Threat Grid 设备
设置和配置指南

版本：2.4.3、2.4.3.1、2.4.2、2.4.3

更新日期： 2018 年 6 月 1 日

思科公司 www.cisco.com

思科 Threat Grid 设备管理员指南

目录

图片清单

引言

思科 Threat Grid 设备可提供高度安全可靠的本地高级恶意软件分析功能，其中包含深度的威胁分析和相关内容。Threat Grid 设备可提供完整的 Threat Grid 恶意软件分析平台，该平台安装在单台 UCS 服务器（思科 UCS C220-M3 或思科 C220 M4）上。借助此平台，在各种合规性和政策限制下运营的组织都能够向该设备提交恶意软件样本。

许多处理敏感数据的组织（例如银行、医疗服务机构等）必须遵循各种监管规定和准则，不得将特定类型的文件（例如恶意软件信息）发送到网络外部进行恶意软件分析。通过在本地部署思科 Threat Grid 设备，组织能够将可疑文档和可疑文件发送至 Threat Grid 设备进行分析，而无需寻求外部帮助。

利用 Threat Grid 设备，安全团队可以使用高度安全的专有静态和动态分析技术分析所有样本。该设备在分析结果与数亿条之前经过分析的恶意软件信息之间建立关联，可全面了解恶意软件的攻击和活动及其分布的相关信息。安全团队可以快速参照数百万个其他样本对单个恶意软件样本中观察到的活动和特征进行关联分析，从历史和全局角度全面了解其行为。此功能可帮助安全团队有效地为组织提供安全保护，抵御来自高级恶意软件的威胁和攻击。

本指南的目标读者

新设备必须先针对组织的网络进行设置和配置，然后才能用于恶意软件分析。本指南的目标用户是负责设置和配置新的 Threat Grid 设备的安全团队 IT 人员。

本文档介绍如何完成新的 Threat Grid 设备的初始设置和配置，以便可以将恶意软件样本提交到该设备进行分析。

有关详细信息，请参阅思科 Threat Grid《*设备管理员指南*》，该文档可从 Cisco.com 的**安装和升级页面**获取。

版本说明

有关详细的更新信息，请参阅 OpAdmin 门户中的《*版本说明*》：

操作菜单 > **更新设备**

版本说明的内容是不断累积的：最新的版本包含之前所有的说明。也可在线获取 PDF 格式版本以及其他 Threat Grid 设备文档：

http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html

版本查询表

有关 Threat Grid 设备的版本信息列表，请参阅内部版本号/版本查询表。

注意： 要查看 Threat Grid 门户 UI 的版本说明，请点击 UI 导航栏中的**帮助**。

新增内容

有关新功能的完整说明，请随时查阅《*版本说明*》和其他版本文档，例如《迁移说明》和《数据保留说明》。此处包含其中的主要重点。

网络出口支持

网络出口在概念上与 VPN 类似，网络出口设置使得在分析过程中生成的任何传出网络流量看上去都像是从该出口位置退出的。在 3.4.61 版本中，已将网络出口定位功能添加到 Threat Grid 云门户中。现在，在 v2.4.3 版本的设备中提供该功能。

此功能用于代替 tg-tunnel 功能。配置文件自动分发，因此不再需要支持人员手动安装或更新。

注意：之前使用 tg-tunnel 的客户需要允许向 4.14.36.142:21413 和 63.97.201.68:21413 发送的出站流量，然后才能安装 2.4.3 版本。除此以外，客户仅需要在启用远程出口之前允许这些流量。

用户无法选择出口。该功能与 tg-tunnel 目前提供的功能相同，只不过是一种由客户控制的切换功能以及自动配置提取/安装功能。

对于之前手动安装 tg-tunnel 配置的任何客户而言，已默认将此开关打开，以避免不必要的有害网络流量泄漏风险。

有关详细信息，请参阅《*Threat Grid 设备指南*》中的“*网络出口配置*”部分。

集群

为进行早期的现场试用，在 v2.4.0 版本中即已引入 Threat Grid 设备集群化功能；在 v2.4.2 版本中，该功能已成为常规功能。

集群化操作的主要目标是，通过链接多个设备（目前为 2 到 5 个）组成集群，提升单个系统的容量。集群中的每台设备在共享的文件系统中保存数据，并将拥有与集群中其他设备相同的数据。

有关当前可用的集群功能的更多信息，请参阅《*Threat Grid 设备管理员指南*》中的“*集群*”部分，以及 Cisco.com 网站上 **Threat Grid 设备安装和升级页面**中的“*集群常见问题解答*”部分。以及 Cisco.com 网站上 Threat Grid 设备安装和升级页面

不支持对 DIRTY 接口使用 IPv4LL 地址空间

虽然文档中从未说明 DIRTY 接口支持使用 IPv4LL 地址空间 (168.254.0.16)，但从版本 2.3.0 开始，IPv4LL 地址空间被识别为已损坏，因此明确不受支持。

自动检索许可证

如果设备连接到互联网，则设备可尝试通过网络检索许可证或者替换已到期的许可证。请注意，自动检索功能目前仅适用于在 2.3 版本软件（2017-08-11）发布后出售或续约的许可证。

更多 Windows 更改

2.3 版本包括以下 Windows 更改：

- 删除 Windows XP，包括从之前允许使用 Windows XP 的设备中删除。
- 现在仅支持 64 位版本的 Windows 7。
- 提交到“winxp”或“win7-x86”虚拟机的样本仍然可用。请注意，应相应更改对“winxp”进行硬编码的任何脚本或客户端。

备份

版本 2.2.4 引入了备份功能。现在，Threat Grid 设备可支持如下操作：向支持 NFS 的存储保存加密备份；从支持 NFS 的存储执行数据初始化；重置为可加载此类备份的空数据库状态。

（请注意，重置与擦除流程不同。当设备需要离开客户现场时，可使用擦除来避免信息泄漏。适用于此目的的擦除流程存在于恢复引导加载程序中，但不适用于在恢复备份之前准备系统。要为恢复备份做准备，请使用重置。）

我们*强烈*建议在使用备份功能之前参阅相关文档。我们提供了其他文档来专门介绍备份功能。请参阅*备份说明和常见问题解答*，以及《*Threat Grid 设备管理指南*》中的“备份”部分提供的补充信息。这两个文档都可以在 Cisco.com 网站的 **Threat Grid 设备安装和升级页面**获取。

Windows XP 相关更改

应 Microsoft 的要求，于 2017 年 7 月 1 日之后（包括 2017 年 7 月 1 日）生产的 Threat Grid 设备将不再包括 Windows XP 许可或发行版。2.2.3 次要版本更新提供了不需要 Windows XP 即可运行的新出厂设置。

与第三方检测和增强服务集成

在版本 2.2 中，现在可通过新的配置页面在设备上配置 OpenDNS、TitaniumCloud 和 VirusTotal 集成。在 OpAdmin 中，依次选择**配置 > 集成**可打开此页面。有关详细信息，请参阅《*Threat Grid 管理员指南*》。

为处置更新服务管理器配置多个 URL

版本 2.2 还能够为处置更新服务管理器配置多个 URL。

ClamAV 签名自动每日更新

版本 2.2 的设备现在可以每天自动下载 ClamAV 签名的更新，从而提高对已知恶意软件的识别能力。此功能默认启用，并可通过 OpAdmin 中新添加的“集成”页面禁用。

LDAP 身份验证

2017 年 1 月 5 日发布的版本 2.1.6 已为 OpAdmin 和 TGSH 对话管理员界面增加 LDAP 身份验证，为拥有多名设备管理员且不希望他们共用相同登录名和密码的客户提供支持。有关详细信息，请参阅《*Threat Grid 管理员指南*》。

思科 UCS C220 M4 服务器

C220 M4 服务器于 2016 年 11 月 17 日发布，包含一个硬件更新并提供安全启动功能。请通过 support@threatgrid.com 联系我们，讨论有关升级的任何问题。

注意： Threat Grid 将继续为 M3 提供支持，直到合同规定的设备生命周期到期。除非另有说明，否则所有相同的 M4 功能都可以现有 M3 的在线更新的方式提供。

M5 服务器升级目前正在开发中。我们强烈鼓励现有 M3 和 M4 客户通过 support@threatgrid.com 联系我们，以讨论您可能遇到的任何问题，例如哪种服务器升级最适合您的需求，以及关于数据迁移、备份、推出策略等的问题。我们认为 M5 升级路径规划的最佳途径就是，满足我们客户的个体性要求。

面向终端的 AMP 私有云集成

版本 2.0.3 包含可使 Threat Grid 设备与 Fire AMP 私有云(现已更名为面向终端的 AMP 私有云)集成的功能，包括在 CLEAN 和 DIRTY 网络接口之间拆分 DNS、CA 管理，以及面向终端的 AMP 私有云集成。

现在，生成的 SSL 证书令 CN 复制为 subjectAltName。这解决了与 SSL 客户端的不兼容性问题，即当存在至少一个 subjectAltName 时，SSL 客户端会忽略 CN 字段。如果使用此类工具，则可能需要重新生成之前由设备生成的任何证书。

版本 2.0

2.0 版是主要版本，基于更新的操作系统。它包括支持未来硬件版本的改进，同时令 Threat Grid 门户 UI 与云版本的一致性更高。这包括大量的较新和更新的行为指标以及其他更改。

详细信息请参阅以版本 3.3.45 开始的《*Threat Grid 门户版本说明*》。（从门户 UI 导航栏选择**帮助**，然后点击版本说明的链接。

支持 - 联系 Threat Grid

您可以通过多种方式请求 Threat Grid 工程师的支持：

- **邮件。**请将您的疑问通过邮件发送至 support@threatgrid.com。
- **创建支持案例。**您需要具有 Cisco.com ID（或生成一个 ID）才能创建支持案例。此外，您还需要提供服务合同编号，此编号包含在订单发票中。使用**思科支持案例管理器**输入您的支持案例。
- **电话。**有关思科的支持热线和联系信息，请参阅**思科联系方式**页面。

如需请求 Threat Grid 团队的支持，请在发送您的请求时提供以下信息：

- 设备版本：“OpAdmin”>“操作”>“更新设备”
- 完整的服务状态（来自 Shell 的服务状态）
- 网络图或说明（如果适用）
- 支持模式（Shell 或网络界面）
- 支持请求详细信息

支持模式

如果您需要获得 Threat Grid 工程师的支持，他们可能要求您启用“支持模式”，此模式是一个实时支持会话，可供 Threat Grid 支持工程师远程访问您的设备。此操作不会影响设备的正常运行。此操作可通过 **OpAdmin 门户支持**菜单完成。（您也可以从 TGSH 对话、从旧版 Face 门户 UI 以及在启动恢复模式时启用**支持模式**。）

启动与 Threat Grid 技术支持的实时支持会话：

在 **OpAdmin** 中，依次选择**支持 > 实时支持会话**，然后点击**启动支持会话**。

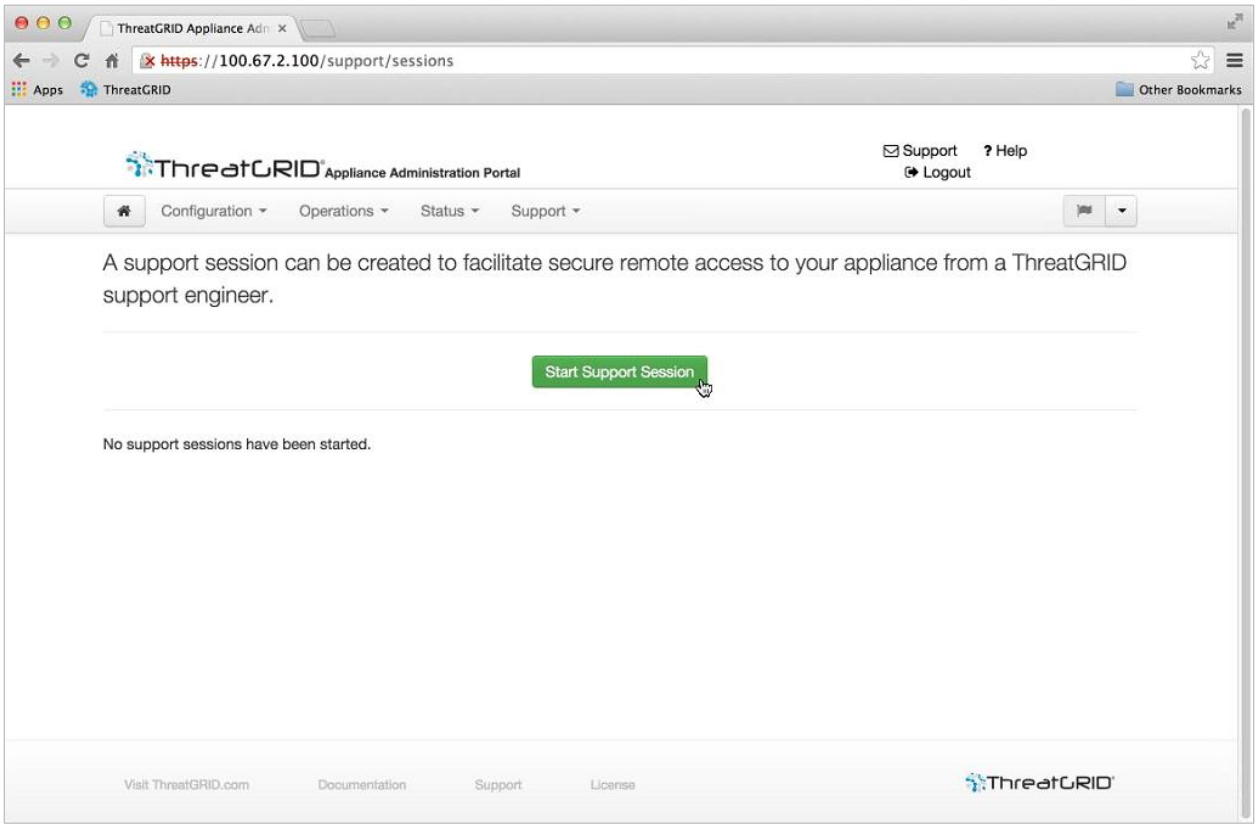
注意：在获得许可之前，您可以跳过 OpAdmin 向导任务流来启用支持模式。

启动支持模式 – 1.4.4 版之前的许可证解决方法

Threat Grid 设备 1.4.4 版中已解决一个许可证问题。如果您的软件版本低于 1.4.4，您将需要至少有一次成功连接到*支持模式*服务器（2015 年 11 月 14 日之后），以便您的许可证被接受。验证许可证时，连接无需为连接中状态或活动状态。

要求：DIRTY 网络需要正常运行，才能执行此步骤。

图 1 - OpAdmin 启动实时支持会话



支持服务器

建立支持会话 需要 Threat GridTG 设备访问以下服务器：

- support-snapshots.threatgrid.com
- rash.threatgrid.com

在活动支持会话期间，防火墙应允许设备访问这两个服务器。

支持快照

支持快照一般是指运行状态下系统的快照，其中包含日志、ps 输出等，可帮助支持人员对任何问题进行故障排除。

1. 验证是否为支持快照服务指定了 SSH。
2. 从**支持**菜单中，选择**支持快照**。
3. 拍摄快照。
4. 生成快照之后，您可以自行下载 .tar.gz 格式的快照，也可以按**提交**，使快照自动上传到 Threat Grid 快照服务器。

计划

思科 Threat Grid 设备是一个预装了 Threat Grid 软件（由思科制造部门在发货前安装）的 Linux 服务器。收到新设备后，您必须针对自己的本地网络环境对新设备进行设置和配置。在开始之前，需要考虑和计划诸多问题。环境要求、硬件要求和网络要求如下所述。

用户文档和在线帮助

Threat Grid 设备 - Threat Grid 设备用户文档，包括本文档、《*Threat Grid 设备管理员指南*》、版本说明、集成指南等，可在 Cisco.com 上的**安装和升级页面**中查看。

Threat Grid 门户 UI 在线帮助 - Threat Grid 门户用户文档，包括版本说明、“使用 Threat Grid”在线帮助、API 文档，而其他信息可从用户界面顶部导航栏中的**帮助**菜单查看。

2.4.3 – 2.4.3.3 新增内容

本指南的主要更改详见下表：

章节标题	页面	更新
网络出口支持	2	新功能说明
不支持 DIRTY 接口使用 IPv4LL 地址空间	2	新章节
tgsh	11	新章节

浏览器

Threat Grid 建议使用以下浏览器:

- Chrome
- Firefox
- Safari
- Microsoft Internet Explorer：**不支持 – 请勿使用。**不建议使用且不支持 Microsoft Internet Explorer。

环境要求

Threat Grid 设备应部署在 UCS C220-M3 或 UCS C220-M4 服务器上。在设置和配置设备之前，请根据服务器的规格确保符合电源、机架空间、冷却和其他方面的必要环境要求。

硬件要求

ADMIN 接口的外形规格为 SFP+。如果要集群化设备，每个设备将需要在 CLUST 接口上具有一个额外的 SFP+ 模块。

注意：必须*先*连接 SFP+ 模块，然后再开启设备电源以启动将要运行配置向导的会话。

如果交换机上未提供 SFP+ 端口，或者 SFP+ 不是理想的接口规格，则可以使用 1000Base-T 收发器（例如：与思科兼容的千兆 RJ-45 铜缆微型 SFP 收发器模块 -GBIC - 10/100/1000 Base-T 铜缆 SFP 模块）。

图 2 - 思科 1000BASE-T 铜缆 SFP (GLC-T)

显示器：您可以在服务器上连接一个显示器，如果配置了 CIMC（思科集成管理控制器），也可以使用远程 KVM。

硬件文档

思科 UCS C220 M4 服务器安装和服务指南：

- 思科 UCS C220 M4 服务器安装和服务指南

思科 UCS C220 M3 服务器安装和服务指南：

- https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220.html

思科 UCS C220 M3 高密度机架式服务器（小型磁盘驱动器型号）规格清单：

- https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/C220M3_SFF_SpecSheet.pdf

