



Dominion KX II-101

Benutzerhandbuch

Version 2.0

Copyright © 2008 Raritan, Inc.
KX2101-0A-G
Februar 2008
255-62-4031-00

Dieses Dokument enthält urheberrechtlich geschützte Informationen. Alle Rechte vorbehalten. Ohne die vorherige ausdrückliche schriftliche Genehmigung von Raritan, Inc. darf kein Teil dieses Dokuments fotokopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

© Copyright 2008 Raritan, Inc. CommandCenter®, Dominion®, Paragon® und das Raritan-Firmenlogo sind Marken oder eingetragene Marken von Raritan, Inc. Alle Rechte vorbehalten. Java® ist eine eingetragene Marke von Sun Microsystems, Inc. Internet Explorer® ist eine eingetragene Marke der Microsoft Corporation. Netscape® und Netscape Navigator® sind eingetragene Marken der Netscape Communication Corporation. Alle anderen Marken oder eingetragenen Marken sind Eigentum der jeweiligen Rechteinhaber.

Einhaltung der FCC-Bestimmungen

In Tests wurde festgestellt, dass das Gerät die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen einhält. Diese Grenzwerte sollen in kommerziell genutzten Umgebungen einen angemessenen Schutz vor Störungen bieten. Das in diesem Handbuch beschriebene Gerät erzeugt, verbraucht und gibt unter Umständen hochfrequente Strahlung ab und kann bei unsachgemäßer Installation und Verwendung zu Störungen des Rundfunk- und Fernsehempfangs führen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

VCCI-Informationen (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 ist nicht verantwortlich für Schäden an diesem Produkt, die durch einen Unfall, ein Missgeschick, durch Missbrauch, Fremdeingriffe am Produkt oder andere Ereignisse entstanden sind, die sich außerhalb der Kontrolle von Raritan befinden oder unter normalen Betriebsbedingungen nicht auftreten.



Inhalt

Kapitel 1	Einleitung	1
<hr/>		
	Überblick über Dominion KX II-101	2
	Produktfotos.....	3
	Produktfeatures	4
	Schnittstellen.....	4
	Netzwerkkonfiguration.....	4
	Systemverwaltungsfunktionen	4
	Verwaltungsfunktionen	4
	Benutzerfunktionen	5
	Stromversorgung.....	5
	Videoauflösung	5
	Montage.....	5
	Paketinhalt.....	6
	Terminologie	6
	Optionales Zubehör	6
Kapitel 2	Wichtige Informationen	7
<hr/>		
	Anmeldung	7
	Standard-IP-Adresse	7
	Service Pack.....	7
Kapitel 3	Installation und Konfiguration	8
<hr/>		
	Konfigurieren des Zielservers	8
	Einstellen der Videoauflösung des Servers	9
	Mausmodi	11
	Anschließen der KX II-101-Einheit.....	16
	Verbinden mit dem Zielserver	18
	Verbinden mit dem Netzwerk.....	22
	Stromversorgung der KX II-101-Einheit	22
	Verwenden des Ports „Admin“	23
	Verwenden des Ports „Local User“	23
	Konfigurieren der Einstellungen der Netzwerk-Firewall.....	23
	Konfigurieren von KX II-101.....	24
	Verwenden der Remote-Konsole	24
	Verwenden eines Terminalemulationsprogramms.....	30

Kapitel 4 Herstellen einer Verbindung mit der KX II-101-Einheit 35

Unterstützte Sprachen	35
Java Runtime Environment (JRE).....	35
Starten der KX II-101-Einheit	36
Aktivieren des direkten Port-Zugriffs.....	37
Layout der KX II-101-Konsole	38
Navigation in der KX II-101-Konsole	39
Menüstruktur der KX II-101-Remote-Konsole	40
Abmelden	40
Verwalten von Favoriten.....	41
Menü „Manage Favorites“ (Favoriten verwalten).....	42
Favorites List (Favoritenliste)	43
Discover Devices - Local Subnet (Geräte erkennen – Lokales Subnetz).....	45
Discover Devices - KX II-101 Subnet (Geräte erkennen – KX II-101-Subnetz).....	47
Add New Favorite (Neuen Favoriten hinzufügen)	48
Seite „Port Access“ (Port-Zugriff)	49

Kapitel 5 Benutzer, Gruppen und Zugriffsberechtigungen 51

Benutzer.....	51
Gruppen.....	51
Beziehung zwischen Benutzern und Gruppen.....	52
Benutzerverwaltung.....	52
Menü „User Management“ (Benutzerverwaltung).....	52
Remote-Authentifizierung	67
Hinweis für CC-SG-Benutzer	67
Unterstützte Protokolle	67
Hinweis zu Microsoft Active Directory	68
Authentifizierung im Vergleich zur Autorisierung	68
Authentication Settings (Authentifizierungseinstellungen)	69
Aktualisieren des LDAP-Schemas	79

Kapitel 6 Virtual KVM Client 88

Überblick	89
Optionen	90
Menüstruktur.....	90
Symbolleiste	91
Mauszeigersynchronisation	92
Tipps zur Maussynchronisation.....	92
Menü „Connection“ (Verbindung)	94
Dialogfeld „Properties“ (Eigenschaften).....	94
Connection Info (Verbindungsinformationen)	96
Exit (Beenden).....	97

Menü „Keyboard“ (Tastatur).....	97
Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)	97
Keyboard Macros (Tastaturmakros).....	98
Erstellen eines Tastaturmakros	98
Ausführen eines Tastaturmakros.....	101
Ändern eines Tastaturmakros	101
Entfernen eines Tastaturmakros	101
Menü „Video“	102
Refresh Screen (Anzeige aktualisieren).....	102
Auto-Sense Video Settings (Videoeinstellungen automatisch erkennen)	103
Calibrate Color (Farbe kalibrieren).....	103
Video Settings (Videoeinstellungen)	104
Menü „Mouse“ (Maus).....	107
Synchronize Mouse (Maus synchronisieren)	107
Single Mouse Cursor (Ein Cursor).....	107
Standard	108
Intelligent	109
Absolute (Absolut).....	111
Virtuelle Medien.....	111
Menü „Tools“ (Extras)	112
Options (Optionen).....	112
Menü „View“ (Ansicht).....	113
View Toolbar (Symbolleiste anzeigen).....	113
Scaling (Skalieren).....	113
Target Screen Resolution (Zielbildschirmauflösung).....	114
Menü „Help“ (Hilfe)	114
About Raritan Virtual KVM Client (Informationen zum Raritan Virtual KVM Client)...	114

Kapitel 7 Virtuelle Medien 115

Überblick	116
Voraussetzungen für die Verwendung virtueller Medien	118
Verwenden virtueller Medien	119
Öffnen einer KVM-Sitzung	120
Herstellen einer Verbindung mit virtuellen Medien.....	121
Lokale Laufwerke.....	121
Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist.....	122
CD-ROM-/DVD-ROM-/ISO-Abbilder	123

Inhalt

Trennen von virtuellen Medien.....	124
File Server Setup (Dateiserver-Setup) (nur für Dateiserver-ISO-Abbilder)	125

Kapitel 8 Geräteverwaltung 127

Menü „Device Settings“ (Geräteeinstellungen)	127
Network Settings (Netzwerkeinstellungen)	129
Network Basis Settings (Basisnetzwerkeinstellungen)	130
LAN Interface Settings (LAN-Schnittstelleneinstellungen)	132
Device Services (Gerätedienste)	134
Keyboard/Mouse Setup (Tastatur/Maus einrichten)	136
Serial Port Settings (Einstellungen für seriellen Port)	137
Date/Time Settings (Datum-/Uhrzeiteinstellungen).....	139
Ereignisverwaltung	140
SNMP Configuration (SNMP-Konfiguration).....	141
Syslog-Konfiguration.....	142
Event Management – Destinations (Ereignisverwaltung – Ziele)	144
Konfigurieren des SNMP-Agenten.....	146
SNMP-Trap-Konfiguration	146
Port Configuration (Port-Konfiguration)	149

Kapitel 9 Stromzufuhrsteuerung 151

Überblick	151
Anschließen des Powerstrips.....	152
Benennen des Powerstrips (Seite „Port“ für Powerstrips)	153
Zuordnen von KVM-Zielservern zu Ausgängen (Seite „Port“).....	155
Anzeigen der Ausgangszuordnungen	158
Steuern des Powerstrip-Geräts	159

Kapitel 10 Sicherheitseinstellungen 161

Menü „Security“ (Sicherheit).....	161
Security Settings (Sicherheitseinstellungen).....	162
Login Limitations (Anmeldebeschränkungen)	163
Strong Passwords (Sichere Kennwörter)	165
User Blocking (Benutzersperrung)	166
Encryption & Share (Verschlüsselung und Freigabe).....	168
Prüfen Ihres Browsers auf AES-Verschlüsselung.....	171

IP Access Control (IP-Zugriffssteuerung).....	171
Kapitel 11 Wartung	174
<hr/>	
Menü Maintenance (Wartung)	174
Audit Log (Prüfprotokoll).....	175
Device Information (Geräteinformationen)	177
Backup/Restore (Sicherung/Wiederherstellung).....	178
Firmware Upgrade (Firmware-Aktualisierung)	180
Upgrade History (Aktualisierungsverlauf)	183
Reboot (Neustart)	183
Kapitel 12 Befehlszeilenschnittstelle (CLI)	185
<hr/>	
Überblick	185
Zugriff auf KX II-101 über die Befehlszeilenschnittstelle	186
SSH-Verbindung mit der KX II-101-Einheit	186
SSH-Zugriff über einen Windows-PC.....	186
SSH-Zugriff über eine UNIX-Workstation	187
Anmelden	187
Navigation in der Befehlszeilenschnittstelle	188
Eingabeaufforderungen der Befehlszeilenschnittstelle.....	188
Vervollständigen der Befehle	188
Syntax der Befehlszeilenschnittstelle - Tipps und Zugriffstasten	189
Allgemeine Befehle für alle Ebenen der Befehlszeilenschnittstelle	189
Befehle der Befehlszeilenschnittstelle.....	190
Diagnostics (Diagnose).....	191
Configuration (Konfiguration).....	192
Befehl „listports“	194
Befehl „Userlist“	194

Diagnose	195
Menü „Diagnostics“ (Diagnose).....	195
Network Interface (Netzwerkschnittstelle).....	196
Network Statistics (Netzwerkstatistik).....	197
Ping Host (Ping an den Host)	199
Trace Route to Host (Route zum Host zurückverfolgen)	200
Device Diagnostics (Gerätediagnose).....	201
Kapitel 14 CC UnManage	204
Überblick	204
Aufheben der Verwaltung von KX II-101 durch CC-SG.....	205
Verwenden von CC-SG im Proxymodus	206
Anhang A Technische Daten	207
KX II-101	207
Kabel.....	208
Software für den Raritan Remote Client	208
Anhang B Gestellmontage	209
Befestigung des Netzadapter-Clips	209
Clip-Typ identifizieren.....	209
Anschlussabdeckung vom Netzadapter entfernen	210
Clip am Netzadapter anbringen.....	210
Anbringen der Gestellhalterungen	211
KX II-101-Halterungen	212
Halterungen an der KX II-101-Einheit zur horizontalen Montage anbringen.....	213
Halterungen an der KX II-101-Einheit zur vertikalen Montage anbringen	214
Index	217

Kapitel 1 Einleitung

In diesem Kapitel

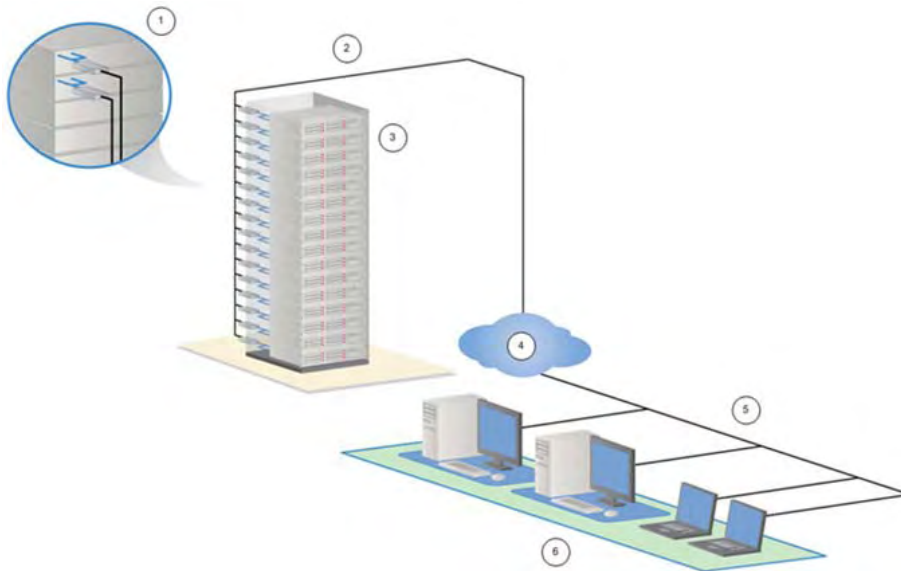
Überblick über Dominion KX II-101	2
Produktfotos	3
Produktfeatures.....	4
Paketinhalt	6
Terminologie	6

Überblick über Dominion KX II-101

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

Der Formfaktor des KX II-101-Dongle erleichtert die Installation in der Nähe des Zielservers, und jede KX II-101-Einheit verfügt über eine eigene IP-Adresse. Jede Einheit wird über PoE (Power-over-Ethernet) oder ein externes Netzteil mit Strom versorgt.

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



- 1 KX II-101
- 2 LAN
- 3 Windows-, Linux- und Sun-Server
- 4 TCP/IP
- 5 LAN
- 6 Remote-Zugriff (Netzwerk)

Produktfotos



Produktfeatures

Schnittstellen

- Integrierte PS/2-KVM-Verbindung
- Optionale USB-Verbindung zur Steuerung und für virtuelle Medien
- Serieller Verwaltungs-Port „Admin“ für anfängliche Geräteeinstellungen und Diagnosen und Zugriff über ein externes Modem
- Ethernet-LAN-Port für automatische 10/100-Base-T-Erkennung, Vollduplex
- LED-Anzeige für Netzwerkaktivität und Status
- Hintergrundbeleuchtete LED-Anzeige bei eingeschaltetem Gerät

Netzwerkkonfiguration

- DHCP oder statische IP-Geräteadresse

Systemverwaltungsfunktionen

- Firmware-Aktualisierung über Ethernet
- Ausfallsichere Firmware-Aktualisierung
- Vom Administrator einstellbare Uhr oder Synchronisation über NTP/SNTP (Network Time Protocol)
- Lokaler SNMP-V2-Agent für ein mit einem Zeitstempel versehenes Administratoraktivitätsprotokoll, der durch den Administrator deaktiviert werden kann
- Unterstützt RADIUS- und LDAP-Authentifizierungsprotokolle

Verwaltungsfunktionen

- Webbasierte Verwaltung
- LDAP-, Active Directory-, RADIUS- oder interne Authentifizierung und Autorisierung
- DHCP oder feste IP-Adressen
- Integration in die Verwaltungsanwendung CommandCenter Secure Gateway (CC-SG) von Raritan

Benutzerfunktionen

- Webbasierter Zugriff über bekannte Browser
- Intuitive grafische Benutzeroberfläche
- Modus für „PC Share“ (PC-Freigabe) für mehr als einen Remote-Benutzer
- TCP-Kommunikation
- Englische Benutzeroberfläche
- Zugriff auf virtuelle Medien
- Absolute Mouse Synchronization
- Plug-and-Play
- 256-Bit-Verschlüsselung des gesamten KVM-Signals, einschließlich Video und virtueller Medien

Stromversorgung

- Stromversorgung über PoE (Power over Ethernet) der Klasse 2
- Alternative Stromversorgung über ein externes Netzteil

Videoauflösung

- Auflösung bis zu 1600 x 1200 bei bis zu 60 Hz

Montage

- Gestellhalterung

Weitere Informationen finden Sie unter *Gestellmontage* (auf Seite 209).

Paketinhalt

Im Lieferumfang jeder KX II-101-Einheit ist Folgendes enthalten:

- KX II-101-Haupteinheit - KVM-over-IP-Dongle
- USB-Kabel (Typ A auf Typ B Mini)
- Stromadapterkit - Wechsel-Gleichstrom 6VDC
- Drei zusätzliche Netzstecker zur weltweiten Verwendung
- Serielles Mini-DIN/DB9-Kabel
- Gestellhalterungskit
- CD-ROM mit Raritan-Benutzerhandbücher und Kurzanleitungen
- Kurzanleitung für die Installation und Konfiguration
- Anwendungshinweise (falls zutreffend)
- Technische Hinweise (falls zutreffend)

Terminologie

Zielserver	Server für den Remote-Zugriff über KX II-101 und die verbundene KVM-Konfiguration.
Remote-PC	Ein Computer mit Windows, Linux, Solaris oder Apple Macintosh® für den Zugriff auf und die Steuerung der Zielserver, die mit KX II-101 verbunden sind.
Serieller Verwaltungspport „Admin“	KX II-101 ist mit einem seriellen Verwaltungspport mit der Bezeichnung „Admin“ ausgestattet. Verbinden Sie den seriellen Port des PC mit dem seriellen Verwaltungspport der KX II-101-Einheit über das mitgelieferte Mini-DIN/DB9-Kabel. Verwenden Sie dann ein standardmäßiges Emulationssoftwarepaket (z. B. HyperTerminal), um auf den seriellen Verwaltungspport zuzugreifen. Der serielle Verwaltungspport „Admin“ wird für die Netzwerkkonfiguration verwendet.
Lokaler Benutzer-Port „Local User“	Ein Port, über den ein Benutzer in der Nähe des Zielservers die systemeigene Tastatur und Maus verwenden kann, ohne die Verbindung zu KX II-101 zu trennen.
Virtuelle Medien	Ermöglicht den Remote-Zugriff eines KVM-Zielservers über einen Client-PC und Netzwerkdateiserver auf Medien.

Optionales Zubehör

- DB15/PS/2- und lokales VGA-Benutzerkabel

Weitere Informationen finden Sie unter *Kabel* (auf Seite 208).

Kapitel 2 Wichtige Informationen

In diesem Kapitel

Anmeldung.....	7
Standard-IP-Adresse	7
Service Pack	7

Anmeldung

- Der standardmäßige KX II-101-Benutzeranmeldename lautet **admin** und das Kennwort **raritan**. Dieser Benutzer besitzt Administratorrechte.
- Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden.
- Das Standardkennwort **raritan** muss in Kleinbuchstaben eingegeben werden.
- Zur Gewährleistung der Sicherheit sollte das Standardkennwort so bald wie möglich geändert werden.

Standard-IP-Adresse

KX II-101 wird mit der standardmäßigen statischen IP-Adresse 192.168.0.192 ausgeliefert. In einem Netzwerk ohne DHCP-Server müssen Sie eine neue statische IP-Adresse, eine Netzmaske und Gateway-Adressen über die serielle KX II-101-Verwaltungskonsole oder die KX II-101-Remote-Konsole konfigurieren.

Weitere Informationen zum Zuweisen von IP-Adressen für KX II-101 über die Remote-Konsole finden Sie unter *Zuweisen einer IP-Adresse* (auf Seite 25). Weitere Informationen zum Einrichten einer IP-Adresse über die serielle Verwaltungskonsole finden Sie unter *Verwenden der lokalen seriellen Konsole* (siehe "Verwenden eines Terminalemulationsprogramms" auf Seite 30).

Service Pack

- KX II-101-Benutzer mit Microsoft Internet Explorer Version 5.01 oder Windows 2000 müssen auf Service Pack 4 (SP4) oder höher aktualisieren.

Kapitel 3 Installation und Konfiguration

In diesem Kapitel

Konfigurieren des Zielservers	8
Anschließen der KX II-101-Einheit	16
Konfigurieren der Einstellungen der Netzwerk-Firewall	23
Konfigurieren von KX II-101	24

Konfigurieren des Zielservers

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

1. *Konfigurieren des Zielservers* (auf Seite 8)
2. *Konfigurieren der Einstellungen der Netzwerk-Firewall* (auf Seite 23)
3. *Anschließen der KX II-101-Einheit* (auf Seite 16)
4. *Konfigurieren von KX II-101* (auf Seite 24)

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

Einstellen der Videoauflösung des Servers

Für optimale Bandbreiteneffizienz und Videoleistung sollten Zielservers 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 KX II-101 unterstützt werden und das Signal keinen Zeilensprung beinhaltet. KX II-101 unterstützt die folgenden Videoauflösungen:

Textmodi

640 x 480 bei 60 Hz	1024 x 768 bei 60 Hz
640 x 480 bei 72 Hz	1024 x 768 bei 70 Hz
640 x 480 bei 75 Hz	1024 x 768 bei 75 Hz
640 x 480 bei 85 Hz	1024 x 768 bei 85 Hz
800 x 600 bei 56 Hz	1152 x 864 bei 60 Hz
800 x 600 bei 60 Hz	1152 x 864 bei 75 Hz
800 x 600 bei 72 Hz	1280 x 1024 bei 60 Hz
800 x 600 bei 75 Hz	1600 x 1200 bei 60 Hz
800 x 600 bei 85 Hz	

Konfigurieren des Zielservers

Einstellen der Sun-Videoauflösung

Sun-Systeme verfügen über zwei Auflösungseinstellungen: eine Befehlszeilenauflösung und eine GUI-Auflösung. Weitere Informationen zu den Auflösungen, die von KX II-101 unterstützt werden, finden Sie unter *Einstellen der Videoauflösung des Servers* (auf Seite 9).

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

Befehlszeilenauflösung

➤ *So überprüfen Sie die Befehlszeilenauflösung:*

- Führen Sie den folgenden Befehl auf Stammebene aus:
eeprom output-device

➤ *So ändern Sie die Befehlszeilenauflösung:*

1. Geben Sie folgenden Befehl ein:

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

Dabei steht 1024x768x75 für eine beliebige Auflösung, die von KX II-101 unterstützt wird.

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
```

Dabei steht 1024x768x75 für eine beliebige Auflösung, die von KX II-101 unterstützt wird.

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
```

Dabei steht 1024x768x75 für eine beliebige Auflösung, die von KX II-101 unterstützt wird.

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
```

Dabei steht 1024x768x75 für eine beliebige Auflösung, die von KX II-101 unterstützt wird.

2. Starten Sie den Computer neu.

Mausmodi

KX II-101 arbeitet in verschiedenen Mausmodi: **Absolute Mouse Synchronization™**, **Intelligent** (ohne animierten Cursor) und **Standard**. Für den Mausmodus **Absolute Mouse Synchronization** müssen die Mausparameter nicht geändert werden. In den Mausmodi **Standard** und **Intelligent** müssen die Mausparameter auf bestimmte Werte festgelegt werden. Diese Werte werden in den folgenden Absätzen dieses Abschnitts beschrieben.

In diesem Abschnitt werden die Mauskonfigurationen beschrieben, die für verschiedene Systeme erforderlich sind.

Windows Vista

➤ *So konfigurieren Sie die Maus:*

1. Wählen Sie **Start > Einstellungen > Systemsteuerung > Maus**.

Konfigurieren des Zielservers

2. Klicken Sie auf die Registerkarte **Zeigeroptionen**. Führen Sie im Bereich **Bewegung** folgende Schritte aus:
 - a. Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Einstellung ein.
 - b. Deaktivieren Sie das Kontrollkästchen **Zeigerbeschleunigung verbessern**.
3. Klicken Sie auf **OK**.

➤ *So deaktivieren Sie die Animations- und Einblendeffekte:*

1. Klicken Sie im Windows-Menü **Start** auf **Systemsteuerung > System > Erweiterte Systemeinstellungen**. Das Dialogfeld **Systemeigenschaften** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Klicken Sie in der Gruppe **Leistung** auf die Schaltfläche **Einstellungen**. Das Dialogfeld **Leistungsoptionen** wird angezeigt.
4. Deaktivieren Sie im Bereich **Benutzerdefiniert** die folgenden Kontrollkästchen:
 - Steuerelemente und Elemente innerhalb von Fenstern animieren
 - Animation beim Minimieren und Maximieren von Fenstern
 - Menüs in Ansicht ein- oder ausblenden
 - Quickinfo in Ansicht ein- oder ausblenden
 - Menüelemente nach Aufruf ausblenden
5. Klicken Sie auf **OK**.
6. Schließen Sie die Systemsteuerung.

Einstellungen für Windows XP

Deaktivieren Sie bei einem KVM-Zielserver mit Microsoft Windows XP das Kontrollkästchen **Zeigerbeschleunigung verbessern**, und stellen Sie die Mausgeschwindigkeit genau auf die mittlere Einstellung ein. Sie finden diese Parameter unter **Systemsteuerung, Maus, Zeigeroptionen**.

Hinweis: Für Zielserver, auf denen Windows 2000 oder XP ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remote-Verbindungen über KX II-101 verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die KX II-101-Verbindung beschränken, da andere Benutzer ggf. schnellere Mausgeschwindigkeiten bevorzugen.

Hinweis: Die Anmeldemasken von Windows XP und 2000 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von KX II-101 empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisation möglicherweise nicht optimal. Wenn Sie sich mit dem Anpassen der Registrierung von Windows-Zielservern auskennen, können Sie in den Anmeldemasken eine bessere KX II-101-Maussynchronisation erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern: Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0.

Einstellungen für Windows 2000

Stellen Sie bei einem Zielserver mit Microsoft Windows 2000 die Mausbeschleunigung auf „Keine“ und die Mausgeschwindigkeit genau auf die mittlere Einstellung ein. Sie finden diese Parameter unter **Systemsteuerung, Maus**.

Konfigurieren des Zielservers

Einstellungen für Linux

Stellen Sie bei einem Zielservers mit grafischen Linux-Benutzeroberflächen die Mausbeschleunigung und den Grenzwert genau auf **1** ein.

Stellen Sie wie oben beschrieben sicher, dass jeder Linux-Zielservers eine von KX II-101 unterstützte Auflösung mit einer standardmäßigen VESA-Auflösung und Aktualisierungsfrequenz verwendet. Ein Linux-Zielservers sollte außerdem so eingestellt sein, dass sich die Deaktivierungszeiten im Bereich von +/- 40 % der VESA-Standardwerte bewegen.

➤ *So überprüfen Sie diese Parameter:*

1. Rufen Sie die Xfree86-Konfigurationsdatei **XF86Config** auf.
2. Deaktivieren Sie in einem Text-Editor alle nicht von KX II-101 unterstützten Auflösungen.
3. Deaktivieren Sie die virtuelle Desktop-Funktion, die nicht von KX II-101 unterstützt wird.
4. Prüfen Sie die Deaktivierungszeiten (+/- 40 % der VESA-Standardwerte).
5. Starten Sie den Computer neu.

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

Einstellungen für Sun Solaris

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

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

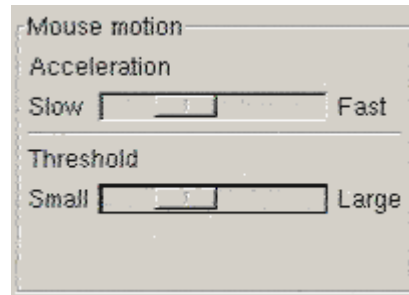
Ein Zielsever mit dem Solaris-Betriebssystem muss eine VGA-Buchse mit TV-Out-Signal haben (mit H- und V-Synchronisation, keine Composite-Synchronisation). Um den Sun-Grafikkartenausgang von der Composite-Synchronisation auf die nicht standardmäßige VGA-Ausgabe zu ändern, geben Sie zunächst den Befehl **Stop+A** aus, um in den BootProm-Modus zu wechseln. Geben Sie dann den Befehl

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

aus, um die Ausgabeauflösung zu ändern. 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 KX II-101 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 einen APKMSUN Guardian-Converter von Raritan.

Stellen Sie bei einem Zielsever mit dem Solaris-Betriebssystem die Mausbeschleunigung und den Grenzwert genau auf **1** ein. Legen Sie diese Werte über die grafische Benutzeroberfläche (siehe unten) oder über die Befehlszeile „xset mouse a t“ fest, wobei „a“ für die Beschleunigung und „t“ für den Grenzwert steht.



Einstellungen für Apple® Macintosh

Verwenden Sie den Mausmodus **Absolute Mouse Synchronization**.

Anschließen der KX II-101-Einheit

Anschließen der KX II-101-Einheit

Die KX II-101-Einheit weist die im Diagramm unten beschriebenen physischen Anschlüsse auf:

Kapitel 3: Installation und Konfiguration



Anschließen der KX II-101-Einheit

- 1 Angeschlossenes Monitor- und PS/2-Kabel (siehe Nr. 3.)
- 2 Mini-USB-Port. Zur Verbindung des Geräts mit dem Zielsystem über das mitgelieferte USB-Kabel, wenn das angeschlossene PS/2-Kabel nicht verwendet wird. Eine USB-Verbindung muss verwendet werden, um den Mausmodus **Absolute Mouse Synchronization** oder die Funktionen für virtuelle Medien nutzen zu können.
- 3 Angeschlossenes Monitor- und PS/2-Kabel. Zur Verbindung des Geräts mit einem Monitor und einem Zielsystem, wenn das USB-Kabel nicht verwendet wird.
- 4 Port „LOCAL USER“. Zur direkten Verbindung von Tastatur, Monitor und Maus (lokal) mit dem Zielsystem über ein optionales PS/2-Kabel.
- 5 Ethernet-LAN/PoE-Port. Bietet LAN-Konnektivität und Stromversorgung über eine PoE LAN-Verbindung.
- 6 Stromanschluss. Anschluss für die Stromversorgung, wenn keine PoE (Power over Ethernet) LAN-Verbindung verwendet wird.
- 7 Hintergrundbeleuchtete LED-Anzeige bei eingeschaltetem Gerät und während des Starts. Bietet Feedback zum Betriebsstatus des Geräts.
- 8 Port „Admin“. Für folgende Funktionen:
 - Konfiguration und Verwaltung des Geräts mit einem auf dem PC installierten Terminalemulationsprogramm.
 - Konfiguration und Verwaltung eines Powerstrips.
 - Anschluss eines externen Modems zum Einwählen.

Verbinden mit dem Zielsystem

Für die Verbindung von KX II-101 mit dem Zielsystem können entweder die integrierten PS/2-Kabel oder das im Lieferumfang enthaltene USB-Kabel verwendet werden. Stellen Sie vor der Verbindung sicher, dass der Monitor des Zielsystems auf eine unterstützte Auflösung und Aktualisierungsfrequenz eingestellt ist (siehe *Einstellen der Videoauflösung des Servers* (auf Seite 9)).

PS/2-Konfiguration

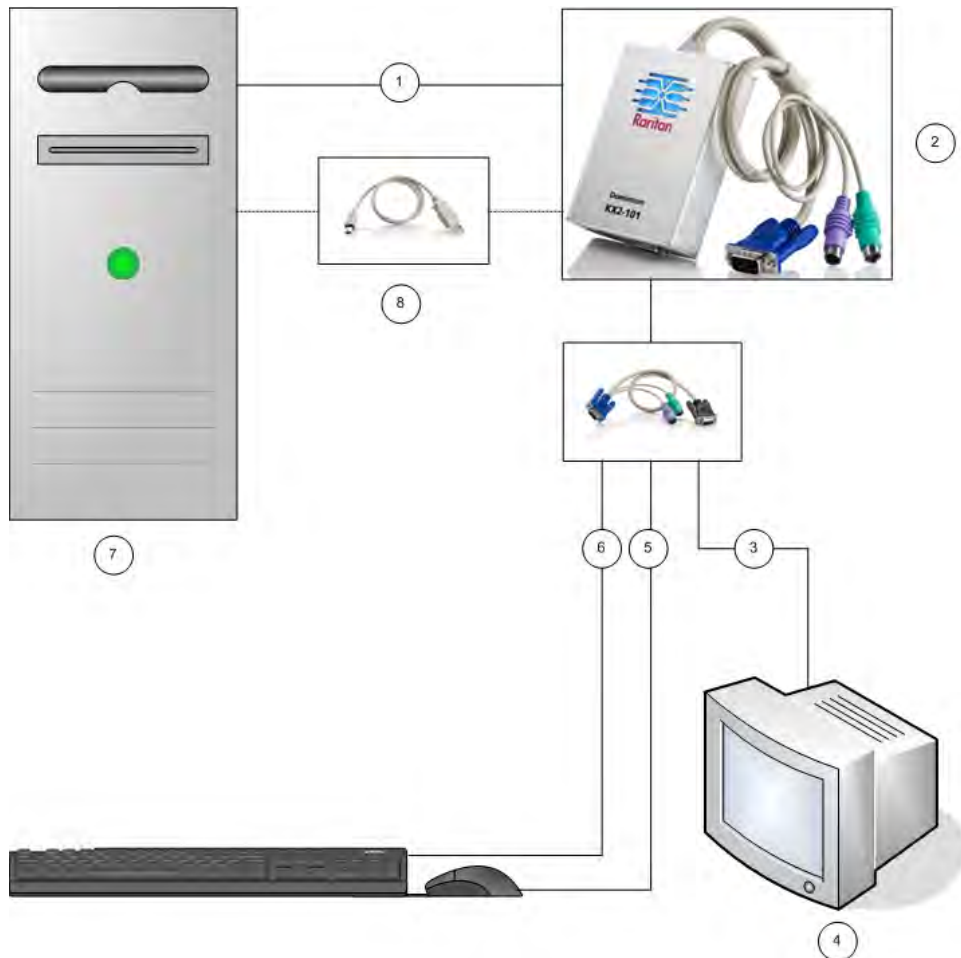
- *So konfigurieren Sie KX II-101 zur Verwendung mit einem PS/2-Zielserver:*
1. Verwenden Sie die angeschlossenen PS/2-Kabel für Tastatur, Video und Maus, um die KX II-101-Einheit mit dem Zielserver zu verbinden.
 2. Verwenden Sie die optionalen PS/2-Kabel, um die lokale Tastatur, den lokalen Monitor und die lokale Maus am Port „Local User“ der KX II-101-Einheit anzuschließen.

Hinweis: KX II-101 muss an das Stromnetz angeschlossen sein, damit der Port „Local User“ funktioniert.

3. Wenn Sie VM-Zugriff (virtuelle Medien) benötigen, schließen Sie den Mini-USB-Stecker an die KX II-101-Einheit und den USB-Stecker an einem USB-Port des Zielservers an.

Anschließen der KX II-101-Einheit

Nach der Verbindung sollte Ihr System wie folgt aussehen:



- 1 Integrierte PS/2-Tastatur-, Video- und Mausverbindungen von KX II-101 zum Zielserver
- 2 KX II-101
- 3 Videoverbindung zum lokalen Monitor (optionales Kabel)
- 4 Lokaler Monitor
- 5 PS/2-Verbindung von KX II-101 zur Maus (optionales Kabel)
- 6 PS/2-Verbindung von KX II-101 zur Tastatur (optionales Kabel)
- 7 Zielserver
- 8 Mitgeliefertes Mini-USB/USB-Kabel von KX II-101 zum Zielserver für den VM-Zugriff (virtuelle Medien)

USB-Konfiguration

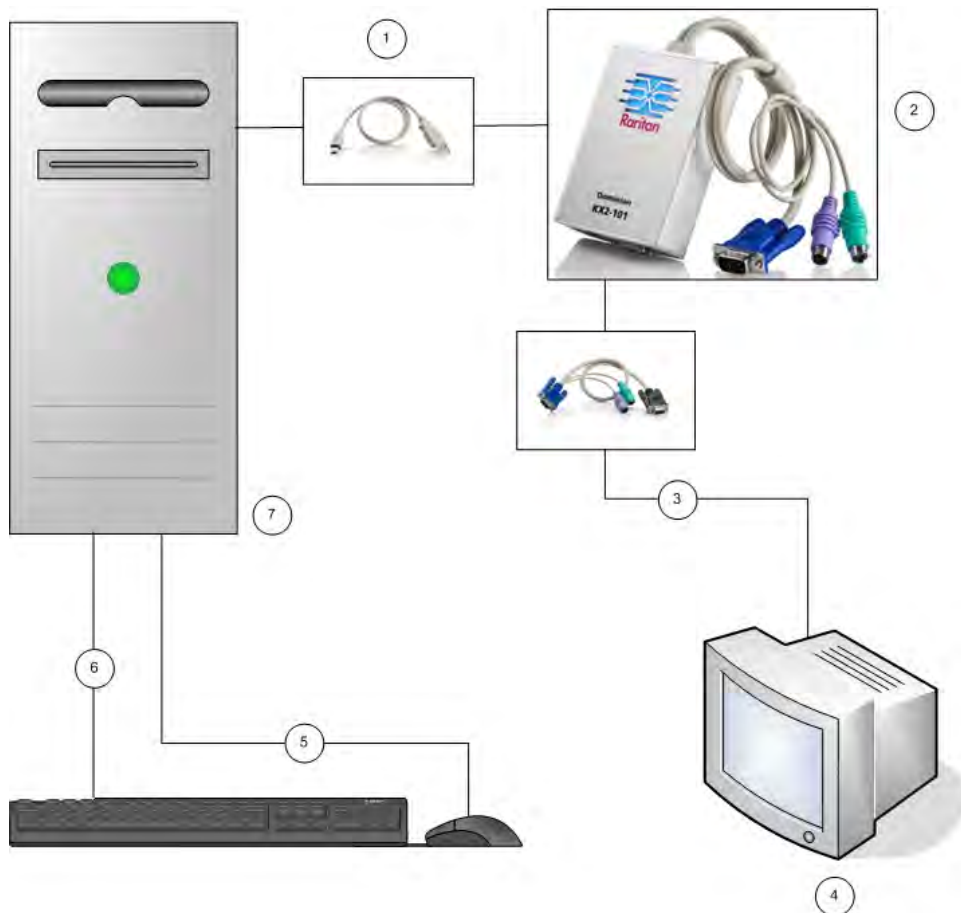
➤ *So konfigurieren Sie KX II-101 zur Verwendung mit einem USB-Zielserver:*

1. Schließen Sie den Mini-USB-Stecker an die KX II-101-Einheit und den USB-Stecker an einem USB-Port des Zielservers an.
2. Verwenden Sie die mitgelieferten PS/2 DKX2-101-LPKVMC-Kabel zur Verbindung des lokalen Video-Ports mit dem Port „Local User“ der KX II-101-Einheit.

Hinweis: KX II-101 muss an das Stromnetz angeschlossen sein, damit der Port „Local User“ funktioniert.

3. Verwenden Sie USB-Kabel, um die Tastatur und die Maus direkt mit dem Zielserver zu verbinden.

Nach der Verbindung sollte Ihr System wie folgt aussehen:



1 Mitgeliefertes Mini-USB/USB-Kabel von KX II-101 zum Zielserver

Anschließen der KX II-101-Einheit

- 2 KX II-101
- 3 Videoverbindung zum lokalen Monitor (optionales Kabel)
- 4 Lokaler Monitor
- 5 USB-Verbindung zwischen Zielservers und Maus
- 6 USB-Verbindung zwischen Zielservers und Tastatur
- 7 Zielservers

Verbinden mit dem 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 verwendet wird, und zeigt damit IP-Datenverkehr mit 10 Mbit/s an. Die grüne LED zeigt eine Verbindungsgeschwindigkeit von 100 Mbit/s an.

Stromversorgung der KX II-101-Einheit

KX II-101 kann entweder über das mitgelieferte Standardnetzteil oder über PoE (Power over Ethernet) mit Strom versorgt werden.

- Stecken Sie für die Standardstromversorgung das mitgelieferte Stromadapterkit in den Stromanschluss und das andere Ende in eine entsprechende Steckdose in der Nähe.
- Verbinden Sie für die Stromversorgung über PoE ein Ende eines 10/100Mbps-Kabels mit dem LAN-Port und das andere Ende mit einem PoE-fähigen LAN.

Nach dem Einschalten wird die KX II-101-Einheit hochgefahren. Dabei blinkt die blaue LED oberhalb des Raritan-Logos für etwa 45 Sekunden. Nach dem Hochfahren leuchtet die LED ständig.

Verwenden des Ports „ Admin “

Über den Port „Admin“ können Sie KX II-101 über ein Terminalemulationsprogramm, wie z. B. HyperTerminal, konfigurieren und einrichten. Verbinden Sie den Mini-DIN-Stecker des mitgelieferten seriellen Kabels mit dem Port „Admin“ der KX II-101-Einheit und den DB9-Stecker mit einem seriellen Port Ihres PC oder Laptops. Die Kommunikationseinstellungen des seriellen Ports sollten wie folgt konfiguriert werden: 115.200 Baud, 8 Datenbits, 1 Stoppbit, keine Parität und keine Flusssteuerung.

Weitere Informationen zur Konfiguration der KX II-101-Einheit über den Port „ Admin “ finden Sie unter Verwenden eines Terminalemulationsprogramms.

Verwenden des Ports „ Local User “

KX II-101 wird mit optionalen Video- und PS/2-Kabeln ausgeliefert, damit Sie eine Tastatur und Maus über den Port „Local User“ mit dem Zielsystem verbinden können. Der Port „Local User“ dient als Durchgang für den Zielsystem, mit dem die KX II-101-Einheit verbunden ist. Er hat keine weiteren Funktionen. KX II-101 muss eingeschaltet sein, damit der Port „Local User“ funktioniert.

Hinweis: Nur PS/2-Hostschnittstellenkonnektivität wird für den lokalen Port unterstützt, und Sie müssen den Zielsystem neu starten, nachdem Sie eine Verbindung zur KX II-101-Einheit über PS/2-Kabel hergestellt haben.

Konfigurieren der Einstellungen der Netzwerk-Firewall

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

Damit Sie die Webzugriffsmöglichkeiten von KX II-101 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-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.

Konfigurieren von KX II-101

KX II-101 kann wie folgt konfiguriert werden:

- Über die webbasierte KX II-101-Remote-Konsole, wobei die Einheit über eine Netzwerkverbindung mit Ihrer Workstation verfügen muss.
- Über ein Terminalemulationsprogramm, wie z. B. HyperTerminal, das eine direkte Verbindung zwischen dem Port „Admin“ der Einheit und Ihrer Workstation erfordert. Das Kabel für diese Verbindung ist im Lieferumfang von KX II-101 enthalten.

In diesem Abschnitt werden beide Konfigurationsmöglichkeiten für KX II-101 beschrieben.

Verwenden der Remote-Konsole

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

So konfigurieren Sie KX II-101:

- Ersetzen Sie das Standardkennwort durch ein neues Kennwort.
- Weisen Sie eine IP-Adresse zu.
- Benennen Sie den Zielservers.
- Erstellen Sie Benutzer und Gruppen.

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 konfigurieren.

1. Melden Sie sich bei einer Workstation an, die eine Netzwerkverbindung mit Ihrer KX II-101-Einheit herstellen kann.
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 der Einheit 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 im Feld **New Password** (Neues Kennwort) das neue Kennwort ein, und geben Sie es im Feld **Confirm New Password** (Neues Kennwort bestätigen) erneut 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

1. Wählen Sie in der KX II-101-Remote-Konsole **Device Settings** > **Network Settings** (Geräteeinstellungen > Netzwerkeinstellungen). Die Seite **Network Basic Settings** (Basisnetzwerkeinstellungen) wird angezeigt.

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *

DominionKX2-101

IP auto configuration

DHCP

Preferred host name (DHCP only)

IP address

192.168.50.241

Subnet mask

255.255.255.0

Gateway IP address

192.168.50.126

Primary DNS server IP address

192.168.50.114

Secondary DNS server IP address

192.168.50.112

OK Reset To Defaults Cancel

Konfigurieren von KX II-101

2. Geben Sie im Feld **Device Name** (Gerätename) einen aussagekräftigen Namen für Ihre KX II-101-Einheit ein. Sie können bis zu 16 alphanumerische Zeichen und Sonderzeichen aber keine Leerstellen verwenden.
3. Wählen Sie in der Dropdown-Liste **IP auto configuration** (Automatische IP-Konfiguration) die IP-Konfiguration aus:
 - **None** (Keine [statisches IP]): Diese Option ist die Standardeinstellung und wird empfohlen, da Dominion KX II-101 ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte. Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.
 - **DHCP**: Bei Auswahl dieser Option werden die Netzwerkparameter vom DHCP-Server beim Hochfahren der KX II-101-Einheit zugewiesen.

Konfigurieren des direkten Port-Zugriffs

➤ *So konfigurieren Sie den direkten Port-Zugriff:*

1. Wählen Sie **Device Settings > Device Services** (Geräteeinstellungen > Gerätedienste). Die Seite **Device Services** (Gerätedienste) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen **Enable Direct Port Access via URL** (Direkten Port-Zugriff über URL aktivieren).
3. Aktivieren Sie den globalen Telnet- oder SSH-Zugriff.
 - Aktivieren Sie das Kontrollkästchen **Enable TELNET Access**, um den TELNET-Zugriff zu aktivieren.
 - Aktivieren Sie das Kontrollkästchen **Enable SSH Access**, um den SSH-Zugriff zu aktivieren.
4. Geben Sie einen gültigen TCP-Port für die ausgewählte Zugriffsart an. Der direkte Port-Zugriff kann z. B. über den Telnet-TCP-Port 7770 konfiguriert werden.

Home > Device Settings > Device Services

Services

Discovery Port *

 Enable TELNET Access

TELNET Port

 Enable SSH Access

SSH Port

 Enable Direct Port Access via URL

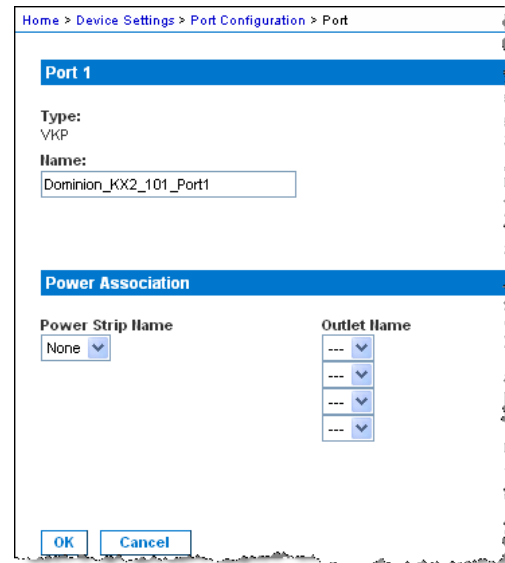
5. Klicken Sie zum Speichern der Informationen auf **OK**.

Benennen des Zielservers

1. Falls noch nicht geschehen, verbinden Sie die KX II-101-Einheit mit dem Zielserver (siehe *Herstellen einer Verbindung mit der KX II-101-Einheit* (auf Seite 35)).
2. Wählen Sie **Device Settings > Port Configuration** (Geräteeinstellungen > Port-Konfiguration). Die Seite **Port Configuration** (Port-Konfiguration) wird angezeigt.

Konfigurieren von KX II-101

3. Klicken Sie unter **Port Name** (Port-Name) auf den Zielsever. Die Seite **Port** wird angezeigt.



4. Geben Sie einen Namen ein (bis zu 32 alphanumerische Zeichen und Sonderzeichen).
5. Klicken Sie auf **OK**.

Erstellen von Benutzern und Gruppen

Benutzergruppen werden bei der lokalen und der Remote-Authentifizierung (über RADIUS oder LDAP) verwendet. Es ist empfehlenswert, Benutzergruppen vor dem Erstellen einzelner Benutzer zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe zugeordnet werden muss.

➤ *So erstellen Sie eine Benutzergruppe:*

1. Öffnen Sie die Seite **Group** (Gruppe) mit einem der folgenden Verfahren:
 - a. Wählen Sie **User Management > Add New User Group** (Benutzerverwaltung > Neue Benutzergruppe hinzufügen), oder
 - b. klicken Sie auf der Seite **User Group List** (Liste der Benutzergruppen) auf die Schaltfläche **Add** (Hinzufügen).
2. Geben Sie im Feld **Groupname** (Gruppenname) einen beschreibenden Namen für die neue Benutzergruppe ein.

3. Legen Sie unter **Permissions** (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen der Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten.
4. Legen Sie unter **Port Permissions** (Port-Berechtigungen) die Port-Berechtigungen fest (**Access** [Zugriff], **VM Access** [VM-Zugriff] und **Power Control** [Stromzufuhrsteuerung]). Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Server-Ports fest, und geben Sie die Zugriffsart an. Standardmäßig sind alle Port-Berechtigungen einschließlich des VM-Zugriffs (virtuelle Medien) deaktiviert. Um virtuelle Medien verwenden zu können, muss diese Berechtigung aktiviert sein.
5. Klicken Sie auf **OK**.

➤ *So erstellen Sie einen neuen Benutzer:*

1. Öffnen Sie die Seite **User** (Benutzer) mit einem der folgenden Verfahren:
 - a. Wählen Sie **User Management > Add New User** (Benutzerverwaltung > Neuen Benutzer hinzufügen), oder
 - b. 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** den vollständigen Namen des Benutzers ein (bis zu 64 Zeichen).
4. Geben Sie im Feld **Password** ein Kennwort ein, und geben Sie es im Feld **Confirm Password** (Kennwort bestätigen) erneut ein (bis zu 64 Zeichen).
5. Wählen Sie in der Dropdown-Liste **User Group** (Benutzergruppe) die Gruppe aus. Die Liste enthält alle von Ihnen erstellten Gruppen sowie die vom System bereitgestellten Standardgruppen (**Admin**, **<Unknown>** [Unbekannt], **Individual Group** [Individuelle Gruppe]). Wenn Sie diesen Benutzer keiner vorhandenen Benutzergruppe zuordnen möchten, wählen Sie in der Dropdown-Liste die Option **Individual Group** (Individuelle Gruppe).
6. Klicken Sie auf **OK**.

Verwenden eines Terminalemulationsprogramms

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

- IP-Adresse
- Adresse der Subnetzmaske
- Gateway-Adresse
- IP-Zugriffssteuerung
- LAN-Geschwindigkeit
- LAN-Schnittstellenmodus

Damit Sie ein Terminalemulationsprogramm mit KX II-101 verwenden können, müssen Sie zunächst das mitgelieferte serielle RS-232-Kabel vom Port „Admin“ der KX II-101-Einheit mit dem COM1-Port Ihres PC verbinden. Weitere Informationen finden Sie unter *Verwenden des Ports „Admin“* (auf Seite 23).

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

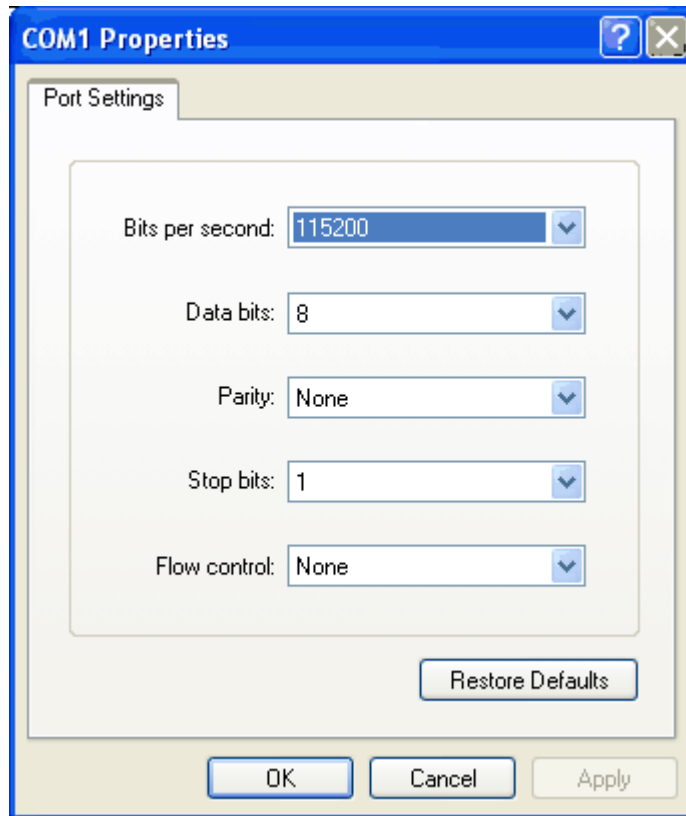
➤ *So verwenden Sie ein Terminalemulationsprogramm zur Konfiguration von KX II-101:*

1. Verbinden Sie KX II-101 über das mitgelieferte serielle RS-232-Kabel mit einem lokalen PC.

Stellen Sie eine Verbindung zwischen dem Port „Admin“ der KX II-101-Einheit und dem COM1-Port des PCs her.

2. Starten Sie das Terminalemulationsprogramm, das Sie zur Konfiguration von KX II-101 verwenden möchten.
3. Legen Sie die folgenden Port-Einstellungen im Terminalemulationsprogramm fest:
 - Bits per second (Bits pro Sekunde): 115200
 - Data bits (Datenbits): 8
 - Parity (Parität): None (Keine)
 - Stop bits (Stoppbits): 1

- Flow control (Flusssteuerung): None (Keine)



4. Stellen Sie eine Verbindung zur KX II-101-Einheit her.
Das Anmeldefenster wird angezeigt.



5. Geben Sie den Administrator-Benutzernamen ein, und drücken Sie die **Eingabetaste**.

Konfigurieren von KX II-101

Sie werden zur Eingabe des Kennworts aufgefordert.

