思科 AMP Threat Grid 设备管理员指南

版本 2.0.3

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。

目录

图片清单

引言

思科 AMP Threat Grid 设备（“TGA”）可提供完整的 AMP Threat Grid 恶意软件分析平台，该平台安装在单台 Cisco UCS 服务器 (UCS C220-M3) 上。Threat Grid 设备提供高度安全而可靠的本地环境，用于执行高级恶意软件分析，其中包含详细的威胁内容和分析。

众多处理敏感数据的组织（例如银行、保险公司、医疗保健机构等）必须遵守各种合规性规定、政策限制和其他准则，严禁将某种类型的文件（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 Threat Grid 设备，这些组织能够将可疑文档和文件发送到该设备进行分析，防止相关数据流出网络。

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

本文档是 TGA 管理员指南。它介绍如何开始使用新的 Threat Grid 设备以及如何管理设备实现最佳恶意软件分析。本指南还为那些将 Threat Grid 设备与其他思科产品和服务（如 ESA 和 WSA 设备和 FireAMP 私有云设备）进行集成的管理员提供信息。

有关 Threat Grid 设备设置和配置的信息，请参阅《*Threat Grid 设备设置和配置指南*》，可在 Threat Grid 设备产品文档页面查看。

新增内容

版本 2.0.3

此版本引入一系列功能以支持 FireAMP 私有云设备集成。这些功能包括在 Clean 和 Dirty 接口之间拆分 DNS 的功能、CA 管理和 FireAMP 集成配置。

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

版本 2.0 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 [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：最新版本包含之前所有的说明。

使用入门

思科 AMP Threat Grid 设备是一种 Linux 服务器，它在随分析样本所需的所有组件出厂前已安装完毕。在收到新设备后，您必须首先根据本地网络环境对其进行设置和配置。

在服务器启动并正常运行后，Threat Grid 设备管理员负责为 Threat Grid 恶意软件分析工具管理组织和用户，以及设备更新和备份，并执行其他服务器管理任务。

更新

我们建议您在使用前更新设备，以便确保安装所有最新的功能和安全更新。

请按照 *“安装更新”* 部分的说明检查最新的版本更新并进行安装。

文档

Threat Grid 设备文档（包括本文档、《*Threat Grid 设备设置和配置指南*》、版本说明的格式版本、集成指南等）可在 Cisco.com 网站上的内部资源页面*安装和升级指南*中进行查看。此页面包含当前和较早设备版本文档的链接。

Threat Grid 设备设置和配置指南

《*Threat Grid 设备设置和配置指南*》是本文档的指南。其中包含详细的设置信息，包括网络接口、推荐的防火墙规则、网络图、配置说明和其他任务。

Threat Grid 设备版本说明

OpAdmin 门户 (OpAdmin Portal) > 操作 (Operations) > 更新设备 (Update Appliance) > 版本说明 (Release Notes)

注意：安装和升级指南页面上同时提供 PDF 格式的 Threat Grid 设备版本说明 - 请参见上文的链接。

Threat Grid 门户版本说明

门户 UI 导航栏 (Portal UI Navigation bar) > 帮助 (Help) > 版本说明 (Release Notes)

Threat Grid 门户在线帮助和 API 文档

Threat Grid 门户的*使用 Threat Grid* 在线帮助、API 文档和其他信息可从 Threat Grid 门户帮助主页访问：

Threat Grid 门户用户界面 (Threat Grid Portal user interface) > 导航栏 (Navigation bar) > 帮助 (Help)

帮助 (Help) 主页随即打开，其中包含文档的链接。

ESA/WSA 设备文档

有关将 ESA 或 WSA 设备连接到 Threat Grid 设备的信息，请参阅“将 ESA/WSA 设备连接到 Threat Grid 设备”。

请参阅 ESA/WSA 的在线帮助或者用户指南了解 *“启用和配置文件信誉和分析服务”* 的说明。

- 《ESA 用户指南》位于：
  http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

- 《WSA 用户指南》位于：
  http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

许可

可在*OpAdmin 配置许可证 (OpAdmin Configuration License)* 页面管理 Threat Grid 许可证：

配置 (Configuration) > 许可证 (License)

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

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的 24 小时时间间隔，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。

假定条件

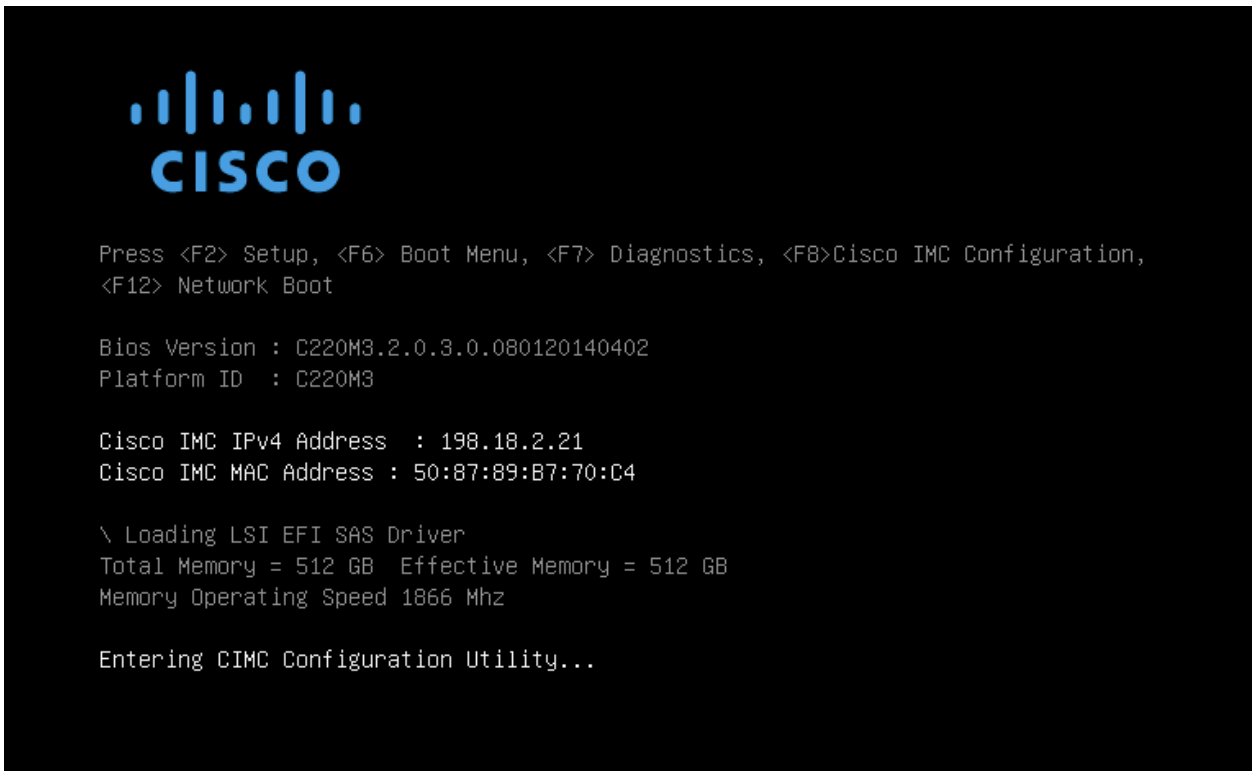
本指南假定，初始设置和配置步骤已经按《*Threat Grid 设备设置和配置指南*》中的说明完成，并且已成功提交并分析初始测试恶意软件样本。

管理

打开电源

打开设备电源，等待设备启动。思科屏幕会短暂显示：

图 1 - 启动期间的思科屏幕

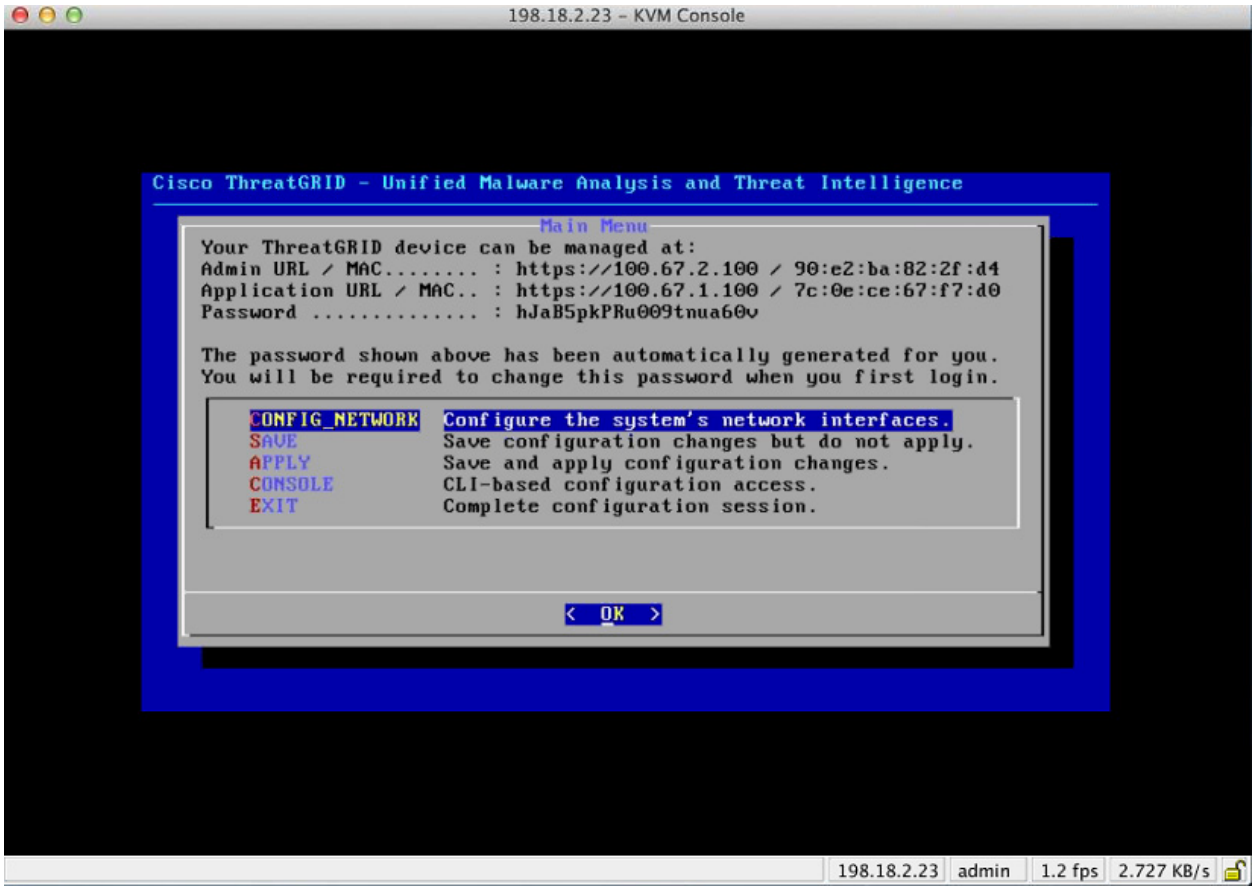


注意： 如果您想要配置 CIMC 界面，请在内存检查完成后按 **F8**。

有关详细信息，请参阅《Threat Grid 设备设置和配置指南》中的 *"配置 CIMC"* 一节。

当成功启动并连接服务器后，**TGSH 对话**显示在控制台上。

图 2 - TGSH 对话



注意：在设置并配置 TG 设备后，TGSH 对话将不再显示密码，在访问和配置 OpAdmin 接口时需要此密码。

丢失密码：如果您以后丢失了此密码，请参阅“恢复丢失的密码”的相关说明。

登录名和密码 - 默认

Threat Grid 门户 UI 管理员

- **登录名：** “admin”
- **密码：** “changeme”

