Forescout®

单机版

《快速安装手册》

版本 8.2

联系信息

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

免费电话（美国）：1.866.377.8771

电话（国际）：1.408.213.3191

客服：1.708.237.6591

关于本文档

- 欲了解更多技术文件，请前往 Forescout 网站资源页面：https://www.forescout.com/company/resources/
- 有反馈或疑问？请致信我们 documentation@forescout.com

法律声明

2020 年 2 月 10 日 17:07:49

目录

欢迎使用 8.2 版本

Forescout 平台提供基础设施和设备可视性、政策管理、业务流程和工作流简化，以加强网络安全。该平台为企业提供实时的网络设备和用户上下文信息。经使用此上下文信息定义政策，帮助确保合规、修复、有适当的网络访问和简化服务操作。

本手册主要介绍已预装 8.0 版本情况下，单机版 CounterACT 装置的安装方法。有些装置可能会预装较新版本。欲使用 8.2 版本，请遵循经批准的升级路径，见版本发布注意事项下划线部分。

更详细的信息或关于升级或关于部署多个装置在企业范围内实施网络保护的信息，请参阅《*Forescout 安装手册*》和《*Forescout 管理手册*》。请参阅 其他 Forescout 文档了解如何查看此类手册的信息。

另外，您也可以导航至支持网站：http://www.forescout.com/support，查看最新的文档、知识库文章和装置的相关更新。

Forescout 包装清单

您的 Forescout 包装包含下列组件：

- CounterACT 装置
- 前面板
- 导轨套件（安装支架）
- 电源线
- DB9 控制台连接线缆（仅用于串行连接）
- 《企业产品安全、环境和监管信息》
- 启动文件（CT-xxxx 装置仅基于硬件改版 5x 和 Forescout 51xx 装置）

概述

按照下列步骤装配 Forescout：

1.制定部署计划

2.设置交换机

3.连接网线并接通电源

4.配置装置

5.远程管理

6.验证连接

7.设置 Forescout 控制台

1.制定部署计划

安装之前，应该确定部署装置的位置并了解装置的接口连接。

确定部署装置的位置

选择安全装置的正确网络位置，对成功部署和提供最佳性能来说极为重要。正确的位置取决于想要的安装目标和网络访问政策。改装置应该能够监控与所需政策相关的流量。例如，如果您的政策依赖于在企业认证服务器的端点监控授权活动，则需要安装此装置，这样它就能看到流入认证服务器的端点流量。

更多关于安装和部署的信息，请参阅*《Forescout 安装手册》*。请参阅 其他 Forescout 文档了解如何查看此手册的信息。

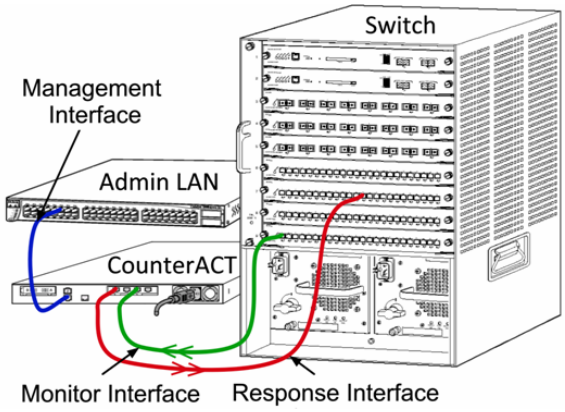
装置接口连接

该装置通常配置有三个连接网络交换机的接口连接。

管理接口

管理接口方便您管理 Forescout 平台并对端点进行查询和深层检测。该接口必须连接至可访问所有网络端点的交换机端口。

每台装置需要单独一个管理接口来连接网络。此连接需要本地 LAN 上的 IP 地址和来自机器的 13000/TCP 端口访问，这将在控制台管理应用程序上运行。管理端口必须可以访问其他网络服务。



网络接入要求

端口	服务	接入或接出 Forescout 平台	功能
22/TCP	SSH	接出	允许远程监测 OS X 和 Linux 端点。 允许 Forescout 平台与网络交换机和路由器通信。
		接入	允许接入 Forescout 平台命令行接口。
2222/TCP	SSH	接入	（高可用性）允许访问作为高可用性对一部分的实体装置。 使用 22/TCP 访问该对的共享（虚拟）IP 地址。
25/TCP	SMTP	接出	允许 Forescout 平台访问企业邮件转发。
53/UDP	DNS	接出	允许 Forescout 平台解析内部 IP 地址。
80/TCP	HTTP	接入	允许 HTTP 重定向。
123/UDP	NTP	接出	允许 Forescout 平台访问本地时间服务器或 ntp.forescout.net。 通过默认 Forescout 平台访问 ntp.foreScout.net
135/TCP	MS-WMI	接出	允许远程监测 Windows 端点。
139/TCP	SMB， MS-RPC	接出	允许远程监测 Windows 端点（对于运行 Windows 7 或较早版本的端点）。
445/TCP			允许远程监测 Windows 端点。
161/UDP	SNMP	接出	允许 Forescout 平台与网络交换机和路由器通信。 有关配置 SNMP 的信息，请参阅 *《Forescout 管理手册》*。

