Dominion® KX II

KX2-116 KX2-216 KX2-416
KX2-132 KX2-232 KX2-432
KX2-464

Benutzerhandbuch

Version 2.0

DKX2-0B-E

Mai 2007

255-62-4023-00

Diese Seite wurde absichtlich leer gelassen.

Urheberrechts- und Markenschutzinformationen

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.

In Nord- und Südamerika erreichen Sie den technischen Kundendienst von Raritan telefonisch unter (732) 764-8886, per Fax unter (732) 764-8887 oder per E-Mail unter tech@raritan.com

Der technische Kundendienst steht Ihnen von Montag bis Freitag zwischen 8:00 und 20:00 Uhr zur Verfügung.

Informationen über regionale Raritan-Niederlassungen finden Sie auf der letzten Seite dieses Handbuchs.

So vermeiden Sie tödliche Stromschläge und Schäden an Raritan-Geräten:

- Verwenden Sie bei einer Produktkonfiguration kein 2-Draht-Netzkabel.
- Überprüfen Sie die Stromanschlüsse am Computer und Monitor auf korrekte Polarität und Erdung.
- Verwenden Sie nur einen Computer oder Monitor mit geerdeten Anschlüssen. Deaktivieren Sie bei der Verwendung einer Reserve-USV die Stromzufuhr für den Computer, Monitor und andere Geräte.

Sicherheitsrichtlinien zur Montage im Serverschrank

Treffen Sie folgende Vorsichtsmaßnahmen bei Raritan-Produkten mit erforderlicher Gestellmontage:

- Die Betriebstemperatur ist in einem geschlossenen Serverschrank u. U. höher als die Raumtemperatur. Die angegebene maximale Umgebungstemperatur für das Gerät darf nicht überschritten werden (weitere Informationen finden Sie in Anhang A: Technische Daten).
- Sorgen Sie im Serverschrank für eine ausreichende Luftzirkulation.
- Bauen Sie die Geräte vorsichtig im Serverschrank ein, um eine ungleichmäßige Belastung der Geräte zu vermeiden.
- Schließen Sie zur Vermeidung einer Stromnetzüberlastung die Geräte ordnungsgemäß am Stromnetz an.
- Sämtliche Geräte müssen korrekt zur Abzweigleitung geerdet sein, vor allem die Verbindungen zur Stromzufuhr wie beispielsweise Powerstrips (mit Ausnahme von Direktverbindungen).

Inhalt

Abbildungen

Kapitel 1: Einleitung

Überblick über den Dominion KX II

Der Dominion KX II ist ein sicherer digitaler KVM-Switch (Tastatur, Video, Maus) der Unternehmensklasse, der den Zugriff auf BIOS-Ebene (und höher) sowie die Steuerung von bis zu 64 Servern über einen Webbrowser von jedem erdenklichen Ort aus ermöglicht. Am Serverschrank ermöglicht der Dominion KX II die Steuerung auf BIOS-Ebene von bis zu 64 Servern und anderen IT-Geräten über nur eine Tastatur, einen Monitor und eine Maus. Die integrierten Remotezugriffsfunktionen des Dominion KX II bieten weltweit über einen Webbrowser die gleichen Steuerungsmöglichkeiten.

Der Dominion KX II lässt sich mittels einer standardmäßigen UTP-Verkabelung (Kategorie 5/5e/6) einfach installieren. Zu seinen erweiterten Features zählen virtuelle Medien, die 128-Bit-Verschlüsselung, zwei Netzteile, die Remote-Stromzufuhrsteuerung, die Integration von Dual-Ethernet, LDAP, RADIUS, Active Directory und Syslog sowie die Webverwaltung. Diese Features ermöglichen Ihnen längere Betriebszeiten, eine höhere Produktivität und maximale Sicherheit – jederzeit und an jedem Ort.

Die Dominion KX II-Produkte können als eigenständige Geräte eingesetzt werden und benötigen kein zentrales Verwaltungsgerät. Für größere Rechenzentren und Unternehmen können mithilfe der Verwaltungsanwendung CommandCenter Secure Gateway (CC-SG) von Raritan zahlreiche Dominion KX II-Einheiten zu einer *einzelnen* logischen Lösung integriert werden (zusammen mit Dominion SX-Einheiten für den seriellen Remotekonsolenzugriff und Dominion KSX-Einheiten für die Remote-/Zweigniederlassungsverwaltung).

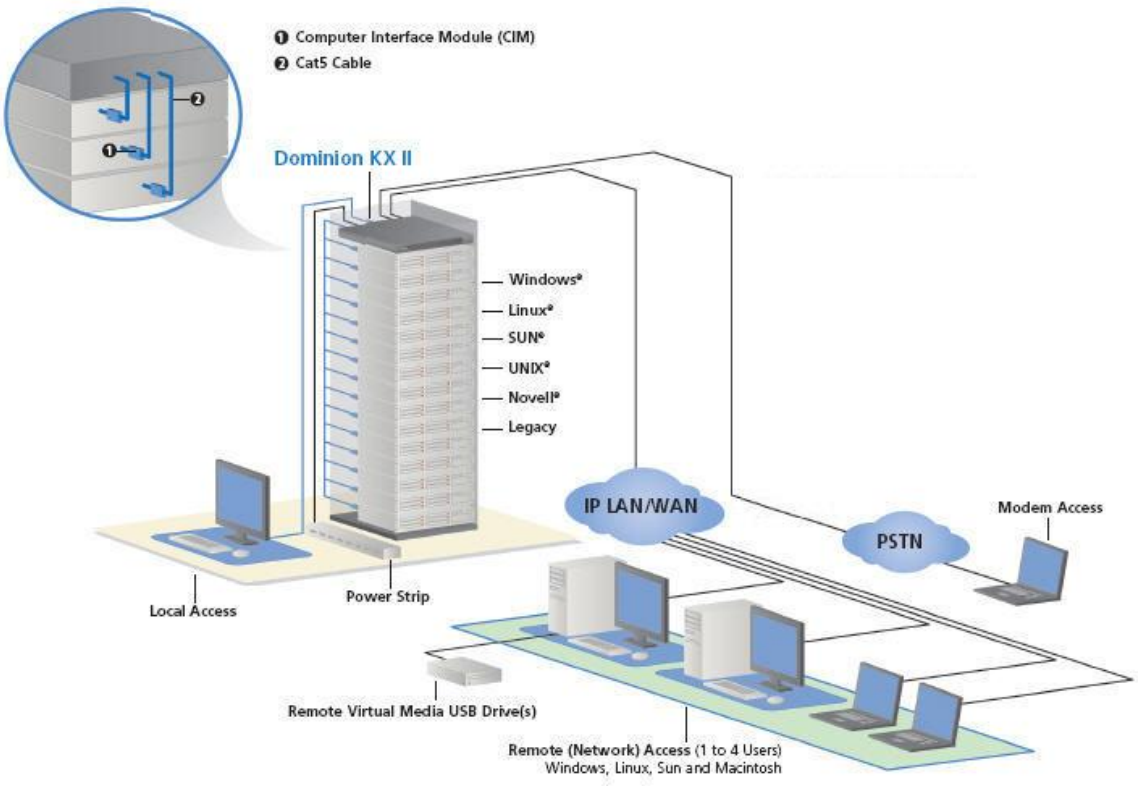

Abbildung 1: Dominion KX II-Konfiguration

Virtuelle Medien

Alle Dominion KX II-Modelle unterstützen virtuelle Medien. Die Vorteile virtueller Medien – Installieren von Remotelaufwerken/-medien auf dem Zielserver zur Unterstützung der Softwareinstallation, Remoteneustarts und -diagnose – stehen nun in allen Dominion KX II-Modellen zur Verfügung.

Jeder Dominion KX II verfügt über virtuelle Medien, um Remoteverwaltungsaufgaben mithilfe einer Vielzahl von CD-, DVD-, USB-, internen und Remotelaufwerken und Abbildern zu ermöglichen. Im Vergleich zu anderen Lösungen unterstützt der Dominion KX II den virtuellen Medienzugriff auf Festplatten und remote installierte Abbilder für mehr Flexibilität und höhere Produktivität.

Virtuelle Mediensitzungen werden durch eine 128-Bit-AES- oder -RC4-Verschlüsselung abgesichert.

Das neue CIM (Computer Interface Module) D2CIM-VUSB unterstützt virtuelle Mediensitzungen mit Zielservern, die über eine USB 2.0-Schnittstelle verfügen. Dieses neue CIM unterstützt darüber hinaus den Mausmodus Absolute Mouse Synchronization™ sowie Remotefirmwareaktualisierungen.

Produktfotos

Abbildung 2: Dominion KX2-116

Abbildung 3: Dominion KX2-432

Abbildung 4: Dominion KX II-CIMs: D2CIM-VUSB (links); D2CIM-PWR (rechts)

Produktfeatures

Hardware

- Integrierter KVM-über-IP-Remotezugriff
- 1U- oder 2U-Einschub (KX2-464); Halterungen im Lieferumfang enthalten
- Zwei Netzteile mit Ausfallsicherung; automatischer Wechsel des Netzteils mit Stromausfallwarnung
- 16, 32 oder 64 (beim KX2-464) Serverports
- Kapazität für mehrere Benutzer (1/2/4 Remotebenutzer, 1 lokaler Benutzer)
- UTP-Serverkabel (Kategorie 5/5e/6)
- Zwei Ethernet-Ports (10/100/1000 LAN) mit Ausfallsicherung
- Während des Betriebs aufrüstbar
- Lokaler Benutzerport für den Serverschrankzugriff
  - Ports für PS/2-Tastatur/Maus
  - Ein USB 2.0-Port an der Vorderseite und drei an der Rückseite für unterstützte USB-Geräte
  - Simultane Reaktion bei Remotebenutzerzugriff
  - Lokale grafische Benutzeroberfläche für die Verwaltung
- Zentralisierte Zugriffssicherheit
- Integrierte Stromzufuhrsteuerung
- LED-Anzeigen für den Status der beiden Netzteile, Netzwerkaktivität und Remotebenutzerstatus
- Taste zum Zurücksetzen der Hardware

Software

- Virtuelle Medien mit CIM D2CIM-VUSB
- Mausmodus Absolute Mouse Synchronization mit CIM D2CIM-VUSB
- Plug-and-Play
- Webbasierte(r) Zugriff und Verwaltung
- Intuitive grafische Benutzeroberfläche
- 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
- SNMP- und Syslog-Verwaltung
- Stromzufuhrsteuerung zur Vermeidung von Fehlern direkt mit Servern verknüpft
- Integration in die Verwaltungsanwendung CommandCenter Secure Gateway (CC-SG) von Raritan
- Feature CC UnManage zum Entfernen eines Geräts aus der CC-SG-Steuerung

Terminologie

In diesem Handbuch wird die im Folgenden erläuterte Terminologie für die Komponenten einer typischen Dominion KX II-Konfiguration verwendet:

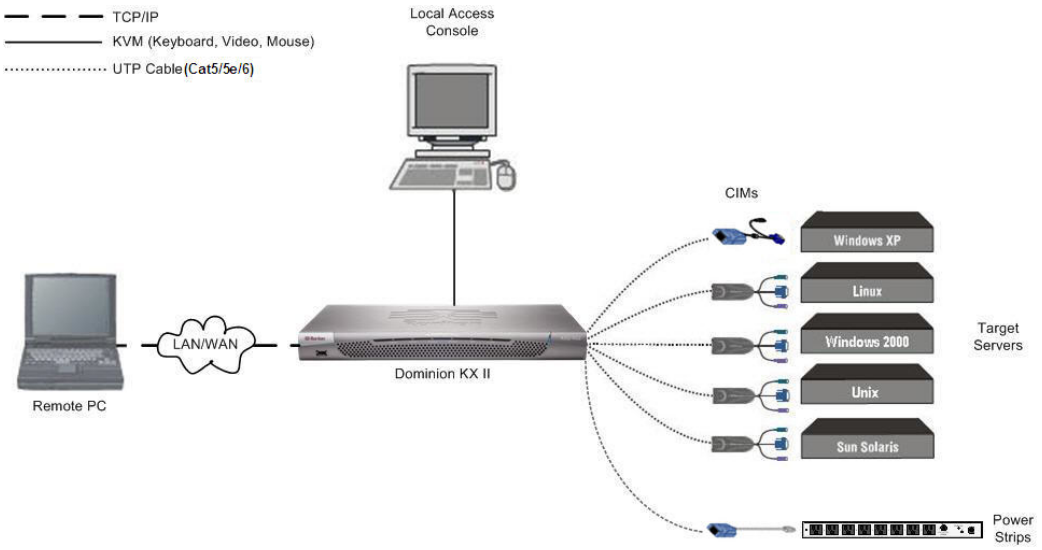

Abbildung 5: Terminologie und Topologie

Remote-PC (Client)	Vernetzte Computer für den Zugriff auf die mit dem Dominion KX II verbundenen Zielserver und deren Steuerung. Eine Liste der vom Dominion KX II unterstützten Remotebetriebssysteme finden Sie unter Unterstützte Betriebssysteme (Clients).
Lokale Zugriffskonsole (Client)	Eine optionale, direkt mit dem Dominion KX II verbundene Benutzerkonsole (bestehend aus Tastatur, Maus und MultiSync-VGA-Monitor) für die lokale Steuerung der Zielserver (direkt am Gestell, nicht über das Netzwerk).
CIMs (Computer Interface Modules)	Dongles, die eine Verbindung mit jedem Zielserver und Raritan-Powerstrip herstellen. Für alle unterstützen Betriebssysteme verfügbar. Informationen zu den vom Dominion KX II unterstützten CIMs finden Sie unter Unterstützte CIMs.
Zielserver	Server mit Videokarten und Benutzeroberflächen (z. B. Windows®, Linux®, Solaris™ usw.), auf die remote über den Dominion KX II zugegriffen wird. Eine Liste der unterstützten Betriebssysteme und CIMs finden Sie unter Unterstützte Betriebssysteme und CIMs (Zielserver).
Powerstrips	Auf Raritan-Powerstrips wird remote über den Dominion KX II zugegriffen.

Paketinhalt

Der Dominion KX II wird als vollständig konfiguriertes, eigenständiges Produkt in einem standardmäßigen 1U-19-Zoll-Gestellchassis (2U für den KX2-464) geliefert. Im Lieferumfang jeder Dominion KX II-Einheit ist Folgendes enthalten:

(1) Dominion KX II-Einheit
(1) Kurzanleitung für die Installation und Konfiguration des Dominion KX II
(1) Raritan-Benutzerhandbuch (CD-ROM)
(1) Gestellmontagekit
(2) Netzkabel
(1) Kat. 5-Netzwerkkabel
(1) Kat. 5-Netzwerk-Crossoverkabel
(1) Vier Gummifüße (für Schreibtischaufstellung)
(1) Anwendungshinweis
(1) Garantiekarte

Benutzerhandbuch

Überblick

Das Benutzerhandbuch zum Dominion KX II enthält die erforderlichen Informationen für die Installation, Einrichtung und Konfiguration, den Zugriff auf Zielserver und Powerstrips, die Verwendung virtueller Medien, die Verwaltung von Benutzern und Sicherheit sowie die Wartung und Diagnose des Dominion KX II.

Dieses Benutzerhandbuch gilt nur für den Dominion KX II (Version 2.0). Informationen zu Version 1.4 finden Sie im *Dominion KX 1.4-Benutzerhandbuch*.

Organisation der Informationen

Das Benutzerhandbuch ist folgendermaßen organisiert:

- Kapitel 1, *Einleitung*. Überblick, Features, Terminologie und Paketinhalt
- Kapitel 2, *Erste Schritte*. Anmeldeinformationen, Standard-IP-Adresse, unterstützte Betriebssysteme, Browser und CIMs
- Kapitel 3, *Installation und Konfiguration*. Zielserverkonfiguration, Firewalleinstellungen, physische Geräteanschlüsse, erste Konfiguration der KX II-Einheit, Remoteauthentifizierung, Benutzer, Gruppen und Zugriffsberechtigungen
- Kapitel 4, *Herstellen einer Verbindung mit dem Dominion KX II*. Benutzeroberflächen, Starten der KX II-Remotekonsole, Dominion KX II-Favoriten
- Kapitel 5, *Zugreifen auf Zielserver*. Zugriff auf, Steuerung von und Wechsel zwischen Zielservern
- Kapitel 6, *Virtual KVM Client*. Zielserversteuerung, Mauszeigersynchronisation, Tastaturmakros und Videoeinstellungen
- Kapitel 7, *Virtuelle Medien*. Konfiguration von virtuellen Medien und Zugriff darauf
- Kapitel 8, *Benutzerverwaltung*. Benutzer- und Gruppenverwaltung, Kennwörter, gruppenbasierte IP-Zugriffssteuerung und Authentifizierungseinstellungen
- Kapitel 9, *Geräteverwaltung*. Netzwerkeinstellungen, Datum/Uhrzeit, Ereignisverwaltung, Netzteilkonfiguration, Portkonfiguration und Stromzufuhrsteuerung
- Kapitel 10, *Sicherheitseinstellungen*. Sicherheitseinstellungen und IP-Zugriffssteuerung
- Kapitel 11, *Wartung*. Prüfprotokoll, Geräteinformationen, Sicherung und Wiederherstellung, Firmware- und CIM-Aktualisierungen, Neustart
- Kapitel 12, *Diagnose*. Netzwerkschnittstelle, Netzwerkstatistik, Ping an den Host, Verfolgen der Route zum Host und KX-Diagnose

- Kapitel 13, *Lokale KX II-Konsole*. Starten der lokalen KX II-Konsole, Zugriff auf Zielserver und lokale Portverwaltung
- Kapitel 14, *CC UnManage*. Entfernen des KX II aus der CC-SG-Steuerung
- Anhang A, *Technische Daten.* Physische Spezifikationen, verwendete Ports, Verbindungsentfernung zum Zielserver und Videoauflösung
- Anhang B, *Aktualisieren des LDAP-Schemas.* Aktualisieren des LDAP-Schemas (für erfahrene Benutzer)
- Anhang C, *Häufig gestellte Fragen (FAQs)*. Allgemeine Fragen, Remotezugriff, universelle virtuelle Medien, Ethernet- und IP-Netzwerke, Server, Installation, lokaler Port, Stromzufuhrsteuerung, Skalierbarkeit, Computer Interface Modules (CIMs), Sicherheit, Verwaltbarkeit, Verschiedenes und Problembehandlung

Verwandte Dokumentation

Weitere Informationen zum Raritan Multi-Platform-Client (MPC) finden Sie im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)*.

Weitere Informationen zur gesamten Produktreihe von Raritan finden Sie im *Raritan-Benutzerhandbuch und in den Kurzanleitungen (CD-ROM)* oder auf der Website von Raritan unter http://www.raritan.com/support/productdocumentation

Kapitel 2: Erste Schritte

Anmeldeinformationen

- Der standardmäßige Dominion KX II-Benutzeranmeldename lautet **admin** und das Standardkennwort **raritan**. Dieser Benutzer besitzt Administratorrechte.
- Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden. Das Standardkennwort **raritan** beispielsweise muss in Kleinbuchstaben eingegeben werden.
- Beim ersten Starten des Dominion KX II müssen Sie dieses Standardkennwort ändern.

Tipp: 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.

Standard-IP-Adresse

Der Dominion KX II wird mit der Standard-IP-Adresse 192.168.0.192 geliefert.

Unterstützte Betriebssysteme (Clients)

Die folgenden Betriebssysteme werden auf der Dominion KX II-Remotekonsole, dem Virtual KVM Client™ und dem Multi-Platform-Client (MPC) unterstützt:

CLIENTBETRIEBSSYSTEM	UNTERSTÜTZUNG VIRTUELLER MEDIEN (VM) AUF CLIENT
Windows XP	Ja
Windows 2000 SP4	Ja
Windows Vista	Ja
Red Hat Linux 9.0	Ja; lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von KX
RedHat Enterprise Workstation 3.0 und 4.0	Ja; lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von KX
SUSE Linux Professional 9.2 und 10	Ja; lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von KX
Fedora™ Core 5 und höher	Ja; lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von KX
Mac®	Nein
Solaris	Nein

Unterstützte Browser

Folgende Browser werden von Dominion KX II unterstützt:

- Internet Explorer 6 und 7
- Firefox® 1.5 und 2.0
- Mozilla® 1.7
- Safari 2.0

Unterstützte Betriebssysteme und CIMs (Zielserver)

Zusätzlich zu den neuen Dominion KX II-D2CIMs werden die meisten Paragon®- und Dominion KX I-CIMs unterstützt. Die folgende Tabelle enthält die unterstützten Betriebssysteme, CIMs, virtuellen Medien und Mausmodi auf Zielservern:

ZIELSERVER	UNTERSTÜTZTE CIMS			VM	MAUSMODI		
	PARAGON CIMS	DOMINION KX I-DCIMS	DOMINION KX II-D2CIMS		AM	IM	SM
Windows XP Windows 2000 Windows 2000 Server Windows 2003 Server Windows Vista	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓	✓	✓
Red Hat Linux 9.0 Red Hat Enterprise Workstation 3.0 und 4.0	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (außer RedHat Enterprise Workstation 3.0)	✓			✓
SUSE Linux Professional 9.2 und 10	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD P2CIM-USBG2 UKVMC USKVMC P2CIM-PS2DUAL	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora Core 3 und höher	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD P2CIM-USBG2 UKVMC USKVMC P2CIM-PS2DUAL	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	P2CIM-AUSB UUSBPD P2CIM-USBG2	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
Alle in Dominion KX I unterstützten Solaris-Betriebssysteme	USKVMC P2CIM-SUN P2CIM-SUSB	DCIM-SUN DCIM-SUSB					✓
IBM AIX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Remote-Powerstrips			D2CIM-PWR				
Serielle Geräte	P2CIM-SER P2CIM-SER-EU AUATC						

Legende:

- VM: Virtuelle Medien (nur D2CIM-VUSB)
- AM: Absolute Mouse Synchronization (nur D2CIM-VUSB)
- IM: Intelligenter Mausmodus
- SM: Standardmausmodus
- ✓: Unterstützt

Hinweis: *D2CIM-VUSB wird auf Sun (Solaris)-Zielservern nicht unterstützt.*

Kapitel 3: Installation und Konfiguration

Überblick

Dieser Abschnitt enthält einen kurzen Überblick über den Installationsprozess. Die einzelnen Schritte werden im Verlauf des Kapitels noch genauer erläutert.

So installieren und konfigurieren Sie den Dominion KX II:

1. Konfigurieren der Zielserver
2. Konfigurieren der Einstellungen für die Netzwerkfirewall
3. Anschließen der Geräte
4. Konfigurieren der Dominion KX II-Einheit

Schritt 1: Konfigurieren der Zielserver

Die Zielserver sind die Computer, auf die über den Dominion KX II zugegriffen wird und die von ihm aus gesteuert werden. Konfigurieren Sie vor der Installation des Dominion KX II *alle* Zielserver, um eine optimale Leistung sicherzustellen. Diese Konfiguration gilt nur für *Zielserver*, nicht jedoch für Clientworkstations (Remote-PCs), die für den Remotezugriff auf den Dominion KX II verwendet werden. Weitere Informationen finden Sie in Kapitel 1: Einführung, Terminologie.

So konfigurieren Sie die Zielserver:

- Prüfen der Videoauflösung
- Prüfen des Desktop-Hintergrunds
- Anpassen der Mauseinstellungen
- Durchführen der betriebssystemspezifischen Maus- und Videokonfiguration

Videoauflösung

Stellen Sie sicher, dass die Videoauflösung und Aktualisierungsfrequenz jedes Zielservers von Dominion KX II unterstützt werden und dass das Signal *keinen Zeilensprung* beinhaltet.

Unterstützte Videoauflösungen

Dominion KX II unterstützt die folgenden Auflösungen:

640 x 350 bei 70 Hz	720 x 400 bei 85 Hz	1.024 x 768 bei 90 Hz
640 x 350 bei 85 Hz	800 x 600 bei 56 Hz	1.024 x 768 bei 100 Hz
640 x 400 bei 56 Hz	800 x 600 bei 60 Hz	1.152 x 864 bei 60 Hz
640 x 400 bei 84 Hz	800 x 600 bei 70 Hz	1.152 x 864 bei 70 Hz
640 x 400 bei 85 Hz	800 x 600 bei 72 Hz	1.152 x 864 bei 75 Hz
640 x 480 bei 60 Hz	800 x 600 bei 75 Hz	1.152 x 864 bei 85 Hz
640 x 480 bei 66,6 Hz	800 x 600 bei 85 Hz	1.152 x 870 bei 75,1 Hz
640 x 480 bei 72 Hz	800 x 600 bei 90 Hz	1.152 x 900 bei 66 Hz
640 x 480 bei 75 Hz	800 x 600 bei 100 Hz	1.152 x 900 bei 76 Hz
640 x 480 bei 85 Hz	832 x 624 bei 75,1 Hz	1.280 x 960 bei 60 Hz
640 x 480 bei 90 Hz	1.024 x 768 bei 60 Hz	1.280 x 960 bei 85 Hz
640 x 480 bei 100 Hz	1.024 x 768 bei 70 Hz	1.280 x 1.024 bei 60 Hz
640 x 480 bei 120 Hz	1.024 x 768 bei 72 Hz	1.280 x 1.024 bei 75 Hz
720 x 400 bei 70 Hz	1.024 x 768 bei 75 Hz	1.280 x 1.024 bei 85 Hz
720 x 400 bei 84 Hz	1.024 x 768 bei 85 Hz	1.600 x 1.200 bei 60 Hz

Hinweis: *Für Composite Sync- und Sync-on-Green-Video ist ein zusätzlicher Adapter erforderlich.*

Desktop-Hintergrund

Für optimale Bandbreiteneffizienz und Bildleistung müssen Zielserver mit grafischen Benutzeroberflächen, wie unter Windows, Linux, X-Windows, Solaris und KDE, konfiguriert werden. Der Desktop-Hintergrund muss nicht *völlig* einfarbig sein, doch können Hintergrundbilder mit Fotos oder komplexen Farbverläufen die Leistung verringern.

Mauseinstellungen

Der Dominion KX II arbeitet in verschiedenen Mausmodi:

- Absolute Mouse Synchronization (nur D2CIM-VUSB)
- Intelligenter Mausmodus (verwenden Sie keinen animierten Cursor)
- Standardmausmodus

In den Mausmodi **Standard** und **Intelligent** müssen die Mausparameter auf bestimmte Werte festgelegt werden. Diese Werte werden weiter unten in diesem Handbuch beschrieben. Für den Mausmodus **Absolute Mouse Synchronization** müssen die Mausparameter nicht geändert werden. Für diesen Modus ist D2CIM-VUSB erforderlich. Die Mauskonfigurationen variieren auf unterschiedlichen Zielbetriebssystemen. Weitere Details finden Sie in der Dokumentation des jeweiligen Betriebssystems.

Der Intelligente Mausmodus funktioniert auf den meisten Windows-Plattformen. Wenn auf dem Zielgerät der Active Desktop aktiviert ist, kann dieser Modus jedoch zu unvorhersehbaren Ergebnissen führen. Weitere Informationen zum Intelligenten Mausmodus finden Sie im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)* (*Anhang B: Bedingungen zur intelligenten Maussynchronisation*). Dieses Handbuch finden Sie auf der Website von Raritan unter http://www.raritan.com/support/productdocumentation oder auf der CD-ROM mit dem Raritan-Benutzerhandbuch und den Kurzanleitungen, die im Lieferumfang von Dominion KX II enthalten ist.

Betriebssystemspezifische Maus- und Videoeinstellungen

Dieser Abschnitt enthält Informationen über die Video- und Mauseinstellungen je nach Betriebssystem, das auf dem Zielserver ausgeführt wird.

Einstellungen für Windows XP/Windows 2003

So konfigurieren Sie Zielserver, auf denen Microsoft Windows XP/2003 ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie **Start > Systemsteuerung > Maus**.
   b. Öffnen Sie die Registerkarte **Zeigeroptionen**. Führen Sie im Bereich **Bewegung** folgende Schritte aus:
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Deaktivieren Sie das Kontrollkästchen **Zeigerbeschleunigung verbessern**.
      - Klicken Sie auf **OK** (Senden).

2. Deaktivieren Sie die Übergangseffekte:
   a. Wählen Sie in der Systemsteuerung die Option **Anzeige**.
   b. Öffnen Sie die Registerkarte **Darstellung**.
   c. Klicken Sie auf die Schaltfläche **Effekte**.
   d. Deaktivieren Sie das Kontrollkästchen **Folgende Übergangseffekte für Menüs und QuickInfos verwenden**.
   e. Klicken Sie auf **OK** (Senden).
   f. Schließen Sie die Systemsteuerung.

Hinweis: *Für Zielserver, auf denen Windows 2000 oder XP ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über den Dominion KX II verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/ -beschleunigung auf die Dominion KX II-Verbindung beschränken.*

Die Anmeldemasken von Windows XP und 2000 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung des Dominion KX II empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisation möglicherweise nicht optimal. Wenn Sie sich mit dem Anpassen der Registrierung von Windows-Zielservern auskennen, können Sie in den Anmeldemasken eine bessere Dominion KX II-Maussynchronisation erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern (HKEY_CURRENT_USER\Systemsteuerung\Maus): MouseSpeed = 0; MouseThreshold 1= 0; MouseThreshold 2 = 0.

Einstellungen für Windows 2000

So konfigurieren Sie Zielserver, auf denen Microsoft Windows 2000 ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie **Start > Systemsteuerung > Maus**.
   b. Öffnen Sie die Registerkarte **Bewegung**.
      - Stellen Sie die Beschleunigung auf **Keine** ein.
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Klicken Sie auf **OK** (Senden).
2. Deaktivieren Sie die Übergangseffekte:
   a. Wählen Sie in der Systemsteuerung die Option **Anzeige**.
   b. Öffnen Sie die Registerkarte **Effekte**.
   c. Deaktivieren Sie das Kontrollkästchen **Folgende Übergangseffekte für Menüs und QuickInfos verwenden**.
   d. Klicken Sie auf **OK** (Senden).
   e. Schließen Sie die Systemsteuerung.

Windows Vista

So konfigurieren Sie Zielserver, auf denen Microsoft Windows Vista ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie **Start > Einstellungen > Systemsteuerung > Maus**.
   b. Öffnen Sie die Registerkarte **Zeigeroptionen**. Führen Sie im Bereich **Bewegung** folgende Schritte aus:
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Deaktivieren Sie das Kontrollkästchen **Zeigerbeschleunigung verbessern**.
      - Klicken Sie auf **OK** (Senden).
2. Deaktivieren Sie die Animations- und Einblendeffekte:
   a. Wählen Sie in der Systemsteuerung die Option **System**.
   b. Wählen Sie **Erweiterte Systemeinstellungen**. Das Dialogfeld **Systemeigenschaften** wird angezeigt.
   c. Öffnen Sie die Registerkarte **Erweitert**.
   d. Klicken Sie in der Gruppe **Leistung** auf die Schaltfläche **Einstellungen**. Das Dialogfeld **Leistungsoptionen** wird angezeigt.
   e. Deaktivieren Sie im Bereich **Benutzerdefiniert** die folgenden Kontrollkästchen:

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

   f. Klicken Sie auf **OK** (Senden).
   g. Schließen Sie die Systemsteuerung.

Einstellungen für Linux

Hinweis: *Die folgenden Einstellungen gelten nur für den Standardmausmodus.*

So konfigurieren Sie Zielserver, auf denen Linux ausgeführt wird (grafische Benutzeroberfläche):

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie **System > Preferences > Mouse** (System > Einstellungen > Maus). Das Dialogfeld **Mouse Preferences** (Mauseinstellungen) wird angezeigt.
   b. Öffnen Sie die Registerkarte **Bewegung**.
   c. Legen Sie die Einstellung für **Speed Acceleration** (Beschleunigung) auf 1 fest.
   d. Legen Sie die Einstellung für **Drag & Drop Threshold** (Drag & Drop-Grenzwert) auf 1 fest.

2. Konfigurieren der Bildschirmauflösung:
   a. Wählen Sie **System > Preferences > Screen Resolution** (System > Einstellungen > Bildschirmauflösung). Das Dialogfeld **Screen Resolution Preferences** (Einstellungen für Bildschirmauflösung) wird angezeigt.
   b. Wählen Sie unter **Resolution** (Auflösung) und **Refresh Rate** (Aktualisierungsfrequenz) Werte, die von Dominion KX II unterstützt werden.

Hinweis: *In vielen grafischen Linux-Umgebungen ändert der Befehl <**CTRL**> <**ALT**> <+> (Strg+Alt+Plus) die Videoauflösung, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei XF86Config durchgeführt wird.*

So konfigurieren Sie Zielserver, auf denen Linux ausgeführt (Befehlszeile):

1. Stellen Sie die Mausbeschleunigung und den Grenzwert genau auf 1 ein. Geben Sie folgenden Befehl ein: **xset mouse 1 1** Die Einstellung sollte bei der Anmeldung übernommen werden.
2. Stellen Sie sicher, dass jeder Linux-Zielserver eine von Dominion KX II unterstützte Auflösung mit einer standardmäßigen VESA-Auflösung und Aktualisierungsfrequenz verwendet.
3. Jeder Linux-Zielserver sollte außerdem so eingestellt sein, dass sich die Deaktivierungszeiten im Bereich von ±40 % der VESA-Standardwerte bewegen.
   - Rufen Sie die Xfree86-Konfigurationsdatei XF86Config auf.
   - Deaktivieren Sie in einem Text-Editor alle nicht von Dominion KX II unterstützten Auflösungen.
   - Deaktivieren Sie die virtuelle Desktop-Funktion (wird nicht von Dominion KX II unterstützt).
   - Prüfen Sie die Deaktivierungszeiten (±40 % der VESA-Standardwerte)
   - Starten Sie den Computer neu.

Hinweis für Red Hat 9-Zielserver

Wenn auf dem Zielserver Red Hat 9 ausgeführt wird und bei Verwendung des D2CIM-VUSB Probleme mit der Tastatur und/oder der Maus auftreten, können Sie eine zusätzliche Konfigurationseinstellung vornehmen.

Tipp: Sie müssen diese Schritte ggf. nach der Installation eines Betriebssystems durchführen.

So konfigurieren Sie Red Hat 9-Server mit dem D2CIM-VUSB:

1. Navigieren Sie zur Konfigurationsdatei Ihres Systems (in der Regel **/etc/modules.conf**).
2. Verwenden Sie einen Editor Ihrer Wahl, und stellen Sie sicher, dass die Zeile **alias usb-controller** in der Datei **modules.conf** wie folgt lautet:
   ```
   alias usb-controller usb-uhci
   ```

   Hinweis: *Wenn die Datei **/etc/modules.conf** bereits eine andere Zeile mit **usb-uhci** enthält, muss die Zeile entfernt oder auskommentiert werden.*
3. Speichern Sie die Datei.
4. Starten Sie das System neu, um die Änderungen zu übernehmen.

Einstellungen für Sun Solaris

So konfigurieren Sie Zielserver, auf denen Sun Solaris ausgeführt wird:

Stellen Sie die Mausbeschleunigung und den Schwellenwert genau auf 1 ein. Dazu haben Sie folgende Möglichkeiten:

– Über die grafische Benutzeroberfläche:

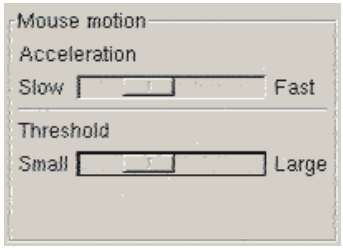

Abbildung 6: Mauskonfiguration unter Solaris

– Über die Befehlszeile:

```
xset mouse a t
```

Dabei ist *a* die Beschleunigung und *t* der Grenzwert.

Für alle Zielserver muss eine vom Dominion KX II unterstützte Anzeigeauflösung konfiguriert werden. Nachfolgend die am häufigsten verwendeten, unterstützten Auflösungen für Sun-Systeme:

1024 x 768 bei 60 Hz
1024 x 768 bei 70 Hz
1024 x 768 bei 75 Hz
1024 x 768 bei 85 Hz
1152 x 900 bei 66 Hz
1152 x 900 bei 76 Hz
1280 x 1024 bei 60 Hz

Zielserver mit dem Solaris-Betriebssystem müssen eine VGA-Buchse mit TV-Out-Signal haben (mit H- und V-Synchronisierung, keine Composite-Synchronisierung).

So ändern Sie den Sun-Grafikkartenausgang von der Composite-Synchronisierung auf die nicht standardmäßige VGA-Ausgabe:

1. Geben Sie den Befehl **Stop+A** aus, um in den BootProm-Modus zu wechseln.
2. Geben Sie den folgenden Befehl aus, um die Ausgabeauflösung zu ändern:

   ```
   setenv output-device screen:r1024x768x70
   ```

3. Starten Sie den Server mit dem Befehl **boot** neu.

Sie können sich stattdessen auch an Ihren Raritan-Ansprechpartner wenden und einen Videoausgabeadapter erwerben.

VORHANDENE EINSTELLUNG	ZU VERWENDENDER VIDEOAUSGABEADAPTER
Sun 13W3 mit Composite-Synchronisierungsausgabe	APSSUN II Guardian-Converter
Sun HD15 mit Composite-Synchronisierungsausgabe	1396C-Converter für die Konvertierung von HD15 zu 13W3 und ein APSSUN II Guardian-Converter, der die Composite-Synchronisierung unterstützt
Sun HD15 mit separater Synchronisierungsausgabe	APKMSUN Guardian-Converter

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 oben in der linken Ecke ein helles Symbol.*

Einstellungen für Apple Macintosh

Bei Zielservern, auf denen ein Apple Macintosh-Betriebssystem ausgeführt wird, sollten Sie D2CIM-VUSB und den Mausmodus Absolute Mouse Synchronization verwenden.

Hinweis: *Wenn Probleme auftreten, aktivieren Sie das Kontrollkästchen* ***Absolute mouse scaling for MAC server*** *(Absolute Mausskalierung für MAC-Server) auf der Seite Port.*

Einstellungen für IBM AIX

So konfigurieren Sie Zielserver, auf denen IBM AIX ausgeführt wird:

Navigieren Sie 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 2: Konfigurieren der Einstellungen für die Netzwerkfirewall

Wenn Sie über eine Netzwerkfirewall auf den Dominion KX II zugreifen möchten, muss die Firewall die Kommunikation über TCP-Port 5000 oder einen anderen von Ihnen festgelegten Port zulassen. Weitere Informationen zum Festlegen eines anderen Erkennungsports finden Sie unter Netzwerkeinstellungen.

Firewalleinstellungen

FEATURES DES DOMINION KX II	BENÖTIGTE FIREWALLEINSTELLUNGEN FÜR EINGEHENDE KOMMUNIKATION
Webzugriffsfunktionen	Port 443 – Standard-TCP-Port für HTTPS-Kommunikation
Automatische Umleitung von HTTP-Anfragen auf HTTPS (damit Benutzer „http://xxx.xxx.xxx.xxx“ anstelle von „https://xxx.xxx.xxx.xxx“ eingeben können)	Port 80 – Standard-TCP-Port für HTTP-Kommunikation

Schritt 3: Anschließen der Geräte

Schließen Sie den Dominion KX II an die Stromversorgung, das Netzwerk, den lokalen PC und die Zielserver an. Die Zahlen im Diagramm entsprechen den Abschnitten, in denen der jeweilige Anschluss beschrieben wird.

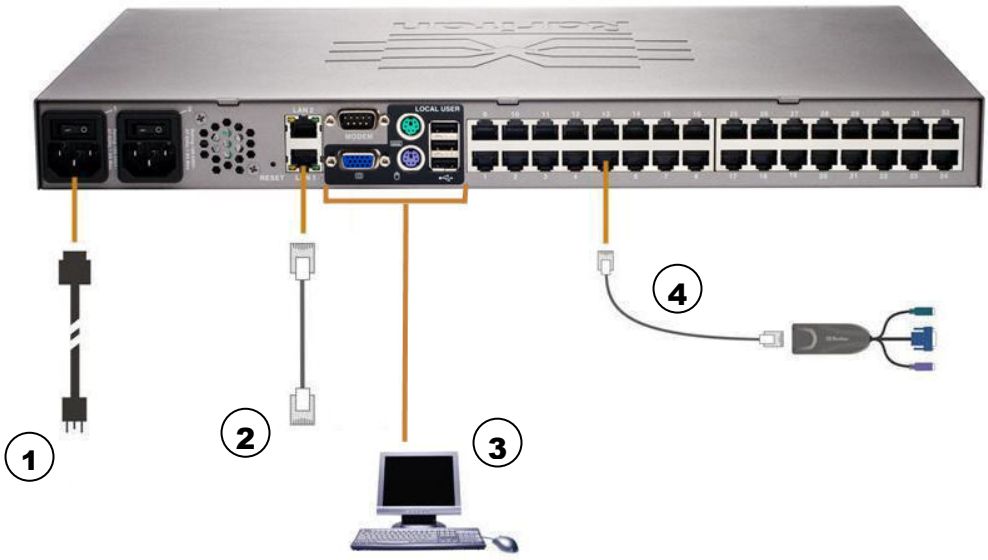

Abbildung 7: Anschlüsse des Dominion KX II

1. Wechselstromversorgung

So schließen Sie die Stromversorgung an:

1. Verbinden Sie das beiliegende Netzkabel mit dem Dominion KX II, und schließen Sie es an eine Netzsteckdose 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.

Hinweis: *Wenn Sie nur ein Netzkabel mit dem System verbinden, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite des Dominion KX II rot, da das System für die automatische Erkennung beider Stromquellen eingerichtet ist. Informationen zum Deaktivieren der automatischen Erkennung für die nicht genutzte Stromquelle finden Sie auf der* *Seite* ***Power Supply Setup*** *(Netzteilkonfiguration)**.*

2. Netzwerkports

Der Dominion KX II ist zu Failoverzwecken (nicht zum Lastenausgleich) mit zwei Ethernet-Ports ausgestattet. Standardmäßig ist nur LAN1 aktiviert, und das automatische Failover ist deaktiviert. Wenn die interne Dominion KX II-Netzwerkschnittstelle oder der mit dem Dominion KX II verbundene Netzwerkswitch nicht verfügbar sein sollte, wird der Port LAN2 unter Verwendung *derselben* IP-Adresse aktiviert, sofern die Option für LAN2 aktiviert wurde.

So stellen Sie eine Netzwerkverbindung her:

1. Verbinden Sie den Netzwerkport LAN1 über ein standardmäßiges Ethernet-Kabel (im Lieferumfang enthalten) mit einem Ethernet-Switch, -Hub oder -Router.

2. Führen Sie die folgenden Schritte aus, wenn Sie die optionalen Ethernet-Failoverfunktionen des Dominion KX II nutzen möchten:
   - Verbinden Sie den Netzwerkport LAN2 über ein standardmäßiges Ethernet-Kabel mit einem Ethernet-Switch, -Hub oder -Router.
   - Aktivieren Sie im Bildschirm **Network Configuration** (Netzwerkkonfiguration) das automatische Failover. (Weitere Informationen finden Sie unter Netzwerkeinstellungen, LAN-Schnittstelleneinstellungen.)

Verwenden Sie nur beide Netzwerkports, wenn Sie einen als Failoverport nutzen möchten.

3. Port für den lokalen Zugriff (lokaler PC)

Für den bequemen Zugriff auf Zielserver am Serverschrank kann der Port für den lokalen Zugriff des Dominion KX II verwendet werden. Der lokale Port wird für die Installation und Konfiguration *benötigt*, aber die weitere Verwendung dieses Ports ist *optional*. Der lokale Port bietet die grafische Benutzeroberfläche der lokalen KX II-Konsole, die für die Verwaltung und für den Zugriff auf Zielserver verwendet wird.

So stellen Sie eine Verbindung zum lokalen Port her:

Schließen Sie einen MultiSync-VGA-Monitor, eine Maus und eine Tastatur an die Ports mit der Bezeichnung „Local User“ (lokaler Benutzer) an. Verwenden Sie eine PS/2- oder USB-Tastatur und -Maus.

4. Zielserverports

Der Dominion KX II wird über standardmäßige UTP-Kabel (Cat 5/5e/6) mit den Zielservern verbunden. Weitere Informationen finden Sie in Anhang A: Technische Daten.

So verbinden Sie einen Zielserver mit dem Dominion KX II:

1. Verwenden Sie das entsprechende CIM (Computer Interface Module). Weitere Informationen zu den CIMs, die mit einem Betriebssystem verwendet werden können, finden Sie unter Unterstützte CIMs.
2. Schließen Sie den HD15-Videostecker des CIM an den Videoport des Zielservers an. Stellen Sie sicher, dass die Videokarte des Zielservers bereits auf eine unterstützte Auflösung und Aktualisierungsfrequenz eingestellt wurde. Für Sun-Server müssen Sie sich zudem vergewissern, dass die Videokarte des Zielservers zur Ausgabe von Standard-VGA (H-und-V-Synchronisation) und nicht zur zusammengesetzten Synchronisation konfiguriert ist.
3. Schließen Sie die Tastatur-/Mausstecker des CIM an die entsprechenden Ports des Zielservers an. Verbinden Sie das CIM über ein standardmäßiges Straight-Through-UTP-Kabel (Cat 5/5e/6) mit einem freien Serverport auf der Rückseite des Dominion KX II.

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 für die **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) (Raritan Computer, Inc. Aktueller Tastaturlayoutcode = 22h [US5 UNIX]).
3. Geben Sie den gewünschten Layoutcode ein (für eine japanische Tastatur beispielsweise **31**).

4. Drücken Sie die Eingabetaste.
5. Schalten Sie die Einheit aus und wieder ein. Das DCIM-SUSB wird zurückgesetzt (Ein- und Ausschalten).
6. Geben Sie auf dem MPC etwas ein, um das Tastaturlayout zu testen.

Schritt 4: Erstkonfiguration des Dominion KX II

Wenn Sie die Dominion KX II-Einheit zum ersten Mal starten, müssen Sie einige Konfigurationseinstellungen über die lokale KX II-Konsole vornehmen:

- Ändern des Standardkennworts.
- Zuweisen der IP-Adresse
- Benennen der Zielserver
- Festlegen der automatischen Netzteilerkennung

Ändern des Standardkennworts

Der Dominion KX II wird mit einem Standardkennwort geliefert. *Beim ersten Starten des Dominion KX II müssen Sie dieses Kennwort ändern.*

So ändern Sie das Standardkennwort:

1. Schalten Sie den Dominion KX II über den bzw. die Netzschalter auf der Rückseite des Geräts ein. Warten Sie, bis der Bootvorgang des Dominion KX II abgeschlossen ist. (Bei Abschluss des Bootvorgangs wird ein Tonsignal ausgegeben.)
2. Nach dem Bootvorgang des Dominion KX II wird die lokale KX II-Konsole auf dem Monitor angezeigt, der an den lokalen Port des Dominion KX II angeschlossen ist. Geben Sie den standardmäßigen Benutzernamen (**admin**) und das standardmäßige Kennwort (**raritan**) ein, und klicken Sie dann auf **Login** (Anmelden). Das Fenster Change Password (Kennwort ändern) wird angezeigt.
3. Geben Sie in das Feld **Old Password** (Altes Kennwort) Ihr altes Kennwort (**raritan**) ein.
4. Geben Sie im Feld **New Password** (Neues Kennwort) das neue Kennwort ein, und geben Sie es im Feld **Confirm New Password** (Neues Kennwort bestätigen) erneut ein. Kennwörter dürfen maximal 64 alphanumerische Zeichen der englischen Sprache sowie die in der unten stehenden Tabelle enthaltenen Sonderzeichen umfassen.
5. Klicken Sie auf **Übernehmen**.
6. Die erfolgreiche Änderung des Kennworts wird bestätigt. Klicken Sie auf **OK** (Senden). Die Seite **Port Access** (Portzugriff) wird angezeigt.

Hinweis: *Das Standardkennwort kann auch mittels des Multi-Platform-Clients (MPC) von Raritan geändert werden. Weitere Informationen hierzu finden Sie im* ***Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)****.*

Gültige Sonderzeichen

ZEICHEN	BESCHREIBUNG	ZEICHEN	BESCHREIBUNG
!	Ausrufezeichen	:	Doppelpunkt
"	Doppeltes Anführungszeichen	;	Strichpunkt
#	Raute	=	Gleichheitszeichen
$	Dollarzeichen	>	Größer-als-Zeichen
%	Prozentzeichen	?	Fragezeichen
&	Kaufmännisches Und	@	At-Zeichen
'	Einfaches Anführungszeichen	[	Linke eckige Klammer
(	Linke runde Klammer	\	Umgekehrter Schrägstrich
)	Rechte runde Klammer	]	Rechte eckige Klammer
*	Sternchen	^	Zirkumflexzeichen
+	Pluszeichen	_	Unterstreichungszeichen
,	Komma	`	Graviszeichen
-	Bindestrich	{	Linke geschweifte Klammer
.	Punkt	|	Senkrechter Strich
/	Schrägstrich	}	Rechte geschweifte Klammer
<	Kleiner-als-Zeichen	~	Tilde

Zuweisen einer IP-Adresse

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

1. Wählen Sie in der lokalen KX II-Konsole **Device Settings** > **Network Settings** (Geräteeinstellungen > Netzwerkeinstellungen) aus. Das Menü Network Settings (Netzwerkeinstellungen) wird angezeigt.

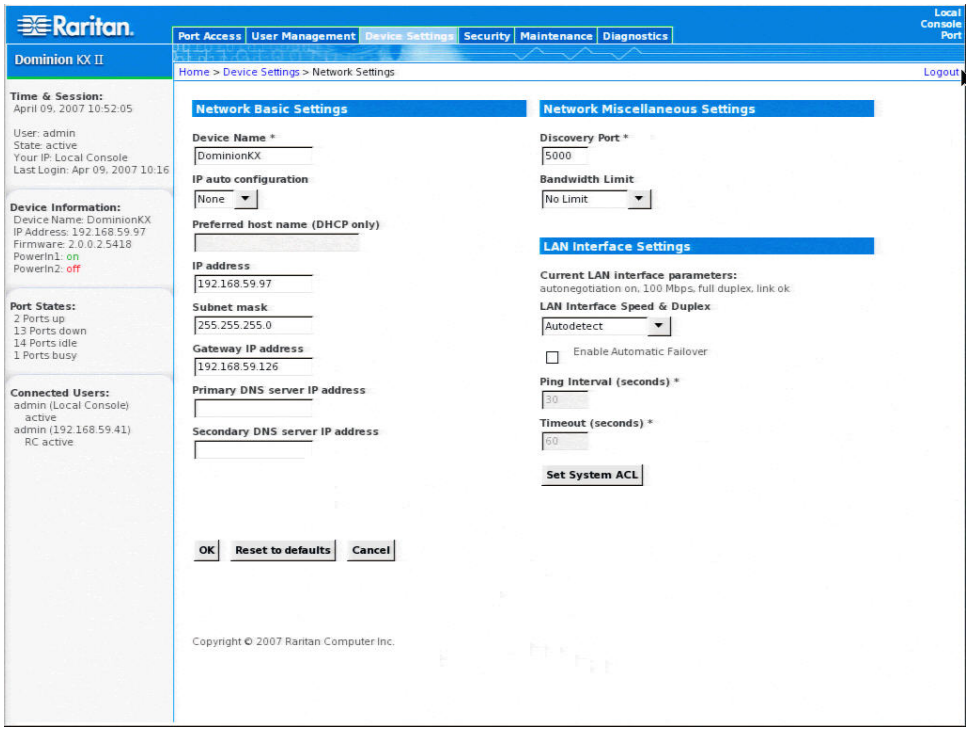

Abbildung 8: Netzwerkeinstellungen

2. Geben Sie im Feld **Device Name** (Gerätename) einen aussagekräftigen Namen für den Dominion KX II ein (bis zu 16 alphanumerische Zeichen und Sonderzeichen, keine Leerzeichen).
3. Wählen Sie in der Dropdownliste **IP auto configuration** (Automatische IP-Konfiguration) die IP-Konfiguration aus:
   - **None** (Keine [statisches IP]): Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben. Diese Option wird empfohlen, da der Dominion KX II ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.
   - **DHCP**: Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server zugewiesen.
4. Wenn Sie die IP-Konfiguration **None** (Keine) verwenden, geben Sie die TCP/IP-Parameter des Dominion KX II ein: **IP address** (IP-Adresse), **Subnet mask** (Subnetzmaske), **Gateway IP address** (Gateway-IP-Adresse), **Primary DNS server IP address** (IP-Adresse des primären Servers) und (optional) **Secondary DNS server IP address** (IP-Adresse des sekundären DNS-Servers).
5. Klicken Sie abschließend auf **OK**.

Die Dominion KX II-Einheit ist jetzt über das Netzwerk zugänglich.

Hinweis: *In manchen Umgebungen legt die Standardeinstellung* ***Autodetect*** *(auto-negotiation) (Automatische Erkennung [automatische Aushandlung]) für* ***LAN Interface Speed & Duplex*** *(LAN-Schnittstellengeschwindigkeit & Duplex) nicht die richtigen Netzwerkparameter fest, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld* ***LAN Interface Speed & Duplex*** *den Wert* ***100 Mbps/Full Duplex*** *(100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk), um dieses Problem zu beheben. Weitere Informationen finden Sie auf der Seite Network Settings (Netzwerkeinstellungen).*

Benennen der Zielserver

So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist (siehe Schritt 3: Anschließen der Geräte, Zielserverports).
2. Wählen Sie in der lokalen KX II-Konsole **Device Settings** > **Port Configuration** (Geräteeinstellungen > Portkonfiguration) aus. Die Seite **Port Configuration** (Portkonfiguration) wird angezeigt.

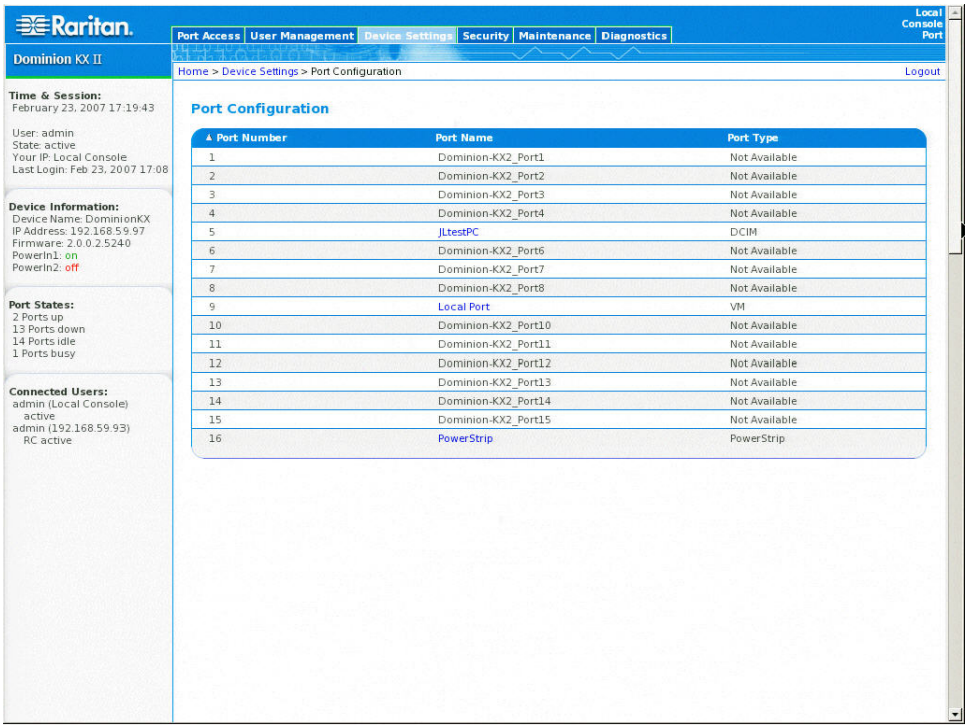

Abbildung 9: Port Configuration (Portkonfiguration)

3. Klicken Sie unter **Port Name** (Portname) auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite Port wird angezeigt.
4. Weisen Sie dem mit diesem Port verbundenen Server einen Namen zu. Der Name darf maximal 32 alphanumerische Zeichen und Sonderzeichen umfassen.
5. Klicken Sie auf **OK** (Senden).

Festlegen der automatischen Netzteilerkennung

Der Dominion KX II bietet zwei Netzteile und kann den Status dieser Netzteile automatisch erkennen und entsprechende Benachrichtigungen ausgeben. Mit der korrekten Konfiguration stellen Sie sicher, dass der Dominion KX II die entsprechenden Benachrichtigungen bei einem Ausfall der Stromversorgung sendet. Die Seite **Power Supply Setup** (Netzteilkonfiguration) ist so konfiguriert, dass beide Netzteile automatisch erkannt werden. Deaktivieren Sie auf dieser Seite die automatische Erkennung des nicht verwendeten Netzteils.

So deaktivieren Sie die automatische Erkennung für das nicht verwendete Netzteil:

1. Wählen Sie in der lokalen KX II-Konsole **Device Settings** > **Power Supply Setup** (Geräteeinstellungen > Netzteilkonfiguration) aus. Die Seite Power Supply Setup (Netzteilkonfiguration) wird angezeigt.
2. Deaktivieren Sie die automatische Erkennung für das *nicht* verwendete Netzteil.

Weitere Informationen finden Sie auf der Seite **Power Supply Setup** (Netzteilkonfiguration).

Hinweis für CC-SG-Benutzer

Wenn Sie den Dominion KX II in einer CC-SG-Konfiguration verwenden, führen Sie die oben beschriebenen Installationsschritte aus. Lesen Sie anschließend das *CommandCenter Secure Gateway-Benutzerhandbuch,* das *Administratorhandbuch* oder das *Bereitstellungshandbuch*, um korrekt fortzufahren. Diese finden Sie auf der Website von Raritan unter **Support**: http://www.raritan.com/support/productdocumentation.

