



# Dominion KX II-101-V2

用户指南  
Release 3.5.0

---

Copyright © 2012 Raritan, Inc.

KX2101V2-v3.5.0-D-CHS

September 2012

255-62-3059-00

---

本文档包含受版权保护的专利信息。版权所有。未经 Raritan, Inc. 明确的事先书面许可，不得对本文档的任何部分进行影印、复制或翻译成其他语言。

© Copyright 2012 Raritan, Inc. 在本指南中提到的所有第三方软件和硬件是各自所有者的注册商标或商标，是各自所有者的财产。

#### FCC 信息

本设备经测试符合 FCC 规则第 15 部分规定的 A 类数字设备限制要求。这些限制旨在合理保护商用安装设备免受有害干扰的影响。本设备产生、使用并辐射射频能量，如果不按说明书安装和使用，可能会对无线通信造成有害干扰。在居民区使用本设备可能会造成有害干扰。

#### VCCI 信息（日本）

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。

事故、灾害、误用、滥用、擅自修改产品或其他不受 Raritan 合理控制的事件造成的产品损坏，或者在非正常工作条件下造成的产品损坏，Raritan 均不承担责任。

如果本产品随机提供电源线，电源线只能供本产品使用。



#### 机架安装安全指导

对于需要在机架上安装的 Raritan 产品，应该采取下列预防措施：

- 封闭机架环境里的工作温度可能比室内温度高。不得超过设备的最大额定环境温度。参看规则部分。
- 保证机架环境通风充分。
- 在机架上小心安装设备，避免机械负荷不均匀。
- 小心连接设备供电电路，避免电路过载。
- 所有设备正确接地至分支电路，尤其是（非直接连接的）配电盘等电源连接。

# 目录

<b>简介</b>	<b>1</b>
<hr/>	
KX II-101-V2 概述 .....	2
KX II-101-V2 帮助 .....	3
帮助新增内容 .....	4
相关文档 .....	4
产品图片 .....	5
产品特点 .....	5
界面 .....	5
网络配置 .....	5
系统管理功能 .....	6
管理功能 .....	6
用户特点 .....	6
电源 .....	7
视频分辨率 .....	7
安装 .....	7
术语 .....	7
包装内容 .....	8
<b>安装和配置</b>	<b>9</b>
<hr/>	
概述 .....	9
默认登录信息 .....	9
快速入门 .....	10
第一步：配置目标服务器 .....	10
第二步：配置网络防火墙设置 .....	20
第三步：连接设备 .....	21
第四步：配置 KX II-101-V2 .....	25
<b>使用目标服务器</b>	<b>33</b>
<hr/>	
界面 .....	33
KX II-101-V2 Remote Console 界面 .....	33
Multi-Platform Client (MPC) .....	41
Virtual KVM Client (VKC) .....	41
概述 .....	42
连接 KVM 目标服务器 .....	42
工具栏按钮和状态栏图标 .....	42
控制目标服务器电源 .....	44

断开 KVM 目标服务器电源.....	45
连接属性 .....	45
连接信息 .....	47
键盘选项 .....	47
视频属性 .....	53
鼠标选项 .....	57
VKC 虚拟媒体 .....	60
工具选项 .....	60
视图选项 .....	64
帮助选项 .....	66

## 虚拟媒体 67

---

概述.....	68
使用虚拟媒体的前提 .....	70
Windows XP 环境下的虚拟媒体.....	71
Linux 环境下的虚拟媒体 .....	72
Mac 环境下的虚拟媒体 .....	73
读写不可用时的条件 .....	74
使用虚拟媒体 .....	74
连接虚拟媒体 .....	75
本地驱动器.....	75
安装 CD-ROM/DVD-ROM/ISO 镜像文件 .....	76
断开虚拟媒体 .....	77

## 用户管理 78

---

用户组 .....	78
用户组列表.....	79
用户和用户组之间的关系.....	79
添加新用户组 .....	79
修改现有用户组.....	83
用户 .....	84
查看 KX II-101-V2 用户列表.....	84
按端口查看用户.....	85
让用户断开端口.....	85
让用户退出 KX II-101-V2（强制退出） .....	86
添加新用户 .....	86
修改现有用户 .....	87
用户锁定和解锁.....	87
验证设置.....	88
实现 LDAP/LDAPS 远程验证 .....	88
Active Directory 服务器返回用户组信息.....	92
实现 LDAP/LDAPS 远程验证 .....	93
通过 RADIUS 返回用户组信息 .....	94

RADIUS 通信交换规范.....	95
用户验证流程.....	96
更改密码.....	98
<b>设备管理</b>	<b>99</b>
网络设置.....	99
网络基本设置.....	100
LAN 接口设置.....	103
设备服务.....	104
启用 Telnet.....	104
启用 SSH.....	104
HTTP 和 HTTPS 端口设置.....	105
输入发现端口.....	105
启用通过 URL 进行直接端口访问.....	105
配置 SNMP 代理.....	106
键盘/鼠标设置.....	108
串行端口设置.....	108
管理端口.....	109
Raritan 电源条控制.....	109
调制解调器.....	109
配置日期/时间设置.....	110
事件管理.....	111
配置事件管理 — 设置.....	111
配置事件管理 — 目的地.....	118
端口配置.....	119
管理 KVM 目标服务器（端口页）.....	120
电源控制.....	121
模拟 KVM 切换器.....	126
用复位按钮复位 KX II-101-V2.....	127
更改默认图形用户界面语言设置.....	128
<b>管理 USB 连接</b>	<b>129</b>
概述.....	129
USB 连接设置.....	130
高级 USB 连接设置.....	131
<b>安全管理</b>	<b>133</b>
安全设置.....	133
登录限制.....	133
强密码.....	134
用户锁定.....	136

加密和共享.....	137
启用 FIPS 140-2.....	139
配置 IP 访问控制 .....	141
SSL 证书 .....	143
安全标志.....	146

## 维护 147

---

审计日志.....	147
设备信息.....	148
备份和恢复 .....	149
升级固件.....	150
升级历史记录 .....	152
出厂复位.....	152
重新启动 KX II-101-V2 .....	153
停止 CC-SG 管理 .....	154

## 诊断 156

---

网络接口页 .....	156
网络统计数据页 .....	156
Ping 主机页 .....	159
跟踪主机路由页 .....	159
设备诊断.....	161

## 命令行界面 163

---

概述.....	163
用命令行界面访问 KX II-101-V2.....	164
用 SSH 连接访问 KX II-101-V2 .....	164
在 Windows PC 上进行 SSH 访问.....	164
在 UNIX/Linux 工作站上进行 SSH 访问 .....	165
登录.....	165
命令行界面导航.....	165
命令行界面提示符 .....	165
自动完成命令输入.....	166
命令行界面语法 — 提示和快捷键.....	166
在命令行界面上常用的命令 .....	166
命令行界面命令 .....	167
诊断.....	168
配置.....	169
Listports 命令 .....	171
Userlist 命令 .....	171

<b>CC-SG 管理</b>	<b>172</b>
概述 .....	172
使 KX II-101-V2 不受 CC-SG 管理 .....	173
在代理模式下使用 CC-SG .....	174
<b>规格</b>	<b>175</b>
物理规格 .....	175
支持的操作系统（客户机） .....	176
支持的浏览器 .....	177
连接器 .....	178
认证调制解调器 .....	178
支持的视频分辨率 .....	178
支持的键盘语言 .....	179
使用的 TCP 端口和 UDP 端口 .....	180
Network Speed Settings .....	182
9 针引脚 .....	183
<b>更新 LDAP 模式</b>	<b>184</b>
返回用户组信息 .....	184
自 LDAP .....	184
从 Microsoft Active Directory 返回 .....	184
设置注册表，允许对模式执行写操作 .....	185
创建新属性 .....	185
给类添加新属性 .....	187
更新模式高速缓存 .....	188
编辑用户成员的 rcusergroup 属性 .....	188
<b>机架安装</b>	<b>192</b>
将 L 型安装支架固定在 KX II-101-V2 上进行水平安装 .....	192
<b>参考资料</b>	<b>194</b>
Java Runtime Environment (JRE) .....	194
IPv6 支持注意事项 .....	195
操作系统 IPv6 支持注意事项 .....	195
键盘、视频和鼠标说明 .....	195
Sun 刀片服务器视频、键盘和鼠标支持限制 .....	195
在本地键盘上进行 BIOS 访问的限制 .....	196
HP UX RX 1600 键盘和鼠标配置 .....	196

目录

Compaq Alpha 和 IBM P 服务器鼠标模式限制 .....	197
Windows 2000 和 Windows 2003 服务器键盘限制 .....	197
CC-SG .....	197
代理模式和 MPC .....	197

**常见问题解答** **198**

---

常见问题解答 .....	198
IPv6 联网 .....	199

**索引** **201**

---



# Ch 1

# 简介

## 在本章内

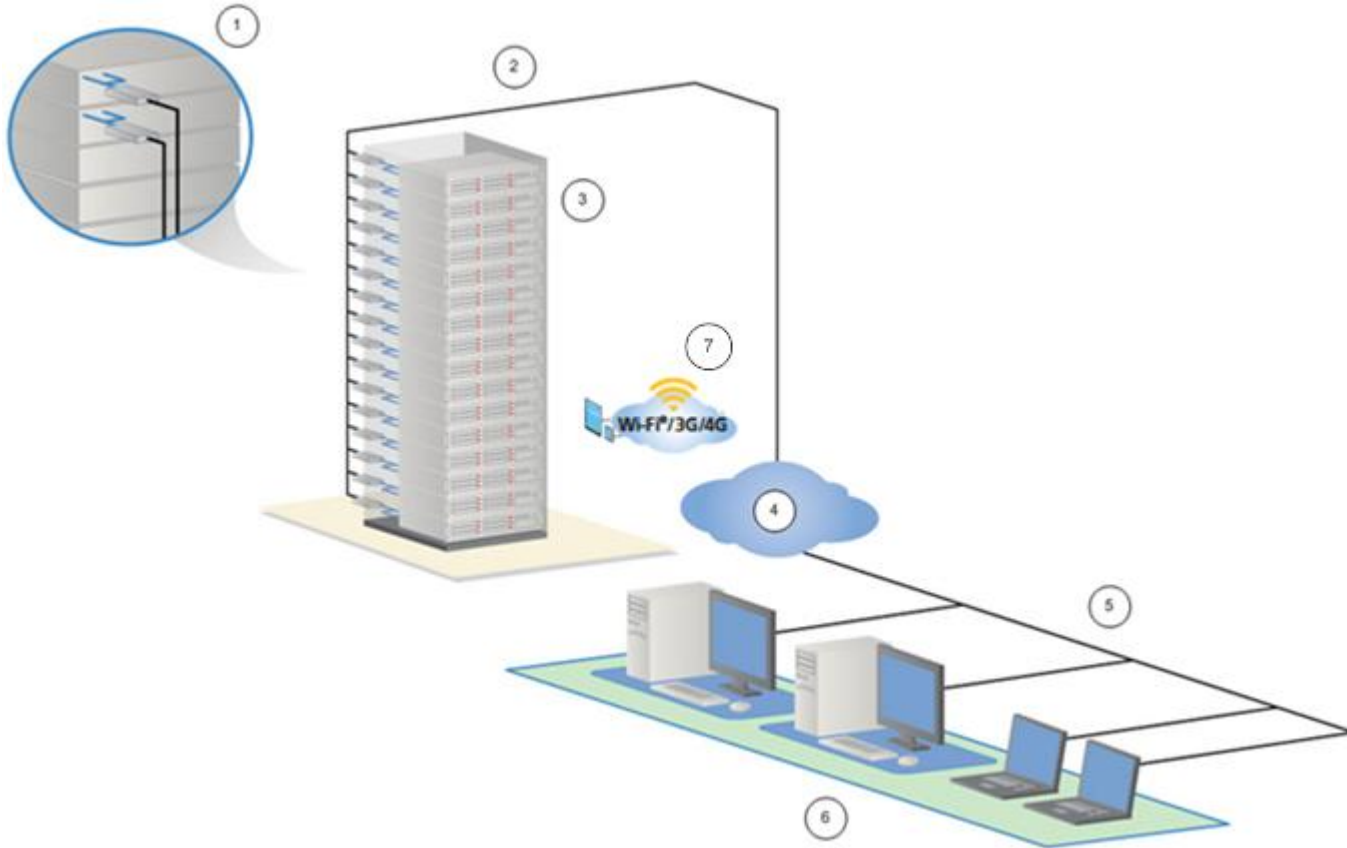
KX II-101-V2 概述 .....	2
KX II-101-V2 帮助 .....	3
产品图片 .....	5
产品特点 .....	5
术语.....	7
包装内容 .....	8

## KX II-101-V2 概述

感谢你购买 Dominion KX II-101-V2。KX II-101-V2 有一个键盘、一个视频和一个鼠标 (KVM) 端口连接目标服务器，有一个 IP 端口连接 IP 网络。在 KX II-101-V2 设备内，来自服务器的 KVM 信号被转换成 IP 格式，经压缩后通过 IP 网络传输。

KX II-101-V2 dongle 结构紧凑，很容易安装在目标服务器附近，每台 KX II-101-V2 设备都有自己的 IP 地址。每台设备通过外部 AC-DC 电源组供电。

KX II-101-V2 既可以作为独立设备工作，也可以利用 Raritan CommandCenter Secure Gateway (CC-SG) 5.4 或更高版本管理工具与其他 Raritan 访问产品集成在一个逻辑解决方案里。



图示符号	
①	KX II-101-V2
②	LAN
③	Windows®、Linux® 和 Sun™ 服务器
④	TCP/IP
⑤	LAN
⑥	远程（网络）访问
⑦	使用 CC-SG 时通过 iPhone® 和 iPad® 进行无线访问

## KX II-101-V2 帮助

KX II-101-V2 帮助说明如何安装、设置和配置 KX II-101-V2。它还说明如何访问目标服务器，如何使用虚拟媒体，如何管理用户和安全，如何维护和诊断 KX II-101-V2。

在使用 KX II-101-V2 之前参看 KX II-101-V2 版本说明了解当前版本的重要信息。

可以在 Raritan 网站上的 Raritan **固件和文档** 页下载 PDF 版本的帮助。Raritan 建议你浏览 Raritan 网站，了解最新的用户指南。

必须在浏览器上启用 **Active Content**（活动内容），才能使用联机帮助。如果使用 Internet Explorer 7，必须启用 **Scriptlets**（代码块）。阅读浏览器帮助文件，了解如何启用这些功能。

---

## 帮助新增内容

根据设备增强功能和/或用户文档变动情况，增加了下列信息。

- FIPS 140-2 加密支持
- 登录安全标志支持
- 利用 iPad® 和 iPhone® 无线访问与 CC-SG 管理的 KX II-101-V2 相连的服务器
- SNMPv3 支持
- 可以把自己的 SSL 证书上载到 KX II-101-V2 上
- 1920x1080 和宽屏视频分辨率支持
- TCP/IP 端口号码可配置（隐藏模式）
- 直接访问 CC-SG 5.4 或更高版本管理的 KX II-101-V2
- Linux® 和 Mac® 虚拟媒体支持
- 日文、繁体中文和简体中文用户界面支持
- 在双协议堆环境下支持 IPv4 和 IPv6
- 让用户断开端口
- 强制用户退出
- 在 KX II-101-V2 上更新 SNMP 陷阱和 SNMP 代理用户界面

请参看 KX II-101-V2 版本说明详细了解设备和本版本的帮助发生了哪些变化。

---

## 相关文档

KX II-101-V2 帮助配有 KX II-101-V2 快速安装指南，后者可以在 **Raritan 网站** (<http://www.raritan.com/support/firmware-and-documentation>) 上的 Raritan 固件和文档页下载。

可以在 **KVM 和串行访问客户机指南**和 Raritan 网站上找到 KX II-101-V2 使用的客户机应用程序的安装要求和使用说明。本帮助在适当的地方说明 KX II-101-V2 使用的特定客户机功能。

---

## 产品图片



KX II-101-V2

---

## 产品特点

---

### 界面

- 集成 PS/2 KVM 连接
- 用于控制和虚拟媒体的 USB 连接
- 用于初始设备配置和诊断、可与外置调制解调器访问和 Raritan 电源条控制一起使用的串行管理端口
- 用于连接监视器的本地端口
- 支持 10/100base-T 自动检测全双工的 Ethernet LAN 端口

---

### 网络配置

- DHCP 或静态 IP 设备地址

---

### 系统管理功能

- 基于 Ethernet 的固件升级
- 故障防护固件升级能力
- 可以人工同步或通过网络时间协议 (NTP/SNTP) 同步的时钟
- 本地管理员活动日志有时间戳；管理员可以禁用的 SNMP V2 代理
- 支持 RADIUS 和 LDAP/LDAPS 验证协议

---

### 管理功能

- 基于 Web 的管理
- LDAP、Active Directory®、RADIUS 或内部验证和授权
- DHCP 分配的地址或固定 IP 地址
- 与 Raritan CommandCenter Secure Gateway (CC-SG) 管理工具集成在一起
- 利用 iPad® 和 iPhone® 无线访问与 CC-SG 管理的 KX II-101-V2 相连的服务器
- FIPS 140-2 支持
- 登录安全标志支持
- SNMPv3 支持
- 可以把自己的 SSL 证书上载到 KX II-101-V2 上
- TCP/IP 端口号码可配置（隐藏模式）
- 在双协议堆环境下支持 IPv4 和 IPv6
- 让用户断开端口
- 强制用户退出

---

### 用户特点

- 通过常用浏览器进行 Web 访问
- 直观图形用户界面
- 允许多个远程用户连接目标服务器的 PC 共享模式
- TCP 通信
- 英文、日文、繁体中文和简体中文用户界面和帮助
- 虚拟媒体访问
- 绝对鼠标同步™
- 即插即用
- KVM 信号（包括视频和虚拟媒体）256 位加密

---

**电源**

- 由外部 AC-DC 适配器供电

---

**视频分辨率**

- 最高 1920x1080 @ 60Hz 和宽屏视频分辨率

---

**安装**

- 机架安装支架
- 

**术语**

术语	说明
目标服务器	通过 KX II-101-V2 及其相连的 KVM 配置远程访问的服务器。
远程 PC	用于访问和控制与 KX II-101-V2 相连的目标服务器的 Windows®、Linux® 或 Apple Macintosh® 计算机。
管理串行端口	用 DB9 连接器（公）将管理串行端口连接到 PC 串行端口，然后用标准仿真软件包（例如 HyperTerminal）访问管理串行端口。管理串行端口用于进行网络配置。
本地用户端口	使靠近目标服务器的用户无需断开 KX II-101-V2 即可使用本机监视器。
虚拟媒体	使目标服务器能远程访问客户机 PC 和网络文件服务器上的媒体。

---

## 包装内容

每台 KX II-101-V2 设备包括：

- KX II-101-V2 - KVM over IP
- KVM 电缆
- 电源适配器 — 配通用适配器的 AC/DC 5VDC
- 安装支架
- 打印版《快速安装指南》
- 印刷版《应用说明》（如适用）
- 印刷版《技术说明》（如适用）



## 在本章内

概述.....	9
默认登录信息.....	9
快速入门.....	10

## 概述

本章介绍如何安装和配置 KX II-101-V2。安装和配置包括下列步骤：

- **第一步：配置目标服务器** (p. 10)
- **第二步：配置网络防火墙设置** (p. 20)
- **第三步：连接设备** (p. 21)
- **第四步：配置 KX II-101-V2** (p. 25)

为了确保最佳性能，要在安装 KX II-101-V2 之前配置通过 KX II-101-V2 访问的目标服务器。注意下列配置要求仅适用于目标服务器，不适用于远程访问 KX II-101-V2 的计算机。

## 默认登录信息

默认	值
用户名	默认用户名是 <code>admin</code> 。此用户有管理权限。
密码	默认密码是 <code>raritan</code> 。 密码区分大小写，必须按在创建密码时使用的大小写输入密码。例如默认密码 <code>raritan</code> 必须全部按小写字母输入。 在首次启动 KX II-101-V2 时，要求你更改默认密码。
IP 地址	KX II-101-V2 使用默认 IP 地址 192.168.0.192。
<b>重要说明：</b> 为备用和业务连续性起见，强烈建议你创建一个备用管理员用户名和密码，把这些信息保持在安全的地方。	

---

## 快速入门

使用 Microsoft® Internet Explorer® v6 或 Windows 2000® 的 KX II-101-V2 用户必须升级到 SP4 或更新的服务包。

KX II-101-V2 有静态默认 IP 地址。在没有 DHCP 服务器的网络上，必须用 KX II-101-V2 串行管理控制台或 KX II-101-V2 Remote Console 配置新的静态 IP 地址、子网掩码和网关地址。

参看**分配 IP 地址** (p. 26)，了解如何用 Remote Console 给 KX II-101-V2 分配 IP 地址。参看**用终端仿真程序配置 KX II-101-V2 (可选)** (p. 30)，了解如何用串行管理控制台设置 IP 地址。

---

### 第一步：配置目标服务器

为了确保最佳性能，要在安装 KX II-101-V2 之前配置通过 KX II-101-V2 访问的目标服务器。注意下列配置要求仅适用于目标服务器，不适用于远程访问 KX II-101-V2 的计算机。

#### 设置服务器视频分辨率

为了实现最佳带宽效率和最佳视频性能，应该将运行 Windows®、X-Windows®、Solaris™ 和 KDE 等图形用户界面的目标服务器的桌面背景设置为常用的淡色图。应避免使用有照片或复杂渐变图案的背景。

确保 KX II-101-V2 支持目标服务器的视频分辨率和刷新速度，而且信号为逐行扫描。KX II-101-V2 支持下列分辨率：

分辨率	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @75Hz
640x400 @56Hz	1024x768 @90Hz
640x400 @84Hz	1024x768 @100Hz
640x400 @85Hz	1152x864 @60Hz
640x480 @60Hz	1152x864 @70Hz
640x480 @66.6Hz	1152x864 @75Hz
640x480 @72Hz	1152x864 @85Hz
640x480 @75Hz	1152x870 @75.1Hz
640x480 @85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz

分辨率	
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @56Hz	1280x960 @85Hz
800x600 @60Hz	1280x1024 @60Hz
800x600 @70Hz	1280x1024 @75Hz
800x600 @72Hz	1280x1024 @85Hz
800x600 @75Hz	1360x768@60Hz
800x600 @85Hz	1366x768@60Hz
800x600 @90Hz	1368x768@60Hz
800x600 @100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @60Hz	1600x1200 @60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

### Sun 视频分辨率

Sun™ 系统有两种分辨率设置，一种是命令行分辨率，另一种是图形用户界面分辨率。参看 [设置服务器视频分辨率](#) (p. 10)，了解 KX II-101-V2 支持的分辨率。

---

*注意：假如支持的分辨率均不起作用，要确保监视器是多同步监视器。某些监视器不使用 H&V 同步。*

---

命令行分辨率

#### ▶ 检查命令行分辨率：

1. 在根目录下运行下列命令：`# eeprom output-device`

#### ▶ 更改命令行分辨率：

1. 运行下列命令：`# eeprom output-device=screen:r1024x768x75`，其中 `1024x768x75` 是 KX II-101-V2 支持的任何分辨率。
2. 重新启动计算机。

图形用户界面分辨率/32 位

► **检查 32 位显示卡的图形用户界面分辨率：**

1. 运行下列命令：`# /usr/sbin/pgxconfig -prconf`

► **更改 32 位显示卡的图形用户界面分辨率：**

1. 运行下列命令：`# /usr/sbin/pgxconfig -res1024x768x75`，其中 `1024x768x75` 是 KX II-101-V2 支持的任何分辨率。
2. 重新启动计算机。

图形用户界面分辨率/64 位

► **检查 64 位显示卡的图形用户界面分辨率：**

1. 运行下列命令：`# /usr/sbin/m64config -prconf`

► **更改 64 位显示卡的分辨率：**

1. 运行下列命令：`# /usr/sbin/m64config -res1024x768x75`，其中 `1024x768x75` 是 KX II-101-V2 支持的任何分辨率。
2. 重新启动计算机。

图形用户界面分辨率/Solaris 8

► **检查 32 位显示卡和 64 位显示卡的 Solaris™ 8 分辨率：**

1. 运行下列命令：`# /usr/sbin/fbconfig -prconf`

► **更改 32 位显示卡和 64 位显示卡的 Solaris 8 分辨率：**

1. 运行下列命令：`# /usr/sbin/fbconfig -res1024x768x75`，其中 `1024x768x75` 是 KX II-101-V2 支持的任何分辨率。
2. 重新启动计算机。

### 鼠标设置

KX II-101-V2 可以在几种鼠标模式下工作：绝对鼠标同步™、智能鼠标模式和标准鼠标模式。

---

*注意：在使用智能鼠标模式时，不要使用动画鼠标。*

---

对于绝对鼠标同步，不必修改鼠标参数。对于标准鼠标模式和智能鼠标模式，必须将鼠标参数设置为特定值，本节讨论这些参数。

在不同的目标服务器操作系统上，鼠标配置会有差异。参看操作系统文档了解详情。

**Windows XP、Windows 2003 和 Windows 2008 设置****▶ 配置运行 Microsoft® Windows XP® 操作系统、Windows 2003® 操作系统或 Windows 2008® 操作系统的 KVM 目标服务器：**

1. 配置鼠标设置：
  - a. 选择“开始>控制面板>鼠标”。
  - b. 单击“指针选项”选项卡。
  - c. 在移动组上：
    - 把鼠标移动速度准确设置为中速。
    - 禁用“增强指针精度”选项。
    - 禁用“捕捉”选项。
    - 单击“确定”按钮。

---

*注意：在目标服务器上运行 Windows 2003 时，如果通过 KVM 访问服务器并执行下列任何操作，即使前面启用了鼠标同步，也可能造成鼠标不同步。为了再次启用鼠标同步，必须在客户机的“鼠标”菜单上选择“同步鼠标”命令。下列操作可能会导致失去鼠标同步：*

— 打开文本编辑器。

— 在 Windows 控制面板上访问“鼠标属性”、“键盘属性”及“电话和模式”选项。

---

2. 禁用过渡效果：
  - a. 在控制面板上选择“显示”。
  - b. 单击“外观”选项卡。
  - c. 单击“效果”。
  - d. 取消“菜单和工具提示使用下列过渡效果”选项。
  - e. 单击“确定”按钮。
3. 关闭控制面板。

---

注意：对于运行 Windows XP、Windows 2000 或 Windows 2008 的 KVM 目标服务器，你可能要创建一个在通过 KX II-101-V2 建立远程连接时使用的用户名。这样，可以把目标服务器的低速鼠标指针移动加速度设置仅限于 KX II-101-V2 连接。

Windows XP、2000 和 2008 登录页恢复到预设的鼠标参数，这些参数不同于为实现最佳 KX II-101-V2 性能而建议的参数。因此，鼠标同步对这些屏幕而言可能不是最佳方案。

注意：只有在你正确调整 Windows 目标服务器上的注册表之后，才继续下一步。可以用 Windows 注册表编辑器更改下列设置，使 KX II-101-V2 在登录页上具有更好的鼠标同步性能：HKey\_USERS\DEFAULT\Control Panel\Mouse: > MouseSpeed = 0; MouseThreshold 1=0; MouseThreshold 2=0。

---

### Windows 7 和 Windows Vista 设置

#### ► 配置运行 Windows Vista® 操作系统的 KVM 目标服务器：

1. 配置鼠标设置：
  - a. 选择“开始>设置>控制面板>鼠标”。
  - b. 在左边的导航面板上选择“高级系统设置”，打开“系统属性”对话框。
  - c. 单击“指针选项”选项卡。
  - d. 在移动组上：
    - 把鼠标移动速度准确设置为中速。
    - 禁用“增强指针精度”选项。
    - 单击“确定”按钮。
2. 禁用动画和淡化效果：
  - a. 在控制面板上选择“系统”选项。
  - b. 选择“性能信息”，然后选择“工具>高级工具>调节”，调节 Windows 外观和性能。
  - c. 单击“高级”选项卡。
  - d. 单击“性能”组里的“设置”按钮，打开“性能选项”对话框。
  - e. 在“定制”选项下取消下列复选框：
    - 动画选项：
      - 窗口用动画显示控件和元素
      - 在最大化和最小化窗口时用动画显示窗口
    - 淡化选项：

- 在视图中淡化或滑动菜单
  - 在视图中淡化或滑动工具提示
  - 在单击后让菜单项淡化
3. 单击确定按钮关闭控制面板。

► **配置运行 Windows 7® 操作系统的 KVM 目标服务器：**

1. 配置鼠标设置：
  - a. 选择 **Start (开始) > Control Panel (控制面板) > Mouse (鼠标)**。
  - b. 单击 **Pointer Options (指针选项)** 选项卡。
  - c. 在 **Motion (移动)** 组上：
    - 把 **Mouse Motion Speed (鼠标移动速度)** 准确设置为中速。
    - 禁用 **Enhanced pointer precision (增强指针精度)** 选项。
    - 单击 **OK (确定)** 按钮。
2. 禁用动画和淡化效果：
  - a. 选择 **Control Panel (控制面板) > System and Security (系统和安全)**。
  - b. 选择 **System(系统)**，在左边的导航面板上选择 **Advanced system settings (高级系统设置)**，打开 **System Properties (系统属性)** 对话框。
  - c. 单击 **Advanced (高级)** 选项卡。
  - d. 单击 **Performance (性能)** 组里的 **Settings (设置)** 按钮，打开 **Performance Options (性能选项)** 对话框。
  - e. 在 **Custom (定制)** 选项下取消下列复选框：
    - 动画选项：
      - **Animate controls and elements inside windows(窗口用动画显示控件和元素)**
      - **Animate windows when minimizing and maximizing(在最大化 and 最小化窗口时用动画显示窗口)**
    - 淡化选项：
      - **Fade or slide menus into view (在视图中淡化或滑动菜单)**
      - **Fade or slide ToolTips into view (在视图中淡化或滑动工具提示)**
      - **Fade out menu items after clicking (在单击后让菜单项淡化)**
3. 单击 **OK (确定)** 按钮，关闭 **Control Panel (控制面板)**。

## Windows 2000 设置

### ▶ 配置运行 Microsoft® Windows 2000® 操作系统的 KVM 目标服务器：

1. 配置鼠标设置：
  - a. 选择 Start (开始) > Control Panel (控制面板) > Mouse (鼠标)。
  - b. 单击 Motion (移动) 选项卡。
    - 将 Acceleration (加速度) 设置为 None (无)。
    - 将 Mouse Motion Speed (鼠标移动速度) 准确设置为中速。
    - 单击 OK (确定) 按钮。
2. 禁用过渡效果：
  - a. 在 Control Panel (控制面板) 上选择 Display (显示)。
  - b. 单击 Effects (效果) 选项卡。
    - 取消 Use the following transition effect for menus and tooltips (菜单和工具提示使用下列过渡效果) 选项。
3. 单击 OK (确定) 按钮，关闭 Control Panel (控制面板)。

---

*注意：对于运行 Windows XP、Windows 2000 或 Windows 2008 的 KVM 目标服务器，你可能要创建一个在通过 KX II-101-V2 建立远程连接时使用的用户名。这样，可以把目标服务器的低速鼠标指针移动/加速度设置仅限于 KX II-101-V2 连接。*

*Windows XP、2000 和 2008 登录页恢复到预设的鼠标参数，这些参数不同于为实现最佳 KX II-101-V2 性能而建议的参数。因此，鼠标同步对这些屏幕而言可能不是最佳方案。*

*注意：只有在你正确调整 Windows 目标服务器上的注册表之后，才继续下一步。可以用 Windows 注册表编辑器更改下列设置，使 KX II-101-V2 在登录页上具有更好的鼠标同步性能：HKey\_USERS\DEFAULT\Control Panel\Mouse: > MouseSpeed = 0; MouseThreshold 1=0; MouseThreshold 2=0。*

---

## Linux 设置 (Red Hat 4/5 和 Fedora 14)

*注意：下列设置仅针对标准鼠标模式进行过优化。*

### ▶ 配置运行 Linux® (图形用户界面) 的 KVM 目标服务器：

1. 配置鼠标设置：
  - a. 选择 Main Menu (主菜单) > Preferences (首选项) > Mouse (鼠标)，打开 Mouse Preferences (鼠标首选项) 对话框。



- b. 单击 Motion (移动) 选项卡。
- c. 在 Speed (速度) 组上把 Acceleration (加速度) 滑动条置于正中央。
- d. 在 Speed (速度) 组上降低 Sensitivity (灵敏度)。
- e. 在 Drag & Drop (拖放) 组上降低 Threshold (阈值)。
- f. 关闭 Mouse Preferences (鼠标首选项) 对话框。

---

*注意：如果这些步骤不起作用，按 Linux 命令行说明书中的说明，发出 `xset mouse 1 1` 命令。*

---

2. 配置屏幕分辨率：
  - a. 选择 Main Menu(主菜单) > System Settings(系统设置) > Display (显示)，打开 Display Settings (显示设置) 对话框。
  - b. 在 Display (显示) 选项卡上选择 KX II-101-V2 支持的分辨率。
  - c. 在 Advanced (高级) 选项卡上验证 KX II-101-V2 支持的刷新速度。

---

*注意：在连接目标服务器之后，在许多 Linux 图形环境下用 <Ctrl> <Alt> <+> 命令更改视频分辨率，滚动显示在 XF86Config 或 /etc/X11/xorg.conf 文件里启用的所有可用分辨率，视你的 X 服务器分发版本而定。*

---

#### ► 配置运行 Linux 的 KVM 目标服务器 (命令行)：

1. 把 Mouse Acceleration (鼠标加速度) 准确设置为 1，把 Threshold (阈值) 准确设置为 1。输入此命令：`xset mouse 1 1`。这些设置在登陆后执行。
2. 确保运行 Linux 的每台目标服务器使用 KX II-101-V2 支持的分辨率 (采用标准 VESA 分辨率和刷新速度)。
3. 还应该设置每台 Linux 目标服务器，使消隐时间在 VESA 标准值的 +/-40% 之内：
  - a. 转到 Xfree86 配置文件 XF86Config。
  - b. 用文本编辑器禁用 KX II-101-V2 不支持的所有分辨率。
  - c. 禁用 (KX II-101-V2 不支持的) 虚拟桌面功能。
  - d. 检查消隐时间 (VESA 标准值的 +/-40%)。
  - e. 重新启动计算机。

---

*注意：如果更改视频分辨率，必须退出目标服务器再登录，视频设置才生效。*

---

Red Hat 和 Fedora KVM 目标服务器注意事项

如果在使用 USB CIM 的目标服务器上运行 Red Hat®，且键盘和/或鼠标出问题，可以尝试其他配置设置。

---

*提示：即使操作系统是刚刚安装的，你可能也需要执行这些步骤。*

---

► **配置使用 USB CIM 的 Red Hat 服务器：**

1. 在系统里找到配置文件（通常是 `/etc/modules.conf`）。
2. 使用你喜欢的编辑器，确保 `modules.conf` 文件里的 `alias usb-controller` 行如下所示：

```
alias usb-controller usb-uhci
```

---

*注意：如果 `/etc/modules.conf` 文件中有另一行使用 `usb-uhci`，必须把此行删除或注释掉。*

---

3. 保存文件。
4. 重新启动系统，更改才会生效。

**Linux 设置（标准鼠标模式）**

---

*注意：下列设置仅针对标准鼠标模式进行过优化。*

---

► **配置运行 Linux®（图形用户界面）的 KVM 目标服务器：**

1. 配置鼠标设置：
  - a. Red Hat 5 用户选择 Main Menu（主菜单）> Preferences（首选项）> Mouse（鼠标），Red Hat 4 用户选择 System（系统）> Preferences（首选项）> Mouse（鼠标），打开 Mouse Preferences（鼠标首选项）对话框。
  - b. 单击 Motion（移动）选项卡。
  - c. 在 Speed（速度）组上把 Acceleration（加速度）滑动条置于正中央。
  - d. 在 Speed（速度）组上降低 Sensitivity（灵敏度）。
  - e. 在 Drag & Drop（拖放）组上降低 Threshold（阈值）。
  - f. 关闭 Mouse Preferences（鼠标首选项）对话框。

---

*注意：如果这些步骤不起作用，按 Linux 命令行说明书中的说明，发出 `xset mouse 1 1` 命令。*

---

2. 配置屏幕分辨率：
  - a. 选择 Main Menu(主菜单)> System Settings(系统设置)> Display (显示)，打开 Display Settings (显示设置)对话框。
  - b. 在 Setting (设置)选项卡上选择 KX II-101-V2 支持的分辨率。
  - c. 单击 OK (确定)按钮。

注意：在连接目标服务器之后，在许多 Linux 图形环境下用 `<Ctrl> <Alt> <+>` 命令更改视频分辨率，滚动显示在 `XF86Config` 或 `/etc/X11/xorg.conf` 文件里启用的所有可用分辨率，视你的 X 服务器版本而定。

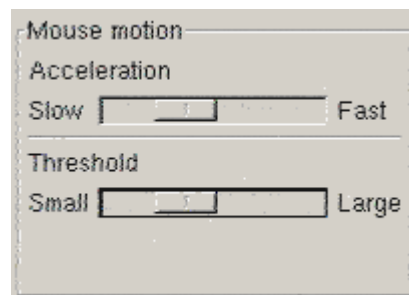
注意：如果更改视频分辨率，必须退出目标服务器再登录，视频设置才生效。

### Sun Solaris 设置

必须将 Solaris™ 目标服务器配置为 KX II-101-V2 支持的其中一个显示分辨率。Sun™ 机器支持的常用分辨率如下：

分辨率
1024x768@60Hz
1024x768@70Hz
1024x768@75Hz
1024x768@85Hz
1280x1024@60Hz

将 Mouse Acceleration (鼠标加速度)值精确设置为 1，将 Threshold (阈值)精确设置为 1。运行 Solaris 操作系统的目标服务器必须输出 VGA 视频 (H&V 同步，而非复合同步)。这既可以在图形用户界面上设置，也可以用命令行命令 `xset mouse a t` 设置，其中 `a` 是加速度，`t` 是阈值。



### ► 将 Sun 视频卡输出由复合同步更改为非默认的 VGA 输出：

1. 发出 Stop+A 命令进入 bootprom 模式。

2. 发出 `#EEPROM output-device=screen:r1024x768x75` 命令更改输出分辨率。
3. 发出 `boot` 命令重新启动服务器。

也可以联系 Raritan 代表购买视频输出适配器。使用复合同步输出的 Sun 服务器，需要配备 APSSUN II Raritan Guardian 转换器才能使用 KX II-101-V2。使用不同的复合同步输出的 HD15 Sun 服务器，需要配备 APKMSUN Raritan Guardian 转换器才能使用 KX II-101-V2。

### **Apple Macintosh 设置**

Mac® 可与 KX II-101-V2 一起工作，但必须使用绝对鼠标同步，并在 KX II-101-V2 Port（端口）页上针对 Mac 服务器启用绝对鼠标模式和鼠标缩放。

#### **▶ 启用此设置：**

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
2. 单击要编辑的端口的端口名称。
3. 在 USB Connection Settings（USB 连接设置）部分选择 Enable Absolute Mouse（启用绝对鼠标）复选框和 Enable Absolute mouse scaling for MAC server（针对 Mac 服务器启用绝对鼠标缩放）复选框。单击 OK（确定）按钮。

参看 [端口配置](#) (p. 119)。

### **IBM AIX 设置**

1. 转到 Style Manager（式样管理器）。
2. 单击 Mouse Settings（鼠标设置），将 Mouse acceleration（鼠标加速度）设置为 1.0，将 Threshold（阈值）设置为 3.0。

---

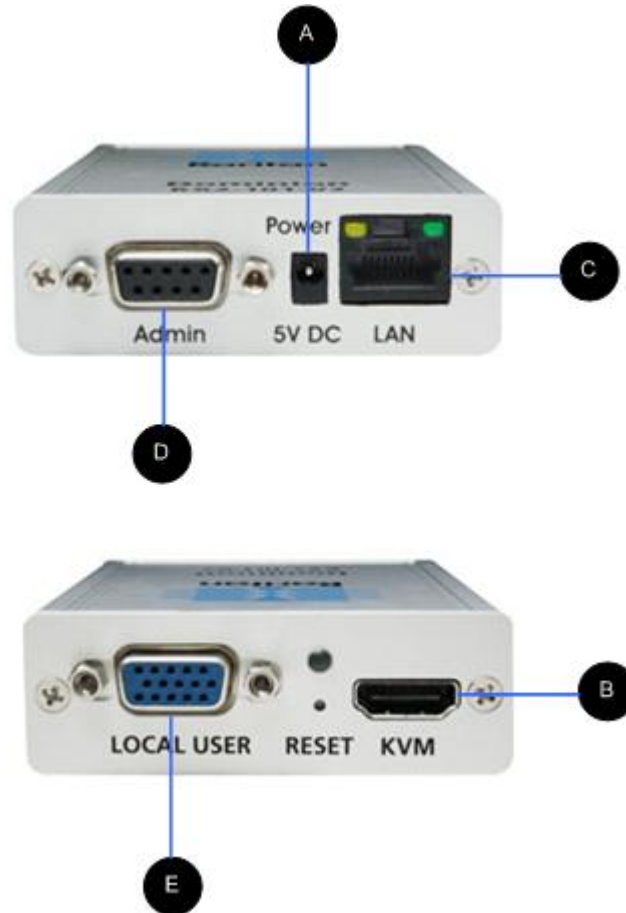
## **第二步：配置网络防火墙设置**

如要通过网络防火墙访问 KX II-101-V2，防火墙必须允许通过 TCP 端口 5000 进行通信。还可以配置 KX II-101-V2 使用另一个你自己指定的 TCP 端口。

为了充分利用 KX II-101-V2 的 Web 访问功能，防火墙必须允许通过 TCP 端口 443 接受入站通信，这是用于 HTTPS 通信的标准 TCP 端口。为了充分利用 KX II-101-V2 的 HTTP 到 HTTPS 重定向（用户可以输入更常用的 `http://xxx.xxx.xxx.xxx`，而不是 `https://xxx.xxx.xxx.xxx`），防火墙还必须允许通过 TCP 端口 80 接受入站通信，这是用于 HTTP 通信的标准 TCP 端口。

### 第三步：连接设备

KX II-101-V2 的物理连接如下图所示。图中的每个字母对应在此介绍的一个设备连接步骤。



#### 图示符号

A	电源连接器	单电源适配器。
B	配有监视器连接器 PS/2 连接器和 USB 连接器的 KVM 电缆（提供）	把随机提供的 KVM 电缆插入目标服务器的键盘端口、视频端口和鼠标端口。
C	Ethernet LAN	提供 LAN 连接。

图示符号

<b>D</b>	Admin (管理) 端口	用于执行下列操作之一： <ul style="list-style-type: none"><li>• 用 PC 上的终端仿真程序配置和管理设备。</li><li>• 配置和管理电源条 (需要适配器, 得另外购买)。</li><li>• 连接外置调制解调器, 拨号连接该设备。</li></ul>
<b>E</b>	Local user (本地用户)	本地端口连接监视器。

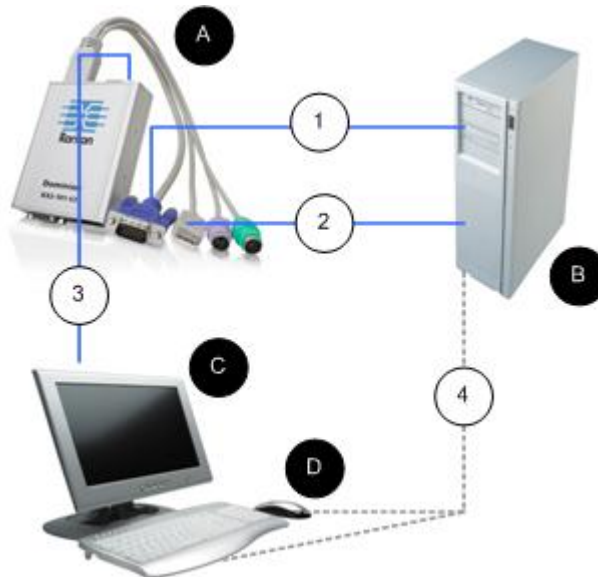
**A: 电源**

用随附的 100-240VAC 输入和 5VDC 输出电源适配器给 KX II-101-V2 供电。对于标准交流电源, 将随附的交流电源适配器插入 Power (电源) 端口, 将另一端插入交流电源插座。

**B: 目标服务器**

用 PS/2 或 USB 连接目标服务器。在连接目标服务器之前, 将目标服务器的视频配置为支持的分辨率。如果使用虚拟媒体或绝对鼠标模式, 必须使用 USB 连接。

**USB 配置**



► **配置 KX II-101-V2 使用 USB 目标服务器：**

1. 随设备附带有 KVM 线缆，其视频接口连接目标服务器视频端口。
2. KVM 线缆的 USB 接口接目标服务器的 USB 端口。
3. 如果必须使用本地视频，把监视器连接到 KX II-101-V2 Local User (本地用户) 端口。**可选**
4. 把 USB 键盘和鼠标直接连接到目标服务器。**可选**