端口	服务	接入或接出 Forescout 平台	功能
162/UDP	SNMP	接入	允许 Forescout 平台从网络交换机和路由器上检索 SNMP 陷阱。 有关配置 SNMP 的信息，请参阅 *《Forescout 管理手册》*。
389/TCP (636)	LDAP	接出	允许 Forescout 平台与活动目录通信。 允许与 Forescout 平台的基于网站的门户通信。
443/TCP	HTTPS	接入	允许使用 TLS 进行 HTTP 重定向。
10006/TCP	SecureConnector 用于 Linux	接入	允许 SecureConnector 透过 TLS 1.2 在 Linux 机器上创建安全连接以连接至该装置。。*SecureConnector* 是个基于代理的脚本，它在连接至网络的同时可进行 Linux 端点管理。
10003/TCP	SecureConnector 用于 Windows	接入	允许 SecureConnector 在 Windows 机器上创建安全的（加密的 TLS）连接以连接至该装置。*SecureConnector* 是个代理，它在连接至网络的同时可进行 Windows 端点管理。请参阅 *《Forescout 管理手册》* 了解更多关于 SecureConnector 的信息。 SecureConnector 连接至装置或企业管理器时，它会被重定向至主机被分配的装置。确保此端口对所有装置和企业管理器开放，从而允许在组织内部透明地移动。
10005/TCP	SecureConnector 用于 OS X	接入	允许 SecureConnector 在 OS X 机器上创建安全的（加密的 TLS）连接以连接至该装置。*SecureConnector* 是个代理，它在连接至网络的同时可进行 OS X 端点管理。请参阅 *《Forescout 管理手册》* 了解更多关于 SecureConnector 的信息。 SecureConnector 连接至装置或企业管理器时，它会被重定向至主机被分配的装置。确保此端口对所有装置和企业管理器开放，从而允许在组织内部透明地移动。
13000/TCP	Forescout 平台	接入/接出	对于只有一台装置的部署——从控制台连接到装置。 对于有多台装置的部署——从控制台连接到该装置设备，再从一台装置连接到另一台装置。装置通信包括使用 TLS 与企业管理器和恢复企业管理器通信。

监控接口

监控接口允许装置监控并追踪网络流量。任何可用接口都可被用作监控接口。

流量镜像至交换机的端口并由该装置监控。802.1Q VLAN 标记的使用取决于被镜像的 VLAN 数量。

- ***单一 VLAN***：监控的流量由单一的 VLAN 生成时，镜像流量则不需要添加 VLAN 标记。
- ***多重 VLAN***：如果监控的流量来自于多个 VLAN，镜像流量则必须添加 802.1Q VLAN 标记。

当两个交换机作为冗余对连接时，该装置必须同时监控两个交换机的流量。

监控接口无需 IP 地址。

响应接口

该装置使用响应接口对流量作出响应。响应流量用于防止恶意行为并执行政策措施。这些措施可能包括，例如，重定向网页浏览器或进行会话屏蔽。相关的交换机端口配置取决于正被监控的流量。

任何可用接口都可被用作响应接口。

- ***单一 VLAN***：监控的流量由单一的 VLAN 生成时，响应端口则必须属于同一个 VLAN。在这种情况下，该装置在该 VLAN 上必须有单一的 IP 地址。
- ***多重 VLAN***：如果监控的流量来自多个 VLAN，响应端口也必须为相同的 VLAN 配置 802.1Q VLAN 标记。该装置则要求每个被监控 VLAN 有一个 IP 地址。