思科提供了一个电源/冷却计算器，可能会对您有所帮助：

- https://mainstayadvisor.com/Go/Cisco/Cisco-UCS-Power-Calculator.aspx

网络要求

Threat Grid 设备需要三个网络：

ADMIN - *“管理”*网络。 必须配置该网络才能设置设备。

- OpAdmin 管理流量（HTTPS）
- SSH
- NFSv4（出站。如果使用 NFS 主机名而不是 IP，此名称将通过 DIRTY DNS 解析。）

CLEAN – “*CLEAN*” 网络用于流入设备的可信入站流量（请求）。这包括多个集成设备。例如，思科邮件安全设备和网络安全设备 (ESA/WSA) 连接到 CLEAN 接口的 IP 地址。

注意：CLEAN 网络接口的 URL *需要*等到 OpAdmin 门户配置完成之后才生效。

以下特定的受限网络流量类型可从 CLEAN 网络出站：

- 远程系统日志连接
- Threat Grid 设备自身发送的邮件消息
- 面向终端的 AMP 私有云设备的处置更新服务连接
- 与以上任意项目相关的 DNS 请求
- LDAP

DIRTY – “*DIRTY*”网络用于从设备流出的出站流量（包括恶意软件流量）。

注意：我们建议使用不同于您的企业 IP 的专用外部 IP 地址（例如，“*DIRTY*”接口），以保护您的内部网络资产。

有关网络接口设置信息和图示，请参阅网络接口小节以及其后的网络接口连接设置部分。

DNS 服务器访问

用于处置更新服务查询、解析远程系统日志连接和解析用于来自 Threat Grid 软件自身通知的邮件服务器以外用途的 DNS 服务器需通过 DIRTY 网络进行访问。

默认情况下，DNS 使用 DIRTY 接口。CLEAN 接口则用于面向终端的 AMP 私有云集成。如果无法通过 DIRTY 接口解析面向终端的 AMP 私有云的主机名，可以在 OpAdmin 界面中配置一个使用 CLEAN 接口的独立 DNS 服务器。

有关其他信息，请参阅《*Threat Grid 设备管理员指南*》。

NTP 服务器访问

NTP 服务器需要通过 “DIRTY” 网络进行访问。

集成 – ESA/WSA/面向终端的 AMP 等

如果要将 Threat Grid 设备与其他思科产品（如 ESA/WSA 设备、面向终端的 AMP 私有云等）一起使用，必须进行额外的规划。

DHCP

如果您已连接到一个配置为使用 DHCP 的网络，请按照《*Threat Grid 设备管理员指南*》中**使用 DHCP** 部分的说明进行操作。

许可证

您会从思科 Threat Grid 收到许可证和密码。

有关许可证的问题，请联系 support@threatgrid.com。

速率限制

许可协议条款约束的设备均受 API 速率限制。这只会影响 API 提交，而不会影响手动样本提交。

速率限制基于滚动时间窗口，而不是日历日。当提交限制用尽时，下一个 API 提交将返回 429 错误，另外还发送回一条消息，说明在重试之前需要等待的时间。有关更详细的说明，请参阅 Threat Grid 门户 UI 中的速率限制常见问题解答条目。

组织和用户

在完成设备的设置和网络配置之后，您需要创建初始的 Threat Grid 组织并添加用户账户，以便用户可以登录并开始提交恶意软件样本进行分析。此任务可能需要在多个组织和用户之间进行规划和协调，具体取决于您的要求。

管理 Threat Grid 组织的信息在《*Threat Grid 设备管理员指南*》中有说明。管理用户的信息在 Threat Grid 门户帮助中有说明。

更新

在安装任何 Threat Grid 设备更新之前，**必须完成**初始设备设置和配置。

我们建议您在完成本指南介绍的初始配置之后立即检查是否有更新。

必须按顺序安装更新。Threat Grid 设备更新必须要等到安装许可证之后才能下载，并且更新过程要求完成初始设备配置。可从《*Threat Grid 设备管理员指南*》中获取关于更新设备的说明。

注意：请验证是否为更新指定了 SSH。

用户界面

在服务器正确连接到网络并通电后，有多个用户界面可用于配置 Threat Grid 设备。请注意，在版本 2.1.6 中，可将 LDAP 身份验证用于 TGSH 对话和 OpAdmin。

TGSH 对话

第一个界面是 **TGSH 对话**，用于配置网络接口。在设备成功启动后，系统会显示 TGSH 对话。

重新连接到 TGSH 对话

TGSH 对话将在控制台上保持打开状态，可以通过将显示器连接到设备或者通过远程 KVM 访问（如果已配置 CIMC）该对话。

要重新连接到 TGSH 对话，请通过 SSH 以用户“**threatgrid**”的身份连接到 Admin IP 地址。

所需的密码可以是随机生成的初始密码（最初在 TGSH 对话中显示），也可以是您在 OpAdmin 门户配置的第一步创建的新管理员密码（相关内容将在下节介绍）。

tgsh

Threat Grid Shell。这是用于执行一些命令（包括 destroy-data 和 forced backup 命令）以及详细的专家调试的管理员接口。要访问 tgsh，请在 TGSH 对话中选择控制台。

注意：OpAdmin 使用与 Threat Grid 用户相同的凭证，因此通过 tgsh 进行任何密码更改/更新也会影响 OpAdmin。

警告：除非 Threat Grid 支持人员有特别指示，否则不支持通过 tgsh 更改网络配置。而应使用 OpAdmin 或 TGSH 对话。

OpAdmin 门户

这是主要的 Threat Grid GUI 配置工具。该设备的大量配置都只能通过 OpAdmin 完成，包括许可证、邮件主机、SSL 证书等。

Threat Grid 门户

Threat Grid 用户界面应用可作为一项云服务提供，也可安装在 Threat Grid 设备上。Threat Grid 云服务与 Threat Grid 设备随附的 Threat Grid 门户之间不进行通信。

CIMC

另一个用户界面是思科集成管理控制器（“CIMC”），用于管理服务器。

网络接口

ADMIN 接口

- 连接到 ADMIN 网络。**仅入站**（来自 ADMIN 网络）。
- OpAdmin UI 流量
- tgsh-dialog 的 SSH（入站）
- 用于备份和集群的 NFSv4（出站。如果使用 NFS 主机名而不是 IP，此名称将通过 DIRTY DNS 解析。） 必须能从所有集群节点进行访问。

注意： ADMIN 接口的外形规格是 SFP+。请参阅图 2 – 思科 1000BASE-T 铜缆 SFP (GLC-T)。

CLUST 接口

之前已保留的非管理 SFP+ 端口，现用于集群。

- 集群化操作所需的 CLUST 接口（可选）
- 需要一个额外的 SFP+ 模块用于直接互连。不需要对此接口进行任何配置。系统将自动分配地址。

CLEAN 接口

- 连接到 CLEAN 网络。必须可从公司网络访问 CLEAN 网络，但不需要出站访问互联网。
- UI 和 API 流量（入站）
- 样本提交
- SMTP（出站连接到已配置的邮件服务器）
- SSH（TGSH 对话的入站访问）
- 系统日志（出站连接到已配置的系统日志服务器）
- ESA/WSA - CSA 集成
- 面向终端的 AMP 私有云集成
- DNS - 可选。
- LDAP（出站）

DIRTY 接口

连接到 DIRTY 网络。需要访问互联网。**仅出站**！

- DNS
  注意：如果您设置了与面向终端的 AMP 私有云的集成，但是无法通过 DIRTY 接口解析面向终端的 AMP 设备的主机名，可以在 OpAdmin 中配置一个使用 CLEAN 接口的独立 DNS 服务器。
- NTP
- 更新
- 正常运行模式下的支持会话
- 支持快照
- 恶意软件样本发起的流量
- 恢复模式支持会话（出站）
- OpenDNS、TitaniumCloud、VirusTotal、ClamAV
- SMTP 出站连接将重定向到内置蜜罐

注意： 虽然文档中从未说明 DIRTY 接口支持使用 IPv4LL 地址空间（168.254.0.16），但从版本 2.3.0 开始，IPv4LL地址空间被识别为已损坏，因此明确不受支持。

CIMC 接口

推荐。如果已配置思科集成管理控制器（“CIMC”）接口，则其可用于服务器管理和维护。有关详细信息，请参阅附录 A - CIMC 配置（推荐）。

登录名和密码 - 默认

网络 UI 管理员

- **登录名：** admin
- **密码：** “changeme”

OpAdmin 和 Shell 用户

先使用 Threat Grid/TGSH 对话随机生成的初始密码，然后使用在 OpAdmin 配置工作流第一步中输入的新密码。

如果丢失密码，请按照《*Threat Grid 设备管理员指南*》**支持**部分中的**丢失密码**相关说明操作。

CIMC（思科集成管理控制器）

- **登录名：** admin
- **密码：** “password”

设置和配置步骤概述

本文档介绍了以下设置和初始配置步骤：

- 服务器设置。
- 网络接口连接设置：
  - Admin
  - CLUST
  - CLEAN
  - DIRTY
- 初始网络配置 - TGSH 对话。
- 主要配置 - OpAdmin 门户。
- 安装更新。
- 对设备设置进行测试：提交样本进行分析。
- 管理配置 - 按照《*Threat Grid 设备管理员指南*》中的说明，在 OpAdmin 门户中完成剩余管理配置任务（许可证安装、邮件服务器、SSL 证书等）。

完成设置和配置所需的时间

完成服务器设置和初始配置步骤大约需要 1 小时的时间。

注意： 在初始设备配置安装步骤期间 TGSH 对话的“应用”部分期间，请耐心等待。这些步骤有时可能需要 10 多分钟才能完成。

服务器设置

首先，连接设备背面的两个电源，然后将随附的 KVM 适配器连接到外部显示器和键盘，并插入服务器前面的 KVM 端口中，如下图所示。

如果配置了 CIMC，则可以使用远程 KVM。. 有关 CIMC 配置的信息，请参阅*附录*中的**配置 CIMC（可选）**。

有关详细的硬件和环境设置信息，请参阅相关的服务器产品文档。上述硬件文档部分提供了访问产品文档的链接。

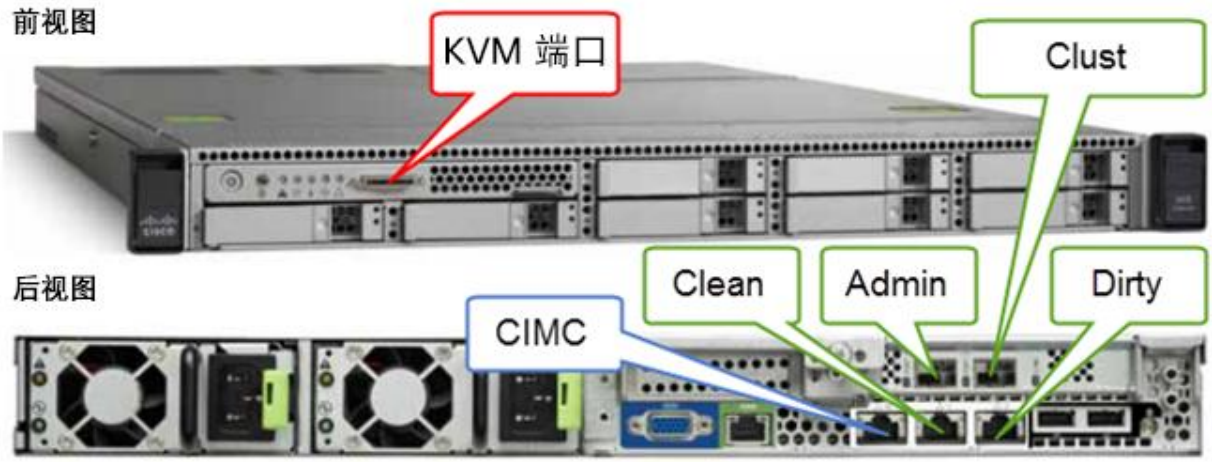
网络接口连接设置

必须先连接 SFP+ 模块，*然后*再开启设备电源以启动将要运行配置向导的会话。但是，SFP 与网络的连接可在开启电源之后、配置之前完成。

找到设备背面的两个 SFP+ 端口和三个以太网端口，然后按照下图所示连接网线：

C220 M3 机架式服务器设置

图 3 - 思科 UCS C220 M3 SFF 机架式服务器



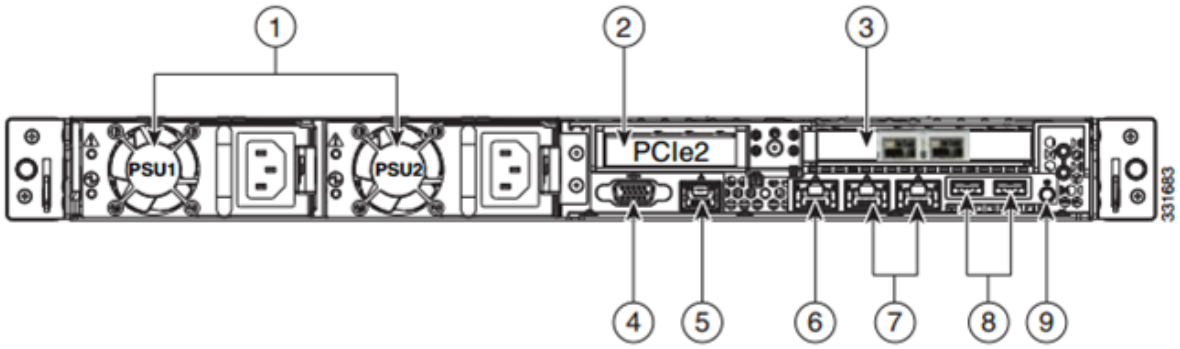
必须正确连接和配置接口，设备才能运行。

注意：您的设备的详细信息可能与上图中显示的信息有所不同。如有任何疑问，请联系 **support@threatgrid.com**。

注意：“CLUST”为可选端口，是保留用于集群功能的非管理 SFP+ 端口。

有关 C220 M3 服务器的详细信息，请参阅下图。

图 4 - 思科 UCS C220 M3 后视图详细信息

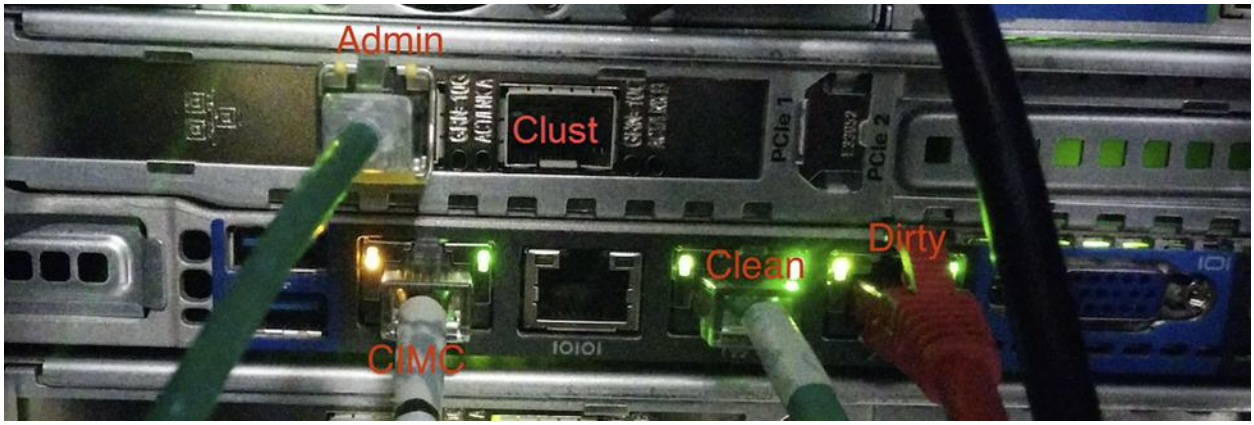


1	电源（最多两个）	6	一个 10/100/1000 以太网专用管理端口
2	插槽 2：提升板上的薄型 PCIe 插槽： （半高，半长，x16 连接，x8 信道宽度）	7	双 1-GbE 端口 （LAN1 和 LAN2）
3	2 个 SFP+ 端口。 插槽 1：ADMIN 插槽 2：CLUST	8	USB 端口
4	VGA 视频连接器	9	后部识别按钮/LED
5	串行端口（RJ-45 连接器）[1]	—	—

注意： 对于版本 1.0-1.2，如果在启动时接口处于未插入状态，则可能需要重新启动。此问题出现于 1.3 以下的版本（不包括需要 SFP 的任何接口，对于 1.3 以上的版本，此类接口仍需在启动时处于插入状态）。可以安全地热插拔在 SFP 中插入的网线。

