



# AVOCENT® UNIVERSAL MANAGEMENT GATEWAY 装置

安装人员/用户指南

#### 欧盟通告

警告:本设备属于 A 类产品。在家用环境下,本产品可能会造成无线电干扰,因此用户可能需要采取充分的保护措施。

### 美国通告

警告: 未经负责合规性一方的明确许可而擅自对本设备进行更改或改装会使用户丧失操作此设备的权利。

**注:**本设备经测试符合 FCC 规范第 15 部分中关于 A 类数字设备的限制。这些限制可为本设备在商业环境下的使用 提供合理保护,防止有害干扰。本设备产生、使用并可能辐射射频能量,如果不按照说明手册进行安装和使用,可 能会对无线电通讯造成有害干扰。本设备在居住区使用时可能会造成有害干扰,在此情况下,用户应自行负责消除 干扰。

#### 加拿大通告

本 A 类数字设备符合加拿大 ICES-003 标准。

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

#### 日本通告

この装置は、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。 VCCI-A

#### 韩国通告

기종별	사용자 안내문		
A급 기기	이기기는 업무용으로 전자파적합등록을 한 기		
(업무용 정보통신기기)	기이오니 판매자 또는 사용자는 이 점을 주의		
	하시기 바라며 만약 잘못 판매 구입 하였을 때		
	에는 가정용으로 교환하시기 바랍니다.		

# Avocent® Universal Management Gateway 装置

安装人员/用户指南

Emerson、Emerson Network Power 和 Emerson Network Power 徽标是艾默生电气公司的商标或服务标志。Avocent、Avocent 徽标、Cyclades、DSView 和 Trellis 是 Avocent 公司的商标或服务标志。所有其他商标均为其各自所有者的财产。本文档可能包含 Avocent 公司的机密信息和/或专有信息。获得或持有本文档的用户无权复制和透露其内容,亦无权制造或销售其描述的任何产品。未经 Avocent 公司明确授权,严禁复制、透露或使用。©2013 Avocent 公司。保留所有权利。

注: 本文档支持的最高版本为2.0。

590-1071-511B

# 使用的符号

注: 以下符号可能会出现在文档中或产品上。

说明



此符号用于对用户发出警示,表明本设备附带的手册中有重要的操作和维护 (保养)说明。



### 危险电压

此符号用于对用户发出警示,表明产品的外壳内有未绝缘的危险电压,其强度 可能对人造成电击危险。



### 加电

此符号说明主开关处于电源接通位置上。



### 断电

此符号说明主开关处于电源断开位置上。



### 保护性接地接线端

此符号说明在与设备进行任何连接之前,必须将此接线端接地。



### 功能性接地接线端

此符号说明此接线端用于形成机箱的等电位接地。

产品概述	1
功能和优点	1
安全访问	1
自动检测	1
Web 用户界面 (UI)	2
VGA 和 USB 连接	2
CLI 设置端口	3
IPv4 和 IPv6 支持	3
安全	3
数据记录、通知、警报和数据缓冲	3
电源管理	3
自动搜索	4
对虚拟媒体和支持智能卡的装置的控制	4
灵活的用户和组	4
DSView 管理软件插件	4
安装	5
装置随附物品清单	5
机架和墙上安装	5
机架安装的安全考虑因素	5
机架安装	5
墙上和 0U 安装的安全考虑因素	6
墙上安装	6
缆线安装、维护和安全说明	7
连接硬件	8
装置接口	8
连接目标	9
打开装置	11
验证连接	11
前面板和后面板电源状态 LED	11
后面板以太网连接 LED	11
后面板自动检测/专用 IP 端口 LED	11
配置装置	11
配置示例	12
使用 Telnet 或 SSH 访问串行目标	14
初始装置设置	17
	17
左按判鬥泊	1/

分配 IP 地址	
本地或通过控制台端口连接	
设置网络	
防火墙	
<b>Web</b> 用户界面	
Web UI 概述	
使用侧面导航栏	
管理员角色	
操作员角色	
用户角色	
选项卡	
目标	
传感器	
事件	
管理	
管理	
装置设置	
SSH	
帮助文件	
电子邮件设置	
网络设置	
网络模式	
桥接组配置	
主机	
路由	
OSPF 和 BGP	
默认值	
用户	
用户角色	
用户	
密码策略	
抢占级别	
添加用户	
身份验证	
用户目标访问	
用户目标权限	
组	
目标	

目标	75
<b></b>	
服务	
王 利	
定义的网络	
送口	
防火墙和 NAT	
业书	
安全	
文	61
会话	61
- 週知日的地 	
剱子1期出 通知日的地	
Sysiog	
电丁邮件	
出 2	
KS-485	
OneWire 坏境	
OneWire 数子输入	
COM 数字输入	
传感器	
登录	
配电	
USB 设备	
备份固件	
固件	
启动	
目标组	54
默认设置	
活动会话	
UMIQ 模块	
KVM 管理	
串行端口警告	
串行数据记录	
串行管理	
搜索	
SP 管理	
端口配置	
许可	

服务处理	理器	
属性.		76
系统.		
会话.		77
SEL		
电源.		
传感器		
日志.		
螯告.		
UMIQ 栲	莫块	
串行控制	制台	
PDU		
传感器和	1事件	83
传感器		
事件		
风扇.		
温度.		
电源.		
CPU 利	口磁盘使用	
附录		
附录 A:	技术规格	
附录 B:	忘记密码	
附录 C:	从网络启动	
附录 D:	创建 SP 文件	
附录 E:	对 SP 进行故障排除	
附录 F:	视频分辨率	
附录 G:	技术支持	



Avocent<sup>®</sup> Universal Management Gateway 装置可用作目标设备的单个本地和远程安全访问点及管理 点。Avocent<sup>®</sup> Universal Management Gateway 装置支持安全的远程数据中心管理和从全球任何地点对 IT 资产进行带外管理。它提供键盘、视频和鼠标 (KVM) 功能,也可以远程执行服务器管理任务, 包括对托管目标设备进行电源控制和控制台访问。多个管理员可同时登录装置,并使用 web 用户 界面 (UI)、命令行界面 (CLI)或 DSView™ 4 管理软件访问和配置装置。

注: 本文档中的所有 DSView 软件实例均指 DSView 4 或更高版本。

Avocent® Universal Management Gateway 装置综合了 KVM over IP、服务处理器管理 (SPM)和访问及串行控制台管理访问。通过它,您可以随时随地进行灵活的目标设备管理控制和安全远程访问。

# 功能和优点

# 安全访问

通过以下本地(模拟控制台端口)和远程(数字IP)选项,您可安全访问本装置:

- LAN/WAN IP 网络连接。
- 串行目标设备连接。授权用户可与目标设备进行 Telnet、SSH v1、SSH v2 或 Raw 连接。对于要 用于串行目标设备连接的 Telnet 或 SSH,必须在有效的"安全配置"中配置 Telnet 或 SSH 服务。
- 控制台连接。管理员可以从本地终端,或从连接到控制台端口并可使用 CLI 的具有终端仿真程序的计算机登录。

# 自动检测

Avocent® Universal Management Gateway 2000 装置具有八个可用于服务处理器 (SP)或串行连接和管理的自动检测端口。另外,还具有专用于 SP 连接和管理的 32 个 RJ-45 端口。Avocent® Universal Management Gateway 4000 和 6000 装置具有 40 个可用于服务处理器 (SP)或串行连接和管理的自动检测端口。

支持自动检测的端口通过装置背面端口号旁边的青绿色短线标出。端口通过绿色或琥珀色连接 LED 指示当前处于活动状态的操作模式。默认情况下,所有能进行自动检测的端口都处于自动模 式。建议将端口设置保持为自动检测。绿色和琥珀色 LED 同时亮起时,即表示处于此状态。如果 将端口静态设置为两种模式之一,将仅亮起一盏相应的 LED。

### 图 1.1: 自动检测端口



### 网络和串行模式

自动检测端口可在网络或串行模式下运行。每种主要模式都具有以端口类别命名的子模式。网络端口类别适用于网络或 SP 连接。端口将自动检测网络目标,但对于 SP 连接目标,则需要手动配置。串行端口类别用于控制台连接或 PDU 连接。默认情况下,串行端口类别将自动检测控制台连接,但对于配电设备 (PDU)连接,则需要手动配置。端口将根据连接到装置的目标自动检测并切换到适当的模式。

当端口处于网络模式时,绿色 LED 将亮起。装置将提供与其连接的网络设备的 IP 地址。这样只是为了连接到要管理或访问的设备。装置不会用作传统网络交换机或通用网络访问防火墙,而 是专用于目标设备访问和管理。

**注意:**由于装置使用 DHCP 分配 IP 地址,它们可能会与生产基础设施的 DHCP 冲突。必须在网络上指定适当的 VLAN 网段划分,以避免发生这种冲突。

也可以为 SP 分配静态 IP 地址,装置可扫描 IP 范围以进行搜索。

当端口处于串行模式时,琥珀色 LED 将亮起。默认情况下,装置将分配控制台端口类别,并自动检测是否应用 Avocent 或 Cisco<sup>®</sup> 软脚位排列。连接到标准 RS-232 服务器控制台的速度、流量控制、奇偶校验和数据大小都是预定义的,但可以按端口进行修改。除了控制台模式,也可将 支持的 Avocent PDU 连接到装置并进行管理。

# Web 用户界面 (UI)

用户和管理员可通过 web UI(使用 HTTPS 访问)执行大多数任务。Web UI 在任何可对装置进行 网络访问的受支持计算机上的 Microsoft Internet Explorer<sup>®</sup> 和 Mozilla Firefox<sup>®</sup> 浏览器中运行。

管理员可以使用 web UI 创建用户帐户、授权组以及配置安全性和端口。授权用户可以通过 web UI 访问连接的设备,以进行故障排除、维护、重启电源或重新启动连接的设备及更改密码。有 关 web UI 的更多信息,请参阅第3章。

### VGA 和 USB 连接

标准 VGA 和 USB 连接可用于连接 LCD 托盘。这些端口位于装置的前面。VGA 控制台端口可用 于启动与目标的会话或执行 NetBoot 固件恢复。USB 端口用于连接 USB 键盘、鼠标、智能卡读 卡器、CD、DVD 或大容量存储设备。

表 1.1: VGA 控制台热键	
键击组合	操作
Alt + Tab	切换至循环列表中的下一视图
Alt + F1	查看 web UI
Alt +F2	查看用户 Shell
Alt + Esc	关闭当前视图和会话

# CLI 设置端口

串行设置端口提供对 CLI 和 Shell 的访问。装置不支持对 Bash Shell 进行 root 访问。CLI 用于管理 和配置装置。

### IPv4 和 IPv6 支持

装置支持双堆栈 IPv4 和 IPv6 协议。管理员可使用 web UI 或 CLI 进行配置,以支持 IPv4 和/或 IPv6 地址。下表说明了装置中提供的 IPv4 和 IPv6 支持。

- DHCP
- DSView 软件集成
- 以太网接口, GB1 (eth0) 和 GB2 (GB2 (eth1))
- 防火墙(IP表)
- HTTPS
- Linux 内核
- 远程身份验证: AD 和 LDAP 服务器
- SSH 和 Telnet 访问
- Syslog 服务器

注: IPv6不支持远程身份验证 NFS、NIS和 IPSec。

# 安全

管理员可通过"安全"设置确定在装置上启用了哪些网络服务。

## 数据记录、通知、警报和数据缓冲

管理员可以设置数据记录、通知和警报,以使用电子邮件和 syslog 消息通知管理员相关问题。管理员也可以本地存储缓冲数据。与装置和连接的服务器或设备相关的消息也可以发送到 syslog 服务器。

### 电源管理

通过 Avocent<sup>®</sup> Universal Management Gateway 装置,授权管理机架配电设备 (PDU) 和服务处理器 (SP) 电源的用户可打开电源、关闭电源,以及通过已插入连接的机架 PDU 的嵌入式 SP 设备重设服务器。

# 自动搜索

管理员可启用自动搜索来查找连接到端口的目标的主机名。自动搜索的默认探测字符串和响应 字符串范围很广。管理员可针对特定站点配置探测字符串和响应字符串。此外,也可通过 DSView 软件配置自动搜索。

### 支持的 SP

装置支持以下供应商提供的机架和刀片式服务器

SP: Dell<sup>®</sup>、HP、IBM<sup>®</sup>、Cisco<sup>®</sup>、Fujitsu<sup>®</sup>、Oracle<sup>®</sup> Sun 以及其他 IPMI 工具。要获取您装置上的固件版本支持的 SP 的完整列表,请访问 www.avocent.com 查看最新发行说明和固件更新。

### 对虚拟媒体和支持智能卡的装置的控制

通过 Avocent® Universal Management Gateway 装置,您可以查看虚拟媒体上的数据、将这些数据移 动到任何目标设备上或从任何目标设备上复制这些数据。通过实现操作系统安装、操作系统恢 复、硬盘恢复或复制、BIOS 更新和目标设备备份,您可以更有效地管理远程系统。

通用访问卡 (CAC)等智能卡可用于存储身份和身份验证信息,以便访问计算机、网络以及实施 安保措施的房间或建筑。

使用装置上的 USB 端口可直接连接虚拟媒体和智能卡读卡器。另外,虚拟媒体和智能卡读卡器 可连接到正在运行远程 web UI 或 DSView 管理软件且使用以太网连接与装置相连的任意远程工 作站。

### 灵活的用户和组

您可以为装置或身份验证服务器上的每个用户定义帐户。管理员默认拥有一个帐户,可以添加 和配置其他用户帐户。根据管理员可分配给自定义用户组的授权,可有选择地限制对端口的访问。

### DSView 管理软件插件

DSView 管理软件可与装置配合使用,使 IT 管理员可通过基于 web 的单一用户界面远程访问、监视和控制目标设备。DSView 软件代理和 SSH 传递功能可对 LAN 和 WAN 客户端进行便捷、安全的远程访问。有关更多信息,请参阅《用于 Avocent<sup>®</sup> Universal Management Gateway 装置的 DSView<sup>™</sup> 4 管理软件插件技术公告》。



安装 Avocent® Universal Management Gateway 装置前,请参阅以下列表,以确保具备随装置一起提供的所有物品,以及进行正确安装所需的其他物品。

# 装置随附物品清单

- 装置快速安装指南 (QIG)
- Avocent® Universal Management Gateway 装置安装支架快速安装指南 (QIG)
- 电源线
- RJ-45 转 DB-9F 交叉适配器
- 安装支架和螺钉
- 安全和法规声明指南

# 机架和墙上安装

您可以将装置安装在机架或机架柜中,或使用可选的墙上安装套件,将装置安装在墙上。

## 机架安装的安全考虑因素

- 环境温度升高:如果在闭合组合架上安装,机架环境的工作温度可能会高于室内环境温度。请
  特别注意切勿超出装置的额定最高环境温度。
- 空气流通减少:将设备安装到机架上时,必须严格保证设备安全操作所需的空气流通量。
- 机械负载:将设备安装到机架上时,当心由于机械负载不均而构成危险。
- 电路超载:应考虑设备与供电电路的连接,以及电路超载可能对过电流保护和供电线路造成的 影响。请遵守设备铭牌上的额定最大电流值。
- 可靠接地:应保持机架安装设备的可靠接地。请特别注意连接到分支电路的非直接式供电连接
  (例如使用插线板时)。

### 机架安装

### 要将装置安装在机架上:

- 1. 拆下 Avocent® Universal Management Gateway 装置每侧的四颗黑色螺钉。调整每个支架的位置, 以防其阻挡装置两侧的通风孔。使用装置随附的八颗铬螺钉,将安装支架紧固到装置上。
- 2. 使用适用于机架的螺钉,将两个滑轨支架安装到机架前面,不要将螺钉拧紧。

3. 从机架背面将装置滑入装有滑轨的同一 U 形位置。确保两条滑轨都牢固地插入装置的支架 中。拧紧装置支架和滑轨的机架螺钉。

### 图 2.1: 机架安装配置的支架连接



# 墙上和 0U 安装的安全考虑因素

允许使用可选的墙上安装套件(单独出售)进行墙上安装。如果在设备机架中进行墙上安装或 0U安装,必须使装置的正面面向机架的侧面,而不是朝向地面或天花板。

### 墙上安装

**注**: 墙上安装套件为可选件,不与装置一起提供,必须单独购买。有关如何购买墙上安装套件的详细信息,请联系 您的 Avocent 代表。

#### 要将装置安装在墙上:

- 使用支架上的插槽或随附的模板作为向导,在胶合板墙上标记出用于固定支架的孔。每个支 架应至少标记两个孔。使用 3/16 英寸钻头在标记的位置钻出导孔。使用螺纹直径为 1/4 英 寸、长度为1英寸的六角头木螺钉(不与墙上安装套件一起提供),将每个支架固定到胶合 板墙上,每个支架至少使用两颗螺钉。
- 拆下装置两侧中间的两颗大圆头螺钉。请务必仅拆下中间的两颗螺钉,以使装置的机盖保持 固定。将装置上的孔与安装支架上的孔对齐,使用随墙上安装套件一起提供的翼形螺钉将装 置固定到支架上,确保插槽朝上或朝下(如图所示)。

#### 图 2.2: 墙上安装配置的支架连接



## 缆线安装、维护和安全说明

#### 警告:为避免潜在的致命触电危险和可能对设备造成的损害,请遵守以下注意事项。

下面列出了在安装或维护缆线之前应阅读的重要安全考虑因素:

- 使用缆线扎带固定缆线时,用力要适中。不要扎得太紧。
- 若要弯曲缆线,弯度不能太大,曲率半径不得超过 25.4 mm。缆线弯度太大或扭结会永久性 损坏缆线的内部结构。
- 需要交叉连接缆线时,请使用规定的接线排、跳线架和组件。不要在任何位置编接或桥接缆线。
- 使 UTP 缆线尽量远离潜在的电磁干扰源,如电缆、变压器和照明装置。不要将缆线捆在导线 管上或将缆线放在电气装置上。
- 每安装一段线路,请务必用缆线测试仪进行检测。检测时不能只听声音。
- 一定要安装插座,以防灰尘和污染物落到触点上。插座的触点必须正面朝上置于齐平安装板上,或置于表面安装盒的左侧/右侧/下方。
- 一定要留出多余的缆线,整齐盘放在天花板中或最近的隐蔽位置。在工作插座侧至少要留出 1.5 m,在跳线架侧至少要留出 3 m。

- 开始前请确定是采用 568A 还是 568B 布线标准。采用相同的布线方案为所有插座和跳线架布 线。不要在同一系统中混合采用 568A 和 568B 两种布线标准。
- 本产品不能通过任何方式直接或间接连接到公用电信网 (PSTN)的接口。
- 一定要遵守所有当地和国家防火和建筑规范。一定要对穿过防火墙的所有缆线采取防火措施。必要时,请使用阻燃缆线。
- 不要拔掉电源接地插头。接地插头是一个重要的安全特性。
- 将电源线插入一个方便随时使用的接地插座。
- 若要断开产品的电源,请从电源插座或产品上拔掉电源线。交流接入口是使本产品断电的主 要断开点。对于拥有多个交流接入口的产品,必须断开所有交流电源线,才能彻底断电。
- 本产品的外壳内没有用户可自行维修的部件。不要打开或拆除产品机盖。

**注意:** 本装置配有一个内部电池,用于支持实时时钟。该电池不可以现场更换,并且用户不得尝试进行更换。如果实时时钟出现错误并且您怀疑是由电池引起的,请访问 http://www.avocent.com/support或联系离您最近的 Avocent技术支持。

• 本产品用于与经国家认可测试实验室 (NRTL) 批准或认证的其他产品配套使用。

# 连接硬件

## 装置接口

下图显示了装置前面的接口。

#### 图 2.3: 装置前面



#### 表 2.1:装置前面的接口

编号	说明
1	LED
2	控制台端口
3	USB连接
4	模拟视频端口

下图显示了装置后面的接口。

#### 图 2.4: 装置后面



#### 表 2.2:装置后面的接口

编 号	说明
1	电源。
2	电源指示 LED。
3	GB2 (eth1) 10/100M/1G以太网端口。可连接到第二条网络或用于故障转移。
4	自动检测端口(仅限 Avocent® Universal Management Gateway 2000 装置。在 4000 和 6000 装置上,所有端口都可进行自动检测)。
5	专用端口(仅限 Avocent® Universal Management Gateway 2000 装置) 。

