Stealthwatch® 系统

硬件配置指南

(适用于 Stealthwatch 系统 v6.9.0)

配置指南：Stealthwatch 系统 v6.9.0 设备

记录日期：2017 年 7 月 6 日

思科商标

目录

1

引言

概述

本指南介绍并说明如何配置以下 Stealthwatch® 系统硬件：

- Stealthwatch 管理控制台 (SMC)
- Stealthwatch 流量收集器™
- Stealthwatch 流量传感器™
- UDP 导向器™

本指南假定您已根据 *Stealthwatch 系统硬件安装指南*中的说明安装了硬件。

有关虚拟版 (VE) 产品的配置，请参阅这些虚拟设备（SMC VE 和流量收集器 Ve、流量传感器 VE 和 UDP 导向器 VE) 的安装和配置指南。

阅读本章内容详细了解本指南以及如何联系支持人员（如果需要）。本章包含以下小节：

目标读者

本指南的主要受众是需要配置所有 Stealthwatch 物理设备的管理员。

Stealthwatch 硬件组件

Stealthwatch 系统由若干硬件组件构成，这些组件会收集、分析并提供您的网络信息以提高网络性能和安全性。本部分介绍主要的 Stealthwatch 组件。

Stealthwatch 管理控制台 (SMC) 是 Stealthwatch 的控制中心。它管理、协调、配置和组织系统所有的不同组件。SMC 客户端软件允许您从任何可以访问 Web 浏览器的本地计算机访问 SMC 的用户友好图形用户界面 (GUI)。通过客户端 GUI，您可以轻松访问关于整个企业关键网段的实时安全和网络信息。

SMC：

- 支持多达 25 个 Stealthwatch 流量收集器
- 提供对分布式主机行为数据库的访问
- 支持多个并行用户
- 提供报告计划程序以自动执行定期报告
- 直接向相关人员和多个第三方系统提供事件转发
- 支持与通过 Stealthwatch 行为分析获得的智能关联的系统日志
- 提供图形化图标以直观地显示流量
- 提供深入分析以排除故障
- 提供统一且可定制的报告
- 及时通知安全漏洞

流量收集器

适用于 NetFlow 的 Stealthwatch 流量收集器收集 NetFlow、cFlow、J-Flow、Packeteer 2、NetStream 和 IPFIX 数据以提供具有成本效益且基于行为的网络保护。适用于 sFlow 的流量收集器收集 sFlow 数据。

流量收集器从多个网络或网段聚合高速网络行为数据，以提供端到端保护并跨地理位置分散的网络提高性能。

当流量收集器接收数据时，无论是进行数据包加密还是碎片化处理，它都会识别已知或未知的攻击、内部误用或配置错误的网络设备。Stealthwatch 识别行为之后，系统就可以为这种类型的行为执行任何您配置为要执行的操作(如果有)。

流量收集器：

- 以流量收集器 4000 这一型号为例，每秒可以从最多 100 万台主机处理多达 12 万条流量记录
- 流量收集器 5000 系列每秒可使用超过 4000 台流量导出设备从数百万台主机处理多达 24 万条流量记录
- 从流量导出设备接收流量设备
- 对流程进行重复数据删除并存储双向流量
- 创建和存储主机配置文件，主机对数据，关注 Index™ 事件，接口数据，主机组数据，VM 数据和 TopN 统计信息
- 存储域配置数据
- 将警报转发至 Stealthwatch 管理控制台
- 支持多达 5 台缓解设备

流量传感器

Stealthwatch 流量传感器是一种网络设备，它的操作原理与传统数据包捕获设备或 IDS 类似，因为它可以插入到交换机端口分析器 (SPAN)、镜像端口或以太网测试访问端口 (TAP) 中。流量传感器可以增强对以下网络区域的可视性：

- 不提供流量导出的位置。
- 提供流量导出，但您想更深入地了解性能指标和数据包数据的位置。

通过将流量传感器定向到任何支持 NetFlow v9 或 IPFIX 的流量收集器，您可以从 NetFlow 获得有价值的详细流量统计信息。当与适用于 NetFlow 的 Stealthwatch 流量收集器结合使用时，流量传感器还可以提供对性能指标和行为指标的深入了解。这些流量绩效指标提供对任何由网络或服务器端应用引起的往返时间延迟的了解。

由于流量传感器具有数据包级的可视性，因此它可以计算往返时间 (RTT)、服务器响应时间 (SRT) 和 TCP 会话数据包损失。它在发送给面向 NetFlow 的 Stealthwatch 流量收集器的 NetFlow 记录中包含所有这些附加字段。

UDP 导向器

UDP 导向器具有高速、高性能 UDP 数据包复制器。UDP 导向器对于向各个收集器重新分发 NetFlow、sFlow、系统日志或简单网络管理协议 (SNMP) 陷阱很有用。它可以从任何无连接 UDP 应用接收数据，然后将数据重新传送至多个目标，从而在需要时复制数据。

身份识别设备

Stealthwatch 系统包括身份识别设备思科 ISE(身份服务引擎)，包括思科 ISE-PIC。这些设备通过被动地从用户身份数据库中提取用户身份验证信息来将 IP 地址映射到用户名。SMC 可以无缝管理多个身份识别设备。

使用下表记录配置 Stealthwatch 设备所需的设置。

设置	SMC	流量收集器	流量传感器	UDP 导向器	身份识别设备
主机名					
IP 地址	192.168.1.11*	192.168.1.4*	192.168.1.7*	192.168.1.2*	192.168.1.100*
子网掩码					
网关					
DNS 服务器					
NTP 服务器					
邮件中继					

*这些是默认 IP 地址。流量收集器 sFlow 默认为 192.168.1.5。流量收集器 5000 系列数据库的默认值为 192.168.1.15。

此外，还可以使用以下设置：

端口导出流量数据(通常为 2055)_____

路由器的 SNMP 只读社区字符串_____
_____

如何使用本指南

除本简介之外，我们还将该指南分为了以下章节：

章	描述
配置系统	如何配置设备以开始处理流量数据
验证通信	如何确立和验证 SMC 正在接收 NetFlow 数据以及如何开启 SLIC 威胁源功能
添加身份识别设备	如何添加身份识别设备
启用 SLIC 威胁源功能	如何在 SMC 客户端中启用 SLIC 威胁源功能

缩写

本指南中运用了以下缩写：

缩写	定义
DNS	域名系统(服务或服务器)
dvPort	分布式虚拟端口
ESX	企业服务器 X
GB	千兆字节
IDS	入侵检测系统
IPS	入侵防御系统
IT	信息技术
MTU	最大传输单位
NTP	网络时间协议
OVF	开放式虚拟化格式
SMC	StealthWatch 管理控制台

缩写	定义
TB	兆兆字节
UUID	全局唯一标识符
VDS	vNetwork 分布式交换机
VE	虚拟版
VLAN	虚拟局域网
VM	虚拟机

其他资源

除本指南之外，下列文档和在线资源也可能很有用。

相关文档

有关 Stealthwatch 设备及其安装和配置的信息，请参阅您的 Stealthwatch 文档。有关 Stealthwatch 产品的信息，请在线参阅思科 Stealthwatch。

Stealthwatch 客户社区网站 (http://community.lancope.com) 中提供了其他信息。如果您没有网站的登录访问权限，请给支持人员发送一封请求访问权限的邮件。

Lancope 博客

Lancope 位于 http://www.lancope.com/blog/ 的*威胁内部*博客提供有关 NetFlow、NetFlow 行业和新的 Stealthwatch 功能的重要信息，以及有关如何使用 Stealthwatch 的提示和诀窍。

Lancope 资源 & 高级网络安全工具

有关 Stealthwatch 的详细信息，请转到 Lancope 资源 & 高级安全网络工具站点 https://www.lancope.com/resources。其中包括在线视频库、白皮书和网络研讨会等资源。

联系支持人员

如果需要技术支持人员，请执行以下操作之一：

- 联系您当地的思科合作伙伴。
- 致电 +1 800-838-6574。
- 使用 Stealthwatch 客户社区网站 (http://community.lancope.com) 上的支持表单提交案例

文档反馈

如果您对本文档有任何评论，请通过 support@lancope.com 与我们联系。感谢您提供反馈意见。

2

配置系统

概述

本章提供配置设备以开始处理流量数据的流程。完成本章中的步骤后，安装和配置过程就完成了。

继续执行操作之前，请参阅第 1 页“引言”中的核对表以了解所需的信息。

流程概述

配置 Stealthwatch 系统需要完成本章中介绍的以下过程：

1. 配置单个设备
2. 配置系统
3. 通过设备管理界面进行配置

配置单个设备

每个设备的初始配置是通过设备设置工具来完成的。第一次访问设备时，系统会显示设备设置工具。根据您的系统，您应该先配置流量传感器和流量收集器，然后配置 UDP 导向器，最后再配置 SMC。完成 SMC 的初始设置后，系统设置工具随即打开，然后即可配置 Stealthwatch 系统。

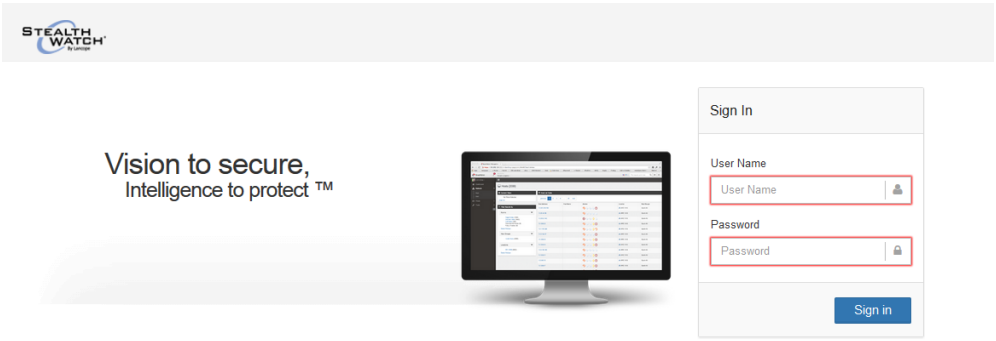
在开始之前，请先收集第 1 页“引言”上“先决条件”部分详细介绍的信息。

注意：取决于环境，您所看到的屏幕与此处展示的屏幕可能略有不同

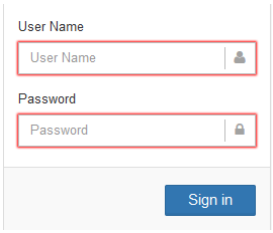
要配置设备，请完成以下步骤：

1. 在浏览器的地址字段中，键入 **https://** 后跟设备的 IP 地址，然后按 **Enter**。
2. 管理登录页面随即打开。键入 **admin** 和 **lan411cope**(两者都区分大小写)，然后点击**登录**。转至步骤 5。