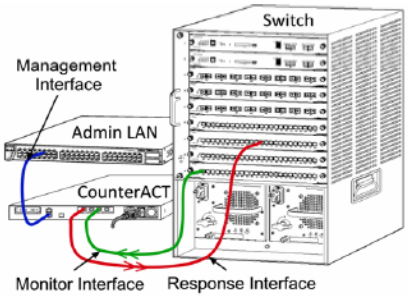
2.设置交换机

A. 交换机连接选项

该装置旨在与多种多样的网络环境无缝集成。为了成功地将装置集成在您的网络中，请验证交换机是否设定为监控所需流量。

有几个选项可用于将该装置连接至您的交换机。

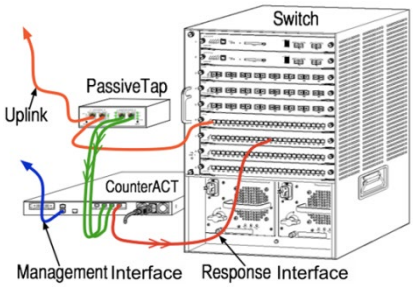
1 标准部署（分开管理、监控和响应接口）



推荐部署使用三个独立的端口。这些端口在 装置接口连接 有说明。

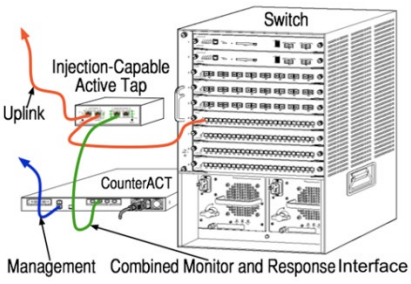
2 被动式内联分接头

该装置可使用被动式内联分接头，不需要连接至交换机监控端口。



被动式内联分接头需要两个监控端口（一个用于上游流量，而另一个用于下游流量），除非是在有*重组*分接头的情况下，它会将两个双相流结合在单独一个端口中。注意，如果连接分接头的端口上的流量被添加了 802.1Q VLAN 标记，那么响应端口也必须添加 802.1Q VLAN 标记。

3 主动式（可插入）内联分接头



该装置可使用主动式内联分接头。如果分接头可以插入，该装置则会将监控端口和响应端口结合在一起，这样就无需在交换机上配置单独的响应端口。无论是上游还是下游交换机配置类型，均可使用此选项。

4 IP 层响应（第 3 层交换机安装）

该装置可以使用自带的管理接口对流量作出响应。尽管这个选项可与任何受监控的流量一起使用，但还是推荐只在装置显示器端口不是任何 VLAN 的一部分，且这样无法使用其他任何交换机端口对监控的流量作出响应时使用。这在监控两个路由器之间的链接时最常出现。这个选项无法对地址解析协议 (ARP) 请求作出响应，它会限制该装置探测针对 IP 地址（包括子网）的扫描的能力。两个路由器之间的流量受到监控时，此限制将不适用。

B. 交换机设置注意事项

VLAN (802.1Q) 标记

- ***监控单一 VLAN***：如果受监控流量来自于单一 VLAN，那么该流量则不需要 802.1Q VLAN 标记。
- ***监控多重 VLAN***：如果受监控的流量来自于两个或多个 VLAN，那么监控端口和响应端口都必须启用 802.1Q VLAN 标记。推荐监控多重 VLAN，因为它在最大限度减少镜像端口数量的同时，也提供最佳的整体覆盖。
- 如果交换机无法在镜像端口上使用 802.1Q VLAN 标记，那么请执行下列操作中的一项：

– 仅镜像单一 VLAN
– 镜像单一、未加标记的上行链路端口
– 使用 IP 层响应选项

- 如果交换机只能镜像一个端口，那么会镜像单一上行链路端口。这可能会被添加标记。一般而言，如果交换机去掉 802.1Q VLAN 标记，您就必须使用 IP 层响应选项。

其他手册

- 在下列情况下，您只能镜像一个接口（允许传送/接收）：

– 如果交换机无法镜像传输的和接收的流量
– 如果交换机无法镜像所有交换机流量
– 如果交换机无法镜像 VLAN 的所有流量

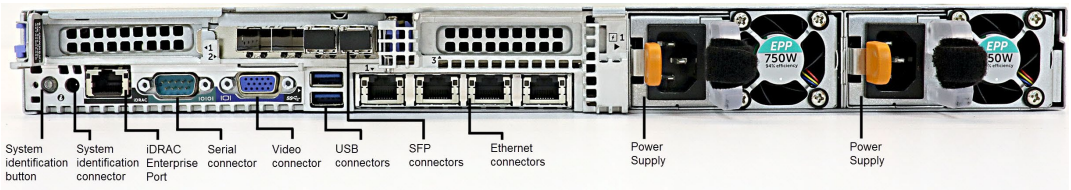
- 请确认您的镜像端口没有过载。
- 有些交换机（例如 Cisco 6509）在进入新的配置之前，可能会要求完全删除当前的端口配置。未删除旧有的端口信息通常会导致交换机去掉 802.1Q 标记。

3.连接网线并接通电源

A. 打开设备包装并连接电缆

1. 将装置和电力电缆从集装箱上搬下来
2. 拿下与装置一起收到的导轨套件。
3. 在装置上安装导轨套件并将装置安装在支架上。
4. 连接装置后面板上的网络接口和交换机端口之间的网线。

后面板样板——CounterACT 装置



您可以使用经 Forescout 测试并认证的 Finisar SFP 替换 Forescout 提供的 SFP。请参阅*《Forescout 安装手册》*了解更多详细信息。

B. 记录接口分配

在数据中心完成装置安装并安装 Forescout 控制台之后，您将收到登记接口分配的提示。这些分配，也被称为*通道定义*，要输入在您首次登录控制台时打开的初始设置向导中。

在下方记录实际的接口分配，并在控制台上完成通道设置时使用它们。

Eth 接口	接口分配（例如，管理、监控和响应）
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

C. 接通装置的电源

1. 将电力电缆连接到装置后面板上的电源连接器上。
2. 将电力电缆的另一端连接到接地的交流电插座上。
3. 将键盘和显示器与装置相连，或者设置装置的串行连接。请参阅*《Forescout 安装手册》*了解更多信息。
4. 在前面板上打开装置的电源。