# 连接目标

### 服务处理器

使用 UTP 缆线可将服务处理器连接到装置上的自动检测或专用端口。有关如何设置服务处理器 的更多信息,请参阅第 39页的"端口配置"。

### 串行

根据需要,使用 UTP 缆线和 DB-9 或 DB-25 控制台适配器,将串行目标连接到装置上的自动检测端口。

装置支持 Avocent 和 Cisco<sup>®</sup> 串行端口两种脚位排列配置。端口将自动检测脚位排列。

#### 要连接串行设备和 PDU:

确保用于连接设备的交叉缆线的脚位排列类型与在软件中为端口(Avocent或Cisco)配置的类型相同。

- 1. 确保要连接的设备处于关闭状态。
- 2. 使用 UTP 交叉缆线将设备连接到装置,必要时使用适配器。

**注**: 为符合 EMC 要求,请使用屏蔽线连接所有端口。

警告:打开装置前,切勿打开连接的设备的电源。

#### 要以菊花链形式将 PDU 连接到装置:

注:执行此过程的前提是您已将一台 PDU 连接到装置上的端口。

- 1. 将具有 RJ-45 接头的 UTP 缆线的一端与连接的 PDU 的输出端口相连。
- 2. 将缆线的另一端与链接的 PDU 的输入端口相连。重复这两个步骤,直到完成连接所需数量的 PDU。

注:为保证性能,每个串行端口连接的插座不得多于128个。

有关如何设置串行目标的更多信息,请参阅第 39页的"端口配置"。

#### KVM

如果您的装置支持 KVM 连接,请使用 UTP 缆线和 UMIQ 模块将 KVM 目标连接到装置上的自动 检测端口。



图 2.5: UMIQ 模块配置

UMIQ-v1 模块具有一个用于连接到装置的 RJ-45 端口。UMIQ-v2 模块具有两个 RJ-45 端口。您可以将任意一个连接到装置,并将另一个连接到服务器上的专用服务处理器端口。缆线长度最长可达 100 米。

有关 KVM 目标的更多信息,请参阅第 48 页的"KVM 管理"。

# 打开装置

装置配有双电源。

#### 要打开装置:

- 1. 将电源线插入装置和电源。
- 2. 打开连接的设备。

# 验证连接

## 前面板和后面板电源状态 LED

装置的前面板上有一个可亮起的双色 LED,用于指示一般状态:

- 装置打开并正常运行时, LED 将亮起绿色。
- 装置正在启动时, LED 将闪烁绿色。
- 发生电源故障、环境温度升高或风扇故障等故障状况时,LED 将亮起琥珀色。如果故障一直 存在,LED 就会一直亮起。
- 装置正在关闭时,LED将闪烁琥珀色。LED熄灭后,即可安全拔出电源线。

## 后面板以太网连接 LED

装置的后面板上有两个 LED, 其中绿色 LED 指示以太网连接状态:

- 如果绿色 LED 一直亮起,则表示以太网连接已建立。
- 如果绿色 LED 闪烁,则表示以太网活动。
- 如果琥珀色 LED 一直亮起,则表示目标会话处于活动状态。
- 如果 LED 都没有亮起,则表示无活动。

### 后面板自动检测/专用 IP 端口 LED

装置的后面板上有两个 LED, 绿色或琥珀色:

- 如果两个 LED 同时亮起,则表示自动检测已启用。
- 存在 KVM 或 SP 连接时,绿色 LED 将亮起。
- 存在串行连接时,琥珀色 LED 将亮起。

# 配置装置

您可以通过 CLI、控制台或以太网端口访问装置,并通过终端或运行终端仿真软件的 PC 访问所 有终端命令。

注: 要使用 DSView 软件进行配置,请参阅《DSView 4 管理软件安装人员/用户指南》。要使用装置的 web UI 进行配置,请参阅第 25 页的"管理"。要使用 Telnet 或 SSH 进行配置,请参阅装置《命令参考指南》。

#### 要将终端连接到装置:

1. 使用对绞线,将运行终端仿真软件的终端或 PC 连接到装置前面板上的控制台端口。已提供 RJ-45 转 DB9(母接头)交叉适配器。

终端设置为 9600 位每秒 (bps)、8 位、1 停止位、无奇偶校验和无流量控制。

2. 打开装置。装置完成初始化后,终端将显示登录横幅和登录提示。

# 配置示例

以下图形和表格显示了典型的装置配置。



图 2.6: 标准 Avocent® Universal Management Gateway 装置配置

表 2.3:标准 Avocent® Universal Management Gateway 装置配置	记明
---	----

编号	说明	编号	说明	
1	电源	11	DSView 服务器	

编号	说明	编号	说明
2	以太网连接	12	远程身份验证
3	用户	13	PC客户端
4	外部传感器连接	14	USB 媒 体
5	自动检测串行或服务处理器连接的端口	15	RJ-45串行设置端口
6	用于 KVM 连接的 UMIQ模块	16	DB9 com 端口
7	KVM交换机	17	用于本地配置的 PC
8	防火墙	18	USB连接(键盘、鼠标或媒体)
9	以太网连接	19	VGA控制台端口
10	局域网 (LAN)	20	用于本地配置和访问的 LCD 托盘

## 使用 Telnet 或 SSH 访问串行目标

如果以下条件均满足,授权用户可使用 Telnet 或 SSH 客户端直接连接到串行目标的控制台。 Telnet 或 SSH:

- 协议已对安全配置中的网络服务启用
- 协议已配置用于端口
- 客户端可用,并在建立连接的计算机上启用

### 要使用 Telnet 通过串行端口连接目标:

要完成此过程,您需要配置用以访问串行端口的用户名、目标名称(例如14-35-60-p-1)、设备 名称(例如ttyS1)、TCP端口别名(例如7001),以及装置的主机名或IP地址。

要使用 Telnet 客户端,请在客户端的对话框中输入信息。

-或-

要在 shell 中使用 Telnet, 请输入以下命令:

# telnet [主机名 | IP 地址]

login: [用户名]:[目标名称 | 设备名称]

一或一

#### # telnet [主机名 | IP 地址] TCP\_端口\_别名

login: [用户名]

### 要关闭 Telnet 会话:

输入为客户端定义的 Telnet 热键。默认为 Ctrl+q 退出。

### 要使用 SSH 通过串行端口连接目标:

要完成此过程,您需要配置用以访问串行端口的用户名、目标名称(例如14-35-60-p-1)、TCP 端口别名(例如7001),设备名称(例如ttyS1),以及装置的主机名或IP地址。

要使用 SSH 客户端,请在客户端的对话框中输入信息。

一或一

要在 shell 中使用 SSH, 请输入以下命令:

### ssh - I [用户名]:[目标名称][主机名 | IP 地址]

一或一

ssh - I [用户名]:[设备名称][主机名 | IP 地址]

一或一

### ssh -l [用户名:TCP 端口别名][主机名 | IP 地址]

### 要关闭 SSH 会话:

在一行的开头,输入为 SSH 客户端定义的热键,然后再加上一个句点。默认为~。



对于已连接的设备,Avocent® Universal Management Gateway 装置提供多种访问方式。请考虑以下安全参数和默认值,以及它们与您的组织安全策略的匹配程度。

Universal Management Gateway 装置提供以下默认设置:

- 启用 DHCP、SSH v2 和 HTTPS。
- 启用所有自动检测端口。
- 启用以太网和 CLI 设置端口。
- 下表是装置内的默认用户帐户。

#### 表 3.1: 默认用户帐户

用户名	角色	密码
admin	管理员	admin
operator	高级用户	operator
user	用户	user

• 仅允许管理员角色进行 shell 访问。

**注**: Avocent 强烈建议您在初始设置后更改默认密码,并创建个人用户帐户。有关更改密码的信息,请参阅第 33页的"*添加用户*"。

# 连接到网络

使用 UTP 缆线将主要网络端口连接到您的网络。要实现冗余,应连接两个网络端口并配置故障转移网络模式。有关更多信息,请参阅第 64 页的"定义的网络"。

# 分配 IP 地址

可通过 DHCP 获取 IP 地址,或分配静态 IP 地址。

# 本地或通过控制台端口连接

您可以通过网络使用支持的 web 浏览器、通过 VGA 控制台使用 LCD 托盘或 KVM 交换机,或通过 CLI 设置端口使用串行缆线和终端仿真软件来配置和管理装置。使用提供的 RJ-45 至 DB9F 适配器 可将终端或工作站连接到 CLI 设置端口。终端设置为:9600、8、N 和 1,无流量控制和 ANSI 仿真。

注:关于使用 CLI 分配 IP 地址的说明,请参阅《Universal Management Gateway 装置命令参考指南》。

装置上的 GB1 (eth0) 端口配置为 DHCP 客户端。如果您的网络设置为使用 DHCP, 首先您必须查 看网络 DHCP 服务器上的 DHCP 租约,找到分配到装置的 IP 地址。然后使用支持的 web 浏览器 导航至 https://<装置 IP>,以连接到装置。

**注**: 若要为访问装置的客户端 PC 提供全面的产品支持,需要使用 Adobe® Flash Player 和 Oracle® Java Runtime。请参阅发行说明,查看支持的 web 浏览器列表。

如果您的网络未设置为使用 DHCP, GB2 (eth1) 端口拥有默认 IP 地址 192.168.1.20。您可以为连接 到 eth1 的 PC 分配 IP 地址 192.168.1.10, 然后使用默认 IP 地址浏览至装置。

#### 要使用 VGA 控制台分配 IP 地址:

- 1. 使用 admin 作为默认用户名和密码登录装置。
- 单击"管理"选项卡下的"网络设置"。有关网络模式的更多信息,请参阅第 64 页的"定义的网络"。

**注**: 应在配置目标前执行对网络模式的更改。添加和配置目标后再更改网络模式可能会中断目标的通信,并需要重新添加和重新配置才能继续运行。

3. 单击表中所需接口的条目,将方法更改为"静态"。

4. 分配所需 IP 值并单击"应用"。

# 设置网络

装置使用 IP 地址将其自身识别为唯一的基于 IP 的目标设备。它支持动态主机配置协议 (DHCP) 和静态 IP 地址分配。

作为网络基础设施设备,装置的 IP 应为静态的,或使用 DHCP 保留以确保始终可通过一致的地 址访问装置。装置上的 GB1 (eth0) 是一个 DHCP 客户端,仅用于帮助进行初始网络访问,但在投 入生产环境前应设置为静态。

可通过 DHCP 获取 IP 地址,也可使用 VGA 控制台或 CLI 设置端口分配静态 IP。

注: 如果使用 DHCP,您必须首先找出分配给装置的 IP地址,方法是查看网络 DHCP服务器上的 DHCP 租约。在浏览器中输入 https://<装置 IP>,以连接装置。

#### 要分配 IP 地址:

- 1. 使用 admin 作为用户名和密码,通过装置的控制台端口登录装置。
- 2. 单击"管理"按钮。
- 3. 单击"网络设置"文件夹。
- 4. 单击表中的"GB1 (eth0)"条目,并将方法更改为"静态"。
- 5. 分配所需的 IP 值并单击"应用"。

## 防火墙

请参考下表, 配置通过防火墙对装置的访问。

|--|

端口	类型
20	FTP一固件更新

端口	类型
21	FTP一固件更新
22	加密的串行会话
80	HTTPS重定向
161	SNMP Set/Get
162	SNMP Trap
443	加密的 Web UI 访问
514	外部 Syslog
623	Serial over LAN 和 IPMI
843	Web UI 数据 一 闪存
2068	加密的 KVM 会话
3211	DSView 搜索 (UDP)
3502	DSView软件装置通信
3871	DSView 通信 (ADSAP2)
4440	Trellis™管理协议
7001-7040	串行
8011	Trellis <sup>™</sup> 平台
8012	Trellis <sup>™</sup> 平台
8080	Java查看器下载
8123	Web UI 数据 — XML
47777-48117	Trellis <sup>™</sup> 平台
50000-59999	SP访问



将 Avocent® Universal Management Gateway 装置连接到网络后,您即可通过装置的 web 用户界面 (UI) 访问装置。Web UI 通过图形用户界面提供对装置及其目标设备的直接访问。

**注**: 有关通过命令行界面或 DSView 软件访问装置的说明,请参阅《Avocent® Universal Management Gateway 装置命令参考指南》或《DSView 4 管理软件安装人员/用户指南》。

# Web UI 概述

### 要登录 web UI:

- 1. 在 Web 浏览器中打开地址 http://<装置.IP>。
- 2. 在登录屏幕中, 输入用户名和密码。
- 3. 登录后, 您将看到"目标"选项卡。

注: 使用 VGA 控制台时,您可以选择其他区域设置或键盘类型。

注: 若要为访问装置的客户端 PC 提供全面的产品支持,需要使用 Adobe® Flash Player 和 Oracle® Java Runtime。请参阅 发行说明,查看支持的 web 浏览器列表。

### 图 4.1: Web UI

arellis	A	ocent Univers	al Managemen	t Gateway			
目标 传感器 事件 管理							
显示 英型	■						
▼ 🗁 装置	名称	端口	类型	状态	拓扑图	IP 地址	电源操作 远程试
▶ 🗀 服务处理器	15-78-C6_12.0.1.20	0	服务处理器	己加电	0	12.0.1.20	送探电源 ▼ SP 余
	15-78-C6_12.0.1.200	0	服务处理器	己加电	0	12.0.1.200	送择电源 ▼ SP 会
▶ 🛄 #4179至約日 ▶ 🗀 PDU	15-78-C6_12.0.1.201	0	服务处理器	己加电	0	12.0.1.201	送择电源 ▼ SP 会
▶ 🗀 电源插座	15-78-C6_12.0.1.202	0	服务处理器	己加电	0	12.0.1.202	送择电源 ▼ SP 会
	15-78-C6_12.0.1.203	0	服务处理器	己加电	0	12.0.1.203	送择电源 ▼ SP 会
	15-78-C6_12.0.1.204	0	服务处理器	己加电	0	12.0.1.204	送择电源 ▼ SP 家
	15-78-C6_12.0.1.205	0	服务处理器	己加电	0	12.0.1.205	送择电源 ▼ SP 会
	15-78-C6_12.0.1.206	0	服务处理器	己加电	0	12.0.1.206	送择电源 ▼ SP 会
	15-78-C6_12.0.1.207	0	服务处理器	己加电	0	12.0.1.207	送择电源 ▼ SP 会
<u>.</u>	15-78-C6_12.0.1.208	0	服务处理器	己加电	0	12.0.1.208	送探电源 ▼ SP 会
	15-78-C6_12.0.1.209	0	服务处理器	已加电	0	12.0.1.209	送探电源▼ SP 会
	15-78-C6_12.0.1.21	0	服务处理器	己加电	0	12.0.1.21	送择电源▼ SP 会
l	15-78-C6_12.0.1.210	0	服务处理器	己加电	0	12.0.1.210	送择电源 ▼ SP 会
	15-78-C6_12.0.1.211	0	服务处理器	已加电	0	12.0.1.211	送择电源 ▼ SP 会
	15-78-C6_12.0.1.212	0	服务处理器	己加电	0	12.0.1.212	送择电源▼ SP 余
	15-78-C6_12.0.1.213	0	服务处理器	己加电	0	12.0.1.213	送择电源▼ SP 会
	15-78-C6_12.0.1.214	0	服务处理器	己加电	0	12.0.1.214	送择电源▼ SP 会
	45 70 00 400 4045		879.4+ Li va 60	77 Auch		40.04.045	SP≵

#### 表 4.1: Web UI

编号	说明
1	标题栏一使用标题栏可访问联机帮助、注销或更改当前用户的密码。
2	选项卡栏一使用选项卡栏可显示和管理目标、传感器、事件、管理及警告。
3	侧面导航栏一侧面导航栏用于显示指定设置或执行操作的窗口。根据显示的选项卡栏和窗口,侧面导航栏的内容会有所不同。
4	内容区一在内容区中可显示和更改由所选的选项卡栏、标题栏和侧面导航栏指定的信息。

# 使用侧面导航栏

侧面导航栏用于显示指定设置或执行操作的窗口。根据所选的选项卡和顶部导航栏以及所显示的窗口,侧面导航栏的内容会有所不同。

#### 图 4.2: 侧面导航栏示例

目标	传感器	事件	管理	]			
	显示 ★型						
▼ 🗁 装置							
▶ 🗀 服夠	予处理器						
🔻 🗁 UM	IQ						
9	UMIQ-17-3E-	2D					
🔻 🗁 串谷	<b>计控制</b> 台						
	15-78-c6-p-2						
🕨 🧀 PD	U						
▶ 🗀 电测	原插座						
1							

# 管理员角色

默认情况下,管理员可访问 web UI 的所有选项卡,包括 UI 的"目标"、"传感器"、"事件"和"管理"选项卡。

默认情况下,管理员的登录名和密码均为 admin。

# 操作员角色

操作员可访问 UI 的"目标"、"传感器"和"事件"选项卡。 默认情况下,操作员的登录名和密码均为 operator。

## 用户角色

用户可访问 UI 的"目标"和"传感器"选项卡。

默认情况下,用户的登录名和密码均为 user。

# 选项卡

选项卡是 web UI 的主要导航区域。在特定选项卡中只能进行特定操作。

# 目标

"目标"选项卡中显示的信息主要为只读信息,用于使用户便于访问目标会话或目标控制。有关更多信息,请参阅第 75页的"目标"。

### 传感器

"传感器"选项卡只在 Avocent® Universal Management Gateway 4000 或 6000 装置中显示。通过此选项卡,您可以查看有关温度、湿度、干触点、烟雾、动作、泄漏和其他支持的环境数据的只读信息。有关更多信息,请参阅第 83 页的"*传感器和事件*"。

### 事件

"事件"选项卡包含装置的事件和警告日志。除了能清除事件和警告条目之外,此选项卡上显示的数据都是只读数据。有关更多信息,请参阅第83页的"传感器和事件"。

### 管理

"管理"选项卡包含管理和操作装置及其目标所需的所有配置和控制设置。唯一不能通过此选项卡 访问的配置参数与 Trellis™ 实时基础设施优化平台的数据收集和监控功能有关。该行为可在 Trellis 平台中得到完全控制。有关更多信息,请参阅下面的章节。



以管理员身份登录时,您可以访问"管理"选项卡。在此选项卡中,您可以配置和管理装置及相关联的目标。

注: 要执行本部分的操作,请先单击"管理"选项卡。

图 5.1: "管理"选项卡概述						
📚 trellis 🔋 🔹 Avocent Universal M	anagement Gateway	帮助 注销 帐户				
目标 传感器 事件 管理		已登录,身份:: admin				
山装置设置	管理 > <u>装置设置</u>					
🗋 默认值	SSH 重新启动 关机					
▼ 🗁 网络设置						
🗋 主机	装置设置	应用				
□ 路由	型号 UMG 6000					
OSPF	序列号 0040148265					
BGP	固件版本 2.1.0.0 rdist					
▼ 100 用户						
□ 组	联系人					
🗋 身份验证	-2 称					
▼ 🗁 目标	-1417					
🗋 端口配置	еи					
SP 管理	14 m					
🗋 串行管理						
○ KVM 管理	机架名称					
	其例信自					
DSView						
自动	447 p.L t+ 7/4					
し個件	带助又件					
USB 设备	帮助文件 URL http://global.avocent.com	/us/olh/univ				
	申源状态					
▼ 2 传感器	- Canada Concert					
COM 数字输入	电源 1 关					
OneWire数字输入	电源 2 开					
OneWire环境传感器						
RS-485 环境传感器	电子邮件设置					
	昭々 聖					
□泄知日的地						
□会话	病口 25					
□支持	用户名					
	密码					
☐ 防火墙和 NAT						
		应用				

# 装置设置

单击侧面导航栏中的"装置设置",查看装置型号、序列号、固件版本和电源状态。您可以输入或 编辑联系人、位置和帮助文件设置,并配置电子邮件设置。 您可以使用屏幕顶端的按钮重新启动、关闭装置或启动与装置的 SSH 会话。 警告:关闭装置前,请务必通过"概述/工具"节点下的 web UI、CLI或 DSView 软件执行关机命令,然后再打开。这将确保访问闪存中的文件系统时不会发生重设,并有助于避免闪存崩溃。

### SSH

单击"SSH"可启动 PC 到装置的基于 SSH 的 CLI 控制台会话。在此,您可以访问管理 CLI、目标会 话和电源操作,以及访问装置 Linux Shell。

### 帮助文件

您可以通过单击屏幕右上方的"帮助"按钮访问装置的联机帮助。

如果您的客户端 PC 不能访问互联网,您可以下载装置用户指南的 PDF,并将其托管在内部 Web 服务器上。要下载用户指南,请访问以下地

址: http://pcs.mktg.avocent.com/@@content/manual/5901071501b.pdf。

下载用户指南并将其托管到服务器后,请在帮助文件 URL 字段中输入其路径。

### 电子邮件设置

装置可为在装置或与其相关联的目标设备上发生的事件生成电子邮件警告。对 SMTP/电子邮件服 务器进行配置后,警告可发送至最多四个电子邮件地址。

有关配置警告及其电子邮件收件人的信息,请参阅"监控"和"通知目的地"部分。

### 网络设置

单击"网络设置",配置主机名、DNS、域名、IPv4 默认网关和 IPv6 默认网关。

### 网络模式

装置提供无代理远程访问和控制。在连接的服务器或客户端上不需要安装特殊的软件或驱动程序。

装置拥有三个物理网络接口(eth0、eth1、priv0)。每个接口都有单独的 MAC 地址,并且可以配置为"正常"、"桥接"或"故障转移"模式。用户界面仅显示公共 GB1 (eth0)和 GB2 (eth1)。可对 40 个专用目标端口进行虚拟配置,使其通过内部 priv0 接口连接。