3. 对于 SMC，登录页面将会打开。



要登录，请执行以下操作：



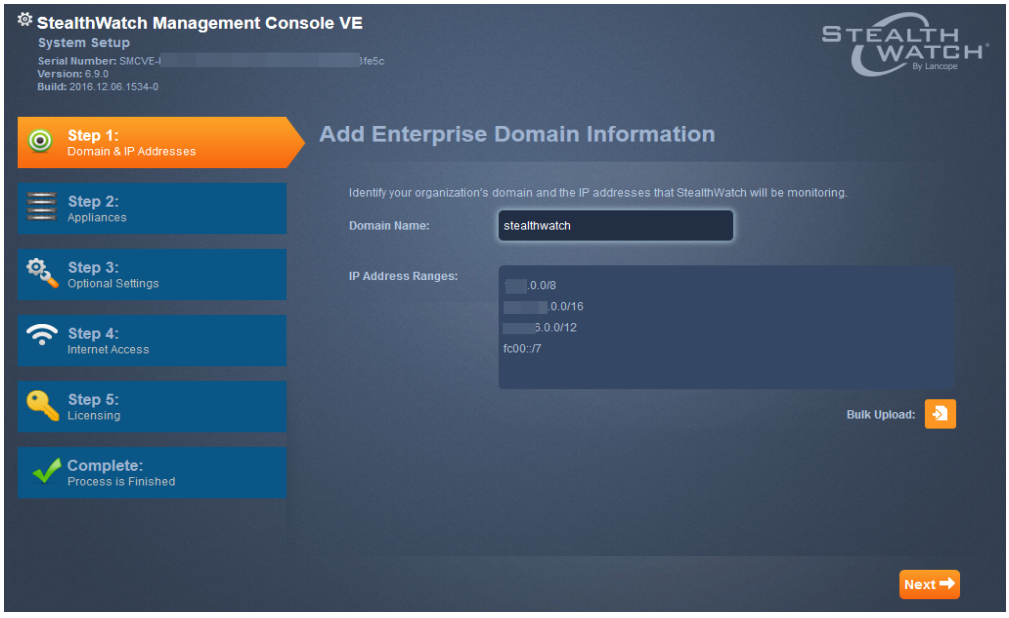
a. 在“用户名”字段中，键入 **admin**。

b. 在“密码”字段中，键入 **lan411cope**。

c. 点击**登录**。

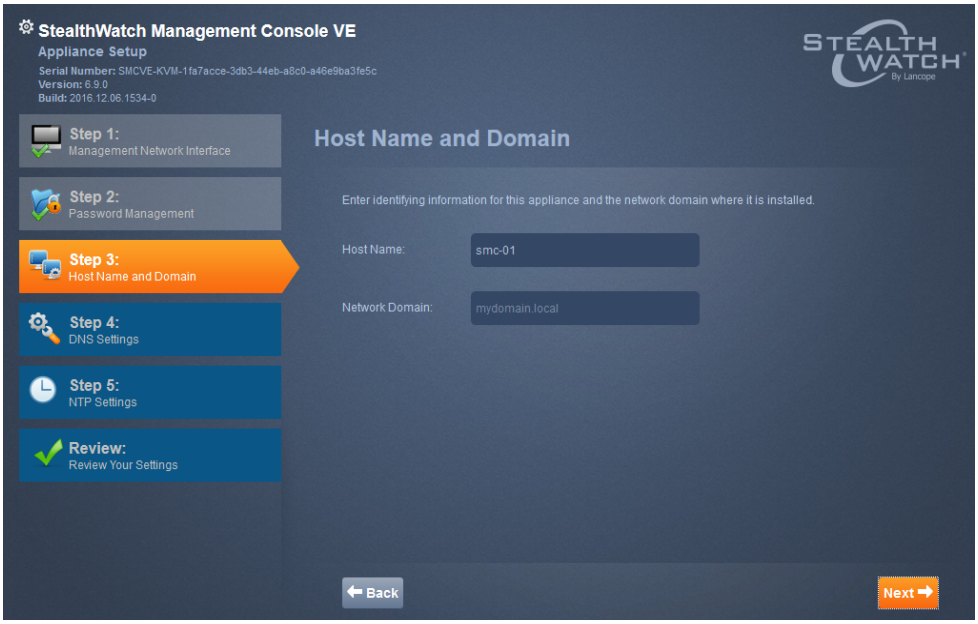
5. “欢迎”页面随即打开。点击**继续**。

“管理网络接口”页面随即打开。

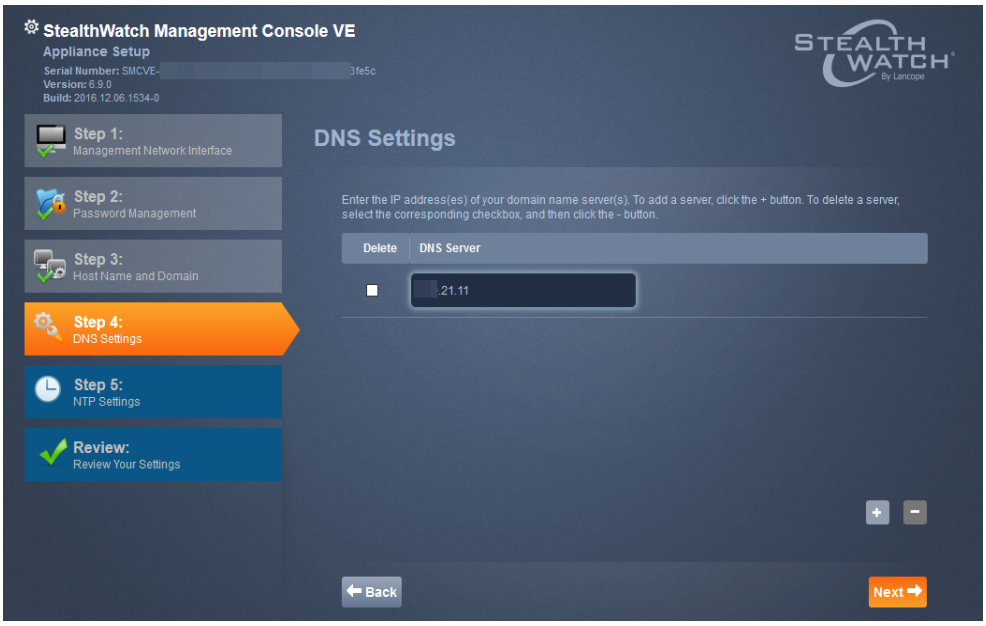


6. 输入设备的 IP 地址，然后点击**下一步**。“密码管理”页面随即打开。

7. 在相应的字段中，键入新的管理密码，然后点击**下一步**。“主机名和域”页面随即打开。



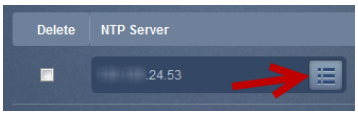
8. 在相应的字段中，键入主机名和网络域名称，然后点击**下一步**。“DNS 设置”页面随即打开。



9. 点击 **+** 按钮，然后键入 DNS 服务器的 IP 地址。点击**下一步**。“NTP 设置”页面随即打开。

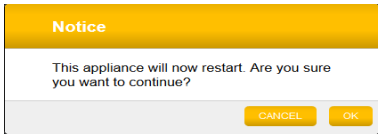
注意：请将第一个 NTP 服务器设置为 pool.ntp.org。这将允许 Stealthwatch 设备访问 NTP 服务器的随机 ntp.org 池，以设置设备的时间。

10. 您可以接受默认设置，也可以输入另一台服务器，方法是输入您的 NTP 服务器的 IP 地址，或通过点击列表图标并从下拉列表中选择一个名称来选择名称。请参阅“通过设备管理界面进行配置”。



11. 点击**下一步**。“审查”页面随即打开。

12. 审查您的设置，然后点击**应用**。确认对话框随即打开。



13. 等待几分钟时间，以便新系统设置生效，然后点击**下一步**。完成后，设备的登录页面随即打开。
14. 输入登录凭证，然后点击**登录**。
15. 您是否还有其他需要配置的设备？
    - 如果有，则返回到第 1 步，并对下一个设备重复此过程。请记住，要最后配置主 SMC。
    - 如果没有，则转至下一步。

