思科 AMP Threat Grid 设备设置和配置指南

2.0.3 版

最后更新时间： 2016 年 5 月 19 日

思科系统公司 www.cisco.com

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址、电话和传真。

封面照片：版权所有 © 2015 年 Mary C. Ecsedy。版权所有。已获得使用许可。美国拱门国家公园含苞待放的仙人掌花。这种植物能够在恶劣而艰苦的环境中有效地保护自己并最大程度地利用资源茁壮成长。

思科 AMP Threat Grid 设备设置和配置指南

目录

图片清单

引言

思科 AMP Threat Grid 设备可提供安全且高度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 (UCS C220-M3) 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 AMP Threat Grid 设备，组织便可向该设备发送可疑文档和文件进行分析，防止这些数据流出网络。

借助 AMP 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来分析所有样本。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 AMP《*Threat Grid 设备管理员指南*》，可在 Cisco.com 上的**安装和升级页面**中查看。

新增内容

2.0.3 版

FireAMP 私有云集成：2.0.3 版包括促进 Threat Grid 设备与 Fire AMP 私有云集成的功能，包括在 CLEAN 和 DIRTY 网络接口之间拆分 DNS 的功能，CA 管理和 FireAMP 私有云集成配置。

2.0 版

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 3.3.45 版开始的《*Threat Grid 门户版本说明*》。（从门户 UI 导航栏选择**帮助 [Help]**，然后点击版本说明的链接。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。）

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。

创建支持请求。您需要具有 Cisco.com ID（或生成一个 ID）才能创建支持请求。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。请通过以下链接输入您的支持请求：
https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case

电话。有关思科的电话号码，请参阅：http://www.cisco.com/c/en/us/support/index.html

如需请求 Threat Grid 团队的支持，请在发送您的请求时包含以下信息：

- 设备版本：**OpAdmin > 操作(Operations) > 更新设备 (Update Appliance)**
- 完整的服务状态（来自外壳的服务状态）
- 网络图或说明（如果适用）
- 支持模式（外壳或 Web 接口）
- 支持请求详细信息

支持模式

如果您向 Threat Grid 工程师请求支持，他们可能要求您启动“支持模式”，这是一种实时支持会话，允许 Threat Grid 支持工程师远程访问您的设备。这不会影响设备的正常运行。此操作可通过 **OpAdmin 门户支持 (Support)** 菜单完成。（您也可以从 TGSH 对话中启用**支持模式 (SUPPORT MODE)**。）

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 (Support) > 实时支持会话 (Live Support Session)**，然后点击**启动支持会话 (Start Support Session)**。

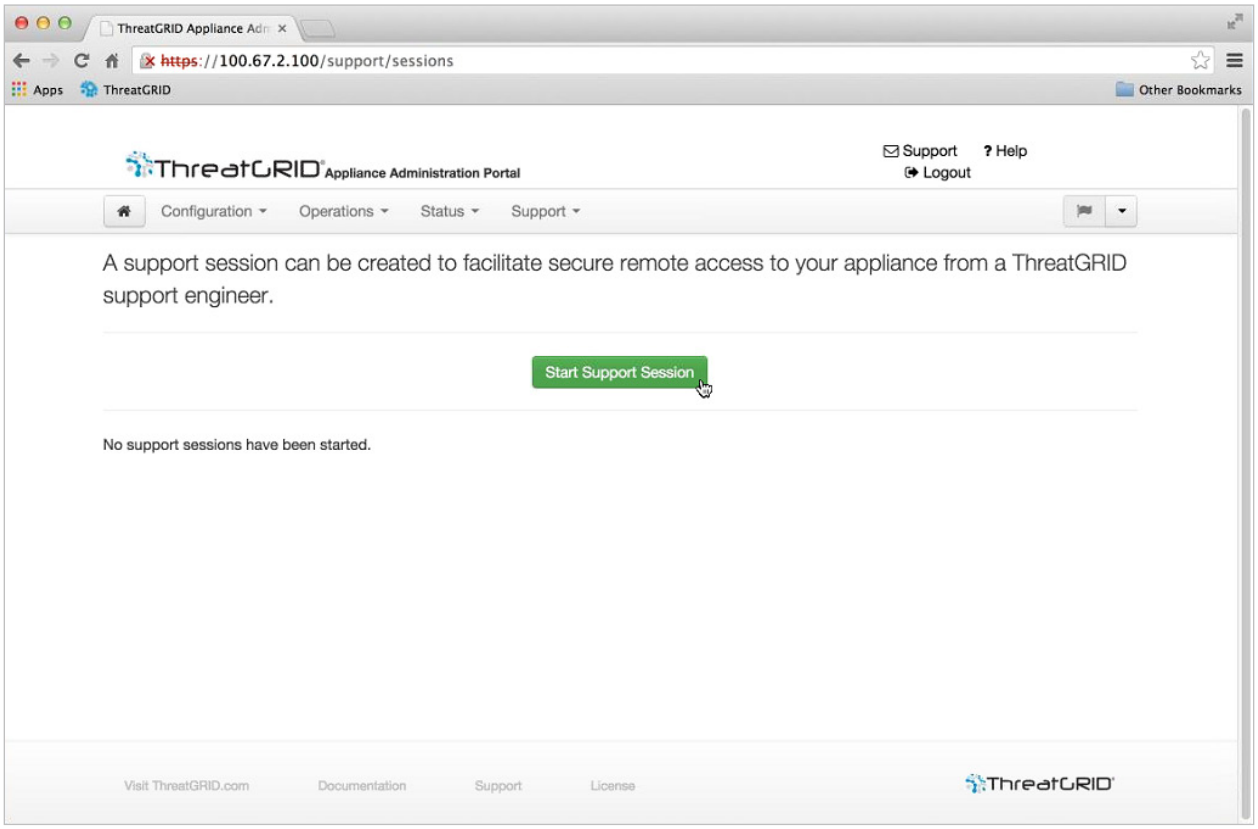
注意：在获得许可之前，您可以跳过 OpAdmin 向导任务流来启用支持模式。

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 启动一个实时支持会话



支持服务器

建立支持会话需要 TG 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系统的快照，包含日志、ps 输出等，帮助支持人员排除任何问题。

1. 验证是否为支持快照服务指定了 SSH。
2. 从**支持 (Support)** 菜单中，选择**支持快照 (Support Snapshots)**。
3. 拍摄快照。
4. 拍摄快照之后，您可以自行下载 .tar.gz 格式的快照，或者可以按**提交 (Submit)**，这样会将快照自动上传到 Threat Grid 快照服务器。

计划

思科 AMP Threat Grid 设备是一个 Linux 服务器，在出厂之前已由思科制造团队安装了 Threat Grid 软件。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 (Help)** 菜单查看。

环境要求

Threat Grid 设备应部署在 UCS C220-M3 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+。如果交换机上没有可用的 SFP+ 端口，或您不需要 SFP+，则可以使用 1000Base-T 收发器（例如思科兼容的千兆 RJ45 铜缆 SFP 收发器模块 Mini-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 M3 服务器安装和服务指南：

http://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：

http://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。

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：以下特定的受限网络流量类型可由 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
- 到 FireAMP 私有云设备的安全状态更新服务连接
- 与以上任意项目相关的 DNS 请求

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，请参阅网络接口和网络接口连接设置。

DNS 服务器访问

用于安全状态更新服务查询、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用途以外的 DNS 服务器需可通过 DIRTY 网络进行访问。

默认情况下，DNS 使用 DIRTY 接口。而 CLEAN 接口则用于 FireAMP 私有云集成。如果在 DIRTY 接口上无法解析 FireAMP 私有云主机名，则可以在 OpAdmin 界面中配置使用 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/FireAMP 等

如果 Threat Grid 设备将与其他思科产品（例如 ESA/WSA 设备、FireAMP 私有云等）一起使用，则可能需要另外进行规划。

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

您会收到来自 Cisco AMP Threat Grid 的许可证和密码。

有关许可证的问题，请通过 dedebeer@cisco.com 联系 Dean De Beer。

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 组织和用户帐户，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 组织和用户的信息在《*Threat Grid 设备管理员指南*》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。更新设备的相关说明位于《*Threat Grid 设备管理员指南*》中。

注意：请验证是否为更新指定了 SSH。

版本说明

有关详细的更新信息，请参阅版本说明，该说明可从 OpAdmin 门户的以下位置获取：

操作 (Operations) 菜单 > **更新设备 (Update Appliance)**

也可**在线查看** PDF 格式的 Threat Grid 设备版本说明。

注意：要查看设备上安装的 Threat Grid Portal 的版本说明，请在其导航栏中点击**帮助 (Help)**。UI 的**帮助 (Help)** 页面（**导航栏 > 帮助 (Help)**）上提供了访问当前 *Threat Grid 门户版本说明*的链接。

Threat Grid 设备用户界面

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：

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）。

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。

AMP 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）

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)。

CLEAN 接口

- 连接到 CLEAN 网络。CLEAN 网络必须可从公司网络进行访问，但不需要出站访问互联网，除非是在恢复模式下。
- UI 和 API 流量（入站）
- 样本提交
- SMTP（出站连接到配置的邮件服务器）
- 恢复模式支持会话（出站）
- SSH（TGSH 对话的入站访问）
- 系统日志（出站连接到配置的系统日志服务器）
- ESA/WSA - CSA 集成
- FireAMP 私有云集成
- DNS - 可选。

DIRTY 接口

- 连接到 DIRTY 网络。需要访问互联网。**仅出站！**
- DNS。
  注意：如果您要设置与 FireAMP 私有云的集成，并且在 DIRTY 接口上无法解析 FireAMP 设备主机名，则可以在 OpAdmin 中配置使用 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

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）。

保留的接口

非管理 SFP+ 端口将保留以供将来使用。

登录名和密码 - 默认

网络 UI 管理员

登录名称： 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。

CIMC（思科集成管理控制器）

登录名称： 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
- 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）。

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。

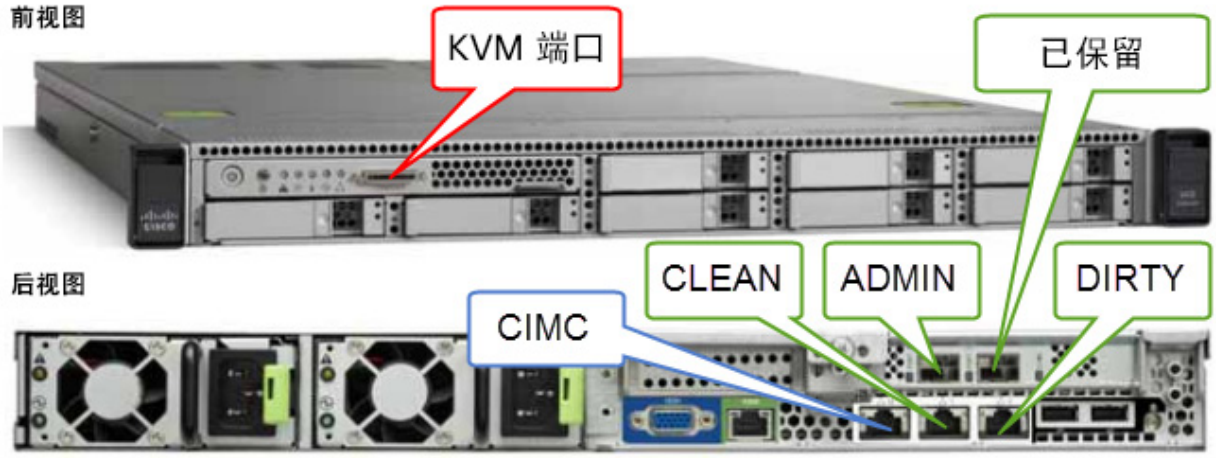
如果配置了 CIMC，则可以使用远程 KVM。有关 CIMC 配置的信息，请参阅*附录*中的**配置 CIMC（可选）**。