```
Login: admin
Password: _
```

6. Geben Sie Ihr Kennwort ein, und drücken Sie die **Eingabetaste**.
Die Eingabeaufforderung für den Port „Admin“ wird angezeigt.

```
Login: admin
Password: MACADDR: 00:0d:5d:03:5d:23

-----
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC          FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153          Idle Timeout: 30min
-----

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

Current Time: Fri Dec 28 19:44:16 2007
Admin Port >
```

7. Geben Sie `config` an der Eingabeaufforderung **Admin Port >** ein, und drücken Sie die **Eingabetaste**.
8. Geben Sie `network` an der Eingabeaufforderung **Config >** ein, und drücken Sie die **Eingabetaste**.
9. Sie können die aktuellen Schnittstelleneinstellungen anzeigen. Geben Sie dazu `interface` an der Eingabeaufforderung **Interface >** ein, und drücken Sie die **Eingabetaste**.

Die aktuellen Schnittstelleneinstellungen werden angezeigt:

```

Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC         FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153        Idle Timeout: 30min
-----
Port No.  Port Name                Port Type  Port Status  Port Availability
1 - Dominion_KXII-101_Port  K0M      up          idle

Current Time: Fri Dec 28 19:52:26 2007

Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface

IP auto configuration: dhcp
IP address: 192.168.50.153
Netmask: 255.255.255.0
Gateway: 192.168.50.126
Ethernet node: Autodetect

Admin Port > Config > Network > _
    
```

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	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>
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	Subnetzmaske	Die IP-Adresse der Subnetzmaske.
gw	IP-Adresse	Die Gateway-IP-Adresse.

Konfigurieren von KX II-101

Befehl	Argument	Optionen
mode	Modus	Der Ethernet-Modus. Folgende Optionen stehen zur Auswahl: auto : Die Geschwindigkeit und der Schnittstellenmodus werden automatisch basierend auf dem Netzwerk festgelegt. 10hdx (10 Mbit/s, Halbduplex) 10fdx (10 Mbit/s, Vollduplex) 100hdx (100 Mbit/s, Halbduplex) 100fdx (100 Mbit/s, Vollduplex)

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.
```

1. Geben Sie nach der Konfiguration von KX II-101 an der Eingabeaufforderung `logout` ein, und drücken Sie die **Eingabetaste**.

Sie werden von der der Befehlszeilenschnittstelle abgemeldet.

Kapitel 4 Herstellen einer Verbindung mit der KX II-101-Einheit

In diesem Kapitel

Unterstützte Sprachen.....	35
Java Runtime Environment (JRE)	35
Starten der KX II-101-Einheit	36
Verwalten von Favoriten	41
Seite „ Port Access “ (Port-Zugriff)	49

Unterstützte Sprachen

KX II-101 bietet Tastaturunterstützung für folgende Sprachen: amerikanisches Englisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Japanisch, Koreanisch, Französisch und Deutsch.

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der KX II-101-Remote-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

Sprachkonfiguration für Linux

Weitere Informationen zum Konfigurieren von Tastaturen mit anderem Layout unter Linux finden Sie unter **Keyboard Type** im Benutzerhandbuch *KVM and Serial Access Clients User Guide*.

Java Runtime Environment (JRE)

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

Starten der KX II-101-Einheit

Für die KX II-101-Remote-Konsole und den MPC ist die JRE erforderlich. Die KX II-101-Remote-Konsole überprüft die Java-Version. Falls die Version falsch oder veraltet ist, werden Sie aufgefordert, eine kompatible Version herunterzuladen.

Raritan empfiehlt zur Gewährleistung einer optimalen Leistung die Verwendung von Java Runtime Environment (JRE) Version 1.5. Die KX II-101-Remote-Konsole und MPC funktionieren auch mit JRE Version 1.4.2_05 oder höher (mit Ausnahme von JRE 1.5.0_02), einschließlich JRE 1.6.x (mit Ausnahme von 1.6.2).

Hinweis: Damit mehrsprachige Tastaturen in der KX II-101-Remote-Konsole (Virtual KVM Client) funktionieren, müssen Sie die mehrsprachige Version der Java Runtime Environment (JRE) installieren.

Starten der KX II-101-Einheit

Wichtig: Unabhängig vom verwendeten Browser müssen Popups für die IP-Adresse des Dominion-Geräts zugelassen werden, damit die KX II-101-Remote-Konsole gestartet werden kann.

Je nach Browser- und Sicherheitseinstellungen werden möglicherweise verschiedene Sicherheits- und Zertifikatwarnungen angezeigt. Sie müssen diese Warnungen bestätigen, um die KX II-101-Remote-Konsole zu starten.

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

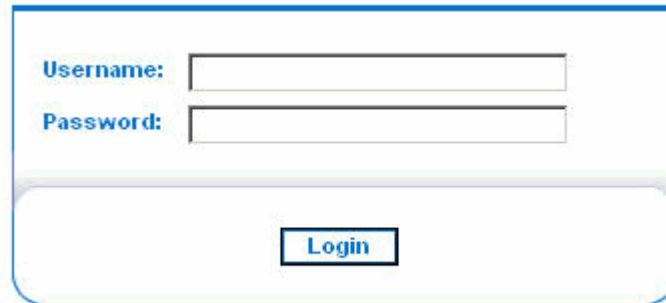
- In the future, do not show this warning (Diese Warnung nicht mehr anzeigen).
- Always trust content from this publisher (Inhalt von diesem Herausgeber immer vertrauen).

➤ *So starten Sie die KX II-101-Remote-Konsole:*

1. Melden Sie sich bei einer Workstation an, die eine Netzwerkverbindung zu KX II-101 herstellen kann und auf der Java Runtime Environment Version 1.4.2_05 oder höher installiert ist (JRE ist verfügbar unter <http://java.sun.com/> <http://java.sun.com>).
2. Starten Sie einen unterstützten Webbrowser, z. B. Internet Explorer (IE) oder Firefox. Siehe Unterstützte Browser.

Kapitel 4: Herstellen einer Verbindung mit der KX II-101-Einheit

3. Geben Sie den folgenden URL ein: `http://IP-ADRESSE`, wobei IP-ADRESSE die der KX II-101-Einheit zugewiesene IP-Adresse ist. Sie können auch „https“ verwenden, den vom Administrator zugewiesenen DNS-Namen der KX II-101-Einheit (sofern ein DNS-Server konfiguriert wurde) oder einfach die IP-Adresse in den Browser eingeben (KX II-101 leitet die IP-Adresse stets von HTTP zu HTTPS um). Das Anmeldefenster wird geöffnet.



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

Aktivieren des direkten Port-Zugriffs

Über direkten Port-Zugriff können Sie auf den KX II-101-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-Remote-Konsole.
2. Wählen Sie **Device Settings > Device Services** (Geräteeinstellungen > Gerätedienste). Die Seite **Device Services** (Gerätedienste) wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Enable Direct Port Access via URL** (Direkten Port-Zugriff über URL aktivieren).
4. Klicken Sie zum Speichern der Einstellungen auf **Save** (Speichern).

Starten der KX II-101-Einheit

- *So definieren Sie einen URL für den direkten Port-Zugriff:*
- Definieren Sie einen URL mit IP-Adresse, Benutzername, Kennwort, und, falls erforderlich, Port-Nummer der KX II-101-Einheit.

Steht nur ein KVM-Port zur Verfügung, ist die Port-Nummer nicht erforderlich.

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

```
https://[IP-Adresse]/dpa.asp?username=[Benutzername]&password=[Kennwort]&port=[Port-Nummer]
```

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

Layout der KX II-101-Konsole

Die KX II-101-Remote-Konsole bietet eine HTML-Oberfläche (vergleichbar mit einem Browser) zur Konfiguration und Verwaltung sowie eine Liste und Auswahl der Zielsever. Die Optionen befinden sich auf verschiedenen Registerkarten.

Nach der erfolgreichen Anmeldung wird die Seite **Port Access** (Port-Zugriff) angezeigt, in der alle Ports mit ihrem Status und ihrer Verfügbarkeit aufgeführt sind.

Navigation in der KX II-101-Konsole

In der Oberfläche der KX II-101-Remote-Konsole haben Sie viele Möglichkeiten für die Navigation und Auswahl.

- *Für die Auswahl von Optionen stehen folgende Möglichkeiten zur Verfügung:*
 - Klicken Sie auf eine Registerkarte, um eine Seite der verfügbaren Optionen anzuzeigen.
 - Zeigen Sie mit dem Cursor auf eine Registerkarte, und wählen Sie die gewünschte Option aus dem Menü aus.
 - Klicken Sie in der angezeigten Menühierarchie (den so genannten „Breadcrumbs“) direkt auf die gewünschte Option.

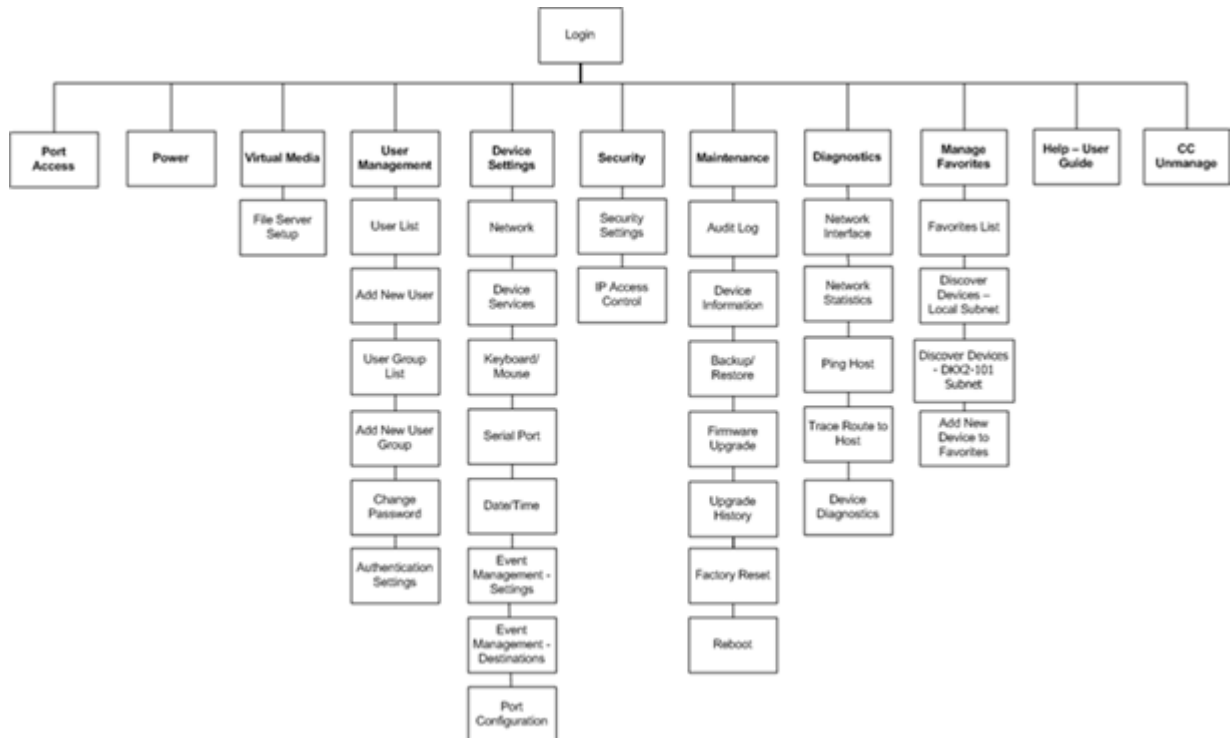
Category	Event	SNMP	Syslog	Audit Log
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure			<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- *So blättern Sie durch Seiten:*
 - Verwenden Sie die **Bild-Auf-** und **Bild-Ab-**Tasten der Tastatur, oder
 - verwenden Sie die Bildlaufleiste auf der rechten Seite.

Starten der KX II-101-Einheit

Menüstruktur der KX II-101-Remote-Konsole

Das folgende Diagramm zeigt alle in der KX II-101-Remote-Konsole verfügbaren Menüoptionen:



Abmelden

➤ *So beenden Sie die KX II-101-Remote-Konsole:*

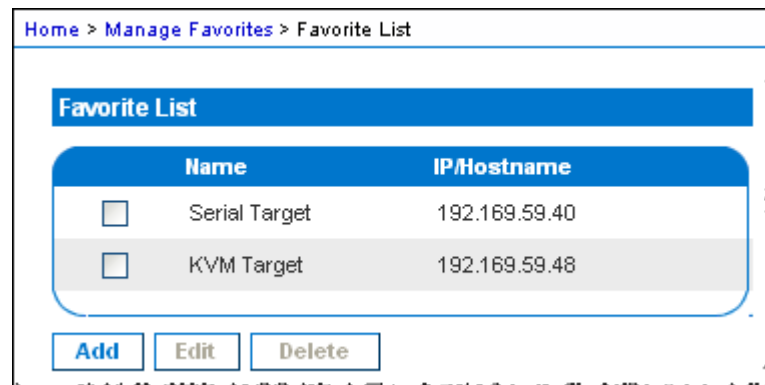
- Klicken Sie oben rechts auf der Seite auf **Logout** (Abmelden).

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

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
- Aufführen der Favoriten nach Name oder IP-Adresse
- Erkennen von KX II-101-Geräten im Subnetz (vor und nach der Anmeldung)
- Abrufen erkannter KX II-101-Geräte vom verbundenen Gerät (nach der Anmeldung)



Verwalten von Favoriten

- *So greifen Sie auf ein bevorzugtes KX II-101-Gerät zu:*
 - Klicken Sie auf den unterhalb von **Favorite Devices** (Bevorzugte Geräte) aufgeführten Namen des gewünschten Geräts. Ein neues Browserfenster wird geöffnet.
- *So wechseln Sie zwischen der Namens- und der IP-Adressenansicht der Liste **Favorite Devices** (Bevorzugte Geräte):*

Anzeigen der Favoriten nach IP-Adresse:

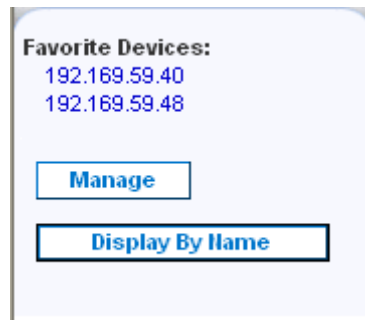
Klicken Sie auf die Schaltfläche **Display by IP** (Nach IP-Adresse anzeigen).

Bevorzugte Geräte, angezeigt nach Name. Klicken Sie zum Wechseln auf **Display by IP** (Nach IP-Adresse anzeigen).

Anzeigen der Favoriten nach Name:

Klicken Sie auf die Schaltfläche **Display by Name** (Nach Name anzeigen).

Bevorzugte Geräte, angezeigt nach IP-Adresse. Klicken Sie zum Wechseln auf **Display by Name** (Nach Name anzeigen).



Menü „ Manage Favorites “ (Favoriten verwalten)

- *So öffnen Sie das Menü „Manage Favorites“ (Favoriten verwalten):*
 - Klicken Sie auf die Schaltfläche **Manage** (Verwalten). Die Seite **Manage Favorites** (Favoriten verwalten) wird angezeigt. Diese Seite enthält die folgenden Optionen:

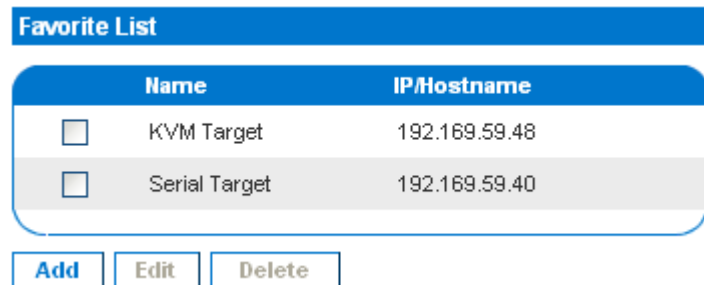
Option	Aktion
Favorites List (Favoritenliste)	Verwalten einer Liste bevorzugter Geräte

Option	Aktion
Discover Devices - Local Subnet (Geräte erkennen – Lokales Subnetz)	Erkennen der Geräte im lokalen Subnetz
Discover Devices - KX II-101 Subnet (Geräte erkennen – KX II-101-Subnetz)	Erkennen der Geräte im Subnetz des KX II-101-Geräts
Add New Device to Favorites (Neues Gerät zu Favoriten hinzufügen)	Hinzufügen, Bearbeiten und Löschen von Geräten in der Favoritenliste

Favorites List (Favoritenliste)

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

- *So öffnen Sie die Seite „Favorites List“ (Favoritenliste):*
 - Wählen Sie **Manage > Favorites List** (Verwalten > Favoritenliste). Die Seite **Favorites List** (Favoritenliste) wird angezeigt.



- *So fügen Sie einen Favoriten hinzu:*
 - Klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Die Seite **Add New Favorite (Neuen Favoriten hinzufügen)** (auf Seite 48) wird angezeigt.

- *So löschen Sie einen Favoriten:*

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

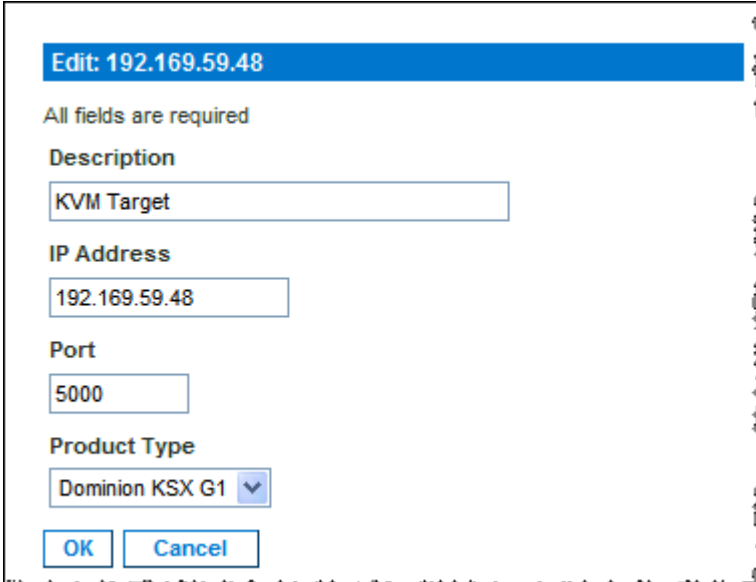
1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten KX II-101-Gerät.

Verwalten von Favoriten

2. Klicken Sie auf die Schaltfläche **Delete** (Löschen). Der Favorit wird aus der Favoritenliste entfernt.

➤ *So bearbeiten Sie einen Favoriten:*

1. Aktivieren Sie auf der Seite **Favorites List** (Favoritenliste) das Kontrollkästchen neben dem gewünschten KX II-101-Gerät.
2. Klicken Sie auf die Schaltfläche **Edit** (Bearbeiten). Die Seite **Edit** (Bearbeiten) wird angezeigt.



Edit: 192.169.59.48

All fields are required

Description

KVM Target

IP Address

192.169.59.48

Port

5000

Product Type

Dominion K5X G1 ▼

OK Cancel

3. Aktualisieren Sie die Felder nach Bedarf:
 - **Description** (Beschreibung): Geben Sie aussagekräftige Informationen ein.
 - **IP Address** (IP-Adresse): Geben Sie die IP-Adresse der KX II-101-Einheit ein.
 - **Port**: Ändern Sie ggf. den Erkennungs.Port.
 - **Product Type** (Produktart).
4. Klicken Sie auf **OK**.

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

Mit dieser Option finden Sie die Geräte im lokalen Subnetz (d. h. dem Subnetz, in dem die KX II-101-Remote-Konsole ausgeführt wird). Sie können direkt von dieser Seite auf die Geräte zugreifen oder sie Ihrer Favoritenliste hinzufügen.

	Name	IP/Hostname
<input type="checkbox"/>	DKX2-101	192.168.50.68
<input type="checkbox"/>	KX_KIM-0050	192.168.50.12
<input type="checkbox"/>	shoalb-sx	192.168.50.239
<input type="checkbox"/>	shoalbkx2	192.168.50.234

➤ *So finden Sie Geräte im lokalen Subnetz:*

1. Wählen Sie **Favorites > Discover Devices - Local Subnet** (Favoriten > Geräte erkennen – Lokales Subnetz). Die Seite **Discover Devices – Local Subnet** (Geräte erkennen – Lokales Subnetz) wird angezeigt.
2. Wählen Sie den entsprechenden Erkennungs-Port aus (Informationen zum Erkennungs-Port finden Sie unter Netzwerkeinstellungen):
 - 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 Port-Nummer im Feld **Discover on Port** (Erkennungs-Port) ein.
 - c. Klicken Sie auf **Save** (Speichern).

Verwalten von Favoriten

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).

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

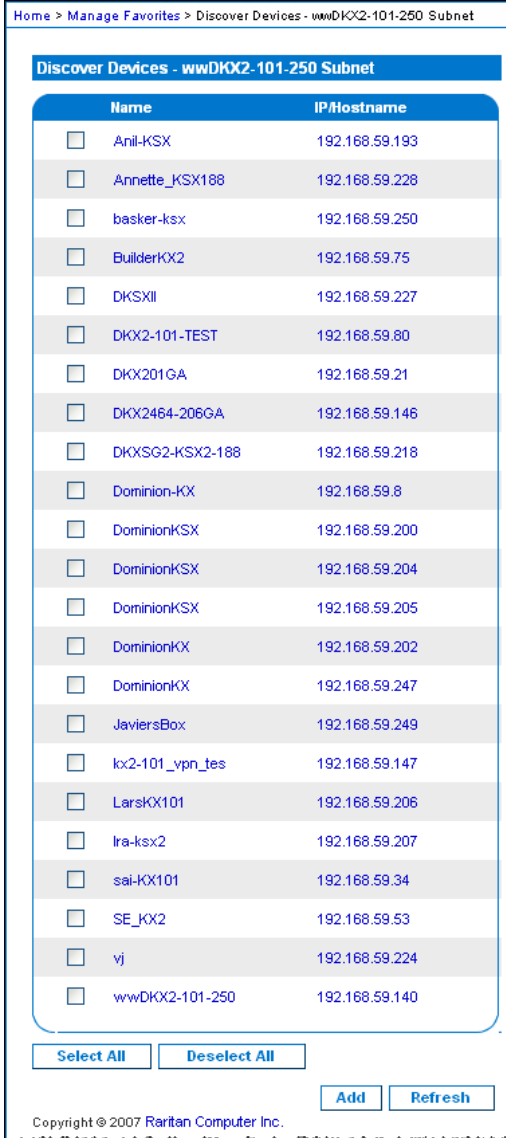
➤ *So greifen Sie auf ein erkanntes Gerät zu:*

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

Discover Devices - KX II-101 Subnet (Geräte erkennen - KX II-101-Subnetz)

Mit dieser Option finden Sie die Geräte im Subnetz des Geräts (d. h. dem Subnetz der KX II-101-Geräte-IP-Adresse selbst). Sie können direkt von dieser Seite auf die Geräte zugreifen oder sie Ihrer Favoritenliste hinzufügen.

Mit diesem Feature arbeiten mehrere KX II-101-Einheiten zusammen und werden automatisch skaliert. Die KX II-101-Remote-Konsole erkennt die KX II-101-Einheiten im KX II-101-Subnetz automatisch.



Name	IP/Hostname
<input type="checkbox"/> Anil-KSX	192.168.59.193
<input type="checkbox"/> Annette_KSX188	192.168.59.228
<input type="checkbox"/> basker-ksx	192.168.59.250
<input type="checkbox"/> BuilderKX2	192.168.59.75
<input type="checkbox"/> DKSXII	192.168.59.227
<input type="checkbox"/> DKX2-101-TEST	192.168.59.80
<input type="checkbox"/> DKX201GA	192.168.59.21
<input type="checkbox"/> DKX2464-206GA	192.168.59.146
<input type="checkbox"/> DKXSG2-KSX2-188	192.168.59.218
<input type="checkbox"/> Dominion-KX	192.168.59.8
<input type="checkbox"/> DominionKSX	192.168.59.200
<input type="checkbox"/> DominionKSX	192.168.59.204
<input type="checkbox"/> DominionKSX	192.168.59.205
<input type="checkbox"/> DominionKX	192.168.59.202
<input type="checkbox"/> DominionKX	192.168.59.247
<input type="checkbox"/> JaviersBox	192.168.59.249
<input type="checkbox"/> kx2-101_vpn_tes	192.168.59.147
<input type="checkbox"/> LarsKX101	192.168.59.206
<input type="checkbox"/> Ira-ksx2	192.168.59.207
<input type="checkbox"/> sai-KX101	192.168.59.34
<input type="checkbox"/> SE_KX2	192.168.59.53
<input type="checkbox"/> vj	192.168.59.224
<input type="checkbox"/> wwDKX2-101-250	192.168.59.140

[Select All](#) [Deselect All](#) [Add](#) [Refresh](#)

Copyright © 2007 Raritan Computer Inc.

Verwalten von Favoriten

- *So finden Sie Geräte im Subnetz des Geräts:*
1. Wählen Sie **Favorites > Discover Devices - KX II-101 Subnet** (Favoriten > Geräte erkennen – KX II-101-Subnetz). Die Seite **Discover Devices – KX II-101 Subnet** (Geräte erkennen – KX II-101-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).

*Tipp: Verwenden Sie die Schaltflächen **Select All** (Alle auswählen) und **Deselect All** (Alle entfernen), um schnell alle Geräte im Subnetz des KX II-101-Geräts auszuwählen bzw. diese Auswahl aufzuheben.*

- *So greifen Sie auf ein erkanntes Gerät zu:*
- Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

Add New Favorite (Neuen Favoriten hinzufügen)

- *So fügen Sie der Favoritenliste ein Gerät hinzu:*
1. Wählen Sie **Manage Favorites > Add New Device to Favorites** (Favoriten verwalten > Neues Gerät zu Favoriten hinzufügen). Die Seite **Add New Favorite** (Neuen Favoriten hinzufügen) wird angezeigt.
 2. Geben Sie im Feld **Description** eine aussagekräftige Beschreibung ein.
 3. Geben Sie die IP-Adresse des Geräts ein.
 4. Ändern Sie ggf. den Erkennungs-Port.
 5. Klicken Sie auf **OK**.

Das Gerät wird Ihrer Favoritenliste hinzugefügt.

