



# Dominion KX II-101-V2

**Benutzerhandbuch**  
**Version 3.5.0**

---

Copyright © 2012 Raritan, Inc.

KX2101V2-v3.5.0-D-G

September 2012

255-62-3059-00

---

Dieses Dokument enthält proprietäre Informationen, die durch Urheberrechtsgesetze geschützt sind. Alle Rechte vorbehalten. Dieses Dokument darf ohne die vorherige schriftliche Zustimmung der Raritan, Inc., weder ganz noch teilweise fotokopiert, reproduziert oder in eine andere Sprache übersetzt werden.

© Copyright 2012 Raritan, Inc. Die in diesem Dokument genannte Software und Hardware anderer Hersteller sind registrierte Marken oder Marken sowie Eigentum der jeweiligen Inhaber.

#### 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 Heiminstitutionen. Dieses Gerät erzeugt, verwendet und strahlt Energie im Radiofrequenzbereich aus. Wenn es nicht gemäß den Anweisungen installiert und verwendet wird, kann sein Betrieb schädliche Interferenzen im Funkverkehr verursachen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

#### Einhaltung der VCCI-Anforderungen (Japan)

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

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

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



**im Serverschrank**

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

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

# Inhalt

<b>Kapitel 1 Einleitung</b>	<b>1</b>
Überblick über KX II-101-V2 .....	2
KX II-101-V2-Hilfe .....	3
Neuerungen im Hilfedokument .....	4
Verwandte Dokumentation .....	4
Produktfotos .....	5
Produktfeatures.....	5
Schnittstellen .....	5
Netzwerkconfiguration .....	5
Systemverwaltungsfunktionen.....	6
Verwaltungsfunktionen .....	6
Benutzerfunktionen.....	7
Stromversorgung .....	7
Videoauflösung .....	7
Montage.....	7
Terminologie .....	7
Paketinhalt .....	8
<b>Kapitel 2 Installation und Konfiguration</b>	<b>9</b>
Überblick .....	9
Standard-Anmeldeinformationen .....	9
Erste Schritte .....	10
Schritt 1: Konfigurieren des Zielservers .....	10
Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall.....	23
Schritt 3: Anschließen der Geräte .....	24
Schritt 4: Konfigurieren von KX II-101-V2 .....	29
<b>Kapitel 3 Arbeiten mit Zielserversn</b>	<b>39</b>
Schnittstellen.....	39
Oberfläche der KX II-101-V2-Remotekonsole.....	39
Multi-Platform-Client (MPC).....	50
Virtual KVM Client (VKC) .....	50
Überblick .....	50
Verbinden mit einem KVM-Zielservers.....	50
Schaltflächen auf der Symbolleiste und Symbole auf der Statusleiste .....	51
Stromzufuhrsteuerung eines Zielservers.....	53
Trennen von KVM-Zielservers.....	54
Properties (Eigenschaften) .....	54
Verbindungsinformationen.....	56
Tastaturoptionen.....	57

Videoeigenschaften .....	63
Mausoptionen .....	69
VKC Virtual Media (Virtuelle Medien) .....	73
Optionen im Menü "Tools" (Extras) .....	73
Ansichtsoptionen .....	78
Hilfeoptionen .....	80

## **Kapitel 4 Virtuelle Medien 81**

---

Überblick .....	82
Voraussetzungen für die Verwendung virtueller Medien .....	84
Virtuelle Medien in einer Windows XP-Umgebung .....	85
Virtuelle Medien in einer Linux-Umgebung .....	86
Virtuelle Medien in einer Mac-Umgebung .....	88
Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist .....	88
Verwenden virtueller Medien .....	89
Herstellen einer Verbindung mit virtuellen Medien .....	90
Lokale Laufwerke .....	90
Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern .....	91
Trennen von virtuellen Medien .....	92

## **Kapitel 5 User Management (Benutzerverwaltung) 93**

---

Benutzergruppen .....	93
User Group List (Liste der Benutzergruppen) .....	94
Beziehung zwischen Benutzern und Gruppen .....	95
Hinzufügen einer neuen Benutzergruppe .....	95
Ändern einer vorhandenen Benutzergruppe .....	100
Benutzer .....	100
Anzeigen der KX II-101-V2-Benutzerliste .....	101
Anzeigen der Benutzer nach Port .....	101
Trennen der Benutzer von Ports .....	102
Abmelden der Benutzer bei KX II-101-V2 (Erzwungene Abmeldung) .....	102
Hinzufügen eines neuen Benutzers .....	103
Ändern eines vorhandenen Benutzers .....	103
Sperrern von Benutzern und Aufheben der Sperrung .....	104
Authentication Settings (Authentifizierungseinstellungen) .....	105
Implementierung der LDAP/LDAPS-Remoteauthentifizierung .....	106
Rückgabe von Benutzergruppeninformationen vom Active Directory-Server .....	111
Implementierung der RADIUS-Remote-Authentifizierung .....	112
Zurückgeben von Benutzergruppeninformationen über RADIUS .....	115
Spezifikationen für den RADIUS-Kommunikationsaustausch .....	115
Benutzerauthentifizierungsprozess .....	117
Ändern von Kennwörtern .....	119

## **Kapitel 6 Geräteverwaltung 120**

---

Network Settings (Netzwerkeinstellungen) .....	120
Network Basis Settings (Basisnetzwerkeinstellungen) .....	121
LAN Interface Settings (LAN-Schnittstelleneinstellungen) .....	125

Device Services (Gerätedienste) .....	126
Aktivieren von Telnet .....	126
Aktivieren von SSH.....	126
HTTP- und HTTPS-Porteinstellungen .....	127
Eingeben des Erkennungsports .....	127
Aktivieren des direkten Port-Zugriffs über URL.....	128
Konfigurieren von SNMP-Agenten .....	128
Keyboard/Mouse Setup (Tastatur/Maus einrichten) .....	131
Serial Port Settings (Einstellungen für seriellen Port).....	132
Port „Admin“.....	132
Steuerung des Powerstrip von Raritan.....	132
Modem.....	133
Konfigurieren von Datum-/Uhrzeiteinstellungen .....	134
Ereignisverwaltung.....	135
Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen).....	135
Konfigurieren der Ereignisverwaltung - Ziele .....	143
Port Configuration (Port-Konfiguration) .....	144
Verwalten von KVM-Zielservern (Seite "Port") .....	145
Stromzufuhrsteuerung .....	147
Analoger KVM-Switch .....	152
Zurücksetzen des KX II-101-V2 mithilfe der Taste "Reset" (Zurücksetzen).....	154
Ändern der Standardeinstellung für die GUI-Sprache .....	155

---

**Kapitel 7 USB-Verbindungen verwalten 156**

Überblick .....	157
USB-Verbindungseinstellungen .....	158
Erweiterte USB-Verbindungseinstellungen.....	159

---

**Kapitel 8 Sicherheitsverwaltung 161**

Security Settings (Sicherheitseinstellungen) .....	161
Anmeldebeschränkungen .....	161
Strong Passwords (Sichere Kennwörter) .....	163
User Blocking (Benutzersperrung) .....	165
Encryption & Share (Verschlüsselung und Freigabe) .....	167
Aktivieren von FIPS 140-2.....	171

Konfigurieren der IP-Zugriffssteuerung.....	173
SSL-Zertifikate .....	176
Sicherheitsmeldung .....	180

## **Kapitel 9   Wartung** **182**

---

Audit Log (Prüfprotokoll) .....	182
Device Information (Geräteinformationen).....	183
Backup/Restore (Sicherung/Wiederherstellung) .....	184
Aktualisieren der Firmware .....	186
Upgrade History (Aktualisierungsverlauf) .....	188
Werksrückstellung.....	189
Neustart der KX II-101-V2-Einheit .....	189
Beenden der CC-SG-Verwaltung .....	191

## **Kapitel 10   Diagnostics (Diagnose)** **193**

---

Network Interface (Netzwerkschnittstelle) .....	193
Network Statistics (Netzwerkstatistik) .....	194
Ping Host (Ping an den Host) .....	196
Seite "Trace Route to Host" (Route zum Host verfolgen).....	196
Device Diagnostics (Gerätediagnose) .....	198

## **Kapitel 11   Kommandozeilenschnittstelle (CLI)** **200**

---

Überblick .....	200
Zugriff auf KX II-101-V2 über die Befehlszeilenschnittstelle.....	201
SSH-Verbindung mit der KX II-101-V2-Einheit.....	201
SSH-Zugriff über einen Windows-PC.....	201
SSH-Zugriff über eine UNIX-/Linux-Workstation .....	202
Anmelden .....	202
Navigation in der Kommandozeilenschnittstelle .....	202
Eingabeaufforderungen der Befehlszeilenschnittstelle .....	202
Vervollständigen von Befehlen .....	203
Syntax der Kommandozeilenschnittstelle – Tipps und Zugriffstasten.....	203
Allgemeine Befehle für alle Ebenen der Befehlszeilenschnittstelle.....	204
Befehle der Befehlszeilenschnittstelle .....	204
Diagnostics (Diagnose) .....	205
Configuration (Konfiguration).....	207
Befehl „listports“ .....	209
Befehl „Userlist“ .....	209

## **Kapitel 12 "CC-SG Management" (CC-SG-Verwaltung) 210**

---

Überblick .....	210
Aufheben der Verwaltung von KX II-101-V2 durch CC-SG .....	211
Verwenden von CC-SG im Proxymodus .....	212

## **Anhang A Technische Daten 213**

---

Physische Spezifikationen .....	213
Unterstützte Betriebssysteme (Clients) .....	214
Unterstützte Browser .....	215
Kabel .....	216
Zertifizierte Modems .....	216
Unterstützte Videoauflösungen .....	216
Unterstützte Tastatursprachen .....	218
Verwendete TCP- und UDP-Ports .....	219
Netzwerk-Geschwindigkeitseinstellungen .....	221
9-polige Pinbelegung .....	222

## **Anhang B Aktualisieren des LDAP-Schemas 224**

---

Zurückgeben von Benutzergruppeninformationen .....	224
Von LDAP .....	224
Von Microsoft Active Directory .....	224
Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen .....	225
Erstellen eines neuen Attributs .....	225
Hinzufügen von Attributen zur Klasse .....	227
Aktualisieren des Schemacache .....	228
Bearbeiten von rcusergroup-Attributen für Benutzermitglieder .....	229

## **Anhang C Gestellmontage 232**

---

L-Halterung an KX II-101-V2 zur horizontalen Montage anbringen .....	232
--	-----

## **Anhang D Wichtige Hinweise 234**

---

Java Runtime Environment (JRE) .....	234
Hinweise zur Unterstützung von IPv6 .....	235
Hinweise zur Unterstützung des Betriebssystems IPv6 .....	235
Hinweise zu Tastatur, Video und Maus .....	235
Einschränkungen bezüglich Video Sun Blade, Tastatur und Mausunterstützung .....	236
Eingeschränkter BIOS-Zugriff von einer lokalen Tastatur .....	236
HP UX RX 1600 – Tastatur- und Mauskonfiguration .....	237
Compaq Alpha und IBM P Server – Einschränkungen beim Mausmodus .....	237
Server "Windows 2000" und "Windows 2003" – Tastatureinschränkungen .....	238
CC-SG .....	238
Proxymodus und MPC .....	238



<b>Anhang E Häufig gestellte Fragen (FAQs)</b>	<b>239</b>
<hr/>	
Allgemeine FAQs .....	239
IPv6-Netzwerk.....	241
<b>Index</b>	<b>243</b>
<hr/>	

# Kapitel 1 Einleitung

## In diesem Kapitel

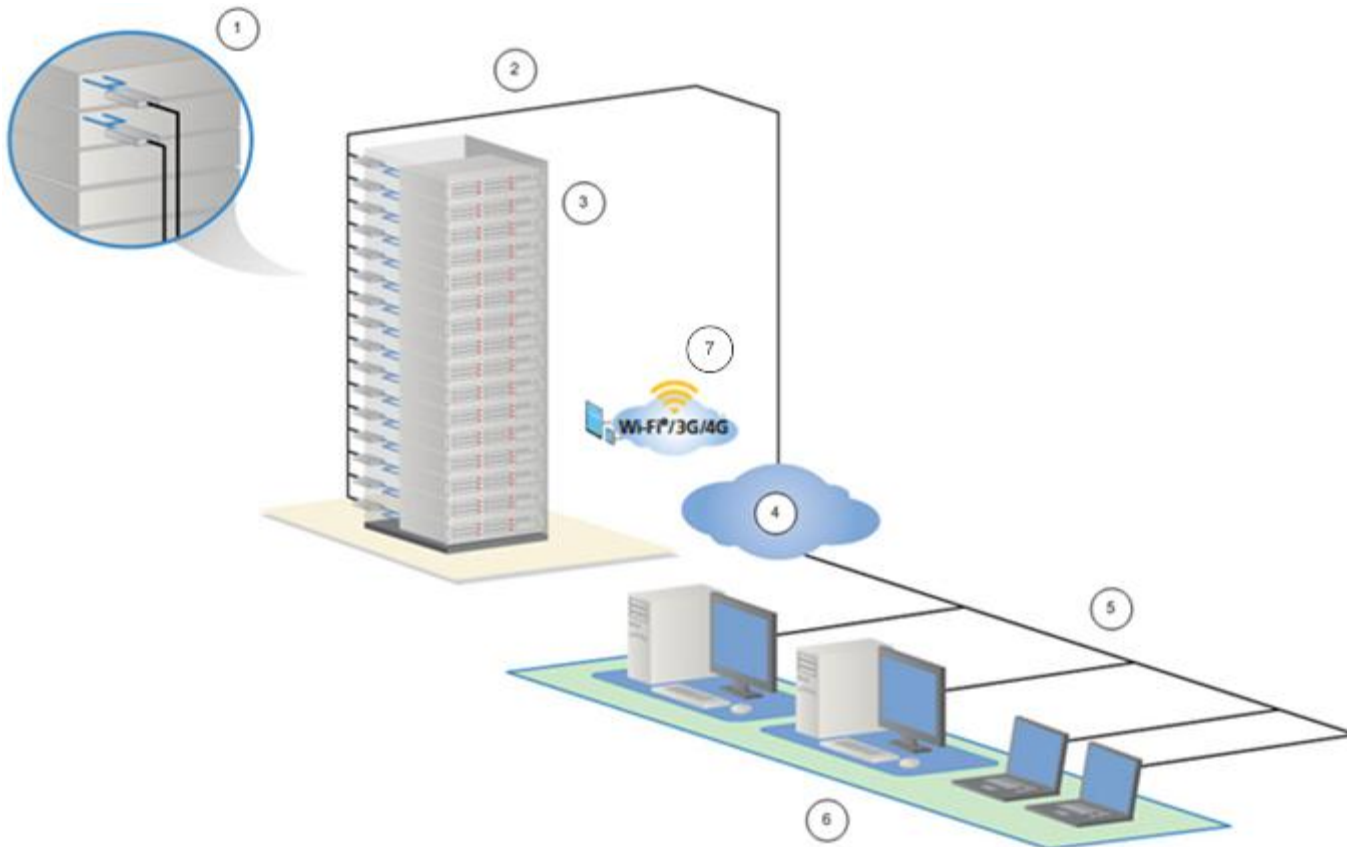
Überblick über KX II-101-V2.....	2
KX II-101-V2-Hilfe.....	3
Produktfotos .....	5
Produktfeatures .....	5
Terminologie .....	7
Paketinhalt .....	8

## Überblick über KX II-101-V2

Vielen Dank, dass Sie sich für Dominion KX II-101-V2 entschieden haben. Dominion KX II-101-V2 bietet einen Tastatur-, Video- und Maus-Port (KVM) zur Verbindung mit einem Zielserver und einen IP-Port zur Verbindung mit einem IP-Netzwerk. In dem KX II-101-V2-Gerät werden KVM-Signale von Ihrem Server in das IP-Format konvertiert und für die Übertragung über ein IP-Netzwerk komprimiert.

Der Formfaktor des KX II-101-V2-Dongle erleichtert die Installation in der Nähe des Zielservers, und jedes KX II-101-V2-Gerät verfügt über eine eigene IP-Adresse. Jedes Gerät wird über ein externes Netzteil mit Strom versorgt.

Das KX II-101-V2 kann als eigenständige Anwendung verwendet oder zu einer einzelnen logischen Lösung integriert werden (zusammen mit anderen Zugriffsprodukten von Raritan), wenn die Verwaltungseinheit CommandCenter Secure Gateway (CC-SG) 5.4 oder eine höhere Verwaltungseinheit von Raritan verwendet wird.



Diagrammschlüssel	
1	KX II-101-V2
2	LAN
3	Windows <sup>®</sup> -, Linux <sup>®</sup> - und Sun <sup>™</sup> -Server
4	TCP/IP
5	LAN
6	Remotezugriff (Netzwerk)
7	Mobiler Zugriff über iPhone <sup>®</sup> und iPad <sup>®</sup> mithilfe von CC-SG

---

## KX II-101-V2-Hilfe

Die KX II-101-V2-Hilfe enthält Informationen zur Installation, Einrichtung und Konfiguration des KX II-101-V2. Sie enthält ebenfalls Informationen zum Zugriff auf Zielsever, zur Verwendung von virtuellen Medien, zur Verwaltung von Benutzern und Sicherheit sowie zur Wartung und Diagnose von Problemen des KX II-101-V2.

Weitere Informationen und wichtige Hinweise zur aktuellen Version entnehmen Sie vor der Verwendung von KX II-101-V2 den KX II-101-V2-Versionshinweisen.

Eine PDF-Version des Hilfedokuments kann von der Seite **Firmware- und Dokumentationsseite von Raritan** auf der Raritan-Website heruntergeladen werden. Besuchen Sie die Raritan-Website, um die jeweils neuesten Benutzerhandbücher einzusehen.

Um die Online-Hilfe zu verwenden, muss die Option "Active Content" (Aktive Inhalte) Ihres Browsers aktiviert sein. Wenn Sie den Internet Explorer 7 verwenden, müssen Sie "Scriptlets" aktivieren. Informationen zur Aktivierung dieser Funktionen finden Sie in der Hilfe Ihres Browsers.

---

### Neuerungen im Hilfedokument

Die folgenden Informationen wurden als Folge von Verbesserungen und Änderung am Gerät und/oder an der Benutzerdokumentation hinzugefügt.

- Unterstützung der Verschlüsselung mit dem FIPS 140-2-Modul
- Unterstützung von Sicherheitsmeldungen beim Anmeldevorgang
- Mobiler Zugriff über iPad® und iPhone® auf Server, die mit einem KX II-101-V2-Gerät verbunden sind, das von CC-SG verwaltet wird
- Unterstützung von SNMPv3
- Hochladen eigener SSL-Zertifikate auf das KX II-101-V2
- Unterstützung von 1920x1080 & Wide Screen-Videoauflösungen
- Konfigurierbare TCP/IP-Portnummern (Stealth Mode)
- Direkter Zugriff auf KX II-101-V2 bei gleichzeitiger Verwaltung mit CC-SG 5.4 oder höher
- Unterstützung Virtueller Medien für Linux® und Mac®
- Unterstützung von Benutzeroberflächen in Japanisch, traditionellem Chinesisch sowie in vereinfachtem Chinesisch
- Unterstützung von IPv4 und IPv6 in einer Dual-Stack-Umgebung
- Trennen der Benutzer von Ports
- Erzwungene Benutzerabmeldung
- Aktualisierungen des SNMP-Traps und der Benutzeroberfläche für SNMP-Agenten bei KX II-101-V2

Weitere Erklärungen zu den Änderungen am Gerät und an dieser Version des Hilfedokuments finden Sie in den Versionshinweisen zu KX II-101-V2.

---

### Verwandte Dokumentation

Zur KX II-101-V2-Hilfe gehört auch eine KX II-101-V2-Kurzanleitung, die Sie auf der **Firmware- und Dokumentationsseite von Raritan** auf der **Raritan-Website** (<http://www.raritan.com/support/firmware-and-documentation>) finden.

Installationsanforderungen und -anweisungen für Client-Anwendungen, die mit <ProductName> verwendet werden, finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**, welches ebenso auf der Raritan-Website verfügbar ist. Spezifische Client-Funktionen, die mit KX II-101-V2 verwendet werden, finden Sie in der Hilfe.

---

## Produktfotos



KX II-101-V2

---

## Produktfeatures

---

### Schnittstellen

- Integrierte PS/2-KVM-Verbindung
- USB-Verbindung zur Steuerung und für virtuelle Medien
- Serieller Verwaltungsport "Admin" für anfängliche Gerätekonfigurationen und -diagnosen und zur Verwendung mit einem externen Modemzugriff und einer Powerstrip-Steuerung von Raritan.
- Lokaler Port für eine Verbindung zum Monitor
- Ethernet-LAN-Port für automatische 10/100-Base-T-Erkennung, Vollduplex

---

### Netzwerkconfiguration

- DHCP oder Statische IP-Geräteadresse

---

### Systemverwaltungsfunktionen

- Firmware-Aktualisierung über Ethernet
- Ausfallsichere Firmware-Aktualisierung
- Eine Uhr, die manuell oder durch Synchronisierung mit Network Time Protocol (NTP/SNTP) eingestellt werden kann
- Lokaler SNMP-V2-Agent für ein mit einem Zeitstempel versehenes Administratoraktivitätsprotokoll, der durch den Administrator deaktiviert werden kann
- Unterstützung von RADIUS- und LDAP/LDAPS-Authentifizierungsprotokollen

---

### Verwaltungsfunktionen

- Webbasierte Verwaltung
- LDAP-, Active Directory®, RADIUS- oder interne Authentifizierung und Autorisierung
- DHCP oder feste IP-Adressen
- Integration in die Verwaltungseinheit CommandCenter Secure Gateway (CC-SG) von Raritan
- Mobiler Zugriff über iPad® und iPhone® auf Server, die mit einem KX II-101-V2-Gerät verbunden sind, das von CC-SG verwaltet wird
- Unterstützung der Verschlüsselung mit dem FIPS 140-2-Modul
- Unterstützung von Sicherheitsmeldungen beim Anmeldevorgang
- Unterstützung von SNMPv3
- Hochladen eigener SSL-Zertifikate auf das KX II-101-V2
- Konfigurierbare TCP/IP-Portnummern (Stealth Mode)
- Unterstützung von IPv4 und IPv6 in einer Dual-Stack-Umgebung
- Trennen der Benutzer von Ports
- Erzwungene Benutzerabmeldung

---

### Benutzerfunktionen

- Webbasierter Zugriff über bekannte Browser
- Intuitive grafische Benutzeroberfläche (GUI)
- Modus „PC Share“ (PC-Freigabe), bei dem mehr als ein Remote-Benutzer zulässig ist
- TCP-Kommunikation
- Unterstützung und Hilfe zu Benutzeroberflächen in Englisch, Japanisch, traditionellem Chinesisch sowie in vereinfachtem Chinesisch
- Zugriff auf virtuelle Medien
- Absolute Mouse Synchronization™
- Plug-and-Play
- 256-Bit-Verschlüsselung des gesamten KVM-Signals, einschließlich Video und virtueller Medien

---

### Stromversorgung

- Wird über einen externen Netzadapter mit Strom versorgt

---

### Videoauflösung

- Auflösungen von bis zu 1920x1080 bei bis zu 60 Hz und Wide Screen-Videoauflösungen

---

### Montage

- Gestellhalterung

---

## Terminologie

Term	Beschreibung
Zielserver	Server für den Remote-Zugriff über das KX II-101-V2 und die verbundene KVM-Konfiguration.
Remote-PC	Ein Computer mit Windows®, Linux® oder Apple Macintosh® für den Zugriff auf und die Steuerung der Zielserver, die mit KX II-101-V2 verbunden sind.
Serieller Verwaltungsport „Admin“	Nutzen Sie den seriellen Verwaltungsport "Admin", um eine Verbindung mit dem seriellen Port des PC über das DB9-Steckerkabel herzustellen. Verwenden Sie dann ein standardmäßiges Emulationssoftwarepaket (z. B. HyperTerminal), um auf den seriellen Verwaltungsport "Admin" zuzugreifen. Der serielle Verwaltungsport "Admin"



Term	Beschreibung
	wird für die Netzwerkkonfiguration verwendet.
Lokaler Benutzer-Port „Local User“	Ermöglicht einem Benutzer, der sich in unmittelbarer Nähe des Zielservers befindet, die Verwendung des systemeigenen Monitors, ohne die Verbindung zu KX II-101-V2 zu trennen.
Virtuelle Medien	Ermöglicht den Remote-Zugriff eines KVM-Zielservers über einen Client-PC und Netzwerkdateiserver auf Medien.

---

## Paketinhalt

Im Lieferumfang jedes KX II-101-V2-Geräts ist Folgendes enthalten:

- KX II-101-V2 – KVM-über-IP
- KVM-Kabel
- Netzadapter – 5VDC mit universellem Adapter
- Gestellhalterungskit
- Kurzanleitung für die Installation und Konfiguration
- Anwendungshinweise (falls zutreffend)
- Technische Hinweise (falls zutreffend)

# Kapitel 2 Installation und Konfiguration

## In diesem Kapitel

Überblick.....	9
Standard-Anmeldeinformationen.....	9
Erste Schritte .....	10

---

## Überblick

In diesem Kapitel wird beschrieben, wie KX II-101-V2 installiert und konfiguriert wird. Die Installation und Konfiguration umfasst folgende Schritte:

- **Schritt 1: Konfigurieren des Zielservers** (siehe "**Schritt 1: Konfigurieren des Zielservers**" auf Seite 10)
- **Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall** (siehe "**Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall**" auf Seite 23)
- **Schritt 3: Anschließen der Geräte** (siehe "**Schritt 3: Anschließen der Geräte**" auf Seite 24)
- **Schritt 4: Konfigurieren von KX II-101-V2** (siehe "**Schritt 4: Konfigurieren von KX II-101-V2**" auf Seite 29)

Um eine optimale Leistung sicherzustellen, müssen Sie vor der Installation von KX II-101-V2 zunächst den Zielserver konfigurieren, auf den Sie über KX II-101-V2 zugreifen möchten. Beachten Sie, dass die folgenden Konfigurationsanforderungen nur für den Zielserver und nicht für die Computer gelten, die Sie für den Remote-Zugriff auf KX II-101-V2 verwenden.

---

## Standard-Anmeldeinformationen

Standard	Wert
Benutzername	Der Standardbenutzername ist "admin". Dieser Benutzer besitzt Administratorrechte.
Kennwort	Das Standardkennwort ist "raritan". 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 KX II-101-V2 müssen Sie das Standardkennwort ändern.

Standard	Wert
IP-Adresse	KX II-101-V2 wird mit der Standard-IP-Adresse 192.168.0.192 geliefert.

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

---

## Erste Schritte

KX II-101-V2-Benutzer mit Microsoft® Internet Explorer® Version 6 oder Windows 2000® müssen auf Service Pack 4 (SP4) oder höher aktualisieren.

Das KX II-101-V2 wird mit der standardmäßigen statischen IP-Adresse ausgeliefert. In einem Netzwerk ohne DHCP-Server müssen Sie eine neue statische IP-Adresse, eine Netzmaske und eine Gateway-Adresse über die serielle KX II-101-V2-Verwaltungskonsole oder die KX II-101-V2-Remote-Konsole konfigurieren.

Weitere Informationen zum Zuweisen von IP-Adressen für KX II-101-V2 über die Remote-Konsole finden Sie unter **Zuweisen einer IP-Adresse** (auf Seite 30). Siehe **Konfigurieren von KX II-101-V2 unter der Verwendung eines Terminalemulationsprogramms (Optional)** (auf Seite 35) für weitere Informationen zum Einrichten einer IP-Adresse über die serielle Verwaltungskonsole.

---

### Schritt 1: Konfigurieren des Zielservers

Um eine optimale Leistung sicherzustellen, müssen Sie vor der Installation von KX II-101-V2 zunächst den Zielserver konfigurieren, auf den Sie über KX II-101-V2 zugreifen möchten. Beachten Sie, dass die folgenden Konfigurationsanforderungen nur für den Zielserver und nicht für die Computer gelten, die Sie für den Remote-Zugriff auf die KX II-101-V2-Einheit verwenden.

### Einstellen der Videoauflösung des Servers

Für optimale Bandbreiteneffizienz und Videoleistung sollten Zielsever mit grafischen Benutzeroberflächen, wie beispielsweise Windows®, X-Windows®, Solaris™ und KDE, mit einem überwiegend einfarbigen, normalen, hellen Hintergrund konfiguriert sein. Hintergrundbilder mit Fotos oder komplexen Farbverläufen sollten vermieden werden.

Stellen Sie sicher, dass die Videoauflösung und die Aktualisierungsfrequenz des Servers von der KX II-101-V2-Einheit unterstützt werden und das Signal keinen Zeilensprung beinhaltet. Die folgenden Auflösungen werden von KX II-101-V2 unterstützt:

Auflösungen	
640 x 350 bei 70Hz	1024 x 768 bei 85Hz
640 x 350 bei 85Hz	1024 x 768 bei 75Hz
640 x 400 bei 56Hz	1024 x 768 bei 90Hz
640 x 400 bei 84Hz	1024 x 768 bei 100Hz
640 x 400 bei 85Hz	1152 x 864 bei 60Hz
640 x 480 bei 60Hz	1152 x 864 bei 70Hz
640 x 480 bei 66,6Hz	1152 x 864 bei 75Hz
640 x 480 bei 72Hz	1152 x 864 bei 85Hz
640 x 480 bei 75Hz	1.152 x 870 bei 75,1Hz
640 x 480 bei 85Hz	1.152 x 900 bei 66Hz
720 x 400 bei 70Hz	1.152 x 900 bei 76Hz
720 x 400 bei 84Hz	1.280 x 720 bei 60Hz
720 x 400 bei 85Hz	1.280 x 960 bei 60Hz
800 x 600 bei 56Hz	1.280 x 960 bei 85Hz
800 x 600 bei 60Hz	1280 x 1024 bei 60Hz
800 x 600 bei 70Hz	1280 x 1024 bei 75Hz
800 x 600 bei 72Hz	1280 x 1024 bei 85Hz
800 x 600 bei 75Hz	1.360 x 768 bei 60Hz
800 x 600 bei 85Hz	1.366 x 768 bei 60Hz
800 x 600 bei 90Hz	1.368 x 768 bei 60Hz
800 x 600 bei 100Hz	1.400 x 1050 bei 60Hz
832 x 624 bei 75,1Hz	1.440 x 900 bei 60Hz
1024 x 768 bei 60Hz	1600 x 1200 bei 60Hz

Auflösungen	
1024 x 768 bei 70Hz	1.680 x 1.050 bei 60Hz
1024 x 768 bei 72Hz	1920 x 1080 bei 60Hz

### **Videoauflösung von Sun**

Sun™-Systeme verfügen über zwei Auflösungseinstellungen: eine Befehlszeilenauflösung und eine GUI-Auflösung. Weitere Informationen zu den Auflösungen, die von KX II-101-V2 unterstützt werden, finden Sie unter **Einstellen der Videoauflösung des Servers** (auf Seite 11).

---

*Hinweis: Falls keine der unterstützten Auflösungen funktioniert, stellen Sie sicher, dass Sie einen Multi-Sync-Monitor verwenden. Einige Monitore funktionieren nicht mit H-und-V-Synchronisation.*

---

#### Befehlszeilenauflösung

▶ **So überprüfen Sie die Befehlszeilenauflösung:**

1. Führen Sie den folgenden Befehl als Stammbenutzer aus: `# eeprom output-device`

▶ **So ändern Sie die Befehlszeilenauflösung:**

1. Geben Sie folgenden Befehl ein: `# eeprom output-device=screen:r1024x768x75`, wobei 1024x768x75 jede von dem KX II-101-V2-Gerät unterstützte Auflösung ist.
2. Starten Sie den Computer neu.

#### GUI-Auflösung/32-Bit

▶ **So überprüfen Sie die GUI-Auflösung von 32-Bit-Karten:**

1. Geben Sie folgenden Befehl ein: `# /usr/sbin/pgxconfig -prconf`

▶ **So ändern Sie die GUI-Auflösung von 32-Bit-Karten:**

1. Geben Sie folgenden Befehl ein: `# /usr/sbin/pgxconfig -res1024x768x75`, wobei 1024x768x75 jede von dem KX II-101-V2-Gerät unterstützte Auflösung ist.
2. Starten Sie den Computer neu.

#### GUI-Auflösung/64-Bit

▶ **So überprüfen Sie die GUI-Auflösung von 64-Bit-Karten:**

1. Geben Sie folgenden Befehl ein: `# /usr/sbin/m64config -prconf`

► **So ändern Sie die Auflösung von 64-Bit-Karten:**

1. Geben Sie folgenden Befehl ein: `# /usr/sbin/m64config -res1024x768x75`, wobei 1024x768x75 jede von dem KX II-101-V2-Gerät unterstützte Auflösung ist.
2. Starten Sie den Computer neu.

GUI-Auflösung/Solaris 8

► **So überprüfen Sie die Auflösung unter Solaris™ 8 für 32-Bit- und 64-Bit-Karten:**

1. Geben Sie folgenden Befehl ein: `# /usr/sbin/fbconfig -prconf`

► **So ändern Sie die Auflösung unter Solaris 8 für 32- und 64-Bit-Karten:**

1. Geben Sie folgenden Befehl ein: `# /usr/sbin/fbconfig -res1024x768x75`, wobei 1024x768x75 jede von dem KX II-101-V2-Gerät unterstützte Auflösung ist.
2. Starten Sie den Computer neu.

**Mauseinstellungen**

KX II-101-V2 arbeitet in verschiedenen Mausmodi: Absolute Mouse Synchronization™ (Mausmodus "Absolute Maussynchronisierung"), Mausmodus "Intelligent" und "Standard".

---

*Hinweis: Verwenden Sie keinen animierten Cursor, wenn Sie den Mausmodus "Intelligent" aktiviert haben.*

---

Für den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisation) müssen die Mausparameter nicht geändert werden. In den Mausmodi "Standard" und "Intelligent" müssen die Mausparameter auf bestimmte Werte festgelegt werden. Diese Werte werden in diesem Absatz näher beschrieben.

Mauskonfigurationen können je nach Ziel-Betriebssystem variieren. Weitere Informationen finden Sie in der Dokumentation für Ihr Betriebssystem.

**Einstellungen für Windows XP, Windows 2003 und Windows 2008**

► **So konfigurieren Sie KVM-Zielsever, auf denen die Betriebssysteme Microsoft® Windows XP®, Windows 2003® oder Windows 2008® ausgeführt werden:**

1. Konfigurieren der Mauseinstellungen:
  - a. Wählen Sie "Start" > "Systemsteuerung" > "Maus" aus.
  - b. Klicken Sie auf die Registerkarte "Zeigeroptionen".
  - c. Führen Sie im Bereich "Bewegung" folgende Schritte aus:

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

---

*Hinweis: Wenn Sie Windows 2003 auf Ihrem Zielsystem ausführen, über KVM auf den Server zugreifen und eine der unten aufgelisteten Aktionen durchführen, kann die Maussynchronisierung deaktiviert werden, wenn diese zuvor aktiviert war. In diesem Fall müssen Sie im Client-Menü "Mouse" (Maus) den Befehl "Synchronize Mouse" (Maus synchronisieren) auswählen, um sie erneut zu aktivieren. Im Folgenden werden die Aktionen aufgelistet, die zur Deaktivierung der Maussynchronisierung führen können:*

*- Öffnen eines Texteditors*

*- Zugreifen auf die Maus- oder Tastatureigenschaften sowie Telefon- und Modusoptionen über die Windows-Systemsteuerung.*

---

2. Deaktivieren Sie die Übergangseffekte:
  - a. Wählen Sie in der Systemsteuerung die Option "Anzeige" aus.
  - b. Klicken Sie auf die Registerkarte "Darstellung".
  - c. Klicken Sie auf "Effekte".
  - d. Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".
  - e. Klicken Sie auf "OK".
3. Schließen Sie die Systemsteuerung.

---

*Hinweis: Für KVM-Zielsever, auf denen Windows XP, Windows 2000 oder Windows 2008 ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über KX II-101-V2 verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die KX II-101-V2-Verbindung beschränken.*

*Die Anmeldeseiten von Windows XP, Windows 2000 und Windows 2008 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von KX II-101-V2 empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisation möglicherweise nicht optimal.*

*Hinweis: Fahren Sie nur fort, wenn Sie sich mit dem Anpassen der Registrierung von Windows-KVM-Zielseverern auskennen. Sie können auf den Anmeldeseiten eine bessere KX II-101-V2-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern:*

*HKey\_USERS\DEFAULT\SystemsteuerungMaus: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.*

---

### **Einstellungen für Windows 7 und Windows Vista**

#### **► So konfigurieren Sie KVM-Zielsever, auf denen Windows Vista® ausgeführt wird:**

1. Konfigurieren der Mauseinstellungen:
  - a. Wählen Sie **Start > Einstellungen > Systemsteuerung > Maus**.
  - b. Wählen Sie "Erweiterte Systemeinstellungen" im linken Navigationsfenster aus. Das Dialogfeld "Systemeigenschaften" wird angezeigt.
  - c. Klicken Sie auf die Registerkarte "Zeigeroptionen".
  - d. 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".
2. Deaktivieren Sie die Animations- und Einblendeffekte:
  - a. Wählen Sie in der Systemsteuerung die Option "System".
  - b. Wählen Sie "Leistungsinformationen" und anschließend "Tools" > "Weitere Tools" > "Darstellung und Leistung von Windows anpassen" aus.
  - c. Klicken Sie auf die Registerkarte "Erweitert".



- d. Klicken Sie in der Gruppe "Leistung" auf die Schaltfläche "Einstellungen", um das Dialogfeld "Leistungsoptionen" zu öffnen.
  - 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
3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

► **So konfigurieren Sie KVM-Zielsever, auf denen Windows 7® ausgeführt wird:**

1. Konfigurieren der Mauseinstellungen:
  - a. Wählen Sie "Start" > "Systemsteuerung" > "Hardware und Sound" > "Maus" aus.
  - b. Klicken Sie auf die Registerkarte "Zeigeroptionen".
  - c. 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.
2. Deaktivieren der Animations- und Einblendeffekte:
  - a. Wählen Sie "Systemsteuerung" > "System und Sicherheit" aus.
  - b. Wählen Sie "System" und anschließend "Erweiterte Systemeinstellungen" im linken Navigationsfenster aus. Das Dialogfeld "Systemeigenschaften" wird angezeigt.
  - c. Klicken Sie auf die Registerkarte "Erweitert".
  - d. Klicken Sie in der Gruppe "Performance" (Leistung) auf die Schaltfläche "Settings" (Einstellungen), um das Dialogfeld "Performance Options" (Leistungsoptionen) zu öffnen.
  - 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
3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

***Einstellungen für Windows 2000***

► **So konfigurieren Sie KVM-Zielserver, auf denen Microsoft® Windows 2000® ausgeführt wird:**

1. Konfigurieren der Mauseinstellungen:
  - a. Wählen Sie "Start" > "Systemsteuerung" > "Maus" aus.
  - b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
    - Stellen Sie die Beschleunigung auf "Keine" ein.
    - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
    - Klicken Sie auf OK.
2. Deaktivieren der Übergangseffekte:
  - a. Wählen Sie in der Systemsteuerung die Option "Anzeige" aus.
  - b. Klicken Sie auf die Registerkarte "Effekte".
    - Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".
3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

---

*Hinweis: Für KVM-Zielsever, auf denen Windows XP, Windows 2000 oder Windows 2008 ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über KX II-101-V2 verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die KX II-101-V2-Verbindung beschränken.*

*Die Anmeldeseiten von Windows XP, Windows 2000 und Windows 2008 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von KX II-101-V2 empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisation möglicherweise nicht optimal.*

*Hinweis: Fahren Sie nur fort, wenn Sie sich mit dem Anpassen der Registrierung von Windows-KVM-Zielseverern auskennen. Sie können auf den Anmeldeseiten eine bessere KX II-101-V2-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern:*

*HKey\_USERS\DEFAULT\Systemsteuerung\Maus: > MouseSpeed = 0; MouseThreshold 1=0; MouseThreshold 2=0.*

---

#### **Linux-Einstellungen (Red Hat 4 und 5 und Fedora 14)**

---

*Hinweis: Die folgenden Einstellungen sind nur für den Mausmodus "Standard" optimiert.*

---

#### ► **So konfigurieren Sie KVM-Zielsever, auf denen Linux® ausgeführt wird (grafische Benutzeroberfläche):**

1. Konfigurieren der Mauseinstellungen:
  - a. Wählen Sie "Main Menu" > "Preferences" > "Mouse" (Hauptmenü > Einstellungen > Maus) aus. Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
  - b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
  - c. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.
  - d. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) die Sensibilität auf niedrig ein.
  - e. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwert auf niedrig ein.
  - f. Schließen Sie das Dialogfeld "Mouse Preferences" (Mauseinstellungen).

---

*Hinweis: Wenn diese Schritte nicht den gewünschten Erfolg erzielen, geben Sie den Befehl "xset mouse 1 1" wie in den Kommandozeilenanweisungen für Linux beschrieben aus.*

---

2. Konfigurieren der Bildschirmauflösung:

- a. Wählen Sie "Main Menu" > "System Settings" > "Display" (Hauptmenü > Systemeinstellungen > Anzeige) aus. Das Dialogfeld "Display Settings" (Anzeigeeinstellungen) wird angezeigt.
- b. Wählen Sie auf der Registerkarte "Display" (Anzeige) eine Auflösung aus, die von KX II-101-V2 unterstützt wird.
- c. Überprüfen Sie auf der Registerkarte "Advanced" (Erweitert), dass die Aktualisierungsfrequenz von KX II-101-V2 unterstützt wird.

---

*Hinweis: Wenn eine Verbindung zum Zielsever hergestellt ist, wird bei vielen grafischen Linux-Umgebungen durch den Befehl "<Strg> <Alt> <+>" die Videoauflösung geändert, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei "XF86Config" oder "/etc/X11/xorg.conf" (je nach X-Server-Distribution) durchgeführt wird.*

---

► **So konfigurieren Sie KVM-Zielsever, auf denen Linux ausgeführt wird (Kommandozeile):**

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-Zielsever eine von KX II-101-V2 unterstützte Auflösung mit einer standardmäßigen VESA-Auflösung und Aktualisierungsfrequenz verwendet.
3. Jeder Linux-Zielsever sollte außerdem so eingestellt sein, dass sich die Deaktivierungszeiten im Bereich von  $\pm 40\%$  der VESA-Standardwerte bewegen.
  - a. Rufen Sie die Xfree86-Konfigurationsdatei **XF86Config** auf.
  - b. Deaktivieren Sie in einem Text-Editor alle nicht von KX II-101-V2 unterstützten Auflösungen.
  - c. Deaktivieren Sie die virtuelle Desktop-Funktion, (nicht von KX II-101-V2 unterstützt).
  - d. Prüfen Sie die Deaktivierungszeiten ( $\pm 40\%$  der VESA-Standardwerte).
  - e. Starten Sie den Computer neu.

---

*Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielsystem abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.*

---

Hinweis für Red Hat- und Fedora KVM-Zielsystem

Wenn auf dem Zielsystem Red Hat® unter Verwendung eines USB-CIM ausgeführt wird und 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-Systeme mit USB-CIMs:**

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.

**Linux-Einstellungen (für den Standardmausmodus)**

---

*Hinweis: Die folgenden Einstellungen sind nur für den Mausmodus "Standard" optimiert.*

---

► **So konfigurieren Sie KVM-Zielsystem, auf denen Linux® ausgeführt wird (grafische Benutzeroberfläche):**

1. Konfigurieren der Mauseinstellungen:
  - a. Red Hat 5-Benutzer: Wählen Sie "Main Menu" > "Preferences" > "Mouse" (Hauptmenü > Einstellungen > Maus) aus. Red Hat 4-Benutzer: Wählen Sie "System" > "Preferences" > "Mouse" (System > Einstellungen > Maus) aus. Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
  - b. Klicken Sie auf die Registerkarte "Motion" (Bewegung).
  - c. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.

- d. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) die Sensibilität auf niedrig ein.
- e. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwert auf niedrig ein.
- f. Schließen Sie das Dialogfeld "Mouse Preferences" (Mauseinstellungen).

---

*Hinweis: Wenn diese Schritte nicht den gewünschten Erfolg erzielen, geben Sie den Befehl "xset mouse 1 1" wie in den Kommandozeilenanweisungen für Linux beschrieben aus.*

---

2. Konfigurieren der Bildschirmauflösung:
  - a. Wählen Sie "Main Menu" > "System Settings" > "Display" (Hauptmenü > Systemeinstellungen > Anzeige) aus. Das Dialogfeld "Display Settings" (Anzeigeeinstellungen) wird angezeigt.
  - b. Wählen Sie auf der Registerkarte "Settings" (Einstellungen) eine Auflösung aus, die von KX II-101-V2 unterstützt wird.
  - c. Klicken Sie auf "OK".

---

*Hinweis: Wenn eine Verbindung zum Zielsever hergestellt ist, wird bei vielen grafischen Linux-Umgebungen durch den Befehl "<Strg> <Alt> <+>" die Videoauflösung geändert, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei "XF86Config" oder "/etc/X11/xorg.conf" (je nach X-Server-Distribution) durchgeführt wird.*

*Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielsever abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.*

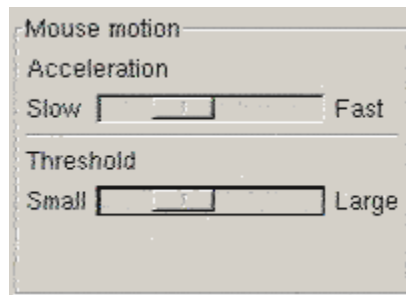
---

### **Einstellungen für Sun Solaris**

Ein Solaris™-Zielsever muss mit einer Anzeigeaufklärung konfiguriert werden, die von KX II-101-V2 unterstützt wird. Nachfolgend die am häufigsten verwendeten, unterstützten Auflösungen für Sun™-Systeme:

Auflösung
1024 x 768 bei 60 Hz
1024 x 768 bei 70 Hz
1024 x 768 bei 75 Hz
1024 x 768 bei 85 Hz
1280 x 1024 bei 60 Hz

Stellen Sie die Mausbeschleunigung und den Schwellenwert auf genau 1 ein. Ein Zielsystem mit dem Solaris-Betriebssystem muss eine VGA-Buchse mit TV-Out-Signal haben (mit H- und V-Synchronisation, keine Composite-Synchronisation). Legen Sie diese Werte über die grafische Benutzeroberfläche oder über die Befehlszeile `xset mouse a t` fest, wobei *a* für die Beschleunigung und *t* für den Schwellenwert steht.



► **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 Befehl `#eeprom output-device=screen:r1024x768x75` aus, um die Ausgabeauflösung zu ändern.
3. Starten Sie den Server mit dem Befehl "boot" neu.

Sie können sich stattdessen auch an Ihren Raritan-Ansprechpartner wenden und einen Videoausgabeadapter erwerben. Für die Verwendung mit der KX II-101-V2-Einheit ist bei Sun-Systemen mit Composite-Synchronisationsausgabe der APSSUN II Guardian-Converter von Raritan erforderlich. HD 15 Sun-Systeme mit separater Synchronisationsausgabe erfordern für die Verwendung mit KX II-101-V2 einen APKMSUN Guardian-Converter von Raritan.

**Einstellungen für Apple Macintosh**

Mac® ist mit KX II-101-V2 direkt kompatibel – es sind keinerlei Installationen notwendig. Sie müssen jedoch den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisation) verwenden und den Mausmodus "Absolute Mouse" (Absolut) und die absolute Mausskalierung für Mac-Server auf der KX II-101-V2-Portseite aktivieren.

► **So aktivieren Sie diese Einstellung:**

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

2. Klicken Sie auf den Port-Namen des Ports, den Sie bearbeiten möchten.
3. Aktivieren Sie im Abschnitt "USB Connection Settings" (USB-Verbindungseinstellungen) die beiden Kontrollkästchen "Enable Absolute Mouse" (Absoluten Mausmodus aktivieren) und "Enable Absolute mouse scaling for MAC server" (Absolute Mausskalierung für Mac-Server aktivieren). Klicken Sie auf "OK".

Siehe **Portkonfiguration** (siehe "**Port Configuration (Port-Konfiguration)**") auf Seite 144).

#### **Einstellungen für IBM AIX**

1. Navigieren Sie zu "Style Manager" (Stilmanager).
2. 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**

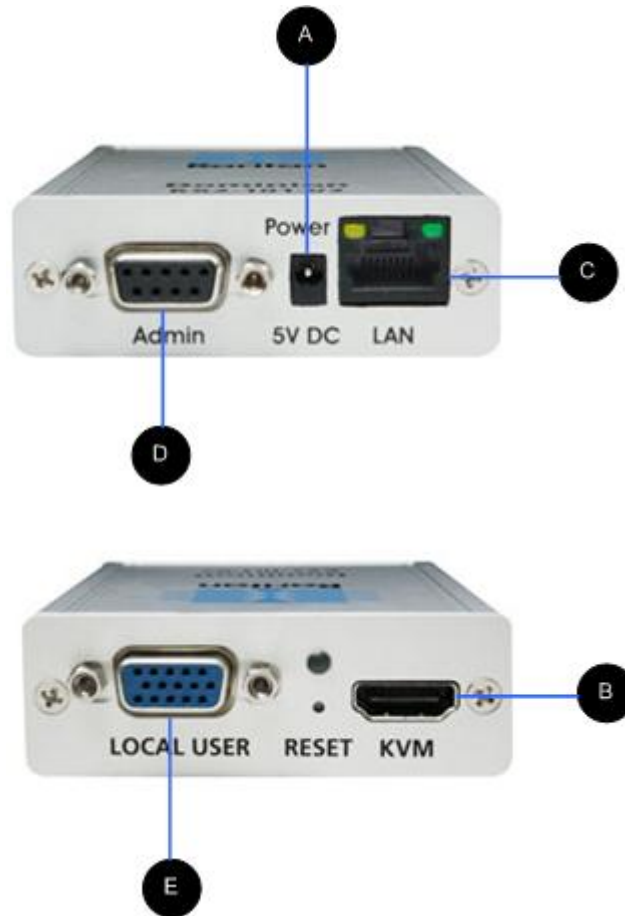
Damit Sie über eine Netzwerk-Firewall auf KX II-101-V2 zugreifen können, muss Ihre Firewall die Kommunikation auf TCP-Port 5000 zulassen. Sie können KX II-101-V2 auch so konfigurieren, dass ein anderer, von Ihnen ausgewählter TCP-Port verwendet wird.

Damit Sie die Webzugriffsmöglichkeiten von KX II-101-V2 nutzen können, muss die Firewall eingehende Kommunikation auf TCP-Port 443 zulassen. Dies ist der TCP-Standard-Port für die HTTPS-Kommunikation. Um die KX II-101-V2-Umleitungsfunktion von HTTP-Anfragen auf HTTPS nutzen zu können (damit Benutzer die bekannteren Adressen "http://xxx.xxx.xxx.xxx" anstelle von "https://xxx.xxx.xxx.xxx" eingeben können), muss die Firewall außerdem die eingehende Kommunikation auf TCP-Port 80 zulassen. Dies ist der TCP-Standard-Port für die HTTP-Kommunikation.



### Schritt 3: Anschließen der Geräte

Die KX II-101-V2-Einheit weist die im Diagramm beschriebenen physischen Anschlüsse auf. Jeder Buchstabe im Diagramm entspricht einem Schritt des hier beschriebenen Geräteverbindungsprozesses.



Diagrammschlüssel		
<b>A</b>	Stromanschluss	Einzelner Netzadapter.
<b>B</b>	KVM-Kabel mit Monitor, PS/2 und USB-Stecker (im Lieferumfang enthalten)	Schließen Sie das mitgelieferte KVM-Kabel an die Tastatur-, Video- und Mausports des Zielservers an.

Diagrammschlüssel		
<b>C</b>	Ethernet LAN	Stellt LAN-Konnektivität her.
<b>D</b>	Port "Admin"	Für folgende Funktionen: <ul style="list-style-type: none"> <li>• Konfiguration und Verwaltung des Geräts mit einem auf dem PC installierten Terminalemulationsprogramm.</li> <li>• Konfiguration und Verwaltung eines Powerstrips (Adapter erforderlich; nicht im Lieferumfang enthalten).</li> <li>• Anschluss eines externen Modems zum Einwählen.</li> </ul>
<b>E</b>	"Local user" (Lokaler Benutzer)	Der lokale Port baut eine Verbindung zu einem Monitor auf.