4.配置装置

在您配置装置之前，请准备好下列信息。

装置主机名	
Forescout 管理密码	将密码保存在安全的位置
管理接口	
装置 IP 地址	
网络掩码	
默认网关 IP 地址	
DNS 域名	
DNS 服务器地址	

打开电源之后，您将被提示开始配置下列信息：

下列提示为示范。有些装置可能会预装其他版本，其提示可能稍有不同。

```
CounterACT 装置启动完成。
按下 <Enter> 键以继续。
```

1. 按下 **Enter** 键。如果您的装置是 Forescout 51xx，则会显示下列菜单：

```
CounterACT <version>-<build> 选项：

1) 配置 Forescout 设备
2) 还原保存的 Forescout 配置
3) 识别并对网络接口重新编号
4) 配置键盘布局
5) 关闭机器
6) 重启机器

选择 (1-6)：1
```

如果您的装置是 CT-xxxx，则会在菜单顶部看到列示的版本是 CounterACT 7.0.0 或 CounterACT 8.0.0。

- 如果您看到的是 CounterACT 7.0.0，则可以升级或者直接安装版本 8.0.0。请参阅 *《Forescout 安装手册》*了解详细信息。升级至或安装版本 8.0.0 之后，您将会看到上述菜单。
- 如果您看到的是 CounterACT 8.0.0，菜单则会提供安装 7.0.0 或配置 8.0.0 的选项，如下所示。如果您选择 7.0.0，则将无法通过 Configuration（配置）菜单重新安装 8.0.0。请参阅 *《Forescout 版本 7.0.0 安装手册》*了解配置 7.0.0 的详细信息。

```
CounterACT 8.0.0-<build> 选项：

1) 安装 CounterACT 7.0.0-<build>
2) 配置 CounterACT 8.0.0-<build>
3) 还原保存的 CounterACT 配置
4) 识别并对网络接口重新编号
5) 配置键盘布局
6) 关闭机器
7) 重启机器

选择 (1-7)：
```

如果配置被中断或者如果您选择的版本错误，则需要使用相关版本的 ISO 文件重置装置影像。请参阅《Forescout 安装手册》了解更多重置装置影像的信息。

2. 键入 1 并按下 **Enter** 键。

```
选择 High Availability Mode（高可用性模式）：

1）  Standard Installation（标准安装）
2）  High Availability（高可用性）— Primary Node（主节点）
3）  添加节点至在现有主要或次要 Active Node（活动节点）

选择 (1-3) [1] ：
```

3. 键入 **1** (标准安装)并按下 **Enter** 键。

```
>>>>>> Forescout 平台 Initial Setup （初始设置）<<<<<<

您将设置 Forescout 平台。在初始设置过程中，将提示您设置基本参数，以便将机器连接至网络。

该阶段完成后，将指示您从 Forescout Console （控制台）完成设置。

继续？（yes/no（是/否））：
```

4. 键入 **是** 并按下 **Enter** 键。

仅运行 8.2 安装时将显示下列提示。

```
验证 Compliance Mode （兼容模式）？（yes/no（是/否））[否] ：
```

5. 除非您的组织需要遵守通用标准和 DoDIN APL 验证，键入 **否** 并按下 **Enter** 键。

```
>>>>>> 选择 CounterACT Installation Type （安装类型） <<<<<<


1) CounterACT 装置
2) CounterACT Enterprise Manager （企业管理人）

选择 (1-2):
```

6. 键入 **1** 并按下 **Enter** 键。设置被初始化。这可能需要一点时间。

```
>>>>>> 选择 Licensing Mode（许可模式）<<<<<<


1) 按照装置许可模式
2) Flexx 许可模式

选择 (1-2) [1]:
```

7. 选择您的部署使用的许可模式。许可模式在购买过程中决定。***确认您的部署使用的许可模式之前，请勿键入任何值***。联系您的 Forescout 销售代表验证您的许可模式或者验证您是否输入了错误的模式。

> *Forescout 51xx 装置不显示该选项。*

8. 如为 按照装置许可模式，则键入 **1**，如为 Flexx 许可模式，则键入 2，并按下 **Enter** 键。

```
>>>>>> 输入机器描述 <<<<<<


输入机器简介（例如纽约办事处）。


描述:
```

9. 键入描述并按下 Enter 键。

显示下列界面：

```
>>>>>> 设置管理员密码 <<<<<<

此密码将被用于以“cliadmin（客户管理员）”的身份登录机器操作系统并
以“管理员”的身份登录 CounterACT 控制台。
密码的长度必须为 6 到 15 个字符，而且应至少包含一种非字母字符。

管理员密码：
```

10. 在 Set Administrator Password（设置管理员密码）提示框中，键入密码字符串（这个字符串不会在屏幕上显示），然后按下 **Enter** 键。您将会收到确认密码的提示。密码的长度必须为 6 到 15 个字符，而且至少要包含一种非字母字符。