C220 M4 机架式服务器设置

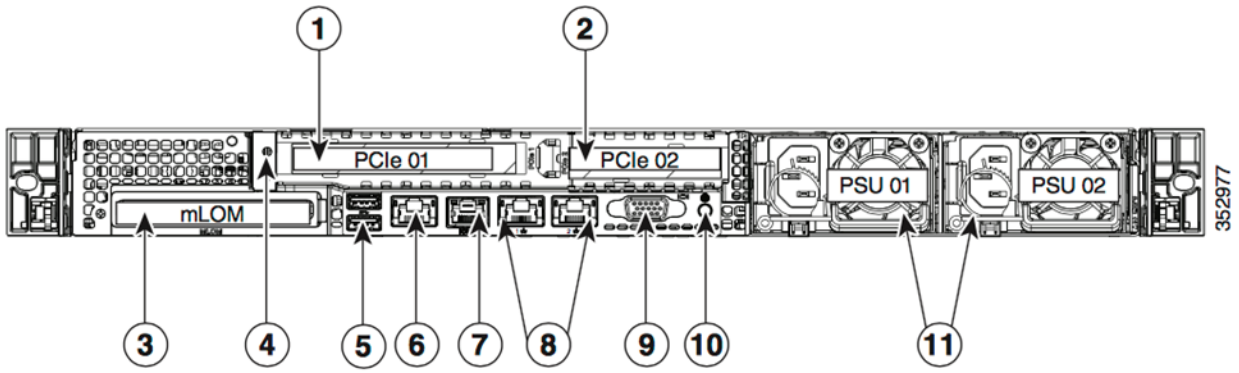
图 5 - 思科 UCS C220 M4 SFF 机架式服务器



注意： 使用端口 3 插槽 2 作为（可选）CLUST 接口。

注意： 您的设备的详细信息可能与上图中显示的信息有所不同。如有任何疑问，请联系 **support@threatgrid.com**。

图 6 - 思科 UCS C220 M4 后视图详细信息



1	PCIe 提升卡 1/插槽 1	7	串行端口（RJ-45 连接器）
2	PCIe 提升卡 2/插槽 2	8	两个千兆以太网端口（LAN1 和 LAN2）
3	模块化板载局域网 (mLOM) 卡插槽	9	VGA 视频端口（DB-15）
4	接地片螺孔（用于直流电源）	10	后部单元标识按钮/LED
5	USB 3.0 端口（两个）	11	电源（最多两个，采用 1+1 冗余模式）
6	1 Gb 以太网专用管理端口		

连接：

1 Admin，CLUST

8 （左）CLEAN

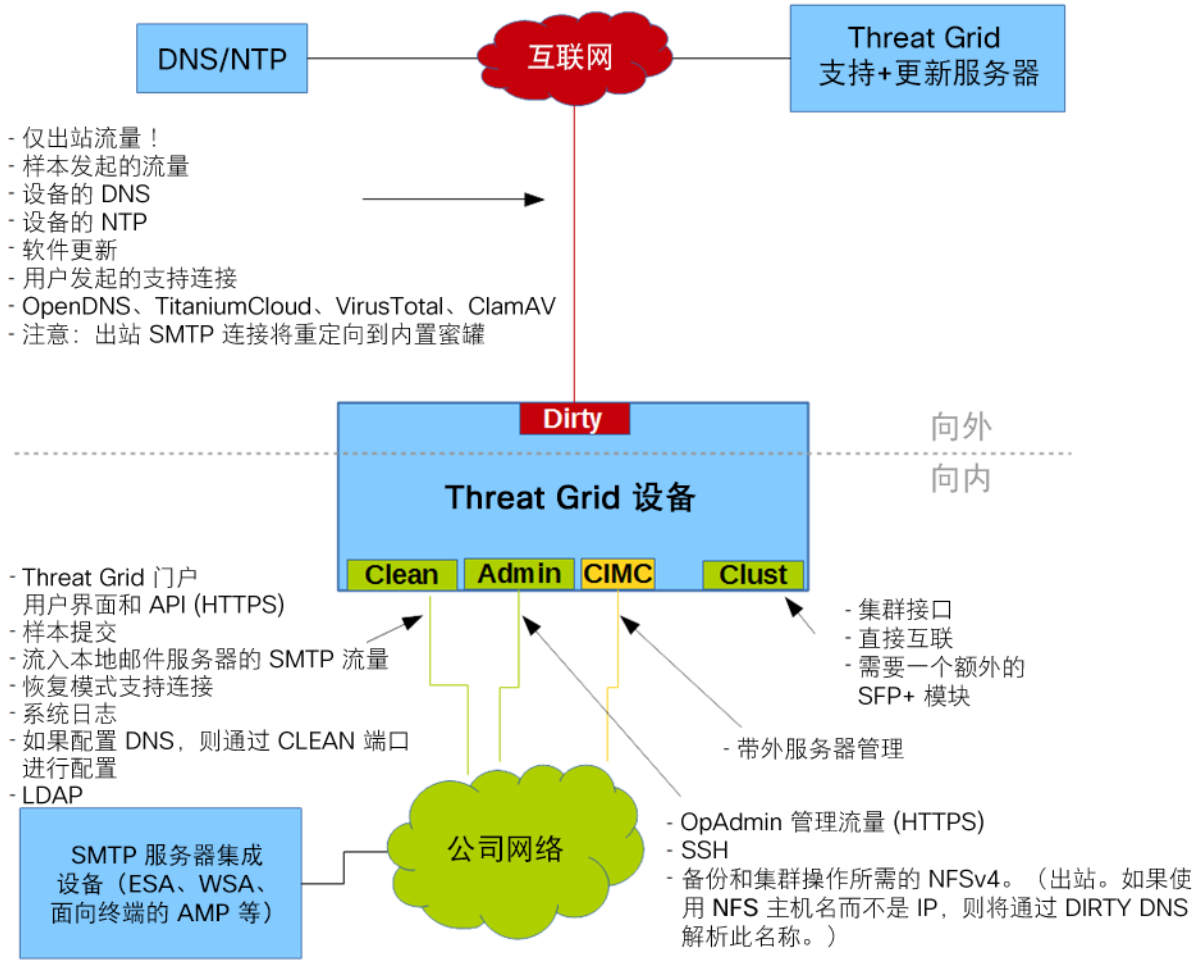
8 （右）DIRTY

6 CIMC

网络接口设置图

本节介绍 Threat Grid 设备最符合逻辑的设置或推荐设置。但是，每个客户的接口设置是不同的。例如，根据您的网络要求，在制定了正确的网络安全措施的情况下，您可能决定将 DIRTY 接口连接至内部，将 CLEAN 接口连接至外部。

图 7 - 网络接口设置图



防火墙规则建议

注意： 在 DIRTY 接口上为端口 22 和 19791 实施严格的传出策略将需要持续跟踪更新，并需要花费更多时间来维护防火墙等功能。请详见下面的配置部分提供的所需目的地址。

注意： 虽然文档中从未说明 DIRTY 接口支持使用 IPv4LL 地址空间（168.254.0.16），但从版本 2.3.0 开始，IPv4LL地址空间被识别为已损坏，因此明确不受支持。

DIRTY 接口出站

源	目标	协议	端口	操作	备注
DIRTY 接口	互联网	任意	任意	允许	允许来自样本的出站流量。（要获得准确结果，需要允许恶意软件使用其适用的端口和协议访问其命令和控制服务器。）

DIRTY 接口入站

源	目标	协议	端口	操作	备注
任意	DIRTY 接口	任意	任意	拒绝	拒绝所有的入站连接

CLEAN 接口出站

源	目标	协议	端口	操作	备注
CLEAN 接口	SMTP 服务器	TCP	25	允许	设备使用 CLEAN 接口启动与已配置的邮件服务器的 SMTP 连接

CLEAN 接口出站（可选）

以下取决于配置的服务。

源	目标	协议	端口	操作	备注
CLEAN 接口	公司 DNS 服务器	TCP/UDP	53	允许	“可选，仅当已配置‘CLEAN DNS’时为必需”
CLEAN 接口	AMP 私有云	TCP	443	允许	“可选，仅当使用面向终端的 AMP 私有云集成时为必需”
CLEAN 接口	系统日志服务器	UDP	514	允许	允许连接到指定为接收系统日志消息和 Threat Grid 通知的服务器
CLEAN 接口	LDAP 服务器	TCP/UDP	389	允许	“可选，仅当已配置 LDAP 时为必需”
CLEAN 接口	LDAP 服务器	TCP	636	允许	“可选，仅当已配置 LDAP 时为必需”

CLEAN 接口入站

源	目标	协议	端口	操作	备注
用户子网	CLEAN 接口	TCP	22		允许 SSH 连接到 TGSH 对话
用户子网	CLEAN 接口	TCP	80		设备 API 和 Threat Grid 用户界面。这将重定向到 HTTPS TCP/443
用户子网	CLEAN 接口	TCP	443		设备 API 和 Threat Grid 用户界面
用户子网	CLEAN 接口	TCP	9443		允许连接到 Threat Grid UI Glovebox

ADMIN 接口出站可选

以下取决于配置的服务。

源	目标	协议	端口	操作	备注
ADMIN 接口	NFSv4 服务器	TCP	2049	允许	“可选，仅当已配置 Threat Grid 设备以向 NFSv4 共享发送备份时为必需”

ADMIN 接口入站

源	目标	协议	端口	操作	备注
ADMIN 子网	ADMIN 接口	TCP	22	允许	允许 SSH 连接到 TGSH 对话
ADMIN 子网	ADMIN 接口	TCP	80	允许	允许访问 OpAdmin 门户接口。这将重定向到 HTTPS TCP/443
ADMIN 子网	ADMIN 接口	TCP	443	允许	允许访问 OpAdmin 门户接口

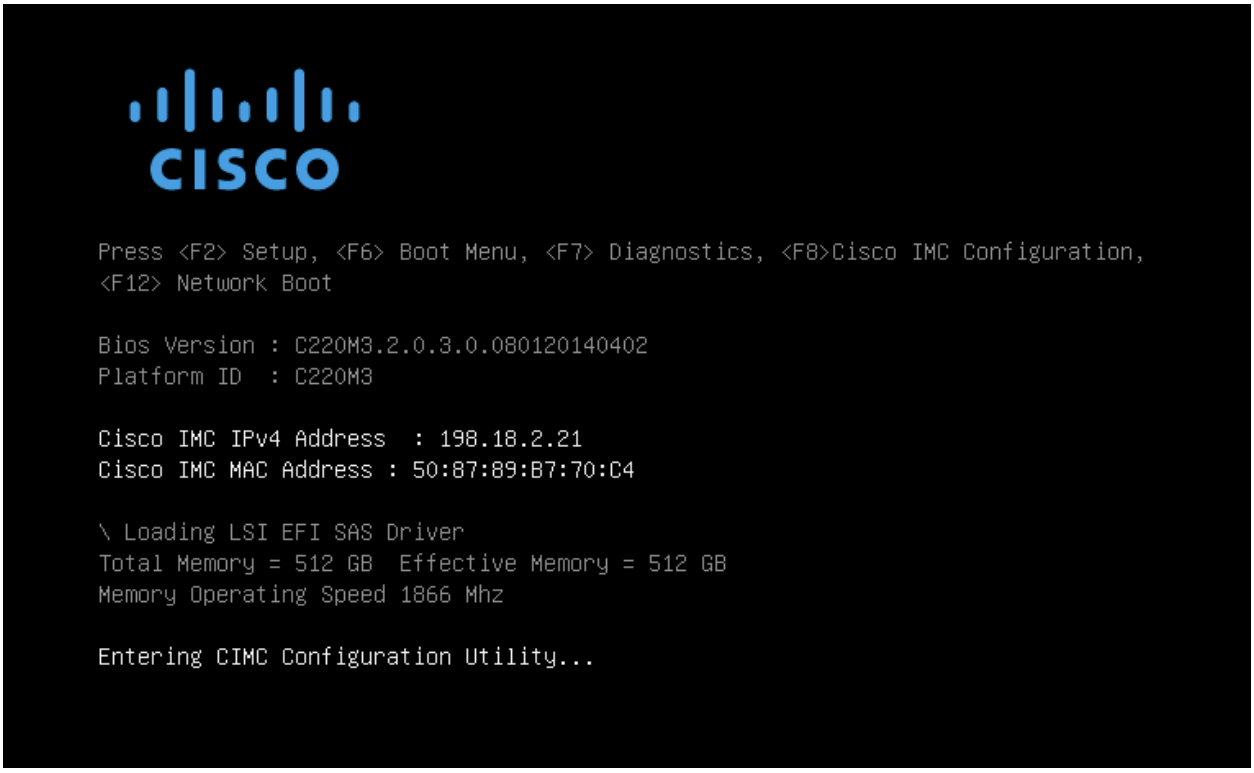
适用于非思科验证/建议的部署的 DIRTY 接口

源	目标	协议	端口	操作	备注
DIRTY 接口	互联网	TCP	22	允许	“更新、支持快照和许可服务”
DIRTY 接口	互联网	TCP/UDP	53	允许	允许出站 DNS
DIRTY 接口	互联网	UDP	123	允许	允许出站 NTP
DIRTY 接口	互联网	TCP	19791	允许	允许连接到 Threat Grid 支持
DIRTY 接口	思科资安防护伞	TCP	443	允许	与第三方检测和增强服务连接
DIRTY 接口	VirusTotal	TCP	443	允许	与第三方检测和增强服务连接
DIRTY 接口	TitaniumCloud	TCP	443	允许	与第三方检测和增强服务连接