Hinweis: *Der Rest dieses Benutzerhandbuchs gilt in erster Linie für die Bereitstellung von Dominion KX II-Einheiten ohne die Integrationsfunktion von CC-SG.*

Remoteauthentifizierung

Hinweis für CC-SG-Benutzer

Wenn der Dominion KX II durch das 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). Die Authentifizierung lokaler Benutzer hängt von der Konfiguration des Dominion KX II ab.

Weitere Informationen zur CC-SG-Authentifizierung finden Sie im *CommandCenter Secure Gateway-Benutzerhandbuch*, im *Administratorhandbuch* oder im *Bereitstellungshandbuch* unter: http://www.raritan.com/support/productdocumentation.

Unterstützte Protokolle

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

Hinweis zu Microsoft Active Directory

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

Authentifizierung im Vergleich zur Autorisierung

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

Wenn der Dominion KX II zur Remoteauthentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

Das Flussdiagramm veranschaulicht diesen Prozess:

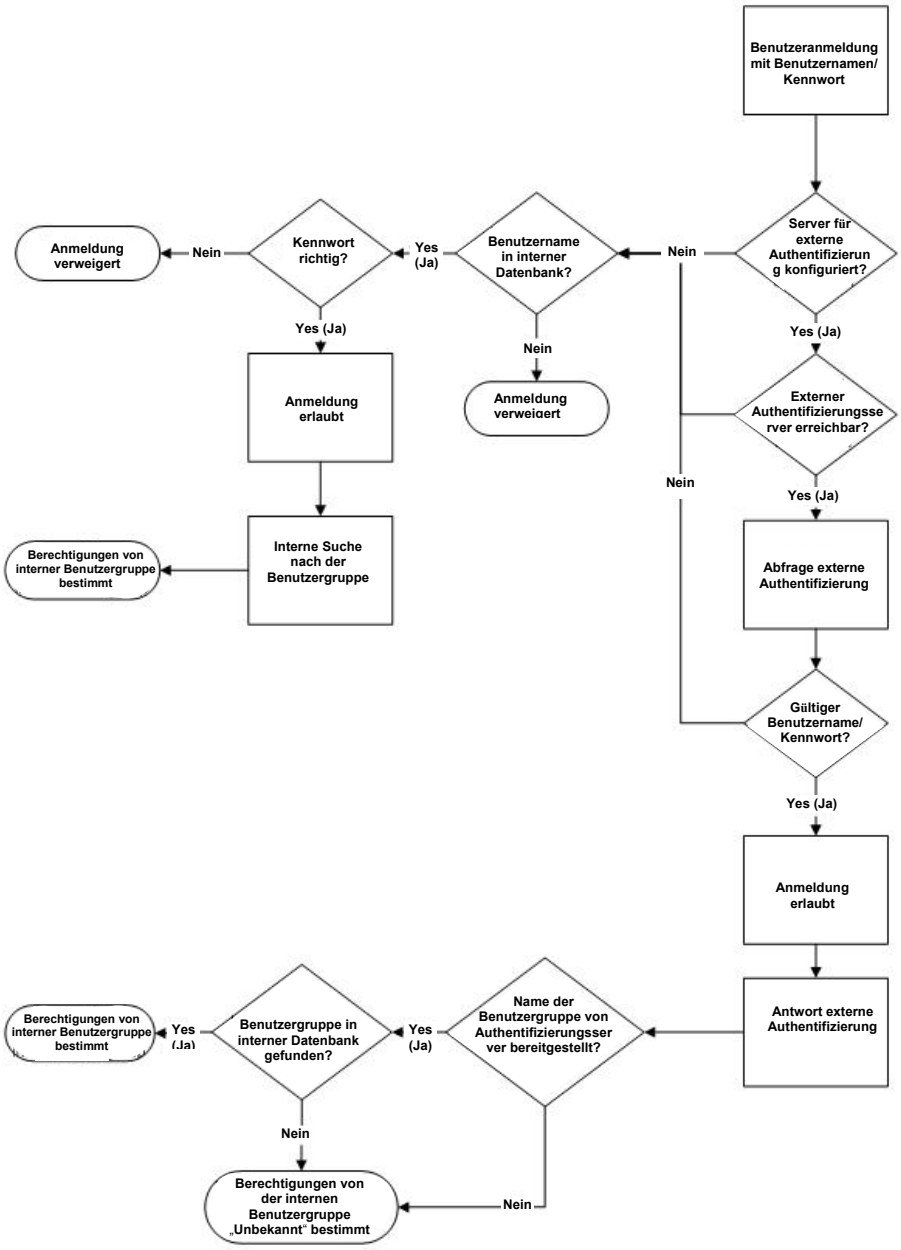

Abbildung 10: Flussdiagramm – Authentifizierung/Autorisierung

Beachten Sie die Bedeutung der Gruppe, der ein Benutzer angehört, und die Notwendigkeit der Konfiguration der Gruppe „Unknown" (Unbekannt). Wenn der externe Authentifizierungsserver einen nicht vom Dominion KX II erkannten Gruppennamen zurückgibt, werden die Berechtigungen dieses Benutzers von der permanenten Gruppe „Unknown" (Unbekannt) bestimmt.

Informationen zur Konfiguration Ihres Authentifizierungsservers, damit dieser bei seiner Antwort auf eine Authentifizierungsanfrage Benutzergruppeninformationen an den Dominion KX II zurückgibt, finden Sie unter Implementierung der LDAP-Remoteauthentifizierung und Implementierung der RADIUS-Remoteauthentifizierung.

Benutzer, Gruppen und Zugriffsberechtigungen

Überblick

Der Dominion KX II 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 Dominion KX II für LDAP oder RADIUS konfiguriert ist, wird zuerst diese Authentifizierung und anschließend die lokale Authentifizierung verarbeitet.

Benutzer

Für den Zugriff auf die Dominion KX II-Einheit sind ein Benutzername und ein Kennwort erforderlich. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf die KX II-Einheit zuzugreifen. Weitere Informationen zum Hinzufügen und Bearbeiten von Benutzern finden Sie unter Benutzerverwaltung.

Gruppen

Jede Dominion KX II-Einheit verfügt über drei Standardbenutzergruppen, die nicht gelöscht werden können:

Admin	Benutzer dieser Gruppe verfügen über vollständige Administratorrechte. Der ursprüngliche werkseitige Standardbenutzer ist Mitglied dieser Gruppe und verfügt über sämtliche Systemrechte.
Unknown	Dies ist die Standardgruppe für Benutzer, die mithilfe von LDAP oder RADIUS extern authentifiziert werden. Wenn der externe LDAP- oder RADIUS-Server keine gültige Benutzergruppe erkennt, wird die Gruppe „Unknown“ (Unbekannt) verwendet.
Individuell Group	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.

Zusätzlich zu den im System bereits vorhandenen Standardgruppen können Sie weitere Gruppen erstellen und entsprechende Berechtigungen für sie festlegen. Weitere Informationen zum Erstellen und Bearbeiten von Benutzergruppen finden Sie unter Benutzerverwaltung.

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 Ihres Dominion KX II 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*, spezifische 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, d.h. die Zugriffsberechtigungen für verschiedene Serverports, ob ein Neustart des Geräts zulässig ist und weitere Funktionen.

Kapitel 4: Herstellen einer Verbindung mit dem Dominion KX II

Benutzeroberflächen

Der Dominion KX II bietet Ihnen verschiedene Benutzeroberflächen, über die Sie jederzeit und überall einfach auf die Einheit zugreifen können. Dazu zählen die lokale KX II-Konsole, die KX II-Remotekonsole und der Multi-Platform-Client (MPC). In der folgenden Tabelle werden diese Oberflächen und ihre Nutzung für den Zielserverzugriff und die lokale sowie die Remoteverwaltung erläutert:

Benutzeroberfläche	Lokal		Remote	
	Zugriff	Admin	Zugriff	Admin
Lokale KX II-Konsole	✓	✓		
KX II-Remotekonsole			✓	✓
Virtual KVM Client			✓	
Multi-Platform-Client (MPC)			✓	✓

Lokale KX II-Konsole – KX II-Geräte

Am Serverschrank erfüllt der Dominion KX II über die lokale KX II-Konsole standardmäßige KVM-Switching- und Verwaltungsfunktionen. Die lokale KX II-Konsole stellt eine direkte KVM-Verbindung (analog) mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch.

Die grafischen Benutzeroberflächen der lokalen KX II-Konsole und der KX II-Remotekonsole ähneln sich in vielen Bereichen. Auf die Unterschiede wird in diesem Benutzerhandbuch hingewiesen. Die Benutzeroberflächen der lokalen KX II-Konsole und der KX II-Remotekonsole sind fast identisch. Die folgenden Optionen stehen nur in der lokalen KX II-Konsole, aber *nicht* in der KX II-Remotekonsole zur Verfügung:

- Lokale Porteinstellungen
- Werksrückstellung

KX II-Remotekonsole – KX II-Geräte

Die Dominion KX II-Remotekonsole bietet eine browserbasierte grafische Benutzeroberfläche, über die Sie auf mit dem Dominion KX II verbundene Zielserver zugreifen und die KX II-Einheit remote verwalten können.

Die KX II-Remotekonsole bietet eine digitale Verbindung mit den angeschlossenen Zielservern. Wenn Sie über die KX II-Remotekonsole auf einen Zielserver zugreifen, wird ein Fenster für den Virtual KVM Client geöffnet. Für jeden Zielserver wird ein Virtual KVM Client aufgerufen, was den gleichzeitigen Zugriff ermöglicht, wenn dieser von der jeweiligen KX II-Einheit unterstützt wird (KX2-116 unterstützt beispielsweise nur eine Remotesitzung).

Die grafischen Benutzeroberflächen der lokalen KX II-Konsole und der KX II-Remotekonsole ähneln sich in vielen Bereichen. Auf die Unterschiede wird in diesem Benutzerhandbuch hingewiesen. Die folgenden Optionen stehen nur in der KX II-Remotekonsole, aber *nicht* in der lokalen KX II-Konsole zur Verfügung:

- Virtuelle Medien
- Favoriten
- **Backup/Restore** (Sicherung/Wiederherstellung)
- Firmwareaktualisierung
- **Upgrade Report** (Aktualisierungsbericht)
- **KX Diagnostics** (KX-Diagnose)

Multi-Platform-Client (MPC) – KX I- und KX II-Geräte

Der Multi-Platform-Client (MPC) von Raritan bietet eine grafische Benutzeroberfläche für den Remotezugriff auf Zielgeräte, die mit Dominion-Einheiten verbunden sind. Der MPC kann für die eigenständige Verwendung oder den Zugriff über einen Browser installiert werden.

Laden Sie nach dem Installieren des Dominion KX II entweder eine eigenständige Version des Raritan MPC herunter, und richten Sie eine erste Netzwerkverbindung ein, oder starten Sie die Anwendung direkt.

Hinweis: *Der MPC unterstützt sowohl KX I- als auch KX II-Geräte. Verwenden Sie den MPC, wenn Sie über eine Benutzeroberfläche auf Server zugreifen möchten, die mit KX I- und KX II-Geräten verbunden sind.*

So starten Sie den MPC direkt:

1. Geben Sie zum Starten des MPC von einem Client, auf dem ein beliebiger Browser ausgeführt wird, **http://IP-ADDESS/mpc** in die Adresszeile ein, wobei **IP-ADDESS** die IP-Adresse des Raritan-Geräts ist. Der MPC wird in einem neuen Fenster gestartet, in dem Menüleiste, Symbolleiste, Bildlaufleiste und Adresszeile **nicht vorhanden** sind. Arbeiten Sie in diesem Fenster, und wechseln Sie durch Drücken von **ALT+TAB** zu anderen geöffneten Fenstern.
2. Beim Start des MPC wird auf der linken Seite des Bildschirms eine Gerätestruktur aller automatisch erkannten Raritan-Geräte im Subnetz angezeigt. Falls die Dominion KX II-Einheit nicht anhand des Namens aufgelistet ist, erstellen Sie durch Auswahl von **Connection > New Profile** (Verbindung > Neues Profil) ein Symbol manuell. Das Fenster **Add Connection** (Verbindung hinzufügen) wird geöffnet.
3. Geben Sie eine Gerätebeschreibung ein sowie einen Verbindungstyp an, fügen Sie die IP-Adresse der Dominion-Einheit hinzu, und klicken Sie auf **OK**. Diese Angaben können Sie später bearbeiten.
4. Doppelklicken Sie im Navigatorfenster auf der linken Seite des Bildschirms auf das Symbol für Ihre Dominion KX II-Einheit.

Umfassende Informationen zum Installieren und Betreiben des MPC finden Sie im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)*. Das Handbuch steht auf der Website von Raritan unter http://www.raritan.com/support/productdocumentation oder auf der in der Dominion-Lieferung enthaltenen CD-ROM von Raritan mit Benutzerhandbüchern und Kurzanleitungen zur Verfügung.

Raritan Remote Client (RRC) – Nur KX I-Geräte

Der Raritan Remote Client (RRC) bietet eine grafische Benutzeroberfläche für den Remotezugriff auf Zielgeräte.

Hinweis: *Der RRC kann **nicht** mit Dominion KX II verwendet werden. Nutzen Sie stattdessen den MPC.*

Unterstützte Sprachen

Der Dominion KX II bietet Tastaturunterstützung für folgende Sprachen: amerikanisches Englisch, britisches Englisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Japanisch, Koreanisch, Französisch und Deutsch.

Hinweise zu unterstützten Sprachen

- Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen KX II-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.
- Aufgrund einer Einschränkung der Java® Runtime Environment (JRE) erhalten Fedora-, Linux- und Solaris-Clients eine ungültige Antwort, wenn auf Tastaturen mit dem Tastaturlayout **UK English** (britisches Englisch) die Taste **Alt Gr** gedrückt wird. Bei Verwendung von Java 1.4.2 oder 1.5 erfassen Fedora, Linux und Solaris keine Ereignisse für die Tastenkombination **Alt Gr**. Mit Java 1.6 hat sich dieses Verhalten verbessert, allerdings werden *keyPressed*-Ereignisse und *keyReleased*-Ereignisse für **Alt Gr** nach wie vor als „unknown key codes“ (unbekannte Tastencodes) identifiziert.

  Wenn eine Taste zusammen mit **Alt Gr** gedrückt wird – z. B. **Alt Gr-4**, also das Euro-Symbol auf Tastaturen mit dem Tastaturlayout **UK English** (britisches Englisch) –, wird nur ein *keyTyped*-Ereignis und ein *keyReleased*-Ereignis für den Wert generiert, aber kein *keyPressed*-Ereignis. In Java 1.6 hingegen wird auch das *keyPressed*-Ereignis generiert.

Java Runtime Environment (JRE)

Wichtig: Sie sollten die Zwischenspeicherung für Java deaktivieren und den Java-Zwischenspeicher leeren. Weitere Informationen finden Sie in der Java-Dokumentation oder im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)*.

Die Dominion KX II-Remotekonsole und der MPC benötigen eine funktionierende JRE. Die Dominion KX II-Remotekonsole überprüft die Java-Version. Falls die Version falsch oder veraltet ist, werden Sie aufgefordert, eine kompatible Version herunterzuladen.

Raritan empfiehlt zur Gewährleistung einer optimalen Leistung die Verwendung von Java® Runtime Environment (JRE) Version 1.5, aber die Dominion KX II-Remotekonsole und MPC funktionieren auch mit JRE Version **1.4.2_05** oder höher (mit Ausnahme von JRE 1.5.0_02). JRE 1.6 wird ebenfalls unterstützt, aber diese Version wurde noch nicht vollständig getestet.

Hinweis: *Damit mehrsprachige Tastaturen in der KX II-Remotekonsole (Virtual KVM Client) funktionieren, müssen Sie die mehrsprachige Version der Java Runtime Environment (JRE) installieren.*

Starten des KX II

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

Hinweis: *Abhängig von den Browser- und Sicherheitseinstellungen werden möglicherweise verschiedene Sicherheits- und Zertifikatwarnungen angezeigt. Sie müssen diese Warnungen bestätigen, um die KX II-Remotekonsole zu starten.*

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

- ☐ *In the future, do not show this warning (Diese Warnung nicht mehr anzeigen)*
- ☐ *Always trust content from this publisher (Inhalt von diesem Herausgeber immer vertrauen)*

So starten Sie die KX II-Remotekonsole:

1. Melden Sie sich bei einer Workstation an, die eine Netzwerkverbindung zum Dominion KX II herstellen kann und auf der Java Runtime Environment v1.4.2_2 oder höher installiert ist (JRE ist verfügbar unter http://java.sun.com/).
2. Starten Sie einen unterstützten Browser, z. B. Internet Explorer (IE) oder Firefox.
3. Geben Sie den folgenden URL ein: **http://*IP-ADRESSE***, wobei **IP-ADRESSE** die der Dominion KX II-Einheit zugewiesene IP-Adresse ist. Sie können auch **https** verwenden, den vom Administrator zugewiesenen DNS-Namen des Dominion KX II (sofern ein DNS-Server konfiguriert wurde) oder einfach die IP-Adresse in den Browser eingeben (KX II leitet die IP-Adresse stets von HTTP zu HTTPS um). Die Anmeldeseite wird angezeigt.

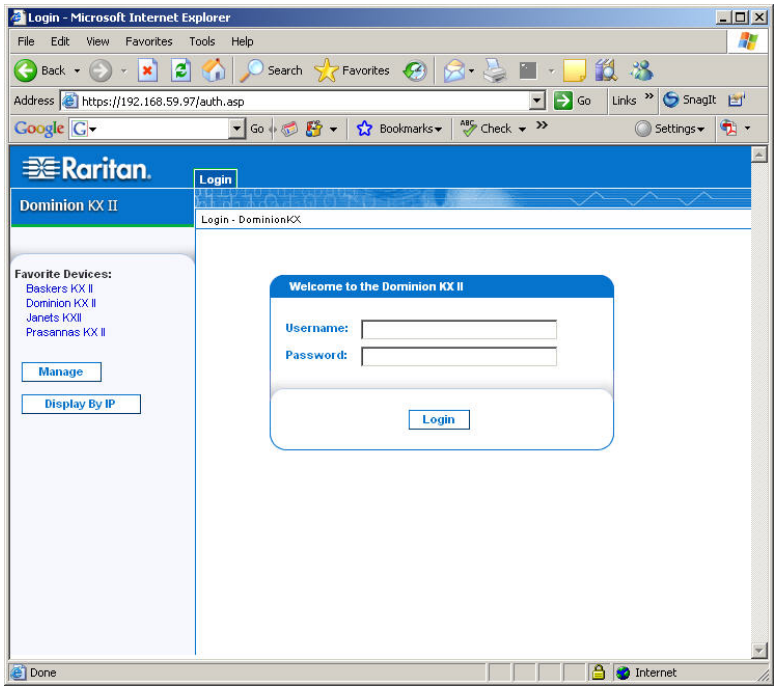

Abbildung 11: Anmeldeseite für die Dominion KX II-Remotekonsole

4. Geben Sie unter **Username** und **Password** Ihren Benutzernamen und das Kennwort ein. Verwenden Sie bei der ersten Anmeldung die werkseitigen Standardeinstellungen (Benutzername **admin**, Kennwort **raritan**) in Kleinbuchstaben. Sie werden aufgefordert, das Standardkennwort zu ändern. Weitere Informationen finden Sie unter Ändern des Standardkennworts.
5. Klicken Sie auf **Login** (Anmelden).

Layout der KX II-Konsolen

Die KX II-Remotekonsole und die lokale KX II-Konsole bieten für die Konfiguration und Verwaltung eine HTML-Oberfläche (vergleichbar mit einem Browser) sowie eine Liste und Auswahl der Zielserver. Die Optionen befinden sich auf verschiedenen Registerkarten.

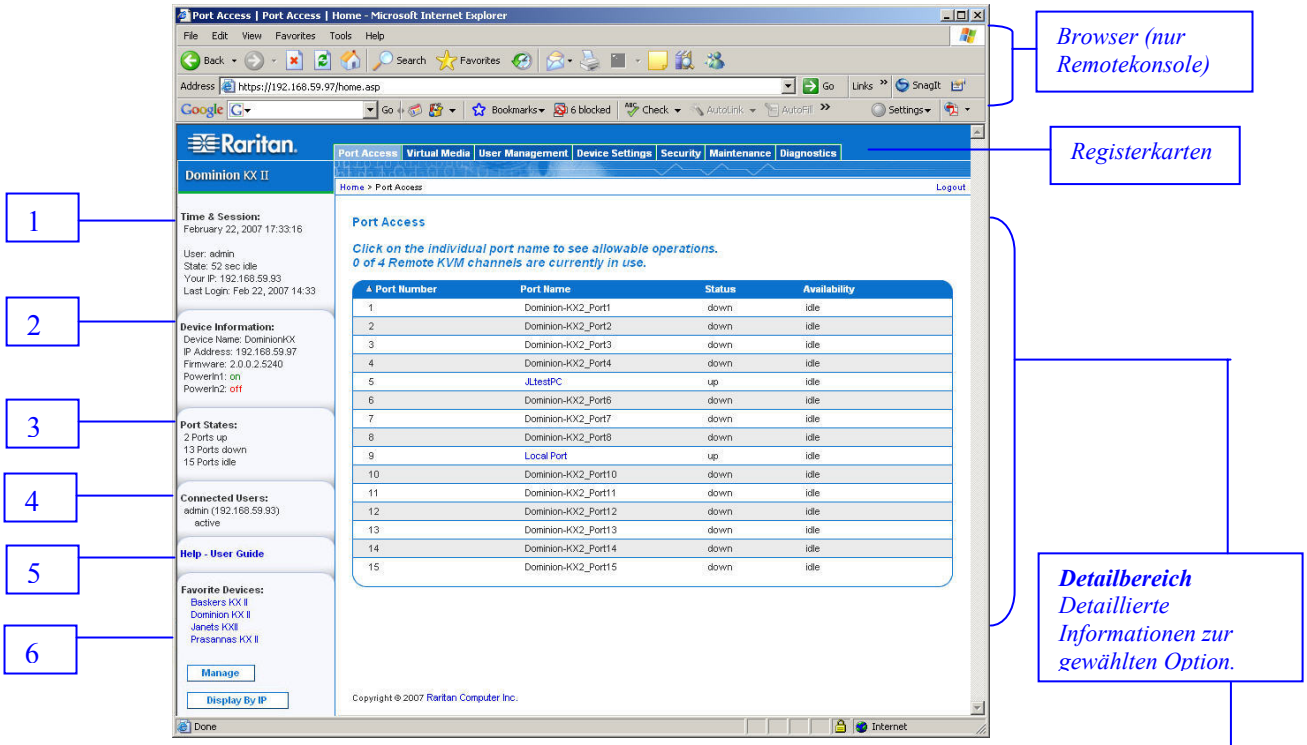

Abbildung 12: Hauptseite der KX II-Remotekonsole

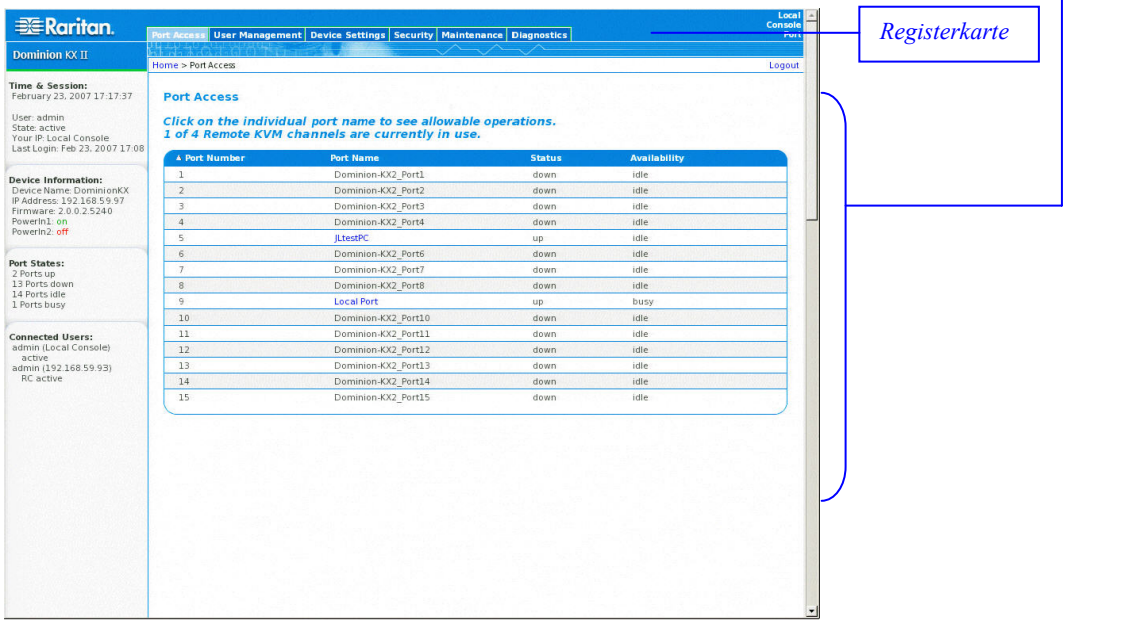

Abbildung 13: Hauptseite der lokalen KX II-Konsole

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. 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.

Die Zahlen in der folgenden Tabelle entsprechen den Zahlen in Abbildung 12.

#	NAME	BESCHREIBUNG
1	Zeit & Sitzung	Datum, Uhrzeit, Benutzername, aktueller Status, IP-Adresse des Clients und letzte Anmeldung
2	Geräteinformationen	Gerätename, IP-Adresse, Firmwareversion und Status der beiden Netzkabel
3	Portstatus	Aktueller Status aller Dominion KX II-Ports
4	Verbundene Benutzer	Liste aller Benutzer, die derzeit mit dem Dominion KX II verbunden sind
5	Hilfe – Benutzerhandbuch	Zugriff auf dieses Benutzerhandbuch (nur KX II-Remotekonsole)
6	Bevorzugte Geräte	Zugriff auf und Verwaltung der Favoritenliste (nur KX II-Remotekonsole)

Navigation in den KX II-Konsolen

In den beiden Dominion KX II-Konsolenoberflächen haben Sie viele Möglichkeiten für die Navigation und Auswahl.

Für die Auswahl von Optionen stehen folgende Möglichkeiten zur Verfügung:

- Klicken Sie auf eine Registerkarte, um eine Seite der verfügbaren Optionen anzuzeigen.
- 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 so genannten „Breadcrumbs“) direkt auf die gewünschte Option.

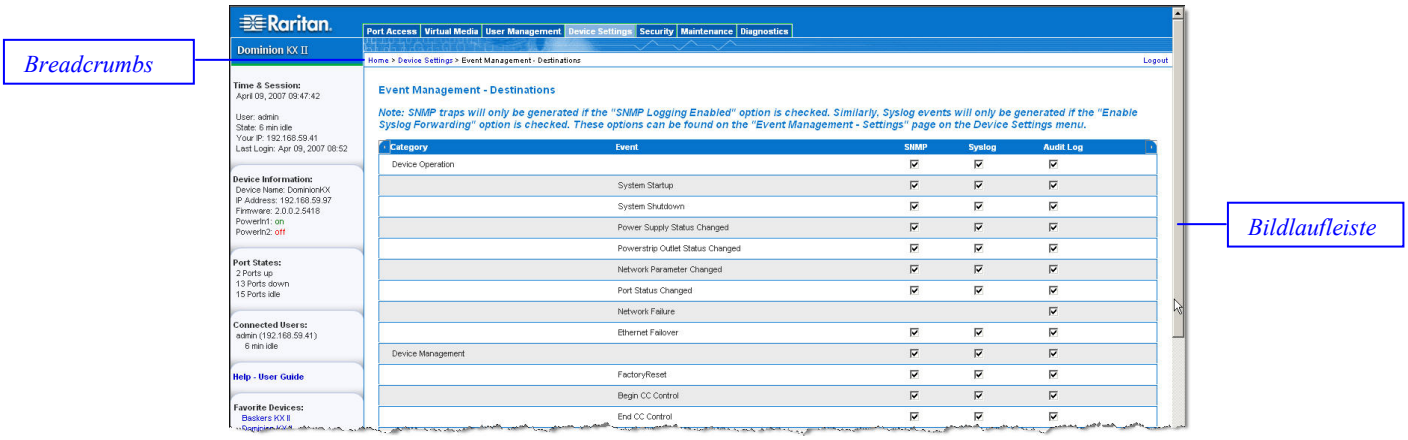

Abbildung 14: Beispiel für Menühierarchie (Breadcrumbs)

So blättern Sie durch Seiten:

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

Weitere Informationen zur Navigation und Auswahl im Raritan Multi-Platform-Client (MPC) finden Sie im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)*.

Abmelden

So beenden Sie die Dominion KX II-Konsolen:

Klicken Sie oben rechts auf der Seite auf **Logout** (Abmelden).

Hinweis: *Durch das Abmelden werden auch alle geöffneten Sitzungen des Virtual KVM Client geschlossen.*

Menüstruktur der KX II-Konsolen

Das folgende Diagramm enthält *alle* Menüoptionen, die in den Oberflächen der KX II-Remotekonsole sowie der lokalen KX II-Konsole zur Verfügung stehen. Auf Abweichungen zwischen den beiden Konsolen wird hingewiesen.

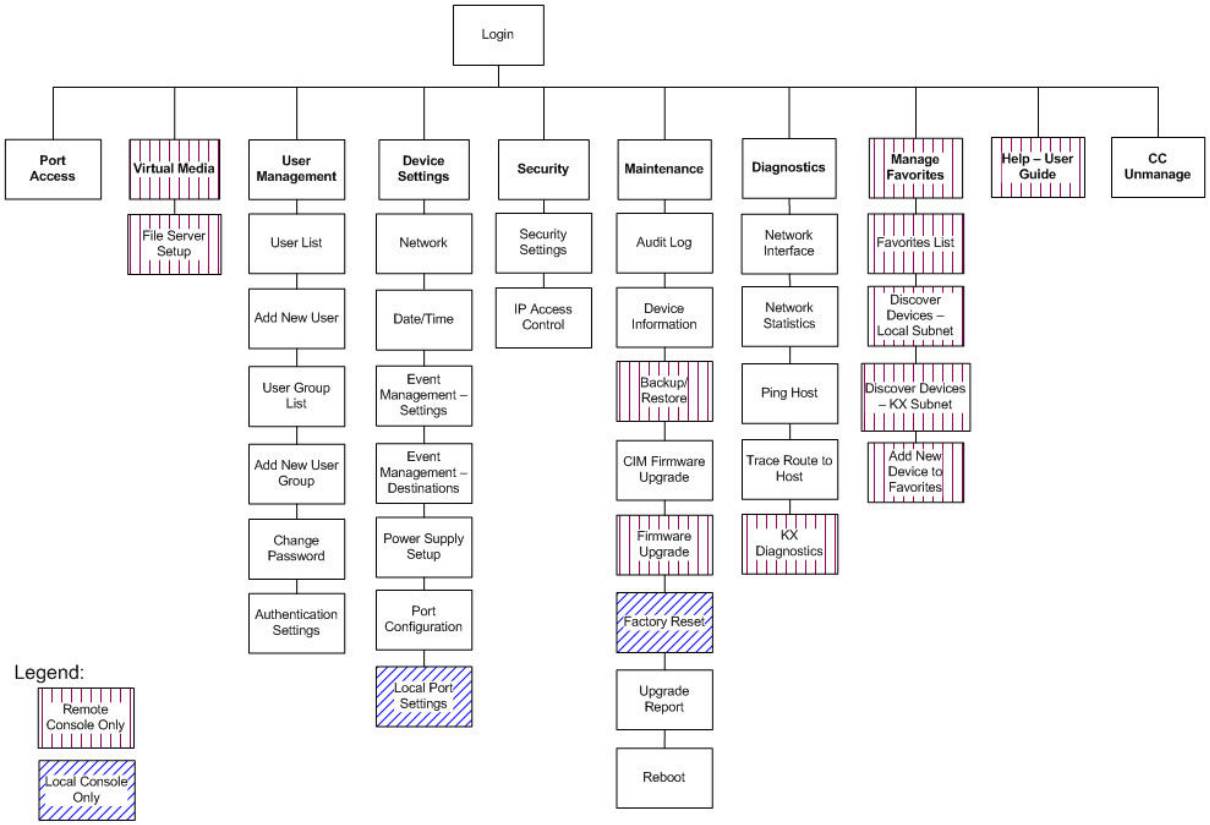

Abbildung 15: Menüstruktur der KX II-Konsolen (lokal und Remote)

Darüber hinaus sind Abweichungen bei den Menüoptionen zwischen der lokalen KX II-Konsole und der KX II-Remotekonsole in der folgenden Tabelle aufgeführt:

OPTION	LOKALE KONSOLE	REMOTEKONSOLE
Virtuelle Medien		✓
File Server Setup (Dateiserver-Setup)		✓
Backup/Restore (Sicherung/Wiederherstellung)		✓
Firmwareaktualisierung		✓
KX Diagnostics (KX-Diagnose)		✓
Manage Favorites (Favoriten verwalten)		✓
Favorites List (Favoritenliste)		✓
Discover Devices – Local Subnet (Geräte erkennen – Lokales Subnetz)		✓
Discover Devices – KX Subnet (Geräte erkennen – KX-Subnetz)		✓
Add New Device to Favorites (Neues Gerät zu Favoriten hinzufügen)		✓
Hilfe – Benutzerhandbuch		✓
Lokale Porteinstellungen	✓	
Werksrückstellung	✓	

Verwalten von Favoriten

Mithilfe des Features **Favorites** (Favoriten) können Sie die häufig verwendeten Geräte organisieren und schnell darauf zugreifen. Der Bereich **Favorite Devices** (Bevorzugte Geräte) befindet sich links unten (Randleiste) auf der Seite **Port Access** (Portzugriff). Hier haben Sie folgende Möglichkeiten:

- Erstellen und Verwalten einer Liste bevorzugter Geräte
- Schnelles Zugreifen auf häufig verwendete Geräte
- Aufführen der Favoriten nach Name oder IP-Adresse
- Erkennen von Dominion KX II-Geräten im Subnetz (vor und nach der Anmeldung)
- Abrufen erkannter Dominion KX II-Geräte vom verbundenen KX-Gerät (nach der Anmeldung)

Hinweis: *Dieses Feature steht nur auf der Dominion KX II-Remotekonsole (nicht auf der lokalen Dominion KX II-Konsole) zur Verfügung.*

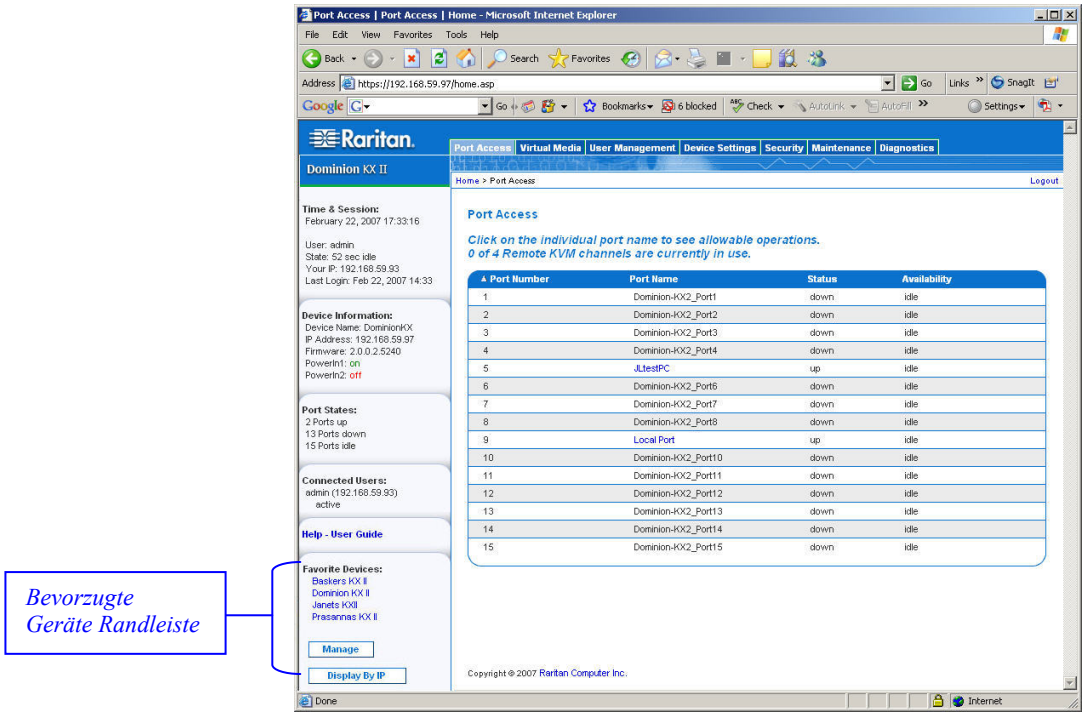

Abbildung 16: Bevorzugte Geräte (Randleiste)

So greifen Sie auf ein bevorzugtes KX II-Gerät zu:

Klicken Sie auf den unterhalb von **Favorite Devices** (Bevorzugte Geräte) aufgeführten Namen des gewünschten Geräts. Ein neues Browserfenster wird geöffnet.

So wechseln Sie zwischen der Namens- und der IP-Adressenansicht der Liste **Favorite Devices** (Bevorzugte Geräte):

Anzeigen der Favoriten nach IP-Adresse:	Anzeigen der Favoriten nach Name:
Klicken Sie auf die Schaltfläche **Display by IP** (Nach IP-Adresse anzeigen).	Klicken Sie auf die Schaltfläche **Display by Name** (Nach Name anzeigen).

Bevorzugte Geräte, angezeigt nach Name

*Klicken Sie zum Wechseln auf **Display by IP**.*

Bevorzugte Geräte, angezeigt nach IP-Adresse

*Klicken Sie zum Wechseln auf **Display by Name**.*

Menü Manage Favorites (Favoriten verwalten)

Das Menü **Manage Favorites** (Favoriten verwalten) bietet folgende Optionen: **Favorites List** (Favoritenliste), **Discover Devices – Local Subnet** (Geräte erkennen – Lokales Subnetz), **Discover Devices – KX Subnet** (Geräte erkennen – KX-Subnetz) und **Add New Device to Favorites** (Neues Gerät zu Favoriten hinzufügen).

So öffnen Sie das Menü **Manage Favorites** (Favoriten verwalten):

Klicken Sie auf die Schaltfläche **Manage** (Verwalten). Die Seite **Manage Favorites** (Favoriten verwalten) wird angezeigt.

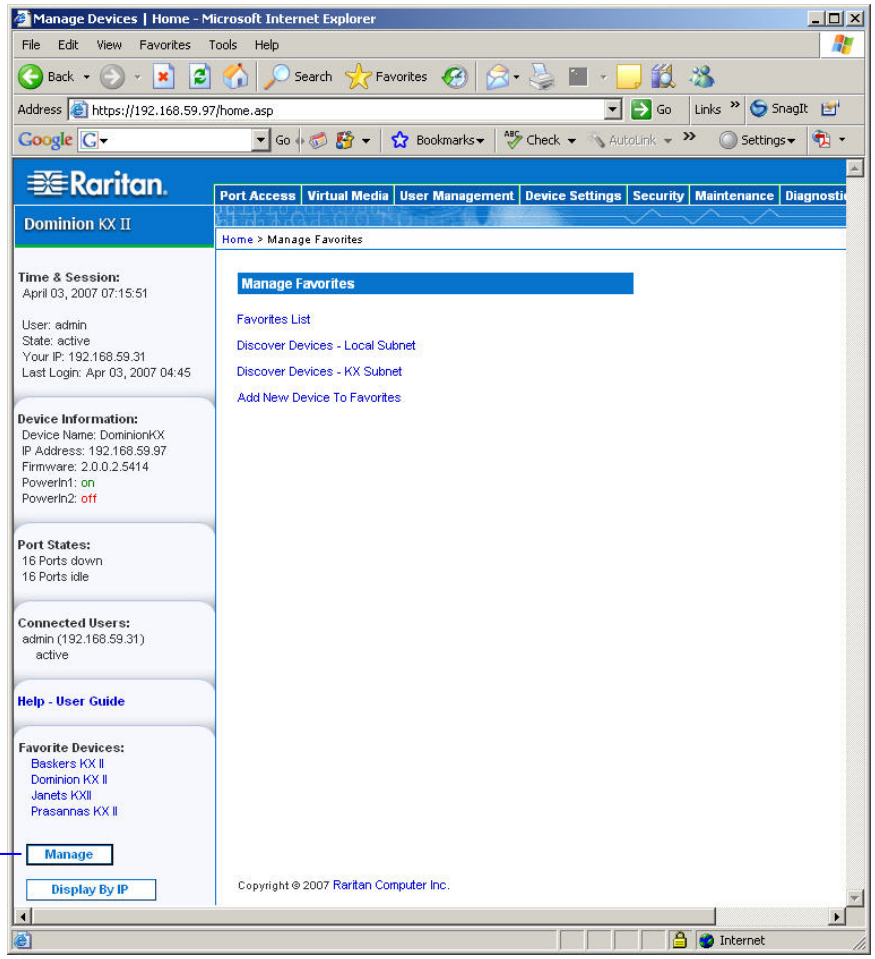

Abbildung 17: Menü Manage Favorites (Favoriten verwalten)

OPTION:	AN:
Favorites List (Favoritenliste)	Verwalten einer Liste bevorzugter Geräte
Discover Devices – Local Subnet (Geräte erkennen – Lokales Subnetz)	Erkennen der Geräte im lokalen Subnetz
Discover Devices – KX Subnet (Geräte erkennen – KX-Subnetz)	Erkennen der Geräte im Subnetz des KX-Geräts
Add New Device to Favorites (Neues Gerät zu Favoriten hinzufügen)	Hinzufügen, Bearbeiten und Löschen von Geräten in der Favoritenliste

Favorites List (Favoritenliste)

Auf der Seite **Favorites List** (Favoritenliste) können Sie der Favoritenliste Geräte hinzufügen und in der Favoritenliste aufgeführte Geräte bearbeiten oder löschen.

So öffnen Sie die Seite **Favorites List** (Favoritenliste):

Wählen Sie **Manage > Favorites List** (Verwalten > Favoritenliste). Die Seite **Favorites List** (Favoritenliste) wird angezeigt.

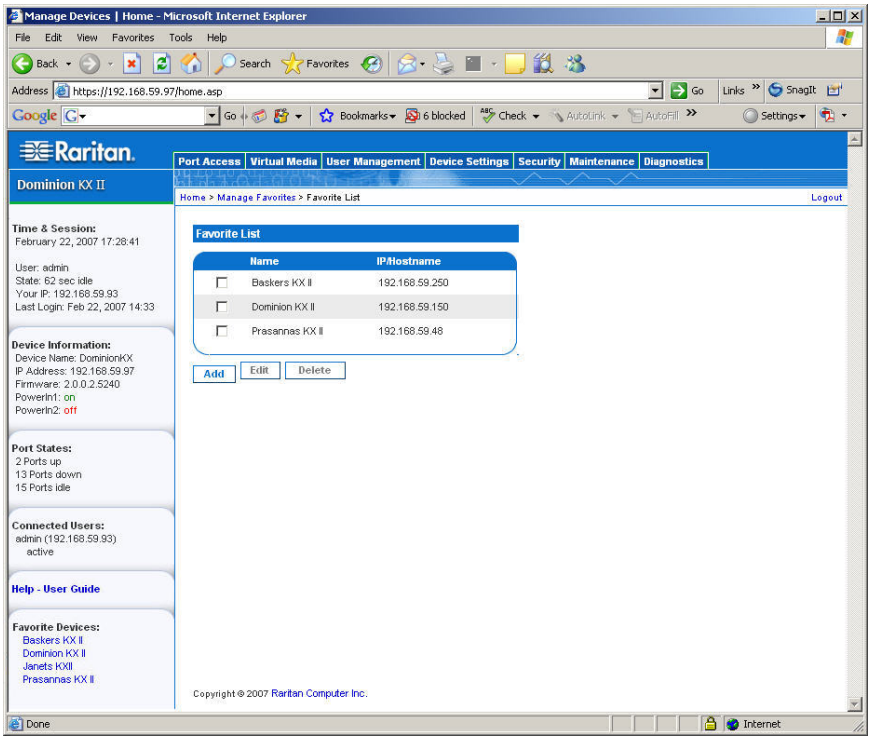

*Abbildung 18: **Favorites List** (Favoritenliste)*

So fügen Sie einen Favoriten hinzu:

Klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Die Seite Add New Favorite (Neuen Favoriten hinzufügen) wird angezeigt.

So löschen Sie einen Favoriten:

Wichtig: Gehen Sie beim Entfernen von Favoriten bedachtsam vor. Sie werden nicht aufgefordert, den Löschvorgang zu bestätigen.

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Dominion KX II-Gerät.
2. Klicken Sie auf die Schaltfläche **Delete** (Löschen). Der Favorit wird aus der Favoritenliste entfernt.

So bearbeiten Sie einen Favoriten:

1. Aktivieren Sie auf der Seite **Favorites List** (Favoritenliste) das Kontrollkästchen neben dem gewünschten Dominion KX II-Gerät.
2. Klicken Sie auf die Schaltfläche **Edit** (Bearbeiten). Die Seite **Edit** (Bearbeiten) wird angezeigt.

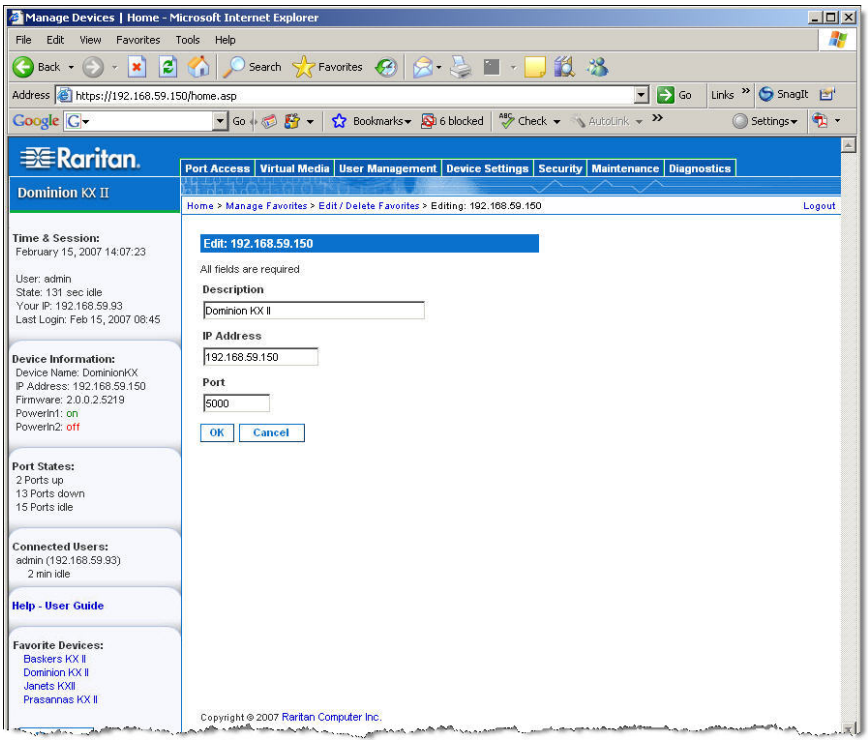

Abbildung 19: Bearbeiten (Favoriteninformationen)

3. Aktualisieren Sie die Felder nach Bedarf:
   - **Description** (Beschreibung): Geben Sie aussagekräftige Informationen ein.
   - **IP Address** (IP-Adresse): Geben Sie die IP-Adresse der Dominion KX II-Einheit ein.
   - **Port**: Ändern Sie ggf. den Erkennungsport.
4. Klicken Sie auf **OK** (Senden).

Discover Devices – Local Subnet (Geräte erkennen – Lokales Subnetz)

Mit dieser Option finden Sie die Geräte im lokalen Subnetz (d. h. dem Subnetz, in dem die Dominion KX II-Remotekonsole ausgeführt wird). Sie können direkt von dieser Seite auf die Geräte zugreifen oder sie Ihrer Favoritenliste hinzufügen.

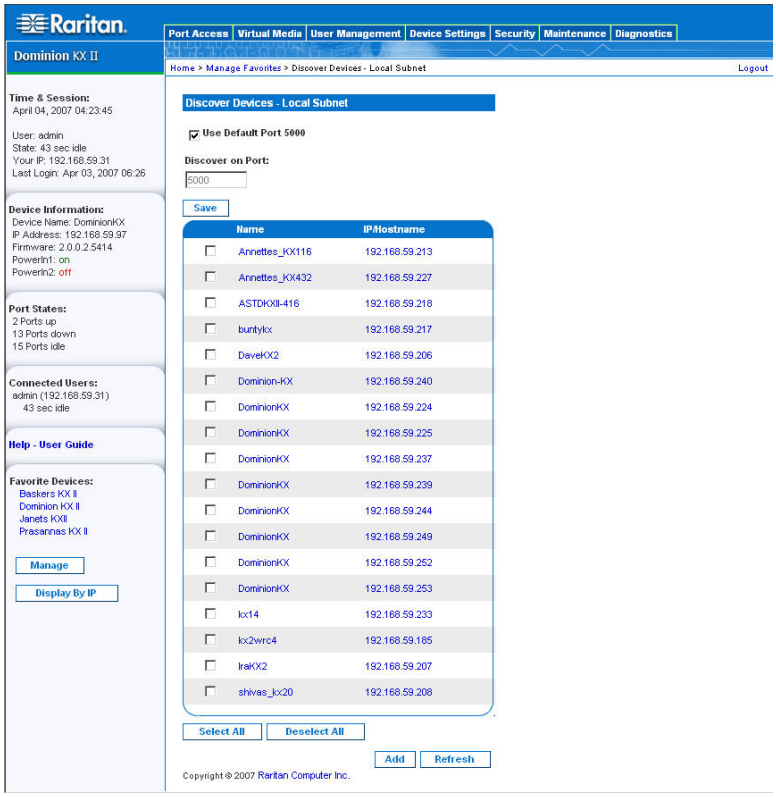

Abbildung 20: Discover Devices - Local Subnet (Geräte erkennen – Lokales Subnetz)

So finden Sie Geräte im lokalen Subnetz:

1. Wählen Sie **Favorites > Discover Devices – Local Subnet** (Favoriten > Geräte erkennen – Lokales Subnetz). Die Seite **Discover Devices – Local Subnet** (Geräte erkennen – Lokales Subnetz) wird angezeigt.
2. Wählen Sie den entsprechenden Erkennungsport aus (Informationen zum Erkennungsport finden Sie unter Verschiedene Netzwerkeinstellungen):
   - Wenn Sie den Standarderkennungsport verwenden möchten, aktivieren Sie das Kontrollkästchen **Use Default Port 5000** (Standardport 5000 verwenden).
   - Wenn Sie einen anderen Erkennungsport verwenden möchten, gehen Sie wie folgt vor:
     a. Deaktivieren Sie das Kontrollkästchen **Use Default Port 5000** (Standardport 5000 verwenden).
     b. Geben Sie die Portnummer im Feld **Discover on Port** (Erkennungsport) ein.
     c. Klicken Sie auf **Save** (Speichern).
3. Klicken Sie auf **Refresh** (Aktualisieren). Die Liste der Geräte im lokalen Subnetz wird aktualisiert.

So fügen Sie der Favoritenliste Geräte hinzu:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Gerätenamen/der IP-Adresse.
2. Klicken Sie auf **Add** (Senden).

*Tipp: Verwenden Sie die Schaltflächen **Select All** (Alle auswählen) und **Deselect All** (Alle entfernen), um schnell alle Geräte im Subnetz der Remotekonsole auszuwählen bzw. diese Auswahl aufzuheben.*

So greifen Sie auf ein erkanntes Gerät zu:

Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

Discover Devices – KX Subnet (Geräte erkennen – KX-Subnetz)

Mit dieser Option finden Sie die Geräte im Subnetz des Dominion KX II-Geräts (d. h. dem Subnetz der KX-Gerät-IP-Adresse selbst). Sie können direkt von dieser Seite auf die Geräte zugreifen oder sie Ihrer Favoritenliste hinzufügen.

Mit diesem Feature arbeiten mehrere Dominion KX II-Einheiten zusammen und werden automatisch skaliert. Die Dominion KX II-Remotekonsole erkennt die Dominion KX II-Einheiten im Subnetz des Dominion KX II automatisch.

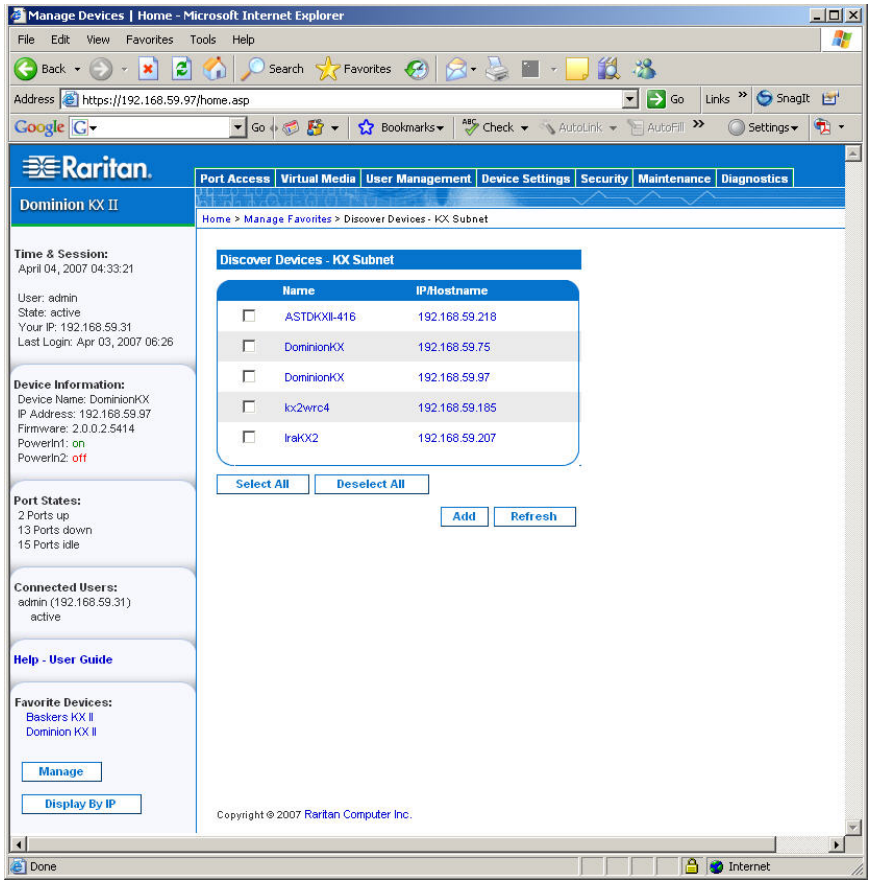

*Abbildung 21: **Discover Devices – KX Subnet** (Geräte erkennen – KX-Subnetz)*

So finden Sie Geräte im Subnetz des KX-Geräts:

1. Wählen Sie **Favorites > Discover Devices – KX Subnet** (Favoriten > Geräte erkennen – KX-Subnetz). Die Seite **Discover Devices – KX Subnet** (Geräte erkennen – KX-Subnetz) wird angezeigt.
2. Klicken Sie auf **Refresh** (Aktualisieren). Die Liste der Geräte im lokalen Subnetz wird aktualisiert.

So fügen Sie der Favoritenliste Geräte hinzu:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Gerätenamen/der IP-Adresse.
2. Klicken Sie auf **Add** (Senden).

*Tipp: Verwenden Sie die Schaltflächen **Select All** (Alle auswählen) und **Deselect All** (Alle entfernen), um schnell alle Geräte im Subnetz des Dominion KX II-Geräts auszuwählen bzw. diese Auswahl aufzuheben.*

So greifen Sie auf ein erkanntes Gerät zu:

Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

Add New Favorite (Neuen Favoriten hinzufügen)

So fügen Sie der Favoritenliste ein Gerät hinzu:

1. Wählen Sie **Manage Favorites > Add New Device to Favorites** (Favoriten verwalten > Neues Gerät zu Favoriten hinzufügen). Die Seite **Add New Favorite** (Neuen Favoriten hinzufügen) wird angezeigt.

