modelle H und E müssen für die Unterstützung der automatischen Erkennung AMM mit der Firmwareversion BPET36K oder höher verwenden.

Hinweis: Bei den IBM-Blade-Center-Modellen E und H unterstützt der KX III nur die automatische Erkennung für AMM[1] als aktives primäres Verwaltungsmodul.

Hinweis: Audio wird für alle KVM-Switch-Ziele deaktiviert.

Erforderliche und empfohlene Blade-Chassis-Konfigurationen

Diese Tabelle enthält Informationen zu Beschränkungen, die für die Konfiguration von Blade-Chassis für KX III gelten. Raritan empfiehlt, die folgenden Informationen zu beachten.

Blade-Chassis	Erforderliche/empfohlene Aktion
Dell® PowerEdge™ M1000e	▪ Deaktivieren Sie den iKVM-GUI-Bildschirmschoner. Ansonsten wird ein Autorisierungsdialogfenster angezeigt, wodurch das iKVM nicht korrekt funktioniert. ▪ Verlassen Sie das iKVM-GUI-Menü, bevor Sie das Dell-Chassis an ein CIM von Raritan anschließen. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Konfigurieren Sie das Hauptmenü der iKVM-GUI so, dass Zielblades nach Slot und nicht nach Name ausgewählt werden. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Wählen Sie im Scan-Setupmenü der iKVM-GUI *keine* Slots für Scanvorgänge aus. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Wählen Sie im Scan-Broadcastmenü der iKVM-GUI *keine* Slots für Tastatur-/Maus-Broadcastvorgänge aus. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Legen Sie zum Aufrufen der iKVM-GUI eine einzelne Tastenfolge fest. Diese Tastenfolge muss auch während der KX III Portkonfiguration identifiziert werden. Ansonsten kann dies zu ungewollten iKVM-Vorgängen aufgrund von Client-Zugriffstasteneingaben führen. ▪ Stellen Sie sicher, dass "Front Panel USB/Video Enabled" (USB/Video auf Vorderseite aktiviert) bei der iKVM-Konfiguration über die Dell-CMC-GUI *nicht* ausgewählt wurde. Ansonsten haben Verbindungen über die Vorderseite des Chassis Priorität vor der KX III Verbindung auf der Rückseite, sodass der iKVM-Betrieb nicht ordnungsgemäß funktioniert. Die Meldung "User has been disabled as front panel is currently active" (Der Benutzer wurde deaktiviert, da die Vorderseite zurzeit aktiv ist) wird angezeigt. ▪ Stellen Sie sicher, dass "Allow access to CMC CLI from iKVM" (Zugriff auf CMC CLI vom iKVM zulassen) bei der iKVM-Konfiguration über die Dell-CMC-GUI *nicht* ausgewählt wurde. ▪ Um zu verhindern, dass die iKVM-GUI bei der Verbindungsherstellung zum Blade-Chassis angezeigt wird, stellen Sie unter "Screen Delay Time" (Bildschirmverzögerungszeit) die Verzögerungszeit auf 8 Sekunden. ▪ Es wird empfohlen, dass während des iKVM-GUI-Flagsetup die Optionen "Timed" (Abgestimmt) und "Displayed" (Angezeigt) ausgewählt werden. Dadurch können Sie die Verbindung zum gewünschten Bladeslot visuell bestätigen.
Dell PowerEdge 1855/1955	▪ Deaktivieren Sie den iKVM-GUI-Bildschirmschoner. Ansonsten wird ein Autorisierungsdialogfenster angezeigt, wodurch das iKVM nicht korrekt funktioniert.

Blade-Chassis	Erforderliche/empfohlene Aktion
	▪ Verlassen Sie das iKVM-GUI-Menü, bevor Sie das Dell-Chassis an ein CIM von Raritan anschließen. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Konfigurieren Sie das Hauptmenü der iKVM-GUI so, dass Zielblades nach Slot und nicht nach Name ausgewählt werden. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Wählen Sie im Scan-Setupmenü der iKVM-GUI *keine* Slots für Scanvorgänge aus. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. ▪ Um zu verhindern, dass die iKVM-GUI bei der Verbindungsherstellung zum Blade-Chassis angezeigt wird, stellen Sie unter "Screen Delay Time" (Bildschirmverzögerungszeit) die Verzögerungszeit auf 8 Sekunden. ▪ Es wird empfohlen, dass während des iKVM-GUI-Flagsetup die Optionen "Timed" (Abgestimmt) und "Displayed" (Angezeigt) ausgewählt werden. Dadurch können Sie die Verbindung zum gewünschten Bladeslot visuell bestätigen.
IBM®/Dell® Auto-Discovery	▪ Es wird empfohlen, die automatische Erkennung zu aktivieren, wenn Sie Zugriffsberechtigungen auf Blade-Ebene anwenden. Ansonsten sollten Sie Zugriffsberechtigungen auf Blade-Chassis-Ebene vergeben. ▪ Secure Shell (SSH) muss auf dem Verwaltungsmodul des Blade-Chassis aktiviert sein. ▪ Der SSH-Port, der auf dem Managementmodul des Blade-Chassis konfiguriert, und die Portnummer, die auf der Seite "Port Configuration" (Portkonfiguration) eingegeben wurde, müssen übereinstimmen.
IBM KX3 Virtuelle Medien	▪ Raritan KX III Virtual Media (Virtuelle Medien wird nur von IBM BladeCenter® Modellen H and E unterstützt. Dies erfordert die Benutzung von D2CIM-DVUSB. Der schwarze D2CIM-DVUS-USB-Niedriggeschwindigkeitsanschluss ist auf der Rückseite der Einheit mit dem Administrative Management Module (AMM) verbunden. Der graue D2CIM-DVUS-USB-Hochgeschwindigkeitsanschluss ist auf der Vorderseite der Einheit mit dem Media Tray (MT) verbunden. Dazu benötigen Sie ein USB-Verlängerungskabel.
Cisco® UCS Server-Chassis	▪ Mit dem KVM-Kabel (N20-BKVM) von Cisco können Sie die Verfahren zur Verwaltung, Konfiguration und Diagnose von Serverblades durchführen, indem Sie Grafik- und USB-Geräte direkt mit dem Serverblade verbinden. ▪ Quelle: *Cisco UCS 5108 Server Chassis Installation Guide- DCIM-USBG2- D2CIM-VUSB- D2CIM-DVUSB (Installationshandbuch für Server-Chassis)*

Hinweis: Alle IBM BladeCenter, die AMM verwenden, müssen die AMM mit der Firmwareversion BPET36K oder höher verwenden, um die Funktion mit KX III sicherzustellen.

Hinweis: Bei den IBM-Blade-Center-Modellen E und H unterstützt der KX III nur die automatische Erkennung für AMM[1] als aktives primäres Verwaltungsmodul.

Beispiel-URL-Formate für Blade-Chassis

Diese Tabelle enthält Beispiel-URL-Formate für Blade-Chassis, die in KX III konfiguriert wurden.

Blade-Chassis	Beispiel-URL-Format
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login • Benutzername: root • Benutzernamenfeld: user • Password: calvin • Kennwortfeld: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • Benutzername: root • Benutzernamenfeld: TEXT_USER_NAME • Password: calvin • Kennwortfeld: TEXT_PASSWORD
IBM® BladeCenter® E oder H	• http://192.168.84.217/private/welcome.ssi

Konfigurieren von USB-Profilen (Seite "Port")

Im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen) auf der Seite "Port" wählen Sie die verfügbaren USB-Profile für einen Port aus. Die auf der Seite "Port" ausgewählten USB-Profile sind die Profile, die für den Benutzer im VKC verfügbar sind, wenn von diesem Port eine Verbindung zu einem KVM-Zielserver hergestellt wird. Die standard Betriebssysteme sind Windows 2000®, Windows XP®, Windows Vista®. Weitere Informationen zu USB-Profilen finden Sie unter USB-Profile.

Hinweis: Um USB-Profile für einen Port festzulegen, muss eine Verbindung zu einem digitalen CIM, VM-CIM oder dualen VM-CIM bestehen, das über die Firmware verfügt, die mit der aktuellen Firmwareversion des KX III kompatibel ist. Siehe **Aktualisieren von CIMs** *(auf Seite 203).*

Die Profile, die für die Zuordnung zu einem Port verfügbar sind, werden in der Liste "Available" (Verfügbar) auf der linken Bildschirmseite angezeigt. Die Profile, die für die Verwendung mit einem Port ausgewählt wurden, werden in der Liste "Selected" (Ausgewählt) auf der rechten Bildschirmseite angezeigt. Wenn Sie in einer der Listen ein Profil auswählen, wird im Feld "Profile Description" (Profilbeschreibung) eine Beschreibung des Profils und dessen Verwendung angezeigt.

Neben der Auswahl einer Reihe von Profilen für einen KVM-Port können Sie außerdem das bevorzugte Profil für den Port angeben und die für einen Port festgelegten Einstellungen für andere KVM-Ports übernehmen.

Hinweis: Informationen zur Verwendung des Mac OS-X-USB-Profils, wenn Sie ein DCIM-VUSB oder DCIM-DVUSB verwenden, finden Sie unter **Mausmodi bei Verwendung des Mac OS-X-USB-Profils** *(siehe "***Mausmodi bei Verwendung des Mac Boot Menü***" auf Seite 56)mit einem DCIM-VUSB.*

So öffnen Sie die Seite "Port":

1. Wählen Sie „Geräteeinstellungen Portkonfiguration". Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des KVM-Ports, den Sie bearbeiten möchten. Die Seite "Port" wird angezeigt.

So wählen Sie die USB-Profile für einen KVM-Port aus:

1. Wählen Sie im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen) ein oder mehrere USB-Profile aus der Liste "Available" (Verfügbar) aus.
   - Halten Sie die Umschalttaste gedrückt und wählen Sie mit der Maus die gewünschten aufeinander folgenden Profile aus.

- Halten Sie die Strg-Taste gedrückt und wählen Sie mit der Maus die gewünschten nicht aufeinander folgenden Profile aus.

2. Klicken Sie auf Hinzufügen. Die ausgewählten Profile werden in der Liste "Selected" (Ausgewählt) angezeigt. Dies sind die Profile, die für den mit dem Port verbundenen KVM-Zielserver verwendet werden können.

So legen Sie ein bevorzugtes USB-Profil fest:

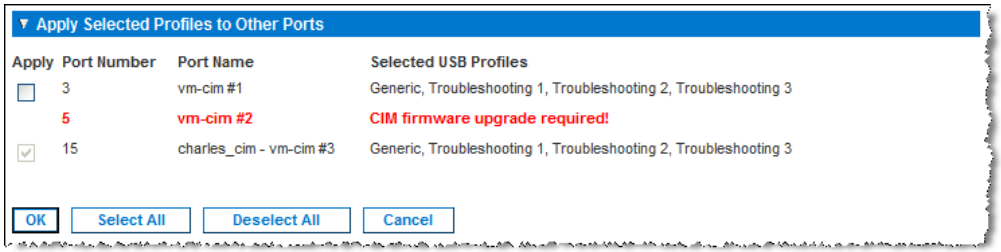
1. Nachdem Sie die verfügbaren Profile für einen Port ausgewählt haben, wählen Sie eines aus dem Menü "Preferred Profile for Port" (Bevorzugtes Profil für Port) aus. Standardmäßig ist das generische Profil festgelegt. Das ausgewählte Profil wird bei der Verbindungsherstellung zum KVM-Zielserver verwendet. Sie können bei Bedarf jedes andere USB-Profil verwenden.
2. Wenn der Checkbox „Aktives Profil wie bevorzugt“ ausgewählt ist, wird diese bevorzugte USB auch als aktives Profil verwendet.

So entfernen Sie ausgewählte USB-Profile:

1. Wählen Sie im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen) ein oder mehrere Profile aus der Liste "Selected" (Ausgewählt) aus.
   - Halten Sie die Umschalttaste gedrückt und wählen Sie mit der Maus die gewünschten aufeinander folgenden Profile aus.
   - Halten Sie die Strg-Taste gedrückt und wählen Sie mit der Maus die gewünschten nicht aufeinander folgenden Profile aus.
2. Klicken Sie auf "Remove" (Entfernen). Die ausgewählten Profile werden in der Liste "Available" (Verfügbar) angezeigt. Diese Profile sind nicht mehr für einen mit diesem Port verbundenen KVM-Zielserver verfügbar.

So übernehmen Sie eine Profilauswahl für mehrere Ports:

1. Aktivieren Sie im Abschnitt "Apply Selected Profiles to Other Ports" (Ausgewählte Profile für andere Ports übernehmen) das Kontrollkästchen "Apply" (Übernehmen) für alle KVM-Ports, für die Sie die aktuelle Auswahl an USB-Profilen übernehmen möchten.



   - Klicken Sie auf "Select All" (Alle auswählen), um alle KVM-Ports auszuwählen.

- Klicken Sie auf "Deselect All" (Auswahl aufheben), um die Auswahl der KVM-Ports aufzuheben.

Lokale KX III Porteinstellungen konfigurieren

Hinweis: Einige Einstellungsänderungen, die auf der Seite "Local Port Settings" (Lokale Porteinstellungen) vorgenommen werden, führen zum Neustart des verwendeten Browsers. Führt eine Einstellungsänderung zum Neustart des Browsers, so ist dies in den hier beschriebenen Schritten vermerkt.

So konfigurieren Sie die lokalen Porteinstellungen:

- Wählen Sie "Device Settings“ "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus. Die Seite "Local Port Settings" (Lokale Porteinstellungen) wird angezeigt.

Standard Lokaler Port Aktivieren

1. Aktivieren Sie das Kontrollkästchen neben "Enable Standard Local Port" (Lokalen Standardport aktivieren). Deaktivieren Sie das Kontrollkästchen, um den Port zu deaktivieren.

   Der lokale Standardport ist standardmäßig aktiviert, kann jedoch bei Bedarf aktiviert werden.

   Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.

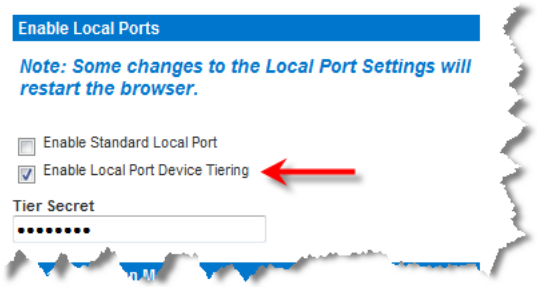
   Hinweis: Wenn Sie die Schichtfunktion verwenden, ist die Standard Local Port Funktion deaktiviert, da beide Funktionen nicht gleichzeitig verwendet werden können.

"Enable Local Port Device Tiering" (Lokaler Port für Geräteschichten aktivieren).

1. Wenn Sie die Schichtfunktion verwenden, wählen Sie das Kontrollkästchen "Enable Local Port Device Tiering" (Geräteschicht für lokalen Port aktivieren) aus und geben den geheimen Schlüssel für die Schicht in das Feld "Tier Secret" (Geheimer Schlüssel der Schicht) ein.

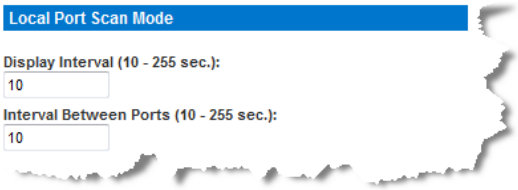
   Um die Schichten zu konfigurieren, müssen Sie auch das Basisgerät auf der Seite "Device Services" (Gerätedienste) konfigurieren.

Weitere Informationen zu Schichten finden Sie unter Konfigurieren und Aktivieren von Schichten.



Konfigurieren Sie ggf. die Einstellungen "Local Port Scan Mode" (Scanmodus für den lokalen Port)

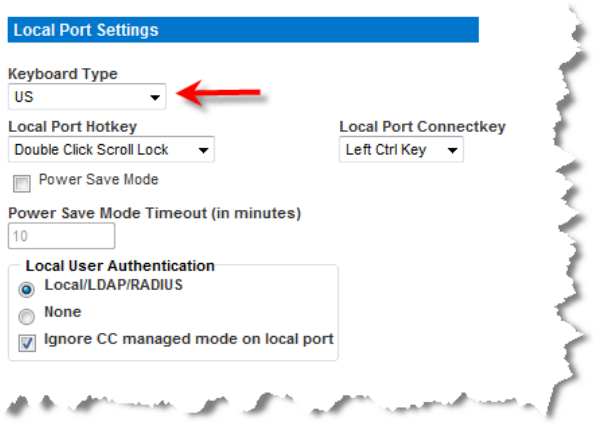
1. Konfigurieren Sie ggf. die Einstellungen "Local Port Scan Mode" (Scanmodus für den lokalen Port). Diese Einstellungen gelten für das Feature "Scan Settings" (Scaneinstellungen), auf das Sie über die Seite "Port" zugreifen. Siehe Scannen von Ports.
   - Geben Sie im Feld "Display Interval (10-255 sec):" (Anzeigeintervall (10-255 Sek.)) die Anzahl Sekunden ein, die das Ziel im Fokus in der Mitte des Fensters "Port Scan" (Port-Scan) angezeigt werden soll.
   - Geben Sie im Feld "Interval Between Ports (10 - 255 sec):" (Intervall zwischen Ports (10 – 255 Sek.)) das Intervall ein, in dem das Gerät zwischen Ports pausieren soll.



Lokalen Konsol-Tastaturtyp Wählen

1. Wählen Sie aus den Optionen in der Dropdown-Liste den geeigneten Tastaturtyp aus.

Der Browser wird neu gestartet, sobald diese Änderung vorgenommen ist.



- US
- US/International (USA/International)
- United Kingdom (Großbritannien)
- Französisch (Frankreich)
- Deutsch (Deutschland)
- Deutsch (Schweiz)
- Simplified Chinese (Vereinfachtes Chinesisch)
- Traditional Chinese (Traditionelles Chinesisch)
- Dubeolsik Hangul (Korean) (Koreanisch)
- JIS (Japanese Industry Standard) (Japanisch [Japanischer Branchenstandard])
- Portugiesisch (Portugal)
- Norwegisch (Norwegen)
- Schwedisch (Schweden)
- Dänisch (Dänemark)
- Belgian (Belgium) (Belgisch)
- Ungarisch
- Spanisch
- Italienisch
- Slowenisch

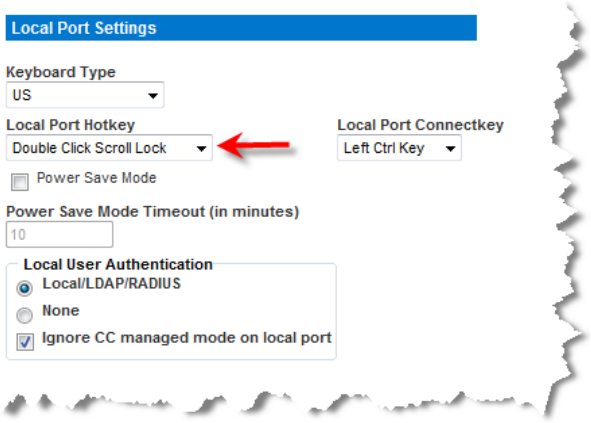
Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen KX III Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

Hinweis: Bei Verwendung einer türkischen Tastatur müssen Sie die Verbindung mit einem Zielserver über den Active KVM Client (AKC) herstellen. Von anderen Raritan-Clients wird es nicht unterstützt.

Wählen Sie unter Local Port Hotkey eine Zugriffstaste für den lokalen Port aus.

1. Wählen Sie die Zugriffstaste für den lokalen Port. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen KX III-Konsole zurückkehren, wenn gerade eine Zielserveroberfläche angezeigt wird. Die Standardoption lautet "Double Click Scroll Lock" (Rollen-Taste zweimal drücken). Sie können jedoch eine andere Tastenkombination aus der Dropdownliste auswählen.

Zugriffstaste	Zu drückende Tastenkombination
Rollen-Taste zweimal drücken	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Num-Feststelltaste zweimal drücken	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.
Feststelltaste zweimal drücken	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Linke Alt-Taste zweimal drücken	Drücken Sie die linke Alt-Taste zweimal kurz hintereinander.
Linke Umschalttaste zweimal drücken	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Linke Strg-Taste zweimal drücken	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.



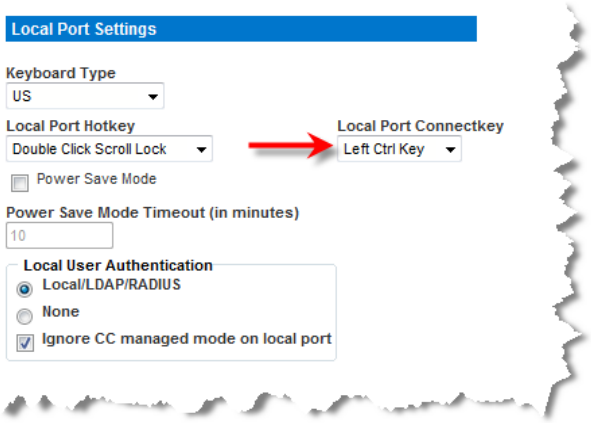
Wählen Sie die Verbindungstaste für den lokalen Port aus.

1. Wählen Sie die Verbindungstaste für den lokalen Port aus. Verwenden Sie eine Verbindungstastenfolge, um eine Verbindung mit einem Zielgerät herzustellen und zu einem anderen Zielgerät zu wechseln.

Sie können anschließend die Zugriffstaste verwenden, um die Verbindung zum Zielgerät zu trennen und zur GUI des lokalen Ports zurückzukehren.

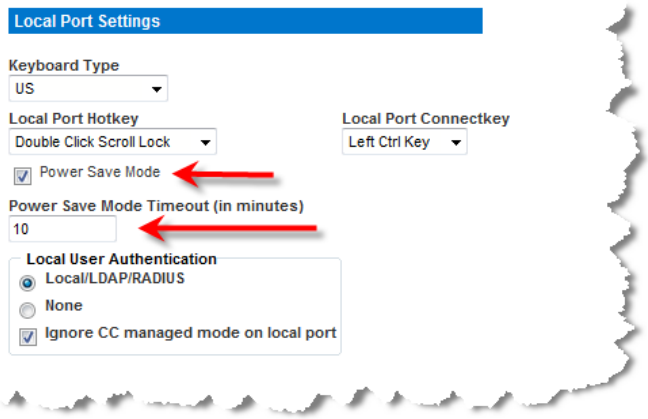
Wenn die Verbindungstaste für den lokalen Port erstellt wurde, erscheint diese im Navigationsfenster der GUI, sodass Sie sie als Referenz verwenden können. Beispiele für Verbindungstastenfolgen finden Sie unter ***Beispiele für Verbindungstasten*** (auf Seite 310).

Die Verbindungstaste ist für Standardserver und Blade-Chassis verfügbar.



Konfigurieren der Power-Speicherungsfunktion (Optional)

1. Führen Sie die folgenden Schritte aus, falls Sie das Stromsparfeature verwenden möchten:
   a. Aktivieren Sie das Kontrollkästchen "Power Save Mode" (Stromsparmodus).
   b. Legen Sie die Zeitspanne (in Minuten) fest, nach der in den Stromsparmodus geschaltet wird.



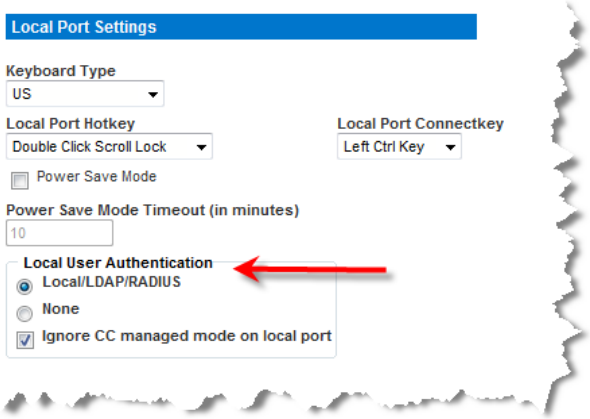
Lokale Benutzerauthentifizierung Wählen

1. Wählen Sie die Methode zur lokalen Benutzerauthentifizierung aus:

- Local/LDAP/RADIUS (Lokal/LDAP/RADIUS): Dies ist die empfohlene Option.

  Weitere Informationen zur Authentifizierung finden Sie unter Remoteauthentifizierung.
- Keine. Der lokale Konsolenzugriff wird nicht authentifiziert.

  Diese Option ist nur für sichere Umgebungen empfehlenswert.



Device Services (Gerätedienste)

Aktivieren von SSH

Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus, damit Administratoren über die SSH v2-Anwendung auf KX III zugreifen können.

So aktivieren Sie den SSH-Zugriff:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus.
3. Geben Sie die SSH-Portinformationen ein. Die standardmäßige SSH-TCP-Portnummer lautet 22, sie kann jedoch geändert werden, um ein höheres Niveau für Sicherheitsvorgänge zu erreichen.
4. Klicken Sie auf OK.

HTTP- und HTTPS-Porteinstellungen

Sie können von KX III verwendete HTTP- und/oder HTTPS-Ports konfigurieren. Wenn Sie z. B. den Standard-HTTP-Port 80 für andere Zwecke nutzen, wird beim Ändern des Ports sichergestellt, dass das Gerät nicht versucht, diesen Port zu verwenden.

So ändern Sie die HTTP- und/oder HTTPS-Porteinstellungen:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Geben Sie die neuen Ports in die Felder "HTTP Port" und/oder "HTTPS Port" ein.
3. Klicken Sie auf OK.

Eingeben des Erkennungsports

Die KX III-Erkennung erfolgt über einen einzelnen konfigurierbaren TCP-Port. Der Standardport lautet 5000, Sie können diesen jedoch für die Verwendung aller TCP-Ports außer 80 und 443 konfigurieren. Wenn Sie über eine Firewall auf KX III zugreifen möchten, müssen die Firewalleinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht-standardmäßigen konfigurierten Port zulassen.

So aktivieren Sie den Erkennungsport:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Geben Sie unter "Discovery Port" (Erkennungsport) den Erkennungsport ein.
3. Klicken Sie auf OK.

Konfigurieren und Aktivieren von Schichten

Mit der Schichtfunktion können Sie über ein KX III Basisgerät auf KX III Ziele und PDUs zugreifen.

Sie können bei Bedarf maximal zwei Schichtebenen an Geräten zu einer Konfiguration hinzufügen oder aus einer Konfiguration löschen.

Beim Einrichten der Geräte verwenden Sie spezifische CIMS für spezifische Konfigurationen.

Eine Beschreibung der Ziele, die Sie in eine Schichtkonfiguration einfügen können, sowie Informationen zu CIM-Kompatibilität und Gerätekonfiguration finden Sie unter Schichten – Zieltypen, unterstützte CIMs und Schichtkonfigurationen.

Die Portkonfiguration, einschließlich der Änderung des CIM-Namens, muss direkt vom jeweiligen Gerät aus durchgeführt werden. Die Konfiguration von Schichtzielports vom Basisgerät aus ist nicht möglich.

Schichten unterstützen auch die Verwendung von KVM-Switches zum Wechseln zwischen Servern. Siehe ***Konfigurieren von KVM-Switches*** (auf Seite 96).

Sobald es konfiguriert ist werden die Basis-und Schichtgeräte auf der Portzugriff-Seite angezeigt. Siehe ***Schichtgeräte – Seite "Port Access" (Portzugriff)*** (auf Seite 18)

Bevor eine Schichtkonfiguration erstellt wird

Nicht unterstützte (siehe "***Zulässige KX III Schichtkonfigurationen***" auf Seite 141) und eingeschränkte Funktionen auf Schichtzielen - KX III

Bevor Sie Schichtgeräte zu einer KX III Schichtkonfiguration hinzufügen:

- Basis-und Schichgeräte müssen mit dem gleichen Firmware-Revision betrieben werden.
- Aktivieren Sie die Basisgeräte auf der Seite "Device Settings" (Geräteeinstellungen). Siehe Konfigurieren von Standardzielservern
- Aktivieren Sie die Schichtgeräte auf der Seite "Local Port Settings" (Lokale Porteinstellungen). Siehe ***Lokale KX III Porteinstellungen konfigurieren*** (auf Seite 133), dann ***Enable Local Port Device Tiering*** (siehe "***"Enable Local Port Device Tiering" (Lokaler Port für Geräteschichten aktivieren).***" auf Seite 133)
- Bevor Sie Schichtgeräte hinzufügen, müssen Sie die Schichten für das Basisgerät und die Schichtgeräte aktivieren. Siehe ***Aktivieren von Schichten*** (auf Seite 143)

Zulässige KX III Schichtkonfigurationen

Bevor eine Schichtkonfiguration erstellt wird (auf Seite 140)

Im Folgenden sehen Sie die zulässigen Schichtkonfigurationen für KX III:

- KX III Basisgerät > KX III Schichtgeräte
- KX III Basisgerät > KX III Schichtgeräte
- Duale Videoportziele, die mit einem Schichtgerät verbunden sind, dürfen nur über das Schichtgerät und über das Basisschichtgerät angeschlossen werden.

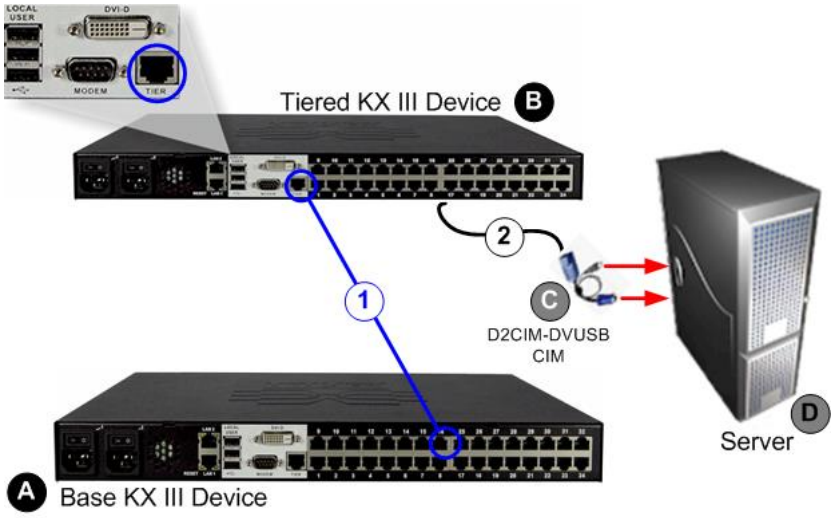
Nicht unterstützte und eingeschränkte Funktionen auf Schichtzielen

Die folgenden Funktionen werden nicht auf Schichtzielen unterstützt:

- Blade-Chassis auf Schichtgeräten
- Audio auf Schichtgeräten
- Smart Cards auf Schichtgeräten
- Virtuelle Medien von Schichtgeräten
- MCCAT als Schichtgerät
- Die Portgruppenverwaltung beschränkt sich auf das Erstellen von Portgruppen mit Mitgliedern, die direkt mit der Basis verbunden sind.
- Duale Videoportziele, die mit einem Schichtgerät verbunden sind, dürfen nur über das Schichtgerät und nicht über das Basisschichtgerät angeschlossen werden.
- Die Absolute Maussynchronization kann möglicherweise nicht richtig synchronisiert werden, wenn Ihre Schichtkonfiguration aus einer Mischung von KX II und KX III-Geräten besteht.
- KX II Basisgerät > KX III Schichtgeräte

Geschichtetes KX III Verbindungsbeispiel

Die folgende Abbildung zeigt die Verkabelungskonfigurationen zwischen einem KX III Schichtgerät und einem KX III Basisgerät.



Schritte	
A	KX III Basisgerät
B	KX III Schichtgerät
C	CIM, um Zielserver an KX III Schichtgerät anzuschließen.
D	Zielserver
1	Base DEVICE (Gerät Schicht-port to Tiered device (gerät) Schicht-port verbindung: ▪ Verbinden Sie eine Ende des Cat5/5e/6 Kabel mit dem Server-Port auf dem KX III Basisgerät. ▪ Schließen Sie das andere Kabelende von Schicht-Port am KX III Schichtgerät an.
2	Geschichtete Gerätverbindung mit dem Tastatur/Video/Maus-Port des Zielservers zu herstellen: ▪ Verbinden Sie das eine Ende des Cat5/5e/6 Kabels mit dem Server-Port auf dem KX III Basisgerät und das andere Ende mit einem unterstützten CIM, wie D2CIM-DVUSB. ▪ Schließen Sie die Tastatur, Maus und Video-Stecker auf der CIM an die entsprechenden Ports auf dem Zielserver an.

Aktivieren von Schichten

So aktivieren Sie Schichten:

1. Wählen Sie von der Schichtbasis-Gerät, „Geräteeinstellungen“ aus, um die Seite „Einstellungen der Gerätdienste“ zu öffnen.
2. Wählen Sie "Enable Tiering as Base" (Schichten als Basis aktivieren) aus.
3. Geben Sie in das Feld "Base Secret" (Geheimer Basisschlüssel) den geheimen Schlüssel ein, der von den Basis- und Schichtgeräten gemeinsam verwendet wird. Dieser geheime Schlüssel ist für die Schichtgeräte zur Authentifizierung des Basisgeräts erforderlich. Sie müssen denselben geheimen Schlüssel für das Schichtgerät eingeben. Klicken Sie auf OK.
4. Aktivieren Sie die Schichtgeräte. Wählen Sie auf dem Schichtgerät "Device Settings“ "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus.

5. Wählen Sie im Bereich "Enable Local Ports" (Lokale Ports aktivieren) die Option "Enable Local Port Device Tiering" (Lokaler Port für Geräteschichten aktivieren) aus.
6. Geben Sie im Feld "Tier Secret" (Geheimer Schlüssel der Schicht) denselben geheimen Schlüssel ein, den Sie für das Basisgerät auf der Seite "Device Settings" (Geräteeinstellungen) eingegeben haben. Klicken Sie auf OK.

Sobald die Geräte aktiviert und konfiguriert sind, werden Sie auf der Seite "Port Access" (Portzugriff) angezeigt.

Wenn KX III als Basisgerät oder Schichtgerät konfiguriert wurde, wird es wie folgt angezeigt:

- Als Basisgerät konfiguriert: Dies wird im Bereich "Device Information" (Geräteinformationen) im linken Bildschirmbereich der KX III Schaltfläche für Basisgeräte angezeigt.
- Als Schichtgerät konfiguriert: Dies wird im Bereich "Device Information" (Geräteinformationen) im linken Bildschirmbereich der KX III Schlatfläche für Schichtgeräte angezeigt.
- Das Basisgerät wird als Basis im linken Bildschirmbereich der Schichtgerät Schaltfläche unter "Connect User" (Benutzer verbinden) identifiziert.
- Die Zielverbindungen von der Basis zu einem Schichtport werden als zwei verbundene Ports angezeigt.

Fern-und Lokalzugriff von Schichtgeräten

Das Basisgerät ermöglicht über eine konsolidierte Portliste auf der Seite "Port Access" (Portzugriff) Remote- und lokalen Zugriff.

Schichtgeräte ermöglichen Remotezugriff über ihre eigenen Portlisten.

Der lokale Zugriff ist bei Schichtgeräten nicht möglich, wenn "Tiering" (Schichten) aktiviert ist.

Auf die Blad-Chassis von einem Basis-Gerät zugreifen

Blade-Chassis angeschlossen an einem KX III Basisgerät sind zugänglich.

Stromversorgungssteuerung von Schichtgeräten

Sie können Ziele, die Teil einer Schichtkonfiguration sind, ein- und ausschalten.

Der Zugriff auf diese Ziele erfolgt auf der Seite "Port Access" (Portzugriff).

Wenn Ziele und Ausgänge zugeordnet sind, steht die Stromzufuhrsteuerung auf der Seite "Port Access" (Portzugriff) zur Verfügung.

Zuordnungen von Zielen und PDU-Ausgängen sind auf diejenigen beschränkt, die am selben KX III angeschlossen sind.

An KX III Basis- oder -Schichtgeräte angeschlossene PDUs werden auf der Dropdown-Seite "Power" (Strom) zusammen mit Statistiken für den ausgewählten Powerstrip angezeigt.

Ebenso steht die Steuerung auf Ausgangsebene zur Verfügung.

Sie können aktuell eingeschaltete Ausgänge ausschalten und einschalten, Sie können jedoch nicht Ausgänge ein- und ausschalten, die aktuell ausgeschaltet sind.

Aktivieren des direkten Port-Zugriffs über URL

Der direkte Portzugriff ermöglicht es Benutzern, die Verwendung der Seite "Login dialog and Port Access" (Anmeldedialog und Port-Zugriff) zu umgehen.

Diese Funktion bietet auch die Möglichkeit, Benutzername und Kennwort direkt einzugeben und das Ziel aufzurufen, wenn Benutzername und Kennwort nicht in der URL enthalten sind.

Direkter Portzugriff URL Syntax für den Virtuellen KVM Client (AKC)

Wenn Sie den VKC und direkten Port-Zugriff verwenden: eine der folgenden Syntaxen für Standard-Ports:

- https://IP-Adresse/dpa.asp?username=Benutzername&kennword=Kennwort&port=Port-Nummer

  Oder

- https://IPaddress/dpa.asp?username=username&password=password&portname=port name

Für Blade-Chassis muss der Port sowohl von der Port-Nummer oder von einem Portnamen und Platznummer bezeichnet werden.

- https://IPaddress/dpa.asp?username=username&password=password&port=port number-slot number

  Blade-Chassis, die mit Port 1 und Slot 2 verbunden sind, werden mit 1-2 angegeben.

- https://IPaddress/dpa.asp?username=username&password=password&port=port name-slot number

  Blade-Chassis, die mit Port 1 und Slot 2 verbunden sind, werden mit 1-2 angegeben.

Benutzername und Kennwort sind optional.

Werden die Benutzername und Kennwörter nicht bereitgestellt, wird ein Dialogfeld für die Anmeldung angezeigt. Nach der Authentifizierung wird der Benutzer direkt mit dem Ziel verbunden.

Für den Port kann eine Port-Nummer oder ein Port-Name angegeben sein.

Wenn Sie einen Port-Namen verwenden, muss dieser eindeutig sein, sonst wird ein Fehler gemeldet.

Bleibt der Port unberücksichtigt, wird ein Fehler gemeldet.

Wenn Sie auf ein Ziel zugreifen, das zu einer dualen Videoportgruppe gehört, wird für den direkten Portzugriff der primäre Port verwendet, um den primären und sekundären Port zu starten.

Direkte Portverbindungen zum sekundären Port werden verweigert, und die standardmäßigen Berechtigungsregeln werden angewendet.

Weitere Informationen zur dualen Videoportgruppe finden Sie unter **Erstellen dualer Videoportgruppen.** (siehe "**Erstellen dualer Videoportgruppen**" auf Seite 173) .

Direkter Portzugriff URL Syntax für Aktiv KVM Client (AKC)

Wenn Sie den VKC und direkten Port-Zugriff verwenden::

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

  Oder

- https://IPaddress/dpa.asp?username=username&password=password&port=port name&client=akc

Für Blade-Chassis muss der Port sowohl von der Port-Nummer oder von einem Portnamen und Platznummer bezeichnet werden.

- https://IPaddress/dpa.asp?username=username&password=password&port=port number-slot number=akc

  Blade-Chassis, die mit Port 1 und Slot 2 verbunden sind, werden mit 1-2 angegeben.

- https://IPaddress/dpa.asp?username=username&password=password&port=port name-slot number=akc

  Blade-Chassis, die mit Port 1 und Slot 2 verbunden sind, werden mit 1-2 angegeben.

Benutzername und Kennwort sind optional.

Werden die Benutzername und Kennwörter nicht bereitgestellt, wird ein Dialogfeld für die Anmeldung angezeigt. Nach der Authentifizierung wird der Benutzer direkt mit dem Ziel verbunden.

Für den Port kann eine Port-Nummer oder ein Port-Name angegeben sein.

Wenn Sie einen Port-Namen verwenden, muss dieser eindeutig sein, sonst wird ein Fehler gemeldet.

Bleibt der Port unberücksichtigt, wird ein Fehler gemeldet.

"Client=akc" ist optional, außer Sie verwenden den AKC.

Wird "Client=akc" nicht verwendet, wird der VKC verwendet.

Wenn Sie auf ein Ziel zugreifen, das zu einer dualen Videoportgruppe gehört, wird für den direkten Portzugriff der primäre Port verwendet, um den primären und sekundären Port zu starten.

Direkte Portverbindungen zum sekundären Port werden verweigert, und die standardmäßigen Berechtigungsregeln werden angewendet.

Weitere Informationen zur dualen Videoportgruppe finden Sie unter **Erstellen dualer Videoportgruppen.** (siehe "**Erstellen dualer Videoportgruppen**" auf Seite 173) .

Direkten Port-Zugriff aktivieren

So aktivieren Sie den direkten Port-Zugriff:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Aktivieren Sie die Option "Enable Direct Port Access via URL" (Direkten Port-Zugriff über URL aktivieren), wenn Sie möchten, dass Benutzer über das Dominion-Gerät durch Eingabe der erforderlichen Parameter in die URL direkten Zugriff auf ein Ziel haben.
3. Klicken Sie auf "OK".

Aktivieren der AKC-Download-Serverzertifikat-Validierung

Wenn Sie den AKC-Client verwenden, können Sie wählen, ob Sie die Funktion "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikatsvalidierung aktivieren) verwenden möchten.

Hinweis: When Sie in IPv4 and IPv6 arbeiten (dual stack Modus with 'AKC-Download-Serverzertifikatsvalidierung aktivieren' Funktion, erfordert Microsoft® ClickOnce® , dass das SERVER Zertifikat CN keine komprimierte Form der IPv6 Adresse enthält.

Andernfalls können Sie AKC nicht erfolgreich herunterladen und starten.

Dies kann jedoch zu einem Konflikt mit den Browsereinstellungen bezüglich des Formats der IPv6-Adressen führen.

Verwenden Sie den Hostnamen des Servers als allgemeinen Namen (CN), oder verwenden Sie komprimierte und nicht komprimierte Formate der IPv6-Adresse als alternativen Namen des Zertifikats.

Option 1: AKC-Download-Serverzertifikatsvalidierung nicht aktivieren (Standardeinstellung)

Wenn Sie die AKC-Download-Serverzertifikatsvalidierung nicht aktivieren, beachten Sie Folgendes: müssen alle Dominion-Gerätebenutzer und CC-SG Bookmark- und Access-Client-Benutzer:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Option 2: Enable AKC Download Server Certificate Validation (Übersicht zur AKC-Download-Serverzertifikat-Validierung aktivieren)

Wenn Sie die AKC-Download-Serverzertifikat-Validierung aktivieren:

- Administratoren müssen ein gültiges Zertifikat auf das Gerät hochladen oder ein selbstsigniertes Zertifikat auf dem Gerät generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.
- Bei der Verwendung von CC-SG Nachbarschaften, müssen Sie AKC auf den einzelnen Mitgliedern aktivieren.

So installieren Sie das selbstsignierte Zertifikat, wenn Sie das Betriebssystem Windows Vista® oder Windows 7 ® verwenden:

1. Fügen Sie die IP-Adresse von KX III zu den vertrauenswürdigen Seiten hinzu und stellen Sie sicher, dass der geschützte Modus deaktiviert ist.
2. Starten Sie den Internet Explorer® und verwenden Sie dabei die IP-Adresse von KX III als URL. Eine Zertifikatsfehlermeldung wird angezeigt.
3. Wählen Sie "View Certificates" (Zertifikate anzeigen) aus.
4. Klicken Sie auf der Registerkarte "Allgemein" auf "Install Certificate" (Zertifikat installieren). Das Zertifikat wird unter den vertrauenswürdigen Stammzertifizierungsstellen gespeichert.
5. Wenn das Zertifikat installiert wurde, sollte die IP-Adresse von KX III von den vertrauenswürdigen Seiten entfernt werden.

So aktivieren Sie die AKC-Download-Serverzertifikatsvalidierung:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Aktivieren Sie das Kontrollkästchen "AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikatsvalidierung) oder lassen Sie die Funktion deaktiviert (Standardeinstellung).
3. Klicken Sie auf OK.

Wenn Sie eine Verbindung zu einem eigenständigen KX III-Gerät herstellen und Support für die AKC-Download-Serverzertifikatsvalidierung aktiviert ist, lautet das gültige IPv6-Format zur Generierung des Zertifikats entweder:

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` wenn eine führende 0 vorhanden ist

  Oder

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` wenn keine Nullkomprimierung vorhanden ist

Konfigurieren von SNMP-Agenten

SNMP-kompatible Geräte, genannt Agenten, speichern Daten über sich selbst in Management Information Bases (MIBs) und geben diese Daten an die SNMP-Manager zurück. Weitere Informationen zum Anzeigen von KX III-MIB finden Sie unter ***Anzeigen der KX III-MIB*** (siehe "***Anzeigen der KX III MIB***" auf Seite 160).

KX III unterstützt die SNMP-Protokollierung für SNMP v1/v2c und/oder v3. SNMP v1/v2c definiert Meldungsformate und Protokollvorgänge, sofern die SNMP-Protokollierung aktiviert ist. SNMP v3 ist eine Sicherheitserweiterung von SNMP, die die Benutzerauthentifizierung, Kennwortverwaltung und Verschlüsselung ermöglicht.

So konfigurieren Sie SNMP-Agenten:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Geben Sie die folgenden Identifier-Informationen des SNMP-Agenten für die MIB-II-Systemgruppenobjekte an:
   a. System Name (Systemname) – Name/Gerätename des SNMP-Agenten
   b. System Contact (Systemkontakt) – Kontaktname für das Gerät
   c. System Location (Systemstandort) – Standort des Geräts
3. Wählen Sie entweder "Enable SNMP v1/v2c" (SNMP v1/v2c aktivieren) und/oder "Enable SNMP v3" (SNMP v3 aktivieren) aus. Sie müssen mindestens eine Option auswählen. <erfoderlich>
4. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v1/v2c aus:
   a. Community – die Communityzeichenfolge des Geräts
   b. Community Type (Community-Typ) – Gewähren Sie Communitybenutzer entweder Lese- oder Lese-/Schreibzugriff

   Hinweis: Eine SNMP-Community ist die Gruppe, der Geräte und Verwaltungsstationen angehören, auf denen SNMP ausgeführt wird. Durch sie können Sie leichter definieren, wohin Informationen gesendet werden. Der Community-Name wird zur Identifizierung der Gruppe verwendet. Das SNMP-Gerät oder der SNMP-Agent kann zu mehreren SNMP-Communities gehören.
5. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v3 aus:

a. Wählen Sie gegebenenfalls "Use Auth Passphrase" (Authentifizierungs-Passphrase verwenden). Wenn eine Passphrase für den exklusiven Zugriff erforderlich ist, können Sie mit "Use Auth Passphrase" (Authentifizierungs-Passphrase verwenden) dieselbe Passphrase für beide verwenden, ohne die Authentifizierungs-Passphrase erneut einzugeben.

b. Security Name (Sicherheitsname) – Der Benutzername oder Name des Dienstkontos der Einheit, die mit dem SNMP-Agenten kommuniziert (max. 32 Zeichen).

c. Authentication Protocol (Authentifizierungsprotokoll) – Das MD5- oder SHA-Authentifizierungsprotokoll, das vom SNMP v3-Agenten verwendet wird.

d. Authentication Passphrase (Authentifizierungs-Passphrase) – Dies wird für den Zugriff auf den SNMP v3-Agenten benötigt (max. 64 Zeichen).

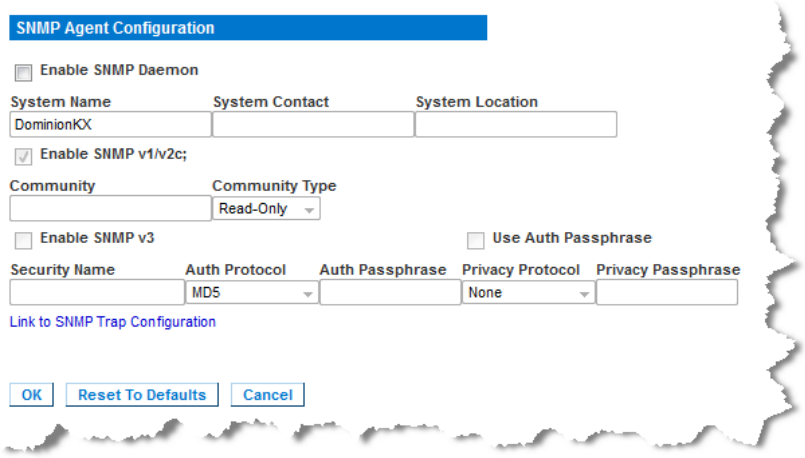
e. Privacy Protocol (Protokoll für exklusiven Zugriff) – Der AES- oder DES-Algorithmus, der zum Verschlüsseln von PDU- und Kontextdaten verwendet wird (falls zutreffend).

f. Privacy Passphrase (Passphrase für exklusiven Zugriff) – Die Passphrase, die für den Zugriff auf den Algorithmus des Protokolls für den exklusiven Zugriff verwendet wird (max. 64 Zeichen).

6. Klicken Sie auf "OK", um den SNMP-Agentendienst zu starten.

Konfigurieren Sie die SNMP-Traps auf der Seite Ereignisverwaltung – Einstellungen, auf die schnell mit einem Klick auf der SNMP-Trap-Linkkonfiguration zugegriffen werden kann. Siehe ***Konfigurieren von SNMP-Traps*** (auf Seite 154)für weitere Informationen zum Erstellen von SNMP-Traps und Liste der KX III SNMP-Traps für eine Liste der verfügbaren KX III SNMP-Traps.

Die Ereignisse, die aufgezeichnet werden, sobald ein SNMP-Trap konfiguriert wurde, werden auf der Seite "Event Management - Destination" (Ereignisverwaltung – Ziele) ausgewählt. Siehe ***Konfigurieren der Ereignisverwaltung – Ziele*** (siehe "***Konfigurieren der Ereignisverwaltung - Ziele***" auf Seite 162).



So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen). Alle Elemente auf der Seite werden auf ihre Standardwerte zurückgesetzt.

WARNUNG: Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen KX III und dem damit verbundenen Router verloren gehen, wenn KX III neu gestartet wird. Das SNMP-Trap "Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

Konfigurieren der Modemeinstellungen

Hinweis: Die KX III 3.0.0 Version bietet keine Modem-Unterstützung, aber die zukünftige Version wird solche haben.

Konfigurieren von Datum-/Uhrzeiteinstellungen

Auf der Seite **Date/Time Settings** (Datum-/Uhrzeiteinstellungen) stellen Sie Datum und Uhrzeit für die KX III-Einheit ein. Hierzu haben Sie zwei Möglichkeiten:

- Datum und Uhrzeit manuell einstellen
- Datum und Uhrzeit mit einem NTP (Network Time Protocol)-Server synchronisieren

So stellen Sie das Datum und die Uhrzeit ein:

1. Wählen Sie Device Settings -- Date/Time (Geräteeinstellungen -- Datum/Uhrzeit). Die Seite Date/Time Settings (Datum-/Uhrzeiteinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdown-Liste Time Zone Ihre Zeitzone aus.
3. Aktivieren Sie das Kontrollkästchen "Adjust for daylight savings time" (an Sommerzeit anpassen), um die Uhrzeit an die Sommerzeit anzupassen.
4. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:
   - User Specified Time (Benutzerdefinierte Zeit) – Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben. Falls Sie die Option "User Specified Time" (Benutzerdefinierte Zeit) ausgewählt haben, geben Sie Datum und Uhrzeit wie folgt ein: Geben Sie im Feld "Time" die Uhrzeit im Format hh:mm ein. (Verwenden Sie das 24-h-Zeitformat.)
   - Synchronize with NTP Server (Mit NTP-Server synchronisieren) – Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
5. Falls Sie die Option "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld "Primary Time Server" (Primärer Zeitserver) die IP-Adresse dieses Servers ein.
   b. Geben Sie im Feld "Secondary Time Server" (Sekundärer Zeitserver) die IP-Adresse dieses Servers ein **Optional**
6. Klicken Sie auf OK.

Ereignisverwaltung

Die KX III Funktion zur Ereignisverwaltung ermöglicht Ihnen die Verteilung von Systemereignissen auf SNMP-Manager, Syslog und das Prüfprotokoll zu aktivieren und zu deaktivieren. Die Ereignisse werden kategorisiert, und Sie können für jedes Ereignis festlegen, ob es an eines oder mehrere Ziele gesendet werden soll.

Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)

Konfigurieren Sie die SNMP-Traps und die syslog-Konfiguration auf der Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen). ***Siehe Konfigurieren von SNMP-Traps*** (siehe "***Konfigurieren von SNMP-Traps***" auf Seite 154).

Aktivieren Sie nach der Konfiguration die SNMP-Traps auf der Seite "Event Management – Destinations" (Ereignisverwaltung – Ziele). Siehe ***Konfigurieren der Ereignisverwaltung – Ziele*** (siehe "***Konfigurieren der Ereignisverwaltung - Ziele***" auf Seite 162).

Konfigurieren von SNMP-Traps

Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung und die Überwachung von Netzwerkgeräten und ihrer Funktionen.

SNMP-Traps werden über ein Netzwerk gesendet, um Informationen zu sammeln.

Die Traps werden auf der Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) konfiguriert. Sie finden eine Liste der KX III SNMP-Traps unter Liste der KX III -SNMP-Traps.

SNMP-kompatible Geräte, genannt Agenten, speichern Daten über sich selbst in Management Information Bases (MIBs) und antworten auf das SNMP-Trap.

SNMP-Agenten werden auf der Seite "Device Services" (Gerätedienste) konfiguriert. Informationen zum ***Konfigurieren von SNMP-Agenten*** (auf Seite 150) finden Sie unter Konfigurieren von SNMP-Agenten, und Informationen zum Anzeigen der ***KX III*** (siehe "***Anzeigen der KX III MIB***" auf Seite 160)]-MIB finden Sie unter Anzeigen der KX III -MIB.

So konfigurieren Sie SNMP (und aktivieren die SNMP-Protokollierung):

1. Wählen Sie "Device Settings Event Management – Settings" (Geräteeinstellungen Ereignisverwaltung – Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Wählen Sie das Kontrollkästchen SNMP-Protokollierung Aktivieren, um die restlichen Kontrollkästchen im Abschnitt zu aktivieren. <erforderlich>
3. Wählen Sie entweder "SNMP v1/v2c Traps Enabled" (SNMP v1/v2c-Traps aktiviert) oder "SNMP Trap v3 Enabled" (SNMP-Trap v3 aktiviert) oder beide Optionen aus. Sie müssen mindestens eine Option auswählen.

   Nachdem Sie die Optionen ausgewählt haben, werden alle dazugehörigen Felder aktiviert. <erfoderlich>

4. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v1/v2c aus:
   a. Destination IP/Hostname (IP-Zieladresse/Hostname) – IP-Adresse oder Hostname des SNMP-Managers. Sie können maximal fünf (5) SNMP-Manager erstellen.

   Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.

   b. Port Number (Portnummer) – Die vom SNMP-Manager verwendete Portnummer.
   c. Community – die Communityzeichenfolge des Geräts

   Hinweis: Eine SNMP-Community ist die Gruppe, der Geräte und Verwaltungsstationen angehören, auf denen SNMP ausgeführt wird. Durch sie können Sie leichter definieren, wohin Informationen gesendet werden. Der Community-Name wird zur Identifizierung der Gruppe verwendet. Das SNMP-Gerät oder der SNMP-Agent kann zu mehreren SNMP-Communities gehören.

5. Aktivieren Sie das Kontrollkästchen "SNMP Trap v3 Enabled" (SNMP-Trap v3 aktiviert), falls es noch nicht aktiviert ist, um die folgenden Felder zu aktivieren. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v3 aus:
   a. Destination IP/Hostname (IP-Zieladresse/Hostname) – IP-Adresse oder Hostname des SNMP-Managers. Sie können maximal fünf (5) SNMP-Manager erstellen.

   Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.

   b. Port Number (Portnummer) – Die vom SNMP-Manager verwendete Portnummer.
   c. Security Name (Sicherheitsname) – Der Benutzername oder Name des Dienstkontos der Einheit, die mit dem SNMP-Agenten kommuniziert (max. 32 Zeichen).
   d. Authentication Protocol (Authentifizierungsprotokoll) – Das MD5- oder SHA-Authentifizierungsprotokoll, das vom SNMP v3-Agenten verwendet wird.
   e. Authentication Passphrase (Authentifizierungs-Passphrase) – Dies wird für den Zugriff auf den SNMP v3-Agenten benötigt (max. 64 Zeichen).
   f. Privacy Protocol (Protokoll für exklusiven Zugriff) – Der AES- oder DES-Algorithmus, der zum Verschlüsseln von PDU- und Kontextdaten verwendet wird (falls zutreffend).
   g. Privacy Passphrase (Passphrase für exklusiven Zugriff) – Die Passphrase, die für den Zugriff auf den Algorithmus des Protokolls für den exklusiven Zugriff verwendet wird (max. 64 Zeichen).

Hinweis: Wenn Sie die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) von der lokalen Konsole aufrufen und eine Bildschirmauflösung kleiner als 1280x1024 verwenden, wird die Spalte "Privacy Passphrase" (Passphrase für exklusiven Zugriff) möglicherweise nicht auf der Seite angezeigt. Blenden Sie in diesem Fall den linken Bildschirmbereich von KX III aus. Siehe Linker Bildschirmbereich

6. Klicken Sie auf "OK", um die SNMP-Traps zu erstellen.

Mithilfe des Links "Link to SNMP Agent Configuration" (Link auf SNMP-Agentenkonfiguration) können Sie die Seite "Devices Services" (Gerätedienste) schnell von der Seite "Event Management – Settings“ (Ereignisverwaltung – Einstellungen) aufrufen.

Die Ereignisse, die aufgezeichnet werden, sobald ein SNMP-Trap konfiguriert wurde, werden auf der Seite "Event Management - Destination" (Ereignisverwaltung – Ziele) ausgewählt. Siehe ***Konfigurieren der Ereignisverwaltung – Ziele*** (siehe "***Konfigurieren der Ereignisverwaltung - Ziele***" auf Seite 162).

KX III unterstützt die SNMP-Protokollierung für SNMP v1/v2c und/oder v3. SNMP v1/v2c definiert Meldungsformate und Protokollvorgänge, sofern die SNMP-Protokollierung aktiviert ist. SNMP v3 ist eine Sicherheitserweiterung von SNMP, die die Benutzerauthentifizierung, Kennwortverwaltung und Verschlüsselung ermöglicht.

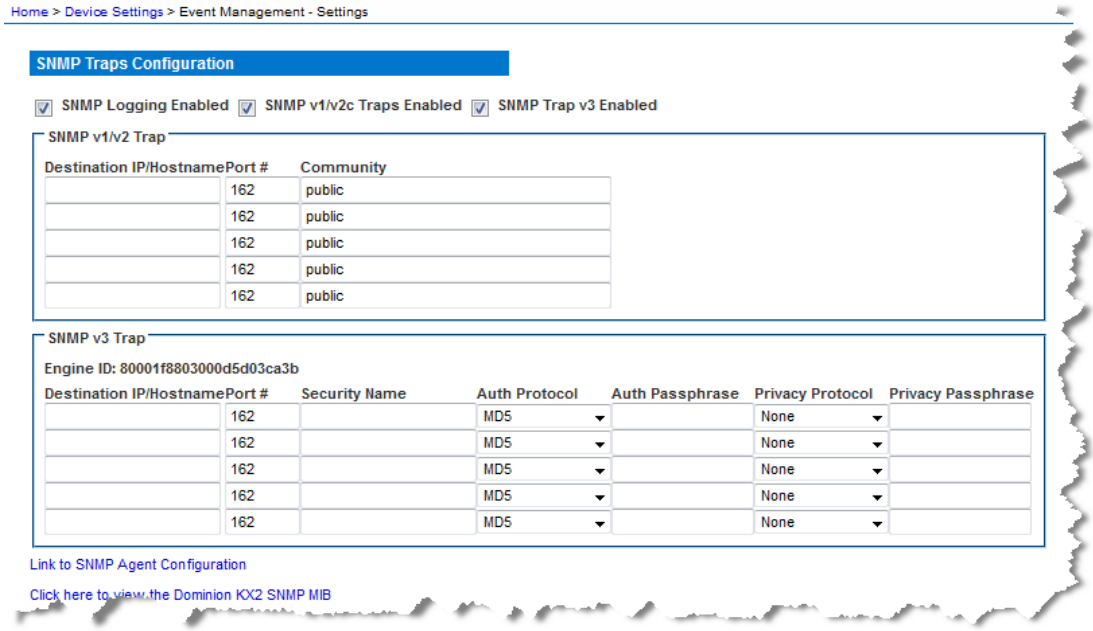
So bearbeiten Sie vorhandene SNMP-Traps:

1. Wählen Sie "Device Settings > Event Management – Settings" (Geräteeinstellungen > Ereignisverwaltung – Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf "OK", um die Änderungen zu speichern.

Hinweis: Wenn Sie die SNMP-Einstellungen deaktivieren, werden die SNMP-Informationen beibehalten, sodass Sie sie nicht erneut eingeben müssen, wenn Sie die Einstellungen wieder aktivieren.

So löschen Sie SNMP-Traps:

- Löschen Sie alle Werte in den Feldern für die SNMP-Traps, und speichern Sie die Änderungen.



Stellen Sie die werkseitigen Standardwerte wieder her, um die SNMP-Konfiguration zu löschen und um die werkseitigen Standardeinstellungen von KX III wieder festzulegen.

So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

WARNUNG: Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen KX III und dem damit verbundenen Router verloren gehen, wenn KX III neu gestartet wird. Das SNMP-Trap "Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

Liste der KX III-SNMP-Traps

SNMP bietet die Möglichkeit, Traps (Benachrichtigungen) zu senden, um einen Administrator zu informieren, wenn eine oder mehrere Bedingungen erfüllt sind.

Die folgende Tabelle enthält die SNMP-Traps von KX III:

Trap-Name	Beschreibung
bladeChassisCommError	Es wurde ein Kommunikationsfehler bei einem an diesen Port angeschlossenen Blade-Chassis-Gerät festgestellt.
cimConnected	Das CIM ist angeschlossen.
cimDisconnected	Das CIM ist nicht angeschlossen.
cimUpdateStarted	Das CIM-Update wird gestartet.
cimUpdateCompleted	Das CIM-Update wurde ausgeführt.
configBackup	Die Gerätekonfiguration wurde gesichert.
configRestore	Die Gerätekonfiguration wurde wiederhergestellt.
deviceUpdateFailed	Das Gerät konnte nicht aktualisiert werden.
deviceUpgradeCompleted	KX III hat die Aktualisierung mittels einer RFP-Datei abgeschlossen.
deviceUpgradeStarted	KX III hat die Aktualisierung mittels einer RFP-Datei begonnen.
factoryReset	Das Gerät wurde auf die Werkseinstellungen zurückgesetzt.
firmwareFileDiscarded	Die Firmware-Datei wurde verworfen.
firmwareUpdateFailed	Die Firmware konnte nicht aktualisiert werden.
firmwareValidationFailed	Die Firmware konnte nicht validiert werden.
groupAdded	Eine Gruppe wurde zum ProductName-System hinzugefügt.
groupDeleted	Eine Gruppe wurde aus dem System gelöscht.
groupModified	Eine Gruppe wurde geändert.
ipConflictDetected	Ein IP-Adressenkonflikt wurde erkannt.
ipConflictResolved	Ein IP-Adressenkonflikt wurde gelöst.
networkFailure	Für eine der Ethernet-Schnittstellen des Produkts besteht keine Netzwerkverbindung mehr.
networkParameterChanged	Die Netzwerkparameter wurden geändert.

Trap-Name	Beschreibung
passwordSettingsChanged	Die Einstellungen für sichere Kennwörter wurden geändert.
portConnect	Ein zuvor authentifizierter Benutzer hat eine KVM-Sitzung gestartet.
portConnectionDenied	Eine Verbindung mit dem Zielport wurde verweigert.
portDisconnect	Die Sitzung des Benutzers einer KVM-Sitzung wird von selbigem ordnungsgemäß geschlossen.
portStatusChange	Der Port ist nicht mehr verfügbar.
powerNotification	Benachrichtigung über den Status der Stromversorgung: 1 = Aktiv, 0 = Inaktiv.
powerOutletNotification	Benachrichtigung über den Status eines Powerstrip-Geräteausgangs.
rebootCompleted	Der Neustart von KX III ist abgeschlossen.
rebootStarted	KX III wird neu gestartet: entweder durch Wiederherstellen der Stromversorgung oder durch einen „Warmstart“ mittels des Betriebssystems.
scanStarted	Ein Zielserverscan wurde gestartet.
scanStopped	Ein Zielserverscan wurde angehalten.
securityBannerAction	Die Sicherheitsmeldung wurde akzeptiert oder abgelehnt.
securityBannerChanged	Die Sicherheitsmeldung wurde geändert.
securityViolation	Ein Sicherheitsproblem ist aufgetreten.
setDateTime	Das Datum und die Uhrzeit wurden für das Gerät eingestellt.
setFIPSMode	Der FIPS-Modus wurde aktiviert.
startCCManagement	Für das Gerät wurde die CommandCenter-Verwaltung gestartet.
stopCCManagement	Die CommandCenter-Verwaltung des Geräts wurde aufgehoben.
userAdded	Ein Benutzer wurde zum System hinzugefügt.
userAuthenticationFailure	Ein Benutzer hat versucht, sich mit einem falschen Benutzernamen und/oder Kennwort anzumelden.
userConnectionLost	Bei einem Benutzer mit aktiver Sitzung ist eine nicht ordnungsgemäße Sitzungstrennung

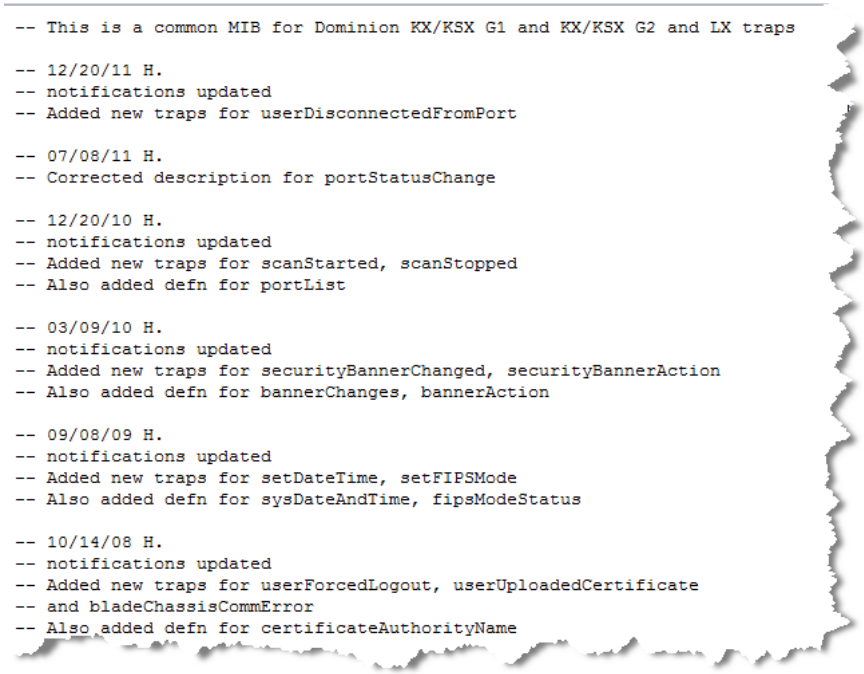
Trap-Name	Beschreibung
	aufgetreten.
userDeleted	Ein Benutzerkonto wurde gelöscht.
userForcedLogout	Ein Benutzer wurde durch "Admin" zwangsabgemeldet.
userLogin	Ein Benutzer hat sich erfolgreich bei KX III angemeldet und wurde authentifiziert.
userLogout	Ein Benutzer hat sich erfolgreich und ordnungsgemäß von KX III abgemeldet.
userModified	Ein Benutzerkonto wurde geändert.
userPasswordChanged	Das Ereignis wird ausgelöst, wenn das Kennwort irgendeines Benutzers des Geräts geändert wird.
userSessionTimeout	Die aktive Sitzung eines Benutzers wurde aufgrund einer Zeitüberschreitung beendet.
userUploadedCertificate	Ein Benutzer hat ein SSL-Zertifikat hochgeladen.
vmImageConnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu installieren. Für jeden Versuch einer Geräte-/Abbildzuordnung (Installation) wird dieses Ereignis generiert.
vmImageDisconnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu deinstallieren.

Anzeigen der KX III MIB

So zeigen Sie die KX III MIB an:

1. Wählen Sie "Device Settings Event Management – Settings" (Geräteeinstellungen Ereignisverwaltung – Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Klicken Sie hier, um die DominionKX3 SNMP MIB Link anzuzeigen. Die MIB-Datei wird in einem Browserfenster geöffnet.

