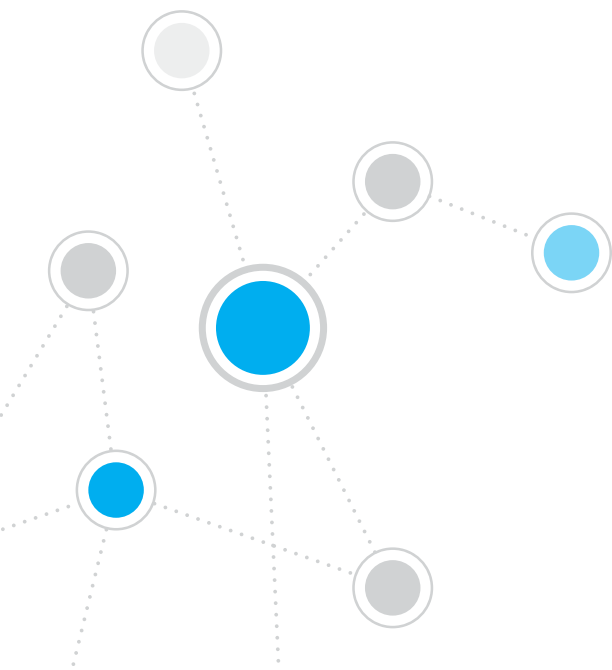




ForeScout CounterACT[®] 7

单一 CounterACT 设备

快速安装指南



目录

欢迎使用 ForeScout CounterACT® 7 版.	3
CounterACT 包装内容物	3
概述	4
1. 制定部署计划	5
决定设备部署位置	5
设备界面连接	5
2. 设置交换机	8
A. 交换机连接选择	8
B. 交换机设置说明	9
3. 连接网线并开机	10
A. 拆除包装并连接缆线	10
B. 记录界面分配	11
C. 打开设备电源	11
4. 配置设备	12
许可证	14
网络连接要求	14
5. 远程管理	15
iDRAC 设置	15
将模块连接至网络	18
登录 iDRAC	18
6. 验证连接情况	19
验证管理界面连接	19
验证交换机/设备连接情况	19
执行 Ping 测试	20
7. 设置 CounterACT 控制台	21
安装 CounterACT 控制台	21
登录	22
执行初始设置	22
联系信息	24

欢迎使用 ForeScout CounterACT® 7 版

ForeScout CounterACT 是一套实体或虚拟安全设备，当有网络装置与应用程序连接到您的网络时，它能以动态方式立即进行识别并评估。由于 CounterACT 并不需要代理，因此它能够搭配您的装置运作 — 无论是受管或无受管、已知或未知、PC 或行动装置、嵌入式或虚拟装置均可。CounterACT 可快速判断使用者、拥有者、操作系统、装置组态、软件、服务、修补程序状态，以及是否存在安全性代理。接下来，它可对这些在网络上来来去去的装置提供修补、控制与持续监控的能力。它还能在与您现有的 IT 基础设施完全整合的前提下完成上述所有功能。



This 本指南描述了单一、独立式 CounterACT 设备的安装。

如需更多详情或了解企业级网络防护部署多个设备的信息，请参阅《CounterACT 安装指南》和《控制台用户手册》。这些文档位于 CounterACT 光盘的 /docs 目录中。

此外，您还可以浏览支援网站：<https://www.forescout.com/support> 获取设备最新的文档、知识库文章和软件更新。

CounterACT 包装内容物

- CounterACT 设备
- 快速安装指南
- CounterACT 光盘（含控制台软件、CounterACT 控制台用户手册和安装指南）
- 保修卡
- 安装支架
- 电源线
- DB9 控制台连接线（仅用于串行连接）

概述

执行以下步骤设置 CounterACT:

1. 制定部署计划
2. 设置交换机
3. 连接网线并开机
4. 配置设备
5. 远程管理
6. 验证连接情况
7. 设置 CounterACT 控制台

1. 制定部署计划

执行安装前，应决定设备的部署位置以及了解设备界面连接。

决定设备部署位置

为设备选择正确的网络位置对于 CounterACT 的成功部署和最佳性能是非常重要的。而正确位置则取决于所需实施目标和网络访问政策。本设备应能监测与所需政策相关的信息流量。例如，如果您的政策依赖于监测从端点到企业验证服务器的授权事件，则需要将本设备安装在能看到流向验证服务器的端点信息流量的位置。