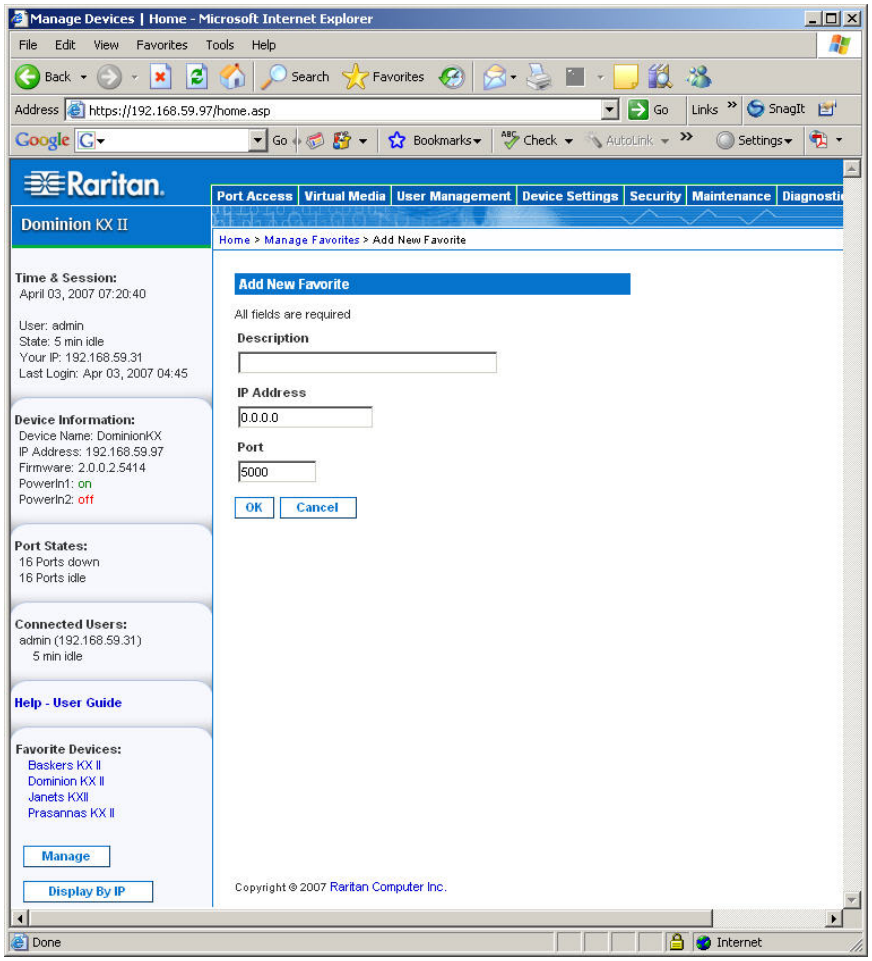

Abbildung 22: Add New Favorite (Neuen Favoriten hinzufügen)

2. Geben Sie im Feld **Description** eine aussagekräftige Beschreibung ein.
3. Geben Sie die IP-Adresse des Geräts ein.
4. Ändern Sie ggf. den Erkennungsport.
5. Klicken Sie auf **OK** (Senden). Das Gerät wird Ihrer Favoritenliste hinzugefügt.

Kapitel 5: Zugreifen auf Zielserver

Seite Port Access (Portzugriff)

Nachdem Sie sich erfolgreich bei der Dominion KX II-Remotekonsole angemeldet haben, wird die Seite **Port Access** (Portzugriff) angezeigt. Diese Seite enthält alle Dominion KX II-Ports, die angeschlossenen Zielserver sowie ihren Status und ihre Verfügbarkeit. Über die Seite **Port Access** (Portzugriff) haben Sie Zugriff auf die mit dem Dominion KX II verbundenen Zielserver. Zielserver sind die Server, die Sie über die Dominion KX II-Einheit steuern möchten. Sie sind an die Dominion KX II-Ports an der Rückseite der Einheit angeschlossen.

Hinweis: *Für jede Verbindung mit einem Zielserver wird ein* ***neues*** *Fenster für den Virtual KVM Client geöffnet.*

So verwenden Sie die Seite **Port Access** (Portzugriff):

1. Klicken Sie in der KX II-Remotekonsole auf die Registerkarte **Port Access** (Portzugriff). Die Seite **Port Access** (Portzugriff) wird angezeigt.

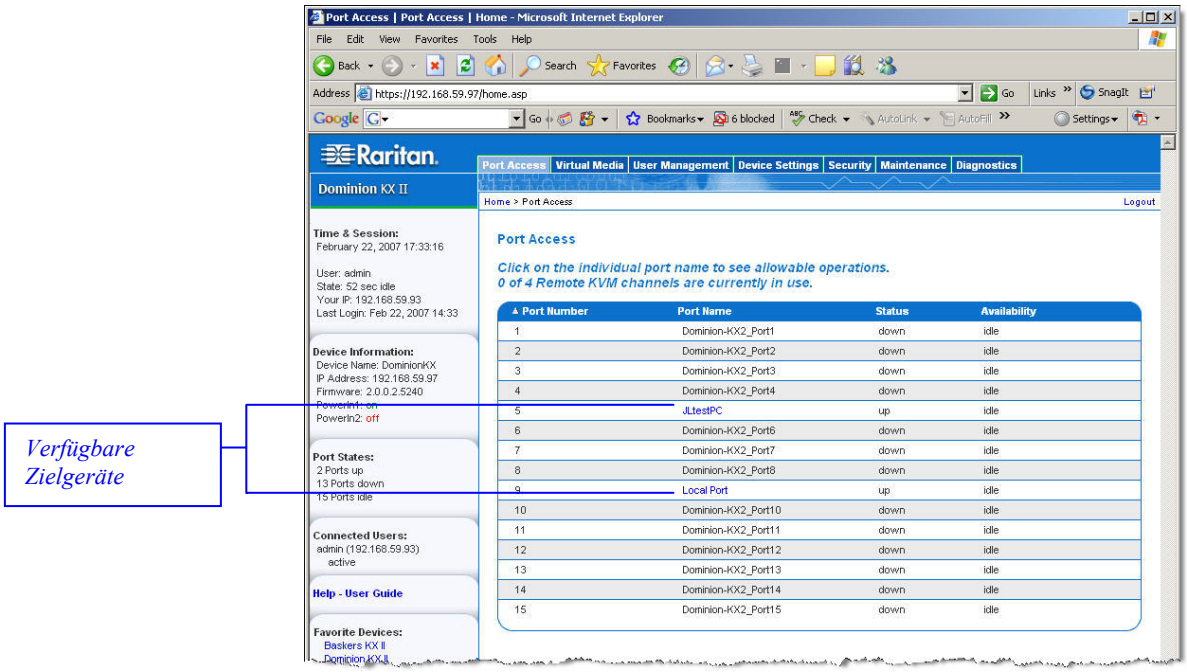

Abbildung 23: Port Access (Portzugriff)

Die Zielserver sind zunächst nach Portnummer sortiert. Sie können die Anzeige nach einer der Spalten sortieren.

- **Port Number** (Portnummer): Die für die Dominion KX II-Einheit verfügbaren Ports werden beginnend mit 1 durchnummeriert. Mit Powerstrips verbundene Ports werden hier *nicht* aufgeführt, was zu Lücken in der Portnummernabfolge führt.
- **Port Name** (Portname): Der Name des Dominion KX II-Ports. Die Standardeinstellung **Dominion-KX2-Port#** können Sie jederzeit in einen aussagekräftigeren Namen ändern. Wenn Sie auf einen Portnamenlink klicken, wird das Menü **Port Action** (Portaktion) geöffnet.
- **Status**: Der Status lautet entweder *Up* (Ein) oder *Down* (Aus).
- **Availability** (Verfügbarkeit): Für die Verfügbarkeit stehen die Werte *Idle* (Inaktiv), *Connected* (Verbunden), *Busy* (Verwendet) und *Unavailable* (Nicht verfügbar) zur Verfügung.

2. Klicken Sie auf den Portnamen des Zielservers, auf den Sie zugreifen möchten. Das Menü **Port Action** (Portaktion) wird angezeigt. Weitere Informationen zu den verfügbaren Menüoptionen finden Sie unter Menü **Port Action** (Portaktion).
3. Wählen Sie im Menü **Port Action** (Portaktion) die gewünschte Menüoption aus.

So ändern Sie die Sortierreihenfolge der Anzeige:

Klicken Sie auf die Spaltenüberschrift, nach der sortiert werden soll. Die Liste der Zielserver wird nach dieser Spalte sortiert.

Menü Port Action (Portaktion)

1. Wenn Sie in der Liste **Port Access** (Portzugriff) auf einen Portnamen klicken, wird das Menü **Port Action** (Portaktion) angezeigt. Dieses Menü enthält nur die Optionen, die für den gewählten Port verfügbar sind. Dazu zählen:
   - **Connect** (Verbinden): Erstellt eine neue Verbindung mit dem Zielserver. Für die KX II-Remotekonsole wird ein neues Fenster des Virtual KVM Client geöffnet. Für die lokale KX II-Konsole wechselt die Anzeige weg von der lokalen Benutzeroberfläche hin zum Zielserver. Auf dem lokalen Port muss die Oberfläche der lokalen KX II-Konsole angezeigt werden, um den Wechsel durchführen zu können.

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

   - **Switch From** (Wechseln von): Wechselt von einer bestehenden Verbindung zum gewählten Port (Zielserver). Diese Menüoption ist für jede offene Verbindung verfügbar (für maximal vier bei Einheiten mit vier Remotebenutzern, für maximal zwei bei Einheiten mit zwei Remotebenutzern und maximal eine bei Einheiten mit einem Remotebenutzer). Sie wird nur angezeigt, wenn eines oder mehrere Fenster des Virtual KVM Client geöffnet sind.

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

   - **Disconnect** (Trennen): Trennt diese Portverbindung und schließt das Fenster 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 II-Konsole nicht zur Verfügung. Verwenden Sie darin zum Trennen des gewechselten Zielservers die Zugriffstaste.*

   - **Power On** (Strom ein): Versorgt den Zielserver über die zugeordnete Steckdose mit Strom. Diese Option wird nur angezeigt, wenn es eine oder mehrere Stromzuordnungen für dieses Zielgerät gibt, wenn dieses ausgeschaltet ist (Portstatus *Down* [Aus]) und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.
   - **Power Off** (Strom aus): Unterbricht die Stromversorgung des Zielservers über die zugeordneten Steckdosen. Diese Option wird nur angezeigt, wenn es eine oder mehrere Stromzuordnungen für dieses Zielgerät gibt, wenn dieses eingeschaltet ist (Portstatus *Up* [Ein]) und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.
   - **Power Cycle** (Ein- und Ausschalten): Schaltet den Zielserver über die zugeordneten Steckdosen ein und aus. Diese Option wird nur angezeigt, wenn es eine oder mehrere Stromzuordnungen für dieses Zielgerät gibt und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.
2. Wählen Sie die gewünschte Menüoption für den Port aus.

Verbinden eines Zielservers

So stellen Sie eine Verbindung mit einem Zielserver her:

1. Klicken Sie in der KX II-Remotekonsole auf die Registerkarte **Port Access** (Portzugriff). Die Seite Port Access (Portzugriff) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü Port Action (Portaktion) wird angezeigt.

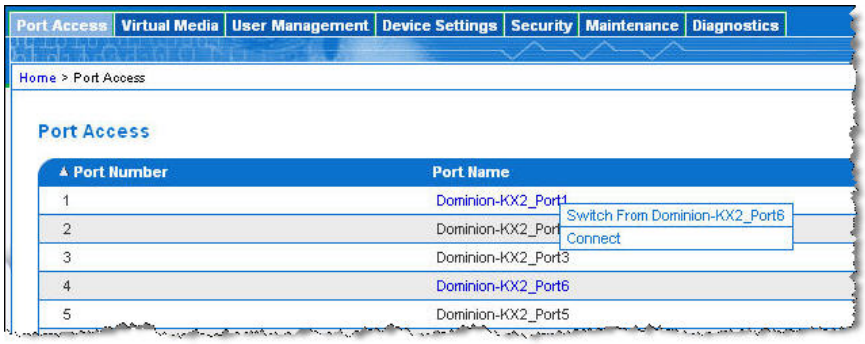

*Abbildung 24: Menü **Port Action** (Portaktion)*

3. Wählen Sie **Connect** (Verbinden). Ein Fenster des Virtual KVM Client wird für den mit dem betreffenden Port verbundenen Zielserver geöffnet.

Wechseln zwischen Zielservern

Über den Dominion KX II können Sie auf mehrere Zielserver zugreifen. Dominion KX II ermöglicht das Wechseln zwischen verschiedenen Zielservern.

***Hinweis:** Dieses Feature ist nur in der Dominion KX II-Remotekonsole verfügbar.*

So wechseln Sie zwischen Zielservern:

1. Rufen Sie die Dominion KX II-Seite **Port Access** (Portzugriff) auf, während bereits auf einen Zielserver zugegriffen wird.
2. Klicken Sie unter **Port Name** (Portname) auf den Portnamen des Zielgeräts, auf das Sie jetzt zugreifen möchten. Das Menü **Port Action** (Portaktion) wird angezeigt.
3. Wählen Sie die Option **Switch From** (Wechseln von). Das Fenster des Virtual KVM Client wechselt zu dem von Ihnen gewählten Zielserver.

Trennen von Zielservern

***Hinweis:** Diese Option steht auf der lokalen KX II-Konsole nicht zur Verfügung. Verwenden Sie darin zum Trennen des gewechselten Zielservers die Zugriffstaste.*

So trennen Sie einen Zielserver:

1. Klicken Sie unter **Port Name** auf den Portnamen des Zielgeräts, das Sie trennen möchten. Das Menü **Port Action** (Portaktion) wird angezeigt.
2. Wählen Sie die Option **Disconnect** (Trennen). Das Fenster des Virtual KVM Client schließt das Fenster des Zielgeräts.

*Tipp: Sie können das Fenster des Virtual KVM Client auch schließen, indem Sie im Menü **Virtual KVM** (Virtueller KVM-Client) die Option **Connection > Exit** (Verbindung > Beenden) wählen.*

Stromzufuhrsteuerung eines Zielservers

Hinweis: *Diese Features stehen nur zur Verfügung, wenn Sie Stromzuordnungen vorgenommen haben. Weitere Informationen finden Sie unter Stromzufuhrsteuerung.*

Ein- und Ausschalten eines Zielservers

So schalten Sie einen Zielserver ein und aus:

1. Klicken Sie in der KX II-Remotekonsole auf die Registerkarte **Port Access** (Portzugriff). Die Seite Port Access (Portzugriff) wird angezeigt.
2. Klicken Sie unter **Port Name** (Portname) auf den entsprechenden Zielserver. Das Menü **Port Action** (Portaktion) wird angezeigt.

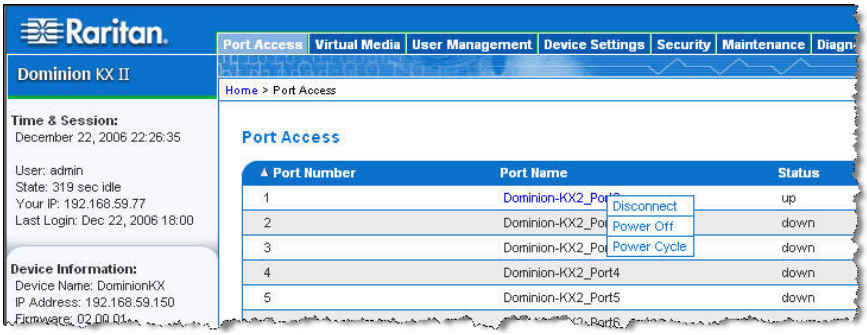

*Abbildung 25: Menü **Port Action** (Portaktion) (Stromoptionen)*

3. Wählen Sie **Power Cycle** (Ein- und Ausschalten). Zur Bestätigung der gewählten Aktion wird eine Meldung angezeigt.

Einschalten eines Zielservers

So schalten Sie einen Zielserver ein:

1. Klicken Sie in der KX II-Remotekonsole auf die Registerkarte **Port Access** (Portzugriff). Die Seite Port Access (Portzugriff) wird angezeigt.
2. Klicken Sie unter **Port Name** (Portname) auf den entsprechenden Zielserver. Das Menü **Port Action** (Portaktion) wird angezeigt.
3. Wählen Sie **Power On** (Strom ein).

Ausschalten eines Zielservers

So schalten Sie einen Zielserver aus:

1. Klicken Sie in der KX II-Remotekonsole auf die Registerkarte **Port Access** (Portzugriff). Die Seite Port Access (Portzugriff) wird angezeigt.
2. Klicken Sie unter **Port Name** (Portname) auf den entsprechenden Zielserver. Das Menü **Port Action** (Portaktion) wird angezeigt.
3. Wählen Sie **Power Off** (Strom aus).

Kapitel 6: Virtual KVM Client

Wenn Sie über die KX II-Remotekonsole auf einen Zielserver zugreifen, wird ein Fenster für den Virtual KVM Client geöffnet. Für *jeden* Zielserver, mit dem eine Verbindung besteht, gibt es einen Virtual KVM Client. Auf diese Fenster greifen Sie über die Windows-Taskleiste zu.

Die Fenster des Virtual KVM Client können minimiert, maximiert und auf dem Desktop verschoben werden.

Hinweis: *Beachten Sie, dass beim Aktualisieren des HTML-Browsers die Verbindung des Virtual KVM Client beendet wird.*

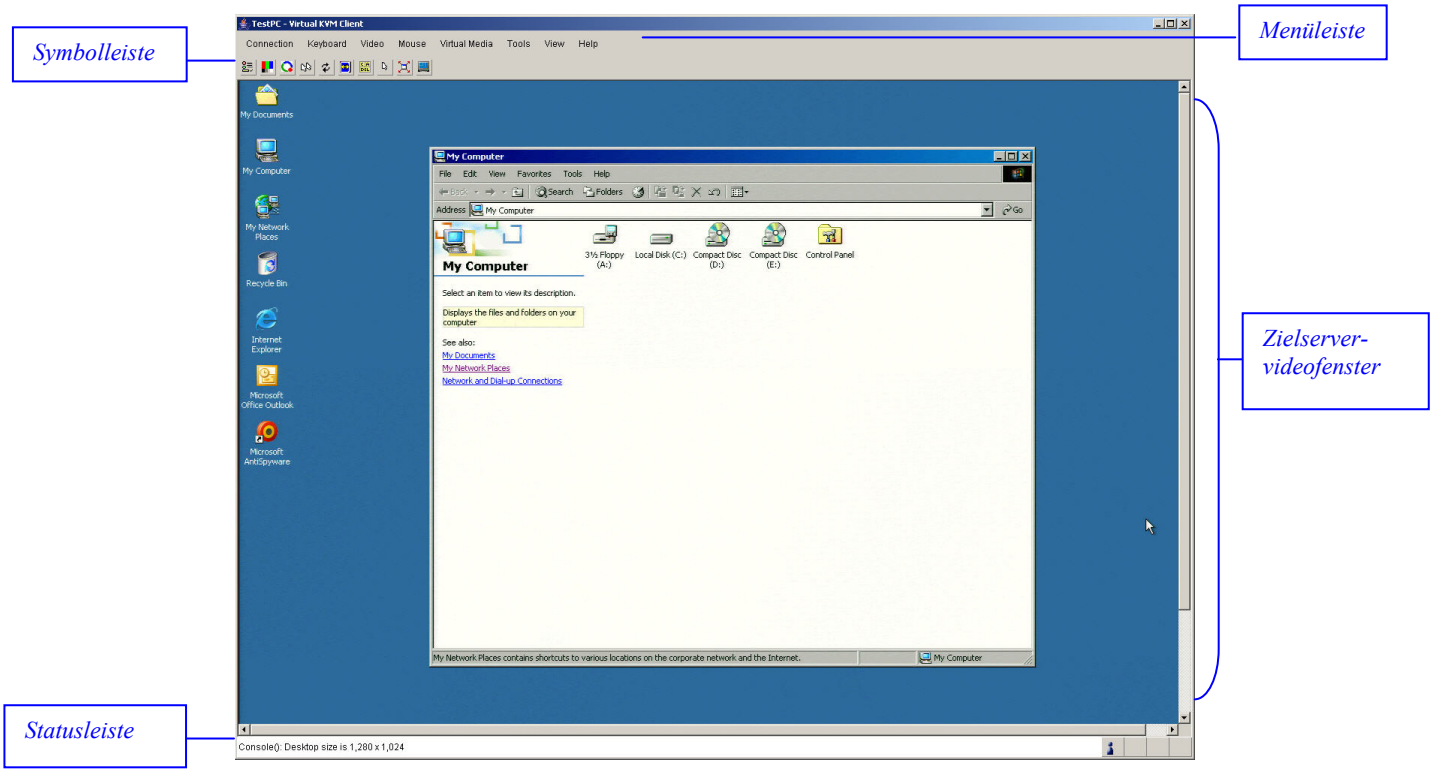

*Abbildung 26: Fenster **Virtual KVM Client** (Virtueller KVM-Client)*

Auf die Features des Virtual KVM Client greifen Sie über das Menü und die Symbolleiste zu.

FEATURE	BESCHREIBUNG
Menüleiste	Dropdownmenüs mit Befehlen und Einstellungen
Symbolleiste	Schaltflächen zum Ausführen häufig verwendeter Features und Befehle
Zielservervideofenster	Anzeige des Zielgeräts
Statusleiste	Echtzeitinformationen zu Verbindungsparametern, der Fenstergröße des Zielservers, gleichzeitigen Verbindungen, Feststellanzeige und Num-Feststellanzeige

Optionen

Menüstruktur

Das folgende Diagramm zeigt alle im Virtual KVM Client verfügbaren Menüoptionen.

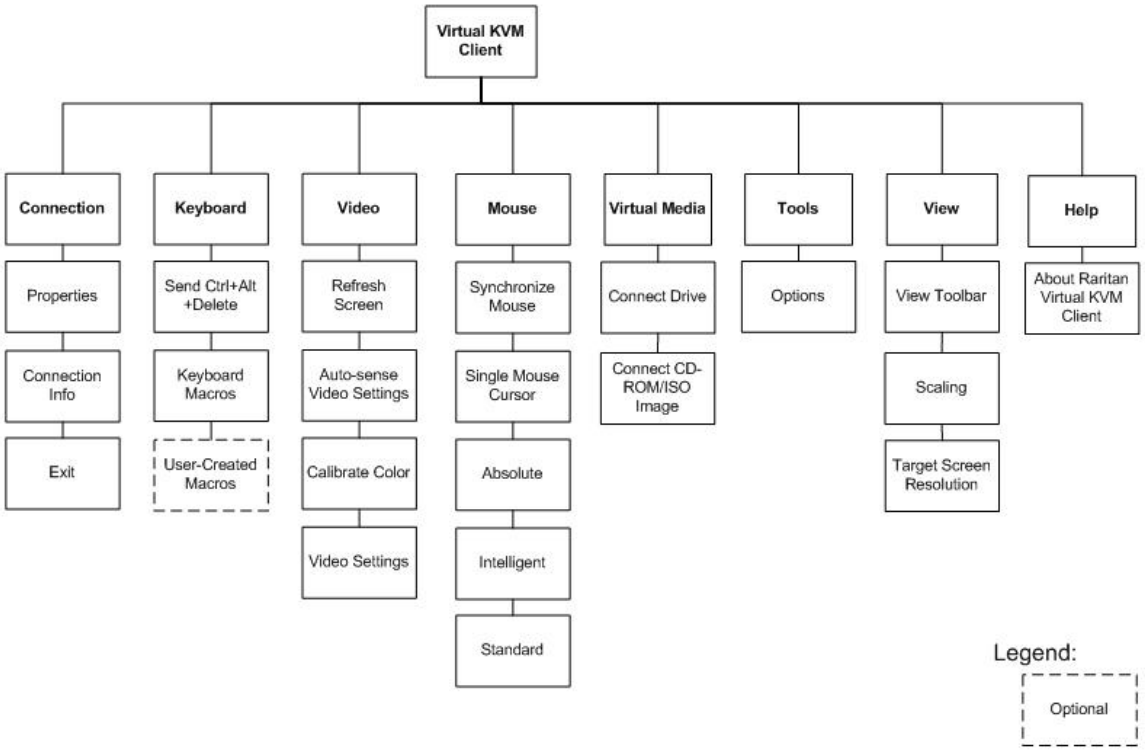

Abbildung 27: Menüstruktur des Virtual KVM Client

Symbolleiste

SCHALT-FLÄCHE	BESCHREIBUNG
	Eigenschaften
	Videoeinstellungen
	Farbkalibrierung
	Synchronisieren der Cursors von Client und Zielserver
	Aktualisieren der Anzeige
	Automatisches Erkennen des Videos
	Senden von **Strg+Alt+Entf**
	Wechsel zwischen Ein-Cursor- und Zwei-Cursor-Modus
	Vollbild
	Anpassen des Videobildes an die Bildschirmgröße

Mauszeigersynchronisation

Bei der Remoteanzeige eines Zielservers mit einer Maus sehen Sie zwei Mauszeiger: Ein Mauszeiger gehört zur Remoteclientworkstation und der andere zum Zielserver. 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 Clientmauszeigers etwas schneller als die des Zielgerätmauszeigers.

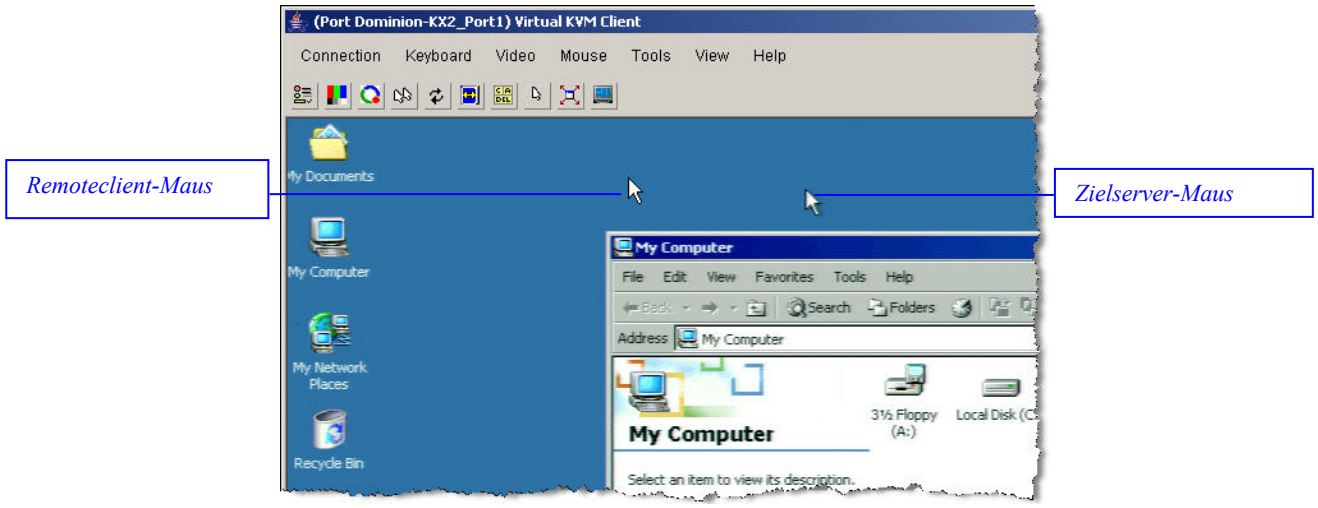

Abbildung 28: Zwei Mauszeiger

Bei schnellen LAN-Verbindungen sollten Sie den Mauszeiger des Virtual KVM Client deaktivieren, um nur den Cursor des Zielservers anzuzeigen. Sie können zwischen den beiden Modi (ein Cursor und zwei Cursor) wechseln. Weitere Informationen zu den verfügbaren Mausmodi finden Sie unter Menü **Mouse** (Maus).

Menü Connection (Verbindung)

Dialogfeld Properties (Eigenschaften)

Die dynamischen Videokomprimierungsalgorithmen von Dominion KX II gewährleisten die Verwendbarkeit der KVM-Konsole unter variierenden Bandbreitenbeschränkungen. Dominion KX II-Einheiten optimieren die KVM-Ausgabe nicht nur für LANs, sondern auch für WAN- und DFÜ-Verbindungen. Diese Einheiten können zudem die Farbtiefe steuern und die Videoausgabe beschränken, um für jede Bandbreite ein optimales Gleichgewicht zwischen Videoqualität und Systemreaktion bereitzustellen.

	Verbindungseigenschaften	Manuelles Anpassen der Bandbreitenoptionen (Verbindungsgeschwindigkeit, Farbtiefe usw.)

Sie können die Parameter im Dialogfeld **Properties** (Eigenschaften) Ihren Anforderungen für unterschiedliche Betriebsumgebungen anpassen.

So legen Sie die Verbindungseigenschaften fest:

1. Wählen Sie **Connection > Properties** (Verbindung > Eigenschaften). Das Dialogfeld **Properties** (Eigenschaften) wird angezeigt.

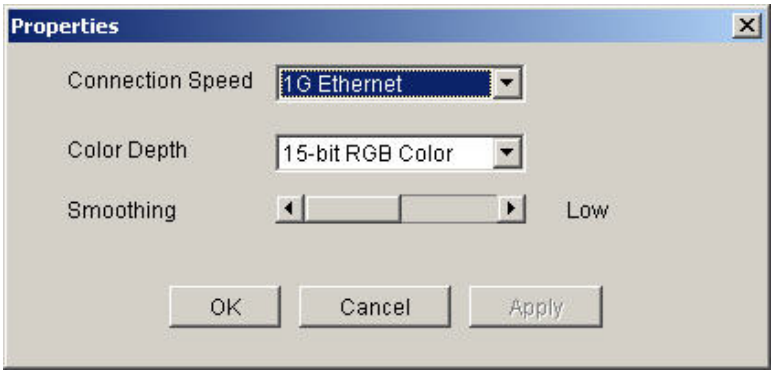

Abbildung 29: Dialogfeld Properties (Eigenschaften)

2. Wählen Sie in der Dropdownliste **Connection Speed** (Verbindungsgeschwindigkeit) die gewünschte Verbindungsgeschwindigkeit aus. Dominion KX II kann die verfügbare Bandbreite automatisch erkennen und die Bandbreitenverwendung nicht beschränken. Sie können die Verwendung jedoch auch an die Bandbreitenbeschränkungen anpassen.

Automatisch
1G Ethernet
100 MB Ethernet
10 MB Ethernet
1,5 MB (MAX DSL/T1)
1 MB (Schnelles DSL/T1)
512 KB (Mittleres DSL/T1)
384 KB (Langsames DSL/T1)
256 KB (Kabel)
128 KB (Dual-ISDN)
56 KB (ISP-Modem)
33 KB (Schnelles Modem)
24 KB (Langsames Modem)

Diese Einstellungen sind nicht als genaue Geschwindigkeitsangaben zu verstehen, sondern als Optimierungen für bestimmte Bedingungen. Der Client und der Server versuchen stets, Videodaten so schnell wie möglich über das Netzwerk zu übertragen, unabhängig von der aktuellen Netzwerkgeschwindigkeit und Codierungseinstellung. Das System arbeitet am schnellsten, wenn die Einstellungen der tatsächlichen Umgebung entsprechen.

3. Wählen Sie in der Dropdownliste **Color Depth** (Farbtiefe) die gewünschte Farbtiefe aus. Der Dominion KX II kann die an Remotebenutzer übertragene Farbtiefe dynamisch anpassen, um die Verwendbarkeit in allen Bandbreiten zu maximieren.

15-Bit-Farbe (RGB)
8-Bit-Farbe (RGB)
4-Bit-Farbe
4-Bit-Graustufen
3-Bit-Graustufen
2-Bit-Graustufen
Schwarzweiß

Wichtig: Für die meisten Verwaltungsaufgaben (Überwachung, erneute Konfiguration von Servern usw.) wird das von den modernen Videografikkarten bereitgestellte vollständige 24-Bit- oder 32-Bit-Farbspektrum nicht benötigt. Durch den Versuch, solch hohe Farbtiefen zu übertragen, wird Netzwerkbandbreite verschwendet.

4. Verwenden Sie den Schieberegler unter **Smoothing** (Glättung), um die gewünschte Glättung auszuwählen (nur im 15-Bit-Farbmodus). Die Glättungsebene bestimmt, wie stark Bildschirmbereiche mit geringer Farbvariation zu einer einheitlichen Farbe zusammengefasst werden. Die Glättung verbessert das Aussehen des Zielgerätbildes, da dadurch das Videorauschen verringert wird.
5. Klicken Sie auf **OK**, um die Eigenschaften festzulegen.

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

Verbindungsinformationen

So erhalten Sie Informationen über die Verbindung des Virtual KVM Client:

Wählen Sie **Connection > Connection Info** (Verbindung > Verbindungsinformationen). Das Fenster **Connection Info** (Verbindungsinformationen) wird angezeigt.

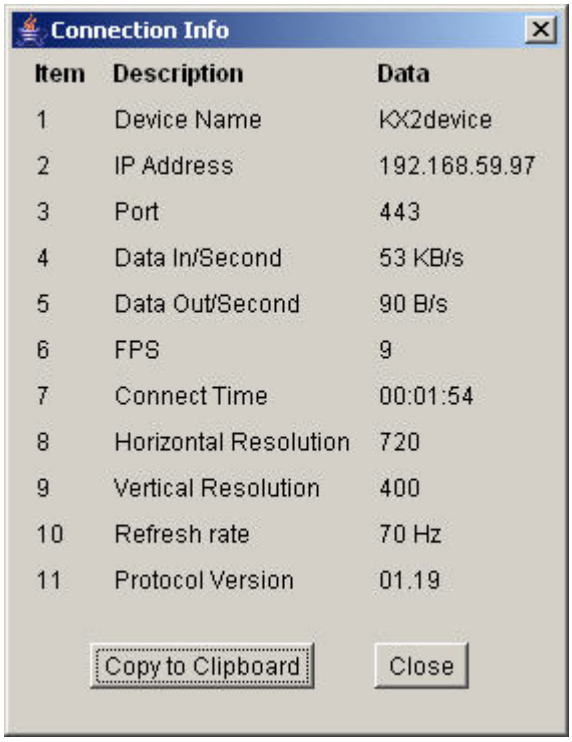

Abbildung 30: Verbindungsinformationen

Zur aktuellen Verbindung werden folgende Informationen angezeigt:

- **Device Name** (Gerätename): Der Name des Dominion KX II-Geräts.
- **IP Address** (IP-Adresse): Die IP-Adresse des Dominion KX II-Geräts.
- **Port**: Der TCP/IP-Port für die KVM-Kommunikation, über den auf das Zielgerät zugegriffen wird.
- **Data In/Second** (Dateneingang/Sekunde): Eingehende Datenrate.
- **Data Out/Second** (Datenausgang/Sekunde): Ausgehende Datenrate.
- **Connect Time** (Verbindungsdauer): Die Verbindungsdauer.
- **FPS**: Frames pro Sekunde der übertragenen Videobilder.
- **Horizontal Resolution** (Horizontale Auflösung): Die horizontale Bildschirmauflösung.
- **Vertical Resolution** (Vertikale Auflösung): Die vertikale Bildschirmauflösung.
- **Refresh Rate** (Aktualisierungsfrequenz): Gibt an, wie häufig die Anzeige aktualisiert wird.
- **Protocol Version** (Protokollversion): Version des RFB-Protokolls.

So kopieren Sie diese Informationen:

Klicken Sie auf **Copy to Clipboard** (In Zwischenablage kopieren). Anschließend können die Informationen in ein Programm Ihrer Wahl eingefügt werden.

Beenden

So schließen Sie den Virtual KVM Client (das Zielgerät, auf das derzeit zugegriffen wird):

Wählen Sie **Connection > Exit** (Verbindung > Beenden).

Menü Keyboard (Tastatur)

Senden von Strg+Alt+Entf

Aufgrund der häufigen Verwendung dieser Tastenkombination ist ein Makro **Strg+Alt+Entf** im Virtual KVM Client vorprogrammiert.

Diese Tastenkombination wird an den Zielserver gesendet, mit dem derzeit eine Verbindung besteht. Wenn Sie aber bei der Verwendung des Virtual KVM Client die Tastenkombination **Strg+Alt+Entf** drücken, wird diese Eingabe aufgrund der Struktur des Betriebssystems zunächst von Ihrem eigenen PC abgefangen, anstatt die Tastenfolge wie gewünscht an den Zielserver zu senden.

	Senden von **Strg+Alt+Entf**	Sendet die Tastenkombination **Strg+Alt+Entf** an den Zielserver.

So senden Sie die Tastenkombination **Strg+Alt+Entf** an den Zielserver:

- Wählen Sie **Keyboard > Send Ctrl+Alt+Delete** (Tastatur > Strg+Alt+Entf senden), oder
- Klicken Sie in der Symbolleiste auf die Schaltfläche **Send Ctrl+Alt+Delete** (Strg+Alt+Entf senden).

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 also einen anderen PC verwenden, werden Ihnen Ihre Makros nicht angezeigt. 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. Im Virtual KVM Client erstellte Tastaturmakros stehen im MPC zur Verfügung und umgekehrt.

Erstellen eines Tastaturmakros

So erstellen Sie ein Tastaturmakro (fügen es hinzu):

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Fenster **Keyboard Macros** (Tastaturmakros) wird angezeigt.

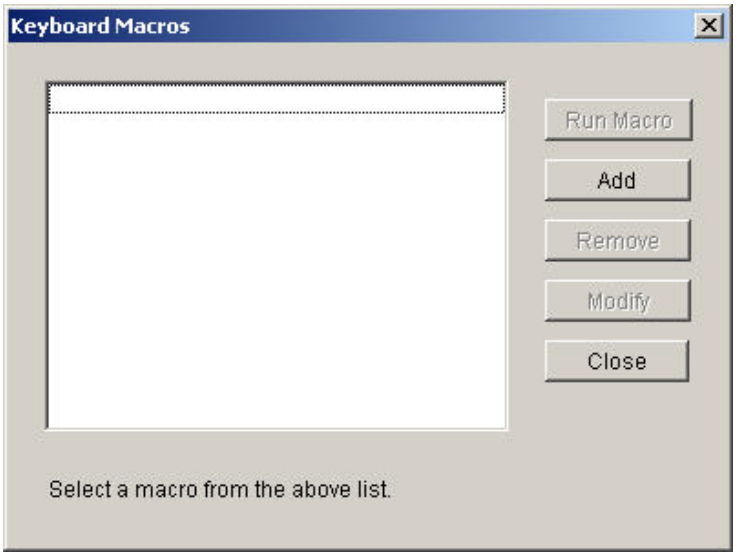

Abbildung 31: Tastaturmakros

2. Klicken Sie auf **Add** (Senden). Das Fenster **Add Keyboard Macro** (Tastaturmakro hinzufügen) wird angezeigt.

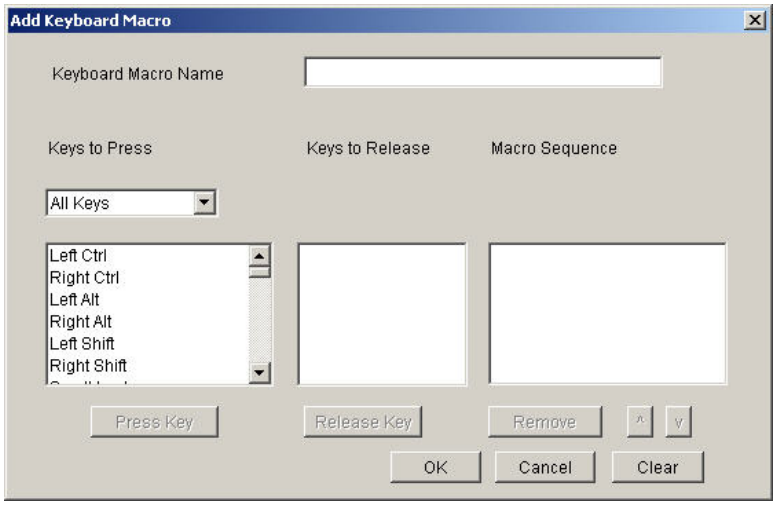

Abbildung 32: Add Keyboard Macro (Tastaturmakro hinzufügen)

3. Geben Sie einen Namen ins Feld **Keyboard Macro Name** (Name des Tastaturmakros) ein. Nachdem das Makro erstellt wurde, wird dieser Name in der Menüleiste des Virtual KVM Client angezeigt. Geben Sie in diesem Fall **Minimize All Windows** (Alle Fenster minimieren) ein.
4. Führen Sie in der Dropdownliste **Keys to Press** (Zu betätigende Tasten) folgende Schritte aus:
   a. Blättern Sie durch die Liste, und wählen Sie die Tasten aus, für die Sie Tastenbetätigungen emulieren möchten (in der Betätigungsreihenfolge).
   b. Klicken Sie nach jeder Auswahl auf die Schaltfläche **Press Key** (Taste betätigen). Jede ausgewählte Taste wird im Feld **Keys to Release** (Freizugebende Tasten) angezeigt.

   In diesem Beispiel wählen Sie zwei Tasten aus: die **Windows**-Taste und die **D**-Taste.
5. Führen Sie im Feld **Keys to Release** (Freizugebende Tasten) folgende Schritte aus:
   a. Wählen Sie die Tasten aus, für die Sie das Freigeben der Taste emulieren möchten (in der Reihenfolge, in der die Tasten freigegeben werden müssen).
   b. Klicken Sie nach jeder Auswahl auf **Release Key** (Taste freigeben).

   In diesem Beispiel müssen die beiden betätigten Tasten auch freigegeben werden.

6. Überprüfen Sie das Feld **Macro Sequence** (Makrosequenz), dessen Inhalt entsprechend Ihrer Auswahl für **Keys to Press** (Zu betätigende Tasten) und **Keys to Release** (Freizugebende Tasten) automatisch generiert wurde. Vergewissern Sie sich, dass die Makrosequenz Ihren Wünschen entspricht. Wenn Sie einen Schritt aus der Sequenz entfernen möchten, markieren Sie diesen, und klicken Sie auf **Remove** (Entfernen).

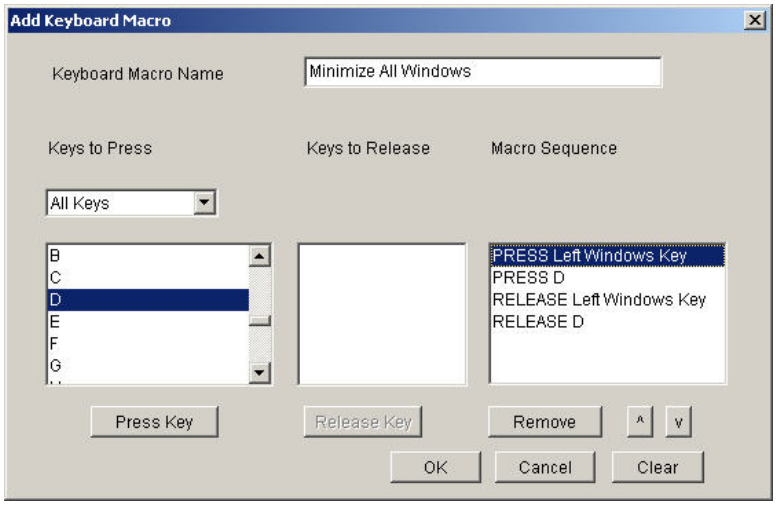

Abbildung 33: Beispiel für ein Tastaturmakro

Tipp: Verwenden Sie die Tasten ∧ und ∨, um die Tastenreihenfolge zu ändern.

7. Klicken Sie im Fenster **Add Keyboard Macro** (Tastaturmakro hinzufügen) auf **OK**, um das Makro zu speichern.
8. Klicken Sie im Fenster **Keyboard Macros** (Tastaturmakros) auf **Close** (Schließen) (). Das erstellte Tastaturmakro wird nun im Menü **Keyboard** (Tastatur) als Option aufgeführt.

*Abbildung 34: Neues Makro im Menü **Keyboard** (Tastatur)*

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So löschen Sie alle Felder, um erneut mit der Auswahl zu beginnen:

Klicken Sie auf die Schaltfläche **Clear** (Löschen).

Ausführen eines Tastaturmakros

Nachdem Sie ein Tastaturmakro erstellt haben, können Sie im Menü **Keyboard** (Tastatur) auf seinen Namen klicken, um es auszuführen.

So führen Sie ein Makro aus (mit obigem Beispiel):

Wählen Sie **Keyboard > Minimize All Windows** (Tastatur > Alle Fenster minimieren).

Sie können das Makro auch im Fenster **Keyboard Macros** (Tastaturmakros) auswählen.

So führen Sie ein Makro aus:

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Fenster **Keyboard Macros** (Tastaturmakros) wird angezeigt.
2. Wählen Sie das gewünschte Makro aus der Liste aus.
3. Klicken Sie auf **Run Macro** (Makro ausführen).

Ändern eines Tastaturmakros

So ändern Sie ein Makro:

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Fenster **Keyboard Macros** (Tastaturmakros) wird angezeigt.
2. Wählen Sie das gewünschte Makro aus der Liste aus.
3. Klicken Sie auf **Modify** (Ändern). Das Fenster **Add/Edit Macro** (Makro hinzufügen/bearbeiten) wird angezeigt.
4. Nehmen Sie die gewünschten Änderungen vor.
5. Klicken Sie auf **OK** (Senden).

Entfernen eines Tastaturmakros

Gehen Sie beim Entfernen von Makros bedachtsam vor. Sie werden nicht aufgefordert, den Löschvorgang zu bestätigen.

So entfernen Sie ein Makro:

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Fenster **Keyboard Macros** (Tastaturmakros) wird angezeigt.
2. Wählen Sie das gewünschte Makro aus der Liste aus.
3. Klicken Sie auf **Remove** (Entfernen). Das Makro wird gelöscht.

Menü Video

Videoeinstellungen können auf verschiedene Art und Weise automatisch aktualisiert werden:

- Die Option **Refresh Screen** (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms.
- Die Option **Auto-sense Video Settings** (Videoeinstellungen automatisch erkennen) erkennt die Videoeinstellungen des Zielservers automatisch.
- Die Option **Calibrate Color** (Farbe kalibrieren) kalibriert das Videobild, um die angezeigten Farben zu verbessern.

Darüber hinaus können Sie die Einstellungen manuell über die Option **Video Settings** (Videoeinstellungen) anpassen.

Refresh Screen (Anzeige aktualisieren)

Die Option **Refresh Screen** (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms. Die gesamte Videoanzeige wird neu erstellt.

	Schaltfläche **Refresh Screen** (Anzeige aktualisieren)

So aktualisieren Sie die Videoeinstellungen:

- Wählen Sie **Video > Refresh Screen** (Video > Anzeige aktualisieren), oder
- Klicken Sie in der Symbolleiste auf die Schaltfläche **Refresh Screen** (Anzeige aktualisieren).

Auto-sense Video Settings (Videoeinstellungen automatisch erkennen)

Die Option **Auto-sense Video Settings** (Videoeinstellungen automatisch erkennen) erzwingt das erneute Erkennen der Videoeinstellungen (Auflösung, Aktualisierungsfrequenz) und erstellt die Videoanzeige neu.

	Schaltfläche **Auto-sense Video Settings** (Videoeinstellungen automatisch erkennen)

So lassen Sie die Videoeinstellungen automatisch erkennen:

- Wählen Sie **Video > Auto-sense Video Settings** (Video > Videoeinstellungen automatisch erkennen), oder
- Klicken Sie in der Symbolleiste auf die Schaltfläche **Auto-sense Video Settings** (Videoeinstellungen automatisch erkennen).

Eine Meldung mit der Information, dass die automatische Anpassung läuft, wird angezeigt.

Calibrate Color (Farbe kalibrieren)

Verwenden Sie den Befehl **Calibrate Color** (Farbe kalibrieren), um die Farbstufen (Farbton, Helligkeit, Sättigung) der übertragenen Videobilder zu optimieren. Die Farbeinstellungen des Dominion KX II basieren auf dem jeweiligen Zielserver.

	Calibrate Color (Farbe kalibrieren)	Passt die Farbeinstellungen an, um die Videoanzeige zu optimieren.

Hinweis: *Die Option* ***Calibrate Color*** *(Farbe kalibrieren) gilt nur für die aktuelle Verbindung.*

So kalibrieren Sie die Farbe:

1. Öffnen Sie auf einem beliebigen Zielserver mit grafischer Benutzeroberfläche eine Remote-KVM-Verbindung.
2. Wählen Sie **Video > Calibrate Color** (Video > Farbe kalibrieren) (oder klicken Sie auf die Schaltfläche **Calibrate Color**). Die Farbkalibrierung des Zielgerätebildschirms wird aktualisiert.

Video Settings (Videoeinstellungen)

Verwenden Sie die Option **Video Settings**, um die Videoeinstellungen manuell anzupassen.

	Video Settings (Videoeinstellungen)	Öffnet die Videoeinstellungen zum manuellen Anpassen der Videoparameter.

So ändern Sie die Videoeinstellungen:

1. Wählen Sie **Video** > **Video Settings** (Video > Videoeinstellungen). Das Fenster **Video Settings** (Videoeinstellungen) wird mit den aktuellen Einstellungen angezeigt.

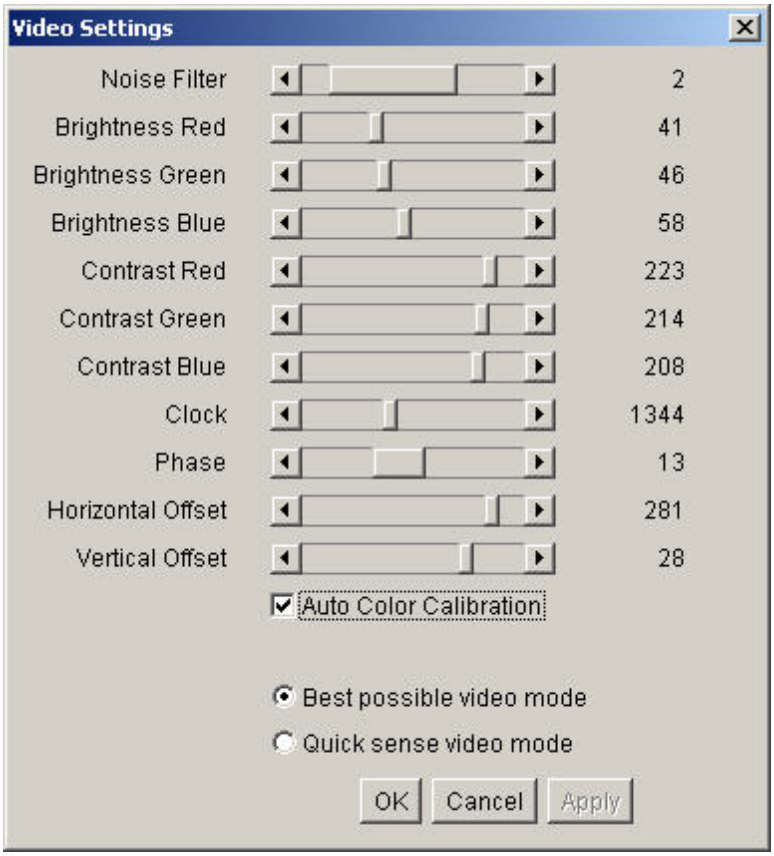

Abbildung 35: Video Settings (Videoeinstellungen)

2. Passen Sie die Einstellungen mithilfe der Schieber an, um das gewünschte Ergebnis zu erzielen (die Auswirkungen geänderter Einstellungen sind sofort erkennbar):
   - **Noise Filter** (Rauschfilter): Der Dominion KX II kann elektrische Störungen aus der Videoausgabe von Grafikkarten herausfiltern. Dieses Feature optimiert die Bildqualität und reduziert die Bandbreite. Höhere Einstellungen übermitteln nur dann Variantenpixel, wenn bei einem Vergleich mit den Nachparpixeln ein starke Farbabweichung vorliegt. Eine zu hohe Einstellung des Schwellwerts kann jedoch zu einer unbeabsichtigten Filterung von gewünschten Bildschirmänderungen führen.

     Niedrigere Einstellungen übermitteln die meisten Pixeländerungen. Eine zu niedrige Einstellung dieses Schwellwerts kann zu einer höheren Bandbreitenverwendung führen.
   - **Brightness** (Helligkeit): Mithilfe dieser Einstellung passen Sie die Helligkeit der Zielserveranzeige an.
     - **Red** (Rot): Steuert die Helligkeit des roten Signals.
     - **Green** (Grün): Steuert die Helligkeit des grünen Signals.
     - **Blue** (Blau): Steuert die Helligkeit des blauen Signals.

- **Color Contrast Settings** (Farbkontrasteinstellungen): Steuern die Kontrasteinstellung.
  - **Contrast Red** (Kontrast Rot): Steuert das rote Signal.
  - **Contrast Green** (Kontrast Grün): Steuert das grüne Signal.
  - **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 bei der Änderung der Einstellungen für Uhr und Phase bedachtsam vor, da dies zu Verzerrungen oder sogar zum Verlust des Videobildes führen kann und Sie möglicherweise die vorherigen Einstellungen nicht wiederherstellen können. Wenden Sie sich an den technischen Kundendienst von Raritan, bevor Sie Änderungen vornehmen.

  - **Clock** (Uhr): Er steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobildes. 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.
- **Offset**: Steuert die Positionierung auf dem Bildschirm.
  - **Horizontal Offset** (Horizontaloffset): Steuert die horizontale Positionierung der Zielserveranzeige auf dem Bildschirm.
  - **Vertical Offset** (Vertikaloffset): Steuert die vertikale Positionierung der Zielserveranzeige auf dem Bildschirm.
- **Auto Color Calibration** (Automatische Farbkalibrierung): Aktivieren Sie dieses Kontrollkästchen, wenn die Farbe automatisch kalibriert werden soll.
- **Video Sensing** (Videoerkennung): Wählen Sie einen Videoerkennungsmodus aus:
  - **Best possible video mode** (Bestmöglicher Videomodus): Beim Wechseln von Zielgeräten oder Zielauflösungen führt der Dominion KX II 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 der Dominion KX II die 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.

3. Klicken Sie auf **Übernehmen**. Die Videoeinstellungen werden geändert.

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.*

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

Menü Mouse (Maus)

Bei der Steuerung eines Zielservers zeigt die KX II-Remotekonsole zwei Cursors an: Ein Cursor gehört zur Clientworkstation und der andere zum Zielserver. Sie können entweder im Ein-Cursor-Modus oder im Zwei-Cursor-Modus arbeiten. Wenn der Zwei-Cursor-Modus korrekt konfiguriert ist, sind die beiden Cursors aneinander ausgerichtet. Hilfe bei Problemen mit der Maussynchronisation finden Sie unter Konfigurieren von Zielservern.

Bei zwei Cursors bietet der Dominion KX II verschiedene Mausmodi:

- **Absolute** (Absolute Mouse Synchronization)
- **Intelligent** (Intelligenter Mausmodus)
- **Standard** (Standardmausmodus)

Synchronize Mouse (Maus synchronisieren)

Im Zwei-Cursor-Modus erzwingt die Option **Synchronize Mouse** (Maus synchronisieren) die erneute Ausrichtung des Zielserver-Mauszeigers am Mauszeiger des Virtual KVM Client.

	Synchronize Mouse (Maus synchronisieren)

So synchronisieren Sie den Mauszeiger:

- Wählen Sie **Mouse > Synchronize Mouse** (Maus > Maus synchronisieren), oder
- Klicken Sie in der Symbolleiste auf die Schaltfläche **Synchronize Mouse** (Maus synchronisieren).

Single Mouse Cursor (Ein Cursor)

Über die Schaltfläche **Single Mouse Cursor** (Ein Cursor) aktivieren Sie den Ein-Cursor-Modus, in dem der Cursor des Zielservers auf dem Bildschirm angezeigt wird, aber nicht der Cursor des lokalen PCs. Im Ein-Cursor-Modus steht die Option **Synchronize Mouse** (Maus synchronisieren) nicht zur Verfügung, da ein einzelner Mauszeiger nicht synchronisiert werden muss.

	Single Mouse Cursor (Ein Cursor)

So gelangen Sie in den Ein-Cursor-Modus:

- Wählen Sie **Mouse > Single Mouse Cursor** (Maus > Ein Cursor), oder
- Klicken Sie in der Symbolleiste auf die Schaltfläche **Single/Double Mouse Cursor** (Ein/Zwei Cursor).

So beenden Sie den Ein-Cursor-Modus:

1. Wenn der Ein-Cursor-Modus aufgerufen wird, wird die folgende Meldung angezeigt. Klicken Sie auf **OK** (Senden).

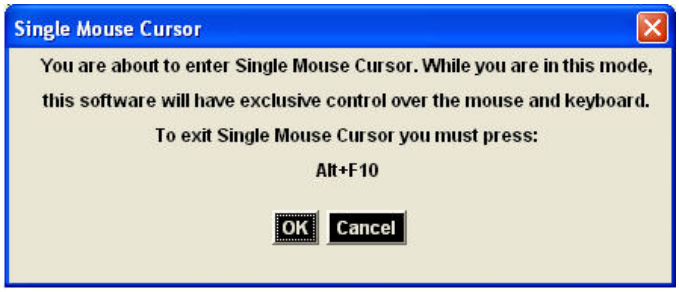

*Abbildung 36: Meldung **Single Mouse Cursor** (Ein Cursor)*

2. Drücken Sie **Alt+F10** auf der Tastatur, um den Ein-Cursor-Modus zu beenden.

Standard

Dies ist der Standardalgorithmus zur Maussynchronisation, der mit relativen Mauspositionen arbeitet. Für den Standardmausmodus müssen die Beschleunigung deaktiviert und andere Mausparameter korrekt eingerichtet werden, damit die Client- und die Servermaus synchron bleiben. Der Standardmausmodus ist voreingestellt.

So gelangen Sie in den Standardmausmodus:

Wählen Sie **Mouse > Standard** (Maus > Standard).

Intelligent

Im Intelligenten Mausmodus erkennt der Dominion KX II die Mauseinstellungen des Zielgeräts und kann die Mauszeiger dementsprechend synchronisieren, wodurch die Mausbeschleunigung auf dem Zielgerät ermöglicht wird. In diesem Modus „tanzt“ der Cursor in der oberen linken Ecke des Bildschirms und berechnet die Beschleunigung. Damit dieser Modus richtig funktioniert, müssen bestimmte Bedingungen erfüllt sein.

Weitere Informationen zum Intelligenten Mausmodus finden Sie im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan* (*Anhang B: Bedingungen zur intelligenten Maussynchronisation)*. Dieses Handbuch finden Sie auf der Website von Raritan unter http://www.raritan.com/support/productdocumentation oder auf der *CD-ROM von Raritan mit Benutzerhandbüchern und Kurzanleitungen*, die im Lieferumfang von Dominion KX II enthalten ist.

So gelangen Sie in den Intelligenten Mausmodus:

Wählen Sie **Mouse > Intelligent** (Maus > Intelligent).