通电和启动

连接了服务器外围设备和网络接口（请勿忘记连接并插入网线）之后，请接通设备电源并等待它启动。思科屏幕会短暂显示：

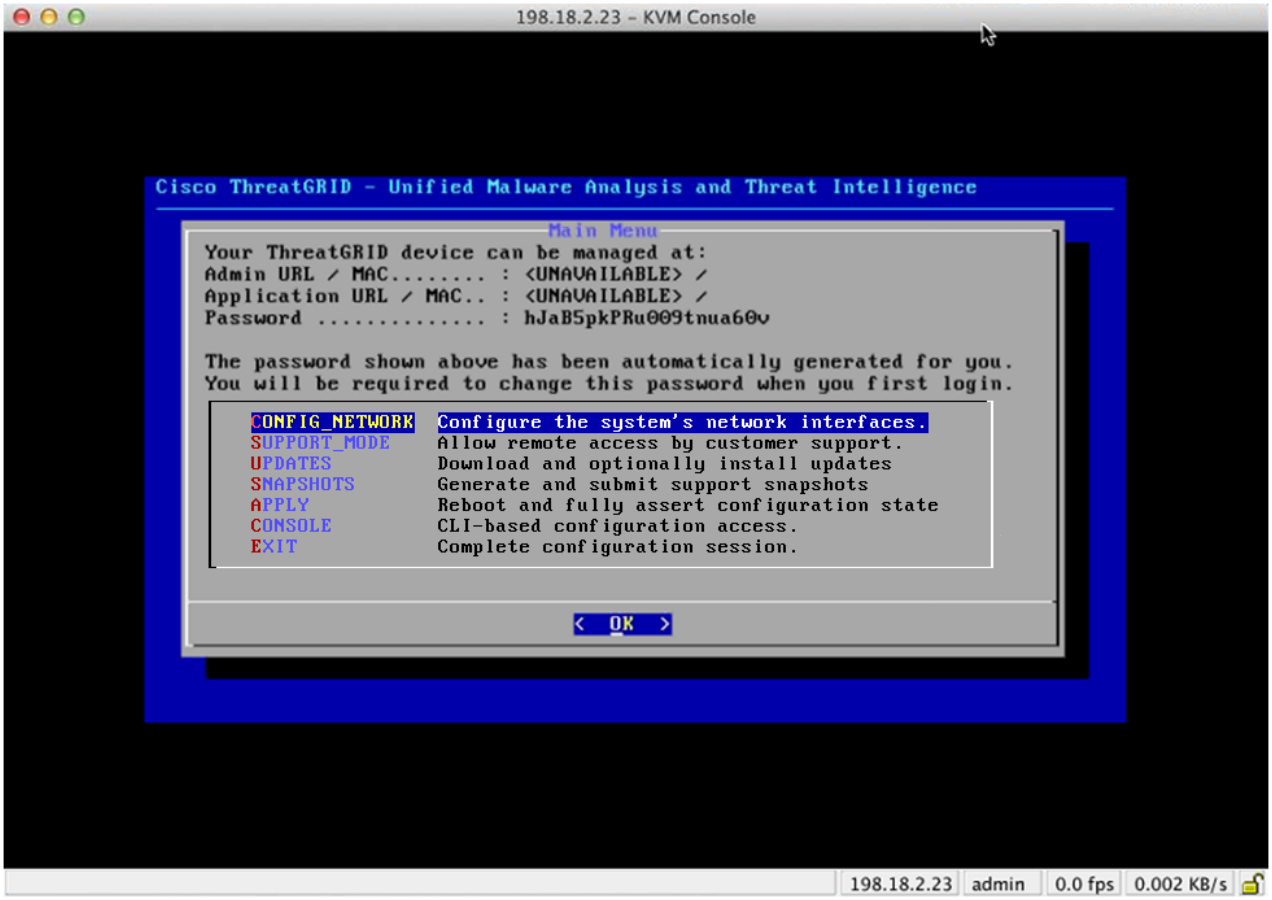
图 8 - 启动期间的思科屏幕



注意：如果您要配置此接口，请在完成内存检查后按 **F8**，然后按照附录 A “配置 CIMC”中的说明操作。

成功启动并连接服务器后，控制台上将显示 **TGSH 对话**：

图 9 - TGSH 对话



ADMIN URL 显示为不可用 - 网络接口连接尚未配置，因此无法访问 OpAdmin 门户来执行此任务。

注意：将管理员密码记录到一个单独的文本文件中，以便在 OpAdmin 门户配置过程中使用（复制粘贴）。

重要信息：TGSH 对话将显示初始管理员密码，稍后在配置工作流步骤中访问和配置 OpAdmin 门户接口时需要该密码。

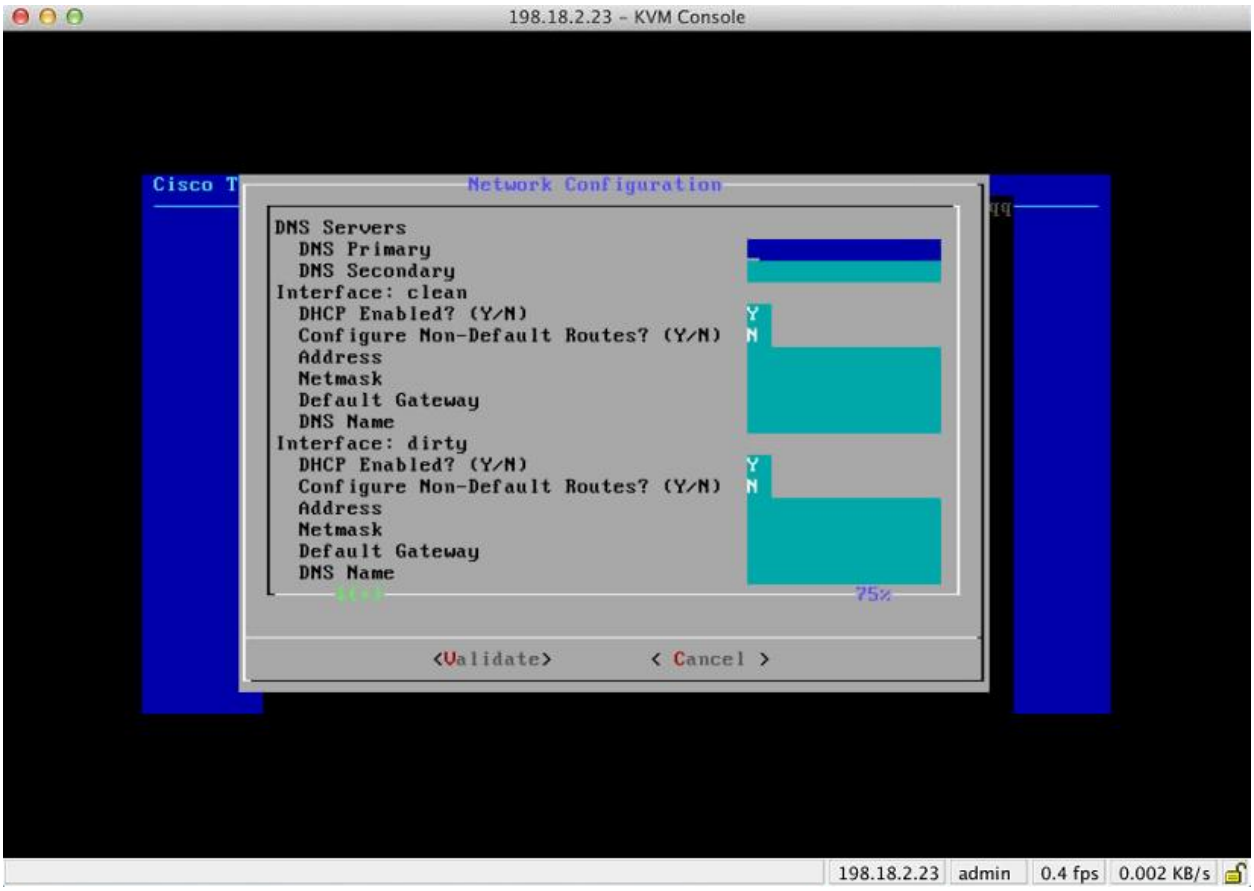
初始网络配置 - TGSH 对话

初始网络配置在 TGSH 对话中完成。此操作的目标是完成基本配置，从而允许访问 OpAdmin 界面工具以完成其余的配置，包括许可证、邮件主机、SSL 证书等。

DHCP 用户：以下步骤假设您使用的是静态 IP 地址。如果您使用 DHCP 获取 IP 地址，则请参阅《*Threat Grid 设备管理员指南*》了解详细信息。

1. 在 TGSH 对话界面中，选择 **CONFIG_NETWORK**。网络配置控制台将会打开：

图 10 - TGSH 对话 - 网络配置控制台

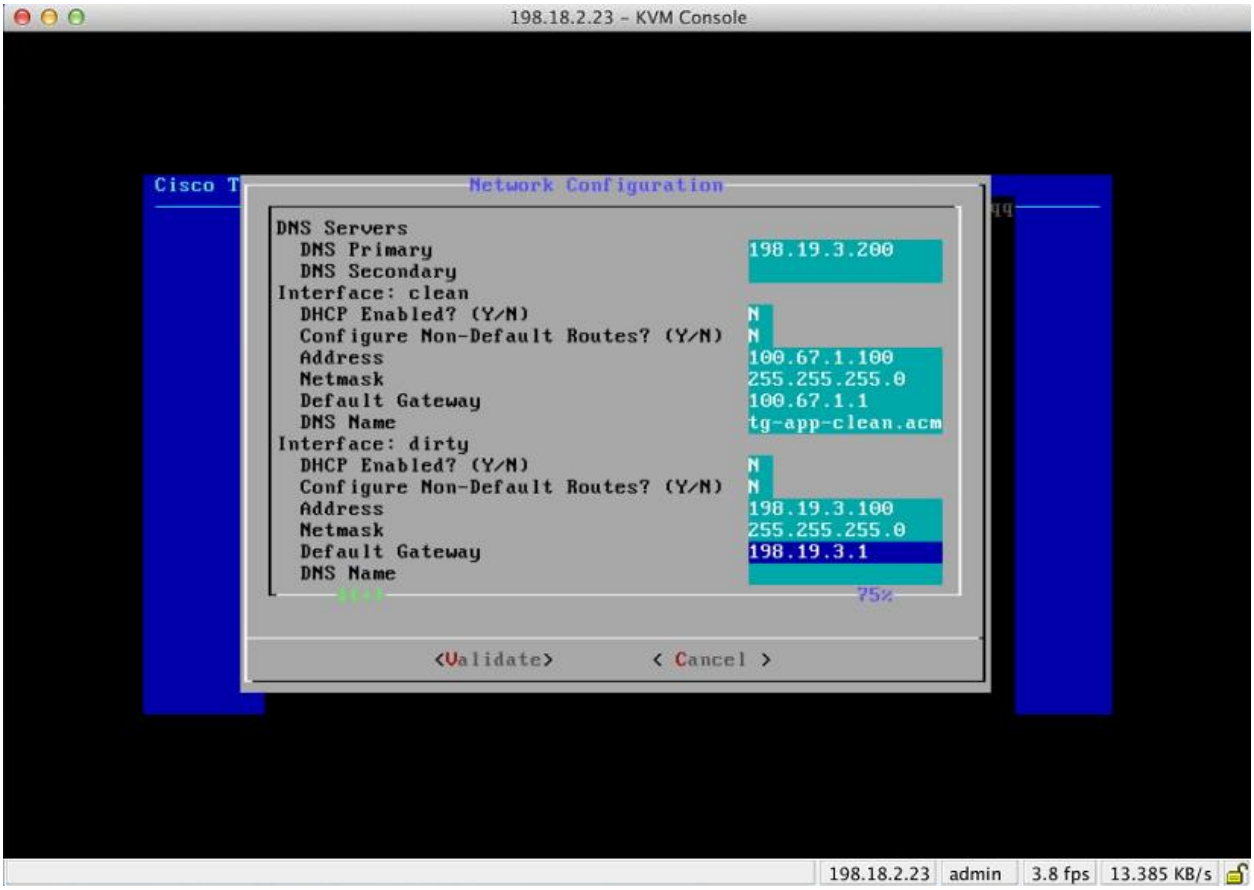


2. 根据您的网络管理员为 CLEAN、DIRTY 和 ADMIN 接口提供的设置填写空白字段。
3. 将**启用 DHCP** 从**是**更改为**否**。

   注意：您需要使用**退格键**删除原字符，才能再输入新的字符。

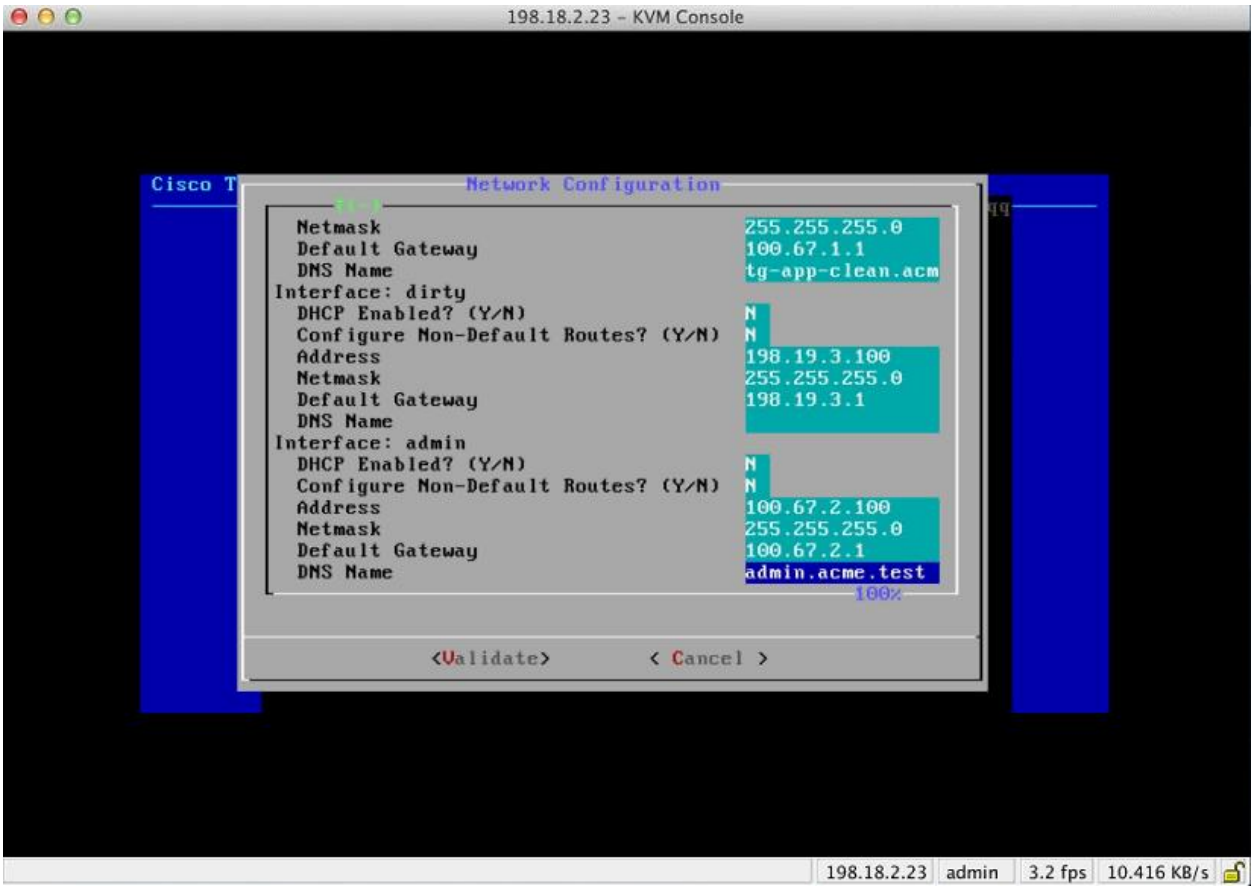
4. **DNS 名称。**如果您的网络为 CLEAN 网络使用了 DNS 名称，则在此处输入该名称。
5. 将**配置非默认路由?** 保留为默认的**否**（除非需要其他路由）。

图 11 - 正在进行网络配置（CLEAN 和 DIRTY）



6. 将 DIRTY 网络的 **DNS 名称**留空。

图 12 - 正在进行网络配置 (ADMIN)