如需更多关于安装和部署的信息，请参阅此包装随附 CounterACT 光盘中的《CounterACT 安装指南》。

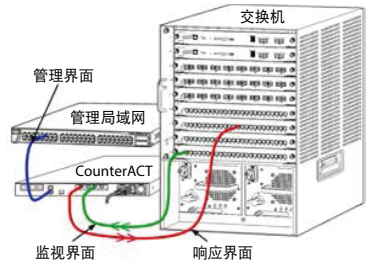
设备界面连接

本设备通常配置了三个连接网络交换机的连接。

管理界面

通过此界面可管理 CounterACT 和执行端点查询与深入检查。此界面必须与能够访问所有网络端点的交换机端口相连接。

每个设备都需要与网络建立单一管理连接。此连接需要本地局域网的一个 IP 地址和执行 CounterACT 控制台管理应用程序的机器的 13000/TCP 端口访问权限。该管理界面必须具有以下网络内容的访问权限：



埠	服务	至或自 CounterACT	功能
22/TCP	SSH	至	允许存取 CounterACT 命令行接口。
2222/TCP			(高可用性) 允许存取属于高可用性丛集的 CounterACT 物理装置。 使用 22/TCP 存取该丛集的共享 (虚拟) IP 地址。
25/TCP	SMTP	自	用于从 CounterACT 发送邮件
53/UDP	DNS	自	允许 CounterACT 解析内部 IP 地址。
80/TCP	HTTP	至	允许 HTTP 复位向。
123/UDP	NTP	自	允许 CounterACT 存取 NTP 时间服务器。 CounterACT 预设使用 ntp.foreScout.net.
135	WMI	自	允许 CounterACT 使用 WMI 执行 Windows 端点的深入研究和控制。
139/TCP	SMB, MS-RPP	自	允许对 Windows 端点进行远程检查 (针对执行 Windows 7 与较早版本的端点)。
445/TCP			允许对 Windows 端点进行远程检查。

埠	服务	至或自 CounterACT	功能
161/UDP	SNMP	自	<p>允许 CounterACT 与网络基础设施装置通讯。例如，交换机和路由器。</p> <p>如需组态 SNMP 的信息，请参阅《CounterACT 控制台使用者手册》。</p>
162/UDP	SNMP	至	<p>许 CounterACT 接收来自网络基础设施装置的 SNMP 陷阱。例如，交换机和路由器。</p> <p>如需组态 SNMP 的信息，请参阅《CounterACT 控制台使用者手册》。</p>
443/TCP	HTTPS	至	允许使用 SSL 进行 TLS 复位向。
2200/TCP	Secure Connector	至	<p>允许 SecureConnector 从 Macintosh/Linux 机器建立与本设备的安全（加密 SSH）连接。当主机连接到网络时，SecureConnector 则为可管理 Macintosh 与 Linux 端点的指令集型代理。</p>
10003/TCP	Secure Connector for Windows	至	<p>允许 SecureConnector 从 Windows 机器建立与本设备的安全（加密 TLS）连接。当主机连接到网络时，SecureConnector 则为可管理 Windows 端点的指令集型代理。请参阅《CounterACT 控制台使用者手册》，以获得有关 SecureConnector 的详细信息。</p> <p>当 SecureConnector 连接到设备或 Enterprise Manager 时，将复位向至其主机所指派的设备。请确认已向所有设备与 Enterprise Manager 开放此端口，以便组织内能获得透明的行动性。</p>
13000/TCP	CounterACT	至	<p>允许控制台连接到本设备。</p> <p>对于具有多个 CounterACT 设备的系统，允许控制台连接到企业管理器以及企业管理器连接到每个设备。</p>

监视界面

此连接允许本设备监视和跟踪网络信息流量。

信息流量被镜像至交换机的一个端口，由本设备进行监视。根据被镜像的 VLAN 数量，信息流量可能或可能不是有标记的 802.1Q VLAN。

单一 VLAN（无标记）：如果监视的信息流量是由单一的 VLAN 生成，镜像的信息流量则不需要有标记的 VLAN。

多个 VLAN（有标记）：如果监视的信息流量是由一个以上的 VLAN 生成，镜像的信息流量则必须有标记的 802.1Q VLAN。

当两个交换机作为冗余对连接时，本设备必须监视来自这两个交换机的信息流量。

监视界面不需要 IP 地址。

响应界面

本设备使用此界面对信息流量做出反应。响应信息流量用于防御恶意活动和执行 NAC 政策行动。这些行动可能包含的示例有重定向网页浏览器或执行防火墙阻拦。相关的交换机端口配置取决于要监测的信息流量。

- **单一 VLAN（无标记）：**如果监视的信息流量是由单一的 VLAN 生成，响应界面则必须配置成为相同 VLAN 的一部分。在此情况下，本设备需要该 VLAN 上的一个 IP 地址。
- **多个 VLAN（有标记）：**如果监视的信息流量是来自一个以上的 VLAN，响应界面则必须配置具有相同 VLAN 的 802.1Q 标记。本设备对于每个受保护的 VLAN 都需要一个 IP 地址。