Absolute (Absolut)

Hinweis: *Der Mausmodus Absolute Mouse Synchronization steht nur für das USB-CIM (D2CIM-VUSB) mit Aktivierung für virtuelle Medien zur Verfügung.*

In diesem Modus werden absolute Koordinaten verwendet, um die Mauszeiger von Client und Zielgerät synchron zu halten, auch wenn für die Zielgerätmaus eine andere Beschleunigung oder Geschwindigkeit eingestellt wurde. Dieser Modus wird auf Servern mit USB-Ports unterstützt. Der Cursor bewegt sich auf dem Zielserver an die exakte Position.

So gelangen Sie in den Mausmodus **Absolute** (Absolut):

Wählen Sie **Mouse > Absolute** (Maus > Absolut).

Virtuelle Medien

Umfassende Informationen zum Einrichten und Verwenden virtueller Medien finden Sie im Kapitel Virtuelle Medien.

Menü Tools (Extras)

Optionen

Über das Menü **Tools** (Extras) können Sie verschiedene Optionen für den Virtual KVM Client wählen: Synchronisieren der Maus im Zwei-Cursor-Modus, Aktivieren der Protokollierung, den Tastaturtyp und die Zugriffstaste, um den Modus **Target Screen Resolution** (Zielbildschirmauflösung) zu beenden.

So legen Sie die Optionen im Menü **Tools** (Extras) fest:

1. Wählen Sie **Tools > Options** (Extras > Optionen). Das Fenster **Options** (Optionen) wird angezeigt.

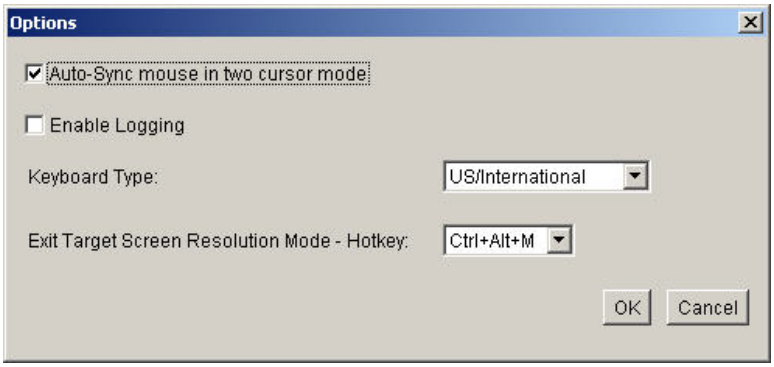

Abbildung 37: (Extras) Optionen

2. Aktivieren Sie die Kontrollkästchen für die gewünschten Optionen.
   - **Auto Sync Mouse in Two Cursor Mode** (Automatische Synchronisation der Maus im Zwei-Cursor-Modus): Bei dieser Option wird der Mauszeiger im Zwei-Cursor-Modus automatisch synchronisiert.
   - **Enable Logging** (Protokollierung aktivieren): Verwenden Sie diese Option nur nach Anweisung des technischen Kundendienstes. Bei dieser Option wird im Basisverzeichnis eine Protokolldatei erstellt.
3. Wählen Sie ggf. in der Dropdownliste **Keyboard Type** (Tastaturtyp) einen Tastaturtyp aus. Folgende Optionen stehen zur Verfügung:
   - US/International (USA/International)
   - French (France) (Französisch)
   - German (Germany) (Deutsch)
   - Japanese (Japanisch)
   - United Kingdom
   - Korean (Korea) (Koreanisch)
4. **Exit Target Screen Resolution Mode – Hotkey** (Zugriffstaste zum Beenden des Modus Zielbildschirmauflösung): Wenn Sie in den Modus **Target Screen Resolution** (Zielbildschirmauflösung) wechseln, wird der Zielserver im Vollbildmodus mit der entsprechenden Auflösung angezeigt. Über diese Zugriffstaste können Sie diesen Modus beenden. Wählen Sie eine Option aus der Dropdownliste.
5. Klicken Sie auf **OK** (Senden).

Menü View (Ansicht)

Anzeigen der Symbolleiste

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).

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 Zielserverdesktop angezeigt, und Sie müssen nicht die Bildlaufleiste verwenden.

So aktivieren bzw. deaktivieren Sie die Skalierung:

Wählen Sie **View > Scaling** (Ansicht > Skalieren).

Zielbildschirmauflösung

Wenn Sie in den Modus **Target Screen Resolution** (Zielbildschirmauflösung) wechseln, wird der Zielserver im Vollbildmodus mit der entsprechenden Auflösung angezeigt. Die Zugriffstaste, über die Sie diesen Modus beenden können, legen Sie im Dialogfeld **Options** (Optionen) fest. Standardmäßig lautet die Tastenkombination **Strg+Alt+M**.

So gelangen Sie in den Modus **Target Screen Resolution** (Zielbildschirmauflösung):

Wählen Sie **View > Target Screen Resolution** (Ansicht > Zielbildschirmauflösung).

So beenden Sie den Modus **Target Screen Resolution** (Zielbildschirmauflösung):

Drücken Sie die unter konfigurierte Zugriffstaste. Standardmäßig ist dies die Tastenkombination **Strg+Alt+M**.

Menü Help (Hilfe)

About Raritan Virtual KVM Client (Informationen zum Raritan Virtual KVM Client)

Diese Menüoption liefert Versionsinformationen zum Virtual KVM Client, falls Sie Unterstützung durch den technischen Kundendienst von Raritan benötigen.

So rufen Sie die Versionsinformationen ab:

Wählen Sie **Help > About Raritan Virtual KVM Client** (Hilfe > Informationen zum Raritan Virtual KVM Client).

Kapitel 7: Virtuelle Medien

Überblick

Virtuelle Medien erweitern die KVM-Funktionen. Sie ermöglichen Zielservern den Remotezugriff auf Medien auf dem Client-PC und Netzwerkdateiservern. Dank dieses Features werden auf dem Client-PC und Netzwerkdateiservern installierte Medien praktisch *virtuell* vom Zielserver installiert. Der Zielserver hat Lese- und Schreibzugriff auf die Medien, als wären sie physisch mit dem Zielserver verbunden. Virtuelle Medien können interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und ISO-Abbilder (Datenträgerabbilder) umfassen.

Virtuelle Medien bieten die Möglichkeit, weitere Aufgaben remote zu erledigen. Dazu zählen:

- Übertragen von Dateien
- Durchführen von Diagnosen
- Installieren oder Reparieren von Anwendungen
- Neustarten von Zielservern im Netzwerk mithilfe eines startbaren CD-ISO-Abbildes, auf das über den Client zugegriffen wird
- Vollständiges Installieren des Betriebssystems

Diese erweiterte KVM-Steuerung macht die meisten Gänge in das Rechenzentrum überflüssig, spart Zeit und Geld und unterstreicht damit die Bedeutung virtueller Medien.

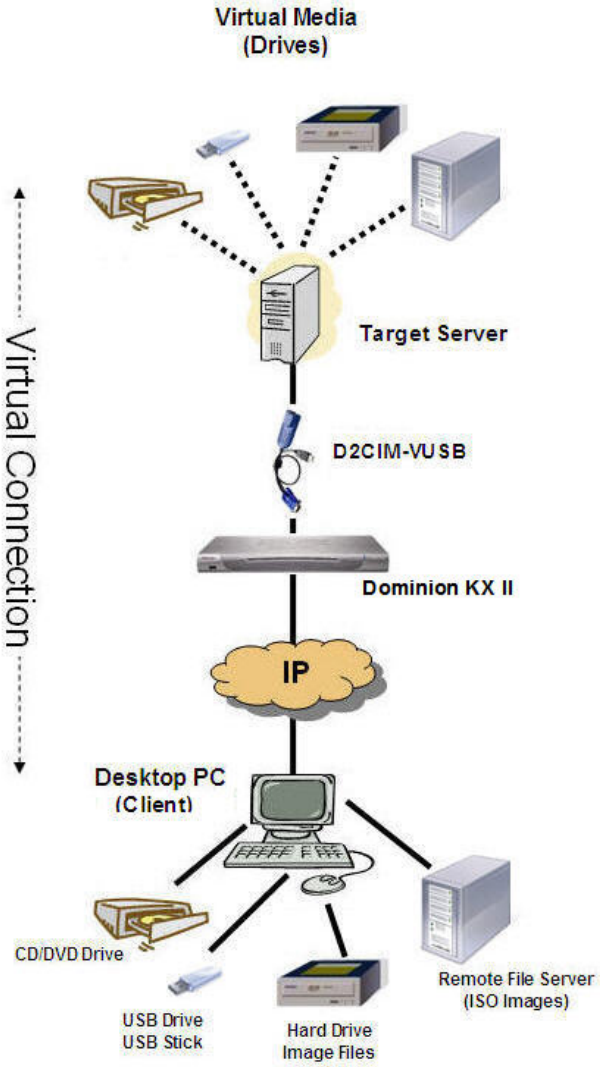

Abbildung 38: Verbindung virtueller Medien

Voraussetzungen für die Verwendung virtueller Medien

Für die Verwendung virtueller Medien müssen folgende Bedingungen erfüllt sein:

Dominion KX II

- Für Benutzer, die Zugriff auf virtuelle Medien benötigen, müssen KX-Berechtigungen 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 festgelegt. Weitere Informationen finden Sie unter Festlegen von Portberechtigungen.
- (Optional) Wenn Sie den Modus **PC-Share** (PC-Freigabe) verwenden möchten, müssen Sie auf der Seite **Security Settings** (Sicherheitseinstellungen) auch den VM-Freigabemodus aktivieren.

Client-PC

- Für bestimmte virtuelle Medienoptionen sind Administratorrechte auf dem Client-PC erforderlich (z. B. Umleitung ganzer Laufwerke).

  Hinweis: *Unter Microsoft Vista müssen Sie das Benutzerkonto-Steuerungsfeld* ***deaktivieren****:* ***Control Panel > User Accounts > User Account Control > turn off*** *(Systemsteuerung > Benutzerkonten > Benutzerkonto-Steuerungsfeld > deaktivieren).*

- USB 2.0-Ports sind schneller und daher vorzuziehen.

Zielserver

- Zielserver müssen über USB angeschlossene Laufwerke unterstützen.
- Auf Zielservern mit Microsoft Windows 2000 müssen alle aktuellen Patches installiert sein.

Verwenden virtueller Medien

Mithilfe des Features **Virtual Media** (Virtuelle Medien) von Dominion KX II können Sie bis zu zwei Laufwerke (unterschiedlichen Typs) installieren. 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 beendet wird.

So verwenden Sie virtuelle Medien:

1. Schließen Sie das Medium 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.
2. Vergewissern Sie sich, dass die entsprechenden Voraussetzungen erfüllt sind.
3. (***Nur bei Dateiserver-ISO-Abbildern***) Wenn Sie auf Dateiserver-ISO-Abbilder zugreifen möchten, lassen Sie diese Dateiserver und Abbilder über die Seite **File Server Setup** (Dateiserver-Setup) der Dominion KX II-Remotekonsole ermitteln.
4. Öffnen Sie eine KVM-Sitzung mit dem entsprechenden Zielserver.

5. Stellen Sie eine Verbindung mit dem virtuellen Medium her.

VIRTUELLES MEDIUM	ENTSPRECHENDE VM-OPTION
Lokale Laufwerke	Connect Drive (Laufwerk verbinden)
Lokale CD-/DVD-Laufwerke	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)
ISO-Abbilder	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)
Dateiserver-ISO-Abbilder	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)

6. Nach Abschluss Ihrer Aufgaben trennen Sie das virtuelle Medium.

Öffnen einer KVM-Sitzung

So öffnen Sie eine KVM-Sitzung:

1. Rufen Sie auf der Dominion KX II-Remotekonsole die Seite **Port Access** (Portzugriff) auf.

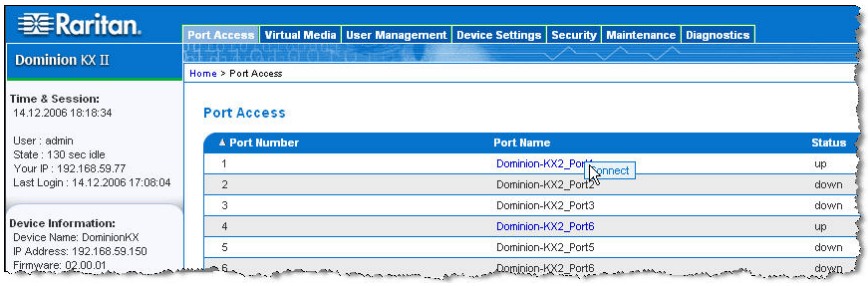

Abbildung 39: Öffnen einer KVM-Sitzung

2. Stellen Sie auf dieser Seite eine Verbindung mit dem Zielserver her:
   a. Klicken Sie unter **Port Name** (Portname) auf den entsprechenden Server.
   b. Wählen Sie im Menü **Port Action** (Portaktion) die Option **Connect** (Verbinden).

Der Zielserver wird in einem Fenster des Virtual KVM Client geöffnet.

Herstellen einer Verbindung mit virtuellen Medien

Lokale Laufwerke

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, nicht jedoch für Netzwerk-, CD-ROM- oder DVD-ROM-Laufwerke. Nur für diese Option ist **Read-Write** (Lese-/Schreibzugriff) verfügbar.

Hinweis: *Zielserver mit bestimmten Versionen des Windows-Betriebssystems akzeptieren möglicherweise keine neuen Massenspeicherverbindungen, nachdem eine NTFS-formatierte Partition (z. B. das lokale Laufwerk C) an sie umgeleitet wurde. Schließen Sie in diesem Fall die KX II-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.*

So greifen Sie auf ein Laufwerk auf dem Clientcomputer zu:

1. Wählen Sie im Virtual KVM Client **Virtual Media > Connect Drive** (Virtuelle Medien > Laufwerk verbinden). Das Dialogfeld **Map Virtual Media Drive** (Virtuelles Medienlaufwerk zuordnen) wird angezeigt.

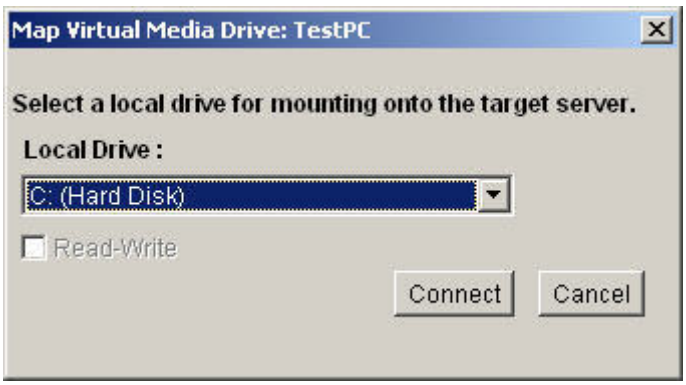

*Abbildung 40: **Map Virtual Media Drive** (Virtuelles Medienlaufwerk zuordnen)*

2. Wählen Sie das entsprechende Laufwerk in der Dropdownliste **Local Drive** (Lokales Laufwerk) aus.
3. Für den Lese- und Schreibzugriff müssen Sie das Kontrollkästchen **Read-Write** (Lese-/Schreibzugriff) aktivieren. Diese Option steht nur für Wechseldatenträger zur Verfügung. Weitere Informationen finden Sie unter Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist. 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.

4. Klicken Sie auf **Connect** (Verbinden). Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist

Der Lese-/Schreibzugriff auf virtuelle Medien ist in den folgenden Situationen nicht verfügbar:

- Bei allen Festplatten
- Wenn das Laufwerk schreibgeschützt ist
- Wenn der Benutzer nicht über eine Lese-/Schreibberechtigung verfügt:
  - Unter **Port Permission** (Portberechtigung) ist für **Access** (Zugriff) die Einstellung *None* (Keine) oder *View* (Ansicht) gewählt.
  - Unter **Port Permission** (Portberechtigung) ist für **VM Access** (VM-Zugriff) die Einstellung *Read-Only* (Schreibgeschützt) oder *Deny* (Ablehnen) gewählt.

CD-ROM-/DVD-ROM-/ISO-Abbilder

Mit dieser Option installieren Sie CD-ROM-, DVD-ROM- und ISO-Abbilder.

So greifen Sie auf ein CD-ROM-, DVD-ROM- oder ISO-Abbild zu:

1. Wählen Sie im Virtual KVM Client **Virtual Media > Connect CD-ROM/ISO Image** (Virtuelle Medien > CD-ROM-/ISO-Abbild verbinden). Das Dialogfeld **Map Virtual Media CD/ISO Image** (CD-/ISO-Abbild als virtuelles Medium zuordnen) wird angezeigt.

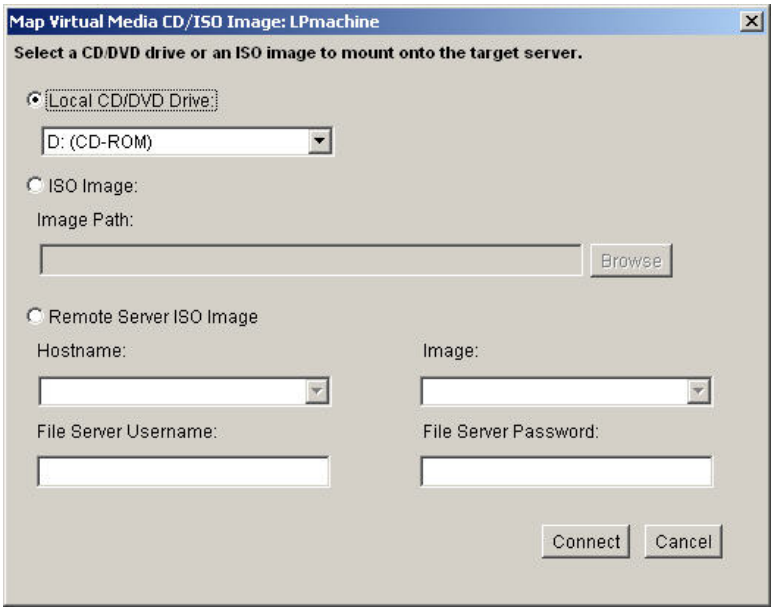

*Abbildung 41: **Map Virtual Media CD/ISO Image** (CD-/ISO-Abbild als virtuelles Medium zuordnen)*

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 Dropdownliste **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 die Schaltfläche **Browse** (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.

   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 den Dropdownlisten **Hostname** und **Image** (Abbild) 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 Dropdownliste enthält nur Elemente, die Sie auf der Dominion KX II-Seite **File Server Setup** (Dateiserver-Setup) konfiguriert haben.
   c. **File Server Username** (Dateiserver-Benutzername). Der für den Zugriff auf den Dateiserver erforderliche Benutzername.
   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.

Trennen von virtuellen Medien

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 die Option* ***Disconnect*** *zu trennen, können Sie auch einfach die KVM-Verbindung beenden.*

File Server Setup (Dateiserver-Setup) (nur für Dateiserver-ISO-Abbilder)

Hinweis: *Dieses Feature ist nur für den Zugriff auf Dateiserver-ISO-Abbilder über virtuelle Medien erforderlich.*

Legen Sie auf der Seite **File Server Setup** (Dateiserver-Setup) der Dominion KX II-Remotekonsole die Dateiserver und Abbildpfade fest, auf die Sie über virtuelle Medien in Dominion KX II zugreifen möchten. Hier angegebene Dateiserver-ISO-Abbilder stehen unter **Remote Server ISO Image** (ISO-Abbild auf Remoteserver) in den Dropdownlisten **Hostname** und **Image** (Abbild) zur Auswahl (im Dialogfeld **Map Virtual Media CD/ISO Image** (CD-/ISO-Abbild als virtuelles Medium zuordnen)).

So legen Sie Dateiserver-ISO-Abbilder für den virtuellen Medienzugriff fest:

1. Wählen Sie in der Dominion KX II-Remotekonsole die Option **Virtual Media** (Virtuelle Medien). Die Seite **File Server Setup** (Dateiserver-Setup) wird angezeigt.

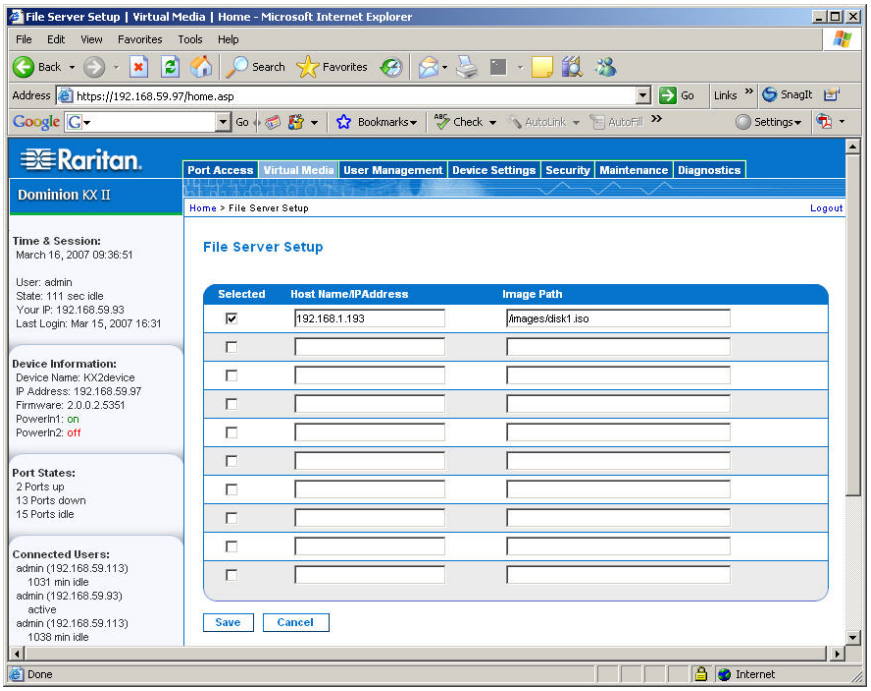

*Abbildung 42: **File Server Setup** (Dateiserver-Setup)*

2. Geben Sie Informationen zu den Dateiserver-ISO-Abbildern ein, auf die Sie zugreifen möchten:
   - **Host Name/IP Address** (Hostname/IP-Adresse). Hostname oder IP-Adresse des Dateiservers.
   - **Image Path** (Abbildpfad). Vollständiger Pfad zum Speicherort des ISO-Abbildes.
3. Aktivieren Sie das Kontrollkästchen **Selected** (Ausgewählt) für alle Medien, die als virtuelle Medien zugänglich sein sollen.
4. Klicken Sie auf **Save** (Speichern). Alle hier angegebenen Medien stehen nun im Dialogfeld **Map Virtual Media CD/ISO Image** (CD-/ISO-Abbild als virtuelles Medium zuordnen) zur Auswahl.

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

Kapitel 8: User Management

Das Menü **User Management** (Benutzerverwaltung) umfasst folgende Optionen: **User List** (Benutzerliste), **Add New User** (Neuen Benutzer hinzufügen), **User Group List** (Liste der Benutzergruppen), **Add New User Group** (Neue Benutzergruppe hinzufügen), **Change Password** (Kennwort ändern) und **Authentication Settings** (Authentifizierungseinstellungen).

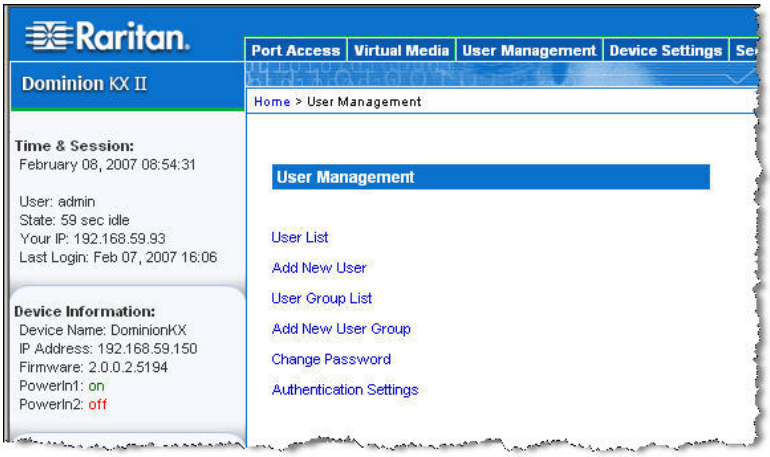

*Abbildung 43: Menü **User Management** (Benutzerverwaltung)*

OPTION	AN:
User List	Anzeigen einer alphabetischen Liste aller Benutzer; Hinzufügen, Ändern oder Löschen von Benutzern
Add New User (Neuen Benutzer hinzufügen)	Hinzufügen neuer Benutzer, Ändern von Benutzerinformationen
User Group List (Liste der Benutzergruppen)	Anzeigen einer alphabetischen Liste aller Benutzergruppen; Hinzufügen, Ändern oder Löschen von Benutzergruppen
Add New User Group (Neue Benutzergruppe hinzufügen)	Hinzufügen neuer Benutzergruppen, Ändern von Informationen zu Benutzergruppen
Ändern des Kennworts	Ändern des Kennworts eines bestimmten Benutzers
Authentication Settings (Authentifizierungseinstellungen)	Konfigurieren der Authentifizierung für den Zugriff auf den Dominion KX II

User List

Die Seite **User List** (Benutzerliste) enthält eine Liste aller Benutzer einschließlich Benutzername, vollständigem Namen und Benutzergruppe. Klicken Sie auf einen Spaltennamen, um die Liste nach einer der Spalten zu sortieren. Auf der Seite **User List** (Benutzerliste) können Sie außerdem Benutzer hinzufügen, ändern oder löschen.

So zeigen Sie die Benutzerliste an:

Wählen Sie **User Management > User List** (Benutzerverwaltung > Benutzerliste). Die Seite **User List** (Benutzerliste) wird angezeigt.

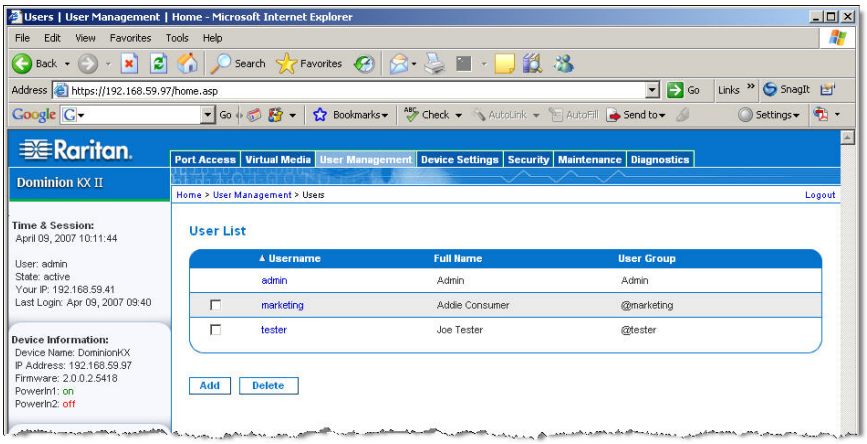

Abbildung 44: User List

So fügen Sie einen neuen Benutzer hinzu:

Klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Die Seite **User** (Benutzer) wird angezeigt. Umfassende Informationen zur Seite **User** (Benutzer) finden Sie unter Add New User (Neuen Benutzer hinzufügen).

So ändern Sie einen vorhandenen Benutzer:

1. Wählen Sie den gewünschten Benutzer aus der Liste aus.
2. Klicken Sie unter **Username** auf den Benutzernamen. Die Seite **User** (Benutzer) wird angezeigt. Umfassende Informationen zum Bearbeiten von Benutzern finden Sie unter Ändern vorhandener Benutzer.

So löschen Sie einen Benutzer:

1. Wählen Sie einen Benutzer aus der Liste aus, indem Sie das Kontrollkästchen links vom Benutzernamen aktivieren.
2. Klicken Sie auf **Löschen**.
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **OK** (Senden).

Add New User (Neuen Benutzer hinzufügen)

Es ist empfehlenswert, Benutzergruppen *vor* dem Erstellen von Dominion KX II-Benutzern zu definieren, da jeder Benutzer einer *vorhandenen* Benutzergruppe hinzugefügt werden muss. Auf der Seite **User** (Benutzer) können Sie neue Benutzer hinzufügen, Benutzerinformationen ändern und deaktivierte Benutzer erneut aktivieren.

Hinweis: *Ein Benutzername kann deaktiviert werden (Deaktivieren des Kontrollkästchens* ***Active*** *[Aktiv]), wenn die Anzahl der fehlgeschlagenen Anmeldeversuche die im Fenster* ***Security Settings*** *(Sicherheitseinstellungen) festgelegte maximale Anzahl der Anmeldeversuche überschritten hat. Weitere Informationen finden Sie unter Sicherheitseinstellungen.*

So fügen Sie einen neuen Benutzer hinzu:

1. Öffnen Sie die Seite **User** (Benutzer) mit einem der folgenden Verfahren:
   - Wählen Sie **User Management** > **Add New User** (Benutzerverwaltung > Neuen Benutzer hinzufügen), oder
   - Klicken Sie auf der Seite **User List** (Benutzerliste) auf die Schaltfläche **Add** (Hinzufügen).

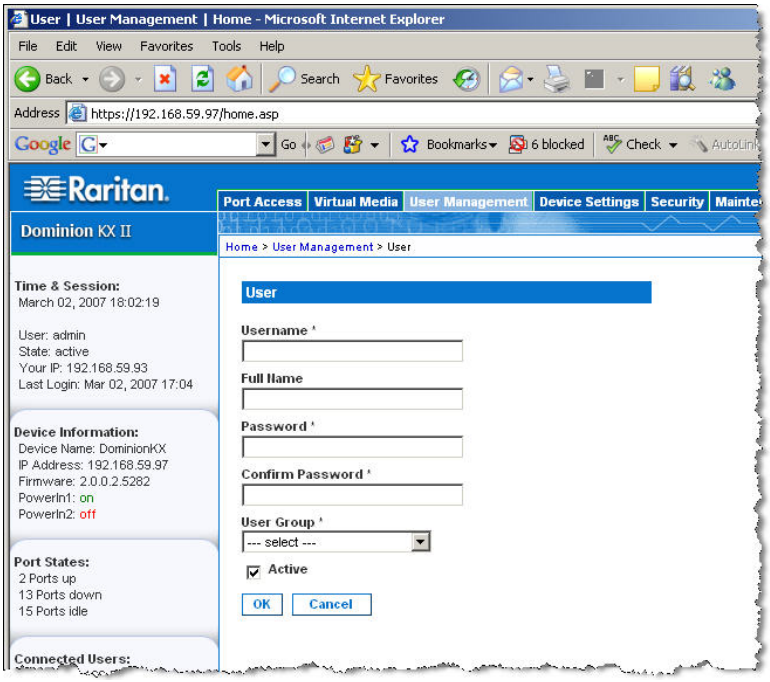

Abbildung 45: Seite ***User*** *(Benutzer)*

2. Geben Sie im Feld **Username** (Benutzername) einen eindeutigen Namen ein (bis zu 16 Zeichen).
3. Geben Sie im Feld **Full Name** den vollständigen Namen des Benutzers ein (bis zu 64 Zeichen).
4. Geben Sie im Feld **Password** ein Kennwort ein, und geben Sie es im Feld **Confirm Password** (Kennwort bestätigen) erneut ein (bis zu 64 Zeichen).
5. Wählen Sie in der Dropdownliste **User Group** (Benutzergruppe) die Gruppe aus. Die Liste enthält alle von Ihnen erstellten Gruppen sowie die vom System bereitgestellten Standardgruppen (<**Unknown**> [Unbekannt] [Standardeinstellung], **Admin** und **Individual Group** [Individuelle Gruppe]). Wenn Sie diesen Benutzer keiner vorhandenen Benutzergruppe zuordnen möchten, wählen Sie in der Dropdownliste die Option **Individual Group** (Individuelle Gruppe).

   Weitere Informationen zu den Berechtigungen einer individuellen Gruppe finden Sie unter Festlegen von Berechtigungen für individuelle Gruppen.

6. Aktivieren Sie das Kontrollkästchen **Active** (Aktiv), um den Benutzer zu aktivieren. Standardmäßig ist dieses Kontrollkästchen aktiviert.
7. Klicken Sie auf **OK** (Senden).

Ändern vorhandener Benutzer

So ändern Sie einen vorhandenen Benutzer:

1. Bearbeiten Sie auf der Seite **User** (Benutzer) () die entsprechenden Felder. (Informationen zum Zugriff auf die Seite **User** (Benutzer) finden Sie unter Add New User (Neuen Benutzer hinzufügen).)
2. Klicken Sie auf **OK** (Senden).

User Group List (Liste der Benutzergruppen)

Benutzergruppen werden bei der lokalen und der Remoteauthentifizierung (über RADIUS oder LDAP) 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.

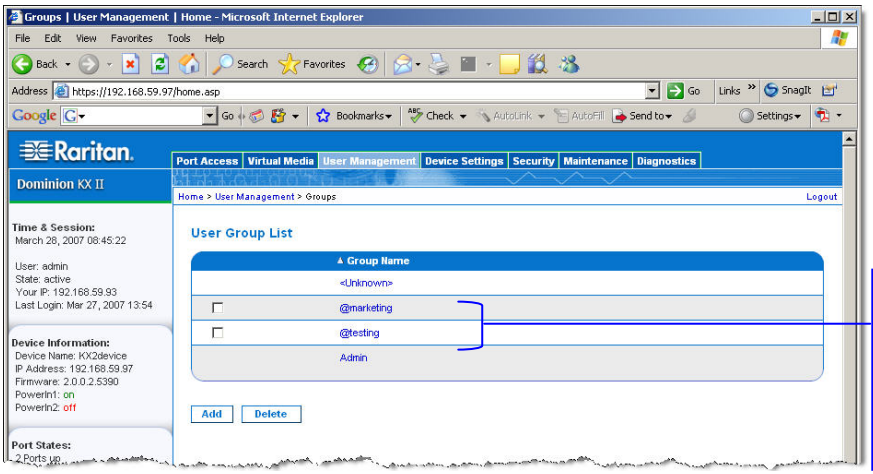

*Abbildung 46: **User Group List** (Liste der Benutzergruppen)*

So fügen Sie eine neue Benutzergruppe hinzu:

Klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Die Seite **Group** (Gruppe) wird angezeigt. Umfassende Informationen zur Seite **Group** (Gruppe) finden Sie unter Add New User Group (Neue Benutzergruppe hinzufügen).

So ändern Sie eine vorhandene Benutzergruppe:

1. Wählen Sie die gewünschte Benutzergruppe aus der Liste aus.
2. Klicken Sie auf den Gruppennamen. Die Seite **Group** (Gruppe) wird angezeigt. Umfassende Informationen zum Bearbeiten von Benutzergruppen finden Sie unter Ändern vorhandener Benutzergruppen.

So löschen Sie eine Benutzergruppe:

Wichtig: Stellen Sie vor dem Löschen einer Gruppe sicher, dass dieser keine Benutzer zugewiesen sind, da diese sonst auch gelöscht werden.

Tipp: Um herauszufinden, welche Benutzer einer bestimmten Gruppe angehören, sortieren Sie die Benutzerliste (Abbildung 44) nach Benutzergruppe.

1. Wählen Sie eine Gruppe aus der Liste aus, indem Sie das Kontrollkästchen links vom Gruppenamen aktivieren.
2. Klicken Sie auf **Löschen**.
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **OK** (Senden).

Add New User Group (Neue Benutzergruppe hinzufügen)

So fügen Sie eine neue Benutzergruppe hinzu:

1. Öffnen Sie die Seite Group (Gruppe) mit einem der folgenden Verfahren:
   - 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).

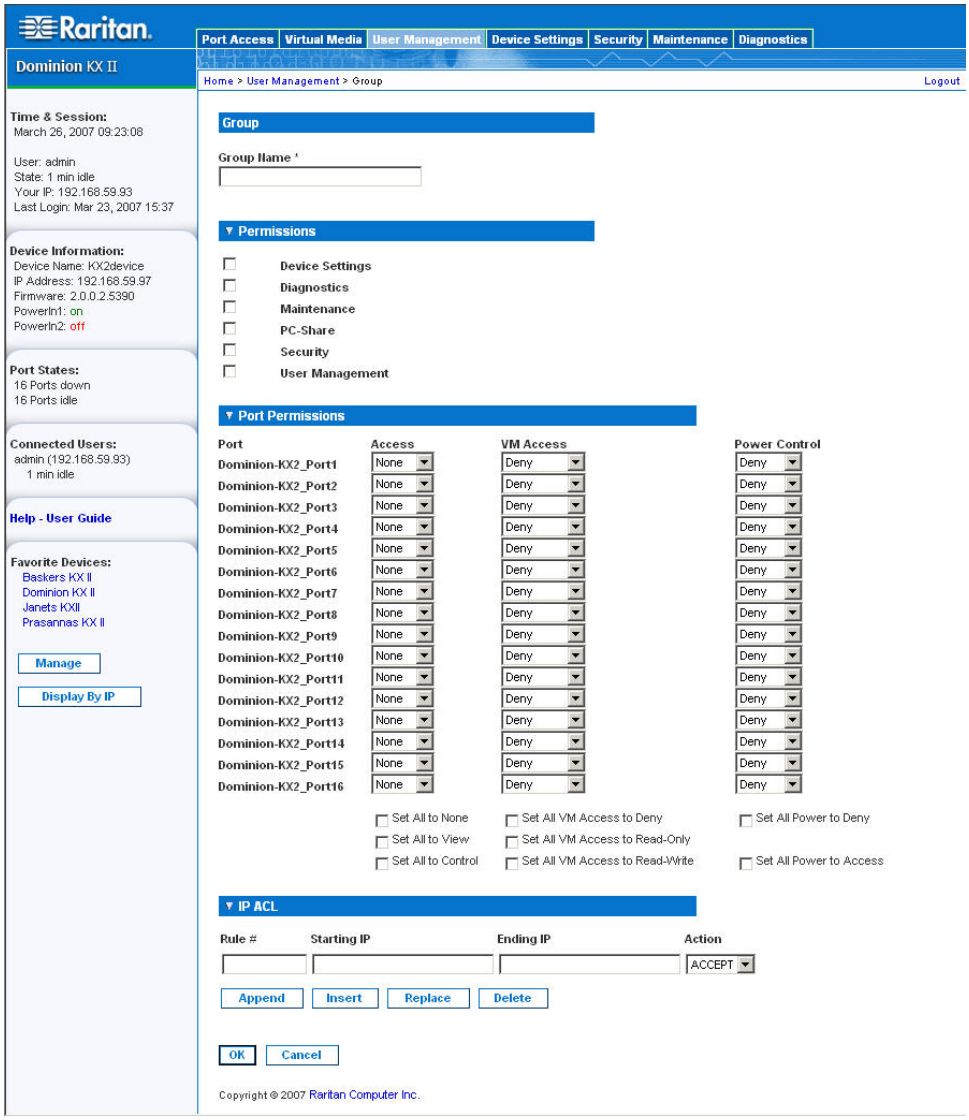

*Abbildung 47: Seite **Group** (Gruppe)*

Die Seite **Group** (Gruppe) umfasst die folgenden Kategorien: **Group** (Gruppe), **Permissions** (Berechtigungen), **Port Permissions** (Portberechtigungen) und **IP ACL** (IP-ACL).

2. Geben Sie im Feld **Group Name** (Gruppenname) einen aussagekräftigen Namen für die neue Benutzergruppe ein.
3. 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. Weitere Informationen finden Sie unter Festlegen von Berechtigungen.

4. Legen Sie unter **Port Permissions** (Portberechtigungen) die Portberechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Serverports fest, und geben Sie den Zugriffstyp an. Weitere Informationen finden Sie unter Festlegen von Portberechtigungen.
5. Legen Sie die IP-ACL fest (optional). Mit diesem Feature können Sie durch die Angabe von IP-Adressen den Zugriff auf das Dominion KX II-Gerät einschränken. Dies gilt **nur** für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für **alle** Zugriffsversuche auf das Gerät gilt (und Priorität hat).
6. Klicken Sie auf **OK** (Senden).

Hinweis: *Im MPC und über die lokale Dominion KX II-Konsole stehen mehrere Verwaltungsfunktionen zur Verfügung. Diese Funktionen können nur von Mitgliedern der Standardgruppe ADMIN verwendet werden.*

Festlegen von Berechtigungen

Wichtig: Wenn das Kontrollkästchen User Management (Benutzerverwaltung) aktiviert ist, können Mitglieder der Gruppe die Berechtigungen aller Benutzer einschließlich ihrer eigenen ändern. Lassen Sie beim Zuordnen dieser Berechtigungen Vorsicht walten.

BERECHTIGUNG	BESCHREIBUNG
Geräteeinstellungen	Netzwerkeinstellungen, Einstellungen für Datum und Uhrzeit, Portkonfiguration (Kanalnamen, Stromzuordnungen), Ereignisverwaltung (SNMP, Syslog), Dateiserver-Setup für virtuelle Medien
Diagnose	Status der Netzwerkschnittstelle, Netzwerkstatistik, Ping an den Host, Verfolgen der Route zum Host, KX-Diagnose
Wartung	Sichern und Wiederherstellen von Datenbanken, Firmwareaktualisierung, Werksrückstellung, Neustart
PC-Share	Gleichzeitiger Zugriff auf ein Zielgerät durch mehrere Benutzer
Sicherheit	SSL-Zertifikat, Sicherheitseinstellungen (VM-Freigabe, PC-Freigabe), IP-ACL
User Management	Benutzer- und Gruppenverwaltung, Remoteauthentifizierung (LDAP/RADIUS), Anmeldeeinstellungen

Festlegen von Portberechtigungen

Sie können für jeden Serverport den Zugriffstyp, den Zugriff auf virtuelle Medien und die Stromzufuhrsteuerung festlegen. Die Standardeinstellung für alle Berechtigungen ist deaktiviert.

ZUGRIFF		VM-ZUGRIFF		STROMZUFUHRSTEUERUNG	
Option	**Beschreibung**	**Option**	**Beschreibung**	**Option**	**Beschreibung**
None* (Keine)	Zugriff vollständig verweigert	**Deny* (Ablehnen)**	Berechtigung für virtuelle Medien wird für diesen Port vollständig verweigert	**Deny* (Ablehnen)**	Zugriff vollständig verweigert
View	Ansicht des Videobildes, aber keine Interaktion mit dem angeschlossenen Zielserver	**Read-Only (Lese-zugriff)**	Zugriff auf virtuelle Medien ist auf das Lesen beschränkt	**Zugriff**	Vollständiger Zugriff
Steuerung	Steuerung des angeschlossenen Zielservers	**Read-Write (Lese-/Schreib-zugriff)**	Vollständiger Zugriff (Lesen und Schreiben) auf virtuelle Medien		

* Standardeinstellung

Tipp: Mithilfe der Kontrollkästchen können Sie schnell für alle Ports dieselben Berechtigungen festlegen.

Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)

Wichtig: Gehen Sie bei der Verwendung der gruppenbasierten IP-Zugriffssteuerung bedachtsam vor. Der Zugriff auf den Dominion KX II 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 Dominion KX II-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. Weitere Informationen finden Sie unter IP-Zugriffssteuerung.

Wichtig: Die IP-Adresse 127.0.0.1 wird vom lokalen Port des Dominion KX II verwendet. Wenn sich 127.0.0.1 beim Erstellen der Zugriffssteuerungsliste im Bereich der gesperrten IP-Adressen befindet, können Sie nicht auf den lokalen Port des Dominion KX II zugreifen.

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

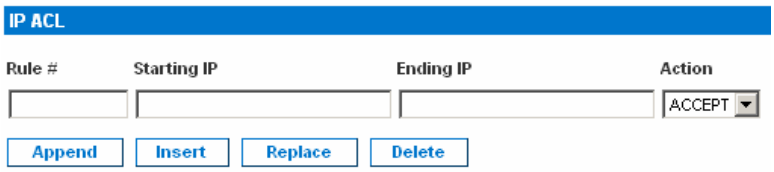

Abbildung 48: Gruppenbasierte IP-Zugriffssteuerungsliste

So fügen Sie Regeln hinzu:

1. Geben Sie im Feld **Starting IP** die IP-Startadresse ein.
2. Geben Sie im Feld **Ending IP** die IP-Endadresse ein.
3. Wählen Sie unter **Action** (Aktion) eine der folgenden Optionen:
   - **Accept** (Akzeptieren): Diese IP-Adressen können auf das Dominion KX II-Gerät zugreifen.
   - **Drop** (Ablehnen): Diesen IP-Adressen wird der Zugriff auf das Dominion KX II-Gerät verweigert.
4. Klicken Sie auf **Append** (Anfügen). Die Regel wird unten in der Liste hinzugefügt.
5. 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 **Löschen**.
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **OK** (Senden).

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

Abbildung 49: Beispiel für eine IP-ACL

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

Ändern vorhandener Benutzergruppen

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.

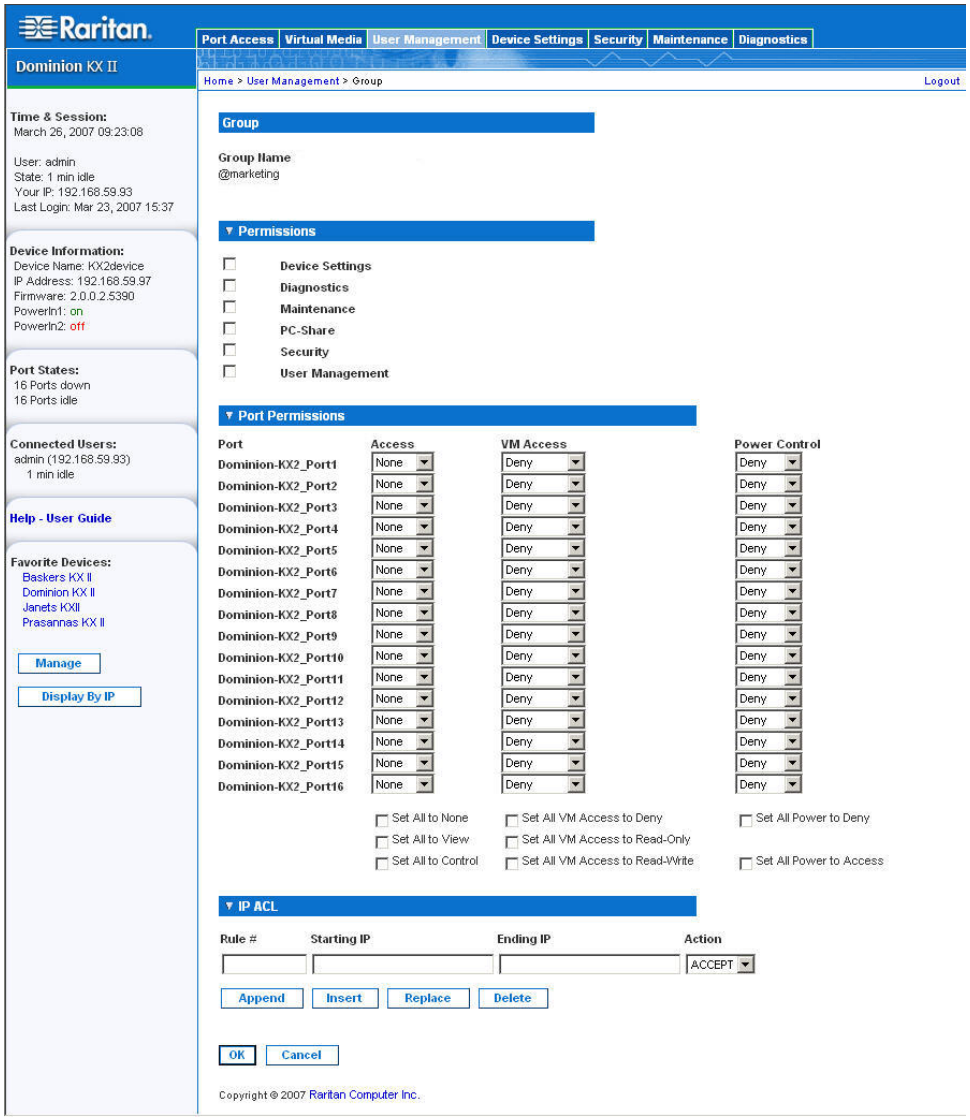

Abbildung 50: Ändern einer Gruppe

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. Weitere Informationen finden Sie unter Festlegen von Berechtigungen.
3. Legen Sie unter **Port Permissions** (Portberechtigungen) die Portberechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Serverports fest, und geben Sie den Zugriffstyp an. Weitere Informationen finden Sie unter Festlegen von Portberechtigungen.
4. Legen Sie die IP-ACL fest (optional). Mit diesem Feature beschränken Sie den Zugriff auf das Dominion KX II-Gerät, indem Sie IP-Adressen angeben. Weitere Informationen finden Sie unter Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste).
5. Klicken Sie auf **OK** (Senden).

Festlegen von Berechtigungen für individuelle Gruppen

So legen Sie Berechtigungen für eine individuelle Benutzergruppe fest:

1. Wählen Sie den gewünschten Benutzer 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** (Senden).

Ändern des Kennworts

So ändern Sie Ihr Kennwort:

1. Wählen Sie **User Management > Change Password** (Benutzerverwaltung > Kennwort ändern). Die Seite **Change Password** (Kennwort ändern) wird angezeigt.

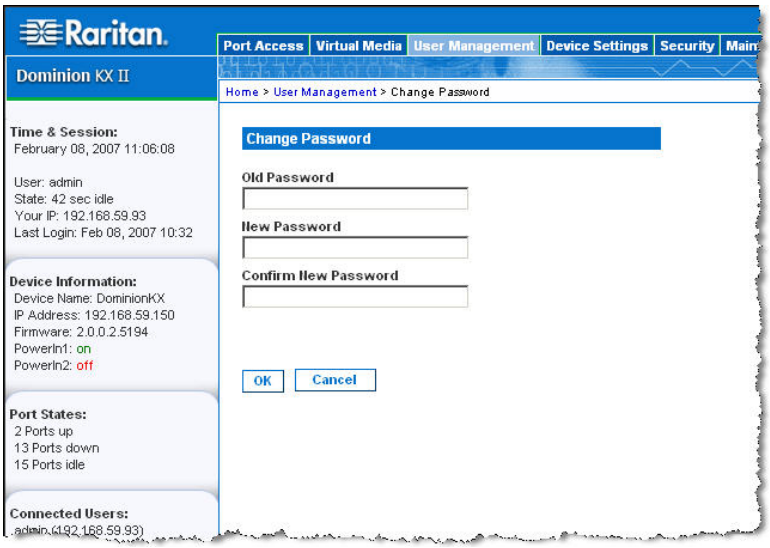

Abbildung 51: Ändern des Kennworts

2. Geben Sie in das Feld **Old Password** (Altes Kennwort) Ihr aktuelles Kennwort ein.
3. Geben Sie im Feld **New Password** (Neues Kennwort) das neue Kennwort ein, und geben Sie es 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** (Senden).
5. Die erfolgreiche Änderung des Kennworts wird bestätigt. Klicken Sie auf **OK** (Senden).

Hinweis: *Wenn sichere Kennwörter verwendet werden müssen, enthält diese Seite Informationen zum erforderlichen Format. Weitere Informationen zu Kennwörtern und sicheren Kennwörtern finden Sie unter Sicherheitseinstellungen – Sichere Kennwörter.*

Authentication Settings (Authentifizierungseinstellungen)

Auf der Seite **Authentication Settings** (Authentifizierungseinstellungen) können Sie die Art der Authentifizierung für den Zugriff auf den Dominion KX II konfigurieren. Weitere Informationen zur Funktionsweise und zu den Unterschieden von Authentifizierung und Autorisierung finden Sie unter Authentifizierung im Vergleich zur Autorisierung.

Hinweis: *Auch wenn Sie eine Remoteauthentifizierung (LDAP oder RADIUS) wählen, kommt die lokale Authentifizierung zum Einsatz.*

So konfigurieren Sie die Authentifizierung:

1. Wählen Sie **User Management > Authentication Settings** (Benutzerverwaltung > Authentifizierungseinstellungen). Die Seite **Authentication Settings** (Authentifizierungseinstellungen) wird angezeigt.

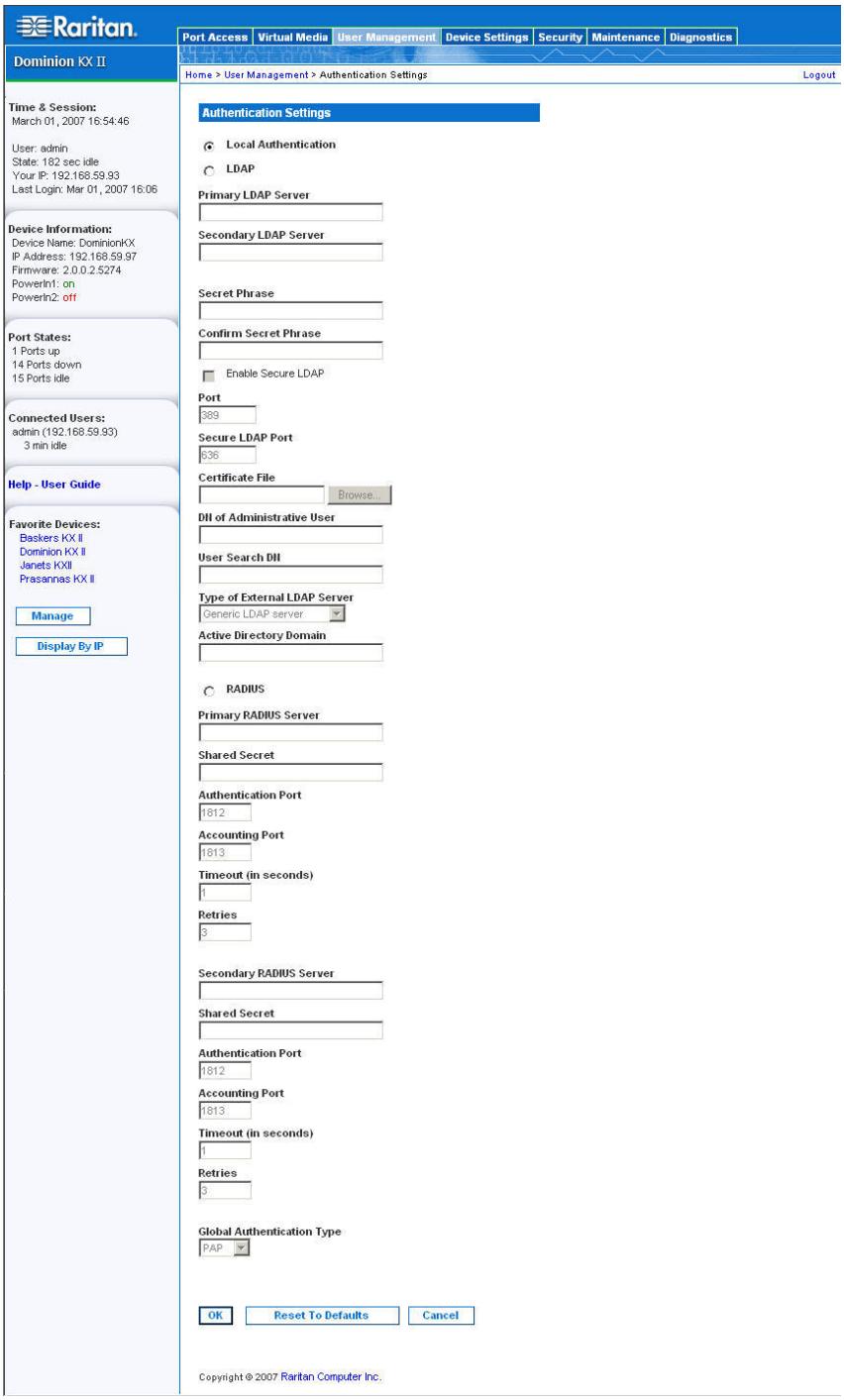

Abbildung 52: Authentication Settings (Authentifizierungseinstellungen)

2. Wählen Sie die Option für das gewünschte Authentifizierungsprotokoll aus. Zur Verfügung stehen **Local Authentication** (Lokale Authentifizierung), **LDAP** oder **RADIUS.** Bei der Option **LDAP** werden die restlichen LDAP-Felder aktiviert, bei der Option **RADIUS** die restlichen RADIUS-Felder.
3. Bei der Option **Local Authentication** (Lokale Authentifizierung) fahren Sie mit Schritt 6 fort.
4. Wenn Sie sich für LDAP entscheiden, lesen Sie den Abschnitt Implementierung der LDAP-Remoteauthentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Bereich **LDAP** der Seite **Authentication Settings** (Authentifizierungseinstellungen).
5. Wenn Sie sich für RADIUS entscheiden, lesen Sie den Abschnitt Implementierung der RADIUS-Remoteauthentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Bereich **RADIUS** der Seite **Authentication Settings** (Authentifizierungseinstellungen).
6. Klicken Sie abschließend auf **OK**, um die Konfiguration zu speichern.

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So kehren Sie zu den Werkseinstellungen zurück:

Klicken Sie auf die Schaltfläche **Reset to Defaults** (Auf Standardeinstellungen zurücksetzen).

Implementierung der LDAP-Remoteauthentifizierung

Lightweight Directory Access Protocol (LDAP) 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-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-Authentifizierungsserver.

Geben Sie für die Verwendung des LDAP-Authentifizierungsprotokolls folgende Informationen ein:

Abbildung 53: Authentifizierungseinstellungen (LDAP)

1. Geben Sie die IP-Adresse oder den DNS-Namen Ihres LDAP-Remoteauthentifizierungsservers im Feld **Primary LDAP Server** (Primärer LDAP-Server) ein. Wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist, muss der DNS-Name verwendet werden.
2. (Optional) Geben Sie die IP-Adresse oder den DNS-Namen Ihres LDAP-Servers zur Sicherung im Feld **Secondary LDAP Server** (Sekundärer LDAP-Server) ein. Wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist, muss der DNS-Name verwendet werden. Für die restlichen Felder gelten die gleichen Einstellungen wie unter **Primary LDAP Server** (Primärer LDAP-Server).
3. Geben Sie den geheimen Serverschlüssel (Kennwort), der für die Authentifizierung beim Remoteauthentifizierungsserver erforderlich ist, im Feld **Secret Phrase** (Geheimer Schlüssel) und ein zweites Mal im Feld **Confirm Secret Phrase** (Geheimen Schlüssel bestätigen) ein.
4. Aktivieren Sie das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren), wenn Sie SSL verwenden möchten. Das Feld **Secure LDAP Port** (Secure LDAP-Port) wird aktiviert. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, über das Dominion KX II sicher mit dem LDAP-Server kommunizieren kann.
5. Der Standardport lautet 389. Verwenden Sie entweder den Standard-TCP-Port für LDAP, oder legen Sie einen anderen Port fest.