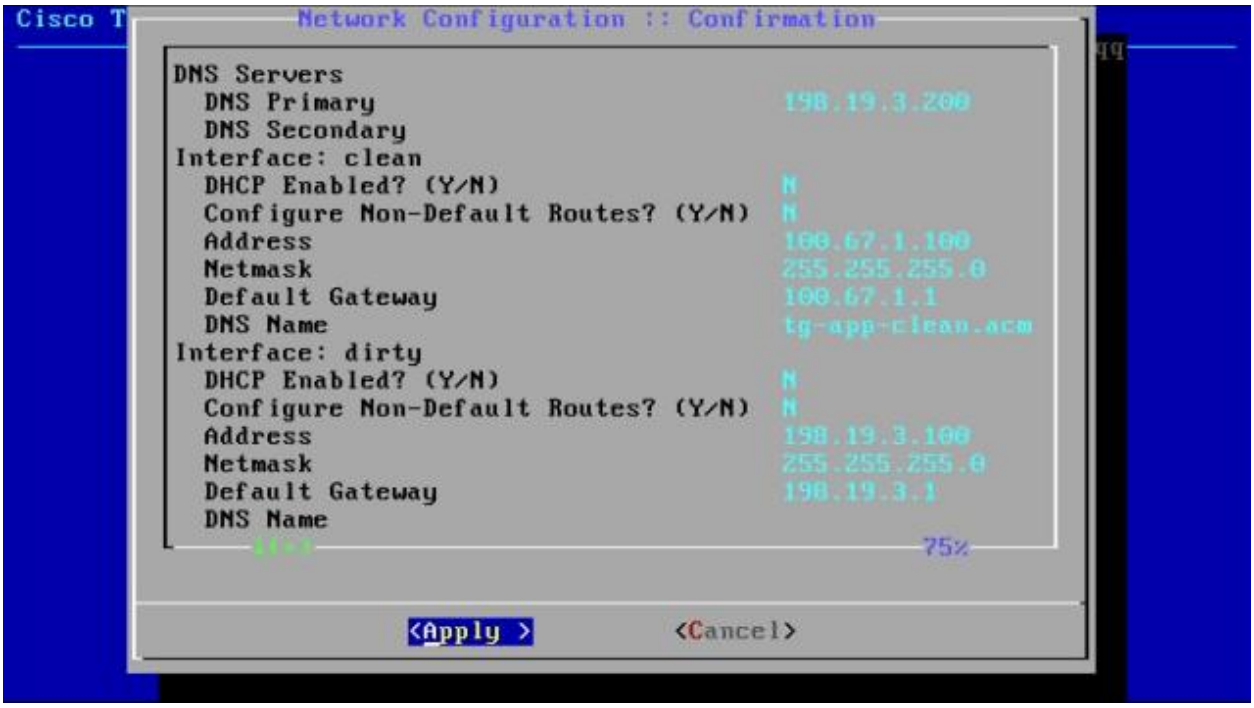


7. 输入了所有网络设置后，按 Tab 键向下移动，然后选择**验证**来验证您输入的内容。

   如果输入了无效值，可能会显示错误。如果是这种情况，请修正错误并重新验证。

   在验证后，网络配置确认会显示您已输入的值：

图 13 - 网络配置确认

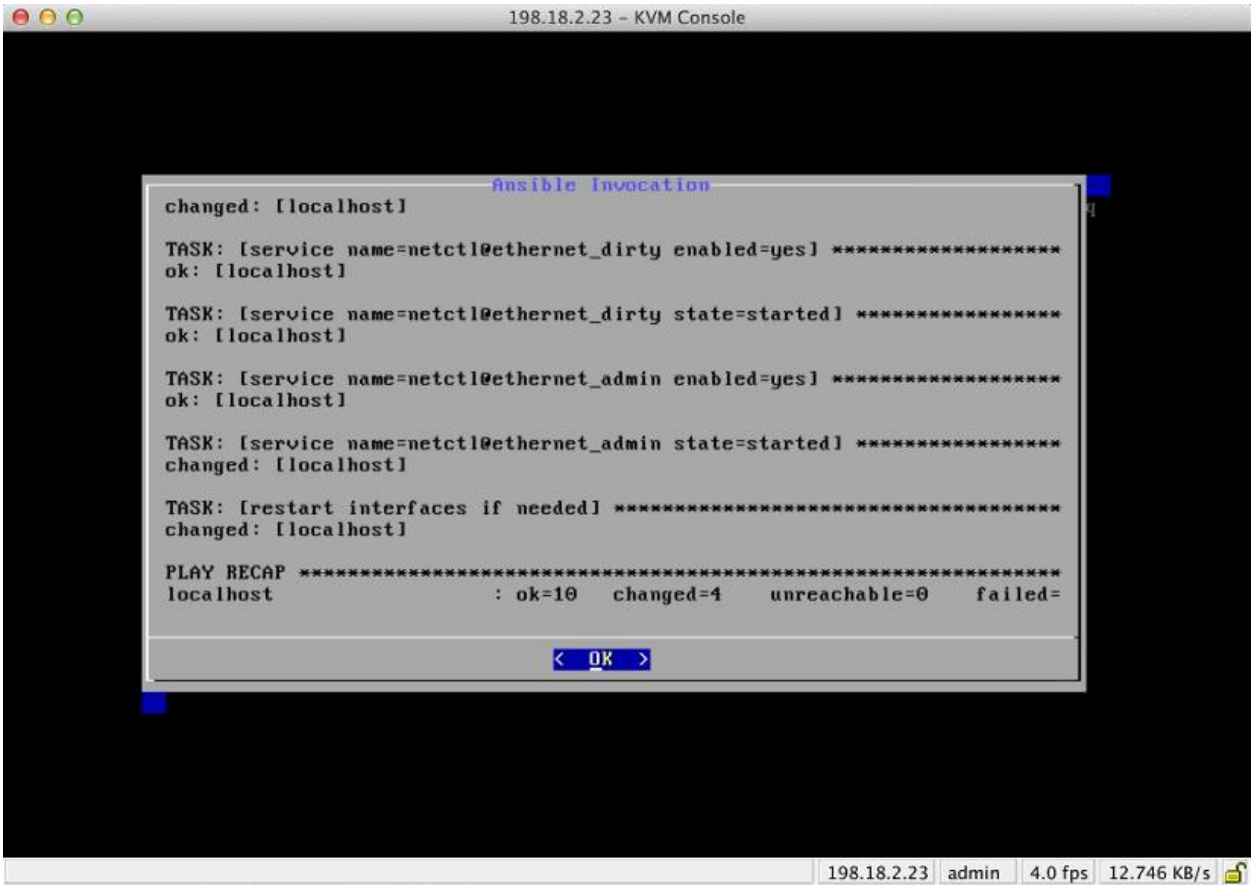


8. 选择**应用**以应用您的配置设置。

   请保持耐心。此步骤可能需要 10 分钟或更长时间才能完成。

   控制台将变为一个空白的灰色框，并且应用设置时屏幕可能会显示滚动配置信息，然后会列出有关所做配置更改的详细信息：

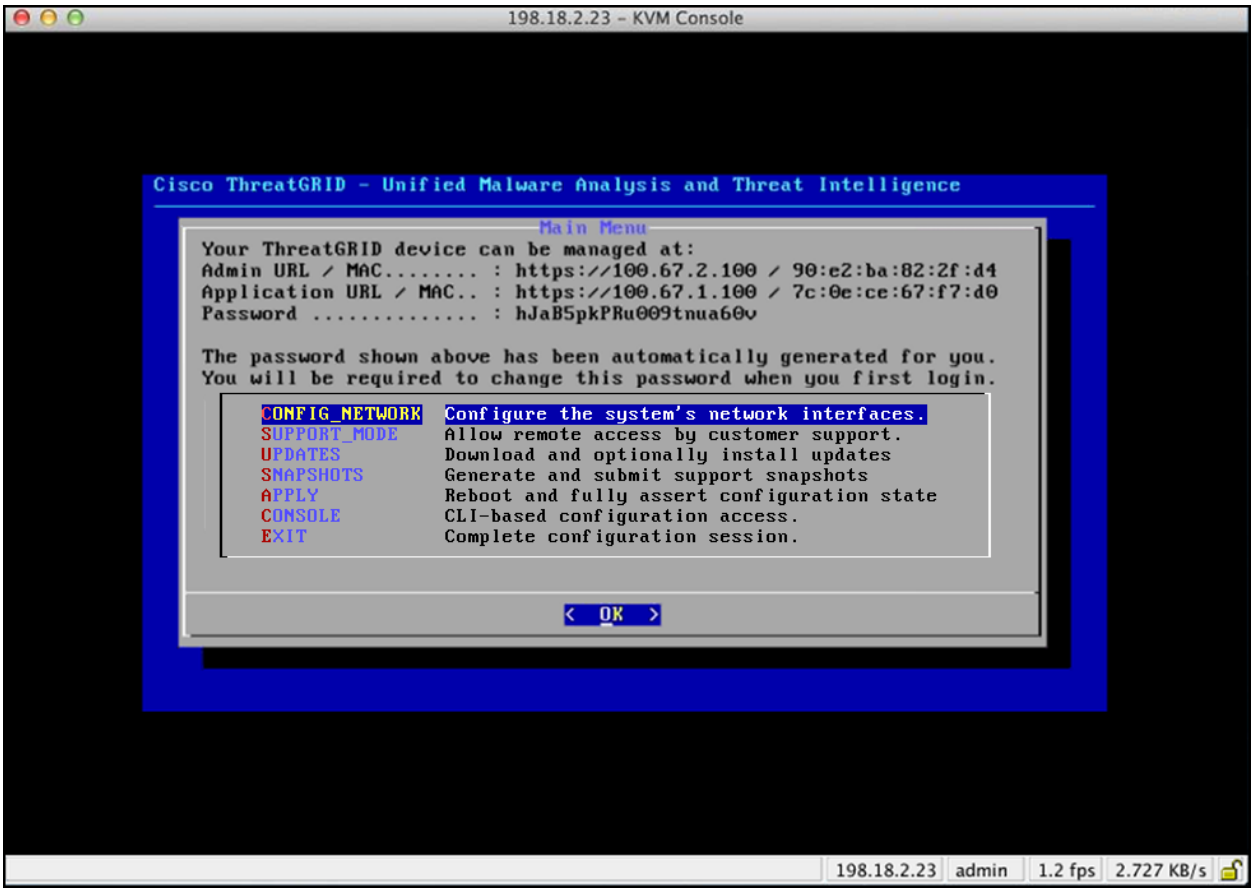
图 14 - 网络配置 - 更改列表



9. 点击**确定**。

   网络配置控制台再次刷新，并显示您输入的 IP 地址。

图 15 - IP 地址



您已完成了设备的网络配置。

注意： CLEAN 接口的 URL 需要等到 OpAdmin 门户配置完成之后才生效。

后续设置步骤：

设备设置过程中的下一个步骤是使用 OpAdmin 门户中的工作流按照下一部分中所述完成剩余配置任务。

配置向导 - OPADMIN 门户

OpAdmin 门户是设备上的 Threat Grid 管理员的门户。这是一个网络用户界面，在 ADMIN 接口上配置 IP 地址后即可使用。

OpAdmin 门户是推荐使用的设备配置工具，而事实上，大量的设备配置也只能通过 OpAdmin 门户界面完成，包括：

- OpAdmin 门户管理员的密码
- 邮件服务器
- DNS 服务器
- NTP 服务器
- SSL 证书
- 集群
- 其他服务器设置
- https://<adminIP>/ 或 https://<adminHostname>/

注意： 并非所有这些设置都是在初始 OpAdmin 门户配置向导工作流中完成。一些设置（例如 SSL 证书和集群）需通过单独的步骤完成，如《*Threat Grid 设备管理员指南*》中所述。该指南可在 cisco.com 的 Threat Grid 设备文档页面中找到。

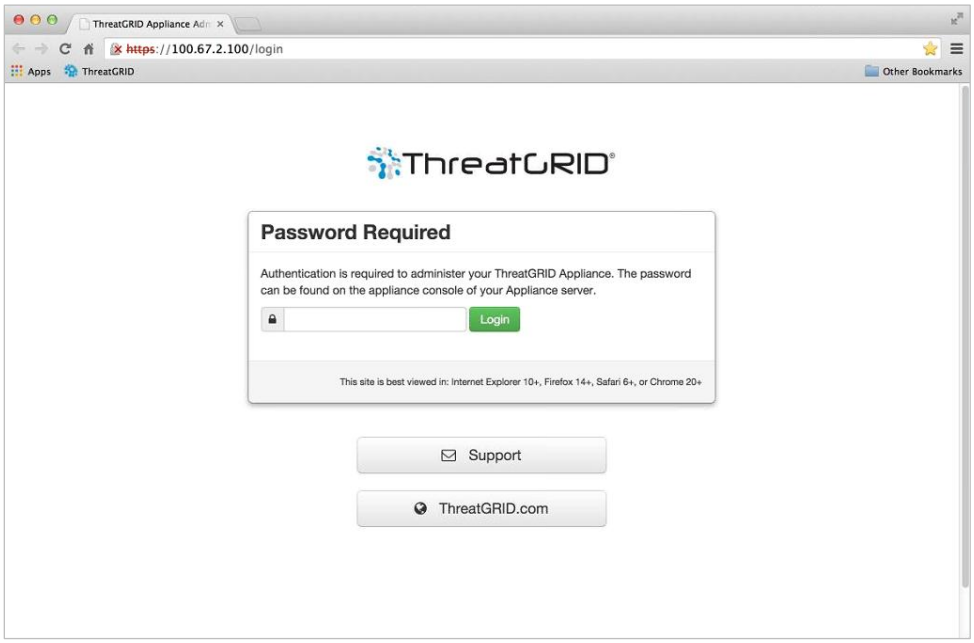
配置工作流

以下部分中的步骤应在一个会话中完成，以减少配置期间中断 IP 地址的可能性。

登录到 OpAdmin 门户

1. 通过您的浏览器访问 OpAdmin 门户界面（带有“https”的 ADMIN URL）。Threat Grid OpAdmin 登录屏幕随即打开：

图 16 - OpAdmin 登录



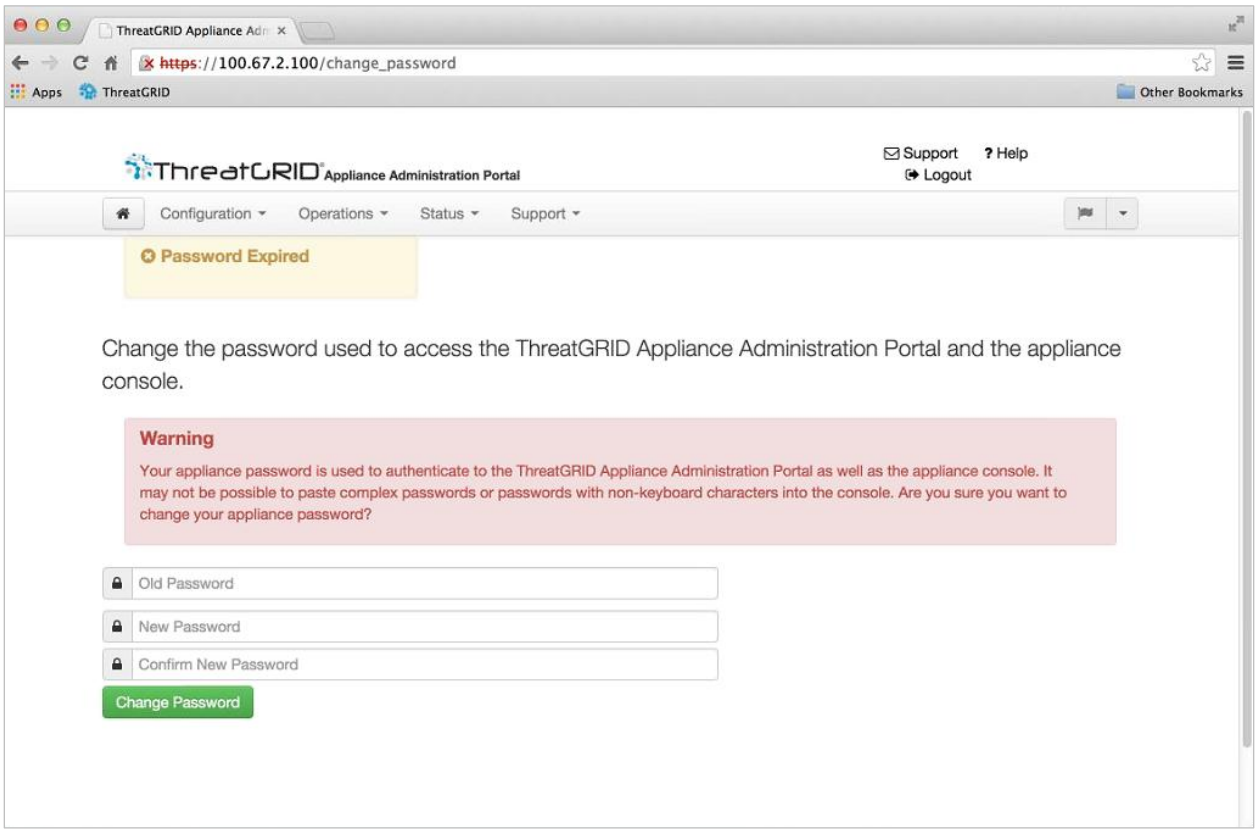
2. 输入您从 TGSH 对话复制的初始 Admin 密码并点击**登录**。*更改密码*页面将会打开。

继续进行下一部分：

Admin 密码更改

初始管理员的密码是在出厂前的 Threat Grid 安装过程中随机生成的，在 TGSH 对话中显示为纯文本。您必须更改初始的 Admin 密码，才能继续配置工作流。

图 17 - OpAdmin 更改密码



1. 从 TGSH 对话的**旧密码**字段中输入密码。（您现在应该将此密码记录在一个文本文件中以备日后使用。）
2. 输入新密码，并确认此密码。
3. 点击**更改密码**。

   密码将会更新。*最终用户许可协议*页面将会打开。

   注意：新密码在 TGSH 对话中不会显示为可见文本，因此请务必要将其记录在某个地方。

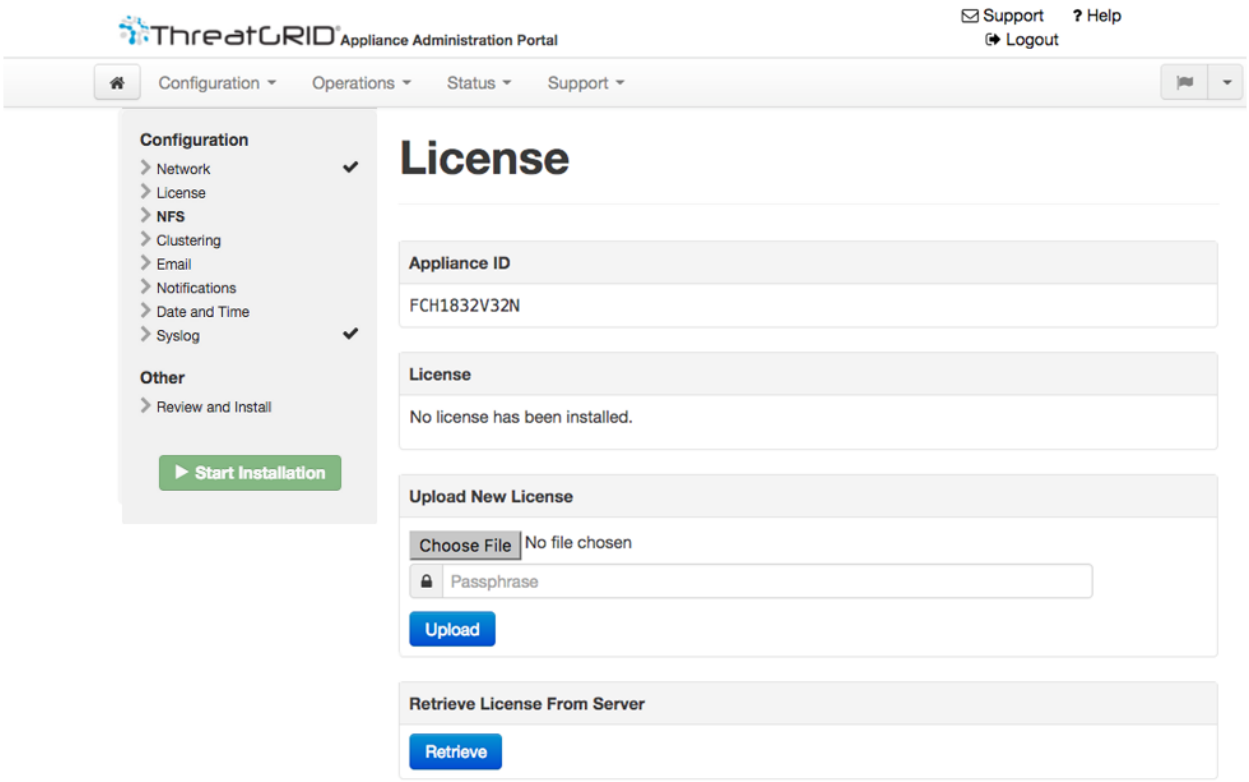
   如果密码丢失，请按照《*Threat Grid 设备管理员指南*》**支持**部分中的*丢失密码*相关说明操作。

继续进行下一部分：

最终用户许可协议

1. 查看最终用户许可协议。
2. 向下滚动到末尾，点击**我已阅读并同意**。*许可证*页面将会打开：

图 18 - “许可证”页面



我们建议您遵照配置工作流程操作，并*在安装许可证之前配置网络*，如下一部分所述网络配置设置。

网络配置设置

如果您在 TGSH 对话中配置了静态网络设置，则在“网络配置”页面中显示的 IP 地址将反映设备网络配置期间您在 TGSH 对话中输入的值。

网络配置和 DHCP

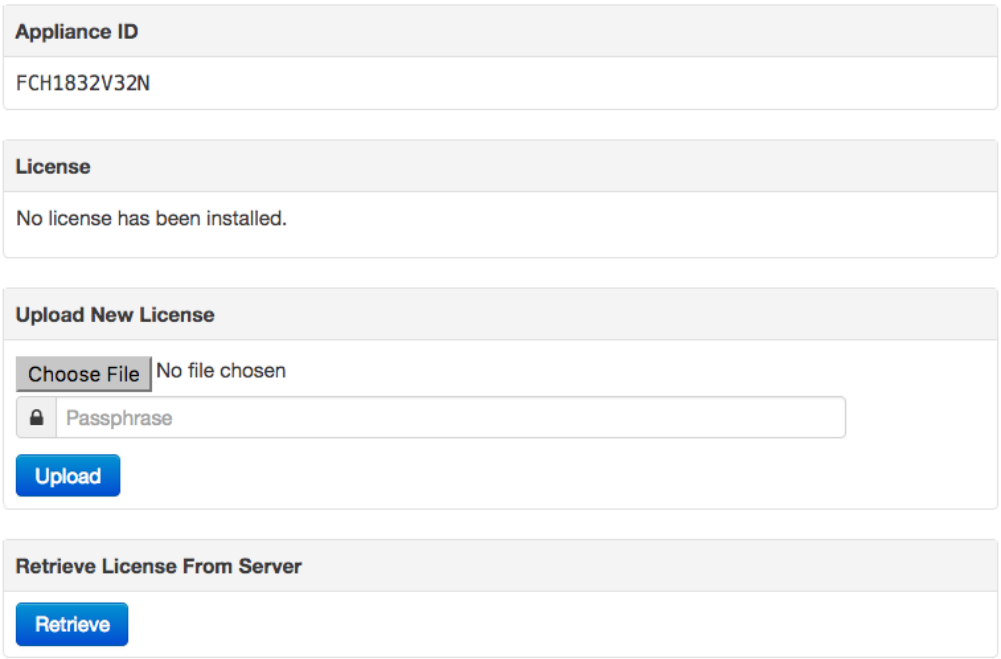
如果您使用 DHCP 进行初始连接并且现在需要将 CLEAN 和 DIRTY IP 网络更改为静态 IP 地址，则按照《*Threat Grid 设备管理员指南*》中***网络 > 使用 DHCP*** 部分中的步骤操作。

继续进行下一部分：

许可证安装

配置网络之后，您即可安装 Threat Grid 许可证。（在 1.4.4 版之前的版本中，您需要启动支持模式才能使许可证被接受。有关详细信息，请参阅启动支持模式 - 1.4.4 版之前的许可证解决方法。）