---

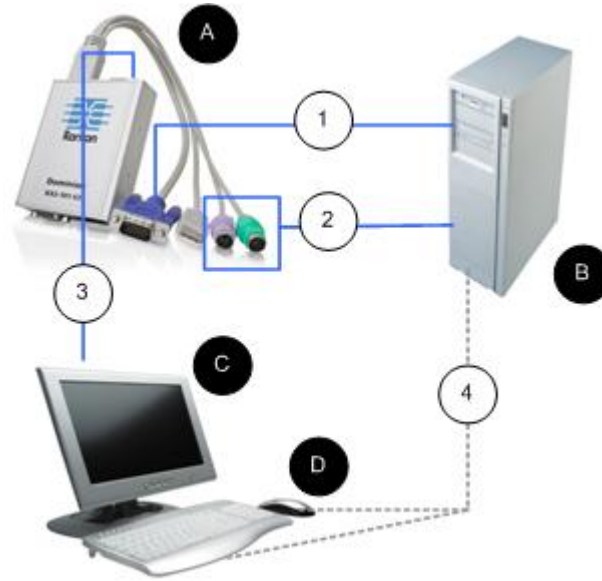
*注意：如果使用虚拟媒体，必须使用 USB 连接。*

---

**USB 连接图示符号**

	KX II-101-V2
	目标服务器
	本地监视器 (可选)。
	本地鼠标和键盘 (可选)
	KX II-101-V2 到目标服务器的视频连接
	KX II-101-V2 到目标服务器的 USB 连接
	KX II-101-V2 Local User (本地用户) 端口到监视器的可选监视器连接
	目标服务器到鼠标和键盘的可选 USB 连接(不提供电缆)

### PS/2 配置



#### ► 配置 KX II-101-V2 使用 PS/2 目标服务器：

1. 随设备附带有 KVM 线缆，其视频接口连接目标服务器视频端口。
2. KVM 线缆的 USB 接口接目标服务器的 USB 端口。
3. 如果必须使用本地视频，把监视器连接到 KX II-101-V2 Local User (本地用户) 端口。**可选**
4. 如果使用 PS/2 键盘和鼠标，用 PS/2 适配器 (不提供) 直接连接目标服务器的 USB 端口。**可选**

*注意：如果使用虚拟媒体，必须使用 USB 连接。*

#### PS/2 连接图示符号

	KX II-101-V2
	目标服务器
	本地监视器
	本地鼠标和键盘 (可选)
	KX II-101-V2 到目标服务器的视频连接



PS/2 连接图示符号	
2	KX II-101-V2 到目标服务器的 KVM 电缆连接
3	可选的 KX II-101-V2 到监视器连接
4	目标服务器到键盘和鼠标的可选 PS/2-USB 适配器连接（不提供电缆）

### C:网络

用标准 Ethernet 网线把标有 LAN 的网络端口连接到 Ethernet 交换机、集线器或路由器。Ethernet 连接上面的 LAN LED 显示 Ethernet 活动情况。在使用 KX II-101-V2 时，黄色 LED 闪烁，表示 IP 流量为 10Mbps。绿色指示灯表示 100Mbps 连接速度。

### D:管理端口

管理端口允许你使用 HyperTerminal 等终端仿真程序进行 KX II-101-V2 配置和设置。Use one DB9M to DB9F straight serial cable to connect from the KX II-101-V2 to the serial port on your PC or laptop.应该如下配置串行端口通信设置：

- 115,200 波特率
- 8 数据位
- 1 停止位
- 无奇偶校验
- 无流控制

### E:本地用户端口

Local User（本地用户）端口充当至目标服务器的直通端口，以便直接连接监视器。本地键盘和鼠标必须直接连接目标服务器。

对于 USB 配置，只有本地视频通过 Local User（本地用户）端口连接目标服务器。键盘和鼠标通过 USB 端口直接连接目标服务器。

---

### 第四步：配置 KX II-101-V2

---

*注意：如果通过网络浏览器配置 KX II-101-V2，必须用交叉电缆连接 KX II-101-V2 和客户机。*

---

### 用 Remote Console 配置 KX II-101-V2

KX II-101-V2 Remote Console 是基于 Web 的应用程序，你可以在配置设备之后，在使用和管理设备之前用它配置设备。在用 Remote Console 配置 KX II-101-V2 之前，必须将工作站和设备与网络相连。

也可以用终端仿真程序配置 KX II-101-V2。参看[用终端仿真程序配置 KX II-101-V2 \(可选\)](#) (p. 30)。

#### 设置新密码

在首次登录 Remote Console 时，系统提示你设置新密码取代默认密码，然后可以配置 KX II-101-V2。

1. 登录到与 KX II-101-V2 设备相连的工作站。
2. 启动支持的网络浏览器，例如 Internet Explorer® (IE) 或 Firefox®。
3. 在浏览器地址栏输入设备的默认 IP 地址：192.168.0.192。
4. 按 Enter 键，打开登录页面。
5. 输入用户名 admin 和密码 raritan。
6. 单击 Login (登录) 按钮，打开 Change Password (更改密码) 页。
7. 在 Old Password (旧密码) 字段里输入 raritan。
8. 在 New Password (新密码) 字段和 Confirm New Password (确认新密码) 字段里输入新密码。密码最长为 64 个字符，可以包含英文字母数字字符和可打印的特殊字符。
9. 单击 Apply (应用) 按钮。显示确认信息，说明密码更改成功。
10. 单击 OK (确定) 按钮，打开 Port Access (端口访问) 页。

#### 分配 IP 地址

下列步骤说明如何在 Network Settings (网络设置) 页上分配 IP 地址。参看[网络设置](#) (p. 99) 全面了解本页上的所有字段和操作。

#### ▶ 分配 IP 地址：

1. 选择 Device Settings (设备设置) > Network (网络)，打开 Network Settings (网络设置) 页。
2. 给 KX II-101-V2 设备指定有意义的设备名称。名称最长 32 个字母数字字符，可以使用有效特殊字符，但不能使用空格。
3. 在 IPv4 部分输入或选择合适的 IPv4 网络设置：
  - a. 必要时在 IP Address (IP 地址) 字段里输入 IP 地址。默认 IP 地址是 192.168.0.192。

- b. 在 Subnet Mask (子网掩码) 字段里输入子网掩码。默认子网掩码是 255.255.255.0。
  - c. 如果在 IP Auto Configuration (IP 自动配置) 下拉列表上选择了 None (无), 在 Default Gateway (默认网关) 字段里输入默认网关。
  - d. 如果在 IP Auto Configuration (IP 自动配置) 下拉列表上选择了 DHCP, 在 Preferred DHCP Host Name (首选 DHCP 主机名) 字段里输入首选 DHCP 主机名。
  - e. 选择 IP Auto Configuration (IP 自动配置)。有三个选项可供选择：
    - None (Static IP) (无[静态 IP]) — 此选项要求你人工指定网络参数。  
建议你选择此选项, 因为 KX II-101-V2 是基础设施设备, 其 IP 地址不应发生变化。
    - DHCP — 联网计算机 (客户机) 用 Dynamic Host Configuration Protocol (动态主机配置协议) 获取 DHCP 服务器分配的唯一 IP 地址和其他参数。  
如果选择此选项, DHCP 服务器分配网络参数。如果使用 DHCP, 在 Preferred host name (首选主机名) 字段里输入首选主机名 (仅限于 DHCP)。最长 63 个字符。
4. 如果要使用 IPv6, 在 IPv6 部分输入或选择合适的 IPv6 网络设置：
- a. 选择 IPv6 复选框, 激活这部分的字段。
  - b. 在 Global/Unique IP Address (全局/唯一 IP 地址) 字段里输入全局/唯一 IP 地址。这是给 KX II-101-V2 分配的 IP 地址。
  - c. 在 Prefix Length (前缀长度) 字段里输入前缀长度。这是 IPv6 地址使用的位数。
  - d. 在 Gateway IP Address (网关 IP 地址) 字段里输入网关 IP 地址。
  - e. Link-Local IP Address (链路-本地 IP 地址)。自动给设备分配此地址, 用于发现邻居, 或者在没有路由器时使用。只读
  - f. Zone ID (域 ID)。标识与此地址关联的设备。只读
  - g. 选择 IP Auto Configuration (IP 自动配置)。有三个选项可供选择：
    - None (无) — 如果不想使用自动 IP 配置, 而是自己设置 IP 地址 (静态 IP), 使用此选项。这是默认选项, 建议使用此选项。

如果给 IP auto configuration (IP 自动配置) 选择 None (无)，后用下列网络基本设置字段：Global/Unique IP Address (全局/唯一 IP 地址)、Prefix Length (前缀长度) 和 Gateway IP Address (网关 IP 地址)，你可以人工设置 IP 配置。

- Router Discovery (路由器发现) — 用此选项自动分配 IPv6 地址，这些地址具有 Global (全局) 或 Unique Local (唯一本地) 意义，超出了 Link Local (链路本地) 的意义，仅适用于直接连接的子网。
5. 如果选择了 DHCP 并启用了 Obtain DNS Server Address (获取 DNS 服务器地址)，选择 Obtain DNS Server Address Automatically (自动获取 DNS 服务器地址)。在选择 Obtain DNS Server Address Automatically (自动获取 DNS 服务器地址) 之后，将使用 DHCP 服务器分配的 DNS 信息。
  6. 如果选择了 Use the Following DNS Server Addresses (使用下列 DNS 服务器地址)，无论是否选择了 DHCP，均用在此输入的地址连接 DNS 服务器。

如果选择了 Use the Following DNS Server Addresses (使用下列 DNS 服务器地址) 选项，输入下列信息。这些地址分别是主 DNS 地址和备用 DNS 地址，当主 DNS 服务器连接由于中断而断开时，将使用备用 DNS 地址。

- a. Primary DNS Server IP Address (主 DNS 服务器 IP 地址)
  - b. Secondary DNS Server IP Address (备用 DNS 服务器 IP 地址)
7. 在填写完之后，单击 OK (确定) 按钮。

参看 **LAN 接口设置** (p. 103) 了解如何配置 Network Settings (网络设置) 页的这个部分。

---

*注意：在某些环境下，默认 LAN Interface Speed & Duplex (LAN 接口速度和双工) 设置中的 Autodetect (autonegotiator) (自动检测[自动协商]) 并不能正确设置网络参数，会引发网络问题。在这些情况下，把 KX II-101-V2 LAN Interface Speed & Duplex (KX II-101-V2 LAN 接口速度和双工) 设置为 100 Mbps/Full Duplex (全双工) 或与网络相适应的其他选项，可以解决这个问题。参看 **网络设置** (p. 99) 页了解详情。*

---

#### **命名目标服务器**

1. 将 KX II-101-V2 连接到目标服务器。
2. 选择 Device Settings (设备设置) > Port Configuration (端口配置)，打开 Port Configuration (端口配置) 页。
3. 单击连接目标服务器所用的端口名称，打开 Port (端口) 页。
4. 输入名称，最多 32 个字母数字字符和特殊字符。

5. 单击 OK (确定) 按钮。

**Port 1**

Type:  
KVM

Name:  
Dominion\_KX2\_101\_Port1

**Power Association**

<b>Power Strip Name</b>	<b>Outlet Name</b>
None ▾	--- ▾
	--- ▾
	--- ▾
	--- ▾

▶ USB Connection Settings

▶ Advanced USB Connection Settings

### 远程验证

#### CC-SG 用户注意事项

在用 CommandCenter Secure Gateway 控制 KX II-101-V2 时，CC-SG 要验证用户和用户组。

参看 **CommandCenter Secure Gateway 用户指南**、**CommandCenter Secure Gateway 管理员指南**或 **CommandCenter Secure Gateway 部署指南**详细了解 CC-SG 验证，这些指南均可在 Raritan 网站 ([www.raritan.com](http://www.raritan.com)) 的 Support (支持) 页上找到。

#### 支持的协议

为了简化用户名和密码管理，KX II-101-V2 可以将验证请求转发到外部验证服务器。支持两种外部验证协议：LDAP/LDAPS 和 RADIUS。

#### Microsoft Active Directory 注意事项

Microsoft® Active Directory® 在本机使用 LDAP/LDAPS 协议，可以充当 LDAP/LDAPS 服务器和 KX II-101-V2 验证源。如果 Microsoft Active Directory 有 IAS (Internet Authorization Server) 组件，Microsoft Active Directory 服务器还可以充当 RADIUS 验证源。

### 创建用户组和用户

为了让用户访问 KX II-101-V2，必须定义用户组和用户，这是初始配置的一部分。

KX II-101-V2 使用系统提供的默认用户组，允许你根据需要创建用户组，并指定适当的权限。

访问 KX II-101-V2 需要用户名和密码。当用户尝试访问 KX II-101-V2 时，要用这些信息验证用户。参看**用户管理 (p. 78)**，详细了解如何添加和编辑用户组和用户。

### 用终端仿真程序配置 KX II-101-V2 (可选)

可以用管理串行控制台和 HyperTerminal 等终端仿真程序设置 KX II-101-V2 的下列配置参数。

- IP address (IP 地址)
- Subnet mask address (子网掩码地址)
- Gateway address (网关地址)
- IP autoconfiguration (IP 自动配置)
- LAN speed (LAN 速度)
- LAN interface mode (LAN 接口模式)

为了与 KX II-101-V2 一起使用终端仿真程序，必须先用随机提供的 RS-232 串行电缆连接 KX II-101-V2 的 Admin (管理) 端口和 PC 的 COM 端口。

为了说明问题，本节以 HyperTerminal 为例说明终端仿真程序。你可以使用任何终端仿真程序。

#### ▶ 用终端仿真程序配置 KX II-101-V2 :

1. 把 KX II-101-V2 连接到本地计算机。
2. 将 KX II-101-V2 的 Admin (管理) 端口连接到 PC 的 COM1 端口。
3. 启动要用于配置 KX II-101-V2 的终端仿真程序：
4. 用终端仿真程序设置下列端口设置：
  - Bits per second (比特率) — 115200
  - Data bits (数据位) — 8
  - Parity (奇偶校验) — None (无)
  - Stop bits (停止位) — 1
  - Flow control (流控制) — None (无)

5. 连接 KX II-101-V2。打开登录页面。
6. 输入管理员用户名，然后按 **Enter** 键。系统提示你输入密码。
7. 输入默认管理员用户名 *admin*，然后按 **Enter** 键。系统提示你输入密码。
8. 在 **Admin Port >** 提示下输入 *config*，然后按 **Enter** 键。
9. 在 **Config >** 提示下输入 *network*，然后按 **Enter** 键。
10. 如要配置新网络设置，在 **Network** 提示下输入 *interface*，后跟下列其中一个命令及其适当的自变量（选项），然后按 **Enter** 键。

命令	自变量	选项
ipauto	none dhcp	<p><b>none</b> — 允许你人工指定设备的 IP 地址。必须在此选项之后使用 <b>ip</b> 命令和 IP 地址，如下列示例所示：</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p><b>dhcp</b> — 在启动时自动给设备分配 IP 地址。</p> <pre>interface ipauto dhcp</pre>
ip	IP address	给设备分配的 IP 地址。在首次人工设置 IP 地址时，必须使用此命令与 <b>ipauto</b> 命令和 <b>none</b> 选项。参看 <b>ipauto</b> 了解详情。在人工分配 IP 地址之后，可以单独用 <b>ip</b> 命令更改 IP 地址。
mask	subnet mask	<p>命令列应该是 "interface"</p> <pre>interface   ip   ...</pre> <p><b>interface   mask  </b> 子网掩码 IP 地址</p> <p><b>interface   gw  </b> 网关 IP 地址</p> <pre>interface   mode   ....</pre>
gw	IP address	网关 IP 地址。
mode	mode	<p>Ethernet 模式。可以使用下列选项：</p> <ul style="list-style-type: none"> <li>▪ <b>auto</b> — 自动根据网络</li> </ul>

命令	自变量	选项
		设置速度和接口模式。 <ul style="list-style-type: none"><li>▪ 10hdx — 10Mbps 半双工</li><li>▪ 10fdx — 10Mbps 全双工</li><li>▪ 100hdx — 100Mbps 半双工</li><li>▪ 100fdx — 100Mbps 全双工</li></ul>

在成功更改设置之后，显示下面这样的确认消息：

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

Network interface configuration successful (网络接口
配置成功)。
```

在完成 KX II-101-V2 配置之后，在命令提示下输入 *logout*，然后按 **Enter** 键退出命令行界面。



## 在本章内

界面.....	33
Virtual KVM Client (VKC).....	41

---

 界面
 

---



---

**KX II-101-V2 Remote Console 界面**

KX II-101-V2 Remote Console 是基于浏览器的图形用户界面，便于你登录与 KX II-101-V2 相连的 KVM 目标服务器和串行目标，远程管理 KX II-101-V2。

KX II-101-V2 Remote Console 提供一个数字连接来连接相连的 KVM 目标服务器。在用 KX II-101-V2 Remote Console 登录 KVM 目标服务器时，打开 Virtual KVM Client 窗口。

*注意：如果用 Internet Explorer® 7 尝试连接目标服务器，可能会遇到权限问题。执行下列操作避免出问题：*

1. 单击 Internet Explorer 上的 Tools (工具) > Internet Options (Internet 选项)，打开 Internet Options (Internet 选项) 对话框。
  2. 单击 Temporary Internet files (Internet 临时文件) 部分的 Settings (设置) 按钮打开 Settings (设置) 对话框。
  3. 在 Check/Uncheck Selected Rows (检查/不检查选择的行) 部分选择 Automatically (自动) 复选框。
  4. 单击 OK (确定) 按钮应用设置。
- 

**启用直接端口访问**

直接端口访问允许你直接访问 KX II-101-V2 Remote Client，无需使用常用的登录页。在启用直接端口访问之后，可以定义一个 URL，直接转到 Port Access (端口访问) 页。

▶ **启用直接端口访问：**

1. 启动 KX II-101-V2 Remote Console。
2. 选择 Device Settings (设备设置) > Device Services (设备服务)，打开 Device Services (设备服务) 页。

3. 选择 **Enable Direct Port Access via URL** (启用通过 URL 进行直接端口访问) 复选框。
4. 单击 **Save** (保存) 按钮。

▶ **定义直接端口访问 URL :**

- 用 **KX II-101-V2** 的 IP 地址、用户名、密码和端口号 (必要时) 定义一个 URL。

直接端口访问 URL 的格式如下：