要配置单独的端口,请参阅第 39页的"端口配置"

```
注: 装置的默认 IP 地址为: GB1 (eth0) = DHCP, GB2 (eth1) = 192.168.1.20
```

#### 正常

在"正常"模式中,公共接口和公共目标端口由防火墙隔开。GB1和 GB2 相互独立运行,并且可 以使用单独的 IP 地址。只能为装置定义一个网关,但在启用装置与任一接口的各种子网进行通 信时,静态路由非常有用。

例如: 接口为 GB1 的装置连接到网关为 192.168.200.1 的 192.168.200.x/24 网络。GB2 连接到网关为 10.1.0.1 的 10.1.0.x/24 网络。如果装置的默认网关设置为 GB1 (eth0),那么装置将不能通过分配给 GB2 的网关与其他 10.x.x.x 网络进行通信。可以将静态路由添加到装置中,以表示 10.1.0.1 应该用于与所有 10.x.x.x 子网通信。

### 故障转移

在"故障转移"模式中,GB1和GB2接口均已激活,并且都拥有唯一的MAC地址,但是它们共享一个通用bond0虚拟接口。共享的bond0接口只存在一个MAC,并且只能分配到一个IP。当需要从装置发送数据时,只有GB1会使用bond0MAC/IP进行发送。当流量发送到bond0MAC/IP时,由于只有GB1使用bond0MAC对ARP请求做出响应,因此只有GB1会接收该流量。如果GB1断开连接,那么GB2会接管所有数据交换的bond0MAC/IP控制。

#### 桥接

在"桥接"模式中,端口 GB1、GB2 和 priv0(包括 priv、spm 和 kvm)都桥接在一起。所有接口同时共享一个虚拟接口 br0,因此只有一个 MAC/IP 用于来自装置操作系统的流量。当装置被置于"桥接"模式时,装置的所有 DHCP 服务都将自动停止,以防与网络上的 DHCP 服务产生冲突。在"桥接"模式下,装置无法搜索或支持 UMIQ 模块。

#### 要配置网络设备:

- 1. 单击侧面导航栏中的"网络设置"。
- 2. 输入主机名。
- 3. 使用下拉列表选择"正常"、"故障转移"或"桥接"模式。
- 4. 在相应字段中输入主次 DNS 地址。
- 5. 输入域名。
- 6. 使用下拉列表选择 IPv4 和 IPv6 默认网关。
- 7. 单击接口名称以进行修改。
  - a. 在 IPv4 标题下的相应字段中输入 MTU、地址、子网掩码、广播和网关。使用下拉列表选择 DHCP 或静态方法。
  - b. 在 IPv6 标题下的相应字段中输入地址、子网掩码和网关。使用下拉列表选择 DHCP 或静态方法。
- 8. 单击"应用"。

# 桥接组配置

管理员可选择要桥接到同一个逻辑桥接组中的网络接口。此功能简化了桥接接口的创建、删除 和维护。您可以通过物理和虚拟接口进行桥接,桥接支持用户创建的接口以及预定义接口。

您可为装置上定义的每个虚拟和物理接口创建桥接组。创建桥接组时,会为其分配一个第三层 IPv4/IPv6地址。将接口添加到桥接组时,会显示一条提示消息,说明分配到接口的所有 IP地址 都将丢失,并且将通过桥接组的 IP地址与可通过桥接组内的端口访问的设备进行通信。

本装置不用于通用以太网桥接。端口桥接功能旨在使通过物理连接与专用接口相连的设备能通 过公用网络基础设施进行访问。如果装置连接到网络交换机时,桥接协议数据单元 (BPDU) 防护 处于活动状态,那么配置桥接接口时必须禁用生成树协议 (STP)。禁用 STP 将使装置存储以太网 帧,并在桥接中相关联的端口之间进行转发,而不进行任何环路检测和预防。

#### 要创建或编辑桥接组配置:

- 1. 单击侧面导航栏中的"网络设置"。
- 2. 在"桥接组配置"标题下,单击"添加"。

一或一
单击现有桥接组以进行编辑。

- 3. 输入桥接组的名称。
- 4. 勾选复选框以启用 STP( 生成树协议) 。
- 5. 使用下拉菜单启用"桥接状态"。
- 6. 从可用桥接接口的列表中,选择要添加到组中的接口并单击"向右箭头"。
- 7. 在 IPv4 标题下输入 MTU(最大传输单元),并使用下拉菜单选择 DHCP 或"静态路由"。如果 使用"静态路由",输入"地址"、"广播"和"网关"。

一或一

在 IPv6 标题下,输入 DHCP 或"静态路由"。如果使用"静态路由",输入"地址"和"网关"。

### 要删除桥接组配置:

- 1. 单击侧面导航栏中的"网络设置"。
- 2. 在"桥接组配置"标题下,勾选要删除的桥接组名称旁的复选框,并单击"删除"。

# 主机

管理员可以为本地网络配置主机名、IP地址和主机别名表。

#### 要添加主机:

- 1. 在侧面导航栏中选择"网络"一"主机"。
- 2. 单击"添加"以添加新的主机。
- 3. 输入要添加的 IP 地址、主机名和主机别名, 然后单击"应用"。

### 要删除主机:

- 1. 在侧面导航栏中选择"网络"-"主机"。
- 2. 单击要删除的主机名, 然后单击"删除"。

# 路由

适当的路由可确保流量从客户端到装置,再从装置返回客户端。装置中的路由表显示连接的网络,以及装置已获知或动态了解的网络。如果将流量指定给远程网络,但装置无法找到与目的 地网络相匹配的特定路由,则它将把流量发回默认网关。这就是某些流量无法按预期发送或接 收的原因。

注: 装置专门设计用于管理设备管理控制台并提供对它的访问,而不用作通用路由器、交换机或数据包过滤器。

至特定网络目的地的静态路由可提高装置做出的关于发送流量时使用哪个接口的决定的准确 性。

**注**: 请务必确保不要将重复的网络地址分配到装置中的多个接口。如果装置中默认的专用网络地址与您的基础设施中已存在的网络产生冲突,还必须对其进行更改。

#### 要添加静态路由:

- 在侧面导航栏中选择"网络"一"静态路由"。将列出所有现有的静态路由,还会显示其目的地 IP/掩码、网关、接口和跃点数值。
- 2. 单击"添加"。
- 3. 在相应的字段中输入目的地 IP、网关和网络掩码值,然后使用下拉菜单选择设备接口。
- 4. 单击"应用"。

#### 要删除静态路由:

- 1. 在侧面导航栏中选择"网络"一"静态路由"。
- 2. 单击要删除的静态路由的名称,然后单击"删除"。

# OSPF 和 BGP

装置支持开放最短路径优先 (OSPF) 和边界网关协议 (BGP) 路由标准及其相关配置。管理员可添加、编辑和删除 OSPF 和 BGP 网络。

### **OSPF**

要使用 OSPF, 管理员必须先配置装置 ID、接口和网络设置。默认情况下, OSPF 与装置的所有接口通信。管理员不能添加接口,但能更改现有接口的状态。

管理员能为装置添加网络,以便与网络中的其他 OSPF 节点相互收发信息。添加网络时,该网络对于装置必须是唯一的。网络值为 CIDR 格式的 IP 地址/子网掩码,例如: 10.12.1.0/24。

### 要配置 OSPF:

- 1. 单击侧面导航栏中的"网络设置"一"OSPF"。
- 2. 勾选复选框以启用 OSPF。

注: 启用或禁用 OSPF 时,将向警告管理器发送警告。

- 3. 输入装置 ID, 然后单击"应用"。装置 ID 应为 IP 地址, 但可以是任意的 32 位数字。装置 ID 在整个 OSPF 域中必须是唯一的。
- 4. 使用下拉菜单将"接口"设置为"主动"或"被动"。OSPF将不会与设置为"被动"的任何接口进行 通信。
- 5. 要添加网络, 输入网络的地址及其区域, 然后单击"添加"。
- 医编辑现有网络,勾选"修改 OSPF 网络"标题下该网络旁的复选框。完成后,单击"应用"。
- 7. 要删除网络,勾选网络旁的复选框,然后单击"删除"。

### BGP

BGP 是用于实现互联网连接冗余的关键协议之一。BGP 装置使用端口 179 上的 TCP 协议互相通信。BGP 只发送包含自上次更新以来已更改的路由条目的增量更新。

BGP 对等体通过装置间的手动配置建立,以在端口 179 上创建 TCP 会话。BGP speaker(发言人) 每 30 秒发送一次保活消息以保持连接。每个 BGP 装置会与与其连接的其他 BGP 装置保持单独的 TCP 会话。

自治系统 (AS)指由一个或多个网络运营商通过单一且定义明确的路由策略运行的一组 IT 网络。 当交换路由信息时,每个自治系统通过唯一的编号被识别。该 16 位编号的范围从 0 到 65535, 其中 64512 到 65535 保留给专用网络使用。自治系统使用 BGP 等外部路由协议在系统间交换路 由信息,并通常使用某种内部网关协议在其内部网络中交换路由信息。网络值为 CIDR 格式的 IP 地址/子网掩码,例如: 10.12.1.0/24。配置的网络将向其所有邻居进行通告。

## 要配置 BGP:

- 1. 单击侧面导航栏中的"网络设置"-"BGP"。
- 2. 勾选复选框以启用 BGP。

注: 启用或禁用 BGP时,将向警告管理器发送警告。

- 输入自治系统编号和装置 ID,然后单击"应用"。装置 ID 应为 IP 地址,但可以是任意的 32 位数字。
- 4. 要添加网络, 输入网络的地址, 然后单击"添加"。
- 5. 要编辑现有网络,勾选"修改 BGP 网络"标题下该网络旁的复选框。完成后,单击"应用"。
- 6. 要删除网络,勾选网络旁的复选框,然后单击"删除"。
- 要添加邻居(对等体),输入其 IP地址和远程自治系统编号,然后单击"添加"。

**注:** 默认的自治系统编号为 64512, 是一个专用的自治系统编号。使用 BGP 时您需要修改此编号,以确保它在网络中的唯一性。

- 要删除现有邻居,勾选"修改 BGP 邻居"标题下该邻居旁的复选框。完成后,单击"应用"。
- 9. 要删除邻居,勾选邻居旁的复选框,并单击"删除"。

# 默认值

在"默认值"选项卡中,您可以将装置恢复为出厂默认设置。

您还可以配置日期和时间、NTP 服务器设置,以及设置时区和夏令时。如果您无法访问 NTP 服务器,可以手动设置日期和时间。

注: 您必须先设置装置的时间,然后才能将其注册到 Trellis™实时基础设施优化平台。

# 用户

根据管理员能分配给自定义用户组的授权,可选择性地限制对端口的访问。连接到设备时,也可以授权组管理电源。装置具有三个默认用户(管理员、操作员和用户)和三个预定义的用户 角色(装置管理员、高级用户和用户)。

# 用户角色

用户角色定义有关装置设置和管理的视图,以及用户可在 web UI 和 CLI 内进行的操作。

### 表 5.1: 用户角色

用户角 色	说明
用户	仅目标访问。
高级用 户	查看装置信息、重新启动装置、断开用户会话连接、目标访问、目标电源操作和查看数据日 志。
装置管 理员	所有用户和管理员功能,包括升级装置、配置装置设置和目标访问。装置管理员角色是唯一可以进行 shell访问的角色。

# 用户

必须为装置或身份验证服务器上的每个用户定义用户帐户。只有管理员能添加和配置其他用户 帐户。每个本地用户帐户都被分配到一个或多个用户组。

**注意:** 运行装置前,请更改默认密码。

# 密码策略

装置的默认用户名和密码是 admin 和 admin。管理员可为所有用户帐户配置全局密码规则。密码的最大长度为 64 个字符。当密码策略从较低级别增加到较高级别时,所有本地用户帐户都将被标记,以便在下次登录时更改密码。

在所有情况下都会对密码进行检查,以确定密码不含回文或重复字符串。

### 表 5.2: 密码策略设置

设 置	说明
无	密码可短至一个字符,也可包含任意字符。密码可立即重复使用,其到期时间默认设置为永不。
弱	密码必须至少包含四个字符,且其中至少有一个数字。用户更改密码时,新密码必须不同于旧密码。 密码默认设置为一年后到期。
中	密码必须至少包含八个字母,包括一个数字和一个大写字母。用户更改密码时,新密码必须不同于旧密码。密码默认设置为90天后到期。
强	密码必须至少包含16个字符,包括一个特殊字符、一个数字和一个大写字母。用户更改密码时,新密码必须不同于旧密码。密码默认设置为30天后到期。

# 抢占级别

用户的抢占级别决定了他们是否能够中断或断开另一用户与目标设备的 KVM 会话。管理员和用户管理员可以为用户帐户或用户定义的用户组指定抢占级别。

默认情况下,用户的有效抢占级别是用户所属的所有用户组中的最高分配值。抢占级别分为 1-6 级,6为最高级。例如,抢占级别为6的用户或用户组可以抢占其他级别为6及以下级别的用户 或用户组。

表 5.3: 用户和用户组抢占			
抢占级别	说明		
6	管理员帐户的默认级别。仅适用于管理员。		
5	工厂操作员帐户的默认级别。仅适用于操作员和管理员。		
4	KVM交换机或串行控制台装置的新本地用户的默认级别。		
3	Avocent® Universal Management Gateway 装置的默认级别。		
2	用户管理员用户组的默认级别。		
1	新用户的默认级别。出厂用户帐户的默认级别。		

抢占级别可通过以下方式使用:

- 用户抢占级别一这是管理员分配给用户的抢占级别。如果该值大于用户所属的用户组的最高抢占级别,则该值将被用作有效的用户抢占级别。
- 组抢占级别一这是分配给用户所属的用户组的抢占级别。如果用户被分配到具有多个不同 抢占级别的用户组,则具有最高抢占级别用户组的抢占级别将会成为用户组的抢占级别。例 如,如果用户属于装置管理员(级别6)和用户(级别1)用户组,则该值将会定义为6。如 果该值大于用户的最高抢占级别,则该值将被用作有效的用户抢占级别。

装置管理员或高级用户也可以指定本地用户界面抢占级别,该级别适用于通过本地界面访问目标设备的用户。

# 添加用户

#### 要添加或修改用户:

- 1. 单击侧面导航栏中的"用户"。
- 单击"添加"创建新用户。将显示"创建用户"屏幕。输入新的用户名和密码,并使用下拉菜单 定义用户角色(用户、高级用户或管理员)。

一或一

单击用户的名称修改该用户。将显示"修改用户"屏幕。输入用户的新密码,并使用下拉 菜单更改用户角色。

- 3. 定义抢占级别。
- 4. 勾选此复选框可在下一次登录时更改密码。
- 5. 勾选此复选框可启用会话超时,并在字段中输入超时的分钟数。
- 6. 勾选此复选框可使密码过期,然后输入过期前的天数或过期日期。
- 7. 勾选此复选框可提醒用户密码将过期,然后在字段中输入提前提醒的天数。
- 勾选此复选框可在帐户不活动时使密码过期,并输入密码过期前帐户处于不活动状态的天数。
- 9. 单击"应用"。

# 身份验证

您可以通过 LDAP 或 DSView 服务器执行本地身份验证。装置还支持远程组授权,以便使用 LDAP 身份验证方法。

为装置配置的任意身份验证方法均用于验证尝试通过 Telnet、SSH 或 Web UI 登录的所有用户。

### 要配置身份验证设置:

- 1. 单击侧面导航栏中的"用户"一"身份验证"。
- 2. 使用"设置"选项卡中的下拉菜单选择密码强度,然后使用箭头按钮选择身份验证顺序。

注: 密码强度为全局设置。

3. 单击"应用"。

# 身份验证服务器

使用身份验证服务器时,您必须先配置其 IP 地址,在多数情况下还要配置其他参数才能使用。 需要对以下身份验证服务器进行配置: LDAP 和 DSView 软件服务器。

#### 要配置 LDAP 身份验证服务器:

- 1. 选择"用户"一"身份验证"一"LDAP"。
- 2. 输入身份验证服务器的 IP 地址。
- 3. 输入基础可分辨名称。
- 4. 在 SSL 模式下拉菜单中,选择"关"、"开"或"Start\_TLS"。
- 5. 输入绑定可分辨名称和密码。
- 6. 输入 PAM 属性。
- 7. 单击"应用"。

### 要配置 DSView 软件身份验证服务器:

- 1. 选择"用户"一"身份验证"一"DSView"。
- 2. 输入进行身份验证的 DSView 服务器的 IP 地址。

注: 这会将所有身份验证请求都转发到 DSView 服务器。

3. 单击"应用"。

# 用户目标访问

创建或修改用户后,单击用户名并选择"目标访问"选项卡可管理该用户的目标。托管目标将显示 在左侧的列中,可用目标将显示在右侧的列中。如果应用了过滤器,则只会显示与过滤器名称 相匹配的目标。如果定义了组,您可以选择按组显示目标。

### 要添加托管目标:

1. 在"可用"列中,浏览至要托管的目标,并单击向左箭头将该目标添加到托管目标。

2. 单击"应用"。

### 要移除托管目标:

1. 在"托管目标"列中,浏览至要移除的目标,并单击向右箭头将该目标从托管目标中移除。

2. 单击"应用"。

# 用户目标权限

创建或修改用户并分配该用户的目标访问权限后,选择用户名并单击"目标权限"选项卡可管理目标权限。

### 要管理目标权限:

1. 在"托管目标"下,单击要管理权限的目标。

2. 勾选相应的复选框,允许或拒绝一般访问权限。

- 对于串行目标,使用下拉菜单选择会话访问,并勾选复选框,终止多个会话或启用多个会话 通知。
- 4. 单击"应用"。

# 组

用户组默认拥有访问和授权权限,或由管理员进行分配。管理员可以修改属于"高级用户"或"用 户"组的用户的许可或访问权限,或创建拥有自定义权限和访问权限的其他组。管理员可以随时 添加、删除或修改任意组的用户的许可和访问权限。

例如,如果管理员将装置配置为限制用户访问某个目标,那么就可以将用户分配到获得特定目标访问授权的组。管理员还可以授权组进行电源管理和数据缓冲区管理。

本文档和软件适用于帐户在远程身份验证服务器上配置为远程用户的用户。远程用户不需要本地帐户。

LDAP 身份验证服务允许组配置。如果远程用户配置为远程组成员,则身份验证服务器会在对用户进行身份验证时将组名称提供给装置。拥有相同名称的本地组也必须在装置上进行配置。如果身份验证服务器对远程用户进行身份验证但没有返回组,则默认情况下会将该远程用户分配到用户组。

## 管理用户组

管理员可创建包含任何用户的自定义用户组。自定义用户组的权限和访问将由顶级用户组权限 决定。

#### 要添加或修改用户组:

- 1. 单击侧面导航栏中的"用户"一"组"。
- 单击"添加"创建新用户组。将显示"创建用户组"屏幕。输入新的用户组名,并使用下拉菜单 定义用户组角色(用户、高级用户或管理员)。

一或一

单击要修改的组名称。将显示"修改组"屏幕。使用下拉菜单更改用户组角色。

- 3. 定义抢占级别。
- 4. 勾选此复选框可启用会话超时,并在字段中输入超时的分钟数。
- 5. 要将用户添加到组,通过选择用户名并单击"添加"按钮,将用户从左侧的"可用用户"框移至 右侧的框中。您可以从左侧的框中选择任意用户,并单击"移除"按钮,将其从组中移除。
- 6. 单击"添加组"。

## 装置管理员组

装置管理员组的成员拥有无法更改的完全管理权限,以及与默认管理员用户相同的访问和配置 授权权限。管理员可以配置端口、添加用户以及管理连接到装置的电源设备。

注: 允许对装置管理员组进行的唯一配置是添加或删除成员。

### 要查看管理员的装置访问权限:

1. 单击侧面导航栏中的"用户"一"组"。将显示"组"屏幕,其中将列出三个默认用户组以及所有 已创建的组。 单击"组名"标题下的"装置管理员"。内容区将显示"成员"屏幕,列出属于管理员组的所有成员(默认成员为管理员)。

## 电源用户组

电源用户组的成员只能访问管理装置的任务。电源用户不能访问端口或电源管理选项,并共享 与管理员相同的所有装置访问权限,除了配置用户帐户和 shell 访问,这两项对于该组是永久禁 用的。

# 用户组

用户组的成员可以访问目标设备(被管理员限制的成员除外),但没有装置的访问权限。管理员可添加装置访问权限和许可,并将用户添加到自定义用户组,以根据需要添加许可和访问权限。默认情况下,"目标访问"和"目标权限"屏幕上的所有选项都被禁用。