TGA 管理员 - OpAdmin 和 threatgrid 用户

OpAdmin 管理员的密码与 " threatgrid " 用户密码相同。它是在 OpAdmin 接口中维护。在初始 TGA 设置期间，默认管理员密码已更改，该步骤一经完成，此密码将不会以可见文本的形式显示。如果密码丢失，您无法登录到 OpAdmin，请遵循下面的“**恢复丢失的密码**”说明。

CIMC（思科集成管理控制器）

- **登录名：** “admin”
- **密码：** “password”

恢复丢失的密码

默认管理员密码仅在初始的设备设置和配置过程中在 TGSH 对话中可见。一经完成初始配置，该密码就不会再以可见文本显示。

如果丢失了管理员密码，无法登录到 OpAdmin，请完成以下步骤：

重新设置丢失的管理员密码

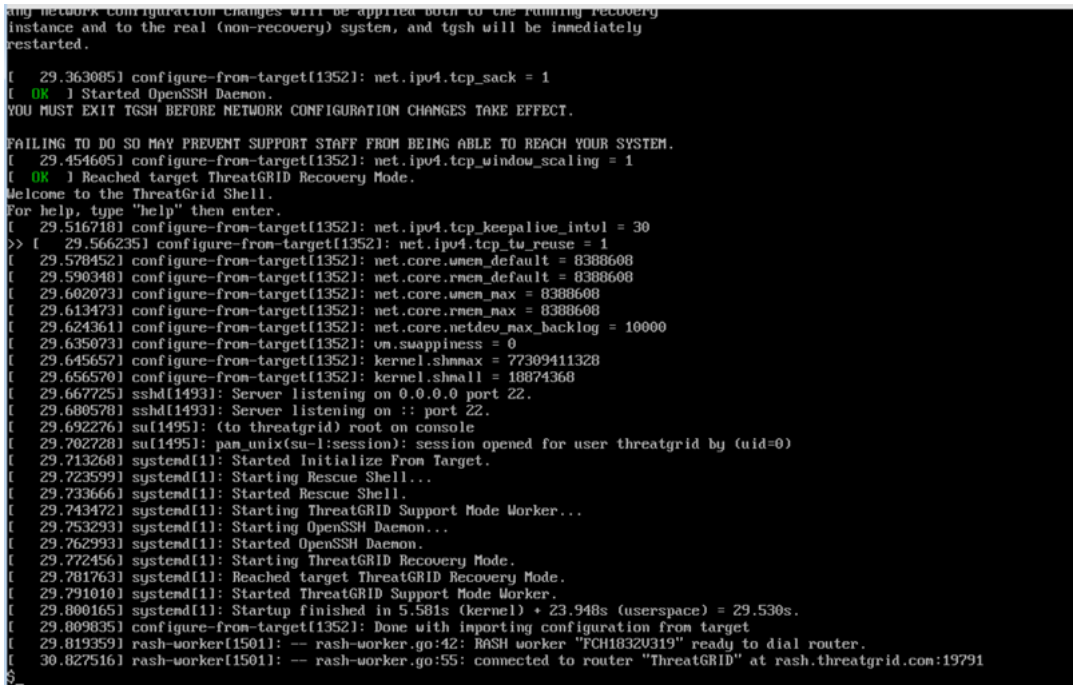
1. 重新启动设备。

   在设备启动期间，屏幕上**将出现一个显示 4 秒钟的窗口，**您可以在该窗口中选择**恢复模式 (Recovery Mode)**，如下所示：

图 3 - 启动菜单 - 恢复模式 (Recovery Mode)

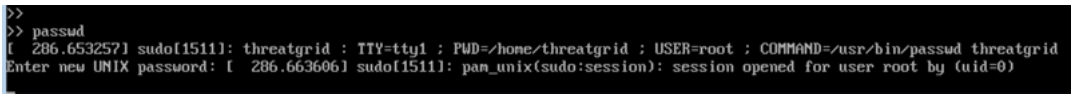
Threat Grid 外壳打开：

图 4 - 恢复模式下的 Threat Grid 外壳



2. 运行 `passwd` 以更改密码：

图 5 - 输入新密码



注意：命令提示符在此模式下并不始终可见，并且日志记录输出可能会显示在您输入的内容上部的任意位置。这不会影响输入；您可以继续“摸索”键入。

3. 忽略 2 行日志输出。请摸索输入密码，按 Enter，然后重新键入密码，并再次按 Enter。密码不会显示。

4. 您**必须**在命令行中键入 `exit` 才能保存新密码。

   如果重新启动，则系统不会保存新密码。如果您不键入 exit，即使一切看起来没有问题，系统仍将以静默方式放弃密码更改。

5. 接下来，请键入命令 `reboot` 并按 Enter 以正常模式启动设备。

安装更新

您必须首先按照《*Threat Grid 设备设置和配置指南*》中所述完成初始设置和配置步骤，才能将 Threat Grid 设备更新为较新的版本。

新设备：如果您的新设备出厂时安装了较早的版本，并且您希望安装更新，则必须先完成初始配置。请勿在所有设备配置完成之前应用更新。

除非已安装许可，否则将不会下载设备更新；并且，如果尚未完全配置设备（包括数据库），则可能无法正确应用设备更新。

Threat Grid 设备更新是通过 OpAdmin 门户应用的。

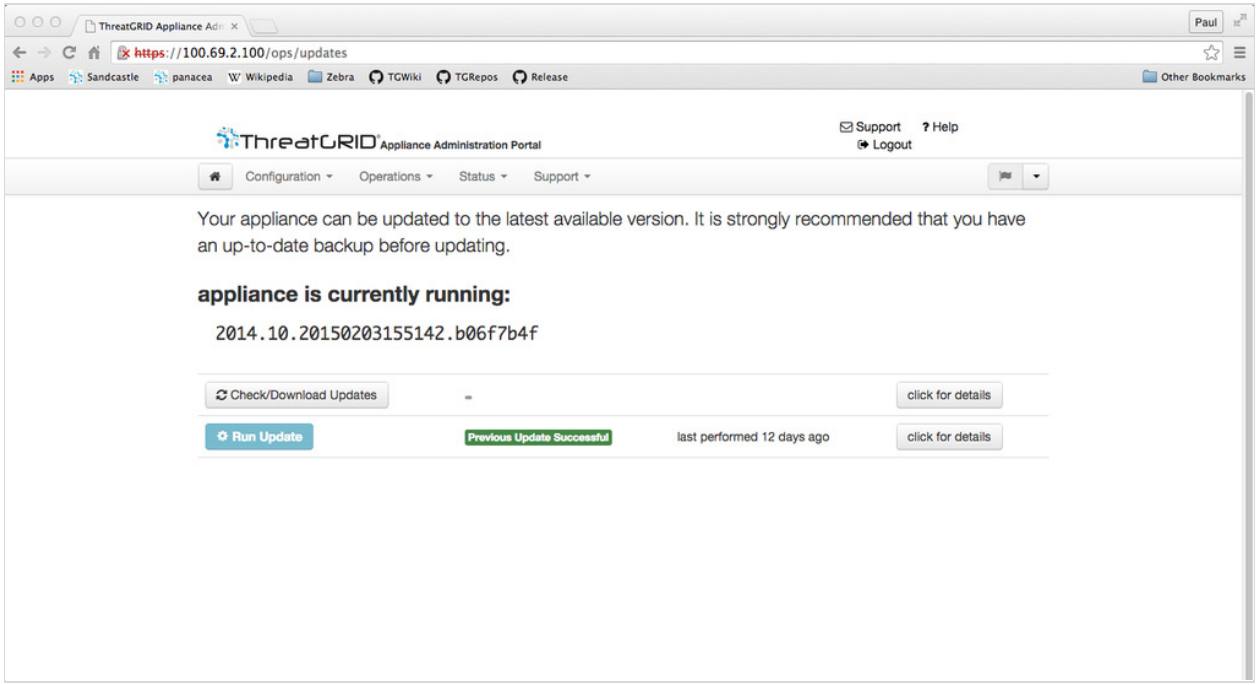
更新是不可逆的：在升级到最新版本后，您无法再将其恢复到先前版本。

要测试更新，请提交一个样本进行分析。

1. 从**操作 (Operations)** 菜单中，选择**更新设备 (Update Appliance)**。

   更新页面将打开，显示设备的当前版本：

图 6 - 设备版本号



2. 点击**检查/下载更新 (Check/Download Updates)**。该软件会检查是否存在设备软件的最新更新/版本，如果有，则会下载相关文件。

   注意：下载过程可能会花费一些时间：

   - 从版本 1.0 更新至 1.0+hotfix2 需要大约 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。

3. 在下载更新后，点击**运行更新 (Run Update)** 进行安装。

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的对应关系：

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	

更新端口

Threat Grid 设备通过 SSH、端口 22 下载版本更新。

- 从设备版本 1.1 起，还可以从文本 (curses) 接口应用版本更新，而不仅仅是从基于 Web 的管理接口 (OpAdmin)，如下所述。
- 自版本 1.3 起，使用 DHCP 的系统需要明确指定 DNS。在以前，情况并非如此。如果系统未将 DNS 服务器明确指定为版本 1.3，则升级会失败。

对更新进行故障排除

数据库升级失败 (database upgrade not successful) 消息表明新设备运行的 PostgreSQL 版本较低，不符合要求。

这是在 2.0 版本的任何升级之前对修复非常重要的一件事情，因为这表明数据库自动迁移过程没有成功。

有关更多信息，请参阅 2.0.1 版的版本说明。

支持 - 与 Threat Grid 联系

如需任何帮助，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。

  https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case
- **电话。**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