```
https://IP  
address/dpa.asp?username=username&password=password
```

---

提示：在定义直接端口访问 URL 之后，在浏览器里把它保存成书签，便于重复使用。

---

**KX II-101-V2 控制台导航**

KX II-101-V2 控制台界面有多种导航方法和选择方法。

▶ **选择一个选项 (使用下列其中一种方法) :**

- 单击一个选项卡。显示一页可用选项。
- 让光标停留在选项卡上，在菜单上选择合适的选项。
- 在分层显示的菜单 (浏览路径) 上直接选择选项。

▶ **多屏幕页面翻页 :**

- 使用键盘上的 **Page Up** 和 **Page Down** 键。
- 使用右边的滚动条。

**左面板**

KX II-101-V2 界面的左面板包含下列信息。注意某些信息是有条件的，只有在你是某类用户并使用某些功能时，才显示这些信息。在此注明这些有条件的信息。

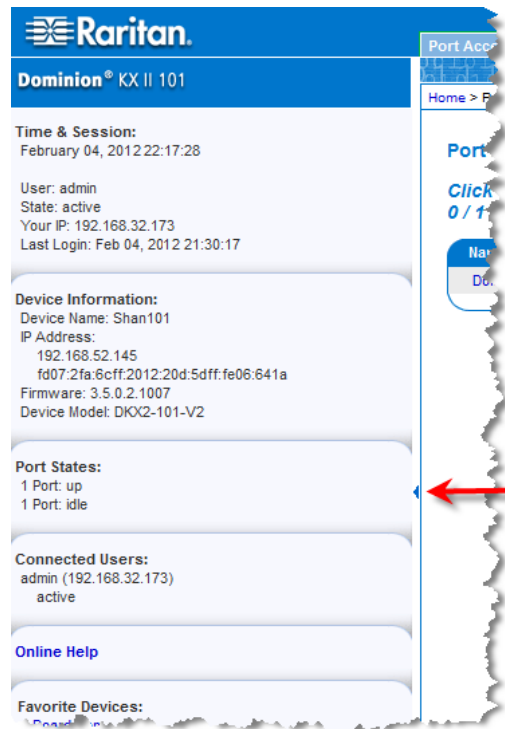
信息	说明	何时显示？
Time & Session (时间和会话)	当前日期和时间	始终
User (用户)	当前用户的用户名	始终

信息	说明	何时显示？
State (状态)	闲置或活动应用程序的当前状态。如果应用程序闲置,它跟踪并显示会话闲置了多长时间。	始终
Your IP (你的 IP)	访问 KX II-101-V2 所用的 IP 地址。	始终
Last Login (上次登录时间)	当前用户上次登录日期和时间。	始终
Under CC-SG Management (受 CC-SG 管理)	负责管理 KX II-101-V2 的 CC-SG 设备的 IP 地址。	当 KX II-101-V2 受 CC-SG 管理时
设备信息	你使用的 KX II-101-V2 的特定信息。	始终
Device Name (设备名称)	给设备指定的名称。	始终
IP Address (IP 地址)	KX II-101-V2 的 IP 地址。	始终是 IPv4 地址,如果配置了 IPv6 还包括 IPv6 地址
Firmware (固件)	当前固件版本。	始终
Device Model (设备型号)	KX II-101-V2 的型号	始终
Port States (端口状态)	KX II-101-V2 使用的端口的状态。	始终
Connect Users (连接用户)	用用户名和 IP 地址标识的、当前连接 KX II-101-V2 的用户。	始终
Online Help (联机帮助)	联机帮助链接。	始终
Favorite Devices (收藏夹设备)	参看管理收藏夹。	始终
FIPS Mode (FIPS 模式)	FIPS 模式: 启用 SSL 证书: 符合 FIPS 模式	在启用 FIPS 时

左面板可以折叠起来增大页面显示面积。

▶ **折叠左面板：**

- 单击左面板中间位置指向左边的蓝色箭头。在折叠左面板之后，可以再次单击蓝色箭头展开面板。



**端口访问页**

在成功登录 KX II-101-V2 Remote Console 之后，打开 Port Access（端口访问）页。本页列出 KX II-101-V2 端口、相连的 KVM 目标服务器及其可用性。Port Access（端口访问）页提供对与 KX II-101-V2 相连的目标服务器的访问。KVM 目标服务器是要通过 KX II-101-V2 设备控制的服务器，它们连接 KX II-101-V2 背板上的端口。

▶ **使用端口访问页：**

1. 单击 KX II-101-V2 Remote Console 上的 Port Access（端口访问）选项卡。打开 Port Access（端口访问）页。显示下列信息：
  - Port Name（端口名称）— KX II-101-V2 端口名称。端口名称最初设置为 Dominion\_KX2\_101\_Port1，但可以将名称更改为更具说明性的名称。单击 Port Name（端口名称）链接打开 Port Action（端口操作）菜单。

- **Availability** (可用性) — 可用性可以是 **Idle** (空闲)、**Connected** (已连接) 或 **Busy** (忙)。
2. 单击要访问的目标服务器对应的端口名称，显示“端口操作”菜单。参看 **端口操作菜单** (p. 37) 详细了解可用菜单项。
  3. 在“端口操作”菜单上选择期望的菜单命令。

### 端口操作菜单

在单击“端口访问”列表上的端口名称时，显示“端口操作”菜单。选择要针对此端口执行的菜单项。注意“端口操作”菜单只列出当前可用的菜单项，视端口状态和可用性而定：

- **Connect** (连接) — 建立至目标服务器的新连接。对于 **KX II-101-V2 Remote Console**，打开新的 **Virtual KVM Client (VKC)** (p. 41) 页。
- **Disconnect** (断开) — 断开此端口，关闭此目标服务器对应的 **Virtual KVM Client** 页。只有在端口状态是工作和连接或工作和忙时，才能使用此菜单项。
- **Power On** (通电) — 通过关联出口给目标服务器通电。只有在目标服务器有一个或多个电源关联，用户有权操作此服务时，才显示此选项。
- **Power Off** (断电) — 通过关联出口断开目标服务器电源。只有在目标服务器有一个或多个电源关联，目标服务器通电（端口状态为工作），用户有权操作此服务时，才显示此选项。
- **Power Cycle** (重新通电) — 通过关联出口给目标服务器重新通电。只有在目标服务器有一个或多个电源关联，用户有权操作此服务时，才显示此选项。

### 管理收藏夹

有一个收藏夹功能，便于你组织管理和迅速访问常用设备。“收藏夹设备”部分位于“端口访问”页左下角（侧面工具栏），便于你：

- 创建和管理收藏夹设备列表
- 迅速访问常用设备
- 按设备名称、IP 地址或 DNS 主机名列出收藏夹
- 发现子网上的 KX II-101-V2 设备（在登录前后）
- 在连接的 Dominion 设备上检索发现的 KX II-101-V2 设备（登录后）

#### ▶ 访问收藏夹 KX II-101-V2 设备：

- 单击设备名称（位于 Favorite Devices[收藏夹设备]）下面。打开该设备对应的新浏览器窗口。

#### ▶ 按名称显示收藏夹：

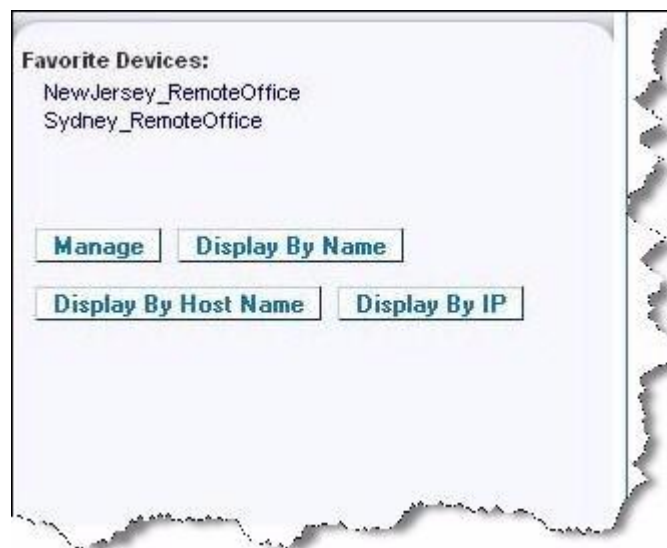
- 单击 Display by Name（按名称显示）。

#### ▶ 按 IP 地址显示收藏夹：

- 单击 Display by IP（按 IP 地址显示）。

#### ▶ 按主机名显示收藏夹：

- 单击 Display by Host Name（按主机名显示）。



**管理收藏夹页****▶ 打开“管理收藏夹”页：**

- 单击左面板上的“管理”按钮，打开“管理收藏夹”页，本页包含下列选项：

使用：	操作：
收藏夹列表	管理收藏夹设备的列表。
发现设备 — 本地子网	发现客户机 PC 本地子网上的 Raritan 设备。
发现设备 — KX II-101-V2 子网	发现 KX II-101-V2 设备子网上的 Raritan 设备。
把设备添加到收藏夹	在收藏夹列表上添加、编辑和删除设备。

**收藏夹列表页**

在“收藏夹列表”页上，可以在收藏夹列表上添加、编辑和删除设备。

**▶ 打开收藏夹列表页：**

- 选择“管理>收藏夹列表”，打开“收藏夹列表”页。

**发现本地子网上的 Raritan 设备**

此选项发现本地子网上的设备，即 KX II-101-V2 Remote Console 运行的子网上的设备。可以在本页上直接访问这些设备，也可以把它们添加到收藏夹列表上。参看 [收藏夹列表页](#) (p. 39)。

**▶ 发现本地子网上的设备：**

- 选择“管理>发现设备 — 本地子网”，打开“发现设备 — 本地子网”页。
- 选择合适的发现端口：
  - 如要使用默认发现端口，选择“使用默认端口 5000”复选框。
  - 使用不同的发现端口：
    - 取消“使用默认端口 5000”复选框。
    - 在“发现端口”字段里输入端口号。
    - 单击“保存”按钮。
- 单击“刷新”按钮，刷新本地子网设备列表。

▶ **把设备添加到收藏夹列表：**

1. 选择设备名称/IP 地址旁边的复选框。
2. 单击“添加”按钮。

▶ **访问被发现的设备：**

单击设备的设备名称或 IP 地址，打开设备对应的新浏览器窗口。

**发现 KX II-101-V2 子网上的 Raritan 设备**

此选项发现设备子网上的设备，即 KX II-101-V2 设备 IP 地址所在的子网上的设备。可以在本“子网”页上直接访问这些设备，也可以把它们添加到收藏夹列表上。参看 [收藏夹列表页](#) (p. 39)。

此功能允许多台 KX II-101-V2 设备自动互操作和自动伸缩。KX II-101-V2 Remote Console 自动发现 KX II-101-V2 子网上的 KX II-101-V2 设备和其他任何 Raritan 设备。

▶ **发现设备子网上的设备：**

1. 选择“管理>发现设备 — KX II-101-V2 子网”，打开“发现设备 — KX II-101-V2 子网”页。
2. 单击“刷新”按钮，刷新本地子网设备列表。

▶ **把设备添加到收藏夹列表：**

1. 选择设备名称/IP 地址旁边的复选框。
2. 单击“添加”按钮。

▶ **访问被发现的设备：**

- 单击设备的设备名称或 IP 地址，打开设备对应的新浏览器窗口。

**添加、编辑和删除收藏夹**

▶ **把设备添加到收藏夹列表：**

1. 选择“管理>把新设备添加到收藏夹”，打开“添加新收藏夹”对话框。
2. 输入有意义的说明。
3. 在“IP 地址/主机名”字段里输入设备 IP 地址/主机名。
4. 必要时更改端口字段里的发现端口。
5. 选择“产品类型”。
6. 单击“确定”按钮，把设备添加到收藏夹列表。



#### ▶ 编辑收藏夹：

1. 在“收藏夹列表”页上选择要编辑的 KX II-101-V2 设备旁边的复选框。
2. 单击“编辑”按钮，打开“编辑”页。
3. 按需要更新字段：
  - 说明
  - IP 地址/主机名 — 输入 KX II-101-V2 设备的 IP 地址
  - 端口（如有必要）
  - 产品类型
4. 单击“确定”按钮。

#### ▶ 删除收藏夹：

---

**重要说明：在删除收藏夹时务必要谨慎，系统不提示你确认删除。**

---

1. 选择要删除的 KX II-101-V2 旁边的复选框。
2. 单击“删除”按钮，把收藏夹从收藏夹列表上删除掉。

#### 注销

#### ▶ 退出 KX II-101-V2：

- 单击页面右上角的 Logout（退出）。

---

*注意：在退出时，同时关闭打开的任何 Virtual KVM Client 会话和串行客户机会话。*

---

#### Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) 是 Raritan 产品系列的图形用户界面，用于远程访问那些通过 IP 设备与 Raritan KVM 相连的目标服务器。参看 Raritan 网站上的 **KVM 和串行访问客户机指南** 详细了解如何使用 MPC，它与用户指南在同一个网页上。这里说明如何启动 MPC。

请注意多种 Raritan 产品使用此客户机。因此，在本节帮助中可能引用其他产品。

---

### Virtual KVM Client (VKC)

请注意多种 Raritan 产品使用此客户机。因此，在本节帮助中可能引用其他产品。

### 概述

无论何时用 Remote Console 访问目标服务器，都打开 Virtual KVM Client (VKC) 窗口。对于每台连接的目标服务器，均有一个 Virtual KVM Client。可以通过 Windows® 任务栏访问这些窗口。

Virtual KVM Client 窗口可以最小化和最大化，可以在计算机桌面上移动位置。

*注意：在刷新 HTML 浏览器时，将关闭 Virtual KVM Client 连接，所以要慎重。*





*注意：如果使用 FireFox 3.0.3，在启动应用程序时可能会出问题。如有问题，可以清除浏览器高速缓存，再启动应用程序。*

### 连接 KVM 目标服务器


#### ▶ 连接 KVM 目标服务器：

1. 单击 KX II-101-V2 Remote Console 上的 Port Access (端口访问) 选项卡，打开 Port Access (端口访问) 页。
2. 单击要访问的目标服务器的端口名称，显示 Port Action (端口操作) 菜单。
3. 单击 Connect (连接) 按钮，Virtual KVM Client) 窗口显示与此端口相连的目标服务器。

### 工具栏按钮和状态栏图标

按钮	按钮名称	说明
	Connection Properties(连接属性)	打开 Modify Connection Properties (修改连接属性) 对话框，可以在此人工调节带宽选项 (例如连接速度、色彩深度、平滑处理等)。
	Video Settings(视频设置)	打开 Video Settings (视频设置) 对话框，可以在此人工调节视频转换参数。
	Color Calibration (颜色校准)	调整颜色设置，减少多余的彩色干扰。 与选择 Video (视频) > Color Calibrate (颜色校准) 相同。 <i>注意：KX II-101-V2 不支持。</i>
	Target Screenshot	单击截取目标服务器图像，把它保存到你选择的文

按钮	按钮名称	说明
	(目标服务器截屏)	件里。
	Audio (音频)	<p>打开一个对话框,可以在与客户机 PC 相连的音频设备列表上选择音频设备。</p> <p>在音频设备连接目标服务器之后,选择断开此设备。</p> <hr/> <p><i>注意: KX II 2.4.0 和更高版本具备此功能。</i></p> <p><i>注意: LX 不支此功能。 KX II-101-V2 不支持此功能。</i></p>
	Synchronize Mouse (同步鼠标)	<p>在双鼠标模式下,强制目标服务器鼠标指针与鼠标指针重新对齐。</p> <p><i>注意: 在选择绝对鼠标模式时不可用。</i></p>
	Refresh Screen (刷新屏幕)	强制刷新显示屏幕。
	Auto-sense Video Settings(自动检测视频设置)	强制刷新视频设置(分辨率和刷新速度)。
	Smart Card (智能卡)	<p>打开一个对话框,可以在与客户机 PC 相连的智能卡读卡器列表上选择智能卡。</p> <hr/> <p><i>注意: KSX II 2.3.0 和更高版本以及 KX II 2.1.10 和更高版本具备此功能。</i></p> <p><i>注意: LX 不支此功能。 KX II-101-V2 不支持此功能。</i></p>
	Send Ctrl+Alt+Del (发送 Ctrl+Alt+Del)	把 Ctrl+Alt+Del 热键发送到目标服务器。
	Single Cursor Mode(单光标模式)	<p>启动单光标模式,屏幕不再显示本地鼠标指针。</p> <p>按 Ctrl+Alt+O 退出此模式。</p>
	Full Screen Mode(全屏模式)	使屏幕最大化,观看目标服务器桌面。

按钮	按钮名称	说明
	Scaling (缩放)	增大或缩小目标服务器视频大小，以便在不使用滚动条的情况下看到目标服务器窗口的所有内容。

---

### 控制目标服务器电源

---

*注意：只有在进行电源关联之后，才能使用这些功能。*

---

▶ **给 KVM 目标服务器重新通电：**

1. 单击 KX II-101-V2 Remote Console 上的 Port Access (端口访问) 选项卡。打开 Port Access (端口访问) 页。
2. 单击适当目标服务器的 Port Name (端口名称)。打开 Port Action (端口操作) 菜单。
3. 选择 Power Cycle (重新通电)。显示确认消息。

▶ **接通目标服务器电源：**

1. 单击 KX II-101-V2 Remote Console 上的 Port Access (端口访问) 选项卡。打开 Port Access (端口访问) 页。
2. 单击适当目标服务器的 Port Name (端口名称)。显示 Port Action (端口操作) 菜单。
3. 选择 Power On (通电)。显示确认消息。

▶ **断开目标服务器电源：**

1. 单击 KX II-101-V2 Remote Console 上的 Port Access (端口访问) 选项卡。打开 Port Access (端口访问) 页。
2. 单击适当目标服务器的 Port Name (端口名称)。显示 Port Action (端口操作) 菜单。
3. 选择 Power Off (断电)。显示确认消息。

---

## 断开 KVM 目标服务器电源

### ▶ 断开目标服务器：

- 单击要断开的目标服务器的端口名称，在显示“端口操作”菜单时，单击“断开”按钮。

*提示：也可以在 Virtual KVM (虚拟 KVM) 菜单上选择 Connection (连接) > Exit (退出)，关闭 Virtual KVM Client 窗口。*

---

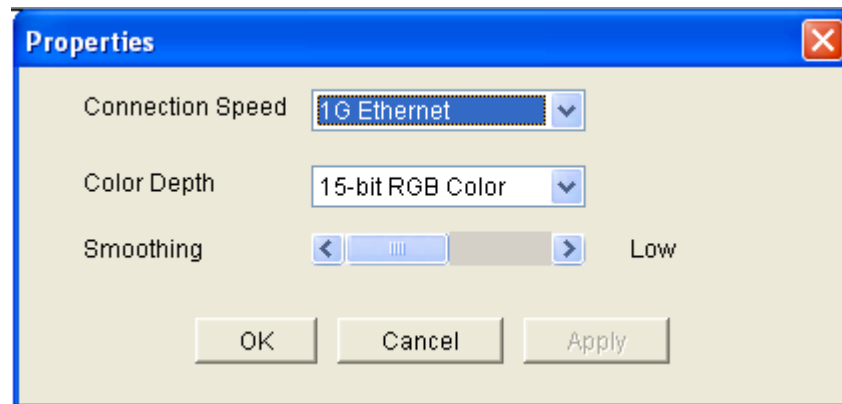
## 连接属性

在不同的可用带宽环境下，动态视频压缩算法确保 KVM 控制台的可用性。设备不仅优化 LAN KVM 输出，还优化 WAN KVM 输出。对于任何带宽，这些设备还控制颜色深度，限制视频输出，从而在视频质量和系统响应时间之间实现最佳平衡。

可以优化 Properties (属性) 对话框上的参数，使其满足不同工作环境的要求。在设置和保存连接属性时，把后续连接的连接属性保存到第二代设备上。

### ▶ 设置连接属性：

- 选择 Connection (连接) > Properties (属性)，或者单击工具栏上的 Connection Properties (连接属性) 按钮 。打开 Properties (属性) 对话框。



*注意：KX II-101 不支持 1G Ethernet。*

---

- 在 Connection Speed (连接速度) 下拉列表上选择连接速度。设备可以动态检测可用带宽，不限制带宽用量。但也可以根据带宽限制，调节此用量。
  - 自动

- 1G Ethernet
- 100 Mb Ethernet
- 10 Mb Ethernet
- 1.5 Mb (最大 DSL/T1)
- 1 Mb (快速 DSL/T1)
- 512 Mb (中速 DSL/T1)
- 384 Mb (低速 DSL/T1)
- 256 Kb (电缆)
- 128 Kb (双 ISDN)
- 56 Kb (ISP 调制解调器)
- 33 Kb (快速调制解调器)
- 24 Kb (低速调制解调器)

注意这些设置对特定条件而言是优化设置，但不是准确速度。无论当前网络速度和编码设置如何，客户机和服务器始终尝试尽可能快地通过网络传输视频。但如何这些设置与实际环境相匹配，系统响应速度最快。

3. 在 **Color Depth** (颜色深度) 下拉列表上选择颜色深度。设备可以动态适应给远程用户传输的颜色深度，使所有带宽的可用性最大化。
  - 15 位 RGB 彩色
  - 8 位 RGB 彩色
  - 4 位彩色
  - 4 位灰度
  - 3 位灰度
  - 2 位灰度
  - 黑白

---

*重要说明：对大多数管理任务（服务器监视、重新配置等）而言，并不需要大多数显示卡支持的 24 位或 32 位真彩色。如果尝试发送这么高的颜色深度，会浪费网络带宽。*

---

4. 用滑动条选择希望的 **Smoothing** (平滑度) (仅 15 位彩色模式)。平滑度确定屏幕区域与小色调变化组合成单一平滑色的尖锐程度。平滑可以减少视频噪声，从而改进目标服务器视频的外观。
5. 单击 **OK** (确定) 按钮设置这些属性。

---

## 连接信息

### ▶ 获取 **Virtual KVM Client** 连接信息：

- 选择 **Connection**（连接）> **Info...**（信息...），打开 **Connection Info**（连接信息）对话框。

显示当前连接的下列信息：

- **Device Name**（设备名称）— 设备的名称。
- **IP Address**（IP 地址）— 设备的 IP 地址。
- **Port**（端口）— 访问目标设备所用的 **KVM** 通信 **TCP/IP** 端口。
- **Data In/Second**（数据输入/秒）— 数据输入速率。
- **Data Out/Second**（数据输出/秒）— 数据输出速率。
- **Connect Time**（连接时间）— 连接持续时间。
- **FPS** — 每秒传输的视频帧数。
- **Horizontal Resolution**（水平分辨率）— 屏幕水平分辨率。
- **Vertical Resolution**（垂直分辨率）— 屏幕垂直分辨率。
- **Refresh Rate**（刷新速度）— 屏幕多久刷新一次。
- **Protocol Version**（协议版本）— **RFB** 协议版本。

### ▶ 复制这些信息：

- 单击 **Copy to Clipboard**（复制到剪贴板），可以把这些信息粘贴到你选择的程序里。

---

## 键盘选项

### 键盘宏

键盘宏确保将针对目标服务器进行的击键组合发送到正确的目标服务器，并由目标服务器解释。否则，**Virtual KVM Client** 所在的计算机（你的客户机 **PC**）可能会解释这些击键组合。

键盘宏存储在客户机 **PC** 上，是 **PC** 特定的。因此，如果使用另一台 **PC**，将看不到自己的键盘宏。此外，如果另一个人使用你的 **PC**，并用不同的用户名登录，他/她可以看到你的键盘宏，因为键盘宏是全局性的。

在 **Virtual KVM Client** 上创建的键盘宏可以在 **MPC** 上使用，反之亦然。但是，在 **Active KVM Client (AKC)** 上创建的键盘宏不能在 **VKC** 或 **MPC** 上使用，反之亦然。

---

*注意：KX II-101 不支持 AKC。*

---

### 导入/导出键盘宏

从 Active KVM Client (AKC) 导出的宏不能导入 Multi-Platform Client (MPC) 或 Virtual KVM Client (VKC)。从 MPC 或 VKC 导出的宏不能导入 AKC。

---

*注意：KX II-101 不支持 AKC。*

---

#### ▶ 导入键盘宏：

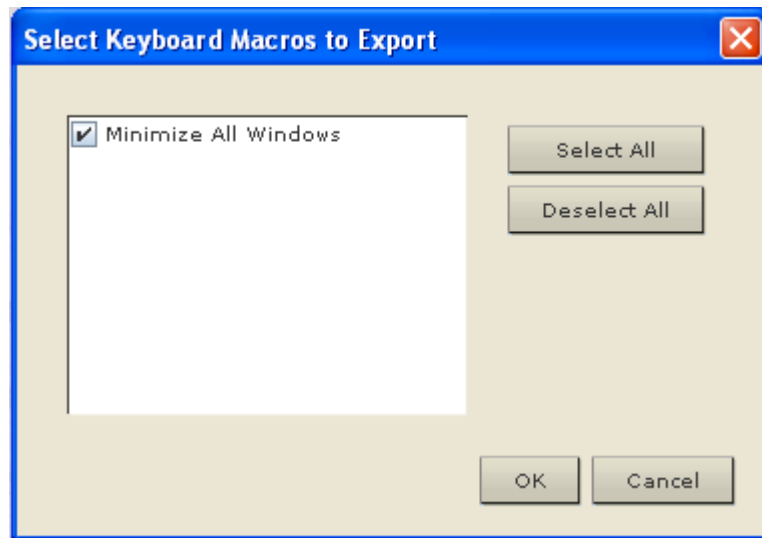
1. 选择 **Keyboard (键盘) > Keyboard Macros (键盘宏)**，打开 **Import Macros (导入宏)** 对话框，找到宏文件所在的文件夹。
2. 单击宏文件，然后单击 **Open (打开)** 按钮导入宏。
  - a. 如果在文件里找到太多宏，显示一条错误消息，单击 **OK (确定)** 按钮中止导入。
  - b. 如果导入失败，打开错误对话框显示一条消息，说明为什么导入失败。单击 **OK (确定)** 按钮继续导入宏，但不导入无法导入的宏。
3. 选择宏对应的复选框导入宏，或者选择 **Select All (全选)** 或 **Deselect All (全部取消)** 选项导入宏。
4. 单击 **OK (确定)** 按钮开始导入。
  - a. 如果找到重复宏，打开 **Import Macros (导入宏)** 对话框。执行下列操作之一：
    - 单击 **Yes (是)** 按钮，用导入的宏替换现有的宏。
    - 单击 **Yes to All (全部是)** 按钮，替换当前选择的宏和找到的其他任何重复宏。
    - 单击 **No (否)** 按钮，保留原始宏，继续导入下一个宏。
    - 单击 **No to All (全部否)** 按钮，保留原始宏，继续导入下一个宏，同时跳过找到的其他任何重复宏。
    - 单击 **Cancel (取消)** 按钮取消导入。
    - 还可以单击 **Rename (重新命名)** 按钮重新命名并导入宏。如果选择 **Rename (重新命名)**，打开 **Rename Macro (重新命名宏)** 对话框。在字段里输入宏的新名称，然后单击 **Ok (确定)** 按钮。关闭对话框，继续导入宏。如果输入的名称与一个现有宏的名称重复，显示一条警告消息，要求你输入另一个宏名称。
  - b. 如果在导入过程中超过允许导入的数量，打开一个对话框。单击 **OK (确定)** 按钮继续导入宏，或者单击 **Cancel (取消)** 按钮停止导入过程。



然后导入宏。如果导入的宏使用已经被使用的热键，不导入新导入宏的热键。

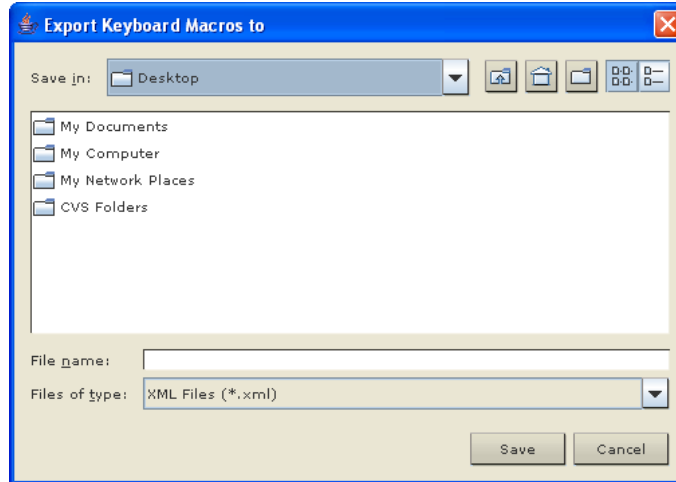
▶ 导出宏：

1. 选择 **Tools(工具)** > **Export Macros(导出宏)**，打开 **Select Keyboard Macros to Export(选择要导出的键盘宏)** 对话框。



2. 选择宏对应的复选框导出宏，或者选择 **Select All(全选)** 或 **Deselect All(全部取消)** 选项导出宏。
3. 单击 **OK(确定)** 按钮打开 **Export Keyboard Macros to(导出键盘宏)** 对话框。找到并选择宏文件。宏文件默认在桌面上。

4. 选择要保存宏文件的文件夹，输入文件名，然后单击 **Save**（保存）按钮。如果宏已经有了，显示一条警告消息。单击 **Yes**（是）按钮覆盖现有宏，或者单击 **No**（否）按钮关闭警告窗口且不覆盖现有宏。



### 创建键盘宏

#### ▶ 创建键盘宏：

1. 单击 **Keyboard**（键盘）> **Keyboard Macros**（键盘宏），打开 **Keyboard Macros**（键盘宏）对话框。
2. 单击 **Add**（添加）按钮打开 **Add Keyboard Macros**（添加键盘宏）对话框。
3. 在 **Keyboard Macro Name**（键盘宏名称）字段里输入键盘宏的名称。在创建键盘宏之后，**Keyboard**（键盘）菜单显示此名称。
4. 在 **Hot-Key Combination**（热键组合）字段里的下拉列表上选择键盘组合。这样，可以用预定义的热键执行键盘宏。<可选>
5. 在 **Keys to Press**（要按的键）下拉列表上选择在执行此命令时，要用哪个键模拟相应的击键。按按键顺序选择这些键。在选择每个键之后，选择 **Add Key**（添加键）。在选择每个键时，**Macro Sequence**（宏序列）字段显示此键，在每次选择之后自动添加 **Release Key**（释放键）命令。

例如创建一个宏，按左 **Ctrl+Esc** 关闭窗口。**Macro Sequence**（宏序列）字段显示的内容如下所示：

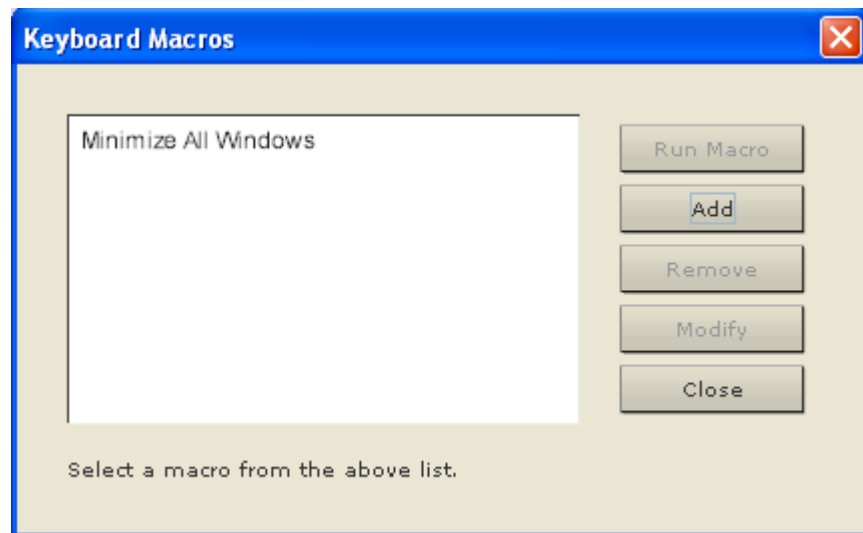
Press Left Alt

Press F4

Release F4

## Release Left Alt

6. 检查 Macro Sequence（宏序列）字段，确保宏序列定义正确无误。
  - a. 如要删除序列中的一个步骤，选择此步骤，然后单击 Remove（删除）按钮。
  - b. 如要更改序列中的步骤顺序，单击一个步骤，然后单击向上或向下箭头按钮，按需要重新排序步骤。
7. 单击 OK（确定）按钮保存宏。单击 Clear（清除）按钮清除所有字段，重新开始创建宏。在单击 OK（确定）按钮之后，打开 Keyboard Macros（键盘宏）对话框，列出新创建的键盘宏。
8. 单击 Close（关闭）按钮关闭 Keyboard Macros（键盘宏）对话框。应用程序的 Keyboard（键盘）菜单现在显示此键盘宏。在菜单上选择并运行新键盘宏，或者按给新键盘宏指定的击键运行它。



► 把给目标服务器发送文本功能用于宏：

1. 单击 Keyboard（键盘）> Sent Text to Target（给目标服务器发送文本），打开 Send Text to Target（给目标服务器发送文本）对话框。
2. 输入要给目标服务器发送的文本。

---

*注意：给目标服务器发送文本功能不支持非英文字符。*

---

3. 如果目标服务器使用美国/国际键盘布局，选择 Target system is set to the US/International keyboard layout（目标系统设置为美国/国际键盘布局）复选框。
4. 单击 OK（确定）按钮。

### 运行键盘宏

在创建键盘宏之后，可以用给它指定的键盘宏执行它，也可以在 **Keyboard**（键盘）菜单上选择并执行它。

#### 通过菜单栏运行宏

在创建宏之后，**Keyboard**（键盘）菜单显示它。在 **Keyboard**（键盘）菜单上单击键盘宏，即可执行它。

#### 用键盘组合运行宏

如果在创建宏时给它指定了键盘组合，可以按指定的击键执行宏。例如同是按 **Ctrl+Alt+0** 键使 **Windows** 目标服务器上的所有窗口最小化。

### 修改和删除键盘宏

#### ▶ 修改宏：

1. 选择 **Keyboard**（键盘）> **Keyboard Macros**（键盘宏）。打开 **Keyboard Macros**（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 **Modify**（修改）。打开 **Add/Edit Macro**（添加/编辑宏）对话框。
4. 修改宏。
5. 单击 **OK**（确定）按钮。

#### ▶ 删除宏：

1. 选择 **Keyboard**（键盘）> **Keyboard Macros**（键盘宏）。打开 **Keyboard Macros**（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 **Remove**（删除）按钮。宏被删除。

与刀片服务器机箱切换热键相同的热键，并不发送到这些机箱上的刀片服务器。

---

## 视频属性


### 刷新屏幕

Refresh Screen（刷新屏幕）命令强制刷新显示屏幕。可以采用几种方法刷新视频设置：

- Refresh Screen（刷新屏幕）命令强制刷新显示屏幕。
- Auto-sense Video Settings（自动检测视频设置）命令自动检测目标服务器的视频设置。

此外，可以用 Video Settings（视频设置）命令人工调节设置。


#### ▶ 执行下列操作之一刷新视频设置：

- 选择 Video（视频）> Refresh Screen（刷新屏幕），或者单击工具栏上的 Refresh Screen（刷新屏幕）按钮 。

### 自动检测视频设置

Auto-sense Video Settings（自动检测视频设置）命令强制重新检测视频设置（分辨率和刷新率），并刷新显示屏幕。

#### ▶ 执行下列操作自动检测视频设置：

- 选择 Video（视频）> Auto-sense Video Settings（自动检测视频设置），或者单击工具栏上的 Auto-Sense Video Settings（自动检测视频设置）按钮 。显示一条消息，说明正在进行自动调节。

### 调节视频设置

用 Video Settings（视频设置）命令人工调节视频设置。

#### ▶ 更改视频设置：

1. 选择 Video（视频）> Video Settings（视频设置），或者单击工具栏上的 Video Settings（视频设置）按钮 ，打开 Video Settings（视频设置）对话框。
2. 按需要调节下列设置。在调节设置时，立刻可以看到调节效果：
  - a. Noise Filter（噪声过滤器）

设备可以过滤来自显示卡的视频输出的电气干扰。此功能可以优化图像质量，减少所需的带宽。只有在与相邻像素相比存在很大的色调变化时，较高的设置才传输可变像素。但如果将阈值设置得太高，可能会无意间将期望的屏幕变化过滤掉。如果设置太低，要传输大多数像素变化。如果将此阈值设置得太小，可能会提高带宽用量。

b. PLL 设置 (PLL Settings) :

**Clock (时钟)** — 控制显示屏显示视频像素的速度。在更改时钟设置时，视频图像会水平伸展或收缩。建议你使用奇数设置。在大多数情况下，不应更改此设置，因为自动检测功能的检测结果通常很精准。

**Phase (相位)** — 相位值在 0-31 之间，在达到 31 之后返回 0。当活动目标服务器显示最佳视频图像时，即停止调节相位值。

- c. **Brightness (亮度)** : 用此设置调节目标服务器显示器的亮度。
- d. **Brightness Red (亮度红色)** — 控制目标服务器显示器的红色信号的亮度。
- e. **Brightness Green (亮度绿色)** — 控制绿色信号的亮度。
- f. **Brightness Blue (亮度蓝色)** — 控制蓝色信号的亮度。
- g. **Contrast Red (对比度红色)** — 控制红色信号对比度。
- h. **Contrast Green (对比度绿色)** — 控制绿色信号。
- i. **Contrast Blue (对比度蓝色)** — 控制蓝色信号。

如果视频图像看上去非常模糊或不聚焦，可以调节时钟设置和相位设置，直到活动目标服务器显示质量较高的图像为止。

---

*警告：在更改时钟设置和相位设置时务必小心。更改时钟设置和相位设置可能会导致屏幕不显示视频，或者视频变形，可能无法返回此前的状态。在进行任何更改之前，请联系 Raritan 技术支持部门。*

---

- j. **Horizontal Offset (水平偏移)** — 控制目标服务器显示器在你的监视器上的水平位置。
- k. **Vertical Offset (垂直偏移)** — 控制目标服务器显示器在你的监视器上的垂直位置。

3. 选择 **Auto Color Calibration (自动颜色校准)** 启用此功能。

4. 选择视频检测模式：

- **Best possible video mode (最佳视频模式)**

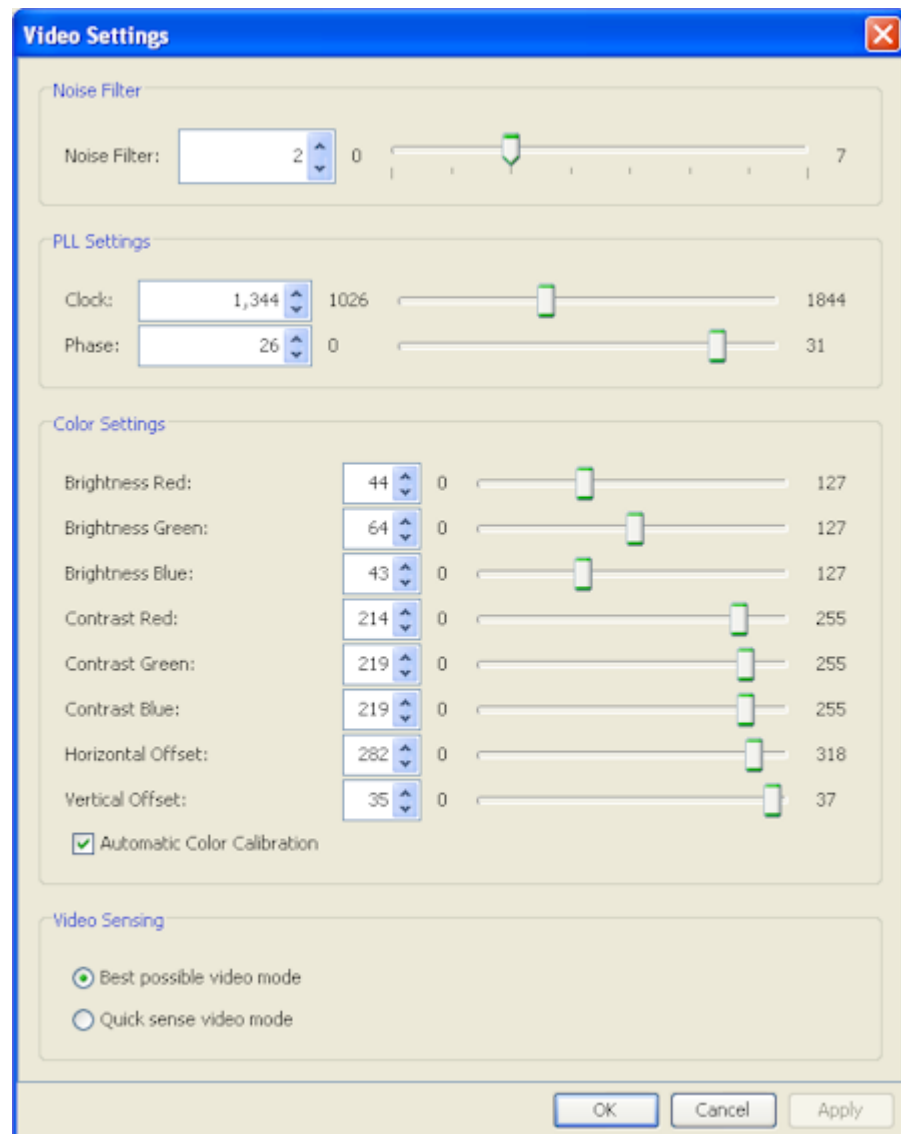
在切换目标服务器或目标分辨率时，设备执行全面自动检测进程。选择此选项校准视频，使视频质量最佳。

- Quick sense video mode (快速检测视频模式)

在选择此选项之后，设备使用快速视频自动检测，迅速显示目标服务器的视频。在目标服务器重新启动之后马上进入其 BIOS 配置时，此选项尤其有用。

5. 单击 **OK** (确定) 按钮应用设置，并关闭对话框。单击 **Apply** (应用) 按钮应用设置，但不关闭对话框。

*注意：在某些 Sun 背景屏幕上，例如有黑边的屏幕，某些 Sun 服务器可能不精确居中。使用另一个背景，或者在屏幕左上角放一个浅色图标。*

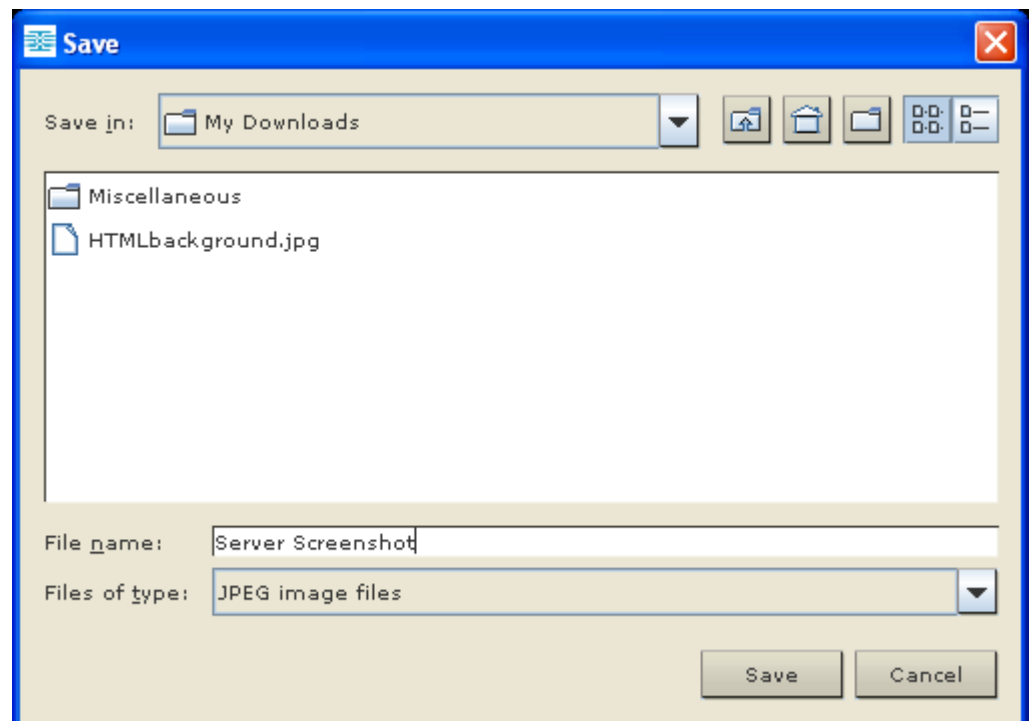


### 使用目标服务器截屏

可以用 **Screenshot from Target server**（目标服务器截屏）命令截取目标服务器屏幕。必要时可以采用 **bitmap**、**JPEG** 或 **PNG** 格式将此截屏保存到所选的文件位置。

#### ▶ 截取目标服务器屏幕：

1. 选择 **Video**（视频）> **Screenshot from Target**（目标服务器截屏），或者单击工具栏上的 **Screenshot from Target**（目标服务器截屏）按钮 。
2. 在 **Save**（保存）对话框上选择文件保存位置，输入文件名，在 **Files of type**（文件类型）下拉列表上选择文件格式。
3. 单击 **Save**（保存）按钮保存截屏。





### 更改最大刷新速率

如果目标服务器上的显示卡使用定制软件，而你通过 MPC 或 VKC 访问目标服务器，可能必须更改监视器的最大刷新速率，刷新速率才会在目标服务器上生效。

#### ▶ 调节监视器刷新速率：

1. 在 Windows® 上选择 Display Properties（显示属性）> Settings（设置）> Advanced（高级），打开 Plug and Play（即插即用）对话框。
2. 单击 Monitor（监视器）选项卡。
3. 设置 Screen refresh rate（屏幕刷新速率）。
4. 单击 OK（确定）按钮，再单击 OK（确定）按钮应用设置。

---

### 鼠标选项

在控制目标服务器时，Remote Console 显示两个鼠标光标：一个属于客户机工作站，另一个属于目标服务器。

你既可以在单鼠标模式下操作，也可以在双鼠标模式下操作。在双鼠标模式下，假如正确配置此选项，两个鼠标光标重叠在一起。

在显示两个鼠标光标时，设备提供几种鼠标模式：

- 绝对（鼠标同步）
- 智能（鼠标模式）
- 标准（鼠标模式）

### 鼠标指针同步

在远程查看使用鼠标的目标服务器时，你会看到两个鼠标指针：一个属于远程客户机工作站，另一个属于目标服务器。当鼠标指针位于 Virtual KVM Client 目标服务器窗口内时，鼠标移动和单击操作直接发送到相连的目标服务器。在移动鼠标时，由于鼠标加速度设置的缘故，客户机鼠标指针相对于目标服务器鼠标指针稍稍提前一点。

在快速 LAN 连接上，可以禁用 Virtual KVM Client 鼠标指针，只看到目标服务器的鼠标指针。可以在两种模式（单鼠标模式和双鼠标模式）之间来回切换。

#### 鼠标同步提示

在配置鼠标同步时，务必遵循下列步骤：

1. 确认选择的视频分辨率和刷新速度是否在此设备支持的范围内。Virtual KVM Client“连接信息”对话框是否显示此设备看到的实际值。

2. 对于 KX II 和 LX 设备，确认电缆长度是否在选择的视频分辨率要求的指定范围内。
3. 确认在安装过程中是否正确配置了鼠标和视频。
4. 单击 Virtual KVM Client 自动检测按钮，强制进行自动检测。
5. 如果这不能改善鼠标同步（Linux、UNIX 和 Solaris KVM 目标服务器）：
  - a. 打开终端窗口。
  - b. 输入下列命令：`xset mouse 1 1`
  - c. 关闭终端窗口。
6. 单击 Virtual KVM Client 鼠标同步按钮 。


#### 智能鼠标模式附加说明

- 确保屏幕左上角没有图标或应用程序，因为这是同步例程执行位置。
- 切勿使用动画鼠标。
- 在 KVM 目标服务器上禁用活动桌面。

#### 同步鼠标

在双鼠标模式下，Synchronize Mouse（同步鼠标）命令强制目标服务器鼠标指针与 Virtual KVM Client 鼠标指针重叠。

#### ▶ 执行下列其中一个操作同步鼠标：

- 选择 Mouse（鼠标）> Synchronize Mouse（同步鼠标），或者单击工具栏上的 Synchronize Mouse（同步鼠标）按钮 。

---

注意：只能在标准鼠标模式和智能鼠标模式下使用此选项。

---

#### 标准鼠标模式

标准鼠标模式使用标准鼠标同步算法，使用相对鼠标位置。为了让客户机鼠标和服务端鼠标保持同步，标准鼠标模式要求禁用鼠标加速度，正确设置其他鼠标参数。

#### ▶ 进入标准鼠标模式：

- 选择 Mouse（鼠标）> Standard（标准）。

### 智能鼠标模式

在智能鼠标模式下，设备可以检测目标服务器鼠标设置，相应地同步鼠标光标，在目标服务器上启用鼠标加速度。智能鼠标模式是非 VM 目标服务器的默认模式。

在同步过程中，鼠标光标跳到屏幕左上角计算加速度。为了让此模式正常工作，必须满足某些条件。

#### ▶ 进入智能鼠标模式：

- 选择 Mouse（鼠标）> Intelligent（智能）。

#### 智能鼠标同步条件

在鼠标闲置时，Mouse（鼠标）菜单上的 **Intelligent Mouse Synchronization**（智能鼠标同步）命令自动同步鼠标指针。为了让此模式正常工作，必须满足下列条件：

- 应该在目标服务器上禁用活动桌面。
- 目标服务器页面左上角不应该有窗口。
- 目标服务器页面左上角不应该有动画背景。
- 目标服务器鼠标光标的形状应该是正常形状，不应是动画光标。
- 目标服务器鼠标速度不应设置为太小或太大的值。
- 应该禁用 **Enhanced pointer precision**（增强指针精度）或 **Snap mouse to default button in dialogs**（在对话框上捕捉鼠标至默认按钮）等高级鼠标属性。
- 在 **Video Settings**（视频设置）窗口上选择 **Best Possible Video Mode**（最佳视频模式）。
- 目标服务器视频的边沿应该清晰可见（即当你滚到目标服务器视频图像边沿时，目标服务器桌面和远程 KVM 控制台窗口之间的黑边应该是可见的）。
- 在使用智能鼠标同步功能时，桌面左上角的文件图标或文件夹图标可能会导致此功能不能正常工作。为了避免此功能出任何问题，Raritan 建议你不要将任何文件图标或文件夹图标放在桌面左上角。

在自动检测目标服务器视频之后，单击工具栏上的 **Synchronize Mouse**（同步鼠标）按钮人工开始鼠标同步。在目标服务器分辨率变化时，如果鼠标指针开始彼此不同步，也可以这么做。

如果智能鼠标同步失败，此模式将切换回标准鼠标同步模式。

请注意在不同的目标服务器操作系统上，鼠标配置会有差异。参看操作系统指南了解详情。同时还要注意，智能鼠标同步对 **Unix** 目标服务器无效。

### 绝对鼠标模式

在此模式下，用绝对坐标使客户机光标和目标服务器光标保持同步，即使目标服务器鼠标设置为不同的加速度或速度也没有关系。具备 USB 端口的服务器支持此模式，VM 目标服务器和双 VM 目标服务器默认使用此模式。

#### ▶ 进入绝对鼠标模式：

- 选择 Mouse (鼠标) > Absolute (绝对)。

---

*注意：绝对鼠标设置要求 USB 目标系统，是给 KX II-101 建议的鼠标设置。*

*注意：对于 KX II，绝对鼠标同步仅用于支持虚拟媒体的 USB CIM (D2CIM-VUSB 和 D2CIM-DVUSB)。*

---

### VKC 虚拟媒体

参看[虚拟媒体](#) (p. 67)一章详细了解如何设置和使用虚拟媒体。

---

### 工具选项

#### 常规设置

#### ▶ 设置工具选项：

1. 选择 Tools (工具) > Options (选项)，打开 Options (选项) 对话框。
2. 只有在技术支持人员的指导下，才能选择 **Enable Logging** (启用日志) 复选框。此选项在主目录下创建一个日志文件。
3. 在 Keyboard Type (键盘类型) 下拉列表上选择键盘类型 (如有必要)。选项包括：
  - US/International (美国/国际英文)
  - French (France) (法文[法国])
  - German (Germany) (德文[德国])
  - Japanese (日文)
  - United Kingdom (英国)
  - Korean (Korea) (朝鲜文[韩国])
  - Belgian (Belgium) (比利时)
  - Norwegian (Norway) (挪威文[挪威])

- Portuguese (葡萄牙文[葡萄牙])
- Danish (Denmark) (丹麦文[丹麦])
- Swedish (Sweden) (瑞典文[瑞典])
- German (Switzerland) (德文[瑞士])
- Hungarian (Hungary) (匈牙利文[匈牙利])
- Spanish (Spain) (西班牙文[西班牙])
- Italian (Italy) (意大利文[意大利])
- Slovenian (斯洛文尼亚文)
- 翻译：French - US (法文 - 美国英文)
- 翻译：French - US (法文 - 美国国际英文)

在 AKC 里，键盘类型默认为本地客户机，所以此选项不适用。此外，KX II-101 和 KX II-101-V2 不支持单光标模式，退出单光标模式功能不适用于这些设备。

#### 4. 配置热键：

- 退出全屏模式 — 热键。在进入全屏模式时，全屏显示目标服务器，使用与目标服务器相同的分辨率。这是退出此模式所用的热键。
- 退出单光标模式 — 热键。在进入单光标模式时，只显示目标服务器鼠标光标。这是退出单光标模式、返回客户机鼠标光标所用的热键。
- 断开目标服务器 — 热键。启用此热键，使用户能迅速断开目标服务器。

关于热键组合，本应用程序不允许你给多个功能指定同一个热键组合。例如如果给断开目标服务器功能指定了 **Q**，不能再把它指定给退出全屏模式功能。此外，如果由于升级而给应用程序添加了一个热键，但此热键的默认值已经使用了，就把下一个可能的值应用于此功能。

#### 5. 单击 OK (确定) 按钮。

**键盘限制****土耳其文键盘**

如果使用土耳其文键盘，必须用 **Active KVM Client (AKC)** 连接目标服务器。Raritan 的其他客户机不支持土耳其文键盘。

**斯洛文尼亚文键盘**

由于 **JRE** 限制，斯洛文尼亚文键盘上的 < 键不起作用。

**Linux 语言配置**

由于 Linux 运行的 Sun JRE 在给用 **System Preferences** (系统首选项) 配置的外文键盘生成正确的键事件时有问题，Raritan 建议你用下表所述的方法配置外文键盘。

语言	配置方法
美国英语/国际	默认值
法文	Keyboard Indicator (键盘指示器)
德文	System Settings (系统设置) (Control Center[控制中心])
日文	System Settings (系统设置) (Control Center[控制中心])
英国英语	System Settings (系统设置) (Control Center[控制中心])
朝鲜文	System Settings (系统设置) (Control Center[控制中心])
比利时	Keyboard Indicator (键盘指示器)
挪威文	Keyboard Indicator (键盘指示器)
丹麦文	Keyboard Indicator (键盘指示器)
瑞典文	Keyboard Indicator (键盘指示器)
匈牙利文	System Settings (系统设置) (Control Center[控制中心])
西班牙文	System Settings (系统设置) (Control Center[控制中心])
意大利文	System Settings (系统设置) (Control Center[控制中心])
斯洛文尼亚文	System Settings (系统设置) (Control Center[控制中心])

语言	配置方法
葡萄牙文	System Settings (系统设置) (Control Center[控制中心])

*注意：在使用 Gnome 作为桌面环境的 Linux 系统上，应该使用 Keyboard Indicator (键盘指示器)。*

### 客户机启动设置

可以配置客户机启动设置，给 KVM 会话定义屏幕设置。

*注意：在使用 MPC 时，LX 设备支持此功能。LX 不支持 VKC 和 AKC 的客户机启动设置。*

#### ► 配置客户机启动设置：

1. 选择“工具>选项”，打开“选项”对话框。
2. 单击“客户机启动设置”选项卡。
  - 配置目标窗口设置：
    - a. 选择“标准调节目标分辨率大小”，用目标窗口的当前分辨率打开窗口。如果目标分辨率大于客户机分辨率，目标窗口尽可能覆盖整个窗口，并显示滚动条（如有必要）。
    - b. 选择“全屏”，按全屏模式打开目标服务器窗口。
  - 配置要在哪个监视器上打开目标查看器：
    - a. 如果要使用与客户机（例如网络浏览器或小程序）相同的应用程序显示方式启动目标查看器，选择“监视器客户机旧启动方式”。
    - b. 选择“在检测到的监视器中选择”，在应用程序当前检测到的监视器列表上选择监视器。如果再也检测不到此前选择的监视器，显示“检测不到当前选择的监视器”。
  - 配置其他启动设置：
    - a. 选择“启用单光标模式”，启用单光标模式作为在访问服务器时的默认鼠标模式。
    - b. 选择“启用缩放视频”，在访问目标服务器时自动缩放目标服务器的显示器。
    - c. 如果希望在全屏模式下显示目标服务器时显示目标服务器的工具栏，选择“固定菜单工具栏”。在全屏模式下显示目标服务器时，只有在把鼠标移动到屏幕顶部时才显示菜单，这是默认设置。
3. 单击“确定”按钮。

### 在 VKC 和 AKC 上配置扫描设置

KX II 和 LX 提供 扫描选择的目标服务器并用幻灯视图显示找到的目标服务器所用的端口扫描功能，使你每次可以监视最多 32 台目标服务器。可以连接这些目标服务器，必要时可以关注一台特定目标服务器。可以扫描标准目标服务器、刀片服务器、分层 Dominion 设备和 KVM 切换器端口。在 Virtual KVM Client (VKC) 或 Active KVM Client (AKC) 上配置扫描设置。参看 在 VKC 和 AKC 上配置扫描设置 了解详情。参看 扫描端口。用“扫描设置”选项卡定制扫描间隔时间和默认显示选项。

#### ▶ 设置扫描设置：

1. 选择“工具>选项”，打开“选项”对话框。
2. 选择“扫描设置”选项卡。
3. 在“显示间隔时间（10-255 秒）：”字段里指定目标服务器在端口扫描窗口中央显示的秒数。
4. 在 Interval Between Ports (10-255 sec):（端口之间的间隔时间 [10-255 秒]：）字段里指定设备在各个端口之间应该暂停的间隔时间。
5. 在“显示”部分更改缩略图大小和“端口扫描”窗口分割方向的默认显示选项。
6. 单击“确定”按钮。

---

### 视图选项

#### 视图工具栏

可以在显示或不显示工具栏的情况下使用 Virtual KVM Client。

#### ▶ 切换工具栏显示（打开和关闭）：

- 选择 View（视图）> View Toolbar（视图工具栏）。

#### 查看状态栏

状态栏默认位于目标服务器窗口底部。

#### ▶ 隐藏状态栏：

- 单击 View（视图）> Status Bar（状态栏）取消状态栏。

#### ▶ 恢复状态栏：

- 单击 View（视图）> Status Bar（状态栏）选择状态栏。



### 缩放

缩放目标窗口，可以看到目标服务器窗口的整个内容。此功能增大或缩小目标视频大小，使之适合 **Virtual KVM Client** 窗口大小，并保持长宽比不变，即使你不使用滚动条也能看到整个目标服务器桌面。

#### ▶ 切换缩放（打开和关闭）：

- 选择 **View**（视图）> **Scaling**（缩放）。

### 全屏模式

在进入全屏模式时，全屏显示目标服务器，使用与目标服务器相同的分辨率。在 **Options**（选项）对话框上指定退出此模式所用的热键，参看 **工具选项** (p. 60)。

在全屏模式下，把鼠标移动到屏幕顶部，将显示全屏模式菜单栏。如果希望在全屏模式下显示工具栏，在 **Tool Options**（工具选项）对话框上选择 **Pin Menu Toolbar**（固定菜单工具栏）选项。参看 **工具选项** (p. 60)。

#### ▶ 进入全屏模式：

- 选择 **View**（视图）> **Full Screen**（全屏）。

#### ▶ 退出全屏模式：

- 按在 **Tool Options**（工具选项）对话框上配置的热键。默认设置是 **Ctrl+Alt+M**。

如果希望始终在全屏模式下访问目标服务器，可以把全屏模式设置为默认模式。

#### ▶ 把全屏模式设置为默认模式：

1. 单击 **Tools**（工具）> **Options**（选项），打开 **Options**（选项）对话框。
2. 单击 **Enable Launch in Full Screen Mode**（启用在全屏模式下启动）图标，单击 **OK**（确定）按钮。

---

## 帮助选项

关于 Raritan Virtual KVM Client

当你需要 Raritan 技术支持部门的协助时，此菜单命令提供 Virtual KVM Client 版本信息。

▶ **获取版本信息：**

1. 选择 **Help (帮助) > About Raritan Virtual KVM Client (关于 Raritan Virtual KVM Client)**。
2. 用 **Copy to Clipboard (复制到剪贴板)** 按钮把对话框上的信息复制到剪贴板文件里，以便稍后在联系支持人员时访问（如有必要）。

## Ch 4

## 虚拟媒体

### 在本章内

概述.....	68
使用虚拟媒体 .....	74
连接虚拟媒体 .....	75
断开虚拟媒体 .....	77

---

## 概述

虚拟媒体允许 KVM 目标服务器远程访问客户机 PC 和网络文件服务器上的媒体，从而扩展了 KVM 功能。在使用此功能时，安装在客户机 PC 和网络文件服务器上的媒体基本上可由目标服务器虚拟加载。随后，目标服务器可以读写这些媒体，就像读写与目标服务器直接相连的媒体一样。虚拟媒体包括内置和 USB 安装的 CD 驱动器和 DVD 驱动器、USB 大容量存储设备、PC 硬盘驱动器、PC 软盘驱动器和 ISO 镜像文件（磁盘镜像文件）。

虚拟媒体允许你远程执行其他任务，例如：

- 传输文件
- 运行诊断
- 安装或修补应用程序
- 完成操作系统安装（如果机器 BIOS 支持）
- 这种扩展 KVM 控制功能使你在大多数情况下不必亲自到数据中心去，可以节省时间和金钱。

Windows®、Mac® 和 Linux™ 客户机支持下列虚拟媒体类型：

- 内置 CD/DVD 驱动器和 USB CD/DVD 驱动器
- USB 海量存储设备
- PC 硬盘
- ISO 镜像文件（磁盘镜像文件）
- 数字音频设备\*

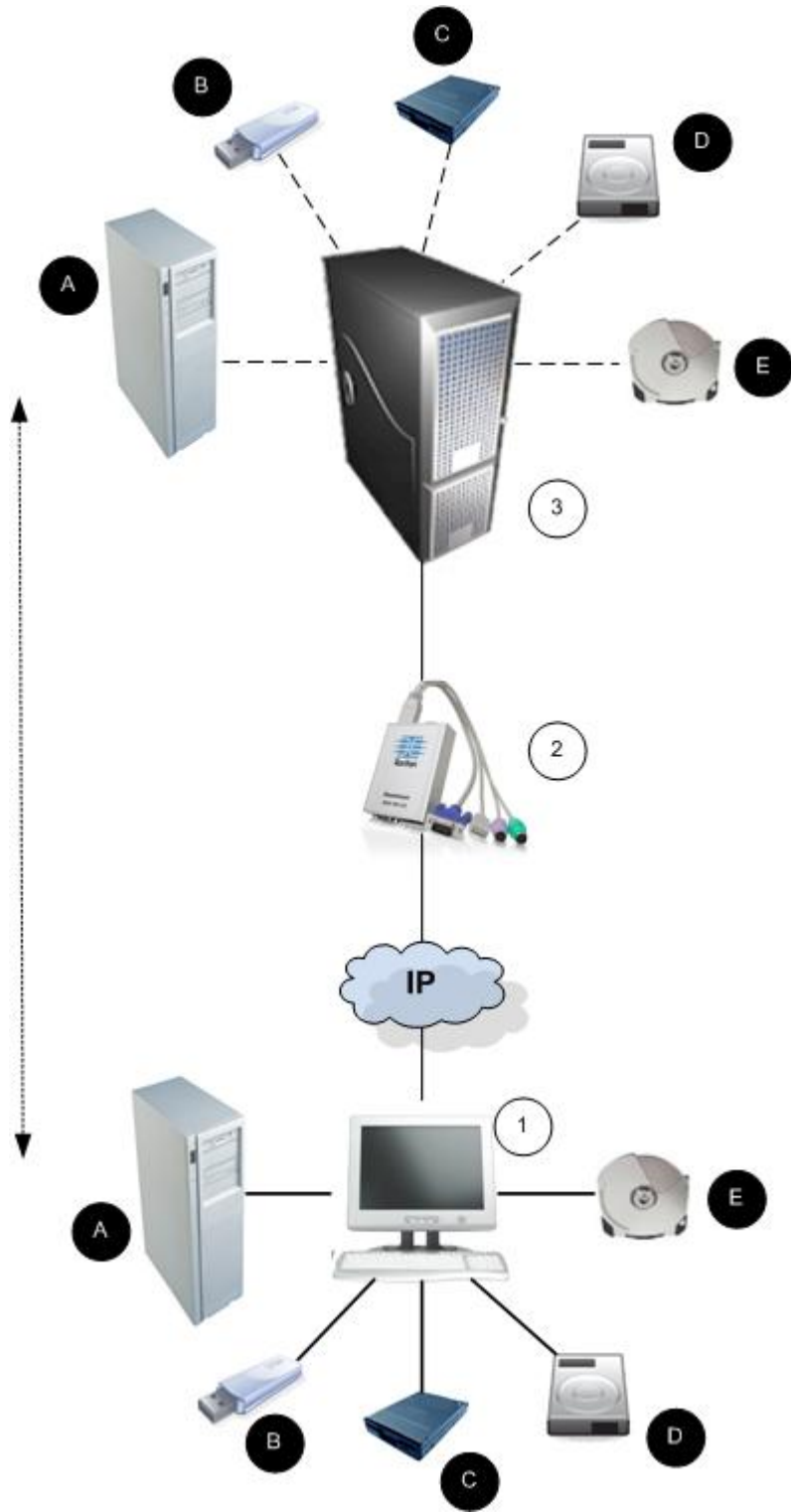
---

*注意：ISO9660 格式是 Raritan 支持的标准，但也可以使用其他 ISO 标准。*

---

支持下列客户机操作系统：

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



---

*注意：如果使用虚拟媒体，必须使用 USB 连接。*

---

### 使用虚拟媒体的前提

可以利用虚拟媒体功能安装最多两个（不同类型的）驱动器，这些驱动器必须是当前应用于目标服务器的 USB 配置文件所支持的驱动器。这些驱动器可以在 KVM 会话持续期间访问。

例如可以安装并使用一个特定的 CD-ROM，在会话结束时断开它。但 CD-ROM 虚拟媒体“通道”仍然保持打开状态，以便你虚拟安装另一个 CD-ROM。只要 USB 配置文件支持 KVM 会话，在 KVM 会话关闭之前，这些虚拟媒体“通道”仍然保持打开状态。

在你希望从目标服务器连接的客户机或网络文件服务器上连接/加装相关媒体，即可使用虚拟媒体。此步骤不一定是第一步，但在尝试访问此媒体之前必须这样做。

为了使用虚拟媒体，必须满足下列条件：

#### Dominion 设备

- 对于需要访问虚拟媒体的用户，必须设置设备权限允许访问相关端口，同时还必须设置这些端口的虚拟媒体访问权限（VM 访问端口权限）。在组一级设置端口权限。
- 设备和目标服务器之间必须有 USB 连接。
- 如果要使用 PC 共享，还必须在 Security Settings（安全设置）页上启用安全设置。**可选**
- 必须给要连接的 KVM 目标服务器选择正确的 USB 配置文件。

#### 客户机 PC

- 某些虚拟媒体选项要求您有客户机 PC 管理权限（例如整个驱动器的驱动器重定向）。

---

*注意：如果使用 Microsoft Vista 或 Windows 7，禁用 User Account Control（用户帐号控制），或者选择 Run as Administrator when starting Internet Explorer（在启动 Internet Explorer 时作为管理员运行）。为此，单击 Start（开始）菜单，找到 IE，用右键单击它，选择 Run as Administrator（作为管理员运行）。*

---

#### 目标服务器

- KVM 目标服务器必须支持 USB 连接的驱动器。
- 运行 Windows 2000 的 KVM 目标服务器必须安装了所有最新补丁。
- USB 2.0 端口速度更快，是首选端口。

---

### **Windows XP 环境下的虚拟媒体**

如果在 Windows® XP 环境下运行 Virtual KVM Client，用户必须具备管理员权限，才能访问除 CD-ROM 连接、ISO 和 ISO 镜像文件之外的任何虚拟媒体。

## Linux 环境下的虚拟媒体

下面的重要信息针对使用虚拟媒体的 Linux® 用户。

### 根用户权限要求

如果在 Linux 客户机上把 CD ROM 安装在目标服务器上，然后卸载此 CD ROM，可能会关闭虚拟媒体连接。在安装软盘之后又把它拆卸掉，也可能会关闭连接。为了避免这些问题，你必须是根用户。

### 权限

用户必须拥有适当的访问权，才能把 Drive/CD-ROM 连接到目标服务器。可以输入下列命令检查权限：

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

在上述示例中，必须把权限更改为允许读访问。

在一个利用其文件工具支持 ACL 的系统中，ls 命令按下列方式更改其属性：

- 对于有默认 ACL 或访问 ACL（它包含三个以上所需的 ACL 项）的文件，ls -l 生成的长格式的 ls(1) 工具在权限字符串后面显示加号 (+)。

在此 /dev/sr0 示例中，用 getfacl -a /dev/sr0 查看用户是否拥有 ACL 定义的访问权。在此示例中，他们有访问权，即使 ls -l 命令输出可能说明他们没有访问权，也可以把 cd-rom 连接到目标服务器。

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

类似的可拆卸设备权限检查显示：