注: 您可以根据需要重命名用户组。组的角色(而非名称)决定了访问和权限级别。

注: 目标访问最为自由,目标权限则最具限制性。

### 组目标访问

创建或修改组后,单击新组名称,然后选择"目标访问"选项卡可管理该组的目标。托管目标将显示在左侧的列中,可用目标将显示在右侧的列中。如果应用了过滤器,则只会显示与过滤器名称相匹配的目标。如果定义了组,您可以选择按组显示目标。

目标访问最为自由。只要用户或用户所在的组拥有访问权限,用户就能访问目标。下表根据用户或组的访问权限显示了目标访问权限。

#### 表 5.4: 组目标访问

用户是否拥有访问权限	组是否拥有访问权限	是否可以访问目标
是	是	是
是	否	是
否	是	是
否	否	否

### 要添加托管目标:

1. 在"可用"列中,浏览至要托管的目标,并单击向左箭头将该目标添加到托管目标。

2. 单击"应用"。

### 要移除托管目标:

1. 在"托管目标"列中,浏览至要移除的目标,并单击向右箭头将该目标从托管目标中移除。

2. 单击"应用"。

### 组目标权限

创建或修改组后,单击新组名称,然后选择"目标权限"选项卡即可管理目标权限。

目标权限最具限制性。只有用户和用户所在的组都拥有目标权限,用户才有目标权限。下表根据用户或组的权限显示了目标权限。

表 5.5: 目标权限

用户是否拥有权限	组是否拥有权限	是否拥有目标权限
是	是	是
是	否	否
否	是	否
否	否	否

#### 要管理目标权限:

1. 在"托管目标"下,单击要管理权限的目标。

- 2. 勾选相应的复选框,允许或拒绝一般访问权限。
- 对于串行目标,使用下拉菜单选择会话访问,并勾选复选框,终止多个会话或启用多个会话 通知。
- 4. 单击"应用"。

# 管理目标设置

如果您有"管理目标设置"的权限,就可以进行以下设置:

- "目标"选项卡 PDU <PDU> 功耗
- "目标"选项卡 PDU <PDU> 能耗
- "目标"选项卡 PDU <PDU> 环境
- "目标"选项卡 PDU <PDU> 设置
- "目标"选项卡 PDU <PDU> 属性
- "目标"选项卡 PDU <PDU> 插座 锁定
- "目标"选项卡 PDU <PDU> 插座 解锁
- "目标"选项卡 PDU <PDU> 插座 保存状态
- "目标"选项卡 PDU <PDU> 电流
- "目标"选项卡 PDU <PDU> 电压
- "目标"选项卡 电源插座 属性 设置
- "目标"选项卡 电源插座 属性 锁定
- "目标"选项卡 电源插座 属性 解锁
- "目标"选项卡 服务处理器 <SP> 系统 电源
- "目标"选项卡 服务处理器 <SP> 系统 外壳
- "目标"选项卡 服务处理器 <SP> 系统 时间
- "目标"选项卡 服务处理器 <SP> 日志 清除日志
- "目标"选项卡 服务处理器 <SP> 警告

## 查看日志

如果您有"查看日志"的权限,就可以进行以下设置:

• "目标"选项卡 - 服务处理器 - <SP> - 日志 - 下载日志

- "目标"选项卡 串行控制台 日志
- "目标"选项卡 服务处理器 <SP> 会话 SoL 会话历史
- "目标"选项卡 服务处理器 <SP> 会话 SEL

### 物理插座控制

如果您有"物理插座控制"的权限,就可以进行以下设置:

- "目标"选项卡 电源插座 <电源插座> 属性 开
- "目标"选项卡 电源插座 <电源插座> 属性 关
- "目标"选项卡 电源插座 <电源插座> 属性 重启
- "目标"选项卡 PDU <PDU> 插座 开
- "目标"选项卡 PDU <PDU> 插座 关
- "目标"选项卡 PDU <PDU> 插座 重启

### 物理 KVM

如果您有"物理 KVM"的权限, 就可以进行以下设置:

- "目标"选项卡 装置 远程访问
- "目标"选项卡 UMIQ <KVM 交换机> 连接

## 虚拟 KVM

如果您有虚拟 KVM 的权限,则可以进行以下配置:

• "目标"选项卡 - 服务处理器 - <SP> - 会话 - 虚拟 KVM/媒体

### 虚拟媒体

如果您有虚拟媒体的权限,则可以进行以下配置:

• "目标"选项卡 - UMIQ - <KVM 交换机>

#### 物理串行

如果您有物理串行的权限,则可以进行以下配置:

- "目标"选项卡 装置 远程访问
- "目标"选项卡 串行控制台 <串行设备> 连接

## 虚拟插座控制

如果您有虚拟插座控制的权限,则可以进行以下配置:

• "目标"选项卡 - 服务处理器 - <SP> - 系统 - 电源

### 查看环境数据

如果您有查看环境数据的权限,则可以进行以下配置:

- "目标"选项卡 电源插座 概述
- "目标"选项卡 服务处理器 <SP> 电源
- "目标"选项卡 服务处理器 <SP> 传感器

## 访问服务处理器

如果您有访问服务处理器的权限,则可以进行以下配置:

- "目标"选项卡 装置 远程访问
- "目标"选项卡 服务处理器 <SP> 会话 SoL 会话
- "目标"选项卡 服务处理器 <SP> 会话 Telnet
- "目标"选项卡 服务处理器 <SP> 会话 SSH
- "目标"选项卡 服务处理器 <SP> 会话 SSH 自动登录
- "目标"选项卡 服务处理器 <SP> 会话 浏览器会话
- "目标"选项卡 服务处理器 <SP> 会话 浏览器会话 自动登录

# 目标

单击侧面导航栏中的"目标",可查看连接的目标及其许可信息的摘要。通过此屏幕,您可以按类型查看目标列表,并了解托管、未托管、拥有活动会话、空闲和没有响应的目标数量。

# 许可

"许可"标题下显示的是全部 SP 许可和剩余许可数量的摘要。可用许可的数量视型号而异。如果 没有足够的许可来搜索或添加目标,您将收到低许可警示。超过可用许可的目标将被忽略。

# 端口配置

装置包含三个预设的虚拟接口,分别名为 priv、kvm 和 spm。它们具有唯一名称和 IP 地址,但全 部共享一个通用 MAC 地址。

这些虚拟接口可用于按类型分隔 IP 设备。默认情况下,仅启用 priv 虚拟端口,并所有带编号的端口都分配到此接口。有一个与分配到 priv 的 IP 相关联的活动 DHCP 范围。您可以将目标端口分配到虚拟接口,以重新分配 VLAN。现在,与不同虚拟接口相关联的两台设备将在第2层由装置内的 MAC 地址分隔开,以增强安全性。您可以配置专用接口,以便通过分隔 SPM 和 KVM 服务器来分割管理流量。

单击侧面导航栏中的"目标"-"端口配置",可查看装置上的每个端口的状态和配置。

### 要配置端口分配:

- 1. 单击"目标"一"端口配置"。
- 2. 选择端口并单击"端口配置"。
- 3. 勾选"启用"复选框。
- 4. 选择"串行"或"网络"。
- 5. 使用下拉菜单选择自动检测。
- 6. 使用下拉菜单选择端口类别。
- 7. 对于"串行",选择"串行控制台"或"串行 PDU"作为配置。
- 8. 单击"应用"。

### 要配置串行设置:

1. 对于连接到端口的串行设备,单击"目标"一"端口配置"一"串行设置"。

2. 选择端口并单击"串行端口设置"。

使用下拉菜单选择状况、速度、奇偶校验、数据大小、停止位、流量和串行脚位排列类型。

注: 默认设置为: 速度=9600, 奇偶校验=无, 数据=8, 停止位=1, 流量控制=无。

4. 单击"应用"。

### 要配置网络设置:

- 1. 单击"目标"一"端口配置"一"网络设置"。
- 2. 使用下拉菜单启用或禁用网络接口。
- 3. 在相应字段中输入 IP 地址、广播地址和 MTU。
- 4. 单击"应用"。

**注:** 如果 IP 地址为空, 用户无法启用接口。

注: 如果需要 DHCP, 接口的 IP 地址应与"DHCP 设置"页面相对应。

### 要创建自定义接口:

- 1. 单击"目标"一"端口配置"一"网络设置"。
- 2. 在"自定义接口"标题下,输入专用接口的名称。
- 3. 使用下拉菜单启用或禁用接口。
- 4. 输入 CIDR 格式的 IP 地址。
- 5. 输入广播地址。
- 6. 输入 MTU。
- 7. 单击"应用"。

注:新创建的接口在 DHCP 服务重启前将不会分配 DHCP 地址。

### 要编辑或删除虚拟接口:

- 1. 单击"目标"一"端口配置"一"网络设置"。
- 2. 勾选要编辑的专用接口旁的复选框。
- 3. 进行更改。

一或一

单击"删除",以删除该接口。

4. 单击"应用"。

## DHCP

创建接口后,转到"DHCP设置"选项卡可配置 DHCP路由。配置完成后,网络将开始分发 IP地址。

## 要配置 DHCP 设置:

1. 单击"目标"一"端口配置"一"DHCP设置"。

2. 勾选复选框以启用 DHCP 服务器。

3. 使用下拉菜单选择租用天数。

4. 在"DHCP全局设置"标题下,单击"添加"以添加新范围。

a. 在"修改范围"屏幕上,输入子网的 IP 地址、开始和结束范围以及子网掩码。

b. 单击"应用"。

5. 在"按 MAC 地址分配"标题下,单击"添加"以添加新的静态租用。

a. 在"修改静态租用"屏幕上, 输入主机名、固定地址和 MAC 地址。

b. 单击"应用"。

通过租用绑定,您可以了解哪些 IP 地址被分配到了 MAC 地址。它会显示范围、开始和结束时间、MAC 地址及主机名。租用时间按天计算。

**注:** "专用接口"列中列出的 IP 地址必须与定义的专用接口配置相匹配,以符合 DHCP 范围。与专用接口相比,可定义的范围数量更多,但只有一个范围能在专用接口上有效。

# SP管理

服务处理器 (SP) 可连接到装置背面任意带编号的目标端口。

没有专用接口的服务处理器将共用被称为边带的 NIC1。边带 SP 只能由装置通过网络进行逻辑通信。需要为 SP 分配装置能与之通信的 IP。

许多 SP 都能配置为使用专用接口或共用(边带) NIC1。装置可通过 IP 以两种方法中的任意一种 与 SP 通信。

当 SP 通过物理连接与装置相连时, SP 的 IP 无法访问网络。OEM 工具将无法与 SP 通信,除非装置被置于桥接模式。SP 管理器会阻止带编号的目标端口之间进行通信,但装置不会。

"SP管理"屏幕显示连接到装置的所有服务处理器 (SP)。您可以在此屏幕中添加、删除和管理 SP 设置。如果装置可以对 SP 进行 IP 访问,并具有支持 SP 类型的相应配置,那么可手动将 SP 添加 到装置。"添加 SP 向导"中必须填写用户名/密码。通用凭据可以预填充到"默认用户"选项卡。您 选择的配置应尽可能与 SP 相匹配。

使用 IPMI的 SP 将使用 KG(十六进制格式)和"加密"设置执行 IPMI 2.0 对称加密密钥,以对基于 UDP 的 IPMI 流量加密。为确保装置能使用 SP 的所有功能,务必在 SP 的配置中启用 IPMI-over-LAN。由于 IPMI 有时为自定义,因而对非标准执行的支持不尽相同。

**注:** SP供应商经常更新固件。装置对每个 SP的支持取决于 SP固件功能。请参阅装置固件发行说明,获取 SP类型和支持的 SP固件版本的完整列表。

您还可以一次添加多个 SP, 方法是创建一个包含要添加的 SP 的 IP 地址、端口、用户名、密码 和 SP 类型的自定义文件。

添加 SP 后,其信息将在"SP 管理"页面的表中显示。

注: 不具备管理员访问权限的用户只能查看他们可以访问的设备。

### 要手动添加 SP:

1. 单击侧面导航栏中的"目标"-"SP管理"。

2. 单击"添加 SP"。

- 3. 输入 SP的 IP 地址和别名。
- 4. 如果要为 SP 提供用户名和密码,取消勾选复选框并输入所需的凭据。如果保持勾选复选框,将从默认用户列表中查找用户名和密码。
- 5. 使用下拉菜单选择适当的 SP 配置。
- 6. 以十六进制格式输入 KG( 可选) 。
- 7. 使用下拉菜单选择加密和组名(可选)。
- 8. 如果要启用 SoL 数据缓冲(SoL 历史),请勾选复选框。
- 9. 单击"应用"。

### 要导入 SP 列表:

- 使用以下格式创建 SP 文件: [#]IP:端口:用户名:密码:配置。有关更多信息,请参阅第 88 页 的"创建 SP 文件"。
- 2. 单击"目标"-"SP管理"。
- 3. 单击"导入 SP"。
- 4. 浏览至存储 SP 文件的位置,单击"导入 SP"并单击"确定"。
- 5. 您开始导入 SP 列表后,它们将填充到 SP 列表中。
- 6. 您可以单击"停止导入",以停止剩余的导入进程。

#### 要编辑 SP:

- 1. 单击"目标"-"SP管理"。
- 2. 单击要编辑的 SP 名称。
- 3. 在"修改 SP"选项卡下,您可以编辑 SP 的名称、用户名和密码,并且根据配置类型,还可以 编辑 KG、加密和 SoL 数据缓冲。
- 4. 单击"应用"。
- 5. 在"SoL"选项卡下,您可以启用 Serial over LAN,并配置波特率、通道包级别限制和重试计数。
- 6. 单击"应用"。

### 要移除 SP:

- 1. 单击"目标"-"SP管理"。
- 2. 在 SP 列表中,选择要移除的 SP 并单击"删除"。

# 搜索

您可在装置路由访问的各个 IP 范围中搜索服务处理器。您可为自动或手动搜索指定最多 20 个 IP 地址范围。搜索到的服务处理器将显示在 SP 管理列表中。

要搜索服务处理器, SP 必须具有搜索范围中的 IP 地址, 且在"默认用户"选项卡中预填充了用户 名和密码。SP 必须为固件发行说明中列举的装置支持的类型。

### 物理搜索

默认情况下,装置具有运行于 priv 虚拟接口上的活动的 DHCP 服务。

通过物理连接与装置相连,并配置为 DHCP 客户端的 SP 将被分配一个 IP,然后进行查询搜索。 默认情况下,DHCP 作用域只会分配给 priv 虚拟端口及相关联的物理端口。默认情况下, spm 和 kvm 虚拟端口没有分配的地址。要将 DHCP 范围分配到 spm 和 kvm 虚拟接口以独立地搜索和管 理设备的特定级别,必须先向虚拟接口分配 IP。Priv 虚拟接口默认为: 192.168.10.1/24。

### 要分配虚拟接口 IP 地址:

- 1. 浏览至位于"管理员"一"目标"一"端口配置"一"网络设置"的"网络设置"页面。
- 2. 使用"状况"下的下拉菜单, 启用接口。
- 3. 输入 IP 地址/掩码和广播地址。
- 4. 单击"应用"。

表 5.6: CIDR 格式示例

对于 IP/掩码组合, IP 地址(CIDR 格式) 有时被称为前缀表示法。所需的 IP/掩码信息指占据按 二进制记数法显示时的子网掩码网络部分的位数。下表进行了举例说明。

十进制记数法	二进制计数法	前缀/CIDR 表示法	示例
255.0.0.0	11111111.0000000.0000000.00000000	/8	10.1.2.3/8
255.255.0.0	11111111.11111111.00000000.0000000	/16	172.18.1.4/16
255.255.255.0	11111111.11111111.11111111.00000000	/24	192.168.1.10/24
255.255.255.252	11111111.11111111.11111111.11111100	/30	176.23.8.1/30

分配虚拟接口 IP 地址后,即可创建新的 DHCP 范围。请务必确保 DHCP 范围适合分配给虚拟接口的 IP,但此范围不包括此 IP(避免发生 IP 冲突的可能性)。对于新范围,虚拟 IP 应分配为网关。

### 要创建动态 DHCP 范围:

- 1. 浏览至"目标"一"端口配置"一"DHCP设置"。
- 2. 在"动态范围"下单击"添加"。
- 3. 输入子网地址、开始和结束范围、子网掩码和网关。
- 4. 单击"应用"。

装置将尝试添加分配了 IP 地址的任意 SP。如果默认用户列表包含有效 SP 凭据,装置将能够利用帐户列表查找匹配的凭据。如果装置能成功登录,SP 将显示在目标列表中。

#### 要添加/编辑默认用户列表中的凭据:

- 1. 浏览至"目标"-"SP管理"-"默认用户"。
- 2. 单击"添加"以添加新用户。

```
一或一
```

单击用户以编辑用户。

- 3. 添加或编辑用户名和密码。
- 4. 根据需要添加或编辑说明。
- 5. 单击"应用"。

# 逻辑搜索

装置能创建最多 20 个搜索队列以用于搜索网络上的 SP。搜索范围定义装置将扫描以查找 SP 的起止 IPv4 地址。可手动(运行一次)或自动(根据定义的时间间隔分钟数运行)运行搜索。

如果装置可以识别 SP 类型,并使用默认用户列表中的凭据登录,那么 SP 将被添加到目标列表。如果装置无法识别或登录 SP,将不会进行任何添加,您将需要手动添加或使用"导入 SP"功能。

#### 要搜索服务处理器:

- 1. 单击导航菜单中的"目标"-"SP管理"-"搜索"。
- 2. 单击"添加"以打开"修改搜索范围"屏幕。
- 3. 输入要搜索的名称,然后在"自"和"至"字段中输入 IP 地址范围。
- 4. 使用下拉菜单手动或自动开始搜索。
- 5. 如果您要按确定的时间间隔自动搜索设备,可输入 10 分钟到 30 天的时间间隔范围。以 ddhh-mm(天数-小时-分钟)格式输入时间间隔,然后单击"应用"。
- 6. 单击"搜索范围开始"以开始搜索过程。

**注**: 重新扫描主要为静态的环境中的相同 IP 范围将消耗装置进程资源和增加不必要的网络流量。建议仅对更改频繁的动态环境使用自动搜索。

## 默认用户

装置包含一个默认用户列表。您可添加或修改默认用户的名称、密码和说明。说明可用于识别 帐户。您还可以单击默认用户旁的复选框,并单击"删除"来将其删除。

#### 要添加或修改默认用户:

- 1. 单击侧面导航栏中的"目标"一"SP管理"一"默认用户"。
- 2. 单击"添加"以添加新用户。

一或一

单击带超链接的用户名以修改该用户。

- 3. 输入或修改用户名和密码。
- 4. 单击"应用"。

# 串行管理

任何自动检测端口都可用于将串行目标连接到装置。自动检测端口支持 Avocent<sup>®</sup> 或 CISCO<sup>™</sup> 软脚位排列模式。连接到适配器时,将自动选择 Avocent 软脚位排列。将装置的自动检测端口连接 到 Avocent ACS 设置端口时,应使用直通缆线和 CISCO 软脚位排列。

UTP 直通缆线连接到 Cisco 或 Sun 目标上的 RJ-45 串行端口。装置将查看串行目标并将 Cisco 软脚 位排列模式自动分配到连接的端口。

## 串行机架 PDU

当将装置的自动检测端口连接到 Cyclades<sup>™</sup> PM10/20 或 Avocent<sup>®</sup> PM PDU 时, CAT5/CAT6 直通缆 线应连接到 PM PDU 的输入/控制台端口。

# 串行控制台端口

将串行端口连接到设备上的控制台端口时,必须为串行端口定义 CAS 配置。CAS 连接协议适用于以下情况:

- 当用户通过 web UI 访问串行端口时,会话将自动使用指定的协议与连接的设备的控制台相 连。
- 当用户远程登录串行端口时, 仅允许使用所选协议进行访问。如果使用另一协议, 访问将被 拒绝。例如, 如果您指定控制台 (SSH) 协议, 那么用户可以使用 SSH 但不能使用 Telnet 来访 问串行端口。

下表显示了当控制台服务器串行端口连接到服务器或设备的控制台端口时,连接协议列表中的选项。

表 5.7: 串行端口连接到设备控制台端口时的连接协议

协议名称	结果	
控制台 (Telnet)	授权用户可使用 Telnet 与连接的设备的控制台相连。	
控制台 (SSH)	授权用户可使用 SSH 与连接的设备的控制台相连。	
控制台 (Telnet/SSH)	授权用户可使用 Telnet 和/或 SSH 同时与连接的设备的控制台相连。配置了多个会话功能后,可通过串行端口同时进行 Telnet 和/或 SSH 会话。	
控制台 (Raw)	授权用户可与连接的设备的控制台进行原始套接字连接。	