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

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：

图 3 - 思科 UCS C220 M3 SFF 机架式服务器



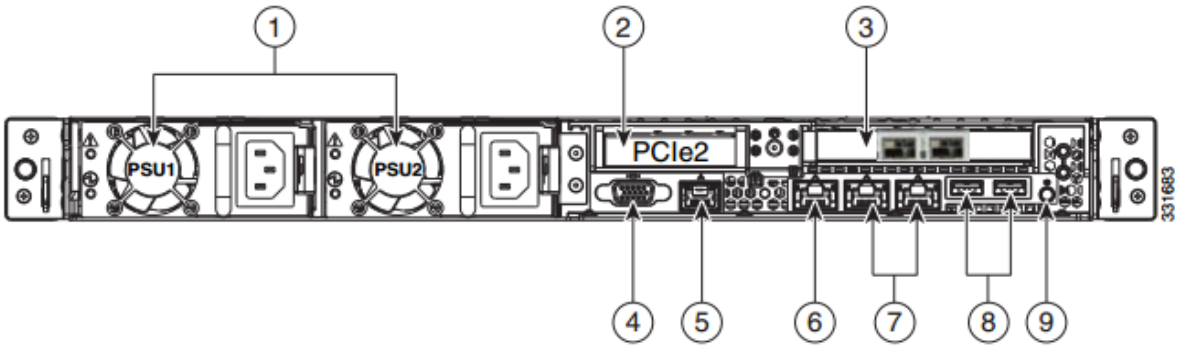
必须正确连接和配置接口，设备才能运行。

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：“已保留”(Reserved) 为非管理 SFP+ 端口，将被保留以供日后使用。

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



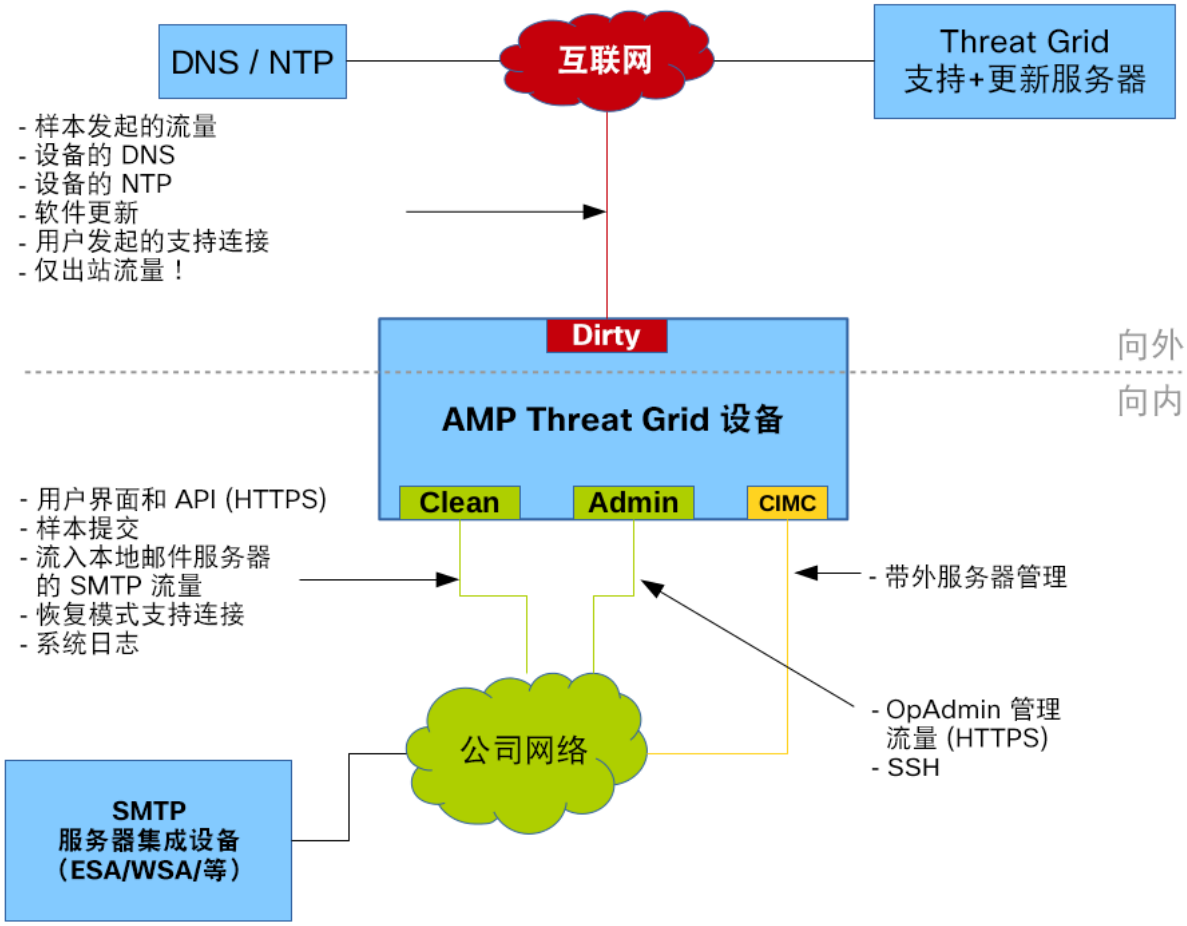
1	电源（最多两个）	6	一个 10/100/1000 以太网专用管理端口
2	插槽 2：提升板上的薄型 PCIe 插槽： （半高，半长，x16 连接，x8 信道宽度）	7	双 1-GbE 端口 (LAN1 和 LAN2)
3	两个 SFP+ 端口。 插槽 1：ADMIN 插槽 2：已保留以备支持备份和存储之用。	8	USB 端口
4	VGA 视频连接器	9	背部识别按钮/LED
5	串行端口（RJ-45 连接器）[1]	–	–

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）。插入 SFP 的网线可以安全地热插拔。

网络接口设置图

本部分介绍 AMP Threat Grid 设备的最合理/建议的设置。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 5 - 网络接口设置图


DNS / NTP
互联网
Threat Grid
支持+更新服务器
- 样本发起的流量
- 设备的 DNS
- 设备的 NTP
- 软件更新
- 用户发起的支持连接
- 仅出站流量！
Dirty
AMP Threat Grid 设备
Clean
Admin
CIMC
向外
向内
- 用户界面和 API (HTTPS)
- 样本提交
- 流入本地邮件服务器
的 SMTP 流量
- 恢复模式支持连接
- 系统日志
- 带外服务器管理
- OpAdmin 管理
流量 (HTTPS)
- SSH
公司网络
SMTP
服务器集成设备
（ESA/WSA/等）

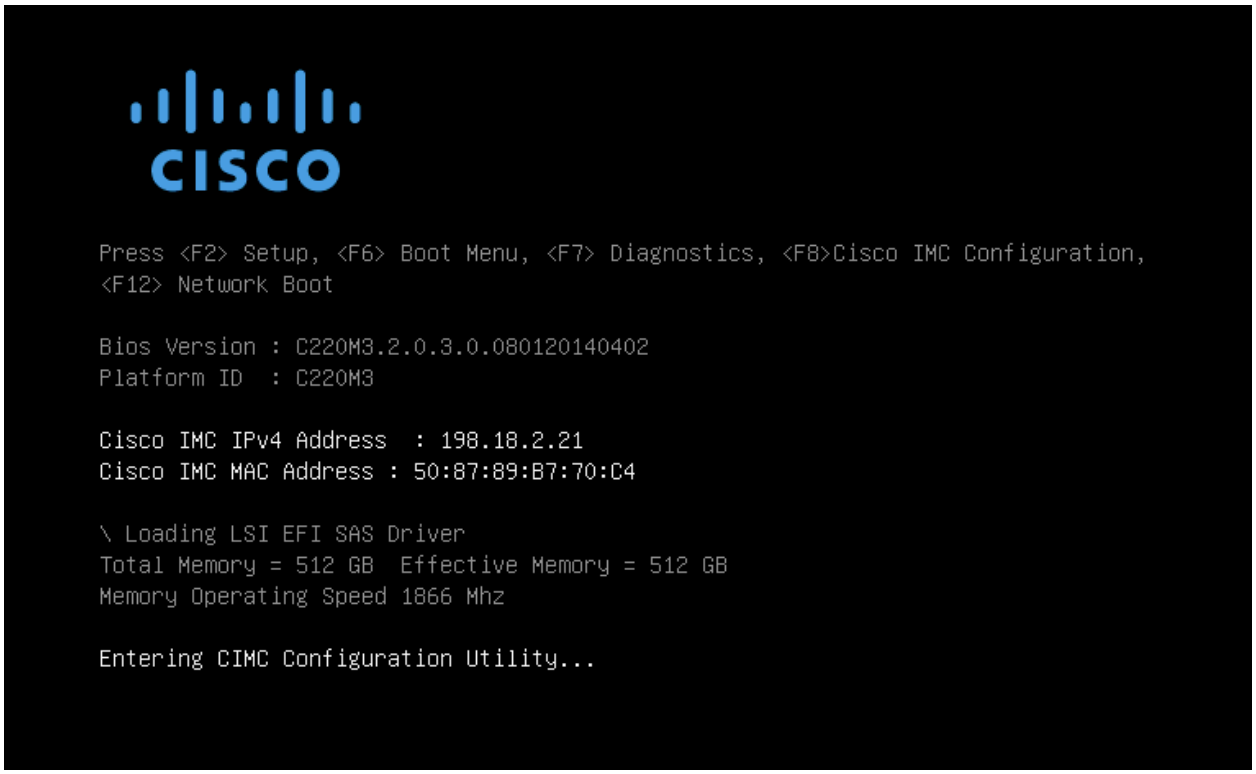
防火墙规则建议

来源	目标	协议/端口	操作	原因
DIRTY 接口	互联网	SMTP	拒绝	防止恶意软件发送垃圾邮件
DIRTY 接口	互联网	TCP/19791	允许	允许连接到 Threat Grid 支持
DIRTY 接口	互联网	TCP/22	允许	更新和支持快照服务
DIRTY 接口	互联网	IP/任何	允许	允许来自恶意软件样本的出站流量 （要获得准确结果，需要允许恶意软件联系其命令和控制服务器。）
DIRTY 接口	互联网	DNS	允许	允许出站 DNS。
DIRTY 接口	互联网	NTP (UDP/123)	允许	允许出站流量访问 NTP。
CLEAN 接口	SMTP 服务器	SMTP	允许	设备使用 CLEAN 接口启动与配置的邮件服务器的 SMTP 连接。（CLEAN 接口不需要出站连接“至互联网”。）
CLEAN 接口	互联网	TCP/19791	允许	允许建立 Thread Grid 恢复模式支持连接
用户网络	CLEAN 接口	TCP/80 TCP/443	允许	设备 API 和用户界面
CLEAN 接口	用户网络	系统日志/可配置	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。
管理网络	ADMIN 接口	TCP/22 TCP/80 TCP/443	允许	SSH OpAdmin 门户接口
用户网络	CLEAN 接口	TCP/9443	允许	允许连接到 Threat Grid UI Glovebox
CLEAN 接口	公司 DNS 服务器	UDP/53 和 TCP/53	允许	可选，仅当已配置 CLEAN DNS 时需要
CLEAN 接口	FireAMP 私有云	TCP/443	允许	可选，仅当已使用 FireAMP 私有云集成时需要