2. 设置交换机

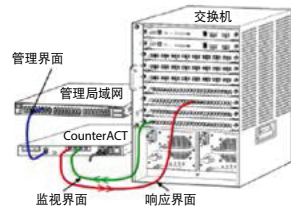
A. 交换机连接选择

本设备是针对无缝集成至广泛的网络环境而设计。若要将本设备成功集成至网络中，请验证交换机是否设置用于监视所需信息流量。

可选择几种方式将本设备连接到交换机。

1. 标准部署（单独的管理、监视和响应界面）

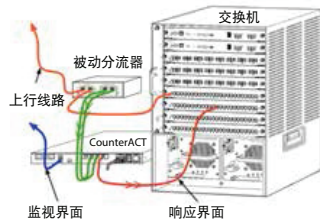
建议部署使用三个单独的端口。关于这些端口的描述请参阅 *设备界面连接*。



2. 被动内联分流器

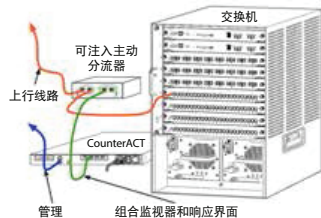
设备可使用一个被动内联分流器来代替连接到一个交换机监视端口。

被动内联分流器需要两个监视端口，“重组”分流器除外，这会把两个双工流组合至一个端口。分流端口和响应界面的信息流量必须以相同的方式配置。例如，如果分流端口的信息流量是有标记的 VLAN(802.1Q)，那么响应界面必须也是有标记的 VLAN 端口。



3. 主动（可注入）内联分流器

当本设备使用可注入内联分流器，可结合监视和响应界面。这不需要在交换机上配置一个单独的响应界面。此选择可用于任何类型的上游或下游交换机配置。



4. IP 层响应（适用于 3 层交换机装置）

本设备可使用自己的管理界面对信息流量作出反应。尽管此选择可用于任何监视的信息流量，但推荐在本设备监视的端口不属于任何 VLAN 时使用，这样本设备不能使用任何其他交换机端口对监视的信息流量作出反应。这种监视连接两个路由器的链接是很普遍。

此选择不能对地址解析协议（ARP）请求作出反应，这会限制本设备针对监视子网中的 IP 地址进行检测扫描的能力。此限制不适用于监视两个路由器之间的信息流量。

B. 交换机设置说明

VLAN (802.1Q) 标记

- **监视单一 VLAN（无标记的信息流量）** 如果监视的信息流量来自单一的 VLAN，那么信息流量则不需要 802.1Q 标记。
- **监视多个 VLAN（有标记的信息流量）** 如果监视的信息流量来自两个或多个 VLAN，则监视和响应界面都必须启用 802.1Q 标记。建议采用“监视多个 VLAN”选择，因为它能尽量减少镜像端口的同时提供最佳的全面覆盖。
- 如果交换机在镜像端口上不能使用 802.1Q VLAN 标记，则执行下列操作之一：
 - 只镜像单一 VLAN
 - 镜像单一没有标记的上行线路端口
 - 使用 IP 层响应选择
- 如果交换机只能镜像一个端口，则镜像单一上行线路端口。这可能有标记。一般来说，如果交换机去除 802.1Q VLAN 标记，则需要使用 IP 层响应选择。

其他说明

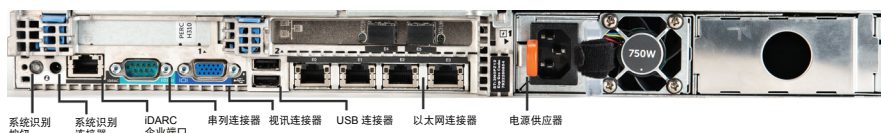
- 如果交换机对收 / 发信息流量都无法镜像，则监视整个交换机、完整的 VLAN（提供收 / 发）或仅一个界面（允许收 / 发）。确认镜像端口不会过载。
- 一些交换机（例如 Cisco 6509）在采用新配置前可能需要完全清除以前的端口配置。不清除旧端口信息的最常见结果是交换机会去除 802.1Q 标记。

3. 连接网线并开机

A. 拆除包装并连接缆线

1. 将设备和电源线从包装箱中取出。
2. 将设备随附的导轨套件取出。
3. 将导轨套件安装在设备上，然后将设备安装在支架上。
4. 使用网线连接设备后面板的网络界面与交换机端口。

后面板示例— CounterACT 装置



B. 记录界面分配

在数据中心完成设备安装和安装 CounterACT 控制台后，您将被提示记录界面分配。当您首次登录控制台时，可在打开的 Initial Setup Wizard（初始设置向导）中输入这些分配，称为通道定义。