### 要编辑一个或多个串行控制台端口:

- 1. 单击"目标"一"串行管理"。
- 2. 在"串行控制台"选项卡下,单击要配置的每个端口的复选框。
- 3. 单击"编辑"按钮。
- 4. 单击"CAS"选项卡以配置 CAS 设置。完成后单击"应用"。
- 5. 单击"数据缓冲"选项卡以配置数据缓冲设置。完成后单击"应用"。
- 6. 单击"警告"选项卡,然后单击"添加"以添加警告字符串。完成后单击"应用"。

注: 请参阅下表, 了解有关 CAS、数据缓冲和警告参数的说明。

表 5.8:	CAS 配置参数
参数	说明
CAS	
端口名 称	与串行端口相关联的名称(别名)。默认: <装置 mac地址>-p-<端口号>
启用自 动搜索	将搜索目标名称,并将该名称与该串行端口相关联。如果失败,将使用端口名称。默认:禁用。
协议	将用于访问串行端口/目标的协议。SSH 一 授权用户可使用 SSH 与连接的设备的控制台相 连。Telnet 一 授权用户可使用 Telnet 与连接的设备的控制台相连。SSH/Telnet 一 授权用户可使用 SSH 和/或 Telnet 同时与连接的设备的控制台相连。Raw 一 授权用户可与连接的设备的控制台进行 原始套接字连接。默认:SSH/Telnet。
TCP 端 口别名	对于 Telnet/Raw 会话:直接连接到串行端口的 TCP 端口。对于 SSH 会话: 与 ttySxx 相似的端口别 名。默认: 70XX,其中 XX 是串行端口号。

参数	说明		
仅在 <b>DCD</b> 打 开时允 许会话	当 DCD 关闭时,装置将拒绝对该串行端口的访问。默认:禁用(DCD 关闭时允许访问)。		
启用自 动响应	当输入数据与在自动响应中配置的一个输入字符串匹配时,输出字符串将被传输到串行端口。默 认:禁用。		
DTR 模 式	DTR模式可设置为以下状态:始终打开。正常 - DTR状态将取决于 CAS 会话是否存在。关闭时间间隔 - 当 CAS 会话关闭时,DTR将在此时间间隔内保持关闭。默认:正常。		
<b>DTR</b> 关 闭时间 间隔	DTR模式关闭时间间隔(单位为毫秒)使用的时间间隔(单位为秒)。默认:100。		
取消换 行	启用取消 CR 字符后的换行符。默认:禁用。		
取消回 车后为 空	启用取消 CR 字符后的 NULL 字符。默认:禁用。		
传输时 间间隔	端口等待将数据发送到远程客户端的时间间隔,单位为毫秒。默认:20。		
中断顺 序	用于将中断信号发送到串行端口的顺序。不适用于 Raw。默认: ~中断。		
中断时 间间隔	中断信号的时间间隔,单位为毫秒。不适用于 Raw。默认: 500。		
登录/注 销多个 会话通 知	启用当新用户登录或用户注销时对多个会话用户的通知。不适用于 Raw。默认:禁用。		
数据缓凇	<del>†</del>		
状态	启用或禁用数据缓冲。默认:禁用。		
类型	显示数据缓冲的类型:本地一将数据缓冲文件存储在本地文件系统中。Syslog一将数据发送到 syslog服务器。默认:本地。		
时间戳	启用后,向本地数据缓冲的数据线添加时间戳。默认:禁用。		
登录/注 销消息	包括数据缓冲中登录和注销的特殊通知。默认:禁用。		
串行会 话记录	启用 一 随时存储数据。 禁用 - CAS 会话未打开时存储数据。默认: 启用。		
警告			
警告字 符串	用于生成事件通知的字符串。默认: 空。		

### 要配置 CAS 配置:

- 1. 单击侧面导航栏中的"目标"一"串行管理"。
- 2. 单击"CAS 配置"选项卡。
- 3. 在"设置"标题下,输入自动搜索超时和探测超时的秒数。
- 要添加自动响应输入和输出字符串,单击"添加"。在"输入字符串"或"输出字符串"字段中输 入新的字符串,并单击"应用"。

一或一

要删除自动输入和输出字符串,请选择要删除的字符串旁的复选框。单击"删除"。

5. 要更改默认的自动搜索超时或探测超时,请执行以下步骤。

- a. 选择"设置"。
- b. 在"自动搜索超时"和"探测超时"字段中输入新值。
- c. 从"自动搜索故障"下拉列表和"探测速度"列表的"默认速度"中选择速度。
- d. 单击"保存"。
- 6. 要添加新的探测、匹配字符串或删除现有字符串,请执行以下步骤。
  - a. 要添加字符串,单击"添加",在"新探测字符串"或"新匹配字符串"字段中输入新字符串, 并单击"保存"。
  - b. 要删除字符串,请选择字符串的复选框并单击"删除"。
- 7. 单击"应用"。

## 电源

单击侧面导航栏中的"目标"一"串行管理",对在"目标"一"端口配置"一"端口分配"一"端口配置" 的"端口类别"下拉菜单中指定的连接配置串行 PDU 的参数进行配置。

### 要编辑串行 PDU 端口:

- 1. 单击"目标"一"串行管理"。
- 2. 在"串行 PDU"选项卡下,单击要配置的各端口的复选框。
- 3. 单击"编辑"按钮。
  - a. 使用下拉列表选择 PDU 类型。
  - b. 勾选复选框以启用速度自动检测。
  - c. 配置轮询率。
  - d. 输入重新启动时间间隔, 然后使用下拉菜单启用或禁用 Syslog、蜂鸣器和软件过电流保护。
- 4. 单击"应用"。

# 串行数据记录

您可以启用串行端口以进行数据记录。

### 要启用串行设备的数据记录:

- 1. 单击"目标"一"串行管理",然后勾选要记录的端口旁的复选框。
- 2. 单击"编辑"。
- 3. 单击"数据缓冲"选项卡,使用下拉菜单将"状态"和"串行会话记录"更改为"启用"。
- 4. 使用下拉菜单选择"类型",并启用或禁用"时间戳"和登录/注销消息。
- 5. 单击"应用"。

与启用的目标端口的串行会话启动后,您可以下载记录的数据。

### 要下载记录的数据:

1. 单击标题栏中的"目标"。

2. 单击侧面导航栏中的"串行控制台",然后单击启用了数据记录的目标。

3. 单击"日志"选项卡,然后单击"下载"日志。

# 串行端口警告

在配置数据缓冲的同一管理区域中,可以定义警告字符串。串行警告字符串是将与串行数据 I/O 进行匹配性比较的文本字符串。如果检测到匹配,装置将发送电子邮件或 syslog 警告,其中包含端口、名称、字符串等。正则表达式可用于字符串匹配。

# **KVM** 管理

Avocent® Universal Management Gateway 装置结合了模拟和数字技术,可对数据中心服务器和虚拟 媒体进行灵活的集中控制,便于远程分支办公室在没有训练有素的操作员的情况下进行操作、 激活和维护。通过 KVM over IP,您可以随时随地灵活控制目标设备管理,并进行安全的远程访问。

装置的 KVM over IP 功能可为企业客户提供以下特性和选项:

- 键盘、视频和鼠标 (KVM) 功能,可配置用于模拟(本地) 或数字(远程) 连接
- 增强的视频分辨率支持,从目标到远程的原始分辨率高达 1600 x 1200 或 1680 x 1050( 宽屏)
- 通过 USB 端口访问的虚拟媒体功能
- 智能卡功能

# UMIQ 模块

Avocent UMIQ 模块是一种适配器,可为装置提供基于 KVM over IP 支持的传统 VGA/USB 功能。 该模块可使模拟 VGA 信号和 USB 信号(键盘、鼠标、大容量存储器、CD/DVD、智能卡-CAC) 数字化,并通过 IP 传输。这样即可为远程用户提供机架体验,无论他们选择在什么地方。

## 图 5.2: UMIQ-v1 模块



### 图 5.3: UMIQ-v2 模块



表 5.9	表 5.9: UMIQ 模块说明		
编 号	说明		
1	模块的 RJ-45 接头。v1 模块具有通过 CAT 5 缆线连接到装置的端口。v2 模块具有可连接到专用 SP 的 另一个端口。		
2	直流电源插头。		
3	视频用VGA连接器。		
4	键盘和鼠标用 USB 连接器。		

UMIQ 模块装有嵌入式 Linux 操作系统,可在 UMIQ 模块加电时启动。UMIQ 模块需要充足的 USB 总线电源才能正常运行。对于不能提供充足电源的服务器、缺少 USB 接口的设备,或 IQ 模 块经常从一个服务器移至另一个服务器的自动配置工作站,直流电源插头非常有用。只要 UMIQ 模块从 USB 或直流电源获得供电,就会被视为电力充足,可以维持与装置的安全 IP 连接和与用 户的 KVM 会话。如果 UMIQ 模块失去供电但仍然与装置相连,将请求装置通过 UTP 缆线传送备 用电源,以防止 UMIQ 模块进入脱机状态。

依靠备用电源运行的 UMIQ 模块不能支持 KVM 会话,但可以保持与装置的连接。UMIQ-v2 模块可保持两个端口之间的桥接,从而确保 SP 始终可以访问。装置将使用直流连接器来满足其全部的电源需求,而 USB 插头将仅用于数据交换。装置从直流或 USB 获取的电量为 5v 0.5a。

将自动检测端口连接到 UMIQ 模块时,应使用直通 UTP 缆线。UMIQ-v1 模块具有一个用于连接装置的 RJ-45 端口。UMIQ-v2 模块具有两个 RJ-45 端口,一个可以连接到装置,另一个可以连接到服务器上的专用服务处理器端口。缆线长度最长可达 100 米。

**警告:** 切勿连接装置和 UMIQ 模块之间的网络(交换机/集线器/防火墙/路由器)。装置输送的电流会损坏除 UMIQ 模块之外的设备。

表 5.10: UMIQ 模块 LED 状态		
LED	状态	说明
	持续亮起	当 UMIQ模块通过 USB 电源运行且处于正常运行状态时,电源 LED 将亮起。
电源	连续单次闪烁	升级期间,UMIQ模块LED将闪烁,频率为2Hz,占空比为50%。
LED	两次闪烁组合	UMIQ模块正在使用通过以太网缆线从装置提供的备用电源。
	三次闪烁组合	提供的电源不足。在目标服务器上的 USB 主机枚举 UMIQ模块之前,可能会出现此情况。
	持续亮起	存在活动的 KVM 会话时,活动 LED 将亮起。
活动	连续单次闪烁(快速)	用于识别 UMIQ模块在装置 web UI 中是启用还是禁用。
LED	连续单次闪烁( 慢速)	活动 LED 定期闪烁,表明 UMIQ 模块已与装置相关联(例如,已被装置搜索到)。
两个 LED	连续单次闪烁(快速并与电源 LED交替)	LED交替快速闪烁,表明固件升级失败。

# 设备

单击侧面导航栏中的"管理"一"目标"一"KVM管理",查看各个连接的 UMIQ 模块。可根据需要对 各列排序。您可以查看各模块的以下信息:

- 端口一连接模块的装置端口。进行初次连接或恢复出厂设置时,装置自动检测到正确的端口号前,端口号为99。
- EID 显示模块中内嵌的唯一电子标识号。
- 状态 显示模块处于"使用中"、"空闲"还是"脱机"状态。
- 管理 -显示模块处于"预搜索"、"托管"还是"未托管"状态。进行初次连接或恢复出厂设置时,由于正在搜索模块,管理状态将从"预搜索"更改为"托管"。
- 装置电源 显示装置是否为模块供电。
- 电源模式 一显示模块的电源状态。"满"表示模块正由装置和目标供电。"部分"表示仅由装置 供电。

# 模块设置

单击一个模块将仅显示它的设置。有关设置的详细说明,请参阅第52页的"默认设置"

勾选复选框可启用或禁用闪存定位器 LED。启用后,模块上的 LED 将会闪烁,以帮助您在机架中找到此模块。

# 升级 UMIQ 模块

通过 UMIQ 模块闪存升级功能,装置管理员可使用最新的可用固件更新 UMIQ 模块。

在闪存存储器通过升级重新编程后,装置将执行软重设,这将终止所有 UMIQ 模块会话。在 UMIQ 模块进行固件更新时,目标设备可能不显示,也可能显示为断开连接状态。闪存更新完成 后,目标设备将正常显示。

装置更新后,UMIQ模块将自动更新。要更改装置固件,请参阅第54页的"*固件*"。

如果在正常升级过程中出现问题,必要时还可能会强制升级 UMIQ 模块。

注: 请访问 www.avocent.com 获取固件升级文件。

### 要升级 UMIQ 模块固件:

1. 单击侧面导航栏中的"目标"一"KVM管理",打开"UMIQ模块"屏幕。

2. 选择要升级的 UMIQ 模块旁的复选框,并单击"升级"。

注意: 在进行固件更新或重启目标设备电源期间断开 UMIQ模块将使模块发生故障,导致 IQ模块必须退回工厂返修。

# 删除脱机模块

装置会为与其连接的各个 UMIQ 模块保留一个数据库。如果您不再需要某个模块,可以将其从数据库中删除。

**注意**: 建议您仅删除脱机模块。如果您删除了仍在使用中的模块,您将失去所有自定义设置,并且必须恢复出厂设置 才能进行管理。

### 要删除脱机 UMIQ 模块:

- 1. 单击侧面导航栏中的"目标"一"KVM管理",打开装置 UMIQ 屏幕。
- 2. 选择要删除的 UMIQ 模块旁的复选框,并单击"删除脱机模块"。

# 恢复出厂设置

配置模块后,您可以将其恢复到出厂默认设置。

### 要将 UMIQ 模块恢复为出厂设置:

- 1. 单击侧面导航栏中的"目标"一"KVM管理",打开装置 UMIQ 屏幕。
- 2. 选择要删除的 UMIQ 模块旁的复选框,并单击"恢复出厂设置"。

注: 恢复出厂设置将删除所有自定义设置。

# 活动会话

如果您的装置型号支持 KVM 连接,单击"目标"一"KVM 管理"可查看 KVM 连接。

"活动会话"窗口将显示以下字段:

- 会话模式 显示会话类型。选项为"正常"和"独占"。"正常"是可与其他用户共享的交互式会话。"独占"是不允许其他用户共享的私有会话。
- 类型 会话类型, 可能是 KVM、虚拟媒体或串行。
- 名称 目标的名称。
- 用户 一 启动会话的用户,可能是用户、本地端口用户或具有本地用户帐户的用户。
- 持续时间 控制台会话的当前时间长度。
- 客户端 连接到会话的客户端计算机的 IP 地址。
- EID 显示模块中内嵌的唯一电子标识。

### 要查看或终止活动会话:

- 1. 单击"活动会话"。
- 2. 选择要终止的会话旁的复选框。单击"终止"。

# 默认设置

KVM 默认设置是即将应用到新 UMIQ 模块的全局设置。这些设置对现有 UMIQ 模块没有任何影响。但是,您可以通过恢复出厂设置操作,将默认设置应用到现有 UMIQ 模块。

常规

在"常规"标题下,您可以选择删除脱机模块或自动升级模块。默认情况下,两种设置均已禁用。 要了解更多信息,请参阅第51页的"删除脱机模块"或第50页的"升级 UMIQ 模块"。

### 共享

在"共享"标题下,您可以启用和选择共享级别。选项包括:"自动"、"独占"和"隐藏"。

- "自动"是自动允许另一用户共享控制台会话的共享选项。尝试访问已在使用中的控制台会话的用户将不会收到共享提示,而是自动登录会话。
- "独占"是不允许其他用户共享的私有共享选项。
- "隐藏"是启动视频查看器窗口会话的共享选项,但您只能查看目标发生的情况,而不能控制
  键盘或鼠标。当前处于活动状态的用户将不会收到访问正在被共享的通知,也不会被要求授权共享。如果用户的抢占级别高于或等于您的抢占级别,则可能不会允许隐藏连接。

当您尝试连接已被另一用户使用的会话时,将出现一个对话框,说明无法查看目标以及当前用 户的名称。此时,您可以请求共享目标访问、抢占用户或使用隐藏模式(如果已启用)。

- 共享连接一当您收到共享连接的提示时,单击"与其他用户共享"。共享目标时,如果没有 其他活动用户,所有用户都可以进行监视和控制。
   单击"确定"后,活动的主用户将收到允许共享的请求,除非启用了"自动"。如果用户确 认,您将可以访问目标。
- 抢占用户连接一当您收到抢占用户会话的提示时,单击"抢占其他用户",将连接请求访问 目标的用户,而断开现有用户与目标的连接。现有用户将收到其会话已被抢占的通知。

要显示共享端口或通道的用户列表,在视频查看器窗口中选择"查看"一"连接的用户"。处于隐藏 模式的用户将不会显示在其中。

### 加密等级

在"加密等级"区域,指定键盘/鼠标、视频和虚拟媒体的加密等级:

- 3DES SSL 3DES 加密
- 128 位 SSL 使用 ARCFOUR (RC4®) SSL 加密的 128 位加密
- AES AES 加密

必须为键盘和鼠标至少指定一个加密等级。如果您指定多个 SSL 加密类型,装置将协调使用两者都支持的最强大的算法。AES 为最强大的算法,其后依次是 128 位、3DES 和 DES。

## 会话设置

在"会话设置"标题下,您可以配置"输入控制超时"、启用和配置会话超时、设置键盘语言、设置 视频分辨率,以及启用视频噪声控制。

**注**: 如果用户连接到屏幕分辨率高于本地计算机的目标,视频查看器窗口将显示部分目标屏幕,以及用于查看屏幕 剩余部分的滚动条。用户可通过调整目标、本地计算机或两者的分辨率,查看整个屏幕。

## 会话抢占

在"会话抢占"标题下,您可以启用抢占并设置超时。

#### 虚拟媒体

在"虚拟媒体"标题下,您可以启用虚拟媒体、锁定到 KVM 会话、允许保留的会话,以及选择虚 拟媒体访问模式。

- 锁定选项指定是否将虚拟媒体会话锁定到目标上的 KVM 会话。如果启用了锁定(默认)并 关闭了 KVM 会话,虚拟媒体会话也将关闭。如果禁用了锁定并关闭了 KVM 会话,虚拟媒体会话仍将保持活动状态。
- 允许保留的会话确保只能使用您的用户名访问虚拟媒体连接,其他用户不能建立与该目标的 KVM 连接。当相关联 KVM 会话断开连接时,根据"虚拟媒体"对话框中的锁定设置,虚拟媒体会话也可能断开连接。
- 通过虚拟媒体访问模式,您可以将映射驱动器的访问模式设置为只读或读写。当访问模式为 只读时,用户将无法向客户端服务器上的映射驱动器写入数据。如果访问模式为读写,用户 将可以在映射驱动器中读写数据。如果映射驱动器设计为只读(例如 CD-ROM 驱动器、DVD-ROM 驱动器或 ISO 映像),那么配置的读写访问模式将被忽略。当映射大容量存 储设备或 USB 可移动媒体等读写驱动器,而您想防止用户向其写入数据时,设置只读模式非 常有用。

您可以同时映射一个 DVD 驱动器和一个大容量存储设备。CD 驱动器、DVD 驱动器或 ISO 磁盘镜像文件将映射为虚拟 CD/DVD 驱动器。

### 智能卡

您可以将智能卡读卡器连接到客户端服务器上可用的 USB 端口,并访问装置上连接的目标。然 后启动 KVM 会话以打开视频查看器。

### 要查看或更改默认设置:

- 1. 单击"默认设置"。
- 2. 如果您要自动删除脱机模块或自动升级模块,请取消勾选复选框。
- 3. 对于共享,选择复选框"启用"、"自动"、"独占"或"隐藏"。
- 4. 对于加密等级,使用下拉菜单选择视频、键盘/鼠标和虚拟媒体的加密等级。
- 5. 对于会话设置:
  - a. 在1到50之间选择"输入控制超时",其中1表示十分之一秒。
  - b. 如果要启用会话超时,请勾选该复选框。
  - c. 设置会话超时(分钟)。
  - d. 从下拉菜单中选择键盘语言。
  - e. 从下拉菜单中选择最大视频分辨率。
  - f. 如果您要启用"视频噪声控制",请勾选该复选框。
- 6. 对于会话抢占:
  - a. 如果允许抢占,请勾选该复选框。
  - b. 在"抢占超时"字段中,输入将显示提示通知您会话即将被抢占的时间(1到120秒)。
  - c. 如果要启用 PPP, 请勾选该复选框。

- 7. 对于虚拟媒体:
  - a. 勾选复选框以启用虚拟媒体、锁定到 KVM 会话或允许保留的会话。
  - b. 设置抢占超时(秒)。
  - c. 从下拉菜单中,选择"虚拟媒体访问模式"。
- 8. 选择复选框以启用智能卡访问。
- 9. 单击"应用"。