接通电源和启动

连接了服务器外围设备和网络接口之后，请接通设备电源并等待它启动。思科屏幕会短暂显示：

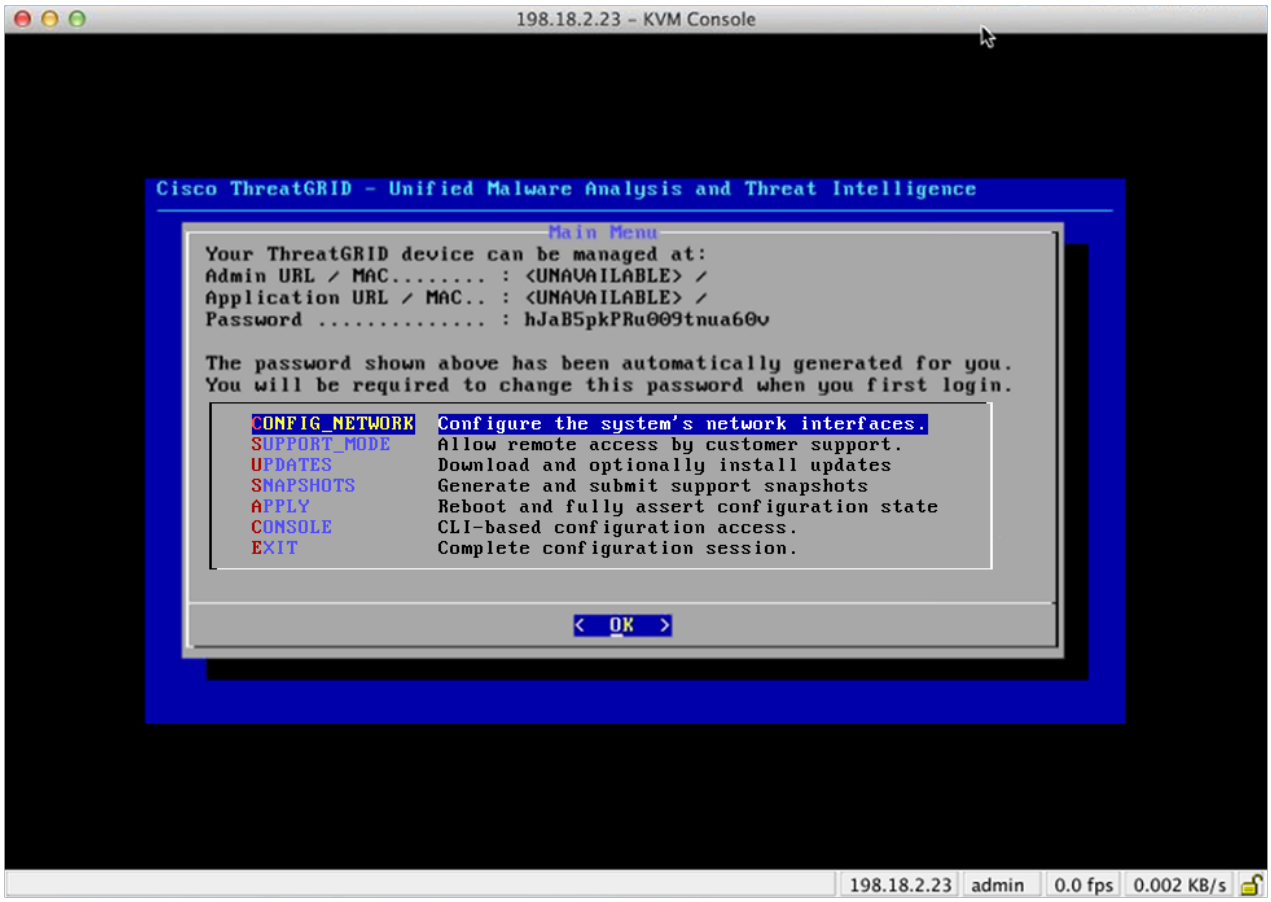
图 6 - 启动期间的思科屏幕



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“*配置 CIMC（可选）*”部分中的说明操作。

成功启动并连接服务器后，控制台上将显示 **TGSH 对话**：

图 7 - 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。

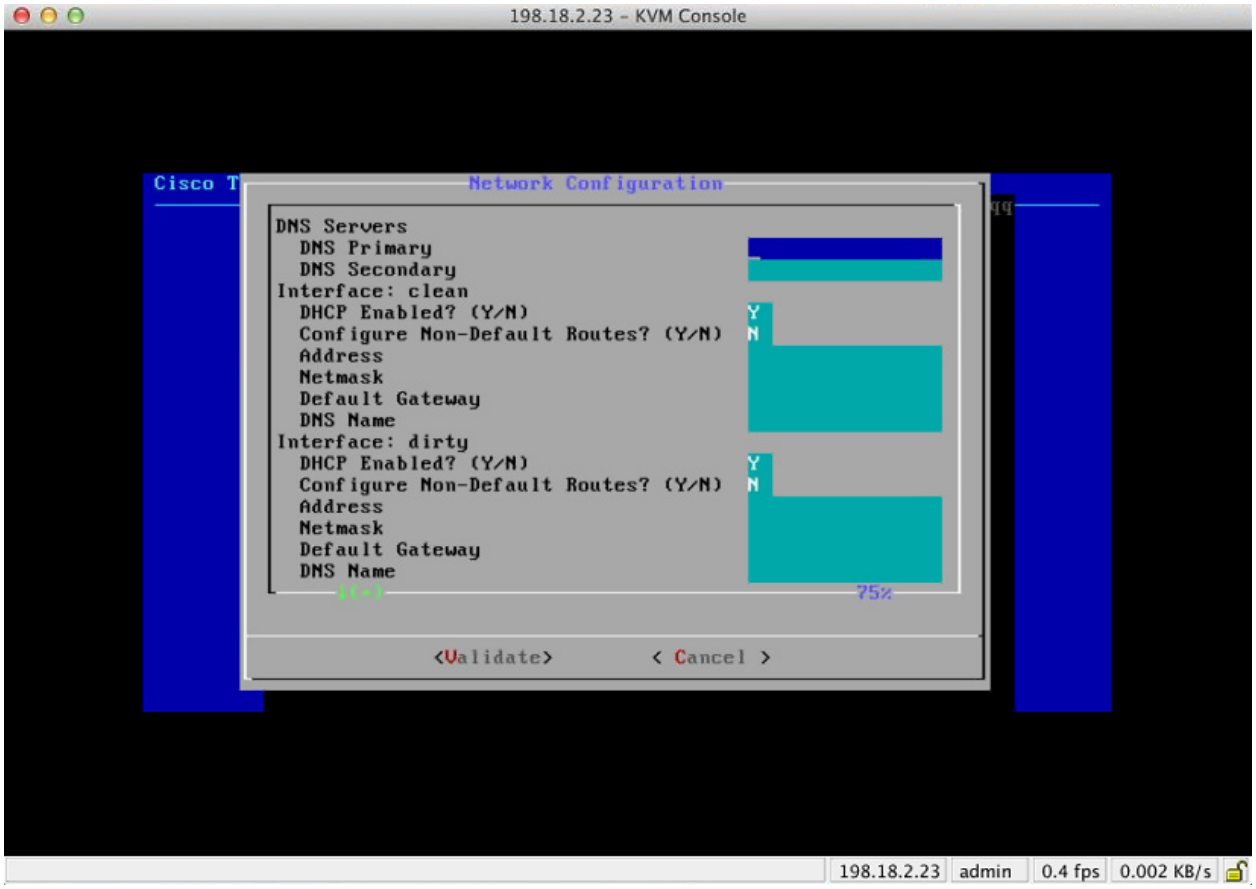
初始网络配置 - TGSH 对话

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”(TGSH Dialog) 界面中，选择 **CONFIG_NETWORK**。网络配置控制台将会打开：

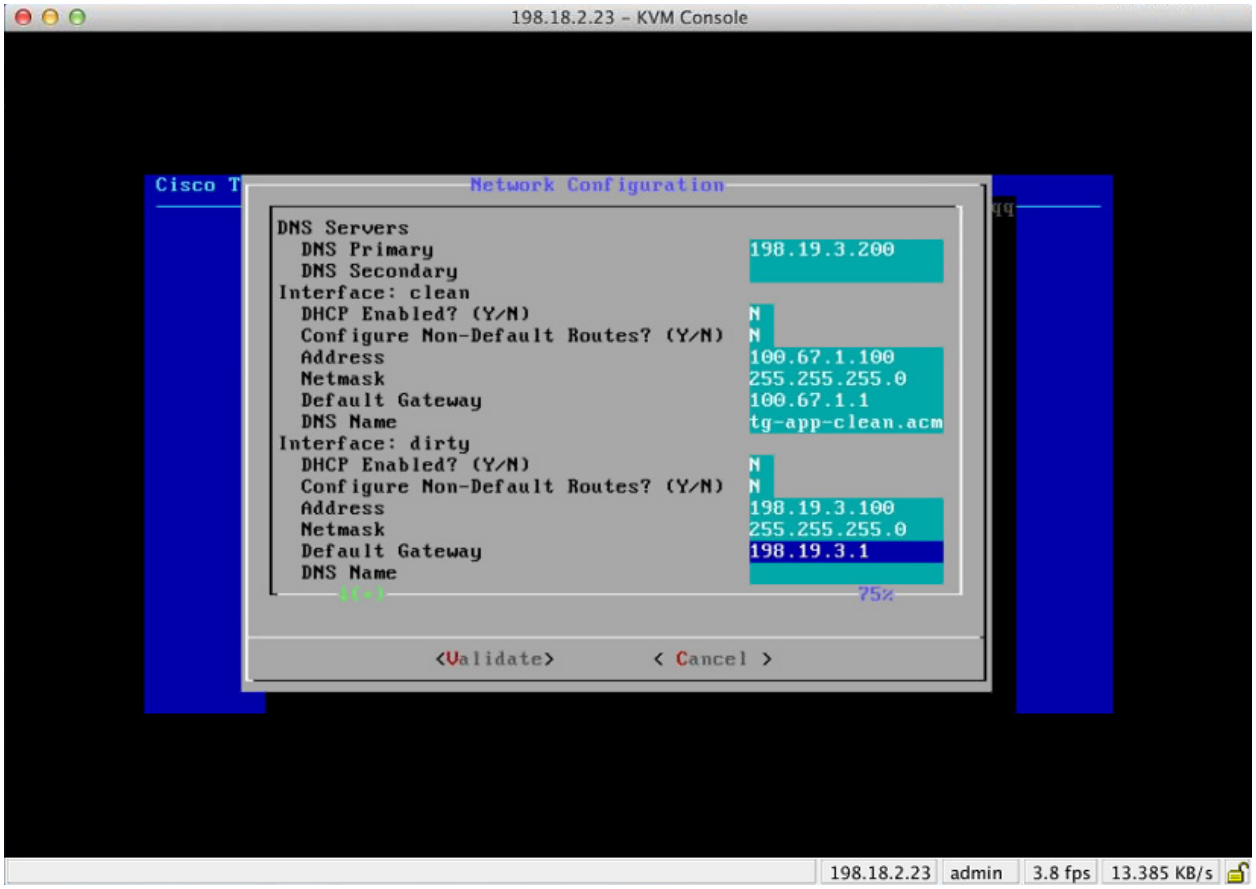
图 8 - TGSH 对话 - 网络配置控制台



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 (DHCP Enabled)** 从 **Y** 更改为 **N**。