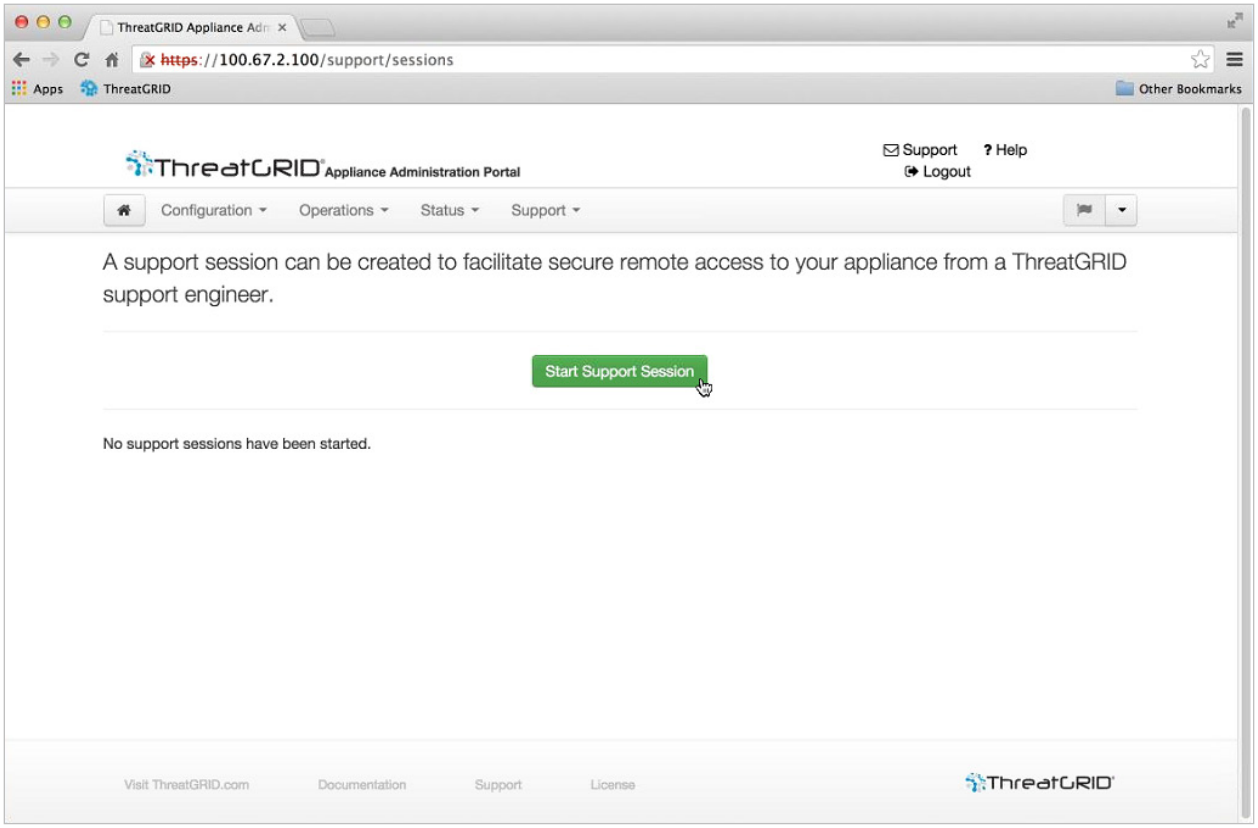
支持模式

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)。

图 7 - 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

支持快照主要是指运行系统的快照，其中包含日志、ps 输出等，可帮助支持人员排除任何问题。

1. 从**支持 (Support)** 菜单中，选择**支持快照 (Support Snapshots)**。
2. 拍摄快照。

3. 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。

备用

在 OpAdmin 中，在“操作”(Operations) >“备份”(Backups) 下

备份包含一组当前在设备上处于活动状态的配置文件，例如安装的 SSL 证书和网络配置。他们不包含有关样本、用户或组织的任何数据。

可以从设备创建并下载多个备份。

配置管理

在设备设置期间，已经按《*Threat Grid 设备设置和配置指南*》中所述执行了初始的 Threat Grid 设备配置。

Threat Grid 设备配置是在 **TGSH 对话 (TGSH Dialog)** 和 **OpAdmin 门户 (OpAdmin Portal)** 界面中进行管理的。

Threat Grid 组织和用户帐户通过 Threat Grid 门户 UI 进行管理（导航栏右上方的**欢迎 [Welcome]** 菜单）。

以下各节详细介绍 TGSH 对话和 OpAdmin 配置任务。

网络接口配置管理 - TGSH 对话

“TGSH 对话”(TGSH Dialog) 界面主要用于管理以下内容：

- 网络接口配置
- 查看 OpAdmin 管理员的密码
- 安装更新
- 启用支持模式
- 创建并提交支持快照

注意： 如果您是使用 DHCP 获取您的 IP，则请跳至以下 *“网络”* 部分：*使用 DHCP*。

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，显示当前网络设置。

2. 根据需要进行更改。

   注意： 您需要使用 **BACKSPACE** 删除原字符，才能再输入新的字符。

3. 将 Dirty 网络的 **DNS 名称 (DNS Name)** 留空。

4. 在您完成更新网络设置后，按 Tab 键向下移动并选择**验证 (Validate)** 来验证您输入的内容。

   如果已输入无效值，则您可能会看到错误。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。

5. 选择**应用 (Apply)** 应用您的配置设置。

   该控制台将成为一个空白的灰色框，然后它将列出所做配置更改的详细信息。

6. 点击**确定 (OK)**。

   网络配置控制台再次刷新，显示您输入的 IP 地址。网络配置现在已完成。

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。

一种重新连接到 TGSH 对话的方式是作为用户 **'threatgrid'** 通过 SSH 连接到管理 IP 地址。所需的密码可以是初始随机生成的密码（最初是显示在 TGSH 对话中），或者是在 OpAdmin 配置的第一步中创建的新管理密码。

密码更新

丢失密码？请参阅上面的 *“使用入门”* 部分中的 *“恢复丢失的密码”*。

在恢复模式下设置网络连接

1. 开始重新启动，并等待出现启动菜单，该菜单只显示大约 5 秒 - 因此请准备就绪（参阅上面的图 3 - 启动菜单 - 支持模式 (Support Mode)）。
2. 选择恢复模式 (Recovery Mode)。等待几分钟以便系统启动。
3. 一旦系统开始运行，请按 Enter 几次以获得一个 CLEAN 命令提示符。
4. 输入 **netctl clean**，然后按如下所示回答：
    - 配置类型 (Configuration type)：静态 (static)
    - IP 地址 (IP Address)：<CLEAN IP 地址>/<网络掩码>
    - 网关地址 (Gateway Address)：<CLEAN 的网关>
    - 路由 (Routes)：<留为空白>
    - 为最后一个问题回答 **y**。
5. 输入 **Exit** 应用配置。

这时，设备将尝试在端口 19791/tcp 上的 Clean 接口上打开一个出站支持连接。

主要配置管理 - OpAdmin 门户

《*Threat Grid 设备设置和配置指南*》中介绍了初始设置和配置向导。新的设备可能需要管理员才能完成附加配置，OpAdmin 设置随着时间的推移可能需要进行更新。

“OpAdmin 门户”(OpAdmin Portal) 是 Threat Grid 设备管理员的主要配置界面。这是一个 Web 门户界面，在 **Admin** 接口上配置 IP 地址后即可使用。

我们推荐使用 OpAdmin 配置您的设备，实际上，许多设备配置只能通过 OpAdmin 进行配置。OpAdmin 用于配置和管理大量重要的 Threat Grid 设备配置设置，包括：

- 管理员密码（OpAdmin 和“threatgrid”用户）
- Threat Grid 许可证
- 速率限制
- SMTP
- SSH
- SSL 证书

- DNS 服务器（包括 FireAMP 私有云集成的 DNS 配置）
- NTP 服务器
- 服务器通知
- 系统日志消息和 Threat Grid 通知远程服务器设置
- CA 证书管理（FireAMP 私有云集成）

注意： OpAdmin 中的配置更新应在一个会话中完成，以便减少配置期间中断 IP 地址的机率。

注意： OpAdmin 不会验证网关条目。如果您输入错误的网关并保存，则 OpAdmin 接口将不可访问。您不得不使用控制台来修复网络配置，如果过去这项操作是在 admin 接口完成的。如果管理仍有效，您可以在 OpAdmin 中修复它并重新启动。

提醒： OpAdmin 使用 HTTPS。将浏览器指向管理 IP 还不够；您必须指向：

https://adminIP/ 或 https://adminHostname/

SSH 密钥

设置 SSH 密钥可以为 Threat Grid 设备管理员提供通过 SSH (`threatgrid@<host>`) 访问 TGSH 对话的权限。

它不提供根访问权限或命令外壳。可以添加多个密钥。

“配置”(Configuration) > SSH

系统日志

除了可以将定期通知设置（在 OpAdmin 中的**配置 [Configuration]** > **通知 [Notifications]** 下）为通过邮件发送系统通知，您还可以配置远程系统日志服务器接收系统日志消息和 Threat Grid 通知。

1. 在 OpAdmin 中，在**配置 (Configuration)** > **系统日志 (Syslog)** 下
2. 在提供的字段中输入服务器 DNS，然后从下拉列表中选择一个协议；TCP 是默认值，另一个值为 UDP。
3. 当您点击**保存 (Save)** 后，请选中**验证 (Verification)** 框以执行 DNS 查询。如果主机无法解析名称，它将输出一个错误，并且不会保存（直到您输入有效的主机名）。

   如果未选中“验证”(Verification) 框，设备将接受任意名称，无论 DNS 是否有效。
4. 点击**保存 (Save)**。

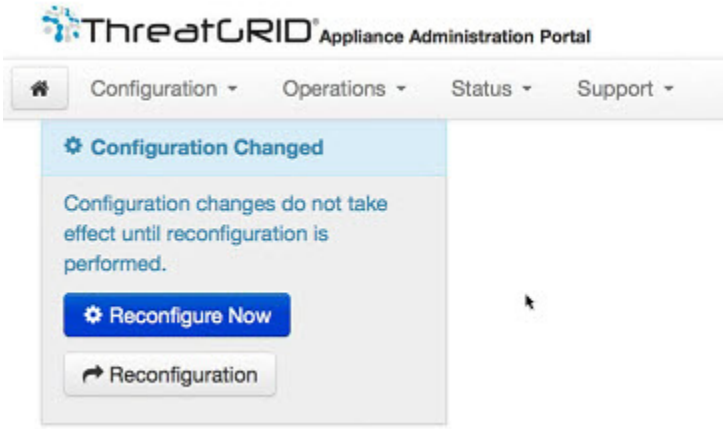
编辑或删除： 如果您需要更新系统日志 DNS，对其进行编辑或将其删除并点击**保存 (Save)** 即可。