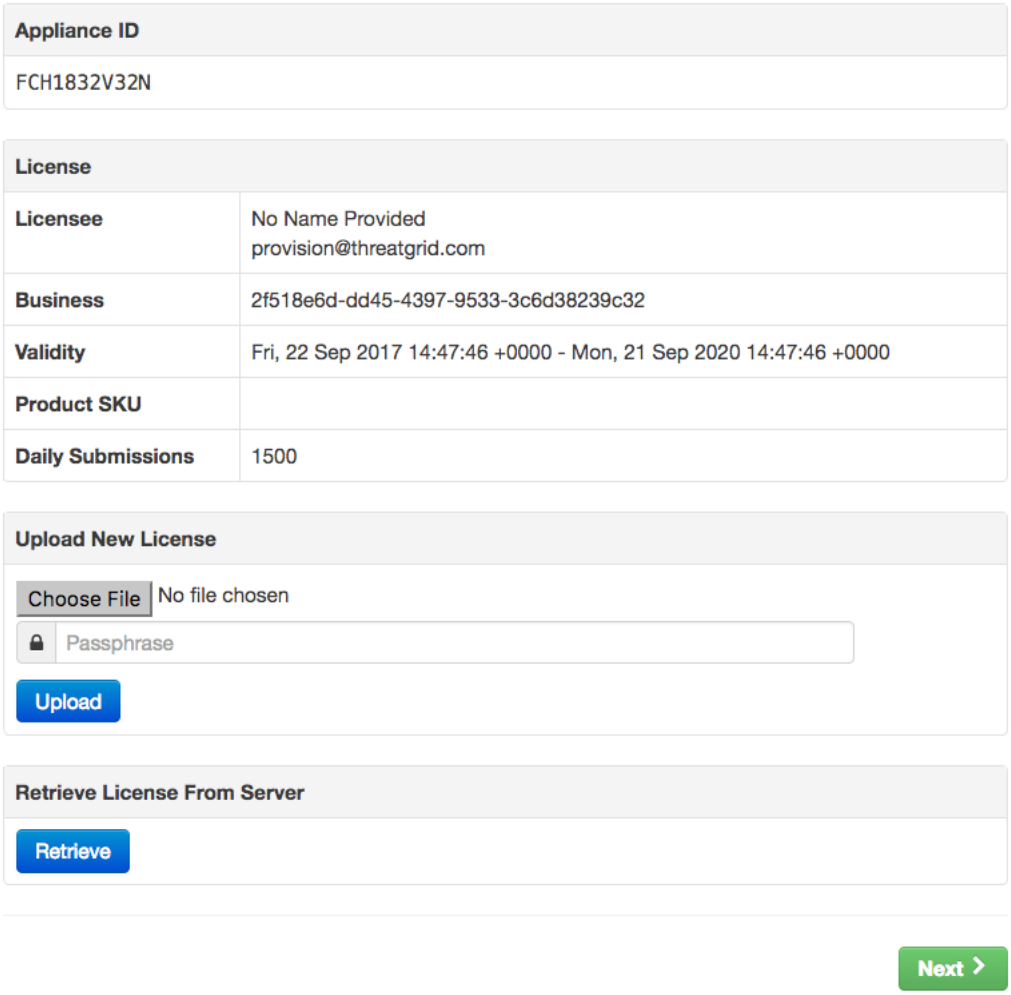
图 19 - 安装前的许可证页面



1. 点击左侧列中的**许可证**。打开*许可证*页面，如上图所示。尚未安装许可证。
2. 在**上传新许可证**下点击**选择文件**，然后从您的文件管理器中选择许可证。

   从服务器检索许可证 - 此外，2.3 版本中也增加了用于选择**检索**的功能。如果设备安装时已具有网络访问权限，则选择此选项将检索网络上的许可证。
3. 将您收到的许可证密码输入“密码”字段中。
4. 点击**上传**进行安装。页面将会刷新，然后您应该会看到您的许可证信息：

图 20 - 成功安装后的许可证信息



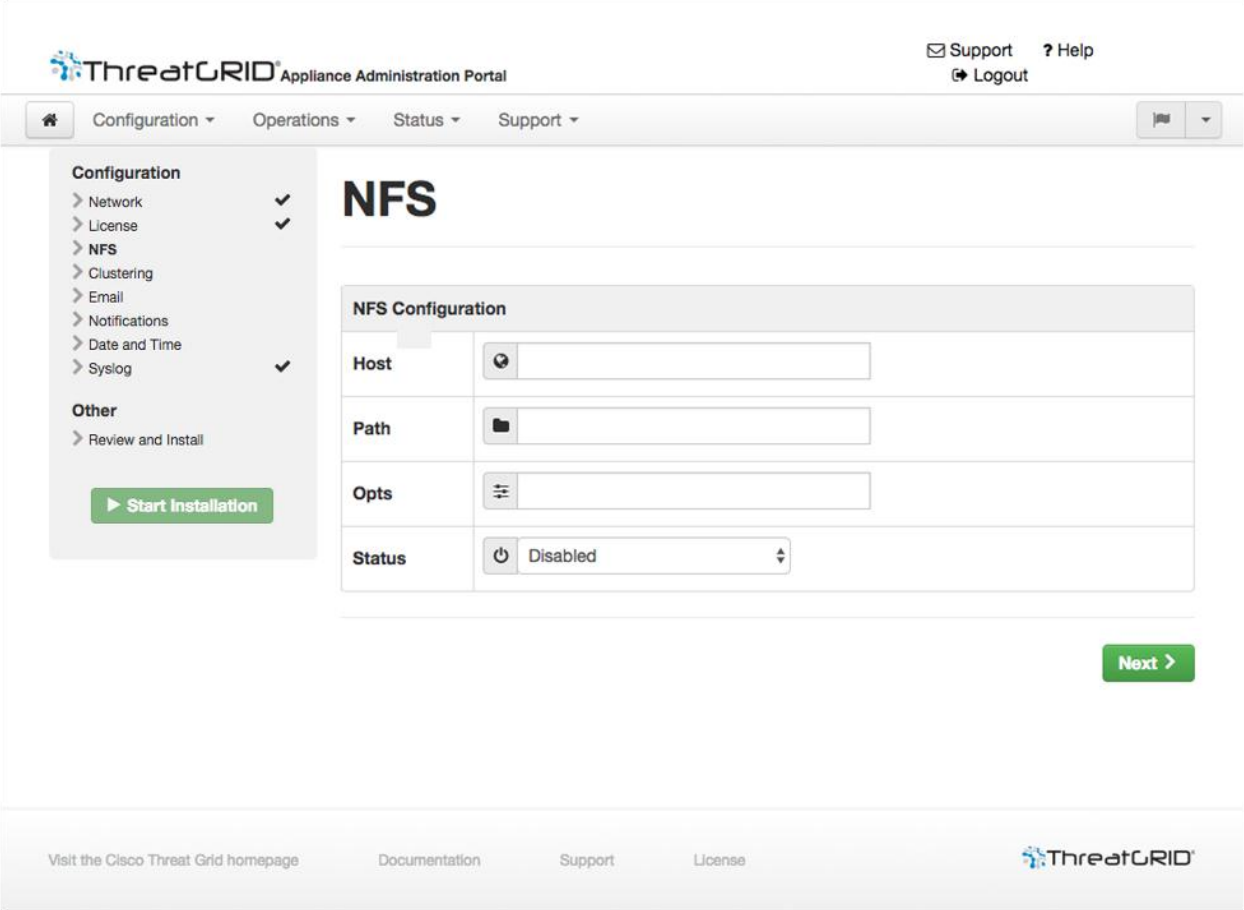
点击 **Next** 继续操作。“***邮件***”**页面**随即打开。

继续进行下一部分：

NFS 配置

工作流程的下一步是 NFS 配置。对于备份和集群，必须执行此任务。（相关详细信息，请参阅《*Threat Grid 设备指南*》中“备份”部分中的 NFS 要求。）

图 21 - NFS 配置



1. 点击左侧列中的 **NFS**。*NFS* 页面随即打开。
2. 按如下方式配置页面：

   主机 - NFSv4 主机服务器。我们建议使用 IP 地址。

   路径 - NFS 主机服务器上的文件存储位置的绝对路径

   选项 - 若此服务器因 NFSv4 而需要不同于标准的 Linux 默认设置，则在此处设置可用的 NFS 安装选项。

   状态 - 从下拉列表中选择“**启用**”（密钥待定）。

3. 点击**下一步**。该页面将刷新并显示一个 **FS 加密密码密钥 ID**。

   第一次配置此页面时，可以看到**删除**或**下载**加密密钥的选项。如果您已启用 NFS，但尚未创建密钥，可以看到**上传**选项。创建密钥后，**上传**将改为**下载**按钮。（如果删除密钥，**下载**按钮将重新变成**上传**。）

   注意：如果该密钥与用于创建备份的密钥正确匹配，则上传后 OpAdmin 中显示的*密钥 ID* 将与已配置路径中的目录名称匹配。如前所述，如果没有加密密钥，将无法恢复备份。

   配置过程包括安装 NFS 存储、安装加密数据，以及从 NFS 存储的内容初始化设备本地数据存储的过程。

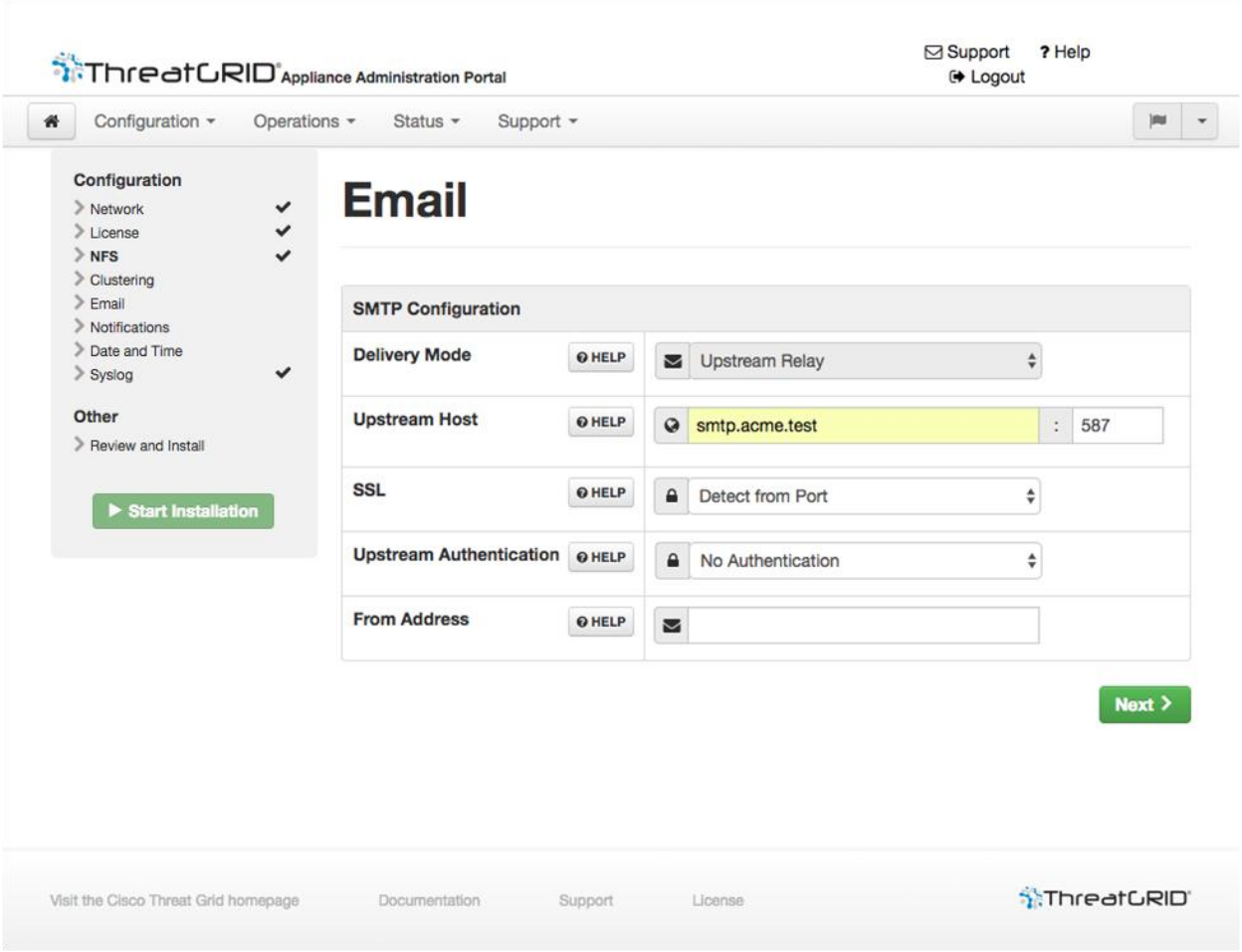
4. 点击**下一步**。“*邮件*”页面随即打开。

继续进行下一部分：

邮件主机配置

工作流程的下一步是配置邮件主机。

图 22 - 邮件主机配置



1. 点击左侧列中的**邮件**。*邮件*页面将会打开。
2. 输入**上游主机**（邮件主机）的名称。
3. 将端口从 587 更改为 **25**。
4. 其他设置保留为默认值。
5. 点击**下一步**。*通知*页面将会打开。

继续进行下一部分：

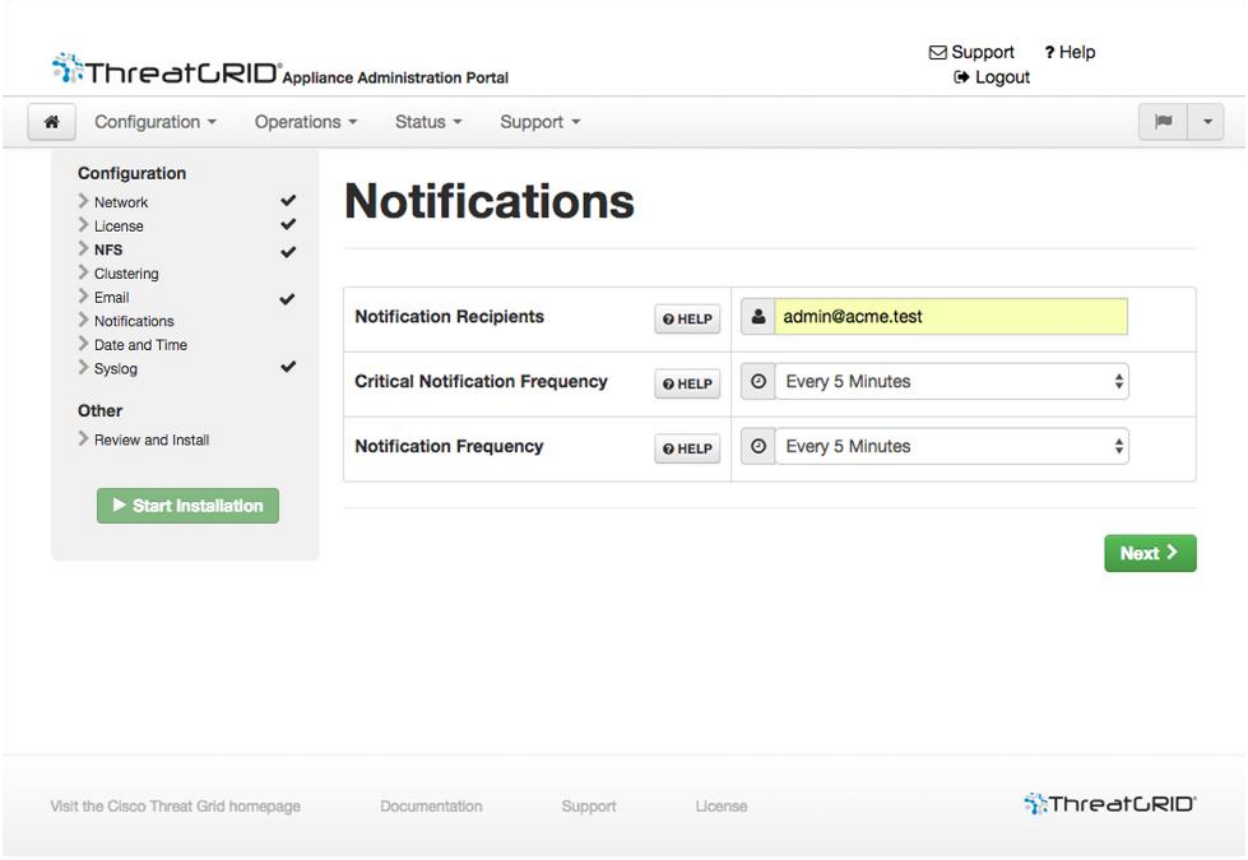
服务器通知配置

工作流程的下一步是配置可以定期发送到一个或多个邮件地址的通知。系统通知将显示在 Threat Grid 门户界面中，但此页面允许您设置也可以通过邮件发送的通知。

系统日志配置

v1.3 更新中包括一个页面，可用来配置一个系统日志服务器以接收系统日志消息和 Thread Grid 通知。有关详细信息，请参阅《*Threat Grid 设备管理员指南*》。

图 23 - 通知配置



1. 首先，通过从下拉列表中选择**重要通知频率**和**通知频率**对其进行设置。
2. 然后，在**通知接收人**中，输入一个或多个邮件地址（以逗号隔开）。
3. 点击**下一步**。*日期和时间*页面将会打开。