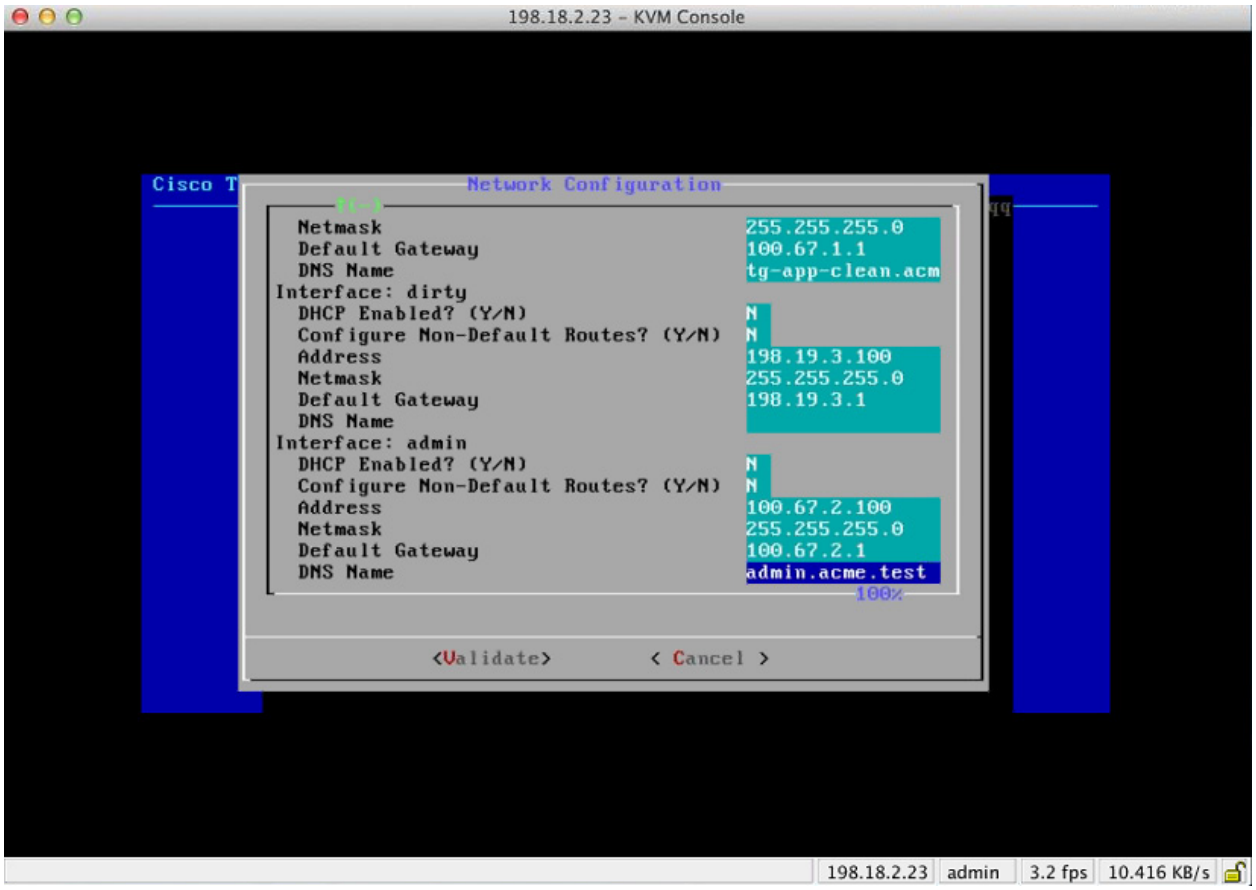
   注意：您需要使用 **BACKSPACE** 删除原字符，才能再输入新的字符。
4. **DNS 名称。**如果您的网络为 CLEAN 网络使用了 DNS 名称，则在此处输入该名称。
5. 将**配置非默认路由？(Configure Non-Default Routes?)** 保留为默认的 **N**（除非需要其他路由）。

图 9 – 正在进行网络配置（CLEAN 和 DIRTY）



6. 将 DIRTY 网络的 **DNS 名称 (DNS Name)** 留空。

图 10 – 正在进行网络配置 (ADMIN)