Seite „ Port Access “ (Port-Zugriff)

Nachdem Sie sich erfolgreich bei der KX II-101-Remote-Konsole angemeldet haben, wird die Seite **Port Access** (Port-Zugriff) angezeigt. Diese Seite enthält den KX II-101-Port, den Status und die Verfügbarkeit. Über die Seite **Port Access** (Port-Zugriff) haben Sie Zugriff auf den mit KX II-101 verbundenen KVM-Zielservers. Ein KVM-Zielservers ist ein Server, den Sie über die KX II-101-Einheit steuern möchten. Er ist mit KX II-101 über die PS/2-Kabel am Gerät verbunden.

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

- So verwenden Sie die Seite „Port Access“ (Port-Zugriff):
1. Klicken Sie in der KX II-101-Remote-Konsole auf die Registerkarte **Port Access** (Port-Zugriff). Die Seite **Port Access** (Port-Zugriff) wird angezeigt:

No.	Name	Availability
1	Dominion_KX2_101_Port5	idle

- **No.** (Nr.): Es steht nur ein Port für KX II-101 zur Verfügung.
 - **Name:** Der Name des KX II-101-Ports. Die Standardeinstellung **Dominion-KX101G2_Port1** können Sie jederzeit in einen aussagekräftigeren Namen ändern.
 - **Availability** (Verfügbarkeit): Für die Verfügbarkeit stehen die Werte **Idle** (Inaktiv), **Connected** (Verbunden), **Busy** (Verwendet) und **Unavailable** (Nicht verfügbar) zur Verfügung.
2. Klicken Sie zum Verbinden mit dem Zielservers auf den Namen des Geräts/Zielservers. Klicken Sie dann auf das Pop-up-Fenster **Connect** (Verbinden). Das Fenster **Virtual KVM Client** wird angezeigt, und die Verfügbarkeit wird als **Busy** (Verwendet) angezeigt.
 3. Klicken Sie zum Trennen der Verbindung mit dem Zielservers auf den Namen des Geräts/Zielservers. Klicken Sie dann auf das Pop-up-Fenster **Disconnect** (Trennen). Das Fenster **Virtual KVM Client** wird geschlossen, und die Verfügbarkeit wird als **Idle** (Inaktiv) angezeigt.

Seite „Port Access“ (Port-Zugriff)

Kapitel 5 Benutzer, Gruppen und Zugriffsberechtigungen

In diesem Kapitel

Benutzer	51
Gruppen	51
Beziehung zwischen Benutzern und Gruppen.....	52
Benutzerverwaltung.....	52
Remote-Authentifizierung.....	67

Benutzer

Für den Zugriff auf die KX II-101-Einheit sind ein Benutzername und ein Kennwort erforderlich. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf die KX II-101-Einheit zuzugreifen. Weitere Informationen zum Hinzufügen und Bearbeiten von Benutzern finden Sie unter *Benutzerverwaltung* (auf Seite 52).

Gruppen

Jede KX II-101-Einheit verfügt über drei Standardbenutzergruppen, die nicht gelöscht werden können:

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.

Beziehung zwischen Benutzern und Gruppen

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.
--	--

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

Beziehung zwischen Benutzern und Gruppen

Benutzer sind Mitglied in einer Gruppe, und Gruppen verfügen über bestimmte Berechtigungen. Sie können Zeit sparen, indem Sie die verschiedenen Benutzer Ihrer KX II-101-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, d. h. die Zugriffsberechtigungen für verschiedene Server-Ports, ob ein Neustart des Geräts zulässig ist und weitere Funktionen.

Benutzerverwaltung

Menü „ User Management “ (Benutzerverwaltung)

Das Menü **User Management** (Benutzerverwaltung) umfasst folgende Optionen:

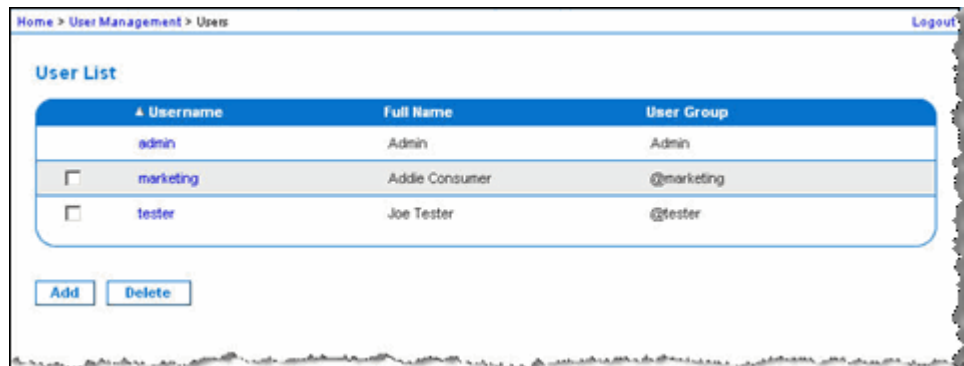
Option	Aktion
User List (Benutzerliste)	Anzeigen einer alphabetischen Liste aller Benutzer; Hinzufügen, Ändern oder Löschen von Benutzern

Option	Aktion
Add New User (Neuen Benutzer hinzufügen)	Hinzufügen neuer Benutzer, Ändern von Benutzerinformationen
User Group List (Liste der Benutzergruppen)	Anzeigen einer alphabetischen Liste aller Benutzergruppen; Hinzufügen, Ändern oder Löschen von Benutzergruppen
Add New User Group (Neue Benutzergruppe hinzufügen)	Hinzufügen neuer Benutzergruppen, Ändern von Informationen zu Benutzergruppen
Change Password (Kennwort ändern)	Ändern des Kennworts eines bestimmten Benutzers
Authentication Settings (Authentifizierungseinstellungen)	Konfigurieren der Authentifizierung für den Zugriff auf KX II-101

User List (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 außerdem Benutzer hinzufügen, ändern oder löschen.

- *So zeigen Sie die Benutzerliste an:*
 - Wählen Sie **User Management > User List** (Benutzerverwaltung > Benutzerliste). Die Seite **User List** (Benutzerliste) wird angezeigt.



- *So fügen Sie einen neuen Benutzer hinzu:*
 - Klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Die Seite **User** (Benutzer) wird angezeigt. Umfassende Informationen zur Seite **User** (Benutzer) finden Sie unter *Add New User (Neuen Benutzer hinzufügen)* (auf Seite 54).
- *So ändern Sie einen vorhandenen Benutzer:*
 1. Wählen Sie den gewünschten Benutzer aus der Liste aus.
 2. Klicken Sie auf den Benutzernamen. Die Seite **User** (Benutzer) wird angezeigt. Umfassende Informationen zum Bearbeiten von Benutzern finden Sie unter *Ändern vorhandener Benutzer* (auf Seite 56).
- *So löschen Sie einen Benutzer:*
 1. Wählen Sie einen Benutzer aus der Liste aus, indem Sie das Kontrollkästchen links vom Benutzernamen aktivieren.
 2. Klicken Sie auf **Delete** (Löschen). Sie werden aufgefordert, den Löschvorgang zu bestätigen.
 3. Klicken Sie auf **OK**.

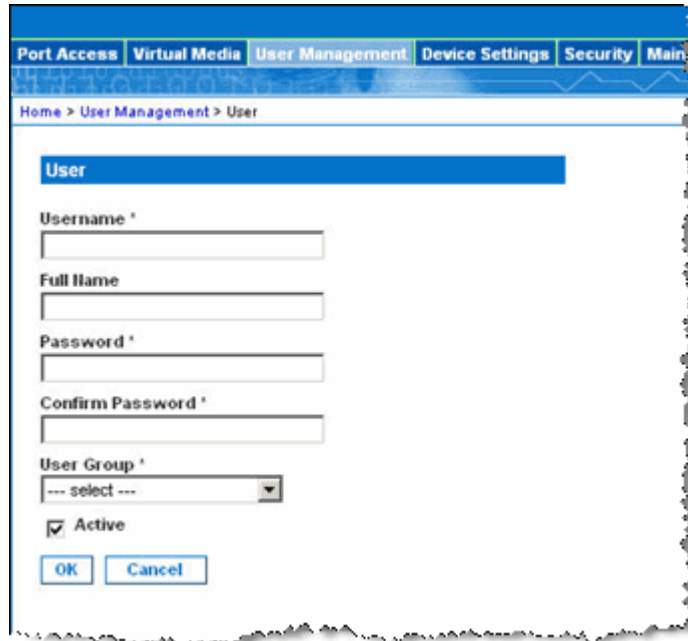
Add New User (Neuen Benutzer hinzufügen)

Es ist empfehlenswert, Benutzergruppen vor dem Erstellen von KX II-101-Benutzern zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe zugewiesen werden muss. Auf der Seite **User** (Benutzer) können Sie neue Benutzer hinzufügen, Benutzerinformationen ändern und deaktivierte Benutzer erneut aktivieren.

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

- *So fügen Sie einen neuen Benutzer hinzu:*
 1. Öffnen Sie die Seite **User** (Benutzer) mit einem der folgenden Verfahren:
 - Wählen Sie **User Management > Add New User** (Benutzerverwaltung > Neuen Benutzer hinzufügen), oder

- klicken Sie auf der Seite **User List** (Benutzerliste) auf die Schaltfläche **Add** (Hinzufügen).



The screenshot shows a web interface for user management. At the top, there is a navigation bar with tabs for 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', 'Security', and 'Main'. Below the navigation bar, the breadcrumb path is 'Home > User Management > User'. The main content area is titled 'User' and contains a form with the following fields: 'Username *', 'Full Name', 'Password *', 'Confirm Password *', 'User Group *' (a dropdown menu with '--- select ---' selected), and a checked checkbox for 'Active'. At the bottom of the form are 'OK' and 'Cancel' buttons.

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

Hinweis: Der Benutzer **Admin** muss der Gruppe **Admin** angehören.

Weitere Informationen zu den Berechtigungen einer individuellen Gruppe finden Sie unter *Festlegen von Berechtigungen für individuelle Gruppen* (auf Seite 61).

Benutzerverwaltung

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

Ändern vorhandener Benutzer

➤ *So ändern Sie einen vorhandenen Benutzer:*

1. Bearbeiten Sie auf der Seite **User** (Benutzer) die entsprechenden Felder. Informationen zum Zugriff auf die Seite **User** (Benutzer) finden Sie unter **Add New User (Neuen Benutzer hinzufügen)** (auf Seite 54).
2. 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. Weitere Informationen finden Sie unter **User Blocking (Benutzersperrung)** (auf Seite 166). 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** (Benutzerverwaltung > Benutzer).

Die Seite **User** (Benutzer) 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 zugreifen.
 - Ist das Kästchen deaktiviert, ist der Benutzer inaktiv und kann nicht auf KX II-101 zugreifen.
3. Klicken Sie auf **OK**.

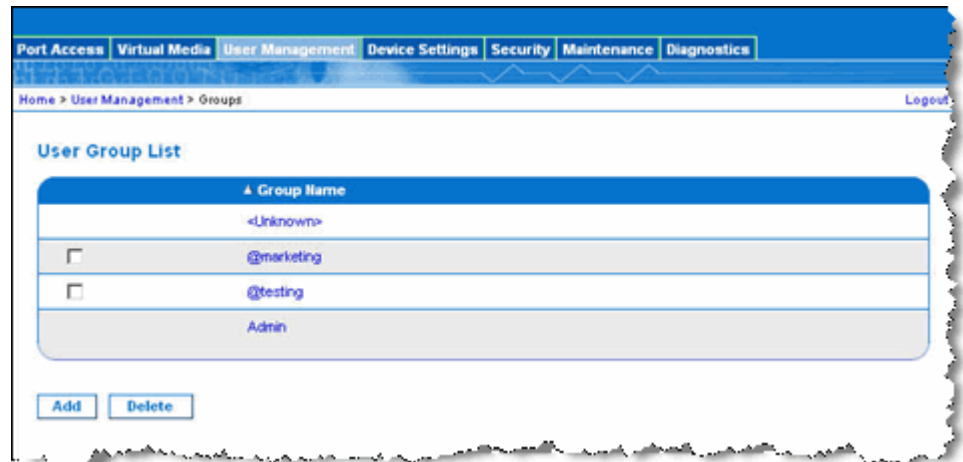
Der Status des Benutzers wird aktualisiert.

User Group List (Liste der Benutzergruppen)

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



- *So fügen Sie eine neue Benutzergruppe hinzu:*
 - Klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Die Seite **Group** (Gruppe) wird angezeigt. Umfassende Informationen zur Seite **Group** (Gruppe) finden Sie unter Add New User Group (Neue Benutzergruppe hinzufügen).
- *So ändern Sie eine vorhandene Benutzergruppe:*
 1. Wählen Sie die gewünschte Benutzergruppe aus der Liste aus.

Benutzerverwaltung

2. Klicken Sie auf den Gruppennamen. Die Seite **Group** (Gruppe) wird angezeigt. Umfassende Informationen zum Bearbeiten von Benutzergruppen finden Sie unter *Ändern vorhandener Benutzergruppen* (auf Seite 65).

➤ *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**.

Add New User Group (Neue Benutzergruppe hinzufügen)

➤ *So fügen Sie eine neue Benutzergruppe hinzu:*

1. Öffnen Sie die Seite **Group** (Gruppe) mit einem der folgenden Verfahren:
 - Wählen Sie **User Management > Add New User Group** (Benutzerverwaltung > Neue Benutzergruppe hinzufügen), oder

- klicken Sie auf der Seite **User Group List** (Liste der Benutzergruppen) auf die Schaltfläche **Add** (Hinzufügen).

The screenshot shows the 'Group' configuration page. It includes a breadcrumb trail 'Home > User Management > Group'. The main sections are:

- Group:** A blue header bar followed by a 'Group Name' input field.
- Permissions:** A blue header bar followed by a list of checkboxes: Device Settings, Diagnostics, Maintenance, PC-Share, Security, and User Management.
- Port Permissions:** A blue header bar followed by a table with columns: Port, Access, VM Access, and Power Control. The rows are 'Dominion_KX2_101_Port1' and 'Power Port 1', both with 'Deny' selected in the dropdown menus.
- IP ACL:** A blue header bar followed by a table with columns: Rule #, Starting IP, Ending IP, and Action. The Action dropdown is set to 'ACCEPT'. Below the table are buttons for 'Append', 'Insert', 'Replace', and 'Delete'.

At the bottom of the form are 'OK' and 'Cancel' buttons.

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

2. Geben Sie im Feld **Group Name** (Gruppenname) einen aussagekräftigen Namen für die neue Benutzergruppe ein.
3. Legen Sie unter **Permissions** (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Weitere Informationen finden Sie unter *Festlegen von Berechtigungen* (auf Seite 60).
4. Legen Sie unter **Port Permissions** (Port-Berechtigungen) die Port-Berechtigungen fest. Geben Sie die Zugriffsart für den KVM-Port und Stromzufuhr-Port an. Weitere Informationen finden Sie unter *Festlegen von Port-Berechtigungen*.

- Legen Sie die IP-ACL fest (optional). Mit diesem Feature können Sie durch die Angabe von IP-Adressen den Zugriff auf das KX II-101-Gerät einschränken. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur *IP-Zugriffssteuerung* (siehe "IP Access Control (IP-Zugriffssteuerung)" auf Seite 171), die für alle Zugriffsversuche auf das Gerät gilt (und Priorität hat).
- Klicken Sie auf **OK**.

*Hinweis: Im MPC stehen mehrere Verwaltungsfunktionen zur Verfügung. Diese Funktionen können nur von Mitgliedern der Standardgruppe **Admin** verwendet werden.*

Festlegen von Berechtigungen

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

Berechtigung	Beschreibung
Device Settings (Geräteeinstellungen)	Netzwerkeinstellungen, Einstellungen für Datum und Uhrzeit, Port-Konfiguration (Channel-Namen, Stromausgangszuordnungen), Ereignisverwaltung (SNMP, Syslog), Dateiserver-Setup für virtuelle Medien.
Diagnostics (Diagnose)	Status der Netzwerkschnittstelle, Netzwerkstatistik, Ping an den Host, Verfolgen der Route zum Host, KX II-101-Diagnose.
Maintenance (Wartung)	Sichern und Wiederherstellen von Datenbanken, Firmware-Aktualisierung, Wiederherstellen der Standardeinstellungen, Neustart.
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/RADIUS), Anmeldeeinstellungen.

Kapitel 5: Benutzer, Gruppen und Zugriffsberechtigungen

Festlegen von Berechtigungen für individuelle Gruppen

- *So legen Sie Berechtigungen für eine individuelle Benutzergruppe fest:*
1. Wählen Sie den gewünschten Benutzer aus der Liste der Gruppen aus. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen.
 2. Klicken Sie auf den Gruppennamen. Die Seite **Group** (Gruppe) wird angezeigt.
 3. Wählen Sie die gewünschten Berechtigungen aus.
 4. Klicken Sie auf **OK**.

Festlegen von Port-Berechtigungen

Sie können für den Server-Port die Zugriffsart, den Zugriff auf virtuelle Medien und die Stromzufuhrsteuerung festlegen. Beachten Sie, dass alle Berechtigungen standardmäßig deaktiviert sind.

Access (Zugriff)		VM Access (VM-Zugriff)		Power Control (Stromzufuhrsteuerung)	
Option	Beschreibung	Option	Beschreibung	Option	Beschreibung
None* (Kein)	Zugriff vollständig verweigert	Deny* (Ablehnen)	Berechtigung für virtuelle Medien wird für diesen Port vollständig verweigert	Deny* (Ablehnen)	Zugriff vollständig verweigert
View (Anzeigen)	Anzeigen des Videobildes, aber keine Interaktion mit dem angeschlossenen Zielservers	Deny* (Ablehnen)	Berechtigung für virtuelle Medien wird für diesen Port vollständig verweigert	Deny* (Ablehnen)	Zugriff vollständig verweigert

Benutzerverwaltung

Access (Zugriff)		VM Access (VM-Zugriff)		Power Control (Stromzufuhrsteuerung)	
Control (Steuern)	Steuerung des angeschlossenen Zielservers	Zugriff auf virtuelle Medien ist auf das Lesen beschränkt	Nur Lesezugriff. Vollständiger Zugriff (Lesen und Schreiben) auf virtuelle Medien	Access (Zugriff)	Vollständiger Zugriff
Control (Steuern)	Steuerung des angeschlossenen Zielservers	Read-Write (Lese-/Schreibzugriff)	Vollständiger Zugriff (Lesen und Schreiben) auf virtuelle Medien	Access (Zugriff) oder Deny (Ablehnen)	Vollständiger Zugriff oder vollständig verweigert

* Standardeinstellung

Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)

Wichtig: Gehen Sie bei der Verwendung der gruppenbasierten IP-Zugriffssteuerung vorsichtig vor. Der Zugriff auf KX II-101 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-Gerät durch Benutzer in der ausgewählten Gruppe auf bestimmte IP-Adressen. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für alle Zugriffsversuche auf das Gerät gilt, zuerst verarbeitet wird und Priorität hat. Weitere Informationen finden Sie unter *IP-Zugriffssteuerung* (siehe "IP Access Control (IP-Zugriffssteuerung)" auf Seite 171).

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

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

➤ *So fügen Sie eine Regel ein:*

1. Geben Sie im Feld **Rule #** 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 Dropdown-Liste **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 im Feld **Rule #** die Nummer der zu ersetzenden Regel ein.
2. Geben Sie Werte in die Felder **Starting IP** (IP-Startadresse) und **Ending IP** (IP-Endadresse) ein.
3. Wählen Sie in der Dropdown-Liste **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 im Feld **Rule #** die Nummer der zu löschenden Regel ein.
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 hier aufgeführt sind. Werden die beiden ACL-Regeln in diesem Beispiel vertauscht, akzeptiert Dominion z. B. gar keine Kommunikation.

IP ACL			
Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▾
<input type="button" value="Append"/> <input type="button" value="Insert"/> <input type="button" value="Replace"/> <input type="button" value="Delete"/>			

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

Ändern vorhandener Benutzergruppen

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

- So ändern Sie eine vorhandene Benutzergruppe:
 1. Bearbeiten Sie auf der Seite **Group** (Gruppe) die entsprechenden Felder, und legen Sie die gewünschten Berechtigungen fest.

The screenshot shows the 'Group' configuration page. At the top, there is a breadcrumb 'Home > User Management > Group'. Below this is a blue header 'Group'. A text input field for 'Group Name' is present. A section titled 'Permissions' contains a list of checkboxes for 'Device Settings', 'Diagnostics', 'Maintenance', 'PC-Share', 'Security', and 'User Management'. Below that is a 'Port Permissions' section with a table:

Port	Access	VM Access	Power Control
Dominion_KX2_101_Port1	Deny	Deny	Deny
Power Port 1	Deny		Deny

Below the table is an 'IP ACL' section with a table for defining rules:

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Buttons for 'Append', 'Insert', 'Replace', and 'Delete' are located below the IP ACL table. At the bottom of the form are 'OK' and 'Cancel' buttons.

2. Legen Sie unter **Permissions** (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Weitere Informationen finden Sie unter *Festlegen von Berechtigungen* (auf Seite 60).
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. Weitere Informationen finden Sie unter *Festlegen von Port-Berechtigungen*.

Benutzerverwaltung

- Legen Sie die IP-ACL fest (optional). Mit diesem Feature beschränken Sie den Zugriff auf das KX II-101-Gerät, indem Sie IP-Adressen angeben. Weitere Informationen finden Sie unter Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste).
- Klicken Sie auf **OK**.

Ändern des Kennworts

➤ *So ändern Sie Ihr Kennwort:*

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



- Geben Sie im Feld **Old Password** (Altes Kennwort) Ihr aktuelles Kennwort ein.
- Geben Sie im Feld **New Password** (Neues Kennwort) das neue Kennwort ein, und geben Sie es im Feld **Confirm New Password** (Neues Kennwort bestätigen) erneut ein. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen.
- Klicken Sie auf **OK**.
- 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 **Sicherheitseinstellungen - Sichere Kennwörter** (siehe "Strong Passwords (Sichere Kennwörter)" auf Seite 165).*

Authentifizierungseinstellungen

Authentifizierungseinstellungen werden später in diesem Kapitel im Rahmen der Remote-Authentifizierung beschrieben. Weitere Informationen finden Sie unter Authentication Settings (Authentifizierungseinstellungen).

Remote-Authentifizierung

Hinweis für CC-SG-Benutzer

Wenn KX II-101 von CommandCenter Secure Gateway gesteuert wird, authentifiziert CC-SG Benutzer und Gruppen, mit Ausnahme von lokalen Benutzern (für die der Zugriff auf den lokalen Port erforderlich ist). Steuert CC-SG die KX II-101-Einheit, erfolgt die Authentifizierung von Benutzern des lokalen Ports über die lokale Benutzerdatenbank oder den für KX II-101 konfigurierten Remote-Authentifizierungsserver (LDAP/LDAPS oder RADIUS). Sie werden nicht über die CC-SG-Benutzerdatenbank authentifiziert.

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

Unterstützte Protokolle

Zur Vereinfachung der Verwaltung von Benutzernamen und Kennwörtern bietet KX II-101 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 das LDAP/LDAPS-Protokoll und kann als LDAP/LDAPS-Server und Authentifizierungsquelle für KX II-101 fungieren. Bei Verwendung der IAS-Komponente (Internetautorisierungsserver) kann ein Microsoft Active Directory-Server auch als RADIUS-Authentifizierungsquelle dienen.

Authentifizierung im Vergleich zur Autorisierung

Bei der Authentifizierung geht es darum, die Identität des Benutzers zu überprüfen. Nach der Authentifizierung dient die Benutzergruppe dazu, die jeweiligen System- und 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 zur Remote-Authentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

Authentication Settings (Authentifizierungseinstellungen)

Auf der Seite **Authentication Settings** (Authentifizierungseinstellungen) können Sie die Art der Authentifizierung für den Zugriff auf KX II-101 konfigurieren. Weitere Informationen zur Funktionsweise und zu den Unterschieden von Authentifizierung und Autorisierung finden Sie unter *Authentifizierung im Vergleich zur Autorisierung* (auf Seite 68).

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

➤ *So konfigurieren Sie die Authentifizierung:*

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

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
 LDAP

Primary LDAP Server
Secondary LDAP Server

Secret Phrase
Confirm Secret Phrase

Enable Secure LDAP

Port
Secure LDAP Port
Certificate File
DN of Administrative User
User Search DN

Type of External LDAP Server
Generic LDAP server
Active Directory Domain

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
LDAP

OK Reset To Defaults Cancel

Remote-Authentifizierung

2. Wählen Sie die Option für das gewünschte Authentifizierungsprotokoll aus. Zur Verfügung stehen **Local Authentication** (Lokale Authentifizierung), **LDAP** 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** entscheiden, lesen Sie den Abschnitt Implementierung der LDAP-Remote-Authentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Bereich **LDAP** der Seite **Authentication Settings** (Authentifizierungseinstellungen).
5. Wenn Sie sich für **RADIUS** entscheiden, lesen Sie den Abschnitt *Implementierung der RADIUS-Remote-Authentifizierung* (auf Seite 76). Dort finden Sie Informationen zum Ausfüllen der Felder im Bereich **RADIUS** der Seite **Authentication Settings** (Authentifizierungseinstellungen).
6. Klicken Sie zum Speichern auf **OK**.
 - *So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).
 - *So stellen Sie die werksseitigen Standardeinstellungen wieder her:*
 - Klicken Sie auf die Schaltfläche **Reset to Defaults** (Standardeinstellungen wiederherstellen).

Implementierung der LDAP-Remote-Authentifizierung

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

Erinnerung: Microsoft Active Directory fungiert als LDAP-Authentifizierungsserver.

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

The screenshot shows a 'Authentication Settings' dialog box. The 'Local Authentication' radio button is selected. Below it are fields for 'Primary LDAP Server', 'Secondary LDAP Server', 'Secret Phrase', and 'Confirm Secret Phrase'. There is a checkbox for 'Enable Secure LDAP'. Below that are 'Port' and 'Secure LDAP Port' fields, and a 'Certificate File' field with a browse button. Further down are 'URI of Administrative User' and 'User Search URI' fields. The 'Type of External LDAP Server' is set to 'Active Directory Domain'. Below this is the 'Active Directory Domain' field. The 'RADIUS' radio button is unselected. Below it are fields for 'Primary RADIUS Server', 'Shared Secret', 'Authentication Port', 'Accounting Port', 'Timeout (in seconds)', and 'Retries'. There is also a 'Secondary RADIUS Server' section with similar fields. At the bottom, the 'Global Authentication Type' is set to 'LDAP'. Buttons for 'OK', 'Reset To Defaults', and 'Cancel' are at the bottom.

Remote-Authentifizierung

1. Geben Sie die IP-Adresse oder den DNS-Namen Ihres LDAP-Remote-Authentifizierungsservers im Feld **Primary LDAP Server** (Primärer LDAP-Server) ein. Wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist, muss der DNS-Name verwendet werden.
2. (Optional) Geben Sie die IP-Adresse oder den DNS-Namen Ihres LDAP-Servers zur Sicherung im Feld **Secondary LDAP Server** (Sekundärer LDAP-Server) ein. Wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist, muss der DNS-Name verwendet werden. Für die restlichen Felder gelten die gleichen Einstellungen wie unter **Primary LDAP Server** (Primärer LDAP-Server).
3. Geben Sie den geheimen Serverschlüssel (Kennwort), der für die Authentifizierung beim Remote-Authentifizierungsserver erforderlich ist, im Feld **Secret Phrase** (Geheimer Schlüssel) und ein zweites Mal im Feld **Confirm Secret Phrase** (Geheimen Schlüssel bestätigen) ein. Verändern Sie das vorhandene Schema nicht. Verwenden Sie den String, der auch für den LDAP-Server verwendet wird.
4. Aktivieren Sie das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren), wenn Sie SSL verwenden möchten. Das Feld **Secure LDAP Port** (Secure LDAP-Port) wird aktiviert. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, über das KX II-101 sicher mit dem LDAP-Server kommunizieren kann.
5. Der Standard-Port lautet 389. Verwenden Sie entweder den Standard-TCP-Port für LDAP, oder legen Sie einen anderen Port fest.
6. Der standardmäßige Secure LDAP-Port ist Port 636. Verwenden Sie entweder den Standard-Port, oder legen Sie einen anderen Port fest. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist.
7. **Certificate File** (Zertifikatdatei): Fragen Sie den Administrator des Authentifizierungsservers nach der CA-Zertifikatdatei im Base64-codierten X-509-Format für den LDAP-Server. Navigieren Sie über die Schaltfläche **Browse** (Durchsuchen) zur entsprechenden Zertifikatdatei. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen **Enable Secure LDAP** (Secure LDAP aktivieren) aktiviert ist.

8. **DN of administrative User** (DN des Administratorbenutzers): Distinguished Name (DN) des Administratorbenutzers. Fragen Sie den Administrator des Authentifizierungsservers nach den Werten, die in dieses Feld eingegeben werden müssen. Ein Wert für **DN of administrative User** könnte wie folgt aussehen:
„cn=Administrator,dc=Benutzer=,dc=testradius,dc=com“.
9. **User Search DN** (DN für Benutzersuche): Bezeichnung des mit LDAP verbundenen Namens und des Anfangspunkts der Suche nach dem angegebenen Basis-DN in der Datenbank. Ein Beispiel für einen Basissuchwert ist: „cn=Benutzer,dc=raritan,dc=com“. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für diese Felder.
10. **Type of external LDAP server** (Typ des externen LDAP-Servers): Wählen Sie eine der folgenden Optionen:
 - **Generic LDAP Server** (Generischer LDAP-Server)
 - **Microsoft Active Directory**: Microsoft hat die LDAP-Verzeichnisdienste in Active Directory für die Verwendung in Windows-Umgebungen implementiert.
11. **Active Directory Domain** (Active Directory-Domäne): Geben Sie den Namen der Active Directory-Domäne ein.

Rückgabe von Benutzergruppeninformationen vom Active Directory-Server

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

*Hinweis: Wenn Sie bereits Kunde von Raritan, Inc. sind und den Active Directory-Server bereits durch Ändern des Active Directory-Schemas konfiguriert haben, unterstützt KX II-101 diese Konfiguration nach wie vor, und Sie müssen den folgenden Vorgang nicht durchführen. Informationen zur Aktualisierung des Active Directory-LDAP-Schemas finden Sie unter **Aktualisieren des LDAP-Schemas** (auf Seite 79).*

- *So aktivieren Sie den AD-Server auf der KX II-101-Einheit:*
1. Erstellen Sie auf der KX II-101-Einheit besondere Gruppen, und weisen Sie ihnen geeignete Berechtigungen zu. Erstellen Sie z. B. Gruppen wie: KVM_Admin, KVM_Operator.
 2. Erstellen Sie auf dem Active Directory-Server neue Gruppen mit denselben Gruppennamen wie die im vorherigen Schritt erstellten Gruppen.
 3. Weisen Sie die KX II-101-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-Einheit. Weitere Informationen finden Sie unter Implementierung der LDAP-Remote-Authentifizierung.

Wichtige Hinweise:

Kapitel 5: Benutzer, Gruppen und Zugriffsberechtigungen

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

Remote-Authentifizierung

Implementierung der RADIUS-Remote-Authentifizierung

Remote Authentication Dial-in User Service (RADIUS) ist ein AAA-Protokoll (Authentifizierung, Autorisierung und Accounting) für Netzwerkzugriffsanwendungen.

- *So verwenden Sie das RADIUS-Authentifizierungsprotokoll:*

The image shows a configuration window titled "RADIUS". It contains two main sections for "Primary Radius Server" and "Secondary Radius Server". Each section has a "Shared Secret" field, an "Authentication Port" field (set to 1812), and an "Accounting Port" field (set to 1813). Below these are "Timeout (in seconds)" (set to 1) and "Retries" (set to 3) fields. At the bottom, there is a "Global Authentication Type" dropdown menu currently set to "PAP".

1. Geben Sie die IP-Adresse des primären und (optional) des sekundären Remote-Authentifizierungsservers in die Felder **Primary Radius Server** (Primärer RADIUS-Server) und **Secondary Radius Server** (Sekundärer RADIUS-Server) ein.

2. Geben Sie den geheimen Serverschlüssel für die Authentifizierung in die Felder unter **Shared Secret** (Gemeinsamer geheimer Schlüssel) ein. Der gemeinsame geheime Schlüssel ist eine Zeichenfolge, die KX II-101 und dem RADIUS-Server bekannt sein muss, damit diese sicher kommunizieren können. Es handelt sich dabei praktisch um ein Kennwort.
3. **Authentication Port** (Authentifizierungs-Port): Der Standardauthentifizierungs-Port lautet 1812. Sie können ihn bei Bedarf ändern.
4. **Accounting Port** (Account-Port): Der standardmäßige Accounting-Port lautet 1813. Sie können ihn bei Bedarf ändern.
5. **Timeout (in seconds)** (Zeitlimit [in Sekunden]): Das Standardzeitlimit beträgt eine Sekunde. Sie können es bei Bedarf ändern. Das Zeitlimit bezeichnet die Zeitspanne, während der KX II-101 auf eine Antwort vom RADIUS-Server wartet, ehe eine weitere Authentifizierungsanforderung gesendet wird.
6. **Retries** (Neuversuche): Standardmäßig beträgt die Anzahl der Neuversuche 3. Sie können sie bei Bedarf ändern. Dieser Wert gibt an, wie oft KX II-101 eine Authentifizierungsanforderung an den RADIUS-Server sendet.
7. **Global Authentication Type** (Globaler Authentifizierungstyp): Wählen Sie eine Option aus der Dropdown-Liste:
 - **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.

Remote-Authentifizierung

Zurückgeben von Benutzergruppeninformationen über RADIUS

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

Ihr Remote-RADIUS-Server kann diese Benutzergruppennamen bereitstellen, indem er ein als RADIUS FILTER-ID implementiertes Attribut zurückgibt. Die FILTER-ID sollte folgendermaßen formatiert sein:

Raritan:G{GRUPPENNAME}

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

Spezifikationen für den RADIUS-Kommunikationsaustausch

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

Attribut	Daten
Anmeldung	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-IP-Address (4)	Die IP-Adresse der KX II-101-Einheit.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Accounting.
User-Password(2):	Das verschlüsselte Kennwort.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Accounting 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 der KX II-101-Einheit.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.

Attribut	Daten
Anmeldung	
Acct-Session-ID (44)	Sitzungs-ID für Accounting.
Abmeldung	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Accounting wird beendet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse der KX II-101-Einheit.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Accounting.

Aktualisieren des LDAP-Schemas

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

Zurückgeben von Benutzergruppeninformationen

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

Von LDAP

Wenn eine LDAP/LDAPS-Authentifizierung erfolgreich ist, bestimmt KX II-101 die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers. Ihr Remote-LDAP-Server kann diese Benutzergruppennamen bereitstellen, indem er ein wie folgt benanntes Attribut zurückgibt:

rciusergroup attribute type: Zeichenfolge

Dies erfordert ggf. eine Schemaerweiterung auf Ihrem LDAP/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. Nähere Informationen hierzu entnehmen Sie der Microsoft-Dokumentation.

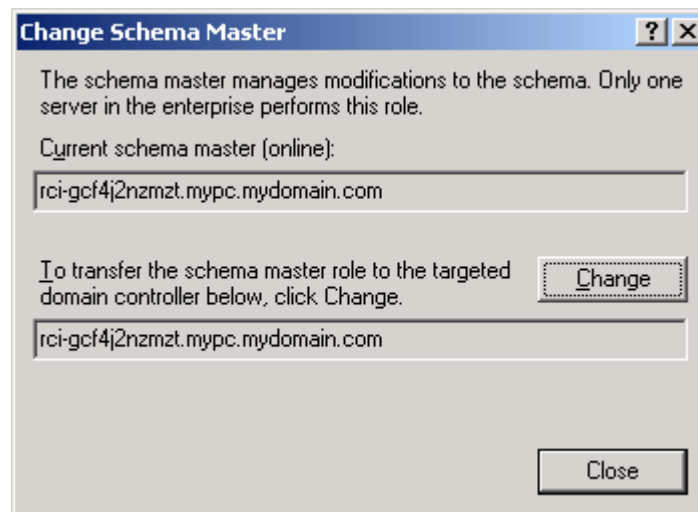
1. Installieren Sie das Schema-Plug-in für Active Directory – Anweisungen hierzu finden Sie in der Microsoft Active Directory-Dokumentation.
2. Starten Sie Active Directory Console, und wählen Sie **Active Directory Schema** (Verzeichnisschema).

Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen

Um einem Domänencontroller das Schreiben im Schema zu erlauben, müssen Sie einen Registrierungseintrag erstellen, der Schemaaktualisierungen zulässt.

➤ *So lassen Sie Schreibvorgänge im Schema zu:*

1. Klicken Sie mit der rechten Maustaste auf den Stammknoten **Active Directory Schema** (Verzeichnisschema) im linken Fensterbereich, und wählen Sie **Operations Master** (Betriebsmaster) aus dem Kontextmenü. Das Dialogfeld **Change Schema Master** (Schemamaster ändern) wird angezeigt.



- (Optional) Aktivieren Sie das Kontrollkästchen **The Schema can be modified on this Domain Controller** (Schema kann auf diesem Domänencontroller geändert werden).
- Klicken Sie auf **OK**.

Erstellen eines neuen Attributs

➤ *So erstellen Sie neue Attribute für die Klasse „rciusergroup“:*

- Klicken Sie im linken Fensterbereich auf das +-Symbol vor **Active Directory Schema** (Active Directory-Schema).
- Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf **Attributes** (Attribute).
- Klicken Sie auf **New** (Neu), und wählen Sie **Attributes** (Attribute) aus. Klicken Sie im angezeigten Hinweisenfenster auf **Continue** (Weiter). Das Dialogfeld **Create New Attribute** (Neues Attribut erstellen) wird geöffnet.

The screenshot shows the 'Create New Attribute' dialog box. It is titled 'Create New Attribute' and contains the following fields:

- 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

At the bottom, there is an unchecked checkbox for 'Multi-Valued' and 'OK' and 'Cancel' buttons.

- Geben Sie im Feld **Common Name** (Allgemeiner Name) den Wert *rciusergroup* ein.

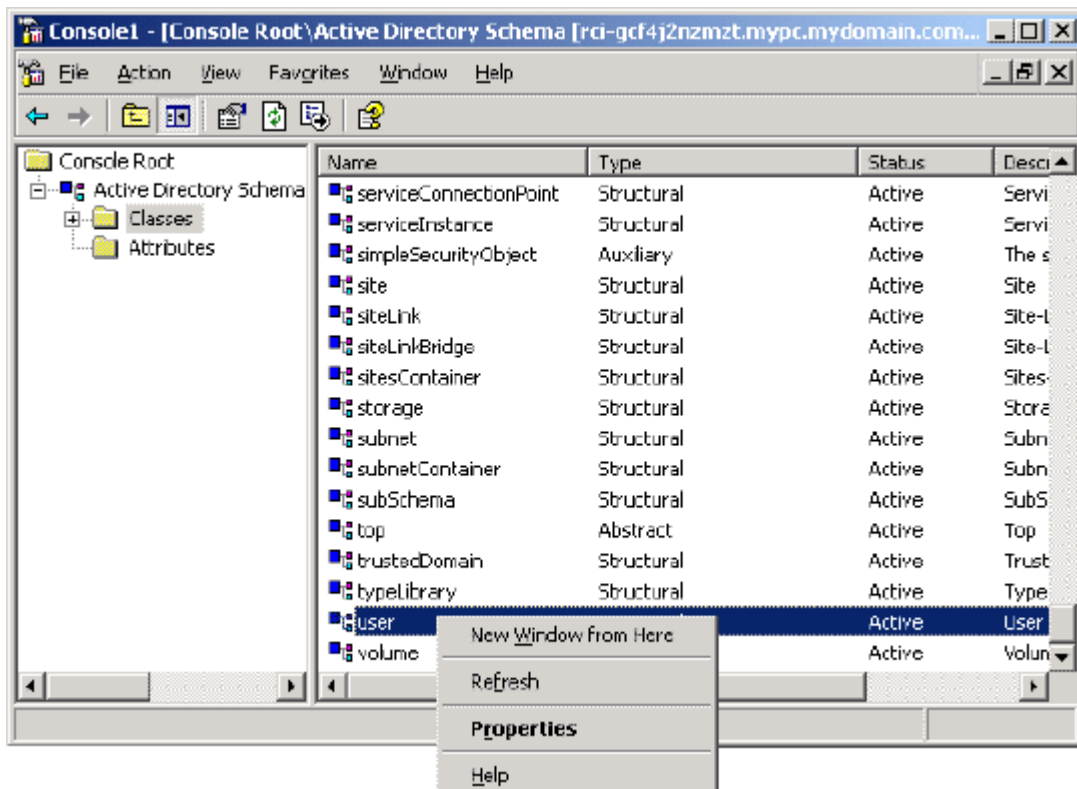
Remote-Authentifizierung

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 Dropdown-Liste **Syntax**, und wählen Sie **Case Insensitive String** (Groß-/Kleinschreibung nicht beachten).
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**.