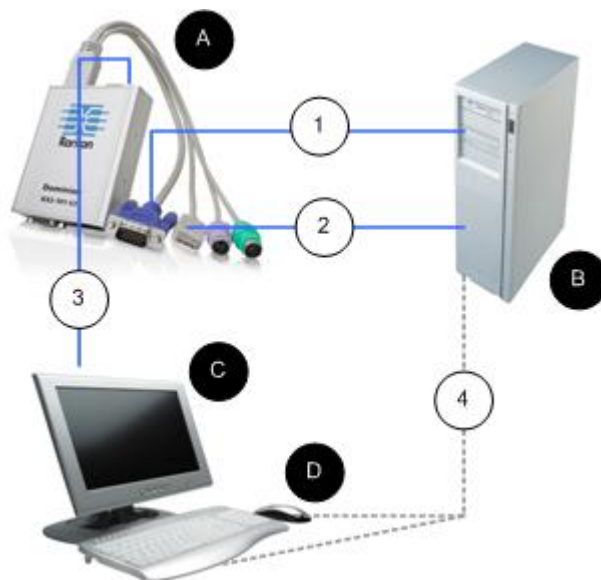
**A: Stromversorgung**

Das KX II-101-V2 wird über einen 100-240V Netzeingang- und 5VDC Netzausgang-Adapter, der in der Lieferung des Geräts mit inbegriffen ist, mit Strom versorgt. Stecken Sie für eine Standardstromversorgung den mitgelieferten Stromadapter in den Stromzufuhr-Port und das andere Ende in eine Steckdose in der Nähe.

**B: Zielserver**

Verwenden Sie entweder den PS/2- oder den USB-Anschluss für eine Verbindung mit dem Zielelement. Stellen Sie vor dem Verbinden sicher, dass der Monitor des Zielservers auf eine unterstützte Auflösung eingestellt ist. Verwenden Sie die USB-Verbindung, wenn Sie virtuelle Medien oder den Mausmodus "Absolut" nutzen.

### USB-Konfiguration



► **So konfigurieren Sie KX II-101-V2 zur Verwendung mit einem USB-Zielserver:**

1. Verwenden Sie das angeschlossene Videokabel, um KX II-101-V2 mit dem Ziel-Videoport zu verbinden.
2. Schließen Sie den USB-Stecker des KVM-Kabels an die KX II-101-V2-Einheit und den USB-Port des Zielservers an.
3. Verbinden Sie einen Monitor mit dem lokalen Port von KX II-101-V2, wenn Sie den lokalen Monitor verwenden möchten. **///Optional**
4. Verbinden Sie die USB-Tastatur und -Maus direkt mit dem Zielelement. **///Optional**

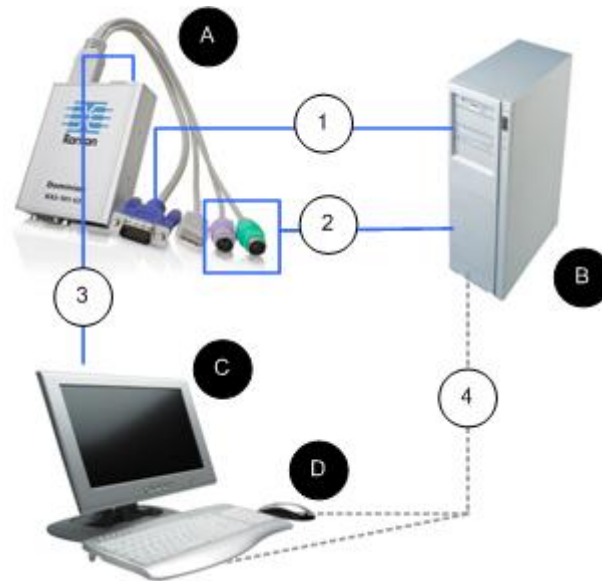
*Hinweis: Wenn Sie virtuelle Medien verwenden, müssen Sie die USB-Verbindung nutzen.*

#### Diagrammschlüssel für USB-Verbindung

<b>A</b>	KX II-101-V2
<b>B</b>	Zielserver
<b>C</b>	Lokaler Monitor (Optional)
<b>D</b>	Lokale Maus und Tastatur (Optional)

Diagrammschlüssel für USB-Verbindung	
1	Videoverbindung von dem KX II-101-V2 mit dem Zielelement
2	USB-Verbindung von dem KX II-101-V2 mit dem Zielelement
3	Optionale Monitorverbindung vom Port "Local User" von KX II-101-V2 zum Monitor
4	Optionale USB-Verbindung vom Zielsever zur Maus und Tastatur (Kabel nicht im Lieferumfang inbegriffen)

### PS/2-Konfiguration



► **So konfigurieren Sie KX II-101-V2 zur Verwendung mit einem PS/2-Zielserver:**









1. Verwenden Sie das angeschlossene Videokabel, um KX II-101-V2 mit dem Ziel-Videoport zu verbinden.
  2. Verbinden Sie einen PS/2-Anschluss des KVM-Kabels mit einem PS/2-Port auf dem Zielelement.
  3. Verbinden Sie einen Monitor mit dem Port "Local User" von KX II-101-V2, wenn Sie den lokalen Monitor verwenden möchten.
- ///Optional**

4. Wenn Sie über eine PS/2-Tastatur und -Maus verfügen, verwenden Sie für den USB-Adapter einen PS/2-Anschluss (nicht im Lieferumfang inbegriffen), um eine direkte Verbindung mit dem USB-Port des Zielelements herzustellen. **///Optional**

---

*Hinweis: Wenn Sie virtuelle Medien verwenden, müssen Sie die USB-Verbindung nutzen.*

---

Diagrammschlüssel für PS/2-Verbindungen	
	KX II-101-V2
	Zielserver
	Lokaler Monitor
	Lokale Maus und Tastatur (Optional)
	Videoverbindung von dem KX II-101-V2 mit dem Zielelement
	Verbindung von dem KX II-101-V2 mit dem Zielserver über ein KVM-Kabel
	Verbindung KX II-101-V2 mit Monitor (Optional)
	Verbindung PS/2-Anschluss mit USB-Adapter (Optional; Kabel im Lieferumfang nicht inbegriffen) vom Zielelement zur Tastatur und Maus

### C: Network (Netzwerk)

Verbinden Sie den Netzwerk-Port „LAN“ über ein standardmäßiges Ethernet-Kabel mit einem Ethernet-Switch, -Hub oder -Router. Die LAN-LEDs über der Ethernet-Verbindung zeigen die Ethernet-Aktivität an. Die gelbe LED blinkt, während KX II-101-V2 verwendet wird, und zeigt damit IP-Datenverkehr mit 10 Mbit/s an. Die grüne LED zeigt eine Verbindungsgeschwindigkeit von 100 Mbit/s an.

#### **D: Port „Admin“**

Über den Port „Admin“ können Sie KX II-101-V2 über ein Terminalemulationsprogramm, wie z. B. HyperTerminal, konfigurieren und einrichten. Verwenden Sie ein serielles DB9M - DB9F Straight-Kabel, um KX II-101-V2 mit dem seriellen Port auf Ihrem PC oder Laptop zu verbinden. Die Kommunikationseinstellungen des seriellen Ports sollten wie folgt konfiguriert werden:

- 115.200 Baud
- 8 Datenbits
- 1 Stoppbit
- Keine Parität
- Keine Flusssteuerung

#### **E: Port "Local User" (Lokaler Benutzer)**

Der Port "Local User" (Lokaler Benutzer) dient als Durchgang für den Monitor des Zielservers und ist somit direkt mit dem Monitor verbunden. Die lokale Tastatur und Maus müssen direkt mit dem Zielserver verbunden werden.

Bei USB-Konfigurationen wird nur der lokale Monitor über den Port „Local User“ mit dem Zielserver verbunden. Tastatur und Maus werden direkt über USB-Ports mit dem Zielserver verbunden.

---

### **Schritt 4: Konfigurieren von KX II-101-V2**

---

*Hinweis: Sie müssen ein Crossover-Kabel zur Verbindung zwischen KX II-101-V2 und Client verwenden, wenn Sie das KX II-101-V2 über einen Webbrowser konfigurieren.*

---

#### **Konfigurieren von KX II-101-V2 unter Verwendung der Remote-Konsole**

Die KX II-101-V2-Remote-Konsole ist eine webbasierte Anwendung, mit der Sie das Gerät vor der Verwendung konfigurieren und danach verwalten können. Bevor Sie KX II-101-V2 über die Remote-Konsole konfigurieren können, müssen Sie Ihre Workstation und das Gerät mit einem Netzwerk verbinden.

Sie können ebenfalls ein Terminalemulationsprogramm zur Konfiguration von KX II-101-V2 verwenden. Siehe **Konfigurieren von KX II-101-V2 unter der Verwendung eines Terminalemulationsprogramms (Optional)** (auf Seite 35).

### **Einrichten eines neuen Kennworts**

Wenn Sie sich zum ersten Mal bei der Remote-Konsole anmelden, werden Sie aufgefordert, das Standardkennwort zu ersetzen. Danach können Sie KX II-101-V2 konfigurieren.

1. Melden Sie sich bei einer Workstation an, die über eine Netzwerkverbindung zu Ihrem KX II-101-V2-Gerät verfügt.
2. Starten Sie einen unterstützten Webbrowser, z. B. Internet Explorer® (IE) oder Firefox®.
3. Geben Sie in der Adresszeile des Browsers die Standard-IP-Adresse des Geräts ein: 192.168.0.192.
4. Drücken Sie die Eingabetaste. Die Anmeldeseite wird angezeigt.
5. Geben Sie den Benutzernamen `admin` und das Kennwort `raritan` ein.
6. Klicken Sie auf "Login" (Anmelden). Die Seite "Change Password" (Kennwort ändern) wird angezeigt.
7. Geben Sie `raritan` im Feld "Old Password" (Altes Kennwort) ein.
8. Geben Sie ein neues Kennwort in die Felder "New Password" (Neues Kennwort) und "Confirm New Password" (Neues Kennwort bestätigen) ein. Das Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie aus druckbaren Sonderzeichen bestehen.
9. Klicken Sie auf "Apply" (Übernehmen). Die erfolgreiche Änderung des Kennworts wird bestätigt.
10. Klicken Sie auf "OK". Die Seite "Port Access" (Port-Zugriff) wird angezeigt.

### **Zuweisen einer IP-Adresse**

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter **Netzwerkeinstellungen** (siehe "**Network Settings (Netzwerkeinstellungen)**" auf Seite 120).

#### **► So weisen Sie eine IP-Adresse zu:**

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen > Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr KX II-101-V2-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.
3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:

- a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
  - b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
  - c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
  - d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
  - e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
    - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.  
Diese Option wird empfohlen, da KX II-101-V2 ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.
    - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.  
Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server zugewiesen. Bei Verwendung von DHCP geben Sie unter "Preferred host name (DHCP only)" (Name des bevorzugten Hosts [Nur DHCP]) einen Wert ein (maximal 63 Zeichen).
4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
- a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.
  - b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem KX II-101-V2 zugeordnet ist.
  - c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.
  - d. Geben Sie die IP-Adresse des Gateway ein.
  - e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lese-zugriff)**
  - f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lese-zugriff)**
  - g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:



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

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

- Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.
5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.
  6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

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

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

Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter **LAN-Schnittstelleneinstellungen** (siehe "**LAN Interface Settings (LAN-Schnittstelleneinstellungen)**") auf Seite 125).

---

*Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des KX II-101-V2 den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben. Weitere Informationen finden Sie auf der Seite **Network Settings** (siehe "**Network Settings (Netzwerkeinstellungen)**") auf Seite 120) (Netzwerkeinstellungen).*

---

#### **Benennen des Zielservers**

1. Verbinden Sie den KX II-101-V2 mit dem Zielservers.
2. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
3. Klicken Sie unter Port Name (Port-Name) auf den Zielservers. Die Seite "Port" wird angezeigt.
4. Geben Sie einen Namen mit bis zu 32 alphanumerische Zeichen und Sonderzeichen ein.

5. Klicken Sie auf "OK".

**Port 1**

Type:  
KVM

Name:  
Dominion\_KX2\_101\_Port1

**Power Association**

Power Strip Name	Outlet Name
None	---
	---
	---
	---

▶ USB Connection Settings

▶ Advanced USB Connection Settings

### **Remoteauthentifizierung**

#### **Hinweis für CC-SG-Benutzer**

Wenn KX II-101-V2 von CommandCenter Secure Gateway gesteuert wird, authentifiziert CC-SG Benutzer und Gruppen.

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

#### **Unterstützte Protokolle**

Zur Vereinfachung der Verwaltung von Benutzernamen und Kennwörtern bietet KX II-101-V2 die Möglichkeit, Authentifizierungsanforderungen an einen externen Authentifizierungsserver weiterzuleiten. Zwei externe Authentifizierungsprotokolle werden unterstützt: LDAP/LDAPS und RADIUS.

### **Hinweis zu Microsoft Active Directory**

Microsoft® Active Directory® verwendet nativ das LDAP/LDAPS-Protokoll und kann als LDAP/LDAPS-Server und Authentifizierungsquelle für KX II-101-V2 fungieren. Bei Verwendung der IAS-Komponente (Internetautorisierungsserver) kann ein Microsoft Active Directory-Server auch als RADIUS-Authentifizierungsquelle dienen.

### ***Erstellen von Benutzergruppen und Benutzern***

Im Rahmen der Erstkonfiguration müssen Sie Benutzergruppen und Benutzer definieren, damit Benutzer auf KX II-101-V2 zugreifen können.

KX II-101-V2 verwendet im System bereits vorhandene Standardbenutzergruppen und ermöglicht es Ihnen, Gruppen zu erstellen und entsprechende Berechtigungen für sie festzulegen.

Für den Zugriff auf KX II-101-V2 sind ein Benutzername und ein Kennwort erforderlich. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf KX II-101-V2 zuzugreifen. Weitere Informationen zum Hinzufügen oder Bearbeiten von Benutzergruppen und Benutzern finden Sie unter **Benutzerverwaltung** (siehe "**User Management (Benutzerverwaltung)**" auf Seite 93).

### **Konfigurieren von KX II-101-V2 unter der Verwendung eines Terminalemulationsprogramms (Optional)**

Sie können die serielle Verwaltungskonsole mit einem Terminalemulationsprogramm, wie z. B. HyperTerminal verwenden, um die folgenden Konfigurationsparameter für KX II-101-V2 festzulegen:

- IP-Adresse
- Adresse der Subnetzmaske
- Gateway-Adresse
- Automatische IP-Konfiguration
- LAN-Geschwindigkeit
- LAN-Schnittstellenmodus

Um zusammen mit dem KX II-101-V2-Gerät ein Terminalemulationsprogramm verwenden zu können, müssen Sie zuerst das mitgelieferte serielle RS-232-Kabel vom Port "Admin" des KX II-101-V2-Geräts mit dem COM1-Port des PCs verbinden.

Zu Demonstrationszwecken wird in diesem Abschnitt HyperTerminal als Terminalemulationsprogramm verwendet. Sie können ein beliebiges Terminalemulationsprogramm verwenden.

#### **► So verwenden Sie ein Terminalemulationsprogramm zur Konfiguration von KX II-101-V2:**

1. Verbinden Sie KX II-101-V2 mit einem lokalen PC.

2. Stellen Sie eine Verbindung zwischen dem Port „Admin“ der KX II-101-V2-Einheit und dem COM1-Port des PCs her.
3. Starten Sie das Terminalemulationsprogramm, das Sie zur Konfiguration von KX II-101-V2 verwenden möchten.
4. Legen Sie die folgenden Port-Einstellungen im Terminalemulationsprogramm fest:
  - Bits pro Sekunde – 115200
  - Datenbits – 8
  - Parität – Keine
  - Stopp-Bits – 1
  - Flusssteuerung – Keine
5. Stellen Sie eine Verbindung zur KX II-101-V2-Einheit her. Die Anmeldeseite wird angezeigt.
6. Geben Sie den Administrator-Benutzernamen ein, und drücken Sie die Eingabetaste. Sie werden zur Eingabe des Kennworts aufgefordert.
7. Geben Sie den standardmäßigen Administrator-Benutzernamen *admin* ein, und drücken Sie die Eingabetaste. Sie werden zur Eingabe Ihres Kennworts aufgefordert.
8. Geben Sie *config* bei der Eingabeaufforderung "Admin Port" > (Port "Admin") ein, und drücken Sie die Eingabetaste.
9. Geben Sie *network* bei der Eingabeaufforderung "Config" > (Konfig) ein, und drücken Sie die Eingabetaste.
10. Sie können neue Netzwerkeinstellungen konfigurieren. Geben Sie dazu "interface" gefolgt von einem der folgenden Befehle und dem entsprechenden Argument (Option) an der Eingabeaufforderung "Network" ein. Drücken Sie dann die Eingabetaste.

Befehl	Argument	Options (Optionen)
ipauto	none dhcp	<p>"none" (Keine): Sie können manuell eine IP-Adresse für das Gerät angeben. Diese Option muss mit dem Befehl "ip" und der IP-Adresse verwendet werden (siehe folgendes Beispiel):</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p>"dhcp": Weist dem Gerät beim Start automatisch eine IP-Adresse zu.</p>

Befehl	Argument	Options (Optionen)
		<code>interface ipauto dhcp</code>
ip	IP-Adresse	Die IP-Adresse, die dem Gerät zugewiesen werden soll. Damit Sie zum ersten Mal manuell eine IP-Adresse festlegen können, muss dieser Befehl mit dem Befehl "ipauto" und der Option "none" verwendet werden. Weitere Informationen finden Sie unter "ipauto". Nachdem Sie einmal manuell eine IP-Adresse zugewiesen haben, müssen Sie nur den Befehl "ip" verwenden, um die IP-Adresse zu ändern.
mask	subnet mask	Befehlszeile sollte "interface" lauten. <code>interface   ip   ...</code> <code>interface   mask   Die IP-Adresse der Subnetzmaske</code> <code>interface   gw   Die Gateway-IP-Adresse</code> <code>interface   mode  </code> <code>....</code>
gw	IP-Adresse	Die Gateway-IP-Adresse.
Modus	Modus	Der Ethernet-Modus. Folgende Optionen stehen zur Auswahl: <ul style="list-style-type: none"> <li>▪ "auto": Die Geschwindigkeit und der Schnittstellenmodus werden automatisch basierend auf dem Netzwerk festgelegt.</li> <li>▪ 10hdx – 10 Mbit/s, Halbduplex</li> <li>▪ 10fdx – 10 Mbit/s, Vollduplex.</li> </ul>

Befehl	Argument	Options (Optionen)
		<ul style="list-style-type: none"><li>▪ 100hdx – 100 Mbit/s, Halbduplex</li><li>▪ 100fdx – 100 Mbit/s, Vollduplex</li></ul>

Nachdem Sie erfolgreich eine Einstellung geändert haben, wird eine Bestätigungsmeldung wie die Folgende angezeigt:

```
Admin Port > Config
Admin Port > Config > Network
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.126

Network interface configuration successful.
(Schnittstellenkonfiguration von Netzwerk
erfolgreich.)
```

Geben Sie nach der Konfiguration von KX II-101-V2 an der Eingabeaufforderung *logout* ein, und drücken Sie die Eingabetaste. Sie werden von der der Befehlszeilenschnittstelle abgemeldet.

## Kapitel 3 Arbeiten mit Zielservern

### In diesem Kapitel

Schnittstellen .....	39
Virtual KVM Client (VKC).....	50

---

### Schnittstellen

---

#### Oberfläche der KX II-101-V2-Remotekonsole

Die KX II-101-V2-Remotekonsole ist eine browserbasierte grafische Benutzeroberfläche, mit der Sie sich an KVM-Zielservern und seriellen Zielgeräten, die mit KX II-101-V2 verbunden sind, anmelden und KX II-101-V2 von einem Remotestandort aus verwalten können.

Die KX II-101-V2-Remotekonsole bietet eine digitale Verbindung mit den angeschlossenen KVM-Zielservern. Wenn Sie sich über die KX II-101-V2-Remotekonsole bei einem KVM-Zielserver anmelden, wird ein Fenster für den Virtual KVM Client geöffnet.

---

*Hinweis: Wenn Sie Internet Explorer®7 verwenden, können bei der Verbindung zu einem Zielserver Berechtigungsfehler auftreten. Um diese Fehler zu vermeiden, führen Sie Folgendes durch:*

1. Klicken Sie im Internet Explorer auf "Tools" (Extras) > "Internet Options" (Internetoptionen), um das Dialogfeld "Internet Options" (Internetoptionen) zu öffnen.
  2. Klicken Sie im Bereich "Temporary Internet Files" (Temporäre Internetdateien) auf "Settings" (Einstellungen). Das Dialogfeld "Settings" (Einstellungen) wird angezeigt.
  3. Wählen Sie im Bereich "Check for newer versions of stored pages" (Nach neueren Versionen gespeicherter Seiten suchen) die Option "Automatically" (Automatisch) aus.
  4. Klicken Sie auf "OK", um die Einstellungen zu übernehmen.
- 

#### Direkten Port-Zugriff aktivieren

Über direkten Port-Zugriff können Sie auf den KX II-101-V2-Remote-Client ohne das übliche Anmeldefenster zugreifen. Wenn der direkte Port-Zugriff aktiviert ist, können Sie einen URL angeben, um direkt zur Seite "Port Access" (Port-Zugriff) zu wechseln.

► **So aktivieren Sie den direkten Port-Zugriff:**

1. Starten Sie die KX II-101-V2-Remote-Konsole.



2. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Services" (Gerätedienste) öffnet sich.
3. Aktivieren Sie das Kontrollkästchen "Enable Direct Port Access via URL" (Direkten Port-Zugriff über URL aktivieren).
4. Klicken Sie auf "Save" (Speichern).

► **So definieren Sie einen URL für den direkten Port-Zugriff:**

- Definieren Sie eine URL mit IP-Adresse, Benutzername, Kennwort, und, falls erforderlich, Port-Nummer von KX II-101-V2.

Verwenden Sie folgendes Format für den URL für direkten Port-Zugriff:

```
https://IP-Adresse/dpa.asp?username=Benutzername&password=Kennwort
```

---

*Tipp: Definieren Sie den URL für den direkten Port-Zugriff einmalig, und speichern Sie ihn in Ihrem Webbrowser als Favorit.*

---

#### **Navigation in der KX II-101-V2-Konsole**

In den Oberflächen der KX II-101-V2-Konsolen haben Sie viele Möglichkeiten für die Navigation und Auswahl.

► **Für die Auswahl von Optionen stehen folgende Möglichkeiten zur Verfügung:**

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

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

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

**Linker Bildschirmbereich**

Der linke Bildschirmbereich der KX II-101-V2-Oberfläche enthält folgende Informationen. Beachten Sie, dass die Anzeige einiger Informationen abhängig vom Benutzer, von der verwendeten Funktion usw. ist. Die bedingten Informationen werden nachfolgend aufgeführt.

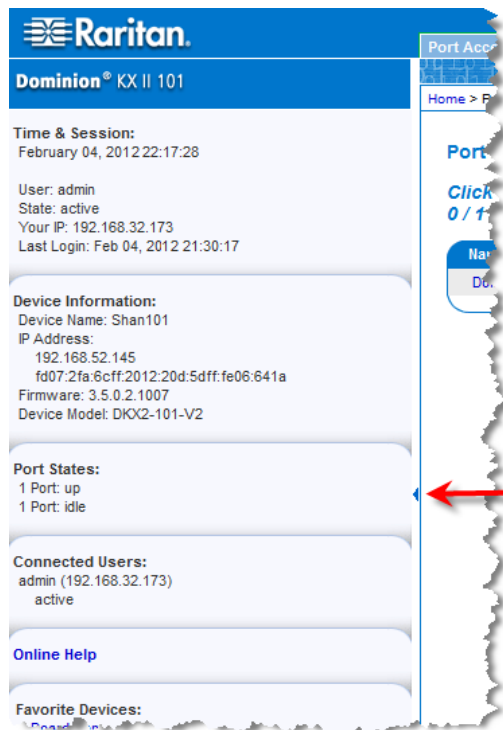
Informationen	Beschreibung	Anzeige
Zeit & Sitzung	Das aktuelle Datum und die aktuelle Zeit.	Immer
Benutzer	Benutzername des aktuellen Benutzers	Immer
Status	Der aktuelle Status der Anwendung, entweder inaktiv oder aktiv. Bei Inaktivität zeichnet die Anwendung die Uhrzeit der inaktiven Sitzung auf und zeigt diese an.	Immer
Ihre IP	Die für den Zugriff auf KX II-101-V2 verwendete IP-Adresse.	Immer
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung des aktuellen Benutzers.	Immer
Unter CC-SG-Verwaltung	Die IP-Adresse des CC-SG-Geräts, das KX II-101-V2 verwaltet.	Wenn KX II-101-V2 von CC-SG verwaltet wird.
Device Information (Geräteinformationen)	Informationen zum verwendeten KX II-101-V2.	Immer
Gerätename	Dem Gerät zugewiesener Name.	Immer
IP-Adresse	Die IP-Adresse des KX II-101-V2.	Immer IPv4 und IPv6 wenn es konfiguriert wurde
Firmware	Aktuelle Version der Firmware.	Immer
Gerätemodell	Modell des KX II-101-V2	Immer
Portstatus	Die Status des Ports, der von KX II-101-V2 verwendet wird.	Immer

Informationen	Beschreibung	Anzeige
Verbundene Benutzer	Die Benutzer, identifiziert durch Benutzernamen und IP-Adresse, die aktuell mit KX II-101-V2 verbunden sind.	Immer
Online-Hilfe	Verknüpfung zur Online-Hilfe.	Immer
Bevorzugte Geräte	Siehe Verwalten von Favoriten.	Immer
FIPS-Modus	FIPS-Modus: Aktiviertes SSL-Zertifikat: Kompatibel mit FIPS-Modus	Wenn FIPS aktiviert ist

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

► **So reduzieren Sie den linken Bildschirmbereich:**

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



**Seite "Port Access" (Port-Zugriff)**

Nachdem Sie sich erfolgreich bei der KX II-101-V2-Remotekonsole angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt. Diese Seite enthält alle KX II-101-V2-Ports, die angeschlossenen KVM-Zielsever sowie deren Verfügbarkeit. Über die Seite "Port Access" (Port-Zugriff) haben Sie Zugriff auf den mit KX II-101-V2 verbundenen KVM-Zielsever. Ein KVM-Zielsever ist ein Server, den Sie über das KX II-101-V2-Gerät steuern möchten. Sie sind mit den KX II-101-V2-Ports auf der Rückseite des Geräts verbunden.

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

1. Klicken Sie in der KX II-101-V2-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt. Diese Seite enthält die folgenden Informationen:
  - Port Name (Portname) – Der Name des KX II-101-V2-Ports. Der Portname ist anfangs zu "Dominion\_KX2\_101\_Port1" eingestellt, aber Sie können ihn jederzeit in einen aussagekräftigeren Namen ändern. Wenn Sie auf einen Portnamenlink klicken, wird das Menü "Port Action" (Portaktion) geöffnet.
  - Availability (Verfügbarkeit) – Für die Verfügbarkeit stehen die Werte Idle (Inaktiv), Connected (Verbunden) oder Busy (Verwendet) zur Verfügung.
2. Klicken Sie auf den Portnamen des Zielsevers, auf den Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt. Informationen zu verfügbaren Menüoptionen finden Sie unter **Menü "Port Action" (Portaktion)** (siehe "**Menü Port Action (Portaktion)**" auf Seite 44).
3. Wählen Sie im Menü "Port Action" (Portaktion) den gewünschten Menübefehl aus.

### Menü Port Action (Portaktion)

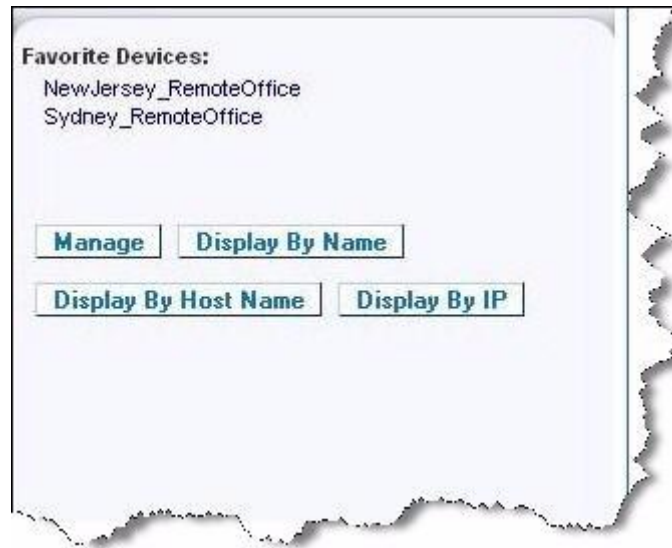
Wenn Sie in der Liste "Port Access" (Portzugriff) auf einen Portnamen klicken, wird das Menü "Port Action" (Portaktion) angezeigt. Wählen Sie die gewünschte Menüoption für den Port aus. Beachten Sie, dass nur je nach Status und Verfügbarkeit des Ports aktuell verfügbare Optionen im Menü "Port Action" (Portaktion) aufgelistet werden:

- Connect (Verbinden) – Erstellt eine neue Verbindung mit dem Zielservers. Für die KX II-101-V2-Remotekonsole wird eine neue **Virtual KVM Client (VKC)** (auf Seite 50)-Seite angezeigt.
- Disconnect (Trennen) – Trennt diese Portverbindung und schließt die Seite des Virtual KVM Client für diesen Zielservers. Diese Menüoption ist nur für den Portstatus Up (Ein) und die Verfügbarkeit Connected (Verbunden) bzw. Up (Ein) und Busy (Verwendet) verfügbar.
- Power On (Strom ein) – Versorgt den Zielservers über die zugeordnete Steckdose mit Strom. Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.
- Power Off (Strom aus) – Unterbricht die Stromversorgung des Zielservers über die zugeordneten Steckdosen. Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht, wenn dieses eingeschaltet ist [Portstatus Up (Ein)] und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.
- Power Cycle (Aus- und Einschalten) – Schaltet den Zielservers über die zugeordneten Steckdosen aus und wieder ein. Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.

### 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" (Port-Zugriff). Hier haben Sie folgende Möglichkeiten:

- Erstellen und Verwalten einer Liste bevorzugter Geräte
  - Schnelles Zugreifen auf häufig verwendete Geräte
  - Auflisten der Favoriten nach Gerätenamen, IP-Adresse oder DNS-Hostname
  - Erkennen von KX II-101-V2-Geräten im Subnetz (vor und nach der Anmeldung)
  - Abrufen erkannter KX II-101-V2-Geräte vom verbundenen Dominion-Gerät (nach der Anmeldung)
- ▶ **So greifen Sie auf ein bevorzugtes KX II-101-V2-Gerät zu:**
- Klicken Sie auf den unterhalb von "Favorite Devices" (Bevorzugte Geräte) aufgeführten Namen des Geräts. Ein neues Browserfenster wird geöffnet.
- ▶ **So zeigen Sie die Favoriten nach Name an:**
- Klicken Sie auf "Display by Name" (Nach Name anzeigen).
- ▶ **So zeigen Sie die Favoriten nach IP-Adresse an:**
- Klicken Sie auf "Display by IP" (Nach IP anzeigen).
- ▶ **So zeigen Sie die Favoriten nach Hostname an:**
- Klicken Sie auf "Display by Host Name" (Nach Hostname anzeigen).



Seite "Manage Favorites" (Favoriten verwalten)

► **So öffnen Sie die Seite "Manage Favorites" (Favoriten verwalten):**

- Klicken Sie auf die Schaltfläche "Manage" (Verwalten) im linken Bildschirmbereich. Die Seite "Manage Favorites" (Favoriten verwalten) wird angezeigt. Diese Seite enthält die folgenden Optionen:

Option	Aktion
"Favorites List" (Favoritenliste)	Verwalten einer Liste bevorzugter Geräte
"Discover Devices - Local Subnet" (Geräte erkennen – Lokales Subnetz)	Erkennen von Raritan-Geräten auf dem lokalen Subnetz des Client-PC.
"Discover Devices - KX II-101-V2 Subnet" (Geräte erkennen – KX II-101-V2-Subnetz)	Erkennen der Raritan-Geräte im Subnetz des KX II-101-V2-Geräts
"Add New Device to Favorites" (Neues Gerät zu Favoriten hinzufügen)	Hinzufügen, Bearbeiten und Löschen von Geräten in der Favoritenliste

**Seite "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.

**Erkennen von Raritan-Geräten auf dem lokalen Subnetz**

Mit dieser Option werden die Geräte auf dem lokalen Subnetz erkannt. Dieses ist das Subnetz, auf dem die KX II-101-V2-Remotekonsole ausgeführt wird. Auf die Geräte können Sie direkt von dieser Seite aus zugreifen, oder Sie können sie zur Favoritenliste hinzufügen. Siehe **Seite "Favorites List"** (siehe "**Seite "Favorites List" (Favoritenliste)**" auf Seite 47) (Favoritenliste).

► **So finden Sie Geräte im lokalen Subnetz:**

1. Wählen Sie "Manage" > "Discover Devices – Local Subnet" (Verwalten > Geräte erkennen – Lokales Subnetz) aus. Die Seite "Discover Devices – Local Subnet" (Geräte erkennen – Lokales Subnetz) wird angezeigt.
2. Wählen Sie den entsprechenden Erkennungsport aus:
  - Wenn Sie den Standarderkennungs-Port verwenden möchten, aktivieren Sie das Kontrollkästchen "Use Default Port 5000" (Standard-Port 5000 verwenden).
  - Wenn Sie einen anderen Erkennungs-Port verwenden möchten, gehen Sie wie folgt vor:
    - a. Deaktivieren Sie das Kontrollkästchen "Use Default Port 5000" (Standard-Port 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" (Hinzufügen).



► **So greifen Sie auf ein erkanntes Gerät zu:**

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

**Erkennen von Raritan-Geräten auf dem KX II-101-V2-Subnetz**

Mit dieser Option werden Geräte auf dem Gerätesubnetz erkannt. Dieses ist das Subnetz der Geräte-IP-Adresse von KX II-101-V2. Auf die Geräte können Sie direkt von der Subnetzseite aus zugreifen, oder Sie können sie zur Favoritenliste hinzufügen. Siehe **Seite "Favorites List"** (siehe "**Seite "Favorites List" (Favoritenliste)**" auf Seite 47) (Favoritenliste).

Mit diesem Feature arbeiten mehrere KX II-101-V2-Geräte zusammen und werden automatisch skaliert. Die KX II-101-V2-Remotekonsole erkennt die KX II-101-V2-Geräte und alle sonstigen Raritan-Geräte im KX II-101-V2-Subnetz automatisch.

► **So finden Sie Geräte im Subnetz des Geräts:**

1. Wählen Sie **Manage > Discover Devices – KX II-101-V2 Subnet** (**Verwalten > Geräte erkennen – KX II-101-V2-Subnetz**) aus. Die Seite "**Discover Devices – KX II-101-V2 Subnet**" (**Geräte erkennen – KX II-101-V2-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**" (**Hinzufügen**).

► **So greifen Sie auf ein erkanntes Gerät zu:**

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

**Hinzufügen, Bearbeiten und Löschen der Favoriten**

► **So fügen Sie der Favoritenliste ein Gerät hinzu:**

1. Wählen Sie "**Manage**" > "**Add New Device to Favorites**" (**Verwalten > Neues Gerät zu Favoriten hinzufügen**) aus. Die Seite "**Add New Favorite**" (**Neuen Favoriten hinzufügen**) wird angezeigt.
2. Geben Sie eine aussagekräftige Beschreibung ein.
3. Geben Sie die IP-Adresse/den Hostnamen des Geräts ein.
4. Ändern Sie ggf. den Erkennungs-Port.

5. Wählen Sie die Produktart aus.
6. Klicken Sie auf "OK". Das Gerät wird Ihrer Favoritenliste hinzugefügt.

► **So bearbeiten Sie einen Favoriten:**

1. Aktivieren Sie auf der Seite "Favorites List" (Favoritenliste) das Kontrollkästchen neben dem gewünschten KX II-101-V2-Gerät.
2. Klicken Sie auf "Edit" (Bearbeiten). Die Seite "Edit" (Bearbeiten) wird angezeigt.
3. Aktualisieren Sie die Felder nach Bedarf:
  - Beschreibung
  - IP Address/Host Name (IP-Adresse/Hostname) – Geben Sie die IP-Adresse des KX II-101-V2-Geräts ein.
  - Port (falls erforderlich)
  - Product Type (Produktart)
4. Klicken Sie auf "OK".

► **So löschen Sie einen Favoriten:**

---

**Wichtig: Gehen Sie beim Löschen von Favoriten sorgfältig vor. Sie werden nicht aufgefordert, den Löschvorgang zu bestätigen.**

---

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten KX II-101-V2-Gerät.
2. Klicken Sie auf "Delete" (Löschen). Der Favorit wird aus der Favoritenliste entfernt.

**Abmelden**

► **So beenden Sie KX II-101-V2:**

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

---

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

---

---

### Multi-Platform-Client (MPC)

Der Multi-Platform-Client (MPC) von Raritan ist eine grafische Benutzeroberfläche für die Produktlinien von Raritan, mit der Sie Remotezugriff auf Zielserver erhalten, die mit KVM-über-IP-Geräten von Raritan verbunden sind. Informationen zur Verwendung des MPC finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**, das auf der Raritan-Website auf der gleichen Seite wie das Benutzerhandbuch zur Verfügung steht. Dort finden Sie Anweisungen zum Starten des MPC.

Beachten Sie, dass dieser Client von verschiedenen Raritan-Produkten verwendet wird. Deshalb können in diesem Hilfeabschnitt Verweise auf andere Produkte vorkommen.

---

### Virtual KVM Client (VKC)

Beachten Sie, dass dieser Client von verschiedenen Raritan-Produkten verwendet wird. Deshalb können in diesem Hilfeabschnitt Verweise auf andere Produkte vorkommen.

---

#### Überblick

Wenn Sie über die Remotekonsole auf einen Zielserver zugreifen, wird ein Fenster für den Virtual KVM Client (VKC) geöffnet. Es steht ein Virtual KVM Client für den Zielserver zur Verfügung, mit dem Sie verbunden sind. Auf dieses Fenster kann über die Windows®-Taskleiste zugegriffen werden.

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.*

*Hinweis: Wenn Sie Firefox 3.0.3 verwenden, kann es zu Problemen beim Starten der Anwendung kommen. Wenn dies der Fall ist, löschen Sie den Browser-Cache und starten Sie die Anwendung erneut.*

---

---






#### Verbinden mit einem KVM-Zielserver








► **So stellen Sie eine Verbindung mit einem KVM-Zielserver her:**


1. Klicken Sie in der KX II-101-V2-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.

3. Klicken Sie auf "Connect" (Verbinden). Das Fenster "Virtual KVM Client" (Virtueller KVM-Client) wird für den mit dem betreffenden Port verbundenen Zielservier geöffnet.

**Schaltflächen auf der Symbolleiste und Symbole auf der Statusleiste**

Schaltfläche	Schaltfläche name	Beschreibung
	Properties (Eigenschaften)	Öffnet das Dialogfeld "Modify Connection Properties" (Verbindungseigenschaften bearbeiten), über das Sie die Bandbreitenooptionen (z. B. Verbindungsgeschwindigkeit, Farbtiefe, Glättung usw.) manuell anpassen können.
	Video Settings (Videoeinstellungen)	Öffnet das Dialogfeld "Video Settings" (Videoeinstellungen), über das Sie die Videokonvertierungsparameter manuell anpassen können.
	Color Calibration (Farbkalibrierung)	Dient zum Anpassen der Farbeinstellungen, um überflüssiges Farbrauschen zu reduzieren. Diese Option ist identisch mit der Auswahl von "Video" > "Color Calibrate" (Video > Farbkalibrierung). <hr/> <i>Hinweis: Nicht verfügbar für KX II-101-V2.</i>
	Target Screenshot (Screenshot des Zielgeräts)	Klicken Sie auf diese Option, um einen Screenshot des Zielservers aufzunehmen und diesen in einer Datei Ihrer Wahl zu speichern.
	Audio	Öffnet ein Dialogfeld, in dem Sie aus einer Liste von Audiogeräten, die an einen Client-PC angeschlossen sind, auswählen können. Nachdem Audiogeräte mit dem Ziel verbunden wurden, können Sie die Verbindung der Geräte durch Auswahl dieser Option trennen. <hr/> <i>Hinweis: Diese Funktion ist im KX II 2.4.0 (und höher) verfügbar.</i> <i>Hinweis: Diese Funktion wird von LX nicht unterstützt. Diese Funktion wird nicht vom Modell KX II-101-V2 unterstützt.</i>

Schaltfläche	Schaltfläche name	Beschreibung
	Synchronize Mouse (Maus synchronisieren)	Zwei-Cursor-Modus erzwingt die erneute Ausrichtung des Zielsevercursors mit dem Cursor.  Hinweis: Nicht verfügbar, wenn der Mausmodus "Absolute Mouse" (Absolut) aktiviert ist.
	Refresh Screen (Anzeige aktualisieren)	Aktualisiert den Videobildschirm.
	Auto-sense Video Settings (Videoeinstellungen automatisch erkennen)	Aktualisiert die Videoeinstellungen (Auflösung, Aktualisierungsfrequenz).
	"Smart Card"	Öffnet ein Dialogfeld, in dem Sie aus einer Liste von Smart Card-Lesegeräten, die an einen Client-PC angeschlossen sind, auswählen können.  <i>Hinweis: Diese Funktion ist im KSX II 2.3.0 (und höher) und im KX II 2.1.10 (und höher) verfügbar.</i>  <i>Hinweis: Diese Funktion wird von LX nicht unterstützt. Diese Funktion wird nicht vom Modell KX II-101-V2 unterstützt.</i>
	Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)	Sendet die Tastenkombination "Strg+Alt+Entf" an den Zielsever.
	Single Cursor Mode (Ein-Cursor-Modus)	Startet den Ein-Cursor-Modus, bei dem der lokale Cursor nicht mehr auf dem Bildschirm angezeigt wird.  Drücken Sie Strg+Alt+O, um diesen Modus zu beenden.
	Vollbildmodus	Maximiert die Anzeige des Zielseverdesktops, so dass er auf dem gesamten Bildschirm angezeigt wird.

Schaltfläche	Schaltfläche name	Beschreibung
	Scaling (Skalieren)	Vergrößert oder verkleinert die Zielvideogröße, sodass Sie den gesamten Inhalt des Zielserversfensters anzeigen können, ohne die Bildlaufleiste verwenden zu müssen.

---

### Stromzufuhrsteuerung eines Zielservers

---

*Hinweis: Diese Features stehen nur zur Verfügung, wenn Sie Stromzuordnungen vorgenommen haben.*

---

► **So schalten Sie einen KVM-Zielserver aus und wieder ein:**

1. Klicken Sie in der KX II-101-V2-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 Cycle" (Aus- und Einschalten) aus. Eine Bestätigungsmeldung wird angezeigt.

► **So schalten Sie einen Zielserver ein:**

1. Klicken Sie in der KX II-101-V2-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) aus. Eine Bestätigungsmeldung wird angezeigt.

► **So schalten Sie einen Zielserver aus:**

1. Klicken Sie in der KX II-101-V2-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) aus. Eine Bestätigungsmeldung wird angezeigt.

---

### Trennen von KVM-Zielsevern

► **So trennen Sie einen Zielsever:**

- Klicken Sie auf den Portnamen des Zielgeräts, das Sie trennen möchten. Wenn das Menü "Port Action" (Portaktion) angezeigt wird, klicken Sie auf "Disconnect" (Trennen).

---

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


---

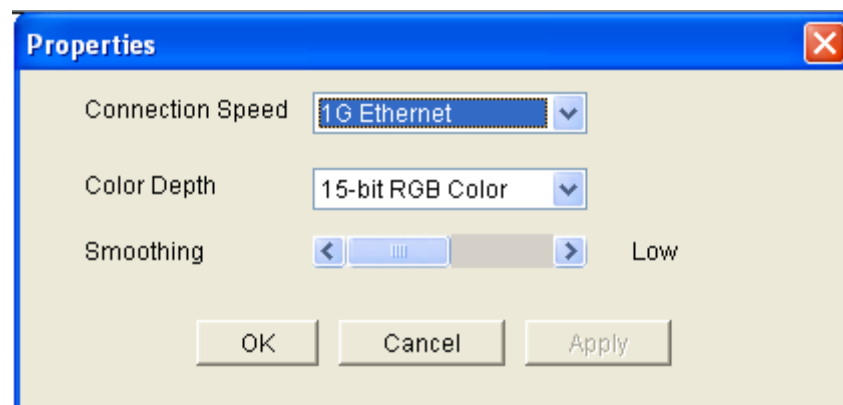
### Properties (Eigenschaften)

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

Sie können die Parameter im Dialogfeld "Properties" (Eigenschaften) Ihren Anforderungen für unterschiedliche Betriebsumgebungen anpassen. Einmal vorgenommene und gespeicherte Verbindungseigenschaften werden auch für spätere Verbindungen zu Geräten der 2. Generation gespeichert.

► **So legen Sie die Verbindungseigenschaften fest:**

1. Wählen Sie "Connection" > "Properties" (Verbindung > Eigenschaften) oder klicken Sie auf die Schaltfläche "Connection Properties" (Verbindungseigenschaften)  in der Symbolleiste. Das Dialogfeld "Properties" (Eigenschaften) wird angezeigt.



---

*Hinweis: 1G Ethernet wird vom KX II-101 nicht unterstützt.*

---

2. Wählen Sie in der Dropdownliste "Connection Speed" (Verbindungsgeschwindigkeit) die gewünschte Verbindungsgeschwindigkeit aus. Das Gerät kann die verfügbare Bandbreite automatisch erkennen und die Bandbreitenverwendung nicht beschränken. Sie können diese Verwendung jedoch auch gemäß den 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 jedoch am schnellsten, wenn die Einstellungen der tatsächlichen Umgebung entsprechen.

3. Wählen Sie in der Dropdownliste "Color Depth" (Farbtiefe) die gewünschte Farbtiefe aus. Das Gerät 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 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 Videoraussehen verringert wird.
5. Klicken Sie auf OK, um die Eigenschaften festzulegen.

---

### Verbindungsinformationen

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

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

Zur aktuellen Verbindung werden folgende Informationen angezeigt:

- Device Name (Gerätename) – Der Name des Geräts.
- IP-Address (IP-Adresse) – Die IP-Adresse des 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 Dauer der Verbindung.
- 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) – Die RFB-Protokollversion.

► **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.

---

## Tastaturoptionen

### Keyboard Macros (Tastaturmakros)

Tastaturmakros gewährleisten, dass für den Zielserver vorgesehene Tastenkombinationen an den Zielserver gesendet und nur von diesem interpretiert werden. Andernfalls werden sie von dem Computer interpretiert, auf dem der Virtual KVM Client ausgeführt wird (Client-PC).

Makros werden auf dem Client-PC gespeichert und sind PC-spezifisch. Wenn Sie einen anderen PC verwenden, können Sie daher Ihre Makros nicht sehen. Wenn eine andere Person Ihren PC verwendet und sich mit einem anderen Benutzernamen anmeldet, werden ihr die Makros angezeigt, da sie für den gesamten Computer gelten.

Im Virtual KVM Client erstellte Tastaturmakros stehen im Multi-Platform Client (MPC) zur Verfügung und umgekehrt. Tastaturmakros, die auf dem Active KVM Client (AKC) erstellt wurden, können jedoch nicht in VKC oder MPC verwendet werden. Dies trifft umgekehrt ebenfalls zu.

---

*Hinweis: AKC wird nicht von KX II-101 unterstützt.*

---

### Tastaturmakros importieren/exportieren

Makros, die von dem Active KVM Client (AKC) exportiert wurden, können nicht in einen Multi-Platform Client (MPC) oder Virtual KVM Client (VKC) importiert werden. Von MPC oder VKC exportierte Makros können nicht in AKC importiert werden.

---

*Hinweis: AKC wird nicht von KX II-101 unterstützt.*

---

#### ► So importieren Sie Makros:

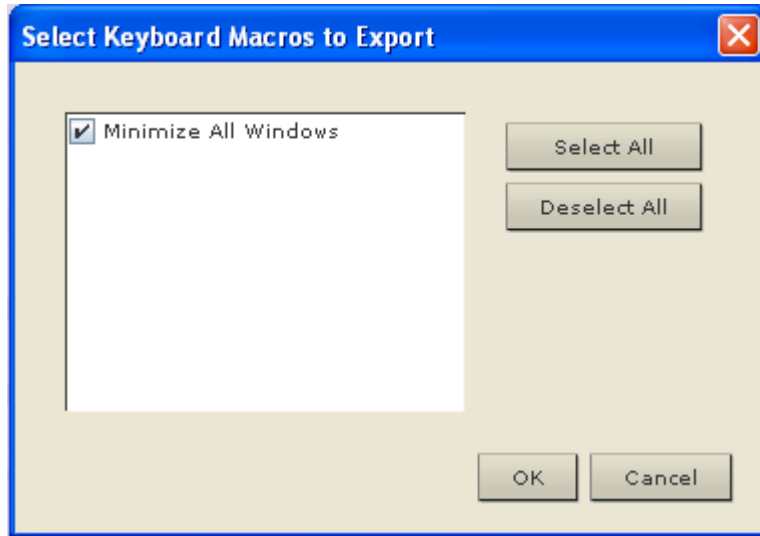
1. Zum Öffnen des Dialogfelds "Import Macros" (Makros importieren) wählen Sie "Keyboard > Import Keyboard Macros" (Tastatur > Tastaturmakros importieren). Navigieren Sie zu dem Ordner, in dem die Makrodatei abgespeichert ist.
2. Klicken Sie auf die Makrodatei und anschließend auf "Open" (Öffnen), um das Makro zu importieren.
  - a. Wenn zu viele Makros in der Datei enthalten sind, wird eine Fehlermeldung angezeigt. Wenn Sie auf "OK" klicken, wird der Import abgebrochen.
  - b. Schlägt der Import fehl, wird ein Dialogfeld "Error" (Fehler) und eine Meldung mit den Gründen für den fehlgeschlagenen Import angezeigt. Klicken Sie auf "OK" und setzen Sie den Import fort, ohne dabei jedoch die Makros zu importieren, bei denen der Import fehlgeschlagen ist.

3. Wählen Sie die zu importierenden Makros aus, indem Sie die entsprechenden Kontrollkästchen markieren, oder verwenden Sie die Option "Select All" (Alle auswählen) bzw. "Deselect All" (Alle deaktivieren).
4. Klicken Sie auf "OK", um den Import zu starten.
  - a. Wird ein doppelt vorhandenes Makro gefunden, wird das Dialogfeld "Import Macros" (Makros importieren) angezeigt. Führen Sie einen der folgenden Schritt aus:
    - Klicken Sie auf "Yes" (Ja), um das bereits vorhandene Makro mit dem importierten zu ersetzen.
    - Klicken Sie auf "Yes to All" (Ja, alle), um die jeweils ausgewählten sowie alle anderen gefundenen doppelten Makros zu ersetzen.
    - Klicken Sie auf "No" (Nein), um das ursprüngliche Makro beizubehalten, und fahren Sie dann mit dem nächsten Makro fort.
    - Klicken Sie auf "No to All" (Nein, nicht alle), um das ursprüngliche Makro beizubehalten, und fahren Sie dann mit dem nächsten Makro fort. Werden weitere doppelte Makros gefunden, werden diese bei dem Vorgang ebenfalls übergangen.
    - Klicken Sie auf "Cancel" (Abbrechen), um den Import abubrechen.
    - Sie können ebenfalls auf "Rename" (Umbenennen) klicken, um das Makro umzubenennen und es dann zu importieren. Wenn Sie "Rename" (Umbenennen) ausgewählt haben, wird das Dialogfeld "Rename Macro" (Makro umbenennen) angezeigt. Geben Sie in das Feld einen neuen Namen für das Makro ein und klicken Sie auf "OK". Das Dialogfeld wird geschlossen und der Vorgang wird fortgesetzt. Wenn es sich bei dem eingegebenen Namen um den eines doppelten Makros handelt, wird eine Warnmeldung angezeigt und Sie werden aufgefordert, einen anderen Namen für den Makro einzugeben.
  - b. Wenn während des Importprozesses die erlaubte Anzahl von importierten Makros überstiegen wird, wird ein Dialogfeld angezeigt. Klicken Sie auf "OK", wenn Sie den Importvorgang der Makros fortsetzen möchten, oder klicken Sie auf "Cancel" (Abbrechen), um den Vorgang zu beenden.

Die Makros werden dann importiert. Wenn ein Makro importiert wird, das eine bereits vorhandene Zugriffstaste enthält, wird die Zugriffstaste für das importierte Makro verworfen.

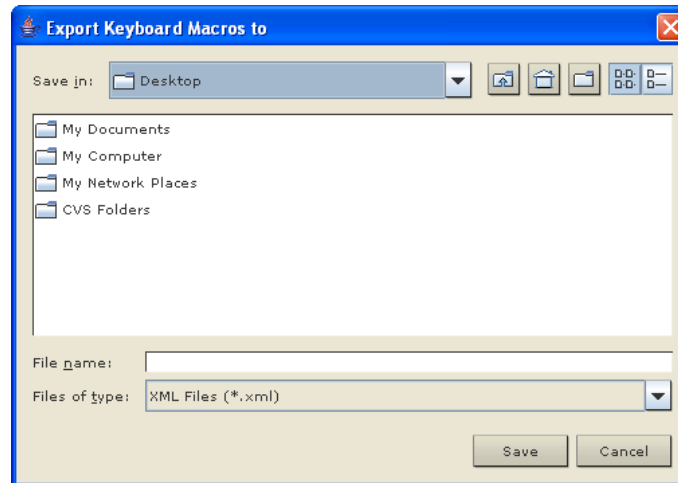
► **So exportieren Sie Makros:**

1. Um das Dialogfeld "Select Keyboard Macros to Export" (Tastaturmakros für den Export auswählen) zu öffnen, wählen Sie "Tools > Export Macros" (Extras > Makros exportieren) aus.