6. Der standardmäßige Secure LDAP-Port ist Port 636. Verwenden Sie entweder den Standardport, oder legen Sie einen anderen Port fest. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist.
7. **Certificate File** (Zertifikatdatei): Fragen Sie den Administrator des Authentifizierungsservers nach der CA-Zertifikatdatei im Base64-codierten X-509-Format für den LDAP-Server. Navigieren Sie über die Schaltfläche **Browse** (Durchsuchen) zur entsprechenden Zertifikatdatei. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist.
8. **DN of administrative User** (DN des Administratorbenutzers): Distinguished Name (DN) des Administratorbenutzers. Fragen Sie den Administrator des Authentifizierungsservers nach den Werten, die in dieses Feld eingegeben werden müssen. Ein Wert für **DN of administrative User** könnte wie folgt aussehen: „cn=Administrator,dc=Benutzer=, dc=testradius,dc=com“.
9. **User Search DN (DN für Benutzersuche):** Bezeichnung des mit LDAP verbundenen Namens und des Anfangspunkts der Suche nach dem angegebenen Basis-DN in der Datenbank. Ein Beispiel für einen Basissuchwert ist: „cn=“Benutzer,dc=raritan,dc=com“. Fragen Sie an den Administrator des Authentifizierungsservers nach den korrekten Werten für diese Felder.
10. **Type of external LDAP server** (Typ des externen LDAP-Servers): Wählen Sie eine der folgenden Optionen:
    - **Generic LDAP Server** (Generischer LDAP-Server)
    - **Microsoft Active Directory**: Microsoft hat die LDAP-Verzeichnisdienste in Active Directory für die Verwendung in Windows-Umgebungen implementiert.
11. **Active Directory Domain** (Active Directory-Domäne): Geben Sie den Namen der Active Directory-Domäne ein.

Rückgabe von Benutzergruppeninformationen von Active Directory Server

Der Dominion KX II unterstützt die Benutzerauthentifizierung zu Active Directory (AD), ohne dass Benutzer lokal im Dominion KX II definiert sein müssen. Dies ermöglicht, die Active Directory-Benutzerkonten und -Kennwörter *ausschließlich* auf dem Active Directory-Server zu verwalten. Die Autorisierungs- und Active Directory-Benutzerrechte werden mit standardmäßigen KX II-Richtlinien und Benutzergruppenrechten, die lokal auf importierte Active Directory-Benutzergruppen angewendet werden, gesteuert und verwaltet.

Hinweis: *Wenn Sie bereits Kunde von Raritan, Inc. sind und den Active Directory-Server bereits durch Ändern des Active Directory-Schemas konfiguriert haben, unterstützt der Dominion KX II diese Konfiguration nach wie vor, und Sie müssen den folgenden Vorgang nicht durchführen. Informationen zur Aktualisierung des Active Directory-LDAP-Schemas finden Sie in* *Anhang B: Aktualisieren des LDAP-Schemas**.*

So aktivieren Sie den AD-Server am Dominion KX II:

1. Erstellen Sie am Dominion KX II besondere Gruppen, und weisen Sie ihnen geeignete Berechtigungen zu. Erstellen Sie z. B. Gruppen wie: KVM_Admin, 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 erstellten Gruppen auf dem AD-Server den Benutzern zu, die den Dominion KX II verwenden werden.
4. Aktivieren und konfigurieren Sie den AD-Server am Dominion KX II. Weitere Informationen finden Sie unter Implementierung der LDAP-Remoteauthentifizierung.

Wichtige Hinweise:

- Bei der Eingabe des Gruppennamens muss die Groß-/Kleinschreibung beachtet werden.
- Der Dominion KX II bietet folgende Standardgruppen, die nicht geändert oder gelöscht werden können: Admin und <Unknown> (Unbekannt). Stellen Sie sicher, dass diese Gruppennamen nicht vom Active Directory-Server verwendet werden.
- Wenn die vom Active Directory-Server zurückgegebenen Gruppeninformationen nicht mit einer KX II-Gruppenkonfiguration übereinstimmen, weist der Dominion KX II den Benutzern, die sich erfolgreich authentifizieren, automatisch die Gruppe <Unknown> (Unbekannt) zu.

Implementierung der RADIUS-Remoteauthentifizierung

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

So verwenden Sie das RADIUS-Authentifizierungsprotokoll:

Abbildung 54: Authentifizierungseinstellungen (RADIUS)

1. Geben Sie die IP-Adresse des primären und (optional) des sekundären Remoteauthentifizierungsservers in die Felder **Primary Radius Server** (Primärer RADIUS-Server) und **Secondary Radius Server** (Sekundärer RADIUS-Server) ein.
2. Geben Sie den geheimen Serverschlüssel für die Authentifizierung in die Felder unter **Shared Secret** (Gemeinsamer geheimer Schlüssel) ein. Der gemeinsame geheime Schlüssel ist eine Zeichenfolge, die dem Dominion KX II und dem RADIUS-Server bekannt sein muss, damit diese sicher kommunizieren können. Es handelt sich dabei praktisch um ein Kennwort.
3. **Authentication Port** (Authentifizierungsport): Der Standardauthentifizierungsport lautet 1812. Sie können ihn bei Bedarf ändern.
4. **Accounting Port** (Kontoführungsport): Der Standardkontoführungsport lautet 1813. Sie können ihn bei Bedarf ändern.
5. **Timeout (in seconds)** (Zeitlimit [in Sekunden]): Das Standardzeitlimit beträgt eine Sekunde. Sie können es bei Bedarf ändern. Das Zeitlimit bezeichnet die Zeitspanne, während der der Dominion KX II auf eine Antwort vom RADIUS-Server wartet, ehe er eine weitere Authentifizierungsanforderung sendet.

6. **Retries** (Erneute Versuche): Standardmäßig beträgt die Anzahl der erneuten Versuche 3. Sie können sie bei Bedarf ändern. Dieser Wert gibt an, wie oft der Dominion KX II eine Authentifizierungsanforderung an den RADIUS-Server sendet.
7. **Global Authentication Type** (Globaler Authentifizierungstyp): Wählen Sie eine Option aus der Dropdownliste:
   - **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.

Zurückgeben von Benutzergruppeninformationen über RADIUS

Wenn ein RADIUS-Authentifizierungsversuch erfolgreich ist, bestimmt das Dominion KX II-Gerät 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 werden:

```
Raritan:G{GROUP_NAME}
```

Dabei ist *GRUPPENNAME* eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört.

Spezifikationen für den RADIUS-Kommunikationsaustausch

Die Dominion KX II-Einheit sendet die folgenden RADIUS-Attribute an Ihren RADIUS-Server:

ATTRIBUT	DATEN
ANMELDUNG	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-IP-Address (4)	Die IP-Adresse der Dominion KX II-Einheit.
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) – Startet die Kontoführung.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse der Dominion KX II-Einheit.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.
ABMELDUNG	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) – Beendet die Kontoführung.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse der Dominion KX II-Einheit.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.

Kapitel 9: Geräteverwaltung

Das Menü **Device Settings** (Geräteeinstellungen) umfasst folgende Optionen: **Network** (Netzwerk), **Date/Time** (Datum/Uhrzeit), **Event Management** (Ereignisverwaltung) (**Settings** [Einstellungen] und **Destinations** [Ziele]), **Power Supply Setup** (Netzteilkonfiguration), **Port Configuration** (Portkonfiguration) und **Local Port Settings** (Lokale Porteinstellungen) (nur lokale Dominion KX II-Konsole).

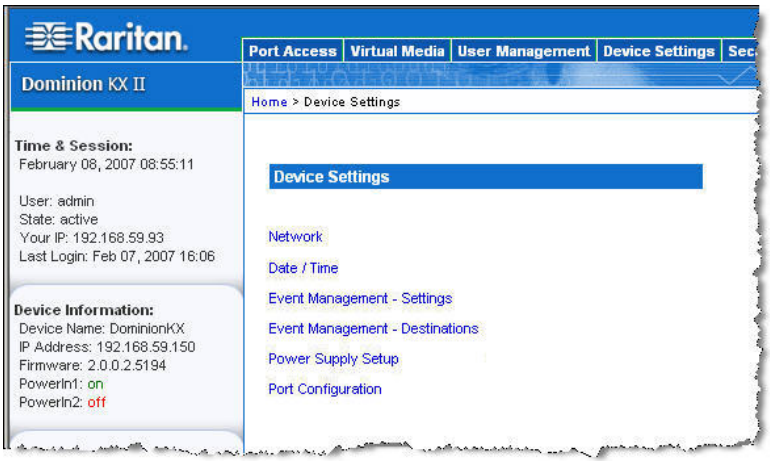

*Abbildung 55: Menü **Device Settings** (Geräteeinstellungen)*

OPTION	AN:
Netzwerk	Anpassen der Netzwerkkonfiguration für den Dominion KX II
Date/Time (Datum/Uhrzeit)	Festlegen von Datum, Uhrzeit, Zeitzone und Network Time Protocol (NTP)
Event Management – Settings (Ereignisverwaltung – Einstellungen)	Konfigurieren von SNMP und Syslog
Event Management – Destinations (Ereignisverwaltung – Ziele)	Auswählen, welche Systemereignisse verfolgt und wohin die Informationen gesendet werden sollen
Power Supply Setup (Netzteilkonfiguration)	Konfigurieren der automatischen Erkennung der Netzteile für den Dominion KX II
Port Configuration (Portkonfiguration)	Konfigurieren von KVM-Ports, CIMs und der Ausgänge
Lokale Porteinstellungen	Konfigurieren des lokalen Ports *(nur lokale Dominion KX II-Konsole)*

Netzwerkeinstellungen

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

Wichtig: Der Dominion KX II muss neu gestartet werden, damit die Netzwerkeinstellungen wirksam werden. Stellen Sie vor dem Ändern der Netzwerkkonfiguration sicher, dass keine weiteren aktiven Verbindungen zum Gerät bestehen, da beim Neustart der KX II-Einheit sämtliche Verbindungen getrennt werden.

Für das Einrichten der IP-Konfiguration gibt es zwei Möglichkeiten:

- Sie benötigen keine Software. Diese Option wird empfohlen (**Static IP** [Statisches IP]). Da der Dominion KX II Teil Ihrer Netzwerkinfrastruktur ist, möchten Sie wahrscheinlich, dass die Adresse möglichst konstant bleibt. Bei dieser Option können Sie die Netzwerkparameter selbst einrichten.
- **DHCP**: Die IP-Adresse wird automatisch von einem DHCP-Server zugewiesen.

So ändern Sie die Netzwerkkonfiguration:

1. Wählen Sie **Device Settings > Network** (Geräteeinstellungen > Netzwerk). Das Menü Network Settings (Netzwerkeinstellungen) wird angezeigt.

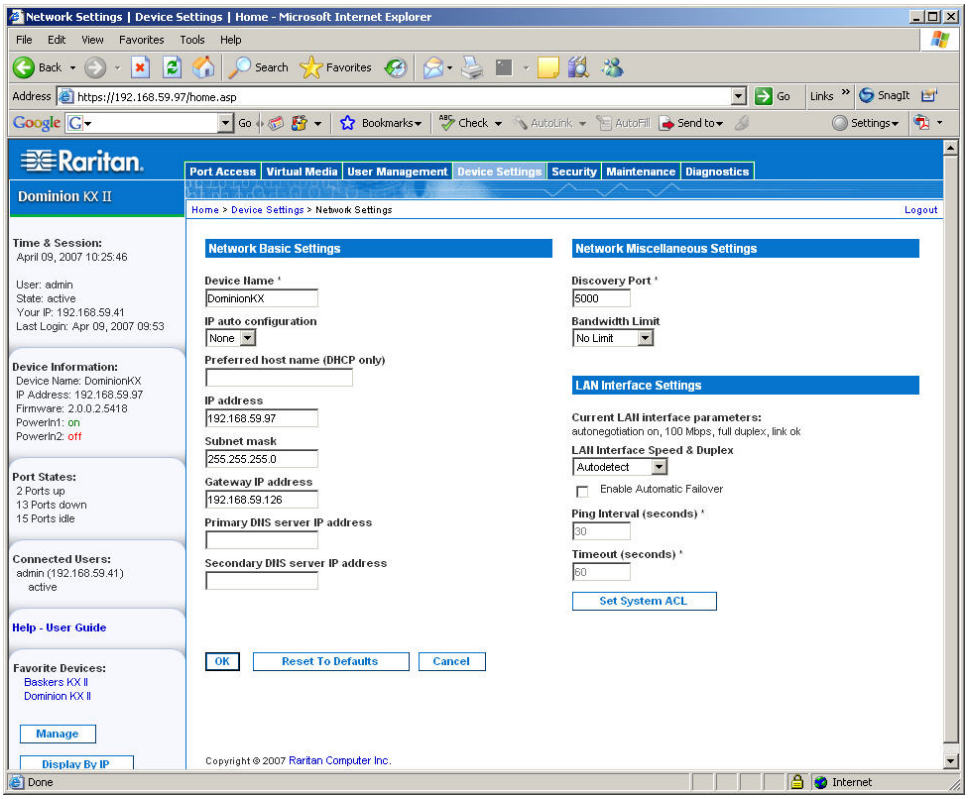

Abbildung 56: Netzwerkeinstellungen

2. Aktualisieren Sie die Basisnetzwerkeinstellungen unter **Network Basic Settings**. Weitere Informationen zu den einzelnen Feldern finden Sie unter Basisnetzwerkeinstellungen.
3. Aktualisieren Sie die verschiedenen Netzwerkeinstellungen unter **Network Miscellaneous Settings**. Weitere Informationen zu den einzelnen Feldern finden Sie unter Verschiedene Netzwerkeinstellungen.

4. Aktualisieren Sie die LAN-Schnittstelleneinstellungen unter **LAN Interface Settings**. Weitere Informationen zu den einzelnen Feldern finden Sie unter LAN-Schnittstelleneinstellungen.
5. Klicken Sie auf **OK**, um die Konfiguration festzulegen. Ist für die vorgenommenen Änderungen ein Neustart des Geräts erforderlich, wird eine entsprechende Meldung angezeigt.

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So kehren Sie zu den Werkseinstellungen zurück:

Klicken Sie auf **Reset to Defaults** (Auf Standardeinstellungen zurücksetzen).

Basisnetzwerkeinstellungen

Abbildung 57: Netzwerkeinstellungen (Basisnetzwerkeinstellungen)

- **Device Name (Gerätename):** Geben Sie einen eindeutigen Namen für das Gerät ein (maximal 16 Zeichen, keine Leerzeichen). Sie sollten das Gerät leicht an seinem Namen erkennen können. Der Standardname für eine Dominion KX II-Einheit lautet **DominionKX**. Auch Remotebenutzern wird dieser Name angezeigt. Hat jedoch ein MPC-Benutzer ein Verbindungsprofil für dieses Gerät erstellt, sieht dieser Benutzer das Feld **Description** (Beschreibung) aus dem Profil.
- **IP auto configuration** (Automatische IP-Konfiguration): Wählen Sie eine Option aus der Dropdownliste:
  - Sie benötigen keine Software. Wählen Sie diese Option, wenn Sie keine automatische IP-Konfiguration möchten, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

    *Wenn Sie diese Option unter **IP auto configuration** (Automatische IP-Konfiguration) gewählt haben, werden die folgenden Felder aktiviert, in denen Sie die IP-Konfiguration manuell vornehmen können.*

    - **IP Address** (IP-Adresse): Die Standard-IP-Adresse lautet **192.168.0.192**.
    - **Subnet Mask** (Subnetzmaske): Die Standardsubnetzmaske lautet **255.255.255.0**.

- **Gateway IP Address** (Gateway-IP-Adresse): Die IP-Adresse des Gateways (falls eines verwendet wird).
- **Primary DNS Server IP Address** (IP-Adresse des primären DNS-Servers): Der primäre DNS-Server zur Übertragung von Namen in IP-Adressen.
- **Secondary DNS-Server IP Address** (IP-Adresse des sekundären DNS-Servers): Der sekundäre DNS-Server zur Übertragung von Namen in IP-Adressen (falls ein solcher verwendet wird).

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

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

Verschiedene Netzwerkeinstellungen

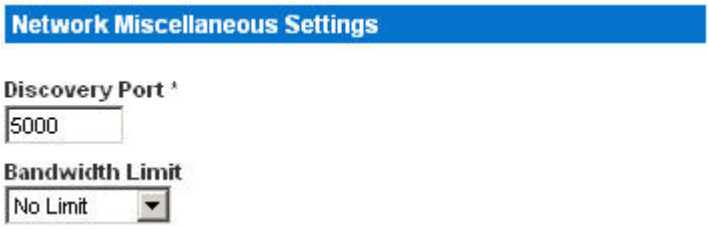

Abbildung 58: Netzwerkeinstellungen (Verschiedene Netzwerkeinstellungen)

- **Discovery Port** (Erkennungsport): Die Dominion KX II-Erkennung erfolgt über einen einzelnen konfigurierbaren TCP-Port. Der Standardport lautet 5000, aber Sie können die Konfiguration ändern und jeden anderen TCP-Port *außer* 80 und 443 verwenden. Wenn Sie über eine Firewall auf die KX II-Einheit zugreifen möchten, müssen die Firewalleinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht standardmäßigen konfigurierten Port zulassen. Weitere Informationen finden Sie unter Konfigurieren der Einstellungen für die Netzwerkfirewall.
- **Bandwidth Limit** (Maximale Bandbreite): Standardmäßig gibt es keine Beschränkung. Wählen Sie eine Option aus der Dropdownliste, um für alle Sitzungen die maximale Bandbreite festzulegen, die dieser Dominion KX II-Einheit zur Verfügung steht. Folgende Optionen stehen zur Verfügung: *No Limit* (Keine Beschränkung), *100 Megabit*, *10 Megabit*, *5 Megabit*, *2 Megabit*, *512 Kilobit*, *256 Kilobit* und *128 Kilobit*.

Hinweis: *Eine geringere Bandbreite kann eine schlechtere Leistung zur Folge haben.*

LAN-Schnittstelleneinstellungen

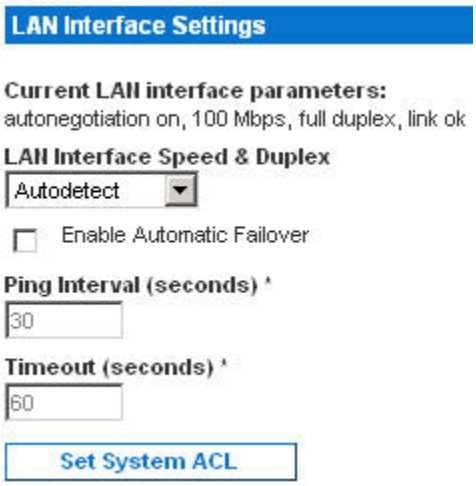

Abbildung 59: Netzwerkeinstellungen (LAN-Schnittstelleneinstellungen)

- Die aktuellen Parametereinstellungen sehen Sie im Feld **Current LAN interface parameters** (Aktuelle LAN-Schnittstellenparameter).
- **LAN Interface Speed & Duplex** (LAN-Schnittstellengeschwindigkeit & Duplex): Wählen Sie eine der verfügbaren Geschwindigkeits- und Duplexkombinationen aus.

Autodetect (Automatische Erkennung)	*Standardoption*
10 Mbps/Half (10 Mbit/s/Halb)	
10 Mbps/Full (10 Mbit/s/Voll)	
100 Mbps/Half (100 Mbit/s/Halb)	
100 Mbps/Full (100 Mbit/s/Voll)	
1000 Mbps/Full (1000 Mbit/s/Voll)	*Gigabit*

  - **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 Duplexoption.*

- **Enable automatic failover (Automatisches Failover aktivieren):** Aktivieren Sie dieses Kontrollkästchen, um zu veranlassen, dass der Dominion KX II die Netzwerkverbindung automatisch mithilfe eines zweiten Netzwerkports wiederherstellt, wenn der aktive Netzwerkport ausfällt. Wenn dieses Kontrollkästchen aktiviert ist, stehen die folgenden beiden Felder zur Verfügung:
  - **Ping Interval (seconds)** (Pingintervall [Sekunden]): Damit legen Sie fest, wie oft der Dominion KX II den Status der Netzwerkverbindung überprüft (ein zu niedrig eingestellter Wert kann unnötigen Netzwerkdatenverkehr verursachen). Das Standardpingintervall beträgt 30 Sekunden.
  - **Timeout (seconds)** (Zeitlimit [Sekunden]): **Timeout bestimmt, wie lange ein Netzwerkport nicht** verfügbar sein muss, bevor der Wechsel ausgeführt wird. **Automatic Failover** (Automatisches Failover) funktioniert nur, wenn beide Netzwerkports mit dem Netzwerk verbunden sind und diese Option aktiviert ist. Das Standardzeitlimit beträgt 60 Sekunden.

Hinweis: *Von Standardpingintervall und Zeitlimit wird eine Bedingung erzeugt, bei deren Eintreten die Remotesitzungen getrennt werden und neu hergestellt werden müssen, wenn das KX-Gerät umzuschalten versucht. Eine Reduzierung dieser Intervalle auf wesentlich geringere Werte ermöglicht den Remotesitzungen zwar das Aufrechterhalten der Verbindung, hat aber auch ein erhöhtes Netzwerkverkehrsaufkommen zur Folge.*

- **Set System ACL** (System-ACL festlegen): Klicken Sie auf diese Schaltfläche, um eine globale Zugriffssteuerungsliste für die Dominion KX II-Einheit festzulegen. Damit wird sichergestellt, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet. Die Seite IP Access Control (IP-Zugriffssteuerung) wird angezeigt.

Hinweis: *Diese ACL-Werte sind global und betreffen die gesamte Dominion KX II-Einheit. Sie können ACLs auch auf Gruppenebene erstellen. Erstellen Sie beispielsweise die Benutzergruppe „Externe Lieferanten“, die nur über einen bestimmten IP-Adressbereich auf den Dominion KX II zugreifen kann. (Weitere Informationen zum Erstellen gruppenspezifischer Zugriffssteuerungslisten finden Sie unter Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)).*

Date/Time Settings (Datum-/Uhrzeiteinstellungen)

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

- Stellen Sie das Datum und die Uhrzeit manuell ein, oder
- Führen Sie eine Synchronisation mit einem NTP (Network Time Protocol)-Server durch.

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.

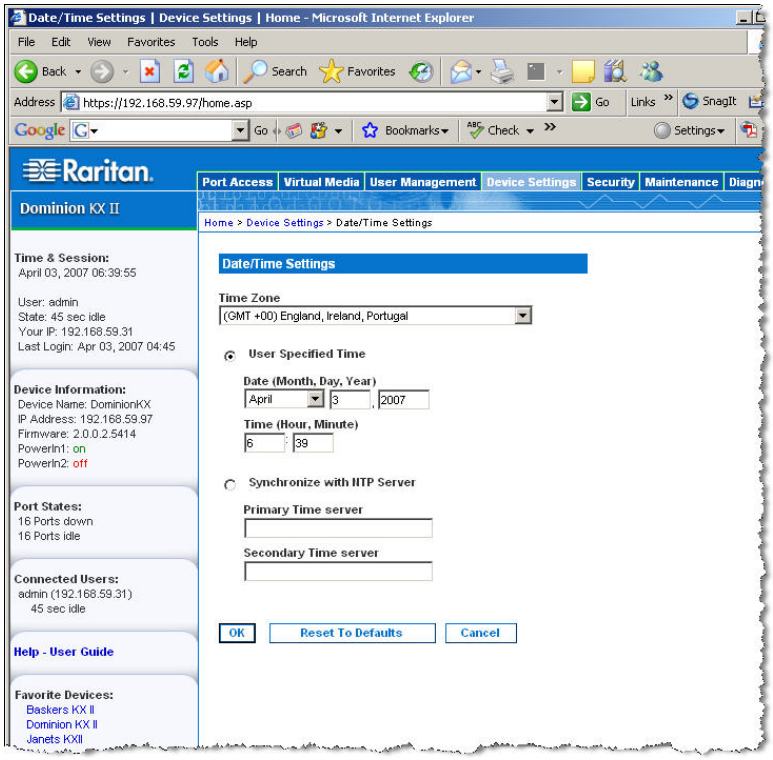

Abbildung 60: Date/Time Settings (Datum-/Uhrzeiteinstellungen)

2. Wählen Sie in der Dropdownliste **Time Zone** *Ihre Zeitzone* aus.
3. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:
   - **User Specified Time** (Benutzerdefinierte Zeit): Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben.
   - **Synchronize with NTP Server** (Mit NTP-Server synchronisieren): Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
4. Falls Sie die Option **User Specified Time** (Benutzerdefinierte Zeit) gewählt haben, geben Sie Datum und Uhrzeit wie folgt ein:
   a. Wählen Sie in der Dropdownliste **Month** den Monat aus.
   b. Geben Sie im Feld **Day** den Tag ein.
   c. Geben Sie im Feld **Year** das Jahr im Format JJJJ ein.
   d. Geben Sie im Feld **Time** die Uhrzeit im Format hh:mm ein. (Verwenden Sie das 24-h-Zeitformat.)

5. Falls Sie die Option **Synchronize with NTP Server** (Mit NTP-Server synchronisieren) gewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld **Primary Time server** (Primärer Zeitserver) die IP-Adresse dieses Servers ein.
   b. (Optional) Geben Sie im Feld **Secondary Time server** (Sekundärer Zeitserver) die entsprechende IP-Adresse ein.
6. Klicken Sie auf **OK** (Senden).

Ereignisverwaltung

Das Dominion KX II-Feature zur Ereignisverwaltung bietet eine Reihe von Fenstern, in denen Sie die Verteilung von Systemereignissen auf SNMP-Manager, Syslog und das Prüfprotokoll aktivieren und deaktivieren können. Die Ereignisse werden kategorisiert, und Sie können für jedes Ereignis festlegen, ob es an eines oder mehrere Ziele gesendet werden soll.

Event Management – Settings (Ereignisverwaltung – Einstellungen)

SNMP-Konfiguration

Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung und die Überwachung von Netzwerkgeräten und ihrer Funktionen. Der Dominion KX II bietet mittels der Ereignisverwaltung Unterstützung für SNMP-Agenten. Weitere Informationen zu SNMP-Agenten und -Traps finden Sie unter Konfigurieren des SNMP-Agenten und SNMP-Trap-Konfiguration.

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.

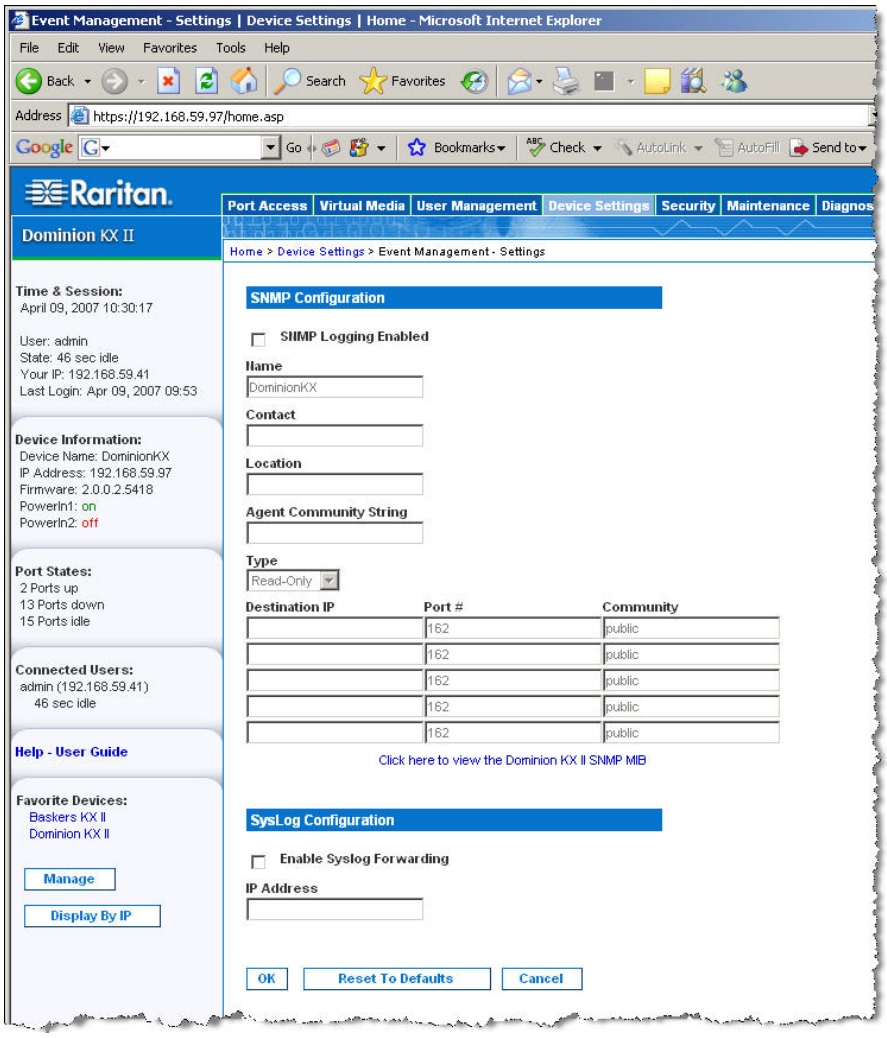

Abbildung 61: Event Management – Settings (Ereignisverwaltung – Einstellungen)

2. Aktivieren Sie das Kontrollkästchen **Enable SNMP Logging** (SNMP-Protokollierung aktivieren), um Zugriff auf die restlichen SNMP-Felder zu erhalten.

3. Geben Sie in die Felder **Name**, **Contact** (Kontakt) und **Location** (Ort) den Namen des SNMP-Agenten (dieser Dominion-Einheit), wie er in der KX II-Konsolenoberfläche angezeigt wird, einen Kontaktnamen für diese Einheit und den physischen Ort der Dominion-Einheit ein.
4. Geben Sie im Feld **Agent Community String** (Communityzeichenfolge des Agenten) die Zeichenfolge der Dominion-Einheit ein. Eine SNMP-Community ist die Gruppe, der Geräte und Verwaltungsstationen, auf denen SNMP ausgeführt wird, angehören. Damit können Sie festlegen, wohin Informationen gesendet werden. Der Communityname dient dazu, die Gruppe zu kennzeichnen. Ein SNMP-Gerät oder -Agent kann mehreren SNMP-Communitys angehören.
5. Legen Sie über die Dropdownliste **Type** (Typ) Lesezugriff (Read-Only) oder Lese-/Schreibzugriff (*Read-Write*) für die Community fest.
6. Konfigurieren Sie maximal fünf SNMP-Manager, indem Sie entsprechende Werte in die Felder **Destination IP** (IP-Zieladresse), **Port #** (Portnummer) und **Community** eingeben.
7. Klicken Sie auf den Link **Click here to view the Dominion-KX2 SNMP MIB** (Klicken Sie hier, um die Dominion-KX2 SNMP MIB anzuzeigen), um auf die SNMP Management Information Base zuzugreifen.
8. Klicken Sie auf **OK** (Senden).

Syslog-Konfiguration

Abbildung 62: Syslog-Konfiguration

So konfigurieren Sie Syslog und aktivieren die Weiterleitung:

1. Aktivieren Sie das Kontrollkästchen **Enable Syslog Forwarding** (Syslogweiterleitung aktivieren), um Geräte-Protokollmeldungen an einen Remote-Syslog-Server zu senden.
2. Geben Sie die IP-Adresse Ihres Syslog-Servers im Feld **IP Address** ein.
3. Klicken Sie auf **OK** (Senden).

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So kehren Sie zu den Werkseinstellungen zurück:

Klicken Sie auf die Schaltfläche **Reset To Defaults** (Auf Standardeinstellungen zurücksetzen).

Event Management – Destinations (Ereignisverwaltung – Ziele)

Systemereignisse können (falls aktiviert) SNMP-Benachrichtigungsereignisse (Traps) generieren oder 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 generiert, wenn das Kontrollkästchen* ***SNMP Logging Enabled*** *(SNMP-Protokollierung aktiviert) aktiviert ist. Syslog-Ereignisse werden nur generiert, wenn das Kontrollkästchen* ***Enable Syslog Forwarding*** *(Syslogweiterleitung aktivieren) aktiviert ist. Beide Optionen befinden sich auf der Seite Event Management – Settings (Ereignisverwaltung – Einstellungen).*

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.

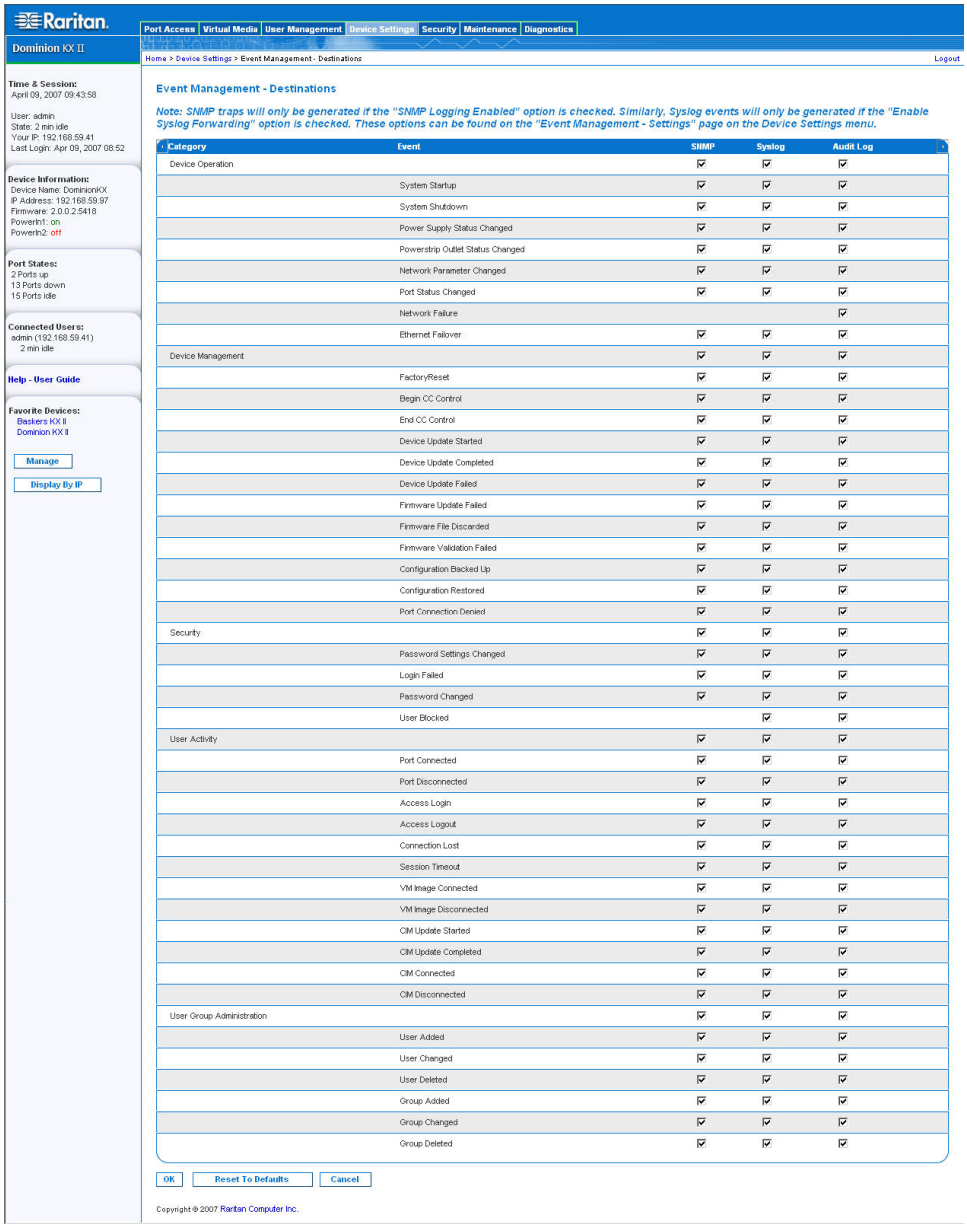

Abbildung 63: ***Event Management – Destinations*** *(Ereignisverwaltung – Ziele)*

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** (Senden).

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So kehren Sie zu den Werkseinstellungen zurück:

Klicken Sie auf die Schaltfläche **Reset To Defaults** (Auf Standardeinstellungen zurücksetzen).

Konfigurieren des 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. Auf der Seite **Event Logging** (Ereignisprotokollierung) können Sie die SNMP-Verbindung zwischen dem Dominion KX II (SNMP-Agent) und einem SNMP-Manager konfigurieren.

SNMP-Trap-Konfiguration

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 Dominion KX II.

TRAP-NAME	BESCHREIBUNG
cimConnected	Ein CIM wird am Dominion KX II-Port angeschlossen.
cimDisconnected	Ein CIM wird entweder vom Dominion KX II-Port getrennt oder ausgeschaltet.
cimUpdateCompleted	Die CIM-Firmwareaktualisierung ist abgeschlossen.
cimUpdateStarted	Die CIM-Firmwareaktualisierung wurde gestartet.
configBackup	Die Gerätekonfiguration wurde gesichert.
configRestore	Die Gerätekonfiguration wurde wiederhergestellt.
deviceUpdateFailed	Das Gerät konnte nicht aktualisiert werden.
deviceUpgradeCompleted	Der Dominion KX II hat die Aktualisierung mittels einer RFP-Datei abgeschlossen.
deviceUpgradeStarted	Der Dominion KX II hat die Aktualisierung mittels einer RFP-Datei begonnen.
ethernetFailover	Ein Ethernet-Failover wurde erkannt; die Wiederherstellung erfolgte auf einer neuen Ethernet-Schnittstelle.
factoryReset	Das Gerät wurde auf die Werkseinstellungen zurückgesetzt.
firmwareFileDiscarded	Die Firmwaredatei wurde verworfen.
firmwareUpdateFailed	Die Firmware konnte nicht aktualisiert werden.
firmwareValidationFailed	Die Firmware konnte nicht validiert werden.
groupAdded	Eine Gruppe wurde zum KX II-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.
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 des KX ist abgeschlossen.
rebootStarted	Der KX wird neu gestartet: entweder durch Wiederherstellen der Stromversorgung oder durch einen „Warmstart“ mittels des Betriebssystems.
securityViolation	Ein Sicherheitsproblem ist aufgetreten.
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 aufgetreten.
userDeleted	Ein Benutzerkonto wurde gelöscht.
userLogin	Ein Benutzer hat sich erfolgreich am KX II angemeldet und wurde authentifiziert.
userLogout	Ein Benutzer hat sich erfolgreich und ordnungsgemäß vom KX II 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.
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.

Seite Power Supply Setup (Netzteilkonfiguration)

Der Dominion KX II 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 der Dominion KX II 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 > Netzteilkonfiguration). Die Seite **Power Supply Setup** (Netzteilkonfiguration) wird angezeigt.

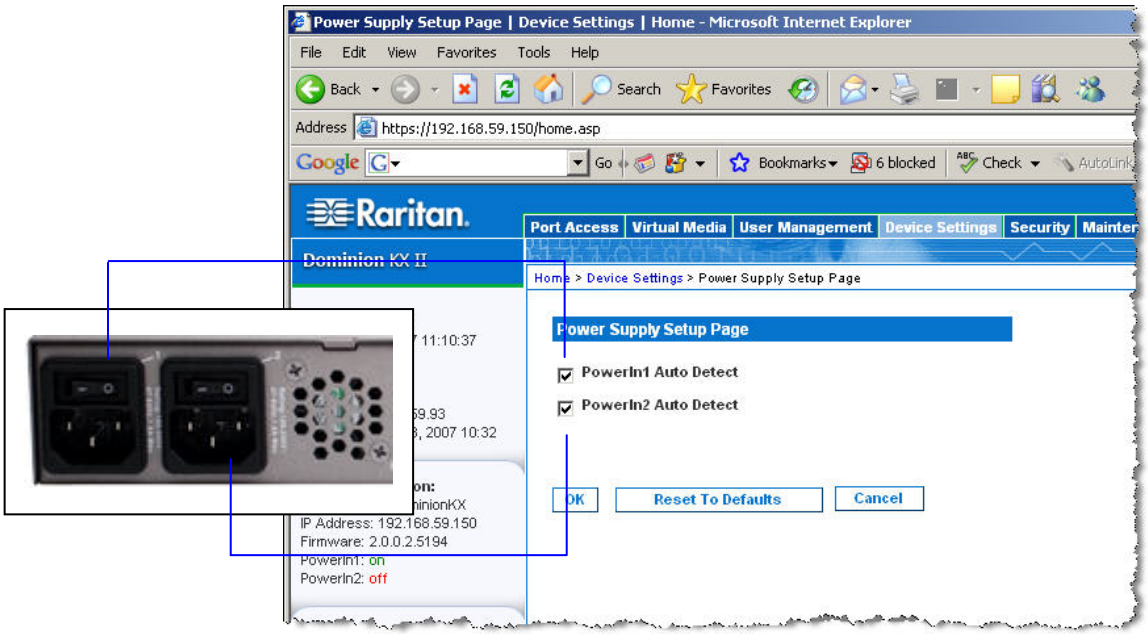

Abbildung 64: Power Supply Setup (Netzteilkonfiguration)

2. Wenn Sie den Strom über das Netzteil 1 zuführen (ganz links auf der Rückseite des Geräts), aktivieren Sie das Kontrollkästchen **PowerIn1 Auto Detect** (Netzteil 1 – Automatische Erkennung).
3. Wenn Sie den Strom über das Netzteil 2 zuführen (ganz rechts auf der Rückseite des Geräts), aktivieren Sie das Kontrollkästchen **PowerIn2 Auto Detect** (Netzteil 2 – Automatische Erkennung).
4. Klicken Sie auf **OK** (Senden).

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 kehren Sie zu den Werkseinstellungen zurück:

Klicken Sie auf die Schaltfläche **Reset To Defaults** (Auf Standardeinstellungen zurücksetzen).

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf die Schaltfläche **Cancel** (Abbrechen).

Hinweis: *Dominion KX II übermittelt den Status der Netzteile NICHT an CommandCenter. Dominion I (Generation 1) hingegen tut dies.*

Seite Port Configuration (Portkonfiguration)

Die Seite **Port Configuration** (Portkonfiguration) enthält eine Liste der Dominion KX II-Ports. Ports, die mit Zielservern oder Powerstrips verbunden sind, werden blau angezeigt und können bearbeitet werden. Ports, an die kein CIM angeschlossen oder für die kein CIM-Name angegeben ist, wird der Standardportname **Dominion-KX2_Port#** zugewiesen, wobei **Port#** für die Nummer des physischen Dominion KX II-Ports steht.

So ändern Sie eine Portkonfiguration:

1. Wählen Sie **Device Settings > Port Configuration** (Geräteeinstellungen > Portkonfiguration). Die Seite **Port Configuration** (Portkonfiguration) wird angezeigt.

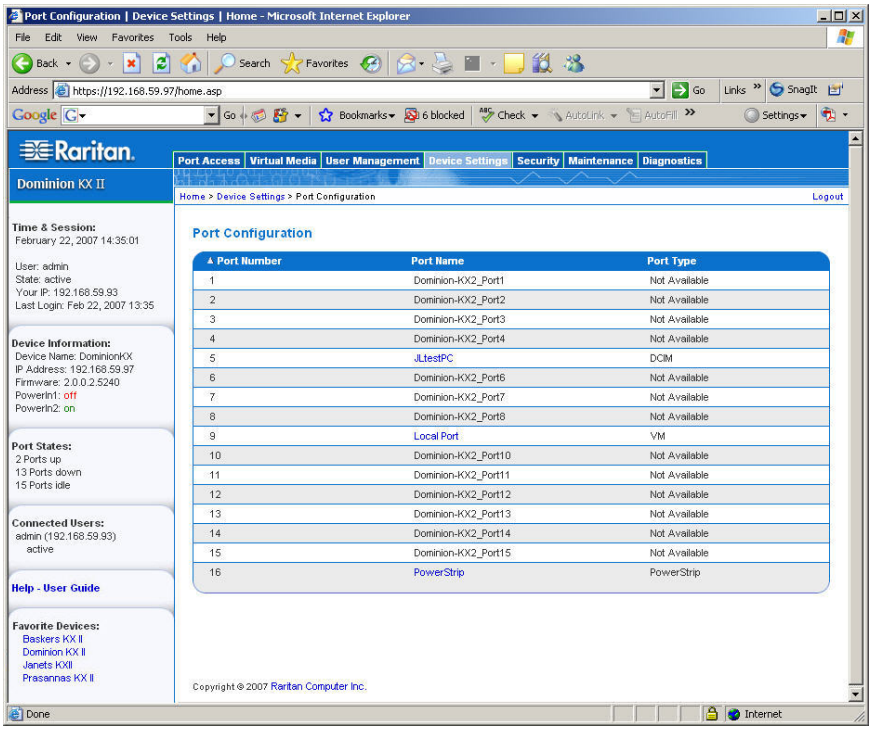

Abbildung 65: Port Configuration (Portkonfiguration)

Der Inhalt der Seite wird zunächst in der Reihenfolge der Portnummern angezeigt. Sie können für eine andere Sortierung jedoch auf eine der Spaltenüberschriften klicken.

- **Port Number** (Portnummer): Die für die Dominion KX II-Einheit verfügbaren Ports werden beginnend mit 1 durchnummeriert.
- **Port Name** (Portname): Der dem Port zugewiesene Name. Ein schwarzer Portname gibt an, dass Name und Port nicht geändert bzw. bearbeitet werden können. Blaue Portnamen können dagegen bearbeitet werden.
- **Port Type** (Porttyp): Der Typ des am Port angeschlossenen CIM.

BETRIEBSSYSTEMTYP	BESCHREIBUNG
DCIM	Dominion CIM
Not Available (Nicht verfügbar)	Kein CIM angeschlossen
PCIM	Paragon CIM
PowerStrip	Power CIM
VM	Virtual Media CIM (D2CIM-VUSB)

2. Klicken Sie auf den Portnamen des Ports, den Sie bearbeiten möchten.
   - Für KVM-Ports wird die Seite Port angezeigt. Auf dieser Seite können Sie die Ports benennen und Stromzuordnungen erstellen.
   - Für Powerstrips wird die Portseite für Powerstrips angezeigt. Auf dieser Seite können Sie die Powerstrips und ihre Ausgänge benennen.

Stromzufuhrsteuerung

Der Dominion KX II ermöglicht die Remotestromzufuhrsteuerung der Zielserver. Für dieses Feature benötigen Sie einen Remotepowerstrip von Raritan und das CIM D2CIM-PWR. Nachdem Sie Stromzuordnungen festgelegt haben, ist die Remotestromzufuhrverwaltung Ihrer Zielserver möglich.

So nutzen Sie das Feature für die Stromzufuhrsteuerung von Dominion KX II:

1. Anschließen des Powerstrips am Zielserver
2. Benennen des Powerstrips
3. Zuordnen von Ausgängen des Powerstrips zum Zielserver
4. Nutzen der Remote-Stromzufuhrverwaltung des Zielservers auf der Seite **Port Access** (Portzugriff)

Anschließen des Powerstrips

Die Zahlen in diesem Diagramm entsprechen den unten genannten Schritten.

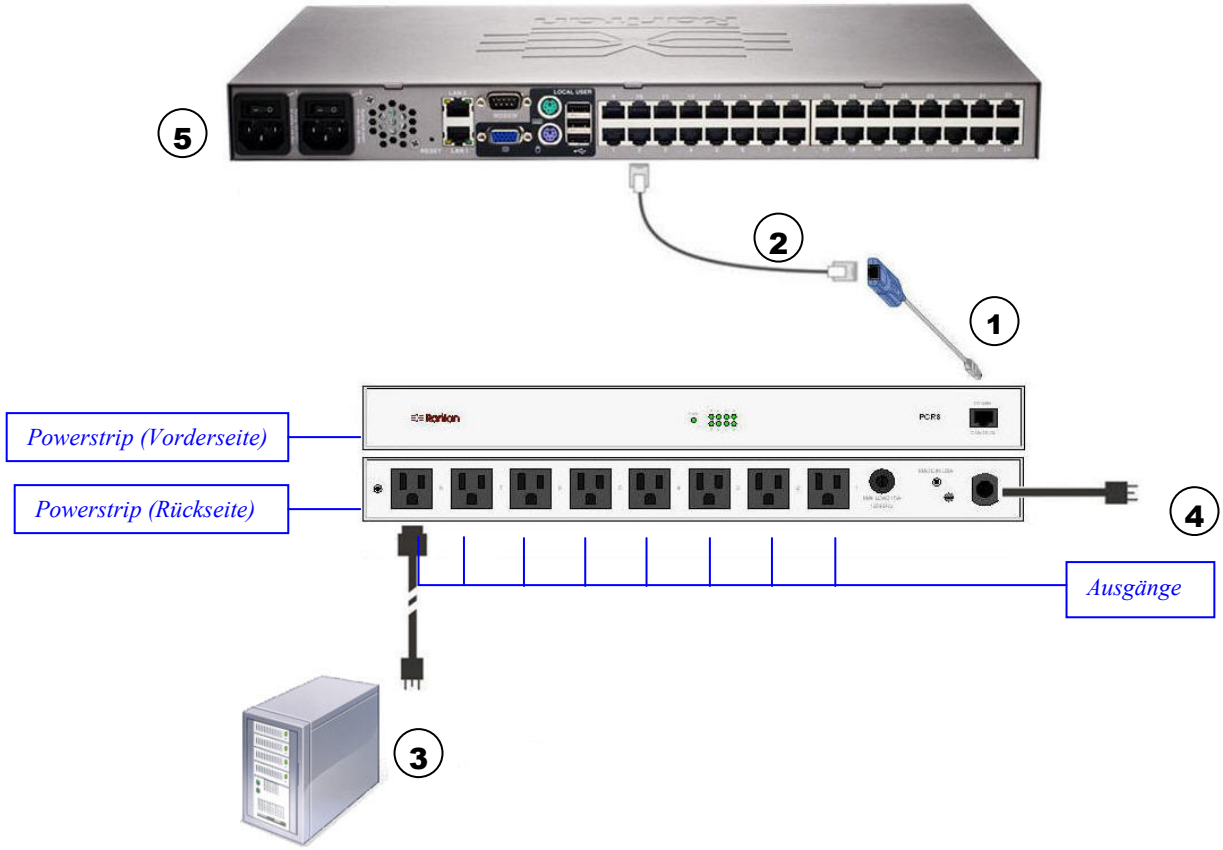

Abbildung 66: Powerstripanschlüsse

So schließen Sie den Powerstrip an:

1. Verbinden Sie den RJ-45-Stecker des D2CIM-PWR mit der RJ-45-Buchse des Powerstrips.
2. Verbinden Sie die RJ-45-Buchse des D2CIM-PWR mit einem der freien weiblichen Systemports des Dominion KX II mittels eines Straight-Through-Kabels der Kategorie 5.
3. Schließen Sie ein Netzkabel am Zielserver und einem verfügbaren Powerstripausgang an.
4. Stecken Sie den Stecker des Netzkabels in eine Steckdose.
5. Schalten Sie die Dominion KX II-Einheit ein.

Benennen des Powerstrips (Seite Port für Powerstrips)

Diese Portseite wird angezeigt, wenn Sie auf der Seite Port Configuration (Portkonfiguration) einen Port auswählen, der mit einem Remotepowerstrip von Raritan verbunden ist. Die Felder **Type** (Typ) und **Name** enthalten bereits Werte. Beachten Sie, dass der CIM-Typ *nicht* geändert werden kann. Die folgenden Informationen werden für jeden Ausgang des Powerstrips angezeigt: Ausgangsnummer, Name und Portzuordnung.

Auf dieser Seite können Sie den Powerstrip und seine Ausgänge benennen. Die Namen dürfen maximal 32 alphanumerische Zeichen sowie Sonderzeichen umfassen.

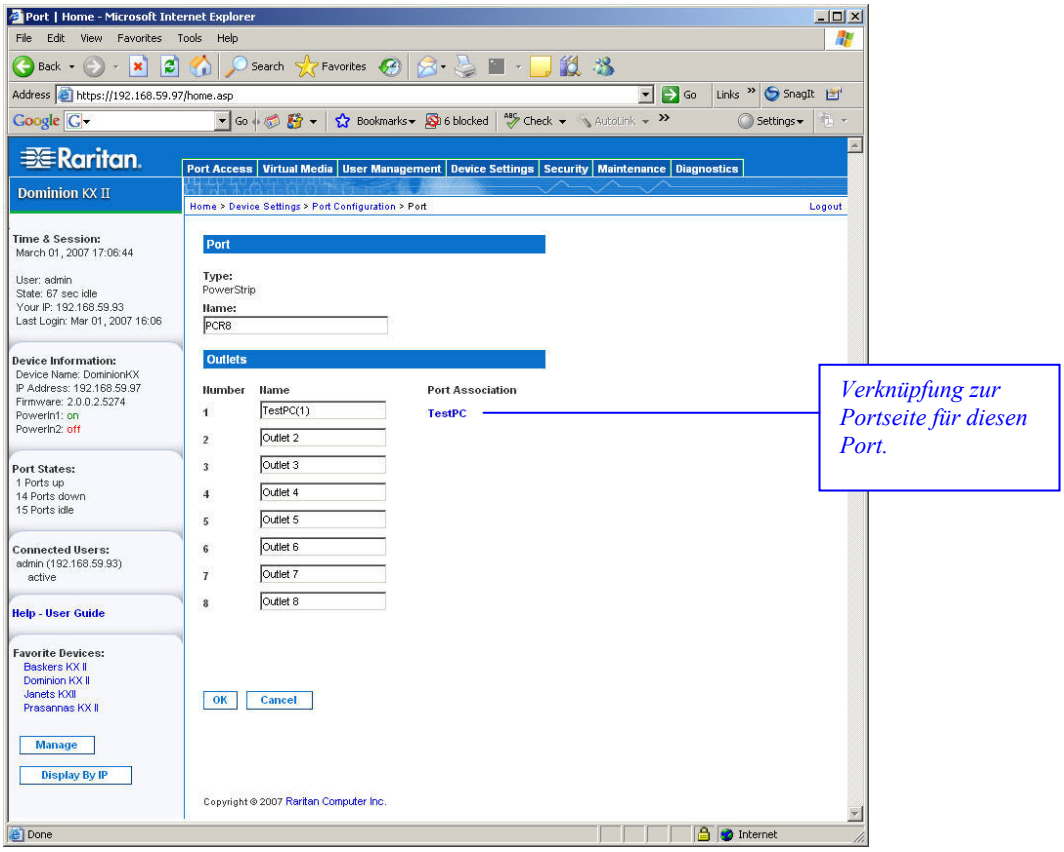

*Abbildung 67: Seite **Port** (Powerstrips)*

***Hinweis:** Wenn ein Powerstrip einem Zielserver (Port) zugeordnet ist, wird der Ausgangsname durch den Namen des Zielservers ersetzt.*

So benennen Sie den Powerstrip (und seine Ausgänge):

***Hinweis:** Das CommandCenter-Dienstgateway erkennt Powerstripnamen mit Leerzeichen nicht.*

1. Geben Sie dem Powerstrip einen Namen, den Sie sich gut merken können.
2. Ändern Sie ggf. den Namen unter **Outlet Name** (Ausgangsname). (Der Standardname ist **Outlet #**.)
3. Klicken Sie auf **OK** (Senden).

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf die Schaltfläche **Cancel** (Abbrechen).

Zuordnen von Zielservern zu Ausgängen (Seite Port)

Diese Portseite wird angezeigt, wenn Sie auf der Seite Port Configuration (Portkonfiguration) einen Port auswählen, der mit einem Zielserver verbunden ist. Auf dieser Seite können Sie Stromzuordnungen vornehmen, den Portnamen ändern und die Einstellungen der Zielserver aktualisieren, falls Sie mit dem CIM D2CIM-VUSB arbeiten. Die Felder **Type** (Typ) und **Name** enthalten bereits Werte. Beachten Sie, dass der CIM-Typ *nicht* geändert werden kann.