以 *cliadmin（客户管理员）*的身份登录装置，然后以 *admin（管理员）*的身份登录控制台。

11. 在 Set Host Name（设置主机名称）提示框中，键入主机名称，然后按下 **Enter** 键。主机名称可在登录控制台时用到，而且会显示在控制台上，以帮助您识别正在查看的 CounterACT 装置。主机名称不得超过 13 个字符。

12. Configure Network Settings（配置网络设置）界面会提示一系列配置参数。在每个提示框中键入一个值，然后按下 **Enter** 键以显示下一个提示框。

- Forescout 组件通过管理接口通信。列示的管理接口数量取决于装置模块。
- **Management IP address（管理 IP 地址）**是 Forescout 平台组件通信所使用接口的地址。只有当用于在 Forescout 平台组件之间通信的接口连接至添加标记的端口时，为此接口添加 VLAN ID。
- 如果有多个 **DNS 服务器地址**，则用空格将每个地址隔开。大部分内部 DNS 服务器可解析外部和内部地址，但是您可能需要添加一台外部解析 DNS 服务器。由于装置执行的所有 DNS 查询都将用于内部地址，因此，外部 DNS 服务器应该被列在最后。

13. Setup Summary（设置概要）界面则会显示。您将被提示执行一般连接测试、重新配置设置或完成设置。键入 **D** 以完成设置。

许可证

配置之后，确保您的装置拥有有效的许可证。您的装置的默认许可状态取决于您的部署正在使用的许可模式。

- 如果您的 Forescout 部署正在 ***Per-Appliance Licensing Mode（单一装置许可模式）***下运行，您现在可以使用演示许可证开始工作，该许可证的有效期是 30 天。在此期间，您应该会收到 Forescout 的永久性的许可证，将它放在磁盘或网络的可访问文件夹中。在 30 天的演示许可证到期之前，从这个位置安装许可证（如有必要，您可以申请演示许可证延期）。

  如果您的演示许可证即将过期，您将收到通过各种方式发来的提示。请参阅*《Forescout 管理手册》*了解更多关于演示许可证提示的信息。

  如果您在使用 Forescout 虚拟系统：

  - 演示许可证则不会在这个阶段自动安装。您必须安装您的 Forescout 代表通过电子邮件发送给您的演示许可证。

- 至少应该有一台 CounterACT 设备可以访问网络。此连接用于在 Forescout 许可证服务器上验证 Forescout 许可证。未在一个月内验证的许可证将被撤销。Forescout 平台将会每天发送一封警告邮件，提醒与服务器之间的通信出错。

  请参阅*《Forescout 安装手册》*了解更多信息。

  请参阅*《Forescout 管理手册》*了解更多关于在单一装置许可模式下许可证管理的信息。

- 如果您的 Forescout 部署正在 ***Flexx Licensing Mode（Flexx 许可模式）***下运行，当许可证权利被创建并可在 Forescout 客户门户获取时，*权利管理员*应该会收到一封电子邮件。可以获取之后，部署的*部署管理员*可在控制台上激活许可证。在许可证被激活之前，将强制执行许可证，因此更改有些控制台配置可能会受到限制。*演示许可证不会在系统安装过程中自动安装。*

  请参阅*《Forescout Flexx 许可操作手册》*了解更多信息。

5.远程管理

iDRAC 设置

集成化戴尔远程访问控制器 (iDRAC) 是一个集成化的服务器系统解决方案，可通过 LAN 或互联网对 CounterACT 装置进行位置独立/操作系统独立的远程访问。使用模块执行 KVM 访问、开启电源/关闭电源/重置以及执行故障排除和维护任务。

执行下列操作，与 iDRAC 模块一起运行：

- 启用并配置 iDRAC 模块
- 将模块连接至网络
- 登录 iDRAC

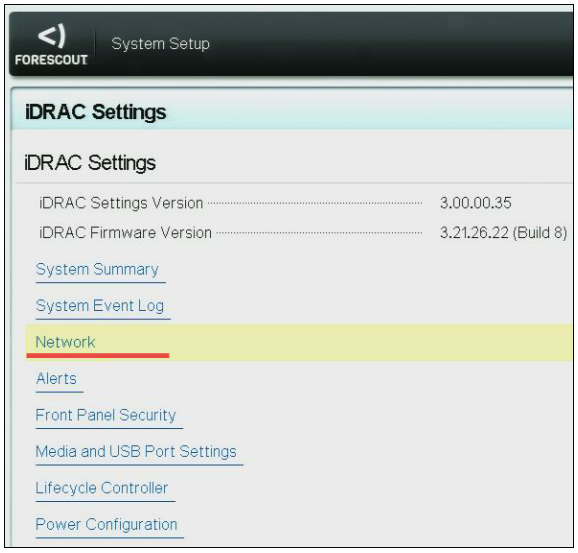
启用并配置 iDRAC 模块

更改 iDRAC 设置，以在 CounterACT 设备上进行远程访问。这个部分描述与 Forescout 平台一起运行所需的基础集成设置。

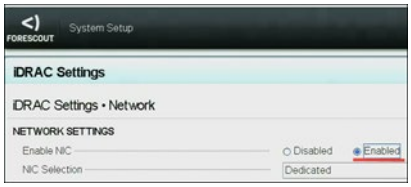
若要配置 iDRAC：

1. 打开管理的装置。
2. 在启动过程中选择 F2。
3. 在 System Setup Main Menu（系统设置主菜单）页面，选择 **iDRAC Settings（iDRAC 设置）**。