16. 配置最后一个或唯一的 SMC 之后，继续下一部分“配置系统”。

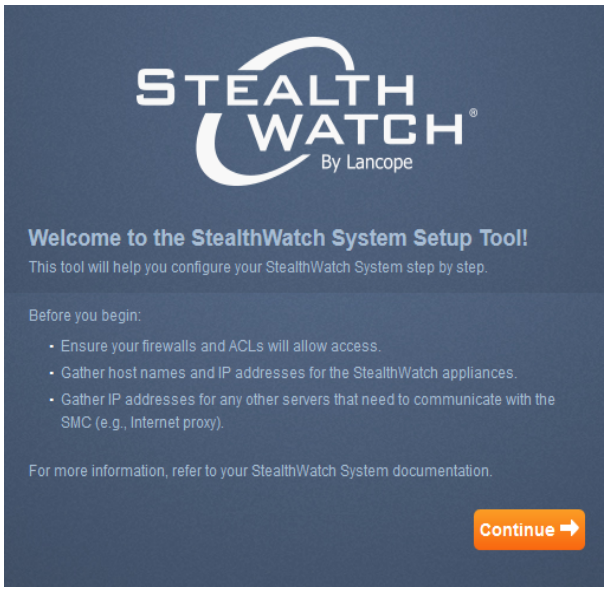
配置系统

完成配置包括 SMC (VE) 在内的所有设备后，即可配置系统。

注意！ SMC 管理的所有设备都必须被激活。否则，SMC 将无法与流量收集器进行通信，系统也无法正确配置。

重要：如果要配置故障切换 SMC，则只需为其系统提供域名，然后单击**下一步**到其余页面。然后，即可在为主 SMC 配置系统时对系统进行设置。

系统设置工具的“欢迎”页面随即打开。



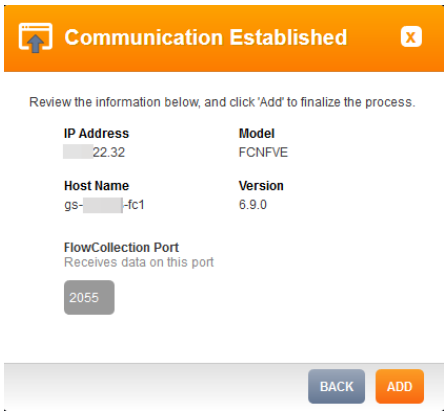
1. 点击**继续**。“添加企业域信息”页面随即打开。

2. 输入系统的 IP 地址范围(您可以使用 CIDR、短横线表示的范围、圆点分隔的子网或 IPv6)或使用批量上传来导入 IP 地址范围的 CSV 文件，然后点击**下一步**。“设备”页面随即打开。

> **注意：**CSV 文件中的 IP 地址必须由下列某种字符分隔：逗号、逗号加空格、空格、回车符。

3. 点击 + 按钮。“添加流量收集器”对话框随即打开。

4. 输入流量收集器 IP 地址，然后点击**下一步**。“通信”对话框随即打开：



条件过程：在此步骤中添加流量收集器或流量传感器时，首先必须已在流量收集器或流量传感器和 Stealthwatch 管理控制台 (SMC) 之间创建管理通道。如果尚未执行此操作，则系统将在该过程进行到此阶段时显示一条错误消息。要为每个流量收集器和流量传感器创建管理通道，请完成以下步骤：

1. 使用您的浏览器和设备的 IP 地址登录到适用的设备管理界面。
2. 在左侧导航窗格中，点击**配置 > 管理系统配置**。
3. 点击**添加新管理系统**。
4. 在“管理系统 IP 地址”字段中，键入 SMC 的 IP 地址。
5. 选中**是 SMC** 复选框。
6. 点击**应用**。
7. 在系统设置工具的“错误”对话框中，点击**取消**，然后点击**应用**。

