Dominion KX III

管理员指南
3.0.0 版

DKX3A-v3.0.0-0B-E

2014 年 2 月

255-62-0002-00

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。

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

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

Virtual KVM Client (VKC) 帮助 212

参考资料 314

Ch 1 简介

在本章内

概述

Dominion KX III 是公司级、安全、KVM 覆盖的 IP 开关，可为 1、2、4 或 8 名用户提供 8 - 64 台服务器的远程 BIOS 级控制。

KX III 附带有标准功能，例如 DVI/HDMI/DisplayPort 数字和模拟视频、音频、虚拟媒体、智能卡/CAC、刀片服务器支持以及移动访问.

单独部署 KX III， 或与 Raritan 的 CommandCenter Secure Gateway (CC-SG) 。

帮助新增内容

- KX III 支持 DVI 视频监视器
- 也为此版本添加：
  - 通过连接到 Raritan 的 Cat5 Reach DVI - 参看 ***Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality（连接 KX III 和 Cat5 Reach DVI - 提供延展的当地端口功能）*** (p. 273)
  - 改变至 Virtual KVM Client (VKC) 和 Active KVM Client (AKC) 连接属性 - 参看 ***Configuring Connection Properties（配置连接属性）*** (参看 "***配置连接属性***" p. 214)
  - 启用和禁用 KX III 远程客户机的收藏夹 - 参看 Managing Favorites（管理收藏夹）
  - 支持全部外部虚拟媒体驱动器类型

包装内容

每台 KX III 均为完整配置的独立产品，可以安装在 1U（KX2-864 为 2U）19" 机架安装机箱上。每台 KX III 设备包括下列零部件：

包装数量	品名
1	KX III 设备
1	KX III 快速安装指南
1	机架安装套件
2	交流电源线
1	4 个橡胶垫（用于桌面安装）
1	应用说明
1	保修卡

KX III 设备图片和功能

硬件

- 集成 KVM-over-IP 远程访问
- 1U 或 2U 机架安装（包括安装托架）
- 具备故障切换功能的双电源；自动切换电源，发出电源故障警报
- 支持下列 CIM：
  - 对于虚拟媒体和绝对鼠标同步，使用下列之一的 CIM：
    - D2CIM-VUSB
    - D2CIM-DVUSB
    - D2CIM-DVUSB-DVI
    - D2CIM-DVUSB-HDMI
    - D2CIM-DVUSB-DP
  - 要求 PS2 连接:
    - DCIM-PS2
- DVI 本地端口对 DVI 监视器支持
  - 从 DVI 至 VGA 转换器的 VGA 支持

  - 通过标准 DVI 电缆对 DVI 支持
- 支持分层，如果使用级联配置，用基础 KX III 设备访问多台其他级联设备。
- 多用户能力（1/2/4/8 个远程用户；1 个本地用户）
- UTP（5/5e/6 类）服务器电缆
- 双 Ethernet 端口 (10/100/1000 LAN)，具备故障切换功能
- 现场升级
- 在机架上访问所用的本地 USB 用户端口
  - USB 键盘/鼠标端口
  - 面板和背板上分别有一个和三个支持 USB 设备的 USB 端口
  - 全面支持本地和远程用户并发访问
  - 本地管理图形用户界面
- 集中访问安全
- 集成电源控制
- 双电源状态、网络活动和远程用户状态 LED 指示灯
- 硬件复位按钮

注意：版本 KX III 3.0.0 不支持调制调节器，但是未来版本将支持。

软件

- Windows®、Mac® 和 Linux® 环境下支持虚拟媒体*
- 绝对（鼠标同步）*

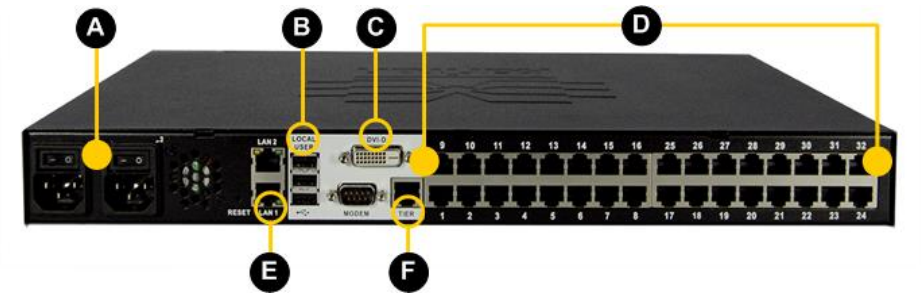
**注意：虚拟媒体和绝对鼠标同步要求使用 D2CIM-VUSB、D2CIM-DVUSB、D2CIM-DVUSB-DVI、D2CIM-DVUSB-HDMI 或 D2CIM-DVUSB-DP CIM.*

- 支持基于 USB 的数字音频
- 可配置的扫描设置支持最多 32 台目标服务器端口扫描和缩略图视图
- Web 访问和管理
- 直观图形用户界面
- 双端口视频输出支持
- KVM 信号（包括视频和虚拟媒体）256 位加密
- LDAP、Active Directory®、RADIUS 或内部验证和授权
- DHCP 寻址或固定 IP 寻址
- 智能卡/CAC 验证
- SNMP、SNMP3 和系统日志管理
- IPv4 和 IPv6 支持
- 与服务器直接关联、旨在防止错误的电源控制
- 与 Raritan CommandCenter Secure Gateway (CC-SG) 管理工具集成
- CC Unmanage 功能（使设备不受 CC-SG 控制）
- Raritan PX1 和 PX2 设备支持

Dominion KX3-832

KX3-832 图片

KX3-832 功能



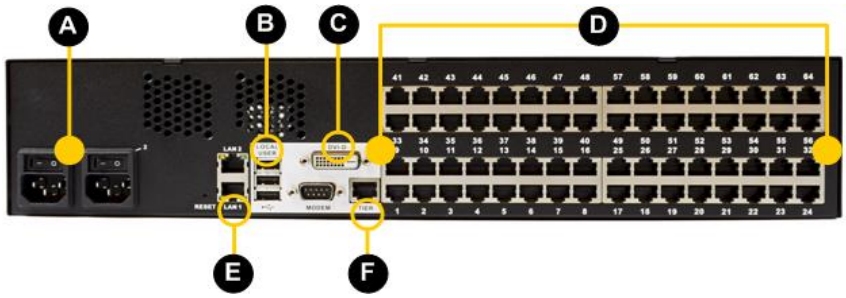
图示符号	
A	双电源 AC 100V/240V
B	本地 USB 端口
C	DVI-D 端口
D	32 KVM 端口 UTP 电缆 (Cat5/5e/6)
E	双 10/100/1000 Gigabit Ethernet 访问
F	分层端口

注意：版本 KX III 3.0.0 不支持调制调节器，但是未来版本将支持。

Dominion KX3-864

KX3-864 图片

KX3-864 功能



图示符号	
A	双电源 AC 100V/240V
B	本地 USB 端口
C	DVI-D 端口
D	64 KVM 端口 UTP 电缆 (Cat5/5e/6)
E	双 10/100/1000 Gigabit Ethernet 访问
F	分层端口

图示符号
注意：版本 KX III 3.0.0 不支持调制调节器，但是未来版本将支持。

每种型号支持的用户数和端口数：

Model（型号）	端口	远程用户数
KX3-864	64	8
KX3-832	32	8
KX3-808	8	8
KX3-464	64	4
KX3-432	32	4
KX3-416	16	4
KX3-232	32	2
KX3-216	16	2
KX3-132	32	1
KX3-116	16	1
KX3-108	8	1

KX III 远程和本地控制台界面

使用远程控制台界面通过网络连接配置和管理 KX III。

本地控制台界面接口从机架的 KX III 访问。

分别查看 ***KX III "远程控制台界面"（Remote Console Interface）***(参看 "***KX III Remote Console 界面***" p. 16)和 ***KX III "本地控制台界面"（Local Console Interface）*** (参看 "***KX III Local Console 界面***" p. 26)。

KX IIIKVM 客户机应用程序

KX III 可与 Virtual KVM Client (VKC) 和 Active KVM Client (AKC) 正常工作

如需获得使用客户机的帮助， 参看 ***Virtual KVM Client (VKC) 帮助*** (p. 212)和 ***Active KVM Client (AKC) 帮助*** (p. 258)。

KX III 联机帮助

KX III 联机帮助为你的首选帮助资源。PDF 版本的帮助为次要资源。

在开始使用 KX III 前，参看 KX III 版本说明以获取当前版本的重要信息。

KVM 客户机帮助作为 KX III 连接帮助的一部分提供。

在线帮助配有 KX III 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 Firmware, Upgrades and Documentation page（固件、升级和文档页）下载。

固件、升级和文件页面同样包括终端用户部分联机帮助，包括 KVM 客户机帮助、Local Console（本地控制台）帮助、Remote Console（远程控制台）帮助（如适用）、技术规格等。的 PDF 版本。

注意：必须在浏览器上启用 Active Content（活动内容），才能使用联机帮助。

Ch 2 入门

在本章内

安装和配置 KX III

如果还未这样做，请安装和配置 KX III。

参看与 KX III 设备随附的 KX III 快速安装指南或从 ***Raritan Support 网站 http://www.raritan.com/support***下载，或参看 ***KX III Installation and Configuration（安装和配置）*** (参看 "***KX III 安装和配置***" p. 27)。

允许弹出

无论使用哪种浏览器，都必须允许设备的 IP 地址弹出对话框，这样才能启动 KX III Remote Console。

安全警告和验证消息

登录 KX III 时，可能显示安全警告和应用程序验证消息。

包括：

- Java™ 安全警告和验证 KX III。参看 ***Java Validation and Access Warning（验证和访问警告）*** (参看 "***Java 验证和访问警告***" p. 9)，以及 ***Installing a Certificate（安装一个证书）*** (参看 "***安装证书***" p. 10)
- 根据你的浏览器和安全设置可能会显示另外的安全警告。参看 ***Additional Security Warnings（其他安全警告）*** (参看 "***其他安全警告***" p. 10)

Java 验证和访问警告

登录至 KX III， Java® 1.7 提示你验证 KX III，然后允许访问应用程序。

Raritan 建议在每个 KX III 设备中安装 SSL 证书，以便减少 Java 警告，并且提升安全。 参看 ***SSL 证书*** (p. 161)。

其他安全警告

即使在为 KX III 安装 SSL 证书后，根据 当你登录 KX III 时，在你的浏览器和安全设置上可能会显示另外的安全警告。

必须接受这些警告消息，才能启动 KX III Remote Console（远程控制台）。

在安全和证书警告消息对话框上选择下列选项，减少在后续登录过程中显示的警告消息数量：

- 今后不显示此警告 (In the future, do not show this warning)
- 总是信任来自此发行商的内容 (Always trust content from this publisher)

安装证书

浏览器可能提示你接受并验证 KX III 的 SSL 证书。

根据 当你登录 KX III 时，在你的浏览器和安全设置上可能会显示另外的安全警告。

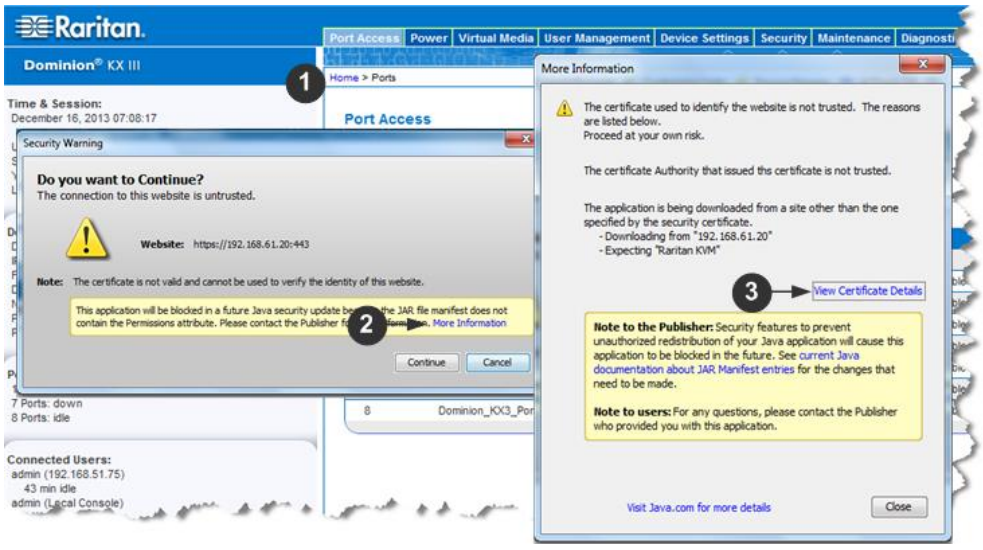
必须接受这些警告消息，才能启动 KX III Remote Console（远程控制台）。如要了解详细信息，参看 ***Security Warnings and Validation Messages（安全警告和验证消息）*** (参看 "*安全警告和验证消息*" p. 9)。

在此提供了两个关于如何在浏览器安装 SSL 证书的示例，两个示例都是使用 Microsoft Internet Explorer 8® 和 Windows 7®。

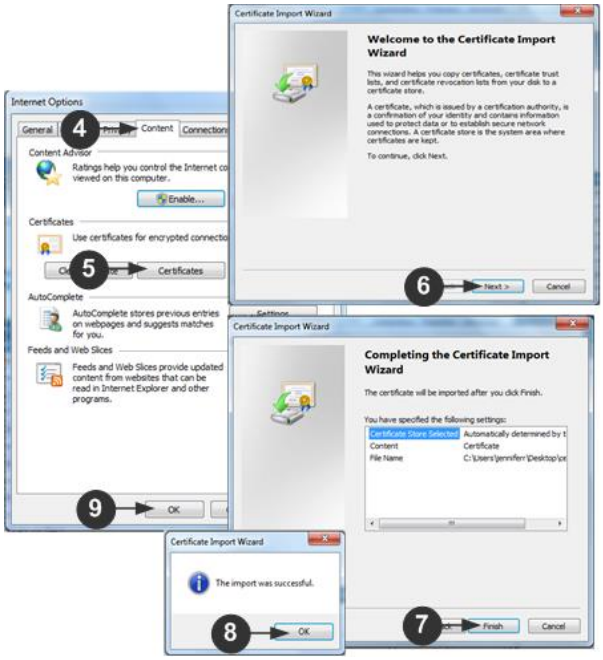
根据你的浏览器和操作系统有特定方法和步骤。参看你的浏览器和操作系统帮助获取更多信息。

示例 1：将证书导入浏览器

在这个示例中，你将证书导入浏览器。



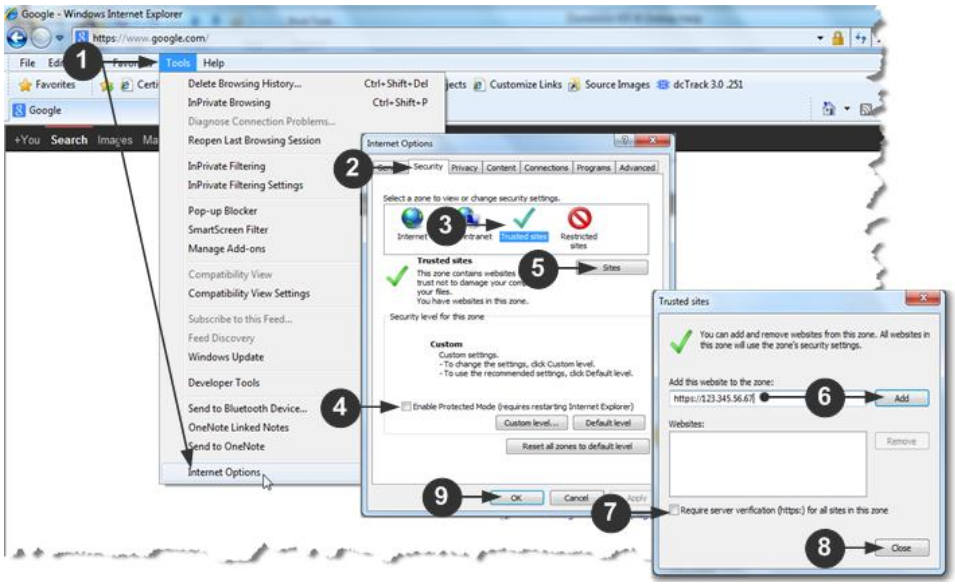
步骤	
1	打开 IE 浏览器，然后登录 KX III。
2	在第一个 Java™ 安全警告时点击 More Information（更多信息）。
3	在 More Information（更多信息）对话框点击 View Certificate Details（查看证书详情）。提示你安装证书。按照 wizard 步骤操作。 *注意：如果浏览器为提示你，手动选择 Tools（工具）> Internet Options（Internet 选项），打开 Internet Options（Internet 选项）对话框。*



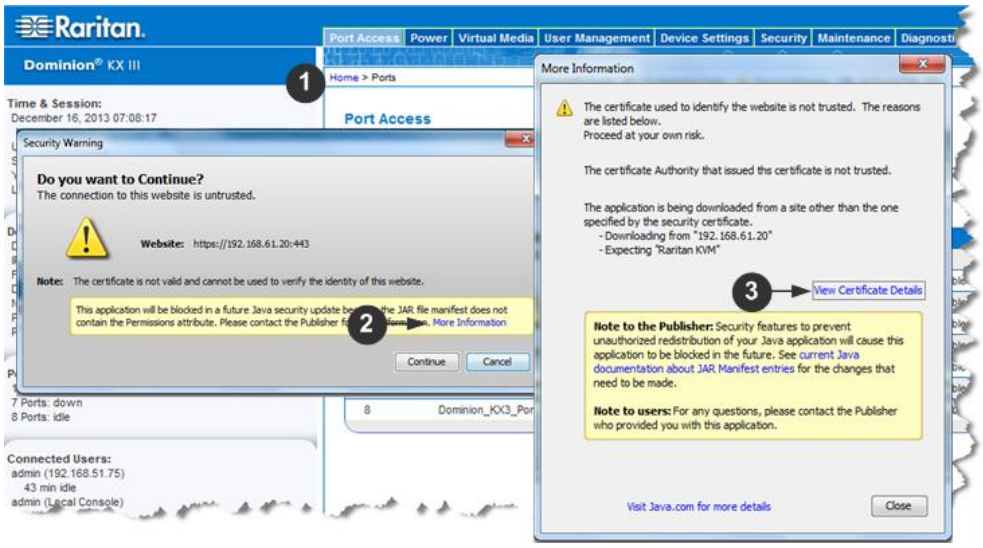
步骤	
4	单击“内容”选项卡。
5	单击证书。
6	Certificate Import Wizard（证书导入精灵）打开，并将在每一个步骤指导你。 ▪ 导入文件 - 浏览确认证书位置 ▪ 证书商店 - 选择储存证书的位置
7	在 Wizard 最后一步点击“完成”。
8	证书已导入。关闭成功信息。
9	在 Internet Option（网络选项）上点击“确定”(OK)以应用更改，关闭然后再次打开浏览器。

示例 2：将 KX III 添加至 Trusted Sites（信任网站）然后 Import（导入）证书

在这个示例中，KX III 的 URL 被添加为 Trusted Sites（信任网站），并且自签名证书也作为其中过程被添加。



步骤	
1	单击 IE 浏览器上的 Tools（工具） Internet > Options（Internet 选项），打开 Internet Options（Internet 选项）对话框。
2	单击“安全性”选项卡。
3	点击 Trusted Sites（信任网站）。
4	禁用保护模式，并接受任何警告。
5	点击网站以打开 Trusted Sites（信任网站）对话框。
6	输入 KX III URL，然后点击 Add（添加）按钮。
7	取消选择为区域进行服务器验证（如适用）。
8	单击 Close（关闭）按钮。
9	在 Internet Option（网络选项）上点击“确定”(OK)以应用更改，关闭然后再次打开浏览器。 然后，导入证书：.



步骤	
1	打开 IE 浏览器，然后登录 KX III。
2	在第一个 Java™ 安全警告时点击 More Information（更多信息）。
3	在 More Information（更多信息）对话框点击 View Certificate Details（查看证书详情）。提示你安装证书。按照 wizard 步骤操作。 如要了解详情，参看*示例 1：导入证书至浏览器* (参看 "*示例 1：将证书导入浏览器*" p. 11)

正在登录 KX III

从任何安装了 Microsoft .NET® 和/或 Java Runtime Environment™的、有网络连接的工作站登录到你的 KX III 远程控制台。

登录，并且使用 KX III 需要你允许弹出。

如需了解关于安全警告和验证消息，以及如何将其去除的信息，参看 ***Security Warnings（安全警告）和 Validation Messages（验证消息）*** (参看 "*安全警告和验证消息*" p. 9)

要登录 KX III：

1. 启动支持的网络浏览器
2. 输入：

- URL - *http:///IP-ADDRESS* 以使用基于 Java 的 Virtual KVM 客户机

  或者

- *http://IP-ADDRESS/akc* 使用基于 Microsoft .NET 的 Active KVM 客户机

IP-ADDRESS 是给你的 KX III 分配的 IP 地址。

你也可以使用 HTTPS 或由你的管理员(如适用)分配的 KX III 的 DNS 名称。

你始终会被从 HTTP 的 IP 地址转到 HTTPS 的 IP 地址。

3. 输入“用户名”和“密码”，然后单击“登录”。
4. 接受用户协议（如适用）。
5. 如果显示安全警告，接受和/或允许访问。

Ch 3 KX III 接口和导航

在本章内

概述

KX III Remote Console 界面和 KX III Local Console 界面是基于 Web 的界面，用于配置、管理、目标服务器列表和选择等目的。

KX III Remote Console 界面

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

KX III 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 III Remote Console 登录 KVM 目标服务器时，打开 Virtual KVM Client 窗口。

KX III Local Console 和 KX III Remote Console 图形用户界面有很多相似之处，凡是有差异的地方，本用户手册都加以说明。KX III Remote Console 有下列选项，但 KX III Local Console 没有这些选项：

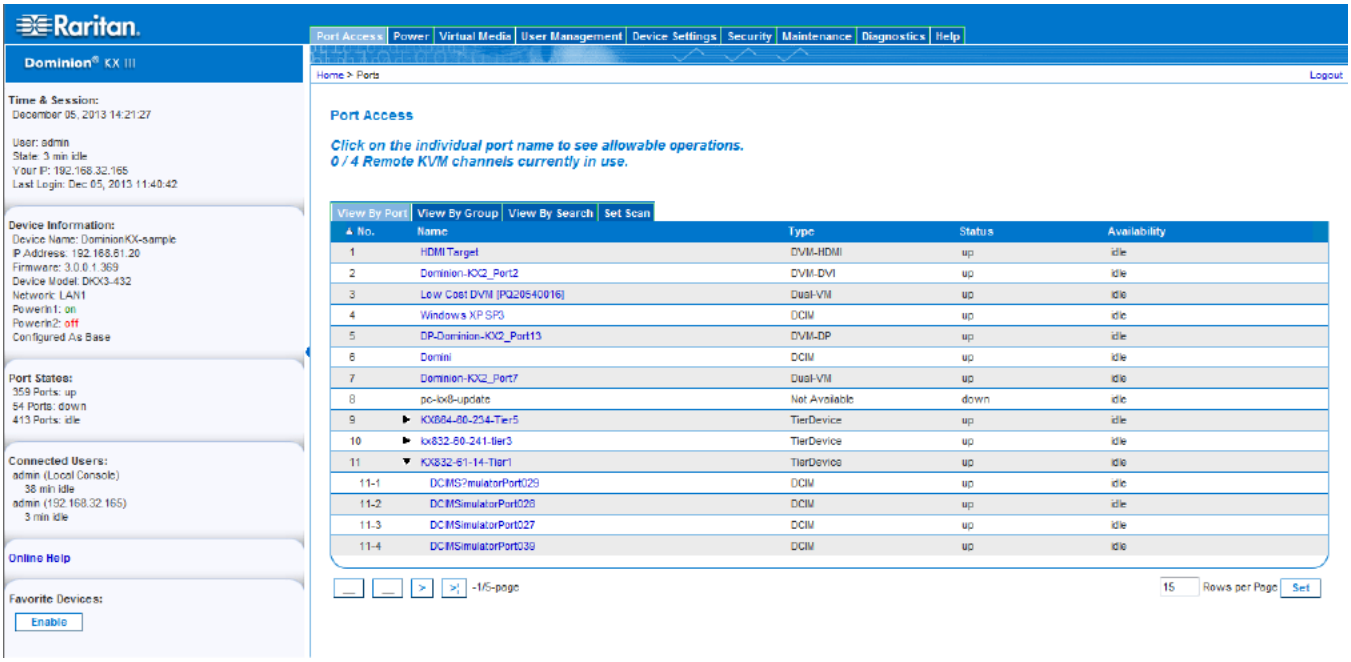
- Virtual Media（虚拟媒体）
- Favorites（收藏夹）
- Backup/Restore（备份/恢复）
- Firmware Upgrade（固件升级）
- SSL Certificates（SSL 证书）
- 音频

端口访问页（Remote Console 显示）

在成功登录之后，打开 Port Access（端口访问）页，列出所有端口及其状态和可用性。

与 KVM 目标服务器（刀片服务器和标准服务器）和电源条相连的端口用蓝色显示。右击任何这些端口以打开端口操作菜单。如需了解详细，参看 ***Port Action Menu（端口操作菜单）*** (参看 "***端口操作菜单***" p. 20)。

对于没有插入 CIM 的端口或 CIM 名称为空白的端口，指定默认端口名称 Dominion-KX3_Port# ，其中 Port# 是 KX III 物理端口编号。



本页有四个选项卡，可以在此按端口、按端口组、按搜索结果或按扫描端口查看端口。

可以单击列标题，按 Port Number（端口号）、Port Name（端口名称）、Status (Up and Down)（状态[工作或停止]）和 Availability (Idle, Connected, Busy, Unavailable, and Connecting)（可用性[空闲、已连接、忙、不可用和正在连接]排序端口。

可以在 Set Scan（设置扫描）选项卡上扫描最多 32 台与 KX III 相连的目标服务器。参看扫描端口 - 远程控制台了解详情。

分层设备 — 端口访问页

如果使用级联配置，用基础 KX III 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。 单击分层设备名称左边的展开箭头图标▶，在“端口访问”页上查看分层设备。参看配置和启用分层详细了解分层。

刀片服务器机箱 — 端口访问页

Port Access（端口访问）页采用可展开的分层形式显示刀片服务器机箱，刀片服务器机箱位于分层结构的根部，根下面显示各个有标号的刀片服务器。单击根机箱旁边的展开箭头图标▶显示各个刀片服务器。

注意：如要按分层顺序查看刀片服务器机箱，必须给刀片服务器机箱配置刀片服务器机箱子类型。

双端口视频组 — 端口访问页

双视频端口组作为双端口类型出现在端口访问页。端口组中的主端口和次端口分别作为双端口 (P) 和双端口 (S) 出现在端口访问页。例如，如果 CIM 类型为 DCIM，则显示“DCIM 双端口 (P)”。

当从远程客户机访问双端口视频组时，可以连接到主端口，这会打开双端口组中主端口和次端口的 KVM 连接窗口。

注意：在创建端口组时，定义双视频主端口。

注意：通过点击主端口远程连接双视频端口组需要两个 KVM 通道。如果没有两个通道，Connect（连接）链接将不显示。

注意：在单击双视频端口组中的辅端口时，不显示 Action（操作）菜单。

注意：不能通过本地端口同时连接主端口和辅端口。

按组查看选项卡

View by Group（按组查看）选项卡显示刀片服务器机箱组、标准端口组和双视频端口组。单击组旁边的展开箭头图标▶显示给此端口组指定的端口。

参看设备管理了解如何创建这些类型的端口组。

按搜索结果查看选项卡

View by Search（按搜索结果查看）选项卡允许你按端口名称进行搜索。搜索功能支持星号 (*) 通配符、全名和部分名称。

设置扫描选项卡

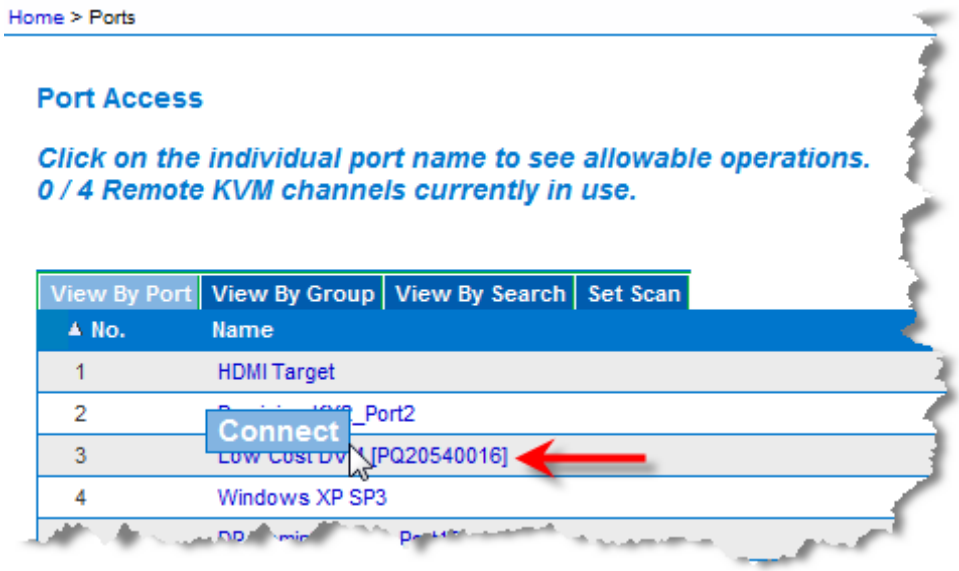
在 Port Access（端口访问）页上的 Set Scan（设置扫描）选项卡访问端口扫描功能。可以用此功能定义一组要扫描的目标服务器。扫描的目标服务器还可以用缩略图视图显示。选择一个缩略图，在 Virtual KVM Client 窗口上打开此目标服务器。

参看远程控制台了解详情。

端口操作菜单

在单击 Port Access（端口访问）列表上的 Port Name（端口名称）时，打开 Port Action（端口操作）菜单。

选择要针对该端口执行的菜单项。注意 Port Action（端口操作）菜单只列出当前可用的选项，视端口状态和可用性而定：



连接

- Connect（连接）— 建立至目标服务器的新连接。

  对于 KX III Remote Console，打开新的 Virtual KVM Client 页。

  对于 KX III Local Console，显示器切换到目标服务器，从本地用户界面切换过去。

  为了在本地端口上执行切换，必须显示 KX III Local Console 界面。

  也可以在本地端口上使用热键切换。

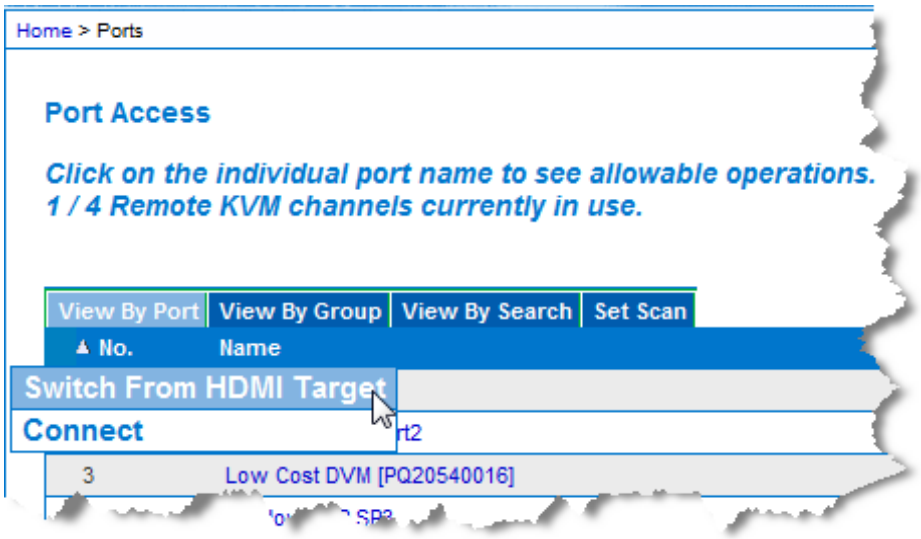
  注意：如果所有连接忙，在 KX III Remote Console 上不能把此选项用于可用端口。

切换自

- Switch From（切换自）— 从现有连接切换到所选端口（KVM 目标服务器）。

  此菜单项只适用于 KVM 目标服务器，且只当 Virtual KVM Client 打开时适用

注意：在 KX III Local Console 上不能使用此菜单项。

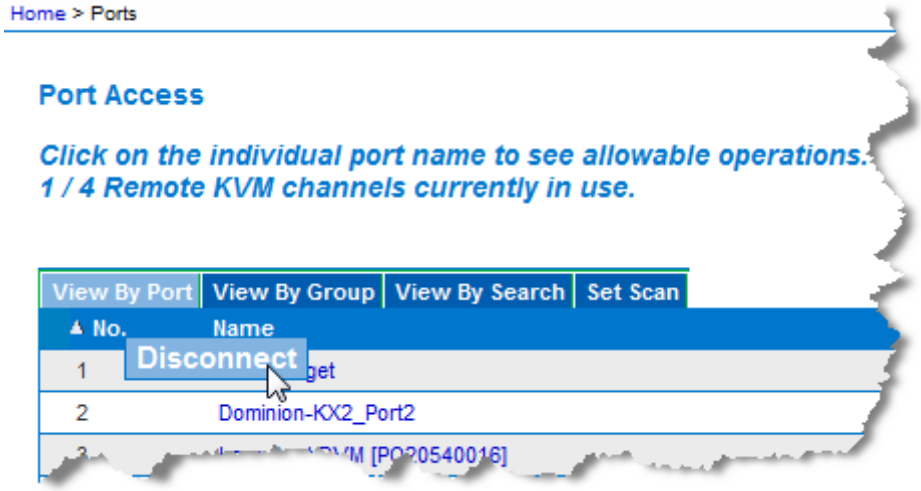


Disconnect（断开）

- 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。

注意：在 KX III Local Console 上不能使用此菜单项。在本地控制台上断开切换目标的唯一方法是使用热键。



开启电源

- 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。

关闭电源

- 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。

重新通电

- 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。

左面板

KX III 界面的左面板包含下列信息。

注意有的信息是有条件的 - 意为其根据你的角色、使用功能而显示。这些有条件的信息在此注明。

信息	Description（说明）	何时显示？
时间和会话 (Time & Session)	当前会话的开始日期和时间。	始终
用户	Username（用户名）	始终
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 III 所用的 IP 地址。	始终
Last Login（上次登录时间）	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 III 的 CC-SG 设备的 IP 地址。	当 KX III 受 CC-SG 管理时。
设备信息	你使用的 KX III 的特定信息。	始终
Device Name（设备名称）	给设备指定的名称。	始终
IP 地址	KX III 的 IP 地址。	始终
Firmware（固件）	当前固件版本。	始终
Device Model（设备型号）	KX III 的型号	始终
序列号	KX III 的序列号	始终
网络	给当前网络指定的名称。	始终
PowerIn1（电源输入 1）	电源 1 接口连接的状态。可以是开、关或自动检测关。	始终

信息	Description（说明）	何时显示？
PowerIn2（电源输入 2）	电源 2 接口连接的状态。可以是开、关或自动检测关。	始终
Configured As Base or Configured As Tiered（配置为基础或配置为分层）	如果使用分层配置，说明你访问的 KX III 设备是基础设备还是分层设备。	当 KX III 是分层配置的一部分时
Port States（端口状态）	KX III 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 III 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。	启用时
FIPS Mode（FIPS 模式）	FIPS 模式：EnabledSSL 证书：FIPS 模式投诉	在启用 FIPS 时

折叠左面板

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。

KX III 控制台导航

KX III 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。

KX III Local Console 界面

KX III Local Console 和 KX III Remote Console 图形用户界面有很多相似之处，凡是有差异的地方，本帮助都加以说明。

如需了解使用 Local Console 的详细信息，参看 ***KX III Local Console - KX III End User Help（中断用户帮助）***(参看 "***KX III Local Console - KX III End User Help（终端用户帮助）***" p. 261)。

Ch 4 KX III 管理员帮助

在本章内

概述

管理员帮助包括一般由 KX III 应用程序管理员执行的特定 KX III 功能信息，例如安全和配置 KX III，管理用户组合用户、管理安全等。

管理员功能一般在 KX III Remote Console 和/或 Local Console 执行。

功能一般由终端用户使用虚拟 KVM 客户机或 活跃 KVM 客户在执行，有的从 Remote Console 或 Local Console 执行的功能在其自己的帮助部分进行了说明。

这些功能包括使用虚拟媒体、配置鼠标设置、使用扫描端口功能、配置视频选项等。

KX III 安装和配置

参看与产品随附的 KX III 快速安装指南或从 Raritan 的支持网站下载，获取基本、最少设置步骤的快速参考。

在此包括但不在 QSG 包括的其他信息和可选步骤包括：

- *额外支持的鼠标设置* (p. 30)
- ***KX III Boot Up 期间的 LED 状态*** (p. 33)
- *连接 VGA 监视器（可选）* (p. 35)
- *第六步：配置键盘语言（可选）* (p. 42)

机架安装

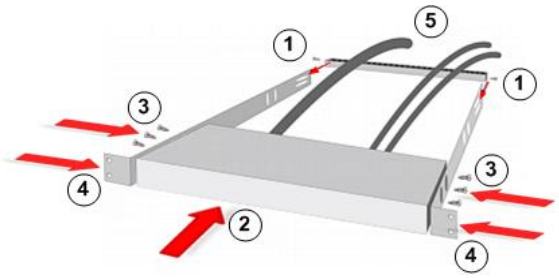
KX III 可以安装在 19" 标准设备机架上的 1U (1.75", 4.4cm) 垂直空间里。

注意：机架安装使用的 Raritan 设备仅供参考，可能并不是你的设备。按照说明是专门针对你的设备的。

正面安装

机架正面安装图中的编号对应介绍这种安装方法的各个步骤。

1. 用提供的两个螺丝把电缆管理槽固定在侧面托架后端。
2. 沿着侧面托架插入 KX III，使其背板正对电缆管理槽，直到面板与侧面托架的耳柄平齐为止。
3. 用剩余螺丝把 KX III 固定在侧面托架上（每侧三个螺丝）。
4. 用自备螺丝、螺栓、锁紧螺帽等把整个设备安装在机架上，把侧面托架的耳柄固定在机架的前滑轨上。
5. 在把电缆连接到 KX III 背板上时，把电缆置于电缆管理槽上。

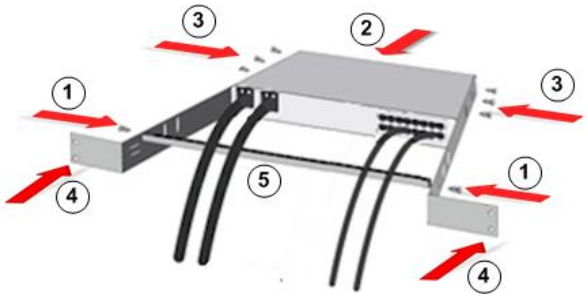


背面安装

机架背面安装图中的编号对应介绍这种安装方法的各个步骤。

1. 用提供的两个螺丝把电缆管理槽固定在侧面托架的前端靠近侧面托架耳柄的地方。
2. 沿着侧面托架插入 KX III，使其背板正对电缆管理槽，直到面板与侧面托架的后端平齐为止。
3. 用剩余螺丝把 KX III 固定在侧面托架上（每侧三个螺丝）。
4. 用自备螺丝、螺栓、锁紧螺帽等把整个设备安装在机架上，把侧面托架的耳柄固定在机架的前滑轨上。

5. 在把电缆连接到用户工作站或切换器背板上时，把电缆置于电缆管理槽上。



默认登录信息

默认值	值
用户名	*admin* 此用户有管理权。
Password（密码）	*raritan* 在首次启动 KX III 时，必须更改默认密码。
IP address	192.168.0.192.

重要说明：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。

第一步：配置网络防火墙设置

TCP Port（TCP 端口）5000

允许网络和防火墙在 TCP Port 5000 上进行通信，以允许远程访问 KX III。

也可以配置 KX III 使用另一个 TCP 端口，然后在该端口上启用通信。

TCP Port（端口） 443

允许访问 TCP 端口 443（标准 HTTPS），这样你可以通过浏览器访问 KX III。

TCP 端口 80

在启用 TCP 端口 80（标准 HTTP）访问之后，自动将 HTTP 请求重定向到 HTTPS。

第二步：配置 KVM 目标服务器

目标服务器视频分辨率

对于支持目标服务器分辨率列表，查看 ***KX III 支持目标服务器视频分辨率*** (参看 "***支持 KX III 的目标服务器视频分辨率***" p. 294) KX III 联机帮助。

鼠标设置

Raritan 建议使用绝对鼠标同步使目标服务器的鼠标设置最少。如需其他鼠标模式，请查看 ***额外支持的鼠标设置*** (p. 30) 。

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关于系。

具备 USB 端口的服务器支持此模式，虚拟媒体 CIM 默认使用此模式。

绝对鼠标同步 要求使用虚拟媒体 CIM：

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

额外支持的鼠标设置

除非另有指示，这些设置被配置在你的目标操作系统中。

鼠标设置

下面是对多种操作系统的鼠标设置。

除非另有指示，这些设置被配置在您的目标操作系统中。

参看 KX III 联机帮助或用户指南了解配置鼠标设置的详细信息。

Windows 7 和 Windows Vista 鼠标设置

在 Windows 7® 和 Windows Vista® 配置这些鼠标设置：

配置移动设置：

- 将 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。

禁用动画和淡化效果：

- Animate controls and elements inside windows（窗口用动画显示控件和元素）
- Animate windows when minimizing and maximizing（在最大化和最小化窗口时用动画显示窗口）
- 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出）

Windows XP、Windows 2003、Windows 2008 鼠标设置

Windows XP®、Windows 2003® 和 Windows 2008® 中配置这些鼠标设置：

配置移动设置：

- 将 Mouse Motion Speed（鼠标移动速度）准确设置为中速。
- 禁用 Enhance pointer precision（增强指针精度）选项。
- 禁用 Snap To（捕捉）选项。

禁用过渡效果：

- 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。

Windows 2000 鼠标设置

配置这些 Windows 2000® 鼠标设置：

配置移动设置：

- 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。

禁用过渡效果：

- 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。

Apple Mac 鼠标设置

配置这些 Apple Mac® 鼠标设置：

需要绝对鼠标同步，以便在 MAC® 操作系统上的 KVM 目标服务器上正确同步鼠标。

为了绝对鼠标同步的运行，需要虚拟媒体 CIM。如需支持 CIM 的列表，参看*支持的计算机接口模块 (CIM) 规格* (p. 296)。

完成了 KX III 安装后，设置 Mac USB 配置文件。如果你不设置这项配置文件，则鼠标不会在 OS X 内同步。

为此，执行下列操作之一：

1. 在 Raritan KVM Client 页上连接目标服务器。
2. 选择：USB 配置文件> 其他配置文件 > Mac OS-X (10.4.9 或更高版本)。

   或者

3. 在 KX III 选择“设备设置”(Device Settings) >“端口配置”(Port Configuration)，单击目标名称以打开 Port（端口）页面。
4. 展开“端口选择 USB 配置文件”部分。
5. 从可用框选择“Mac OS-X (10.4.9)或更高版本”，然后勾选 Add（添加）将其添加至已选框。
6. 在已选框单击“Mac OS-X (10.4.9)或更高版本”框。这会自动将其添加至 Preferred Profile（偏好配置文件）下拉列表。
7. 从偏好配置文件下拉列表选择“Mac OS-X (10.4.9)或更高版本”，然后选择“设置活跃配置文件为偏好配置文件”（Set Active Profile As Preferred Profile）之下的勾选框

- 单击 OK（确定）按钮应用。

Linux 鼠标设置

配置这些 Linux® 鼠标设置：

- （仅标准鼠标模式）将 Mouse Acceleration（鼠标加速度）准确设置为 1，将 Threshold（阈值）准确设置为 1。输入下列命令：`xset mouse 1 1`。如要在登录后执行，应该这样设置。

Sun Solaris 鼠标设置

配置 Sun® Solaris™ 鼠标设置:

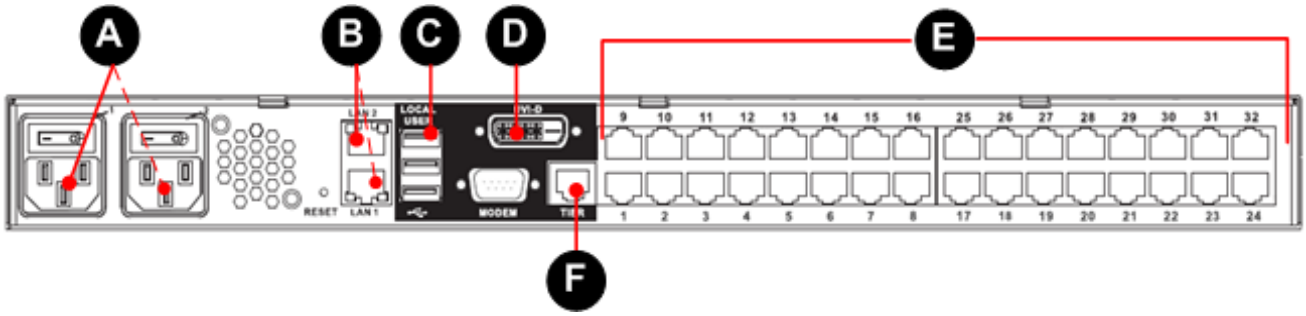
- 将 Mouse Acceleration（鼠标加速度）值精确设置为 1，将 Threshold（阈值）精确设置为 1。
- 确保显示卡设置为支持的分辨率，其输出为 VGA（而不是复合同步）。

IBM AIX 鼠标设置

配置 IBM AIX® 鼠标设置：

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

第三步：连接设备



A.交流电源

连接电源：

1. 将随附的交流电源线接到 KX III 上，将另一端插入交流电源插座。
2. 为了实现双电源故障切换保护，将随附的第二根交流电源线接到 KX III 上，将另一端插入与第一根电源线不同的电源插座。

KX III Boot Up 期间的 LED 状态

在启动 KX III 时，LED 灯会出现如下情况：

- 当第一次通电：
  - 所有频道 LED 都开启
  - 电源 LED 关闭
- 在开启相位：
  - 所有频道 LED 都关闭
  - 如果两个电源都开启，则电源 LED 为蓝色

- 如果一个电源开启，则电源 LED 为红色

B.网络端口

KX III 有两个 Ethernet 端口，用于故障切换（而非负荷平衡）。

在默认情况下，只有 LAN1 端口处于活动状态，禁用自动故障切换。

如果你想在其连接的 KX III 内部网络接口或网络开关不可用时 LAN2 使用相同 IP 地址，请启用网络故障切换。

要连接到网络：

1. 用标准 Ethernet 电缆将标有 LAN1 的网络端口连接到 Ethernet 交换机、集线器或路由器。
2. 使用任选的 KX III Ethernet 故障切换功能：
   a. 用标准 Ethernet 电缆将标有 LAN2 的网络端口连接到 Ethernet 交换机、集线器或路由器。
   b. 在 KX III 的 Network Configuration（网络配置）页上启用 Automatic Failover（自动故障切换）。

C. LOCAL USER（本地用户）端口（Local Console）。

要连接键盘和鼠标

- 把 USB 键盘和鼠标和键盘连接到 KX III 背面的相应 Local User（本地用户）端口。

在用户界面页面的机架处使用 KX III Local User（本地用户）端口管理服务器访问和目标服务器访问。

在安装和设置时需要本地用户，但在后续使用中是可选的。

D. 本地 DVI-D Port（端口）

标准的 DVI 线被用于连接至本地 DVI 监视器或键盘托盘(不包括 KX III)。

连接至 Raritan 的 T1700-LED 键盘托盘 DVI 端口。

使用要求的 DVI-D 至 VGA 转换器连接 VGA 监视器。

连接到一台 DVI 监视器

本地监视器必须支持最少 1024x768 的分辨率。

要连接到一台 DVI 监视器：

1. 把 USB 键盘和鼠标和键盘连接到 KX III 背面的相应 Local User（本地用户）端口。
2. 请将 DVI 接线的一头插入到 KX III 后方的 DIV-D 端口。
3. 将 DVI 接线的另一头插入到 DVI 监视器的 DVI 端口上。

连接 VGA 监视器（可选）

连接 VGA 监视器：

1. 把 USB 键盘和鼠标和键盘连接到 KX III 背面的相应 Local User（本地用户）端口。
2. 将 DVI-D 至 VGA 转换器插入 KX III 背面的 DVI-D 端口 ，通过顺时针方向转动其螺丝将其固定。
3. 连接一条 VGA 电缆至 DVI-D 至 VGA 转换器，将另一端连至你的 VGA 监视器，通过扭紧螺丝固定。

注意：DVI-D 至 VGA 转换器不包括在 KX III 内。联系 Raritan Sales 获取更多信息。

E.把目标服务器连接到 KX III

要将目标服务器连接到 KX III：

1. 连接 CIM 上的键盘、鼠标和视频插头至目标服务器相应的端口。
2. 通过 Cat5/5e/6 接线把 CIM 插入 KX III 背面的相应可用服务器端口。

F.分层（可选）

查看***配置和启用分层*** (p. 121, ***http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#33184***)

第四步：配置 KX III

对于接下来的步骤，你必须更改默认密码并且在 Local Console 给 KX III 分配其 IP 地址。

所有的其他步骤可以通过支持的网络浏览器使用 KX III 的默认 IP 地址从 Local Console 或 KX III Remote Console 执行。

需要 Java® 1.7 （或更高)）或 Microsoft .NET® 3.5（或之后版本）以使用 KX III。

更改默认密码

在首次启动 KX III 时，必须更改默认密码。

更改默认密码：

1. 设备启动后，使用默认用户名 *admin* 和密码 *raritan* 登录。单击“登录”(Login)。
2. 输入旧密码 *raritan*，然后输入并重新输入新密码。

   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。
3. 单击 Apply（应用）按钮单击确认页面上的 OK（确定）按钮。

分配一个 IP 地址给 KX III

要分配 IP 地址给 KX III：

1. 选择 Device Settings（设备设置）> Network（网络）。打开 Network Settings（网络设置）页。
2. 给 KX III 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. 然后，配置 IPv4、IPv6 和 DNS 设置。

配置 IPv4 配置

1. 在 IPv4 部分输入或选择合适的 IPv4 网络设置：
   a. 必要时输入 IP Address（IP 地址）。默认 IP 地址是 192.168.0.192。
   b. 输入 Subnet Mask（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），输入 Default Gateway（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，输入 Preferred DHCP Host Name（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 III 是基础设施设备，其 IP 地址不应发生变化。

  如果你想在主 Ethernet 端口（或其连接的开关/路由器）失败时确保使用冗余故障切换功能，选择此选项。如果其失败， KX III 故障转移至有相同 IP 地址的第二网络端口，以确保没有中断。

- 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 服务器指定网络参数。

  如果使用 DHCP，输入 Preferred host name（首选主机名）（仅限于 DHCP）。最长 63 个字符。

2. 然后，配置 IPv6 和/或 DNS 设置。

配置 IPv6 设置

1. 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，在设备上启用 IPv6。

   b. 输入 Global/Unique IP Address（全局/唯一 IP 地址）。这是给 KX III 分配的 IP 地址。

   c. 输入 Prefix Length（前缀长度）。这是 IPv6 地址使用的位数。

   d. 输入 Gateway IP Address（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。**Read-Only（只读）**

   f. Zone ID（域 ID）。标识与此地址关联的设备。**Read-Only（只读）**

   g. 选择 IP auto configuration（IP 自动配置）选项：

   - 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 III 是基础设施设备，其 IP 地址不应发生变化。

如果你想在主 Ethernet 端口（或其连接的开关/路由器）失败时确保使用冗余故障切换功能，选择此选项。如果其失败， KX III 故障转移至有相同 IP 地址的第二网络端口，以确保没有中断。

如果给 IP auto configuration（IP 自动配置）选择 None（无）：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）— 用于选项自动分配 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，仅应用于直接连接的子网。

2. 然后，配置 DNS 设置。

配置 DNS 设置

1. 如果选择了 DHCP，启用了 Obtain DNS Server Address（获取 DNS 服务器地址），就选择 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 服务器提供的 DNS 信息。
2. 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）
3. 在填写完之后，单击 OK（确定）按钮。

现在 KX III 设备可通过网络访问了。

命名你的目标服务器

▶ **命名目标服务器：**

1. 连接所有目标服务器（如果尚未连接）。
2. 选择选择“设备设置”(Device Settings) >“端口配置”(Port Configuration)，单击要重新命名的目标服务器的 Port Name（端口名称）。
3. 输入服务器名称。

最多 32 个字母数字和特殊字符。

4. 单击 OK（确定）。

指定电源自动检测

KX III 提供双电源

当使用两个电源时，KX III 将自动检测它们并提醒你它们的状态。

此外，在 Power Supply Setup（电源供应设置）页面的 Powerln1 和 Powerln2 Auto Detect（自动检测）的勾选框都被自动勾选。

如果你只在使用一个电源供应，你可以启用只自动检测使用的电源供应。

针对使用的电源启用自动检测：

1. 选择“设备设置”(Device Settings) >“电源设置”(Power Supply Setup)。打开 Power Supply Setup（电源设置）页。
2. 如果把电源输入线插入一号电源（设备背面最左边的电源），选择 Powerln1 Auto Detect（电源输入 1 自动检测）选项。
3. 如果把电源输入线插入二号电源（设备背面最右边的电源），选择 Powerln2 Auto Detect（电源输入 2 自动检测）选项。
4. 单击 OK（确定）。

如果选择任一个复选框，但仅连接电源输入，设备面板上的电源 LED 指示灯为红色。

配置日期/时间设置（可选）

也可以配置日期和时间设置。

如果启用 LDAPS 验证，日期和时间设置会影响 SSL 证书验证。

设置日期和时间：

1. 选择“设备设置”(Device Settings) >“日期/时间”(Date/Time)。打开 Date/Time Settings（日期/时间设置）页。
2. 在 Time Zone（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 Adjust for daylight savings time（调节夏令时）复选框。
4. 选择日期和时间设置方法：
   - User Specified Time（用户指定时间）— 选择此选项人工输入日期和时间。针对 User Specified Time（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 小时时钟）。

- Synchronize with NTP Server（与 NTP 服务器同步）— 使用此选项使日期和时间与 Network Time Protocol (NTP) 服务器同步。

5. 对于 Synchronize with NTP Server（与 NTP 服务器同步）选项：
   a. 输入 Primary Time Server（主时间服务器）的 IP 地址。
   b. 输入 Secondary Time Server（备用时间服务器）的 IP 地址。**任选**（可选）

注意：如果 Network （网络页面）中 Network Settings（网络设置）的 DHCP 被选择，则 NTP 服务器默认自动从 DHCP 服务器获取 IP 地址。

通过选择 Override DHCP 勾选框，人工输入 NTP 服务器 IP 地址。

6. 单击 OK（确定）。

创建用户组和用户

CC-SG 用户注意事项

在用 CommandCenter Secure Gateway 控制 KX III 时，CC-SG 验证用户和组，只有需要本地端口访问的本地用户除外。

当 CC-SG 控制 KX III 时，根据在 KX III 上配置的本地用户数据库或远程验证服务器（LDAP/LDAPS 或 RADIUS）验证本地端口用户。不根据 CC-SG 用户数据库验证这些用户。

如要进一步了解 CC-SG 验证，参看 **CommandCenter Secure Gateway 用户指南**、**CommandCenter Secure Gateway 管理员指南**或 **Deployment Guide 部署指南**，这些指南均可在 ***Raritan 网站 http://www.raritan.com***的支持页上找到。

支持的协议

为了简化用户名和密码管理，KX III 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 III 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。

第五步：启动 KX III Remote Console（远程控制台）

从任何安装了 Microsoft .NET® 和/或 Java Runtime Environment®的 有网络连接的工作站登录到你的 KX III 远程控制台。

启动 KX III 远程控制台：

1. 启动支持的网络浏览器
2. 输入：
   - URL - *http:///IP-ADDRESS* 以使用基于 Java 的 Virtual KVM 客户机

     或者

   - *http:///IP-ADDRESS/akc* 使用基于 Microsoft .NET 的 Active KVM 客户机

   IP-ADDRESS 是给你的 KX III 分配的 IP 地址。

   你也可以使用 HTTPS 或由你的管理员(如适用)分配的 KX III 的 DNS 名称。
3. 你始终会被从 HTTP 的 IP 地址转到 HTTPS 的 IP 地址。
4. 输入用户名和密码。单击“登录”(Login)。

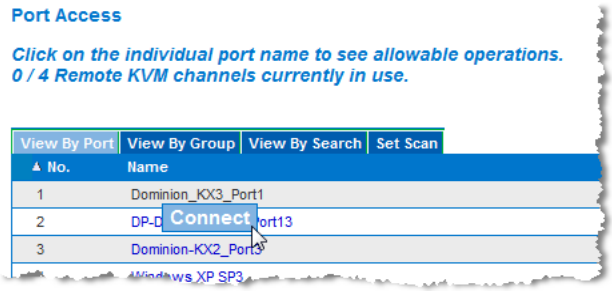
远程访问和控制目标服务器

KX III Port Access（端口访问）页显示一个列表，列出 KX III 的所有端口、相连的目标服务器及其状态和可用性。

从 KX III 访问目标服务器

访问目标服务器：

1. 在 KX III Port Access（端口访问）页面，点击你想访问的目标的 Port Name（端口名称）。显示 Port Action（端口操作）菜单。

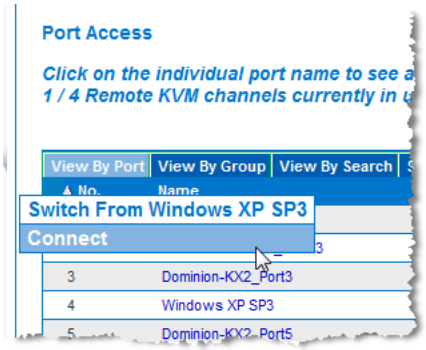


2. 在 Port Action（端口操作）菜单上选择 Connect（连接）。打开 KVM 窗口显示与目标服务器的连接。

在目标服务器之间切换

在 KVM 目标服务器之间切换：

1. 如果已经使用了一台目标服务器，访问 KX III“端口访问”页。
2. 单击要访问的目标服务器的端口名称，显示“端口操作”菜单。
3. 在“端口操作”菜单上选择“切换自”选项，显示你选择的新目标服务器。



从一台目标服务器断开连接

断开目标服务器：

- 在端口访问页面，单击要断开的目标服务器的端口名称，然后在端口操作菜单出现后点击“断开”。

  或者

- 关闭 KVM 客户机窗口

第六步：配置键盘语言（可选）

注意：如果使用美国/国际英语键盘，不需要执行此步骤。

如果使用美国英语之外的语言，必须将键盘配置为适当的语言。

此外，客户机和 KVM 目标服务器的键盘语言必须相同。

参看操作系统文档，进一步了解如何更改键盘布局。

更改键盘布局代码（Sun 目标服务器）

如果你使用 DCIM-SUSB，要将键盘布局更改为另一种语言，执行此步骤。

更改键盘布局代码（仅限于 DCIM-SUSB）：

1. 在 Sun™ 工作站上打开 Text Editor（文本编辑器）窗口。

2. 检查 Num Lock 键是否处于激活状态，然后按键盘上的左 Ctrl 键和 Del 键，或从键盘菜单选择选项“设置 CIM 键盘/鼠标选项”。

   Caps Lock 指示灯开始闪烁，表示 CIM 处于 Layout Code Change（布局代码更改）模式。

   文本窗口中显示：`Raritan Computer, Inc.Current keyboard layout code`（当前键盘布局代码）`= 22h (US5 UNIX)`。
3. 输入期望的布局代码（例如 *31* 表示日文键盘）。按 Enter 键。
4. 关闭设备，再接通设备电源。DCIM-SUSB 执行复位操作（重新通电）。
5. 确认显示的字符是否正确。

第七步：创建和安装 SSL 证书：

Raritan 强烈建议你在每个 KX III 设备中安装自己的 SSL 证书。

此项安全最佳实践可减少 Java® 警告消息的数量，并防止中间人攻击。

它同时可以防止未来的 Java 版本和浏览器版本阻止访问你的 KX III 设备。

如需创建和安装 SSL 证书的信息，请参见 ***SSL 证书*** (p. 161)。

机架式 PDU（电源条）出口控制

概述

KX III 允许你控制 Raritan PX 和 RPC 系列机架式 PDU（电源条）电源接口。 通过 D2CIM-PWR 连接 KX III。

在设置 PX 或 RPC 系列电源条并把它们连接到 KX III 之后，可以在 KX III 界面上的 Powerstrip（电源条）页上控制电源条及其电源接口。单击页面顶部的 Power（电源）菜单，即可访问本页。

Powerstrip（电源条）页显示与用户有适当端口访问权的 KX III 相连的机架式 PDU。 在分层配置情况下，Powerstrip（电源条）页同时显示与用户有适当端口访问权的基础 KX III 和分层 KX III 相连的机架式 PDU。

注意：参看 ***Raritan PX 用户指南****了解如何设置 PX。*

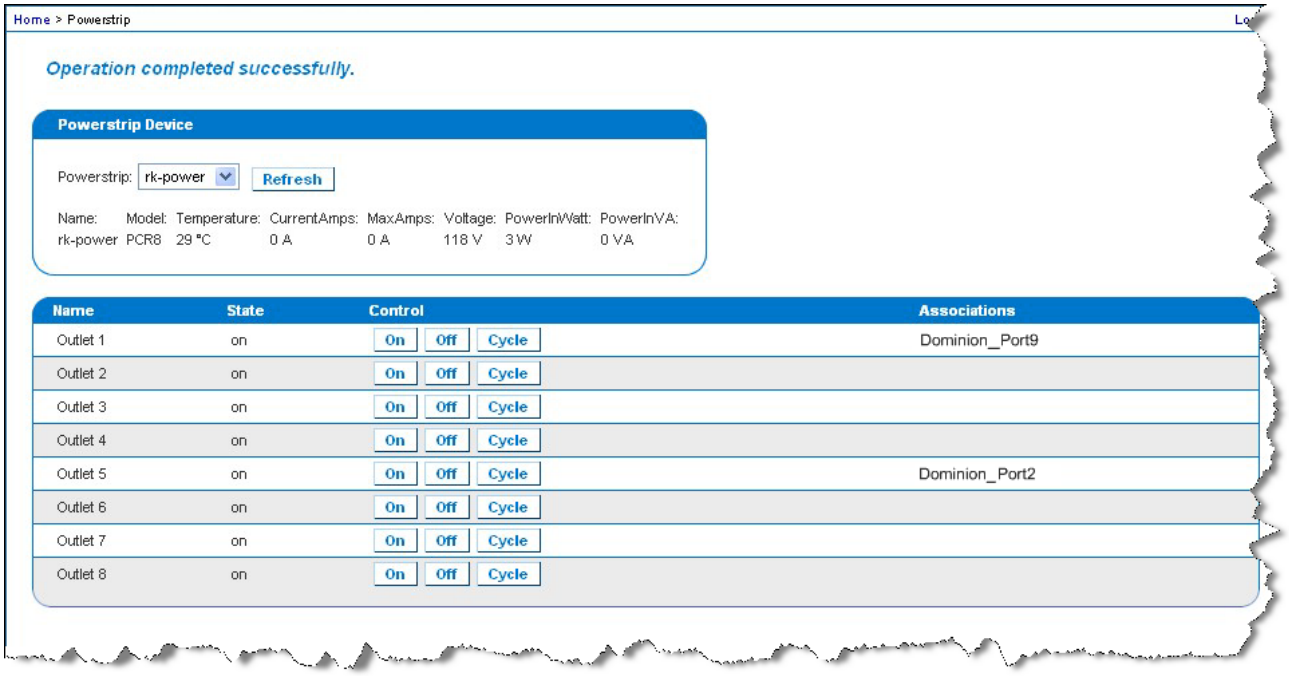
可以在 Powerstrip（电源条）页上给出口通电、断电和重新通电。还可以查看下列电源条信息和出口信息：

- 电源条设备信息
  - Name（名称）
  - Model（型号）
  - 温度

- 电流（安培）
- 最大电流
- 电压
- 功率（瓦）
- 功率（伏安）

- 出口显示信息：
  - 名称 — 在配置出口时给它指定的名称。
  - State（状态）— 出口的开或关状态。
  - 控制 — 给出口通电、断电或重新通电。
  - 关联 — 与出口关联的端口。

最初打开 Powerstrip（电源条）页时，Powerstrip（电源条）下拉列表显示当前与 KX III 相连的电源条。此外，还显示与当前选择的电源条相关的信息。如果没有任何电源条连接 KX III，本页的 Powerstrip Device（电源条设备）部分显示 No powerstrips found（找不到电源条）消息。



接通/断开出口电源和重新通电

▶ **接通出口电源：**

1. 单击 Power（电源）菜单访问 Powerstrip（电源条）页。

2. 在 Powerstrip（电源条）下拉列表上选择要接通哪个 PX 机架式 PDU（电源条）的电源。
3. 单击 Refresh（刷新）按钮查看电源控制。
4. 点击你想打开电源的出口旁边的 On （开启）。
5. 单击 OK（确定）按钮关闭 Power On（通电）确认对话框。接通出口电源，其状态为 on（开）。