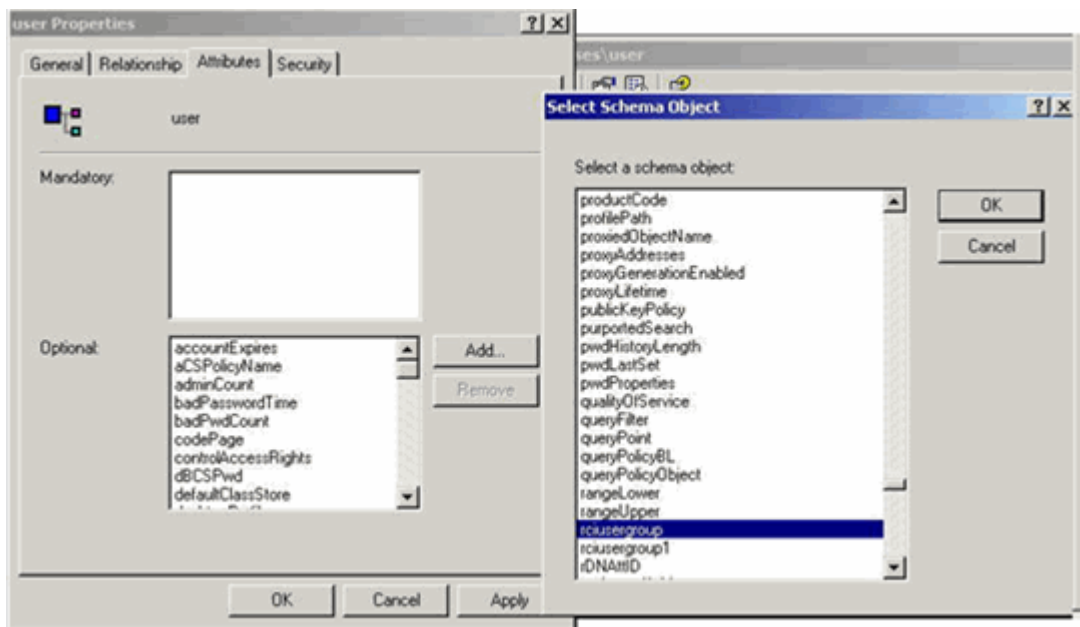
Hinzufügen von Attributen zur Klasse

➤ *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** (Benutzer), und klicken Sie mit der rechten Maustaste darauf.



3. Wählen Sie **Properties** (Eigenschaften) aus dem Kontextmenü. Das Fenster **User Properties** (Benutzereigenschaften) wird geöffnet.
4. Klicken Sie auf die Registerkarte **Attributes** (Attribute), um sie zu öffnen.



5. Klicken Sie auf **Add** (Hinzufügen).
6. Wählen Sie in der Liste **Select Schema Object** (Schemaobjekt auswählen) den Eintrag **rcusergroup** aus.
7. Klicken Sie im Dialogfeld **Select Schema Object** (Schemaobjekt auswählen) auf **OK**.
8. Klicken Sie im Dialogfeld **User Properties** (Benutzereigenschaften) auf **OK**.

Aktualisieren des Schemacache

➤ *So aktualisieren Sie den Schemacache:*

1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf **Active Directory Schema** (Active Directory-Schema), und wählen Sie **Reload the Schema** (Schema neu laden) aus dem Kontextmenü.
2. Minimieren Sie die Active Directory-Schema-MMC-Konsole (Microsoft Management Console).

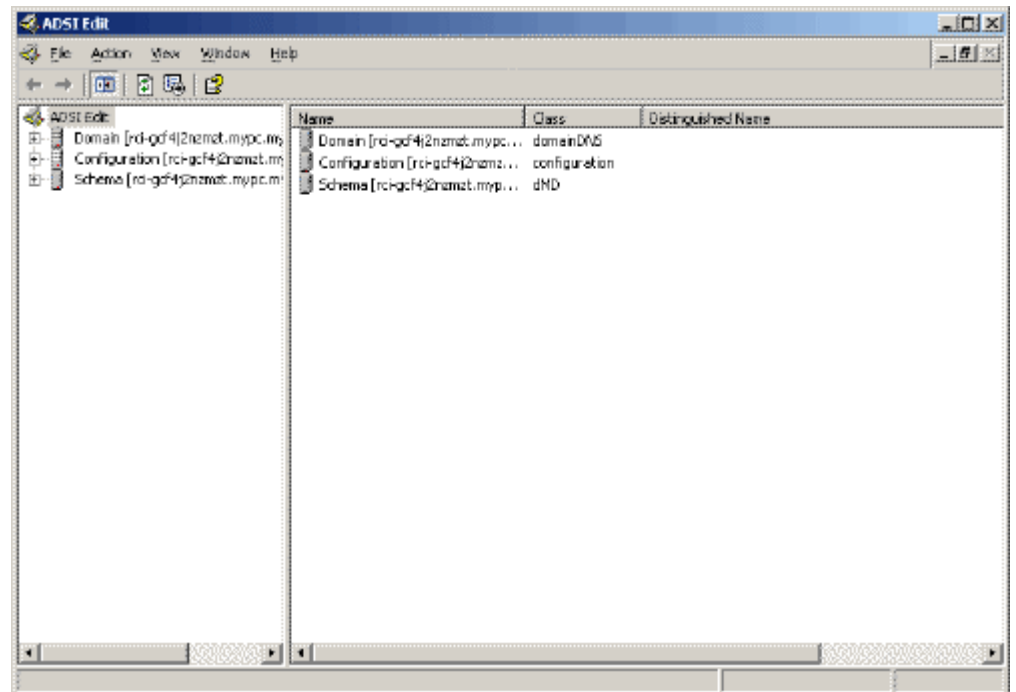
Remote-Authentifizierung

Bearbeiten von rcusergroup-Attributen für Benutzermitglieder

Verwenden Sie zum Ausführen des Active Directory-Skripts auf einem Server unter Windows 2003 das von Microsoft bereitgestellte Skript (verfügbar auf der Windows 2003 Server-Installations-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.

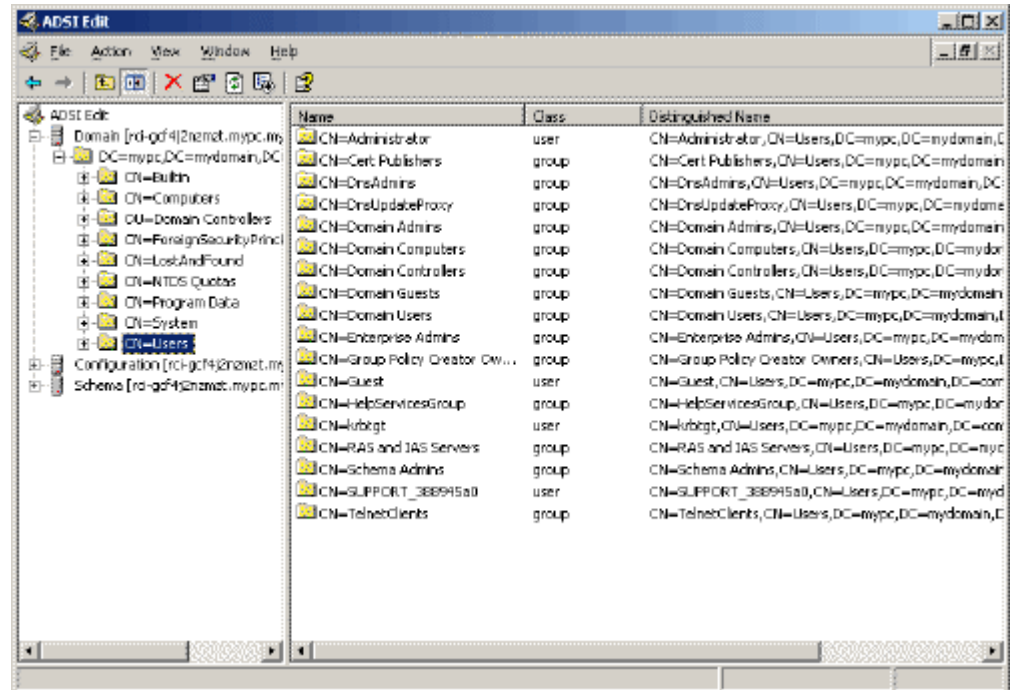
➤ *So bearbeiten Sie die einzelnen Benutzerattribute innerhalb der Gruppe „rcusergroup“:*

1. Wählen Sie auf der Installations-CD **Support > Tools**.
2. Doppelklicken Sie zur Installation der Support-Tools auf **SUPTOOLS.MSI**.
3. Wechseln Sie zum Installationsverzeichnis der Support-Tools.
4. Führen Sie **adsiedit.msc** aus. Das Fenster **ADSI Edit** (ADSI-Bearbeitung) wird angezeigt.



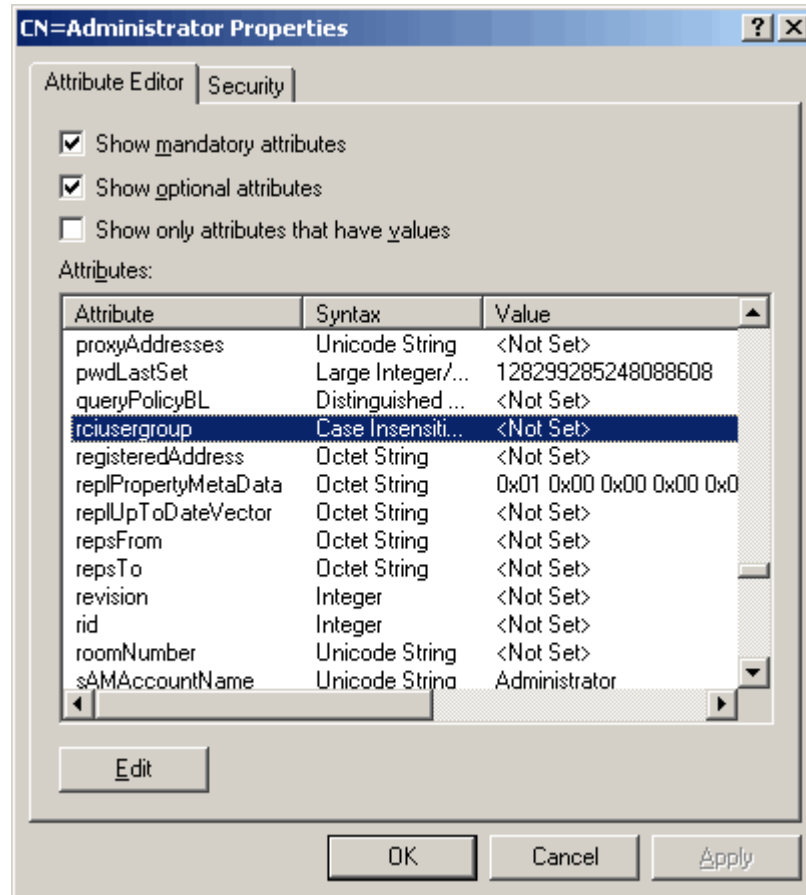
5. Öffnen Sie die Domäne.

6. Klicken Sie im linken Fensterbereich auf den Ordner **CN=User** (CN=Benutzer).

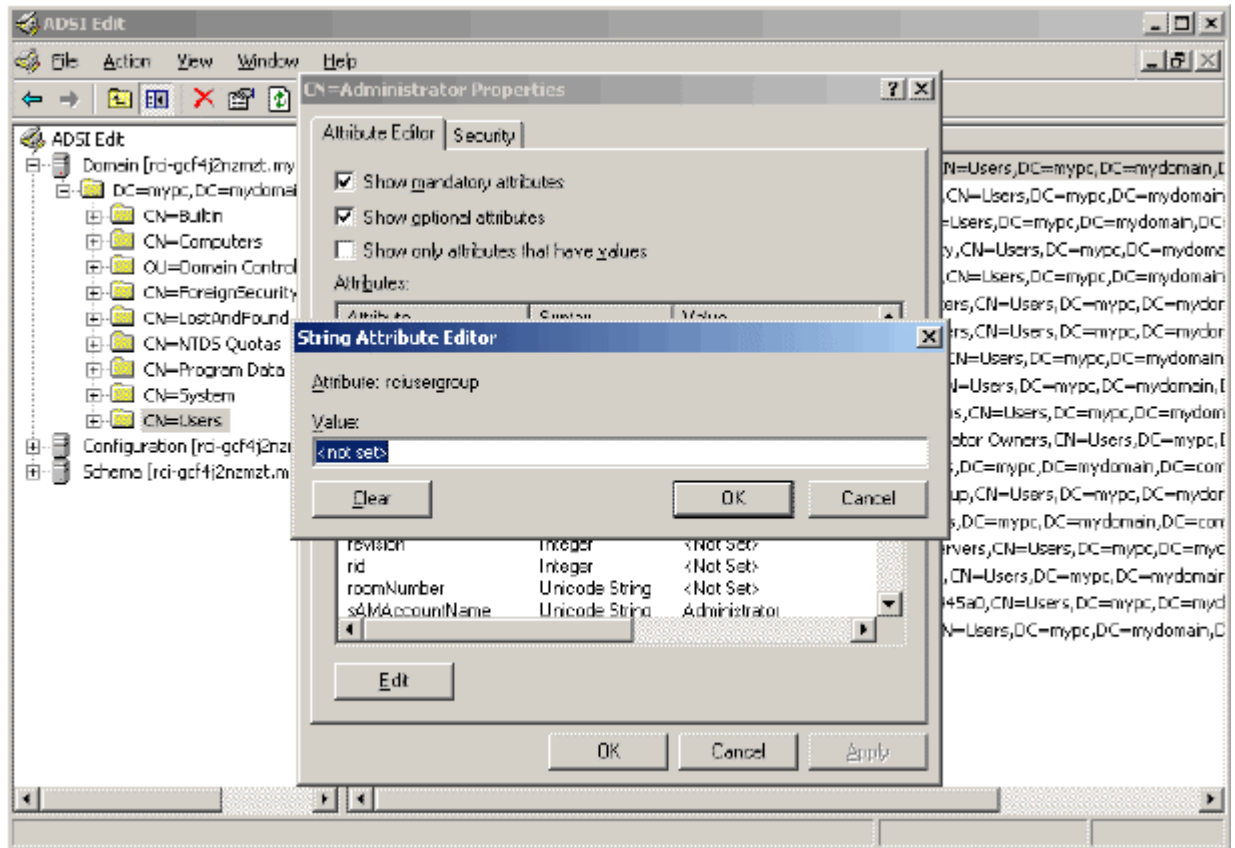


7. Navigieren Sie im rechten Fensterbereich zu dem Namen des Benutzers, dessen Eigenschaften geändert werden sollen. Klicken Sie mit der rechten Maustaste auf den Benutzernamen, und wählen Sie **Properties** (Eigenschaften) aus dem Kontextmenü.
8. Klicken Sie auf die Registerkarte **Attribute Editor** (Attributeditor), um sie, falls nötig, zu öffnen.

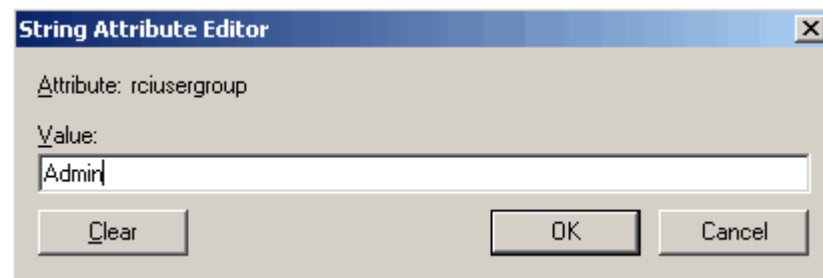
9. Wählen Sie **rciusergroup** in der Liste **Attributes** (Attribute) aus.



10. Klicken Sie auf **Edit** (Bearbeiten). Das Dialogfeld **String Attribute Editor** (Attributeditor für Zeichenfolgen) wird angezeigt.



11. Geben Sie die Benutzergruppe (erstellt in Dominion KX II-101) in das Feld **Edit Attribute** (Attribut bearbeiten) ein.



12. Klicken Sie auf **OK**.

Kapitel 6 Virtual KVM Client

In diesem Kapitel

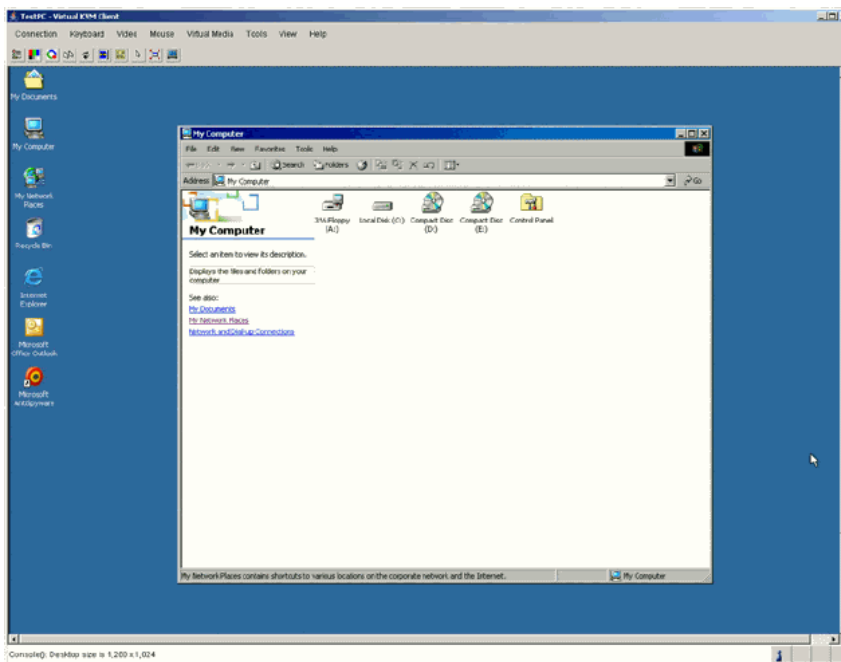
Überblick.....	89
Optionen	90
Mauszeigersynchronisation	92
Menü „ Connection “ (Verbindung).....	94
Menü „ Keyboard “ (Tastatur).....	97
Menü „ Video “	102
Menü „ Mouse “ (Maus).....	107
Virtuelle Medien	111
Menü „ Tools “ (Extras)	112
Menü „ View “ (Ansicht)	113
Menü „ Help “ (Hilfe).....	114

Überblick

Wenn Sie über die KX II-101-Remote-Konsole auf einen Zielsever zugreifen, wird ein Fenster für den Virtual KVM Client geöffnet.

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.



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

Feature	Beschreibung
Menüleiste	Dropdown-Menüs mit Befehlen und Einstellungen
Symbolleiste	Schaltflächen zum Ausführen häufig verwendeter Features und Befehle
Zielsever-Videofenster	Anzeige des Zielgeräts

Optionen

Feature	Beschreibung
Statusleiste	Echtzeitinformationen zu Verbindungsparametern, der Fenstergröße des Zielservers, gleichzeitigen Verbindungen, Feststellanzeige und Num-Feststellanzeige

Optionen











Menüstruktur

Die folgende Liste enthält alle im Virtual KVM Client verfügbaren Menüs und Menüoptionen.

- Menü **Connection** (Verbindung):
 - Properties (Eigenschaften)
 - Connection Info (Verbindungsinformationen)
 - Exit (Beenden)
- Menü **Keyboard** (Tastatur):
 - Send Ctrl + Alt + Delete (STRG+ALT+ENTF senden)
 - Keyboard Macros (Tastaturmakros)
 - Keyboard Mouse Options (Tastatur-/Mausoptionen)
 - User-Created Macros (Benutzerdefinierte Makros); optional
- Menü **Video**:
 - Refresh Screen (Anzeige aktualisieren)
 - Auto-Sense Video Settings (Videoeinstellungen automatisch erkennen)
 - Calibrate Color (Farbe kalibrieren)
 - Video Settings (Videoeinstellungen)
- Menü **Mouse** (Maus):
 - Synchronize Mouse (Maus synchronisieren)
 - Single Mouse Cursor (Ein Cursor)
 - Absolute (Absolut)
 - Intelligent

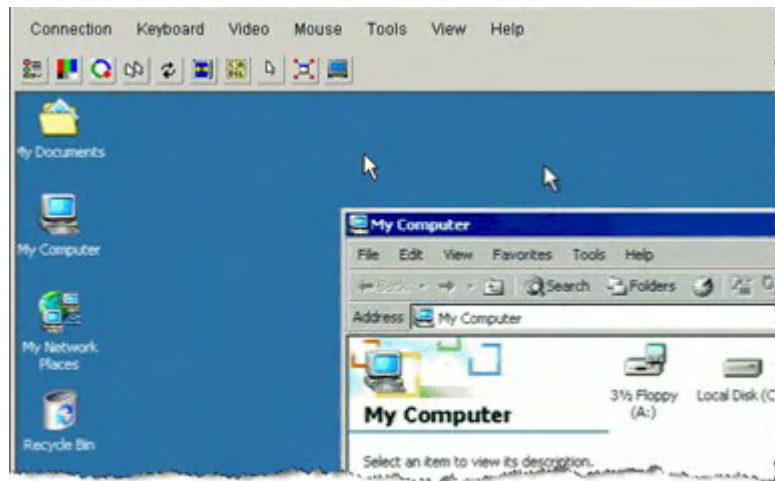
- Standard
- Menü **Virtual Media** (Virtuelle Medien):
 - Connect Drive (Laufwerk verbinden)
 - Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)
- Menü **Tools** (Extras):
 - Options (Optionen)
- Menü **View** (Ansicht):
 - View Toolbar (Symbolleiste anzeigen)
 - Scaling (Skalieren)
 - Target Screen Resolution (Zielbildschirmauflösung)
- Menü **Help** (Hilfe):
 - About Raritan Virtual KVM Client (Informationen zum Raritan Virtual KVM Client)

Symbolleiste

Schaltfläche	Beschreibung
	Properties (Eigenschaften)
	Video Settings (Videoeinstellungen)
	Calibrate Color (Farbe kalibrieren)
	Synchronize Mouse (Maus synchronisieren)
	Refresh Screen (Anzeige aktualisieren)
	Auto-sense video (Video automatisch erkennen)
	Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)
	Single Mouse Cursor (Ein Cursor)
	Full Screen (Vollbild)
	Resize video to fit screen (Videobild an die Bildschirmgröße anpassen)

Mauszeigersynchronisation

Bei der Remoteanzeige eines Zielservers mit einer Maus sehen Sie zwei Mauszeiger: 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 Zielgerätmauszeigers.




Bei schnellen LAN-Verbindungen sollten Sie den Mauszeiger des Virtual KVM Client deaktivieren, um nur den Cursor des Zielservers anzuzeigen. Sie können zwischen den beiden Modi (ein Cursor und zwei Cursor) wechseln. Weitere Informationen zu den verfügbaren Mausmodi finden Sie unter *Menü „ Mouse “ (Maus)* (auf Seite 107).

Tipps zur Maussynchronisation

Führen Sie bei der Maussynchronisation folgende Schritte aus:

1. Stellen Sie sicher, dass die ausgewählte Videoauflösung und Aktualisierungsfrequenz vom KX II-101-Gerät unterstützt wird. Im Dialogfeld **Virtual KVM Client Connection Info** (Virtual KVM Client - Verbindungsinformationen) werden die tatsächlich von KX II-101 erkannten Werte angezeigt.
2. Stellen Sie sicher, dass die Kabellänge die Grenzwerte für die ausgewählte Videoauflösung nicht überschreitet.

3. Stellen Sie sicher, dass Maus und Monitor während der Installation richtig konfiguriert wurden. Weitere Informationen finden Sie unter Installation und Konfiguration.
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 den Befehl `xset mouse 1 1` ein.
 - c. Schließen Sie das Terminalfenster.
6. Klicken Sie im Virtual KVM Client auf die Schaltfläche  zur Maussynchronisation.

Weitere Hinweise zum intelligenten Mausmodus

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

Menü „ Connection “ (Verbindung)

Dialogfeld „ Properties “ (Eigenschaften)

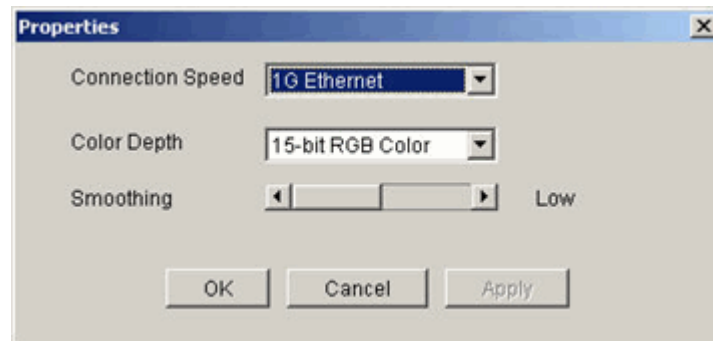
Die dynamischen Videokomprimierungsalgorithmen von KX II-101 gewährleisten die Verwendbarkeit der KVM-Konsole unter variierenden Bandbreitenbeschränkungen. KX II-101-Einheiten optimieren die KVM-Ausgabe nicht nur für LANs, sondern auch für WAN-Verbindungen. Diese Einheiten können zudem die Farbtiefe steuern und die Videoausgabe beschränken, um für jede Bandbreite ein optimales Gleichgewicht zwischen Videoqualität und Systemreaktion bereitzustellen.

	Properties (Eigenschaft en)	Manuelles Anpassen der Bandbreitenoptionen (Verbindungsgeschwindigkeit, Farbtiefe usw.)
---	-----------------------------------	--

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

➤ *So legen Sie die Verbindungseigenschaften fest:*

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



2. Wählen Sie in der Dropdown-Liste **Connection Speed** (Verbindungsgeschwindigkeit) die gewünschte Verbindungsgeschwindigkeit aus. KX II-101 kann die verfügbare Bandbreite automatisch erkennen und die Bandbreitenverwendung nicht beschränken. Sie können die Verwendung jedoch auch an die Bandbreitenbeschränkungen anpassen.

Automatisch

1G Ethernet

100 MB Ethernet

- 10 MB Ethernet
- 1,5 MB (MAX DSL/T1)
- 1 MB (Schnelles DSL/T1)
- 512 KB (Mittleres DSL/T1)
- 384 KB (Langsames DSL/T1)
- 256 KB (Kabel)
- 128 KB (Dual-ISDN)

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

3. Wählen Sie in der Dropdown-Liste **Color Depth** (Farbtiefe) die gewünschte Farbtiefe aus. KX II-101 kann die an Remote-Benutzer übertragene Farbtiefe dynamisch anpassen, um die Verwendbarkeit in allen Bandbreiten zu maximieren.

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

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

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

Menü „Connection“ (Verbindung)

5. Klicken Sie auf **OK**, um die Eigenschaften festzulegen.
- *So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).

Connection Info (Verbindungsinformationen)

- *So erhalten Sie Informationen über die Verbindung des Virtual KVM Client:*
- Wählen Sie **Connection > Connection Info** (Verbindung > Verbindungsinformationen). Das Fenster **Connection Info** (Verbindungsinformationen) wird angezeigt.

Zur aktuellen Verbindung werden folgende Informationen angezeigt:

- **Device Name** (Gerätename): Name des KX II-101-Geräts.
 - **IP Address** (IP-Adresse): IP-Adresse des KX II-101-Geräts.
 - **Port**: 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): Dauer der Verbindung.
 - **FPS**: Frames pro Sekunde der übertragenen Videobilder.
 - **Horizontal Resolution** (Horizontale Auflösung): Horizontale Bildschirmauflösung.
 - **Vertical Resolution** (Vertikale Auflösung): Vertikale Bildschirmauflösung.
 - **Refresh Rate** (Aktualisierungsfrequenz): Gibt an, wie häufig die Anzeige aktualisiert wird.
 - **Protocol Version** (Protokollversion): Version des RFB-Protokolls.
- *So kopieren Sie diese Informationen:*
 - Klicken Sie auf **Copy to Clipboard** (In Zwischenablage kopieren). Anschließend können die Informationen in ein Programm Ihrer Wahl eingefügt werden.

Exit (Beenden)


- *So schließen Sie den Virtual KVM Client (das Zielgerät, auf das derzeit zugegriffen wird):*
 - Wählen Sie **Connection > Exit** (Verbindung > Beenden).

Menü „ Keyboard “ (Tastatur)

Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)

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

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

	Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)	Sendet die Tastenkombination Strg+Alt+Entf an den Zielserversender.
---	--	---

- *So senden Sie die Tastenkombination „Strg+Alt+Entf“ an den Zielserversender:*
 - Wählen Sie **Keyboard > Send Ctrl+Alt+Delete** (Tastatur > Strg+Alt+Entf senden), oder
 - klicken Sie auf der Symbolleiste auf die Schaltfläche **Send Ctrl+Alt+Delete** (Strg+Alt+Entf senden).

Keyboard Macros (Tastaturmakros)

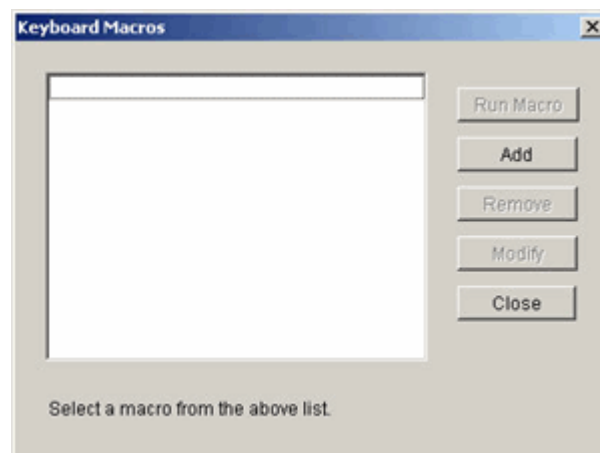
Tastaturmakros gewährleisten, dass für den Zielsystem vorgesehene Tastenkombinationen an den Zielsystem gesendet und nur von diesem interpretiert werden. Andernfalls werden sie von dem Computer interpretiert, auf dem der Virtual KVM Client ausgeführt wird (Client-PC).

Makros werden auf dem Client-PC gespeichert und sind PC-spezifisch. Wenn Sie also einen anderen PC verwenden, werden Ihnen Ihre Makros nicht angezeigt. Wenn eine andere Person Ihren PC verwendet und sich mit einem anderen Benutzernamen anmeldet, werden ihr die Makros angezeigt, da sie für den gesamten Computer gelten. Im Virtual KVM Client erstellte Tastaturmakros stehen im MPC zur Verfügung und umgekehrt.

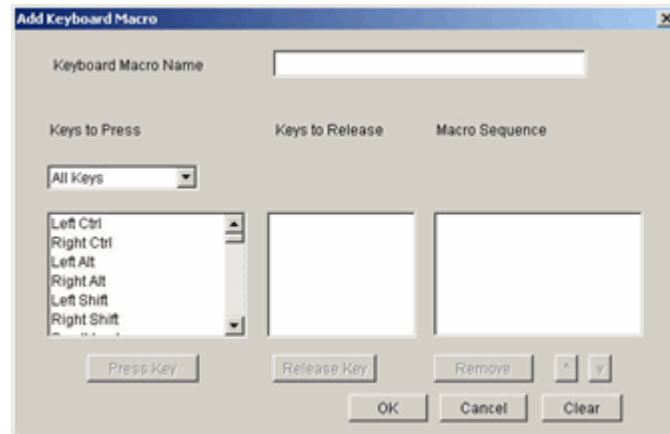
Erstellen eines Tastaturmakros

➤ *So erstellen Sie ein Tastaturmakro (fügen es hinzu):*

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



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



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

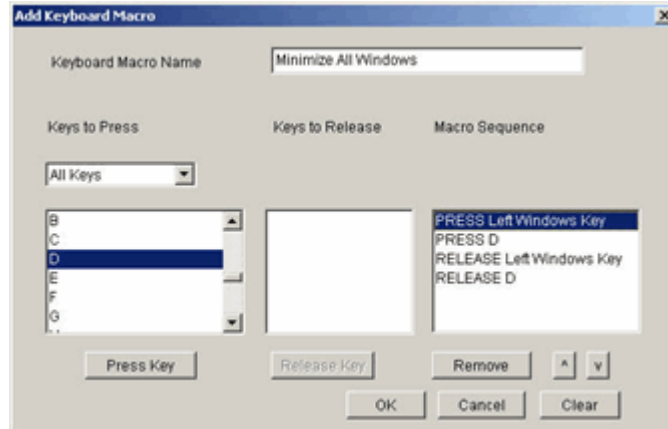
In diesem Beispiel wählen Sie zwei Tasten aus: die **Windows**-Taste und die **D**-Taste.

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

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

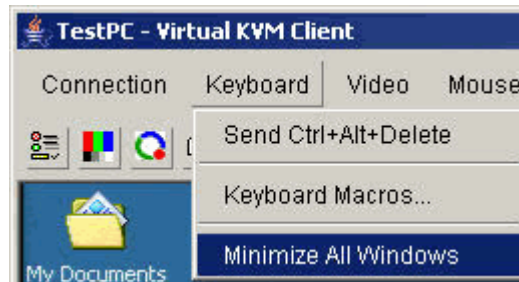
Menü „Keyboard“ (Tastatur)

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



Tipp: Verwenden Sie die Tasten **^** und **v**, um die Tastenreihenfolge zu ändern.

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



- *So löschen Sie alle Felder, um erneut mit der Auswahl zu beginnen:*
 - Klicken Sie auf die Schaltfläche **Clear** (Löschen).

Ausführen eines Tastaturmakros

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

- *So führen Sie ein Makro aus (mit obigem Beispiel):*
 - Wählen Sie **Keyboard > Minimize All Windows** (Tastatur > Alle Fenster minimieren).

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

- *So führen Sie ein Makro aus:*
 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 **Run Macro** (Makro ausführen).

Ändern eines 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**.

Entfernen eines Tastaturmakros

- *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.

Menü „ Video “

Videoeinstellungen können auf verschiedene Art und Weise automatisch aktualisiert werden:

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

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

Refresh Screen (Anzeige aktualisieren)


Die Option **Refresh Screen** (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms.



- *Führen Sie einen der folgenden Schritte aus, um die Videoeinstellungen zu aktualisieren:*
- Wählen Sie **Video > Refresh Screen** (Video > Anzeige aktualisieren).
 - Klicken Sie auf der Symbolleiste auf die Schaltfläche **Refresh Screen** (Anzeige aktualisieren).

Auto-Sense Video Settings (Videoeinstellungen automatisch erkennen)

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


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

- *Führen Sie für die automatische Erkennung der Videoeinstellungen einen der folgenden Schritte aus:*
 - Wählen Sie **Video > Auto-sense Video Settings** (Video > Videoeinstellungen automatisch erkennen).
 - Klicken Sie auf der Symbolleiste auf die Schaltfläche **Auto-sense Video Settings** (Videoeinstellungen automatisch erkennen).

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

Calibrate Color (Farbe kalibrieren)

Verwenden Sie den Befehl **Calibrate Color** (Farbe kalibrieren), um die Farbstufen (Farbton, Helligkeit, Sättigung) der übertragenen Videobilder zu optimieren. Die Farbeinstellungen der KX II-101-Einheit basieren auf dem jeweiligen Zielservers.

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

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

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

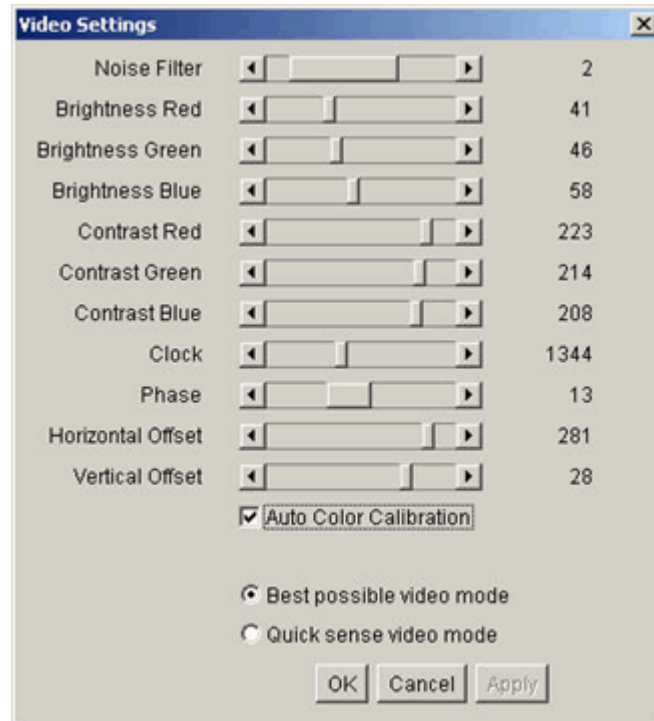
Video Settings (Videoeinstellungen)

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

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

➤ *So ändern Sie die Videoeinstellungen:*

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



2. Passen Sie die Einstellungen mithilfe der Schieberegler an, um das gewünschte Ergebnis zu erzielen (die Auswirkungen geänderter Einstellungen sind sofort erkennbar):

- **Noise Filter** (Rauschfilter): KX II-101 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 ein starke Farbabweichung vorliegt. Eine zu hohe Einstellung des Schwellwerts kann jedoch zu einer unbeabsichtigten Filterung von gewünschten Bildschirmänderungen führen. Niedrigere Einstellungen übermitteln die meisten Pixeländerungen. Eine zu niedrige Einstellung dieses Schwellwerts kann zu einer höheren Bandbreitenverwendung führen.
- **Brightness** (Helligkeit): Mithilfe dieser Einstellung passen Sie die Helligkeit der Zielserveranzeige an.
 - **Red** (Rot): Steuert die Helligkeit des roten Signals.
 - **Green** (Grün): Steuert die Helligkeit des grünen Signals.
 - **Blue** (Blau): Steuert die Helligkeit des blauen Signals.
- **Color Contrast Settings** (Farbkontrasteinstellungen): Steuern die Kontrasteinstellung.
 - **Contrast Red** (Kontrast Rot): Steuert das rote Signal.
 - **Contrast Green** (Kontrast Grün): Steuert das grüne Signal.
 - **Contrast Blue** (Kontrast Blau): Steuert das blaue Signal.
- Wenn das Videobild extrem verschwommen oder unscharf wirkt, können die Einstellungen für die Uhr und die Phase so gewählt werden, dass auf dem aktiven Zielserver ein besseres Bild angezeigt wird.