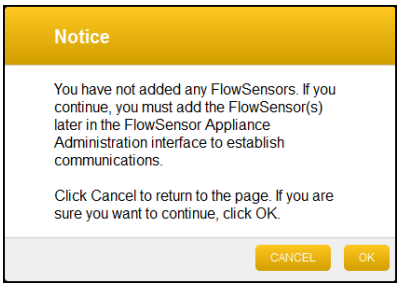
5. 点击**添加**。流量收集器将添加至系统：

6. 点击**下一步**。“设备流量传感器”页面随即打开。

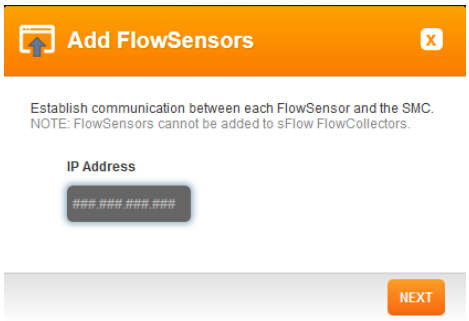
7. 您是否有要添加的流量传感器？

   - 如果有，请点击 **+** 按钮，然后转到第 9 步。
   - 如果没有，请点击**下一步**转到下一步。

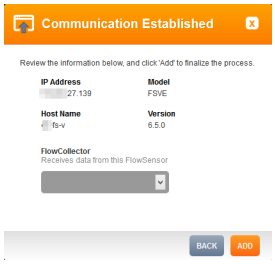
8. 警告消息随即显示。点击**确定**。转到步骤 14。



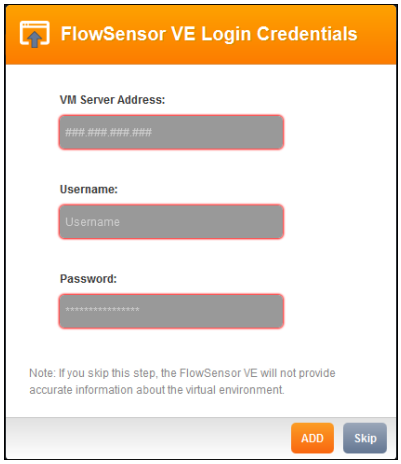
9. 点击 **+** 按钮。“添加流量传感器”对话框随即显示。



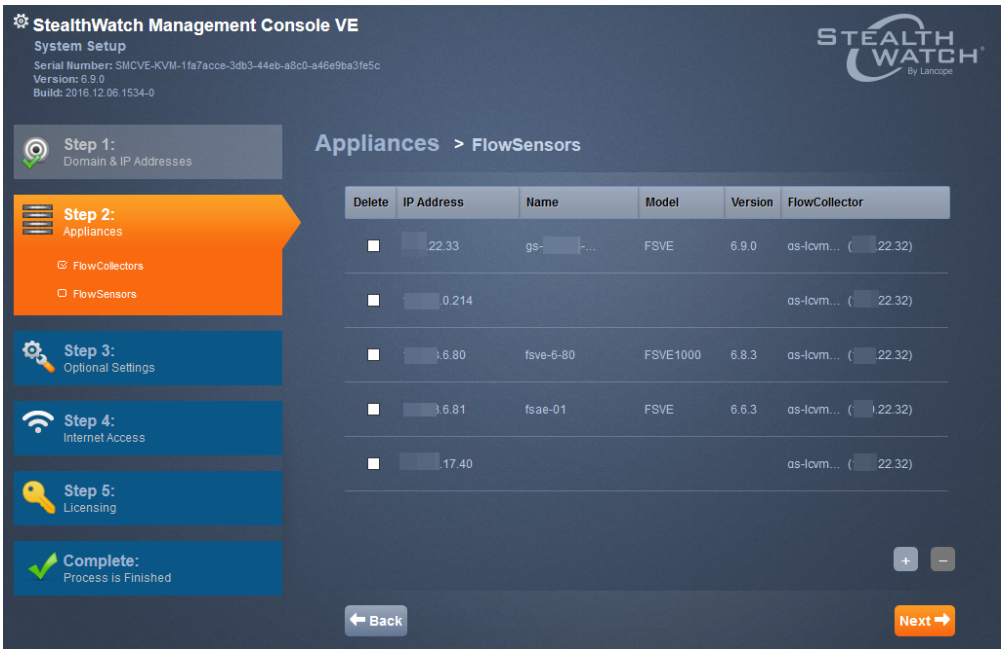
10. 键入 IP 地址，然后点击**确定**。“通信已建立”对话框随即显示。



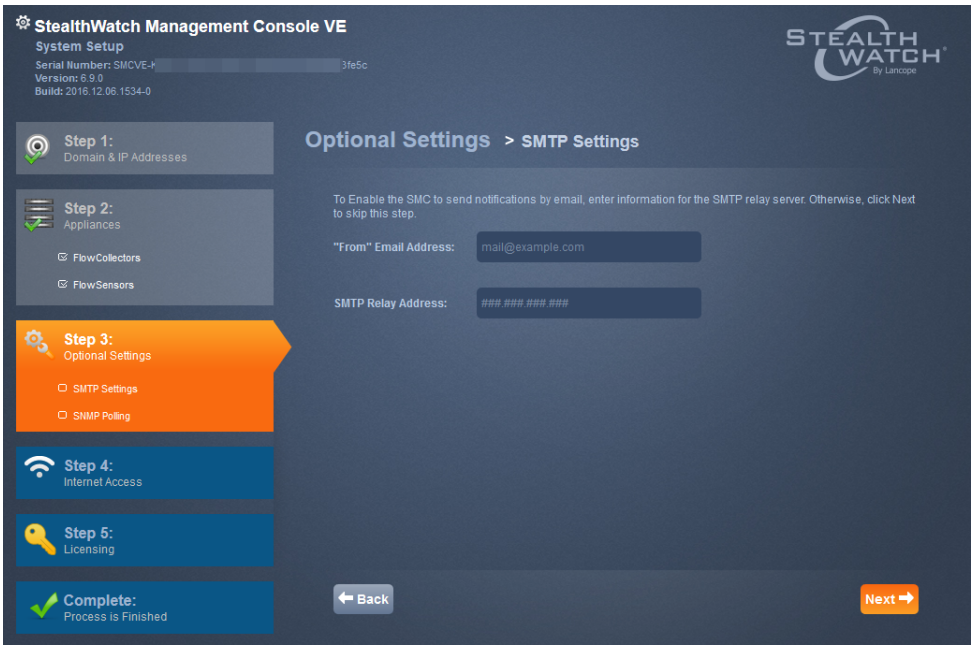
11. 从下拉列表中选择一个流量收集器，然后点击**添加**。



流量传感器已添加。



12. 点击**下一步**。“SMTP 设置”页面随即打开：

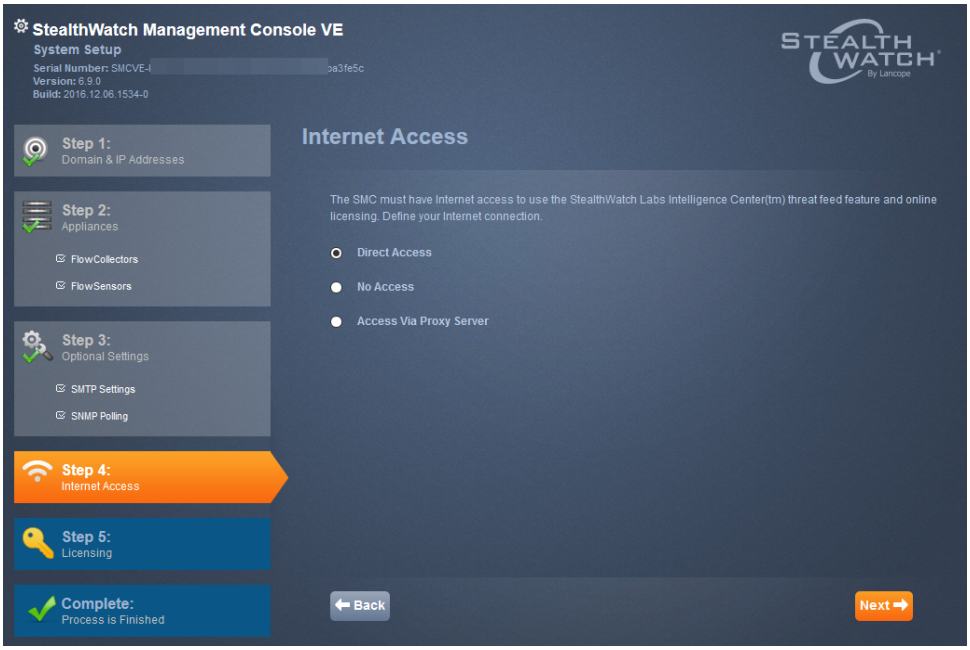


13. SMC 发送邮件时，请在“发件人”字段中输入所需的邮件地址。
14. 输入 SMTP 中继地址，然后点击下一步。“SNMP 设置”页面随即打开：

15. 如有必要，请修改设置(此处只能设置一个字符串)，然后点击**下一步**。

> **注意：**如果选择“SNMP 版本 3”，则必须输入用户名，然后才可以选择选项“身份验证”和“加密”。

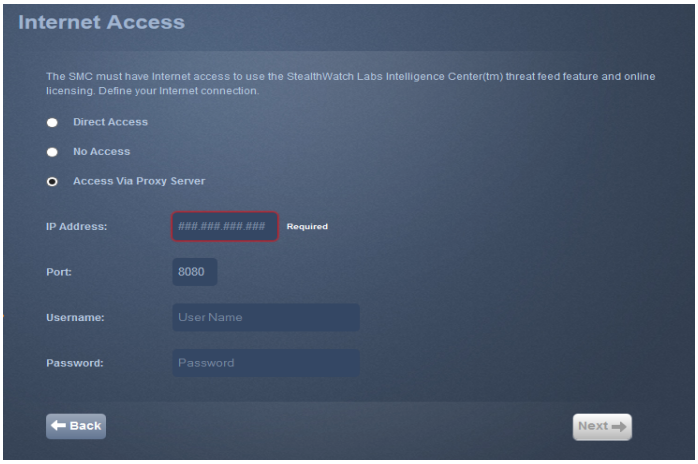
16. “互联网访问(SMC)”页面随即打开。



17. 选择合适的互联网访问类型：

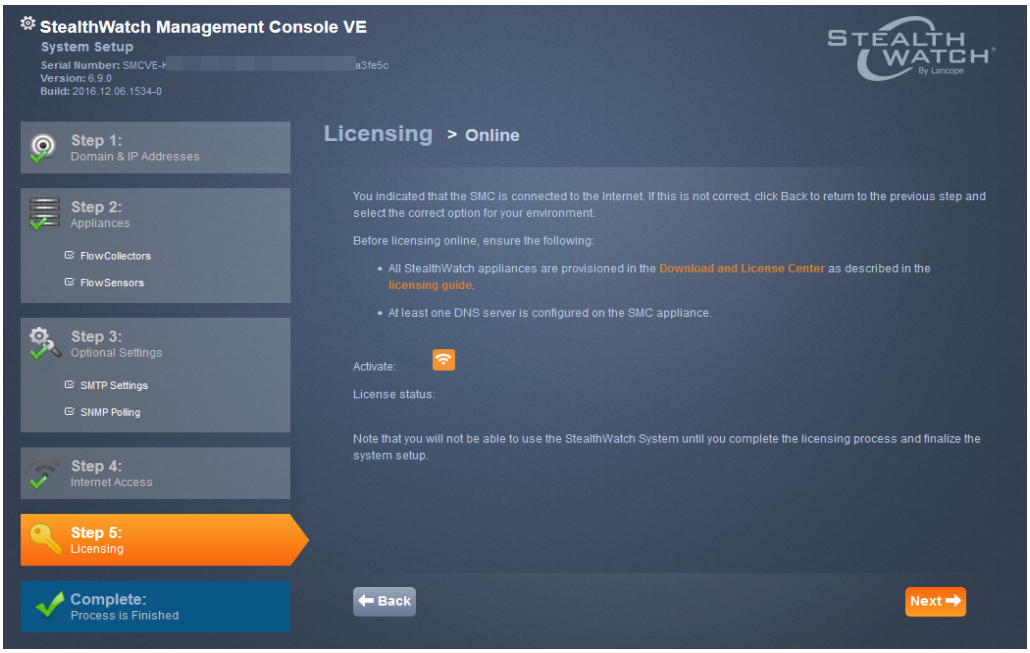
- **不访问**：您的 SMC 不会连接到互联网。您必须获取访问权限才能从下载和许可中心获得许可证。点击“脱机”页面上的**下一步**打开“完成”页面。

- **通过代理服务器访问**：您的 SMC 通过代理服务器连接到互联网。代理设置随即显示。



完成代理服务器的设置，然后点击**下一步**。

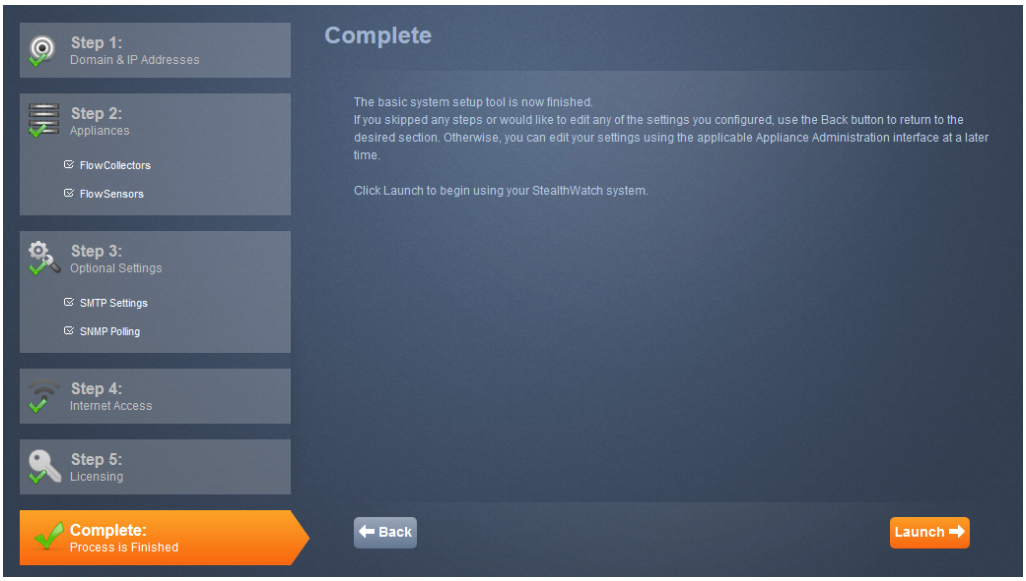
20. 如果选择了“直接访问”或完成了代理设置，“许可”页面随即打开：



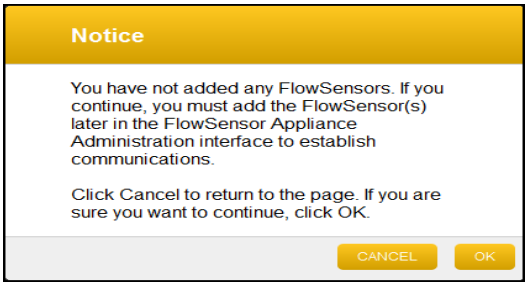
21. 点击“下载和许可中心”链接。获取 *下载和许可 Stealthwatch 产品*文档中所述的许可证。
22. 获取许可证后，点击**激活**。

> **注意：**如果设备未注册，系统会显示一条消息。

23. 点击**确定**。“完成”页面随即打开。



24. 点击**启动**转到 SMC 客户端登录页面。一条消息随即显示。如果您尚未获得设备许可，则会收到一条消息，向您提供与尚未获得许可的设备相关的信息。下面是一个示例消息：