# 目标组

单击侧面导航栏中的"目标"一"目标组"。您可以在此屏幕中创建组目标。单击"添加"以创建新的 空组,或选择现有组并单击"删除"以删除该组。

## 要修改组:

- 1. 单击"目标"一"目标组", 然后单击要修改的组名称。
- 2. 从右侧的"可用"列表中选择一个或多个目标,单击向左箭头将其添加到组内容中。

注: 可使用过滤字符串缩小目标列表范围。

3. 单击"应用"。

# 启动

单击侧面导航栏中的"启动"可显示启动设置。"引导程序配置"定义装置加载操作系统的位置。您可以加载上一次正确配置,它是运行正常的最新的系统设置。

## 要配置"引导程序配置":

- 1. 单击"启动"。
- 2. 选择引导程序固件的文件名。
- 3. 单击"应用", 然后单击"重新启动"。

# 固件

装置支持存储两个固件映像。这些映像与将操作系统和配置合并在一起的双引导系统中的不同 操作系统行为相似。通过 DSView 管理软件或 web UI 升级固件时,装置会将活动配置复制到新 的固件映像插槽中,并将这些配置与新固件操作系统合并。

安装新映像文件后,装置将重新引导至第二个固件映像插槽。映像插槽1和2的配置相同,但 是之后的所有更改都将仅应用到当前引导的映像中。如果您遇到与新固件映像有关的问题,可 以重新引导至旧映像。

固件升级后,最早的映像将被新固件覆盖。

单击侧面导航栏中的"固件",可查看当前固件版本、升级到最新版本、备份或删除固件。

### 要下载装置固件:

- 1. 在 http://www.avocent.com 中浏览至产品更新部分,找到适用于您的 Avocent® Universal Management Gateway 装置的固件。
- 2. 将新固件保存到 /tmp 目录。

通过 web UI升级固件需要耗时 90 分钟到两小时。在此期间,装置将显示为脱机。如果在升级期间会话超时,升级将被取消。为此,建议您先禁用会话超时,再升级固件。

## 要禁用会话超时:

- 1. 单击侧面导航栏中的"用户"。
- 2. 单击执行升级的用户。
- 3. 取消选择"会话超时"复选框。
- 4. 单击"应用"。

### 要升级固件:

- 1. 单击侧面导航栏中的"固件", 然后单击"升级"。
- 2. 浏览至保存已下载固件的 /tmp 目录。在确认框中单击"确定"。
- 3. 进度栏将显示升级的状态。装置处理更新时将重新启动。

之后启动装置时,新旧固件都将在启动屏幕上显示。装置将通过 web UI 的启动页面上定义的映像启动。

# 备份固件

管理员可为装置的固件和配置创建备份映像。创建图像时,不得对配置进行任何更改。完成 后,装置将重新启动。备份图像将驻留在装置中,但必须先下载才能使用。有关 Netboot 恢复步 骤的信息,请参阅第 87页的"从网络启动"。

#### 要备份装置固件:

- 1. 在"图像管理"下输入图像名称。
- 2. 单击"创建备份图像",并单击"确定"。

注: 装置一次只能存储一个映像。

### 要删除映像:

选择要删除的映像旁的复选框,并单击"删除映像"。

# **USB**设备

单击侧面导航栏中的"USB设备",可查看所有连接的USB设备的名称、类型、信息和状态。您 也可以启用或禁用装置上的所有USB端口,以及弹出任意设备,使其能正常关闭。

## 要安装 USB 大容量存储设备:

1. 单击"USB 设备"。

2. 勾选设备旁的复选框,并单击"启动"。当设备的状态更改为"请勿移除"时,设备将安装在/media/usbhd-port1-4 目录中。

### 要卸载 USB 大容量存储设备:

1. 单击"USB 设备"。

2. 勾选设备旁的复选框,并单击"停止"。当设备状态更改为"可安全移除"时,即可安全移除设备。

# 配电

连接的电源设备可用于远程电源管理。通过装置,授权进行电源管理的用户可以开关电源和重设插入连接的 PDU 的设备。

以下电源设备类型可连接到为电源配置的任意端口:

• Avocent 电源管理配电设备 (PM PDU)。

# 登录

管理员可更改支持 PDU 类型的登录密码。装置使用该密码与 PDU 进行通信(相同类型的所有 PDU 只能使用一个密码)。

### 要更改 PDU 密码:

- 1. 选择"配电"一"登录"。
- 2. 要更改 PDU 的密码,请在具有相应标记的部分输入密码。
- 3. 单击"应用"。

# 传感器

传感器端口位于装置的背面,用于从支持的传感器收集数据。传感器不会被自动检测到,而必须手动添加并启用。要查看传感器上的状态,单击"传感器"。

注: 某些装置型号不含传感器端口。

### 图 5.4: 传感器端口



#### 表 5.11: 传感器端口

编号	名称	类型
1	SNSR/COM2 (RS-485)	温度、湿度和水
2	DO2( 数字输出)	蜂鸣器、警示灯和门锁
3	DI1/DI2( 数字输入)	振动、烟雾、泄露、门或动作
4	TH1/TH2( 1线)	温度、湿度和干触点

下表显示了可收集的数据。

表 5.12:	环境测量
---------	------

测量	单位
温度	摄氏度/华氏度
湿度	%相对湿度
门状态	活动/不活动
泄漏状态	活动/不活动
动作状态	活动/不活动
振动状态	活动/不活动
烟雾状态	活动/不活动

# COM 数字输入

COM 数字输入 (DI) 传感器用于查看和监控动作及烟雾,可连接到装置背面的 DI1/DI2 端口。

属性	说明	默认值
传感器编号	传感器 ID( 只读)	系统定义值
启用	启用或禁用	启用
名称	传感器名称	传感器 ID
类型	烟雾、门、泄漏或动作。只有在添加了传感器后才能选择传感器类型。	烟雾
默认状态	打开或关闭	打开
位置	传感器的位置或方位	空

### 要添加、启用或移除 COM 数字输入传感器:

- 1. 单击"管理"一"传感器"一"COM 数字输入"。
- 2. 输入传感器的名称。

表 5.13: COM 传感器属性

- 3. 选择端口(DI1或DI2)。
- 4. 选择传感器的类型并单击"添加"。
- 5. 单击传感器名称,选择正常状态,并单击"启用"。
- 6. 要移除传感器,单击传感器名称,并单击"移除"。

# OneWire 数字输入

OneWire 数字输入会收集烟雾、泄漏和动作数据,可连接到装置背面的 DI1/DI2 端口。

属性	说明	默认值
传感器编号	传感器 ID( 只读)	系统定义值
启用	启用或禁用	启用
名称	传感器名称	传感器 ID
默认状态	关闭或打开	打开
位置	传感器的位置或方位	空

属性	说明	默认值
类型	传感器类型: 自定义、烟雾、泄露或动作	自定义
地址	传感器的序列号(只读)	传感器的信息

### 要检测、启用/禁用或编辑 OneWire 数字输入传感器:

- 1. 单击"管理"一"传感器"一"OneWire 数字输入"。
- 2. 单击"检测",搜索新的传感器。
- 3. 单击传感器编号,然后选择传感器类型或更新正常状态。
- 4. 单击"启用", 启用或禁用传感器。

# OneWire 环境

OneWire环境传感器会收集温度和湿度数据。他们可连接到装置背面的 TH1/TH2 端口。

属性	说明	默认值
启用	启用或禁用	启用
名称	传感器名称	传感器 ID
类型	温度或湿度( 只读)	温度
地址	传感器的序列号( 只读)	传感器的信息
位置	用户定义的传感器位置	空

#### 表 5.15: OneWire 环境传感器属性

### 要检测、启用/禁用或编辑 OneWire 环境传感器:

- 1. 单击"管理"一"传感器"一"OneWire环境传感器"。
- 2. 单击"检测",搜索新的传感器。
- 3. 单击传感器编号,然后单击"启用"或"禁用",以启用或禁用传感器。

# RS-485 环境

RS-485 环境传感器会收集温度、湿度和水的数据。它们可连接到装置背面的 SNSR/COM2 端口。 表 5.16: RS-485 环境传感器属性

属性	说明	默认值
传感器编号	传感器 ID( 只读)	系统定义值
启用	启用或禁用	启用
名称	传感器名称	传感器 ID
类型	温度或湿度( 只读)	温度
地址	传感器的序列号(只读)	传感器的信息
位置	传感器的位置或方位	空

## 要添加、启用或移除 RS-485 环境传感器:

- 1. 单击"管理"一"传感器"一"RS-485环境传感器"。
- 2. 使用下拉菜单选择传感器的"类型"和"地址"。
- 3. 输入传感器的名称和湿度名称(如适用)。

- 4. 单击"添加"。
- 5. 勾选复选框以启用传感器,并单击"应用"。
- 6. 要移除传感器,单击传感器名称,并单击"移除"。

# 监控

装置将监控各种事件并生成通知。您可以配置装置,以存储通知或将通知发送到不同的目的 地,供立即使用或留待日后分析。所有事件都将自动添加到"事件摘要"选项卡,并且不能关闭。 配置后,装置传感器数据可为任何事件触发 syslog 或电子邮件警告。数字输出 (DO)继电器仅用 于装置背面的事件。它们可以切换继电器以启用风扇或警报。

# 电子邮件

您可以配置装置,以将警告发送到某个电子邮件地址。

### 要配置电子邮件警告:

 从侧面导航栏转到"装置设置"一"电子邮件设置",并输入电子邮件服务器的 IP 地址、端口 号、用户名和密码。

注: 建议您为装置创建电子邮件帐户。该帐户将作为发送通知电子邮件的帐户。

- 2. 单击"应用"。
- 从侧面导航栏转到"监控"。在"通知规则"标题下,勾选您要接收电子邮件警告的事件复选框。
- 从侧面导航栏转到"监控"一"通知目的地"。在"电子邮件地址"标题下,输入接收通知的电子 邮件地址。
- 5. 单击"应用"。

# Syslog

您可以在装置上最多配置四个 syslog 规则。Syslog 规则最多可以分配到六个 syslog 设施级别。Syslog 规则可以将警告转发到外部 syslog 服务器或日志文件。

您可以设置以下事件类型的消息记录:

- 与装置有关的事件
- SP上的传感器生成的传感器警报

消息可发送到用户定义的目的地。

## 消息过滤级别

您可以基于下列任意或所有级别,按照消息的严重性进行过滤:

- 紧急
- 关键
- 错误

- 通知
- 信息
- 调试

### 要配置 syslog 消息过滤:

- 1. 从侧面导航栏转到"监控"。从下拉列表选择设施:
- 2. 在"通知规则"标题下,勾选要接收 syslog 警告的事件的复选框,并单击"应用"。
- 3. 从侧面导航栏转到"监控"一"通知目的地",并在 Syslog 标题下,单击要配置的规则旁边的"配置"。
- 4. 在"Syslog 规则"页面的"配置 Syslog 规则"下输入"目的地"和"标签"。目的地可以是 IP 地址或日 志文件名称。
- 5. 在"设备"标题下,使用箭头选择本地设施。
- 6. 在"严重性"标题下,使用箭头选择严重性。
- 7. 单击"应用"。

# 数字输出

数字输出是远程控制的继电器端口,在装置的背面标记为 DO1/DO2,可用于打开或关闭能驱动 警报器、灯光和锁的电路。

### 要配置"数字输出"通知:

- 从侧面导航栏转到"监控"。在"通知规则"标题下,勾选要触发数字输出继电器的事件的复选框。
- 2. 单击"应用"。

注: 数字输出 (DO) 继电器仅用于装置背面的事件。

- 从侧面导航栏转到"监控"一"通知目的地",然后输入"数字输出 1"和"数字输出 2"的数字输出
  名称和位置。
- 4. 单击"应用"。

注: 触发数字输出继电器后,使用覆盖功能可进行重设。

# 通知目的地

装置会为各种事件生成通知。您可以配置装置,以将通知引导或存储到不同的目的地,供立即 使用或留待日后分析。

### 要配置事件目的地:

- 1. 单击导航菜单中的"监控"一"通知目的地"。
- 2. 在 Syslog 标题下,使用下拉菜单选择设施。

- 3. 在"远程服务器"一"IPv4"或"远程服务器"一"IPv6"字段中输入地址或主机名,以将 syslog 消息 发送到远程 IPv4 或 IPv6 syslog 服务器。
- 4. 选择"装置控制台",将消息发送到装置的控制台。
- 5. 在"SNMP Trap"标题下的"群组"字段中输入在一个或多个 SNMP Trap 服务器中定义的群组名称,然后在服务器字段中输入最多五个服务器的 IP 地址。
- 6. 在 SMS 标题下的相应字段中输入 SMS 服务器、端口和寻呼机号码信息。
- 7. 在"电子邮件"标题下的相应字段中输入"服务器"、"端口"和"目的地电子邮件"信息。
- 在"管理软件"标题下的"服务器位置"字段中输入用于发送事件通知的 DSView 3 服务器 IP 地址。在相应字段中输入 DSView 3 服务器的 syslog 服务器端口号、SSH 信息和缓冲区警告信息。
- 9. 单击"应用"。

# 会话

装置允许多个用户同时登录和运行会话。通过会话屏幕,您可以查看所有活动会话,并删除任何不需要的会话。单击"会话"可查看装置上所有打开的会话。

## 要删除会话:

- 1. 单击侧面导航栏中的"会话"。将显示会话屏幕,并列出所有与装置的装置和目标会话。
- 选择要删除的会话旁的复选框,然后单击"删除"按钮。数秒后,会话屏幕将重新显示打开的 会话,但不会显示您删除的会话。

# 支持

单击侧面导航栏中的"支持"可配置诊断记录。您可以创建和保存可下载并发送到技术支持的日志 文件。该日志文件显示正在运行的进程和正在使用的内存。

### 要启用系统监控:

- 1. 单击"支持"。
- 2. 勾选复选框以启用系统监控。
- 3. 设置频率(单位为分钟)并单击"应用"。

#### 要下载日志文件:

- 1. 单击"支持"。
- 2. 单击"下载日志"。
- 3. 浏览至保存位置并单击"保存"。

# 安全

单击侧面导航栏中的"安全", 启用或禁用以下网络服务:

- Telnet
- ICMP
- SSH

- HTTPS
- HTTPS 重定向

# 证书

默认情况下,装置安装有控制 Web 服务和允许通过 HTTPS 访问的证书。此外,还可以导入和配置第三方证书。导入第三方证书将替换默认的装置证书。如果要删除第三方证书并恢复默认证书,请联系 Avocent 专业服务。

注: 第三方证书必须为 PKCS12 格式。

## 要导入第三方证书:

- 1. 单击侧面导航栏中的"安全"。
- 2. 在"导入第三方证书"下, 输入并确认证书和密钥密码短语。
- 3. 单击"导入"。
- 4. 浏览至证书位置,并单击"打开"。
- 5. 单击"应用"并重启装置。

### 图 5.5: 第三方证书

目标	传感器	事件	管理						已登录,身份::admin
身份 ▼目标	验证			•	管理 > <u>安全性</u> SSH 重新启动关	n			
」。4世 DisP Di#約 Di KVI Di 目标	학理 行管理 M 管理 示组				目用 Teinet □ SSH 端口 22 HTTPS 端口 443				取補 应用
DSView D 启动	w				UMG 活动证书列表				
	1.49				序列号	公用名	组织	过期	
#3rb	em.				cc046d00cbb29d48	UMG Root Certificate	Emerson Network Power	30/06/20	
90 <u>0</u>									
受羽 ▼ 传感器 CO One One RS-	r M 数字输入 eWire数字输入 eWire环境传感 -485 环境传感				<b>导入第三方证书</b> 证书和密钥密码短语 确认密码矩语				
▼ 🗀 监控					<b>S</b> t				10% 応用
〕逋	目的地								
会话									
- 安全性									
防火墙	和 NAT			Ţ					

# 防火墙和 NAT

通过防火墙和 NAT 功能,管理员可以配置管理装置内流量过滤、IP 转发和地址转换的规则。

注: 装置专门设计用于管理设备管理控制台并提供对它的访问,而不用作通用路由器、交换机或数据包过滤器。

防火墙和 NAT 功能根据网络、主机、接口和服务的一系列命名定义构建而成。在配置"防火墙和 NAT"策略前,您必须定义策略规则中要使用的对象。最好先定义接口,然后定义策略规则将引 用的网络,最后定义主机和服务。以下部分对各个对象进行了说明。

装置已包含不同主机、网络和接口的信息,并在定义或搜索这些对象时进行创建。例如,将 UMIQ 模块连接到装置时,将创建与分配到 UMIQ 目标的名称相匹配的主机定义。

# 接口

默认情况下,"接口"选项卡会列出装置中定义的所有物理和虚拟接口,您可以通过单击侧面导航 栏中的"防火墙和 NAT"进行访问。

新的虚拟接口可设置用于专用端口,方法是单击"管理"一"目标"一"端口配置"一"网络设置"。有关创建接口的更多信息,请参阅第 39页的"端口配置"。

## 图 5.6: "接口"选项卡

理 > <u>防火搞和 NAT</u> SSH				
□ = = = = = = = = = = = = = = = = = = =				
安口设置				
外部接口(公共) 可用 eth1	包含 eth0			
	->			
应用 取消				
内部接口〈专用〉 可用	包含			
spm kvm eth1	-> priv			
<u></u> 应用 取消				
<b>h部防火墙接口信息</b>				
接口	MAC 地址	IP 地址		
eth0	00:e0:86:15:78:c6	10.207.26.36		

接口	MAC 地址	IP 地址	
priv	00:01:af:31:0b:c7	192.168.10.1/24	

通过该选项卡,您可以指定内部或外部接口在 NAT 和防火墙规则中的使用方法。指定为"内部"的接口为专用接口,指定为"外部"的接口为公共接口。

尝试在 NAT 或防火墙规则中引用接口前,确保至少指定一个"外部"接口和一个"内部"接口。还 应确保IP 地址在屏幕底部的表中得到了正确解析。如果 IP 地址错误,将从"包含"列表移至"可用" 列表,再移回"包含"列表以刷新表中的数据。

### 要移动接口:

1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"接口"选项卡。

- 在"外部接口(公共)"标题下,单击要从"可用"字段中移出的接口,然后单击"向右箭头", 将其移至"包含"字段。
- 3. 必要时,单击"向左箭头"将接口移回"可用"字段。
- 4. 根据需要,对"外部"或"内部"标题下的每个接口重复上述步骤。

# 定义的网络

网络定义通过 CIDR 格式的 IP 地址指示 IP 范围。子网地址/ID 是 IP 地址字段的相应值与用前缀 表示法表示的子网掩码相结合。

定义网络并将其与接口相关联是将单个 NAT 或防火墙规则应用于驻留在 IP 范围内的任意和所有 主机 IP 的有效方式。

**注**: 网络定义的创建有助于对 IP 范围内的主机进行分组,但并不是所有 NAT 和防火墙规则类型都需要创建网络定义。

例如, IP 地址为 192.168.0.2、子网掩码为 255.255.255.0 的主机属于 192.168.0.0 网络。使用前缀标记法表示子网掩码可有效标示网络地址的哪个部分是子网 ID、哪个部分代表子网内可能存在的所有主机。指定装置上的网络定义中 192.168.0.1-254 的 IP 范围最好使用 CIDR 格式地址 192.168.0.0/24。

这一过程可有效地将名称分配到 IP 范围或整个网络。NAT 和防火墙规则只取决于定义名称。 图 5.7: "网络"选项卡

Admin	Administration > Firewall and NAT						
S	SSH Reboot Shutdown						
Policy	icy Interfaces Hosts Networks Services						
	Add A Network Definition    Apply  Cancel						
	Name      Interface Name      IP Address (CIDR Format)						
	Defined Networks        Apply      Delete      Cancel						
		Name	Interface Name	IP Address (CIDR Format)			
		Sample	kvm	192.0.2.0/24			

### 要添加网络定义:

- 1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"网络"选项卡。
- 2. 在"名称"字段中, 输入网络定义的名称。
在"接口名称"字段中,输入接口名称,以及属于当前定义网络或具有当前定义网络访问权限的IP。名称必须与"接口"选项卡中列出的虚拟或物理接口之一相匹配。

注: 网络和接口名称都必须是介于3到40个字母数字字符之间的唯一名称。

- 4. 在"IP地址"字段中,输入 CIDR 格式的有效网络子网 ID。
- 5. 单击"应用"。

#### 要修改或删除定义的网络:

- 1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"网络"选项卡。
- 2. 在"定义的网络"标题下,勾选您要修改或删除的网络旁边的复选框。
- 3. 进行更改并单击"应用"。
  - 一或一

单击"删除",以删除该定义的网络。

## 主机

需要单独引用单个 IP/主机而不是与网络定义相关联的其他主机,或需要唯一地引用具有各自的 NAT 或防火墙规则的多个主机时,可在 NAT 和防火墙规则中使用主机定义。