断开出口电源：

1. 点击你想关闭电源的出口旁边的 off（关闭）。
2. 单击 OK（确定）。单击 Power Off（断电）对话框上的 OK（确定）按钮。
3. 单击 Power Off（断电）确认对话框上的 OK（确定）按钮。断开出口电源，其状态为 off（关）。

给出口重新通电：

1. 点击你想重新通电的出口旁边的 Cycle（重新通电）。打开 Power Cycle Port（给端口重新通电）对话框。
2. 单击 OK（确定）。给出口重新通电（注意这可能需要几秒钟时间）。
3. 在重新通电结束之后，打开对话框。单击 OK（确定）按钮关闭对话框。

USB 配置文件

概述

为了使 KX III 能支持更多不同的 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标准的 USB 配置文件。

Generic（默认值）USB 配置文件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®）的特定要求。

还有许多配置文件（用平台名称和 BIOS 版本号命名）可增强目标服务器的虚拟媒体功能，例如在 BIOS 级操作时。

USB 配置文件在 KX III Remote Console 和 KX III Local Console 的 Device Settings（设备设置） Port Configuration（端口配置） Port（端口）页上配置。

设备管理员可以用 USB 配置文件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。

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 Virtual KVM Client 上选择这些预先选择的配置文件。

例如假如服务器正在运行 Windows® 操作系统，最好使用 Generic 配置文件。

要在 BIOS 菜单上更改设置，或者要用虚拟媒体启动，BIOS 配置文件可能更合适，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 提供的任何一个标准 USB 配置文件，请联系 Raritan 技术支持部门寻求协助。

CIM 兼容性

为了使用 USB 配置文件，必须使用安装了最新固件的虚拟媒体 CIM。如需虚拟媒体 CIM 列表，参看 *支持的计算机接口模块 (CIM) 规格* (p. 296)。

可用的 USB 配置文件

最新版 KX III 配备如下表所述的 USB 配置文件。Raritan 提供的每次固件升级均包括新配置文件。在增加新配置文件时，在帮助中加以说明。

USB 配置文件	Description（说明）
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS 将此配置文件或 Generic 配置文件用于 Dell PowerEdge 1950/2950/2970/6950/R200 BIOS。 限制： ▪ 无
仅 BIOS Dell OptiPlex ™ 的键盘和鼠标	Dell OptiPlex BIOS 访问（仅键盘和鼠标） 在使用 D2CIM-VUSB 时，用此配置文件给 Dell OptiPlex BIOS 提供键盘功能。在使用新的 D2CIM-DVUSB 时，使用 Generic 配置文件。 注意： ▪ Optiplex 210L/280/745/GX620 需要 D2CIM-DVUSB 和 Generic 配置文件才能支持虚拟媒体 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不支持虚拟媒体
BIOS Dell Optiplex 790	在 BIOS 操作过程中，将此配置文件用于 Dell Optiplex 790 。 警告： ▪ 每当连接或断开虚拟媒体时，均触发 USB 枚举 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不支持绝对鼠标同步 ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
仅 BIOS Dell Optiplex 790 键盘	在 BIOS 操作中使用 Keyboard Macros 时，为 Dell Optiplex 790 使用此配置文件。本配置仅启用键盘。 限制： ▪ 鼠标已禁用。 ▪ 虚拟 CD-ROM 和磁盘驱动器被禁用

USB 配置文件	Description（说明）
仅 BIOS DellPowerEdge 键盘和鼠标	Dell PowerEdge BIOS 访问（仅键盘和鼠标） 在使用 D2CIM-VUSB 时，用此配置文件给 Dell PowerEdge BIOS 提供键盘功能。在使用新的 D2CIM-DVUSB 时，使用 Generic 配置文件。 注意： ▪ PowerEdge 650/1650/1750/2600/2650 BIOS 不支持 USB CD-ROM 和磁盘驱动器作为启动盘 ▪ PowerEdge 750/850/860/1850/2850/SC1425 BIOS 需要 D2CIM-DVUSB 和 Generic 配置文件才能支持虚拟媒体 ▪ 在 BIOS 下操作时，将 BIOS Dell PowerEdge 1950/2950/2970/6950/R200 或 Generic 配置文件用于 PowerEdge 1950/2950/2970/6950/R200 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不支持绝对鼠标同步™ ▪ 不支持虚拟媒体
BIOS ASUS P4C800 Motherboard	在 Asus P4C800 系统上用此配置文件通过虚拟媒体访问 BIOS 和 boot。 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
BIOS Generic	BIOS Generic 当 Generic 操作系统配置文件对 BIOS 不起作用时，使用此配置文件。 警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不支持绝对鼠标同步™ ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS 在操作系统安装过程中，将此配置文件用于 HP Proliant DL145 PhoenixBIOS。 限制：

USB 配置文件	Description（说明）
	▪ USB 总线速度限于全速 (12 MBps)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 使用此配置文件，用虚拟媒体启动 HP Compaq DC7100/DC7600 系列台式机。 限制： ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS 在 BIOS 操作过程中，将此配置文件用于 IBM® Thinkcentre Lenovo 系统板（828841U 型）。 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
IBM BladeCenter H with Advanced Management Module	当 D2CIM-VUSB 或 D2CIM-DVUSB 连接高级管理模块时，用此配置文件启用虚拟媒体功能。 限制： ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 和 BIOS Lenovo ThinkPad X61（用虚拟媒体启动） 使用此配置文件，用虚拟媒体启动 T61 和 X61 系列笔记本。 限制： ▪ USB 总线速度限于全速 (12 MBps)
Generic	Generic USB 配置文件的特性类似旧版 KX3 的特性。把此配置文件用于 Windows 2000®操作系统、Windows XP®操作系统、Windows Vista®操作系统和更新操作系统。 限制： ▪ 无
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) 在用 HP SmartStart CD 安装操作系统时，将此配置文件用于 HP Proliant DL360/DL380 G4 系列服务器。 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不支持绝对鼠标同步™
HP Proliant DL360/DL380 G4	HP Proliant DL360/DL380 G4（Windows 2003 Server 安装）

USB 配置文件	Description（说明）
（Windows 2003® Server 安装）	在不用 HP SmartStart CD 安装 Windows 2003 Server 时，将此配置文件用于 HP Proliant DL360/DL380 G4 系列服务器。 限制： ▪ USB 总线速度限于全速 (12 MBps)
Linux®	通用 Linux 配置文件 这是通用 Linux 配置文件；将它用于 Redhat Enterprise Linux、SuSE Linux Enterprise Desktop 和其他分发版本。 限制： ▪ 不支持绝对鼠标同步™
BIOS Mac®	BIOS Mac 将此配置文件用于 Mac BIOS。 限制： ▪ 不支持绝对鼠标同步™ ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器 如果你使用这个 USB 配置文件，在使用 Using the Mac Boot 菜单时参看 ***Mouse Modes*** (参看 "***使用 Mac Boot Menu 时的鼠标模式***" p. 52)，以在使用 Mac Boot 菜单时获得鼠标模式信息
MAC OS X®（10.4.9 和更高版本）	MAC OS X®（10.4.9 和更高版本） 此配置文件补偿最新版 Mac OS-X 引入的鼠标坐标缩放比例。如果远程鼠标位置和本地鼠标位置在桌面边沿附近不同步，就选择此选项。 限制： ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) 将此配置文件用于采用 Phoenix/AwardBIOS v6.00PG 的 RUBY-9715VG2A 系列工业主板。 限制： ▪ USB 总线速度限于全速 (12 MBps) ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS 将此配置文件用于采用 Phoenix/AwardBIOS 的 Supermicro 系列主板。 限制：

USB 配置文件	Description（说明）
	▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器
Suse 9.2	SuSE Linux 9.2 将此配置文件用于 SuSE Linux 9.2 分发版本。 限制： ▪ 不支持绝对鼠标同步™ ▪ USB 总线速度限于全速 (12 MBps)
Troubleshooting 1	Troubleshooting 配置文件 1 ▪ 第一海量存储设备 ▪ 键盘和鼠标 (Type 1) ▪ USB 总线速度限于全速 (12 MBps) ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器 警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。
Troubleshooting 2	Troubleshooting 配置文件 2 ▪ 第一键盘和鼠标 (Type 2) ▪ 海量存储设备 ▪ USB 总线速度限于全速 (12 MBps) ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器 警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。
Troubleshooting 3	Troubleshooting 配置文件 3 ▪ 第一海量存储设备 ▪ 键盘和鼠标 (Type 2) ▪ USB 总线速度限于全速 (12 MBps) ▪ 不能同时使用虚拟 CD-ROM 和磁盘驱动器 警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。
Use Full Speed for Virtual Media CIM（针对虚拟媒体 CIM 使用全速）	Use Full Speed for virtual media CIM（针对虚拟媒体 CIM 使用全速） 此配置文件的特性类似在选择 Full Speed for Virtual Media CIM（虚拟媒体 CIM 全速）选项时，旧版 KX3 的特性。可用于那些不能处理高速 USB 设备的 BIOS。 限制：

USB 配置文件	Description（说明）
	▪ USB 总线速度限于全速 (12 MBps)
Use Full Speed for Keyboard and Mouse USB	此配置文件把 Dual-VM CIM 上的键盘和鼠标 USB 接口设置为 Full Speed（全速）。可用于那些不能正确处理低速 USB 设置的设备。 限制： ▪ 键盘和鼠标 USB 接口的 USB 总线速度设置为全速 (12 MBps)

使用 Mac Boot Menu 时的鼠标模式

与 USB 配置文件工作时，如需使用 Mac Boot Menu 内的鼠标，你必须使用单鼠标模式，因为绝对鼠标模式在 BIOS 中不被支持。

配置要在启动菜单上使用的鼠标：

1. 重新启动 Mac，在重新启动过程中按 Option 键打开 Boot（启动）菜单。此时鼠标没有响应。
2. 选择单鼠标模式鼠标先响应

   注意：在 Single Mouse（单鼠标）模式下，鼠标速度可能很慢。

3. 在退出 Boot（启动）菜单回到 OS X 之后，退出 Single Mouse（单鼠标）模式，切换回 Absolute Mouse（绝对鼠标）模式。

给 KVM 端口选择配置文件

KX III 配备一组 USB 配置文件，你可以根据 KVM 端口所连的 KVM 目标服务器的特性，给 KVM 端口指定这些配置文件。可以在 Device Settings（设备设置） Port Configuration（端口配置） Port（端口）页、KX III Remote Console 或 ProductName Local Console 上给 KVM 端口指定 USB 配置文件。

指定配置文件的管理员很可能必须是特定目标服务器的管理员。在此之后，可以通过 Virtual KVM Client (VKC)选择这些配置文件。如果尚未指定配置文件，可以选择 USB Profile（USB 配置文件）> Other Profiles（其他配置文件）访问任何一个可用的配置文件。

在给 KVM 端口指定 USB 配置文件之后，当用户连接 KVM 目标服务器时，可以使用这些配置文件。如有必要，用户可以在 Virtual KVM Client (VKC)的 USB Profile（USB 配置文件）菜单上选择一个 USB 配置文件。

如要了解如何给 KVM 端口指定 USB 配置文件，参看***配置 USB 配置文件（端口页）*** (p. 113)。

用户管理

用户组

KX III 在内部存储所有用户名和组名的列表，以便确定访问权和权限。这些信息在内部采用加密格式存储。有几种验证方式，这种验证方式称为本地验证。必须验证所有用户。如果给 KX III 配置了 LDAP/LDAPS 或 RADIUS，先进行此验证，再进行本地验证。

每台 KX III 有三个默认用户组。不能删除这些用户组：

用户	Description（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组的成员，具有所有系统权限。此外，Admin 用户必须是 Admin 组的成员。
Unknown（未知）	这是那些用 LDAP/LDAPS 或 RADIUS 进行外部验证或系统未知的用户的默认组。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）组。此外，新创建的任何用户均自动放入此组，直到给他们指定另一个组为止。
Individual Group（个人组）	个人组基本上是一个人的“组”。也就是说，特定用户位于自己的组里，与其他实际组没关于联。可以在个人组里使用 @ 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组相同的权限。

KX III 最多允许创建 254 个用户组。 在 KX III 上最多可以创建 254 个用户组。

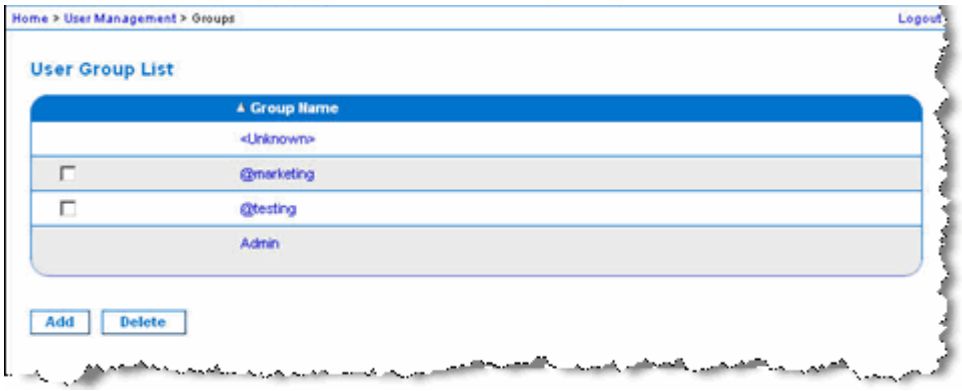
用户组列表

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 III 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。

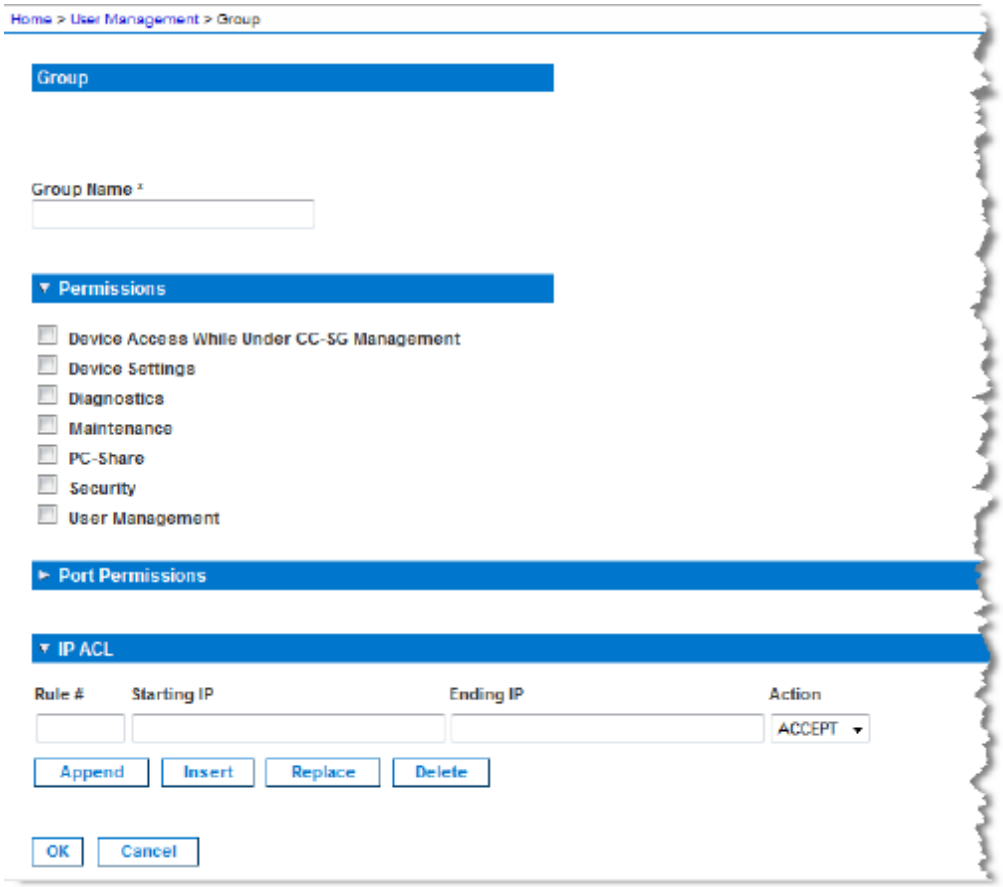
也可以选择不让特定用户与用户组关联。在此情况下，可以把此用户归入个人用户组。

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）。
3. 选择要给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。
4. 指定此用户组的用户使用的服务器端口和访问类型。 参看 ***设置端口权限*** (p. 57)。
5. 设置 IP ACL（IP 访问控制表）。此功能通过指定 IP 地址来限制对 KX III 设备的访问。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（并确定优先级）。参看***基于组的 IP 访问控制表*** (p. 58)。 任选
6. 单击 OK（确定）。



设置权限

权限	Description（说明）
Device Access While Under CC-SG Management（在 CC-SG 管理下的设备访问）	在 CC-SG 上针对 KX III 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。可以在上访问此设备。 在直接访问受 CC-SG 管理的设备时，在 KX III 上记录访问活动和连接活动。根据 KX III 验证设置执行用户验证。 *注意：Admin（管理员）用户组默认有此权限。*
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。
诊断	网络接口状态、网络统计数据、ping 主机、主机跟踪路由、KX III 诊断
维护	备份和恢复数据库、固件升级、工厂复位、重新启动。
PC-Share（PC 共享）	多个用户同时访问同一个目标。 如果使用分层配置，用基础 KX III 设备访问多台其他分层设备，所有设备必须使用相同的 PC 共享设置。参看配置和启用分层详细了解分层。
安全	SSL 证书、安全设置（VM 共享和 PC 共享）、IP ACL。
用户管理	用户和用户组管理、远程验证 (LDAP/LDAPS/RADIUS)、登录设置。 如果使用分层配置，用基础 KX III 设备访问多台其他分层设备，所有设备上的用户设置、用户组设置和远程验证设置必须保持一致。参看配置和启用分层详细了解分层。

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）	观看视频，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。 为了让一个用户组里的所有用户看到添加的 KVM 切换器，必须授予每个用户控制访问权。如果他们没有此权限，在稍后添加 KVM 切换器时，他们看不到切换器。 必须授予控制访问权，才能激活与音频或智能卡有关的控制。

虚拟媒体访问	
选项	**Description（说明）**
Deny（拒绝）	端口彻底拒绝虚拟媒体权限
Read-Only（只读）	虚拟媒体访问仅限于读访问
Read-Write（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

对于刀片服务器机箱，端口访问权限控制对给刀片服务器机箱配置的 URL 的访问。选项是 Deny（拒绝）或 Control（控制）。此外，机箱上的每个刀片服务器都有自己的独立端口权限设置。

如果使用级联配置，用基础 KX III 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。分层设备执行逐个端口控制。参看配置和启用分层详细了解分层。

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。

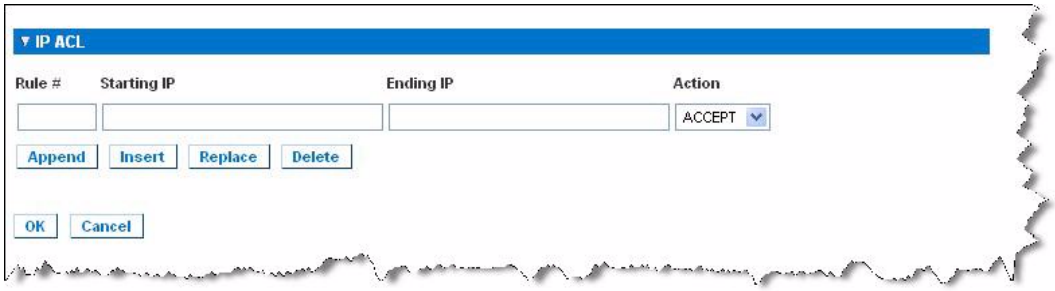
基于组的 IP 访问控制表

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 III。

此功能按所选组里的用户，将 KX III 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 III 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 III 设备。

- Drop（拒绝）— 设置为 Drop（拒绝）的 IP 地址拒绝访问 KX III 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。

修改现有用户组

注意：对于 Admin 组启用了所有权限，你无法对此进行更改。

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。
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. 57)。
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 III 设备的访问。参看***基于组的 IP 访问控制表*** (p. 58)。
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<unknown>（未知）用户组。

提示：为了确定特定用户组的用户，按 User Group（用户组）排序 User List（用户列表）。

1. 单击 Group Name（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”。
3. 在系统提示你确认删除时，单击 OK（确定）按钮。

Users（用户）

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

最多可以给每个用户组创建 254 个用户。

如果使用级联配置，用基础 KX III 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。 用户需要拥有访问基础设备所需的权限，以及在必要时访问各台级联设备所需的权限。

当用户登录到基础设备时，查询每台级联设备，用户可以访问他们有权限的每台目标服务器。 参看配置和启用级联详细了解级联。

添加新用户

最好在创建 KX III 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. 150)。*

▶ 添加新用户：

1. 选择“用户管理”(User Management) >“添加新用户”(Add New User)，或者单击 User List（用户列表）页上的 Add（添加）按钮。
2. 在 Username（用户名）字段里输入唯一姓名（最长 16 个字符）。
3. 在 Full Name（全名）字段里输入用户全名（最长 64 个字符）。
4. 在 Password（密码）字段里输入密码，在 Confirm Password（确认密码）字段里再次输入密码（最长 64 个字符）。
5. 在 User Group（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. 58)。
6. 如要激活此新用户，选择“活动”复选框。单击“确定”按钮。

查看 KX III 用户列表

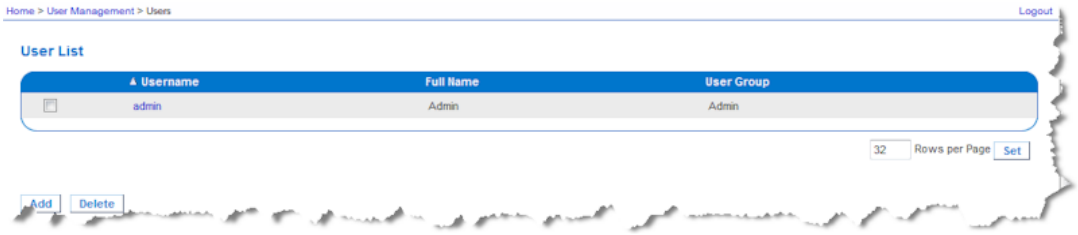
User List（用户列表）页显示所有用户的列表，包括他们的用户名、全名和用户组。可以单击任何一个列名称，按任何一列排序列表。可以在 User List（用户列表）页上添加、修改或删除用户。

有用户管理权限的 KX III 用户可以在必要时让用户断开端口或退出系统(强制退出)。参看 ***让用户断开端口*** (p. 63)和 ***让用户退出 KX III（强制退出）*** (参看 "***让用户退出 KX III（强制退出）***" p. 63)。

如要查看每个用户连接的目标服务器端口，参看***按端口查看用户*** (p. 62)。

查看用户列表：

- 选择“用户管理”(User Management) >“用户列表”(User List)。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。 不列出在扫描端口时访问的端口。

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（2）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）— 客户电脑的 IP 地址访问 KX III
- 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 III。

---

*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 III。参看***让用户退出 KX III（强制退出）** *(p. 63)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 III（强制退出）

如果你是管理员，可以让已登录 KX III 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. 63)。

让用户退出 KX III：

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。

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. 61)，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。

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 III 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。

如果使用级联配置，用基础 KX III 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。基础设备和级联设备必须使用相同的验证设置。

可以在 Authentication Settings（验证设置）页上配置在访问 KX III 时所用的验证的类型。

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。
3. 单击 

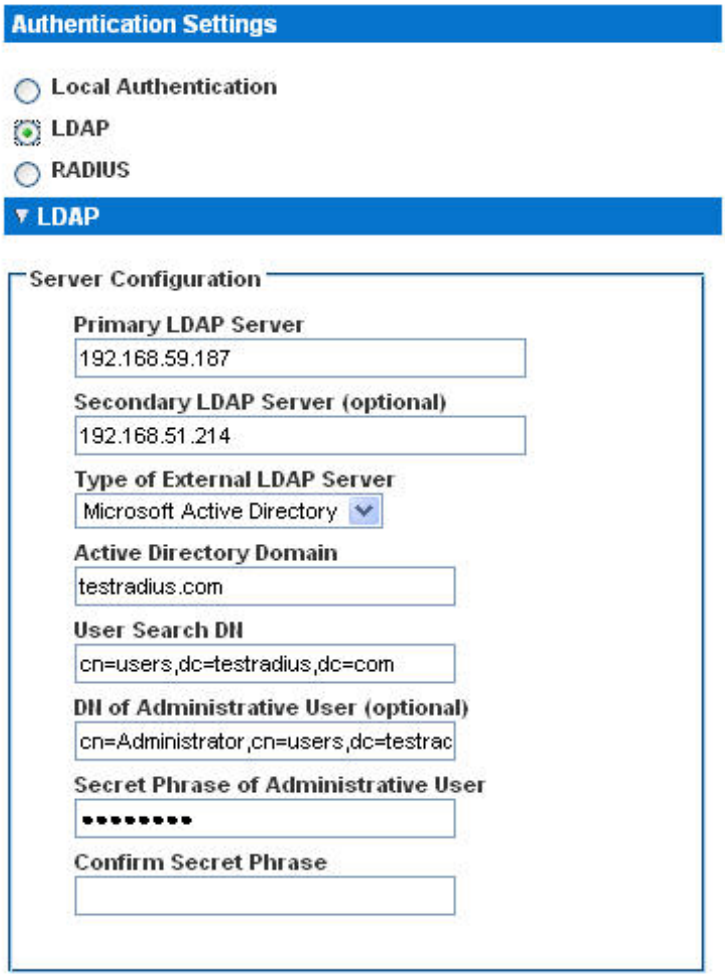
图标展开本页的 LDAP 部分。

   服务器配置

4. 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。
5. 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**
6. 外部 LDAP 服务器的类型。
7. 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。

8. 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。
9. 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。
10. 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）。



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 III 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。

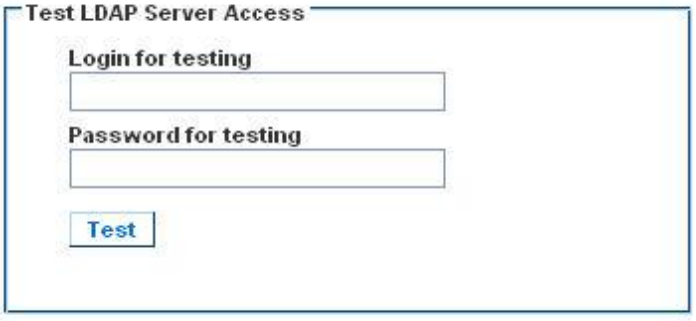
注意：如果选择 Enable LDAPS Server Certificate Validation（启用 LDAPS 服务器证书验证）选项，除了使用 CA 根证书验证，服务器主机名必须与服务器证书上的公用名相匹配。

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 III，新证书才生效。

测试 LDAP 服务器访问

17. 由于成功配置 LDAP 服务器和 KX III 进行远程验证有时很复杂，所以 KX III 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 III 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。



从 Active Directory 服务器返回用户组信息

KX III 支持用 Active Directory® (AD) 进行用户验证，不要求在 KX III 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 III 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 III 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 III 上启用 AD 服务器：

1. 用 KX III 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 III 用户指定在第二步中创建的用户组。
4. 在 KX III 上正确启用和配置 AD 服务器。参看*实现 LDAP/LDAPS 远程验证* (p. 65)。

重要说明

- 组名称区分大小写。
- KX III 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 III 用户组配置，KX III 自动给成功验证的用户指定<未知>用户组。
- 如果使用回拨号码，必须输入下列区分大小写的字符串：*msRADIUSCallbackNumber*。
- 根据 Microsoft 的建议，应该使用有用户帐号的 Global Groups（全局组），而不使用 Domain Local Groups（域本地组）。

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：

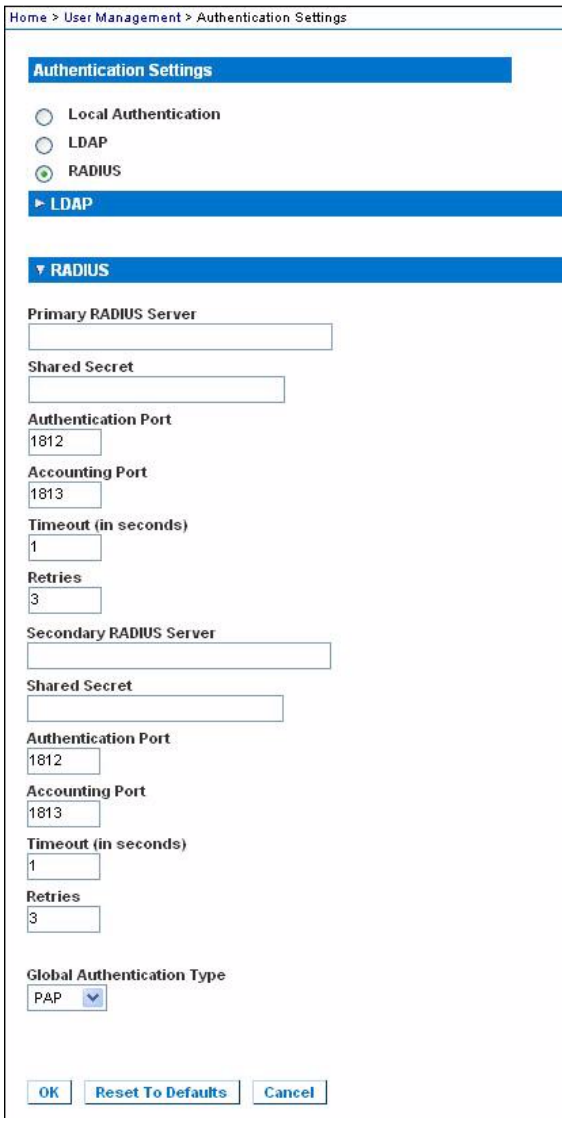
1. 单击 User Management（用户管理）> Authentication Settings（验证设置），打开 Authentication Settings（验证设置）页。
2. 单击 RADIUS 单选按钮启用本页的 RADIUS 部分。
3. 单击 RADIUS 图标展开本页的 RADIUS 部分。
4. 在 Primary RADIUS Server（主 RADIUS 服务器）字段和 Secondary RADIUS Server（备用 RADIUS 服务器）字段里分别输入主远程验证服务器和备用远程验证服务器的 IP 地址（最多 256 个字符）。
5. 在 Shared Secret（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 III 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 III 在发送另一个验证请求之前，等待 RADIUS 服务器做出响应的时间。
9. Retries（重试次数）默认次数是 3 次。

   这是 KX III 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。



Cisco ACS 5.x for RADIUS 验证

如果使用 Cisco ACS 5.x 服务器，在给 KX III 配置 RADIUS 验证之后，在 Cisco ACS 5.x 服务器上执行下列步骤。

注意：下列步骤包括访问每个页面所用的 Cisco 菜单和菜单项。请阅读 Cisco 文档了解每个步骤的最新信息，详细了解如何执行这些步骤。

- 添加 KX III 作为 AAA 客户机（**必填**）— Network Resources（网络资源）> Network Device Group（网络设备组）> Network Device and AAA Clients（网络设备和 AAA 客户机）
- 添加/编辑用户（**必填**）— Network Resources（网络资源）> Users and Identity Stores（用户和身份存储）> Internal Identity Stores（内部身份存储）> Users（用户）
- 配置默认网络访问启用 CHAP 协议（**可选**）— Policies（策略）> Access Services（访问服务）> Default Network Access（默认网络访问）
- 创建验证策略规则控制访问（**必填**）— Policy Elements（策略元素）> Authorization and Permissions（验证和权限）> Network Access（网络访问）> Authorization Profiles（验证配置文件）
  - Dictionary Type（词典类型）： RADIUS-IETF
  - RADIUS Attribute（RADIUS 属性）： Filter-ID
  - Attribute Type（属性类型）： String
  - Attribute Value（属性值）：Raritan:G{KVM_Admin}（其中 KVM_Admin 是在 Dominion KVM 切换器本地创建的用户组名称）。区分大小写。
- 配置会话条件（日期和时间）（**必填**）— Policy Elements（策略元素）> Session Conditions（会话条件）> Date and Time（日期和时间）
- 配置/创建网络访问验证策略（**必填**）— Access Policies（访问策略）> Access Services（访问服务）> Default Network Access（默认网络访问）>Authorization（验证）

通过 RADIUS 返回用户组信息

当 RADIUS 验证尝试成功时，KX III 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。

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

其中 GROUP_NAME 字符串是用户所属的用户组的名称，Dial Back Number 是与用户帐号关联的号码，KX III 要用此号码回拨用户帐号。

RADIUS 通信交换规范

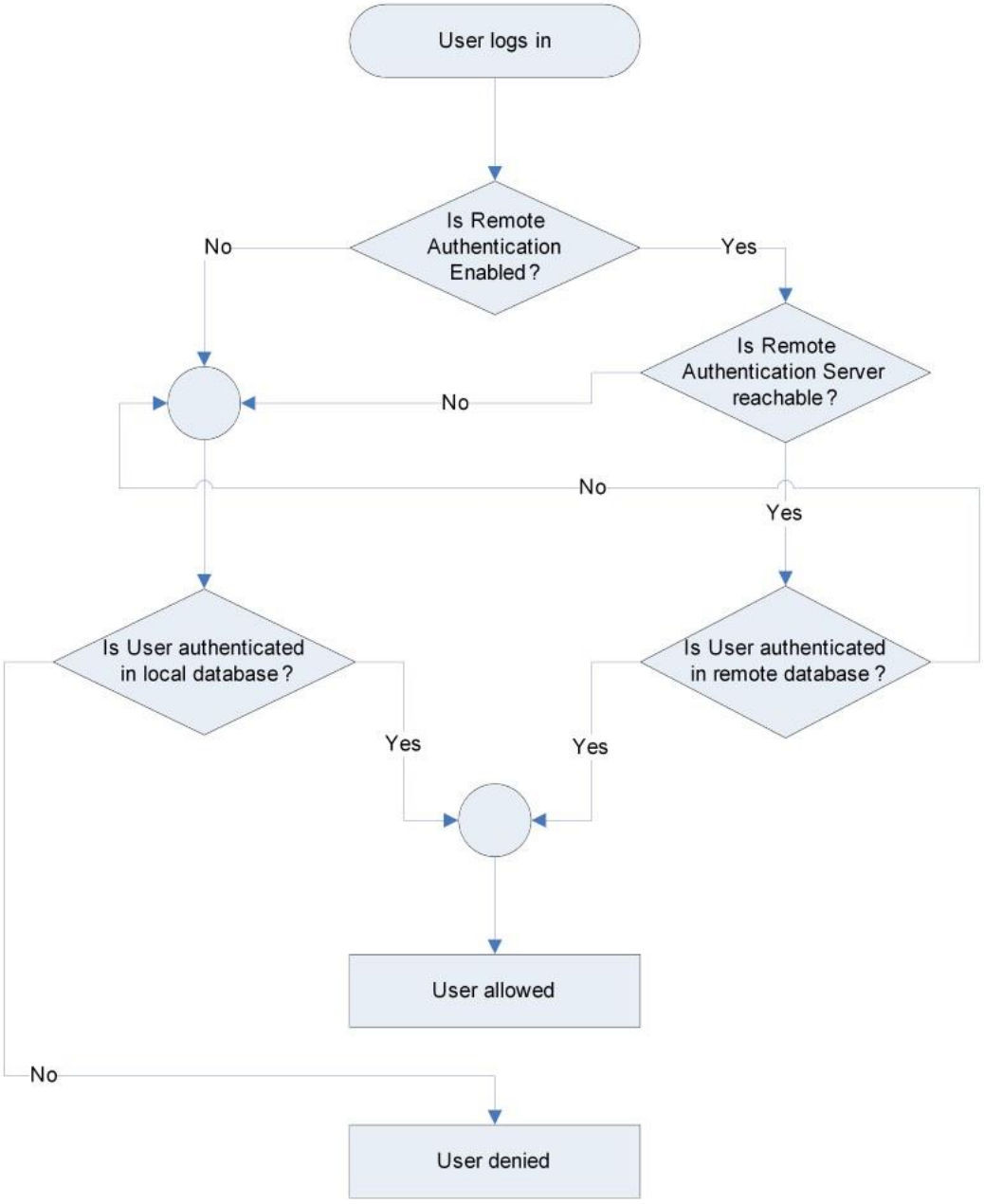
KX III 把下列 RADIUS 属性发送到 RADIUS 服务器：

属性	数据
登录	
Access-Request (1)	
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-IP-Address (4)	KX III 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。
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 III 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。
退出	
Accounting-Request(4)	

属性	数据
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 III 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

远程验证流程如下图所示：

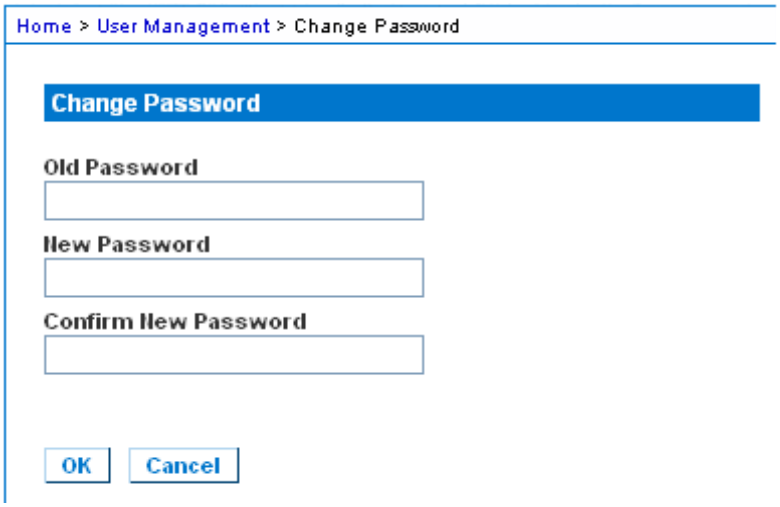


更改密码

更改你的 KX III 密码：

1. 选择“用户管理”(User Management) >“更改密码”(Change Password)。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）。
5. 在成功更改密码之后，显示确认信息。单击 OK（确定）。

*注意：如果使用的是强密码，则此页将显示关于这种密码所要求格式的信息。如要进一步了解密码和强密码，在联机帮助中参看***强密码** *(p. 152)*。



设备管理

网络配置

用 Network Settings（网络设置）页定制 KX III 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 III 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. 77)。
3. 更新 LAN Interface Settings（LAN 接口设置）。参看 ***LAN 接口设置*** (p. 81)。
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*** (参看 "***网络配置***" p. 77)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 III 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 III 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 III 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。

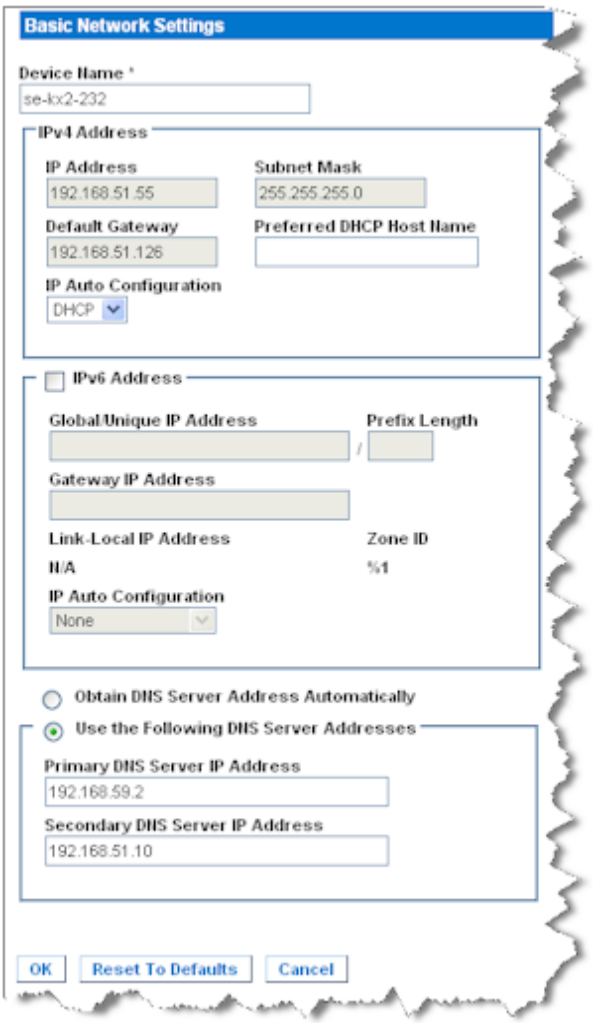
   a. Primary DNS Server IP Address（主 DNS 服务器 IP 地址）

   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. 81)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 III LAN Interface Speed & Duplex（KX III 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*** (参看 "**网络配置**" p. 77)页了解详情。*



Raritan.

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。

1. 选择“设备设置”(Device Settings) >“网络”(Network)。打开 Network Settings（网络设置）页面。
2. 在下列选项上选择 LAN Interface Speed 和 Duplex（LAN 接口速度和双工）：
   - Autodetect（自动检测，默认选项）
   - 10 Mbps/Half（10 Mbps/半双工）— 两个 LED 指示灯闪烁
   - 10 Mbps/Full（10 Mbps/全双工）— 两个 LED 指示灯闪烁
   - 100 Mbps/Half（100 Mbps/半双工）— 黄色 LED 指示灯闪烁
   - 100 Mbps/Full（100 Mbps/全双工）— 黄色 LED 指示灯闪烁
   - 1000 Mbps/Full（1000 Mbps/全双工）(Gigabit) — 绿色 LED 指示灯闪烁
   - 半双工提供双向通信，但每次只允许一个方向通信，不允许两个方向同时通信。
   - 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设置。

   参看***网络速度设置*** (p. 300)了解详情。
3. 选择 Enable Automatic Failover（启用自动故障切换）复选框，允许 KX III 在活动网络端口发生故障时，自动用备用网络端口恢复网络连接。

   注意：由于只有在实际发生故障之后才激活故障切换端口，所以 Raritan 建议你不要监视故障切换端口，或者只有在发生故障切换之后才监视此端口。

   在启用此选项之后，使用下列两个字段：
   - Ping Interval (seconds)（Ping 间隔时间[秒]）— ping 间隔时间决定 KX III 多久检查一次至指定网关的网络路径的状态。默认 ping 间隔时间是 30 秒。
   - Timeout (seconds)（超时[秒]）— 超时决定在进行故障切换之前，指定网关在多长时间内不能通过网络连接访问。

注意：可以根据本地网络的情况，配置最佳 ping 间隔时间和超时。在设置超时时，应该考虑到至少要发送两个或多个 ping 请求并返回响应。例如假如网络利用率很高，频繁进行故障切换，超时值应该是 ping 间隔时间的 3-4 倍。

4. 选择带宽。
5. 单击 OK（确定）按钮应用 LAN 设置。

配置端口

访问 Port Configuration（端口配置）页

访问端口配置：

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

   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。

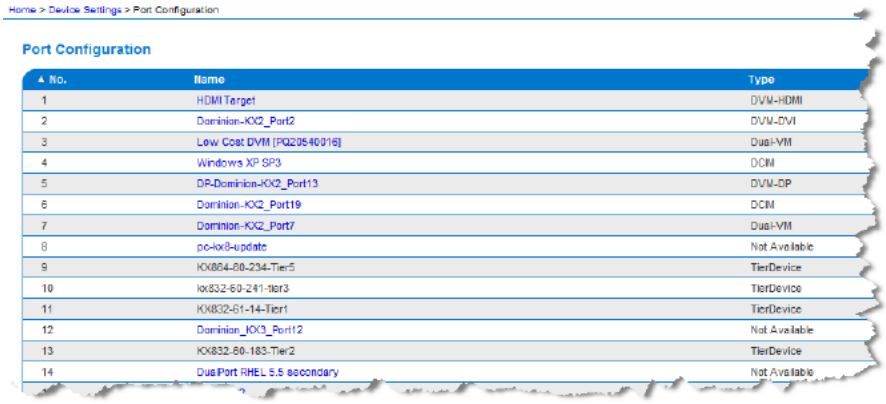
2. 单击要编辑的端口的端口名称。
   - 对于 KVM 端口，打开 KVM Port（端口）页和刀片服务器机箱。
   - 对于机架式 PDU，打开机架式 PDU（电源条）Port（端口）页。可以在本页上命名机架式 PDU 及其出口。

“端口配置”页

Port Configuration（端口配置）页显示 KX III 端口列表。

在端口状态为停机时，其状态显示 Not Available（不可用）。在取出端口上的 CIM 或停电时，端口可能停机。

注意：对于刀片服务器机箱，可以更改刀片服务器机箱名称，但不能更改刀片服务器插槽名称。



Port Number（端口号）

从 1 到 KX III 设备的总端口数进行编号。

Port Name（端口名称）

对于没有插入 CIM 的端口或 CIM 名称为空白的端口，指定默认端口名称 ，其中 Port# 是 KX III 物理端口编号。

还可以重新命名目前没有连接 CIM 的 KX III 的端口，把它的状态设置为不可用。

执行下列其中一个操作重新命名端口并把它的状态设置为不可用：

- 重新命名端口。在连接 CIM 时，将使用此 CIM 名称。
- 重新命名端口，选择 Persist name on Next CIM Insertion（在下次插入 CIM 时保留名称）选项。在连接 CIM 时，把给此 CIM 指定的名称复制到此 CIM 里。
- 选择 Reset to Defaults（复位到默认设置）选项，把端口（包括名称）复位到出厂默认设置。在连接 CIM 时，将使用此 CIM 名称。

注意：不要在端口 (CIM) 名称中使用撇号。

在重新命名端口之后，随时可以按 Reset to Default（复位到默认设置）按钮让它恢复到默认端口名称。

在把端口名称恢复到默认名称时，删除现有的任何电源关联，如果端口是一个端口组的成员，同时把它从此端口组删除掉。

Port type（端口类型）

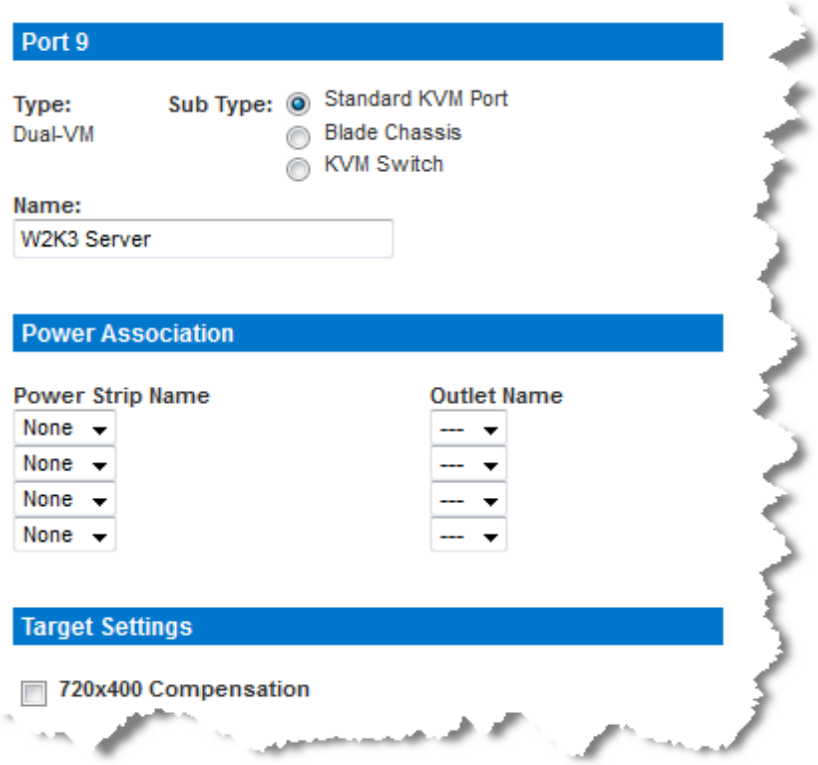
Port type（端口类型）包括：

- DCIM — Dominion CIM
- TierDevice - 级联设备
- Not Available（不可用）— 没有插 CIM
- DVM-DP — 显示端口 CIM
- DVM-HDMI - HDMI CIMsws'
- DVM-DVI — DVI CIM
- PowerStrip（机架式 PDU）— 相连的电源条
- VM - D2CIM - VUSB CIM
- Dual - VM - D2CIM-DVUSB CIM
- Blade Chassis（刀片服务器机箱）— 刀片服务器机箱和与机箱关联的刀片服务器（按分层顺序显示）
- KVM Switch（KVM 切换器）— 通用 KVM 切换器连接
- PCIM — Paragon CIM

配置标准目标服务器

命名目标服务器：

1. 连接所有目标服务器（如果尚未连接）。参看第三步：连接设备，了解如何连接设备。
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. 单击要重新命名的目标服务器的 Port Name（端口名称）。打开 Port（端口）页。
4. 选择“标准 KVM 端口”作为端口子类型。
5. 给连接此端口的服务器指定一个名称。名称最长为 32 个字符，可以使用字母数字字符和特殊字符。
6. 单击 OK（确定）。



配置 KVM 切换器

KX III 还支持用热键切换目标服务器。除了用热键切换标准服务器，刀片服务器机箱和分层配置还支持 KVM 切换。

重要说明：为了让用户组看到你创建的 KVM 切换器，必须先创建切换器，再创建用户组。如果现有用户组需要看到你即将创建的 KVM 切换器，必须重新创建此用户组。

配置 KVM 切换器：

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. 单击要重新命名的目标服务器的端口名称，打开 Port（端口）页。
3. 选择 KVM 切换器。
4. 选择 KVM 切换器型号。

   注意：下拉列表只显示一台切换器。
5. 选择 KVM 切换热键。
6. 输入最大目标端口号 (2-32)。
7. 在 KVM Switch Name（KVM 切换器名称）字段里输入此端口连接的名称。
8. 激活 KVM 切换热键要应用的目标服务器。选择每个端口对应的 Active（活动）复选框，说明这些端口连接了目标服务器。
9. 可以在本页的 KVM 管理链接部分配置至可用的网络浏览器接口的连接。
   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动）复选框，仍然可以在链接字段里输入并保存信息。在选择 Active（活动）复选框之后，必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。
   b. URL Name（URL 名称）— 输入接口 URL。
   c. Username（用户名）— 输入访问接口所用的用户名。
   d. Password（密码） — 输入访问接口所用的密码。
   e. Username（用户名）字段 — 输入要在 URL 中使用的用户名参数。例如 *username*=admin，其中 *username* 是用户名字段。
   f. Password（密码）字段 — 输入要在 URL 中使用的密码参数。例如 *password*=raritan，其中 *password* 是密码字段。

10. 单击 OK（确定）按钮。

更改 KVM 切换器端口或 URL 的活动状态：

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. 单击要重新命名的目标服务器的端口名称，打开 Port（端口）页。
3. 取消 KVM 切换器目标端口或 URL 旁边的 Active（活动）复选框更改其活动状态。
4. 单击 OK（确定）按钮。

配置 CIM 端口

KX III 支持用标准 CIM 和数字 CIM 把服务器连接到 KX III。

配置 CIM：

1. 选择“设备设置”(Device Settings) >“端口配置”(Port Configuration)。打开 Port Configuration（端口配置）页。
2. 单击要重新命名的目标服务器的 Port Name（端口名称）。打开 Port（端口）页。
3. 选择“标准 KVM 端口”作为端口子类型。
4. 给连接此端口的服务器指定一个名称。名称最长为 32 个字符，可以使用字母数字字符和特殊字符。
5. 必要时在 Power Association（电源关联）部分使一个电源条与此出口关联。
6. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。
7. 对于数字 CIM，在 Display Native Resolution（本机显示分辨率）下拉列表上选择视频分辨率，设置与你的监视器的本机显示分辨率相同的目标服务器分辨率。

   如果使用 HDMI CIM，某些操作系统/显示卡组合可能会限制 RGB 值范围。选择 DVI Compatibility Mode（DVI 兼容模式）复选框提高色彩质量。
8. 单击 OK（确定）。

配置机架式 PDU（电源条）目标

可以利用 KX III 把机架式 PDU（电源条）连接到 KX III 端口。

在 KX III Port Configuration（端口配置）页上配置 KX III 机架式 PDU。

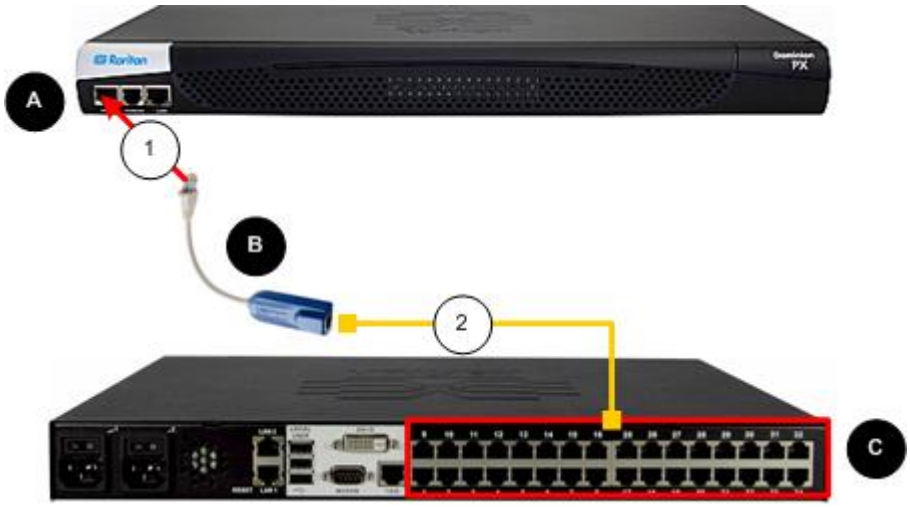
注意：Raritan 建议每次不超过八 (8) 个机架 PUD(电源条) 连接在 KX III 上，否则性能可能受到影响。

连接机架式 PDU

用 D2CIM-PWR CIM 把 Raritan PX 系列机架式 PDU（电源条）连接到 Dominion 设备。

▶ **连接机架式 PDU：**

1. 把 D2CIM-PWR 的 RJ-45 连接器（公头）插入机架式 PDU 串行端口上的 RJ-45 连接器（母头）。
2. 用直通 Cat5 电缆将 D2CIM-PWR 的 RJ-45 连接器（阴）连接到 KX III 的任何一个可用系统端口连接器（阴）。
3. 用交流电源线连接目标服务器和可用的机架式 PDU 出口。
4. 把 PDU 连接到交流电源。
5. 接通设备电源。



图示符号	
A	有串行端口的 PX 机架 PDU

B	D2CIM-PWR
C	KX III
1	D2CIM-PWR 至机架 PDU 串行端口连接
2	通过 Cat5 电缆，D2CIM-PWR 至 KX III 目标服务器端口

命名机架式 PDU（电源条端口页）

注意：可以在 PX 和 KX III 上命名 PX 机架式 PDU（电源条）。

在把 Raritan 远程机架式 PDU 连接到 KX III 之后， Port Configuration（端口配置）页显示此 PDU。单击页面上的电源端口名称访问它。自动填充 Type（类型）字段和 Name（名称）字段。

注意：不能更改 CIM 类型。

显示机架 PDU 上每个出口的下列信息：[Outlet（出口）] Number（编号）、Name（名称）和 Port Association（端口关联）。

在本页上命名机架式 PDU 及其接口。名称最长为 32 个字母数字字符，可以包含特殊字符。

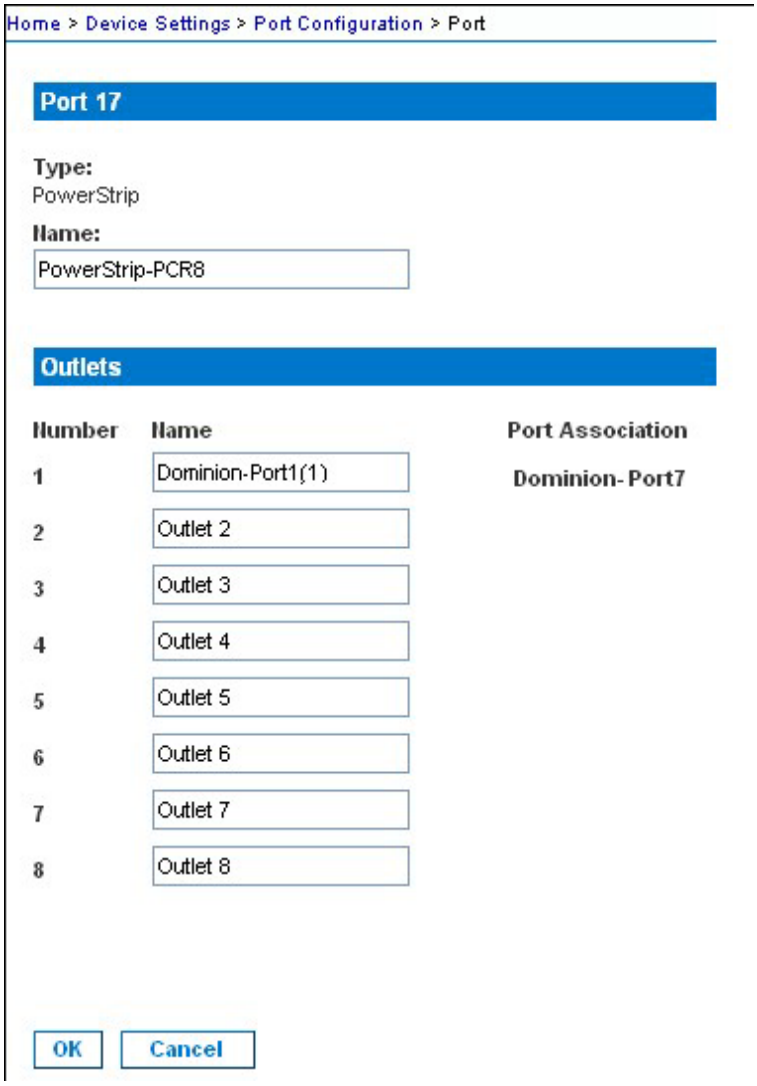
注意：在使机架式 PDU 与目标服务器（端口）关联时，用目标服务器名称取代出口名称（即使给此出口指定了其他名称也如此）。

命名机架式 PDU 和出口：

注意：CommandCenter Service Gateway 不能识别包含空格的机架式 PDU 名称。

1. 在 Name（名称）字段里输入机架式 PDU 的名称（如有必要）。
2. 根据需要更改 [Outlet（出口）] Name（名称）。（出口名称默认为 outlet #。）

3. 单击 OK（确定）。


Home > Device Settings > Port Configuration > Port
Port 17
Type:
PowerStrip
Name:
PowerStrip-PCR8
Outlets
Number
Name
Port Association
1
Dominion-Port1(1)
Dominion- Port7
2
Outlet 2
3
Outlet 3
4
Outlet 4
5
Outlet 5
6
Outlet 6
7
Outlet 7
8
Outlet 8
OK
Cancel

使出口与目标服务器关联

单击 Port Configuration（端口配置）页上的一个端口，打开 Port（端口）页。

如果出口被连接到与端口相连的相同服务器，可以与目标服务器产生电源关联。

一台服务器最多可以有四个电源插头，可以使每个电源插头与不同的机架式 PDU（电源条）关联。可以在本页上定义这些关联，以便在 Port Access（端口访问）页上对服务器执行通电、断电和重新通电操作。

为了使用此功能，你需要：

- Raritan 远程机架式 PDU
- 电源 CIM (D2CIM-PWR)

创建电源关联

▶ **创建电源关联（使机架式 PDU 出口与 KVM 目标服务器关联）：**

注意：在使机架式 PDU 与目标服务器（端口）关联时，用目标服务器名称取代出口名称（即使给此出口指定了其他名称也如此）。

1. 在端口配置页面，选择你要与 PDU 关联的目标服务器。
2. 在 Power Strip Name（电源条名称）下拉列表上选择机架式 PDU。
3. 在 Outlet Name（出口名称）下拉列表上选择此机架式 PDU 的出口。
4. 对于所有期望的电源关联，重复第一步和第二步。
5. 单击 OK（确定）。显示一条确认消息。

删除电源关联

在把目标服务器和/或机架式 PDU 与设备断开时，应该先删除所有电源关联。如果在目标服务器与机架式 PDU 关联的情况下把目标服务器从设备上删除掉，电源关联仍然存在。在这种情况下，在 Device Settings（设置设置）页上不能访问被断开的目标服务器对应的 Port Configuration（端口配置）页，所以不能正常删除电源关联。

▶ **删除机架式 PDU 关联：**

1. 在 Power Strip Name（电源条名称）下拉列表上选择相应的机架式 PDU。
2. 在 Outlet Name（出口名称）下拉列表上选择此机架式 PDU 的相应出口。
3. 在 Outlet Name（出口名称）下拉列表上选择 None（无）。
4. 单击 OK（确定）。删除机架式 PDU/出口关联，并显示一条确认消息。

在把机架式 PDU 从目标服务器上删除之后删除机架式 PDU 关联：

1. 单击 Device Settings（设备设置）> Port Configuration（端口配置），然后单击活动目标服务器。
2. 使活动目标服务器与被断开的电源端口关联。这将删除被断开的目标服务器的电源关联。
3. 最终使活动目标服务器与正确的电源端口关联。

配置刀片服务器机箱

除了标准服务器和机架式 PDU（电源条），还可以控制与 KX III 设备端口相连的刀片服务器机箱。每次最多可以管理八个刀片服务器机箱。

如果刀片服务器机箱类型是支持的类型，在连接刀片服务器机箱之后自动检测机箱。

在检测到刀片机箱时，给它指定一个默认名称，Port Access（端口访问）页显示此刀片服务器机箱、标准目标服务器和机架式 PDU。

如果刀片服务器机箱类型不是支持的类型，必须人工配置刀片服务器。必须把刀片服务器机箱配置为刀片服务器机箱子型号。

参看*端口访问页（**Remote Console** 显示）* (p. 17)了解详情。

刀片服务器机箱配置选项

除了 HP 刀片服务器机箱和 Cisco® UCS 刀片服务器机箱，可以在 Port（端口）页上配置通用刀片服务器机箱、IBM® 刀片服务器机箱和 Dell® 刀片服务器机箱。

必须给与刀片服务器机箱相连的端口配置刀片服务器机箱型号。

可以给刀片服务器配置的具体信息，取决于你使用的刀片服务器品牌。如要具体了解每种支持的刀片服务器机箱，参看本节中相应的主题。

Dell

- Dell PowerEdge® 1855、1955 和 M1000e

  Dell PowerEdge 1855/1955 刀片服务器还允许你让每个刀片服务器连接 Dominion 设备的一个端口。在采用这种方法连接时，还可以将它们组合在一起创建刀片服务器组。

IBM

- IBM BladeCenter® Model E 和 H

Generic

- Generic（通用）选项允许你配置不是 Dell PowerEdge® 1855、1955 和 M1000e、IBM BladeCenter® Models E 和 H、HP BladeSystem c3000 和 c7000，或 Cisco UCS 刀片服务器的刀片机箱。

HP

- 通过从 Dominion 设备到每个刀片服务器机箱的个别连接，支持 HP BladeSystem c3000/c7000 和 Cisco UCS 刀片服务器。

  用 Port Group Management（端口组）功能将端口组合成一个机箱。

人工和自动发现刀片服务器机箱配置

刀片服务器机箱有两种工作模式：人工配置和自动发现，视刀片服务器机箱的功能而定。

如果给刀片服务器机箱配置了自动发现，Dominion 设备跟踪并更新下列各项：

- 何时把新刀片服务器添加到刀片服务器机箱。
- 何时把现有刀片服务器从刀片服务器机箱中删除掉。

注意：在使用 IBM BladeCenter E 型和 H 型的情况下，KX III 只自动发现作为主管理模块的 AMM[1]。

热键组合访问刀片机箱

还支持用热键切换 KVM 访问刀片服务器机箱。

对于那些支持用户选择热键的刀片服务器机箱，Port Configuration（端口配置）页将显示这些热键选项。

对于有预定义热键的刀片服务器机箱，在选择刀片服务器机箱之后，Port Configuration（端口配置）页自动填充这些热键。

例如将 KVM 访问切换到 IBM BladeCenter H 的默认热键是 NumLock+NumLock+SlotNumber，所以在配置过程中选择 IBM BladeCenter H 时，默认应用此热键。参看刀片服务器文档，详细了解热键。

连接到刀片服务器机箱接口

如果有可用的刀片服务器机箱网络浏览器接口，可以配置至刀片服务器机箱网络浏览器接口的连接。在机箱一级，最多可以定义四个连接。

第一个连接保留用于连接刀片服务器机箱管理模块 GUI，

例如技术支持人员可以用此连接迅速确定机箱配置。

管理刀片服务器机箱

刀片服务器机箱可以用 Virtual KVM Client (VKC)、Active KVM Client (AKC)、和 CC-SG 管理。

通过 VKC 和 AKC 管理刀片服务器的方法与管理标准目标服务器的方法相同。

参看用户帮助和 **CC-SG 管理员指南**了解详情。

注意：对刀片服务器机箱进行的任何更改，将传递到这些客户机应用程序。

重要说明：在断开刀片服务器机箱和 Dominion 设备之间的 CIM 的电源时，或者断开 CIM 和 Dominion 设备连接时，关闭此前建立的至此刀片服务器机箱的所有连接。在重新连接 CIM 或给它通电时，必须重新建立连接。