Hinweis: Wenn Sie eine Lese-/Schreibberechtigung für die MIB-Datei haben, können Sie in einem MIB-Editor Änderungen an der Datei vornehmen.



```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps

-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateTime, setFIPSMode
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

SysLog-Konfiguration

So konfigurieren Sie Syslog und aktivieren die Weiterleitung:

1. Wählen Sie "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) aus, um Geräte-Protokollmeldungen an einen Remote-Syslog-Server zu senden.
2. Geben Sie die IP-Adresse/den Hostnamen Ihres Syslog-Servers im Feld "IP Address" (IP-Adresse) ein.
3. Klicken Sie auf "OK".

Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.

Stellen Sie die werkseitigen Standardwerte wieder her, um die syslog-Konfiguration zu löschen.

Konfigurieren der Ereignisverwaltung - Ziele

Systemereignisse generieren (falls aktiviert) SNMP-Benachrichtigungsereignisse (Traps) oder können in Syslog oder dem Prüfprotokoll protokolliert werden. Auf der Seite "Event Management - Destinations" (Ereignisverwaltung – Ziele) legen Sie fest, welche Systemereignisse verfolgt und wohin diese Informationen gesendet werden sollen.

Hinweis: SNMP-Traps werden nur erzeugt, wenn die Option "SNMP Logging Enabled" (SNMP-Protokollierung aktiviert) ausgewählt ist. Syslog-Ereignisse werden nur erzeugt, wenn die Option "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) ausgewählt ist. Beide Optionen befinden sich auf der Seite "Event Management - Settings" (Ereignisverwaltung - Einstellungen). Siehe **Configuring Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)** *(siehe "***Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)***" auf Seite 154).*

So wählen Sie Ereignisse und ihr Ziel aus:

1. Wählen Sie "Device Settings > Event Management – Destinations" (Geräteeinstellungen > Ereignisverwaltung – Ziele). Die Seite "Event Management - Destinations" (Ereignisverwaltung – Ziele) wird angezeigt.

   Die Systemereignisse sind nach "Device Operation" (Gerätebetrieb), "Device Management" (Geräteverwaltung), "Security" (Sicherheit), "User Activity" (Benutzeraktivität) und "User Group Administration" (Benutzergruppenverwaltung) kategorisiert.

2. Aktivieren Sie die Kontrollkästchen der Ereignisse, die Sie aktivieren bzw. deaktivieren möchten, und geben Sie an, wohin die Informationen gesendet werden sollen.

   Tipp: Ganze Kategorien können durch Aktivieren bzw. Deaktivieren der entsprechenden Kategorie-Kontrollkästchen aktiviert bzw. deaktiviert werden.

   ---

3. Klicken Sie auf "OK".

So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

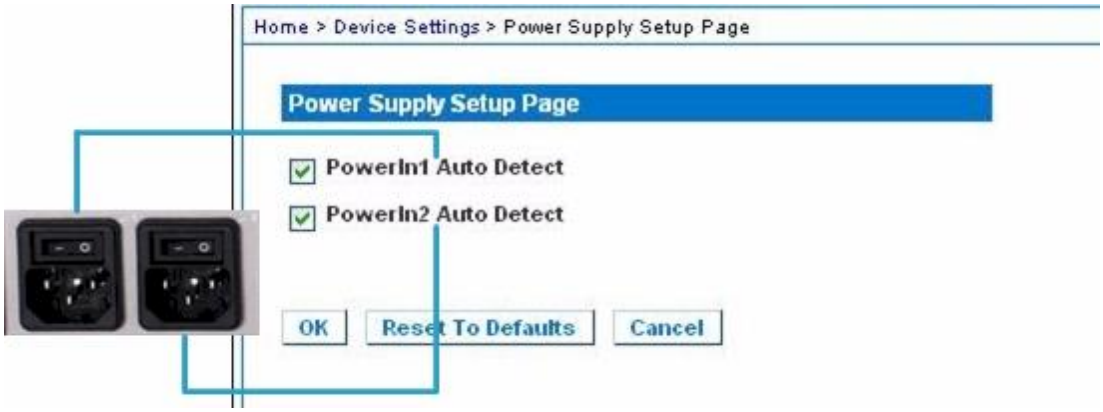
WARNUNG: Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen KX III und dem damit verbundenen Router verloren gehen, wenn KX III neu gestartet wird. Das SNMP-Trap "Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

Netzteilkonfiguration

KX III bietet zwei Netzteile und kann den Status dieser Netzteile automatisch erkennen und entsprechende Benachrichtigungen ausgeben. Geben Sie auf der Seite "Power Supply Setup" (Netzteilkonfiguration) an, ob Sie eines oder beide Netzteile verwenden. Mit der korrekten Konfiguration stellen Sie sicher, dass KX III die entsprechenden Benachrichtigungen bei einem Ausfall der Stromversorgung sendet. Wenn beispielsweise Netzteil 1 ausfällt, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite der Einheit rot.

So aktivieren Sie die automatische Erkennung für die verwendeten Netzteile:

1. Wählen Sie "Device Settings > Power Supply Setup" (Geräteeinstellungen und Netzteilkonfiguration) aus. Die Seite "Power Supply Setup" (Netzteilkonfiguration) wird angezeigt.



2. Wenn Sie den Strom über das Netzteil 1 zuführen (ganz links auf der Rückseite des Geräts), wählen Sie die Option "PowerIn1 Auto Detect" (Netzteil 1 – Automatische Erkennung) aus.
3. Wenn Sie den Strom über das Netzteil 2 zuführen (ganz rechts auf der Rückseite des Geräts), wählen Sie die Option "PowerIn2 Auto Detect" (Netzteil 2 – Automatische Erkennung) aus.

4. Klicken Sie auf OK.

Hinweis: Wenn eines dieser Kontrollkästchen aktiviert ist und das entsprechende Netzteil zurzeit nicht angeschlossen ist, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite der Einheit rot.

So deaktivieren Sie die automatische Erkennung:

- Deaktivieren Sie das Kontrollkästchen für das entsprechende Netzteil.

So stellen Sie die werksseitigen Standardeinstellungen wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Hinweis: KX III übermittelt den Status der Netzteile NICHT an CommandCenter. Dominion I (Generation 1) hingegen tut dies.

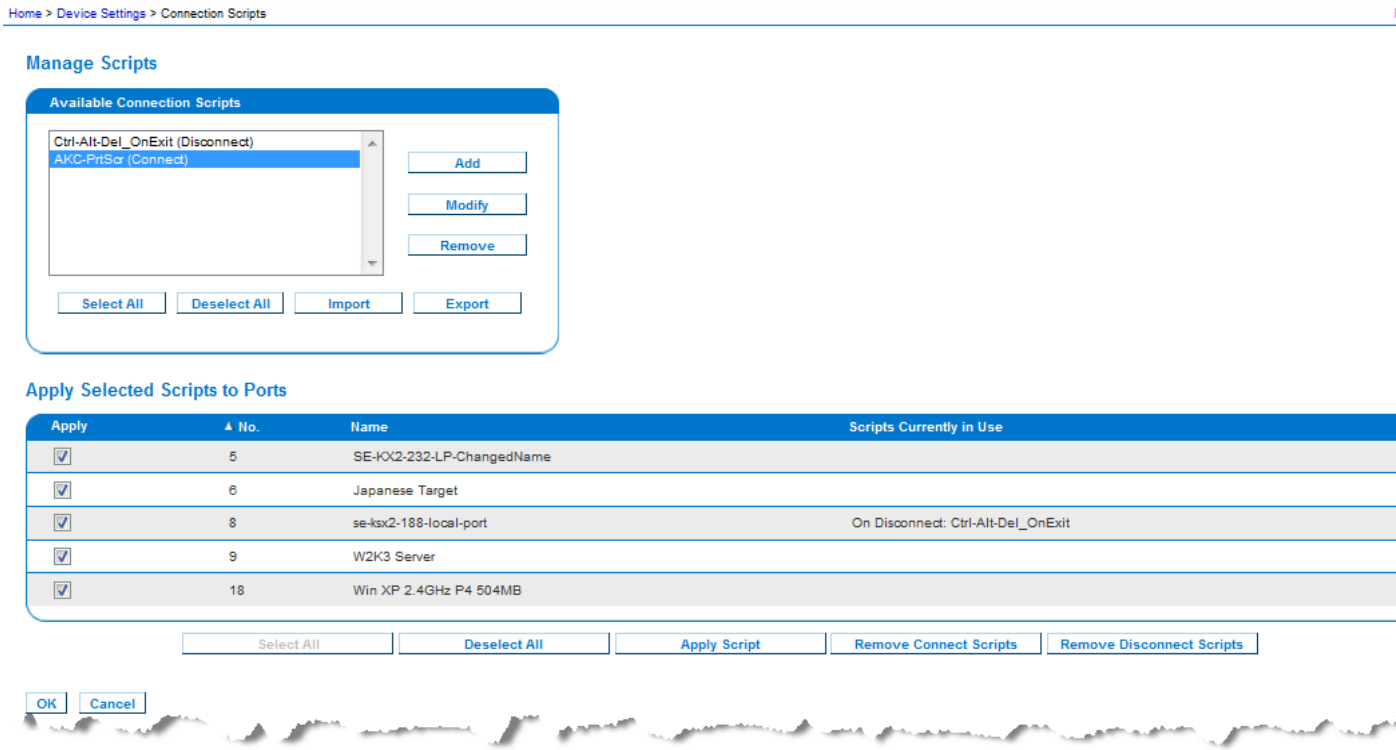
Verbindungs- und Trennungsskripts

Der KX III bietet die Möglichkeit, beim Herstellen oder Trennen der Verbindung mit einem Ziel Tastenmakroskripts auszuführen.

Auf der Seite "Connection Scripts" (Verbindungsskripts) können Sie eigene Skripts erstellen und bearbeiten, um beim Herstellen oder Trennen der Verbindung mit Zielen zusätzliche Aktionen auszuführen.

Stattdessen können Sie auch vorhandene Verbindungsskripts im XML-Dateiformat importieren. Im KX III erstellte Skripts können auch im XML-Dateiformat exportiert werden.

Auf dem KX III können insgesamt 16 Skripts verarbeitet werden.



Anwenden und Entfernen von Skripts

So wenden Sie ein Skript auf Ziele an:

1. Klicken Sie auf "Device Settings" (Geräteeinstellungen) "Keyboard/Mouse" (Tastatur/Maus). Die Seite "Connection Scripts" (Verbindungsskripts) wird geöffnet.
2. Wählen Sie das Skript, das auf das bzw. die Ziele angewendet werden soll, im Abschnitt "Available Connection Scripts" (Verfügbare Verbindungsskripts) aus. Auf ein Ziel kann ein Skript "On Connect" (Beim Verbinden) und ein Skript "On Disconnect" (Beim Trennen der Verbindung) angewendet werden.

Hinweis: Den Zielen kann jeweils nur ein Skript hinzugefügt werden.

3. Wählen Sie im Abschnitt "Apply Selected Scripts to Ports" (Ausgewählte Skripts auf Ports anwenden) die Ziele aus, auf die Sie das Skript anwenden möchten. Verwenden Sie hierfür entweder "Select All" (Alle auswählen), oder klicken Sie auf die entsprechenden Kontrollkästchen links neben den Zielen, um das Skript nur auf ausgewählte Ziele anzuwenden.
4. Klicken Sie auf "Apply Scripts" (Skripts anwenden). Sobald das Skript dem Ziel hinzugefügt wurde, wird es in der Spalte "Scripts Currently in Use" (Aktuell verwendete Skripts) im Abschnitt "Apply Selected Scripts to Ports" (Ausgewählte Skripts auf Ports anwenden) angezeigt.

So entfernen Sie ein Skript von einem Ziel:

1. Wählen Sie im Abschnitt "Apply Selected Scripts to Ports" (Ausgewählte Skripts auf Ports anwenden) das bzw. die Ziele aus, von dem bzw. denen Sie das Skript entfernen möchten. Klicken Sie dazu auf "Select All" (Alle auswählen), oder aktivieren Sie das Kontrollkästchen links neben dem jeweiligen Ziel, um das Skript nur von bestimmten Zielen zu entfernen.
2. Klicken Sie auf "Remove Connect Scripts" (Verbindungsskripts entfernen), um die Verbindungsskripts zu entfernen, oder auf "Remove Disconnect Scripts" (Trennungsskripts entfernen), um die Skripts zum Trennen der Verbindung zu entfernen.

Hinzufügen von Skripts

Hinweis: Sie können auch Skripts hinzufügen, die außerhalb von KX III erstellt wurden, und sie dann als XML-Dateien importieren. Siehe **Importieren und Exportieren von Skripts** *(auf Seite 169).*

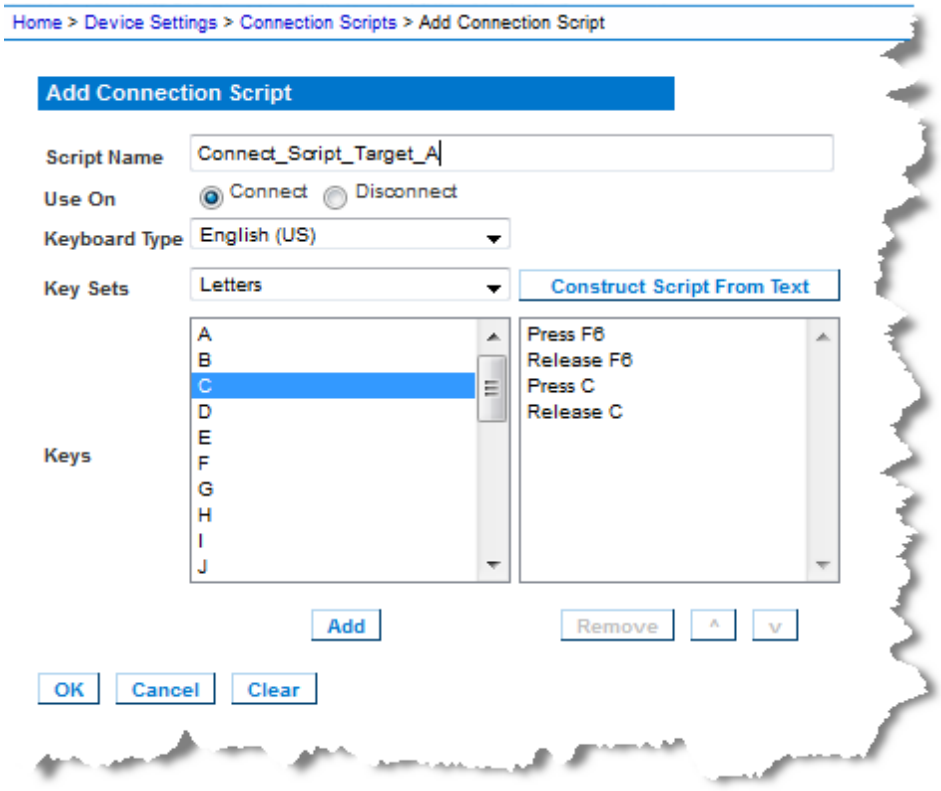
So erstellen Sie ein Skript:

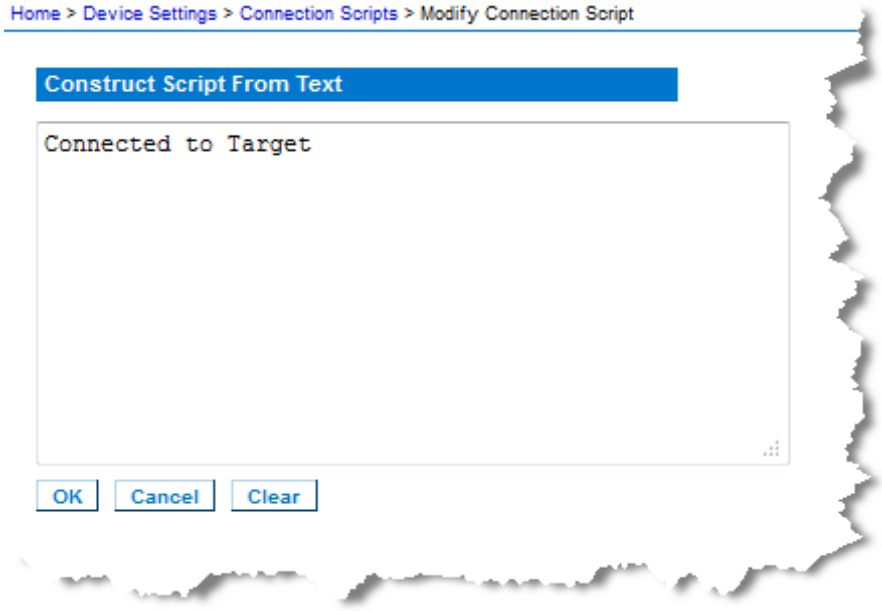
1. Klicken Sie auf "Device Settings" (Geräteeinstellungen) "Keyboard/Mouse" (Tastatur/Maus). Die Seite "Connection Scripts" (Verbindungsskripts) wird geöffnet.
2. Klicken Sie im Abschnitt "Available Connection Scripts" (Verfügbare Verbindungsskripts) auf „Add" (Hinzufügen). Die Seite „Add Connection Scripts" (Verbindungsskripts) wird geöffnet.
3. Geben Sie einen Namen für das Skript mit maximal 32 Zeichen ein. Der Name wird nach dem Erstellen des Skripts im Abschnitt "Available Connection Scripts" (Verfügbare Verbindungsskripts) der Seite "Configure Scripts" (Skripts konfigurieren) angezeigt.

4. Wählen Sie entweder "Connect" (Verbinden) oder "Disconnect" (Trennen) als Typ des zu erstellenden Skripts aus. Verbindungsskripts werden für eine neue Verbindung oder beim Wechseln zu einem Ziel verwendet.
5. Wählen Sie die für das verwendete Ziel erforderliche Tastatur aus.
6. Wählen Sie in der Dropdownliste "Key Sets" (Tastensätze) den Tastaturtastensatz aus, mit dem Sie das Skript erstellen möchten. Sobald ein Tastensatz ausgewählt wurde, werden die ausgewählten Tastensatzoptionen in das Feld "Add" (Hinzufügen) unter der Dropdownliste "Key Sets" (Tastensätze) eingetragen.
7. Wählen Sie eine Taste im Feld "Add" (Hinzufügen) aus, und klicken Sie auf "Add" (Hinzufügen), um sie in das Feld "Script" (Skript) zu verschieben. Zum Entfernen einer Taste aus dem Feld "Script" (Skript) wählen Sie die Taste aus, und klicken Sie auf "Remove" (Entfernen). Wenn Sie die Reihenfolge der Tasten ändern möchten, wählen Sie sie aus, und verwenden Sie die Symbole "Up" (Nach oben) und "Down" (Nach unten).

   Das Skript kann aus einer oder mehreren Tasten bestehen. Darüber hinaus können Sie die im Skript zu verwendenden Tasten mischen und abgleichen.

   Wählen Sie z. B. F1-F16, um den Funktionstastensatz im Feld "Add" (Hinzufügen) anzuzeigen. Wählen Sie eine Funktionstaste, und fügen Sie sie dem Feld "Script" (Skript) hinzu. Wählen Sie als Nächstes "Letters" (Buchstaben) in der Dropdownliste "Key Set" (Tastensatz) aus, und fügen Sie dem Skript eine Buchstabentaste hinzu.
8. Wahlweise können Sie Text hinzufügen, der angezeigt wird, sobald das Skript ausgeführt wird.
   a. Klicken Sie auf "Construct Script from Text" (Skript aus Text erstellen), um die Seite "Construct Script From Text" (Skript aus Text erstellen) zu öffnen.
   b. Geben Sie das Skript in das Textfeld ein. Geben Sie z. B. "Connected to Target" (Mit Ziel verbunden) ein.
   c. Klicken Sie auf der Seite "Construct Script From Text" (Skript aus Text erstellen) auf "OK".
9. Klicken Sie auf "OK", um das Skript zu erstellen.


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
^
v
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

Ändern von Skripts

So ändern Sie vorhandene Skripts:

1. Klicken Sie auf "Device Settings" (Geräteeinstellungen) "Keyboard/Mouse" (Tastatur/Maus). Die Seite "Connection Scripts" (Verbindungsskripts) wird geöffnet.
2. Wählen Sie das zu ändernde Skript im Abschnitt "Available Connection Scripts" (Verfügbare Verbindungsskripts) aus, und klicken Sie auf "Modify" (Ändern). Die Seite befindet sich nun im Bearbeitungsmodus.
3. Nehmen Sie bei Bedarf Änderungen vor. Klicken Sie anschließend auf "OK".

Importieren und Exportieren von Skripts

Sie können nun Verbindungs- und Trennungsskripts im XML-Dateiformat importieren und exportieren. Tastaturmakros können weder im- noch exportiert werden.

Hinweis: Die Import- und Exportfunktion ist über die lokale Konsole nicht verfügbar.

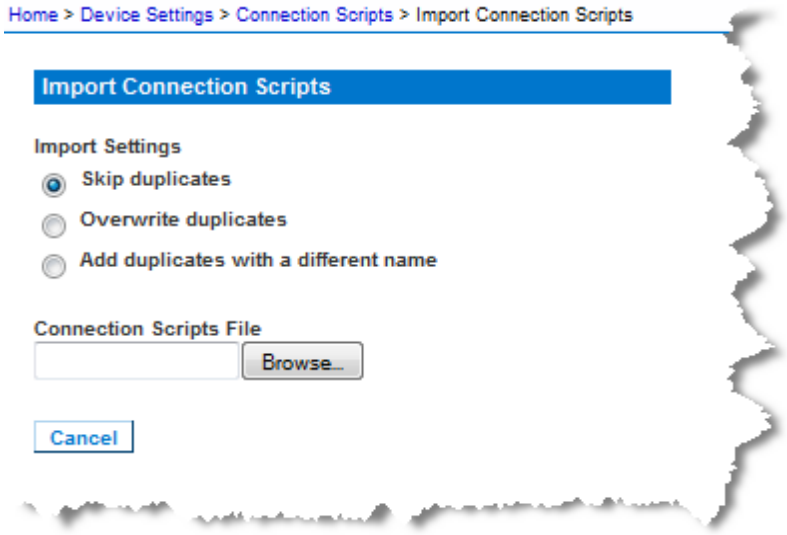
Importierte Skripts können mit der Funktion "Modify" (Ändern) im KX III bearbeitet werden. Sobald ein importiertes Skript jedoch einem Port zugeordnet wird, kann es nicht mehr geändert werden. Entfernen Sie das Skript aus dem Port, um es zu ändern. Siehe ***Anwenden und Entfernen von Skripts*** (auf Seite 165).

So importieren Sie ein Skript:

1. Klicken Sie auf "Device Settings" (Geräteeinstellungen) "Keyboard/Mouse" (Tastatur/Maus). Die Seite "Connection Scripts" (Verbindungsskripts) wird geöffnet.
2. Klicken Sie im Abschnitt "Available Connection Scripts" (Verfügbare Verbindungsskripts) auf "Import" (Importieren). Die Seite "Import Connection Scripts" (Verbindungsskripts importieren) wird geöffnet.
3. Wählen Sie die Einstellung zum Importieren.
   - "Skip duplicates" (Duplikate überspringen) – Bereits im KX III vorhandene Skripts werden nicht in den Import einbezogen.
   - "Overwrite duplicates" (Duplikate überschreiben) – Bereits im KX III vorhandene Skripts werden durch das neue, importierte Skript überschrieben.

- "Add duplicates with a different name" (Duplikate mit anderem Namen hinzufügen) – Doppelte Skripts werden beim Importieren umbenannt, sodass vorhandene Skripts nicht überschrieben werden. Vom KX III wird dem Dateinamen eine Zahl zugewiesen, um das Skript vom Original zu unterscheiden.

4. Verwenden Sie die Funktion zum Durchsuchen, um die zu importierenden XML-Skriptdateien zu suchen.
5. Klicken Sie auf "Importieren". Die Seite "Configuration Scripts" (Konfigurationsskripts) wird geöffnet, und die importierten Skripts werden angezeigt.



So exportieren Sie ein Trennungsskript:

1. Klicken Sie auf "Device Settings" (Geräteeinstellungen) "Configuration Scripts" (Konfigurationsskripts). Die Seite "Configuration Scripts" (Konfigurationsskripts) wird geöffnet.
2. Wählen Sie das zu exportierende Skript im Abschnitt "Available Connection Scripts" (Verfügbare Verbindungsskripts) aus, und klicken Sie auf "Export" (Exportieren). Daraufhin wird ein Dialogfeld mit der Frage angezeigt, ob die XML-Datei geöffnet oder gespeichert werden soll.
3. Speichern Sie die XML-Datei, oder öffnen Sie sie in einem XML-Editor. Wenn Sie die XML-Datei speichern, wird sie in Ihrem Standardordner für Downloads abgelegt.

Portgruppenverwaltung

Die Portgruppenverwaltung bezieht sich auf Folgendes:

- Bladeservergruppe – der Zusammenschluss von Ports, die mit verschiedenen Bladetypen verbunden sind, zu einer Gruppe, die das Blade-Chassis repräsentiert Siehe ***Konfigurieren von HP- und Cisco UCS-Blade-Chassis (Portgruppenverwaltung)*** (auf Seite 121)
- Duale Videoportgruppe – das Erstellen von Portgruppen, die erweiterte Dekstopkonfigurationen auf Zielservern ermöglichen Siehe ***Erstellen dualer Videoportgruppen*** (auf Seite 173).
- Portrguppe – das Erstellen von Standardportgruppen, wobei die Einstellungen für einen primären Port für alle sekundären Ports in der Gruppe übernommen werden Siehe ***Erstellen von Portgruppen*** (auf Seite 172).

Erstellen von Portgruppen

KX III unterstützt den Zusammenschluss von mehreren Ports zu einer einzelnen Portgruppe. Portgruppen bestehen nur aus Ports, die als Standard-KVM-Ports konfiguriert sind. Ein Port kann nur einer einzigen Gruppe angehören.

Ports, die für eine Porgruppe zur Verfügung stehen, werden in der Liste "Select Port for Group Available" (Port für Gruppe auswählen > Verfügbar) angezeigt. Nachdem ein Port zu einer Portgruppe hinzugefügt wurde, steht er nicht mehr für eine andere Portgruppe zur Verfügung. Entfernen Sie den Port aus der vorhandenen Portgruppe, um ihn in einer neuen Portgruppe zu verwenden.

Aktionen für das Verbinden und Trennen, die vom primären Port ausgeführt werden, werden für die sekundären Ports in der Gruppe übernommen, ausgenommen der Stromzufuhrsteuerung.

Portgruppen werden mithilfe der Option "Backup and Restore" (Sicherung und Wiederherstellung) wiederhergestellt (siehe ***Backup and Restore*** (siehe "***Backup/Restore (Sicherung/Wiederherstellung)***" auf Seite 199) (Sicherung und Wiederherstellung)).

Hinweis: Informationen zum Erstellen von Portgruppen für Blade-Chassis finden Sie unter **Konfigurieren von HP- und Cisco USC-Blade-Chassis (Portgruppenverwaltung)** *(siehe "***Konfigurieren von HP- und Cisco UCS-Blade-Chassis (Portgruppenverwaltung)***" auf Seite 121), und Informationen zum Erstellen von dualen Videoportgruppen finden Sie unter Erstellen dualer Videoportgruppen.*

So erstellen Sie eine Portgruppe:

1. Wählen Sie "Device Settings > Port Group Management" (Geräteeinstellungen > Portgruppenverwaltung) aus. Die Seite "Port Group Management" (Portgruppenverwaltung) wird angezeigt. Alle vorhandenen Portgruppen werden angezeigt.
2. Klicken Sie auf Hinzufügen. Die Seite wird aktualisiert, und es werden alle verfügbaren Optionen für Portgruppen angezeigt.
3. Aktivieren Sie das Optionsfeld "Port Group" (Portgruppe).
4. Wählen Sie die Ports aus, die Sie zur Gruppe hinzufügen möchten, indem Sie im Textfeld "Available" (Verfügbar) auf die Ports und anschließend auf "Add" (Hinzufügen) klicken, um sie zum Textfeld "Selected" (Ausgewählt) hinzuzufügen.
5. Klicken Sie auf "OK", um die Portgruppe zu erstellen. Die Portgruppe wird jetzt auf der Seite "Port Group Management" (Portgruppenverwaltung) angezeigt.

Erstellen dualer Videoportgruppen

Mit dualen Videoportgruppen können Sie zwei Videoports in eine Gruppe gruppieren. Verwenden Sie diese Funktion, wenn Sie einen Server mit zwei Videokarten/-ports verbinden müssen und Sie gleichzeitig über denselben Client auf beide Ports zugreifen möchten.

Hinweis: Duale Videoportgruppen werden von Modellen mit nur einem KVM-Kanal, wie z. B. KX2-108 und KX2-116, nicht unterstützt.

Hinweis: Nachdem eine duale Videoportgruppe erstellt wurde, steht sie über die lokale Konsole und über den Remoteclient zur Verfügung. Jedoch wird der erweiterte Desktop nicht von der lokalen Konsole unterstützt.

Dual Video-Portgruppen werden auf der Seite für den Portzugriff als Dual Port-Typen angezeigt. Die primären und sekundären Ports, die Teil einer Portgruppe sind, werden auf der Seite für den Portzugriff jeweils als Dual Port(P) und Dual Port(S) angezeigt. Wenn der CIM-Typ beispielsweise DCIM lautet, wird "DCIM Dual Port (P)" angezeigt.

Jede Gruppe muss einen primären und einen sekundären Port enthalten. Die für den primären Port verwendete Konfiguration wird für alle sekundären Ports in der Gruppe verwendet. Wenn ein Port aus der Gruppe entfernt wird, wird er als unabhängiger Port behandelt, und Sie können eine neue Konfiguration anwenden.

Wenn Sie auf eine Dual Port-Videogruppe über den Remote-Client zugreifen, stellen Sie eine Verbindung zum primären Port her, der das Fenster für die KVM-Verbindung für die primären und sekundären Ports der Dual Port-Gruppe öffnet.

Die Sitzungen können vom Remoteclient auf einem oder mehreren Monitoren gestartet und angezeigt werden.

Die Ausrichtung, die auf dem Gerät für das Ziel konfiguriert wurde, muss mit der tatsächlichen Konfiguration des Betriebssystems auf dem Zielgerät übereinstimmen.

Es wird empfohlen, dass der Verbindungsclient dieselbe Bildschirmausrichtung aufweist.

Wichtig: Informationen zu Einschränkungen, Empfehlungen usw., die Ihre spezifische Umgebung betreffen, finden Sie unter Duale Videoportgruppen.

So erstellen Sie eine duale Videoportgruppe:

1. Wählen Sie "Device Settings > Port Group Management" (Geräteeinstellungen > Portgruppenverwaltung) aus. Die Seite "Port Group Management" (Portgruppenverwaltung) wird angezeigt. Alle vorhandenen Portgruppen werden angezeigt.

2. Klicken Sie auf Hinzufügen. Die Seite "Port Group" (Portgruppe) wird angezeigt, and all verfügbar ports are displayed in the Wählen Sie Ports for 'Gruppe: bereich.

   Hinweis: Wenn ein Port bereits zu einer Bladeserver-Portgruppe, einer anderen dualen Videoportgruppe oder einer Standardportgruppe gehört, steht der Port nicht zur Verfügung, da Ports jeweils nur zu einer Gruppe gehören können.

3. Aktivieren Sie das Optionsfeld "Dual Video Port Group" (Duale Videoportgruppe).
4. Klicken Sie im Bereich "Select Ports for Group" (Ports für Gruppen auswählen) auf den Port, den Sie als primären Port festlegen möchten, und klicken Sie anschließend auf "Add" (Hinzufügen), um ihn zum Textfeld "Selected" (Ausgewählt) hinzuzufügen. Sie müssen zuerst den primären Port hinzufügen.

   Hinweis: Idealerweise sollten die auf jeden Port angewendeten Berechtigungen in der Portgruppe gleich sein. Ist dies nicht der Fall, werden die Berechtigungen des Ports mit den restriktivsten Berechtigungen auf die Portgruppe angewendet. Sollte zum Beispiel die VM-Zugriffsverweigerung auf einen Port und VM-Lese-/Schreibzugriff auf einen anderen Port angewendet sein, wird die VM-Zugriffsverweigerung auf die Portgruppe angewendet. Weitere Informationen darüber, welche Auswirkungen Portberechtigungen auf Dual Video-Portgruppen haben, finden Sie unter **Berechtigungen und Zugriff auf Dual Video-Portgruppen** *(siehe "***Berechtigungen und Zugriff auf duale Videoportgruppen***" auf Seite 234).*

5. Klicken Sie auf den Port, den Sie als sekundären Port festlegen möchten, und klicken Sie anschließend auf "Hinzufügen", um ihn zum Textfeld "Selected" (Ausgewählt) hinzuzufügen.
6. Wählen Sie die Ausrichtung der Seite aus. Wählen Sie eine Ausrichtung, die am besten mit Ihrem Monitorsetup funktioniert.
7. Klicken Sie auf "OK", um die Portgruppe zu erstellen.

   Dual Video-Portgruppen werden auf der Seite für den Portzugriff als Dual Port-Typen angezeigt. Die primären und sekundären Ports, die Teil einer Portgruppe sind, werden auf der Seite für den Portzugriff jeweils als Dual Port(P) und Dual Port(S) angezeigt. Wenn der CIM-Typ beispielsweise DCIM lautet, wird "DCIM Dual Port (P)" angezeigt.

Hinweis: Duale Videoportziele, die mit einem Schichtgerät verbunden sind, dürfen nur über das Schichtgerät und nicht über das Basisschichtgerät angeschlossen werden.

Ändern der Standardeinstellung für die GUI-Sprache

Die grafische Benutzeroberfläche (GUI) von KX III für Englisch, unterstützt auch die folgenden lokalisierten Sprachen:

- Japanisch
- Simplified Chinese (Vereinfachtes Chinesisch)
- Traditional Chinese (Traditionelles Chinesisch)

So ändern Sie die GUI-Sprache:

1. Wählen Sie "Device Settings" (Geräteeinstellungen) "Language" (Sprache). Die Seite "Language Settings" (Spracheinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdownliste "Language" (Sprache) die Sprache für die GUI aus.
3. Klicken Sie auf "Apply" (Übernehmen). Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen), um die Sprache wieder auf "English" (Englisch) zurückzusetzen.

Hinweis: Sobald Sie eine neue Sprache übernehmen, wird die Online-Hilfe ebenfalls Ihrer Sprachauswahl entsprechend lokalisiert.

Sicherheitsverwaltung

Security Settings (Sicherheitseinstellungen)

Auf der Seite "Security Settings" (Sicherheitseinstellungen) können Sie Anmeldebeschränkungen angeben, Benutzer blockieren, Kennwortregeln festlegen und Daten verschlüsseln und freigeben.

Für den Austausch öffentlicher und privater Schlüssel werden SSL-Zertifikate von Raritan verwendet, die zusätzliche Sicherheit bieten. Raritan-Webserverzertifikate sind selbstsigniert. Java-Applet-Zertifikate sind durch ein VeriSign-Zertifikat signiert. Die Verschlüsselung gewährleistet, dass Ihre Daten vor Lauschangriffen gesichert sind und diese Zertifikate stellen sicher, dass Sie sich auf die Raritan Inc. Einheit verlassen können.

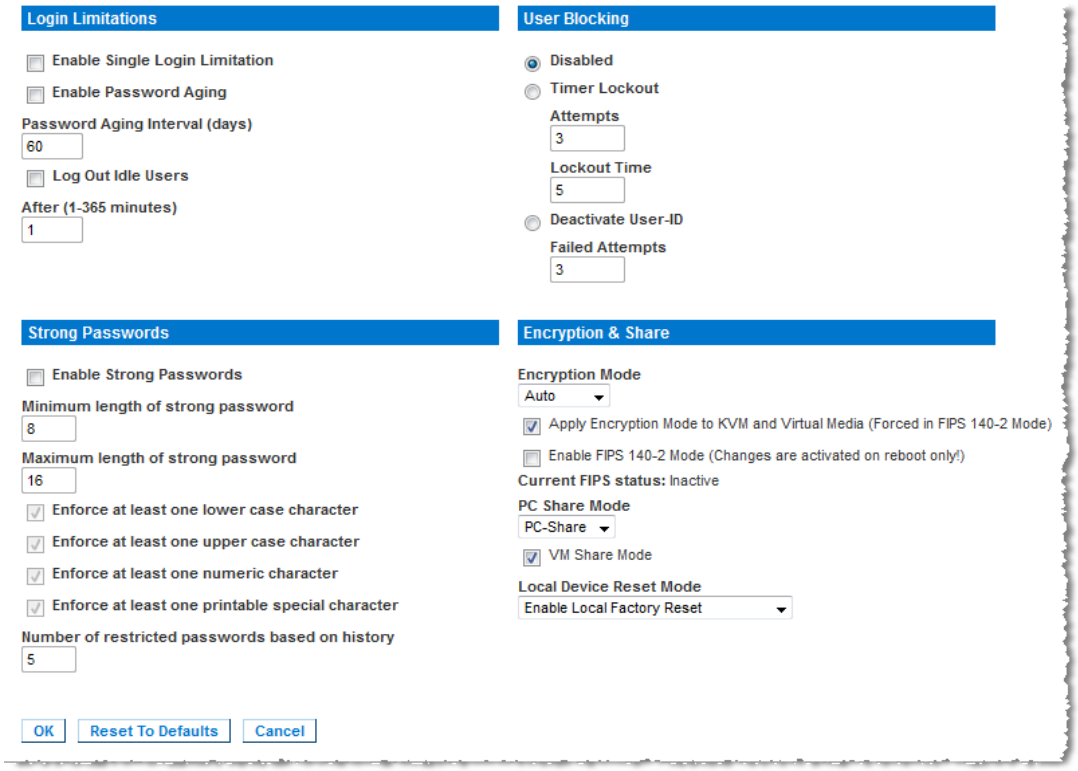
So konfigurieren Sie die Sicherheitseinstellungen:

1. Wählen Sie **Security > Security Settings** (Sicherheit > Sicherheitseinstellungen). Die Seite **Security Settings** (Sicherheitseinstellungen) wird angezeigt.
2. Aktualisieren Sie ggf. die Einstellungen unter ***Login Limitations (Anmeldebeschränkungen)*** (siehe "***Anmeldebeschränkungen***" auf Seite 176).

3. Aktualisieren Sie ggf. die Einstellungen unter ***Strong Passwords (Sichere Kennwörter)*** (auf Seite 178).
4. Aktualisieren Sie ggf. die Einstellungen für ***User Blocking (Benutzersperrung)*** (auf Seite 180).
5. Aktualisieren Sie ggf. die Einstellungen unter Encryption & Share (Verschlüsselung und Freigabe).
6. Klicken Sie auf "OK".

So stellen Sie die Standardwerte wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

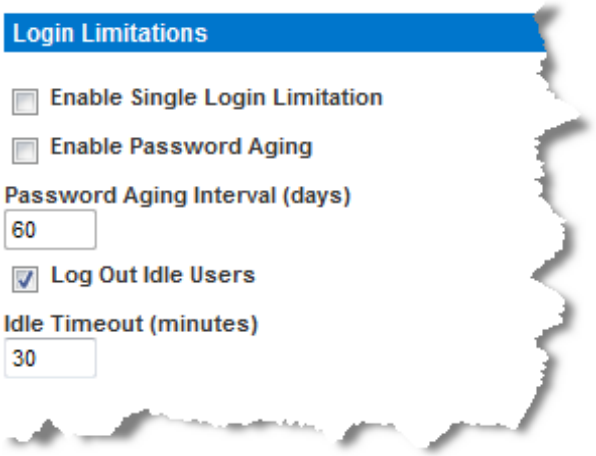


Anmeldebeschränkungen

Mithilfe von Anmeldebeschränkungen können Sie Beschränkungen für Einzelanmeldungen, die Geltungsdauer von Kennwörtern und das Abmelden inaktiver Benutzer festlegen.

Beschränkung	Beschreibung
"Enable single login	Wenn Sie dieses Kontrollkästchen aktivieren, ist

Beschränkung	Beschreibung
limitation" (Beschränkung für Einzelanmeldung aktivieren)	pro Benutzername immer nur eine Anmeldung zulässig. Ist es dagegen deaktiviert, kann eine Benutzername-/Kennwortkombination von mehreren Client-Workstations gleichzeitig verwendet werden, um eine Verbindung mit dem Gerät herzustellen.
"Enable Password Aging" (Erneuerung des Kennworts aktivieren)	Wenn Sie dieses Kontrollkästchen aktivieren, müssen alle Benutzer ihr Kennwort abhängig von der Anzahl der Tage, die Sie im Feld "Password Aging Interval" (Intervall für Kennworterneuerung) eingegeben haben, regelmäßig ändern. Dieses Feld ist aktiv und erforderlich, wenn Sie das Kontrollkästchen "Enable Password Aging" (Erneuerung des Kennworts aktivieren) aktiviert haben. Geben Sie den Zeitraum in Tagen an, nach dessen Ablauf ein Kennwort geändert werden muss. Der Standardwert ist 60 Tage.
"Log out idle users, After (1-365 minutes)" (Inaktive Benutzer abmelden, Nach (1-365 Minuten))	Aktivieren Sie das Kontrollkästchen "Log off idle users" (Inaktive Benutzer abmelden), um die Verbindung von Benutzern automatisch zu trennen, wenn der im Feld "After (1-365 minutes)" [Nach (1-365 Minuten)] angegebene Zeitraum abgelaufen ist. Wenn keine Tastatur- oder Mausaktivitäten stattfinden, werden alle Sitzungen und Ressourcen abgemeldet. Für virtuelle Mediensitzungen gibt es hingegen kein Zeitlimit. Das Feld "After" (Nach) dient zum Festlegen der Zeitspanne (in Minuten), nach der ein inaktiver Benutzer abgemeldet wird. Dieses Feld ist aktiv, wenn Sie das Kontrollkästchen "Log Out Idle Users" (Inaktive Benutzer abmelden) aktiviert haben. Als Feldwert können bis zu 365 Minuten eingegeben werden.



Strong Passwords (Sichere Kennwörter)

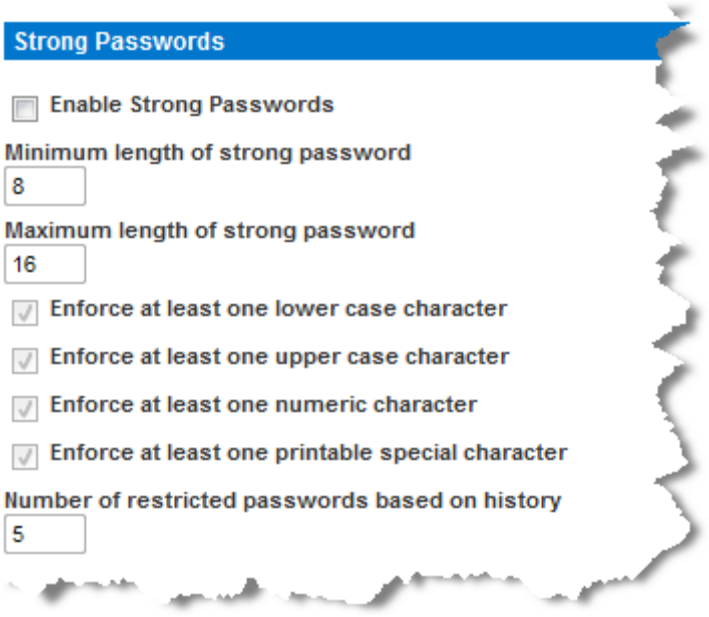
Sichere Kennwörter sorgen für eine sicherere lokale Authentifizierung des Systems. Im Bereich "Strong Passwords" (Sichere Kennwörter) können Sie das Format gültiger lokaler KX III-Kennwörter wie Mindest- und Höchstlänge, erforderliche Zeichen und Aufbewahrung des Kennwortverlaufs festlegen.

Damit ein Kennwort sicher ist, muss es eine Mindestlänge von acht Zeichen haben sowie mindestens ein alphabetisches Zeichen und ein nicht-alphabetisches Zeichen (Satzzeichen oder Ziffer) umfassen. Darüber hinaus dürfen die ersten vier Zeichen des Kennworts und des Benutzernamens nicht identisch sein.

Wenn Sie diese Option aktivieren, gelten die Regeln für sichere Kennwörter. Benutzer, deren Kennwörter nicht den Kriterien für sichere Kennwörter entsprechen, werden bei der nächsten Anmeldung automatisch aufgefordert, ihr Kennwort zu ändern. Ist das Kontrollkästchen deaktiviert, gilt nur die Standardformatvalidierung. Bei aktiviertem Kontrollkästchen sind die folgenden Felder aktiv und erforderlich:

Feld	Beschreibung
Minimum length of strong password (Mindestlänge des sicheren Kennworts)	Kennwörter müssen mindestens 8 Zeichen umfassen. Die Standardeinstellung gibt 8 Zeichen vor, aber der Administrator kann das Minimum auf 63 Zeichen erweitern.
Maximum length of strong password (Höchstlänge des sicheren Kennworts)	Die standardmäßige Mindestlänge eines Kennworts beträgt 8 Zeichen, aber der Administrator kann die Höchstlänge auf 16 Zeichen einstellen. Die Höchstlänge sicherer Kennwörter

Feld	Beschreibung
	beträgt 63 Zeichen.
Enforce at least one lower case character (Mindestens einen Kleinbuchstaben erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Kleinbuchstaben enthalten.
Enforce at least one upper case character (Mindestens einen Großbuchstaben erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Großbuchstaben enthalten.
Enforce at least one numeric character (Mindestens eine Ziffer erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens eine Ziffer enthalten.
Enforce at least one printable special character (Mindestens ein druckbares Sonderzeichen erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens ein (druckbares) Sonderzeichen enthalten.
Number of restricted passwords based on history (Anzahl unzulässiger Kennwörter basierend auf Verlauf)	Dieses Feld bezieht sich auf die Verlaufstiefe, d. h. die Anzahl vorheriger Kennwörter, die nicht wiederholt werden dürfen. Ein Bereich zwischen 1 und 12 ist möglich, der Standardwert liegt bei 5.



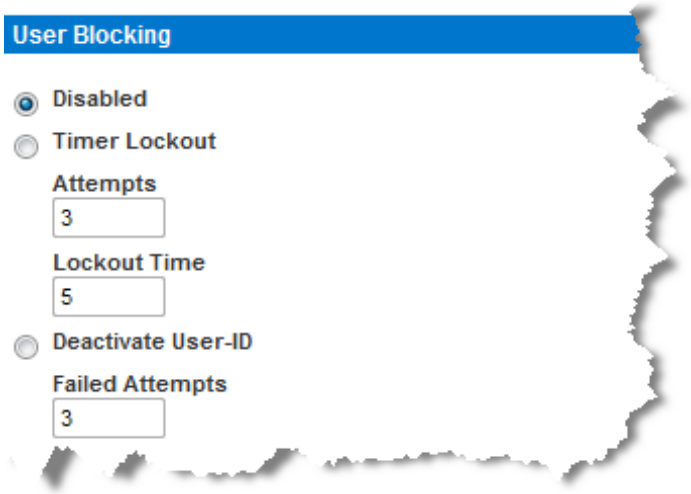
User Blocking (Benutzersperrung)

Mithilfe der Optionen unter "User Blocking" (Benutzersperrung) geben Sie die Kriterien an, anhand derer Benutzer nach der festgelegten Zahl von Anmeldefehlversuchen am Zugriff auf das System gehindert werden.

Die drei Optionen schließen sich gegenseitig aus.

Option	Beschreibung
"Disabled" (Deaktiviert)	Dies ist die Standardoption. Benutzer werden unabhängig von der Anzahl fehlgeschlagener Anmeldeversuche nicht blockiert.

Option	Beschreibung
"Timer Lockout" (Zeitliche Sperre)	Benutzern wird der Zugriff auf das System für den festgelegten Zeitraum verweigert, nachdem sie eine bestimmte Anzahl von Anmeldefehlversuchen überschritten haben. Bei dieser Option stehen die folgenden Felder zur Verfügung: ▪ "Attempts" (Versuche) – Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche ein, nach der ein Benutzer gesperrt wird. Ein Bereich zwischen 1 und 10 ist möglich, der Standardwert liegt bei 3 Versuchen. ▪ "Lockout Time" (Dauer der Sperre) – Geben Sie die Zeitspanne ein, für die der Benutzer gesperrt wird. Ein Bereich zwischen 1 und 1.440 Minuten ist möglich, der Standardwert liegt bei 5 Minuten. *Hinweis: Administratoren sind von einer zeitlichen Sperre ausgenommen.*
"Deactivate User-ID" (Benutzer-ID deaktivieren)	Diese Option legt fest, dass dem Benutzer nach der Anzahl der im Feld "Failed Attempts" (Fehlversuche) angegebenen Anmeldefehlversuche der Zugriff auf das System verweigert wird. ▪ "Failed Attempts" (Fehlversuche) – Geben Sie die Anzahl der Anmeldefehlversuche ein, nach der die Benutzer-ID eines Benutzers deaktiviert wird. Dieses Feld steht zur Verfügung, wenn Sie die Option "Deactivate User-ID" (Benutzer-ID deaktivieren) wählen. Der gültige Bereich liegt zwischen 1 und 10. Wenn eine Benutzer-ID nach der angegebenen Anzahl der Anmeldefehlversuche deaktiviert wird, muss der Administrator das Benutzerkennwort ändern und das Benutzerkonto wieder aktivieren, indem er auf der Seite "User" (Benutzer) das Kontrollkästchen "Active" (Aktiv) aktiviert.



Verschlüsselung und Freigabe

Mithilfe der Einstellungen unter "Encryption & Share" (Verschlüsselung und Freigabe) können Sie die Art der Verschlüsselung, PC- und VM-Freigabemodi sowie die Art der Zurücksetzung festlegen, wenn die Taste "Reset" (Zurücksetzen) an der KX III-Einheit gedrückt wird.

WARNUNG: Wenn Sie einen Verschlüsselungsmodus auswählen, der von Ihrem Browser nicht unterstützt wird, können Sie von Ihrem Browser aus nicht auf KX III zugreifen.

Konfiguration von Verschlüsselung und Freigabe

Bemerken Sie, dass die Leistung beeinflusst werden könnte, sobald die Verschlüsselung aktiviert ist. Der Umfang der Leistungsauswirkung hängt von dem Verschlüsselungsmodus ab.

Für die bestmögliche Video-Leistung und Durchsatz, deaktivieren Sie die Verschlüsselung, wenn Ihre Sicherheitspolitik dies zulässt.

Encryption Share (Verschlüsselung und Freigabe konfigurieren)

1. Wählen Sie eine Option aus der Dropdownliste "Encryption Mode" (Verschlüsselungsmodus) aus.

   Wenn Sie einen Verschlüsselungsmodus ausgewählt haben, wird eine Warnung angezeigt, dass Sie keine Verbindung zu KX III mehr herstellen können, falls Ihr Browser den gewählten Modus nicht unterstützt.

Die Warnung lautet "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the KX III" (Wenn Sie den Verschlüsselungsmodus festlegen, stellen Sie sicher, dass Ihr Browser diesen unterstützt, ansonsten können Sie keine Verbindung zu KX III herstellen).

Verschlüsselungsmodus	Beschreibung
Automatisch	Dies ist die empfohlene Option. KX III verwendet automatisch das höchstmögliche Verschlüsselungsniveau. Sie *müssen* "Auto" (Automatisch) auswählen, damit Gerät und Client erfolgreich die verwendeten FIPS-konformen Algorithmen verarbeiten können.
RC4	Sichert Benutzernamen, Kennwörter und KVM-Daten einschließlich Videoübertragungen mithilfe der Verschlüsselungsmethode RSA RC4. Dies ist ein 128-Bit-SSL-Protokoll (Secure Sockets Layer), das während der Anfangsverbindungsauthentifizierung einen privaten Kommunikations-Channel zwischen dem KX III Gerät und dem Remote-PC bereitstellt. Wenn Sie den Modus FIPS 140-2 aktivieren und RC4 ausgewählt wurde, erhalten Sie eine Fehlermeldung. Im Modus FIPS 140-2 ist RC4 nicht verfügbar.
AES-128	Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 128 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option (AES-128) darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter ***Prüfen Ihres Browsers auf AES-Verschlüsselung*** (auf Seite 186).
AES-256	Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 256 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst

Verschlüsselungsmodus	Beschreibung
	keine Verbindung herstellen können. Weitere Informationen finden Sie unter ***Prüfen Ihres Browsers auf AES-Verschlüsselung*** (auf Seite 186).

Hinweis: Wenn Sie Windows XP® mit Service Pack 2 verwenden, kann Internet Explorer® 7 keine Remoteverbindung zu KX III herstellen, wenn die AES-128-Verschlüsselung verwendet wird.

2. Apply Encryption Mode to KVM and Virtual Media (Verschlüsselungsmodus auf KVM und virtuelle Medien anwenden): Wenn Sie dieses Kontrollkästchen aktivieren, wird der gewählte Verschlüsselungsmodus auf KVM und virtuelle Medien angewendet. Nach der Authentifizierung werden die KVM- und virtuellen Mediendaten ebenfalls mit der 128-Bit-Verschlüsselung übertragen.
3. Für das Arbeiten in Regierungs- und anderen Hochsicherheitsumgebungen muss der Modus FIPS 140-2 durch Aktivieren des Kontrollkästchens "Enable FIPS 140-2" (Aktivieren von FIPS 140-2) ausgewählt werden. Weitere Informationen zur Aktivierung von FIPS 140-2 finden Sie unter ***Aktivieren von FIPS 140-2*** (auf Seite 186).
4. Modus "PC Share" (PC-Freigabe) – Bestimmt den globalen gleichzeitigen KVM-Remotezugriff und ermöglicht bis zu acht Remotebenutzern die gleichzeitige Anmeldung bei einer KX III-Einheit sowie die gleichzeitige Anzeige und Steuerung desselben Zielservers über das Gerät. Klicken Sie auf die Dropdownliste, um eine der folgenden Optionen auszuwählen:
   - Private (Privat) – Keine PC-Freigabe. Dies ist der Standardmodus. Jeder Zielserver ist jeweils nur für einen Benutzer exklusiv zugänglich.
   - PC-Share (PC-Freigabe) – Bis zu acht Benutzer (Administratoren oder Nicht-Administratoren) können gleichzeitig auf KVM-Zielserver zugreifen. Jeder Remotebenutzer besitzt dieselbe Kontrolle über Tastatur und Maus. Beachten Sie jedoch, dass eine ungleichmäßige Steuerung auftritt, wenn ein Benutzer seine Tastatur- bzw. Mauseingabe nicht unterbricht.
5. Wählen Sie bei Bedarf den Modus "VM Share" (VM-Freigabe) aus. Diese Option steht nur zur Verfügung, wenn der PC-Freigabemodus aktiviert wurde. Wenn dieses Kontrollkästchen aktiviert ist, werden virtuelle Medien für mehrere Benutzer freigegeben, d. h. diese können gemeinsam auf dieselbe virtuelle Mediensitzung zugreifen. Standardmäßig ist dieses Kontrollkästchen deaktiviert.

6. Wählen Sie bei Bedarf den Modus "Local Device Reset" (Lokales Gerät zurücksetzen) aus. Diese Option legt fest, welche Maßnahmen ergriffen werden, wenn die Taste zum Zurücksetzen der Hardware auf der Rückseite des Geräts gedrückt wird. Weitere Informationen finden Sie unter Zurücksetzen von KX III mithilfe der Taste "Reset" (Zurücksetzen). Wählen Sie eine der folgenden Optionen aus:

Modus zum Zurücksetzen eines lokalen Geräts	Beschreibung
Enable Local Factory Reset (Lokale Werkrücksetzung aktivieren, Standardeinstellung)	Setzt das KX III-Gerät auf die werksseitigen Standardeinstellungen zurück.
Enable Local Admin Password Reset (Lokale Administrator-Kennwortrücksetzung aktivieren)	Setzt nur das Kennwort des lokalen Administrators zurück. Das Kennwort wird auf "raritan" zurückgesetzt.
Disable All Local Resets (Alle lokalen Rücksetzungen deaktivieren)	Es wird keine Rücksetzungsmaßnahme ergriffen.

Hinweis: Wenn Sie P2CIM-AUSBDUAL oder P2CIM-APS2DUAL zum Anschließen eines Ziels an zwei KX IIIn verwenden und der private Zugriff auf die Ziele erforderlich ist, muss für beide KVM-Switches die Option "Private" (Privat) als PC-Freigabemodus ausgewählt werden.

Zusätzliche Informationen zur Verwendung von Paragon CIMs mit KX III finden Sie **unter Unterstützte Paragon-CIMS und Konfigurationen** *(siehe "***Unterstützte Paragon II CIMS und Konfigurationen***" auf Seite 328).*

Prüfen Ihres Browsers auf AES-Verschlüsselung

Wenn Sie nicht wissen, ob Ihr Browser AES nutzt, gleichen Sie das mit dem Browserhersteller ab oder navigieren Sie zur Website https://www.fortify.net/sslcheck.html und verwenden Sie dabei den Browser mit der zu prüfenden Verschlüsselungsmethode. Diese Website erkennt die Verschlüsselungsmethode Ihres Browsers und zeigt einen Bericht an.

Die AES-256-Bit-Verschlüsselung wird nur von folgenden Webbrowsern unterstützt:

- Firefox®
- Internet Explorer®

Für die AES-256-Bit-Verschlüsselung müssen außerdem die Sicherheitsrichtliniendateien für eine unbeschränkte Schlüssellänge der Java Cryptography Extension (JCE) installiert werden.

Diese sogenannten "Unlimited Strength Jurisdiction Policy Files" der verschiedenen JREs™ Versionen finden Sie unter folgendem Link im Bereich "Other Downloads" (Weitere Downloads):

- JRE1.7 - javase/downloads/jce-7-download-432124.html

Aktivieren von FIPS 140-2

Für das Arbeiten in Regierungs- und anderen Hochsicherheitsumgebungen ist es möglicherweise erforderlich, den Modus FIPS 140-2 zu aktivieren.

KX III verfügt über ein integriertes FIPS 140-2-validiertes kryptografisches Modul, das gemäß Abschnitt G.5 der FIPS 140-2 Implementation Guidance auf einer Linux® Plattform ausgeführt wird.

Nach der Aktivierung dieses Moduls muss der private Schlüssel, der zur Generierung des SSL-Zertifikats verwendet wird, intern erzeugt werden. Dieser kann nicht heruntergeladen oder exportiert werden.

Beachten Sie, dass die Leistung beeinflusst werden könnte, sobald der FIPS 140-2 Mode aktiviert ist.

So aktivieren Sie FIPS 140-2:

1. Öffnen Sie die Seite "Security Settings" (Sicherheitseinstellungen).
2. Aktivieren Sie den FIPS 140-2-Modus, indem Sie im Abschnitt "Encryption Share" (Verschlüsselung Freigabe) der Seite "Security Settings" (Sicherheitseinstellungen) das Kontrollkästchen "Enable FIPS 140-2" (Aktivieren von FIPS 140-2) aktivieren.

   Sie nutzen FIPS 140-2-zugelassene Algorithmen für die externe Kommunikation, sobald Sie sich im FIPS 140-2-Modus befinden.

Das kryptografische FIPS-Modul wird für die Verschlüsselung von KVM-Sitzungsdaten verwendet. Dabei handelt es sich um Video-, Tastatur-, Maus- und Smart Card-Daten sowie um die Daten von virtuellen Medien.

3. Starten Sie KX III neu. <erforderlich>

   Sobald der FIPS-Modus aktiviert ist, wird im Abschnitt "Device Information" (Geräteinformationen) im linken Fenster der Bildschirmanzeige "FIPS Mode: Enabled" (FIPS-Modus aktiviert) angezeigt.

   Zusätzliche Sicherheit bietet das Erzeugen einer neuen Zertifikatsregistrierungsanforderung, nachdem der FIPS-Modus aktiviert wurde. Diese wird mithilfe des erforderlichen Schlüsselcodes erzeugt. Laden Sie das Zertifikat hoch, nachdem es signiert wurde, oder erzeugen Sie ein selbstsigniertes Zertifikat. Der SSL-Zertifikatstatus wird von "Not FIPS Mode Compliant" (Nicht FIPS-konform) zu "FIPS Mode Compliant" (FIPS-konform) aktualisiert.

   Ist der FIPS-Modus aktiviert, können keine Schlüsseldateien herunter- oder hochgeladen werden. Die aktuell erzeugte CSR wird der Schlüsseldatei intern zugeordnet. Das SSL-Zertifikat der CA und der zugehörige private Schlüssel sind nicht in der vollständigen Wiederherstellung der gesicherten Datei enthalten. Der Schlüssel kann nicht von KX III exportiert werden.

Anforderungen für die Unterstützung von FIPS 140-2

KX III unterstützt FIPS 140-20-zugelassene Verschlüsselungsalgorithmen. Dadurch können SSL-Server und Client erfolgreich die für die verschlüsselte Sitzung verwendete Verschlüsselungsfolge verarbeiten, sobald ein Client exklusiv für den Modus FIPS 140-2 konfiguriert ist.

Im Folgenden finden Sie Hinweise zur Verwendung von FIPS 140-2 mit KX III:

KX III

- Nehmen Sie auf der Seite Security Settings (Sicherheitseinstellungen) für "Encryption & Share" (Verschlüsselung & Freigabe) die Einstellung auf "Auto" (Automatisch) vor. Siehe Encryption & Share (Verschlüsselung und Freigabe).

Microsoft-Client

- Am Client-Computer und im Internet Explorer muss "FIPS 140-2" aktiviert sein.

So aktivieren Sie "FIPS 140-2" auf einem Windows-Client:

1. Wählen Sie "Systemsteuerung" > "Verwaltung" > "Lokale Sicherheitsrichtline" aus, um das Dialogfeld "Lokale Sicherheitseinstellungen" zu öffnen.

2. Wählen Sie in der Navigationsstruktur "Lokale Richtlinien" > "Sicherheitsoptionen" aus.
3. Aktivieren Sie "Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signierung verwenden".
4. Starten Sie den Client-Computer neu.

So aktivieren Sie "FIPS 140-2" im Internet Explorer:

1. Wählen Sie im Internet Explorer "Extras" > "Internetoptionen", und klicken Sie auf die Registerkarte "Erweitert".
2. Aktivieren Sie das Kontrollkästchen "TLS 1.0 verwenden".
3. Starten Sie den Browser neu.

Konfigurieren der IP-Zugriffssteuerung

Mithilfe der IP-Zugriffssteuerung können Sie den Zugriff auf KX III steuern. Die IP-Zugriffssteuerung schränkt jeglichen Verkehr bezüglich des Zugriffs auf KX III ein, sodass für NTP-Server, RADIUS-Hosts, DNS-Hosts usw. der Zugriff auf >productname< gewährt werden muss.

Durch das Einrichten einer globalen Zugriffssteuerungsliste (Access Control List, ACL) stellen Sie sicher, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet. Die IP-Zugriffssteuerung funktioniert global und betrifft die gesamte KX III-Einheit. Sie können den Zugriff auf das Gerät jedoch auch auf Gruppenebene steuern. Weitere Informationen zur Steuerung auf Gruppenebene finden Sie unter ***Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)*** (auf Seite 64).

Wichtig: Die IP-Adresse "127.0.0.1" wird vom lokalen Port der KX III-Einheit verwendet. Beim Erstellen der IP-Zugriffssteuerungsliste darf sich 127.0.0.1 nicht im Bereich der gesperrten IP-Adressen befinden, sonst können Sie nicht auf den lokalen Port der KX III-Einheit zugreifen.

So verwenden Sie die IP-Zugriffssteuerung:

1. Wählen Sie "Security > IP Access Control" (Sicherheit > IP-Zugriffssteuerung), um die Seite "IP Access Control" (IP-Zugriffssteuerung) zu öffnen.
2. Aktivieren Sie das Kontrollkästchen "Enable IP Access Control" (IP-Zugriffssteuerung aktivieren) sowie die restlichen Felder auf der Seite.
3. Wählen Sie unter "Default Policy" (Standardrichtlinie) eine der im Folgenden genannten Optionen. Damit legen Sie fest, welche Maßnahme für IP-Adressen, die außerhalb der von Ihnen festgelegten Bereiche liegen, ergriffen werden soll.
   - Accept (Akzeptieren) – Diese IP-Adressen können auf das KX III-Gerät zugreifen.

- Drop (Ablehnen) – Diesen IP-Adressen wird der Zugriff auf das KX III-Gerät verweigert.

So fügen Sie Regeln hinzu:

1. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.

   Hinweis: Die IP-Adresse sollte unter Verwendung der CIDR-Notation (Classless Inter-Domain Routing) eingegeben werden. (Hierbei werden die ersten 24 Bits als Netzwerkadresse verwendet.)

2. Wählen Sie in der Dropdown-Liste "Policy" (Richtlinie) eine Richtlinie aus.
3. Klicken Sie auf "Append" (Anfügen). Die Regel wird am Ende der Liste hinzugefügt.

So fügen Sie eine Regel ein:

1. Geben Sie im Feld "Rule #" (Regelnummer) eine Regelnummer ein. Diese ist für den Befehl **Insert** (Einfügen) erforderlich.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.
3. Wählen Sie in der Dropdown-Liste "Policy" (Richtlinie) eine Richtlinie aus.
4. Klicken Sie auf "Insert" (Einfügen). Wenn die eingegebene Regelnummer einer bereits vorhandenen entspricht, wird die neue Regel vor der vorhandenen Regel eingefügt, und alle Regeln werden um eine Position nach unten verschoben.

Tipp: Mithilfe der Regelnummern können Sie die Reihenfolge, in der die Regeln erstellt werden, besser steuern.

So ersetzen Sie eine Regel:

1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.
3. Wählen Sie in der Dropdown-Liste "Policy" (Richtlinie) eine Richtlinie aus.
4. Klicken Sie auf "Replace" (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

So löschen Sie eine Regel:

1. Geben Sie die zu löschende Regelnummer an.
2. Klicken Sie auf "Delete" (Löschen).
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf "OK".

SSL-Zertifikate

Das SSL-Protokoll (Secure Socket Layer) wird für den gesamten verschlüsselten Netzwerkdatenverkehr zwischen KX III und einem mit der Einheit verbundenen Client verwendet.

Wenn eine Verbindung hergestellt wird, muss sich KX III gegenüber einem Client, der ein kryptografisches Zertifikat verwendet, identifizieren.

Es kann eine Zertifikatsregistrierungsanforderung (Certificate Signing Request, CSR) erzeugt werden und ein von der Zertifizierungsstelle (Certificate Authority, CA) signiertes Zertifikat auf dem KX III Gerät installiert werden.

Die CA prüft die Identität des Absenders der CSR.

Anschließend sendet die CA ein signiertes Zertifikat an den Absender. Das Zertifikat mit der Signatur der renommierten CA wird verwendet, um für die Identität des Zertifikatsinhabers zu bürgen.

Wichtig: Vergewissern Sie sich, dass das Datum und die Uhrzeit für

KX III richtig eingestellt sind.

Wenn ein selbstsigniertes Zertifikat erstellt wird, wird das Datum und die Uhrzeit von KX III zum Berechnen des Gültigkeitszeitraums verwendet. Wenn das Datum und die Uhrzeit von KX III ungenau sind, ist möglicherweise der Zeitraum des Zertifikats falsch, was bei der Validierung des Zertifikats zu Fehlern führen kann. Siehe ***Konfigurieren von Datum-/Uhrzeiteinstellungen*** (auf Seite 153).

Hinweis: Die CSR muss auf KX III generiert werden.

Hinweis: Beim Aktualisieren der Firmware werden das aktive Zertifikat und die CSR nicht ersetzt.

So erstellen und installieren Sie ein SSL-Zertifikat:

1. Sicherheit > Zertifikate.
2. Füllen Sie die folgenden Felder aus:
   a. Common Name (Allgemeiner Name) – Der Netzwerkname der KX III Einheit, nachdem diese im Netzwerk installiert wurde (normalerweise der vollqualifizierte Domainname). Der allgemeine Name ist mit dem Namen identisch, der für den Zugriff auf KX III über einen Webbrowser verwendet wird, allerdings ohne das Präfix "http://". Sollte der hier angegebene Name nicht dem tatsächlichen Netzwerknamen entsprechen, wird im Browser eine Sicherheitswarnung angezeigt, wenn über HTTPS auf KX III zugegriffen wird.
   b. Organizational Unit (Organisationseinheit) – In diesem Feld wird angegeben, zu welcher Abteilung der Organisation das KX III Gerät gehört.
   c. Organization (Organisation) – Der Name der Organisation, zu der das KX III Gerät gehört.
   d. Locality/City (Lokalität/Stadt) – Die Stadt, in der sich die Organisation befindet.
   e. State/Province (Bundesland/Region) – Das Bundesland oder die Region, in dem/der sich die Organisation befindet.
   f. Country (ISO code) [Land (ISO-Code)] – Das Land, in dem sich die Organisation befindet. Der ISO-Code ist der aus zwei Buchstaben bestehende Code der Internationalen Organisation für Normung, z. B. "DE" für Deutschland oder "US" für die USA.
   g. Challenge Password (Challenge-Kennwort) – Einige Zertifizierungsstellen verlangen ein Challenge-Kennwort für die Authentifizierung von späteren Änderungen des Zertifikats (z. B. Widerruf des Zertifikats). Zutreffend wenn ein CSR für CA-Zertifikation generiert wird

h. Confirm Challenge Password (Challenge-Kennwort bestätigen) – Bestätigung des Challenge-Kennworts. Zutreffend wenn ein CSR für CA-Zertifikation generiert wird

i. Email (E-Mail) – Die E-Mail-Adresse einer Kontaktperson, die für KX III und dessen Sicherheit verantwortlich ist.

j. Key Length (Schlüssellänge) – Die Länge des erzeugten Schlüssels in Bits. Der Standardwert beträgt 1024.

3. Führen Sie einen der folgenden Schritte aus:

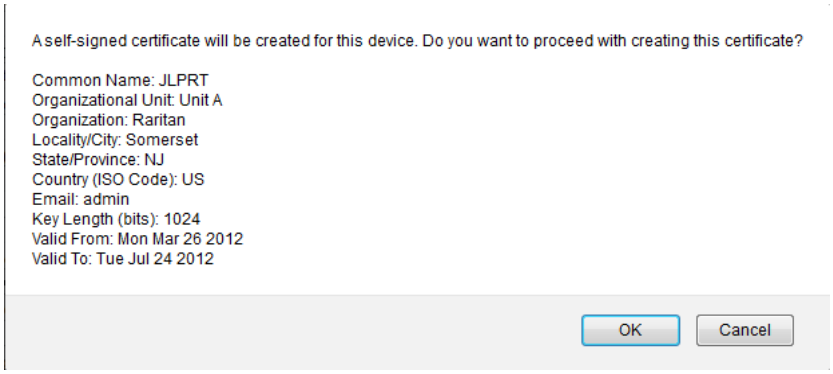
- Um ein selbstsigniertes Zertifikat zu erzeugen, führen Sie Folgendes aus:

a. Aktivieren Sie das Kontrollkästchen "Create a Self-Signed Certificate" (Selbst signiertes Zertifikat erstellen), wenn Sie ein selbst signiertes Zertifikat erstellen müssen. Wenn Sie diese Option aktivieren, generiert KX III das Zertifikat basierend auf Ihren Eingaben, das als signierende Zertifizierungsstelle fungiert. Die CSR muss nicht exportiert und nicht zum Generieren eines signierten Zertifikats verwendet werden.

b. Geben Sie die Anzahl der Tage für den Gültigkeitszeitraum an. Vergewissern Sie sich, dass das Datum und die Uhrzeit von KX III richtig sind, andernfalls kann ein ungültiges Datum zum Erstellen des Gültigkeitszeitraums für das Zertifikat verwendet werden.

c. Klicken Sie auf "Create" (Erstellen).

d. Eine Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "OK", um es zu schließen.

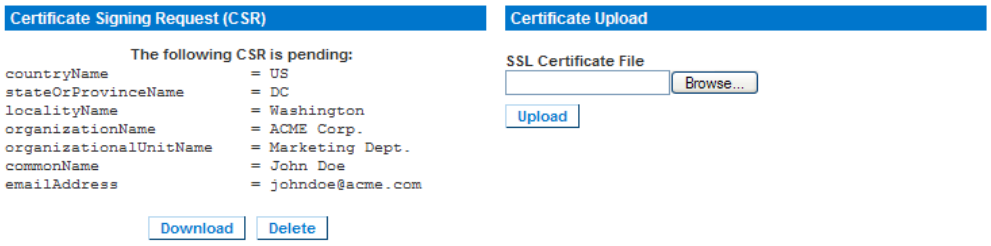


e. Starten Sie KX III neu, um die Zertifikate zu aktivieren.

- Um einen CSR zu generieren und dies zum CA zur Zertifizierung zu senden:

a. Klicken Sie auf "Create" (Erstellen).

b. Ein Dialogfeld wird angezeigt, das alle eingegebenen Informationen enthält.



c. Sie können die CSR und die Datei, die den bei der Erzeugung verwendeten privaten Schlüssel enthalten, herunterladen, indem Sie auf die Schaltfläche "Download" (Herunterladen) klicken.

d. Senden Sie die gespeicherte CSR zur Zertifizierung an eine Zertifizierungsstelle. Sie erhalten von dieser das neue Zertifikat.

Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.

- Sobald Sie das Zertifikat von CA erhalten, laden Sie es in KX III hoch, indem Sie auf die Schaltfläche Hochladen klicken.
- Starten Sie KX III neu, um die Zertifikate zu aktivieren.

Nach Abschluss diese Schritte verfügt KX III über ein eigenes Zertifikat zur Identifizierung gegenüber den Clients.

Wichtig: Wenn Sie die CSR auf der KX III Einheit löschen, kann diese nicht wiederhergestellt werden. Wenn Sie sie versehentlich gelöscht haben, müssen Sie die drei oben beschriebenen Schritte erneut durchführen. Um dies zu vermeiden, verwenden Sie die Downloadfunktion, sodass Sie über eine Kopie der CSR und des privaten Schlüssels verfügen.

Sicherheitsmeldung

KX III ermöglicht Ihnen, eine Sicherheitsmeldung zum Anmeldeprozess von KX III hinzuzufügen. Wenn diese Funktion aktiviert ist, müssen Benutzer vor dem Zugriff auf >ProductName< die Sicherheitsvereinbarung akzeptieren oder ablehnen. Die in einer Sicherheitsmeldung enthaltenen Informationen werden im Dialogfeld "Restricted Service Agreement" (Eingeschränkte Dienstvereinbarung) angezeigt, nachdem Benutzer nach Eingabe Ihrer Anmeldeinformationen auf KX III zugegriffen haben.

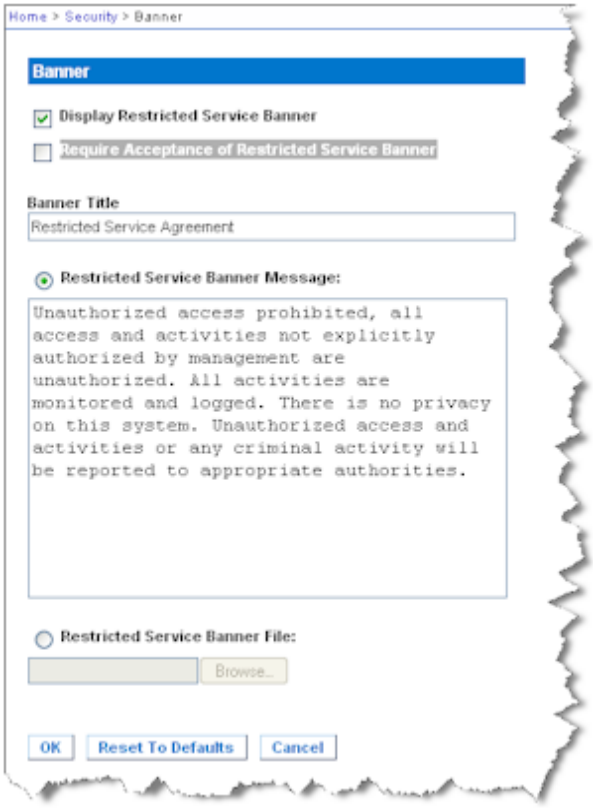
Die Überschrift und der Text der Sicherheitsmeldung kann angepasst werden, oder Sie können den Standardtext verwenden. Die Sicherheitsmeldung kann auch so konfiguriert werden, dass Benutzer die Sicherheitsvereinbarung akzeptieren müssen, bevor sie auf KX III zugreifen, oder die Sicherheitsmeldung kann einfach nach dem Anmeldevorgang angezeigt werden. Wenn die Funktion zum Akzeptieren oder Ablehnen aktiviert ist, wird die Auswahl des Benutzers im Prüfprotokoll protokolliert.

So konfigurieren Sie eine Sicherheitsmeldung:

1. Klicken Sie auf "Security" > "Banner" (Sicherheit > Meldung), um die Seite "Banner" (Meldung) zu öffnen.
2. Wählen Sie "Display Restricted Service Banner" (Meldung für eingeschränkten Dienst anzeigen) aus, um die Funktion zu aktivieren.
3. Wenn Benutzer die Meldung vor dem Anmeldeprozess bestätigen sollen, wählen Sie "Require Acceptance of Restricted Service Banner" (Akzeptieren der Meldung für eingeschränkten Dienst erforderlich) aus. Um die Meldung zu akzeptieren, müssen Benutzer ein Kontrollkästchen aktivieren. Wenn Sie diese Einstellung nicht aktivieren, wird die Sicherheitsmeldung nach der Anmeldung des Benutzers nur angezeigt. In diesem Fall ist keine Bestätigung durch den Benutzer erforderlich.
4. Ändern Sie ggf. den Namen der Meldung. Diese Informationen werden den Benutzern als Teil der Meldung angezeigt. Es können bis zu 64 Zeichen verwendet werden.
5. Bearbeiten Sie die Informationen im Textfeld "Restricted Services Banner" (Meldung zum eingeschränkten Dienst). Sie können maximal 6000 Zeichen eingeben oder eine Textdatei hochladen. Führen Sie hierfür einen der folgenden Schritte aus:
   a. Bearbeiten Sie den Text, indem Sie manuell in das Textfeld tippen. Klicken Sie auf "OK".

b. Laden Sie Informationen aus einer .txt-Datei hoch, indem Sie das Optionsfeld "Restricted Services Banner File" (Datei für Sicherheitsmeldung für eingeschränkte Dienste) auswählen und auf "Browse" (Durchsuchen) klicken, um die Datei zu suchen und hochzuladen. Klicken Sie auf "OK". Nachdem die Datei hochgeladen wurde, wird der Text aus der Datei im Textfeld "Restricted Services Banner Message" (Meldung zum eingeschränkten Dienst) angezeigt.

Hinweis: Eine Textdatei kann nicht vom lokalen Port hochgeladen werden.



Wartung

Audit Log (Prüfprotokoll)

Alle KX III-Systemereignisse werden protokolliert. Das Prüfprotokoll kann bis zu 2 K Daten speichern, bevor die ältesten Einträge überschrieben werden. Zur Vermeidung des Verlusts von Prüfprotokolldaten exportieren Sie die Daten an einen Syslog-Server oder SNMP Manager. Konfigurieren Sie den Syslog-Server oder SNMP-Manager auf der Seite "Device Settings" (Geräteeinstellungen) > "Event Management" (Ereignisverwaltung). Informationen darüber, welche Daten im Prüfprotokoll und im Syslog erfasst werden, finden Sie unter ***Im Prüfprotokoll und im Syslog erfasste Ereignisse*** (auf Seite 370).

So zeigen Sie das Prüfprotokoll für Ihre KX III-Einheit an:

1. Wählen Sie **Maintenance > Audit Log** (Wartung > Prüfprotokoll). Die Seite "Audit Log" (Prüfprotokoll) wird angezeigt.

   Die Seite "Audit Log" (Prüfprotokoll) enthält Ereignisse sortiert nach Datum und Uhrzeit, wobei die letzten Ereignisse zuerst aufgeführt werden. Das Prüfprotokoll enthält die folgenden Informationen:

   - Date (Datum) – Datum und Uhrzeit des Ereignisses, basierend auf dem 24-h-Zeitformat.
   - Event (Ereignis) – Der Ereignisname, wie er auf der Seite "Event Management" (Ereignisverwaltung) aufgeführt wird.
   - Description (Beschreibung) – Detaillierte Beschreibung des Ereignisses.

So speichern Sie das Prüfprotokoll:

Hinweis: Sie können das Prüfprotokoll nur mithilfe der KX III-Remotekonsole speichern, nicht jedoch mit der lokalen Konsole.

1. Klicken Sie auf "Save to File" (Speichern unter). Ein Dialogfeld zum Speichern der Datei wird angezeigt.
2. Wählen Sie einen Dateinamen und Speicherort aus, und klicken Sie auf "Save" (Speichern). Das Prüfprotokoll wird mit dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.

So blättern Sie durch das Prüfprotokoll:

- Verwenden Sie die Links **[Older]** ([Älter]) und **[Newer]** ([Neuer]).

Geräteinformationen

Die Seite "Device Information" (Geräteinformationen) enthält detaillierte Angaben zu Ihrem KX III Gerät und den verwendeten CIMs. Diese Informationen benötigen Sie, wenn Sie sich mit dem technischen Kundendienst von Raritan in Verbindung setzen.

So zeigen Sie Informationen zu Ihrer KX III Einheit und den CIMs an:

- Wählen Sie "Maintenance Device Information" (Wartung Geräteinformationen). Die Seite "Device Information" (Geräteinformationen) wird angezeigt.

Zu der KX III Einheit werden folgende Informationen angezeigt:

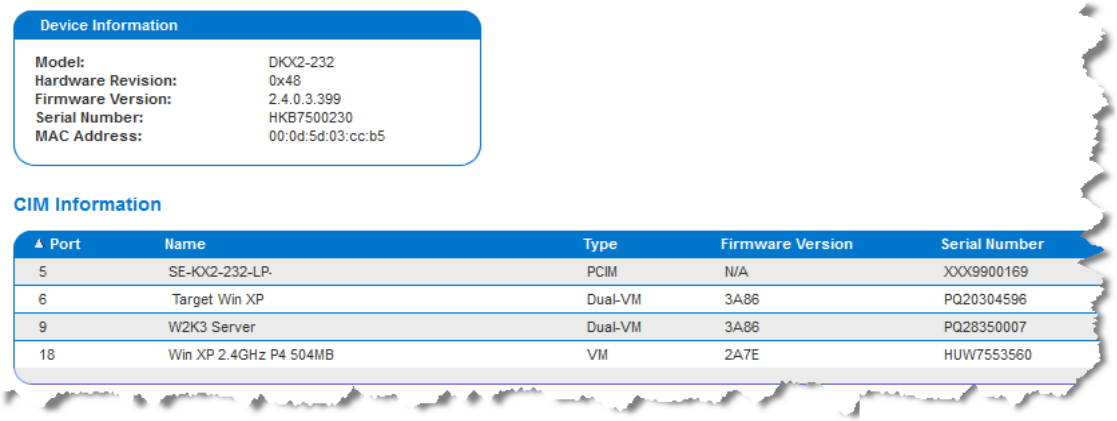
- Modell
- Hardware Revision (Hardware-Revision)
- Firmware-Version
- Seriennummer
- MAC-Adresse

Zu den verwendeten CIMs werden folgende Informationen angezeigt:

- Port (Number) [Port (Nummer)]
- Name
- Type of CIM (CIM-Typ) – DCIM, PCIM, Gestell-PDU, VM, DVM-DP, DVM-HDMI, DVM-DVI
- Firmware-Version
- "Serial Number of the CIM" (Seriennummer des CIM) – Diese Nummer wird direkt aus dem CIM abgerufen.
  - P2CIM-PS2
  - P2CIM-APS2DUAL
  - P2CIM-AUSBDUAL
  - P2CIM-AUSB
  - P2CIM-SUN
  - P2CIM-SUSB
  - P2CIM-SER
  - DCIM-PS2
  - DCIM-USB
  - DCIM-USBG2
  - DCIM-SUN
  - DCIM-SUSB

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB

Hinweis: Nur der numerische Teil der Seriennummern werden für den DCIM-USB, DCIM-PS2 und USB DCIM-G2 CIMs angezeigt. Zum Beispiel: XXX1234567 wird angezeigt. Das Seriennummer-Präfix GN ist für die CIMs, die feldkonfigurierte Seriennummern haben, angezeigt.



Backup/Restore (Sicherung/Wiederherstellung)

Auf der Seite Sicherung/Wiederherstellung können Sie die Einstellungen und die Konfiguration der KX III sichern und wiederherstellen.

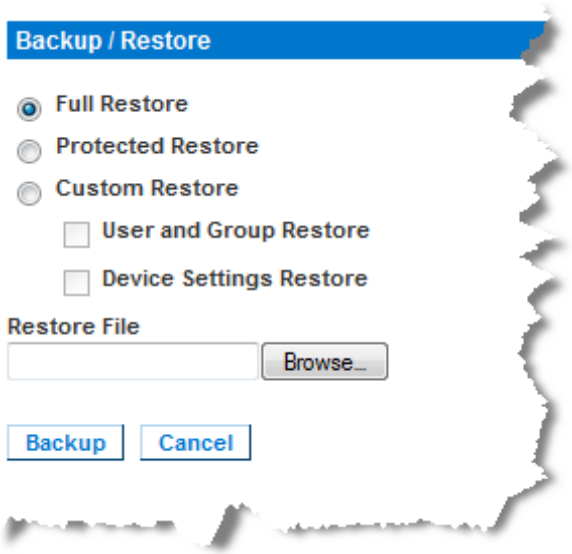
Dieses Feature dient nicht nur der Gewährleistung der Geschäftskontinuität, sondern Sie können damit auch viel Zeit sparen.

So können Sie Ihrem Team beispielsweise schnell von einem anderen KX III aus Zugriff gewähren, indem Sie die Benutzerkonfigurationseinstellungen des verwendetenKX III sichern und auf dem neuen KX III wiederherstellen.

Sie können auch eine KX III einrichten und deren Konfiguration auf mehrere andere KX III Geräte kopieren.

So greifen Sie auf die Seite „Backup/Restore“ (Sicherung/Wiederherstellung) zu:

- Wählen Sie "Maintenance > Backup/Restore" (Wartung Sicherung/Wiederherstellung). Die Seite "Backup/Restore" (Sicherung/Wiederherstellung) wird angezeigt.



Hinweis: Es wird immer das komplette System gesichert. Bei der Wiederherstellung können Sie zwischen einer vollständigen und einer teilweisen Wiederherstellung wählen.

Wenn Sie Internet Explorer 7 (oder höher) zur Sicherung Ihres KX III verwenden:

1. Klicken Sie auf "Backup" (Sichern). Das Dialogfeld "File Download" (Dateidownload) mit der Schaltfläche "Open" (Öffnen) wird angezeigt. Klicken Sie nicht auf "Open" (Öffnen).

Bei Internet Explorer 7 (oder höher) wird Internet Explorer als Standardanwendung zum Öffnen von Dateien verwendet. Sie werden aufgefordert, die Datei zu öffnen oder sie zu speichern. Um dies zu verhindern, müssen Sie eine Änderung vornehmen, sodass WordPad® als Standardanwendung zum Öffnen von Dateien verwendet wird.

2. Dies funktioniert wie folgt:
   a. Speichern Sie die Sicherungsdatei. Die Sicherungsdatei wird unter dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.
   b. Ist die Datei gespeichert, navigieren Sie zu dieser und klicken mit der rechten Maustaste darauf. Klicken Sie im dem Kontextmenü auf "Eigenschaften".
   c. Klicken Sie auf der Registerkarte "Allgemein" auf die Schaltfläche "Ändern", und wählen Sie im angezeigten Dialogfeld "WordPad" aus.

So stellen Sie Ihr KX III wieder her:

WARNUNG: Gehen Sie bei der Wiederherstellung Ihrer KX III auf eine frühere Version vorsichtig vor. Die bei der Sicherung gespeicherten Benutzernamen und Kennwörter werden wiederhergestellt. Wenn Sie sich nicht mehr an die alten Anmeldedaten für den Administrator erinnern können, wird Ihnen der Zugriff auf KX III verweigert.

Falls Sie zum Zeitpunkt der Sicherung eine andere IP-Adresse verwendet haben, wird auch diese wiederhergestellt. Wenn Sie DHCP konfiguriert haben, sollten Sie diesen Vorgang nur ausführen, wenn Sie Zugriff auf den lokalen Port haben, um nach der Aktualisierung die IP-Adresse zu prüfen.

1. Wählen Sie eine Wiederherstellungsart aus:
   - Full Restore (Vollständige Wiederherstellung) – Das gesamte System wird wiederhergestellt. Wird normalerweise für herkömmliche Sicherungs- und Wiederherstellungszwecke verwendet.
   - Protected Restore (Geschützte Wiederherstellung) – Alle Daten werden wiederhergestellt, mit Ausnahme von gerätespezifischen Informationen wie IP-Adresse, Name usw. Mit dieser Option können Sie eine KX III einrichten und deren Konfiguration auf mehrere andere KX III Geräte kopieren.
   - Custom Restore (Benutzerdefinierte Wiederherstellung) – Bei dieser Option stehen Ihnen die Kontrollkästchen "User and Group Restore" (Wiederherstellung von Benutzern und Gruppen) und "Device Settings Restore" (Wiederherstellung der Geräteeinstellungen) zur Auswahl zur Verfügung.

- User and Group Restore (Wiederherstellung von Benutzern und Gruppen) – Diese Option umfasst nur Benutzer- und Gruppeninformationen. Bei dieser Option *werden* das Zertifikat und die Dateien für den privaten Schlüssel nicht wiederhergestellt. Verwenden Sie sie, um schnell Benutzer auf einem anderen KX III einzurichten.
- Device Settings Restore (Wiederherstellung der Geräteeinstellungen) – Diese Option umfasst nur Geräteeinstellungen wie Stromzuordnungen, USB-Profile, Konfigurationsparameter hinsichtlich Blade-Chassis sowie Portgruppenzuordnungen. Verwenden Sie sie, um schnell die Geräteinformationen zu kopieren.

2. Klicken Sie auf Durchsuchen. Das Dialogfeld "Choose file" (Datei auswählen) wird angezeigt.
3. Navigieren Sie zur gewünschten Sicherungsdatei, markieren Sie sie, und klicken Sie auf "Open" (Öffnen). Die ausgewählte Datei wird im Feld "Restore File" (Datei wiederherstellen) aufgeführt.
4. Klicken Sie auf Wiederherstellen. Die Konfiguration wird basierend auf der gewählten Wiederherstellungsart wiederhergestellt.

USB Profile Management (USB-Profilverwaltung)

Auf der Seite "USB Profile Management" (USB-Profilverwaltung) können Sie benutzerdefinierte Profile hochladen, die vom technischen Kundendienst von Raritan bereitgestellt werden. Diese Profile dienen zur Erfüllung der Anforderungen Ihrer Zielserverkonfiguration, falls die verfügbaren Standardprofile diese nicht erfüllen. Der technische Kundendienst von Raritan stellt die benutzerdefinierten Profile bereit und hilft Ihnen bei der Erstellung einer Lösung für die speziellen Anforderungen Ihres Zielservers.

So öffnen Sie die Seite "USB Profile Management" (USB-Profilverwaltung):

- Wählen Sie Wartung > USB-Profilverwaltung aus. Die Seite "USB Profile Management" (USB-Profilverwaltung) wird geöffnet.

So laden Sie ein benutzerdefiniertes Profil auf Ihr KX III:

1. Klicken Sie auf Durchsuchen. Das Dialogfeld "Choose file" (Datei auswählen) wird angezeigt.
2. Navigieren Sie zur gewünschten Datei des benutzerdefinierten Profils, markieren Sie sie und klicken Sie auf "Open" (Öffnen). Die ausgewählte Datei wird im Feld "USB Profile File" (USB-Profildatei) aufgeführt.
3. Klicken Sie auf Senden. Das benutzerdefinierte Profil wird hochgeladen und in der Tabelle "Profile" (Profil) angezeigt.

Hinweis: Wenn während des Ladevorgangs eine Fehlermeldung oder Warnung angezeigt wird [z. B. "Overwriting an existing custom profile" (Ein bestehendes benutzerdefiniertes Profil wird überschrieben)], können Sie den Ladevorgang fortsetzen, indem Sie auf "Upload" (Hochladen) klicken, oder abbrechen, indem Sie auf "Cancel" (Abbrechen) klicken.

So löschen Sie ein benutzerdefiniertes Profil von Ihrem KX III:

1. Aktivieren Sie das Kontrollkästchen, das zu der Zeile der Tabelle gehört, in der das zu löschende benutzerdefinierte Profil aufgeführt ist.
2. Klicken Sie auf Löschen. Das benutzerdefinierte Profil wird gelöscht und aus der Tabelle "Profile" (Profil) entfernt.

Wie bereits erwähnt, können Sie ein benutzerdefiniertes Profil vom System löschen, auch wenn es noch als aktives Profil festgelegt ist. Dadurch werden alle bestehenden virtuellen Mediensitzungen beendet.

Handhaben von Konflikten bei Profilnamen

Ein Namenskonflikt zwischen benutzerdefinierten und Standard-USB-Profilen kann beim Durchführen einer Firmwareaktualisierung entstehen. Dies kann auftreten, wenn ein benutzerdefiniertes Profil, das erstellt und in die Liste der Standardprofile aufgenommen wurde, über den gleichen Namen verfügt wie ein neues USB-Profil, das im Rahmen der Firmwareaktualisierung heruntergeladen wird.

In diesem Fall wird das bereits bestehende benutzerdefinierte Profil mit dem Zusatz "old_" versehen. Wenn beispielsweise ein benutzerdefiniertes Profil mit dem Namen "GenericUSBProfile5" erstellt wurde und ein Profil mit dem gleichen Namen während einer Firmwareaktualisierung heruntergeladen wird, wird die bestehende Datei in "old_GenericUSBProfile5" umbenannt.

Sie können das bestehende Profil ggf. löschen. Weitere Informationen finden Sie unter ***USB Profile Management (USB-Profilverwaltung)*** (auf Seite 202).

Aktualisieren von CIMs

Gehen Sie wie unten beschrieben vor, um CIMs mithilfe der im Speicher des KX III Geräts abgelegten Firmwareversionen zu aktualisieren. Im Allgemeinen werden alle CIMs aktualisiert, wenn Sie die Gerätefirmware über die Seite Firmware Upgrade (Firmwareaktualisierung) aktualisieren.

So aktualisieren Sie CIMs mithilfe des KX III Speichers:

1. Wählen Sie "Maintenance“ "CIM Firmware Upgrade" (Wartung CIM-Firmwareaktualisierung) aus. Die Seite "CIM Firmware Upgrade" (CIM-Firmwareaktualisierung) wird geöffnet.

Sie erkennen die CIMs leicht an den Angaben in den Feldern "Port", "Name", "Type" (Typ), "Current CIM Version" (Aktuelle CIM-Version) und "Upgrade CIM Version" (Neue CIM-Version).

2. Aktivieren Sie für alle CIMs, die aktualisiert werden sollen, das Kontrollkästchen "Selected" (Ausgewählt).
3. Klicken Sie auf "Upgrade" (Aktualisieren). Sie werden aufgefordert, die Aktualisierung zu bestätigen.
4. Klicken Sie auf OK, um fortzufahren. Während des Vorgangs werden Statusleisten angezeigt. Die Aktualisierung dauert maximal zwei Minuten pro CIM.

KX III Firmware Aktualisieren

Auf der Seite "Firmware Upgrade" (Firmwareaktualisierung) können Sie die Firmware von KX III und allen damit verbundenen CIMs aktualisieren. Diese Seite ist nur in KX III Fernkonsole verfügbar.

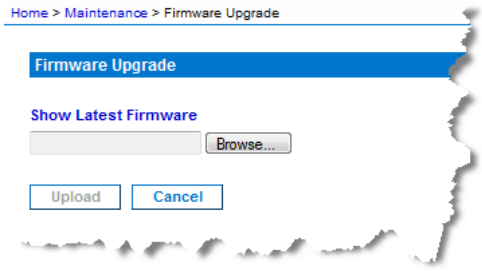
Aktualisieren der Firmware

Wichtig: Schalten Sie während der Aktualisierung die KX III Einheit nicht aus und trennen Sie nicht die Verbindung zu den CIMs, da dies zu Schäden an der Einheit bzw. den CIMs führen könnte.

So aktualisieren Sie die KX III Einheit:

1. Suchen Sie die entsprechende Raritan-Firmwaredistributionsdatei (*.RFP) auf der Seite für Firmwareaktualisierungen der ***Raritan-Website http://www.raritan.com***.
2. Entpacken Sie die Datei. Lesen Sie alle Anweisungen in den Firmware-ZIP-Dateien sorgfältig durch, bevor Sie die Aktualisierung durchführen.

   Hinweis: Kopieren Sie die Firmware-Aktualisierungsdatei vor dem Hochladen auf einen lokalen PC. Laden Sie die Datei nicht von einem Netzwerklaufwerk.
3. Wählen Sie "Maintenance Firmware Upgrade" (Wartung Firmware-Aktualisierung). Die Seite "Firmware Upgrade" (Firmwareaktualisierung) wird angezeigt.



4. Klicken Sie auf die Schaltfläche Browse (Durchsuchen), um zu dem Verzeichnis zu navigieren, in dem Sie die Aktualisierungsdatei entpackt haben.
5. Klicken Sie auf der Seite "Firmware Upgrade" (Firmware-Aktualisierung) auf "Upload" (Hochladen).

   Ihnen werden Informationen zur Aktualisierung und den Versionsnummern sowie zu den CIMs (falls Sie das entsprechende Kontrollkästchen aktiviert haben) angezeigt.

   Hinweis: Zu diesem Zeitpunkt werden verbundene Benutzer abgemeldet, und neue Anmeldeversuche werden blockiert.
6. Klicken Sie auf "Upgrade" (Aktualisieren). Warten Sie, bis der Vorgang abgeschlossen ist. Während des Vorgangs werden Statusinformationen und Fortschrittsleisten angezeigt. Nach Abschluss der Aktualisierung wird die Einheit neu gestartet (ein Tonsignal zeigt an, dass der Neustart abgeschlossen ist).
7. Schließen Sie den Browser, wenn Sie dazu aufgefordert werden, und warten Sie ungefähr fünf Minuten, bevor Sie sich erneut bei der KX III Einheit anmelden.

Upgrade History (Aktualisierungsverlauf)

KX III liefert Informationen über die Aktualisierungen, die auf KX III und den angeschlossenen CIMs durchgeführt wurden.

So zeigen Sie den Aktualisierungsverlauf an:

- Wählen Sie "Maintenance > Upgrade History" (Wartung > Aktualisierungsverlauf). Die Seite "Upgrade History" (Aktualisierungsverlauf) wird angezeigt.

Es werden Informationen zu den ausgeführten KX III-Aktualisierungen, dem Endstatus der Aktualisierung, den Start- und Abschlusszeiten sowie den vorherigen und aktuellen Firmwareversionen angezeigt. Es werden außerdem Informationen zu den CIMs bereitgestellt. Diese können angezeigt werden, indem Sie auf den Link der entsprechenden Aktualisierung klicken. Die folgenden CIM-Informationen stehen zur Verfügung:

- "Type" (Typ) – Der CIM-Typ
- "Port" (Port) – Der Port, an dem das CIM angeschlossen ist
- "User" (Benutzer) – Der Benutzer, der die Aktualisierung durchgeführt hat
- "IP" (IP) – IP-Adresse der Firmware
- "Start Time" (Startzeit) – Startzeit der Aktualisierung
- "End Time" (Abschlusszeit) – Abschlusszeit der Aktualisierung
- "Previous Version" (Vorherige Version) – Vorherige CIM-Firmwareversion
- "Upgrade Version" (Neue Version) – Aktuelle CIM-Firmwareversion
- "CIMs" (CIMs) – Aktualisierte CIMs
- "Result" (Ergebnis) – Das Ergebnis der Aktualisierung (erfolgreich oder fehlgeschlagen)

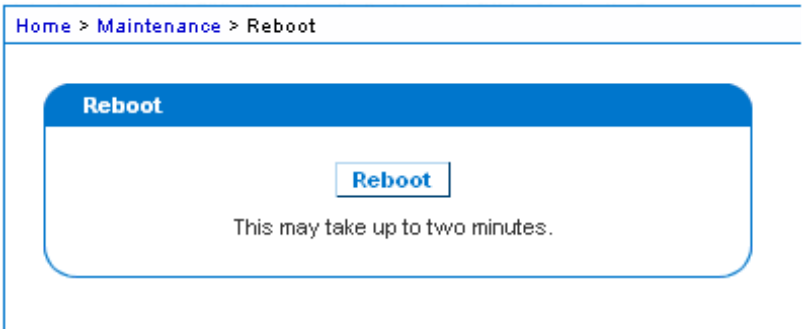
Neustart der KX III-Einheit

Auf der Seite "Reboot" (Neustart) können Sie KX III auf sichere und kontrollierte Weise neustarten. Dies ist die empfohlene Methode zum Neustarten.

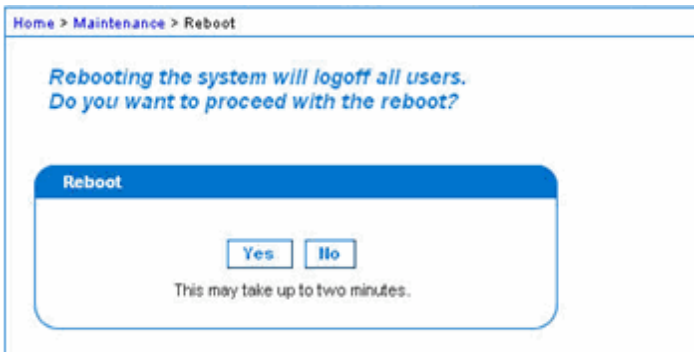
Wichtig: Alle seriellen und KVM-Verbindungen werden getrennt und alle Benutzer abgemeldet.

So starten Sie die KX III-Einheit neu:

1. Wählen Sie **Maintenance > Reboot** (Wartung > Neustart). Die Seite **Reboot** (Neustart) wird angezeigt.



2. Klicken Sie auf "Reboot" (Neustart). Sie werden aufgefordert, die Aktion zu bestätigen. Klicken Sie auf "Yes" (Ja), um fortzufahren.



Beenden der CC-SG-Verwaltung

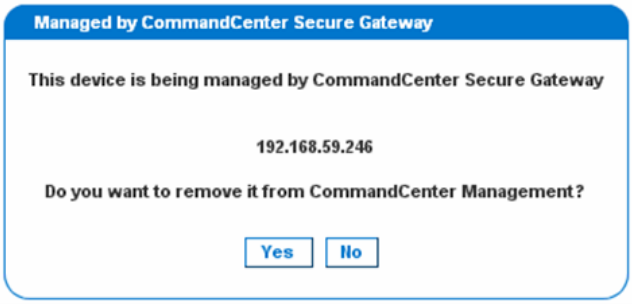
Wenn KX III von CC-SG verwaltet wird und Sie direkt auf das Gerät zugreifen möchten, erhalten Sie eine Meldung, dass das Gerät von CC-SG verwaltet wird.

Wenn Sie KX III über CC-SG verwalten und die Verbindung zwischen CC-SG und KX III nach Ablauf des festgelegten Zeitlimits (normalerweise 10 Minuten) getrennt wird, können Sie die CC-SG-Verwaltungssitzung über die KX III Konsole beenden.

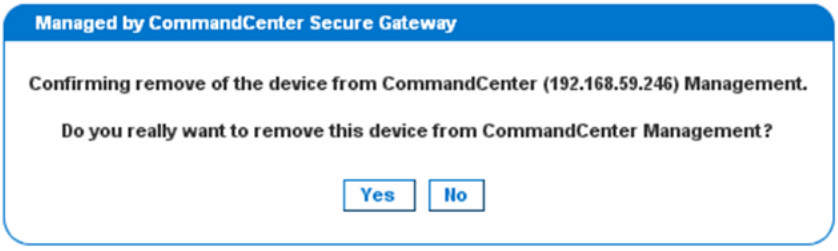
Hinweis: Sie müssen über die entsprechenden Berechtigungen zum Beenden der CC-SG-Verwaltung des KX III verfügen. Die Option "Stop CC-SG Management" (CC-SG-Verwaltung beenden) steht nur zur Verfügung, wenn Sie zurzeit CC-SG für die Verwaltung von KX III verwenden.

So beenden Sie die CC-SG-Verwaltung eines KX III Geräts:

1. Klicken Sie auf "Maintenance“ "Stop CC-SG Management" (Wartung > CC-SG-Verwaltung beenden). Eine Meldung, dass das Gerät von CC-SG verwaltet wird, wird angezeigt. Ebenso wird eine Option zum Beenden der CC-SG-Verwaltung für das Gerät angezeigt.



2. Klicken Sie auf "Yes" (Ja), um den Vorgang zum Beenden der CC-SG-Verwaltung für das Gerät zu starten. Eine Bestätigungsmeldung wird angezeigt, in der Sie aufgefordert werden, das Beenden der CC-SG-Verwaltung für das Gerät zu bestätigen.



3. Klicken Sie auf "Yes" (Ja), um die CC-SG-Verwaltung für das Gerät zu beenden. Wenn die CC-SG-Verwaltung beendet wurde, wird eine Bestätigungsmeldung angezeigt.

Diagnose

Network Interface (Netzwerkschnittstelle)

KX III liefert Informationen zum Status der Netzwerkschnittstelle.

So zeigen Sie Informationen zur Netzwerkschnittstelle an:

- Wählen Sie “Diagnostics Network Interface" (Diagnose Netzwerkschnittstelle). Die Seite "Network Interface" (Netzwerkschnittstelle) wird angezeigt.

Diese Seite enthält die folgenden Informationen:

- Funktionsfähigkeit der Ethernet-Schnittstelle
- Erreichbarkeit des Gateways
- Derzeit aktiver LAN-Port

So aktualisieren Sie diese Informationen:

- Klicken Sie auf "Refresh" (Aktualisieren).

Network Statistics (Netzwerkstatistik)

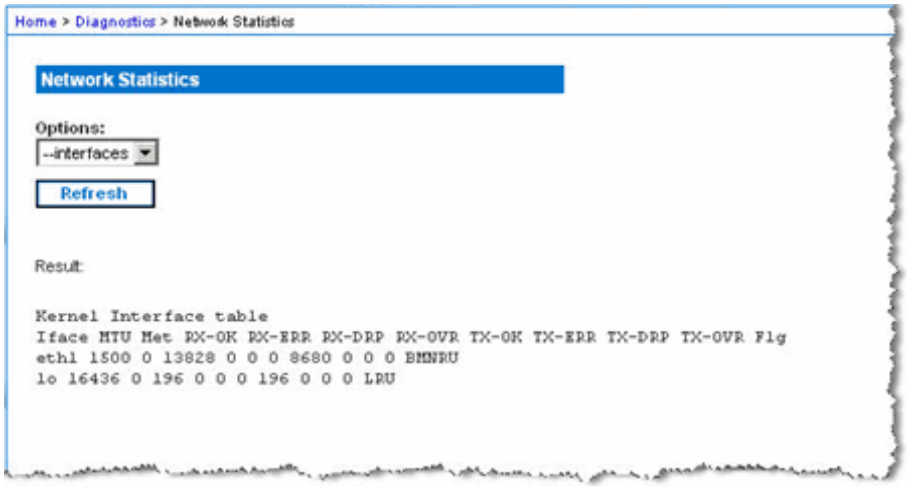
KX III liefert Statistiken über die Netzwerkschnittstelle.

So zeigen Sie Statistiken über die Netzwerkschnittstelle an:

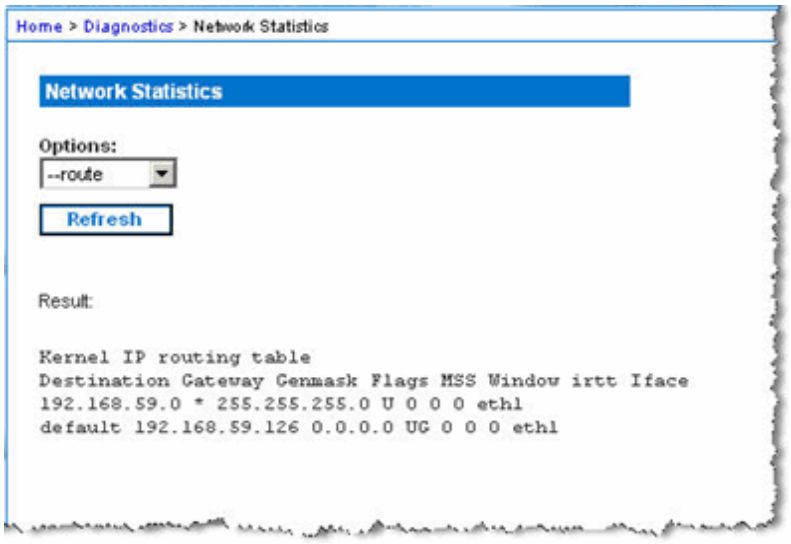
1. Wählen Sie **Diagnostics > Network Statistics** (Diagnose > Netzwerkstatistik). Die Seite **Network Statistics** (Netzwerkstatistik) wird angezeigt.
2. Wählen Sie eine Option aus der Dropdown-Liste **Options**:

- Statistics (Statistiken) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.

- Interfaces (Schnittstellen) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



- Route – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



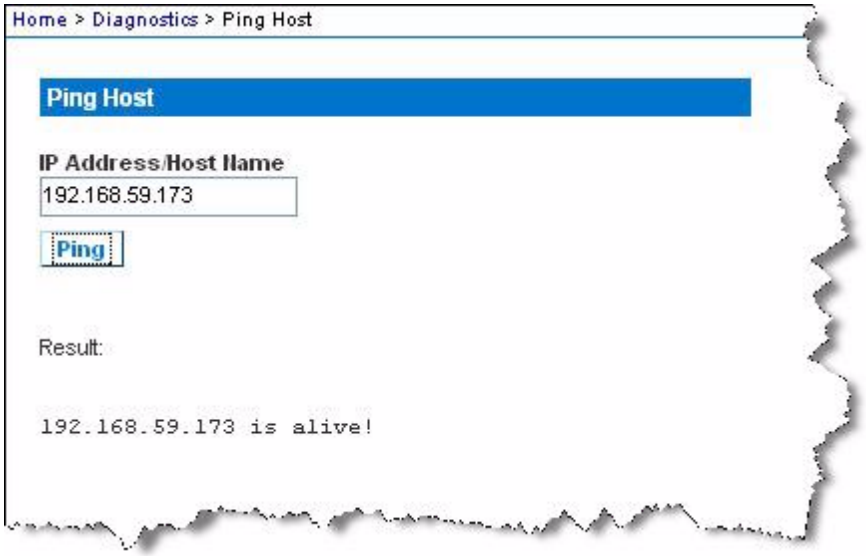
3. Klicken Sie auf "Refresh" (Aktualisieren). Die entsprechenden Informationen werden im Feld "Result" (Ergebnis) angezeigt.

Ping Host (Ping an den Host)

Ping ist ein Netzwerktool, mit dem getestet werden kann, ob ein bestimmter Host oder eine IP-Adresse über ein IP-Netzwerk erreichbar ist. Mithilfe der Seite "Ping Host" (Ping an den Host) können Sie herausfinden, ob ein Zielserver oder eine andere KX III-Einheit erreichbar ist.

So senden Sie ein Ping an den Host:

1. Wählen Sie "Diagnostics" > "Ping Host" (Diagnose > Ping an den Host) aus. Die Seite "Ping Host" (Ping an den Host) wird angezeigt.



2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

3. Klicken Sie auf "Ping". Die Ping-Ergebnisse werden im Feld "Result" (Ergebnis) angezeigt.

Seite "Trace Route to Host" (Route zum Host verfolgen)

Trace Route ist ein Netzwerk-Tool, mit dem die Route zum angegebenen Hostnamen oder zur angegebenen IP-Adresse bestimmt werden kann.

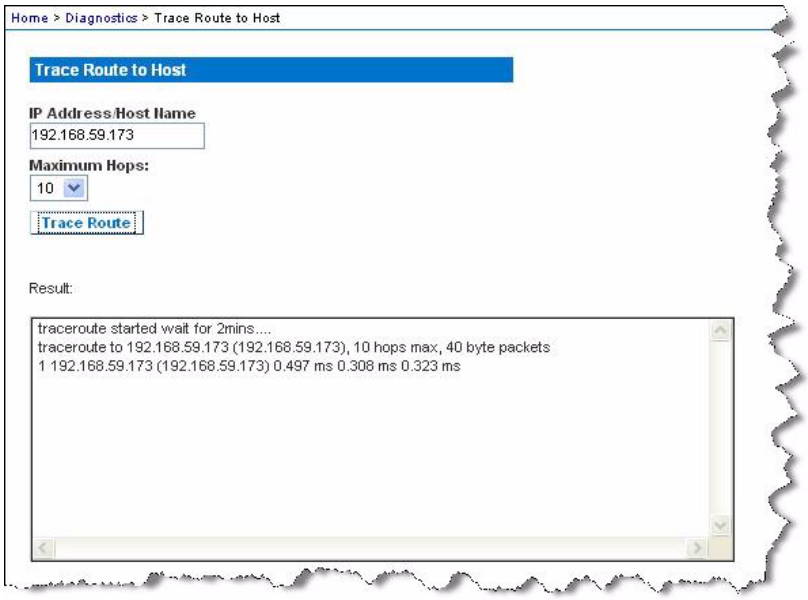
So verfolgen Sie die Route zum Host:

1. Wählen Sie "Diagnostics > Trace Route to Host" (Diagnose > Route zum Host verfolgen). Die Seite "Trace Route to Host" (Route zum Host verfolgen) wird geöffnet.

2. Geben Sie die IP-Adresse oder den Hostnamen in das Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

   Hinweis: Der Hostname darf maximal 232 Zeichen lang sein.

3. Wählen Sie die maximale Anzahl an Hops aus der Dropdown-Liste (5 bis 50 in 5er-Schritten).
4. Klicken Sie auf "Trace Route" (Route verfolgen). Der Befehl zum Verfolgen der Route wird für den angegebenen Hostnamen bzw. die angegebene IP-Adresse und die maximale Anzahl an Hops ausgeführt. Die Ausgabe der Routenverfolgung wird im Feld "Result" (Ergebnis) angezeigt.



Device Diagnostics (Gerätediagnose)

Hinweis: Diese Seite ist für die Außendienstmitarbeiter von Raritan gedacht. Verwenden Sie sie nur unter Anleitung des technischen Kundendienstes.

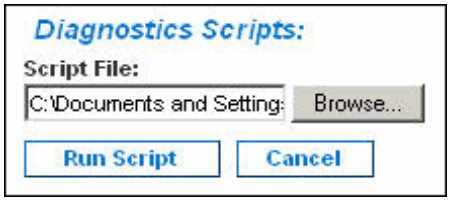
Auf der Seite "Device Diagnostics" (Gerätediagnose) werden die Diagnoseinformationen von KX III auf den Client-PC heruntergeladen. Auf dieser Seite haben Sie zwei Möglichkeiten:

- Führen Sie während einer Sitzung zum Debuggen eines schwerwiegenden Fehlers ein vom technischen Kundendienst von Raritan bereitgestelltes Spezialdiagnoseskript aus. Das Skript wird auf das Gerät hochgeladen und ausgeführt. Nachdem das Skript ausgeführt wurde, können Sie die Diagnosemeldungen mithilfe der Funktion "Save to File" (Speichern unter) herunterladen.
- Laden Sie das Protokoll der Gerätediagnose vom KX III-Gerät auf den Client herunter, um eine Übersicht der Diagnosemeldungen zu erhalten. Diese verschlüsselte Datei wird anschließend an den technischen Kundendienst von Raritan gesendet. Nur Raritan kann diese Datei interpretieren.

Hinweis: Auf diese Seite können nur Benutzer mit Administratorrechten zugreifen.

So führen Sie die KX III-Systemdiagnose aus:

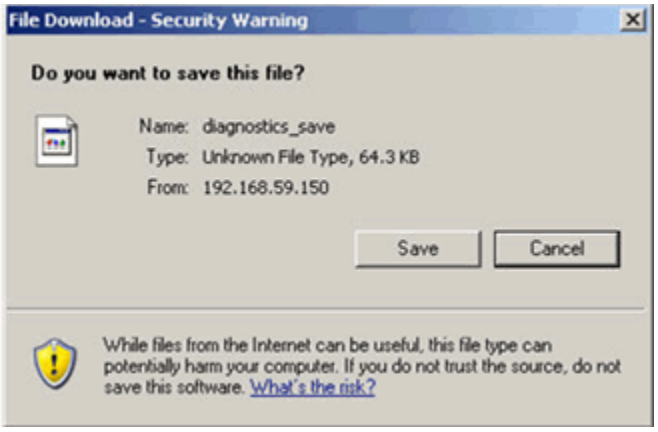
1. Wählen Sie "Diagnostics" > "KX III Diagnostics" (Diagnose > KX III-Diagnose) aus. Die KX III-Diagnoseseite wird angezeigt.
2. So führen Sie eine Diagnoseskriptdatei aus, die Sie per E-Mail vom technischen Kundendienst von Raritan erhalten haben:
   a. Rufen Sie die Diagnosedatei von Raritan ab, und entpacken Sie sie gegebenenfalls.
   b. Klicken Sie auf "Browse" (Durchsuchen). Das Dialogfeld "Choose File" (Datei auswählen) wird angezeigt.
   c. Navigieren Sie zur gewünschten Diagnosedatei, und markieren Sie sie.
   d. Klicken Sie auf "Open" (Öffnen). Die Datei wird im Feld "Script File" (Skriptdatei) angezeigt.



e. Klicken Sie auf "Run Script" (Skript ausführen). Senden Sie diese Datei an den technischen Kundendienst von Raritan.

3. So erstellen Sie eine Diagnosedatei, die Sie an den technischen Kundendienst von Raritan senden können:

   a. Klicken Sie auf "Save to File" (Speichern unter). Das Dialogfeld "File Download" (Dateidownload) wird angezeigt.



   b. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.

   c. Navigieren Sie zum gewünschten Verzeichnis, und klicken Sie auf "Save" (Speichern).

   d. Senden Sie diese Datei an die vom technischen Kundendienst von Raritan angegebene E-Mail-Adresse.

KX III Lokale Konsole

Sie können am Serverschrank über den lokalen Port auf KX III zugreifen und die Einheit verwalten. Zugriff auf KX III Funktionen werden via Lokale Konsole bereitgestellt.

Die Mehrheit der Administrator-Funktionen werden in der Regel in der KX-III-Remote-Konsole und / oder von der lokalen Konsole durchgeführt.

Dieser Bereich spezifiziert die Administrator-Aufgaben. Für Anwenderaufgaben in der lokalen Konsole, siehe Benutzer hilfe.

Sicherheit und Authentifizierung

Zur Verwendung der lokalen KX III-Konsole müssen Sie zunächst mit einem gültigen Benutzernamen und Kennwort authentifiziert werden. KX III verfügt über ein vollständig integriertes Authentifizierungs- und Sicherheitsschema, unabhängig davon, ob Sie über das Netzwerk oder den lokalen Port auf das Gerät zugreifen. In jedem Fall ermöglicht KX III den Zugriff nur auf die Server, für die ein Benutzer über eine Zugriffsberechtigung verfügt. Weitere Informationen zum Festlegen des Serverzugriffs und der Sicherheitseinstellungen finden Sie unter Benutzerverwaltung.

Wenn Ihr KX III für externe Authentifizierungsdienste (LDAP/LDAPS, RADIUS oder Active Directory) konfiguriert wurde, werden Authentifizierungsversuche in der lokalen Konsole auch durch den externen Authentifizierungsdienst authentifiziert.

Hinweis: Sie können für den lokalen Konsolenzugriff auch festlegen, dass keine Authentifizierung erfolgen soll. Diese Option wird jedoch nur für sichere Umgebungen empfohlen.

So verwenden Sie die lokale KX III-Konsole:

1. Schließen Sie an die lokalen Ports auf der Rückseite des KX III-Geräts eine Tastatur, eine Maus und eine Videoanzeige an.
2. Starten Sie KX III. Die Oberfläche der lokalen KX III-Konsole wird angezeigt.

Lokale Porteinstellungen von der lokalen KX III Konsole konfigurieren

Der lokale Standardport kann über die Remotekonsole auf der Seite "Port Configuration" (Portkonfiguration) oder über die lokale Konsole auf der Seite "Local Port Settings" (Lokale Porteinstellungen) konfiguriert werden.

Auf der Seite "Local Port Settings" (Lokale Porteinstellungen) können Sie viele Einstellungen für die lokale KX III-Konsole anpassen. Dazu zählen die Tastatur, die Zugriffstasten, die Verzögerung beim Videowechsel, der Stromsparmodus, die Auflösungseinstellungen für die lokale Benutzeroberfläche sowie die lokale Benutzerauthentifizierung.

Hinweis: Auf diese Funktionen können nur Benutzer mit Administratorrechten zugreifen.

Hinweis: Einige Einstellungsänderungen, die auf der Seite "Local Port Settings" (Lokale Porteinstellungen) vorgenommen werden, führen zum Neustart des verwendeten Browsers. Führt eine Einstellungsänderung zum Neustart des Browsers, so ist dies in den hier beschriebenen Schritten vermerkt.

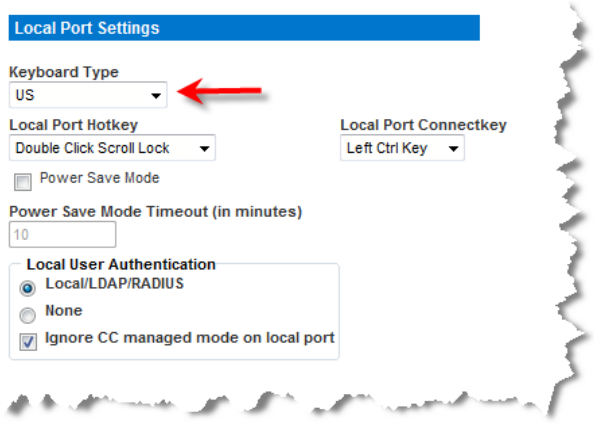
So konfigurieren Sie die lokalen Porteinstellungen:

1. Wählen Sie "Device Settings“ "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus. Die Seite "Local Port Settings" (Lokale Porteinstellungen) wird angezeigt.

Lokalen Konsol-Tastaturtyp Wählen

1. Wählen Sie aus den Optionen in der Dropdown-Liste den geeigneten Tastaturtyp aus.

   Der Browser wird neu gestartet, sobald diese Änderung vorgenommen ist.



- US
- US/International (USA/International)
- United Kingdom (Großbritannien)
- Französisch (Frankreich)
- Deutsch (Deutschland)
- Deutsch (Schweiz)
- Simplified Chinese (Vereinfachtes Chinesisch)
- Traditional Chinese (Traditionelles Chinesisch)
- Dubeolsik Hangul (Korean) (Koreanisch)
- JIS (Japanese Industry Standard) (Japanisch [Japanischer Branchenstandard])
- Portugiesisch (Portugal)
- Norwegisch (Norwegen)
- Schwedisch (Schweden)
- Dänisch (Dänemark)
- Belgian (Belgium) (Belgisch)
- Ungarisch
- Spanisch
- Italienisch
- Slowenisch

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen KX III Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

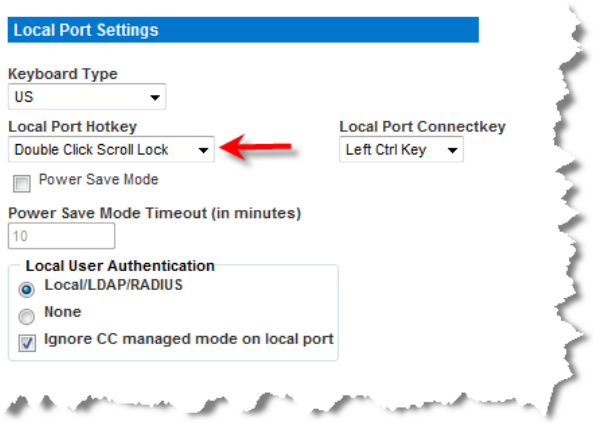
Hinweis: Bei Verwendung einer türkischen Tastatur müssen Sie die Verbindung mit einem Zielserver über den Active KVM Client (AKC) herstellen. Von anderen Raritan-Clients wird es nicht unterstützt.

Wählen Sie unter Local Port Hotkey eine Zugriffstaste für den lokalen Port aus.

1. Wählen Sie die Zugriffstaste für den lokalen Port. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen KX III-Konsole zurückkehren, wenn gerade eine Zielserveroberfläche angezeigt wird. Die Standardoption lautet "Double Click Scroll Lock" (Rollen-Taste zweimal drücken). Sie können jedoch eine andere Tastenkombination aus der Dropdownliste auswählen.

Zugriffstaste	Zu drückende Tastenkombination
Rollen-Taste zweimal drücken	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Num-Feststelltaste zweimal drücken	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.
Feststelltaste zweimal drücken	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Linke Alt-Taste zweimal	Drücken Sie die linke Alt-Taste

Zugriffstaste	Zu drückende Tastenkombination
drücken	zweimal kurz hintereinander.
Linke Umschalttaste zweimal drücken	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Linke Strg-Taste zweimal drücken	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.



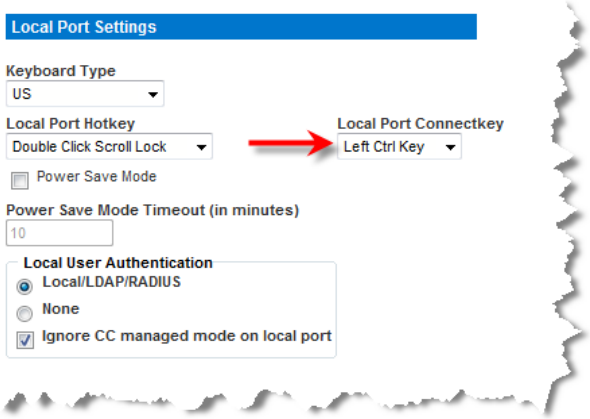
Wählen Sie die Verbindungstaste für den lokalen Port aus.

1. Wählen Sie die Verbindungstaste für den lokalen Port aus. Verwenden Sie eine Verbindungstastenfolge, um eine Verbindung mit einem Zielgerät herzustellen und zu einem anderen Zielgerät zu wechseln.

   Sie können anschließend die Zugriffstaste verwenden, um die Verbindung zum Zielgerät zu trennen und zur GUI des lokalen Ports zurückzukehren.

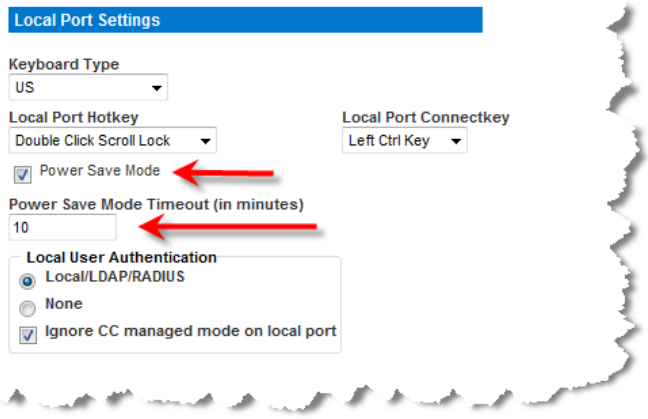
   Wenn die Verbindungstaste für den lokalen Port erstellt wurde, erscheint diese im Navigationsfenster der GUI, sodass Sie sie als Referenz verwenden können. Beispiele für Verbindungstastenfolgen finden Sie unter ***Beispiele für Verbindungstasten*** (auf Seite 310).

Die Verbindungstaste ist für Standardserver und Blade-Chassis verfügbar.



Konfigurieren der Power-Speicherungsfunktion (Optional)

1. Führen Sie die folgenden Schritte aus, falls Sie das Stromsparfeature verwenden möchten:
   a. Aktivieren Sie das Kontrollkästchen "Power Save Mode" (Stromsparmodus).
   b. Legen Sie die Zeitspanne (in Minuten) fest, nach der in den Stromsparmodus geschaltet wird.



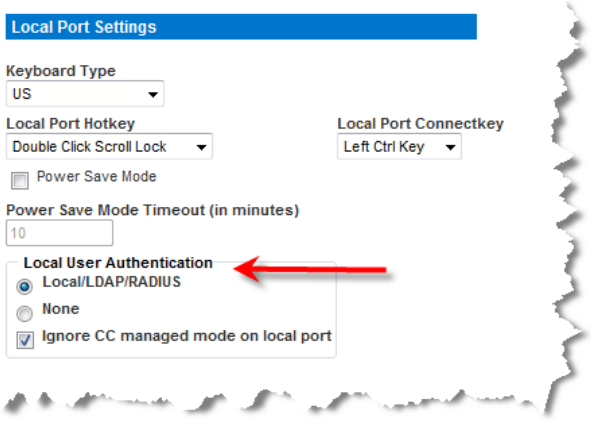
Lokale Benutzerauthentifizierung Wählen

1. Wählen Sie die Methode zur lokalen Benutzerauthentifizierung aus:
   - Local/LDAP/RADIUS (Lokal/LDAP/RADIUS): Dies ist die empfohlene Option.

     Weitere Informationen zur Authentifizierung finden Sie unter Remoteauthentifizierung.

- Keine. Der lokale Konsolenzugriff wird nicht authentifiziert.

  Diese Option ist nur für sichere Umgebungen empfehlenswert.

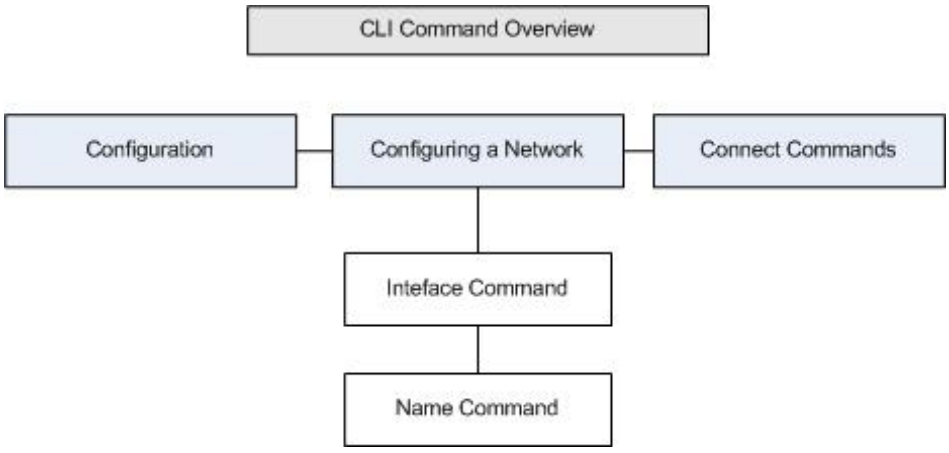


Befehlszeilenschnittstelle (CLI)

Überblick

Die Kommandozeilenschnittstelle (Command Line Interface, CLI) kann verwendet werden, um die KX III-Netzwerkschnittstelle zu konfigurieren und Diagnosefunktionen durchzuführen, vorausgesetzt, Sie verfügen über die erforderlichen Berechtigungen.

Das folgenden Abbildungen bieten eine Übersicht über die Befehle der Kommandozeilenschnittstelle. Eine Liste der Befehle, einschließlich Definitionen und Verknüpfungen zu den Abschnitten in diesem Kapitel, die Beispiele für diese Befehle enthalten, finden Sie unter ***Befehle der Kommandozeilenschnittstelle*** (siehe "***Befehle der Befehlszeilenschnittstelle***" auf Seite 227).



Die folgenden allgemeinen Befehle können auf allen Ebenen der Befehlszeilenschnittstelle der Abbildung oben verwendet werden: "top", "history", "log off", "quit", "show" und "help"

Zugriff auf KX III über die Kommandozeilenschnittstelle

Verwenden Sie eine der folgenden Methoden, um auf die KX III-Einheit zuzugreifen:

- SSH (Secure Shell) über IP-Verbindung

Verschiedene SSH-Clients stehen hier zur Verfügung:

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client von ssh.com - ***www.ssh.com http://www.ssh.com***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

SSH-Verbindung mit KX III

Verwenden Sie zur Verbindung mit KX III einen SSH-Client, der SSH V2 unterstützt. Sie müssen den SSH-Zugriff auf der Seite "Devices Services" (Gerätedienste) aktivieren.

Hinweis: Aus Sicherheitsgründen werden SSH-V1-Verbindungen von KX III nicht unterstützt.

SSH-Zugriff über einen Windows-PC

So öffnen Sie eine SSH-Sitzung über einen Windows®-PC:

1. Starten Sie die SSH-Clientsoftware.
2. Geben Sie die IP-Adresse des KX III-Servers ein. Beispielsweise 192.168.0.192.
3. Wählen Sie "SSH" aus (der standardmäßige Konfigurations-Port lautet 22).
4. Klicken Sie auf "Open" (Öffnen).

Die Eingabeaufforderung `login as:` (Anmelden als:) wird angezeigt.

Siehe ***Anmelden*** (auf Seite 223).

SSH-Zugriff über eine UNIX-/Linux-Workstation

- **Geben Sie den folgenden Befehl ein, um eine SSH-Sitzung über eine UNIX®-/Linux®-Workstation zu öffnen und sich als Admin-Benutzer anzumelden:**