Warnhinweis: Gehen Sie bei der Änderung der Einstellungen für Uhr und Phase vorsichtig vor, da dies zu Verzerrungen oder sogar zum Verlust des Videobildes führen kann und Sie möglicherweise die vorherigen Einstellungen nicht wiederherstellen können. Wenden Sie sich an den technischen Kundendienst von Raritan, bevor Sie Änderungen vornehmen.

- **Clock** (Uhr): Diese Option steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobildes. Als Einstellung werden ungerade Zahlen empfohlen. Üblicherweise sollte diese Einstellung nicht geändert werden, da die automatische Erkennung meist korrekt ist.
 - **Phase**: Die Phasenwerte liegen zwischen 0 und 31 und werden zyklisch durchlaufen. Halten Sie bei dem Phasenwert an, der das beste Videobild für den aktiven Zielservier ergibt.
 - **Offset** (Versatz): Steuert die Positionierung auf dem Bildschirm.
 - **Horizontal Offset** (Horizontaler Versatz): Steuert die horizontale Positionierung der Zielservieranzeige auf dem Bildschirm.
 - **Vertical Offset** (Vertikaler Versatz): Steuert die vertikale Positionierung der Zielservieranzeige auf dem Bildschirm.
 - **Auto Color Calibration** (Automatische Farbkalibrierung): Aktivieren Sie dieses Kontrollkästchen, wenn die Farbe automatisch kalibriert werden soll.
 - **Video Sensing** (Videoerkennung): Wählen Sie einen Videoerkennungsmodus aus:
 - **Best possible video mode** (Bestmöglicher Videomodus): Beim Wechseln von Zielgeräten oder Zielauflösungen führt KX II-101 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 KX II-101-Gerät die schnelle automatische Erkennung des Videomodus durch, um das Bild des Zielgeräts schneller anzuzeigen. Diese Option eignet sich insbesondere für die Eingabe der BIOS-Konfiguration eines Zielservers nach einem Neustart.
3. Klicken Sie auf **Apply** (Übernehmen). Die Videoeinstellungen werden geändert.

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

Menü „ Mouse “ (Maus)

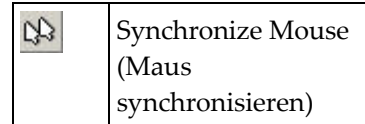
Bei der Steuerung eines Zielservers zeigt die KX II-101-Remotekonsole zwei Cursor an: Ein Cursor gehört zur Client-Workstation und der andere zum Zielserver. Sie können entweder im Ein-Cursor-Modus oder im Zwei-Cursor-Modus arbeiten. Wenn der Zwei-Cursor-Modus korrekt konfiguriert ist, sind die beiden Cursor aneinander ausgerichtet. Hilfe bei Problemen mit der Maussynchronisation finden Sie unter Konfigurieren des Zielservers.

Bei zwei Cursor bietet das KX II-101-Gerät verschiedene Mausmodi:

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

Synchronize Mouse (Maus synchronisieren)

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



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

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

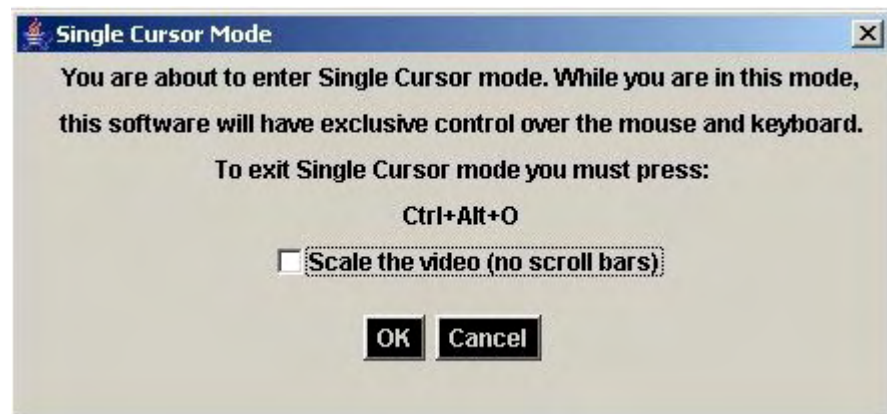
Single Mouse Cursor (Ein Cursor)

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



Menü „Mouse“ (Maus)

- *Führen Sie einen der folgenden Schritte aus, um den Ein-Cursor-Modus zu aktivieren:*
 - Wählen Sie **Mouse > Single Mouse Cursor** (Maus > Ein Cursor).
 - Klicken Sie auf der Symbolleiste auf die Schaltfläche **Single/Double Mouse Cursor** (Ein/Zwei Cursor).
- *So beenden Sie den Ein-Cursor-Modus:*
 1. Wenn der Ein-Cursor-Modus aufgerufen wird, wird die folgende Meldung angezeigt. Klicken Sie auf **OK**.



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

Standard

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

- *So gelangen Sie in den Standardmausmodus:*
 - Wählen Sie **Mouse > Standard** (Maus > Standard).

Intelligent

Im intelligenten Mausmodus erkennt das KX II-101-Gerät die Mauseinstellungen des Zielgeräts und kann die Mauszeiger dementsprechend synchronisieren, wodurch die Mausbeschleunigung auf dem Zielgerät ermöglicht wird. In diesem Modus „tanzt“ der Cursor in der oberen linken Ecke des Bildschirms und berechnet die Beschleunigung. Damit dieser Modus richtig funktioniert, müssen bestimmte Bedingungen erfüllt sein.

Weitere Informationen zum intelligenten Mausmodus finden Sie im Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan (Anhang B: Bedingungen zur intelligenten Maussynchronisation). Dieses Handbuch finden Sie auf der Website von Raritan unter <http://www.raritan.com/support/productdocumentation> oder auf der CD-ROM von Raritan mit Benutzerhandbüchern und Kurzanleitungen, die im Lieferumfang von KX II-101 enthalten ist.

➤ *So gelangen Sie in den intelligenten Mausmodus:*

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

Bedingungen für die intelligente Maussynchronisation

Die Option **Intelligent Mouse Synchronization** (Intelligente Maussynchronisation) im Menü **Mouse** (Maus) synchronisiert automatisch die Cursor in Inaktivitätsphasen. Zur korrekten Synchronisation müssen 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 Zielgeschwindigkeit des Cursors muss auf die mittlere Stufe eingestellt sein.
- Erweiterte Mauseigenschaften, wie **Zeigerbeschleunigung verbessern** oder **In Dialogfeldern automatisch zur Standardschaltfläche springen**, müssen deaktiviert sein.
- Wählen Sie im Fenster **Video Settings** (Videoeinstellungen) die Option **Best Possible Video Mode** (Bestmöglicher Videomodus).

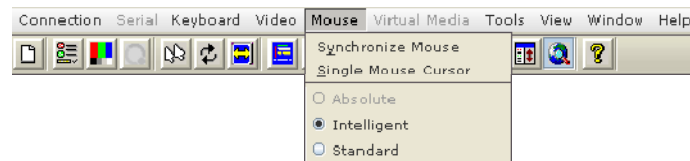
Menü „Mouse“ (Maus)

- 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 **Remote KVM Console** (Remote-KVM-Konsole) sichtbar sein.
- Wenn Sie die Funktion zur intelligenten Maussynchronisation nutzen, können Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu Problemen führen. Um Probleme mit dieser Funktion zu vermeiden, empfiehlt Raritan, Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu entfernen.

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

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

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



Absolute (Absolut)

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

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

- *So gelangen Sie in den Mausmodus „Absolute“ (Absolut):*
 - Wählen Sie **Mouse > Absolute** (Maus > Absolut).

Virtuelle Medien

Umfassende Informationen zum Einrichten und Verwenden virtueller Medien finden Sie im Kapitel *Virtuelle Medien* (auf Seite 115).

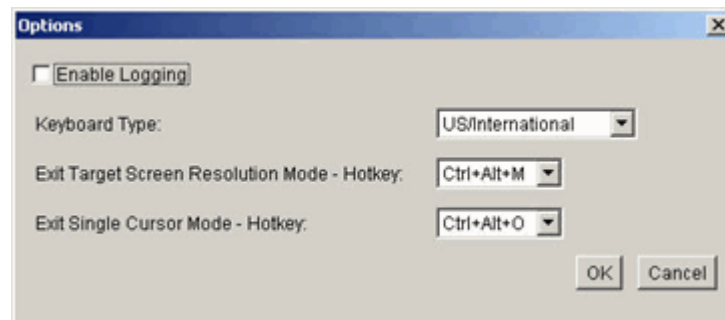
Menü „ Tools “ (Extras)

Options (Optionen)

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

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

1. Wählen Sie **Tools > Options** (Extras > Optionen). Das 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)
 - Belgian (Belgisch)
 - Norwegian (Norwegisch)

- Danish (Dänisch)
 - Swedish (Schwedisch)
4. **Exit Target Screen Resolution Mode – Hotkey** (Zugriffstaste zum Beenden des Modus Zielbildschirmauflösung): Wenn Sie in den Modus **Target Screen Resolution** (Zielbildschirmauflösung) wechseln, wird der Zielservers im Vollbildmodus mit der entsprechenden Auflösung angezeigt. Über diese Zugriffstaste können Sie diesen Modus beenden. Wählen Sie eine Option aus der Dropdown-Liste.
 5. **Exit Single Cursor Mode - Hotkey** (Zugriffstaste zum Beenden des Ein-Cursor-Modus): Im Ein-Cursor-Modus wird nur der Cursor des Zielservers angezeigt. Mit dieser Zugriffstaste können Sie den Ein-Cursor-Modus beenden und den Cursor des Client wieder anzeigen. Treffen Sie Ihre Auswahl in der Dropdown-Liste.
 6. Klicken Sie auf **OK**.

Menü „ View “ (Ansicht)

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).

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 Zielservers-Desktop angezeigt, und Sie müssen nicht die Bildlaufleiste verwenden.

- *So aktivieren bzw. deaktivieren Sie die Skalierung:*
 - Wählen Sie **View > Scaling** (Ansicht > Skalieren).

Menü „Help“ (Hilfe)

Target Screen Resolution (Zielbildschirmauflösung)

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

- *So gelangen Sie in den Modus „Target Screen Resolution“ (Zielbildschirmauflösung):*
 - Wählen Sie **View > Target Screen Resolution** (Ansicht > Zielbildschirmauflösung).

- *So beenden Sie den Modus „Target Screen Resolution“ (Zielbildschirmauflösung):*
 - Drücken Sie die im Dialogfeld **Options** (Optionen) konfigurierte Zugriffstaste. Standardmäßig ist dies die Tastenkombination **Strg+Alt+M**.

*Hinweis für CC-SG-Benutzer: **Target Screen Resolution** (Zielbildschirmauflösung) ist deaktiviert; der Vollbildmodus ist nur verfügbar, wenn das KX II-101-Gerät nicht über CC-SG verwaltet wird.*

Menü „ Help “ (Hilfe)

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

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

- *So rufen Sie die Versionsinformationen ab:*
 - Wählen Sie **Help > About Raritan Virtual KVM Client** (Hilfe > Informationen zum Raritan Virtual KVM Client).

Kapitel 7 Virtuelle Medien

In diesem Kapitel

Überblick.....	116
Voraussetzungen für die Verwendung virtueller Medien.....	118
Verwenden virtueller Medien.....	119
Öffnen einer KVM-Sitzung.....	120
Herstellen einer Verbindung mit virtuellen Medien	121
Trennen von virtuellen Medien	124
File Server Setup (Dateiserver-Setup) (nur für Dateiserver-ISO-Abbilder)	125

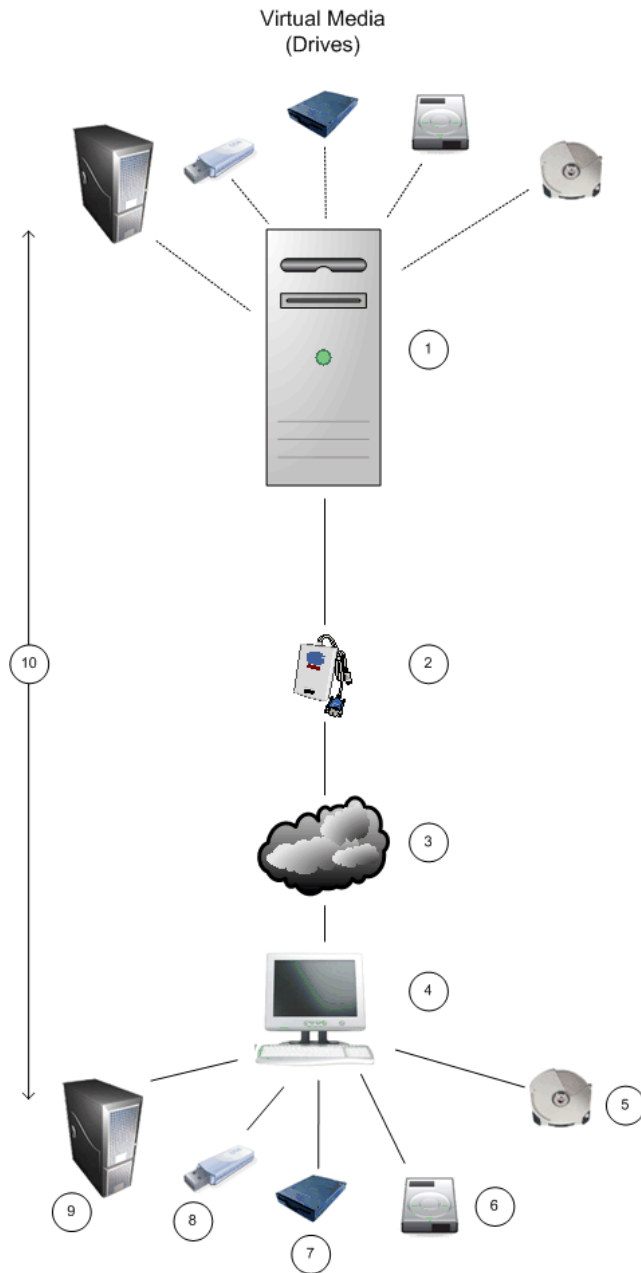
Überblick

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 Zielserver installiert. Der Zielserver hat Lese- und Schreibzugriff auf die Medien, als wären sie physisch mit dem Zielserver verbunden. Virtuelle Medien können interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten, 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.



- 1 Zielserver
- 2 KX II-101
- 3 IP-Netzwerkverbindung von KX II-101 zur lokalen Workstation
- 4 Lokale Workstation
- 5 CD-/DVD-Laufwerk

Voraussetzungen für die Verwendung virtueller Medien

- 6 Festplatte für Bilddateien
- 7 Diskettenlaufwerk
- 8 USB-Stick
- 9 Remote-Dateiserver (ISO-Abbilder)
- 10 Virtuelle Verbindung

Voraussetzungen für die Verwendung virtueller Medien

Für die Verwendung virtueller Medien müssen folgende Bedingungen erfüllt sein:

KX II-101

- Für Benutzer, die Zugriff auf virtuelle Medien benötigen, müssen KX II-101-Berechtigungen eingerichtet werden, die den Zugriff auf die relevanten Ports gestatten, sowie der virtuelle Medienzugriff (Port-Berechtigung **VM Access** [VM-Zugriff]) für diese Ports. Port-Berechtigungen werden auf Gruppenebene festgelegt. Weitere Informationen finden Sie unter Festlegen von Port-Berechtigungen.
- Zwischen dem KX II-101-Gerät und dem Zielsystem muss eine USB-Verbindung bestehen.
- Wenn Sie den Modus **PC-Share** (PC-Freigabe) verwenden möchten, müssen Sie auf der Seite **Security Settings** (Sicherheitseinstellungen) auch das Kontrollkästchen **VM Share Mode** (VM-Freigabemodus) aktivieren.

Client-PC

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

Hinweis: Unter Windows Vista müssen Sie die Benutzerkontensteuerung wie folgt deaktivieren: Wählen Sie **Systemsteuerung > Benutzerkonten > Benutzerkontensteuerung ein- oder ausschalten**.

Wenn Sie die Vista-Kontoberechtigungen nicht ändern möchten, führen Sie Internet Explorer als Administrator aus. Klicken Sie dazu auf das Menü **Start**, klicken Sie mit der rechten Maustaste auf **Internet Explorer**, und wählen Sie **Als Administrator ausführen** aus dem Kontextmenü.

- USB 2.0-Ports sind schneller und daher vorzuziehen.

Zielserver

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

Verwenden virtueller Medien

Mithilfe des Features **Virtual Media** (Virtuelle Medien) von KX II-101 können Sie bis zu zwei Laufwerke (unterschiedlichen Typs) installieren. Diese Laufwerke sind während der VM-Sitzung zugänglich.

➤ *So verwenden Sie virtuelle Medien:*

1. Schließen Sie das Medium an den Client-PC oder Netzwerkdateiserver an, auf den Sie über den Zielserver zugreifen möchten. Dieser Schritt muss nicht als erster erfolgen, jedoch bevor Sie versuchen, auf das Medium zuzugreifen.
2. Vergewissern Sie sich, dass die entsprechenden **Voraussetzungen** (siehe "Voraussetzungen für die Verwendung virtueller Medien" auf Seite 118) erfüllt sind.
3. (Nur bei Dateiserver-ISO-Abbildern) Wenn Sie auf Dateiserver-ISO-Abbilder zugreifen möchten, lassen Sie diese Dateiserver und Abbilder über die Seite **File Server Setup (Dateiserver-Setup)** (siehe "File Server Setup (Dateiserver-Setup) (nur für Dateiserver-ISO-Abbilder)" auf Seite 125) der KX II-101-Remote-Konsole ermitteln.

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

4. Öffnen Sie eine KVM-Sitzung mit dem entsprechenden Zielserver.
5. Stellen Sie eine Verbindung mit dem virtuellen Medium her.

Virtuelles Medium	Entsprechende VM-Option
Lokale Laufwerke	Connect Drive (Laufwerk verbinden) (siehe "Lokale Laufwerke" auf Seite 121)

Öffnen einer KVM-Sitzung

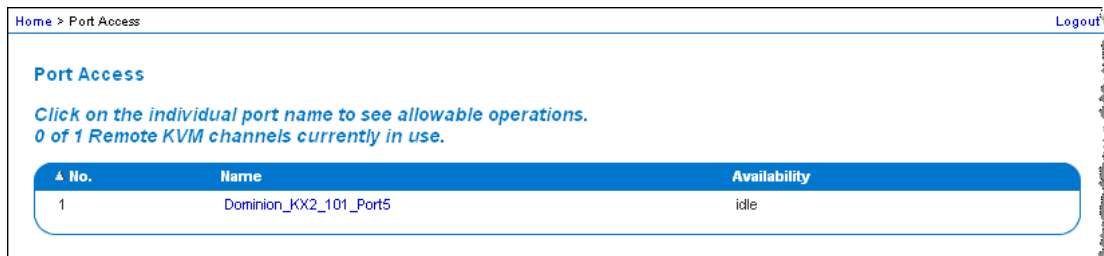
Virtuelles Medium	Entsprechende VM-Option
Lokale CD-/DVD-Laufwerke	Connect CD-ROM/ISO Image (<i>CD-ROM-/ISO-Abbild verbinden</i>) (siehe "CD-ROM-/DVD-ROM-/ISO-Abbilder" auf Seite 123)
ISO-Abbilder	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)
Dateiserver-ISO-Abbilder	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)

Nach Abschluss Ihrer Aufgaben **trennen Sie die Verbindung zum virtuellen Medium** (siehe "Trennen von virtuellen Medien" auf Seite 124).

Öffnen einer KVM-Sitzung

➤ *So öffnen Sie eine KVM-Sitzung:*

1. Rufen Sie in der KX II-101-Remote-Konsole die Seite **Port Access** (Port-Zugriff) auf.



2. Stellen Sie auf dieser Seite eine Verbindung mit dem Zielserver her:
 - a. Klicken Sie auf den Namen des Zielservers.
 - b. Wählen Sie im Popup-Menü **Connect** (Verbinden) aus.



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

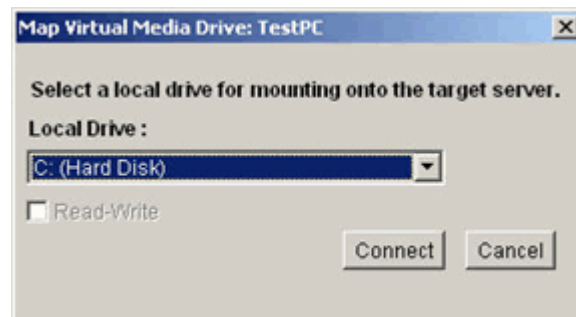
Herstellen einer Verbindung mit virtuellen Medien

Lokale Laufwerke

Mit dieser Option installieren Sie ein gesamtes Laufwerk. Das gesamte Festplattenlaufwerk wird auf dem Zielserver virtuell installiert. Verwenden Sie diese Option nur für Festplatten und externe Laufwerke, nicht jedoch für Netzwerk-, CD-ROM- oder DVD-ROM-Laufwerke. Nur für diese Option ist **Read-Write** (Lese-/Schreibzugriff) verfügbar.

Hinweis: KVM-Zielserver mit bestimmten Versionen des Windows-Betriebssystems akzeptieren möglicherweise keine neuen Massenspeicherverbindungen, nachdem eine NTFS-formatierte Partition (z. B. das lokale Laufwerk C) an sie umgeleitet wurde. Schließen Sie in diesem Fall die KX II-101-Remote-Konsole, und stellen Sie erneut eine Verbindung her, bevor Sie ein weiteres virtuelles Mediengerät umleiten. Wenn andere Benutzer mit demselben Zielserver verbunden sind, müssen auch sie diese Verbindung trennen.

- So greifen Sie auf ein Laufwerk auf dem 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 Wechseldatenträger zur Verfügung. Weitere Informationen finden Sie unter *Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist* (auf Seite 122). Bei dieser Option können Sie Daten auf dem angeschlossenen USB-Datenträger lesen und schreiben.

Herstellen einer Verbindung mit virtuellen Medien

WARNUNG: Den Lese-/Schreibzugriff zu aktivieren kann gefährlich sein! Wenn mehrere Einheiten gleichzeitig auf dasselbe Laufwerk zugreifen, kann dies zu Datenbeschädigungen führen. Sollten Sie den Schreibzugriff nicht benötigen, deaktivieren Sie dieses Kontrollkästchen.

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

Hinweis: Besteht keine USB-Verbindung zum Zielsystem, wird die folgende Warnmeldung eingeblendet: „The virtual media capability is set up but will not be available until the USB cable is connected or the target is powered on. Please check your USB connectivity or see if the target is powered on.“ (Die Funktion für virtuelle Medien ist eingerichtet, steht jedoch erst zur Verfügung, wenn das USB-Kabel angeschlossen oder das Ziel eingeschaltet wird. Prüfen Sie Ihre USB-Verbindung, oder stellen Sie sicher, dass das Ziel eingeschaltet ist.) Beheben Sie das Problem, und schließen Sie das Laufwerk wieder an.

Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist

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

- Bei allen Festplatten
- Wenn das Laufwerk schreibgeschützt ist
- Wenn der Benutzer nicht über eine Lese-/Schreibberechtigung verfügt:
 - Unter **Port Permission** (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.

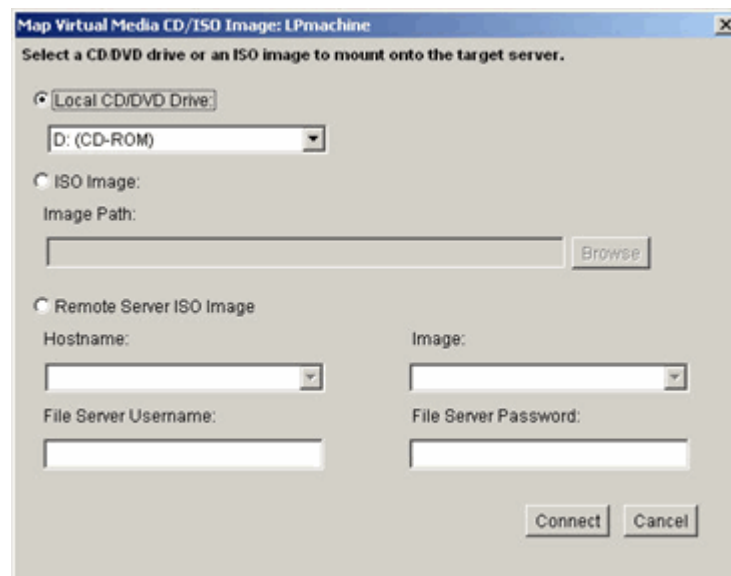
CD-ROM-/DVD-ROM-/ISO-Abbilder

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:

Trennen von virtuellen Medien

- a. Wählen Sie die Option **ISO Image** (ISO-Abbild). Mit dieser Option greifen Sie auf ein Laufwerkabbild einer CD, DVD oder Festplatte zu. Nur das ISO-Format wird unterstützt.
 - b. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen).
 - c. Navigieren Sie zu dem Pfad des gewünschten Laufwerkabbilds, und klicken Sie auf **Open** (Öffnen). Der Pfad wird in das Feld **Image Path** (Abbildpfad) geladen.
 - 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 den Dropdown-Listen **Hostname** und **Image** (Abbild) einen Hostnamen und ein Abbild aus. Zur Verfügung stehen die Dateiserver und Abbildpfade, die Sie auf der Seite **File Server Setup** (Dateiserver-Setup) konfiguriert haben. Die Dropdown-Liste enthält nur Elemente, die Sie auf der KX II-101-Seite **File Server Setup** (Dateiserver-Setup) konfiguriert haben.
 - c. **File Server Username** (Dateiserver-Benutzername): Der für den Zugriff auf den Dateiserver erforderliche Benutzername.
 - d. **File Server Password** (Dateiserver-Kennwort): Das für den Zugriff auf den Dateiserver erforderliche Kennwort (Eingabe erfolgt verdeckt).
 - e. Klicken Sie auf **Connect** (Verbinden).

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

Trennen von virtuellen Medien

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

*Hinweis: Anstatt das virtuelle Medium über die Option **Disconnect** zu trennen, können Sie auch einfach die KVM-Verbindung beenden.*

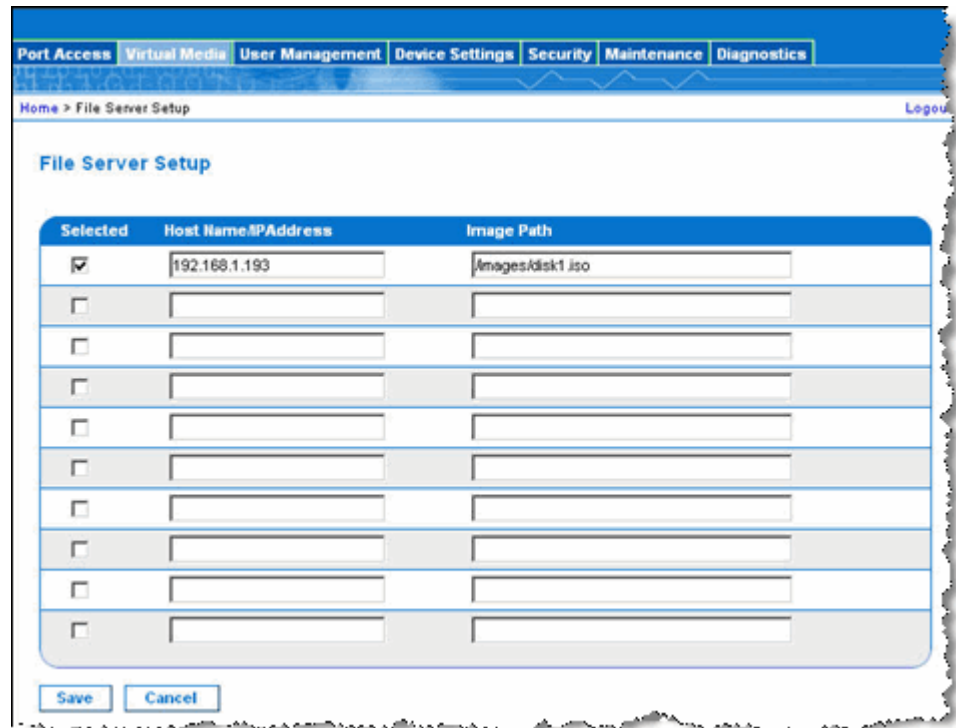
File Server Setup (Dateiserver-Setup) (nur für Dateiserver-ISO-Abbilder)

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

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

Legen Sie auf der Seite **File Server Setup** (Dateiserver-Setup) der KX II-101-Remote-Konsole die Dateiserver und Abbildpfade fest, auf die Sie über virtuelle Medien in KX II-101 zugreifen möchten. Hier angegebene Dateiserver-ISO-Abbilder stehen unter **Remote Server ISO Image** (ISO-Abbild auf Remote-Server) in den Dropdown-Listen **Hostname** und **Image** (Abbild) zur Auswahl (im Dialogfeld *Map Virtual Media CD/ISO Image (CD-/ISO-Abbild als virtuelles Medium zuordnen)* (siehe "CD-ROM-/DVD-ROM-/ISO-Abbilder" auf Seite 123)).

- So legen Sie Dateiserver-ISO-Abbilder für den virtuellen Medienzugriff fest:
 1. Wählen Sie in der KX II-101-Remote-Konsole **Virtual Media** (Virtuelle Medien). Die Seite **File Server Setup** (Dateiserver-Setup) wird angezeigt.



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

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

Kapitel 8 Geräteverwaltung

In diesem Kapitel

Menü „ Device Settings “ (Geräteeinstellungen).....	127
Network Settings (Netzwerkeinstellungen).....	129
Device Services (Gerätedienste).....	134
Keyboard/Mouse Setup (Tastatur/Maus einrichten)	136
Serial Port Settings (Einstellungen für seriellen Port).....	137
Date/Time Settings (Datum-/Uhrzeiteinstellungen)	139
Ereignisverwaltung	140
Port Configuration (Port-Konfiguration)	149

Menü „ Device Settings “ (Geräteeinstellungen)

Das Menü **Device Settings** (Geräteeinstellungen) umfasst folgende Optionen: **Network** (Netzwerk), **Device Services** (Gerätedienste), **Keyboard/Mouse** (Tastatur/Maus), **Serial Port** (Serieller Port), **Date/Time** (Datum/Uhrzeit), **Event Management - Settings** (Ereignisverwaltung - Einstellungen), **Event Management - Destinations** (Ereignisverwaltung - Ziele) und **Port Configuration** (Port-Konfiguration).

Option	Aktion
Network (Netzwerk)	Anpassen der Netzwerkkonfiguration für KX II-101.
Device Services (Gerätedienste)	Konfigurieren des KX II-101-Netzwerk-Ports und Aktivieren des TELNET- und SSH-Zugriffs.
Keyboard/Mouse (Tastatur/Maus)	Konfigurieren der Erkennung der von KX II-101 gesendeten Tastatur- und Maussignale durch den Zielservers.
Serial Port (Serieller Port)	Auswählen und Konfigurieren der Funktion des seriellen Ports von KX II-101.
Date/Time (Datum/Uhrzeit)	Festlegen von Datum, Uhrzeit, Zeitzone und Network Time Protocol (NTP)
Event Management – Settings (Ereignisverwaltung – Einstellungen)	Konfigurieren von SNMP und Syslog.

Menü „Device Settings“ (Geräteeinstellungen)

Option	Aktion
Event Management – Destinations (Ereignisverwaltung – Ziele)	Auswählen, welche Systemereignisse verfolgt und wohin die Informationen gesendet werden sollen.
Port Configuration (Port-Konfiguration)	Konfigurieren von KVM-Ports und Ausgängen.

Network Settings (Netzwerkeinstellungen)

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

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

- **None** (Keine): Hierbei handelt es sich um die empfohlene Standardoption (**Static IP** [Statisches IP]). Da die KX II-101-Einheit Teil Ihrer Netzwerkinfrastruktur ist, möchten Sie wahrscheinlich, dass die Adresse möglichst konstant bleibt. Bei dieser Option können Sie die Netzwerkparameter selbst einrichten.
- **DHCP**: Die IP-Adresse wird automatisch von einem DHCP-Server zugewiesen.

➤ *So ändern Sie die Netzwerkkonfiguration:*

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

The screenshot shows the 'Network Settings' page with two main sections: 'Network Basic Settings' and 'LAN Interface Settings'.

Network Basic Settings:

- Device Name: DKX2-101
- IP auto configuration: DHCP
- Preferred host name (DHCP only):
- IP address: 192.168.50.74
- Subnet mask: 255.255.255.0
- Gateway IP address: 192.168.50.126
- Primary DNS server IP address: 192.168.50.114
- Secondary DNS server IP address: 192.168.50.112

LAN Interface Settings:

- Note: For reliable network communication, configure the Dominion KX2-101 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX2-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.
- Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok
- LAN Interface Speed & Duplex: Autodetect
- Bandwidth Limit: No Limit
- Set System ACL button

Buttons at the bottom: OK, Reset To Defaults, Cancel.

2. Aktualisieren Sie die Basisnetzwerkeinstellungen unter **Network Basic Settings**. Weitere Informationen zu den einzelnen Feldern finden Sie unter Network Basic Settings (Basisnetzwerkeinstellungen).

Network Settings (Netzwerkeinstellungen)

3. Aktualisieren Sie die LAN-Schnittstelleneinstellungen unter **LAN Interface Settings**. Weitere Informationen zu den einzelnen Feldern finden Sie unter LAN Interface Settings (LAN-Schnittstelleneinstellungen).
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 brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).
 - *So stellen Sie die werksseitigen Standardeinstellungen wieder her:*
 - Klicken Sie auf **Reset to Defaults** (Standardeinstellungen wiederherstellen).

Network Basis Settings (Basisnetzwerkeinstellungen)

Network Basic Settings

Device Name *
DKX2-101

IP auto configuration
DHCP

Preferred host name (DHCP only)
[Empty]

IP address
192.168.59.99

Subnet mask
255.255.255.0

Gateway IP address
192.168.59.126

Primary DNS server IP address
192.168.59.2

Secondary DNS server IP address
192.168.51.10

OK Reset To Defaults Cancel

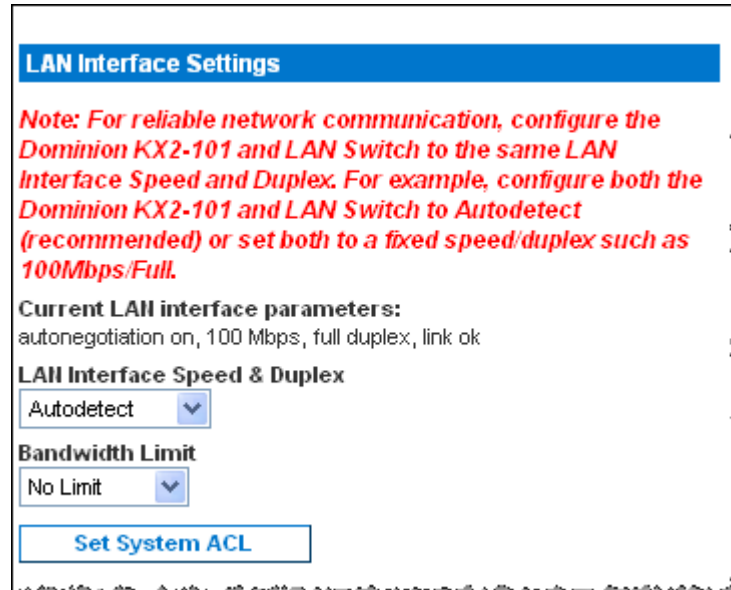
- **Device Name** (Gerätename): Geben Sie einen eindeutigen Namen für das Gerät ein (maximal 16 Zeichen, keine Leerzeichen). Sie sollten das Gerät leicht an seinem Namen erkennen können. Der Standardname für eine KX II-101-Einheit lautet „DKX2-101“. Auch Remote-Benutzern wird dieser Name angezeigt. Hat jedoch ein MPC-Benutzer ein Verbindungsprofil für dieses Gerät erstellt, wird diesem Benutzer das Feld **Description** (Beschreibung) aus dem Profil angezeigt.
- **IP auto configuration** (Automatische IP-Konfiguration): Wählen Sie eine Option aus der Dropdown-Liste:
 - **None** (Keine): Wählen Sie diese Option, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen möchten (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

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

- **IP Address** (IP-Adresse): Die Standard-IP-Adresse lautet 192.168.0.192.
- **Subnet Mask** (Subnetzmaske): Die Standardsubnetzmaske lautet 255.255.255.0.
- **Gateway IP Address** (Gateway-IP-Adresse): Die IP-Adresse des Gateways (falls eines verwendet wird).
- **Primary DNS Server IP Address** (IP-Adresse des primären DNS-Servers): Der primäre DNS-Server zur Übertragung von Namen in IP-Adressen.
- **Secondary DNS-Server IP Address** (IP-Adresse des sekundären DNS-Servers): Der sekundäre DNS-Server zur Übertragung von Namen in IP-Adressen (falls ein solcher verwendet wird).
- **DHCP**: Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

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

LAN Interface Settings (LAN-Schnittstelleneinstellungen)



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

Autodetect (Automatische Erkennung)	Standardoption
10 Mbps/Half (10 Mbit/s/Halbduplex)	Beide LEDs blinken
10 Mbps/Full (10 Mbit/s/Vollduplex)	Beide LEDs blinken
100 Mbps/Half (100 Mbit/s/Halbduplex)	Gelbe LED blinkt

100 Mbps/Full (100 Mbit/s/Vollduplex)		Gelbe LED blinkt
1000 Mbps/Full (1000 Mbit/s/Vollduplex)	Gigabit	Grüne LED blinkt

Half-duplex (Halbduplex) sorgt für Kommunikation in beide Richtungen, jedoch nicht gleichzeitig.

Full-duplex (Vollduplex) ermöglicht die gleichzeitige Kommunikation in beide Richtungen.

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

- **Bandwidth Limit** (Maximale Bandbreite): Wählen Sie eine verfügbare Bandbreite aus.
 - 128 Kilobit
 - 256 Kilobit
 - 512 Kilobit
 - 2 Megabit
 - 5 Megabit
 - 10 Megabit
 - 100 Megabit
 - No Limit (Keine Beschränkung)
- **Set System ACL** (System-ACL festlegen): Klicken Sie auf diese Schaltfläche, um eine globale Zugriffssteuerungsliste für die KX II-101-Einheit festzulegen. Damit wird sichergestellt, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet. Die Seite *IP Access Control* (siehe "IP Access Control (IP-Zugriffssteuerung)" auf Seite 171) (IP-Zugriffssteuerung) wird angezeigt.

Hinweis: Diese ACL-Werte sind global und betreffen die gesamte KX II-101-Einheit. Sie können ACLs auch auf Gruppenebene erstellen. Erstellen Sie beispielsweise die Benutzergruppe „ Externe Lieferanten “, die nur über einen bestimmten IP-Adressbereich auf KX II-101 zugreifen kann. (Weitere Informationen zum Erstellen gruppenspezifischer Zugriffssteuerungslisten finden Sie unter Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)).

Device Services (Gerätedienste)

Geben Sie die Verbindungsoptionen für KX II-101 auf der Seite **Device Services** (Gerätedienste) an.

Home > Device Settings > Device Services

Services

Discovery Port *
5000

Enable TELNET Access

TELNET Port
23

Enable SSH Access

SSH Port
22

Enable Direct Port Access via URL

OK Reset To Defaults Cancel

➤ *So konfigurieren Sie den Erkennungs-Port:*

1. Wählen Sie **Device Settings > Device Services** (Geräteeinstellungen > Gerätedienste). Die Seite **Device Services** (Gerätedienste) wird angezeigt.
2. Geben Sie den Netzwerk-Port ein, der von KX II-101 zur Kommunikation mit dem Client-PC verwendet wird.
3. Klicken Sie zum Speichern der Einstellungen auf **Save** (Speichern).