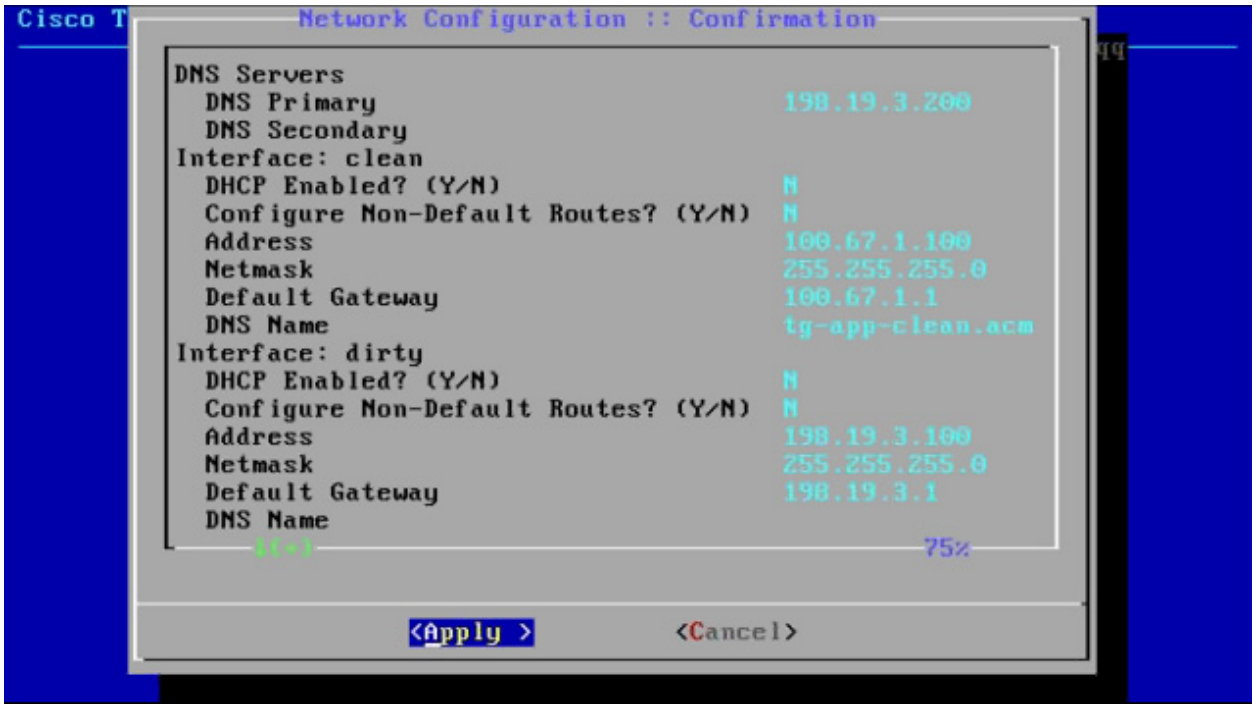


7. 输入了所有网络设置后，按 Tab 键向下移动，然后选择**验证 (Validate)** 来验证您输入的内容。

   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。

   验证后，网络配置确认将显示您输入的值：

图 11 – 网络配置确认

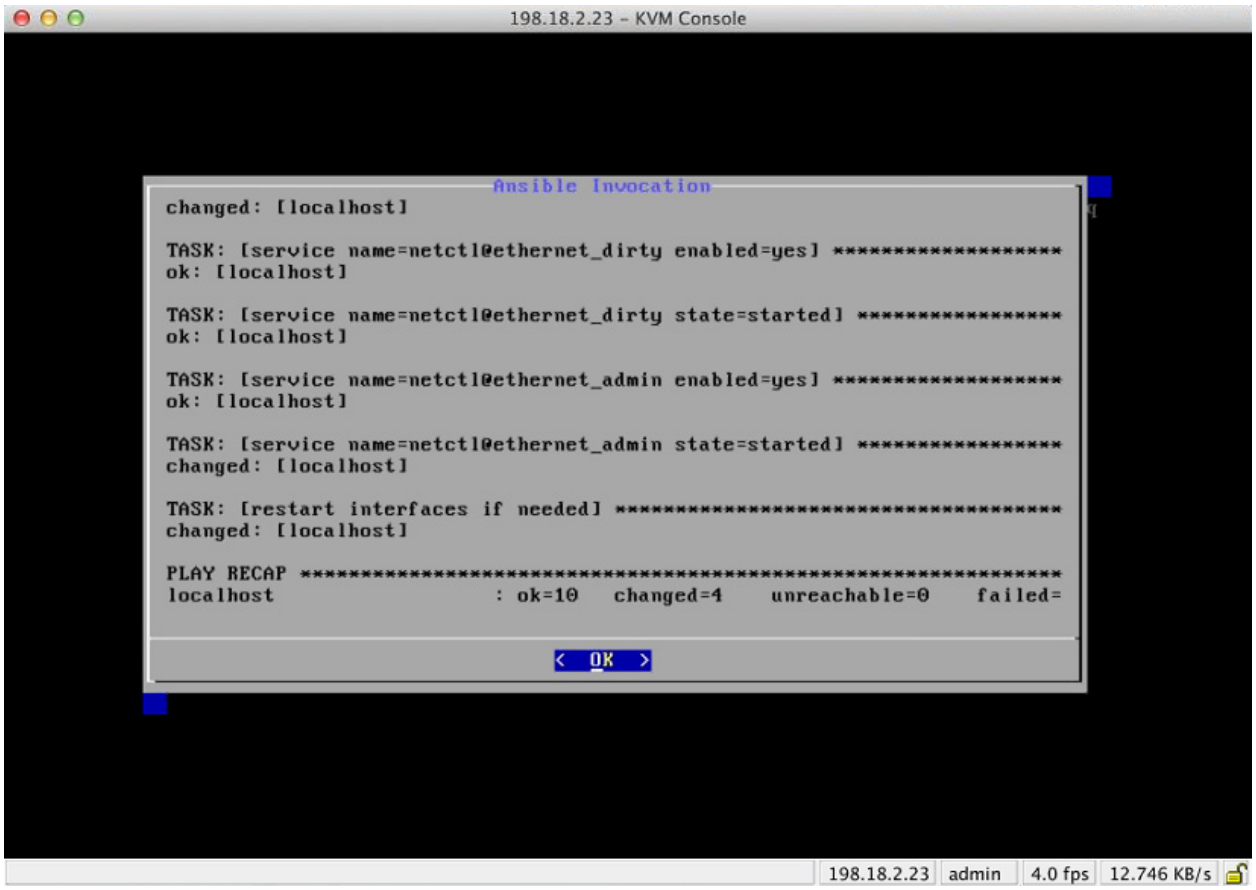


8. 选择**应用 (Apply)** 应用您的配置设置。

   请保持耐心。此步骤可能需要 10 分钟或更长时间才能完成。

   控制台将成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的配置更改的详细信息：

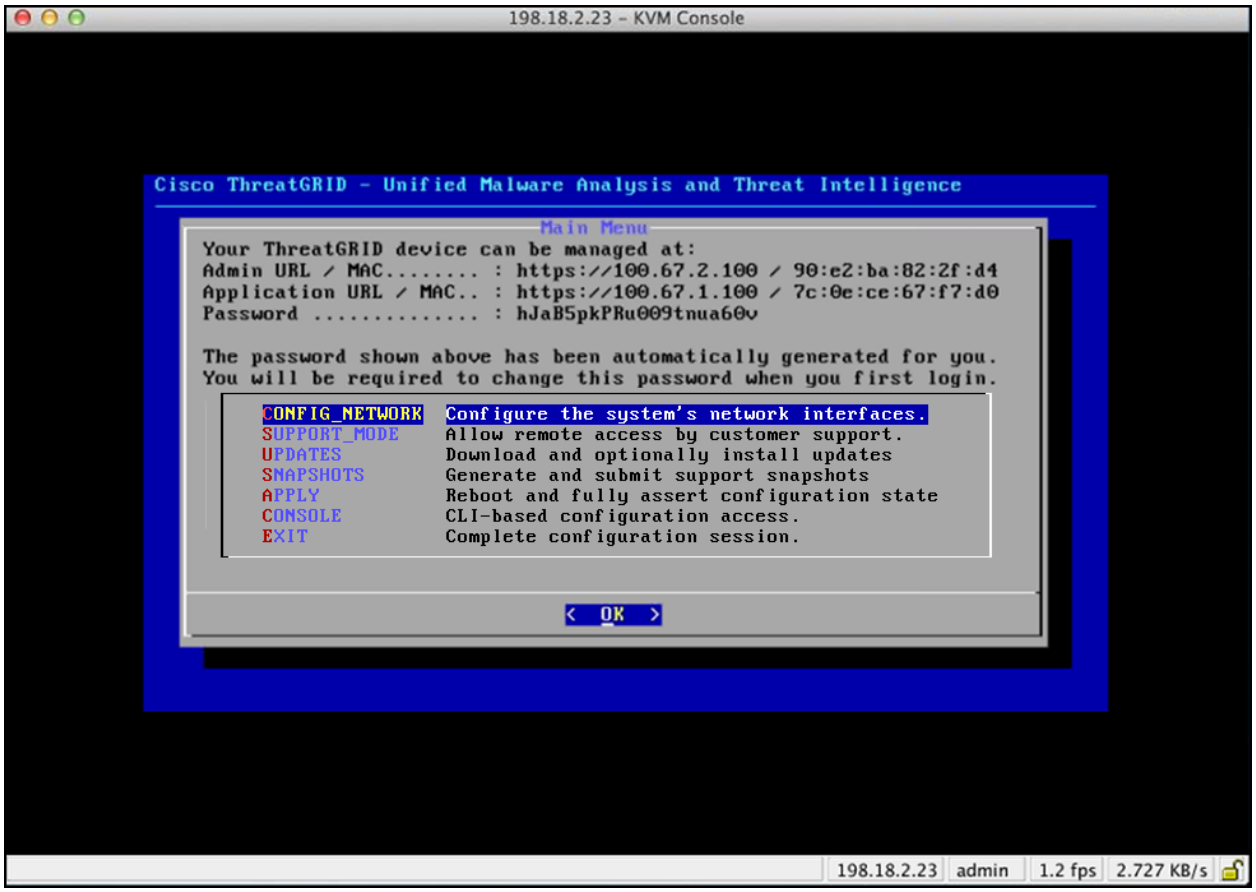
图 12 – 网络配置 – 所做更改的列表



9. 点击**确定 (OK)**。

   网络配置控制台将会再次刷新并显示您输入的 IP 地址：

图 13 – 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：

设备设置的下一个步骤是使用 OpAdmin 门户中的工作流按照下一部分“OPADMIN 门户配置向导”中的描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
- 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。有些设置（例如 SSL 证书）通过单独的步骤完成，如《*Threat Grid 设备管理员指南*》中所述。

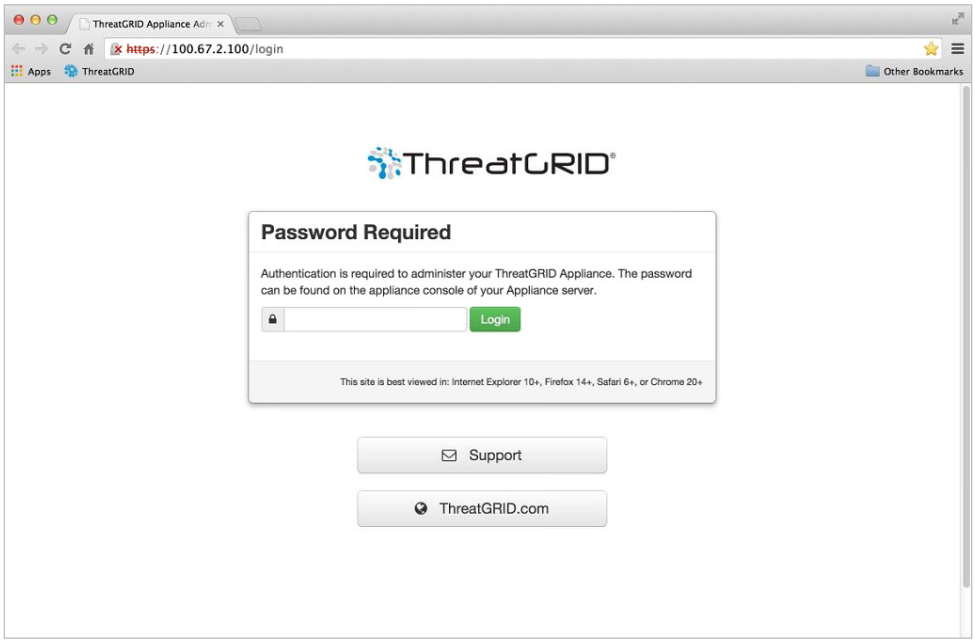
配置工作流

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 14 - OpAdmin 登录



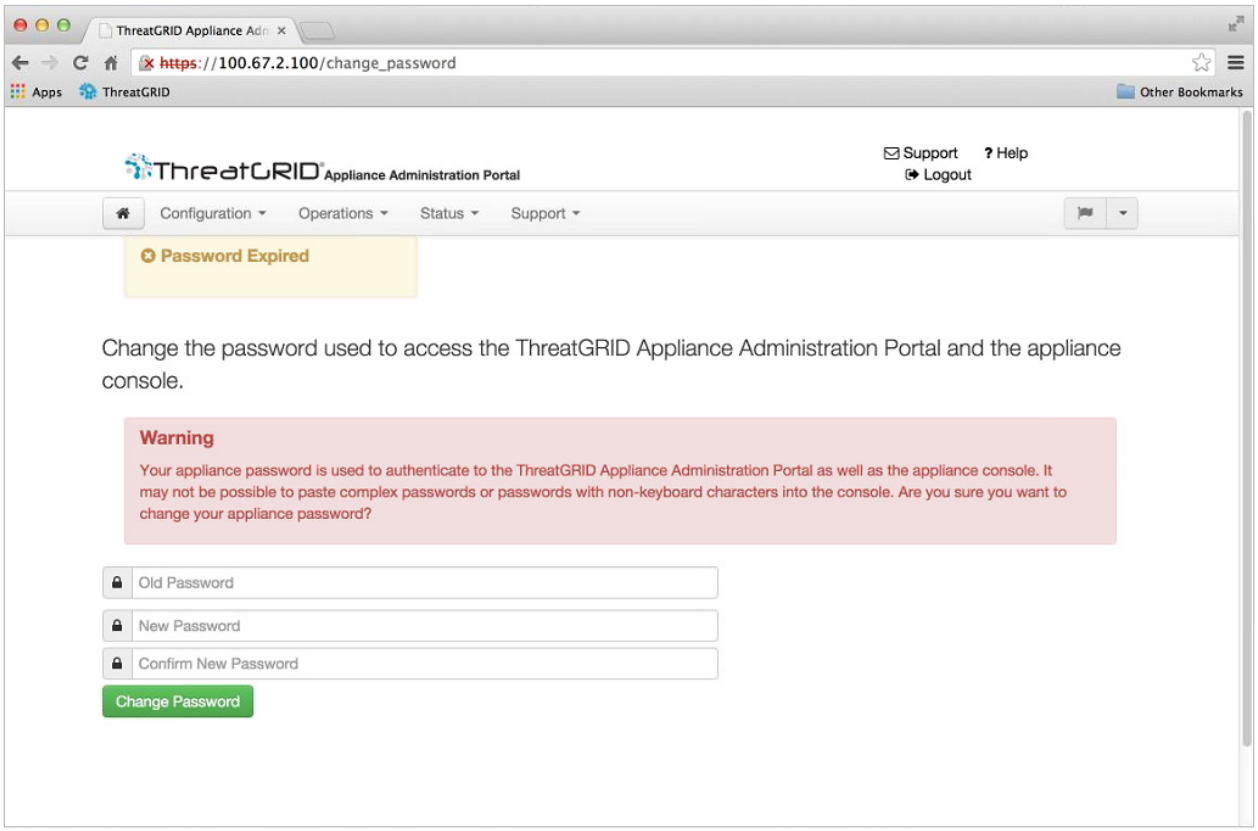
2. 输入您从 TGSH 对话复制的默认 Admin 密码并点击**登录 (Login)**。*更改密码 (Change Password)* 页面将会打开。

继续进行下一部分：

管理员密码修改

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 15 - OpAdmin 更改密码



1. 从 TGSH 对话的**旧密码 (Old Password)** 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 (End User License Agreement)* 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。

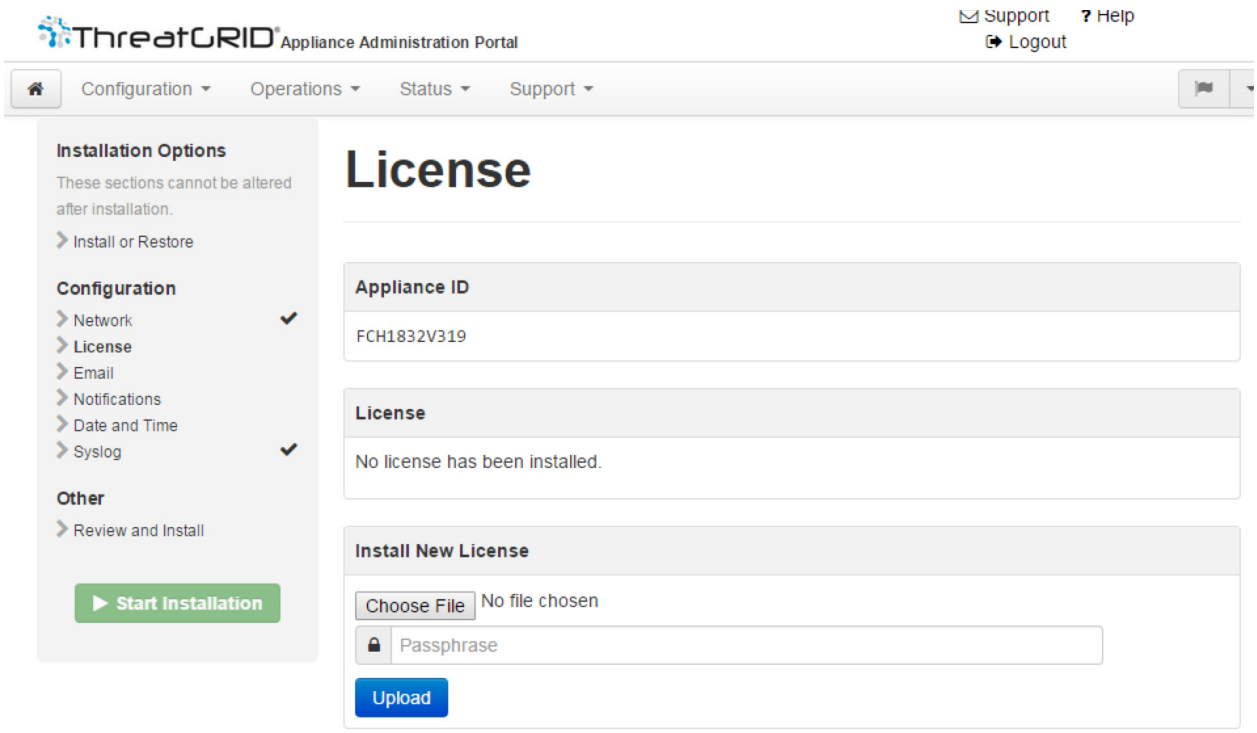
   如果密码丢失，请按照《*Threat Grid 设备管理员指南*》**支持**部分中的*丢失密码*相关说明操作。

继续进行下一部分：

最终用户许可协议

1. 审核最终用户许可协议。
2. 向下滚动到末尾，点击**我已阅读并同意 (I HAVE READ AND AGREE)**。*许可证 (License)* 页面将会打开：