Ein Server kann maximal vier Netzschalter haben, und Sie können jedem einen anderen 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:

- Remotepowerstrip(s) von Raritan
- Power CIMs (D2CIM-PWR)

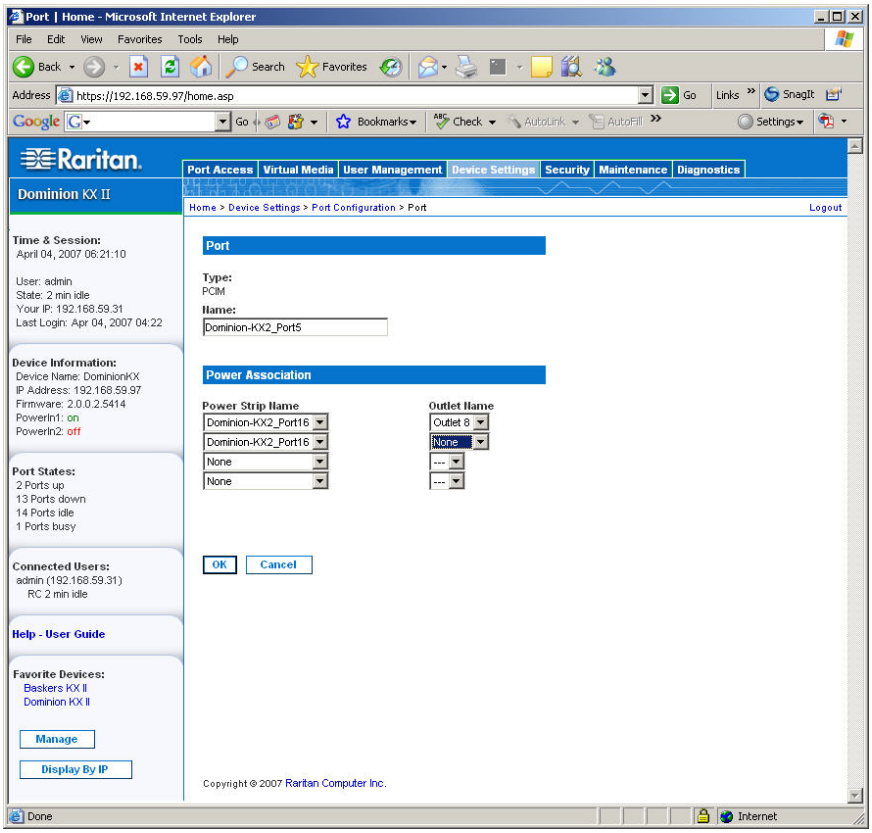

*Abbildung 68: Seite **Port** (KVM-Ports)*

So stellen Sie Stromzuordnungen her (ordnen Powerstripausgänge Zielservern zu):

***Hinweis:** Wenn ein Powerstrip einem Zielserver (Port) zugeordnet ist, wird der Ausgangsname durch den Namen des Zielservers ersetzt.*

1. Wählen Sie einen Powerstrip in der Dropdownliste **Power Strip Name** (Powerstripname) aus.
2. Wählen Sie einen Ausgang für diesen Powerstrip in der Dropdownliste **Outlet Name** (Ausgangsname) aus.
3. Wiederholen Sie die Schritte 1 und 2 für alle gewünschten Stromzuordnungen.
4. Klicken Sie auf **OK** (Senden). Eine Bestätigungsmeldung wird angezeigt.

So ändern Sie den Portnamen:

1. Geben Sie einen aussagekräftigen Namen im Feld **Name** ein. Der Name des Zielservers wäre eine gute Wahl. Der Name darf maximal 32 alphanumerische Zeichen und Sonderzeichen umfassen.
2. Klicken Sie auf **OK** (Senden).

So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:

Klicken Sie auf die Schaltfläche **Cancel** (Abbrechen).

So entfernen Sie eine Powerstripzuordnung:

1. Wählen Sie einen Powerstrip in der Dropdownliste **Power Strip Name** (Powerstripname) aus.
2. Wählen Sie einen Ausgang für diesen Powerstrip in der Dropdownliste **Outlet Name** (Ausgangsname) aus.
3. Wählen Sie in der Dropdownliste **Outlet Name** (Ausgangsname) die Option **None** (Keine).
4. Klicken Sie auf **OK** (Senden). Diese Powerstrip-/Ausgangszuordnung wird entfernt. Eine Bestätigungsmeldung wird angezeigt.

Hinweis für die Verwendung des CIMs D2CIM-VUSB

Wenn Sie das CIM D2CIM-VUSB verwenden, stehen Ihnen auf der Seite **Port** weitere Einstellungen zur Verbesserung der Leistung zur Verfügung.

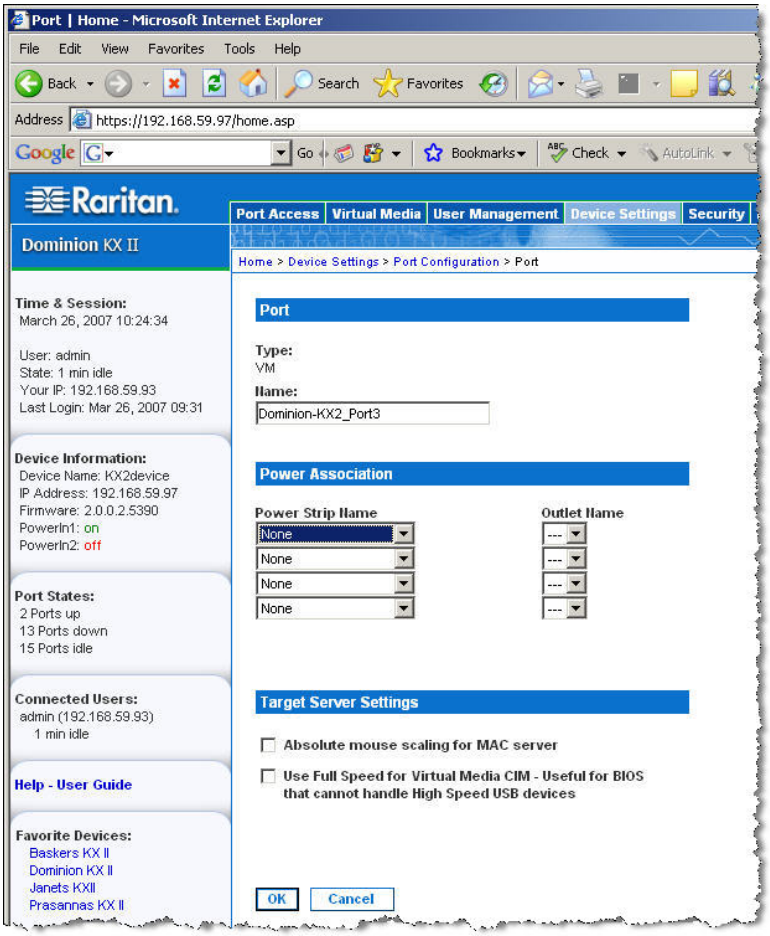

*Abbildung 69: Seite **Port** (Zielservereinstellungen für D2CIM-VUSB)*

Wenn Synchronisationsprobleme auftreten und Sie das CIM D2CIM-VUSB für einen Mac-Zielserver verwenden, aktivieren Sie das Kontrollkästchen **Absolute mouse scaling for MAC server** (Absolute Mausskalierung für MAC-Server).

Bestimmte BIOS-Konfigurationen unterstützen USB-Hochgeschwindigkeitsfunktionen nicht, und das automatische Aushandeln funktioniert nicht. Bei BIOS-Problemen mit dem Zielserver aktivieren Sie das Kontrollkästchen **Use Full Speed for Virtual Media CIM** (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden).

Hinweis: *Für SUSE 9.2-Zielserver aktivieren Sie die Option* ***Use Full Speed for Virtual Media CIM*** *(Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) für die betreffenden Zielserverports. SUSE 9.2 arbeitet nicht mit dem virtuellen Medien-CIM, wenn Hochgeschwindigkeit ausgehandelt wird.*

Kapitel 10: Sicherheitseinstellungen

Das Menü **Security** (Sicherheit) umfasst folgende Optionen: **Security Settings** (Sicherheitseinstellungen) und **IP Access Control** (IP-Zugriffssteuerung).

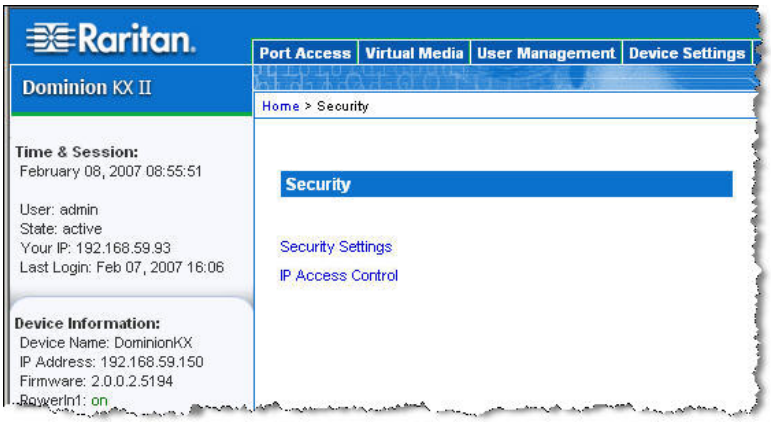

*Abbildung 70: Menü **Security** (Sicherheit)*

OPTION	AN:
Sicherheitseinstellungen	Konfigurieren von Sicherheitseinstellungen für Anmeldebeschränkungen, sichere Kennwörter, die Benutzerblockierung sowie Verschlüsselung und Freigabe
IP Access Control (IP-Zugriffssteuerung)	Steuerung des Zugriffs auf die Dominion KX II-Einheit. Durch das Einrichten einer globalen Zugriffssteuerungsliste stellen Sie sicher, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet.

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 stellt sicher, dass Ihre Informationen nicht in falsche Hände geraten, und anhand dieser Zertifikate sehen Sie, dass es sich um Raritan, Inc. handelt.

So konfigurieren Sie die Sicherheitseinstellungen:

1. Wählen Sie **Security > Security Settings** (Sicherheit > Sicherheitseinstellungen). Die Seite **Security Settings** (Sicherheitseinstellungen) wird angezeigt.

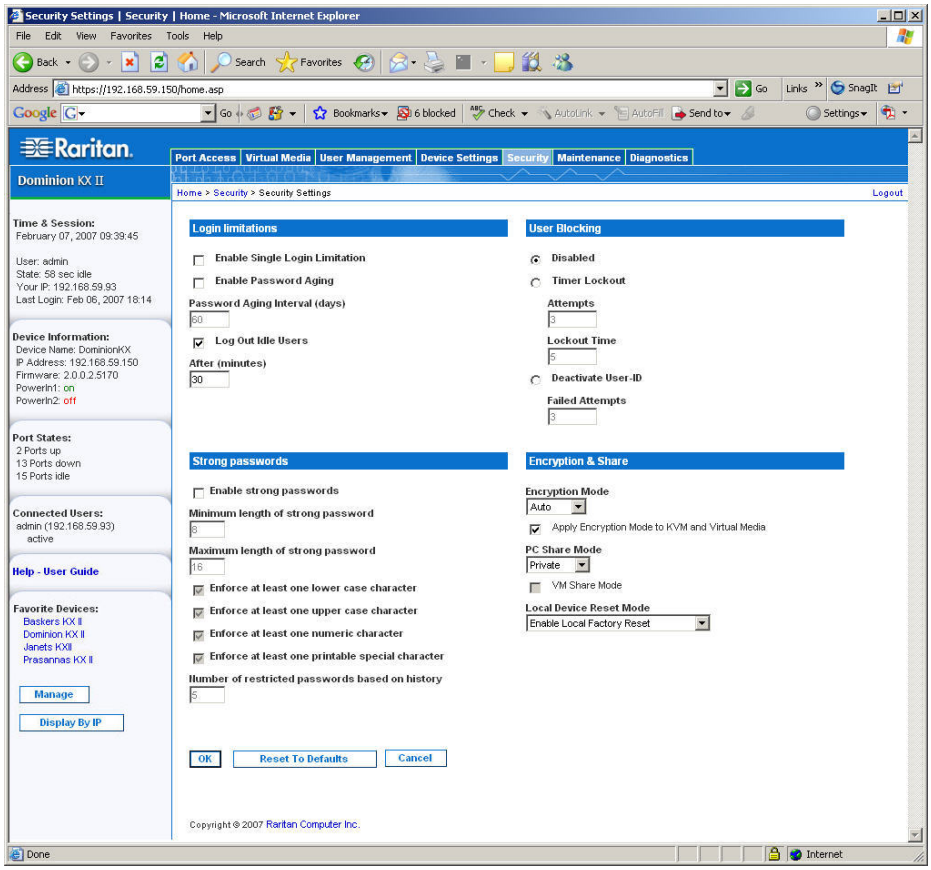

Abbildung 71: Sicherheitseinstellungen

Die Felder sind in den folgenden Gruppen zusammengefasst: **Login Limitations** (Anmeldebeschränkungen), **Strong Passwords** (Sichere Kennwörter), **User Blocking** (Benutzerblockierung) und **Encryption & Share** (Verschlüsselung und Freigabe).

2. Aktualisieren Sie ggf. die Einstellungen für die Anmeldebeschränkungen.
3. Aktualisieren Sie ggf. die Einstellungen für sichere Kennwörter.
4. Aktualisieren Sie ggf. die Einstellungen für die Benutzerblockierung.
5. Aktualisieren Sie ggf. die Einstellungen für Verschlüsselung und Freigabe.
6. Klicken Sie abschließend auf **OK**.

So schließen Sie die Seite, ohne Ihre Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So stellen Sie die Standardwerte wieder her:

Klicken Sie auf **Reset to Defaults** (Auf Standardeinstellungen zurücksetzen).

Anmeldebeschränkungen

Mithilfe von Anmeldebeschränkungen können Sie Beschränkungen auf Einzelanmeldungen, die Geltungsdauer von Kennwörtern und das Abmelden inaktiver Benutzer festlegen.

- **Enable Single Login Limitation** (Beschränkung auf eine Anmeldung aktivieren): Wenn Sie dieses Kontrollkästchen aktivieren, ist pro Benutzername immer nur eine Anmeldung zulässig. Ist es dagegen deaktiviert, kann eine Benutzername-/Kennwortkombination von mehreren Clientworkstations gleichzeitig verwendet werden, um eine Verbindung mit dem Gerät herzustellen.
- **Enable Password Aging** (Kennwortablauf 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 den Kennwortablauf) eingegeben haben, regelmäßig ändern.
  - **Password Aging Interval (days)** (Intervall für den Kennwortablauf [Tage]): Dieses Feld ist aktiv und erforderlich, wenn Sie das Kontrollkästchen **Enable Password Aging** (Kennwortablauf 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** (Inaktive Benutzer abmelden): Aktivieren Sie dieses Kontrollkästchen, wenn eine Benutzersitzung nach einer bestimmten Inaktivitätsphase automatisch getrennt werden soll. Geben Sie die Zeitspanne ins Feld **After** (Nach) ein. Wenn keine Tastatur- oder Mausaktivitäten stattfinden, werden alle KVM-Sitzungen und -Ressourcen abgemeldet. Für virtuelle Mediensitzungen gibt es hingegen kein Zeitlimit.
  - **After (minutes)** (Nach [Minuten]): Die 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.

Sichere Kennwörter

Sichere Kennwörter sorgen für eine sicherere lokale Authentifizierung des Systems. Im Bereich **Strong Passwords** (Sichere Kennwörter) können Sie Kriterien für das Format gültiger lokaler KX II-Kennwörter wie Mindest- und Höchstlänge, erforderliche Zeichen und Aufbewahrung des Kennwortverlaufs festlegen.

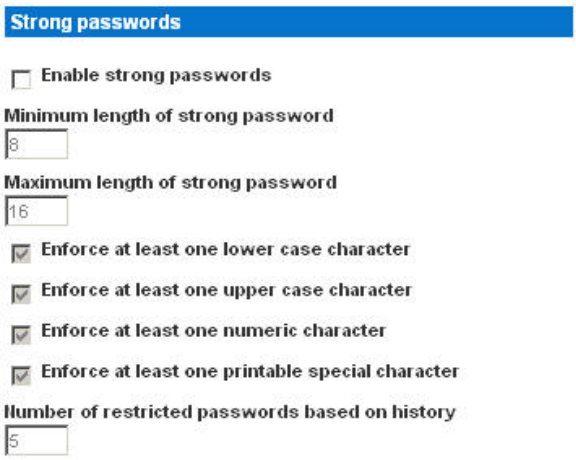

Abbildung 72: Sicherheitseinstellungen (Sichere Kennwörter)

- **Enable strong passwords** (Sichere Kennwörter aktivieren): Damit ein Kennwort sicher ist, muss es eine Mindestlänge von acht Zeichen sowie mindestens ein alphabetisches Zeichen und ein nicht-alphabetisches Zeichen (Satzzeichen oder Ziffer) haben. Darüber hinaus dürfen die ersten vier Zeichen des Kennworts und des Benutzernamens nicht identisch sein.

  Wenn Sie dieses Kontrollkästchen 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:
  - **Minimum length of strong password** (Mindestlänge des sicheren Kennworts): Kennwörter müssen mindestens 8 Zeichen umfassen. Es dürfen aber bis zu 63 Zeichen sein.
  - **Maximum length of strong password** (Höchstlänge des sicheren Kennworts): Die Standardlänge liegt bei 16 Zeichen, es dürfen aber bis zu 64 Zeichen sein.
  - **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 gibt an, wie weit der Kennwortverlauf zurückreicht, d. h. die Anzahl früherer Kennwörter, die nicht wiederholt werden dürfen. Ein Bereich zwischen 1 und 12 ist möglich, der Standardwert liegt bei 5.

Benutzerblockierung

Mithilfe der Optionen unter **User Blocking** (Benutzerblockierung) geben Sie die Kriterien an, anhand derer Benutzer nach der festgelegten Zahl fehlgeschlagener Anmeldeversuche am Zugriff auf das System gehindert werden. Die drei Optionen schließen sich gegenseitig aus.

- **Disabled** (Deaktiviert): Dies ist die Standardoption. Benutzer werden unabhängig von der Anzahl fehlgeschlagener Anmeldeversuche nicht blockiert.
- **Timer Lockout** (Zeitliche Sperre): Benutzern wird der Zugriff auf das System für den festgelegten Zeitraum verweigert, nachdem sie eine bestimmte Anzahl fehlgeschlagener Anmeldeversuche überschritten haben. Bei dieser Option stehen die folgenden Felder zur Verfügung:
  - **Attempts** (Versuche): Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche ein, nach der ein Benutzer blockiert wird. Ein Bereich zwischen 1 und 10 ist möglich, der Standardwert liegt bei 3 Versuchen.
  - **Lockout Time** (Blockierdauer): Geben Sie an, wie lange der Benutzer gesperrt ist. Ein Bereich zwischen 1 und 1.440 Minuten ist möglich, der Standardwert liegt bei 5 Minuten.

- **Deactivate User-ID** (Benutzer-ID deaktivieren): Diese Option legt fest, dass dem Benutzer nach der Anzahl der im Feld **Failed Attempts** (Fehlversuche) angegebenen fehlgeschlagenen Anmeldeversuche der Zugriff auf das System verweigert wird.
  - **Failed Attempts** (Fehlversuche): Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche 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.

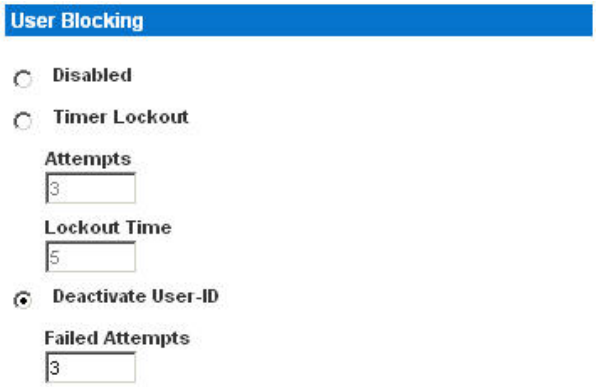

Abbildung 73: Sicherheitseinstellungen (Benutzerblockierung)

Wenn eine Benutzer-ID nach der angegebenen Zahl fehlgeschlagener Anmeldeversuche 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 zum Zurücksetzen an der Dominion KX II-Einheit gedrückt wird.

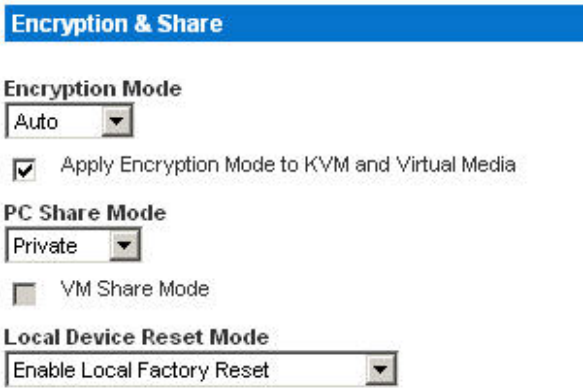

Abbildung 74: Sicherheitseinstellungen (Verschlüsselung und Freigabe)

- **Encryption Mode** (Verschlüsselungsmodus): Wählen Sie eine Option aus der Dropdownliste. Wenn Sie einen Verschlüsselungsmodus gewählt haben, wird eine Warnung angezeigt, dass Sie keine Verbindung zum Dominion KX II mehr herstellen können, falls Ihr Browser den gewählten Modus nicht unterstützt.

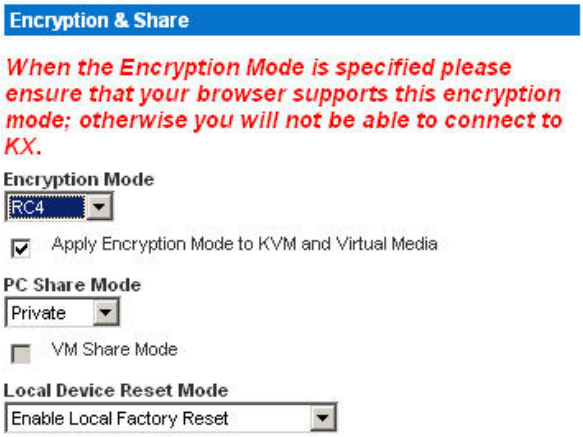

Abbildung 75: Sicherheitseinstellungen (Warnhinweis zum Verschlüsselungsmodus)

  - **Auto** (Automatisch): Diese Option wird empfohlen. Der Dominion KX II handelt die höchstmögliche Verschlüsselungsebene automatisch aus.
  - **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 Kommunikationskanal zwischen der Dominion KX II-Einheit und dem Remote-PC bereitstellt.
  - **AES-128**: Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology für die Verschlüsselung elektronischer Daten mit einer Schlüssellänge von 128 Bit. Achten Sie bei Auswahl dieser Option 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.
- **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.
- **PC Share Mode** (PC-Freigabemodus): Bestimmt den *globalen* gleichzeitigen KVM-Remotezugriff und ermöglicht bis zu acht Remotebenutzern die gleichzeitige Anmeldung an einer Dominion KX II-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 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.

- **VM Share Mode** (VM-Freigabemodus): Diese Option steht nur zur Verfügung, wenn Sie den PC-Freigabemodus aktiviert haben. 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.
- **Local Device Reset Mode** (Modus zum Zurücksetzen eines lokalen Geräts): 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 Taste zum Zurücksetzen. Wählen Sie eine der folgenden Optionen:
  - **Enable Local Factory Reset** (Lokale Werkrücksetzung aktivieren) (Standardeinstellung): Setzt die Dominion KX II-Einheit auf die Werkseinstellungen zurück.
  - **Enable Local Admin Password Reset** (Lokale Administratorkennwortrücksetzung 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.

Prüfen Ihres Browsers auf AES-Verschlüsselung

Falls Sie wissen möchten, ob Ihr Browser AES verwendet, erkundigen Sie sich beim Hersteller, oder navigieren Sie mithilfe des Browsers und der zu prüfenden Verschlüsselungsmethode zu folgender Website: https://www.fortify.net/sslcheck.html. Diese Website erkennt die Verschlüsselungsmethode Ihres Browsers und zeigt einen entsprechenden Bericht an.

IP Access Control (IP-Zugriffssteuerung)

Mithilfe der IP-Zugriffssteuerung können Sie den Zugriff auf die Dominion KX II-Einheit kontrollieren. 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-Einheit. Sie können den Zugriff auf die Einheit jedoch auch auf Gruppenebene steuern. Weitere Informationen zur Steuerung auf Gruppenebene finden Sie unter Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste).

Wichtig: Die IP-Adresse 127.0.0.1 wird vom lokalen Port des Dominion KX II verwendet. Wenn sich 127.0.0.1 beim Erstellen der IP-Zugriffssteuerungsliste im Bereich der gesperrten IP-Adressen befindet, können Sie nicht auf den lokalen Port des Dominion KX II zugreifen.

So verwenden Sie die IP-Zugriffssteuerung:

1. Öffnen Sie die Seite **IP Access Control** (IP-Zugriffssteuerung) mit einem der folgenden Verfahren:
   - Wählen Sie **Security > IP Access Control** (Sicherheit > IP-Zugriffssteuerung), oder
   - Klicken Sie auf der Seite Network Settings (Netzwerkeinstellungen) auf die Schaltfläche **Set System ACL** (System-ACL festlegen).

Die Seite **IP Access Control** (IP-Zugriffssteuerung) wird angezeigt.

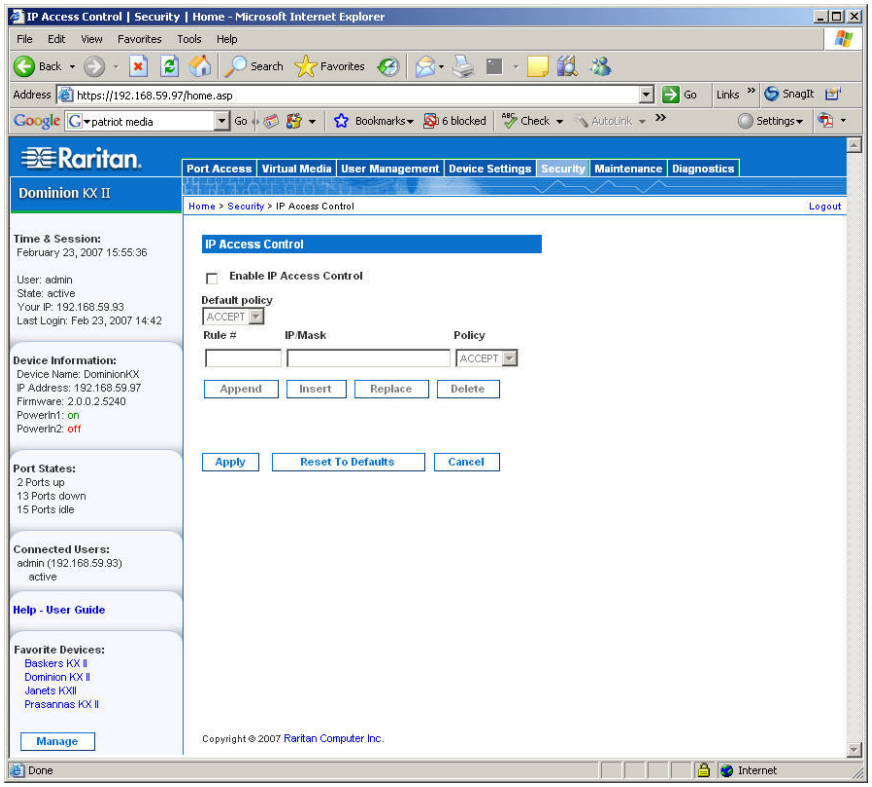

*Abbildung 76: **IP Access Control** (IP-Zugriffssteuerung)*

2. Aktivieren Sie das Kontrollkästchen **Enable IP Access Control** (IP-Zugriffssteuerung aktivieren), um die IP-Zugriffssteuerung sowie die restlichen Felder auf der Seite zu aktivieren.

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 Dominion KX II-Gerät zugreifen.
   - **Drop** (Ablehnen): Diesen IP-Adressen wird der Zugriff auf das Dominion KX II-Gerät verweigert.

So fügen Sie Regeln hinzu:

1. Geben Sie die IP-Adresse und die Subnetzmaske im Feld **IP/Mask** (IP/Maske) ein.
2. Wählen Sie in der Dropdownliste **Policy** eine Richtlinie aus.
3. Klicken Sie auf **Append** (Anfügen). Die Regel wird unten in der Liste hinzugefügt.
4. Wiederholen Sie die Schritte 1 bis 3, 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 die IP-Adresse und die Subnetzmaske im Feld **IP/Mask** (IP/Maske) ein.
3. Wählen Sie in der Dropdownliste **Policy** 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.

So ersetzen Sie eine Regel:

1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld **IP/Mask** (IP/Maske) ein.
3. Wählen Sie in der Dropdownliste **Policy** 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 **Löschen**.
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **OK** (Senden).

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

Kapitel 11: Wartung

Das Menü **Maintenance** (Wartung) enthält folgende Optionen: **Audit Log** (Prüfprotokoll), **Device Information** (Geräteinformationen), **Backup/Restore** (Sicherung/Wiederherstellung), **CIM Firmware Upgrade** (CIM-Firmwareaktualisierung), **Firmware Upgrade** (Firmwareaktualisierung), **Factory Reset** (Werksrückstellung) (nur lokale Dominion KX II-Konsole), **Upgrade Report** (Aktualisierungsbericht) und **Reboot** (Neustart).

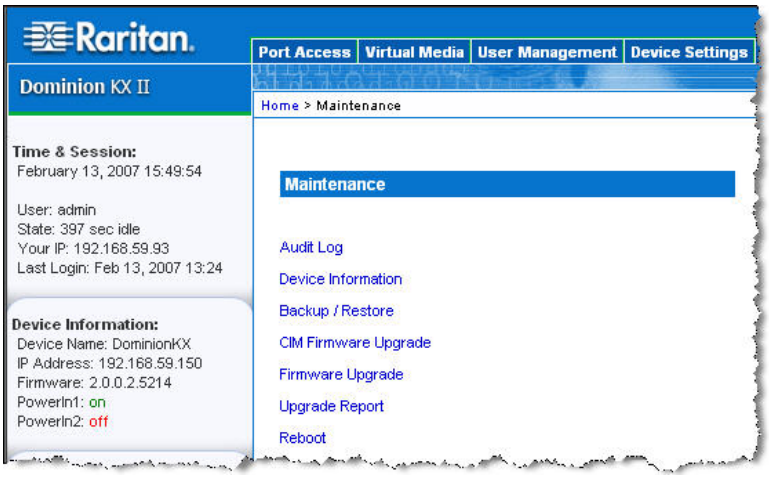

*Abbildung 77: Menü **Maintenance** (Wartung)*

OPTION	AN:	LOKAL	REMOTE
Prüfprotokoll	Anzeigen von Dominion KX II-Ereignissen sortiert nach Datum und Uhrzeit	✓	✓
Geräteinformationen	Anzeigen von Informationen über den Dominion KX II und die CIMs	✓	✓
Backup/Restore (Sicherung/Wiederherstellung)	Sichern und Wiederherstellen der KX II-Konfiguration		✓
CIM Firmware Upgrade (CIM-Firmwareaktualisierung)	Aktualisieren der CIMs mithilfe der im Speicher des Dominion KX II abgelegten Firmwareversionen	✓	✓
Firmwareaktualisierung	Aktualisieren der Dominion KX II-Firmware		✓
Werksrückstellung	Durchführen einer Werksrückstellung	✓	
Upgrade Report (Aktualisierungsbericht)	Anzeigen von Informationen zur letzten Aktualisierung	✓	✓
Reboot (Neustart)	Neustarten der Dominion KX II-Einheit	✓	✓

Prüfprotokoll

Alle Dominion KX II-Systemereignisse werden protokolliert.

So zeigen Sie das Prüfprotokoll für Ihre Dominion KX II-Einheit an:

Wählen Sie **Maintenance > Audit Log** (Wartung > Prüfprotokoll). Die Seite **Audit Log** (Prüfprotokoll) wird angezeigt.

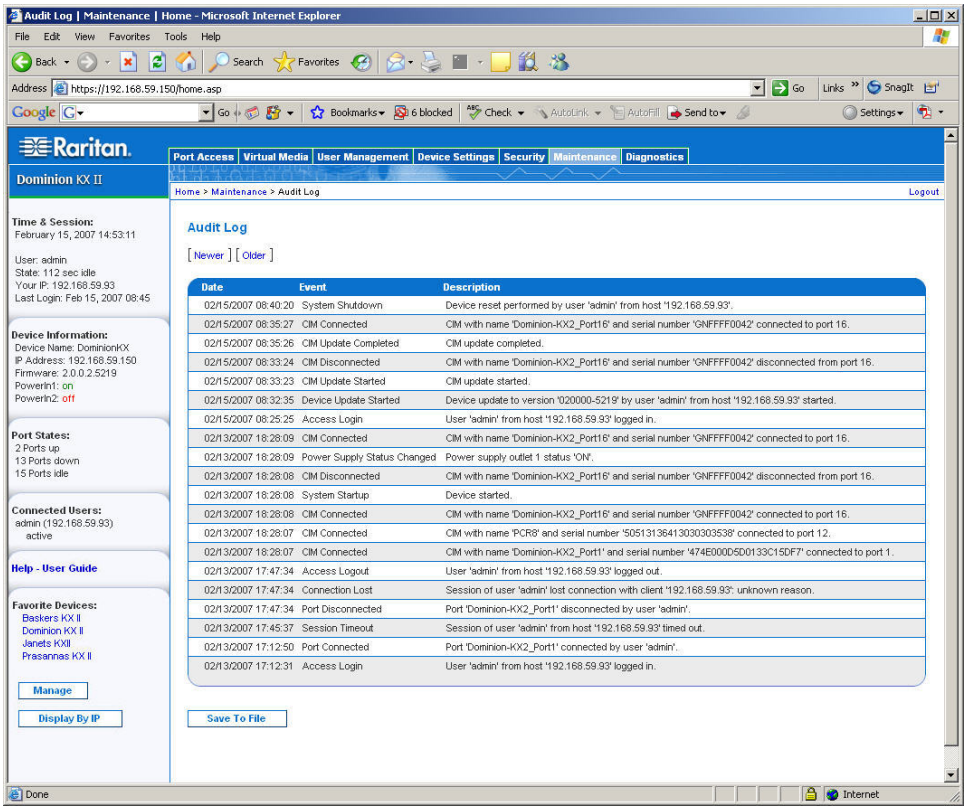

Abbildung 78: Prüfprotokoll

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 im 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 Dominion KX II-Remotekonsole speichern, nicht jedoch mit der lokalen Dominion KX II-Konsole.*

1. Klicken Sie auf die Schaltfläche **Save to File** (Speichern unter). Das Dialogfeld **Save File** (Datei speichern) 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 Clientcomputer 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 Dominion KX II-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 zum Dominion KX II und den CIMs an:

Wählen Sie **Maintenance > Device Information** (Wartung > Geräteinformationen). Die Seite **Device Information** (Geräteinformationen) wird angezeigt.

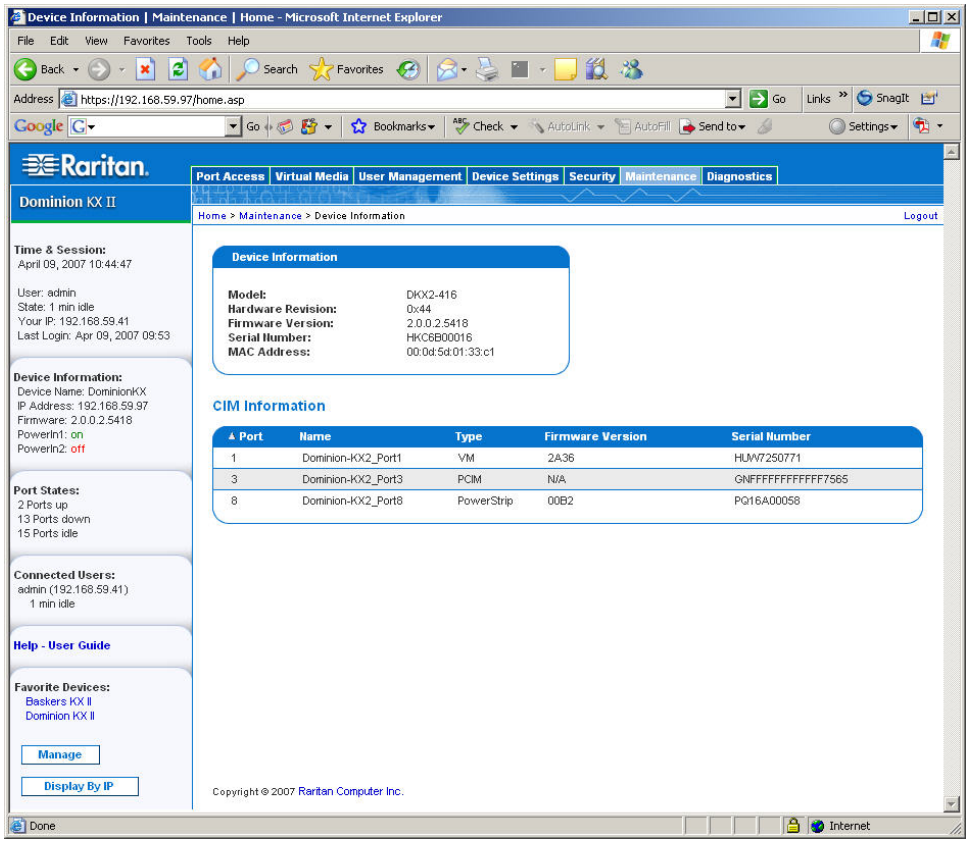

Abbildung 79: Geräteinformationen

Zum Dominion KX II werden folgende Informationen angezeigt: **Modell**, **Hardwareversion**, **Firmwareversion**, **Seriennummer** und **MAC-Adresse**.

Zu den verwendeten CIMs werden folgende Informationen angezeigt: **Port** (Portnummer), **Name**, **Typ** (des CIM: DCIM, PCIM, Power Strip oder VM), Firmwareversion und Seriennummer.

Sicherung und Wiederherstellung

Auf der Seite **Backup/Restore** (Sicherung/Wiederherstellung) können Sie die Einstellungen und die Konfiguration des Dominion KX II sichern und wiederherstellen. Dieses Feature dient nicht nur der Gewährleistung der Geschäftskontinuität, sondern Sie können damit auch viel Zeit sparen. Sie können Ihrem Team beispielsweise schnell von einem anderen Dominion KX II Zugriff gewähren, in dem Sie die Benutzerkonfigurationseinstellungen des verwendeten KX II sichern und auf dem neuen Gerät wiederherstellen. Sie können auch einen Dominion KX II einrichten und seine Konfiguration auf mehrere andere KX II-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.

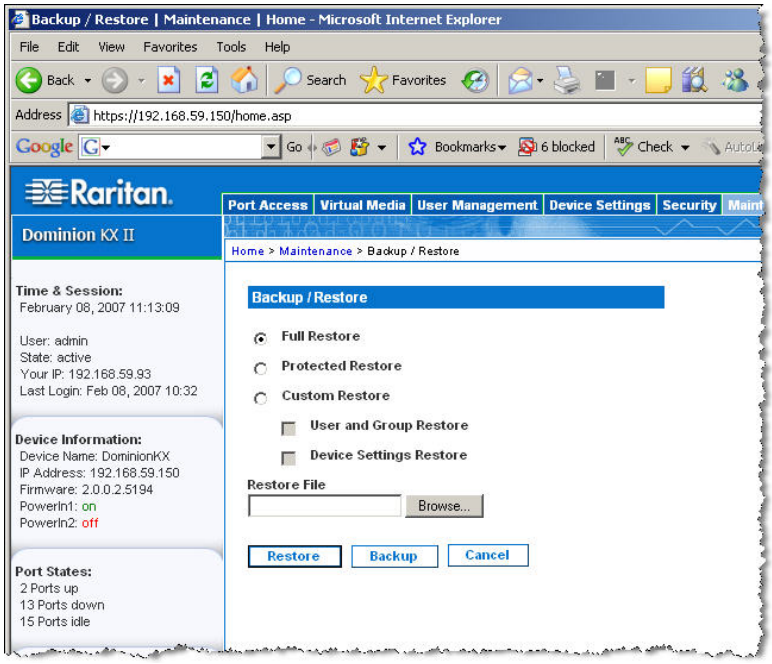

Abbildung 80: Backup/Restore (Sicherung/Wiederherstellung)

Hinweis: *Es wird immer das komplette System gesichert. Bei der Wiederherstellung können Sie zwischen einer vollständigen und einer teilweisen Wiederherstellung wählen.*

So sichern Sie den Dominion KX II:

1. Klicken Sie auf **Backup** (Sichern). Das Dialogfeld **File Download** (Dateidownload) wird angezeigt.
2. Klicken Sie auf **Save** (Speichern). Das Dialogfeld **Save As** (Speichern unter) wird angezeigt.
3. Wählen Sie einen Speicherort aus, geben Sie einen Dateinamen an, und klicken Sie auf **Save** (Speichern). Das Dialogfeld **Download Complete** (Download abgeschlossen) wird angezeigt.
4. Klicken Sie auf **Schließen**. Die Sicherungsdatei wird mit dem festgelegten Namen *lokal* am ausgewählten Ort auf dem Clientcomputer gespeichert.

So stellen Sie den Dominion KX II wieder her:

WARNUNG: Gehen Sie bei der Wiederherstellung Ihres Dominion KX II auf eine frühere Version bedachtsam 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 den KX II 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. Diese Option wird üblicherweise für die herkömmliche Sicherung und Wiederherstellung verwendet.
   - **Protected Restore** (Geschützte Wiederherstellung). Alle Daten mit *Ausnahme* von gerätespezifischen Informationen wie Seriennummer, MAC-Adresse, IP-Adresse, Name, Portnamen usw. werden wiederhergestellt. Mithilfe dieser Option können Sie einen Dominion KX II einrichten und die Konfiguration auf mehrere andere KX II-Geräte kopieren.
   - **Custom Restore** (Benutzerdefinierte Wiederherstellung). Unter dieser Option stehen die Kontrollkästchen **User and Group Restore** (Wiederherstellung von Benutzern und Gruppen) und **Device Settings Restore** (Wiederherstellung der Geräteeinstellungen) zur Verfügung. Aktivieren Sie die gewünschten Kontrollkästchen:
     - **User and Group Restore** (Wiederherstellung von Benutzern und Gruppen). Diese Option umfasst nur Benutzer- und Gruppeninformationen. Verwenden Sie sie, um schnell Benutzer auf einem anderen Dominion KX II einzurichten.
     - **Device Settings Restore** (Wiederherstellung der Geräteeinstellungen). Diese Option umfasst nur die Geräteeinstellungen. Verwenden Sie sie, um schnell die Geräteinformationen zu kopieren.
2. Klicken Sie auf die Schaltfläche **Browse** (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 **Restore** (Wiederherstellen). Die Konfiguration wird basierend auf der gewählten Wiederherstellungsart wiederhergestellt.

CIM-Aktualisierung

Gehen Sie wie unten beschrieben vor, um CIMs mithilfe der im Speicher der Dominion KX II-Einheit abgelegten Firmwareversionen zu aktualisieren. Im Allgemeinen werden alle CIMs aktualisiert, wenn Sie die Gerätefirmware über die Seite Firmware Upgrade (Firmwareaktualisierung) aktualisieren. Verwenden Sie die Seite **CIM Upgrade** (CIM-Aktualisierung), um neue CIMs zu aktualisieren.

Hinweis: *Nur D2CIM-VUSB und D2CIM-PWR können auf dieser Seite aktualisiert werden.*

So aktualisieren Sie CIMs mithilfe des Dominion KX II-Speichers:

1. Wählen Sie **Maintenance > CIM Firmware Upgrade** (Wartung > CIM-Firmwareaktualisierung). Die Seite **CIM Upgrade from KX Flash** (CIM-Aktualisierung aus KX-Flash) wird angezeigt.

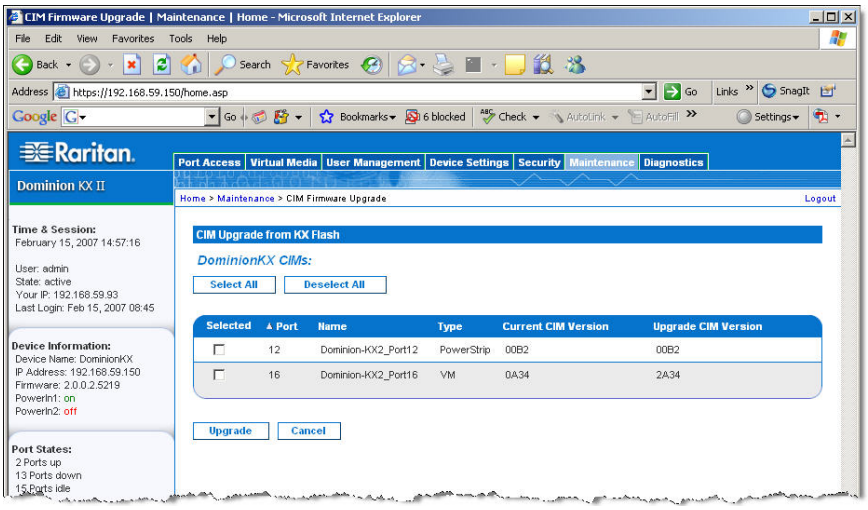

Abbildung 81: CIM Upgrade from KX Flash (CIM-Aktualisierung aus KX-Flash)

2. 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).
3. Aktivieren Sie für alle CIMs, die aktualisiert werden sollen, das Kontrollkästchen **Selected** (Ausgewählt).

*Tipp: Verwenden Sie die Schaltflächen **Select All** (Alle auswählen) und **Deselect All** (Alle entfernen), um schnell alle CIMs auszuwählen bzw. diese Auswahl aufzuheben.*

4. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren). Sie werden aufgefordert, die Aktualisierung zu bestätigen.
5. Klicken Sie auf **OK**, um fortzufahren. Während des Vorgangs werden Statusleisten angezeigt. Die Aktualisierung dauert maximal zwei Minuten pro CIM.

So verlassen Sie die Seite, ohne die CIMs zu aktualisieren:

Klicken Sie auf die Schaltfläche **Cancel** (Abbrechen).

Firmwareaktualisierung

Auf der Seite **Firmware Upgrade** (Firmwareaktualisierung) können Sie die Firmware Ihrer Dominion KX II-Einheit und aller angeschlossenen CIMs aktualisieren. Diese Seite ist nur in der *KX II-Remotekonsole* verfügbar.

Wichtig: Schalten Sie während der Aktualisierung die Dominion KX II-Einheit nicht aus, und trennen Sie die CIMs nicht, da dies zu Schäden an der Einheit bzw. den CIMs führen könnte.

So aktualisieren Sie die Dominion KX II-Einheit:

1. Suchen Sie die entsprechende Raritan-Firmwaredistributionsdatei (*.RFP) auf der Raritan-Webseite für Firmwareaktualisierungen: http://www.raritan.com/support/firmwareupgrades, und laden Sie die Datei herunter.
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 Firmwareaktualisierungsdatei vor dem Hochladen auf einen lokalen PC. Laden Sie die Datei nicht von einem Netzwerklaufwerk.*

3. Wählen Sie **Maintenance > Firmware Upgrade** (Wartung > Firmwareaktualisierung). Die Seite **Firmware Upgrade** (Firmwareaktualisierung) wird angezeigt.

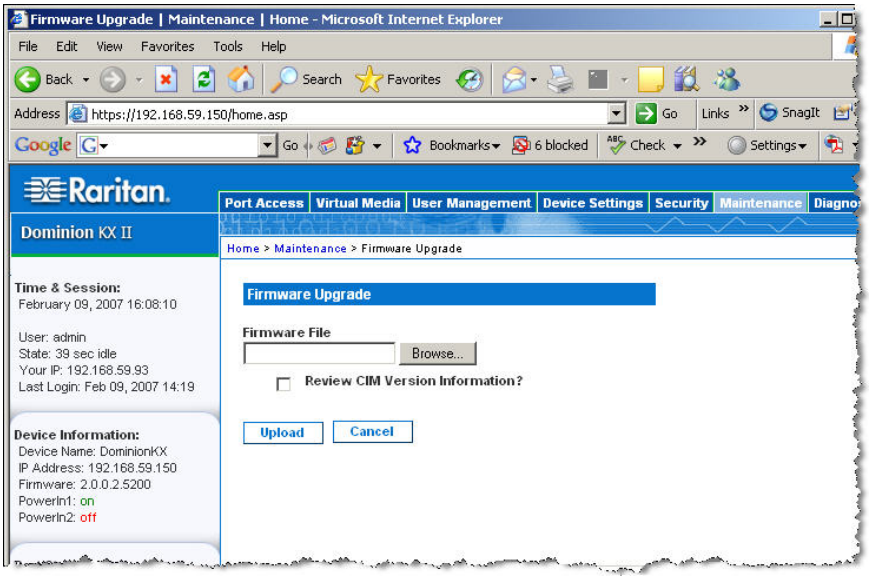

Abbildung 82: Firmwareaktualisierung

4. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um zu dem Verzeichnis zu navigieren, in dem Sie die Aktualisierungsdatei entpackt haben.
5. Aktivieren Sie das Kontrollkästchen **Review CIM Version Information?** (CIM-Versionsinformationen überprüfen?), wenn Informationen zu den Versionen der verwendeten CIMs angezeigt werden sollen.
6. Klicken Sie auf der Seite **Firmware Upgrade** (Firmwareaktualisierung) auf **Upload** (Hochladen). Ihnen werden Informationen zur Aktualisierung und den Versionsnummern sowie zu den CIMs (falls Sie das entsprechende Kontrollkästchen aktiviert haben) angezeigt.

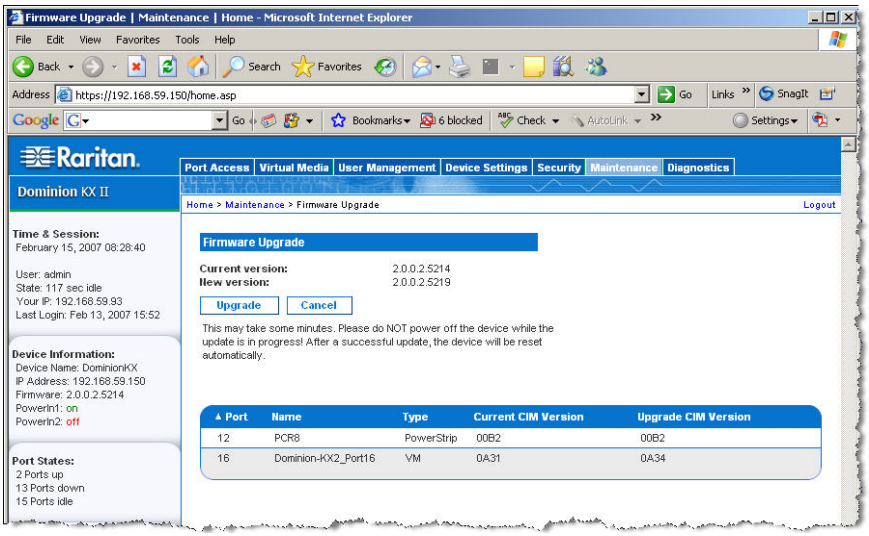

Abbildung 83: Überprüfung der Firmwareaktualisierung

Hinweis: *Zu diesem Zeitpunkt werden verbundene Benutzer abgemeldet, und neue Anmeldeversuche werden blockiert.*

7. Klicken Sie auf **Upgrade** (Aktualisieren). Warten Sie, bis der Vorgang abgeschlossen ist. Während des Vorgangs werden Statusinformationen und Statusleisten angezeigt. Nach Abschluss der Aktualisierung wird die Einheit neu gestartet (ein Tonsignal zeigt den Neustart an).

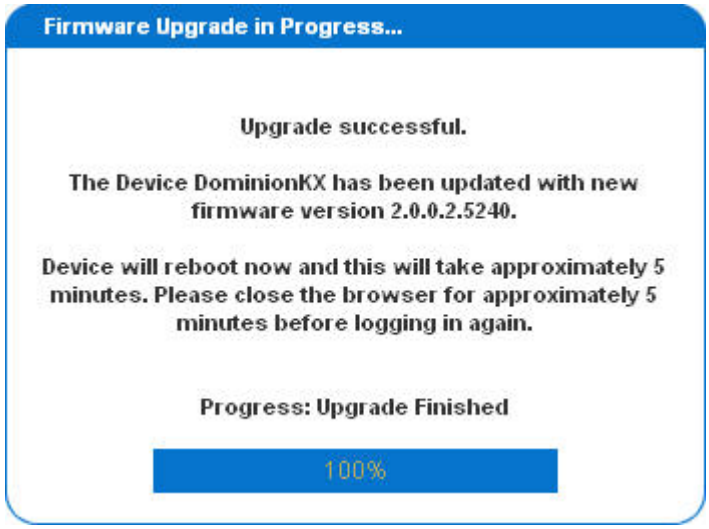

Abbildung 84: Erfolgreiche Firmwareaktualisierung

8. Schließen Sie den Browser, wenn Sie dazu aufgefordert werden, und warten Sie ungefähr fünf Minuten, bevor Sie sich erneut beim Dominion KX II anmelden.

Weitere Informationen zur Aktualisierung der Gerätefirmware mithilfe des Multi-Platform-Clients finden Sie im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)*.

Upgrade Report (Aktualisierungsbericht)

Dominion KX II liefert Informationen über die Aktualisierungen, die auf der KX II-Einheit und den angeschlossenen CIMs durchgeführt wurden.

So zeigen Sie den Aktualisierungsbericht an:

Wählen Sie **Maintenance > Upgrade Report** (Wartung > Aktualisierungsbericht). Die Seite **Upgrade Report** (Aktualisierungsbericht) wird angezeigt.

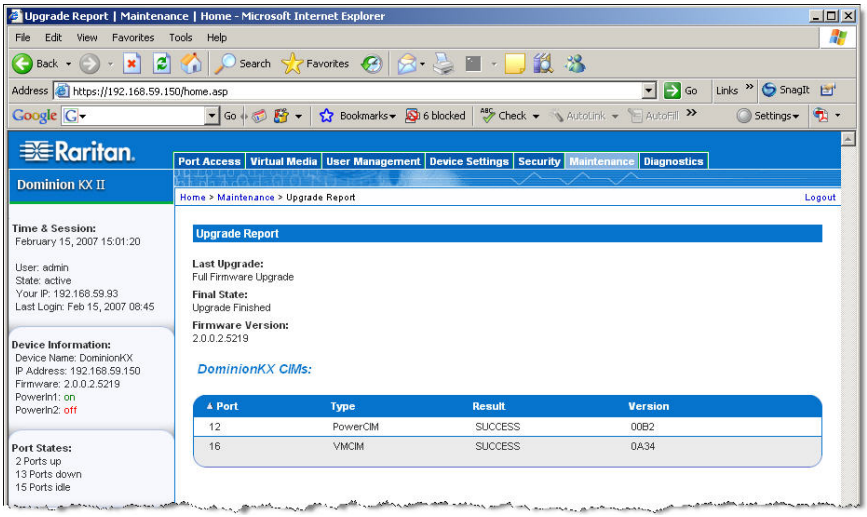

*Abbildung 85: **Upgrade Report** (Aktualisierungsbericht)*

Hier sehen Sie Informationen zur letzten Dominion KX II-Aktualisierung, zu ihrem endgültigen Status und zur Firmwareversion. Außerdem enthält die Seite Informationen zu den CIMs:

- **Port**: Der Port, an dem das CIM angeschlossen ist.
- **Type** (Typ): Der CIM-Typ.
- **Result** (Ergebnis): Das Ergebnis der Aktualisierung (erfolgreich oder fehlgeschlagen).
- **Version**: Die CIM-Firmwareversion.

Reboot (Neustart)

Auf der Seite **Reboot** (Neustart) können Sie die Dominion KX II-Einheit sicher und kontrolliert neu starten. Dieses Neustartverfahren wird empfohlen.

Wichtig: Alle KVM-Verbindungen werden getrennt und alle Benutzer abgemeldet.

So starten Sie den Dominion KX II neu:

1. Wählen Sie **Maintenance > Reboot** (Wartung > Neustart). Die Seite **Reboot** (Neustart) wird angezeigt.

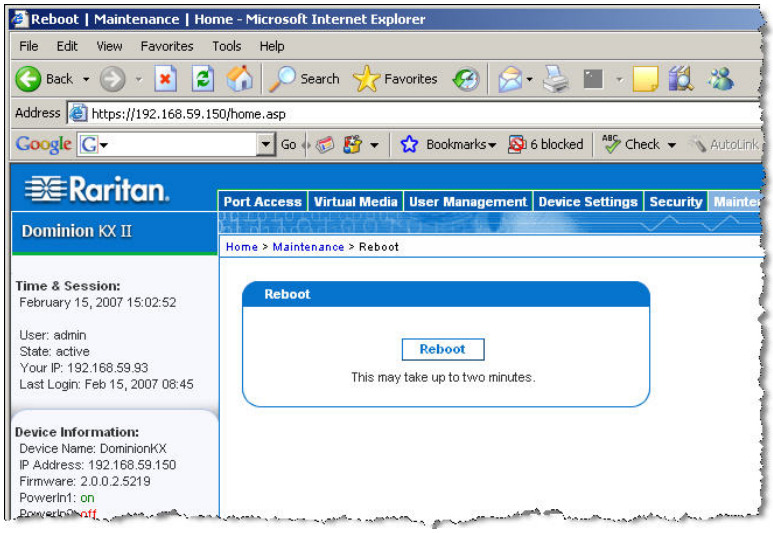

*Abbildung 86: **Reboot** (Neustart)*

2. Klicken Sie auf die Schaltfläche Reboot (Neu starten). Sie werden aufgefordert, die Aktion zu bestätigen.

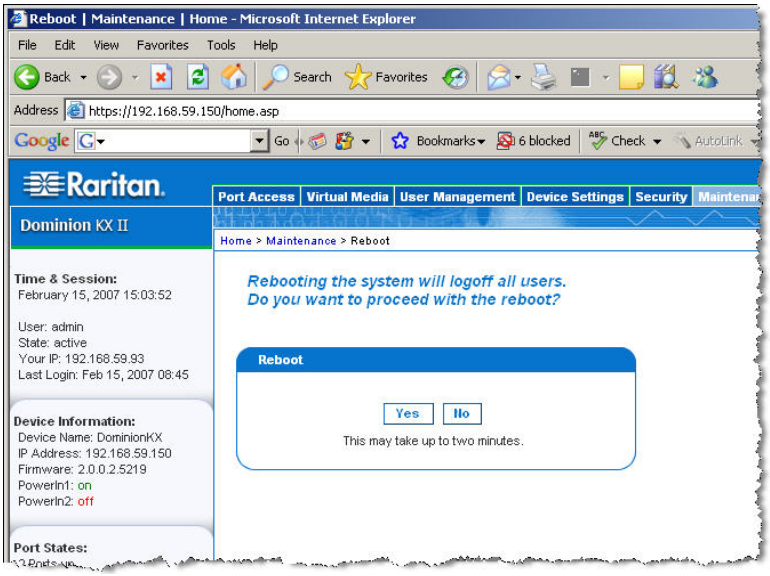

Abbildung 87: Bestätigung des Neustarts

3. Klicken Sie auf **Yes** (Ja), um fortzufahren.

So verlassen Sie die Seite, ohne einen Neustart durchzuführen:

Klicken Sie auf **No** (Nein).