```
ssh -l admin 192.168.30.222
```

Die Eingabeaufforderung für das Kennwort wird angezeigt.

Siehe ***Anmelden*** (auf Seite 223).

Anmelden

- **Geben Sie zum Anmelden den Benutzernamen „admin“ wie gezeigt ein:**

1. Melden Sie sich als `admin` an.
2. Die Eingabeaufforderung für das Kennwort wird angezeigt. Geben Sie das Standardkennwort ein: *raritan*

   Der Begrüßungsbildschirm wird angezeigt. Sie sind jetzt als Administrator angemeldet.

Wenn Sie den folgenden Abschnitt ***Navigation in der Kommandozeilenschnittstelle*** (auf Seite 223) gelesen haben, können Sie die Schritte zur Erstkonfiguration durchführen.

Navigation in der Kommandozeilenschnittstelle

Vor der Verwendung der Kommandozeilenschnittstelle sollten Sie sich mit der Navigation und Syntax in der Kommandozeilenschnittstelle vertraut machen. Es stehen Ihnen außerdem einige Tastenkombinationen zur Verfügung, mit denen die Verwendung der Kommandozeilenschnittstelle erleichtert wird.

Vervollständigen von Befehlen

Die Kommandozeilenschnittstelle unterstützt das Vervollständigen teilweise eingegebener Befehle. Drücken Sie die Tabulatortaste, wenn Sie die ersten Zeichen eines Eintrags eingegeben haben. Wenn die Zeichen mit einem Befehl eindeutig übereinstimmen, vervollständigt die Kommandozeilenschnittstelle den Eintrag.

- Wird keine Übereinstimmung gefunden, zeigt die Kommandozeilenschnittstelle die gültigen Einträge für die Ebene an.
- Wenn mehrere Übereinstimmungen gefunden werden, zeigt die Kommandozeilenschnittstelle alle gültigen Einträge an.

Geben Sie weiteren Text ein, damit eine eindeutige Übereinstimmung gefunden werden kann, und vervollständigen Sie den Eintrag mithilfe der Tabulatortaste.

Syntax der Kommandozeilenschnittstelle – Tipps und Zugriffstasten

Tipps

- Befehle werden in alphabetischer Reihenfolge aufgeführt.
- Bei Befehlen wird die Groß-/Kleinschreibung nicht beachtet.
- Parameternamen bestehen aus einem Wort ohne Unterstrich.
- Für Befehle ohne Argumente werden standardmäßig die aktuellen Einstellungen für den Befehl angezeigt.
- Wenn Sie nach dem Befehl ein Fragezeichen (?) eingeben, wird die Hilfe für diesen Befehl angezeigt.
- Ein senkrechter Strich (|) zeigt eine Auswahl im Bereich der optionalen oder erforderlichen Schlüsselwörter oder Argumente an.

Zugriffstasten

- Drücken Sie die Pfeil-nach-oben-Taste, um den letzten Eintrag anzuzeigen.
- Drücken Sie die Rücktaste, um das zuletzt eingegebene Zeichen zu löschen.
- Drücken Sie "Strg+C", um einen Befehl zu beenden oder abzubrechen, wenn Sie die falschen Parameter eingegeben haben.
- Drücken Sie die Eingabetaste, um den Befehl auszuführen.
- Drücken Sie die Tabulatortaste, um einen Befehl zu vervollständigen. Beispiel: `Admin Port > Conf.` Das System zeigt dann die Eingabeaufforderung `Admin Port > Config >` an.

Allgemeine Befehle für alle Ebenen der Kommandozeilenschnittstelle

Im Folgenden werden die Befehle aufgelistet, die auf allen Ebenen der Kommandozeilenschnittstelle verfügbar sind. Diese Befehle dienen auch zur Navigation in der Kommandozeilenschnittstelle.

Befehle	Beschreibung
top	Wechselt zur höchsten Ebene der Hierarchie der Kommandozeilenschnittstelle oder der Eingabeaufforderung "username" (Benutzername).
history	Zeigt die letzten 200 Befehle an, die der Benutzer in die Kommandozeilenschnittstelle von KX III eingegeben hat.
help	Zeigt eine Übersicht der Syntax der Kommandozeilenschnittstelle an.
quit	Der Benutzer kehrt eine Ebene zurück.
logout	Beendet die Benutzersitzung.

Erstkonfiguration über die Kommandozeilenschnittstelle

Hinweis: Diese Schritte unter Verwendung der Kommandozeilenschnittstelle sind optional, da dieselbe Konfiguration auch über KVM erfolgen kann. Weitere Informationen finden Sie unter **Erste Schritte** *(auf Seite 9).*

KX III-Geräte werden werksseitig mit Standardeinstellungen geliefert. Wenn Sie das Gerät zum ersten Mal einschalten und verbinden, müssen Sie die folgenden Grundparameter einstellen, sodass vom Netzwerk aus sicher auf das Gerät zugegriffen werden kann.

1. Kennwort des Administrators zurücksetzen. Alle KX III-Geräte verfügen zunächst über dasselbe Standardkennwort. Um Sicherheitsverletzungen zu vermeiden, müssen Sie deshalb das Administratorkennwort "raritan" in ein benutzerdefiniertes Kennwort für Administratoren, die das KX III-Gerät verwalten, ändern.
2. IP-Adresse, Subnetzmaske und Gateway-IP-Adresse für Remotezugriff zuweisen.

Einstellen von Parametern

Um Parameter einzustellen, müssen Sie sich als Administrator anmelden. Auf der höchsten Ebene wird die Eingabeaufforderung "Username" > (Benutzername) angezeigt, der bei der Erstkonfiguration "admin" lautet. Geben Sie den Befehl "top" ein, um zur höchsten Menüebene zurückzukehren.

Hinweis: Wenn Sie sich mit einem anderen Benutzernamen angemeldet haben, wird dieser anstatt "admin" angezeigt.

Einstellen von Netzwerkparametern

Netzwerkparameter werden mithilfe des Befehls "interface" konfiguriert:

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

Wenn der Befehl akzeptiert wird, trennt das Gerät automatisch die Verbindung. Sie müssen die Verbindung zum Gerät unter Verwendung der neuen IP-Adresse und des Benutzernamens und des Kennworts, die Sie im Abschnitt zum Zurücksetzen des werkseitigen Standardkennworts erstellt haben, erneut herstellen.

Wichtig: Wenn Sie das Kennwort vergessen, muss KX III über die Taste "Reset" (Zurücksetzen) auf der Rückseite von KX III auf die Werkseinstellungen zurückgesetzt werden. Die Schritte zur Erstkonfiguration müssen in diesem Fall erneut durchgeführt werden.

KX III verfügt nun über die Grundkonfiguration, und Sie können von einem Remotestandort aus (SSH oder GUI) sowie lokal mithilfe des lokalen seriellen Ports auf die Einheit zugreifen. Der Administrator muss Benutzer und Gruppen, Dienste, Sicherheit und serielle Ports, über die die seriellen Zielgeräte an KX III angeschlossen sind, konfigurieren.

Eingabeaufforderungen der Befehlszeilenschnittstelle

Die Eingabeaufforderung der Befehlszeilenschnittstelle zeigt die aktuelle Befehlsebene an. Die Stammebene der Eingabeaufforderung ist der Anmeldename. Bei einer direkten Verbindung mit dem seriellen Port "Admin" mit einem Terminalemulationsprogramm ist "Admin Port" (Admin-Port) die Stammebene eines Befehls:

```
admin >
```

Befehle der Befehlszeilenschnittstelle

- Geben Sie `admin > help` ein.

Befehl	Beschreibung
config	Wechselt zum Konfigurationsuntermenü.
diagnostics	Wechselt zum Diagnoseuntermenü.
help	Zeigt einen Überblick der Befehle an.
history	Anzeigen des Befehlszeilenverlaufs der aktuellen Sitzung.
listports	Listet die verfügbaren Ports auf.
logout	Abmelden von der aktuellen Sitzung der Befehlszeilenschnittstelle.
top	Rückkehr zum Stammmenü.
userlist	Listet aktive Benutzersitzungen auf.

- Geben Sie `admin > config > network` ein.

Befehl	Beschreibung
help	Zeigt einen Überblick der Befehle an.
history	Anzeigen des Befehlszeilenverlaufs der aktuellen Sitzung.
interface	Einstellen/Empfangen von Netzwerkparametern
ipv6_interface	Einstellen/Empfangen von IPv6-Netzwerkparametern
logout	Abmelden von der aktuellen Sitzung der Befehlszeilenschnittstelle.
name	Gerätenamenkonfiguration
quit	Kehrt zum vorherigen Menü zurück.
stop	Rückkehr zum Stammmenü.

Sicherheitsprobleme

Wichtige Elemente, die Sie bei der Sicherheit für Konsolenserver beachten sollten:

- Verschlüsselung des Datenverkehrs zwischen Bedienerkonsole und dem KX III-Gerät
- Authentifizierung und Autorisierung von Benutzern
- Sicherheitsprofil

KX III unterstützt diese drei Elemente. Sie müssen jedoch vor dem Gebrauch konfiguriert werden.

Verwalten der Befehle für die Konsolenserverkonfiguration von KX III

Hinweis: Die Befehle der Kommandozeilenschnittstelle bleiben für SSH- und lokale Portzugriffssitzungen gleich.

Auf den Netzwerkbefehl kann über das Menü "Configuration" (Konfiguration) des KX III zugegriffen werden.

Konfigurieren des Netzwerks

Die Netzwerkmenübefehle werden verwendet, um den KX III-Netzwerkadapter zu konfigurieren.

Befehle	Beschreibung
interface	Konfiguriert die Netzwerkschnittstelle des KX III-Geräts.
name	Netzwerknamenkonfiguration
ipv6	Einstellen/Empfangen von IPv6-Netzwerkparametern

Befehl "interface"

Der Befehl "interface" wird zur Konfiguration der Netzwerkschnittstelle des KX III verwendet. Verwenden Sie folgende Syntax für den Befehl "interface":

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Einstellen/Empfangen von Ethernet-Parametern

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Beispiel für den Befehl "interface"

Der folgende Befehl aktiviert die Schnittstelle Nr. 1, legt die IP-Adresse, Maske und Gateway-Adressen sowie den Modus auf automatische Erkennung fest.

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

Befehl "name"

Der Befehl "name" wird zur Konfiguration des Netzwerknamens verwendet. Verwenden Sie folgende Syntax für den Namen:

```
name [devicename <devicename>] [hostname <hostname>]
```

Gerätenamenkonfiguration

```
devicename <devicename>   Device Name

hostname   <hostname>     Preferred host name (DHCP
only)
```

Beispiel für den Befehl "name"

Folgender Befehl legt den Netzwerknamen fest:

```
Admin > Config > Network > name devicename My-KSX2
```

Befehl "IPv6"

Verwenden Sie den Befehl "IPv6", um die IPv6-Netzwerkparameter festzulegen und bestehende IPv6-Parameter abzurufen.