➤ *So aktivieren Sie den TELNET-Zugriff:*

1. Wählen Sie **Device Settings > Device Services** (Geräteeinstellungen > Gerätedienste). Die Seite **Device Services** (Gerätedienste) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen **Enable TELNET Access** (TELNET-Zugriff aktivieren).
3. Geben Sie den Netzwerk-Port ein, der für den TELNET-Zugriff auf KX II-101 verwendet wird.

4. Klicken Sie zum Speichern der Einstellungen auf **Save** (Speichern).
- *So aktivieren Sie den SSH-Zugriff:*
1. Wählen Sie **Device Settings > Device Services** (Geräteeinstellungen > Gerätedienste). Die Seite **Device Services** (Gerätedienste) wird angezeigt.
 2. Aktivieren Sie das Kontrollkästchen **Enable SSH Access** (SSH-Zugriff aktivieren).
 3. Geben Sie den Netzwerk-Port ein, der für den SSH-Zugriff auf KX II-101 verwendet wird.
 4. Klicken Sie zum Speichern der Einstellungen auf **Save** (Speichern).

Aktivieren des direkten Port-Zugriffs

Über direkten Port-Zugriff können Sie auf den KX II-101-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. Wählen Sie **Device Settings > Device Services** (Geräteeinstellungen > Gerätedienste). Die Seite **Device Services** (Gerätedienste) wird angezeigt.
 2. Aktivieren Sie das Kontrollkästchen **Enable Direct Port Access via URL** (Direkten Port-Zugriff über URL aktivieren).
 3. Klicken Sie zum Speichern der Einstellungen auf **Save** (Speichern).

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

- Definieren Sie einen URL mit IP-Adresse, Benutzername, Kennwort, und, falls erforderlich, Port-Nummer der KX II-101-Einheit. Steht nur ein KVM-Port zur Verfügung, ist die Port-Nummer nicht erforderlich.

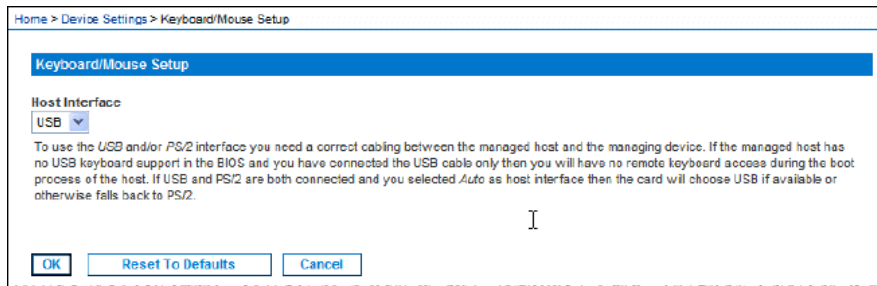
Verwenden Sie folgendes Format für den URL für direkten Port-Zugriff:

`https://[IP-Adresse]/dpa.asp?username=[Benutzername]&password=[Kennwort]&port=[Port-Nummer]`

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

Keyboard/Mouse Setup (Tastatur/Maus einrichten)

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



- **Host Interface** (Host-Schnittstelle): Bestimmt, ob KX II-101 Tastatur- und Mausdaten über eine PS/2- oder USB-Verbindung sendet.
 - **Auto** (Automatisch): Bei dieser Einstellung verwendet KX II-101 eine USB-Verbindung, falls verfügbar, und ansonsten eine PS/2-Verbindung.
 - **USB**: Zwingt KX II-101, die USB-Verbindung zum Senden der Tastatur- und Mausdaten an das Hostgerät zu verwenden.
 - **PS/2**: Zwingt KX II-101, die PS/2-Verbindung zum Senden der Tastatur- und Mausdaten an das Hostgerät zu verwenden.
- *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 festzulegen, wie KX II-101 den seriellen Port verwendet.

➤ *So konfigurieren Sie den seriellen Port:*

1. Wählen Sie **Device Settings > Serial Port** (Geräteeinstellungen > Serieller Port). Die Seite **Serial Port Settings** (Einstellungen für seriellen Port) wird angezeigt.

2. Wählen Sie die Funktion für den seriellen Port aus:
 - **Admin Port** (Verwaltungs-Port): Wählen Sie diese Option, um eine direkte Verbindung zwischen KX II-101 und einem Client-PC herzustellen, um auf die erweiterten Konfigurationsoptionen zuzugreifen.
 - **PowerStrip Control** (PowerStrip-Steuerung): Wählen Sie diese Option, um KX II-101 mit einem seriell gesteuerten Powerstrip zu verbinden.
 - **Modem**: Wählen Sie diese Option, um ein externes Modem mit KX II-101 zu verbinden, um den DFÜ-Zugriff bereitzustellen.
3. Legen Sie die Einstellungen für die Option Modem wie folgt fest:
 - a. Wählen Sie die Datengeschwindigkeit zwischen KX II-101 und dem Modem in der Dropdown-Liste **Serial line speed** (Geschwindigkeit der seriellen Verbindung) aus.
 - b. Füllen Sie das Feld **Modem init string** (String für Modeminitialisierung) aus.

Serial Port Settings (Einstellungen für seriellen Port)

- c. Füllen Sie das Feld **Modem server IP address** (IP-Adresse für Modem-Server) aus. Hierbei handelt es sich um die Adresse, die der Benutzer eingibt, um die KX II-101-Webschnittstelle aufzurufen, sobald die Verbindung über das Modem hergestellt ist.
 - d. Füllen Sie das Feld **Modem client IP address** (IP-Adresse für Modem-Client) aus. Hierbei handelt es sich um die Adresse, die dem Benutzer nach der Verbindungsherstellung über das Modem zugewiesen wird.
4. Klicken Sie auf **OK**.

Date/Time Settings (Datum-/Uhrzeiteinstellungen)

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

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

Hinweis: KX II-101 unterstützt keine Sommerzeit.

➤ *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. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:

Ereignisverwaltung

- **User Specified Time** (Benutzerdefinierte Zeit): Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben.
 - **Synchronize with NTP Server** (Mit NTP-Server synchronisieren): Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
4. Falls Sie die Option **User Specified Time** (Benutzerdefinierte Zeit) ausgewählt haben, geben Sie Datum und Uhrzeit wie folgt ein:
 - a. Wählen Sie in der Dropdown-Liste **Month** einen Monat aus.
 - b. Geben Sie im Feld **Day** den Tag ein.
 - c. Geben Sie im Feld **Year** das Jahr im Format JJJJ ein.
 - d. Geben Sie im Feld **Time** die Uhrzeit im Format HH:MM ein (verwenden Sie das 24-Std-Zeitformat.)
 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. (Optional) Geben Sie im Feld **Secondary Time server** (Sekundärer Zeitserver) die entsprechende IP-Adresse ein.
 6. Klicken Sie auf **OK**.

Ereignisverwaltung

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

SNMP Configuration (SNMP-Konfiguration)

Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung und die Überwachung von Netzwerkgeräten und ihrer Funktionen. KX II-101 bietet über die Ereignisverwaltung Unterstützung für SNMP-Agenten. Weitere Informationen zu SNMP-Agenten und -Traps finden Sie unter *Konfigurieren des SNMP-Agenten* (auf Seite 146) und *SNMP-Trap-Konfiguration* (auf Seite 146).

- *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.

Home > Device Settings > Event Management - Settings

SNMP Configuration

SNMP Logging Enabled

Name
sai-Dlx2101

Contact
SAI

Location
FSD

Agent Community String

Type
Read-Write

Destination IP	Port #	Community
192.168.51.150	162	public
	162	public
	162	public
	162	public
	162	public

[Click here to view the Dominion KX2-101 SNMP MIB](#)

SysLog Configuration

Enable Syslog Forwarding

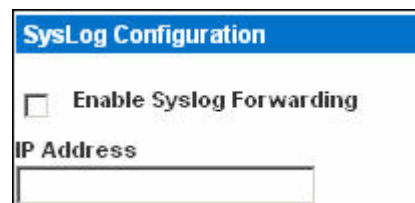
IP Address

OK Reset To Defaults Cancel

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

3. Geben Sie in die Felder **Name**, **Contact** (Kontakt) und **Location** (Ort) den Namen des SNMP-Agenten (dieser Dominion-Einheit), wie er in der KX II-101-Konsolenoberfläche angezeigt wird, einen Kontaktnamen für diese Einheit und den physischen Ort der Dominion-Einheit ein.
4. Geben Sie im Feld **Agent Community String** (Community-String des Agenten) den String der Dominion-Einheit ein. Eine SNMP-Community ist die Gruppe, der Geräte und Verwaltungsstationen, auf denen SNMP ausgeführt wird, angehören. Damit können Sie festlegen, wohin Informationen gesendet werden. Der Community-Name dient dazu, die Gruppe zu kennzeichnen. Ein SNMP-Gerät oder -Agent kann mehreren SNMP-Communitys angehören.
5. Legen Sie über die Dropdown-Liste **Type** (Typ) Lesezugriff (Read-Only) oder Lese-/Schreibzugriff (Read-Write) für die Community fest.
6. Konfigurieren Sie maximal fünf SNMP-Manager, indem Sie entsprechende Werte in die Felder **Destination IP** (IP-Zieladresse), **Port #** (Port-Nummer) und **Community** eingeben.
7. Klicken Sie auf den Link **Click here to view the KX II-101 SNMP MIB** (Klicken Sie hier, um die KX II-101 SNMP MIB anzuzeigen), um auf die SNMP Management Information Base zuzugreifen.
8. Klicken Sie auf **OK**.

Syslog-Konfiguration



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

- *So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).

- *So stellen Sie die werksseitigen Standardeinstellungen wieder her:*
 - Klicken Sie auf die Schaltfläche **Reset To Defaults** (Standardeinstellungen wiederherstellen).

Event Management - Destinations (Ereignisverwaltung - Ziele)

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

*Hinweis: SNMP-Traps werden nur generiert, wenn das Kontrollkästchen **SNMP Logging Enabled** (SNMP-Protokollierung aktiviert) aktiviert ist. Syslog-Ereignisse werden nur generiert, wenn das Kontrollkästchen **Enable Syslog Forwarding** (Syslog-Weiterleitung aktivieren) aktiviert ist. Beide Optionen befinden sich auf der Seite **Event Management - Settings** (Ereignisverwaltung - Einstellungen). Siehe **Event Management - Settings** (Ereignisverwaltung - Einstellungen).*

➤ *So wählen Sie Ereignisse und ihr Ziel aus:*

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

Category	Event	SNMP	Syslog	Audit Log	
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Ethernet Fallover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Device Management	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
End OC Control		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Device Update Started		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Device Update Completed		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Device Update Failed		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Firmware Update Failed		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Firmware File Discarded		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Firmware Validation Failed		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration Backed Up		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration Restored		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Port Connection Denied		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Security		Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
User Activity	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Port Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

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 brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).

- *So stellen Sie die werksseitigen Standardeinstellungen wieder her:*
 - Klicken Sie auf die Schaltfläche **Reset To Defaults** (Standardeinstellungen wiederherstellen).

Warnhinweis: Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisation zwischen KX II-101 und dem damit verbundenen Router verloren gehen, wenn KX II-101 neu gestartet wird. Das SNMP-Trap „reboot completed“ (Neustart abgeschlossen) wird dadurch nicht protokolliert.

Konfigurieren des SNMP-Agenten

SNMP-kompatible Geräte, genannt Agenten, speichern Daten über sich selbst in Management Information Bases (MIBs) und geben diese Daten an die SNMP-Manager zurück. Auf der Seite **Event Logging** (Ereignisprotokollierung) können Sie die SNMP-Verbindung zwischen KX II-101 (SNMP-Agent) und einem SNMP-Manager konfigurieren.

SNMP-Trap-Konfiguration

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

Trap-Name	Beschreibung
configBackup	Die Gerätekonfiguration wurde gesichert.
configRestore	Die Gerätekonfiguration wurde wiederhergestellt.
deviceUpdateFailed	Das Gerät konnte nicht aktualisiert werden.
deviceUpgradeCompleted	KX II-101 hat die Aktualisierung mittels einer RFP-Datei abgeschlossen.
deviceUpgradeStarted	KX II-101 hat die Aktualisierung mittels einer RFP-Datei begonnen.
factoryReset	Das Gerät wurde auf die Werkseinstellungen zurückgesetzt.

Trap-Name	Beschreibung
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-System hinzugefügt.
groupDeleted	Eine Gruppe wurde aus dem System gelöscht.
groupModified	Eine Gruppe wurde geändert.
ipConflictDetected	Ein IP-Adressenkonflikt wurde erkannt.
ipConflictResolved	Ein IP-Adressenkonflikt wurde gelöst.
networkFailure	Für eine der Ethernet-Schnittstellen des Produkts besteht keine Netzwerkverbindung mehr.
networkParameterChanged	Die Netzwerkparameter wurden geändert.
passwordSettingsChanged	Die Einstellungen für sichere Kennwörter wurden geändert.
portConnect	Ein zuvor authentifizierter Benutzer hat eine KVM-Sitzung gestartet.
portConnectionDenied	Eine Verbindung mit dem Zielport wurde verweigert.
portDisconnect	Die Sitzung des Benutzers einer KVM-Sitzung wird von selbigem ordnungsgemäß geschlossen.
portStatusChange	Der Port ist nicht mehr verfügbar.
powerNotification	Benachrichtigung über den Status der Stromversorgung: 1 = Aktiv, 0 = Inaktiv.
powerOutletNotification	Benachrichtigung über den Status eines Powerstrip-Geräteausgangs.
rebootCompleted	Der Neustart von KX II-101 ist abgeschlossen.
rebootStarted	KX II-101 wird neu gestartet: entweder durch Wiederherstellen der Stromversorgung oder durch einen „Warmstart“ mittels des Betriebssystems.
securityViolation	Ein Sicherheitsproblem ist aufgetreten.
startCCManagement	Für das Gerät wurde die CommandCenter-Verwaltung gestartet.

Ereignisverwaltung

Trap-Name	Beschreibung
stopCCManagement	Die CommandCenter-Verwaltung des Geräts wurde aufgehoben.
userAdded	Ein Benutzer wurde zum System hinzugefügt.
userAuthenticationFailure	Ein Benutzer hat versucht, sich mit einem falschen Benutzernamen und/oder Kennwort anzumelden.
userConnectionLost	Bei einem Benutzer mit aktiver Sitzung ist eine nicht ordnungsgemäße Sitzungstrennung aufgetreten.
userDeleted	Ein Benutzerkonto wurde gelöscht.
userLogin	Ein Benutzer hat sich erfolgreich bei KX II-101 angemeldet und wurde authentifiziert.
userLogout	Ein Benutzer hat sich erfolgreich und ordnungsgemäß von KX II-101 abgemeldet.
userModified	Ein Benutzerkonto wurde geändert.
userPasswordChanged	Das Ereignis wird ausgelöst, wenn das Kennwort irgendeines Benutzers des Geräts geändert wird.
userSessionTimeout	Die aktive Sitzung eines Benutzers wurde aufgrund einer Zeitüberschreitung beendet.
vmImageConnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu installieren. Für jeden Versuch einer Geräte-/Abbildzuordnung (Installation) wird dieses Ereignis generiert.
vmImageDisconnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu deinstallieren.

Port Configuration (Port-Konfiguration)

Die Seite **Port Configuration** (Port-Konfiguration) enthält eine Liste der KX II-101-Ports. Ports, die mit KVM-Zielserversn 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.

No.	Name	Type
1	Dominion_KX2_101_Port1	KVM
2	Power Port 1	PowerStrip

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 Number** (Port-Nummer): Die für die KX II-101-Einheit verfügbaren Ports werden beginnend mit 1 durchnummeriert.
- **Port Name** (Port-Name): 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** (Port-Typ): Der Typ des am Port angeschlossenen Ziels.

Port-Typ	Beschreibung
PowerStrip	Powerstrip
KVM	KVM-Ziel

2. Klicken Sie auf den Port-Namen des Ports, den Sie bearbeiten möchten.

Port Configuration (Port-Konfiguration)

- Für KVM-Ports wird die Seite Port angezeigt. 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 die Ausgänge benennen.

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

Kapitel 9 Stromzufuhrsteuerung

In diesem Kapitel

Überblick.....	151
Anschließen des Powerstrips	152
Benennen des Powerstrips (Seite „ Port “ für Powerstrips).....	153
Zuordnen von KVM-Zielservern zu Ausgängen (Seite „ Port “).....	155
Anzeigen der Ausgangszuordnungen.....	158
Steuern des Powerstrip-Geräts	159

Überblick

KX II-101 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 zu verwenden:*
1. Verbinden Sie den Powerstrip mit dem Zielserver.
 2. Benennen Sie den Powerstrip.
 3. Ordnen Sie einen Ausgang des Powerstrips dem Zielserver zu.
 4. Schalten Sie die Ausgänge des Powerstrips auf der Seite **Powerstrip Device (Powerstrip-Gerät)** (siehe "Steuern des Powerstrip-Geräts" auf Seite 159) ein und aus.

Anschließen des Powerstrips



- 1 DKX2-101-SPDUC-kabel (nicht im Lieferumfang enthalten) von KX II-101 zum Raritan-Powerstrip
- 2 Raritan-Powerstrip

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

1. Verbinden Sie den Mini-DIM9M-Stecker des DKX2-101-SPDUC-Kabels mit dem Port „Admin“ der KX II-101-Einheit.
2. Verbinden Sie den RJ45M-Stecker des DKX2-101-SPDUC-Kabels mit dem seriellen Port des Raritan-Powerstrips.
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.

Benennen des Powerstrips (Seite „ Port “ für Powerstrips)

Diese Portseite wird angezeigt, wenn Sie auf der Seite Port Configuration (Port-Konfiguration) einen Port auswählen, der mit einem Remote-Powerstrip von Raritan verbunden ist. Die Felder **Type** und **Name** sind bereits ausgefüllt. Die folgenden Informationen werden für jeden Ausgang des Powerstrips angezeigt: Ausgangsnummer, Name und Port-Zuordnung.

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

Benennen des Powerstrips (Seite „Port“ für Powerstrips)

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:
Dominion_KX2_101_Port1

Power Association

Power Strip Name	Outlet Name
None	---

Target Server Settings

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)

OK Cancel

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

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

Hinweis: CommandCenter Service Gateway erkennt Powerstrip-Namen mit Leerzeichen nicht.

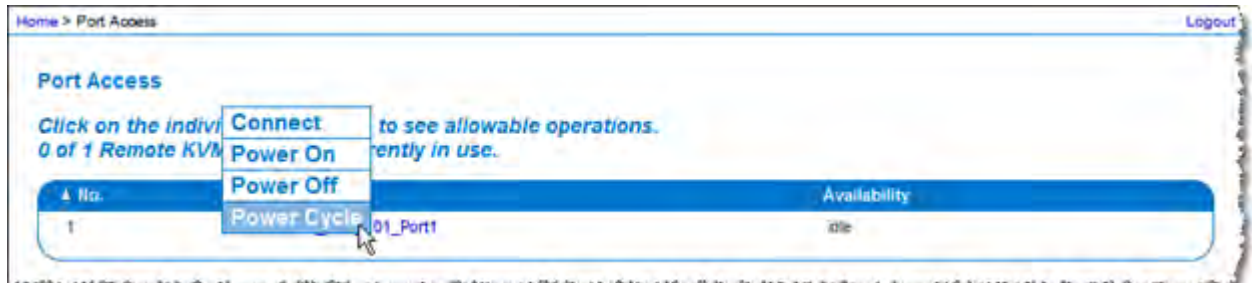
1. Geben Sie dem Powerstrip einen Namen, den Sie sich gut merken können.

2. Ändern Sie ggf. den Namen unter **Outlet Name** (Ausgangsname).
(Der Standardname ist **Outlet #.**)
 3. Klicken Sie auf **OK**.
- *So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
- Klicken Sie auf **Cancel** (Abbrechen).

Zuordnen von KVM-Zielservers zu Ausgängen (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 maximal vier Netzschalter haben, die Sie einem Powerstrip zuordnen können. Auf dieser Seite können Sie diese Zuordnungen definieren, damit Sie auf der 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. Weitere Informationen finden Sie unter **Anschließen des Powerstrips** (auf Seite 152).*

- *So stellen Sie Stromzuordnungen her (ordnen Powerstrip-Ausgänge KVM-Zielservers 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.

Zuordnen von KVM-Zielservern zu Ausgängen (Seite „Port“)

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.
Ein Powerstrip mit zwei Ausgangszuordnungen ist unten dargestellt.

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:
Dominion_KX2_101_Port1

Power Association

Power Strip Name	Outlet Name
Power Port 1 ▼	Dominion_KX2_101_Port1(7) ▼
	Dominion_KX2_101_Port1(8) ▼
	None ▼
	None ▼

Target Server Settings

- 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)

OK Cancel

- *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.
 2. Klicken Sie auf **OK**.

- *So brechen Sie den Vorgang ab, ohne die Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).

- *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.

Anzeigen der Ausgangszuordnungen

➤ 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.

Home > Device Settings > Port Configuration > Port

Port 2

Type:
PowerStrip

Name:

Outlets

Number	Name	Port Association
1	<input type="text" value="Outlet 1"/>	
2	<input type="text" value="Outlet 2"/>	
3	<input type="text" value="Outlet 3"/>	
4	<input type="text" value="Outlet 4"/>	
5	<input type="text" value="Outlet 5"/>	
6	<input type="text" value="Outlet 6"/>	
7	<input type="text" value="Dominion_KX2_101_Port1"/>	Dominion_KX2_101_Port1
8	<input type="text" value="Dominion_KX2_101_Port1"/>	Dominion_KX2_101_Port1

- *So bearbeiten Sie die Konfiguration des Stromzufuhr-Ports:*
 - Benennen Sie den Stromzufuhr-Port im Feld **Port 2 > Name** um.
 - Benennen Sie den Ausgang im Feld **Outlets > Name** (Ausgänge > Name) um. Der Ausgangsname wird auf der Seite **Powerstrip Device** (Powerstrip-Gerät) angezeigt. Weitere Informationen finden Sie unter *Steuern des Powerstrip-Geräts* (auf Seite 159).
 - 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. Weitere Informationen finden Sie unter *Zuordnen von KVM-Zielservern zu Ausgängen* (Seite „**Port**“) (auf Seite 155).

Steuern des Powerstrip-Geräts

Sie können das Powerstrip-Gerät über die Seite **Powerstrip Device** (Powerstrip-Gerät) steuern. Auf dieser Seite können Sie jeden Ausgang des Powerstrips ein- und ausschalten.

Home > Powerstrip

Powerstrip Device

Powerstrip: Power Port 1 - PCR8

Name: Power Port 1 Model: PCR8 Temperature: 41 °C CurrentAmps: 0.6 A MaxAmps: 1.2 A Voltage: 107 V PowerInWatt: 60 W PowerInVA: 60 VA

<p>Outlet 1</p> <p>off</p> <p>1</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>	<p>Outlet 3</p> <p>off</p> <p>3</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>	<p>Outlet 5</p> <p>off</p> <p>5</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>	<p>Outlet 7</p> <p>on</p> <p>7</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>
<p>Outlet 2</p> <p>off</p> <p>2</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>	<p>Outlet 4</p> <p>off</p> <p>4</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>	<p>Outlet 6</p> <p>off</p> <p>6</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>	<p>Outlet 8</p> <p>on</p> <p>8</p> <p><input type="button" value="On"/> <input type="button" value="Off"/></p>

Steuern des Powerstrip-Geräts

➤ *So steuern Sie den mit der KX II-101-Einheit verbundenen Powerstrip:*

1. Wählen Sie **Home > Powerstrip** (Start > Powerstrip).

Die Seite **Powerstrip Device** (Powerstrip-Gerät) wird angezeigt.

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**.

Der Stromanschuss wird ein- oder ausgeschaltet.

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

Kapitel 10 Sicherheitseinstellungen

In diesem Kapitel

Menü „ Security “ (Sicherheit)	161
Security Settings (Sicherheitseinstellungen)	162
IP Access Control (IP-Zugriffssteuerung)	171

Menü „ Security “ (Sicherheit)

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

Option	Aktion
Security Settings (Sicherheitseinstellungen)	Konfigurieren von Sicherheitseinstellungen für Anmeldebeschränkungen, sichere Kennwörter, die Benutzersperrung sowie Verschlüsselung und Freigabe.
IP Access Control (IP-Zugriffssteuerung)	Zugriffssteuerung für Ihre KX II-101-Einheit. Durch das Einrichten einer globalen Zugriffssteuerungsliste stellen Sie sicher, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet.

Security Settings (Sicherheitseinstellungen)

Auf der Seite **Security Settings** (Sicherheitseinstellungen) können Sie Anmeldebeschränkungen angeben, Benutzer sperren, Kennwortregeln festlegen sowie Daten verschlüsseln und freigeben.

Für den Austausch öffentlicher und privater Schlüssel werden SSL-Zertifikate von Raritan verwendet, die zusätzliche Sicherheit bieten. Raritan-Webserverzertifikate sind selbstsigniert, Java-Applet-Zertifikate sind durch ein VeriSign-Zertifikat signiert. Die Verschlüsselung stellt sicher, dass Ihre Informationen nicht in falsche Hände geraten, und anhand dieser Zertifikate sehen Sie, dass es sich um Raritan, Inc. handelt.

➤ *So konfigurieren Sie die Sicherheitseinstellungen:*

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

Home > Security > Security Settings

Login limitations

- Enable Single Login Limitation
- Enable Password Aging
- Password Aging Interval (days):
- Log Out Idle Users
- After (minutes):

Strong passwords

- Enable strong passwords
- Minimum length of strong password:
- Maximum length of strong password:
- 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:

User Blocking

- Disabled
- Timer Lockout
- Attempts:
- Lockout Time:
- Deactivate User-ID
- Failed Attempts:

Encryption & Share

- Encryption Mode:
- Apply Encryption Mode to KVM and Virtual Media
- PC Share Mode:
- VM Share Mode
- Disable Local Port Output
- Local Device Reset Mode:

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

2. Aktualisieren Sie ggf. die Einstellungen unter *Login Limitations (Anmeldebeschränkungen)* (auf Seite 163).
 3. Aktualisieren Sie ggf. die Einstellungen unter *Strong Passwords (Sichere Kennwörter)* (auf Seite 165).
 4. Aktualisieren Sie ggf. die Einstellungen für *User Blocking (Benutzersperrung)* (auf Seite 166).
 5. Aktualisieren Sie ggf. die Einstellungen unter *Encryption & Share (Verschlüsselung und Freigabe)*.
 6. Klicken Sie auf **OK**.
- *So schließen Sie die Seite, ohne Ihre Änderungen zu speichern:*
 - Klicken Sie auf **Cancel** (Abbrechen).
 - *So stellen Sie die Standardwerte wieder her:*
 - Klicken Sie auf **Reset to Defaults** (Standardeinstellungen wiederherstellen).

Login Limitations (Anmeldebeschränkungen)

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

Beschränkung	Beschreibung
Enable Single Login Limitation (Beschränkung auf Einzelanmeldung aktivieren):	Wenn Sie dieses Kontrollkästchen aktivieren, ist pro Benutzername immer nur eine Anmeldung zulässig. Ist es dagegen deaktiviert, kann eine Benutzername-/Kennwortkombination von mehreren Client-Workstations gleichzeitig verwendet werden, um eine Verbindung mit dem Gerät herzustellen.

Security Settings (Sicherheitseinstellungen)

Beschränkung	Beschreibung
<p>Enable Password Aging (Erneuerung des Kennworts aktivieren):</p>	<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>Password Aging Interval (days) (Intervall für Kennworterneuerung [Tage]): Dieses Feld ist aktiv und erforderlich, wenn Sie das Kontrollkästchen Enable Password Aging (Kennworterneuerung aktivieren) aktiviert haben. Geben Sie den Zeitraum in Tagen an, nach dessen Ablauf ein Kennwort geändert werden muss. Der Standardwert ist 60 Tage.</p>
<p>Log Out Idle Users (Inaktive Benutzer abmelden):</p>	<p>Aktivieren Sie dieses Kontrollkästchen, wenn eine Benutzersitzung nach einer bestimmten Inaktivitätsphase automatisch getrennt werden soll. Geben Sie die Zeitspanne im Feld After (Nach) ein. Wenn keine Tastatur- oder Mausaktivitäten stattfinden, werden alle Sitzungen und Ressourcen abgemeldet. Für virtuelle Mediensitzungen gibt es hingegen kein Zeitlimit.</p> <p>After (minutes) (Nach [Minuten]): Die Zeitspanne (in Minuten), nach der ein inaktiver Benutzer abgemeldet wird. Dieses Feld ist aktiv, wenn Sie das Kontrollkästchen Log Out Idle Users (Inaktive Benutzer abmelden) aktiviert haben.</p>

Strong Passwords (Sichere Kennwörter)

Sichere Kennwörter sorgen für eine sicherere lokale Authentifizierung des Systems. Im Bereich **Strong Passwords** (Sichere Kennwörter) können Sie Kriterien für das Format gültiger lokaler KX II-101-Kennwörter wie Mindest- und Höchstlänge, erforderliche Zeichen und Aufbewahrung des Kennwortverlaufs festlegen.

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

- **Enable strong passwords** (Sichere Kennwörter aktivieren): Damit ein Kennwort sicher ist, muss es eine Mindestlänge von acht Zeichen sowie mindestens ein alphabetisches Zeichen und ein nicht-alphabetisches Zeichen (Satzzeichen oder Ziffer) haben. Darüber hinaus dürfen die ersten vier Zeichen des Kennworts und des Benutzernamens nicht identisch sein. Wenn Sie dieses Kontrollkästchen aktivieren, gelten die Regeln für sichere Kennwörter. Benutzer, deren Kennwörter nicht den Kriterien für sichere Kennwörter entsprechen, werden bei der nächsten Anmeldung automatisch aufgefordert, ihr Kennwort zu ändern. Ist das Kontrollkästchen deaktiviert, gilt nur die Standardformatvalidierung. Bei aktiviertem Kontrollkästchen sind die folgenden Felder aktiv und erforderlich:
 - **Minimum length of strong password** (Mindestlänge des sicheren Kennworts): Kennwörter müssen mindestens 8 Zeichen umfassen. Es dürfen aber bis zu 63 Zeichen sein.
 - **Maximum length of strong password** (Höchstlänge des sicheren Kennworts): Die Standardlänge liegt bei 16 Zeichen, es dürfen aber bis zu 64 Zeichen sein.

Security Settings (Sicherheitseinstellungen)

- **Enforce at least one lower case character** (Mindestens einen Kleinbuchstaben erzwingen): Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Kleinbuchstaben enthalten.
- **Enforce at least one upper case character** (Mindestens einen Großbuchstaben erzwingen): Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens einen Großbuchstaben enthalten.
- **Enforce at least one numeric character** (Mindestens eine Ziffer erzwingen): Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens eine Ziffer enthalten.
- **Enforce at least one printable special character** (Mindestens ein druckbares Sonderzeichen erzwingen): Wenn dieses Kontrollkästchen aktiviert ist, muss das Kennwort mindestens ein (druckbares) Sonderzeichen enthalten.
- **Number of restricted passwords based on history** (Anzahl unzulässiger Kennwörter basierend auf Verlauf): Dieses Feld gibt an, wie weit der Kennwortverlauf zurückreicht, d. h. die Anzahl früherer Kennwörter, die nicht wiederholt werden dürfen. Ein Bereich zwischen 1 und 12 ist möglich, der Standardwert liegt bei 5.

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.

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

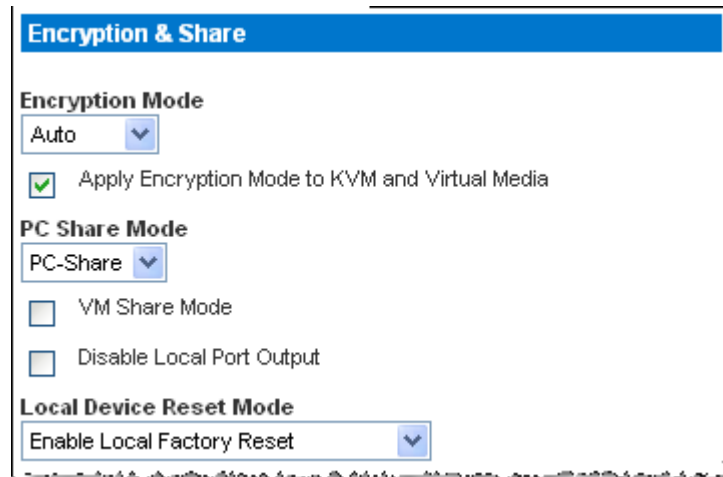
- **Deactivate User-ID** (Benutzer-ID deaktivieren): Diese Option legt fest, dass dem Benutzer nach der Anzahl der im Feld **Failed Attempts** (Fehlversuche) angegebenen Anmeldefehlversuche der Zugriff auf das System verweigert wird.
 - **Failed Attempts** (Fehlversuche): Geben Sie die Anzahl der Anmeldefehlversuche ein, nach der die Benutzer-ID eines Benutzers deaktiviert wird. Dieses Feld steht zur Verfügung, wenn Sie die Option **Deactivate User-ID** (Benutzer-ID deaktivieren) wählen. Der gültige Bereich liegt zwischen 1 und 10.

The screenshot shows a configuration window titled "User Blocking". It has two radio buttons: "Disabled" and "Timer Lockout". Below these are two input fields: "Attempts" with the value "3" and "Lockout Time" with the value "5". The "Deactivate User-ID" radio button is selected. Below it is another input field: "Failed Attempts" with the value "3".

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)** (siehe "Add New User (Neuen Benutzer hinzufügen)" auf Seite 54) das Kontrollkästchen **Active** (Aktiv) aktiviert.

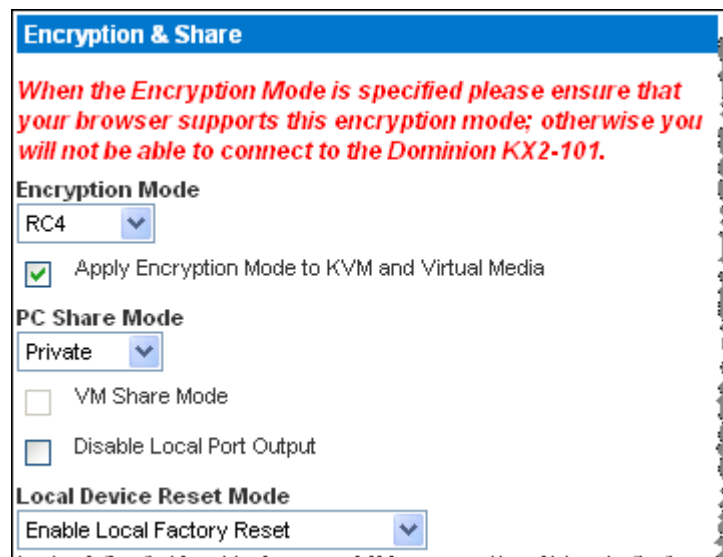
Encryption & Share (Verschlüsselung und Freigabe)

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 Reset-Taste an der KX II-101-Einheit gedrückt wird.



The screenshot shows the 'Encryption & Share' configuration page. The 'Encryption Mode' dropdown is set to 'Auto'. The checkbox 'Apply Encryption Mode to KVM and Virtual Media' is checked. Under 'PC Share Mode', the dropdown is set to 'PC-Share', and the checkboxes for 'VM Share Mode' and 'Disable Local Port Output' are unchecked. Under 'Local Device Reset Mode', the dropdown is set to 'Enable Local Factory Reset'.

- **Encryption Mode** (Verschlüsselungsmodus): Wählen Sie eine Option aus der Dropdown-Liste. Wenn Sie einen Verschlüsselungsmodus ausgewählt haben, wird eine Warnung angezeigt, dass Sie keine Verbindung zur KX II-101-Einheit mehr herstellen können, falls Ihr Browser den gewählten Modus nicht unterstützt.



The screenshot shows the 'Encryption & Share' configuration page with a warning message in red text: *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 Dominion KX2-101.* The 'Encryption Mode' dropdown is set to 'RC4'. The checkbox 'Apply Encryption Mode to KVM and Virtual Media' is checked. Under 'PC Share Mode', the dropdown is set to 'Private', and the checkboxes for 'VM Share Mode' and 'Disable Local Port Output' are unchecked. Under 'Local Device Reset Mode', the dropdown is set to 'Enable Local Factory Reset'.

- **Auto** (Automatisch): Diese Option wird empfohlen. KX II-101 handelt die höchstmögliche Verschlüsselungsebene automatisch aus.
- **RC4**: Sichert Benutzernamen, Kennwörter und KVM-Daten einschließlich Videoübertragungen mithilfe der Verschlüsselungsmethode RSA RC4. Dies ist ein 128-Bit-SSL-Protokoll (Secure Sockets Layer), das während der Anfangsverbindungsauthentifizierung einen privaten Kommunikations-Channel zwischen der KX II-101-Einheit und dem Remote-PC bereitstellt.
- **AES-128**: Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology für die Verschlüsselung elektronischer Daten mit einer Schlüssellänge von 128 Bit. Achten Sie bei Auswahl dieser Option darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter *Prüfen Ihres Browsers auf AES-Verschlüsselung* (auf Seite 171).
- **AES-256**: Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology für die Verschlüsselung elektronischer Daten mit einer Schlüssellänge von 256 Bit. Achten Sie bei Auswahl dieser Option darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter *Prüfen Ihres Browsers auf AES-Verschlüsselung* (auf Seite 171).
- **Apply Encryption Mode to KVM and Virtual Media** (Verschlüsselungsmodus auf KVM und virtuelle Medien anwenden): Wenn Sie dieses Kontrollkästchen aktivieren, wird der gewählte Verschlüsselungsmodus auf KVM und virtuelle Medien angewendet. Nach der Authentifizierung werden die KVM- und virtuellen Mediendaten ebenfalls mit der 128-Bit-Verschlüsselung übertragen.
- **PC Share Mode** (PC-Freigabemodus): Bestimmt den globalen gleichzeitigen KVM-Remote-Zugriff und ermöglicht bis zu acht Remote-Benutzern die gleichzeitige Anmeldung bei einer KX II-101-Einheit sowie die gleichzeitige Anzeige und Steuerung desselben Zielservers über das Gerät. Klicken Sie auf die Dropdown-Liste, um eine der folgenden Optionen auszuwählen:
 - **Private** (Privat): Keine PC-Freigabe; dies ist der Standardmodus. Jeder Zielservier ist jeweils nur für einen Benutzer exklusiv zugänglich.

Security Settings (Sicherheitseinstellungen)

- **PC-Share** (PC-Freigabe): Bis zu acht Benutzer (Administratoren oder Nicht-Administratoren) können gleichzeitig auf KVM-Zielserver zugreifen. Jeder Remote-Benutzer besitzt dieselbe Kontrolle über Tastatur und Maus. Beachten Sie jedoch, dass eine ungleichmäßige Steuerung auftritt, wenn ein Benutzer seine Tastatur- bzw. Mauseingabe nicht unterbricht.
- **VM Share Mode** (VM-Freigabemodus): Diese Option steht nur zur Verfügung, wenn Sie den PC-Freigabemodus aktiviert haben. Wenn dieses Kontrollkästchen aktiviert ist, werden virtuelle Medien für mehrere Benutzer freigegeben, d. h. diese können gemeinsam auf dieselbe virtuelle Mediensitzung zugreifen. Standardmäßig ist dieses Kontrollkästchen deaktiviert.
- **Local Device Reset Mode** (Modus zum Zurücksetzen eines lokalen Geräts): Diese Option legt fest, welche Maßnahmen ergriffen werden, wenn die Reset-Taste auf der Rückseite des Geräts gedrückt wird. Weitere Informationen finden Sie unter Reset-Taste. Wählen Sie eine der folgenden Optionen:
 - **Enable Local Factory Reset** (Lokale Rücksetzung auf die Werkseinstellungen aktivieren) (Standardeinstellung): Setzt die KX II-101-Einheit auf die werksseitigen Standardeinstellungen zurück.
 - **Enable Local Admin Password Reset** (Lokale Administratorkennwortrücksetzung aktivieren): Setzt nur das Kennwort des lokalen Administrators zurück. Das Kennwort wird auf **raritan** zurückgesetzt.
 - **Disable All Local Resets** (Alle lokalen Rücksetzungen deaktivieren): Es wird keine Rücksetzungsmaßnahme ergriffen.