通用刀片服务器机箱配置

Generic Blade Chassis（通用刀片服务器机箱）选择只提供人工配置操作模式。 参看***支持的刀片服务器机箱型号*** (p. 107)、***支持的刀片服务器机箱 CIM*** (参看 "***刀片服务器机箱支持的 CIM***" p. 107) 和***要求和建议的刀片服务器机箱配置*** (p. 110)了解在配置刀片服务器机箱时所需的其他重要信息。参看 ***Dell 机箱电缆长度和视频分辨率*** (p. 302)了解在与 KX III 一起使用 Dell® 机箱时的电缆长度和视频分辨率。

配置机箱：

1. 将刀片服务器连接到 KX III。参看第三步：连接设备了解详情。
2. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
3. 在 Port Configuration（端口配置）页上单击要配置的刀片服务器机箱的名称。打开 Port（端口）页。
4. 选择 Blade Chassis（刀片服务器机箱）单选按钮。本页显示配置刀片服务器机箱所需的字段。
5. 在 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表上选择 Generic（通用）。
6. 适当配置刀片服务器机箱。
   a. Switch Hot Key Sequence（切换热键）— 定义从 KVM 切换到刀片服务器机箱所用的热键。Switch Hot Key Sequence（切换热键）必须匹配刀片服务器机箱上的 KVM 模块使用的热键。
   b. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 不适用。

c. Maximum Number of Slots（最大插槽数）— 输入刀片服务器机箱可用的默认最大插槽数。

d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。 不适用。

e. Username（用户名）— 不适用。

f. Password（密码）— 不适用。

7. 必要时更改刀片服务器机箱名称。

8. 选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。

9. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 

展开本页的这个部分。

第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

---

a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。

b. URL — 输入接口 URL。 **要求**

c. Username（用户名）— 输入访问接口所用的用户名。 **任选**

d. Password（密码）— 输入访问接口所用的密码。 **任选**

注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

---

e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 103)，了解如何添加 Web 浏览器界面。 **任选**

10. USB 配置文件信息不应用于通用配置。

11. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。

12. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。

在 Display Native Resolution（本机显示分辨率）下拉列表上选择 CIM 本机显示分辨率。这 是数字 CIM 的首选分辨率和定时模式。在选择分辨率之后，把分辨率应用于 CIM。

1. 如果不选择分辨率，默认使用 1024x1280@60Hz 分辨率。
2. 单击 OK（确定）按钮保存配置。

Dell 刀片服务器机箱配置

参看***支持的刀片服务器机箱型号*** (p. 107)、***支持的刀片服务器机箱 CIM*** (参看 "***刀片服务器机箱支持的 CIM***" p. 107) 和***要求和建议的刀片服务器机箱配置*** (p. 110)了解在配置刀片服务器机箱时所需的其他重要信息。参看 ***Dell 机箱电缆长度和视频分辨率*** (p. 302)了解在与 KX III 一起使用 Dell® 机箱时的电缆长度和视频分辨率。

添加刀片服务器机箱：

1. 将刀片服务器连接到 KX III。参看第三步：连接设备了解详情。
2. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
3. 在 Port Configuration（端口配置）页上单击要配置的刀片服务器机箱的名称。打开 Port（端口）页。
4. 选择 Blade Chassis（刀片服务器机箱）单选按钮。本页显示配置刀片服务器机箱所需的字段。
5. 在 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表上选择 Dell 刀片服务器机箱型号。

配置 Dell PowerEdge M1000e：

1. 如果选择了 Dell PowerEdge™ M1000e，可以使用自动发现。适当配置刀片服务器机箱。 在配置可自动发现的刀片服务器机箱之前，必须先配置它允许通过指定端口号进行 SSH 通信（参看设备服务）。此外，此前必须在刀片服务器机箱上创建了一个用户帐号，该用户帐号有相应的验证证书。
   a. Switch Hot Key Sequence（切换热键）— 选择从 KVM 切换到刀片服务器所用的热键。 Switch Hot Key Sequence（切换热键）必须匹配刀片服务器机箱上的 KVM 模块使用的热键。
   b. Maximum Number of Slots（最大插槽数）— 自动输入刀片服务器机箱可用的默认最大插槽数。

c. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 输入刀片服务器机箱的主 IP 地址。 **自动发现模式需要此设置**

d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。必要时更改端口号。 **自动发现模式需要此设置**

e. Username（用户名）— 输入访问刀片服务器机箱所用的用户名。**自动发现模式需要此设置**

f. Password（密码）— 输入访问刀片服务器机箱所用的密码。 **自动发现模式需要此设置**

2. 如果希望 KX III 自动发现机箱上的刀片服务器，选择 Blade Auto-Discovery（刀片服务器自动发现）复选框，然后单击 Discover Blades on Chassis Now（现在发现机箱上的刀片服务器）按钮。本页显示发现的刀片服务器。

3. 必要时更改刀片服务器机箱名称。如果机箱已经命名了，此字段自动填充机箱名称。如果机箱尚未命名，KX III 给机箱指定一个名称。KX III 的默认刀片服务器机箱命名常规是 Blade_Chassis_Port#。

4. 如果在 Manual（人工）模式下操作，选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。

   如果在 Auto-discovery（自动发现）模式下操作，Installed（已安装）字段在发现过程中显示安装了刀片服务器的插槽。

5. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 ► Blade Chassis Managed Links 展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

   注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

   ---

   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。

   b. URL — 输入接口 URL。 参看*刀片服务器机箱 URL 格式例子* (p. 111)，了解 Dell M1000e 配置例子。

   c. Username（用户名）— 输入访问接口所用的用户名。

   d. Password（密码）— 输入访问接口所用的密码。

注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 103)，了解如何添加 Web 浏览器界面。

6. USB 配置文件不应用于 Dell 机箱。
7. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。
8. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。

在 Display Native Resolution（本机显示分辨率）下拉列表上选择 CIM 本机显示分辨率。这 是数字 CIM 的首选分辨率和定时模式。在选择分辨率之后，把分辨率应用于 CIM。

1. 如果不选择分辨率，默认使用 1024x1280@60Hz 分辨率。
2. 单击 OK（确定）按钮保存配置。

配置 Dell PowerEdge 1855/1955：

1. 如果选择了 Dell PowerEdge 1855/1955，*不能使用*自动发现。适当配置刀片服务器机箱。
   a. Switch Hot Key Sequence（切换热键）— 选择从 KVM 切换到刀片服务器所用的热键。 对于 Dell 1855/1955 型号，KX III 阻止所有现有热键组合。如果把 Generic（通用）配置应用于 Dell 1855，只阻止一个现有热键。
   b. Maximum Number of Slots（最大插槽数）— 自动输入刀片服务器机箱可用的默认最大插槽数。
   c. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 不适用。
   d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。 不适用。
   e. Username（用户名）— 不适用。
   f. Password（密码）— 不适用。
2. 必要时更改刀片服务器机箱名称。

3. 选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。
4. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 

展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

   注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

   ---

   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。
   b. URL — 输入接口 URL。 参看刀片服务器机箱 URL 格式示例了解 Dell PowerEdge 1855/1955 配置示例。
   c. Username（用户名）— 输入访问接口所用的用户名。
   d. Password（密码）— 输入访问接口所用的密码。

   注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

   ---

   e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 103)，了解如何添加 Web 浏览器界面。
5. USB 配置文件不应用于 Dell 机箱。
6. 单击 OK（确定）按钮保存配置。

IBM 刀片服务器机箱配置

参看*支持的刀片服务器机箱型号* (p. 107)、*支持的刀片服务器机箱 **CIM*** (参看 "*刀片服务器机箱支持的 **CIM***" p. 107) 和*要求和建议的刀片服务器机箱配置* (p. 110)了解在配置刀片服务器机箱时所需的其他重要信息。参看 ***Dell 机箱电缆长度和视频分辨率*** (p. 302)了解在与 KX III 一起使用 Dell® 机箱时的电缆长度和视频分辨率。

添加刀片服务器机箱：

1. 将刀片服务器连接到 KX III。参看第三步：连接设备了解详情。
2. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
3. 在 Port Configuration（端口配置）页上单击要配置的刀片服务器机箱的名称。打开 Port（端口）页。
4. 选择 Blade Chassis（刀片服务器机箱）单选按钮。本页显示配置刀片服务器机箱所需的字段。
5. 在 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表上选择 IBM® 刀片服务器机箱型号。

配置 IBM BladeCenter H 和 E：

1. 如果选择了 IBM BladeCenter® H 或 E，可以使用自动发现。适当配置刀片服务器机箱。 在配置可自动发现的刀片服务器机箱之前，必须先配置它允许通过指定端口号进行 SSH 通信（参看设备服务）。此外，此前必须在刀片服务器机箱上创建了一个用户帐号，该用户帐号有相应的验证证书。 KX III 只支持 AMM[1] 自动发现。
   a. Switch Hot Key Sequence（切换热键）— 预定义。
   b. Maximum Number of Slots（最大插槽数）— 自动输入刀片服务器机箱可用的默认最大插槽数。
   c. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 输入刀片服务器机箱的主 IP 地址。 **自动发现模式需要此设置**
   d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。必要时更改端口号。 **自动发现模式需要此设置**
   e. Username（用户名）— 输入访问刀片服务器机箱所用的用户名。**自动发现模式需要此设置**
   f. Password（密码）— 输入访问刀片服务器机箱所用的密码。 **自动发现模式需要此设置**

2. 如果希望 KX III 自动发现机箱上的刀片服务器，选择 Blade Auto-Discovery（刀片服务器自动发现）复选框，然后单击 Discover Blades on Chassis Now（现在发现机箱上的刀片服务器）按钮。本页显示发现的刀片服务器。
3. 必要时更改刀片服务器机箱名称。如果机箱已经命名了，此字段自动填充机箱名称。如果机箱尚未命名，KX III 给机箱指定一个名称。KX III 的默认刀片服务器机箱命名常规是 Blade_Chassis_Port#。
4. 如果在 Manual（人工）模式下操作，选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。

   如果在 Auto-discovery（自动发现）模式下操作，Installed（已安装）字段在发现过程中显示安装了刀片服务器的插槽。
5. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 

展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

   注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

   ---

   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。
   b. URL — 输入接口 URL。参看***刀片服务器机箱 URL 格式例子*** (p. 111)，了解 IBM BladeCenter 配置例子。
   c. Username（用户名）— 输入访问接口所用的用户名。
   d. Password（密码）— 输入访问接口所用的密码。

   注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

   ---

   e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 103)，了解如何添加 Web 浏览器界面。

6. 必要时给刀片服务器机箱定义 USB 配置文件，或者选择现有的 USB 配置文件。单击 USB Profiles（USB 配置文件）-> Select USB Profiles for Port（给端口选择 USB 配置文件）图标 

或 Apply（应用）-> Select Profiles to Other Ports（给其他端口选择配置文件）图标 

，展开本页的这些部分。参看 ***配置 USB 配置文件（端口页）*** (p. 113)。
7. 单击 OK（确定）按钮保存配置。

配置 IBM BladeCenter（其他）：

1. 如果选择了 IBM BladeCenter（其他），*不能使用*自动发现。适当配置刀片服务器机箱。
   a. Switch Hot Key Sequence（切换热键）— 选择从 KVM 切换到刀片服务器所用的热键。
   b. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 输入刀片服务器机箱的主 IP 地址。 不适用。
   c. Maximum Number of Slots（最大插槽数）— 输入刀片服务器机箱可用的默认最大插槽数。
   d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。 不适用。
   e. Username（用户名）— 不适用。
   f. Password（密码）— 不适用。
2. 必要时更改刀片服务器机箱名称。
3. 选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。如果刀片服务器尚未命名，KX III 给刀片服务器指定一个名称。默认刀片服务器命名常规是 Blade_Chassis_Port#_Slot#。
4. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 

展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

---

a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。

b. URL — 输入接口 URL。参看*刀片服务器机箱 URL 格式例子* (p. 111)，了解 IBM BladeCenter 配置例子。

c. Username（用户名）— 输入访问接口所用的用户名。

d. Password（密码）— 输入访问接口所用的密码。

注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

---

e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看*添加网络浏览器界面注意事项* (p. 103)，了解如何添加 Web 浏览器界面。

5. IBM（其他）配置不使用 USB 配置文件。
6. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。
7. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。

在 Display Native Resolution（本机显示分辨率）下拉列表上选择 CIM 本机显示分辨率。这 是数字 CIM 的首选分辨率和定时模式。在选择分辨率之后，把分辨率应用于 CIM。

1. 如果不选择分辨率，默认使用 1024x1280@60Hz 分辨率。
2. 单击 OK（确定）按钮保存配置。

添加网络浏览器界面注意事项

可以添加一个网络浏览器界面，建立至使用嵌入 Web 服务器的设备的连接。也可以用网络浏览器界面连接任何 Web 应用程序，例如与 RSA、DRAC 或 ILO Processor 卡关联的 Web 应用程序。

必须配置 DNS，否则不解析 URL。如果输入 IP 地址，不必配置 DNS。

添加网络浏览器界面：

1. 输入 Web Browser Interface（网络浏览器界面）的默认名称。必要时更改 Name（名称）字段里的名称。

2. 在 URL 字段里输入 Web 应用程序的 URL 或域名。必须输入 Web 应用程序要读取的用户名和密码所在的 URL。

   使用下列正确格式：

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

3. 输入访问此界面所需的用户名和密码。**可选**
4. 如果输入用户名和密码，在 Username（用户名）字段和 Password（密码）字段里输入 Web 应用程序登录屏幕所用的用户名字段和密码字段的字段名称。必须查看登录屏幕的 HTML 源代码找到字段名称，而非字段标签。

查找字段名称注意事项：

- 在 Web 应用程序登录页面的 HTML 源代码里搜索字段标签，例如 Username 和 Password。
- 在找到字段标签之后，查看标签旁边类似下面这样的代码：name="user"。引号里面的单词就是字段名。

HP 和 Cisco UCS 刀片服务器机箱配置（端口组管理）

KX III 可以将与某些类型的刀片服务器相连的端口组合成一个组，表示刀片服务器机箱。尤其是在从每个刀片服务器将 Dell® PowerEdge™ 连接到一个 KX III 端口时，将 Cisco® UCS、HP® 刀片服务器和 Dell PowerEdge 1855/1955 刀片服务器组合在一起。

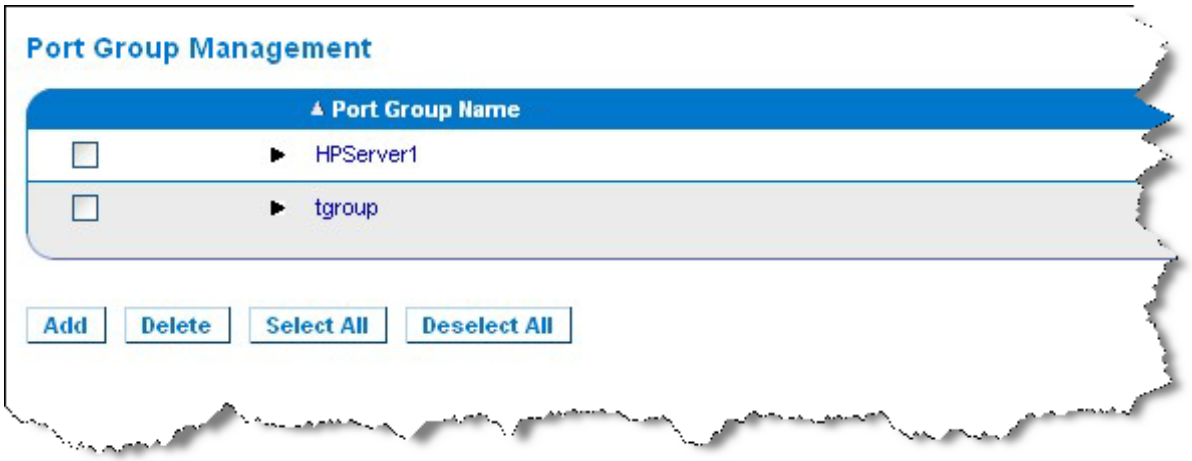
在 Port Group Management(端口组管理)页上，机箱用 Port Group Name（端口组名称）标识，组定义为 Blade Server Group（刀片服务器组）。Port Group（端口组）只包括作为标准 KVM 端口配置的端口，不包括作为刀片服务器机箱配置的端口。一个端口只能是一个组的成员。

与刀片服务器机箱上的集成 KVM 模块相连的端口配置为刀片服务器机箱子类型。这些端口可以包括在端口组里。

如果 KX III 端口连接刀片服务器机箱上的集成 KVM 模块，但不连接各个刀片服务器，这些端口配置为刀片服务器机箱子类型。这些端口不能包括在端口组里，Select Port for Group（给组选择端口）和 Available（可用）列表不显示它们。

如果将一个标准 KVM 端口包括在端口组里，然后将它重新配置为刀片服务器机箱子类型，必须先将它从端口组里删除掉。

Port Groups（端口组）用 Backup and Restore（备份和恢复）选项恢复（参看***备份和恢复*** (p. 169)）。



▶ 添加端口组：

1. 单击 Device Settings（设备设置）> Port Group Management（端口组管理），打开 Port Group Management（端口组管理）页。
2. 单击 Add（添加）按钮打开 Port Group（端口组）页。
3. 输入 Port Group Name（端口组名称）。端口组名称不区分大小写，最多 32 个字符。

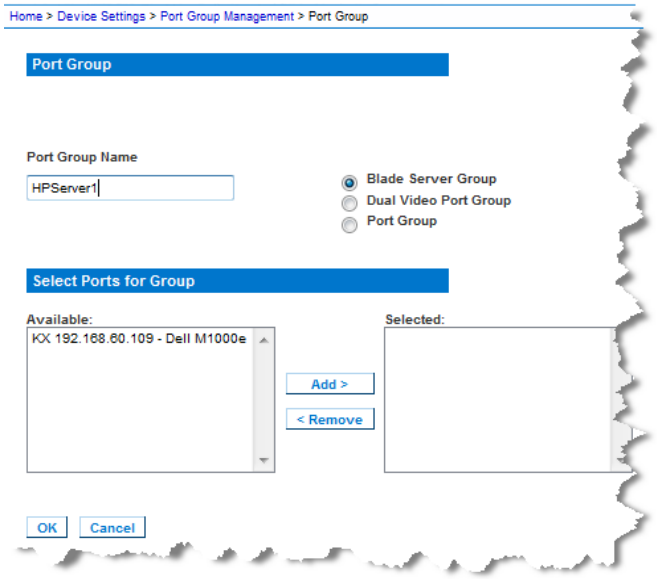
4. 选择 Blade Server Group（刀片服务器组）复选框。

   如果要指定将这些端口连接到刀片服务器机箱（例如 HP c3000 或 Dell PowerEdge 1855）上的刀片服务器，选择 Blade Server Group（刀片服务器组）复选框。

   注意：虽然每个刀片服务器连接一个 KX III 端口，但这对那些希望根据机箱组织管理 HP 刀片服务器的 CC-SG 用户来说尤其重要。

5. 在 Select Ports for Group（给组选择端口）部分，单击 Available（可用）字段里的一个端口。单击 Add（添加）按钮将该端口添加到组。该端口被移动到 Selected（已选择）字段。

6. 单击 OK（确定）按钮添加端口组。



编辑端口组信息：

1. 在 Port Group Management（端口组管理）页上单击要编辑的端口组的链接。打开 Port Group（端口组）页。
2. 根据需要编辑信息。
3. 单击 OK（确定）按钮保存更改。

删除端口组：

1. 在 Port Group Management（端口组管理）页上单击要删除的端口组对应的复选框。
2. 单击“删除”。
3. 单击确认消息上的 OK（确定）按钮。

支持的刀片服务器机箱型号

下表列出 KX III 支持的刀片服务器机箱型号，以及在 KX III 应用中配置机箱型号时应给它们选择的相应配置文件。如果选择了 Blade Chassis（刀片服务器机箱）单选按钮，显示 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表，可以在 Port Configuration（端口配置）页上选择这些型号的列表。如要详细了解如何配置每种刀片服务器机箱，参看本节中相应的主题。

刀片服务器机箱型号	KX III 配置文件
Cisco® UCS	用端口组管理功能配置。参看 ***HP 和 Cisco UCS 刀片服务器机箱配置（端口组管理）*** (p. 105)
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM（其他）
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM（其他）
IBM BladeCenter HT	IBM（其他）
IBM BladeCenter E	IBM BladeCenter E
HP®	用端口组管理功能配置。参看 ***HP 和 Cisco UCS 刀片服务器机箱配置（端口组管理）*** (p. 105)

刀片服务器机箱支持的 CIM

通过 KX III 管理的刀片服务器机箱支持下列 CIM：

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

下表列出 KX III 支持的每种刀片服务器机箱型号使用的 CIM。

刀片服务器机箱	连接方法	推荐的 CIM
Generic	如果在连接被配置为 Generic 的刀片服务器机箱时使用 D2CIM-VUSB 或 D2CIM-DVUSB，可以在 Port Configuration（端口配置）页和客户机的 USB Profile（USB 配置文件）菜单上选	• DCIM-PS2 • DCIM-USBG2

刀片服务器机箱	连接方法	推荐的 CIM
	择 USB 配置文件。但通用刀片服务器机箱不支持虚拟媒体，客户机禁用 Virtual Media（虚拟媒体）菜单。	
Cisco® UCS 服务器机箱	用 Cisco KVM 电缆 (N20-BKVM) 把音频设备和 USB 设备直接连接到刀片服务器上，可以执行刀片服务器管理、配置和诊断操作。 资料来源：*Cisco UCS 5108 服务器机箱安装指南*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB
Dell® PowerEdge™ 1855	包括下列三个 KVM 模块之一： • 模拟 KVM Ethernet 切换模块（标准） • 数字访问 KVM 切换模块（可选） • KVM 切换模块（在 2005 年 4 月之前销售的系统上是标准配置） 这些切换器配有定制插口，允许把两个 PS/2 设备和一台监视器连接到系统上。 资料来源：*Dell PowerEdge 1855 用户指南*	• DCIM-PS2
Dell PowerEdge 1955	可以安装两种 KVM 模块之一： • 模拟 KVM 切换模块 • 数字访问 KVM 切换模块 两个模块都允许你用随系统一并提供的定制电缆，把一个 PS/2 兼容键盘、一个鼠标和一台监视器连接到系统上。 资料来源：*Dell PowerEdge 1955 用户手册*	• DCIM-PS2
Dell PowerEdge M1000e	KVM 切换模块 (iKVM) 集成在此机箱上。 iKVM 兼容下列外设： • USB 键盘和 USB 鼠标 • 支持 DDC 的 VGA 监视器 资料来源：*Dell Chassis Management Controller, Firmware Version 1.0 用户指南*	• DCIM-USBG2
HP® BladeSystem c3000	HP c-Class 刀片服务器 SUV 电缆允许你直接把监视器和 USB 设备接到刀片服务器上，可以执行刀片服务器机箱管理、配置和诊断操作。 资料来源：*HP Proliant™ BL480c 刀片服务器维护和维修指南*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB（用于标准 KVM 端口操作，没有 KVM 选

刀片服务器机箱	连接方法	推荐的 CIM
		项）
HP BladeSystem c7000	HP c-Class 刀片服务器 SUV 电缆允许你直接把监视器和 USB 设备接到刀片服务器上，可以执行刀片服务器管理、配置和诊断操作。 资料来源：*HP ProLiant BL480c 刀片服务器维护和维修指南*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB（用于标准 KVM 端口操作）
IBM® BladeCenter® S	高级管理模块 (AMM) 给所有刀片服务器机箱提供系统管理功能和键盘/视频/鼠标 (KVM) 多路复用。 AMM 连接包括：一个串行端口、一个视频连接端口、一个远程管理端口 (Ethernet) 和两个 USB v2.0 端口（连接键盘和鼠标）。 资料来源：*实现 IBM BladeCenter S 机箱*	• DCIM-USBG2
IBM BladeCenter H	BladeCenter H 机箱标准配置一个高级管理模块。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	最新型 BladeCenter E 机箱 (8677-3Rx) 标准配置一个高级管理模块。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	BladeCenter T 机箱标准配置一个高级管理模块。 与标准 BladeCenter 机箱相比，BladeCenter T 机箱上的 KVM 模块和管理模块是分离部件。管理模块面板上只有 LED 指示灯显示其状态。所有 Ethernet 连接和 KVM 连接均通过背板连接 LAN 模块和 KVM 模块。 机箱背面的 KVM 模块是热交换模块，有两个 PS/2 插口连接键盘和鼠标，有一个系统状态显示板，有一个 HD-15 视频插口。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-PS2
IBM BladeCenter HT	BladeCenter HT 机箱标准配置一个高级管理模块。此模块具备机箱管理能力和本地 KVM 功能。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-USBG2

注意：为了支持自动发现，IBM BladeCenter Model H 和 E 必须使用固件版本为 BPET36K 或更高版本的 AMM。

注意：在使用 IBM BladeCenter E 型和 H 型的情况下，KX III 只自动发现作为主管理模块的 AMM[1]。

注意：对所有目标服务器禁用音频。

要求和建议的刀片服务器机箱配置

下表说明在配置刀片服务器机箱使用 KX III 时要考虑的限制和约束。Raritan 建议你采用下列所有信息。

刀片服务器机箱	要求/建议的操作
Dell® PowerEdge™ M1000e	▪ 禁用 iKVM GUI 屏幕保护。如果不这样做，将显示 Authorize（授权）对话框，iKVM 不能正常工作。 ▪ 退出 iKVM GUI 菜单，将 Dell 机箱连接到 Raritan CIM。 ▪ 配置 iKVM GUI 主菜单，按插槽或名称选择目标刀片服务器。如果不这样做，iKVM 可能无法正常工作。 ▪ *切勿*在 iKVM GUI Setup Scan（设置扫描）菜单上给任何插槽指定扫描操作，否则 iKVM 可能无法正常工作。 ▪ *切勿*在 iKVM GUI Setup Broadcast（设置广播）菜单上给任何插槽指定广播键盘/鼠标操作。如果不这样做，iKVM 可能无法正常工作。 ▪ 指定一个热键调用 iKVM GUI。此热键还必须在 KX III 端口配置过程中加以确认。否则在客户机上输入热键时，iKVM 可能会误操作。 ▪ 确保在用 Dell CMC GUI 配置 iKVM 过程中*不*选择 Front Panel USB/Video Enabled（启用面板 USB/视频）。否则，机箱面板上的连接的优先级高于背板上的 KX III 连接，致使 iKVM 不能正常工作。显示一条消息：由于面板当前处于活动状态，用户被禁用。 ▪ 确保在用 Dell CMC GUI 配置 iKVM 过程中*不*选择 Allow access to CMC CLI from iKVM（允许在 iKVM 上访问 CMC CLI）。 ▪ 如在连接刀片服务器机箱之后不显示 iKVM GUI，将 Screen Delay Time（屏幕延迟时间）设置为 8 秒。 ▪ 建议在 iKVM GUI Flag Setup（标志设置）过程中选择 Timed（定时）和 Displayed（显示）。这样，你可以直观确认至期望的刀片服务器插槽的连接。
Dell PowerEdge	▪ 禁用 iKVM GUI 屏幕保护。如果不这样做，将显示 Authorize（授

刀片服务器机箱	要求/建议的操作
1855/1955	权）对话框，iKVM 不能正常工作。 ▪ 退出 iKVM GUI 菜单，将 Dell 机箱连接到 Raritan CIM。 ▪ 配置 iKVM GUI 主菜单，按插槽或名称选择目标刀片服务器。如果不这样做，iKVM 可能无法正常工作。 ▪ *切勿*在 iKVM GUI Setup Scan（设置扫描）菜单上给任何插槽指定扫描操作，否则 iKVM 可能无法正常工作。 ▪ 如在连接刀片服务器机箱之后不显示 iKVM GUI，将 Screen Delay Time（屏幕延迟时间）设置为 8 秒。 ▪ 建议在 iKVM GUI Flag Setup（标志设置）过程中选择 Timed（定时）和 Displayed（显示）。这样，你可以直观确认至期望的刀片服务器插槽的连接。
IBM®/Dell® 自动发现	▪ 建议你在应用刀片服务器级访问权时，启用自动发现。否则，在刀片服务器机箱上设置访问权。 ▪ 必须在刀片服务器机箱管理模块上启用 Secure Shell (SSH)。 ▪ 在刀片服务器管理模块上配置的 SSH 端口必须与在 Port Configuration（端口配置）页上输入的端口号相同。
IBM KX3 虚拟媒体	▪ 只有 IBM BladeCenter® Models H 和 E 支持 Raritan KX III 虚拟媒体。要求使用 D2CIM-DVUSB。黑色 D2CIM-DVUSB 低速 USB 插头连接设备背板上的高级管理模块 (AMM)。灰色 D2CIM-DVUSB 高速 USB 插头连接设备面板上的媒体托盘 (Media Tray, MT)。要求使用 USB 延长电缆。
Cisco® UCS 服务器机箱	▪ 用 Cisco KVM 电缆 (N20-BKVM) 把音频设备和 USB 设备直接连接到刀片服务器上，可以执行刀片服务器管理、配置和诊断操作。 ▪ 资料来源：*Cisco UCS 5108 服务器机箱安装指南 — DCIM-USBG2 - D2CIM-VUSB - D2CIM-DVUSB*

注意：所有 IBM BladeCenter 必须使用固件版本为 BPET36K 或更高版本的 AMM，才能与 KX III 一起工作。

注意：在使用 IBM BladeCenter E 型和 H 型的情况下，KX III 只自动发现作为主管理模块的 AMM[1]。

刀片服务器机箱 URL 格式例子

下表举例说明在 KX III 上给刀片服务器机箱配置的 URL 格式。

刀片服务器机箱	URL 格式例子
Dell® M1000e	• URL：https://192.168.60.44/cgi-bin/webcgi/login • Username（用户名）： root

刀片服务器机箱	URL 格式例子
	• Username Field（用户名字段）：user • Password（密码）： calvin • Password Field（密码字段）： password
Dell 1855	• URL： https://192.168.60.33/Forms/f_login • Username（用户名）： root • Username Field（用户名字段）：TEXT_USER_NAME • Password（密码）： calvin • Password Field（密码字段）：TEXT_PASSWORD
IBM® BladeCenter® E 型和 H 型	• http://192.168.84.217/private/welcome.ssi

配置 USB 配置文件（端口页）

在 Port（端口）页的 Select USB Profiles for Port（给端口选择 USB 配置文件）部分给一个端口选择可用的 USB 配置文件。当 VKC 用户通过该端口连接 KVM 目标服务器时，可以使用在 Port（端口）页上选择的 USB 配置文件。默认的是 Windows 2000®操作系统、Windows XP®操作系统、Windows Vista®操作系统配置文件。参看 USB 配置文件了解 USB 配置文件。

---

*注意：为了给端口设置 USB 配置文件，必须把安装了兼容固件的 CIM、VM-CIM 或 Dual VM-CIM 连接到安装了最新版固件的 KX III。参看***升级 CIM** *(p. 172)*。

左边的 Available（可用）列表显示可以给端口指定的配置文件。右边的 Selected（已选择）列表显示给端口选择的配置文件。在任何一个列表上选择一个配置文件时，Profile Description（配置文件说明）字段显示该配置文件的说明和用途。

除了选择一组配置文件使它们可用于一个 KVM 端口，还可以给该端口指定首选配置文件，将这些设置应用于一个端口，而不应用于其他 KVM 端口。

---

*注意：如果使用 DCIM-VUSB 或 DCIM-DVUSB 虚拟媒体 CIM，参看***在使用 Mac Boot 菜单时的鼠标模式** *(参看 "***使用 Mac Boot Menu 时的鼠标模式***" p. 52)了解如何使用 Mac OS-X® USB 配置文件。*

▶ **打开端口页：**

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

▶ **给 KVM 端口选择 USB 配置文件：**

1. 在 Select USB Profiles for Port（给端口选择 USB 配置文件）部分的 Available（可用）列表上选择一个或多个 USB 配置文件。
   - 按住 Shift 单击选择几个连续配置文件。
   - 按住 Ctrl 单击选择几个不连续的配置文件。
2. 单击“添加”。Selected（已选择）列表显示选择的配置文件。这是可用于与此端口相连的 KVM 目标服务器的配置文件。

指定首选 USB 配置文件：

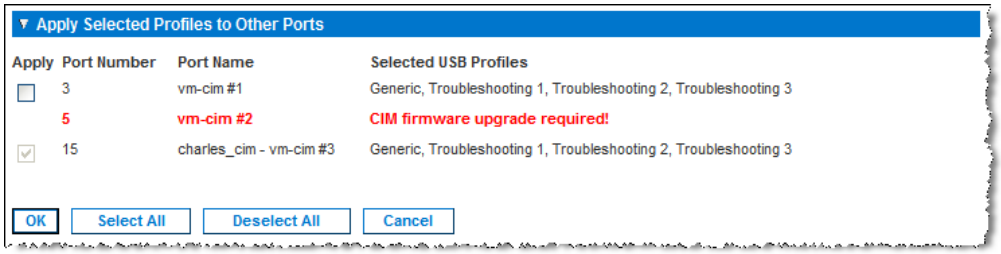
1. 在给一个端口选择多个可用配置文件之后，在 Preferred Profile for Port（首选端口配置文件）菜单上选择一个配置文件。默认值是 Generic。在连接 KVM 目标服务器时，使用所选的配置文件。必要时可以更改为其他任何 USB 配置文件。
2. 如果 Set Active Profile As Preferred Profile（设置活跃配置文件为偏好配置文件）勾选框被勾选，这个偏好 USB 也被用作活跃配置文件。

删除选择的 USB 配置文件：

1. 在 Select USB Profiles for Port（给端口选择 USB 配置文件）部分的 Selected（选择）列表上选择一个或多个配置文件。
   - 按住 Shift 单击选择几个连续配置文件。
   - 按住 Ctrl 单击选择几个不连续的配置文件。
2. 单击 Remove（删除）按钮。Available（可用）列表显示选择的配置文件。这些配置文件不再可用于与此端口相连的 KVM 目标服务器。

将选择的配置文件应用于多个端口：

1. 在 Apply Selected Profiles to Other Ports（将选择的配置文件应用于其他端口）部分选择要应用最新选择的 USB 配置文件的 KVM 端口对应的 Apply（应用）复选框。



   - 如要选择所有 KVM 端口，单击 Select All（全选）。
   - 如要取消所有 KVM 端口，单击 Deselect All（全部取消）。

配置 KX III 本地端口设置

注意：在 Local Port Settings（本地端口设置）页上更改某些设置之后，要重新启动正在使用的浏览器。如果在更改设置时重新启动浏览器，将记录设置步骤。

配置本地端口设置：

- 选择“设备设置”(Device Settings) >“本地端口设置”(Local Port Settings)。打开 Local Port Settings（本地端口设置）页。

启用标准本地端口

1. 选择 Enable Standard Local Port（启用标准本地端口）旁边的复选框启用它。取消此复选框禁用它。

   默认启用标准本地端口，但可以在必要时禁用它。

   在进行更改时，重新启动浏览器。

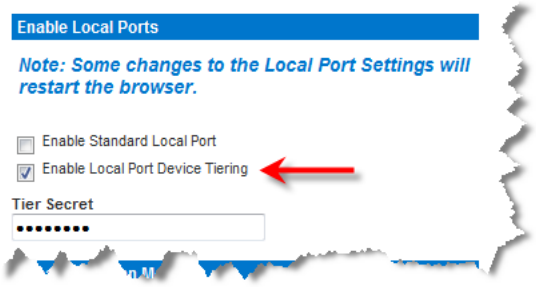
   注意：如果使用级联功能，将关闭标准本地端口特征，因为不能同时使用这两个功能。

启用本地端口设备级联

1. 如果使用级联功能，选择 Enable Local Port Device Tiering（启用本地端口设备级联）复选框，在 Tier Secret（级联密码）字段里输入级联密码。

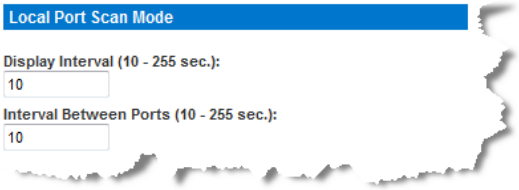
   为了配置级联，还必须在 Device Services（设备服务）页上配置基础设备。

   参看配置和启用分层详细了解分层。



配置 Local Port Scan Mode（本地端口扫描模式）设置

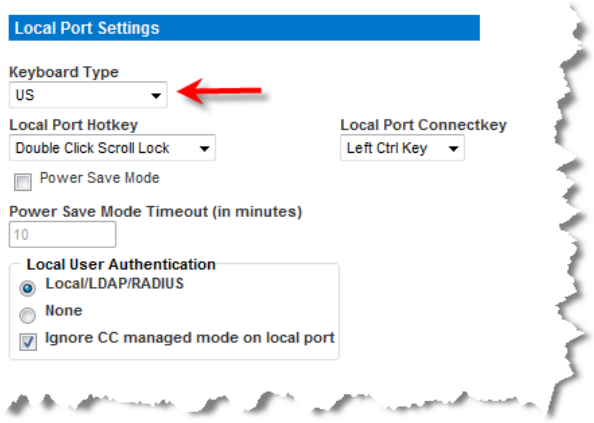
1. 必要时配置本地端口扫描模式设置。这些设置应用于在“端口”页上访问的“扫描设置”功能。参看扫描端口。
   - 在“显示间隔时间（10-255 秒）：”字段里指定目标服务器在端口扫描窗口中央显示的秒数。
   - 在“端口之间的间隔时间（10-255 秒）：”字段里指定设备在各个端口之间应该暂停的间隔时间。



选择 local console 键盘类型

1. 在键盘类型下拉列表上的选项中选择合适的键盘类型。

   在进行更改时，重新启动浏览器。



- US（美国英语）
- US/International（美国英文/国际）
- 英国
- 法文（法国）
- 德文（德国）
- 德文（瑞士）
- Simplified Chinese（简体中文）
- Traditional Chinese（繁体中文）
- Dubeolsik Hangul（朝鲜文）
- JIS（日本工业标准）
- 葡萄牙文（葡萄牙）
- 挪威文（挪威）
- 瑞典文（瑞典）
- 丹麦文（丹麦）
- Belgian (Belgium)（比利时）
- 匈牙利文
- 西班牙文
- 意大利文
- 斯洛文尼亚文

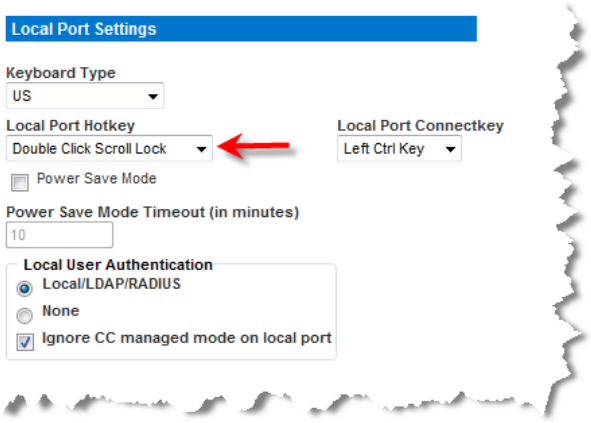
注意：中文键盘、日文键盘和朝鲜文键盘仅用于显示。KX III Local Console 功能目前不支持本地语言输入。

注意： 如果使用土耳其文件盘，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。

选择“本地端口热键”(Local Port Hotkey)。

1. 选择本地端口热键。在显示目标服务器界面时，可以用本地端口热键返回 KX III Local Console 界面。默认设置是按双击 Scroll Lock，但可以在下拉列表上选择任何组合键：

热键：	执行此操作：
双击 Scroll Lock	迅速按两次 Scroll Lock 键
双击 Num Lock	迅速按两次 Num Lock 键
双击 Caps Lock	迅速按两次 Caps Lock 键
双击左 Alt 键	迅速按两次左 Alt 键
双击左 Shift 键	迅速按两次左 Shift 键
双击左 Ctrl 键	迅速按两次左 Ctrl 键



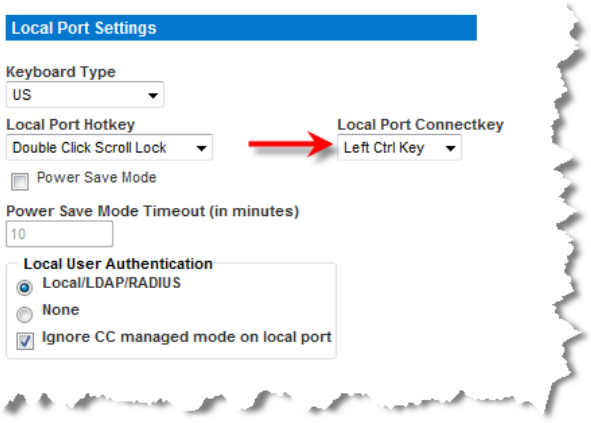
选择 Local Port Connect key（本地端口连接键）。

1. 选择 Local Port Connect key（本地端口连接键）。用连接键连接目标服务器，切换到另一台目标服务器。

   可以用热键断开目标服务器，返回本地端口 GUI。

   在创建本地端口连接键之后，GUI 导航面板显示该键，所以你可以用它作为参考。参看***连接键示例*** (p. 263)了解连接键顺序示例。

   连接键适用于标准服务器和刀片服务器机箱。

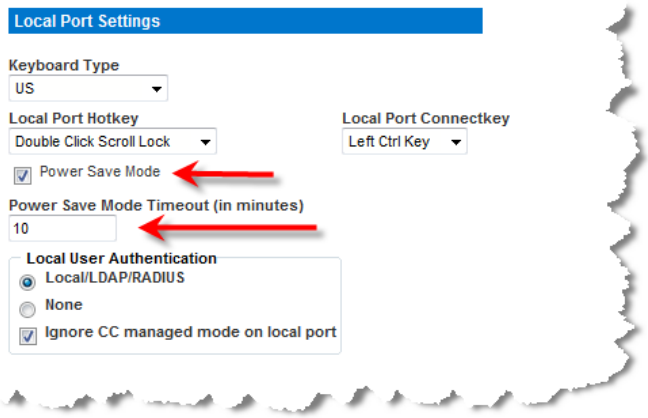


配置节电功能（可选）

1. 如果要使用节电功能：

   a. 选择 Power Save Mode（节电模式）复选框。

b. 设置在启动节电模式之前经过的时间（分钟）。

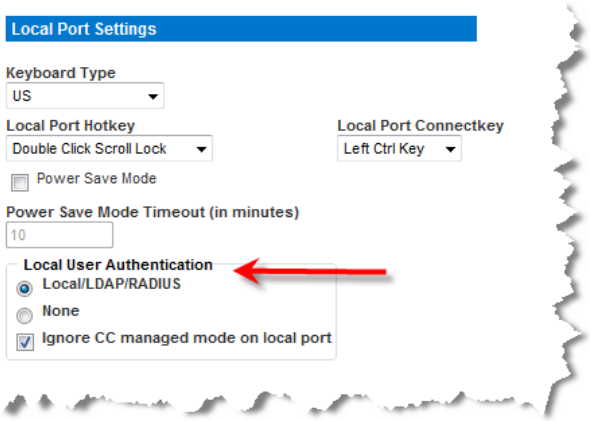


选择本地用户验证

1. 选择本地用户验证类型。
   - Local/LDAP/RADIUS。这是建议的选项。

     如要进一步了解验证，参看远程验证。
   - 不用安装任何软件。本地控制台访问不使用验证。

     建议你只在安全环境下使用此选项。



设备服务

启用 SSH

启用 SSH 访问，允许管理员通过 SSH v2 应用程序访问 KX III。

▶ **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 III 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 III 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 III，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。

配置和启用分层

分层功能允许你通过一台基础 KX III 设备访问多个 KX III 目标和多个电源条。

可以按需要在分层配置中增删设备，最多可以配置两层设备。

在设置设备时，要针对特定配置使用特定的 CIM。

参看分层 — 目标类型、支持的 CIM 和分层配置了解分层配置可包括的目标服务器、CIM 兼容性和设备配置信息。

必须在每台设备上直接进行端口配置，报告更改 CIM 名称。不能在基础设备上配置分层目标端口。

分层还支持用 KVM 切换器在服务器之间来回切换。参看***配置 KVM 切换器*** (p. 86)。

配置后，基准和分层设备会显示在端口访问页面上。参看***分层设备 — 端口访问页*** (p. 18)

在创建分层配置前

在创建分层配置前，参看***准许的 KX III 分层配置*** (参看 "***准许 KX III 分层配置***" p. 121) 和 分层目标不支持的功能和有限支持的功能。

在添加分层设备到 KX III 分层配置前：

- 基础和分层设备都必须使用相同固件版本操作。
- 在 Device Settings（设备设置）页上启用基础设备。参看配置标准目标服务器
- 在 Local Port Settings（本地端口设置）页上启用分层设备。参看***配置 KX III 本地端口设置*** (p. 115)，然后***启用本地端口设备级联*** (p. 115)
- 针对基础设备和分层设备启用分层。参看***启用分层*** (p. 123)

准许 KX III 分层配置

在分层设备前，查看***创建分层配置前*** (参看 "***在创建分层配置前***" p. 121)。

下面是准许的 KX III 分层配置：

- KX III 基础设备 > KX III 分层设备
- KX III 基础设备 > KX II 分层设备
- 双视频端口目标服务器应通过分层设备连接分层设备

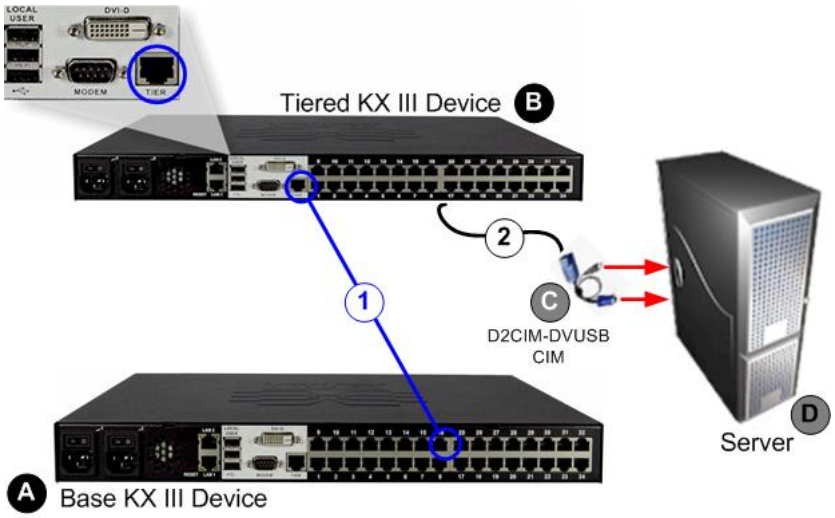
分层目标不支持的功能和有限支持的功能

分层目标不支持下列功能：

- 分层设备上的刀片服务器机箱
- 分层设备上的音频
- 分层设备上的智能卡
- 虚拟媒体分层设备
- 用作分层设备的 MCCAT
- 端口组管理仅限于针对直接连接基础设备的成员创建端口组。
- 当双视频端口目标服务器连接分层设备时，不应通过基础设备访问目标服务器。
- 如果你的分层配置包含 KX III 和 KX II 混合设备，绝对鼠标同步可能会出现错误
- AKX II 基础设备 > KX III 分层设备

分层 KX III 连接示例

下图说明 KX III 分层设备和 KX III 基础设备之间的布线配置。



步骤	
A	KX III 基础设备
B	KX III 分层设备
C	将目标服务器连接至 KX III 分层设备的 CIM。
D	目标服务器
1	基础设备分层端口至分层设备分层端口连接： ▪ 将 Cat5/5e/6 电缆末端连入 KX III 基础设备的目标服务器端口。 ▪ 将接线的另外一头插入到 KX III 分层设备的分层端口。
2	分层设备与目标服务器键盘/视频/鼠标端口连接： ▪ 将 Cat5/5e/6 电缆的一端连接至 KX III 分层设备的目标服务器端口，另一端至支持的 CIM，如 D2CIM-DVUSB。 ▪ 连接 CIM 上的键盘、鼠标和视频插头至目标服务器相应的端口。

启用分层

启用级联：

1. 从层级基础设备，选择 Device Settings（设备设置）> Device Services（设备服务）以打开 Device Service Settings（设备服务设置）页面。
2. 选择 Enable Tiering as Base（作为基础启用级联）。
3. 在 Base Secret（基本密码）字段里输入基础设备和级联设备共用的密码。如果级联设备要验证基础设备，需要此密码。对级联设备输入相同密码。单击 OK（确定）。
4. 启用级联设备。在级联设备上选择 Device Settings（设备设置）> Local Port Settings（本地端口设置）。
5. 在页面的 Enable Local Ports（启用本地端口）部分选择 Enable Local Port Device Tiering（启用本地端口设备级联）。
6. 在 Tier Secret（级联密码）字段里输入此前在 Device Settings（设备设置）页上输入的基础设备的密码。单击 OK（确定）。

在启用并配置设备之后，Port Access（端口访问）页显示这些设备。

在把 KX III 配置为基础设备或分层设备之后，如下显示它们：

- 在 KX III 界面左面板的 Device Information（设备信息）部分显示 Configured As Base Device（配置为基础设备），表示这是基础设备。
- 在 KX III 界面左面板的 Device Information（设备信息）部分显示 Configured As Tier Device（配置为分层设备），表示这是分层设备。
- 在分层设备界面左面板的 Connect User（连接用户）下面，显示 Base（基础）表示基础设备。
- 从基础设备到分层端口的目标连接用两个已连接端口表示。

从分层设备的远程和本地访问

可以通过 Port Access（端口访问）页上的合并端口列表，远程和本地访问基础设备。

可以通过分层设备的端口列表，远程访问分层设备。

在启用 Tiering（分层）之后，在分层设备上不能使用本地访问。

从基础设备访问刀片服务器机箱

刀片服务器机箱直接连至可访问的 KX III 基础设备。

从分层设备的电源控制

可以接通和断开作为级联配置组成部分的目标服务器的电源。

在 Port Access（端口访问）页上访问这些目标服务器。

如果目标服务器与出口关联，可以在 Port Access（端口访问）页上使用电源控制。

目标服务器和 PDU 出口关联仅限于那些同一台 KX III 相连的设备。

Power（电源）页下拉列表显示与基础或级联 KX III 相连的 PDU，以及所选电源条的统计数据。

还可以使用出口级控制。

尤其是可以断开当前通电的出口，但不能给当前断电的出口重新通电。

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。

为虚拟 KVM 客户机（VKC）直接端口访问 URL 语法

如果使用 Virtual KVM Client (VKC)和直接端口访问 ,使用 标准端口使用下列语法之一：

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

  或者

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

对于刀片服务器机箱，端口必须是通过端口号或名称以及插槽号指定的。

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

  例如端口号-插槽号是 1-2 ，刀片服务器机箱则连至端口 1，插槽 2。

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

  例如端口号-插槽号是 Port 1-2 ，刀片服务器机箱则连至端口 1，插槽 2。

Username 和 password 是可选的。

如果不使用用户名和密码，将显示登录对话框，用户在验证之后直接连接目标服务器。

port 可以是端口号或端口名称。

如果使用端口名称，名称必须是唯一的，否则系统报告出错。

如果忽略端口，系统报告错误。

如果访问作为双端口视频组组成部分的目标服务器，要用主端口同时启动主端口和辅端口。

拒绝与辅端口建立直接端口连接，并应用常规权限规则。

参看**创建双视频端口组** (p. 148)了解双端口视频组功能。 。

Active KVM Client (AKC) 的直接端口访问 URL 语法

如果使用 Active KVM Client (AKC)和直接端口访问，使用：

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

  或者

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

对于刀片服务器机箱，端口必须是通过端口号或名称以及插槽号指定的。

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

  例如端口号-插槽号是 1-2 ，刀片服务器机箱则连至端口 1，插槽 2。

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

  例如端口号-插槽号是 Port 1-2 ，刀片服务器机箱则连至端口 1，插槽 2。

Username 和 password 是可选的。

如果不使用用户名和密码，将显示登录对话框，用户在验证之后直接连接目标服务器。

port 可以是端口号或端口名称。

如果使用端口名称，名称必须是唯一的，否则系统报告出错。

如果忽略端口，系统报告错误。

Client=akc 是可选的，除非你使用 AKC 客户机。

如果没有 client=akc，使用 Virtual KVM Client (VKC) 客户机。

如果访问作为双端口视频组组成部分的目标服务器，要用主端口同时启动主端口和辅端口。

拒绝与辅端口建立直接端口连接，并应用常规权限规则。

参看**创建双视频端口组** (p. 148)了解双端口视频组功能。 。

启用直接端口访问。

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。

启用 AKC 下载服务器证书验证

如果使用 AKC 客户机，可以选择使用 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）功能，也可以选择不使用此功能。

注意：在 IPv4 和 IPv6 双协议堆模式下使用 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）功能时，Microsoft® ClickOnce® 要求服务器证书 CN 不包含零压缩格式的 IPv6 地址。

如果服务器证书 CN 包含零压缩格式的 IPv6 地址，不能成功下载并启动 AKC。

但对于此格式的 IPv6 地址，这可能会与浏览器性能发生冲突。

在公用名 (CN) 中使用服务器主机名，或者在证书的 Subject Alternative Name（主题别名）中包括压缩格式或非压缩格式的 IPv6 地址。

选项 1：Do Not Enable AKC Download Server Certificate Validation（不启用 AKC 下载服务器证书验证，默认设置）

如果不启用 AKC 下载服务器证书验证， 所有 Dominion 设备用户和 CC-SG Bookmark and Access Client 用户必须：

- 确保当前不阻止来自正在访问的设备的 IP 地址的 cookies。
- Windows Vista、Windows 7 和 Windows 2008 服务器用户应该确保正在访问的设备的 IP 地址位于浏览器的 Trusted Sites Zone（信任网站区域），在访问设备时不在 Protected Mode（保护模式）下。

选项 2：启用 AKC 下载服务器证书验证

如果启用 AKC 下载服务器证书验证：

- 管理员必须把有效证书上载到设备上，或者在设备上生成自签名证书。证书必须有有效主机名。
- 每个用户必须把 CA 证书（或自签名证书）添加到浏览器的 Trusted Root CA 仓库。
- 在使用 CC-SG 邻居时，你必须启用每个邻居成员的 AKC。

使用 Windows Vista® 操作系统和 Windows 7® 操作系统时如要安装自签名证书：

1. 把 KX III IP 地址加入 Trusted Site Zone（信任站点区域），确保关闭 Protected Mode（保护模式）。
2. 用 KX III IP 地址作为 URL 启动 Internet Explorer®。显示一条证书错误消息。

3. 选择 View Certificates（查看证书）。
4. 单击 General（常规）选项卡上的 Install Certificate（安装证书）。然后把证书安装在 Trusted Root Certification Authorities（信任根证书颁发机构）里。
5. 在安装证书之后，应把 KX III IP 地址从 Trusted Site Zone（信任站点区域）删除掉。

如要启用 AKC 下载服务器证书验证：

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 AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）复选框，或者禁用此功能（默认）。
3. 单击 OK（确定）按钮。

如果正连接 KX III 独立设备且已启用 AKC 下载服务器证书验证支持，生成该证书的有效 IPv6 格式将是：

- `CN=[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]`，有前导 0

  或者

- `CN=[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]`，无零压缩

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 III MIB*** (参看 "***查看 KX III MIB***" p. 138) 了解如何查看 KX III MIB。

KX III 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）。至少要选择一个选项。**要求**
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。

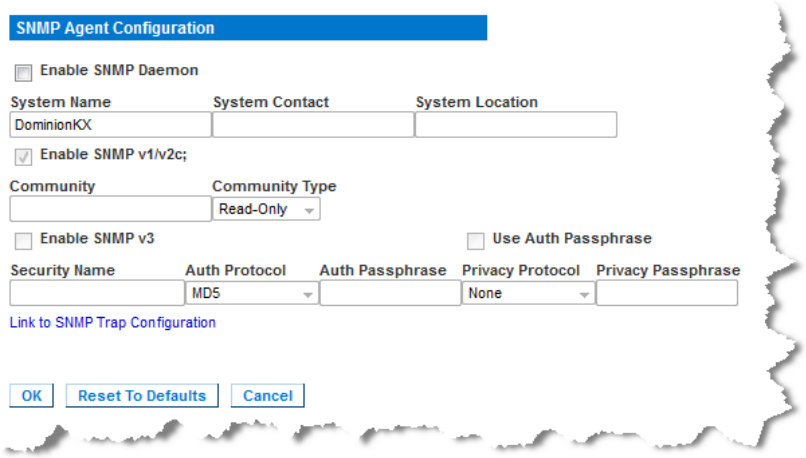
注意：SNMP 公用名是设备和运行 SNMP 的工作站所属的设备组，有助于定义要把信息发送到哪里。公用名用于标识此设备组。SNMP 设备或代理可能属于多个 SNMP 公用名。

---

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，可以通过点击 SNMP 陷阱配置链接迅速打开。参看***配置 SNMP 陷阱*** (p. 133)了解如何创建 SNMP 陷阱，参看 KX III SNMP 陷阱列表了解所有可用的 KX III 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*** (p. 139)。



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 III 之后，KX III 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。

配置调制解调器设置

注意：版本 KX III 3.0.0 不支持调制调节器，但是未来版本将支持。

配置日期/时间设置

在 Date/Time Settings（日期/时间设置）页上给 KX III 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”(Device Settings) >“日期/时间”(Date/Time)。打开 Date/Time Settings（日期/时间设置）页。
2. 在 Time Zone（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 Adjust for daylight savings time（调节夏令时）复选框。
4. 选择日期和时间设置方法：
   - User Specified Time（用户指定时间）— 选择此选项人工输入日期和时间。针对 User Specified Time（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 小时时钟）。
   - Synchronize with NTP Server（与 NTP 服务器同步）— 使用此选项使日期和时间与 Network Time Protocol (NTP) 服务器同步。
5. 对于 Synchronize with NTP Server（与 NTP 服务器同步）选项：
   a. 输入 Primary Time Server（主时间服务器）的 IP 地址。
   b. 输入 Secondary Time Server（备用时间服务器）的 IP 地址。**任选**（可选）
6. 单击 OK（确定）。

事件管理

可以用 KX III 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*** (p. 133)。

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*** (p. 139)。

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 III SNMP 陷阱列表了解所有 KX III SNMP 陷阱。

符合 SNMP 规范的设备（称为代理）把关于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. 129)了解如何配置 SNMP 代理，参看***查看 KX III MIB*** (p. 138) 了解如何查看 KX III MIB。

配置 SNMP（启用 SNMP 日志）：

1. 选择“设备设置”(Device Settings) >“事件管理 – 设置”(Event Management – Settings)。打开 Event Management - Settings（事件管理 — 设置）页。
2. 选择 SNMP Logging Enabled（启用 SNMP 日志）勾选框，以启用部分内其余勾选框。**要求**（要求）
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）。至少要选择一个选项。

   在选择选项之后，启用所有相关字段。**要求**
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）

注意：如果通过 Local Console 访问 Event Management - Settings（事件管理 — 设置）页，且屏幕分辨率低于 1280x1024，本页可能不显示 Privacy Passphrase（隐私密码）列。如果出现这种情况，隐藏 KX III 的左面板。参看左面板。

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*** (p. 139)。

KX III 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。

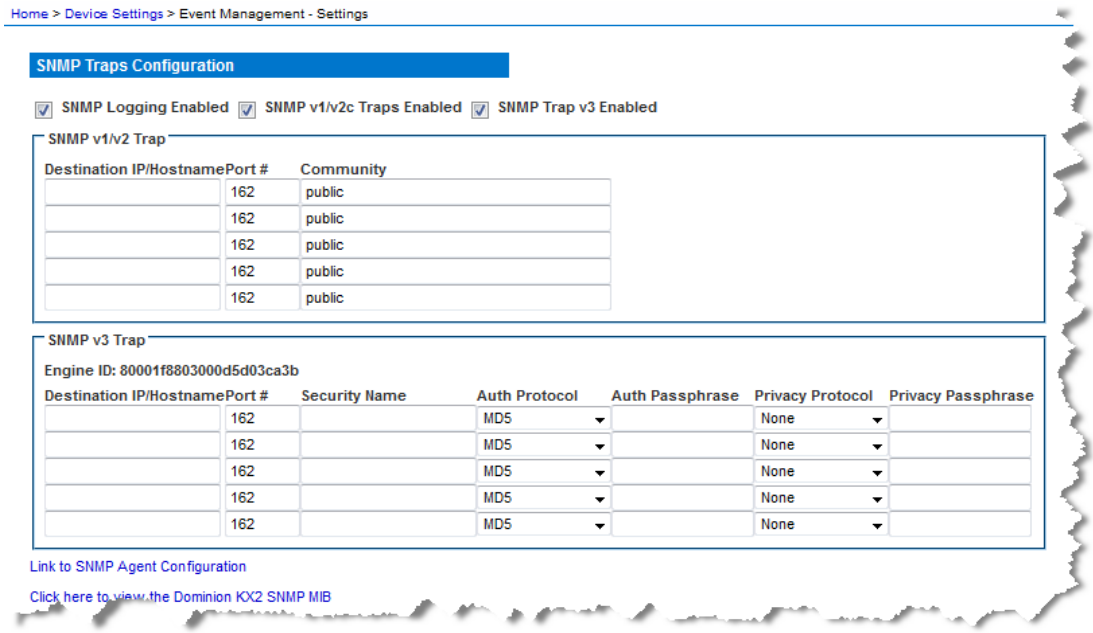
编辑现有的 SNMP 陷阱：

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 III 恢复到出厂默认设置。

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 III 之后，KX III 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 III SNMP 陷阱列表

在满足一个或多个条件时，SNMP 可以发送陷阱或通知，将此事通知管理员。

下表列出 KX III SNMP 陷阱：

陷阱名称	Description（说明）
bladeChassisCommError	检测到与此端口相连的刀片服务器机箱发生通信

陷阱名称	Description（说明）
	错误。
cimConnected	已连接 CIM。
cimDisconnected	已断开 CIM。
cimUpdateStarted	CIM 更新开始了。
cimUpdateCompleted	CIM 更新完成了。
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 III 用 RFP 文件完成了更新。
deviceUpgradeStarted	KX III 开始用 RFP 文件更新。
factoryReset	设备已被复位到出厂默认设置。
firmwareFileDiscarded	固件文件被丢弃。
firmwareUpdateFailed	固件更新失败。
firmwareValidationFailed	固件验证失败。
groupAdded	给 KX III 系统添加了一个组。
groupDeleted	在系统里删除了一个组。
groupModified	修改了一个组。
ipConflictDetected	检测到 IP 地址冲突。
ipConflictResolved	解决了 IP 地址冲突。
networkFailure	产品的 Ethernet 接口不再通过网络通信。
networkParameterChanged	更改了网络参数。
passwordSettingsChanged	更改了强密码设置。
portConnect	此前验证的用户开始了 KVM 会话。
portConnectionDenied	连接目标服务器端口被拒绝。
portDisconnect	参与 KVM 会话的一个用户正确关闭了会话。
portStatusChange	端口不可用。
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。

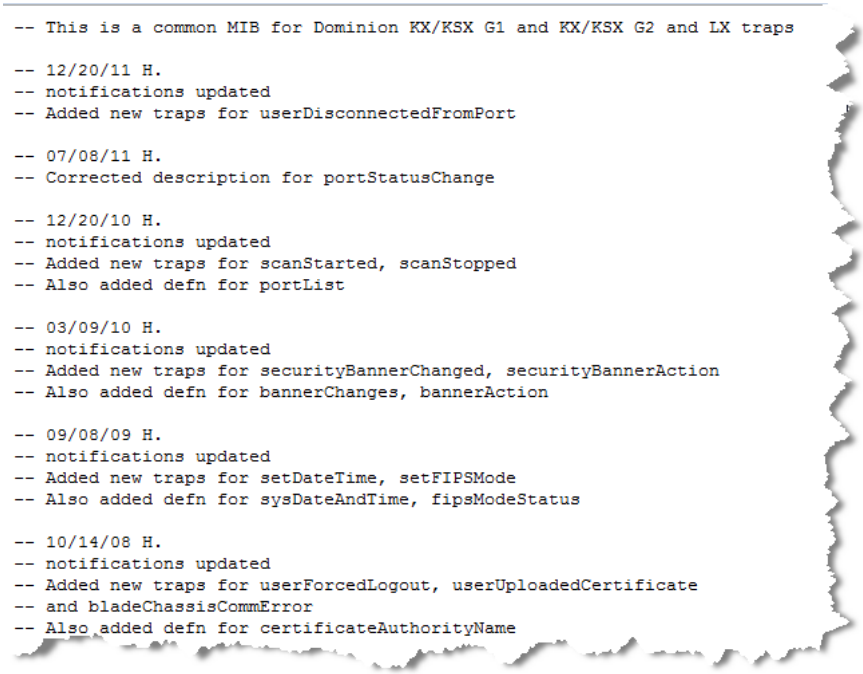
陷阱名称	Description（说明）
rebootCompleted	KX III 重新启动完毕。
rebootStarted	KX III 已开始采用系统重新通电或操作系统热启动方式重新启动。
scanStarted	已开始扫描目标服务器。
scanStopped	已停止扫描目标服务器。
securityBannerAction	接受/拒绝了安全标志。
securityBannerChanged	更改了安全标志。
securityViolation	违反安全。
setDateTime	已设置设备日期和时间。
setFIPSMode	启用了 FIPS 模式。
startCCManagement	设备受 CommandCenter 管理。
stopCCManagement	设备不再受 CommandCenter 管理。
userAdded	给系统添加了一个用户。
userAuthenticationFailure	用户尝试用错误用户名和/或密码登录。
userConnectionLost	有活动会话的用户遇到异常会话终止现象。
userDeleted	一个用户帐号被删除了。
userForcedLogout	管理员强制用户退出了。
userLogin	用户成功登录 KX III 并通过验证。
userLogout	用户采用正确方法成功退出 KX III。
userModified	一个用户帐号被修改了。
userPasswordChanged	如果修改设备的任何用户的密码，就触发此事件。
userSessionTimeout	有活动会话的用户由于超时而终止会话。
userUploadedCertificate	用户上载了 SSL 证书。
vmImageConnected	用户尝试在使用虚拟媒体的目标服务器上安装设备或镜像文件。 对于每个设备/镜像文件映射（安装）尝试，均生成此事件。
vmImageDisconnected	用户尝试在使用虚拟媒体的目标服务器上卸载设备或镜像文件。