```

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

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

```

这要求授予用户可拆卸设备只读权限：

```

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

```

然后可以把此驱动器连接到目标服务器。

### Mac 环境下的虚拟媒体

下面的重要信息针对使用虚拟媒体的 Mac® 用户。

#### 活动系统分区

- 不能在 Mac 客户机上使用虚拟媒体安装活动系统分区。

#### 驱动器分区

- 不同的操作系统有下列驱动器分区限制：
  - Windows 和 Mac 目标服务器不能读 Linux 格式化分区
  - Windows® 和 Linux® 不能读 Mac 格式化分区
  - Linux 只支持 Windows FAT 分区
  - Mac 支持 Windows FAT 和 NTFS 分区

- Mac 用户必须卸载已安装的所有设备，才能连接目标服务器。用 `>diskutil umount /dev/disk1s1` 命令卸载设备，用 `diskutil mount /dev/disk1s1` 重新安装设备。

---

### 读写不可用时的条件

在下列情况下，虚拟媒体读写功能不可用：

- Linux® 和 Mac® 客户机
- 所有硬盘
- 当驱动器有写保护时
- 当用户没有读写权限时：
  - Port Permission Access（端口权限访问）被设置为 None（无）或 View（查看）
  - Port Permission VM Access（端口权限 VM 访问）被设置为 Read-Only（只读）或 Deny（拒绝）

---

## 使用虚拟媒体

参看 [使用虚拟媒体的前提](#) (p. 70) 了解如何开始使用虚拟媒体。

### ▶ 使用虚拟媒体：

1. 如果要访问文件服务器 ISO 镜像文件，在 Remote Console File Server Setup(文件服务器设置)页上指定这些文件服务器和镜像文件。

---

*注意：ISO9660 格式是 Raritan 支持的标准，但也可以使用其他 CD-ROM 扩展。*

---

2. 与相应的目标服务器建立 KVM 会话。
  - a. 在 Remote Console 上打开 Port Access（端口访问）页。
  - b. 在端口访问页上连接目标服务器：
    - 单击相应的目标服务器的 Port Name（端口名称）。
    - 在 Port Action（端口操作）菜单上选择 Connect（连接）命令，在 Virtual KVM Client 窗口上打开目标服务器。
3. 连接虚拟媒体：

对于：	选择此虚拟媒体选项：
本地驱动器	Connect Drive（连接驱动器）
本地 CD/DVD 驱动器	Connect CD-ROM/ISO（连接 CD-ROM/ISO）

对于：	选择此虚拟媒体选项：
ISO 镜像文件	Connect CD-ROM/ISO（连接 CD-ROM/ISO）
文件服务器 ISO 镜像文件	Connect CD-ROM/ISO（连接 CD-ROM/ISO）

在完成任务之后，断开虚拟媒体。参看 [断开虚拟媒体](#) (p. 77)。

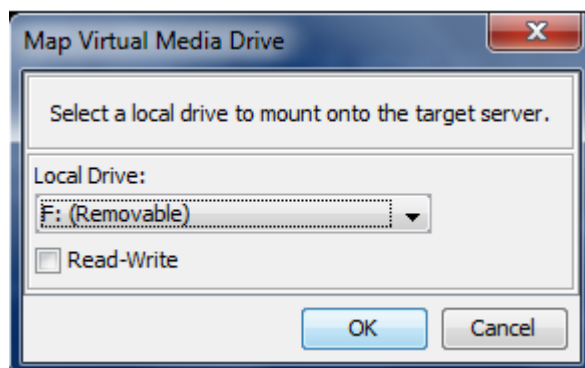
## 连接虚拟媒体

### 本地驱动器

此选项安装整个驱动器，这意味着采用虚拟方式将整个磁盘驱动器安装在目标服务器上。将此选项仅用于硬盘和外置驱动器。不包括网络驱动器、CD-ROM 驱动器或 DVD-ROM 驱动器。这是唯一一个有读写权限的选项。

#### 访问客户计算机上的驱动器：

1. 在 Virtual KVM Client 上选择 Virtual Media（虚拟媒体）> Connect Drive（连接驱动器），打开 Map Virtual Media Drive（映射虚拟媒体驱动器）对话框。（）



2. 在 Local Drive（本地驱动器）下拉列表上选择驱动器。
3. 如果需要读写功能，选择 Read-Write（读写）复选框。不能拆卸的驱动器禁用此选项。参看 [读写不可用时的条件](#) (p. 74)了解详情。如果选择此复选框，可以读写连接的 USB 磁盘。

**警告：**启用读写访问可能很危险！在多个实体上同时访问同一个驱动器，可能会导致数据损坏。如果不需要写访问权，不要选择此复选框。

4. 单击 OK（确定）按钮采用虚拟方式把此媒体安装在目标服务器上，可以像访问其他任何驱动器一样访问此媒体。

---

## 安装 CD-ROM/DVD-ROM/ISO 镜像文件

此选项安装 CD-ROM、DVD-ROM 和 ISO 镜像文件。

---

*注意* :ISO9660 格式是 Raritan 支持的标准,但也可以使用其他 CD-ROM 扩展。

---

### ▶ 访问 CD-ROM、DVD-ROM 和 ISO 镜像文件：

1. 在 Virtual KVM Client 上选择 Virtual Media (虚拟媒体) > Connect CD-ROM/ISO Image (连接 CD-ROM/ISO 镜像文件), 打开 Map Virtual Media CD/ISO Image (映射虚拟媒体 CD/ISO 镜像文件) 对话框。
2. 对于内置和外置 CD-ROM 驱动器或 DVD-ROM 驱动器：
  - a. 选择 Local CD/DVD Drive (本地 CD/DVD 驱动器) 选项。
  - b. 在 Local CD/DVD Drive (本地 CD/DVD 驱动器) 下拉列表上选择驱动器。下拉列表显示所有可用的内置和外置 CD 驱动器和 DVD 驱动器的名称。
  - c. 单击 Connect (连接) 按钮。
3. 对于 ISO 镜像文件：
  - a. 选择 ISO Image (ISO 镜像文件) 选项。如果要访问 CD、DVD 或硬盘的磁盘镜像文件, 使用此选项。ISO 格式是支持的唯一格式。
  - b. 单击 Browse (浏览) 按钮。
  - c. 找到要使用的磁盘镜像文件所在的路径, 单击 Open (打开) 按钮, Image Path (镜像文件路径) 字段自动填充此路径。
  - d. 单击 Connect (连接) 按钮。
4. 对于文件服务器上的远程 ISO 镜像文件：
  - a. 选择 Remote Server ISO Image (远程服务器 ISO 镜像文件) 选项。
  - b. 在 Hostname (主机名) 和 Image (镜像文件) 下拉列表上选择主机名和镜像文件。可以使用的文件服务器和镜像文件路径是你在 File Server Setup (文件服务器设置) 页上配置的文件服务器和镜像文件路径。下拉列表只显示在 File Server Setup (文件服务器设置) 页上配置的项目。
  - c. File Server Username (文件服务器用户名) — 访问文件服务器所需的用户名。名称可以包括域名, 例如 mydomain/username。
  - d. File Server Password (文件服务器密码) — 访问文件服务器所需的密码 (输入时字段显示星号)。

- e. 单击 **Connect**（连接）按钮。

采用虚拟方式把此媒体安装在目标服务器上，可以像访问其他任何驱动器一样访问此媒体。

---

*注意：如果使用 Linux® 目标服务器上的文件，在使用虚拟媒体复制文件之后，用 **Linux Sync**（同步）命令查看复制的文件。在执行同步之前，可能不显示复制的文件。*

*注意：如果使用 Windows 7® 操作系统®，在安装本地 CD/DVD 驱动器或本地/远程 ISO 镜像文件时，Windows 的 My Computer（我的计算机）文件夹默认不显示可拆卸磁盘。如要查看此文件夹里的本地 CD/DVD 驱动器或本地/远程 ISO 镜像文件，选择 **Tools**（工具）> **Folder Options**（文件夹选项）> **View**（查看），取消 **Hide empty drives in the Computer folder**（计算机文件夹隐藏空驱动器）。*

*注意：由于第三方软件的技术限制，不能使用 IPv6 地址通过虚拟媒体访问远程 ISO 镜像文件。*

---

## 断开虚拟媒体

### ▶ 断开虚拟媒体驱动器：

- 对于本地驱动器，选择 **Virtual Media**（虚拟媒体）> **Disconnect Drive**（断开驱动器）。
- 对于 CD-ROM、DVD-ROM 和 ISO 镜像文件，选择 **Virtual Media**（虚拟媒体）> **Disconnect CD-ROM/ISO Image**（断开 CD-ROM/ISO 镜像文件）。

---

*注意：除了用 **Disconnect**（断开）命令断开虚拟媒体，关闭 KVM 连接也同时关闭虚拟媒体。*

---

## 在本章内

用户组 .....	78
用户 .....	84
验证设置 .....	88
更改密码 .....	98

---

 用户组

每台 KX II-101-V2 在出厂时有三个默认用户组。不能删除这些用户组：

用户	说明
Admin（管理员）	本组用户具有所有管理权限。出厂默认的最初用户是本用户组的成员，具有所有系统权限。此外，Admin 用户必须是 Admin 用户组成员。
未知	这是用 LDAP/LDAPS 或 RADIUS 进行外部验证的用户或系统未知的用户所属的默认用户组。如果外部 LDAP/LDAPS 或 RADIUS 服务器不确定一个有效用户组，就使用 Unknown（未知）用户组。此外，新创建的任何用户均自动放入此用户组，直到给他们指定另一个用户组为止。
Individual Group（个人组）	个人组基本上是一个人的“用户组”。也就是说，特定用户在自己的用户组里，与其他实际用户组没有关联。可以在用户组名称上使用 @ 符号，表示这是个人组。个人组允许一个用户帐号具有与一个用户组相同的权限。

KX II-101-V2 最多允许创建 254 个用户组。

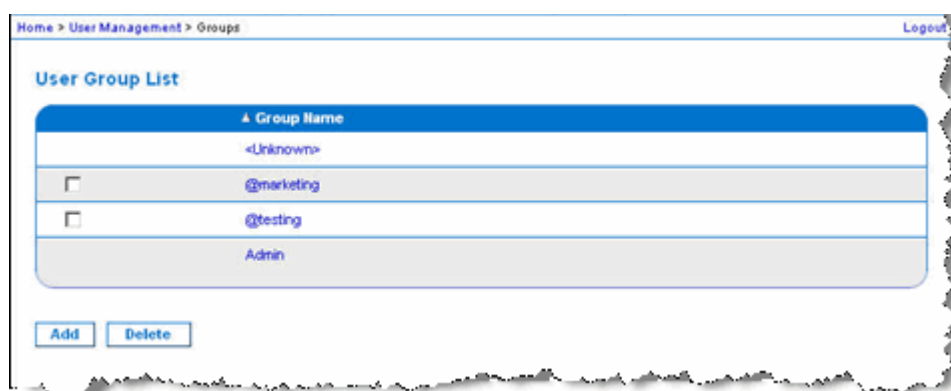
## 用户组列表

在本地验证和远程验证（通过 RADIUS 或 LDAP/LDAPS 进行的）中，要使用用户组。在创建个人用户之前定义用户组是个好主意，因为在添加一个用户时，必须给该用户指定一个现有用户组。

“用户组列表”页显示所有用户组的列表，可以单击“组名称”列标题按升序顺序或降序顺序排序用户组。还可以在“用户组列表”页上添加、修改或删除用户组。

### ▶ 列出用户组：

- 选择“用户管理>用户组列表”，打开“用户组列表”页。



## 用户和用户组之间的关系

用户属于一个用户组，用户组有权限。把 KX II-101-V2 的众多用户分成多个用户组，同时管理一个用户组里所有用户的权限，而不是分别管理每个用户的权限，这样可以节省时间。

也可以选择不让特定用户与用户组关联。在此情况下，可以把此用户归入个人用户组。

在成功验证之后，设备用用户组信息确定用户权限，例如哪些服务器端口可以访问，是否允许重新启动设备，能否执行其他功能。

## 添加新用户组

### ▶ 添加新用户组：

1. 选择 User Management（用户管理）> Add New User Group（添加新用户组），或者单击 User Group List（用户组列表）页上的 Add（添加）按钮。
2. 在 Group Name（组名）字段里输入新用户组的说明性名称（最多 64 个字符）。

- 选择要给予此用户组所有用户指定的权限旁边的复选框。参看 [设置权限](#) (p. 82)。

#### 设置端口权限

对于每个服务器端口，可以指定用户组具有的访问类型，以及虚拟媒体和电源控制的端口访问类型。请注意所有权限的默认设置是 **Deny**（拒绝）。

端口访问	
选项	说明
Deny（拒绝）	彻底拒绝访问
View（观看）	查看视频，但不与相连的目标服务器交互操作
Control（控制）	控制相连的目标服务器。如果同时授予虚拟媒体访问权和电源控制访问权，必须给此组指定控制。

虚拟媒体访问	
选项	说明
拒绝	端口彻底拒绝虚拟媒体权限。
只读	虚拟媒体访问仅限于读访问。
读写	虚拟媒体全访问（读写）。

电源控制访问	
选项	说明
Deny（拒绝）	拒绝对目标服务器进行电源控制
Access（访问）	目标服务器电源控制全访问

#### 基于组的 IP 访问控制表

**重要说明：**在使用基于组的 IP 访问控制时务必谨慎。如果 IP 地址在拒绝访问的地址范围内，可能无法访问 **KX II-101-V2**。



此功能按所选组里的用户，将 KX II-101-V2 设备访问限于特定 IP 地址。此功能仅应用于属于特定组的用户，与 IP 访问控制表功能不一样，后者应用于对设备进行的所有访问，首先处理，并确定优先级。

**重要说明：不能封锁 KX II-101-V2 本地端口使用的 IP 地址 127.0.0.1。**

使用 Group（用户组）页的 IP ACL 部分，根据用户组添加、插入、替换和删除 IP 访问控制规则。

#### ▶ 添加（附加）规则：

1. 在 Starting IP（开始 IP）字段里输入开始 IP 地址。
2. 在 Ending IP（结束 IP）字段里输入结束 IP 地址。
3. 在可用选项中选择操作：
  - Accept（接受）— 设置为 Accept（接受）的 IP 地址允许访问 KX II-101-V2 设备。
  - Drop（拒绝）— 设置为 Drop（拒绝）的 IP 地址拒绝访问 KX II-101-V2 设备。
4. 单击 Append（附加）。此规则被添加到规则列表末尾。对于要输入的每个规则，重复第一步到第四步。

#### ▶ 插入规则：

1. 输入规则编号（#）。在使用 Insert（插入）命令时，需要规则编号。
2. 在 Starting IP（开始 IP）和 Ending IP（结束 IP）字段里分别输入开始 IP 地址和结束 IP 地址。
3. 在 Action（操作）下拉列表上选择操作。
4. 单击 Insert（插入）。如果输入的规则编号与现有规则编号相同，将新规则放在现有规则前面，列表上的所有规则向下移。

#### ▶ 替换规则：

1. 指定要替换的规则编号。

2. 在 **Starting IP** (开始 IP) 和 **Ending IP** (结束 IP) 字段里分别输入开始 IP 地址和结束 IP 地址。
3. 在 **Action** (操作) 下拉列表上选择操作。
4. 单击 **Replace** (替换)。新规则取代规则编号相同的旧规则。

**删除规则：**

1. 指定要删除的规则编号。
2. 单击 **Delete** (删除) 按钮。
3. 在系统提示你确认删除时，单击 **OK** (确定) 按钮。

**重要说明：**按 **ACL** 规则的输入顺序对它们求值。例如此处的示例，如果两个 **ACL** 规则的顺序相反，**Dominion** 根本不接受通信。

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT
Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```

*提示：规则编号便于你更好地控制规则创建顺序。*

**设置权限**

**重要说明：**选择 **User Management** (用户管理) 复选框，允许用户组成员更改所有用户的权限，包括他们自己的权限。认真考虑是否要授予这些权限。

权限	说明
Device Access While Under CC-SG Management (在 CC-SG 管理下的设备访问)	<p>在 CC-SG 上针对 KX II-101-V2 设备启用 Local Access (本地访问) 之后，允许有此权限的用户和用户组用 IP 地址直接访问此设备。可以在 Remote Console、MPC、VKC 和 AKC 上访问此设备。</p> <p>在直接访问受 CC-SG 管理的设备时，在 KX II-101-V2 上记录访问活动和连接活动。根据 KX II-101-V2 验证设置执行用户验证。</p> <p><i>注意：Admin (管理员) 用户组默认有此权限。</i></p>
Device Settings (设备设置)	网络设置、日期/时间设置、端口配置 (通道名称和电源关联)、事件管理 (SNMP 和系统日志)、虚拟媒体文件服务器设置

权限	说明
Diagnostics( 诊断)	网络接口状态、网络统计数据、ping 主机、主机跟踪路由和 KX II-101-V2 诊断
Maintenance ( 维护)	备份和恢复数据库、固件升级、出厂默认设置复位和重新启动
Modem Access ( 调制解调器访问)	用调制解调器连接 KX II-101-V2 设备所需的权限。
PC-Share ( PC 共享)	多个用户同时访问同一台目标服务器
Security ( 安全)	SSL 证书、安全设置 ( 虚拟媒体共享和 PC 共享) 和 IP 访问控制表
User Management ( 用户管理)	用户和用户组管理、远程验证 (LDAP/LDAPS/RADIUS) 和登录设置

### 设置个人组权限

#### ▶ 设置个人用户组权限：

1. 在列出的用户组中找到个人用户组。个人组的组名里可能使用 @ 符号。
2. 单击 Group Name ( 组名称) ，打开 Group ( 用户组) 页。
3. 选择适当的权限。
4. 单击 OK ( 确定) 按钮。

---

### 修改现有用户组

---

*注意：给 Admin 用户组启用所有权限，你不能更改这些权限。*

---

#### ▶ 修改现有用户组：

1. 在 Group ( 用户组) 页上更改适当的字段，设置适当的权限。
2. 给该组设置 Permissions ( 权限) 。选择要给此组所有用户指定的权限前面的复选框。参看 [设置权限](#) (p. 82) 。
3. 设置 Port Permissions ( 端口权限) 。指定此组的用户可以访问的服务器端口 ( 和访问类型) 。参看 [设置端口权限](#) (p. 80) 。

4. 设置 IP ACL (IP 访问控制表) (可选)。此功能指定 IP 地址来限制对 KX II-101-V2 设备的访问。参看**基于组的 IP 访问控制表** (p. 80)。
5. 单击 OK (确定) 按钮。

▶ **删除用户组：**

---

**重要说明：**如果删除有用户的组，自动给这些用户指定<未知>用户组。

---

*提示：*为了确定特定用户组的用户，按用户组排序用户列表。

---

1. 单击“组名称”左边的复选框，在列出的组中选择一个组。
2. 单击“删除”按钮。
3. 在系统提示你确认删除时，单击“确定”按钮。

---

## 用户

必须给用户指定用户名和密码，才能访问 KX II-101-V2。当用户尝试访问 KX II-101-V2 时，要用这些信息验证用户。

---

### 查看 KX II-101-V2 用户列表

User List (用户列表) 页显示所有用户的列表，包括他们的用户名、全名和用户组。可以单击任何一个列名称，按任何一列排序列表。可以在 User List (用户列表) 页上添加、修改或删除用户。

如要查看每个用户连接的端口，参看按端口查看用户。

▶ **查看用户列表：**

- 选择 User Management (用户管理) > User List (用户列表)，打开 User List (用户列表) 页。

---

## 按端口查看用户

User By Ports（按端口查看用户）页列出已验证的所有本地用户和远程用户，以及他们连接的端口。只列出与端口之间的永久连接。

如果同一个用户在多个客户机上登录系统，本页针对他们建立的每个连接显示其用户名。例如如果一个用户在两个客户机上登录系统，列出两次他/她的姓名。

本页显示下列用户信息和端口信息：

- **Port Number**（端口号）— 给用户连接的端口指定的端口号
- **Port Name**（端口名称）— 给用户连接的端口指定的端口名称

---

*注意：如果用户不连接目标服务器，在 **Port Name**（端口名称）下面显示 **Local Console** 或 **Remote Console**。*

---

- **Username**（用户名）— 用户登录并建立目标服务器连接所用的用户名
- **Access From**（访问自）— 他们访问的 KX II-101-V2 的 IP 地址
- **Status**（状态）— 连接的当前活动状态或闲置状态

### ▶ 按端口查看用户：

- 选择 **User Management**（用户管理）> **User by Port**（按端口查看用户），打开 **User by Port**（按端口查看用户）页。

---

## 让用户断开端口

在让用户断开端口时，让他们断开目标服务器端口，但不让他们退出 KX II-101-V2。

---

*注意：在退出用户时，让他们断开目标服务器端口，并让他们退出 KX II-101-V2。参看让用户退出 KX II-101-V2（强制退出）(p. 86) 了解如何强制用户退出。*

---

### ▶ 让用户断开端口：

1. 选择 **User Management**（用户管理）> **User by Port**（按端口查看用户），打开 **User by Port**（按端口查看用户）页。
2. 选择要断开目标服务器的用户的用户名旁边的复选框。
3. 单击 **Disconnect User from Port**（让用户断开端口）按钮。
4. 单击确认消息窗口上的 **OK**（确定）按钮断开用户。
5. 显示一条确认消息，说明用户断开端口了。

---

### 让用户退出 KX II-101-V2 (强制退出)

如果你是管理员，可以让已登录 KX II-101-V2 的任何验证用户退出系统。也可以让用户在端口级断开端口。参看 [让用户断开端口](#) (p. 85)。

#### ▶ 让用户退出 KX II-101-V2 :

1. 选择 **User Management** (用户管理) > **User by Port** (按端口查看用户)，打开 **User by Port** (按端口查看用户) 页。
2. 选择要断开目标服务器的用户的用户名旁边的复选框。
3. 单击 **Force User Logoff** (强制用户退出) 按钮。
4. 单击 **Logoff User** (退出用户) 确认消息窗口上的 **OK** (确定) 按钮。

---

### 添加新用户

最好在创建 KX II-101-V2 用户之前先定义用户组，因为在添加用户时，必须给用户指定一个现有用户组。参看 [添加新用户组](#)。

可以在 **User** (用户) 页上添加新用户，修改用户信息，重新激活被停用的用户。

---

*注意：在登录失败次数超过在 **Security Settings** (安全设置) 页上设置的最大登录尝试次数之后，可以停用用户名。参看 [安全设置](#) (p. 133)。*

---

#### ▶ 添加新用户：

1. 选择“用户管理>添加新用户”，或者单击“用户列表”页上的“添加”按钮。
2. 在“用户名”字段里输入唯一姓名（最长 16 个字符）。
3. 在“全名”字段里输入用户全名（最长 64 个字符）。
4. 在“密码”字段里输入密码，在“确认密码”字段里再次输入密码（最长 64 个字符）。
5. 在“用户组”下拉列表上选择用户组。

如果不想使此用户与现有 **User Group** (用户组) 关联，在下拉列表上选择 **Individual Group** (个人组)。如要进一步了解如何设置个人组权限，参看 [设置个人组权限](#) (p. 83)。

6. 如要激活此新用户，选择“活动”复选框。单击“确定”按钮。

---

## 修改现有用户

### ▶ 修改现有用户：

1. 选择 **User Management**（用户管理）> **User List**（用户列表），打开 **User List**（用户列表）页。
2. 在 **User List**（用户列表）页列出的用户中找到要修改的用户。
3. 单击用户名。打开 **User**（用户）页。
4. 在 **User**（用户）页上更改适当的字段。参看 **添加新用户** (p. 86)，了解如何访问 **User**（用户）页。
5. 如要删除用户，单击 **Delete**（删除）按钮。系统提示你确认删除。
6. 单击 **OK**（确定）按钮。

---

## 用户锁定和解锁

管理员可以阻止用户访问系统，也可以由系统根据安全设置自动阻止用户。参看 **用户锁定** (p. 136)。被锁定的用户变成不活动用户，管理员可以解除锁定，让他/她再次成为活动用户。

### ▶ 用户锁定或解锁：

1. 选择 **User Management**（用户管理）> **User List**（用户列表），打开 **User List**（用户列表）页。
2. 选择或取消 **Active**（活动）复选框。
  - 如果选择此复选框，用户变成活动用户，被授予 **KX II-101-V2** 访问权。
  - 如果取消此复选框，用户变成不活动用户，不能访问 **KX II-101-V2**。
3. 单击 **OK**（确定）按钮，更新用户的活动状态。

---

## 验证设置

验证是确定用户是否是他/她声称的人这一过程。在验证用户之后，用该用户的组确定其系统权限和端口权限。用户的指定权限决定授予他/她哪种访问权。这叫授权。

如果给 KX II-101-V2 配置了远程验证，外部验证服务器主要用于验证，而不是授权。

---

*注意：即使选择远程验证（LDAP/LDAPS 或 RADIUS），如果找不到用户，仍然选择本地验证数据库。*

---

### ▶ 配置验证：

1. 选择“用户管理>验证设置”，打开“验证设置”页。
2. 选择要使用的验证协议选项（本地验证、LDAP/LDAPS 或 RADIUS）。如果选择 LDAP 选项，激活其余 LDAP 字段；如果选择 RADIUS 选项，激活其余 RADIUS 字段。
3. 如果选择“本地验证”，跳到第六步。
4. 如果选择 LDAP/LDAPS，阅读实现 LDAP 远程验证一节，了解如何填写“验证设置”页上 LDAP 部分的字段。
5. 如果选择 RADIUS，阅读实现 RADIUS 远程验证一节，了解如何填写“验证设置”页上 RADIUS 部分的字段。
6. 单击“确定”按钮保存设置。

### ▶ 恢复出厂默认设置：

- 单击“复位到默认设置”按钮。

---

### 实现 LDAP/LDAPS 远程验证

Lightweight Directory Access Protocol (LDAP/LDAPS) 是联网协议，用于查询基于 TCP/IP 运行的目录服务。客户机连接 LDAP/LDAPS 服务器（默认 TCP 端口是 389），开始 LDAP 会话。客户机给服务器发送操作请求，服务器返回响应。

---

*提示：Microsoft Active Directory 在本机充当 LDAP/LDAPS 验证服务器。*

---

### ▶ 使用 LDAP 验证协议：

1. 单击 User Management（用户管理）> Authentication Settings（验证设置），打开 Authentication Settings（验证设置）页。
2. 选择 LDAP 单选按钮启用本页的 LDAP 部分。



- 单击  图标展开本页的 LDAP 部分。

### 服务器配置

- 在 Primary LDAP Server (主 LDAP 服务器) 字段里输入 LDAP/LDAPS 远程验证服务器的 IP 地址或 DNS 名称 (最多 256 个字符)。在选择 Enable Secure LDAP (启用安全 LDAP) 选项和 Enable LDAPS Server Certificate Validation (启用 LDAPS 服务器证书验证) 选项之后, 必须使用 DNS 名称与 LDAP 服务器证书的 CN 相匹配。
- 在 Secondary LDAP Server (备用 LDAP 服务器) 字段里输入 LDAP/LDAPS 服务器的 IP 地址或 DNS 名称 (最多 256 个字符)。在选择 Enable Secure LDAP (启用安全 LDAP) 选项之后, 必须使用 DNS 名称。注意其他字段共享 Primary LDAP Server (主 LDAP 服务器) 字段的设置。**可选**
- 外部 LDAP 服务器的类型。
- 选择外部 LDAP/LDAPS 服务器。在下列可用选项中选择:
  - Generic LDAP Server (通用 LDAP 服务器)。
  - Microsoft Active Directory。Active Directory 是 Microsoft 在 Windows 环境下实现的 LDAP/LDAPS 目录服务。
- 如果选择了 Microsoft Active Directory 输入 Active Directory Domain (Active Directory 域) 名称, 例如 *acme.com*。向 Active Directory 管理员索取特定域名。
- 在 User Search DN (用户搜索标识名) 字段里输入标识名, 说明在 LDAP 数据库的什么地方开始搜索用户信息。最长可以使用 64 个字符。基本搜索值示例: `cn=Users,dc=raritan,dc=com`。向验证服务器管理员咨询在这些字段输入的适当值。
- 在 DN of Administrative User (管理用户标识名) 字段里输入管理用户标识名 (最多 64 个字符)。如果 LDAP 服务器只允许管理员以管理用户身份搜索用户信息, 填写此字段。向验证服务器管理员咨询在此字段输入的适当值。管理用户标识名值示例:  
`cn=Administrator,cn=Users,dc=testradius,dc=com`。**可选**

11. 如果输入了 Distinguished Name for the Administrative User (管理用户标识名), 必须输入在远程验证服务器上验证管理用户标识名时所用的密码。在 Secret Phrase (密码) 字段里输入密码, 在 Confirm Secret Phrase (确认密码) 字段里再次输入密码 (最长 128 个字符)。

**Authentication Settings**

Local Authentication

LDAP

RADIUS

**LDAP**

**Server Configuration**

**Primary LDAP Server**  
192.168.59.187

**Secondary LDAP Server (optional)**  
192.168.51.214

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

**Active Directory Domain**  
testradius.com

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

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

**Secret Phrase of Administrative User**  
.....

**Confirm Secret Phrase**

#### LDAP/LDAP 安全

12. 如果要使用 SSH, 选择 Enable Secure LDAP (启用安全 LDAP) 复选框。启用 Enable LDAPS Server Certificate Validation (启用 LDAPS 服务器证书验证) 复选框。Secure Sockets Layer (SSL) 是允许 KX II-101-V2 与 LDAP/LDAPS 服务器通信的加密协议。
13. 默认 Port (端口) 是 389。既可以使用标准 LDAP TCP 端口, 也可以指定另一个端口。

14. 默认 Secure LDAP Port (安全 LDAP 端口) 是 636。既可以使用默认端口，也可以指定另一个端口。只有在选择 Enable Secure LDAP (启用安全 LDAP) 复选框之后，才启用此字段。
15. 选择 Enable LDAPS Server Certificate Validation (启用 LDAPS 服务器证书验证) 复选框，用此前上载的 CA 根证书文件验证服务器提供的证书。如果不想使用此前上载的 CA 根证书文件，不要选择此复选框。如果禁用此功能，表示接受未知认证机构签发的证书。只有在选择 Enable Secure LDAP (启用安全 LDAP) 复选框之后，才能使用此复选框。

---

*注意：如果选择 Enable LDAPS Server Certificate Validation (启用 LDAPS 服务器证书验证) 选项，除了使用 CA 根证书验证，服务器主机名必须与服务器证书上的公用名相匹配。*

---

16. 必要时上载 CA 根证书文件。如果选择了“启用安全 LDAP”复选框，启用此字段。咨询验证服务器管理员，获取 LDAP 服务器所用的 Base64 编码 X-509 格式的 CA 证书文件。单击“浏览”按钮找到证书文件。如果用新证书取代 LDAP/LDAPS 服务器证书，必须重新启动 KX II-101-V2，新证书才生效。



**LDAP / Secure LDAP**

Enable Secure LDAP

**Port**  
389

**Secure LDAP Port**  
636

Enable LDAPS Server Certificate Validation

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

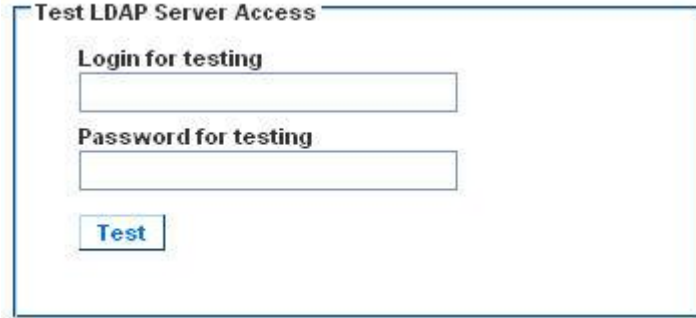
Upload

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

### 测试 LDAP 服务器访问

17. 由于成功配置 LDAP 服务器和 KX II-101-V2 进行远程验证有时很复杂，所以 KX II-101-V2 使你能在 Authentication Settings (验证设置) 页上测试 LDAP 配置。为了测试 LDAP 配置，分别在 Login for testing (测试登录名) 和 Password for testing (测试密码) 字段里输入登录名和密码。这是你为访问 KX II-101-V2 输入的用户名和密码，LDAP 服务器将用它们验证你的身份。单击 Test (测试) 按钮。

在测试完成之后显示一条消息，告诉你测试成功了；如果测试失败，将显示详细错误消息。显示成功结果，或者详细说明失败错误消息。如果测试成功，还显示在 LDAP 服务器上检索的有关测试用户的组信息。



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

---

### Active Directory 服务器返回用户组信息

KX II-101-V2 支持用 Active Directory® (AD) 进行用户验证，不要求在 KX II-101-V2 本地定义用户。这样，可以在 AD 服务器上单独维护 Active Directory 用户帐号和密码。授权和 AD 用户权限通过标准 KX II-101-V2 策略和用户组权限控制和管理，其中策略和用户组权限在本地应用于 AD 用户组。

---

**重要事项：**如果你是现有的 Raritan 客户，已经通过更改 AD 模式配置了 Active Directory 服务器，KX II-101-V2 仍然支持此配置，你不必执行下列操作。参看更新 LDAP 模式了解如何更新 AD LDAP/LDAPS 模式。

---

► 在 KX II-101-V2 上启用 AD 服务器：

1. 用 KX II-101-V2 创建特殊用户组，给这些用户组指定适当的权限，例如创建 KVM\_Admin 和 KVM\_Operator 等用户组。
2. 在 Active Directory 服务器上创建新用户组，其名称与在上一步中使用的名称相同。
3. 在 AD 服务器上给 KX II-101-V2 用户指定在第二步中创建的用户组。
4. 在 KX II-101-V2 上正确启用和配置 AD 服务器。参看 **实现 LDAP/LDAPS 远程验证** (p. 88)。

### 重要说明

- 组名称区分大小写。
- KX II-101-V2 有下列不能更改或删除的默认用户组：管理员和<未知>。确认 Active Directory 服务器不使用相同的用户组名称。
- 如果 Active Directory 服务器返回的用户组信息不匹配 KX II-101-V2 用户组配置，KX II-101-V2 自动给成功验证的用户指定<未知>用户组。

### 实现 LDAP/LDAPS 远程验证

Remote Authentication Dial-in User Service (RADIUS) 是供网络访问应用程序使用的 AAA (authentication, authorization, and accounting) 协议。

#### ▶ 使用 RADIUS 验证协议：

1. 单击 User Management (用户管理) > Authentication Settings (验证设置)，打开 Authentication Settings (验证设置) 页。
2. 单击 RADIUS 单选按钮启用本页的 RADIUS 部分。
3. 单击  图标展开本页的 RADIUS 部分。
4. 在 Primary RADIUS Server (主 RADIUS 服务器) 字段和 Secondary RADIUS Server (备用 RADIUS 服务器) 字段里分别输入主远程验证服务器和备用远程验证服务器的 IP 地址 (最多 256 个字符)。
5. 在 Shared Secret (共享密码) 字段里输入验证所用的服务器密码 (最多 128 个字符)。

共享密码是 KX II-101-V2 和 RADIUS 服务器进行安全通信所要了解的字符串。它从本质上讲是密码。

6. 默认 Authentication Port (验证端口) 是 1812，但可以按需要更改端口。
7. 默认 Accounting Port (记帐端口) 是 1813，但可以按需要更改端口。
8. Timeout (超时) 按秒记录，默认超时是 1 秒，但可以按需要更改超时。

超时是 KX II-101-V2 在发送另一个验证请求之前，等待 RADIUS 服务器做出响应的的时间。

9. Retries (重试次数) 默认次数是 3 次。

这是 KX II-101-V2 给 RADIUS 服务器发送一个验证请求的次数。

10. 在 Global Authentication Type (全局验证类型) 下拉列表上选择选项：
  - PAP — 如果选择 PAP，采用纯文本方式发送密码。PAP 不支持交互操作。在建立连接之后，作为数据包发送用户名和密码，而不是让服务器发送登录提示并等待响应。

- CHAP — 如果选择 CHAP，服务器随时可以请求验证。CHAP 的安全性比 PAP 高。

Home > User Management > Authentication Settings

**Authentication Settings**

Local Authentication  
 LDAP  
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type  
PAP ▼

### 通过 RADIUS 返回用户组信息

当 RADIUS 验证尝试成功时，KX II-101-V2 根据给定用户的组的权限确定他/她的权限。

远程 RADIUS 服务器可以返回作为 RADIUS FILTER-ID 实现的属性，从而提供这些用户组名称。FILTER-ID 应该如下格式化：  
Raritan:G{GROUP\_NAME}，其中 GROUP\_NAME 字符串是用户所属组的名称。

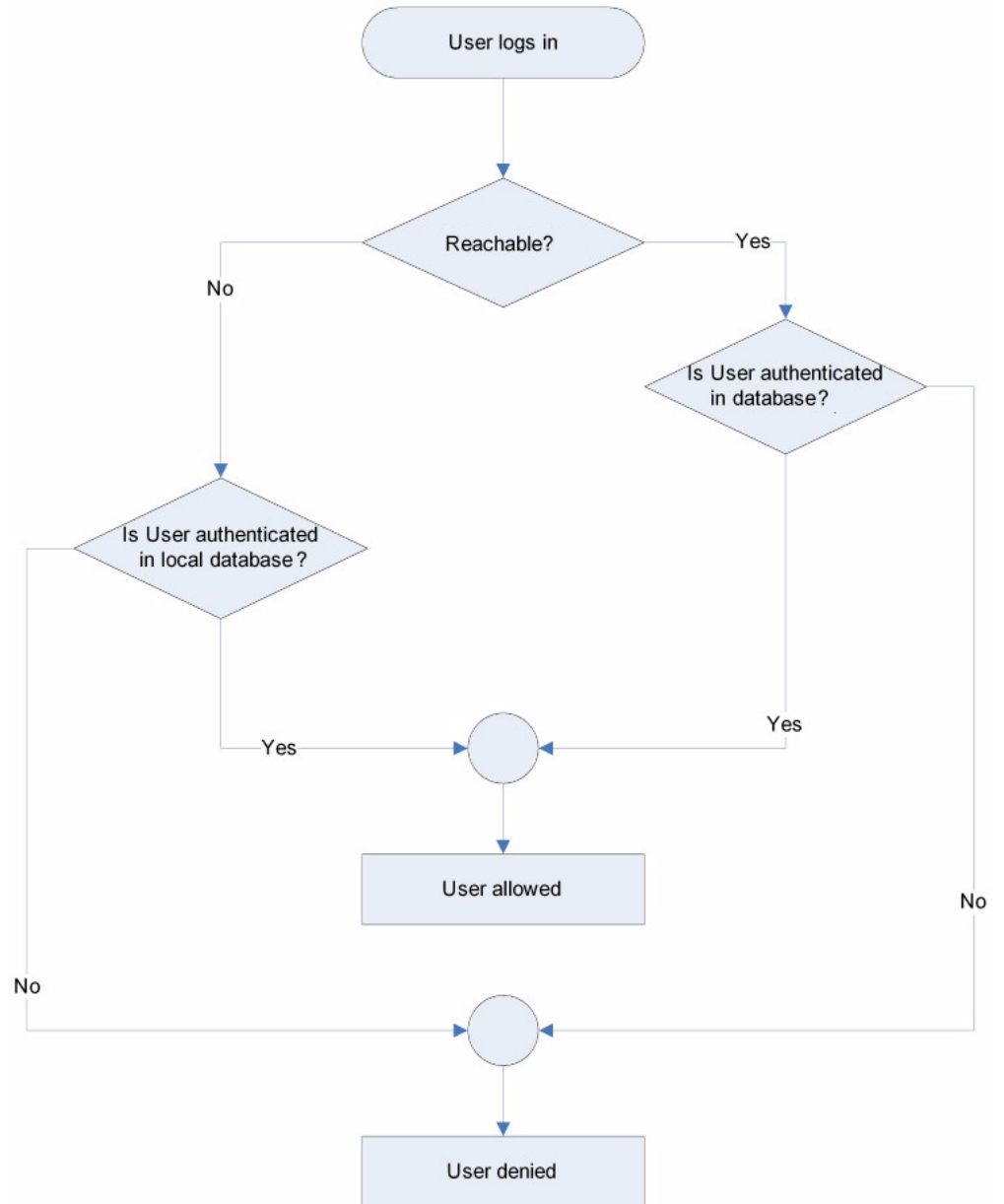
**RADIUS 通信交换规范**

KX II-101-V2 把下列 RADIUS 属性发送到 RADIUS 服务器：

属性	数据
<b>登录</b>	
Access-Request (1)	
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-IP-Address (4)	KX II-101-V2 的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	记帐用的会话 ID。
User-Password (2)	加密密码。
<b>开始记帐</b>	
Accounting-Request(4)	
Acct-Status (40)	Start(1) — 开始记帐。
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-Port (5)	始终是 0。
NAS-IP-Address (4)	KX II-101-V2 的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	记帐用的会话 ID。
<b>退出</b>	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) — 停止记帐。
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-Port (5)	始终是 0。
NAS-IP-Address (4)	KX II-101-V2 的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	记帐用的会话 ID。

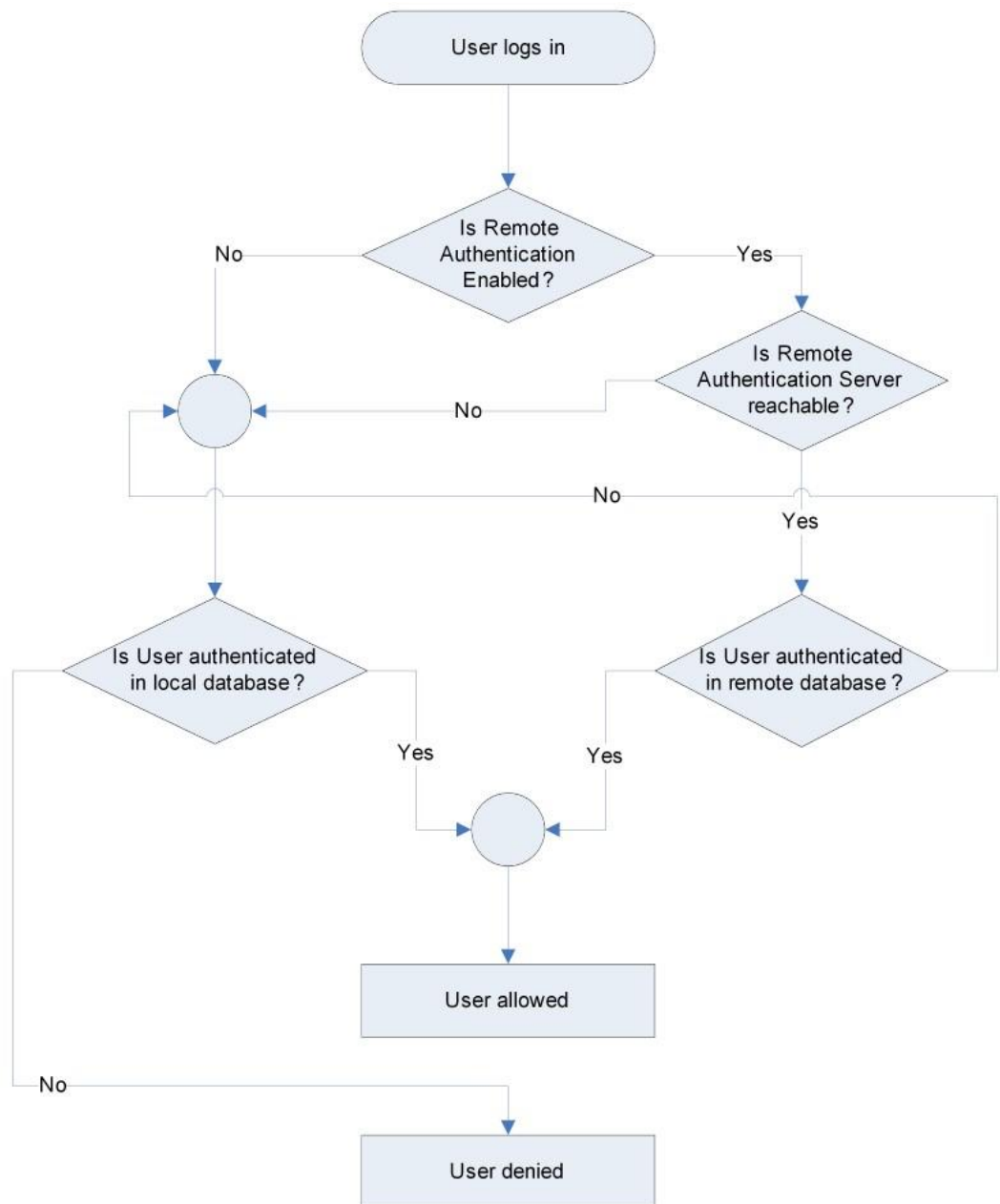
### 用户验证流程

在配置设备验证和授权本地用户时，根据下列流程顺序验证用户证书：





远程验证流程如下图所示：



---

## 更改密码

► **更改密码：**

1. 选择 **User Management(用户管理) > Change Password(更改密码)**。  
打开 **Change Password (更改密码)** 页。
2. 在 **Old Password (旧密码)** 字段里输入当前密码。
3. 在 **New Password (新密码)** 字段里输入新密码。在 **Confirm New Password (确认新密码)** 字段里再次输入新密码。密码最长为 64 个字符，可以包含英文字母数字字符和特殊字符。
4. 单击 **OK (确定)** 按钮。
5. 显示确认信息，说明密码更改成功。单击 **OK (确定)** 按钮。

---

*注意：如果使用强密码，本页显示强密码格式信息。如要进一步了解密码和强密码，参看[强密码](#) (p. 134)。*

---

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

## 在本章内

网络设置 .....	99
设备服务 .....	104
键盘/鼠标设置 .....	108
串行端口设置 .....	108
配置日期/时间设置 .....	110
事件管理 .....	111
端口配置 .....	119
模拟 KVM 切换器 .....	126
用复位按钮复位 KX II-101-V2 .....	127
更改默认图形用户界面语言设置 .....	128

---

**网络设置**

用 **Network Settings** (网络设置) 页定制 KX II-101-V2 网络配置 (例如 IP 地址、发现端口和 LAN 接口参数)。

有两个选项可用于设置 IP 配置：

- **None** (无, 默认值) — 这是建议的选项 (静态 IP)。由于 KX II-101-V2 是网络基础设施的组成部分, 很可能不希望 IP 地址频繁变化。此选项使你能设置网络参数。
- **DHCP** — 如果选择此选项, 由 DHCP 服务器自动分配 IP 地址。

▶ **更改网络配置：**

1. 选择 **Device Settings** (设备设置) > **Network** (网络)。打开 **Network Settings** (网络设置) 页。
2. 更新 **Network Basic Settings** (基本网络设置)。参看 **安全基本设置** (参看 "**网络基本设置**" p. 100)。
3. 更新 **LAN Interface Settings** (LAN 接口设置)。参看 **LAN 接口设置** (p. 103)。
4. 单击 **OK** (确定) 按钮设置这些配置。如果所作的更改要求重新启动设备, 显示一条重新启动消息。

▶ **复位到出厂前默认值：**

- 单击 **Reset to Defaults** (复位到默认值)。

## 网络基本设置

下列步骤说明如何在 **Network Settings**（网络设置）页上分配 IP 地址。参看 **网络设置** (p. 99) 全面了解本页上的所有字段和操作。

### ► 分配 IP 地址：

1. 选择 **Device Settings**（设备设置）> **Network**（网络），打开 **Network Settings**（网络设置）页。
2. 给 **KX II-101-V2** 设备指定有意义的设备名称。名称最长 32 个字母数字字符，可以使用有效特殊字符，但不能使用空格。
3. 在 **IPv4** 部分输入或选择合适的 **IPv4** 网络设置：
  - a. 必要时在 **IP Address**（IP 地址）字段里输入 IP 地址。默认 IP 地址是 **192.168.0.192**。
  - b. 在 **Subnet Mask**（子网掩码）字段里输入子网掩码。默认子网掩码是 **255.255.255.0**。
  - c. 如果在 **IP Auto Configuration**（IP 自动配置）下拉列表上选择了 **None**（无），在 **Default Gateway**（默认网关）字段里输入默认网关。
  - d. 如果在 **IP Auto Configuration**（IP 自动配置）下拉列表上选择了 **DHCP**，在 **Preferred DHCP Host Name**（首选 DHCP 主机名）字段里输入首选 DHCP 主机名。
  - e. 选择 **IP Auto Configuration**（IP 自动配置）。有三个选项可供选择：
    - **None (Static IP)**（无[静态 IP]）— 此选项要求你人工指定网络参数。  
建议你选择此选项，因为 **KX II-101-V2** 是基础设施设备，其 IP 地址不应发生变化。
    - **DHCP** — 联网计算机（客户机）用 **Dynamic Host Configuration Protocol**（动态主机配置协议）获取 **DHCP** 服务器分配的唯一 IP 地址和其他参数。  
如果选择此选项，**DHCP** 服务器分配网络参数。如果使用 **DHCP**，在 **Preferred host name**（首选主机名）字段里输入首选主机名（仅限于 **DHCP**）。最长 63 个字符。
4. 如果要使用 **IPv6**，在 **IPv6** 部分输入或选择合适的 **IPv6** 网络设置：
  - a. 选择 **IPv6** 复选框，激活这部分的字段。
  - b. 在 **Global/Unique IP Address**（全局/唯一 IP 地址）字段里输入全局/唯一 IP 地址。这是给 **KX II-101-V2** 分配的 IP 地址。

- c. 在 **Prefix Length** (前缀长度) 字段里输入前缀长度。这是 IPv6 地址使用的位数。
- d. 在 **Gateway IP Address** (网关 IP 地址) 字段里输入网关 IP 地址。
- e. **Link-Local IP Address** (链路-本地 IP 地址)。自动给设备分配此地址，用于发现邻居，或者在没有路由器时使用。只读
- f. **Zone ID** (域 ID)。标识与此地址关联的设备。只读
- g. 选择 **IP Auto Configuration** (IP 自动配置)。有三个选项可供选择：
  - **None** (无) — 如果不想使用自动 IP 配置，而是自己设置 IP 地址 (静态 IP)，使用此选项。这是默认选项，建议使用此选项。  
如果给 **IP auto configuration** (IP 自动配置) 选择 **None** (无)，启用下列网络基本设置字段：**Global/Unique IP Address** (全局/唯一 IP 地址)、**Prefix Length** (前缀长度) 和 **Gateway IP Address** (网关 IP 地址)，你可以人工设置 IP 配置。
  - **Router Discovery** (路由器发现) — 用此选项自动分配 IPv6 地址，这些地址具有 **Global** (全局) 或 **Unique Local** (唯一本地) 意义，超出了 **Link Local** (链路本地) 的意义，仅适用于直接连接的子网。
5. 如果选择了 **DHCP** 并启用了 **Obtain DNS Server Address** (获取 DNS 服务器地址)，选择 **Obtain DNS Server Address Automatically** (自动获取 DNS 服务器地址)。在选择 **Obtain DNS Server Address Automatically** (自动获取 DNS 服务器地址) 之后，将使用 DHCP 服务器分配的 DNS 信息。
6. 如果选择了 **Use the Following DNS Server Addresses** (使用下列 DNS 服务器地址)，无论是否选择了 **DHCP**，均用在此输入的地址连接 DNS 服务器。  
如果选择了 **Use the Following DNS Server Addresses** (使用下列 DNS 服务器地址) 选项，输入下列信息。这些地址分别是主 DNS 地址和备用 DNS 地址，当主 DNS 服务器连接由于中断而断开时，将使用备用 DNS 地址。
  - a. **Primary DNS Server IP Address** (主 DNS 服务器 IP 地址)
  - b. **Secondary DNS Server IP Address** (备用 DNS 服务器 IP 地址)
7. 在填写完之后，单击 **OK** (确定) 按钮。

参看 **LAN 接口设置** (p. 103)了解如何配置 Network Settings (网络设置) 页的这个部分。

*注意：在某些环境下，默认 LAN Interface Speed & Duplex (LAN 接口速度和双工) 设置中的 Autodetect (autonegotiator) (自动检测[自动协商]) 并不能正确设置网络参数，会引发网络问题。在这些情况下，把 KX II-101-V2 LAN Interface Speed & Duplex (KX II-101-V2 LAN 接口速度和双工) 设置为 100 Mbps/Full Duplex (全双工) 或与网络相适应的其他选项，可以解决这个问题。参看**网络设置** (p. 99)页了解详情。*

**Basic Network Settings**

Device Name \*  
se-4x2-232

**IPv4 Address**

IP Address	Subnet Mask
192.168.51.55	255.255.255.0
Default Gateway	Preferred DHCP Host Name
192.168.51.126	

IP Auto Configuration  
DHCP

**IPv6 Address**

Global Unique IP Address	Prefix Length
	/
Gateway IP Address	
Link-Local IP Address	Zone ID
::A	%1

IP Auto Configuration  
None

Obtain DNS Server Address Automatically

Use the Following DNS Server Addresses

Primary DNS Server IP Address
192.168.59.2
Secondary DNS Server IP Address
192.168.51.10

OK Reset To Defaults Cancel

---

## LAN 接口设置

Current LAN interface parameters (当前 LAN 接口参数) 字段显示当前参数设置。

- 选择 LAN Interface Speed & Duplex (LAN 接口速度和双工) 设置。
  - Autodetect (自动检测, 默认选项)
  - 10 Mbps/Half (10 Mbps/半双工) — 黄色 LED 指示灯闪烁
  - 10 Mbps/Full (10 Mbps/全双工) — 黄色 LED 指示灯闪烁
  - 100 Mbps/Half (100 Mbps/半双工) — 黄色 LED 指示灯闪烁, 绿色 LED 指示灯常亮
  - 100 Mbps/Full (100 Mbps/全双工) — 黄色 LED 指示灯闪烁, 绿色 LED 指示灯常亮

半双工提供双向通信, 但每次只允许一个方向通信, 不允许双向同时通信。

全双工允许双向同时通信。

---

*注意: 在半双工或全双工通信中, 以 10 Mbps 运行时偶尔也会出问题。如果出问题, 尝试使用另一个速度和双工。*

---

参看 **网络基本设置** (see "**Network Speed Settings**" p. 182)。

- 选择 Bandwidth Limit (带宽限制)。
  - No Limit (无限制)
  - 128 KB
  - 256 KB
  - 512 KB
  - 2 MB
  - 5 MB
  - 10 MB
  - 100 MB

需要新截屏

---

## 设备服务

可以在 **Device Services**（设备服务）页上配置下列功能：

- 启用 SSH 访问
- 输入发现端口
- 启用直接端口访问
- 启用 Telnet 访问
- 配置 HTTP 和 HTTPS 设置
- 配置 SNMP 代理

---

### 启用 Telnet

如果要用 Telnet 访问 KX II-101-V2，必须先在命令行界面或浏览器上访问 KX II-101-V2。

▶ **启用 Telnet：**

1. 选择 **Device Settings**（设备设置）> **Device Services**（设备服务），然后选择 **Enable TELNET Access**（启用 Telnet 访问）复选框。
2. 输入 Telnet 端口号。
3. 单击 **OK**（确定）按钮。

在启用 Telnet 访问之后，可以用它访问 KX II-101-V2 并设置其余参数。

---

### 启用 SSH

启用 SSH 访问，允许管理员通过 SSH v2 应用程序访问 KX II-101-V2。

▶ **启用 SSH 访问：**

1. 选择 **Device Settings**（设备设置）> **Device Services**（设备服务），打开 **Device Service Settings**（设备服务设置）页。
2. 选择 **Enable SSH Access**（启用 SSH 访问）。
3. 输入 **SSH Port**（SSH 端口）信息。标准 SSH TCP 端口号是 22，但可以更改端口号提高安全操作水平。
4. 单击 **OK**（确定）按钮。



---

## HTTP 和 HTTPS 端口设置

可以配置供 KX II-101-V2 使用的 HTTP 端口和/或 HTTPS 端口。例如如果把默认 HTTP 端口 80 用于其他目的，更改此端口可以确保设备不尝试使用此端口。

### 更改 HTTP 和/或 HTTPS 端口设置：

1. 选择 **Device Settings**（设备设置）> **Device Services**（设备服务），打开 **Device Service Settings**（设备服务设置）页。
2. 在 **HTTP Port**（HTTP 端口）字段和/或 **HTTPS Port**（HTTPS 端口）字段里输入新端口。
3. 单击 **OK**（确定）按钮。

---

## 输入发现端口

KX II-101-V2 在一个可配置的 TCP 端口上执行发现。默认值是端口 5000，但可以配置使用除 80 和 443 之外的任何 TCP 端口。为了越过防火墙访问 KX II-101-V2，防火墙设置必须允许通过默认端口 5000 或在此配置的非默认端口进行双向通信。

### 启用发现端口：

1. 选择 **Device Settings**（设备设置）> **Device Services**（设备服务），打开 **Device Service Settings**（设备服务设置）页。
2. 输入 **Discovery Port**（发现端口）。
3. 单击 **OK**（确定）按钮。

---

## 启用通过 URL 进行直接端口访问

直接端口访问允许用户绕过设备的 **Login**（登录）对话框和 **Port Access**（端口访问）页。此功能还允许用户在 URL 不包含用户名和密码的情况下，直接输入用户名和密码访问目标服务器。

下面说明有关直接端口访问的重要 URL 信息：

如果使用 VKC 和直接端口访问：

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

### 启用直接端口访问：

1. 选择 **Device Settings**（设备设置）> **Device Services**（设备服务），打开 **Device Service Settings**（设备服务设置）页。

2. 如果希望用户通过 URL 传递必要参数，通过 **Dominion** 直接访问目标服务器，选择 **Enable Direct Port Access via URL**（启用通过 URL 进行直接端口访问）。
3. 单击 **OK**（确定）按钮。

---

### 配置 SNMP 代理

符合 SNMP 规范的设备（称为代理）把有关它们的数据存储在管理信息库 (MIB) 里，并把这些数据返回给 SNMP 管理器。参看[查看 KX II-101-V2 MIB](#) (p. 116) 了解如何查看 KX II-101-V2 MIB。

---

*KX II-101-V2 支持 SNMP v1/v2c 和/或 v3 版本的 SNMP 日志。在启用 SNMP 日志之后，SNMP v1/v2c 定义消息格式和协议操作。SNMP v3 是 SNMP 的安全扩展，提供用户验证、密码管理和加密。*

---

#### ▶ 配置 SNMP 代理：

1. 选择 **Device Settings**（设备设置）> **Device Services**（设备服务），打开 **Device Service Settings**（设备服务设置）页。
2. 输入 MIB-II System Group 对象的下列 SNMP 代理标识符信息：
  - a. **System Name**（系统名称）— SNMP 代理的名称/设备名称
  - b. **System Contact**（系统联系人）— 与设备相关的联系人姓名
  - c. **System Location**（系统位置）— 设备位置
3. 选择 **Enable SNMP v1/v2c**（启用 SNMP v1/v2c）和/或 **Enable SNMP v3**（启用 SNMP v3）。至少要选择一项。<必需>
4. 填写下列 SNMP v1/v2c 陷阱字段（必要时）：
  - a. **Community**（公用名）— 设备的公用串
  - b. **Community Type**（公用名类型）— 给公用名用户指定 **Read-Only**（只读）访问权或 **Read-Write**（读写）访问权。

---

*注意：SNMP 公用名是设备和运行 SNMP 的工作站所属的设备组，有助于定义要把信息发送到哪里。公用名用于标识此设备组。SNMP 设备或代理可能属于多个 SNMP 公用名。*

---

5. 填写下列 SNMP v3 陷阱字段（必要时）：
  - a. 如果需要验证密码，选择 **Use Auth Passphrase**（使用验证密码）。如果需要 **Privacy Passphrase**（隐私密码），可以选择 **Use Auth Passphrase**（使用验证密码）使用相同密码，不必再次输入 **Auth Passphrase**（验证密码）。
  - b. **Security Name**（安全名称）— 要与 SNMP 代理通信的实体的用户名或服务帐号名（最长 32 个字符）。

- c. Authentication Protocol (验证协议) — SNMP v3 代理使用的 MD5 或 SHA 验证协议
  - d. Authentication Passphrase (验证密码) — 访问 SNMP v3 代理所需的密码 (最长 64 个字符)
  - e. Privacy Protocol (隐私协议) — 必要时用于加密 PDU 和上下文数据的 AES 算法或 DES 算法
  - f. Privacy Passphrase (隐私密码) — 访问隐私协议算法所需的密码 (最长 64 个字符)
6. 单击 OK (确定) 按钮启动 SNMP 代理服务。

在 Event Management - Settings (事件管理 — 设置) 页上配置 SNMP 陷阱, 可以单击 SNMP Trap Configuration (SNMP 陷阱配置) 链接迅速打开此页面。参看配置 SNMP 陷阱了解如何创建 SNMP 陷阱, 参看 KX II-101-V2 SNMP 陷阱列表了解所有可用的 KX II-101-V2 SNMP 陷阱。

在配置 SNMP 陷阱之后, 在 Event Management - Destination (事件管理 — 目标) 页上选择已捕捉的事件。参看配置事件管理 — 目的地。

▶ **复位到出厂默认设置：**

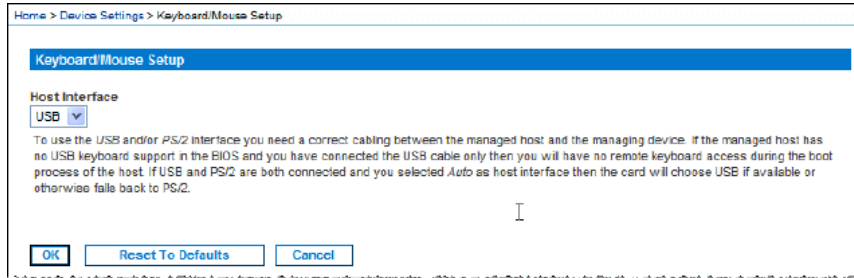
- 单击 Reset to Defaults (复位到默认设置) 按钮。本页上的所有项都设置为默认值。

警告：在使用基于 UDP 的 SNMP 陷阱时, 在重新启动 KX II-101-V2 之后, KX II-101-V2 和相连的路由器可能会不同步, 致使重新启动操作不能完成 SNMP 陷阱记录。

---

## 键盘/鼠标设置

用 Keyboard/Mouse Setup (键盘/鼠标设置) 页配置 KX II-101-V2 和主机设备之间的键盘接口和鼠标接口。



1. 单击 Device Settings (设备设置) > Keyboard/Mouse (键盘/鼠标)。
2. 选择 Host Interface (主机接口)。此选择决定 KX II-101-V2 是通过 PS/2 连接还是 USB 连接发送键盘数据和鼠标数据。
  - Auto (自动) — 在选择此设置之后, 如果 USB 连接可用, KX II-101-V2 使用此连接, 否则使用 PS/2 连接。
  - USB — 强制 KX II-101-V2 用 USB 连接把键盘数据和鼠标数据发送到主机设备。
  - PS/2 — 强制 KX II-101-V2 用 PS/2 连接把键盘数据和鼠标数据发送到主机设备。

---

*注意: 如果在前端使用 Raritan 切换器和 KX II-101-V2, 必须把主机接口设置为 PS/2, 配置才能正常工作。参看模拟 KVM 切换器 (p. 126)。*

---

3. 单击 OK (确定) 按钮。
- ▶ **复位到出厂前默认设置:**
- 单击 Reset to Defaults (复位到默认设置)。

---

## 串行端口设置

用 Serial Port Settings (串行端口设置) 页设置 KX II-101-V2 如何使用集成的串行端口。

---

## 管理端口

### ▶ 配置管理串行端口：

1. 选择 **Device Settings**(设备设置)> **Serial Port**(串行端口) 打开 **Serial Port Settings** (串行端口设置) 页。
2. 选择 **Admin Port** (管理端口) 单选按钮。
3. 选择其中一个选项，直接在客户机 PC 上连接 **KX II-101-V2**，通过 **Hyperterminal** 等程序访问命令行界面。参看 **命令行界面** (p. 163)。
4. 在 **Serial Settings** (串行设置) 部分配置下列字段：
  - **Speed** (速度)
  - **Stop Bits** (停止位)
  - **Data Bits** (数据位)
  - **Handshake** (握手)
  - **Parity** (奇偶校验)
5. 单击 **OK** (确定) 按钮。

---

## Raritan 电源条控制

### ▶ 配置电源条串行端口：

1. 选择 **Device Settings**(设备设置)> **Serial Port**(串行端口) 打开 **Serial Port Settings** (串行端口设置) 页。
2. 选择 **PowerStrip Control** (电源条控制) 单选按钮。在将 **KX II-101-V2** 连接到 **Raritan** 电源条时，选择此选项。
3. 单击 **OK** (确定) 按钮。

---

## 调制解调器

### ▶ 配置调制解调器串行端口：

1. 选择 **Device Settings**(设备设置)> **Serial Port**(串行端口) 打开 **Serial Port Settings** (串行端口设置) 页。
2. 选择 **Modem**(调制解调器) 单选按钮。在将外置调制解调器连接到 **KX II-101-V2** 提供拨号访问时，选择此选项。
3. 在 **Modem Settings** (调制解调器设置) 部分配置下列字段：
  - **Serial line speed** (串行线路速度)
  - **Modem Init String** (调制解调器初始化字符串) — 必须用此字段显示的默认字符串启用调制解调器访问。

- Modem server IP address (调制解调器服务器 IP 地址) — 在通过调制解调器建立连接之后，用户输入的用于访问 KX II-101-V2 web 界面的地址。
  - Modem client IP address (调制解调器客户机 IP 地址) — 在通过调制解调器建立连接之后，给用户分配的地址。
4. 单击 OK (确定) 按钮。

参看 **调制解调器访问线缆连接** (参看 "**调制解调器访问线缆连接**" p. 110) 详细了解调制解调器访问所用的线缆连接，参看 **认证的调制解调器** (参看 "**认证调制解调器**" p. 178) 详细了解与 KX II-101-V2 一起使用的通过认证的调制解调器。参看 **KVM 和串行访问客户机指南** 中的在 **MPC** 上**创建、修改和删除配置文件**，了解在通过调制解调器连接 KX II-101-V2 时，如何配置使性能最佳的设置。

#### 调制解调器访问线缆连接

用下列线缆连接配置将 KX II-101-V2 连接到调制解调器：

1. 用管理串行电缆连接 KX II-101-V2。
2. 将一个 9 针公母转接器连接到管理串行电缆上。
3. 将一根零调制解调器电缆连接到公母转接器的另一边。
4. 将 9 针公母转接器连接到零调制解调器电缆的另一端。
5. 用 DB9-DB25 公调制解调器电缆连接调制解调器电缆和调制解调器。

---

## 配置日期/时间设置

在 **Date/Time Settings** (日期/时间设置) 页上给 KX II-101-V2 指定日期和时间。有两种 IP 地址配置方法：

- 人工设置日期和时间。
- 使日期和时间与 **Network Time Protocol (NTP)** 服务器同步。

#### ▶ 设置日期和时间：

1. 选择“设备设置>日期/时间”，打开“日期/时间设置”页。
2. 在“时区”下拉列表上选择你所在的时区。
3. 如要调节夏令时，选择“调节夏令时”复选框。
4. 选择日期和时间设置方法：
  - 用户指定时间 — 选择此选项人工输入日期和时间。针对“用户指定时间”选项输入日期和时间。时间使用 **hh:mm** 格式 (使用 **24** 小时制)。

- 与 NTP 服务器同步 — 选择此选项使日期和时间与 Network Time Protocol (NTP) 服务器同步。
5. 对于与 NTP 服务器同步选项：
    - a. 在“主时间服务器”字段里输入主时间服务器的 IP 地址。
    - b. 在“备用时间服务器”字段里输入备用时间服务器的 IP 地址。可选
  6. 单击“确定”按钮。

---

## 事件管理

可以用 KX II-101-V2 事件管理功能允许和禁止把系统事件发送到 SNMP 管理器、系统日志和审计日志。这些事件分成不同的类别，你可以确定要把每个事件发送到一个目的地还是几个目的地。

---

### 配置事件管理 — 设置

在 Event Management - Settings (事件管理 — 设置) 页上配置 SNMP 陷阱和系统日志配置。参看配置 SNMP 陷阱。

在配置 SNMP 陷阱之后，在 Event Management - Settings (事件管理 — 设置) 页上启用这些 SNMP 陷阱。参看配置事件管理 — 目的地。

### 配置 SNMP 陷阱

Simple Network Management Protocol (SNMP) 是用于网络管理和网络设备及其功能监视的协议。通过网络发送 SNMP 陷阱收集信息。陷阱在 Event Management - Settings (事件管理 — 设置) 页上配置。参看 KX II-101-V2 SNMP 陷阱列表了解所有 KX II-101-V2 SNMP 陷阱。

符合 SNMP 规范的设备 (称为代理) 把有关它们的数据存储在管理信息库 (MIB) 里，并对 SNMP 陷阱做出响应。SNMP 代理在 Device Services (设备服务) 页上配置。参看配置 SNMP 代理 (p. 106) 了解如何配置 SNMP 代理，参看查看 KX II-101-V2 MIB (p. 116) 了解如何查看 KX II-101-V2 MIB。

#### ► 配置 SNMP (启用 SNMP 日志)：

1. 选择 Device Settings (设备设置) > Event Management - Settings (事件管理 — 设置)，打开 Event Management - Settings (事件管理 — 设置) 页。
2. 选择 SNMP Logging Enabled (启用 SNMP 日志) 选项启用其余 SNMP 字段。<必需>
3. 选择 SNMP v1/v2c Traps Enabled (启用 SNMP v1/v2c 陷阱) 和/或 SNMP v3 Trap Enabled (启用 SNMP v3 陷阱)。至少要选择一项。在选择选项之后，启用所有相关字段。<必需>

4. 填写下列 SNMP v1/v2c 陷阱字段（必要时）：
  - a. Destination IP/Hostname（目的地 IP/主机名）— SNMP 管理器的 IP 地址或主机名。最多可以创建 5 个 SNMP 管理器

---

*注意：IPv6 地址长度不能超过主机名长度，即 80 个字符。*

---

  - b. Port Number（端口号）— SNMP 管理器使用的端口号
  - c. Community（公用名）— 设备的公用串

---

*注意：SNMP 公用名是设备和运行 SNMP 的工作站所属的设备组，有助于定义要把信息发送到哪里。公用名用于标识此设备组。SNMP 设备或代理可能属于多个 SNMP 公用名。*

---
5. 如果尚未启用字段，选择 SNMP v3 Trap Enabled（启用 SNMP v3 陷阱）复选框启用下列字段。填写下列 SNMP v3 陷阱字段（必要时）：
  - a. Destination IP/Hostname（目的地 IP/主机名）— SNMP 管理器的 IP 地址或主机名。最多可以创建 5 个 SNMP 管理器

---

*注意：IPv6 地址长度不能超过主机名长度，即 80 个字符。*

---

  - b. Port Number（端口号）— SNMP 管理器使用的端口号
  - c. Security Name（安全名称）— 要与 SNMP 代理通信的实体的用户名或服务帐号名（最长 32 个字符）。
  - d. Authentication Protocol（验证协议）— SNMP v3 代理使用的 MD5 或 SHA 验证协议
  - e. Authentication Passphrase（验证密码）— 访问 SNMP v3 代理所需的密码（最长 64 个字符）
  - f. Privacy Protocol（隐私协议）— 必要时用于加密 PDU 和上下文数据的 AES 算法或 DES 算法
  - g. Privacy Passphrase（隐私密码）— 访问隐私协议算法所需的密码（最长 64 个字符）
6. 单击 OK（确定）按钮创建 SNMP 陷阱。



单击 **Event Management - Settings** (事件管理 — 设置) 页上的 **Link to SNMP Agent Configuration** (链接 SNMP 代理配置) 链接迅速打开 **Devices Services** (设备服务) 页。

在配置 SNMP 陷阱之后，在 **Event Management - Destination** (事件管理 — 目标) 页上选择已捕捉的事件。参看配置事件管理 — 目的地。

---

*KX II-101-V2 支持 SNMP v1/v2c 和/或 v3 版本的 SNMP 日志。在启用 SNMP 日志之后，SNMP v1/v2c 定义消息格式和协议操作。SNMP v3 是 SNMP 的安全扩展，提供用户验证、密码管理和加密。*

---

▶ **编辑现有的 SNMP 陷阱：**

1. 选择 **Device Settings** (设备设置) > **Event Management - Settings** (事件管理 — 设置)，打开 **Event Management - Settings** (事件管理 — 设置) 页。
2. 进行必要的更改，然后单击 **OK** (确定) 按钮保存更改。

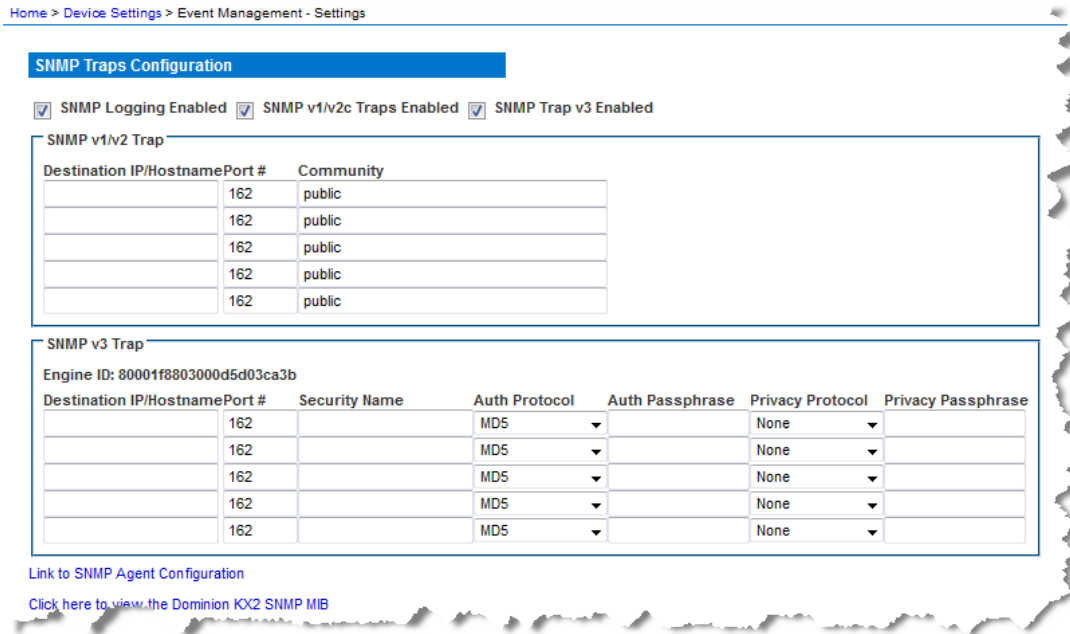
注意：在任何时候禁用 SNMP 设置时，要保存这些 SNMP 信息，在重新启用这些设置时不必再次输入信息。

▶ 删除 SNMP 陷阱：

- 清除所有陷阱字段并保存。

用复位到出厂默认设置功能删除 SNMP 配置，让 KX II-101-V2 恢复到出厂默认设置。

警告：在使用基于 UDP 的 SNMP 陷阱时，在重新启动 KX II-101-V2 之后，KX II-101-V2 和相连的路由器可能会不同步，致使重新启动操作不能完成 SNMP 陷阱记录。



**KX II-101-V2 SNMP 陷阱列表**

在符合一个或多个条件时，SNMP 可以发送陷阱或通知，告知管理员。下表列出 KX II-101-V2 SNMP 陷阱：

陷阱名称	说明
configBackup	设备配置已备份。
configRestore	设备配置已恢复。
deviceUpdateFailed	设备更新失败。
deviceUpgradeCompleted	KX II-101-V2 通过 RFP 文件完成更新。

陷阱名称	说明
deviceUpgradeStarted	KX II-101-V2 已通过 RFP 文件开始更新。
factoryReset	设备已恢复到出厂默认值。
firmwareFileDiscarded	固件文件已被丢弃。
firmwareUpdateFailed	固件更新失败。
firmwareValidationFailed	固件确认失败。
groupAdded	组已被添加到 KX II-101-V2 系统。
groupDeleted	组已从系统中删除。
groupModified	组已修改。
networkFailure	产品的 Ethernet 接口不能再进行网络通信。
networkParameterChanged	更改了网络参数。
networkParameterChangedv2	更改了 KX II-101-V2 网络参数。
passwordSettingsChanged	强密码设置已更改。
portConnect	此前验证的用户已开始 KVM 会话。
portConnectv2	此前验证的 KX II-101-V2 用户已开始 KVM 会话。
portConnectionDenied	到目标端口的连接被拒绝了。
portDisconnect	参与 KVM 会话的用户正确关闭了会话。
portDisconnectv2	参与 KVM 会话的 KX II-101-V2 用户正确关闭了会话。
portStatusChange	端口不再可用。
powerNotification	电源出口状态通知：1=活动、0=非活动。
powerOutletNotification	电源条设备出口状态通知。
rebootCompleted	KX II-101-V2 重新启动完毕。
rebootStarted	KX II-101-V2 已开始采用系统循环加电或操作系统热重新启动方式重新启动。
securityBannerAction	接受/拒绝了安全标志。
securityBannerChanged	更改了安全标志。
securityViolation	安全冲突。
setDateTime	已设置设备日期和时间。
setFIPSMODE	启用了 FIPS 模式。

陷阱名称	说明
startCCManagement	设备已被置于 CommandCenter 管理之下。
stopCCManagement	设备不再受 CommandCenter 管理。
userAdded	用户已被添加到系统中。
userAuthenticationFailure	用户尝试用错误用户名和/或密码登录。
userConnectionLost	有活动会话的用户发生异常会话终止。
userDeleted	用户帐号已被删除。
userForcedLogout	管理员强制用户退出了。
userLogin	用户成功登录 KX II-101-V2 并通过验证。
userLogout	用户成功退出 KX II-101-V2。
userModified	用户帐号已被修改。
userPasswordChanged	如果修改此设备的任何用户的密码，均触发此事件。
userSessionTimeout	有活动会话的用户因超时造成会话终止。
userUploadedCertificate	用户上传了 SSL 证书。
vmlImageConnected	用户尝试用虚拟媒体功能在目标上加载设备或镜像文件。针对对设备/镜像文件映射（加载）进行的每次尝试，都生成此事件。
vmlImageDisconnected	用户尝试用虚拟媒体功能卸载目标上的设备或镜像文件。

#### 查看 *KX II-101-V2 MIB*

##### ▶ 查看 *KX II-101-V2 MIB* :

1. 选择 Device Settings (设备设置) > Event Management - Settings (事件管理 — 设置)，打开 Event Management - Settings (事件管理 — 设置) 页。
2. 单击 [Click here to view the Dominion KX2 SNMP MIB](#) (单击这里查看 Dominion KX2 SNMP MIB) 链接，用浏览器窗口打开 MIB 文件。

---

注意：如果你有 MIB 文件读写权限，用 MIB 编辑器修改文件。

---