继续进行下一部分：

NTP 服务器配置

可在此处识别 NTP（“网络时间协议”）服务器。

1. 输入 **NTP 服务器** IP 或 NTP 名称。

如果有多个 NTP 服务器，请以空格或逗号将其隔开。

2. 忽略当前系统时间并与浏览器同步。
3. 点击**下一步**。

   *查看和安装*页面将会打开，并且所有配置步骤旁边都显示复选框。

继续进行下一部分：

查看和安装配置设置

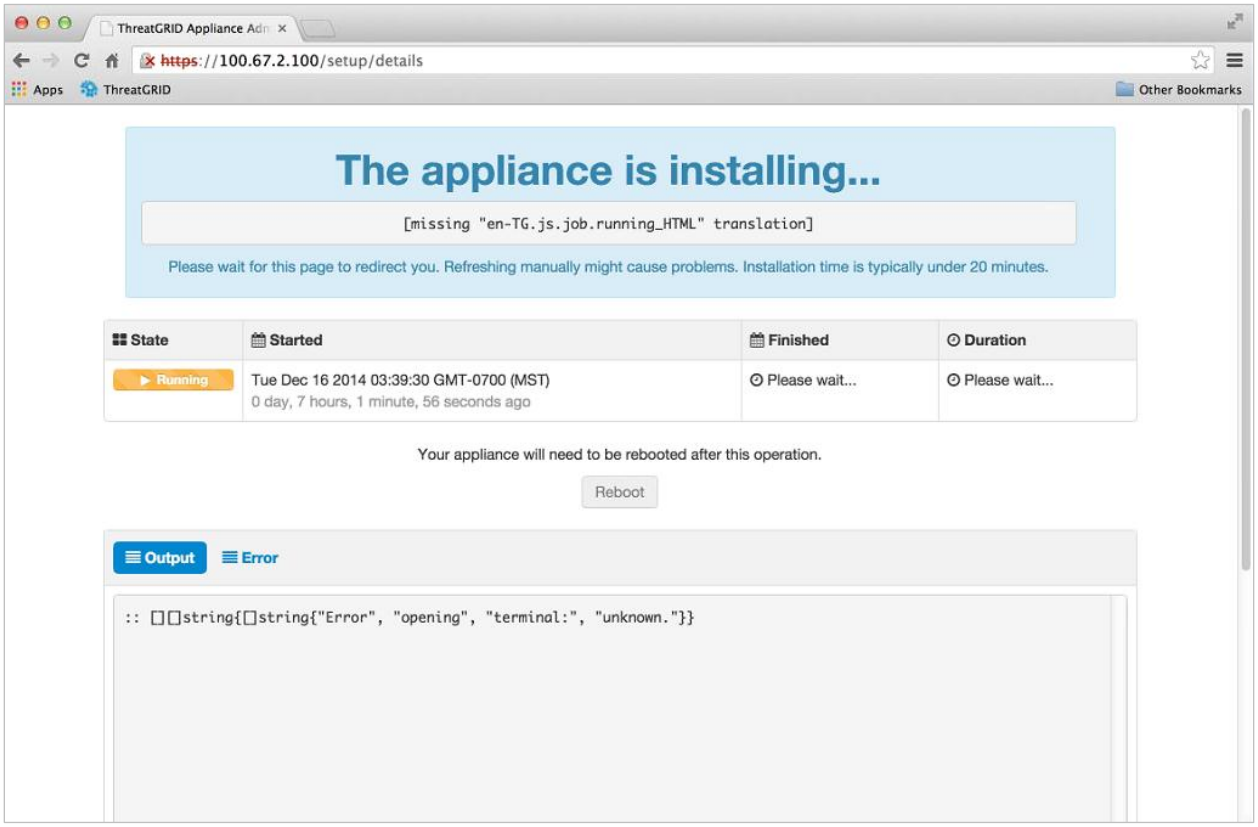
输入了网络配置设置后，必须按照如下所述安装这些设置。

1. 在*查看和安装*页面中，点击**开始安装**。

   将会安装配置脚本，并且您会看到消息：“*设备正在安装...*”。

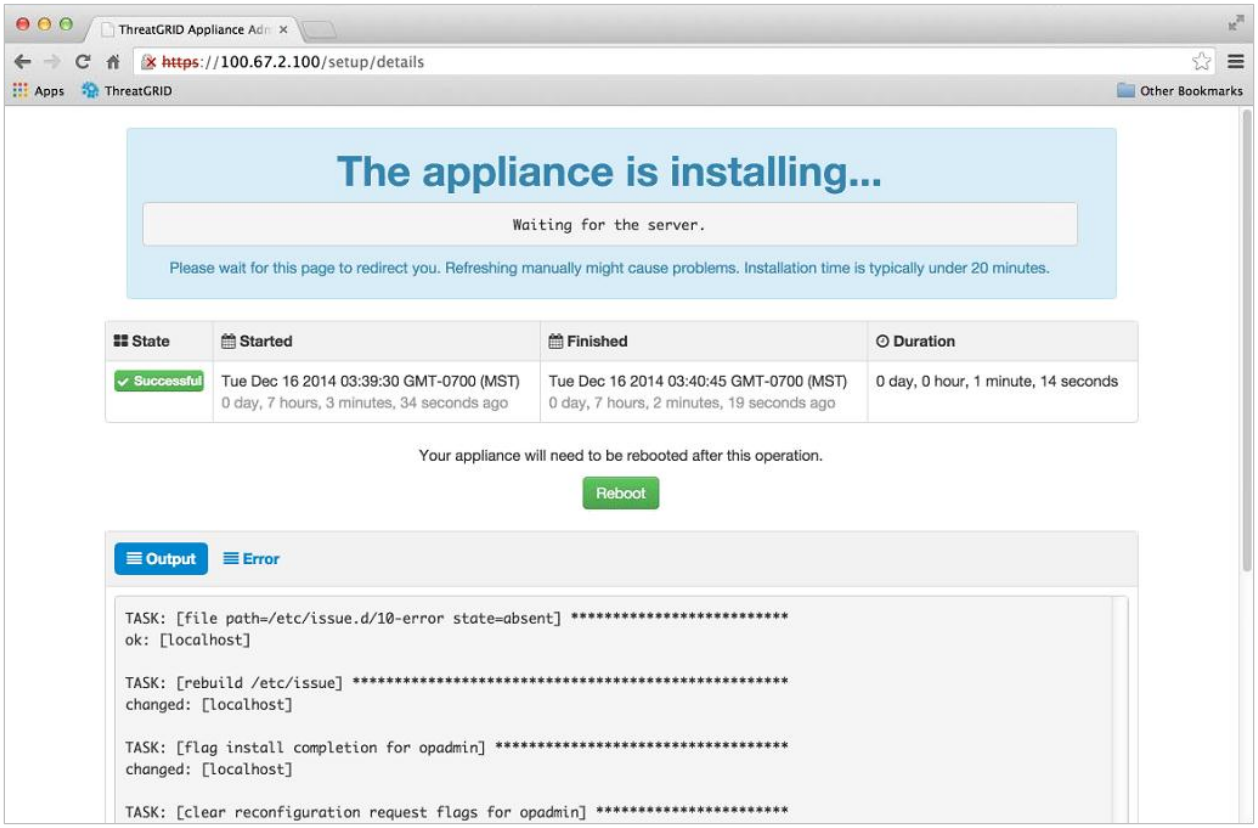
注意：请保持耐心。完成此步骤可能需要 10 多分钟的时间。应用配置之后，屏幕将会显示配置信息。

图 24 - 设备正在安装



2. 成功安装后，状态将从橙色的**正在运行**更改为绿色的**成功**消息，以确认安装成功。**重新启动**按钮将变为绿色，并显示配置输出：

图 25 - 成功的设备安装

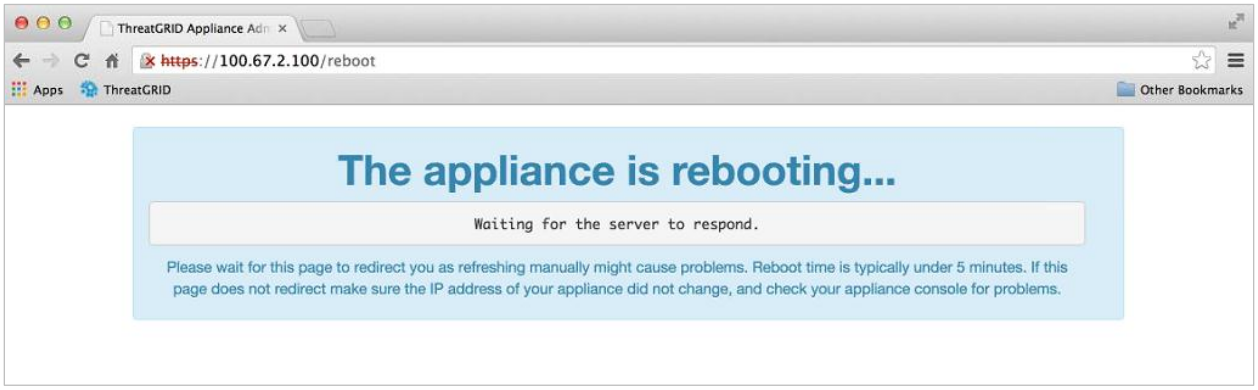


3. 成功安装之后，点击**重新启动**。您会看到消息“*设备正在重新启动*”。

   重新启动过程可能需要长达 5 分钟时间。

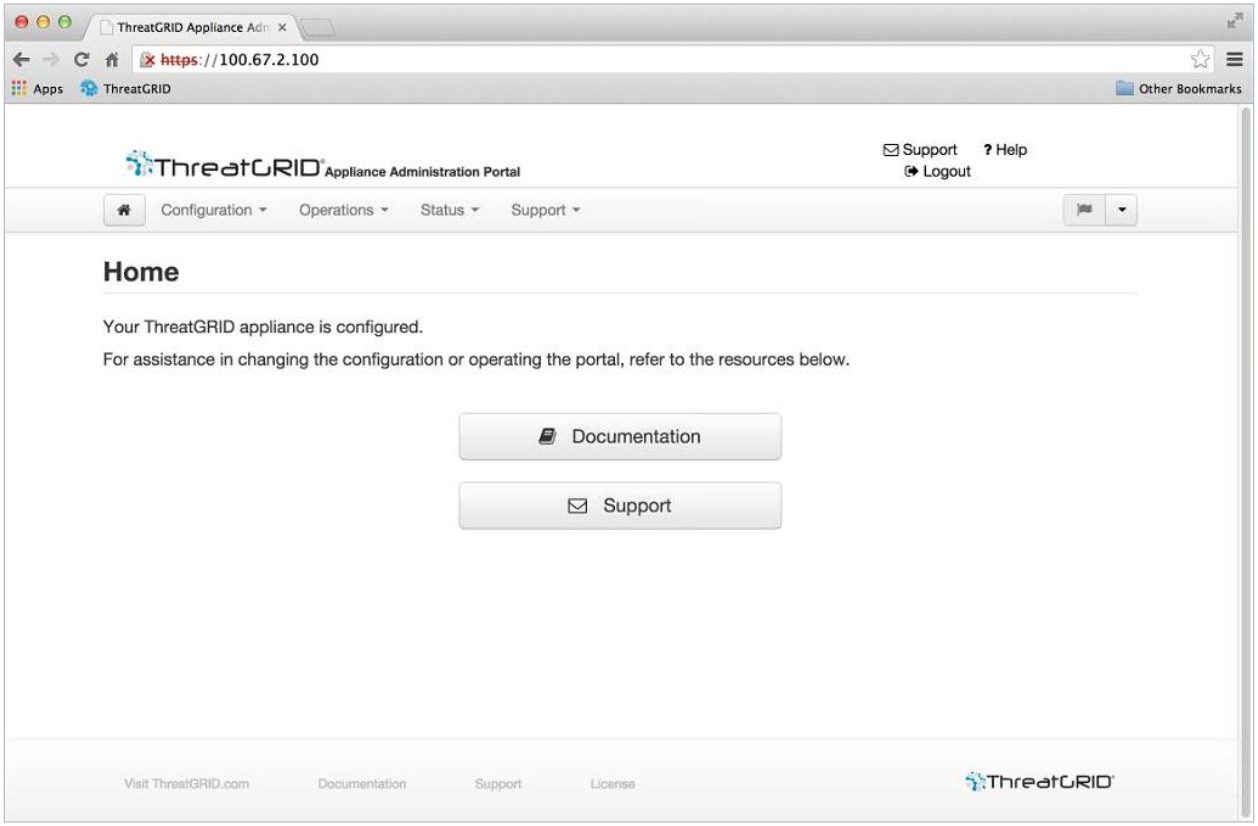
设备重新启动时，请勿做任何更改。

图 26 - 设备正在重新启动



设备成功重新启动之后，您将看到确认设备已配置的消息：

图 27 - 设备已配置



设备现在已经设置并且初始配置已完成。

安装 THREAT GRID 设备更新

完成初始的 Threat Grid 设备设置之后，建议您安装任何可用的更新，然后再继续。

Threat Grid 设备更新通过 **OpAdmin** 门户来应用。

从**操作**菜单中，选择**更新设备**。更新页面将会打开，其中显示设备当前的内部版本号。

点击**检查/下载更新**。该软件将检查是否有 Threat Grid 设备软件的最新更新/更新版本，如果有，则下载。这可能要花点时间。

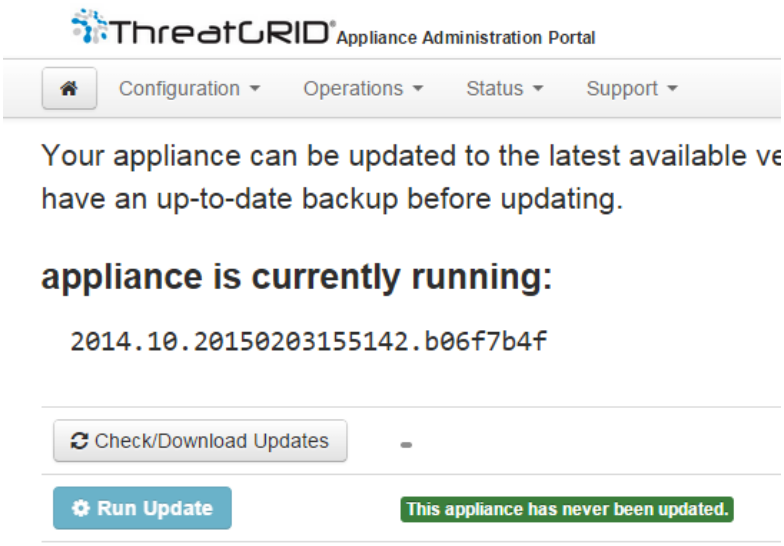
下载更新之后，点击**运行更新 (Run Update)** 安装它们。

有关安装更新的详细信息，请参阅《*Threat Grid 设备管理员指南*》。

设备内部版本号

可以在“更新”页面上查看设备的内部版本号：OpAdmin **操作** > **更新设备**：

图 28 - 设备内部版本号



内部版本号/版本查询表

可以在“更新”页面上查看设备的内部版本号（OpAdmin **操作** > **更新设备**），如上图所示。设备内部版本号与以下版本号相对应：

内部版本号	版本	发布日期	说明
2017.12.20180601200650.e0c052b0.rel	2.4.3.3	2018 年 6 月 1 日	修复集群初始化、修剪过时的 ES/PG 迁移支持
2017.12.20180519011227.ed8a11e9.rel	2.4.3.2	2018 年 5 月 19 日	适用于 CVE-2018-1000085 的 ClamAV 更新。漏洞修复。
2017.12.20180501005218.4e3746f4.rel	2.4.3.1	2018 年 5 月 1 日	更新检查时用于 DDL 错误检测的 PG 架构报告
2017.12.20180427231427.e616a2f2.rel	2.4.3	2018 年 4 月 27 日	远程虚拟出口定位；直接“单机到集群”迁移
2017.12.20180302174440.097e2883.rel	2.4.2	2018 年 3 月 2 日	集群
2017.12.20180219033153.bb5e549b.rel	2.4.1	2018 年 2 月 19 日	OpAdmen 支持集群。将门户软件刷新到 3.4.59。
2017.12.20180130110951.rel	2.4.0.1	2018 年 1 月 30 日	ClamAV 安全更新
2017.12.20171214191003.4b7fea16.rel	2.4	2017 年 12 月 14 日	集群 EFT。jp/kr contsubs。将门户刷新到 3.4.57。
2016.05.201711300223355.1c7bd023.rel	2.3.3	2017 年 11 月 30 日	2.4 升级程序的起点
2016.05.20171007215506.0700e1db.rel	2.3.2	2017 年 10 月 7 日	ElasticSearch 分片数量减少。

内部版本号	版本	发布日期	说明
2016.05.20170828200941.e5eab0a6.rel	2.3.1	2017 年 8 月 28 日	漏洞修复。
2016.05.20170810212922.28c79852.rel	2.3	2017 年 8 月 11 日	自动下载许可证。将门户软件刷新到 3.4.47。
2016.05.20170710175041.77c0b12f.rel	2.2.4	2017 年 7 月 10 日	此版本引入了备份功能。
2016.05.20170519231807.db2f167e.rel	2.2.3	2017 年 5 月 20 日	此次要版本更新提供了不需要 Windows XP 即可运行的新出厂设置。
2016.05.20170508195308.b8dc88ed.rel	2.2.2	2017 年 5 月 8 日	次要版本更新，对网络配置和操作系统组件进行了若干更改以支持即将推出的功能。
2016.05.20170323020633.f82e66fe.rel	2.2.1	2017 年 3 月 24 日	禁用 SSLv3；修复一个资源问题
2016.05.20170308211223.c92516ee.rel	2.2 mfg	2017 年 3 月 8 日	仅在制造上有所更改。对客户无影响。未通过更新服务器进行部署。
2016.05.20170303034712.1b205359.rel	2.2	2017 年 3 月 3 日	有关存储迁移、修剪、Mask UI、多种处置的更新。
2016.05.20170105200233.32f70432.rel	2.1.6	2017 年 1 月 7 日	为 OpAdmin/ tgsh-dialog 提供 LDAP 身份验证支持
2016.05.20161121134140.489f130d.rel	2.1.5	2016 年 11 月 21 日	ElasticSearch5；修复 CSA 性能问题。
2016.05.20160905202824.f7792890.rel	2.1.4	2016 年 9 月 5 日	主要面向制造业