在下方记录物理界面分配，在控制台中完成通道设置时使用它们。

以太网界面	界面分配 (例如，管理、监视、响应)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. 打开设备电源

1. 使用电源线连接设备后面板的电源连接器。
2. 将电源线的另一端连接到接地的交流电插座。
3. 将键盘和监视器连接到设备上或设置设备的串行连接。
请参阅 CounterACT 光盘《CounterACT 安装指南》。
4. 从设备前面板开机。

重要信息：拔插头前必先关闭机器。

4. 配置设备

配置设备前，请准备以下信息。

<input type="checkbox"/> 设备主机名	
<input type="checkbox"/> CounterACT 管理员密码	将密码保存在安全位置
<input type="checkbox"/> 管理界面	
<input type="checkbox"/> 设备 IP 地址	
<input type="checkbox"/> 网络掩码	
<input type="checkbox"/> 默认网关 IP 地址	
<input type="checkbox"/> DNS 域名	
<input type="checkbox"/> DNS 服务器地址	

开机后，您将被以下信息提示开始配置。

CounterACT 设备启动完成。
按 **<Enter>** 继续。

1. 按 **Enter** 显示以下菜单：

1) 配置 **CounterACT**
2) 恢复保存的 **CounterACT** 配置
3) 标识网络界 并重新编号
4) 配置键盘布局
5) 关机
6) 重启机器
选项 (1-6)：1

2. 选择 **1** - 配置 CounterACT。出现提示时：

继续：（是/否）？

按 **Enter** 开始设置。

3. 将打开 **High Availability Mode**（高可用性模式）菜单。按 **Enter** 选择标准安装。
4. 将显示 **CounterACT Initial Setup**（CounterACT 初始设置）提示。按 **Enter** 继续。
5. 将打开 **Select CounterACT Installation Type**（选择 CounterACT 安装类型）菜单。输入 **1**，按 **Enter** 安装标准CounterACT 设备。设置将初始化。这可能需要一些时间。


6. 出现 **Enter Machine Description**（输入机器描述）输入标识该设备的简短文本，按 **Enter**。
将显示以下内容：

>>>>>> 设置管理员密码 <<<<<<

此密码用于以“根用户”身份登录机器的操作系统和以“管理员”身份登录 CounterACT 控制台。

密码应为 6 - 15 个字符，应包含至少一个非字母字符。

管理员密码：

7. 出现 **Set Administrator Password**（设置管理员密码）提示时，输入密码字符串（不是屏幕的应答字符串），然后按 **Enter**。您将被提示确认密码。密码必须为 6 - 15 个字符，应包含至少一个非字母字符。
-  以用户身份登录设备，以管理员身份登录控制台。
8. 出现 **Set Host Name**（设置主机名）提示时，输入一个主机名，然后按 **Enter**。主机名可在登录控制台时使用，并且显示在控制台上，帮助您识别正在查看的 CounterACT 设备。
9. **Configure Network Settings**（配置网络设置）屏幕会提示您输入一系列配置参数。按照每个提示输入一个值，按 **Enter** 继续。
- CounterACT 组件通过管理界面通信。列出的管理界面数量取决于设备型号。
 - **Management IP address**（管理 IP 地址）是 CounterACT 组件通信界面的地址。只用于在连接到有标记端口的 CounterACT 组件之间通信的情况下为此界面添加一个 VLAN ID。
 - 如果有一个以上的 **DNS 服务器地址**，用空格隔开每个地址——大多数内部 DNS 服务器可解析外部和内部地址，但您可能需要包含一个外部解析 DNS 服务器。因为设备执行的所有 DNS 查询几乎所有都是内部地址，所以外部 DNS 服务器应列在最后。
10. 将显示 **Setup Summary**（设置摘要）屏幕。您将被提示执行一般连接测试、重新配置设置或完成设置。输入 **D** 完成设置。

许可证

安装后，您必须安装 CounterACT 代表提供的初始演示许可证。此许可证在初始控制台设置时安装。此初始演示许可证具有一定天数的有效期。您必须在有效期结束前安装一个永久许可证。我们将通过电子邮件向您通知到期日。此外，控制台的 Appliances/Devices（设备/装置）窗格也会显示关于到期日和许可证状态的信息。

一旦您获得了永久许可证，ForeScout 许可服务器会每天对它验证一次。Device Details（装置详情）窗格会显示许可证提醒警告和违规情形。

达一个月无法验证为可延长的许可证将被撤回。请参阅《CounterACT 安装指南》了解关于许可证的更多信息。

网络连接要求

至少一个 CounterACT 装置（设备或企业管理器）必须能够访问互联网。此连接被 ForeScout 许可证服务器用来验证 CounterACT 许可证。

无法验证为可延长达一个月的许可证将被撤回。CounterACT 会每天发送一封说明与服务器有通信错误的警告电子邮件。

5. 远程管理

iDRAC 设置

集成戴尔远程控制器 (iDRAC) 是一个集成服务器系统解决方案，让您可通过本地局域网或互联网远程访问 CounterACT 设备/企业管理器，不受位置/操作系统限制。使用此模块可执行 KVM 访问、开机/关机/重置和执行故障检修与保养任务。