重新配置

当对配置设置进行更改时，会在配置菜单下方显示浅蓝色的警报。当对任意 OpAdmin 配置设置完成更新时，必须在单独的步骤中保存重新配置。

1. 点击**配置已更改 (Configuration Changed)**。**重新配置 (Reconfiguration)** 对话框随即打开：

图 8 - 立即重新配置



2. 点击**重新配置 (Reconfigure)** 将您的更改应用到设备。

使用 DHCP

大多数设备用户使用的网络不是由 DHCP 配置的。但是，如果您已连接到配置为使用 DHCP 的网络，请阅读此部分。

注意： 如果初始设备网络配置使用的是 DHCP，您现在需要切换到静态 IP 地址，请参阅下面的 *“网络配置和 DHCP”*。

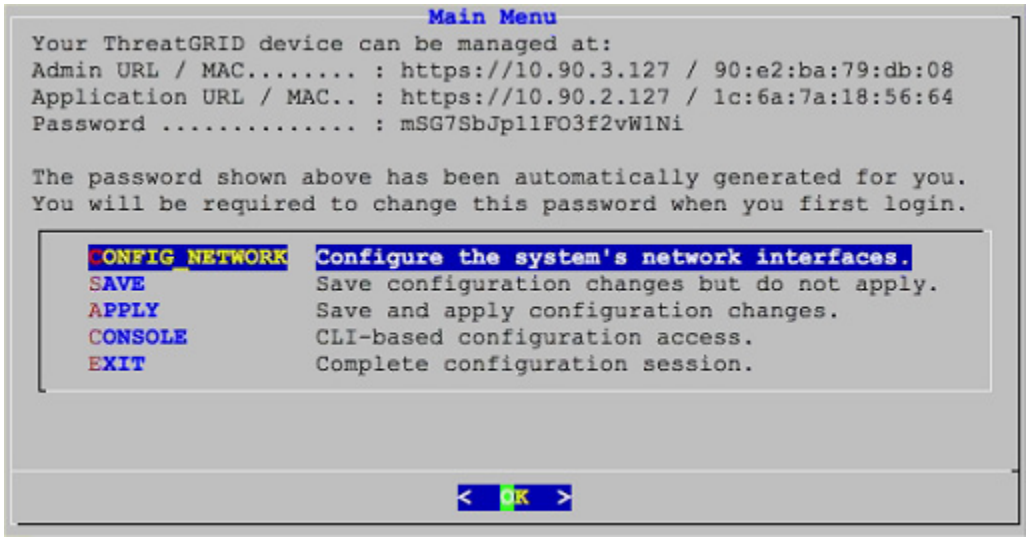
TGSH 对话显示您访问和配置 OpAdmin 门户接口所需的信息。

DHCP 的 IP 地址可能不会在您的设备启动后立即显示。请耐心等待！

DHCP 的显式 DNS

自版本 1.3 起，使用 DHCP 的系统需要明确指定 DNS。在以前，情况并非如此。如果系统未将 DNS 服务器明确指定为版本 1.3，则升级会失败。

图 9 - TGSH 对话（连接到一个配置为使用 DHCP 的网络）



- **管理员 URL (Admin URL)：** 管理员网络。您需要此地址才能继续 OpAdmin 的剩余配置任务。
- **应用 URL (Application URL)：** Clean 网络。

注意： 这是完成 OpAdmin 配置后要使用的地址，用于访问 Threat Grid 应用。

- 未显示 DIRTY 网络。
- **密码 (Password)** 为设备安装过程中随机生成的初始管理员密码。您稍后需要更改此密码，作为 OpAdmin 配置过程的第一步。

如果您计划永久地使用 DHCP，则不需要其他网络配置，除非您需要将“管理 IP”(Admin IP) 地址更改为静态。

网络配置和 DHCP

- 如果初始配置使用了 DHCP，并且您现在需要为所有三个网络将 IP 分配从 DHCP 调整为永久的静态 IP 地址，请执行下面的步骤：

注意： OpAdmin 不会验证网关条目。如果您输入错误的网关并保存，则 OpAdmin 接口将不可访问。您不得不使用控制台来修复网络配置，如果过去这项操作是在 admin 接口完成的。如果管理仍有效，您可以在 OpAdmin 中修复它并重新启动。

1. 在左侧列中，点击**网络 (Network)**。（尽管在“许可证”[License] 窗口中选中**配置 [Configuration] > 网络 [Network]**，但 DHCP 网络配置尚未完成。）

   网络配置 (Network Configuration) 页面随即打开。

Clean

2. **IP 分配 (IP Assignment)。**从下拉列表选择**静态 (Static)**。
3. **IP 地址 (IP Address)。**为 **CLEAN** 网络接口输入静态 IP 地址。
4. 酌情完成**子网掩码 (Subnet mask)** 和**网关 (Gateway)**。
5. 选中**验证 DNS 名称 (Validate DNS Name)**，验证 DNS 是否已解析为您输入的 IP 地址。

Dirty

6. **IP 分配 (IP Assignment)。**从下拉列表选择静态 (Static)。
7. **IP 地址 (IP Address)。**为 **DIRTY** 网络接口输入静态 IP 地址。
8. 酌情完成**子网掩码 (Subnet mask)** 和**网关 (Gateway)**。

管理

在初始设备设置和配置期间，已使用 **TGSH 对话**配置了 Admin 网络设置。

DNS

9. 完成**首选 DNS (Primary DNS)** 和**辅助 DNS (Secondary DNS)** 服务器字段。

保存您的设置

10. 完成后，请点击**下一步（应用配置） (Next (Applies Configuration))** 保存您的网络配置设置。

SMTP/邮件

可通过*邮件 (Email)* 页面管理邮件配置。

时间

NTP 服务器是在*日期和时间 (Date and Time)* 页面上管理的。

应用 DHCP 配置

要应用您的 DHCP 配置设置，请点击**配置已更改 (Configuration Changed)**，然后点击**立即重新配置 (Reconfigure Now)**。

SSL 证书和 THREAT GRID 设备

所有进出 Threat Grid 设备的网络流量均是使用 SSL 进行加密。有关如何管理 SSL 证书的完整说明不属于本指南的范围。但是，本指南会提供以下信息协助您按步骤设置 SSL 证书以支持 Threat Grid 设备连接到 ESA/WSA 设备、FireAMP 私有云和其他集成。

使用 SSL 的接口

在 Threat Grid 设备上有两个使用 SSL 的接口：

- Threat Grid 门户 UI 和 API 的 **Clean** 接口，以及集成（ESA/WSA 设备、FireAMP 私有云处置更新服务等）。
- **OpAdmin 门户 (OpAdmin Portal)** 的 **Admin** 接口。

支持的 SSL/TLS 版本

- TLSv1.0
- TLSv1.1
- TLSv1.2

不支持 SSL 证书

我们目前不支持客户提供的 CA 证书，我们不支持使用自签名证书的邮件服务器。

注意： 通过允许客户导入自己的受信任证书或 CA 证书，2.0.3 版已克服这些限制。

SSL 证书 - 自签名默认

Threat Grid 设备出厂时安装了一组自签名 SSL 证书和密钥。一组自签名 SSL 证书和密钥用于 **Clean** 界面，而另一组则用于**管理 (Admin)** 接口。设备 SSL 证书可以由管理员替换。

默认 Threat Grid 设备 SSL 证书主机名（通用名称）是 " *pandem* "，有效期为 10 年。如果在配置过程中将其他主机名分配给 Threat Grid 设备，则证书中的主机名和 CN 将不再匹配。证书中的主机名还必须与连接的 ESA 或 WSA 设备或其他集成的思科设备或服务所预期的主机名匹配，这是因为许多客户端应用需要 SSL 证书，其中用于证书中的 CN 与设备的主机名匹配。

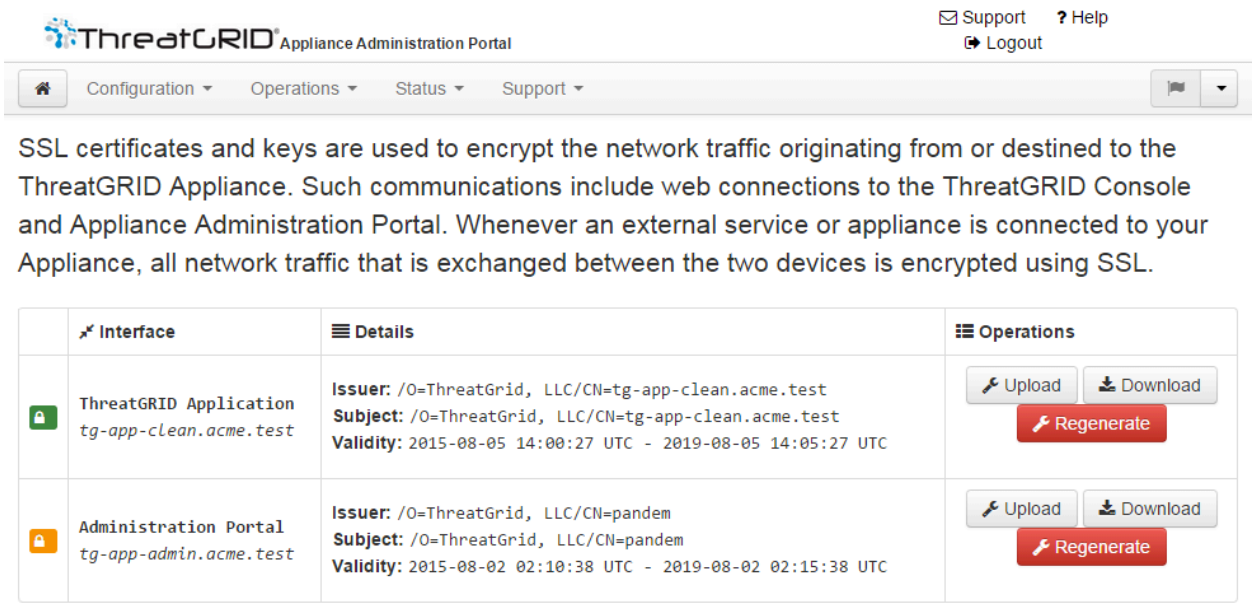
配置入站连接的 SSL 证书

其他思科产品（例如 ESA 和 WSA 设备以及 FireAMP 私有云）可与 Threat Grid 设备集成并向其提交样本。从 Threat Grid 设备的角度来看，这些集成是*入站*连接。集成设备或其他设备必须能够信任 Threat Grid 设备的 SSL 证书，因此您将需要将其从 TGA 导出（首先请确保 SSL 证书在 CN 字段中使用正确的主机名，如有需要请重新生成或将其替换），然后将其导入集成的设备或服务。

可在 **SSL 证书配置 (SSL Certificate Configuration)** 页面中配置用于入站 SSL 连接的 Threat Grid 设备上的证书。**Clean** 和 **Admin** 接口的 SSL 证书可独立配置。

选择 **OpAdmin > 配置 (Configuration) > SSL**。“SSL 证书配置”(SSL Certificate configuration) 页面随即打开：

图 10 - SSL 证书配置页面



上述图中有两个 SSL 证书：“ThreatGRID Application”是 **CLEAN** 接口，“Administration Portal”是 **Admin** 接口。

CN 验证

在“SSL 证书配置”(SSL Certificate configuration) 页面中，彩色挂锁图标表示 TG 设备上 SSL 证书的状态。主机名必须与 SSL 证书中使用的 CN（“通用名称”）匹配。如果它们不匹配，您就需要一个使用当前主机名的证书替换该证书。请参阅下面的“替换 SSL 证书”。

- 绿色挂锁图标表示 CLEAN 接口主机名与 SSL 证书中使用的 CN（“通用名称”）匹配。
- 黄色挂锁为警告，表示“管理”(Admin) 接口主机名与 SSL 证书中的 CN 不匹配。您需要一个使用当前主机名的证书替换该证书。

替换 SSL 证书

由于各种原因，某些时候通常需要替换 SSL 证书。例如，SSL 证书到期或主机名变更。您可能也需要添加或替换 SSL 证书以便支持 Threat Grid 设备和其他思科设备和服务器之间的集成。

ESA/WSA 设备和其他 CSA 思科集成设备可能需要 SSL 证书，在该证书中公用名称与 Threat Grid 设备主机名匹配。在这种情况下，您需要替换默认 SSL 证书，并使用与要从中访问 Threat Grid 设备的主机相同的主机名生成一个新的证书。

在您将 Threat Grid 设备与 FireAMP 私有云进行集成以使用其处置更新服务的情况下，您将需要安装 FireAMP 私有云 SSL 证书以使 Threat Grid 设备能够信任该连接。

有若干方式可以在 Threat Grid 设备上替换 SSL 证书：

- 重新生成新的 SSL 证书，它将对 CN 使用当前的主机名。
- 下载 SSL 证书
- 上传新的 SSL 证书。这可以是商业或企业 SSL 证书或是您使用 OpenSSL 自行制作的 SSL 证书。
- 生成您自己的 SSL 证书 - 使用 OpenSSL 的示例