内部版本号	版本	发布日期	说明
2016.05.20160811044721.6af0fa61.rel	2.1.3	2016 年 8 月 11 日	离线更新支持密钥，支持 M4 擦除。
2016.05.20160715165510.baed88a3.rel	2.1.2	2016 年 7 月 15 日	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	2016 年 7 月 6 日	
2016.05.20160621044600.092b23fc	2.1	2016 年 6 月 21 日	
2015.08.20160501161850.56631ccd	2.0.4	2016 年 5 月 1 日	版本 2.1 更新的起点。必须先升级到版本 2.0.4，然后才能更新到版本 2.1。
2015.08.20160315165529.599f2056	2.0.3	2016 年 3 月 15 日	引入 AMP 集成、CA 管理和分离 DNS。
2015.08.20160217173404.ec264f73	2.0.2	2016 年 2 月 18 日	
2017.12.20180302174440.097e2883.rel	2.4.2	2018 年 3 月 2 日	集群
2017.12.20180219033153.bb5e549b.rel	2.4.1	2018 年 2 月 19 日	OpAdmen 支持集群。门户软件刷新到 3.4.59。
2017.12.20180130110951.rel	2.4.0.1	2018 年 1 月 30 日	ClamAV 安全更新
2015.08.20160211192648.7e3d2e3a	2.0.1	2016 年 2 月 12 日	
2015.08.20160131061029.8b6bc1d6	2.0	2016 年 2 月 11 日	强制从此版本更新到版本 2.0.1。
2014.10.20160115122111.1f09cb5f	1.4.6	2016 年 1 月 27 日	2.0.4 更新的起点。

内部版本号	版本	发布日期	说明
2014.10.20151123133427.898f70c2	v1.4.5	2015 年 11 月 25 日	
2014.10.20151116154826.9af96403	v1.4.4		
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1+hotfix1		
2014.10.20150203155142.b06f7b4f	v1.1		
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0+hotfix2 **注意：**版本 1.0+hotfix2 是强制更新，可对更新系统本身进行修复，使该系统无需拆分大文件即可对其进行处理。		
2014.10.20141125162158.8afc5e2f	v1.0		

注意：对于版本 1.0-1.2 而言，如果未在启动时插入接口，则可能需要重新启动。这是 1.3 版本之前的一个问题（需要 SFP 的任何接口除外，这样的接口在 1.3 版本之后仍需要在启动时插入）。插入 SFP 的网线可以安全地热插拔。

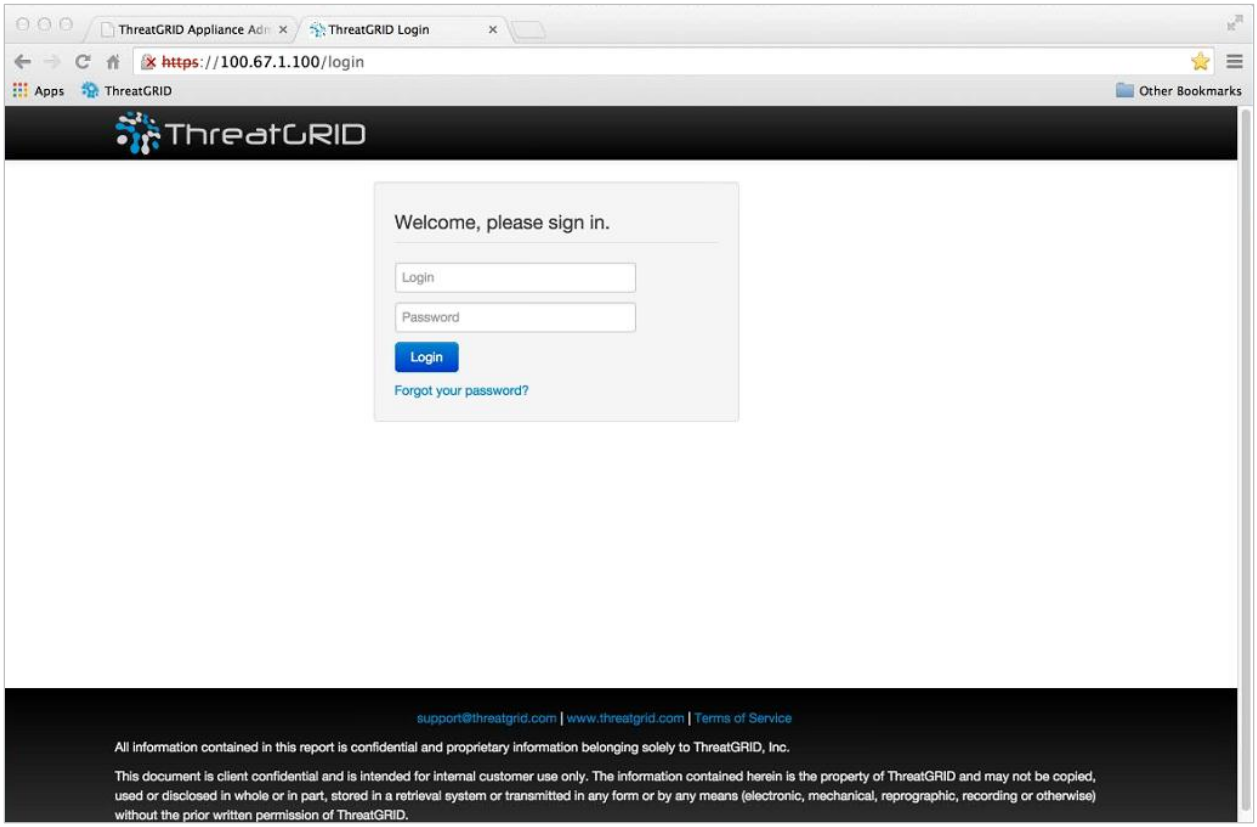
注意：从 1.0 更新至 1.0+hotfix2 的过程大约需要 15 分钟。从版本 1.0 应用完全更新升级至 1.3（无数据迁移）大约需要 30 分钟。

测试设置的设备 - 提交样本

Threat Grid 设备更新为当前版本之后，用来测试设备是否已正确配置的最终测试就是使用 Threat Grid 软件提交恶意软件样本。

1. 访问您配置为 CLEAN 接口的地址，登录 Threat Grid 门户。Threat Grid 登录页面将会打开：

图 29 - Threat Grid 门户登录页面



2. 输入默认的登录名称和密码：**admin/changeme**
3. 点击**登录**。主 Threat Grid *样本分析*页面将打开。
4. 在右上角的**提交样本**框中，选择样本文件或输入 *URL* 以提交进行恶意软件分析。
5. 点击**上传样本**。Threat Grid 样本分析流程即启动。

   您会看到样本将经历分析的几个阶段。在分析期间，样本将在*提交*部分列出。分析完成后，分析结果应显示在*样本*部分中，详细信息显示在分析报告中。

设备管理

Threat Grid 设备完成设置和初始配置后，即可由设备管理员进行操作。

版本说明、更新、SSL 证书、添加用户和其他管理员任务及主题都记录在《*Threat Grid 设备管理员指南*》中。

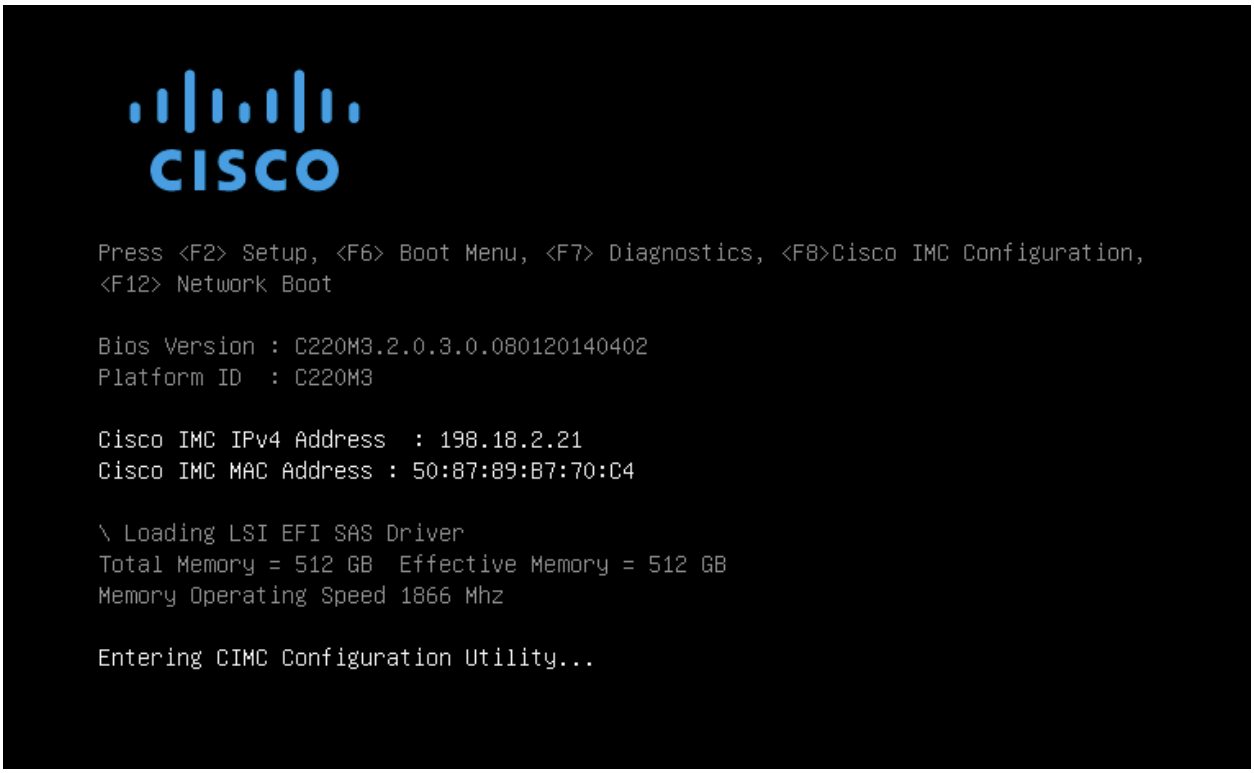
附录 A - CIMC 配置（推荐）

服务器启动时显示的第一个窗口是思科窗口，您可以通过此窗口进入思科集成管理控制器（“CIMC”）配置实用程序。CIMC 界面可用于远程服务器管理。

您需要在设备上直接连接一个显示器和键盘。

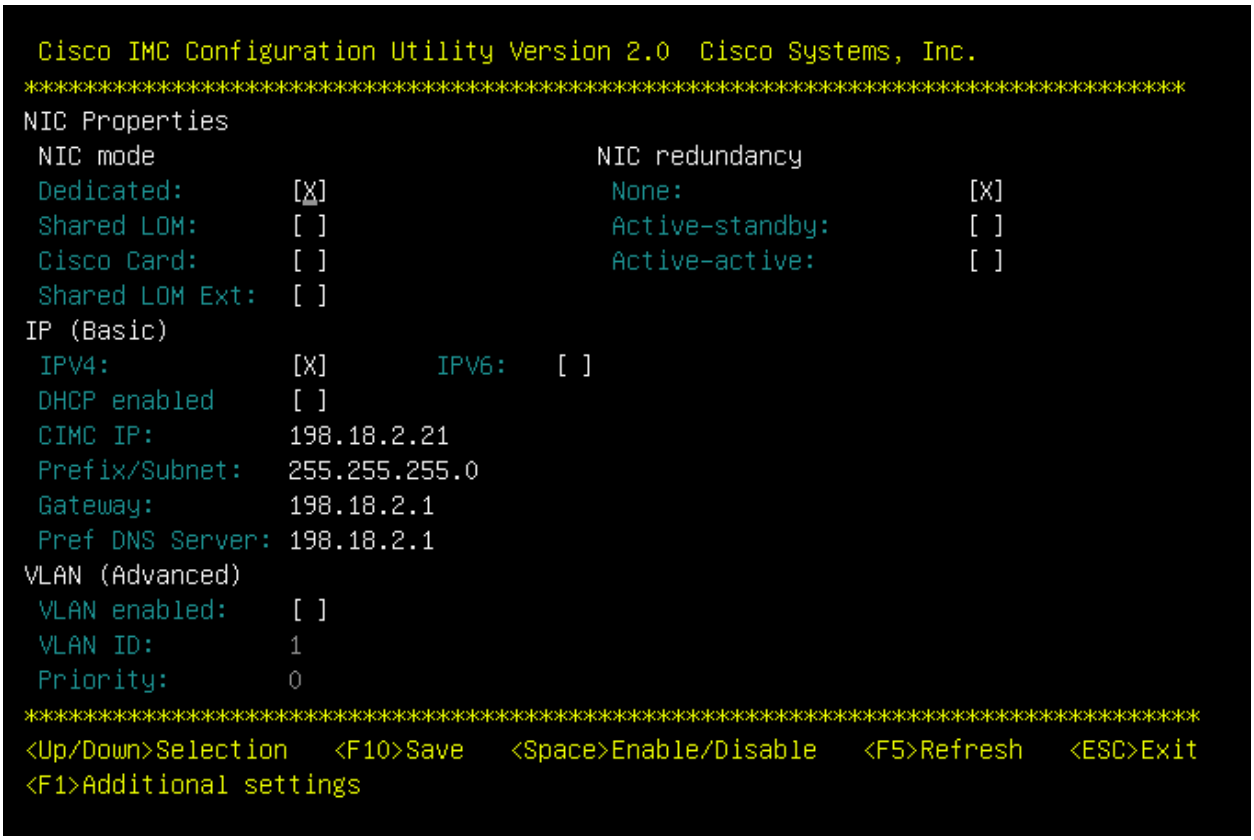
1. 接通服务器电源。思科屏幕随即打开：

图 30 - 思科屏幕 - 按 F8 进入 CIMC 配置实用程序



2. 内存检查完成后，按 **F8** 进入 CIMC 配置实用程序：

图 31 - CIMC 配置实用程序



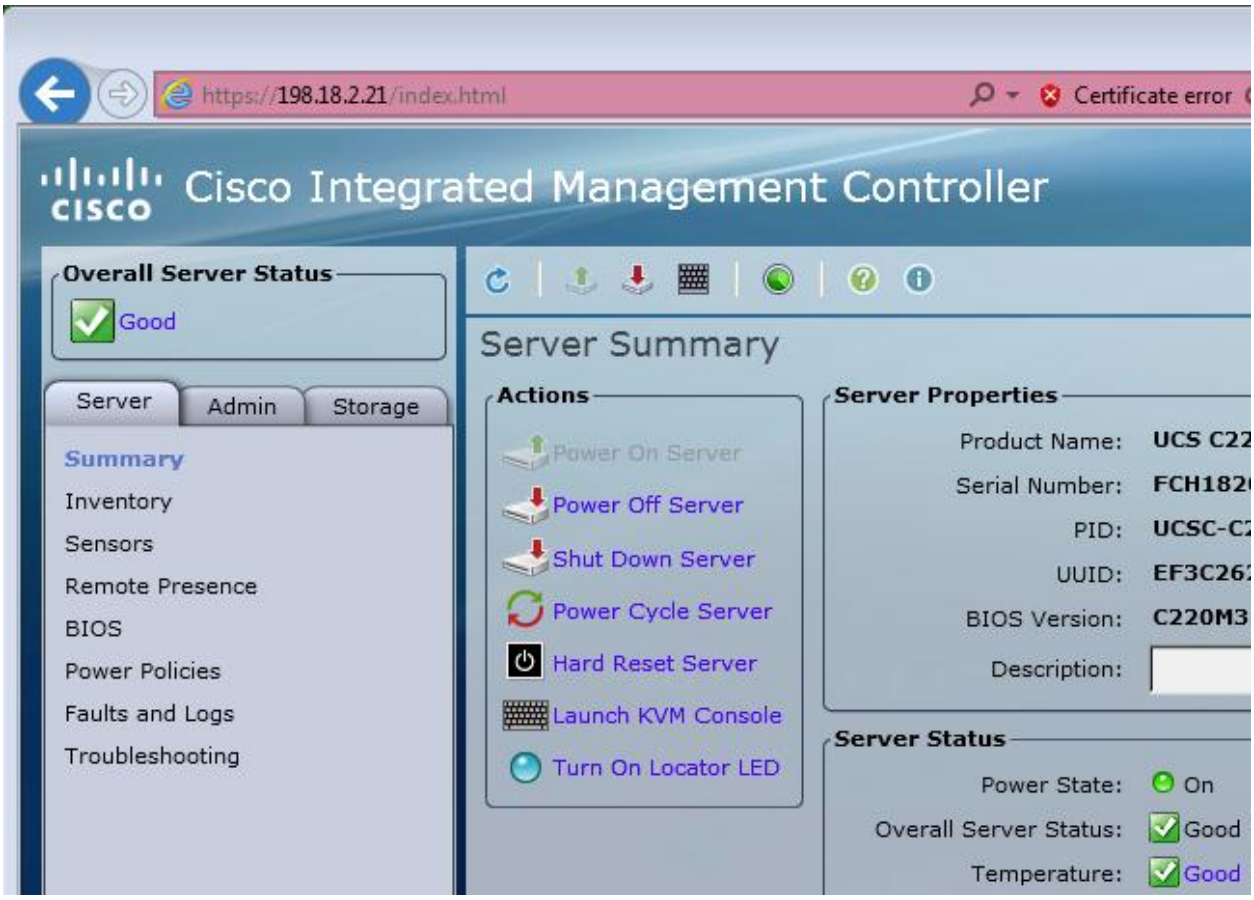
3. 在 CIMC 配置实用程序中，设置将用于远程服务器管理的 IP 地址。

完成后，保存并退出。

此时，您可在 Web 浏览器中输入 https://*<CIMC-IP address>*/ 来对服务器进行远程管理

初始用户名是“**admin**”，密码是“**password**”。

图 32 – 思科集成管理控制器 (CIMC) 界面



现在，您可以使用 CIMC 界面查看服务器运行状况，以及远程打开 KVM 以完成剩余的设置步骤。

索引