25. 从右上角的“欢迎管理用户”下拉列表中点击**管理设备**打开设备管理界面，然后继续下一部分第 25 页“通过设备管理界面进行配置”。

26. 您是否有 UDP 导向器？

- 如果有，请继续下一部分“从 SMC 配置 UDP 导向器”。
- 如果没有，请继续“通过设备管理界面进行配置”部分。

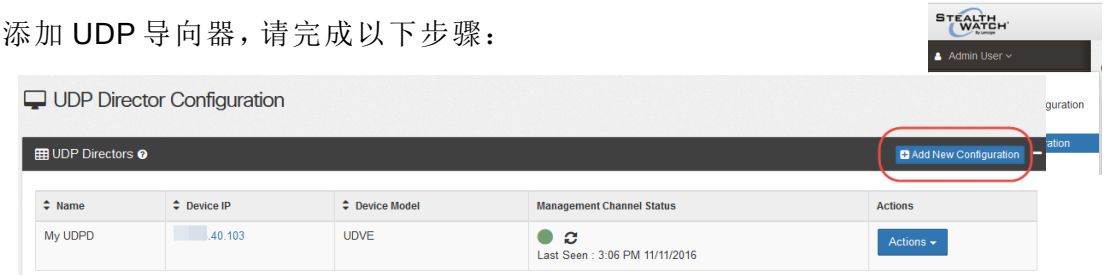
从 SMC 配置 UDP 导向器

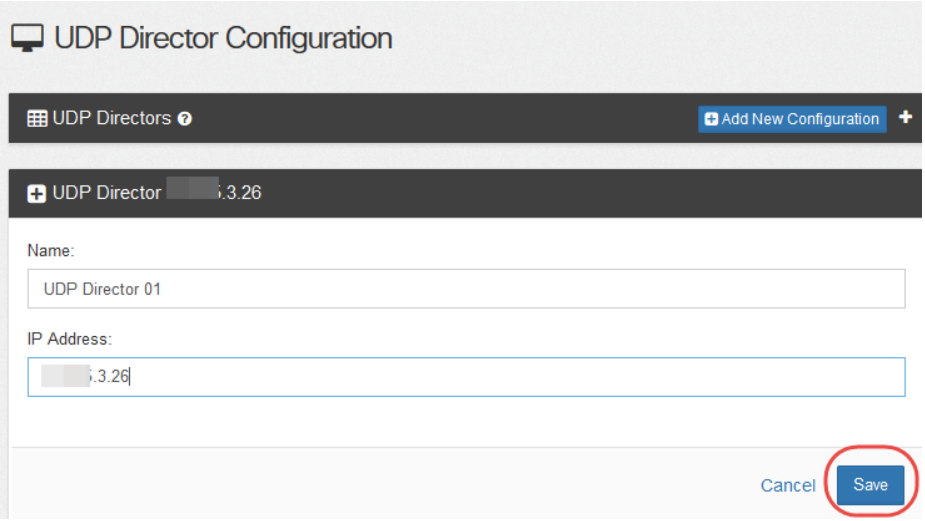
如果您的 Stealthwatch 系统中有 UDP 导向器，则可以从 SMC Web App 配置，以便 SMC 管理 UDP 导向器。要从 UDP 导向器本身进行管理，请参阅“配置 UDP 导向器规则”。

注意：SSL 用于从 UDP 导向器向 Stealthwatch 管理控制台 (SMC) 发送消息。

添加 UDP 导向器

要添加 UDP 导向器，请完成以下步骤：

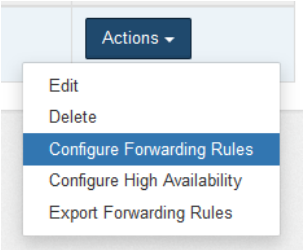




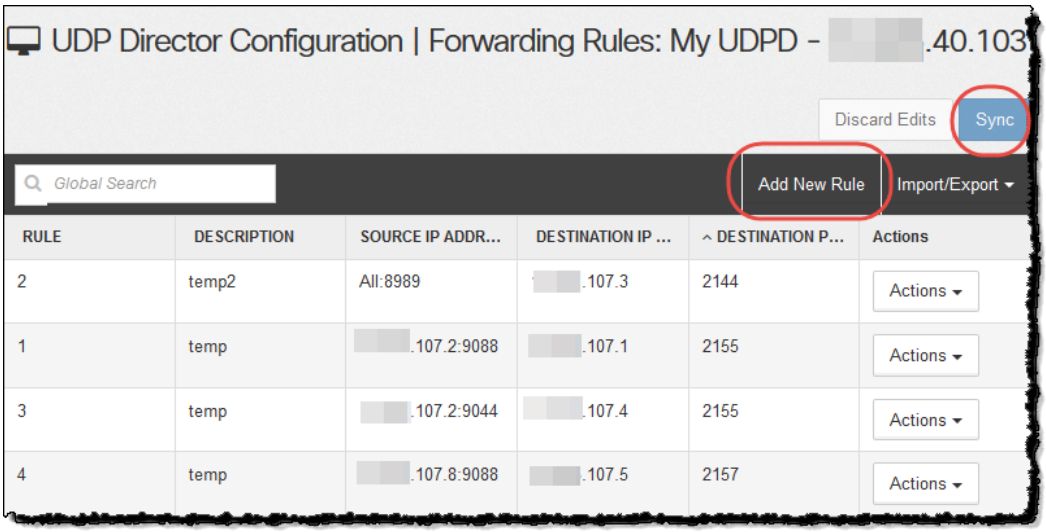
配置转发规则

添加 UDP 导向器后，您就可以为其配置转发规则了。

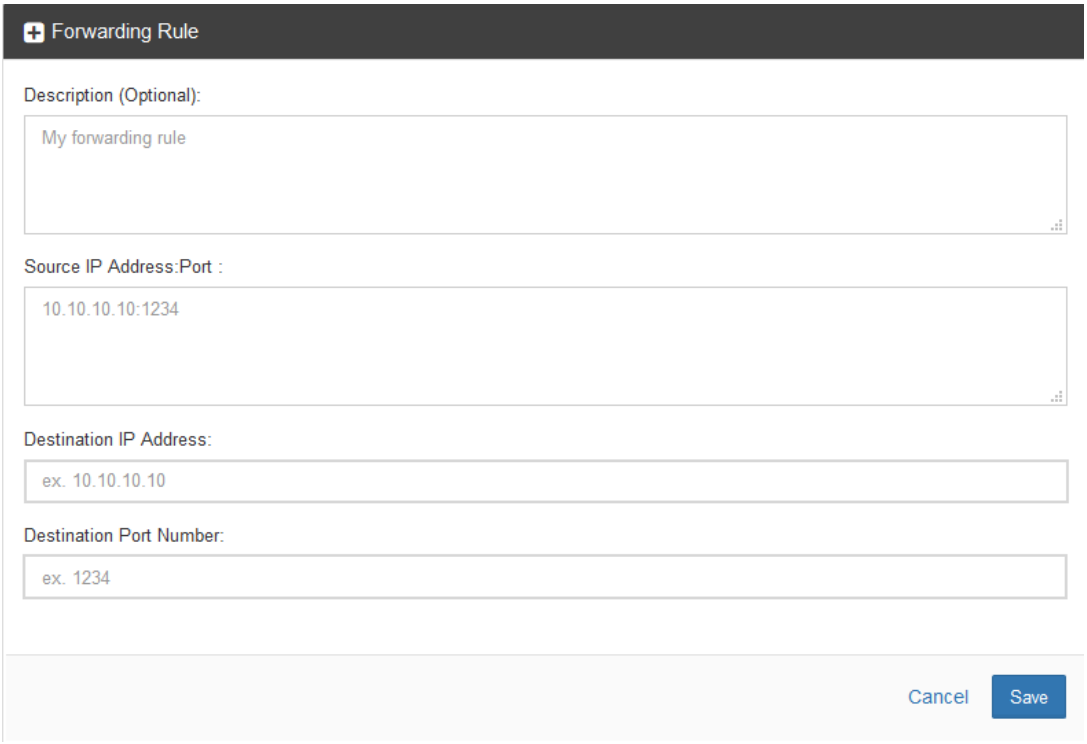
要为 UDP 导向器配置转发规则，请完成以下步骤：



1. 选择**操作 > 配置转发规则**。“转发规则”页面随即打开。



2. 点击**添加新规则**。



3. 在“说明”字段中，输入识别该规则的简短说明。
4. 在“源 IP 地址:端口列表”字段中，键入向 UDP 导向器发送数据的设备的 IP 地址，后跟通过其发送数据的端口号。

注意：

- 使用语法 [IP 地址]:[端口号]，如以下示例中所示。
- 您可以使用无类别域间路由 (CIDR) 表示法来输入一系列 IP 地址。
- 您可以键入“All”，在该端口上接受来自任何源 IP 地址的数据。
- 您可以将“源 IP 地址:端口”组合添加到新行中，从而在规则内添加这些组合。

示例：

- 10.11.16.38：5322
- 192.168.0.0/16:9000
- All:2055

5. 在“目标 IP 地址”字段中，输入从 UDP 导向器接收数据的设备的 IP 地址。
6. 在“目标端口号”字段中，输入接收设备的端口号。
7. 点击**保存**。新规则将添加到“转发规则”页面上的表格中。
8. 是否确定要同步更改？

a. 如果要同步，请点击页面顶部的“同步”按钮。系统会保存新规则。

b. 如果不同步，请点击页面顶部的“弃用编辑”按钮。如果屏幕上显示“配置”对话框，请点击**是**。

8. 根据需要重复该过程，以添加转发规则。
9. 继续下一部分“通过设备管理界面进行配置”。

注意：如果您希望有一个辅助 UDP 导向器，则必须已添加导向器且带有至少一条转发规则。首先您需要配置主 UDP 导向器，然后对辅助导向器重复该配置过程。有关配置 HA 设备的说明，请转到第 33 页“配置主 UDP 导向器 HA”。

通过设备管理界面进行配置

本部分提供以下过程，以通过其设备管理界面来完成虚拟设备的配置：

1. 登录设备管理界面
2. 配置系统时间
3. 配置系统
4. 配置 UDP 导向器 HA
5. 重新启动设备

登录设备管理界面

要登录设备管理 (Admin) 界面，请完成以下步骤：

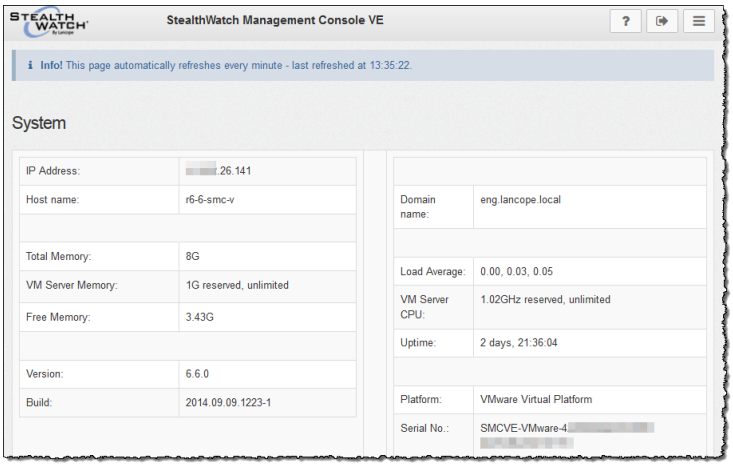
注意：

- Stealthwatch 支持的浏览器是 Internet Explorer 9 及更高版本，以及 Firefox 3 及更高版本。
- 如果在加载任何页面时遇到问题，请清除浏览器缓存，关闭浏览器并重新打开，然后再次登录。