这一过程能有效地将名称分配到 IP 地址,然后在 NAT 和防火墙规则中使用该名称。

默认情况下,主机列表将由连接到装置或装置搜索到的 SP 或 UMIQ 模块进行填充。您可以创建 新的主机条目来表示任意 IP,而不考虑设备。

注: 主机的创建有利于区分单个 IP, 但并不是所有的 NAT 和防火墙规则类型都需要。

图 5.8: "主机"选项卡
管理 > <u>防火</u>
SSH 重新启动 关机 关机
策略 接口 主机 网络 服务

添加用户定义的主机

添加主机

应用 取消	ſ		
主机名	IPv4 地	址	网络接口名称
	0.0.0.0		priv

#### UMG 定义的主机

主机名	IPv4 地址	网络接口名称
UMIQ-17-3E-2D	192.168.10.100	priv

#### 用户定义的主机

应用	取消删除		
	主机名	IPv4 地址	网络接口名称
	test1	192.168.0.10	priv

#### 要添加主机:

- 1. 在侧面导航栏中选择"网络"一"主机"。
- 2. 单击"添加"以添加新的主机。
- 输入代表主机的名称、IPv4 地址,以及可与该主机通信的物理或虚拟接口。然后单击"应用"。新主机定义将在"自定义主机"表中显示。

注: 网络接口必须是"接口"选项卡中列出的接口之一。

#### 要删除主机:

- 1. 在侧面导航栏中选择"网络"一"主机"。
- 2. 单击要删除的主机名, 然后单击"删除"。

## 服务

服务定义表示程序和网络按其 TCP/UDP 端口号或端口范围进行通信。服务定义对于端口的网络 地址转换 (PAT) 必不可少。PAT 使用单个外部 IP 和唯一的端口表示唯一的内部 IP/端口。

例如,如果两个不受支持的机架 PDU 连接到装置的专用端口,并分配有专用/内部 IP 地址,每个 PDU 都有一个 web 管理控制台,那么使用两个 NAT 规则就可允许外部管理员访问这些机架 PDU 的 web 管理界面。每个 NAT 规则会使用唯一的服务定义来代表装置公共/外部 IP 中的机架 PDU web 管理界面的 TCP 端口。例如 8080 的服务定义会针对第一个机架 PDU 转换为 80,8081 会针 对第二个机架 PDU 转换为 80。

IP 协议支持 65535 个端口,而互联网编号分配机构 (IANA) 为常用/周知 TCP 和 UDP 端口创建了登记表,这些端口代表了不同的程序和服务。在确定您想创建 NAT 和防火墙规则的应用程序或

流量使用哪些端口时,应查阅该登记表。一些应用程序并未向 IANA 登记其全部端口,而会在其 产品手册中特别纳入端口使用表。

默认情况下,装置有多个周知端口/端口范围定义为系统服务。这些服务大都包含在装置的默认 防火墙策略中,以便支持装置提供的各种特性。

注: 网络定义的创建对于粒度有必要,但不为所有类型的 NAT 和防火墙规则所必需。

#### 图 5.9: "服务"选项卡

管理 > 防火	<u> </u>				
SSH	重新启动	关机			
第略 接口	主机 网络	服冬			

添加服务定义

应用 取消				
服务名称	服务协议	服务地址	开始服务端口	结束服务端口
	TCP 🔻			

#### 系统服务

服务名称	服务协议	服务地址	开始服务端口	结束服务端口
srv-PING	icmp	any	0	0
srv-FTP-Data	tcp	any	20	20
srv-FTP-Commands	tcp	any	21	21
srv-SSH-Serial-Session	tcp	any	22	22
srv-Telnet-Session	tcp	any	23	23
srv-DHCPD	udp	any	67	68
srv-TFTP-Services	tcp	any	69	69
srv-UMG-Web-UI	tcp	any	80	80
srv-SNMP	udp	any	161	161
srv-SNMP-Traps	udp	any	162	162
srv-External-syslog	tcp	any	514	514
srv-Web-UI	tcp	any	443	443
srv-Modbus	tcp	any	502	502
srv-Adobe-Flex	tcp	any	843	843
srv-DS-View-proxy	tcp	any	1078	1078
srv-KVM-session	tcp	any	2068	2068
srv-Discovery-protocol	tcp	any	3211	3211

#### 要创建服务定义:

- 1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"服务"选项卡。
- 2. 在"服务名称"字段中,输入该服务要用的名称。

注: 服务名称可为 3-40 个字母数字字符。

- 3. 在"服务地址"字段,为服务输入有效的 CIDR 格式子网 ID。例如, 192.168.10.0/24。
- 为 IP 协议输入开始服务端口和结束服务端口。

注: 有效值为 0-65535。

5. 单击"应用"。新服务定义将显示到用户定义的服务定义表。

#### 要修改或删除用户定义的服务定义:

1. 单击侧面导航栏中的"防火墙和 NAT", 然后单击"服务"选项卡。

2. 在"户定义的服务"表中,勾选要修改或删除的服务旁的复选框。

- 3. 进行更改并单击"应用"。
  - 一或一

单击"删除",以删除该服务定义。

## 策略

管理员可通过 NAT 和/或防火墙策略控制流入、流出和流经装置的 IP 流量。

管理员可创建策略,允许外部主机或服务器直接与安全连接到装置专用端口的 IP 设备( 主机) 通信。NAT 或转发策略将允许流量绕过正常的身份验证和装置内置的权限安全性。建议仅在经 选择的少数情况下绕开安全性。

例如, 驻留在生产网络中的 SP 管理工具 (HP SIM) 可直接与连接到装置专用端口的 SP (iLO) 通信, 以便进行监控、配置和固件更新。但是用户会话不被允许绕开装置的安全性, 并且 SP 交互由基于装置的权限管理。这可通过允许管理工具访问 SP 的简单 NAT 或 IP 转发策略规则实现。此外, 防火墙过滤规则会阻止用户使用由管理工具使用的 NAT/转发规则。

应使用以下标准在 NAT 规则或 IP 转发规则之间做出决定,以提供对专用主机的绕过访问。IP 转发规则要求专用 IP 网络/子网相对于其他生产网络,甚至装置的其他专用网络具有唯一性。如果与两个装置的专用端口/主机相关联的 IP 网络完全相同,那么当外部主机尝试将流量发送给其中一个装置的专用主机时,无法在这两个装置中做出正确的路由选择。NAT 规则的优势在于多个装置的专用端口/主机可以具有相同的 IP 网络/子网,而不会产生相同的路由冲突。装置支持两种形式的 NAT: 1-to-1 NAT(IP 伪装) 和端口地址转换(PAT/NAT overload)。

对于利用 IP 转发策略规则成功进行的端到端通信,专用主机必须将最近的装置 IP 作为其网关, 且所有外部主机必须具有引用专用网络/子网和最近的装置 IP 的路由(静态或动态)。

注: 此处的"最近"是指属于相同网络的 IP,或不同网络中最近的可路由 IP。

#### NAT 流

进入接口(流入)的流量会在应用任何过滤规则和做出任何路由决策前,根据 NAT 规则进行转换。退出接口(流出)的流量会在应用过滤规则和做出路由决策后,根据 NAT 规则进行转换。

#### 图 5.10: NAT 流



#### 表 5.17: NAT 流说明表

编号	说明
1	外部。
2	内部。
3	内部接口上的流入 NAT。
4	外部接口上的流入 NAT。
5	内部接口上的流出 NAT。
6	外部接口上的流出 NAT。

## 防火墙流

进入装置(输入)的流量在通过 NAT 规则和路由决策后,受到过滤规则限制。退出装置(输出)的流量在做出路由决策和 NAT 规则执行任何转换前,受到过滤规则限制。

#### 图 5.11: 防火墙流



#### 表 5.18: 防火墙流说明表

编号	说明
1	外部。
2	内部。
3	内部接口上的输入过滤。
4	外部接口上的输入过滤。
5	内部接口上的输出过滤。
6	外部接口上的输出过滤。

#### 防火墙和 NAT 流

流经装置的预期已经过转换和过滤的流量,将需要同时应用设计用于与流量模式适当匹配的 NAT和防火墙规则。流量进入装置时,先进行转换再进行过滤;流量退出装置时,先进行过滤 再进行转换。

例如,如果输入流量通过了已转换目的地地址的流入 NAT 规则,那么过滤规则与目的地地址相匹配的唯一方法是使过滤规则与经转换的目的地地址模式相匹配,而不是与流量的原始目的地地址相匹配。这是由于地址在过滤前先进行了转换。

#### 图 5.12: 防火墙和 NAT 流



#### 表 5.19: 防火墙和 NAT 流说明

编号	说明
1	外部。
2	内部。
3	外部接口上的输出过滤前内部接口上的流入 NAT。
4	内部接口上的输出过滤前外部接口上的流入 NAT。
5	内部接口上的流出 NAT 前同一内部接口上的输出 过滤。
6	外部接口上的流出 NAT 前同一外部接口上的输出过滤。
7	内部接口上的输入过滤前同一内部接口上的流入 NAT。
8	外部接口上的输入过滤前同一外部接口上的流入 NAT。

## NAT 设置

管理员可添加或配置 NAT 策略,以进行地址转换。根据环境和装置中的路由,可能有必要在流量流入 (pre-routing) 或流量流出 (post-routing) 时进行 NAT 设置。

表 5.20:N	AT 设置定义
参数	定义
方向	流入/出执行 NAT 的接口的流量方向。
顺序	从顶部到底部,流量被比作寻找模式匹配的 NAT 策略的条目。
接口	进行流量模式匹配检查及执行 NAT 的接口。
源	此处列举的源主机/网络会进行流量模式匹配检查。
目的地	此处列举的目的地主机/网络会进行流量模式匹配检查。
服务	此处列举的服务会进行流量模式匹配检查。
转换的源	替换流量中显示的源值的符合此 NAT 策略模式的主机/接口地址。如果不想转换目的地地址,那 么在此字段中输入"any"。
转换的目 的地	替换流量中显示的目的地值的符合此 NAT 策略模式的主机/接口地址。如果不想转换目的地地 址,那么在此字段中输入"any"。
转换的服 务	替换流量中显示的值的符合此 NAT策略模式的目的地服务(TCP/UDP端口)。如果不想转换目的地端口,那么在此字段中输入"any"。

#### 要添加 NAT 策略:

- 1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"策略"选项卡。
- 2. 在"NAT 设置"部分的"添加 NAT 策略"标题下,您可以使用下拉菜单选择"方向"字段下的"出 站"或"入站"来添加 NAT 策略。
- 3. 输入以下内容的有效名称:"接口"、"源"、"目的地"、"服务"、"转换的源"、"转换的目的地" 和"转换的服务"。

注: 有效名称必须为3到40个字母数字字符。

- 4. 使用下拉菜单激活或取消激活"规则状态"。
- 5. 单击"应用"。新 NAT 策略将在"已定义的 NAT 策略"标题下显示。

#### 要修改或删除 NAT 策略:

- 1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"策略"选项卡。
- 2. 在"已定义的 NAT 策略"标题下,勾选要编辑或删除的策略旁的复选框。
- 3. 在要编辑的行内进行更改,并单击"应用"。

一或一

单击"删除"以删除该策略。

#### 防火墙设置

默认情况下,装置中会预填充支持装置功能的系统定义的防火墙策略规则。管理员可创建其他 防火墙策略规则,以便放宽或增强装置的默认安全状态。

#### 表 5.21: 防火墙设置定义

参数	定义
方向	流入/出执行 NAT 的接口的流量方向。
顺序	从顶部到底部,流量被比作寻找模式匹配的 NAT 策略的条目。
接口	进行流量模式匹配检查及执行 NAT 的接口。
源	此处列举的源主机/网络会进行流量模式匹配检查。

参数	定义
目的地	此处列举的目的地主机/网络会进行流量模式匹配检查。
服务	此处列举的服务会进行流量模式匹配检查。
操作	要对符合此规则模式的流量执行的操作。
连接状态	此规则将应用于与所选连接状态类型相匹配的流量。 - 不需要:流量与任何已知连接均不相关。 - 新建:流量已启动新连接,或与两个方向都尚无数据包的连接相关联。 - 已建立:流量与两个方向都有数据包的连接相关联。 - 已关联:流量正在启动新连接,但与现有连接相关联,例如FTP数据传输或ICMP错误。
规则状态	定义规则状态是否为活动。

#### 要添加防火墙策略:

- 1. 单击侧面导航栏中的"防火墙和 NAT",然后单击"策略"选项卡。
- 在"防火墙设置"部分中,使用"添加防火墙策略"标题下的下拉菜单选择"方向"下的"输入"、"输出"或"转发"。
- 3. 输入以下内容的有效名称:"顺序"、"接口"、"源"、"目的地"和"服务"。

注: 有效名称必须为3到40个字母数字字符。

- 4. 使用下拉菜单选择"操作"、"连接状态"和"规则状态"。
- 5. 单击"应用"。

对于每个规则,都必须从"策略"下拉菜单中选择一项操作("接受"、"放弃"、"拒绝"或"记录")。所选操作将在与规则中指定的所有标准相匹配的 IP 包上执行。

如果从下拉菜单中选择"记录",将在 syslog 中为符合此规则的流量创建条目,而不会执行具体的"接受"、"拒绝"或"放弃"操作。要记录并"接受"或记录并"拒绝"/"放弃",另一条规则必须遵循 具有相同流量模式和所需"接受"、"拒绝"、"放弃"操作的记录规则。管理员可配置日志等级、日 志前缀,以及是否在"日志选项"部分记录 TCP 序列、TCP 选项和 IP 选项。

如果从下拉菜单中选择"拒绝",管理员可从具有下拉菜单的"拒绝"中选择一个选项;丢弃数据包 并发送所选类型的回复包。

#### 要修改或删除防火墙策略:

- 1. 单击侧面导航栏中的"防火墙和 NAT", 然后单击"策略"选项卡。
- 2. 在"自定义防火墙策略"标题下,勾选要编辑或删除的策略旁的复选框。
- 3. 进行更改并单击"应用"。

一或一

单击"删除"以删除该策略。



登录装置时,"目标"选项卡是默认视图。"目标"选项卡视图包括侧面导航栏和"目标"表。

注: 要执行本部分的操作,请先单击选项卡栏中的"目标"。

#### 图 6.1: "目标"选项卡

目标 传恩器 事件 管理									
■ 「「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」	目标 > 装置								
▼合装置	名称	编口	类型	状态	拓扑图	IP 地址	电源操作	远程访问	
▶ 🗀 服务处理器	15-78-C6_12.0.1.10	0	服务处理器	己加电	0	12.0.1.10	选择电源 ▼	SP 会话	
UMIQ-17-3E-2D	15-78-C6_12.0.1.100	0	服务处理器	己加电	0	12.0.1.100	选择电源 ▼	SP 会话	
	15-78-C6_12.0.1.101	0	服务处理器	已加电	0	12.0.1.101	选择电源 ▼	SP 会话	
<b>1</b> 5-78-c6-p-2	15-78-C6_12.0.1.102	0	服务处理器	己加电	0	12.0.1.102	选择电源 ▼	SP 会话	
▼  PDU  15.70 of P1 1	15-78-C6_12.0.1.103	0	服务处理器	己加电	0	12.0.1.103	选择电源 ▼	SP 会话	
■ 19-78-CDF1_1 ▼ □申源插座	15-78-C6_12.0.1.104	0	服务处理器	己加电	0	12.0.1.104	选择电源 ▼	SP 会话	
<b>1</b> 5-78-c6P1_1_1	15-78-C6_12.0.1.105	0	服务处理器	己加电	0	12.0.1.105	选择电源 ▼	SP 会话	
15-78-c6P1_1_10	15-78-C6_12.0.1.106	0	服务处理器	己加电	0	12.0.1.106	选择电源 ▼	SP 会话	
<b>15-78-c6P1_1_2</b>	15-78-C6_12.0.1.107	0	服务处理器	己加电	0	12.0.1.107	选择电源 ▼	SP 会话	
15-78-c6P1_1_3	15-78-C6_12.0.1.108	0	服务处理器	己加电	0	12.0.1.108	选择电源 ▼	SP 会话	
<b>1</b> 15-78-c6P1_1_5	15-78-C6_12.0.1.109	0	服务处理器	己加电	0	12.0.1.109	选择电源 ▼	SP 会话	
<b>15-78-c6P1_1_6</b>	15-78-C6_12.0.1.11	0	服务处理器	己加电	0	12.0.1.11	选择电源 ▼	SP 会话	
15-78-c6P1_1_7	15-78-C6_12.0.1.110	0	服务处理器	己加电	0	12.0.1.110	选择电源 ▼	SP 会话	
15-78-66P1_1_8	15-78-C6_12.0.1.111	0	服务处理器	已加电	0	12.0.1.111	选择电源▼	SP 会话	
	15-78-C6_12.0.1.112	0	服务处理器	己加电	0	12.0.1.112	选择电源▼	SP会话	
	15-78-C6_12.0.1.113	0	服务处理器	己加电	0	12.0.1.113	选择电源 ▼	SP 会话	
	15-78-C6_12.0.1.114	0	服务处理器	己加电	0	12.0.1.114	选择电源 ▼	SP 会话	

#### 表 6.1: "目标"选项卡说明

编号	说明
1	侧面导航栏
2	目标表

通过侧面导航栏,您可以访问装置及其相关联的目标。通过"目标"表,您可以查看关于目标的信息,并打开与目标的会话。可根据列标题对"目标"表进行排序,并根据首选项调整各个列宽的大小。用户注销时,自定义内容将恢复为默认设置。根据所做选择,可通过三种格式查看目标:列表视图、组视图或类型视图:

- 列表视图是在父装置节点下分组的目标的平面列表。选择装置列表项将显示"目标摘要"屏幕。
- 类型视图显示所有按目标类型分组的目标。
- 组视图仅显示定义的目标组及其内容。不在组中的目标将不可见。分属多个组的目标将显示在 每个组中。组视图显示"管理"选项卡中已创建的目标组。

表 6.2: 状态说明	
状态值	说明
使用中	会话处于活动状态
正在升级	会话正在升级
加电	一个或多个插座处于正在打开的过程中
断电	目标正在关闭
无电源	未检测到电源
局部电源	目标的插座部分处于打开状态,部分处于关闭状态
锁定关闭	一个或多个插座在关闭位置被锁定
已断电	已关闭一个或多个插座
锁定打开	一个或多个插座在打开位置被锁定
空闲	无活动会话
己加电	插座己打开
未知	无可用状态

注: 如果应用了过滤器,将仅显示与目标匹配的状态。

## 服务处理器

您可以在"目标"选项卡下查看可用服务处理器及其相关联的装置。单击侧面导航栏中的"服务处 理器"可查看和/或修改其配置设置。

## 属性

单击"属性"选项卡可查看服务处理器的常规信息和 FRU 信息。

## 系统

通过"系统"选项卡,您可以查看托管目标设备的电源状态和指示器 LED(如可用)的状态、管理 电源、远程打开和关闭 LED,以及查看和控制时间设置。

#### 要查看和控制电源状态:

- 1. 单击 SP 名称。
- 2. 单击"系统"选项卡。将出现系统信息窗口,并显示目标设备的当前电源状态。
- 3. 从下拉列表,选择所需的电源操作。
- 4. 单击"应用"。

#### 要查看和控制 SP 的指示器 LED:

- 1. 单击 SP 名称。
- 2. 单击"系统"选项卡。将出现"系统信息"窗口,目标设备的当前机箱 LED 状态将在"机箱"标题 下显示。
- 3. 要更改目标设备的指示器状态,请完成以下任意步骤:

要打开 LED 并在指定的秒数内使其保持闪烁状态,请单击"指示器闪烁"旁的按钮,然后在"秒"字段输入秒数。

一或一

要打开 LED 并使其保持闪烁,单击"指示器打开"旁的按钮。

一或一

要关闭 LED, 单击"指示器关闭"旁的按钮。

4. 单击"应用"。"指示器状态"将反映您进行的变更。

#### 要查看和控制时间设置:

- 1. 单击 SP 名称。
- 2. 单击"系统"选项卡。
- 3. 选择"与装置同步"或"与客户端 PC 同步",并单击"应用"。

## 会话

从"会话"选项卡可与装置上的 SP 建立会话。"会话"页面显示的按钮因 SP 的功能和查看该页面用 户的权限而异。要启动会话,单击您所需会话类型的相应按钮。如果用户不具有操作权限,或 SP 不支持该操作,那么该操作的相应按钮将显示为灰色。