使用 iDRAC 模块执行以下任务：

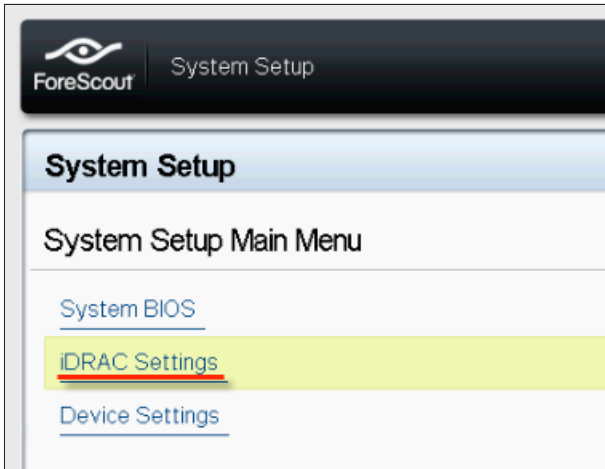
- 启用和配置 iDRAC 模块
- 将模块连接至网络
- 登录 iDRAC

启用和配置 iDRAC 模块

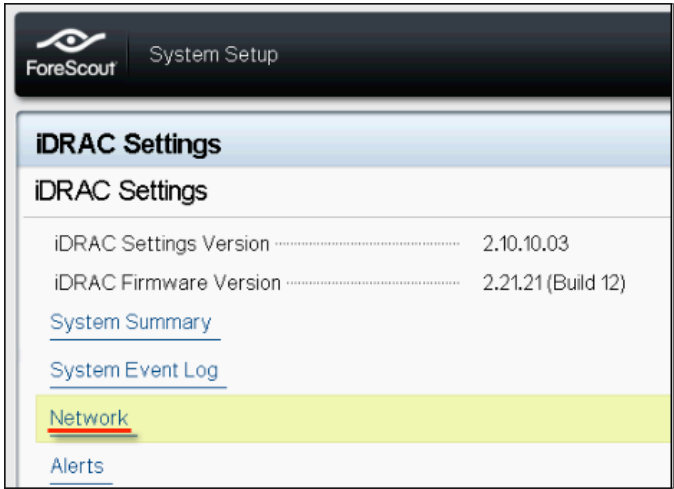
更改 iDRAC 设置，在 CounterACT 装置上启用远程访问。此节描述了与 CounterACT 一起使用的所需基本集成设置。

配置 iDRAC：

1. 打开受管理的系统。
2. 在开机自检 (POST) 时按 F2。
3. 在 System Setup Main Menu（系统设置主菜单）页面上，选择 **iDRAC Settings**（iDRAC 设置）。



4. 在 iDRAC Settings（iDRAC 设置）页面上，选择 **Network**（网络）。



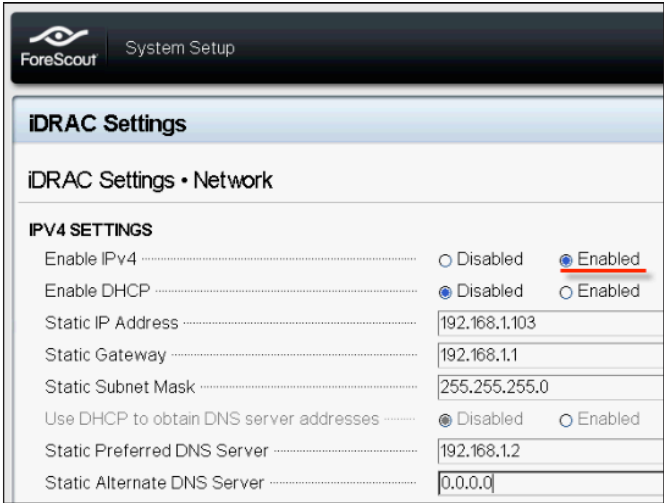
5. 配置以下网络设置：

- **网络设置。** 确认 **Enable NIC**（启用 NIC）字段是否设置为 **Enabled**（启用）。



- **普通设置。** 在 DNS DRAC Name（DNS DRAC 名称）字段中，您可以更新动态 DNS（可选）。

- **IPV4 设置。**确认 **Enable IPv4**（启用 IPv4）字段是否设置为 **Enabled**（启用）。将 **Enable DHCP**（启用 DHCP）字段设置为 **Enabled**（启用）使用动态 IP 地址分配或设置为 Disabled（禁用）使用静态 IP 地址分配。如启用，DHCP 会自动给 iDRAC 分配 IP 地址、网关和子网掩码。如禁用，在 **Static IP Address**（静态 IP 地址）、**Static Gateway**（静态网关）和 **Static Subnet Mask**（静态子网掩码）字段中输入值。