Kapitel 12: Diagnose

Menü Diagnostics (Diagnose)

Auf den Diagnoseseiten können Sie Probleme behandeln. Sie sind hauptsächlich für den Administrator des KX II-Geräts gedacht. Auf allen Diagnoseseiten (außer **KX Diagnostics** [KX-Diagnose]) werden übliche Netzwerkbefehle ausgeführt. Die angezeigten Informationen sind das Ergebnis dieser Befehle.

Mithilfe der folgenden Optionen im Menü **Diagnostics** (Diagnose) können Sie Fehler in den Netzwerkeinstellungen beheben und diese konfigurieren:

- **Network Interface** (Netzwerkschnittstelle)
- **Network Statistics** (Netzwerkstatistik)
- **Ping Host** (Ping an den Host)
- **Trace Route to Host** (Route zum Host zurückverfolgen)

Die Option **KX Diagnostics** (KX-Diagnose) sollten Sie nur gemeinsam mit dem technischen Kundendienst von Raritan verwenden.

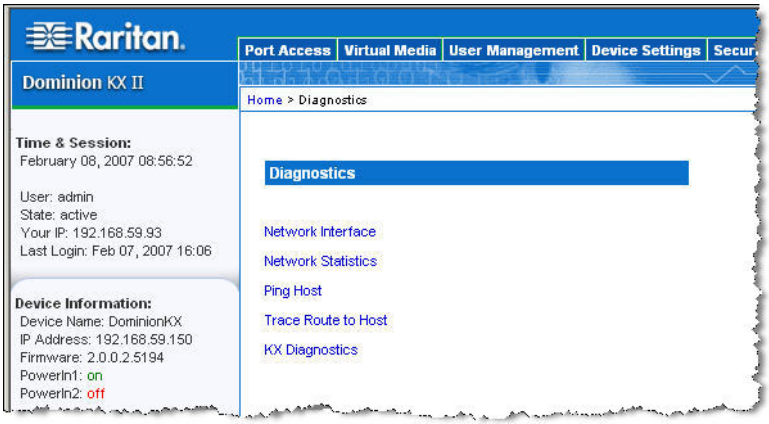

Abbildung 88: Menü Diagnostics (Diagnose)

OPTION	AN:
Network Interface (Netzwerkschnittstelle)	Abrufen des Status der Netzwerkschnittstelle
Network Statistics (Netzwerkstatistik)	Abrufen von Statistiken über das Netzwerk
Ping Host (Ping an den Host)	Ermitteln, ob ein bestimmter Host über ein IP-Netzwerk erreichbar ist
Trace Route to Host (Route zum Host zurückverfolgen)	Ermitteln der Route bis zum gewählten Host
KX Diagnostics (KX-Diagnose)	Verwendung nur nach Anweisung durch den technischen Kundendienst von Raritan (*nur KX II-Remotekonsole*)

Seite Network Interface (Netzwerkschnittstelle)

Der Dominion KX II 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.

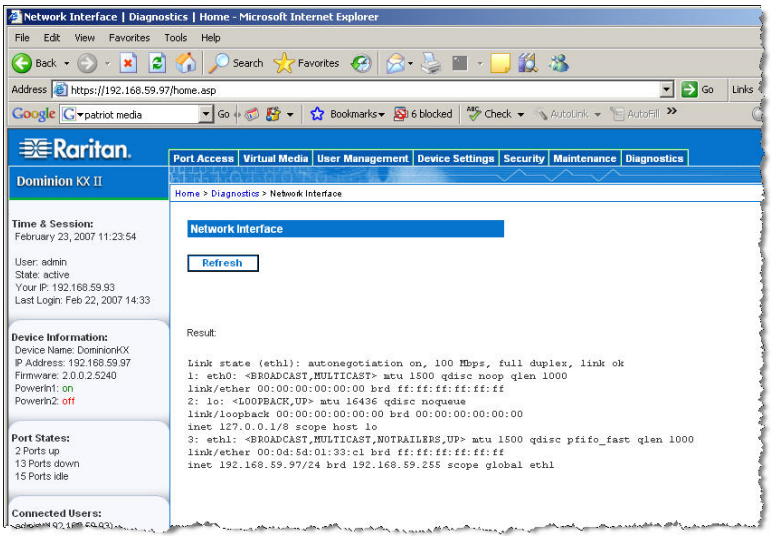

*Abbildung 89: **Network Interface** (Netzwerkschnittstelle)*

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 die Schaltfläche **Refresh** (Aktualisieren).

Seite Network Statistics (Netzwerkstatistik)

Der Dominion KX II 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 Dropdownliste **Options**:
   - **Statistics** (Statistik): Eine Seite, die der hier gezeigten ähnelt, wird erstellt.

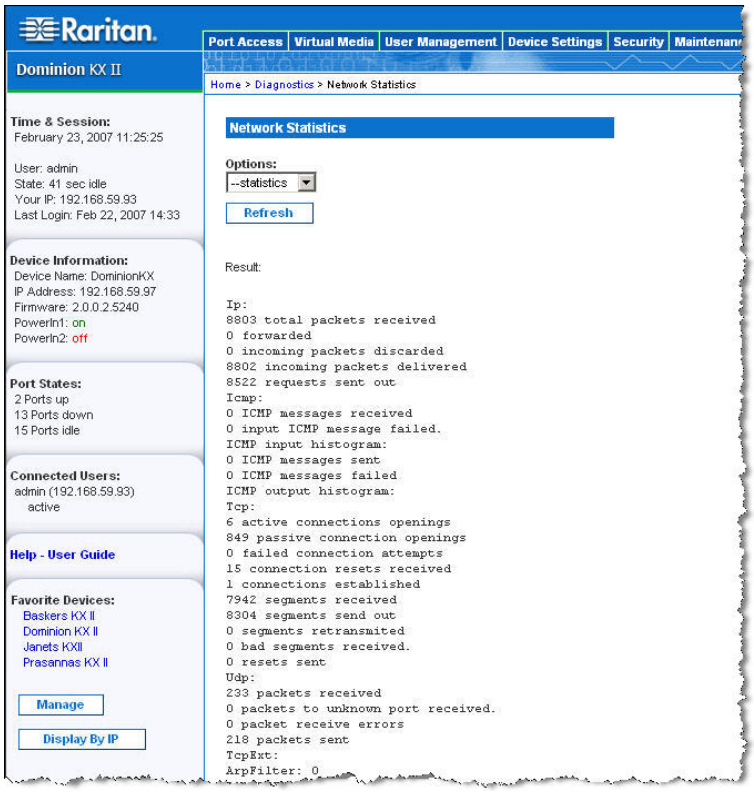

Abbildung 90: Network Statistics (statistics) (Netzwerkstatistik [Statistik])

   - **Interfaces** (Schnittstellen): Eine Seite, die der hier gezeigten ähnelt, wird erstellt.

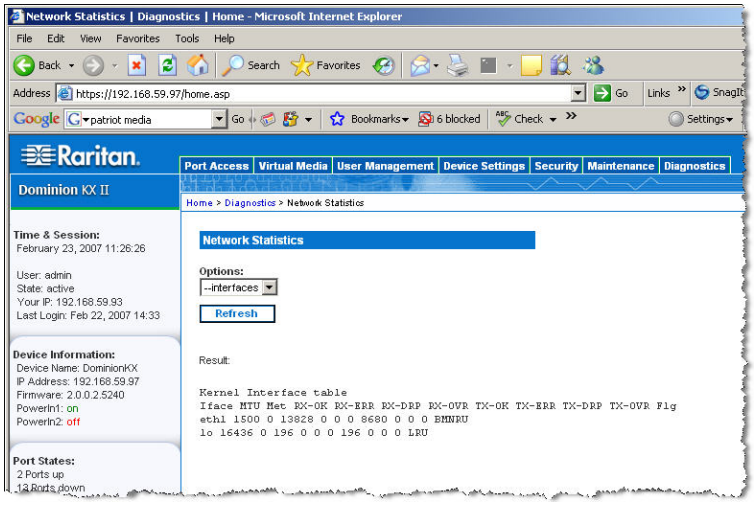

Abbildung 91: Network Statistics (interfaces) (Netzwerkstatistik [Schnittstellen])

- **Route**: Eine Seite, die der hier gezeigten ähnelt, wird erstellt.

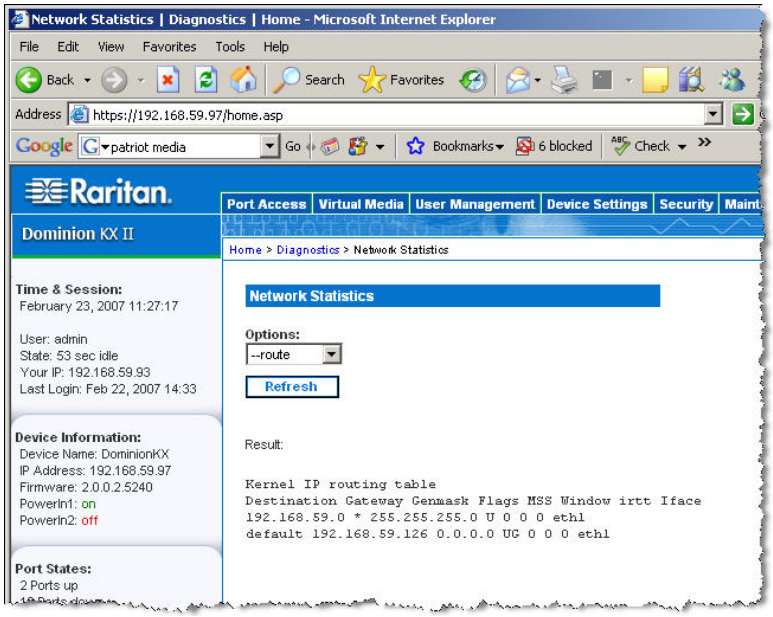

Abbildung 92: Network Statistics (route) (Netzwerkstatistik [Route])

3. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Die entsprechenden Informationen werden im Feld **Result** (Ergebnis) angezeigt.

Seite 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 Dominion KX II-Einheit erreichbar ist.

So senden Sie ein Ping an den Host:

1. Wählen Sie **Diagnostics > Ping Host** (Diagnose > Ping an den Host). Die Seite **Ping Host** (Ping an den Host) wird angezeigt.

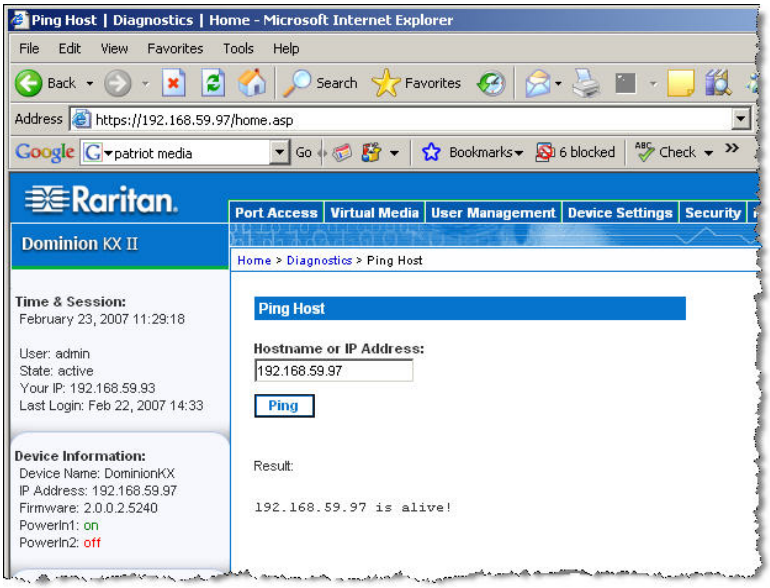

*Abbildung 93: **Ping Host** (Ping an den Host)*

2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld **Hostname or IP Address** (Hostname oder IP-Adresse) ein.
3. Klicken Sie auf **Ping**. Die Ping-Ergebnisse werden im Feld **Result** (Ergebnis) angezeigt.

Seite Trace Route to Host (Route zum Host zurückverfolgen)

Die Routenverfolgung ist ein Netzwerktool, mit dem Sie die Route bis zum angegebenen Hostnamen oder der IP-Adresse zurückverfolgen können.

So verfolgen Sie die Route bis zum Host zurück:

1. Wählen Sie **Diagnostics > Trace Route to Host** (Diagnose > Route zum Host zurückverfolgen). Die Seite **Trace Route to Host** (Route zum Host zurückverfolgen) wird angezeigt.

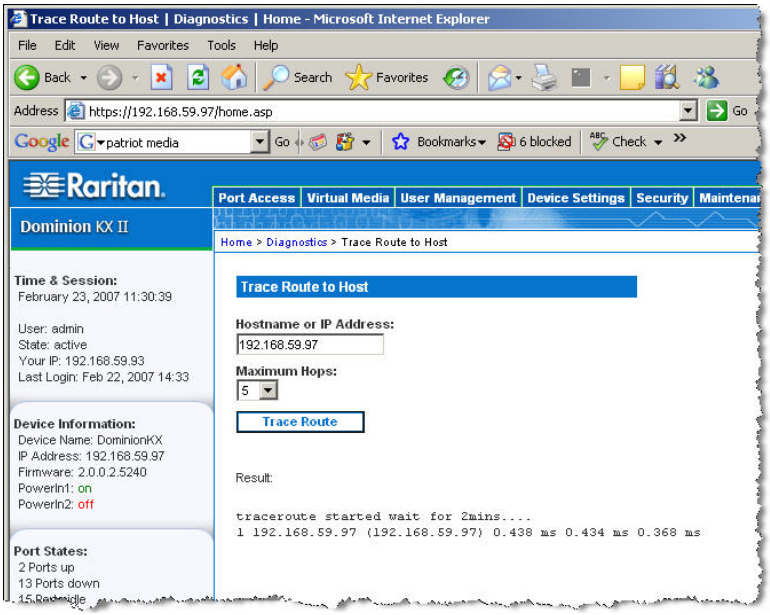

*Abbildung 94: **Trace Route to Host** (Route zum Host zurückverfolgen)*

2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld **Hostname or IP Address** (Hostname oder IP-Adresse) ein.
3. Wählen Sie in der Dropdownliste **Maximum Hops** (Maximale Teilstrecken) eine Option aus (5 oder 10).
4. Klicken Sie auf die Schaltfläche **Trace Route** (Route zurückverfolgen). Der Befehl wird für den angegebenen Hostnamen oder die IP-Adresse sowie die maximale Zahl der Teilstrecken ausgeführt. Das Ergebnis der Routenverfolgung wird im Feld **Result** (Ergebnis) angezeigt.

KX Diagnostics (KX-Diagnose)

Hinweis: *Diese Seite ist für die Außendienstmitarbeiter von Raritan gedacht. Verwenden Sie sie nur unter Anleitung des technischen Kundendienstes.*

Über die Seite **KX Diagnostics** (KX-Diagnose) können Sie Diagnoseinformationen vom Dominion KX II auf den Clientcomputer laden. Auf dieser Seite haben Sie drei Möglichkeiten:

- **Befehlszeilenschnittstelle**: Aktivieren oder deaktivieren Sie die Befehlszeilenschnittstelle. Mithilfe dieses Features kann ein Mitarbeiter des technischen Kundendienstes von Raritan einen Standard-SSH-Client öffnen, eine Verbindung mit der Einheit herstellen und Diagnosefunktionen remote ausführen.
- **Diagnoseskripts:** Führen Sie während einer Sitzung zum Debuggen eines schwerwiegenden Fehlers ein vom technischen Kundendienst von Raritan bereitgestelltes Spezialskript aus. Das Skript wird auf die Einheit hochgeladen und ausgeführt. Nachdem das Skript ausgeführt wurde, können Sie die Diagnosemeldungen über die Schaltfläche **Save to File** (Speichern unter) herunterladen.
- **KX-Diagnoseprotokoll**: Laden Sie eine Übersicht der Diagnosemeldungen von der KX II-Einheit auf den Client. 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 II-Systemdiagnose aus:

1. Wählen Sie **Diagnostics > KX Diagnostics** (Diagnose > KX-Diagnose). Die Seite **KX Diagnostics** (KX-Diagnose) wird angezeigt.

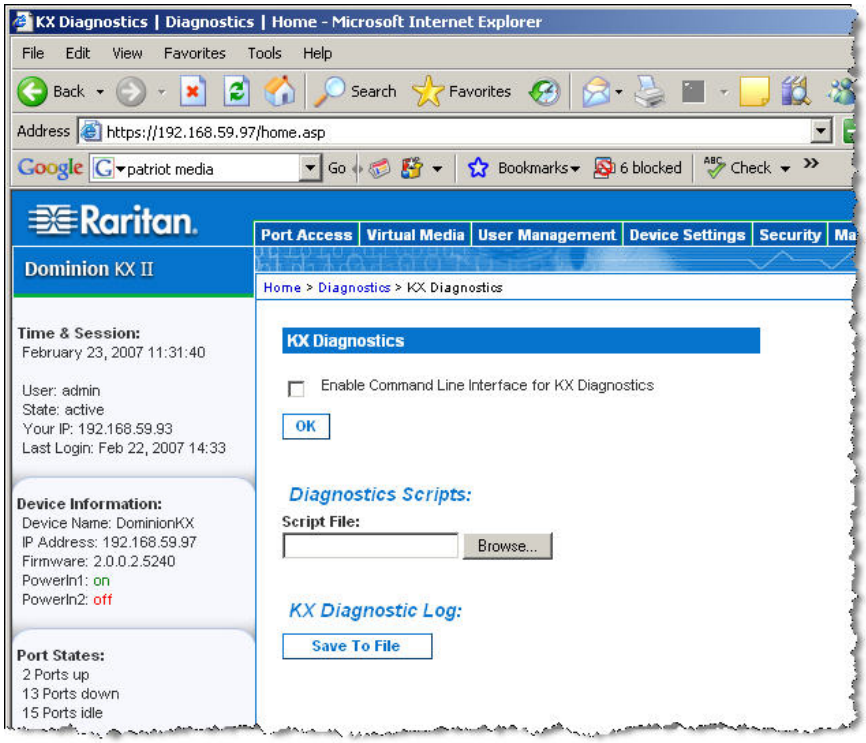

Abbildung 95: ***KX Diagnostics*** *(KX-Diagnose)*

2. So aktivieren Sie die Befehlszeilenschnittstelle für den technischen Kundendienst von Raritan:

   Hinweis: *Für dieses Feature ist UDP-Port 21 erforderlich.*

   a. Aktivieren Sie das Kontrollkästchen **Enable Command Line Interface for KX Diagnostics** (Befehlszeilenschnittstelle für KX-Diagnose aktivieren).

   b. Klicken Sie auf **OK** (Senden).

   c. UDP-Port 21 muss offen sein und dem technischen Kundendienst von Raritan zur Verfügung stehen.

   d. Darüber hinaus benötigt der technische Kundendienst das Administratorkennwort für den KX II.

   e. Nachdem der technische Kundendienst seine Tests abgeschlossen hat, stellen Sie den ursprünglichen Zustand des UDP-Ports 21 wieder her.

3. 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 die Schaltfläche **Browse** (Durchsuchen). Das Dialogfeld **Choose file** (Datei auswählen) wird angezeigt.

   c. Navigieren Sie zu der Diagnosedatei, und markieren Sie sie.

   d. Klicken Sie auf **Open**. Die Datei wird im Feld **Script File** (Skriptdatei) angezeigt.

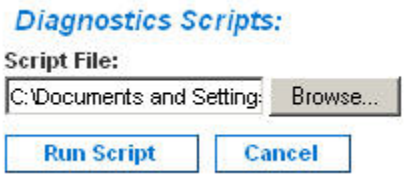

Abbildung 96: Diagnoseskripts

   e. Klicken Sie auf **Run Script** (Skript ausführen).

   f. Senden Sie diese Datei, wie in Schritt 4 beschrieben, an den technischen Kundendienst von Raritan.

4. So erstellen Sie eine Diagnosedatei, die Sie an den technischen Kundendienst von Raritan senden können:

   a. Klicken Sie auf die Schaltfläche **Save to File** (Speichern unter). Das Dialogfeld **File Download** (Dateidownload) wird angezeigt.

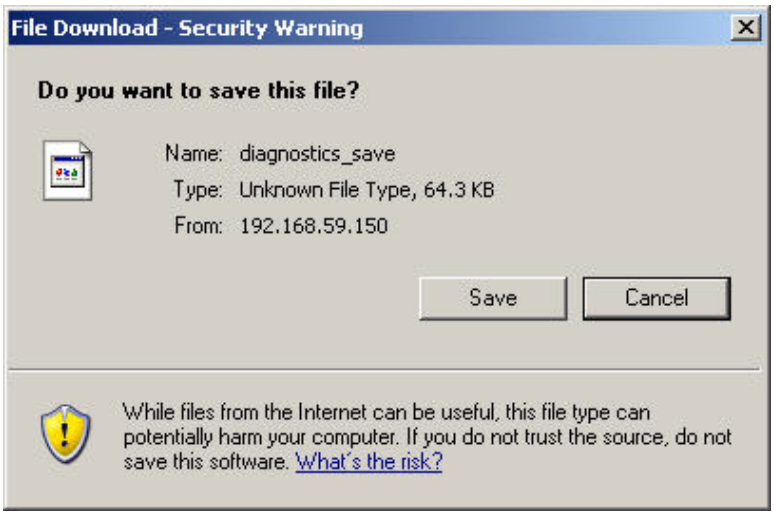

Abbildung 97: File Download (Dateidownload)

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.

Kapitel 13: Lokale KX II-Konsole

Lokale KX II-Konsole

Sie können am Serverschrank über den lokalen Port auf den Dominion KX II zugreifen und ihn verwalten. Dieser lokale Port bietet eine browserbasierte grafische Benutzeroberfläche, mit der Sie schnell und komfortabel zwischen den Servern wechseln können. Die lokale Dominion KX II-Konsole stellt eine direkte analoge Verbindung mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch. Die lokale KX II-Konsole bietet dieselben Verwaltungsfunktionen wie die Dominion KX II-Remotekonsole.

Die lokale Dominion KX II-Konsole unterstützt Tastaturen für folgende Sprachen: amerikanisches Englisch, britisches Englisch, Deutsch, Französisch, Japanisch, Koreanisch, vereinfachtes Chinesisch und traditionelles Chinesisch.

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

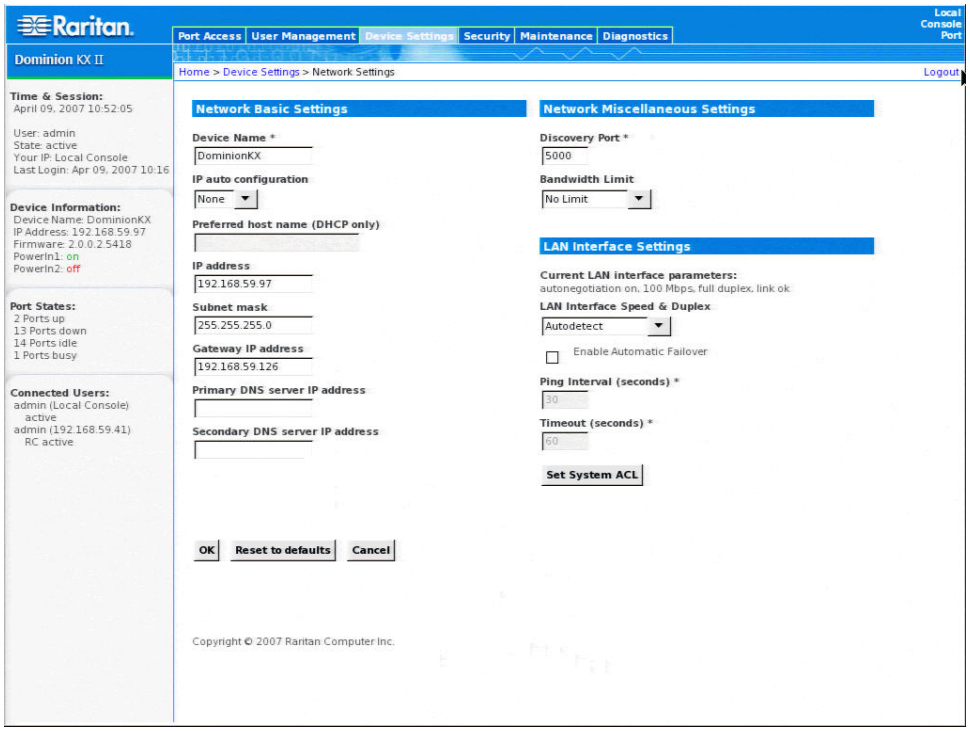

Abbildung 98: Lokale Dominion KX II-Konsole

Physische Anschlüsse

Die physischen Anschlüsse für die lokalen Ports finden Sie auf der Rückseite des Dominion KX II.

Abbildung 99: Lokale Ports am Dominion KX II

Monitor: Schließen Sie einen standardmäßigen MultiSync-VGA-Monitor am HD15-Videoport (weiblich) an.

Tastatur: Schließen Sie *entweder* eine standardmäßige PS/2-Tastatur am Mini-DIN6-Tastaturport (weiblich) *oder* eine standardmäßige USB-Tastatur an einem der USB Typ A-Ports (weiblich) an.

Maus: Schließen Sie *entweder* eine standardmäßige PS/2-Maus am Mini-DIN6-Mausport (weiblich) *oder* eine standardmäßige USB-Maus an einem der USB Typ A-Ports (weiblich) an.

Taste zum Zurücksetzen

Auf der Rückseite der Dominion KX II-Einheit befindet sich eine Taste zum Zurücksetzen. Sie ist etwas zurückgesetzt, damit sie nicht unbeabsichtigt gedrückt wird (Sie benötigen einen spitzen Gegenstand, um die Taste zu betätigen).

Abbildung 100: Taste zum Zurücksetzen (Rückseite der Einheit)

Welche Maßnahmen ergriffen werden, wenn die Taste zum Zurücksetzen gedrückt wird, legen Sie über die grafische Benutzeroberfläche fest. Weitere Informationen finden Sie unter Sicherheitseinstellungen, Verschlüsselung und Freigabe.

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.*

So setzen Sie die Einheit zurück:

1. Schalten Sie die Dominion KX II-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 die Dominion KX II-Einheit wieder ein.
4. Halten Sie die Taste weitere fünf bis zehn Sekunden gedrückt. Wenn die Einheit zurückgesetzt wurde, ertönen zwei kurze Tonsignale.

Starten der lokalen KX II-Konsole

Gleichzeitige Benutzer

Die lokale Dominion KX II-Konsole stellt einen unabhängigen Zugriffspfad zu den angeschlossenen Zielservern bereit. Die Verwendung der lokalen KX II-Konsole hindert andere Benutzer nicht daran, gleichzeitig eine Netzwerkverbindung herzustellen. Auch wenn Remotebenutzer mit dem Dominion KX II verbunden sind, können Sie gleichzeitig über die lokale Konsole im Serverschrank auf die Server zugreifen.

Sicherheit und Authentifizierung

Zur Verwendung der lokalen Dominion KX II-Konsole müssen Sie zunächst mit einem gültigen Benutzernamen und Kennwort authentifiziert werden. Der Dominion KX II stellt ein vollständig integriertes Authentifizierungs- und Sicherheitsschema bereit, unabhängig davon, ob Sie über das Netzwerk oder den lokalen Port auf das Gerät zugreifen. In beiden Fällen lässt der Dominion KX II nur den Zugriff auf die Server zu, für die ein Benutzer Zugriffsberechtigungen besitzt. (Weitere Informationen zum Festlegen des Serverzugriffs und der Sicherheitseinstellungen finden Sie unter Benutzerverwaltung.)

Wenn Ihr Dominion KX II für externe Authentifizierungsdienste (LDAP, RADIUS, Active Directory oder CC-SG von Raritan) 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 II-Konsole:

1. An den lokalen Ports auf der Rückseite der Dominion KX II-Einheit müssen eine Tastatur, eine Maus und eine Videoanzeige angeschlossen sein. Weitere Informationen zu den lokalen Portanschlüssen finden Sie unter Physische Anschlüsse.
2. Starten Sie die Dominion KX II-Einheit. Die Oberfläche der lokalen KX II-Konsole wird angezeigt.

Oberfläche der lokalen KX II-Konsole

Die Oberfläche der lokalen KX II-Konsole sieht fast genauso aus wie die Oberfläche der KX II-Remotekonsole. Auf die Unterschiede wird in diesem Benutzerhandbuch hingewiesen. Weitere Informationen finden Sie unter Benutzeroberflächen, KX II-Konsolen und Menüstruktur der KX II-Konsolen.

Verfügbare Auflösungen

Die lokale KX II-Konsole bietet folgende Auflösungen, um verschiedene Monitore zu unterstützen:

- 800x600
- 1024x768
- 1280x1024

Alle Auflösungen unterstützen eine Aktualisierungsfrequenz von 60 Hz und 75 Hz.

Zugreifen auf Zielserver

Serveranzeige

Nachdem Sie sich bei der lokalen KX II-Konsole angemeldet haben, wird die Seite **Port Access** (Portzugriff) angezeigt. Diese Seite enthält alle Dominion KX II-Ports, die angeschlossenen Zielserver sowie ihren Status und ihre Verfügbarkeit.

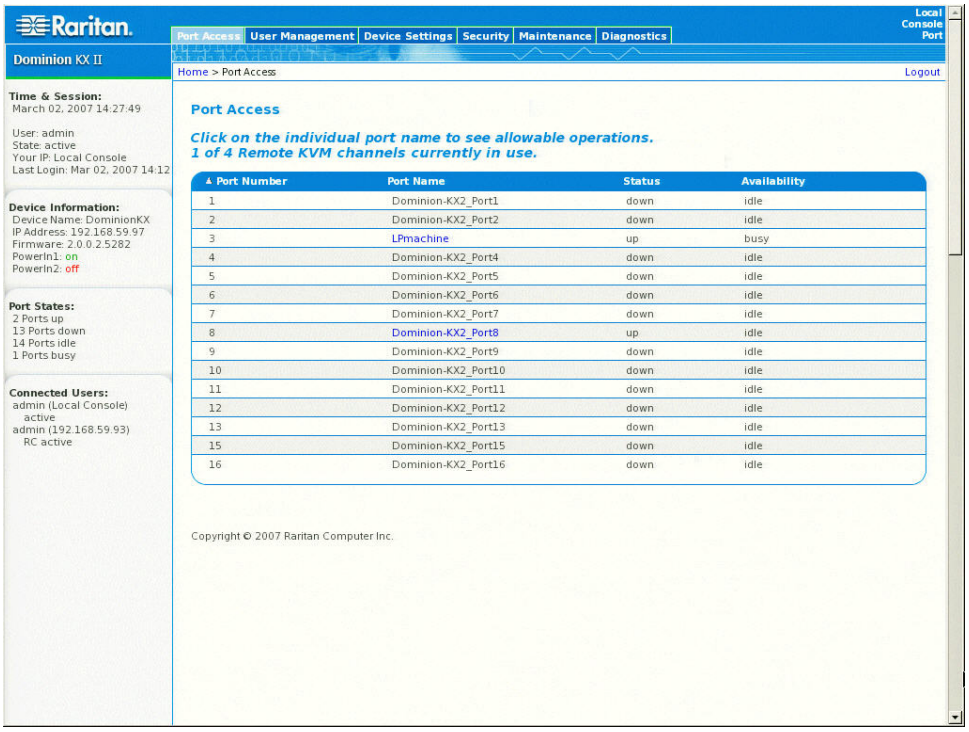

Abbildung 101: Zugriff über den lokalen Konsolenport

Die Zielserver sind zunächst nach Portnummer sortiert. Sie können die Anzeige nach einer der Spalten sortieren.

- **Port Number** (Portnummer): Die für die Dominion KX II-Einheit verfügbaren Ports werden beginnend mit 1 durchnummeriert. Mit Powerstrips verbundene Ports werden hier *nicht* aufgeführt, was zu Lücken in der Portnummernabfolge führt.
- **Port Name** (Portname): Der Name des Dominion KX II-Ports. Die Standardeinstellung **Dominion-KX2-Port#** können Sie jederzeit in einen aussagekräftigeren Namen ändern. Wenn Sie auf einen Portnamenlink klicken, wird das Menü **Port Action** (Portaktion) geöffnet. Weitere Informationen zu den verfügbaren Menüoptionen finden Sie unter Menü **Port Action** (Portaktion).
- **Status**: Der Status lautet entweder *Up* (Ein) oder *Down* (Aus).
- **Availability** (Verfügbarkeit): Gültige Werte sind *Idle* (Inaktiv), *Connected* (Verbunden), *Busy* (Verwendet) und *Unavailable* (Nicht verfügbar).

So ändern Sie die Sortierreihenfolge:

Klicken Sie auf die Spaltenüberschrift, nach der sortiert werden soll. Die Liste der Zielserver wird nach dieser Spalte sortiert.

Zugriffstasten

Da die Oberfläche der lokalen Dominion KX II-Konsole vollständig durch die Oberfläche des Zielservers ersetzt wird, auf den Sie zugreifen, müssen Sie über eine Zugriffstaste zwischen den beiden Oberflächen wechseln.

Über die Zugriffstaste für den lokalen Port können Sie schnell die Benutzeroberfläche der lokalen KX II-Konsole aufrufen, wenn gerade ein Zielserver angezeigt wird. Gemäß der Voreinstellung müssen Sie die Rollen-Taste zweimal kurz hintereinander drücken. Sie können jedoch (auf der Seite **Local Port Settings** [Lokale Porteinstellungen]) eine andere Tastenkombination als Zugriffstaste festlegen. Weitere Informationen finden Sie unter Local Port Settings (Lokale Porteinstellungen).

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). Die Videoanzeige wechselt zur Oberfläche des Zielservers.

Zurückkehren zur Oberfläche der lokalen KX II-Konsole

Wichtig: Die Standardzugriffstaste für die lokale KX II-Konsole besteht darin, die Rollen-Taste zweimal kurz hintereinander zu drücken. Diese Tastenkombination können Sie auf der Seite Local Port Settings (Lokale Porteinstellungen) ändern.

So kehren Sie vom Zielserver zur lokalen KX II-Konsole zurück:

Drücken Sie die Zugriffstaste (voreingestellt ist die Rollen-Taste) zweimal kurz hintereinander. Die Videoanzeige wechselt von der Oberfläche des Zielservers zur Oberfläche der lokalen Dominion KX II-Konsole.

Verwaltung über den lokalen Port

Der Dominion KX II kann entweder über die lokale KX II-Konsole oder die KX II-Remotekonsole verwaltet werden. Beachten Sie, dass die lokale KX II-Konsole auch Zugriff auf die folgenden Verwaltungsfunktionen bietet:

- Lokale Porteinstellungen
- Werksrückstellung

Hinweis: *Auf diese Funktionen können nur Benutzer mit Administratorrechten zugreifen.*

Lokale Porteinstellungen (nur lokale KX II-Konsole)

Auf der Seite **Local Port Settings** (Lokale Porteinstellungen) können Sie viele Einstellungen für die lokale KX II-Konsole anpassen. Dazu zählen die Tastatur, die Zugriffstaste für den lokalen Port, die Verzögerung beim Videowechsel, der Stromsparmodus, die Auflösungseinstellungen für die lokale Benutzeroberfläche sowie die lokale Benutzerauthentifizierung.

Hinweis: *Dieses Feature ist nur auf der lokalen Dominion KX II-Konsole verfügbar.*

So konfigurieren Sie die lokalen Porteinstellungen:

1. Wählen Sie **Device Settings > Local Port Settings** (Geräteeinstellungen > Lokale Porteinstellungen). Die Seite **Local Port Settings** (Lokale Porteinstellungen) wird angezeigt.

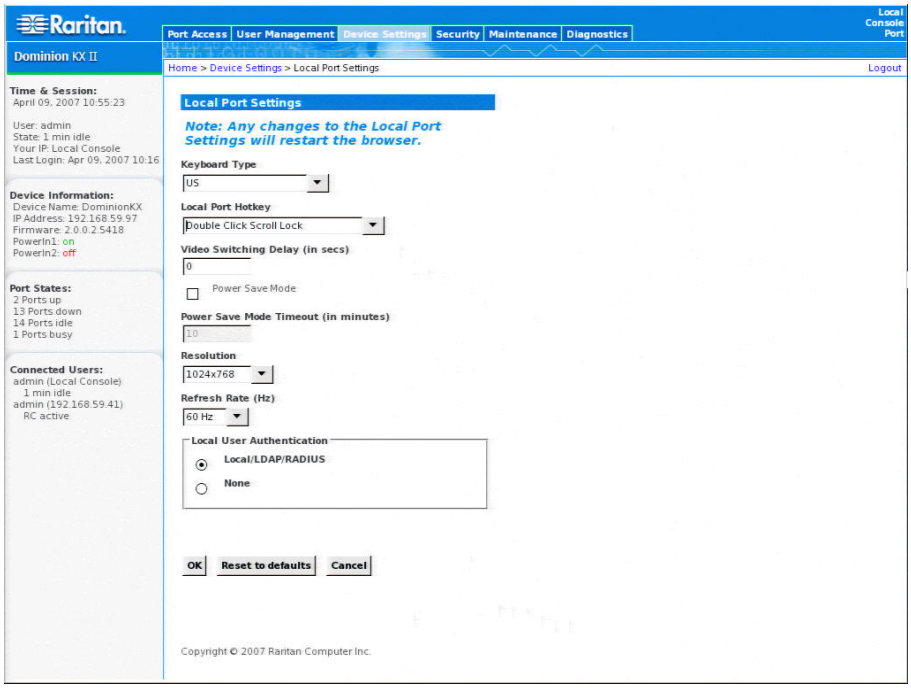

Abbildung 102: Lokale Porteinstellungen

2. Wählen Sie in der Dropdownliste **Keyboard Type** (Tastaturtyp) die entsprechende Option aus:
   - US
   - US/International (USA/International)
   - UK
   - **French** (Französisch)
   - **German** (Deutsch)
   - **JIS** (Japanese Industry Standard) (Japanisch [Japanischer Branchenstandard])
   - **Simplified Chinese** (Vereinfachtes Chinesisch)

- **Traditional Chinese** (Traditionelles Chinesisch)
- **Dubeolsik Hangul** (Korean) (Koreanisch)

3. Wählen Sie unter **Local Port Hotkey** eine Zugriffstaste für den lokalen Port aus. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen KX II-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 wählen.

HOTKEY (ZUGRIFFSTASTE):	ZU DRÜCKENDE TASTENKOMBINATION
Double Click Scroll Lock (Rollen-Taste zweimal drücken)	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Double Click Num Lock (Num-Feststelltaste zweimal drücken)	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.
Double Click Caps Lock (Feststelltaste zweimal drücken)	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Double Click Left Alt key (Linke Alt-Taste zweimal drücken)	Drücken Sie die linke Alt-Taste zweimal kurz hintereinander.
Double Click Left Shift key (Linke Umschalttaste zweimal drücken)	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Double Click Left Ctrl key (Linke Strg-Taste zweimal drücken)	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.

4. Legen Sie ggf. im Feld **Video Switching Delay** (Verzögerung beim Videowechsel) einen Wert zwischen 0 und 5 Sekunden fest. Üblicherweise wird der Wert 0 verwendet, wenn nicht mehr Zeit benötigt wird (manche Monitore benötigen mehr Zeit, um das Videobild zu wechseln).
5. 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.
6. Wählen Sie in der Dropdownliste **Resolution** die Auflösung für die lokale KX II-Konsole aus:
   - 800x600
   - 1024x768
   - 1280x1024
7. Wählen Sie in der Dropdownliste **Refresh Rate** die Aktualisierungsfrequenz aus:
   - 60 Hz
   - 75 Hz
8. Wählen Sie unter **Local User Authentication** eine Methode zur lokalen Benutzerauthentifizierung aus:
   - **Local/LDAP/RADIUS** (Lokal/LDAP/RADIUS): Diese Option wird empfohlen. Weitere Informationen zur Authentifizierung finden Sie unter Remoteauthentifizierung und Authentifizierung im Vergleich zur Autorisierung.
   - Sie benötigen keine Software. Der lokale Konsolenzugriff wird nicht authentifiziert. Diese Option ist *nur für sichere Umgebungen* empfehlenswert.
9. Klicken Sie auf **OK** (Senden).

So schließen Sie die Seite, ohne Ihre Änderungen zu speichern:

Klicken Sie auf **Cancel** (Abbrechen).

So stellen Sie die Standardwerte wieder her:

Klicken Sie auf **Reset to Defaults** (Auf Standardeinstellungen zurücksetzen).

Werksrückstellung (nur lokale KX II-Konsole)

Hinweis: *Dieses Feature ist nur auf der lokalen Dominion KX II-Konsole verfügbar.*

Der Dominion KX II bietet über die Benutzeroberfläche der lokalen Konsole verschiedene Rücksetzungsmodi.

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.*

So führen Sie eine Werksrückstellung durch:

1. Wählen Sie **Maintenance > Factory Reset** (Wartung > Werksrückstellung). Die Seite **Factory Reset** (Werksrückstellung) wird angezeigt.

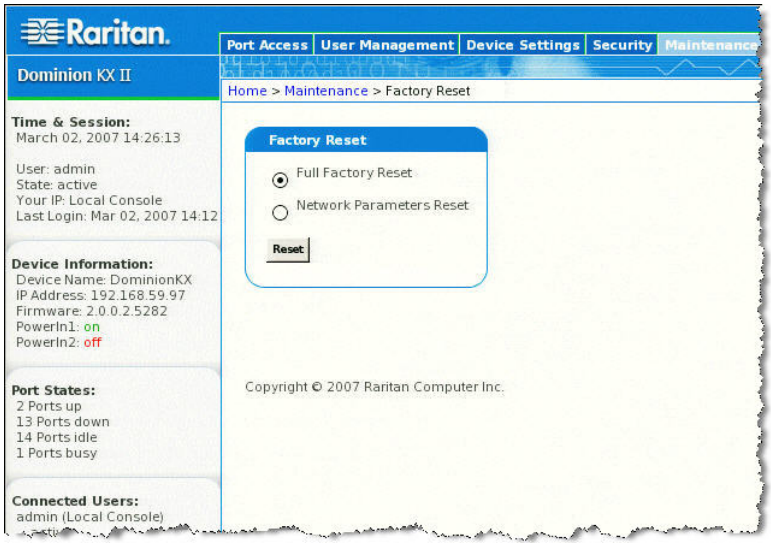

Abbildung 103: Werksrückstellung (nur lokale Konsole)

2. Wählen Sie die entsprechende Rückstellungsoption aus.
   - **Full Factory Reset** (Vollständige Werksrückstellung): Damit entfernen Sie die gesamte Konfiguration und setzen die Einheit 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** (Netzwerkparameterrückstellung): Damit setzen Sie die Netzwerkparameter der Einheit (die Sie über **Device Settings > Network Settings** [Geräteeinstellungen > Netzwerkeinstellungen] festgelegt haben) auf die Standardeinstellungen zurück:

Automatische IP-Konfiguration
IP-Adresse
Subnetzmaske
Gateway-IP-Adresse
IP-Adresse des primären DNS-Servers
IP-Adresse des sekundären DNS-Servers
Erkennungsport
Maximale Bandbreite
LAN-Schnittstellengeschwindigkeit & Duplex
Automatisches Failover
Pingintervall (Sekunden)
Zeitlimit (Sekunden)

   Da hierbei alle Netzwerkeinstellungen verloren gehen, werden Sie aufgefordert, diesen Vorgang zu bestätigen.
3. Klicken Sie auf **Reset** (Zurücksetzen), um fortzufahren. Sie werden aufgefordert, die Werksrückstellung zu bestätigen.
4. Klicken Sie auf die Schaltfläche **Really Reset** (Wirklich zurücksetzen), um fortzufahren. Nach Abschluss dieses Vorgangs wird die Dominion KX II-Einheit automatisch neu gestartet.

Kapitel 14: CC UnManage

Überblick

Wenn ein Dominion KX II-Gerät über CommandCenter Secure Gateway gesteuert wird und Sie versuchen, über die Dominion KX II-Remotekonsole direkt auf das Gerät zuzugreifen, wird die folgende Meldung angezeigt (nach Eingabe eines gültigen Benutzernamens und Kennworts):

*Abbildung 104: Meldung **Device Managed by CC-SG** (Gerät wird von CC-SG verwaltet)*

Aufheben der CC-SG-Verwaltung des Dominion KX II

Sie können nur direkt auf das Gerät zugreifen, wenn die CC-SG-Steuerung des Dominion KX II aufgehoben wird. Wenn der KX II jedoch keine Heartbeat-Nachrichten von CommandCenter empfängt (z. B. weil sich CommandCenter nicht im Netzwerk befindet), können Sie die CC-SG-Steuerung des KX II aufheben, um auf das Gerät zuzugreifen. Dazu dient das Feature **CC UnManage**.

***Hinweis:** Für dieses Feature sind Wartungsrechte erforderlich.*

Wenn keine Heartbeat-Nachrichten empfangen werden, wird die folgende Meldung angezeigt, sobald Sie versuchen, direkt auf das Gerät zuzugreifen:

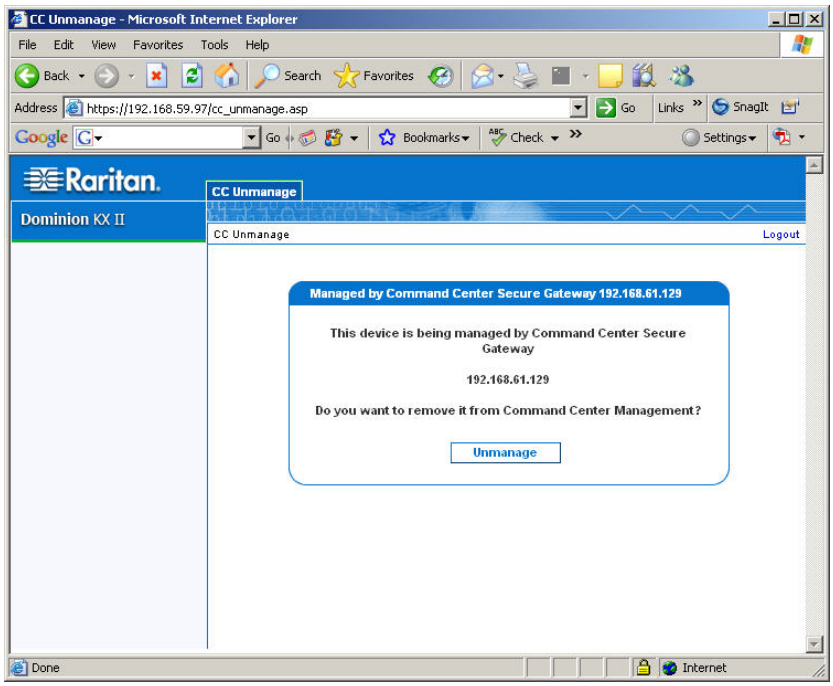

Abbildung 105: Aufheben der CC-SG-Verwaltung

So heben Sie die CC-SG-Verwaltung des Geräts auf (Feature CC UnManage):

1. Klicken Sie auf die Schaltfläche **Unmanage** (Verwaltung aufheben). Sie werden aufgefordert, die Aktion zu bestätigen.

Abbildung 106: Bestätigen von CC UnManage

2. Klicken Sie auf die Schaltfläche **Really Unmanage** (Verwaltung wirklich aufheben). Es wird eine Meldung mit der Bestätigung angezeigt, dass die CC-Verwaltung des Geräts aufgehoben wurde.

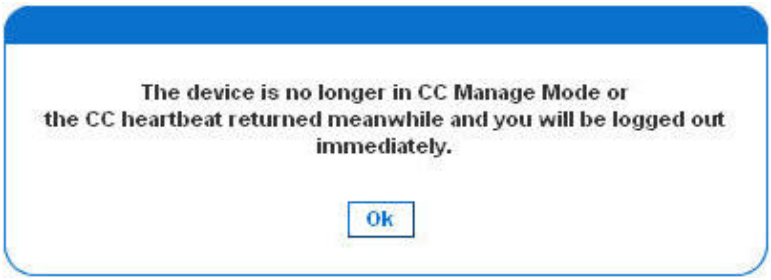

Abbildung 107: CC-Verwaltung des Geräts aufgehoben

3. Klicken Sie auf **OK** (Senden). Die Seite Port Access (Portzugriff) wird angezeigt.

Anhang A: Technische Daten

Umgebungsanforderungen

BETRIEB	
Temperatur	0℃ - 40℃ (32℉ - 104℉)
Luftfeuchtigkeit	20 % bis 85 % relative Luftfeuchtigkeit
Höhe über NN	Nicht zutreffend
Erschütterung	5-55-5 HZ, 0,38 mm, 1 Minute pro Zyklus; 30 Minuten für jede Achse (X, Y, Z)
Stoß	Nicht zutreffend
LAGERUNG	
Temperatur	0℃ - 50℃ (32℉ -122℉)
Luftfeuchtigkeit	10 % bis 90 % relative Luftfeuchtigkeit
Höhe über NN	Nicht zutreffend
Erschütterung	5-55-5 HZ, 0,38 mm, 1 Minute pro Zyklus; 30 Minuten für jede Achse (X, Y, Z)
Stoß	Nicht zutreffend

Physische Spezifikationen

TEILE-NUMMER	DKX2-116	DKX2-132	DKX2-216	DKX2-232	DKX2-416	DKX2-432
Produktbeschreibung	Dominion KX II mit 16 Ports, Netzwerk- und lokaler Portzugriff über einen Kanal; virtuelle Medien, zwei Netzteile	Dominion KX II mit 32 Ports, Netzwerk- und lokaler Portzugriff über einen Kanal; virtuelle Medien, zwei Netzteile	Dominion KX II mit 16 Ports, Netzwerk- und lokaler Portzugriff über zwei Kanäle; virtuelle Medien, zwei Netzteile	Dominion KX II mit 32 Ports, Netzwerk- und lokaler Portzugriff über zwei Kanäle; virtuelle Medien, zwei Netzteile	Dominion KX II mit 16 Ports, Netzwerk- und lokaler Portzugriff über vier Kanäle; virtuelle Medien, zwei Netzteile	Dominion KX II mit 32 Ports, Netzwerk- und lokaler Portzugriff über vier Kanäle; virtuelle Medien, zwei Netzteile
Gewicht	8,95 lbs 3,9 kg	9,0 lbs 4,1 kg	8,59 lbs 3,9 kg	9,0 lbs 4,1 kg	9,04 lbs 4,1 kg	9,48 lbs 4,3 kg
Produktabmessungen (b x t x h)	1,75 Zoll x 17,32 Zoll x 11,4 Zoll 44 mm x 439 mm x 290 mm	1,75 Zoll x 17,32 Zoll x 11,4 Zoll 44 mm x 439 mm x 290 mm	1,75 Zoll x 17,32 Zoll x 11,4 Zoll 44 mm x 439 mm x 290 mm	1,75 Zoll x 17,32 Zoll x 11,4 Zoll 44 mm x 439 mm x 290 mm	1,75 Zoll x 17,32 Zoll x 11,4 Zoll 44 mm x 439 mm x 290 mm	1,75 Zoll x 17,32 Zoll x 11,4 Zoll 44 mm x 439 mm x 290 mm
Liefergewicht	14,85 lbs 6,7 kg	14,9 lbs 6,8 kg	14,49 lbs 6,6 kg	14,9 lbs 6,8 kg	14,94 lbs 6,8 kg	15,38 lbs 7,0 kg
Lieferabmessungen (b x t x h)	22 Zoll x 16,6 Zoll x 6,5 Zoll 559 mm x 422 mm x 165 mm	22 Zoll x 16,6 Zoll x 6,5 Zoll 559 mm x 422 mm x 165 mm	22 Zoll x 16,6 Zoll x 6,5 Zoll 559 mm x 422 mm x 165 mm	22 Zoll x 16,6 Zoll x 6,5 Zoll 559 mm x 422 mm x 165 mm	22 Zoll x 16,6 Zoll x 6,5 Zoll 559 mm x 422 mm x 165 mm	22 Zoll x 16,6 Zoll x 6,5 Zoll 559 mm x 422 mm x 165 mm
UPC-Code	785813624055	785813624079	785813624086	785813625021	785813625359	785813625380
Stromversorgung	Zwei Netzteile 100/240 V 50/60 Hz 0,6 A 25,4 Watt	Zwei Netzteile 100/240 V 50/60 Hz 0,6 A 26 Watt	Zwei Netzteile 100/240 V 50/60 Hz 0,6 A 26,3 Watt	Zwei Netzteile 100/240 V 50/60 Hz 0,6 A 27 Watt	Zwei Netzteile 100/240 V 50/60 Hz 1 A 62 Watt	Zwei Netzteile 100/240 V 50/60 Hz 1 A 64 Watt

Stromversorgung

PARAMETER		WERT
Eingang		
	Frequenz	50/60 Hz
	Spannungsbereich	100/240 VAC
	Maximaler Effektivstrom	0,6 A
	Wechselstrom-Betriebsbereich	100 bis 240 VAC (+-10 %), 47 bis 63 Hz
Ausgang		
	+5 VDC, +12 VDC	Nicht zutreffend
	-5 VDC, -12 VDC	Nicht zutreffend
Max. Gleichstrom-Leistungsausgang		Nicht zutreffend
	Max. Wechselstrom-Leistung	Nicht zutreffend
	Max. Wärmeabfuhr	Nicht zutreffend
Voltampere-Leistung		Nicht zutreffend

Computer Interface Modules (CIMs)

TEILE-NUMMER	D2CIM-VUSB	DCIM-PS2	DCIM-USB	DCIM-SUSB
Produktbeschreibung	Dominion KX II-CIM [USB-Port mit virtuellen Medien]	Dominion KX I- und II-CIM [PS/2-Port]	Dominion KX I- und II-CIM [USB-Port]	Dominion KX I- und II-CIM [USB-Port für Sun]
Produktgewicht	0,2 lbs	0,2 lbs	0,2 lbs	0,2 lbs
Produktabmessungen (b x t x h)	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	1,3 Zoll x 3,0 Zoll x 0,6 Zoll
Liefergewicht	0,2 lbs	0,2 lbs	0,2 lbs	0,2 lbs
Lieferabmessungen (b x t x h)	7,2 Zoll x 9 Zoll x 0,6 Zoll	7,2 Zoll x 9 Zoll x 0,6 Zoll	7,2 Zoll x 9 Zoll x 0,6 Zoll	7,2 Zoll x 9 Zoll x 0,6 Zoll
UPC-Code	785813332004	785813338532	785813338518	785813338556

TEILE-NUMMER	DCIM-SUN	D2CIM-PWR	D2CIM-VUSB-32PAC	D2CIM-VUSB - 64PAC
Produktbeschreibung	Dominion KX I- und II-CIM [Sun-Port, HD15-Video]	Dominion KX II-CIM für Remotepowerstrips	Großpaket mit 32 D2CIM-VUSB	Großpaket mit 64 D2CIM-VUSB
Produktgewicht	0,2 lbs	0,2 lbs	6,4 lbs 2,72 kg	12,8 lbs 5,4 kg
Produktabmessungen (b x t x h)	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	(1,3 Zoll x 3,0 Zoll x 0,6 Zoll)*32 [(25,4 mm x 76,2 mm x 15,2 mm)*32]	(1,3 Zoll x 3,0 Zoll x 0,6 Zoll)*64 [(25,4 mm x 76,2 mm x 15,2 mm)*64]
Liefergewicht	0,2 lbs	0,2 lbs	8,01 lbs 3,63 kg	18,13 lbs 8,16 kg
Lieferabmessungen (b x t x h)	7,2 Zoll x 9 Zoll x 0,6 Zoll	7,2 Zoll x 9 Zoll x 0,6 Zoll	21,65 Zoll x 12,20 Zoll x 4,33 Zoll 533,4 mm x 304,8 mm x 101,6 mm	22,64 Zoll x 9,45 Zoll x 12,99 Zoll 558,8 mm x 228,6 mm x 304,8 mm
UPC-Code	785813338549	785813332011	785813332028	785813332035

Remoteverbindung

Netzwerk: 10BASE-T-, 100BASE-T- und 1000BASE-T (Gigabit)-Ethernet
Protokolle: TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP

KVM-Eigenschaften

Tastatur: PS/2 oder USB
Maus: PS/2 oder USB
Video: VGA

Verwendete TCP- und UDP-Ports

- **HTTP, Port 80**: Alle vom Dominion KX II über HTTP (Port 80) empfangenen Anforderungen werden zur Gewährleistung der Sicherheit automatisch an HTTPS weitergeleitet. Der Dominion KX II beantwortet Anforderungen aus Gründen der Benutzerfreundlichkeit über Port 80. Auf diese Weise müssen Benutzer für den Zugriff auf den Dominion KX II im URL-Feld nicht explizit „https://“ eingeben. Die Sicherheit ist jedoch vollständig gewährleistet.
- **HTTPS, Port 443**: Dieser Port dient nur einem Zweck: zum Senden der über das Web zugänglichen Dominion KX II-Clients (KX II-Konsolen, MPC) an den Benutzer. Über diesen Port erfolgt keine andere Kommunikation. Wenn Sie die Webzugriffsfunktionen des Dominion KX II nicht verwenden möchten und die Verwendung der Clientsoftware auf der CD-ROM bevorzugen, können Sie den Zugriff auf Port 443 über Ihre Firewall untersagen. Die Funktionsweise des Dominion KX II wird dadurch nicht beeinträchtigt.
- **Dominion KX II-Protokoll (Raritan KVM-über-IP), konfigurierbarer Port 5000**: Mit Ausnahme der oben beschriebenen Ports wird die gesamte Kommunikation zum Dominion KX II über nur einen konfigurierbaren TCP-Port übertragen. Standardmäßig ist der Port 5000 eingestellt. Sie können jedoch einen anderen TCP-Port Ihrer Wahl konfigurieren (mit Ausnahme von 80 und 443). Informationen zum Konfigurieren dieser Einstellung finden Sie unter Netzwerkeinstellungen.
- **SNTP (Zeitserver) über den konfigurierbaren UDP-Port 123 (optional)**: Der Dominion KX II 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.
- **LDAP über die konfigurierbaren Ports 389 und 636 (optional)**: Wenn der Dominion KX II zur Remoteauthentifizierung von Benutzeranmeldungen über das LDAP-Protokoll konfiguriert ist, werden die Ports 389 und 636 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden.
- **RADIUS über den konfigurierbaren Port 1812 (optional)**: Wenn der Dominion KX II zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist, wird der Port 1812 oder 1813 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden.
- **RADIUS-Kontoführung über den konfigurierbaren Port 1813**: Wenn der Dominion KX II 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 Dominion KX II 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 (optional):** Port 161 wird für eingehende/ausgehende SNMP-Lese- und Schreiboperationen, Port 162 für ausgehenden Datenverkehr für SNMP-Traps verwendet.
- **UDP-Port 21**: Port 21 wird für die Befehlszeilenschnittstelle des Dominion KX II verwendet (wenn Sie mit dem technischen Kundendienst von Raritan zusammenarbeiten).