本文以下各节将对这些进行说明。

重新生成 SSL 证书

在 v1.3 版本之前的 Threat Grid 设备中需要使用 OpenSSL 或其他 SSL 工具手动生成新的 SSL 证书，现在则不再有此需要。不过，该方法仍然有效，如以下生成您自己的 SSL 证书 - 使用 OpenSSL 的示例中所述。

注意： 执行此任务之前，应将 Threat Grid 设备升级到 1.4.2 或更高版本。

在 **OpAdmin SSL 证书配置 (SSL Certificate Configuration)** 页面中，点击**重新生成 (Regenerate)**。在证书的 CN 字段中使用设备当前主机名的 Threat Grid 设备上会生成新的自签 SSL 证书。CN 验证挂锁图标是否为绿色。可按下一节所述内容下载重新生成的证书（.cert 文件），并可安装在集成设备上。

下载 SSL 证书

可以下载 Threat Grid SSL 证书，而不是密钥，并且可以将其安装在您的集成设备上，如此它便可信任来自 TG 设备的连接。此步骤您只需要 .cert 文件。

1. 在“OpAdmin SSL 证书配置”(OpAdmin SSL Certificate Configuration) 页面上，点击您希望获取的证书旁边的**下载 (Download)**。就会下载 SSL 证书。
2. 接下来，像安装任何其他 SSL 证书一样，在 ESA/WSA 设备、FireAMP 公共云或其他集成的思科产品上安装下载的 SSL 证书。

上传 SSL 证书

如果贵组织内已有商业或公司 SSL 证书就位，您可以使用该证书为 TGA 生成新的 SSL 证书，并在 ESA/WSA 或其他集成设备上使用 CA 证书。

生成您自己的 SSL 证书 - 使用 OpenSSL 的示例

另一方法是手动生成您自己的 SSL 证书，例如当本地尚无 SSL 证书基础设施就位，并且您无法通过其他手段获取 SSL 证书的情况下。稍后即可按上文所述上传此证书。

此示例说明为“Acme Company”生成新的自签 SSL 证书的命令。该示例使用 OpenSSL，这是一个用于创建和管理 OpenSSL 证书、密钥和其他文件的标准开源 SSL 工具。

注意： OpenSSL 不是思科产品，思科不对其提供技术支持。请在网络上搜索有关使用 OpenSSL 的更多信息。思科提供*思科 SSL* 这个 SSL 库用于生成 SSL 证书。

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout
tgapp.key -nodes -out tgapp.cert -subj "/C=US/ST=New
York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

- **openssl**：OpenSSL。
- **req**：指定我们希望使用 X.509 证书签名请求 (CSR) 管理。
  “X.509” 是公钥基础设施标准，SSL 和 TLS 使用该标准进行密钥和证书管理。我们希望创建新的 X.509 证书，因此，我们使用此子命令。
- **-x509**：通过告知实用程序我们希望制作自签证书而不是像通常那样生成证签名请求，从而修改先前的子命令。
- **-days 3650**：此选项设置证书将被视为有效的时间长度。此处我们将其设置为 10 年。
- **-newkey rsa:4096**：指定我们希望同时生成新证书和新密钥。我们在前面的步骤中未创建签署证书所需的密钥，因此，我们需要与证书一起创建它。rsa:4096 部分告知制作一个长度为 4096 位的 RSA 密钥。
- **-keyout**：此行告知 OpenSSL 将我们创建的已生成的密钥文件放到哪里。
- **-nodes**：这将告知 OpenSSL 跳过该选择，以便利用口令来保护证书安全。当服务器启动时，设备需要能够在无用户干扰的情况下读取文件。口令可以阻止此类情况的发生，因为我们需要在每次重新启动后输入口令。
- **-out**：告知 OpenSSL 将我们创建的证书放到哪里。
- **-subj**：示例：

  C=US：国家/地区。

  ST=New York：州。

  L=Brooklyn：位置。

  O=Acme Co：所有者名称。

  CN=tgapp.acmeco.com：请输入 Threat Grid 设备 FQDN（“完全限定域名”）。这包括 Threat Grid 设备（我们的示例中为 " tgapp " ）的主机名以及附加到末尾的关联域名 (“acmeco.com”)。

  重要信息：您需要至少更改公用名称，以匹配 Threat Grid 设备 CLEAN 接口的 FQDN。

一旦生成新的 SSL 证书后，请使用 SSL 页面的**上传 (Upload)** 按钮将其上传到 Threat Grid 设备，并同时将其上传到 ESA/WSA 设备（仅限 .cert）。

配置出站连接的 SSL 证书

2.0.3 版的 Threat Grid 设备包括支持与 FireAMP 私有云进行集成以使用处置更新服务的功能。

配置 DNS

默认情况下，DNS 使用 Dirty 接口。如因 Clean 接口未用于集成而无法在 Dirty 接口上解析集成设备或服务（例如 FireAMP 私有云）的主机名时，则可以在 OpAdmin 中配置使用 Clean 接口的独立 DNS 服务器。

在 **OpAdmin** 中，选择**配置 (Configuration) > 网络 (Network)**，并完成 Dirty 和 Clean 网络的 DNS 字段，然后点击**保存 (Save)**。

CA 证书管理

版本 2.0.3 新增功能之一即*出站* SSL 连接的 CA 证书管理 truststore 新页面，如此 TGA 便可信任 FireAMP 私有云向其发送有关已分析样本被视为恶意的通知。

在 **OpAdmin** 中，选择**配置 (Configuration) > CA 证书 (CA Certificates)**。选择：

1. **从主机导入 (Import from Host)。**从服务器检索证书。“从服务器检索证书”(Retrieve certificates from server) 对话框随即打开。
2. 输入 FireAMP 私有云的**主机 (Host)** 和**端口 (Port)** 并点击**检索 (Retrieve)**。系统即会检索证书。

或

从剪贴板导入 (Import from Clipboard)。从剪贴板粘贴 PEM，并点击**添加证书 (Add Certificate)**。

3. 点击**导入 (Import)**。

处置更新服务管理

此任务是从 Threat Grid 门户 UI 内部执行的。

1. 从**我的帐户 (My Account)** 下拉列表中选择**管理 FireAMP 集成 (Manage FireAMP Integration)**。“处置更新服务”(Disposition Update Service) 页面随即打开。
2. 输入**FireAMP 私有云 URL (FireAMP Private Cloud URL)**、FireAMP 配置门户提供的**管理员用户名 (admin user name)** 和**密码 (password)**，并点击**配置 (Config)**。

有关 FireAMP 私有云设备集成的详细信息，请参阅“将 Threat Grid 设备连接到思科 FireAMP 私有云”：

将 ESA/WSA 设备连接到 Threat Grid 设备

思科产品（如 ESA/WSA 和其他设备、设备、服务等）可以通过 SSL 加密连接实现与 Threat Grid 设备的集成，以便向其提交潜在恶意软件样本以进行分析。在 Threat Grid 设备与 ESA/WSA设备之间的集成是由思科沙盒 API（“CSA API”）启用的，通常称为“CSA 集成”。

为了 ESA/WSA 设备可以连接到 Threat Grid 设备，Threat Grid 设备的 SSL 证书 CN 必须与其当前主机名匹配，同时必须是集成 ESA/WSA 设备预期的主机名。

集成设备必须与 Threat Grid 设备注册后才能提交样本进行分析。在集成的 ESA/WSA 设备可以在 Threat Grid 设备处注册前，ESA/WSA 管理员必须首先为其设备和网络环境设置 SSL 证书连接。

本节介绍设置 Threat Grid 设备与集成的 ESA/WSA 设备和其他思科产品进行通信的必要步骤。

ESA/WSA 文档的链接

请参阅 ESA/WSA 的在线帮助或者用户指南了解 *“启用和配置文件信誉和分析服务”* 的说明。

- 《ESA 用户指南》位于：
  http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
- 《WSA 用户指南》位于：
  http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

1. 主机名必须匹配 CN 和 ESA/WSA 预期的主机名

   Threat Grid 设备 SSL 证书中的 CN 必须与其当前的主机名匹配。对于与集成的 ESA/WSA 设备的成功连接，这也必须是集成的 ESA/WSA 设备识别 TGA 的同一主机名。

   根据您的需要，您可能需要重新生成 Threat Grid 设备上的自签 SSL 证书，以便其在 CN 字段中使用当前的主机名，接着将其下载到您正在工作的环境中，将其上传并安装到集成的 ESA/WSA 设备上。

   或者，您可能需要通过上传企业或商业 SSL 证书（或手动生成的证书）来替换当前的 TGA SSL 证书。

   有关详细说明，请参阅：“配置入站连接的 SSL 证书”。

   一旦完成 SSL 证书设置，下一步即验证 Threat Grid 设备与 ESA/WSA 设备是否可以相互通信。

2. 检验连接

   思科 ESA/WSA 设备必须能够通过您的网络连接到 Threat Grid 设备的 **CLEAN** 接口

   按照产品相应指南的说明来确认 TGA 和 ESA/WSA 设备可以彼此通信。（请参见上述链接。）

3. 将思科 ESA/WSA/其他设备注册到 Threat Grid 设备。

   根据那些将自身自动注册到 Threat Grid 设备的产品的说明文档配置 ESA/WSA 设备。

4. 完成 ESA/WSA 文件分析配置。

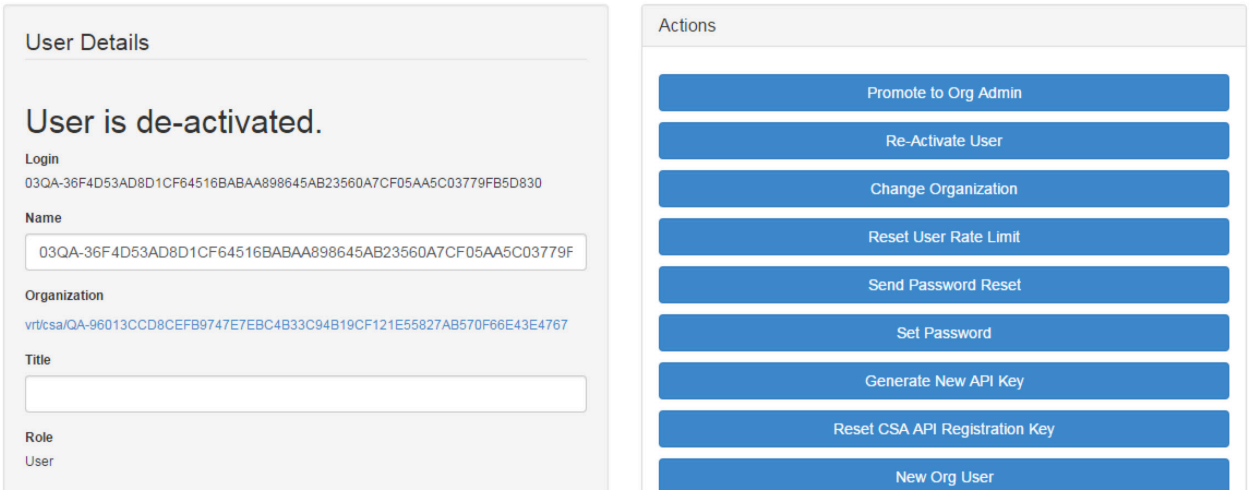
在连接设备注册后，会使用设备 ID 作为登录 ID 自动创建一个新的 Threat Grid 用户，同时会基于同一 ID 创建一个新组织。新的设备用户帐户必须由管理员激活，如下节中所述。