```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps

-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateAndTime, setFIPSMODE
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

### 系统日志配置

#### ► 配置系统日志（启用系统日志转发）：

1. 选择 **Enable Syslog Forwarding**（启用系统日志转发），把设备消息记录到远程系统日志服务器上。
2. 在 **IP Address**（IP 地址）字段里输入系统日志服务器的 IP 地址/主机名。
3. 单击 **OK**（确定）按钮。

---

注意：IPv6 地址长度不能超过主机名长度，即 80 个字符。

---

用复位到出厂默认设置功能删除系统日志配置，让 KX II-101-V2 恢复到出厂默认设置。

#### ► 复位到出厂默认设置：

1. 单击 **Reset to Defaults**（复位到默认设置）按钮。

---

### 配置事件管理 — 目的地

如果启用了系统事件，系统事件可以生成 SNMP 通知事件（陷阱），也可以记录到系统日志和审计日志里。在 **Event Management - Destinations**（事件管理 — 目的地）页上选择要跟踪的系统事件，以及要把这些信息发送到哪里。

---

*注意：只有在选择 **SNMP Logging Enabled**（启用 SNMP 日志）选项之后，才会生成 **SNMP** 陷阱。只有在选择 **Enable Syslog Forwarding**（启用系统日志转发）选项之后，才会生成系统日志事件。两个选项都在 **Event Management - Settings**（事件管理 — 设置）页上。参看**配置事件管理 — 设置** (p. 111)。*

---

#### ▶ 选择事件及其目的地：

1. 选择 **Device Settings**（设备设置）> **Event Management - Destinations**（事件管理 — 目的地），打开 **Event Management - Destinations**（事件管理 — 目的地）页。

系统事件按 **Device Operation**（设备操作）、**Device Management**（设备管理）、**Security**（安全）、**User Activity**（用户活动）和 **User Group Administration**（用户组管理）分成不同的类别。

2. 选择你要启用或禁用的事件对应的复选框，以及信息目的地对应的复选框。

---

*提示：分别选择或清除 **Category**（类别）复选框，启用或禁用整个类别。*

---

3. 单击 **OK**（确定）按钮。

#### ▶ 复位到出厂默认设置：

- 单击 **Reset to Defaults**（复位到默认设置）按钮。

**警告：**在使用基于 **UDP** 的 **SNMP** 陷阱时，在重新启动 **KX II-101-V2** 之后，**KX II-101-V2** 和相连的路由器可能会不同步，致使重新启动操作不能完成 **SNMP** 陷阱记录。

## 端口配置

Port Configuration（端口配置）页显示 KX II-101-V2 端口列表。与 KVM 目标服务器或电源条相连的端口用蓝色显示，可以编辑。

### 更改端口配置：

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。

排序

本页最初按端口号顺序显示，但可以单击列标题按任何字段排序。

- **Port Name**（端口名称）— 给端口指定的名称。用黑色显示端口名称，表示不能更改名称，不能编辑端口；用蓝色显示的端口名称可以编辑。

---

*注意：不要在端口名称中使用撇号(')。*

---

- **Port Type**（端口类型）— 与端口相连的目标服务器的类型：

端口类型	说明
电源条	电源条/PDU
KVM	KVM 目标服务器

### 编辑端口名称：

1. 单击要编辑的端口的端口名称。
  - 对于 KVM 端口，打开 Port（端口）页。可以在本页上命名端口，创建电源关联，设置目标服务器设置。
  - 对于电源条，打开电源条 Port（端口）页。可以在本页上命名电源条及其出口。参看 [电源控制](#) (p. 121)。

---

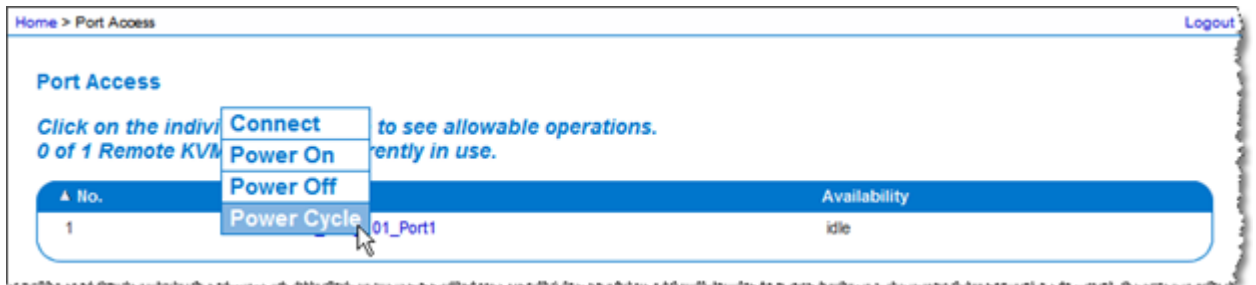
*注意：只有在 Raritan 电源条连接 KX II-101-V2 并正确配置之后，才启用 Power Port 1（电源端口 1）连接，否则，该连接被禁用。*

---

### 管理 KVM 目标服务器（端口页）

在端口配置页上选择与目标服务器相连的端口时，打开本端口页。可以在本页上创建电源关联，将端口名称更改为说明性更强的名称。

一台服务器最多可以有四个电源插头，你可以使它们与电源条关联。可以在本页上定义这些关联，以便在端口访问页上如下所示接通服务器电源、断开服务器电源和给服务器重新通电。



*注意：如要使用此功能，必须给设备连接一个 Raritan Dominion PX 电源条。参看连接电源条。*

#### ▶ 访问端口配置：

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
2. 单击要编辑的端口的端口名称。

*注意：只有在 Raritan 电源条连接 KX II-101-V2 并正确配置之后，才启用 Power Port 1（电源端口 1）连接，否则禁用此连接。*

#### 重新命名端口

#### ▶ 更改端口名称：

1. 输入说明性名称，例如目标服务器的名称。名称最长为 32 个字母数字字符，可以包含特殊字符。

*注意：不要在端口名称中使用撇号(')。*

2. 单击 OK（确定）按钮。

有效特殊字符

字符	说明	字符	说明
!	感叹号	;	分号



字符	说明	字符	说明
"	双引号	=	等号
#	英镑符号	>	大于号
\$	美元符号	?	问号
%	百分号	@	@ 符号
&	& 符号	[	左方括号
(	左圆括号	\	反斜杠
)	右圆括号	]	右方括号
*	星号	^	^ 符号
+	加号	_	下划线
,	逗号	`	重音符号
-	短划线	{	左花括号
.	句号		管道符
/	斜杠	}	右花括号
<	小于号	~	代字号
:	冒号		

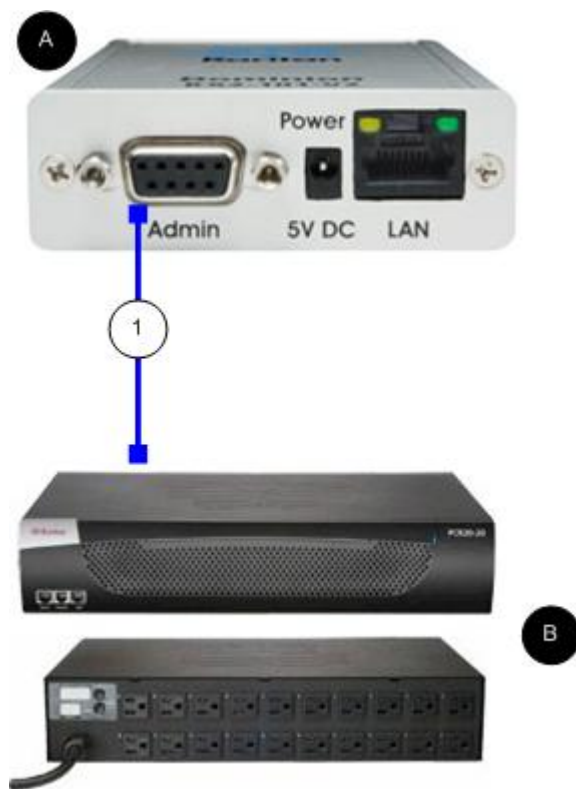
### 电源控制

KX II-101-V2 提供目标服务器远程电源控制。如要利用此功能，必须有一个 Raritan 远程电源条。

#### ▶ 使用 KX II-101-V2 电源控制功能：

- 用 DKX2-101-V2-PDU 连接器（不提供，但可以向当地分销商或 Raritan 购买）把电源条连接到目标服务器。参看连接电源条。
- 命名电源条（不提供，但可以向当地分销商或 Raritan 购买）。参看 [重新命名电源条（电源条端口页）](#) (p. 123)。
- 使电源条出口与目标服务器关联。参看 [管理 KVM 目标服务器（端口页）](#) (p. 120)。
- 在 Power Strip Device（电源条设备）页上开关电源条的出口。参看控制电源条设备。

连接电源条



图示符号	
A	KX II-101-V2
B	Raritan 电源条。
1	连接 KX II-101-V2 和 Raritan 电源条所用的 DKX2-101-V2-PDU (DB9-RJ45 转接头) 连接器 (未画出)。

► 把 KX II-101-V2 连接到 Raritan 电源条：

1. 把 DKX2-101-V2-PDU( DB9-RJ45 转接器)电缆的插入 KX II-101-V2 的 Admin (管理) 端口。
2. 用五类电缆把 DKX2-101-V2-PDU 连接到 Raritan 电源条上的串行端口连接器。
3. 用交流电源线的一端连接目标服务器，另一端连接电源条上的可用电源条出口。

4. 将电源条连接到交流电源。
5. 接通 Raritan 电源条电源。
6. 单击 **Device Settings**(设备设置) > **Serial Port**(串行端口) 打开 **Serial Port** (串行端口) 页。
7. 选择 电源条 **Control** (电源条控制) 单选按钮，然后单击 **OK** (确定) 按钮。在此之后，**Remote Console** 显示 **Power** (电源) 菜单。

#### 重新命名电源条 (电源条端口页)

在 KX II-101-V2 连接 Raritan 远程电源条之后，**Port** (端口) 页显示连接端口，可以在 **Port Configuration** (端口配置) 页上打开此端口。自动填充 **Type** (类型) 字段和 **Name** (名称) 字段。显示电源条上每个电源接口的信息：**Outlet Number** (电源接口号)、**Name** (名称) 和 **Port Association** (端口关联)。

在本页上命名电源条及其电源接口。所有名称最长为 32 个字母数字字符，可以包含特殊字符。

---

*注意：在将电源条关联到目标服务器 (端口) 时，电源接口名称将替换为目标服务器名称 (即使给此电源接口指定了其他名称也是如此)。*

---

#### ► 命名电源条 (和电源接口)：

---

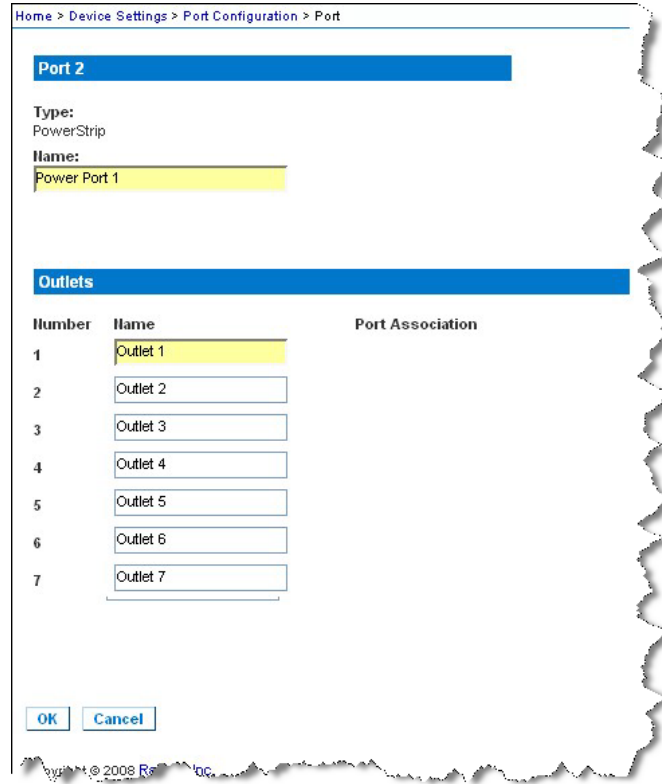
*注意：CommandCenter Service Gateway 无法识别有空格的电源条名称。*

---

1. 将电源条名称更改为便于记忆的名称。
2. 必要时更改电源接口名称。(电源接口名称默认为电源接口号。)
3. 单击 **OK** (确定) 按钮。

▶ 取消而不保存更改：

- 单击 **Cancel**（取消）按钮。



**管理电源关联**

▶ **创建电源关联（使电源条电源接口与 KVM 目标服务器关联）：**

*注意：在使电源条与目标服务器（端口）关联时，用端口名称替换电源接口名称。可以在 **Port 2**（端口 2）页上更改此名称。*

1. 在 **Power Strip Name**（电源条名称）下拉列表上选择电源条。
2. 在 **Outlet Name**（电源接口名称）下拉列表上选择电源接口。
3. 针对每个希望的电源关联，重复第一步和第二步。
4. 单击 **OK**（确定）按钮。显示确认消息。