```
Ipv6_interface mode enable ipauto none ip
2001:db8:290c:1291::17 prefixlen 128 gw
2001:db8:290c:1291::1
```

Duale Videoportgruppen

Für Server mit dualen Videokarten ist der Remote-Zugriff mit einer erweiterten Desktopkonfiguration möglich, die für Remote-Benutzer zur Verfügung steht. Hierfür müssen duale Videoportgruppen erstellt werden.

Erweiterte Desktopkonfigurationen ermöglichen Ihnen, das Desktop des Zielservers auf zwei Monitoren und nicht nur auf einem Monitor anzuzeigen.

Sobald Sie eine duale Videoportgruppe ausgewählt haben, werden alle Portkanäle in dieser Gruppe gleichzeitig geöffnet.

Siehe **Erstellen dualer Videoportgruppen.** (siehe "**Erstellen dualer Videoportgruppen**" auf Seite 173)

In diesem Abschnitt finden Sie wichtige Informationen bezüglich dualer Videoportgruppen.

Hinweis: Duale Videoportgruppen werden von Modellen mit nur einem KVM-Kanal, wie z. B. KX2-108 und KX2-116, nicht unterstützt.

Empfehlungen für duale Portvideofunktion

Legen Sie für die primäre und sekundäre Anzeige des Zielservers dieselbe Videoauflösung fest, um die Maussynchronisierung beizubehalten und das regelmäßige erneute Synchronisieren zu minimieren.

Abhängig von der gewünschten Ausrichtung muss die obere Anzeige (vertikale Ausrichtung) oder die linke Anzeige (horizontale Ausrichtung) als primäre Anzeige festgelegt werden. Diese Anzeige enthält die aktive Menüauswahl für virtuelle Medien-, Audio-, Smart Card- und Mausvorgänge.

Um eine intuitive Mausbewegung und -steuerung zu erhalten, müssen die folgenden Elemente dieselbe Anzeigeausrichtung aufweisen:

- Primäre und sekundäre Displays von Client PC
- Duale Videoportgruppen-Konfiguration von KX II/KX III
- Primäre und sekundäre Displays von Zielserver

Nur die folgenden Client-Starteinstellungen werden für duale Portvideoanzeigen verwendet:

- Wählen Sie die Standardanzeige oder den Vollbild-Fenstermodus beim Starten des KVM-Clients.
- Aktivieren der Videoskalierung
- Aktivieren der Menüsymbolleiste für das Anheften im Vollbildmodus

Der Ein-Cursor-Modus wird nicht empfohlen, wenn Sie duale Videoports im Vollbildmodus auf einem Client-Monitor anzeigen. Hierfür benötigen Sie den vorhandenen Ein-Cursor-Modus, um die andere Ansicht zu öffnen und anzuzeigen.

Duale Videoportgruppen Unterstützte Mausmodi

Betriebssysteme auf dem Zielgerät	Unterstützte Mausmodi	Anmerkungen
Alle Windows® Betriebssysteme	Mausmodi "Intelligent", "Standard" und "Single Mouse" (Ein Cursor)	Wenn der Modus "Stretch" (Strecken) von der Videokarte des Zielservers unterstützt wird, wird der Mausmodus "Absolute" (Absolut) ordnungsgemäß ausgeführt. Beim Modus "Stretch" (Strecken) verwaltet der Zielserver die duale Anzeige als eine zusammenhängende virtuelle Anzeige. Beim Modus "Extended" (Erweitert) dagegen behandelt

Betriebssysteme auf dem Zielgerät	Unterstützte Mausmodi	Anmerkungen
		der Zielserver die Anzeigen als zwei unabhängige Anzeigen. Für den Modus "Extended" (Erweitert) wird der intelligente Mausmodus empfohlen.
Linux®	Mausmodi "Intelligent" und "Standard"	Bei Linux® können im Ein-Cursor-Modus Anzeige- und Mausbewegungsprobleme auftreten. Raritan empfiehlt Linux-Benutzern, den Ein-Cursor-Modus nicht zu verwenden.
Mac ® Betriebssystem	Ein-Cursor-Modus	Für Mac-Ziele mit mehreren Monitoren, verwenden Sie eine Standard-Maus im Einzel-Cursor-Modus.

CIMs, die für die Unterstützung der dualen Videofunktion erforderlich sind

Die folgenden digitalen CIMs unterstützten die duale Videoportfunktion:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

Wichtige Informationen zu den digitalen CIMs finden Sie unter Zeitabstimmung und Videoauflösung für digitales CIM des Zielservers. Siehe Supported Computer Interface Module (CIMs) Specifications for CIM specifications.

Wenn das ursprüngliche CIM, das mit einem primären oder sekundären Videoport verbunden ist, getrennt und mit einem anderen CIM ersetzt wird, wird der Port aus der Dual Port-Videogruppe entfernt. Fügen Sie gegebenenfalls den Port erneut zur Gruppe hinzu.

Hinweis: Das verwendete CIM hängt von den Anforderungen dies Zielservers ab.

Hinweise zur Verwendbarkeit der dualen Videoportgruppe

Die Verwendung der dualen Videoporgruppe wirkt sich auf die folgenden Funktionen aus:

- Client-Starteinstellungen, die mithilfe von "Tools Options Client Launch Settings" (Extras > Optionen > Client-Starteinstellungen) in Virtual KVM Client (VKC) und Active KVM Client (AKC) Clients wie folgt für duale Videoportgruppen konfiguriert werden:
  - Die Einstellungen des Fenstermodus werden verwendet.
  - Die Monitoreinstellungen werden NICHT verwendet. Stattdessen wird die in der Anzeigeausrichtung konfigurierte Portgruppenverwaltung verwendet.
  - Die Einstellung "Other - Enable Single Mouse Cursor" (Sonstiges – Ein-Cursor-Modus aktivieren) wird NICHT verwendet.
  - Die Einstellung "Other - Enable Scale Video" (Sonstiges – "Video skalieren" aktivieren) wird verwendet.
  - Die Einstellung "Other - Pin Menu Toolbar" (Sonstiges – Menüsymbolleiste anheften) wird verwendet.
- Für das Ziehen und Verschieben von Elementen zwischen den Fenstern der primären und sekundären Zielgeräte müssen Sie die Maustaste drücken und loslassen, während das Element von einem Fenster in das andere verschoben wird.
- Wenn auf Linux® und Mac®-Zielservern die Feststelltaste, Rollen-Taste und Num-Feststelltaste aktiviert ist, wird die Anzeige für die Feststelltaste in der Statusleiste des primären Portfensters angezeigt, jedoch möglicherweise nicht in der Statusleiste des sekundären Portfensters.

Berechtigungen und Zugriff auf duale Videoportgruppen

Idealersweise sollten die Berechtigungen für alle Ports in der Portgruppe identisch sein. Andernfalls werden die Berechtigungen des Ports mit den meisten Einschränkungen für die Portgruppe verwendet.

Wenn z. B. "VM Access Deny" (VM-Zugriff ablehnen) für einen Port und "VM Access Read-Write" (VM-Zugriff Lesen/Schreiben) für einen anderen Port verwendet wird, wird "VM Access Deny" (VM-Zugriff ablehnen) für die Portgruppe verwendet.

Wenn ein Benutzer nicht über die entsprechenden Berechtigungen für den Zugriff auf einen Port in einer dualen Videoportgruppe verfügt, wird nur der Port angezeigt, für den der Benutzer Zugriffsberechtigungen hat. Wenn ein Benutzer keine Zugriffsberechtigungen für beide Ports hat, wird der Zugriff verweigert.

Wenn der Benutzer versucht, auf den Port zuzugreifen, wird eine Meldung mit dem Hinweis angezeigt, dass der Port entweder nicht verfügbar ist oder der Benutzer nicht über die erforderlichen Zugriffsberechtigungen verfügt.

Beispielkonfiguration einer dualen Videoportgruppe

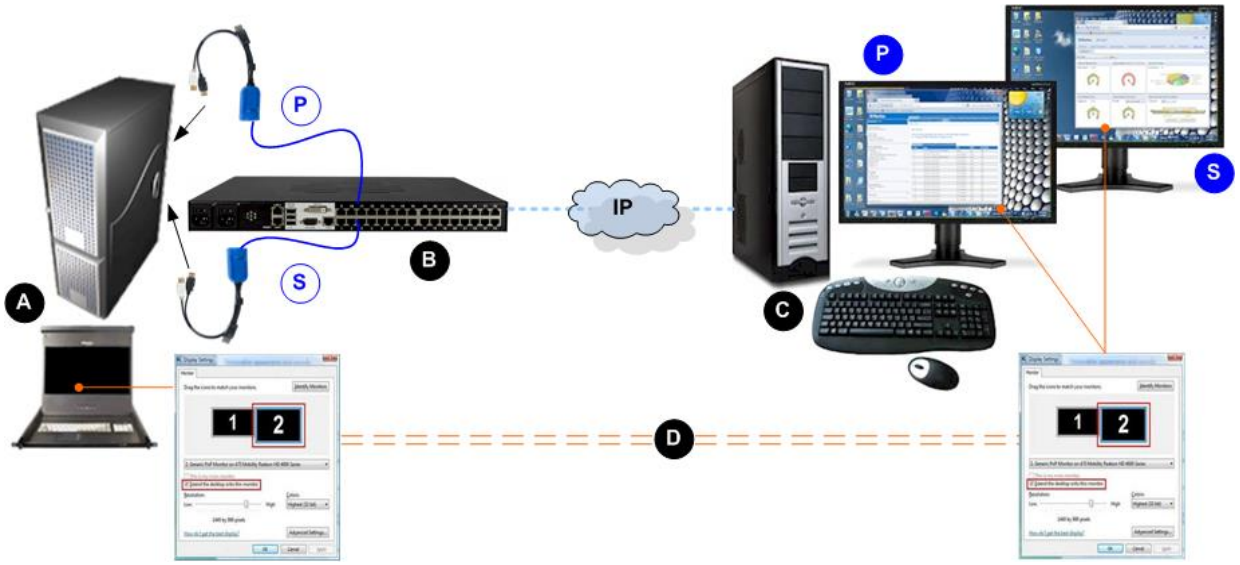
Folgendes ist ein allgemeines Beispiel.

Ihre Konfiguration kann hinsichtlich folgender Elemente abweichen: verwendeter CIM-Typ, Port, der als primärer Port verwendet wird, Ports, zu denen Sie eine Verbindung herstellen usw.

In diesem Beispiel wird Folgendes verwendet:

- ein Zielserver mit zwei Videoports
- Videoport 1 des Zielservers als primärer Port und Videoport 2 des Zielservers als sekundärer Port
- Ein KX3-832-Gerät
- ein D2CIM-DVUSB-DP CIM
- Ein Zielserver und Remoteclient mit dem Betriebssystem Microsoft® Windows 7®
- Mausmodus "Intelligent"

Eine erweiterte Desktopansicht auf dem Zielserver und Remoteclient; deshalb wird KX III so konfiguriert, dass die Anzeigeausrichtung "Horizontal - Primary (Left), Secondary (Right)" (Horizontal - Primär \[Links], Sekundäre \[Rechts]) unterstützt wird.



Diagrammschlüssel	
A	Remote Client - Konfigurieren Sie die Duale Videoportgruppe und Display-Einstellungen
B	KX III

Diagrammschlüssel	
P	Verbindung vom ersten Videoport des Zielgeräts zu KX III
S	Verbindung vom zweiten Videoport des Zielgeräts zu KX III
IP-Verbindung zwischen KX III und Remoteclient	
C	Zielserver - Konfigurieren Sie die Dualen Videoportgruppe-Einstellungen
D	Anzeigeeinstellungen sind das gleiche auf dem Remoteclient and Zielserver (Empfohlen)
P	Anzeige des primären Ports (auf der Seite "Port Group Management" \[Portgruppenverwaltung] in KX III definiert)
S	Anzeige des sekundären Ports (auf der Seite "Port Group Management" \[Portgruppenverwaltung] in KX III definiert)

Duale Portvideokonfigurations-Schritte

Schritt 1: Konfigurieren der Anzeige des Zielservers

Die Ausrichtung, die auf dem Gerät für das Ziel konfiguriert wurde, muss mit der tatsächlichen Konfiguration des Betriebssystems auf dem Zielgerät übereinstimmen.

Es wird empfohlen, dass der Verbindungsclient dieselbe Bildschirmausrichtung aufweist.

Informationen zu den Anzeigeausrichtungen und Mausmodi finden Sie unter Anzeigeausrichtung, allgemeine Ausrichtung und Mausmodi der dualen Videoportgruppe

Hinweis: Informationen zu den Schritten und zur Konfiguration der Anzeigeeinstellungen finden Sie in der Benutzerdokumentation Ihres Zielservers oder Betriebssystems.

So konfigurieren Sie die Anzeige- und Mauseinstellungen des Zielservers:

1. Konfigurieren Sie auf dem Zielserver die Anzeigeausrichtung für jeden Videoport so, dass sie mit der Anzeigeausrichtung auf dem Remoteclient übereinstimmt.

   Wenn Sie z. B. die Ausrichtung des erweiterten Desktops von links nach rechts über zwei Monitore auf dem Remoteclient verwenden, legen Sie für die Anzeigeausrichtung auf dem Zielserver dieselben Einstellungen fest.

2. Stellen Sie sicher, dass die Grafikeinstellungen Ihres Zielservers bereits so konfiguriert sind, dass eine unterstützte Auflösung und Aktualisierungsfrequenz eingestellt sind. Siehe ***Unterstützte Bildauflösung der Zielserver*** (siehe "***KX III Unterstützte Bildauflösung der Zielserver***" auf Seite 347, ***http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#32872***)

Hinweis: Wenn die primären und sekundären Zielanzeigen auf unterschiedliche Auflösungen festgelegt sind, bleibt die Maus nicht synchronisiert und muss regelmäßig über das Zielfenster oben links neu synchronisiert werden.

Schritt 2: Anschließen des Zielservers an KX III

Duale Videoportgruppen können mit vorhandenen Portverbindungen oder neuen Portverbindungen erstellt werden.

Für die folgenden Schritte werden neue Verbindungen erstellt.

Informationen zum Erstellen einer dualen Videoportgruppe mit vorhandenen Verbindungen finden Sie unter Schritt 4: Erstellen dualer Videoportgruppen.

So schließen Sie die Geräte an:

1. Installieren und schalten Sie den Zielserver gemäß den Herstelleranweisungen ein, falls Sie dies noch nicht getan haben.
2. Schließen Sie den Videoanschluss jedes CIM an die Videoausgangsports des Zielgeräts an und schließen Sie die USB-Kabel an die freien USB-Ports auf dem Zielgerät an.
3. Schließen Sie jedes CIM mithilfe eines Kabels der Kat. 5/6 an KX III an.
4. Falls dies noch nicht geschehen ist:
   a. Schließen Sie KX III an eine Netzsteckdose mit dem Netzkabel an.
   b. Verbinden mit dem KX III Netzwerk-Port und Lokaler Port (bei Bedarf)
   c. Konfigurieren von KX III. Informationen zur Verwendung des KX III finden Sie unter ***Erste Schritte*** (auf Seite 9).
5. Einen unterstützten Webbrowser starten.
6. Geben Sie ein:
   - Die URL - *http://IP-ADDRESS* um den virtuellen, Java-basierten KVM Client zu verwenden

     Oder

   - *http://IP-ADDRESS/akc* für den Microsoft .Net-basierten Aktiv KVM Client

Die *IP-ADRESSE* ist die Ihrem KX III zugewiesene IP-Adresse ist.

Sie können auch HTTPS, oder den DNS-Namen von KX III verwenden, der von Ihrem Administrator zugewiesen wurde (falls zutreffend).

Sie werden immer auf die IP-Adresse von HTTP auf HTTPS umgeleitet.

7. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, dann klicken Sie auf Einloggen.
8. Benutzervereinbarung annehmen (wenn zutreffend).
9. Wenn die Sicherheitswarnung erscheint, annehmen und/oder Zugang erlauben.

Schritt 3: Konfigurieren des Mausmodus und der Ports

Nachdem Sie den Zielserver über die Videoports des Zielservers an KX III angeschlossen haben, erkennt er die Verbindung und zeigt die Ports auf der Seite "Port Configuration" (Portkonfiguration) an.

Siehe, **Anweisungen hierzu finden Sie unter Konfigurieren von Standardzielservern**

Nachdem die Ports konfiguriert sind, können Sie in einer dualen Videoportgruppe gruppiert werden.

Hinweis: Vorhandene Ports müssen nicht konfiguriert werden, wenn diese bereits konfiguriert sind. Siehe ***Erstellen dualer Videoportgruppen*** *(auf Seite 173)*

Konfigurieren Sie den Mausmodus des Zielservers, nachdem Sie das Ziel angeschlossen haben. Siehe, **Duale Videoportgruppen unterstützte Mausmodi** (auf Seite 231)

Schritt 4: Erstellen dualer Videoportgruppen

Siehe ***Erstellen dualer Videoportgruppen.*** (siehe "***Erstellen dualer Videoportgruppen***" auf Seite 173)

Schritt 5: Starten einer dualen Videoportgruppe

Nachdem Sie die duale Videoportgruppe erstellt haben, wird sie auf der Seite "Port Access" (Portzugriff) angezeigt.

Zwei KVM-Kanäle sind erforderlich, um remote durch Klicken auf den primären Port eine Verbindung zur Dual Video-Portgruppe herzustellen. Sollten keine zwei Kanäle verfügbar sein, wird der Verbindungslink nicht angezeigt.

Zeitüberschreitungen bei Sitzungen, die auf KX III konfiguriert werden, werden für beide Ports einer dualen Videogruppe übernommen.

So starten Sie eine duale Videoportgruppe:

- Klicken Sie auf der Seite "Port Access" (Portzugriff) auf den Namen des primären Ports, und klicken Sie anschließend auf "Connect" (Verbinden).

Beide Verbindungen werden gleichzeitig gestartet und in zwei verschiedenen Fenstern angezeigt.

Wenn die Fenster angezeigt werden, können Sie sie basierend auf Ihren Anzeigeeinstellungen verschieben. Wenn Sie z. B. den erweiterten Desktopmodus verwenden, können die Portfenster zwischen den Monitoren verschoben werden.

Raritan-Client-Navigation bei der Verwendung von dualen Videoportgruppen

Wenn Sie auf den Clients den Vollbildmodus verwenden, können Sie wie folgt zwischen den Ports umschalten:

- VKC
  - Drücken Sie die Alt- + Tab-Taste.
  - Drücken Sie bei Mac®-Clients die F3-Taste und wählen Sie anschließend die Portanzeige aus.

- AKC
  - Klicken Sie mit der Maus außerhalb des Anzeigefensters, und drücken Sie anschließend die Alt- + Tab-Taste.

Direkter Portzugriff und duale Videoportgruppen

Der direkte Portzugriff ermöglicht es Benutzern, die Verwendung der Seite "Login dialog and Port Access" (Anmeldedialog und Port-Zugriff) zu umgehen.

Diese Funktion bietet auch die Möglichkeit, Benutzername und Kennwort direkt einzugeben und das Ziel aufzurufen, wenn Benutzername und Kennwort nicht in der URL enthalten sind.

Wenn Sie auf ein Ziel zugreifen, das zu einer dualen Videoportgruppe gehört, wird für den direkten Portzugriff der primäre Port verwendet, um den primären und sekundären Port zu starten.

Direkte Portverbindungen zum sekundären Port werden verweigert, und die standardmäßigen Berechtigungsregeln werden angewendet.

Weitere Informationen zur dualen Videoportgruppe finden Sie unter **Erstellen dualer Videoportgruppen.** (siehe "**Erstellen dualer Videoportgruppen**" auf Seite 173).

Weitere Informationen finden Sie unter **Aktivieren des direkten Port-Zugriffs über URL**.

Auf der Seite "Ports" angezeigte duale Videoportgruppen

Hinweis: Der primäre duale Videoport wird beim Erstellen der Portgruppe definiert.

Hinweis: Zwei KVM-Kanäle sind erforderlich, um remote durch Klicken auf den primären Port eine Verbindung zur Dual Video-Portgruppe herzustellen. Sollten keine zwei Kanäle verfügbar sein, wird der Verbindungslink nicht angezeigt.

Bei Dual Video-Portgruppen ist der primäre Port in einer Portprüfung enthalten, der sekundäre Port ist jedoch nicht enthalten, wenn eine Verbindung über einen Remote-Client hergestellt wird. Beide Ports können über den lokalen Port in die Prüfung aufgenommen werden.

Weitere Informationen zu den auf der Seite "Ports" angezeigten Elementen finden Sie unter Seite Port Access (Portzugriff) (Anzeige der Remotekonsole), und Informationen zum Ausführen von Scans finden Sie unter Scannen von Ports.

Aktualisieren des LDAP-Schemas

Zurückgeben von Benutzergruppeninformationen

Verwenden Sie die Informationen in diesem Abschnitt, um Benutzergruppeninformationen zurückzugeben (und die Autorisierung zu unterstützen), sobald die Authentifizierung erfolgreich war.

Von LDAP/LDAPS

Wenn eine LDAP/LDAPS-Authentifizierung erfolgreich ist, bestimmt KX III die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers. Ihr Remote-LDAP-Server kann diese Benutzergruppennamen bereitstellen, indem er ein wie folgt benanntes Attribut zurückgibt:

rciusergroup attribute type: string

Dies erfordert ggf. eine Schemaerweiterung auf Ihrem LDAP/LDAPS-Server. Bitten Sie den Administrator des Authentifizierungsservers, dieses Attribut zu aktivieren.

Darüber hinaus wird für Microsoft® Active Directory® das Standard-LDAP-Attribut "memberOf" verwendet.

Von Microsoft Active Directory

Hinweis: Diese Aktualisierung sollte nur von einem erfahrenen Active Directory-Administrator durchgeführt werden.

Die Rückgabe von Benutzergruppeninformationen von Microsoft® Active Directory für Windows 2000®-Server erfordert die Aktualisierung des LDAP-/LDAPS-Schemas. Weitere Informationen finden Sie in Ihrer Microsoft-Dokumentation.

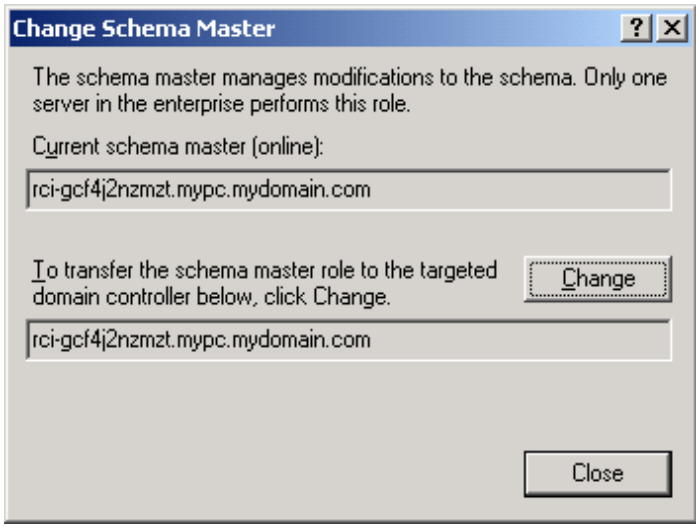
1. Installieren Sie das Schema-Plug-in für Active Directory. Entsprechende Anweisungen finden Sie in der Dokumentation für Microsoft Active Directory.
2. Starten Sie Active Directory Console und wählen Sie "Active Directory Schema" (Active Directory-Schema) aus.

Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen

Um einem Domänencontroller das Schreiben im Schema zu erlauben, müssen Sie einen Registrierungseintrag erstellen, der Schemaaktualisierungen zulässt.

So lassen Sie Schreibvorgänge im Schema zu:

1. Klicken Sie mit der rechten Maustaste auf den Stammknoten des Active Directory® Schema im linken Fensterbereich, und wählen Sie "Operations Master" (Betriebsmaster) aus dem Kontextmenü aus. Das Dialogfeld **Change Schema Master** (Schemamaster ändern) wird angezeigt.



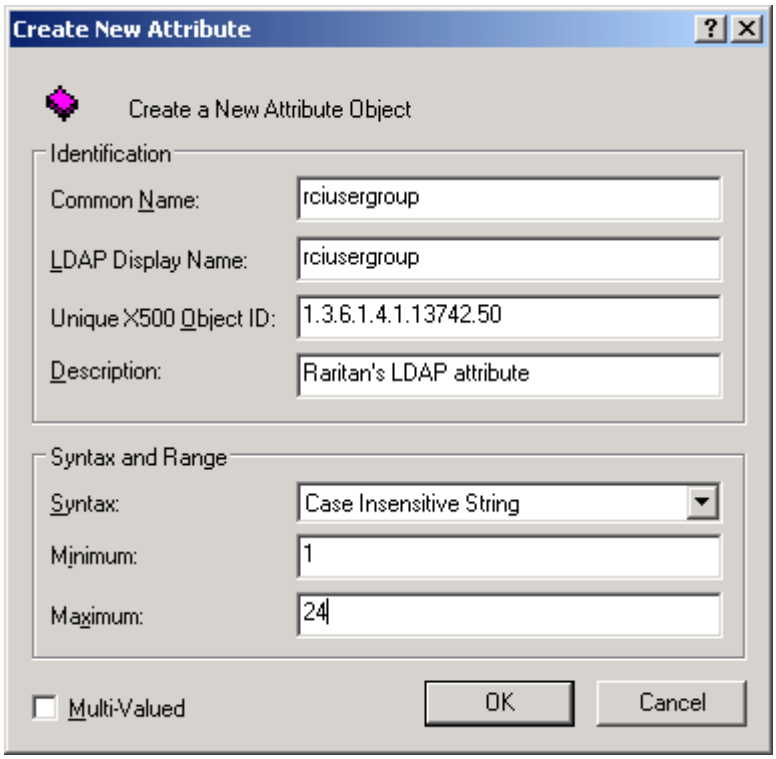
2. Aktivieren Sie das Kontrollkästchen "Schema can be modified on this Domain Controller" (Schema kann auf diesem Domänencontroller geändert werden). ***///Optional***
3. Klicken Sie auf "OK".

Erstellen eines neuen Attributs

So erstellen Sie neue Attribute für die Klasse "rciusergroup":

1. Klicken Sie im linken Fensterabschnitt auf das +-Symbol vor Active Directory® Schema.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Attributes" (Attribute).

3. Klicken Sie auf "New" (Neu) und wählen Sie "Attribute" (Attribut) aus. Klicken Sie im angezeigten Hinweisfenster auf "Continue" (Weiter). Das Dialogfeld "Create New Attribute" (Neues Attribut erstellen) wird geöffnet.

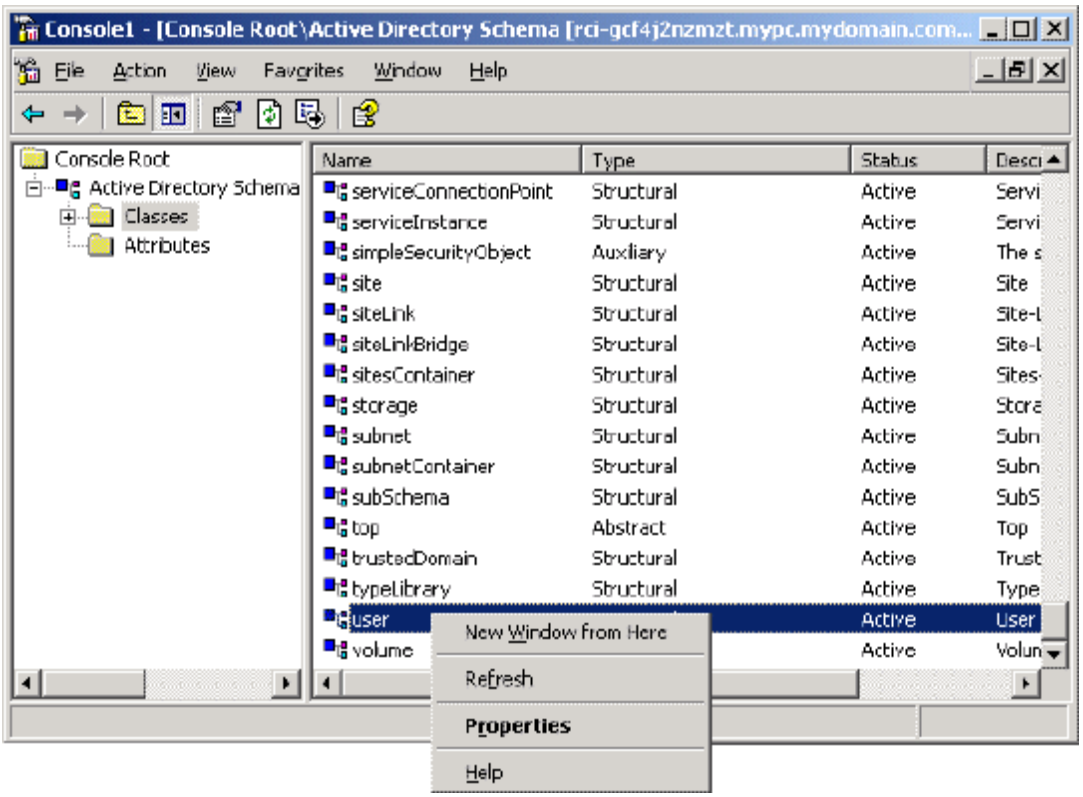


4. Geben Sie im Feld "Common Name" (Allgemeiner Name) den Wert *rciusergroup* ein.
5. Geben Sie im Feld "LDAP Display Name" (LDAP-Anzeigename) den Wert *rciusergroup* ein.
6. Geben Sie im Feld "Unique x5000 Object ID" (Eindeutige X500-OID) den Wert *1.3.6.1.4.1.13742.50* ein.
7. Geben Sie eine aussagekräftige Beschreibung im Feld "Description" (Beschreibung) ein.
8. Klicken Sie auf die Dropdownliste "Syntax" und wählen Sie "Case Insensitive String" (Groß-/Kleinschreibung nicht beachten) aus.
9. Geben Sie im Feld "Minimum" den Wert *1* ein.
10. Geben Sie im Feld "Maximum" den Wert *24* ein.
11. Klicken Sie zum Erstellen des neuen Attributs auf OK.

Hinzufügen von Attributen zur Klasse

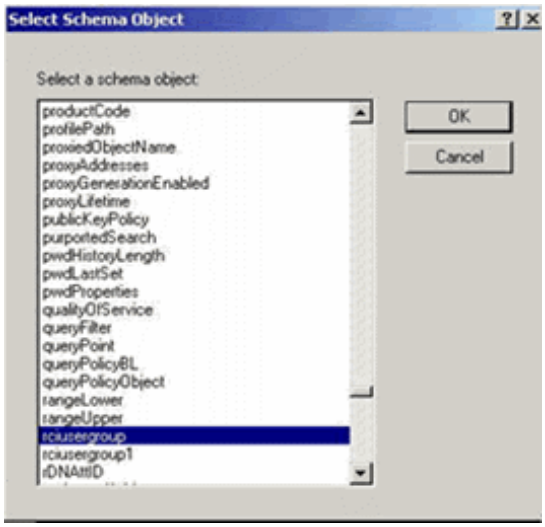
So fügen Sie der Klasse Attribute hinzu:

1. Klicken Sie im linken Fensterbereich auf "Classes" (Klassen).
2. Suchen Sie im rechten Fensterbereich den Wert "User Class" (Benutzerklasse) und klicken Sie mit der rechten Maustaste darauf.



3. Wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü. Das Dialogfeld "User Properties" (Benutzereigenschaften) wird geöffnet.
4. Klicken Sie auf die Registerkarte "Attributes" (Attribute), um diese zu öffnen.
5. Klicken Sie auf "Add" (Hinzufügen).

6. Wählen Sie in der Liste "Select Schema Object" (Schemaobjekt auswählen) den Eintrag "rciusergroup" aus.



7. Klicken Sie im Dialogfeld "Select Schema Object" (Schemaobjekt auswählen) auf OK.
8. Klicken Sie im Dialogfeld "User Properties" (Benutzereigenschaften) auf OK.

Aktualisieren des Schemacache

So aktualisieren Sie den Schemacache:

1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Active Directory® Schema", und wählen Sie "Reload the Schema" (Schema neu laden) aus.
2. Minimieren Sie die Active Directory-Schema-MMC-Konsole (Microsoft® Management Console).

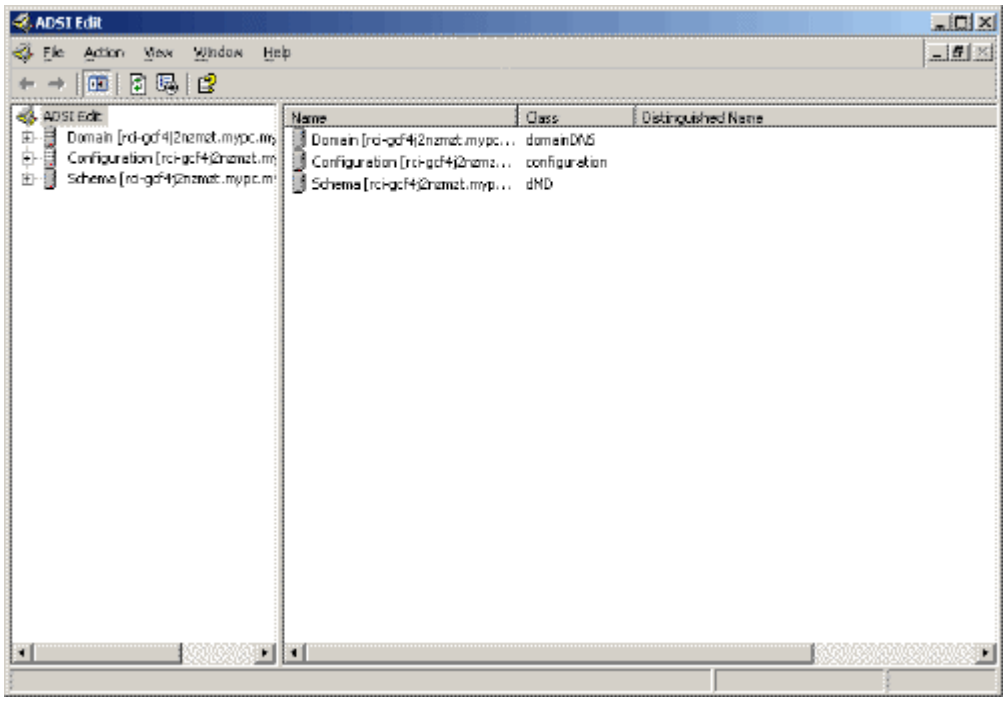
Bearbeiten von rciusergroup-Attributen für Benutzermitglieder

Verwenden Sie zum Ausführen des Active Directory®-Skripts auf einem Windows 2003®-Server das von Microsoft® bereitgestellte Skript (verfügbar auf der Windows 2003-Serverinstallations-CD). Diese Skripts werden bei der Installation von Microsoft® Windows 2003 mit installiert. ADSI (Active Directory Service Interface) fungiert hierbei als Low-Level-Editor für Active Directory und ermöglicht so das Durchführen allgemeiner Verwaltungsaufgaben wie Hinzufügen, Löschen und Verschieben von Objekten mit einem Verzeichnisdienst.

So bearbeiten Sie die einzelnen Benutzerattribute innerhalb der Gruppe "rciusergroup":

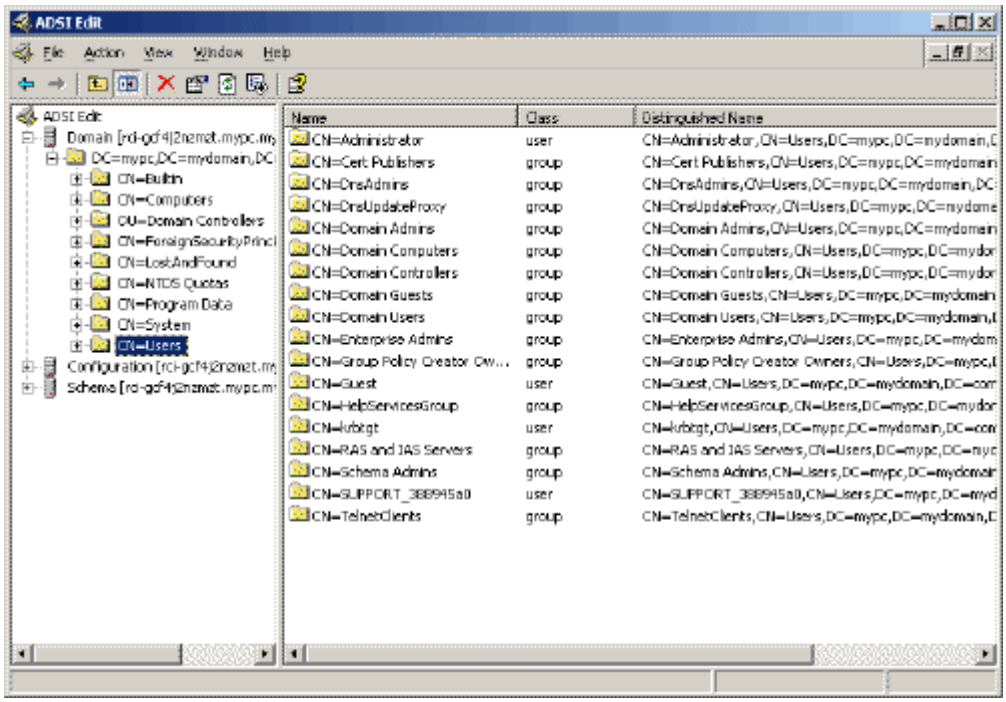
1. Wählen Sie auf der Installations-CD "Support" > "Tools" aus.

2. Doppelklicken Sie zur Installation der Support-Tools auf "SUPTOOLS.MSI".
3. Wechseln Sie zum Installationsverzeichnis der Support-Tools. Führen Sie "adsiedit.msc" aus. Das Fenster "ADSI Edit" (ADSI-Bearbeitung) wird angezeigt.



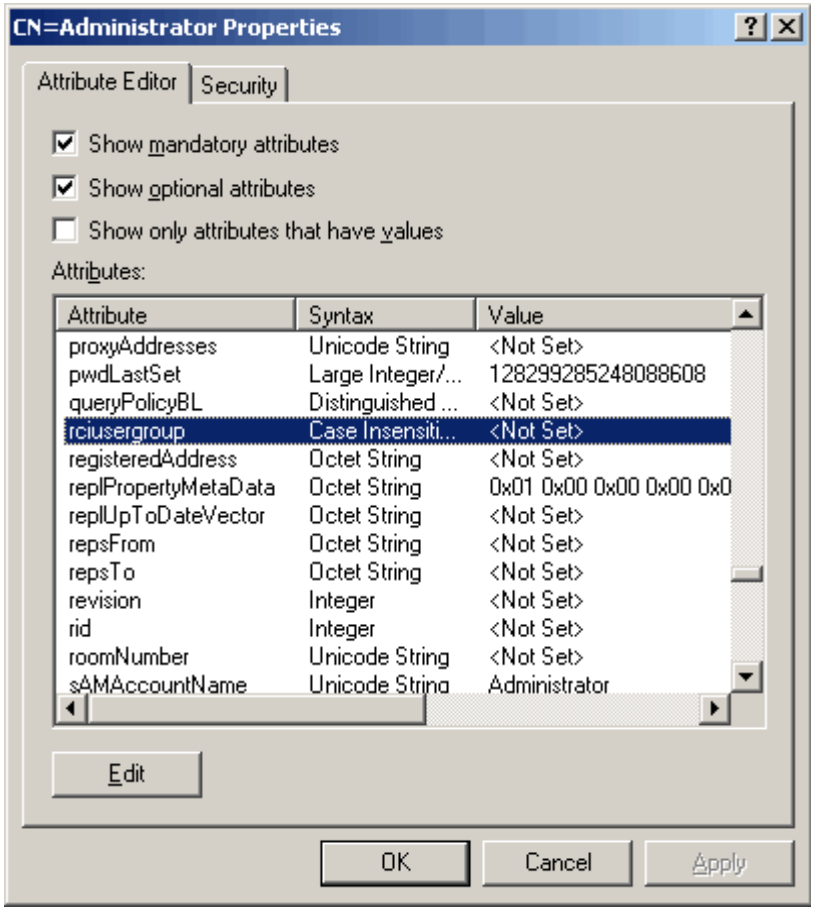
4. Öffnen Sie die Domäne.

5. Klicken Sie im linken Fensterbereich auf den Ordner "CN=Users" (CN=Benutzer).

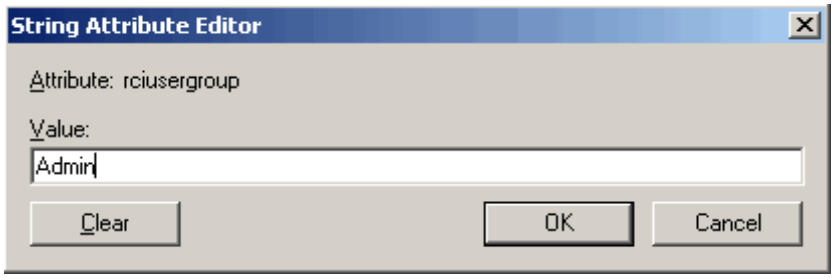


6. Navigieren Sie im rechten Fensterbereich zu dem Namen des Benutzers, dessen Eigenschaften geändert werden sollen. Klicken Sie mit der rechten Maustaste auf den Benutzernamen, und wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü aus.

7. Klicken Sie auf die Registerkarte "Attribute Editor" (Attributeditor), um sie anzuzeigen, wenn sie noch nicht geöffnet ist. Wählen Sie in der Liste "Attributes" (Attribute) "rciusergroup" aus.



8. Klicken Sie auf "Edit" (Bearbeiten). Das Dialogfeld "String Attribute Editor" (Attributeditor für Zeichenfolgen) wird angezeigt.
9. Geben Sie die Benutzergruppe (erstellt in KX III) in das Feld "Edit Attribute" (Attribut bearbeiten) ein. Klicken Sie auf OK.

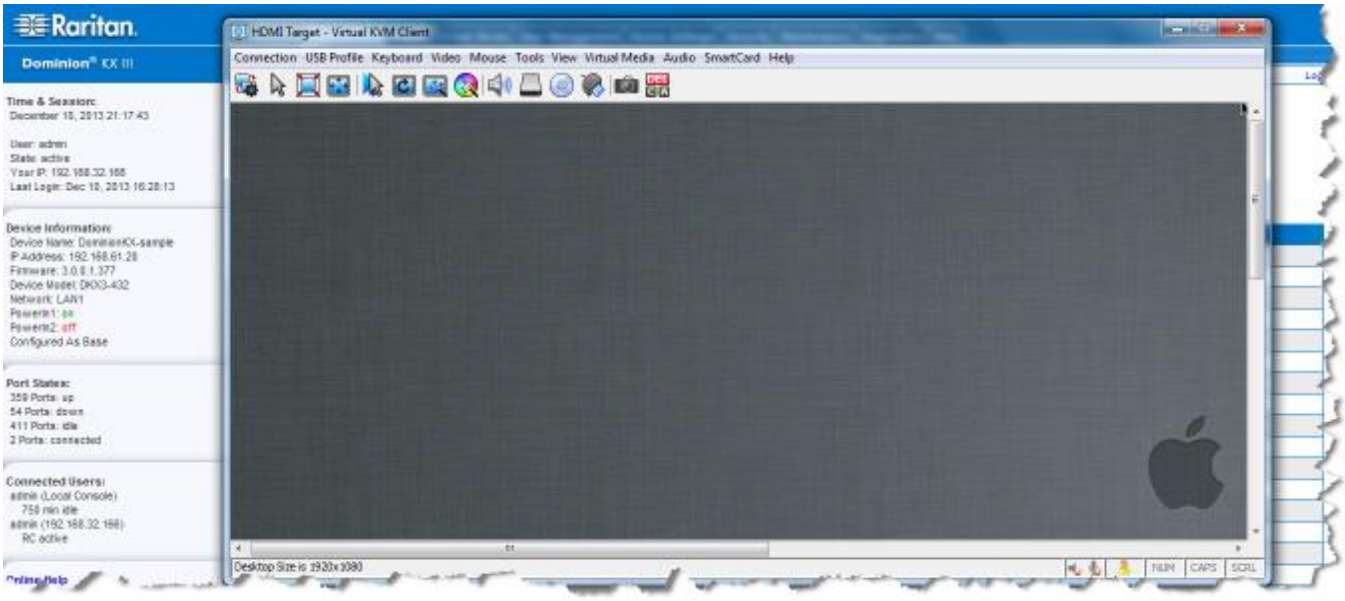


Kapitel 5 Virtual KVM Klient (VKC) Hilfe

In diesem Kapitel

Überblick

Wenn Sie über die Remotekonsole auf einen Zielserver zugreifen, wird ein Fenster für den Virtual KVM Client (VKC) geöffnet.



Es steht ein Virtual KVM Client für jeden verbundenen Zielserver zur Verfügung.

Die Fenster des Virtual KVM Client können minimiert, maximiert und auf dem Desktop verschoben werden.

WICHTIG: Beachten Sie, dass beim Aktualisieren des Browsers die Verbindung des Virtual KVM Client beendet wird.

Der Virtual KVM Client (VKC) und der Active KVM Client (AKC) sind Schnittstellen, mit denen auf Remoteziele zugegriffen werden kann.

VKC und AKC ähnliche Eigenschaften mit Ausnahme der nachfolgend aufgeführten Punkte über identische Leistungsmerkmale:

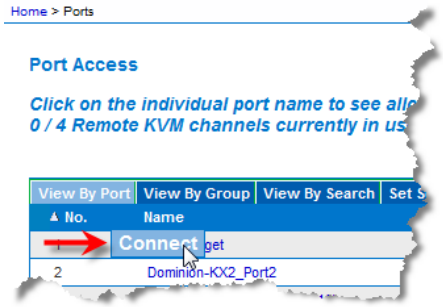
- Mindestanforderungen an das System
- Unterstützte Betriebssysteme und Browser
- Auf dem AKC erstellte Tastaturmakros können im VKC nicht genutzt werden.
- Konfiguration des direkten Portzugriffs (siehe **Aktivieren des direkten Port-Zugriffs über URL**)
- Konfiguration der AKC-Serverzertifikat-Validierung (siehe **Voraussetzungen für die Verwendung des AKC** (siehe "**Voraussetzungen für die Verwendung von AKC**" auf Seite 306))

Verbinden eines Zielservers

Sobald Sie in KX III Remote eingeloggt sind, greifen Sie auf die Zielserver über den Virtual KVM Client (VKC) oder den Active KVM Client (AKC) zu.

So schließen Sie einen verfügbaren Zielserver oder dualen Monitorzielserver an:

1. Auf der Portzugang-Seite klicken Sie unter Port Name (Portname) auf den Portnamen des Zielservers, an den Sie sich anschliessen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Klicken Sie auf/// ///Connect (Verbinden).



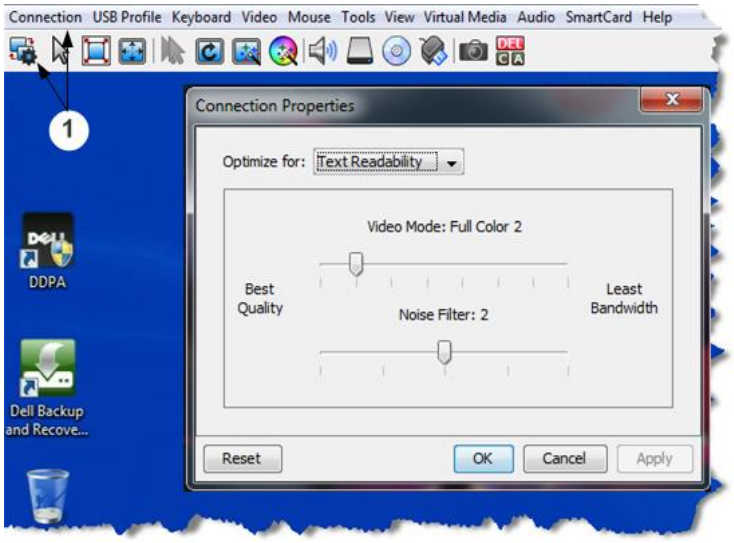
Weitere Informationen zu verfügbaren Menüoptionen finden Sie unter ***Menü "Port Action" (Portaktion*** (siehe "***Menü Port Action (Portaktion)***" auf Seite 20)).

Konfiguration von Verbindungseigenschaften

Zugriff zu Verbindungseigenschaften

Zugriff zu Verbindungseigenschaften:

1	Klicken Sie auf Verbindung > Eigenschaften oder klicken Sie auf Verbindung ... Um den Verbindungseigenschaften-Dialog zu öffnen.



Über Verbindungseigenschaften

Virtual KVM Client (VKC) und Active KVM Client (AKC)

Verbindungseigenschaften verwalten die Streaming Video-Leistung über eine Fernverbindung mit dem Zielserver.

Die Eigenschaften werden nur für Ihre Verbindung angewendet - sie haben keine Auswirkungen auf den Anschluss von anderen Benutzern auf den gleichen Zielservern über VKC und AKC.

Wenn Sie die Verbindungseigenschaften ändern, werden sie von VKC und AKC beibehalten.

Standard Verbindungs-Eigenschaftseinstellungen - Optimiert für die beste Leistung

KX III kommt konfiguriert, um eine optimale Leistung für die Mehrzahl der Video-Streaming-Bedingungen zu bieten.

Standard Verbindungseinstellungen sind:

- Optimisierung für: Textlesbarkeit - Video-Modi sind entworfen, um die Textlesbarkeit zu maximieren.

  Diese Einstellung ist ideal für Allgemeine IT und Computer-Anwendungen, sowie für Server-Administration.

- Videomodus - Standardeinstellungen ist Vollständige Farben 2.

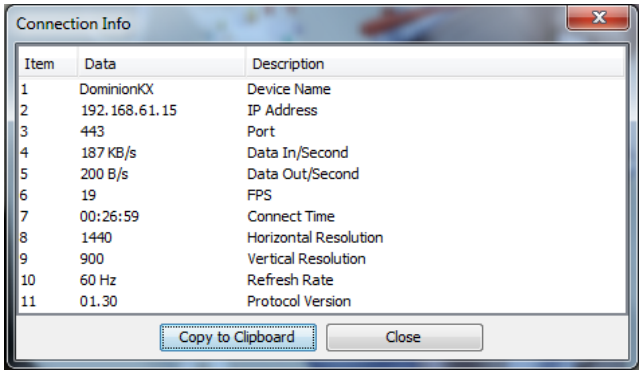
  Video-Frames übertragen in hochwertigen, 24-Bit-Farbe. Diese Einstellung eignet sich, wenn ein Hochgeschwindigkeits-LAN verwendet wird.

- Rauschfilter - Standardeinstellungen ist 2.

  Die Rauschfiltereinstellung muss nicht häufig geändert werden.

Klicken Sie auf „Zurücksetzen“ in dem Verbindungseigenschaften-Dialog, wenn Sie die Einstellungen jederzeit auf die Standardeinstellungen zurückzusetzen möchten.

Tipp: Verwenden Sie das Dialogfeld „Verbindungsinformationen“, um die Verbindung in Echtzeit zu überwachen. Siehe **Zugang and Kopieren-Verbindungsinformationen** *(auf Seite 256)*



Optimisierung für: Auswahl

Textlesbarkeit

Wenn Textlesbarkeit ausgewählt ist, werden alle Video-Modi eingestellt, um qualitativ hochwertigen, lesbaren Text zu liefern.

Diese Einstellung ist ideal, wenn Sie mit Computer-GUIs arbeiten oder bei der Durchführung von Server-Administration, etc.

Wenn es in Vollfarbe-Modi arbeitet, wird eine leichte Kontrastanhebung vorgesehen, und der Text wird klarer sein.

In geringeren Video-Qualität-Modi wird die Bandbreite auf Kosten der Genauigkeit verringert.

Farbgenauigkeit

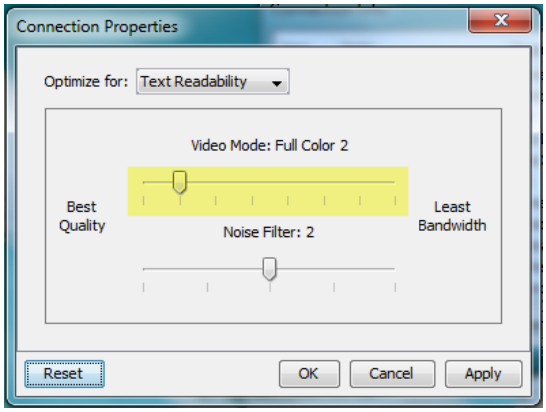
Wenn die Farbgenauigkeit ausgewählt ist, werden alle Video-Modi in Vollfarbe mit flachen Farbverhalten dargestellt.

Diese Einstellung gilt für die Wiedergabe von Videoströmen, wie Filme oder andere Broadcast-Streams.

In geringeren Videoqualität-Modi wird die Schärfe von feinen Einzelheiten, wie Text verringert.

Videomodus

Der Videomodus-Slider kontrolliert jede Video-Frame-Codierung und beeinflussend die Videoqualität, Bildrate und Bandbreite.



In der Regel führt das Bewegen des Schiebereglers nach links zu einer höheren Qualität auf Kosten der höheren Bandbreite, und in einigen Fällen zu einer niedrigeren Bildrate.

Das Bewegen des Schiebereglers auf der rechten Seite ermöglicht stärkere Kompression, die Verringerung der Bandbreite pro Rahmen, aber die Videoqualität wird reduziert.

In Situationen, wo die Systembandbreite ein limitierender Faktor ist, bewegen Sie den Videomodus-Schieberegler nach rechts.

Wenn die Textlesbarkeit als Optimierte Einstellung ausgewählt ist, bieten die vier Modi reduzierte Farbauflösung oder keine Farbe.

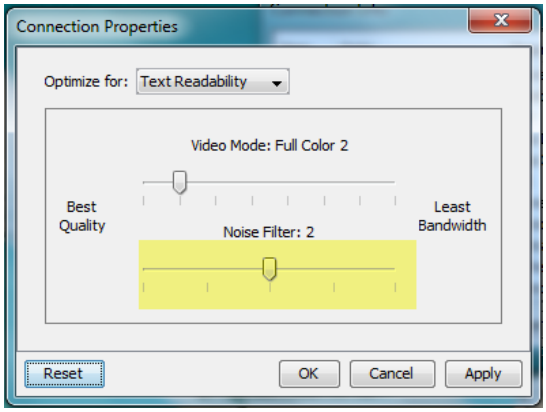
Diese Modi sind für die Administrationsarbeit, wo Text-und GUI-Elemente Priorität haben und wo die Bandbreite sehr hoch ist.

Klicken Sie auf „Zurücksetzen“ in dem Verbindungseigenschaften-Dialog, wenn Sie die Einstellungen jederzeit auf die Standardeinstellungen zurückzusetzen möchten.

Noise Filter (Rauschfilter)

Bitte ändern Sie die Rauschfiltereinstellungen nicht, außer wenn es nötig ist. Die Standardeinstellung funktioniert in den meisten Situationen gut.

Der Rauschfilter kontrolliert, wie viel Interface-Rauschen durch die KX III aufgenommen wird.



Das Verschieben des Rauschfilter-Sliders nach links verringert die Filterschwelle, was zu höherer dynamischer Video-Qualität führt. Aber mehr Lärm kann durchkommen, was zu höheren Bandbreiten und niedrigeren Bildraten führt.

Das Verschieben des Reglers nach rechts erhöht die Schwelle, ermöglicht weniger Lärm und benutzt weniger Bandbreite.

Das Bewegen des Rauschfilters auf der rechten Seite kann beim Zugriff auf einen Computer über GUI Verbindungen mit eingeschränkter Bandbreite nützlich sein.

Klicken Sie auf „Zurücksetzen“ in dem Verbindungseigenschaften-Dialog, wenn Sie die Einstellungen jederzeit auf die Standardeinstellungen zurückzusetzen möchten.

Verbindungsinformationen

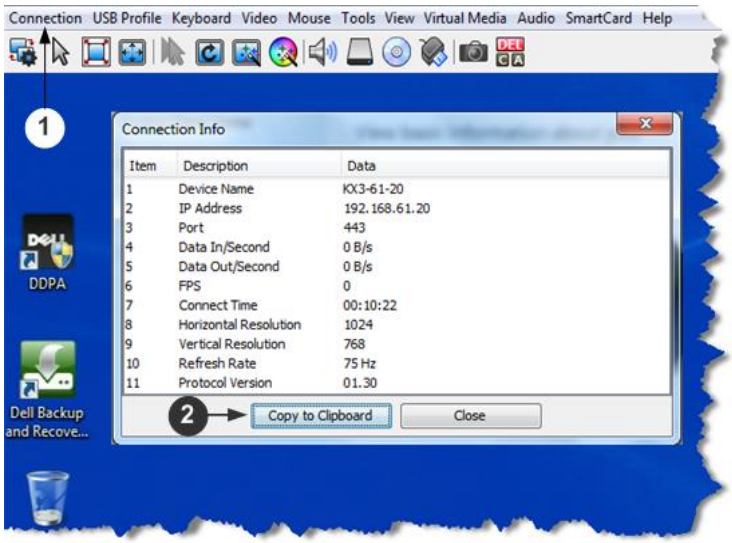
Öffnen Sie den Verbindungsinformationen-Dialog für echtzeitige Verbindungsinformationen, und kopieren Sie die Informationen nach Bedarf.

Dies ist nützlich, wenn Sie zum Beispiel Echtzeit-Informationen über die aktuellen Verbindungen sammeln wollen. Siehe ***Konfiguration von Verbindungseigenschaften*** (auf Seite 251)

Zur aktuellen Verbindung werden folgende Informationen angezeigt:

- KX III Name – Der Name von KX III.
- IP-Address (IP-Adresse) – Die IP-Adresse des KX III.
- Port – Der TCP/IP-Port für die KVM-Kommunikation, über den auf KX III zugegriffen wird.
- Data In/Second (Dateneingang/Sekunde) – Eingehende Datenrate von KX III.
- Data Out/Second (Datenausgang/Sekunde) – Ausgehende Datenrate KX III.
- Connect Time (Verbindungsdauer) – Die Dauer der Verbindung.
- FPS - Video Bilder pro Sekunde, erhalten von KX III.
- Horizontale Auflösung - Horizontale Auflösung des Zielservers.
- Vertikale Auflösung - Vertikale Auflösung des Zielservers.
- Aktualisierungsfrequenz - Aktualisierungsfrequenz von dem Zielserver.
- Protokoll Version - Raritan Kommunikationsprotokoll-Version.

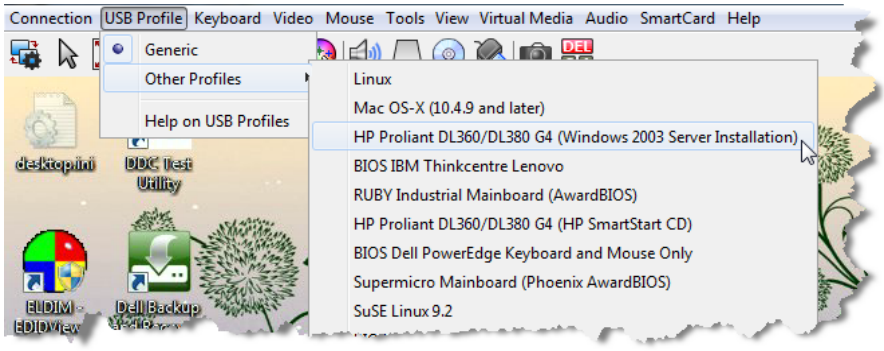
Zugang and Kopieren-Verbindungsinformationen



Schritte	
1	Klicken Sie auf Verbindung > Info ... Um den Verbindungs-Infodialog zu öffnen.
2	Klicken Sie auf "Copy to Clipboard" (In Zwischenablage kopieren). Fügen Sie die Informationen in der ausgewählten Datei ein.

USB-Profile

Bestimmen Sie ein USB-Profil für einen Zielserver aus der Virtual KVM Client (VKC), indem Sie auf „USB-Profil“ im Menü klicken.



Wählen Sie ein USB-Profil, das am besten auf den KVM-Zielserver zutrifft.

Wenn beispielsweise der Server ausgeführt wird und der Benutzer das Windows®-Betriebssystem verwenden möchte, ist es sinnvoll, das generische Profil zu verwenden.

Wenn der Benutzer jedoch die Einstellungen im BIOS-Menü ändern oder von einem virtuellen Medienlaufwerk einen Neustart ausführen möchte, kann, je nach Zielservermodell, ein BIOS-Profil eher geeignet sein.

Weitere Informationen zu **USB-Profilen** (siehe "**USB-Profile**" auf Seite 49) finden Sie unter USB-Profile.

Tastatur

STRG+ALT+ENTF-Makro Senden

Aufgrund der häufigen Verwendung dieser Tastenkombination ist ein Makro STRG+ALT+ENTF vorprogrammiert.

Wählen Sie Keyboard > Send Ctrl+Alt+Delete (Tastatur > Strg+Alt+Entf senden), oder klicken Sie auf die Ctrl+Alt+Delete Taste 

in der Symbolleiste wird diese Tastenfolge an den Server oder den KVM-Switch gesendet, mit dem Sie zurzeit verbunden sind.

Wenn Sie aber bei der Verwendung des MPC oder RRC die Tastenkombination STRG+ALT+ENTF drücken, wird diese Eingabe aufgrund der Struktur des Windows-Betriebssystems zunächst von Ihrem eigenen PC interpretiert, anstatt die Tastenfolge wie gewünscht an den Zielserver zu senden.

Senden LeftAlt+Tab

Tastatur Auswählen > Senden LeftAlt + Tab um zwischen den offenenen Fenstern auf dem Zielserver oder KVM-Switch zu wechseln.

Einstellungen für CIM-Tastatur/Mausoptionen

So greifen Sie auf das DCIM-USBG2-Setupmenü zu:

1. Klicken Sie mit der Maus in ein Fenster, wie z. B. Windows-Editor (Windows® Betriebssystem) o. Ä.
2. Wählen Sie die Optionen für "Set CIM Keyboard/Mouse options" (CIM-Tastatur/-Maus festlegen) aus. Dies ist das Äquivalent für das Senden von linke Strg-Taste und Num Lock an das Ziel. Die Optionen für das CIM-Setupmenü werden angezeigt.
3. Legen Sie die Sprache und Mauseinstellungen fest.

4. Verlassen Sie das Menü, um zur normalen CIM-Funktionalität zurückzukehren.

Text zum Ziel Senden

Um die Funktion "Send Text to Target" (Text an Ziel senden) für das Makro zu verwenden:

1. Klicken Sie auf Tastatur > Text zum Ziel senden Text zum Ziel sSenden Dialog erscheint.
2. Geben Sie den Text ein, den Sie im Ziel sehen möchten.

Hinweis: Nicht-englische Zeichen werden nicht von der Text-zum Ziel-Senden-Funktion unterstützt.

3. Wenn das Ziel eine US / Internationale Tastaturbelegung verwendet, wählen Sie das Kontrollkästchen "Zielsystem in den USA / Internationale Tastaturbelegung“.
4. Klicken Sie auf OK.

Keyboard Macros (Tastaturmakros)

Tastaturmakros gewährleisten, dass für den Zielserver vorgesehene Tastenkombinationen an den Zielserver gesendet und nur von diesem interpretiert werden. Andernfalls werden sie von dem Computer interpretiert, auf dem der Virtual KVM Client ausgeführt wird (Client-PC).

Makros werden auf dem Client-PC gespeichert und sind PC-spezifisch. Wenn Sie einen anderen PC verwenden, können Sie daher Ihre Makros nicht sehen.

Wenn eine andere Person Ihren PC verwendet und sich mit einem anderen Benutzernamen anmeldet, werden ihr die Makros angezeigt, da sie für den gesamten Computer gelten.

Tastaturmakros, die auf dem Active KVM Client (AKC) erstellt wurden, können jedoch nicht in VKC verwendet werden. Dies trifft umgekehrt ebenfalls zu.

Neues Makro erstellen

So erstellen Sie ein Makro:

1. Klicken Sie auf "Keyboard“ > "Keyboard Macros" (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Klicken Sie auf Hinzufügen. Das Dialogfeld Add Keyboard Macro (Tastaturmakro hinzufügen) wird angezeigt.

3. Geben Sie im Feld "Keyboard Macro Name" (Name des Tastaturmakros) einen Namen für das Makro ein. Dieser Name wird nach der Erstellung im Tastaturmenü angezeigt.
4. Wählen Sie in der Dropdownliste im Feld "Hot-Key Combination" (Zugriffstastenkombination) eine Tastenkombination aus. Dies ermöglicht es Ihnen, das Makro mit einer vordefinierten Tastenkombination auszuführen.
5. Wählen Sie in der Dropdownliste "Keys to Press" (Zu betätigende Tasten) alle Tasten aus, die Sie verwenden möchten, um die Tastenkombination zu emulieren, die zum Ausführen des Befehls verwendet wird. Wählen Sie die Tasten in der Reihenfolge aus, in der sie betätigt werden sollen. Wählen Sie nach jeder gewählten Taste "Add Key" (Taste hinzufügen) aus. Nach der Auswahl jeder Taste wird diese im Feld "Macro Sequence" (Makrosequenz) angezeigt und ein Befehl zum Freigeben der Taste wird automatisch hinzugefügt.

   Erstellen Sie beispielsweise ein Makro zum Schließen eines Fensters durch die Tastenkombination "Linke Strg-Taste+Esc". Dieses wird im Feld "Macro Sequenz" (Makrosequenz) wie folgt angezeigt:

   Press Left Alt (Linke Alt-Taste drücken)

   Press F4 (F4 drücken)

   Esc

   Release F4 (F4 loslassen)

   Esc

   Release Left Alt (Linke Alt-Taste loslassen)
6. Überprüfen Sie das Feld "Macro Sequence" (Makrosequenz), um sicherzustellen, dass die Makrosequenz korrekt definiert wurde.
   a. Wenn Sie einen Schritt aus der Sequenz entfernen möchten, markieren Sie diesen, und klicken Sie auf "Remove" (Entfernen).
   b. Wenn Sie die Reihenfolge der Schritte in der Sequenz ändern möchten, klicken Sie auf den Schritt und anschließend auf die Pfeil-nach-oben- oder Pfeil-nach-unten-Taste, um die Position des Schritts wie gewünscht zu ändern.
7. Klicken Sie zum Speichern des Makros auf "OK". Klicken Sie auf "Clear" (Löschen), um alle Felder zu löschen und erneut mit der Auswahl zu beginnen. Wenn Sie auf "OK" klicken, wird das Dialogfenster "Keyboard Macros" (Tastaturmakros) mit dem neuen Tastaturmakro angezeigt.
8. Klicken Sie im Dialogfeld "Keyboard Macros" (Tastaturmakros) auf "Close" (Schließen). Das Makro wird nun im Tastaturmenü der Anwendung angezeigt.
9. Wählen Sie das neue Makro im Menü aus, um es auszuführen, oder verwenden Sie die dem Makro zugeordnete Tastenkombination.

Makros Importieren

So importieren Sie Makros:

1. Zum Öffnen des Dialogfelds "Import Macros" (Makros importieren) wählen Sie "Keyboard Import Keyboard Macros" (Tastatur > Tastaturmakros importieren). Navigieren Sie zu dem Ordner, in dem die Makrodatei abgespeichert ist.
2. Klicken Sie auf die Makrodatei und anschließend auf "Open" (Öffnen), um das Makro zu importieren.
   a. Wenn zu viele Makros in der Datei enthalten sind, wird eine Fehlermeldung angezeigt. Wenn Sie auf "OK" klicken, wird der Import abgebrochen.
   b. Schlägt der Import fehl, wird ein Dialogfeld "Error" (Fehler) und eine Meldung mit den Gründen für den fehlgeschlagenen Import angezeigt. Klicken Sie auf "OK" und setzen Sie den Import fort, ohne dabei jedoch die Makros zu importieren, bei denen der Import fehlgeschlagen ist.
3. Wählen Sie die zu importierenden Makros aus, indem Sie die entsprechenden Kontrollkästchen markieren, oder verwenden Sie die Option "Select All" (Alle auswählen) bzw. "Deselect All" (Alle deaktivieren).
4. Klicken Sie auf "OK", um den Import zu starten.
   a. Wird ein doppelt vorhandenes Makro gefunden, wird das Dialogfeld "Import Macros" (Makros importieren) angezeigt. Führen Sie einen der folgenden Schritt aus:

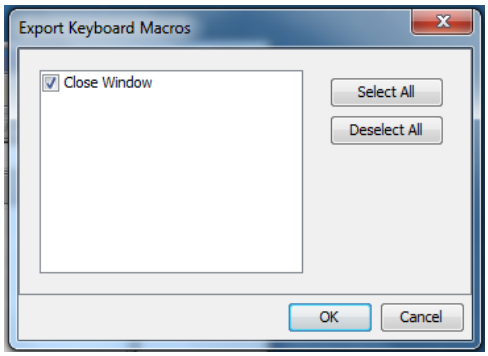
- Klicken Sie auf "Yes" (Ja), um das bereits vorhandene Makro mit dem importierten zu ersetzen.
- Klicken Sie auf "Yes to All" (Ja, alle), um die jeweils ausgewählten sowie alle anderen gefundenen doppelten Makros zu ersetzen.
- Klicken Sie auf "No" (Nein), um das ursprüngliche Makro beizubehalten, und fahren Sie dann mit dem nächsten Makro fort.
- Klicken Sie auf "No to All" (Nein, nicht alle), um das ursprüngliche Makro beizubehalten, und fahren Sie dann mit dem nächsten Makro fort. Werden weitere doppelte Makros gefunden, werden diese bei dem Vorgang ebenfalls übergangen.
- Klicken Sie auf "Cancel" (Abbrechen), um den Import abzubrechen.
- Sie können ebenfalls auf "Rename" (Umbenennen) klicken, um das Makro umzubenennen und es dann zu importieren. Wenn Sie "Rename" (Umbenennen) ausgewählt haben, wird das Dialogfeld "Rename Macro" (Makro umbenennen) angezeigt. Geben Sie in das Feld einen neuen Namen für das Makro ein und klicken Sie auf "OK". Das Dialogfeld wird geschlossen und der Vorgang wird fortgesetzt. Wenn es sich bei dem eingegebenen Namen um den eines doppelten Makros handelt, wird eine Warnmeldung angezeigt und Sie werden aufgefordert, einen anderen Namen für den Makro einzugeben.

b. Wenn während des Importprozesses die erlaubte Anzahl von importierten Makros überstiegen wird, wird ein Dialogfeld angezeigt. Klicken Sie auf "OK", wenn Sie den Importvorgang der Makros fortsetzen möchten, oder klicken Sie auf "Cancel" (Abbrechen), um den Vorgang zu beenden.

Die Makros werden dann importiert. Wenn ein Makro importiert wird, das eine bereits vorhandene Zugriffstaste enthält, wird die Zugriffstaste für das importierte Makro verworfen.

Makros Exportieren

1. Um das Dialogfeld "Select Keyboard Macros to Export" (Tastaturmakros für den Export auswählen) zu öffnen, wählen Sie "Tools Export Macros" (Extras > Makros exportieren) aus.



2. Wählen Sie die zu exportierenden Makros aus, indem Sie die entsprechenden Kontrollkästchen markieren, oder verwenden Sie die Option "Select All" (Alle auswählen) bzw. "Deselect All" (Alle deaktivieren).
3. Klicken Sie auf "OK". Ein „Tastaturmakros Exportieren“-Dialog wird angezeigt. Hier können Sie die gewünschte Makrodatei lokalisieren und auswählen. Das Makro ist standardmäßig auf Ihrem Desktop vorhanden.
4. Wählen Sie den Ordner aus, in dem Sie die Makrodatei abspeichern möchten, geben Sie einen Namen für die Datei ein und klicken Sie auf "Save" (Speichern). Wenn das Makro bereits vorhanden ist, wird eine Warnmeldung angezeigt.
5. Klicken Sie auf "Yes" (Ja), um das vorhandene Makro zu überschreiben, oder auf "No" (Nein), um die Meldung zu schließen. Das Makro wird dann nicht überschrieben.

Videoeigenschaften

Aktualisieren der Anzeige

Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms. Videoeinstellungen können auf verschiedene Art und Weise automatisch aktualisiert werden:

- Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms.
- Mit dem Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) werden die Videoeinstellungen des Zielservers automatisch erkannt.
- Mit dem Befehl "Calibrate Color" (Farbe kalibrieren) wird das Videobild kalibriert, um die angezeigten Farben zu verbessern.

Darüber hinaus können Sie die Einstellungen manuell über den Befehl "Video Settings" (Videoeinstellungen) anpassen.

Führen Sie einen der folgenden Schritte aus, um die Videoeinstellungen zu aktualisieren:

- Wählen Sie "Video“ > "Refresh Screen" (Video > Anzeige aktualisieren) aus oder klicken Sie auf die Schaltfläche "Refresh Screen“ (Anzeige aktualisieren)  in der Symbolleiste.

Automatische Erkennung von Videoeinstellungen

Der Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) erzwingt das erneute Erkennen der Videoeinstellungen (Auflösung, Aktualisierungsfrequenz) und erstellt die Videoanzeige neu.

Führen Sie zur automatischen Erkennung der Videoeinstellungen die folgenden Schritte aus:

- Wählen Sie "Video“ > "Auto-sense Video Settings" (Video > Videoeinstellungen automatisch erkennen) aus oder klicken Sie auf die Schaltfläche "Auto-Sense Video Settings" (Videoeinstellungen automatisch erkennen).  in der Symbolleiste.

  Eine Meldung mit der Information, dass die automatische Anpassung läuft, wird angezeigt.

Kalibrieren der Farben

Verwenden Sie den Befehl "Calibrate Color" (Farbe kalibrieren), um die Farbstufen (Farbton, Helligkeit, Sättigung) der übertragenen Videobilder zu optimieren. Die Farbeinstellungen basieren auf dem jeweiligen Zielserver.

Hinweis: Der Befehl "Calibrate Color" (Farbe kalibrieren) gilt nur für die aktuelle Verbindung.

Um die Farbe zu kalibrieren, führen Sie Folgendes durch:

- Wählen Sie Video > Calibrate Color (Video Farbe kalibrieren), oder klicken Sie auf die Schaltfläche Calibrate Color  in der Symbolleiste.

  Die Farbkalibrierung des Zielgerätebildschirms wird aktualisiert.

Konfigurieren von Videoeinstellungen

Verwenden Sie den Befehl "Video Settings" (Videoeinstellungen), um die Videoeinstellungen manuell anzupassen.

So ändern Sie die Videoeinstellungen:

1. Wählen Sie "Video“ > "Video Settings" (Video > Videoeinstellungen) aus, um das Dialogfeld "Video Settings" (Videoeinstellungen) aufzurufen.
2. Passen Sie die folgenden Einstellungen nach Wunsch an. Wenn Sie die Einstellungen anpassen, sind die Änderungen sofort sichtbar:
   a. PLL Settings (PLL-Einstellungen)

      Clock (Uhr) – Diese Option steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobilds. Als Einstellung werden ungerade Zahlen empfohlen. Üblicherweise sollte diese Einstellung nicht geändert werden, da die automatische Erkennung meist korrekt ist.

      Phase – Die Phasenwerte liegen zwischen 0 und 31 und werden zyklisch durchlaufen. Halten Sie bei dem Phasenwert an, der das beste Videobild für den aktiven Zielserver ergibt.

   b. Brightness (Helligkeit): Mithilfe dieser Einstellung passen Sie die Helligkeit der Zielserveranzeige an.

   c. Brightness Red (Helligkeit – Rot) – Steuert die Helligkeit der Anzeige des Zielservers für das rote Signal.

d. Brightness Green (Helligkeit – Grün) – Steuert die Helligkeit des grünen Signals.

e. Brightness Blue (Helligkeit – Blau) – Steuert die Helligkeit des blauen Signals.

f. Contrast Red (Kontrast – Rot) – Steuert den Kontrast des roten Signals.

g. Contrast Green (Kontrast – Grün) – Steuert das grüne Signal.

h. Contrast Blue (Kontrast – Blau) – Steuert das blaue Signal.

Wenn das Videobild extrem verschwommen oder unscharf wirkt, können die Einstellungen für die Uhr und die Phase so gewählt werden, dass auf dem aktiven Zielserver ein besseres Bild angezeigt wird.

Warnhinweis: Gehen Sie beim Ändern der Einstellungen für die Uhr und die Phase sorgfältig vor. Änderungen können zu Verzerrungen oder sogar zum Verlust des Videobildes führen, und Sie können möglicherweise die vorherigen Einstellungen nicht wiederherstellen. Wenden Sie sich an den technischen Kundendienst von Raritan, bevor Sie Änderungen vornehmen.

---

i. Horizontal Offset (Horizontaloffset) – Steuert die horizontale Positionierung der Zielserveranzeige auf dem Bildschirm.

j. Vertical Offset (Vertikaloffset) – Steuert die vertikale Positionierung der Zielserveranzeige auf dem Bildschirm.

3. Wählen Sie "Automatic Color Calibration" (Automatische Farbkalibrierung) aus, um diese Funktion zu aktivieren.

4. Wählen Sie den Videoerkennungsmodus aus:

   - Best possible video mode (Bestmöglicher Videomodus)

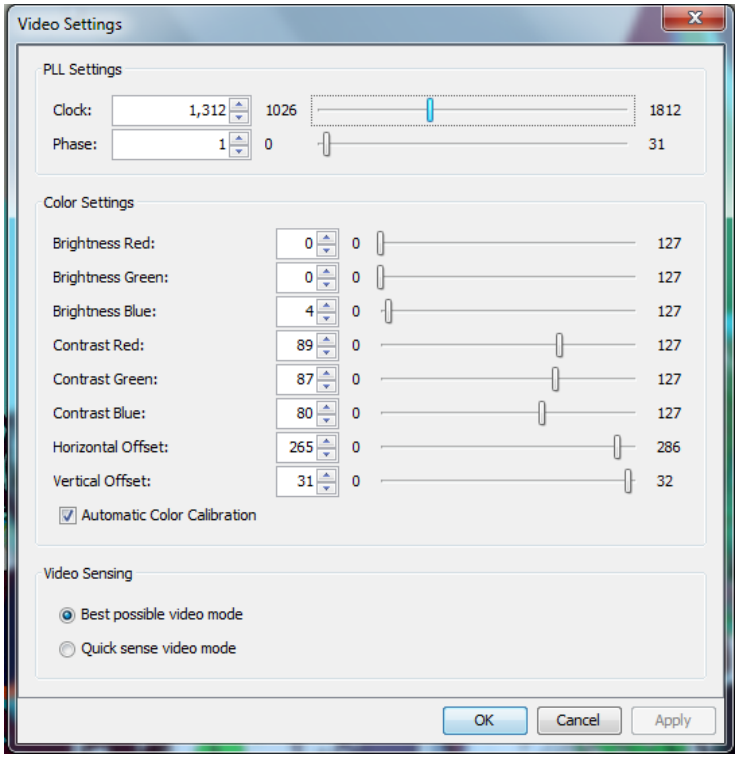
   Beim Wechseln von Zielgeräten oder Zielauflösungen führt das Gerät die vollständige automatische Erkennung durch. Bei dieser Option wird das Videobild so kalibriert, dass die bestmögliche Bildqualität erzielt wird.

   - Quick sense video mode (Videomodus schnell erkennen)

   Bei dieser Option führt das Gerät eine schnelle automatische Erkennung des Videomodus durch, um das Bild des Zielgeräts schneller anzuzeigen. Diese Option eignet sich insbesondere für die Eingabe der BIOS-Konfiguration eines Zielservers nach einem Neustart.

5. Klicken Sie auf OK, um die Einstellungen zu übernehmen, und schließen Sie das Dialogfenster. Klicken Sie auf "Apply" (Übernehmen), um die Einstellungen zu übernehmen, ohne das Dialogfenster zu schließen.

Hinweis: Einige Sun-Hintergrundanzeigen (z. B. Anzeigen mit sehr dunklen Rändern) werden auf bestimmten Sun-Servern nicht exakt zentriert abgebildet. Verwenden Sie einen anderen Hintergrund, oder platzieren Sie auf der Anzeige oben links ein helleres Symbol.



Screenshot vom Zielgerät-Befehl

Mit dem Befehl "Screenshot from Target" (Screenshot vom Zielgerät) können Sie einen Screenshot vom Zielserver aufnehmen. Speichern Sie diesen Screenshot ggf. an einem Speicherort Ihrer Wahl als Bitmap-, JPEG- oder PNG-Datei ab.

So nehmen Sie einen Screenshot vom Zielserver auf:

1. Wählen Sie "Video“ "Screenshot from Target" (Video > Screenshot vom Zielgerät) aus oder klicken Sie auf die Schaltfläche "Screenshot from Target" (Screenshot vom Zielgerät) in der Symbolleiste.
2. Wählen Sie im Dialogfenster "Save" (Speichern) den Speicherort für die Datei aus, benennen Sie sie und wählen Sie ein Dateiformat aus der Dropdownliste "Files of Type" (Dateitypen) aus.
3. Klicken Sie zum Speichern des Screenshots auf "Save" (Speichern).

Mausoptionen

Wenn Sie sich im Zwei-Cursor-Modus befinden und die Option ordnungsgemäß konfiguriert wurde, werden die Cursor aneinander ausgerichtet.

In Dualmodus, wenn ein Zielserver gesteuert wird, wird die Fernkonsole zwei Mauscursors anzeigen: Ein Cursor gehört zur KX III Client-Workstation und der andere zum Zielserver.

Sie können entweder im Ein-Cursor-Modus oder im Zwei-Cursor-Modus arbeiten.

Bei zwei Cursorn bietet das Gerät verschiedene Mausmodi:

- "Absolute" (Absolute Mouse Synchronization)
- "Intelligent" (Intelligenter Mausmodus)
- "Standard" (Standardmausmodus)

Wenn sich der Mauszeiger im Zielserverfenster des Virtual KVM Client befindet, werden Mausbewegungen und Klicks direkt an den angeschlossenen Zielserver übermittelt.

Aufgrund der Mausbeschleunigungseinstellungen sind die Bewegungen des Client-Mauszeigers etwas schneller als die des Zielgerätmauszeigers.

Bei schnellen LAN-Verbindungen können Sie den einzelnen Mauszeigermodus verwenden und nur den Cursor des Zielservers anzeigen.

Sie können zwischen den beiden Modi (ein Cursor und zwei Cursor) wechseln.

Dual-Mausmodi

Absolute Mouse Synchronization

In diesem Modus werden absolute Koordinaten verwendet, um die Cursor von Client und Zielgerät synchron zu halten, auch wenn für die Maus des Zielgeräts eine andere Beschleunigung oder Geschwindigkeit eingestellt wurde.

Dieser Modus wird von Servern mit USB-Ports unterstützt und ist der Standardmodus für Virtuelle Medien CIMs.

Absolute Mouse Synchronization erfodert die Verwendung von Virtuellen Medien CIM :

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

So gelangen Sie in die Absolute Maus-Synchronization:

- Wählen Sie Mouse > Absolute.

Der schwarze Anschluss am DVUSB CIM wird zum Anschließen von Maus und Tastatur verwendet. Der graue Anschluss wird für virtuelle Medien verwendet.

Achten Sie darauf, dass immer beide Anschlüsse des CIM mit dem Gerät verbunden sind. Es ist möglich, dass das Gerät nicht ordnungsgemäß funktioniert, wenn nicht alle Stecker an den Zielserver angeschlossen sind.