在 Threat Grid 设备上激活新设备用户帐户。

当 ESA/WSA 设备或其他集成连接并自行注册到 Threat Grid 设备时，会自动创建一个新的 Threat Grid 用户帐户。此用户帐户的初始状态为“已停用”(de-activated)。与任何其他 Threat Grid 用户相同，必须由一个 Threat Grid 设备管理员手动激活设备用户帐户，然后才能使用它来提交恶意软件样本以进行分析。

1. 请以管理员身份登录 Threat Grid 门户 UI。
2. 从导航栏**欢迎 (Welcome)** 菜单中，选择**管理用户 (Manage Users)**。**Threat Grid 用户 (Threat Grid Users)** 页面随即打开。
3. 打开设备用户帐户的**用户详细信息 (User Details)** 页面（您可能需要使用“搜索”[Search] 来找到它）。用户状态当前为“已停用”(de-activated)：

图 11 - 用户详细信息 (User Details) 页面 > 重新激活用户



4. 点击**重新激活用户 (Re-Activate User)**。会打开一个对话框要求您确认。
5. 在对话框中点击**重新激活 (Re-Activate)** 进行确认。

ESA/WSA 或其他集成设备现在可以与 Threat Grid 设备进行通信。

将 Threat Grid 设备连接到思科 FireAMP 私有云

您必须按以下顺序在设备上执行 Threat Grid 设备处置更新服务和 FireAMP 私有云集成设置任务，尤其是当您在设置新设备的情况下。如果您在集成已经过设置和配置的设备，以下顺序就不那么重要了。

从 Threat Grid 设备的角度来看，此连接为外发连接。此集成不使用 CSA API。

有关必须在另一端执行的任务的详细信息，请参阅 FireAMP 私有云文档。

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
1	按常规方式设置并配置 Threat Grid 设备（“TGA”）（即尚无集成）。	
2		按常规方式设置并配置 FireAMP 私有云（即尚无集成）。
3		**为 TGA 集成配置 FireAMP 私有云：** 选择**集成 (Integrations) > Threat Grid** 并转到 **连接到 Threat Grid (Connection to Threat Grid)** 部分。 要完成与 Threat Grid 设备的连接，您必须信任它。您需要其 DNS 主机名、SSL 证书和 API 密钥。 转到 TGA 列中的步骤 3.1 以找到此信息。

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
3.1	**SSL 证书：** 如果需要，在“Threat Grid 设备 OpAdmin”(Threat Grid Appliance OpAdmin) 界面中，选择**配置 (Configuration) > SSL** 重新生成新的 SSL 证书来替换默认证书，然后将其下载并安装在 FireAMP 私有云设备中。（TGA SSL 证书在SSL 证书和 THREAT GRID 设备中有说明。） **主机名** 选择**配置 (Configuration) > 主机名 (Hostname)** **API 密钥**： API 密钥可以在“Threat Grid Face 门户 UI”(Threat Grid Face Portal UI) 中用于集成的帐户的**用户详细信息 (User Details)** 页面中找到： 1. 转到**Threat Grid 门户 UI (Threat Grid Portal UI)**。 2. 从右上方“欢迎”(Welcome) 菜单（位于导航栏的右上角）中，选择**管理用户 (Manage Users)**。 3. 导航（如果需要可使用“搜索”[Search]）集成的用户帐户的**用户详细信息 (User Details)** 页面，并复制**API 密钥 (API Key)**。请注意执行此操作无需为“admin”用户，而可以是 Threat Grid 设备上为此用途特别创建的其他用户。	

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
3.2		完成**连接到 Threat Grid (Connection to Threat Grid)** 字段： 1. 输入 TGA 主机名 2. 输入用于集成的帐户的 Threat Grid API 密钥。 3. 选择 TGA SSL 证书文件。 4. 点击“保存配置”(Save Configuration)。 5. 点击“测试连接”(Test Connection)。 6. 一旦连接测试通过，您将需要在 FireAMP 私有云上运行“重新配置”(Reconfiguration) 以应用更改。 严格来说，这将允许 AMP 与 Threat Grid 设备进行通信，而您此时便可将样本上传到 TG。但是，您必须完成剩余步骤以设置处置更新服务，以便将处置结果发送到 TGA。 （有关详细信息，请参阅 FireAMP 私有云的用户文档。）
4	**设置处置更新服务** 以下步骤说明如何设置处置更新服务	

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
4.1	**配置 DNS（如果需要）：** Clean 接口用于 FireAMP 集成。但在默认情况下，DNS 使用 Dirty 接口。如果在 Dirty 接口上无法解析 FireAMP 私有云主机名，则可以在 OpAdmin 中配置使用 Clean 接口的独立 DNS 服务器。 在 OpAdmin 中，选择**配置 (Configuration) > 网络 (Network)**，并完成 **Dirty** 和 **Clean** 网络上的 DNS 字段，然后点击**保存 (Save)**。	
4.2	**CA 证书管理：** 下一步是将 FireAMP 私有云 SSL 证书下载或复制/粘贴到 Threat Grid 设备，以便其信任集成设备： 1. 在 OpAdmin 中，选择**配置 (Configuration) > CA 证书 (CA Certificates)**。您可以从 FireAMP 私有云主机选择要导入的 SSL 证书，或从剪贴板导入。 2. 选择要导入的证书并点击**从主机导入 (Import from Host)**。**从服务器检索证书 (Retrieve certificates from server)** 对话框随即打开。输入 FireAMP 设备处置服务的**主机 (Host)** 和**端口 (Port)** 并点击**检索 (Retrieve)**。 3. 系统即会检索证书。 4. 点击**导入 (Import)**。 （或点击**从剪贴板导入 [Import from Clipboard]**。从剪贴板粘贴 PEM，并点击**添加证书 [Add Certificate]**。）	

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
4.3	**FireAMP 集成管理：** 在 Threat Grid Face 门户 UI 中，从右上方菜单中选择**管理 FireAMP 集成 (Manage FireAMP Integration)**。“处置更新服务”(Disposition Update Service) 窗口随即打开。 输入 AMP 处置更新服务 URL（您可以在 FireAMP 设备上找到它：选择**集成 [Integrations] > Threat Grid > FireAMP 私有云详细信息 [FireAMP Private Cloud Details]**）。 输入您的**管理员用户名 (admin user name)** 和**密码 (password)**，并点击**配置 (Config)**。	

管理 THREAT GRID 组织和用户

安装在设备上的 Threat Grid 具有默认组织和管理员用户。一旦设备设置并且网络配置完成后，您可以创建更多的组织和用户帐户，这样人们就可以登录并开始提交恶意软件样本进行分析。

添加组织、用户和管理员可能需要在多个用户和组织中进行规划和协调，具体情况取决于您的组织。

创建新组织

用户始终与组织关联；在添加用户之前，您必须首先创建要添加用户的组织。

重要信息：一旦在此界面中创建组织后即无法将其删除，因此请谨慎安排此任务。

1. 请以管理员身份登录 Threat Grid 门户。
2. 点击位于左上角的**欢迎 (Welcome)** 下拉链接，并选择 **管理组织 (Manage Orgs)**。组织 (Organizations) 页面打开，列出设备上的所有组织。
3. 点击位于屏幕右上角的**添加组织 (Add Org)** 按钮。将打开属性 (Properties) 对话框。
4. 所有字段都是必填字段。

   名称 (Name)。添加一个组织名称（目前对名称没有大小限制）。

   行业 (Industry)。从行业 (Industry) 下拉菜单中选择行业类型。如果列表上的行业都不适用，则请将其设置为未知 (Unknown)，并与 Threat Grid 支持 (support@threatgrid.com) 联系请求添加选项。

   完成其他选项。

   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。许可证中的速率限制会应用到组织。

   设置默认的*用户*提交速率限制。您还可以对个别用户设置样本提交速率，如 Threat Grid 门户在线帮助的 *“使用 Threat Grid”*（从导航栏中选择帮助**帮助 [Help] > 使用 Threat Grid 在线帮助 [Using Threat Grid Online Help]**）中所述。

   速率限制基于滚动时间的 24 小时时间间隔，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。

   优先级 (Priority) 字段消失；现在请输入“50”。
5. 点击**创建**。现在创建了新的组织，并且在组织列表中可以看到。

管理用户

有关管理用户帐户（包括集成的思科 ESA/WSA 设备和其他设备的帐户）的说明和文档，请参阅 Threat Grid 门户 UI 在线帮助。从导航栏选择**帮助 (Help) > 使用 Threat Grid 在线帮助 (Using Threat Grid Online Help) > 管理用户 (Managing Users)**。

隐私和样本可见性

用于将样本提交到 Threat Grid 的隐私和样本可见性模型相对简单：除非样本被指定为专用，否则那些位于提交者组织以外的用户可以看到这些样本。一般来说，只有那些与提供样本的用户位于同一组织的用户才能看到专用样本。

如果提交敏感文档或存档类型进行分析，则隐私是一个尤为重要的考虑因素。当与搜索 API 结合时，那些具有 Threat Grid 访问权限的用户就可以相对容易地找到敏感材料。当将样本提交到本地 Threat Grid 设备而不是 Threat Grid 云时，这个问题就不再那么重要了，但 TGA 管理员仍然需要理解隐私和样本可见性。

Threat Grid 设备上的隐私和可见性

隐私和样本可见性模型是在 Threat Grid 设备上进行修改，在威胁由“CSA 集成”CSA 集成是指思科产品（例如 ESA/WSA 设备和其他设备或服务）通过 CSA API 集成（注册）到 Threat Grid 设备。

默认情况下，Threat Grid 设备上的所有样本提交都是公开的，可以由任何其他设备用户查看，包括 CSA 集成，无论他们属于哪个组织。

所有设备用户均可以查看所有其他用户所提交样本的全部详细信息。

非 CSA Threat Grid 用户可以向 Threat Grid 设备提交专用样本，在这种情况下仅提交者组织内的其他 Threat Grid 设备用户（包括 CSA 集成）可以查看样本。

下表使用以下术语说明 Threat Grid 设备上的隐私和样本可见性：

CSA 集成 CSA 集成是指通过 CSA API 在 Threat Grid 设备上注册的 ESA/WSA 设备和其他思科设备或服务。默认情况下，由 CSA 集成提交到 Threat Grid 设备的样本是公开的。

Threat Grid 用户 - 公共 由普通 Threat Grid 用户提交到 Threat Grid 设备的公共样本（即非 CSA 集成）。

例如，通过 Threat Grid 门户用户界面或通过使用 Threat Grid 本机 API 提交样本的设备管理员或恶意软件分析人员。

Threat Grid 用户 - 专用 由普通 Threat Grid 用户提交到 Threat Grid 设备的专用样本。

在这种情况下，专用样本对于提交者组织外部的设备上的所有其他用户均不可见。（样本将对提交者组织内的 CSA 集成可见。）

图 12 - Threat Grid 设备上的隐私和可视性

	由以下人员访问时样本的可视性：			
样本提交者：	来自同一组织的 Threat Grid 用户	来自不同组织的 Threat Grid 用户	来自同一组织的 CSA 集成	来自不同组织的 CSA 集成
Threat Grid 用户 - 公共	完全	完全	完全	完全
Threat Grid 用户 - 专用	完全	无	完全	无
CSA 集成（ESA/WSA 设备等） 默认情况下，所有提交到 Threat Grid 设备的 CSA 提交都是公共的	完全	完全	完全	完全