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



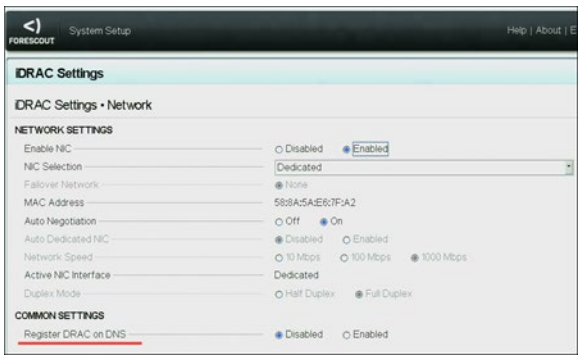
5. 在进行 **iDRAC Settings（iDRAC 设置）** > **Network （网络）**> **Network settings**（网络设置）设置时，验证 **Enable NIC（启用 NIC）**字段是否被设置为 **Enabled（已启用）**。



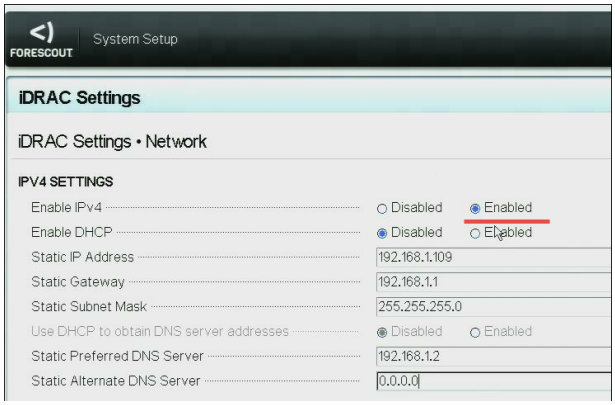
6. （可选）在进行 iDRAC Settings（iDRAC 设置） > Network （网络）> Common Settings（通用设置）设置时，更新动态 DNS：

   a. *将在 DNS 上登记* iDRAC 设置为 ***Enabled（已启用）***。

   b. *在* DNS iDRAC Name （DNS iDRAC 名称） 字段输入动态 DNS。



7. 在进行 iDRAC Settings （iDRAC 设置）> Network （网络）> IPV4 Settings （IPV4 设置）设置时：



- 验证 **Enable IPv4（启用 IPv4）**字段是否被设置为 **Enabled（已启用）**。
- 将 **Enable DHCP（启用 DHCP）**字段设置为 **Enabled（已启用）**，以使用动态 IP 地址。DHCP 将为 iDRAC 自动分配 **IP Address（IP 地址）**、**Gateway（网关）**和 **Subnet Mask（子网掩码）**。

  或

  将 **Enable DHCP（启用 DHCP）**字段设置为 **Enabled（已禁用）**，以使用静态 IP 地址。并在 **Static IP Address（静态 IP 地址）**、**Static Gateway（静态网关）**和 **Static Subnet Mask（静态子网掩码）输入值**。

8. 选择 **Back（后退）**。

9. 在进行 iDRAC Settings （iDRAC 设置）> User Configuration（用户配置）设置时：

为根用户配置下列 User Configuration（用户配置）字段：

- ***Enable User（启用用户）***。验证该字段是否被设置为 **Enabled（已启用）**。

  此配置的用户名与 Forescout 用户名不一样。

- *LAN User Privileges（LAN 用户权利）*请选择 **Administrator（管理员）**。
- *Serial Port User Privilege（串行端口用户权利）请选择* **Administrator（管理员）。**
- *Change Password（更改密码）*。设置用户登录的密码。