Intelligent

Im Mausmodus "Intelligent" erkennt das Gerät die Mauseinstellungen des Zielgeräts und kann die Cursor dementsprechend synchronisieren, wodurch die Mausbeschleunigung auf dem Zielgerät ermöglicht wird. Intelligenter Mausmodus wird standardmäßig für nicht-VM-Ziele verwendet.

So gelangen Sie in den intelligenten Mausmodus

So gelangen Sie in den intelligenten Mausmodus:

- Wählen Sie "Mouse Intelligent" (Maus > Intelligent).

Bedingungen für die intelligente Maussynchronisation

Der Befehl "Intelligent Mouse Synchronization" (Intelligente Maussynchronisierung) im Menü "Mouse" (Maus) synchronisiert automatisch die Cursor in Inaktivitätsphasen. Zur korrekten Synchronisierung müssen jedoch folgende Bedingungen erfüllt sein:

- Der Active Desktop muss auf dem Zielgerät deaktiviert sein.
- Oben in der linken Ecke auf der Zielseite dürfen keine Fenster angezeigt werden.
- Oben in der linken Ecke auf der Zielseite darf kein animierter Hintergrund vorhanden sein.
- Der Zielcursor muss standardmäßig und nicht animiert sein.
- Die Geschwindigkeit des Zielcursors darf nicht auf sehr hohe oder sehr niedrige Werte eingestellt sein.
- Erweiterte Mauseigenschaften wie "Enhanced pointer precision" (Zeigerbeschleunigung verbessern) oder "Snap mouse to default button in dialogs" (In Dialogfeldern automatisch zur Standardschaltfläche springen) müssen deaktiviert sein.
- Wählen Sie im Fenster "Video Settings" (Videoeinstellungen) die Option "Best Possible Video Mode" (Bestmöglicher Videomodus) aus.
- Die Ränder des Zielvideos müssen deutlich sichtbar sein. Ein schwarzer Rand muss also bei einem Bildlauf zu einem Rand des Zielvideobilds zwischen dem Zieldesktop und dem Fenster der KVM-Remotekonsole sichtbar sein.
- Wenn Sie die Funktion zur intelligenten Maussynchronisierung nutzen, können Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu Problemen führen. Um Probleme mit dieser Funktion zu vermeiden, empfiehlt Raritan, Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu entfernen.

Initiieren Sie nach dem automatischen Erkennen des Zielvideos manuell eine Maussynchronisierung. Klicken Sie dazu in der Symbolleiste auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren). Dies gilt auch bei Änderung der Auflösung des Zielgeräts, wenn die Cursor nicht mehr synchronisiert sind.

Schlägt die intelligente Maussynchronisierung fehl, wird die Standardeinstellung der Maussynchronisierung wiederhergestellt.

Beachten Sie, dass die Mauskonfigurationen auf unterschiedlichen Zielbetriebssystemen variieren. Weitere Informationen finden Sie in den Richtlinien für Ihr Betriebssystem. Die intelligente Maussynchronisierung ist für UNIX-Zielgeräte nicht verfügbar.

Mausmodus "Standard"

Beim Mausmodus "Standard" wird ein Standard-Maussynchronisierungsalgorithmus mit relativen Mauspositionen verwendet. Für den Mausmodus "Standard" müssen die Mausbeschleunigung deaktiviert und andere Mausparameter korrekt eingerichtet werden, damit die Client- und die Servermaus synchron bleiben.

So gelangen Sie in den Mausmodus "Standard":

- Wählen Sie **Mouse > Standard** (Maus > Standard).

Tipps zur Maussynchronisation

Wenn Sie Probleme mit der Maussynchronisation haben:

1. Stellen Sie sicher, dass die ausgewählte Videoauflösung und die Aktualisierungsfrequenz vom Gerät unterstützt werden. Im Dialogfeld "KVM Client Connection Info" (Virtual KVM Client – Verbindungsinformationen) werden die tatsächlich vom Gerät erkannten Werte angezeigt.
2. Erzwingen Sie eine automatische Erkennung, indem Sie im KVM Client auf die Schaltfläche zur automatischen Erkennung klicken.
3. Führen Sie folgende Schritte aus, falls dadurch die Maussynchronisation (bei Linux-, UNIX- und Solaris-KVM-Zielservern) nicht verbessert wird:
   a. Öffnen Sie ein Terminalfenster.
   b. Geben Sie den folgenden Befehl: `xset mouse 1 1` ein.
   c. Schließen Sie das Terminalfenster.
4. Klicken Sie im KVM Client auf die Schaltfläche zur Maussynchronisierung .  .

Synchronize Mouse (Maus synchronisieren)

Im Zwei-Cursor-Modus erzwingt der Befehl "Synchronize Mouse" (Maus synchronisieren) die erneute Ausrichtung des Zielserver-Mauszeigers am Mauszeiger des Virtual KVM Client.

Führen Sie einen der folgenden Schritte aus, um die Maus zu synchronisieren:

- Wählen Sie "Mouse“ "Synchronize Mouse" (Maus > Maus synchronisieren) aus oder klicken Sie auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren) in der Symbolleiste klicken.

Hinweis: Diese Option steht nur in den Mausmodi "Standard" und "Intelligent" zur Verfügung.

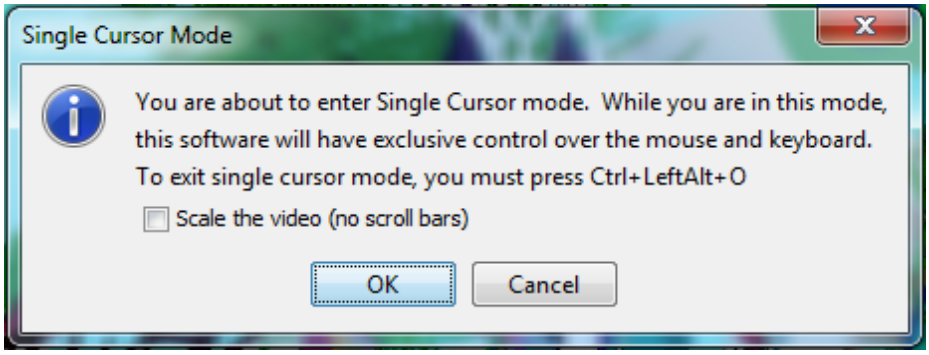
Ein-Cursor-Modus

Beim Ein-Cursor-Modus wird nur der Cursor des Zielservers verwendet; der lokale Mauszeiger wird nicht mehr angezeigt.

Hinweis: Der Ein-Cursor-Modus funktioniert nicht auf Windows- oder Linux-Zielgeräten, wenn der Client auf einer virtuellen Maschine ausgeführt wird.

Führen Sie einen der folgenden Schritte aus, um den Ein-Cursor-Modus zu aktivieren:

- Wählen Sie Mouse > Single Mouse Cursor (Maus Ein Cursor).
- Klicken Sie die Taste "Single/Double Mouse Cursor“ (Ein/Zwei Cursor) in der Symbolleiste.



So beenden Sie den Ein-Cursor-Modus:

1. Drücken Sie Strg+Alt+O auf der Tastatur, um den Ein-Cursor-Modus zu beenden.

Optionen im Menü "Tools" (Extras)

"General Settings" (Allgemeine Einstellungen)

So legen Sie die Optionen im Menü „Tools“ (Extras) fest:

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Enable Logging" (Protokollierung aktivieren) nur nach Anweisung durch den technischen Kundendienst.

   Bei dieser Option wird im Basisverzeichnis eine Protokolldatei erstellt.
3. Wählen Sie ggf. in der Dropdown-Liste "Keyboard Type" (Tastaturtyp) einen Tastaturtyp aus.

   Folgende Optionen stehen zur Verfügung:

   - US/International (USA/International)
   - Französisch (Frankreich)
   - Deutsch (Deutschland)
   - Japanisch
   - United Kingdom (Großbritannien)
   - Koreanisch (Korea)
   - Französisch (Belgien)
   - Norwegisch (Norwegen)
   - Portugiesisch (Portugal)
   - Dänisch (Dänemark)
   - Schwedisch (Schweden)
   - Deutsch (Schweiz)
   - Hungarian (Hungary) (Ungarisch)
   - Spanisch (Spanien)
   - Italienisch (Italien)
   - Slowenisch
   - Übersetzung: Französisch – Englisch (USA)
   - Übersetzung: Französisch – Englisch (USA/International)

   Beim AKC entspricht der Tastaturtyp standardmäßig dem lokalen Client. In diesem Fall trifft die Option nicht zu.
4. Konfigurieren von Zugriffstasten:

- Exit Full Screen Mode - Hotkey (Zugriffstaste zum Beenden des Vollbildmodus).

  Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver.

  Diese Zugriffstaste wird zum Beenden des Modus verwendet.

- "Exit Single Cursor Mode - Hotkey" (Zugriffstaste zum Beenden des Ein-Cursor-Modus):

  Im Ein-Cursor-Modus wird nur der Cursor des Zielservers angezeigt.

  Diese Zugriffstaste wird zum Beenden des Ein-Cursor-Modus verwendet, sodass der Client-Cursor wieder angezeigt wird.

- "Disconnect from Target - Hotkey" (Zugriffstaste zum Trennen der Verbindung mit dem Ziel):

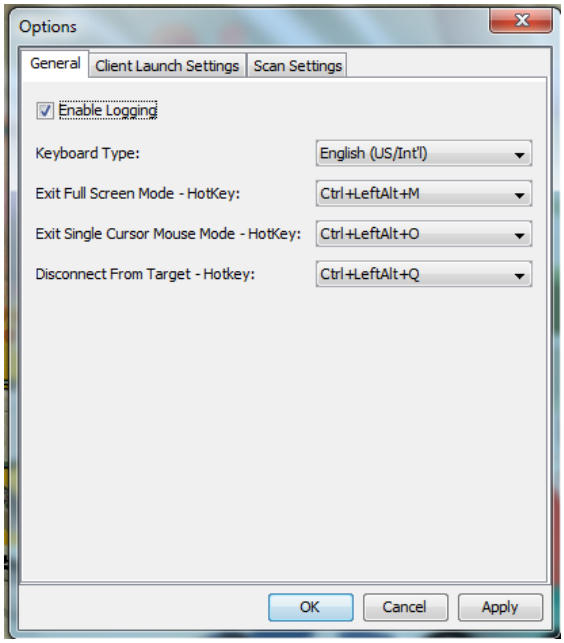
  Aktivieren Sie diese Zugriffstaste, damit Benutzer die Verbindung mit dem Ziel unverzüglich trennen können.

Bei der Kombination mehrerer Zugriffstasten kann eine Tastenkombination jeweils nur einer Funktion zugewiesen werden.

Wenn die Taste "Q" beispielsweise bereits der Funktion "Disconnect from Target" (Verbindung mit dem Ziel trennen) zugewiesen ist, ist sie für die Funktion "Exit Full Screen Mode" (Vollbildmodus beenden) nicht mehr verfügbar.

Wenn eine Zugriffstaste bei einer Aktualisierung hinzugefügt wird und der Standardwert für die Taste bereits verwendet wird, wird der Funktion stattdessen der nächste verfügbare Wert zugewiesen.

5. Klicken Sie auf OK.



Tastaturbeschränkungen

Türkische Tastaturen

Bei Verwendung einer türkischen Tastatur müssen Sie die Verbindung mit einem Zielserver über den Active KVM Client (AKC) herstellen. Von anderen Raritan-Clients wird es nicht unterstützt.

Slowenische Tastaturen

Aufgrund einer JRE-Beschränkung funktioniert die Taste < auf slowenischen Tastaturen nicht.

Sprachkonfiguration für Linux

Da mit der Sun-JRE auf einem Linux-Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenereignissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Sprache	Konfigurationsmethode
USA/Int.	Standard
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch (Deutschland)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Sprache	Konfigurationsmethode
Japanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Belgisch	Keyboard Indicator (Tastaturanzeige)
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.

Client Launch Settings (Client-Starteinstellungen)

Mithlife des Konfigurierens von "Client Launch Settings" (Client-Starteinstellungen) können Sie die Bildschirmeinstellungen für eine KVM-Sitzung definieren.

So konfigurieren Sie Starteinstellungen für den Client:

1. Wählen Sie "Tools" (Extras), "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Klicken Sie auf die Registerkarte "Client Launch Settings" (Client-Starteinstellungen).
   - So konfigurieren Sie die Zielfenstereinstellungen:

a. Wählen Sie "Standard - sized to target Resolution" (Standard - Größe an Zielauflösung anpassen) aus, um das Fenster mit der aktuellen Auflösung des Ziels zu öffnen. Wenn die Zielauflösung größer als die Client-Auflösung ist, bedeckt das Zielfenster soviel Bildschirmfläche wie möglich. Gegebenenfalls werden Bildlaufleisten hinzugefügt.

b. Wählen Sie "Full Screen" (Vollbild) aus, um das Zielfenster im Vollbildmodus zu öffnen.

- So konfigurieren Sie den Monitor, auf dem der Ziel-Viewer gestartet wird:

a. Wählen Sie "Monitor Client Was Launched from" (Monitor-Client gestartet von) aus, wenn der Ziel-Viewer in derselben Anzeige wie die auf dem Client verwendete Anwendung gestartet werden soll (z. B. ein Webbrowser oder ein Applet).

b. Wählen Sie "Select From Detected Monitors" (Aus gefundenen Monitoren auswählen) aus, um einen Monitor aus einer Liste mit Monitoren auszuwählen, die momentan von der Anwendung gefunden werden. Wenn ein zuvor ausgewählter Monitor nicht mehr gefunden wird, wird "Currently Selected Monitor Not Detected" (Aktuell ausgewählter Monitor nicht gefunden) angezeigt.

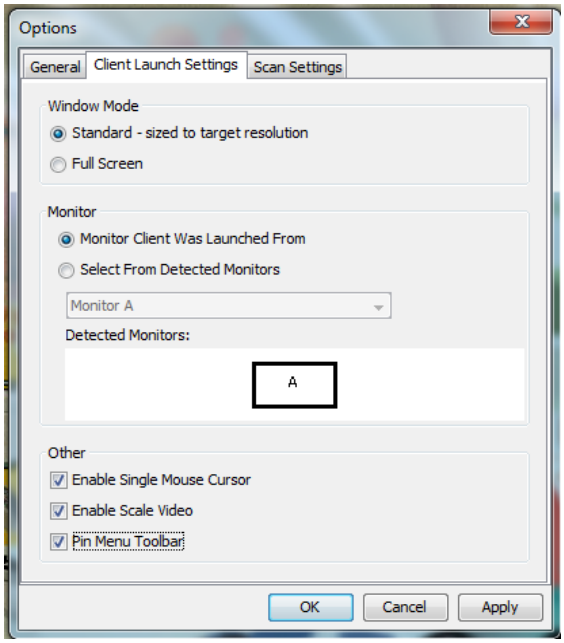
- So konfigurieren Sie zusätzliche Starteinstellungen:

a. Wählen Sie "Enable Single Cursor Mode" (Ein-Cursor-Modus aktivieren), um den Ein-Cursor-Modus bei Zugriff auf den Server als Standardmausmodus zu aktivieren.

b. Wählen Sie "Enable Scale Video" ("Video skalieren" aktivieren) aus, damit die Anzeige auf dem Zielserver automatisch skaliert wird, sobald auf ihn zugegriffen wird.

c. Wählen Sie "Pin Menu Toolbar" (Menüsymbolleiste anheften), wenn die Symbolleiste auf dem Ziel im Vollbildmodus sichtbar bleiben soll. Wenn sich das Ziel im Vollbildmodus befindet, ist das Menü in der Standardeinstellung nur sichtbar, wenn Sie mit der Maus auf den oberen Bildschirmrand zeigen.

3. Klicken Sie auf OK.



Konfigurieren von Port-Scaneinstellungen über VKC und AKC

Die Konfiguration von Port-Scannen-Optionen in VKC un AKC gilt für das Scannen von der KX III Remote Konsole.

Um ***Port-Scan Optionen für die Lokale Konsole*** (siehe "***Konfigurieren von Lokale Konsole-Scaneinstellungen***" auf Seite 316)zu konfigurieren, siehe Configure Local Console Scan Settings

VERWENDUNG die Port-Scanfunktion, mit der nach ausgewählten Zielen gesucht werden kann. Die Ziele werden dann in einer Bildschirmpräsentationsansicht angezeigt. So können Sie bis zu 32 Ziele gleichzeitig überwachen.

Sie können je nach Bedarf eine Verbindung mit mehreren Zielen herstellen oder sich auf ein bestimmtes Ziel konzentrieren. Scanvorgänge können Standardziele, Blade-Server, Dominion-Schichtgeräte und KVM-Switch-Ports umfassen.

Konfigurieren Sie die Scaneinstellungen entweder über den Virtual KVM Client (VKC) oder den Active KVM Client (AKC).

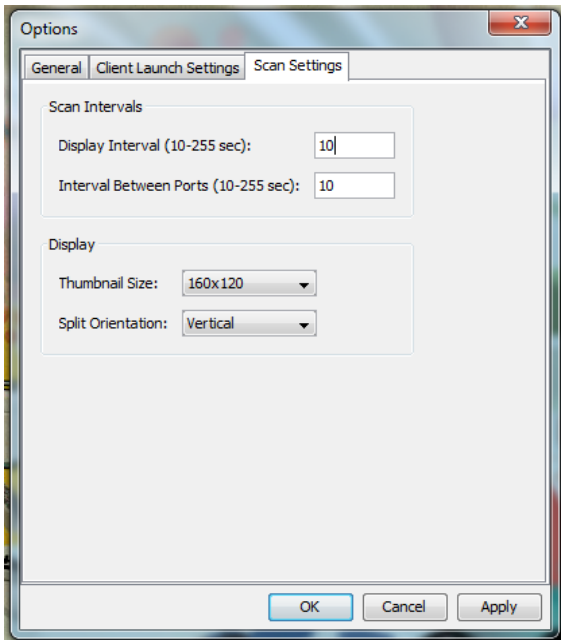
Siehe Scannen von Ports - Fernkonsole

Den Scanintervall und die Standardanzeigeoptionen legen Sie auf der Schaltfläche "Scan Settings" (Scaneinstellungen) fest.

Port-Scan konfigurieren

So legen Sie die Scaneinstellungen fest:

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Wählen Sie die Registerkarte "Scan Settings" (Scaneinstellungen) aus.
3. Geben Sie im Feld "Display Interval (10-255 sec):" (Anzeigeintervall (10-255 Sek.)) die Anzahl Sekunden ein, die das Ziel im Fokus in der Mitte des Fensters "Port Scan" (Port-Scan) angezeigt werden soll.
4. Geben Sie im Feld "Interval Between Ports (10 - 255 sec):" (Intervall zwischen Ports (10-255 Sek.)) das Intervall ein, in dem das Gerät zwischen Ports pausieren soll.
5. Ändern Sie im Abschnitt "Display" (Anzeige) die Standardanzeigeoptionen für die Größe der Miniaturansichten und die Teilung der Ausrichtung des Fensters "Port Scan" (Port-Scan).
6. Klicken Sie auf "OK".



Ansichtsoptionen

View Toolbar (Symbolleiste anzeigen)

Sie können den Virtual KVM Client mit oder ohne die Symbolleiste verwenden.

So blenden Sie die Symbolleiste ein bzw. aus:

- Wählen Sie **View > View Toolbar** (Ansicht > Symbolleiste anzeigen).

"View Status Bar" (Statusleiste anzeigen)

Standardmäßig wird die Statusleiste unten im Zielfenster angezeigt.

So blenden Sie die Statusleiste aus:

- Klicken Sie auf "View" (Ansicht) > "Status Bar" (Statusleiste), um die Option zu deaktivieren.

So stellen Sie die Statusleiste wieder her:

- Klicken Sie auf "View" (Ansicht) > "Status Bar" (Statusleiste), um die Option zu aktivieren.

Scaling (Skalieren)

Das Skalieren des Zielfensters ermöglicht die Anzeige des gesamten Inhalts des Zielserverfensters.

Dieses Feature vergrößert oder verkleinert das Zielvideobild unter Beibehaltung des Seitenverhältnisses, um es an die Fenstergröße des Virtual KVM Client anzupassen. Somit wird der gesamte Zielserver-Desktop angezeigt, und Sie müssen nicht die Bildlaufleiste verwenden.

So aktivieren bzw. deaktivieren Sie die Skalierung:

- Wählen Sie View > Scaling (Ansicht > Skalieren).

Vollbildmodus

Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver.

Die Zugriffstaste, über die Sie diesen Modus beenden können, legen Sie im Dialogfeld "Options" (Optionen) fest (siehe ***Tool Options*** (siehe "***Optionen im Menü "Tools" (Extras)***" auf Seite 272) (Tool-Optionen)).

Wenn Sie im Vollbildmodus den Mauszeiger an den oberen Bildschirmrand schieben, wird die Menüleiste für den Vollbildschirmmodus angezeigt.

Wenn die Menüleiste im Vollbildmodus sichtbar bleiben soll, aktivieren Sie die Option "Pin Menu Toolbar" (Menüsymbolleiste anheften) im Dialogfeld "Tool Options" (Tool-Optionen). Siehe ***Tool Options*** (siehe "***Optionen im Menü "Tools" (Extras)***" auf Seite 272) (Tool-Optionen).

So gelangen Sie in den Vollbildmodus:

- Wählen Sie Ansicht > Vollbild aus oder klicken Sie auf die Vollbild-Taste.  .

So beenden Sie den Vollbildmodus:

- Drücken Sie die im Dialogfeld "Options" (Optionen) konfigurierte Zugriffstaste. Standardmäßig lautet die Tastenkombination "Strg+Alt+M".

Wenn Sie immer im Vollbildmodus auf das Ziel zugreifen möchten, können Sie den Vollbildmodus als Standardeinstellung auswählen.

So aktivieren Sie den Vollbildmodus als Standardmodus:

1. Klicken Sie auf "Tools" (Extras) > "Options" (Optionen), um das Dialogfeld "Options" (Optionen) zu öffnen.
2. Wählen Sie "Enable Launch in Full Screen Mode" (Start im Vollbildmodus aktivieren), und klicken Sie auf "OK".

Virtual Media (Virtuelle Medien)

Alle KX III Modelle unterstützen virtuelle Medien. Virtuelle Medien erweitern die KVM-Funktionen. Sie ermöglichen KVM-Zielservern den Remotezugriff auf Medien auf einem Client-PC und Netzwerkdateiservern.

Mit dieser Funktion werden Medien, die auf dem Client-PC und den Netzwerkdateiservern bereitgestellt sind, im Grunde virtuell vom Zielserver bereitgestellt. Der Zielserver kann dann Lese- und Schreibzugriffe auf diese Medien durchführen, als wären die Medien physisch an den Zielserver angeschlossen.

Jeder KX III verfügt über virtuelle Medien, um Remoteverwaltungsaufgaben mithilfe einer Vielzahl von CD-, DVD-, USB-, Audiowiedergabe- und -aufnahmegeräten, internen und Remotelaufwerken und Abbildern zu ermöglichen.

Virtuelle Medien-Sitzungen sind durch 128-Bit or 256-Bit AES- oder RC4-Verschlüsselung gesichert.

Voraussetzungen für die Verwendung virtueller Medien

KX III Vorbereitungen

- Für Benutzer, die Zugriff auf virtuelle Medien benötigen, müssen Berechtigungen für das KX III Gerät eingerichtet werden, die den Zugriff auf die relevanten Ports gestatten, sowie der virtuelle Medienzugriff \[Portberechtigung "VM Access" (VM-Zugriff)] für diese Ports. Portberechtigungen werden auf Gruppenebene eingerichtet.
- Zwischen dem Gerät und dem Zielserver muss eine USB-Verbindung bestehen.
- Wenn Sie die PC-Freigabe verwenden möchten, müssen die Security Settings(Sicherheitseinstellungen) auf der Seite "Security Settings" (Sicherheitseinstellungen) aktiviert sein.**Optional**
- Sie müssen das richtige USB-Profil für den KVM-Zielserver auswählen, zu dem Sie eine Verbindung herstellen.

Remote-PC

- Für bestimmte virtuelle Medienoptionen sind Administratorrechte auf dem Remote-PC erforderlich (z. B. Umleitung ganzer Laufwerke).

Hinweis: Wenn Sie Windows Vista or Windows 7 verwenden, deaktivieren Sie "User Account Control" (Benutzerkontensteuerung), oder wählen Sie beim Start von Internet Explorer "Run as Administrator" (Als Administrator ausführen) aus. Klicken Sie dazu auf das Menü "Start", klicken Sie mit der rechten Maustaste auf "Internet Explorer", und wählen Sie "Run as Administrator" (Als Administrator ausführen) aus.

Zielserver

- KVM-Zielserver müssen über USB angeschlossene Laufwerke unterstützen.
- USB 2.0-Ports sind schneller und daher vorzuziehen.

CIM erfoderlich für Virtuelle Medien

Für die Verwendung von virtuellen Medien müssen Sie eine der folgenden CIM verwenden:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Der schwarze Anschluss am DVUSB CIM wird zum Anschließen von Maus und Tastatur verwendet. Der graue Anschluss wird für virtuelle Medien verwendet.

Achten Sie darauf, dass immer beide Anschlüsse des CIM mit dem Gerät verbunden sind. Es ist möglich, dass das Gerät nicht ordnungsgemäß funktioniert, wenn nicht alle Stecker an den Zielserver angeschlossen sind.

Installieren von lokalen Laufwerken

Mit dieser Option installieren Sie ein gesamtes Laufwerk. Das gesamte Festplattenlaufwerk wird auf dem Zielserver virtuell installiert.

Verwenden Sie diese Option nur für Festplatten und externe Laufwerke. Netzwerklaufwerke, CD-ROM- oder DVD-ROM-Laufwerke sind nicht enthalten.

Notiz zum Installieren von lokalen Laufwerken

KVM-Zielserver unter dem Betriebssystem Windows XP® kann möglicherweise keine neuen Massenspeicherverbindungen akzeptieren, nachdem eine NTFS-formatierte Partition (z. B. das lokale Laufwerk C) an sie umgeleitet wurde.

Schließen Sie in diesem Fall die Remotekonsole, und stellen Sie erneut eine Verbindung her, bevor Sie ein weiteres virtuelles Mediengerät umleiten. Wenn andere Benutzer mit demselben Zielserver verbunden sind, müssen auch sie diese Verbindung trennen.

Unterstützte Aufgaben Via Virtuelle Medien

Virtuelle Medien bieten die Möglichkeit, Aufgaben extern zu erledigen. Dazu zählen:

- Übertragen von Dateien
- Durchführen von Diagnosen
- Installieren oder Reparieren von Anwendungen
- Vollständiges Installieren des Betriebssystems
- Aufnehmen und Wiedergeben von digitalen Audiodateien

Unterstützte Virtuelle Medientypen

Für Windows®, Mac® und Linux™-Clients werden die folgenden virtuellen Medientypen unterstützt:

- Interne und externe Laufwerke
- Interne und per USB angeschlossene CD- und DVD-Laufwerke
- USB-Massenspeichergeräte
- PC-Festplatte
- ISO-Abbilder (Datenträgerabbilder)
- Digitale Audiogeräte*

Hinweis: ISO9660 wird standardmäßig von Raritan unterstützt. Andere ISO-Standards können jedoch ebenfalls verwendet werden.

Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist

Der Lese-/Schreibzugriff auf virtuelle Medien ist in den folgenden Situationen nicht verfügbar:

- Für Linux® und Mac® Clients
- Wenn das Laufwerk schreibgeschützt ist
- Wenn der Benutzer nicht über eine Lese-/Schreibberechtigung verfügt.
  - Unter Port Permission (Port-Berechtigung) ist für Access (Zugriff) die Einstellung None (Kein) oder View (Anzeigen) ausgewählt.
  - Unter Port Permission (Port-Berechtigung) ist für VM Access (VM-Zugriff) die Einstellung Read-Only (Schreibgeschützt) oder Deny (Ablehnen) ausgewählt.

Unterstützte Virtuelle Medien-Betriebssysteme

Die folgenden Client-Betriebssysteme werden unterstützt:

- Windows®-7 Betriebssystem
- Windows 8 Betriebssystem
- Windows XP® Betriebssystem
- openSUSE® 11.4 Celadon (x86_64)
- Fedora® 18
- RHEL® 6.4
- OSX Mountain Lion® 10.7 (und höher)
- Solaris® 10

Der Active KVM Client (AKC) kann verwendet werden, um Medieniarten zu montieren aber nur für Windows-Betriebssysteme.

Anzahl der unterstützten Map Virtual Media Drive (Virtuelle Medienlaufwerke)

Mit dem Feature für virtuelle Medien können Sie bis zu zwei Laufwerke (verschiedenen Typs) mounten, die durch das aktuell dem Zielgerät zugeordnete USB-Profil unterstützt werden. Diese Laufwerke sind während der KVM-Sitzung zugänglich.

Sie können beispielsweise eine bestimmte CD-ROM installieren, verwenden und nach Fertigstellung Ihrer Arbeit wieder trennen. Der virtuelle Medienkanal für CD-ROMs bleibt jedoch offen, sodass Sie eine andere CD-ROM virtuell installieren können. Diese virtuellen Medienkanäle bleiben offen, bis die KVM-Sitzung geschlossen wird (vorausgesetzt, sie werden vom USB-Profil unterstützt).

Um das virtuelle Medium zu verwenden, schließen Sie es an den Client-PC oder Netzwerkdateiserver an, auf den Sie über den Zielserver zugreifen möchten.

Dieser Schritt muss nicht als erster erfolgen, jedoch bevor Sie versuchen, auf das Medium zuzugreifen.

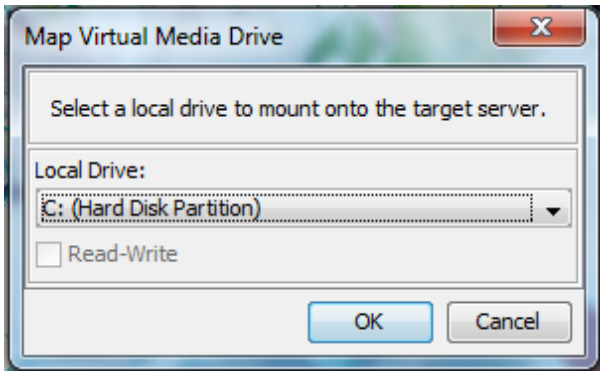
Trennen und Anschließen vom Virtuellen Medien

So greifen Sie auf ein Virtuelles Medienlaufwerk auf dem Client-Computer zu

So greifen Sie auf ein Virtuelles Medien Laufwerk auf dem Client-Computer zu:

1. Wählen Sie im Virtual KVM Client Virtual Media > Connect Drive

   oder klicken Sie auf die Connect Drive... Taste  . Das Dialogfeld Map Virtual Media Drive (Virtuelles Medienlaufwerk zuordnen) wird angezeigt.



2. Wählen Sie das entsprechende Laufwerk in der Dropdown-Liste Local Drive (Lokales Laufwerk) aus.

   Für den Lese- und Schreibzugriff müssen Sie das Kontrollkästchen "Read-Write" (Lese-/Schreibzugriff) aktivieren.

   Diese Option steht nur für Wechsellaufwerke zur Verfügung. Weitere Informationen finden Sie unter Fälle, in denen ***Lese-/Schreibzugriff nicht verfügbar ist*** (siehe "***Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist***" auf Seite 283).

   Bei dieser Option können Sie Daten auf dem angeschlossenen USB-Datenträger lesen und schreiben.

   WARNUNG: Den Lese-/Schreibzugriff zu aktivieren kann gefährlich sein! Wenn mehrere Einheiten gleichzeitig auf dasselbe Laufwerk zugreifen, kann dies zu Datenbeschädigungen führen. Sollten Sie den Schreibzugriff nicht benötigen, deaktivieren Sie dieses Kontrollkästchen.

3. Klicken Sie auf OK. Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern

Mit dieser Option installieren Sie CD-ROM-, DVD-ROM- und ISO-Abbilder.

Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

So greifen Sie auf ein CD-ROM-, DVD-ROM- oder ISO-Abbild zu:

1. Wählen Sie im Virtual KVM Client Virtual Media > CD-ROM/ISO Bild verbinden, oder klicken Sie auf die CD-ROM/ISO Verbinden Taste  . Das Dialogfeld "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) wird angezeigt.
2. Gehen Sie bei internen und externen CD-ROM- und DVD-ROM-Laufwerken folgendermaßen vor:
   a. Wählen Sie die Option "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk).
   b. Wählen Sie das entsprechende Laufwerk in der Dropdown-Liste "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk) aus. Diese Liste enthält alle verfügbaren internen und externen CD- und DVD-Laufwerksnamen.
   c. Klicken Sie auf/// ///Connect (Verbinden).
3. Gehen Sie bei ISO-Abbildern folgendermaßen vor:
   a. Wählen Sie die Option "ISO Image" (ISO-Abbild). Mit dieser Option greifen Sie auf ein Laufwerkabbild einer CD, DVD oder Festplatte zu. Nur das ISO-Format wird unterstützt.
   b. Klicken Sie auf Durchsuchen.
   c. Navigieren Sie zu dem Pfad des gewünschten Laufwerkabbilds, und klicken Sie auf Open (Öffnen). Der Pfad wird in das Feld "Image Path" (Abbildpfad) geladen.
   d. Klicken Sie auf/// ///Connect (Verbinden).
4. Gehen Sie bei Remote-ISO-Abbildern auf einem Dateiserver folgendermaßen vor:
   a. Wählen Sie die Option "Remote Server ISO Image" (ISO-Abbild auf Remoteserver).
   b. Wählen Sie in der Dropdown-Liste einen Hostnamen und ein Abbild aus. Zur Verfügung stehen die Dateiserver und Abbildpfade, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben. Die Dropdown-Liste enthält nur Elemente, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben.

c. File Server Username (Dateiserver-Benutzername) – Der für den Zugriff auf den Dateiserver erforderliche Benutzername. Der Name darf den Domänennamen, wie z. B. meinedomäne/Benutzername, enthalten.

d. File Server Password (Dateiserver-Kennwort) – Das für den Zugriff auf den Dateiserver erforderliche Kennwort (Eingabe erfolgt verdeckt).

e. Klicken Sie auf/// ///Connect (Verbinden).

Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

Hinweis: Wenn Sie Dateien auf einem Linux® Ziel bearbeiten, verwenden Sie den Befehl "Linux Sync" (Linux-Synchronisierung), nachdem die Dateien mithilfe eines virtuellen Mediums kopiert wurden, um die kopierten Dateien anzuzeigen. Die Dateien werden möglicherweise erst angezeigt, nachdem die Synchronisierung durchgeführt wurde.

Hinweis: Wenn Sie mit dem Windows 7® Betriebssystem® arbeiten, werden Wechseldatenträger nicht standardmäßig im Windows-Ordner "Arbeitsplatz" angezeigt, sobald Sie ein lokales CD-/DVD-Laufwerk oder ein lokales oder Remote-ISO-Abbild montieren. Um das lokale CD-/DVD-Laufwerk oder das lokale oder Remote-ISO-Abbild in diesem Ordner anzuzeigen, wählen Sie "Extras“ > "Ordneroptionen" > "Ansicht" aus und deaktivieren Sie die Option "Leere Laufwerke im Ordner "Computer" ausblenden".

Hinweis: Aufgrund von technischen Einschränkungen der Drittanbieter-Software können Sie bei Verwendung einer IPv6-Adresse nicht über virtuelle Medien auf ein Remote-ISO-Abbild zugreifen.

Trennen von Virtuellen Medienlaufwerken

So trennen Sie virtuelle Medienlaufwerke:

- Wählen Sie für lokale Laufwerke Virtual Media Disconnect Drive (Virtuelle Medien Laufwerk trennen).
- Wählen Sie für CD-ROM-, DVD-ROM- und ISO-Abbilder Virtual Media Disconnect CD-ROM/ISO Image (Virtuelle Medien CD-ROM-/ISO-Abbild trennen).

Hinweis: Anstatt das virtuelle Medium über den Befehl "Disconnect" (Trennen) zu trennen, können Sie auch einfach die KVM-Verbindung beenden.

Virtuelle Medien in einer Windows XP-Umgebung

Wenn Sie den Virtual KVM Client oder Active KVM Client in einer Windows® XP-Umgebung ausführen, Benutzer müssen über Administratorrechte verfügen, um auf andere Medientypen als CD-ROM-Verbindungen, ISO-Dateien und ISO-Abbilder zugreifen zu können.

Virtuelle Medien in einer Linux-Umgebung

Aktive Systempartitionen

Sie können keine aktiven Systempartitionen von einem Linux-Client bereitstellen.

Vor dem Herstellen einer virtuellen Medienverbindung muss die Bereitstellung von Linux Ext3/4-Laufwerkpartitionen mit dem Befehl "umount /dev/<device label>" aufgehoben werden.

Laufwerkpartitionen

Die folgenden Einschränkungen für Laufwerkpartitionen gelten für verschiedene Betriebssysteme:

- Windows® und Mac-Ziele können keine unter Linux formatierten Partitionen lesen.
- Windows und Linux können keine unter Mac formatierten Partitionen lesen.
- Von Linux werden nur Windows FAT-Partitionen unterstützt.

Erforderliche Stammbenutzerberechtigung

Ihre virtuelle Medienverbindung wird ggf. beendet, wenn Sie ein CD-ROM-Laufwerk von einem Linux-Client auf einem Ziel bereitstellen und anschließend die Bereitstellung des CD-ROM-Laufwerks aufheben.

Um diese Probleme zu vermeiden, melden Sie sich als Stammbenutzer an.

Virtuelle Medien in einer Mac-Umgebung

Aktive Systempartition

Sie können keine virtuellen Medien für aktive Systempartitionen für einen Mac-Client verwenden.

Laufwerkpartitionen

Die folgenden Einschränkungen für Laufwerkpartitionen gelten für verschiedene Betriebssysteme:

- Windows® und Mac-Ziele können keine unter Linux formatierten Partitionen lesen.
- Windows kann keine unter Mac formatierten Partitionen lesen.
- Mac unterstützt Windows FAT und NTFS.
- Mac-Benutzer müssen alle bereits installierten Geräte deinstallieren, um eine Verbindung mit einem Zielserver herzustellen. Verwenden Sie den Befehl "diskutil umount /dev/disk1s1", um das Gerät zu deinstallieren, und "diskutil mount /dev/disk1s1", um es erneut zu installieren.

Dateiserver-Setup für virtuelle Medien (nur für Dateiserver-ISO-Abbilder)

Dieses Feature ist nur für den Zugriff auf Dateiserver-ISO-Abbilder über virtuelle Medien erforderlich. Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

Hinweis: Der Dateiserver muss SMB/CIFS unterstützen.

Legen Sie auf der Seite "File Server Setup" (Dateiserver-Setup) der Remotekonsole die Dateiserver und Abbildpfade fest, auf die Sie über virtuelle Medien zugreifen möchten. Hier angegebene Dateiserver-ISO-Abbilder stehen im Dialogfenster "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) unter "Remote Server ISO Image" (ISO-Abbild auf Remoteserver) in den Dropdownlisten "Hostname" und "Image" (Abbild) zur Auswahl. Siehe ***Mounten von CD-ROM-/DVD-ROM-/ISO-Abbildern*** (siehe "***Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern***" auf Seite 286).

So legen Sie Dateiserver-ISO-Abbilder für den virtuellen Medienzugriff fest:

1. Wählen Sie in der Remotekonsole "Virtual Media" (Virtuelle Medien) aus. Die Seite "File Server Setup" (Dateiserver-Setup) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Selected" (Ausgewählt) für alle Medien, die als virtuelle Medien zugänglich sein sollen.
3. Geben Sie Informationen zu den Dateiserver-ISO-Abbildern ein, auf die Sie zugreifen möchten:
   - IP Address/Host Name (IP-Adresse/Hostname) – Hostname oder IP-Adresse des Dateiservers.

- Image Path (Abbildpfad) – Vollständiger Pfad zum Speicherort des ISO-Abbildes. Zum Beispiel /sharename0/path0/image0.iso, \sharename1\path1\image1.iso usw.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

4. Klicken Sie auf Save. Alle hier angegebenen Medien stehen nun im Dialogfeld Map Virtual Media CD/ISO Image (CD-/ISO-Abbild als virtuelles Medium zuordnen) zur Auswahl.

Hinweis: Wenn Sie eine Verbindung zu einem Windows 2003® Server herstellen und versuchen, ein ISO-Abbild vom Server zu laden, ist es möglich, dass Sie die Fehlermeldung "Virtual Media mounting on port failed“ erscheint. Unable to connect to the file server or incorrect File Server username and password". (Installation der virtuellen Medien auf Port fehlgeschlagen. Verbindung mit Dateiserver konnte nicht hergestellt werden oder falsches Kennwort bzw. falschen Benutzernamen für Dateiserver verwendet.) angezeigt bekommen. Falls dies eintritt, deaktivieren Sie unter den Richtlinien für den Domänen-Controller die Option "Microsoft Network Server: Digitally Sign Communications" (Microsoft-Netzwerk [Server]: Kommunikation digital signieren).

Smart Cards

Verwenden des KX III, können Sie ein Smart Card-Lesegerät auf einem Zielserver installieren, um die Smart Card-Authentifizierung sowie die dazugehörigen Anwendungen zu unterstützen.

Eine Liste der unterstützten Smart Cards, Smart Card-Lesegeräte und Informationen zu zusätzlichen Systemanforderungen finden Sie unter unterstützte und nicht unterstützte ***Smart Card-Lesegeräte und unter minimale Smart Card Systemanforderungen*** (siehe "***Mindestanforderungen an Smart Cards, CIMS und Unterstützte und Nicht unterstützte Smart Card-Lesegeräte***" auf Seite 291).

Hinweis: Das USB-Smart Card-Token (eToken NG-OTP) wird nur vom Remoteclient unterstützt.

Das Mounten von Smart Card-Lesegeräten wird auch von der lokalen Konsole unterstützt.

Siehe ***Smart Card-Zugriff von der lokalen Konsole in der Hilfe Ihres Dominion-Geräts*** (siehe "***Smart Card-Zugriff von der lokalen Konsole***" auf Seite 318).

Mindestanforderungen an Smart Cards, CIMS und Unterstützte und Nicht unterstützte Smart Card-Lesegeräte

Bevor Sie ein Smart Card-Lesegerät verwenden, überprüfen Sie das Folgende:

- ***Mindestanforderungen an Smart Cards*** (auf Seite 356)
- ***Spezifikationen der unterstützten Computer Interface Modules (CIMs)*** (auf Seite 349)
- Unterstützte und nicht unterstützte Smart Card-Lesegeräte

Smart Card-Lesegerät beim Zugriff authenzifizieren

Beim Remote-Zugriff auf den Server haben Sie die Möglichkeit, ein angeschlossenes Smart Card-Lesegerät auszuwählen und auf dem Server zu montieren.

Der Zielserver verwendet Smart Card-Authentifizierung. Diese Art der Authentifizierung wird nicht beim Anmelden am Gerät verwendet. Änderungen bezüglich der Smart Card-PIN und den Anmeldeinformationen erfordern daher keine Aktualisierungen der Gerätekonten.

PC-Freigabemodus Datenschutzeinstellungen Smart Cards

Wenn auf dem Gerät der Modus "PC-Share" (PC-Freigabe) aktiviert ist, können mehrere Benutzer gleichzeitig auf den Zielserver zugreifen.

Ist jedoch ein Smart Card-Lesegerät an das Ziel angeschlossen, ist, unabhängig vom Modus "PC-Share" (PC-Freigabe), nur der exklusive Zugriff möglich.

Zusätzlich ist das Smart Card-Lesegerät während einer gemeinsamen Sitzung deaktiviert, bis der exklusive Zugriff auf den Server verfügbar wird.

Smart Card-Lesegeräte Erkannt

Nach dem Herstellen einer KVM-Verbindung zum Zielserver werden ein Smart Card-Menü und eine Smart Card-Schaltfläche in VKC und AKC angezeigt.

Nachdem das Menü geöffnet oder auf die Smart Card-Schaltfläche geklickt wurde, werden die Smart Card-Lesegeräte angezeigt, die als an den Remoteclient angeschlossen erkannt werden.

In diesem Dialogfeld können Sie weitere Smart Card-Lesegeräte hinzufügen, die Liste der an das Ziel angeschlossenen Smart Card-Lesegeräte aktualisieren und Smart Card-Lesegeräte entfernen.

Sie können auch eine Smart Card entfernen oder wieder einführen. Diese Funktion kann verwendet werden, um das Betriebssystem eines Zielservers zu benachrichtigen, das das Entfernen und Wiedereinführen erfordert, um das entsprechende Dialogfeld für die Anmeldung anzuzeigen. Mithilfe dieser Funktion kann die Benachrichtigung an ein individuelles Ziel gesendet werden, ohne andere KVM-Sitzungen zu beeinträchtigen.

Montieren eines Smart Card-Lesegerätes

Nach der Installation des Kartenlesegeräts und der Smart Card auf dem Zielserver, funktioniert der Server so, als wären das Kartenlesegerät und die Smart Card direkt am Server angeschlossen.

Abhängig von den Einstellungen in den Richtlinien zur Entfernung der Karte im Betriebssystem des Zielservers wird beim Entfernen der Smart Card oder des Smart Card-Lesegeräts die Benutzersitzung gesperrt, oder Sie werden abgemeldet.

Ist die KVM-Sitzung unterbrochen, weil Sie beendet wurde oder Sie auf ein neues Ziel umgeschaltet haben, wird das Smart Card-Kartenlesegerät automatisch vom Zielserver deinstalliert.

So montieren Sie ein Smart Card-Lesegerät vom VKC oder AKC:

1. Klicken Sie auf das Menü "Smart Card", und wählen Sie anschließend "Smart Card Reader" (Smart Card-Lesegerät) aus. Sie können auch auf die Schaltfläche "Smart Card“  in der Symbolleiste klicken.
2. Wählen Sie im Dialogfeld "Select Smart Card Reader" (Smart Card-Lesegerät auswählen) das Smart Card-Lesegerät aus.
3. Klicken Sie auf "Mount".

4. Ein Dialogfeld wird geöffnet, in dem der Fortschritt angezeigt wird. Aktivieren Sie das Kontrollkästchen "Mount selected card reader automatically on connection to targets" (Ausgewähltes Kartenlesegerät bei Verbindung zu Zielen automatisch mounten), um das Smart Card-Lesegerät automatisch zu installieren, wenn Sie das nächste Mal eine Verbindung zu einem Ziel herstellen. Klicken Sie auf "OK", um den Installationsvorgang zu starten.

Smart Card-Lesegerät Aktualisieren

So aktualisieren Sie die Smart Card im Dialogfeld "Select Smart Card Reader" (Smart Card-Lesegerät auswählen):

- Klicken Sie auf "Refresh List" (Liste aktualisieren), wenn Sie ein neues Smart Card-Lesegerät an den Cient-PC angeschlossen haben.

So senden Sie Benachrichtigungen über das Entfernen und Wiedereinführen einer Smart Card an das Ziel:

So senden Sie Benachrichtigungen über das Entfernen und Wiedereinführen einer Smart Card an das Ziel:

- Wählen Sie das aktuell installierte Smart Card-Lesegerät aus, und klicken Sie auf die Schaltfläche "Remove/Reinsert" (Entfernen/Wiedereinführen).

So entfernen Sie ein Smart Card-Lesegerät

So unmounten Sie ein Smart Card-Lesegerät:

- Wählen Sie das Smart Card-Lesegerät aus, das Sie unmouten möchten, und klicken Sie auf die Schaltfläche "Unmount".

Digitale Audiogeräte

KX III unterstützt unterstützt bidirektionale End-to-End-Audioverbindungen für digitale Audiowiedergabe- und -aufnahmegeräte von einem Remoteclient zu einem Zielserver.

Der Zugriff auf die Audiogeräte erfolgt über eine USB-Verbindung.

Aktuelle Geräte-Firmware ist erforderlich.

Eines der folgenden CIMS muss verwendet werden:

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Windows®, Linux® und Mac® Betriebssysteme werden unterstützt. Virtual KVM Client (VKC) und Active KVM Client (AKC) unterstützt die Verbindung zu den Audiogeräten.

Hinweis: Da Audio-CDs nicht von virtuellen Medien unterstützt werden, können sie nicht mit der Audiofunktion verwendet werden.

Vor der Verwendung der Audiofunktion wird empfohlen, die audiobezogenen Informationen in den folgenden Abschnitten der Hilfe zu lesen:

- ***Unterstützte Formate für Audiogeräte*** (auf Seite 294)
- ***Empfehlungen für duale Portvideofunktion*** (auf Seite 231)
- ***Unterstützte Mausmodi*** (siehe "***Duale Videoportgruppen Unterstützte Mausmodi***" auf Seite 231)
- ***CIMs, die für die Unterstützung der dualen Videofunktion erforderlich sind*** (auf Seite 232)
- Wichtige Hinweise,**, *Audio*** (auf Seite 388)

Unterstützte Formate für Audiogeräte

KX III unterstützt jeweils ein Wiedergabegerät und ein Aufnahmegerät auf einem Ziel. Folgende Formate für Audiogeräte werden unterstützt:

- Stereo, 16 Bit, 44,1 K
- Mono, 16 Bit, 44,1 K
- Stereo, 16 Bit, 22,05 K
- Mono, 16 Bit, 22,05 K
- Stereo, 16 Bit, 11,025 K
- Mono, 16 Bit, 11,025 K

Empfehlungen und Anforderungen für die Audiowiedergabe und -aufnahme

Audiopegel

- Legen Sie den Zielaudiopegel auf eine Einstellung im mittleren Bereich fest.

  Auf einem Windows®Client legen Sie den Audiopegel beispielsweise auf 50 oder niedriger fest.

Diese Einstellung muss über das Wiedergabe- oder Aufnahmeaudiogerät und nicht über die Audiogerätesteuerung des Clients konfiguriert werden.

Empfehlungen für Audioverbindungen bei aktiviertem Modus "PC Share" (PC-Freigabe)

Wenn Sie die Audiofunktion bei aktiviertem Modus "PC Share" (PC-Freigabe) verwenden, werden die Audiowiedergabe und -aufnahme unterbrochen, wenn ein zusätzliches Audiogerät an das Zielgerät angeschlossen wird.

Beispielsweise schließt Benutzer A ein Wiedergabegerät an Ziel1 an und führt eine Anwendung für die Audiowiedergabe aus. Anschließend schließt Benutzer B ein Aufnahmegerät an dasselbe Ziel an. Die Wiedergabesitzung von Benutzer A wird unterbrochen, und die Audioanwendung muss möglicherweise neu gestartet werden.

Die Unterbrechung erfolgt, weil das USB-Gerät mit der neuen Gerätekonfiguration eine neue Nummer erhält.

Es kann einige Zeit dauern, bis ein Treiber für das neue Gerät auf dem Zielgerät installiert ist.

Audioanwendungen können die Wiedergabe vollständig beenden, den nächsten Titel aufrufen oder einfach die Wiedergabe fortsetzen.

Das genaue Verhalten hängt davon ab, wie die Audioanwendung das Trennen/erneute Anschließen handhabt.

Anforderungen an die Bandbreite

Die folgende Tabelle gibt Aufschluss über die Bandbreitenanforderungen für Audiowiedergabe und -aufnahme zum Übertragen von Audiosignalen im Rahmen der einzelnen ausgewählten Formate.

Audioformat	Anforderung an die Netzwerkbandbreite
44,1 KHz, 16 Bit Stereo	176 KB/s
44,1 KHz, 16 Bit Mono	88.2 KB/s

Audioformat	Anforderung an die Netzwerkbandbreite
2,05 KHz, 16 Bit Stereo	88.2 KB/s
22,05 KHz, 16 Bit Mono	44.1 KB/s
11,025 KHz, 16 Bit Stereo	44.1 KB/s
11,025 KHz, 16 Bit Mono	Audio 22,05 KB/s

In der Praxis ist die Bandbreite zum Verbinden von Audiogeräten mit einem Ziel höher. Der Grund sind die Tastatur- und Videodaten, die beim Öffnen und Verwenden einer Audioanwendung auf dem Ziel in Anspruch genommen werden.

Als allgemeine Empfehlung gilt, dass mindestens 1,5 MB für die Verbindung verfügbar sein müssen, bevor die Wiedergabe oder Aufnahme erfolgt.

Videoinhalte in hoher Qualität mit Verbindungen ganz in Farbe und hohen Auflösungen des Zielbildschirms nehmen jedoch weitaus mehr Bandbreite in Anspruch und wirken sich erheblich auf die Audioqualität aus.

Um die Qualitätsverschlechterung zu verringern, gibt es eine Reihe von empfohlenen Client-Einstellungen, die die Auswirkung auf die Video- und Audioqualität bei niedrigeren Bandbreiten reduzieren:

- Verbinden Sie die Audiowiedergabe mit den Formaten niedrigerer Qualität. Die Auswirkung der Inanspruchnahme von Bandbreite durch Video ist bei Verbindungen mit 11 K deutlich weniger ausgeprägt als mit 44 K.
- Legen Sie den Wert für die Verbindungsgeschwindigkeit unter "Connection Properties" (Verbindungseigenschaften) entsprechend der Client-zu-Server-Verbindung fest.
- Legen Sie unter "Connection Properties" (Verbindungseigenschaften) die Farbtiefe auf einen möglichst niedrigen Wert fest. Durch Reduzieren der Farbtiefe auf 8-Bit-Farbe wird deutlich weniger Bandbreite in Anspruch genommen.
- Set Smoothing (Glättung, to High. Dies verbessert das Aussehen des Zielgerätbbildes, da dadurch das Videorauschen verringert wird.
- Legen Sie den Rauschfilter unter "Video Settings" (Videoeinstellungen) auf 7 (höchster Wert) fest, sodass für die Änderungen am Zielbildschirm eine niedrigere Bandbreite verwendet wird.

Speichern der Audioeinstellungen

Die Einstellungen für Audiogeräte werden pro KX III Gerät übernommen.

Nachdem die Einstellungen für das Audiogerät konfiguriert und auf KX III gespeichert wurden, werden diese Einstellungen für dieses Gerät verwendet.

Sie können beispielsweise ein Windows® -Audiogerät konfigurieren, um ein Stereoformat mit 16 Bit, 44,1 K zu verwenden.

Wenn Sie die Verbindung zu verschiedenen Zielen herstellen und dieses Windows-Audiogerät verwenden, wird das Stereoformat mit 16 Bit, 44,1 K auf jedem Zielserver angewendet.

Für Wiedergabe- und Aufnahmegeräte werden die für das Gerät verwendeten Einstellungen für Gerätetyp, Geräteformat und Puffer gespeichert.

Informationen zum Anschließen und Konfigurieren eines Audiogeräts finden Sie unter ***Anschließen und Abschalten eines digitalen Audiogeräts*** (siehe "***Anschließen und Entfernen eines digitalen Audiogeräts***" auf Seite 299), und Informationen zu den Zwischenspeichereinstellungen des Audiogeräts finden Sie unter Anpassen der Zwischenspeichergröße für Aufnahme und Wiedergabe (Audioeinstellungen).

Wenn Sie die Audiofunktion im Modus "PC Share" (PC-Freigabe) und "VM Share" (VM-Freigabe) verwenden, damit mehrere Benutzer gleichzeitig auf dasselbe Audiogerät auf dem Ziel zugreifen können, werden die Audiogeräteeinstellungen des Benutzers, der die Sitzung initiiert, für alle Benutzer übernommen, die der Sitzung beitreten.

Wenn ein Benutzer einer Audiositzung beitritt, werden die Einstellungen des Zielgeräts verwendet. Siehe ***Verbinden mit mehreren Zielen von einem Remoteclient*** (auf Seite 298).

Verbinden mit mehreren Zielen von einem Remoteclient

Sie können Audio von einem Remoteclient gleichzeitig auf maximal vier (4) Zielservern wiedergeben.

Weitere Informationen zum Anschließen von Audiogeräten finden Sie unter ***Anschließen und Entfernen eines digitalen Audiogeräts*** (auf Seite 299).

Ein Lautsprechersymbol  wird am Ende der Statusleiste im Client-Fenster angezeigt. Wenn kein Audio verwendet wird, ist dieses Symbol abgeblendet. Wenn das Lautsprechersymbol und das Mikrofonsymbol  in der Statusleiste angezeigt werden, wird die Sitzung beim Streamen aufgezeichnet.

Hinweis: Wenn eine Audiositzung im Gange ist, müssen Sie sicherstellen, dass die Sitzung aktiv bleibt, oder das Zeitlimit für die Inaktivität von KX III ändern, sodass die Audiositzung nicht beendet wird.

Betriebssystem Audio Playback Unterstützung

In der folgenden Tabelle sehen Sie, welcher Raritan-Client die Audiowiedergabe/-aufnahme für die verschiedenen Betriebssysteme unterstützt:

Betriebssystem	Unterstützung der Audiowiedergabe und -aufnahme:
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC)
Linux®	• Virtual KVM Client (VKC)
Mac®	• Virtual KVM Client (VKC)

Anschließen und Entfernen eines digitalen Audiogeräts

Die Einstellungen für Audiogeräte werden pro KX III Gerät übernommen.

Nachdem die Einstellungen für das Audiogerät konfiguriert und auf KX III gespeichert wurden, werden diese Einstellungen für dieses Gerät verwendet.

Weitere Informationen finden Sie unter ***Speichern der Audioeinstellungen*** (auf Seite 297).

Hinweis: Wenn Sie die Audiofunktion verwenden, während der Modus "PC Share" (PC-Freigabe) und "VM Share" (VM-Freigabe) ausgeführt wird, lesen Sie bitte die wichtigen **Hinweise unter Empfehlungen und Anforderungen für die Audiowiedergabe und -aufnahme** *(siehe "***Empfehlungen und Anforderungen für die Audiowiedergabe und -aufnahme***" auf Seite 295). Siehe auch* **Verbinden mit mehreren Zielen von einem Remoteclient** *(auf Seite 298).*

Digitale Audiogeräte Anschließen

So stellen Sie die Verbindung zu einem Audiogerät her:

1. Verbinden Sie das Audiogerät mit dem Remoteclient-PC, bevor Sie die Browserverbindung mit dem KX III.
2. Stellen Sie auf der Seite "Port Access" (Portzugriff) eine Verbindung zum Zielserver her.
3. Klicken Sie anschließend auf das Audio-Symbol  in der Symbolleiste klicken.

   Das Dialogfeld "Connect Audio Device" (Audiogerät verbinden) wird angezeigt. Eine Liste der verfügbaren, an den Remoteclient-PC angeschlossenen Audiogeräte wird angezeigt.

   Hinweis: Sind keine verfügbaren Audiogeräte mit dem Remote-Client-PC verbunden, wird das Audio-Symbol abgeblendet dargestellt.
4. Aktivieren Sie das Kontrollkästchen "Connect Playback Device" (Wiedergabegerät verbinden), wenn Sie ein Wiedergabegerät anschließen.
5. Wählen Sie das zu verbindende Gerät in der Dropdownliste aus.
6. Wählen Sie das Audioformat für das Wiedergabegerät in der Dropdownliste "Format" (Format)

   Hinweis: Wählen Sie das gewünschte Format entsprechend der verfügbaren Netzwerkbandbreite aus. Formate mit niedrigeren Abtastfrequenzen nehmen weniger Bandbreite in Anspruch und sind gegenüber Netzwerküberlastungen ggf. toleranter.

7. Aktivieren Sie das Kontrollkästchen "Connect Recording Device" (Aufnahmegerät verbinden), wenn Sie ein Aufnahmegerät anschließen.

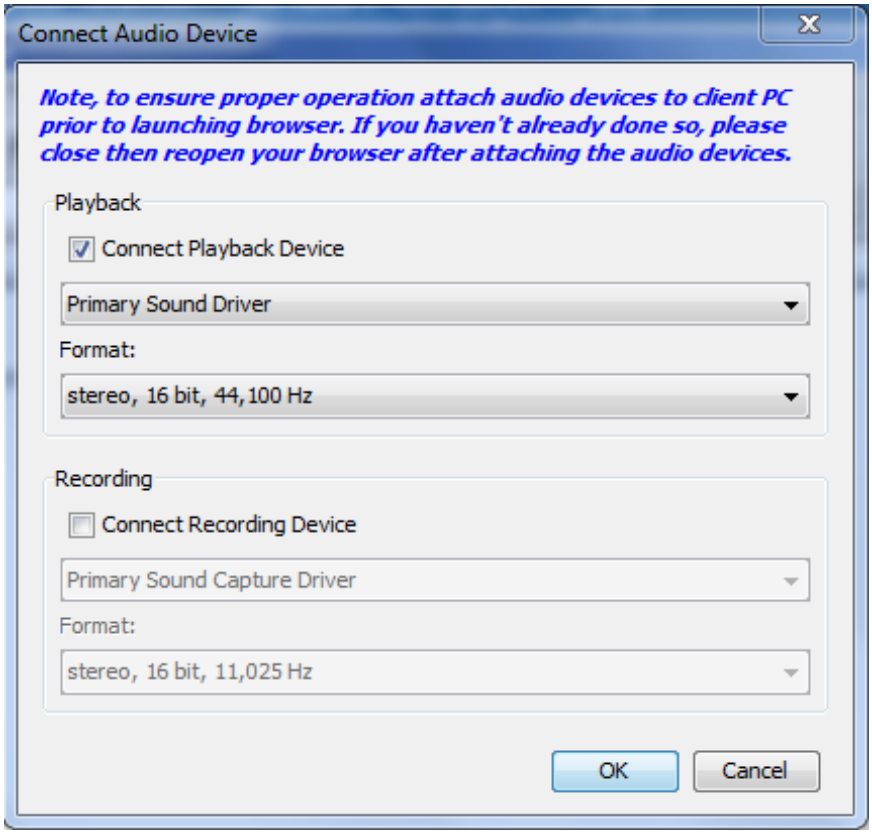
   Hinweis: Die in der Dropdownliste "Connect Recording Device" (Aufnahmegerät verbinden) aufgeführten Gerätenamen werden für Java-Clients auf maximal 30 Zeichen gekürzt.

8. Wählen Sie das zu verbindende Gerät in der Dropdownliste aus.
9. Wählen Sie das Audioformat für das Aufnahmegerät in der Dropdownliste "Format" (Format)
10. Klicken Sie auf OK. Sobald die Audioverbindung hergestellt wurde, wird eine Bestätigungsmeldung angezeigt. Klicken Sie auf OK.

    Konnte keine Verbindung hergestellt werden, wird eine Fehlermeldung angezeigt.

    Nach dem Herstellen der Audioverbindung wird das Menü "Audio" in "Disconnect Audio" (Audio trennen) geändert. Darüber hinaus werden die Einstellungen für das Audiogerät gespeichert und für das Audiogerät angewendet.

Ein Lautsprechersymbol wird am Ende der Statusleiste im Client-Fenster angezeigt. Wenn kein Audio verwendet wird, ist dieses Symbol abgeblendet. Wenn das Lautsprechersymbol und das Mikrofonsymbol in der Statusleiste angezeigt werden, wird die Sitzung beim Streamen aufgezeichnet.



So schalten Sie das Audiogerät aus

So trennen Sie das Audiogerät:

- Klicken Sie auf das Audio-Symbol in der Symbolleiste, und wählen Sie "OK", wenn Sie zur Bestätigung der Abschaltung aufgefordert werden. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf OK.

Anpassen der Puffergröße für Aufnahme und Wiedergabe (Audioeinstellungen)

Nachdem ein Audiogerät angeschlossen wurde, können Sie die Puffergröße für die Aufnahme und Wiedergabe entsprechend anpassen.

Mit dieser Funktion können Sie die Audioqualität steuern, die den Einschränkungen in der Bandbreite oder Netzwerkspitzen unterliegt.

Das Erhöhen der Puffergröße verbessert die Audioqualität, kann sich aber auf die Sendegeschwindigkeit auswirken.

Die maximal verfügbare Puffergröße beträgt 400 Millisekunden. Höhere Werte wirken sich zu stark auf die Audioqualität aus.