2. Wählen Sie die zu exportierenden Makros aus, indem Sie die entsprechenden Kontrollkästchen markieren, oder verwenden Sie die Option "Select All" (Alle auswählen) bzw. "Deselect All" (Alle deaktivieren).
3. Klicken Sie auf "OK". Das Dialogfeld "Export Keyboard Macros to" (Tastaturmakros exportieren nach) wird angezeigt. Wählen Sie die gewünschte Makrodatei aus. Das Makro ist standardmäßig auf Ihrem Desktop vorhanden.

4. Wählen Sie den Ordner aus, in dem Sie die Makrodatei abspeichern möchten, geben Sie einen Namen für die Datei ein und klicken Sie auf "Save" (Speichern). Wenn das Makro bereits vorhanden ist, wird eine Warnmeldung angezeigt. Klicken Sie auf "Yes" (Ja), um das vorhandene Makro zu überschreiben, oder auf "No" (Nein), um die Meldung zu schließen. Das Makro wird dann nicht überschrieben.



### Erstellen eines Tastaturmakros

#### ► So erstellen Sie ein Makro:

1. Klicken Sie auf "Keyboard" > "Keyboard Macros" (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Klicken Sie auf "Add" (Hinzufügen). Das Dialogfeld "Add Keyboard Macro" (Tastaturmakro hinzufügen) wird angezeigt.
3. Geben Sie im Feld "Keyboard Macro Name" (Name des Tastaturmakros) einen Namen für das Makro ein. Dieser Name wird nach der Erstellung im Tastaturmenü angezeigt.
4. Wählen Sie in der Dropdownliste im Feld "Hot-Key Combination" (Zugriffstastenkombination) eine Tastenkombination aus. Dies ermöglicht es Ihnen, das Makro mit einer vordefinierten Tastenkombination auszuführen. **///Optional**
5. Wählen Sie in der Dropdownliste "Keys to Press" (Zu betätigende Tasten) alle Tasten aus, die Sie verwenden möchten, um die Tastenkombination zu emulieren, die zum Ausführen des Befehls verwendet wird. Wählen Sie die Tasten in der Reihenfolge aus, in der sie betätigt werden sollen. Wählen Sie nach jeder gewählten Taste "Add Key" (Taste hinzufügen) aus. Nach der Auswahl jeder Taste wird diese im Feld "Macro Sequence" (Makrosequenz) angezeigt und ein Befehl zum Freigeben der Taste wird automatisch hinzugefügt.

Erstellen Sie beispielsweise ein Makro zum Schließen eines Fensters durch die Tastenkombination "Linke Strg-Taste+Esc". Dieses wird im Feld "Macro Sequenz" (Makrosequenz) wie folgt angezeigt:

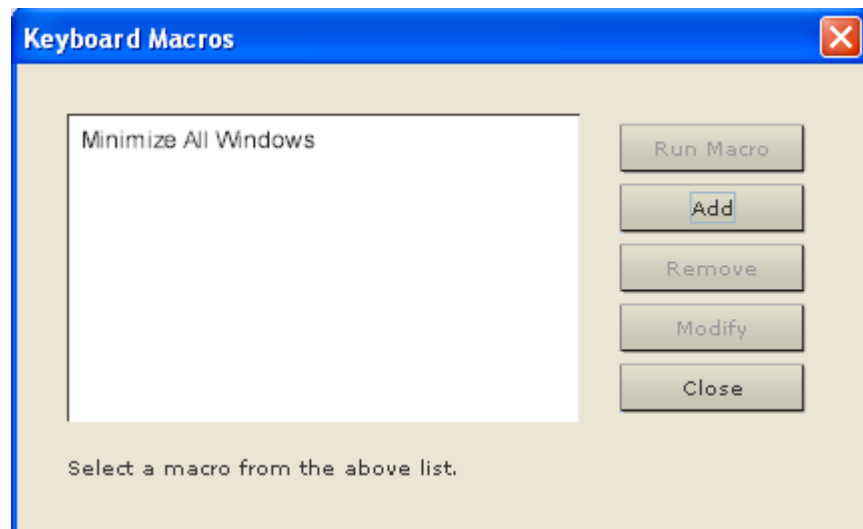
Press Left Alt (Linke Alt-Taste drücken)

Press F4 (F4 drücken)

Release F4 (F4 loslassen)

Release Left Alt (Linke Alt-Taste loslassen)

6. Überprüfen Sie das Feld "Macro Sequence" (Makrosequenz), um sicherzustellen, dass die Makrosequenz korrekt definiert wurde.
  - a. Wenn Sie einen Schritt aus der Sequenz entfernen möchten, markieren Sie diesen, und klicken Sie auf "Remove" (Entfernen).
  - b. Wenn Sie die Reihenfolge der Schritte in der Sequenz ändern möchten, klicken Sie auf den Schritt und anschließend auf die Pfeil-nach-oben- oder Pfeil-nach-unten-Taste, um die Position des Schritts wie gewünscht zu ändern.
7. Klicken Sie zum Speichern des Makros auf "OK". Klicken Sie auf "Clear" (Löschen), um alle Felder zu löschen und erneut mit der Auswahl zu beginnen. Wenn Sie auf "OK" klicken, wird das Dialogfenster "Keyboard Macros" (Tastaturmakros) mit dem neuen Tastaturmakro angezeigt.
8. Klicken Sie im Dialogfeld "Keyboard Macros" (Tastaturmakros) auf "Close" (Schließen). Das Makro wird nun im Tastaturmenü der Anwendung angezeigt. Wählen Sie das neue Makro im Menü aus, um es auszuführen, oder verwenden Sie die dem Makro zugeordnete Tastenkombination.



► **Um die Funktion "Send Text to Target" (Text an Ziel senden) für das Makro zu verwenden:**

1. Klicken Sie auf der Tastatur > "Send Text to Target" (Text an Ziel senden) Das Dialogfeld "Send Text to Target" (Text an Ziel senden) wird angezeigt.
2. Geben Sie den Text ein, der an das Zielgerät gesendet werden soll.

---

*Hinweis: Die Funktion "Send Text to Target" (Text an Ziel senden) unterstützt nur englische Zeichen.*

---

3. Wenn das Ziel ein US-amerikanisches Tastaturlayout (US-International) benutzt, aktivieren Sie das Kontrollkästchen "Target system is set to the US/International keyboard layout" (System ist auf amerikanisches Tastaturlayout (US-International) eingestellt).
4. Klicken Sie auf "OK".

#### **Ausführen eines Tastaturmakros**

Wenn Sie ein Tastaturmakro erstellt haben, können Sie es über das zugeordnete Tastaturmakro ausführen oder es aus dem Tastaturmenü auswählen.

#### **Ausführen eines Makros über die Menüleiste**

Ein erstelltes Makro wird im Menü "Keyboard" (Tastatur) angezeigt. Führen Sie das Tastaturmakro aus, indem Sie im Menü "Keyboard" (Tastatur) auf das Makro klicken.

#### **Ausführen eines Makros mithilfe einer Tastaturkombination**

Wenn Sie beim Erstellen eines Makros eine Tastenkombination zugewiesen haben, können Sie das Makro durch Drücken der entsprechenden Tasten ausführen. Drücken Sie beispielsweise gleichzeitig die Tasten Strg+Alt+0, um alle Fenster auf einem Windows-Zielsever zu minimieren.

#### **Bearbeiten und Löschen von Tastaturmakros**

► **So ändern Sie ein Makro:**

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

5. Klicken Sie auf OK.

► **So entfernen Sie ein Makro:**

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Dialogfeld "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.

Tastenkombinationen, die sich mit Blade-Chassis-Tastenfolgen überschneiden, werden nicht an die Blades in diesem Chassis gesendet.

---

## Videoeigenschaften


### Aktualisieren der Anzeige

Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms. Videoeinstellungen können auf verschiedene Art und Weise automatisch aktualisiert werden:

- Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms.
- Mit dem Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) werden die Videoeinstellungen des Zielservers automatisch erkannt.

Darüber hinaus können Sie die Einstellungen manuell über den Befehl "Video Settings" (Videoeinstellungen) anpassen.

► **Führen Sie einen der folgenden Schritte aus, um die Videoeinstellungen zu aktualisieren:**


- Wählen Sie "Video" > "Refresh Screen" (Video > Anzeige aktualisieren) aus oder klicken Sie auf die Schaltfläche "Refresh Screen"  (Anzeige aktualisieren) in der Symbolleiste.



### Auto-Sense Video Settings (Videoeinstellungen automatisch erkennen)

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


#### ▶ Führen Sie zur automatischen Erkennung der Videoeinstellungen die folgenden Schritte aus:

- Wählen Sie "Video" > "Auto-sense Video Settings" (Video > Videoeinstellungen automatisch erkennen) aus oder klicken Sie auf die Schaltfläche "Auto-Sense Video Settings"  (Videoeinstellungen automatisch erkennen) in der Symbolleiste. Eine Meldung mit der Information, dass die automatische Anpassung läuft, wird angezeigt.

### Konfigurieren von Videoeinstellungen

Verwenden Sie den Befehl "Video Settings" (Videoeinstellungen), um die Videoeinstellungen manuell anzupassen.

#### ▶ So ändern Sie die Videoeinstellungen:

1. Wählen Sie "Video" > "Video Settings" (Video > Videoeinstellungen) aus oder klicken Sie auf die Schaltfläche "Video Settings"  (Videoeinstellungen) in der Symbolleiste, um das Dialogfeld "Video Settings" (Videoeinstellungen) zu öffnen.
2. Passen Sie die folgenden Einstellungen nach Wunsch an. Wenn Sie die Einstellungen anpassen, sind die Änderungen sofort sichtbar:
  - a. Noise Filter (Rauschfilter)

Das Gerät 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 Nachbarpixeln eine starke Farbabweichung vorliegt. Eine zu hohe Einstellung des Grenzwerts kann jedoch zu einer unbeabsichtigten Filterung von gewünschten Bildschirmänderungen führen. Niedrigere Einstellungen übermitteln die meisten Pixeländerungen. Eine zu niedrige Einstellung dieses Grenzwerts kann zu einer höheren Bandbreitenverwendung führen.
  - b. PLL Settings (PLL-Einstellungen)

Clock (Uhr) – Diese Option steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobilds. Als Einstellung werden ungerade Zahlen empfohlen. Üblicherweise sollte diese Einstellung nicht geändert werden, da die automatische Erkennung meist korrekt ist.

Phase – Die Phasenwerte liegen zwischen 0 und 31 und werden zyklisch durchlaufen. Halten Sie bei dem Phasenwert an, der das beste Videobild für den aktiven Zielservern ergibt.

- c. Brightness (Helligkeit): Mithilfe dieser Einstellung passen Sie die Helligkeit der Zielserververanzeige an.
- d. Brightness Red (Helligkeit – Rot) – Steuert die Helligkeit der Anzeige des Zielservers für das rote Signal.
- e. Brightness Green (Helligkeit – Grün) – Steuert die Helligkeit des grünen Signals.
- f. Brightness Blue (Helligkeit – Blau) – Steuert die Helligkeit des blauen Signals.
- g. Contrast Red (Kontrast – Rot) – Steuert den Kontrast des roten Signals.
- h. Contrast Green (Kontrast – Grün) – Steuert das grüne Signal.
- i. 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 Zielservern ein besseres Bild angezeigt wird.

---

*Warnung: Gehen Sie beim Ändern der Einstellungen für die Uhr und die Phase sorgfältig vor. Änderungen können zu Verzerrungen oder sogar zum Verlust des Videobildes führen, und Sie können möglicherweise die vorherigen Einstellungen nicht wiederherstellen. Wenden Sie sich an den technischen Kundendienst von Raritan, bevor Sie Änderungen vornehmen.*

---

- j. Horizontal Offset (Horizontaloffset) – Steuert die horizontale Positionierung der Zielserververanzeige auf dem Bildschirm.
  - k. Vertical Offset (Vertikaloffset) – Steuert die vertikale Positionierung der Zielserververanzeige auf dem Bildschirm.
3. Wählen Sie "Automatic Color Calibration" (Automatische Farbkalibrierung) aus, um diese Funktion zu aktivieren.
  4. Wählen Sie den Videoerkennungsmodus aus:

- Best possible video mode (Bestmöglicher Videomodus)

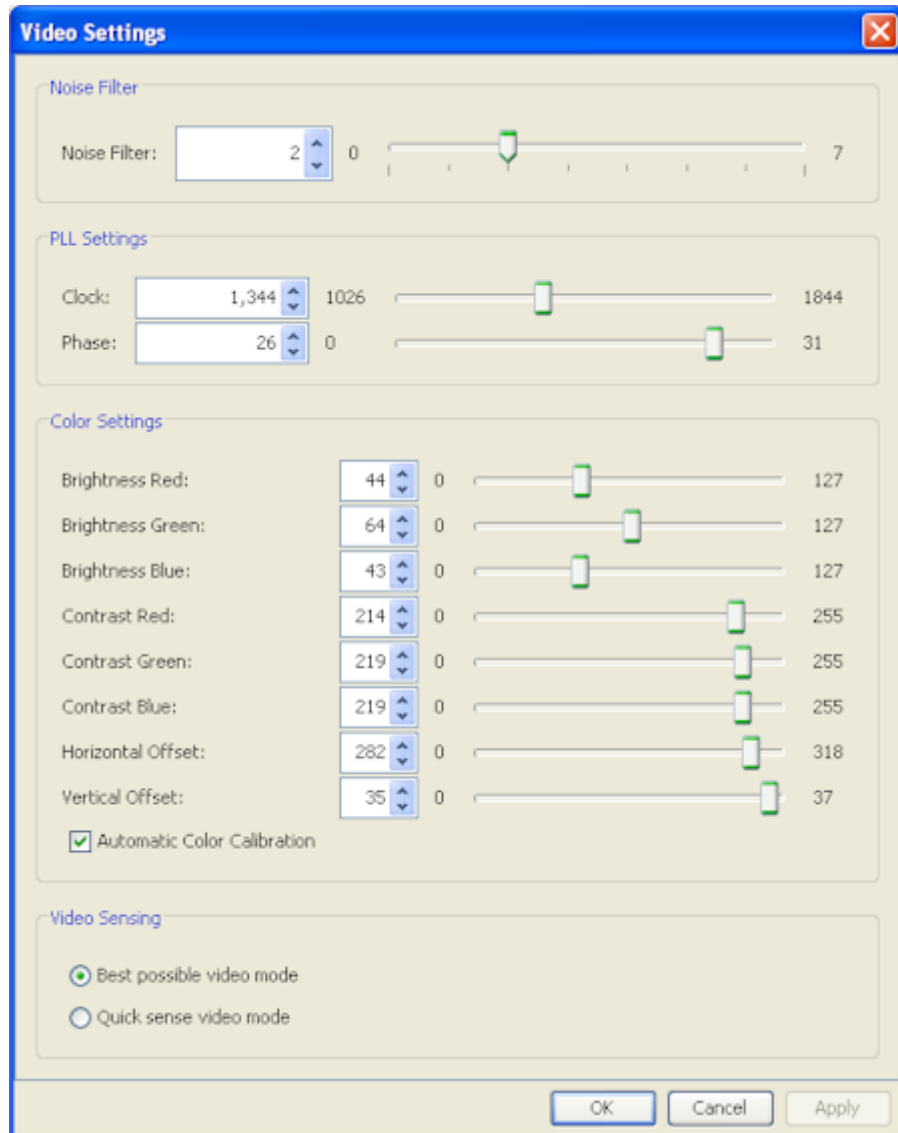
Beim Wechseln von Zielgeräten oder Zielauflösungen führt das Gerät die vollständige automatische Erkennung durch. Bei dieser Option wird das Videobild so kalibriert, dass die bestmögliche Bildqualität erzielt wird.

- Quick sense video mode (Videomodus schnell erkennen)

Bei dieser Option führt das Gerät eine schnelle automatische Erkennung des Videomodus durch, um das Bild des Zielgeräts schneller anzuzeigen. Diese Option eignet sich insbesondere für die Eingabe der BIOS-Konfiguration eines Zielservers nach einem Neustart.

5. Klicken Sie auf OK, um die Einstellungen zu übernehmen, und schließen Sie das Dialogfenster. Klicken Sie auf "Apply" (Übernehmen), um die Einstellungen zu übernehmen, ohne das Dialogfenster zu schließen.


*Hinweis: Einige Sun-Hintergrundanzeigen (z. B. Anzeigen mit sehr dunklen Rändern) werden auf bestimmten Sun-Servern nicht exakt zentriert abgebildet. Verwenden Sie einen anderen Hintergrund, oder platzieren Sie auf der Anzeige oben links ein helleres Symbol.*

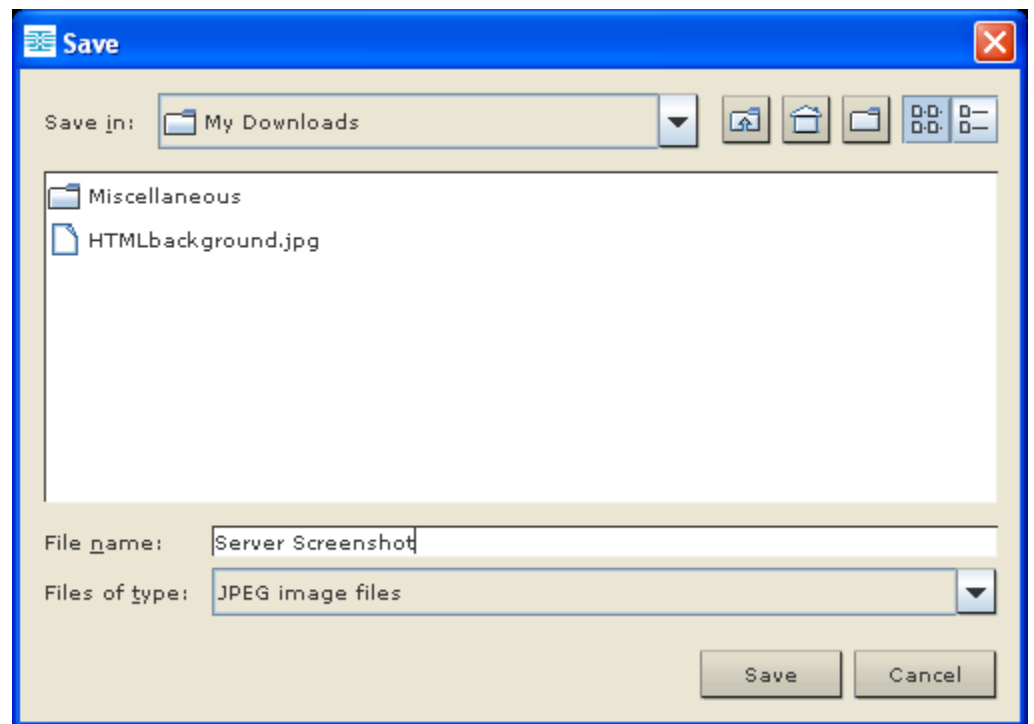


### Verwenden der Funktion "Screenshot from Target" (Screenshot vom Zielgerät)

Mit dem Befehl "Screenshot from Target" (Screenshot vom Zielgerät) können Sie einen Screenshot vom Zielsever aufnehmen. Speichern Sie diesen Screenshot ggf. an einem Speicherort Ihrer Wahl als Bitmap-, JPEG- oder PNG-Datei ab.

#### ► So nehmen Sie einen Screenshot vom Zielsever auf:

1. Wählen Sie "Video" > "Screenshot from Target" (Video > Screenshot vom Zielgerät) aus oder klicken Sie auf die Schaltfläche "Screenshot from Target"  (Screenshot vom Zielgerät) in der Symbolleiste.
2. Wählen Sie im Dialogfenster "Save" (Speichern) den Speicherort für die Datei aus, benennen Sie sie und wählen Sie ein Dateiformat aus der Dropdownliste "Files of Type" (Dateitypen) aus.
3. Klicken Sie zum Speichern des Screenshots auf "Save" (Speichern).



### Ändern der höchsten Aktualisierungsrate

Wenn die von Ihnen verwendete Videokarte kundenspezifische Software verwendet und Sie über MPC oder VKC auf das Ziel zugreifen, kann es erforderlich sein, die maximale Aktualisierungsrate des Monitors zu ändern, damit die Aktualisierungsrate für das Ziel wirksam wird.

#### ► So stellen Sie die Aktualisierungsrate des Monitors ein:

1. Wählen Sie unter Windows® "Eigenschaften von Anzeige" > "Einstellungen" > "Erweitert" aus, um das Dialogfeld "Eigenschaften von Plug-and-Play-Monitor" zu öffnen.
2. Klicken Sie auf die Registerkarte "Monitor".
3. Legen Sie die "Screen Refresh Rate" (Bildschirmaktualisierungsrate) fest.
4. Klicken Sie auf "OK" und anschließend erneut auf "OK", um die Einstellungen zu übernehmen.

---

### Mausoptionen

Bei der Steuerung eines Zielservers zeigt die Remotekonsole zwei Cursor an: Ein Cursor gehört zur Client-Workstation und der andere zum Zielservers.

Sie können entweder im Ein-Cursor-Modus oder im Zwei-Cursor-Modus arbeiten. Wenn Sie sich im Zwei-Cursor-Modus befinden und die Option ordnungsgemäß konfiguriert wurde, werden die Cursor aneinander ausgerichtet.

Bei zwei Cursors bietet das Gerät verschiedene Mausmodi:

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


### Mauszeigersynchronisation

Bei der Remoteanzeige eines Zielservers mit einer Maus werden zwei Cursor angezeigt: Ein Mauszeiger gehört zur Remote-Client-Workstation 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 Client-Mauszeigers etwas schneller als die des Zielgerätmauszeigers.

Bei schnellen LAN-Verbindungen können 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.

Tipps zur Maussynchronisation

Führen Sie bei der Konfiguration der Maussynchronisierung folgende Schritte aus:

1. Stellen Sie sicher, dass die ausgewählte Videoauflösung und die Aktualisierungsfrequenz vom Gerät unterstützt werden. Im Dialogfeld "Virtual KVM Client Connection Info" (Virtual KVM Client – Verbindungsinformationen) werden die tatsächlich vom Gerät erkannten Werte angezeigt.
2. Stellen Sie sicher, dass die Kabellänge bei KX II- und LX-Geräten die Grenzwerte für die ausgewählte Videoauflösung nicht überschreitet.
3. Stellen Sie sicher, dass Maus und Monitor während der Installation richtig konfiguriert wurden.
4. Führen Sie eine automatische Erkennung durch, indem Sie im Virtual KVM Client auf die Schaltfläche "Auto-sense Video" (Video automatisch erkennen) klicken.
5. Führen Sie folgende Schritte aus, falls dadurch die Maussynchronisation (bei Linux-, UNIX- und Solaris-KVM-Zielservern) nicht verbessert wird:
  - a. Öffnen Sie ein Terminalfenster.
  - b. Geben Sie folgenden Befehl ein: `xset mouse 1 1`
  - c. Schließen Sie das Terminalfenster.
6. Klicken Sie im Virtual KVM Client auf die Schaltfläche zur Maussynchronisierung .

**Weitere Hinweise zum Mausmodus "Intelligent"**


- Stellen Sie sicher, dass sich links oben auf dem Bildschirm keine Symbole oder Anwendungen befinden, da in diesem Bereich die Synchronisierungsroutine ausgeführt wird.
- Verwenden Sie keinen animierten Cursor.
- Deaktivieren Sie den Active Desktop auf KVM-Zielsevern.

Synchronize Mouse (Maus synchronisieren)

Im Zwei-Cursor-Modus erzwingt der Befehl "Synchronize Mouse" (Maus synchronisieren) die erneute Ausrichtung des Zielsever-Mauszeigers am Mauszeiger des Virtual KVM Client.

► **Führen Sie einen der folgenden Schritte aus, um die Maus zu synchronisieren:**

- Wählen Sie "Mouse" > "Synchronize Mouse" (Maus > Maus synchronisieren) aus oder klicken Sie auf die Schaltfläche

"Synchronize Mouse"  (Maus synchronisieren) in der Symbolleiste.

---

*Hinweis: Diese Option steht nur in den Mausmodi "Standard" und "Intelligent" zur Verfügung.*

---

**Mausmodus "Standard"**

Beim Mausmodus "Standard" wird ein Standard-Maussynchronisierungsalgorithmus mit relativen Mauspositionen verwendet. Für den Mausmodus "Standard" müssen die Mausbeschleunigung deaktiviert und andere Mausparameter korrekt eingerichtet werden, damit die Client- und die Servermaus synchron bleiben.

► **So gelangen Sie in den Mausmodus "Standard":**

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



### **Intelligenter Mausmodus**

Im Mausmodus "Intelligent" erkennt das Gerät die Mauseinstellungen des Zielgeräts und kann die Cursor dementsprechend synchronisieren, wodurch die Mausbeschleunigung auf dem Zielgerät ermöglicht wird. Intelligenter Mausmodus wird standardmäßig für nicht-VM-Ziele verwendet.

Bei der Synchronisierung "tanzt" der Cursor in der oberen linken Ecke des Bildschirms und berechnet die Beschleunigung. Damit dieser Modus richtig funktioniert, müssen bestimmte Bedingungen erfüllt sein.

#### ► **So gelangen Sie in den intelligenten Mausmodus:**

- Wählen Sie "Mouse > Intelligent" (Maus > Intelligent).

#### **Bedingungen für die intelligente Maussynchronisation**

Der Befehl "Intelligent Mouse Synchronization" (Intelligente Maussynchronisierung) im Menü "Mouse" (Maus) synchronisiert automatisch die Cursor in Inaktivitätsphasen. Zur korrekten Synchronisierung müssen jedoch folgende Bedingungen erfüllt sein:

- Der Active Desktop muss auf dem Zielgerät deaktiviert sein.
- Oben in der linken Ecke auf der Zielseite dürfen keine Fenster angezeigt werden.
- Oben in der linken Ecke auf der Zielseite darf kein animierter Hintergrund vorhanden sein.
- Der Zielcursor muss standardmäßig und nicht animiert sein.
- Die Geschwindigkeit des Zielcursors darf nicht auf sehr hohe oder sehr niedrige Werte eingestellt sein.
- Erweiterte Mauseigenschaften wie "Enhanced pointer precision" (Zeigerbeschleunigung verbessern) oder "Snap mouse to default button in dialogs" (In Dialogfeldern automatisch zur Standardschaltfläche springen) müssen deaktiviert sein.
- Wählen Sie im Fenster "Video Settings" (Videoeinstellungen) die Option "Best Possible Video Mode" (Bestmöglicher Videomodus) aus.
- Die Ränder des Zielvideos müssen deutlich sichtbar sein. Ein schwarzer Rand muss also bei einem Bildlauf zu einem Rand des Zielvideobilds zwischen dem Zieldesktop und dem Fenster der KVM-Remotekonsole sichtbar sein.
- Wenn Sie die Funktion zur intelligenten Maussynchronisierung nutzen, können Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu Problemen führen. Um Probleme mit dieser Funktion zu vermeiden, empfiehlt Raritan, Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu entfernen.

Initiiieren Sie nach dem automatischen Erkennen des Zielvideos manuell eine Maussynchronisierung. Klicken Sie dazu in der Symbolleiste auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren). Dies gilt auch bei Änderung der Auflösung des Zielgeräts, wenn die Cursor nicht mehr synchronisiert sind.

Schlägt die intelligente Maussynchronisierung fehl, wird die Standardeinstellung der Maussynchronisierung wiederhergestellt.

Beachten Sie, dass die Mauskonfigurationen auf unterschiedlichen Zielbetriebssystemen variieren. Weitere Informationen finden Sie in den Richtlinien für Ihr Betriebssystem. Die intelligente Maussynchronisierung ist für UNIX-Zielgeräte nicht verfügbar.

### **Mausmodus "Absolut"**

In diesem Modus werden absolute Koordinaten verwendet, um die Cursor von Client und Zielgerät synchron zu halten, auch wenn für die Maus des Zielgeräts eine andere Beschleunigung oder Geschwindigkeit eingestellt wurde. Dieser Modus wird von Servern mit USB-Ports unterstützt und ist der Standardmodus für VM- und duale VM-Ziele.

#### ► So gelangen Sie in den Mausmodus „Absolute“ (Absolut):

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

---

*Hinweis: Die absolute Mauseinstellung erfordert ein USB-Zielsystem und wird als Mauseinstellung für den KX II-101 empfohlen.*

*Hinweis: Der Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) steht für KX II-Geräte nur für USB-CIMs (D2CIM-VUSB und D2CIM-DVUSB) mit Aktivierung der virtuellen Medien zur Verfügung.*

---

### **VKC Virtual Media (Virtuelle Medien)**

Umfassende Informationen zum Einrichten und Verwenden virtueller Medien finden Sie im Kapitel **Virtuelle Medien** (auf Seite 81).

---

### **Optionen im Menü "Tools" (Extras)**

#### **"General Settings" (Allgemeine Einstellungen)**

#### ► So legen Sie die Optionen im Menü "Tools" (Extras) fest:

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Enable Logging" (Protokollierung aktivieren) nur nach Anweisung durch den technischen Kundendienst. Bei dieser Option wird im Basisverzeichnis eine Protokolldatei erstellt.

3. Wählen Sie ggf. in der Dropdown-Liste "Keyboard Type" (Tastaturtyp) einen Tastaturtyp aus. Folgende Optionen stehen zur Verfügung:

- US/International (USA/International)
- French (France) (Französisch)
- German (Germany) (Deutsch)
- Japanese (Japanisch)
- United Kingdom (Großbritannien)
- Korean (Korea) (Koreanisch)
- French (Belgium) (Französisch, Belgien)
- Norwegian (Norway) (Norwegisch)
- Portugiesisch (Portugal)
- Danish (Denmark) (Dänisch)
- Swedish (Sweden) (Schwedisch)
- German (Deutsch, Schweiz)
- Hungarian (Hungary) (Ungarisch)
- Spanish (Spain) (Spanisch)
- Italian (Italy) (Italienisch)
- Slovenian (Slowenisch)
- Übersetzung: Französisch – Englisch (USA)
- Übersetzung: Französisch – Englisch (USA/International)

Beim AKC entspricht der Tastaturtyp standardmäßig dem lokalen Client. In diesem Fall trifft die Option nicht zu. Darüber hinaus unterstützen die Modelle KX II-101 und KX II-101-V2 den Ein-Cursor-Modus nicht. Daher ist die Funktion "Exit Single Cursor Mode" (Ein-Cursor-Modus beenden) für diese Geräte nicht verfügbar.

4. Konfigurieren von Zugriffstasten:

- "Exit Full Screen Mode - Hotkey" (Zugriffstaste zum Beenden des Vollbildmodus). Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver. Diese Zugriffstaste wird zum Beenden des Modus verwendet.
- "Exit Single Cursor Mode - Hotkey" (Zugriffstaste zum Beenden des Ein-Cursor-Modus). Im Ein-Cursor-Modus wird nur der Cursor des Zielservers angezeigt. Diese Zugriffstaste wird zum Beenden des Ein-Cursor-Modus verwendet, sodass der Client-Cursor wieder angezeigt wird.

- "Disconnect from Target - Hotkey" (Zugriffstaste zum Trennen der Verbindung mit dem Ziel): Aktivieren Sie diese Zugriffstaste, damit Benutzer die Verbindung mit dem Ziel unverzüglich trennen können.

Bei der Kombination mehrerer Zugriffstasten kann eine Tastenkombination jeweils nur einer Funktion zugewiesen werden. Wenn die Taste "Q" beispielsweise bereits der Funktion "Disconnect from Target" (Verbindung mit dem Ziel trennen) zugewiesen ist, ist sie für die Funktion "Exit Full Screen Mode" (Vollbildmodus beenden) nicht mehr verfügbar. Wenn eine Zugriffstaste bei einer Aktualisierung hinzugefügt wird und der Standardwert für die Taste bereits verwendet wird, wird der Funktion stattdessen der nächste verfügbare Wert zugewiesen.

5. Klicken Sie auf "OK".

**Tastaturbeschränkungen**

**Türkische Tastaturen**

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

**Slowenische Tastaturen**

Aufgrund einer JRE-Beschränkung funktioniert die Taste < auf slowenischen Tastaturen nicht.

**Sprachkonfiguration für Linux**

Da mit der Sun-JRE auf einem Linux-Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenergebnissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Sprache	Konfigurationsmethode
USA/Int.	Standard
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch (Deutschland)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Japanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Sprache	Konfigurationsmethode
Belgisch	Keyboard Indicator (Tastaturanzeige)
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

---

*Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.*

---

#### **Client Launch Settings (Client-Starteinstellungen)**

Mithilfe des Konfigurierens von "Client Launch Settings" (Client-Starteinstellungen) können Sie die Bildeinstellungen für eine KVM-Sitzung definieren.

---

*Hinweis: LX-Geräte unterstützen diese Funktion im MPC. Keine Unterstützung der Client-Starteinstellung im VKC und AKC durch LX.*

---

#### **► So konfigurieren Sie Starteinstellungen für den Client:**

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Klicken Sie auf die Registerkarte "Client Launch Settings" (Client-Starteinstellungen).
  - So konfigurieren Sie die Zielfenstereinstellungen:
    - a. Wählen Sie "Standard - sized to target Resolution" (Standard - Größe an Zielauflösung anpassen) aus, um das Fenster mit der aktuellen Auflösung des Ziels zu öffnen. Wenn die Zielauflösung größer als die Client-Auflösung ist, bedeckt das Zielfenster soviel Bildschirmfläche wie möglich. Gegebenenfalls werden Bildlaufleisten hinzugefügt.

- b. Wählen Sie "Full Screen" (Vollbild) aus, um das Zielfenster im Vollbildmodus zu öffnen.
    - So konfigurieren Sie den Monitor, auf dem der Ziel-Viewer gestartet wird:
      - a. Wählen Sie "Monitor Client Was Launched from" (Monitor-Client gestartet von) aus, wenn der Ziel-Viewer in derselben Anzeige wie die auf dem Client verwendete Anwendung gestartet werden soll (z. B. ein Webbrowser oder ein Applet).
      - b. Wählen Sie "Select From Detected Monitors" (Aus gefundenen Monitoren auswählen) aus, um einen Monitor aus einer Liste mit Monitoren auszuwählen, die von der Anwendung gefunden wurden. Wenn ein zuvor ausgewählter Monitor nicht mehr gefunden wird, wird "Currently Selected Monitor Not Detected" (Aktuell ausgewählter Monitor nicht gefunden) angezeigt.
        - So konfigurieren Sie zusätzliche Starteinstellungen:
          - a. Wählen Sie "Enable Single Cursor Mode" (Ein-Cursor-Modus aktivieren), um den Ein-Cursor-Modus bei Zugriff auf den Server als Standardmausmodus zu aktivieren.
          - b. Wählen Sie "Enable Scale Video" ("Video skalieren" aktivieren) aus, damit die Anzeige auf dem Zielsever automatisch skaliert wird, sobald auf ihn zugegriffen wird.
          - c. Wählen Sie "Pin Menu Toolbar" (Menüsymbolleiste anheften), wenn die Symbolleiste auf dem Ziel im Vollbildmodus sichtbar bleiben soll. Wenn sich das Ziel im Vollbildmodus befindet, ist das Menü in der Standardeinstellung nur sichtbar, wenn Sie mit der Maus auf den oberen Bildschirmrand zeigen.
3. Klicken Sie auf "OK".

### Konfigurieren von Scaneinstellungen über VKC und AKC

KX II- und LX-Geräte bieten eine Port-Scanfunktion, mit der nach ausgewählten Zielen gesucht werden kann. Die Ziele werden dann in einer Bildschirmpräsentationsansicht angezeigt. So können Sie bis zu 32 Ziele gleichzeitig überwachen. Sie können je nach Bedarf eine Verbindung mit mehreren Zielen herstellen oder sich auf ein bestimmtes Ziel konzentrieren. Scanvorgänge können Standardziele, Blade-Server, Dominion-Schichtgeräte und KVM-Switch-Ports umfassen. Konfigurieren Sie die Scaneinstellungen entweder über den Virtual KVM Client (VKC) oder den Active KVM Client (AKC). Weitere Informationen finden Sie unter Konfigurieren von Scaneinstellungen über VKC und AKC. Siehe Scannen von Ports. Das Scanintervall und die Standardanzeigeeoptionen legen Sie auf der Registerkarte "Scan Settings" (Scaneinstellungen) fest.

#### ► So legen Sie die Scaneinstellungen fest:

1. Wählen Sie "Tools" (Extras) > "Options" (Optionen). Das Dialogfeld "Options" (Optionen) wird angezeigt.

2. Wählen Sie die Registerkarte "Scan Settings" (Scaneinstellungen) aus.
3. Geben Sie im Feld "Display Interval (10-255 sec):" (Anzeigeintervall (10-255 Sek.)) die Anzahl Sekunden ein, die das Ziel im Fokus in der Mitte des Fensters "Port Scan" (Port-Scan) angezeigt werden soll.
4. Geben Sie im Feld "Interval Between Ports (10 - 255 sec):" (Intervall zwischen Ports (10-255 Sek.)) das Intervall ein, in dem das Gerät zwischen Ports pausieren soll.
5. Ändern Sie im Abschnitt "Display" (Anzeige) die Standardanzeigeoptionen für die Größe der Miniaturansichten und die Teilung der Ausrichtung des Fensters "Port Scan" (Port-Scan).
6. Klicken Sie auf "OK".

---

## Ansichtsoptionen

### View Toolbar (Symbolleiste anzeigen)

Sie können den Virtual KVM Client mit oder ohne die Symbolleiste verwenden.

► **So blenden Sie die Symbolleiste ein bzw. aus:**

- Wählen Sie **View > View Toolbar** (Ansicht > Symbolleiste anzeigen).

### "View Status Bar" (Statusleiste anzeigen)

Standardmäßig wird die Statusleiste unten im Zielfenster angezeigt.

► **So blenden Sie die Statusleiste aus:**

- Klicken Sie auf "View" (Ansicht) > "Status Bar" (Statusleiste), um die Option zu deaktivieren.

► **So stellen Sie die Statusleiste wieder her:**

- Klicken Sie auf "View" (Ansicht) > "Status Bar" (Statusleiste), um die Option zu aktivieren.

### Scaling (Skalieren)

Das Skalieren des Zielfensters ermöglicht die Anzeige des gesamten Inhalts des Zielserversfensters. 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).

### Vollbildmodus

Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver. Die Zugriffstaste, über die Sie diesen Modus beenden können, legen Sie im Dialogfeld "Options" (Optionen) fest (siehe "**Tool Options**" (**Tool-Optionen**)) (siehe "**Optionen im Menü 'Tools' (Extras)**" auf Seite 73)).

Wenn Sie im Vollbildmodus den Mauszeiger an den oberen Bildschirmrand schieben, wird die Menüleiste für den Vollbildschirmmodus angezeigt. Wenn die Menüleiste im Vollbildmodus sichtbar bleiben soll, aktivieren Sie die Option "Pin Menu Toolbar" (Menüsymbolleiste anheften) im Dialogfeld "Tool Options" (Tool-Optionen). Siehe "**Tool Options**" (**Tool-Optionen**) (siehe "**Optionen im Menü 'Tools' (Extras)**" auf Seite 73)).

#### ► So gelangen Sie in den Vollbildmodus:

- Wählen Sie "View" > "Full Screen" (Ansicht > Vollbild) aus.

#### ► So beenden Sie den Vollbildmodus:

- Drücken Sie die im Dialogfeld "Options" (Optionen) konfigurierte Zugriffstaste. Standardmäßig lautet die Tastenkombination "Strg+Alt+M".

Wenn Sie immer im Vollbildmodus auf das Ziel zugreifen möchten, können Sie den Vollbildmodus als Standardeinstellung auswählen.

#### ► So aktivieren Sie den Vollbildmodus als Standardmodus:

1. Klicken Sie auf "Tools" (Extras) > "Options" (Optionen), um das Dialogfeld "Options" (Optionen) zu öffnen.
2. Wählen Sie "Enable Launch in Full Screen Mode" (Start im Vollbildmodus aktivieren), und klicken Sie auf "OK".



---

### Hilfeoptionen

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

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

► **So rufen Sie die Versionsinformationen ab:**

1. Wählen Sie "Help" > "About Raritan Virtual KVM Client" (Hilfe > Informationen zum Raritan Virtual KVM Client) aus.
2. Verwenden Sie die Schaltfläche "Copy to Clipboard" (In Zwischenablage kopieren), um die im Dialogfeld enthaltenen Informationen in eine Zwischenablagedatei zu kopieren, sodass auf diese bei Bedarf später bei Hilfestellung durch den Kundendienst zugegriffen werden kann.

## Kapitel 4 Virtuelle Medien

### In diesem Kapitel

Überblick.....	82
Verwenden virtueller Medien .....	89
Herstellen einer Verbindung mit virtuellen Medien.....	90
Trennen von virtuellen Medien .....	92

---

## Überblick

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

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

- Übertragen von Dateien
- Durchführen von Diagnosen
- Installieren oder Reparieren von Anwendungen
- Vollständiges Installieren des Betriebssystems (falls dies vom BIOS unterstützt wird)
- Diese erweiterte KVM-Steuerung macht die meisten Gänge in das Rechenzentrum überflüssig und spart dadurch Zeit und Geld.

Für Windows®, Mac®- und Linux™-Clients werden die folgenden virtuellen Medientypen unterstützt:

- Interne und per USB angeschlossene CD- und DVD-Laufwerke
- USB-Massenspeichergeräte
- PC-Festplatte
- ISO-Abbilder (Datenträgerabbilder)
- Digitale Audiogeräte\*

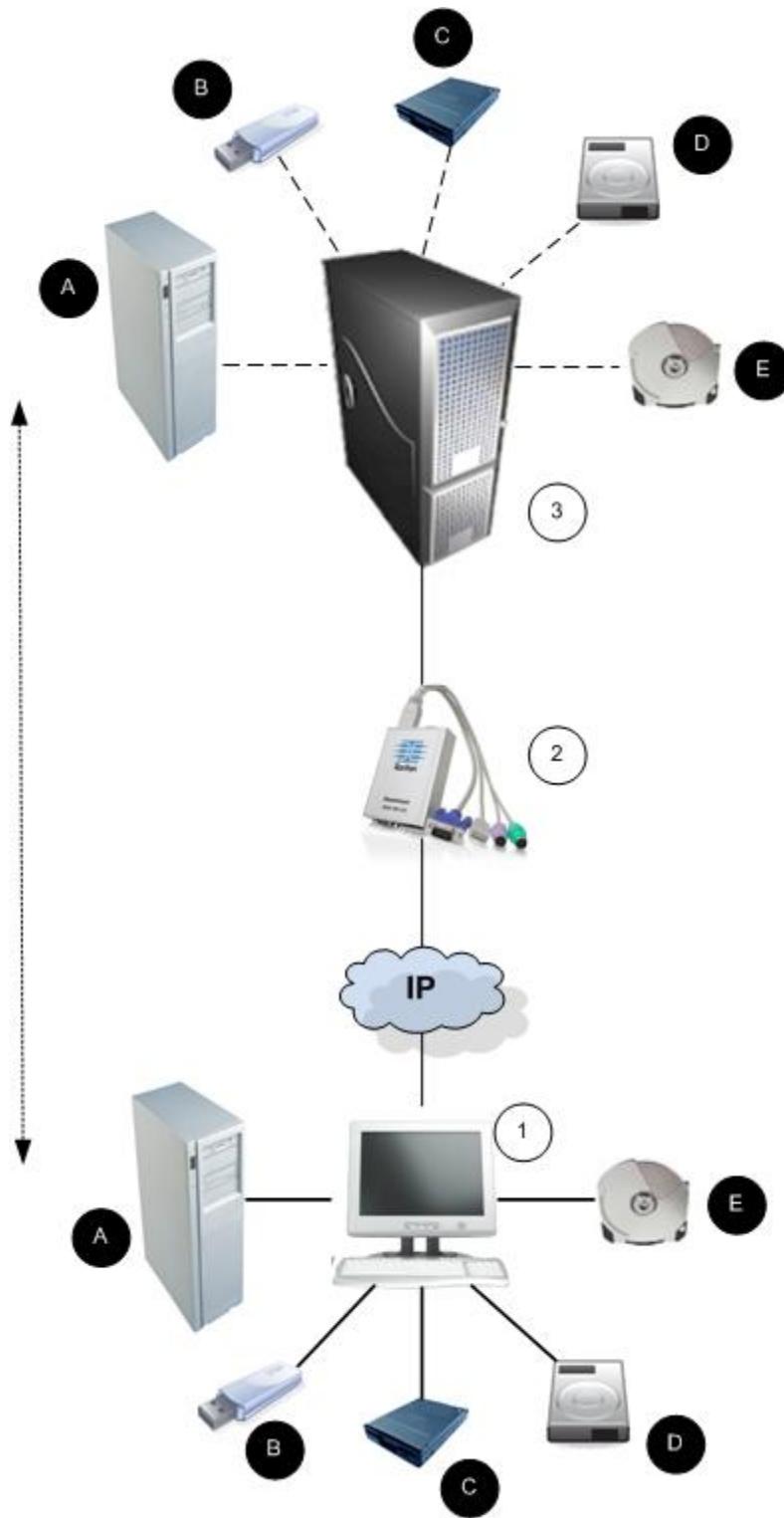
---

*Hinweis: ISO9660 wird standardmäßig von Raritan unterstützt. Andere ISO-Standards können jedoch ebenfalls verwendet werden.*

---

Die folgenden Client-Betriebssysteme werden unterstützt:

- Windows
- Mac OS X 10.5, 10.6 und 10.7
- Red Hat Desktop 4.0 und 5.0
- Open SUSE 10, 11
- Fedora 13 und 14



---

*Hinweis: Wenn Sie virtuelle Medien verwenden, müssen Sie die USB-Verbindung nutzen.*

---

### **Voraussetzungen für die Verwendung virtueller Medien**

Mit dem Feature für virtuelle Medien können Sie bis zu zwei Laufwerke (verschiedenen Typs) installieren, die durch das aktuell dem Zielgerät zugeordnete USB-Profil unterstützt werden. Diese Laufwerke sind während der KVM-Sitzung zugänglich.

Sie können beispielsweise eine bestimmte CD-ROM installieren, verwenden und nach Fertigstellung Ihrer Arbeit wieder trennen. Der virtuelle Medienkanal für CD-ROMs bleibt jedoch offen, sodass Sie eine andere CD-ROM virtuell installieren können. Diese virtuellen Medienkanäle bleiben offen, bis die KVM-Sitzung geschlossen wird (vorausgesetzt, sie werden vom USB-Profil unterstützt).

Um das virtuelle Medium zu verwenden, schließen Sie es an den Client-PC oder Netzwerkdateiserver an, auf den Sie über den Zielserver zugreifen möchten. Dieser Schritt muss nicht als erster erfolgen, jedoch bevor Sie versuchen, auf das Medium zuzugreifen.

Für die Verwendung virtueller Medien müssen folgende Bedingungen erfüllt sein:

#### Dominion-Gerät

- Für Benutzer, die Zugriff auf virtuelle Medien benötigen, müssen die Geräteberechtigungen für den Zugriff auf die relevanten Ports sowie der virtuelle Medienzugriff (Portberechtigung VM Access [VM-Zugriff]) für diese Ports eingerichtet werden. Portberechtigungen werden auf Gruppenebene eingerichtet.
- Zwischen dem Gerät und dem Zielserver muss eine USB-Verbindung bestehen.
- Wenn Sie die PC-Freigabe verwenden möchten, müssen die Security Settings (Sicherheitseinstellungen) auf der Seite "Security Settings" (Sicherheitseinstellungen) aktiviert sein. **Optional**
- Sie müssen das richtige USB-Profil für den KVM-Zielserver auswählen, zu dem Sie eine Verbindung herstellen.

#### Client-PC

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

---

*Hinweis: Wenn Sie Windows Vista or Windows 7 verwenden, deaktivieren Sie "User Account Control" (Benutzerkontensteuerung), oder wählen Sie beim Start von Internet Explorer "Run as Administrator" (Als Administrator ausführen) aus. Klicken Sie dazu auf das Menü "Start", klicken Sie mit der rechten Maustaste auf "Internet Explorer", und wählen Sie "Run as Administrator" (Als Administrator ausführen) aus.*

---

Zielserver

- KVM-Zielserver müssen über USB angeschlossene Laufwerke unterstützen.
- Auf KVM-Zielservern mit Windows 2000 müssen alle aktuellen Patches installiert sein.
- USB 2.0-Ports sind schneller und daher vorzuziehen.

---

**Virtuelle Medien in einer Windows XP-Umgebung**

Wenn Sie den Virtual KVM Client oder Active KVM Client in einer Windows® XP-Umgebung ausführen, Benutzer müssen über Administratorrechte verfügen, um auf andere Medientypen als CD-ROM-Verbindungen, ISO-Dateien und ISO-Abbilder zugreifen zu können.

---

## Virtuelle Medien in einer Linux-Umgebung

Die folgenden Informationen zur Verwendung von virtuellen Medien sind für Linux®-Benutzer relevant.

### Erforderliche Stammbenutzerberechtigung

Ihre virtuelle Medienverbindung wird ggf. beendet, wenn Sie ein CD-ROM-Laufwerk von einem Linux-Client auf einem Ziel bereitstellen und anschließend die Bereitstellung des CD-ROM-Laufwerks aufheben. Die Verbindung wird auch beendet, wenn ein Diskettenlaufwerk bereitgestellt wurde und dann eine Diskette entnommen wird. Um diese Probleme zu vermeiden, melden Sie sich als Stammbenutzer an.

### Berechtigungen

Zum Verbinden des Laufwerks bzw. der CD-ROM mit dem Ziel müssen Benutzer über die entsprechenden Zugriffsberechtigungen verfügen. Dies kann mit folgenden Befehlen geprüft werden:

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0
brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

Im obigen Beispiel muss die Berechtigung geändert werden und Lesezugriff gewährt werden.

In einem System, das Zugriffssteuerungslisten in seinen Dateidienstprogrammen unterstützt, ändert der Befehl "ls" (Ist) seine Funktionsweise wie folgt:

- Für Dateien, die eine Standard-Zugriffssteuerungsliste oder eine Zugriffssteuerungsliste mit mehr als den drei erforderlichen ACL-Einträgen enthalten, zeigt das Dienstprogramm "ls(1)" (Ist (1))" in der langen von "ls -l" (ls -l) erzeugten Form ein Pluszeichen (+) nach der Berechtigungszeichenfolge an.

Dies wird im Beispiel oben für "/dev/sr0, use getfacl -a /dev/sr0" angegeben, um festzustellen, ob der Benutzer im Rahmen einer Zugriffssteuerungsliste Zugriff erhalten hat. In diesem Fall trifft dies zu, sodass der Benutzer eine Verbindung mit der CD-ROM zum Ziel herstellen kann, auch wenn die Ausgabe des Befehls "ls -l" (Ist -l) gegenteilig lautet.

```

guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---

```

Eine ähnliche Prüfung der Berechtigungen für ein Wechselmedium ergibt Folgendes:

```

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
> getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---

```

Dies erfordert, dass der Benutzer schreibgeschützten Zugriff auf das Wechselmedium erhält:

```

root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

```

Das Laufwerk steht dann für die Verbindung mit dem Ziel zur Verfügung.



---

### Virtuelle Medien in einer Mac-Umgebung

Die folgenden Informationen zur Verwendung von virtuellen Medien sind für Mac®-Benutzer relevant.

#### Aktive Systempartitionen

- Sie können keine virtuellen Medien verwenden, um aktive Systempartitionen für einen Mac-Client bereitzustellen.

#### Laufwerkpartitionen

- Die folgenden Einschränkungen für Laufwerkpartitionen gelten für verschiedene Betriebssysteme:
  - Windows- und Mac-Ziele können keine unter Linux formatierten Partitionen lesen.
  - Windows® und Linux® können keine unter Mac formatierten Partitionen lesen.
  - Von Linux werden nur Windows FAT-Partitionen unterstützt.
  - Mac unterstützt Windows FAT und NTFS.
- Mac-Benutzer müssen alle bereits installierten Geräte deinstallieren, um eine Verbindung mit einem Zielsystem herzustellen. Verwenden Sie den Befehl ">diskutil umount /dev/disk1s1", um das Gerät zu deinstallieren, und "diskutil mount /dev/disk1s1", um es erneut zu installieren.

---

### Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist

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

- Für Linux®- und Mac®-Clients
- Bei allen Festplatten
- Wenn das Laufwerk schreibgeschützt ist
- Wenn der Benutzer nicht über eine Lese-/Schreibberechtigung verfügt.
  - Unter **Port Permission** (Port-Berechtigung) ist für **Access** (Zugriff) die Einstellung **None** (Kein) oder **View** (Anzeigen) ausgewählt.
  - Unter **Port Permission** (Port-Berechtigung) ist für **VM Access** (VM-Zugriff) die Einstellung **Read-Only** (Schreibgeschützt) oder **Deny** (Ablehnen) ausgewählt.