1. 在浏览器的地址字段中，键入 **https://**，再键入设备的 IP 地址，然后按 **Enter**。
2. 您是否在打开 SMC 设备管理界面？
   - 如果是，“登录”页面将会打开。点击右上角的“设置”图标，然后点击**管理设备**。

- 如果不是，则虚拟设备“登录”页面将会打开。

3. 在**用户名**字段中，键入 **admin**。
4. 在**密码**字段中，键入在设备设置中创建的管理密码。
5. 点击**登录**。设备管理界面主页将会打开。



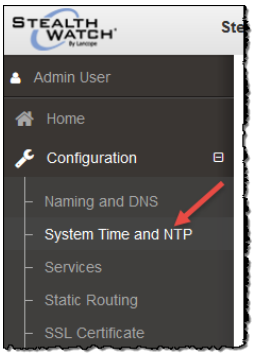
6. 继续下一部分“配置系统时间”。

配置系统时间

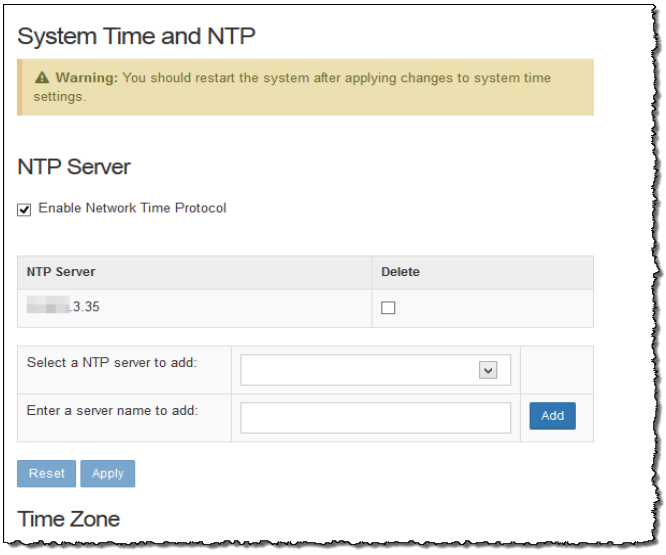
要配置设备上的网络时间协议 (NTP) 和系统时间(时区)设置，请完成以下步骤：

注意！ 使用与用于流量收集器及向 SMC 提供信息的其他设备相同的 NTP 服务器。如果您有流量收集器 5000 系列设备，请在数据库和引擎中配置 NTP 和系统时间设置，以使它们相同。

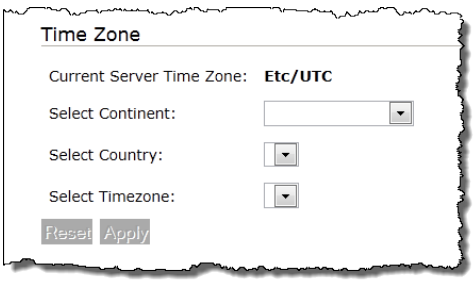
1. 在设备管理界面导航窗格中，点击**配置**旁边的加号 (+)，然后点击**系统时间和 NTP**。



“NTP 服务器”页面将会打开，其中显示您使用设备设置工具在初始配置中设置的 NTP 服务器。



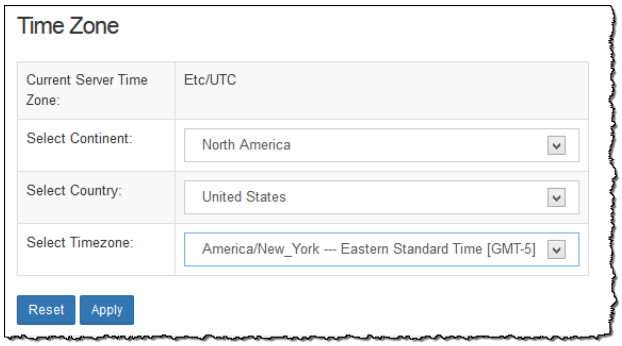
2. 向下滚动到该页的“时区”部分以配置设备系统时间。



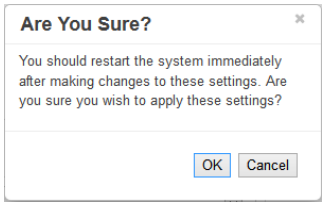
3. 执行以下操作：

   - 从下拉列表中选择“大陆”。
   - 从下拉列表中选择“国家/地区”。
   - 从下拉列表中选择“时区”。

   “应用”通知随即显示。



4. 点击**应用**以使更改成为永久更改。确认窗口随即打开。



5. 点击**确定**。

6. 您是在配置流量传感器还是 UDP 导向器？

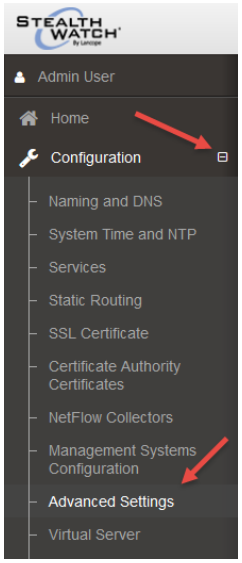
   - 如果在配置流量传感器，请继续下一部分 配置流量传感器 。
   - 如果在配置 UDP 导向器，请继续 配置 UDP 导向器规则 部分。
   - 如果二者都不是，请继续重新启动设备部分。

配置流量传感器

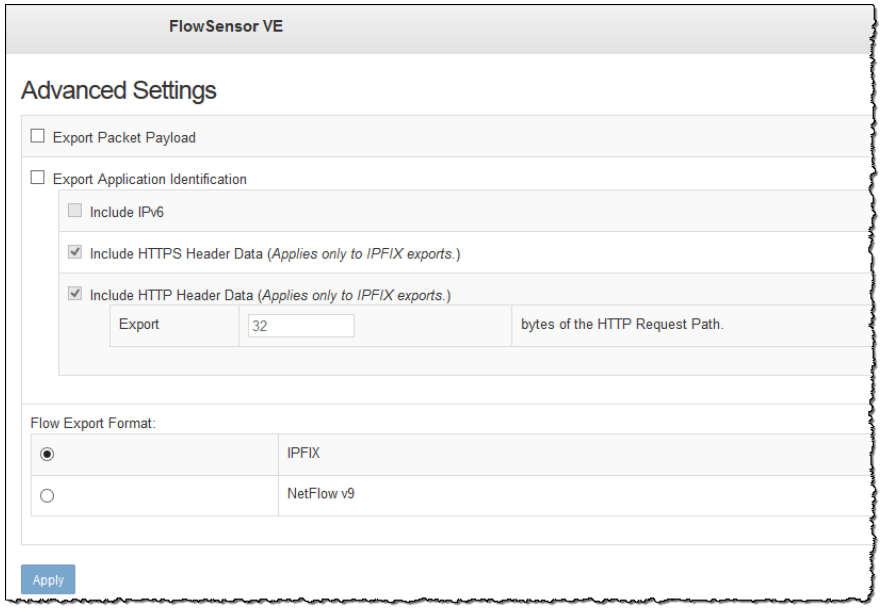
流量传感器的配置需要增加一个步骤，即配置应用 ID 和负载。

要配置流量传感器如何导出应用标识和负载数据，请完成以下步骤：

1. 在导航页中，点击“配置”菜单旁边的加号，然后点击**高级设置**。



“导出设置”页面随即打开。



2. 选择适用于您的网络的设置：

项目	说明
导出数据包负载	允许您指定流量传感器在其发送至收集器的数据中是否包含二进制负载数据的前 26 个字节。
导出应用标识	允许您指定流量传感器在向收集器发送数据之前是否尝试识别应用。此外，必须启用此设置，下列设置才会生效： **包括 IPv6** - 允许您指定流量传感器是否分析 IPv4 和 IPv6 数据包。禁用此设置时，流量传感器仅分析 IPv4 数据包。 **导出 HTTPS 报头数据** - 允许您指定流量传感器在其发送至收集器的数据中是否包含 HTTPS 流量的报头。数据中包含 SSL 公共名称和 SSL 组织名称。此设置需要将“流类型”设置为 IPFIX。最大值为 256 字节。 **导出 HTTP 报头数据** - 允许您指定流量传感器在其发送至收集器的数据中是否包含 HTTP 流量的报头。选中此设置时，可通过一个辅助字段来指定流量传感器纳为流量数据一部分的 HTTP 路径(以字节为单位) 的最大长度。此设置需要将“流类型”设置为 IPFIX。
流导出格式	允许您指定流量传感器是使用 IPFIX 还是使用 NetFlow v9 将流量数据发送到收集器。
缓存模式	允许您选择以下设置之一： **为所有监控端口使用单个共享缓存 -** • 当存在非对称路由时使用。 • 应用和延迟计算的单状态表。 • 使用较少内存。 • 降低整体 pps 处理速率。 • 导致在多个接口上创建一个 NetFlow 事件。 • 仅当流量传感器只有两个端口并且通过 TAP 连接时使用 **为每个监控端口使用独立缓存 -** • 允许跨每个流量传感器接口对数据包进行重复数据删除。 • 使用较多内存。 • 提高整体 pps 处理速率。 • 每个接口保持自己的延迟和应用数据库。 • 为发现给定数据包的每个接口生成唯一的 NetFlow 记录。