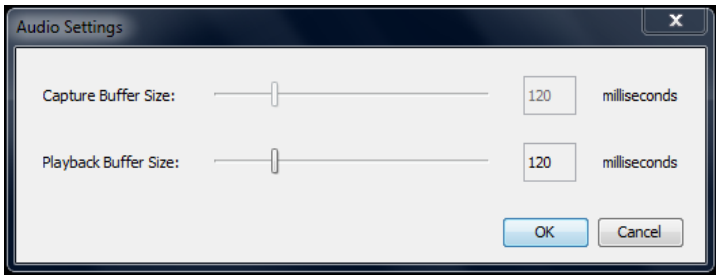
Die Puffergröße kann jederzeit angepasst werden, auch während einer Audiositzung.

Die Audioeinstellungen werden in VKC oder AKC konfiguriert.

Audioeinstellungen Anpassen

So passen Sie die Audioeinstellungen an:

1. Wählen Sie "Audio Settings" (Audioeinstellungen) aus dem Menü "Audio" aus. Das Dialogfeld "Audio Settings" (Audioeinstellungen) wird angezeigt.
2. Passen Sie gegebenenfalls die Puffergröße für Aufnahme und/oder Wiedergabe an. Klicken Sie auf OK.



Versioninformation - Virtual KVM Client

Dieser Menübefehl liefert Versionsinformationen zum Virtual KVM Client, falls Sie Unterstützung durch den technischen Kundendienst von Raritan benötigen.

So rufen Sie die Versionsinformationen ab:

1. Wählen Sie "Help" > "About Raritan Virtual KVM Client" (Hilfe > Informationen zum Raritan Virtual KVM Client) aus.

2. Verwenden Sie die Schaltfläche "Copy to Clipboard" (In Zwischenablage kopieren), um die im Dialogfeld enthaltenen Informationen in eine Zwischenablagedatei zu kopieren, sodass auf diese bei Bedarf später bei Hilfestellung durch den Kundendienst zugegriffen werden kann.

Kapitel 6 Aktive KVM Klient (AKC) Hilfe

In diesem Kapitel

Überblick

Der Aktive KVM Client (AKC) beruht auf Microsoft Windows .NET® Technologie.

Der AKC basiert auf Microsoft Windows .NET-Technologie. Sie können den Client in Windows-Umgebungen benutzen, ohne die Java Runtime Environment (JRE) zu verwenden, welche zur Ausführung des Virtual KVM Client (VKC) und des Multi-Platform-Client (MPC) von Raritan erforderlich ist..

Der AKC funktioniert auch mit CC-SG.

Der AKC und VKC verfügen mit Ausnahme der nachfolgend aufgeführten Punkte über identische Leistungsmerkmale:

- Auf dem AKC erstellte Tastaturmakros können im VKC nicht genutzt werden.
- Konfiguration des direkten Portzugriffs (siehe Aktivieren des direkten Port-Zugriffs über URL)
- Konfiguration der AKC-Serverzertifikat-Validierung (siehe ***Voraussetzungen für die Verwendung des AKC*** (siehe "***Voraussetzungen für die Verwendung von AKC***" auf Seite 306))
- AKC ladet automatisch die Eigenschaften, VKC nicht. Siehe Verwalten von Favoriten.

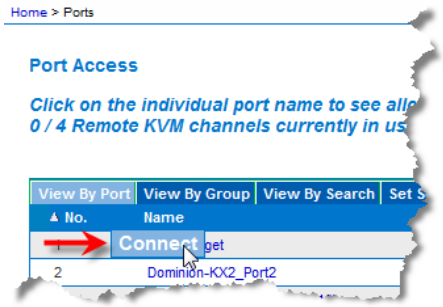
Weitere Informationen zum Verwenden der Funktionen, siehe ***Virtual KVM Client (VKC) Hilfe*** (siehe "***Virtual KVM Klient (VKC) Hilfe***" auf Seite 249).

Verbinden eines Zielservers

Sobald Sie in KX III Remote eingeloggt sind, greifen Sie auf die Zielserver über den Virtual KVM Client (VKC) oder den Active KVM Client (AKC) zu.

So schließen Sie einen verfügbaren Zielserver oder dualen Monitorzielserver an:

1. Auf der Portzugang-Seite klicken Sie unter Port Name (Portname) auf den Portnamen des Zielservers, an den Sie sich anschliessen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Klicken Sie auf/// ///Connect (Verbinden).



Weitere Informationen zu verfügbaren Menüoptionen finden Sie unter ***Menü "Port Action" (Portaktion*** (siehe "***Menü Port Action (Portaktion)***" auf Seite 20)).

AKC Unterstütztes Microsoft .NET Framework

Für AKC ist Windows .NET® Version 3.5, 4.0 oder 4.5 erforderlich. AKC funktioniert mit den installierten Versionen 3.5 und 4.0.

AKC unterstützte Betriebssysteme

Wurde der AKC über Internet Explorer® gestartet, bietet er Ihnen die Möglichkeit, über KX II 2.2 (oder höher) auf Zielserver zuzugreifen.

AKC ist kompatibel mit den folgenden Plattformen:

- Windows XP® Betriebssystem
- Windows Vista®-Betriebssystem (bis 64 Bit)
- Windows Vista®-Betriebssystem (bis 64 Bit)
- Windows Vista®-Betriebssystem (bis 64 Bit)

Hinweis: Sie müssen Windows 7 verwenden, wenn WINDOWS PC FIPs aktiviert ist und Sie mithilfe von AKC und einer Smart Card auf ein Ziel zugreifen.

Da .NET für die Ausführung von AKC benötigt wird, erhalten Sie, wenn Sie .NET nicht oder eine nicht unterstützte Version von .NET installiert haben, eine Meldung, in der Sie aufgefordert werden, die Version von .NET zu prüfen.

Hinweis: Raritan empfiehlt Benutzern des Betriebssystems Windows XP® zu überprüfen, ob eine funktionierende Version von .NET 3.5 oder 4.0 bereits installiert ist, bevor Sie AKC starten. Wenn Sie nicht sicherstellen, dass Ihre .NET-Version funktioniert, werden Sie nicht aufgefordert, die .NET-Version zu überprüfen, sondern werden aufgefordert, eine Datei herunterzuladen.

AKC Unterstützte Browser

- Internet Explorer® 8 (und höher)

  Wenn Sie versuchen, den AKC mit einem anderen Browser als IE 8 (oder höher) zu öffnen, wird Ihnen eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, zu prüfen, welchen Browser Sie verwenden und ggf. Internet Explorer zu verwenden.

Voraussetzungen für die Verwendung von AKC

Cookies Zulassen

Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.

KX III IP-Adressen in „Vertrauenswürdigen Seitenzonen‘ inbegriffen

Die Benutzer von Windows Vista®, Windows® 7 und Windows 2008 Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Seitenzonen" hinzugefügt wurde.

Geschützten Modus Deaktivieren

Die Benutzer von Windows Vista®, Windows® 7 und Windows 2008 Servern müssen sicherstellen, dass der "Geschützte Modus" nicht aktiv ist, wenn auf KX III zugegriffen wird.

AKC-Download-Serverzertifikatsvalidierung aktivieren

Wenn der Geräte- (oder CC-SG-)Administrator die Option "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikatsvalidierung aktivieren) ausgewählt hat, beachten Sie Folgendes:

- Administratoren müssen ein gültiges Zertifikat auf das Gerät hochladen oder ein selbstsigniertes Zertifikat auf dem Gerät generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

Wenn Sie AKC vom CC-SG-Administrations-Client aus starten, benötigen Sie JRE™ 1.7 (oder höher).

Kapitel 7 KX III Fernkonsole - KX III Anwender-Hilfe

In diesem Kapitel

Überblick

Das Lokale Konsole-Interface bietet Zugriff auf KX III wenn dieses Gestell benutzt wird.

Dieser Bereich enthält Hilfe für Aufgaben von Anwendern auf der Lokalen Konsole.

Zugreifen auf einen Zielserver

So greifen Sie auf einen Zielserver zu:

1. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Connect" (Verbinden) aus. Die Videoanzeige wechselt zur Oberfläche des Zielservers.

Lokale Konsole Videoauflösungen

Sobald der Monitor mit der KX III Lokalen Konsole verbunden ist, erkennt KX III die ursprüngliche Auflösung des Monitors. Dies ist in der Regel die größte Auflösung, die vom Monitor unterstützt wird.

Solange die ursprüngliche Auflösung des Monitors durch die lokale Konsole unterstützt wird, verwendet KX III diese Auflösung

Wenn die ursprüngliche Auflösung nicht unterstützt ist und keine andere Auflösung durch den Monitor und die lokale Konsole unterstützt wird, verwendet KX III die Auflösung des letzten Monitors, der mit der lokalen Konsole verbunden war.

Zum Beispiel, verbinden Sie ein Monitor-Set auf 1600x1200@60Hz zum KX III Lokale Konsole. KX III benutzt diese Auflösung, da diese Scanfunktion von der lokalen Konsole unterstützt ist.

Wenn der nächste Monitor, den Sie mit der lokalen Konsole verbinden möchten, nicht auf eine unterstützte Auflösung eingestellt ist, verwendet KX III die Auflösung von 1024x768 @ 60.

Für eine Liste von unterstützten Lokale Konsole Videoauflösungen, siehe ***Supported KX III Local Port DVI Resolutions*** (siehe "***Unterstützte Lokale KX III Port-DVI-Auflösung***" auf Seite 349).

Videomodi und Auflösungsnotizen für weitere Informationen (siehe "***Videomodi und Auflösungshinweise***" auf Seite 382).

Gleichzeitige Benutzer

Die lokale KX III Konsole stellt einen unabhängigen Zugriffspfad zu den angeschlossenen KVM-Zielservern bereit.

Die Verwendung der lokalen Konsole hindert andere Benutzer nicht daran, gleichzeitig eine Netzwerkverbindung herzustellen. Auch wenn Remotebenutzer mit KX III verbunden sind, können Sie gleichzeitig über die lokale Konsole im Serverschrank auf die Server zugreifen.

Zugriffstasten und Verbindungstasten

Da die Schaltfläche der lokalen KX III Konsole vollständig durch die Schaltfläche des Zielservers ersetzt wird, auf den Sie zugreifen, wird eine Zugriffstaste verwendet, um die Verbindung zu einem Ziel zu trennen und zur GUI des lokalen Ports zurückzukehren.

Um eine Verbindung zu einem Ziel herzustellen oder zwischen Zielen zu wechseln wird eine Verbindungstaste verwendet.

Über die Zugriffstaste für den lokalen Port können Sie schnell die Benutzeroberfläche der lokalen KX III Konsole aufrufen, wenn gerade ein Zielserver angezeigt wird.

Weitere Informationen finden Sie unter Lokale Porteinstellungen für die lokale KX III-Konsole.

Zurückkehren zur Schaltfläche der lokalen KX III Konsole

So kehren Sie vom Zielserver zur lokalen KX III Konsole zurück:

- Drücken Sie die Rollen-Taste zweimal kurz hintereinander.

  Die Videoanzeige wechselt von der Schaltfläche des Zielservers zur Schaltfläche der lokalen KX III Konsole.

Diese Tastenkombination können Sie auf der Seite "Local Port Settings" (Lokale Porteinstellungen) ändern. Siehe **Konfigurieren der lokalen KX III-Porteinstellungen von der lokalen Konsole** aus.

Beispiele für Verbindungstasten

Standardserver	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
Auf einen Port über die GUI des lokalen Ports zugreifen	Zugriff auf Port 5 über die GUI des lokalen Ports: • Linke Alt-Taste drücken > Taste "5" drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Zwischen Ports wechseln	Von Port 5 auf Port 11 wechseln: • Linke Alt-Taste drücken > Taste "1" drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Verbindung zu einem Zielgerät trennen und zur GUI	Verbindung zum Zielport 11 trennen und zur GUI des lokalen Ports zurückkehren (zu der Seite, von der aus Sie eine Verbindung zum

Standardserver	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
des lokalen Ports zurückkehren	Zielgerät hergestellt haben): • Double Click Scroll Lock (Rollen-Taste zweimal drücken)
Blade-Chassis	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
Auf einen Port über die GUI des lokalen Ports zugreifen	Zugriff auf Port 5, Slot 2: • Linke Alt-Taste drücken Taste "5" drücken und wieder loslassen Taste "-" drücken und wieder loslassen Taste "2" drücken und wieder loslassen Linke Alt-Taste wieder loslassen
Zwischen Ports wechseln	Von Zielport 5, Slot 2 auf Port 5, Slot 11 wechseln: • Linke Alt-Taste drücken Taste "5" drücken und wieder loslassen Taste "-" drücken und wieder loslassen Taste "1" drücken und wieder loslassen Linke Alt-Taste wieder loslassen
Verbindung zu einem Zielgerät trennen und zur GUI des lokalen Ports zurückkehren	Verbindung zum Zielport 5, Slot 11 trennen und zur GUI des lokalen Ports zurückkehren (zu der Seite, von der aus Sie eine Verbindung zum Zielgerät hergestellt haben): • Double Click Scroll Lock (Rollen-Taste zweimal drücken)

Spezielle Tastenkombinationen für Sun

Die folgenden Tastenkombinationen für spezielle Tasten von Sun™ Microsystems-Servern sind für den lokalen Port verfügbar. Diese speziellen Tasten sind im Menü "Keyboard" (Tastatur) verfügbar, wenn Sie eine Verbindung zu einem Sun-Zielserver herstellen.

Sun-Taste	Tastenkombination für lokalen Port
Again	Strg+Alt+F2
Props	Strg+Alt+F3
Undo	Strg+Alt+F4
Stop A	Untbr a
Front	Strg+Alt+F5
Copy	Strg+Alt+F6
Open	Strg+Alt+F7
Find	Strg+Alt+F9
Cut	Strg+Alt+F10
Paste	Strg+Alt+F8
Mute (Stummschaltung)	Strg+Alt+F12
Compose	Strg+Alt+Nummernfeld *
Vol +	Strg+Alt+Nummernfeld +
Vol -	Strg+Alt+Nummernfeld -
Stop	Keine Tastenkombination
Stromversorgung	Keine Tastenkombination

Scannen von Ports – Lokale Konsole

Eine Port-Scanfunktion, mit der nach ausgewählten Zielen gesucht werden kann. Die Ziele werden dann in einer Bildschirmpräsentationsansicht angezeigt.

Diese Funktion ermöglicht die Überwachung von bis zu 32 Zielen auf einmal, da Sie sich jeden Zielserver einzeln, wie es während der Diashow angezeigt wird, ansehen können.

Sie können je nach Bedarf eine Verbindung mit mehreren Zielen herstellen oder sich auf ein bestimmtes Ziel konzentrieren.

Scanvorgänge können Standardziele, Blade-Server, Dominion-Schichtgeräte und KVM-Switch-Ports umfassen.

Bei Dual Video-Portgruppen ist der primäre Port in einer Portprüfung enthalten, der sekundäre Port ist jedoch nicht enthalten, wenn eine Verbindung über einen Remote-Client hergestellt wird. Beide Ports können über den lokalen Port in die Prüfung aufgenommen werden.

Klicken Sie auf das Thumbnail eines Zielserver, um den Scan-Modus zu verlassen und mit dem Ziel zu verbinden, oder verwenden Sie die Lokal-Port ConnectKey Sequenz.

Um den Scan-Modus zu verlassen, klicken Sie auf die Schaltfläche „Stop Scan“ in der Miniaturansicht oder verwenden Sie die Tastenfolge „DisconnectKey“.

Hinweis: Die Scan-Port-Funktion ist von der Fernkosole und der lokalen Konsole verfügbar, aber die Funktionen können unterschiedlich sein. Siehe Scannen von Ports - Fernkonsole

Scannen von Ports Slide Show – Lokale Konsole

Beim Starten eines Scanvorgangs wird das Fenster "Port Scan" (Port-Scan) geöffnet.

Jedes gefundene Ziel wird als Miniaturansicht in einer Bildschirmpräsentation angezeigt.

In der Bildschirmpräsentation wird in einem Standardintervall von 10 Sekunden oder in dem von Ihnen angegebenen Intervall durch die Miniaturansichten der Ziele geblättert.

Beim Blättern durch die Ziele wird das Ziel, das sich im Fokus der Bildschirmpräsentation befindet, in der Mitte der Seite angezeigt.

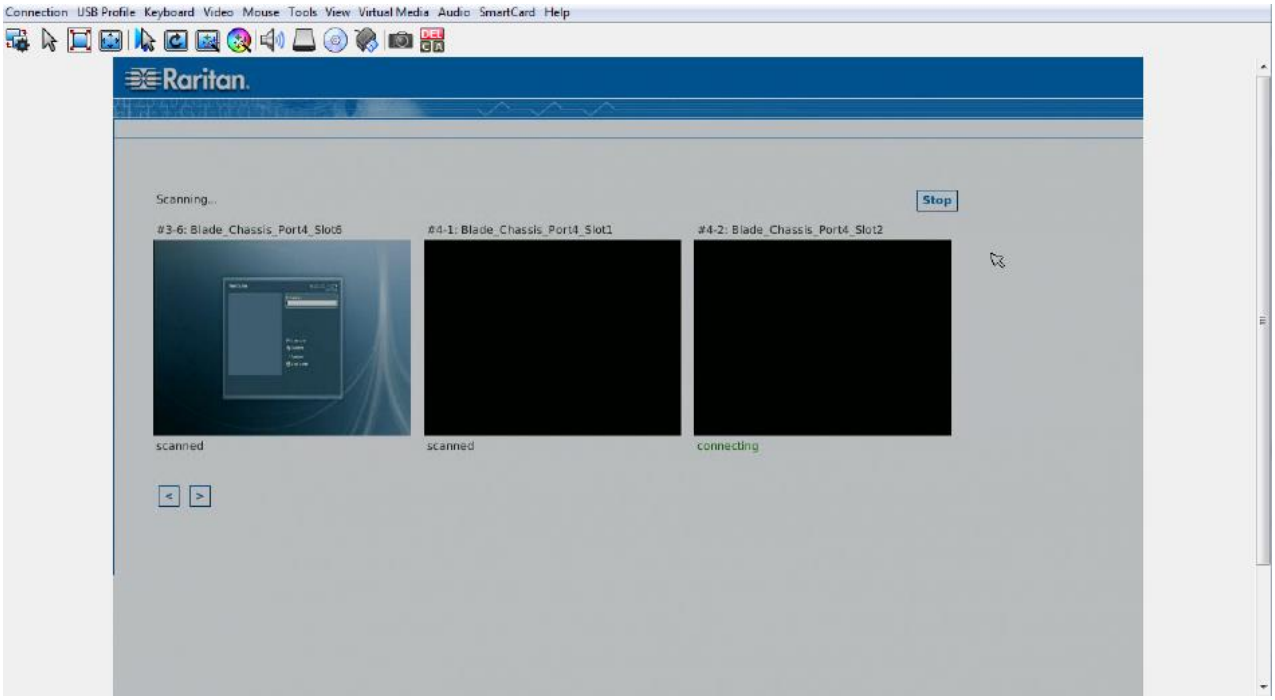
Der Name des Ziels wird unter der entsprechenden Miniaturansicht und in der Taskleiste unten im Fenster angezeigt.

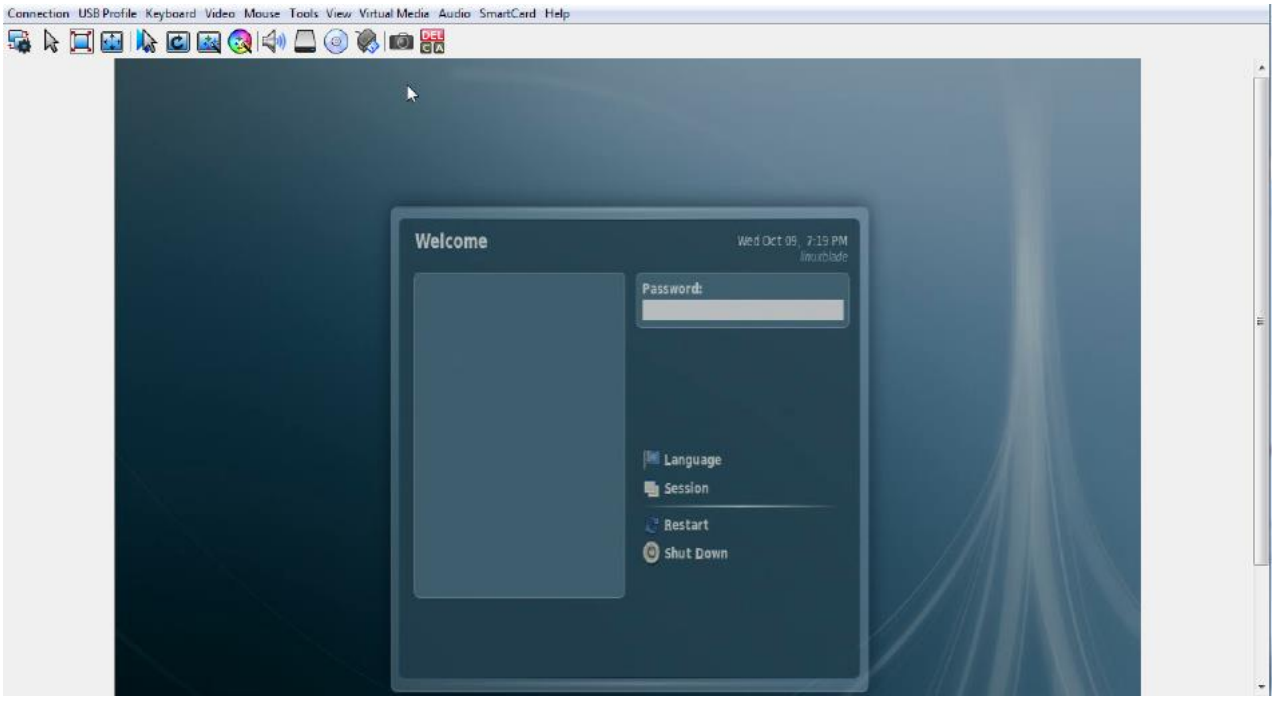
Ist ein Ziel belegt, wird statt der Seite zum Zugreifen auf den Zielserver ein leerer Bildschirm angezeigt.

Konfigurieren Sie die Zeit zwischen der Diashow Thumbnail-Drehung und dem Thumbnail-Fokus Intervall auf der lokalen Seite Port-Einstellungen.

Konfigurieren von Lokale Konsole-Scaneinstellungen (auf Seite 316)

Hinweis: Konfigurieren Sie die Scaneinstellungen für die Fernkonsole entweder über den Virtual KVM Client (VKC) oder den Active KVM Client (AKC). Siehe **Konfigurieren von Port-Scaneinstellungen über VKC und AKC** *(auf Seite 277)*


Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Raritan.
Scanning...
Stop
#3-6: Blade_Chassis_Port4_Slot6
#4-1: Blade_Chassis_Port4_Slot1
#4-2: Blade_Chassis_Port4_Slot2
scanned
scanned
connecting

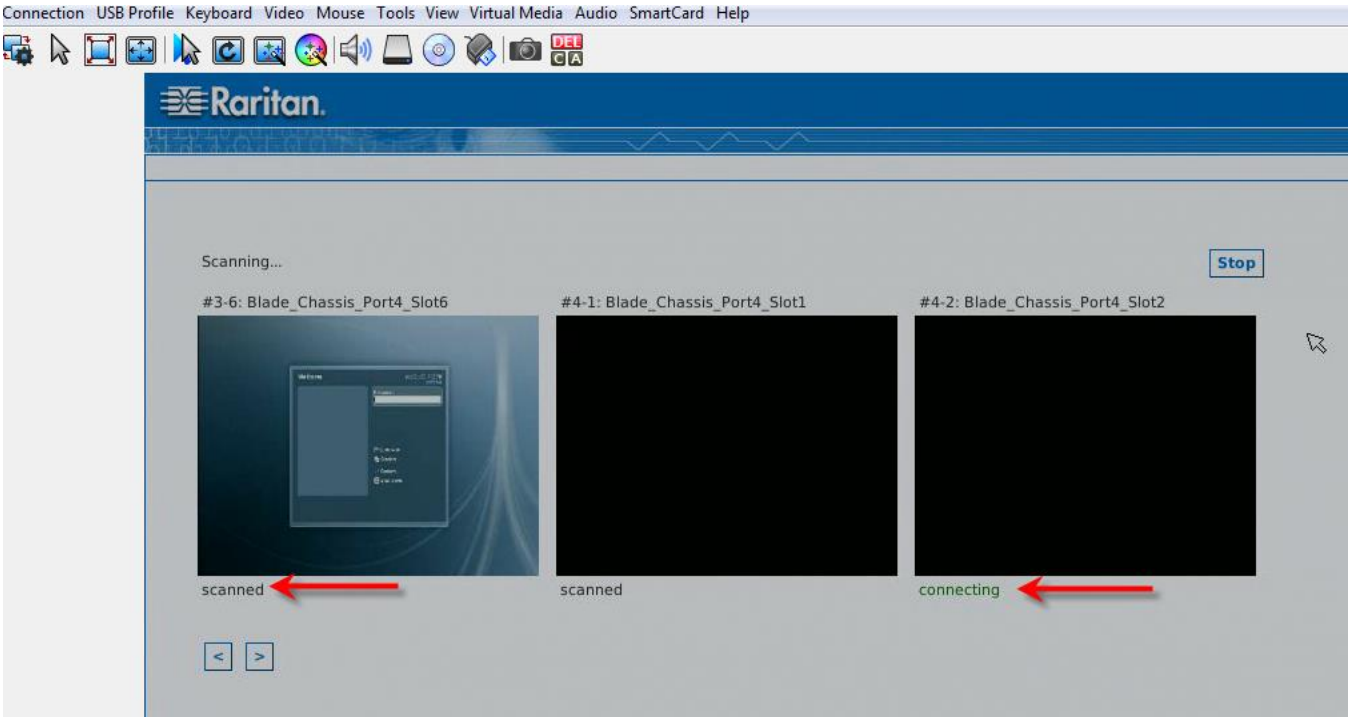

Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Welcome
Password:
Language
Session
Restart
Shut Down

Zielstatus-Anzeige während Portscannen - Lokale Konsole

In der Miniaturansicht auf der lokalen Konsole wird der Status der einzelnen Ziele unter dem Vorschaubild auf der Seite angezeigt.

Der Scannen-Status für alle Ziele wird wie folgt angezeigt:

- nicht gescannt
- Verbindung wird hergestellt
- gescannt
- gesprungen



Konfigurieren von Lokale Konsole-Scaneinstellungen

So konfigurieren Sie die lokalen Porteinstellungs-Optionen:

Hinweis: Konfigurieren Sie die Scaneinstellungen für die Fernkonsole entweder über den Virtual KVM Client (VKC) oder den Active KVM Client (AKC). Siehe **Konfigurieren von Port-Scaneinstellungen über VKC und AKC** *(auf Seite 277)*

So konfigurieren Sie die lokalen Porteinstellungen:

1. Wählen Sie in der lokalen Konsole die Geräteeinstellungen aus.
2. Im Bereich lokale Porteinstellung, wählen Sie Lokaler Port Scannenmodus.

3. Ändern Sie den Display-Intervall nach Bedarf:
   - Intervall Anzeigen - ändert den Scan-Display-Intervall
   - Intervall Zwischen Ports - Änderung des Intervalls mit dem Wechseln zwischen verschiedenen Ports, während des Scannens.

So suchen Sie nach Zielen - Lokale Konsole

So suchen Sie nach Zielen:

1. Klicken Sie auf der Seite "Port Access" (Portzugriff) auf die Registerkarte "Set Scan" (Scanfunktion einstellen).
2. Wählen Sie die Ziele aus, die in die Suche einbezogen werden sollen, indem Sie das Kontrollkästchen links neben dem jeweiligen Ziel aktivieren. Durch Aktivieren des Kontrollkästchens oben in der Zielspalte können Sie auch alle Ziele auswählen.
3. Lassen Sie das Kontrollkästchen "Up Only" (Nur ein) aktiviert, wenn nur Ziele in die Suche einbezogen werden sollen, die eingeschaltet sind. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie alle Ziele, egal ob ein- oder ausgeschaltet, in die Suche einbeziehen möchten.
4. Klicken Sie auf "Scan" (Scannen), um die Suche zu starten.

   Jedes gescannte Ziel wird in einer Bildschirmpräsentation auf der Seite angezeigt.

Smart Card-Zugriff von der lokalen Konsole

Um mit einer Smart Card auf einen Server auf der lokalen Konsole zuzugreifen, schließen Sie ein Smart Card-USB-Lesegerät an KX III an. Nutzen Sie dazu einen der USB-Ports auf KX III.

Sobald ein Smart Card-Lesegerät am KX III ein- oder ausgesteckt wird, wird dies von KX III automatisch erkannt.

Eine Liste der unterstützten Smart Cards und Informationen zu zusätzlichen Systemanforderungen finden Sie unter Unterstützte und nicht unterstützte Smart Card-Lesegeräte und ***unter Mindestanforderungen an Smart Cards*** (siehe "***Mindestanforderungen an Smart Cards***" auf Seite 356).

Nach der Installation des Kartenlesegeräts und der Smart Card auf dem Zielserver, funktioniert der Server so, als wären das Kartenlesegerät und die Smart Card direkt am Server angeschlossen.

Abhängig von den Einstellungen in den Richtlinien zur Entfernung der Karte im Betriebssystem des Zielservers wird beim Entfernen der Smart Card oder des Smart Card-Lesegeräts die Benutzersitzung gesperrt, oder Sie werden abgemeldet.

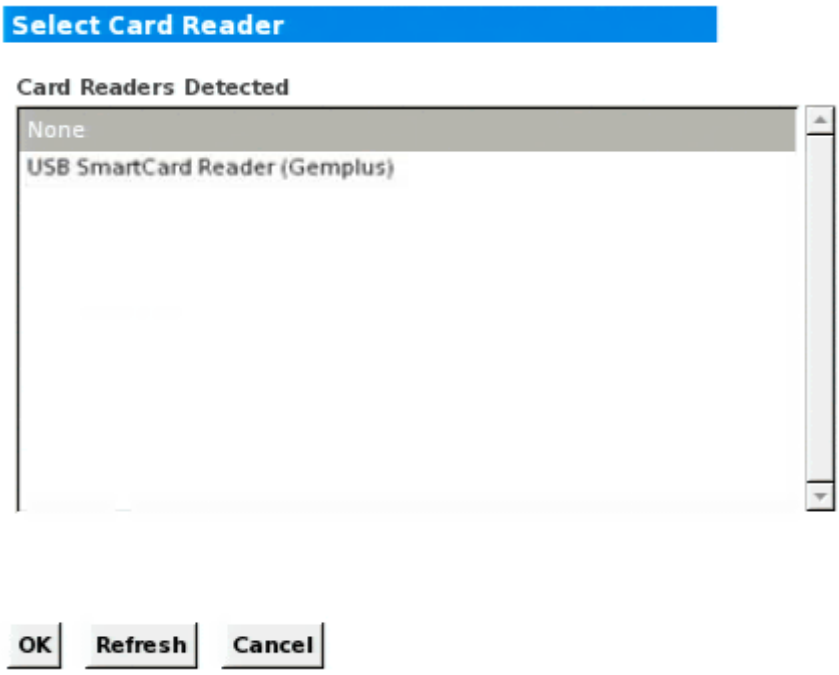
Ist die KVM-Sitzung unterbrochen, weil Sie beendet wurde oder Sie auf ein neues Ziel umgeschaltet haben, wird das Smart Card-Kartenlesegerät automatisch vom Zielserver deinstalliert.

So mounten Sie ein Smart Card-Lesegerät über die lokale KX III-Konsole auf einem Ziel.

1. Stecken Sie ein Smart Card-USB-Lesegerät am KX III-Gerät ein. Nutzen Sie dazu einen der USB-Ports des Geräts. Sobald das Smart Card-Lesegerät angeschlossen ist, wird es von KX III erkannt.
2. Klicken Sie in der lokalen Konsole auf "Tools" (Extras).
3. Wählen Sie in der Liste "Card Readers Detected" (Erkannte Smart Card-Lesegeräte) das Smart Card-Lesegerät aus. Wählen Sie in der Liste die Option "None" (Keines) aus, wenn Sie keines der Lesegeräte mounten möchten.
4. Klicken Sie auf "OK". Sobald das Smart Card-Lesegerät hinzugefügt wurde, wird auf der Seite eine Meldung angezeigt, die Sie darauf hinweist, dass der Vorgang erfolgreich abgeschlossen wurde. Der jeweilige Status "Selected" (Ausgewählt) oder "Not Selected" (Nicht ausgewählt) wird im linken Fenster der Seite unter "Card Reader" (Smart Card-Lesegerät) angezeigt.

So aktualisieren Sie die Liste "Card Readers Detected" (Erkannte Smart Card-Lesegeräte):

- Klicken Sie auf "Refresh" (Aktualisieren), wenn ein neues Smart Card-Lesegerät gemounted wurde. Die Liste "Card Readers Detected" (Erkannte Smart Card-Lesegeräte) wird aktualisiert und zeigt die neu hinzugefügten Smart Card-Lesegeräte an.



USB-Profiloptionen der lokalen Konsole

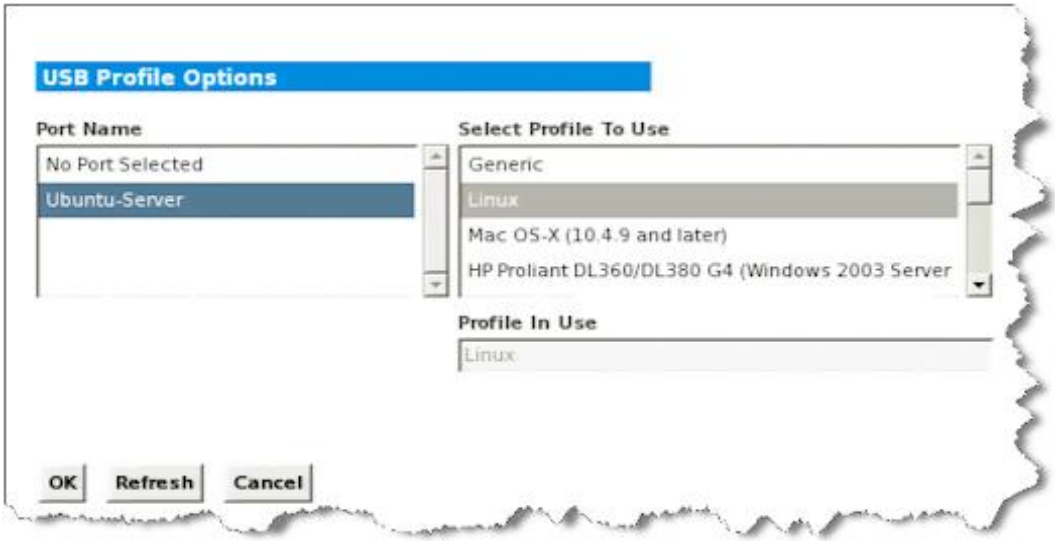
Wählen Sie im Abschnitt "USB Profile Options" (USB-Profiloptionen) auf der Seite "Tools" (Extras) ein verfügbares USB-Profil aus.

Die Ports, die Profilen zugewiesen werden können, werden im Feld "Port Name" angezeigt, und die für einen Port verfügbaren Profile werden im Feld "Select Profile To Use" (Zu verwendendes Profil auswählen) angezeigt, nachdem der Port ausgewählt wurde. Die Profile, die für die Verwendung mit einem Port ausgewählt wurden, werden im Feld "Profile In Use" (Verwendetes Profil) angezeigt.

So weisen Sie einem Port der lokalen Konsole ein USB-Profil hinzu:

1. Wählen Sie im Feld "Port Name" den Port aus, den Sie dem USB-Profil zuweisen möchten.
2. Wählen Sie im Feld "Select Profile To Use" (Zu verwendendes Profil auswählen) das gewünschte Profil aus den für den Port verfügbaren Profilen aus.

3. Klicken Sie auf "OK". Das USB-Profil wird für den lokalen Port übernommen und im Feld "Profile In Use" (Verwendetes Profil) angezeigt.



KX III Lokale Konsole Werksrückstellung

Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern.

*Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter Prüfprotokoll, **Audit Log** (siehe "**Audit Log (Prüfprotokoll)**" auf Seite 196).*

So führen Sie eine Werksrückstellung durch:

1. Wählen Sie "Maintenance“ "Factory Reset" (Wartung > Werksrücksetzung) aus. Die Seite "Factory Reset" (Werksrücksetzung) wird angezeigt.
2. Wählen Sie die entsprechende Rücksetzungsoption aus:
   - Full Factory Reset (Vollständige Werksrücksetzung) – Damit entfernen Sie die gesamte Konfiguration und setzen das Gerät komplett auf die werkseitigen Standardeinstellungen zurück. Beachten Sie, dass Verwaltungsverbindungen mit CommandCenter dadurch unterbrochen werden. Da diese Rückstellung so umfassend ist, werden Sie dazu aufgefordert, den Vorgang zu bestätigen.

- Network Parameter Reset (Netzwerkparameterrücksetzung) – Damit setzen Sie die Netzwerkparameter des Geräts auf die Standardwerte zurück [Klicken Sie auf "Device Settings“ "Network Settings" (Geräteeinstellungen > Netzwerkeinstellungen), um auf diese Informationen zuzugreifen]:

3. Klicken Sie auf "Reset" (Zurücksetzen), um fortzufahren. Da hierbei alle Netzwerkeinstellungen verloren gehen, werden Sie aufgefordert, die Werksrücksetzung zu bestätigen.
4. Klicken Sie zum Fortfahren auf "OK". Nach Abschluss des Vorgangs wird das KX III Gerät automatisch neu gestartet.

Zurücksetzen des KX III mithilfe der Taste "Reset" (Zurücksetzen)

Auf der Rückseite des Geräts befindet sich die Taste "Reset" (Zurücksetzen). Sie ist etwas zurückgesetzt, damit sie nicht unbeabsichtigt gedrückt wird (Sie benötigen einen spitzen Gegenstand, um die Taste zu betätigen).

Welche Maßnahmen ergriffen werden, wenn die Taste "Reset" (Zurücksetzen) gedrückt wird, legen Sie auf der Seite „Encryption & Share" (Verschlüsselung & Freigabe) fest. Sehen Sie Verschlüsselung & Freigabe in Online-Hilfe.

Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern.

*Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter **Audit Log** (siehe "**Audit Log (Prüfprotokoll)**" auf Seite 196).*

So setzen Sie das Gerät zurück:

1. Schalten Sie die KX III-Einheit aus.
2. Verwenden Sie einen spitzen Gegenstand, und halten Sie die Taste zum Zurücksetzen damit gedrückt.
3. Halten Sie die Taste zum Zurücksetzen gedrückt und schalten Sie gleichzeitig das KX III-Gerät wieder ein.

4. Halten Sie die Taste "Reset" (Zurücksetzen) weitere zehn Sekunden gedrückt.

Anhang A Verbinden Sie KX III und Cat5 Reach DVI - Erweiterte Lokale Portfunktionalität

In diesem Kapitel

Überblick

Ein erweiterter lokaler Port erweitert die Reichweite des lokalen Ports, beispielsweise zu einem anderen KVM-Switch.

Dies kann durch die Konfiguration eines KX III mit einem Raritan Cat5 Reach DVI Sender und Empfänger erreicht werden, die dann an einer Remote-Konsole oder an einem anderen Gerät angeschlossen sind.

Sobald es an dem Cat5 Reach DVI angeschlossen ist, kann auf den KX III von bis zu 152 m entfernt zugegriffen werden.

Die Verbindung des KX III zum Cat5 Reach DVI mit der Verkettung von Ethernet-Switches kann die KX-III-Reichweite bis zu 914 m verlängern.

Über Cat5 Reach DVI

Für Einzelheiten über Cat5 Reach DVI, siehe das Cat5 Reach DVI Online-Benutzerhandbuch, verfügbar auf ***Raritan Unterstützungsseite http://www.raritan.com/support***.

Für weitere Informationen über Cat5 Reach DVI, oder für Informationen über den Kauf, ***kontaktieren Sie Raritan*** (***http://www.raritan.com/contact-us/***).

Verbinden Sie KX III und Cat5 Reach DVI

Hinweis: Die verwendeten Bilder für die Diagramme sind nicht zu KX III spezifiziert, aber die Verbindungen sind korrekt.

Dieser Abschnitt stellt drei Szenarien in Bezug auf die KVM-Switches dar.

- KX III zwischen jedem KVM-Switch und seiner lokalen Konsole anschließen.
- KX III zwischen zwei KVM-Switch anschließen.
- Schließen Sie den KX III zwischen einem Computer/Server und einem KVM-Switch an.

Schalten Sie alle Geräte aus, bevor Sie die Verbindung herstellen.

Für Informationen über die Einstellung der Lokolen Fernkonsole, siehe **Connecting a Keyboard/Mouse/Video Source** in **Cat5 Reach DVI Help**.

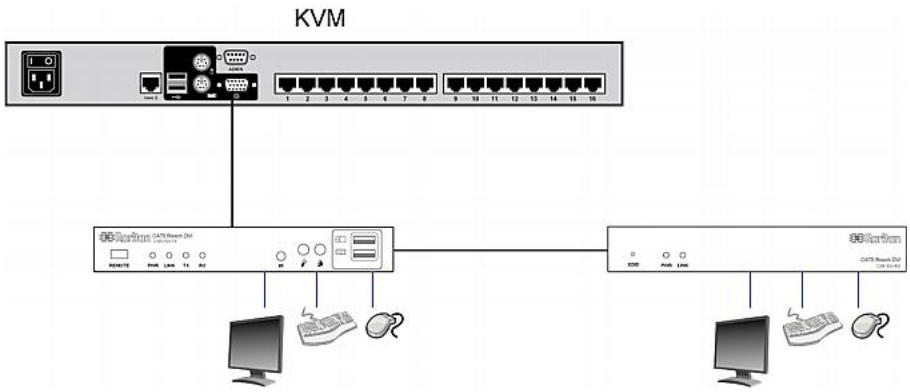
Verbinden Sie KX III und Cat5 Reach DVI:

1. Richten Sie die lokale und Fernkonsole mit Cat5 Reach DVI Transmitter und Empfänger aus.

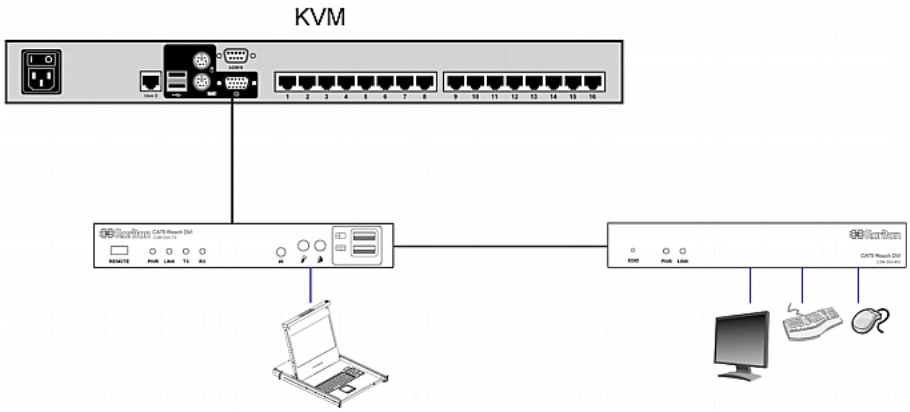
   Basic Installation in **Cat5 Reach DVI Hilfe**.

2. Verwenden Sie ein Cat5e / 6 Kabel, um den Sender und Empfänger zu verbinden.
3. Schließen Sie den Transmitter und den Empfänger an eine geeignete Stromquelle an.
4. Verbinden Sie den lokalen Konsolenport des KVM-Switches mit dem Transmitter.
   a. Schließen Sie ein Ende des DVI Kabels von Raritan an dem DVI-IIN-Port auf dem Transmitter und das andere Ende an dem KVM Switch-Video-Port an.
   b. Schließen Sie den USB-B Port des Kabels von Raritan an dem Transmitter und das andere Ende an dem KVM-Switch-Lokal-USB-Port-an.

5. Schalten Sie den KVM-Switch ein.



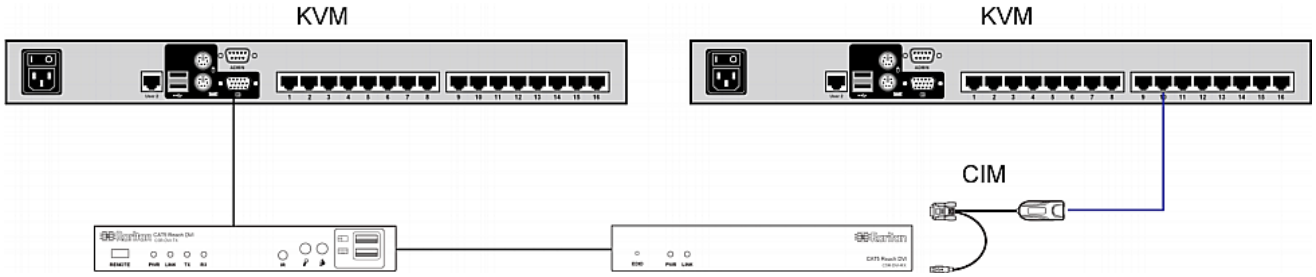
Tipp: Die lokale oder Fernkonsole kann mit einem KVM-Zeichner anstatt einem Set von Tastatur/Maus/Monitor ausgerüstet werden. Siehe die untenstehende Illustration.



Um die Distanz zwischen zwei geschichteten KVM Switch zu erhöhen:

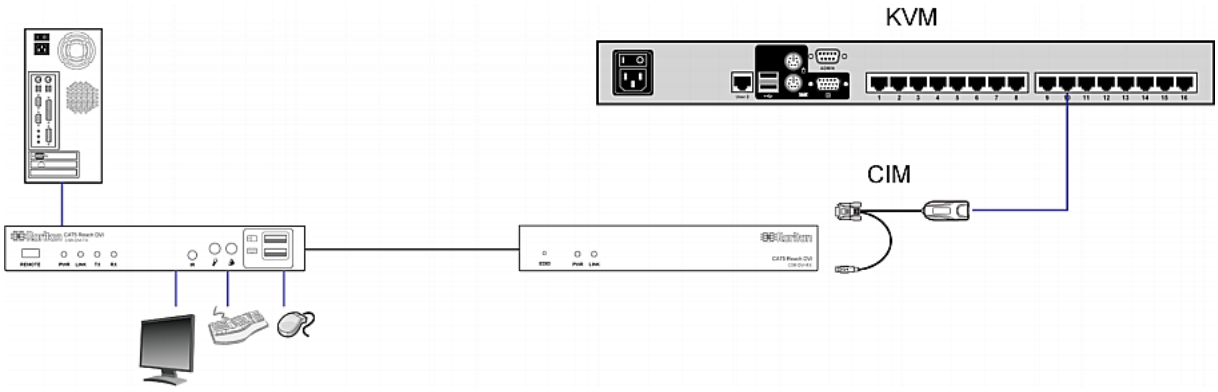
1. Richten Sie eine Fernkonsole ein, indem Sie den Empfänger an einem KVM-Switch anschließen.
   a. Verbinden Sie einen Server über ein USB CIM mit dem Empfänger.
   b. Verbinden Sie diesen USB CIM mit einem der Portkanäle auf dem KVM-Switch via einem Cat5-Kabel.
2. Verwenden Sie ein Cat5e / 6 Kabel, um den Sender und den Empfänger zu verbinden.
3. Schließen Sie den Transmitter und den Empfänger an eine geeignete Stromquelle an.
4. Schließen Sie den KVM-Switch an den Transmitter an.

5. Schalten Sie beide KVM-Switch ein.



Um die Distanz zwischen Computer und KVM Switch zu erhöhen:

1. Richten Sie eine optionale lokale Konsole mit dem Transmitter ein.
2. Richten Sie eine Fernkonsole ein, indem Sie den Empfänger an einem KVM-Switch anschließen.
3. Verwenden Sie ein Cat5e / 6 Kabel, um den Sender und den Empfänger zu verbinden.
4. Schließen Sie den Transmitter und den Empfänger an eine geeignete Stromquelle an.
5. Schließen Sie den Transmitter an den Computer an.
6. Schalten Sie den Computer ein.



Anhang B Zugreifen auf einen Paragon II vom KX III

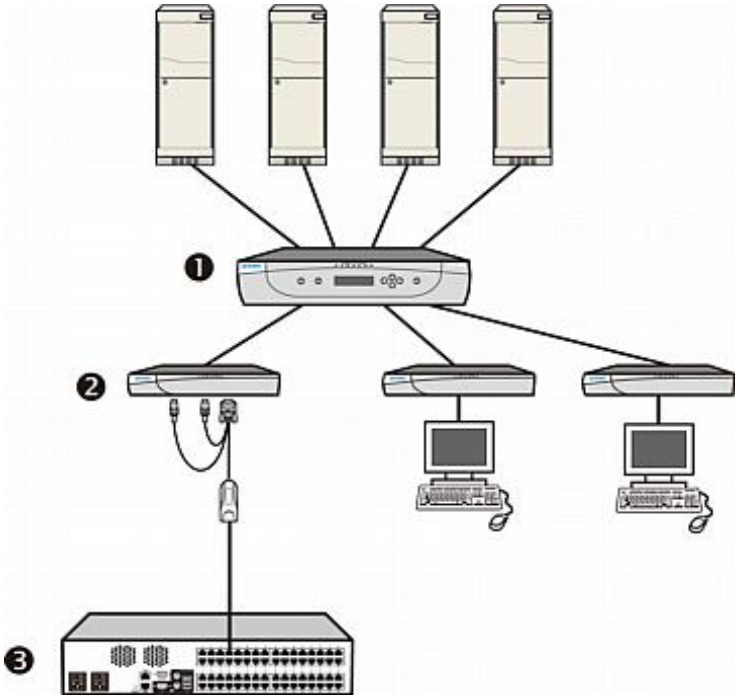
In diesem Kapitel

Überblick

Sie können das Paragon II-System an ein KX III anschließen, das von CC-SG verwaltet wird, sodass Sie über CC-SG auf Paragon II zugreifen können.

Diese Abbildung zeigt die Konfigration für die Integration von KX III.

Hinweis: Die Bilder dienen nur als Beispiele und können möglicherweise nicht genauso aussehen wie Ihr Gerät.



1	Das Paragon II-System mit Paragon II-Switches, Server und Benutzer-Stationen
2	Die Benutzer-Station mit angeschlossenem DCIM-USB-G2

3	KX III

Wenn Sie über KX III oder CC-SG auf das Paragon II-System zugreifen (sofern KX III von CC-SG verwaltet wird), wird der Anmeldebildschirm der Paragon-Bildschirmbenutzerschnittstelle angezeigt, damit Sie sich anmelden können.

In dieser Integration können Sie alle ivorhandenen OSUI Funktionen mit der vorhandenen Paragon II Firmware oder alle KX III Funktionen, die mit der vorhandenen KX III. Firmware implementiert sind, ausführen, ausser der Virtual Media Funktion.

Wenn Sie über KX III auf die Paragon-Bildschirmbenutzerschnittstelle zugreifen, versuchen Sie NICHT, die Maus manuell zu synchronisieren. Sie benötigen keine Maus für die Bildschirmbenutzerschnittstelle. Die Synchronisierung der Maus verzögert die Reaktionszeit der Tastatur um Sekunden.

Weitere Informationen finden Sie unter ***Unterstützte Paragon- II CIMS und Konfigurationen*** (siehe "***Unterstützte Paragon II CIMS und Konfigurationen***" auf Seite 328).

Unterstützte Paragon II CIMS und Konfigurationen

KX III unterstützt die P2CIM-APS2DUAL- und P2CIM-AUSBDUAL-CIMs, die zwei RJ45-Verbindungen zu unterschiedlichen KVM-Switches enthalten.

Die Unterstützung dieser CIMs beinhaltet einen zweiten Pfad für den Zugriff auf das Ziel, falls einer der KVM-Switches blockiert ist oder ein Fehler auftritt.

Paragon CIM	Unterstützung	Keine Unterstützung
P2CIM-APS2DUAL	• Server mit IBM®-PS/2-Tastatur- und -Mausports • Automatische Schräglaufkompensierung (wenn CIMs an Paragon II angeschlossen sind, nicht an einem KX III) • Mausmodus "Intelligent" • Mausmodus "Standard"	• Virtuelle Medien • Smart Cards • Mausmodus "Absolut" • Verwendung mit Blade-Chassis • Kaskadierte KVM-Konfigurationen

Paragon CIM	Unterstützung	Keine Unterstützung
P2CIM-AUSBDUAL	• Server mit USB- oder SUN™-USB-Tastatur- und -Mausports • Automatische Schräglaufkompensierung (wenn CIMs an Paragon II angeschlossen sind, nicht an einem KX III) • Mausmodus "Intelligent" • Mausmodus "Standard"	• Virtuelle Medien • Smart Cards • Mausmodus "Absolut" • Verwendung mit Blade-Chassis • Kaskadierte KVM-Konfigurationen

KX III-zu-KX III Paragon CIM Handbuch

Berücksichtigen Sie die folgenden Richtlinien zur Systemkonfiguration, wenn Sie Paragon-CIMs in einer KX III zu KX III Konfiguration verwenden:

Gleichzeitiger Zugriff

Beide KX III KVM-Switches müssen gemäß derselben Richtlinie für gleichzeitigen Zugriff auf Ziele konfiguriert werden: entweder beide "PC-Share" (PC-Freigabe) oder beide "Private" (Privat).

Wenn der private Zugriff auf Ziele erforderlich ist, müssen beide KVM-Switches entsprechend konfiguriert werden:

- Legen Sie unter "Security“ "Security Settings" "Encryption Share" (Sicherheit > Sicherheitseinstellungen > Verschlüsselung und Freigabe) den PC-Freigabemodus auf "Private" (Privat) fest.

Dies gewährleistet, dass der gleichzeitige Zugriff auf Ziele für alle Ziele von allen Benutzergruppen untersagt ist.

KX III ermöglicht eine detailliertere Steuerung des gleichzeitigen Zugriffs auf Ziele auf Benutzergruppenbasis. Dies wird erreicht, indem Sie die Gruppenberechtigungen für die PC-Freigabe festlegen. Dies ist jedoch die einzige erzwungene Eigenschaft innerhalb eines KX III. Sie dürfen sich nicht auf die PC-Freigabeberechtigungen für Benutzergruppen verlassen, wenn der exklusive Zugriff mithilfe von P2CIM-APS2DUAL oder P2CIM-AUSBDUAL mit KX III gewährleistet werden muss.

Aktualisieren des CIM-Namens

Die P2CIM-APS2- und P2CIM-AUSB-Namen werden im CIM-Speicher abgelegt. Es gibt zwei Speicherorte für die Paragon-Namenskonvention (12 Zeichen) und die KX III Namenskonvention (32 Zeichen).

Bei der ersten Verbindung zu einem KX III wird der Paragon-Name aus dem Speicher aufgerufen und von KX III in den CIM-Speicherort geschrieben. Nachfolgende Abfragen des CIM-Namens oder Aktualisierungen des CIM-Namens vom KX III finden an dem von KX III verwendeten Speicherort statt. KX III führt am von Paragon II verwendeten Speicherort keine Aktualisierungen aus.

Wenn der CIM-Name von einem KX III aktualisiert wird, findet der andere KX III den aktualisierten Namen und ruft diesen ab, sobald die Verbindung zu diesem Ziel wieder hergestellt wird. Der Name wird erst zu diesem Zeitpunkt auf dem anderen KX III aktualisiert.

Portstatus und -verfügbarkeit

Der Portstatus, der auf der KX III Seite "Port Access" (Portzugriff) entweder als "Up" (Ein) oder "Down" (Aus) angezeigt wird, wird aktualisiert, um anzuzeigen, ob das CIM eingeschaltet und mit dem KX III Port verbunden ist.

Die Portverfügbarkeit, die auf der KX III Seite "Port Access " (Portzugriff) als "Idle" (Inaktiv), "Busy" (Verwendet) oder "Connected" (Verbunden) angezeigt wird, wird nur aktualisiert, um die Aktivität auf dem Ziel anzuzeigen, das vom selben KX III initiiert wurde.

Wenn eine Verbindung zum Ziel vom anderen KX III vorhanden ist, wird die Verfügbarkeit geprüft, sobald ein Verbindungsversuch stattfindet. Der Zugriff wird gemäß der PC-Freigaberichtlinie des KX III verweigert oder zugelassen. Die Verfügbarkeit wird erst zu diesem Zeitpunkt auf dem anderen KX III aktualisiert.

Wenn der Zugriff verweigert wird, weil das Ziel verwendet wird, wird eine Benachrichtigung angezeigt.

Arbeiten mit CC-SG

Von CC-SG initiierten Vorgänge basieren auf dem Status, der Verfügbarkeit und dem CIM-Namen, die vom verwalteten KX III gemeldet werden. Wenn das Ziel mit zwei verwalteten KX III verbunden ist und die Geräte zu CC-SG hinzugefügt werden, werden zwei Knoten erstellt. Jeder Knoten enthält eine eigene zugeordnete oob-kvm-Schnittstelle. Sie können auch von jedem KX III einen einzelnen Knoten mit einer oob-kvm-Schnittstelle konfigurieren.

Wenn die KX IIIn für den Modus "Private" (Privat) konfiguriert wurden, wird der Benutzer bei einem zweiten Verbindungsversuch benachrichtigt, dass die Verbindung nicht hergestellt werden kann und der Zugriff verweigert wurde.

Wenn mithilfe des Fensters "CC-SG Port Profile" (CC-SG-Portprofil) ein Portname geändert wird, wird der geänderte Name an den verwalteten KX III geleitet. Der entsprechende Portname des anderen KX III wird erst in CC-SG aktualisiert, wenn über die oob-kvm-Schnittstelle des anderen KX III ein Verbindungsversuch zum Zielport stattfindet.

Richtlinien für KX III zu Paragon II

P2CIM-APS2DUAL oder P2CIM-AUSBDUAL kann mit KX III und Paragon II verbunden werden.

Gleichzeitiger Zugriff

Sowohl KX III und Paragon II müssen gemäß derselben Richtlinie für gleichzeitigen Zugriff auf Ziele konfiguriert werden.

Betriebsmodus von Paragon II	Modusbeschreibung	Unterstützt?
Private (Privat)	Nur ein Benutzer kann	Unterstützt.

Betriebsmodus von Paragon II	Modusbeschreibung	Unterstützt?
	jeweils auf einen Server oder ein anderes Gerät auf einem bestimmten Kanalport exklusiv zugreifen.	Sowohl Paragon II und KX III müssen auf "Private" (Privat) festgelegt sein. Die Einstellung "Private" (Privat) wird für das KX III Gerät, jedoch nicht für die Benutzergruppe, übernommen. Paragon II verwendet die Farbe Rot, um den Status "Verwendet" oder die Farbe Grün, um den Status "Verfügbar" anzuzeigen.
PC-Share (PC-Freigabe)	Ein Server oder anderes Gerät auf einem bestimmten Kanalport kann von mehreren Benutzern ausgewählt und gesteuert werden, jedoch erhält jeweils nur ein Benutzer die Tastatur- und Maussteuerung.	Unterstützt. "PC Share Idle Timeout" (Zeitlimit für Inaktivität der PC-Freigabe), das auf Paragon II konfiguriert wird, wird nicht unterstützt. Beide Benutzer können die Tastatur- und Maussteuerung gleichzeitig verwenden. Paragon II verwendet die Farbe Grün, um den Status "Verfügbar" anzuzeigen. Dies wird auch angezeigt, wenn ein anderer Benutzer bereits auf das Ziel zugreift.
Public View (Öffentliche Ansicht)	Während ein Benutzer auf einen Server oder auf ein anderes Gerät auf einem bestimmten Kanalport zugreift, können andere Benutzer diesen Kanalport auswählen, und die Videoausgabe von diesem Gerät anzeigen. Jedoch kann nur der erste Benutzer die Tastatur- und Maussteuerung verwenden, bis er die Verbindung trennt oder	Nicht unterstützt. Dieser Modus kann nicht verwendet werden, wenn das CIM mit Paragon II und KX III verbunden ist. Paragon II verwendet die Farbe Gelb, um den P-Ansichtsmodus anzuzeigen.

Betriebsmodus von Paragon II	Modusbeschreibung	Unterstützt?
	umschaltet.	

Aktualisieren des CIM-Namens

- Von Paragon II aktualisierte CIM-Namen werden an dem CIM-Speicherort gespeichert und von dort abgerufen, der der Paragon-Namenskonvention entspricht.
- Von KX III aktualisierte CIM-Namen werden an dem CIM-Speicherort gespeichert und von dort abgerufen, sodass es der KX III Namenskonvention entspricht.
- Aktualisierungen des CIM-Namens werden nicht zwischen Paragon II und KX III übertragen.

Unterstützte Verbindungsdistanzen zwischen Paragon II und KX III

Wenn SieKX III als Front-End eines Paragon-Systems verwenden, müssen Sie die maximal mögliche Kabellänge (Distanz) berücksichtigen, um eine gute Videoqualität zu erhalten.

Die unterstützte Distanz von der Paragon II-User-Station zum Zielserver beträgt 152 m Kabellänge. Größere Entfernungen beeinträchtigen die Videoleistung.

Die unterstützte Entfernung von KX III zur Paragon II -User-Station beträgt 45 m Kabellänge.

Anschließen von Paragon II an KX III

So schließen Sie das Paragon II-System an KX III an:

1. Prüfen Sie, ob die Paragon II User-Station, die Sie an KX IIIanschließen möchten, die Firmware Version 4.6 (oder höher) aufweist. Falls nicht, aktualisieren Sie die Firmware.

   Folgende Paragon II User-Stationen können verwendet werden:

   - P2-UST
   - P2-EUST
   - P2-EUST/C

   Siehe **Paragon II Hilfe** für Informationen über Aktualisierung.

2. Verbinden Sie die Anschlüsse mit den USB- und Videoports auf der Benutzerstation.

   Wenn es sich bei dem System um ein zwei- oder dreischichtiges System handelt, muss die Paragon II Benutzerstation an die Basiseinheit (erste Schicht) angeschlossen sein.

3. Schließen Sie die Paragon II User-Station mithilfe eines UTP-Kabels (Kat. 5) mit einer Länge von maximal 45 m an ein KX IIIGerät an.
   - Schließen Sie ein Ende des Kabels an den RJ-45-Port des DCIMs und das andere Kabelende an einen Kanalport auf dem KX III Gerät an.
4. Wenn Sie mehrere Zugriffspfade zum selben Paragon II-System in KX III oder CC-SG benötigen, wiederholen Sie die Schritte 1 bis 3, um zusätzliche User-Stationen an KX III anzuschließen.

Anhang C Verwaltung von KX III in dcTrack

In diesem Kapitel

Überblick

dcTrack® von Raritan ist eine komplette Rechenzentrum-Infrastruktur-Management-Lösung (DCIM), die Informationen über Ihre Einrichtungen, Netzwerke und IT in Echtzeit bietet.

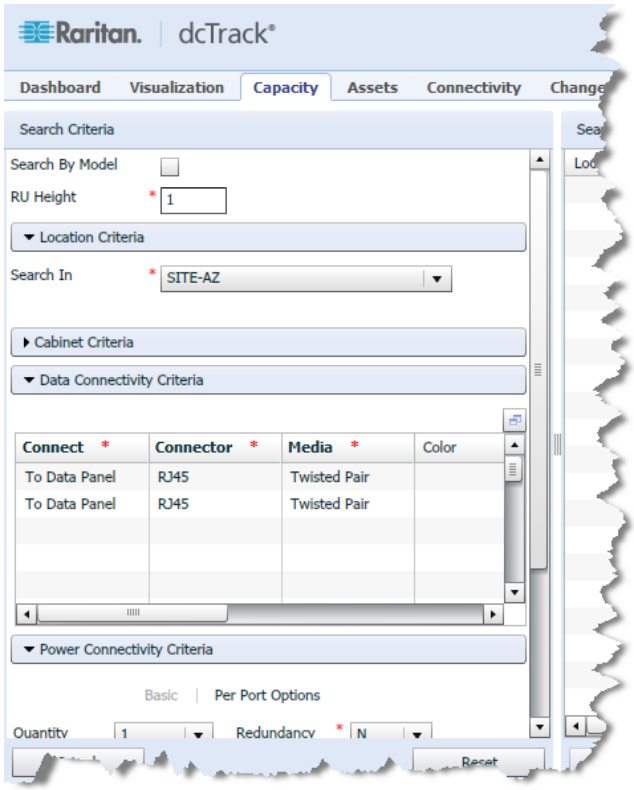
dcTrack visualisiert Ihre Infrastruktur von Rechenzentren und Einrichtungs-Manager verwalten die Platzierung von IT-Geräten, informieren über die Kapazitätsmanagement-Entscheidungen und bieten immer eine genaue Übersicht über Rechenzentrums-Ressourcen wie KX III.

Platz in einem Kabinett für KX III lokalisieren

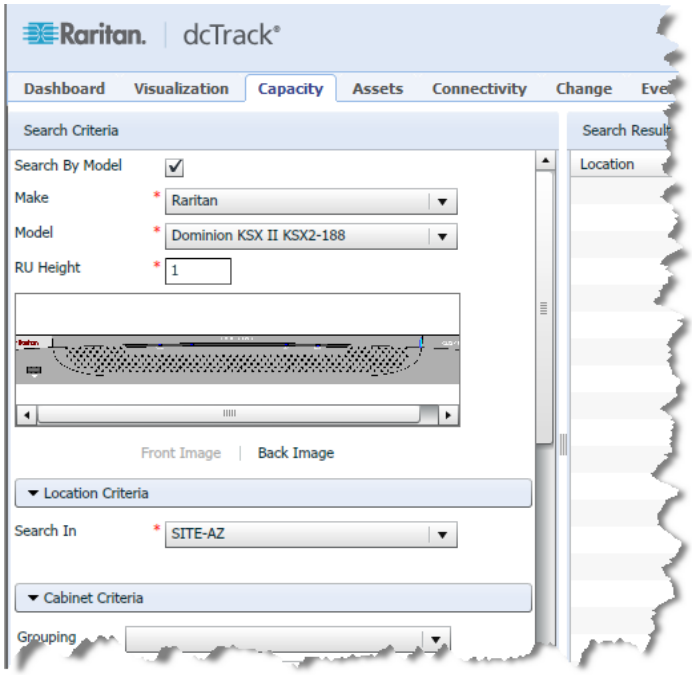
Verwenden Sie die Funktionalität von dcTrack Kapzität-Management, um genug Platz für Ihr KX III im Kabinett zu finden.

Suche nach:

- Rack-Einheiten - dcTracks sucht nach einem Kabinett mit genug öffenen Rack-Einheiten für KX III.



- Herstellen und Gestalten - dcTrack sucht nach einen Kabinett mit genügend Platz auf Grund der KX III Abmessungen, Anschlüsse und so weiter.



Siehe, **Kapazität-Management - Lokalisiert und Speichert den Kabinett-Platz für einen Artikel**in **dcTrack Hilfe**.

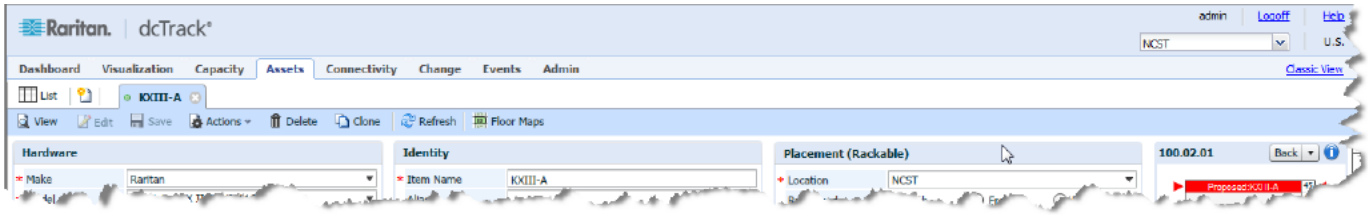
KX III Geräte zu dcTrack hinzufügen

Verwalten Sie KX III Geräte in dcTrack®, indem Sie sie zu einer Anwendung hinzufügen.

Es gibt verschiedene Möglichkeiten, Geräte zur dcTrack hinzuzufügen.

KX III zu dcTrack manuell hinzufügen

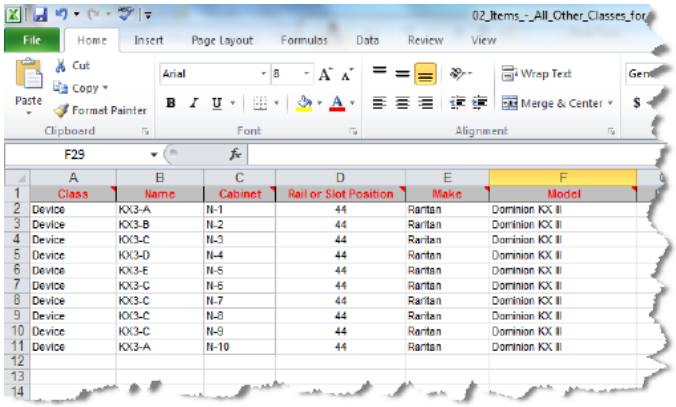
Fügen Sie ein KX III manuell hinzu, wenn Sie ein oder nur ein paar Geräte hinzufügen



Neue Elemente in dcTrack manuell in **dcTrack Hilfe**erstellen..

KX III Geräte in dcTrack importieren

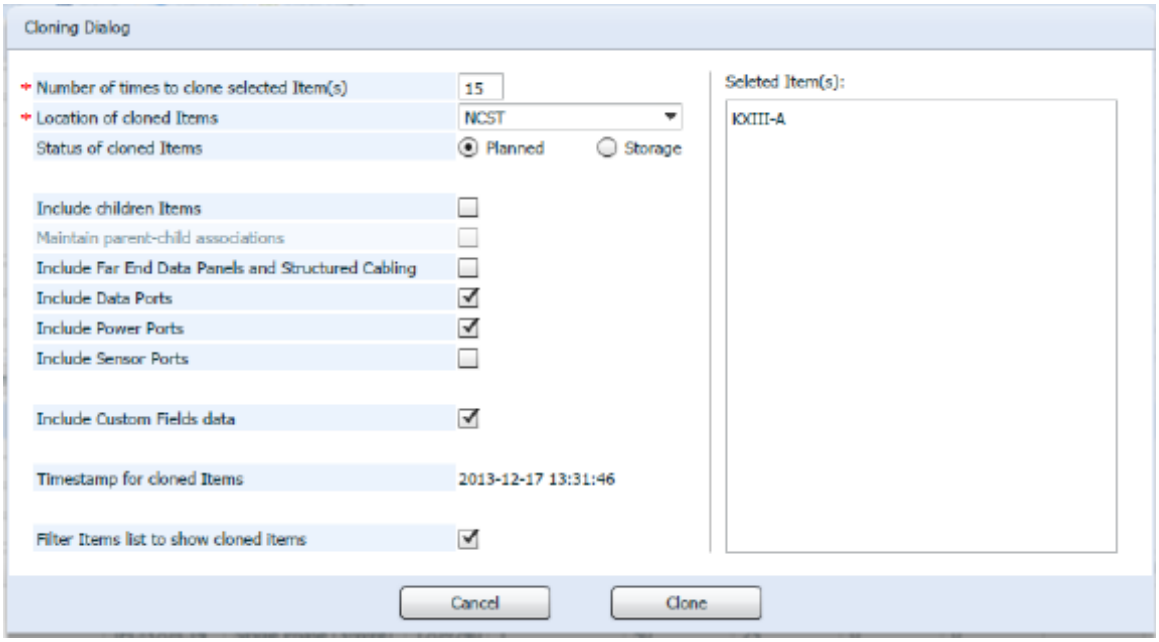
Wenn Sie eine große Anzahl von KX III hinzufügen, füllen Sie die 02_Items_-_All_Other_Classes_for_3.x.xls Tabellenkalkulation - die von Raritan vorgesehen ist - mit den KX III Informationen, und importieren Sie dann die Tabelle in dcTrack ® mit dem Import-Assistenten.



Siehe **neue Elemente zu dcTrack mit dem Import-Wizard hinzufügen,** in **dcTrack Hilfe**.

Vorhandene KX III Geräte klonen

Verwenden Sie Klonen, wenn Sie einen KX III hinzugefügt haben und ihn zusammen mit seinen Strom-und Daten Schaltungen (falls Sie sie erstellt haben), Ports, benutzerdefinierten Feldern und so weiter, klonen wollen.



Beachten Sie, dass das gesamte Gehäuse, zusammen mit den Elementen in der Box und deren Verbindungen und abhängigen Geräten auch gekont werden können.

Wenn Sie einen KX III zu einem Kabinett hinzugefügt haben und die gleiche Kabinettkonfiguration in Ihrem Rechenzentrum verwenden, können Sie das Kabinett klonen.

Erstellung von neuen Elementen und Kabinetten mit Klonverfahrenin**dcTrack Hilfe**.

Daten und Stromversorgung für KX III erstellen

Sobald der KX III in dcTrack® existiert, erstellen Sie die Dateien und Stromversorgung dafür.

Schaltungen können erstellt werden, wenn Sie KX III hinzufügen.

Nachdem die Schaltungen erstellt worden sind, reichen Sie eine Anfrage ein, um sie in dem Datenzentrum zu erstellen.

Siehe **Neue Stromkreise für Elemente bauen** in **dcTrack Hilfe.**

Artikel hinzufügen für KX III einreichen

Sobald Sie KX III zu dcTrack® hinzugefügt haben, reichen Sie eine Installierungs-Anfrage ein.

Die Anfrage löste die Änderungssteuerungsprozesse aus, beginnend mit einem Arbeitsauftrag, um KX III im Datenzentrum physisch zu installieren.

Siehe, **"Artikel Installieren"-Anfrage aus dem Aktion-Menü** in **dcTrack Hilfe**.

Verwaltung von KX III Arbeitsauftrag

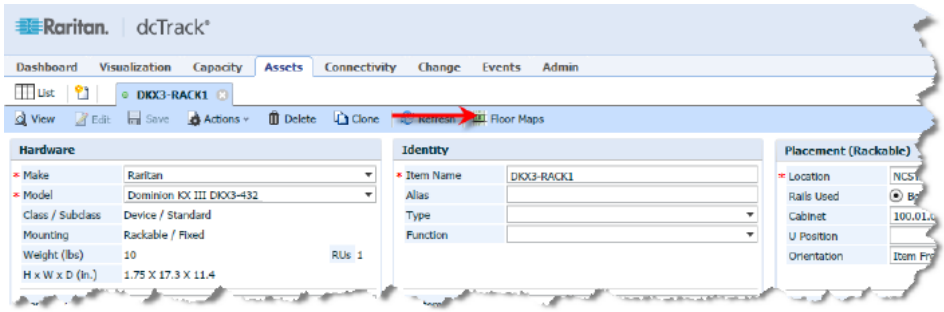
Sofern der Bypass-Modus aktiviert ist, in welchem Fall dcTrack® den Änderungskontrollprozess einer Artikelanfrage nicht verwaltet, wird der Arbeitsauftrag von dcTrack Gatekeeper verwaltet.

Siehe, **Arbeitsaufträge verwalten** oder **Bypass-Anforderung** in **dcTrack Hilfe**.

KX III in Kabinettelevation und auf dem Lageplan visualisieren

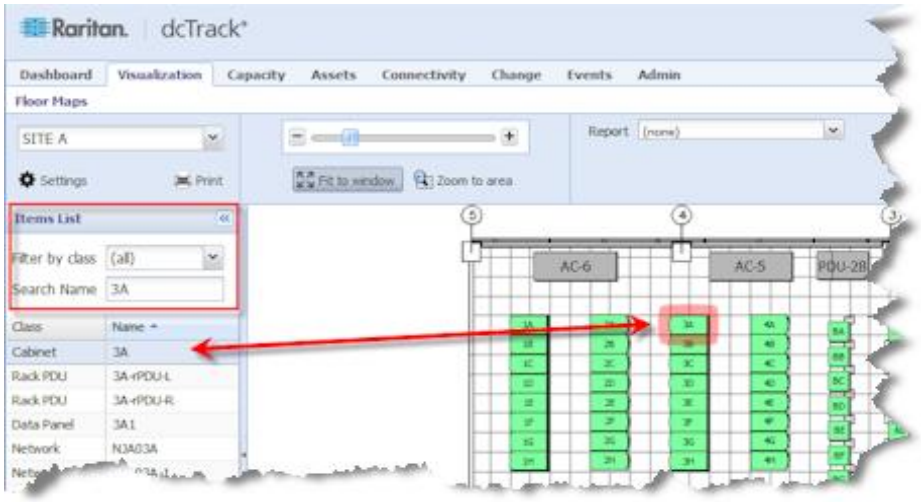
Wenn Sie KX III zu dcTrack ® hinzufügen, können Sie es in einem Kabinett platzieren.

Falls zu dem Standort des Rechenzentrums ein Lageplan gehört und das Kabinett, indem sich das KX III befindet, mit einem Kabinettobjekt auf dem Lageplan verknüpft ist, können Sie auf diesen Lageplan von der KX III Seite in dcTrack zugreifen.



Siehe **Öffnen eines Lageplans von einer Artikel-Seite** in **dcTrack Hilfe**.

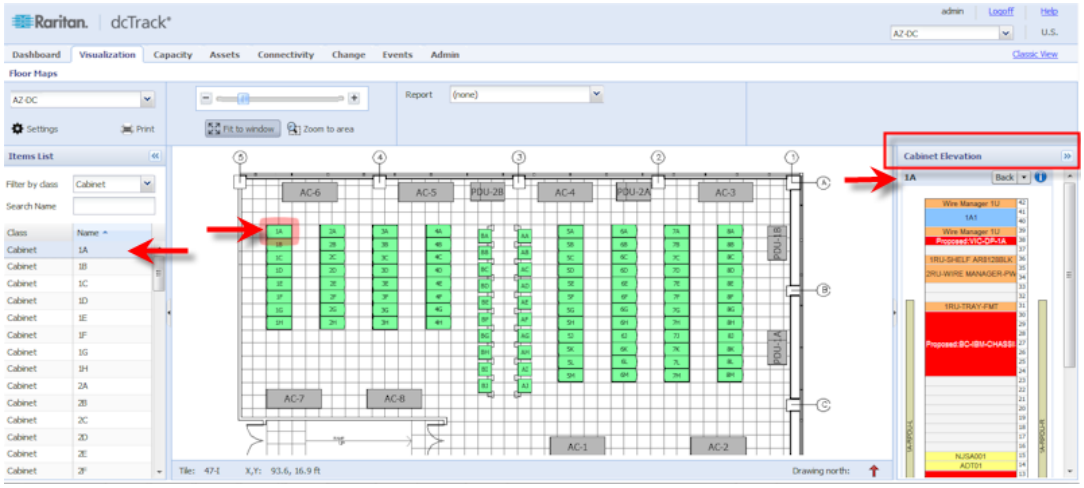
Sobald Sie auf der Lageplan-Seite sind, sehen Sie sich den Standort des KX III Kabinetts an.



Raritan.

Siehe **Artikel auf dem Lageplan und der Artikelliste lokalisieren** in **dcTrack Hilfe**.

Sie können sich KX III auch in der Kabinettelevation aus dem Lageplan anschauen.



Siehe **Kabinettelevationen - Lageplan (Web-Client)** in **dcTrack Hilfe**.

Verwaltung von KX III Lebenszyklus

Sobald der KX III installiert wird, wird sein Zyklus in Ihrem Rechenzentrum verwaltet.

KX III verschieben

Anfrage einreichen, um KX III zu verschieben:

- Von einem Kabinett zu einem anderen Kabinett
- Von einem Standort zu einem anderen Standort
- Von einer Position zu einer anderen Position

Siehe **Anfragen in Bezug auf die Verschiebung eines Artikels** in **dcTrack Hilfe**.

Schaltet die Stromversorgung von KX III ein oder aus.

Anfragen zum Ein-und Ausschalten der Stromversorgung von KX III einreichen, wenn benötigt.

Siehe **Anfragen zum Ein-und Ausschalten der Stromversorgung einreichen** in **dcTrack Hilfe**.

Schaltet einen KX III ein oder aus.

Anfragen zum Ein-und Ausschalten des KX III einreichen, zum Beispiel, wenn es vorübergehend aus Wartungsgründen entfernt ist.

Siehe **Anfragen einreichen, um Artikel auf der Seite annzuehmen und zu entfernen,** in **dcTrack Hilfe**.

KX III aus dem Inventar entfernen

Reichen Sie eine Anfrage ein, wenn Sie das KX III vorübergehend entfernen möchten.

Siehe **Anfrage einreichen, um einen Artikel aus dem Invantar zu entfernen** in **dcTrack Hilfe**.

Außerbetriebnahme eines KX III, um es zu archivieren

Reichen Sie eine Anfrage ein, um das KX III Ausserbetrieb zu setzen, wenn Sie es aus Ihrem Inventar entfernen möchten.

Siehe **Außerbetriebnahme eines installierten Artikels, um ihn zu archivieren,** in **dcTrack Hilfe**.

Anhang D Technische Daten

In diesem Kapitel

Hardware

KX III Abmessungen und physische Spezifikationen

Dominion KX III Modell	Beschreibung	Stromversorgung und Wärmeableitung	Abmessungen (B x T x H)	Gewicht	Bedienungs-Temperatur	Luftfeuchtigkeit
DKX3-108	▪ 8 Serverports ▪ 1 Remote-Benutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll 439x334x44 mm	8.60lbs 3,9 kg	0º - 45º C 32º - 113º F	0% bis 85% relative Luftfeuchtigkeit
DKX3-116	▪ 16 Serverports ▪ 1 Remote-Benutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll 439x334x44 mm	8.60lbs 3,9 kg	0º - 45º C 32º - 113º F	0% bis 85% relative Luftfeuchtigkeit
DKX3-132	▪ 32 Serverports ▪ 1 Remote-	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W	17,3 Zoll x 13,15 Zoll x 1,73 Zoll 439x334x44 mm	8.60lbs 3,9 kg	0º - 45º C 32º - 113º F	0% bis 85% relative Luftfeuchtigkeit

Dominion KX III Modell	Beschreibung	Stromversorgung und Wärmeableitung	Abmessungen (B x T x H)	Gewicht	Bedienungs-Temperatur	Luftfeuchtigkeit
	Benutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	52 KCAL				
DKX3-216	▪ 16 Serverports ▪ 2 Remote-Benutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll	9.08lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x334x44 mm	4,12 kg	32º - 113º F	
DKX3-232	▪ 32 Serverports ▪ 2 Fernbenutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll	9.08lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x334x44 mm	4,12 kg	32º - 113º F	
DKX3-416	▪ 16 Serverports ▪ 4 Fernbenutzer ▪ 1 lokaler Port für Verwendung am Serversc	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll	9.08lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x334x44 mm	4,12 kg	32º - 113º F	

Dominion KX III Modell	Beschreibung	Stromversorgung und Wärmeableitung	Abmessungen (B x T x H)	Gewicht	Bedienungs-Temperatur	Luftfeuchtigkeit
	hrank					
DKX3-432	▪ 32 Serverports ▪ 4 Remote-Benutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll	9.08lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x334x44 mm	4,12 kg	32º - 113º F	
DKX3-464	▪ 64 Serverports ▪ 4 Fernbenutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,3 Zoll x 3,5 Zoll	12.39lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x338x89 mm	5,62 kg	32º - 113º F	
DKX3-808	▪ 8 Serverports ▪ 8 Fernbenutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,15 Zoll x 1,73 Zoll	9.96lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x334x44 mm	4,52 kg	32º - 113º F	
DKX3-832	▪ 32 Serverports ▪ 8 Remote-	Zwei Netzteile 110V/240V, 50-60Hz	17,3 Zoll x 13,15 Zoll x 1,73 Zoll	9.96lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit

Dominion KX III Modell	Beschreibung	Stromversorgung und Wärmeableitung	Abmessungen (B x T x H)	Gewicht	Bedienungs-Temperatur	Luftfeuchtigkeit
	Benutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	1.8A 60W 52 KCAL	439x334x44 mm	4,52 kg	32º - 113º F	
DKX3-864	▪ 64 Serverports ▪ 8 Fernbenutzer ▪ 1 lokaler Port für Verwendung am Serverschrank	Zwei Netzteile 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3 Zoll x 13,3 Zoll x 3,5 Zoll	12.39lbs	0º - 45º C	0% bis 85% relative Luftfeuchtigkeit
			439x338x89 mm	5,62 kg	32º - 113º F	

KX III Unterstützte Bildauflösung der Zielserver

- 640x350@70Hz
- 640x350@85Hz
- 640x400@56Hz
- 640x400@84Hz
- 640x400@85Hz
- 640x480@60Hz
- 640x480@66.6Hz
- 640x480@72Hz
- 640x480@75Hz
- 640x480@85Hz
- 720x400@70Hz
- 720x400@84Hz
- 720x400@85Hz
- 800x600@56Hz
- 800x600@60Hz
- 800x600@70Hz
- 800x600@72Hz
- 800x600@75Hz
- 800x600@85Hz
- 800x600@90Hz
- 800x600@100Hz
- 832x624@75.1Hz
- 1024 x 768 Pixel, 60 Hz
- 1024 x 768 Pixel, 70 Hz
- 1024x768@72Hz
- 1024 x 768 Pixel, 85 Hz
- 1024 x 768 Pixel, 75 Hz
- 1024x768@90Hz
- 1024x768@100Hz
- 1152x864@60Hz
- 1152x864@70Hz
- 1152x864@75Hz
- 1152x864@85Hz
- 1152x870@75.1Hz
- 1.280 x 720 bei 60Hz

- 1280x960@60Hz
- 1280x960@85Hz
- 1280 x 1024 Pixel, 60 Hz
- 1280x1024@75Hz
- 1280x1024@85Hz
- 1.360 x 768 bei 60Hz
- 1.366 x 768 bei 60Hz
- 1.368 x 768 bei 60Hz
- 1.400 x 1050 bei 60Hz
- 1.440 x 900 bei 60Hz
- 1600 x 1200 @ 60 Hz
- 1.680 x 1.050 bei 60Hz
- 1920 x 1080 bei 60Hz

KX III Unterstützte Bildauflösung der Zielserver, Verbindungsdistanz und Bildwiederholungsfrequenz - KX III

Die maximal unterstützte Distanz hängt von mehreren Faktoren ab. Dazu gehören der Typ/die Qualität des Kabels der Kategorie 5, der Servertyp und -hersteller, der Videodriver und Monitor, die Umgebungsbedingungen und die Erwartungen des Benutzers.

In der folgenden Tabelle wird die maximale Entfernung zum Zielserver für verschiedene Videoauflösungen und Aktualisierungsfrequenzen angegeben:

Bildauflösung der Zielserver	Maximale Entfernung
1024x768@60Hz (und unter)	150' (45 m)
1280 x 1024 Pixel, 60 Hz	100' (30 m)
1280×720@60Hz	75' (22 m)
1600 x 1200 @ 60 Hz	50' (15 m)
1920 x 1080 bei 60Hz	50' (15 m)

Von KX III unterstützte Videoauflösungen finden Sie unter ***Unterstützte Videoauflösungen*** (siehe "***KX III Unterstützte Bildauflösung der Zielserver***" auf Seite 347).

Hinweis: Aufgrund der Vielzahl an Serverherstellern und -typen, Betriebssystemversionen, Videodriver usw. sowie der subjektiven Auffassung von Videoqualität kann Raritan nicht für die Leistung bei allen Distanzen in allen Umgebungen garantieren.

Unterstützte Lokale KX III Port-DVI-Auflösung

- 1920x1080@60
- 1280x720@60
- 1024x768@60 (Standard)
- 1024x768@75
- 1280x1024@60
- 1280x1024@75
- 1600x1200@60
- 800x480@60
- 1280x768@60
- 1366x768@60
- 1360x768@60
- 1680x1050@60
- 1440x900@60

Spezifikationen der unterstützten Computer Interface Modules (CIMs)

Digitale CIMs unterstützen Display Data Channels (DDC) und Enhanced Extended Display Identification Data (E-EDID).

CIM-Modell	Beschreibung	Abmessungen (B x T x H)	Gewicht
D2CIM-DVUSB	Dualer USB-CIM für virtuelle Medien auf BIOS-Ebene, Smartcard/CAC, Audio und Absolute Mouse Synchronization (Absolute Maussynchronisierung) 	43 x 90 x 19 mm	0,11 kg