▶ **删除电源条关联：**

1. 在 **Power Strip Name**（电源条名称）下拉列表上选择相应的电源条。

2. 在 **Outlet Name**（电源接口名称）下拉列表上选择相应的电源条电源接口。
3. 在 **Outlet Name**（电源接口名称）下拉列表上选择 **None**（无）。
4. 单击 **OK**（确定）按钮。电源条/电源接口关联被删除了。显示确认消息。

▶ **显示电源端口配置：**

- 选择 **Home**（主页）> **Device Settings**（设备设置）> **Port Configuration**（端口配置）> [power port name（电源端口名称）]。Outlets（电源接口）下面显示电源条电源接口关联。

▶ **编辑电源端口配置：**

1. 编辑端口 **Name**（名称）字段更改电源端口名称。
2. 编辑关联电源接口 **Name**（名称）字段更改电源接口名称。**Power Strip Device**（电源条设备）页显示电源接口名称。参看控制电源条设备。
3. 单击电源接口名称旁边的 **Port Association**（端口关联）链接并在 **Port 1**（端口 1）页上编辑它，即可更改电源接口关联。

### 控制电源条设备

用电源条设备页控制出口设备。可以在本页上开关电源条上的每个出口。

▶ **控制与 KX II-101-V2 相连的电源条：**

1. 选择 **Home**（主页）> **Powerstrip**（电源条），打开 **电源条 Device**（电源条设备）页。
2. 单击每个出口对应的 **On**（开）或 **Off**（关）按钮开关出口。
3. 在提示你确认选择时，单击 **OK**（确定）。

---

*注意：KX II-101-V2 只能控制一个电源条，不能在电源条（电源条）菜单上选择另一个电源条。*

---

---

## 模拟 KVM 切换器

可以配置 Raritan 模拟 KVM 切换器与 KX II-101-V2 一起工作。

经认证，KX II-101-V2 兼容下列 Raritan KVM 切换器：

- SwitchMan SW2、SW4 和 SW8
- Master Console MX416 和 MXU

可能兼容 Raritan 或其他供应商的类似产品，但不能保证支持这些产品。

---

*注意：为了让 KX II-101-V2 与模拟 KVM 切换器一起工作，必须把切换目标服务器所用的切换热键设置为 Scroll Lock 默认值。*

---

### ► 配置 Raritan 模拟 KVM 切换器：

1. 在 Keyboard/Mouse Setup（键盘/鼠标设置）页上把 Host Interface（主机接口）设置为 PS/2。如果不这样做，在 Analog KVM Switch Configuration（模拟 KVM 切换器配置）页上尝试配置模拟 KVM 切换器时，系统显示错误消息：“必须用 PS/2 访问 KVM 切换器。请先启用 PS/2！”参看 [键盘/鼠标设置](#) (p. 108)。
2. 单击 Device Settings（设备设置）> Analog KVM Switch（模拟 KVM 切换器），打开 Analog KVM Switch Configuration（模拟 KVM 切换器配置）页。
3. 选择 Use Analog KVM Switch（使用模拟 KVM 切换器）复选框激活字段。
4. 在 Switch Type（切换器类型）下拉列表上选择 Raritan 切换器类型。
  - Raritan MCC
  - Raritan MX
  - Raritan MXU
  - Raritan Switchman
5. 根据选择的切换器类型，在 Port Count（端口数）字段里输入可用端口数。必要时更改端口数，或者使用默认端口数。不同切换器的默认端口数如下：
  - Raritan MCC - 8
  - Raritan MX - 16
  - Raritan MXU - 16
  - Raritan Switchman - 2
6. 选择 Security Setting（安全设置）复选框启用安全。
7. 输入访问 KVM 切换器所用的密码。

8. 单击 OK（确定）按钮配置模拟 KVM 切换器。

► **把模拟 KVM 切换器恢复到默认设置：**

- 单击 Reset to Defaults（复位到默认设置）。

## 用复位按钮复位 KX II-101-V2

设备背板上有 **Reset**（复位）按钮。此按钮深陷在背板上，防止意外复位（需要用尖物体按此按钮）。

在按 **Reset**（复位）按钮时执行的操作，要在图形用户界面上定义。参看 [加密和共享](#)。

► **复位设备：**

1. 断开 KX II-101-V2 电源。
2. 使用尖头物按下复位按钮。
3. 继续按住复位按钮，重新接通 KX II-101-V2 设备电源。
4. 按住复位按钮 10 秒钟。
5. 释放 **Reset**（复位）按钮，KX II-101-V2 重新启动。这个过程通常需要三分钟。

---

注意：如果在复位之后设置 KX II-101-V2 恢复到出厂默认设置，相应设置 IP 地址、用户名和其他选项。

---



---

### 更改默认图形用户界面语言设置

KX II-101-V2 图形用户界面支持下列本地化语言：

- Japanese (日文)
- Simplified Chinese (简体中文)
- Traditional Chinese (繁体中文)

► **更改图形用户界面语言：**

1. 选择 **Device Settings**(设备设置)> **Language**(语言) 打开 **Language Settings** (语言设置) 页。
2. 在 **Language** (语言) 下拉列表上选择要应用于图形用户界面的语言。
3. 单击 **Apply** (应用) 按钮。单击 **Reset Defaults** (复位默认设置) 恢复到英文。

---

注意：在应用新语言之后，联机帮助也是本地化语言的，与你选择的语言相同。

---



## 在本章内

概述.....	129
USB 连接设置.....	130
高级 USB 连接设置.....	131

## 概述

为了使 KX II-101-V2 兼容更多不同的 KVM 目标服务器，Raritan 针对众多操作系统级和 BIOS 级服务器实现推出一组自定义的 USB 配置文件供你实时选择。

USB Connection Settings (USB 连接设置) 部分的默认 USB 连接设置可满足部署的绝大多数 KVM 目标服务器配置的要求。还提供其他配置文件满足其他常部署的服务器配置(例如 Linux® 和 Mac OS X)的特定需求。还有许多配置文件(用平台名称和 BIOS 版本号命名)可增强虚拟媒体功能与目标服务器的兼容性，例如在 BIOS 级操作时。

USB 配置文件在 KX II-101-V2 Remote Console 的 Device Settings (设备设置) > Port Configuration (端口配置) > Port (端口) 页上配置。设备管理员可以给端口配置最能满足用户需求和目标服务器配置需求的配置文件。

**警告：**在 Advanced USB Connection Settings (高级 USB 连接设置) 部分进行的选择，可能会使 KX II-101-V2 和目标服务器之间发生配置问题。

因此，Raritan 强烈建议你单击 Port (端口) 页上 Advanced USB Connection Settings (高级 USB 连接设置) 部分的自定义 **KX II-101-V2 USB 配置文件配置表** 超链接阅读最新说明。可以在已知的 USB 配置文件上找到在发布本手册时可用的信息。

连接 KVM 目标服务器的用户可以根据 KVM 目标服务器的工作状态，在这些 USB 连接设置中进行选择。例如假如服务器正在运行，用户想使用 Windows® 操作系统，最好使用默认设置。但如果用户要在 BIOS 菜单上更改设置，或者要用虚拟媒体启动，使用不同的 USB 连接设置可能更合适，视目标服务器型号而定。

如果给定的 KVM 目标服务器不能使用 Raritan 提供的任何一个 USB 连接设置，请联系 Raritan 技术支持部门寻求协助。

## USB 连接设置

### ▶ 给目标服务器定义 USB 连接：

1. 单击 Device Settings (设备设置) > Port Configuration (端口配置)，打开 Port Configuration (端口配置) 页。单击要配置的端口。
2. 单击 USB Connection Settings (USB 连接设置)，展开 USB Connection Settings (USB 连接设置) 部分。
3. 选择要使用的 USB 连接设置：
  - Enable Absolute Mouse (启用绝对鼠标) — 只有在使用 USB 键盘/鼠标接口时才适用
  - Use Full Speed (使用全速) — 可用于那些不能处理高速 USB 设备的 BIOS
  - Absolute mouse scaling for MAC server (Mac 服务器绝对鼠标缩放) — 只有在使用 USB 键盘/鼠标接口时才适用
  - USB Sun Keyboard support (USB Sun 键盘支持) — 只有在使用 USB 键盘/鼠标接口时才适用
4. 单击 OK (确定) 按钮。

### ▼ USB Connection Settings

- Enable Absolute Mouse  
(applies only if USB is active Keyboard/Mouse Interface)
- Use Full Speed - Useful for BIOS  
that cannot handle High Speed USB devices
- Absolute mouse scaling for MAC server  
(applies only if USB is active Keyboard/Mouse Interface)
- USB SUN Keyboard support  
(applies only if USB is active Keyboard/Mouse Interface)

### ▶ Advanced USB Connection Settings

## 高级 USB 连接设置

警告：在 Advanced USB Connection Settings（高级 USB 连接设置）部分进行的选择，可能会使 KX II-101-V2 和目标服务器之间发生配置问题。因此，Raritan 强烈建议你单击 Port（端口）页上 Advanced USB Connection Settings（高级 USB 连接设置）部分的相应链接，参看已知的 USB 配置文件或自定义 KX II-101-V2 USB 配置文件连接配置表。

### ▶ 给目标服务器定义高级 USB 连接：

1. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。单击要配置的端口。
2. 单击 Advanced USB Connection Settings（高级 USB 连接设置）展开此部分。
3. 单击自定义 **KX II-101 USB 配置文件配置表** 链接，访问适用于 Advanced USB Connection Settings（高级 USB 连接设置）部分的建议配置。
4. 按需要配置下列项目：
  - a. Virtual Media Interface #1 Type（虚拟媒体接口 1 类型）
  - b. 选择 Remove Unused VM Interface #1 From Device Configuration（在设备配置上删除不使用的虚拟媒体接口 1）复选框，删除指定的（1 号）虚拟媒体类型接口。
  - c. Virtual Media Interface #2 Type（虚拟媒体接口 2 类型）
  - d. 选择 Remove Unused VM Interface #2 From Device Configuration（在设备配置上删除不使用的虚拟媒体接口 2）复选框，删除指定的（2 号）虚拟媒体类型接口。

5. 单击 OK (确定) 按钮。

▼ Advanced USB Connection Settings

**IMPORTANT: Please follow the reference guide provided at this link.**

User Defined KX II-101 USB Profile Configuration Table

Virtual Media Interface #1 Type

CD-ROM ▼

Remove Unused VM Interface #1 From Device Configuration  
(useful for BIOS that cannot accommodate empty drives)

Virtual Media Interface #2 Type

Removable Disk ▼

Remove Unused VM Interface #2 From Device Configuration  
(useful for BIOS that cannot accommodate empty drives)

## 在本章内

安全设置 .....	133
配置 IP 访问控制 .....	141
SSL 证书 .....	143
安全标志 .....	146

---

**安全设置**

可以在 **Security Settings**（安全设置）页上指定登录限制、用户锁定、密码规则、加密和共享设置。

▶ **配置安全设置：**

1. 选择 **Security**（安全）> **Security Settings**（安全设置），打开 **Security Settings**（安全设置）页。
2. 必要时更新 **登录限制**（p. 133）设置。
3. 适当更新 **强密码**（p. 134）设置。
4. 适当更新 **用户锁定**（p. 136）设置。
5. 适当更新加密和共享设置。
6. 单击 **OK**（确定）按钮。

▶ **复位到出厂默认设置：**

- 单击 **Reset to Defaults**（复位到默认设置）。

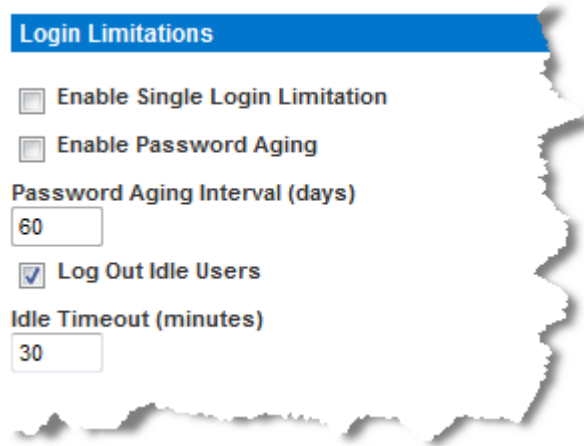
---

**登录限制**

可以用登录限制指定单点登录限制、密码有效期限制和闲置用户退出限制。

限制	说明
Enable single logon limitation（启用单点登录限制）	如果选择此选项，每个用户任何时候都只需登录一次。如果取消此选项，可以同时几个客户机工作stations上输入指定的用户名/密码组合访问设备。
Enable password aging（启用密码有效期）	如果选择此选项，所有用户必须根据在 <b>Password Aging Interval</b> （密码有效天数）字段里指定的天数定期更改密码。  如果选择 <b>Enable Password Aging</b> （启用密码有效

限制	说明
	期)复选框, 启用此字段, 必须填写此字段。输入必须在多少天之后更改密码。默认值是 60 天。
Log off idle users, After (在此之后退出闲置用户, 1-365 分钟)	选择 Log off idle users (退出用户) 复选框, 在经过 After (1-365 minutes) (在此之后[1-365 分钟]) 字段里指定的时间之后, 自动断开用户。如果没有键盘活动或鼠标活动, 注销所有会话和所有资源。但如果正在进行虚拟媒体会话, 此会话不超时。  After (在此之后) 字段用于设置在多久 (分钟) 之后退出闲置用户。如果选择 Log Out Idle Users (退出闲置用户) 选项, 启用此字段。最大可以输入 365 分钟作为字段值。



### 强密码

强密码给系统提供更安全的本地验证。可以利用强密码指定有效 KX II-101-V2 本地密码的格式, 例如最小长度、最大长度、要求的字符和密码历史保留期。

强密码要求用户创建的密码至少有 8 个字符, 其中至少有一个字母字符和一个非字母字符 (标点符号或数字)。此外, 密码前四个字符不能与用户名相同。

如果选择此选项, 强制应用强密码规则。如果用户密码不符合强密码标准的规定, 自动要求用户在下次登录时更改密码。如果取消此选项, 强制执行标准格式验证。如果选择此选项, 启用下列字段, 必须填写这些字段:

字段	说明
Minimum length of strong	密码至少要有 8 个字符。默认值是 8,

字段	说明
password(强密码最小长度)	但管理员可以把最小长度更改为 63 个字符。
Maximum length of strong password(强密码最大长度)	默认最小值是 8，但管理员可以把默认最大值设置为 16 个字符。强密码最大长度为 63 个字符。
Enforce at least one lower case character (强制至少有一个小写字符)	如果选择此复选框，密码至少要有一个小写字符。
Enforce at least one upper case character (强制至少有一个大写字符)	如果选择此复选框，密码至少要有一个大写字符。
Enforce at least one numeric character (强制至少有一个数字字符)	如果选择此复选框，密码至少要有数字字符。
Enforce at least one printable special character (强制至少有一个可打印特殊字符)	如果选择此复选框，密码至少要有可打印特殊字符。
Number of restricted passwords based on history (受限历史密码数)	此字段说明密码历史深度，即可以重复使用的旧密码数。范围是 1-12，默认值是 5。

### Strong Passwords

Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history

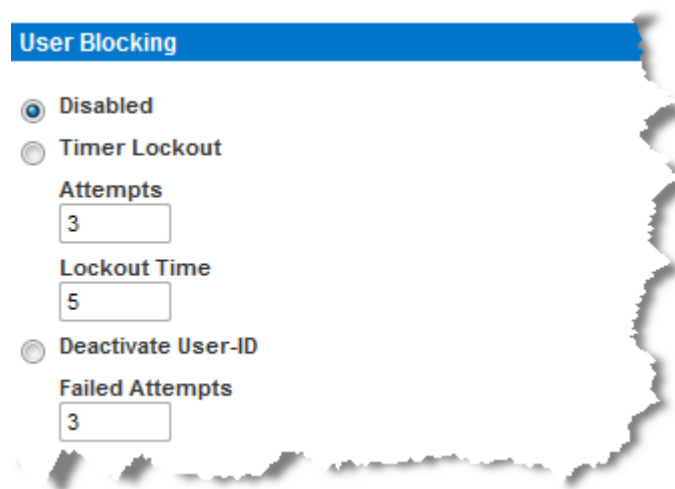
5

### 用户锁定

“用户锁定”选项指定用户锁定标准，在达到指定的登录失败次数之后禁止用户访问系统。

三个选项相互排斥：

选项	说明
禁用	默认选项。无论验证失败多少次，都不锁定用户。
定时器锁定	<p>在登录失败次数超过指定的次数之后，在指定的时间内拒绝用户访问系统。如果选择此选项，启用下列字段：</p> <ul style="list-style-type: none"> <li>尝试次数 — 在锁定用户之前的登录失败次数。有效范围是 1-10 次，默认值是 3 次。</li> <li>锁定时间 — 用户锁定时间。有效范围是 1-1440 分钟，默认值是 5 分钟。</li> </ul> <p><i>注意：管理员用户不受定时器锁定设置的约束。</i></p>
停用用户 ID	<p>如果选择此选项，在达到在“失败次数”字段指定的登录失败次数之后，拒绝用户访问系统。</p> <ul style="list-style-type: none"> <li>失败次数 — 在停用用户的用户 ID 之前的登录失败次数。如果选择“停用用户 ID”选项，启用此字段。有效范围是 1-10 次。</li> </ul> <p>如果在指定的登录失败次数之后停用一个用户 ID，管理员必须在“用户”页上更改密码，并选择“活动”复选框才能激活此用户帐号。</p>





## 加密和共享

可以用 Encryption & Share（加密和共享）设置指定所用的加密类型，PC 和虚拟媒体共享模式，以及在按 KX II-101-V2 Reset（复位）按钮时执行的复位的类型。

警告：如果选择浏览器不支持的加密模式，不能通过浏览器访问 KX II-101-V2。

### ► 配置加密和共享：

1. 在 Encryption Mode（加密模式）下拉列表上选择其中一个选项。

在选择加密模式时显示警告消息，说明如果浏览器不支持选择的模式，不能连接 KX II-101-V2。警告消息：在指定加密模式时，请确保浏览器支持此加密模式，否则不能连接 KX II-101-V2。

加密模式	说明
自动	这是建议的选项。KX II-101-V2 自动协商最高级加密。  <i>必须选择 Auto（自动），设备和客户机才能成功协商使用符合 FIPS 规范的算法。</i>
RC4	加密用户名、密码和 KVM 数据，包括用 RSA RC4 加密方法传输视频。这是 128 位 Secure Sockets Layer (SSL) 协议，在最初验证连接过程中，在 KX II-101-V2 设备和远程 PC 之间提供专用通信通道。  如果后用 FIPS 140-2 模式并选择 RC4，将显示错误消息。在 FIPS 140-2 模式下不能使用 RC4。
AES-128	Advanced Encryption Standard (AES) 是 National Institute of Standards and Technology 制定的电子数据加密规范。128 是密钥长度。如果指定 AES-128，要确保浏览器支持它，否则不能建立连接。参看 <a href="#">检查浏览器的 AES 加密</a> (参看 " <a href="#">检查浏览器是否支持 AES 加密</a> " p. 139)了解详情。
AES-256	Advanced Encryption Standard (AES) 是 National Institute of Standards and Technology 制定的电子数据加密规范。256 是密钥长度。如果指定 AES-256，要确保浏览器支持它，否则不能建立连接。参看 <a href="#">检查浏览器的 AES 加密</a> (参看 " <a href="#">检查浏览器是否支持</a>

加密模式	说明
	<b>AES 加密</b> p. 139)了解详情。

注意：MPC 始终协商最高级加密，在加密模式没有设置为自动的情况下使其匹配。

注意：如果运行 Windows XP® SP2 操作系统，Internet Explorer 7 不能用 AES-128 加密算法远程连接 KX II-101-V2。

2. Apply Encryption Mode to KVM and Virtual Media (将加密模式应用于 KVM 和虚拟媒体)。如果选择此选项，将选择的加密模式应用于 KVM 和虚拟媒体。在验证之后，KVM 数据和虚拟媒体数据也用 128 位加密模式传输。
3. 对于政府机构和其他需要高度安全的环境，选择 Enable FIPS 140-2 (启用 FIPS 140-2) 复选框启用 FIPS 140-2 模式。参看**启用 FIPS 140-2** (p. 139)了解如何启用 FIPS 140-2。
4. PC Share Mode (PC 共享模式) — 决定全局并发远程 KVM 访问，最多允许八个远程用户同时登录 KX II-101-V2，同时通过此设备观看和控制同一台目标服务器。单击下拉列表选择下列其中一个选项：
  - Private (独占) — 无 PC 共享。这是默认模式，每台目标服务器可由一个用户采用独占方式访问。
  - PC-Share (PC 共享) — KVM 目标服务器最多可让八个用户 (管理员和非管理员) 同时访问，但每个远程用户有相同的键盘和鼠标控制权，如果一个用户不停止输入或移动鼠标，他们的控制可能不尽相同。
5. 必要时选择 VM Share Mode (VM 共享模式)。如果启用 PC-Share (PC 共享) 模式，自动启用此选项。如果选择此选项，允许多个用户共享虚拟媒体，即几个用户可以访问同一个虚拟媒体会话。默认值是禁用。
6. 必要时选择 Local Device Reset Mode (本地设备复位模式)。此选项指定在按 (设备背面的) 硬件 Reset (复位) 按钮时，要执行哪些操作。参看**用复位按钮复位 KX II-101-V2** (p. 127) 了解详情。选择下列其中一个选项：

本地设备复位模式	说明
Enable Local Factory Reset (启用本地出厂复位，默认值)	把 KX II-101-V2 设备复位到出厂默认设置。
Enable Local Admin Password Reset (启用本地管理员密码复	只复位本地管理员密码，把密码恢复到 raritan。

本地设备复位模式	说明
位)	
Disable All Local Resets(禁用所有本地复位)	不执行复位操作。

### 检查浏览器是否支持 AES 加密

KX II-101-V2 支持 AES-256。如果不知道浏览器是否使用 AES，可以向浏览器开发商咨询，或者给浏览器设置要检查的加密方法，然后访问 <https://www.fortify.net/sslcheck.html> 网站。此网站检测浏览器使用的加密方法，并显示检测报告。

---

*注意：Internet Explorer® 6 不支持 AES 128 位和 256 位加密。*

---

AES256 的要求和支持的配置

只有下列网络浏览器支持 AES 256 位加密：

- Firefox® 2.0.0.x、3.0.x 和更高版本
- Internet Explorer 7 和 8

除了浏览器支持，AES 256 位加密还要求安装 Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files。

各种 JRE™ 版本的 Jurisdiction files 可以在下列链接的 Other downloads（其他下载）部分找到：

- JRE1.7 - javase/downloads/jce-7-download-432124.html

---

### 启用 FIPS 140-2

对于政府机构和其他需要高度安全的环境，可能要启用 FIPS 140-2 模式。KX II-101-V2 使用 Linux® 平台运行的嵌入式 FIPS 140-2 验证加密模块，按 FIPS 140-2 实现指导原则第 G.5 节指导原则进行加密。在启用此模式之后，必须在内部生成私有密钥才能生成 SSL 证书；私有密钥不能下载或导出。

#### ▶ 启用 FIPS 140-2：

1. 打开 Security Settings（安全设置）页。
2. 在 Security Settings（安全设置）页的 Encryption & Share（加密和共享）部分选择 Enable FIPS 140-2（启用 FIPS 140-2）复选框，启用 FIPS 140-2 模式。将在 FIPS 140-2 模式下把 FIPS 140-2 批准的算法用于外部通信。用 FIPS 加密模块加密 KVM 会话流量，包括视频数据、键盘数据、鼠标数据、虚拟媒体数据和智能卡数据。

### 3. 重新启动 KX II-101-V2。<必需>

在激活 FIPS 模式之后，屏幕左面板的 Device Information(设备信息)部分显示 FIPS Mode: Enabled (FIPS 模式：启用)。

为了增强安全，在激活 FIPS 模式之后还可以创建新证书签名请求。此请求用所需的密钥创建。在签名证书之后上载证书，或者创建一个自签名证书。SSL Certificate (SSL 证书) 状态从 Not FIPS Mode Compliant (不符合 FIPS 模式) 更新为 FIPS Mode Compliant (符合 FIPS 模式)。

在激活 FIPS 模式之后，不能下载或上载密钥文件。最新创建的 CSR 在内部与密钥文件关联。此外，CA 签发的 SSL 证书及其私有密钥并不包括在备份文件的全恢复中。不能导出 KX II-101-V2 上的密钥。

### FIPS 140-2 支持要求

KX II-101-V2 支持使用 FIPS 140-20 批准的加密算法。这样，当客户机配置为仅 FIPS 140-2 模式时，SSL 服务器和客户机可以成功协商加密会话所用的加密算法。

下面是 FIPS 140-2 和 KX II-101-V2 使用建议：

### KX II-101-V2

- 在 Security Settings (安全设置) 页上把 Encryption & Share (加密和共享) 设置为 Auto (自动)。参看加密和共享。

### Microsoft 客户机

- 应该在客户计算机和 Internet Explorer 上禁用 FIPS 140-2。

#### ▶ 在 Windows 客户机上启用 FIPS 140-2：

1. 选择 Control Panel (控制面板) > Administrative Tools (管理工具) > Local Security Policy (本地安全策略)，打开 Local Security Settings (本地安全设置) 对话框。
2. 在导航树上选择 Select Local Policies (选择本地策略) > Security Options (安全选项)。
3. 启用 System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing (系统加密：把符合 FIPS 规范的算法用于加密、散列和签名)。
4. 重新启动客户计算机。

#### ▶ 在 Internet Explorer 上启用 FIPS 140-2：

1. 在 Internet Explorer 上选择 Tools(工具)> Internet Options( Internet 选项)，单击 Advanced (高级) 选项卡。

2. 选择 Use TLS 1.0 (使用 TLS 1.0) 复选框。
3. 重新启动浏览器。

---

## 配置 IP 访问控制

可以用 IP 访问控制来控制对 KX II-101-V2 的访问。可以设置一个全局访问控制表 (ACL)，确保设备不响应来自被禁 IP 地址的数据包。

---

**重要说明** :KX II-101-V2 本地端口使用的 IP 地址是 127.0.0.1。在创建 IP 访问控制表时，如果 127.0.0.1 在被禁 IP 地址范围内，你不能访问 KX II-101-V2 本地端口。

---

### ▶ 使用 IP 访问控制：

1. 选择 Security (安全) > IP Access Control (IP 访问控制)，打开 IP Access Control (IP 访问控制) 页。打开 IP Access Control (IP 访问控制) 页。
2. 选择 Enable IP Access Control (启用 IP 访问控制) 复选框启用 IP 访问控制和本页上的其他字段。
3. 选择 Default Policy (默认策略)。这是针对不在指定范围内的 IP 地址执行的操作。
  - Accept (接受) — 允许 IP 地址访问 KX II-101-V2 设备。
  - Drop (拒绝) — 拒绝 IP 地址访问 KX II-101-V2 设备。

### ▶ 添加 (附加) 规则：

1. 在 IPv4/Mask (IPv4/子网掩码) 字段或 IPv6/Prefix Length (IPv6/前缀长度) 字段里输入 IP 地址和子网掩码。

---

*注意：IP 地址应该采用 CIDR (Classless Inter-Domain Routing) 表示法输入，CIDR 由两部分组成。最重要的部分是网络地址，它指定整个网络或一个子网。最不重要的部分是标识符。在/后面的前缀说明子网掩码长度。*

---

2. 在 Policy (策略) 下拉列表上选择策略。
3. 单击 Append (附加) 按钮把此规则添加到规则列表末尾。

### ▶ 插入规则：

1. 输入规则编号 (#)。在使用 Insert (插入) 命令时，需要规则编号。
2. 在 IPv4/Mask (IPv4/子网掩码) 字段或 IPv6/Prefix Length (IPv6/前缀长度) 字段里输入 IP 地址和子网掩码。
3. 在 Policy (策略) 下拉列表上选择策略。

- 单击 **Insert**（插入）按钮。如果输入的规则编号与现有规则编号相同，将新规则插入现有规则前面，列表上的所有规则向下移一位。

---

*提示：可以利用规则编号更好地控制规则创建顺序。*

---

▶ **替换规则：**

- 指定要替换的规则编号。
- 在 **IPv4/Mask**（IPv4/子网掩码）字段或 **IPv6/Prefix Length**（IPv6/前缀长度）字段里输入 IP 地址和子网掩码。
- 在 **Policy**（策略）下拉列表上选择策略。
- 单击 **Replace**（替换）按钮，新规则取代规则编号相同的旧规则。

▶ **删除规则：**

- 指定要删除的规则编号。
- 单击 **Delete**（删除）按钮。
- 系统提示你确认删除。单击 **OK**（确定）按钮。

[Home](#) > [Security](#) > [IP Access Control](#)

### IP Access Control

**Enable IP Access Control**

**Default Policy**

ACCEPT ▾

Rule #	IPv4/Mask or IPv6/Prefix Length	Policy
--------	---------------------------------	--------

<input type="text"/>	<input type="text"/>	ACCEPT ▾
----------------------	----------------------	----------

**Append**

**Insert**

**Replace**

**Delete**

**OK**

**Reset To Defaults**

**Cancel**

如只允许访问一个 IP 地址并封锁其他所有 IP 地址，将规则的子网掩码更改为 /32。例如如果尝试排除来自 192.168.51 子网的所有访问，但 Default Policy（默认策略）是 Accept（接受），可以添加一个规则将 IP/MASK（IP/掩码）设置为 192.168.51.00/24，将策略设置为 DROP（拒绝）。如果尝试排除来自 192.168.51 子网的所有访问，但来自一个特定 IP 地址（192.168.51.105）的访问除外，Default Policy（默认策略）是 Accept（接受），可以：

1. 添加规则 1，将 IP/Mask（IP/掩码）设置为 192.168.51.105/32，将策略设置为 Accept（接受）。
2. 添加规则 2，将 IP/Mask（IP/掩码）设置为 192.168.51.0/24，将策略设置为 Drop（拒绝）。

如果改变规则 1 和规则 2 的顺序，192.168.51.105 也可能无法访问 KX II-101-V2，因为它也可能被遇到的第一个规则拒绝。

---

## SSL 证书

KX II-101-V2 把 Secure Socket Layer (SSL) 协议用于它和相连客户机之间的任何加密网络流量。在建立连接时，KX II-101-V2 利用加密证书向客户机表明自己的身份。

可以创建证书签名请求 (CSR)，把 CA 签名的证书安装在 KX II-101-V2 上。CA 验证 CSR 发出人的身份。CA 然后返回一个证书，包含它给发出人的签名。经知名 CA 签名的证书用于确保证书持有人的身份。

---

**重要说明：确保正确设置 KX II-101-V2 日期/时间。**

在创建自签名证书时，要用 KX II-101-V2 日期和时间计算有效期。如果 KX II-101-V2 日期和时间不准确，证书的有效开始日期和结束日期可能错误，造成证书验证失败。参看 [配置日期/时间设置](#) (p. 110)。

---

*注意：必须在 KX II-101-V2 上创建 CSR。*

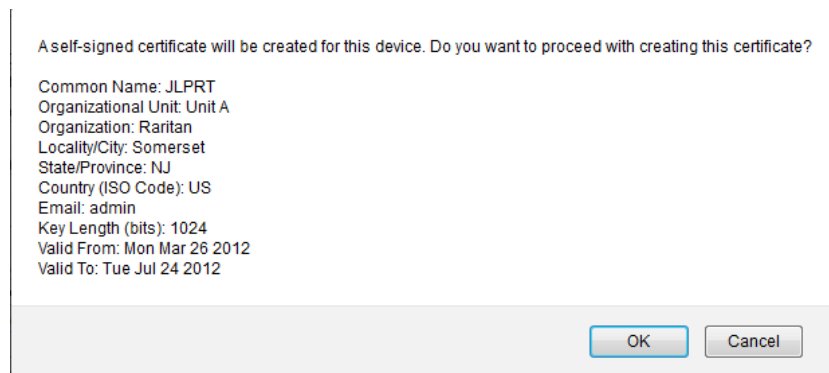
---

*注意：在升级固件时，并不替换活动证书和 CSR。*

### ► 创建和安装 SSL 证书：

1. 选择 Security（安全）> Certificate（证书）。
2. 填写下列字段：
  - a. Common name（公用名）— 在网络上安装 KX II-101-V2 之后使用的网络名称（通常是全限定域名）。公用名与用网络浏览器访问 KX II-101-V2 时使用的名称相同，但没有 http:// 前缀。如果在此指定的名称与实际网络名称不相同，在用 HTTPS 访问 KX II-101-V2 时，浏览器会显示安全警告。

- b. **Organizational unit** (机构单位) — 此字段用于指定 KX II-101-V2 属于一个机构的哪个部门。
  - c. **Organization** (机构) — KX II-101-V2 所属的机构的名称。
  - d. **Locality/City** (地区/城市) — 机构所在的城市。
  - e. **State/Province** (省市) — 机构所在的省市。
  - f. **Country (ISO code)** (国家[ISO 代码]) — 机构所在的国家。这是双字母 ISO 代码，例如 DE 表示德国，US 表示美国。
  - g. **Challenge Password** (挑战密码) — 某些验证中心需要用挑战密码对随后的证书变动进行授权 (例如取消证书)。必要时输入挑战密码。
  - h. **Confirm Challenge Password** (确认挑战密码) — 确认挑战密码。
  - i. **Email** (电子邮件) — 负责 KX II-101-V2 及其安全的联系人的电子邮件地址。
  - j. **Key length** (密钥长度) — 生成的密钥位数。默认值是 1024。
3. 执行下列操作之一：
- a. 如果必须创建自签名证书，选择 **Create a Self-Signed Certificate** (创建自签名证书) 复选框。在选择此选项之后，KX II-101-V2 根据你输入的信息创建证书，并充当证书签名机构。不必导出 CSR 并用它创建签名证书。
  - b. 指定有效天数。确保 KX II-101-V2 日期和时间准确无误，否则会用错误日期创建证书的有效开始日期和结束日期。
  - c. 单击 **Create** (创建) 按钮。
  - d. 显示确认对话框，单击 **OK** (确定) 按钮关闭对话框。
  - e. 重新启动 KX II-101-V2 激活自签名证书。



或者



- f. 指定有效天数。确保 KX II-101-V2 日期和时间准确无误，否则会用错误日期创建证书的有效开始日期和结束日期。
- g. 单击 **Create**（创建）按钮。
- h. 对话框列出你输入的所有信息，以及证书的有效开始日期和结束日期。如果信息正确无误，单击 **OK**（确定）按钮创建 **CSR**。
- i. 重新启动 KX II-101-V2 把保存的 **CSR** 发送到 **CA** 进行 **SSL** 验证。

#### ▶ 下载 CSR 证书：

1. 可以单击 **Download**（下载）按钮下载 **CSR** 和在创建它时所用的私有密钥所在的文件。

---

*注意：CSR 与专用密钥文件相匹配，应作相应的处理。如果签名证书不匹配在生成原始 CSR 时所用的专用密钥，证书没有任何意义。这适用于上载和下载 CSR 和专用密钥文件。*

---

2. 把保存的 **CSR** 发送到 **CA** 进行验证。你将收到来自 **CA** 的新证书。

#### ▶ 上载签名证书：

1. 单击 **Upload**（上载）按钮把证书上载到 KX II-101-V2 上。

---

*注意：CSR 与专用密钥文件相匹配，应作相应的处理。如果签名证书不匹配在生成原始 CSR 时所用的专用密钥，证书没有任何意义。这适用于上载和下载 CSR 和专用密钥文件。*

---

Certificate Signing Request (CSR)	Certificate Upload
<p>The following CSR is pending:</p> <pre>countryName          = US stateOrProvinceName  = DC localityName         = Washington organizationName     = ACME Corp. organizationalUnitName = Marketing Dept. commonName           = John Doe emailAddress          = johndoe@acme.com</pre> <p style="text-align: center;"> <input type="button" value="Download"/> <input type="button" value="Delete"/> </p>	<p>SSL Certificate File</p> <p><input type="text"/> <input type="button" value="Browse..."/></p> <p><input type="button" value="Upload"/></p>

在完成这三个步骤之后，KX II-101-V2 可以用此证书向客户机表明自己的身份。

---

**重要说明：如果销毁了 KX II-101-V2 上的 CSR，没有办法把它找回来！如果误删除了证书，必须重复上述三个步骤。为了避免出现这种情况，可以使用下载功能保留 CSR 及其私有密钥的副本。**

---

---

## 安全标志

KX II-101-V2 使你能给 KX II-101-V2 登录过程增加安全标志。此功能要求用户在访问 KX II-101-V2 之前接受或拒绝安全协议。在用户用自己的登录证书访问 KX II-101-V2 之后，**Restricted Service Agreement**（有限服务协议）对话框显示在安全标志上输入的信息。

安全标志的标题和措词可以定制，也可以使用默认文本。还可以配置安全标志，要求用户在访问 KX II-101-V2 之前接受安全协议，还是只在登录过程中显示安全协议。如果启用接受或拒绝功能，把用户所做的选择记录在审计日志里。

### ► 配置安全标志：

1. 单击 **Security**（安全）> **Banner**（标志）打开 **Banner**（标志）页。
2. 选择 **Display Restricted Service Banner**（显示有限服务标志）启用此功能。
3. 如果要求用户在继续登录过程之前确认标志，选择 **Require Acceptance of Restricted Service Banner**（要求接受有限服务标志）。用户选择一个复选框，即可确认标志。如果不启用此设置，只在用户登录后显示安全标志，不要求用户确认标志。
4. 必要时更改标志的标题。此信息作为标志的一部分给用户显示。最长可以使用 **64** 个字符。
5. 编辑 **Restricted Services Banner Message**（有限服务标志消息）文本框里的信息。最多可以在文本文件里输入或上载 **6000** 个字符。为此，执行下列操作之一：
  - a. 用人工法把文字输入文本框。单击 **OK**（确定）按钮。
6. 选择 **Restricted Services Banner File**（有限服务标志文件）单选按钮，用 **Browse**（浏览）功能找到并上载 **.txt** 文件，即可上载信息。单击 **OK**（确定）按钮。在上载文件之后，**Restricted Services Banner Message**（有限服务标志消息）文本框显示文件里的文字。

## 在本章内

审计日志 .....	147
设备信息 .....	148
备份和恢复 .....	149
升级固件 .....	150
升级历史记录 .....	152
出厂复位 .....	152
重新启动 KX II-101-V2 .....	153
停止 CC-SG 管理 .....	154

---

**审计日志**

给 KX II-101-V2 系统事件创建一个日志。审计日志最多可以存储大约 2K 数据，之后开始覆盖最旧的数据项。为了避免丢失审计日志数据，要把这些数据导出到系统日志服务器或 SNMP 管理器上。在 **Device Settings**(设备设置) > **Event Management** (事件管理) 页上配置系统日志服务器或 SNMP 管理器。

▶ **查看 KX II-101-V2 审计日志：**

1. 选择 **Maintenance** (维护) > **Audit Log** (审计日志)。打开 **Audit Log** (审计日志) 页。

**Audit Log** (审计日志) 页按日期和时间显示事件 (最新的事件列在前面)。审计日志显示下列信息：

- **Date** (日期) — 事件发生日期和时间 (24 小时时钟)。
- **Event** (事件) — **Event Management** (事件管理) 页列出的事件名称。
- **Description** (说明) — 事件详细说明。

▶ **保存审计日志：**

1. 单击 **Save to File** (保存到文件) 按钮。打开 **Save File** (保存文件) 对话框。
2. 选择希望的文件名和保存位置，单击 **Save** (保存) 按钮。采用指定的名称和位置，将审计文件保存在本地客户机上。

▶ **审计日志翻页：**

- 使用 **[Older]** (较旧) 和 **[Newer]** (较新) 链接。

---

## 设备信息

设备信息页显示有关 KX II-101-V2 设备的详细信息。如果必须联系 Raritan 技术支持部门，这些信息很有用。

▶ **查看有关 KX II-101-V2 的信息：**

- 选择 Maintenance (维护) > Device Information (设备信息)，打开 Device Information (设备信息) 页。

显示下列 KX II-101-V2 信息：

- Model (型号)
- Hardware Revision (硬件版本)
- Firmware Version (固件版本)
- Serial Number (序列号)
- MAC Address (MAC 地址)

## 备份和恢复

可以在“备份/恢复”页上备份和恢复 KX II-101-V2 的设置和配置。

除了用备份和恢复功能增强业务连续性，还可以把它用作节省时间的方法。例如备份使用中的 KX II-101-V2 的用户配置设置，把这些配置恢复到新的 KX II-101-V2 上，可以通过另一台 KX II-101-V2 给团队提供访问。还可以设置一台 KX II-101-V2，把它的配置复制到多台 KX II-101-V2 设备。

### ▶ 访问备份/恢复页：

- 选择 Maintenance（维护）> Backup/Restore（备份/恢复），打开 Backup/Restore（备份/恢复）页。

*注意：备份总是以完整的系统备份形式进行，恢复既可以是完整恢复，也可以是部分恢复，视你的选择而定。*

### ▶ 如果使用 Internet Explorer 7 或更高版本备份 KX II-101-V2：

- 单击 Backup（备份），打开 File Download（文件下载）对话框，对话框上有 Open（打开）按钮，不要单击 Open（打开）按钮。

在使用 IE 6 和更高版本时，把 IE 用作打开文件的默认应用程序，所以系统提示你打开文件，而不是保存文件。如要避免出现这种情况，必须把打开文件所用的默认应用程序更改为 Wordpad®。

- 为此修改设置：
  - 保存备份文件。采用指定的名称和位置，把备份文件保存在本地客户机上。

- b. 在保存文件之后找到文件，用右键单击它，单击 **Properties** (属性)。
- c. 单击 **General** (常规) 选项卡上的 **Change** (更改) 按钮，然后选择 **Wordpad**。

► **恢复 KX II-101-V2 :**

警告：在把 KX II-101-V2 恢复到旧版本时务必要谨慎。将恢复在备份文件时使用的用户名和密码。如果忘记旧管理用户名和密码，不能访问 KX II-101-V2。

此外，如果在备份时使用不同的 IP 地址，也恢复此 IP 地址。如果配置使用 DHCP，可能只有在访问本地端口检查更新之后的 IP 地址时，才要执行此操作。

1. 选择要执行的恢复类型：
  - **Full Restore** (全恢复) — 完整恢复整个系统，通常用于传统备份和恢复。
  - **Protected Restore** (保护恢复) — 除了 IP 地址、名称等设备特定的信息，恢复其他所有配置。如果选择此选项，可以设置一台 KX II-101-V2，把配置复制到多台 KX II-101-V2 设备。
  - **Custom Restore** (定制恢复) — 如果选择此选项，可以选择 **User and Group Restore** (用户和用户组恢复) 和/或 **Device Settings Restore** (设备设置恢复)：
    - **User and Group Restore** (用户和用户组恢复) — 选择此选项只包括用户信息和用户组信息。选择此选项不恢复证书文件和专用密钥文件。用此选项迅速恢复不同的 KX II-101-V2。
    - **Device Settings Restore** (设备设置恢复) — 选择此选项只包括设备设置，例如电源关联、USB 配置文件、与刀片服务器机箱有关的配置参数和端口组指定。用此选项迅速复制设备信息。
2. 单击“浏览”按钮，打开“选择文件”对话框。
3. 找到并选择相应的备份文件，单击“打开”按钮，“恢复文件”字段列出选择的文件。
4. 单击“恢复”按钮，根据选择的恢复类型恢复配置。

---

## 升级固件

用固件升级页升级 KX II-101-V2 的固件。

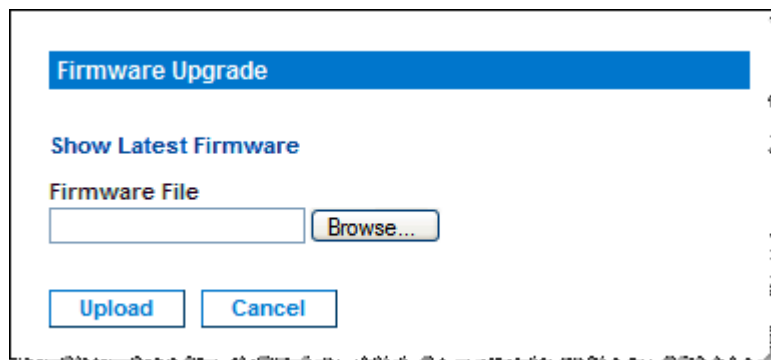
**重要说明：**在升级过程中，不要断开 KX II-101-V2 设备电源，否则很可能

会损坏设备。

---

► 升级 KX II-101-V2 设备：

1. 选择 Maintenance (维护) > Firmware Upgrade (固件升级)，打开 Firmware Upgrade (固件升级) 页。



2. 单击 Firmware Upgrades (固件升级) > KX II-101-V2 页上的 Show Latest Firmware (显示最新固件) 链接，找到相应的 Raritan 固件分发文件 (\*.RFP)，并下载该文件。
3. 解压升级文件，仔细阅读固件 ZIP 文件包含的所有说明，然后升级固件。