图 16 - 许可证 (License) 页面



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

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”(Network Configuration) 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。

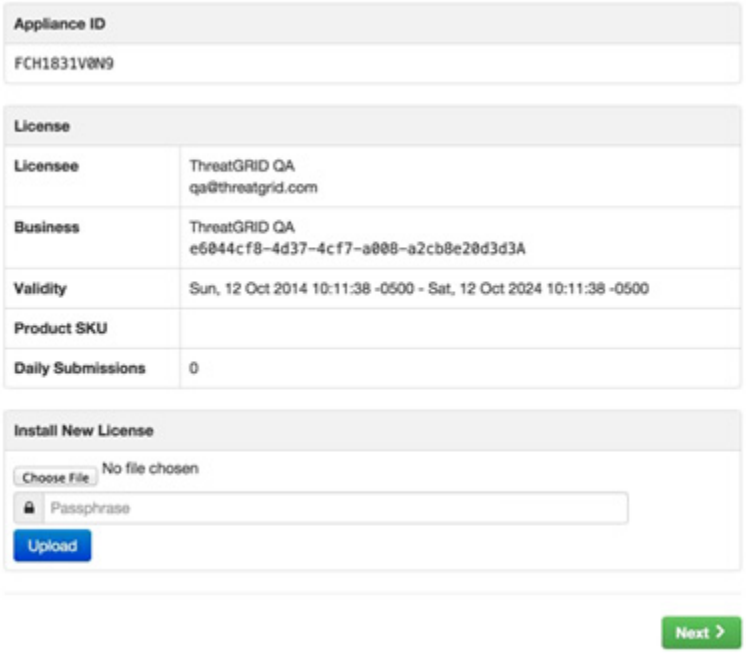
继续进行下一部分：

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。

1. 点击左侧列中的**许可证 (License)**。*许可证 (License)* 页面将会打开。尚未安装许可证。
2. 在**安装新许可证 (Install New License)** 下点击**浏览 (Browse)**，然后从您的文件管理器中选择许可证。
3. 将您收到的许可证密码输入“密码”(Passphrase) 字段中。
4. 点击**上传 (Upload)** 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 17 - 成功安装后的许可证信息



5. 点击**下一步 (Next)** 继续操作。*邮件 (Email)* 页面将会打开。

继续进行下一部分：

邮件主机配置

工作流的下一步是配置邮件主机。

1. 点击左侧列中的**邮件 (Email)**。*邮件 (Email)* 页面将会打开。
2. 输入**上游主机 (Upstream Host)**（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 (Next)**。*通知 (Notifications)* 页面将会打开。

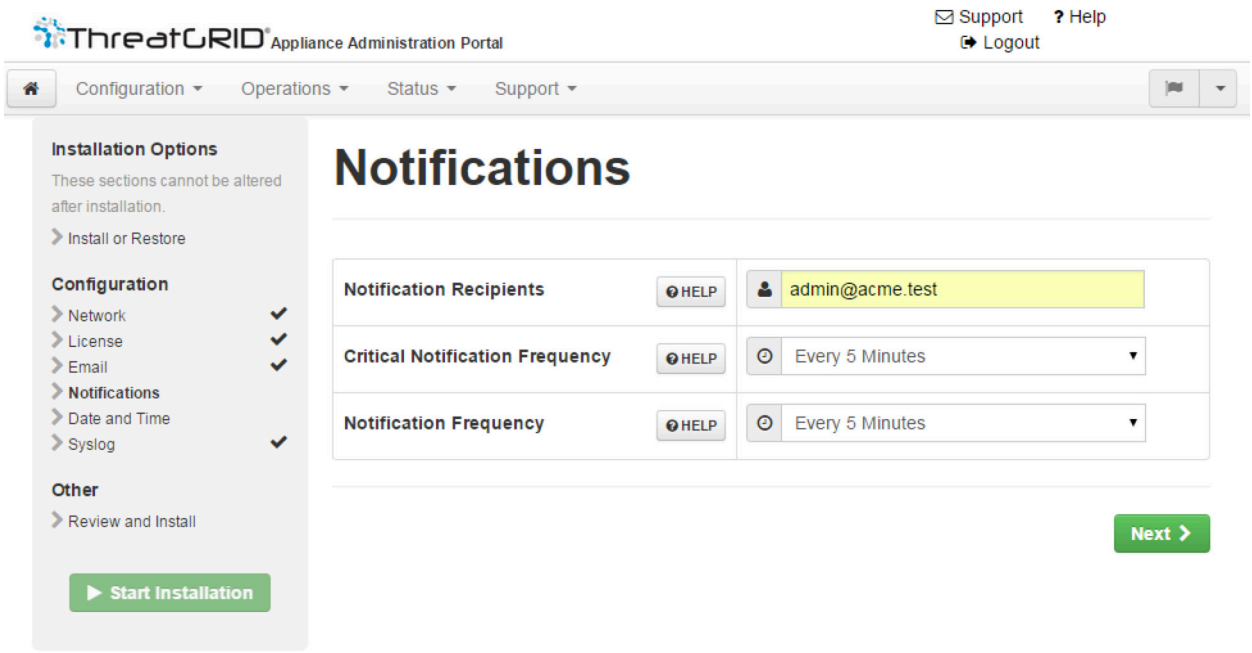
继续进行下一部分：

服务器通知配置

工作流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。

注意： 更新 v1.3 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 18 - 通知配置



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

继续进行下一部分：

NTP 服务器配置

此处可用来识别 NTP（“网络时间协议”）服务器。

1. 输入 **NTP 服务器 (NTP Server)** 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 (Next)**。

   查看和安装 (Review and Install) 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

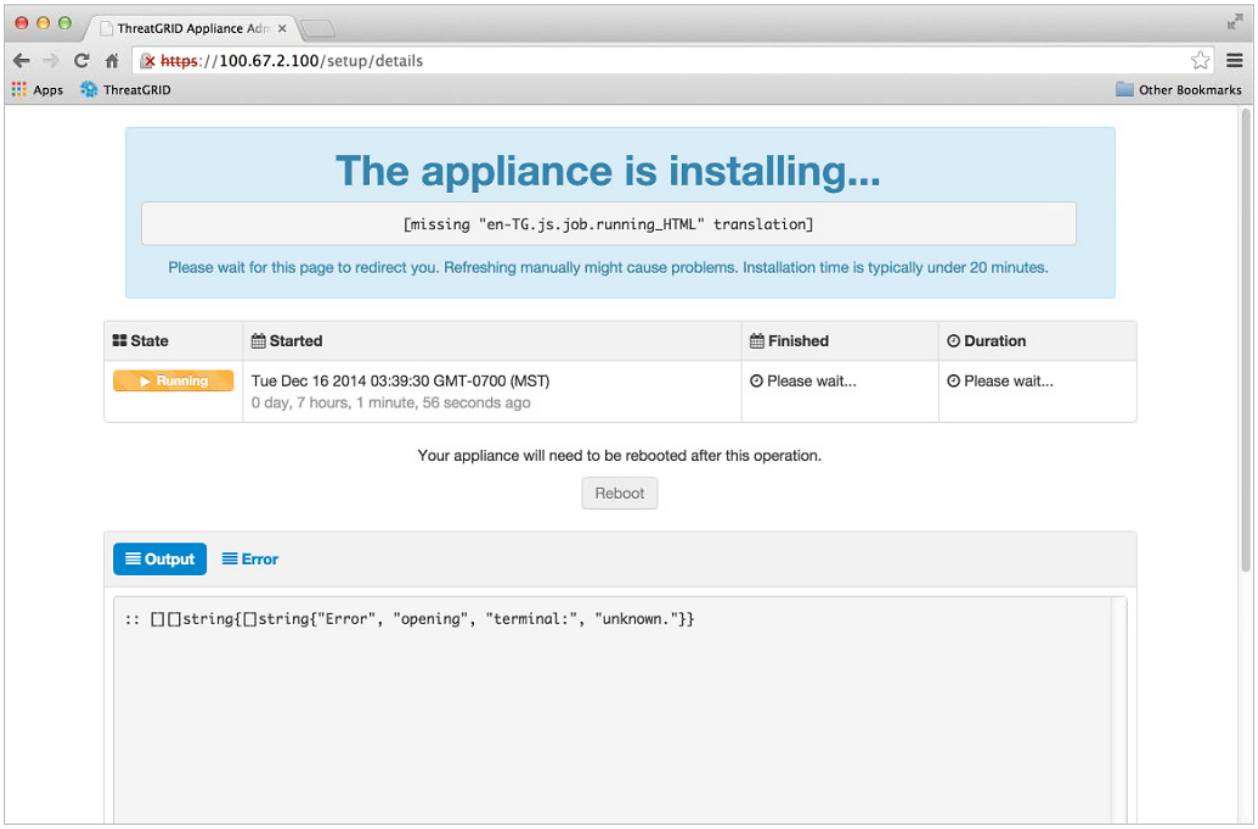
输入了网络配置设置后，必须按照如下所述安装这些设置。

1. 在*查看和安装 (Review and Install)* 页面中，点击**开始安装 (Start Installation)**。

   将会安装配置脚本，并且您会看到消息：*设备正在安装... (The appliance is installing...)*。

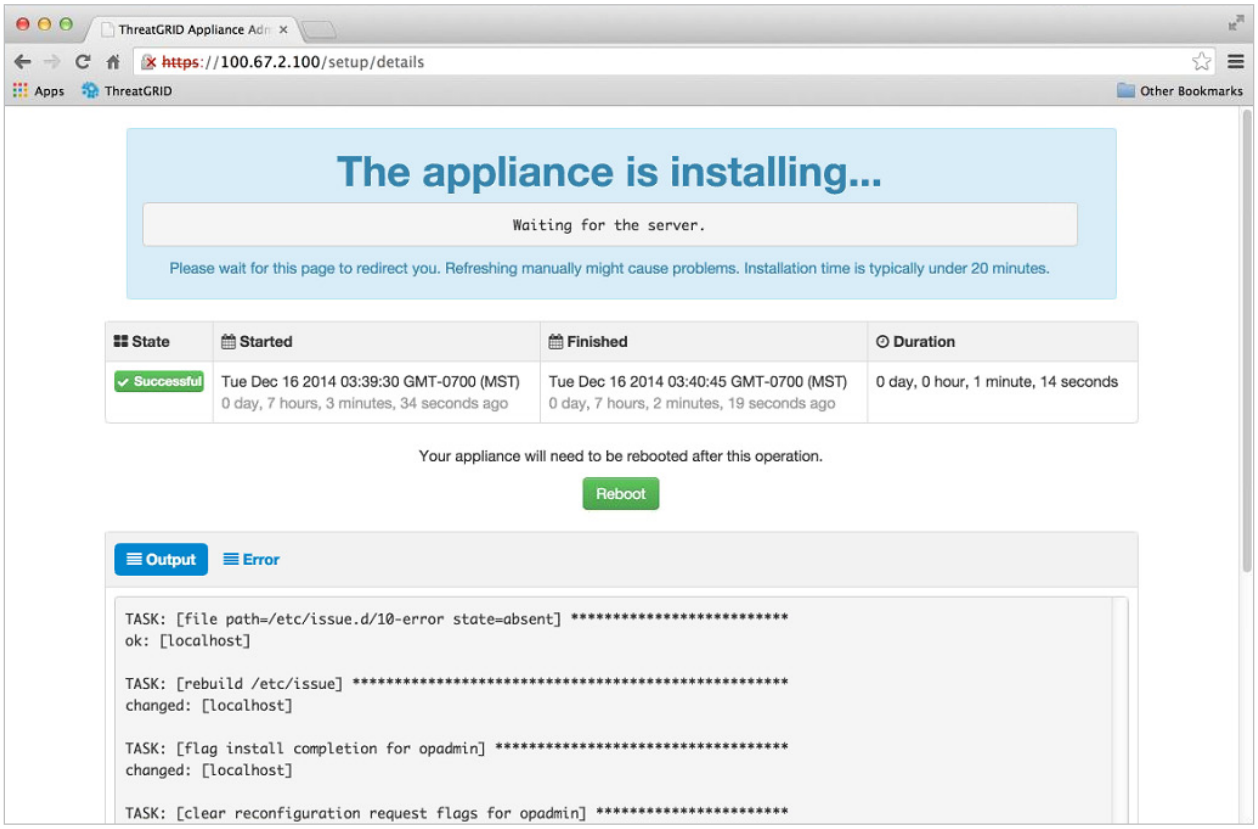
注意：请保持耐心。完成此步骤可能需要 10 多分钟的时间。应用配置之后，屏幕将会显示配置信息。