3. 点击 **应用** 保存设置。
4. 继续第 35 页“重新启动设备”部分。

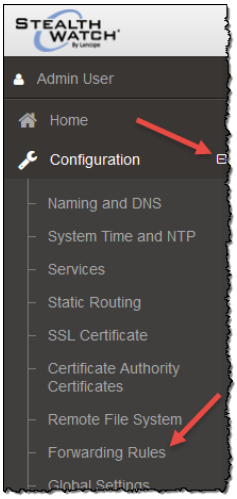
配置 UDP 导向器规则

如果您不是从 SMC 管理 UDP 导向器，则可以在“设备管理”页面上配置转发规则。对于 UDP 导向器，您需要将导出器配置为将要转发的流量发送至 eth0 的 IP 地址。然后，UDP 导向器将从 eth0 转发这些流量，同时为转发的数据包保留每个导出器的原始 IP 和 MAC 地址。

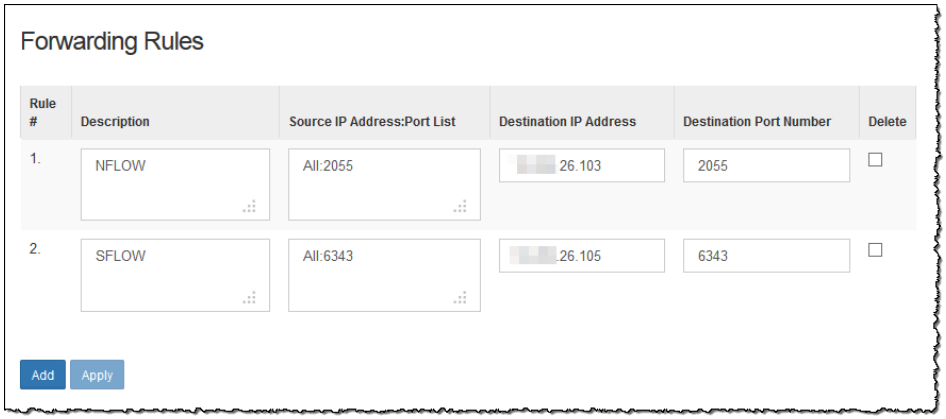
注意：对于混乱的接收，Lancope 建议您对所有感兴趣的流量使用跨越过滤器。网络必须允许正在使用的端口上的流量从导出器传输至 UDP 导向器，然后再传输至接收器 (ACL)。

要为 UDP 导向器配置规则，请执行以下步骤：

1. 在导航窗格中，点击**配置**旁边的加号 (+)，然后点击**转发规则**。



“转发规则”页面随即打开。



2. 在“说明”字段中，输入规则说明。
3. 在“源 IP 地址:端口列表”字段中，键入向 UDP 导向器发送数据的设备的 IP 地址，然后键入通过其发送数据的端口号。使用以下语法：

[IP 地址]:[端口号] as in 10.201.1.41:2057

注意：

- 要从特定端口接收来自任何设备的所有流量，请键入 **All:[端口号]**。例如，键入 **All:3123**
- 您还可以使用 CIDR(无类别的域间路由)符号来输入 IP 地址范围。例如，键入 **172.200.1.0/16:9000**

提示：

- 尽可能为输入使用“All”或 CIDR 范围来限制引擎所需的解析量。为输入使用许多单独的 IP 地址会使引擎更加努力地工作。
- 此外，还可以为输入流量使用替代端口，然后将该流量重定向到所需的输出端口。例如，您无需将端口 55431 的所有流量都发送至一个规则，而是可以将这些流量分开，方法是让之前使用端口 55431 的导出器的 1/3 改用虚拟端口 44440。然后，可以让 1/3 的导出器使用端口 44441，剩余 1/3 的导出器使用端口 44442。然后，将端口 44440、44441 和 44442 的所有流量重定向到单个目标端口 55431。

4. 要添加另一个条目，请按 **Enter** 并键入下一个 IP 地址和端口号。
5. 在“目标 IP 地址”字段中，键入从 UDP 导向器接收数据的设备的 IP 地址。
6. 在“目标端口号”字段中，键入接收设备的端口号。
7. 如果有多个设备将数据发送到 UDP 导向器以转发至其他接收设备，请点击**添加**。

   显示新行，您可以在其中输入设置。重复此步骤，直到为此 UDP 导向器输入所有设备为止。

8. 完成后，点击**应用**。“UDP 导向器配置”屏幕随即会刷新，系统也随即会更新配置文件。所有错误都会显示在屏幕顶部。
9. 您是否在配置 UDP 导向器 HA?

   - 如果是，请继续下一部分 配置 UDP 导向器 HA。
   - 如果不是，请继续第 35 页“重新启动设备”部分。

配置 UDP 导向器 HA

UDP 导向器高可用性允许用户配置冗余 UDP 导向器 2000 设置。两个节点都是完全冗余节点，但一次只有一个节点在线。在线节点在对中称为主节点，而离线节点为辅助节点。如果对中的主节点发生故障，辅助节点取而代之成为主节点。

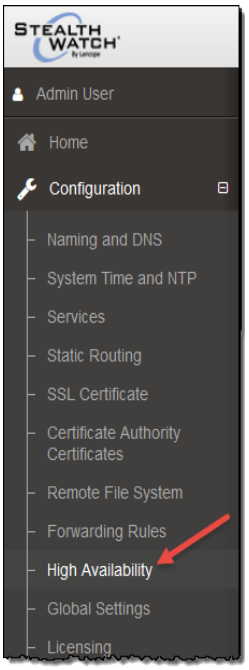
重要：对于 HA 系统中的 UDP 导向器，必须有至少一个规则。如果已为 UDP 导向器配置了规则，建议导出(保存规则配置文件)UDP 导向器规则，然后将文件导入到第二个 UDP 导向器，以确保每个导向器的规则匹配。

您首先需要配置主 UDP 导向器，然后对辅助导向器重复此配置过程。如果两个 UDP 导向器都是新的，则必须遵循本指南中每一部分的步骤操作。但如果辅助导向器已配置为 Stealthwatch 系统上的设备，则只需登录到辅助 UDP 导向器并按照此处所述配置其 HA 组件。

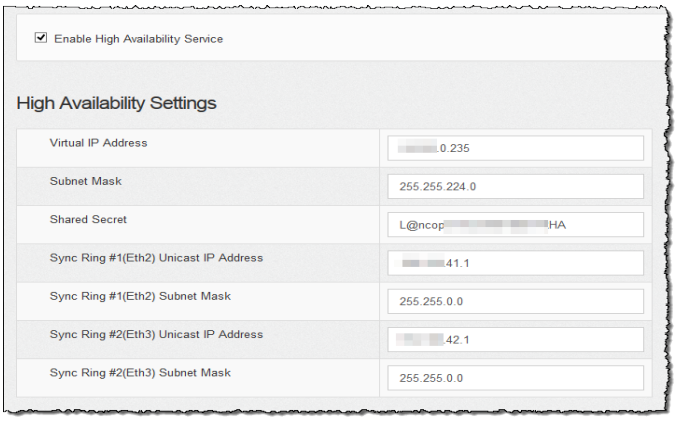
配置主 UDP 导向器 HA

要配置主 UDP 导向器，请执行以下步骤：

1. 在 UDP 导向器管理界面的导航窗格中，点击**配置**旁边的加号 (+)，然后点击**高可用性**。



2. 在“启用高可用性集群”页面上，选择中“高可用性设置”中的“启用高可用性”复选框。



3. 在“虚拟 IP 地址”和“子网掩码”字段中，输入主 UDP 导向器的 IP 地址。(辅助导向器的 IP 地址与之相同)。

> **注意：**虚拟 IP 地址应与单播地址位于同一子网。

4. 在“共享密钥”字段中，为两个 UDP 导向器键入一个字符串。(这将被加密以便安全传输。)
5. 在“同步环 1 (Eth2)单播 IP 地址”的字段中，输入 IP 地址和子网掩码。(单址广播 IP 地址标识单个网络目标。)
6. 在“同步环 2 (Eth3)单播 IP 地址”的字段中，输入 IP 地址和子网掩码。

> **注意：**每个 IP 地址(eth0、eth02、eth03)都必须位于其自己单独的单播子网中。

7. 在查看该设置后，点击**应用**设置配置。
8. 继续下一部分以配置集群的第二个 UDP 导向器。

配置辅助 UDP 导向器 HA

要配置辅助 UDP 导向器，请执行以下步骤：

1. 登录到 HA 对的辅助 UDP 导向器 2000 的设备管理界面。
2. 使用配置第一个设备时每个字段完全相同的值配置此屏幕上的所有参数(包括在第一个设备上可能已更改的所有高级参数)，但以下参数除外：

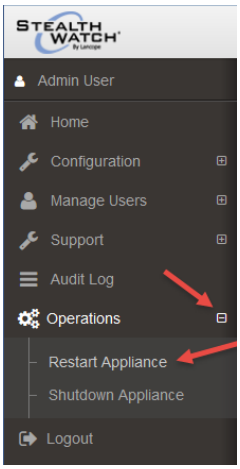
   - 同步环 1 (Eth2) 单播 IP 地址 - 在主要设备上的此字段中您配置的项输入其他 IP 地址，但是此地址必须与主要设备上提供的“同步环 1 单播”地址在同一个子网中。
   - 同步环 2 (Eth3) 单播 IP 地址 - 在主要设备上的此字段中您配置的项输入其他 IP 地址，但是此地址必须与主要设备上提供的“同步环 2 单播”地址在同一个子网中。

3. 点击**应用**保存更改，并在此设备上启动集群服务。
4. 点击“升级”按钮指定主设备。
5. 继续下一部分。

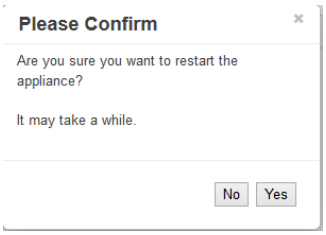
重新启动设备

要重新启动设备，请执行以下步骤：

1. 在设备管理界面菜单上，选择**操作 > 重新启动设备**。



确认对话框随即打开。



2. 点击 **Yes**。
3. 您是否配置了流量收集器？
   - 如果是，请继续下一章“验证通信”。
   - 如果没有，则转至下一步。
6. 您是否配置了流量传感器或 UDP 导向器？
   - 如果是，恭喜您，您现在已经完成了设备的安装和配置！ 重新启动后，流量传感器将开始从 VM 环境收集数据并将其发送到 NetFlow 收集器。重新启动后，