ForeScout System Setup

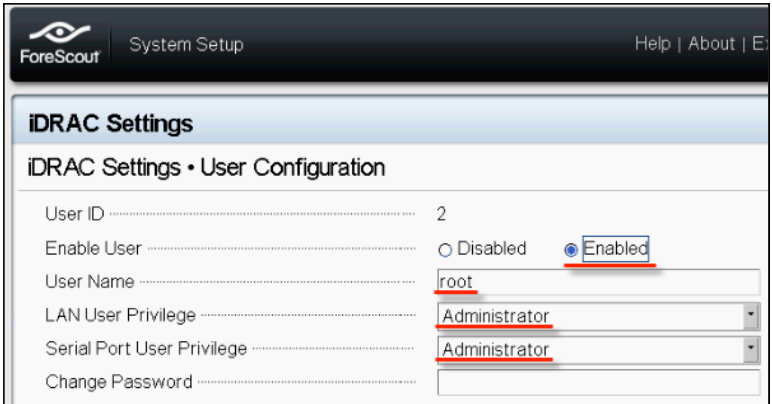
iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

Enable IPv4	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Enable DHCP	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Static IP Address	192.168.1.103
Static Gateway	192.168.1.1
Static Subnet Mask	255.255.255.0
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Static Preferred DNS Server	192.168.1.2
Static Alternate DNS Server	0.0.0.0

6. 选择 **Back**（返回）。
7. 选择 **User Configuration**（用户配置）。
8. 配置以下用户配置字段：
 - **Enable User**（启用用户）。确认此字段是否设置为 Enabled（启用）。
 - **User Name**（用户名）。输入一个用户名。
 - **LAN and Serial Port User Privileges**（本地局域网和串行端口用户权限）。将权限级别设置为 Administrator（管理员）。
 - **Change Password**（更改密码）。设置用户登录的密码。



ForeScout System Setup Help | About | E

iDRAC Settings

iDRAC Settings • User Configuration

User ID	2
Enable User	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
User Name	root
LAN User Privilege	Administrator
Serial Port User Privilege	Administrator
Change Password	

9. 选择 **Back**（返回），然后选择 **Finish**（完成）。确认更改的设置。网络设置保存后，系统重启。

将模块连接至网络

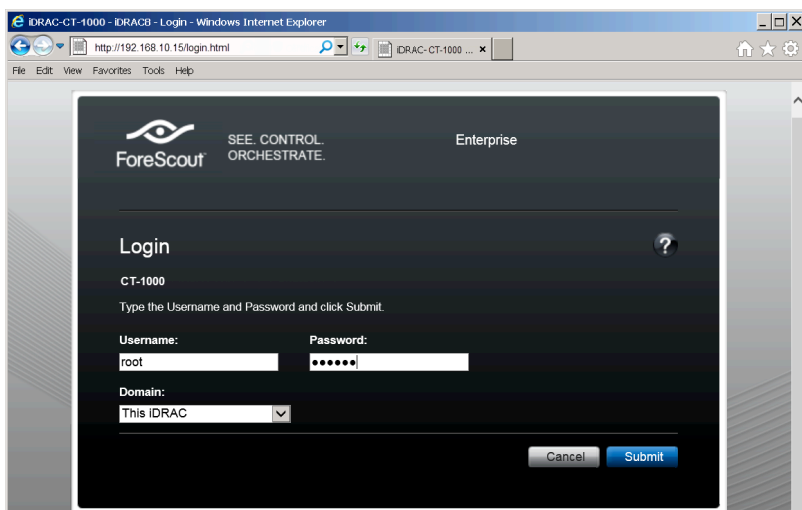
iDRAC 连接到以太网网络。通常会将它连接到管理网络。下图显示了 CT-1000 设备后面板上的 iDRAC 端口位置。



登录 iDRAC

登录 iDRAC:

1. 访问在 **iDRAC Settings**（iDRAC 设置）> **Network**（网络）中配置的 IP 地址或域名。



2. 输入在 iDRAC 系统设置的 User Configuration（用户配置）页面中配置的用户名和密码。
3. 选择 **Submit**（提交）。

如需更多关于 iDRAC 的信息，请参阅 [《iDRAC 用户指南》](#)。

更新默认凭据是重要。

6. 验证连接情况

验证管理界面连接

若要测试管理界面连接，登录设备，执行以下命令：

```
fstool linktest
```

将显示以下信息：

```
管理界  状态
Ping  默认网关信息
Ping  统计信息
执行域名解析测试
测试摘要
```

验证交换机/设备连接情况

退出数据中心前，请确认交换机已正确连接到设备。要执行此操作，在设备上为检测的每个界面执行 `fstool ifcount` 命令。

```
fstool ifcount eth0 eth1 eth2
```