图 19 - 设备正在安装



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

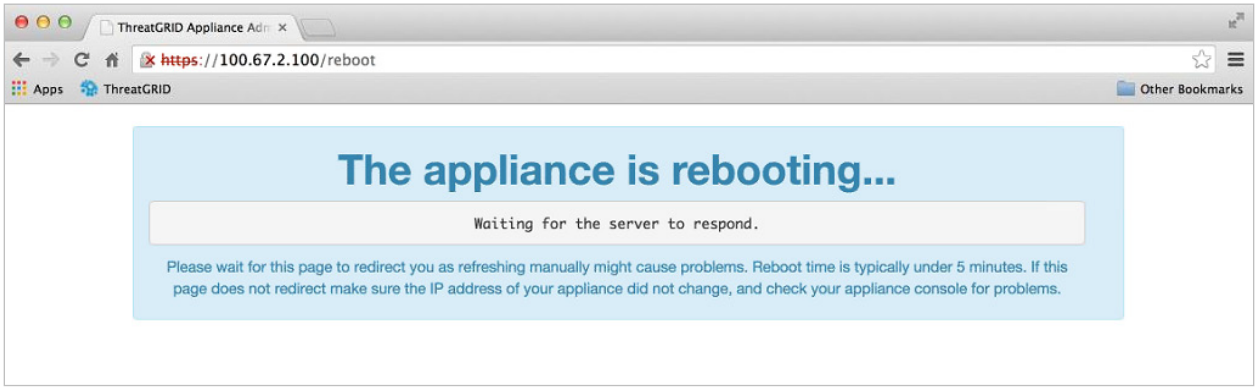
图 20 - 成功的设备安装



3. 成功安装之后，点击**重新启动 (Reboot)**。您会看到消息 *“设备正在重新启动”(The appliance is rebooting)*。重新启动过程可能需要长达 5 分钟时间。

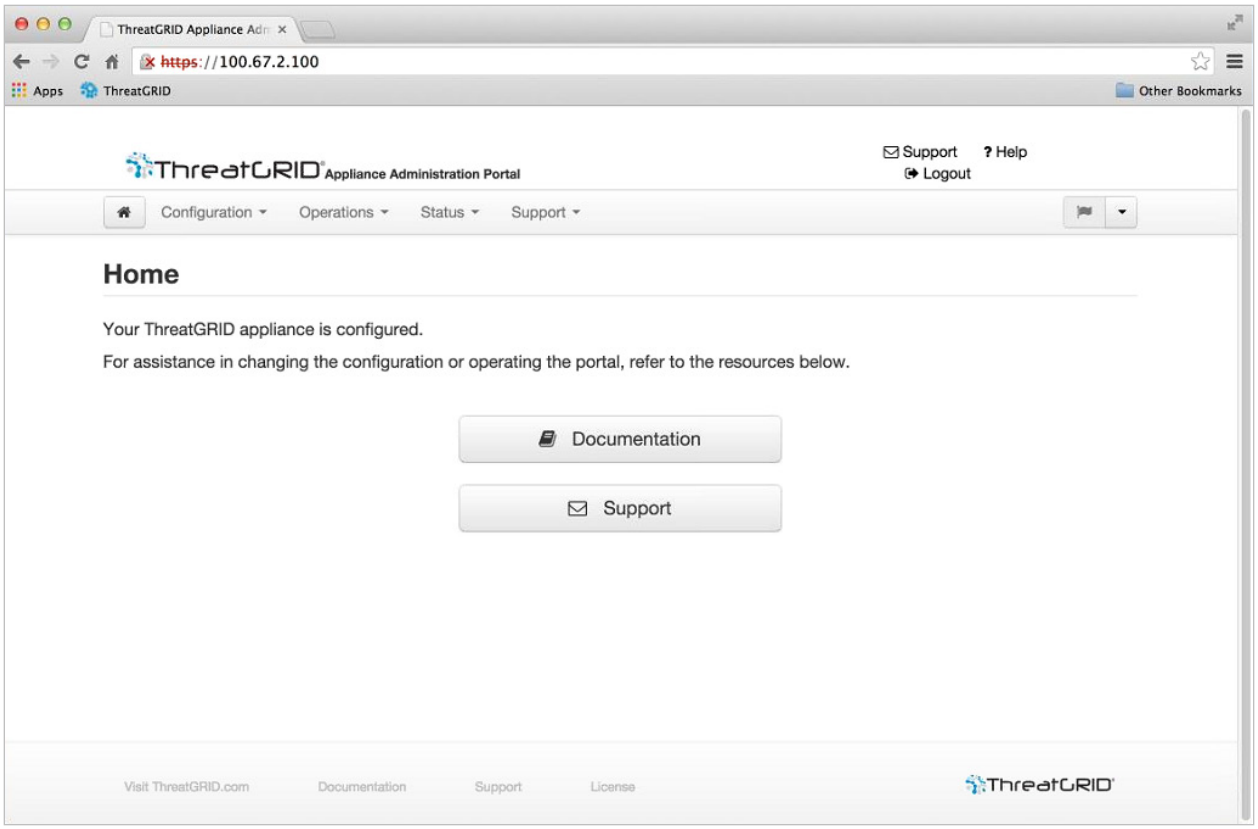
设备重新启动时，请勿做任何更改。

图 21 - 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 22 - 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。

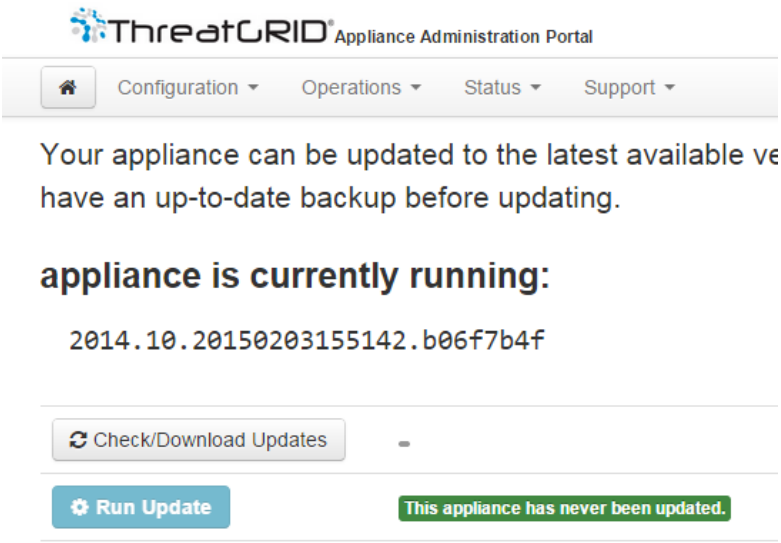
1. 从**操作 (Operations)** 菜单中，选择**更新设备 (Update Appliance)**。更新页面将会打开，其中显示设备当前的内部版本号。
2. 点击**检查/下载更新 (Check/Download Updates)**。该软件将检查是否有 Threat Grid 设备软件的最新更新/更新版本，如果有，则下载。此过程可能需要一些时间。
3. 在下载更新后，点击**运行更新 (Run Update)** 进行安装。

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

设备的内部版本号可以在“更新”(Updates) 页面上查看：OpAdmin **操作 (Operations)** > **更新设备 (Update Appliance)**：

图 23 – 设备内部版本号



设备内部版本号/版本查询表

设备的内部版本号可以在“更新”(Updates) 页面上查看：（OpAdmin **操作 [Operations]** > **更新设备 [Update Appliance]**），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
2015.08.20160315165529.599f2056	2.0.3	2016 年 3 月 15 日
2015.08.20160217173404.ec264f73	2.0.2	2016 年 2 月 18 日
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
2014.10.20160115122111.1f09cb5f	1.4.6 **注意：**此为 2.0 升级的起点。	2016 年 1 月 27 日
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。

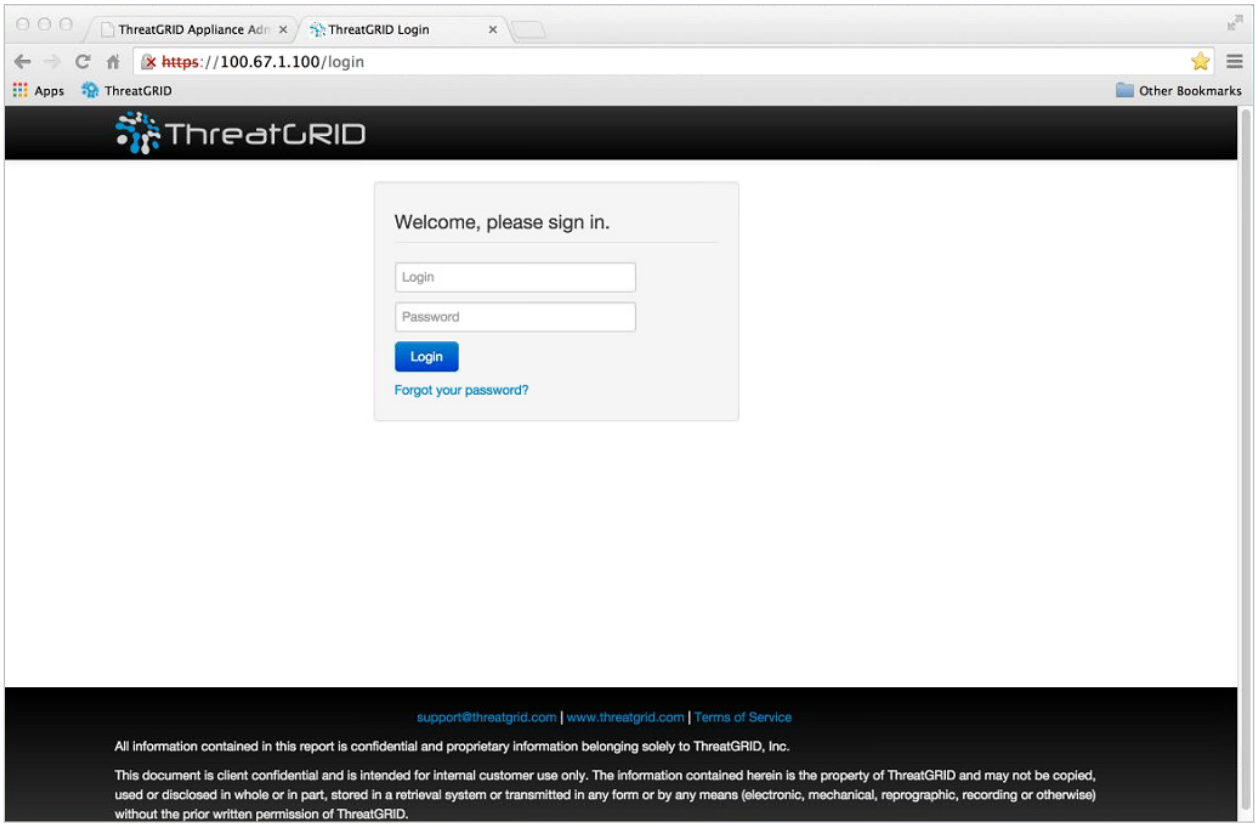
注意：从 1.0 更新至 1.0+hotfix2 大约需要 15 分钟。从版本 1.0 应用完全更新升级至 1.3（无数据迁移）大约需要 30 分钟。