查看 KX III MIB

查看 KX III MIB：

1. 选择“设备设置”(Device Settings) >“事件管理 – 设置”(Event Management – Settings)。打开 Event Management - Settings（事件管理 — 设置）页。
2. 单击 Click here to view the Dominion KX3（单击这里查看 Dominion KX3）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 setDateTime, setFIPSMode
-- Also added defn for sysDateAndTime, fipsModeStatus

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

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。

用复位到默认设置功能删除系统日志配置。

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. 132)。*

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。

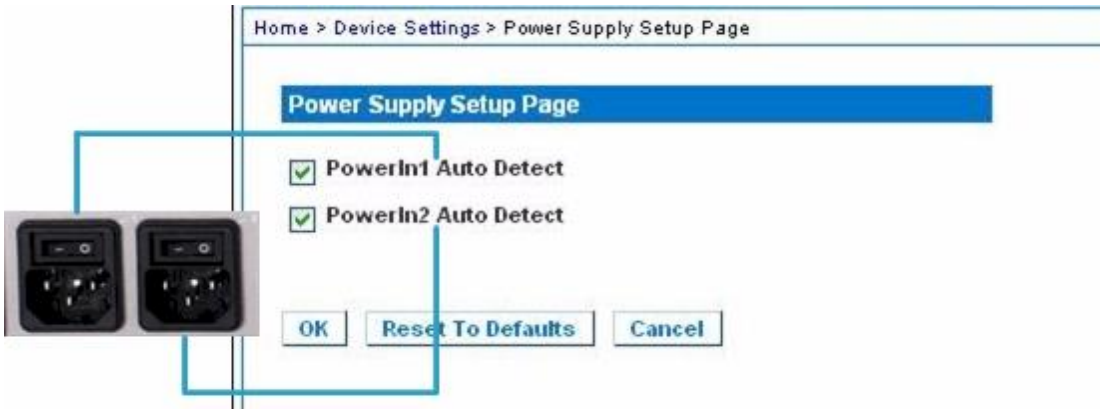
警告：在使用基于 UDP 的 SNMP 陷阱时，在重新启动 KX III 之后，KX III 和相连的路由器可能会不同步，致使重新启动操作不能完成 SNMP 陷阱记录。

电源设置

KX III 有两个电源，可以自动检测这些电源的状态并发出通知。在 Power Supply Setup（电源设置）页上指定是要使用一个电源，还是使用两个电源。正确配置电源，确保在一个电源发生故障时，KX III 能发送相应的通知。例如假如电源 1 发生故障，设备面板上的电源 LED 指示灯变成红色。

针对使用的电源启用自动检测：

1. 选择 Device Settings（设备设置）> Power Supply Setup（电源设置）。打开 Power Supply Setup（电源设置）页。



2. 如果将电源输入线插入电源 1（设备背面最左边的电源），选择 PowerIn1 Auto Detect（电源输入 1 自动检测）选项。
3. 如果将电源输入线插入电源 2（设备背面最右边的电源），选择 PowerIn2 Auto Detect（电源输入 2 自动检测）选项。
4. 单击 OK（确定）按钮。

注意：如果选择任一个复选框，但实际上并没有连接电源输入，设备面板上的电源 LED 指示灯变成红色。

关闭自动检测：

- 取消相应电源对应的复选框。

复位到出厂默认设置：

- 单击 Reset to Defaults（复位到默认设置）按钮。

注意：KX III 不向 CommandCenter 报告电源状态。但是，Dominion I（第一代）向 CommandCenter 报告电源状态。

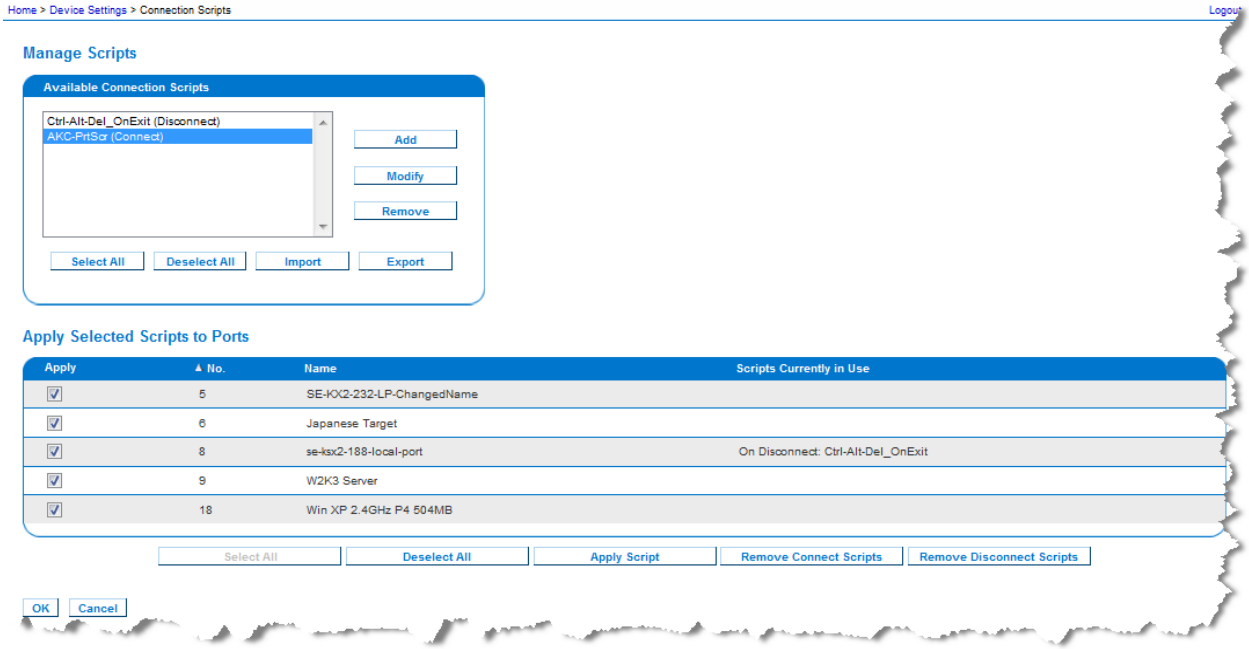
连接和断开脚本

在连接或断开目标服务器时，KX III 可以执行键盘宏脚本。

可以在 Connection Scripts（连接脚本）页上创建和编辑自己的脚本，在连接或断开目标服务器时执行附加操作。

还可以导入 XML 文件格式的现有连接脚本。还可以把在 KX III 上创建的脚本导出成 XML 文件格式。

最多可以在 KX III 上保存 16 个脚本。



应用和删除脚本

把脚本应用于目标服务器：

1. 单击 Device Settings（设备设置）> Connection Scripts（连接脚本）。打开 Connection Scripts（连接脚本）页。
2. 在 Available Connection Scripts（可用的连接脚本）部分选择要应用于目标服务器的脚本。可以把一个 'On Connect'（连接时使用）脚本和一个 'On Disconnect'（断开时使用）脚本应用于一台目标服务器。

   注意：每次只能把一个脚本添加到目标服务器。
3. 在 Apply Selected Scripts to Ports（把选择的脚本应用于端口）部分选择 Select All（全选）按钮选择要应用此脚本的目标服务器，或者单击要应用此脚本的每台目标服务器左边的复选框选择目标服务器。

4. 单击 Apply Scripts（应用脚本）按钮。在把脚本添加到目标服务器之后， Apply Selected Scripts to Ports（把选择的脚本应用于端口）部分的 Scripts Currently in Use（当前使用的脚本）列显示此脚本。

把脚本从目标服务器上删除掉：

1. 在 Apply Selected Scripts to Ports（把选择的脚本应用于端口）部分选择 Select All（全选）按钮选择要删除脚本的目标服务器，或者单击要删除脚本的每台目标服务器左边的复选框选择目标服务器。
2. 单击 Remove Connect Scripts（删除连接脚本）按钮删除连接脚本，或者单击 Remove Disconnect Scripts（删除断开脚本）按钮删除断开脚本。

添加脚本

*注意：你也可以添加此前在 KX III 之前的其他地方创建的脚本，并把它们作为 XML 文件导入。参看***导入和导出脚本** *(p. 145)*。

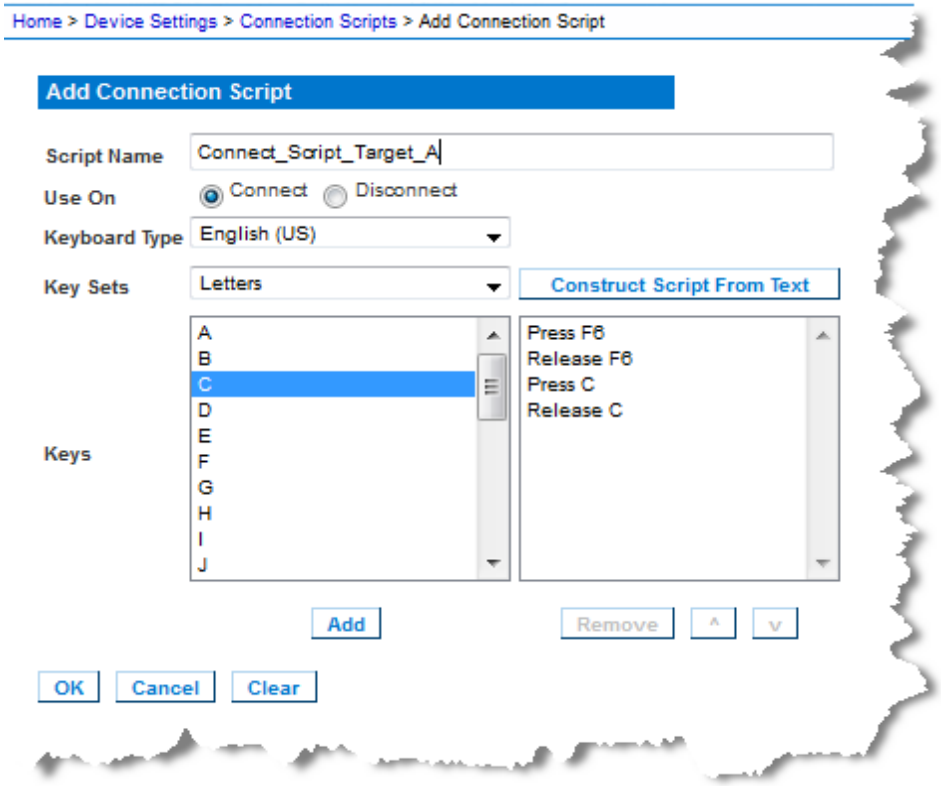
创建脚本：

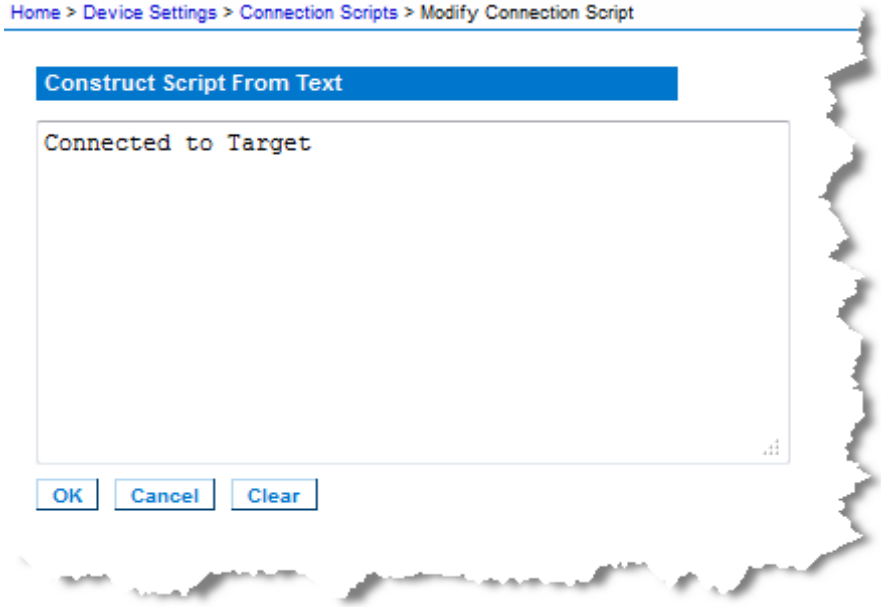
1. 单击 Device Settings（设备设置）> Connection Scripts（连接脚本）。打开 Connection Scripts（连接脚本）页。
2. 单击 Available Connection Scripts（可用的连接脚本）部分的 Add（添加）按钮，打开 Add Connection Script（添加连接脚本）页。
3. 输入最长 32 个字符的脚本名称。在创建脚本之后，Configure Scripts（配置脚本）页的 Available Connection Scripts（可用的连接脚本）部分显示此名称。
4. 选择 Connect（连接）或 Disconnect（断开）作为要创建的脚本的类型。连接脚本在建立新连接时或切换到目标服务器时使用。
5. 给你使用的目标服务器选择所需的键盘类型。
6. 在 Key Sets（键设置）下拉列表上选择创建脚本所用的键盘键设置。在选择键设置之后，Key Sets（键设置）下拉列表下面的 Add（添加）字段自动填充选择的键设置选项。
7. 在 Add（添加）字段里选择一个键，单击 Add（添加）按钮把它移动到 Script（脚本）字段里。在 Script（脚本）自动里选择一个键，单击 Remove（删除）按钮把它删除掉。选择键，单击 Up（向上）图标和 Down（向下）图标重新排序。

   脚本可以包含一个或多个键。也可以在脚本里搭配使用多个键。

   例如选择 F1-F16 显示在 Add（添加）字段里设置的功能键。选择一个功能键，把它添加到 Script（脚本）字段里。接下来在 Key Set（键设置）字段里选择 Letters（字母），把字母键添加到脚本里。

8. 可以输入在执行脚本时显示的可选文本。
   a. 单击 Construct Script from Text（根据文本创建脚本）按钮，打开 Construct Script from Text（根据文本创建脚本）页。
   b. 在文本字段里输入脚本。例如，输入 Connected to Target（连接目标服务器）。
   c. 单击 Construct Script from Text（根据文本创建脚本）页上的 OK（确定）按钮。
9. 单击 OK（确定）按钮创建脚本。


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
^
v
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

修改脚本

修改现有脚本：

1. 单击 Device Settings（设备设置）> Connection Scripts（连接脚本）。打开 Connection Scripts（连接脚本）页。
2. 在 Available Connection Scripts（可用的连接脚本）部分选择要修改的脚本，然后单击 Modify（修改）按钮。本页进入编辑模式。
3. 根据需要进行更改。在完成后，单击 OK（确定）按钮。

导入和导出脚本

可以导入和导出 XML 文件格式的连接脚本和断开脚本。不能导入或导出键盘宏。

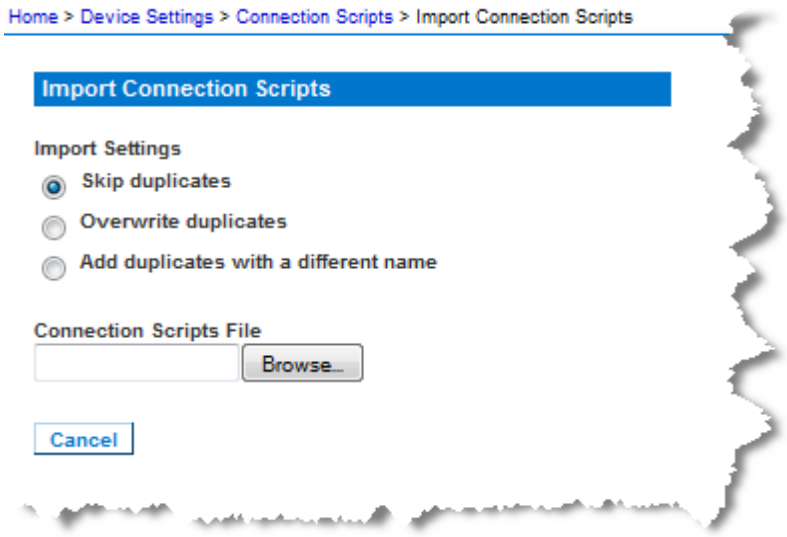
注意：不能在 Local Console 上使用导入和导出功能。

可以在 KX III 上用修改功能编辑导入的脚本。但在导入的脚本与端口关联之后，不能再修改脚本。删除脚本与端口之间的关联，即可修改脚本。参看***应用和删除脚本*** (p. 141)。

导入脚本：

1. 单击 Device Settings（设备设置）> Connection Scripts（连接脚本）。打开 Connection Scripts（连接脚本）页。
2. 单击 Available Connection Scripts（可用的连接脚本）部分的 Import（导入）按钮，打开 Import Connection Scripts（导入连接脚本）页。
3. 选择导入设置。
   - Skip duplicates（跳过重复项）— 不导入 KX III 已经有的脚本。
   - Overwrite duplicates（覆盖重复项）— 用新导入的脚本覆盖 KX III 已经有的脚本。
   - Add duplicates with a different name（用不同的名称添加重复项）— 在导入时重新命名重复项，不覆盖现有脚本。KX III 给文件名指定一个编号，把它与原脚本区分开。
4. 用浏览功能找到要导入的 XML 脚本文件。

5. 单击 Import（导入）按钮。打开 Configuration Scripts（配置脚本）页显示导入的脚本。



导出断开脚本：

1. 单击 Device Settings（设备设置）> Configuration Scripts（配置脚本）打开 Configuration Scripts（配置脚本）页。
2. 在 Available Connection Scripts（可用的连接脚本）部分选择要导出的脚本，然后单击 Export（导出）按钮。打开一个对话框，提示你打开或保存 XML 文件。
3. 保存 XML 文件，或者用 XML 编辑器打开此文件。如果保存 XML 文件，默认把它保存在 Download 文件夹里。

端口组管理

端口组管理指的是：

- 刀片服务器组 — 把与某些类型的刀片服务器相连的端口组合成表示刀片服务器机箱的端口组。参看 ***HP 和 Cisco UCS 刀片服务器机箱配置（端口组管理）*** (p. 105)了解详情。
- 双视频端口组 — 创建可显示目标服务器扩展桌面配置的端口组。参看 ***创建双视频端口组*** (p. 148)。
- 端口组 — 创建标准端口组把主端口的设置应用于同组里的所有辅端口。参看***创建端口组*** (p. 147)。

创建端口组

KX III 支持把多个端口组合成一个端口组 。端口组只包括作为标准 KVM 端口配置的端口。一个端口只能是一个组的成员。

Select Port for Group（给组选择端口）> Available（可用）列表显示端口组可以包括的端口。在把一个端口添加到端口组之后，不能再把它添加到另一个端口组里。把端口从当前端口组里删除掉，可以把它添加到新端口组里。

在主端口上执行的连接操作和断开操作应用于同组里的辅端口，但电源控制操作例外。

Port Groups（端口组）用 Backup and Restore（备份和恢复）选项恢复（参看***备份和恢复*** (p. 169)）。

注意：参看 **HP 和 Cisco UCC 刀片服务器机箱配置（端口组管理）** *(参看 "***HP 和 Cisco UCS 刀片服务器机箱配置（端口组管理）***" p. 105) 了解如何创建刀片服务器端口组，参看创建双端口视频组了解如何创建双视频端口组。*

▶ **创建端口组：**

1. 选择 Device Settings（设备设置）> Port Group Management（端口组管理）。打开 Port Group Management（端口组管理）页。显示现有的所有端口组。
2. 单击“添加”。页面刷新，显示所有可用的端口组选项。
3. 选择 Port Group（端口组）单选按钮。
4. 在 Available（可用）文本字段里选择要添加到端口组的端口，然后单击 Add（添加）按钮把它移动到 Selected（选择）文本字段里。
5. 单击 OK（确定）按钮创建端口组。Port Group Management（端口组管理）页显示端口组。

创建双视频端口组

可以利用双视频端口组功能把两个视频端口组合成一个端口组。在必须连接有两个显示卡/端口的服务器并在同一个远程客户机上同时访问两个端口时，可以使用此功能。

注意：KX3-108 和 KX3-116 模型等只有一个 KVM 通道的设备不支持双视频端口组。

注意：在创建双视频端口组之后，可以在 Local Console 和 Remote Console 上访问此端口组。但是，Local Console 不支持扩展桌面。

双视频端口组作为双端口类型出现在端口访问页。端口组中的主端口和次端口分别作为双端口 (P) 和双端口 (S) 出现在端口访问页。例如，如果 CIM 类型为 DCIM，则显示“DCIM 双端口 (P)”。

每个端口组必须有一个主端口和一个辅端口。把应用于主端口的配置应用于同组里的所有辅端口。如果把一个端口从端口组里删除掉，此端口即被视为独立端口，可以把新配置应用于此端口。

当从远程客户机访问双端口视频组时，可以连接到主端口，这会打开双端口组中主端口和次端口的 KVM 连接窗口。

必要时可以在一台或多台远程客户机上启动会话，并在监视器上观看会话。

在设备上给目标服务器配置的方向设置必须与目标服务器操作系统的实际配置相同。

建议在连接客户机时使用相同的屏幕方向

重要说明：参看双视频端口组一节了解可能会影响特定操作系统环境的限制和建议。

创建双端口视频组：

1. 选择 Device Settings（设备设置）> Port Group Management（端口组管理）。打开 Port Group Management（端口组管理）页。显示现有的所有端口组。
2. 单击“添加”。打开 Port Group（端口组）页，Select Ports for Group（给组选择端口）部分显示所有可用端口。

   注意：如果一个端口已经是刀片服务器端口组、另一个双视频端口组或标准端口组的组成部分，此端口不再是其中一个选项，因为一个端口只能属于一个端口组。
3. 选择 Dual Video Port Group（双视频端口组）单选按钮。

4. 单击 Select Ports for Group（给组选择端口）部分显示的要指定为主端口的端口， 然后单击 Add（添加）按钮把它添加到 Selected（选择）文本字段里。确保先添加主端口。

*注意：理想情况下，应用于端口组中每个端口的权限应相同。如不同，则将带有最严格权限的端口的权限应用于端口组。例如，如果 VM Access Deny（VM 访问拒绝）应用到一个端口，VM Access Read-Write（VM 访问读写）应用于另一个端口，则将 VM Access Deny（VM 访问拒绝）应用到端口组。参看*权限和双视频端口组访问 *(参看 "权限和双视频端口组访问权" p. 197)，了解端口权限如何影响双视频端口组。*

5. 单击要指定为辅端口的端口， 然后单击 Add（添加）按钮把它添加到 Selected（选择）文本字段里。
6. 选择页面方向。选择最适合监视器设置的方向。
7. 单击 OK（确定）按钮创建端口组。

双视频端口组作为双端口类型出现在端口访问页。端口组中的主端口和次端口分别作为双端口 (P) 和双端口 (S) 出现在端口访问页。例如，如果 CIM 类型为 DCIM，则显示“DCIM 双端口 (P)”。

注意： 当双视频端口目标服务器连接分层设备时，只应通过分层设备访问目标服务器，不应通过基础设备访问目标服务器。

更改默认图形用户界面语言设置

KX III 图形用户界面支持下列本地化语言：

- 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“设备设置”(Device Settings) >“语言”（language）。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。

安全管理

安全设置

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

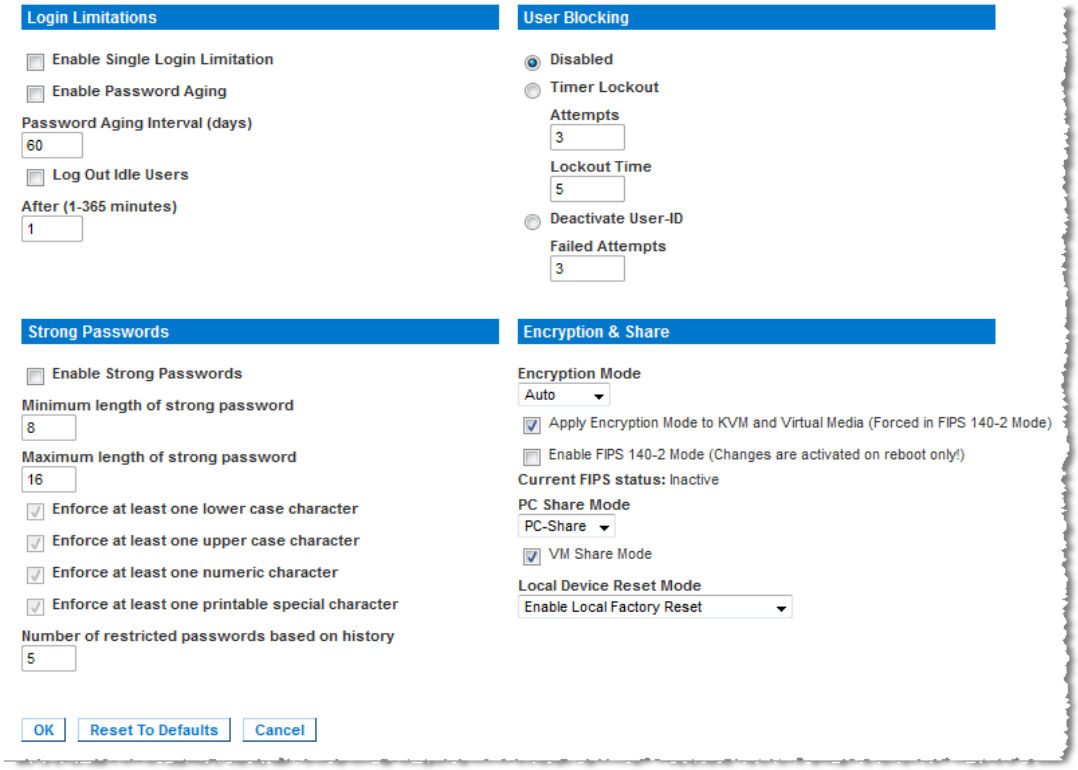
Raritan SSL 证书用于交换公共密钥和专用密钥，进一步增强安全。Raritan Web 服务器证书是自签名证书。Java 小程序证书是 VeriSign 签名的证书。加密确保信息不被他人偷听，这些证书确保你可以相信实体是 Raritan, Inc.。

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. 151)设置。
3. 适当更新*强密码* (p. 152)设置。
4. 适当更新*用户锁定* (p. 154)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）。

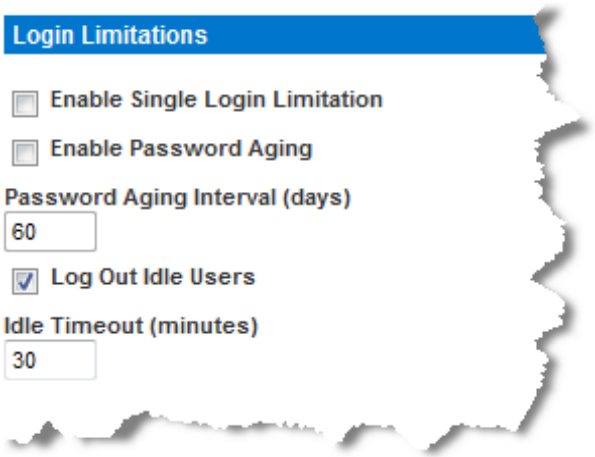


登录限制

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，可以同时在几个客户机工作站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 Password Aging Interval（密码有效天数）字段里指定的天数定期更改密码。 如果选择 Enable Password Aging（启用密码有效期）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,	选择 Log off idle users（退出用户）复选框，在经

限制	说明
After（在此之后退出闲置用户，1-365 分钟）	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

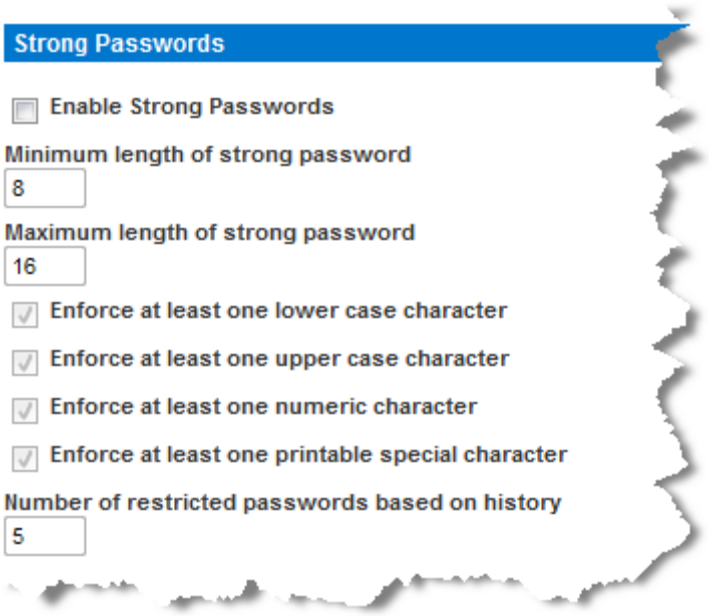
强密码给系统提供更安全的本地验证。可以利用强密码指定有效 KX III 本地密码的格式，例如最小长度、最大长度、要求的字符和密码历史保留期。

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 password（强密码最小长度）	密码至少要有 8 个字符。默认值是 8，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

字段	说明
	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，密码至少要有一个数字字符。
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，密码至少要有一个可打印特殊字符。
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。

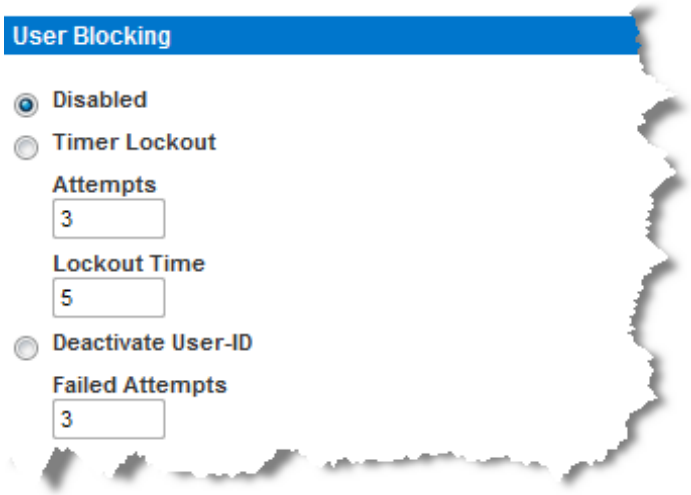


用户锁定

“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	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： ▪ 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。 ▪ 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。 *注意：管理员用户不受定时器锁定设置的约束。*
停用用户 ID	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。 ▪ 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。 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。



加密与共享

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 III 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 III。

配置加密与共享

注意在启用加密后，视频性能可能会收到影响。性能影响的范围大学根据加密模式而定。

如需获得最佳的视频性能，如果你的安全政策允许，请禁用加密。

▶ **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 III。

   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 III。

加密模式	Description（说明）
Auto（自动）	这是建议的选项。KX III 自动协商最高级加密。 *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。
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 III 设备和远程 PC 之间提供专用通信通道。 如果启用 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***检查浏览器的 AES 加密*** (p. 157)了解详情。
AES-256	Advanced Encryption Standard (AES) 是

加密模式	Description（说明）
	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***检查浏览器的 AES 加密*** (p. 157)了解详情。

注意：如果运行 Windows XP® SP2，Internet Explorer 7® 不能用 AES-128 加密算法远程连接 KX III。

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. 157)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 III，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 III 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 III 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。

注意：在使用 P2CIM-AUSBDUAL 或 P2CIM-APS2DUAL 把目标服务器连接到两台 KX III 时，如果需要独占访问目标服务器，必须把两台 KVM 切换器的 PC Share（PC 共享）模式设置为 Private（独占）。

*参看***支持的 Paragon CIMS 和配置** *(参看 "***支持的 Paragon II CIM 和配置***" p. 278)进一步了解如何一起使用 Paragon CIM 和 KX III。*

检查浏览器的 AES 加密

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。

下列网络浏览器支持 AES 256 位加密：

- Firefox®
- Internet Explorer®

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™ 的 Jurisdiction Files 可以在下列网站的 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，可能需要启用 FIPS 140-2 模式。

KX III 使用嵌入的、在 Linux® 平台上运行的 FIPS 140-2 认证加密模块，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。

注意在启用 FIPS 140-2 模式后，性能可能会收到影响。

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 和 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 III。**要求**

   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 III 上的密钥。

FIPS 140-2 支持要求

KX III 支持使用 FIPS 140-2 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 III 使用建议：

KX III

- 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 III 的访问。注意 IP 访问控制限制任何形式的流量访问 KX III，所以必须给 NTP 服务器、RADIUS 主机、DNS 主机等授予 KX III 访问权。

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。IP 访问控制是全局性的，影响整个 KX III，但也可以在组一级控制对设备的访问。参看*基于组的 IP 访问控制表* (p. 58)进一步了解组级控制。

重要说明：KX III 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，127.0.0.1 不应在被禁的 IP 地址范围内，否则不能访问 KX III 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。
2. 选择 Enable IP Access Control（启用 IP 访问控制）复选框，启用本页上的其他字段。
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 III 设备。
   - Drop（拒绝）— 拒绝 IP 地址访问 KX III 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，前 24 位用作网络地址）格式输入。

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。
4. 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，把新规则放在现有规则前面，列表上的所有规则向下移。

提示：可以利用规则号更好地控制规则的创建顺序。

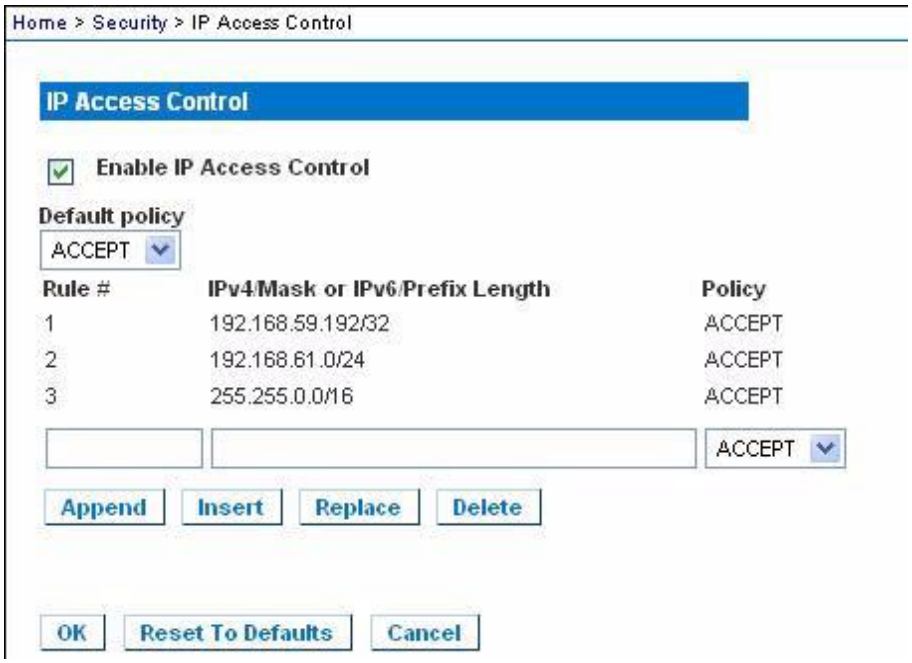
替换规则：

1. 指定要替换的规则编号。
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。
4. 单击 Replace（替换）按钮，用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. 系统提示你确认删除。单击 OK（确定）按钮。



SSL 证书

KX III 将 Secure Socket Layer (SSL) 协议用于它和相连客户机之间的所有加密网络流量。

在建立连接时，KX III 必须采用加密证书向客户机表明自己的身份。

可以生成证书签名请求 (Certificate Signing Request, CSR)，将验证中心签名的证书安装在 KX III 上。

CA 验证 CSR 发出人的身份。

验证中心然后返回一个证书，包含它给发出人的签名。经知名验证中心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 III日期/时间。

在创建自签名证书时，要用 KX III 日期和时间计算有效期。如果 KX III 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. 132)。

注意：必须在 KX III 上创建 CSR。

注意：在升级固件时，并不替换活动证书和 CSR。

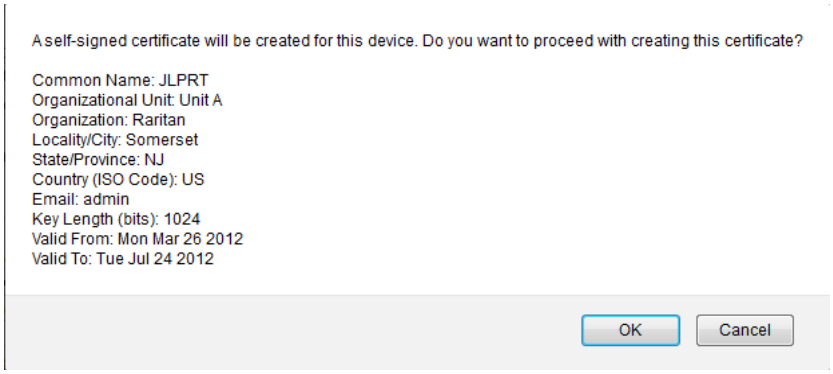
创建和安装 SSL 证书：

1. 选择“安全”(Security) >“证书”(Certificate)。
2. 填写下列字段：
   a. Common name（公用名）— 在网络上安装 KX III 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 III 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 III 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 III 归机构的哪个部门所有。
   c. Organization（机构）— KX III 所属机构的名称。
   d. Locality/City（地区/城市）— 机构所在的城市。
   e. State/Province（州/省）— 机构所在的州或省。
   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）。当生成 CSR 以获得 CA 证书时适用。
   h. Confirm Challenge Password（确认挑战密码）— 确认挑战密码。当生成 CSR 以获得 CA 证书时适用。
   i. Email（电子邮件）— 负责当收集 CSR 以获得 CA 证书时适用。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. 要生成，执行下列操作之一：
   - 生成自签证书，执行下列操作：
   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 III 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 III 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。

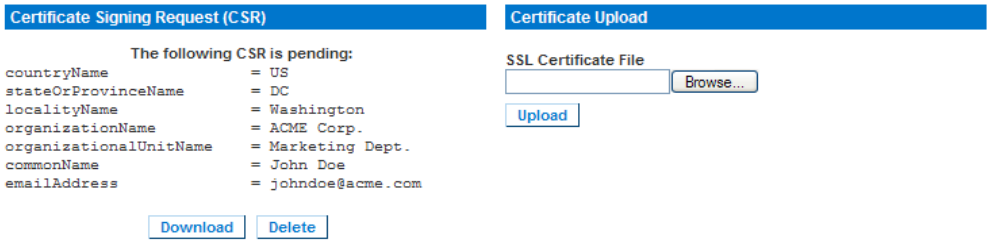


e. 重新启动 KX III 激活 CSR。

- 生成 CSR 发送给 CA 以获取证书：

a. 单击 Create（创建）按钮。

b. 消息列出你输入的所有信息。



c. 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。

d. 将保存的 CSR 发送到验证中心进行验证。你将收到来自验证中心的新证书。

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。

- 收到来自 CA 的证书后，单击 Upload（上载）按钮把证书上载到 KX III 上。
- 重新启动 KX III 激活证书。

在完成这些步骤之后，KX III 有了自己的证书，可以用此证书向客户机表明自己的身份了。

重要说明：如果销毁了KX III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 及其专用密钥的副本。

安全标志

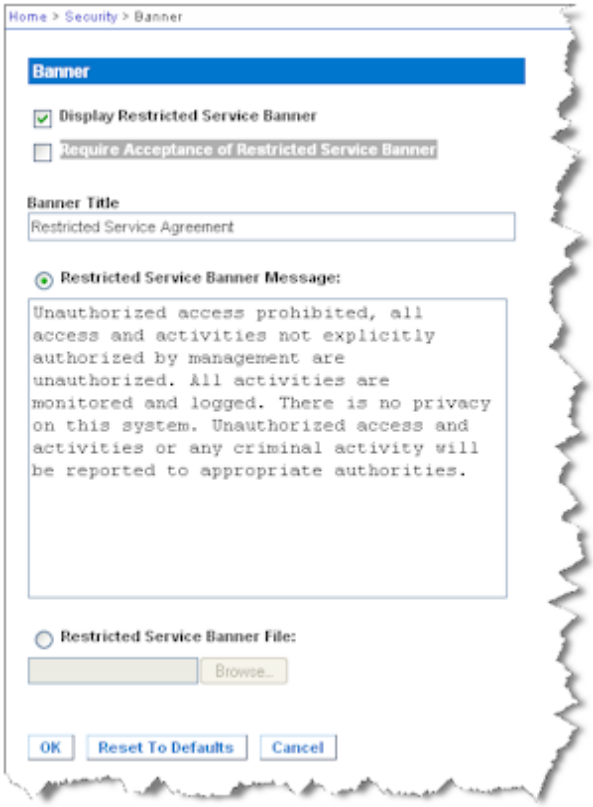
KX III 使你能给 KX III 登录过程增加安全标志。此功能要求用户在访问 KX III 之前接受或拒绝安全协议。在用户用自己的登录证书访问 KX III 之后，Restricted Service Agreement（有限服务协议）对话框显示在安全标志上输入的信息。

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 III 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。
   b. 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。

注意：不能在本地端口上载文本文件。



维护

审计日志

给 KX III 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。 参看*审计日志和系统日志记录的事件* (p. 313)，详细了解审计日志和系统日志记录哪些信息。

查看 KX III 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：

注意：只能在 KX III Remote Console 上保存审计，在 KX III Local Console 上不能保存。

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

Device Information（设备信息）页显示 KX III 设备和所用 CIM 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 KX III 和 CIM 信息：

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

显示 KX III 的下列信息：

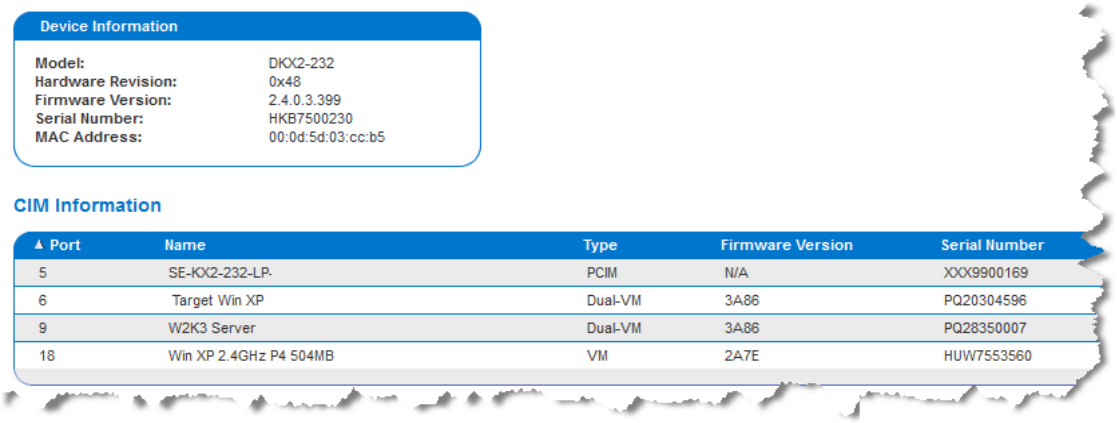
- Model（型号）
- Hardware Revision（硬件版本）
- Firmware Version（固件版本）
- Serial Number（序列号）
- MAC 地址

显示所用的 CIM 的下列信息：

- Port (number)（端口号）
- Name（名称）
- Type of CIM（CIM 类型）— DCIM、PCIM、机架式 PDU、VM、DVM-DP、DVM-HDMI 和 DVM-DVI
- Firmware Version（固件版本）
- Serial Number of the CIM（CIM 序列号）— 这是直接从支持的 CIM 获取的号码。
  - P2CIM-PS2
  - P2CIM-APS2DUAL
  - P2CIM-AUSBDUAL
  - P2CIM-AUSB
  - P2CIM-SUN
  - P2CIM-SUSB
  - P2CIM-SER
  - DCIM-PS2
  - DCIM-USB
  - DCIM-USBG2
  - DCIM-SUN
  - DCIM-SUSB
  - D2CIM-VUSB

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB

注意：对于 DCIM-USB、DCIM-PS2 和 DCIM-USB G2 CIMs，只显示序列号的数字部分。例如，显示 XXX1234567。显示有字段配置序列号 GIM 的序列号前缀 GM。



Device Information

Model:	DKX2-232
Hardware Revision:	0x48
Firmware Version:	2.4.0.3.399
Serial Number:	HKB7500230
MAC Address:	00:0d:5d:03:cc:b5

CIM Information

Port	Name	Type	Firmware Version	Serial Number
5	SE-KX2-232-LP-	PCIM	N/A	XXX9900169
6	Target Win XP	Dual-VM	3A86	PQ20304596
9	W2K3 Server	Dual-VM	3A86	PQ28350007
18	Win XP 2.4GHz P4 504MB	VM	2A7E	HUW7553560

备份和恢复

可以在 Backup/Restore（备份/恢复）页上备份和恢复 KX III 的设置和配置。

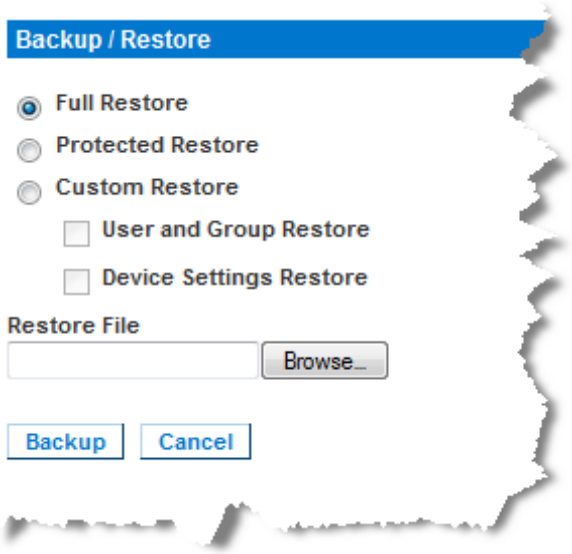
除了用备份和恢复功能增强业务连续性，还可以将它用作节省时间的方法。

例如备份使用中的 KX III 的用户配置设置，将这些配置恢复到新的 KX III 上，可以通过另一台 KX III 给团队提供访问。

还可以设置一台 KX III，将它的配置复制到多台 KX III 设备上。

访问备份/恢复页：

- 选择“维护”(Maintenance) >“备份/恢复”(Backup/Restore)。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，取决于你的选择。

如果使用 Internet Explorer 7 或更高版本备份 KX III：

1. 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 7 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®。

2. 为此修改设置：

   a. 保存备份文件。采用指定的名称和位置，将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 III：

警告：在把 KX III 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。如果不记得旧管理用户名和密码，不能访问 KX III。

此外，如果在备份时使用不同的 IP 地址，也恢复该 IP 地址。如果设备配置使用 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，全部恢复。如果选择此选项，可以设置一台 KX III，将它的配置复制到多台 KX III 设备上。
   - Custom Restore（定制恢复）— 如果选择此选项，可以选择 User and Group Restore（用户和组恢复）和/或 Device Settings Restore（设备设置恢复）。
     - User and Group Restore（用户和组恢复）— 此选项只包括用户信息和组信息。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 KX III 上的用户。
     - Device Settings Restore（设备设置恢复）— 此选项只包括设备设置，例如电源关联、USB 配置文件、与刀片服务器机箱关于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 Browse（浏览）按钮打开 Choose File（选择文件）对话框。
3. 找到并选择相应的备份文件，单击 Open（打开）按钮。Restore File（恢复文件）字段列出选择的文件。
4. 单击 Restore（恢复）按钮。根据选择的恢复类型恢复配置。

USB 配置文件管理

可以在 USB Profile Management（USB 配置文件管理）页上上载 Raritan 技术支持部门提供的定制配置文件。在标准配置文件不能满足目标服务器配置的要求时，这些配置文件可以满足它们的要求。Raritan 技术支持部门提供定制配置文件，与你一起验证解决方案是否满足目标服务器的特定要求。

Access（访问）访问 USB 配置文件管理页：

- Xuanz > 维护 > USB 配置文件管理 。USB 配置文件 usb 配置文件打开 USB Profile Management（USB 配置文件管理）页。

将定制配置文件上载到 KX III：

1. 单击 Browse（浏览）按钮打开 Choose File（选择文件）对话框。
2. 找到并选择相应的定制配置文件，单击 Open（打开）按钮。USB Profile File（USB 配置文件）字段列出选择的文件。
3. 单击“上载”。上载定制配置文件，Profile（配置文件）表显示该定制配置文件。

注意：如果在上载过程中显示错误消息或警告消息（例如覆盖现有的定制配置文件），可以单击 Upload（上载）按钮继续上载，或者单击 Cancel（取消）按钮取消上载。

将定制配置文件从 KX III 上删除掉：

1. 选择要删除的定制配置文件所在表行对应的复选框。
2. 单击“删除”。删除定制配置文件，Profile（配置文件）表不再显示该定制配置文件。

可以将定制配置文件从系统上删除掉，虽然它仍然被指定为活动配置文件。这样会中断正在进行的任何虚拟媒体会话。

处理配置文件名称冲突

在执行固件升级时，定制 USB 配置文件和标准 USB 配置文件之间可能会发生命名冲突。如果创建一个定制配置文件，并把它添加到标准配置文件列表上，但它的名称与作为固件升级组成部分下载的新 USB 配置文件相同，就会发生这种情况。

如果发生这些情况，现有的定制配置文件被标记为 old_。例如假如创建了名为 GenericUSBProfile5 的定制配置文件，但在固件升级过程中下载一个同名配置文件，就把现有文件命名为 old_GenericUSBProfile5。

必要时可以删除现有配置文件。参看 ***USB 配置文件管理*** (p. 171)了解详情。

升级 CIM

使用 KX III 设备内存存储的固件，通过此步骤升级 CIM。在用 Firmware Upgrade（固件升级）页升级设备固件时，通常同时升级 CIM。

用 KX III 内存升级 CIM：

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

   显示 Port (number)（端口号）、Name（名称）、Type（类型）、Current CIM Version（当前 CIM 版本）和 Upgrade CIM Version（升级 CIM 版本），CIM 标识一目了然。
2. 选择要升级的每个 CIM 对应的 Selected（选择）复选框。
3. 单击 Upgrade（升级）。系统提示你确认升级。
4. 单击 OK（确定）按钮继续升级。在升级过程中显示进度条。每个 CIM 的升级时间不超过 2 分钟。

升级 KX III 固件

用 Firmware Upgrade（固件升级）页升级 KX III 和所有相连 CIM 的固件。本页只能在 KX III Remote Console 上打开。

固件升级

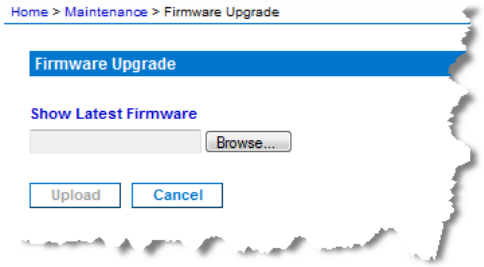
重要说明：在升级过程中切勿关闭KX III设备或断开 CIM，否则可能会损坏设备或 CIM。

升级 KX III 设备：

1. 在 ***Raritan 网站 http://www.raritan.com***的 Firmware Upgrades(固件升级）网页上找到合适的 Raritan 固件分发文件 (*.RFP)。
2. 解压文件。请在升级之前仔细阅读固件 ZIP 文件中的所有说明。

注意：先把固件升级文件复制到本地 PC，然后上载这些文件。切勿从网络驱动器上加载文件。

3. 选择“维护”(Maintenance) >“固件升级”(Firmware Upgrade)。打开 Firmware Upgrade（固件升级）页。



4. 单击 Browse（浏览）按钮，找到升级文件解压目录。
5. 单击 Firmware Upgrade（固件升级）页上的 Upload（上载）。

   显示升级信息和版本号信息，等待你确认（如果选择了 Review CIM Information[查看 CIM 信息]，也显示此信息）：

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。

6. 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。在升级结束之后，设备重新启动（发出一声蜂鸣声，表示重新启动结束）。
7. 在提示时关闭浏览器，等待大约五分钟即可再次登录 KX III。

升级历史记录

KX III 显示有关在 KX III 和相连 CIM 上执行的升级的信息。

查看升级历史记录：

- 选择“维护>升级历史记录”，打开“升级历史记录”页。

显示有关已进行的 KX III 升级的信息：最终升级状态、开始时间和结束时间、旧固件版本和当前固件版本。同时显示有关 CIM 的信息，单击升级对应的显示链接即可查看这些信息。显示下列 CIM 信息：

- 类型 — CIM 的类型
- 端口 — CIM 连接的端口
- 用户 — 执行升级的用户
- IP — 固件所在位置的 IP 地址
- 开始时间 — 升级开始时间
- 结束时间 — 升级结束时间
- 旧版本 — CIM 旧固件版本
- 升级版本 — 当前 CIM 固件版本
- CIM — 升级的 CIM
- 结果 — 升级结果（成功或失败）

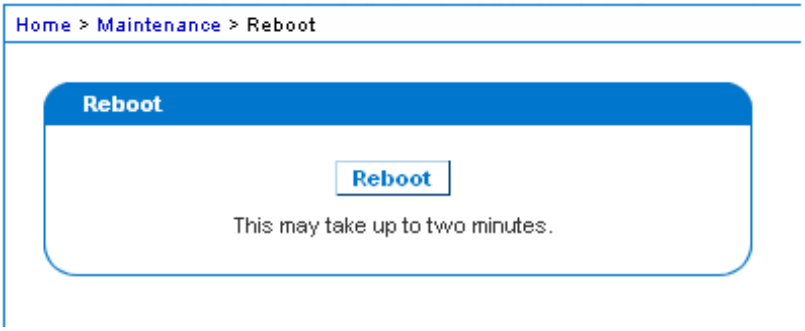
重新启动 KX III

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 III。这是建议的重新启动方法。

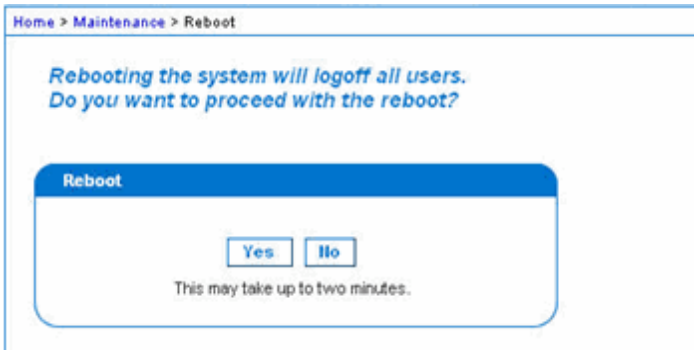
重要说明：必须关闭所有 KVM 连接和串行连接，必须退出所有用户。

重新启动 KX III：

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

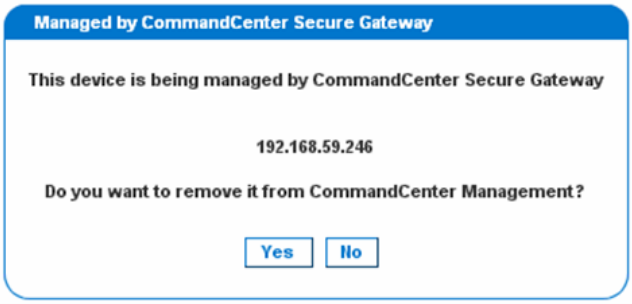
当 KX III 受 CC-SG 管理时，如果尝试直接访问该设备，系统通知你它受 CC-SG 管理。

如果你通过 CC-SG 管理 KX III，CC-SG 和 KX III 之间的连接在指定的超时间隔（通常是 10 分钟）之后断开，可以在 KX III 控制台上终止 CC-SG 管理会话。

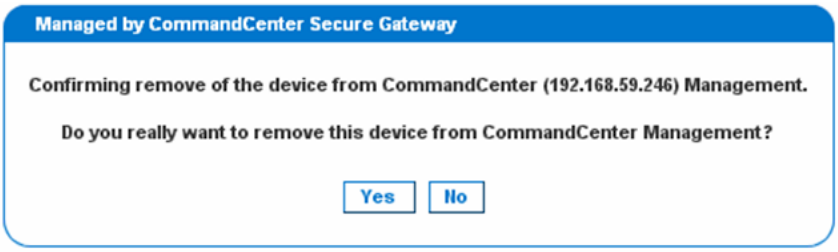
注意：必须具备适当的权限，才能终止 KX III CC-SG 管理。此外，除非当前用 CC-SG 管理 KX III，否则不显示 Stop CC-SG Management（停止 CC-SG 管理）选项。

停止 KX III 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。



3. 单击 Yes（是）按钮，让设备不再受 CC-SG 管理。在终止 CC-SG 管理之后，显示一条确认消息。

诊断

网络接口页

KX III 显示网络接口状态信息。

▶ **查看网络接口信息：**

- 选择“诊断”(Diagnostics) >“网络接口”(Network Interface)。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

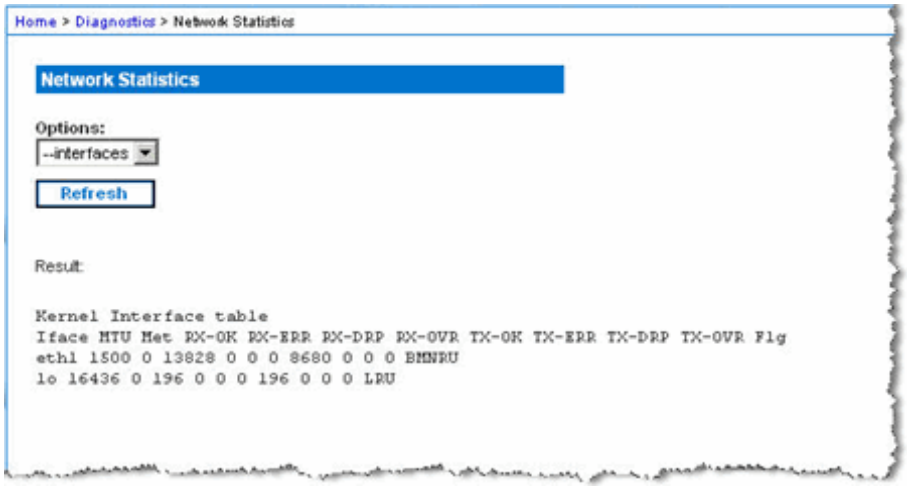
KX III 显示网络接口统计数据。

▶ **查看网络接口统计数据：**

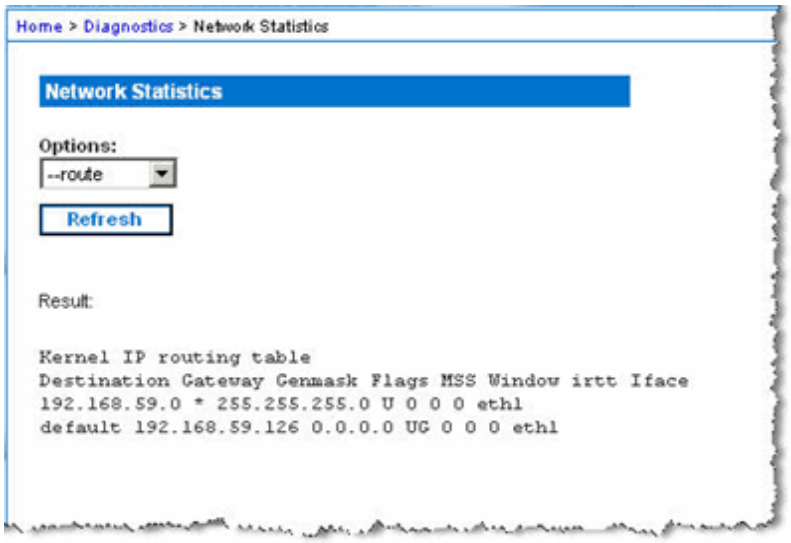
1. 选择 Diagnostics（诊断）> Network Statistics（网络统计数据），打开 Network Statistics（网络统计数据）页。
2. 在 Options（选项）下拉列表上选择适当的选项：

- Statistics（统计数据）— 生成类似下面这样的页面。

- Interfaces（接口）— 生成类似下面这样的页面。



- Route（路由）— 生成类似下面这样的页面。



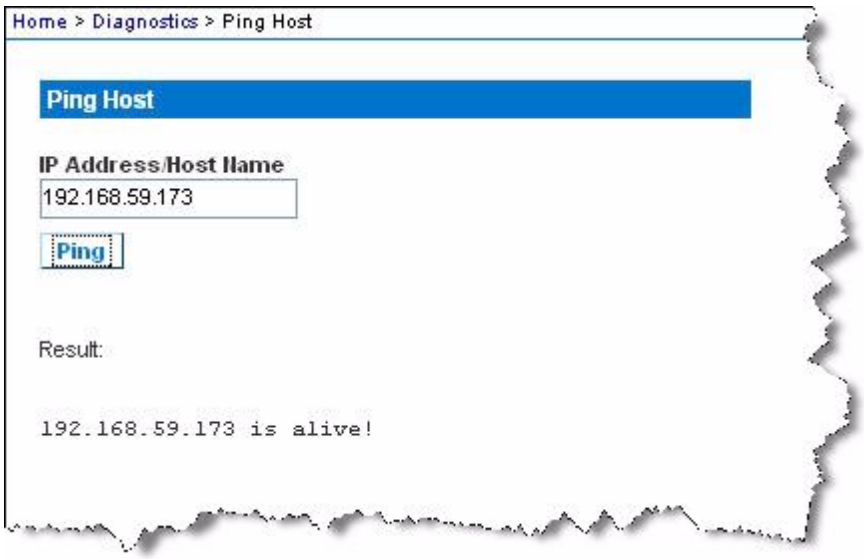
3. 单击 Refresh（刷新）按钮，Result（结果）字段显示相关信息。

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 III 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

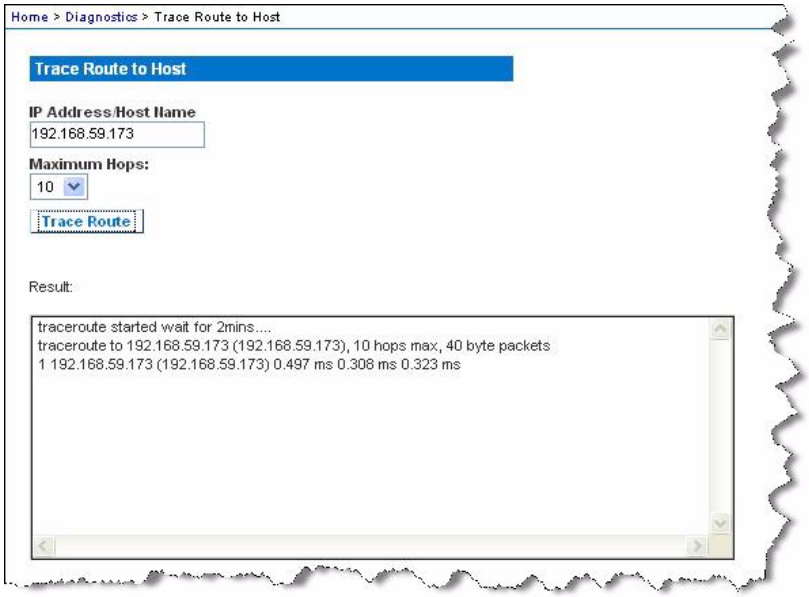
跟踪路由是网络工具，用于确定至指定主机名或 IP 地址的路由。

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。

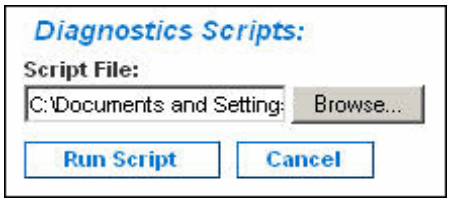
设备诊断功能把 KX III 上的诊断信息下载到客户机上。可以在本页上执行两个操作：

- 在严重错误调试会话中执行 Raritan 技术支持部门提供的专用诊断脚本。把此脚本上载到设备上执行。在执行此脚本之后，可以单击“保存到文件”按钮下载诊断消息。
- 把 KX III 设备诊断消息截屏对应的设备诊断日志下载到客户机上。然后把此加密文件发送给 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。