（以空格隔开每个界面）。

此工具持续显示指定界面的网络信息流量。它以两种模式工作：按界面或按 VLAN。模式可在显示屏中进行更改。显示以下每个信息流量类别的位 / 秒和百分比：

- 监视界面应主要看到 90 % 以上的镜像信息流量。
- 响应界面应主要看到广播信息流量。
- 监视和响应界面应都能看到预期的 VLAN。

命令选项：

```
v - 以 VLAN 模式显示
I - 以界 模式显示
P - 显示上一个
N - 显示下一个
q - 退出显示
```

VLAN 模式：

update=[4] [eth3: 14 vlans]					
Interface/Vlan	Total	Broadcast	Mirrored	*To my MAC	*From my MAC
eth3.untagged	4Mbps	0.2%	99.8%	0.0%	0.0%
eth3.1	9Mbps	0.0%	100.0%	0.0%	0.0%
eth3.2	3Mbps	0.1%	99.9%	0.0%	0.0%
eth3.4	542bps	100.0%	0.0%	0.0%	0.0%
eth3.20	1Kbps	100.0%	0.0%	0.0%	0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext-> [q]uit					

界面模式：

update=[31] [eth0: 32 vlans] [eth1: 1 vlans]					
Interface	Total	Broadcast	Mirrored	*To my MAC	*From my MAC
eth0	3Kbps	42.3%	0.0%	14.1%	43.7%
eth1	475bps	0.0%	100.0%	0.0%	0.0%

*To my MAC — 目标 MAC 是设备的 MAC。

*From my MAC — 从此设备发送的信息流量（源 MAC 是设备的 MAC。目标可能是广播或单播）。

如果您看不到任何信息流量，请确认该界面是否启动。在设备上使用以下命令：

ifconfig [interface name] up

执行 Ping 测试

从设备向网络桌面执行一个 Ping 测试来验证连接情况。

执行测试：

1. 登录设备。
2. 执行以下命令：**Ping [network desktop IP]** 默认情况下，设备本身不回复 Ping。

7. 设置 CounterACT 控制台

安装 CounterACT 控制台

CounterACT 控制台是用于查看、跟踪和分析本设备检查的活动的中央管理应用程序。可使用此控制台定义 NAC、威胁防护、防火墙和其他政策。请参阅《CounterACT 控制台用户手册》了解更多信息。

您必须提供一部执行 CounterACT 主控台应用程序软件的机器。最低的硬件要求为：

- 非专用的机器，并执行：
 - Windows XP、Windows Vista 或 Windows 7
 - Windows Server 2003 或 Server 2008
 - Linux
- Pentium 3, 1 GHz
- 2 GB 的内存
- 1 GB 的磁盘空间

执行控制台安装有两种方法：

使用设备内置的安装软件。

1. 从控制台电脑打开浏览器窗口。
2. 在浏览器地址行中输入 http://<Appliance_ip>/install
<Appliance ip> 指此设备的 IP 地址。此浏览器显示控制台安装窗口。
3. 遵循屏幕上的指示。

从 CounterACT CD-ROM (唯读光盘) 安装

1. 将 CounterACT CD ROM (唯读光盘) 插入 DVD (数位视频光盘) 驱动器中。
2. 使用浏览器打开 CD ROM (唯读光盘) 中的 **ManagementSetup.htm** 文件。
3. 遵循屏幕上的指示。