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. 通过访问配置为 CLEAN 接口的地址登录到 AMP Threat Grid 门户。Threat Grid 登录页面将会打开：

图 24 - 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 (Login)**。主要的 Threat Grid *样本分析 (Sample Analysis)* 页面将打开。
4. 在右上角的**提交样本 (Submit a Sample)** 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 (Upload Sample)**。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 (Submissions)* 部分列出。分析完成后，分析结果应显示在*样本 (Samples)* 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。

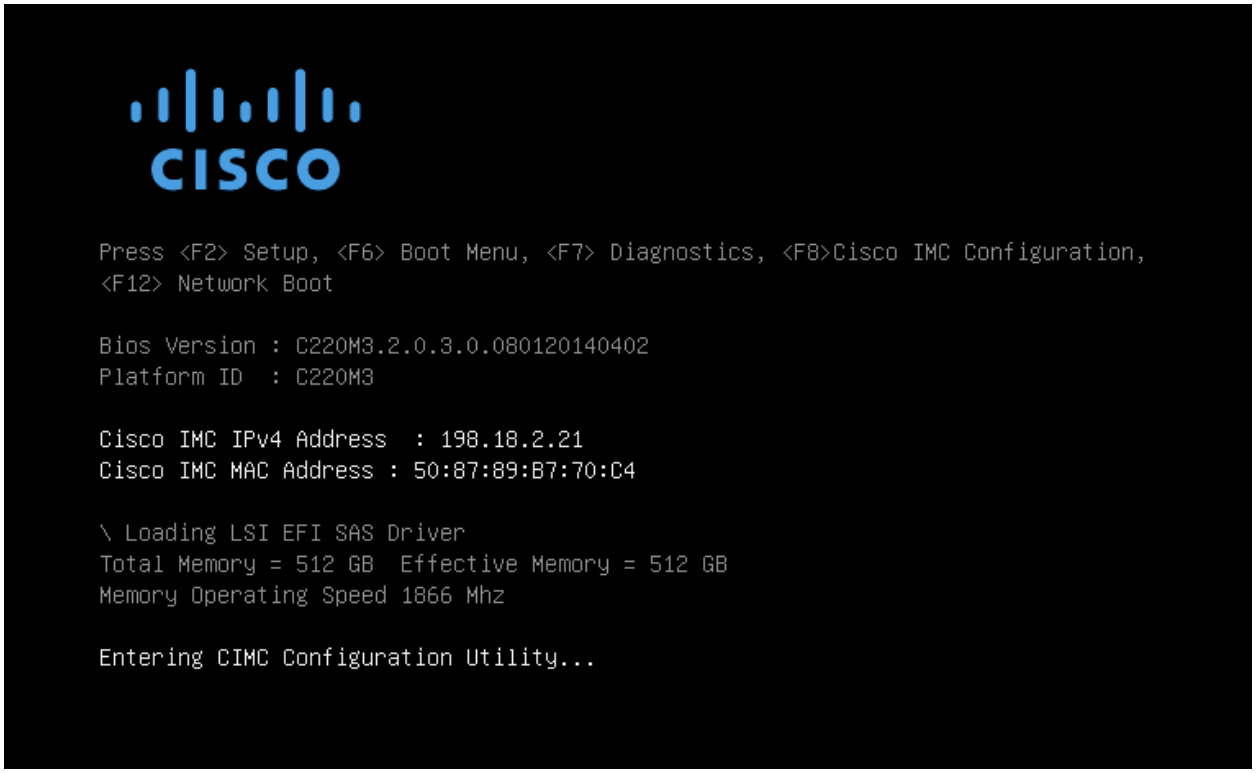
附录 A - CIMC 配置（推荐）

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。

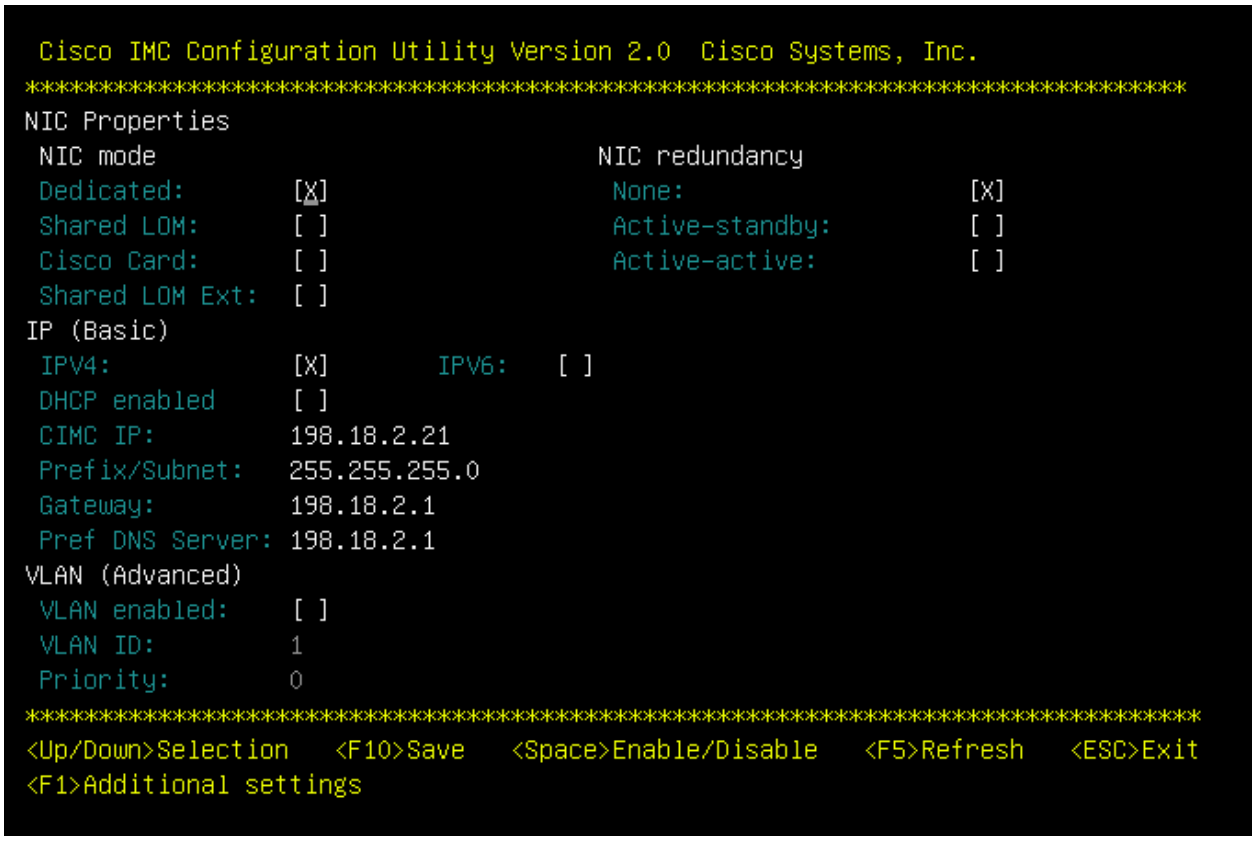
1. 接通服务器电源。思科屏幕随即打开：

图 25 - 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 26 – CIMC 配置实用程序

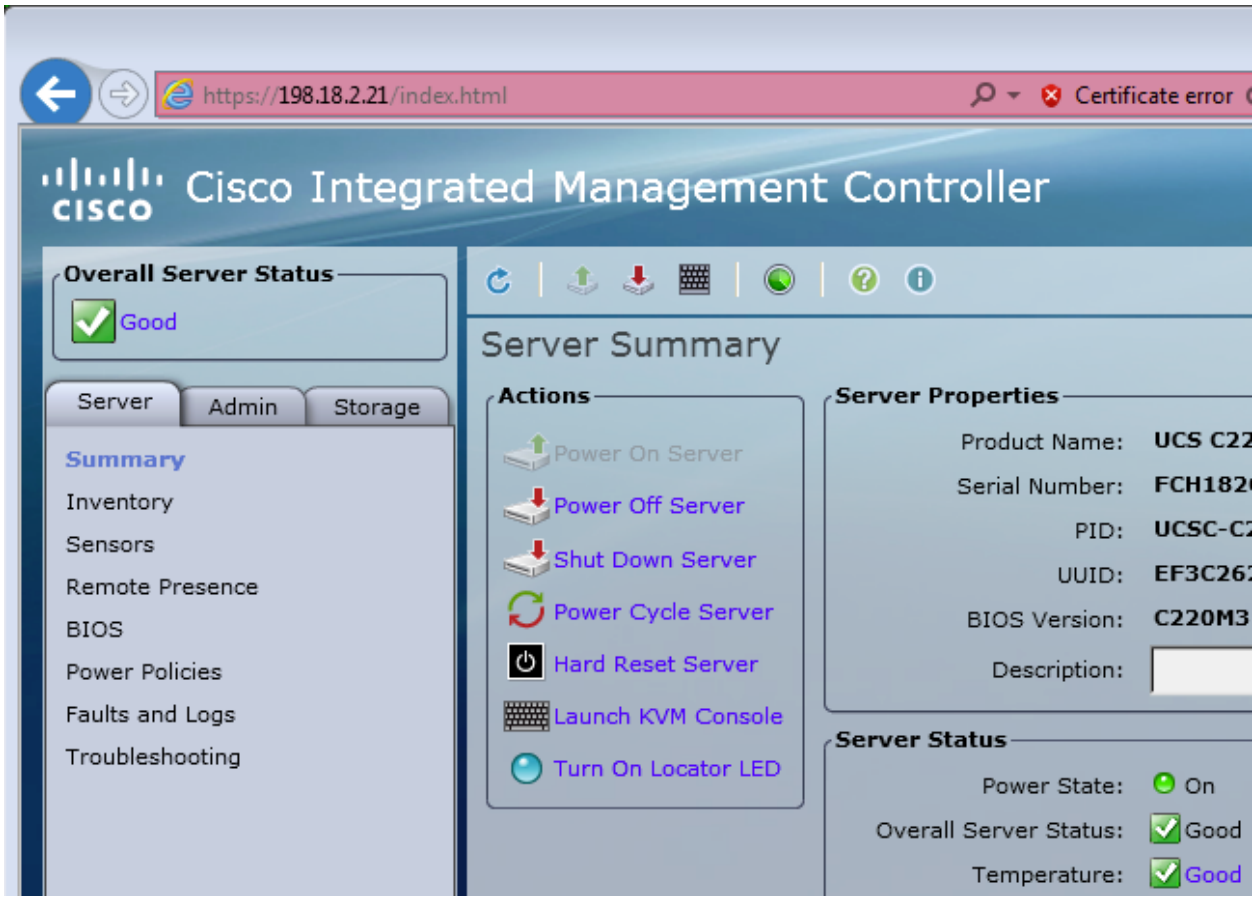


3. 在 CIMC 配置实用程序中，设置将用于远程服务器管理的 IP 地址。

4. 完成后，保存并退出。
   此时，您即可在 Web 浏览器中输入 https://*<CIMC-IP address>*/ 来对服务器进行远程管理

5. 初始用户名是“**admin**”，密码是“**password**”。

图 27 - 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，以及打开 KVM 远程完成剩余的设置步骤。