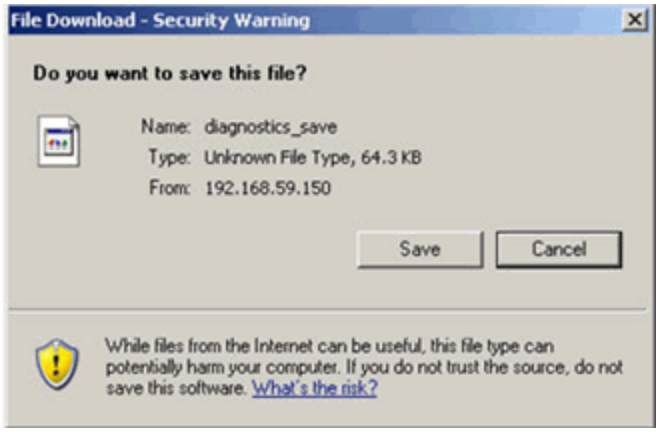
运行 KX III 系统诊断：

1. 选择“诊断> KX III 诊断”，打开“KX III 诊断”页。
2. 执行 Raritan 技术支持部门通过电子邮件发给你的诊断脚本文件：
   a. 接受并解压（必要时）Raritan 提供的诊断文件。
   b. 单击“浏览”按钮，打开“选择文件”对话框。
   c. 找到并选择诊断文件。
   d. 单击“打开”按钮，“脚本文件”字段显示此文件。



   e. 单击“运行脚本”按钮。把此文件发送给 Raritan 技术支持部门。
3. 创建要发送给 Raritan 技术支持部门的诊断文件：

a. 单击“保存到文件”按钮，打开“文件下载”对话框。



b. 单击“保存”按钮，打开“另存为”对话框。

c. 找到希望的目录，然后单击“保存”按钮。

d. 按 Raritan 技术支持部门的指示，通过电子邮件发送此文件。

KX III Local Console

KX III 通过本地端口提供机架访问和管理。访问 KX III 功能通过 Local Console 提供。

主要管理员功能一般在 KX III Remote Console 和 Local Console 执行。

这部分专门针对管理员任务。对于从 Local Console 执行任务的终端用户，参看 User Help（用户帮助）。

安全和验证

为了使用 KX III Local Console，必须先用有效用户名和密码进行验证。无论访问是通过网络还是本地端口进行的，KX III 均具备全集成验证和安全模式。无论在哪种情况下，KX III 都只允许用户访问那些他们有权访问的服务器。参看用户管理，进一步了解如何指定服务器访问权和安全设置。

如果给 KX III 配置了外部验证服务（LDAP/LDAPS、RADIUS 或 Active Directory），在本地控制台上进行的验证尝试也通过外部验证服务进行验证。

注意：也可以不给本地控制台访问指定验证：建议你只有在安全环境下才使用此选项。

使用 KX III Local Console：

1. 把键盘、鼠标和监视器连接到 KX III 背板上的本地端口。

2. 启动 KX III。显示 KX III Local Console 界面。

从 Local Console 配置 KX III 本地端口设置

可以在 Remote Console 的 Port Configuration（端口配置）页上或 Local Console 的 Local Port Settings（本地端口设置）页上配置标准本地端口。

可以在 Local Port Settings（本地端口设置）页上定制 KX III Local Console 的许多设置，包括键盘、热键、视频切换延迟、节电模式、本地用户界面分辨率设置和本地用户验证。

注意：只有具有管理权限的用户能访问这些功能。

注意：在 Local Port Settings（本地端口设置）页上更改某些设置之后，要重新启动正在使用的浏览器。如果在更改设置时重新启动浏览器，将记录设置步骤。

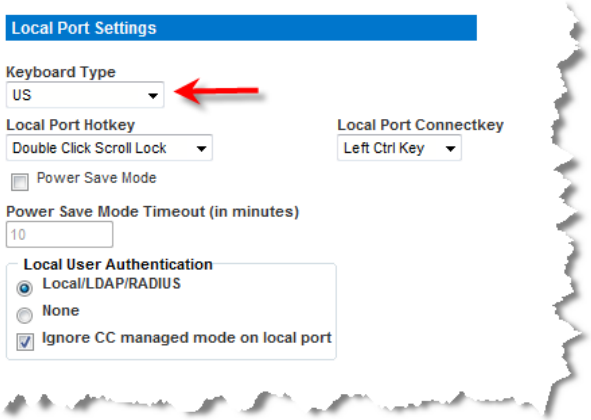
配置本地端口设置：

1. 选择“设备设置”(Device Settings) >“本地端口设置”(Local Port Settings)。打开 Local Port Settings（本地端口设置）页。

选择 local console 键盘类型

1. 在键盘类型下拉列表上的选项中选择合适的键盘类型。

   在进行更改时，重新启动浏览器。



- US（美国英语）
- US/International（美国英文/国际）
- 英国
- 法文（法国）
- 德文（德国）
- 德文（瑞士）
- Simplified Chinese（简体中文）
- Traditional Chinese（繁体中文）
- Dubeolsik Hangul（朝鲜文）
- JIS（日本工业标准）
- 葡萄牙文（葡萄牙）
- 挪威文（挪威）
- 瑞典文（瑞典）
- 丹麦文（丹麦）
- Belgian (Belgium)（比利时）
- 匈牙利文
- 西班牙文
- 意大利文
- 斯洛文尼亚文

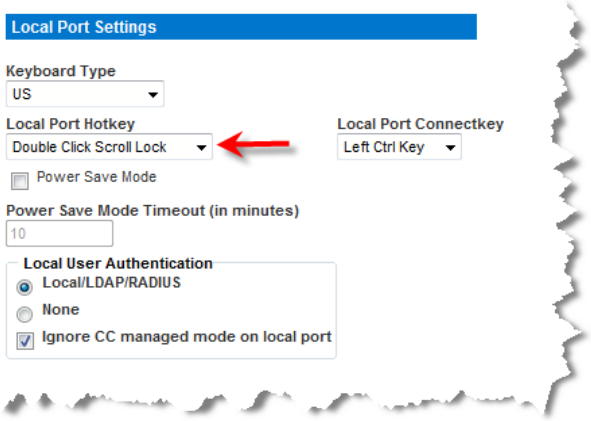
注意：中文键盘、日文键盘和朝鲜文键盘仅用于显示。KX III Local Console 功能目前不支持本地语言输入。

注意： 如果使用土耳其文件盘，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。

选择“本地端口热键”(Local Port Hotkey)。

1. 选择本地端口热键。在显示目标服务器界面时，可以用本地端口热键返回 KX III Local Console 界面。默认设置是按双击 Scroll Lock，但可以在下拉列表上选择任何组合键：

热键：	执行此操作：
双击 Scroll Lock	迅速按两次 Scroll Lock 键
双击 Num Lock	迅速按两次 Num Lock 键
双击 Caps Lock	迅速按两次 Caps Lock 键
双击左 Alt 键	迅速按两次左 Alt 键
双击左 Shift 键	迅速按两次左 Shift 键
双击左 Ctrl 键	迅速按两次左 Ctrl 键



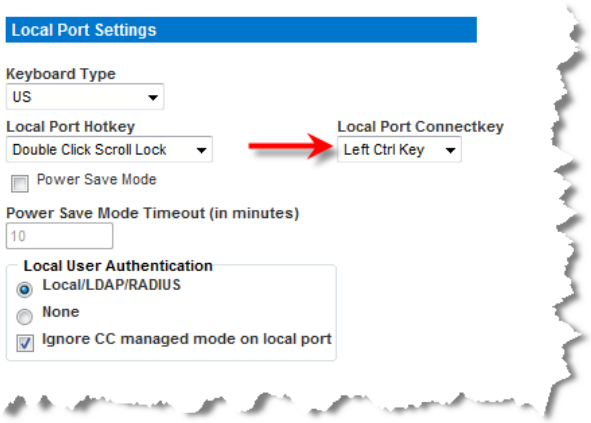
选择 Local Port Connect key（本地端口连接键）。

1. 选择 Local Port Connect key（本地端口连接键）。用连接键连接目标服务器，切换到另一台目标服务器。

   可以用热键断开目标服务器，返回本地端口 GUI。

   在创建本地端口连接键之后，GUI 导航面板显示该键，所以你可以用它作为参考。参看***连接键示例*** (p. 263)了解连接键顺序示例。

   连接键适用于标准服务器和刀片服务器机箱。

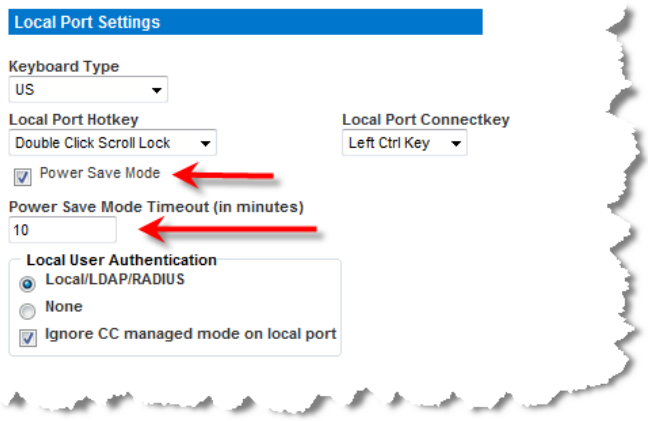


配置节电功能（可选）

1. 如果要使用节电功能：

   a. 选择 Power Save Mode（节电模式）复选框。

b. 设置在启动节电模式之前经过的时间（分钟）。

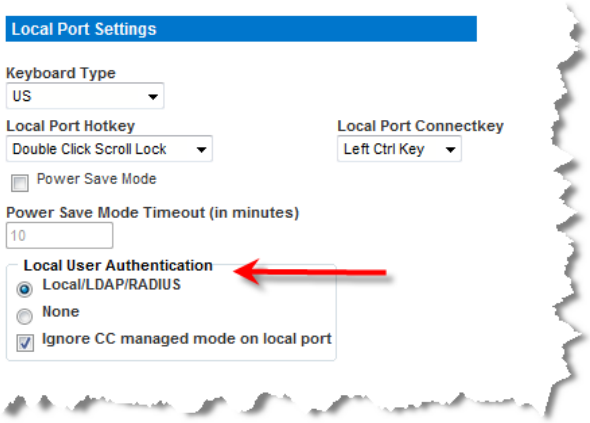


选择本地用户验证

1. 选择本地用户验证类型。
   - Local/LDAP/RADIUS。这是建议的选项。

     如要进一步了解验证，参看远程验证。
   - 不用安装任何软件。本地控制台访问不使用验证。

     建议你只在安全环境下使用此选项。

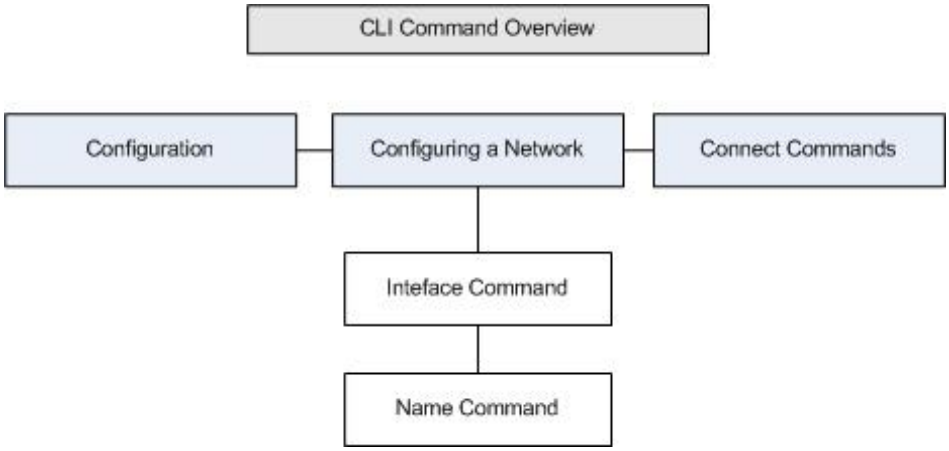


命令行界面

概述

假如你有适当的权限，可以用命令行界面配置 KX III 网络接口，执行诊断功能。

下图概述命令行界面命令。参看*命令行界面命令* (p. 191)了解所有命令清单，包括命令定义和本章各节的链接，相应的各节举例说明这些命令。



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、log off、quit、show 和 help。

用命令行界面访问 KX III

用下列方法之一访问 KX III：

- 基于 IP 连接的 SSH (Secure Shell)

可以使用多种 SSH 客户机，这些客户机可以在下列网站上下载：

- 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***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

用 SSH 连接访问 KX III

用支持 SSHv2 的任何 SSH 客户机连接 KX III。必须在 Devices Services（设备服务）页上启用 SSH 访问。

注意：出于安全原因，KX III 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 III 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。

显示 `login as:` 提示符。

参看*登录* (p. 188)。

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。

参看*登录* (p. 188)。

登录

▶ **如要登录，如下输入用户名 admin：**

1. 作为 `admin` 登录
2. 显示 Password 提示符。输入默认密码：*raritan*

   显示欢迎消息。你现在作为管理员登录了。

首先阅读下面的*命令行界面导航* (p. 189)一节，然后执行初始配置任务。

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。

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

下列命令可以在所有命令行界面上执行。这些命令还有助于导航命令行界面。

命令	说明
top	返回命令行界面级联结构的最高层，即 username 提示符。

命令	说明
history	显示用户在 KX III 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。
quit	让用户返回第一级。
logout	注销用户会话。

用命令行界面进行初始配置

*注意：命令行界面使用步骤是可选的，因为可以在 KVM 上进行相同的配置。参看*入门 *(p. 9)**了解详情。*

KX III 设备出厂时有默认出厂设置。在首次通电并连接设备时，必须设置下列基本参数，才能通过网络安全访问设备：

1. 更改管理员密码。所有 KX III 设备有相同的默认密码。因此，为了避免违反安全要求，必须将管理员密码从 raritan 更改为负责管理 KX III 设备的管理员的定制密码。
2. 指定 IP 地址、子网掩码和网关 IP 地址，从而启用远程访问。

设置参数

为了设置参数，必须登录设备获得管理权限。最高级显示 `Username>` 提示符，初始配置是 `admin`。输入 top 命令，返回最高级菜单。

注意：如果用不同的用户名登录，将显示该用户名，而不显示 admin。

设置网络参数

用 interface 命令配置网络参数。

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

如果命令被接受，设备自动断开连接。必须使用新 IP 地址和在复位出厂默认密码部分输入的用户名和密码，重新连接设备。

重要说明：如果忘记了密码，必须按 KX III 背面的 Reset（复位）按钮，把 KX III 复位到出厂默认设置。在复位到出厂默认设置之后，必须再次执行初始配置。

KX III 现在有基本配置，可以通过 SSH 和 GUI 远程访问它，也可以通过本地串行端口在本地访问它。管理员必须配置用户、用户组、服务和安全，以及串行目标服务器连接 KX III 所用的串行端口。

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 >
```

命令行界面命令

- 输入 `admin > help`。

命令	说明
config	切换到 config 子菜单。
diagnostics	切换到 diag 子菜单。
help	显示命令概述。
history	显示当前会话的命令行历史记录。
listports	列出可访问的端口。
logout	退出当前命令行界面会话。
top	返回根菜单。
userlist	列出活动用户会话。

- 输入 `admin > config > network`。

命令	说明
help	显示命令概述。
history	显示当前会话的命令行历史记录。
interface	设置/获取网络参数。
ipv6_interface	设置/获取 IPv6 网络参数。
logout	退出当前命令行界面会话。
name	设备名称配置。
quit	返回上一个菜单。
stop	返回根菜单。

安全问题

在解决控制台服务器的安全问题时要考虑的因素：

- 加密在操作员控制台和 KX III 设备之间发送的数据流量。
- 提供用户验证和授权。
- 安全配置文件。

KX III 支持所有这些要素，但必须在使用之前进行配置。

管理 KX III 控制台服务器配置命令

注意：SSH 和本地端口访问会话的命令行界面命令相同。

Network 命令可以在 KX III 的 Configuration（配置）菜单上访问。

配置网络

网络菜单命令用于配置 KX III 网络适配器。

命令	说明
interface	配置 KX III 设备网络接口。
name	网络名称配置。
ipv6	设置/获取 IPv6 网络参数。

Interface 命令

Interface 命令用于配置 KX III 网络接口。interface 命令语法如下：

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Interface 命令示例

下列命令启用接口 1，设置 IP 地址、子网掩码和网关地址，将 mode 设置为自动检测。

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

Name 命令

name 命令用于配置网络名称。name 命令语法如下：

```
name [devicename <devicename>] [hostname <hostname>]
```

设备名称配置

```
devicename <devicename>   Device Name

hostname   <hostname>     Preferred host name (DHCP
only)
```

name 命令示例

下列命令设置网络名称：

```
Admin > Config > Network > name devicename My-KSX2
```

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
```

双视频端口组

远程用户可以利用扩展桌面配置远程访问有两个显示卡的服务器。为此，要创建双端口视频组。

可以利用扩展桌面配置在两台监视器上观看目标服务器桌面，而不是只用一台标准监视器。

在选择双端口视频组之后，同时打开此组里的所有端口通道。

参看**创建双视频端口组** (p. 148)。

阅读本节了解双端口视频组重要信息。

注意：KX3-108 和 KX3-116 模型等只有一个 KVM 通道的设备不支持双视频端口组。

双端口视频建议

把目标服务器的主显示器和辅显示器设置为相同的视频分辨率，使鼠标保持同步，最大限度地减少定期同步次数。

根据希望的显示方向，上显示（垂直方向）或左显示（水平方向）应该是指定的主显示方向。显示器有活动菜单，可以选择虚拟媒体、音频、智能卡和鼠标操作。

为了实现直观的鼠标运动和控制，下列各项的显示方向应该相同：

- 客户 PC 的主要和次要显示
- KX II/KX III 的双视频端口组配置
- 目标服务器的主要和词语显示

只有下列 Client Launch Settings（客户机启动设置）要应用于双端口视频显示：

- 在启动 KVM 客户机时，选择标准显示模式或全屏窗口模式
- 启用视频缩放
- 启用在全屏模式下固定菜单工具栏

在一台客户机监视器上采用全屏模式显示双视频端口时，建议不要使用单鼠标模式。访问和观看另一个显示器需要退出单鼠标模式。

参看双视频端口组支持鼠标模式

目标服务器操作系统	支持的鼠标模式	备注
所有 Windows® 操作系统	智能鼠标模式、标准鼠标模式和单鼠标模式	如果目标服务器显示卡支持拉伸模式，绝对鼠标模式也能正常工作。 在拉伸模式下，目标服务器把双显示器视为一个虚拟显示器进行管理。 在扩展模式下的情形与此相反，目标服务器把显示器视为两个独立显示器。建议在扩展模式下使用智能鼠标模式。
Linux®	智能模式和标准鼠标模式	如果 Linux® 用户使用单鼠标模式，可能会发生显示问题和鼠标运动问题。Raritan 建议 Linux 用户不要使用单鼠标模式。
Mac® 操作系统	单鼠标模式	对于有多个监视器的 Mac 目标，使用一个为 Single-Cursor

目标服务器操作系统	支持的鼠标模式	备注
		模式的标准鼠标。

双视频支持要求的 CIM

下列 CIM 支持双视频端口功能：

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

参看数字 CIM 目标服务器时间设置和视频分辨率了解数字 CIM 重要信息。参看支持的计算机接口模块 (CIM) 规格了解 CIM 规格。

如果与主视频端口和次端口连接的原 CIM 断开或者被另一 CIM 替换，该端口将从双端口视频组移除。 必要时把此端口重新添加到端口组。

注意：使用的 CIM 视目标服务器的要求而定。

双端口视频组可用性说明

在使用双端口视频组功能时，会影响下列功能。

- 在 Virtual KVM Client (VKC) 和 Active KVM Client (AKC)客户机的 Tools（工具） Options（选项） Client Launch Settings（客户机启动设置）上配置的 Client Launch Settings（客户机启动设置）要如下应用于双视频端口组：
  - 要应用 Window Mode（窗口模式）设置
  - 不应用 Monitor(监视器)设置。要应用在 Port Group Management（端口组管理）页上配置的 Display Orientation（显示方向）。
  - 不应用 Other - Enable Single Mouse Cursor（其他 — 启用单鼠标光标）设置
  - 要应用 Other - Enable Scale Video（其他 — 启用缩放视频）设置
  - 要应用 Other - Pin Menu Toolbar（其他 — 固定菜单工具栏）设置

- 如果在主目标服务器窗口和辅目标服务器窗口之间拖放对象，在把对象从一个窗口移动到另一个窗口时，要求先释放鼠标键，然后再按鼠标键。
- 在 Linux® 和 Mac® 目标服务器上，在激活 Caps Scroll 和 Num Lock 键时，主端口窗口的状态栏显示 Caps Lock 指示器，但辅端口窗口的状态栏并不显示指示器。

权限和双视频端口组访问权

应用于端口组里每个端口的权限应该相同。如果权限不相同，要把限制最多的端口权限应用于端口组。

例如如果把 VM Access Deny（VM 拒绝访问）应用于一个端口，把 VM Access Read-Write（VM 读写访问）应用于另一个端口，要把 VM Access Deny（VM 拒绝访问）应用于此端口组。

如果用户没有适当权限访问作为双视频端口组组成部分的端口，只显示他/她有权访问的端口。如果用户无权访问任何一个端口，系统拒绝访问。

当用户尝试访问不可用的端口或自己无权访问的端口时，显示一条消息说明端口不可用或他/她无权访问此端口。

双端口视频组配置示例

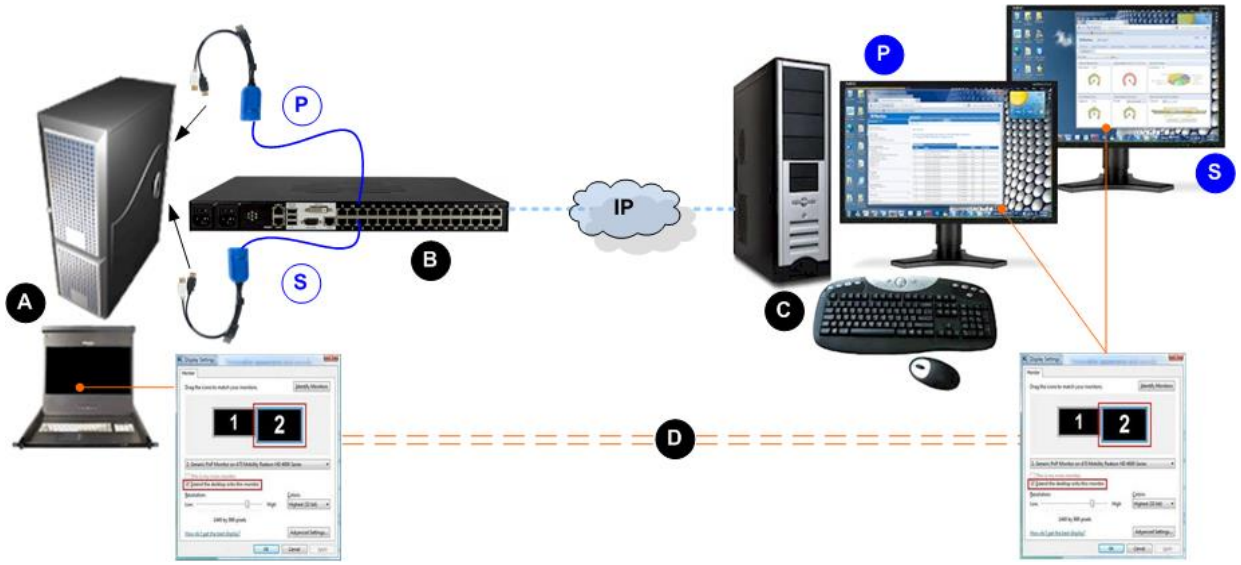
下面为一个总示例。

实际配置可能会有差异，视所用的 CIM 的类型、指定为主端口的端口、要连接的端口等因素而定。

在此示例中，我们使用：

- 一台有两个视频端口的目标服务器
- 目标服务器视频端口 1 是主端口，目标服务器视频端口 2 是辅端口
- 一个 KX3-832 设备：
- 一个 D2CIM-DVUSB-DP CIM
- 运行 Microsoft® Windows 7® 操作系统的目标服务器和客户机
- 智能鼠标模式

目标服务器和远程客户机扩展桌面视图，以便配置 KX III 支持“水平 — 主端口（左），辅端口（右）”显示方向。



图示符号	
A	远程客户机 - 配置双端口视频组并显示设置
B	KX III
P	目标服务器主要（第一个）视频端口到 KX III 的连接

图示符号	
S	目标服务器次要（第二个）视频端口到 KX III 的连接
KX III 和远程客户机之间的 IP 连接	
C	目标服务器 - 配置显示设置并启动双端口视频组
D	显示设置与远程客户机和目标服务器（推荐）上的一致
P	水平 - 主要（左）-（在 KX III 的 Port Group Management [端口组管理]页上定义）
S	次要（右）-（在 KX III 的 Port Group Management [端口组管理]页上定义）

双端口视频配置步骤

第一步：配置目标服务器显示设置

在设备上给目标服务器配置的方向设置必须与目标服务器操作系统的实际配置相同。

建议在连接客户机时使用相同的屏幕方向

如需获取显示方向和鼠标模式信息，参看双视频端口组显示方向、校准和鼠标模式了解显示方向和鼠标模式。

注意：参看目标服务器用户手册或操作系统用户手册了解如何正确配置显示设置。

配置目标服务器显示设置和鼠标设置：

1. 在目标服务器上给每个视频端口配置目标服务器显示方向，使其与远程客户机的显示方向相同。

   例如如果在远程客户机的两台监视器上使用从左到右的扩展桌面方向，给目标服务器设置相同的显示方向。

2. 确保已给目标服务器视频设置了支持的分辨率和刷新速度。参看***支持目标服务器视频分辨率*** (参看 "***支持 KX III 的目标服务器视频分辨率***" p. 294, ***http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#32872***)

   注意：如果目标主显示器和辅助显示器设置为不同的分辨率，鼠标将不能同步，且需要定期从左上方的目标窗口重新同步。

第二步：把目标服务器连接到 KX III

可以根据现有端口连接或新端口连接创建双端口视频组。

这里假设要创建新连接。

如果要根据现有连接创建双端口视频组，参看第四步：创建双视频端口组。

连接设备：

1. 如果尚未安装目标服务器，根据制造商提供的说明书安装目标服务器并通电。
2. 把每个 CIM 的视频插头插入目标服务器的视频输出端口，然后把 USB 电缆插入目标服务器上空闲的 USB 端口。
3. 用 CAT5/6 电缆把每个 CIM 连接到 KX III。
4. 如果尚未连接：
   a. 提供的电源线把 把 KX III 连接到交流电源。
   b. 连接 KX III 网络端口和本地端口（如果需要）
   c. 配置 KX III。参看入门 (p. 9)了解如何开始使用设备。
5. 启动支持的网络浏览器
6. 输入：
   - URL - *http://IP-ADDRESS* 以使用基于 Java 的 Virtual KVM 客户机

     或者

   - *http://IP-ADDRESS/akc* 使用基于 Microsoft .NET 的 Active KVM 客户机

   IP-ADDRESS 是给你的 KX III 分配的 IP 地址。

   你也可以使用 HTTPS 或由你的管理员(如适用)分配的 KX III 的 DNS 名称。

   你始终会被从 HTTP 的 IP 地址转到 HTTPS 的 IP 地址。
7. 输入“用户名”和“密码”，然后单击“登录”。
8. 接受用户协议（如适用）。
9. 如果显示安全警告，接受和/或允许访问。

第三步：配置鼠标模式和端口

在通过目标服务器视频端口把目标服务器连接到 KX III 之后，它将检测此连接，Port Configuration（端口配置）页显示视频端口。

参看**配置标准目标服务器**了解配置步骤。

在配置端口之后，可以把端口组合成双视频端口组。

---

*注意：在创建双端口视频组时，如果已配置了现有端口，不必再配置这些端口。参看**创建双视频端口组** (p. 148)。*

在连接目标服务器之后，配置目标服务器鼠标模式。参看**双视频端口组支持鼠标模式** (参看 "**参看双视频端口组支持鼠标模式**" p. 195)

第四步：创建双视频端口组

参看***创建双视频端口组*** (p. 148)。

第五步：启动双端口视频组

在创建双视频端口组之后，Port Access（端口访问）页显示双视频端口组。

通过点击主端口远程连接双视频端口组需要两个 KVM 通道。如果没有两个通道，Connect（连接）链接将不显示。

在 KX III 上配置的会话超时要有用于双视频端口组的两个端口。

启动双视频端口组：

- 在 Port Access（端口访问）页上单击主端口名称，然后单击 Connect（连接）按钮。

立刻启动两个连接，每个窗口显示一个连接。

在打开窗口之后，可以根据自己使用的显示设置移动窗口。例如如果使用扩展桌面模式，可以在两个监视器之间来回移动端口窗口。

在使用双视频端口组时的 Raritan 客户机导航

在客户机上使用全屏模式时，如下切换端口：

- VKC
  - 按 Alt+Tab
  - 对于 Mac® 客户机，先按 F3，然后选择端口显示
- AKC
  - 用鼠标单击显示窗口外面，然后按 Alt+Tab

直接端口访问和双端口视频组

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。

如果访问作为双端口视频组组成部分的目标服务器，要用主端口同时启动主端口和辅端口。

拒绝与辅端口建立直接端口连接，并应用常规权限规则。

参看**创建双视频端口组** (p. 148)了解双端口视频组功能。。

参看**启用通过 URL 进行直接端口访问**了解直接端口访问信息。

端口页显示双端口视频组

注意：在创建端口组时，定义双视频主端口。

注意：通过点击主端口远程连接双视频端口组需要两个 KVM 通道。如果没有两个通道，Connect（连接）链接将不显示。

对于双视频端口组，主端口包含在端口扫描中，但是从远程客户机连接时，次端口不包含在内。在从 Local Port（本地端口）进行扫描时两个端口均可包含在内。

参看端口访问页（Remote Console 显示）了解 Port（端口）页显示的信息，参看扫描端口了解如何执行扫描。

更新 LDAP 模式

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）。

从 LDAP/LDAPS 返回

当 LDAP 验证成功时，KX III 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启用此属性。

此外，对于 Microsoft® Active Directory®，还使用标准 LDAP memberOf。

自 Microsoft Active Directory

注意：仅供有经验的 Active Directory® 管理员尝试使用。

从 Windows 2000® 操作系统服务器上的 Microsoft® Active Directory 返回用户组信息，需要更新 LDAP/LDAPS 模式。参看 Microsoft 文档了解详情。

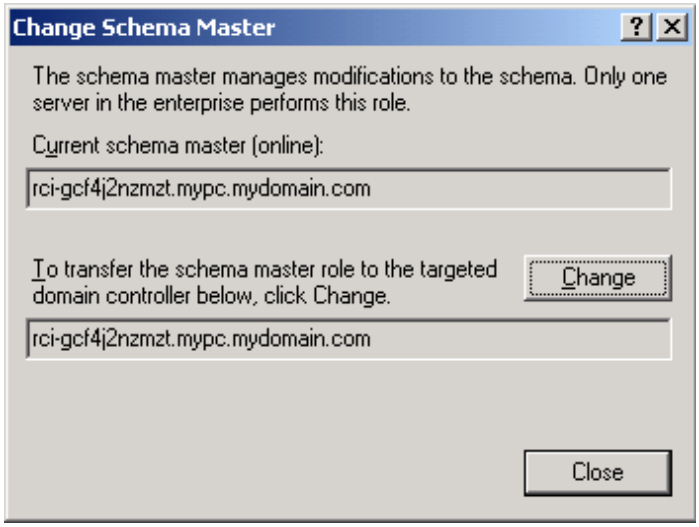
1. 安装 Active Directory 模式插件。参看 Microsoft Active Directory 文档了解说明。
2. 运行 Active Directory Console（Active Directory 控制台），选择 Active Directory Schema（Active Directory 模式）。

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。



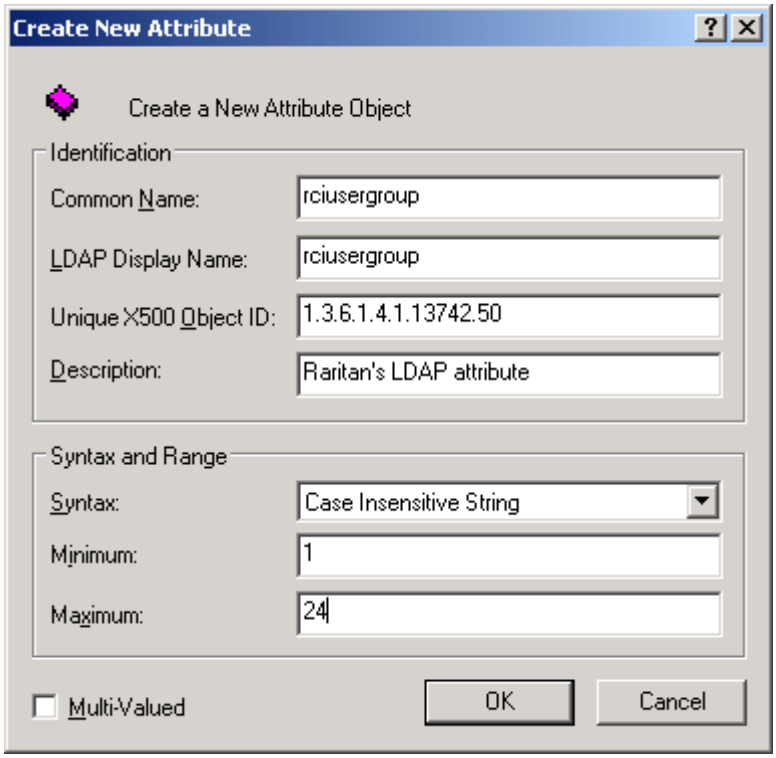
2. 选择 Schema can be modified on this Domain Controller(可以在此域控制器上修改模式）复选框。**可选**
3. 单击 OK（确定）按钮。

创建新属性

给 rciusergroup 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）。

3. 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。



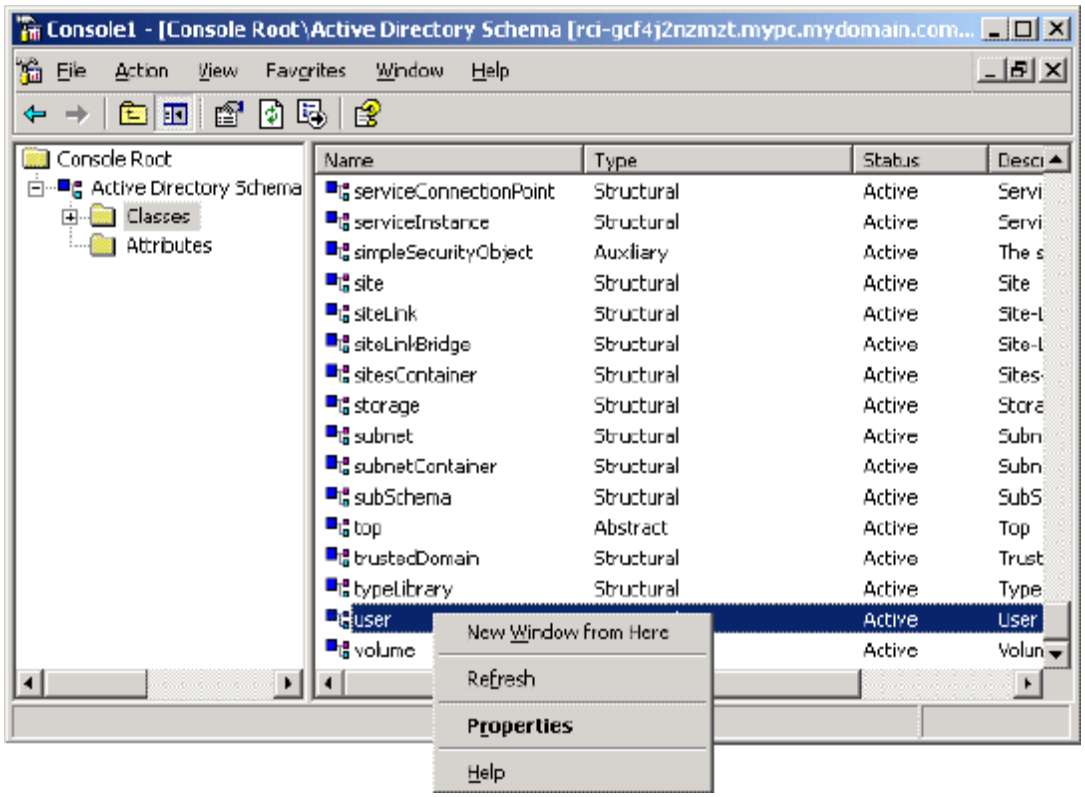
4. 在 Common Name（公用名）字段里输入 *rciusergroup*。
5. 在 LDAP Display Name（LDAP 显示名称）字段里输入 *rciusergroup*。
6. 在 Unique x5000 Object ID（唯一 x5000 对象 ID）字段里输入 *1.3.6.1.4.1.13742.50*。
7. 在 Description（说明）字段里输入有意义的说明。
8. 单击 Syntax（语法）下拉箭头，在列表上选择 Case Insensitive String（不区分大小写的字符串）。
9. 在 Minimum（最小值）字段里输入 *1*。
10. 在 Maximum（最大值）字段里输入 *24*。
11. 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：

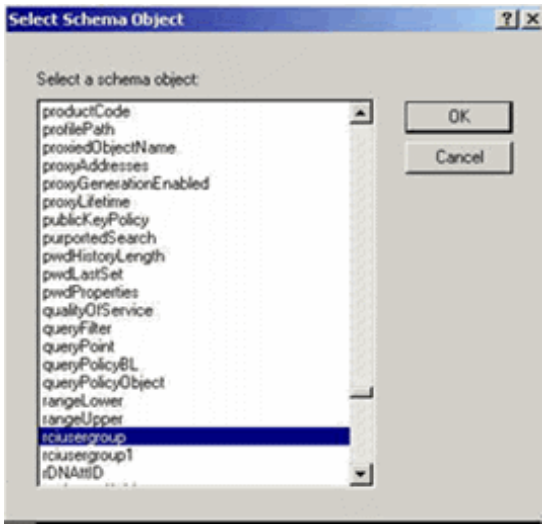
1. 单击窗口左面板上的 Classes（类）。

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。

6. 在 Select Schema Object（选择模式对象）列表上选择 rciusergroup。



7. 单击 Select Schema Object（选择模式对象）对话框上的 OK（确定）按钮。
8. 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：

1. 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）。
2. 最小化 Active Directory Schema MMC (Microsoft® Management Console) 控制台。

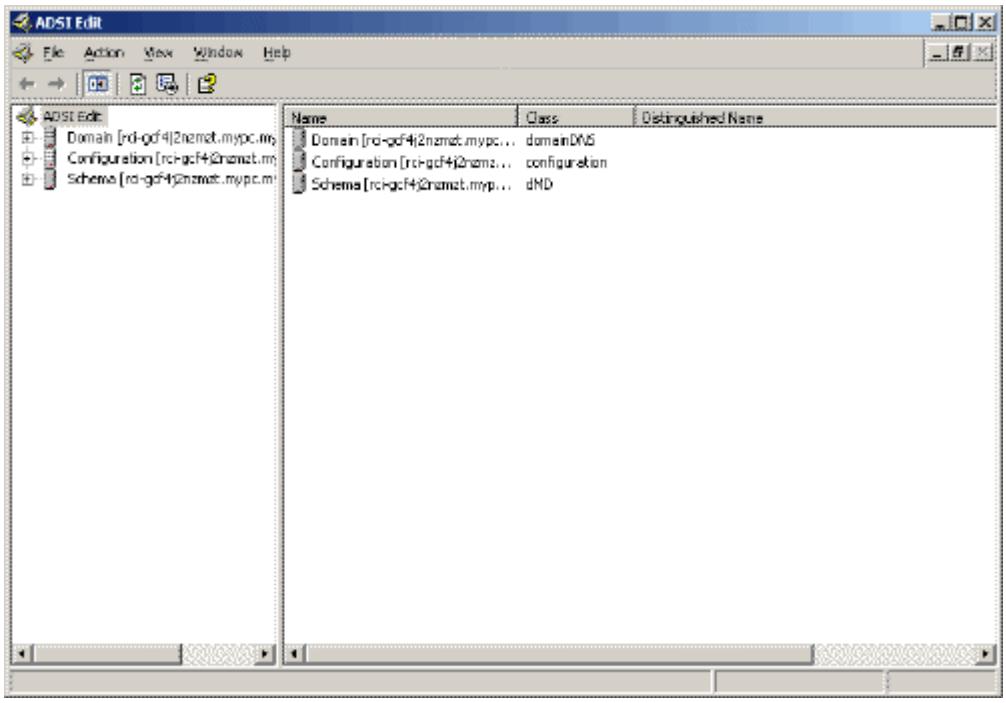
编辑用户成员的 rciusergroup 属性

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：

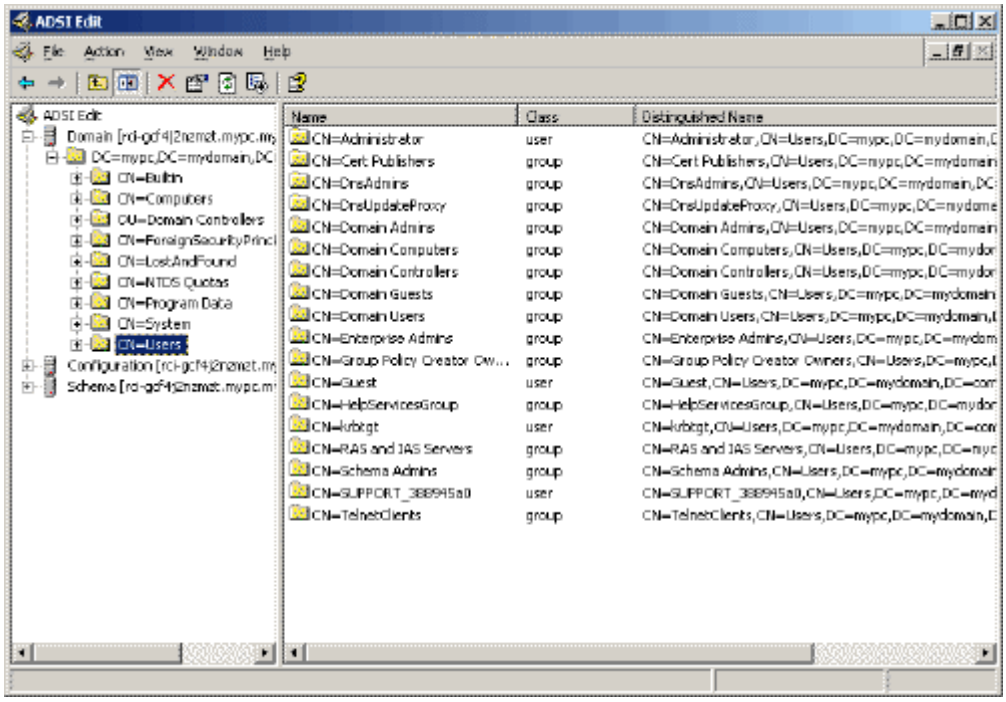
1. 在安装 CD 上选择 Support（支持）> Tools（工具）。
2. 双击 SUPTOOLS.MSI 安装支持工具。

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。



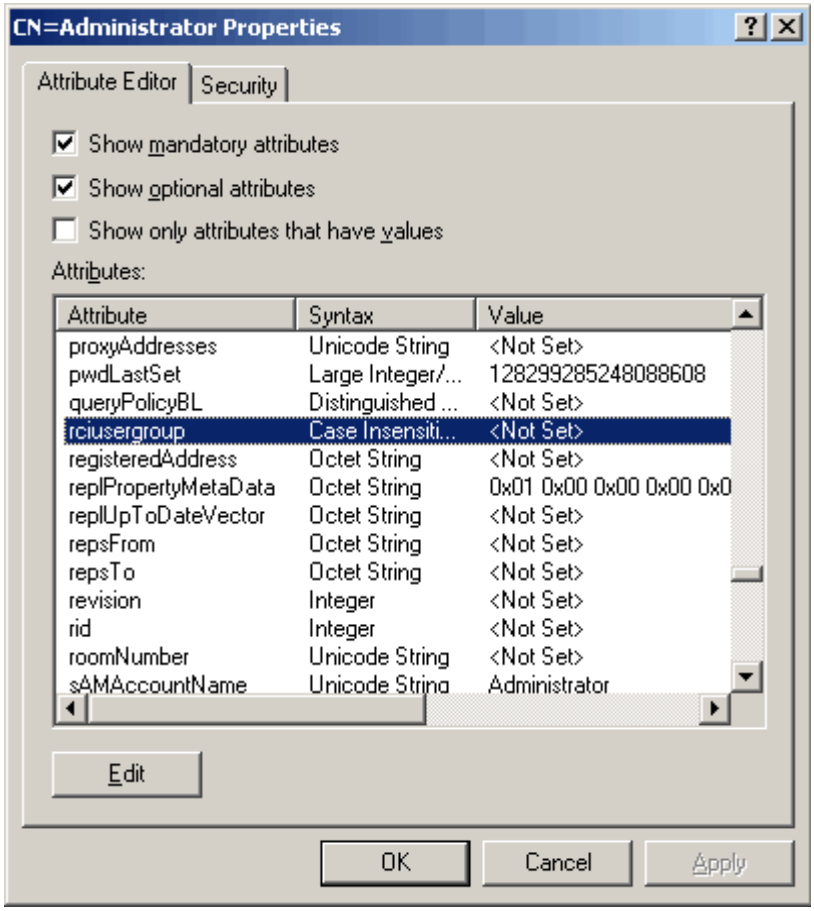
4. 打开 Domain（域）。

5. 在窗口左面板上选择 CN=Users 文件。



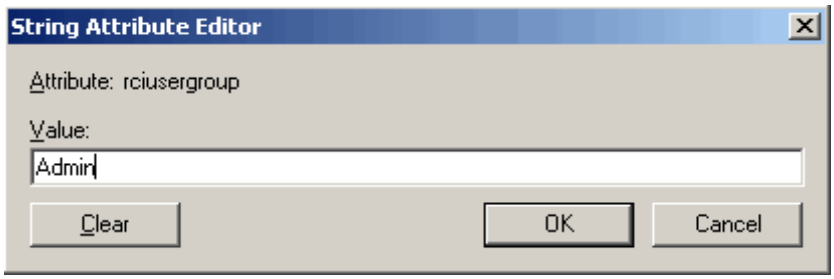
6. 在右面板上找到要调节其属性的用户名。用右键单击用户名，选择 Porperties（属性）。

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 rciusergroup。



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 III 上创建的）用户组。单击 OK（确定）按钮。

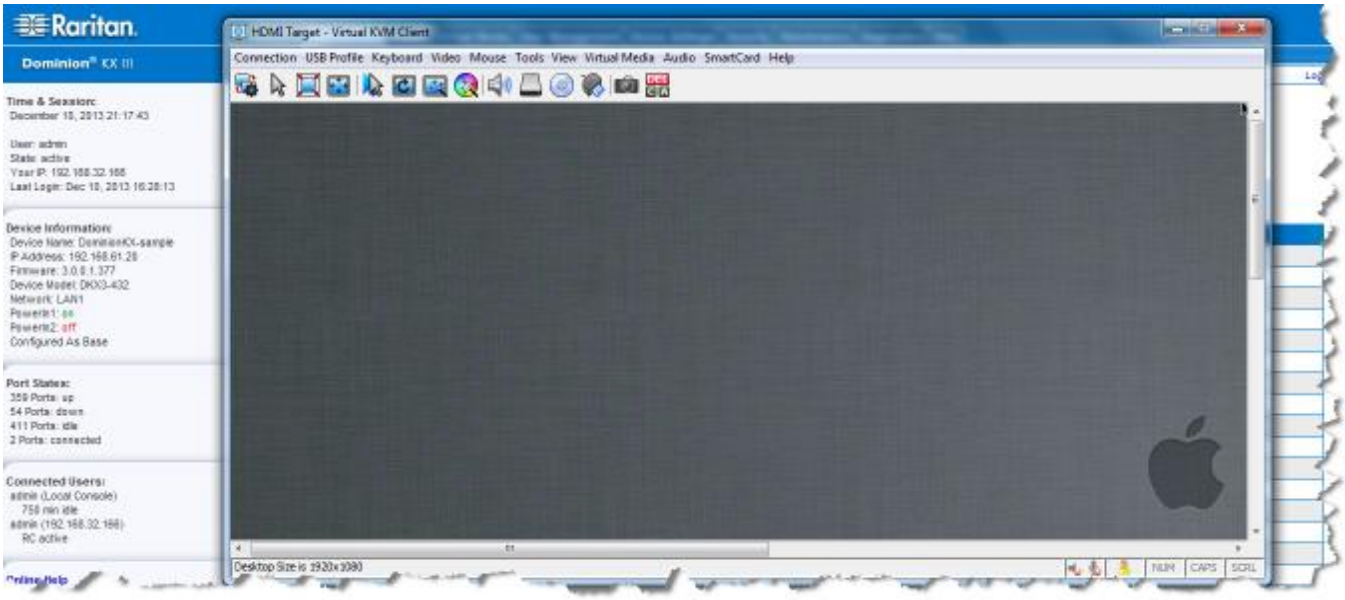


Ch 5 Virtual KVM Client (VKC) 帮助

在本章内

概述

无论何时从 KX III 的端口访问页面的 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。

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。

重要事项 :在刷新浏览器时，关闭 Virtual KVM Client 连接，所以要慎重。

Virtual KVM Client (VKC) 和 Active KVM Client (AKC) 是访问远程目标服务器所用的界面。

VKC 和 AKC 有相似的功能 除下列各项：

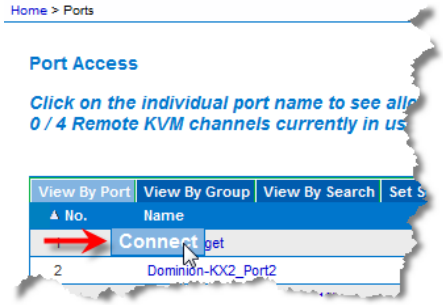
- 最低系统要求
- 支持的操作系统和浏览器
- VKC 不使用在 AKC 里创建的键盘宏。
- 直接端口访问配置（参看**启用通过 URL 进行直接端口访问**）。
- AKC 服务器证书验证配置（参看**使用 AKC 的前提** (p. 260)）。

连接到目标服务器

登录至 KX III Remote，通过 Virtual KVM Client (VKC) 或 Active KVM Client (AKC) 访问目标服务器。

连接可用目标服务器或双监视器目标服务器：

1. 单击要连接的目标服务器的“端口名称”(Port Name)。打开 Port Action（端口操作）菜单。
2. 单击 Connect（连接）。



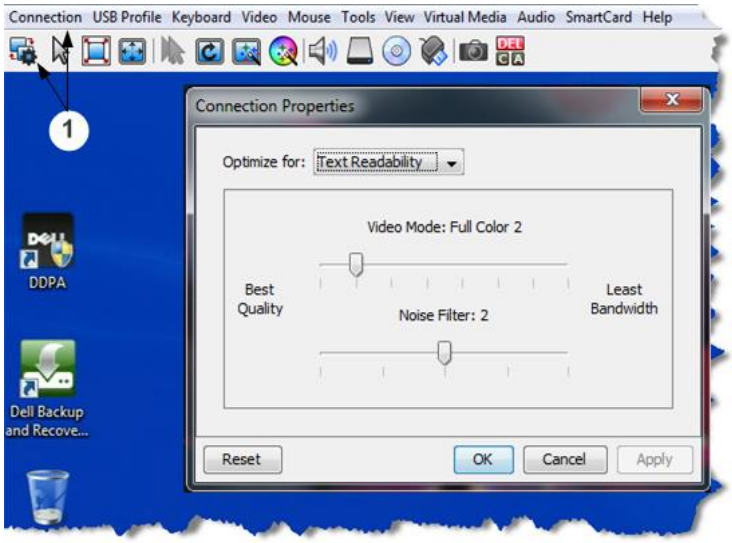
参看*端口操作菜单* (p. 20)详细了解其他可用菜单项。

配置连接属性

访问连接属性

访问连接属性：

1. 单击连接 > 属性，或单击连接...图标打开连接属性对话框。



关于连接属性

Virtual KVM Client (VKC) 和 Active KVM Client (AKC) 支持连接属性管理。

连接属性管理流视频性能而非远程连接至目标服务器。

属性只应用于你的连接 - 它们不影响其他用户通过 VKC 或 AKC 连接并访问相同目标服务器。

如果你更改连接属性，它们由 VKC 和 AKC 保留。

默认值连接属性设置 - 优化至最佳性能

KX III 已经配置，已为主要视频流环境提供最佳性能。

默认值连接设置：

- 优化：文本可读 - 视频模式的设计是为了将文本可读最大化。

  本设置对一般 IT 和计算机应用程序，例如性能服务器管理来说是理想的。

- 视频模式 - 默认至真彩色 2。

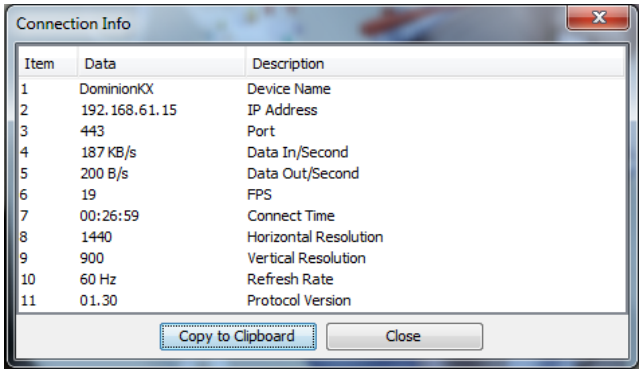
  视频帧转换质量高，24 位真彩色。本设置在使用高速 LAN 时适用。

- 噪声过滤器 - 默认 2。

  噪声过滤器设置不需要经常被改变。

任何时候，点击 Connection Properties（连接属性）对话框则复位回到默认设置。

提示：使用连接信息对话框监控实时连接。参看 **Access and Copy Connection Information（访问和拷贝连接信息）** *(p. 218)*



优化：选择

文本可读

当选择文本可读时，所有视频模式的设计是为了提供高质量、可读的文本。

此设置在使用计算机 CUI，例如执行服务器管理等时为理想状态。

在全颜色模式工作时，提供轻微的对比度提升，且文本更清晰。

在低质量视频模式中，带宽降低但准确率也降低。

颜色准确性

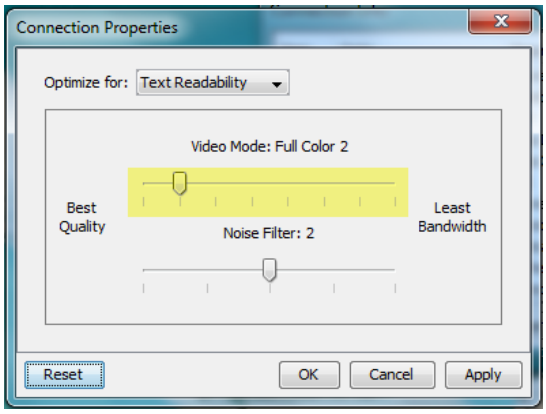
选择颜色准确性时，所有视频模式都还原为完整颜色和原色响应。

本设置适用于查看视频流，例如电影或其他广播流。

在低质量视频模式中，牺牲了如文本在内的细节清晰度。

视频模式

视频模式滑块控制每个视频帧的编码，影响视频质量、帧率和带宽。



一般来说，将滑块移至左侧会带来更高的质量，但同时会使用更高的带宽，在有的情况下，也会导致更低的帧率。

将滑块移至右侧则会带来更强的压缩，减少每帧的带宽，但同时视频质量降低。

如果在有的情况下，系统带宽为限制性因素，将视频模式滑块移至右侧可带来更高的帧率。

选择文本可读性为优化设置时，四个最右端的模式提供减少的颜色分辨率甚至无颜色。

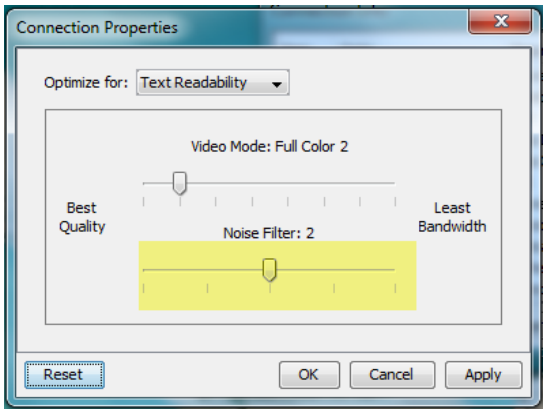
这些模式适合管理工作时使用，在管理工作中，文本和 GUI 元素优先，而带宽则为最佳。

任何时候，点击 Connection Properties（连接属性）对话框则复位回到默认设置。

Noise Filter（噪声过滤器）

除非有特殊需要，否则不要改变噪声过滤器设置。默认设置在大多数情况下可以良好工作。

噪声过滤器控制 KX III 吸收的帧间噪声量。



将噪声过滤器的滑块移至左侧可降低过滤器阀值，带来更高的动态视频质量。但是，这样更多噪声可能通过，导致跟高的带宽和更低的帧率。

将滑块移至右侧可增加阀值，使噪声更低且使用更少带宽。 视频非自然效果会大一些。

将噪声过滤器移至右侧可能在通过带宽收到严格限制的连接访问计算机 GUI 时实用。

任何时候，点击 Connection Properties（连接属性）对话框则复位回到默认设置。

连接信息

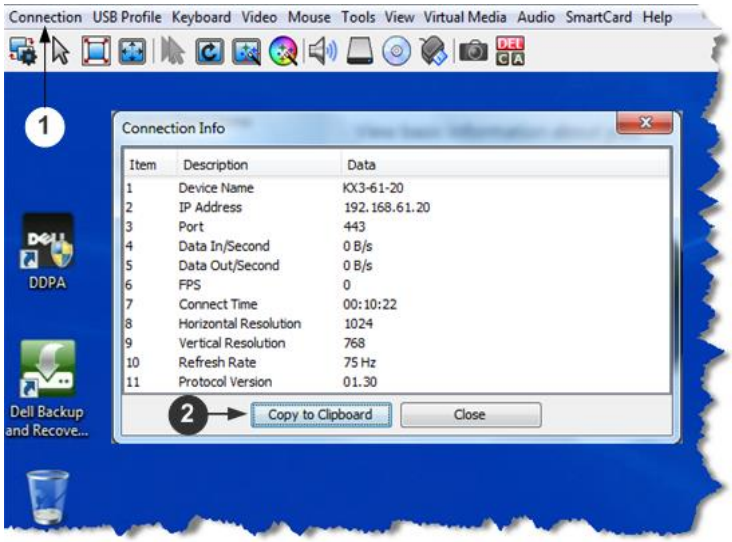
打开连接信息对话框获得实时连接信息，从对话框拷贝需要的信息。

这非常实用，例如，你想收集你目前连接的实时信息。参看***配置连接属性*** (p. 214)

显示当前连接的下列信息：

- KX III 名称 - KX III 的名称。
- IP Address（IP 地址）— KX III 的 IP 地址。
- Port（端口）— 访问 KX III 所用的 KVM 通信 TCP/IP 端口。
- Data In/Second（数据输入/秒）— 从 KX III 收集数据速率。
- Data Out/Second（数据输出/秒）— 发送给 KX III 的数据速率。
- Connect Time（连接时间）— 目前连接持续时间。
- FPS - 从 KX III 接收的视频帧/秒传输。
- 水平分辨率 - 目标服务器的水平分辨率。
- 垂直分辨率 - 目标服务器的垂直分辨率。
- 刷新速率 - 目标服务器的刷新速率。
- Protocol Version（协议版本）— Raritan 沟通协议版本。

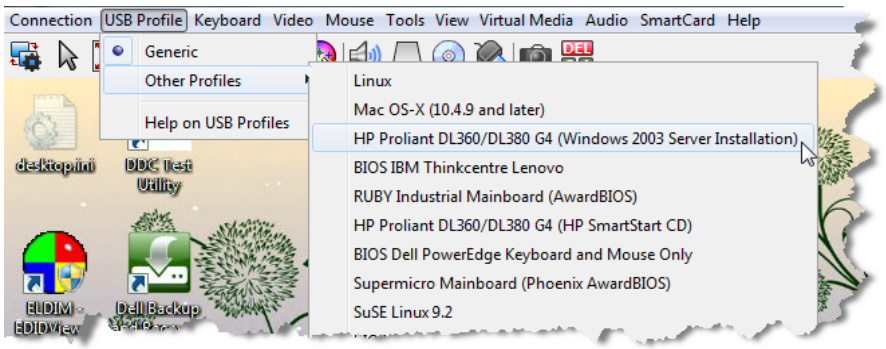
Access and Copy Connection Information（访问和拷贝连接信息）



步骤	
1	单击连接 > 信息...打开连接信息对话框。
2	单击 Copy to Clipboard（复制到剪贴板）。复制信息至你选择的文件夹。

USB 配置文件

通过点击菜单中的 USB 配置文件，为 Virtual KVM Client (VKC) 的目标服务器设置 USB 配置文件，然后从菜单选项中选择。



选择一个能最好使用 KVM 目标服务器的 USB 配置文件。

例如假如服务器正在运行 Windows® 操作系统，最好使用 Generic 配置文件。

或者，要在 BIOS 菜单上更改设置，或者要用虚拟媒体启动，BIOS 配置文件可能更合适，视目标服务器型号而定。

参看 **USB 配置文件** (p. 46)联机帮助详细了解 USB 配置文件。

键盘

发送 Ctrl+Alt+Del 宏

由于频繁使用 Ctrl+Alt+Delete，所以预先设置了 Ctrl+Alt+Delete 宏。

选择“键盘”(Keyboard) >“发送 Ctrl+Alt+Delete”(Send Ctrl+Alt+Delete)，或点击 Ctrl+Alt+Delete 键 

把此组合键发送到当前连接的目标服务器或 KVM 切换器。

反之，如果按 Ctrl+Alt+Delete 键，PC 可能要先解释此命令（这是由 Windows 操作系统的结构决定的），而不是像希望的那样把组合键发送到目标服务器。

发送 LeftAlt+Tab

选择键盘 > 发送左 Alt + Tab 以在用你连接的目标服务器或 KVM 打开 windows 间切换。

设置 CIM 键盘/鼠标选项

访问 DCIM-USBG2 设置菜单：

1. 将鼠标放在 Note Pad（Windows® 操作系统）或类似编辑器窗口上。
2. 选择 Set CIM Keyboard/Mouse（设置 CIM 键盘/鼠标）选项。这相当于将左 Ctrl 和 Num Lock 信号发送到目标服务器。然后显示 CIM 设置菜单选项。
3. 设置语言和鼠标设置。
4. 退出菜单，返回正常 CIM 功能。

向目标系统发送文本

如要把 Send Text to Target（给目标服务器发送文本）功能用于宏：

1. 点击键盘 > 向目标系统发送文本。向目标系统发送文本对话框显示。
2. 输入你想发送给目标的文本。

注意：向目标系统发送文本功能不支持非英文字母的语言。

3. 如果目标使用美国/国际键盘布局，选择“目标系统设置为美国/国际键盘布局”勾选框。
4. 单击 OK（确定）。

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，并由该目标服务器解释。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，如果你使用另一台 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。

创建在 Virtual KVM Client (VKC) 中的键盘宏不能被用在 Active KVM Client (AKC)，反之亦然。

创建一个新宏

创建键盘宏：

1. 选择“键盘”(Keyboard) >“键盘宏”(Keyboard Macros)。打开 Keyboard Macros（键盘宏）对话框。
2. 单击“添加”。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，你可以用预定义的热键执行键盘宏。**任选**
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）按钮。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：

   按住左 Alt

   按 F4。

   Esc

   释放 F4

   Esc

   释放左 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，选择该步骤，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。
9. 在菜单上选择并运行新宏，或者按给新宏指定的击键运行它。

导入宏

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：

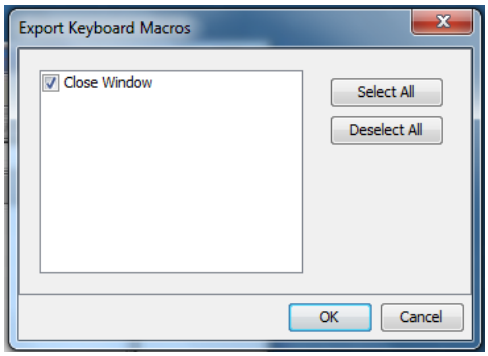
- 单击 Yes（是）按钮，用导入的宏替换现有的宏。
- 单击 Yes to All（全部是）按钮，替换当前选择的宏和找到的其他任何重复宏。
- 单击 No（否）按钮，保留原始宏，继续导入下一个宏。
- 单击 No to All（全部否）按钮，保留原始宏，继续导入下一个宏，同时跳过找到的其他任何重复宏。
- 单击 Cancel（取消）按钮取消导入。
- 还可以单击 Rename（重新命名）按钮重新命名并导入宏。如果选择 Rename（重新命名），打开 Rename Macro（重新命名宏）对话框。在字段里输入宏的新名称，然后单击 Ok（确定）按钮。关闭对话框，继续导入宏。如果输入的名称与一个现有宏的名称重复，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。一个“导出键盘宏到”的对话框显示找到并选择宏文件。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。

5. 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。

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。
- Calibrate Color（校准颜色）命令校准视频，从而增强正在显示的颜色。

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 Refresh Screen（刷新屏幕）按钮  （位于工具栏）。

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 Auto-Sense Video Settings（自动检测视频设置）按钮。