Prüfen Ihres Browsers auf AES-Verschlüsselung

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

Hinweis: Die AES-128-Bit- oder -256-Bit-Verschlüsselung wird von 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 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

Für die AES-256-But-Verschlüsselung müssen außerdem die Sicherheitsrichtliniendateien für eine unbeschränkte Schlüssellänge der Java Cryptography Extension (JCE) installiert werden.

Diese so genannten „Unlimited Strength Jurisdiction Policy Files“ der verschiedenen JRE-Versionen finden Sie unter folgenden Links im Bereich **Other Downloads** (Weitere Downloads):

- JRE 1.4.2 - <http://java.sun.com/j2se/1.4.2/download.html>
- JRE 1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

IP Access Control (IP-Zugriffssteuerung)

Mithilfe der IP-Zugriffssteuerung können Sie den Zugriff auf die KX II-101-Einheit kontrollieren. Durch das Einrichten einer globalen Zugriffssteuerungsliste (Access Control List, ACL) stellen Sie sicher, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet. Die IP-Zugriffssteuerung funktioniert global und betrifft die gesamte KX II-101-Einheit. Sie können den Zugriff auf die Einheit jedoch auch auf Gruppenebene steuern. Weitere Informationen zur Steuerung auf Gruppenebene finden Sie unter Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste).

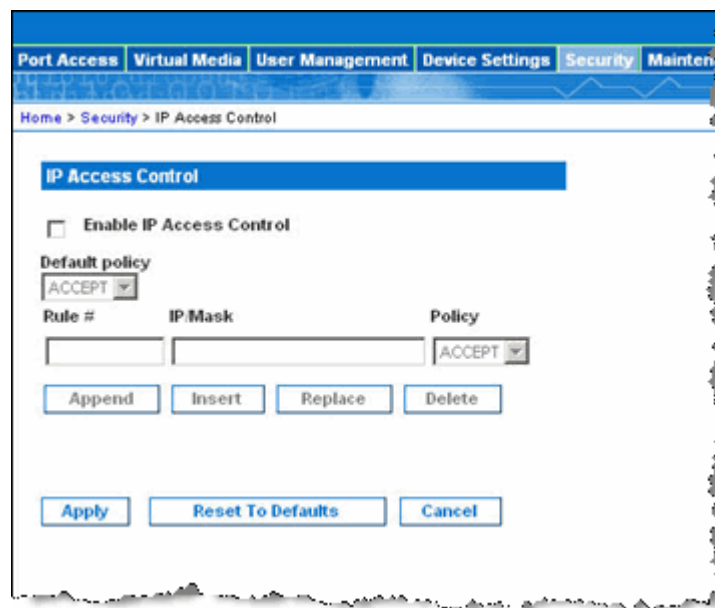
Wichtig: Die IP-Adresse 127.0.0.1 wird vom lokalen Port der KX II-101-Einheit verwendet. Wenn sich 127.0.0.1 beim Erstellen der

IP-Zugriffssteuerungsliste im Bereich der gesperrten IP-Adressen befindet, können Sie nicht auf den lokalen Port der KX II-101-Einheit zugreifen.

➤ *So verwenden Sie die IP-Zugriffssteuerung:*

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

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



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** (Zulassen): Diese IP-Adressen können auf das KX II-101-Gerät zugreifen.
 - **Drop** (Ablehnen): Diesen IP-Adressen wird der Zugriff auf das KX II-101-Gerät verweigert.

➤ *So fügen Sie Regeln hinzu:*

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

➤ *So fügen Sie eine Regel ein:*

1. Geben Sie im Feld **Rule #** eine Regelnummer ein. Diese ist für den Befehl **Insert** (Einfügen) erforderlich.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld **IP/Mask** (IP/Maske) ein.
3. Wählen Sie in der Dropdown-Liste **Policy** eine Richtlinie aus.
4. Klicken Sie auf **Insert** (Einfügen). Wenn die eingegebene Regelnummer einer bereits vorhandenen entspricht, wird die neue Regel vor der vorhandenen Regel eingefügt, und alle Regeln werden um eine Position nach unten verschoben.

➤ *So ersetzen Sie eine Regel:*

1. Geben Sie im Feld **Rule #** die Nummer der zu ersetzenden Regel ein.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld **IP/Mask** (IP/Maske) ein.
3. Wählen Sie in der Dropdown-Liste **Policy** eine Richtlinie aus.
4. Klicken Sie auf **Replace** (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

➤ *So löschen Sie eine Regel:*

1. Geben Sie im Feld **Rule #** die Nummer der zu löschenden Regel ein.
2. Klicken Sie auf **Delete** (Löschen).
3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **OK**.

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

Kapitel 11 Wartung

In diesem Kapitel

Menü Maintenance (Wartung).....	174
Audit Log (Prüfprotokoll)	175
Device Information (Geräteinformationen)	177
Backup/Restore (Sicherung/Wiederherstellung)	178
Firmware Upgrade (Firmware-Aktualisierung).....	180
Upgrade History (Aktualisierungsverlauf).....	183
Reboot (Neustart).....	183

Menü Maintenance (Wartung)

Das Menü Maintenance (Wartung) enthält folgende Optionen: Audit Log (Prüfprotokoll), Device Information (Geräteinformationen), Backup/Restore (Sicherung/Wiederherstellung), Firmware Upgrade (Firmware-Aktualisierung), Factory Reset (Wiederherstellen der werksseitigen Standardeinstellungen), Upgrade History (Aktualisierungsverlauf) und Reboot (Neustart).

Audit Log (Prüfprotokoll)

Alle KX II-101-Systemereignisse werden protokolliert.

➤ *So zeigen Sie das Prüfprotokoll für Ihre KX II-101-Einheit an:*

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

Home > Maintenance > Audit Log Logout

Audit Log

[Older]

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

[Save To File](#)

Audit Log (Prüfprotokoll)

Die Seite **Audit Log** (Prüfprotokoll) enthält Ereignisse sortiert nach Datum und Uhrzeit, wobei die letzten Ereignisse zuerst aufgeführt werden. Das Prüfprotokoll enthält die folgenden Informationen:

- **Date** (Datum): Datum und Uhrzeit des Ereignisses im 24-h-Zeitformat.
- **Event** (Ereignis): Der Ereignisname, wie er auf der Seite **Event Management** (Ereignisverwaltung) aufgeführt wird.
- **Description** (Beschreibung): Detaillierte Beschreibung des Ereignisses.

➤ *So speichern Sie das Prüfprotokoll:*

Hinweis: Sie können das Prüfprotokoll nur mithilfe der KX II-101-Remote-Konsole speichern, nicht jedoch mit der lokalen Konsole.

1. Klicken Sie auf die Schaltfläche **Save to File** (Speichern unter). Das Dialogfeld **Save File** (Datei speichern) wird angezeigt.
2. Wählen Sie einen Dateinamen und Speicherort aus, und klicken Sie auf **Save** (Speichern). Das Prüfprotokoll wird mit dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.

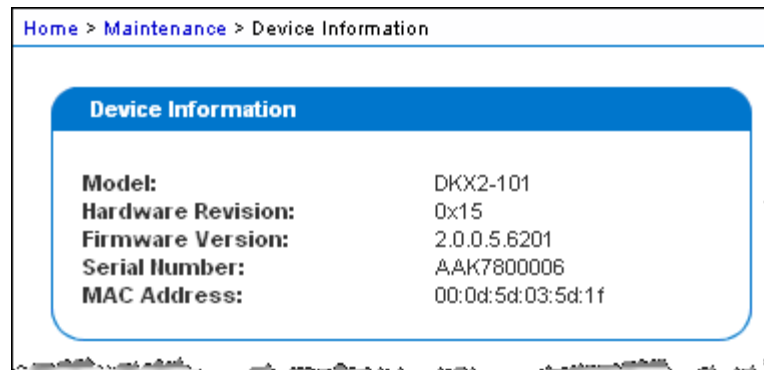
➤ *So blättern Sie durch das Prüfprotokoll:*

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

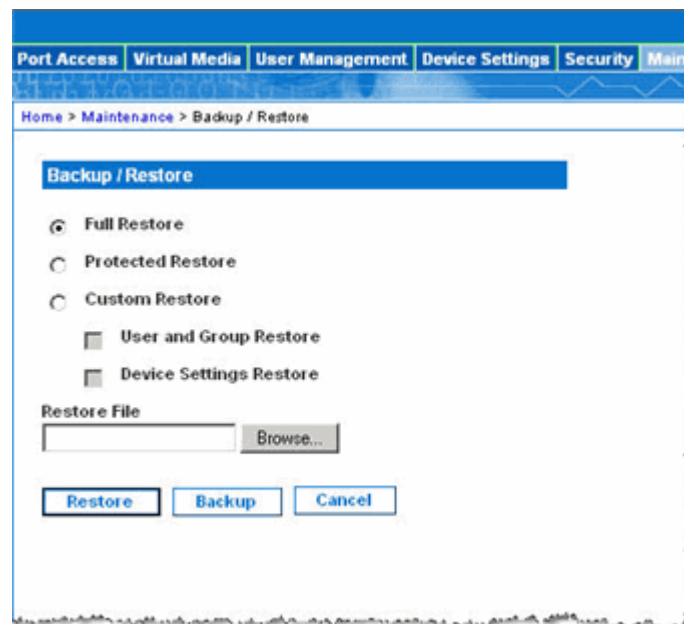


Zu der KX II-101-Einheit werden folgende Informationen angezeigt: Modell, Hardware-Version, Firmware-Version, Seriennummer und MAC-Adresse.

Backup/Restore (Sicherung/Wiederherstellung)

Auf der Seite **Backup/Restore** (Sicherung/Wiederherstellung) können Sie die Einstellungen und die Konfiguration der KX II-101-Einheit sichern und wiederherstellen. Dieses Feature dient nicht nur der Gewährleistung der Geschäftskontinuität, sondern Sie können damit auch viel Zeit sparen. Sie können Sie Ihrem Team beispielsweise schnell von einem anderer KX II-101-Einheit Zugriff gewähren, indem Sie die Benutzerkonfigurationseinstellungen des verwendeten KX II-101-Geräts sichern und auf dem neuen KX II-101-Gerät wiederherstellen. Sie können auch eine KX II-101-Einheit einrichten und deren Konfiguration auf mehrere andere KX II-101-Geräte kopieren.

- *So greifen Sie auf die Seite „Backup/Restore“ (Sicherung/Wiederherstellung) zu:*
 - Wählen Sie **Maintenance > Backup/Restore** (Wartung > Sicherung/Wiederherstellung). Die Seite **Backup/Restore** (Sicherung/Wiederherstellung) wird angezeigt.



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

➤ *So sichern Sie die KX II-101-Einheit:*

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

➤ *So stellen Sie die KX II-101-Einheit wieder her:*

WARNUNG: Gehen Sie bei der Wiederherstellung Ihrer KX II-101-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-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. Diese Option wird üblicherweise für die herkömmliche Sicherung und Wiederherstellung verwendet.
 - **Protected Restore** (Geschützte Wiederherstellung): Alle Daten mit Ausnahme von gerätespezifischen Informationen wie Seriennummer, MAC-Adresse, IP-Adresse, Name usw. werden wiederhergestellt. Mithilfe dieser Option können Sie eine KX II-101-Einheit einrichten und die Konfiguration auf mehrere andere KX II-101-Geräte kopieren.

Firmware Upgrade (Firmware-Aktualisierung)

- **Custom Restore** (Benutzerdefinierte Wiederherstellung): Unter dieser Option stehen die Kontrollkästchen **User and Group Restore** (Wiederherstellung von Benutzern und Gruppen) und **Device Settings Restore** (Wiederherstellung der Geräteeinstellungen) zur Verfügung. Aktivieren Sie die gewünschten Kontrollkästchen:
 - **User and Group Restore** (Wiederherstellung von Benutzern und Gruppen): Diese Option umfasst nur Benutzer- und Gruppeninformationen. Verwenden Sie sie, um schnell Benutzer auf einem anderen KX II-101-Gerät einzurichten.
 - **Device Settings Restore** (Wiederherstellung der Geräteeinstellungen): Diese Option umfasst nur die Geräteeinstellungen. Verwenden Sie sie, um schnell die Geräteinformationen zu kopieren.
- 2. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen). Das Dialogfeld **Choose file** (Datei auswählen) wird angezeigt.
- 3. Navigieren Sie zur gewünschten Sicherungsdatei, markieren Sie sie, und klicken Sie auf **Open** (Öffnen). Die ausgewählte Datei wird im Feld **Restore File** (Datei wiederherstellen) aufgeführt.
- 4. Klicken Sie auf **Restore** (Wiederherstellen). Die Konfiguration wird basierend auf der gewählten Wiederherstellungsart wiederhergestellt.

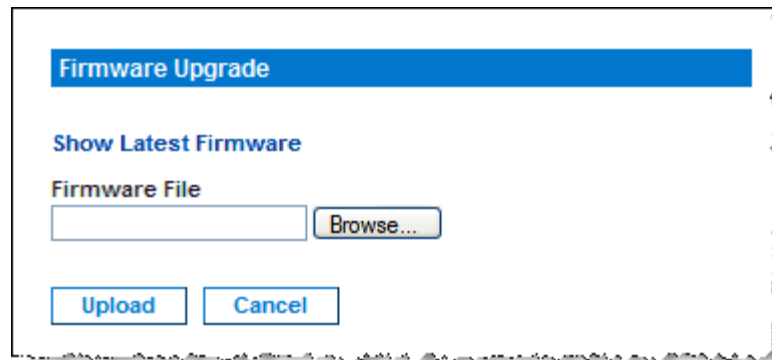
Firmware Upgrade (Firmware-Aktualisierung)

Auf der Seite **Firmware Upgrade** (Firmware-Aaktualisierung) können Sie die Firmware Ihrer KX II-101-Einheit aktualisieren. Diese Seite ist nur in der KX II-101-Remote-Konsole verfügbar.

Wichtig: Schalten Sie während der Aktualisierung die KX II-101-Einheit nicht aus, da dies zu Schäden an der Einheit führen könnte.

➤ *So aktualisieren Sie die KX II-101-Einheit:*

1. Wählen Sie **Maintenance > Firmware Upgrade** (Wartung > Firmware-Aktualisierung). Die Seite **Firmware Upgrade** (Firmware-Aktualisierung) wird angezeigt.

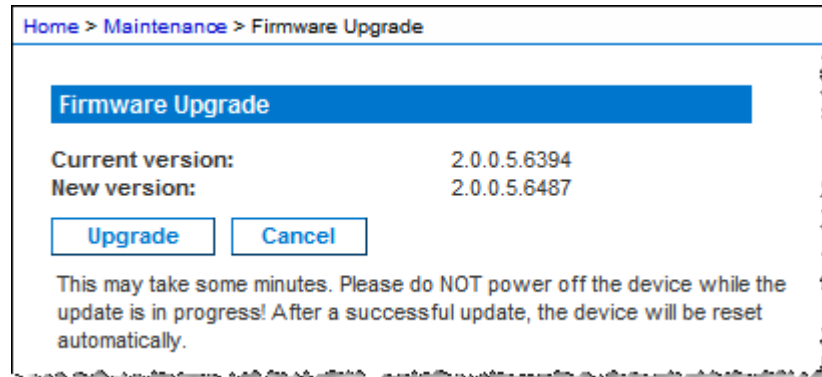


2. Klicken Sie auf die Verknüpfung **Show Latest Firmware** (Aktuelle Firmware anzeigen), navigieren Sie zur entsprechenden Raritan-Firmware-Distributiondatei (*.RFP) auf der Seite **Firmware Upgrades > KX II-101** (Firmware-Aktualisierungen > KX II-101), und laden Sie die Datei herunter.
3. Entpacken 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.

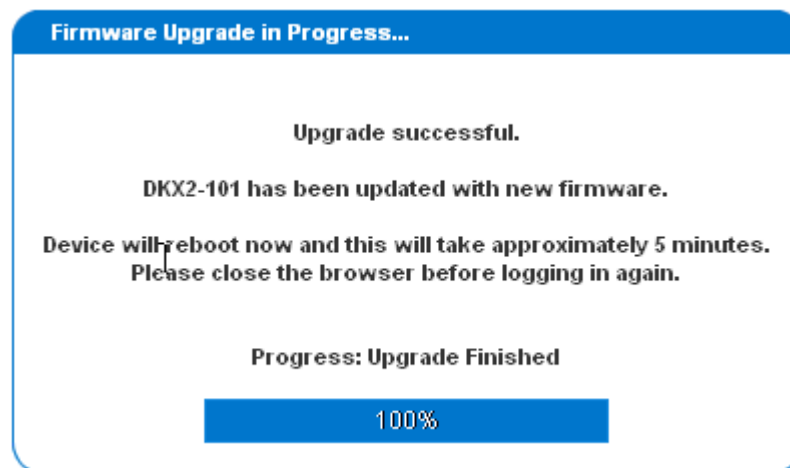
Firmware Upgrade (Firmware-Aktualisierung)

4. Klicken Sie auf der Seite **Firmware Upgrade** (Firmware-Aktualisierung) auf **Upload** (Hochladen). Zur Bestätigung werden Informationen zur Aktualisierung und Versionsnummer 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 die Einheit neu gestartet.



6. Schließen Sie den Browser, wenn Sie dazu aufgefordert werden, und warten Sie ungefähr fünf Minuten, bevor Sie sich erneut bei der KX II-101-Einheit anmelden.

Weitere Informationen zur Aktualisierung der Geräte-Firmware mithilfe des Multi-Platform-Clients finden Sie im Benutzerhandbuch zum Multi-Platform-Client (MPC) von Raritan.

Upgrade History (Aktualisierungsverlauf)

KX II-101 liefert Informationen über die Aktualisierungen, die auf der KX II-101-Einheit und den angeschlossenen CIMs durchgeführt wurden.

- *So zeigen Sie den Aktualisierungsverlauf an:*
 - Wählen Sie **Maintenance > Upgrade History** (Wartung > Aktualisierungsverlauf). Die Seite **Upgrade History** (Aktualisierungsverlauf) wird angezeigt.

Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:30	January 09, 2000 20:32	2.0.0.5.6236	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:18	January 09, 2000 20:20	2.0.0.5.6191	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.65	January 06, 2000 17:58	January 06, 2000 18:01	2.0.0.1.6126	2.0.0.5.6191	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 2000 00:02	January 01, 2000 00:04	99.99.99.2.9999	2.0.0.1.6126	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 1970 00:06	January 01, 1970 00:09	2.0.0.1.5974	99.99.99.2.9999	Successful
Full Firmware Upgrade						2.0.0.1.5974	Failed

Reboot (Neustart)

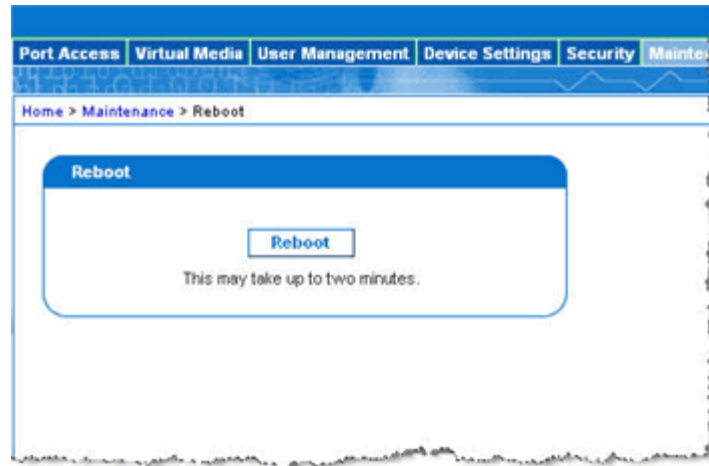
Auf der Seite **Reboot** (Neustart) können Sie die KX II-101-Einheit sicher und kontrolliert neu starten. Dieses Neustartverfahren wird empfohlen.

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

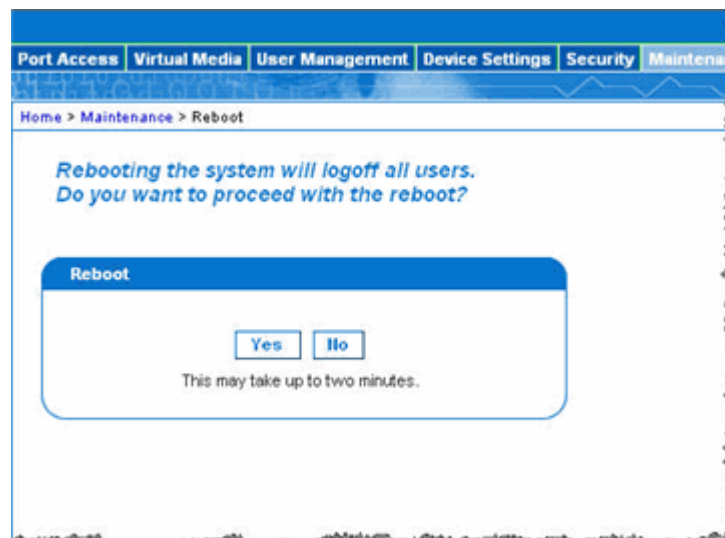
Reboot (Neustart)

➤ *So starten Sie die KX II-101-Einheit neu:*

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



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



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

➤ *So verlassen Sie die Seite, ohne einen Neustart durchzuführen:*

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

Kapitel 12 Befehlszeilenschnittstelle (CLI)

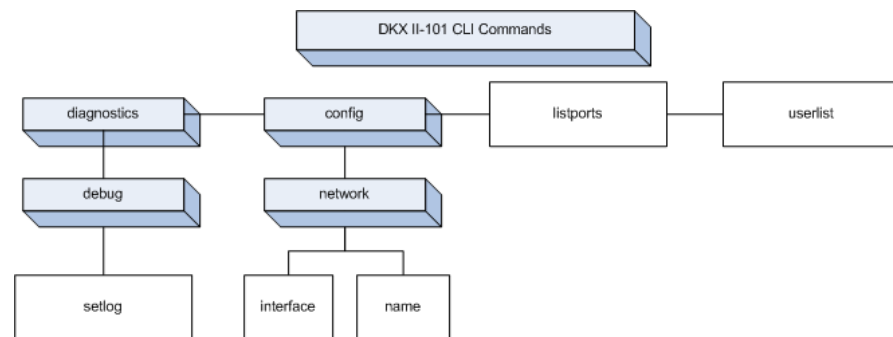
In diesem Kapitel

Überblick.....	185
Zugriff auf KX II-101 über die Befehlszeilenschnittstelle.....	186
SSH-Verbindung mit der KX II-101-Einheit.....	186
Anmelden	187
Navigation in der Befehlszeilenschnittstelle.....	188
Befehle der Befehlszeilenschnittstelle	190

Überblick

Dieses Kapitel enthält eine Übersicht über die Befehle der Befehlszeilenschnittstelle (CLI), die mit KX II-101 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 190).

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 über die Befehlszeilenschnittstelle

Verwenden Sie eine der folgenden Methoden, um auf die KX II-101-Einheit 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

Verschiedene 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>)
- Applet SSH Client - www.netspace.org/ssh (<http://www.netspace.org/ssh>)
- OpenSSH Client - 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-Remote-Clients einrichten. Weitere Informationen finden Sie unter **Device Services (Gerätedienste)** (auf Seite 134).*

SSH-Verbindung mit der KX II-101-Einheit

Verwenden Sie zur Verbindung einen SSH-Client, der SSH V2 unterstützt. Sie müssen den SSH-Zugriff auf der Seite **Devices Services** (Gerätedienste) aktivieren. Weitere Informationen finden Sie unter **Device Services (Gerätedienste)** (auf Seite 134).

Hinweis: Aus Sicherheitsgründen werden SSH-V1-Verbindungen von KX II-101 nicht unterstützt.

SSH-Zugriff über einen Windows-PC

➤ *So öffnen Sie eine SSH-Sitzung über einen Windows-PC:*

1. Starten Sie eine SSH-Client-Software, wie z. B. PuTTY.
2. Geben Sie die IP-Adresse des KX II-101-Servers ein: 192.168.0.192.
3. Wählen Sie SSH (der standardmäßige Konfigurations-Port lautet 22).
4. Klicken Sie auf die Schaltfläche **Open** (Öffnen).

5. Folgende Eingabeaufforderung wird angezeigt:

login as: (Anmelden als:)

Die Anmeldeinformationen finden Sie unter Anmelden.

SSH-Zugriff über eine UNIX-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.

Die Anmeldeinformationen finden Sie unter Anmelden.

Anmelden

- Geben Sie zum Anmelden den Benutzernamen „admin“ wie gezeigt ein:

Login: admin

Die Eingabeaufforderung für das Kennwort wird angezeigt. Geben Sie das Standardkennwort raritan ein.

Password:

Der Begrüßungsbildschirm wird angezeigt. Sie sind jetzt als Administrator angemeldet.

```

Login: admin
Password:

-----
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC         FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153        Idle Timeout: 30min
-----

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

Current Time: Wed Dec 26 14:37:00 2007

Admin Port > _
    
```

Lesen Sie den folgenden Abschnitt *Navigation in der Befehlszeilenschnittstelle* (siehe "Navigation in der Befehlszeilenschnittstelle" auf Seite 188), und führen Sie dann die anfänglichen Konfigurationsaufgaben unter *Verwenden eines Terminalemulationsprogramms* (auf Seite 30) durch.

Navigation in der Befehlszeilenschnittstelle

Vor der Verwendung der Befehlszeilenschnittstelle sollten Sie sich mit der Navigation und Syntax in der Befehlszeilenschnittstelle vertraut machen. Außerdem gibt es einige Tastenkombinationen, mit denen die Verwendung der Befehlszeilenschnittstelle vereinfacht wird.

Eingabeaufforderungen der Befehlszeilenschnittstelle

Die Eingabeaufforderung der Befehlszeilenschnittstelle zeigt die aktuelle Befehlsebene an. Die Stammebene der Eingabeaufforderung ist der Anmeldename. Bei einer direkten Verbindung mit dem seriellen Port „Admin“ mit einem Terminalemulationsprogramm ist **Admin Port** die Stammebene eines Befehls:

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

Bei TELNET/SSH ist **admin** die Stammebene des Befehls:

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

Vervollständigen der Befehle

Die Befehlszeilenschnittstelle unterstützt das Vervollständigen teilweise eingegebener Befehle. Drücken Sie nach Eingabe der ersten Zeichen die **Tab**-Taste. Führen die Zeichen zu einer eindeutigen Übereinstimmung, vervollständigt die Befehlszeilenschnittstelle den Eintrag.

- Wird keine Übereinstimmung gefunden, zeigt die Befehlszeilenschnittstelle die gültigen Einträge für die Ebene an.
- Werden mehr als eine mögliche Übereinstimmung gefunden, zeigt die Befehlszeilenschnittstelle die gültigen Einträge an.
- Geben Sie weiteren Text ein, damit eine eindeutige Übereinstimmung gefunden werden kann, und vervollständigen Sie den Eintrag mithilfe der **Tab**-Taste.

Syntax der Befehlszeilenschnittstelle - 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.
- Die Eingabe eines Fragezeichens (?) nach einem Befehl zeigt die Hilfe für den Befehl an.
- Ein vertikaler 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 **Tab**-Taste, 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	Wechsel zur höchsten Ebene der Hierarchie der Befehlszeilenschnittstelle oder der Eingabeaufforderung „username“.
history	Zeigt die letzten 200 Befehle an, die der Benutzer in die Befehlszeilenschnittstelle von KX II-101 eingegeben hat.

Befehle der Befehlszeilenschnittstelle

Befehl	Beschreibung
help	Zeigt eine Übersicht der Syntax der Befehlszeilenschnittstelle an.
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).
<i>diagnostics</i> (siehe "Diagnostics (Diagnose)" auf Seite 191)	Wechsel zum Menü Diagnostics (Diagnose).
<i>debug</i> (auf Seite 191)	Wechsel zum Menü Debug .
help	Anzeigen einer Übersicht der Syntax der Befehlszeilenschnittstelle.
history	Anzeigen des Befehlszeilenverlaufs der aktuellen Sitzung.
interface	Konfigurieren der Netzwerkschnittstelle von KX II-101.
<i>listports</i> (siehe "Befehl „ listports “" auf Seite 194)	Auflistung von Port, Port-Name, Port-Typ, Port-Status und Port-Verfügbarkeit.
logout	Abmelden von der aktuellen Sitzung der Befehlszeilenschnittstelle.
<i>name</i> (siehe "Befehl „ name “" auf Seite 193)	Festlegen des Gerätenamens.
<i>network</i> (siehe "Network (Netzwerk)" auf Seite 192)	Anzeigen der Netzwerkkonfiguration und Möglichkeit, die Netzwerkeinstellungen zu konfigurieren.
quit	Rückkehr zum vorherigen Befehl.

<i>setlog</i> (siehe "Befehl „ Setlog ““ auf Seite 191)	Festlegen der Protokollierungsoptionen für das Gerät.
top	Rückkehr zum Stammmenü.
<i>userlist</i> (siehe "Befehl „ Userlist ““ auf Seite 194)	Auflistung der Anzahl der aktiven Benutzer, Benutzernamen, Port und Status.

Diagnostics (Diagnose)

Im Menü **Diagnostics** (Diagnose) können Sie die Protokollierungsoptionen für die verschiedenen Module von KX II-101 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 festzulegen.

Befehl „ Setlog “

Mit dem Befehl **Setlog** können Sie die Protokollierungsebene für verschiedene Module von KX II-101 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.

Befehle der Befehlszeilenschnittstelle

Befehloption	Beschreibung
module	Modulname
level	Diagnoseebene: err warn info debug trace
vflag	Art des Verbose-Flag: timestamp module thread fileline
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 verwendet.

Befehl	Beschreibung
interface	Konfigurieren der Netzwerkschnittstelle der KX II-101-Einheit.

name	Festlegen des Gerätenamens.
------	-----------------------------

Befehl „ name “

Der Befehl **name** wird zur Konfiguration des Geräte- und Hostnamens verwendet.

Verwenden Sie folgende Syntax für den Gerätenamen:

```
name devicename <>
```

Verwenden Sie folgende Syntax für den Hostnamen:

```
name hostname <>
```

Beispiel für den Befehl „name“

Folgender Befehl legt den Gerätenamen fest:

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

Folgender Befehl legt den Hostnamen fest:

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

Befehl „ interface “

Der Befehl **interface** wird zur Konfiguration der Netzwerkschnittstelle von KX II-101 verwendet. Wird der Befehl angenommen, trennt die Einheit 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. Weitere Informationen finden Sie unter *Installation und Konfiguration* (auf Seite 8).

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.

Befehloption	Beschreibung
ipauto	Statische oder dynamische IP-Adresse.
ip ipaddress	IP-Adresse der KX II-101-Einheit, die für den Zugriff über das IP-Netzwerk zugewiesen wurde.

Befehle der Befehlszeilenschnittstelle

Befehloption	Beschreibung
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 „ 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_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 13 Diagnose

In diesem Kapitel

Menü „Diagnostics“ (Diagnose).....	195
Network Interface (Netzwerkschnittstelle).....	196
Network Statistics (Netzwerkstatistik).....	197
Ping Host (Ping an den Host).....	199
Trace Route to Host (Route zum Host zurückverfolgen).....	200
Device Diagnostics (Gerätediagnose).....	201

Menü „Diagnostics“ (Diagnose)

Auf den Diagnoseseiten können Sie Probleme behandeln. Sie sind hauptsächlich für den Administrator des KX II-101-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.

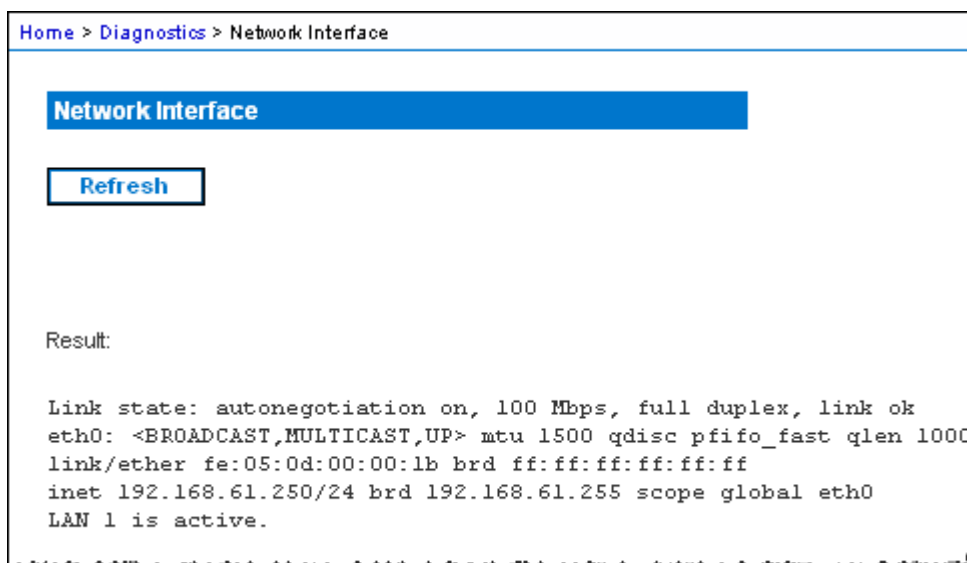
Folgende Optionen stehen zur Verfügung:

Option	Aktion
Network Interface (Netzwerkschnittstelle)	Abrufen des Status der Netzwerkschnittstelle
Network Statistics (Netzwerkstatistik)	Abrufen von Statistiken über das Netzwerk
Ping Host (Ping an den Host)	Ermitteln, ob ein bestimmter Host über ein IP-Netzwerk erreichbar ist
Trace Route to Host (Route zum Host zurückverfolgen)	Ermitteln der Route bis zum gewählten Host
Device Diagnostics (Gerätediagnose)	Verwendung nur nach Anweisung durch den technischen Kundendienst von Raritan (nur Remote-Konsole)

Network Interface (Netzwerkschnittstelle)

KX II-101 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.



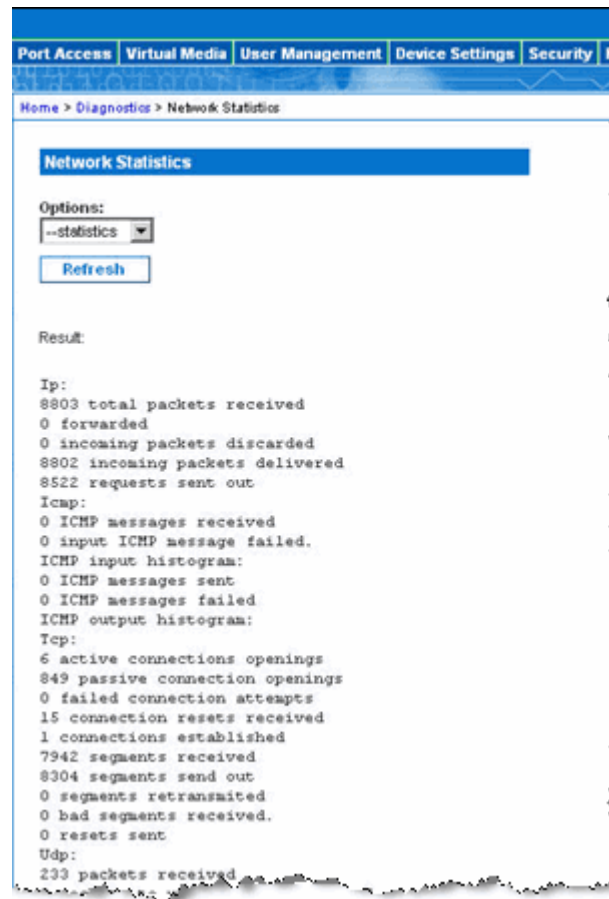
Diese Seite enthält die folgenden Informationen:

- Funktionsfähigkeit der Ethernet-Schnittstelle
 - Erreichbarkeit des Gateways
 - Derzeit aktiver LAN-Port
- *So aktualisieren Sie diese Informationen:*
- Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Network Statistics (Netzwerkstatistik)

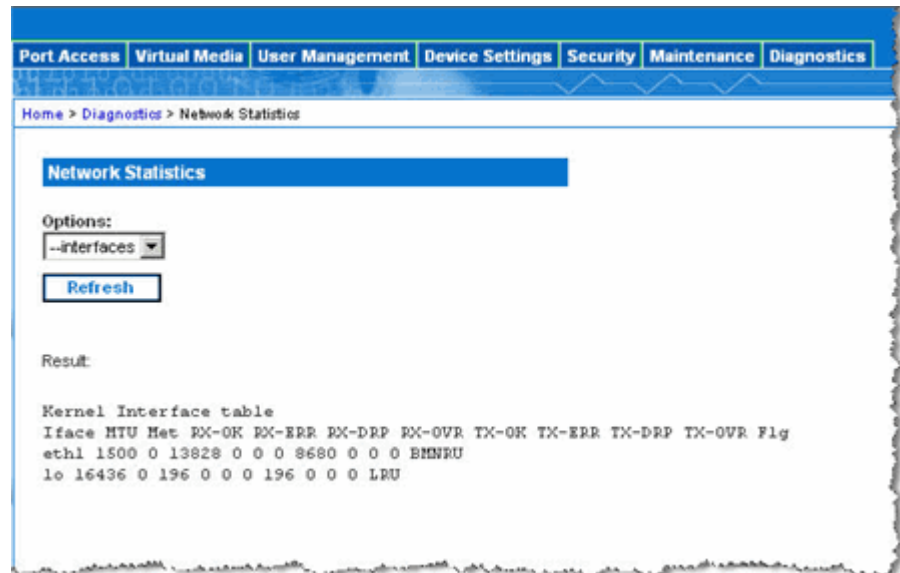
KX II-101 liefert Statistiken über die Netzwerkschnittstelle.