Verbindungsentfernung zum Zielserver und Videoauflösung

Die maximal unterstützte Entfernung hängt von mehreren Faktoren ab. Dazu gehören der Typ/die Qualität des CAT5-Kabels, der Servertyp und -hersteller, der Videotreiber 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:

VIDEOAUFLÖSUNG	AKTUALISIERUNGSFREQUENZ	MAXIMALE ENTFERNUNG
1600x1200	60	15 m
1280x1024	60	30 m
1024x768	60	45 m

Die Verwendung von Paragon CIMs ermöglicht keine größere Entfernung zwischen dem Dominion KX II und dem Zielserver.

Aufgrund der Vielzahl an Serverherstellern und -typen, Betriebssystemversionen, Videotreiber usw. sowie die subjektive Auffassung von Videoqualität kann Raritan nicht für die Leistung bei allen Entfernungen in allen Umgebungen garantieren.

Informationen zu den vom Dominion KX II unterstützten Videoauflösungen finden Sie unter Unterstützte Videoauflösungen.

Anhang B: Aktualisieren des LDAP-Schemas

Hinweis: *Die in diesem Kapitel beschriebenen Verfahren sollten nur von erfahrenen Benutzern durchgeführt werden.*

Zurückgeben von Benutzergruppeninformationen

Verwenden Sie die Informationen in diesem Kapitel, um Benutzergruppeninformationen zurückzugeben (und die Autorisierung zu unterstützen), sobald die Authentifizierung erfolgreich war.

Von LDAP

Wenn eine LDAP-Authentifizierung erfolgreich ist, bestimmt der Dominion KX II 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: Zeichenfolge
```

Dies erfordert ggf. eine Schemaerweiterung auf Ihrem LDAP-Server. Bitten Sie den Administrator des Authentifizierungsservers, dieses Attribut zu aktivieren.

Darüber hinaus wird 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-Schemas. Nähere Informationen hierzu entnehmen Sie der Microsoft-Dokumentation.

1. Installieren Sie das Schema-Plug-in für Active Directory – Anweisungen hierzu finden Sie in der Microsoft Active Directory-Dokumentation.
2. Starten Sie Active Directory Console, und wählen Sie **Active Directory Schema** (Verzeichnisschema).

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.

1. Klicken Sie mit der rechten Maustaste auf den Stammknoten **Active Directory Schema** (Verzeichnisschema) im linken Fensterabschnitt, und klicken Sie anschließend auf **Operations Master** (Betriebsmaster).
2. Aktivieren Sie das Kontrollkästchen **The Schema may be modified on this Domain Controller** (Schema kann auf diesem Domänencontroller geändert werden).
3. Klicken Sie auf **OK** (Senden).

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** (Active Directory-Schema).
2. Klicken Sie im linken Fensterabschnitt mit der rechten Maustaste auf **Attributes** (Attribute).
3. Klicken Sie auf **New** (Neu), und wählen Sie **Attributes** (Attribute) aus. Klicken Sie im angezeigten Hinweisfenster auf **Continue** (Weiter). Das Fenster **Create New Attribute** (Neues Attribut erstellen) wird geöffnet.

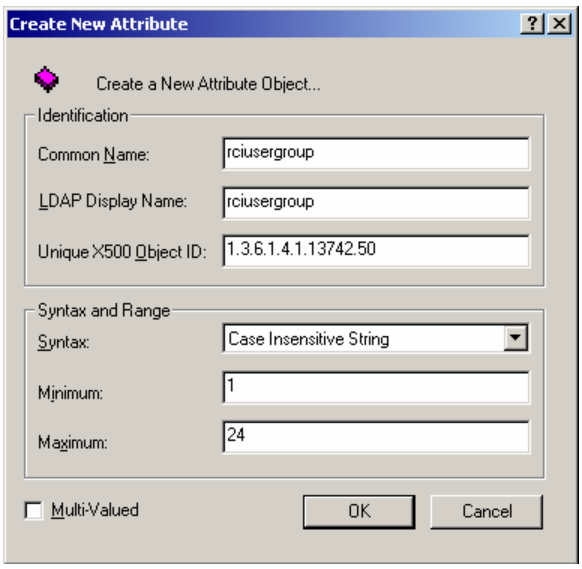

Abbildung 108: Neues Attribut erstellen

4. Geben Sie ins Feld **Common Name** (Allgemeiner Name) den Wert **rciusergroup** ein.
5. Geben Sie ins Feld **LDAP Display Name** (LDAP-Anzeigename) den Wert **rciusergroup** ein.
6. Geben Sie ins Feld **Unique x5000 Object ID** (Eindeutige X500-OID) den Wert **1.3.6.1.4.1.13742.50** ein.
7. Klicken Sie auf die Dropdownliste **Syntax**, und wählen Sie **Case Insensitive String** (Groß-/Kleinschreibung nicht beachten).
8. Geben Sie ins Feld **Minimum** den Wert **1** ein.
9. Geben Sie ins Feld **Maximum** den Wert **24** ein.
10. Klicken Sie zum Erstellen des neuen Attributs auf **OK**.

Hinzufügen von Attributen zur Klasse

1. Klicken Sie im linken Fensterabschnitt auf **Classes** (Klassen).
2. Suchen Sie im rechten Fensterabschnitt den Wert **user** (Benutzer), und klicken Sie darauf mit der rechten Maustaste.
3. Wählen Sie im Kontextmenü den Befehl **Properties** (Eigenschaften). Das Fenster **User Properties** (Benutzereigenschaften) wird geöffnet.
4. Klicken Sie auf die Registerkarte **Attributes** (Attribute).
5. Klicken Sie auf **Add** (Senden).
6. Wählen Sie in der Liste **Schema Object** (Schemaobjekt) den Eintrag **rciusergroup**.

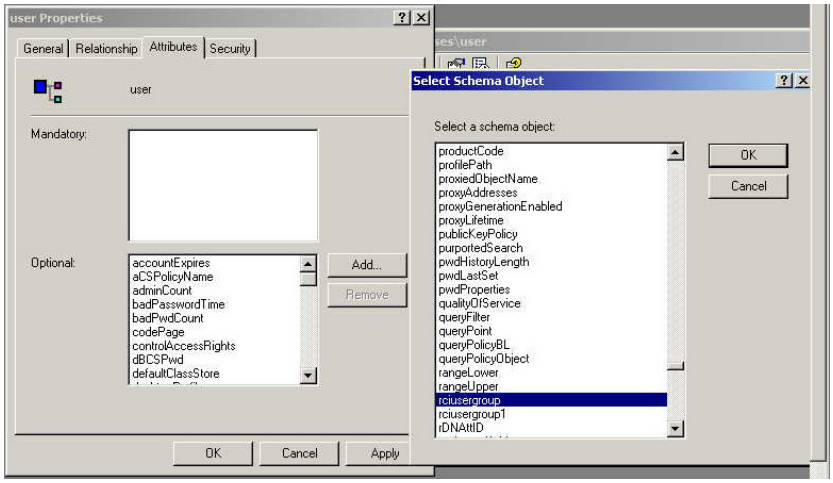

Abbildung 109: Hinzufügen des Attributs zur Klasse

7. Klicken Sie auf **OK** (Senden).
8. Klicken Sie auf **OK** (Senden).

Aktualisieren des Schemacache

1. Klicken Sie im linken Fensterabschnitt mit der rechten Maustaste auf **Active Directory Schema** (Active Directory-Schema), und wählen Sie im Kontextmenü den Befehl **Reload the Schema** (Schema neu laden).
2. Minimieren Sie die Active Directory-Schema-MMC-Konsole.

Bearbeiten von RCI-Benutzergruppenattributen für Benutzermitglieder

Verwenden Sie zum Ausführen des Active Directory-Skripts auf einem Server unter Windows 2003 das von Microsoft bereitgestellte Skript. 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. Weitere Informationen hierzu finden Sie auf der Website von Microsoft: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/ebca3324-5427-471a-bc19-9aa1decd3d40.mspx.

So bearbeiten Sie die einzelnen Benutzerattribute innerhalb der Gruppe **rciusergroup:**

1. Klicken Sie im Windows-Startmenü auf **Ausführen.**

2. Geben Sie **regsvr adsiedit.msc** ein. Das Fenster **ADSI Edit** (ADSI-Bearbeitung) wird angezeigt.

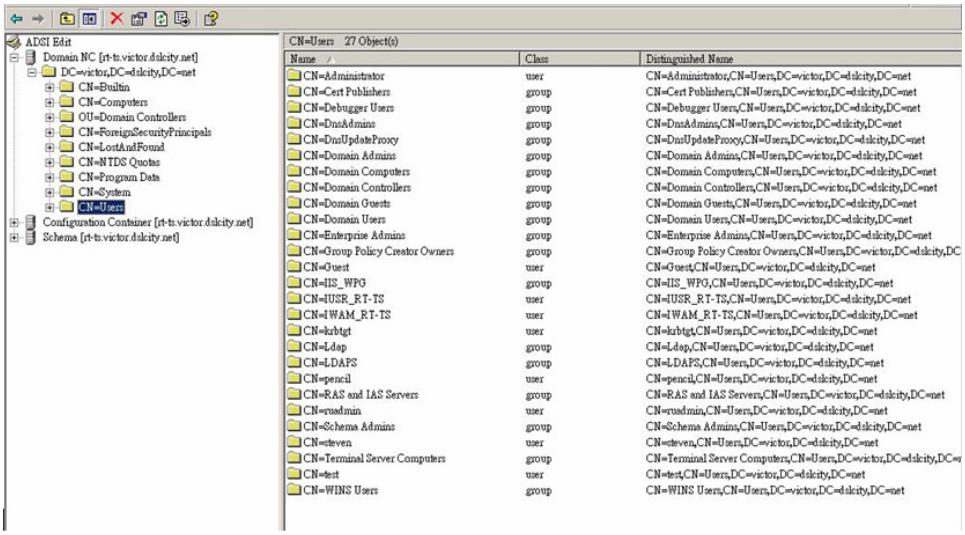

Abbildung 110: ADSI-Bearbeitung

3. Klicken Sie im rechten Fensterbereich auf den Ordner **CN=User** (CN=Benutzer).
4. Navigieren Sie im rechten Fensterbereich zu dem Namen des Benutzers, dessen Eigenschaften geändert werden sollen. Rechtsklicken Sie auf den Benutzernamen, und wählen Sie **Properties** (Eigenschaften).
5. Klicken Sie auf die Registerkarte **Attributes** (Attribute).
6. Klicken Sie auf den Dropdownpfeil von **Select a property to view** (Anzuzeigende Eigenschaft auswählen), und wählen Sie den Listeneintrag **rciusergroup** aus.

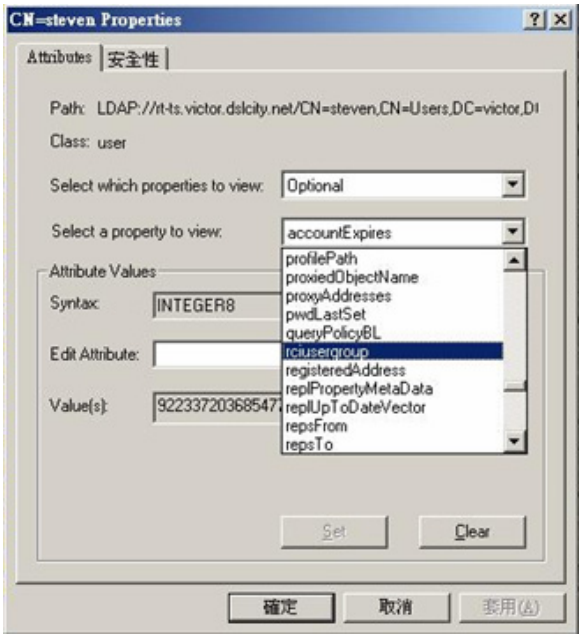

Abbildung 111: Benutzereigenschaften

7. Geben Sie im Fensterbereich **Attribute Values** (Attributwerte) im Feld **Edit Attribute** (Attribut bearbeiten) den Benutzernamen ein, der für RRC zurückgegeben werden soll.

Abbildung 112: Attribut bearbeiten (Hinzufügen des Benutzers zur KX II-Gruppe)

8. Klicken Sie auf **Set** (Festlegen).
9. Klicken Sie auf **OK**.

Anhang C: Häufig gestellte Fragen (FAQs)

Allgemeine Fragen

FRAGE	ANTWORT
Was ist Dominion KX II?	Der Dominion KX II ist ein digitaler KVM-Switch (Tastatur, Video, Maus) der zweiten Generation, der IT-Administratoren den Zugriff auf 16, 32 oder 64* Server und deren Steuerung über das Netzwerk mit Funktionen auf BIOS-Ebene erlaubt. Der Dominion KX II 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 Platz sparende Dominion KX II die gleiche Funktionalität, den gleichen Bedienkomfort und die gleiche Kostenersparnis wie herkömmliche analoge KVM-Switches. Der Dominion KX II 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 ermöglicht.
Inwiefern unterscheidet sich Dominion KX II von Remotesteuerungs-software?	Beim Remoteeinsatz des Dominion KX II gleicht die Schnittstelle auf den ersten Blick Software zur Remotesteuerung wie pcAnywhere™, Windows®-Terminaldienste/Remote Desktop, VNC usw. Dominion KX II ist allerdings keine Software-, sondern eine Hardwarelösung und somit leistungsfähiger: • Betriebssystem- und hardwareunabhängig – Der Dominion KX II kann zur Verwaltung von Servern mit vielen beliebten Betriebssystemen, darunter Intel®, Sun®, PowerPC mit Windows, Linux®, Solaris™ usw., verwendet werden. • Statusunabhängig/Agent-frei – Der Dominion KX II 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 II verwaltet werden. • Zugriff auf BIOS-Ebene – Dominion KX II 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.
Welche neuen Features hat der Dominion KX II im Vergleich zum KX I?	Der Dominion KX II bietet viele interessante neue Features wie virtuelle Medien, zwei Netzteile, duales Gigabit-Ethernet, allgemeine webbasierte Benutzeroberflächen, einen lokalen Port der nächsten Generation usw.

FRAGE	ANTWORT
Wie funktioniert die Migration vom Dominion KX I auf den Dominion KX II?	Grundsätzlich können Sie als KX I-Kunde Ihre vorhandenen Switches noch viele Jahre nutzen. Wenn Ihr Rechenzentrum wächst, können Sie die neuen KX II-Modelle erwerben und einsetzen. Die zentrale Verwaltungsanwendung von Raritan, CommandCenter® Secure Gateway, und der Multi-Platform-Client (MPC) unterstützen sowohl KX I- als auch KX II-Switches nahtlos.
Funktionieren meine bisherigen KX I-CIMs mit dem Dominion KX II-Switch?	Ja, vorhandene KX I-CIMs funktionieren mit dem Dominion KX II-Switch. Darüber hinaus können auch ausgewählte Paragon CIMs damit eingesetzt werden. Dies erleichtert Paragon I-Kunden, die zu KVM-über-IP wechseln möchten, die Migration zu KX II.
Kann der Dominion KX II in einem Gestell montiert werden?	Ja. Der Dominion KX II 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 II?	Der Dominion KX II ist nur 1U hoch (eine Ausnahme bildet das Modell KX2-464*, welches 2U hoch ist), passt in ein 19-Zoll-Standardgestell und ist nur 11,4 Zoll (29 cm) tief.

* KX2-464 ist ab dem 2. Quartal 2007 verfügbar

Remotezugriff

<table>
<tr><th>FRAGE</th><th>ANTWORT</th></tr>
<tr><td>Wie viele Benutzer erhalten mit einem Dominion KX II Remotezugriff auf Server?</td><td>Die Dominion KX II-Modelle 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 DKX2-116 können bis zu acht Remotebenutzer auf einen einzelnen Zielserver zugreifen und diesen steuern. Bei Zwei-Kanal-Geräten wie dem DKX2-216 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 auf ähnliche Weise bis zu acht Benutzer pro Kanal auf vier Server zugreifen und diese steuern. Dies ergibt insgesamt 32 (8 x 4) Benutzer.</td></tr>
<tr><td>Können zwei Personen gleichzeitig denselben Server anzeigen?</td><td>Ja, bis zu acht Personen können gleichzeitig auf einen einzelnen Server zugreifen und diesen steuern.</td></tr>
<tr><td>Können zwei Personen auf denselben Server zugreifen (einer an einem entfernten Standort und einer über den lokalen Port)?</td><td>Ja, der lokale Port ist von den Remoteports vollständig unabhängig. Der lokale Port kann mithilfe des Features PC-Share (PC-Freigabe) auf denselben Server zugreifen.</td></tr>
<tr><td>Welche Hardware-, Software- oder Netzwerkkonfiguration ist für den Zugriff auf Dominion KX II über einen Client erforderlich?</td><td>Da der Dominion KX II über das Web verfügbar ist, muss auf Clients keine spezielle Software für den Zugriff installiert werden. (Für den Zugriff auf den Dominion KX II mittels Modem ist ein optionaler Client auf Raritan.com verfügbar.)

Der Zugriff auf den Dominion KX II ist mit einem gängigen Web-browser möglich. Hierzu zählen: Internet Explorer, Mozilla™ und Firefox. Dank des Java-basierten Multi-Plattform-Clients (MPC) von Raritan und des neuen Virtual KVM Client™ ist der Zugriff auf den Dominion KX II nun von Windows-, Linux-, Sun Solaris- und Macintosh®-Desktops aus möglich.

Dominion KX II-Administratoren können mithilfe einer praktischen browserbasierten Oberfläche auch die Remoteverwaltung von Servern durchführen (Kennwörter und Sicherheit einrichten, Server umbenennen, IP-Adressen ändern usw.).</td></tr>
<tr><td>Wie groß ist das für den Zugriff auf den Dominion KX II verwendete Applet? Wie lange dauert das Herunterladen?</td><td>Das Applet Virtual KVM Client für den Zugriff auf den Dominion KX II ist etwa 500 KB groß. Die folgende Tabelle zeigt, wie lange das Herunterladen des Applets bei verschiedenen Netzwerkgeschwindig-keiten dauert:
<table>
<tr><td>100 Mbit/s</td><td>Theoretisch 100 Mbit</td><td>0,05 Sekunden</td></tr>
<tr><td>60 Mbit/s</td><td>Beinahe 100 Mbit</td><td>0,08 Sekunden</td></tr>
<tr><td>10 Mbit/s</td><td>Theoretisch 10 Mbit</td><td>0,4 Sekunden</td></tr>
<tr><td>6 Mbit/s</td><td>Beinahe 10 Mbit</td><td>0,8 Sekunden</td></tr>
<tr><td>512 Kbit/s</td><td>Kabelmodem-Downloadgeschwindigkeit (normal)</td><td>8 Sekunden</td></tr>
</table>
</td></tr>
</table>

FRAGE	ANTWORT
Wie greife ich auf die an einem Dominion KX II angeschlossenen Server zu, wenn das Netzwerk nicht verfügbar ist?	Der Dominion KX II besitzt einen dedizierten Modemport für den Anschluss eines externen Modems. Mit einem extern angeschlossenen Modem ist der Remotezugriff auf Server auch bei einem Netzwerkausfall möglich. Darüber hinaus können Sie mit den lokalen Ports des Dominion KX II jederzeit und unabhängig vom Netzwerkzustand über das Gestell auf die Server zugreifen.
Gibt es einen Client für andere Betriebssysteme als Windows?	Ja. Sowohl der Virtual KVM Client als auch der Multi-Platform-Client (MPC) ermöglichen es Benutzern, die nicht über ein Windows-Betriebssystem verfügen, über die Dominion KX I- und KX II-Switches Verbindungen mit den Zielservern herzustellen. MPC kann über den Webbrowser oder als eigenständige Version betrieben werden. Weitere Informationen finden Sie unter Virtual KVM Client und im *Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan und Raritan Remote Client (RRC)*.
Meine Modem-verbindung wurde getrennt, und ich erhielt eine Meldung mit dem Hinweis, dass ein unerwarteter Verbindungsfehler aufgetreten ist und die Verbindung abgebrochen wurde. Was kann ich tun?	Dieses Problem könnte damit zusammenhängen, dass zwischen den Verbindungsversuchen per Modem ein zu geringer Zeitabstand bestand. Starten Sie das KX-Gerät sowie das Modem neu, und warten Sie künftig mindestens zwei (2) Minuten, bis Sie einen erneuten Verbindungsversuch unternehmen.
Während einer Sitzung des Virtual KVM Client klemmt manchmal die **Alt**-Taste. Was kann ich in diesem Fall tun?	Dieses Problem kann auftreten, wenn die **Alt**-Taste gedrückt und nicht losgelassen wird. Wenn bei gedrückter **Alt**-Taste z. B. die Leertaste gedrückt wird, kann der Fokus vom Zielserver zum Client-PC wechseln. Das lokale Betriebssystem interpretiert diese Tastenkombination und löst die Aktion für die Tastenkombination im aktiven Fenster aus (auf dem Client-PC).

Universelle virtuelle Medien

FRAGE	ANTWORT
Welche Dominion KX II-Modelle unterstützen virtuelle Medien?	Alle Dominion KX II-Modelle unterstützen virtuelle Medien. Sie sind als eigenständige Angebote oder im Rahmen von CommandCenter Secure Gateway, einer zentralen Verwaltungsanwendung, verfügbar.
Welche Arten virtueller Medien unterstützt der Dominion KX II?	Folgende Medienarten werden von Dominion KX II unterstützt: interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und Remotelaufwerke.
Welche Voraussetzungen müssen für virtuelle Medien erfüllt sein?	Für virtuelle Medien wird das neue CIM D2CIM-VUSB benötigt. Es unterstützt virtuelle Mediensitzungen mit Zielservern, die über eine USB 2.0-Schnittstelle verfügen. Dieses neue CIM ist in günstigen Paketen mit 32 oder 64 Stück verfügbar und unterstützt den Mausmodus Absolute Mouse Synchronization sowie die Remotefirmwareaktualisierung.
Sind virtuelle Medien sicher?	Ja. Virtuelle Mediensitzungen werden durch eine 128-Bit-AES- oder -RC4-Verschlüsselung abgesichert.

Ethernet und IP-Netzwerk

<table>
<tr><th>FRAGE</th><th>ANTWORT</th></tr>
<tr><td>Bietet der Dominion KX II duale Gigabit-Ethernet-Ports für redundantes Failover oder zum Lasten-ausgleich?</td><td>Ja. Der Dominion KX II 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 II den sekundären Netzwerkport mit derselben IP-Adresse, wodurch sichergestellt wird, dass der Server-betrieb nicht unterbrochen wird. Hierzu muss der Administrator jedoch das automatische Failover aktivieren.</td></tr>
<tr><td>Wie viel Bandbreite benötigt der Dominion KX II?</td><td>Der Dominion KX II verfügt über die KVM-über-IP-Technologie der nächsten Generation – und damit über die beste derzeit verfügbare Videokomprimierung. Raritan hat für die hohe Qualität der Videoübertragung und die niedrige Auslastung der Bandbreite zahlreiche Auszeichnungen erhalten.

Raritan ist der Pionier der KVM-über-IP-Funktionalität, die Benutzern die Anpassung ihrer Videoparameter ermöglicht, um Netzwerkband-breite einzusparen. Wird die Verbindung mit einem Dominion KX II beispielsweise über ein DFÜ-Modem hergestellt, kann die Video-übertragung zur Gewährleistung der Produktivität und hoher Leistung auf Graustufen eingestellt werden.

Die folgenden Daten beziehen sich auf die Standardvideoeinstellungen des Dominion KX II. Diese Einstellungen können an die jeweilige Umgebung angepasst werden. Als allgemeine Regel für die Bandbreitennutzung (mit Dominion KX-Standardeinstellungen) gilt:

Als allgemeine Regel für die Bandbreitennutzung (mit Dominion KX II-Standardeinstellungen) gilt: 0,5 Mbit/s pro aktivem KVM-Benutzer (der mit einem Server verbunden ist und diesen verwendet), mit gelegentlichen Spitzen von bis zu 2 Mbit/s. Hierbei handelt es sich um eine sehr konservative Schätzung, da die Bandbreitennutzung normalerweise geringer ist.

Die für eine Videoübertragung benötigte Bandbreite hängt von der auf dem verwalteten Server ausgeführten Aufgabe ab. Je mehr Bildwechsel, desto höher die erforderliche Bandbreite. Die folgende Tabelle enthält einige Anwendungsfälle und die erforderliche Bandbreitennutzung mit Dominion KX II-Standardeinstellungen in einem 10 Mbit/s-Netzwerk:

<table>
<tr><td>Windows-Desktop im Standbymodus</td><td>0 Mbit/s</td></tr>
<tr><td>Cursorbewegung auf Desktop</td><td>0,18 Mbit/s</td></tr>
<tr><td>Verschieben von statischem 400 x 600-Fenster/Dialogfeld</td><td>0,35 Mbit/s</td></tr>
<tr><td>Navigieren im Startmenü</td><td>0,49 Mbit/s</td></tr>
<tr><td>Bildlauf einer gesamten Textseite</td><td>1,23 Mbit/s</td></tr>
<tr><td>Ausführen des Bildschirmschoners 3D Maze</td><td>1,55 Mbit/s</td></tr>
</table>
</td></tr>
<tr><td>Welche ist die lang-samste Verbindung (geringste Bandbreite), mit der der Dominion KX II betrieben werden kann?</td><td>Für annehmbare KX-Leistung über eine Modemverbindung werden mindestens 33 Kbit/s empfohlen.</td></tr>
</table>

FRAGE	ANTWORT
Welche Geschwindigkeit haben die Ethernet-Schnittstellen des Dominion KX II?	Dominion KX II unterstützt sowohl Gigabit- als auch 10/100-Ethernet. Der KX II unterstützt zwei 10/100/1000-Ethernet-Schnittstellen mit konfigurierbaren Geschwindigkeits- und Duplexeinstellungen (entweder automatisch erkannt oder manuell eingestellt).
Kann ich auf den Dominion KX II über eine Wirelessverbindung zugreifen?	Ja. Der Dominion KX II 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 II verfügt, können Server auf BIOS-Ebene drahtlos konfiguriert und verwaltet werden.
Kann der Dominion KX II über das WAN (Internet) oder nur über das Firmen-LAN verwendet werden?	Egal, ob die Verbindung über das Firmen-LAN, das wenig prognostizierbare WAN (Internet), ein Kabelmodem oder ein DFÜ-Modem hergestellt wird, die KVM-über-IP-Technologie des Dominion KX II passt sich an die Verbindung an.
Kann ich den Dominion KX II mit einem VPN verwenden?	Ja. Der Dominion KX II verwendet von Schicht 1 bis Schicht 4 Standard-IP-Technologien. Der Datenverkehr kann leicht über Standard-VPNs geleitet werden.
Wie viele TCP-Ports müssen in meiner Firewall geöffnet sein, um den Netzwerkzugriff auf den Dominion KX II zu ermöglichen? Sind diese Ports konfigurierbar?	Nur einer. Der Dominion KX II schützt das Netzwerk, indem er für seinen Betrieb nur einen einzelnen TCP-Port benötigt. Dieser Port ist vollständig konfigurierbar, was zusätzliche Sicherheit bietet. Beachten Sie hierzu, dass zur Nutzung der optionalen Webbrowser-funktionen des Dominion KX II auch der Standard-HTTPS-Port 443 geöffnet sein muss.
Wird für den Betrieb des Dominion KX II ein externer Authentifizierungsserver benötigt?	Nein. Der Dominion KX II ist ein vollständig unabhängiges Gerät. Sobald dem Dominion KX II eine IP-Adresse zugewiesen wurde, ist er mit seinen integrierten Webbrowser- und Authentifizierungsfunktionen betriebsbereit. Wird ein externer Authentifizierungsserver (wie LDAP, Active Directory®, RADIUS usw.) verwendet, unterstützt der Dominion KX II dies ebenfalls. Sollte dieser ausfallen, verwendet der Dominion KX II seine eigene interne Authentifizierung. Der Dominion KX II ermöglicht die einfache Installation, die vollständige Unabhängigkeit von einem externen Server und maximale Flexibilität.
Kann der Dominion KX II zusammen mit CITRIX verwendet werden?	Wenn der Dominion KX II korrekt konfiguriert wurde, funktioniert er in der Regel mit Produkten für den Remotezugriff wie CITRIX; Raritan kann jedoch nicht für eine akzeptable Leistung garantieren. Produkte wie CITRIX verwenden ähnliche Technologien zur Videoumleitung wie digitale KVM-Switches. Das bedeutet, dass gleichzeitig zwei KVM-über-IP-Technologien genutzt werden.
Kann der Dominion KX II DHCP verwenden?	DHCP-Adressen können zwar verwendet werden, Raritan empfiehlt jedoch die Verwendung fester Adressen, da es sich beim Dominion KX II 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 II herstellen. Woran kann das liegen?	Der Dominion KX II 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 KX II-Gerät muss auf 100 MB/Vollduplex oder die für das Netzwerk zutreffende Einstellung justiert werden. • Doppelte IP-Adresse. Wenn der KX II 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 KX II-Standardport geändert werden (oder das andere Gerät muss geändert werden). • Wird die IP-Adresse eines KX II geändert oder kommt ein neues KX II-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.

Server

FRAGE	ANTWORT
Ist der Betrieb des Dominion KX II 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 II so entwickelt, dass er vollständig unabhängig von jedem externen Server ist. Wird zum Beispiel das Rechenzentrum von einem gefährlichen Windows-Wurm oder Virus befallen, benötigen Administratoren die KVM-Lösung, um das Problem zu beheben. Daher darf die KVM-Lösung in Bezug auf die Funktion auf keinen Fall auf dieselben Windows-Server (oder irgendeinen anderen Server) angewiesen sein. Der Dominion KX II ist diesbezüglich vollständig unabhängig. Selbst wenn Sie sich entscheiden, den Dominion KX II zur Authentifizierung abhängig von einem Active Directory-Server zu konfigurieren, wird die eigene Authentifizierung des Dominion KX II aktiviert, sollte der Active Directory-Server nicht zur Verfügung stehen.
Muss ich einen Web-server wie Microsoft-Internetinformations-dienste (IIS) installieren, um die Webbrowser-funktion des Dominion KX II zu nutzen?	Nein. Der Dominion KX II ist ein vollständig unabhängiges Gerät. Sobald dem Dominion KX II eine IP-Adresse zugewiesen wurde, ist er mit seinen integrierten Webbrowser- und Authentifizierungsfunktionen betriebsbereit.
Welche Software muss ich installieren, um auf den Dominion KX II von einer bestimmten Workstation aus zuzugreifen?	Sie benötigen keine Software. Sie benötigen nur einen Webbrowser, um auf den Dominion KX II zuzugreifen (für den Zugriff auf den Dominion KX II mittels Modem ist auf der Raritan-Website Raritan.com allerdings auch ein optionaler Client erhältlich.) Für Benutzer, die kein Windows-Betriebssystem verwenden, steht jetzt auch ein Java-basierter Client zur Verfügung.
Wie konfiguriere ich einen Server für die Verbindung mit einem Dominion KX II?	Legen Sie die Mausparameter fest, um die Maussynchronisation bei Remoteverbindungen zu optimieren, und deaktivieren Sie die Features für die Stromzufuhrverwaltung, die sich auf die Bildschirmanzeige auswirken. Wenn Sie jedoch den neuen Adapter D2CIM-VUSB verwenden (der den Mausmodus Absolute Mouse Synchronization™ unterstützt), müssen Sie die Mausparameter nicht manuell festlegen.
Was enthält das Dominion KX II-Paket?	Das Paket enthält Folgendes: (a) Dominion KX II-Einheit, (b) Kurzanleitung, (c) 19-Zoll-Standardgestellhalterung, (d) CD-ROM mit Benutzerhandbuch, (e) Netzwerkkabel, (f) Crossoverkabel, (g) Netzkabel, (h) Garantie und andere Dokumentation.

Installation

FRAGE	ANTWORT
Was muss ich außer dem Switch von Raritan zur Installation des Dominion KX II bestellen?	Für jeden Server, den Sie am Dominion KX II anschließen möchten, benötigen Sie ein Dominion oder Paragon Computer Interface Module (CIM). Hierbei handelt es sich um einen direkt am Tastatur-, Video- und Mausport des Servers angeschlossenen Adapter.
Welche Art von Cat5-Kabel muss ich für meine Installation verwenden?	Für den Dominion KX II 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 „Cat5“-Kabeln die Rede. Tatsächlich kann jedes UTP-Kabel für den Dominion KX II verwendet werden.
Welche Arten von Servern können am Dominion KX II angeschlossen werden?	Der Dominion KX II ist vollständig anbieterunabhängig. Jeder Server mit standardmäßigem Tastatur-, Video- und Mausport kann angeschlossen werden.
Wie werden Server am Dominion KX II angeschlossen?	Für jeden Server, den Sie am Dominion KX II anschließen möchten, benötigen Sie ein Dominion oder Paragon CIM, das direkt am Tastatur-, Video- und Mausport des Servers angeschlossen wird. Anschließend verbinden Sie jedes CIM mittels Standard-UTP-Kabel (Twisted-Pair) wie z. B. Kat. 5, Kat. 5e oder Kat. 6 mit dem Dominion KX II.
In welcher Entfernung zum Dominion KX II müssen die Server aufgestellt sein?	Server können im Allgemeinen abhängig vom Servertyp bis zu 45 m vom Dominion KX II entfernt sein. (Weitere Informationen finden Sie auf der Website von Raritan oder unter Verbindungsentfernung zum Zielserver.) Für das neue CIM D2CIM-VUSB, das virtuelle Medien und den Mausmodus **Absolute Mouse Synchronization** unterstützt, wird eine Entfernung von 30 m empfohlen.
Einige Betriebssysteme stürzen ab, wenn die Tastatur- oder Mausverbindung während des Betriebs getrennt wird. Wie wird der durch den Wechsel zu einem anderen Server verursachte Absturz von am Dominion KX II angeschlossenen 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. Diese Technologie beruht auf über 15 Jahren Erfahrung und wurde weltweit auf Millionen von Servern implementiert.
Müssen auf den am Dominion KX II angeschlossenen Servern irgendwelche Agents installiert werden?	Die mit einem Dominion KX II verbundenen Server erfordern keine Installation von Softwareagents, da die Verbindung des Dominion KX II mit dem Tastatur-, Video- und Mausport des Servers direkt über Hardware hergestellt wird.

FRAGE	ANTWORT
Wie viele Server können an jeder Dominion KX II-Einheit angeschlossen werden?	Die Dominion KX II-Modelle bieten 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 II trenne und an einer anderen Dominion KX II-Einheit oder an einem anderen Port desselben Dominion KX II anschließe?	Der Dominion KX II aktualisiert automatisch die Serverportnamen, wenn Server an anderen Ports angeschlossen werden. Diese automatische Aktualisierung betrifft nicht nur den Port für den lokalen Zugriff, sondern auch alle Remoteclients und die optionale Verwaltungsanwendung 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 II an?	Wenn Sie nur wenige seriell gesteuerte Geräte besitzen, können Sie diese mit dem seriellen Adapter von Raritan (AUATC) oder dem neuen Seriell-Converter P2CIM-SER am Dominion KX II anschließen. Bei mehr als vier seriell gesteuerten Geräten empfehlen wir allerdings die Verwendung der Dominion SX-Serie sicherer Konsolenserver von Raritan. Für viele serielle Geräte bietet Dominion SX umfassendere Funktionen zu einem günstigeren Preis als Dominion KX II. Die SX-Reihe lässt sich einfach bedienen, konfigurieren und verwalten und kann vollständig in die Implementierung einer Dominion-Serie integriert werden. Insbesondere viele UNIX- und Netzwerkadministratoren begrüßen den direkten SSH-Wechsel zu einer Dominion SX-Einheit.

Lokaler Port

FRAGE	ANTWORT
Kann ich auf meine Server direkt über das Gestell zugreifen?	Ja. Der in einem Gestell montierte Dominion KX II funktioniert genau wie ein herkömmlicher KVM-Switch: Er ermöglicht die Steuerung von bis zu 64 Servern mit nur einer Tastatur, Maus und einem Monitor.
Verhindere ich den Remotezugriff anderer Benutzer auf die Server, wenn ich den lokalen Port verwende?	Nein. Der lokale Dominion KX II-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 II verfügt am lokalen Port über PS/2- und USB-Tastatur-/Mausports. Die USB-Ports verwenden USB v1.1 und unterstützen nur Tastaturen und Mäuse und keine USB-Geräte wie Scanner oder Drucker.
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 KX II 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, während ich den lokalen Port verwende?	Der lokale Port zeigt die angeschlossenen Server über dieselbe Oberfläche an wie der Remoteclient. Durch ein einfaches Klicken stellen Sie eine Verbindung mit einem Server her.
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 II 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 II mithilfe der Failoverfunktion auf seine eigene, interne Authentifizierungsdatenbank um. Der Dominion KX II verfügt über eine eigenständige Authentifizierung für die sofortige Installation.

FRAGE	ANTWORT
Wird diese Änderung auch auf die für den Remotezugriff verwendeten Clients übertragen, wenn ich zum Ändern des Namens eines angeschlossenen Servers den lokalen Port verwende? Wird die Änderung auch von der optionalen Anwendung CommandCenter übernommen?	Ja. Der lokale Port ist mit den für den Remotezugriff verwendeten Clients und mit der optionalen Verwaltungsanwendung CommandCenter Secure Gateway von Raritan synchronisiert. Wenn Sie den Namen eines Servers über die Bildschirmschnittstelle des Dominion KX II ändern, werden alle Remoteclients und externen Verwaltungsserver in Echtzeit aktualisiert.
Wird diese Änderung auch von der Bildschirmanzeige des lokalen Ports übernommen, wenn ich die Tools zur Remoteverwaltung des Dominion KX II zum Ändern des Namens eines angeschlossenen Servers verwende?	Ja. Wenn Sie den Namen eines Servers von einem entfernten Standort aus oder mittels der optionalen Verwaltungsanwendung CommandCenter Secure Gateway von Raritan ändern, wird die Bildschirmanzeige des Dominion KX II sofort aktualisiert.
Manchmal sehe ich „Schatten“ auf der Benutzeroberfläche des lokalen Ports. Wie kommt dies zustande?	Dieser Schatteneffekt tritt bei LCD-Monitoren auf, die lange Zeit eingeschaltet bleiben. Die LCD-Eigenschaften und die elektrische/statische Ladung können zu solchen Schatten führen.

Stromzufuhrsteuerung

FRAGE	ANTWORT
Verfügt der Dominion KX II über zwei Netzteile?	Alle Dominion KX II-Modelle verfügen über zwei Stromeingänge und Netzteile mit automatischem Failover. Sollte ein Stromeingang oder Netzteil ausfallen, wechselt der KX II automatisch zum anderen.
Erkennt das Netzteil des Dominion KX II 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 benachrichtigt, falls ein Netzteil oder Stromeingang ausfällt?	Die LED-Anzeige an der Vorderseite des KX II-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.
Welche Funktionen zur Stromzufuhrsteuerung bietet der Dominion KX II?	Die Powerstrips von Raritan zur Remote-Stromzufuhrsteuerung können an den Dominion KX II angeschlossen werden, um die Stromzufuhr der Zielserver zu steuern. Sie müssen lediglich einmal einen Konfigurationsschritt ausführen und können anschließend durch Klicken mit der rechten Maustaste auf den entsprechenden Servernamen einen abgestürzten Server einschalten, ausschalten bzw. ein- und ausschalten. Diese Art von Neustart ist mit dem physischen Trennen des Servers vom Stromnetz und dem erneuten Anschließen vergleichbar.
Unterstützt der Dominion KX II Server mit mehreren Netzteilen? Spielt es eine Rolle, wenn jedes Netzteil an einem anderen Powerstrip angeschlossen ist?	Ja. Der Dominion KX II kann leicht zur Unterstützung mehrerer Netzteile, die an verschiedenen Powerstrips angeschlossen sind, konfiguriert werden. An ein KX II-Gerät können bis zu acht (8) Powerstrips angeschlossen werden. Pro Zielserver können vier Netzteile mit mehreren Powerstrips verbunden werden.
Erfordert die Remote-Stromzufuhrsteuerung eine spezielle Serverkonfiguration?	Einige Server verfügen über Standard-BIOS-Einstellungen, die verhindern, dass der Server nach dem Wiederherstellen der Stromzufuhr automatisch neu gestartet wird. Nähere Informationen hierzu finden Sie im Serverbenutzerhandbuch.
Welche Arten von Powerstrips unterstützt der Dominion KX II?	Zur Nutzung der integrierten Benutzeroberfläche für die Stromzufuhrsteuerung des Dominion KX II (und speziell für die integrierte Sicherheit) müssen Sie Raritan-Powerstrips für die Remote-Stromzufuhrsteuerung (RPC) verwenden. Diese RPCs sind in verschiedenen Buchsen-, Stecker- und Amperevariationen erhältlich. Für den Anschluss eines RPC am KX II-Gerät müssen Sie das CIM D2CIM-PWR erwerben.

Skalierbarkeit

FRAGE	ANTWORT
Wie kombiniere ich mehrere Dominion KX II-Einheiten zu einer Einzellösung?	Mehrere Dominion KX II-Einheiten müssen nicht physisch miteinander verbunden werden. Die einzelnen Dominion KX II-Einheiten werden stattdessen mit dem Netzwerk verbunden und fungieren automatisch als Einzellösung, wenn sie zusammen mit der optionalen Verwaltungs-anwendung CommandCenter Secure Gateway (CC-SG) von Raritan bereitgestellt werden. CC-SG dient als einziger Zugriffspunkt für den Remotezugriff und die Remoteverwaltung. CC-SG bietet bequeme Tools wie die gemeinsame Konfiguration, die gemeinsame Firmwareaktualisierung und eine einzelne Authentifizierung und Authentifizierungsdatenbank. CommandCenter bietet außerdem die ausgeklügelte Serversortierung, Berechtigungen und Zugriffsfunktionen. CommandCenter Secure Gateway bietet außerdem eine ausgeklügelte Serversortierung, Berechtigungen und Zugriffsfunktionen. Wenn Sie die optionale Verwaltungsanwendung CC-SG von Raritan nicht bereitstellen möchten, arbeiten mehrere Dominion KX II-Einheiten nach wie vor automatisch zusammen und werden automatisch skaliert: Die Remotebenutzeroberfläche des KX II und der Multi-Platform-Client erkennen Dominion KX II-Einheiten automatisch. Auf nicht erkannte Dominion KX II-Einheiten können Sie über ein benutzer-definiertes Profil zugreifen.
Kann ich einen vorhandenen analogen KVM-Switch am Dominion KX II anschließen?	Ja. Analoge KVM-Switches können an einem der Dominion KX II-Serverports angeschlossen werden. Verwenden Sie einfach ein PS/2 Computer Interface Module (CIM), und schließen Sie es an den Benutzerports des vorhandenen analogen KVM-Switches an. Analoge KVM-Switches besitzen unterschiedliche technische Daten, und Raritan bietet keine Gewähr für die Kompatibilität analoger KVM-Switches von Drittanbietern. Wenden Sie sich an den technischen Support von Raritan, wenn Sie hierzu weitere Informationen benötigen. Die analogen Raritan-Switches Paragon® und Paragon II sind mittels IP-Reach® IP-fähig.

Computer Interface Modules (CIMs)

FRAGE	ANTWORT
Kann ich Computer Interface Modules (CIMs) vom analogen Matrix-KVM-Switch Paragon von Raritan mit dem Dominion KX II verwenden?	Ja. Bestimmte Paragon Computer Interface Modules (CIMs) können mit Dominion KX II verwendet werden (eine aktuelle Liste zertifizierter CIMs finden Sie auf der Raritan-Website bei den Versionshinweisen zu Dominion KX II). Da Paragon CIMs jedoch teurer sind als Dominion KX II-CIMs (sie umfassen Technologie für die Videoübertragung über eine Entfernung von 300 m), sollten im Allgemeinen keine Paragon CIMs zur Verwendung mit Dominion KX II erworben werden. Werden Paragon CIMs am Dominion KX II angeschlossen, übertragen diese Video wie Dominion KX II-CIMs über eine Entfernung von 45 m und nicht über 300 m (wie beim Anschluss an Paragon).
Kann ich Dominion KX II-Computer Interface Modules (CIMs) mit dem analogen Matrix-KVM-Switch Paragon von Raritan verwenden?	Nein. Dominion KX II-Computer Interface Modules (CIMs) übertragen Videobilder über eine Entfernung von 15 m bis 45 m und können daher nicht mit Paragon verwendet werden, denn hierfür sind CIMs erforderlich, die Videobilder über eine Entfernung von 300 m übertragen. Um sicherzustellen, dass alle Raritan-Kunden immer die bestmögliche Videoqualität erhalten (eine typische Eigenschaft von Raritan) sind CIMs der Dominion-Serie nicht mit Paragon kompatibel.

Sicherheit

FRAGE	ANTWORT
Welche Art von Verschlüsselung verwendet der Dominion KX II?	Der Dominion KX II verwendet sowohl für die SSL-Kommunikation als auch für den eigenen Datenstrom die standardmäßige und sehr sichere 128-Bit-RC4- oder -AES-Verschlüsselung. Zwischen den Remoteclients und dem Dominion KX II werden keinerlei Daten unverschlüsselt übertragen.
Unterstützt der Dominion KX II die AES-Verschlüsselung, die im Rahmen des vom US-amerikanischen National Institute of Standards and Technology entwickelten FIP-Standards empfohlen wird?	Der Dominion KX II verwendet die AES (Advanced Encryption Standard)-Verschlüsselung 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 II 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 II Tastatur-, Maus- und Videodaten zur Gewährleistung einer hohen Sicherheit.
Wie wird der Dominion KX II in externe Authentifizierungsserver wie Active Directory®, RADIUS oder LDAP integriert?	Der Dominion KX II kann leicht zur Weiterleitung aller Authentifizierungsanforderungen an einen externen Server wie LDAP, Active Directory oder RADIUS konfiguriert werden. Für jeden authentifizierten Benutzer empfängt der Dominion KX II vom Authentifizierungsserver die Benutzergruppe, der dieser Benutzer angehört. Der Dominion KX II bestimmt daraufhin die Zugriffsrechte entsprechend der Gruppe, der der Benutzer angehört.
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 II die Verwendung sicherer Kennwörter?	Ja. Der Administrator kann im Dominion KX II die Prüfung sicherer Kennwörter konfigurieren um sicherzustellen, dass benutzerdefinierte Kennwörter unternehmensinternen Richtlinien bzw. Behördenvorschriften genügen und nicht von Hackern geknackt werden können.

<table>
<tr><th>FRAGE</th><th>ANTWORT</th></tr>
<tr><td>Welche Verschlüsse-lungsebene wird erreicht, wenn der Verschlüsselungsmodus des Dominion KX II auf Auto (Automatisch) eingestellt ist?</td><td>Welche Verschlüsselungsebene automatisch ausgehandelt wird, hängt vom verwendeten Browser ab:

<table><tr><th>Browser</th><th>Verschlüsselungsebene</th></tr><tr><td>Internet Explorer 6</td><td>RC4</td></tr><tr><td>Internet Explorer 7</td><td>AES-128</td></tr><tr><td>Firefox 1.5</td><td>RC4</td></tr><tr><td>Firefox 2.0</td><td>RC4</td></tr><tr><td>Mozilla 1.7</td><td>RC4</td></tr><tr><td>Safari 2.0.4</td><td>AES-128</td></tr></table></td></tr>
</table>

Bedienkomfort

FRAGE	ANTWORT
Kann der Dominion KX II von einem entfernten Standort aus über einen Webbrowser verwaltet und konfiguriert werden?	Ja. Der Dominion KX II 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 II-Konfiguration sichern und wieder-herstellen?	Ja. Die Dominion KX II-Konfigurationen für Benutzer und Geräte können zur späteren Wiederherstellung (z. B. nach einer Katastrophe) vollständig gesichert werden. Die Funktionen zur Sicherung und Wiederherstellung des Dominion KX II können auch von einem entfernten Standort über das Netzwerk bzw. über einen Webbrowser genutzt werden.
Welche Funktionen zur Prüfung oder Protokol-lierung bietet der Dominion KX II?	Der Dominion KX II protokolliert alle wichtigen Benutzerereignisse mit einem Datums- und Zeitstempel. Zu den protokollierten Ereignissen zählen u. a.: die Benutzeran- und -abmeldung, der Benutzerzugriff auf einen bestimmten Server, fehlgeschlagene Anmeldeversuche, Konfigurationsänderungen usw.
Kann der Dominion KX II in Syslog integriert werden?	Ja. Der Dominion KX II besitzt nicht nur eigene interne Protokollfunktionen, sondern er kann auch alle protokollierten Ereignisse an einen zentralen Syslog-Server senden.
Kann der Dominion KX II in SNMP integriert werden?	Ja. Der Dominion KX II besitzt nicht nur eigene interne Protokoll-funktionen, sondern er kann auch SNMP-Traps an SNMP-Verwaltungssysteme wie HP Openview und CC-NOC von Raritan senden.
Kann die interne Uhr des Dominion KX II mit einem Zeitserver synchronisiert werden?	Ja. Der Dominion KX II unterstützt das Standard-NTP-Protokoll für die Synchronisierung mit einem Firmenzeitserver oder mit einem öffentlichen Zeitserver (vorausgesetzt, ausgehende NTP-Anforde-rungen können über die Firmenfirewall übertragen werden).

Verschiedenes

FRAGE	ANTWORT
Wie lautet die Standard-IP-Adresse des Dominion KX II?	192.168.0.192
Wie lauten der Standardbenutzername und das Standardkennwort des Dominion KX II?	Der Standardbenutzername des KX II lautet **admin** und das Standardkennwort **raritan** (beides mit Kleinbuchstaben geschrieben). Für eine höchstmögliche Sicherheit wird der Administrator des Dominion KX II 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 KX II verfügt über eine Taste zum Zurücksetzen am Gerät, mit der der Auslieferungszustand des Geräts wiederhergestellt werden kann. Dadurch wird auch das Administratorkennwort zurückgesetzt.

Problembehandlung

FRAGE	ANTWORT
Ich habe mich über Firefox beim Dominion KX II angemeldet und anschließend ein weiteres Firefox-Fenster geöffnet. Ich wurde mit dem zweiten Browserfenster automatisch beim selben Dominion KX II angemeldet. Ist das korrekt?	Ja, diese Verhaltensweise ist korrekt und entspricht der Funktionsweise von Browsern und Cookies.
Ich bin über Firefox beim Dominion KX II angemeldet und versuche, mich auf demselben Client mit einer anderen Firefox-Sitzung bei einem anderen Dominion KX II-Gerät anzumelden. Dadurch werde ich bei beiden KX II-Geräten abgemeldet. Ist diese Verhaltensweise korrekt?	Ja, für den Zugriff auf zwei verschiedene Dominion KX II-Geräte müssen Sie entweder die erste Sitzung beenden oder einen anderen Client-PC verwenden.
Wenn ich eine KVM-Sitzung mit dem Browser Firefox durchführe und bestimmte Dialogfelder wie **Connection Properties** (Verbindungseigenschaften) und **Video Settings** (Videoeinstellungen) im Virtual KVM Client geöffnet werden, wird Firefox blockiert. (Dies gilt auch für andere Firefox-Sitzungen.) Was kann ich tun?	Dieses Verhalten ist normal, da bei Firefox alle Sitzungen miteinander verbunden sind. Wenn Sie das Dialogfeld des Virtual KVM Client schließen, wird Firefox nicht mehr blockiert.

255-62-4023-00

Hauptsitz

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel.: (732) 764-8886
Fax. (732) 764-8887
Email: sales@raritan.com
Web: www.raritan.com

Raritan America

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel.: (732) 764-8886
Fax. (732) 764-8887
Email: sales@raritan.com
Web: www.raritan.com

Firmenhauptsitz Asien-Pazifik

Raritan Asia Pacific, Inc.
5F, 121 , Lane 235 , Pao-Chiao Road,
Hsin Tien 231,
Taipei, Taiwan, ROC
Tel.: (886) 2 8919-1333
Fax. (886) 2 8919-1338
Email: sales.asia@raritan.com
Web: raritan-ap.com

Raritan-Niederlassung in China

Raritan Beijing
No. 35 Financial St, Xicheng District
Room 1035, Block C,
Corporate Square
Peking 100032, China
Tel.: (86) 10-8809-1890
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Shanghai
Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai, China
(200030)
Tel.: (86) 21 5425-2499
Fax. (86) 21 5425-3992
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Guangzhou
1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou (510075), China Raritan
Tel.: (86) 20 8755-5581
Fax. (86) 20 8755-5571
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Korea

#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel.: (82) 2 557-8730
Fax. (82) 2 557-8733
E-Mail: sales.korea@raritan.com
Web: raritan.co.kr

Raritan Japan

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku, Tokyo 104-0033, Japan
Tel.: (81) 03-3523-5991
Fax. (81) 03-3523-5992
E-Mail: sales@raritan.co.jp
Web: raritan.co.jp

Raritan Osaka
3rd Floor,
Osaka Kagaku Sen'I Kaikan Bldg.
4-6-8 Kawara-machi, Chuo-ku,
Osaka 541-0048, Japan
Tel.: (81) 03-3523-5953
Fax. (81) 03-3523-5992
Web: raritan.co.jp

Raritan-Niederlassungen in Australien

Raritan Melbourne
Level 2, 448 St Kilda Rd.,
Melbourne, VIC3004
Australien
Tel.: (61) 3-9866-6887
E-Mail: sales.au@raritan.com
Web: raritan.com.au

Raritan Sydney
PO BOX A386,
Sydney, NSW2000, Australien
Tel.: (61) 2-9029-2558
E-Mail: sales.au@raritan.com
Web: raritan.com.au

Raritan India

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli Gurgaon Rd, Gurgaon 122 002
Haryana, Indien
Tel.: (91) 124 410-7881
Fax. (91) 124 410-7880
E-Mail: enquiry.india@raritan.com
Web: raritan.co.in

Raritan Taiwan
5F, 121, Lane 235, Pao-Chiao Road
Hsin-Tien City
Taipei Hsien, Taiwan, ROC
Tel.: (886) 2 8919-1333
Fax. (886) 2 8919-1338
E-Mail: sales.taiwan@raritan.com
Web: raritan.com.tw

Raritan Singapore
350 Orchard Road
#11-08, Suite 21, Shaw House
Singapur 238868
Tel.: (65) 6725 9871
Fax: (65) 6725 9872
E-Mail: sales.ap@raritan.com
Web: raritan-ap.com

Firmenhauptsitz in Europa

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
Niederlande
Tel.: (31) 10-284-4040
Fax. (31) 10-284-4049
E-Mail: sales.europe@raritan.com
Web: www.raritan.fr
www.raritan.de

Raritan France

120 Rue Jean Jaurès
F-92300 Levallois-Perret
Tel.: (33) 14-756-2039
Fax. (33) 14-756-2061
E-Mail: sales.france@raritan.com
Web: www.raritan.fr

Raritan Deutschland GmbH

Lichtstraße 2
D-45127 Essen
Tel.: (49) 201-747-98-0
Fax. (49) 201-747-98-50
E-Mail: sales.germany@raritan.com
Web: www.raritan.de

Raritan Italia

Via dei Piatti 4
20123 Milan
Italien
Tel.: (39) 02-454-76813
Fax. (39) 02-861-749
E-Mail: sales.italy@raritan.com
Web: raritan.it
www.raritan.info

Raritan Canada

Raritan Inc.
4 Robert Speck Pkwy., Suite 1500
Mississauga, ON L4Z 1S1
Kanada
Tel.: 1-905-949-3650
E-Mail: sales.canada@raritan.com
Web: raritan.ca

Raritan U.K.

9th Floor, 12-20 Camomile St
London EC3A 7EX, Großbritannien
Tel.: (44) (0)20-7614-7700
E-Mail: sales.uk@raritan.com
Web: raritan.co.uk