   （位于工具栏）。

  显示一条消息，说明正在进行自动调节。

校准颜色

用 Calibrate Color（校准颜色）命令优化传输的视频图像的色阶（色调、亮度和饱和度）。不同的目标服务器使用不同的颜色设置。

注意：Calibrate Color（校准颜色）命令只应用于当前连接。

▶ **执行下列操作校准颜色：**

- 选择“视频”(Video) >“校准颜色”(Calibrate Color)，或单击“校准颜色”(Calibrate Color) 按钮  （位于工具栏）。

  目标服务器屏幕反映颜色校准。

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），打开视频 Settings（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. PLL 设置 (PLL Settings)：

      Clock（时钟）— 控制显示屏幕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。

   b. 亮度 (Brightness)：该设置用于调整目标服务器显示的亮度。
   c. Brightness Red（亮度红色）— 控制目标服务器显示器的红色信号的亮度。
   d. Brightness Green（亮度绿色）— 控制绿色信号的亮度。
   e. Brightness Blue（亮度蓝色）— 控制蓝色信号的亮度。
   f. Contrast Red（对比度红色）— 控制红色信号对比度。
   g. Contrast Green（对比度绿色）— 控制绿色信号。
   h. 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 Clock（时钟）设置和 Phase（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。

i. 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。

j. 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）

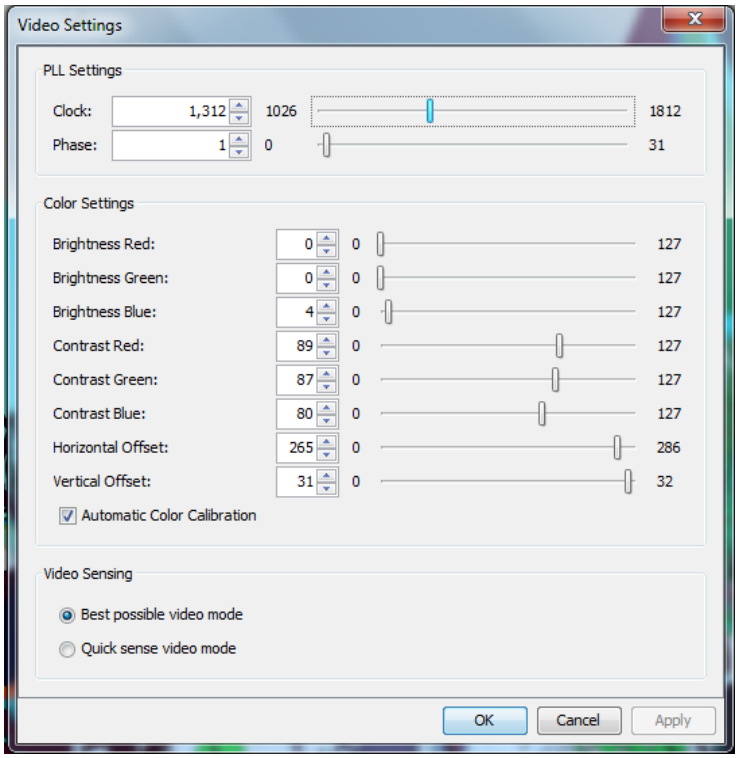
   在切换目标服务器或目标分辨率时，设备执行全面自动检测进程。选择此选项校准视频，使视频质量最佳。

   - 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。



目标服务器截屏(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。如果需要，可以采用 bitmap、JPEG 或 PNG 格式把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），或者单击目标服务器截屏按钮  （位于工具栏）。
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。

鼠标选项

在双鼠标模式下，假如适当配置此选项，两个鼠标光标重叠。

在双鼠标模式下，在控制目标服务器时，Remote Console 显示两个鼠标光标：一个是 KX III 客户机工作站的鼠标光标，另一个是目标服务器的鼠标光标。

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。

在有两个鼠标光标时，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）

当鼠标指针位于 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。

在鼠标移动时，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，你可以使用单鼠标模式，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。

双鼠标模式

绝对鼠标同步

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关于系。

具备 USB 端口的服务器支持此模式，虚拟媒体 CIM 默认使用此模式。

绝对鼠标同步 要求使用虚拟媒体 CIM：

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

▶ **进入绝对鼠标同步：**

- 选择“鼠标”(Mouse) >“绝对”(Absolute)。

注意 DVUSB CIM 上的黑色连接器用于连接键盘和鼠标。灰色连接器用于连接虚拟媒体。

用 CIM 的两个插头连接设备。如果两个插头不连接目标服务器，设备可能不能正常工作。

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。

进入智能鼠标模式

▶ **进入智能鼠标模式：**

- 选择“鼠标”(Mouse) >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。

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器鼠标保持同步，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）。

鼠标同步提示

如果你的鼠标同步出现问题：

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。KVM Client“连接信息”对话框是否显示此设备看到的实际值。
2. 单击 KVM Client 自动检测按钮，强制进行自动检测。
3. 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。
4. 单击 KVM Client 鼠标同步按钮  。

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 KVM Client 鼠标指针重叠。

执行下列操作之一同步鼠标：

- 选择 Mouse（鼠标） Synchronize Mouse（同步鼠标），或者单击 Synchronize Mouse（同步鼠标）按钮  （位于工具栏）。

注意：只能在标准鼠标模式和智能鼠标模式下使用此选项。

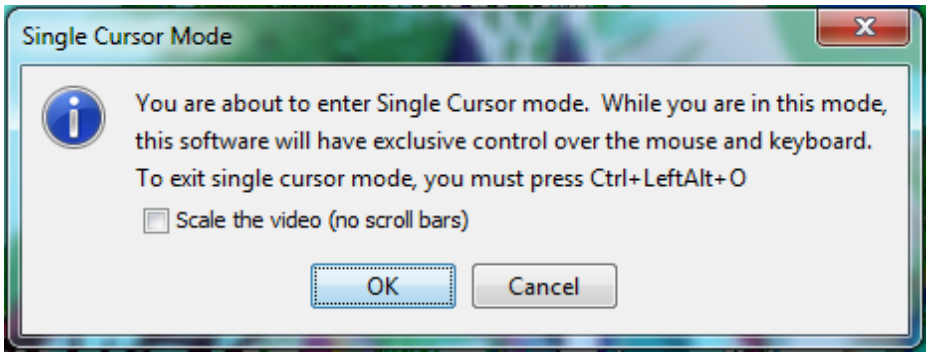
单鼠标模式

单鼠标模式只使用目标服务器鼠标光标，屏幕不再显示本地鼠标指针。

注意：在虚拟机上运行客户机时，Windows 或 Linux 目标服务器不支持单鼠标模式。

执行下列操作之一进入单鼠标模式：

- 选择“鼠标”(Mouse) >“单鼠标光标”(Single Mouse Cursor)。
- 单击 Single/Double Mouse Cursor（单/双鼠标光标）按钮  （位于工具栏）。



退出单鼠标模式：

1. 按键盘上的 Ctrl+Alt+O 退出单鼠标模式。

工具选项

常规设置

设置工具选项：

1. 点击“工具”(Tools) >“选项”(Options)。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（美国英文/国际）

- 法文（法国）
- 德文（德国）
- 日文
- 英国
- 朝鲜文（韩国）
- 法文（比利时）
- 挪威文（挪威）
- 葡萄牙文（葡萄牙）
- 丹麦文（丹麦）
- 瑞典文（瑞典）
- 德文（瑞士）
- Hungarian (Hungary)（匈牙利文[匈牙利]）
- 西班牙文（西班牙）
- 意大利文（意大利）
- 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。

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。

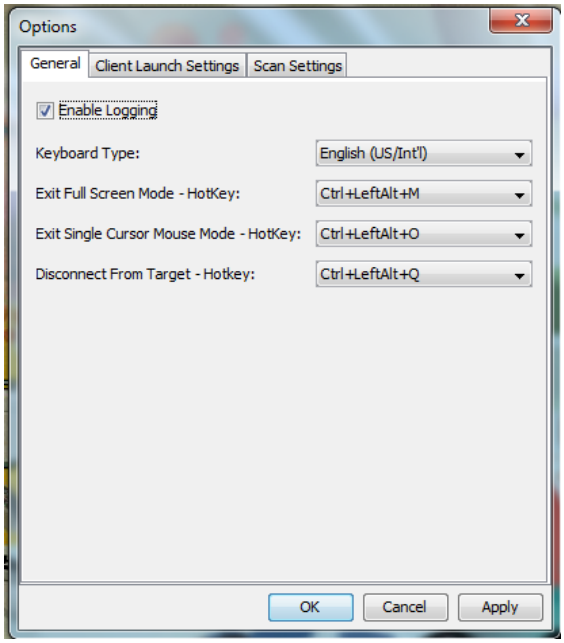
     启用此热键，使用户能迅速断开目标服务器。

   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）。



键盘限制

土耳其文键盘

如果使用土耳其文件盘，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])

语言	配置方法
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])
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。

▶ **配置客户机启动设置：**

1. 点击“工具”(Tools) >“选项”(Options)。打开 Options（选项）对话框。
2. 单击 Client Launch Settings（客户机启动设置）选项卡。
   - 配置目标窗口设置：
   a. 选择 Standard - sized to target Resolution（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 Full Screen（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 Monitor Client Was Launched from（监视器客户机旧启动方式）。

b. 选择 Select From Detected Monitors（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 Currently Selected Monitor Not Detected（检测不到当前选择的监视器）。

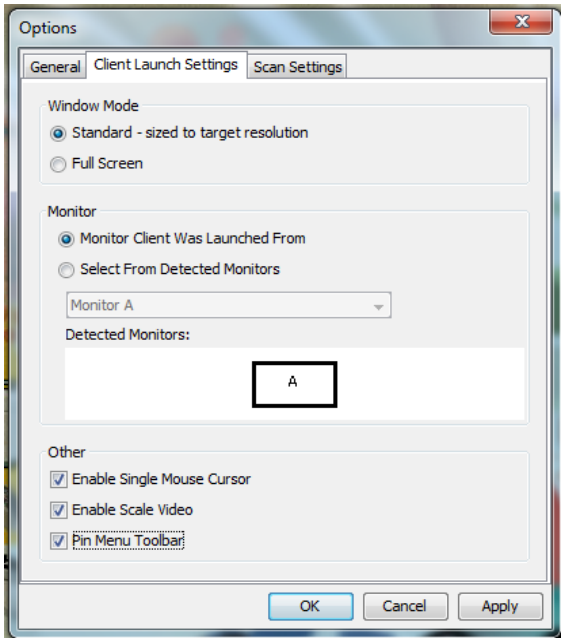
- 配置其他启动设置：

a. 选择 Enable Single Cursor Mode（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 Enable Scale Video（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 Pin Menu Toolbar（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 OK（确定）。



配置在 VKC 和 AKC 上配置端口扫描设置。

配置 VKC 和 AKC 的端口扫描选项适用于从 KX III Remote Console 扫描。

要为 Local Console 配置端口扫描选项，参看***配置本地控制台扫描选项（Configure Local Console Scan Settings)*** (参看 "***配置本地控制台扫描设置***" p. 268)

用途 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。

参看扫描端口 - 远程控制台了解详情。

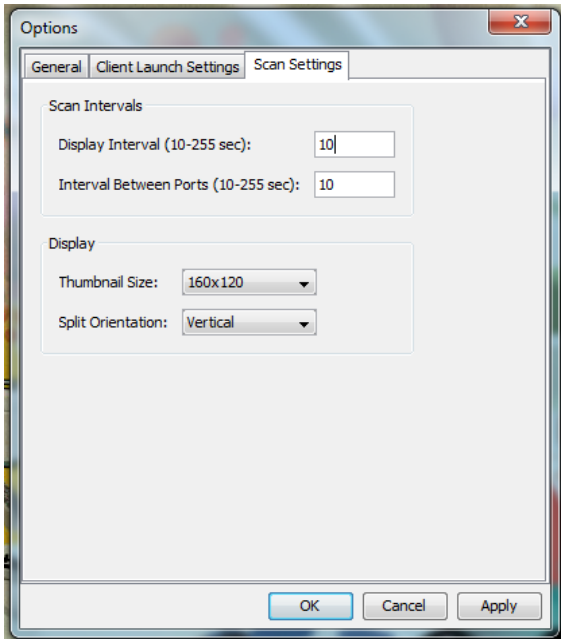
用 Scan Settings（扫描设置）选项卡定制扫描间隔时间和默认显示选项。

配置端口扫描

▶ **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“视图”(View) >“缩放”(Scaling)。

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. 232)。

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. 232)。

▶ **进入全屏模式：**

- 选择查看 > 全屏，或单击全屏按钮  。

▶ **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。

虚拟媒体

所有 KX III 设备都支持虚拟媒体。虚拟媒体允许目标服务器通过客户机 PC 和网络文件服务器远程访问媒体，从而扩展了 KVM 功能。

通过这种功能，在客户机 PC 和网络文件服务器上安装的媒体本质上是以虚拟方式安装在目标服务器上。然后目标服务器即可读写该媒体，就像与目标服务器本身物理连接的媒体一样。

每台 KX III 均支持虚拟媒体，可以用绝大部分 CD、DVD、USB、音频播放设备、音频录音设备、内置驱动器、远程驱动器和镜像文件执行远程管理任务。

虚拟媒体会话用 128 或 256 位 AES 或 RC4 加密算法加以保护。

使用虚拟媒体的前提

KX III 前提条件

- 对于需要访问虚拟媒体的用户，必须将 KX III 权限设置为允许访问相关端口，允许这些端口进行虚拟媒体访问（虚拟媒体访问端口权限）。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**任选**。
- 必须给要连接的 KVM 目标服务器选择正确的 USB 配置文件。

远程 PC

- 某些虚拟媒体选项要求远程 PC 有管理权限（例如整个设备的驱动器重定向）。

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 连接设备。
- USB 2.0 端口速度较快，首选使用此类端口。

虚拟媒体需要 CIM

你必须使用下列之一的 CIM 以使用虚拟媒体：

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

注意 DVUSB CIM 上的黑色连接器用于连接键盘和鼠标。灰色连接器用于连接虚拟媒体。

用 CIM 的两个插头连接设备。如果两个插头不连接目标服务器，设备可能不能正常工作。

安装本地驱动器

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。

安装本地驱动器备注

运行 Windows XP® 操作系统的 KVM 目标服务器，在把 NTFS 格式化分区（例如本地 C 盘）重定向到这些目标服务器之后，可能不接受新的海量存储设备连接。

如果出现这些情况，重定向另一个虚拟媒体设备，关闭 Remote Console，然后重新连接它。如果其他用户连接同一台目标服务器，他们也必须关闭目标服务器连接。

通过虚拟媒体支持的任务

虚拟媒体允许你远程执行下列任务：

- 传输文件
- 运行诊断
- 安装或修补应用程序
- 操作系统完整安装
- 数字音频录制和播放

支持的虚拟媒体类型

Windows®、Mac® 和 Linux™ 客户机支持下列虚拟媒体类型：

- 内置和外置硬盘
- 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。

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：

- 对于 Linux® 和 Mac® 客户机
- 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）

支持虚拟媒体操作系统

支持下列客户机操作系统：

- Windows® 7 操作系统
- Windows 8 操作系统
- Windows XP® 操作系统
- openSUSE® 11.4 Celadon (x86_64)
- Fedora® 18
- RHEL® 6.4
- OSX Mountain Lion® 10.7 (和更高版本)
- Solaris® 10

Active KVM Client (AKC) 可被用于安装虚拟每天类型 但仅为 Windows 操作系统

支持的虚拟每天驱动器数量

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，所以实际上可以安装另一个 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。

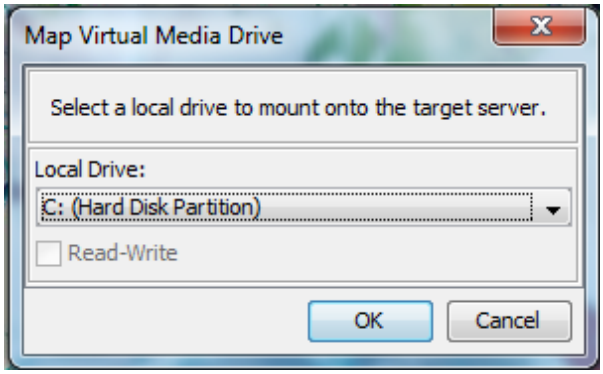
这不是前提，但在尝试访问此媒体之前，必须这样做。

连接和断开虚拟媒体

通过客户机访问虚拟媒体驱动器

▶ 访问客户计算机上的虚拟媒体驱动器：

1. 在 Virtual KVM Client 上选择 Virtual Media（虚拟媒体）> Connect Drive（连接驱动器），或点击 Connect Drive...（连接驱动器...）按钮  。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。

   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. 242)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！从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。

3. 单击 OK（确定）。采用虚拟方式将此媒体安装在目标服务器上。可以像访问其他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），或点击 Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 镜像文件）按钮  。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）。
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. 导航到要使用的磁盘镜像文件所在的路径，单击 Open（打开）。Image Path（镜像文件路径）字段自动填充该路径。
   d. 单击 Connect（连接）。
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）页上配置的那些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）。

采用虚拟方式将此媒体安装在目标服务器上。可以像访问其他驱动器一样访问此媒体。

注意：如果使用 Linux® 目标系统上的文件，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，Window 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。

断开虚拟媒体驱动器

▶ 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：使用 Disconnect（断开）命令除了断开虚拟媒体，在关闭 KVM 连接时还同时关闭虚拟媒体。

Windows XP 环境下的虚拟媒体

如果在 Windows® XP 环境下运行 Virtual KVM Client 和 Active 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

活动系统分区

不能在 Linux 客户机上安装活动系统分区。

必须在建立虚拟媒体连接之前用 umount /dev/<device label> 命令卸载 Linux Ext3/4 驱动器分区。

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

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。

为了避免这些问题，你必须是根用户。

Mac 环境下的虚拟媒体

活动系统分区

不能在 Mac 客户机上使用虚拟媒体作为活动系统分区。

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 不能读 Mac 格式化分区
- 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。

虚拟媒体文件服务器设置（仅文件服务器 ISO 镜像文件）

只有在用虚拟媒体访问文件服务器 ISO 镜像文件时，才需要此功能。ISO9660 格式是 Raritan 支持的标准，但也可以使用其他 CD-ROM 扩展。

注意：文件服务器必须支持 SMB/CIFS。

用 Remote Console File Server Setup（文件服务器设置）页指定要用虚拟媒体访问的文件服务器和镜像文件路径。在此指定的文件服务器 ISO 镜像文件，可以在 Map Virtual Media CD/ISO Image（映射虚拟媒体 CD/ISO 镜像文件）对话框上 Remote Server ISO Image（远程服务器 ISO 镜像文件）下面的 Hostname（主机名）和 Image（镜像文件）下拉列表上选择。参看***安装 CD-ROM/DVD-ROM/ISO 镜像文件*** (p. 244)。

指定要通过虚拟媒体访问的文件服务器 ISO 镜像文件：

1. 在 Remote Console 上选择 Virtual Media（虚拟媒体），打开 File Server Setup（文件服务器设置）页。
2. 选择要作为虚拟媒体访问的所有媒体对应的 Selected（选择）复选框。
3. 输入要访问的文件服务器 ISO 镜像文件的信息：
   - IP Address/Host Name（IP 地址/主机名）— 文件服务器的主机名或 IP 地址
   - Image Path（镜像文件路径）— ISO 镜像文件所在位置的全路径名例如 /sharename0/path0/image0.iso、\sharename1\path1\image1.iso 等。

   注意：主机名长度不能超过 232 个字符。
4. 单击 Save（保存）按钮。在此指定的所有媒体，可以在 Map Virtual Media CD/ISO Image（映射虚拟媒体 CD/ISO 镜像文件）对话框上选择。

注意：如果连接 Windows 2003® Server 并尝试加载服务器上的 ISO 镜像文件，系统显示错误消息："在端口安装虚拟媒体失败。不能连接文件服务器，或者文件服务器名称和密码错误。"如果发生这种情况，禁用 Microsoft Network Server:Digitally Sign Communications（Microsoft 网络服务器：数字签名通信）选项。

智能卡

使用 KX III， 可以在目标服务器上安装智能卡读卡器支持智能卡验证和相关应用。

如要了解支持的智能卡、智能卡读卡器和其他系统要求清单，参看***智能卡读卡器和最低系统要求、CIM 和支持的/不支持的智能卡读卡器*** (p. 248)。

注意：只有远程客户机支持 USB 智能卡令牌 (eToken NG-OTP)。

Local Console 还支持智能卡读卡器安装。

参看 Dominion 设备帮助中的 ***Local Console 智能卡访问*** (p. 269)。

智能卡读卡器和最低系统要求、CIM 和支持的/不支持的智能卡读卡器

在开始之前正在使用智能卡读卡器前，请查看如下信息：

- ***智能卡最低系统要求*** (p. 302)
- ***支持的计算机接口模块 (CIM) 规格*** (p. 296)
- 支持的和不支持的智能卡读卡器

访问智能卡读卡器时的验证

在远程访问服务器时，可以选择所连接的智能卡读卡器，把它安装在服务器上。

智能卡验证用于与目标服务器进行验证，并非用于登录目标服务器。因此，更改智能卡 PIN 和证书不需要更新设备帐号。

使用智能卡时的 PC Share Mode（PC 共享模式）和隐私设置

在设备上启用 PC-Share（PC 共享）模式之后，多个用户可以同时访问一台目标服务器。

但如果目标服务器连接智能卡读卡器，无论是否选择了 PC-Share（PC 共享）模式，设备都执行隐私保护策略。

此外，如果你加入目标服务器共享会话，将禁止安装智能卡读卡器，直到可以独占访问目标服务器为止。

检测到智能卡读卡器

在与目标服务器建立 KVM 会话之后，可以使用 AKC 和 VKC 上的 Smart Card（智能卡）菜单和按钮。

在 Smart Card（智能卡）按钮或 Smart Card（智能卡）从菜单选择后，一个对话框中将显示检测到的、与远程客户机相连的智能卡读卡器。

可以在此对话框上连接其他智能卡读卡器，刷新与目标服务器相连的智能卡读卡器的列表，断开智能卡读卡器。

还可以取出或重新插入智能卡。可以用此功能通知目标服务器操作系统，必须取出/重新插入智能卡才能显示相应的登录对话框。可以用此功能给一台目标服务器发送通知，但不影响其他 KVM 活动会话。

安装智能卡读卡器

在目标服务器上安装读卡器之后，可以像使用直接连接的读卡器一样使用服务器上的读卡器和智能卡。

在取下智能卡或智能卡读卡器之后，根据在目标服务器操作系统上设置的取卡策略，系统要么锁定用户会话，要么不让你退出系统。

在因关闭 KVM 会话或切换到新目标服务器而终止 KVM 会话之后，自动把智能卡读卡器从目标服务器上卸载掉。

从 AKC 或 VKC 安装智能卡读卡器：

1. 单击 Smart Card（智能卡）菜单，然后选择 Smart Card Reader（智能卡读卡器）。也可以单击 Smart Card（智能卡）按钮  （位于工具栏）。
2. 在 Select Smart Card Reader（选择智能卡读卡器）对话框上选择智能卡读卡器。
3. 单击 Mount（安装）按钮。
4. 打开进度对话框。选择 Mount selected card reader automatically on connection to targets（在连接目标服务器时自动安装选择的读卡器）复选框，在下次连接服务器时自动安装智能卡读卡器。单击 OK（确定）按钮开始安装。

更新智能卡读卡器

在 Select Smart Card Reader（选择智能卡读卡器）对话框上更新智能卡：

- 如果客户 PC 连接新智能卡读卡器，单击 Refresh List（刷新列表）。

发送智能卡取出和重新插入通知

▶ **给目标服务器发送智能卡取出和重新插入通知：**

- 选择当前安装的智能卡读卡器，然后单击 Remove/Reinsert（取出/重新插入）按钮。

卸载（移除）智能卡读卡器

▶ **卸载智能卡读卡器：**

- 选择要卸载的智能卡读卡器，然后单击 Unmount（卸载）按钮。

数字音频

KX III 支持 在远程客户机和目标服务器之间给数字音频播放和录音设备建立的端到端双向数字音频连接。

通过 USB 连接访问音频设备。

需要当前设备固件。

必须使用下列之一的 CIM：

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

支持 Windows®、Linux® 和 Mac® 操作系统。Virtual KVM Client (VKC) 和 Active KVM Client (AKC)支持连接到音频设备。

注意：虚拟媒体不支持音频 CD，所以不使用音频功能。

Raritan 建议你在开始使用音频功能之前阅读帮助文件中下列章节中关于音频的信息：

- ***支持的音频设备格式*** (p. 251)
- ***双端口视频建议*** (p. 195)
- ***支持的鼠标模式*** (参看 "***参看双视频端口组支持鼠标模式***" p. 195)
- ***双视频支持要求的 CIM*** (p. 196)
- 参考资料和***音频*** (p. 329)

支持的音频设备格式

KX III 支持 每次在一台目标服务器上只支持一台播放设备和一台录音设备。支持下列音频设备格式：

- 立体声 16 位 44.1K
- 单声道 16 位 44.1K
- 立体声 16 位 22.05K
- 单声道 16 位 22.05K
- 立体声 16 位 11.025K
- 单声道 16 位 11.025K

音频播放和录音建议及要求

音量

- 把目标服务器的音量设置为中等设置，

  例如在 Windows® 客户机上把音频设置为 50 或更低。

此设置必须在音频播放设备或录音设备上设置，不在客户机的音频设备控制部分设置。

在启用 PC 共享模式时的音频连接建议

如果在 PC 共享模式下使用音频功能，在把其他音频播放和录音设备连接到目标服务器时，音频播放和录音中断。

例如用户 A 把播放设备连接到目标服务器 1 运行音频播放应用程序，然后用户 B 把录音设备连接到同一台目标服务器。用户 A 的播放会话中断，可能需要重新启动音频应用程序。

必须用新设备配置枚举 USB 设备，所以会发生会话中断现象。

目标服务器安装新设备驱动程序可能需要一些时间。

音频应用程序可能停止播放，也可能跳到下一段，也可能继续播放，

具体情况取决于音频应用程序在设计时如何处理断开/重新连接事件。

带宽要求

下表详细说明在每种选择的格式下传输音频时的音频播放和录音带宽要求。

音频格式	网络带宽要求
44.1 KHz 16 位立体声	176 Kbps

音频格式	网络带宽要求
44.1 KHz 16 位单声道	88.2 Kbps
2.05 KHz 16 位立体声	88.2 Kbps
22.05 KHz 16 位单声道	44.1 Kbps
11.025 KHz 16 位立体声	44.1 Kbps
11.025 KHz 16 位单声道	音频 22.05 Kbps

实际上，由于在目标服务器上打开并使用音频应用程序时，键盘数据和视频数据要消耗带宽，所以连接音频设备和目标服务器所用的带宽比上述数值大。

建议你在使用播放和录音功能之前至少要包括 1.5MB 连接带宽。

但是，如果目标服务器屏幕使用很高的屏幕分辨率显示很多全彩色内容，要消耗比上述数值大得多的带宽，会严重影响音频质量。

可以采用很多建议的客户机设置，降低视频在小带宽情况下对音频质量的影响：

- 用质量较低的格式连接音频播放设备。在使用 11k 连接时，视频消耗带宽造成的影响比在使用 44k 连接时小得多。
- 在 Connection Properties（连接属性）下面，把连接速度设置为与客户机服务器连接最匹配的值。
- 在 Connection Properties（连接属性）下面，尽可能把色彩深度设置为最小值。把色彩深度降到 8 位彩色，可以大幅降低消耗的带宽
- 把 Smoothing（平滑度）设置为 High（高），通过减少显示的视频噪声来改善目标服务器视频的外观
- 在 Video（视频）设置下面，把 Noise Filter（噪声过滤器）设置为 7（最大值），当目标服务器屏幕发生变化时使用较小带宽

保存音频设置

应用 KX III 设备的音频设备设置。

在 KX III 上配置并保存音频设备设置之后，把相同的设置应用于此设备。

例如可以配置 Windows® 音频设备使用立体声 16 位 44.1K 格式。

在连接不同的目标服务器并使用此 Windows 音频设备时，把立体声 16 位 44.1K 格式应用于每个目标服务器。

对于播放和录音设备，保存应用于此设备的设备类型、设备格式和缓冲区设置。

参看***连接和断开数字音频设备*** (参看 "***从数字音频设备连接和断开***" p. 254)了解如何连接并配置音频设备，参看调节录音和播放缓冲区大小（音频设置）了解音频设备缓冲区设置。

如果在 PC 共享模式和 VM 共享模式下使用音频功能，使多个用户可以立刻访问目标服务器上的同一台音频设备，要把发起会话的用户的音频设备设置应用于要加入会话的所有用户。

因此，当用户加入音频会话时，使用目标服务器设置。 参看***在一个远程客户机上连接多台目标服务器*** (p. 253)。

在一个远程客户机上连接多台目标服务器

在一个远程客户机上同时连接四（4）台目标服务器。

参看***从数字音频设备连接和断开*** (p. 254)了解如何连接音频设备。

扬声器图标  在客户机窗口底部的状态栏显示。在不使用音频时，扬声器图标变成灰色。当扬声器和麦克风图标  显示在状态栏时，表示正在录制音频会话。

注意：在进行音频会话时，确保让会话保持活动状态，也可以更改 KX III 的闲置超时时间，使音频会话不会超时。

操作系统音频播放支持

参看下表了解每种操作系统可以用哪种 Raritan 客户机进行音频播放/录音：

操作系统	支持音频播放和录音的客户机
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC)
Linux®	• Virtual KVM Client (VKC)

操作系统	支持音频播放和录音的客户机
Mac®	• Virtual KVM Client (VKC)

从数字音频设备连接和断开

应用 KX III 设备的音频设备设置。

在 KX III 上配置并保存音频设备设置之后，把相同的设置应用于此设备。

*参看**保存音频设置*** (p. 253)了解详情。

*注意：如果在 PC 共享模式和 VM 共享模式下使用音频功能，参看***音频播放和录音建议及要求** *(p. 251)了解重要信息。 参看***在一个远程客户机上连接多台目标服务器** *(p. 253)*。

连接数字音频设备

▶ **连接音频设备：**

1. 在用浏览器建立至 KX II 的连接之前，把音频设备连接到远程客户机 PC。 KX III。
2. 在 Port Access（端口访问）页上连接目标服务器。
3. 在连接目标服务器之后，单击 Audio（音频）图标  （位于工具栏）。

   打开 Connect Audio Device（连接音频设备）对话框，列出与远程客户机 PC 相连的可用音频设备。

   注意：如果没有与远程客户机 PC 相连的可用音频设备，Audio（音频）图标变成灰色。
4. 如果当前连接播放设备，选择 Connect Playback Device（连接播放设备）。
5. 在下拉列表上选择要连接的设备。
6. 在 Format:（格式：）下拉列表上选择播放设备音频格式。

   注意：根据可用的网络带宽选择要使用的格式。采样速率较低的格式消耗的带宽较小，可以容忍较大的网络拥塞。
7. 如果当前连接录音设备，选择 Connect Recording Device（连接录音设备）。

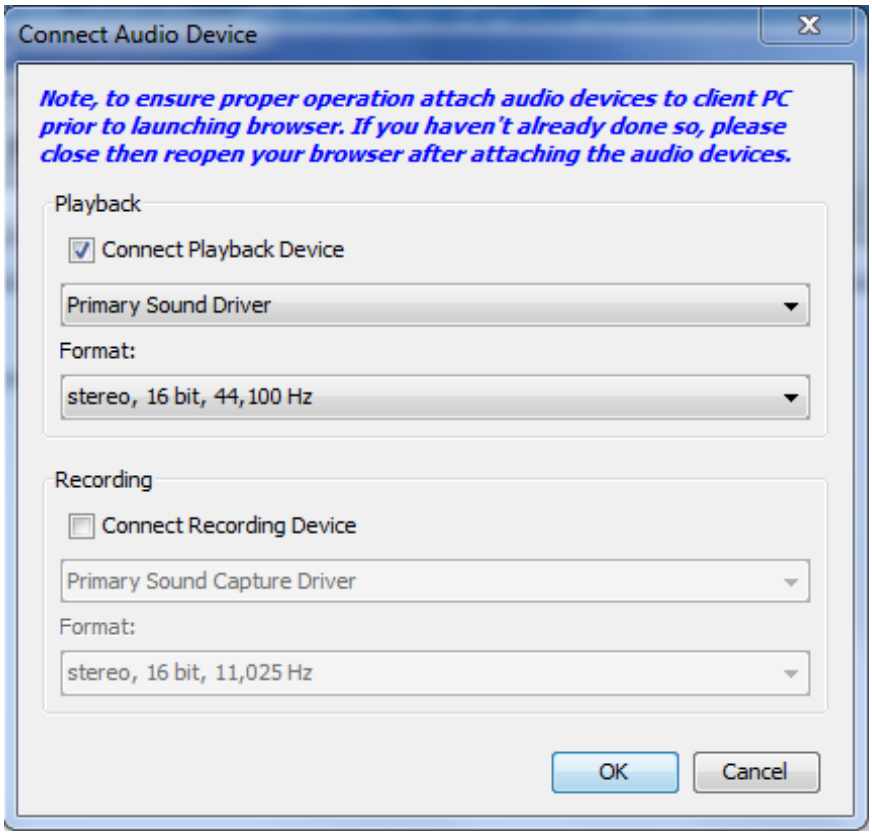
注意：对 Java 客户机而言，Connect Recording Device（连接录音设备）下拉列表列出的设备名称被截断，最长 30 个字符。

8. 在下拉列表上选择要连接的设备。
9. 在 Format:（格式：）下拉列表上选择录音设备音频格式。
10. 单击 OK（确定）。在建立音频连接之后，显示一条确认消息。单击 OK（确定）。

    如果不建立连接，显示一条错误消息。

    在建立音频连接之后，Audio（音频）菜单变成 Disconnect Audio（断开音频）。可以保存音频设备设置，并把它应用于音频设备。

    扬声器图标  在客户机窗口底部的状态栏显示。在不使用音频时，扬声器图标变成灰色。当扬声器和麦克风图标  显示在状态栏时，表示正在录制音频会话。



断开音频设备

断开音频设备：

- 单击工具栏上的 Audio（音频）图标，  当系统提示你确认断开时选择 OK（确定）按钮。显示一条确认消息。单击 OK（确定）。

调节录音和播放缓冲区大小（音频设置）

在连接音频设备之后，可以在必要时调节录音和播放缓冲区大小。

在带宽有限或网络高峰期，可以用此功能控制音频质量。

增大缓冲区大小可以提高音频质量，但可能会影响传输速度。

最大缓冲区大小是 400 毫秒，超过此值会严重影响音频质量。

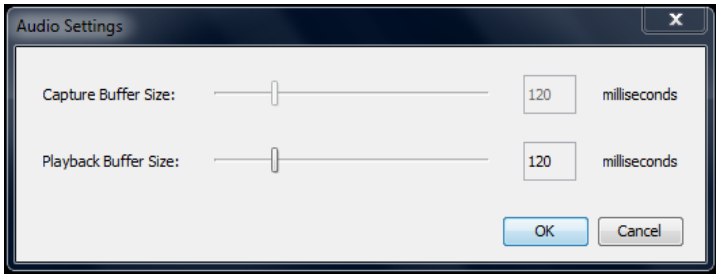
随时可以按需要调节缓冲区大小，包括在音频会话过程中。

音频设置在 AKC 或 VKC 上配置。

调整音频设置

调整音频设置：

1. 在 Audio（音频）菜单上选择 Audio Settings（音频设置），打开 Audio Settings（音频设置）对话框。
2. 按需要调节录音和/或播放缓冲区大小，单击 OK（确定）。



版本信息 - 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）按钮将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 6 Active KVM Client (AKC) 帮助

在本章内

概述

Active KVM Client (AKC) 的依据为 Microsoft Windows .NET® 技术。

这允许用户在不使用 Java® Runtime Environment (JRE) 的 Windows 环境下运行此客户机，而运行 Raritan Virtual KVM Client (VKC) 需要 Java Runtime Environment (JRE)。。

AKC 还可与 CC-SG 一起工作。

AKC 和 VKC 具有相似的功能，只有下列各项除外：

- VKC 不使用在 AKC 里创建的键盘宏。
- 直接端口访问配置（参看启用通过 URL 进行直接端口访问）。
- AKC 服务器证书验证配置（参看*使用 AKC 的前提* (p. 260)）。
- AKC 自动加载收藏夹，VKC 则不会。参看管理收藏夹。

如需获取功能的详细信息，参看 ***Virtual KVM Client (VKC) 帮助*** (p. 212)。

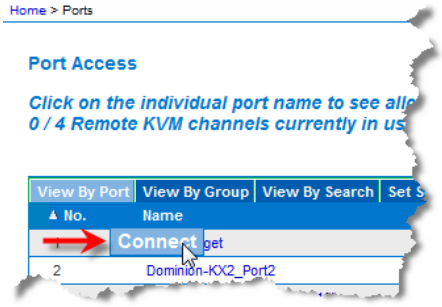
连接到目标服务器

登录至 KX III Remote，通过 Virtual KVM Client (VKC) 或 Active KVM Client (AKC) 访问目标服务器。

连接可用目标服务器或双监视器目标服务器：

1. 单击要连接的目标服务器的“端口名称”(Port Name)。打开 Port Action（端口操作）菜单。

2. 单击 Connect（连接）。



参看*端口操作菜单* (p. 20)详细了解其他可用菜单项。

AKC 支持 Microsoft .NET Framework

Active KVM Client(AKC) 需要 Windows .NET® 3.5、4.0 或 4.5 版本。AKC 可以同时使用 3.5 和 4.0。

AKC 支持的操作系统

在 Internet Explorer® 上启动 Active KVM Client（AKC） 时，可以通过 KX III 访问目标服务器。

AKC 与下列平台兼容：

- Windows XP® 操作系统
- Windows Vista® 操作系统（64 位）
- Windows 7® 操作系统（64 位）
- Windows 8® 操作系统（64 位）

注意：如果打开 WINDOWS PC FIPS，并用 AKC 和智能卡访问目标服务器，必须使用 Windows 7。

由于运行 AKC 需要 .NET，如果没有安装 .NET，或者安装了不支持的 .NET 版本，将显示一条消息告诉你检查 .NET 版本。

注意：Raritan 建议 Windows XP® 操作系统用户在启动 AKC 之前确认是否安装了 .NET 3.5 或 .NET 4.0。如果不确认已安装的 .NET 版本是否能正常工作，系统可能会提示你下载一个文件，而不是显示默认消息提醒你检查 .NET 版本。

AKC 支持的浏览器

- Internet Explorer® 8 （和更高版本）

  如果尝试在除 IE 8 （和更高版本）之外的浏览器上打开 AKC，系统显示一条错误消息告诉你检查浏览器并切换到 Internet Explorer。

使用 AKC 的前提

允许 Cookies

确保当前不阻止来自正在访问的设备的 IP 地址的 cookies。

在“Trusted Sites Zone（信任网站区域）”中包括 KX III IP 地址

Windows Vista®、Windows® 7 和 Windows 2008 服务器用户应该确保正在访问的设备的 IP 地址位于浏览器的 Trusted Sites Zone（信任网站区域）。

禁用“保护模式”。

Windows Vista®、Windows® 7 和 Windows 2008 服务器用户应该确保在访问设备时不在 Protected Mode（保护模式）下。

启用 AKC 下载服务器证书验证

如果设备或 CC-SG 管理员启用了 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）选项：

- 管理员必须把有效证书上载到设备上，或者在设备上生成自签名证书。证书必须有有效主机名。
- 每个用户必须把 CA 证书（或自签名证书）添加到浏览器的 Trusted Root CA 仓库。

在 CC-SG Admin Client 上启动 Active KVM Client 时，必须有 JRE™ 1.7.x（或更高版本）。

Ch 7 KX III Local Console - KX III End User Help（终端用户帮助）

在本章内

概述

本地控制台界面接口从机架的 KX III 访问。

这部分包括本地控制台的终端用户执行的任务。

访问目标服务器

▶ **访问目标服务器：**

1. 单击要访问的目标服务器的 Port Name（端口名称）。显示 Port Action（端口操作）菜单。
2. 在 Port Action（端口操作）菜单上选择 Connect（连接）。监视器切换到目标服务器界面。

Local Console 视频分辨率

显示器连接到 KX Local Console 上时，KX III 检测到显示器的原始分辨率。这是显示器支持的最大分辨率。

只要 Local Console 支持显示器的原始分辨率，KX III 则会使用该分辨率。

如果 Local Console 不支持原始分辨率，且显示器和 Local Console 不支持其他分辨率，则 KX III 使用连接到 Local Console 的最后一台显示器的分辨率。

例如，你连接了分辨率设置为 1600x1200@60Hz 的显示器到 KX III Local Console。KX III 则使用该分辨率，因为 Local Console 支持此分辨率。

如果你连接到 Local Console 的下一个显示器分辨率不被支持，则 KX III 使用值为 1024x768@60 的分辨率。

如需获取支持的 Local Console 视频分辨率，参看 ***Supported KX III Local Port DVI Resolutions（支持的 KX III 本地端口 DVI 分辨率）*** (p. 296)。

也可查看*视频模式和分辨率备注* (p. 324)获取其他信息。

并发用户

KX III Local Console 提供一个独立访问路径，可以访问相连的 KVM 目标服务器。

在使用本地控制台时，并不妨碍其他用户同时通过网络连接目标服务器。即使远程用户连接了 KX III，你也可以在机架上同时通过本地控制台访问服务器。

热键和连接键

由于 KX III Local Console 界面被你访问的目标服务器的界面取代了，所以用热键断开目标服务器，返回本地端口 GUI。

用连接键连接目标服务器，在多台目标服务器之间来回切换。

在显示目标服务器时，可以用本地端口热键迅速返回 KX III Local Console 用户界面。

参看 KX III Local Console 本地端口设置了解详情。

返回 KX III Local Console 界面

从目标服务器返回 KX III Local Console：

- 迅速按两次 Scroll Lock 键。

  监视器从目标服务器界面切换到 KX III Local Console 界面。

可以在 Local Port Settings（本地端口设置）页上更改此键组合。在 **Local Console 上配置 KX III 本地端口设置**。

连接键示例

标准服务器

连接键操作	热键例子
在本地端口 GUI 上访问端口	在本地端口 GUI 上访问端口 5： • 按住左 ALT > 按 5 > 释放左 ALT
切换端口	从目标服务器端口 5 切换到端口 11： • 按住左 ALT > 按 1 > 按 1 > 释放左 ALT
断开目标服务器，返回本地端口 GUI	断开目标服务器端口 11，返回本地端口 GUI（连接目标服务器所用的页面）： • 双击 Scroll Lock

刀片服务器机箱

连接键操作	热键例子
在本地端口 GUI 上访问端口	访问端口 5、插槽 2： • 按住左 ALT > 按并释放 5 > 按并释放 ->按并释放 2 > 释放左 ALT
切换端口	从目标服务器端口 5、插槽 2 切换到端口 5、插槽 11： • 按住左 ALT > 按并释放 5 > 按并释放 ->按并释放 1 > 释放左 ALT
断开目标服务器，返回本地端口 GUI	断开目标服务器端口 5、插槽 11，返回本地端口 GUI（连接目标服务器所用的页面）： • 双击 Scroll Lock

Sun 特殊组合键

在本地端口上使用下列 Sun Microsystems™ 服务器特殊组合键。在连接 Sun 目标服务器之后，可以在 Keyboard（键盘）菜单上访问这些特殊组合键：

Sun 键	本地端口组合键
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	没有组合键
Power	没有组合键

扫描端口 — Local Console

使用扫描选择的目标服务器并用单独缩略图的幻灯视图显示找到的目标服务器。

这项功能使你每次可以监视最多 32 台目标服务器，因为你可以在每个目标服务器在幻灯试图显示时单独查看每个目标服务器。

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。

对于双视频端口组，主端口包含在端口扫描中，但是从远程客户机连接时，次端口不包含在内。在从 Local Port（本地端口）进行扫描时两个端口均可包含在内。

单击任何目标服务器的缩略图以退出扫描模式并连接至服务器，或使用 Local Port ConnectKey（本地端口连接键）序号。

要退出扫描模式，点击缩略视图 Stop Scan（退出扫描）键，或使用 DisconnectKey（断开连接键）序号热键。

注意：从 Remote Console 和 Local Console 都可用扫描端口功能，但是功能稍有不同。 参看扫描端口 - 远程控制台了解详情。

扫描端口滑块显示 — Local Console

在开始扫描时，打开 Port Scan（端口扫描）窗口。

在发现每台目标服务器之后，幻灯视图用缩略图形式显示此目标服务器。

幻灯视图根据默认的 10 秒间隔时间或你指定的间隔时间对目标服务器缩略图进行翻页。

当扫描功能对目标服务器翻页时，页面中央显示的目标服务器是幻灯的核心。

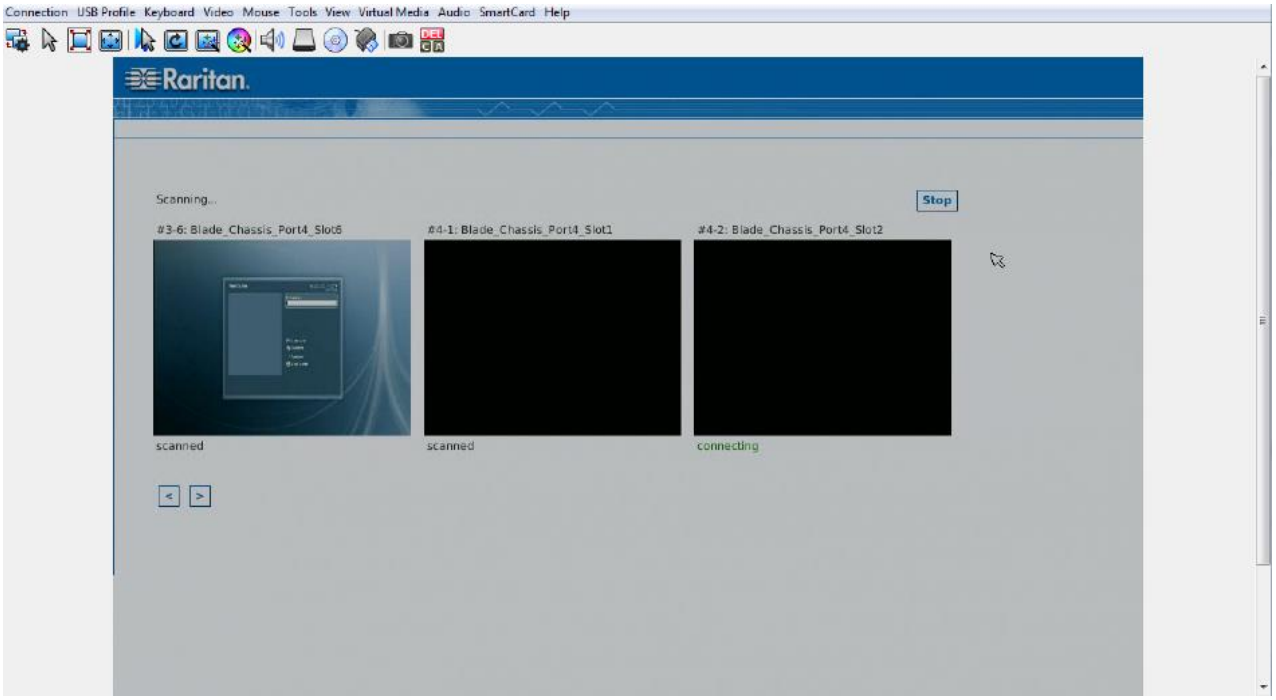
目标服务器缩略图下面显示目标服务器名称，窗口底部的任务栏也显示目标服务器名称。

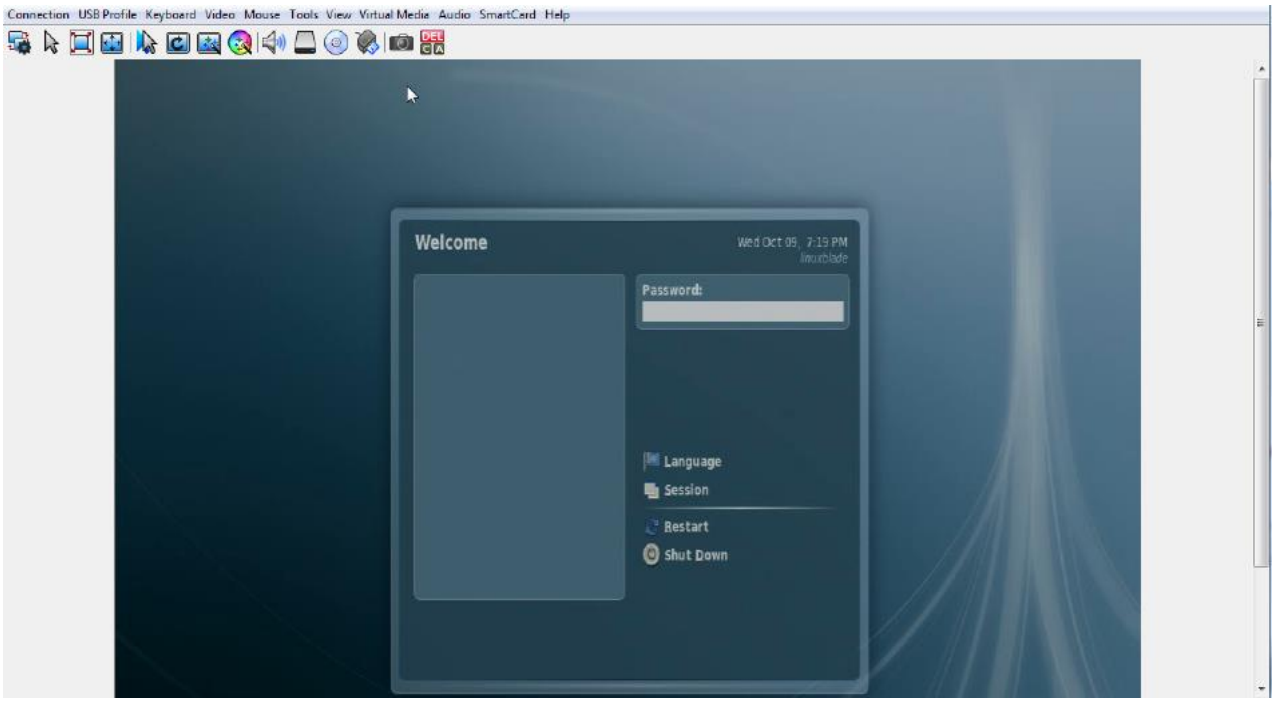
如果目标服务器忙，显示空白屏幕，而不显示目标服务器访问页。

配置滑块显示缩略图的轮换时间和 Local Port Settings（本地端口设置）页面的缩略图关注时间间隔。

参看 ***配置本地控制台扫描设置*** (p. 268)

*注意：在 Virtual KVM Client (VKC) 或 Active KVM Client (AKC) 上为 Remote Console 配置扫描设置。参看*在 **VKC** 和 **AKC** 上配置端口扫描设置 *(参看 "*配置在 **VKC** 和 **AKC** 上配置端口扫描设置。*" p. 237)。*



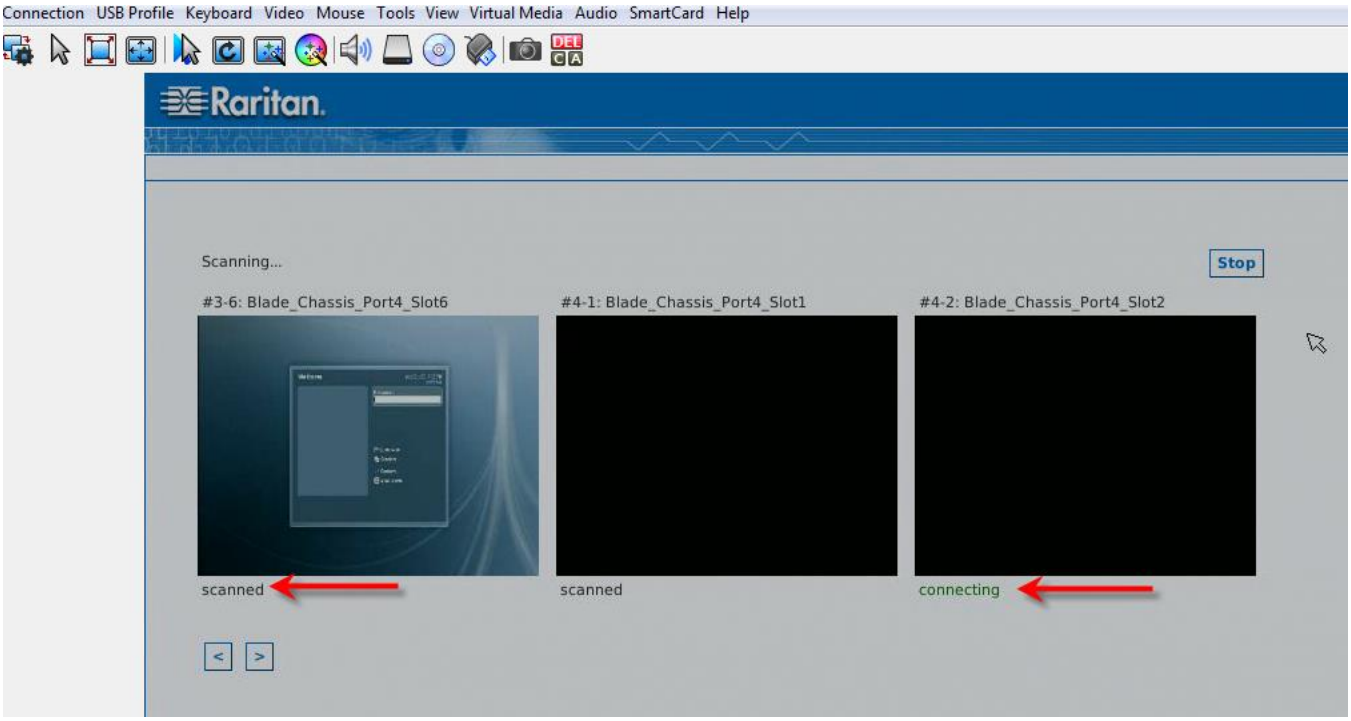

Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Welcome
Wed Oct 09, 7:19 PM
linuxblade
Password:
Language
Session
Restart
Shut Down

端口扫描时目标状态指示灯 - Local Console

Local Console 的缩略图，每个目标服务器的状态都显示在页面的缩略图下直到其为滑块显示模式。

每个目标服务器的扫描状态显示为：

- 未扫描
- 正在连接...
- 已扫描
- 跳过



配置本地控制台扫描设置

按照如下操作配置本地控制台端口选项。

*注意：在 Virtual KVM Client (VKC) 或 Active KVM Client (AKC) 上为 Remote Console 配置扫描设置。参看*在 VKC 和 AKC 上配置端口扫描设置 *(参看 "*配置在 VKC 和 AKC 上配置端口扫描设置。*" p. 237)。*

▶ **配置本地控制台端口设置：**

1. 在 Local Console 上选择 Device Settings（设备设置）。

2. 在 Local Port Settings（本地端口设置）部分，选择 Local Port Scan Mode（本地端口扫描模式）。
3. 根据需要更改间隔时间。
   - 间隔时间 - 更改扫描显示间隔时间。
   - 端口间时间间隔 - 更改扫描时转换到不同端口的间隔时间。

扫描目标服务器 - Local Console

▶ **扫描目标服务器：**

1. 单击 Port Access（端口访问）页上的 Set Scan（设置扫描）选项卡。
2. 选择每台目标服务器左边的复选框选择要扫描的目标服务器，或者选择目标服务器列上面的复选框选择所有目标服务器。
3. 如果只想扫描工作的目标服务器，选择 Up Only（仅工作的）复选框。如果要扫描所有目标服务器（无论工作还是停机），取消此复选框。
4. 单击 Scan（扫描）按钮开始扫描。

   在扫描每台目标服务器之后，本页用幻灯视图显示此目标服务器。

Local Console 智能卡访问

为了在 Local Console 上用智能卡访问服务器，必须使用 KX III 的其中一个 USB 端口，把 USB 智能卡读卡器插入 KX III。

在 KX III 上插拔智能卡读卡器之后，KX III 自动检测智能卡读卡器。

参看支持的和不支持的智能卡读卡器和*智能卡最低系统要求* (p. 302)了解支持的智能卡清单和其他系统要求。

在目标服务器上安装读卡器之后，可以像使用直接连接的读卡器一样使用服务器上的读卡器和智能卡。

在取下智能卡或智能卡读卡器之后，根据在目标服务器操作系统上设置的取卡策略，系统要么锁定用户会话，要么不让你退出系统。

在因关闭 KVM 会话或切换到新目标服务器而终止 KVM 会话之后，自动把智能卡读卡器从目标服务器上卸载掉。

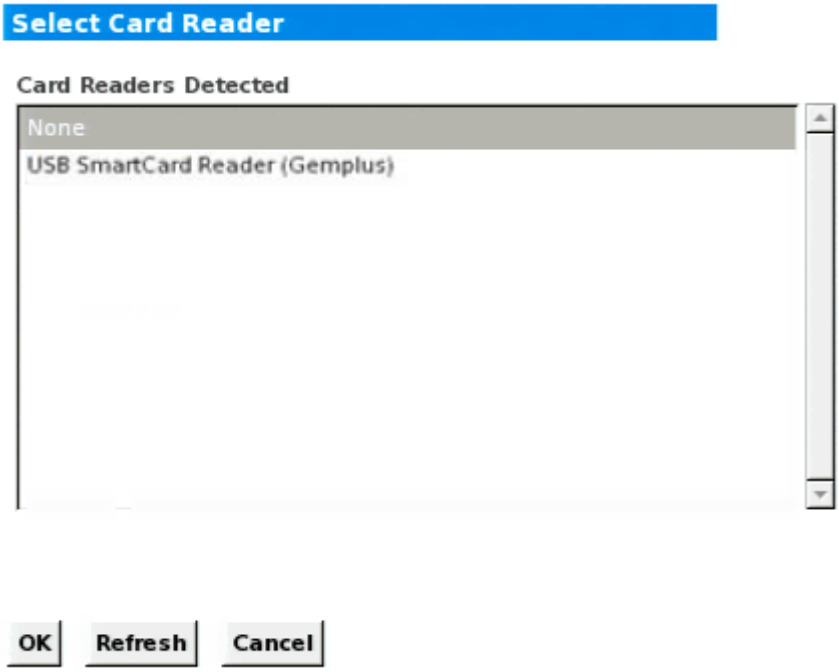
▶ **通过 KX III Local Console 把智能卡安装在目标服务器上：**

1. 使用 KX III 的其中一个 USB 端口，把 USB 智能卡读卡器插入此设备。在连接智能卡读卡器之后，KX III 检测智能卡读卡器。
2. 单击 Local Console 上的 Tools（工具）。

3. 在 Card Readers Detected（检测到的读卡器）列表上选择智能卡读卡器。如果不想安装智能卡读卡器，选择 None（无）。
4. 单击 OK（确定）按钮。在添加智能卡读卡器之后，页面显示一条消息，说明你成功完成了操作。在页面左面板上的 Card Reader（读卡器）下面，显示 Selected（已选择）或 Not Selected（未选择）状态。

更新检测到的读卡器列表：

- 如果安装了新智能卡，单击 Refresh（刷新）按钮。刷新 Card Readers Detected（检测到的读卡器）列表，反映新添加的智能卡读卡器。



Local Console USB 配置文件选项

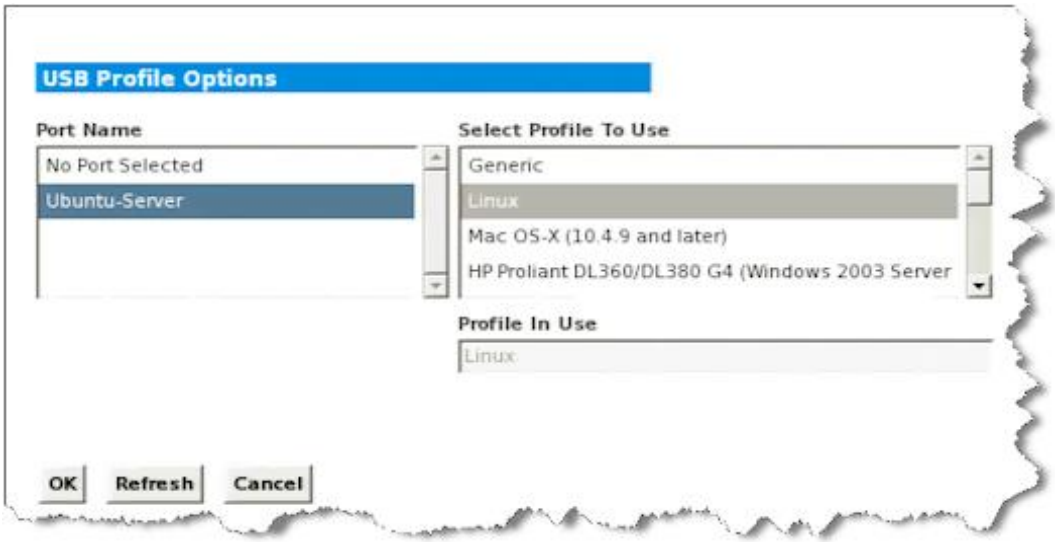
在 Tools（工具）页的 USB Profile Options（USB 配置文件选项）部分选择可用的 USB 配置文件。

Port Name（端口名称）字段显示可以指定配置文件的端口，在选择端口之后，Select Profile To Use（选择要使用的配置文件）字段显示可供此端口使用的配置文件。Profile In Use（使用的配置文件）字段显示给端口选择的配置文件。

把 USB 配置文件应用于 Local Console 端口：

1. 在 Port Name（端口名称）字段里选择要把 USB 配置文件应用于哪个端口。

2. 在 Select Profile to Use（选择要使用的配置文件）字段里给端口选择要使用的配置文件。
3. 单击 OK（确定）按钮把 USB 配置文件应用于本地端口，Profile In Use（使用的配置文件）字段显示此配置文件。



KX III Local Console 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** (p. 165)。*

执行出厂复位：

1. 选择“维护”(Maintenance) >“出厂复位”(Factory Reset)。打开 Factory Reset（出厂复位）页。
2. 在下列选项中选择合适的复位选项：
   - Full Factory Reset（全出厂复位）— 删除整个配置，将设备彻底复位到出厂默认值。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。
   - Network Parameter Reset（网络参数复位）— 将设备的网络参数复位到默认值（单击 Device Settings（设备设置）> Network Settings（网络设置）访问这些信息）。
3. 单击 Reset（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 OK（确定）按钮继续。在复位结束之后，KX III 设备自动重新启动。

用设备上的复位按钮复位 KX III

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 Encryption & Share（加密和共享）页上定义。参看加密与共享 （在联机帮助中）。

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** (p. 165)。*

复位设备：

1. 断开 KX III 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 III 设备电源。
4. 按住复位按钮 10 秒钟。

Ap A Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality（连接 KX III 和 Cat5 Reach DVI - 提供延展的当地端口功能）

在本章内

概述

扩展的本地端口将本地端口的范围扩大到 KX II 位置的机架之外，例如至另一个 KVM 切换器。

可以通过配置 KX III 使其与 Raritan Cat5 Reach DVI 发送器和接收器搭配而实现，发送器和接收器随后连接至远程控制器或其他设备。

连接到 Cat5 Reach DVI 后，KX III 可以在最远 500 英尺（152 米）处被访问。

通过黛西链接 Ethernet 切换器延长器连接 KX III 到 Cat5 Reach DVI 可将 KX III 的范围扩大到最大 3000 英尺（914 米）。

关于 Cat5 Reach DVI

如需获取 Cat5 Reach DVI 的详细信息，参看 ***Raritan Support 页面 http://www.raritan.com/support***的 Cat5 Reach DVI 联机帮助。

Contact Raritan（联系 Raritan）(***http://www.raritan.com/contact-us/***)获取 Cat5 Reach DVI 的更多信息，或获取关于购买的相关信息。

连接一个 KX III 和 Cat5 Reach DVI

注意：用在图解中的图片不是专门针对 KX III 的，但是连接是准确的。

这部分介绍了关于 KVM 切换器的三个场景。

- 将任何 KVM 切换器和其本地控制台与 Cat5 Reach DVI 相连。
- 在两个 KVM 切换器间连接 Cat5 Reach DVI。
- 将一台电脑/服务器和一个 KVM 切换器中间连接 Cat5 Reach DVI。

在连接前关闭所有设备。

如需获取设置本地和远处控制台的信息，参看 **Cat5 Reach DVI 帮助**中的 **Connecting a Keyboard/Mouse/Video Source（连接一个键盘、鼠标、视频资源）**获取更多信息。