UDP 将开始收集数据并将其发送到配置的目标。

- 如果没有，则转至下一步。

7. 您是否有身份识别设备？

   - 如果有，请转至下一章“添加身份识别设备。
   - 如果没有，则转至下一步。

8. 您是否有 SLIC 功能？

   - 如果有，请转至“启用 SLIC 威胁源功能”一章。
   - 如果没有，恭喜您，您已经完成了 SMC 的配置。重新启动后，系统将开始与流量收集器进行通信。

3

验证通信

概述

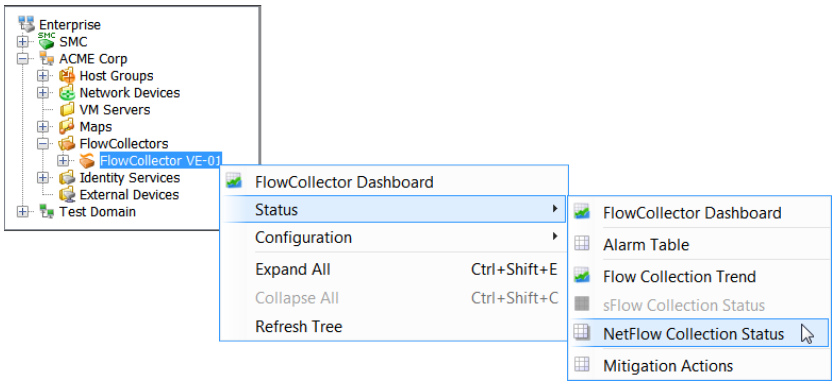
在您许可 Stealthwatch 设备后，您必须验证您正在接收 NetFlow 数据。要验证，请完成本章中详细介绍的以下步骤：

注意！ 完成前一节中的所有授权过程后，在开始执行本节中的过程之前，请等待 30 分钟。

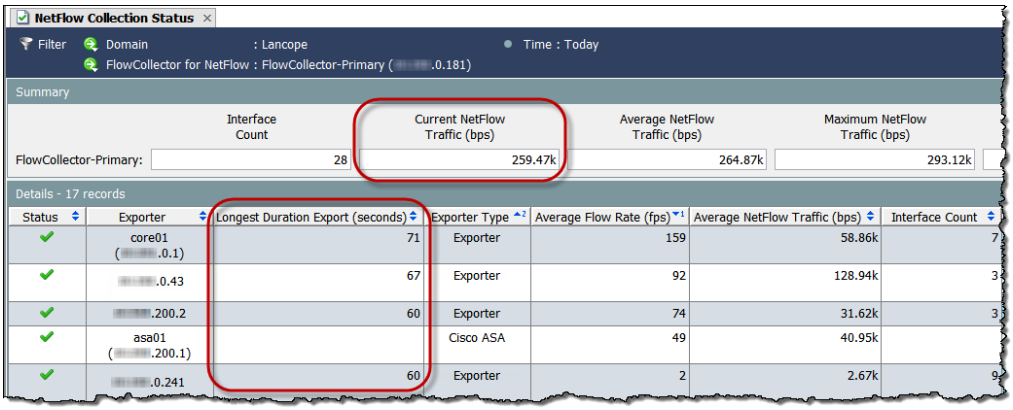
验证 NetFlow 数据收集

在将流量收集器添加到 SMC 后，流量收集器将向 SMC 传达流量信息，SMC 通过各种文档以一种用户友好的方式显示这些信息。要确认您确实在收集 NetFlow 数据，请完成以下步骤：

1. 在企业树中，右键点击“流量收集器”并选择 **状态 > NetFlow 收集状态**。



NetFlow 收集状态文档随即打开。



2. 查看文档顶部的**当前 NetFlow 流量**字段。此统计信息显示了正在观察的 NetFlow 流量。您是否看到了任何流量？

   - 如果看到，请转至下一步。
   - 如果没有，请检查您的导出器/路由器配置。(有关帮助，请参阅 *SMC 客户端联机帮助*。)然后，转至下一步。

3. 查看**最长持续时间导出**列。您可能需要通过右键点击列标题并从弹出式菜单中选择**持续时间最长的导出**来添加此列。是否每个导出器的值都低于 100？

   - 如果是，则缓存导出计时器正常。
   - 如果不是，值更高表示缓存导出计时器不正常，这可能导致警报不实。请检查您的导出器/路由器配置。(有关帮助，请参阅 *SMC 客户端联机帮助*。)

4. 您是否有身份识别设备？

   - 如果有，请转至下一章“添加思科 ISE。
   - 如果没有，则转至下一步。

5. 您是否有 SLIC 功能？

   - 如果有，请转至“启用 SLIC 威胁源功能”一章。
   - 如果没有，恭喜您，您已经完成了设备的配置。

4

添加思科 ISE

概述

如果您有身份识别设备，可以将其添加至 SMC。本章介绍添加思科 ISE(身份服务引擎)的过程。

添加思科 ISE

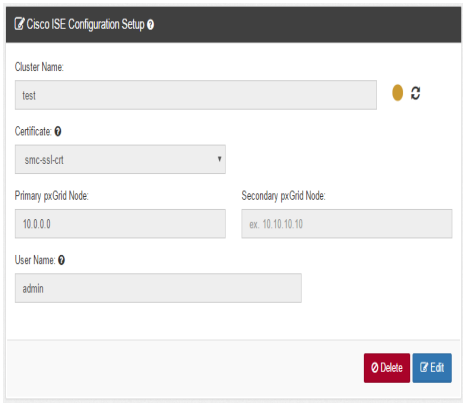
注意：

- 您可以将多个独立的思科ISE群集添加到一个域。
- 将思科 ISE-PIC 添加到 Stealthwatch 系统的过程与此处描述的过程相同。有关设置思科 ISE-PIC 的进一步信息，请参阅您的思科 ISE 文档。

要添加思科 ISE，请完成以下步骤：

1. 在 SMC Web 应用界面的菜单上，选择**部署 > 思科 ISE 配置**。

“添加思科 ISE”对话框随即打开。



2. 为思科 ISE 集群键入一个名称。您必须为使用思科 ISE 集群的每个 Stealthwatch 系统域配置该集群。
3. 选择设备证书。此证书的名称与您在设备管理 (Admin) 界面中的“SSL 证书”页面上的“友好名称”字段中输入的名称相同，从而使设备验证其作为客户端的身份 (即该证书是 SMC 向 ISE 展示的客户端证书)。
4. 键入设备正在与之集成的 ISE 集群上主 pxGrid 节点的 IP 地址。
5. (可选) 键入设备正在与之集成的 ISE 集群上辅助 pxGrid 节点的 IP 地址。此节点用于故障切换。如果与主要节点的连接失败，则使用辅助节点。
6. 键入您在思科 ISE 设备上为您的用户帐户配置的用户名。此名称显示在 ISE 设备中 ISE 集群上的 pxGrid 客户端列表中。
7. 点击**添加 > 确定**。思科 ISE 已添加至“身份识别服务”文件夹中的域。
8. 您是否有 SLIC 功能？
   - 如果有，请继续阅读下一章启用 SLIC 威胁源功能。
   - 如果没有，恭喜您，您已经完成了设备的配置。

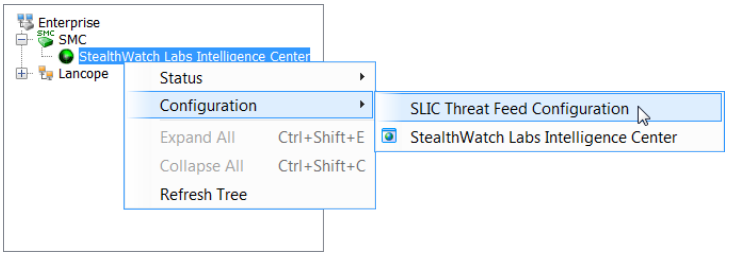
4

启用 SLIC 威胁源功能

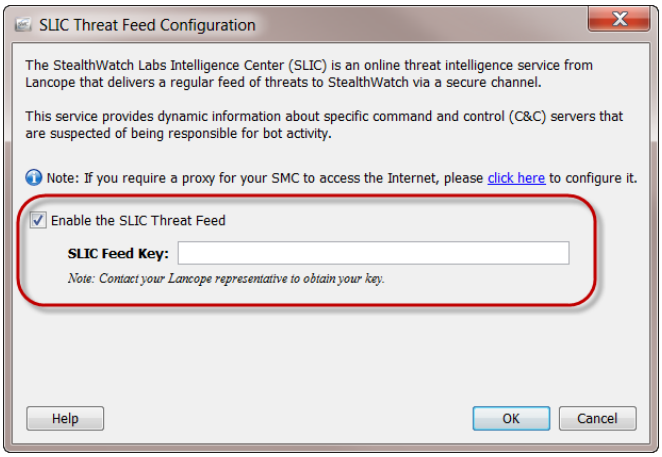
安装和配置 Stealthwatch 包的最后一步是通过 SMC 客户端接口启用 SLIC 威胁源。

请完成以下步骤：

1. 在企业树中，右键点击 **Stealthwatch 实验室智能中心**分支，然后选择**配置 > SLIC 威胁源配置**。



“SLIC 威胁源配置”对话框随即打开。



2. 选中“启用 SLIC 威胁源”复选框。
3. 在“SLIC 源密钥”字段中，键入您的密钥。

4. 点击**确定**。在 10 分钟内，企业树将更新“命令”&“控制服务器”(C&C) 主机组分支，以显示到目前为止所识别现用 C&C 服务器的列表。

祝贺您！您现在可以开始享受 Stealthwatch 系统带给您的诸多安全和网络监控的好处了。要获得进一步的帮助，请参阅 *Stealthwatch 管理控制台用户指南*或 SMC 客户端界面联机帮助。点击**帮助**。