登录

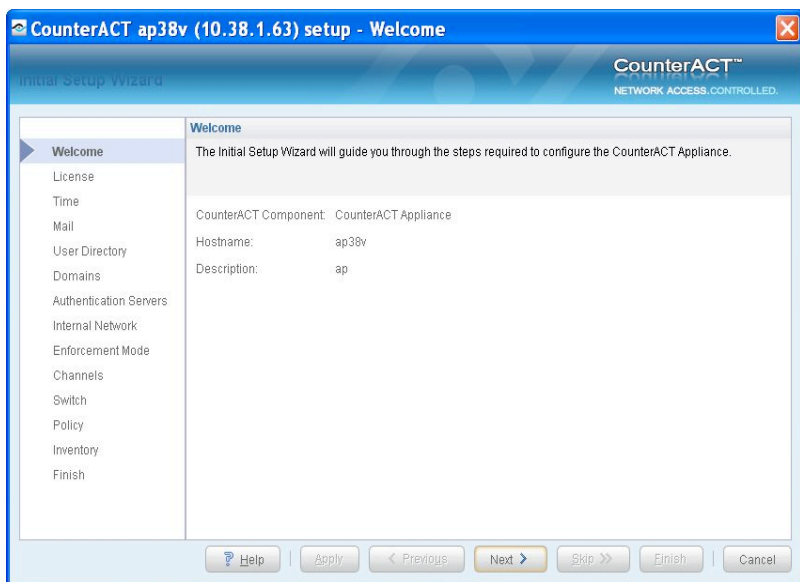
安装完成后，您可登录 CounterACT 控制台。

1. 从创建的快捷方式位置选择 CounterACT 图标。
2. 在 **IP/Name**（IP/名称）字段中输入设备的 IP 地址或主机名。
3. 在 **User Name**（用户名）字段中，输入 **admin**。
4. 在 **Password**（密码）字段中，输入在设备安装过程中创建的密码。
5. 选择 **Login**（登录）启动控制台。



执行初始设置

首次登录后，会显示 Initial Setup Wizard（初始设置向导）。本向导将引导您完成必要的配置步骤，确保 CounterACT 快速有效地启动执行。



开始初始设置前

使用此向导前，请准备以下信息：

信息	值
<input type="checkbox"/> 您的组织使用的 NTP 服务器地址（可选）。	
<input type="checkbox"/> 内部邮件中继 IP 地址。如果设备不允许 SMTP 信息流量，这可允许从 CounterACT 发送电子邮件（可选）。	
<input type="checkbox"/> CounterACT 管理员的电子邮件地址。	
<input type="checkbox"/> 在数据中心定义的监视和响应界面。	
<input type="checkbox"/> 对于没有 DHCP 的网段或 VLAN，此网段或 VLAN 与监视界面直接连接，CounterACT 要对每个这样的 VLAN 使用一个永久 IP 地址。企业管理器设置不需要此信息。	
<input type="checkbox"/> 设备将保护的 IP 地址范围（所有内部地址，包含未使用的地址）。	
<input type="checkbox"/> 用户目录账户信息和用户目录服务器 IP 地址。	
<input type="checkbox"/> 域证书，包含域管理账户名和密码。	
<input type="checkbox"/> 验证服务器，使 CounterACT 可分析哪些网络主机得到成功验证。	
<input type="checkbox"/> 核心交换机 IP 地址、供应商和 SNMP 参数。	

请参阅《CounterACT 控制台用户手册》或在线帮助了解使用此向导的信息。

联系信息

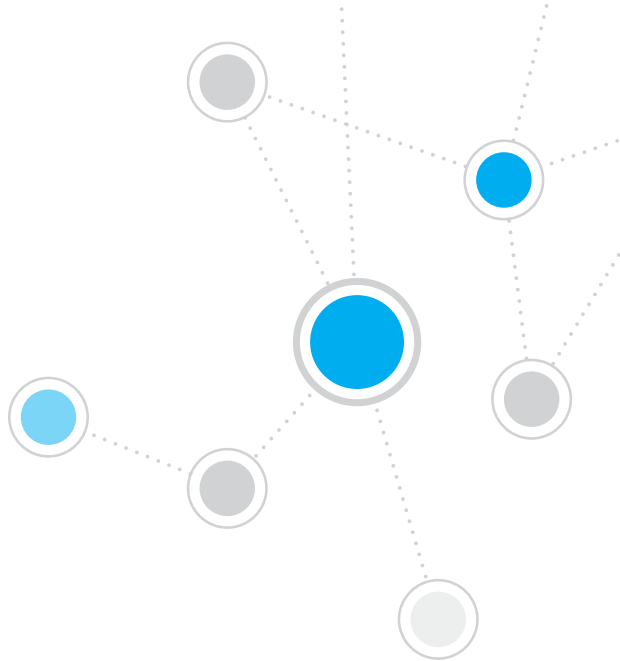
如需 ForeScout 技术支援，请发送邮件至 support@forescout.com 或致电：

- 免费电话（美国）：+1-866-377-8771
- 电话（国际）：+1-408-213-3191
- 支援：+1-708-237-6591
- 传真：+1-408-371-2284

©2016 ForeScout Technologies, Inc. 产品受美国专利保护：#6,363,489、#8,254,286、#8,590,004 和 #8,639,800。保留所有权利。

ForeScout Technologies 和 ForeScout 标志是 ForeScout Technologies, Inc 的商标。所有其他商标为各自所有人所有。

使用任何 ForeScout 产品均应遵守 www.forescout.com/eula 上的 ForeScout 终端用户许可协议的条款。



ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

免费电话（美国）： +1-866-377-8771

电话（国际）： +1-408-213-3191

支援： +1-708-237-6591

传真： +1-408-371-2284

400-00020-01