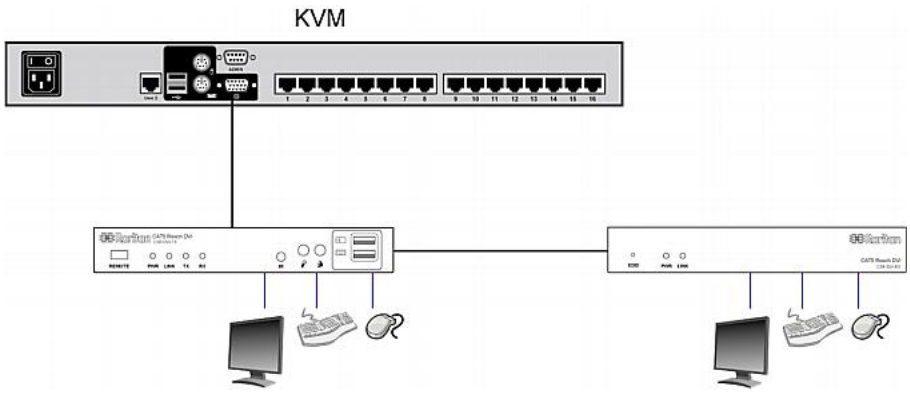
要连接 KX III 和 Cat5 Reach DVI：

1. 如果尚未连接，分别设置有 Cat5 Reach DVI 发送器和接收器的本地和远处控制台。

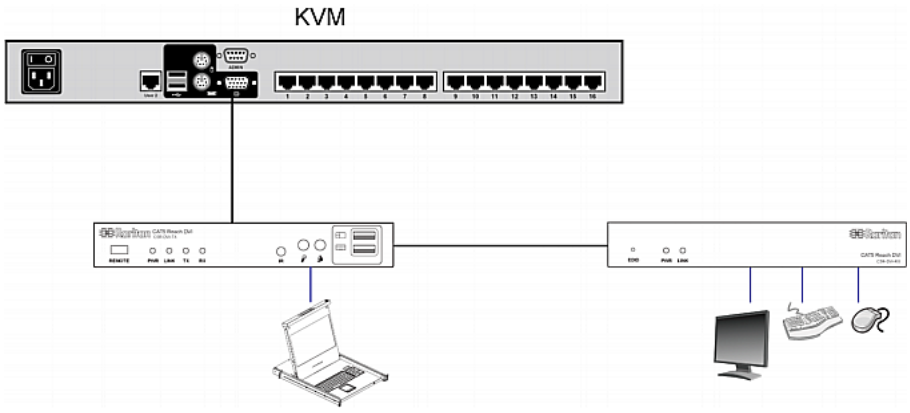
   参看 **Cat5 Reach DVI 帮助**中的 **Basic Installation（基本安装）**获取更多信息。

2. 使用 Cat5r/6 电缆连接发送器和接收器。
3. 分别把发送器和接收器插入合适的电源。
4. 将 KVM 切换器的本地控制台端口连至发送器。
   a. 将 Raritan 提供的 DVI 电缆的一头插入发送器的 DVI-I IN 端口，另一头则插入 KVM 切换器的视频端口。
   b. 将 Raritan 提供的 USB- B 连接器插入发送器的 USB- B 端口，另一头则插入 KVM 切换器的本地 USB -A 端口。

5. 打开 KVM 切换器。



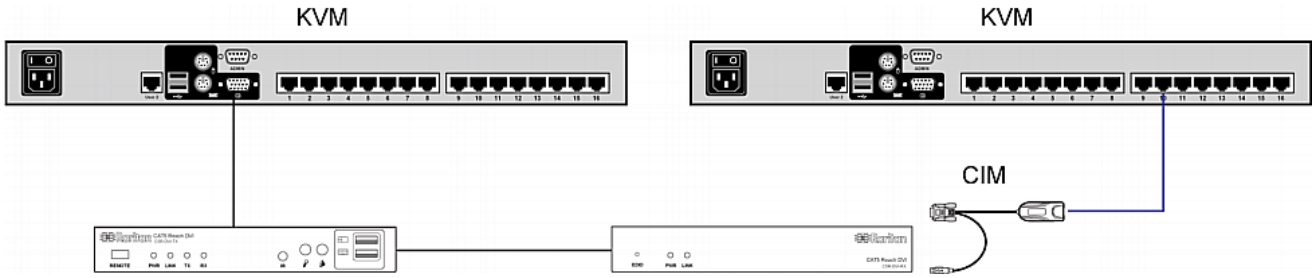
提示：本地或远程控制台可以装备 KVM 可折叠式切换器而非一系列键盘、鼠标和显示器。请参看下面的解释。



如需增加两个分层 KVM 切换器间的距离：

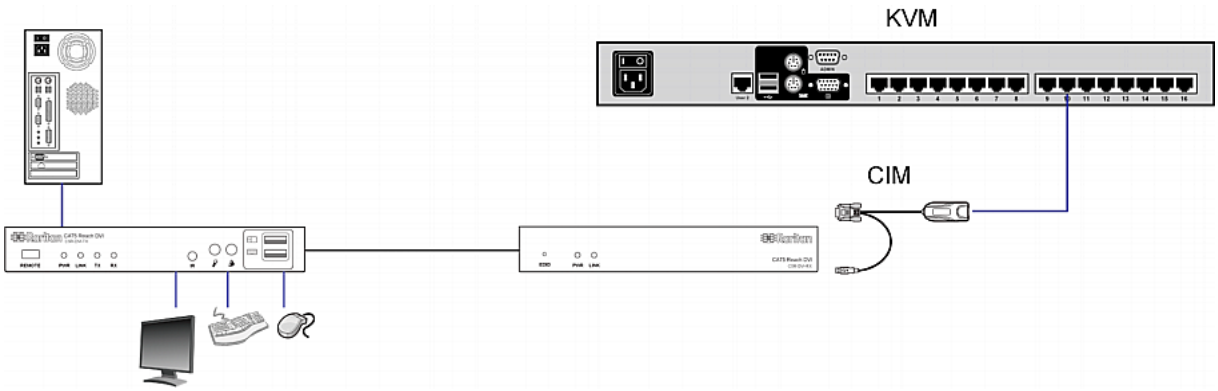
1. 通过将接收器与一个 KVM 切换器相连设置远程控制台。
   a. 将 USB CIM 插入接收器。
   b. 通过 Cat5 电缆将 USB CIM 连接至 KVM 切换器上的任何通道。
2. 使用 Cat5r/6 电缆连接发送器和接收器。
3. 分别把发送器和接收器插入合适的电源。
4. 将 KVM 切换器连至发送器。

5. 打开两个 KVM 切换器。



如需增加任何电脑和 KVM 切换器间的距离：

1. 设置一个可选带发送器的本地控制台。
2. 通过将接收器连接至 KVM 切换器设置一个远程控制台。
3. 使用 Cat5r/6 电缆连接发送器和接收器。
4. 分别把发送器和接收器插入合适的电源。
5. 把计算机连接到发送器。
6. 打开计算机。



Ap B 从 KX III 访问 Paragon II

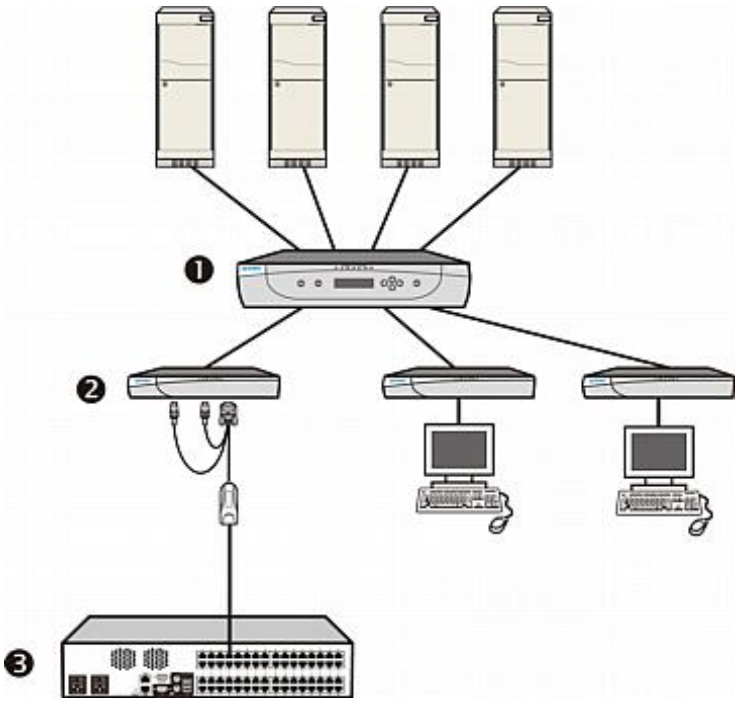
在本章内

概述

把 Paragon II 系统连接到一台受 CC-SG 管理的 KX III 设备，这样就可以在 CC-SG 上访问 Paragon II 了。

下图说明集成了 KX III 的配置。

注意：图像只为示例之用，可能与你的设备不完全一样。



❶	由 Paragon II 切换器、服务器和用户工作站构成的 Paragon II 系统
❷	插入 DCIM-USB G2 用户工作站
❸	KX III

如果 KX III 受 CC-SG 管理，在 KX III 或 CC-SG 上访问 Paragon II 系统时，显示 Paragon II OSUI 屏幕供你登录。

在此集成配置里，可以执行最新 Paragon II 固件实现的任何 OSUI 功能或最新 KX III 固件实现的任何 KX III 功能，虚拟媒体功能除外。

在 KX III 上访问 Paragon II OSUI 时，切勿尝试人工同步鼠标。在 OSUI 屏幕上不使用鼠标，鼠标同步会导致键盘响应延迟数秒钟。

参看*支持的 Paragon II CIM 和配置* (p. 278)了解详情。

支持的 Paragon II CIM 和配置

KX III 支持 P2CIM-APS2DUAL 和 P2CIM-AUSBDUAL CIM，提供两个 RJ45 端口连接不同的 KVM 切换器。

支持下列 CIM，在其中一台 KVM 切换器被锁定或发生故障时，可以采用备用路径访问目标服务器。

Paragon CIM	支持	不支持
P2CIM-APS2DUAL	• 配备 IBM® PS/2 型键盘端口和鼠标端口的服务器 • 自动纠偏补偿（当 CIM 连接 Paragon II 而非 KX III 时） • 智能鼠标模式 • 标准鼠标模式	• 虚拟媒体 • 智能卡 • 绝对鼠标模式 • 与刀片服务器机箱一起使用 • 串联 KVM 配置
P2CIM-AUSBDUAL	• 配备 USB 型或 Sun™ USB 型键盘端口和鼠标端口的服务器 • 自动纠偏补偿（当 CIM 连接 Paragon II 而非 KX III 时） • 智能鼠标模式 • 标准鼠标模式	• 虚拟媒体 • 智能卡 • 绝对鼠标模式 • 与刀片服务器机箱一起使用 • 串联 KVM 配置

KX III-至-KX III Paragon CIM 指南

在 KX III-至-KX III 配置中使用 Paragon CIM 时，应该遵循下列系统配置原则：

并发访问

无论是双 PC 共享模式还是独占模式，都应该给两台 KX III KVM 切换器配置相同的目标服务器并发访问策略。

如果需要独占访问目标服务器，必须相应配置两台 KVM 切换器：

- 选择 Security（安全）> Security Settings（安全设置）> Encryption & Share（加密和共享），把 PC Share（PC 共享）模式设置为 Private（独占）。

这样保证禁止所有用户组同时访问所有目标服务器。

KX III 考虑到更大的粒度控制，允许你给每个用户组设置目标服务器并发访问。设置用户组 PC 共享权限即可进行粒度控制。但这仅在 KX III 边界范围内有效。如果当 KX III 使用 P2CIM-APS2DUAL 或 P2CIM-AUSBDUAL 时必须保证隐私，不能使用用户组 PC 共享权限。

CIM 名称更新

P2CIM-APS2 名称和 P2CIM-AUSB 名称存储在 CIM 的内存里。有两个存储单元，可以满足 Paragon 命名常规（12 个字符）和 KX III 命名常规（32 个字符）要求。

在首次连接 KX III 时，在内存里检索 Paragon 名称，把它写入 KX III 使用的 CIM 存储单元。此后在 KX III 上查询 CIM 名称或更新 CIM 名称时，更改 KX III 使用的存储单元。KX III 并不更新 Paragon II 使用的存储单元。

如果一台 KX III 更新 CIM 名称，另一台 KX III 在下次尝试连接此目标服务器时检测并检索已更新的名称。在此之前，并不在另一台 KX III 上更新名称。

端口状态和可用性

更新 KX III Port Access（端口访问）页显示的端口状态（Up [工作]或 Down [停止]），说明 CIM 是否通电并连接 KX III 端口。

更新 KX III Port Access（端口访问）页显示的端口可用性（Idle [空闲]、Busy [忙]或 Connected [已连接]），只说明在同一台 KX III 上发起并在目标服务器上执行的活动。

如果目标服务器已连接其他 KX III，只有在尝试建立连接时才检查可用性。拒绝或允许访问，与在 KX III 上设置的 PC 共享策略保持一致。在此之前，并不在另一台 KX III 上更新可用性。

如果由于目标服务器忙而拒绝访问，就显示通知。

在 CC-SG 上操作

在 CC-SG 上发出的操作建立在受管 KX III 报告的状态、可用性和 CIM 名称之上。当目标服务器连接两台受管 KX III 并且两台设备已添加到 CC-SG，将创建两个节点，每个节点有与之关联的 oob-kvm 接口。也可以在每台 KX III 上只给一个节点配置一个 oob-kvm 接口。

如果给 KX III 配置 Private（独占）模式，在尝试建立第二个连接时，通知用户不能建立连接并拒绝访问。

在 CC-SG Port Profile（端口配置文件）面板上更改端口名称时，把更改后的名称推送到受管的 KX III。在尝试通过另一台 KX III 连接目标服务器端口之前，不在 CC-SG 上更新另一台 KX III 的相应端口名称。

KX III-至-Paragon II 指南

P2CIM-APS2DUAL 或 P2CIM-AUSBDUAL 可以连接 KX III 和 Paragon II。

并发访问

必须给 KX III 和 Paragon II 配置相同的目标服务器并发访问策略。

Paragon II 操作模式	模式说明	支持？
独占	一个特定通道端口连接的一台服务器或其他设备，每次只能供一个用户采用独占方式访问。	支持。 Paragon II 和 KX III 必须设置为 Private（独占）模式。Private（独占）设置应用于 KX III 设备，而不是根据用户组应用。 Paragon II 显示红色表示忙，显示绿色表示可用。
PC 共享	一个特定通道端口连接的一台服务器或其他设备可供多个用户访问，但每次只有一个用户拥有键盘和鼠标控制权。	支持。 但不支持在 Paragon II 上配置的 PC Share Idle Timeout（PC 共享空闲超时）。二者都有并发键盘和鼠标控制权。 Paragon II 显示绿色表示可用。如果另一个用户正在访问目标服务器，也是如此。
公共查看	当一个用户正在访问一个特定通道端口连接的一台	不支持。 在把 CIM 连接到 Paragon

Paragon II 操作模式	模式说明	支持？
	服务器或其他设备时，其他用户可以选择此通道端口观看此设备的视频输出。但在他们断开连接或切换到其他目标服务器之前，只有第一个用户拥有键盘和鼠标控制权。	II 和 KX III 时，不能使用此模式。 Paragon II 显示黄色表示它处于 P-View（公共查看）模式。

CIM 名称更新

- 在 Paragon II 上更新的 CIM 名称存储在 Paragon 命名常规对应的 CIM 存储单元里，并在此检索它。
- 在 KX III 上更新的 CIM 名称存储在 KX III 命名常规对应的 CIM 存储单元里，并在此检索它。
- 不在 Paragon II 和 KX III 之间广播 CIM 名称更新。

Paragon II 和 KX III 间的支持连接距离

在把 KX III 用作 Paragon 系统的前端时，应该限制电缆长度（距离）实现较好的视频质量。

Paragon II 用户工作站到目标服务器的最大电缆长度（距离）是 500 英尺（152 米）。如果距离较大，视频质量也许能接受，也许无法接受。

KX III 到 Paragon 用户工作站的最大电缆长度（距离）是 150 英尺（45 米）。

把 Paragon II 连接到 KX III

把 Paragon II 系统连接到 KX III：

1. 检查要连接到 KX III 的 Paragon II 用户工作站是否安装了 v4.6（或更高版本）的固件。如果没有安装，要升级用户工作站。

   Paragon II 用户工作站可以是下列用户工作站之一：

   - P2-UST
   - P2-EUST
   - P2-EUST/C

   参看 **Paragon II 帮助**获取关于升级的信息。

2. 将相应的 DCIM-USB 插入 Paragon II 用户工作站的 USB 和视频端口。

如果系统是两层或三层系统，确保 Paragon II 用户工作站连接基础 KX III 设备（第一层）。

3. 用最长 150 英尺（45 米）的 Cat5 UTP 电缆把 Paragon II 用户工作站连接到一台 KX III 设备。
   - 把电缆的一端插入 DCIM 的 RJ-45 端口，把另一端插入 KX III 设备的其中一个通道端口。
4. 如果要在 KX III 或 CC-SG 上用多条路径访问同一个 Paragon II 系统，重复第一步到第三步把其他用户工作站连接到 KX III。

Ap C 在 dcTrack 管理 KX III

在本章内

概述

Raritan 的 dcTrack® 是一个完整的 Data Center Infrastructure Management (DCIM)（数据中心基础设施管理）解决方案，它为你提供关于设施、网络和 IT 实时信息。

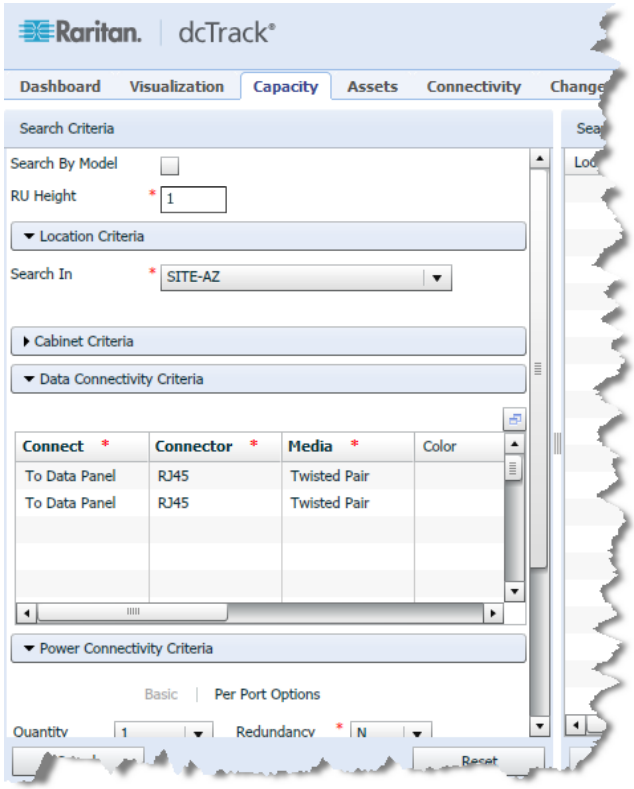
dcTrack 将你的设施视觉化，帮助数据中心和设施管理员管理 IT 设备的位置、通知容量管理决定、掌握如 KX III 在内的数据中心资产的精确信息。

在 Cabinet（储存）内寻找 KX III 的位置空间

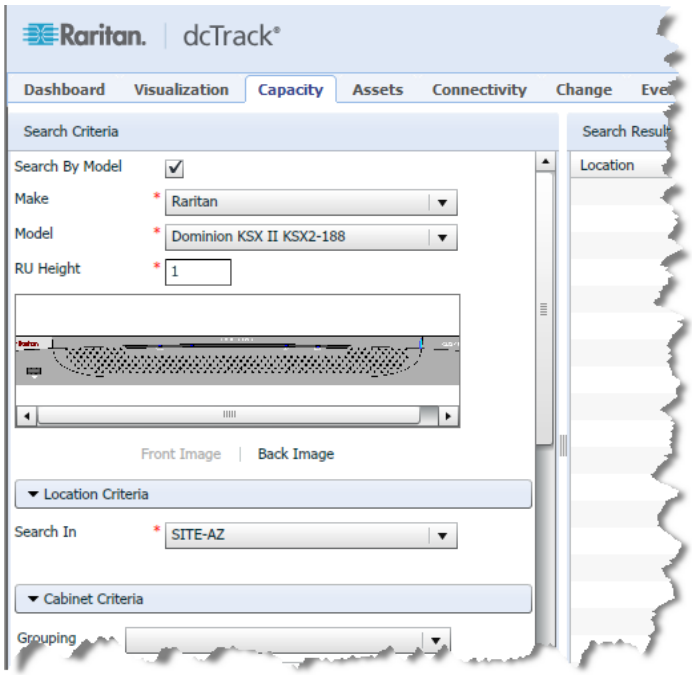
使用 dcTrach 的容量管理功能在数据中心的储存内寻找 KX III 的位置空间。

搜索：

- 机架单位 - dcTrach 寻找储存内有足够机架单位的开放空间容纳 KX III。



- 制作和型号 - 根据 KX III 的尺寸、连接等，cTrach 寻找储存内有足够机架单位的开放空间容纳 KX III。



在 **dcTrack 帮助**中参看**容量管理 - 定位并为物品预订储存空间**。

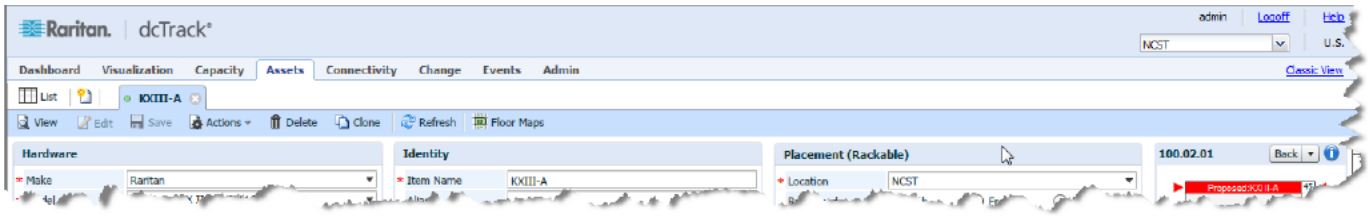
将 KX III 设备添加至 dcTrack

通过将 KX III 设备添加至应用程序在 dcTrack® 中管理 KX III 设备。

根据你的需要，有很多种方式添加设备至 KX III 设备。

人工添加 KX III 至 dcTrack

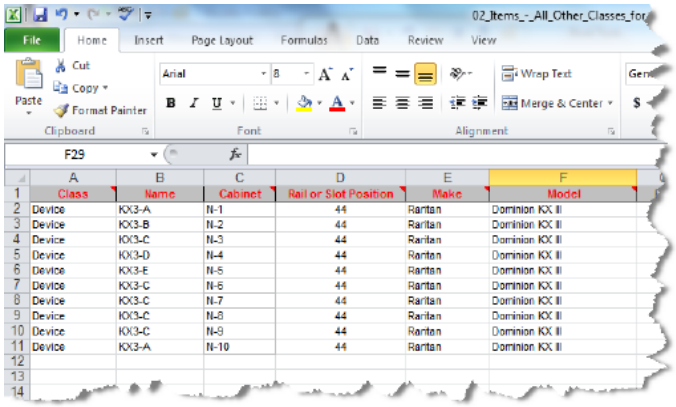
如果你在添加一个或几个设备时人工添加 KX III



在 **dcTrack 帮助**中参看**在 dcTrack 中人工创建新项目**。

将 KX III 设备导入 dcTrack

如果你要添加很多 KX III，在由 Raritan 提供的 02_Items_-_All_Other_Classes_for_3.x.xls 电子数据表中填写 KX III 的信息，然后通过 Import Wizard（导入精灵）将电子数据表导入 dcTrack®。

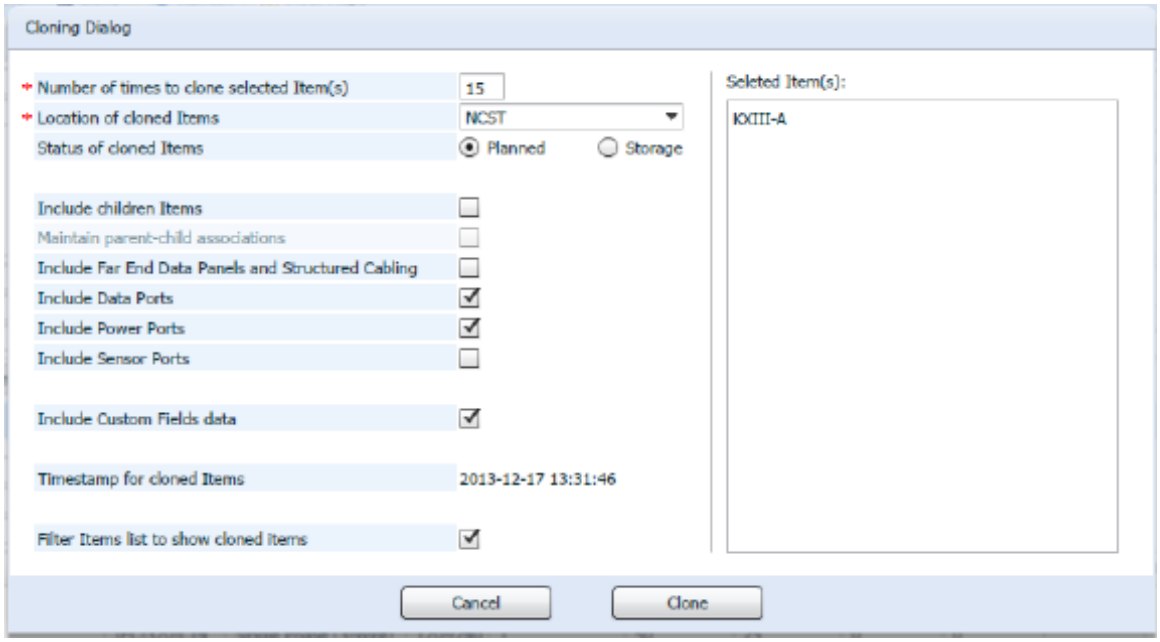


Class	Name	Cabinet	Rail or Slot Position	Make	Model
Device	KX3-A	N-1	44	Raritan	Dominion KX II
Device	KX3-B	N-2	44	Raritan	Dominion KX II
Device	KX3-C	N-3	44	Raritan	Dominion KX II
Device	KX3-D	N-4	44	Raritan	Dominion KX II
Device	KX3-E	N-5	44	Raritan	Dominion KX II
Device	KX3-C	N-6	44	Raritan	Dominion KX II
Device	KX3-C	N-7	44	Raritan	Dominion KX II
Device	KX3-C	N-8	44	Raritan	Dominion KX II
Device	KX3-C	N-9	44	Raritan	Dominion KX II
Device	KX3-A	N-10	44	Raritan	Dominion KX II

在 **dcTrack 帮助**中参看**使用 Import Wizard（导入精灵）将新项目添加到 dcTrack**。

克隆现有 KX III 设备

如果你已经添加了一个 KX III 并想克隆其与其电压和数据电路（如果你已经创建了这些）、端口、自定义域等，使用克隆功能。



注意，整个储存已经其中含有的项目和其连接以及子设备也都可以被克隆。

所以，如果你在储存内添加了一个 KX III 并使用通过你的数据中心使用相同储存配置，你可以克隆此储存。

在 **dcTrack 帮助**中参看**通过克隆创建新项目和储存**。

为 KX III 创建数据和电源电流

当 KX III 存在与 dcTrack®中后，为其创建数据和电源电流。

电流可以在添加 KX III 时创建，也可以之后创建。

电流创建后，提交申请请求以将其创建在数据中心中。

在 **dcTrack 帮助**中参看**为项目创建新电流**。

为 KX III 提交添加项目请求

将 KX III 添加至 dcTrack® 后，提交一个安装项目请求。

请求使改变控制过程开始，从工作命令开始，直至手动安装 KX III 至数据中心。

在 **dcTrack 帮助**中参看**从操作菜单提交一个安装项目请求**。

管理 KX III 工作命令

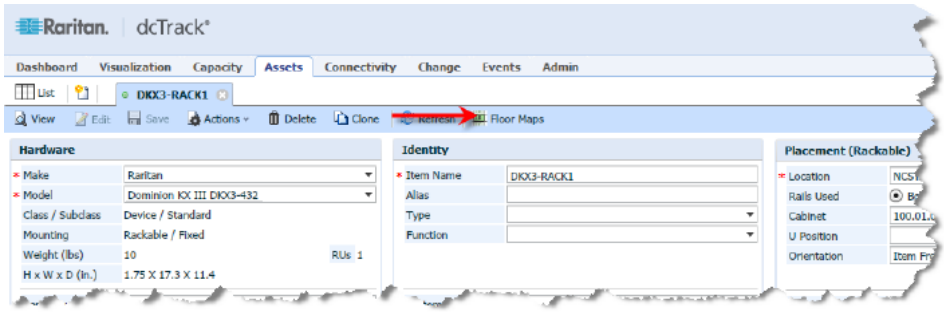
除非启用 Request Bypass 模式，在这时 dcTrack® 不管理项目请求带来的更改控制过程，安装 KX III 的工作命令由 dcTrack Gatekeeper 管理。

在 **dcTrack 帮助**中参看**管理工作请求**或 **Request Bypass（请求旁路）**。

将 KX III 在储存中的高度和平面位置视觉化

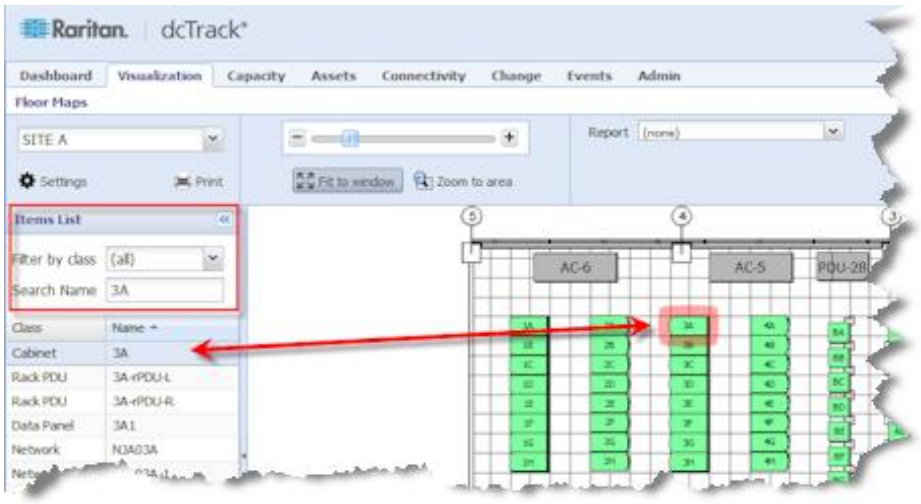
添加 KX III 至 dcTrack® 时，你将其放入储存中。

如果储存位于数据中心的位置有平面图与其相连，且 KX III 位于的储存与平面图上的储存图像相连，那你可以从 dcTrack 中的 KX III 页访问平面图。



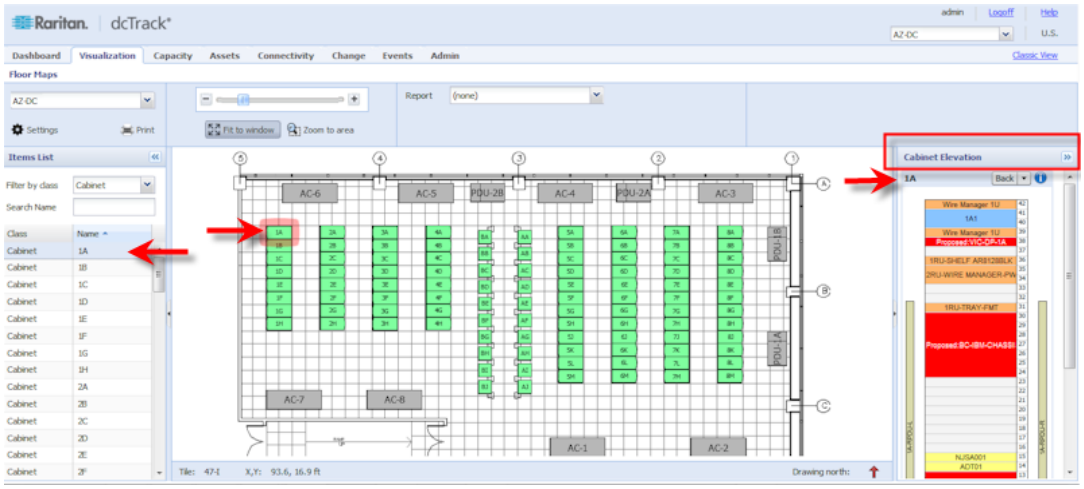
在 **dcTrack 帮助**中参看**从一个项目的页面打开平面图**。

在平面图页面后，在平面图和项目列表上参看 KX III 应该位于的储存的位置。



在 **dcTrack 帮助**中参看**定位在平面图和项目列表（Web 客户机）上的项目**。

你也可以从平面图上查看 KX III 在储存中的高度。



在 **dcTrack 帮助**中参看**储存高度 - 平面图（Web 客户机）**。

管理 KX III 生命周期

KX III 安装后，在你的数据中心中管理其生命周期。

移动 KX III

从这里提交移动 KX III 的请求：

- 一个储存到另一个储存
- 一个位置到另一个位置
- 一个导轨位置到另一个导轨位置

在 **dcTrack 帮助**中参看**移动项目请求**。

KX III 开关电源

如果需要，提交请求以打开或关闭 KX III 的电源。

在 **dcTrack 帮助**中参看**提交请求以打开或关闭设备电源**。

带一台 KX III 到或离场。

提交请求以带一台 KX III 到或离场，例如因为维护原因，其被暂时移除。

在 **dcTrack 帮助**中参看**提交请求带一台 KX III 到或离场**。

解除一台 KX III 的运作将其转移至贮存

如果你计划暂时将其移至离场位置，提交请求以解除一台 KX III 的运作将其转移至贮存。

在 **dcTrack 帮助**中参看**提交请求解除一台 KX III 的运作将其转移至贮存**。

解除一台 KX III 的运作将其归档

提交请求以解除一台 KX III 的运作将其归档以将其移除库存进行处理。

在 **dcTrack 帮助**中参看**提交请求以解除一台 KX III 的运作将其归档**。

Ap D 规格

在本章内

硬件

KX III 尺寸和物理规格

Dominion KX III 模型	Description（说明）	电源和热损耗	尺寸（宽 x 深 x 高）	重量	操作温度	湿度
DKX3-108	▪ 8 个服务器端口 ▪ 1 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	8.60lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	3.9 公斤	32º - 113º F	
DKX3-116	▪ 16 个服务器端口 ▪ 1 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	8.60lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	3.9 公斤	32º - 113º F	
DKX3-132	▪ 32 个服务器端口 ▪ 1 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	8.60lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	3.9 公斤	32º - 113º F	
DKX3-216	▪ 16 个服	双电源	17.3" x 13.15" x	9.08lbs	0º - 45º C	0-85 %

Dominion KX III 模型	Description（说明）	电源和热损耗	尺寸（宽 x 深 x 高）	重量	操作温度	湿度
	务器端口 ▪ 2 个远程用户 ▪ 1 个在机架上使用的本地端口	110V/240V，50-60Hz 1.8A 60W 52 KCAL	1.73" 439x334x44 mm	 4.12 公斤	 32º - 113º F	RH
DKX3-232	▪ 32 个服务器端口 ▪ 2 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73" 439x334x44 mm	9.08lbs 4.12 公斤	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-416	▪ 16 个服务器端口 ▪ 4 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73" 439x334x44 mm	9.08lbs 4.12 公斤	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-432	▪ 32 个服务器端口 ▪ 4 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73" 439x334x44 mm	9.08lbs 4.12 公斤	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-464	▪ 64 个服务器端口 ▪ 4 个远程用户 ▪ 1 个在机架上使用	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.3" x 3.5" 439x338x89 mm	12.39lbs 5.62 公斤	0º - 45º C 32º - 113º F	0-85 % RH

Dominion KX III 模型	Description（说明）	电源和热损耗	尺寸（宽 x 深 x 高）	重量	操作温度	湿度
	的本地端口					
DKX3-808	▪ 8 个服务器端口 ▪ 8 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.96lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	4.52 公斤	32º - 113º F	
DKX3-832	▪ 32 个服务器端口 ▪ 8 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.96lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	4.52 公斤	32º - 113º F	
DKX3-864	▪ 64 个服务器端口 ▪ 8 个远程用户 ▪ 1 个在机架上使用的本地端口	双电源 110V/240V，50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.3" x 3.5"	12.39lbs	0º - 45º C	0-85 % RH
			439x338x89 mm	5.62 公斤	32º - 113º F	

支持 **KX III** 的目标服务器视频分辨率

- 640x350@70Hz
- 640x350@85Hz
- 640x400@56Hz
- 640x400@84Hz
- 640x400@85Hz
- 640x480@60Hz
- 640x480@66.6Hz
- 640x480@72Hz
- 640x480@75Hz
- 640x480@85Hz
- 720x400@70Hz
- 720x400@84Hz
- 720x400@85Hz
- 800x600@56Hz
- 800x600@60Hz
- 800x600@70Hz
- 800x600@72Hz
- 800x600@75Hz
- 800x600@85Hz
- 800x600@90Hz
- 800x600@100Hz
- 832x624@75.1Hz
- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@72Hz
- 1024x768@85Hz
- 1024x768@75Hz
- 1024x768@90Hz
- 1024x768@100Hz
- 1152x864@60Hz
- 1152x864@70Hz
- 1152x864@75Hz
- 1152x864@85Hz
- 1152x870@75.1Hz

- 1280x720@60Hz
- 1280x960@60Hz
- 1280x960@85Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1280x1024@85Hz
- 1360x768@60Hz
- 1366x768@60Hz
- 1368x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz

目标服务器视频分辨率支持的连接距离和刷新速率

最大支持距离受许多因素的影响，包括五类电缆类型/质量、服务器类型和制造商、显卡卡驱动程序和监视器、环境条件和用户期望值。

下表概述各种视频分辨率和刷新速度对应的最大目标服务器距离：

目标服务器视频分辨率	最大距离
1024x768@60Hz（和更低）	150 英尺（45 米）
1280x1024@60Hz	100 英尺（30 米）
1280×720@60Hz	75 英尺（22 米）
1600x1200@60Hz	50 英尺（15 米）
1920x1080@60Hz	50 英尺（15 米）

参看 ***KX III 支持的目标服务器视频分辨率*** (参看 "***支持 KX III 的目标服务器视频分辨率***" p. 294)了解 KX III 支持的视频分辨率。

注意：由于服务器制造商和服务器类型很多，操作系统版本很多，显卡驱动程序很多，视频质量评判存在主观性，Raritan 不能保证在所有环境下达到所有距离要求。

Supported KX III Local Port DVI Resolutions（支持的 KX III 本地端口 DVI 分辨率）

- 1920x1080@60
- 1280x720@60
- 1024x768@60（默认）
- 1024x768@75
- 1280x1024@60
- 1280x1024@75
- 1600x1200@60
- 800x480@60
- 1280x768@60
- 1366x768@60
- 1360x768@60
- 1680x1050@60
- 1440x900@60

支持的计算机接口模块 (CIM) 规格

数字 CIM 支持 Display Data Channels (DDC) 和 Enhanced Extended Display Identification Data (E-EDID)。

CIM 型号	Description（说明）	尺寸（宽 x 深 x 高）	重量
D2CIM-DVUSB	用于 BIOS 虚拟媒体、智能卡/CAC、音频和绝对鼠标同步的双 USB CIM 	1.7" x 3.5" x 0.8"; 43 x 90 x 19mm	0.25 磅；0.11 千克
D2CIM-VUSB	用于虚拟媒体和绝对鼠标同步的 USB CIM	1.3" x 3.0" x 0.6"; 33 x 76 x 15mm	0.20 磅；0.09 千克

CIM 型号	Description（说明）	尺寸（宽 x 深 x 高）	重量
			
D2CIM-DVUSB-DVI	实现数模转换并支持虚拟媒体、智能卡/CAC、音频、绝对鼠标同步和相对鼠标同步的数字 CIM 	1.7" x 3.5" x 0.8"; 43 x 90 x 19mm	0.25 磅；0.11 千克
D2CIM-DVUSB-DP	实现数模转换并支持虚拟媒体、智能卡/CAC、音频、绝对鼠标同步和相对鼠标同步的数字 CIM 	1.7" x 3.5" x 0.8"; 43 x 90 x 19mm	0.25 磅；0.11 千克
D2CIM-DVUSB-HDMI	实现数模转换并支持虚拟媒体、智能卡/CAC、音频、绝对鼠标同步和相对鼠标同步的数字 CIM 	1.7" x 3.5" x 0.8"; 43 x 90 x 19mm	0.25 磅；0.11 千克
DCIM-PS2	PS2 的 CIM	1.3" x 3.0" x 0.6"; 33 x 76 x 15mm	0.20 磅；0.09 千克

CIM 型号	Description（说明）	尺寸（宽 x 深 x 高）	重量
			
DCIM-USBG2	USB 和 Sun USB CIM 	1.3" x 3.0" x 0.6"; 33 x 76 x 15mm	0.20 磅；0.09 千克

注意 DVUSB CIM 上的黑色连接器用于连接键盘和鼠标。灰色连接器用于连接虚拟媒体。

用 CIM 的两个插头连接设备。如果两个插头不连接目标服务器，设备可能不能正常工作。

Mac 的支持数字视频 CIM

使用一个数字视频 CIM 连接至如下 Mac® 端口：

Mac 端口	CIM
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort 或 Thunderbolt	D2CIM-DVUSB-DP

如果 Mac 的 HDMI 或 DisplayPort 视频有迷你连接器，可能需要被动调节器电缆在数字 CIM 上连接至完整尺寸的 HDMI 和 DisplayPort。

或者，D2CIM-VUSB 或 D2CIM-DVUSB 使用 Mac VGA 调节器。注意这可能不太可靠，视频质量可能受到影响。

如需获得 Mac 的 KX III 2.5.0（和更高版本）支持的专用模式，参看 ***数字 CIM 专用模式和标准模式*** (参看 "***数字 CIM 的专用模式和标准模式***" p. 299)。

数字 CIM 定时模式

下面列出 KX III 通过数字 CIM 与视频源通信时使用的默认定时模式。

使用的定时模式视视频源的本机分辨率而定。

- 1920x1080@60Hz
- 1600x1200@60Hz
- 1280x1024@60Hz（应用于数字 CIM 的默认分辨率）
- 1440x900@60Hz
- 1024x768@60Hz

参看联机帮助中的***配置 CIM 端口*** (p. 87)获取更多信息。

数字 CIM 的专用模式和标准模式

下面列出 KX III 3.0.0（和更高版本）支持的其他专用分辨率和定时模式及标准分辨率和定时模式。

数字 CIM 专用模式

- 720x400@70Hz IBM, VGA
- 640x480@60Hz IBM, VGA
- 640x480@67Hz Apple Mac® II
- 640x480@72Hz VESA
- 640x480@75Hz VESA
- 800x600@56Hz VESA
- 800x600@60Hz VESA
- 800x600@72Hz VESA
- 800x600@75Hz VESA
- 832x624@75Hz Apple Mac II
- 1024x768@60Hz VESA
- 1024x768@70Hz VESA
- 1024x768@75Hz VESA
- 1280x1024@75Hz VESA
- 1152x870@75Hz Apple Mac II

数字 CIM 标准模式

- 1152x864@75Hz VESA
- 1280x960@60Hz VESA
- 1280x1024@60Hz VESA
- 1360x768@60Hz VESA
- 1400x1050@60Hz VESA
- 1440x900@60Hz VESA
- 1600x1200 @60Hz VESA
- 1680x1050@60Hz VESA
- 1920x1080@60Hz VESA

DVI 兼容模式

如果用 HDMI CIM 连接安装了 Intel 显示卡的 Dell Optiplex 目标服务器或安装了 HDMI 视频端口的 Mac® Mini，可能需要 DVI 兼容模式。

选择此模式确保来自目标服务器的视频质量很好。

参看联机帮助中的*配置 CIM 端口* (p. 87)。

支持的远程连接

远程连接	详细信息
网络	10BASE-T、100BASE-T 和 1000BASE-T (Gigabit) Ethernet
协议	TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS 和 LDAP/LDAPS

网络速度设置

KX III 网络速度设置

网络切换端口设置	Auto（自动）	1000/全双工	100/全双工	100/半双工	10/全双工	10/半双工
Auto（自动）	最高可用速度	1000/全双工	KX III：100/全双工 切换器 :100/半双工	100/半双工	KX III：10/全双工 切换器：10/半双工	10/半双工
1000/全双工	1000/全双工	1000/全双工	没有通信	没有通信	没有通信	没有通信

KX III 网络速度设置						
100/全双工	KX III：100/半双工 切换器 :100/全双工	KX III：100/半双工 切换器 :100/全双工	100/全双工	KX III：100/半双工 切换器 :100/全双工	没有通信	没有通信
100/半双工	100/半双工	100/半双工	KX III：100/全双工 切换器 :100/半双工	100/半双工	没有通信	没有通信
10/全双工	KX III：10/半双工 切换器：10/全双工	没有通信	没有通信	没有通信	10/全双工	KX III：10/半双工 切换器：10/全双工
10/半双工	10/半双工	没有通信	没有通信	没有通信	KX III：10/全双工 切换器：10/半双工	10/半双工

图注：

不像期望的那样工作

支持

工作；不建议

Ethernet 规范不支持；产品通信，但会发生冲突

根据 Ethernet 规范，这应该是“没有通信”，但要注意 KX III 的特性与期望的特性有偏差

注意：为了进行可靠网络通信，配置 KX III 和 LAN 交换机使用相同的 LAN 接口速度和双工。例如将 KX III 和 LAN 交换机均配置为 Autodetect（自动检测，建议配置），或者设置为 100Mbps/全双工等固定速度/双工。

Dell 机箱电缆长度和视频分辨率

为了保持视频质量，Raritan 建议你在 KX III 上连接 Dell® 刀片服务器机箱时，使用下列电缆长度和视频分辨率：

视频分辨率	电缆长度
1024x768@60Hz	50' (15.24 m)
1280x1024@60Hz	50' (15.24 m)
1600x1200@60Hz	30' (9.14 m)

智能卡最低系统要求

本地端口要求

通过本地端口连接 KX III 的基本互操作要求：

- 在本地连接的所有设备（智能卡读卡器或令牌）必须符合 USB CCID 规范。

目标服务器要求

在使用智能卡读卡器时，目标服务器有基本的互操作要求：

- IFD（智能卡读卡器）控制器必须是标准 USB CCID 设备驱动程序（与通用 Microsoft® USB CCID 驱动程序相当）。
- 需要使用 CIM 或 D2CIM-DVUSB (Dual-VM CIM)，它必须使用 3A6E 或更高版本的固件。
- 如果每个刀片服务器使用一个 CIM，支持刀片服务器机箱连接。
- IBM® BladeCenter Model H 和 E 只有在启用自动发现之后才支持刀片服务器机箱连接，每个机箱使用一个 CIM。

Windows XP 目标服务器

Windows XP® 操作系统必须运行 Windows XP SP3，才能同时使用智能卡和 KX III。如果在目标服务器 Windows XP 环境下使用 .NET 3.5，必须使用 SP1。

Linux 目标服务器

如果使用 Linux® 目标服务器，必须满足下列要求，才能同时使用智能卡读卡器和 Raritan 设备。

- CCID 要求

  如果 Linux 目标服务器不能识别 Raritan D2CIM-DVUSB VM/CCID 是智能卡读卡器，可能必须把 CCID 驱动程序升级到 v1.3.8 或更高版本，同时更新驱动程序配置文件 (Info.plist)。

操作系统	CCID 要求
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

远程客户机要求

远程客户机基本互操作要求是：

- IFD（智能卡读卡器）控制器必须是符合 PC/SC 规范的设备驱动程序。
- 必须能使用 ICC（智能卡）资源管理器，它必须符合 PC/SC 规范。
- JRE® Java® 1.7 和智能卡 API 必须可供 Raritan 客户机应用程序使用。

远程 Linux 客户机要求

如果使用 Linux® 客户机，必须满足下列要求，才能同时使用智能卡读卡器和 Raritan 设备。

注意：如果有一个或多个目标服务器 KVM 会话处于活动状态，用户插入智能卡登录客户机所需的时间可能较长。同时正在向这些目标登录。

- PC/SC 要求

操作系统	要求的 PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- 创建 Java® 库链接

  在升级到 RHEL 4、RHEL 5 和 FC 10 之后，必须创建 libpcsclite.so 软链接，例如 ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so，假定安装包把库安装在 /usr/lib 或 /user/local/lib 文件夹里。

- PC/SC 后台进程

  在重新启动 pcsc 后台进程（框架资源管理器）时，同时重新启动浏览器。

支持的智能卡读卡器

Type（类型）	供应商	Model（型号）	验证
USB	SCM Microsystems	SCR331	本地和远程验证
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	本地和远程验证
USB	ActivIdentity	ActivIdentity USB Reader v3.0	本地和远程验证
USB	Gemalto®	GemPC USB-SW	本地和远程验证
USB 键盘/读卡器组合	Dell®	USB Smart Card Reader Keyboard	本地和远程验证
USB 键盘/读卡器组合	Cherry GmbH	G83-6744 SmartBoard	本地和远程验证
SIM 尺寸智能卡 USB 读卡器	Omnikey	6121	本地和远程验证
集成 (Dell Latitude D620)	O2Micro	OZ776	仅远程
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	仅远程
PCMCIA	SCM Microsystems	SCR243	仅远程

注意：SCM Microsystems SCR331 智能卡读卡器必须使用 SCM Microsystems 固件 v5.25。

不支持的智能卡读卡器

下表列出 Raritan 测试后发现 Raritan 设备不支持的读卡器列表。

如果智能卡读卡器既不在支持的智能卡读卡器表上，也不在不支持的智能卡读卡器表上，Raritan 不能保证它能与此设备一起工作。

Type（类型）	供应商	Model（型号）	Notes（备注）
USB 键盘/读卡器组合	HP®	ED707A	无中断端点 => 不兼容 Microsoft® 驱动程序
USB 键盘/读卡器组合	SCM Microsystems	SCR338	专用读卡器实现技术（不符合 CCID 规范）

Type（类型）	供应商	Model（型号）	Notes（备注）
USB 令牌	Aladdin®	eToken PRO™	专用实现技术

音频播放和录音建议及要求

音量

- 把目标服务器的音量设置为中等设置，

  例如在 Windows® 客户机上把音频设置为 50 或更低。

此设置必须在音频播放设备或录音设备上设置，不在客户机的音频设备控制部分设置。

在启用 PC 共享模式时的音频连接建议

如果在 PC 共享模式下使用音频功能，在把其他音频播放和录音设备连接到目标服务器时，音频播放和录音中断。

例如用户 A 把播放设备连接到目标服务器 1 运行音频播放应用程序，然后用户 B 把录音设备连接到同一台目标服务器。用户 A 的播放会话中断，可能需要重新启动音频应用程序。

必须用新设备配置枚举 USB 设备，所以会发生会话中断现象。

目标服务器安装新设备驱动程序可能需要一些时间。

音频应用程序可能停止播放，也可能跳到下一段，也可能继续播放，

具体情况取决于音频应用程序在设计时如何处理断开/重新连接事件。

带宽要求

下表详细说明在每种选择的格式下传输音频时的音频播放和录音带宽要求。

音频格式	网络带宽要求
44.1 KHz 16 位立体声	176 Kbps
44.1 KHz 16 位单声道	88.2 Kbps
2.05 KHz 16 位立体声	88.2 Kbps
22.05 KHz 16 位单声道	44.1 Kbps
11.025 KHz 16 位立体声	44.1 Kbps

音频格式	网络带宽要求
11.025 KHz 16 位单声道	音频 22.05 Kbps

实际上，由于在目标服务器上打开并使用音频应用程序时，键盘数据和视频数据要消耗带宽，所以连接音频设备和目标服务器所用的带宽比上述数值大。

建议你在使用播放和录音功能之前至少要包括 1.5MB 连接带宽。

但是，如果目标服务器屏幕使用很高的屏幕分辨率显示很多全彩色内容，要消耗比上述数值大得多的带宽，会严重影响音频质量。

可以采用很多建议的客户机设置，降低视频在小带宽情况下对音频质量的影响：

- 用质量较低的格式连接音频播放设备。在使用 11k 连接时，视频消耗带宽造成的影响比在使用 44k 连接时小得多。
- 在 Connection Properties（连接属性）下面，把连接速度设置为与客户机服务器连接最匹配的值。
- 在 Connection Properties（连接属性）下面，尽可能把色彩深度设置为最小值。把色彩深度降到 8 位彩色，可以大幅降低消耗的带宽
- 把 Smoothing（平滑度）设置为 High（高），通过减少显示的视频噪声来改善目标服务器视频的外观
- 在 Video（视频）设置下面，把 Noise Filter（噪声过滤器）设置为 7（最大值），当目标服务器屏幕发生变化时使用较小带宽

Mac 环境下的音频

在 Mac® 环境下使用音频功能时，存在下列已知问题。

- 在通过 Virtual KVM Client (VKC)访问播放设备时，Mac 客户机上的 Connect Audio（连接音频）面板只列出一个播放设备。列出的设备是默认设备，在 Connect Audio（连接音频）面板上显示为 Java Sound Audio Engine。
- 通过 Skype® 在 Mac 目标服务器上使用音频时，可能会造成音频恶化。

支持的音频/虚拟媒体数和智能卡连接数

下面说明可以同时在客户机和目标服务器之间建立的音频/虚拟媒体和智能卡连接数：

- 1 个智能卡
- 1 个虚拟媒体
- 1 个智能卡和 1 个虚拟媒体
- 2 个虚拟媒体

KX III 支持的键盘语言

KX III 支持下表列出的键盘语言。

*注意：中文键盘、日文键盘和朝鲜文键盘仅用于显示；KX III Local Console 功能目前不支持本地语言输入。如要进一步了解非英文键盘，参看***参考资料** *(p. 314)*。

注意：如果你使用 Linux 操作系统，Raritan 强烈建议你用系统配置的键盘更改语言。

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
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

语言	地区	键盘布局
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

Mac Mini BIOS 键盘命令

在利用 Mac Snow Leopard® 与 Mac Lion® 相连基于 Intel 的 Mac® Mini 目标服务器上测试过下列 BIOS 命令。服务器与 KX III 通过 D2CIM-DVUSB 和 D2CIM-VUSB CIM 相连。参看如下获得支持秘钥和任何注释。

击键	Description（说明）	虚拟媒体 CIM	双虚拟媒体 CIM	Mac Lion 服务器 HDMI CIM
在启动时按 C	从可启动的 CD 或 DVD 启动，例如 Mac OS X 安装光碟	✓	✓	
启动时按 D	用 Apple Hardware Test (AHT) 启动	✓ 可能需要 BIOS Mac 配置文件使鼠标正常工作	✓ 可能需要 BIOS Mac 配置文件使鼠标正常工作	✓ 可能需要 BIOS Mac 配置文件使鼠标正常工作
按 Option-Command-P-R，直到再次听到启动声为止。	复位 NVRAM		✓	✓
启动时按 Option	用 Startup Manager 启动，可以选择要从中启动的 Mac OS X 卷。	✓	✓	✓
按 Eject 或 F12，或者按住鼠标键	弹出光盘等可拆卸媒体	✓	✓	
启动时按 N	从兼容的网络服务器 (NetBoot) 启动	✓	✓	✓
启动时按 T	在目标磁盘模式下启动			✓

击键	Description（说明）	虚拟媒体 CIM	双虚拟媒体 CIM	Mac Lion 服务器 HDMI CIM
启动时按 Shift	在安全模式下启动，临时禁用登录项	✓	✓	LION 启动至安全模式的已知问题。红色的“Safe Mode（安全模式）”在 Lion 中不显示
启动时按 Command-V	在详细模式下启动。管理	✓	✓	✓
启动时按 Command-S	在单用户模式下启动	✓	✓	✓
启动时按 Option-N	尝试从 NetBoot 服务器上用默认引导镜像文件启动	✓	✓	✓
启动时按 Command-R	在 Lion 恢复模式 1 下启动	不适用	不适用	✓

使用 Windows 键盘访问 Mac 目标服务器

Windows® 键盘可被用来访问连接至 KX III 的 Mac®。Windows 秘钥然后被用来模仿特别的 Mac 秘钥。这与直接将 Windows 键盘连接至 Mac 一样。

使用的 TCP 端口和 UDP 端口

端口	Description（说明）
HTTP，端口 80	可以按需要配置此端口。参看 ***HTTP 和 HTTPS 端口设置*** (p. 120)。 为安全起见，KX III 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 III 响应端口 80，用户不必明确输入 URL 地址即可访问 KX III。
HTTPS，端口 443	可以按需要配置此端口。参看 ***HTTP 和 HTTPS 端口设置*** (p. 120)。 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 (Virtual KVM Client (VKC)) 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 III (Raritan KVM-over-IP) 协议，	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。

端口	Description（说明）
可配置端口 5000	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。如要详细了解如何配置此设置，参看*网络设置* (参看 "*网络配置*" p. 77)。
SNTP(时间服务器)，可配置 UDP 端口 123	KX III 有一个任选功能，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。**任选**
LDAP/LDAPS，可配置端口 389 或 636	如果给 KX III 配置了用 LDAP/LDAPS 协议进行远程验证用户登录，将使用端口 389 或 636，但可以配置系统使用你指定的任何端口。**任选**
RADIUS，可配置端口 1812	如果给 KX III 配置了用 RADIUS 协议进行远程验证用户登录，将使用端口 1812，但也可以配置系统使用你指定的任何端口。**任选**
RADIUS 记帐，可配置端口 1813	如果给 KX III 配置了用 RADIUS 协议进行远程验证用户登录，同时将 RADIUS 记帐用于事件日志，将用端口 1813 或你指定的任何端口传输日志通知。
SYSLOG，可配置 UDP 端口 514	如果配置 KX III 将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。**任选**
TCP 端口 22	端口 22 用于 KX III 命令行界面（在与 Raritan 技术支持部门一起工作时）。
SSH	(Secure Shell) 可以配置 SSH 端口。默认端口是 22。

软件

支持的操作系统和浏览器

操作系统	浏览器
Windows 7® 家庭高级版 SP1 64-bit	▪ Internet Explorer® 10 和 11 ▪ Firefox® 25 ▪ Chrome® 31 ▪ Safari® 5.1.7
Windows 7 终极版 SP1 64-bit	▪ Internet Explorer 8、9、11 ▪ Firefox 25 ▪ Chrome 31

操作系统	浏览器
Windows 7 终极版 32-bit	▪ Internet Explorer 8 ▪ Firefox 25 ▪ Chrome 31
Windows 8® 64-bit	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
Windows 服务器 2012® 标准版 64-bit	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
Windows XP® 有 SP 3 的家庭版	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
openSUSE® 11.4 Celadon (x86_64)	▪ Firefox 16.0.2
Fedora® 18（球形奶牛）	▪ Firefox 24
RHEL 6.4	▪ Firefox 21
OS X Mountain Lion® 10.8.5 *	▪ Firefox 25（推荐） ▪ Safari 6.1
Solaris® 10 64-bit	▪ Firefox 3.6.23
Mac® 10.7.5	▪ Safari 6.0.5 ▪ Firefox 25

**注意：从 OS X 10.8.2 升级至 OS X 10.8.3 时，Safari® 可能会阻止 Java™。*

Mac 的 JRE 要求和浏览器注意事项

Java Runtime Environment 对 Mac 的要求

在使用 Virtual KVM Client (VKC) 通过 KX III 访问目标服务器时在 PC 和 Mac 上安装 Java Runtime Environment 7 (JRE)®。

这保证了为在远程访问目标服务器/PC/Mac 时，提供高性能，KVM-over-IP 视频处理。

JRE 的 Mac 最新版可以在 Apple Support 网站下载。

Mac 的浏览器注意事项

在某些浏览器中，Java 可能被默认禁用。为了使用 KX III，需要启用 Java 和所有安全警告。

特定版本的 Safari® 因为安全原因会阻止 Java。因为 Java 要求使用 KX III，Raritan 建议你使用 Firefox® 作为替换。

此外，可能会要求你浏览一系列消息。如果显示这些消息，选择“Do Not Block（不要阻止）”。

Java 和 Microsoft .NET 要求

需要 Java® 1.7 （或更高)）或 Microsoft .NET® 3.5（或之后版本）以使用 KX III

KX III 检查你的目前 Java 版本，如果不适应，会提示你对其进行升级。

参看 ***Java Runtime Environment (JRE) 备注*** (p. 314) 获取其他信息。

多语言键盘 JRE 要求

为了在 KX III 和 Virtual KVM Client（VKC）上使用多语言键盘，要安装多语言版本的 JRE™。

审计日志和系统日志记录的事件

下面列出并说明 KX III 审计日志和系统日志记录的事件。

- Access Login（访问登录）— 用户已登录 KX III
- Access Logout（访问退出）— 用户已退出 KX III
- Active USB Profile（活动 USB 配置文件）— USB 配置文件活动
- CIM Connected（CIM 已连接）— CIM 已连接
- CIM Disconnected（CIM 已断开）— CIM 已断开
- Connection Lost（连接中断）— 断开了目标服务器连接
- Disconnected User（已断开用户）— 用户已断开端口
- End CC Control（结束 CC 控制）— CC-SG 管理结束
- Login Failed（登录失败）— 用户登录失败
- Password Changed（密码已更改）— 密码已更改
- Port Connect（端口连接）— 端口已连接
- Port Disconnect（端口断开）— 端口断开
- Port Status Change（端口状态变化）— 端口状态变化
- Scan Started（扫描已开始）— 已开始扫描目标服务器
- Scan Stopped（扫描已停止）— 已停止扫描目标服务器
- Session Timeout（会话超时）— 发生会话超时
- VM Image Connected（VM 镜像文件已连接）— VM 镜像文件已连接
- VM Image Disconnected（VM 镜像文件已断开）— VM 镜像文件已断开

Ap E 参考资料

在本章内

概述

本节重点说明在使用 KX III 时的注意事项。将记录未来升级，可通过 KX III Remote Console 界面的 Help（帮助）链接查看升级信息。

注意：本节中的部分主题涉及到 Raritan 的多种其他设备，因为各种设备受这些信息的影响。

Java Runtime Environment (JRE) 备注

禁用 Java 高速缓存并清除 Java 高速缓存。

强烈建议你禁用 Microsoft Windows® 中的 Java 高速缓存，并清除 Java 高速缓存。

▶ **要禁用 Java 高速缓存并清除缓存：**

1. 从 Windows “开始”(Start) 菜单中单击“控制面板”(Control Panel)。
2. 双击“Java”图标以启动它。将出现“Java 控制面板”(Java Control Panel)。
3. 要禁用 Java 高速缓存，请执行下列操作：

a. 从“常规”(General) 选项卡，单击“设置”(Settings) 按钮。将显示“临时文件设置”(Temporary Files Settings) 对话框。

b. 单击“查看小应用程序”(View Applets) 按钮。将打开“Java 小应用程序高速缓存查看器”(Java Applet Cache Viewer)：

c. 取消选中“启用高速缓存”(Enable Caching) 复选框。

d. 单击 OK（确定）。

4. 要清除 Java 高速缓存，请执行下列操作：

a. 从“临时文件设置”(Temporary Files Settings) 对话框中，单击“删除文件”(Delete Files) 按钮。将显示“删除临时文件”(Delete Temporary Files) 对话框。

b. 选择要删除的临时文件。

c. 单击 OK（确定）。

Java 不在 Mac 上正常加载

如果你在使用 Mac® 并在从 Mac® 端口访问表连接到设备时看到如下消息，则 Java™ 没有正常加载：

“在获取开放目标服务器列表时出错，请在几秒钟后重试”。

如果出现此消息，从如下网站检查你的 Java 安装：
http://www.java.com/en/download/testjava.jsp
http://www.java.com/en/download/testjava.jsp

如果你的 Java 程序显示不活跃，你可以从本页面将其启用。如果它没有被正确安装，一个消息会提示你，然后你可以重新安装 Java。

IPv6 支持注意事项

操作系统 IPv6 支持注意事项

Java

Java™ 1.7 在下列平台上支持 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
- Solaris 10 和更高版本
- Windows XP® SP1 和 Windows 2003®、Windows Vista® 和 Windows 7 操作系统

Java *不*支持下列 IPv6 配置：

- J2SE 在 Microsoft® Windows® 上不支持 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。如要了解详情，参看 http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html。

Windows

- Windows XP 和 Windows 2003 用户必须安装 Microsoft IPv6 服务包才能启用 IPv6。
- 对于在 Windows XP 上运行 AKC 和 IPv6，要把可执行文件 kxgui.exe 添加到防火墙例外表上。查看客户机上的日志文件确定 kxgui.exe 文件存储位置的完整路径。