相同的基本隐私规则会应用到 Threat Grid 设备与 FireAMP 私有云的集成。

擦除设备

V1.4.4 将启用新的启动菜单选项，将允许您擦除 Threat Grid 设备的磁盘。

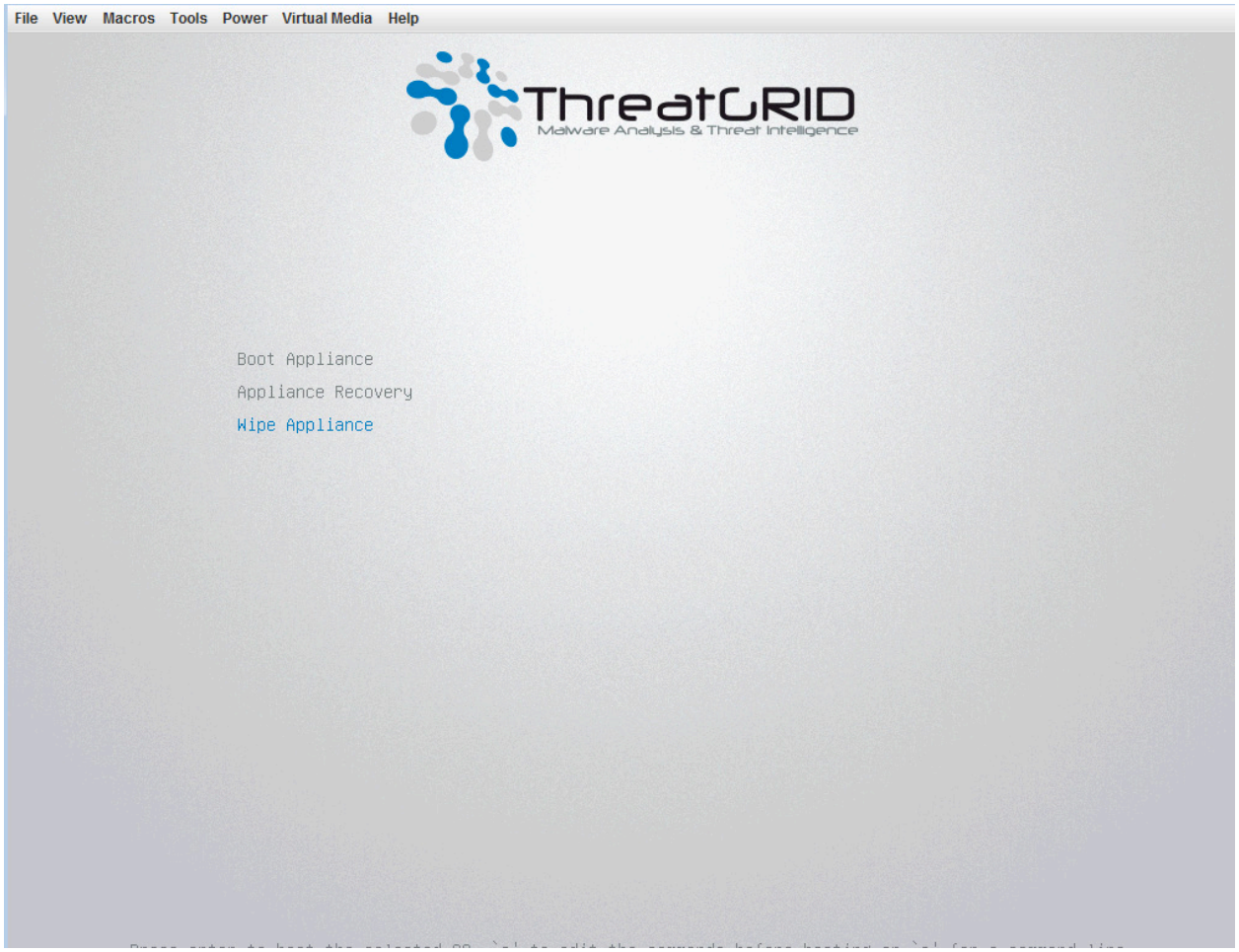
在停止使用设备或者将其返回给思科演示版本租借计划前，请使用擦除设备 (Wipe Appliance) 选项从设备删除所有数据。此过程有多种变体可用，某些过程执行其他通道，对使用高级技术进行数据检索的尝试提供安全防范。（请注意这些技术被视为对现代硬盘编码无效，因此即使最快的单通道擦除选项被视为安全和充分。）

重要信息：在执行此操作后，设备将不再运行，无需返回到思科进行重新镜像。

1. 重新启动设备。

   在启动期间，**设备将显示一个 4 秒的窗口**，在这里您可以选择**擦除设备 (Wipe Appliance)**：

图 13 - 擦除设备



2. 此选项需要以下用户名和密码：

   用户名： “wipe”

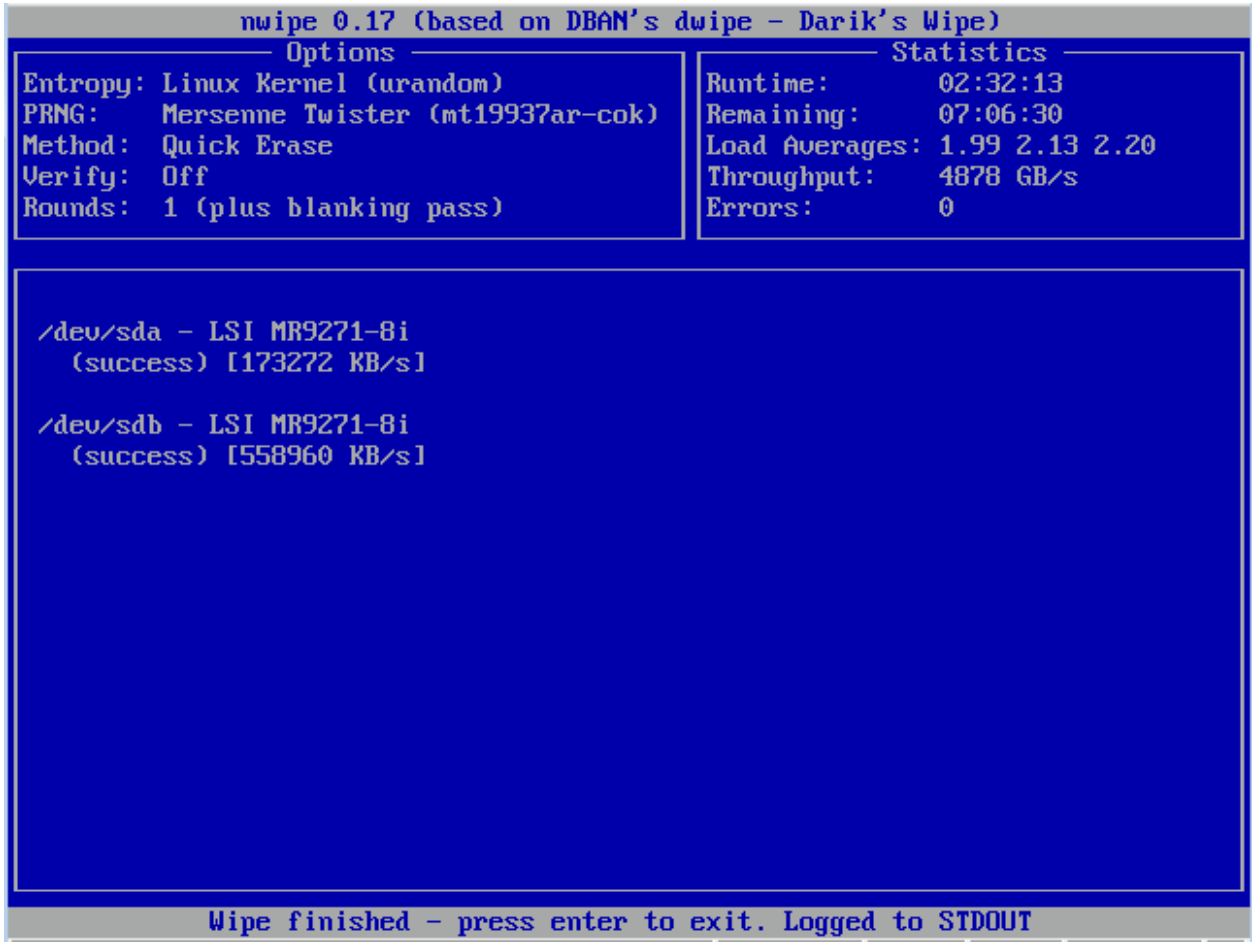
   密码： “I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION”

3. 接下来，选择一个擦除选项。请参阅“擦除选项”了解每个选项的大约运行时间。

图 14 - 擦除选项

4. 当擦除操作完成后，将显示擦除已完成 (**Wipe Finished**) 屏幕：

图 15 - 擦除已完成



5. 按 **Enter** 键退出。

擦除选项

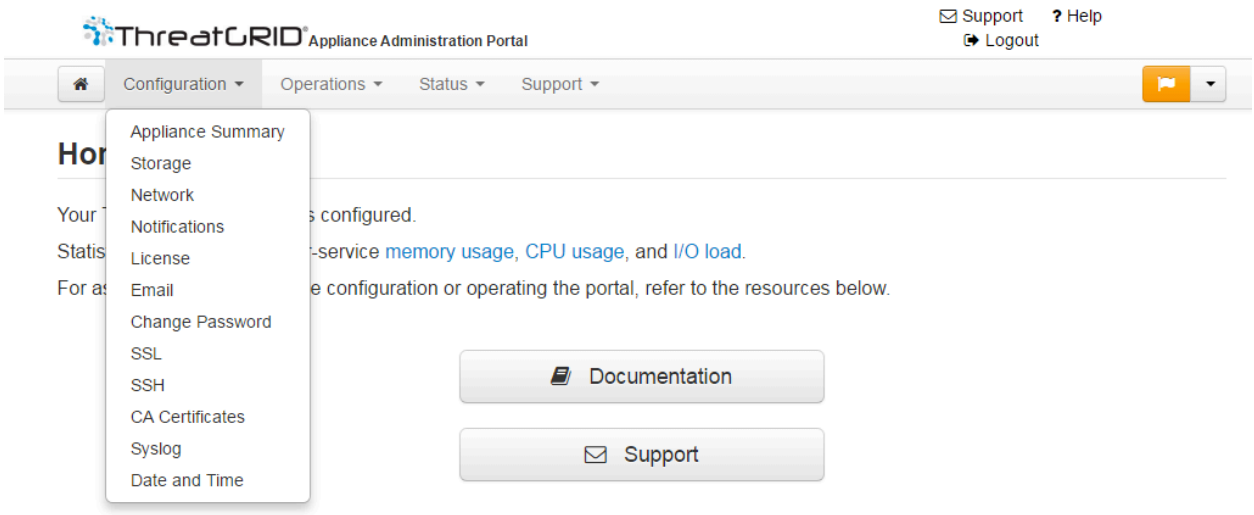
擦除选项	大约运行时间
擦除（快速：零磁盘）(Wipe (Fast: Zero Disks))	2.5 小时
擦除（3 通道 DOD 方法）(Wipe (3-pass DOD method))	16 小时
擦除（随机覆盖）(Wipe (Random Overwrite))	12 小时