---

*注意：先把固件升级文件复制到本地 PC，然后上载这些文件。切勿从网络驱动器加载文件。单击 **Browse** (浏览) 按钮找到升级文件解压目录。*

---

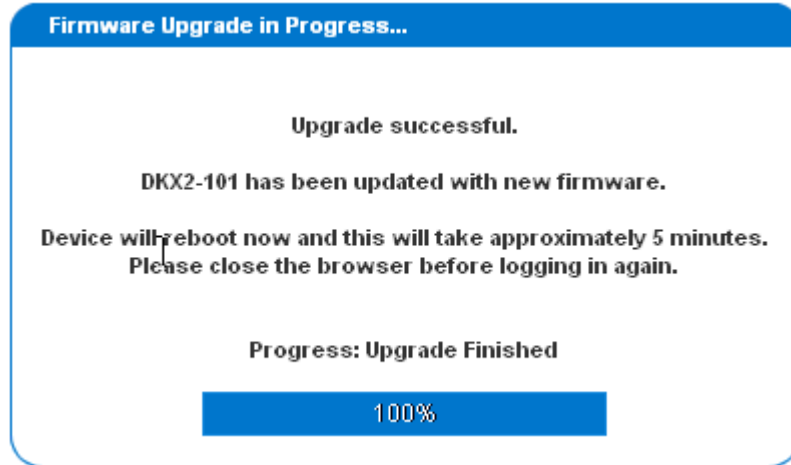
4. 单击 Firmware Upgrade (固件升级) 页上的 Upload (上载) 按钮，显示有关升级和版本号的信息。

---

*注意：此时，已连接的用户都将被注销，新的登录尝试都将被阻止。*

---

- 单击 **Upgrade**（升级）。等待升级完成。在升级过程中显示状态信息和进度条。在完成升级之后，设备重新启动。



- 在系统提示时关闭浏览器，等待大约五分钟即可再次登录 KX II-101-V2。

参看 **KVM 和串行访问客户机用户指南**了解在使用 **Multi-Platform Client** 时如何升级设备固件。

---

## 升级历史记录

KX II-101-V2 提供有关在 KX II-101-V2 上进行的升级的信息。

▶ **查看升级历史记录：**

- 选择 **Maintenance**（维护）> **Upgrade History**（升级历史记录），打开 **Upgrade History**（升级历史记录）页。

---

## 出厂复位

*注意：建议在执行出厂复位之前保存审计日志。在执行出厂复位时删除审计日志，不在审计日志里记录复位事件。如要进一步了解如何保存审计日志，参看**审计日志**。*

▶ **执行出厂复位：**

- 选择“维护>出厂复位”，打开“出厂复位”页。
- 在下列选项中选择合适的复位选项：



- 全出厂复位 — 删除整个配置，把设备彻底复位到出厂前默认值。注意用 **CommandCenter** 定义的任何管理关联被断开。由于这种复位是全复位，系统提示你确认出厂复位。
  - 网络参数复位 — 把设备的网络参数复位到默认值（单击“设备设置>网络设置”访问这些信息）：
3. 单击“复位”按钮继续。由于将永久丢失所有网络设置，系统提示你确认出厂复位。
  4. 单击“确定”按钮继续。在复位结束之后，KX II-101-V2 设备自动重新启动。

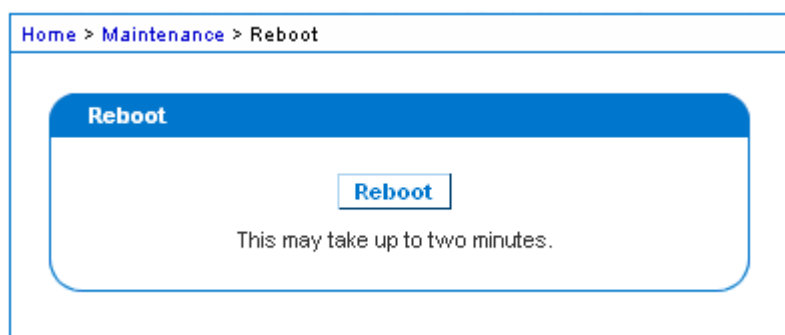
## 重新启动 KX II-101-V2

Reboot（重新启动）页提供一种安全的受控方法，可以在此重新启动 KX II-101-V2。这是建议的重新启动方法。

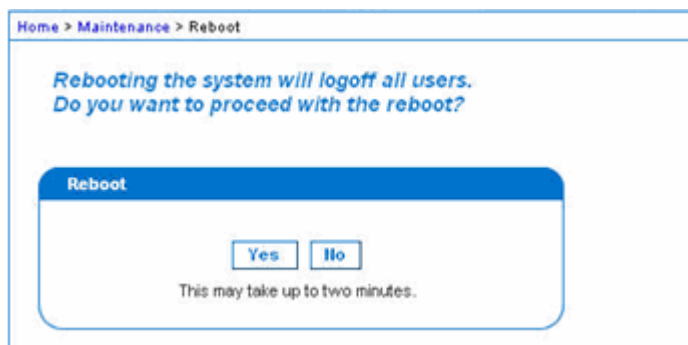
**重要说明：必须关闭所有 KVM 连接和串行连接，必须退出所有用户。**

### ▶ 重新启动 KX II-101-V2：

1. 选择 Maintenance（维护）> Reboot（重新启动），打开 Reboot（重新启动）页。



2. 单击 Reboot（重新启动）按钮。系统提示你确认操作。单击 Yes（是）按钮继续重新启动。



---

## 停止 CC-SG 管理

当 KX II-101-V2 受 CC-SG 管理时，如果尝试直接访问此设备，系统通知你它受 CC-SG 管理。

如果你通过 CC-SG 管理 KX II-101-V2，而且 CC-SG 和 KX II-101-V2 之间的连接在超时间隔时间（通常是 10 分钟）之后断开，可以在 KX II-101-V2 控制台上停止 CC-SG 管理会话。

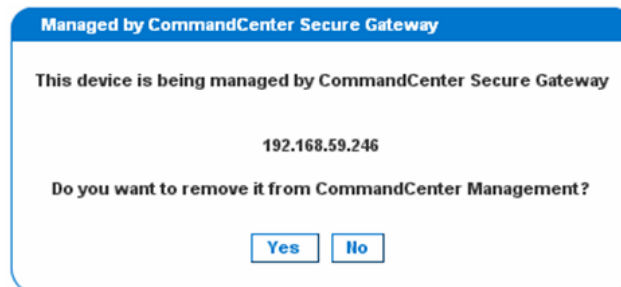
---

*注意：必须具备适当的权限，才能终止 KX II-101-V2 CC-SG 管理。此外，除非当前用 CC-SG 管理 KX II-101-V2，否则不显示 Stop CC-SG Management（停止 CC-SG 管理）选项。*

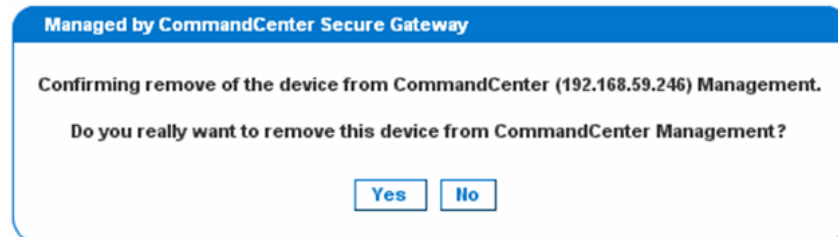
---

### ▶ 停止 KX II-101-V2 CC-SG 管理：

1. 单击 Maintenance（维护）> Stop CC-SG Management（停止 CC-SG 管理）。显示一条消息，说明设备现在受 CC-SG 管理。同时显示一个选项，可以用此选项让设备不再受 CC-SG 管理。



2. 单击 Yes（是）按钮，让设备不再受 CC-SG 管理。显示一条确认消息，请你确认不再让 CC-SG 管理设备。



- 单击 **Yes** (是) 按钮，让设备不再受 **CC-SG** 管理。在停止 **CC-SG** 管理之后，显示一条确认消息。



诊断页用于排除故障，主要供 KX II-101-V2 设备管理员使用。所有 **Diagnostics**（诊断）页（**Device Diagnostics** [设备诊断]除外）均运行标准网络命令，显示的信息就是这些命令的输出。**Diagnostics**（诊断）菜单项有助你调试和配置网络设置。

**Device Diagnostics**（设备诊断）选项应在 Raritan 技术支持部门的指导下使用。

### 在本章内

网络接口页 .....	156
网络统计数据页 .....	156
Ping 主机页 .....	159
跟踪主机路由页 .....	159
设备诊断 .....	161

---

## 网络接口页

KX II-101-V2 显示网络接口状态信息。

### ▶ 查看网络接口信息：

- 选择 **Diagnostics**（诊断）> **Network Interface**（网络接口），打开 **Network Interface**（网络接口）页。

显示下列信息：

- **Ethernet** 接口工作还是停止。
- 是否可以对网关执行 **ping** 命令。
- 当前活动的 **LAN** 端口。

### ▶ 刷新这些信息：

- 单击 **Refresh**（刷新）按钮。

---

## 网络统计数据页

KX II-101-V2 显示网络接口统计数据。

### ▶ 查看网络接口统计数据：

1. 选择 **Diagnostics**（诊断）> **Network Statistics**（网络统计数据），打开 **Network Statistics**（网络统计数据）页。

2. 在 Options (选项) 下拉列表上选择适当的选项：
  - Statistics (统计数据) — 生成类似下面这样的页面。



Home > Diagnostics > Network Statistics

**Network Statistics**

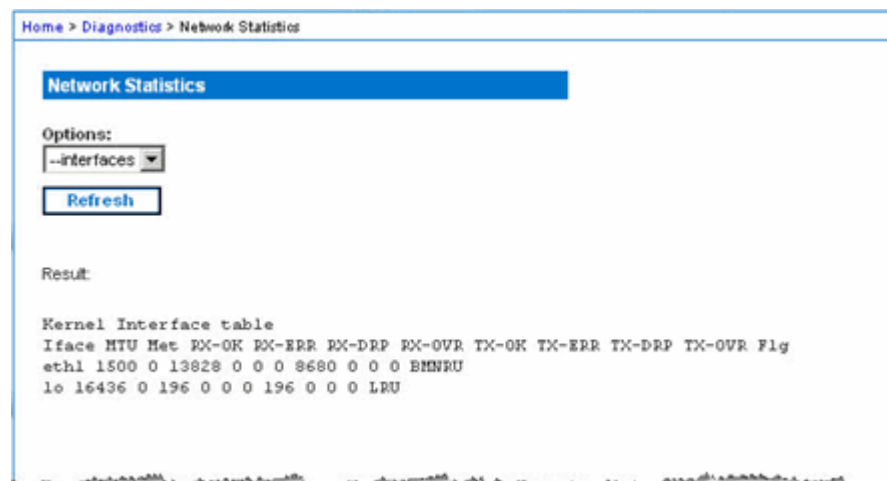
Options:  
 ▼

Result:

```

Ip:
8803 total packets received
0 forwarded
0 incoming packets discarded
8802 incoming packets delivered
8522 requests sent out
Icmp:
0 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
0 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
Tcp:
6 active connections openings
849 passive connection openings
0 failed connection attempts
15 connection resets received
1 connections established
7942 segments received
8304 segments send out
0 segments retransmited
0 bad segments received.
0 resets sent
Udp:
233 packets received
  
```

- Interfaces (接口) — 生成类似下面这样的页面。



Home > Diagnostics > Network Statistics

**Network Statistics**

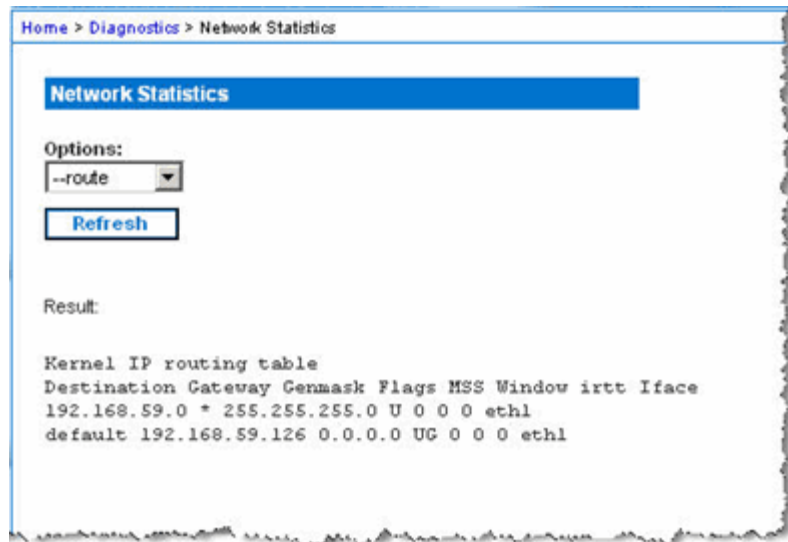
Options:  
 ▼

Result:

```

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（路由）— 生成类似下面这样的页面。



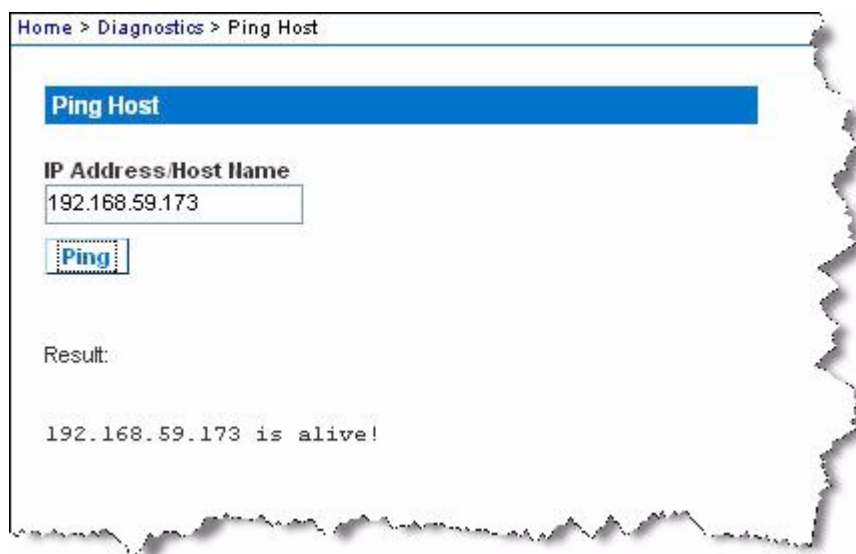
3. 单击 Refresh（刷新）按钮，Result（结果）字段显示相关信息。

## Ping 主机页

Ping 是网络工具，用于测试特定主机或 IP 地址是否可以通过 IP 网络访问。可以在 Ping Host (Ping 主机) 页上确定目标服务器或另一台 KX II-101-V2 是否可访问。

### ► Ping 主机：

1. 选择 Diagnostics (诊断) > Ping Host (Ping 主机)。打开 Ping Host (Ping 主机) 页。



2. 在 IP Address/Host Name (IP 地址/主机名) 字段里输入主机名或 IP 地址。

---

*注意：主机名长度不能超过 232 个字符。*

---

3. 单击 Ping。Result (结果) 字段显示 ping 结果。

## 跟踪主机路由页

跟踪路由是网络工具，用于确定至指定主机名或 IP 地址的路由。

### ► 跟踪主机路由：

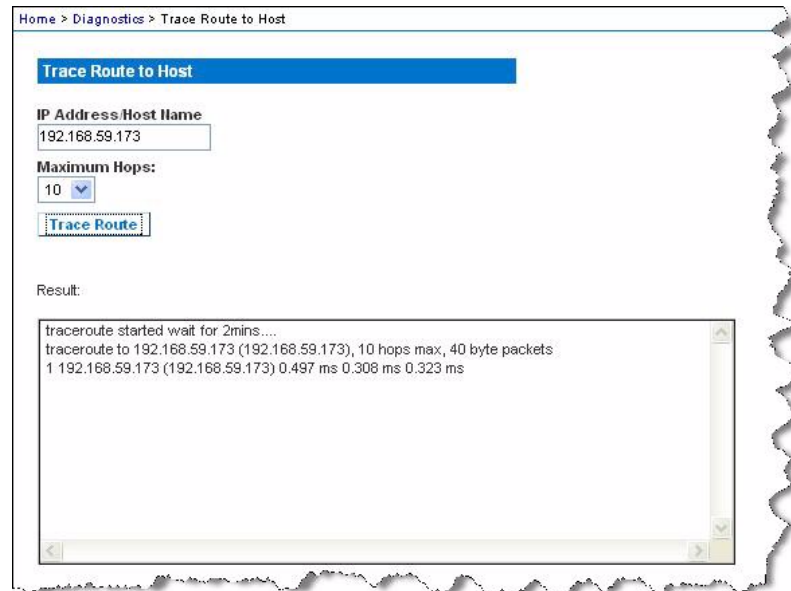
1. 选择 Diagnostics (诊断) > Trace Route to Host (跟踪主机路由)，打开 Trace Route to Host (跟踪主机路由) 页。
2. 在 IP Address/Host Name (IP 地址/主机名) 字段里输入 IP 地址或主机名。

---

注意：主机名长度不能超过 232 个字符。

---

3. 在 **Maximum Hops**（最大跳数）下拉列表上选择最大跳数（5-50，依次递增 5）。
4. 单击 **Trace Route**（跟踪路由）按钮，针对指定的主机名或 IP 地址和最大跳数执行跟踪路由命令。Result（结果）字段显示跟踪路由的输出。





## 设备诊断

*注意：本页供 Raritan 现场工程师使用，或者在 Raritan 技术支持人员的指导下使用。*

设备诊断页将 KX II-101-V2 上的诊断信息下载到客户机上。无论是否运行 Raritan 技术支持部门提供的任选诊断脚本，均生成设备诊断日志。诊断脚本生成更多信息，这些信息可用于诊断问题。

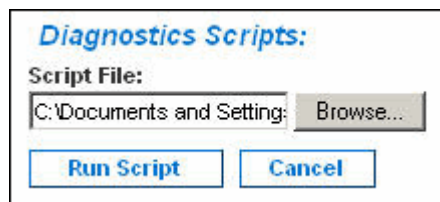
使用下列设置：

- **Diagnostics Scripts** (诊断脚本) — 在严重错误调试会话过程中，加载 Raritan 技术支持部门提供的专用脚本。将此脚本上载到设备上执行。  
**可选**
- **Device Diagnostic Log** (设备诊断日志) — 将 KX II-101-V2 设备上的诊断消息快照下载到客户机上，然后将此加密文件发送给 Raritan 技术支持部门。只有 Raritan 能阅读此文件。

*注意：只有具有管理权限的用户才能访问本页。*

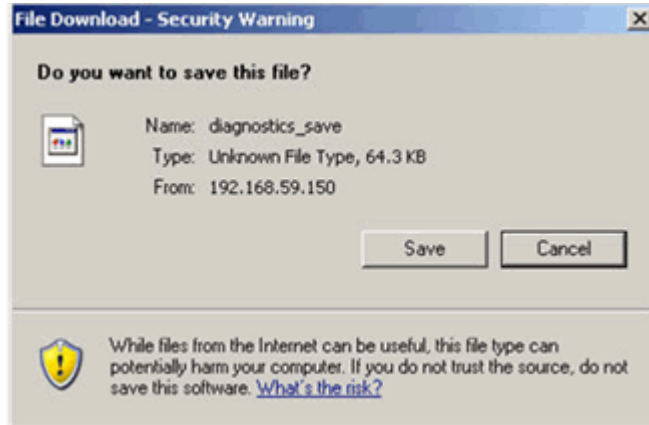
### ▶ 运行 KX II-101-V2 系统诊断：

1. 选择 **Diagnostics** (诊断) > **Device Diagnostics** (设备诊断)，打开 **Device Diagnostics** (设备诊断) 页。
2. (任选) 如果你收到了 Raritan 技术支持部门提供的诊断脚本文件，执行下列步骤，否则跳到第三步。
  - a. 接受并解压 (必要时) Raritan 提供的诊断文件。
  - b. 单击 **Browse** (浏览) 按钮，打开 **Choose File** (选择文件) 对话框。
  - c. 找到并选择此诊断文件。
  - d. 单击 **Open** (打开) 按钮，**Script File** (脚本文件) 字段显示此文件：



- e. 单击 **Run Script** (运行脚本)。
3. 创建诊断文件，把它发送给 Raritan 技术支持部门：

- a. 单击 **Save to File**（保存到文件）按钮，打开 **File Download**（文件下载）对话框。



- b. 单击 **Save**（保存）按钮，打开 **Save As**（另存为）对话框。
  - c. 找到希望的目录，然后单击 **Save**（保存）按钮。
4. 按 Raritan 技术支持部门的指示，通过电子邮件发送此文件。

## 在本章内

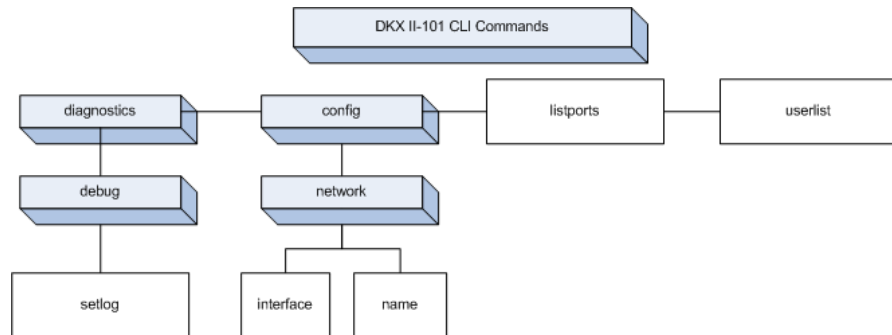
概述.....	163
用命令行界面访问 KX II-101-V2 .....	164
用 SSH 连接访问 KX II-101-V2 .....	164
登录.....	165
命令行界面导航 .....	165
命令行界面命令 .....	167

---

## 概述

本章概述可与 KX II-101-V2 一起使用的命令行界面命令。参看 **命令行界面命令** (p. 167) 了解命令列表和命令定义，以及本章（有命令示例的）各节的链接。

下图概述命令行命令：



---

*注意：可以在各级命令行界面到上图所示的界面上使用下列常用命令：top、history、logout、quit 和 help。*

---

---

## 用命令行界面访问 KX II-101-V2

用下列方法之一访问 KX II-101-V2：

- 基于 IP 连接的 TELNET
- 基于 IP 连接的 SSH (Secure Shell)
- 通过电缆连接的 RS-232 串行接口和 HyperTerminal 等终端仿真程序的多功能管理串行端口

可以使用许多 SSH/TELNET 客户机，这些客户机可以在下列网址下载：

- PuTTY — <http://www.chiark.greenend.org.uk/~sgtatham/putty/>  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- ssh.com 推出的 SSH Client — [www.ssh.com](http://www.ssh.com) <http://www.ssh.com>
- Applet SSH Client — [www.netbeans.org/ssh](http://www.netbeans.org/ssh)  
<http://www.netbeans.org/ssh>
- OpenSSH Client — [www.openssh.org](http://www.openssh.org) <http://www.openssh.org>

---

*注意：在用 SSH 或 TELNET 访问命令行界面时，要求你在 KX II-101-V2 Remote Client 的 Device Services (设备服务) 页上设置访问权。参看设备服务 (p. 104)。*

---

---

## 用 SSH 连接访问 KX II-101-V2

用支持 SSHv2 的任何 SSH 客户机连接设备。必须在 Devices Services (设备服务) 页上启用 SSH 访问。参看设备服务 (p. 104)。

---

*注意：出于安全考虑，KX II-101-V2 不支持 SSH V1 连接。*

---

---

### 在 Windows PC 上进行 SSH 访问

▶ 在 Windows® PC 上启动 SSH 会话：

1. 启动 SSH 客户机软件。
2. 输入 KX II-101-V2 服务器的 IP 地址，例如 192.168.0.192。
3. 选择 SSH，它使用默认配置端口 22。
4. 单击 Open (打开) 按钮。
5. 显示 login as: 提示符。

---

## 在 UNIX/Linux 工作站上进行 SSH 访问

- ▶ 如要在 UNIX®/Linux® 工作站上启动 SSH 会话，用 admin 用户名登录，输入下列命令：

```
ssh -l admin 192.168.30.222
```

显示 Password 提示符。

---

## 登录

- ▶ 登录：

1. Login (登录名)：admin
2. 显示 password (密码) 提示符。输入默认密码：*raritan*。

显示欢迎消息。现在可以作为管理员登录。

在阅读后面的[命令行界面导航](#) (p. 165)一节之后，可以如[用终端仿真程序配置 KX II-101-V2 \(可选\)](#) (p. 30)所述执行初始配置任务。

---

## 命令行界面导航

在使用命令行界面之前，必须了解命令行界面导航和语法。还有一些组合键可以简化命令行界面的使用。

---

### 命令行界面提示符

命令行界面提示符表示当前命令级。提示符的根部分是登录名。对于使用端口仿真应用程序的直接 admin 串行端口连接，Admin Port 是命令的根部分。

```
admin >
```

对于 TELNET/SSH，admin 是命令的根部分：

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

0

---

### 自动完成命令输入

命令行界面支持自动完成部分输入的命令。在输入命令的前面几个字符之后，按 **Tab** 键。如果这些字符形成唯一匹配，命令行界面自动完成命令输入。

- 如果找不到匹配项，命令行界面显示该级对应的有效输入。
- 如果找到多个匹配项，命令行界面显示所有有效输入。

输入其余字符使输入变成唯一的，按 **Tab** 键完成命令输入。

---

### 命令行界面语法 — 提示和快捷键

提示

- 按字母顺序列出命令。
- 命令不区分大小写。
- 参数名称是一个单词，没有下划线。
- 没有自变量的命令默认显示命令的当前设置。
- 在命令后面输入问号 (?)，显示命令帮助。
- 管道符 (|) 表示在一组可选或必要的关键字或自变量中进行选择。

快捷键

- 按 **Up** 箭头键显示最后输入的命令。
- 按 **Backspace** 删除最后输入的字符。
- 按 **Ctrl+C** 终止命令，或者取消参数输入错误的命令。
- 按 **Enter** 执行命令。
- 按 **Tab** 完成命令输入。例如输入 `Admin Port > Conf`，系统显示 `Admin Port > Config >` 提示符。

---

### 在命令行界面上常用的命令

命令行界面命令列出可在所有命令行界面上执行的命令。这些命令还有助于导航命令行界面。

命令	说明
top	返回命令行界面分层结构的最高层，即 <code>username</code> 提示符。
history	显示用户在 <code>KX II-101-V2</code> 命令行界面上输入的最后 200 个命令。
help	显示命令行界面语法概述。

命令	说明
quit	让用户返回第一级。
logout	注销用户会话。

## 命令行界面命令

下表列出并说明所有可用的命令行界面命令。

命令	说明
config	切换到 <b>Configuration</b> （配置）菜单。
diagnostics	切换到 <b>Diagnostics</b> （诊断）菜单。参看 <b>诊断</b> (p. 168)。
debug	切换到 <b>Debug</b> （调式）菜单。参看 <b>调试</b> (p. 168)。
help	显示命令行界面语法概述。
history	显示当前会话的命令行历史记录。
interface	配置 <b>KX II-101-V2</b> 网络接口。
ipv6_interface	设置/获取 <b>IPv6</b> 网络参数。
listports	列出端口、端口名称、端口类型、端口状态和端口可用性。参看 <b>Listports 命令</b> (p. 171)。
logout	退出当前命令行界面会话。
name	设置设备名称。参看 <b>Name 命令</b> (p. 170)。
network	显示网络配置，允许你配置网络设置。参看 <b>网络</b> (p. 169)。
quit	返回上一个命令。
setlog	设置设备日志记录选项。参看 <b>Setlog 命令</b> (p. 168)。
top	返回根菜单。
userlist	列出活动用户数、用户名、端口和状态。参看 <b>Userlist 命令</b> (p. 171)。

## 诊断

Diagnostics (诊断) 菜单允许您给 KX II-101-V2 的不同模块设置日志记录选项。只有在得到 Raritan 技术支持工程师的指示后，才应设置日志记录选项。这些日志记录选项使支持工程师能获得调试和排除故障所需的适当信息。在得到支持工程师的指示时，他/她会告诉您如何设置日志记录选项，如何生成日志文件并把它发送给 Raritan 技术支持部门。

**重要事项：**日志记录选项必须在 Raritan 技术支持工程师的监督下设置。

## 调试

Diagnostics (诊断) > Debug (调试) 菜单允许您选择 **Setlog** 命令，给 KX II-101-V2 设置日志记录选项。

### Setlog 命令

Setlog 命令允许你给 KX II-101-V2 的不同模块设置日志记录级别，查看每个模块的当前日志记录级别。Setlog 命令语法如下：

```
setlog [module <module>] [level <level>] [vflag <vflag>] [verbose <on|off>]
```

```
Set/Get diag log level
```

Setlog 命令选项如下表所述。Raritan 技术支持部门会告诉你如何配置这些设置。

命令选项	说明
module	模块名称。
level	诊断级别： <ul style="list-style-type: none"> <li>▪ err (错误)</li> <li>▪ warn (警告)</li> <li>▪ info (信息)</li> <li>▪ debug (调试)</li> <li>▪ trace (跟踪)</li> </ul>
vflag	verbose 标志类型： <ul style="list-style-type: none"> <li>▪ timestamp (时间戳)</li> <li>▪ module (模块)</li> <li>▪ thread (线程)</li> <li>▪ fileline (文件行)</li> </ul>



命令选项	说明
verbose [on off]	开关 <code>verbose</code> 日志记录。

**Setlog 命令示例**

下列 `Setlog` 命令将 `libpp_serial` 模块的日志记录级别设置为 `debug`，且打开 `verbose` 日志记录。

```
Setlog module libpp_serial level debug verbose on
```

**配置**

**Configuration**（配置）菜单允许您访问在配置网络接口并设置设备名称时所用的网络命令。

**网络**

**Configuration**（配置）> **Network**（网络）命令用于配置 `KX II-101-V2` 网络连接和设备名称。

命令	说明
interface	配置 <code>KX II-101-V2</code> 设备网络接口。
name	设置设备名称。
ipv6_interface	设置/获取 IPv6 网络参数。

**Interface 命令**

**interface** 命令用于配置 `KX II-101-V2` 网络接口。在接受此命令时，设备断开 **HTTP/HTTPS** 连接，并初始化新网络连接。所有 **HTTP/HTTPS** 用户必须用新 **IP** 地址及正确的用户名和密码重新连接设备。参看安装和配置。

**interface** 命令语法如下：

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <auto/10hdx/10fdx/100hdx/100fdx>]
```

**network** 命令选项如下表所述。

命令选项	说明
ipauto	静态或动态 IP 地址
ip ipaddress	给 KX II-101-V2 分配的 IP 地址，以便通过 IP 网络进行访问
mask subnetmask	IP 管理员提供的子网掩码
gw ipaddress	IP 管理员提供的网关 IP 地址
mode <auto   100fdx>	将 Ethernet Mode 设置为自动检测或强制 100Mbps 全双工 (100fdx)

**Interface 命令示例**

下列命令设置 IP 地址、掩码和网关地址，并将模式设置为自动检测。

```
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

**Name 命令**

name 命令用于配置设备名称和主机名。

**语法**

```
name [unitname name] [domain name] [force <true|false>]
```

**name 命令示例**

下列命令设置设备名称：

```
Admin Port > Config > Network > name unitname <unit name>
domain <host name> force trues
```

**IPv6 命令**

用 IPv6 命令设置 IPv6 网络参数，获取现有的 IPv6 参数。

```
Ipv6_interface mode enable ipauto none ip
2001:db8:290c:1291::17 prefixlen 128 gw
2001:db8:290c:1291::1
```

---

**Listports 命令**

Listports 命令列出活动用户数、用户名、端口和状态。

**Listports 命令示例**

```
Admin Port > listports
Port Port                Port Port  Port
No.  Name                    Type Status Availability
1 - Dominion_KXII-101_V2_Port KVM  up      idle
```

---

**Userlist 命令**

Userlist 命令列出端口、端口名称、端口类型、端口状态和端口可用性。

**Userlist 命令示例**