Samba

- 在使用 Samba 时，虚拟媒体不支持 IPv6。

AKC 下载服务器证书验证 IPv6 支持备注

如果正连接 KX III 独立设备且已启用 AKC 下载服务器证书验证支持，生成该证书的有效 IPv6 格式将是：

- `CN=[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]`，有前导 0

  或者

- `CN=[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]`，无零压缩

双协议堆登录性能问题

如果在双协议堆配置下使用 KX III，必须在 KX III 上正确配置域名系统 (DNS)，在登录时才能避免出现延迟现象。

参看*添加网络浏览器界面提示* (参看 "*添加网络浏览器界面注意事项*" p. 103)了解如何在 KX III 上配置 DNS。

CIM 备注

在 Linux 目标服务器上使用 Windows 三键鼠标

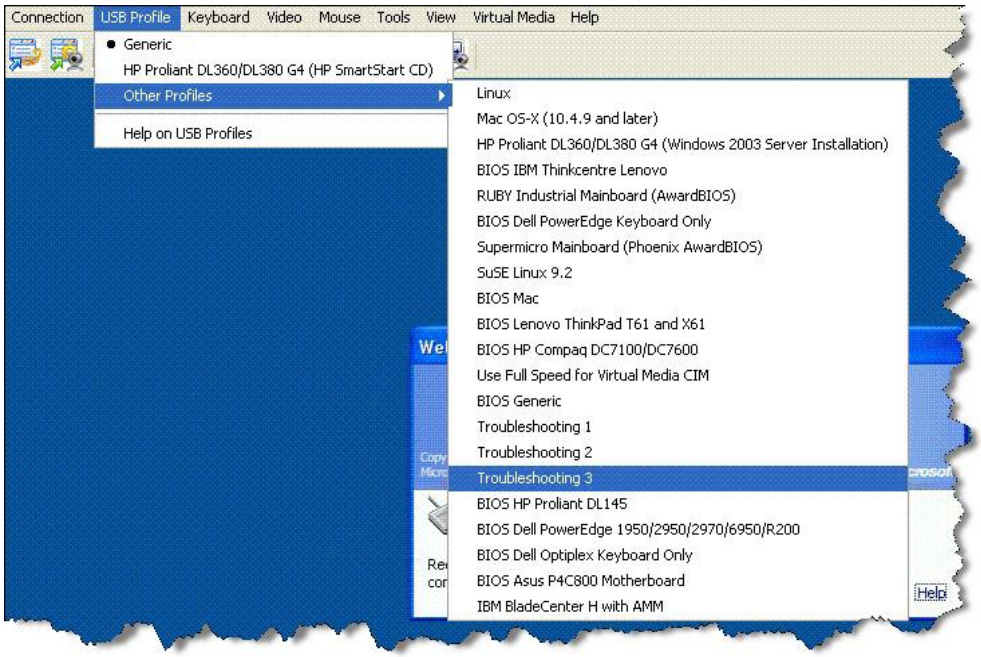
在与 Linux® 目标服务器相连的 Windows® 客户机上使用三键鼠标时，左鼠标按钮可能被映射到 Windows 客户机三键鼠标的中间按钮。

Windows 2000 虚拟媒体 USB 组合设备特性

与 USB 非组合设备一样，Windows 2000® 操作系统不支持 Raritan D2CIM-VUSB 等 USB 组合设备。

因此，对于被 D2CIM-VUSB 映射的设备，不显示 Safely Remove Hardware（安全拆除硬件）系统托盘图标，在断开设备时可能显示一条警告消息。Raritan 尚未从此消息上发现任何问题。

Raritan 的美国工程部开发了一个支持 Safely Remove Hardware（安全拆除硬件）图标的配置，不再显示此 Windows 消息。这 Configuration（配置）：requires the use of theD2CIM-DVUSB 虚拟媒体 adapter 和故障排除 3USB 配置文件 that configures theD2CIM-DVUSBas a non-composite USBDEVICEsupporting a single 虚拟媒体连接.Raritan 在美国和日本成功测试了此配置。



虚拟媒体备注

不能从 Linux 客户机连接设备

如果你不能从安装 Java™ 1.7.0(升级 45 更高版本)的 Linux® Fedora™ 18 客户机上连接目标服务器上的虚拟每天驱动器，请禁用客户机 Fedora 18 上的 SELinux 以解决这一问题。

不能从 Mac 客户机写入/自一个文件

如果你从运行 Java™ 1.7 的 Safari® 6.1 的 Mac® 10.8.5 客户机连接 KX III 而不能在目标服务器上写入/自一个文件或访问虚拟媒体，请按照以下步骤纠正这一问题：

1. 在 Safari，选择偏好设置。
2. 在 Security（安全）选项卡下选择 Manage Website Settings（管理网络设置）。
3. 点击“Website for KX3（KX3 的网站）”。
4. 选择下拉菜单中的“Run in safe mode（在安全模式下运行）”。
5. 重启 Safari。

在 Windows 环境下通过 VKC 和 AKC 使用虚拟媒体

Windows XP® 操作系统管理员权限和标准用户权限不同于 Windows Vista® 操作系统和 Windows 7® 操作系统的管理员权限和标准用户权限。

在 Vista 或 Windows 7 上启用虚拟媒体之后，用户访问控制 (UAC) 给用户提供访问应用程序所需的最低权限。例如针对 Internet Explorer® 提供的 Run as Administrator（作为管理员运行）选项允许用户执行管理员级任务，否则即使用户使用管理员登录名登录，也不能访问这些任务。

这两个功能都影响用户可通过 Virtual KVM Client (VKC) 和 Active KVM Client (AKC) 访问的虚拟媒体类型。参看 Microsoft® 帮助文件，进一步了解这些功能及其用法。

下面列出用户在 Windows 环境下可以通过 VKC 和 AKC 访问的虚拟媒体。这些功能按每个 Windows 用户角色可以访问的客户机功能和虚拟媒体功能进行分类。

Windows XP

如果在 Windows XP 环境下运行 VKC 和 AKC，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。

Windows Vista 和 Windows 7

如果在 Windows Vista 或 Windows 7 环境下运行 VKC 和 AKC，并启用 UAC，可以根据用户的 Windows 角色访问下列媒体类型：

客户机	管理员	标准用户
AKC 和 VKC	访问： • 固定驱动器和固定驱动器分区 • 可拆卸驱动器 • CD/DVD 驱动器 • ISO 镜像文件 • 远程 ISO 镜像文件	访问： • 可拆卸驱动器 • CD/DVD 驱动器 • ISO 镜像文件 • 远程 ISO 镜像文件

在添加文件之后不刷新虚拟媒体

在安装虚拟媒体驱动器之后，如果给该驱动器添加了文件，目标服务器可能不立刻显示这些文件。断开虚拟媒体连接，然后重新连接虚拟媒体。

虚拟媒体 Linux 驱动器列出两次

对于 KX III，当用户作为根用户登录 Linux™ 客户机时，Local Drive（本地驱动器）下拉列表列出两次驱动器。

例如你会看到 eg /dev/sdc 和 eg /dev/sdc1，其中第一个驱动器是引导扇区，第二个驱动器是磁盘的第一个分区。

访问 Windows 2000 Server 上的虚拟媒体

不能用 D2CIM-VUSB 访问 Windows 2000® Server 上的虚拟媒体本地驱动器。

断开 Mac 和 Linux 虚拟媒体 USB 驱动器

在 Linux® 或 Mac® 环境下：

- 对于 Linux 用户来说，如果有 /dev/sdb and /dev/sdb1，客户机仅使用 /dev/sdb1 并宣传其为可拆卸磁盘
- /dev/sdb 对客户来说不可用。
- 对于 Linux 用户来说，如果有 /dev/sdb 但没有 /dev/sdb1，/dev/sdb 被用作可拆卸磁盘
- 对于 Mac 用户来说，/dev/disk1 和 /dev/disk1s1 被使用

使用虚拟媒体时的目标服务器 BIOS 启动时间

如果采用虚拟方式将介质安装在目标服务器上，某些目标服务器的 BIOS 启动时间可能较长。

▶ 缩短启动时间：

1. 关闭 Virtual KVM Client，彻底释放虚拟媒体驱动器。
2. 重新启动目标服务器。

在虚拟媒体连接使用高速时虚拟媒体连接失败

在某些情况下，如果在使用高速 USB 连接时目标服务器出问题，或者目标服务器由于其他连接器和电缆造成信号弱而出现 USB 协议问题，可能不能选择 Use Full Speed for Virtual Media CIM（虚拟媒体 CIM 使用全速）（例如通过 dongle 连接刀片服务器）。

USB 端口和配置文件备注

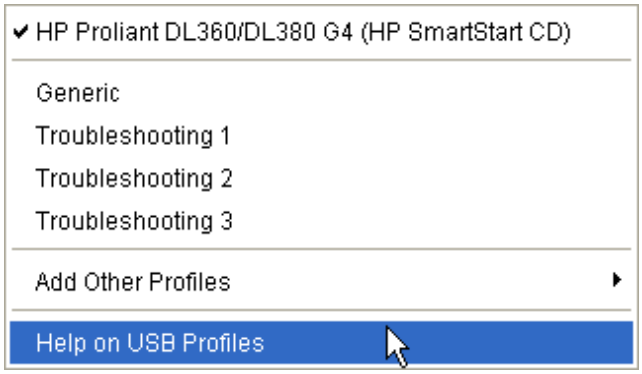
VM-CIM 和 DL360 USB 端口

HP® DL360 服务器背板上有一个 USB 端口，面板上还有一个 USB 端口。不能同时使用 DL360 的两个 USB 端口。因此，不能在 DL360 服务器上使用双 VM-CIM。

但是，如果将 USB2 集线器作为工作区连接到设备背板上的 USB 端口，可以将双 VM-CIM 插入集线器。

帮助选择 USB 配置文件

在 Virtual KVM Client (VKC) 上连接 KVM 目标服务器时，可以通过 USB Profile（USB 配置文件）菜单上的 Help on USB Profiles（USB 配置文件帮助）命令查看 USB 配置文件信息。



USB Profile Help（USB 配置文件帮助）窗口显示 USB 配置文件帮助。如要详细了解特定 USB 配置文件，参看可用的 USB 配置文件。

Raritan 针对众多操作系统级和 BIOS 级服务器实现推出一组标准的 USB 配置文件。这些配置文件旨在使远程 USB 设备配置和目标服务器配置实现最佳匹配。

Generic 配置文件可以满足大多数常部署的目标服务器配置的要求。

额外配置文件可以满足其他常部署的服务器配置（例如 Linux® 和 Mac MAC OS X®）的特定要求。

还有许多定制配置文件（用平台名称和 BIOS 版本号命名）可增强目标服务器的虚拟媒体功能，例如在 BIOS 级操作时。

Add Other Profiles（添加其他配置文件）便于你访问系统上可用的其他配置文件。在此列表上选择的配置文件被添加到 USB Profile（USB 配置文件）菜单上。其中包括一组故障排除配置文件，旨在协助你确定配置局限性。

USB Profile（USB 配置文件）菜单选项可以在 Console Device Settings（控制台设备设置）> Port Configuration（端口配置）页上配置。

如果 Raritan 提供的所有标准 USB 配置文件都不满足目标服务器要求，Raritan 技术支持部门可与你一起针对该目标服务器设计定制解决方案。Raritan 建议你：

1. 在 Raritan 网站 (www.raritan.com) 的 Firmware Upgrade（固件升级）页上查看最新版本说明，看看是否有可供你的配置使用的解决方案。
2. 如果没有，请在联系 Raritan 技术支持部门时提供下列信息：
   a. 目标服务器信息、制造商和型号，以及 BIOS、开发商和版本。
   b. 指定用途（例如重定向镜像文件，以便重新加载 CD 上的服务器操作系统）。

在使用智能卡读卡器时更改 USB 配置文件

在某些情况下，必须针对目标服务器更改 USB 配置文件。例如在目标服务器发生 High Speed USB（高速 USB）连接速度问题时，可能必须把连接速度更改为 Use Full Speed for Virtual Media CIM（针对虚拟媒体 CIM 使用全速）。

在更改配置文件时，可能显示 New Hardware Detected（检测到新硬件）消息，必须凭借管理权限登录目标服务器才能重新安装 USB 驱动程序。只有在目标服务器最初几次发现 USB 设备的新设置时，才会出现这种情况。在此之后，目标服务器会正确选择驱动程序。

视频模式和分辨率备注

使用 Mac 时，视频图像显示很暗

如果你在使用有 HDMI 视频端口的 Mac® 且视频看起来很暗，启用 CIM 上的 DVI 兼容模式解决这一问题。

参看*配置 CIM 端口* (p. 87)。

黑色条纹/栏显示在本地端口

特定的服务器和视频分辨率在本地端口显示时可能在屏幕边缘有黑色条纹

如果出现这种情况：

1. 尝试一个不同的分辨率，或
2. 如果在使用数字 CIM，则更改端口配置页面的显示原始分辨率至另一分辨率，或
3. 如果使用 HDMI CIM，使用 DVI 兼容模式。

联系 Raritan 技术支持部门寻求协助。

Sun 组合同步视频

不支持 Sun™ 组合同步视频。

SUSE/VESA 视频模式

SuSE X.org 配置工具 SaX2 采用 X.org 配置文件里的模式行项生成视频模式。这些视频模式不精确对应 VESA 视频模式定时（即使选择了 VESA 监视器）。另一方面，KX III 依靠精确的 VESA 模式定时进行正确同步。这一视差可能会导致黑边，失去图像的几个部分，引入噪声。

配置 SUSE 视频显示：

1. 生成的配置文件 /etc/X11/xorg.conf 包括 Monitor 节，本节有一个名为 UseModes 的选项。例如
   UseModes "Modes[0]"
2. 要么（用 #）备注此行，要么将它删除掉。
3. 重新启动 X 服务器。

在进行此项更改之后，将使用来自 X 服务器的内部视频模式定时，它精确对应 VESA 视频模式定时，使 KX III 能正常显示视频。

键盘备注

法文键盘

^ 符号（仅 Linux 客户机）

当 Linux® 客户机使用法文键盘时，Virtual KVM Client (VKC)将 Alt Gr+9 键组合当作 ^ 符号处理。

输入 ^ 符号：

按法文键盘上的 ^ 键（位于 P 键右边），立刻按 spacebar。

也可以创建一个由下列命令构成的宏：

1. 按住右 Alt
2. 按 9。
3. 释放 9。
4. 释放右 Alt。

注意：这些步骤不适用于（元音上的）抑扬音符号。在所有情况下，可以用法文键盘上的 ^ 键（位于 P 键右边）与另一个字符组合起来，输入抑扬音符号。

重音符号（仅 Windows XP® 操作系统客户机）

当 Windows XP® 客户机使用法文键盘时，在 Virtual KVM Client (VKC)上输入 Alt Gr+7 键组合，即可输入重音符号，但显示两个符号。

注意：Linux® 客户机不会发生这种情况。

数字键盘

在使用法文键盘时，在 Virtual KVM Client (VKC)上输入数字键盘符号显示如下：

数字键盘符号	显示为
/	;
。	;

代字号

在使用法文键盘时，在 Virtual KVM Client (VKC)上输入 Alt Gr+2 键组合不转换成代字号 (~)。

▶ **输入代字号：**

创建一个由下列命令构成的宏：

- 按住右 Alt
- 按 2
- 释放 2
- 释放右 Alt

键盘语言首选项（Fedora Linux 客户机）

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
英国英语	System Settings（系统设置）(Control Center[控制中心])
法文	Keyboard Indicator（键盘指示器）
德文	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])
瑞士德文	System Settings（系统设置）(Control Center[控制中心])
挪威文	Keyboard Indicator（键盘指示器）
瑞典文	Keyboard Indicator（键盘指示器）
丹麦文	Keyboard Indicator（键盘指示器）
日文	System Settings（系统设置）(Control Center[控制中心])
朝鲜文	System Settings（系统设置）(Control

语言	配置方法
美国英语/国际	默认值
	Center[控制中心])
斯洛文尼亚文	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])
Portuguese（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）。

在 Linux 客户机上使用匈牙利文键盘时，只有 JRE 1.6 （和更高版本）支持带双锐音符号的拉丁字母 Ü 和带双锐音符号的拉丁字母 Ö。

在 Fedora® Linux 客户机上可以采用几种方法设置键盘语言首选项。为了让键正确映射到 Virtual KVM Client (VKC)，必须使用下列方法。

用系统设置功能设置键盘语言：

1. 在工具栏上选择 System（系统）> Preferences（首选项）> Keyboard（键盘）。
2. 打开 Layouts（布局）选项卡。
3. 添加或选择相应的语言。
4. 单击 Close（关闭）按钮。

用键盘指示器设置键盘语言：

1. 用右键单击任务栏，选择 Add to Panel（添加到面板）。
2. 在 Add to Panel（添加到面板）对话框上用右键单击 Keyboard Indicator（键盘指示器），在菜单上选择 Open Keyboard Preferences（打开键盘首选项）。
3. 在 Keyboard Preferences（键盘首选项）对话框上单击 Layouts（布局）选项卡。
4. 按需要添加和删除语言。

宏未在 Linux 目标服务器上保存

如果你在 Linux® Fedora™ 18 系统并有 Java™ 1.7.0（升级 45 和更高版本）的目标服务器创建并保持宏收到如下错误消息，禁用目标服务器的 Fedora 18 中的 SELinux 以解决这一问题。

"在尝试写入新键盘宏时出错。没有添加键盘宏。"

Mac 键盘键不支持远程访问

在将 Mac® 用作客户机时，Java™ Runtime Environment (JRE™) 不捕捉 Mac® 键盘上的下列键：

- F9
- F10
- F11
- F14
- F15
- 增大音量
- 降低音量
- 静音
- 移除

因此，Virtual KVM Client (VKC) 不能处理在 Mac 客户机键盘上输入的这些键。

鼠标备注

鼠标指针同步 (Fedora)

在双鼠标模式下连接运行 Fedora® 7 的目标服务器时，如果目标服务器鼠标指针和本地鼠标指针不同步，把鼠标模式改成智能模式或标准模式即可实现同步。

单鼠标模式也可能只适合进行更好的控制。

重新同步鼠标光标：

- 使用 Virtual KVM Client（VKC）上的 Synchronize Mouse（同步鼠标）选项。

连接受 CC-SG 控制的目标服务器时为单鼠标模式

在用 Firefox® 连接受 CC-SG 控制、采用 DCIM-PS2 或 DCIM-USBG2 的 KX III 目标服务器时，如果在 Virtual KVM Client（VKC）上更改单鼠标模式，VKC 窗口不再是聚焦窗口，鼠标不响应。

如果发生这种情况，单击鼠标左键，后者按 Alt+Tab，即可让 VKC 窗口重新聚焦。

音频

音频播放和录音问题

可能会中断音频连接的功能

如果在连接音频设备时使用下列任何功能，可能会中断音频连接。Raritan 建议你在连接音频设备时不要使用这些功能：

- 自动检测视频
- 本地端口扩展使用
- 添加用户

同时使用目标服务器上的录音设备和播放设备存在的问题

在某些目标服务器上，由于 USB 集线器及其 USB 端口管理方式的缘故，可能无法同时连接录音设备和播放设备。考虑选择带宽消耗较小的音频格式。

如果这样还不能解决问题，把 D2CIM-DVUSB CIM 的键盘和鼠标端口连接到目标服务器的不同端口。如果这样还不能解决问题，把设备连接到 USB 集线器，再把集线器连接到目标服务器。

Linux 环境下的音频

在 Linux® 环境下使用音频功能时，存在下列已知问题。

- Linux® 用户用默认音频设备播放音频。如果选择非默认声卡，可能没有声音。
- SuSE 11 客户机要求通过 YAST 安装 Javas_1_6_0-sun-alsa（java-1_6_0-sun ALSA 支持）。
- 对于有内置麦克风的 Logitech® 耳机，只能使用 Mono Capture（单声道录音）选项。
- 为了显示设备，如果你运行 SUSE 11 并使用 ALSA 驱动程序，退出 KX III，

  此外，如果多次连接和断开音频设备，可能会多次列出此设备，而不是只列出一次。

- 在 Fedora Core® 13 目标服务器上使用音频功能时，把音频设置为 16 位 44k 可以大幅降低播放噪音。

Windows 环境下的音频

在通过 Virtual KVM Client (VKC)访问播放设备时，Windows® 64 位客户机上的 Connect Audio（连接音频）面板只列出一个播放设备。

列出的音频设备是默认设备，在 Connect Audio（连接音频）面板上显示为 Java Sound Audio Engine。

智能卡备注

Virtual KVM Client (VKC) Smart Card 连接至 Fedora Servers

如果在 Virtual KVM Client (VKC) 上用智能卡连接 Linux® Fedora® 服务器，要把 pcsc-lite 库升级到 1.4.102-3 或更高版本。

CC-SG 备注

在 CC-SG 代理模式下不知道 Virtual KVM Client 版本

在代理模式下，在 CommandCenter Secure Gateway (CC-SG) 上启动 VKC 时，不知道 Virtual KVM Client（VKC） 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）。

在设备不同端口之间移动

如果在同一台 Raritan 设备的不同端口之间移动，并在一分钟内恢复管理，CC-SG 可能显示一条错误消息。

如果恢复管理，将更新显示器显示的信息。

浏览器备注

解决在使用 Fedora 服务器时出现的 Firefox 冻结问题

如果访问 Firefox® 并使用 Fedora® 服务器，在打开 Firefox 时可能会出现冻结现象。

在服务器上安装 libnpjp2.so Java™ 插件可以解决这个问题。

Ap F 常见问题解答

在本章内

常见问题解答

问题	解答
Dominion KX III 是什么样的设备？	Dominion KX III 是第三代数字 KVM（键盘、视频和鼠标）切换器，允许八个 IT 管理员利用 BIOS 级功能通过网络访问和控制 8、16、32、64 台服务器。Dominion KX III 完全独立于硬件和操作系统；即使服务器停机，用户也可以排除服务器故障并重新配置服务器。 在机架部分，Dominion KX III 提供与传统的模拟 KVM 切换器相同的功能和便利性，同样节省空间和成本。但是，Dominion KX III 还集成了业界表现最佳的 KVM-over-IP 技术，允许多个管理员在任何联网工作站及 iPhone® 和 iPad® 上访问服务器 KVM 控制台。

问题	解答
KX III 与 KX II 有何不同？	KX III 是 KX II 的新一代版本。KX III 有现代化硬件设计和增加的计算能力和储存，为 IT 管理提供了 KVM-over-IP 访问，并且对广播应用程序的 IP 访问性能极佳。KX III 拥有 KX II 的所有功能，还有如下提升： KX III 的新视频引擎支持很多种类的应用程序，从传统的计算机应用程序到最具动态的、需要美妙 30 帧、1920x1080 视频、24 比特颜色、数字音频、双监视器和 DVI、HDMI、DisplayPort 和 VGA 视频的广播应用程序。 KX III 是行业第一个基于 DVI 的本地端口，其普遍用户界面为机架管理和服务器访问提供了新水平的产量和性能。 KX III 型号有分层端口，以连接多个 Dominion KX III 切换器并访问连接的服务器。通过一个统一的端口列表最多可访问 1024 台服务器。 KX III 支持所有 KX II 支持的 Dminion 和 Paragon II CIM。
Dominion KX III 与远程控制软件有哪些不同？	在远程使用 Dominion KX III 时，其界面看上去类似远程控制软件，例如 pcAnywhere™、Windows® Terminal Services/Remote Desktop、VNC 等。但是，由于 Dominion KX III 不是软件，而是一种硬件解决方案，因此功能更强大： 独立于操作硬件和操作系统 — Dominion KX III 可用于管理运行行许多常用操作系统的服务器，包括运行 Windows、Linux®、Solaris™ 等的 Intel®、Sun® 和 PowerPC 服务器。 独立于状态/无代理 – Dominion KX IIKX IIII 不要求运行受管服务器的操作系统，也不要求在受管服务器上安装任何特殊软件。 带外 — 即使受管服务器自己的网络连接不可用，仍然可以通过 Dominion KX III 管理服务器。 BIOS 级访问 - 即使服务器开机挂起、要求启动到安全模式或要求改变系统 BIOS 参数，Dominion KX III 仍能顺畅工作，完成这些配置。

问题	解答
Dominion KX III 是否可以安装在机架上？	可以。Dominion KX III 标配 19 英寸机架安装托架。它还可以反向安装在机架上，让服务器端口向外。
Dominion KX III 体积有多大？	Dominion KX III 只有 1U 高（KX3-864 和 KX3-464 除外，为 2U），适合安装在 19" 标准机架上，深度只有 11.4" (29cm)。Dominion KX3-832 和 KX3-864 的深度为 13.8" (36cm)。

远程访问

问题	解答
多少个用户可以远程访问每台 Dominion KX III 上的服务器？	Dominion KX III 设备每个用户通道最多支持八个用户建立远程连接，他们可以同时访问和控制一台目标服务器。对于 DKX3-116 等单通道设备，最多可以让八个远程用户访问和控制一台目标服务器。对于 DKX3-216 等双通道设备，第一个通道最多可以让八个远程用户访问和控制服务器，第二个通道最多可以让另外八个远程用户访问和控制服务器。对于四通道设备，每个通道最多支持八个用户，总共支持 32 (8 x 4) 个用户访问和控制四台服务器。同理，对于八通道设备，一个通道最多支持八个用户访问一台服务器，八个通道最多支持 32 个用户。
是否可以用 iPhone 或 iPad 远程访问服务器？	可以。用户可以用 iPhone 和 iPad 访问与 KX III 相连的服务器。
两个人是否可以同时看到同一台服务器？	可以。实际上最多可以让八个人同时访问和控制任何一台服务器。
两个人是否可以同时访问同一台服务器，其中一个人远程访问服务器，另一个人通过本地端口访问服务器？	可以。本地端口完全独立于远程端口。本地端口可以用 PC 共享功能访问同一台服务器。

<table>
<tr><th>问题</th><th>解答</th></tr>
<tr><td>要从客户机访问 Dominion KX III，需要哪些硬件、软件或网络配置？</td><td>由于 Dominion KX III 完全可以通过 Web 访问，因此不要求客户在客户机上安装专用访问软件。

注意：版本 KX III 3.0.0 不支持调制调节器，但是未来版本将支持。

可以用主流网络浏览器访问 Dominion KX III，包括：Internet Explorer® 和 Firefox®。

Dominion KX IIIadministrators can also perform 远程管理 :(set 密码相同 and 安全,重命名服务器, 更改 IP Address（IP 地址）：, etc.)正在使用 a convenient 基于浏览器界面：.</td></tr>
<tr><td>访问 Dominion KX III 所用的小程序文件有多大？下载时间有多长？</td><td>访问 Dominion KX III 所用的 Virtual KVM Client (VKC) 小程序大小约为 500KB。下图显示了以不同网络速度检索 Dominion KX III 的小程序所需的时间：

<table><tr><td>100Mbps</td><td>理论上 100MB 网络速度</td><td>.05 秒</td></tr><tr><td>60Mbps</td><td>实际上可能 100MB 网络速度</td><td>.08 秒</td></tr><tr><td>10Mbps</td><td>理论上 10MB 网络速度</td><td>.4 秒</td></tr><tr><td>6Mbps</td><td>实际上可能 10MB 网络速度</td><td>.8 秒</td></tr><tr><td>512Kbps</td><td>电缆调制解调器下载速度（典型）</td><td>8 秒</td></tr></table></td></tr>
<tr><td>你们是否提供 Windows KVM 客户机？</td><td>可以。我们有一个本机 .NET Windows 客户机，叫做 Raritan Active KVM Client (AKC)。参看 Active KVM Client (AKC) 帮助 (p. 258)</td></tr>
<tr><td>你们是否提供非 Windows KVM 客户机？</td><td>可以。Virtual KVM Client (VKC) 允许非 Windows 用户连接数据中心的目标服务器。参看 Virtual KVM Client (VKC) 帮助 (p. 212)</td></tr>
</table>

问题	解答
KVM Client 是否支持多种语言？	可以。Dominion KX III 的远程 HTML 用户界面和 KVM Client 支持日文、简体中文和繁体中文。可以单独使用，也可以通过 CC-SG 使用。
KVM 客户机是否支持双 LCD 监视器？	可以。对于那些要在桌面上使用多台 LCD 监视器提高生产力的客户，Dominion KX III 可以按全屏模式或标准模式启动与多台监视器的多个 KVM 会话。
是否支持有双显示卡的服务器？	是的，支持有双显示卡，远程用户可以使用扩展桌面配置远程访问有双显示卡的服务器。

通用虚拟媒体

问题	解答
哪些 Dominion KX III 型号支持虚拟媒体？	所有 Dominion KX III 型号都支持虚拟媒体。可以单独使用虚拟媒体，也可以通过 Raritan 的集中管理设备 CommandCenterr® Secure Gateway 使用虚拟媒体。
Dominion KX III 支持哪几类虚拟媒体？	Dominion KX III 支持下列几种虚拟媒体：内置和 USB 连接的 CD/DVD 驱动器、USB 海量存储设备、PC 硬盘和 ISO 镜像文件。

问题	解答
虚拟媒体有什么要求？	需要一个 Dominion KX III 虚拟媒体 CIM。有两个基于 VGA 的 CIM：一个 D2CIM-VUSB 或 D2CIM-DVUSB。 D2CIM-VUSB 有一个单 USB 连接器，供那些要在操作系统级使用虚拟媒体的客户使用。 D2CIM-DVUSB 有两个 USB 连接器，供那些要在 BIOS 级使用虚拟媒体的客户使用。智能卡验证、分层和数字音频还需要 D2CIM-DVUSB。 两种 CIM 都支持与（支持 USB 2.0 接口的）目标服务器进行虚拟媒体会话。CIM 包装数量有 32 个和 64 个两种，这些 CIM 支持绝对鼠标同步™和远程固件更新。 我们的 CIM 支持传统的模拟 VGA 视频。有三种新推出的双虚拟媒体 CIM 支持数字视频格式，包括 DVI、HDMI 和 DisplayPort，它们分别是 D2CIM-DVUSB-DVI、D2CIM-DVUSB-HDMI 和 D2CIM-DVUSB-DP。
虚拟媒体是否安全？	可以。虚拟媒体会话用 128 位 AES、256 位 AES 或 128 位 RC4 加密算法加密。
虚拟媒体真的支持音频？	可以。支持与 Dominion KX III 相连的服务器播放音频和录音。你可以用台式机或笔记本上的扬声器听在数据中心的远程服务器上播放的声音。还可以用台式机或笔记本上的麦克风在远程服务器上录音。需要使用数字 CIM 或 D2CIM-DVUSB 双虚拟媒体 CIM。
什么是 USB 配置文件？	为了使用虚拟媒体等 USB 服务，某些服务器需要使用专门配置的 USB 接口。USB 配置文件给服务器定制 KX III USB 接口，以便适应这些服务器特有的特点。
为什么要使用 USB 配置文件？	最常见的情况是在访问虚拟媒体设备时，如果 BIOS 不全面支持 USB 规范，需要在 BIOS 级使用 USB 配置文件。但是，有时在 BIOS 级使用配置文件是为了实现其他目的，例如使 Mac 服务器和 Linux 服务器实现鼠标同步。
如何使用 USB 配置文件？	管理员可以在 KX III 端口配置页上配置各个端口或端口组使用特定的 USB 配置文件。必要时也可以在 KX III 客户机上选择 USB 配置文件。参看用户指南了解详情。

问题	解答
在使用虚拟媒体时，是否始终要设置 USB 配置文件？	否。在许多情况下，在操作系统级使用虚拟媒体或在 BIOS 级工作但不访问虚拟媒体时，使用默认 USB 配置文件就可以了。
可以使用哪些配置文件？可以在哪里进一步了解配置文件？	参看用户指南了解可用配置文件详情。

带宽和 KVM-over-IP 性能

问题	解答
KVM-over-IP 系统如何使用带宽？	Dominion KX III 提供全新的视频处理，带来灵活、高性能的视频、高效使用带宽以及任何时间/任何地点通过 LAN、WAN 或网络的访问。 Dominion KX III 把目标服务器的键盘信号、视频信号和鼠标信号进行数字化处理、压缩和加密，通过 IP 网络把 IP 数据包发送到远程客户机建立与用户的远程会话。TheKX IIIprovides an at-the-rack experience based on its industry-leading 视频：processing algorithms. 屏幕变化（例如视频）占用绝大部分带宽，键盘活动和鼠标活动所用的带宽要小得多. 必须注意只有在用户处于活动状态时，才使用带宽。使用的带宽大小取决于服务器显示屏的变化情况。 如果视频没有变化，即用户不与服务器交互操作，通常不使用带宽。如果用户移动鼠标或输入字符，使用的带宽很小。如果显示器运行复杂的屏幕保护或播放视频，要使用较大的带宽。
带宽对 KVM-over-IP 性能有什么影响？	通常要在带宽和性能之间找到一个平衡点。可用带宽越大，可以实现更好的性能。在带宽很有限的情况下，性能可能会下降。Dominion KX III 经过优化，在众多环境下可以实现很高的性能。

问题	解答
哪些因素影响带宽？	有许多因素决定了要使用多大带宽。如上所述，主要因素是目标服务器屏幕的变化情况。这取决于用户的任务和操作。 其他因素包括服务器视频分辨率、联网速度和特性、KVM 客户机连接属性、客户机 PC 资源和显示卡噪声。
KX III 执行常见任务需要多大带宽？	带宽主要取决于用户的任务和操作。服务器屏幕变化越大，使用的带宽越大。
我应如何优化性能和带宽？	KX III 远程客户机有许多设置，可以用这些设置优化带宽和性能。在标准 LAN/WAN 环境下，默认设置具有机架访问级性能，带宽用量较小。 **优化目的.**使用此设置以配置视频引擎给为视频/广播应用程序的标准 IT/计算机应用程序。 **压缩。**将滑块移到左边，以获得最高的视频质量；移到右边，则获得最少的带宽。 **NoiseFilter（过滤器.** In most cases, the 默认设置 will work 最佳, however 你可以：move to the 左 for more responsive 视频：and to the 右 for 较低：bandwidth. 可降低带宽的其他措施包括：： ▪ 使用单色桌面背景，而不使用复杂图像。 ▪ 禁用屏幕保护 ▪ 在目标服务器上使用较低的分辨率 ▪ 取消 Windows 的“在拖动窗口时显示窗口内容”选项 ▪ 使用简单图像、主题和桌面（例如 Windows Classic）。
我想通过 Internet 联网。联网性能如何？	联网性能取决于远程客户机和 KX III 之间的 Internet 连接的带宽和延迟时间。在使用电缆调制解调器或高速 DSL 连接时，性能与 LAN/WAN 连接相仿。在使用低速链路时，采用上述建议提高性能。
我的网络环境有很高的带宽 ◦如何优化性能？	默认设置工作状态良好。你可以将连接属性设置移到左侧以降低视频性能。

问题	解答
最高支持多高的远程 (IP) 视频分辨率？	Dominion KX III 是首款也是唯一一款 KVM-over-IP 切换器，支持全高清晰度远程视频分辨率 1920x1080，同时数字视频帧数可达每秒 30 帧。 此外，还支持包括 1600x1200、1680x1050 和 1440x900 在内的宽屏格式，所以远程用户可以使用目前的高分辨率监视器。
音频需要多大带宽？	取决于所用音频格式的类型，但如果希望听到 CD 音质的声音，大约要使用 1.5Mbps 带宽。
配备 DVI 端口的服务器有何优点？	配备同时支持 DVI-A（模拟）和 DVI-I（集成模拟和数字）的 DVI 端口的服务器，可以利用 Raritan ADVI-VGA 等简单的无源适配器把服务器的 DVI 端口转换成 VGA 插头，从而连接 KX III CIM 的 VGA 插头。 具备 DVI 端口支持 DVI-I 或 DVI-D（数字）的服务器可以使用新的 D2CIM-DVUSB-DVI CIM。

IPv6 联网

问题	解答
什么是 IPv6？	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。 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。 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。
为什么 KX III 支持 IPv6 联网？	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。
双协议堆是什么？为什么需要它？	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。

问题	解答
如何在 KX III 上启用 IPv6？	在 Network Settings（网络设置）页上选择 Device Settings（设备设置）选项卡。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 III 时会发生什么情况？	KX III 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。 使用 KX III 的双堆结构，这些服务器可通过以下途径访问：(1) IPv4 地址、(2) IPv6 地址或 (3) 主机名。所以，KX III 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 III 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 www.ipv6.org 上了解 IPv6。《KX III 用户指南》说明 KX III 对 IPv6 的支持。

服务器

问题	解答
Dominion KX III 是否依赖 Windows 服务器才能工作？	绝对不依赖 Windows 服务器。由于用户要求 KVM 基础架构在任何情况下都始终可用（因为他们可能需要使用 KVM 基础架构来修复问题），因此 Dominion KX III 设计为完全独立于任何外部服务器。
把服务器连接到 Dominion KX III 需要做哪些准备工作？	设置鼠标参数选项让用户实现最佳鼠标同步，同时关闭那些会影响屏幕显示的屏幕保护程序和电源管理功能。
鼠标同步怎么样？	过去 KVM-over-IP 鼠标同步是一件很麻烦的事情。Dominion KX III 的绝对鼠标同步功能使鼠标完全同步，不需要在 Windows 和 Apple® Mac 服务器上更改服务器鼠标设置。对于其他服务器，可以使用智能鼠标模式或快速单鼠标模式避免更改服务器鼠标设置。
Dominion KX III 包装箱里都有哪些东西？	包括：(1) Dominion KX III 设备，(2) 快速安装指南，(3) 标准 19" 机架安装托架，(4) 用户手册 CD-ROM，(6) 适合当地使用的交流电源线，(7) 保修卡和其他文档。

刀片服务器

问题	解答
是否可以把刀片服务器连接到 Dominion KX III？	可以。Dominion KX III 支持下列主要刀片服务器制造商推出的常用刀片服务器产品：HP®、IBM®、Dell® 和 Cisco®。
支持哪些刀片服务器？	支持下列产品：Dell PowerEdge® 1855、1955 和 M1000e；HP BladeSystem c3000 和 c7000；IBM BladeCenter® H、E 和 S；Cisco UCS B 系列。
应该使用哪种 CIM？	取决于你使用的特定型号刀片服务器的 KVM 端口的类型。支持下列 CIM：DCIM-PS2、DCIM-USBG2、D2CIM-VUSB 和 D2CIM-DVUSB。
可以使用哪些访问和控制？	Dominion KX III 提供安全的自动化 KVM 访问：(1) 在机架上访问，(2) 基于 IP 的远程访问，(3) 通过 CommandCenter 访问，(4) 通过调制解调器访问。
是否必须用键盘在不同的刀片服务器之间来回切换？	某些刀片服务器要求你用热键在不同的刀片服务器之间来回切换。在使用 Dominion KX III 时，不必使用这些热键。只需单击刀片服务器名称，Dominion KX III 就自动切换到此刀片服务器，不需要使用热键。
是否可以访问刀片服务器管理模块？	可以。可以定义管理模块 URL，并在 Dominion KX III 或 CommandCenter Secure Gateway 上访问管理模块。如果这样配置，只需单击一下即可访问管理模块。
Dominion KX III 可以连接多少刀片服务器？	为了保证性能和可靠性，最多可以把八个任何型号的刀片服务器机箱连接到一台 Dominion KX III。Raritan 建议你将设备支持的远程连接数加倍。例如对于有两个远程通道的 KX3-216，我们建议你最多连接四个刀片服务器机箱。当然，可以把各台服务器连接到其余服务器端口。
我们是使用 CommandCenter Secure Gateway 的大企业客户，是否可以通过 CommandCenter Secure Gateway 访问刀片服务器？	可以。在 Dominion KX III 上配置刀片服务器之后，CommandCenter Secure Gateway 用户可以通过 KVM 连接访问这些服务器。此外，刀片服务器按机箱和 CommandCenter Secure Gateway 定制视图进行组织管理。

问题	解答
如果使用带内 KVM 访问或嵌入式 KVM 访问，会发什么情况？	可以在 CommandCenter Secure Gateway 上配置刀片服务器带内访问和嵌入式访问。
我们要在部分刀片服务器上运行 VMware®。是否支持它？	可以。在使用 CommandCenter Secure Gateway 时，可以显示和访问在刀片服务器上运行的虚拟机。
是否支持虚拟媒体？	这取决于刀片服务器。HP 刀片服务器支持虚拟媒体。IBM BladeCenter（BladeCenter T 除外）配置得当也支持虚拟媒体。必须使用虚拟媒体 CIM — D2CIM-VUSB 或 D2CIM-DVUSB。
是否支持绝对鼠标同步？	在刀片服务器机箱上安装了内置 KVM 切换器的服务器，通常不支持绝对鼠标技术。对于 HP 刀片服务器和部分 Dell 刀片服务器，每个刀片服务器连接一个 CIM，所以支持绝对鼠标同步。
刀片服务器访问是否安全？	可以。在访问刀片服务器时，使用所有标准的 Dominion KX III 安全功能，例如 128 位加密或 256 位加密。此外，还有刀片服务器特定的安全功能，例如刀片服务器访问权限和热键封锁，防止未经授权的访问。
Dominion KSX II 或 KX III-101 是否支持刀片服务器？	这些产品现在不支持刀片服务器。

安装

问题	解答
除了 Dominion KX III 设备本身，我还需要向 Raritan 订购哪些部件才能安装 Dominion KX III？	连接 Dominion KX III 的每台服务器需要一个 Dominion 或 Paragon 计算机接口模块 (CIM)，这是直接插入服务器的键盘端口、视频端口和鼠标端口的适配器。
在安装设备时应该使用哪种 Cat5 电缆？	Dominion KX III 可以使用任何标准 UTP（非屏蔽双绞线）电缆，包括 Cat5、5e 类或 Cat6。在 Raritan 手册和销售材料上，我们统称这些电缆为 Cat5 电缆。实际上，任何品牌的 UTP 电缆都能满足 Dominion KX III 的要求。

问题	解答
哪些类型的服务器可以连接 Dominion KX III？	Dominion KX III 支持任何制造商生产的服务器。只要服务器配备标准键盘端口、视频端口和鼠标端口，都可以连接到 Dominion KX II。此外，可以使用 P2CIM-SER CIM 控制配备串行端口的服务器。
如何把服务器连接到 Dominion KX III？	连接 Dominion KX III 的服务器需要一个 Dominion 或 Paragon CIM，此 CIM 直接连接服务器键盘端口、视频端口和鼠标端口。然后用 Cat5、5e 或 Cat6 等标准 UTP（非屏蔽双绞线）电缆把每个 CIM 连接到 Dominion KX III。
服务器和 Dominion KX III 可以相距多远？	服务器通常可与 Dominion KX III 相距最远 150 英尺（45 米），视服务器类型而定。（参看*目标服务器视频分辨率支持连接距离和刷新频率* (参看 "*目标服务器视频分辨率支持的连接距离和刷新速率*" p. 295)）对于支持虚拟媒体和绝对鼠标同步的 D2CIM-VUSB CIM，建议的距离为 100 英尺（30 米）。
在工作过程中断开键盘或鼠标时，某些操作系统会锁住。在从与 Dominion KX III 相连的服务器切换出来时，是什么防止这些服务器锁定？	每个 Dominion 计算机接口模块 (DCIM) dongle 给相连的服务器充当虚拟键盘和虚拟鼠标。这种技术称为 KME (keyboard/mouse emulation)。Raritan 的 KME 技术是数据中心级的，经过实践检验，其可靠性远远超过低端 KVM 切换器使用的技术：这是 15 年开发经验的结晶，已在全球应用于数百万台服务器。
是否需要在与 Dominion KX III 相连的服务器上安装任何代理？	与 Dominion KX III 相连的服务器不需要安装任何软件代理，因为 Dominion KX III 通过硬件直接连接服务器的键盘端口、视频端口和鼠标端口。
每台 Dominion KX III 设备可以连接多少台服务器？	1U Dominion KX III 设备有 8 个、16 个或 32 个服务器端口，2U 设备有 64 个服务器端口。这是业界最高的数字 KVM 切换器端口密度。
如果把一台服务器与 Dominion KX II 设备断开，然后把它重新连接到另一台 Dominion KX II 设备，或者把它连接到同一台 Dominion KX II 设备的其他端口，会发生什么情况？	当服务器从一个端口移动到另一个端口时，Dominion KX III 自动更新服务器端口名称。此外，这种自动更新不能影响本地访问端口，而且还广播到所有远程客户机和任选的 CommandCenter Secure Gateway 管理工具。

问题	解答
如何把 Cisco 路由器/交换机或无头式 Sun 服务器等串行控制 (RS-232) 设备连接到 Dominion KX III？	如果只有几台串行控制设备，可以用 Raritan P2CIM-SER 串行转换器把它们连接到 Dominion KX III。 可以也可以考虑部署 Dominion KSX II，它集成了 KVM 和串行切换器。DKSX-144 有四个 KVM-over-IP 端口和四个串行端口。 DKSX-188 有八个 KVM-over-IP 端口和八个串行端口。 但是，如果有很多串行控制设备，建议使用 Raritan Dominion SX 安全控制台服务器系列产品。Dominion SX 的串行功能比 Dominion KX II 多，价格较低。SX 易于使用、配置和管理，可与 Dominion 系列产品完全集成在一起。

本地端口 - KX III

问题	解答
是否可以在机架上直接访问服务器？	可以。在机架上，Dominion KX III 像传统 KVM 切换器那样工作，可以用一个键盘、显示器和鼠标控制最多 64 台服务器。可以采用基于浏览器的用户界面在服务器之间来回切换，也可以用热键切换。
是否可以合并多台 KX III 的本地端口？	可以。可以利用 KX II 切换器的分层功能，把多台 KX III 的本地端口连接到另一台 KX III。然后可以在数据中心的一个点，通过合并端口列表访问与 KX II 设备相连的服务器。
在使用本地端口时，是否妨碍其他用户远程访问服务器？	否。Dominion KX III 本地端口具有对服务器的完全独立的访问路径。这意味着用户可以在机架本地访问服务器，且不会减少可同时远程访问机架的用户数量。
是否可以在本地端口上使用 USB 键盘或鼠标？	可以。Dominion KX III 本地端口包括 USB 键盘端口和鼠标端口。Dominion KX III 切换器没有 PS/2 本地端口。使用 PS/2 键盘和鼠标的客户应该使用 PS/2-USB 适配器。

问题	解答
在机架上访问时是否有显示屏进行本地访问？	有，不过 Dominion KX III 的机架访问提供的不仅仅是传统的 OSD。Dominion KX III 的本地端口为机架访问提供业界第一个基于浏览器的界面，使用同一界面进行本地访问和远程访问。此外，可以在机架上执行大多数管理功能。
在使用本地端口时，如何选择不同的服务器？	本地端口采用与远程客户机相同的用户界面显示相连的服务器。用户只需单击鼠标或按热键，即可连接服务器。
如何确保只有授权用户可以通过本地端口访问服务器？	尝试使用本地端口的用户必须进行与远程访问相同的验证。这意味着： 如果 Dominion KX III 配置为与外部 RADIUS、LDAP 或 Active Directory 服务器交互，则尝试访问本地端口的用户将针对同一服务器进行认证。 如果外部验证服务器不可用，Dominion KX III 使用自己的内部验证数据库进行验证。 Dominion KX III 具有自己的独立验证，支持即时安装。

扩展本地端口

问题	解答
什么是扩展本地端口？	Dominion KX2-808、KX2-832 和 KX2-864 具备扩展本地端口。相对的 Dominion KX III 型号没有扩展的本地端口。相反，所有的 KX III 型号有一个分层端口。 如需扩展 KX III 的数字本地端口，你可以使用 Raritan Cat5 Reach DVI 产品帮助本地和远程访问至最多 500 米。 参看***Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality（连接 KX III 和 Cat5 Reach DVI - 提供延展的当地端口功能）*** (p. 273)

双电源

问题	解答
Dominion KX III 是否有双电源选件？	可以。所有 Dominion KX III 型号都配有双交流电源输入和具有自动故障切换功能的电源。如果其中一个电源输入或电源发生故障，KX III 自动切换到另一个电源输入或电源。
Dominion KX III 使用的电源是否自动检测电压设置？	可以。Dominion KX III 的电源可以在 100-240 伏 50-60 赫兹的交流电压范围内使用。
如果电源或电源输入发生故障，是否通知我？	Dominion KX III 面板 LED 通知用户电源发生故障。还在审计日志里添加一个条目，并在 KX 远程客户机用户界面上显示此条目。如果管理员配置了 SNMP 事件或系统日志事件，还生成 SNMP 事件或系统日志事件。

智能电源条 (PDU) 控制

问题	解答
Dominion KX III 具备哪些远程电源控制功能？	Raritan 智能 PDU 可以连接 Dominion KX III 对目标服务器和其他设备进行电源控制。对于服务器，在进行简单的一次性配置步骤之后，只需单击服务器名称即可接通或断开服务器电源，或者给挂起的服务器重新通电。
Dominion KX III 支持哪些类型的电源条？	Raritan'sDominionPX™ and 远程电源控制(RPC)电源条：. 这些电源条有许多出口、插口和不同的电流额定值。注意不要把 PM 系列的电源条连接到 Dominion KX III，因为这些电源条没有出口开关功能。
一台 Dominion KX III 可以连接多少 PDU？	一台 Dominion KX III 设备最多可以连接八个 PDU。
如何把 PDU 连接到 Dominion KX III？	用 D2CIM-PWR 把电源条连接到 Dominion KX III。必须单独购买 D2CIM-PWR，PDU 不带 D2CIM-PWR。
Dominion KX III 是否支持具有多个电源的服务器？	可以。可以轻松配置 Dominion KX III 支持与多个电源条相连的多电源服务器。每台目标服务器最多可以连接四个电源。

问题	解答
Dominion KX III 是否显示 PDU 统计数据和测量数据？	可以。检索 PDU 级电源统计数据并给用户显示这些数据，包括功率、电流和电压。
远程电源控制是否要求对相连的服务器进行特殊配置？	某些服务器配备默认 BIOS 设置，使服务器在掉电并重新通电之后不自动重新启动。对于这些服务器，参看相应的服务器说明书更改此设置。
在给服务器重新通电时，会发生什么情况？	注意这实际上相当于拔下服务器的交流电源插头，然后再插上插头。

Ethernet 和 IP 联网

问题	解答
Dominion KX III 的 Ethernet 接口速度是多少？	Dominion KX III 支持 Gigabit Ethernet 和 10/100Mbps Ethernet。KX III 支持两个 10/100/1000Mbps Ethernet 接口，可以配置速度和双工设置（自动检测或人工设置）。
是否可以通过无线连接访问 Dominion KX III？	可以。Dominion KX III 不仅使用标准 Ethernet，而且很节省带宽，同时提供质量非常高的视频。因此，如果无线客户机与 Dominion KX III 有网络连接，可以在 BIOS 级采用无线方式配置和管理服务器。
Dominion KX III 是否有双 Gigabit Ethernet 端口实现冗余故障切换或负载平衡？	可以。Dominion KX III 配有双 Gigabit Ethernet 端口实现冗余故障切换功能。如果主 Ethernet 端口（或与之相连的交换机/路由器）发生故障，Dominion KX III 将切换到具有相同 IP 地址的备用网络端口，确保服务器操作不中断。注意：管理员必须启用自动故障切换。
是否可以通过 VPN 使用 Dominion KX III？	可以。Dominion KX III 在第 1 层到第 4 层使用标准 Internet 协议 (IP) 技术。很容易采用 VPN 技术通过隧道发送流量。
是否可以同时使用 KX III 和代理服务器？	可以。假设远程客户机 PC 配置正确，KX III 可与 SOCKS 代理服务器一起使用。阅读用户手册或联机帮助了解详情。
为了启用对 Dominion KX III 的网络访问，必须在防火墙上打开多少 TCP 端口？	需要两个端口：发现其他 Dominion 设备并在 Raritan 设备和 CC-SG 之间通信所用的 TCP 端口 5000，以及 HTTPS 通信端口 443。

问题	解答
这些端口是否可以配置？	可以。管理员可以配置 Dominion KX III 的 TCP 端口。
是否可以将 Dominion KX III 与 CITRIX 一起使用？	Dominion KX III 可与正确配置的 Citrix 等远程访问产品一起使用，但 Raritan 无法保证它能实现可接受的性能。客户应该知道，Citrix 等产品使用的视频重定向技术在概念上类似数字化 KVM 切换器，所以可以同时使用这两种 KVM-over-IP 技术。
Dominion KX III 是否可以使用 DHCP？	可以使用 DHCP 分配的地址，但 Raritan 建议你使用固定地址，因为 Dominion KX III 是基础架构设备，通过固定 IP 地址可以更有效地访问和管理 Dominion KX III。
我通过 IP 网络连接 Dominion KX III 时出问题，这很可能是什么问题？	Dominion KX III 依赖 LAN/WAN 网络。可能会发生这些问题： Ethernet 自动协商。在某些网络上，10/100 自动协商无法正确工作，而且必须把 Dominion KX III 设备设置为 100Mbps/全双工或适合其网络的选项。 IP 地址重复。如果 Dominion KX III 的 IP 地址与另一台设备的 IP 地址相同，网络连接可能会不一致。 端口 5000 冲突。如果另一台设备正在使用端口 5000，必须更改 Dominion KX III 的默认端口（或者更改另一台设备使用的端口）。 在更改 Dominion KX III 的 IP 地址，或者更换新的 Dominion KX III 时，必须留有足够的时间让整个第 2 层和第 3 层网络知道它的 IP 地址和 MAC® 地址。

本地端口合并、分层和级联

问题	解答
如何把多台 Dominion KX III 设备整合在一起构成一个解决方案？	如要把多台 KX III 设备连起来进行合并本地访问，可以利用 KX III 的分层功能把多台分层（级联）KX III 切换器的分层端口连接到基础 KX III。然后可以在数据中心的一个点，通过合并端口列表访问与 KX III 设备相连的服务器。 必须用分层端口把分层 KX III 切换器连接到基础切换器。 可以在数据中心甚至远程 PC 上通过合并端口列表进行访问。可以通过分层端口列表或采用搜索方式（使用通配符），访问与分层 KX III 相连的所有服务器。 支持两层；在分层配置里，最多可以访问 1024 台设备。还支持远程电源控制。 未来版本将支持通过分层访问方式访问虚拟媒体、智能卡和刀片服务器。当然，只有在通过标准远程连接进行访问时，才能使用这些功能。 虽然通过合并端口列表访问远程 IP 服务器很方便，但为了实现最佳性能，建议你在 CommandCenter 上或服务器直接连接的 KX III 上访问分层服务器。
是否必须把多台 Dominion KX III 设备物理连起来？	多台 Dominion KX III 设备不需要物理连接在一起。Instead, eachDominion KX IIIUnit（设备）：connects to thenetwork, and they automatically work together as a single 解决方案：if deployed 发生 Raritan'sCommandCenter Secure Gateway 使用(CC-SG)设备. CC-SGacts as a singleAccess（访问 point for 远程访问 and. CC-SG 有一些便捷工具，例如综合配置、综合固件更新、单一验证和授权数据库。 用 CC-SG 集中管理远程访问的客户可以充分利用 KX III 的分层(级联)功能把多台 KX III 切换器的本地端口组合在一起，在数据中心的一个控制台上最多可以本地访问 1024 台服务器。
CC-SG 是否是必需的？	对于想单独使用(不使用中央管理系统)的客户，多台 Dominion KX III 设备仍然通过 IP 网络实现互操作，可以伸缩。可以在 Dominion KX III web 用户界面访问多台 KX III 切换器。

问题	解答
是否可以把现有的模拟 KVM 切换器连接到 Dominion KX III？	可以。模拟 KVM 切换器可以连接到 Dominion KX III 的其中一个服务器端口。Simply use a USB 计算机接口模块 (Computer Interface Module/CIM), and attach it to the 用户端口：of the existing 模拟 KVM 切换器. 采用分层结构把多台在本地端口支持热键切换的模拟 KVM 切换器连接到一台 Dominion KX III 切换器，即可远程或在数据中心通过合并端口列表切换这些模拟 KVM 切换器。 请注意模拟 KVM 切换器的规格各不相同，Raritan 不能保证所有第三方模拟 KVM 切换器都能互操作。联系 Raritan 技术支持部门了解详情。

计算机接口模块 (CIM)

问题	解答
你们的 CIM 支持哪些视频格式？	我们的 CIM 支持传统的模拟 VGA 视频。三种新推出的 CIM 支持数字视频格式，包括 DVI、HDMI 和 DisplayPort，它们分别是 D2CIM-DVUSB-DVI、D2CIM-DVUSB-HDMI 和 D2CIM-DVUSB-DP。
Raritan 模拟矩阵 KVM 切换器 Paragon 的计算机接口模块 (CIM) 是否可用于 Dominion KX III？	可以。某些 Paragon 计算机接口模块 (CIM) 可用于 Dominion KX IIXKIIII。（请查看网站上的 Raritan Dominion KX III 版本注释获得最新版发布的 CIM） 但是，由于 Paragon CIM 比 Dominion KX III CIM 昂贵（因为它们采用视频传输距离最远达 1000 英尺 [304 米] 的技术），通常不建议用户购买 Paragon CIM 用于 Dominion KX III。另外要注意在把 Paragon CIM 连接到 Dominion KX III 时，Paragon CIM 的视频传输距离最远为 150 英尺（46 米）（而不是 1000 英尺 [304 米]），与 Dominion KX III CIM 连接到 Paragon 时的视频传输距离相同。

问题	解答
Dominion KX III 是否支持 Paragon Dual CIM？	可以。Dominion KX III 支持 Paragon II Dual CIM（P2CIM-APS2DUAL 和 P2CIM-AUSBDUAL），可以把数据中心的两台服务器连接到两台不同的 Dominion KX II 切换器。 如果一台 KX III 切换器不可用，可以通过第二台 KX III 切换器访问服务器，从而实现冗余访问，使远程 KVM 访问权加倍。 请注意这些 CIM 是 Paragon CIM，所以它们不支持 KX III 高级功能，例如虚拟媒体和绝对鼠标、音频等。

安全

问题	解答
Dominion KX III 是否通过 FIPS 140-2 认证？	Dominion KX III 使用嵌入的、在 Linux 平台上运行的 FIPS 140-2 认证加密模块，按 FIPS 140-2 实现指导原则进行加密。用此加密模块加密 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。
Dominion KX III 使用哪种加密？	Dominion KX III 在 SSL 通信和自己的数据流中使用业界标准（且极为安全）的 256 位 AES 加密、128 位 AES 加密或 128 位加密。也就是说，远程客户机和 Dominion KX III 之间不会传输未经加密机制完全保护的数据。
Dominion KX III 是否支持美国政府 NIST 和 FIPS 标准建议的 AES 加密？	可以。Dominion KX III 使用高级加密标准 (AES) 加密提高安全性。可用 256-bit 和 128-bit。 AES 是美国政府批准的加密算法，是 National Institute of Standards and Technology (NIST) 的 FIPS Standard 197 建议的算法。
Dominion KX III 是否允许加密视频数据？还是只加密键盘数据和鼠标数据？	与竞争对手推出的只加密键盘数据和鼠标数据的解决方案不同的是，Dominion KX III 不会牺牲安全：它加密键盘数据、鼠标数据和视频数据。

问题	解答
Dominion KX III 如何集成 Active Directory、RADIUS 或 LDAP 等外部验证服务器？	可以通过非常简单的配置，让 Dominion KX III 把所有验证请求转发到 LDAP、Active Directory 或 RADIUS 等外部服务器。对于每个经过验证的用户，Dominion KX III 从验证服务器了解此用户所属的用户组。Dominion KX III 随后根据此用户所属的用户组来确定此用户的访问权限。
如何存储用户名和密码？	如果使用 Dominion KX III 的内部验证功能，采用加密格式存储用户名和密码等所有敏感信息。也就是说，包括 Raritan 技术支持部门或产品设计部门人员在内的任何人，都无法获取这些用户名和密码。
Dominion KX III 是否支持强密码？	可以。Dominion KX III 具有管理员可以配置的强密码检查功能，确保用户创建的密码符合公司和/或政府标准，并能抵御强力黑客攻击。
是否可以把自己的数字证书上载到 Dominion KX IIKX IIII？	可以。客户可以把自签名证书或证书机构提供的数字证书上载到 Dominion KX III 上增强验证和安全通信。
KX III 是否支持可配置的安全标志？	可以。对于在用户登录之前需要显示安全消息的政府机构、军队和其他对安全要求很高的客户，KX III 可以显示用户可配置的标志消息，可以有选择地要求用户接受安全协议。
我们的安全策略不允许使用标准 TCP 端口号。是否可以更改这些端口号？	可以。对于要避免使用标准 TCP/IP 端口号并增强安全的客户，Dominion KX III 允许管理员配置替代端口号。

智能卡和 CAC 验证

问题	解答
Dominion KX III 是否支持智能卡和 CAC 验证？	可以。支持对目标服务器进行智能卡和 DoD Common Access Card (CAC) 验证。
CAC 是什么？	CAC 经过 Homeland Security Presidential Directive 12 (HSPD-12) 批准，是美国政府开发的一种供军人和政府员工使用的智能卡。CAC 是采用多种技术的多用途智能卡，其目的是用作单一身份证。参看 FIPS 201 标准了解详情。

问题	解答
哪些 KX III 设备支持智能卡/CAC？	所有 Dominion KX III 设备都支持智能卡/CAC。Dominion KX III-101 目前不支持智能卡和 CAC。
大企业客户和中小企业客户是否也使用智能卡？	可以。但是，使用智能卡最多的机构是美国联邦政府。
哪些 CIM 支持智能卡/CAC？	D2CIM-DVUSB、D2CIM-DVUSB-DVI、D2CIM-DVUSB-HDMI 和 D2CIM-DVUSB-DP 是必需的 CIM。
支持哪些智能卡读卡器？	要求的读卡器标准是 USB CCID 和 PC/SC。参看用户指南了解认证读卡器清单和详情。
是否可以在本地端口和 CommandCenter 上进行智能卡/CAC 验证？	可以。可以在本地端口和 CommandCenter 上进行智能卡/CAC 验证。如要在本地端口进行验证，把兼容的智能卡读卡器连接到 Dominion KX III 的 USB 端口。

可管理性

问题	解答
Dominion KX III 是否可以通过网络浏览器进行远程管理和配置？	可以。Dominion KX III 完全可以通过网络浏览器进行远程配置。注意这不要求你在工作站上安装适当版本的 Java Runtime Environment (JRE)。除了 Dominion KX III 的 IP 地址初始设置，可以通过网络完全设置关于解决方案的任何配置。（实际上，使用交叉 Ethernet 电缆和 Dominion KX III 的默认 IP 地址时，甚至可以通过网络浏览器配置初始设置。）
是否可以备份和恢复 Dominion KX III 的配置？	可以。 可以通过网络远程使用 Dominion KX III 的备份和恢复功能，也可以通过 Web 浏览器使用。
Dominion KX III 具备什么样的审计和记录功能？	为了实现完整的跟踪记录，Dominion KX III 记录所有主要用户事件，并附带日期和时间戳。例如报告的事件包括（但不仅限于）：用户登录、用户退出、用户访问特定服务器、登录失败、配置更改等。

问题	解答
Dominion KX III 是否可以集成系统日志？	可以。除了 Dominion KX III 自己的内部记录功能，Dominion KX III 还可以把所有记录事件发送到中央系统日志服务器。
Dominion KX III 是否可以集成 SNMP？	可以。除了 Dominion KX III 自己的内部记录功能，Dominion KX III 还可以把 SNMP 陷阱发送到 SNMP 管理器。支持 SNMP v2 和 SNMP v3。
管理员是否可以让用户退出？	可以。管理员可以查看哪些用户登录了哪些端口，可以在必要时让用户退出特定端口或退出设备。
Dominion KX III 的内部时钟是否可与时间服务器同步？	可以。Dominion KX III 支持业界标准的 NTP 协议，用于与公司时间服务器同步或与任何公共时间服务器同步（假设允许出站 NTP 请求通过公司防火墙）。

文档和支持

问题	解答
是否有联机帮助？	可以。可以在 raritan.com 上找到联机帮助和支持文档，也可以在 KX III 用户界面上找到联机帮助。 联机帮助包括 KX III 管理和终端用户使用 Remote Console（远程控制台）的信息、Virtual KVM Client (VKC) Active KVM Client (AKC) 和 Local Console（本地控制台），以及 KX III 技术规格、参考资料、用 Paragon II 使用 KX III、连接 KX III 至 Cat5 Reach DVI、连接 KX III 至 T1700-LED，等等。
可以在哪里找到 Dominion KX III 支持文档？	可以在 raritan.com 的 KX III 找到支持文档。按固件版本列出支持文档。
有哪些支持文档？	有快速安装指南、联机帮助、从管理员角度的 PDF 版本的帮助和一本用户指南、版本说明和其他信息。
如果我有特殊服务器，应该使用哪种 CIM？	参看 CIM Guide 和 KX III 支持文档。新推出的数字视频 CIM 支持 DVI、HDMI 和 DisplayPort 视频标准。

问题	解答
KX III 硬件保修期有多长？	Dominion KX III 的标准保修期为两年，可以延长到五年。

其他

问题	解答
Dominion KX III 的默认 IP 地址是什么？	192.168.0.192
Dominion KX III 的默认用户名和密码是什么？	KX III 的默认用户名和密码是 admin/raritan [全部小写]。但是，为了实现最高级别的安全，Dominion KX III 强制管理员在首次启动 Dominion KX III 设备时更改默认管理用户名和密码。
我更改了 Dominion KX III 的管理密码，但后来忘记了；是否可以找回密码？	Dominion KX III 有一个硬件复位按钮，可以按此按钮让设备复位到出厂默认设置，把设备的管理员密码复位到默认密码。
如何从 Dominion KX II 迁移到 Dominion KX III？	KX II 客户通常可以继续使用现有的切换器许多年。随着数据中心的扩大，客户可以购买使用新的 KX III 设备。Raritan 的集中管理设备 CommandCenter Secure Gateway (CC-SG) 版本 6.0 支持 KX II 切换器和 KX III 切换器。
现有的 KX II CIM 是否可与 Dominion KX III 切换器一起使用？	可以。现有的 KX II CIM 可与 Dominion KX III 切换器一起使用。此外，Paragon CIM 也可与 KX III 一起使用。这样，想过渡到 KVM-over-IP 的 Paragon II 客户很容易迁移到 KX III。但是，你可能想考虑使用 D2CIM-VUSB CIM 和 D2CIM-DVUSB CIM，它们支持虚拟媒体和绝对鼠标、音频同步。此外，还有支持 DVI、HDMI 和 DisplayPort 的数字视频 CIM。

索引

符号

A

B

C

D

E

F

G

H

I

J

K

L

M

N

P

R

S

T

U

V

W

二划

三划

四划

五划

六划

七划

八划

九划

十划

十一划

十二划

十三划

十四划

十五划

十六划

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