## Verwenden virtueller Medien

Lesen Sie die Hinweise zu den **Voraussetzungen für die Verwendung virtueller Medien** (auf Seite 84), bevor Sie virtuelle Medien verwenden.

► **So verwenden Sie virtuelle Medien:**

1. Wenn Sie auf Dateiserver-ISO-Abbilder zugreifen möchten, lassen Sie diese Dateiserver und Abbilder über die Seite "Remote Console File Server Setup" (Remotekonsolen-Dateiserver-Setup) erkennen.

---

*Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.*

---

2. Öffnen Sie eine KVM-Sitzung mit dem entsprechenden Zielserver.
  - a. Rufen Sie über die Remotekonsole die Seite "Port Access" (Portzugriff) auf.
  - b. Stellen Sie auf dieser Seite eine Verbindung mit dem Zielserver her:
    - Klicken Sie unter "Port Name" (Portname) auf den entsprechenden Server.
    - Wählen Sie im Menü "Port Action" (Portaktion) den Befehl "Connect" (Verbinden) aus. Der Zielserver wird in einem Fenster des Virtual KVM Client geöffnet.
3. 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" (CD-ROM/ISO verbinden)
ISO-Abbilder	"Connect CD-ROM/ISO" (CD-ROM/ISO verbinden)
Dateiserver-ISO-Abbilder	"Connect CD-ROM/ISO" (CD-ROM/ISO verbinden)

Nach Abschluss Ihrer Aufgaben trennen Sie die Verbindung zum virtuellen Medium. Siehe **Trennen von virtuellen Medien** (auf Seite 92)

---

## Herstellen einer Verbindung mit virtuellen Medien

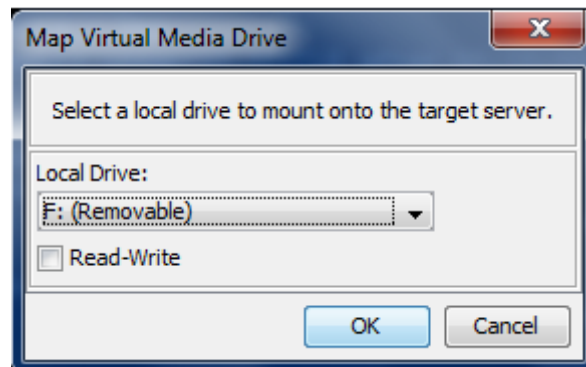
---

### 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. Netzwerklaufwerke, CD-ROM- oder DVD-ROM-Laufwerke sind nicht enthalten. Nur für diese Option ist "Read/Write" (Lese-/Schreibzugriff) verfügbar.

► **So greifen Sie auf ein Laufwerk auf dem Client-Computer 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. ()



2. Wählen Sie das entsprechende Laufwerk in der Dropdown-Liste **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 Wechsellaufwerke zur Verfügung. Weitere Informationen finden Sie unter **Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist** (auf Seite 88). 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 "OK". Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

---

**Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern**

---

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

---

*Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.*

---

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

1. Wählen Sie im Virtual KVM Client "Virtual Media > 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.
2. Gehen Sie bei internen und externen CD-ROM- und DVD-ROM-Laufwerken folgendermaßen vor:
  - a. Wählen Sie die Option "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk).
  - b. Wählen Sie das entsprechende Laufwerk in der Dropdown-Liste "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk) aus. Diese Liste enthält alle verfügbaren internen und externen CD- und DVD-Laufwerksnamen.
  - c. Klicken Sie auf "Connect" (Verbinden).
3. Gehen Sie bei ISO-Abbildern folgendermaßen vor:
  - a. Wählen Sie die Option "ISO Image" (ISO-Abbild). Mit dieser Option greifen Sie auf ein Laufwerkabbild einer CD, DVD oder Festplatte zu. Nur das ISO-Format wird unterstützt.
  - b. Klicken Sie auf "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.
  - d. Klicken Sie auf "Connect" (Verbinden).
4. Gehen Sie bei Remote-ISO-Abbildern auf einem Dateiserver folgendermaßen vor:
  - a. Wählen Sie die Option "Remote Server ISO Image" (ISO-Abbild auf Remoteserver).
  - b. Wählen Sie in der Dropdown-Liste einen Hostnamen und ein Abbild aus. Zur Verfügung stehen die Dateiserver und Abbildpfade, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben. Die Dropdown-Liste enthält nur Elemente, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben.

- c. "File Server Username" (Dateiserver-Benutzername) – Der für den Zugriff auf den Dateiserver erforderliche Benutzername. Der Name darf den Domännennamen, wie z. B. meinedomäne/Benutzername, enthalten.
- d. "File Server Password" (Dateiserver-Kennwort) – Das für den Zugriff auf den Dateiserver erforderliche Kennwort (Eingabe erfolgt verdeckt).
- e. Klicken Sie auf "Connect" (Verbinden).

Das Medium wird auf dem Zielsever virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

---

*Hinweis: Wenn Sie Dateien auf einem Linux®-Ziel bearbeiten, verwenden Sie den Befehl "Linux Sync" (Linux-Synchronisierung), nachdem die Dateien mithilfe eines virtuellen Mediums kopiert wurden, um die kopierten Dateien anzuzeigen. Die Dateien werden möglicherweise erst angezeigt, nachdem die Synchronisierung durchgeführt wurde.*

*Hinweis: Wenn Sie mit dem Windows 7®-Betriebssystem® arbeiten, werden Wechseldatenträger nicht standardmäßig im Windows-Ordner "Arbeitsplatz" angezeigt, sobald Sie ein lokales CD-/DVD-Laufwerk oder ein lokales oder Remote-ISO-Abbild mounten. Um das lokale CD-/DVD-Laufwerk oder das lokale oder Remote-ISO-Abbild in diesem Ordner anzuzeigen, wählen Sie "Extras" > "Ordneroptionen" > "Ansicht" aus und deaktivieren die Option "Leere Laufwerke im Ordner "Computer" ausblenden".*

*Hinweis: Aufgrund von technischen Einschränkungen der Drittanbieter-Software können Sie bei Verwendung einer IPv6-Adresse nicht über virtuelle Medien auf ein Remote-ISO-Abbild zugreifen.*

---

## Trennen von virtuellen Medien

### ► So trennen Sie virtuelle Medienlaufwerke:

- Wählen Sie für lokale Laufwerke "Virtual Media" > "Disconnect Drive" (Virtuelle Medien > Laufwerk trennen) aus.
- Wählen Sie für CD-ROM-, DVD-ROM- und ISO-Abbilder "Virtual Media > Disconnect CD-ROM/ISO Image" (Virtuelle Medien > CD-ROM-/ISO-Abbild trennen) aus.

---

*Hinweis: Anstatt das virtuelle Medium über den Befehl "Disconnect" (Trennen) zu trennen, können Sie auch einfach die KVM-Verbindung beenden.*

---

# Kapitel 5 User Management (Benutzerverwaltung)

## In diesem Kapitel

Benutzergruppen .....	93
Benutzer .....	100
Authentication Settings (Authentifizierungseinstellungen) .....	105
Ändern von Kennwörtern .....	119

---

## Benutzergruppen

Jedes KX II-101-V2 enthält standardmäßig drei Benutzergruppen. Diese Gruppen können nicht gelöscht werden:

Benutzer	Beschreibung
Admin	Benutzer dieser Gruppe verfügen über vollständige Administratorrechte. Der ursprüngliche werkseitige Standardbenutzer ist Mitglied dieser Gruppe und verfügt über sämtliche Systemrechte. Außerdem muss der Benutzer "Admin" der Gruppe "Admin" angehören.
Unknown (Unbekannt)	Dies ist die Standardgruppe für Benutzer, die extern über LDAP/LDAPS oder RADIUS authentifiziert werden oder die im System unbekannt sind. Wenn der externe LDAP/LDAPS- oder RADIUS-Server keine gültige Benutzergruppe erkennt, wird die Gruppe "Unknown" (Unbekannt) verwendet. Außerdem wird jeder neu erstellte Benutzer automatisch in diese Gruppe aufgenommen, bis der Benutzer einer anderen Gruppe zugewiesen wird.
Individual Group (Individuelle Gruppe)	Eine individuelle Gruppe ist im Prinzip eine aus einer Person bestehende "Gruppe". Dies bedeutet, dass sich der Benutzer in seiner eigenen Gruppe befindet und nicht mit anderen echten Gruppen verknüpft ist. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen. In individuellen Gruppen können Benutzerkonten dieselben Rechte wie eine Gruppe aufweisen.

In KX II-101-V2 können bis zu 254 Benutzergruppen erstellt werden.

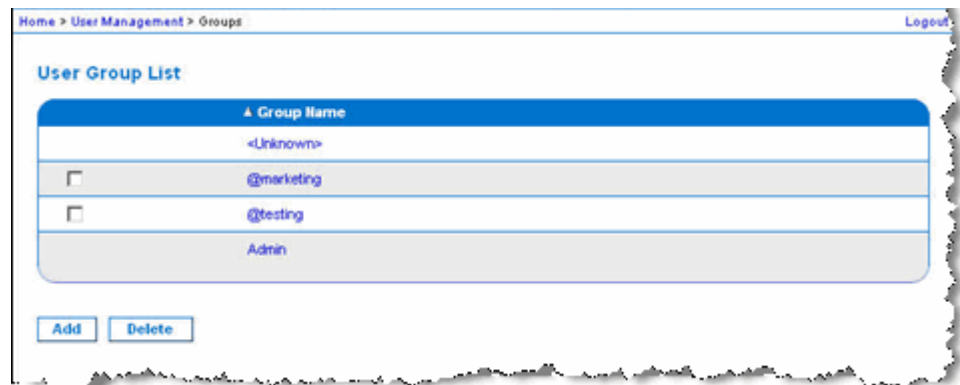
### User Group List (Liste der Benutzergruppen)

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

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

► **So zeigen Sie eine Liste der Benutzergruppen an:**

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



---

### Beziehung zwischen Benutzern und Gruppen

Benutzer sind Mitglied in einer Gruppe, und Gruppen verfügen über bestimmte Berechtigungen. Sie können Zeit sparen, indem Sie die verschiedenen Benutzer Ihrer KX II-101-V2-Einheit in Gruppen organisieren. So können Sie die Berechtigungen aller Benutzer in einer Gruppe auf einmal verwalten anstatt für jeden Benutzer einzeln.

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

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

---

### Hinzufügen einer neuen Benutzergruppe

► **So fügen Sie eine neue Benutzergruppe hinzu:**

1. Wählen Sie "User Management > Add New User Group" (Benutzerverwaltung > Neue Benutzergruppe hinzufügen) oder klicken Sie auf der Seite "User Group List" (Liste der Benutzergruppen) auf die Schaltfläche "Add" (Hinzufügen).
2. Geben Sie im Feld "Group Name" (Gruppenname) einen aussagekräftigen Namen für die neue Benutzergruppe ein (bis zu 64 Zeichen).
3. Aktivieren Sie die Kontrollkästchen neben den Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe **Festlegen von Berechtigungen** (auf Seite 98).

### Festlegen von Port-Berechtigungen

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

Portzugriff	
Option	Beschreibung
Deny (Ablehnen)	Zugriff vollständig verweigert
View (Anzeigen)	Anzeigen des Videobildes, aber keine Interaktion mit dem angeschlossenen Zielserver
Control	Steuerung des angeschlossenen Zielservers Die



(Steuern)	Option "Control" (Steuern) muss der Gruppe zugeordnet sein, wenn der Zugriff auf virtuelle Medien und Stromzufuhrsteuerung ebenso gewährt wird.
-----------	---

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

Zugriff auf Stromzufuhrsteuerung	
Option	Beschreibung
Deny (Ablehnen)	Keine Berechtigung für die Stromzufuhrsteuerung auf dem Zielsystem
Access (Zugriff)	Volle Berechtigung für die Stromzufuhrsteuerung auf einem Zielsystem

#### Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)

**Wichtig: Gehen Sie bei der Verwendung der gruppenbasierten IP-Zugriffssteuerung bedachtsam vor. Der Zugriff auf KX II-101-V2 kann Ihnen verweigert werden, wenn sich Ihre IP-Adresse in einem Bereich befindet, der keine Zugriffsberechtigung hat.**

Mit diesem Feature beschränken Sie den Zugriff auf das KX II-101-V2-Gerät durch Benutzer in der ausgewählten Gruppe auf bestimmte IP-Adressen. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für alle Zugriffsversuche auf das Gerät gilt, zuerst verarbeitet wird und Priorität hat.

**Wichtig: Die IP-Adresse 127.0.0.1 wird vom lokalen KX II-101-V2-Port verwendet und kann nicht gesperrt werden.**

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

Rule #	Starting IP	Ending IP	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT <input type="button" value="v"/>

► **So fügen Sie Regeln hinzu:**

1. Geben Sie im Feld "Starting IP" (IP-Startadresse) die IP-Startadresse ein.
2. Geben Sie im Feld "Ending IP" (IP-Endadresse) die IP-Endadresse ein.
3. Wählen Sie unter "Action" (Aktion) eine der folgenden Optionen:
  - Accept (Akzeptieren) – Diese IP-Adressen können auf das KX II-101-V2-Gerät zugreifen.
  - Drop (Ablehnen) – Diesen IP-Adressen wird der Zugriff auf das KX II-101-V2-Gerät verweigert.
4. Klicken Sie auf "Append" (Anfügen). Die Regel wird unten in der Liste hinzugefügt. Wiederholen Sie die Schritte 1 bis 4, um weitere Regeln hinzuzufügen.

► **So fügen Sie eine Regel ein:**

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

► **So ersetzen Sie eine Regel:**

1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie Werte in die Felder "Starting IP" (IP-Startadresse) und "Ending IP" (IP-Endadresse) ein.
3. Wählen Sie in der Dropdownliste "Action" (Aktion) eine Option aus.

4. Klicken Sie auf "Replace" (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

► **So löschen Sie eine Regel:**

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

---

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

---

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

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

---

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

---

### 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
Gerätezugriff unter CC-SG-Verwaltung	<p>Ermöglicht Benutzern und Benutzergruppen mit dieser Berechtigung den direkten Zugriff auf KX II-101-V2 unter Verwendung einer IP-Adresse, wenn die Option "Local Access" (Lokaler Zugriff) für das Gerät in CC-SG aktiviert ist. Es kann von der lokalen und der Remotekonsole sowie vom MPC, VKC und AKC auf das Gerät zugegriffen werden.</p> <p>Wird unter CC-SG-Verwaltung direkt auf ein Gerät zugegriffen, werden Zugriff und Verbindungsaktivitäten auf KX II-101-V2 protokolliert. Die Benutzerauthentifizierung erfolgt gemäß den KX II-101-V2-Authentifizierungseinstellungen.</p> <hr/> <p><i>Hinweis: Die Benutzer der Gruppe "Admin" verfügen standardmäßig über diese</i></p>

Berechtigung	Beschreibung
	<i>Berechtigung.</i>
Device Settings (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 II-101-V2-Diagnose
Wartung	Sichern und Wiederherstellen von Datenbanken, Firmwareaktualisierung, Werksrückstellung, Neustart
Modem Access (Modemzugriff)	Berechtigung zur Verwendung des Modems, um eine Verbindung zum KX II-101-V2-Gerät herzustellen.
PC-Share (PC-Freigabe)	Gleichzeitiger Zugriff auf ein Zielgerät durch mehrere Benutzer
Security (Sicherheit)	SSL-Zertifikat, Sicherheitseinstellungen (VM-Freigabe, PC-Freigabe), IP-ACL
User Management (Benutzerverwaltung)	Benutzer- und Gruppenverwaltung, Remoteauthentifizierung (LDAP/LDAPS/RADIUS), Anmeldeeinstellungen

### Festlegen von Berechtigungen für eine individuelle Gruppe

#### ► So legen Sie Berechtigungen für eine individuelle Benutzergruppe fest:

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

---

## Ändern einer vorhandenen Benutzergruppe

---

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

---

► **So ändern Sie eine vorhandene Benutzergruppe:**

1. Bearbeiten Sie auf der Seite "Group" (Gruppe) die entsprechenden Felder, und legen Sie die gewünschten Berechtigungen fest.
2. Legen Sie unter "Permissions" (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe **Festlegen von Berechtigungen** (auf Seite 98).
3. Legen Sie unter "Port Permissions" (Port-Berechtigungen) die Port-Berechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Server-Ports fest, und geben Sie die Zugriffsart an. Siehe **Festlegen von Portberechtigungen** (siehe **"Festlegen von Port-Berechtigungen"** auf Seite 95).
4. Legen Sie die IP-ACL fest (optional). Mit diesem Feature beschränken Sie den Zugriff auf das KX II-101-V2-Gerät, indem Sie IP-Adressen angeben. Siehe **Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)** (auf Seite 96).
5. Klicken Sie auf "OK".

► **So löschen Sie eine Benutzergruppe:**

---

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

---

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

---

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

---

## Benutzer

Benutzern müssen Benutzernamen und Kennwörter zugeordnet werden, damit sie auf KX II-101-V2 zugreifen können. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf KX II-101-V2 zuzugreifen.

---

### Anzeigen der KX II-101-V2-Benutzerliste

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

Informationen zum Anzeigen der Ports, mit denen jeder Benutzer verbunden ist, finden Sie unter Anzeigen der Benutzer nach Port.

► **So zeigen Sie die Benutzerliste an:**

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

---

### Anzeigen der Benutzer nach Port

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

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

Diese Seite enthält die folgenden Benutzer- und Portinformationen:

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

---

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

---

- Username (Benutzername) – Benutzername für Benutzeranmeldungen und Zielverbindungen
- Access From (Zugriff von) – IP-Adresse des KX II-101-V2, auf den die Benutzer zugreifen
- Status – aktueller aktiver oder inaktiver Status der Verbindung

► **So zeigen Sie die Benutzer nach Port an:**

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

---

### Trennen der Benutzer von Ports

Wenn Benutzer getrennt werden, werden sie vom Zielport getrennt, ohne dass sie bei KX II-101-V2 abgemeldet werden.

---

*Hinweis: Beim Abmelden der Benutzer werden sie vom Zielport getrennt und bei KX II-101-V2 abgemeldet. Weitere Informationen zur erzwungenen Abmeldung von Benutzern finden Sie unter **Abmelden der Benutzer bei KX II-101-V2 (Erzwungene Abmeldung)** (auf Seite 102).*

---

► **So trennen Sie Benutzer vom Port:**

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

---

### Abmelden der Benutzer bei KX II-101-V2 (Erzwungene Abmeldung)

Wenn Sie Administrator sind, können Sie alle lokal authentifizierte Benutzer, die auf KX II-101-V2 angemeldet sind, abmelden. Benutzer können auch auf Portebene getrennt werden. Siehe **Trennen der Benutzer von Ports** (auf Seite 102).

► **So melden Sie einen Benutzer bei KX II-101-V2 ab:**

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

---

## Hinzufügen eines neuen Benutzers

Es ist empfehlenswert, Benutzergruppen vor dem Erstellen von KX II-101-V2-Benutzern zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe zugewiesen werden muss. Siehe **Hinzufügen einer neuen Benutzergruppe**.

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

---

*Hinweis: Ein Benutzername kann deaktiviert werden, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche die auf der Seite "Security Settings" (Sicherheitseinstellungen) festgelegte maximale Anzahl der Anmeldeversuche überschritten hat. Siehe **Sicherheitseinstellungen** (siehe "**Security Settings (Sicherheitseinstellungen)**" auf Seite 161).*

---

### ► So fügen Sie einen neuen Benutzer hinzu:

1. 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).
2. Geben Sie im Feld "Username" (Benutzername) einen eindeutigen Namen ein (bis zu 16 Zeichen).
3. Geben Sie im Feld "Full Name" (Vollständiger Name) den vollständigen Namen des Benutzers ein (bis zu 64 Zeichen).
4. Geben Sie im Feld "Password" (Kennwort) ein Kennwort ein, und anschließend im Feld "Confirm Password" (Kennwort bestätigen) erneut (bis zu 64 Zeichen).
5. Wählen Sie in der Dropdown-Liste "User Group" (Benutzergruppe) die Gruppe aus.

Wenn Sie diesen Benutzer keiner vorhandenen Benutzergruppe zuordnen möchten, wählen Sie in der Dropdownliste die Option "Individual Group" (Individuelle Gruppe) aus. Weitere Informationen zu den Berechtigungen einer individuellen Gruppe finden Sie unter **Festlegen von Berechtigungen für eine individuelle Gruppe** (auf Seite 99).

6. Lassen Sie das Kontrollkästchen "Active" (Aktiv) aktiviert, um den neuen Benutzer zu aktivieren. Klicken Sie auf "OK".

---

## Ändern eines vorhandenen Benutzers

### ► So ändern Sie einen vorhandenen Benutzer:

1. Öffnen Sie die Seite "User List" (Benutzerliste) unter "User Management" > "User List" (Benutzerverwaltung > Benutzerliste).



2. Wählen Sie den Benutzer aus der Liste auf der Seite "User List" (Benutzerliste) aus.
3. Klicken Sie auf den Benutzernamen. Die Seite "User" (Benutzer) wird angezeigt.
4. Bearbeiten Sie auf der Seite "User" (Benutzer) die entsprechenden Felder. Informationen zum Zugriff auf die Seite "User" (Benutzer) finden Sie unter **Hinzufügen eines neuen Benutzers** (auf Seite 103).
5. Klicken Sie auf "Delete" (Löschen), um einen Benutzer zu löschen. Sie werden aufgefordert, den Löschvorgang zu bestätigen.
6. Klicken Sie auf OK.

---

### Sperrern von Benutzern und Aufheben der Sperrung

Der Zugriff eines Benutzers auf das System kann vom Administrator oder automatisch aufgrund der Sicherheitseinstellungen gesperrt werden. Siehe **Benutzersperrung** (siehe "**User Blocking (Benutzersperrung)**" auf Seite 165). Ein gesperrter Benutzer wird inaktiv. Die Sperrung kann vom Administrator wieder aufgehoben werden.

► **So sperren Sie einen Benutzer oder heben die Sperrung auf:**

1. Wählen Sie "User Management > User List" (Benutzerverwaltung > Benutzerliste). Die Seite "User List" (Benutzerliste) wird angezeigt.
2. Aktivieren oder deaktivieren Sie das Kontrollkästchen "Active" (Aktiv).
  - Wenn das Kästchen aktiviert ist, wird der Benutzer aktiviert und kann auf KX II-101-V2 zugreifen.
  - Ist das Kästchen deaktiviert, ist der Benutzer inaktiv und kann nicht auf KX II-101-V2 zugreifen.
3. Klicken Sie auf "OK". Der Status des Benutzers wird aktualisiert.

---

## Authentication Settings (Authentifizierungseinstellungen)

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

Wenn KX II-101-V2 zur Remote-Authentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

---

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

---

### ► So konfigurieren Sie die Authentifizierung:

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

### ► So stellen Sie die werksseitigen Standardeinstellungen wieder her:

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

---

### Implementierung der LDAP/LDAPS-Remoteauthentifizierung


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

---

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

---

#### ► So verwenden Sie das LDAP-Authentifizierungsprotokoll:

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

#### Serverkonfiguration

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

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

**Optional**

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

### Authentication Settings

Local Authentication

LDAP

RADIUS

#### LDAP

##### Server Configuration

**Primary LDAP Server**  
192.168.59.187

**Secondary LDAP Server (optional)**  
192.168.51.214

**Type of External LDAP Server**  
Microsoft Active Directory

**Active Directory Domain**  
testradius.com

**User Search DN**  
cn=users,dc=testradius,dc=com

**DN of Administrative User (optional)**  
cn=Administrator,cn=users,dc=testrac

**Secret Phrase of Administrative User**  
••••••••

**Confirm Secret Phrase**

#### LDAP/LDAP Secure

12. Aktivieren Sie das Kontrollkästchen "Enable Secure LDA" (Secure LDAP aktivieren), wenn Sie SSL verwenden möchten. Dadurch wird das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, über das KX II-101-V2 sicher mit dem LDAP/LDAPS-Server kommunizieren kann.

13. Der Standardport lautet 389. Verwenden Sie entweder den Standard-TCP-Port für LDAP oder legen Sie einen anderen Port fest.
14. Der standardmäßige Secure LDAP-Port lautet 636. Verwenden Sie entweder den Standardport oder legen Sie einen anderen Port fest. Dieses Feld wird nur verwendet, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist.
15. Aktivieren Sie das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren), und verwenden Sie die zuvor hochgeladene CA-Stammzertifikatdatei zur Validierung des vom Server bereitgestellten Zertifikats. Wenn Sie die zuvor hochgeladene CA-Stammzertifikatdatei nicht verwenden möchten, lassen Sie das Kontrollkästchen deaktiviert. Die Deaktivierung dieser Funktion entspricht der Annahme des Zertifikats einer unbekanntes Zertifizierungsstelle. Dieses Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert wurde.

---

*Hinweis: Ist zusätzlich zur CA-Stammzertifikat-Validierung die Option "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert, muss der Hostname des Servers mit dem bereitgestellten allgemeinen Namen im Serverzertifikat übereinstimmen.*

---

16. Laden Sie die CA-Stammzertifikatdatei hoch, falls dies erforderlich ist. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist. Fragen Sie den Administrator des Authentifizierungsservers nach der CA-Zertifikatdatei im Base64-codierten X-509-Format für den LDAP-/LDAPS-Server. Navigieren Sie über die Schaltfläche "Browse" (Durchsuchen) zur entsprechenden Zertifikatdatei. Wenn Sie ein Zertifikat für den LDAP-/LDAPS-Server durch ein neues Zertifikat ersetzen, müssen Sie KX II-101-V2 neu starten, damit das neue Zertifikat wirksam wird.



**LDAP / Secure LDAP**

Enable Secure LDAP

**Port**  
389

**Secure LDAP Port**  
636

Enable LDAPS Server Certificate Validation

**Root CA Certificate File**  
Browse...

Upload

**Note: Reboot device after certificate file is uploaded.**

#### Testen des LDAP-Serverzugriffs

17. KX II-101-V2 bietet Ihnen aufgrund der Komplexität einer erfolgreichen Konfiguration von LDAP-Server und KX II-101-V2 zur Remoteauthentifizierung die Möglichkeit, die LDAP-Konfiguration auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) zu testen. Um die Authentifizierungseinstellungen zu testen, geben Sie den Anmeldenamen in das Feld "Login for testing" (Anmeldung für Test) und das Kennwort in das Feld "Password for testing" (Kennwort für Test) ein. Das sind der Benutzername und das Kennwort, die Sie für den Zugriff auf KX II-101-V2 eingegeben haben und die vom LDAP-Server für Ihre Authentifizierung verwendet werden. Klicken Sie auf "Test".

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



The image shows a dialog box titled "Test LDAP Server Access". Inside the dialog, there are two text input fields. The first is labeled "Login for testing" and the second is labeled "Password for testing". Below these fields is a button labeled "Test".

---

### Rückgabe von Benutzergruppeninformationen vom Active Directory-Server

KX II-101-V2 unterstützt die Benutzerauthentifizierung zu Active Directory® (AD), ohne dass Benutzer lokal in KX II-101-V2 definiert sein müssen. Dadurch können Active Directory-Benutzerkonten und -Kennwörter ausschließlich auf dem Active Directory-Server verwaltet werden. Die Autorisierungs- und Active Directory-Benutzerrechte werden mit standardmäßigen KX II-101-V2-Richtlinien und Benutzergruppenrechten, die lokal auf Active Directory-Benutzergruppen angewendet werden, gesteuert und verwaltet.

---

**WICHTIG: Wenn Sie bereits Kunde von Raritan, Inc. sind und den Active Directory-Server bereits durch Ändern des Active Directory-Schemas konfiguriert haben, unterstützt KX II-101-V2 diese Konfiguration nach wie vor, und Sie müssen den folgenden Vorgang nicht durchführen. Informationen zur Aktualisierung des Active Directory-LDAP/LDAPS-Schemas finden Sie unter Aktualisieren des LDAP-Schemas.**

---

► **So aktivieren Sie den AD-Server auf der KX II-101-V2-Einheit:**

1. Erstellen Sie auf der KX II-101-V2-Einheit besondere Gruppen und weisen Sie ihnen geeignete Berechtigungen zu. Erstellen Sie z. B. Gruppen wie "KVM\_Admin" und "KVM\_Operator".
2. Erstellen Sie auf dem Active Directory-Server neue Gruppen mit denselben Gruppennamen wie die im vorherigen Schritt erstellten Gruppen.



3. Weisen Sie die KX II-101-V2-Benutzer auf dem AD-Server den Gruppen zu, die Sie in Schritt 2 erstellt haben.
4. Aktivieren und konfigurieren Sie den AD-Server auf der KX II-101-V2-Einheit. Siehe **Implementierung der LDAP/LDAPS-Remoteauthentifizierung** (auf Seite 106).

**Wichtige Hinweise:**


- Bei der Eingabe des Gruppennamens muss die Groß-/Kleinschreibung beachtet werden.
- KX II-101-V2 bietet folgende Standardgruppen, die nicht geändert oder gelöscht werden können: "Admin" und "<Unknown>" (Unbekannt). Stellen Sie sicher, dass diese Gruppennamen nicht auch vom Active Directory-Server verwendet werden.
- Wenn die vom Active Directory-Server zurückgegebenen Gruppeninformationen nicht mit der KX II-101-V2-Gruppenkonfiguration übereinstimmen, weist KX II-101-V2 den Benutzern, die sich erfolgreich authentifizieren, automatisch die Gruppe "<Unknown>" (Unbekannt) zu.

---

**Implementierung der RADIUS-Remote-Authentifizierung**

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

► **So verwenden Sie das RADIUS-Authentifizierungsprotokoll:**

1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Klicken Sie auf das Optionsfeld "RADIUS", um den Abschnitt "RADIUS" der Seite zu aktivieren.
3. Klicken Sie auf das -Symbol, um den Abschnitt "RADIUS" zu erweitern.
4. Geben Sie in den Feldern "Primary Radius Server" (Primärer RADIUS-Server) und "Secondary Radius Server" (Sekundärer RADIUS-Server) die jeweiligen IP-Adressen des primären und optionalen sekundären Remote-Authentifizierungsservers ein (bis zu 256 Zeichen).
5. Geben Sie im Feld "Shared Secret" (Gemeinsamer geheimer Schlüssel) den geheimen Schlüssel für die Authentifizierung ein (bis zu 128 Zeichen).

Der gemeinsame geheime Schlüssel ist eine Zeichenfolge, die KX II-101-V2 und dem RADIUS-Server bekannt sein muss, damit diese sicher kommunizieren können. Es handelt sich dabei praktisch um ein Kennwort.

6. Der Standardport für "Authentication Port" (Authentifizierungsport) lautet 1812, kann jedoch nach Bedarf geändert werden.
7. Der Standardport für "Accounting Port" (Kontoführungsport) lautet 1813, kann jedoch nach Bedarf geändert werden.
8. Das "Timeout" (Zeitlimit) wird in Sekunden aufgezeichnet. Der Standardwert beträgt 1 Sekunde, kann jedoch bei Bedarf geändert werden.

Das Zeitlimit bezeichnet die Zeitspanne, während der KX II-101-V2 auf eine Antwort vom RADIUS-Server wartet, ehe eine weitere Authentifizierungsanforderung gesendet wird.

9. Die standardmäßige Anzahl an Neuversuchen beträgt 3.  
Dieser Wert gibt an, wie oft KX II-101-V2 eine Authentifizierungsanforderung an den RADIUS-Server sendet.
10. Wählen Sie in der Dropdownliste den "Global Authentication Type" (Globaler Authentifizierungstyp) aus:
  - PAP – Mit PAP werden Kennwörter als unformatierter Text gesendet. PAP ist nicht interaktiv. Benutzername und Kennwort werden als ein Datenpaket gesendet, sobald eine Verbindung hergestellt wurde. Der Server sendet nicht zuerst eine Anmeldeaufforderung und wartet auf eine Antwort.

- CHAP – Mit CHAP kann der Server jederzeit eine Authentifizierung anfordern. CHAP bietet mehr Sicherheit als PAP.

Home > User Management > Authentication Settings

**Authentication Settings**

Local Authentication  
 LDAP  
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type  
PAP ▼

---

### Zurückgeben von Benutzergruppeninformationen über RADIUS

Wenn ein RADIUS-Authentifizierungsversuch erfolgreich ist, bestimmt KX II-101-V2 die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers.

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

---

### Spezifikationen für den RADIUS-Kommunikationsaustausch

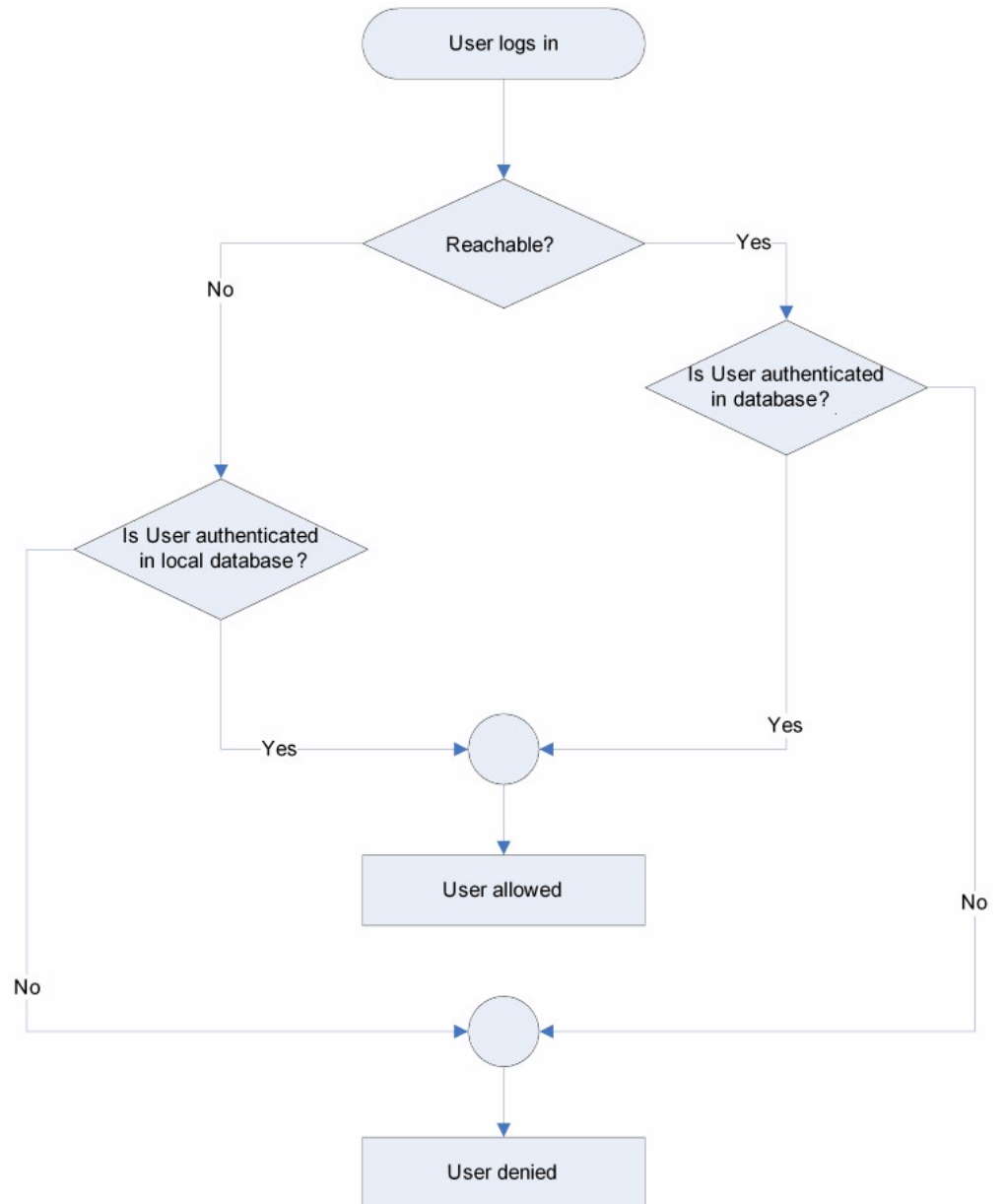
KX II-101-V2 sendet die folgenden RADIUS-Attribute an Ihren RADIUS-Server:

Attribut	Daten
<b>Anmelden</b>	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-IP-Address (4)	Die IP-Adresse des KX II-101-V2.
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.
<b>Accounting-Request(4)</b>	
Acct-Status (40)	Start(1) – Kontoführung wird gestartet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des KX II-101-V2.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.
<b>Abmelden</b>	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) – Kontoführung wird beendet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.

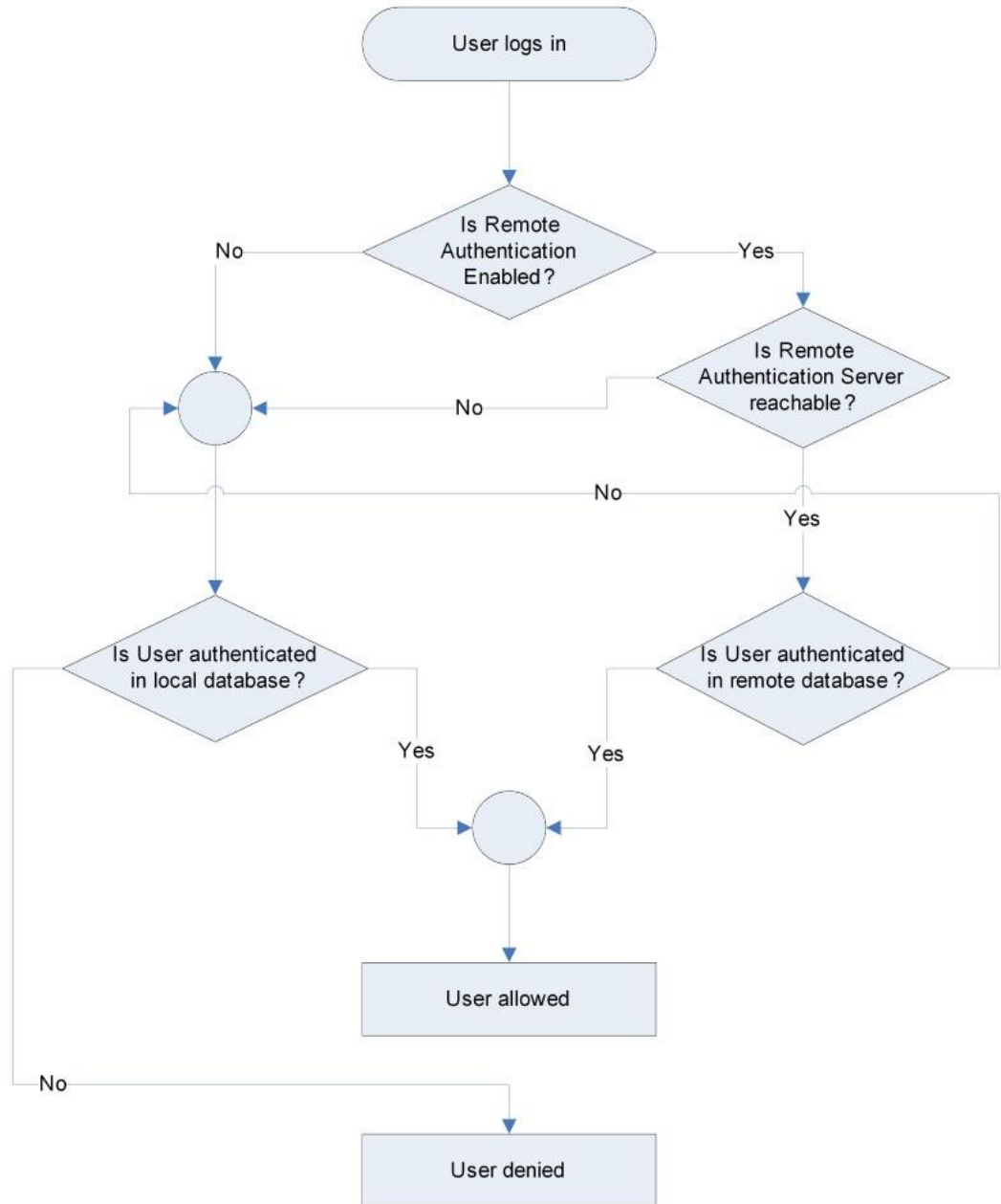
Attribut	Daten
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des KX II-101-V2.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.

### Benutzerauthentifizierungsprozess

Wenn das Gerät so konfiguriert wurde, dass lokale Benutzer authentifiziert und autorisiert werden, wird die Reihenfolge, in der die Benutzerdaten geprüft werden, durch den folgenden Vorgang bestimmt:



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



---

## Ändern von Kennwörtern

► **So ändern Sie Ihr Kennwort:**

1. Wählen Sie "User Management" > "Change Password" (Benutzerverwaltung > Kennwort ändern). Die Seite "Change Password" (Kennwort ändern) wird angezeigt.
2. Geben Sie im Feld "Old Password" (Altes Kennwort) Ihr aktuelles Kennwort ein.
3. Geben Sie in das Feld "New Password" (Neues Kennwort) ein neues Kennwort ein. Geben Sie das Kennwort im Feld "Confirm New Password" (Neues Kennwort bestätigen) erneut ein. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen.
4. Klicken Sie auf OK.
5. Die erfolgreiche Änderung des Kennworts wird bestätigt. Klicken Sie auf OK.

---

*Hinweis: Wenn sichere Kennwörter verwendet werden müssen, enthält diese Seite Informationen zum erforderlichen Format. Weitere Informationen zu Kennwörtern und sicheren Kennwörtern finden Sie unter **Sichere Kennwörter** (siehe "**Strong Passwords (Sichere Kennwörter)**" auf Seite 163).*

---

The screenshot shows a web interface for changing a password. At the top, there is a breadcrumb trail: "Home > User Management > Change Password". Below this is a blue header bar with the text "Change Password". The form contains three input fields: "Old Password", "New Password", and "Confirm New Password". At the bottom of the form, there are two buttons: "OK" and "Cancel".



# Kapitel 6 Geräteverwaltung

## In diesem Kapitel

Network Settings (Netzwerkeinstellungen).....	120
Device Services (Gerätedienste).....	126
Keyboard/Mouse Setup (Tastatur/Maus einrichten).....	131
Serial Port Settings (Einstellungen für seriellen Port) .....	132
Konfigurieren von Datum-/Uhrzeiteinstellungen.....	134
Ereignisverwaltung .....	135
Port Configuration (Port-Konfiguration) .....	144
Analoger KVM-Switch.....	152
Zurücksetzen des KX II-101-V2 mithilfe der Taste "Reset" (Zurücksetzen) .....	154
Ändern der Standardeinstellung für die GUI-Sprache.....	155

---

## Network Settings (Netzwerkeinstellungen)

Auf der Seite "Network Settings" (Netzwerkeinstellungen) können Sie die Netzwerkkonfiguration (z. B. IP-Adresse, Erkennungsport und LAN-Schnittstellenparameter) für Ihre KX II-101-V2-Einheit anpassen.

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

- None (default) [Keine (Standard)] – Dies ist die empfohlene Option (statisches IP). Da die KX II-101-V2-Einheit Teil Ihrer Netzwerkinfrastruktur ist, möchten Sie wahrscheinlich, dass die Adresse möglichst konstant bleibt. Bei dieser Option können Sie die Netzwerkparameter selbst einrichten.
- DHCP – Mit dieser Option wird die IP-Adresse automatisch durch einen DHCP-Server zugewiesen.

### ► So ändern Sie die Netzwerkkonfiguration:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Aktualisieren der Basisnetzwerkeinstellungen. Siehe **Basisnetzwerkeinstellungen** (siehe "**Network Basis Settings (Basisnetzwerkeinstellungen)**" auf Seite 121).
3. Aktualisieren der LAN-Schnittstelleneinstellungen. Siehe **LAN-Schnittstelleneinstellungen** (siehe "**LAN Interface Settings (LAN-Schnittstelleneinstellungen)**" auf Seite 125).
4. Klicken Sie auf OK, um die Konfiguration festzulegen. Ist für die vorgenommenen Änderungen ein Neustart des Geräts erforderlich, wird eine entsprechende Meldung angezeigt.

► **So kehren Sie zu den Werkseinstellungen zurück:**

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

---

**Network Basis Settings (Basisnetzwerkeinstellungen)**

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter **Netzwerkeinstellungen** (siehe "**Network Settings (Netzwerkeinstellungen)**" auf Seite 120).

► **So weisen Sie eine IP-Adresse zu:**

1. Wählen Sie "Device Settings > Network" (Geräteeinstellungen > Netzwerk). Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr KX II-101-V2-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.
3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
  - a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
  - b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
  - c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
  - d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
  - e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
    - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.  
Diese Option wird empfohlen, da KX II-101-V2 ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.
    - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

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

4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
  - a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.
  - b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem KX II-101-V2 zugeordnet ist.
  - c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.
  - d. Geben Sie die IP-Adresse des Gateway ein.
  - e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lese-zugriff)**
  - f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lese-zugriff)**
  - g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
    - None (Keine) – Wählen Sie diese Option aus, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

Wenn für "IP auto configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlänge) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.
    - Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.
5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.

6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

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

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

Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter **LAN-Schnittstelleneinstellungen** (siehe "**LAN Interface Settings (LAN-Schnittstelleneinstellungen)**" auf Seite 125).

*Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des KX II-101-V2 den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben. Weitere Informationen finden Sie auf der Seite **Network Settings** (siehe "**Network Settings (Netzwerkeinstellungen)**" auf Seite 120) (Netzwerkeinstellungen).*

**Basic Network Settings**

Device Name \*  
se-kx2-232

**IPv4 Address**

IP Address: 192.168.51.55      Subnet Mask: 255.255.255.0

Default Gateway: 192.168.51.126      Preferred DHCP Host Name:

IP Auto Configuration: DHCP

**IPv6 Address**

Global Unique IP Address: / Prefix Length:

Gateway IP Address:

Link-Local IP Address: N/A      Zone ID: %1

IP Auto Configuration: None

Obtain DNS Server Address Automatically

Use the Following DNS Server Addresses

Primary DNS Server IP Address: 192.168.59.2

Secondary DNS Server IP Address: 192.168.51.10

OK    Reset To Defaults    Cancel

---

### LAN Interface Settings (LAN-Schnittstelleneinstellungen)

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

- Wählen Sie die Einstellungen "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) aus.
  - "Autodetect (default option)" [Automatische Aushandlung (Standardoption)]
  - "10 Mbps/Half" (10 Mbit/s/Halb) – Gelbe LED blinkt
  - "10 Mbps/Full" (10 Mbit/s/Voll) – Gelbe LED blinkt
  - "100 Mbps/Half" (100 Mbit/s/Halb) - Gelbe LED blinkt und die grüne LED leuchtet kontinuierlich
  - "100 Mbps/Full" (100 Mbit/s/Voll) - Gelbe LED blinkt und die grüne LED leuchtet kontinuierlich

"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.*

---

Siehe **Netzwerk-Geschwindigkeitseinstellungen** (auf Seite 221).

- Wählen Sie die maximale Bandbreite aus.
  - No Limit (Keine Beschränkung)
  - 128 Kilobit
  - 256 Kilobit
  - 512 Kilobit
  - 2 Megabit
  - 5 Megabit
  - 10 Megabit
  - 100 Megabit

**NEUER SCREENSHOT ERFORDERLICH**

---

## Device Services (Gerätedienste)

Auf der Seite "Device Services" (Gerätedienste) können Sie die folgenden Funktionen konfigurieren:

- SSH-Zugriff aktivieren
- Erkennungsport eingeben
- Direkten Portzugriff aktivieren
- Telnet-Zugriff aktivieren
- Konfigurieren von HTTP- und HTTPS-Einstellungen
- Konfigurieren von SNMP-Agenten

---

### Aktivieren von Telnet

Wenn Sie Telnet für den Zugriff auf KX II-101-V2 verwenden möchten, greifen Sie zuerst über die Kommandozeilenschnittstelle oder einen Browser auf KX II-101-V2 zu.

► **So aktivieren Sie Telnet:**

1. Wählen Sie "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus, und aktivieren Sie das Kontrollkästchen "Enable TELNET Access" (TELNET-Zugriff aktivieren).
2. Geben Sie den Telnet-Port ein.
3. Klicken Sie auf OK.

Wenn der Telnet-Zugriff aktiviert ist, können Sie über diesen auf KX II-101-V2 zugreifen und die verbleibenden Parameter einstellen.

---

### Aktivieren von SSH

Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus, damit Administratoren über die SSH v2-Anwendung auf KX II-101-V2 zugreifen können.

► **So aktivieren Sie den SSH-Zugriff:**

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

---

### HTTP- und HTTPS-Porteinstellungen

Sie können von KX II-101-V2 verwendete HTTP- und/oder HTTPS-Ports konfigurieren. Wenn Sie z. B. den Standard-HTTP-Port 80 für andere Zwecke nutzen, wird beim Ändern des Ports sichergestellt, dass das Gerät nicht versucht, diesen Port zu verwenden.

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

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

---

### Eingeben des Erkennungsports

Die KX II-101-V2-Erkennung erfolgt über einen einzelnen konfigurierbaren TCP-Port. Der Standardport lautet 5000, Sie können diesen jedoch für die Verwendung aller TCP-Ports außer 80 und 443 konfigurieren. Wenn Sie über eine Firewall auf KX II-101-V2 zugreifen möchten, müssen die Firewallinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht-standardmäßigen konfigurierten Port zulassen.

► **So aktivieren Sie den Erkennungspport:**

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



---

### Aktivieren des direkten Port-Zugriffs über URL

Der direkte Portzugriff ermöglicht es Benutzern, die Verwendung der Seite "Login dialog and Port Access" (Anmeldedialog und Port-Zugriff) zu umgehen. Diese Funktion bietet auch die Möglichkeit, Benutzername und Kennwort direkt einzugeben und das Ziel aufzurufen, wenn Benutzername und Kennwort nicht in der URL enthalten sind.

Wichtige URL-Informationen für den direkten Portzugriff:

Wenn Sie den VKC und direkten Port-Zugriff verwenden:

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

#### ► So aktivieren Sie den direkten Port-Zugriff:

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

---

### Konfigurieren von SNMP-Agenten

SNMP-kompatible Geräte, genannt Agenten, speichern Daten über sich selbst in Management Information Bases (MIBs) und geben diese Daten an die SNMP-Manager zurück. Weitere Informationen zum Anzeigen von KX II-101-V2-MIB finden Sie unter **Anzeigen der KX II-101-V2-MIB** (auf Seite 141).

---

*KX II-101-V2 unterstützt die SNMP-Protokollierung für SNMP v1/v2c und/oder v3. SNMP v1/v2c definiert Meldungsformate und Protokollvorgänge, sofern die SNMP-Protokollierung aktiviert ist. SNMP v3 ist eine Sicherheitserweiterung von SNMP, die die Benutzerauthentifizierung, Kennwortverwaltung und Verschlüsselung ermöglicht.*

---

#### ► So konfigurieren Sie SNMP-Agenten:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Geben Sie die folgenden Identifier-Informationen des SNMP-Agenten für die MIB-II-Systemgruppenobjekte an:
  - a. System Name (Systemname) – Name/Gerätename des SNMP-Agenten

- b. System Contact (Systemkontakt) – Kontaktname für das Gerät
  - c. System Location (Systemstandort) – Standort des Geräts
3. Wählen Sie entweder "Enable SNMP v1/v2c" (SNMP v1/v2c aktivieren) und/oder "Enable SNMP v3" (SNMP v3 aktivieren) aus. Sie müssen mindestens eine Option auswählen.<erforderlich>
  4. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v1/v2c aus:
    - a. Community – die Communityzeichenfolge des Geräts
    - b. Community Type (Community-Typ) – Gewähren Sie Communitybenutzer entweder Lese- oder Lese-/Schreibzugriff

---

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

---

5. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v3 aus:
  - a. Wählen Sie gegebenenfalls "Use Auth Passphrase" (Authentifizierungs-Passphrase verwenden). Wenn eine Passphrase für den exklusiven Zugriff erforderlich ist, können Sie mit "Use Auth Passphrase" (Authentifizierungs-Passphrase verwenden) dieselbe Passphrase für beide verwenden, ohne die Authentifizierungs-Passphrase erneut einzugeben.
  - b. Security Name (Sicherheitsname) – Der Benutzername oder Name des Dienstkontos der Einheit, die mit dem SNMP-Agenten kommuniziert (max. 32 Zeichen).
  - c. Authentication Protocol (Authentifizierungsprotokoll) – Das MD5- oder SHA-Authentifizierungsprotokoll, das vom SNMP v3-Agenten verwendet wird.
  - d. Authentication Passphrase (Authentifizierungs-Passphrase) – Dies wird für den Zugriff auf den SNMP v3-Agenten benötigt (max. 64 Zeichen).
  - e. Privacy Protocol (Protokoll für exklusiven Zugriff) – Der AES- oder DES-Algorithmus, der zum Verschlüsseln von PDU- und Kontextdaten verwendet wird (falls zutreffend).
  - f. Privacy Passphrase (Passphrase für exklusiven Zugriff) – Die Passphrase, die für den Zugriff auf den Algorithmus des Protokolls für den exklusiven Zugriff verwendet wird (max. 64 Zeichen).
6. Klicken Sie auf "OK", um den SNMP-Agentendienst zu starten.