```
Admin Port > Userlist
Active user number: 1
User Name | From          | Status
-----
-
admin     | Admin Port    | active
```

## 在本章内

概述.....	172
使 KX II-101-V2 不受 CC-SG 管理.....	173
在代理模式下使用 CC-SG .....	174

---

## 概述

CC-SG 可以管理 KX II-101-V2。可以利用 iPad® 和 iPhone® 无线访问 CC-SG 管理的 KX II-101-V2。参看 CC-SG 手册了解如何把 KX II-101-V2 添加到 CC-SG 使其受 CC-SG 管理，如何无线访问此设备的设置信息。

当 KX II-101-V2 设备受 CommandCenter Secure Gateway 控制，而你尝试用 KX II-101-V2 Remote Console 直接访问此设备时，在输入有效用户名和密码之后显示下列消息：

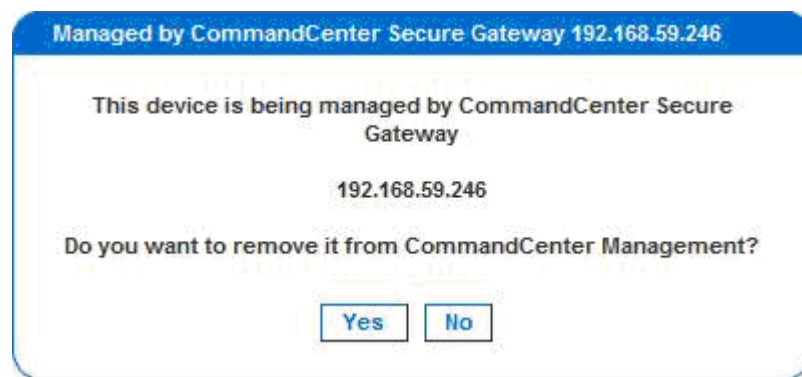


## 使 KX II-101-V2 不受 CC-SG 管理

除非 KX II-101-V2 不受 CC-SG 控制，否则不能直接访问此设备。但如果 KX II-101-V2 接收不到来自 CommandCenter 的心跳信号消息（例如 CommandCenter 不联网），可以解除 CC-SG 对 KX II-101-V2 的控制，以便访问此设备。可以用 CC Unmanage（取消 CC 管理）功能完成此操作。

*注意：使用此功能需要维护权限。*

如果接收不到心跳信号消息，在尝试直接访问设备时，显示下列消息：

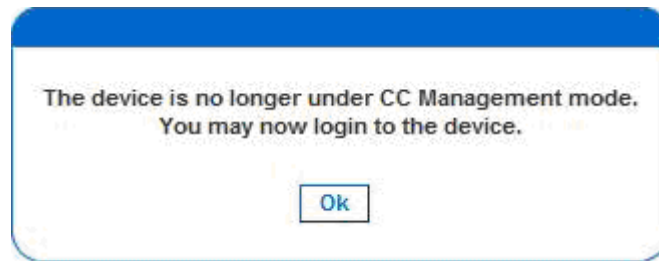


► 使设备不受 CC-SG 管理（使用取消 CC 管理）：

1. 单击 Yes（是）按钮，系统提示你确认操作。



- 单击 **Yes**（是）按钮，显示一条消息确认此设备不再受 CC 管理。



- 单击 **OK**（确定）按钮，打开 KX II-101-V2 登录页。

---

## 在代理模式下使用 **CC-SG**

在 CC-SG 代理模式下不能检测 Virtual KVM Client 版本

在处于代理模式下的 CommandCenter Secure Gateway (CC-SG) 上启动 Virtual KVM Client 时，不知道 Virtual KVM Client 版本。在 About Raritan Virtual KVM Client（关于 Raritan Virtual KVM Client）对话框上，版本显示为 Version Unknown（未知版本）。

代理模式和 MPC

在 CC-SG 配置下使用 KX II-101-V2 时，如果要使用 Multi-Platform Client (MPC)，不要使用 CC-SG 代理模式。

## 在本章内

物理规格 .....	175
支持的操作系统（客户机） .....	176
支持的浏览器 .....	177
连接器 .....	178
认证调制解调器 .....	178
支持的视频分辨率 .....	178
支持的键盘语言 .....	179
使用的 TCP 端口和 UDP 端口 .....	180
Network Speed Settings .....	182
9 针引脚 .....	183

## 物理规格

KX II-101-V2...	说明
体积	0U 形、水平或垂直机架安装（含支架）
尺寸 (DxWxH)	4.055" x 2.913" x 1.063"; 103 x 74 x 27mm
重量	0.6498 磅/0.295 千克
电源	AC/DC (100-240V~/ 6VDC) 电源适配器或 Power over Ethernet (PoE)；符合 IEEE 802.3af Mid-Span Power Insertion Signal-Pair Power Insertion Class 2 PoE 供电设备要求（7 瓦以下）
工作温度	0° - 40°C (32° - 104°F)
湿度	20%-85% 相对湿度
指示灯： 蓝色 RARITAN 背光标志  黄色和绿色 LED	启动和电源指示灯 网络活动和连接速度指示灯
本地连接：	1 个用于把 USB 键盘/鼠标和虚拟媒体连接到目标服务器的 Mini USB 端口  1 个用于建立 RS-232 全功能调制解调器连接和 Dominion PX 连接的 MiniDIN9 多功能串

KX II-101-V2...	说明
	行端口
远程连接： 网络协议	1 个 Ethernet (RJ45) 端口，有活动状态指示灯 TCP/IP、TELNET、SSH、HTTP、HTTPS、安全 LDAP、RADIUS、LDAP、SNMP v2 和 v3、DHCP 和 SNTP、双协议堆：IPv4 和 IPv6
保修	两年加高级更换*

## 支持的操作系统（客户机）

Virtual KVM Client 和 Multi-Platform Client (MPC) 支持下列操作系统：

客户机操作系统	客户机是否支持虚拟媒体 (VM)？
Windows 7™	是
Windows XP®	是
Windows 2008®	是
Windows Vista®	是
Windows 2000® SP4 Server	是
Windows 2003® Server	是
Windows 2008® Server	是
Red Hat® Desktop 5.0	是
Red Hat Desktop 4.0	是
Open SUSE 10, 11	是
Fedora® 13 和 14	是
Mac® OS	是
Solaris™	否
Linux®	是，ISO 镜像文件



JRE™ 插件可用于 Windows® 32 位和 64 位操作系统。只能在 32 位浏览器、64 位 IE7 或 IE8 浏览器上启动 MPC 和 VKC。

下表列出 Java™ 32 位和 64 位 Windows 操作系统的要求。

模式	操作系统	浏览器
Windows x64 32 位模式	Windows XP®	<ul style="list-style-type: none"> <li>Internet Explorer® 6.0 SP1+/7.0/IE 8</li> <li>Firefox® 1.06 - 4 或更高版本</li> </ul>
	Windows Server 2003®	<ul style="list-style-type: none"> <li>Internet Explorer 6.0 SP1++/IE 7/IE 8</li> <li>Firefox 1.06 - 3</li> </ul>
	Windows Vista®	<ul style="list-style-type: none"> <li>Internet Explorer 7.0 或 8.0</li> </ul>
	Windows 7®	<ul style="list-style-type: none"> <li>Internet Explorer 9.0</li> <li>Firefox 1.06 - 4 或更高版本</li> </ul>
Windows x64 64 位模式	Windows XP	64 位操作系统、32 位浏览器：
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	<ul style="list-style-type: none"> <li>Internet Explorer 6.0 SP1+/7.0/8.0</li> <li>Firefox 1.06 - 4 或更高版本</li> </ul>
	Windows Server 2003	64 位模式、64 位浏览器：
	Windows Server 2008	
	Windows 7	

## 支持的浏览器

KX II-101-V2 支持下列浏览器：

- Internet Explorer® 7-9
- Firefox® 4 或更高版本
- Safari® 3 或更高版本

---

## 连接器

接口类型	长度		说明
	英寸	厘米	
配有 PS/2 连接器和 USB 连接器的 KVM 电缆	15"	38 cm	集成电缆
MiniDin9(M) 到 DB9(F)	72"	182 cm	串行电缆
DKX2-101-SPDUC(可选)	70.86"	180 cm	用于连接 Dominion PX 的电缆

---

## 认证调制解调器

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

---

## 支持的视频分辨率

确保 KX II-101-V2 支持每台服务器的视频分辨率和刷新率，而且信号是逐行扫描。

视频分辨率和电缆长度是实现鼠标同步的两个重要因素。

KX II-101-V2 支持下列分辨率：

分辨率	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @75Hz
640x400 @56Hz	1024x768 @90Hz
640x400 @84Hz	1024x768 @100Hz
640x400 @85Hz	1152x864 @60Hz
640x480 @60Hz	1152x864 @70Hz

分辨率	
640x480 @66.6Hz	1152x864 @75Hz
640x480 @72Hz	1152x864 @85Hz
640x480 @75Hz	1152x870 @75.1Hz
640x480 @85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @56Hz	1280x960 @85Hz
800x600 @60Hz	1280x1024 @60Hz
800x600 @70Hz	1280x1024 @75Hz
800x600 @72Hz	1280x1024 @85Hz
800x600 @75Hz	1360x768@60Hz
800x600 @85Hz	1366x768@60Hz
800x600 @90Hz	1368x768@60Hz
800x600 @100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @60Hz	1600x1200 @60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

注意：复合同步视频和绿色同步视频需要额外的适配器。

注意：可能默认不支持某些分辨率。如果看不到分辨率，先插上监视器电源插头，然后拔掉插头，再插上 CIM。

注意：如果不显示 1440x900 和 1680x1050 分辨率，但目标服务器的显卡支持这两种分辨率，可能需要使用 DDC-1440 或 DDC-1680 适配器。

## 支持的键盘语言

KX II-101-V2 支持下表列出的键盘语言。

语言	地区	键盘布局
美国英文	美国和大多数英语国家：例如加拿大、澳大利亚和新西兰。	美国键盘布局

语言	地区	键盘布局
美国国际英文	美国和大多数英语国家 :例如荷兰	美国键盘布局
英国英文	英国	英国键盘布局
繁体中文	香港和台湾	繁体中文
简体中文	中国大陆	简体中文
朝鲜文	韩国	朝鲜文
日文	日本	JIS 键盘
法文	法国	法文 (AZERTY) 键盘布局
德文	德国和奥地利	德文键盘 (QWERTZ) 布局
法文	比利时	比利时
挪威文	挪威	挪威文
丹麦文	丹麦	丹麦文
瑞典文	瑞典	瑞典文
匈牙利文	匈牙利	匈牙利文
斯洛文尼亚文	斯洛文尼亚	斯洛文尼亚文
意大利文	意大利	意大利文
西班牙文	西班牙和大多数西班牙语国家	西班牙文
葡萄牙文	葡萄牙	葡萄牙文

---

使用的 TCP 端口和 UDP 端口


端口	说明
HTTP, 端口 80	可以按需要配置此端口。参看 <b>HTTP 和 HTTPS 端口设置</b> (p. 105)。为安全起见, KX II-101-V2 把通过 HTTP (端口 80) 接收到的所有请求自动转发到 HTTPS。在保证安全的情况下, 为方便用户起见, KX II-101-V2 响应端口 80, 用户不必明确输入 URL 地址即可访问 KX II-101-V2。
HTTPS, 端口 443	可以按需要配置此端口。参看 <b>HTTP 和 HTTPS 端口设置</b> (p. 105)。此端口用于实现多个目的, 包括 HTML 客户机使用的 Web 服务器, 把客户机软件 (MPC/KVC) 下载到客户机的主机上, 把 KVM 数据流和虚拟媒体数据流传输到客户机上。
KX II-101-V2 (Raritan KVM-over-IP) 协议, 可配置端口 5000	此端口用于发现其他 Dominion 设备, 用于在 Raritan 设备和系统 (包括 CC-SG) 之间通信。此端口默认设置为端口 5000, 但可以配置它使用当前空闲的任何 TCP 端口。参看 <b>网络设置</b> (p. 99) 详细了解如何配置此设置。
SNTP(时间服务器), 可配置 UDP 端口 123	KX II-101-V2 有可选功能, 使内部时钟与中央时间服务器同步。此功能要求使用 UDP 端口 123 (SNTP 标准端口), 但也可以配置它使用你指定的任何端口。 <b>可选</b>
LDAP/LDAPS, 可配置端口 389 或 636	如果配置 KX II-101-V2 用 LDAP/LDAPS 协议远程验证用户登录, 将使用端口 389 或 636, 但也可以配置系统使用你指定的任何端口。 <b>可选</b>
RADIUS, 可配置端口 1812	如果配置 KX II-101-V2 用 RADIUS 协议远程验证用户登录, 将使用端口 1812, 但也可以配置系统使用你指定的任何端口。 <b>可选</b>
RADIUS 记帐, 可配置端口 1813	如果配置 KX II-101-V2 用 RADIUS 协议远程验证用户登录, 同时把 RADIUS 记帐用于事件日志记录, 将用端口 1813 或你指定的其他端口传输日志通知。
SYSLOG, 可配置 UDP 端口 514	如果配置 KX II-101-V2 把消息发送到系统日志服务器, 将用指定端口通信, 即 UDP 端口 514。
SNMP 默认 UDP 端口	端口 161 用于入站/出站读写 SNMP 访问, 端口 162 用于 SNMP 陷阱出站流量。 <b>可选</b>
TCP 端口 22	端口 22 用于 KX II-101-V2 命令行界面 (在与 Raritan 技术支持部门一起工作时)。

## Network Speed Settings


### KX II-101-V2 network speed setting

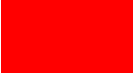
Network switch port setting		Auto	100/Full	100/Half	10/Full	10/Half
Network switch port setting	Auto	Highest Available Speed	KX II-101-V2: 100/Full Switch: 100/Half	100/Half	KX II-101-V2: 10/Full Switch: 10/Half	10/Half
	100/Full	KX II-101-V2: 100/Half Switch: 100/Full	100/Full	KX II-101-V2: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	KX II-101-V2: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	KX II-101-V2: 10/Half Switch: 10/Full	No Communication	No Communication	10/Full	KX II-101-V2: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	KX II-101-V2: 10/Full Switch: 10/Half	10/Half


Legend:

 Does not function as expected

 Supported

 Functions; not recommended

 NOT supported by Ethernet specification; product will communicate, but collisions will occur

 Per Ethernet specification, these should be “no communication,” however, note that the KX II-101-V2 behavior deviates from expected behavior

---

*Note: For reliable network communication, configure the KX II-101-V2 and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the KX II-101-V2 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100MB/s/Full.*

---

## 9 针引脚

引脚编号	
1	DTR (输出)
2	TXD (输出)
3	RXD (输入)
4	DCD/DSR (输入) *
5	GND
6	DTR (输出)
7	CTS (输入)
8	RTS (输出)
9	RI (输入)

---

*注意：本章介绍的步骤仅供有经验的用户尝试使用。*

---

### 在本章内

返回用户组信息 .....	184
设置注册表，允许对模式执行写操作 .....	185
创建新属性 .....	185
给类添加新属性 .....	187
更新模式高速缓存 .....	188
编辑用户成员的 rciusergroup 属性 .....	188

---

## 返回用户组信息

在成功验证之后，用本节中的信息返回用户组信息（有助于授权）。

---

### 自 LDAP

当 LDAP 验证成功时，KX II-101-V2 根据给定用户组的权限确定他/她的权限。远程 RADIUS 服务器可以返回一个如下所述的属性，从而提供这些用户组名称：

rciusergroup                      属性类型：字符串

这可能需要 LDAP/LDAPS 服务器上的模式扩展。请验证服务器管理员后  
用此属性。

---

### 从 Microsoft Active Directory 返回

*注意：仅供有经验的 Active Directory® 管理员尝试。*

---

在 Windows 2000® 操作系统上从 Microsoft® Active Directory 返回用户组信息时，需要更新 LDAP/LDAPS 模式。参看 Microsoft 文档了解详情。

1. 安装 Active Directory 模式插件。参看 Microsoft Active Directory 文档了解说明。
2. 运行 Active Directory Console（Active Directory 控制台），选择 Active Directory Schema（Active Directory 模式）。



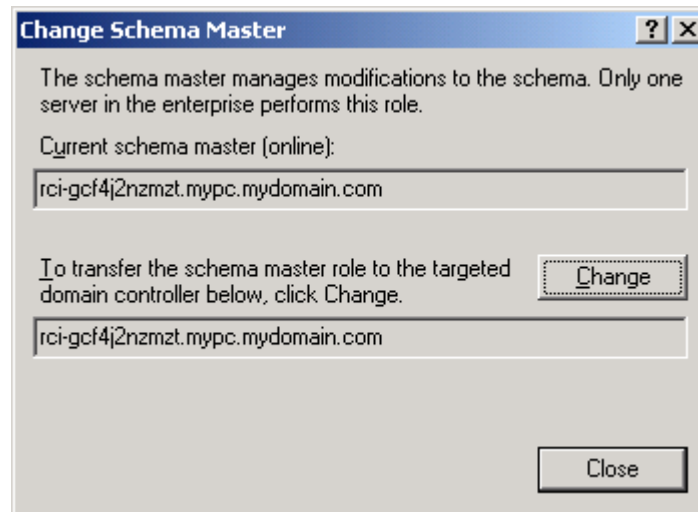
---

## 设置注册表，允许对模式执行写操作

为了让域控制器写入模式，必须设置一个注册表项允许更新模式。

▶ **允许对模式执行写操作：**

1. 用右键单击窗口左面板上的 Active Directory® Schema 根节点，然后单击 Operations Master (主操作) 打开 Change Schema Master (更改主模式) 对话框。



2. 选择 Schema can be modified on this Domain Controller(可以在此域控制器上修改模式) 复选框。可选
3. 单击 OK (确定) 按钮。

---

## 创建新属性

▶ **给 rcigroup 类创建新属性：**

1. 单击窗口左面板上 Active Directory® Schema 前面的 + 号。
2. 用右键单击左面板上的 Attributes (属性)。

- 单击 **New** (新建)，然后选择 **Attribute** (属性)。在显示警告消息时，单击 **Continue** (继续) 按钮，打开 **Create New Attribute** (创建新属性) 对话框。

**Create New Attribute**

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

Multi-Valued

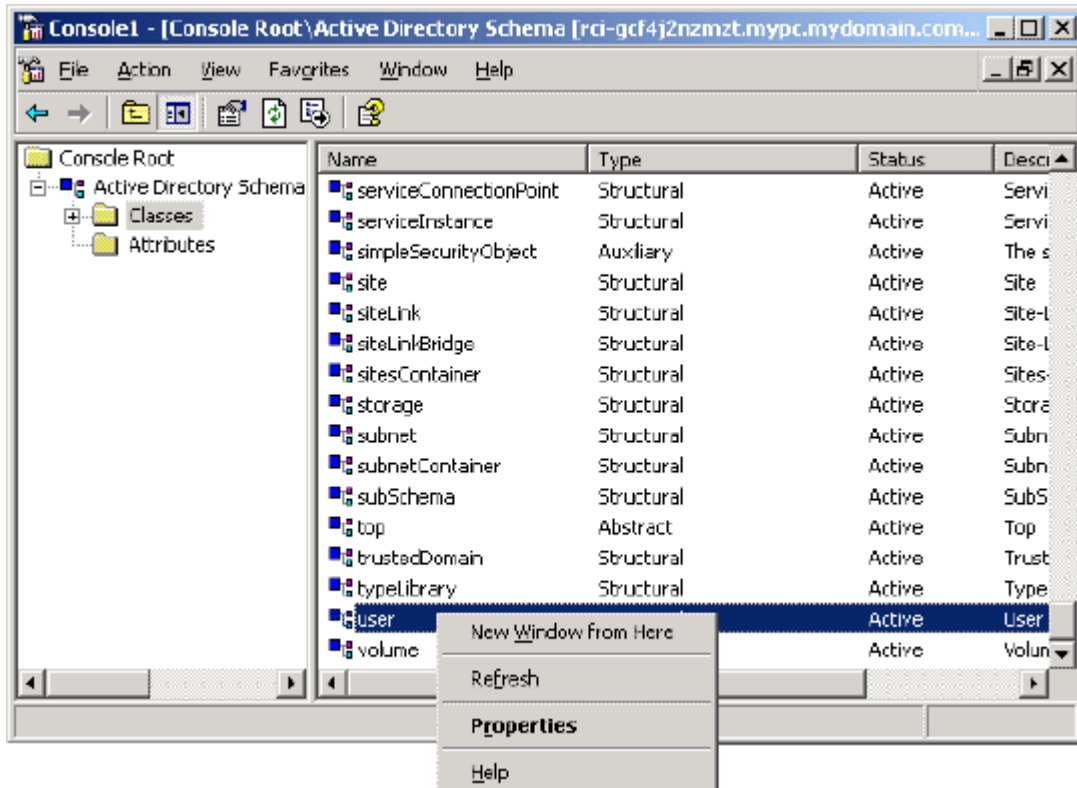
OK Cancel

- 在 **Common Name** (公用名) 字段里输入 *rciusergroup*。
- 在 **LDAP Display Name** (LDAP 显示名称) 字段里输入 *rciusergroup*。
- 在 **Unique x5000 Object ID** (唯一 x5000 对象 ID) 字段里输入 *1.3.6.1.4.1.13742.50*。
- 在 **Description** (说明) 字段里输入有意义的说明。
- 单击 **Syntax** (语法) 下拉箭头，在列表上选择 **Case Insensitive String** (不区分大小写的字符串)。
- 在 **Minimum** (最小值) 字段里输入 *1*。
- 在 **Maximum** (最大值) 字段里输入 *24*。
- 单击 **OK** (确定) 按钮创建新属性。

## 给类添加新属性

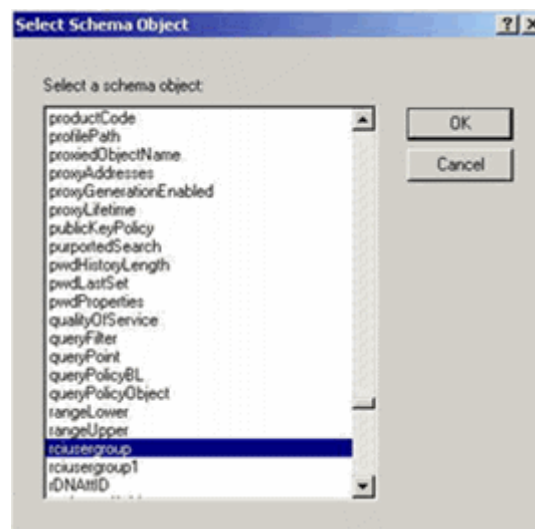
### ▶ 给类添加新属性：

1. 单击窗口左面板上的 **Classes**（类）。
2. 在右面板上找到用户类，用右键单击它。



3. 在菜单上选择 **Properties**（属性）。打开 **User Properties**（用户属性）对话框。
4. 单击 **Attributes**（属性）选项卡打开它。
5. 单击 **Add**（添加）按钮。

- 在 Select Schema Object (选择模式对象) 列表上选择 `rciusergroup`。



- 单击 Select Schema Object (选择模式对象) 对话框上的 OK (确定) 按钮。
- 单击 User Properties (用户属性) 对话框上的 OK (确定) 按钮。

---

## 更新模式高速缓存

► **更新模式高速缓存：**

- 用右键单击窗口左面板上的 Active Directory® Schema，选择 Reload the Schema (重新加载模式)。
- 最小化 Active Directory Schema MMC (Microsoft® Management Console) 控制台。

---

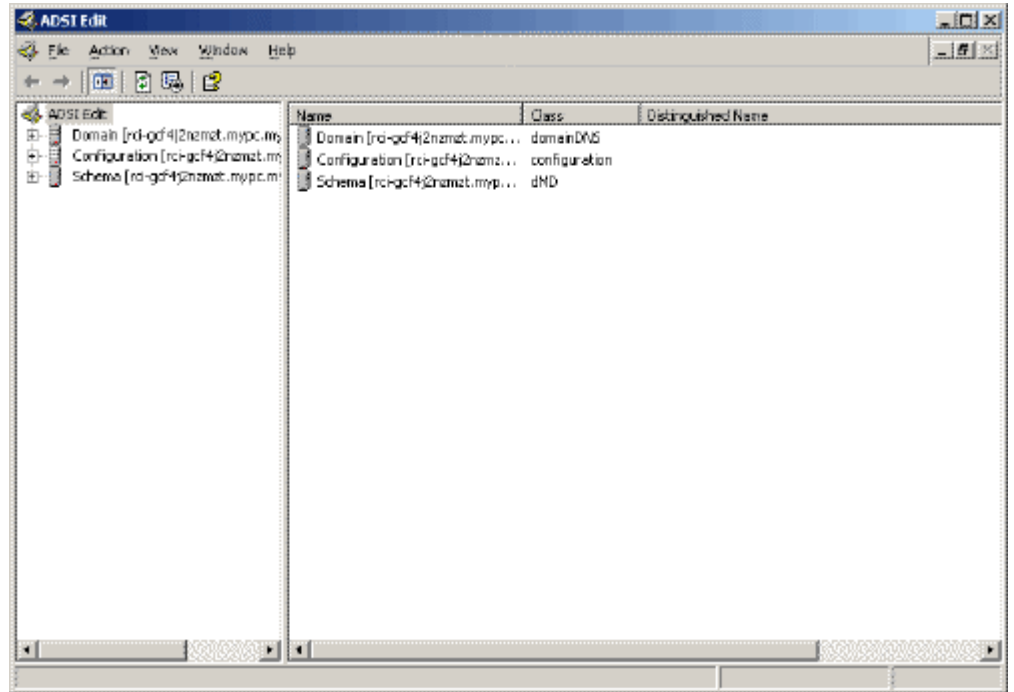
## 编辑用户成员的 `rciusergroup` 属性

如要在 Windows 2003® 上运行 Active Directory® 脚本，要使用 Microsoft® 提供的脚本（在 Windows 2003 Server 安装 CD 上）。在安装 Microsoft® Windows 2003 时，把这些脚本加载到系统上。ADSI (Active Directory Service Interface) 充当低级 Active Directory 编辑器，允许你利用目录服务执行添加对象、删除对象和移动对象等常见管理任务。

► **编辑用户组 `rciusergroup` 的个别用户属性：**

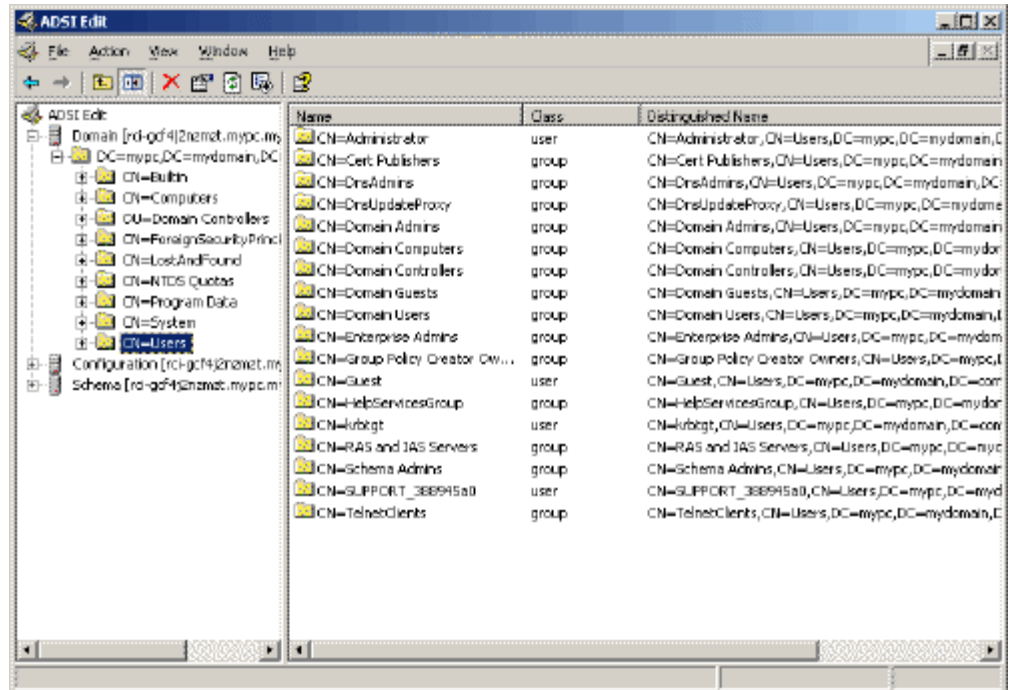
- 在安装 CD 上选择 Support (支持) > Tools (工具)。
- 双击 SUPTOOLS.MSI 安装支持工具。

3. 进入支持工具安装目录，运行 `adsiedit.msc`，打开 ADSI Edit (ADSI 编辑) 对话框。



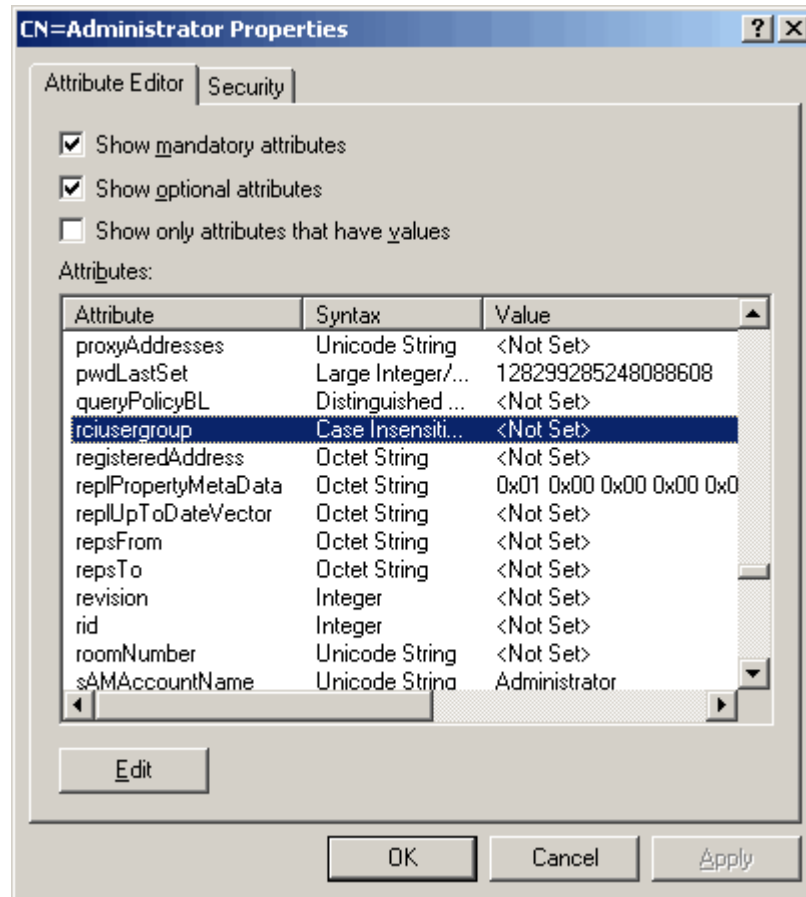
4. 打开 Domain (域)。

5. 在窗口左面板上选择 CN=Users 文件。

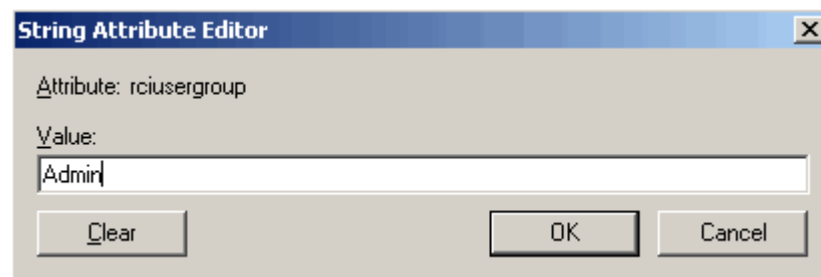


6. 在右面板上找到要调节其属性的用户名。用右键单击用户名，选择 Properties（属性）。

7. 如果尚未打开 Attribute Editor (属性编辑器) 选项卡, 单击它。在 Attributes (属性) 列表上选择 rcusergroup。



8. 单击 Edit (编辑) 按钮, 打开 String Attribute Editor (字符串属性编辑器) 对话框。
9. 在 Edit Attribute (编辑属性) 字段里输入 (在 KX II-101-V2 上创建的) 用户组。单击 OK (确定) 按钮。



KX II-101-V2 设备可以垂直或水平安装在服务器机架的任一边，既可以面对面安装，也可以面向同一个方向安装。用随 KX II-101-V2 一起提供的安装支架和螺丝安装。

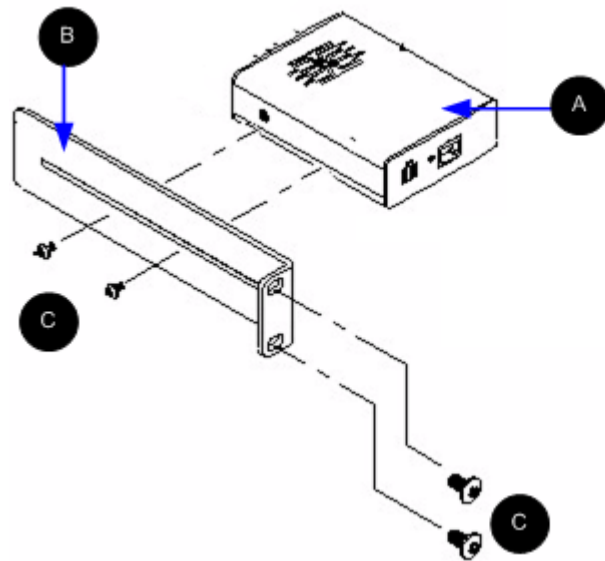
### 在本章内

将 L 型安装支架固定在 KX II-101-V2 上进行水平安装.....192

## 将 L 型安装支架固定在 KX II-101-V2 上进行水平安装

1. 用随附的螺丝将 L 型安装支架固定在 KX II-101-V2 上。调整支架位置，然后拧紧螺丝。
2. 用（机架制造商提供的）机架安装螺丝将 L 型支架总成安装在机架上。


下图说明将 KX II-101-V2 安装在左边。如要将 KX II-101-V2 安装在右边，可遵循上述说明，但将安装支架固定在 KX II-101-V2 右边。



### 图示符号

<b>A</b>	KX II-101-V2
<b>B</b>	L 型支架



图示符号	
	螺丝

## 在本章内

Java Runtime Environment (JRE) .....	194
IPv6 支持注意事项 .....	195
键盘、视频和鼠标说明 .....	195
CC-SG .....	197

---

**Java Runtime Environment (JRE)**


---

**重要说明：**建议你禁用 **Java™** 高速缓存，并清除 **Java** 高速缓存。请阅读 **Java** 文档或 **KVM** 和串行访问客户机指南了解详情。

---

LX、KX II、KX II-101 和 KX II-101-V2 Remote Console 和 MPC 要求安装 Java Runtime Environment™ (JRE™)，因为 Remote Console 要检查 Java 版本。如果版本错误或陈旧，系统会提示你下载兼容版本。

Raritan 建议你用 JRE v1.7 优化性能，但 Remote Console 和 MPC 可以使用 JRE v1.6.x 和更高版本，1.6.2 除外。

---

*注意：*为了在 LX、KX II、KX II-101 和 KX II-101-V2 Remote Console (Virtual KVM Client) 上使用多语言键盘，要安装多语言版本的 JRE。

---

---

## IPv6 支持注意事项

---

### 操作系统 IPv6 支持注意事项

#### Java

对于下列平台，Java™ 1.6 支持 IPv6：

- Solaris™ 10 和更高版本
- Linux® kernel 2.1.2 和更高版本/RedHat 6.1 和更高版本

对于下列平台，Java 不支持 IPv6 配置：

- Microsoft® Windows® 运行的 J2SE 不支持 IPv6。

#### Linux

- 在使用 IPv6 时，建议你使用 Linux kernel 2.4.0 或更高版本。
- 必须安装支持 IPv6 的 kernel，或者必须启用 IPv6 选项重构 kernel。
- 在使用 IPv6 时，还必须安装几个网络工具。访问 <http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html> 了解详情。

#### Windows

- Windows XP 和 Windows 2003 用户必须安装 Microsoft IPv6 服务包才能启用 IPv6。

#### Mac Leopard

- 对于 Mac® Leopard®, KX II v2.0.20 不支持 IPv6。

---

## 键盘、视频和鼠标说明

下列设备有某些键盘限制、视频限制或鼠标限制。必要时采取权宜之计。

---

### Sun 刀片服务器视频、键盘和鼠标支持限制

#### 视频

如果通过 KX II-101-V2 访问 Sun™ Blade 100，在启动 Sun Blade 时，本地端口视频或远程连接视频可能无法正常工作。为了避免这一问题，确保使用 Sun Open Boot Firmware 4.17.1 或更高版本。

#### 键盘和鼠标

由于 Sun Blade 不支持多个键盘，而且不提供本地键盘端口或鼠标端口，不能同时使用 KX II-101-V2 和本地键盘。但是，可以用远程键盘和鼠标控制 Sun Blade。

### 在本地键盘上进行 BIOS 访问的限制

在使用绝对鼠标同步时需要 USB 连接，但本节所述的键盘不支持通过 USB 连接访问本地键盘。如要在 BIOS 或虚拟媒体上通过本地端口访问本地键盘，要遵循下列配置：

键盘	要使用的配置
Dell® OptiPlex™ GX280 - BIOS A03	本地键盘和远程键盘可以利用 Newlink USB 到 PS/2 适配器访问 BIOS 和虚拟媒体。  在 Keyboard/Mouse Setup (键盘/鼠标设置) 页上将 Host Interface (主机接口) 设置为 PS/2。参看 <a href="#">键盘/鼠标设置</a> (p. 108)。
Dell Dimension 2400– BIOS A05	在 Keyboard/Mouse Setup (键盘/鼠标设置) 页上将 Host Interface (主机接口) 设置为 PS/2。参看 <a href="#">键盘/鼠标设置</a> (p. 108)。
Dell Optiplex 170L - BIOS A07	PS/2 和 PS/2 到 USB 适配器。  在 Keyboard/Mouse Setup (键盘/鼠标设置) 页上将 Host Interface (主机接口) 设置为 PS/2。参看 <a href="#">键盘/鼠标设置</a> (p. 108)。
Dell Server 1850	为了使 BIOS A06 能识别虚拟媒体安装的可拆除 USB 闪存，在 Dell 服务器和 KX II-101-V2 之间使用 PS/2 连接和 USB 连接。  在 Keyboard/Mouse Setup (键盘/鼠标设置) 页上将 Host Interface (主机接口) 设置为 PS/2。参看 <a href="#">键盘/鼠标设置</a> (p. 108)。

### HP UX RX 1600 键盘和鼠标配置

如果使用运行 UNIX® 的 HP® UX RX 1600，采取下列措施将设备连接到目标服务器：

- 确认是否使用 KX II-101-V2 固件 2.0.20.5.6964 或更高版本。
- 使用随 KX II-101-V2 一起提供的 USB 电缆。
- 在 Keyboard/Mouse Setup (键盘/鼠标设置) 页上将 Host Interface (主机接口) 设置为 USB。参看 [键盘/鼠标设置](#) (p. 108)。
- 确认没有在 Port (端口) 页上选择 Enable Absolute Mouse (启用绝对鼠标) 复选框和 Use Full Speed (使用全速) 复选框。
- 使用智能鼠标模式或标准鼠标模式。不要使用绝对鼠标模式。

---

### Compaq Alpha 和 IBM P 服务器鼠标模式限制

在通过 KX II-101-V2 连接 Compaq® Alpha 服务器或 IBM® P 服务器时，必须使用单鼠标模式。参看 *使用目标服务器* (p. 33)。

---

### Windows 2000 和 Windows 2003 服务器键盘限制

在使用 Windows 2000® 操作系统和 Windows 2003® 服务器时，由于操作系统限制，美国国际英文键盘布局不能使用下列键盘组合键。

- 右 Alt+D
- 右 Alt+I
- 右 Alt+L

---

*注意：在明确标注美国/国际标记的键盘上，右 Alt 可能标记为 AltGr。*

---

---

## CC-SG

---

### 代理模式和 MPC

如果在 CC-SG 配置下使用 KX II，假如要使用 Multi-Platform Client (MPC)，切勿使用 CC-SG 代理模式。

## 在本章内

常见问题解答 .....	198
IPv6 联网.....	199

## 常见问题解答

问题	解答
Dominion KX II-101-V2 和上一代 Dominion KX II-101 有什么区别??	Dominion KX II-101-V2 是最新一代的经济型。V2 实际上具备上一代 KX II-101 的所有功能，还增加了很多令人激动的新功能。V2 版本不支持 Power-over-Ethernet (PoE) 端口或 PS/2 本地端口。
Dominion KX II-101-V2 是如何工作的?	Dominion KX II-101-V2 连接服务器的键盘端口、视频端口和鼠标端口。它捕捉、数字化并压缩视频信号，然后采用功能很强的 Raritan 帧接收器技术和压缩技术将信号传输到远程客户机 PC。Dominion KX II-101-V2 通过直观用户界面提供丰富的功能。它还可以通过 CommandCenter® Secure Gateway 用其他管理设备进行集中管理。
Dominion KX II-101-V2 可以远程控制哪些类型的计算机?	Dominion KX II-101-V2 独立于目标服务器硬件、操作系统或应用软件工作，访问目标服务器的主要输入/输出设备 — 键盘、视频和鼠标。因此，凡是配备标准 PC 键盘接口和鼠标接口、标准 PC 视频 (VGA) 的任何硬件，均可与 Dominion KX II-101-V2 一起工作。
是否有安全功能防止他人擅自远程连接目标服务器?	有。KX II-101-V2 提供多层安全保护 — 连接验证和远程会话过程中的数据传输安全。用用户名、密码和私有密钥验证用户。Dominion KX II-101-V2 可以利用 Dominion KX II-101-V2 上的本地数据库验证用户，也可以利用外部 AAA 服务器 (LDAP、Active Directory® 或 RADIUS) 验证用户。所有键盘数据、视频数据和鼠标数据可以用 256 位 AES 加密。
Dominion KX II-101-V2 支持哪些类型的虚拟媒体?	KX II-101-V2 支持下列类型的媒体：内置 CD/DVD 驱动器、USB 连接的 CD/DVD 驱动器、USB 大容量存储设备、PC 硬盘驱动器和远程驱动器镜像文件。
虚拟媒体是否安全?	是。虚拟媒体会话用 256 位 AES 加密。
KX2-101-V2 是否有本地端口?	是，有一个 VGA/USB 本地端口，但需要用本地端口电缆连接。为了在本地访问相连的服务器，要把 LCD 监视器接到 KX2-101-V2 的 Local VGA (本地 VGA) 端口。把 USB 键盘和鼠标直接连接到目标服务器。

问题	解答
最新版有哪些新功能？	<p>v3.5（和更高版本）增加了下列功能：</p> <ul style="list-style-type: none"> <li>• 1920x1080 视频分辨率</li> <li>• iPad/iPhone 访问（需要 CC-SG）</li> <li>• 双协议堆 IPv6</li> <li>• FIPS 140-2 加密模块</li> <li>• 退出用户并断开端口</li> <li>• SNMPv3</li> <li>• Linux 和 Mac 客户机增加了虚拟媒体支持</li> <li>• 日文、繁体中文和简体中文用户界面支持</li> <li>• 帮助菜单</li> <li>• 安全标志</li> <li>• 客户 SSL 证书上载</li> <li>• 可配置端口号</li> </ul>

## IPv6 联网

问题	解答
什么是 IPv6？	<p>IPv6 是 Internet Protocol Version 6 的缩写。IPv6 是下一代 IP 协议，将取代目前使用的 IP Version 4 (IPv4) 协议。</p> <p>IPv6 解决了 IPv4 存在的许多问题，例如 IPv4 地址数很有限。它还在路由和网络自动配置等方面较 IPv4 有了重大改进。IPv6 有望逐步取代 IPv4，在未来数年内将出现二者共存局面。</p> <p>从管理员角度看，IPv6 解决了 IP 网络最头痛的一个问题，那就是 IP 网络配置和管理。</p>
为什么 KX II-101-V2 支持 IPv6 联网？	<p>美国政府部门和国防部规定现在必须购买支持 IPv6 的产品。此外，许多企业和国家（例如中国）将在未来几年内过渡到 IPv6。</p>
双协议堆是什么？为什么需要它？	<p>双协议堆就是可同时支持 IPv4 协议和 IPv6 协议。由于要逐步从 IPv4 过渡到 IPv6，所以双协议堆是 IPv6 支持的基本要求。</p>

问题	解答
如何在 KX II-101-V2 上启用 IPv6 ？	在 <b>Network Settings</b> （网络设置）页上选择 <b>Device Settings</b> （设备设置）选项卡启用 IPv6。启用 IPv6 寻址模式，选择人工或自动配置。参看用户指南了解详情。
如果要使用的外部服务器使用 IPv6 地址，使用 KX II-101-V2 时会发生什么情况？	KX II-101-V2 可以通过外部服务器的 IPv6 地址访问这些服务器，例如 SNMP 管理器、系统日志服务器或 LDAP 服务器。  可以利用 KX II-101-V2 的双协议堆体系结构访问这些外部服务器：(1) IPv4 地址、(2) IPv6 地址或 (3) 主机名。所以，KX II-101-V2 支持许多客户的 IPv4/IPv6 混合环境。
如果网络不支持 IPv6，会发生什么情况？	在出厂时，KX II-101-V2 默认联网协议设置为纯 IPv4。如果准备使用 IPv6，要根据上述说明启用 IPv6/IPv4 双协议堆。
可以在哪里进一步了解 IPv6 ？	可以在 <a href="http://www.ipv6.org">www.ipv6.org</a> 上了解 IPv6。KX II-101-V2 用户指南介绍 KX II-101-V2 对 IPv6 的支持。



# 索引

## 9

9 针引脚 - 183

## A

### A

电源 - 22

Active Directory 服务器返回用户组信息 - 92

Apple Macintosh 设置 - 20

## B

### B

目标服务器 - 22

## C

### C

网络 - 25

CC-SG - 197

CC-SG 用户注意事项 - 29

CC-SG 管理 - 172

Compaq Alpha 和 IBM P 服务器鼠标模式限制 - 197

## D

### D

管理端口 - 25

## E

### E

本地用户端口 - 25

## F

FIPS 140-2 支持要求 - 140

## H

HP UX RX 1600 键盘和鼠标配置 - 196

HTTP 和 HTTPS 端口设置 - 105, 181

## I

IBM AIX 设置 - 20

Interface 命令 - 169

IPv6 支持注意事项 - 195

IPv6 命令 - 170

IPv6 联网 - 199

## J

Java Runtime Environment (JRE) - 194

## K

KX II-101-V2 Remote Console 界面 - 33

KX II-101-V2 SNMP 陷阱列表 - 114

KX II-101-V2 帮助 - 3

KX II-101-V2 控制台导航 - 34

KX II-101-V2 概述 - 2

## L

LAN 接口设置 - 28, 99, 102, 103

Linux 设置 (Red Hat 4/5 和 Fedora 14) - 16

Linux 设置 (标准鼠标模式) - 18

Linux 环境下的虚拟媒体 - 72

Listports 命令 - 167, 171

## M

Mac 环境下的虚拟媒体 - 73

Microsoft Active Directory 注意事项 - 29

Multi-Platform Client (MPC) - 41

## N

Name 命令 - 167, 170

Network Speed Settings - 103, 182

## P

Ping 主机页 - 159

PS/2 配置 - 24

## R

RADIUS 通信交换规范 - 95

Raritan 电源条控制 - 109

## S

Setlog 命令 - 167, 168

SSL 证书 - 143

Sun Solaris 设置 - 19

## 索引

Sun 刀片服务器视频、键盘和鼠标支持限制 - 195

Sun 视频分辨率 - 11

## U

USB 连接设置 - 130

USB 配置 - 22

Userlist 命令 - 167, 171

## V

Virtual KVM Client (VKC) - 37, 41

VKC 虚拟媒体 - 60

## W

Windows 2000 设置 - 16

Windows 2000 和 Windows 2003 服务器键盘限制 - 197

Windows 7 和 Windows Vista 设置 - 14

Windows XP 环境下的虚拟媒体 - 71

Windows XP、Windows 2003 和 Windows 2008 设置 - 13

## 三划

工具栏按钮和状态栏图标 - 42

工具选项 - 60, 65

## 四划

支持的协议 - 29

支持的视频分辨率 - 178

支持的浏览器 - 177

支持的键盘语言 - 179

支持的操作系统（客户机） - 176

升级历史记录 - 152

升级固件 - 150

从 Microsoft Active Directory 返回 - 184

分配 IP 地址 - 10, 26

认证调制解调器 - 110, 178

## 五划

本地驱动器 - 75

术语 - 7

左面板 - 34

电源 - 7

电源控制 - 119, 121

代理模式和 MPC - 197

用 Remote Console 配置 KX II-101-V2 - 26

用 SSH 连接访问 KX II-101-V2 - 164

用户 - 84

用户和用户组之间的关系 - 79

用户组 - 78

用户组列表 - 79

用户特点 - 6

用户验证流程 - 96

用户锁定 - 87, 133, 136

用户锁定和解锁 - 87

用户管理 - 30, 78

用命令行界面访问 KX II-101-V2 - 164

用终端仿真程序配置 KX II-101-V2(可选) - 10, 26, 30, 165

用复位按钮复位 KX II-101-V2 - 127, 138

包装内容 - 8

让用户退出 KX II-101-V2（强制退出） - 85, 86

让用户断开端口 - 85, 86

出厂复位 - 152

加密和共享 - 137

发现 KX II-101-V2 子网上的 Raritan 设备 - 40

发现本地子网上的 Raritan 设备 - 39

## 六划

机架安装 - 192

在 UNIX/Linux 工作站上进行 SSH 访问 - 165

在 VKC 和 AKC 上配置扫描设置 - 64

在 Windows PC 上进行 SSH 访问 - 164

在本地键盘上进行 BIOS 访问的限制 - 196

在代理模式下使用 CC-SG - 174

在命令行界面上常用的命令 - 166

网络 - 167, 169

网络设置 - 26, 28, 99, 100, 102, 181

网络统计数据页 - 156

网络配置 - 5

网络接口页 - 156

网络基本设置 - 99, 100

自 LDAP - 184

自动完成命令输入 - 166

自动检测视频设置 - 53

全屏模式 - 65

创建用户组 and 用户 - 30

创建键盘宏 - 50  
 创建新属性 - 185  
 产品图片 - 5  
 产品特点 - 5  
**安全设置** - 86, 133  
 安全标志 - 146  
 安全管理 - 133  
 安装 - 7  
 安装 CD-ROM/DVD-ROM/ISO 镜像文件 - 76  
 安装和配置 - 9  
 设备诊断 - 161  
 设备服务 - 104, 164  
 设备信息 - 148  
 设备管理 - 99  
 设置个人组权限 - 83, 86  
 设置权限 - 80, 82, 83  
 设置服务器视频分辨率 - 10, 11  
 设置注册表, 允许对模式执行写操作 - 185  
 设置新密码 - 26  
 设置端口权限 - 80, 83  
 导入/导出键盘宏 - 48  
 收藏夹列表页 - 39, 40

## 七划

远程验证 - 29  
 运行键盘宏 - 52  
 更改密码 - 98  
 更改最大刷新速率 - 57  
 更改默认图形用户界面语言设置 - 128  
 更新 LDAP 模式 - 184  
 更新模式高速缓存 - 188  
 连接 KVM 目标服务器 - 42  
 连接电源条 - 122  
 连接信息 - 47  
 连接虚拟媒体 - 75  
 连接属性 - 45  
 连接器 - 178  
 串行端口设置 - 108  
 返回用户组信息 - 184  
 系统日志配置 - 117  
 系统管理功能 - 6  
 快速入门 - 10  
 启用 FIPS 140-2 - 138, 139  
 启用 SSH - 104  
 启用 Telnet - 104  
 启用直接端口访问 - 33

启用通过 URL 进行直接端口访问 - 105  
 诊断 - 156, 167, 168

## 八划

规格 - 175  
 事件管理 - 111  
 物理规格 - 175  
 使 KX II-101-V2 不受 CC-SG 管理 - 173  
 使用目标服务器 - 33, 197  
 使用目标服务器截屏 - 56  
 使用的 TCP 端口和 UDP 端口 - 180  
 使用虚拟媒体 - 74  
 使用虚拟媒体的前提 - 70, 74  
 命令行界面 - 109, 163  
**命令行界面导航** - 165  
**命令行界面命令** - 163, 167  
 命令行界面语法 — 提示和快捷键 - 166  
 命令行界面提示符 - 165  
 命名目标服务器 - 28  
 备份和恢复 - 149  
 注销 - 41  
 审计日志 - 147  
 实现 LDAP/LDAPS 远程验证 - 88, 92, 93  
 视图工具栏 - 64  
 视图选项 - 64  
 视频分辨率 - 7  
 视频属性 - 53  
 刷新屏幕 - 53  
 参考资料 - 194

## 九划

帮助选项 - 66  
 帮助新增内容 - 4  
 按端口查看用户 - 85  
 标准鼠标模式 - 58  
 查看 KX II-101-V2 MIB - 106, 111, 116  
 查看 KX II-101-V2 用户列表 - 84  
 查看状态栏 - 64  
 相关文档 - 4  
 界面 - 5, 33  
 重新启动 KX II-101-V2 - 153  
 重新命名电源条 (电源条端口页) - 121, 123  
 重新命名端口 - 120  
 修改现有用户 - 87  
 修改现有用户组 - 83

修改和删除键盘宏 - 52  
将 L 型安装支架固定在 KX II-101-V2 上进行  
  水平安装 - 192  
客户机启动设置 - 63  
给类添加新属性 - 187  
绝对鼠标模式 - 60

## 十划

配置 - 169  
配置 IP 访问控制 - 141  
配置 SNMP 代理 - 106, 111  
配置 SNMP 陷阱 - 111  
配置日期/时间设置 - 110, 143  
配置事件管理 — 目的地 - 118  
配置事件管理 — 设置 - 111, 118  
高级 USB 连接设置 - 131  
读写不可用时的条件 - 74, 75  
调节视频设置 - 53  
调制解调器 - 109  
调制解调器访问电缆连接 - 110  
调试 - 167, 168  
通过 RADIUS 返回用户组信息 - 94  
验证设置 - 88

## 十一划

控制目标服务器电源 - 44  
控制电源条设备 - 125  
基于组的 IP 访问控制表 - 80, 84  
检查浏览器是否支持 AES 加密 - 137, 139  
虚拟媒体 - 60, 67  
常见问题解答 - 198  
常规设置 - 60  
  **第一步：配置目标服务器** - 9, 10  
  **第二步：配置网络防火墙设置** - 9, 20  
  **第三步：连接设备** - 9, 21  
  **第四步：配置 KX II-101-V2** - 9, 25  
停止 CC-SG 管理 - 154  
断开 KVM 目标服务器电源 - 45  
**断开虚拟媒体** - 75, 77  
添加、编辑和删除收藏夹 - 40  
添加新用户 - 86, 87  
添加新用户组 - 79  
维护 - 147

## 十二划

智能鼠标模式 - 59  
强密码 - 98, 133, 134  
登录 - 165  
登录限制 - 133  
编辑用户成员的 rcigroup 属性 - 188

## 十三划

概述 - 9, 42, 68, 129, 163, 172  
输入发现端口 - 105  
跟踪主机路由页 - 159  
键盘、视频和鼠标说明 - 195  
键盘/鼠标设置 - 108, 126, 196  
键盘宏 - 47  
键盘限制 - 62  
键盘选项 - 47  
简介 - 1  
鼠标设置 - 12  
鼠标指针同步 - 57  
鼠标选项 - 57

## 十四划

模拟 KVM 切换器 - 108, 126  
管理 KVM 目标服务器（端口页） - 120, 121  
管理 USB 连接 - 129  
管理功能 - 6  
管理电源关联 - 124  
管理收藏夹 - 38  
管理收藏夹页 - 39  
管理端口 - 109  
端口访问页 - 36  
端口配置 - 20, 119  
端口操作菜单 - 37  
缩放 - 65

## 十六划

操作系统 IPv6 支持注意事项 - 195  
默认登录信息 - 9

## ▶ 美国/加拿大/拉丁美洲

星期一至星期五

上午 8:00 - 傍晚 8:00 东部时间

电话：800-724-8090 或 732-764-8886

对于 CommandCenter NOC：按 6，然后按 1

对于 CommandCenter Secure Gateway：按 6，然后按 2

传真：732-764-8887

有关 CommandCenter NOC 的电子邮件：tech-ccnoc@raritan.com

有关其他所有产品的电子邮件：tech@raritan.com

## ▶ 中国

### 北京

星期一至星期五

上午 9:00 - 下午 6:00 当地时间

电话：+86-10-88091890

### 上海

星期一至星期五

上午 9:00 - 下午 6:00 当地时间

电话：+86-21-5425-2499

### 广州

星期一至星期五

上午 9:00 - 下午 6:00 当地时间

电话：+86-20-8755-5561

## ▶ 印度

星期一至星期五

上午 9:00 - 下午 6:00 当地时间

电话：+91-124-410-7881

## ▶ 日本

星期一至星期五

上午 9:30 - 下午 5:30 当地时间

电话：+81-3-3523-5991

电子邮件：support.japan@raritan.com

## ▶ 欧洲

### 欧洲

星期一至星期五

上午 8:30 - 下午 5:00 GMT+1 中欧时间

电话：+31-10-2844040

电子邮件：tech.europe@raritan.com

### 英国

星期一至星期五

上午 8:30 - 下午 5:00 GMT

电话：+44(0)20-7090-1390

### 法国

星期一至星期五

上午 8:30 - 下午 5:00 GMT+1 CET

电话：+33-1-47-56-20-39

### 德国

星期一至星期五

上午 8:30 - 下午 5:30 GMT+1 CET

电话：+49-20-17-47-98-0

电子邮件：rg-support@raritan.com

## ▶ 澳大利亚墨尔本

星期一至星期五

上午 9:00 - 下午 6:00 当地时间

电话：+61-3-9866-6887

## ▶ 台湾

星期一至星期五

上午 9:00 - 下午 6:00 GMT-5 标准时间 GMT-4 夏令时

电话：+886-2-8919-1333

电子邮件：support.apac@raritan.com