D2CIM-VUSB	USB-CIM für virtuelle Medien und Absolute Mouse Synchronization (Absolute Maussynchronisierung)	33 x 76 x 15 mm	0,09 kg

CIM-Modell	Beschreibung	Abmessungen (B x T x H)	Gewicht
			
D2CIM-DVUSB-DVI	Digitales CIM mit digital-zu-analoger Konvertierung und Unterstützung für virtuelle Medien, Smartcard/CAC, Audio, Absolute und Relative Mouse Synchronization (Absolute und relative Maussynchronisierung) 	43 x 90 x 19 mm	0,11 kg
D2CIM-DVUSB-DP	Digitales CIM mit digital-zu-analoger Konvertierung und Unterstützung für virtuelle Medien, Smartcard/CAC, Audio, Absolute und Relative Mouse Synchronization (Absolute und relative Maussynchronisierung) 	43 x 90 x 19 mm	0,11 kg

CIM-Modell	Beschreibung	Abmessungen (B x T x H)	Gewicht
D2CIM-DVUSB-HDMI	Digitales CIM mit digital-zu-analoger Konvertierung und Unterstützung für virtuelle Medien, Smartcard/CAC, Audio, Absolute und Relative Mouse Synchronization (Absolute und relative Maussynchronisierung) 	43 x 90 x 19 mm	0,11 kg
DCIM-PS2	CIM für PS2 	33 x 76 x 15 mm	0,09 kg
DCIM-USBG2	CIM für USB und Sun-USB 	33 x 76 x 15 mm	0,09 kg

Der schwarze Anschluss am DVUSB CIM wird zum Anschließen von Maus und Tastatur verwendet. Der graue Anschluss wird für virtuelle Medien verwendet.

Achten Sie darauf, dass immer beide Anschlüsse des CIM mit dem Gerät verbunden sind. Es ist möglich, dass das Gerät nicht ordnungsgemäß funktioniert, wenn nicht alle Stecker an den Zielserver angeschlossen sind.

Unterstütztes Digital Video CIMs für Mac

Verwenden Sie einen digitalen Video CIM, um zu den folgenden Mac ® Ports zu verbinden:

Mac Port	CIM
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort oder Thunderbolt	D2CIM-DVUSB-DP

Wenn der Mac-HDMI-oder Displayport-Video einen Mini-Anschluss hat, kann ein passives Adapter-Kabel erforderlich sein, um die Vollgröße HDMI und Displaystecker an den digitalen CIM anzuschließen.

Anderenfalls können Sie den Mac-VGA-Adapter mit dem D2CIM-VUSB oder D2CIM-DVUSB verwenden. Beachten Sie, dass diese möglicherweise weniger zuverlässig sind und die Videoqualität daran leiden kann.

Für Informationen über die etablierten Modi, die von KX III 2.5.0 (und höher) für Mac unterstützt werden, siehe ***Digital CIM bewährte und standardmäßige Modi*** (auf Seite 352).

Digital CIM Zeitabstimmungsmodi

Die folgenden standardmäßigen Zeitabstimmungsmodi werden verwendet, wenn KX III über ein digitales CIM mit einer Videoquelle kommuniziert.

Die verwendeten Zeitabstimmungsmodi hängen von der systemeigenen Auflösung der Videoquelle ab.

- 1920 x 1080 bei 60Hz
- 1600 x 1200 @ 60 Hz
- 1280 x 1024 @ 60 Hz (Standardauflösung für digitale CIMs)
- 1.440 x 900 bei 60Hz
- 1024 x 768 Pixel, 60 Hz

Siehe ***Konfigurieren von CIM-Ports*** (auf Seite 98) weitere Informationen finden Sie online.

Digital CIM Bewährte und standardmäßige Modi

Die folgenden zusätzlichen bewährten und standardmäßigen Auflösungs- und Zeitabstimmungsmodi werden von KX III 3.0.0 (und höher) unterstützt.

Digital CIM Bewährte Modi

- 720x400@70Hz IBM, VGA
- 640x480@60Hz IBM, VGA
- 640x480@67Hz Apple Mac® II
- 640x480@72Hz VESA
- 640x480@75Hz VESA
- 800x600@56Hz VESA
- 800x600@60Hz VESA
- 800x600@72Hz VESA
- 800x600@75Hz VESA
- 832x624@75Hz Apple Mac II
- 1024x768@60Hz VESA
- 1024x768@70Hz VESA
- 1024x768@75Hz VESA
- 1280x1024@75Hz VESA
- 1152x870@75Hz Apple Mac II

Digital CIM Standardmäßige Modi

- 1152 x 864 @ 75 Hz VESA
- 1280 x 960 @ 60 Hz VESA
- 1280 x 1024 @ 60 Hz VESA
- 1360 x 768 @ 60 Hz VESA
- 1400 x 1050 @ 60 Hz VESA
- 1440 x 900 @ 60 Hz VESA
- 1600 x 1200 @ 60 Hz VESA
- 1680 x 1050 @ 60 Hz VESA
- 1920 x 1080 @ 60 Hz VESA

DVI-Kompatibilitätsmodus

Der DVI-Kompatibilitätsmodus wird verwendet, wenn Sie ein HDMI CIM verwenden, um die Verbindung über eine Intel-Videokarte oder einen Mac® Mini mit einem HDMI-Controller zu einem Dell Optiplex-Zielgerät herzustellen.

Die Auswahl dieses Modus gewährleistet eine gute Videoqualität von den Zielgeräten.

Siehe ***Konfigurieren von CIM-Ports*** (auf Seite 98) In Online-Hilfe.

Unterstützte Remoteverbindungen

Remoteverbindung	Details
Netzwerk	10BASE-T-, 100BASE-T- und 1000BASE-T (Gigabit)-Ethernet
Protokolle	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Netzwerk-Geschwindigkeitseinstellungen

Netzwerk-Geschwindigkeitseinstellung von KX III

Porteinstellung Netzwerkswitch		Automatisch	1000/Voll	100/Voll	100/Halb	10/Voll	10/Halb
	Automatisch	Höchste verfügbare Geschwindigkeit	1000/Voll	KX III: 100/Voll Switch: 100/Halb	100/Halb	KX III: 10/Voll Switch: 10/Halb	10/Halb
	1000/Voll	1000/Voll	1000/Voll	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation
	100/Voll	KX III: 100/Halb Switch: 100/Voll	KX III: 100/Halb Switch: 100/Voll	100/Voll	KX III: 100/Halb Switch: 100/Voll	Keine Kommunikation	Keine Kommunikation
	100/Halb	100/Halb	100/Halb	KX III: 100/Voll Switch: 100/Halb	100/Halb	Keine Kommunikation	Keine Kommunikation
	10/Voll	KX III: 10/Halb Switch: 10/Voll	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	10/Voll	KX III: 10/Halb Switch: 10/Voll
	10/Halb	10/Halb	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	KX III: 10/Voll Switch: 10/Halb	10/Halb

Legende:

Funktioniert nicht wie erwartet

Unterstützt

Funktionen; nicht empfohlen

NICHT von Ethernet-Spezifikationen unterstützt; Produkt kommuniziert, es treten allerdings Kollisionen auf.

Laut Ethernet-Spezifikation sollte hier "Keine Kommunikation" gelten, beachten Sie jedoch, dass das Verhalten des KX III vom erwarteten Verhalten abweicht.

Hinweis: Um eine zuverlässige Netzwerkkommunikation zu erhalten, konfigurieren Sie LAN-Schnittstellengeschwindigkeit und Duplex für KX III und den LAN-Switch auf den gleichen Wert. Konfigurieren Sie beispielsweise KX III und den LAN-Switch auf "Autodetect" (Automatische Erkennung, empfohlen) oder stellen Sie sie auf eine festes Geschwindigkeit/Duplex wie 100MB/s/Voll.

Kabellängen und Videoauflösungen für Dell-Chassis

Um gute Videoqualität zu erreichen, empfiehlt Raritan die Verwendung der folgenden Kabellängen und Videoauflösungen, wenn Sie von KX III eine Verbindung mit Dell® Blade-Chassis herstellen:

Videoauflösung	Kabellänge
1024 x 768 Pixel, 60 Hz	50' (15,24 m)
1280 x 1024 Pixel, 60 Hz	50' (15,24 m)
1600 x 1200 @ 60 Hz	30' (9,14 m)

Mindestanforderungen an Smart Cards

Anforderungen für den lokalen Port

Die grundlegende Kompatibilitätsanforderung für die Nutzung des lokalen Ports von KX III ist:

- Alle Geräte (Smart Card-Lesegeräte oder Token), die lokal angeschlossen werden, müssen USB CCID-konform sein.

Zielserver-Anforderungen

Die grundlegenden Kompatibilitätsanforderungen für die Verwendung von Smart Card-Lesegeräten am Zielserver sind:

- Der IFD-Handler (Smart Card-Lesegerät) muss ein standardmäßiger USB CCID-Gerätedriver sein (vergleichbar mit dem allgemeinen Microsoft USB CCID-Driver).
- Ein digitales CIM oder ein D2CIM-DVUSB (Dual-VM CIM) mit Firmwareversion 3A6E oder höher ist erforderlich.
- Wo ein CIM pro Blade verwendet wird, werden Blade-Chassis-Serververbindungen unterstützt.
- Blade-Chassis-Serververbindungen mit einem CIM pro Chassis werden nur für die IBM® BladeCenter® Modelle H und E mit aktivierter automatischer Erkennung unterstützt.

Windows XP-Ziele

Windows XP®Betriebssystemziele müssen auf Windows XP SP3 laufen, um Smart Cards mit KX III zu verwenden. Wenn Sie .NET 3.5 in einer Windows XP-Umgebung auf dem Zielserver verwenden, müssen Sie SP1 verwenden.

Linux-Ziele

Wenn Sie ein Linux® Ziel verwenden, müssen die folgenden Voraussetzungen erfüllt sein, um Smart Card-Lesegeräte mit dem Raritan-Gerät zu verwenden.

- CCID-Anforderungen

  Wird das Raritan D2CIM-DVUSB VM/CCID von Ihrem Linux-Ziel nicht als Smart Card-Lesegerät erkannt, kann es erforderlich sein, den CCID-Treiber auf die Version 1.3.8 oder höher und die Treiberkonfigurationsdatei (Info.plist) zu aktualisieren.

Betriebssystem	CCID-Anforderungen
RHEL 5	CCID-1.3.8-1.el5
SuSE 11	PCSC-CCID-1.3.8-3.12

Fedora® Core 10	CCID-1.3.8-1.fc10.i386

Remoteclient-Anforderungen

Die grundlegenden Anforderungen für Kompatibilität am Remoteclient sind:

- Der IFD-Handler (Smart Card-Lesegerät) muss ein PC/SC-konformer Gerätetreiber sein.
- Die ICC-Ressourcenverwaltung (Smart Card) muss verfügbar und PC/SC-konform sein.
- Die JRE® Java® 1,7mit Smart Card API muss für die Verwendung durch die Raritan-Client-Anwendung verfügbar sein.

Fern-Linux-Clients-Anforderungen

Wenn Sie Linux® Client benutzen, müssen die folgenden Anforderungen erfüllt werden, um ein Smart Card-Lesegeräte mit dem Raritan-Gerät zu benutzen.

Hinweis: Die Benutzeranmeldung am Client beim Einführen der Karte kann möglicherweise länger dauern, wenn eine oder mehrere aktive KVM-Sitzungen mit Zielen bestehen. Dies ist darauf zurückzuführen, dass der Anmeldeprozess an diese Ziele ebenfalls bearbeitet wird.

- PC/SC-Anforderungen

Betriebssystem	Erforderliches PC/SC-System
RHEL 5	PCSC-Lite-1.4.4-0.1.el5
SuSE 11	PCSC-Lite-1.4.102-1.24
Fedora® Core 10	PCSC-Lite-1.4.102.3.fc10.i386

- Erstellen eines Links zu einer Java®-Bibliothek

  Nach der Aktualisierung von RHEL 4, RHEL 5 und FC 10 muss ein Soft-Link zur libpcsclite.so Datei erstellt werden. Dieser könnte zum Beispiel folgendermaßen aussehen: ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so. Dabei wird davon ausgegangen, dass bei der Installation des Pakets die Bibliotheken in /usr/lib or /user/local/lib abgelegt werden.

- PC/SC-Daemon

  Nachdem der PCSC-Daemon (Ressourcenverwaltung im Framework) neu gestartet wurde, starten Sie den Browser erneut

Unterstützte Smart Card-Lesegeräte

Typ	Anbieter	Modell	Geprüft
USB	SCM Microsystems	SCR331	Geprüft für lokalen und Remotezugriff
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Geprüft für lokalen und Remotezugriff
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Geprüft für lokalen und Remotezugriff
USB	Gemalto®	GemPC USB-SW	Geprüft für lokalen und Remotezugriff
USB-Tastatur mit Kartenlesegerät	Dell®	USB-Tastatur mit Smart Card-Lesegerät	Geprüft für lokalen und Remotezugriff
USB-Tastatur mit Kartenlesegerät	Cherry GmbH	G83-6744 SmartBoard	Geprüft für lokalen und Remotezugriff
USB-Lesegerät für Karten in SIM-Größe	Omnikey	6121	Geprüft für lokalen und Remotezugriff
Integriert (Dell Latitude D620)	O2Micro	OZ776	Nur Remotezugriff
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Nur Remotezugriff
PCMCIA	SCM Microsystems	SCR243	Nur Remotezugriff

Hinweis: SCM Microsystems SCR331 Smart Card-Lesegeräte dürfen nur mit der SCM Microsystems-Firmware v5.25 verwendet werden.

Nicht unterstützte Smart Card-Lesegeräte

In dieser Tabelle finden Sie Lesegeräte, die von Raritan mit dem Raritan-Gerät getestet wurden, nicht funktioniert haben und deshalb nicht unterstützt werden.

Wenn ein Smart Card-Lesegerät nicht in den Listen für unterstützte und nicht unterstützte Lesegeräte aufgeführt ist, bietet Raritan keine Gewähr für die Funktion des Lesegeräts mit dem Gerät.

Typ	Anbieter	Modell	Notizen
USB-Tastatur mit Kartenlesegerät	HP®	ED707A	Kein Interrupt-Endpunkt => nicht mit Microsoft®-Driver kompatibel
USB-Tastatur mit Kartenlesegerät	SCM Microsystems	SCR338	Proprietäre Implementierung eines Kartenlesegeräts (nicht CCID-konform)

Typ	Anbieter	Modell	Notizen
USB-Token	Aladdin®	eToken PRO™	Proprietäre Implementierung

Empfehlungen und Anforderungen für die Audiowiedergabe und -aufnahme

Audiopegel

- Legen Sie den Zielaudiopegel auf eine Einstellung im mittleren Bereich fest.

  Auf einem Windows®Client legen Sie den Audiopegel beispielsweise auf 50 oder niedriger fest.

Diese Einstellung muss über das Wiedergabe- oder Aufnahmeaudiogerät und nicht über die Audiogerätesteuerung des Clients konfiguriert werden.

Empfehlungen für Audioverbindungen bei aktiviertem Modus "PC Share" (PC-Freigabe)

Wenn Sie die Audiofunktion bei aktiviertem Modus "PC Share" (PC-Freigabe) verwenden, werden die Audiowiedergabe und -aufnahme unterbrochen, wenn ein zusätzliches Audiogerät an das Zielgerät angeschlossen wird.

Beispielsweise schließt Benutzer A ein Wiedergabegerät an Ziel1 an und führt eine Anwendung für die Audiowiedergabe aus. Anschließend schließt Benutzer B ein Aufnahmegerät an dasselbe Ziel an. Die Wiedergabesitzung von Benutzer A wird unterbrochen, und die Audioanwendung muss möglicherweise neu gestartet werden.

Die Unterbrechung erfolgt, weil das USB-Gerät mit der neuen Gerätekonfiguration eine neue Nummer erhält.

Es kann einige Zeit dauern, bis ein Treiber für das neue Gerät auf dem Zielgerät installiert ist.

Audioanwendungen können die Wiedergabe vollständig beenden, den nächsten Titel aufrufen oder einfach die Wiedergabe fortsetzen.

Das genaue Verhalten hängt davon ab, wie die Audioanwendung das Trennen/erneute Anschließen handhabt.

Anforderungen an die Bandbreite

Die folgende Tabelle gibt Aufschluss über die Bandbreitenanforderungen für Audiowiedergabe und -aufnahme zum Übertragen von Audiosignalen im Rahmen der einzelnen ausgewählten Formate.

Audioformat	Anforderung an die Netzwerkbandbreite
44,1 KHz, 16 Bit Stereo	176 KB/s
44,1 KHz, 16 Bit Mono	88.2 KB/s
2,05 KHz, 16 Bit Stereo	88.2 KB/s
22,05 KHz, 16 Bit Mono	44.1 KB/s
11,025 KHz, 16 Bit Stereo	44.1 KB/s
11,025 KHz, 16 Bit Mono	Audio 22,05 KB/s

In der Praxis ist die Bandbreite zum Verbinden von Audiogeräten mit einem Ziel höher. Der Grund sind die Tastatur- und Videodaten, die beim Öffnen und Verwenden einer Audioanwendung auf dem Ziel in Anspruch genommen werden.

Als allgemeine Empfehlung gilt, dass mindestens 1,5 MB für die Verbindung verfügbar sein müssen, bevor die Wiedergabe oder Aufnahme erfolgt.

Videoinhalte in hoher Qualität mit Verbindungen ganz in Farbe und hohen Auflösungen des Zielbildschirms nehmen jedoch weitaus mehr Bandbreite in Anspruch und wirken sich erheblich auf die Audioqualität aus.

Um die Qualitätsverschlechterung zu verringern, gibt es eine Reihe von empfohlenen Client-Einstellungen, die die Auswirkung auf die Video- und Audioqualität bei niedrigeren Bandbreiten reduzieren:

- Verbinden Sie die Audiowiedergabe mit den Formaten niedrigerer Qualität. Die Auswirkung der Inanspruchnahme von Bandbreite durch Video ist bei Verbindungen mit 11 K deutlich weniger ausgeprägt als mit 44 K.
- Legen Sie den Wert für die Verbindungsgeschwindigkeit unter "Connection Properties" (Verbindungseigenschaften) entsprechend der Client-zu-Server-Verbindung fest.
- Legen Sie unter "Connection Properties" (Verbindungseigenschaften) die Farbtiefe auf einen möglichst niedrigen Wert fest. Durch Reduzieren der Farbtiefe auf 8-Bit-Farbe wird deutlich weniger Bandbreite in Anspruch genommen.
- Set Smoothing (Glättung, to High. Dies verbessert das Aussehen des Zielgerätbbildes, da dadurch das Videorauschen verringert wird.
- Legen Sie den Rauschfilter unter "Video Settings" (Videoeinstellungen) auf 7 (höchster Wert) fest, sodass für die Änderungen am Zielbildschirm eine niedrigere Bandbreite verwendet wird.

Audiofunktion in einer Mac-Umgebung

Die folgenden Probleme sind in einer Mac®-Umgebung bekannt.

- Bei Mac-Clients wird bei dem Zugriff auf das Gerät über Virtual KVM Client (VKC) nur ein Wiedergabegerät im Fenster "Connect Audio" (Audio verbinden) aufgeführt. Das aufgeführte Gerät ist das Standardgerät und wird im Fenster "Connect Audio" (Audio verbinden) als Java Sound-Audiomodul angezeigt.
- Wenn Sie die Audiofunktion über Skype® auf einem Mac-Ziel verwenden, kann dies dazu führen, dass die Audiosignale verzerrt werden.

Anzahl der unterstützten Audio-/virtuellen Medien- und Smart Card-Verbindungen

Nachfolgend wird die Anzahl der Audio-/virtuellen Medien- und Smart Card-Verbindungen aufgeführt, die gleichzeitig von einem Client mit einem Ziel hergestellt werden können:

- 1 Smart Card-Verbindung
- 1 virtuelle Medienverbindungen
- 1 Smart Card- und 1 virtuelle Medienverbindung
- 2 virtuelle Medienverbindungen

KX III Unterstützte Tastatursprachen

KX III bietet Tastaturunterstützung für die in der folgenden Tabelle aufgeführten Sprachen.

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen KX III Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt. Weitere Informationen zu nicht US-amerikanischen Tastaturen finden Sie unter **Wichtige Hinweise** *(auf Seite 371).*

Hinweis: Raritan empfiehlt Ihnen für Änderungen der Spracheinstellungen die Verwendung von "system-config-keyboard", wenn Sie in einer Linux-Umgebung arbeiten.

Sprache	Regionen	Tastaturlayout
US English (Englisch USA)	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. Kanada, Australien und Neuseeland.	US-amerikanisches Tastaturlayout
US English International (Englisch USA/International)	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. die Niederlande.	US-amerikanisches Tastaturlayout
UK English (Englisch Großbritannien)	United Kingdom (Großbritannien)	Englisches Tastaturlayout (Großbritannien)
Chinese Traditional (Traditionelles Chinesisch)	Hongkong, Republik China (Taiwan)	Chinese Traditional (Traditionelles Chinesisch)

Sprache	Regionen	Tastaturlayout
Chinese Simplified (Vereinfachtes Chinesisch)	Festland der Volksrepublik China	Chinese Simplified (Vereinfachtes Chinesisch)
Korean (Koreanisch)	Südkorea	Dubeolsik Hangul
Japanese (Japanisch)	Japan	JIS-Tastatur (Japanischer Branchenstandard)
French (Französisch)	Frankreich	Französisches (AZERTY-)Tastaturlayout
German (Deutsch)	Deutschland und Österreich	Deutsche Tastatur (QWERTZ-Layout)
French (Französisch)	Belgien	Belgian (Belgisch)
Norwegian (Norwegisch)	Norwegen	Norwegian (Norwegisch)
Danish (Dänisch)	Dänemark	Danish (Dänisch)
Swedish (Schwedisch)	Schweden	Swedish (Schwedisch)
Hungarian (Ungarisch)	Ungarn	Hungarian (Ungarisch)
Slovenian (Slowenisch)	Slowenien	Slovenian (Slowenisch)
Italian (Italienisch)	Italien	Italian (Italienisch)
Spanish (Spanisch)	Spanien und die meisten spanischsprachigen Länder	Spanish (Spanisch)
Portuguese (Portugiesisch)	Portugal	Portuguese (Portugiesisch)

Tastenkombinationen für Mac Mini BIOS

Die folgenden BIOS-Befehle wurden auf Intal-basierten MAC® Mini-Zielservern und Mac Lion® Servern mit Snow Leopard-Betriebssytem getestet. Die Server wurden zu einem KX III mit D2CIM-DVUSB und D2CIM-VUSB CIM angeschlossen. Siehe untenstehend die unterstützten Schlüssel und Hinweise.

Tastenkombination	Beschreibung	Virtual Media CIM	Duale Virtual Media CIM	Mac Lion Server HDMI CIM
Drücken Sie C während Startup	Start von einer bootbaren CD oder DVD, wie Mac OS X Install Disk	✓	✓	
D-Taste während des Startvorgangs drücken	Im Apple Hardware Test (AHT) starten	✓ Kann BIOS Mac Profil für das Funktionieren der Maus benötigen	✓ Kann BIOS Mac Profil für das Funktionieren der Maus benötigen	✓ Kann BIOS Mac Profil für das Funktionieren der Maus benötigen
Wahltaste-Befehlstaste-P-R drücken, bis Sie zum zweiten Mal ein Startsignal hören	NVRAM zurücksetzen		✓	✓
Wahltaste während des Startvorgangs drücken	In Startup Manager starten, indem Sie ein Max OS X-Volume zum Starten auswählen können.	✓	✓	✓
Auswurftaste oder F12 drücken oder Maustaste gedrückt halten	Wirft alle Wechselmedien, wie z. B. optische Datenträger, aus.	✓	✓	
N-Taste während des Startvorgangs drücken	Versucht, von einem kompatiblen Netzwerkserver (NetBoot) zu starten.	✓	✓	✓
T-Taste während des Startvorgangs drücken	Im Festplattenmodus starten			✓
Umschalttaste während des Startvorgangs	Im gesicherten Modus starten und vorübergehende	✓	✓	Bekanntes Problem mit LION, um

Tastenkombination	Beschreibung	Virtual Media CIM	Duale Virtual Media CIM	Mac Lion Server HDMI CIM
drücken	Anmeldungselemente deaktivieren			abgesicherten Modus zu starten. „Sicheres Modus“ in rot erscheint nicht fürLion
Befehlstaste-V während des Startvorgangs drücken	Mit ausführlichem Protokoll starten	✓	✓	✓
Befehlstaste-S während des Startvorgangs drücken	Im Einzelbenutzermodus starten	✓	✓	✓
Auswahltaste-N während des Startvorgangs drücken	Von einem NetBoot-Server mithilfe eines standardmäßigen Startabbilds starten	✓	✓	✓
Befehlstaste-R während des Startvorgangs drücken	Von Lion Recovery1 starten	Nicht zutreffend	Nicht zutreffend	✓

Verwendung von Windows Tastatur zum Zugang von Mac-Zielenn

Eine Windows® Tastatur kann dafür verwendet werden, um einen auf einen Mac® zuzugreifen, der mit KX III verbunden ist. Windows-Tasten werden dann verwendet, um die speziellen Mac-Tasten zu emulieren. Dies ist das gleiche wie die Verbindung einer Windows-Tastatur an den Mac.

Verwendete TCP- und UDP-Ports

Port	Beschreibung
HTTP, Port 80	Dieser Port kann bei Bedarf konfiguriert werden. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 139). Alle von KX III über HTTP (Port 80) empfangenen Anforderungen werden standardmäßig zur Gewährleistung der Sicherheit automatisch an HTTPS weitergeleitet. Der KX III beantwortet Anforderungen aus Gründen der Benutzerfreundlichkeit über Port 80. Auf diese Weise müssen Benutzer

Port	Beschreibung
	für den Zugriff auf KX III im URL-Feld keine Eingaben vornehmen. Die Sicherheit ist jedoch vollständig gewährleistet.
HTTPS, Port 443	Dieser Port kann bei Bedarf konfiguriert werden. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 139). Dieser Port wird standardmäßig für verschiedene Zwecke verwendet, z. B. für den Webserver des HTML-Clients, das Herunterladen von Clientsoftware (Virtual KVM Client (VKC)) auf den Clienthost oder die Übertragung von KVM- oder virtuellen Mediendatenströmen zum Client.
KX III Protokoll (Raritan KVM-über-IP), konfigurierbarer Port 5000	Dieser Port wird zur Erkennung anderer Dominion-Geräte und zur Kommunikation zwischen Raritan-Geräten und -Systemen verwendet, einschließlich CC-SG für Geräte, für die die CC-SG-Verwaltung verfügbar ist. Standardmäßig ist der Port 5000 eingestellt. Sie können jedoch jeden anderen TCP-Port konfigurieren, der nicht verwendet wird. Informationen zum Konfigurieren dieser Einstellung finden Sie unter ***Netzwerkeinstellungen*** (siehe "***Network Settings (Netzwerkeinstellungen)***" auf Seite 86).
SNTP (Zeitserver) über den konfigurierbaren UDP-Port 123	Der KX III bietet optional die Möglichkeit, die interne Uhr mit einem zentralen Zeitserver zu synchronisieren. Diese Funktion erfordert die Verwendung des UDP-Ports 123 (Standardport für SNTP), sie kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
LDAP/LDAPS über den konfigurierbaren Port 389 oder 936	Wenn der KX III zur Remoteauthentifizierung von Benutzeranmeldungen über das LDAP-/LDAPS-Protokoll konfiguriert ist, wird Port 389 oder 636 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden.**Optional**
RADIUS über den konfigurierbaren Port 1812	Wenn der KX III zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist, wird Port 1812 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
RADIUS-Kontoführung über den konfigurierbaren Port 1813	Wenn der KX III zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist und auch die RADIUS-Kontoführung zur Ereignisprotokollierung verwendet, wird Port 1813 oder ein zusätzlicher Port Ihrer Wahl zur Übertragung von Protokollbenachrichtigungen verwendet.
SYSLOG über den konfigurierbaren UDP-Port 514	Wenn der KX III zum Senden von Meldungen an einen Syslog-Server konfiguriert ist, werden die angegebenen Ports für die Kommunikation verwendet (verwendet UDP-Port 514).
SNMP-Standard-UDP-Ports	Port 161 wird für eingehende/ausgehende SNMP-Lese- und -Schreibvorgänge, Port 162 für ausgehenden Datenverkehr für SNMP-Traps verwendet. **Optional**

Port	Beschreibung
TCP-Port 22	Port 22 wird für die Kommandozeilenschnittstelle des KX III verwendet (wenn Sie mit dem technischen Kundendienst von Raritan zusammenarbeiten).
SSH	(Secure Shell) SSH-Port kann konfiguriert werden. Der Standard-Port lautet 22.

Software

Unterstützte Betriebssysteme und Browser

Betriebssysteme	Suchprogramme
Windows 7® Home Premium SP1 64-bit	▪ Internet Explorer® 10 und 11 ▪ Firefox® 25 ▪ Chrome® 31 ▪ Safari® 5.1.7
Windows 7 Ultimate SP1 64-bit	▪ Internet Explorer 8,9,11 ▪ Firefox 25 ▪ Chrome 31
Windows 7 Ultimate 32-bit	▪ Internet Explorer 8 ▪ Firefox 25 ▪ Chrome 31
Windows 8® 64-bit	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
Windows Server 2012® Standard 64-bit	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
Windows XP® Home Edition mit SP 3	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
openSUSE® 11.4 Celadon (x86_64)	▪ Firefox 16.0.2
Fedora® 18 (Speherical Cow)	▪ Firefox 24
RHEL 6.4	▪ Firefox 21
OS X Mountain Lion® 10.8.5 *	▪ Firefox 25 (empfohlen) ▪ Safari 6.1

Betriebssysteme	Suchprogramme
Solaris® 10 64-bit	▪ Firefox 3.6.23
Mac® 10.7.5	▪ Safari 6.0.5 ▪ Firefox 25

**Hinweis: Nach der Aktualisierung von OS X 10.8.2 auf OS X 10.8.3, Safari®, kann Java™ blockiert werden.*

Java Anforderungen und Browser-Berücksichtigungen für Mac

Java Runtime Umgebungsanforderungen installieren

Installieren Sie Java Runtime Umgebungsanforderungen 7 (JRE)® auf PCs und Macs® , wenn Virtual KVM Client (VKC) zum Zugriff des Zielservers via KX III verwendet wird.

Dies gewährleistet eine hohe Leistung und die KVM-over-IP-Video-Verarbeitung beim Remote-Zugriff auf die Zielserver / PCs / Macs.

Die neueste Version der JRE für Mac kann von der Apple-Support-Webseite heruntergeladen werden.

Browser-Berücksichtigungen für Mac

Java kann standardmäßig in bestimmten Browsern deaktiviert sein. Bitte aktivieren Sie Java und alle Sicherheitswarnungen, um KX III zu verwenden.

Einige Versionen von Safari ® blockieren Java aus Sicherheitsgründen. Da Java benötigt wird, um KX III zu verwenden, empfiehlt Raritan die Verwendung von Firefox ®.

Darüber hinaus kann es erforderlich sein, durch eine Reihe von Meldungen zu navigieren. Wählen Sie „Nicht Blockieren“, wenn diese Nachrichten angezeigt werden.

Java und Microsoft .NET Anforderungen

Java® 1.7 (oder höher) oder Microsoft .NET® 3.5 (oder höher) ist für die Verwendung von KX III erfoderlich.

KX III überprüft Ihre aktuelle Java-Version und fordert zu einer Aktualisierung auf, wenn es nicht mehr kompatibel ist.

Siehe ***Java Runtime Environment (JRE) Notizen*** (siehe "***Java Runtime Environment (JRE) Hinweise***" auf Seite 371) für weitere Informationen.

Mehrsprachige Tastatur JRE Anforderung

Damit mehrsprachige Tastaturen in KX III und Virtual KVM Client funktionieren, müssen Sie die mehrsprachige Version von JRE™ installieren.

Im Prüfprotokoll und im Syslog erfasste Ereignisse

In der folgenden Liste werden die Ereignisse mit Beschreibung aufgeführt, die im Prüfprotokoll und Syslog von KX III erfasst werden:

- Access Login (Zugriffsanmeldung) – Ein Benutzer hat sich bei KX III angemeldet.
- Access Logout (Zugriffsabmeldung) – Ein Benutzer hat sich von KX III abgemeldet.
- Active USB Profile (Aktives USB-Profil) – Das USB-Profil ist aktiv.
- CIM Connected (CIM angeschlossen) – Ein CIM wurde angeschlossen.
- CIM Disconnected (CIM getrennt) – Ein CIM wurde getrennt.
- Connection Lost (Verbindung unterbrochen) – Die Verbindung mit dem Ziel wurde unterbrochen.
- Disconnected User (Getrennter Benutzer) – Ein Benutzer wurde von einem Port getrennt.
- End CC Control (CC-Steuerung beenden) – Die CC-SG-Verwaltung wurde beendet.
- Login Failed (Anmeldung fehlgeschlagen) – Es trat ein Fehler bei der Benutzeranmeldung auf.
- Password Changed (Kennwort geändert) – Das Kennwort wurde geändert.
- Port Connect (Port verbunden) – Die Verbindung zu einem Port wurde hergestellt.
- Port Disconnect (Port getrennt) – Die Verbindung zum Port wurde getrennt.
- Port Status Change (Änderung des Portstatus) – Der Portstatus wurde geändert.
- Scan Started (Scanvorgang gestartet) – Ein Zielscanvorgang wurde gestartet.
- Scan Stopped (Scanvorgang angehalten) – Ein Zielscanvorgang wurde angehalten.
- Session Timeout (Zeitüberschreitung bei der Sitzung) – Bei der Sitzung ist eine Zeitüberschreitung aufgetreten.
- VM Image Connected (VM-Abbild verbunden) – Ein VM-Abbild wurde verbunden.
- VM Image Disconnected (VM-Abbild getrennt) – Ein VM-Abbild wurde getrennt.

Anhang E Wichtige Hinweise

In diesem Kapitel

Überblick

Dieser Abschnitt enthält wichtige Hinweise zur Verwendung des KX III. Zukünftige Aktualisierungen werden dokumentiert und sind online über den Link "Help" (Hilfe) auf der Benutzeroberfläche der KX III Remotekonsole verfügbar.

Hinweis: Einige Kapitel in diesem Abschnitt beziehen sich auf andere Geräte von Raritan, da diese Informationen auf verschiedene Geräte zutreffen.

Java Runtime Environment (JRE) Hinweise

Sie sollten die Zwischenspeicherung für Java deaktivieren und den Java-Zwischenspeicher leeren.

Sie sollten die Zwischenspeicherung für Java caching in Microsoft Windows®deaktivieren und den Java™-Zwischenspeicher leeren.

Sie sollten die Zwischenspeicherung für Java deaktivieren und den Java-Zwischenspeicher leeren.

1. Klicken Sie im Windows Menü Start auf Control Panel (Systemsteuerung).
2. Doppelklicken Sie auf das Symbol Java, um Java zu starten. Die Java-Systemsteuerung wird geöffnet.
3. So deaktivieren Sie die Java-Zwischenspeicherung:

a. Klicken Sie auf der Registerkarte General dann auf die Schaltfläche Settings (Einstellungen). Das Dialogfeld Temporary Internet Files (Temporäre Internetdateien) wird geöffnet:

b. Klicken Sie auf die Schaltfläche View Applets (Applets anzeigen). Der Java Applet Cache Viewer wird geöffnet:

c. Deaktivieren Sie das Kontrollkästchen Enable Caching (Zwischenspeicherung aktivieren).

d. Klicken Sie auf OK.

4. So leeren Sie den Java-Zwischenspeicher:

a. Klicken Sie im Dialogfeld Temporary Files Settings (Einstellungen für temporäre Dateien) auf die Schaltfläche Delete Files (Dateien löschen). Das Dialogfeld Delete Temporary Files (Temporäre Dateien löschen) wird geöffnet:

b. Wählen Sie die temporären Dateien aus, die Sie löschen möchten.

c. Klicken Sie auf OK.

Java wird nicht ordnungsgemäß auf Mac geladen

Wenn Sie einen Mac®verwenden und die folgende Meldung sehen, wenn Sie ein Gerät aus der KX III Port-Zugriff-Tabelle anschließen, ist Java ™ nicht richtig geladen:

"Fehler beim Abrufen der Liste der offenen Ziele, versuchen Sie es in ein paar Sekunden erneut."

Falls dies entritt, prüfen Sie Ihre Java Installation von dieser Webseite aus: ***http://www.java.com/en/download/testjava.jsp*** ***http://www.java.com/en/download/testjava.jsp***

Wenn Ihre Java Applet inaktiv ist, kann es auf dieser Webseite aktiviert werden. Wenn es nicht korrekt installiert wird, wird eine Nachricht erscheinen und Sie können Java erneut installieren.

Hinweise zur Unterstützung von IPv6

Betriebssystem Hinweise zur Unterstützung von IPv6

Java

Java™ 1.7 unterstützt IPv6 bei folgenden Produkten:

- Solaris™ 10 (und höher)
- Linux® kernel 2.1.2 (und höher)/RedHat 6.1 (und höher)
- Solaris 10 (und höher)
- Windows XP® SP1 und Windows 2003®, Windows Vista® und Windows 7 Betriebssysteme

Die folgenden IPv6-Konfigurationen werden *nicht* von Java unterstützt:

- J2SE 1.4 unterstützt kein IPv6 auf Microsoft® Windows®.

Linux

- Es wird empfohlen, bei Nutzung von IPv6 Linux Kernel 2.4.0 oder höher zu verwenden.
- Ein IPv6-aktivierter Kernel muss installiert werden, oder der Kernel muss mit aktivierten IPv6-Optionen wiederhergestellt werden.
- Bei der Verwendung von IPv6 und Linux müssen außerdem einige Netzwerkdienste installiert werden. Weitere Informationen finden Sie unter http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html.

Windows

- Windows XP- und Windows 2003-Benutzer müssen Microsoft Service Pack für IPv6 installieren, um IPv6 zu aktivieren.
- Für AKC mit IPv6 unter Windows XP müssen Sie die ausführbare Datei "kxgui.exe" zur Ausnahmeliste Ihrer Firewall hinzufügen. Zeigen Sie die Protokolldatei auf dem Client an, um den vollständigen Pfad für den Speicherort der Datei "kxgui.exe" zu ermitteln.

Samba

- Bei der Verwendung von Samba zusammen mit virtuellen Medien wird kein IPv6 unterstützt.

AKC-Download-Serverzertifikatsvalidierung IPv6 Unterstützungshinweise

Wenn Sie eine Verbindung zu einem eigenständigen KX III-Gerät herstellen und Support für die AKC-Download-Serverzertifikatsvalidierung aktiviert ist, lautet das gültige IPv6-Format zur Generierung des Zertifikats entweder:

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` wenn eine führende 0 vorhanden ist

  Oder

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` wenn keine Nullkomprimierung vorhanden ist

Leistungsprobleme bei Dual Stack-Anmeldungen

Wenn Sie KX III in einer Dual Stack-Konfiguration verwenden, ist es wichtig, dass Sie das Domänensystem (DNS) korrekt in KX III konfiguriert haben, um Verzögerungen beim Amelden zu vermeiden.

Siehe ***Tipps für das Hinzufügen einer Webbrowser-Schaltfläche in Bezug auf Informationen über das Konfigurieren von Ihrer DNS in*** (siehe "***Tipps zum Hinzufügen einer Webbrowseroberfläche***" auf Seite 119) KX III.

CIM Notizen

Windows-3-Tasten-Maus auf Linux-Zielgeräten

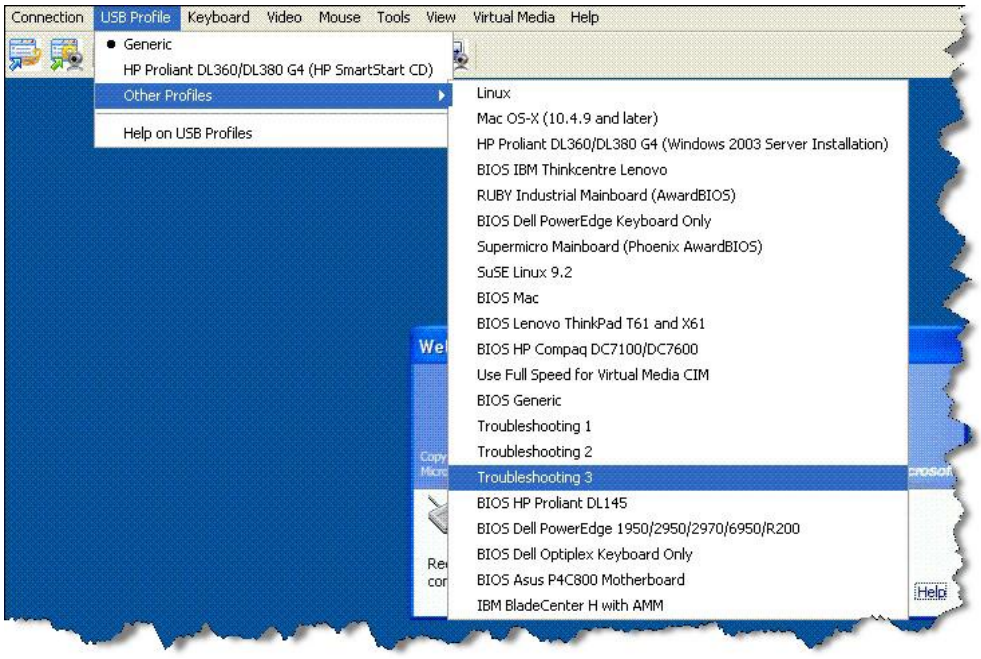
Wenn Sie auf einem Windows®-Client eine 3-Tasten-Maus verwenden und eine Verbindung zu einem Linux®-Zielgerät herstellen, wird die linke Maustaste möglicherweise der mittleren Taste der 3-Tasten-Maus des Windows-Client zugeordnet.

Composite-USB-Geräteverhalten bei virtuellen Medien auf Windows 2000

Das Betriebssystem Windows 2000® unterstützt Composite-USB-Geräte (z. B. D2CIM-VUSB von Raritan) nicht im gleichen Maße wie Non-Composite-USB-Geräte.

Aus diesem Grund wird das Symbol zum sicheren Entfernen der Hardware im Infobereich der Taskleiste bei Laufwerken, die von D2CIM-VUSB zugeordnet wurden, nicht angezeigt, und beim Verbinden des Geräts wird möglicherweise eine Warnmeldung angezeigt. Es wurden von Raritan jedoch keine daraus resultierenden Probleme oder Fehler festgestellt.

Die Entwicklungsabteilung von Raritan in den USA hat eine Konfiguration entwickelt, die das Symbol zum sicheren Entfernen der Hardware unterstützt und die Warnmeldung unterdrückt. Um diese Konfiguration nutzen zu können, müssen Sie den D2CIM-DVUSB-Adapter für virtuelle Medien sowie das USB-Profil "Troubleshooting 3" (Fehlerbehebung 3) verwenden, wodurch D2CIM-DVUSB als Non-Composite-USB-Gerät mit Unterstützung für eine einzelne virtuelle Medienverbindung konfiguriert wird. Diese Konfiguration wurde von Raritan in den USA und Japan erfolgreich getestet.



Virtual Media Hinweis (Virtuelle Medien)

Kann die Laufwerke von Linux Clients nicht verbinden

Wenn Sie nicht zu einem virtuellen Laufwerk auf einem Zielserver verbinden können, wenn Sie von einem Client auf Linux Fedora ® ™ 18 mit Java ™ 1.7.0 (Update 45 und höher) anschließen, deaktivieren Sie SELinux in Fedora 18 auf dem Client, um das Problem zu lösen.

Kann nicht Zu/Von einer Datei von einem Mac-Client geschrieben werden

Wenn Sie an KX III von einem Mac® 10.8.5 Client, mit Safari® 6.1 und Java™1.7 anschließen möchten und die Datei auf dem Zielserver nicht schreiben können oder keinen Zugrif zu den virtuellen Medien haben, machen Sie Folgendes, um das Problem zu lösen:

1. In Safari, wählen Sie Präfrenzen.
2. Wählen Sie auf der Registerkarte "Sicherheit" die Webseiteneinstellung Verwalten.
3. Klicken Sie auf „Webseite für KX3“.
4. „Sicheres Modus“ Auswählen.
5. Safari neu starten.

Virtuelle Medien über den VKC und den AKC in einer Windows-Umgebung

Die Berechtigungen für den Systemadministrator und den Standardbenutzer unter dem Betriebssystem Windows XP® unterscheiden sich von den Berechtigungen unter den Betriebssystemen Windows Vista® und Windows 7®.

Ist die "User Access Control (UAC)" (Benutzerzugriffssteuerung) unter Windows Vista oder Windows 7 aktiviert, so bietet diese die Berechtigungen der niedrigsten Stufe, die ein Benutzer für eine Anwendung benötigt. Beispielsweise ist die Option "Run as Administrator" (Als Administrator ausführen) für Internet Explorer® verfügbar, um Benutzern die Ausführung spezieller Aufgaben auf Administratorebene zu gestatten. Diese Berechtigung würde sonst nicht bestehen, selbst wenn der Benutzer über ein Administratorkonto verfügt.

Diese beiden Funktionen wirken sich darauf aus, auf welchen Typ virtueller Medien von Benutzern über den Virtual KVM Client (VKC) und den Active KVM Client (AKC) zugegriffen werden kann. Weitere Informationen zu diesen Funktionen und deren Verwendung finden Sie in Ihrer Microsoft ® Hilfe.

Im Folgenden finden Sie eine Liste mit Typen virtueller Medien, auf die über den VKC und den AKC aus einer Windows-Umgebung zugegriffen werden kann. Die Funktionen sind nach Client-Funktionen und Funktionen der virtuellen Medien aufgeteilt, die den einzelnen Windows-Benutzerfunktionen zugewiesen sind.

Windows XP

Wenn Sie den VKC und den AKC in einer Windows XP-Umgebung ausführen, müssen Benutzer über Administratorrechte verfügen, um auf andere Medientypen als CD-ROM-Verbindungen, ISO-Dateien und ISO-Abbilder zugreifen zu können.

Windows Vista und Windows 7

Wenn Sie den VKC und den AKC in einer Windows Vista- oder Windows 7-Umgebung bei aktivierter UAC ausführen, kann, je nach Windows-Benutzerfunktion, auf die folgenden virtuellen Medientypen zugegriffen werden.

Client	Administrator	Standard-Benutzer

Client	Administrator	Standard-Benutzer
AKC und VKC	Zugriff auf: • Fest installierte Laufwerke und deren Partitionen • Wechsellaufwerke • CD-/DVD-Laufwerke • ISO-Abbilder • Remote-ISO-Abbilder	Zugriff auf: • Wechsellaufwerke • CD-/DVD-Laufwerke • ISO-Abbilder • Remote-ISO-Abbilder

Virtuelle Medien werden nach dem Hinzufügen von Dateien nicht aktualisiert

Nach der Installation eines virtuellen Medienlaufwerks werden dem Laufwerk hinzugefügte Dateien möglicherweise nicht unmittelbar auf dem Zielserver angezeigt. Trennen Sie die virtuelle Medienverbindung und stellen Sie sie erneut her.

Zwei Listeneinträge für das Linux-Laufwerk für virtuelle Medien

Für KX III werden die Laufwerke für Benutzer, die bei Linux™-Clients als Stammbenutzer angemeldet sind, in der Dropdownliste "Local Drive" (Lokales Laufwerk) zweimal aufgeführt.

Beispielsweise werden "eg /dev/sdc" und "eg /dev/sdc1" angezeigt, wobei das erste Laufwerk der Bootsektor und das zweite Laufwerk die erste Partition auf der Festplatte ist.

Zugriff auf virtuelle Medien auf Windows 2000

Der Zugriff auf virtuelle Medien auf einem lokalen Laufwerk auf einem Windows 2000® Server ist mit D2CIM-VUSB nicht möglich.

Mac und Linux Virtuelle Medien USB Laufwerke Trennen

In einer Linux® oder Mac® Umgebung:

- Für Linux-Benutzer, wenn es /dev/sdb und /dev/sdb1 gibt, verwendet der Client nur /dev/sdb1.
- /dev/sdb ist nicht für den Benutzer verfügbar.
- Für Linux-Benutzer, wenn es /dev/sdb aber kein /dev/sdb1 gibt, wird /dev/sdb als entfernbares Gerät verwendet
- Für Mac-Benutzer wird /dev/disk1 und /dev/disk1s1 verwendet

Bootzeit des Ziel-BIOS bei Verwendung von virtuellen Medien

Das BIOS bestimmter Zielgeräte benötigt möglicherweise mehr Zeit zum Hochfahren, wenn virtuelle Medien auf dem Zielgerät installiert sind.

So verkürzen Sie die Bootzeit:

1. Schließen Sie den Virtual KVM Client, sodass die virtuellen Medienlaufwerke vollständig freigegeben werden.
2. Starten Sie das Zielgerät neu.

Fehler bei Hochgeschwindigkeitsverbindungen mit virtuellen Medien

Unter bestimmten Umständen kann es erforderlich sein, die Verbindungsgeschwindigkeit "Use Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) auszuwählen. Zum Beispiel bei Problemen des Ziels mit der USB-Hochgeschwindigkeitsverbindung oder wenn beim Ziel USB-Protokollfehler aufgrund von Signalstörungen, zusätzlichen Anschlüssen und Kabeln auftreten. (beispielsweise eine Verbindung zu einem Bladeserver über ein Dongle).

USB-Ports und -Profilhinweise

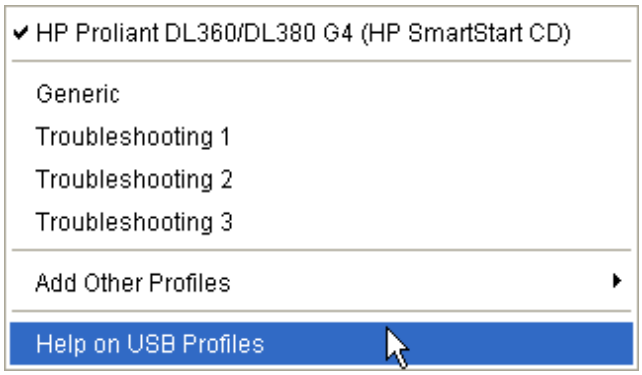
VM-CIMs und DL360 USB-Ports

HP® DL360-Server verfügen über einen USB-Port auf der Rückseite des Geräts und einen weiteren auf der Vorderseite. Mit DL360 können nicht beide Ports gleichzeitig verwendet werden. Deshalb kann ein duales VM-CIM auf DL360-Servern nicht verwendet werden.

Sie können jedoch einen USB2-Hub an den USB-Port auf der Rückseite des Geräts angeschlossen werden, an den wiederum ein duales VM-CIM angeschlossen werden kann.

Hilfe beim Auswählen von USB-Profilen

Wenn Sie im Virtual KVM Client (VKC) mit einem KVM-Zielserver verbunden sind, können Sie Informationen zu USB-Profilen über den Befehl "Help on USB Profiles" (Hilfe bei USB-Profilen) im Menü "USB Profile" (USB-Profil) anzeigen.



Das Fenster "USB Profile Help" (Hilfe für USB-Profile) wird angezeigt. Weitere Informationen zu speziellen USB-Profilen finden Sie unter Verfügbare USB-Profile.

Raritan stellt eine Standardauswahl an USB-Konfigurationsprofilen für eine große Anzahl an Serverimplementierungen für Betriebssysteme und auf BIOS-Ebene an. Diese sorgen für optimale Übereinstimmung bei Konfigurationen von Remote-USB-Geräten und Zielservern.

Das Profil "Generic" (Generisch) erfüllt die Anforderungen der meisten häufig bereitgestellten Zielserverkonfigurationen.

Weitere Profile stehen zur Verfügung, um die speziellen Anforderungen anderer häufig bereitgestellter Serverkonfigurationen (z. B. Linux®, Mac OS X®) zu erfüllen.

Außerdem stehen einige Profile (festgelegt nach Plattformname und BIOS-Revision) zur Verfügung, die erstellt wurden, um die Kompatibilität der Funktion der virtuellen Medien mit dem Zielserver zu verbessern (wenn z. B. auf BIOS-Ebene gearbeitet wird).

Mit "Add Other Profiles" (Weitere Profile hinzufügen) haben Sie Zugriff auf andere auf dem System verfügbare Profile. Aus dieser Liste ausgewählte Profile werden zum Menü "USB Profile" (USB-Profil) hinzugefügt. Dazu gehört eine Reihe von Problembehebungsprofilen, mit denen Sie Konfigurationsbeschränkungen ermitteln können.

Die ausgewählten Profile im Menü "USB Profile" (USB-Profil) sind unter "Console Device Settings" > "Port Configuration" (Konsolengeräteeinstellungen > Portkonfiguration) konfigurierbar.

Sollte keines der Standard-USB-Profile von Raritan Ihren Zielserveranforderungen entsprechen, können Sie zusammen mit dem technischen Kundendienst von Raritan eine den Anforderungen Ihres Zielgeräts entsprechende Lösung erarbeiten. Raritan empfiehlt, Folgendes zu überprüfen:

1. Überprüfen Sie die neuesten Versionshinweise auf der Seite "Firmware Upgrade" (Firmwareaktualisierung) der Raritan-Website (www.raritan.com), um festzustellen, ob für Ihre Konfiguration bereits eine Lösung verfügbar ist.
2. Wenn dies nicht der Fall ist, stellen Sie die folgenden Informationen zur Verfügung, wenn Sie sich an den technischen Kundendienst von Raritan wenden:
    a. Zielserverinformationen, Hersteller, Modell, BIOS, Hersteller und Version
    b. Verwendungszweck (z. B. Umleiten eines Abbildes, um das Betriebssystem eines Servers von CD neu zu laden)

Ändern eines USB-Profils bei Verwendung eines Smart Card-Lesegeräts

Unter bestimmten Umständen kann es erforderlich sein, das USB-Profil für einen Zielserver zu ändern. Zum Beispiel wenn Sie bei Problemen des Ziels mit der USB-Hochgeschwindigkeitsverbindung die Verbindungsgeschwindigkeit auf "Use Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) ändern möchten.

Nachdem ein Profil geändert wurde, erhalten Sie die Meldung "New Hardware Detected" (Neue Hardware gefunden) und werden aufgefordert, sich mit Administratorberechtigung am Ziel anzumelden, um den USB-Treiber erneut zu installieren. Meistens geschieht dies nur die ersten Male, wenn das Ziel die neuen Einstellungen für das USB-Gerät erkennt. Danach wählt das Ziel den richtigen Treiber aus.

Videomodi und Auflösungshinweise

Video Bild erscheint dunkel bei Verwendung von Mac

Wenn Sie einen Mac ® mit einem HDMI-Video-Anschluss verwenden und das Video zu dunkel erscheint, aktivieren Sie den DVI-Kompatibilitätsmodus auf dem CIM, um das Problem zu lösen.

Siehe ***Konfigurieren von CIM-Ports*** (auf Seite 98)

Schwarz Stripe/Bar(s) Wird auf Lokaler Port Angezeigt

Bestimmte Server-und Video-Auflösungen können auf dem lokalen Port mit kleinen schwarzen Balken am Bildschirmrand angezeigt werden.

Falls dies entritt:

1. Versuchen Sie eine andere Auflösung, oder
2. Wenn Sie einen digitalen CIM verwenden, ändern Sie die „Ursprüngliche Auflösung Zeigen“ auf der Port-Konfigurationsseite, oder
3. Wenn HDMI CIM verwendet wird, wenden Sie den DVI Kompatibilitätsmodus an.

Wenden Sie sich an den technischen Support von Raritan.

Sun Composite Synch Video

Sun™ Composite Synch Video wird nicht unterstützt.

Videomodi für SUSE/VESA

Das SuSE X.org-Konfigurationstool "SaX2" erzeugt Videomodi mithilfe von Modeline-Einträgen in der X.org-Konfigurationsdatei. Diese Videomodi stimmen nicht exakt mit der Zeitabstimmung des VESA-Videomodus überein (auch wenn ein VESA-Monitor ausgewählt wurde). Andererseits verwendet KX III die Zeitabstimmung des VESA-Videomodus für die ordnungsgemäße Synchronisierung und verlässt sich auf deren Richtigkeit. Diese Unstimmigkeit kann zu schwarzen Rändern, fehlenden Abschnitten im Bild und Rauschen führen.

So konfigurieren Sie die SUSE-Videoanzeige:

1. Die erzeugte Konfigurationsdatei "/etc/X11/xorg.conf" enthält einen Abschnitt zum Monitor mit einer Option, die als "UseModes" bezeichnet wird, Z. B.
   UseModes "Modes[0]".
2. Kommentieren Sie diese Zeile aus (mit #) oder löschen Sie sie vollständig.
3. Starten Sie den X-Server neu.

Durch diese Änderung wird die interne Zeitabstimmung für den Videomodus des X-Servers verwendet, der exakt mit der Zeitabstimmung des VESA-Videomodus übereinstimmt und so zur gewünschten Videoanzeige auf KX III führt.

Tastatur-Hinweise

Französische Tastatur

Zirkumflexzeichen (nur Linux-Clients)

Der Virtual KVM Client (VKC) unterstützt bei Verwendung einer französischen Tastatur mit Linux®-Clients nicht die Tastenkombination "Alt Gr+9" für das Zirkumflexzeichen (^).

So stellen Sie das Zirkumflexzeichen dar:

Drücken Sie auf einer französischen Tastatur die ^-Taste (rechts neben der P-Taste) und unmittelbar danach die Leertaste.

Alternativ können Sie ein Makro erstellen, das aus folgender Befehlsabfolge besteht:

1. Rechte Alt-Taste drücken
2. Taste "9" drücken
3. Taste "9" loslassen

4. Rechte Alt-Taste loslassen

Hinweis: Dieser Vorgang kann bei der Verwendung des Zirkumflexzeichens mit anderen Buchstaben (als Akzent über Vokalen) nicht durchgeführt werden. In diesem Fall verwenden Sie die ^-Taste (rechts neben der P-Taste) auf französischen Tastaturen.

Akzentzeichen (nur Windows XP-Betriebssystem-Benutzer)

Von Virtual KVM Client (VKC) aus wird bei Verwendung der Tastenkombination "Alt Gr+7" das Akzentzeichen zweimal dargestellt, wenn eine französische Tastatur für Windows XP®-Clients verwendet wird.

Hinweis: Dies trifft nicht auf Linux® Clients zu.

Nummernblock

Von Virtual KVM Client (VKC) aus werden die Zeichen auf dem Nummernblock bei französischen Tastaturen wie folgt dargestellt:

Zeichen auf dem Nummernblock	Dargestellt als
/	;
.	;

Tilde

Von Virtual KVM Client (VKC) aus wird bei Verwendung einer französischen Tastatur durch die Tastenkombination "Alt Gr+2" nicht das Tilde-Symbol (~) angezeigt.

So stellen Sie die Tilde dar:

Erstellen Sie mit der folgenden Befehlsabfolge ein Makro:

- Rechte Alt-Taste drücken
- Taste "2" drücken
- Taste "2" loslassen
- Rechte Alt-Taste loslassen

Einstellungen der Tastatursprache (Fedora Linux-Clients)

Da bei Sun™ JRE™ auf einem Linux® Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenereignissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Ländervariante	Konfigurationsmethode
USA/Int.	Standardwert
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Deutsch (Schweiz)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Japanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.

Bei Verwendung einer ungarischen Tastatur mit einem Linux-Client werden die lateinischen Buchstaben "U" mit Doppelakut und "O" mit Doppelakut nur dargestellt, wenn JRE 1.6 verwendet wird.

Es gibt mehrere Methoden, die Einstellungen der Tastatursprache bei Fedora Linux-Clients festzulegen. Die folgende Methode muss angewendet werden, um die Tasten für den Virtual KVM Client (VKC) korrekt zuzuordnen.

So legen Sie die Tastatursprache unter "System Settings" (Systemeinstellungen) fest:

1. Wählen Sie in der Symbolleiste "System“ "Preferences" "Keyboard" (System > Einstellungen > Tastatur) aus.
2. Öffnen Sie die Registerkarte "Layouts" (Tastatursprache).
3. Wählen Sie die entsprechende Sprache aus oder fügen Sie sie hinzu.
4. Klicken Sie auf Close (Schließen).

So legen Sie die Tastatursprache unter "Keyboard Indicator" (Tastaturanzeige) fest:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie "Add to Panel" (Zu Panel hinzufügen) aus.
2. Klicken Sie im Dialogfeld "Add to Panel" (Zu Panel hinzufügen) mit der rechten Maustaste auf "Keyboard Indicator" (Tastaturanzeige) und wählen Sie aus dem Kontextmenü "Open Keyboard Preferences" (Tastatureinstellungen öffnen) aus.
3. Klicken Sie im Dialogfeld "Keyboard Preferences" (Tastatureinstellungen) auf die Registerkarte "Layouts" (Tastatursprache).
4. Fügen Sie Sprachen wie gewünscht hinzu oder löschen Sie sie.

Makros sind nicht auf dem Linux Zielserver gespeichert

Wenn Sie die folgende Fehlermeldung erhalten, wenn Sie ein Makro auf einem Zielserver unter Linux Fedora ® ™ 18 mit Java ™ 1.7.0 (Update 45 und höher) erstellen und speichern, deaktivieren Sie SELinux in Fedora 18 auf dem Zielserver, um das Problem zu lösen.