Konfigurieren Sie die SNMP-Traps auf der Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen). Diese Seite können Sie schnell aufrufen, indem Sie auf den Link "Link to SNMP Trap Configuration" (Link zur SNMP-Trap-Konfiguration) klicken. Weitere Informationen zum Erstellen von SNMP-Traps finden Sie unter Konfigurieren von SNMP-Traps, und eine Liste der verfügbaren KX II-101-V2-SNMP-Traps finden Sie unter Liste der KX II-101-V2-SNMP-Traps.

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

**SNMP Agent Configuration**

Enable SNMP Daemon

System Name: DominionKX      System Contact:      System Location:

Enable SNMP v1/v2c;

Community:      Community Type: Read-Only

Enable SNMP v3       Use Auth Passphrase

Security Name:      Auth Protocol: MD5      Auth Passphrase:      Privacy Protocol: None      Privacy Passphrase:

[Link to SNMP Trap Configuration](#)

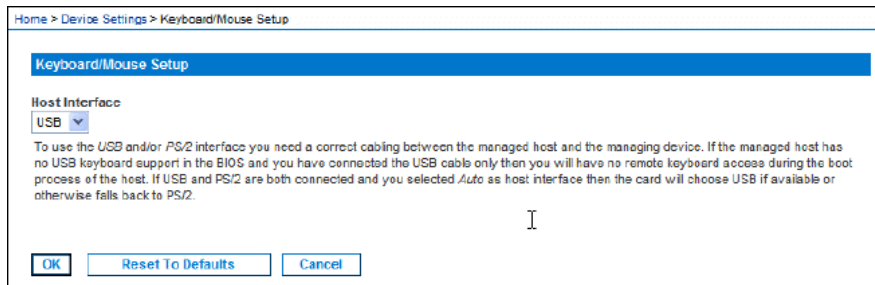
► **So stellen Sie die werksseitigen Standardeinstellungen wieder her:**

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

**WARNUNG:** Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen KX II-101-V2 und dem damit verbundenen Router verloren gehen, wenn KX II-101-V2 neu gestartet wird. Das SNMP-Trap "Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

## Keyboard/Mouse Setup (Tastatur/Maus einrichten)

Konfigurieren Sie die Tastatur- und Mausschnittstelle zwischen dem KX II-101-V2-Gerät und dem Hostgerät über die Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten).



1. Klicken Sie auf "Device Settings > Keyboard/Mouse" (Geräteeinstellungen > Tastatur/Maus).
2. Wählen Sie die gewünschte Einstellung unter "Host Interface" (Host-Schnittstelle) aus. Durch diese Auswahl legen Sie fest, ob KX II-101-V2 Tastatur- und Mausdaten über eine PS/2- oder USB-Verbindung sendet.
  - "Auto" (Automatisch) – Bei dieser Einstellung verwendet KX II-101-V2 eine USB-Verbindung (falls verfügbar), andernfalls greift das Gerät standardmäßig auf eine PS/2-Verbindung zu.
  - USB – Zwingt KX II-101-V2, die USB-Verbindung zum Senden der Tastatur- und Mausdaten an das Hostgerät zu verwenden.
  - PS/2 – Zwingt KX II-101-V2, die PS/2-Verbindung zum Senden der Tastatur- und Mausdaten an das Hostgerät zu verwenden.

---

*Hinweis: Wenn Sie auf der Vorderseite des KX II-101-V2-Geräts einen Switch von Raritan verwenden, müssen Sie die Einstellungen der Host-Schnittstelle zu "PS/2" abändern, um sicherzustellen, dass die Konfiguration ordnungsgemäß funktioniert. Siehe **Analoger KVM-Switch** (auf Seite 152).*

---

3. Klicken Sie auf "OK".
  - ▶ **So stellen Sie die werksseitigen Standardeinstellungen wieder her:**
    - Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

---

## Serial Port Settings (Einstellungen für seriellen Port)

Verwenden Sie die Seite "Serial Port Settings" (Einstellungen für seriellen Port), um zu konfigurieren, wie der KX II-101-V2 den seriellen Port verwendet.

---

### Port „Admin“

► **So konfigurieren Sie den seriellen Port "Admin":**

1. Wählen Sie "Device Settings > Serial Port" (Geräteeinstellungen > Serieller Port). Die Seite "Serial Port Settings" (Einstellungen für seriellen Port) wird angezeigt.
2. Aktivieren Sie das Optionsfeld "Admin Port" (Port "Admin").
3. Wählen Sie eine dieser Optionen aus, um eine direkte Verbindung von einem Client-PC mit KX II-101-V2 herzustellen und über ein Programm wie z. B. Hyperterminal auf die Befehlszeilenschnittstelle zuzugreifen. Siehe **Befehlszeilenschnittstelle (CLI)** (siehe "**Kommandozeilenschnittstelle (CLI)**" auf Seite 200).
4. Konfigurieren Sie im Bereich "Serial Settings" (Serielle Einstellungen) die folgenden Felder:
  - Speed (Geschwindigkeit)
  - Stop bits (Stoppbits)
  - Data bits (Datenbits)
  - Handshake
  - Parity (Parität)
5. Klicken Sie auf "OK".

---

### Steuerung des Powerstrip von Raritan

► **So konfigurieren Sie den seriellen Powerstrip-Port:**

1. Wählen Sie "Device Settings > Serial Port" (Geräteeinstellungen > Serieller Port). Die Seite "Serial Port Settings" (Einstellungen für seriellen Port) wird angezeigt.
2. Aktivieren Sie das Optionsfeld "PowerStrip Control" (Steuerung des PowerStrip). Wählen Sie diese Option aus, wenn Sie das KX II-101-V2-Gerät mit einem Powerstrip von Raritan verbinden.
3. Klicken Sie auf "OK".

---

## Modem

### ► So konfigurieren Sie den seriellen Modem-Port:

1. Wählen Sie "Device Settings > Serial Port" (Geräteeinstellungen > Serieller Port). Die Seite "Serial Port Settings" (Einstellungen für seriellen Port) wird angezeigt.
2. Aktivieren Sie das Optionsfeld "Modem". Wählen Sie diese Option, wenn Sie ein externes Modem mit dem KX II-101-V2-Gerät verbinden, um den DFÜ-Zugriff bereitzustellen.
3. Konfigurieren Sie im Bereich "Serial Settings" (Serielle Einstellungen) die folgenden Felder:
  - Serial line speed (Geschwindigkeit der seriellen Verbindung)
  - Modem init string (String für Modeminitialisierung) – Der in dem Feld angezeigte Standard-String muss verwendet werden, um den Modemzugriff zu ermöglichen.
  - Modem server IP address (IP-Adresse des Modemservers) – Die Adresse, die der Benutzer eingibt, um die KX II-101-V2-Webschnittstelle aufzurufen, sobald die Verbindung über das Modem hergestellt ist.
  - Modem client IP address (IP-Adresse für Modem-Client) - Die Adresse, die dem Benutzer nach der Verbindungsherstellung über das Modem zugewiesen wird.
4. Klicken Sie auf "OK".

Siehe **Kabelverbindungen für Modemzugriff** (auf Seite 133) für weitere Informationen zu der Kabelverbindung für Modemzugriff, und siehe **Zertifizierte Modems** (auf Seite 216) für weitere Informationen zu zertifizierten Modems, die mit dem KX II-101-V2-Gerät verwendet werden können. Informationen zu Einstellungen für optimale Leistung bei der Verbindung mit KX II-101-V2 über ein Modem finden Sie im Abschnitt **Creating, Modifying and Deleting Profiles in MPC - Generation 2 Devices** (Erstellen, Ändern und Löschen von Profilen im MPC – Geräte der 2. Generation) des Benutzerhandbuchs **KVM and Serial Access Clients Guide**.

### Kabelverbindungen für Modemzugriff

Konfigurieren Sie die Kabelverbindung wie folgt, um KX II-101-V2 mit einem Modem zu verbinden:

1. Verbinden Sie ein serielles Admin-Kabel mit KX II-101-V2.
2. Verbinden Sie einen 9-poligen Invertieradapter (Stecker/Stecker) mit dem seriellen Admin-Kabel.
3. Verbinden Sie die andere Seite des Invertieradapters mit einem Nullmodemkabel.

4. Verbinden Sie den 9-poligen Invertieradapter (Stecker/Stecker) mit dem anderen Ende des Nullmodemkabels.
5. Verbinden Sie zwischen dem Nullmodemkabel und dem Modem ein DB9 und ein DB25 Steckermodemkabel miteinander.

---

## Konfigurieren von Datum-/Uhrzeiteinstellungen

Auf der Seite **Date/Time Settings** (Datum-/Uhrzeiteinstellungen) stellen Sie Datum und Uhrzeit für die KX II-101-V2-Einheit ein. Hierzu haben Sie zwei Möglichkeiten:

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

► **So stellen Sie das Datum und die Uhrzeit ein:**

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

---

## Ereignisverwaltung

Das KX II-101-V2-Feature zur Ereignisverwaltung ermöglicht Ihnen die Verteilung von Systemereignissen auf SNMP-Manager, Syslog und das Prüfprotokoll zu aktivieren und zu deaktivieren. Die Ereignisse werden kategorisiert, und Sie können für jedes Ereignis festlegen, ob es an eines oder mehrere Ziele gesendet werden soll.

---

### Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)

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

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

### Konfigurieren von SNMP-Traps

Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung und die Überwachung von Netzwerkgeräten und ihrer Funktionen. SNMP-Traps werden über ein Netzwerk gesendet, um Informationen zu sammeln. Die Traps werden auf der Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) konfiguriert. Eine Liste der KX II-101-V2-SNMP-Traps finden Sie unter Liste der KX II-101-V2-SNMP-Traps.

SNMP-kompatible Geräte, genannt Agenten, speichern Daten über sich selbst in Management Information Bases (MIBs) und antworten auf das SNMP-Trap. SNMP-Agenten werden auf der Seite "Device Services" (Gerätedienste) konfiguriert. Informationen zum Konfigurieren von SNMP-Agenten finden Sie unter **Konfigurieren von SNMP-Agenten** (auf Seite 128), und Informationen zum Anzeigen der KX II-101-V2-MIB finden Sie unter **Anzeigen der KX II-101-V2-MIB** (auf Seite 141).

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

1. Wählen Sie "Device Settings > Event Management – Settings" (Geräteeinstellungen > Ereignisverwaltung – Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Wählen Sie "SNMP Logging Enabled" (SNMP-Protokollierung aktiviert) aus, um die verbleibenden Kontrollkästchen zu aktivieren. <erforderlich>



3. Wählen Sie entweder "SNMP v1/v2c Traps Enabled" (SNMP v1/v2c-Traps aktiviert) oder "SNMP Trap v3 Enabled" (SNMP-Trap v3 aktiviert) oder beide Optionen aus. Sie müssen mindestens eine Option auswählen. Nachdem Sie die Optionen ausgewählt haben, werden alle dazugehörigen Felder aktiviert. <erforderlich>
4. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v1/v2c aus:
  - a. Destination IP/Hostname (IP-Zieladresse/Hostname) – IP-Adresse oder Hostname des SNMP-Managers. Sie können maximal fünf (5) SNMP-Manager erstellen.

---

*Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.*

---

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

---

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

---

5. Aktivieren Sie das Kontrollkästchen "SNMP Trap v3 Enabled" (SNMP-Trap v3 aktiviert), falls es noch nicht aktiviert ist, um die folgenden Felder zu aktivieren. Füllen Sie gegebenenfalls die folgenden Felder für SNMP v3 aus:
  - a. Destination IP/Hostname (IP-Zieladresse/Hostname) – IP-Adresse oder Hostname des SNMP-Managers. Sie können maximal fünf (5) SNMP-Manager erstellen.

---

*Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.*

---

- b. Port Number (Portnummer) – Die vom SNMP-Manager verwendete Portnummer.
- c. Security Name (Sicherheitsname) – Der Benutzername oder Name des Dienstkontos der Einheit, die mit dem SNMP-Agenten kommuniziert (max. 32 Zeichen).
- d. Authentication Protocol (Authentifizierungsprotokoll) – Das MD5- oder SHA-Authentifizierungsprotokoll, das vom SNMP v3-Agenten verwendet wird.
- e. Authentication Passphrase (Authentifizierungs-Passphrase) – Dies wird für den Zugriff auf den SNMP v3-Agenten benötigt (max. 64 Zeichen).

- f. Privacy Protocol (Protokoll für exklusiven Zugriff) – Der AES- oder DES-Algorithmus, der zum Verschlüsseln von PDU- und Kontextdaten verwendet wird (falls zutreffend).
  - g. Privacy Passphrase (Passphrase für exklusiven Zugriff) – Die Passphrase, die für den Zugriff auf den Algorithmus des Protokolls für den exklusiven Zugriff verwendet wird (max. 64 Zeichen).
6. Klicken Sie auf "OK", um die SNMP-Traps zu erstellen.

Mithilfe des Links "Link to SNMP Agent Configuration" (Link auf SNMP-Agentenkonfiguration) können Sie die Seite "Devices Services" (Gerätedienste) schnell von der Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) aufrufen.

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

---

*KX II-101-V2 unterstützt die SNMP-Protokollierung für SNMP v1/v2c und/oder v3. SNMP v1/v2c definiert Meldungsformate und Protokollvorgänge, sofern die SNMP-Protokollierung aktiviert ist. SNMP v3 ist eine Sicherheitserweiterung von SNMP, die die Benutzerauthentifizierung, Kennwortverwaltung und Verschlüsselung ermöglicht.*

---

► **So bearbeiten Sie vorhandene SNMP-Traps:**

1. Wählen Sie "Device Settings > Event Management – Settings" (Geräteeinstellungen > Ereignisverwaltung – Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf "OK", um die Änderungen zu speichern.

*Hinweis: Wenn Sie die SNMP-Einstellungen deaktivieren, werden die SNMP-Informationen beibehalten, sodass Sie sie nicht erneut eingeben müssen, wenn Sie die Einstellungen wieder aktivieren.*

► **So löschen Sie SNMP-Traps:**

- Löschen Sie alle Werte in den Feldern für die SNMP-Traps, und speichern Sie die Änderungen.

Stellen Sie die werkseitigen Standardwerte wieder her, um die SNMP-Konfiguration zu löschen und die werkseitigen Standardeinstellungen von KX II-101-V2 wieder festzulegen.

**WARNUNG:** Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen KX II-101-V2 und dem damit verbundenen Router verloren gehen, wenn KX II-101-V2 neu gestartet wird. Das SNMP-Trap "Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

Home > Device Settings > Event Management - Settings

**SNMP Traps Configuration**

SNMP Logging Enabled  SNMP v1/v2c Traps Enabled  SNMP Trap v3 Enabled

SNMP v1/v2 Trap

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

SNMP v3 Trap

Engine ID: 80001f8803000d5d03ca3b

Destination IP/Hostname	Port #	Security Name	Auth Protocol	Auth Passphrase	Privacy Protocol	Privacy Passphrase
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	

[Link to SNMP Agent Configuration](#)

[Click here to view the Dominion KX2 SNMP MIB](#)

**Liste der KX II-101-V2-SNMP-Traps**

SNMP bietet die Möglichkeit, Traps (Benachrichtigungen) zu senden, um einen Administrator zu informieren, wenn eine oder mehrere Bedingungen erfüllt sind. Die folgende Tabelle enthält die SNMP-Traps von KX II-101-V2.

Trap-Name	Beschreibung
configBackup	Die Gerätekonfiguration wurde gesichert.

Trap-Name	Beschreibung
configRestore	Die Gerätekonfiguration wurde wiederhergestellt.
deviceUpdateFailed	Das Gerät konnte nicht aktualisiert werden.
deviceUpgradeCompleted	KX II-101-V2 hat die Aktualisierung mittels einer RFP-Datei abgeschlossen.
deviceUpgradeStarted	KX II-101-V2 hat die Aktualisierung mittels einer RFP-Datei begonnen.
factoryReset	Das Gerät wurde auf die Werkseinstellungen zurückgesetzt.
firmwareFileDiscarded	Die Firmware-Datei wurde verworfen.
firmwareUpdateFailed	Die Firmware konnte nicht aktualisiert werden.
firmwareValidationFailed	Die Firmware konnte nicht validiert werden.
groupAdded	Eine Gruppe wurde zum KX II-101-V2-System hinzugefügt.
groupDeleted	Eine Gruppe wurde aus dem System gelöscht.
groupModified	Eine Gruppe wurde geändert.
networkFailure	Für eine der Ethernet-Schnittstellen des Produkts besteht keine Netzwerkverbindung mehr.
networkParameterChanged	Die Netzwerkparameter wurden geändert.
networkParameterChangedv2	Die Netzwerkparameter des KX II-101-V2 wurden geändert.
passwordSettingsChanged	Die Einstellungen für sichere Kennwörter wurden geändert.
portConnect	Ein zuvor authentifizierter Benutzer hat eine KVM-Sitzung gestartet.
portConnectv2	Ein zuvor authentifizierter KX II-101-V2-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.
portDisconnectv2	Die Sitzung des KX II-101-V2-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.

Trap-Name	Beschreibung
powerOutletNotification	Benachrichtigung über den Status eines Powerstrip-Geräteausgangs.
rebootCompleted	Der Neustart von KX II-101-V2 ist abgeschlossen.
rebootStarted	KX II-101-V2 wird neu gestartet: entweder durch Wiederherstellen der Stromversorgung oder durch einen „Warmstart“ mittels des Betriebssystems.
securityBannerAction	Die Sicherheitsmeldung wurde akzeptiert oder abgelehnt.
securityBannerChanged	Die Sicherheitsmeldung wurde geändert.
securityViolation	Ein Sicherheitsproblem ist aufgetreten.
setDateTime	Das Datum und die Uhrzeit wurden für das Gerät eingestellt.
setFIPSMode	Der FIPS-Modus wurde aktiviert.
startCCManagement	Für das Gerät wurde die CommandCenter-Verwaltung gestartet.
stopCCManagement	Die CommandCenter-Verwaltung des Geräts wurde aufgehoben.
userAdded	Ein Benutzer wurde zum System hinzugefügt.
userAuthenticationFailure	Ein Benutzer hat versucht, sich mit einem falschen Benutzernamen und/oder Kennwort anzumelden.
userConnectionLost	Bei einem Benutzer mit aktiver Sitzung ist eine nicht ordnungsgemäße Sitzungstrennung aufgetreten.
userDeleted	Ein Benutzerkonto wurde gelöscht.
userForcedLogout	Ein Benutzer wurde durch "Admin" zwangsabgemeldet.
userLogin	Ein Benutzer hat sich erfolgreich bei KX II-101-V2 angemeldet und wurde authentifiziert.
userLogout	Ein Benutzer hat sich erfolgreich und ordnungsgemäß von KX II-101-V2 abgemeldet.
userModified	Ein Benutzerkonto wurde geändert.
userPasswordChanged	Das Ereignis wird ausgelöst, wenn das Kennwort irgendeines Benutzers des Geräts geändert wird.
userSessionTimeout	Die aktive Sitzung eines Benutzers wurde aufgrund einer Zeitüberschreitung beendet.
userUploadedCertificate	Ein Benutzer hat ein SSL-Zertifikat hochgeladen.

Trap-Name	Beschreibung
vmlImageConnected	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.
vmlImageDisconnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu deinstallieren.

#### **Anzeigen der KX II-101-V2-MIB**

##### ► So zeigen Sie die KX II-101-V2-MIB an:

1. Wählen Sie "Device Settings > Event Management – Settings" (Geräteeinstellungen > Ereignisverwaltung – Einstellungen). Die Seite "Event Management – Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Klicken Sie auf den Link "Click here to view the Dominion KX2 SNMP MIB" (Klicken Sie hier, um die Dominion-KX2 SNMP MIB anzuzeigen). Die MIB-Datei wird in einem Browserfenster geöffnet.

---

*Hinweis: Wenn Sie eine Lese-/Schreibberechtigung für die MIB-Datei haben, können Sie in einem MIB-Editor Änderungen an der Datei vornehmen.*