附录 - OPADMIN 菜单

我们提供以下屏幕截图说明在 OpAdmin 内执行多种任务时可用的多个菜单选项：

配置 (Configuration) 菜单

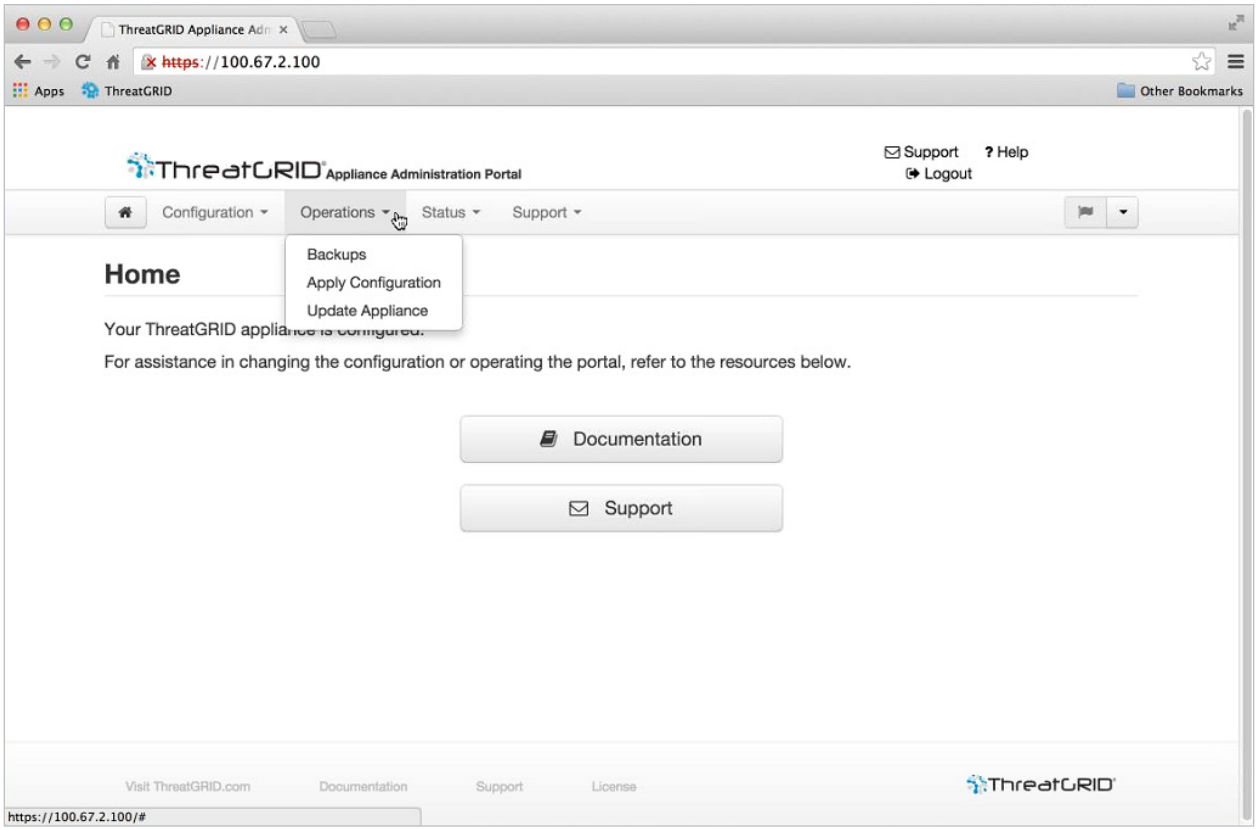
图 16 - OpAdmin 配置菜单



注意：如果您未来需要对您的 OpAdmin 配置设置进行更改，则必须从配置 (Configuration) 菜单访问这些设置以便进入编辑模式。

操作 (Operations) 菜单

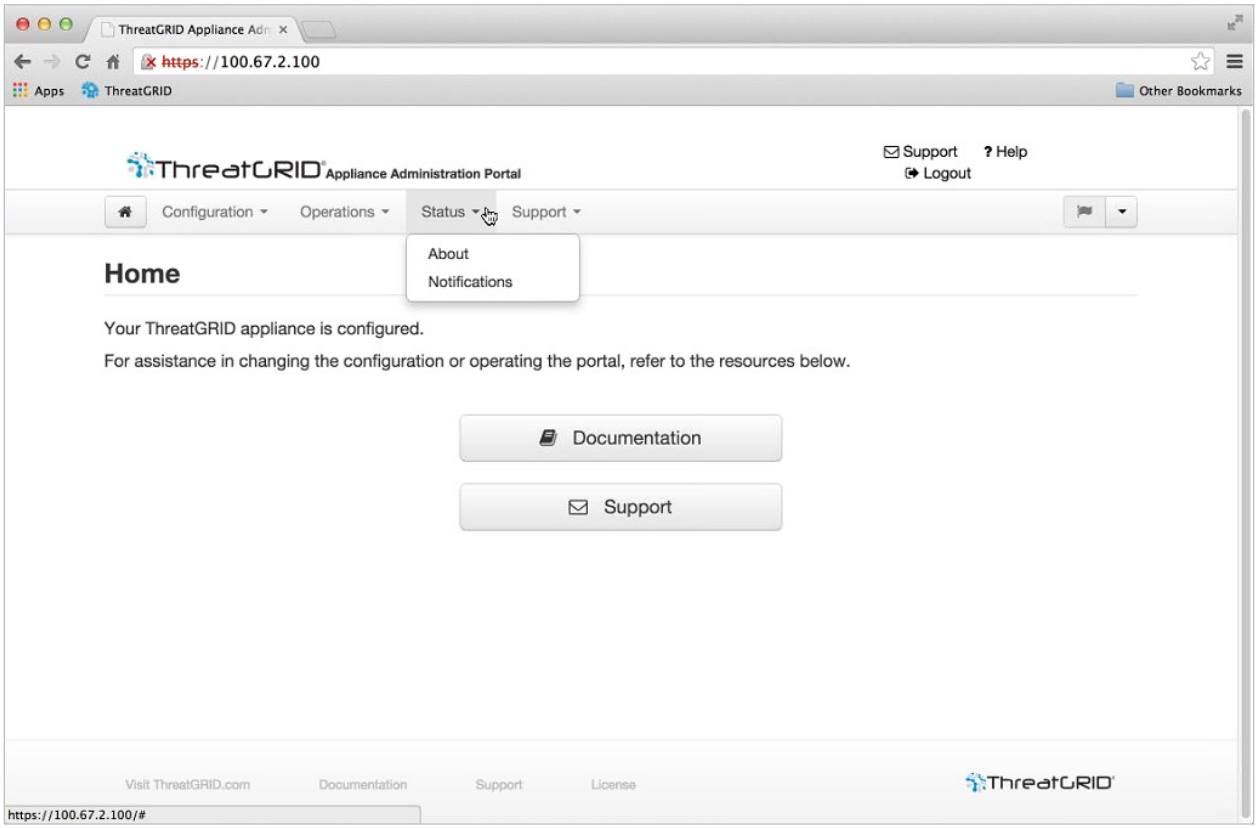
图 17 - OpAdmin 操作菜单



注意： 请选择**更新设备 (Update Appliance)** 来查看版本说明。

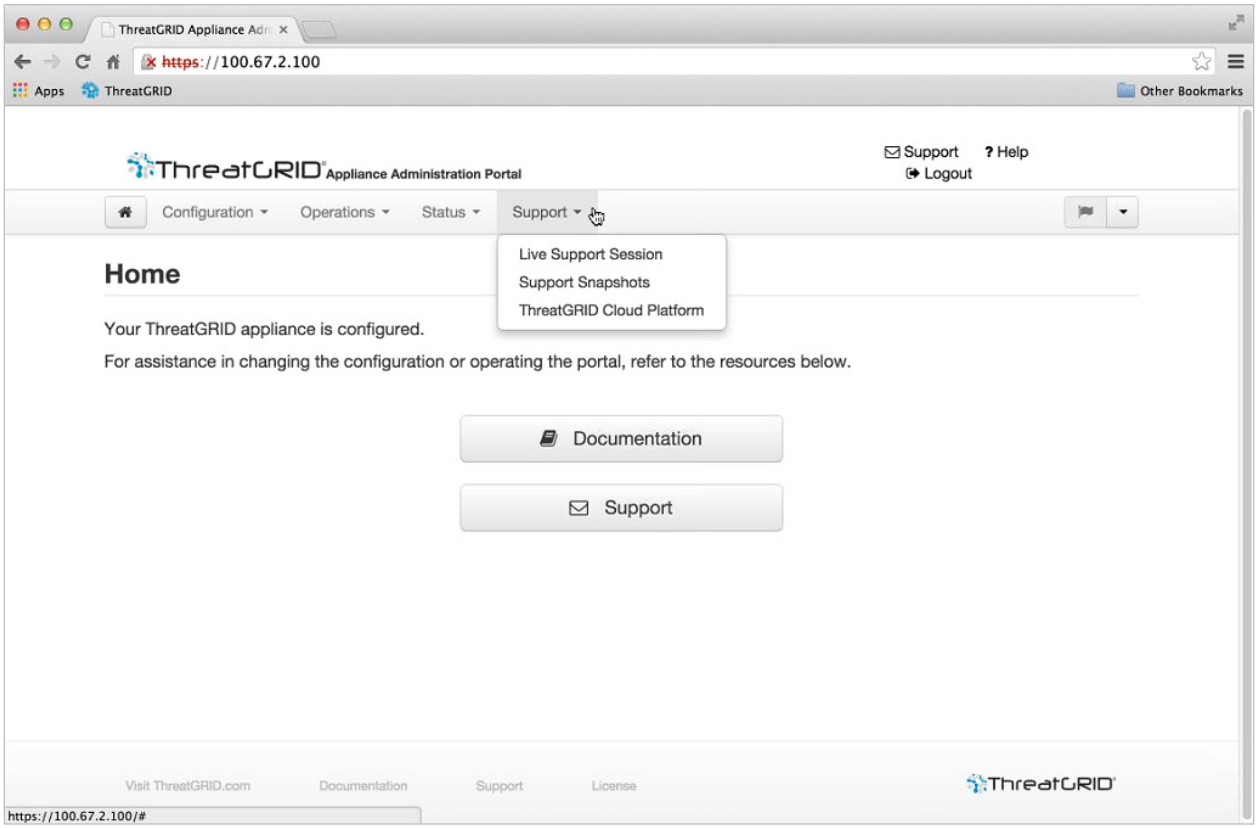
状态 (Status) 菜单

图 18 - OpAdmin 状态菜单



支持 (Support) 菜单

图 19 - OpAdmin 支持菜单



您可以通过此菜单访问到实时支持会话（支持模式）；请参阅支持部分了解详细信息。