```
"Ein Fehler ist aufgetreten, beim Versuch die neuen
Tastatur-Makros zu schreiben. Makro wurde nicht
hinzugefügt“
```

Mac Tastaturschlüssel sind nicht für Fernzugriff unterstützt

Wenn Macintosh® als Client verwendet wird, funktionieren die folgenden Tasten auf der Mac® Tastatur unter Verwendung von Java™ Runtime Environment (JRE™) nicht.

- F9
- F10
- F11
- F14
- F15
- Volume Up (Lautstärke höher)
- Volume Down (Lautstärke niedriger)
- Ton aus
- Eject (Ausgabe)

Deshalb können diese Tasten bei Verwendung von Virtual KVM Client (VKC) zusammen mit einer Mac-Clienttastatur nicht verwendet werden.

Maus-Hinweise

Mauszeigersynchronisierung (Fedora)

Wenn bei Verwendung von FedoraR 7 eine Verbindung zu einem Zielserver über den Zwei-Cursor-Modus besteht und die Synchronisierung der lokalen und der Ziel-Cursor nach einiger Zeit unterbrochen wird, kann durch das Ändern des Mausmodus von "Intelligent" in "Standard" oder umgekehrt die Synchronisierung verbessert werden.

Der Ein-Cursor-Modus ermöglicht ebenfalls eine verbesserte Steuerung.

So synchronisieren Sie die Cursor erneut:

- Verwenden Sie die Option "Synchronize Mouse" (Maus synchronisieren) im Virtual KVM Client.

Ein-Cursor-Modus – Verbinden mit einem Zielgerät unter CC-SG-Steuerung

Wenn Sie Firefox® benutzen, um eine Verbindung zu einem KX III Zielgerät unter CC-SG-Steuerung herzustellen, und DCIM-PS2 oder DCIM-USBG2 verwenden, erscheint das VKC-Fenster nicht mehr als Fokusfenster, wenn Sie im Virtual KVM Client in den Ein-Cursor-Modus wechseln, und die Maus reagiert nicht mehr.

Drücken Sie in diesem Fall die linke Maustaste oder die Alt-+Tab-Taste, um den Fokus auf das VKC-Fenster zurückzuschalten.

Audio

Probleme bei der Audiowiedergabe und -aufnahme

Funktionen, die eine Audioverbindung stören können

Wenn Sie eine der folgenden Funktionen verwenden und ein Audiogerät angeschlossen ist, wird die Audioverbindung möglicherweise unterbrochen. Raritan empfiehlt, diese Funktionen nicht zu verwenden, wenn ein Audiogerät angeschlossen ist:

- Automatische Videoerkennung
- Extensive Nutzung des lokalen Ports
- Hinzufügen von Benutzern

Probleme bei gleichzeitiger Verwendung eines Aufnahme- und eines Wiedergabegeräts auf einem Ziel

Auf einigen Zielen ist es aufgrund des USB-Hub-Controllers und der entsprechenden Verwaltung der USB-Ports nicht möglich, Aufnahme- und Wiedergabegeräte gleichzeitig anzuschließen. Wählen Sie ggf. ein Audioformat aus, das eine geringere Bandbreite erfordert.

Wenn das Problem dadurch nicht behoben wird, schließen Sie die Tastatur und Maus des D2CIM-DVUSB CIM an einen anderen Port des Ziels an. Wird dadurch das Problem nicht behoben, schließen Sie das Gerät an einen USB-Hub an, und verbinden Sie den Hub mit dem Ziel.

Audiofunktion in einer Linux-Umgebung

Die folgenden Probleme sind bei der Verwendung der Audiofunktion in einer Linux®-Umgebung bekannt.

- Linux®-Benutzer sollten das Audiostandardgerät für die Wiedergabe verwenden. Die Tonsignale werden möglicherweise nicht ordnungsgemäß übertragen, wenn eine andere als die Standard-Soundkarte ausgewählt wurde.
- Für SuSE 11-Clients muss Javas_1_6_0-sun-alsa (ALSA-Unterstützung für java-1_6_0-sun) über YAST installiert werden.
- Für Logitech ®-Headsets mit integriertem Mikrofon steht nur die Option "Mono Capture" (Aufnahme in Monoqualität) zur Verfügung.
- Wenn Sie SUSE 11 und einen ALSA-Driver verwenden, melden Sie sich vom KX III ab, und melden Sie sich dann erneut an, um das Gerät anzuzeigen.

  Wenn Sie die Verbindung zum Audiogerät mehrfach herstellen und trennen, wird das Gerät außerdem möglicherweise mehrfach statt nur einmal angezeigt.

- Bei Verwendung der Audiofunktion mit einem auf Mono 16 Bit, 44 K eingestellten Fedora Core® 13-Ziel kann es während der Aufnahme zu erheblichen Störungen kommen.

Audiofunktion in einer Windows-Umgebung

Auf Windows®-64-Bit-Clients wird bei Zugriff auf das Gerät über den Virtual KVM Client (VKC) und den Multi-Platform-Client (MPC) nur ein Wiedergabegerät im Fenster "Connect Audio" (Audio verbinden) aufgeführt.

Das Audiogerät ist das Standardgerät und wird im Fenster "Connect Audio" (Audio verbinden) als Java Sound-Audiomodul aufgeführt.

"Smart Card“-Hinweise

Virtual KVM Client (VKC) Smart Card-Verbindungen zu Fedora-Servern

Wenn Sie eine Smart Card für die Verbindung zu einem Linux® Fedora®-Server über Virtual KVM Client (VKC) verwenden, aktualisieren Sie die PCSC-Lite-Bibliothek auf 1.4 102-3 oder höher.

CC-SG Hinweise

Version des Virtual KVM Client im CC-SG-Proxymodus nicht bekannt

Wenn der virtuelle KVM Client (VKC) über CommandCenter Secure Gateway (CC-SG) im Proxymodus gestartet wird, ist die Version des VKC Client unbekannt.

Im Dialogfeld "About Raritan Virtual KVM Client" (Informationen zum Raritan Virtual KVM Client) wird die Version als "Version Unknown" (Version unbekannt) angezeigt.

Wechseln zwischen Ports auf einem Gerät

Wenn Sie zwischen Ports desselben Raritan-Geräts wechseln und die Verwaltung innerhalb von einer Minute wieder aufnehmen, zeigt CC-SG möglicherweise eine Fehlermeldung an.

Die Anzeige wird aktualisiert, wenn Sie die Verwaltung wieder aufnehmen.

Suchprogramm-Hinweise

Lösen von Problemen mit dem Einfrieren von Firefox bei der Benutzung von Fedora

Wenn Sie Firefox ® verwenden und einen Fedora ® Server benutzen, ist es möglich, dass Firefox beim Öffnen einfriert.

Um dieses Problem zu lösen, installieren Sie das Java™-Plug-in libnpjp2.so auf dem Server.

Anhang F Häufig gestellte Fragen

In diesem Kapitel

Allgemeine häufig gestellte Fragen (FAQs)

Frage	Antwort
Was ist Dominion KX III?	Dominion KX III ist ein digitaler KVM-Switch (Tastatur, Video, Maus) der dritten Generation, der einem, zwei, vier oder acht IT-Administrator(en) den Zugriff auf 8, 16, 32 oder 64 Server und deren Steuerung über das Netzwerk mit Funktionen auf BIOS-Ebene erlaubt. Der Dominion KX III ist vollständig unabhängig von Hardware und Betriebssystem. Sie können die Problembehandlung und Neukonfiguration von Servern auch bei nicht betriebsbereiten Servern ausführen. Im Serverschrank montiert, bietet der platzsparende Dominion KX III die gleiche Funktionalität, den gleichen Bedienkomfort und die gleiche Kostenersparnis wie herkömmliche analoge KVM-Switches. Der Dominion KX III verfügt jedoch auch über die leistungsfähigste KVM-über-IP-Technologie der Branche, die mehreren Administratoren den Zugriff auf Server-KVM-Konsolen über eine beliebige vernetzte Workstation sowie über ® und iPad® ermöglicht.

Frage	Antwort
	KX III ist die nächste Generation von KX II. Mit einem modernen Hardware-Design und mit erhöhter Rechenleistung und Speicherplatz bietet KX-III einen KVM-over-IP-Zugriff für die IT-Verwaltung, sowie hochleistungsfähigen IP-Zugang für Broadcast-Anwendungen. KX III enthält virtuell alle KX II Funktionen und Eigenschaften mit den folgenden Entwicklungen: Die neue Video-Engine von KX III unterstützt eine breite Palette von Anwendungen von traditionellen Computer-Anwendungen bis zu den dynamischsten Broadcast Anwendungen, die 30 Bilder pro Sekunde 1920x1080 Video-, 24-Bit-Farbe, Digital-Audio, Dual-Monitore und DVI, HDMI, Displayport und VGA Video benötigen. Mit dem ersten DVI-basierten lokalen Port der Branche bietet die Benutzeroberfläche von KX III eine neue Ebene der Produktivität und Leistung für at-the-rack-Adminstration und Serverzugang. Alle KX-III-Modelle verfügen über einen Schichtport, um mehrere Dominion KX III Switch miteinander zu verbinden und an dem Server anzuschließen. Auf bis zu 1024 Server kann über eine konsolidierte Portliste zugegriffen werden. KX III unterstützt alle Dominion und Paragon II CIMs Modelle.

Frage	Antwort
Inwiefern unterscheidet sich Dominion KX III von Remotesteuerungs-Software?	Bei der Remoteverwendung von Dominion KX III erscheint die Benutzeroberfläche zunächst ähnlich der Software zur Remotesteuerung wie pcAnywhere™, Windows® Terminal Services/Remote Desktop, VNC, etc. Da Dominion KX III jedoch keine Software-, sondern eine Hardwarelösung ist, ist das Gerät wesentlich leistungsstärker. Hardware- und betriebssystemunabhängig – Der Dominion KX III kann zur Verwaltung von Servern mit vielen beliebigen Betriebssystemen verwendet werden. Dazu zählen Intel®, Sun®, PowerPC running Windows, Linux®, Solaris™, etc. Statusunabhängig/Agent-frei – Dominion KX IIKX IIII erfordert nicht, dass das Betriebssystem des verwalteten Servers ausgeführt wird oder dass auf dem verwalteten Server spezielle Software installiert ist. Out-of-Band – Auch wenn die Netzwerkverbindung des verwalteten Servers nicht verfügbar ist, kann der Server trotzdem mit dem Dominion KX III verwaltet werden. Zugriff auf BIOS-Ebene – Dominion KX III funktioniert auch dann fehlerfrei und ermöglicht die erforderliche Konfiguration, wenn der Server nicht hochfährt, im abgesicherten Modus gestartet werden muss oder wenn seine BIOS-Systemparameter geändert werden müssen.
Kann der Dominion KX III in einem Gestell montiert werden?	Ja. Der Dominion KX III wird mit 19-Zoll-Gestellhalterungen geliefert. Er kann auch umgekehrt im Gestell montiert werden, sodass die Serverports nach vorne zeigen.
Wie groß ist der Dominion KX III?	Der Dominion KX III ist nur 1U hoch (mit Ausnahme der Modelle KX3-864 und KX3-464, welche 2U hoch sind), passt in ein 19-Zoll-Standardgestell und ist nur 29 cm tief. Die Modelle Dominion KX3-832 und KX3-864 sind 13.8" (36 cm) tief.

Remotezugriff

Frage	Antwort
Wie viele Benutzer erhalten mit einem Dominion KX III Remotezugriff auf Server?	Die Modelle des Dominion KX III bieten bis zu acht Benutzern pro Kanal Remoteverbindungen für den gleichzeitigen Zugriff auf einen einzelnen Zielserver und dessen Steuerung. Bei Ein-Kanal-Geräten wie dem DKX3-116 können bis zu acht Remotebenutzer auf einen einzelnen Zielserver zugreifen und diesen steuern. Bei Zwei-Kanal-Geräten, wie dem DKX3-216, können bis zu acht Benutzer auf Kanal eins auf den Server zugreifen und diesen steuern, und weiteren acht Benutzern steht Kanal zwei zur Verfügung. Bei Vier-Kanal-Geräten können bis zu acht Benutzer pro Kanal auf vier Server zugreifen und diese steuern. Dies ergibt insgesamt 32 (8 x 4) Benutzer. Bei Acht-Kanal-Geräten können bis zu acht Benutzer auf einen einzelnen Server zugreifen. Insgesamt können dabei maximal 32 Benutzer die 8 Kanäle verwenden.
Kann ich von meinem iPhone oder iPad remote auf die Server zugreifen?	Ja. Benutzer können über ihr iPhone oder iPad auf Server zugreifen, die mit dem KX III verbunden sind.
Können zwei Personen gleichzeitig denselben Server anzeigen?	Ja. Tatsächlich können bis zu acht Personen gleichzeitig auf einen einzelnen Server zugreifen und diesen steuern.
Können zwei Personen auf denselben Server zugreifen (einer an einem entfernten Standort und einer über den lokalen Port)?	Ja. Der lokale Port ist vollständig unabhängig von den Remote-"Ports". Über den lokalen Port können sie mithilfe des PC-Freigabe-Features auf denselben Server zugreifen.

<table>
<tr><th>Frage</th><th>Antwort</th></tr>
<tr><td>Welche Hardware-, Software- oder Netzwerkkonfiguration ist für den Zugriff auf Dominion KX III über einen Client erforderlich?</td><td>Da der Dominion KX III über das Web verfügbar ist, muss auf Clients keine spezielle Software für den Zugriff installiert werden.

Hinweis: Die KX III 3.0.0 Version bietet keine Modem-Unterstützung, aber die zukünftige Version wird solche haben.

Der Zugriff auf den Dominion KX III ist mit einem gängigen Web-browser möglich. Hierzu zählen: Internet Explorer® und Firefox®. Sie können über den Windows ® Client von Raritan, die Java™ basierte Multiplattform und Virtual KVM Client™ über Windows-, Linux- und Macintosh® Desktop-Computer auf den Dominion KX III zugreifen.

Die Administratoren von Dominion KX III können auch die Fernverwaltung (Kennwörter und Sicherheit einstellen, Server umbenennen, IP-Adresse ändern etc.) über eine komfortable Browser-basierte Schnittstelle ausführen.</td></tr>
<tr><td>Wie groß ist das für den Zugriff auf den Dominion KX III verwendete Applet? Wie lange dauert das Abrufen?</td><td>Das Applet Virtual KVM Client (VKC) für den Zugriff auf den Dominion KX III ist etwa 500 KB groß. Die folgende Tabelle zeigt, wie lange das Herunterladen des Applets bei verschiedenen Netzwerkgeschwindigkeiten dauert:

<table>
<tr><td>100 Mbit/s</td><td>Theoretisch
100 Mbit</td><td>0.5
Sekunden</td></tr>
<tr><td>60 Mbit/s</td><td>Beinahe
100 Mbit</td><td>0.8
Sekunden</td></tr>
<tr><td>10 Mbit/s</td><td>Theoretisch
10 Mbit</td><td>.4
Sekunden</td></tr>
<tr><td>6 Mbit/s</td><td>Beinahe 10 Mbit</td><td>.8
Sekunden</td></tr>
<tr><td>512 Kbit/s</td><td>Kabelmodem-Dow
nloadgeschwindigk
eit (normal)</td><td>8 Sekunden</td></tr>
</table>
</td></tr>
</table>

Frage	Antwort
Haben Sie einen Windows-KVM-Client?	Ja. Wir verfügen über einen systemeigenen .NET-Windows-Client, den Raritan Active KVM Client (AKC). Siehe ***Aktive KVM Client (AKC) Hilfe*** (siehe "***Aktive KVM Klient (AKC) Hilfe***" auf Seite 304)
Haben Sie einen Nicht-Windows-KVM-Client?	Ja. Der Virtual KVM Client ermöglicht es Benutzern, die nicht über ein Windows-Betriebssystem verfügen, Verbindungen mit den Zielservern im Rechenzentrum herzustellen. Siehe ***Virtual KVM Client (VKC) Hilfe*** (siehe "***Virtual KVM Klient (VKC) Hilfe***" auf Seite 249)
Unterstützen Ihre KVM Clients mehrere Sprachen?	Ja. Die HTML-Remotebenutzeroberfläche des Dominion KX II und die KVM Clients unterstützen Japanisch, vereinfachtes Chinesisch und traditionelles Chinesisch. Diese Unterstützung ist sowohl eigenständig als auch über CC-SG verfügbar.
Unterstützen Ihre KVM-Clients duale LCD-Monitore?	Ja. Für Kunden, die ihre Produktivität mithilfe mehrerer LCD-Monitore auf dem Schreibtisch verbessern möchten, kann der Dominion KX III KVM-Sitzungen auf mehreren Monitoren im Vollbild- oder im Standardmodus starten.
Unterstützten Sie Server mit dualen Videokarten?	Ja, duale Videokarten werden mit einer erweiterten Desktopkonfiguration unterstützt, die dem Remote-Benutzer zur Verfügung steht.

Universelle virtuelle Medien

Frage	Antwort
Welche Dominion KX III-Modelle unterstützen virtuelle Medien?	Alle Dominion KX III-Modelle unterstützen virtuelle Medien. Sie sind als eigenständige Angebote oder im Rahmen von CommandCenter® Secure Gateway, der zentralen Verwaltungsanwendung von Raritan, verfügbar.

Frage	Antwort
Welche Arten virtueller Medien unterstützt der Dominion KX III?	Dominion KX III unterstützt die folgenden Medientypen: Interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und ISO-Abbilder.
Welche Voraussetzungen müssen für virtuelle Medien erfüllt sein?	Ein Dominion KX III-CIM für virtuelle Medien ist erforderlich. Es gibt zwei VGA-basierte CIMs: D2CIM-VUSB oder D2CIM-DVUSB. Das D2CIM-VUSB besitzt einen USB-Anschluss und ist für Kunden gedacht, die virtuelle Medien auf Betriebssystemebene verwenden. Das D2CIM-DVUSB besitzt zwei USB-Anschlüsse und sollte von Kunden erworben werden, die virtuelle Medien auf BIOS-Ebene einsetzen möchten. Das D2CIM-DVUSB ist ebenfalls für die Smart Card-Authentifizierung, die Schichtfunktion/Kaskadieren und digitales Audio erforderlich. Beide unterstützen virtuelle Mediensitzungen mit Zielservern, die über eine USB 2.0-Schnittstelle verfügen. Diese CIMs sind in günstigen Paketen zu 32 oder 64 Stück verfügbar und unterstützen den Mausmodus "Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) sowie Remote-Firmwareaktualisierungen. Unsere CIMs unterstützen analoges VGA-Video. Drei neue duale virtuelle Medien-CIMs unterstützen die digitalen Videoformate, einschließlich DVI, HDMI und DisplayPort. Hierzu gehören D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI und D2CIM-DVUSB-DP.
Sind virtuelle Medien sicher?	Ja. Virtuelle Mediensitzungen werden durch eine 256-Bit-AES-, 128-Bit-AES- oder 128Bit-RC4-Verschlüsselung abgesichert.

Frage	Antwort
Wird die Audiofunktion von virtuellen Medien wirklich unterstützt?	Ja. Unterstützt wird die Audiowiedergabe und -aufnahme auf einem mit dem Dominion KX III verbundenen Server. Sie können Sound- und Audiodateien auf einem Remoteserver im Rechenzentrum über die an Ihrem Desktop-PC oder Laptop angeschlossenen Lautsprechern wiedergeben. Außerdem können Sie mit einem an Ihrem PC oder Laptop angeschlossenen Mikrofon Audiodateien aufnehmen. Ein digitales CIM oder das duale D2CIM-DVUSB-CIM für virtuelle Medien ist erforderlich.
Was ist ein USB-Profil?	Bestimmte Server benötigen eine speziell konfigurierte USB-Schnittstelle für USB-basierte Dienste wie virtuelle Medien. Durch die USB-Profile wird die USB-Schnittstelle des KX IIKX IIII auf den Server abgestimmt, sodass sie den speziellen Eigenschaften des Servers entspricht.
Warum sollte ich ein USB-Profil verwenden?	USB-Profile sind meistens auf BIOS-Ebene erforderlich, wo möglicherweise keine vollständige Unterstützung für die USB-Spezifikation beim Zugriff auf virtuelle Medienlaufwerke besteht. Profile werden jedoch manchmal auch auf Betriebssystemebene verwendet, z. B. für die Maussynchronisierung bei Mac und Linux-Servern.
Wie wird ein USB-Profil verwendet?	Auf der Seite zur KX II-Portkonfiguration können individuelle Ports oder Gruppen von Ports vom Administrator konfiguriert werden, sodass ein spezielles USB-Profil verwendet wird. Ein USB-Profil kann ggf. auch im KX III-Client ausgewählt werden. Nähere Informationen hierzu finden Sie im Benutzerhandbuch.
Muss ich immer ein USB-Profil verwenden, wenn ich virtuelle Medien nutze?	Nein Nein, in vielen Fällen reicht das Standard-USB-Profil bei der Verwendung von virtuellen Medien auf Betriebssystemebene oder bei Vorgängen auf BIOS-Ebene ohne Zugriff auf virtuelle Medien aus.
Welche Profile stehen zur Verfügung? Wo erhalte ich weitere Informationen?	Informationen zu den verfügbaren Profilen sowie weitere Details finden Sie im Benutzerhandbuch.

Bandbreite und KVM-über-IP-Leistung

Frage	Antwort
Wie wird in KVM-über-IP-Systemen die Bandbreite genutzt?	Dominion KX III digitalisiert, komprimiert und verschlüsselt die Tastatur-, Video- und Maussignale des Zielservers und übermittelt IP-Pakete über das IP-Netzwerk an den Remoteclient, um die Remotesitzung für den Benutzer herzustellen. Dominion KX III digitalisiert, komprimiert und verschlüsselt die Tastatur-, Video- und Maussignale des Zielservers und übermittelt IP-Pakete über das IP-Netzwerk an den Remoteclient, um die Remotesitzung für den Benutzer herzustellen. Durch die branchenführenden Videoverarbeitungs-Algorithmen von Dominion KX III haben Sie das Gefühl, direkt am Serverschrank zu arbeiten. Bildwechsel (z. B. bei Videoanzeigen) benötigen den größten Teil der verwendeten Bandbreite, während Tastatur- und Mausaktivitäten wesentlich weniger verbrauchen. Es ist wichtig zu beachten, dass die Bandbreite nur dann verwendet werden kann, wenn der Benutzer aktiv ist. Wie viel Bandbreite genutzt wird, hängt von der Anzahl der Bildwechsel auf dem Server ab. Wenn keine Bildwechsel stattfinden (der Benutzer also nicht mit dem Server interagiert), wird normalerweise keine Bandbreite genutzt. Wenn der Benutzer die Maus bewegt oder ein Zeichen eingibt, wird eine geringe Menge an Bandbreite genutzt. Wenn auf dem Bildschirm ein komplexer Bildschirmschoner oder ein Video läuft, erhöht sich die genutzte Bandbreite.
Welche Auswirkungen hat die Bandbreite auf die KVM-über-IP-Leistung?	Generell hängen Bandbreite und Leistung zusammen. Je mehr Bandbreite verfügbar ist, desto besser kann die Leistung sein. In Umgebungen mit eingeschränkter Bandbreite kann die Leistung verringert werden. Der Dominion KX III wurde so entwickelt, dass bei einer großen Anzahl verschiedener Umgebungen eine sehr gute Leistung erzielt wird.

Frage	Antwort
Welche Faktoren beeinträchtigen die Bandbreite?	Wie viel Bandbreite genutzt wird, hängt von mehreren Faktoren ab. Der primäre Faktor ist, wie oben erwähnt, die Anzahl der Bildwechsel auf dem Zielserver. Zu den anderen Faktoren zählen Videoauflösung des Servers, Netzwerkgeschwindigkeit und -eigenschaften, Ressourcen des Client-PC sowie Rauschen der Grafikkarte.
Wie viel Bandbreite verwendet KX III für allgemeine Aufgaben?	Die Bandbreitennutzung hängt primär von den Aufgaben und Aktionen des Benutzers ab. Je mehr Bildwechsel, desto höher die erforderliche Bandbreite.

Frage	Antwort
Wie kann ich die Leistung und die Bandbreite optimalisieren?	Der KX III bietet verschiedene Einstellungen auf den Remoteclients für den Benutzer, um Bandbreite und Leistung zu optimieren. Die Standardeinstellungen bieten Leistung auf Serverschrankebene in Standard-LAN-/WAN-Umgebungen bei sparsamer Nutzung der Bandbreite. **Optimisierung Für.** Verwenden Sie diese Einstellung, um den Video-Engine für Standard IT / EDV-Anwendungen oder für Video / Broadcast-Anwendungen zu konfigurieren. **Kompression.** Bewegen Sie den Schieberegler auf der linken Seite für die höchstmögliche Videoqualität und auf der rechten Seite für die geringste Menge an Bandbreite. **Geräuschfilter.** In den meisten Fällen wird die Standardeinstellung am besten funktionieren, aber Sie können es auf der linken Seite für zugänglichere Videos und auf der rechten Seite für geringere Bandbreite bewegen. Zu den weiteren Tipps für die Verringerung der Bandbreite zählen: ▪ Verwendung eines einfarbigen Hintergrunds anstatt eines komplexen Bildes ▪ Deaktivierung der Bildschirmschoner ▪ Verwendung einer niedrigeren Videoauflösung auf dem Zielserver ▪ Deaktivierung der Option "Show window contents while dragging" (Fensterinhalte beim Verschieben anzeigen) in Windows ▪ Verwendung von einfachen Bildern, Motiven und Desktops (z. B. Windows Classic)

Frage	Antwort
Ich möchte eine Verbindung über das Internet herstellen. Welche Art von Leistung kann ich erwarten?	Dies hängt von der Bandbreite und der Latenz der Internetverbindung zwischen Ihrem Remoteclient und dem KX III ab. Mit einer Verbindung über Kabelmodem oder über eine Hochgeschwindigkeits-DSL-Verbindung kann die Leistung mit der einer LAN-/WAN-Verbindung vergleichbar sein. Bei Verknüpfungen mit niedrigerer Geschwindigkeit können Sie mithilfe der oben beschriebenen Vorschläge die Leistung verbessern.
Ich verfüge über eine Umgebung mit hoher Bandbreite. Wie kann ich die Leistung optimieren?	Die Standardeinstellungen werden gut funktionieren. Sie können die Einstellungen von Verbindungseigenschaften auf der linken Seite bewegen, um die Videoleistung zu verbessern.
Welche maximale Remote-Videoauflösung (über IP) wird unterstützt?	Der Dominion KX III ist der erste und einzige KVM-über-IP-Switch, der eine vollständige Remote-Videoauflösung in High Definition (HD) von 1920x1080 unterstützt. Außerdem werden gängige Breitbildformate unterstützt, einschließlich 1600x1200, 1680x1050 und 1440x900, so dass Remotebenutzer mit den aktuellen hochauflösenden Monitoren arbeiten können.
Wie viel Bandbreite wird für Audio in Anspruch genommen?	Dies hängt vom Typ des verwendeten Audioformats ab. Zur Wiedergabe von Audio in CD-Qualität werden rund 1,5 Mbit/s in Anspruch genommen.
Was muss ich bei Servern mit DVI-Ports beachten?	Server mit DVI-Ports, die DVI-A (analog) und DVI-I (analog und digital integriert) unterstützen, können einen preisgünstigen, passiven Adapter, wie den ADVI-VGA von Raritan, verwenden, um den DVI-Port des Servers in einen VGA-Stecker zu konvertieren, der an den VGA-Stecker eines KX III-CIM angeschlossen werden kann. Server mit DVI-Ports, die DVI-I oder DVI-D (digital) unterstützen, können das neue D2CIM-DVUSB-DVI CIM verwenden.

IPv6-Netzwerk

Frage	Antwort
Was ist IPv6?	IPv6 ist das Akronym für "Internet Protocol Version 6". IPv6 ist das Akronym für "Internet Protocol Version 6". IPv6 ist das IP-Protokoll der nächsten Generation, das die aktuelle Version 4 (IPv4) ersetzt. In IPv6 werden einige Probleme von IPv4 wie die begrenzte Anzahl an IPv4-Adressen behoben. IPv4 wird so auch in einigen Bereichen wie Routing und automatische Netzwerkkonfiguration verbessert. IPv6 soll IPv4 schrittweise ersetzen, wobei beide Versionen für einige Jahre parallel existieren werden. Durch IPv6 wird eines der größten Probleme eines IP-Netzwerks, aus Sicht des Administrators, angegangen: die Konfiguration und Verwaltung eines IP-Netzwerks.
Warum unterstützt KX III IPv6-Netzwerke?	US-Regierungsbehörden sowie das US-amerikanische Verteidigungsministerium werden demnächst IPv6-kompatible Produkte erwerben. In den nächsten Jahren werden auch viele Unternehmen und Länder wie China auf IPv6 umstellen.
Was bedeutet "Dual Stack" und warum ist diese Funktion erforderlich?	"Dual Stack" ist eine Funktion zur gleichzeitigen Unterstützung von IPv4- und IPv6-Protokollen. Durch den graduellen Übergang von IPv4 zu IPv6 ist "Dual Stack" eine grundlegende Anforderung bei der IPv6-Unterstützung.
Wie kann ich auf der KX III Einheit IPv6 aktivieren?	Diese Einstellung können Sie über die Seite "Network Settings" (Netzwerkeinstellungen) auf der Registerkarte "Device Settings" (Geräteeinstellungen) vornehmen. Aktivieren Sie die Option "IPv6 Addressing" (IPv6-Adressen verwenden) und wählen Sie die manuelle oder automatische Konfiguration aus. Nähere Informationen hierzu finden Sie im Benutzerhandbuch.

Frage	Antwort
Was passiert, wenn ich einen externen Server mit einer IPv6-Adresse habe, den ich mit KX III verwenden möchte?	Der Dominion KX II kann über die IPv6-Adressen auf externe Server zugreifen (z. B. einen SNMP-Manager, Syslog-Server oder LDAP-Server). Durch die Verwendung der Dual-Stack-Architektur von KX III kann auf diese externen Server über Folgendes zugegriffen werden: (1) eine IPv4-Adresse, (2) eine IPv6-Adresse oder (3) einen Hostnamen. KX III unterstützt demnach also die gemischte IPv4-/IPv6-Umgebung, über die viele Kunden verfügen.
Was passiert, wenn mein Netzwerk IPv6 nicht unterstützt?	Die Standard-Netzwerkeinstellungen des KX III sind werkseitig nur für IPv4 eingestellt. Wenn Sie IPv6 verwenden möchten, folgen Sie den oben beschriebenen Anweisungen zum Aktivieren der IPv4-/IPv6-Dual-Stack-Funktion.
Wo erhalte ich weitere Informationen zu IPv6?	Allgemeine Informationen zu IPv6 finden Sie unter www.ipv6.org. Im Benutzerhandbuch des KX III wird die Unterstützung für IPv6 des KX III erläutert.

Server

Frage	Antwort
Ist der Betrieb des Dominion KX III von einem Windows-Server abhängig?	Auf keinen Fall. Da Sie darauf angewiesen sind, dass die KVM-Infrastruktur unter allen Umständen stets verfügbar ist (um auftretende Probleme zu lösen), wurde der Dominion KX III so entwickelt, dass er vollständig unabhängig von jedem externen Server ist.
Wie konfiguriere ich einen Server für die Verbindung mit einem Dominion KX III?	Legen Sie die Mausparameter fest, um die Maussynchronisation zu optimieren, und deaktivieren Sie die Bildschirmschoner und die Features für die Stromzufuhrverwaltung, die sich auf die Bildschirmanzeige auswirken.

Frage	Antwort
Was muss ich bei der Maussynchronisierung beachten?	In der Vergangenheit war die Maussynchronisation mit KVM-über-IP sehr frustrierend. Die Absolute Mouse Synchronization (absolute Maussynchronisation) von Dominion KX III ermöglicht eine hervorragend synchronisierte Maus, ohne dass die Mauseinstellung des Servers auf den Windows- und Apple® Mac-Servern geändert werden muss. Für andere Server kann der Modus "Intellligent Mouse" (Intelligente Maus) oder der schnelle Ein-Cursor-Modus verwendet werden, um das Ändern der Mauseinstellungen auf dem Server zu vermeiden.
Was enthält das Dominion KX III-Paket?	Das Paket enthält Folgendes: (1) Dominion KX III-Einheit, (2) Kurzanleitung, (3) 19-Zoll-Standardgestellhalterung, (4) CD-ROM mit Benutzerhandbuch, (6) Netzkabel, (7) Garantie und andere Dokumentation.

Bladeserver

Frage	Antwort
Kann ich Bladeserver an Dominion KX III anschließen?	Ja. Dominion KX III unterstützt bekannte Bladeservermodelle der führenden Bladeserverhersteller: HP®, IBM®, Dell® and Cisco®.
Welche Bladeserver werden unterstützt?	Die folgenden Modelle werden unterstützt: Dell PowerEdge® 1855, 1955 und M1000e; HP BladeSystem c3000 und c7000; IBM BladeCenter® H, E und S; Cisco UCS B-Serie.
Welches CIM soll ich verwenden?	Dies hängt vom Typ der KVM-Ports der jeweiligen Marke und dem Modell des verwendeten Bladeservers ab. Die folgenden CIMs werden unterstützt: DCIM-PS2, DCIM-USBG2, D2CIM-VUSB und D2CIM-DVUSB.

Frage	Antwort
Welche Arten von Zugriff und Steuerung sind verfügbar?	Dominion KX III ermöglicht automatisierten und sicheren KVM-Zugriff: (1) am Serverschrank, (2) von einem Remotestandort aus über IP, (3) über das CommandCenter und (4) über Modem.
Muss ich Zugriffstasten verwenden, um zwischen Blades zu wechseln?	Bei einigen Bladeservern müssen Sie Zugriffstasten verwenden, um zwischen Blades zu wechseln. Bei Dominion KX III müssen Sie diese Zugriffstasten nicht verwenden. Klicken Sie einfach auf den Namen des Bladeservers und Dominion KX III wechselt automatisch zum entsprechenden Blade, ohne dass Sie eine Zugriffstaste verwenden müssen.
Habe ich Zugriff auf das Verwaltungsmodul des Bladeservers?	Ja. Sie können die URL des Verwaltungsmoduls definieren und über Dominion KX III oder über CommandCenter Secure Gateway darauf zugreifen. Wenn konfiguriert, können Sie mit einem Klick darauf zugreifen.
Wie viele Bladeserver kann ich an Dominion KX III anschließen?	Aus Gründen der Leistung und Zuverlässigkeit können Sie, unabhängig vom Modell, bis zu acht Blade-Chassis an ein Dominion KX III anschließen. Raritan empfiehlt, bis zu doppelt so viele Remote-Verbindungen, wie sie das Gerät unterstützt, anzuschließen. Bei einem KX3-216 mit zwei Remotekanälen empfiehlt Raritan beispielsweise, bis zu vier Bladeserver-Chassis anzuschließen. Sie können natürlich individuelle Server an die übrigen Serverports anschließen.
Ich bin ein Firmenkunde und verwende CommandCenter Secure Gateway. Kann ich über CommandCenter Secure Gateway auf die Bladeserver zugreifen?	Ja. Wenn die Bladeserver auf Dominion KX III konfiguriert sind, kann der CommandCenter Secure Gateway-Benutzer über KVM-Verbindungen auf diese zugreifen. Außerdem können die Bladeserver nach Chassis oder nach benutzerdefinierten CommandCenter Secure Gateway-Ansichten gruppiert werden.
Kann In-Band- oder eingebetteter KVM-Zugriff ebenfalls konfiguriert werden?	In-Band- und eingebetteter Zugriff auf Bladeserver kann in CommandCenter Secure Gateway konfiguriert werden.
Auf einigen meiner Bladeserver führe ich VMware® aus. Wird dies unterstützt?	Ja. Ja, mit CommandCenter Secure Gateway können Sie virtuelle Geräte, die auf Bladeservern ausgeführt werden, anzeigen und auf diese zugreifen.

Frage	Antwort
Werden virtuelle Medien unterstützt?	Dies hängt vom Bladeserver ab. HP-Blades unterstützen virtuelle Medien. IBM BladeCenter (ausgenommen BladeCenter T) unterstützt virtuelle Medien, sofern dies entsprechend konfiguriert wurde. Sie müssen ein virtuelles Medien-CIM, D2CIM-VUSB oder D2CIM-DVUSB verwenden.
Wird die absolute Maussynchronisierung unterstützt?	Server mit internen KVM-Switches innerhalb der Blade-Chassis unterstützen normalerweise keine absolute Maustechnologie. Für HP-Bladeserver und einige Dell-Bladeserver kann ein CIM an jedes Blade angeschlossen werden, sodass die absolute Maussynchronisation unterstützt wird.
Ist der Bladezugriff sicher?	Ja. Beim Bladezugriff werden alle standardmäßigen Dominion KX III-Sicherheitsfunktionen wie 128-Bit- oder 256-Bit-Verschlüsselung verwendet. Außerdem sind bladespezifische Sicherheitsfeatures wie Zugriffsberechtigungen pro Blade und Zugriffstastenblockierung verfügbar, mit deren Hilfe ein unautorisierter Zugriff verhindert wird.
Unterstützt Dominion KSX II oder KX III-101 Blade Server?	Zurzeit unterstützen diese Produkte keine Bladeserver.

Montage

Frage	Antwort
Was muss ich außer dem Switch von Raritan zur Installation des Dominion KX III bestellen?	Für jeden Server, den Sie am Dominion KX III anschließen möchten, benötigen Sie ein Dominion oder Paragon Computer Interface Module (CIM). Hierbei handelt es sich um einen direkt an die Tastatur-, Video- und Mausports des Servers angeschlossenen Adapter.

Frage	Antwort
Welche Art von Kat5-Kabel muss ich für meine Installation verwenden?	Für den Dominion KX III kann jedes Standard-UTP-Kabel (unabgeschirmtes Twisted-Pair-Kabel) verwendet werden, egal ob Kategorie 5, 5e oder 6. In unseren Handbüchern und Marketingunterlagen ist der Einfachheit halber oftmals nur von "Kat5"-Kabeln die Rede. Tatsächlich kann jedes UTP-Kabel für den Dominion KX III verwendet werden.
Welche Arten von Servern können am Dominion KX III angeschlossen werden?	Der Dominion KX III ist vollständig anbieterunabhängig. Jeder Server mit standardmäßigen Tastatur-, Video- und Mausports kann angeschlossen werden. Darüber hinaus können Server mit seriellen Ports über das P2CIM-SER CIM gesteuert werden.
Wie werden Server am Dominion KX III angeschlossen?	Für jeden Server, den Sie am Dominion KX III anschließen möchten, benötigen Sie ein Dominion oder Paragon CIM, das direkt an die Tastatur-, Video- und Mausports des Servers angeschlossen wird. Anschließend verbinden Sie jedes CIM mittels Standard-UTP-Kabel (unabgeschirmtes Twisted-Pair) wie z. B. Kategorie 5, 5e oder 6 mit dem Dominion KX III.
In welcher Distanz zum Dominion KX III müssen die Server aufgestellt sein?	Server können im Allgemeinen abhängig vom Servertyp bis zu 45 m vom Dominion KX III entfernt sein. Für die D2CIM-VUSB-CIMs, die virtuelle Medien und die absolute Maussynchronisierung unterstützen, wird eine Distanz von 30 m empfohlen.
Einige Betriebssysteme stürzen ab, wenn Tastatur oder Maus im Betrieb getrennt werden. Wie wird der durch den Wechsel zu einem anderen Server verur-sachte Absturz von am Dominion KX III ange-schlossenen Servern verhindert?	Jeder Dominion Computer Interface Module-Kopierschutzstecker (DCIM) fungiert als virtuelle Tastatur und Maus für den Server, an dem der Kopierschutzstecker angeschlossen ist. Hierbei spricht man von der KME-Technologie (Keyboard/Mouse Emulation, Tastatur-/Mausemulation). Die KME-Technologie von Raritan besitzt Rechenzentrumsqualität und ist weitaus zuverlässiger als die von einfacheren KVM-Switches: es enthält mehr als 15 Jahre Erfahrung und wurde auf Millionen von Servern weltweit eingesetzt.

Frage	Antwort
Müssen auf den am Dominion KX III angeschlossenen Servern irgendwelche Agents installiert werden?	Die mit einem Dominion KX III verbundenen Server erfordern keine Installation von Softwareagents, da die Verbindung des Dominion KX III mit dem Tastatur-, Video- und Mausport des Servers direkt über Hardware hergestellt wird.
Wie viele Server können an jeder Dominion KX III-Einheit angeschlossen werden?	Die Dominion KX III-Modelle bieten 8, 16 bzw. 32 Serverports in einem 1U-Chassis oder 64 Serverports in einem 2U-Chassis. Dies ist die höchste Portdichte für digitale KVM-Switches der Branche.
Was passiert, wenn ich einen Server vom Dominion KX III trenne und an einer anderen Dominion KX III-Einheit oder an einem anderen Port desselben Dominion KX III anschließe?	Der Dominion KX III aktualisiert automatisch die Serverportnamen, wenn Server an anderen Ports angeschlossen werden. Diese auto-matische Aktualisierung betrifft nicht nur den Port für den lokalen Zugriff, sondern auch alle Remoteclients und die optionale Verwal-tungsanwendung CommandCenter Secure Gateway.
Wie schließe ich ein seriell gesteuertes Gerät (RS-232), wie einen Cisco-Router/-Switch oder einen Headless-Sun-Server, am Dominion KX III an?	Wenn Sie nur wenige seriell gesteuerte Geräte besitzen, können Sie diese mit dem seriellen Konverter "P2CIM-SER" von Raritan an Dominion KX III anschließen. Kunden können Dominion KSX II, ein integrierter KVM- und serieller Switch, verwenden. DKSX-144 enthält vier KVM-über-IP-Ports und vier serielle Ports. DKSX-188 enthält acht KVM-über-IP-Ports und acht serielle Ports. Bei mehreren seriell gesteuerten Geräten empfehlen wir allerdings die Verwendung der Dominion SX-Serie der sicheren Konsolenserver von Raritan. Dominion SX bietet umfassendere serielle Funktionen zu einem günstigeren Preis als Dominion KX III. Die SX-Reihe lässt sich einfach bedienen, konfigurieren und verwalten und kann vollständig in die Implementierung einer Dominion-Serie integriert werden.

Lokaler Port - KX IIII

Frage	Antwort
Kann ich auf meine Server direkt über das Gestell zugreifen?	Ja. Der in einem Gestell montierte Dominion KX III funktioniert genau wie ein herkömmlicher KVM-Switch: Er ermöglicht die Steuerung von bis zu 64 Servern mit nur einer Tastatur, einer Maus und einem Monitor. Sie können mithilfe der browserbasierten Benutzeroberfläche oder mithilfe einer Zugriffstaste zwischen den Servern umschalten.
Kann ich die lokalen Ports mehrerer KX III-Geräte konsolidieren?	Ja. Sie können die lokalen Ports mehrerer KX II-Switches mit einem anderen KX III verbinden, indem Sie die Schichtfunktion von KX III verwenden. Anschließend können Sie von einem einzigen Ort im Rechenzentrum mithilfe einer konsolidierten Portliste auf die mit den KX III-Geräten verbundenen Server zugreifen.
Verhindere ich den Remotezugriff anderer Benutzer auf die Server, wenn ich den lokalen Port verwende?	Nein Der lokale Dominion KX III-Port besitzt einen vollständig unabhängigen Zugriffspfad auf die Server. Dies bedeutet, ein Benutzer kann lokal über das Gestell auf die Server zugreifen, ohne die Anzahl der Benutzer einzuschränken, die gleichzeitig von einem entfernten Standort aus auf das Gestell zugreifen.
Kann ich am lokalen Port eine USB-Tastatur oder Maus anschließen?	Ja. Der Dominion KX III verfügt am lokalen Port über USB-Tastatur- und Mausports. Dominion KX III Switch hat keinen PS/2 Lokal Port. Kunden mit PS/2-Tastaturen und -Mäusen müssen einen PS/2-zu-USB-Adapter verwenden.
Gibt es eine Bildschirmanzeige (OSD) für den lokalen Zugriff am Serverschrank?	Ja, aber der Zugriff auf den Dominion KX II am Serverschrank geht weit über konventionelle Bildschirmanzeigen hinaus. Der lokale Port des Dominion KX III bietet die erste browserbasierte Oberfläche für den lokalen und Remotezugriff auf den Serverschrank. Darüber hinaus können fast alle Verwaltungsfunktionen am Serverschrank ausgeführt werden.
Wie wähle ich zwischen Servern aus, während ich den lokalen Port verwende?	Der lokale Port zeigt die angeschlossenen Server über dieselbe Oberfläche an wie der Remoteclient. Benutzer können durch ein einfaches Klicken der Maus oder mithilfe einer Zugriffstaste die Verbindung zu einem Server herstellen.

Frage	Antwort
Wie stelle ich sicher, dass nur berechtigte Benutzer über den lokalen Port auf Server zugreifen?	Für die Benutzer, die den lokalen Port verwenden möchten, gilt die gleiche Authentifizierungsebene wie für Benutzer, die von einem entfernten Standort zugreifen. Dies bedeutet: Wenn der Dominion KX III zur Interaktion mit einem externen RADIUS-, LDAP- oder Active Directory® Server konfiguriert wurde, erfolgt die Authentifizierung von Benutzern, die versuchen, auf den lokalen Port zuzugreifen, über denselben Server. Ist der externe Authentifizierungsserver nicht verfügbar, schaltet der Dominion KX III auf seine eigene, interne Authentifizierungsdatenbank um. Der Dominion KX III verfügt über eine eigenständige Authentifizierung für die sofortige Installation.

Erweiterter lokaler Port

Frage	Antwort
Was ist der erweiterte lokale Port?	Die Modelle KX2-808 und KX2-832 und KX2-864 verfügen über einen erweiterten lokalen Port. Die entsprechenden Dominion KX III Modelle haben keinen erweiterten lokalen Port. Stattdessen haben KX III Modelle einen Schichtport. Um den digitalen lokalen Port des KX III zu verlängern, können Sie das Produkt Raritan Cat5 Reach DVI für lokalen und Remote-Zugriff auf bis zu 500 Meter verwenden. Siehe ***Verbinden Sie KX III und Cat5 Reach DVI - Erweiterte Lokale Portfunktionalität*** (auf Seite 323)

Zwei Netzteile

Frage	Antwort
Verfügt der Dominion KX III über zwei Netzteile?	Ja. Alle Dominion KX III-Modelle verfügen über zwei Stromeingänge und Netzteile mit automatischem Failover. Sollte ein Stromeingang oder Netzteil ausfallen, wechselt der KX III automatisch zum anderen.
Erkennt das Netzteil des Dominion KX III automatisch die Spannungseinstellungen?	Ja. Das Netzteil des Dominion KX II kann für einen Spannungsbereich von 100 bis 240 V bei 50 bis 60 Hz verwendet werden.
Werde ich benachrich-tigt, falls ein Netzteil oder Stromeingang ausfällt?	Die LED-Anzeige an der Vorderseite des Dominion KX III-Geräts zeigt einen Ausfall der Stromversorgung an. Darüber hinaus wird ein entsprechender Eintrag an das Prüfprotokoll gesendet und in der Benutzeroberfläche des KX II-Remoteclients angezeigt. Falls der Administrator dies konfiguriert hat, werden SNMP- oder Syslog-Ereignisse generiert.

Steuerung über Intelligent Power Distribution Unit (PDU)

Frage	Antwort
Welche Funktionen zur Remote-Stromzufuhrsteuerung bietet der Dominion KX III?	Die intelligenten PDUs von Raritan können an Dominion KX III angeschlossen werden, um die Stromzufuhr der Zielserver und anderer Geräte zu steuern. Für Server müssen Sie lediglich einmal einen Konfigurationsschritt ausführen und können anschließend durch Klicken auf den entsprechenden Servernamen einen abgestürzten Server einschalten, ausschalten bzw. ein- und ausschalten.
Welche Arten von Powerstrips unterstützt der Dominion KX III?	Dominion PX™- und Remote Power Control-(RPC-) Powerstrips von Raritan. Diese sind in vielen Steckdosen-, Stecker-Variationen erhältlich. Die PM-Serie der Powerstrips darf nicht an Dominion KX III angeschlossen werden, da diese Powerstrips das Umschalten der Ausgangsebene nicht ermöglichen.
Wie viele PDUs können an jede Dominion KX III-Einheit angeschlossen werden?	An ein Dominion KX III-Gerät können bis zu acht PDUs angeschlossen werden.

Frage	Antwort
Wie schließe ich die PDU an Dominion KX III an?	Für den Anschluss eines Powerstrips am Dominion KX III müssen Sie das CIM D2CIM-PWR verwenden. Das D2CIM-PWR muss separat erworben werden; es gehört nicht zum Lieferumfang der PDU.
Unterstützt der Dominion KX III Server mehrere Netzteile?	Ja. Der Dominion KX III kann leicht zur Unterstützung von Servern mit mehreren Netzteilen, die an verschiedenen Powerstrips angeschlossen sind, konfiguriert werden. Pro Zielserver können vier Netzteile angeschlossen werden.
Zeigt Dominion KX III Statistiken und Messungen von der PDU an?	Ja. Stromzufuhrstatistiken auf PDU-Ebene, einschließlich Stromzufuhr, Strom und Spannung, werden von der PDU abgerufen und angezeigt.
Erfordert die Remote-Stromzufuhrsteuerung eine spezielle Serverkonfiguration für die angeschlossenen Server?	Einige Server verfügen über Standard-BIOS-Einstellungen, die verhindern, dass der Server nach dem Wiederherstellen der Strom-zufuhr automatisch neu gestartet wird. Informationen zum Ändern dieser Einstellung finden Sie in der Dokumentation des entsprechenden Servers.
Was passiert, wenn ich einen Server aus- und wieder einschalte?	Dies ist mit dem physischen Trennen des Servers vom Stromnetz und dem erneuten Anschließen vergleichbar.

Ethernet und IP-Netzwerk

Frage	Antwort
Welche Geschwindigkeit haben die Ethernet-Schnittstellen des Dominion KX III?	Der Dominion KX III unterstützt sowohl Gigabit- als auch 10/100-Ethernet. Der KX III unterstützt zwei 10/100/1000-Ethernet-Schnittstellen mit konfigurierbaren Geschwindigkeits- und Duplexeinstellungen (entweder automatisch erkannt oder manuell eingestellt).
Kann ich auf den Dominion KX III über eine Drahtlosverbindung zugreifen?	Ja. Der Dominion KX III verwendet nicht nur das Standard-Ethernet, sondern auch eine sehr sparsame Bandbreite mit Video in hoher Qualität. Wenn also ein Wirelessclient über eine Netzwerkverbindung zum Dominion KX III verfügt, können Server auf BIOS-Ebene drahtlos konfiguriert und verwaltet werden.

Frage	Antwort
Bietet der Dominion KX III duale Gigabit-Ethernet-Ports für redundantes Failover oder zum Lastenausgleich?	Ja. Der Dominion KX III verfügt über duale Gigabit-Ethernet-Ports für redundante Failoverfunktionen. Fällt der primäre Ethernet-Port (oder der Switch/Router, an dem der Ethernet-Port angeschlossen ist) aus, verwendet der Dominion KX III den sekundären Netzwerkport mit derselben IP-Adresse, wodurch sichergestellt wird, dass der Serverbetrieb nicht unterbrochen wird. Hierzu muss der Administrator jedoch das automatische Failover aktivieren.
Kann ich den Dominion KX III mit einem VPN verwenden?	Ja. Der Dominion KX III verwendet Schicht 1 bis Schicht 4 Standard-IP-Technologien. Der Datenverkehr kann leicht über Standard-VPNs geleitet werden.
Kann ich den KX III mit einem Proxyserver verwenden?	Ja. Der KX III kann mit einem SOCKS-Proxyserver verwendet werden, vorausgesetzt, der Remote-Client-PC ist entsprechend konfiguriert. Weitere Informationen finden Sie in der Benutzerdokumentation oder der Online-Hilfe.
Wie viele TCP-Ports müssen in meinem Firewall geöffnet sein, um den Netzwerkzugriff auf den Dominion KX III zu ermöglichen?	Es sind zwei Ports erforderlich: TCP-Port 5000 zur Erkennung anderer Dominion-Geräte und zur Kommunikation zwischen Raritan-Geräten und CC-SG und natürlich Port 443 für die HTTPS-Kommunikation.
Sind diese konfigurierbar?	Ja. Die TCP-Ports des Dominion KX III können vom Administrator konfiguriert werden.
Kann der Dominion KX III zusammen mit CITRIX verwendet werden?	Wenn der Dominion KX III korrekt konfiguriert wurde, funktioniert er in der Regel mit Produkten für den Remotezugriff wie CITRIX; Raritan kann jedoch nicht für eine akzeptable Leistung garantieren. Kunden sollten wissen, dass Produkte wie CITRIX ähnliche Technologien zur Videoumleitung wie digitale KVM-Switches verwenden. Das bedeutet, dass gleichzeitig zwei KVM-über-IP-Technologien genutzt werden.
Kann der Dominion KX III DHCP verwenden?	DHCP-Adressen können zwar verwendet werden, Raritan empfiehlt jedoch die Verwendung fester Adressen, da es sich beim Dominion KX III um ein Infrastrukturgerät handelt, bei dem eine feste IP-Adresse den Zugriff und die Wartung vereinfacht.

Frage	Antwort
Ich kann über mein IP-Netzwerk keine Verbindung zum Dominion KX III herstellen. Woran kann das liegen?	Der Dominion KX III ist auf Ihr LAN/WAN angewiesen. Folgende Probleme könnten die Ursache sein: Automatische Ethernet-Aushandlung. In manchen Netzwerken funktioniert die automatische 10/100-Aushandlung nicht ordnungsgemäß, und das Dominion KX III-Gerät muss auf 100 MB/Vollduplex oder die für das Netzwerk zutreffende Einstellung justiert werden. Doppelte IP-Adresse. Wenn der Dominion KX III und ein anderes Gerät dieselbe IP-Adresse haben, wird die Netzwerkverbindung möglicherweise gestört. Port 5000-Konflikte. Verwendet ein anderes Gerät den Port 5000, muss der Dominion KX III-Standardport geändert werden (oder das andere Gerät muss geändert werden). Wird die IP-Adresse eines Dominion KX III geändert oder kommt ein neues Dominion KX III-Gerät hinzu, muss dem System ausreichend Zeit gegeben werden, um die IP- und MAC®-Adressen in den Schicht 2- und Schicht 3-Netzwerken zu verbreiten.

Lokale Portkonsolidierung, Schichten und Kaskadieren

Frage	Antwort
Wie verbinde ich mehrere Dominion KX III-Einheiten physisch zu einer Einzellösung?	Um für einen konsolidierten lokalen Zugriff mehrere KX III-Geräte physisch zu verbinden, können Sie die lokalen Ports mehrerer KX III-Schicht-Switches (kaskadierte Geräte) mit einem KX III-Basisgerät verbinden, das die Schichtfunktion von KX III verwendet. Anschließend können Sie von einem einzigen Ort im Rechenzentrum mithilfe einer konsolidierten Portliste auf die mit den KX III-Geräten verbundenen Server zugreifen. Der Schicht-Port muss verwendet werden, um den KX III-Schicht-Switch mit dem Basis-Switch zu verbinden. Der Zugriff über die konsolidierte Portliste ist im Rechenzentrum oder auch von einem Remote-PC verfügbar. Der Zugriff auf alle an das KX III-Gerät angeschlossene Server kann über eine hierarchische Portliste oder über eine Suche (mit Platzhalter) erfolgen. Es werden zwei Ebenen von Schichten unterstützt. In einer Schichtkonfiguration kann auf maximal 1024 Geräte zugegriffen werden. Die Remote-Stromzufuhrsteuerung wird auch unterstützt. Der Zugriff auf virtuelle Medien, Smart Cards und Blade-Server über einen Schichtzugriff wird in einer zukünftigen Version unterstützt. Diese Funktionen stehen natürlich zur Verfügung, wenn sie über eine standardmäßige Remote-Verbindung aufgerufen werden. Der Zugriff auf den Remote-IP-Server über eine konsolidierte Portliste ist zwar praktisch, aber für eine optimale Leistung empfehlen wir den Remotezugriff auf den Schichtserver vom CommandCenter oder über den mit dem Server verbundenen KX III.

Frage	Antwort
Muss ich die Dominion KX III-Geräte physisch miteinander verbinden?	Mehrere Dominion KX III-Einheiten müssen nicht physisch miteinander verbunden werden. Die einzelnen Dominion KX III-Einheiten werden stattdessen mit dem Netzwerk verbunden und fungieren automatisch als Einzellösung, wenn sie zusammen mit der Verwaltungsanwendung CommandCenter Secure Gateway (CC-SG) von Raritan bereitgestellt werden. CC-SG funktioniert als zentrale Anlaufstelle für den Fernzugriff und die Verwaltung. CC-SG bietet eine bedeutende Palette von Tools, wie z.B. gemeinsame Konfiguration, Firmware-Update und eine einzelne Authentifizierungs- und Autorisierungsdatenbank. Wenn Sie CC-SG für zentralisierten Remotezugriff verwenden, können Sie die Schichtfunktion (Kaskadieren) von KX III nutzen, um lokale Ports mehrerer KX III-Switches zu konsolidieren und von einer Konsole im Rechenzentrum auf maximal 1024 Server zugreifen.
Ist CC-SG erforderlich?	Wenn Sie die Standalone-Verwendung (ohne zentrales Verwaltungssystem) nutzen möchten, arbeiten mehrere KX III-Einheiten weiterhin über das IP-Netzwerk zusammen und werden automatisch skaliert. Sie können von der webbasierten Benutzeroberfläche des KX III auf mehrere Dominion KX III-Switches zugreifen.

Frage	Antwort
Kann ich einen vorhandenen analogen KVM-Switch am Dominion KX III anschließen?	Ja. Analoge KVM-Switches können an einem der Dominion KX II-Serverports angeschlossen werden. Verwenden Sie einfach ein USB-Computer Interface Module (CIM), und schließen Sie es an die Benutzerports des vorhandenen analogen KVM-Switches an. Die Analog KVM-Schalter unterstützen die Hotkey-basierte Schalter. Diese können auf ihren lokalen Ports zu einem Dominion KX III Schalter abgestuft und über eine konsolidierte Portliste, sowohl aus der Ferne, als auch im Rechenzentrum, eingeschaltet werden. Analoge KVM-Switches besitzen unterschiedliche technische Daten, und Raritan bietet keine Gewähr für die Kompatibilität analoger KVM-Switches von Drittanbietern. □?

Computer Interface Modules (CIMs)

Frage	Antwort
Welche Videotypen werden von Ihren CIMs unterstützt?	Unsere CIMs unterstützen analoges VGA-Video. Drei neue CIMs unterstützen die digitalen Videoformate, einschließlich DVI, HDMI und DisplayPort. Hierzu gehören D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI und D2CIM-DVUSB-DP.

Frage	Antwort
Kann ich Computer Interface Modules (CIMs) vom analogen Matrix-KVM-Switch Paragon von Raritan mit dem Dominion KX III verwenden?	Ja. Bestimmte Paragon Computer Interface Modules (CIMs) können mit Dominion KX III verwendet werden. (Eine aktuelle Liste zertifizierter CIMs finden Sie auf der Raritan-Webseite bei den Versionshinweisen zu Dominion KX III). Da Paragon CIMs jedoch teurer sind als Dominion KX III-CIMs (sie umfassen Technologie für die Videoübertragung über eine Entfernung von 304 m), sollten im Allgemeinen keine Paragon CIMs zur Verwendung mit Dominion KX III erworben werden. Werden Paragon CIMs am Dominion KX III angeschlossen, übertragen diese Video wie Dominion KX III-CIMs über eine Entfernung von 46 m und nicht über 304 m (wie beim Anschluss an Paragon.
Unterstützt Dominion KX III Paragon Dual CIMs?	Ja. Dominion KX III unterstützt auch Paragon II Dual CIMs (P2CIM-APS2DUAL und P2CIM-AUSBDUAL), die Server im Rechenzentrum mit zwei verschiedenen Dominion KX III-Switches verbinden können. Wenn ein KX III-Switch nicht verfügbar ist, können Sie über den zweiten KX III-Switch auf den Server zugreifen. Dies ermöglicht einen redundanten Zugriff und erhöht den KVM-Remotezugriff. Hierbei handelt es sich um Paragon CIMs, die die erweiterten Funktionen von KX III, wie virtuelle Medien, absolute Maus usw., nicht unterstützen.

Sicherheit

Frage	Antwort
Ist die Dominion KX III-Einheit FIPS 140-2 zertifiziert?	Dominion KX III verfügt über ein integriertes FIPS 140-2 validiertes kryptografisches Modul, das gemäß der FIPS 140-2-Implementierungsanweisung auf einer Linux-Plattform ausgeführt wird. Dieses kryptografische Modul wird für die Verschlüsselung von KVM-Sitzungsdaten verwendet. Dabei handelt es sich um Video-, Tastatur-, Maus- und Smart Card-Daten sowie um die Daten von virtuellen Medien.
Welche Art von Verschlüsselung verwendet der Dominion KX III?	Der Dominion KX III verwendet sowohl für die SSL-Kommunikation als auch für den eigenen Datenstrom die standardmäßige und sehr sichere 256-Bit-AES- , 128-Bit AES- oder 128-Bit-Verschlüsselung. Zwischen den Remoteclients und dem Dominion KX III werden keinerlei Daten unverschlüsselt übertragen.
Unterstützt der Dominion KX III die AES-Verschlüsselung, die im Rahmen des vom US-amerikanischen National Institute of Standards and Technology entwickelten FIP-Standards empfohlen wird?	Ja. Der Dominion KX III verwendet AES (Advanced Encryption Standard) für noch mehr Sicherheit. Bei AES handelt es sich um einen von den US-Behörden genehmigten kryptografischen Algorithmus, der vom National Institute of Standards and Technology (NIST) in FIPS (Federal Information Processing Standard) 197 empfohlen wird.
Ermöglicht der Dominion KX III die Verschlüsselung von Videodaten? Oder werden nur Tastatur- und Mausdaten verschlüsselt?	Im Gegensatz zu Konkurrenzprodukten, die nur Tastatur- und Mausdaten verschlüsseln, verschlüsselt der Dominion KX III Tastatur-, Maus-, Video- und virtuelle Mediendaten zur Gewährleistung einer hohen Sicherheit.
Wie wird der Dominion KX III in externe Authentifizierungsserver wie Active Directory, RADIUS oder LDAP integriert?	Der Dominion KX III kann leicht für die Weiterleitung aller Authentifizierungsanforderungen an einen externen Server, wie LDAP, Active Directory oder RADIUS, konfiguriert werden. Für jeden authentifizierten Benutzer empfängt der Dominion KX III vom Authentifizierungsserver die Benutzergruppe, der dieser Benutzer angehört. Der Dominion KX III bestimmt daraufhin die Zugriffsrechte entsprechend der Gruppe, der der Benutzer angehört.

Frage	Antwort
Wie werden Benutzernamen und Kennwörter gespeichert?	Bei der Verwendung der internen Authentifizierungsfunktionen des Dominion KX II werden alle wichtigen Informationen wie Benutzernamen und Kennwörter in einem verschlüsselten Format gespeichert. Niemand (und hierzu zählen auch der technische Support und die Entwicklungsabteilung von Raritan) kann diese Benutzernamen und Kennwörter abrufen.
Unterstützt der Dominion KX III die Verwendung sicherer Kennwörter?	Ja. Der Administrator kann im Dominion KX III die Prüfung sicherer Kennwörter konfigurieren, um sicherzustellen, dass benutzerdefinierte Kennwörter unternehmensinternen Richtlinien bzw. Behördenvorschriften genügen, und nicht von Hackern geknackt werden können.
Kann ich mein eigenes digitales Zertifikat auf den Dominion KX IIKX IIII hochladen?	Ja. Sie können selbstsignierte Zertifikate oder digitale Zertifikate einer Zertifizierungsstelle auf Dominion KX III hochladen, um die Authentifizierung und die sichere Kommunikation zu verbessern.
Unterstützt KX III eine konfigurierbare Sicherheitsmeldung?	Ja. Für Behörden, Militär und andere sicherheitsbewusste Kunden, die eine Sicherheitsmeldung vor der Benutzeranmeldung erfordern, kann KX III eine vom Benutzer konfigurierbare Sicherheitsmeldung anzeigen und optional das Akzeptieren der Bedingungen anfordern.
Meine Sicherheitsrichtlinie ermöglicht nicht die Verwendung von standardmäßigen TCP-Portnummern. Kann ich sie ändern?	Ja. Wenn Sie die standardmäßigen TCP/IP-Portnummern vermeiden möchten, um die Sicherheit zu erhöhen, ermöglicht Dominion KX III dem Administrator die Konfiguration alternativer Portnummern.

Smart Card- und CAC-Authentifizierung

Frage	Antwort
Unterstützt Dominion KX III Smart Card- und CAC-Authentifizierung?	Ja. Smart Card- und DoD Common Access Card (CAC)-Authentifikation an Zielservern wird unterstützt.

Frage	Antwort
Was ist CAC?	CAC wird in der Richtlinie Homeland Security Presidential Directive 12 (HSPD-12) angeordnet und ist ein Smart Card-Typ, der von der US-Regierung erstellt und vom US-amerikanischen Militär und den US-amerikanischen Regierungsmitarbeitern verwendet wird. Bei der CAC-Karte handelt es sich um eine multitechnologische Mehrzweckkarte; Ziel ist, nur eine ID-Karte zu verwenden. Weitere Informationen finden Sie in den Standards FIPS 201.
Welche KX III-Modelle unterstützen Smart Cards/CAC?	Alle Dominion KX III-Modelle werden unterstützt. Dominion KX III-101 unterstützt derzeit noch keine Smart Cards und CAC.
Verwenden Unternehmens- und SMB-Kunden auch Smart Cards?	Ja. Die Bundesregierung der USA weist den intensivsten Einsatz von Smart Cards auf.
Welche CIMs unterstützen Smart Cards/CAC?	Die erforderlichen CIMs sind: D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI und D2CIM-DVUSB-DP.
Welche Smart Card-Lesegeräte werden unterstützt?	Die unterstützten Standards bei Lesegeräten sind USB CCID und PC/SC. Eine Liste der zertifizierten Lesegeräte sowie weitere Informationen finden Sie in der Benutzerdokumentation.
Funktioniert die Smart Card-/CAC-Authentifizierung am lokalen Port und über Command Center?	Ja. Die Smart Card-/CAC-Authentifizierung funktioniert am lokalen Port und über Command Center. Schließen Sie für den lokalen Port ein kompatibles Smart Card-Lesegerät an den USB-Port von Dominion KX III an.

Bedienkomfort

Frage	Antwort
Kann der Dominion KX III von einem entfernten Standort aus über einen Webbrowser verwaltet und konfiguriert werden?	Ja. Der Dominion KX III kann von einem entfernten Standort aus über einen Webbrowser vollständig konfiguriert werden. Hierzu muss auf Ihrer Workstation jedoch die entsprechende Version der Java Runtime Environment (JRE) installiert sein. Außer der anfänglichen Einstellung der IP-Adresse des Dominion KX II können alle Lösungsparameter vollständig über das Netzwerk eingerichtet werden. (Über ein Ethernet-Crossoverkabel und die Dominion KX II-Standard-IP-Adresse können Sie sogar die Anfangseinstellungen mit einem Webbrowser konfigurieren.)
Kann ich die Dominion KX III-Konfiguration sichern und wiederherstellen?	Ja. Die Dominion KX II-Konfigurationen für Benutzer und Geräte können zur späteren Wiederherstellung (z. B. nach einer Katastrophe) vollständig gesichert werden. Die Dominion KX III Backup-und Wiederherstellungsfunktionen können über das Netzwerk ferngesteuert oder durch Ihren Web-Browser verwendet werden.
Welche Funktionen zur Prüfung oder Protokol-lierung bietet der Dominion KX III?	Der Dominion KX III protokolliert alle wichtigen Benutzerereignisse mit einem Datums- und Zeitstempel. Z.B. Benutzeran- und -abmeldung, der Benutzerzugriff auf einen bestimmten Server, fehlgeschlagene Anmeldeversuche, Konfigurationsänderungen usw. werden protokolliert,
Kann der Dominion KX III in Syslog integriert werden?	Ja. Der Dominion KX III besitzt nicht nur eigene interne Protokollfunktionen, sondern er kann auch alle protokollierten Ereignisse an einen zentralen Syslog-Server senden.
Kann der Dominion KX III in SNMP integriert werden?	Ja. Der Dominion KX III besitzt nicht nur eigene interne Protokollfunktionen, sondern er kann auch SNMP-Traps an SNMP-Verwaltungssysteme senden. SNMP v2 und v3 werden unterstützt.
Kann ein Administrator Benutzer abmelden?	Ja, Administratoren können anzeigen, welche Benutzer bei welchen Ports angemeldet sind, und können einen Benutzer gegebenenfalls von einem bestimmten Port oder Gerät abmelden.

Frage	Antwort
Kann die interne Uhr des Dominion KX II mit einem Zeitserver synchronisiert werden?	Ja. Der Dominion KX III unterstützt das Standard-NTP-Protokoll für die Synchronisierung mit einem Firmenzeitserver oder mit einem öffentlichen Zeitserver (vorausgesetzt, ausgehende NTP-Anforderungen können über den Firmenfirewall übertragen werden).

Dokumentation und Support

Frage	Antwort
Gibt es eine Online-Hilfe?	Ja. Die Online-Hilfe steht mit der Dokumentation auf raritan.com sowie in der Benutzeroberfläche des KX III zur Verfügung. Die Online-Hilfe enthält KX III Verwaltungs und Anwender-Informationen zur Verwendung der Remote-Konsole, Virtueller KVM Client (VKC) Aktiv KVM Client (AKC) und der lokalen Konsole sowie KX-III-Daten-, Informationsnoten über die Verwendung von KX III mit Paragon II, über die Verbindung KX III mit Cat5 Reach DVI, über die Verbindung KX III mit T1700-LED, und so weiter.
Wo finde ich Dokumentation zu Dominion KX III?	Die Dokumentation steht auf raritan.com bereit. Die Dokumentation wird nach Firmwareversion aufgeführt.
Welche Dokumentation steht zur Verfügung?	Eine Kurzanleitung, eine Online-Hilfe, eine PDF-Version von dem Administrator-Benutzerhandbuch und ein Benutzerhandbuch, sowie Versionshinweise und weitere Informationen stehen zur Verfügung.
Welches CIM muss ich für welchen Server verwenden?	Informationen hierzu finden Sie im CIM Handbuch, das in der KX III-Dokumentation enthalten ist. DVI-, HDMI- und DisplayPort-Videostandards werden mit den neuen digitalen Video-CIMs unterstützt.
Wie lange ist die Garantiezeit für die Hardware des KX III?	Für den Dominion KX III gilt eine standardmäßige Garantie von 2 Jahren, die auf 5 Jahre verlängert werden kann.

Verschiedenes

Frage	Antwort
Wie lautet die Standard-IP-Adresse des Dominion KX III?	192.168.0.192
Wie lauten der Standardbenutzername und das Standardkennwort des Dominion KX III?	Der Standardbenutzername des Dominion KX II lautet "admin" und das Standardkennwort "raritan" (beides mit Kleinbuchstaben geschrieben). Für eine höchstmögliche Sicherheit wird der Administrator des Dominion KX III jedoch beim ersten Hochfahren der Einheit gezwungen, diese Standardeinstellungen zu ändern.
Ich habe mein Dominion KX II-Kennwort geändert und vergessen. Kann mir Raritan helfen, das Kennwort abzurufen?	Der Dominion KX III verfügt über eine Taste zum Zurücksetzen am Gerät, mit der der Auslieferungszustand des Geräts wiederhergestellt werden kann. Dadurch wird auch das Standardkennwort zurückgesetzt.
Wie funktioniert die Migration vom Dominion KX II auf den Dominion KX III?	Grundsätzlich können Sie als KX II-Kunde Ihre vorhandenen Switches noch viele Jahre nutzen. Wenn Ihr Rechenzentrum wächst, können Sie die neuen KX III-Modelle erwerben und einsetzen. Die zentrale Verwaltungsanwendung von Raritan, CommandCenter Secure Gateway (CC-SG), und 6.0 Release unterstützen sowohl KX II- als auch KX III-Switches nahtlos.
Funktionieren meine bisherigen KX II-CIMs mit den Dominion KX III-Switches?	Ja. Vorhandene KX II-CIMs funktionieren mit dem Dominion KX III-Switch. Darüber hinaus können auch ausgewählte Paragon CIMs mit KX III eingesetzt werden. Dies erleichtert Paragon I-Kunden, die zu KVM-über-IP wechseln möchten, die Migration zu KX III. Sie sollten jedoch auch die CIMs D2CIM-VUSB und D2CIM-DVUSB in Erwägung ziehen, die virtuelle Medien und den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisation) unterstützen. Darüber hinaus sind digitale Video-CIMs erhältlich, die DVI, HDMI und DisplayPort unterstützen.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

USA/Kanada/Lateinamerika

Montag bis Freitag
08:00 bis 20:00 Uhr ET (Eastern Time)
Tel.: 800-724-8090 oder 732-764-8886
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.
Fax: 732-764-8887
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

China

Peking

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-10-88091890

Shanghai

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-21-5425-2499

GuangZhou

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-20-8755-5561

Indien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +91-124-410-7881

Japan

Montag bis Freitag
09:30 bis 17:30 Uhr Ortszeit
Tel.: +81-3-3523-5991
E-Mail: support.japan@raritan.com

Europa

Europa

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +31-10-2844040
E-Mail: tech.europe@raritan.com

Großbritannien

Montag bis Freitag
08:30 bis 17:00 Uhr GMT
Telefon +44(0)20-7090-1390

Frankreich

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +33-1-47-56-20-39

Deutschland

Montag bis Freitag
08:30 bis 17:30 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0
E-Mail: rg-support@raritan.com

Melbourne, Australien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +61-3-9866-6887

Taiwan

Montag bis Freitag
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit
Tel.: +886-2-8919-1333
E-Mail: support.apac@raritan.com