---

```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps
-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort
-- 07/08/11 H.
-- Corrected description for portStatusChange
-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList
-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction
-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateAndTime, setFIPSMODE
-- Also added defn for sysDateAndTime, fipsModeStatus
-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

### **SysLog-Konfiguration**

► **So konfigurieren Sie Syslog und aktivieren die Weiterleitung:**

1. Wählen Sie "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) aus, um Geräte-Protokollmeldungen an einen Remote-Syslog-Server zu senden.
2. Geben Sie die IP-Adresse/den Hostnamen Ihres Syslog-Servers im Feld "IP Address" (IP-Adresse) ein.
3. Klicken Sie auf "OK".

---

*Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.*

---

Stellen Sie die werkseitigen Standardwerte wieder her, um die syslog-Konfiguration zu löschen und die werkseitigen Standardeinstellungen von KX II-101-V2 wieder festzulegen.

► **So stellen Sie die werksseitigen Standardeinstellungen wieder her:**

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

---

### Konfigurieren der Ereignisverwaltung - Ziele

Systemereignisse generieren (falls aktiviert)  
SNMP-Benachrichtigungsereignisse (Traps) oder können in Syslog oder dem Prüfprotokoll protokolliert werden. Auf der Seite "Event Management - Destinations" (Ereignisverwaltung – Ziele) legen Sie fest, welche Systemereignisse verfolgt und wohin diese Informationen gesendet werden sollen.

---

*Hinweis: SNMP-Traps werden nur erzeugt, wenn die Option "SNMP Logging Enabled" (SNMP-Protokollierung aktiviert) ausgewählt ist. Syslog-Ereignisse werden nur erzeugt, wenn die Option "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) ausgewählt ist. Beide Optionen befinden sich auf der Seite "Event Management - Settings" (Ereignisverwaltung - Einstellungen). Siehe **Configuring Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)** (siehe "Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)" auf Seite 135).*

---

#### ► So wählen Sie Ereignisse und ihr Ziel aus:

1. Wählen Sie "Device Settings > Event Management – Destinations" (Geräteeinstellungen > Ereignisverwaltung – Ziele). Die Seite "Event Management - Destinations" (Ereignisverwaltung – Ziele) wird angezeigt.

Die Systemereignisse sind nach "Device Operation" (Gerätebetrieb), "Device Management" (Geräteverwaltung), "Security" (Sicherheit), "User Activity" (Benutzeraktivität) und "User Group Administration" (Benutzergruppenverwaltung) kategorisiert.

2. Aktivieren Sie die Kontrollkästchen der Ereignisse, die Sie aktivieren bzw. deaktivieren möchten, und geben Sie an, wohin die Informationen gesendet werden sollen.

---

*Tipp: Ganze Kategorien können durch Aktivieren bzw. Deaktivieren der entsprechenden Kategorie-Kontrollkästchen aktiviert bzw. deaktiviert werden.*

---

3. Klicken Sie auf "OK".



► **So stellen Sie die werksseitigen Standardeinstellungen wieder her:**

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

WARNUNG: Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen KX II-101-V2 und dem damit verbundenen Router verloren gehen, wenn KX II-101-V2 neu gestartet wird. Das SNMP-Trap "Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

---

## Port Configuration (Port-Konfiguration)

Die Seite "Port Configuration" (Port-Konfiguration) enthält eine Liste der KX II-101-V2-Ports. Ports, die mit KVM-Zielservern oder Powerstrips verbunden sind, werden blau angezeigt und können bearbeitet werden.

► **So ändern Sie eine Port-Konfiguration:**

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.

Sorting (Sortieren)

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

- "Port Name" (Portname) – Der dem Port zugewiesene Name. Ein schwarzer Port-Name gibt an, dass Name und Port nicht geändert bzw. bearbeitet werden können. Blaue Port-Namen können dagegen bearbeitet werden.

---

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

---

- Port Type (Porttyp) – Der Typ des am Port angeschlossenen Ziels.

Porttyp	Beschreibung
PowerStrip	Powerstrip/PDU
KVM	KVM-Ziel

► **So bearbeiten Sie einen Portnamen:**

1. Klicken Sie auf den Portnamen des Ports, den Sie bearbeiten möchten.

- Die Seite "Port" für KVM-Ports wird geöffnet. Auf dieser Seite können Sie die Ports benennen sowie Stromausgangszuordnungen und Zielsereinstellungen vornehmen.
- Für Powerstrips wird die Portseite für Powerstrips angezeigt. Auf dieser Seite können Sie die Powerstrips und ihre Ausgänge benennen. Siehe **Stromzufuhrsteuerung** (auf Seite 147).

---

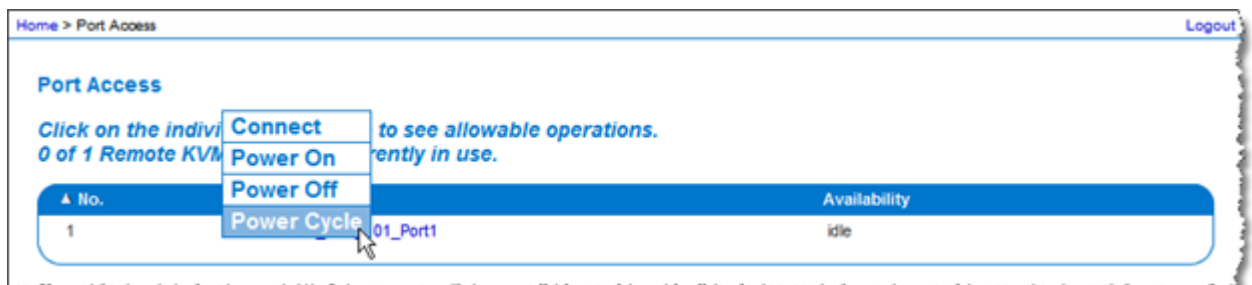
*Hinweis: Die Verknüpfung "Power Port 1" (Stromzufuhr – Port 1) steht nur zur Verfügung, wenn ein Powerstrip von Raritan mit KX II-101-V2 verbunden und konfiguriert ist. Ansonsten ist die Verknüpfung deaktiviert.*

---

### Verwalten von KVM-Zielservern (Seite "Port")

Diese Portseite wird angezeigt, wenn Sie auf der Seite Port Configuration (Port-Konfiguration) einen Port auswählen, der mit einem Zielserver verbunden ist. Auf dieser Seite können Sie Stromzuordnungen vornehmen und einen aussagekräftigeren Port-Namen eingeben.

Ein Server kann über maximal vier Netzschalter verfügen, die Sie dem Powerstrip zuordnen können. Auf dieser Seite können Sie diese Zuordnungen definieren, damit Sie über die Seite "Port Access" (Port-Zugriff) den Server einschalten, ausschalten sowie aus- und wieder einschalten können (siehe unten).




---

*Hinweis: Für diese Funktion muss ein Raritan Dominion PX-Powerstrip mit dem Gerät verbunden sein. Siehe Anschließen des Powerstrips.*

---

#### ► So greifen Sie auf eine Portkonfiguration zu:

1. Wählen Sie "Device Settings > Port Configuration" (Geräteeinstellungen > Port-Konfiguration). Die Seite "Port Configuration" (Port-Konfiguration) wird angezeigt.
2. Klicken Sie auf den Port-Namen des Ports, den Sie bearbeiten möchten.

---

*Hinweis: Die Verknüpfung "Power Port 1" (Stromzufuhr – Port 1) steht nur zur Verfügung, wenn ein Powerstrip von Raritan mit KX II-101-V2 verbunden und konfiguriert ist. Ansonsten ist die Verknüpfung deaktiviert.*

---

### Einen Port umbenennen

► **So ändern Sie den Port-Namen:**

1. Geben Sie einen aussagekräftigen Namen wie den Namen des Zielservers ein. Der Name darf maximal 32 alphanumerische Zeichen und Sonderzeichen umfassen.

---

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

---

2. Klicken Sie auf "OK".

Gültige Sonderzeichen

Zeichen	Beschreibung	Zeichen	Beschreibung
!	Ausrufezeichen	;	Strichpunkt
"	Doppeltes Anführungszeichen	=	Gleichheitszeichen
#	Raute	>	Größer-als-Zeichen
\$	Dollarzeichen	?	Fragezeichen
%	Prozentzeichen	@	At-Zeichen
&	Kaufmännisches Und	[	Linke eckige Klammer
(	Linke runde Klammer	\	Umgekehrter Schrägstrich
)	Rechte runde Klammer	]	Rechte eckige Klammer
*	Sternchen	^	Zirkumflexzeichen
+	Pluszeichen	_	Unterstrichzeichen
,	Komma	`	Graviszeichen
-	Bindestrich	{	Linke geschweifte Klammer
.	Punkt		Senkrechter Strich

Zeichen	Beschreibung	Zeichen	Beschreibung
/	Schrägstrich	}	Rechte geschweifte Klammer
<	Kleiner-als-Zeichen	~	Tilde
:	Doppelpunkt		

---

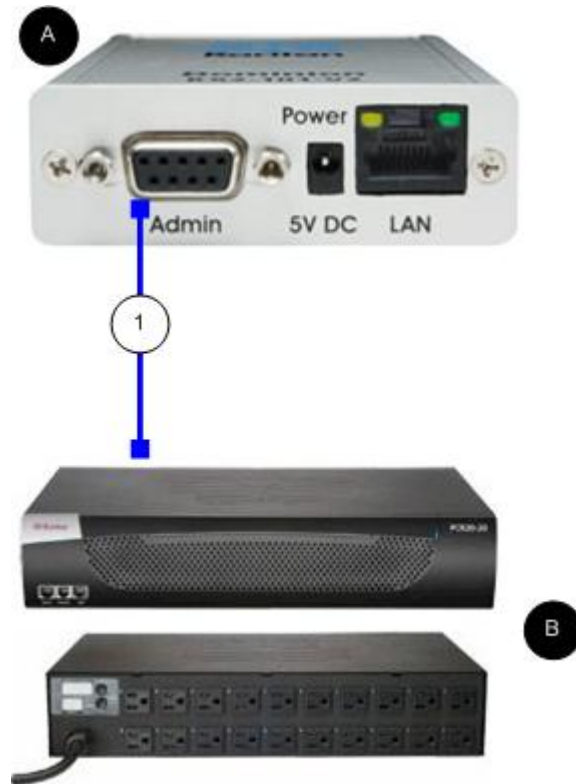
### Stromzufuhrsteuerung

KX II-101-V2 ermöglicht die Remote-Stromzufuhrsteuerung eines Zielservers. Für diese Funktion benötigen Sie einen Remote-Powerstrip von Raritan.

► **Führen Sie folgende Schritte aus, um das Feature für die Stromzufuhrsteuerung von KX II-101-V2 zu verwenden:**

- Schließen Sie den Powerstrip mit einem DKX2-101-V2-PDU-Kabel (nicht im Lieferumfang enthalten und kann über Ihren Händler oder über Raritan bezogen werden) an den Zielserver an. Siehe Anschließen des Powerstrips.
- Benennen des Powerstrips (nicht im Lieferumfang enthalten und kann über Ihren Händler oder über Raritan bezogen werden). Siehe **Benennen des Powerstrips (Seite "Port" für Powerstrips)** (auf Seite 149).
- Ordnen Sie einen Ausgang des Powerstrips dem Zielserver zu. Siehe **Verwalten von KVM-Zielservern (Seite "Port")** (auf Seite 145).
- Schalten Sie die Ausgänge des Powerstrips auf der Seite Powerstrip Device (Powerstrip-Gerät) ein und aus. Siehe Steuern eines Powerstrip-Geräts.

### Anschließen des Powerstrips



Diagrammschlüssel	
<b>A</b>	KX II-101-V2
<b>B</b>	Raritan-Powerstrip
<b>1</b>	DKX2-101-V2-PDU-Kabel (DB9-RJ45-Adapter) (nicht im Lieferumfang enthalten) von KX II-101-V2 zu einem Powerstrip von Raritan.

► **So verbinden Sie die KX II-101-V2-Einheit mit einem Raritan-Powerstrip:**

1. Schließen Sie das DKX2-101-V2-PDU-Kabel (DB9-RJ45-Adapter) an den Administrationsport des KX II-101-V2 an.
2. Schließen Sie das DKX2-101-V2-PDU-Kabel an den seriellen Port des Raritan-Powerstrips mithilfe eines Kabels der Kategorie 5 an.
3. Schließen Sie ein Netzkabel am Zielsystem und einem verfügbaren Powerstrip-Ausgang des Powerstrips an.

4. Stecken Sie den Stecker des Netzkabels in eine Steckdose.
5. Schalten Sie den Raritan-Powerstrip EIN.
6. Klicken Sie auf "Device Settings" > "Serial Port" (Geräteeinstellungen > Serieller Port), um die Seite "Serial Port" (Serieller Port) zu öffnen.
7. Aktivieren Sie das Optionsfeld "Power Strip Control" (Steuerung des Powerstrip) und klicken Sie auf "OK". Anschließend ist das Menü "Power" (Strom) auf der Remotekonsole verfügbar.

#### **Benennen des Powerstrips (Seite "Port" für Powerstrips)**

Wenn KX II-101-V2 mit einem Remote-Powerstrip von Raritan verbunden ist, wird der Port auf der Seite "Port" angezeigt. Sie können diesen Port dann über die Seite "Configuration" (Konfiguration) öffnen. Die Felder "Type" (Typ) und "Name" sind bereits ausgefüllt. Die folgenden Informationen werden für jeden Ausgang des Powerstrips angezeigt: Outlet Number (Ausgangsnummer), Name und Port Association (Portzuordnung).

Auf dieser Seite können Sie den Powerstrip und die Ausgänge benennen. Jeder Name darf maximal 32 alphanumerische Zeichen umfassen und Sonderzeichen enthalten.

---

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

---

#### **► So benennen Sie den Powerstrip (und seine Ausgänge):**

---

*Hinweis: CommandCenter Service Gateway erkennt Powerstrip-Namen 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). (Ausgangsnamen werden standardmäßig als "Outlet number" (Ausgangsnummer) angezeigt.)
3. Klicken Sie auf "OK".

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

- Klicken Sie auf "Cancel" (Abbrechen).

Number	Name	Port Association
1	Outlet 1	
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	

**Stromzuordnungen verwalten**

► **So stellen Sie Stromzuordnungen her (ordnen Powerstrip-Ausgänge KVM-Zielservern zu):**

---

*Hinweis: Wird ein Powerstrip einem Zielserver (Port) zugeordnet, wird der Ausgangsname durch den Port-Namen ersetzt. Sie können diesen Namen auf der Seite "Port 2" ändern.*

---

1. Wählen Sie einen Powerstrip in der Dropdown-Liste "Power Strip Name" (Powerstrip-Name) aus.
2. Wählen Sie in der Dropdown-Liste "Outlet Name" (Ausgangsname) den Ausgang aus.
3. Wiederholen Sie die Schritte 1 und 2 für alle gewünschten Stromzuordnungen.
4. Klicken Sie auf "OK". Eine Bestätigungsmeldung wird angezeigt.

► **So entfernen Sie eine Powerstrip-Zuordnung:**

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

► **So zeigen Sie die Konfiguration des Stromzufuhr-Ports an:**

- Wählen Sie "Home > Device Settings > Port Configuration > [power port name]" (Start > Geräteeinstellungen > Port-Konfiguration > [Name des Stromzufuhr-Ports]). Die Ausgangszuordnungen für den Powerstrip werden unter Outlets (Ausgänge) angezeigt.

► **So bearbeiten Sie die Konfiguration des Stromzufuhr-Ports:**

1. Ändern Sie den Namen des Stromzufuhr-Ports, indem Sie das Feld "Port Name" (Portname) bearbeiten.
2. Benennen Sie den Ausgang im zugehörigen Feld "Outlets Name" (Ausgangsnamen) um. Der Ausgangsname wird auf der Seite "Powerstrip Device" (Powerstrip-Gerät) angezeigt. Siehe Steuern eines Powerstrip-Geräts.
3. Ändern Sie die Ausgangszuordnung, indem Sie auf die Verknüpfung "Port Association" (Port-Zuordnung) neben dem Ausgangsnamen klicken und die Zuordnung auf der Seite "Port 1" bearbeiten.

### Steuern eines Powerstrip-Geräts

Steuern Sie das Powerstrip-Gerät über die Seite "Power Strip Device" (Powerstrip-Gerät). Auf dieser Seite können Sie jeden Ausgang des Powerstrips ein- und ausschalten.

► **So steuern Sie den mit KX II-101-V2 verbundenen Powerstrip:**

1. Wählen Sie "Home > Powerstrip" (Start > Powerstrip). Die Seite "Power Strip Device" (Powerstrip-Gerät) wird geöffnet.
2. Klicken Sie für jeden Ausgang auf die Schaltfläche "On" (Ein) oder "Off" (Aus), um ihn ein- oder auszuschalten.
3. Klicken Sie zum Bestätigen auf "OK".

---

*Hinweis: KX II-101-V2 kann nur einen Powerstrip steuern. Sie können keinen weiteren Powerstrip im Menü "Powerstrip" auswählen.*

---



---

## Analoger KVM-Switch

Sie können einen analogen KVM-Switch von Raritan so konfigurieren, dass er mit KX II-101-V2 kompatibel ist.

Die Kompatibilität von KX II-101-V2 wurde an den folgenden KVM-Switches überprüft:

- SwitchMan SW2, SW4 und SW8
- Master Console MX416 und MXU

Möglicherweise sind ähnliche Produkte von Raritan oder anderen Anbietern ebenfalls kompatibel; eine Unterstützung dieser Geräte kann jedoch nicht gewährleistet werden.

---

*Hinweis: Damit KX II-101-V2 mit analogen KVM-Switches kompatibel ist, müssen Sie die Switch-Zugriffstaste, mit deren Hilfe Sie zwischen den Zielen wechseln können, auf die Standardeinstellung der Rollen-Taste einstellen.*

---

### ► So konfigurieren Sie einen analogen KVM-Switch von Raritan:

1. Stellen Sie die Hostschnittstelle auf der Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten) auf PS/2. Wenn Sie dies nicht tun, wird Ihnen beim Konfigurieren eines analogen KVM-Switches der Fehler "PS/2 is needed to access the KVM Switch. Please enable PS/2 first!" (PS/2 wird für den Zugriff auf den KVM-Switch benötigt. Aktivieren Sie zuerst PS/2!) auf der Seite "Analog KVM Switch Configuration" (Konfiguration eines analogen KVM-Switches) angezeigt. Siehe **Tastatur/Maus einrichten**) (siehe **"Keyboard/Mouse Setup (Tastatur/Maus einrichten)"** auf Seite 131).
2. Klicken Sie auf "Device Settings > Analog KVM Switch" (Geräteeinstellungen > Analoger KVM-Switch). Die Seite "Analog KVM Switch Configuration" (Konfiguration eines analogen KVM-Switches) wird geöffnet.
3. Markieren Sie das Kontrollkästchen "Use Analog KVM Switch" (Analogen KVM-Switch verwenden), um die Felder zu aktivieren.
4. Wählen Sie den Switchtyp von Raritan in der Dropdownliste "Switch Type" (Switchtyp) aus:
  - Raritan MCC
  - Raritan MX
  - Raritan MXU
  - Raritan Switchman

5. Geben Sie im Feld "Port Count" (Portanzahl) die Anzahl der verfügbaren Ports basierend auf dem ausgewählten Switchtyp ein. Ändern Sie bei Bedarf die Port-Anzahl oder verwenden Sie die Standardanzahl. Die Standardeinstellungen bei der Switch-Auswahl bzw. die Standardanzahl der Ports sind:
  - Raritan MCC - 8
  - Raritan MX - 16
  - Raritan MX - 16
  - Raritan Switchman - 2
6. Aktivieren Sie das Kontrollkästchen "Security Setting" (Sicherheitseinstellung), um die Sicherheitseinstellung zu aktivieren.
7. Geben Sie das Passwort für den Zugriff auf den KVM-Switch ein.
8. Klicken Sie auf "OK", um den analogen KVM-Switch zu konfigurieren.

► **So stellen Sie die Standardeinstellungen für den analogen KVM-Switch wieder her:**

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

#### Analog KVM Switch Configuration

**Note: Changing one of the following options will close all kvm and virtual media sessions.**

Use Analog KVM Switch

Switch Type

Raritan MCC ▼

Port Count

8

Security Setting

Password

OK

Reset To Defaults

Cancel

---

## Zurücksetzen des KX II-101-V2 mithilfe der Taste "Reset" (Zurücksetzen)

Auf der Oberseite des Geräts befindet sich die Taste "Reset" (Zurücksetzen). Sie ist etwas zurückgesetzt, damit sie nicht unbeabsichtigt gedrückt wird (Sie benötigen einen spitzen Gegenstand, um die Taste zu betätigen).

Welche Maßnahmen ergriffen werden, wenn die Taste "Reset" (Zurücksetzen) gedrückt wird, legen Sie über die grafische Benutzeroberfläche fest. Siehe **Encryption & Share (Verschlüsselung und Freigabe)**.

► **So setzen Sie das Gerät zurück:**

1. Schalten Sie die KX II-101-V2-Einheit aus.
2. Verwenden Sie einen spitzen Gegenstand, und halten Sie die Taste zum Zurücksetzen damit gedrückt.
3. Halten Sie die Taste zum Zurücksetzen gedrückt und schalten Sie gleichzeitig das KX II-101-V2-Gerät wieder ein.
4. Halten Sie die Taste "Reset" (Zurücksetzen) weitere zehn Sekunden gedrückt.
5. Lassen Sie die Taste "Reset" (Zurücksetzen) los und KX II-101-V2 wird neu gestartet. Dies dauert für gewöhnlich drei Minuten.

---

*Hinweis: Wenn KX II-101-V2 beim Zurücksetzen auf die standardmäßigen Werkseinstellungen zurückgesetzt wird, werden ebenfalls die IP-Adresse, der Benutzername und weitere Optionen umgestellt.*

---



---

## Ändern der Standardeinstellung für die GUI-Sprache

Die grafische Benutzeroberfläche (GUI) von KX II-101-V2 unterstützt die folgenden lokalisierten Sprachen:

- Japanese (Japanisch)
- Simplified Chinese (Vereinfachtes Chinesisch)
- Traditional Chinese (Traditionelles Chinesisch)

► **So ändern Sie die GUI-Sprache:**

1. Wählen Sie "Device Settings" (Geräteeinstellungen) > "Language" (Sprache). Die Seite "Language Settings" (Spracheinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdownliste "Language" (Sprache) die Sprache für die GUI aus.
3. Klicken Sie auf "Apply" (Übernehmen). Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen), um die Sprache wieder auf "English" (Englisch) zurückzusetzen.

---

*Hinweis: Sobald Sie eine neue Sprache übernehmen, wird die Online-Hilfe ebenfalls Ihrer Sprachauswahl entsprechend lokalisiert.*

---

## Kapitel 7 USB-Verbindungen verwalten

### In diesem Kapitel

Überblick.....	157
USB-Verbindungseinstellungen .....	158
Erweiterte USB-Verbindungseinstellungen .....	159

---

## Überblick

Um die Kompatibilität des KX II-101-V2 auf verschiedene KVM-Zielserver auszuweiten, bietet Raritan eine benutzerdefinierte Auswahl an USB-Konfigurationsprofiloptionen in Echtzeit für die Implementierung auf vielen Betriebssystemen und Servern auf BIOS-Ebene an.

Die standardmäßigen USB-Verbindungseinstellungen erfüllt die Anforderungen der großen Mehrheit der bereitgestellten KVM-Zielserverkonfigurationen. Weitere Konfigurationselemente stehen zur Verfügung, um die speziellen Anforderungen anderer häufig bereitgestellten Serverkonfigurationen (z. B. Linux® und Mac OS X) zu erfüllen. Außerdem stehen einige Konfigurationselemente (festgelegt nach Plattformname und BIOS-Revision) zur Verfügung, die erstellt wurden, um die Kompatibilität der Funktion der virtuellen Medien mit dem Zielsystem zu verbessern (wenn z. B. auf BIOS-Ebene gearbeitet wird).

USB-Profile werden unter "Device Settings" > "Port Configuration" > "Port" (Geräteeinstellungen > Portkonfiguration > Port) auf der Remotekonsole des KX II-101-V2 konfiguriert. Ein Geräteadministrator kann den Port mit den Profilen konfigurieren, die den Anforderungen des Benutzers und der Zielsystemkonfiguration am besten entsprechen.

**WARNUNG:** Es ist möglich, dass basierend auf Ihrer Auswahl im Bereich "Advanced USB Connection Settings" (Erweiterte Einstellungen der USB-Verbindung) Konfigurationsprobleme zwischen KX II-101-V2 und dem Zielsystem auftreten.

Aufgrunddessen empfiehlt Raritan ausdrücklich, dass Sie sich unter dem aktuellsten Hyperlink "User Defined KX II-101-V2 USB Profile Configuration Table" (Benutzerdefinierte Konfigurationstabelle für KX II-101-V2-USB-Profile) diesbezüglich informieren. Die zum Zeitpunkt dieser Veröffentlichung verfügbaren Informationen können unter Bekannte USB-Profile nachgelesen werden.

Ein Benutzer, der eine Verbindung zu einem KVM-Zielsystem herstellt, wählt zwischen diesen USB-Verbindungseinstellungen aus, je nach Betriebsstatus des KVM-Zielsystems. Wenn beispielsweise der Server ausgeführt wird und der Benutzer das Windows®-Betriebssystem verwenden möchte, ist es sinnvoll, die Standardeinstellungen zu verwenden. Wenn der Benutzer jedoch die Einstellungen im BIOS-Menü ändern oder von einem virtuellen Medienlaufwerk einen Neustart ausführen möchte, kann, je nach Zielsystemmodell, eine andere Einstellung für die USB-Verbindung eher geeignet sein.

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

## USB-Verbindungseinstellungen

► **So legen Sie die USB-Verbindungen für den Zielserver fest:**

1. Klicken Sie auf "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration), um die Seite "Port Configuration" (Portkonfiguration) zu öffnen. Klicken Sie auf den Port, den Sie konfigurieren möchten.
2. Klicken Sie auf "USB Connection Settings" (USB-Verbindungseinstellungen), um den Bereich "USB Connection Settings" (USB-Verbindungseinstellungen) zu erweitern.
3. Wählen Sie die USB-Verbindungseinstellungen aus, die Sie nutzen möchten:
  - Enable Absolute Mouse (Mausmodus "Absolut" aktivieren) – Trifft nur zu, wenn der USB-Anschluss eine aktive Tastatur/Maus-Schnittstelle ist
  - "Use Full Speed" (Volle Geschwindigkeit nutzen) – Hilfreich bei einem BIOS, das sich nicht an Hochgeschwindigkeits-USB-Geräte anpassen kann
  - "Absolute mouse scaling for MAC server" (Absolute Mausskalierung für MAC-Server) – Trifft nur zu, wenn der USB-Anschluss eine aktive Tastatur/Maus-Schnittstelle ist
  - USB Sun Keyboard support (Sun USB-Tastaturunterstützung) – Trifft nur zu, wenn der USB-Anschluss eine aktive Tastatur/Maus-Schnittstelle ist
4. Klicken Sie auf "OK".

### ▼ USB Connection Settings

- Enable Absolute Mouse**  
(applies only if USB is active Keyboard/Mouse Interface)
- Use Full Speed - Useful for BIOS**  
that cannot handle High Speed USB devices
- Absolute mouse scaling for MAC server**  
(applies only if USB is active Keyboard/Mouse Interface)
- USB SUN Keyboard support**  
(applies only if USB is active Keyboard/Mouse Interface)

### ► Advanced USB Connection Settings

---

## Erweiterte USB-Verbindungseinstellungen

WARNUNG: Es ist möglich, dass basierend auf Ihrer Auswahl im Bereich "Advanced USB Connection Settings" (Erweiterte Einstellungen der USB-Verbindung) Konfigurationsprobleme zwischen KX II-101-V2 und dem Zielservers auftreten. Daher empfiehlt Raritan ausdrücklich, dass Sie sich unter Bekannte USB-Profilen oder unter der Tabelle "User Defined KX II-101-V2 USB Profiles Connection Configuration" (Benutzerdefinierte Konfigurationstabelle für KX II-101-V2-USB-Profilen) informieren, die Sie auf der Seite "Port" durch Klicken auf den Bereich "Advanced USB Connection Settings" (Erweiterte USB-Verbindungseinstellungen) aufrufen können.

► **So legen Sie die USB-Verbindungen für den Zielservers fest:**

1. Klicken Sie auf "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration), um die Seite "Port Configuration" (Portkonfiguration) zu öffnen. Klicken Sie auf den Port, den Sie konfigurieren möchten.
2. Klicken Sie auf "Advanced USB Connection Settings" (Erweiterte USB-Verbindungseinstellungen), um den Bereich zu erweitern.
3. Klicken Sie auf die Tabelle "User Defined KX II-101 USB Profile Configuration" (Benutzerdefinierte KX II-101 USB-Profilkonfiguration), um auf die empfohlenen Konfigurationen zuzugreifen und diese auf den Bereich "Advanced USB Connection Settings" (Erweiterte USB-Verbindungseinstellungen) anzuwenden.
4. Konfigurieren Sie nach Bedarf die folgenden Komponenten:
  - a. Virtual Media Interface #1 Type (Virtuelle Medienschnittstelle Typ 1)
  - b. Aktivieren Sie das Kontrollkästchen "Remove Unused VM Interface #1 From Device Configuration" (Unbenutzte Schnittstelle 1 von der Gerätekonfiguration entfernen), um die angegebene VM-Typ-Schnittstelle (für #1) zu entfernen.
  - c. Virtual Media Interface #2 Type (Virtuelle Medienschnittstelle Typ 2)
  - d. Aktivieren Sie das Kontrollkästchen "Remove Unused VM Interface #2 From Device Configuration" (Unbenutzte Schnittstelle 2 von der Gerätekonfiguration entfernen), um die angegebene VM-Typ-Schnittstelle (für #2) zu entfernen.



5. Klicken Sie auf "OK".

▼ Advanced USB Connection Settings

**IMPORTANT: Please follow the reference guide provided at this link.**

User Defined KX II-101 USB Profile Configuration Table

Virtual Media Interface #1 Type

CD-ROM ▼

Remove Unused VM Interface #1 From Device Configuration  
(useful for BIOS that cannot accommodate empty drives)

Virtual Media Interface #2 Type

Removable Disk ▼

Remove Unused VM Interface #2 From Device Configuration  
(useful for BIOS that cannot accommodate empty drives)

# Kapitel 8      Sicherheitsverwaltung

## In diesem Kapitel

Security Settings (Sicherheitseinstellungen) .....	161
Konfigurieren der IP-Zugriffssteuerung .....	173
SSL-Zertifikate .....	176
Sicherheitsmeldung .....	180

---

## Security Settings (Sicherheitseinstellungen)

Auf der Seite "Security Settings" (Sicherheitseinstellungen) können Sie Anmeldebeschränkungen angeben, Benutzer blockieren, Kennwortregeln festlegen und Daten verschlüsseln und freigeben.

### ► So konfigurieren Sie die Sicherheitseinstellungen:

1. Wählen Sie **Security > Security Settings** (Sicherheit > Sicherheitseinstellungen). Die Seite **Security Settings** (Sicherheitseinstellungen) wird angezeigt.
2. Aktualisieren Sie ggf. die Einstellungen unter **Login Limitations (Anmeldebeschränkungen)** (siehe "**Anmeldebeschränkungen**" auf Seite 161).
3. Aktualisieren Sie ggf. die Einstellungen unter **Strong Passwords (Sichere Kennwörter)** (auf Seite 163).
4. Aktualisieren Sie ggf. die Einstellungen für **User Blocking (Benutzersperrung)** (auf Seite 165).
5. Aktualisieren Sie ggf. die Einstellungen unter Encryption & Share (Verschlüsselung und Freigabe).
6. Klicken Sie auf "OK".

### ► So stellen Sie die Standardwerte wieder her:

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

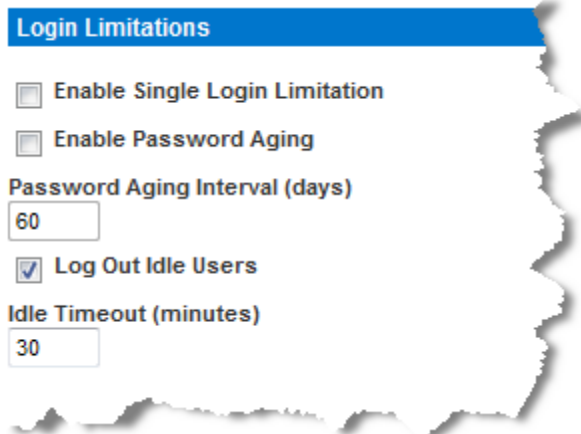
---

## Anmeldebeschränkungen

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

Beschränkung	Beschreibung
"Enable single login limitation"	Wenn Sie dieses Kontrollkästchen aktivieren, ist pro Benutzername immer nur eine Anmeldung

<b>Beschränkung</b>	<b>Beschreibung</b>
(Beschränkung für Einzelanmeldung aktivieren)	zulässig. Ist es dagegen deaktiviert, kann eine Benutzername-/Kennwortkombination von mehreren Client-Workstations gleichzeitig verwendet werden, um eine Verbindung mit dem Gerät herzustellen.
"Enable Password Aging" (Erneuerung des Kennworts aktivieren)	<p>Wenn Sie dieses Kontrollkästchen aktivieren, müssen alle Benutzer ihr Kennwort abhängig von der Anzahl der Tage, die Sie im Feld "Password Aging Interval" (Intervall für Kennworterneuerung) eingegeben haben, regelmäßig ändern.</p> <p>Dieses Feld ist aktiv und erforderlich, wenn Sie das Kontrollkästchen "Enable Password Aging" (Erneuerung des Kennworts aktivieren) aktiviert haben. Geben Sie den Zeitraum in Tagen an, nach dessen Ablauf ein Kennwort geändert werden muss. Der Standardwert ist 60 Tage.</p>
"Log out idle users, After (1-365 minutes)" (Inaktive Benutzer abmelden, Nach (1-365 Minuten))	<p>Aktivieren Sie das Kontrollkästchen "Log off idle users" (Inaktive Benutzer abmelden), um die Verbindung von Benutzern automatisch zu trennen, wenn der im Feld "After (1-365 minutes)" [Nach (1-365 Minuten)] angegebene Zeitraum abgelaufen ist. Wenn keine Tastatur- oder Mausaktivitäten stattfinden, werden alle Sitzungen und Ressourcen abgemeldet. Für virtuelle Mediensitzungen gibt es hingegen kein Zeitlimit.</p> <p>Das Feld "After" (Nach) dient zum Festlegen der Zeitspanne (in Minuten), nach der ein inaktiver Benutzer abgemeldet wird. Dieses Feld ist aktiv, wenn Sie das Kontrollkästchen "Log Out Idle Users" (Inaktive Benutzer abmelden) aktiviert haben. Als Feldwert können bis zu 365 Minuten eingegeben werden.</p>



### Strong Passwords (Sichere Kennwörter)

Sichere Kennwörter sorgen für eine sicherere lokale Authentifizierung des Systems. Im Bereich "Strong Passwords" (Sichere Kennwörter) können Sie das Format gültiger lokaler KX II-101-V2-Kennwörter wie Mindest- und Höchstlänge, erforderliche Zeichen und Aufbewahrung des Kennwortverlaufs festlegen.

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

Wenn Sie diese Option aktivieren, gelten die Regeln für sichere Kennwörter. Benutzer, deren Kennwörter nicht den Kriterien für sichere Kennwörter entsprechen, werden bei der nächsten Anmeldung automatisch aufgefordert, ihr Kennwort zu ändern. Ist das Kontrollkästchen deaktiviert, gilt nur die Standardformatvalidierung. Bei aktiviertem Kontrollkästchen sind die folgenden Felder aktiv und erforderlich:

Feld	Beschreibung
Minimum length of strong password (Mindestlänge des sicheren Kennworts)	Kennwörter müssen mindestens 8 Zeichen umfassen. Die Standardeinstellung gibt 8 Zeichen vor, aber der Administrator kann das Minimum auf 63 Zeichen erweitern.
Maximum length of strong password (Höchstlänge des sicheren Kennworts)	Die standardmäßige Mindestlänge eines Kennworts beträgt 8 Zeichen, aber der Administrator kann die Höchstlänge auf 16 Zeichen einstellen. Die Höchstlänge sicherer Kennwörter beträgt 63 Zeichen.

Feld	Beschreibung
Enforce at least one lower case character (Mindestens einen Kleinbuchstaben erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Kleinbuchstaben enthalten.
Enforce at least one upper case character (Mindestens einen Großbuchstaben erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Großbuchstaben enthalten.
Enforce at least one numeric character (Mindestens eine Ziffer erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens eine Ziffer enthalten.
Enforce at least one printable special character (Mindestens ein druckbares Sonderzeichen erzwingen)	Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens ein (druckbares) Sonderzeichen enthalten.
Number of restricted passwords based on history (Anzahl unzulässiger Kennwörter basierend auf Verlauf)	Dieses Feld bezieht sich auf die Verlaufstiefe, d. h. die Anzahl vorheriger Kennwörter, die nicht wiederholt werden dürfen. Ein Bereich zwischen 1 und 12 ist möglich, der Standardwert liegt bei 5.

### Strong Passwords

Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history

5

---

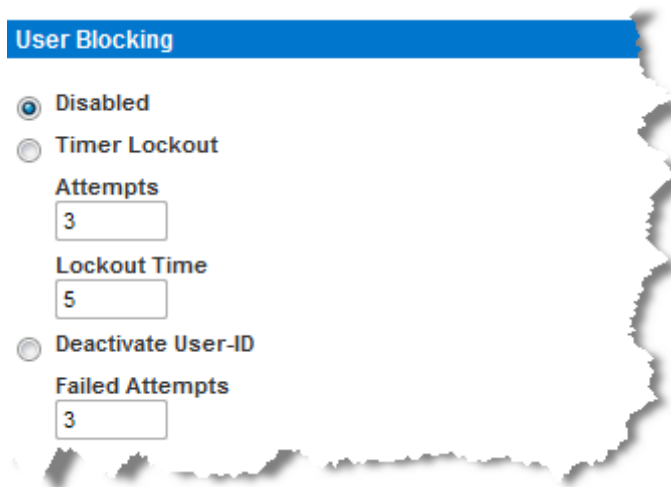
**User Blocking (Benutzersperrung)**

Mithilfe der Optionen unter "User Blocking" (Benutzersperrung) geben Sie die Kriterien an, anhand derer Benutzer nach der festgelegten Zahl von Anmeldefehlversuchen am Zugriff auf das System gehindert werden.

Die drei Optionen schließen sich gegenseitig aus.

<b>Option</b>	<b>Beschreibung</b>
"Disabled" (Deaktiviert)	Dies ist die Standardoption. Benutzer werden unabhängig von der Anzahl fehlgeschlagener Anmeldeversuche nicht blockiert.

Option	Beschreibung
<p>"Timer Lockout" (Zeitliche Sperre)</p>	<p>Benutzern wird der Zugriff auf das System für den festgelegten Zeitraum verweigert, nachdem sie eine bestimmte Anzahl von Anmeldefehlversuchen überschritten haben. Bei dieser Option stehen die folgenden Felder zur Verfügung:</p> <ul style="list-style-type: none"> <li>▪ "Attempts" (Versuche) – Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche ein, nach der ein Benutzer gesperrt wird. Ein Bereich zwischen 1 und 10 ist möglich, der Standardwert liegt bei 3 Versuchen.</li> <li>▪ "Lockout Time" (Dauer der Sperre) – Geben Sie die Zeitspanne ein, für die der Benutzer gesperrt wird. Ein Bereich zwischen 1 und 1.440 Minuten ist möglich, der Standardwert liegt bei 5 Minuten.</li> </ul> <hr/> <p><i>Hinweis: Administratoren sind von einer zeitlichen Sperre ausgenommen.</i></p>
<p>"Deactivate User-ID" (Benutzer-ID deaktivieren)</p>	<p>Diese Option legt fest, dass dem Benutzer nach der Anzahl der im Feld "Failed Attempts" (Fehlversuche) angegebenen Anmeldefehlversuche der Zugriff auf das System verweigert wird.</p> <ul style="list-style-type: none"> <li>▪ "Failed Attempts" (Fehlversuche) – Geben Sie die Anzahl der Anmeldefehlversuche ein, nach der die Benutzer-ID eines Benutzers deaktiviert wird. Dieses Feld steht zur Verfügung, wenn Sie die Option "Deactivate User-ID" (Benutzer-ID deaktivieren) wählen. Der gültige Bereich liegt zwischen 1 und 10.</li> </ul> <p>Wenn eine Benutzer-ID nach der angegebenen Anzahl der Anmeldefehlversuche deaktiviert wird, muss der Administrator das Benutzerkennwort ändern und das Benutzerkonto wieder aktivieren, indem er auf der Seite "User" (Benutzer) das Kontrollkästchen "Active" (Aktiv) aktiviert.</p>



### Encryption & Share (Verschlüsselung und Freigabe)

Mithilfe der Einstellungen unter "Encryption & Share" (Verschlüsselung und Freigabe) können Sie die Art der Verschlüsselung, PC- und VM-Freigabemodi sowie die Art der Zurücksetzung festlegen, wenn die Taste "Reset" (Zurücksetzen) an der KX II-101-V2-Einheit gedrückt wird.

**WARNUNG:** Wenn Sie einen Verschlüsselungsmodus auswählen, der von Ihrem Browser nicht unterstützt wird, können Sie von Ihrem Browser aus nicht auf KX II-101-V2 zugreifen.

► **So konfigurieren Sie die Verschlüsselung und Freigabe:**

1. Wählen Sie eine Option aus der Dropdownliste "Encryption Mode" (Verschlüsselungsmodus) aus.

Wenn Sie einen Verschlüsselungsmodus ausgewählt haben, wird eine Warnung angezeigt, dass Sie keine Verbindung zu KX II-101-V2 mehr herstellen können, falls Ihr Browser den gewählten Modus nicht unterstützt. Die Warnung lautet "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the KX II-101-V2" (Wenn Sie den Verschlüsselungsmodus festlegen, stellen Sie sicher, dass Ihr Browser diesen unterstützt, ansonsten können Sie keine Verbindung zu KX II-101-V2 herstellen).

Verschlüsselungsmodus	Beschreibung
Automatisch	Dies ist die empfohlene Option. KX II-101-V2 verwendet automatisch das höchstmögliche Verschlüsselungsniveau.  Sie <i>müssen</i> "Auto" (Automatisch) auswählen,



Verschlüsselungsmodus	Beschreibung
	damit Gerät und Client erfolgreich die verwendeten FIPS-konformen Algorithmen verarbeiten können.
RC4	<p>Sichert Benutzernamen, Kennwörter und KVM-Daten einschließlich Videoübertragungen mithilfe der Verschlüsselungsmethode RSA RC4. Dies ist ein 128-Bit-SSL-Protokoll (Secure Sockets Layer), das während der Anfangsverbindungsauthentifizierung einen privaten Kommunikations-Channel zwischen dem KX II-101-V2-Gerät und dem Remote-PC bereitstellt.</p> <p>Wenn Sie den Modus FIPS 140-2 aktivieren und RC4 ausgewählt wurde, erhalten Sie eine Fehlermeldung. Im Modus FIPS 140-2 ist RC4 nicht verfügbar.</p>
AES-128	<p>Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 128 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option (AES-128) darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter <b>Prüfen Ihres Browsers auf AES-Verschlüsselung</b> (auf Seite 171).</p>
AES-256	<p>Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 256 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option (AES-256) darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter <b>Prüfen Ihres Browsers auf AES-Verschlüsselung</b> (auf Seite 171).</p>

*Hinweis: Der MPC verwendet immer das höchste Verschlüsselungsniveau und entspricht der Einstellung unter "Encryption Mode" (Verschlüsselungsmodus), wenn diese nicht auf "Auto" eingestellt ist.*

---

*Hinweis: Wenn Sie Windows XP® mit Service Pack 2 verwenden, kann der Internet Explorer® 7 keine Remoteverbindung zu KX II-101-V2 herstellen, wenn die AES-128-Verschlüsselung verwendet wird.*

---

2. Apply Encryption Mode to KVM and Virtual Media (Verschlüsselungsmodus auf KVM und virtuelle Medien anwenden): Wenn Sie dieses Kontrollkästchen aktivieren, wird der gewählte Verschlüsselungsmodus auf KVM und virtuelle Medien angewendet. Nach der Authentifizierung werden die KVM- und virtuellen Mediendaten ebenfalls mit der 128-Bit-Verschlüsselung übertragen.
3. Für das Arbeiten in Regierungs- und anderen Hochsicherheitsumgebungen muss der Modus FIPS 140-2 durch Aktivieren des Kontrollkästchens "Enable FIPS 140-2" (Aktivieren von FIPS 140-2) ausgewählt werden. Weitere Informationen zur Aktivierung von FIPS 140-2 finden Sie unter **Aktivieren von FIPS 140-2** (auf Seite 171).
4. Modus "PC Share" (PC-Freigabe) – Bestimmt den globalen gleichzeitigen KVM-Remotezugriff und ermöglicht bis zu acht Remotebenutzern die gleichzeitige Anmeldung bei einer KX II-101-V2-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 Zielservers ist jeweils nur für einen Benutzer exklusiv zugänglich.
  - PC-Share (PC-Freigabe) – Bis zu acht Benutzer (Administratoren oder Nicht-Administratoren) können gleichzeitig auf KVM-Zielservers zugreifen. Jeder Remotebenutzer besitzt dieselbe Kontrolle über Tastatur und Maus. Beachten Sie jedoch, dass eine ungleichmäßige Steuerung auftritt, wenn ein Benutzer seine Tastatur- bzw. Mauseingabe nicht unterbricht.
5. Wählen Sie bei Bedarf den Modus "VM Share" (VM-Freigabe) aus. Diese Option steht nur zur Verfügung, wenn der PC-Freigabemodus aktiviert wurde. Wenn dieses Kontrollkästchen aktiviert ist, werden virtuelle Medien für mehrere Benutzer freigegeben, d. h. diese können gemeinsam auf dieselbe virtuelle Mediensitzung zugreifen. Standardmäßig ist dieses Kontrollkästchen deaktiviert.
6. Wählen Sie bei Bedarf den Modus "Local Device Reset" (Lokales Gerät zurücksetzen) aus. Diese Option legt fest, welche Maßnahmen ergriffen werden, wenn die Taste zum Zurücksetzen der Hardware auf der Rückseite des Geräts gedrückt wird. Weitere Informationen finden Sie unter **Zurücksetzen von KX II-101-V2 mithilfe der Taste "Reset" (Zurücksetzen)** (siehe "**Zurücksetzen des KX II-101-V2 mithilfe der Taste "Reset" (Zurücksetzen)**" auf Seite 154). Wählen Sie eine der folgenden Optionen aus:

<b>Modus zum Zurücksetzen eines lokalen Geräts</b>	<b>Beschreibung</b>
Enable Local Factory Reset (Lokale Werkrücksetzung aktivieren, Standardeinstellung)	Setzt das KX II-101-V2-Gerät auf die werksseitigen Standardeinstellungen zurück.
Enable Local Admin Password Reset (Lokale Administrator-Kennwortrücksetzung aktivieren)	Setzt nur das Kennwort des lokalen Administrators zurück. Das Kennwort wird auf "raritan" zurückgesetzt.
Disable All Local Resets (Alle lokalen Rücksetzungen deaktivieren)	Es wird keine Rücksetzungsmaßnahme ergriffen.

### Prüfen Ihres Browsers auf AES-Verschlüsselung

KX II-101-V2 unterstützt AES-256. 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.

---

*Hinweis: Die AES-128-Bit- oder -256-Bit-Verschlüsselung wird vom Internet Explorer® 6 nicht unterstützt.*

---

Voraussetzungen und unterstützte Konfigurationen für die AES-256-Bit-Verschlüsselung

Die AES-256-Bit-Verschlüsselung wird nur von folgenden Webbrowsern unterstützt:

- Firefox® 2.0.0.x und 3.0 x (und höher)
- Internet Explorer 7 und 8

Für die AES-256-Bit-Verschlüsselung müssen außerdem die Sicherheitsrichtliniendateien für eine unbeschränkte Schlüssellänge der Java™ Cryptography Extension® (JCE®) installiert werden.

Diese sogenannten "Unlimited Strength Jurisdiction Policy Files" der verschiedenen JRE™-Versionen finden Sie unter folgendem Link im Bereich "Other Downloads" (Weitere Downloads):

- JRE1.7 - [javase/downloads/jce-7-download-432124.html](http://javase/downloads/jce-7-download-432124.html)

---

### Aktivieren von FIPS 140-2

Für das Arbeiten in Regierungs- und anderen Hochsicherheitsumgebungen ist es möglicherweise erforderlich, den Modus FIPS 140-2 zu aktivieren. KX II-101-V2 verfügt über ein integriertes FIPS 140-2-validiertes kryptografisches Modul, das gemäß Abschnitt G.5 der FIPS 140-2 Implementation Guidance auf einer Linux®-Plattform ausgeführt wird. Nach der Aktivierung dieses Moduls muss der private Schlüssel, der zur Generierung des SSL-Zertifikats verwendet wird, intern erzeugt werden. Dieser kann nicht heruntergeladen oder exportiert werden.

► **So aktivieren Sie FIPS 140-2:**

1. Öffnen Sie die Seite "Security Settings" (Sicherheitseinstellungen).

2. Aktivieren Sie den FIPS 140-2-Modus, indem Sie im Abschnitt "Encryption & Share" (Verschlüsselung & Freigabe) der Seite "Security Settings" (Sicherheitseinstellungen) das Kontrollkästchen "Enable FIPS 140-2" (Aktivieren von FIPS 140-2) aktivieren. Sie nutzen FIPS 140-2-zugelassene Algorithmen für die externe Kommunikation, sobald Sie sich im FIPS 140-2-Modus befinden. Das kryptografische FIPS-Modul wird für die Verschlüsselung von KVM-Sitzungsdaten verwendet. Dabei handelt es sich um Video-, Tastatur-, Maus- und Smart Card-Daten sowie um die Daten von virtuellen Medien.
3. Führen Sie einen Neustart der entsprechenden KX II-101-V2-Einheit durch. <erforderlich>

Sobald der FIPS-Modus aktiviert ist, wird im Abschnitt "Device Information" (Geräteinformationen) im linken Fenster der Bildschirmanzeige "FIPS Mode: Enabled" (FIPS-Modus aktiviert) angezeigt.

Zusätzliche Sicherheit bietet das Erzeugen einer neuen Zertifikatsregistrierungsanforderung, nachdem der FIPS-Modus aktiviert wurde. Diese wird mithilfe des erforderlichen Schlüsselcodes erzeugt. Laden Sie das Zertifikat hoch, nachdem es signiert wurde, oder erzeugen Sie ein selbstsigniertes Zertifikat. Der SSL-Zertifikatsstatus wird von "Not FIPS Mode Compliant" (Nicht FIPS-konform) zu "FIPS Mode Compliant" (FIPS-konform) aktualisiert.

Ist der FIPS-Modus aktiviert, können keine Schlüsseldateien herunter- oder hochgeladen werden. Die aktuell erzeugte CSR wird der Schlüsseldatei intern zugeordnet. Das SSL-Zertifikat der CA und der zugehörige private Schlüssel sind nicht in der vollständigen Wiederherstellung der gesicherten Datei enthalten. Der Schlüssel kann nicht von KX II-101-V2 exportiert werden.

#### **Anforderungen für die Unterstützung von FIPS 140-2**

KX II-101-V2 unterstützt FIPS 140-20-zugelassene Verschlüsselungsalgorithmen. Dadurch können SSL-Server und Client erfolgreich die für die verschlüsselte Sitzung verwendete Verschlüsselungsfolge verarbeiten, sobald ein Client exklusiv für den Modus FIPS 140-2 konfiguriert ist.

Im Folgenden finden Sie Hinweise zur Verwendung von FIPS 140-2 mit KX II-101-V2:

#### **KX II-101-V2**

- Nehmen Sie auf der Seite Security Settings (Sicherheitseinstellungen) für "Encryption & Share" (Verschlüsselung & Freigabe) die Einstellung auf "Auto" (Automatisch) vor. Siehe Encryption & Share (Verschlüsselung und Freigabe).

#### Microsoft-Client

- Am Client-Computer und im Internet Explorer muss "FIPS 140-2" aktiviert sein.

#### ► So aktivieren Sie "FIPS 140-2" auf einem Windows-Client:

1. Wählen Sie "Systemsteuerung" > "Verwaltung" > "Lokale Sicherheitsrichtlinie" aus, um das Dialogfeld "Lokale Sicherheitseinstellungen" zu öffnen.
2. Wählen Sie in der Navigationsstruktur "Lokale Richtlinien" > "Sicherheitsoptionen" aus.
3. Aktivieren Sie "Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signierung verwenden".
4. Starten Sie den Client-Computer neu.

#### ► So aktivieren Sie "FIPS 140-2" im Internet Explorer:

1. Wählen Sie im Internet Explorer "Extras" > "Internetoptionen", und klicken Sie auf die Registerkarte "Erweitert".
2. Aktivieren Sie das Kontrollkästchen "TLS 1.0 verwenden".
3. Starten Sie den Browser neu.

---

## Konfigurieren der IP-Zugriffssteuerung

Mithilfe der IP-Zugriffssteuerung können Sie den Zugriff auf KX II-101-V2 steuern. Durch das Einrichten einer globalen Zugriffssteuerungsliste (Access Control List, ACL) stellen Sie sicher, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet.

---

**Wichtig: Die IP-Adresse "127.0.0.1" wird vom lokalen Port der KX II-101-V2-Einheit 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 der KX II-101-V2-Einheit zugreifen.**

---

#### ► So verwenden Sie die IP-Zugriffssteuerung:

1. Öffnen Sie die Seite "IP Access Control" (IP-Zugriffssteuerung), indem Sie "Security" > "IP Access Control" (Sicherheit > IP-Zugriffssteuerung) auswählen. Die Seite "IP Access Control" (IP-Zugriffssteuerung) wird angezeigt.

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 KX II-101-V2-Gerät zugreifen.
  - Drop (Ablehnen) – Diesen IP-Adressen wird der Zugriff auf das KX II-101-V2-Gerät verweigert.

► **So fügen Sie Regeln hinzu:**

1. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.

---

*Hinweis: Die IP-Adresse sollte unter Verwendung der CIDR-Notation (Classless Inter-Domain Routing) eingegeben werden. Eine CIDR-Notation besteht aus zwei Komponenten. Der wichtigste Bestandteil ist die Netzwerkadresse, mit deren Hilfe ein ganzes Netzwerk oder Subnetz identifiziert wird. Die am wenigsten wichtige Komponente ist der Identifier (Bezeichner). Die Präfixlänge nach dem "/"-Zeichen identifiziert die Länge der Subnetzmaske.*

---

2. Wählen Sie in der Dropdown-Liste "Policy" (Richtlinie) eine Richtlinie aus.
3. Klicken Sie auf "Append" (Anfügen). Die Regel wird am Ende der Liste hinzugefügt.

► **So fügen Sie eine Regel ein:**

1. Geben Sie eine Regelnummer ein (#). Diese ist für den Befehl "Insert" (Einfügen) erforderlich.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.
3. Wählen Sie in der Dropdown-Liste "Policy" (Richtlinie) eine Richtlinie aus.
4. Klicken Sie auf "Insert" (Einfügen). Wenn die eingegebene Regelnummer einer bereits vorhandenen entspricht, wird die neue Regel vor der vorhandenen Regel eingefügt, und alle Regeln werden um eine Position nach unten verschoben.

---

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

---

► **So ersetzen Sie eine Regel:**

1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.
3. Wählen Sie in der Dropdown-Liste "Policy" (Richtlinie) eine Richtlinie aus.
4. Klicken Sie auf "Replace" (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

► **So löschen Sie eine Regel:**

1. Geben Sie die zu löschende Regelnummer an.
2. Klicken Sie auf "Delete" (Löschen).
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf "OK".

---

[Home](#) > [Security](#) > [IP Access Control](#)

---

### IP Access Control

Enable IP Access Control

Default Policy

ACCEPT ▾

Rule #	IPv4/Mask or IPv6/Prefix Length	Policy
--------	---------------------------------	--------

<input type="text"/>	<input type="text"/>	ACCEPT ▾
----------------------	----------------------	----------

Append

Insert

Replace

Delete

OK

Reset To Defaults

Cancel



Um nur den Zugriff auf eine IP-Adresse zuzulassen und alle anderen zu blockieren, ändern Sie die Subnetzmaske für die Regel zu /32. Wenn Sie z. B. sämtliche Zugriffe auf das Subnetz '192.168.51' verhindern möchten und für "Default Policy" (Standardrichtlinie) "Accept" (Akzeptieren) angegeben ist, würden Sie mit einer auf 192.168.51.00/24 eingestellten IP/MASK und einer auf "DROP" (Ablehnen) eingestellten Richtlinie "Append a Rule" (Eine Regel hinzufügen) auswählen. Oder, wenn Sie alle Zugriffe von dem Subnetz 192.168.51 verhindern möchten (mit Ausnahme von einer bestimmten IP-Adresse (192.168.51.105)) und für die "Default Policy" (Standardrichtlinie) "Accept" (Akzeptieren) angegeben ist, dann würden Sie wie folgt vorgehen:

1. Append Rule 1 (Regel 1 hinzufügen) mit einer IP/Mask eingestellt auf 192.168.51.105/32 und einer Richtlinie "Accept" (Akzeptieren).
2. Append Rule 2 (Regel 2 hinzufügen) mit einer IP/Mask eingestellt auf 192.168.51.105/24 und einer Richtlinie "Accept" (Akzeptieren).

Wenn Sie Regel 1 und 2 vertauschen würden, könnte 192.168.51.105 auch nicht auf KX II-101-V2 zugreifen, da es in diesem Fall von der ersten gefundenen Regel abgelehnt werden würde.

---

## SSL-Zertifikate

Das SSL-Protokoll (Secure Socket Layer) wird für den gesamten verschlüsselten Netzwerkdatenverkehr zwischen KX II-101-V2 und einem mit der Einheit verbundenen Client verwendet. Wenn eine Verbindung hergestellt wird, muss sich KX II-101-V2 gegenüber einem Client, der ein kryptografisches Zertifikat verwendet, identifizieren.

Es kann eine Zertifikatsregistrierungsanforderung (Certificate Signing Request, CSR) erzeugt und ein von der Zertifizierungsstelle (Certificate Authority, CA) signiertes Zertifikat auf dem KX II-101-V2-Gerät installiert werden. Die CA prüft die Identität des Absenders der CSR. Anschließend sendet die CA ein signiertes Zertifikat an den Absender. Das Zertifikat mit der Signatur der renommierten CA wird verwendet, um für die Identität des Zertifikatsinhabers zu bürgen.

---

**Wichtig: Vergewissern Sie sich, dass das Datum und die Uhrzeit für KX II-101-V2 richtig eingestellt sind.**

---

Wenn ein selbstsigniertes Zertifikat erstellt wird, wird das Datum und die Uhrzeit von KX II-101-V2 zum Berechnen des Gültigkeitszeitraums verwendet. Wenn das Datum und die Uhrzeit von KX II-101-V2 ungenau sind, ist möglicherweise der Zeitraum des Zertifikats falsch, was bei der Validierung des Zertifikats zu Fehlern führen kann. Siehe **Konfigurieren von Datum-/Uhrzeiteinstellungen** (auf Seite 134).

---

*Hinweis: Die CSR muss auf KX II-101-V2 generiert werden.*

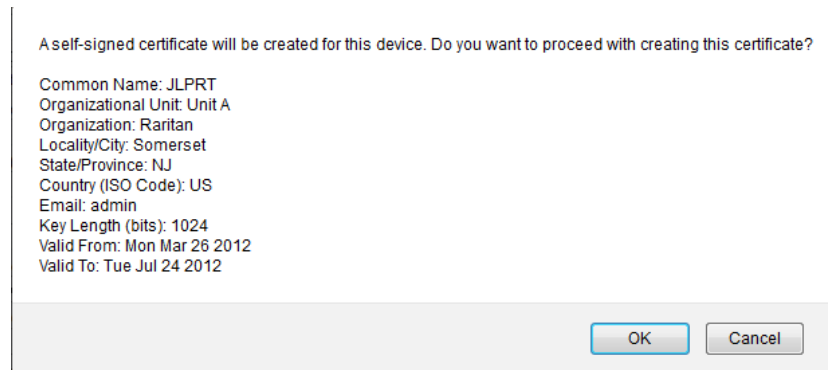
*Hinweis: Beim Aktualisieren der Firmware werden das aktive Zertifikat und die CSR nicht ersetzt.*

---

► **So erstellen und installieren Sie ein SSL-Zertifikat:**

1. Wählen Sie "Security" > "Certificate" (Sicherheit > Zertifikat) aus.
2. Füllen Sie die folgenden Felder aus:
  - a. Common Name (Allgemeiner Name) – Der Netzwerkname der KX II-101-V2-Einheit, nachdem diese im Netzwerk installiert wurde (normalerweise der vollqualifizierte Domainname). Der allgemeine Name ist mit dem Namen identisch, der für den Zugriff auf KX II-101-V2 über einen Webbrowser verwendet wird, allerdings ohne das Präfix "http://". Sollte der hier angegebene Name nicht dem tatsächlichen Netzwerknamen entsprechen, wird im Browser eine Sicherheitswarnung angezeigt, wenn über HTTPS auf KX II-101-V2 zugegriffen wird.
  - b. Organizational Unit (Organisationseinheit) – In diesem Feld wird angegeben, zu welcher Abteilung der Organisation das KX II-101-V2-Gerät gehört.
  - c. Organization (Organisation) – Der Name der Organisation, zu der das KX II-101-V2-Gerät gehört.
  - d. Locality/City (Lokalität/Stadt) – Die Stadt, in der sich die Organisation befindet.
  - e. State/Province (Bundesland/Region) – Das Bundesland oder die Region, in dem/der sich die Organisation befindet.
  - f. Country (ISO code) [Land (ISO-Code)] – Das Land, in dem sich die Organisation befindet. Der ISO-Code ist der aus zwei Buchstaben bestehende Code der Internationalen Organisation für Normung, z. B. "DE" für Deutschland oder "US" für die USA.
  - g. Challenge Password (Challenge-Kennwort) – Einige Zertifizierungsstellen verlangen ein Challenge-Kennwort für die Authentifizierung von späteren Änderungen des Zertifikats (z. B. Widerruf des Zertifikats). Geben Sie gegebenenfalls ein Kennwort ein.
  - h. Confirm Challenge Password (Challenge-Kennwort bestätigen) – Bestätigung des Challenge-Kennworts.
  - i. Email (E-Mail) – Die E-Mail-Adresse einer Kontaktperson, die für KX II-101-V2 und dessen Sicherheit verantwortlich ist.

- j. Key Length (Schlüssellänge) – Die Länge des erzeugten Schlüssels in Bits. Die Standardlänge ist 1024.
3. Führen Sie einen der folgenden Schritt aus:
- a. Aktivieren Sie das Kontrollkästchen "Create a Self-Signed Certificate" (Selbst signiertes Zertifikat erstellen), wenn Sie ein selbst signiertes Zertifikat erstellen müssen. Wenn Sie diese Option aktivieren, generiert KX II-101-V2 das Zertifikat basierend auf Ihren Eingaben, das als signierende Zertifizierungsstelle fungiert. Die CSR muss nicht exportiert und nicht zum Generieren eines signierten Zertifikats verwendet werden.
  - b. Geben Sie die Anzahl der Tage für den Gültigkeitszeitraum an. Vergewissern Sie sich, dass das Datum und die Uhrzeit von KX II-101-V2 richtig sind, andernfalls kann ein ungültiges Datum zum Erstellen des Gültigkeitszeitraums für das Zertifikat verwendet werden.
  - c. Klicken Sie auf "Create" (Erstellen).
  - d. Eine Bestätigungsdiaologfeld wird angezeigt. Klicken Sie auf "OK", um es zu schließen.
  - e. Starten Sie KX II-101-V2 neu, um das selbstsignierte Zertifikat zu aktivieren.



Oder

- f. Geben Sie die Anzahl der Tage für den Gültigkeitszeitraum an. Vergewissern Sie sich, dass das Datum und die Uhrzeit von KX II-101-V2 richtig sind, andernfalls kann ein ungültiges Datum zum Erstellen des Gültigkeitszeitraums für das Zertifikat verwendet werden.
- g. Klicken Sie auf "Create" (Erstellen).
- h. Ein Dialogfeld wird angezeigt, das alle eingegebenen Informationen sowie den Gültigkeitszeitraum des Zertifikats enthält. Wenn die Informationen richtig sind, klicken Sie auf "OK", um die CSR zu generieren.

- i. Starten Sie KX II-101-V2 neu, um die gespeicherte CSR zur SSL-Zertifizierung an eine Zertifizierungsstelle.

► **So laden Sie ein CSR-Zertifikat herunter:**

1. Sie können die CSR und die Datei, die den bei der Erzeugung verwendeten privaten Schlüssel enthalten, herunterladen, indem Sie auf die Schaltfläche "Download" (Herunterladen) klicken.

---

*Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.*

---

2. Senden Sie die gespeicherte CSR zur Zertifizierung an eine Zertifizierungsstelle. Sie erhalten von dieser das neue Zertifikat.

► **So laden Sie ein signiertes Zertifikat hoch:**

1. Laden Sie das Zertifikat für KX II-101-V2 hoch, indem Sie auf die Schaltfläche "Upload" (Hochladen) klicken.

---

*Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.*

---

Certificate Signing Request (CSR)	Certificate Upload
<p>The following CSR is pending:</p> <pre>countryName           = US stateOrProvinceName  = DC localityName          = Washington organizationName     = ACME Corp. organizationalUnitName = Marketing Dept. commonName            = John Doe emailAddress          = johndoe@acme.com</pre> <p style="text-align: center;"> <input type="button" value="Download"/> <input type="button" value="Delete"/> </p>	<p>SSL Certificate File</p> <p><input type="text"/> <input type="button" value="Browse..."/></p> <p><input type="button" value="Upload"/></p>

Nach Abschluss dieser drei Schritte verfügt KX II-101-V2 über ein eigenes Zertifikat zur Identifizierung gegenüber den Clients.

---

**Wichtig: Wenn Sie die CSR auf der KX II-101-V2-Einheit löschen, kann diese nicht wiederhergestellt werden. Wenn Sie sie versehentlich gelöscht haben, müssen Sie die drei oben beschriebenen Schritte erneut durchführen. Um dies zu vermeiden, verwenden Sie die Downloadfunktion, sodass Sie über eine Kopie der CSR und des privaten Schlüssels verfügen.**

---

---

## Sicherheitsmeldung

KX II-101-V2 ermöglicht Ihnen, eine Sicherheitsmeldung zum Anmeldeprozess von KX II-101-V2 hinzuzufügen. Wenn diese Funktion aktiviert ist, müssen Benutzer vor dem Zugriff auf >ProductName< die Sicherheitsvereinbarung akzeptieren oder ablehnen. Die in einer Sicherheitsmeldung enthaltenen Informationen werden im Dialogfeld "Restricted Service Agreement" (Eingeschränkte Dienstvereinbarung) angezeigt, nachdem Benutzer nach Eingabe Ihrer Anmeldeinformationen auf KX II-101-V2 zugegriffen haben.

Die Überschrift und der Text der Sicherheitsmeldung kann angepasst werden, oder Sie können den Standardtext verwenden. Die Sicherheitsmeldung kann auch so konfiguriert werden, dass Benutzer die Sicherheitsvereinbarung akzeptieren müssen, bevor sie auf KX II-101-V2 zugreifen, oder die Sicherheitsmeldung kann einfach nach dem Anmeldevorgang angezeigt werden. Wenn die Funktion zum Akzeptieren oder Ablehnen aktiviert ist, wird die Auswahl des Benutzers im Prüfprotokoll protokolliert.

► **So konfigurieren Sie eine Sicherheitsmeldung:**

1. Klicken Sie auf "Security" > "Banner" (Sicherheit > Meldung), um die Seite "Banner" (Meldung) zu öffnen.
2. Wählen Sie "Display Restricted Service Banner" (Meldung für eingeschränkten Dienst anzeigen) aus, um die Funktion zu aktivieren.
3. Wenn Benutzer die Meldung vor dem Anmeldeprozess bestätigen sollen, wählen Sie "Require Acceptance of Restricted Service Banner" (Akzeptieren der Meldung für eingeschränkten Dienst erforderlich) aus. Um die Meldung zu akzeptieren, müssen Benutzer ein Kontrollkästchen aktivieren. Wenn Sie diese Einstellung nicht aktivieren, wird die Sicherheitsmeldung nach der Anmeldung des Benutzers nur angezeigt. In diesem Fall ist keine Bestätigung durch den Benutzer erforderlich.
4. Ändern Sie ggf. den Namen der Meldung. Diese Informationen werden den Benutzern als Teil der Meldung angezeigt. Es können bis zu 64 Zeichen verwendet werden.
5. Bearbeiten Sie die Informationen im Textfeld "Restricted Services Banner" (Meldung zum eingeschränkten Dienst). Sie können maximal 6000 Zeichen eingeben oder eine Textdatei hochladen. Führen Sie hierfür einen der folgenden Schritte aus:
  - a. Bearbeiten Sie den Text, indem Sie manuell in das Textfeld tippen. Klicken Sie auf "OK".

6. Laden Sie Informationen aus einer .txt-Datei hoch, indem Sie das Optionsfeld "Restricted Services Banner File" (Datei für Sicherheitsmeldung für eingeschränkte Dienste) auswählen und auf "Browse" (Durchsuchen) klicken, um die Datei zu suchen und hochzuladen. Klicken Sie auf "OK". Nachdem die Datei hochgeladen wurde, wird der Text aus der Datei im Textfeld "Restricted Services Banner Message" (Meldung zum eingeschränkten Dienst) angezeigt.

## Kapitel 9    **Wartung**

### **In diesem Kapitel**

Audit Log (Prüfprotokoll).....	182
Device Information (Geräteinformationen) .....	183
Backup/Restore (Sicherung/Wiederherstellung) .....	184
Aktualisieren der Firmware.....	186
Upgrade History (Aktualisierungsverlauf).....	188
Werksrückstellung .....	189
Neustart der KX II-101-V2-Einheit.....	189
Beenden der CC-SG-Verwaltung .....	191

---

### **Audit Log (Prüfprotokoll)**

Alle KX II-101-V2-Systemereignisse werden protokolliert. Das Prüfprotokoll kann bis zu 2 K Daten speichern, bevor die ältesten Einträge überschrieben werden. Zur Vermeidung des Verlusts von Prüfprotokolldaten exportieren Sie die Daten an einen Syslog-Server oder SNMP Manager. Konfigurieren Sie den Syslog-Server oder SNMP-Manager auf der Seite "Device Settings" (Geräteeinstellungen) > "Event Management" (Ereignisverwaltung).

► **So zeigen Sie das Prüfprotokoll für Ihre KX II-101-V2-Einheit an:**

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

Die Seite "Audit Log" (Prüfprotokoll) enthält Ereignisse sortiert nach Datum und Uhrzeit, wobei die letzten Ereignisse zuerst aufgeführt werden. Das Prüfprotokoll enthält die folgenden Informationen:

- Date (Datum) – Datum und Uhrzeit des Ereignisses, basierend auf dem 24-h-Zeitformat.
- Event (Ereignis) – Der Ereignisname, wie er auf der Seite "Event Management" (Ereignisverwaltung) aufgeführt wird.
- Description (Beschreibung) – Detaillierte Beschreibung des Ereignisses.

► **So speichern Sie das Prüfprotokoll:**

1. Klicken Sie auf "Save to File" (Speichern unter). Ein Dialogfeld zum Speichern der Datei wird angezeigt.
2. Wählen Sie einen Dateinamen und Speicherort aus, und klicken Sie auf "Save" (Speichern). Das Prüfprotokoll wird mit dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.

► **So blättern Sie durch das Prüfprotokoll:**

- Verwenden Sie die Links **[Older]** ([Älter]) und **[Newer]** ([Neuer]).

---

## **Device Information (Geräteinformationen)**

Die Seite "Device Information" (Geräteinformationen) bietet detaillierte Informationen zu Ihrem KX II-101-V2-Gerät. Diese Informationen benötigen Sie, wenn Sie sich mit dem technischen Kundendienst von Raritan in Verbindung setzen.

► **So zeigen Sie Informationen zu Ihrer KX II-101-V2-Einheit an:**

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

Zu der KX II-101-V2-Einheit werden folgende Informationen angezeigt:

- Model (Modell)
- Hardware Revision (Hardware-Revision)
- Firmware Version (Firmware-Version)
- Serial Number (Seriennummer)
- MAC Address (MAC-Adresse)



## Backup/Restore (Sicherung/Wiederherstellung)

Auf der Seite "Backup/Restore" (Sicherung/Wiederherstellung) können Sie die Einstellungen und die Konfiguration der KX II-101-V2-Einheit sichern und wiederherstellen.

Dieses Feature dient nicht nur der Gewährleistung der Geschäftskontinuität, sondern Sie können damit auch viel Zeit sparen. So können Sie Ihrem Team beispielsweise schnell von einer anderen KX II-101-V2-Einheit aus Zugriff gewähren, indem Sie die Benutzerkonfigurationseinstellungen des verwendeten KX II-101-V2-Geräts sichern und auf dem neuen KX II-101-V2-Gerät wiederherstellen. Sie können auch eine KX II-101-V2-Einheit einrichten und deren Konfiguration auf mehrere andere KX II-101-V2-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.

**Backup / Restore**

Full Restore

Protected Restore

Custom Restore

User and Group Restore

Device Settings Restore

Restore File

---

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

---

► **Wenn Sie Internet Explorer 7 (oder höher) zur Sicherung Ihres KX II-101-V2 verwenden:**

1. Klicken Sie auf "Backup" (Sichern). Das Dialogfeld "File Download" (Dateidownload) mit der Schaltfläche "Open" (Öffnen) wird angezeigt. Klicken Sie nicht auf "Open" (Öffnen).

Bei Internet Explorer 6 (und höher) wird Internet Explorer als Standardanwendung zum Öffnen von Dateien verwendet. Sie werden aufgefordert, die Datei zu öffnen oder sie zu speichern. Um dies zu verhindern, müssen Sie eine Änderung vornehmen, sodass WordPad® als Standardanwendung zum Öffnen von Dateien verwendet wird.

2. Dies funktioniert wie folgt:
  - a. Speichern Sie die Sicherungsdatei. Die Sicherungsdatei wird unter dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.
  - b. Ist die Datei gespeichert, navigieren Sie zu dieser und klicken mit der rechten Maustaste darauf. Klicken Sie im dem Kontextmenü auf "Eigenschaften".
  - c. Klicken Sie auf der Registerkarte "Allgemein" auf die Schaltfläche "Ändern", und wählen Sie im angezeigten Dialogfeld "WordPad" aus.

► **So stellen Sie die KX II-101-V2-Einheit wieder her:**

**WARNUNG:** Gehen Sie bei der Wiederherstellung Ihrer KX II-101-V2-Einheit auf eine frühere Version vorsichtig vor. Die bei der Sicherung gespeicherten Benutzernamen und Kennwörter werden wiederhergestellt. Wenn Sie sich nicht mehr an die alten Anmeldedaten für den Administrator erinnern können, wird Ihnen der Zugriff auf die KX II-101-V2-Einheit verweigert.

Falls Sie zum Zeitpunkt der Sicherung eine andere IP-Adresse verwendet haben, wird auch diese wiederhergestellt. Wenn Sie DHCP konfiguriert haben, sollten Sie diesen Vorgang nur ausführen, wenn Sie Zugriff auf den lokalen Port haben, um nach der Aktualisierung die IP-Adresse zu prüfen.

1. Wählen Sie eine Wiederherstellungsart aus:
  - "Full Restore" (Vollständige Wiederherstellung) – Das gesamte System wird wiederhergestellt. Wird normalerweise für herkömmliche Sicherungs- und Wiederherstellungszwecke verwendet.

- "Protected Restore" (Geschützte Wiederherstellung) – Alle Daten werden wiederhergestellt, mit Ausnahme von gerätespezifischen Informationen wie IP-Adresse, Name usw. Mit dieser Option können Sie eine KX II-101-V2-Einheit einrichten und deren Konfiguration auf mehrere andere KX II-101-V2-Geräte kopieren.
  - "Custom Restore" (Benutzerdefinierte Wiederherstellung) – Bei dieser Option stehen Ihnen die Kontrollkästchen "User and Group Restore" (Wiederherstellung von Benutzern und Gruppen) und "Device Settings Restore" (Wiederherstellung der Geräteeinstellungen) zur Verfügung.
    - "User and Group Restore" (Wiederherstellung von Benutzern und Gruppen) – Diese Option umfasst nur Benutzer- und Gruppeninformationen. Bei dieser Option werden das Zertifikat und die Dateien für den privaten Schlüssel *nicht* wiederhergestellt. Verwenden Sie sie, um schnell Benutzer auf einem anderen KX II-101-V2-Gerät einzurichten.
    - Device Settings Restore (Wiederherstellung der Geräteeinstellungen) – Diese Option umfasst nur Geräteeinstellungen wie Stromzuordnungen, USB-Profile, Konfigurationsparameter hinsichtlich Blade-Chassis sowie Portgruppenzuordnungen. Verwenden Sie sie, um schnell die Geräteinformationen zu kopieren.
2. Klicken Sie auf "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.

---

## Aktualisieren der Firmware

Auf der Seite Firmware Upgrade (Firmware-Aktualisierung) können Sie die Firmware von KX II-101-V2 aktualisieren.

---

**Wichtig: Schalten Sie während der Aktualisierung KX II-101-V2 nicht aus, da dies zu Schäden am Gerät führen könnte.**

---

► **So aktualisieren Sie das KX II-101-V2-Gerät:**

1. Wählen Sie "Maintenance > Firmware Upgrade" (Wartung > Firmware-Aktualisierung). Die Seite "Firmware Upgrade" (Firmwareaktualisierung) wird angezeigt.

2. Klicken Sie auf die Verknüpfung "Show Latest Firmware" (Aktuelle Firmware anzeigen), navigieren Sie zur entsprechenden Raritan-Firmware-Distributionsdatei (\*.RFP) auf der Seite "Firmware Upgrades > KX II-101-V2" (Firmware-Aktualisierungen > KX II-101-V2), und laden Sie die Datei herunter.
3. Entpacken Sie die Datei, und lesen Sie alle Anweisungen in den Firmware-ZIP-Dateien sorgfältig durch, bevor Sie die Aktualisierung durchführen.

---

*Hinweis: Kopieren Sie die Firmware-Aktualisierungsdatei vor dem Hochladen auf einen lokalen PC. Laden Sie die Datei nicht von einem Netzwerklaufwerk. Klicken Sie auf die Schaltfläche "Browse" (Durchsuchen), um zu dem Verzeichnis zu navigieren, in dem Sie die Aktualisierungsdatei entpackt haben.*

---

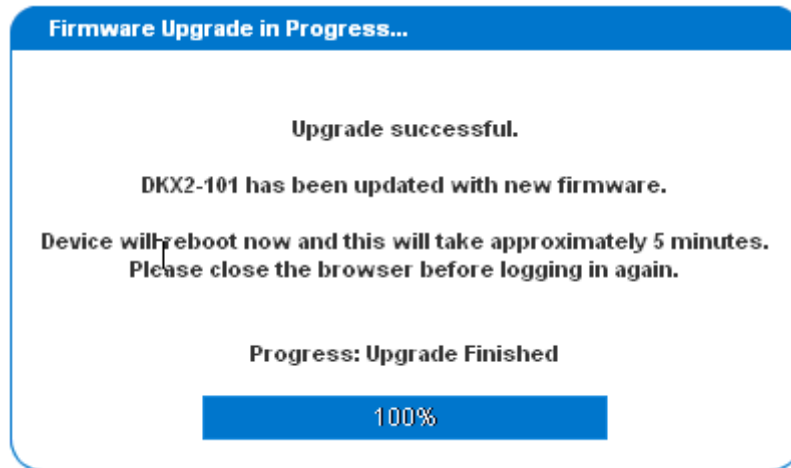
4. Klicken Sie auf der Seite "Firmware Upgrade" (Firmware-Aktualisierung) auf "Upload" (Hochladen). Informationen zur Aktualisierung und Versionsnummer werden angezeigt.

---

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

---

5. Klicken Sie auf "Upgrade" (Aktualisieren). Warten Sie, bis der Vorgang abgeschlossen ist. Während des Vorgangs werden Statusinformationen und Fortschrittsleisten angezeigt. Nach Abschluss der Aktualisierung wird das Gerät neu gestartet.



6. Schließen Sie den Browser, wenn Sie dazu aufgefordert werden, und warten Sie ungefähr fünf Minuten, bevor Sie sich erneut bei KX II-101-V2 anmelden.

Weitere Informationen zur Aktualisierung der Geräte-Firmware mithilfe des Multi-Platform-Clients finden Sie im Benutzerhandbuch **KVM and Serial Access Clients**.

---

## Upgrade History (Aktualisierungsverlauf)

Das KX II-101-V2 liefert Informationen über Aktualisierungen, die auf dem KX II-101-V2-Gerät durchgeführt wurden.

► **So zeigen Sie den Aktualisierungsverlauf an:**

- Wählen Sie "Maintenance > Upgrade History" (Wartung > Aktualisierungsverlauf). Die Seite "Upgrade History" (Aktualisierungsverlauf) wird angezeigt.

---

## Werksrückstellung

---

*Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern. Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter **Prüfprotokoll**.*

---

► **So führen Sie eine Werksrückstellung durch:**

1. Wählen Sie "Maintenance" > "Factory Reset" (Wartung > Werksrücksetzung) aus. Die Seite "Factory Reset" (Werksrücksetzung) wird angezeigt.
2. Wählen Sie die entsprechende Rücksetzungsoption aus:
  - "Full Factory Reset" (Vollständige Werksrücksetzung) – Damit entfernen Sie die gesamte Konfiguration und setzen das Gerät komplett auf die werkseitigen Standardeinstellungen zurück. Beachten Sie, dass Verwaltungsverbindungen mit CommandCenter dadurch unterbrochen werden. Da diese Rückstellung so umfassend ist, werden Sie dazu aufgefordert, den Vorgang zu bestätigen.
  - "Network Parameter Reset" (Netzwerkparameterrücksetzung) – Damit setzen Sie die Netzwerkparameter des Geräts auf die Standardwerte zurück [Klicken Sie auf "Device Settings" > "Network Settings" (Geräteeinstellungen > Netzwerkeinstellungen), um auf diese Informationen zuzugreifen]:
3. Klicken Sie auf "Reset" (Zurücksetzen), um fortzufahren. Da hierbei alle Netzwerkeinstellungen verloren gehen, werden Sie aufgefordert, die Werksrücksetzung zu bestätigen.
4. Klicken Sie zum Fortfahren auf "OK". Nach Abschluss des Vorgangs wird das KX II-101-V2-Gerät automatisch neu gestartet.

---

## Neustart der KX II-101-V2-Einheit

---

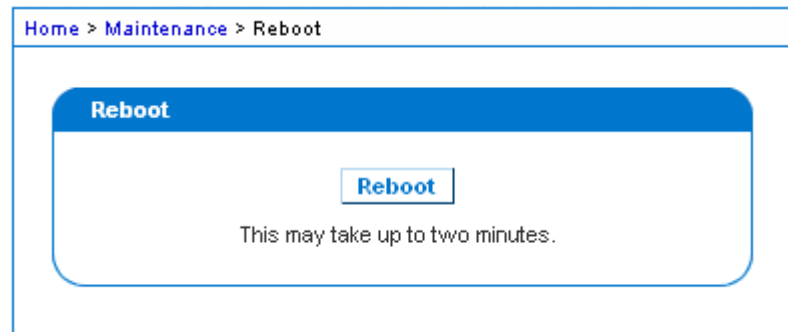
Auf der Seite "Reboot" (Neustart) können Sie KX II-101-V2 auf sichere und kontrollierte Weise neustarten. Dies ist die empfohlene Methode zum Neustarten.

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

---

► **So starten Sie die KX II-101-V2-Einheit neu:**

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



2. Klicken Sie auf "Reboot" (Neustart). Sie werden aufgefordert, die Aktion zu bestätigen. Klicken Sie auf "Yes" (Ja), um fortzufahren.



---

## Beenden der CC-SG-Verwaltung

Wenn KX II-101-V2 von CC-SG verwaltet wird und Sie direkt auf das Gerät zugreifen möchten, erhalten Sie eine Meldung, dass das Gerät von CC-SG verwaltet wird.

Wenn KX II-101-V2 über CC-SG verwaltet und die Verbindung zwischen CC-SG und KX II-101-V2 nach Ablauf des festgelegten Zeitlimits (normalerweise 10 Minuten) getrennt wird, können Sie die CC-SG-Verwaltungssitzung über die KX II-101-V2-Konsole beenden.

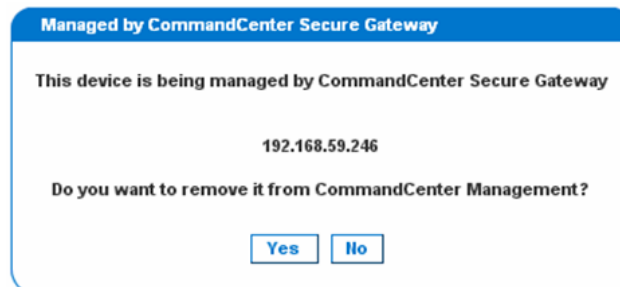
---

*Hinweis: Sie müssen über die entsprechenden Berechtigungen zum Beenden der CC-SG-Verwaltung des KX II-101-V2 verfügen. Die Option "Stop CC-SG Management" (CC-SG-Verwaltung beenden) steht nur zur Verfügung, wenn Sie zurzeit CC-SG für die Verwaltung von KX II-101-V2 verwenden.*

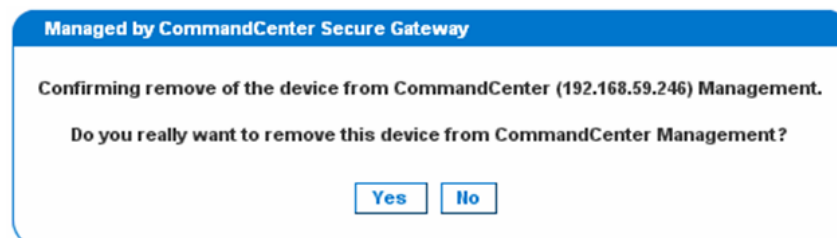
---

► **So beenden Sie die CC-SG-Verwaltung eines KX II-101-V2-Geräts:**

1. Klicken Sie auf "Maintenance" > "Stop CC-SG Management" (Wartung > CC-SG-Verwaltung beenden). Eine Meldung, dass das Gerät von CC-SG verwaltet wird, wird angezeigt. Ebenso wird eine Option zum Beenden der CC-SG-Verwaltung für das Gerät angezeigt.



2. Klicken Sie auf "Yes" (Ja), um den Vorgang zum Beenden der CC-SG-Verwaltung für das Gerät zu starten. Eine Bestätigungsmeldung wird angezeigt, in der Sie aufgefordert werden, das Beenden der CC-SG-Verwaltung für das Gerät zu bestätigen.





3. Klicken Sie auf "Yes" (Ja), um die CC-SG-Verwaltung für das Gerät zu beenden. Wenn die CC-SG-Verwaltung beendet wurde, wird eine Bestätigungsmeldung angezeigt.



## Kapitel 10 Diagnostics (Diagnose)

Auf den Diagnoseseiten können Sie Probleme behandeln. Sie sind hauptsächlich für den Administrator des KX II-101-V2-Geräts gedacht. Auf allen Diagnoseseiten (außer Device Diagnostics [Gerätediagnose]) werden übliche Netzwerkbefehle ausgeführt. Die angezeigten Informationen sind das Ergebnis dieser Befehle. Mithilfe der Optionen im Menü "Diagnostics" (Diagnose) können Sie Fehler in den Netzwerkeinstellungen beheben und diese konfigurieren.

Die Option "Device Diagnostics" (Gerätediagnose) sollten Sie nur gemeinsam mit dem technischen Kundendienst von Raritan verwenden.

### In diesem Kapitel

Network Interface (Netzwerkschnittstelle) .....	193
Network Statistics (Netzwerkstatistik) .....	194
Ping Host (Ping an den Host) .....	196
Seite "Trace Route to Host" (Route zum Host verfolgen) .....	196
Device Diagnostics (Gerätediagnose) .....	198

---

### Network Interface (Netzwerkschnittstelle)

KX II-101-V2 liefert Informationen zum Status der Netzwerkschnittstelle.

► **So zeigen Sie Informationen zur Netzwerkschnittstelle an:**

- Wählen Sie "Diagnostics > Network Interface" (Diagnose > Netzwerkschnittstelle). Die Seite "Network Interface" (Netzwerkschnittstelle) wird angezeigt.

Diese Seite enthält die folgenden Informationen:

- Funktionsfähigkeit der Ethernet-Schnittstelle
- Erreichbarkeit des Gateways
- Derzeit aktiver LAN-Port

► **So aktualisieren Sie diese Informationen:**

- Klicken Sie auf "Refresh" (Aktualisieren).

## Network Statistics (Netzwerkstatistik)

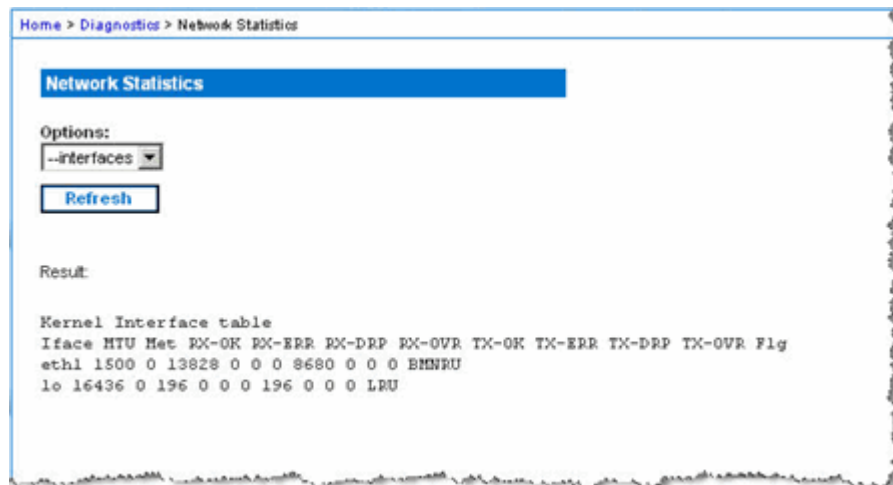
KX II-101-V2 liefert Statistiken über die Netzwerkschnittstelle.

► **So zeigen Sie Statistiken über die Netzwerkschnittstelle an:**

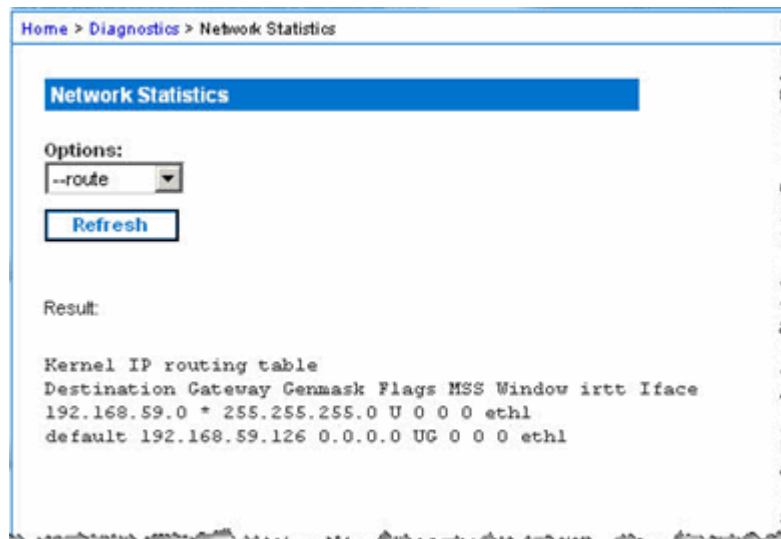
1. Wählen Sie **Diagnostics > Network Statistics** (Diagnose > Netzwerkstatistik). Die Seite **Network Statistics** (Netzwerkstatistik) wird angezeigt.
2. Wählen Sie eine Option aus der Dropdown-Liste **Options**:
  - Statistics (Statistiken) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



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



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



3. Klicken Sie auf "Refresh" (Aktualisieren). Die entsprechenden Informationen werden im Feld "Result" (Ergebnis) angezeigt.

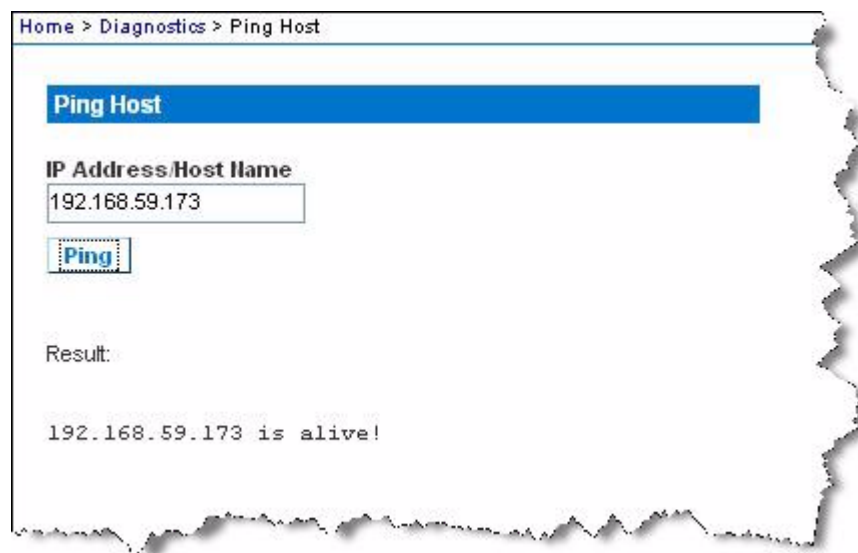
---

## Ping Host (Ping an den Host)

Ping ist ein Netzwerktool, mit dem getestet werden kann, ob ein bestimmter Host oder eine IP-Adresse über ein IP-Netzwerk erreichbar ist. Mithilfe der Seite "Ping Host" (Ping an den Host) können Sie herausfinden, ob ein Zielsystem oder eine andere KX II-101-V2-Einheit erreichbar ist.

► **So senden Sie ein Ping an den Host:**

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



2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

---

*Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.*

3. Klicken Sie auf "Ping". Die Ping-Ergebnisse werden im Feld "Result" (Ergebnis) angezeigt.

---

## Seite "Trace Route to Host" (Route zum Host verfolgen)

Trace Route ist ein Netzwerk-Tool, mit dem die Route zum angegebenen Hostnamen oder zur angegebenen IP-Adresse bestimmt werden kann.

► **So verfolgen Sie die Route zum Host:**

1. Wählen Sie "Diagnostics > Trace Route to Host" (Diagnose > Route zum Host verfolgen). Die Seite "Trace Route to Host" (Route zum Host verfolgen) wird geöffnet.

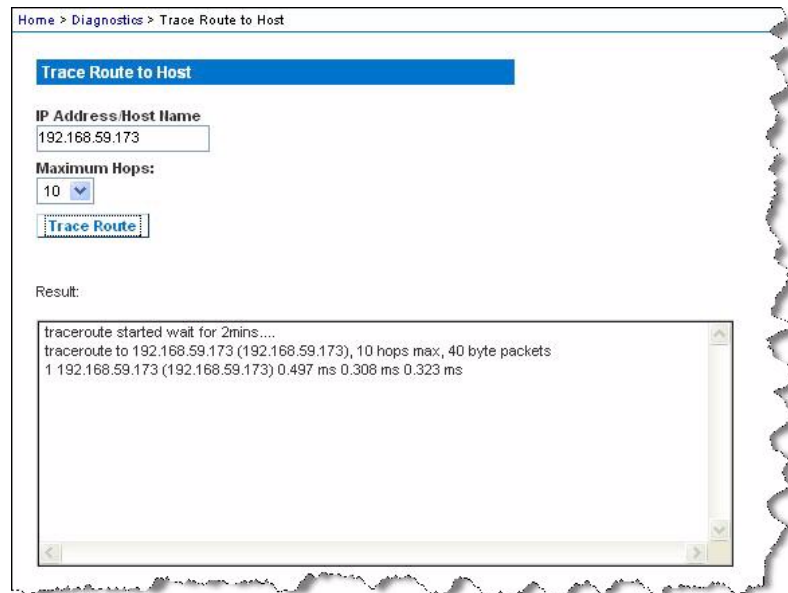
2. Geben Sie die IP-Adresse oder den Hostnamen in das Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

---

*Hinweis: Der Hostname darf maximal 232 Zeichen lang sein.*

---

3. Wählen Sie die maximale Anzahl an Hops aus der Dropdown-Liste (5 bis 50 in 5er-Schritten).
4. Klicken Sie auf "Trace Route" (Route verfolgen). Der Befehl zum Verfolgen der Route wird für den angegebenen Hostnamen bzw. die angegebene IP-Adresse und die maximale Anzahl an Hops ausgeführt. Die Ausgabe der Routenverfolgung wird im Feld "Result" (Ergebnis) angezeigt.



---

## Device Diagnostics (Gerätediagnose)

---

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

---

Auf der Seite "Device Diagnostics" (Gerätediagnose) werden die Diagnoseinformationen von KX II-101-V2 auf den Client-PC heruntergeladen. Sie können ein Gerätediagnoseprotokoll mit oder ohne ein optionales Diagnoseskript vom technischen Kundendienst von Raritan generieren. Ein Diagnoseskript bietet mehr Informationen bei Problemen.

Verwenden Sie die folgenden Einstellungen:

- Diagnostics Scripts (Diagnoseskripts) – Lädt während einer Sitzung zum Debuggen eines schwerwiegenden Fehlers ein vom technischen Kundendienst von Raritan bereitgestelltes Speziaskript. Das Skript wird auf das Gerät hochgeladen und ausgeführt.  
**///Optional**
- Device Diagnostic Log (Gerätediagnoseprotokoll) – Lädt eine Übersicht der Diagnosemeldungen vom KX II-101-V2-Gerät auf den Client. Diese verschlüsselte Datei wird anschließend an den technischen Kundendienst von Raritan gesendet. Nur Raritan kann diese Datei interpretieren.

---

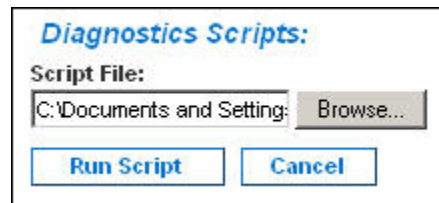
*Hinweis: Auf diese Seite können nur Benutzer mit Administratorrechten zugreifen.*

---

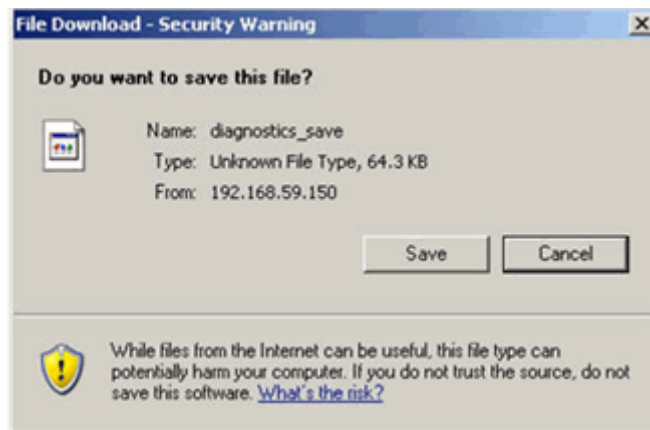
► **So führen Sie die KX II-101-V2-Systemdiagnose aus:**

1. Wählen Sie "Diagnostics > Device Diagnostics" (Diagnose > Gerätediagnose). Die Seite "Device Diagnostics" (Gerätediagnose) wird angezeigt.
2. (Optional) Führen Sie die folgenden Schritte durch, wenn Sie eine Datei mit einem Diagnoseskript vom technischen Kundendienst von Raritan erhalten haben. Fahren Sie ansonsten mit Schritt 3 fort.
  - a. Rufen Sie die Diagnosedatei von Raritan ab, und entpacken Sie sie gegebenenfalls.
  - b. Klicken Sie auf "Browse" (Durchsuchen). Das Dialogfeld "Choose file" (Datei auswählen) wird angezeigt.
  - c. Navigieren Sie zu der Diagnosedatei, und markieren Sie sie.

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



- e. Klicken Sie auf "Run Script" (Skript ausführen).
3. Erstellen Sie eine Diagnosedatei, die Sie an den technischen Kundendienst von Raritan senden können:
    - a. Klicken Sie auf "Save to File" (Speichern unter). Das Dialogfeld "File Download" (Dateidownload) wird angezeigt.



- b. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.
  - c. Navigieren Sie zum gewünschten Verzeichnis, und klicken Sie auf "Save" (Speichern).
4. Senden Sie diese Datei an die vom technischen Kundendienst von Raritan angegebene E-Mail-Adresse.



# Kapitel 11 Kommandozeilenschnittstelle (CLI)

## In diesem Kapitel

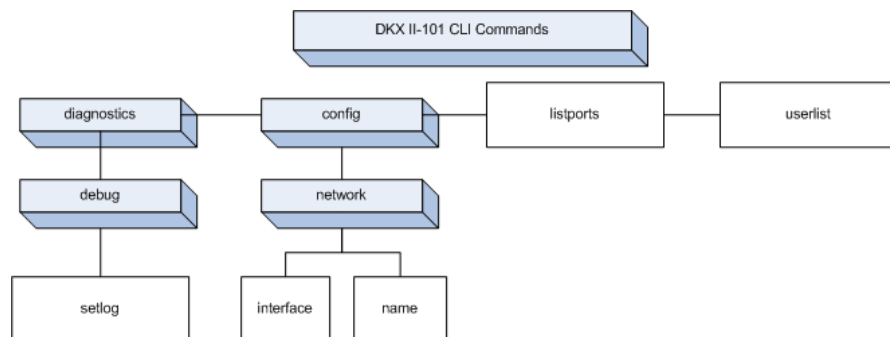
Überblick.....	200
Zugriff auf KX II-101-V2 über die Befehlszeilenschnittstelle .....	201
SSH-Verbindung mit der KX II-101-V2-Einheit.....	201
Anmelden.....	202
Navigation in der Kommandozeilenschnittstelle.....	202
Befehle der Befehlszeilenschnittstelle.....	204

---

## Überblick

Dieses Kapitel enthält eine Übersicht über die Befehle der Befehlszeilenschnittstelle (CLI), die mit KX II-101-V2 verwendet werden können. Eine Liste der Befehle und Definitionen sowie die Verknüpfungen zu den Abschnitten in diesem Kapitel, die Beispiele für diese Befehle enthalten, finden Sie unter **Befehle der Befehlszeilenschnittstelle** (auf Seite 204).

Das folgende Diagramm bietet eine Übersicht über die Befehle der Befehlszeilenschnittstelle:



---

*Hinweis: Die folgenden allgemeinen Befehle können auf allen Ebenen der Befehlszeilenschnittstelle der Abbildung oben verwendet werden: "top", "history", "logout", "quit" und "help".*

---

---

## Zugriff auf KX II-101-V2 über die Befehlszeilenschnittstelle

Verwenden Sie eine der folgenden Methoden, um auf das KX II-101-V2-Gerät zuzugreifen:

- TELNET über IP-Verbindung
- SSH (Secure Shell) über IP-Verbindung
- Serieller Multifunktionsverwaltungs-Port über serielle RS-232-Schnittstelle mithilfe des mitgelieferten Kabels und einem Terminalemulationsprogramm, wie HyperTerminal

Mehrere SSH/TELNET-Clients stehen hier zur Verfügung:

- PuTTY – <http://www.chiark.greenend.org.uk/~sgtatham/putty/>  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SSH Client von ssh.com - [www.ssh.com](http://www.ssh.com) <http://www.ssh.com>
- Applet SSH Client - [www.netbeans.org/ssh](http://www.netbeans.org/ssh)  
<http://www.netbeans.org/ssh>
- OpenSSH Client - [www.openssh.org](http://www.openssh.org) <http://www.openssh.org>

---

*Hinweis: Für den Zugriff auf die Befehlszeilenschnittstelle über SSH oder TELNET müssen Sie den Zugriff auf der Seite "Device Services" (Gerätedienste) des KX II-101-V2-Remote-Clients einrichten. Siehe **Gerätedienste** (siehe "**Device Services (Gerätedienste)**" auf Seite 126).*

---



---

## SSH-Verbindung mit der KX II-101-V2-Einheit

Verwenden Sie zur Verbindung mit dem Gerät einen SSH-Client, der SSH V2 unterstützt. Sie müssen den SSH-Zugriff auf der Seite "Devices Services" (Gerätedienste) aktivieren. Siehe **Gerätedienste** (siehe "**Device Services (Gerätedienste)**" auf Seite 126).

---

*Hinweis: Aus Sicherheitsgründen werden SSH-V1-Verbindungen von KX II-101-V2 nicht unterstützt.*

---

### SSH-Zugriff über einen Windows-PC

► **So öffnen Sie eine SSH-Sitzung über einen Windows®-PC:**

1. Starten Sie die SSH-Clientsoftware.
2. Geben Sie die IP-Adresse des KX II-101-V2-Servers ein. Beispielsweise 192.168.0.192.
3. Wählen Sie "SSH" aus (der standardmäßige Konfigurations-Port lautet 22).
4. Klicken Sie auf "Open" (Öffnen).

- Die Eingabeaufforderung `login as:` (Anmelden als:) wird angezeigt.

---

### SSH-Zugriff über eine UNIX-/Linux-Workstation

- ▶ Geben Sie den folgenden Befehl ein, um eine SSH-Sitzung über eine UNIX®-/Linux®-Workstation zu öffnen und sich als Admin-Benutzer anzumelden:

```
ssh -l admin 192.168.30.222
```

Die Eingabeaufforderung für das Kennwort wird angezeigt.

---

## Anmelden

- ▶ So melden Sie sich an:

- Login: admin
- Die Eingabeaufforderung für das Kennwort wird angezeigt. Geben Sie das Standardkennwort ein: *raritan*.

Der Begrüßungsbildschirm wird angezeigt. Sie sind jetzt als Administrator angemeldet.

Lesen Sie den folgenden Abschnitt **Navigation in der Befehlszeilenschnittstelle** (siehe "**Navigation in der Kommandozeilenschnittstelle**" auf Seite 202) und führen Sie dann die ersten unter **Konfigurieren von KX II-101-V2 unter der Verwendung eines Terminalemulationsprogramms (Optional)** (auf Seite 35) beschriebenen Konfigurationsaufgaben durch.

---

## Navigation in der Kommandozeilenschnittstelle

Vor der Verwendung der Kommandozeilenschnittstelle sollten Sie sich mit der Navigation und Syntax in der Kommandozeilenschnittstelle vertraut machen. Es stehen Ihnen außerdem einige Tastenkombinationen zur Verfügung, mit denen die Verwendung der Kommandozeilenschnittstelle erleichtert wird.

---

### Eingabeaufforderungen der Befehlszeilenschnittstelle

Die Eingabeaufforderung der Befehlszeilenschnittstelle zeigt die aktuelle Befehlsebene an. Die Stammebene der Eingabeaufforderung ist der Anmeldeame. Bei einer direkten Verbindung mit dem seriellen Port "Admin" mit einem Terminalemulationsprogramm ist "Admin Port" (Admin-Port) die Stammebene eines Befehls:

```
admin >
```

Bei TELNET/SSH ist "admin" die Stammebene des Befehls:

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

```
0
```

---

### Vervollständigen von Befehlen

Die Kommandozeilenschnittstelle unterstützt das Vervollständigen teilweise eingegebener Befehle. Drücken Sie die Tabulatortaste, wenn Sie die ersten Zeichen eines Eintrags eingegeben haben. Wenn die Zeichen mit einem Befehl eindeutig übereinstimmen, vervollständigt die Kommandozeilenschnittstelle den Eintrag.

- Wird keine Übereinstimmung gefunden, zeigt die Kommandozeilenschnittstelle die gültigen Einträge für die Ebene an.
- Wenn mehrere Übereinstimmungen gefunden werden, zeigt die Kommandozeilenschnittstelle alle gültigen Einträge an.

Geben Sie weiteren Text ein, damit eine eindeutige Übereinstimmung gefunden werden kann, und vervollständigen Sie den Eintrag mithilfe der Tabulatortaste.

---

### Syntax der Kommandozeilenschnittstelle – Tipps und Zugriffstasten

#### Tipps

- Befehle werden in alphabetischer Reihenfolge aufgeführt.
- Bei Befehlen wird die Groß-/Kleinschreibung nicht beachtet.
- Parameternamen bestehen aus einem Wort ohne Unterstrich.
- Für Befehle ohne Argumente werden standardmäßig die aktuellen Einstellungen für den Befehl angezeigt.
- Wenn Sie nach dem Befehl ein Fragezeichen (?) eingeben, wird die Hilfe für diesen Befehl angezeigt.
- Ein senkrechter Strich (|) zeigt eine Auswahl im Bereich der optionalen oder erforderlichen Schlüsselwörter oder Argumente an.

#### Zugriffstasten

- Drücken Sie die Pfeil-nach-oben-Taste, um den letzten Eintrag anzuzeigen.
- Drücken Sie die Rücktaste, um das zuletzt eingegebene Zeichen zu löschen.
- Drücken Sie "Strg+C", um einen Befehl zu beenden oder abubrechen, wenn Sie die falschen Parameter eingegeben haben.
- Drücken Sie die Eingabetaste, um den Befehl auszuführen.
- Drücken Sie die Tabulatortaste, um einen Befehl zu vervollständigen. Beispiel: `Admin Port > Conf.` Das System zeigt dann die Eingabeaufforderung `Admin Port > Config >` an.

### Allgemeine Befehle für alle Ebenen der Befehlszeilenschnittstelle

Unter Befehle der Befehlszeilenschnittstelle finden Sie eine Liste der Befehle, die auf allen Ebenen der Befehlszeilenschnittstelle verfügbar sind. Diese Befehle dienen auch zur Navigation in der Befehlszeilenschnittstelle.

Befehl	Beschreibung
top	Wechselt zur höchsten Ebene der Hierarchie der Kommandozeilenschnittstelle oder der Eingabeaufforderung "username" (Benutzername).
history	Zeigt die letzten 200 Befehle an, die der Benutzer in die Befehlszeilenschnittstelle von KX II-101-V2 eingegeben hat.
help	Anzeigen einer Übersicht der Syntax der Befehlszeilenschnittstelle.
quit	Der Benutzer kehrt eine Ebene zurück.
logout	Beendet die Benutzersitzung.

### Befehle der Befehlszeilenschnittstelle

In der Tabelle unten sind alle verfügbaren Befehle der Befehlszeilenschnittstelle aufgeführt und beschrieben.

Befehl	Beschreibung
config	Wechsel zum Menü "Configuration" (Konfiguration).
diagnostics	Wechsel zum Menü "Diagnostics" (Diagnose). Siehe <b>Diagnose</b> (siehe " <b>Diagnostics (Diagnose)</b> " auf Seite 205).
debug	Wechsel zum Menü "Debug". Siehe <b>Debug</b> (auf Seite 206).
help	Anzeigen einer Übersicht der Syntax der Befehlszeilenschnittstelle.
history	Anzeigen des Befehlszeilenverlaufs der aktuellen Sitzung.
interface	Konfigurieren der Netzwerkschnittstelle von KX II-101-V2.
ipv6_interface	Einstellen/Empfangen von IPv6-Netzwerkparametern

Befehl	Beschreibung
config	Wechsel zum Menü "Configuration" (Konfiguration).
diagnostics	Wechsel zum Menü "Diagnostics" (Diagnose). Siehe <b>Diagnose</b> (siehe " <b>Diagnostics (Diagnose)</b> " auf Seite 205).
listports	Auflistung von Port, Port-Name, Port-Typ, Port-Status und Port-Verfügbarkeit. Siehe <b>Befehl "Listports"</b> (siehe " <b>Befehl „listports“</b> " auf Seite 209).
logout	Abmelden von der aktuellen Sitzung der Befehlszeilenschnittstelle.
name	Festlegen des Gerätenamens. Siehe <b>Befehl "Name"</b> (siehe " <b>Befehl „name“</b> " auf Seite 208).
network	Anzeigen der Netzwerkkonfiguration und Möglichkeit, die Netzwerkeinstellungen zu konfigurieren. Siehe <b>Netzwerk</b> (siehe " <b>Network (Netzwerk)</b> " auf Seite 207).
quit	Rückkehr zum vorherigen Befehl.
setlog	Festlegen der Protokollierungsoptionen für das Gerät. Siehe <b>Befehl "Setlog"</b> (siehe " <b>Befehl „Setlog“</b> " auf Seite 206).
top	Rückkehr zum Stammmenü.
userlist	Auflistung der Anzahl der aktiven Benutzer, Benutzernamen, Port und Status. Siehe <b>Befehl "Userlist"</b> (siehe " <b>Befehl „Userlist“</b> " auf Seite 209).

---

### Diagnostics (Diagnose)

Im Menü **Diagnostics** (Diagnose) können Sie die Protokollierungsoptionen für die verschiedenen Module von KX II-101-V2 festlegen. Sie sollten die Protokollierungsoptionen nur festlegen, wenn Sie von einem Mitarbeiter des technischen Kundendienstes von Raritan dazu aufgefordert werden. Diese Protokollierungsoptionen liefern einem Kundendienstmitarbeiter die richtigen Informationen zum Debuggen und zur Fehlerbehebung. Sie erhalten von einem Kundendienstmitarbeiter die Anweisungen, wie Sie die Protokollierungsoptionen festlegen und wie Sie eine Protokolldatei erstellen müssen, die dann an den technischen Kundendienst von Raritan gesendet wird.

---

**Wichtig: Legen Sie die Protokollierungsoptionen nur unter Anleitung eines Mitarbeiters des technischen Kundendienstes von Raritan fest.**

---

## Debug

Im Menü **Diagnostics > Debug** (Diagnose > Debug) können Sie den Befehl **Setlog** auswählen, um die Protokollierungsoptionen für KX II-101-V2 festzulegen.

### Befehl „Setlog“

Mit dem Befehl "Setlog" können Sie die Protokollierungsebene für verschiedene Module von KX II-101-V2 festlegen und die aktuellen Protokollierungsebenen für jedes Modul anzeigen. Verwenden Sie folgende Syntax für den Befehl "Setlog":

```
setlog [module <module>] [level <level>] [vflag <vflag>] [verbose <on|off>]
Set/Get diag log level
```

Die Optionen des Befehls "Setlog" sind in der folgenden Tabelle beschrieben. Der technische Kundendienst von Raritan hilft Ihnen bei der Konfiguration dieser Einstellungen.

Befehlsoption	Beschreibung
module	Modulname
level	Diagnoseebene: <ul style="list-style-type: none"> <li>▪ err</li> <li>▪ warn</li> <li>▪ info</li> <li>▪ debug</li> <li>▪ trace</li> </ul>
vflag	Art des Verbose-Flag: <ul style="list-style-type: none"> <li>▪ timestamp</li> <li>▪ module</li> <li>▪ thread</li> <li>▪ fileline</li> </ul>
verbose [on off]	Schaltet die Verbose-Protokollierung ein oder aus.

Beispiel für den Befehl „Setlog“

Der folgende Befehl "Setlog" legt die Protokollierungsebene zum Debuggen mit Verbose-Protokollierung für das Modul „libpp\_serial“ fest.

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

## Configuration (Konfiguration)

Über das Menü **Configuration** (Konfiguration) können Sie auf die Netzwerkbefehle zum Konfigurieren der Netzwerkschnittstelle und zum Festlegen des Gerätenamens zugreifen.

### Network (Netzwerk)

Die Befehle unter "Configuration > Network" (Konfiguration > Netzwerk) werden zur Konfiguration der Netzwerkverbindung und des Gerätenamens von KX II-101-V2 verwendet.

Befehl	Beschreibung
interface	Konfiguriert die Netzwerkschnittstelle des KX II-101-V2-Geräts.
name	Festlegen des Gerätenamens.
ipv6_interface	Einstellen/Empfangen von IPv6-Netzwerkparametern

#### Befehl „interface“

Der Befehl "interface" wird zur Konfiguration der Netzwerkschnittstelle von KX II-101-V2 verwendet. Wird der Befehl angenommen, trennt das Gerät die HTTP/HTTPS-Verbindung und initialisiert eine neue Netzwerkverbindung. Alle HTTP/HTTPS-Benutzer müssen sich erneut über die neue IP-Adresse und den richtigen Benutzernamen und das entsprechende Kennwort mit dem Gerät verbinden. Siehe **Installation und Konfiguration** (auf Seite 9).

Verwenden Sie folgende Syntax für den Befehl "interface":

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

Die Optionen des Befehls "interface" sind in der folgenden Tabelle beschrieben.

Befehlsoption	Beschreibung
ipauto	Statische oder dynamische IP-Adresse
ip ipaddress	IP-Adresse des KX II-101-V2-Geräts, die



Befehloption	Beschreibung
	für den Zugriff über das IP-Netzwerk zugewiesen wurde
mask subnetmask	Subnetzmaske, die vom IP-Administrator vergeben wurde
gw ipaddress	Gateway-IP-Adresse, die vom IP-Administrator vergeben wurde
mode <auto   100fdx>	Legt den Ethernet-Modus auf automatische Erkennung oder 100Mbit/s Vollduplex (100fdx) fest.

Beispiel für den Befehl „interface“

Der folgende Befehl legt die IP-Adresse, Maske und Gateway-Adressen sowie den Modus auf automatische Erkennung fest.

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

### **Befehl „name“**

Der Befehl "name" wird zur Konfiguration des Einheits- und Hostnamens verwendet.

Syntax

```
name [unitname name] [domain name] [force <true|false>]
```

Beispiel für den Befehl „name“

Folgender Befehl legt den Einheitsnamen fest:

```
Admin Port > Config > Network > name unitname <unit name>
domain <host name> force trues
```

### **Befehl "IPv6"**

Verwenden Sie den Befehl "IPv6", um die IPv6-Netzwerkparameter festzulegen und bestehende IPv6-Parameter abzurufen.

```
Ipv6_interface mode enable ipauto none ip
2001:db8:290c:1291::17 prefixlen 128 gw
2001:db8:290c:1291::1
```

---

**Befehl „listports“**

Mit dem Befehl "listports" können Sie die Anzahl der aktiven Benutzer, Benutzernamen, den Port und Status anzeigen.

Beispiel für den Befehl „listports“

```
Admin Port > listports
Port Port                Port Port  Port
No.  Name                Type Status Availability
1 - Dominion_KXII-101_V2_Port KVM  up    idle
```

---

**Befehl „Userlist“**

Mit dem Befehl "Userlist" können Sie den Port, Port-Namen, Port-Typ, Port-Status und die Port-Verfügbarkeit anzeigen.

Beispiel für den Befehl „Userlist“