访问"会话"页面有两种方式。第一种是在"目标"选项卡中单击"装置",然后单击"远程访问"下的"SP 会话"链接。

and the second s	trellis Avocent Universal Management Gateway										
目标 後感器 事件 管理											
显示【类型】	目标 > <u>装置</u>										
▼□装置	名称	端口	类型	状态	拓扑图	IP 绝址	电源操作	远程访问			
▼ 🗁 服务处理器	15-78-C6_12.0.3.104	0	服务处理器	己加电	0	12.0.3.104	选择电源▼	SP 会话			
<b>15-78-C6_12.0.1.0</b>	15-78-C6_12.0.1.1	0	服务处理器	己加电	0	12.0.1.1	选择电源 ▼	SP 会话			
15-78-C6_12.0.1.1 15-78-C6_12.0.1.10	15-78-C6_12.0.1.10	0	服务处理器	己加电	0	12.0.1.10	选择电源 ▼	SP 会话			
	15-78-C6_12.0.1.100	0	服务处理器	己加电	0	12.0.1.100	选择电源▼	SP 会话			
▶ 🗋 串行控制台	15-78-C6_12.0.1.101	0	服务处理器	己加电	0	12.0.1.101	选择电源▼	SP 会话			
▶ 🧰 PDU	15-78-C6_12.0.1.102	0	服务处理器	己加电	0	12.0.1.102	→ 送择电源	SP 会话			
▶ 🗀 电源插座	15-78-C6_12.0.1.103	0	服务处理器	己加电	0	12.0.1.103	→ 送择电源	SP 会话			
1	15-78-C6_12.0.1.104	0	服务处理器	己加电	0	12.0.1.104	→ 送择电源	SP 会话			
In the second	15-78-C6_12.0.1.105	0	服务处理器	己加电	0	12.0.1.105	→ 送择电源	SP 会话			
	15-78-C6_12.0.1.106	0	服务处理器	己加电	0	12.0.1.106	选择电源▼	SP 会话			
	15-78-C6_12.0.1.107	0	服务处理器	己加电	0	12.0.1.107	选择电源▼	SP 会话			

### 图 6.2: "会话"页面访问

第二种是在侧面导航栏中单击一个 SP, 然后单击"会话"选项卡。

図 C2 "今迁"页面注词 2

图 0.3: 云语 贝国的问	2					
目标 传感器 事件 管理						
显示 _类型▼_	目标 > 1	5 <u>-78-C6 12.0.1.1</u> 	重昌电源			
▼ 🗁 装置	属性 系	统 SEL 会话 电源 传感器	路 日志 警告			
▼ 合服务处理器 ■ 15-78-C6_12.0.1.0	启动会话	871 at 00 jun dal 75 . 1071 at 7	<b>5</b> W			
<b>1</b> 5-78-C6_12.0.1.1		服务每控制管:图形	虚拟 KVM 媒体	(E)th		
		服务处理器:Web 服务处理器:CII	SOL SOL SOL SOL	LID史 浏览器 SSH Tel	net	
▶ 🤮 単行弦制音 ▶ 🤐 PDU	目标会话		CON HIMLEN			
▶ 🗀 电源插座		删影余				
	. E	开始时间	上次时间	用户	目标	类型
	"					

如果您有相应权限,也可查看或删除任何目标会话。

#### 要删除会话:

- 1. 在"会话"页面,勾选要删除的会话旁的复选框。
- 2. 单击"删除"。

### SEL

"SEL"选项卡显示从服务处理器返回的所有 SEL 条目。

## 电源

单击"电源"选项卡可查看目标设备的功耗信息。单击"刷新"可刷新功耗信息。

### 传感器

单击"传感器"选项卡可查看目标设备的传感器信息。单击"刷新"可刷新传感器信息。

日志

单击"日志"选项卡可下载或清除日志文件历史。

## 警告

单击"警告"选项卡可启用和配置目标设备的 SNMP 警告目的地。通过此屏幕,您可以更改警告的 群组名和 IP 字段。

注: 屏幕选项因 SP 的功能而有所不同。

## UMIQ 模块

您可以在"目标"选项卡下查看可用的 UMIQ 模块。单击侧面导航栏中的 UMIQ 可查看其设置。单击"连接"可打开与所选 UMIQ 的 KVM 会话。

#### 要查看可用的 UMIQ:

1. 单击侧面导航栏中的"UMIQ",然后单击目标以查看其状态和电源状态。

2. 单击"连接",打开与目标的 KVM 会话。

## 串行控制台

您可以在"目标"选项卡下查看可用的串行目标。

#### 要查看可用的串行目标:

- 1. 单击侧面导航栏中的"串行控制台",然后单击目标以查看属性和日志。
- 2. 单击"连接",打开与目标进行的串行会话。
- 3. 单击"属性",查看目标的属性。
- 4. 单击"日志",查看目标的日志文件。您还可以从此屏幕下载和清除日志文件。

#### PDU

每个 PDU 及其相关联的插座都列在"目标"选项卡下。单击侧面导航栏中的 PDU 可查看和/或修改 其配置设置。关于 PDU、电路和插座的只读信息,请查看以下选项卡:"属性"、"插座"、"概 述"、"电流"、"电压"、"功耗"、"能耗"和"环境"。要修改插座、PDU、相位、电路或环境的配 置,请单击"设置"选项卡。

#### 属性

#### 要管理 PDU:

- 1. 单击要管理的 PDU。
- 2. 单击"开"、"关"、"重启"、"重新启动"、"重设硬件过电流保护"或"恢复出厂默认值"。

注: 电源控制(开、关和重启)将应用于 PDU 的所有插座。

3. 单击"应用"。

#### 插座

通过选择"插座"选项卡,您可以查看插座的状态、数量和名称,还可以打开、关闭、重启、锁定 和解锁所选插座。

#### 要管理插座:

- 1. 单击 PDU 以管理其插座。
- 2. 单击"插座"选项卡。
- 3. 勾选插座名称旁边的复选框。
- 4. 单击"开"、"关"、"重启"、"锁定"、"解锁"或"保存状态"按钮。

#### 概述

通过选择"概述"选项卡,您可以查看 PDU 的名称、插座、电流、电压、功率、功率因数、能量 和警报。

#### 电流

通过选择"电流"选项卡,您可以重设最大、最小和平均电流值。

#### 要重设值:

- 1. 选择要重设的 PDU 和/或插座。
- 2. 单击"重设值"。

#### 电压

通过选择"电压"选项卡,您可以重设最大、最小和平均电压值。

#### 要重设值:

- 1. 选择要重设的 PDU 和/或插座。
- 2. 单击"重设值"。

#### 功耗

通过选择"功耗"选项卡,您可以重设最大、最小和平均功耗值。

#### 要重设值:

- 1. 选择要重设的 PDU 和/或插座。
- 2. 单击"重设值"。

#### 能耗

通过选择"能耗"选项卡,您可以重设平均能耗值。

#### 要重设值:

- 1. 选择要重设的 PDU 和/或插座。
- 2. 单击"重设值"。

#### 环境

通过选择"环境"选项卡,您可以重设最大、最小和平均温度值。

#### 要重设值:

1. 选择要重设的 PDU 和/或传感器。

2. 单击"重设值"。

#### 设置

通过选择"设置"选项卡,您可以查看和更改插座、PDU、相位、电路和环境的设置。

#### 要配置插座设置:

- 1. 选择要管理的 PDU。
- 2. 单击"设置"选项卡。
- 3. 单击"插座"。
- 选择要配置的插座并单击"编辑"。您可以更改"加电后延迟"、"断电后延迟",以及"高关键"、"高警示"、"电流低警示"和"低关键"阈值。
- 5. 完成后单击"保存"。

#### 要配置 PDU 设置:

- 1. 选择要管理的 PDU。
- 2. 单击"设置"选项卡。
- 3. 单击"PDU"。
- 4. 选择要配置的 PDU 并单击"编辑"。您可以配置"冷启动延迟",以及"高关键"、"高警示"、"低警示"和"低关键"阈值。
- 5. 完成后单击"保存"。

#### 要配置相位设置:

- 1. 选择要管理的 PDU。
- 2. 单击"设置"选项卡。
- 3. 单击"相位"。
- 选择要配置的相位并单击"编辑"。您可以配置"高关键"、"高警示"、"低警示"和"低关键"阈值。
- 5. 完成后单击"保存"。

#### 要配置电路设置:

- 1. 选择要管理的 PDU。
- 2. 单击"设置"选项卡。
- 3. 单击"电路"。
- 选择要配置的电路并单击"编辑"。您可以配置"高关键"、"高警示"、"低警示"和"低关键"阈值。
- 5. 完成后单击"保存"。

#### 要配置环境设置:

- 1. 选择要管理的 PDU。
- 2. 单击"设置"选项卡。
- 3. 单击"环境"。
- 选择要配置的传感器并单击"编辑"。您可以配置传感器的名称、单位,以及"高关键"、"高警示"、"低警示"和"低关键"阈值。
- 5. 完成后单击"保存"。



# 传感器和事件

## 传感器

通过"传感器"选项卡,您可以查看连接到装置的外部传感器的名称、值、时间和位置。此外,您还可以查看数字输入的类型和警告。

## 事件

装置将为各种事件生成通知和警告。装置上发生事件时,事件将保存在事件日志中。如果您是管理员,您可以通过单击"事件摘要"选项卡查看或清除时间,或单击"警告摘要"选项卡查看和清除警告。操作员可以查看事件或警告,但不能将其清除。

清除事件会将它从装置日志中移除。可同时选择列表中的多个事件并将其清除。发生的事件的历 史记录将保留在"事件摘要"选项卡中。清除活动警告会将所有相关联的数字输出重设为非活动状态。

#### 表 7.1: 警告默认阈值

警告	默认阈值
风扇	5000 RPM*
温度(前部传感器)	大于 50℃*
温度(后部传感器)	大于 66℃*
电源	关闭*
CPU	大于 98%
数据分区	大于 90%
*默认设置为硬编码。	

### 风扇

如果风扇未运行,或降至硬编码阈值以下,您将收到风扇警告。

## 温度

如果温度升至硬编码阈值以上,您将收到温度警告。 前部温度传感器位于前面板上,还有两台位于后面板上。

## 电源

电源传感器显示电源是关闭还是打开。如果最初插入了两根电源线,拔出其中一根时您将收到警告。如果最初只插入了一根电源线,你将不会收到警告。

## CPU 和磁盘使用

CPU 和磁盘使用是系统警告。

# 附录 A: 技术规格

发 <b>入:</b> 设不成 类别	Ħ
自动检测端口	
编号	8或40
连接器	RJ-45
尺寸	
形态因数	1U机架,可安装
长x深x高	50.8 厘米 x43.41 厘米 x4.32 厘米
重量(不包括 缆线)	6.44 千克
SETUP 端口	
数量	1
类型	串行
连接器	RJ-45
本地端口	
数量/类型	1/DB15
网络连接	
数量	2
类型	10/100/1000 以太网
连接器	RJ-45
USB 设备端口	
数量	4
类型	USB 2.0
电源规格	
连接器	2
类型	IEC
电源	
交流输入范围	100-240 VAC
交流频率	50/60 Hz
交流输入电流 额定值	2A
环境大气状况额	质定值
温度	0-50°C
湿度	20%至 85%,非凝结
安全及电磁兼 容标准、认证 和标志	本产品获得的安全认证及电磁兼容认证使用以下一个或多个标记: CMN( 证书型 号) 、MPN( 厂商部件号) 或"销售级别型号"标记。电磁兼容和/或安全报告及证书中引用 的标记打印在产品粘贴的标签上。

# 附录 B: 忘记密码

如果所有管理员帐户都被锁定,请联系技术支持部门并提供装置序列号。技术支持部门将提供一个密钥,以将装置重设为使用默认帐户的出厂默认值。

## 附录 C: 从网络启动

如果您的装置出现问题,可执行"Netboot恢复"并加载新的出厂默认装置固件,或将之前保存的备份映像文件恢复到装置中。

"Netboot恢复"文件可从 Avocent 技术支持获取。该文件必须放到 FTP 服务器上才能使"Netboot恢复"进程起作用。备份映像文件也可作为"Netboot恢复"文件放到 FTP 服务器上。

#### 要执行"Netboot恢复":

- 1. 打开或重新启动装置。
- 2. 选择"Netboot恢复"。
- 3. 输入 udhcpc 以通过 GB1 (eth0) 请求装置的 DHCP 地址。
  - 一或一

如果需要将静态 IP 分配到 GB1 (eth0) 或 GB2 (eth1), 请输入以下命令:

NETBOOT> ifconfig eth<x> <IP 地址> NETBOOT> route add default gw <网关 ip> eth<x>

6. 向装置分配 IP [和可选网关]后,可通过输入以下命令下载固件:
 NETBOOT> nboot ftp://<用户名>:<密码>@<ftp 服务器>/<路径/文件名>。

## 附录 D: 创建 SP 文件

要将服务处理器列表导入装置,必须先创建一个包含 SP 的文件。文件的每一行必须为以下格式: IP:端口:用户名:密码:配置。对要添加到列表中的每个 SP 重复使用此格式。语法说明请参阅表 D.1。

必须使用冒号分隔各个参数。如果用户名或密码使用了冒号,必须将整个用户名或密码放到引号中。

下面举例说明了有效的 SP 文件格式:

#这是有效 SP 文件格式的示例

192.168.200.154:0:root:calvin:drac5

192.168.10.130:0:admin:"pass:word":ilo2

## 表 D.1: SP 文件格式

参数	说明
#	用于在需要时添加评论。如果您添加评论,必须输入#作为评论行的第一个字符。
IP	SP目标的 IP地址。
端口	当前未使用。为此参数输入 0。
用户名	SP的管理员名称。
密码	SP的管理员密码。
配置	SP的类型。如果 SP类型未知,则输入*。

#### 表 D.2: 动态属性说明

端口	说明
22	SSH端口是否打开并侦听连接?
23	Telnet端口是否打开并侦听连接?
80	该 SP 是否有 Web 接口 (HTTP)?
443	该 SP 是否有安全 Web 接口 (HTTPS/SSL)?

#### 表 D.3: 支持的 SP

SP 类型	SP 类型	SP 类型
ipmi 1.5	ilo4	rsa_II
ipmi 2.0	ilo3	cisco_us
idrac7	ilo2	fsc_irmc
idrac6	ilo	fsc_irmc_II
drac5	elom	m1000e_cmc
dell_10g	ilom	drac_mc
drac4	alom	hp_blade system
	generic	blade_center

## 附录 E: 对 SP 进行故障排除

如果您无法搜索或手动添加 SP, 请尝试以下方法:

- 确认在服务器的 BIOS 中启用了 SP。
  - 某些 SP 设置存储于主 BIOS 中 <F2> 或 <DEL>。
  - 某些 SP 设置存储于备用 BIOS 中 <ctrl+D><ctrl+E><F8>。
  - 某些 SP 设置同时存储于主 BIOS 和备用 BIOS 中。
- 如果 SP 通过物理连接与装置或网络相连,请确保 SP 使用的是专用接口。
- 如果要对 SP 进行逻辑管理,请确保 SP 与 NIC1 共享或共用边带。
- 确保用户名和密码配置正确。
- 访问 SP BIOS 并重设密码以确保凭据的准确性。
- 确保 SP 分配了适当的 IP 地址。
- 确保装置和 SP 处于或可访问同一网络。
- 网络必须与 SP 的 IP 地址相匹配,并且必须能将 SP 路由到装置所连接的网络。这通常可以使用装置命令 shell 的 ping 命令进行测试。
  - 如果您无法 ping SP,则 SP 可能仅允许通过 IPMI 进行通信。如果用户名/密码和网络路由都正确,装置将能与仅允许 IPMI 的 SP 通信。
- DHCP 以请求-应答的方式运作。SP 必须先请求 DHCP 地址,装置才能提供该地址。许多 SP 即使已关闭,或缆线已断开连接并重新连接,仍会保留分配的 DHCP IP 地址。解决这一问题的最佳方法就是强制 SP 使用静态 IP 地址(保存/重新启动),然后在连接到装置时将它重设为 DHCP。这会促使 SP 向装置请求地址,这样装置即可搜索 SP。
- 如果 SP 可访问且用户名/密码是正确的,请确认 SP 中的 IPMI(或 Telnet/SSH,视情况而定) 是否启用,或是否将 IPMI 分配到适当的 NIC 接口。在装置发行说明中确认所需的 SP 通信协议和固件版本。

# 附录 F: 视频分辨率

下表列出了 UMIQ 模块的 EDID 支持的视频分辨率。

表 F.1: 支持的视频分辨率

视频 分辨率	标准	宽屏	标准 1024 x 768	标准 1280 x 1024	标准 1600 x 1200	宽屏 1280 x 800	宽屏 1680 x 1050	宽屏 1920 x 1080
640 x 400 @ 60 Hz	x	x	x	x	x	x	x	
640 x 480 @ 60 Hz	x	x	x	x	x	x	x	
640 480 @ 67 Hz	x	x	x	x	x	x	x	
640 x 480 @ 72 Hz	x	x	x	х	x	x	x	
640 x 480 @ 75 Hz	x	x	x	x	x	х	x	
704 x 528 @ 60 Hz	x	x	x	х	x	х	x	
704 x 528 @ 72 Hz	x	x	x	х	x	х	x	
720 x 400 @ 70 Hz	x	x	x	х	x	х	x	
720 x 400 @ 88 Hz	x	x	x	х	х	х	х	
720 x 480 @ 60 Hz	x	x	x	х	х	х	х	
768 x 576 @ 60 Hz	x	x	x	х	x	х	x	
768 x 576 @ 72 Hz	x	x	x	х	x	х	x	
800 x 500 @ 60 Hz	x	x	x	х	x	х	x	
800 x 600 @ 56 Hz	x	x	x	х	x	х	x	
800 x 600 @ 60 Hz	x	x	x	х	x	х	x	
800 x 600 @ 72 Hz	x	x	x	х	x	х	x	
800 x 600 @ 75 Hz	x	x	x	х	x	х	x	
832 x 624 @ 75 Hz	x	x	x	х	x	х	x	
853 x 480 @ 60 Hz	x	x	x	х	x	х	x	
896 x 672 @ 60 Hz	x	x	x	х	x	х	x	
896 x 672 @ 75 Hz	x	x	x	х	x	х	x	
896 x 672 @ 85 Hz	x	x	x	х	x	х	x	
960 x 720 @ 60 Hz	x	x	x	х	x	х	x	
960 x 720 @ 75 Hz	x	x	x	х	x	х	x	
960 x 720 @ 85 Hz	x	x	x	х	x	х	x	
1024 x 640 @ 60 Hz	x	x	x	х	x	х	x	
1024 x 640 @ 75 Hz	x	x	x	х	х	х	х	
1024 x 768 @ 60 Hz	x*	x	x*	x*	x*	х	x	
1024 x 768 @ 70 Hz	x	x	x	х	x	х	x	
1024 x 768 @ 75 Hz	x	x	x	х	x	х	x	
1024 x 768 @ 85 Hz	x	x	x	х	x	х	x	
1024 x 768 @ 87 Hz	x	x	x	x	x	x	x	
1152 x 864 @ 60 Hz	x	x		x	x	x	x	
1152 x 864 @ 70 Hz	x	x		x	x	х	x	
1152 x 864 @ 75 Hz	x	x		x	x	х	x	
1280 x 720 @ 60 Hz	x	х		x	x	x	x	

视频 分辨率	标准	宽屏	标准 1024 x 768	标准 1280 x 1024	标准 1600 x 1200	宽屏 1280 x 800	宽屏 1680 x 1050	宽屏 1920 x 1080
1280 x 720 @ 70 Hz	х	x		х	х	х	х	
1280 x 720 @ 75 Hz	х	x		х	х	х	х	
1280 x 720 @ 85 Hz	х	x		х	х	х	х	
1280 x 768 @ 60 Hz	х	x		х	х	х	х	
1280 x 800 @ 60 Hz	x	x		х	х	x*	x*	
1280 x 800 @ 75 Hz	х	x		х	х	х*	х*	
1280 x 960 @ 60 Hz	х	x		х	х		х	
1280 x 960 @ 75 Hz	х	x		х	х		х	
1280 x 1024 @ 60 Hz	х	x		х	х		х	
1280 x 1024 @ 75 Hz	х	x		х	х		х	
1360 x 768 @ 60 Hz	х	x			х		х	
1365 x 768 @ 60 Hz	х	x			х		х	
1400 x 1050 @ 60 Hz	х	x			х		х	
1400 x 1050 @ 72 Hz	x	x			х		х	
1400 x 1050 @ 75 Hz	x	x			х		х	
1400 x 1050 @ 85 Hz	x	x			х		х	
1440 x 900 @ 60 Hz	x	x*			х		х	
1440 x 900 @ 75 Hz	x	x*			х		х	
1600 x 900 @ 60 Hz	х	x			х		х	
1600 x 900 @ 75 Hz	х	x			х		х	
1600 x 900 @ 85 Hz	x	x			х		х	
1600 x 1200 @ 60 Hz	x	x			Х*		х	
1680 x 1050 @ 60 Hz	x	x					X*	
1920 x 1080 @ 60 Hz	x	x						x*

注: \*表示首选/默认分辨率。

## 附录 G: 技术支持

如果您在 Avocent 产品的安装或操作中遇到任何问题,我们的技术支持人员将为您提供帮助。如果发生问题,请按下列步骤尽快取得服务。

#### 解决问题:

- 1. 查看此手册中相关的章节,确定此故障是否能通过所列的操作步骤得到解决。
- 2. 访问 www.avocent.com/support,并利用以下资源之一:

搜索知识库或使用在线服务请求。

一或一

选择"Technical Support Contacts",查找离您最近的 Avocent 技术支持部所在地。