10. 选择 **Back（后退）**，然后选择 **Finish（完成）**。确认更改的设置。

配置的设置会被保存，而且系统会重启。

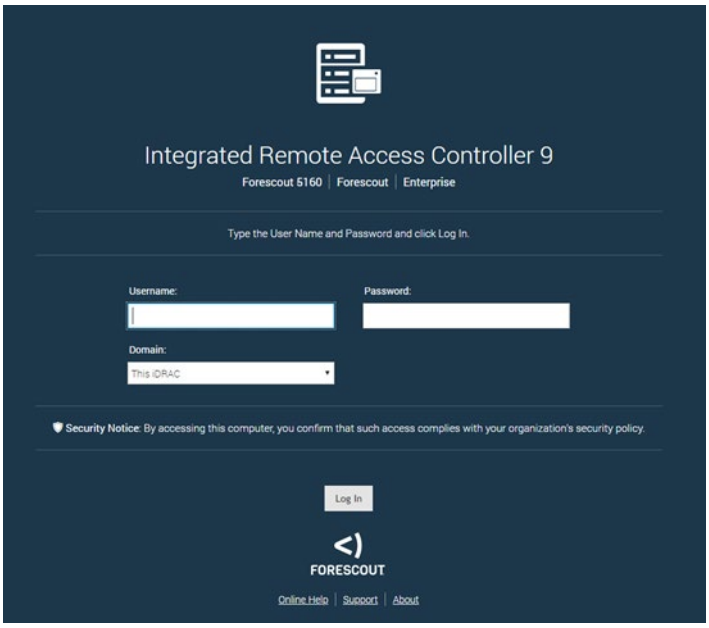
将模块连接至网络

iDRAC 连接至以太网。一般的惯例是将它连接到管理网络。下图显示 CT-1000 装置后面板上的 iDRAC 端口位置：

登录 iDRAC

若要登录 iDRAC：

1. 浏览至在 **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）页面配置的 Username（用户名）和 Password（密码）。
3. 选择 **Submit（提交）**。

更多关于 iDRAC 的信息，请参阅 *《iDRAC 用户手册》*。您的在下列地址访问此手册：

https://forescout.com/company/resources/idrac-9-user-guide/

欲识别您的许可模式：

- 在控制台选择 **Help（帮助） > About Forescout（关于 Forescout）**。

更新默认的 root（根）密码非常重要，如果您还没有更新的话。

6.验证连接

验证管理接口连接

若要测试管理接口连接，登录该装置并运行下列命令：

fstool linktest

则会显示下列信息：

```
管理接口状态
正在 Ping 默认网关信息
Ping 统计数据
正在执行名称解析测试
测试总结
```

执行 Ping 测试

从装置到网络桌面，运行下列命令以验证连接：

Ping <network_desktop_IP_address>

7.设置 Forescout 控制台

安装控制台

控制台是用于查看端点的详细信息并对其进行控制的 Forescout 管理应用程序。此信息由 CounterACT 设备收集。请参阅*《Forescout 管理手册》*了解更多信息。

您必须提供存放 Forescout 控制台应用程序软件的机器。最低硬件要求：

- 非专用机器，运行：
  - Windows 7/8/8.1/10
  - Windows 服务器 2008/2008 R2/2012/2012 R2/2016/2019
  - Linux RHEL/CentOS 7
  - macOS 10.12/10.13/10.14
- 内存 2GB
- 磁盘空间 1GB