```
Admin Port > Userlist
Active user number: 1
User Name | From      | Status
-----
-
admin    | Admin Port | active
```

# Kapitel 12 "CC-SG Management" (CC-SG-Verwaltung)

## In diesem Kapitel

Überblick.....	210
Aufheben der Verwaltung von KX II-101-V2 durch CC-SG.....	211
Verwenden von CC-SG im Proxymodus .....	212

---

## Überblick

CC-SG kann zum Verwalten von KX II-101-V2 verwendet werden. Sobald die CC-SG-Verwaltung aktiv ist, kann via iPad® und iPhone® auf KX II-101-V2 mobil zugegriffen werden. Informationen zum Hinzufügen von KX II-101-V2 zur Verwaltung Ihres Geräts mit CC-SG, und Informationen dazu, wie Sie mobilen Zugriff zu Ihrem Gerät herstellen können, finden Sie in der Dokumentation für CC-SG-Verwaltung.

Wenn ein KX II-101-V2-Gerät über CommandCenter Secure Gateway gesteuert wird und Sie versuchen, über die KX II-101-V2-Remotekonsole direkt auf das Gerät zuzugreifen, wird die folgende Meldung angezeigt (nach Eingabe eines gültigen Benutzernamens und Kennworts):



---

## Aufheben der Verwaltung von KX II-101-V2 durch CC-SG

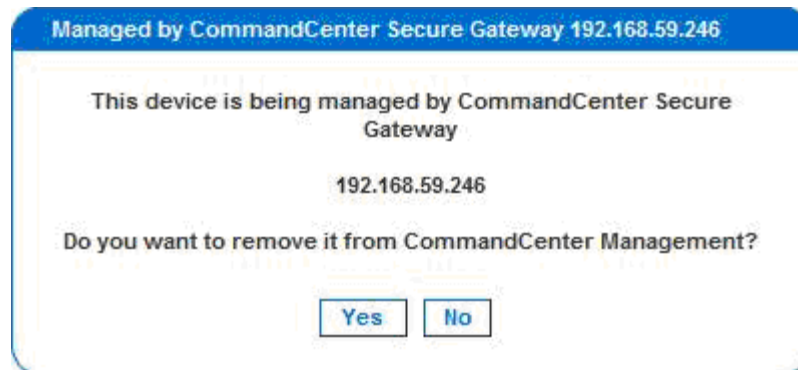
Sie können nur direkt auf das Gerät zugreifen, wenn die CC-SG-Steuerung von KX II-101-V2 aufgehoben wird. Wenn KX II-101-V2 jedoch keine Heartbeat-Nachrichten von CommandCenter empfängt (z. B. weil sich CommandCenter nicht im Netzwerk befindet), können Sie die CC-SG-Steuerung von KX II-101-V2 aufheben, 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.

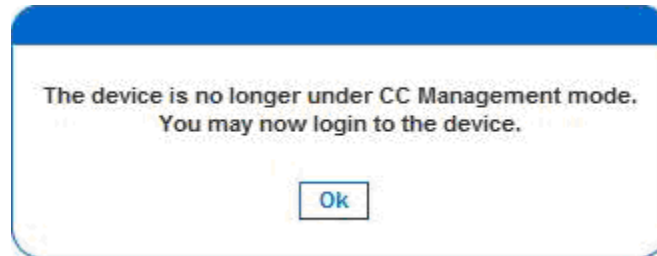


► **So heben Sie die CC-SG-Verwaltung des Geräts auf (Feature „CC UnManage“):**

1. Klicken Sie auf "Yes" (Ja). Sie werden aufgefordert, die Aktion zu bestätigen.



2. Klicken Sie auf "Yes" (Ja). Es wird eine Meldung mit der Bestätigung angezeigt, dass die CC-Verwaltung des Geräts aufgehoben wurde.



3. Klicken Sie auf "OK". Die KX II-101-V2-Anmeldeseite wird angezeigt.

---

## Verwenden von CC-SG im Proxymodus

Version des Virtual KVM Client nicht bekannt im CC-SG-Proxymodus

Wenn der Virtual KVM Client über CommandCenter Secure Gateway (CC-SG) im Proxymodus gestartet wird, ist die Version des Virtual KVM Client unbekannt. Im Dialogfeld **About Raritan Virtual KVM Client** (Informationen zum Raritan Virtual KVM Client) wird die Version als „Version Unknown“ (Version unbekannt) angezeigt.

Proxymodus und MPC

Wenn Sie KX II-101-V2 in einer CC-SG-Konfiguration verwenden, sollten Sie den CC-SG-Proxymodus nicht verwenden, wenn Sie den Multi-Platform-Client (MPC) verwenden möchten.

# Anhang A Technische Daten

## In diesem Kapitel

Physische Spezifikationen .....	213
Unterstützte Betriebssysteme (Clients) .....	214
Unterstützte Browser .....	215
Kabel.....	216
Zertifizierte Modems .....	216
Unterstützte Videoauflösungen .....	216
Unterstützte Tastatursprachen .....	218
Verwendete TCP- und UDP-Ports.....	219
Netzwerk-Geschwindigkeitseinstellungen .....	221
9-polige Pinbelegung.....	222

---

## Physische Spezifikationen

KX II-101-V2...	Beschreibung
Formfaktor	Formfaktor Null-U (0 Höhenheiten); vertikale oder horizontale Gestellmontage (Halterungen inklusive)
Abmessungen (T x B x H)	103 x 74 x 27mm
Gewicht	0.6498 lbs; 0.295 kg
Stromversorgung	Netzadapter (100-240V~/ 6VDC) oder Power over Ethernet (PoE); kompatibel mit IEEE 802.3af Mid-Span-Einspeisung Signalpaareinspeisung Stromversorgung eines Geräts über PoE der Klasse 2 (unter 7Wts)
Betriebstemperatur	0° C bis 40° C
Luftfeuchtigkeit	20% bis 85% relative Luftfeuchtigkeit
Anzeige: Blaues hintergrundbeleuchtetes RARITAN-Logo  Gelbe und grüne LED	Start- und Stromanzeige Anzeige für Netzwerkaktivität und Verbindungsgeschwindigkeit
Lokale Verbindung:	1 - Mini-USB-Port für USB-Tastatur/-Maus und Verbindung zu virtuellen Medien 1 - Mini-DIN9-Port für seriellen

KX II-101-V2...	Beschreibung
	Multifunktions-Port für alle RS-232-Funktionen, Modemverbindung und Dominion PX-Konnektivität
Remote-Verbindung: Netzwerk Protokolle	1 Ethernet (RJ45)-Port mit Anzeige für den Status der Netzwerkaktivität TCP/IP, TELNET, SSH, HTTP, HTTPS, Secure LDAP, RADIUS, LDAP, SNMP v2 und v3, DHCP und SNTP, Dual-Stack: IPv4 und IPv6
Garantie	2 Jahre mit erweitertem Austausch*

## Unterstützte Betriebssysteme (Clients)

Die folgenden Betriebssysteme werden auf dem Virtual KVM Client und dem Multi-Platform-Client (MPC) unterstützt:

Client-Betriebssystem	Unterstützung virtueller Medien (VM) auf dem Client?
Windows 7®	Yes (Ja)
Windows XP®	Yes (Ja)
Windows 2008®	Yes (Ja)
Windows Vista®	Yes (Ja)
Windows 2000® SP4-Server	Yes (Ja)
Windows 2003® Server	Yes (Ja)
Windows 2008® Server	Yes (Ja)
Red Hat® Desktop 5.0	Yes (Ja)
Red Hat Desktop 4.0	Yes (Ja)
Open SUSE 10, 11	Yes (Ja)
Fedora® 13 und 14	Yes (Ja)
Mac® OS	Yes (Ja)
Solaris™	Nein
Linux®	Ja, für ISO-Abbilder

Das JRE™-Plug-in ist für Windows® 32-Bit- und 64-Bit-Betriebssysteme verfügbar. MPC und VKC können nur über einen 32-Bit-Browser und die 64-Bit-Browser IE7 oder IE8 gestartet werden.

Im Folgenden werden die Anforderungen von Java™ unter den Windows-Betriebssystemen (32 und 64 Bit) aufgelistet:

Modus	Betriebssystem	Browser
Windows x64 32-Bit-Modus	Windows XP®	<ul style="list-style-type: none"> <li>• Internet Explorer® 6.0 SP1+ oder 7.0, IE 8</li> <li>• Firefox® 1.06 – 4 oder höher</li> </ul>
	Windows Server 2003®	<ul style="list-style-type: none"> <li>• Internet Explorer 6.0 SP1++, IE 7, IE 8</li> <li>• Firefox 1.06 – 3</li> </ul>
	Windows Vista®	<ul style="list-style-type: none"> <li>• Internet Explorer 7.0 oder 8.0</li> </ul>
	Windows 7®	<ul style="list-style-type: none"> <li>• Internet Explorer 9.0</li> <li>• Firefox 1.06 – 4 oder höher</li> </ul>
Windows x64 64-Bit-Modus	Windows XP	64-Bit-Betriebssystem, 32-Bit-Browser:
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	64-Bit-Modus, 64-Bit-Browser:
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	
		<ul style="list-style-type: none"> <li>• Internet Explorer 7.0 oder 8.0</li> </ul>

---

## Unterstützte Browser

KX II-101-V2 unterstützt die folgenden Browser:

- Internet Explorer® 7 bis 9
- Firefox® 4 oder höher
- Safari® 3 oder höher



## Kabel

Schnittstellentyp	Länge		Beschreibung
	Zoll	Zentimeter	
KVM-Kabel mit PS/2- und USB-Anschluss	15"	38 cm	Integriertes Kabel
Mini-DIN9 (M) zu DB9 (F)	72"	182 cm	Serielles Kabel
DKX2-101-V2-PDU (optional)	70.86"	180 cm	Kabel für die Verbindung mit einer Dominion PX-Einheit

## Zertifizierte Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

## Unterstützte Videoauflösungen

Stellen Sie sicher, dass die Videoauflösung und die Aktualisierungsfrequenz aller Zielsever von KX II-101-V2 unterstützt werden und das Signal keinen Zeilensprung beinhaltet.

Die Videoauflösung und die Kabellänge sind wichtige Faktoren für die Maussynchronisierung.

Die folgenden Auflösungen werden von KX II-101-V2 unterstützt:

Auflösungen	
640 x 350 bei 70Hz	1024 x 768 bei 85Hz
640 x 350 bei 85Hz	1024 x 768 bei 75Hz
640 x 400 bei 56Hz	1024 x 768 bei 90Hz
640 x 400 bei 84Hz	1024 x 768 bei 100Hz
640 x 400 bei 85Hz	1152 x 864 bei 60Hz
640 x 480 bei 60Hz	1152 x 864 bei 70Hz

Auflösungen	
640 x 480 bei 66,6Hz	1152 x 864 bei 75Hz
640 x 480 bei 72Hz	1152 x 864 bei 85Hz
640 x 480 bei 75Hz	1.152 x 870 bei 75,1Hz
640 x 480 bei 85Hz	1.152 x 900 bei 66Hz
720 x 400 bei 70Hz	1.152 x 900 bei 76Hz
720 x 400 bei 84Hz	1.280 x 720 bei 60Hz
720 x 400 bei 85Hz	1.280 x 960 bei 60Hz
800 x 600 bei 56Hz	1.280 x 960 bei 85Hz
800 x 600 bei 60Hz	1280 x 1024 bei 60Hz
800 x 600 bei 70Hz	1280 x 1024 bei 75Hz
800 x 600 bei 72Hz	1280 x 1024 bei 85Hz
800 x 600 bei 75Hz	1.360 x 768 bei 60Hz
800 x 600 bei 85Hz	1.366 x 768 bei 60Hz
800 x 600 bei 90Hz	1.368 x 768 bei 60Hz
800 x 600 bei 100Hz	1.400 x 1050 bei 60Hz
832 x 624 bei 75,1Hz	1.440 x 900 bei 60Hz
1024 x 768 bei 60Hz	1600 x 1200 bei 60Hz
1024 x 768 bei 70Hz	1.680 x 1.050 bei 60Hz
1024 x 768 bei 72Hz	1920 x 1080 bei 60Hz

---

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

*Hinweis: Einige Auflösungen stehen standardmäßig nicht zur Verfügung. Wird eine Auflösung nicht angezeigt, stecken Sie zuerst den Monitor an, stecken Sie den Monitor wieder aus und anschließend das CIM ein.*

*Hinweis: Werden die Auflösungen 1440 x 900 und 1680 x 1050 nicht angezeigt, jedoch von der Grafik-Adapterkarte des Zielservers unterstützt, ist möglicherweise ein DDC-1440- oder DDC-1680-Adapter erforderlich.*

---

## Unterstützte Tastatursprachen

KX II-101-V2 bietet Tastaturunterstützung für die in der folgenden Tabelle aufgeführten Sprachen.

Sprache	Regionen	Tastaturlayout
US English (Englisch USA)	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. Kanada, Australien und Neuseeland.	US-amerikanisches Tastaturlayout
US English International (Englisch USA/International)	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. die Niederlande.	US-amerikanisches Tastaturlayout
UK English (Englisch Großbritannien)	United Kingdom (Großbritannien)	Englisches Tastaturlayout (Großbritannien)
Chinese Traditional (Traditionelles Chinesisch)	Hongkong, Republik China (Taiwan)	Chinese Traditional (Traditionelles Chinesisch)
Chinese Simplified (Vereinfachtes Chinesisch)	Festland der Volksrepublik China	Chinese Simplified (Vereinfachtes Chinesisch)
Korean (Koreanisch)	Südkorea	Dubeolsik Hangul
Japanese (Japanisch)	Japan	JIS-Tastatur (Japanischer Branchenstandard)
French (Französisch)	Frankreich	Französisches (AZERTY-)Tastaturlayout
German (Deutsch)	Deutschland und Österreich	Deutsche Tastatur (QWERTZ-Layout)
French (Französisch)	Belgien	Belgian (Belgisch)
Norwegian (Norwegisch)	Norwegen	Norwegian (Norwegisch)

<b>Sprache</b>	<b>Regionen</b>	<b>Tastaturlayout</b>
Danish (Dänisch)	Dänemark	Danish (Dänisch)
Swedish (Schwedisch)	Schweden	Swedish (Schwedisch)
Hungarian (Ungarisch)	Ungarn	Hungarian (Ungarisch)
Slovenian (Slowenisch)	Slowenien	Slovenian (Slowenisch)
Italian (Italienisch)	Italien	Italian (Italienisch)
Spanish (Spanisch)	Spanien und die meisten spanischsprachigen Länder	Spanish (Spanisch)
Portuguese (Portugiesisch)	Portugal	Portuguese (Portugiesisch)

---

## Verwendete TCP- und UDP-Ports

Port	Beschreibung
HTTP, Port 80	Dieser Port kann bei Bedarf konfiguriert werden. Siehe <b>HTTP- und HTTPS-Porteinstellungen</b> (auf Seite 127). Alle von KX II-101-V2 über HTTP (Port 80) empfangenen Anforderungen werden standardmäßig zur Gewährleistung der Sicherheit automatisch an HTTPS weitergeleitet. KX II-101-V2 beantwortet Anforderungen aus Gründen der Benutzerfreundlichkeit über Port 80. Auf diese Weise müssen Benutzer für den Zugriff auf KX II-101-V2 im URL-Feld keine Eingaben vornehmen. Die Sicherheit ist jedoch vollständig gewährleistet.
HTTPS, Port 443	Dieser Port kann bei Bedarf konfiguriert werden. Siehe <b>HTTP- und HTTPS-Porteinstellungen</b> (auf Seite 127). Dieser Port wird standardmäßig für verschiedene Zwecke verwendet, z. B. für den Webserver des HTML-Clients, das Herunterladen von Clientsoftware (MPC/VKC) auf den Clienthost oder die Übertragung von KVM- oder virtuellen Mediendatenströmen zum Client.
KX II-101-V2-Protokoll (Raritan KVM-über-IP), konfigurierbarer Port 5000	Dieser Port wird zur Erkennung anderer Dominion-Geräte und zur Kommunikation zwischen Raritan-Geräten und -Systemen verwendet, einschließlich CC-SG für Geräte, für die die CC-SG-Verwaltung verfügbar ist. Standardmäßig ist der Port 5000 eingestellt. Sie können jedoch jeden anderen TCP-Port konfigurieren, der nicht verwendet wird. Informationen zum Konfigurieren dieser Einstellung finden Sie unter <b>Netzwerkeinstellungen</b> (siehe " <b>Network Settings (Netzwerkeinstellungen)</b> " auf Seite 120).
SNTP (Zeitserver) über den konfigurierbaren UDP-Port 123	KX II-101-V2 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. <b>///Optional</b>
LDAP/LDAPS über den konfigurierbaren Port 389 oder 936	Wenn KX II-101-V2 zur Remoteauthentifizierung von Benutzeranmeldungen über das LDAP-/LDAPS-Protokoll konfiguriert ist, wird Port 389 oder 636 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. <b>Optional</b>
RADIUS über den konfigurierbaren Port 1812	Wenn KX II-101-V2 zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist, wird Port 1812 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. <b>Optional</b>
RADIUS-Kontoführung über den konfigurierbaren Port 1813	Wenn KX II-101-V2 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	Wenn KX II-101-V2 zum Senden von Meldungen an einen Syslog-Server konfiguriert ist, werden die angegebenen Ports für die


UDP-Port 514	Kommunikation verwendet (verwendet UDP-Port 514).
SNMP-Standard-UDP-Ports	Port 161 wird für eingehende/ausgehende SNMP-Lese- und -Schreibvorgänge, Port 162 für ausgehenden Datenverkehr für SNMP-Traps verwendet. <b>///Optional</b>
TCP-Port 22	Port 22 wird für die Kommandozeilenschnittstelle des KX II-101-V2 verwendet (wenn Sie mit dem technischen Kundendienst von Raritan zusammenarbeiten).

## Netzwerk-Geschwindigkeitseinstellungen


### Netzwerk-Geschwindigkeitseinstellung von KX II-101-V2

Porteinstellung Netzwerk- switch	Automatisch	100/Voll	100/Halb	10/Voll	10/Halb
<b>Automatisch</b>	Höchste verfügbare Geschwindigkeit	KX II-101-V2: 100/Voll Switch: 100/Halb	100/Halb	KX II-101-V2: 10/Voll Switch: 10/Halb	10/Halb
<b>100/Voll</b>	KX II-101-V2: 100/Halb Switch: 100/Voll	100/Voll	KX II-101-V2: 100/Halb Switch: 100/Voll	Keine Kommunikation	Keine Kommunikation
<b>100/Halb</b>	100/Halb	KX II-101-V2: 100/Voll Switch: 100/Halb	100/Halb	Keine Kommunikation	Keine Kommunikation
<b>10/Voll</b>	KX II-101-V2: 10/Halb Switch: 10/Voll	Keine Kommunikation	Keine Kommunikation	10/Voll	KX II-101-V2: 10/Halb Switch: 10/Voll
<b>10/Halb</b>	10/Halb	Keine Kommunikation	Keine Kommunikation	KX II-101-V2: 10/Voll Switch: 10/Halb	10/Halb

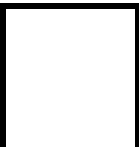
Legende:

 Funktioniert nicht wie erwartet

 Unterstützt

 Funktionen; nicht empfohlen

 NICHT von Ethernet-Spezifikationen unterstützt; Produkt kommuniziert, es treten allerdings Kollisionen auf.

 Laut Ethernet-Spezifikation sollte hier "Keine Kommunikation" gelten, beachten Sie jedoch, dass das Verhalten des KX II-101-V2 vom erwarteten Verhalten abweicht.

---

*Hinweis: Um eine zuverlässige Netzwerkkommunikation zu erhalten, konfigurieren Sie LAN-Schnittstellengeschwindigkeit und Duplex für KX II-101-V2 und den LAN-Switch auf den gleichen Wert. Konfigurieren Sie beispielsweise KX II-101-V2 und den LAN-Switch auf "Autodetect" (Automatische Erkennung, empfohlen) oder stellen Sie sie auf ein(e) feste(s) Geschwindigkeit/Duplex wie 100MB/s/Voll.*

---

---

## 9-polige Pinbelegung

Beschreibung des Pols	
1	DTR (aus)
2	TXD (aus)
3	RXD (ein)
4	DCD/DSR (ein) *
5	GND
6	DTR (aus)
7	CTS (ein)
8	RTS (aus)
9	RI (ein)





## Anhang B Aktualisieren des LDAP-Schemas

---

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

---

### In diesem Kapitel

Zurückgeben von Benutzergruppeninformationen .....	224
Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen .....	225
Erstellen eines neuen Attributs.....	225
Hinzufügen von Attributen zur Klasse .....	227
Aktualisieren des Schemacache .....	228
Bearbeiten von rciusergroup-Attributen für Benutzermitglieder .....	229

---

### Zurückgeben von Benutzergruppeninformationen

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

---

#### Von LDAP

Wenn eine LDAP/LDAPS-Authentifizierung erfolgreich ist, bestimmt KX II-101-V2 die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers. Ihr Remote-LDAP-Server kann diese Benutzergruppennamen bereitstellen, indem er ein wie folgt benanntes Attribut zurückgibt:

rciusergroup                      attribute type: string

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

---

#### Von Microsoft Active Directory

---

*Hinweis: Diese Aktualisierung sollte nur von einem erfahrenen Active Directory®-Administrator durchgeführt werden.*

---

Die Rückgabe von Benutzergruppeninformationen von Microsoft® Active Directory für Windows 2000®-Server erfordert die Aktualisierung des LDAP-/LDAPS-Schemas. Weitere Informationen finden Sie in Ihrer Microsoft-Dokumentation.

1. Installieren Sie das Schema-Plug-in für Active Directory. Entsprechende Anweisungen finden Sie in der Dokumentation für Microsoft Active Directory.

2. Starten Sie Active Directory Console und wählen Sie "Active Directory Schema" (Active Directory-Schema) aus.

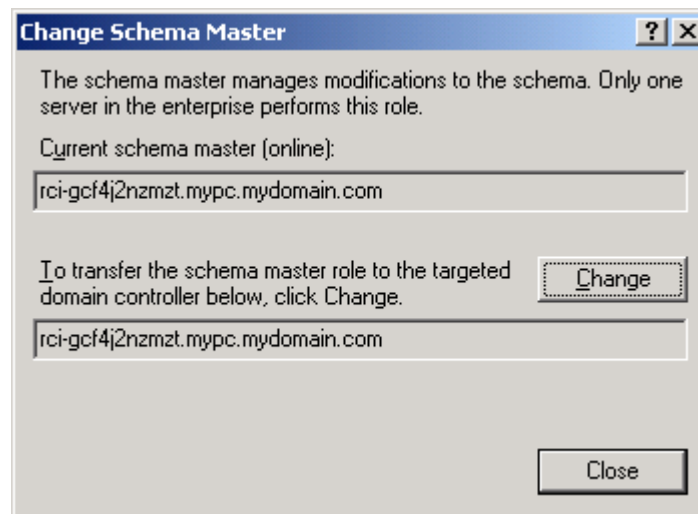
---

## Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen

Um einem Domänencontroller das Schreiben im Schema zu erlauben, müssen Sie einen Registrierungseintrag erstellen, der Schemaaktualisierungen zulässt.

► **So lassen Sie Schreibvorgänge im Schema zu:**

1. Klicken Sie mit der rechten Maustaste auf den Stammknoten des Active Directory® Schema im linken Fensterbereich, und wählen Sie "Operations Master" (Betriebsmaster) aus dem Kontextmenü aus. Das Dialogfeld **Change Schema Master** (Schemamaster ändern) wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen "Schema can be modified on this Domain Controller" (Schema kann auf diesem Domänencontroller geändert werden). **///Optional**
3. Klicken Sie auf "OK".

---

## Erstellen eines neuen Attributs

► **So erstellen Sie neue Attribute für die Klasse "rciusergroup":**

1. Klicken Sie im linken Fensterabschnitt auf das +-Symbol vor Active Directory® Schema.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Attributes" (Attribute).

3. Klicken Sie auf "New" (Neu) und wählen Sie "Attribute" (Attribut) aus. Klicken Sie im angezeigten Hinweisfenster auf "Continue" (Weiter). Das Dialogfeld "Create New Attribute" (Neues Attribut erstellen) wird geöffnet.

**Create New Attribute**

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

Multi-Valued

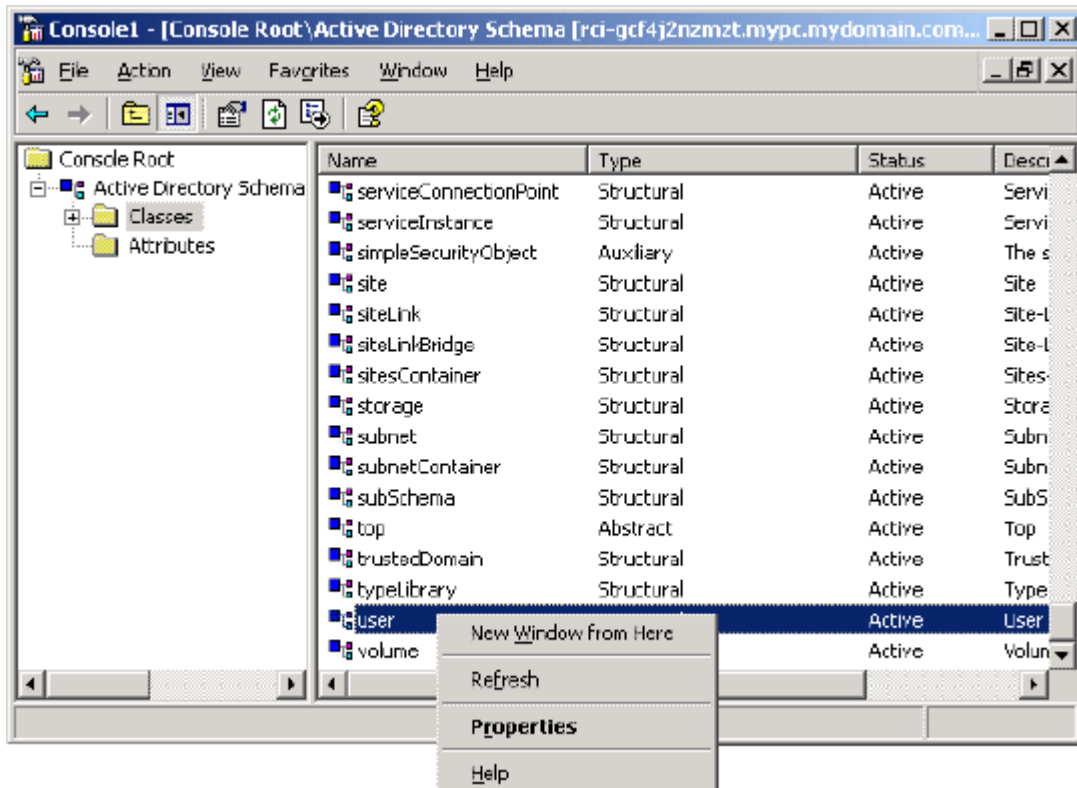
OK Cancel

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

## Hinzufügen von Attributen zur Klasse

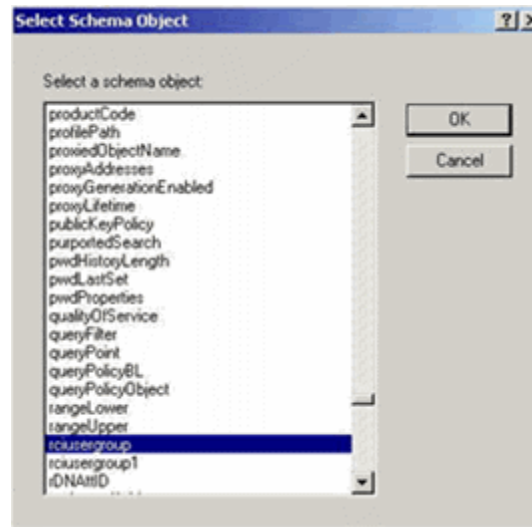
### ► So fügen Sie der Klasse Attribute hinzu:

1. Klicken Sie im linken Fensterbereich auf "Classes" (Klassen).
2. Suchen Sie im rechten Fensterbereich den Wert "User Class" (Benutzerklasse) und klicken Sie mit der rechten Maustaste darauf.



3. Wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü. Das Dialogfeld "User Properties" (Benutzereigenschaften) wird geöffnet.
4. Klicken Sie auf die Registerkarte "Attributes" (Attribute), um diese zu öffnen.
5. Klicken Sie auf "Add" (Hinzufügen).

- Wählen Sie in der Liste "Select Schema Object" (Schemaobjekt auswählen) den Eintrag "rciusergroup" aus.



- Klicken Sie im Dialogfeld "Select Schema Object" (Schemaobjekt auswählen) auf OK.
- Klicken Sie im Dialogfeld "User Properties" (Benutzereigenschaften) auf OK.

---

## Aktualisieren des Schemacache

► **So aktualisieren Sie den Schemacache:**

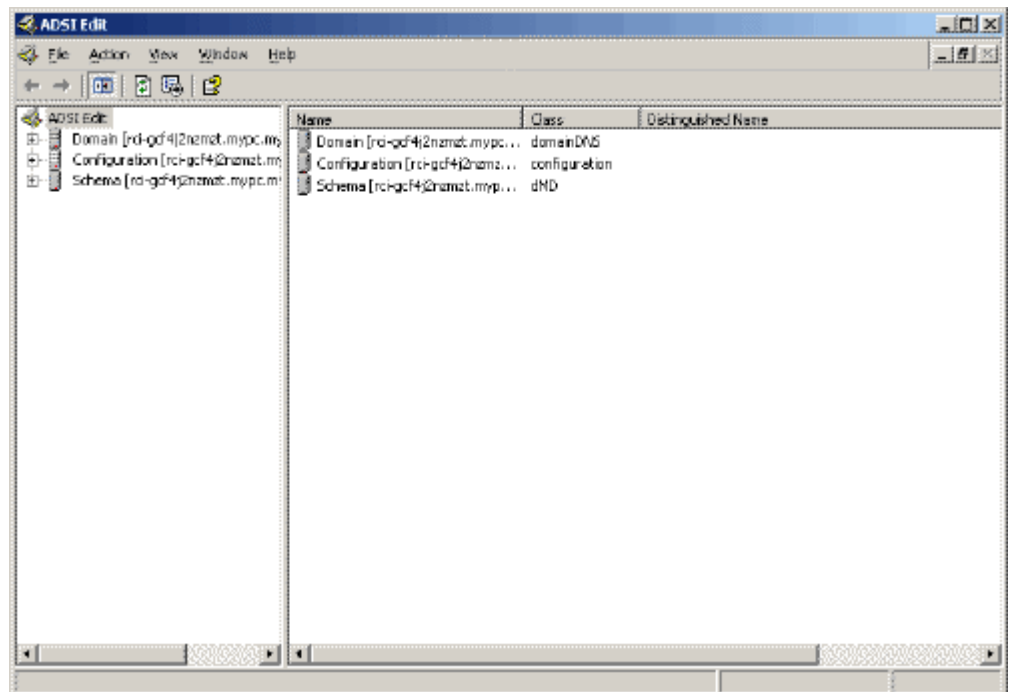
- Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Active Directory® Schema", und wählen Sie "Reload the Schema" (Schema neu laden) aus.
- Minimieren Sie die Active Directory-Schema-MMC-Konsole (Microsoft® Management Console).

## Bearbeiten von rcusergroup-Attributen für Benutzermitglieder

Verwenden Sie zum Ausführen des Active Directory®-Skripts auf einem Windows 2003®-Server das von Microsoft® bereitgestellte Skript (verfügbar auf der Windows 2003-Serverinstallations-CD). Diese Skripts werden bei der Installation von Microsoft® Windows 2003 mit installiert. ADSI (Active Directory Service Interface) fungiert hierbei als Low-Level-Editor für Active Directory und ermöglicht so das Durchführen allgemeiner Verwaltungsaufgaben wie Hinzufügen, Löschen und Verschieben von Objekten mit einem Verzeichnisdienst.

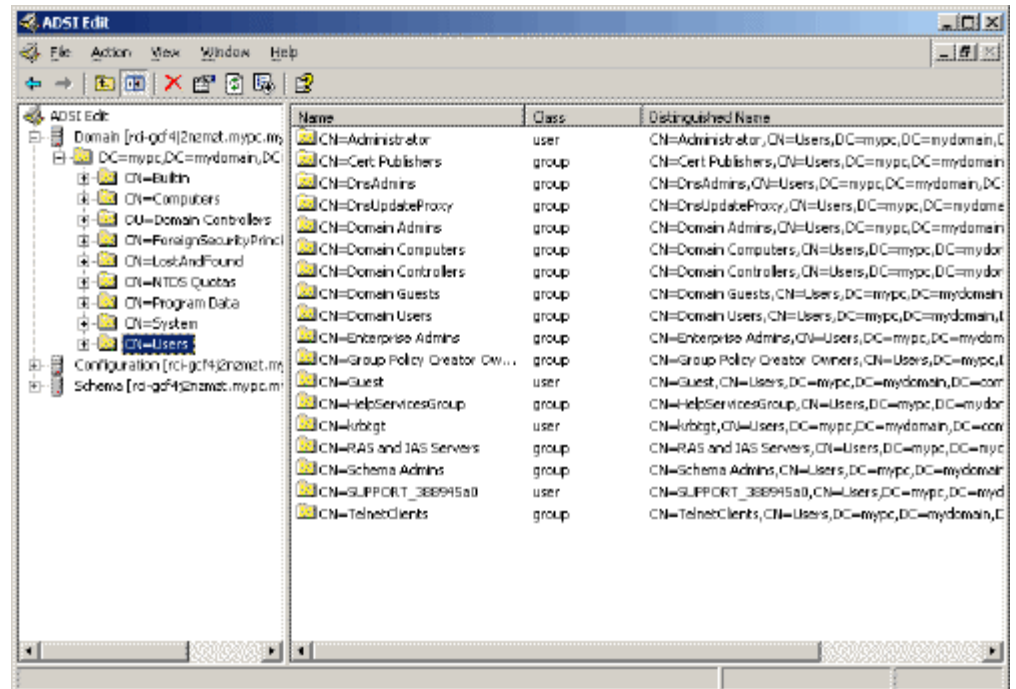
► **So bearbeiten Sie die einzelnen Benutzerattribute innerhalb der Gruppe "rcusergroup":**

1. Wählen Sie auf der Installations-CD "Support" > "Tools" aus.
2. Doppelklicken Sie zur Installation der Support-Tools auf "SUPTOOLS.MSI".
3. Wechseln Sie zum Installationsverzeichnis der Support-Tools. Führen Sie "adsiedit.msc" aus. Das Fenster "ADSI Edit" (ADSI-Bearbeitung) wird angezeigt.



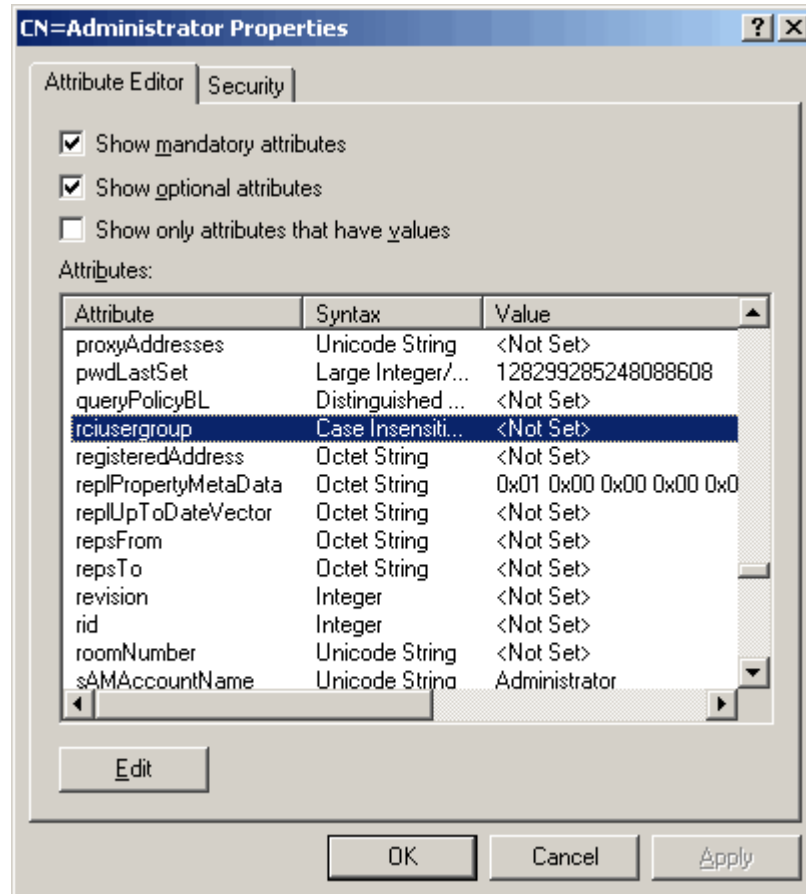
4. Öffnen Sie die Domäne.

5. Klicken Sie im linken Fensterbereich auf den Ordner "CN=Users" (CN=Benutzer).

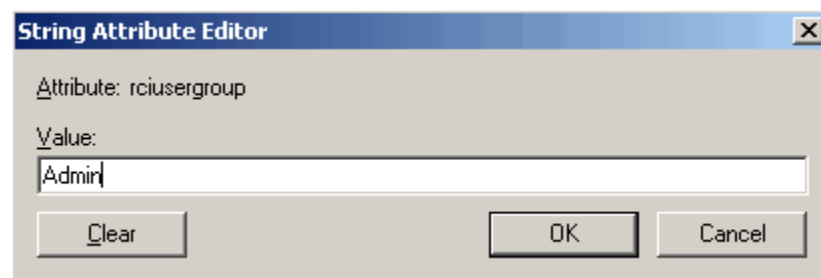


6. Navigieren Sie im rechten Fensterbereich zu dem Namen des Benutzers, dessen Eigenschaften geändert werden sollen. Klicken Sie mit der rechten Maustaste auf den Benutzernamen, und wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü aus.

7. Klicken Sie auf die Registerkarte "Attribute Editor" (Attributeditor), um sie anzuzeigen, wenn sie noch nicht geöffnet ist. Wählen Sie in der Liste "Attributes" (Attribute) "rciusergroup" aus.



8. Klicken Sie auf "Edit" (Bearbeiten). Das Dialogfeld "String Attribute Editor" (Attributeditor für Zeichenfolgen) wird angezeigt.
9. Geben Sie die Benutzergruppe (erstellt in KX II-101-V2) in das Feld "Edit Attribute" (Attribut bearbeiten) ein. Klicken Sie auf OK.





## Anhang C Gestellmontage

Das KX II-101-V2-Gerät kann vertikal oder horizontal mit der Vorder- oder Rückseite nach vorne zeigend auf beiden Seiten des Servergestells montiert werden. Verwenden Sie die im KX II-101-V2-Kit enthaltenen Halterungen und Schrauben.

### In diesem Kapitel

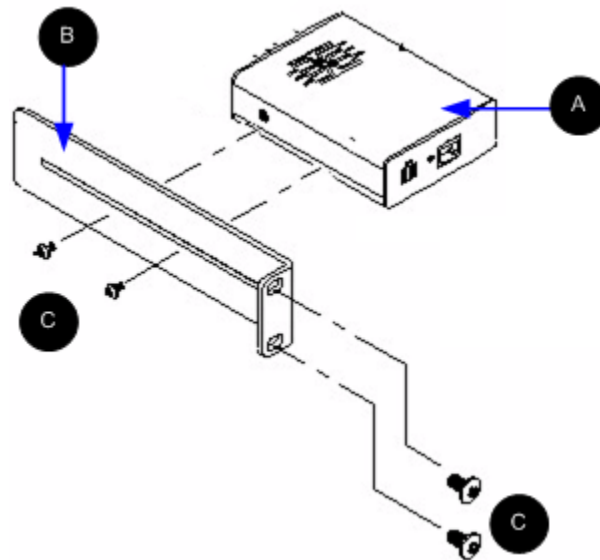
L-Halterung an KX II-101-V2 zur horizontalen Montage anbringen .....232

---

#### L-Halterung an KX II-101-V2 zur horizontalen Montage anbringen

1. Bringen Sie die L-Halterung an KX II-101-V2 mit den im Lieferumfang enthaltenen Schrauben an. Richten Sie die Halterungen vor dem Festziehen der Schrauben aus.
2. Befestigen Sie die L-Halterung mit den vom Gestellhersteller bereitgestellten Schrauben zur Gestellmontage am Gestell.

In der folgenden Abbildung ist die Befestigung von KX II-101-V2 auf der linken Seite des Gestells dargestellt. Befolgen Sie diese Anleitungen auch, um das KX II-101-V2-Gerät auf der rechten Gestellseite zu befestigen. Bringen Sie dabei jedoch die Halterungen auf der rechten Seite von KX II-101-V2 an.



#### Diagrammschlüssel

	KX II-101-V2
---	--------------

Diagrammschlüssel	
	L-Halterung
	Schrauben

## Anhang D Wichtige Hinweise

### In diesem Kapitel

Java Runtime Environment (JRE) .....	234
Hinweise zur Unterstützung von IPv6 .....	235
Hinweise zu Tastatur, Video und Maus .....	235
CC-SG .....	238

---

### Java Runtime Environment (JRE)

---

**Wichtig: Sie sollten die Zwischenspeicherung für Java™ deaktivieren und den Java-Cache leeren. Weitere Informationen finden Sie in der Java-Dokumentation oder im Benutzerhandbuch "KVM and Serial Access Clients Guide".**

---

Für die Remotekonsole LX, KX II, KX II-101 und KX II-101-V2 und den MPC ist Java Runtime Environment™ (JRE™) erforderlich, da die Remotekonsole die Java-Version überprüft. Falls die Version falsch oder veraltet ist, werden Sie dazu aufgefordert, eine kompatible Version herunterzuladen.

Raritan empfiehlt zur Gewährleistung einer optimalen Leistung die Verwendung von JRE Version 1.7. Die Remotekonsole und der MPC funktionieren jedoch auch mit JRE Version 1.6.x oder höher (mit Ausnahme von 1.6.2).

---

*Hinweis: Damit mehrsprachige Tastaturen in der Remotekonsole LX, KX II, KX II-101 und KX II-101-V2 (Virtual KVM Client) funktionieren, müssen Sie die mehrsprachige Version von JRE installieren.*

---

---

## Hinweise zur Unterstützung von IPv6

---

### Hinweise zur Unterstützung des Betriebssystems IPv6

#### Java

Java™ 1.6 unterstützt IPv6 bei folgenden Produkten:

- Solaris™ 10 (und höher)
- Linux® Kernel 2.1.2 (und höher)/RedHat 6.1 (und höher)

Die folgenden IPv6-Konfigurationen werden *nicht* von Java unterstützt:

- J2SE unterstützt kein IPv6 auf Microsoft® Windows®.

#### Linux

- Es wird empfohlen, bei Nutzung von IPv6 Linux Kernel 2.4.0 oder höher zu verwenden.
- Ein IPv6-aktivierter Kernel muss installiert werden, oder der Kernel muss mit aktivierten IPv6-Optionen wiederhergestellt werden.
- Bei der Verwendung von IPv6 und Linux müssen außerdem einige Netzwerkdienste installiert werden. Weitere Informationen finden Sie unter <http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html>.

#### Windows

- Windows XP- und Windows 2003-Benutzer müssen Microsoft Service Pack für IPv6 installieren, um IPv6 zu aktivieren.

#### Mac Leopard

- Die KX II-Version 2.0.20 unterstützt für Mac® Leopard® kein IPv6.

---

## Hinweise zu Tastatur, Video und Maus

Die folgende Ausrüstung ist auf einige Tastaturen, Videos oder Mäuse beschränkt. Es wird ggf. eine Umgebungslösung bereitgestellt.

---

## Einschränkungen bezüglich Video Sun Blade, Tastatur und Mausunterstützung

### Video

Wenn Sie auf ein Sun™ Blade 100 mit einem KX II-101-V2 zugreifen, funktionieren das Video auf dem lokalen Port oder eine Remote-Verbindung möglicherweise nicht richtig, wenn das Sun Blade hochfährt. Um dieses Problem zu umgehen, sollten Sie die Firmware Sun Open Boot 4.17.1 (oder höher) verwenden.

### Tastatur und Maus

Da von Sun Blades nicht mehrere Tastaturen unterstützt werden und keine lokale Tastatur bzw. kein lokaler Mausport bereitgestellt wird, kann KX II-101-V2 nicht zeitgleich mit einer lokalen Tastatur verwendet werden. Eine Remote-Tastatur und -Maus können jedoch für Sun Blades verwendet werden.

---

## Eingeschränkter BIOS-Zugriff von einer lokalen Tastatur

Bei der Verwendung des Mausmodus "Absolute Mouse Synchronisation" (Absolute Maussynchronisierung) wird eine USB-Verbindung benötigt. Die Tastaturen in diesem Bereich unterstützen jedoch keine USB-Verbindung zu der lokalen Tastatur. Um über das BIOS Zugriff auf die lokale Tastatur oder über den lokalen Port auf virtuelle Medien zu erhalten, führen Sie folgende Konfigurationen durch:

Tastatur	Zu verwendende Konfiguration
Dell® OptiPlex™ GX280 - BIOS A03	Für lokale und Remote-Tastaturen kann auf BIOS und virtuelle Medien mithilfe eines Newlink USB-bis PS/2-Adapters zugegriffen werden.  Stellen Sie die Hostschnittstelle auf der Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten) auf PS/2 ein. Siehe <b>Tastatur/Maus einrichten</b> (siehe " <b>Keyboard/Mouse Setup (Tastatur/Maus einrichten)</b> " auf Seite 131).
Dell Dimension 2400– BIOS A05	Stellen Sie die Hostschnittstelle auf der Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten) auf PS/2 ein. Siehe <b>Tastatur/Maus einrichten</b> (siehe " <b>Keyboard/Mouse Setup (Tastatur/Maus einrichten)</b> " auf Seite 131).
Dell Optiplex 170L - BIOS A07	PS/2 und ein PS/2-bis-USB-Adapter.  Stellen Sie die Hostschnittstelle auf der Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten) auf PS/2 ein. Siehe <b>Tastatur/Maus einrichten</b> (siehe " <b>Keyboard/Mouse Setup (Tastatur/Maus einrichten)</b> " auf Seite 131).

Tastatur	Zu verwendende Konfiguration
Dell Server 1850	<p>Damit die BIOS-Version A06 ein über virtuelle Medien installiertes USB-Wechsellaufwerk erkennt, verwenden Sie die PS/2- and USB-Anschlüsse zwischen dem Dell-Server und KX II-101-V2.</p> <p>Stellen Sie die Hostschnittstelle auf der Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten) auf PS/2 ein. Siehe <b>Tastatur/Maus einrichten</b>) (siehe "<b>Keyboard/Mouse Setup (Tastatur/Maus einrichten)</b>" auf Seite 131).</p>

---

### HP UX RX 1600 – Tastatur- und Mauskonfiguration

Wenn Sie ein HP® UX RX 1600 mit UNIX® verwenden, gehen Sie wie folgt vor, um das Gerät mit dem Ziel zu verbinden:

- Vergewissern Sie sich, dass Sie die Firmware KX II-101-V2 2.0.20.5.6964 (oder höher) verwenden.
- Verwenden Sie das USB-Kabel, das im Lieferumfang von KX II-101-V2 enthalten ist.
- Stellen Sie auf der Seite "Keyboard/Mouse Setup" (Tastatur/Maus einrichten) das Feld "Host Interface" (Hostschnittstelle) auf "USB" ein. Siehe **Tastatur/Maus einrichten**) (siehe "**Keyboard/Mouse Setup (Tastatur/Maus einrichten)**" auf Seite 131).
- Vergewissern Sie sich, dass auf der Seite "Port" die Kontrollkästchen "Enable Absolute Mouse" (Absoluten Mausmodus aktivieren) und "Use Full Speed" (Volle Geschwindigkeit verwenden) deaktiviert sind.
- Verwenden Sie entweder den Mausmodus "Intelligent" oder "Standard". Verwenden Sie nicht den Mausmodus "Absolute" (Absolut).

---

### Compaq Alpha und IBM P Server – Einschränkungen beim Mausmodus

Wenn Sie über das KX II-101-V2-Gerät eine Verbindung zu Compaq® Alpha-Servern oder IBM® P-Servern herstellen, müssen Sie den Mausmodus "Single" (Ein-Cursor) verwenden. Siehe **Arbeiten mit Zielservers** (auf Seite 39).

---

### **Server "Windows 2000" und "Windows 2003" – Tastatureinschränkungen**

Aufgrund einer das Betriebssystem betreffenden Einschränkung funktionieren die folgenden Tastaturkombinationen nicht mit einem amerikanischen Tastaturlayout (US-International), wenn ein Windows 2000®-Betriebssystem und die Windows 2003®-Server verwendet werden.

- Rechte Alt-Taste +D
- Rechte Alt-Taste+I
- Rechte Alt-Taste+L

---

*Hinweis: Die rechte Alt-Taste ist möglicherweise als "AltGr" auf solchen Tastaturen gekennzeichnet, die über spezielle US/International-Kennzeichnungen auf den Tasten verfügen.*

---

---

## **CC-SG**

---

### **Proxymodus und MPC**

Wenn Sie den KX II in einer CC-SG-Konfiguration verwenden, sollten Sie den CC-SG-Proxymodus nicht verwenden, wenn Sie den Multi-Platform-Client (MPC) nutzen möchten.

## Anhang E Häufig gestellte Fragen (FAQs)

### In diesem Kapitel

Allgemeine FAQs.....	239
IPv6-Netzwerk .....	241

### Allgemeine FAQs

Frage	Antwort
Was ist der Unterschied zwischen Dominion KX II-101-V2 und der vorherigen Generation Dominion KX II-101? ?	Das Dominion KX II-101-V2 ist die neueste Generation eines preisgünstigen Modells. Das V2 unterstützt fast alle Funktionen der früheren Generation Dominion KX II-101, sowie viele weitere interessante Funktionen. Die V2-Version unterstützt keine Power-over-Ethernet-Verbindung und auch keinen lokalen PS2-Port.
Wie funktioniert das Dominion KX II-101-V2?	Dominion KX II-101-V2 wird an den Tastatur-, Video- und Mausports eines Servers angeschlossen. Es fängt das Videosignal ein, digitalisiert und komprimiert es, bevor es mithilfe des leistungsstarken Frame-Grabbers sowie der Kompressionstechnologie von Raritan übertragen wird. Dominion KX II-101-V2 verfügt aufgrund seiner intuitiven Benutzeroberfläche über vielfältige Funktionen. Es kann ebenfalls mit anderen Verwaltungsgeräten über CommandCenter® Secure Gateway zentral verwaltet werden.
Welche Computer können durch das Dominion KX II-101-V2-Gerät ferngesteuert werden?	Dominion KX II-101-V2 arbeitet unabhängig von der Hardware, dem Betriebssystem oder der Anwendungssoftware eines Zielservers, indem es auf die wichtigsten Eingangs-/Ausgangsgeräte des Servers zugreift: Tastatur, Monitor und Maus. Daher kann sowohl jegliche Hardware, die von einer PC-Standardtastatur und von Standard-Maussschnittstellen unterstützt wird, als auch ein PC-Standardmonitor (VGA) mit Dominion KX II-101-V2 verwendet werden.
Gibt es Sicherheitsfunktionen, die meine Zielserver vor nicht autorisierten Remote-Verbindungen schützt?	Ja. Das KX II-101-V2 bietet eine Vielzahl von Sicherheitsfunktionen – eine Verbindungsauthentifizierung und Datenübertragung während eines Fernzugriffs. Benutzernamen, Passwörter und private Schlüssel werden zur Authentifizierung von Benutzern verwendet. Dominion KX101-V2 kann Benutzer über die Datenbank authentifizieren, die sich lokal auf dem Dominion KX101-V2 befindet, oder über externe AAA-Server (LDAP, Active Directory® oder RADIUS). Alle Tastatur-, Monitor- und Mausdaten werden mit bis zu 256-bit AES verschlüsselt.
Welche Arten virtueller Medien unterstützt der Dominion KX II-101-V2?	Folgende Medienarten werden von Dominion KX II-101-V2 unterstützt: interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und Remotelaufwerke für Bilder.
Sind virtuelle Medien sicher?	Ja. Virtuelle Mediensitzungen werden durch eine 256-bit-AES-Verschlüsselung abgesichert.



Frage	Antwort
Hat der KX2-101-V2 einen lokalen Port?	Ja, er hat einen lokalen VGA/USB-Port, es ist jedoch kein lokales Portkabel erforderlich. Um lokal auf den verbundenen Server zugreifen zu können, schließen Sie Ihren LCD-Monitor an den lokalen VGA-Port des KX2-101-V2 an. Verbinden Sie die USB-Tastatur und -Maus direkt mit dem Zielsystem.
Welche neuen Funktionen sind in der neuesten Version verfügbar?	Ab Version 3.5 sind ab sofort folgende Funktionen verfügbar: <ul style="list-style-type: none"><li>• Videoauflösung von 1920x1080</li><li>• iPad/iPhone-Zugriff (CC-SG erforderlich)</li><li>• Dual-Stack IPv6</li><li>• Verschlüsselungsmodul FIPS 140-2</li><li>• Abmelden eines Benutzers und Trennen der Portverbindung</li><li>• SNMPv3</li><li>• Zusätzliche Unterstützung für virtuelle Medien von Linux und Mac-Clients</li><li>• Unterstützung von Benutzeroberflächen in Japanisch, traditionellem Chinesisch sowie in vereinfachtem Chinesisch</li><li>• Menü „Help“ (Hilfe)</li><li>• Sicherheitsmeldung bei Anmeldung</li><li>• Hochladen von SSL-Zertifikaten durch Kunden</li><li>• Konfigurierbare Portnummern</li></ul>

## IPv6-Netzwerk

Frage	Antwort
Was ist IPv6?	<p>IPv6 ist das Akronym für "Internet Protocol Version 6". IPv6 ist das IP-Protokoll der nächsten Generation, welches die aktuelle Version des IP-Protokolls (IPv4) ersetzen wird.</p> <p>In IPv6 werden einige Probleme von IPv4 wie die begrenzte Anzahl an IPv4-Adressen behoben. IPv4 wird so auch in einigen Bereichen wie Routing und automatische Netzwerkkonfiguration verbessert. IPv6 soll IPv4 schrittweise ersetzen, wobei beide Versionen für einige Jahre parallel existieren werden.</p> <p>Durch IPv6 wird eines der größten Probleme eines IP-Netzwerks, aus Sicht des Administrators, angegangen: die Konfiguration und Verwaltung eines IP-Netzwerks.</p>
Warum unterstützt >ProductName> IPv6-Netzwerke?	<p>US-Regierungsbehörden sowie das US-amerikanische Verteidigungsministerium werden demnächst IPv6-kompatible Produkte erwerben. In den nächsten Jahren werden auch viele Unternehmen und Länder wie China auf IPv6 umstellen.</p>
Was bedeutet "Dual Stack" und warum ist diese Funktion erforderlich?	<p>"Dual Stack" ist eine Funktion zur gleichzeitigen Unterstützung von IPv4- und IPv6-Protokollen. Durch den graduellen Übergang von IPv4 zu IPv6 ist "Dual Stack" eine grundlegende Anforderung bei der IPv6-Unterstützung.</p>
Wie kann ich auf der KX II-101-V2-Einheit IPv6 aktivieren?	<p>Diese Einstellung können Sie über die Seite "Network Settings" (Netzwerkeinstellungen) auf der Registerkarte "Device Settings" (Geräteeinstellungen) vornehmen. Aktivieren Sie die Option "IPv6 Addressing" (IPv6-Adressen verwenden) und wählen Sie die manuelle oder automatische Konfiguration aus. Nähere Informationen hierzu finden Sie im Benutzerhandbuch.</p>

Anhang E: Häufig gestellte Fragen (FAQs)

Frage	Antwort
Was passiert, wenn ich einen externen Server mit einer IPv6-Adresse habe, den ich mit KX II-101-V2 verwenden möchte?	Der KX II-101-V2 kann über die IPv6-Adressen auf externe Server zugreifen (z. B. einen SNMP-Manager, Syslog-Server oder LDAP-Server).  <Durch die Verwendung der Dual-Stack-Architektur des KX II-101-V2, kann auf diese externen Server über Folgendes zugegriffen werden: (1) eine IPv4-Adresse, (2) eine IPv6-Adresse oder (3) einen Hostnamen. KX II-101-V2 unterstützt demnach also die gemischte IPv4-/IPv6-Umgebung, über die viele Kunden verfügen.
Was passiert, wenn mein Netzwerk IPv6 nicht unterstützt?	Die Standard-Netzwerkeinstellungen des KX II-101-V2 sind werkseitig nur für IPv4 eingestellt. Wenn Sie IPv6 verwenden möchten, folgen Sie den oben beschriebenen Anweisungen zum Aktivieren der IPv4-/IPv6-Dual-Stack-Funktion.
Wo erhalte ich weitere Informationen zu IPv6?	Allgemeine Informationen zu IPv6 finden Sie unter <a href="http://www.ipv6.org">www.ipv6.org</a> . Im Benutzerhandbuch des KX II-101-V2 wird die Unterstützung für IPv6 des KX II-101-V2 erläutert.

# Index

## 9

9-polige Pinbelegung - 222

## A

### A

Stromversorgung - 25  
Abmelden - 49  
Abmelden der Benutzer bei KX II-101-V2  
(Erzwungene Abmeldung) - 102  
Aktivieren des direkten Port-Zugriffs über URL  
- 128  
Aktivieren von FIPS 140-2 - 169, 171  
Aktivieren von SSH - 126  
Aktivieren von Telnet - 126  
Aktualisieren der Anzeige - 63  
Aktualisieren der Firmware - 186  
Aktualisieren des LDAP-Schemas - 224  
Aktualisieren des Schemacache - 228  
Allgemeine Befehle für alle Ebenen der  
Befehlszeilenschnittstelle - 204  
Allgemeine FAQs - 239  
Analoger KVM-Switch - 131, 152  
Ändern der höchsten Aktualisierungsrate - 69  
Ändern der Standardeinstellung für die  
GUI-Sprache - 155  
Ändern einer vorhandenen Benutzergruppe -  
100  
Ändern eines vorhandenen Benutzers - 103  
Ändern von Kennwörtern - 119  
Anforderungen für die Unterstützung von FIPS  
140-2 - 172  
Anmeldebeschränkungen - 161  
Anmelden - 202  
Anschließen des Powerstrips - 148  
Ansichtsoptionen - 78  
Anzeigen der Benutzer nach Port - 101  
Anzeigen der KX II-101-V2-Benutzerliste - 101  
Anzeigen der KX II-101-V2-MIB - 128, 135,  
141  
Arbeiten mit Zielservern - 39, 237  
Audit Log (Prüfprotokoll) - 182  
Aufheben der Verwaltung von KX II-101-V2  
durch CC-SG - 211  
Ausführen eines Tastaturmakros - 62  
Authentication Settings  
(Authentifizierungseinstellungen) - 105

Auto-Sense Video Settings  
(Videoeinstellungen automatisch erkennen)  
- 64

## B

### B

Zielserver - 25  
Backup/Restore  
(Sicherung/Wiederherstellung) - 184  
Bearbeiten und Löschen von Tastaturmakros -  
62  
Bearbeiten von rcusergroup-Attributen für  
Benutzermitglieder - 229  
Beenden der CC-SG-Verwaltung - 191  
Befehl - 205, 206, 207, 208, 209  
Befehle der Befehlszeilenschnittstelle - 200,  
204  
Benennen des Powerstrips (Seite - 147, 149  
Benennen des Zielservers - 33  
Benutzer - 100  
Benutzerauthentifizierungsprozess - 117  
Benutzerfunktionen - 7  
Benutzergruppen - 93  
Beziehung zwischen Benutzern und Gruppen -  
95

## C

### C

Network (Netzwerk) - 28  
CC-SG - 238  
Client Launch Settings  
(Client-Starteinstellungen) - 76  
Compaq Alpha und IBM P Server –  
Einschränkungen beim Mausmodus - 237  
Configuration (Konfiguration) - 207

## D

### D

Port - 29  
Debug - 204, 206  
Device Diagnostics (Gerätediagnose) - 198  
Device Information (Geräteinformationen) -  
183  
Device Services (Gerätedienste) - 126, 201  
Diagnostics (Diagnose) - 193, 204, 205  
Direkten Port-Zugriff aktivieren - 39

## E

### E

- Port - 29
- Einen Port umbenennen - 146
- Eingabeaufforderungen der Befehlszeilenschnittstelle - 202
- Eingeben des Erkennungsports - 127
- Eingeschränkter BIOS-Zugriff von einer lokalen Tastatur - 236
- Einleitung - 1
- Einrichten eines neuen Kennworts - 30
- Einschränkungen bezüglich Video Sun Blade, Tastatur und Mausunterstützung - 236
- Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen - 225
- Einstellen der Videoauflösung des Servers - 11, 12
- Einstellungen für Apple Macintosh - 22
- Einstellungen für IBM AIX - 23
- Einstellungen für Sun Solaris - 21
- Einstellungen für Windows 2000 - 17
- Einstellungen für Windows 7 und Windows Vista - 15
- Einstellungen für Windows XP, Windows 2003 und Windows 2008 - 13
- Encryption & Share (Verschlüsselung und Freigabe) - 167
- Ereignisverwaltung - 135
- Erkennen von Raritan-Geräten auf dem KX II-101-V2-Subnetz - 48
- Erkennen von Raritan-Geräten auf dem lokalen Subnetz - 47
- Erste Schritte - 10
- Erstellen eines neuen Attributs - 225
- Erstellen eines Tastaturmakros - 60
- Erstellen von Benutzergruppen und Benutzern - 35
- Erweiterte USB-Verbindungseinstellungen - 159
- Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen) - 135, 143

## F

- Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist - 88, 90
- Festlegen von Berechtigungen - 95, 98, 100

- Festlegen von Berechtigungen für eine individuelle Gruppe - 99, 103
- Festlegen von Port-Berechtigungen - 95, 100

## G

- Geräteverwaltung - 120
- Gestellmontage - 232
- Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste) - 96, 100

## H

- Häufig gestellte Fragen (FAQs) - 239
- Herstellen einer Verbindung mit virtuellen Medien - 90
- Hilfeoptionen - 80
- Hinweis für CC-SG-Benutzer - 34
- Hinweis zu Microsoft Active Directory - 35
- Hinweise zu Tastatur, Video und Maus - 235
- Hinweise zur Unterstützung des Betriebssystems IPv6 - 235
- Hinweise zur Unterstützung von IPv6 - 235
- Hinzufügen einer neuen Benutzergruppe - 95
- Hinzufügen eines neuen Benutzers - 103, 104
- Hinzufügen von Attributen zur Klasse - 227
- Hinzufügen, Bearbeiten und Löschen der Favoriten - 48
- HP UX RX 1600 – Tastatur- und Mauskonfiguration - 237
- HTTP- und HTTPS-Porteinstellungen - 127, 220

## I

- Implementierung der LDAP/LDAPS-Remoteauthentifizierung - 106, 112
- Implementierung der RADIUS-Remote-Authentifizierung - 112
- Installation und Konfiguration - 9, 207
- Installieren von CD-ROM-/DVD-ROM-/ISO-Abbildern - 91
- Intelligenter Mausmodus - 72
- IPv6-Netzwerk - 241

## J

- Java Runtime Environment (JRE) - 234

## K

- Kabel - 216
- Kabelverbindungen für Modemzugriff - 133
- Keyboard Macros (Tastaturmakros) - 57

Keyboard/Mouse Setup (Tastatur/Maus einrichten) - 131, 152, 236, 237  
 Kommandozeilenschnittstelle (CLI) - 132, 200  
 Konfigurieren der Ereignisverwaltung - Ziele - 143  
 Konfigurieren der IP-Zugriffssteuerung - 173  
 Konfigurieren von  
 Datum-/Uhrzeiteinstellungen - 134, 177  
 Konfigurieren von KX II-101-V2 unter der Verwendung eines  
 Terminalemulationsprogramms (Optional) - 10, 29, 35, 202  
 Konfigurieren von KX II-101-V2 unter Verwendung der Remote-Konsole - 29  
 Konfigurieren von Scaneinstellungen über VKC und AKC - 77  
 Konfigurieren von SNMP-Agenten - 128, 135  
 Konfigurieren von SNMP-Traps - 135  
 Konfigurieren von Videoeinstellungen - 64  
 KX II-101-V2-Hilfe - 3

## L

LAN Interface Settings  
 (LAN-Schnittstelleneinstellungen) - 33, 120, 124, 125  
 L-Halterung an KX II-101-V2 zur horizontalen Montage anbringen - 232  
 Linker Bildschirmbereich - 41  
 Linux-Einstellungen (für den Standardmausmodus) - 20  
 Linux-Einstellungen (Red Hat 4 und 5 und Fedora 14) - 18  
 Liste der KX II-101-V2-SNMP-Traps - 138  
 Lokale Laufwerke - 90

## M

Mauseinstellungen - 13  
 Mausmodus - 71, 73  
 Mausoptionen - 69  
 Mauszeigersynchronisation - 70  
 Menü Port Action (Portaktion) - 43, 44  
 Modem - 133  
 Montage - 7  
 Multi-Platform-Client (MPC) - 50

## N

Navigation in der  
 Kommandozeilenschnittstelle - 202  
 Navigation in der KX II-101-V2-Konsole - 40  
 Network (Netzwerk) - 205, 207

Network Basis Settings  
 (Basisnetzwerkeinstellungen) - 120, 121  
 Network Interface (Netzwerkschnittstelle) - 193  
 Network Settings (Netzwerkeinstellungen) - 30, 33, 120, 121, 124, 220  
 Network Statistics (Netzwerkstatistik) - 194  
 Netzwerk-Geschwindigkeitseinstellungen - 125, 221  
 Netzwerkkonfiguration - 5  
 Neuerungen im Hilfedokument - 4  
 Neustart der KX II-101-V2-Einheit - 189

## O

Oberfläche der KX II-101-V2-Remotekonsole - 39  
 Optionen im Menü - 73, 79

## P

Paketinhalt - 8  
 Physische Spezifikationen - 213  
 Ping Host (Ping an den Host) - 196  
 Port - 132  
 Port Configuration (Port-Konfiguration) - 23, 144  
 Produktfeatures - 5  
 Produktfotos - 5  
 Properties (Eigenschaften) - 54  
 Proxymodus und MPC - 238  
 Prüfen Ihres Browsers auf  
 AES-Verschlüsselung - 168, 171  
 PS/2-Konfiguration - 27

## R

Remoteauthentifizierung - 34  
 Rückgabe von Benutzergruppeninformationen vom Active Directory-Server - 111

## S

Scaling (Skalieren) - 79  
 Schaltflächen auf der Symbolleiste und Symbole auf der Statusleiste - 51  
 Schnittstellen - 5, 39  
 Schritt 1  
 Konfigurieren des Zielsevers - 9, 10  
 Schritt 2  
 Konfigurieren der Einstellungen für die Netzwerkfirewall - 9, 23  
 Schritt 3  
 Anschließen der Geräte - 9, 24  
 Schritt 4

## Index

Konfigurieren von KX II-101-V2 - 9, 29  
Security Settings (Sicherheitseinstellungen) - 103, 161  
Seite - 43, 46, 47, 48, 196  
Serial Port Settings (Einstellungen für seriellen Port) - 132  
Server - 238  
Sicherheitsmeldung - 180  
Sicherheitsverwaltung - 161  
Sperrungen von Benutzern und Aufheben der Sperrung - 104  
Spezifikationen für den RADIUS-Kommunikationsaustausch - 115  
SSH-Verbindung mit der KX II-101-V2-Einheit - 201  
SSH-Zugriff über eine UNIX-/Linux-Workstation - 202  
SSH-Zugriff über einen Windows-PC - 201  
SSL-Zertifikate - 176  
Standard-Anmeldeinformationen - 9  
Steuern eines Powerstrip-Geräts - 151  
Steuerung des Powerstrip von Raritan - 132  
Stromversorgung - 7  
Stromzufuhrsteuerung - 145, 147  
Stromzufuhrsteuerung eines Zielservers - 53  
Stromzuordnungen verwalten - 150  
Strong Passwords (Sichere Kennwörter) - 119, 161, 163  
Syntax der Kommandozeilenschnittstelle – Tipps und Zugriffstasten - 203  
SysLog-Konfiguration - 142  
Systemverwaltungsfunktionen - 6

## T

Tastaturbeschränkungen - 75  
Tastaturmakros importieren/exportieren - 57  
Tastaturoptionen - 57  
Technische Daten - 213  
Terminologie - 7  
Trennen der Benutzer von Ports - 102  
Trennen von KVM-Zielservers - 54  
Trennen von virtuellen Medien - 89, 92

## U

Überblick - 9, 50, 82, 157, 200, 210  
Überblick über KX II-101-V2 - 2  
Unterstützte Betriebssysteme (Clients) - 214  
Unterstützte Browser - 215  
Unterstützte Protokolle - 34  
Unterstützte Tastatursprachen - 218

Unterstützte Videoauflösungen - 216  
Upgrade History (Aktualisierungsverlauf) - 188  
USB-Konfiguration - 26  
USB-Verbindungen verwalten - 156  
USB-Verbindungseinstellungen - 158  
User Blocking (Benutzersperrung) - 104, 161, 165  
User Group List (Liste der Benutzergruppen) - 94  
User Management (Benutzerverwaltung) - 35, 93

## V

Verbinden mit einem KVM-Zielservers - 50  
Verbindungsinformationen - 56  
Vervollständigen von Befehlen - 203  
Verwalten von Favoriten - 45  
Verwalten von KVM-Zielservers (Seite - 145, 147)  
Verwaltungsfunktionen - 6  
Verwandte Dokumentation - 4  
Verwenden der Funktion - 68  
Verwenden virtueller Medien - 89  
Verwenden von CC-SG im Proxymodus - 212  
Verwendete TCP- und UDP-Ports - 219  
Videoauflösung - 7  
Videoauflösung von Sun - 12  
Videoeigenschaften - 63  
View Toolbar (Symbolleiste anzeigen) - 78  
Virtual KVM Client (VKC) - 44, 50  
Virtuelle Medien - 73, 81  
Virtuelle Medien in einer Linux-Umgebung - 86  
Virtuelle Medien in einer Mac-Umgebung - 88  
Virtuelle Medien in einer Windows XP-Umgebung - 85  
VKC Virtual Media (Virtuelle Medien) - 73  
Vollbildmodus - 79  
Von LDAP - 224  
Von Microsoft Active Directory - 224  
Voraussetzungen für die Verwendung virtueller Medien - 84, 89

## W

Wartung - 182  
Werksrückstellung - 189  
Wichtige Hinweise - 234

## Z

Zertifizierte Modems - 133, 216

Zugriff auf KX II-101-V2 über die  
Befehlszeilenschnittstelle - 201  
Zurückgeben von  
Benutzergruppeninformationen - 224  
Zurückgeben von  
Benutzergruppeninformationen über  
RADIUS - 115  
Zurücksetzen des KX II-101-V2 mithilfe der  
Taste - 154, 169  
Zuweisen einer IP-Adresse - 10, 30



## ▶ USA/Kanada/Lateinamerika

Montag bis Freitag  
08:00 bis 20:00 Uhr ET (Eastern Time)  
Tel.: 800-724-8090 oder 732-764-8886  
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.  
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.  
Fax: 732-764-8887  
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com  
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

## ▶ China

### Peking

Montag bis Freitag  
09:00 bis 18:00 Uhr Ortszeit  
Tel.: +86-10-88091890

### Shanghai

Montag bis Freitag  
09:00 bis 18:00 Uhr Ortszeit  
Tel.: +86-21-5425-2499

### GuangZhou

Montag bis Freitag  
09:00 bis 18:00 Uhr Ortszeit  
Tel.: +86-20-8755-5561

## ▶ Indien

Montag bis Freitag  
09:00 bis 18:00 Uhr Ortszeit  
Tel.: +91-124-410-7881

## ▶ Japan

Montag bis Freitag  
09:30 bis 17:30 Uhr Ortszeit  
Tel.: +81-3-3523-5991  
E-Mail: support.japan@raritan.com

## ▶ Europa

### Europa

Montag bis Freitag  
08:30 bis 17:00 Uhr GMT+1 MEZ  
Tel.: +31-10-2844040  
E-Mail: tech.europe@raritan.com

### Großbritannien

Montag bis Freitag  
08:30 bis 17:00 Uhr GMT  
Telefon +44(0)20-7090-1390

### Frankreich

Montag bis Freitag  
08:30 bis 17:00 Uhr GMT+1 MEZ  
Tel.: +33-1-47-56-20-39

### Deutschland

Montag bis Freitag  
08:30 bis 17:30 Uhr GMT+1 MEZ  
Tel.: +49-20-17-47-98-0  
E-Mail: rg-support@raritan.com

## ▶ Melbourne, Australien

Montag bis Freitag  
09:00 bis 18:00 Uhr Ortszeit  
Tel.: +61-3-9866-6887

## ▶ Taiwan

Montag bis Freitag  
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit  
Tel.: +886-2-8919-1333  
E-Mail: support.apac@raritan.com