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



Network Statistics (Netzwerkstatistik)

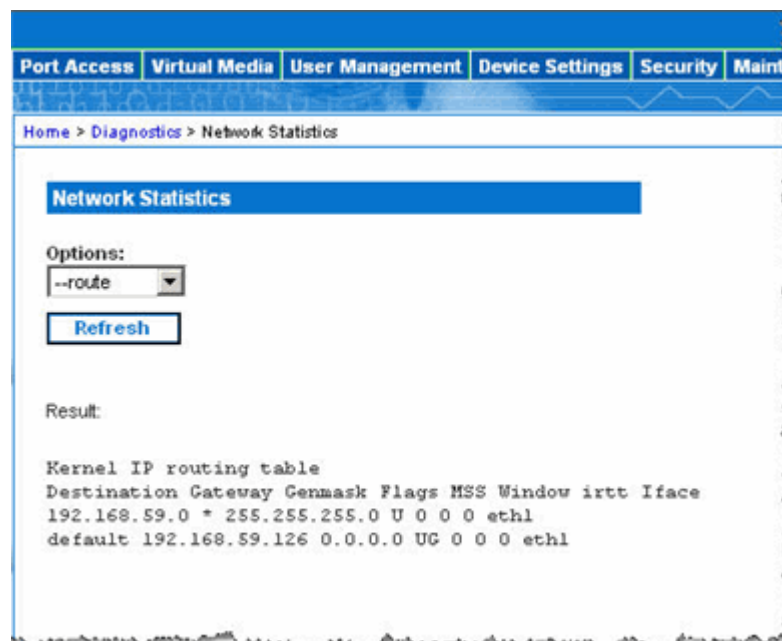
- **Interfaces** (Schnittstellen): Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



The screenshot shows the 'Network Statistics' page in a web interface. At the top, there is a navigation bar with tabs: Port Access, Virtual Media, User Management, Device Settings, Security, Maintenance, and Diagnostics. Below the navigation bar, the breadcrumb path is 'Home > Diagnostics > Network Statistics'. The main content area has a blue header 'Network Statistics'. Underneath, there is an 'Options:' section with a dropdown menu set to '--interfaces' and a 'Refresh' button. Below the options, the 'Result:' section displays the following text:

```
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1 1500 0 13828 0 0 0 8680 0 0 0 BMNRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
```

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



The screenshot shows the 'Network Statistics' page in a web interface, similar to the previous one. The navigation bar and breadcrumb path are the same. The 'Options:' section has a dropdown menu set to '--route' and a 'Refresh' button. Below the options, the 'Result:' section displays the following text:

```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.59.0 * 255.255.255.0 U 0 0 0 eth1
default 192.168.59.126 0.0.0.0 UG 0 0 0 eth1
```

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

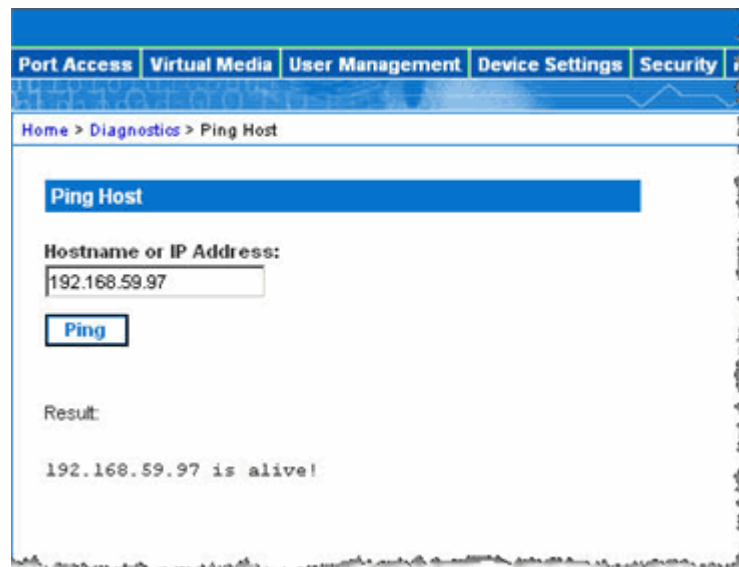
Die entsprechenden Informationen werden im Feld **Result** (Ergebnis) angezeigt.

Ping Host (Ping an den Host)

Ping ist ein Netzwerktool, mit dem getestet werden kann, ob ein bestimmter Host oder eine IP-Adresse über ein IP-Netzwerk erreichbar ist. Mithilfe der Seite **Ping Host** (Ping an den Host) können Sie herausfinden, ob ein Zielserver oder eine andere KX II-101-Einheit erreichbar ist.

➤ *So senden Sie ein Ping an den Host:*

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



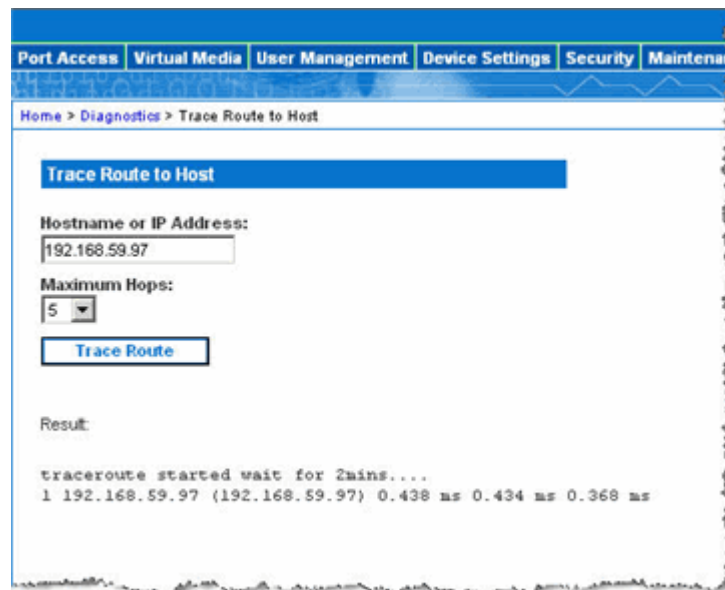
2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld **Hostname or IP Address** (Hostname oder IP-Adresse) ein.
3. Klicken Sie auf **Ping**. Die Ping-Ergebnisse werden im Feld **Result** (Ergebnis) angezeigt.

Trace Route to Host (Route zum Host zurückverfolgen)

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

➤ *So verfolgen Sie die Route bis zum Host zurück:*

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



2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld **Hostname or IP Address** (Hostname oder IP-Adresse) ein.
3. Wählen Sie in der Dropdown-Liste **Maximum Hops** (Maximale Teilstrecken) eine Option aus (5 bis 50 in Schritten von 5).
4. Klicken Sie auf die Schaltfläche **Trace Route** (Route zurückverfolgen). Der Befehl wird für den angegebenen Hostnamen oder die IP-Adresse sowie die maximale Zahl der Teilstrecken ausgeführt. Das Ergebnis der Routenverfolgung wird im Feld **Result** (Ergebnis) angezeigt.

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 der KX II-101-Einheit 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:

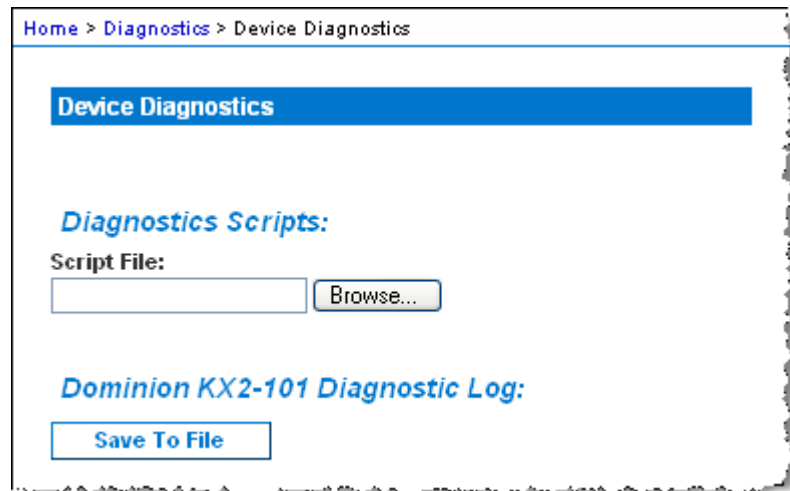
- **Diagnostics Scripts** (Diagnoseskripts) (optional): Lädt während einer Sitzung zum Debuggen eines schwerwiegenden Fehlers ein vom technischen Kundendienst von Raritan bereitgestelltes Speziaskript. Das Skript wird auf die Einheit hochgeladen und ausgeführt.
- **Device Diagnostic Log** (Gerätediagnoseprotokoll): Lädt eine Übersicht der Diagnosemeldungen von der KX II-101-Einheit auf den Client. Diese verschlüsselte Datei wird anschließend an den technischen Kundendienst von Raritan gesendet. Nur Raritan kann diese Datei interpretieren.

Hinweis: Auf diese Seite können nur Benutzer mit Administratorrechten zugreifen.

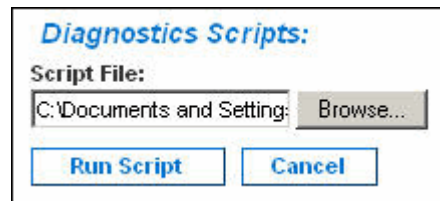
➤ *So führen Sie die KX II-101-Systemdiagnose aus:*

1. Wählen Sie **Diagnostics > Device Diagnostics** (Diagnose > Gerätediagnose). Die Seite **Device Diagnostics** (Gerätediagnose) wird angezeigt.

Device Diagnostics (Gerätediagnose)

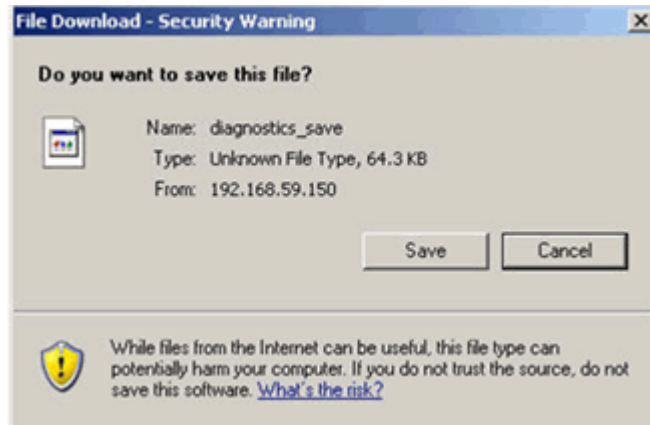


2. (Optional) Führen Sie die folgenden Schritte durch, wenn Sie eine Datei mit einem Diagnoseskript vom technischen Kundendienst von Raritan erhalten haben. Fahren Sie ansonsten mit Schritt 3 fort.
 - a. Rufen Sie die Diagnosedatei von Raritan ab, und entpacken Sie sie gegebenenfalls.
 - b. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen). Das Dialogfeld **Choose file** (Datei auswählen) wird angezeigt.
 - c. Navigieren Sie zu der Diagnosedatei, und markieren Sie sie.
 - d. Klicken Sie auf **Open** (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 die Schaltfläche **Save to File** (Speichern unter). Das Dialogfeld **File Download** (Datei-Download) 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 14 CC UnManage

In diesem Kapitel

Überblick.....	204
Aufheben der Verwaltung von KX II-101 durch CC-SG.....	205
Verwenden von CC-SG im Proxymodus.....	206

Überblick

Wenn ein KX II-101-Gerät über CommandCenter Secure Gateway gesteuert wird und Sie versuchen, über die KX II-101-Remote-Konsole direkt auf das Gerät zuzugreifen, wird die folgende Meldung angezeigt (nach Eingabe eines gültigen Benutzernamens und Kennworts):

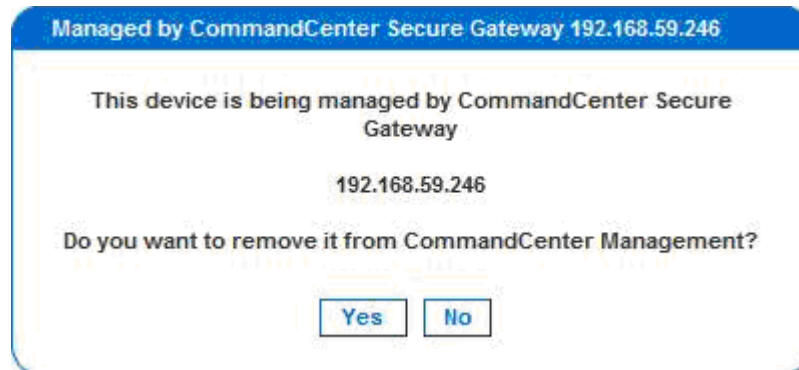


Aufheben der Verwaltung von KX II-101 durch CC-SG

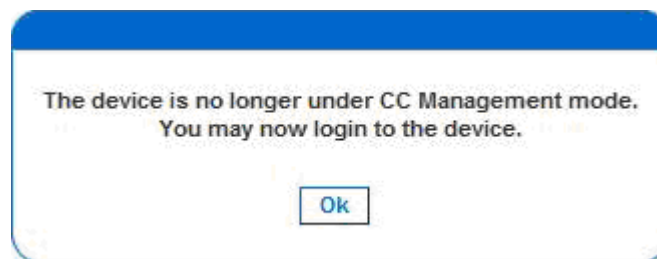
Sie können nur direkt auf das Gerät zugreifen, wenn die CC-SG-Steuerung von KX II-101 aufgehoben wird. Wenn KX II-101 jedoch keine Heartbeat-Nachrichten von CommandCenter empfängt (z. B. weil sich CommandCenter nicht im Netzwerk befindet), können Sie die CC-SG-Steuerung von KX II-101 aufheben, um auf 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 die Schaltfläche **Yes** (Ja). Sie werden aufgefordert, die Aktion zu bestätigen.
 2. Klicken Sie auf die Schaltfläche **Yes** (Ja). Es wird eine Meldung mit der Bestätigung angezeigt, dass die CC-Verwaltung des Geräts aufgehoben wurde.



3. Klicken Sie auf **Yes** (Ja). Die KX II-101-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 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

KX II-101.....	207
Kabel.....	208
Software für den Raritan Remote Client.....	208

KX II-101

Formfaktor	Formfaktor Null-U (0 Höhenheiten); vertikale oder horizontale Gestellmontage (Halterungen inklusive)
Abmessungen (T x B x H)	103 x 74 x 27 mm
Gewicht	0,286 kg
Stromversorgung	Netzadapter (100-240V~/ 6VDC) oder Power over Ethernet (PoE) Mid-Span-Einspeisung Signalpaareinspeisung
Betriebstemperatur	0° - 40°C
Luftfeuchtigkeit	20 % bis 85 % relative Luftfeuchtigkeit
Anzeige: Blaues hintergrundbeleuchtetes RARITAN-Logo Netzwerk-Port	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 Multifunktions-Port für alle RS-232-Funktionen, Modemverbindung und Dominion PX-Konnektivität

Kabel

Remote-Verbindung: Netzwerkprotokolle	Ein 10/100 Ethernet (RJ45)-Port TCP/IP, HTTP, HTTPS, UDP, RADIUS, LDAP, SNMP, DHCP
Bildschirmauflösungen: PC-Grafikmodus SUN®-Videomodus	720 x 400 (für DOS) 640 x 480 bei 60/72/75/85 Hz, 800 x 600 bei 56/60/72/75/85 Hz, 1024 x 768 bei 60/70/75/85 Hz, 1152 x 864 bei 60/75 Hz, 1280 x 1024 bei 60 Hz, 1600 x 1200 bei 60 Hz
Zertifizierungen:	UL/CUL, FCC Klasse A, CB, CE Klasse A und VCCI Klasse A

Kabel

Schnittstellentyp	Länge (cm)	Beschreibung
Video	38 cm	Integriertes Kabel
PS/2	38 cm	Integriertes Kabel
Mini-USB zu USB (M)	45 cm	USB-Kabel
Mini-DIN9 (M) zu DB9 (F)	182 cm	Serielles Kabel
DKX2-101-LPKVMC	10 cm	Kabel für die Integration des lokalen Ports
DKX2-101-SPDUC	180 cm	Kabel für die Verbindung mit einer Dominion PX-Einheit

Software für den Raritan Remote Client

Betriebssystemanforderungen: Windows XP / NT / ME / 2000

Anhang B Gestellmontage

Die KX II-101-Einheit 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-Kit enthaltenen Halterungen und Schrauben.

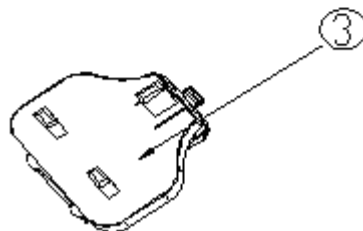
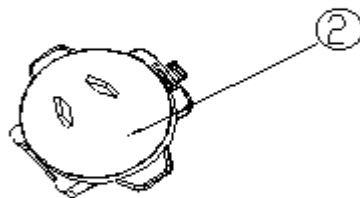
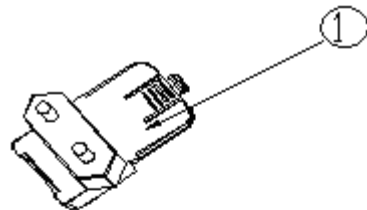
In diesem Kapitel

Befestigung des Netzadapter-Clips.....	209
Anbringen der Gestellhalterungen.....	211

Befestigung des Netzadapter-Clips

Clip-Typ identifizieren

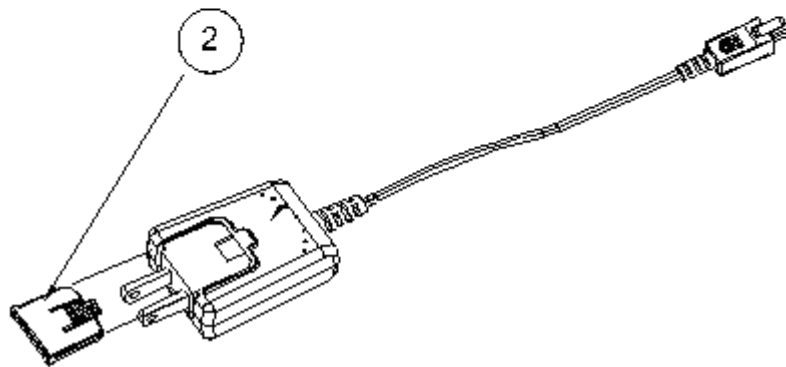
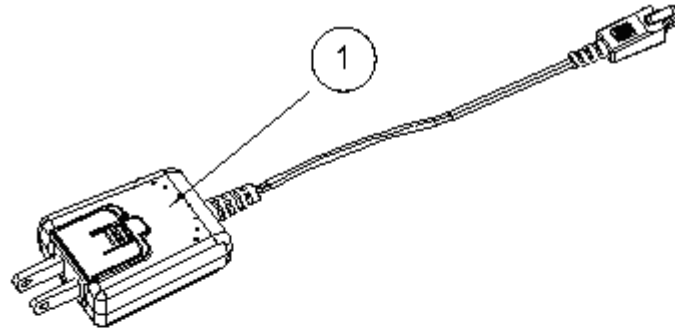
1. Clip für EU/Europa
2. Clip für Australien
3. Clip für Großbritannien



Befestigung des Netzadapter-Clips

Anschlussabdeckung vom Netzadapter entfernen

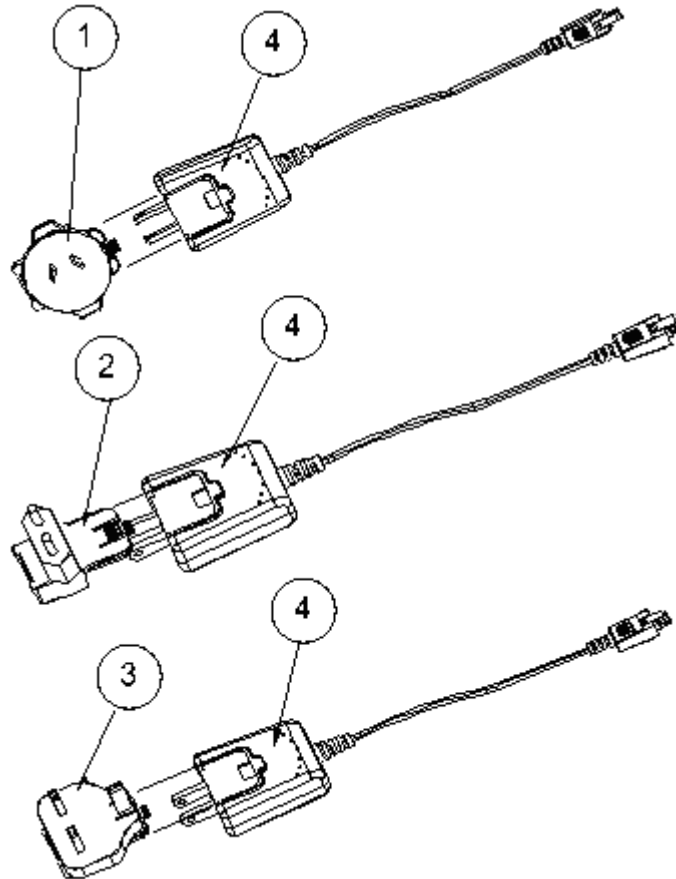
1. Netzadapter
2. Anschlussabdeckung Zum Entfernen drücken.



Clip am Netzadapter anbringen

1. Clip für Australien
2. Clip für EU/Europa
3. Clip für Großbritannien

4. Netzadapter

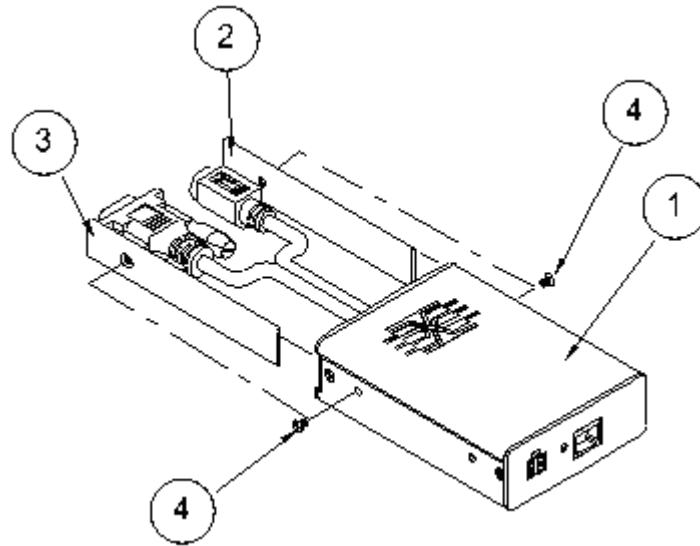


Anbringen der Gestellhalterungen

1. KX II-101-Einheit
2. Rechte Platte
3. Linke Platte
4. Schrauben

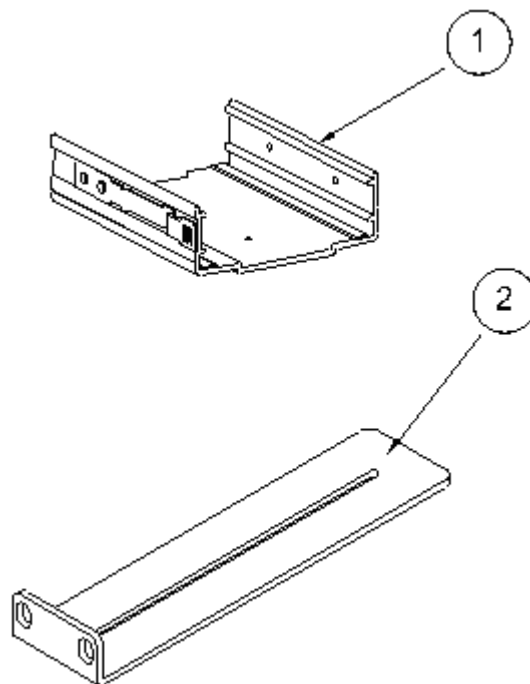
Anbringen der Gestellhalterungen

- Entfernen Sie die Schrauben von der KX II-101-Einheit.
- Schieben Sie die linke und rechte Platte von der KX II-101-Einheit weg.



KX II-101-Halterungen

1. U-Halterung
2. L-Halterung



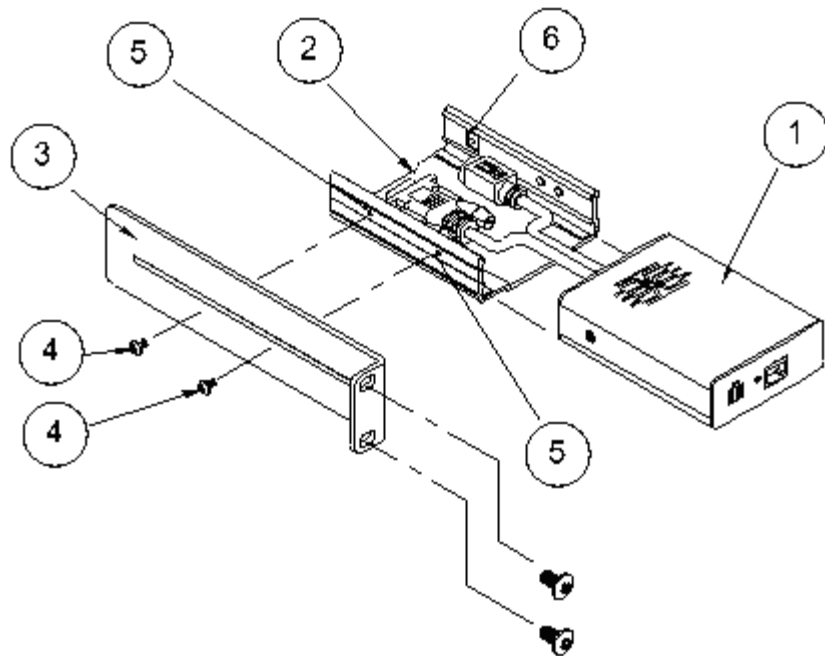
Halterungen an der KX II-101-Einheit zur horizontalen Montage anbringen

1. KX II-101-Einheit
2. U-Halterung
3. L-Halterung
4. Schrauben
5. Befestigungsloch
6. Verriegelung

Anbringen der Gestellhalterungen

- Bringen Sie die U-Halterung an der L-Halterung mit den im Lieferumfang enthaltenen Schrauben an. Richten Sie die Halterungen vor dem Festziehen der Schrauben aus.
- Befestigen Sie die Halterungen mit den vom Gestellhersteller bereitgestellten Schrauben zur Gestellmontage am Gestell.
- Schieben Sie die KX II-101-Einheit mit der KVM-Buchse zum Ziel zeigend in die U-Halterung. Ziehen Sie an der Verriegelung, und lassen Sie sie wieder los, damit die KX II-101-Einheit in der U-Halterung einrastet.

In der folgenden Abbildung ist die Befestigung der KX II-101-Einheit auf der linken Seite des Gestells dargestellt. Befolgen Sie diese Anleitungen auch, um die KX II-101-Einheit auf der rechten Gestellseite zu befestigen. Bringen Sie dabei jedoch die Halterungen auf der rechten Seite der KX II-101-Einheit an.



Halterungen an der KX II-101-Einheit zur vertikalen Montage anbringen

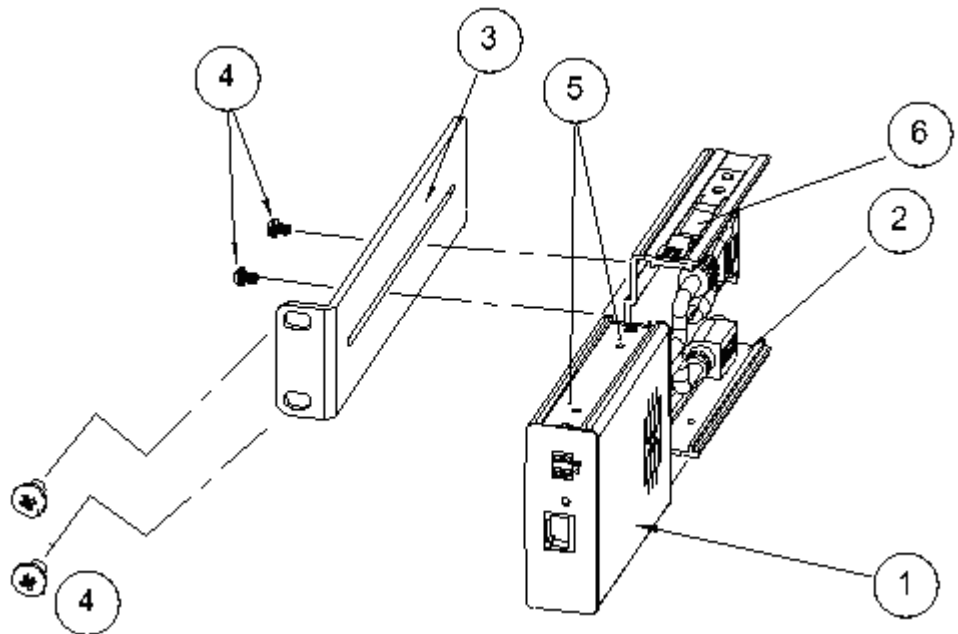
1. KX II-101-Einheit
2. U-Halterung
3. L-Halterung
4. Schrauben
5. Befestigungsloch

6. Verriegelung

Bringen Sie die U-Halterung an der L-Halterung mit den im Lieferumfang enthaltenen Schrauben an. Richten Sie die Halterungen vor dem Festziehen der Schrauben aus.

Befestigen Sie die Halterungen mit den vom Gestellhersteller bereitgestellten Schrauben zur Gestellmontage am Gestell.

Schieben Sie die KX II-101-Einheit mit der KVM-Buchse zum Ziel zeigend in die U-Halterung. Ziehen Sie an der Verriegelung, und lassen Sie sie wieder los, damit die KX II-101-Einheit in der U-Halterung einrastet.



Index

A

- Abmelden • 40
- About Raritan Virtual KVM Client
(Informationen zum Raritan Virtual KVM Client) • 114
- Absolute (Absolut) • 111
- Add New Favorite (Neuen Favoriten hinzufügen) • 43, 48
- Add New User (Neuen Benutzer hinzufügen) • 54, 56, 167
- Add New User Group (Neue Benutzergruppe hinzufügen) • 58
- Aktivieren des direkten Port-Zugriffs • 37
- Aktualisieren des LDAP-Schemas • 74, 79
- Aktualisieren des Schemacache • 83
- Allgemeine Befehle für alle Ebenen der Befehlszeilenschnittstelle • 189
- Anbringen der Gestellhalterungen • 212
- Ändern des Kennworts • 66
- Ändern eines Tastaturmakros • 101
- Ändern vorhandener Benutzer • 54, 56
- Ändern vorhandener Benutzergruppen • 58, 65
- Anmelden • 187
- Anmeldung • 7
- Anschließen der KX II-101-Einheit • 8, 16
- Anschließen des Powerstrips • 152, 155
- Anschlussabdeckung vom Netzadapter entfernen • 211
- Anzeigen der Ausgangszuordnungen • 158
- Audit Log (Prüfprotokoll) • 175
- Aufheben der Verwaltung von KX II-101 durch CC-SG • 205
- Ausführen eines Tastaturmakros • 101
- Authentication Settings
(Authentifizierungseinstellungen) • 69
- Authentifizierung im Vergleich zur Autorisierung • 68, 69
- Authentifizierungseinstellungen • 67
- Auto-Sense Video Settings
(Videoeinstellungen automatisch erkennen) • 103

B

- Backup/Restore
(Sicherung/Wiederherstellung) • 178
- Bearbeiten von rcusergroup-Attributen für Benutzermitglieder • 84
- Befehl • 190, 191, 193, 194
- Befehle der Befehlszeilenschnittstelle • 185, 190
- Befehlszeilenschnittstelle (CLI) • 185
- Befestigung des Netzadapter-Clips • 210
- Benennen des Powerstrips (Seite) • 153
- Benennen des Zielservers • 27
- Benutzer • 51
- Benutzer, Gruppen und Zugriffsberechtigungen • 51
- Benutzerfunktionen • 5
- Benutzerverwaltung • 51, 52
- Beziehung zwischen Benutzern und Gruppen • 52

C

- Calibrate Color (Farbe kalibrieren) • 103
- CC UnManage • 204
- CD-ROM-/DVD-ROM-/ISO-Abbilder • 120, 123, 125
- Clip am Netzadapter anbringen • 211
- Clip-Typ identifizieren • 210
- Configuration (Konfiguration) • 192
- Connection Info (Verbindungsinformationen) • 96

D

- Date/Time Settings
(Datum-/Uhrzeiteinstellungen) • 139
- Debug • 190, 191
- Device Diagnostics (Gerätediagnose) • 201
- Device Information (Geräteinformationen) • 177
- Device Services (Gerätedienste) • 134, 186
- Diagnose • 195
- Diagnostics (Diagnose) • 190, 191
- Dialogfeld • 94

Index

Discover Devices - KX II-101 Subnet (Geräte erkennen – KX II-101-Subnetz) • 47

Discover Devices - Local Subnet (Geräte erkennen – Lokales Subnetz) • 45

E

Eingabeaufforderungen der Befehlszeilenschnittstelle • 188

Einleitung • 1

Einrichten eines neuen Kennworts • 24

Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen • 80

Einstellen der Sun-Videoauflösung • 10

Einstellen der Videoauflösung des Servers • 9, 10, 18

Einstellungen für Apple® Macintosh • 15

Einstellungen für Linux • 14

Einstellungen für Sun Solaris • 14

Einstellungen für Windows 2000 • 13

Einstellungen für Windows XP • 13

Encryption & Share (Verschlüsselung und Freigabe) • 168

Entfernen eines Tastaturmakros • 101

Ereignisverwaltung • 140

Erstellen eines neuen Attributs • 81

Erstellen eines Tastaturmakros • 98

Erstellen von Benutzern und Gruppen • 28

Event Management – Destinations (Ereignisverwaltung – Ziele) • 144

Exit (Beenden) • 97

F

Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist • 121, 122

Favorites List (Favoritenliste) • 43

Festlegen von Berechtigungen • 59, 60, 65

Festlegen von Berechtigungen für individuelle Gruppen • 55, 61

Festlegen von Port-Berechtigungen • 61

File Server Setup (Dateiserver-Setup) (nur für Dateiserver-ISO-Abbilder) • 119, 125

Firmware Upgrade (Firmware-Aktualisierung) • 180

G

Geräteverwaltung • 127

Gestellmontage • 5, 210

Gruppen • 51

Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste) • 62

H

Halterungen an der KX II-101-Einheit zur horizontalen Montage anbringen • 214

Halterungen an der KX II-101-Einheit zur vertikalen Montage anbringen • 215

Herstellen einer Verbindung mit der KX II-101-Einheit • 27, 35

Herstellen einer Verbindung mit virtuellen Medien • 121

Hinweis für CC-SG-Benutzer • 67

Hinweis zu Microsoft Active Directory • 68

Hinzufügen von Attributen zur Klasse • 82

I

Implementierung der LDAP-Remote-Authentifizierung • 71

Implementierung der RADIUS-Remote-Authentifizierung • 70, 76

Installation und Konfiguration • 8, 193

Intelligent • 109

IP Access Control (IP-Zugriffssteuerung) • 60, 63, 133, 171

J

Java Runtime Environment (JRE) • 35

K

Kabel • 6, 209

Keyboard Macros (Tastaturmakros) • 98

Keyboard/Mouse Setup (Tastatur/Maus einrichten) • 136

Konfigurieren der Einstellungen der Netzwerk-Firewall • 8, 23

Konfigurieren des direkten Port-Zugriffs • 26

Konfigurieren des SNMP-Agenten • 141, 146

Konfigurieren des Zielservers • 8

Konfigurieren von KX II-101 • 8, 24
 KX II-101 • 208
 KX II-101-Halterungen • 213

L

LAN Interface Settings
 (LAN-Schnittstelleneinstellungen) • 132
 Layout der KX II-101-Konsole • 38
 Login Limitations (Anmeldebeschränkungen)
 • 163
 Lokale Laufwerke • 119, 121

M

Mausmodi • 11
 Mauszeigersynchronisation • 92
 Menü • 42, 52, 92, 94, 97, 102, 107, 112, 113,
 114, 127, 161, 195
 Menü Maintenance (Wartung) • 174
 Menüstruktur • 90
 Menüstruktur der KX II-101-Remote-Konsole
 • 40
 Montage • 5

N

Navigation in der Befehlszeilenschnittstelle •
 188
 Navigation in der KX II-101-Konsole • 39
 Network (Netzwerk) • 190, 192
 Network Basis Settings
 (Basisnetzwerkeinstellungen) • 130
 Network Interface (Netzwerkschnittstelle) •
 196
 Network Settings (Netzwerkeinstellungen) •
 129
 Network Statistics (Netzwerkstatistik) • 197
 Netzwerkkonfiguration • 4

O

Öffnen einer KVM-Sitzung • 120
 Optionales Zubehör • 6
 Optionen • 90
 Options (Optionen) • 112

P

Paketinhalt • 6
 Ping Host (Ping an den Host) • 199
 Port Configuration (Port-Konfiguration) • 149
 Produktfeatures • 4
 Produktfotos • 3
 Prüfen Ihres Browsers auf
 AES-Verschlüsselung • 169, 171
 PS/2-Konfiguration • 19

R

Reboot (Neustart) • 183
 Refresh Screen (Anzeige aktualisieren) • 102
 Remote-Authentifizierung • 67
 Rückgabe von Benutzergruppeninformationen
 vom Active Directory-Server • 74

S

Scaling (Skalieren) • 113
 Schnittstellen • 4
 Security Settings (Sicherheitseinstellungen) •
 162
 Seite • 49
 Send Ctrl+Alt+Delete (Strg+Alt+Entf senden) •
 97
 Serial Port Settings (Einstellungen für seriellen
 Port) • 137
 Service Pack • 7
 Sicherheitseinstellungen • 161
 Single Mouse Cursor (Ein Cursor) • 107
 SNMP Configuration (SNMP-Konfiguration)
 • 141
 SNMP-Trap-Konfiguration • 141, 146
 Software für den Raritan Remote Client • 209
 Sperren von Benutzern und Aufheben der
 Sperrung • 56
 Spezifikationen für den
 RADIUS-Kommunikationsaustausch • 78
 SSH-Verbindung mit der KX II-101-Einheit •
 186
 SSH-Zugriff über eine UNIX-Workstation •
 187
 SSH-Zugriff über einen Windows-PC • 186
 Standard • 108

Index

Standard-IP-Adresse • 7
Starten der KX II-101-Einheit • 36
Steuern des Powerstrip-Geräts • 151, 159
Stromversorgung • 5
Stromversorgung der KX II-101-Einheit • 22
Stromzufuhrsteuerung • 151
Strong Passwords (Sichere Kennwörter) • 67, 163, 165
Symbolleiste • 91
Synchronize Mouse (Maus synchronisieren) • 107
Syntax der Befehlszeilenschnittstelle - Tipps und Zugriffstasten • 189
Syslog-Konfiguration • 142
Systemverwaltungsfunktionen • 4

T

Target Screen Resolution (Zielbildschirmauflösung) • 114
Technische Daten • 208
Terminologie • 6
Tipps zur Maussynchronisation • 92
Trace Route to Host (Route zum Host zurückverfolgen) • 200
Trennen von virtuellen Medien • 120, 124

U

Überblick • 89, 116, 151, 185, 204
Überblick über Dominion KX II-101 • 2
Unterstützte Protokolle • 67
Unterstützte Sprachen • 35
Upgrade History (Aktualisierungsverlauf) • 183
USB-Konfiguration • 21
User Blocking (Benutzersperrung) • 56, 163, 166
User Group List (Liste der Benutzergruppen) • 57
User List (Benutzerliste) • 53

V

Verbinden mit dem Netzwerk • 22
Verbinden mit dem Zielservers • 18
Vervollständigen der Befehle • 188
Verwalten von Favoriten • 41

Verwaltungsfunktionen • 4
Verwenden der Remote-Konsole • 24
Verwenden des Ports • 23, 30
Verwenden eines
 Terminalemulationsprogramms • 7, 30, 188
Verwenden virtueller Medien • 119
Verwenden von CC-SG im Proxymodus • 207
Video Settings (Videoeinstellungen) • 104
Videoauflösung • 5
View Toolbar (Symbolleiste anzeigen) • 113
Virtual KVM Client • 88
Virtuelle Medien • 111, 115
Von LDAP • 79
Von Microsoft Active Directory • 80
Voraussetzungen für die Verwendung virtueller Medien • 118, 119

W

Wartung • 174
Wichtige Informationen • 7
Windows Vista • 11

Z

Zugriff auf KX II-101 über die Befehlszeilenschnittstelle • 186
Zuordnen von KVM-Zielservers zu Ausgängen (Seite • 155, 159
Zurückgeben von Benutzergruppeninformationen • 79
Zurückgeben von Benutzergruppeninformationen über RADIUS • 78
Zuweisen einer IP-Adresse • 7, 25



➤ *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.: +81-3-3523-5994
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+1 MEZ
Tel.: +44-20-7614-77-00

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 17:00 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0

➤ *Korea*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +82-2-5578730

➤ *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: tech.rap@raritan.com