可通过下列途径执行控制台安装：

使用装置内置的安装软件。

1. 在控制台计算机上打开浏览器窗口。
2. 在浏览器地址行键入下列地址：

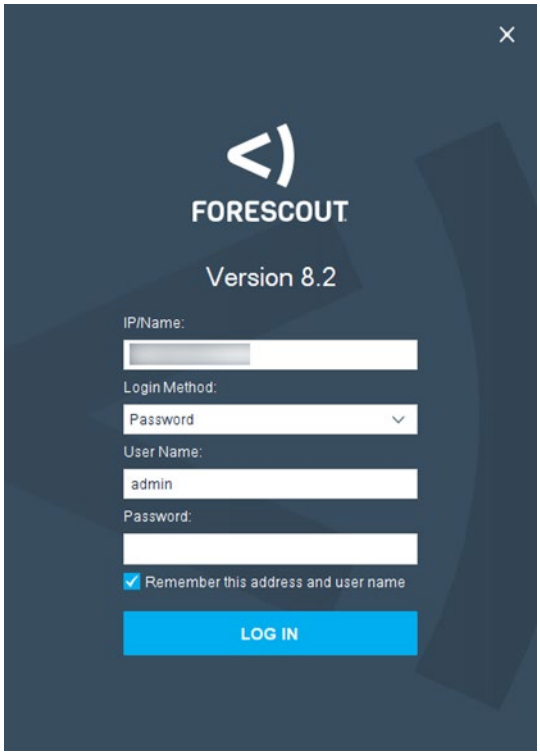
   http://<Appliance_ip>/install

   其中 Appliance_ip 是该装置的 IP 地址。浏览器即会显示控制台安装窗口。
3. 按照界面上显示的提示操作。

登录

安装完成之后，您可以登录控制台。

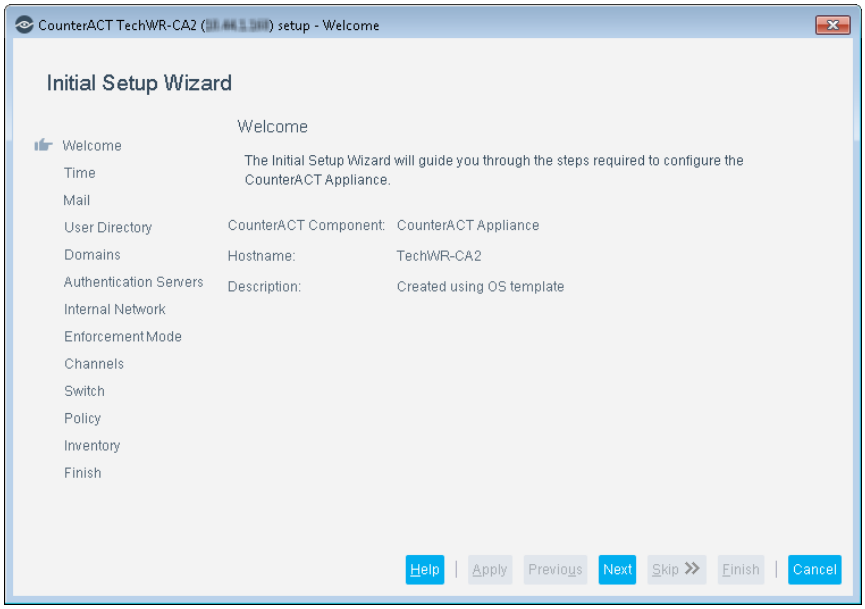
1. 在您创建的快捷方式位置选择 Forescout 图标。



2. 在 **IP/Name（IP/名称）**字段输入装置的 IP 地址或主机名称。
3. 在 **User Name（用户名）**字段，输入管理员。
4. 在 **Password（密码）**字段，输入您在安装装置过程中创建的密码。
5. 选择 **Login（登录）**，启动控制台。

进行初始设置

首次登录时，初始设置向导即会打开。该向导会指导您完成必要的配置步骤，以设置 Forescout 平台并使其快速高效地运行。



开始初始设置之前

在您按照向导操作之前，请准备好下列信息：

向导所需的信息	值
您的组织所使用的 NTP 地址（可选）	
允许发送邮件提醒的内部邮件转发 IP 地址，如果装置不允许 SMTP 流量（可选）	
Forescout 管理员电子邮箱地址	
监控和响应接口	
对于无 DHCP 的分段/VLAN，则是响应接口直接连接的网络分段/VLAN，以及 Forescout 平台在每个此类 VLAN 使用的永久性 IP 地址。	
此装置将监控的 IP 地址范围（所有内部地址，包括未使用的地址）	
LDAP 用户账户信息和 LDAP 服务器 IP 地址	
域凭证，包括域管理账户名称和密码	
验证服务器，这样 Forescout 平台就可以分析已被验证成功的网络主机	
交换机 IP 地址、供应商和 SNMP 参数	

请参阅 *《Forescout 管理手册》*或在线帮助，了解操作向导有关的信息。

其他 Forescout 文档

有关其他 Forescout 功能和模块的信息，请参阅下列资源：

- 文档下载
- 文档门户
- Forescout 帮助工具

文档下载

文档下载可从 Forescout 技术文档页面或两个 Forescout 门户中的其中一个进入，这取决于部署使用的许可模式。

- ***Per-Appliance Licensing Mode（单一装置许可模式）***——产品更新门户
- ***Flexx Licensing Mode（Flexx 许可模式）***——客户门户

也可以从这些门户上下载软件。

欲识别您的许可模式：

- 在控制台选择 **Help（帮助） > About Forescout（关于 Forescout）**。

Forescout 技术文档页面

可通过 Forescout 技术文档页面访问可搜索的文档门户网站，以及转至各类技术文档的 PDF 链接。

若要访问 Forescout 技术文档页面：

- 前往 https://www.Forescout.com/company/technical-documentation/

产品更新门户

产品更新门户提供转至 Forescout 版本发布、基础和内容模块、eyeExtend 产品以及相关文档的链接。该门户同时也提供一系列其他文档。

若要访问产品更新门户：

- 前往 https://updates.forescout.com/support/index.php?url=counteract 并选择您想要了解的版本。

客户门户

Forescout 客户门户的 Downloads（下载）页面提供转至已购买 Forescout 版本发布、基础和内容模块、eyeExtend 产品以及相关文档的链接。如果您拥有软件的许可证权利，软件及相关的文档则会显示在 Downloads（下载）页面。

若要查看 Forescout 客户门户上的文档：

- 前往 https://Forescout.force.com/support/ 并选择 **Downloads（下载）**。

文档门户

Forescout 文档门户是可搜索的、基于网页的文档库，其中包含关于 Forescout 工具、功能和集成的信息。

若要访问文档门户：

- 前往 https://updates.forescout.com/support/files/counteract/docs_portal/ 并使用您的客户支持凭证登录。

Forescout 帮助工具

直接从控制台查看信息。

控制台帮助按钮

使用上下文有关的 *Help（帮助）*按钮，快速查看关于您正在进行的任务或主题的信息。

《Forescout 管理手册》

- 在 **Help（帮助）**菜单中选择 **Administration Guide（管理手册）**。

插件帮助文件

- 安装插件后，选中 **Tools（工具）** > **Options（选项）** > **Modules（模块）**，选中该插件并选中 **Help（帮助）**。

文档门户

- 在 **Help（帮助）**菜单中选择 **Documentation Portal（文档门户）**访问 文档门户。