Threat Grid 设备管理员指南

版本：2.2.4

更新日期：2017 年 7 月 10 日

思科系统公司 www.cisco.com

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上面所提及的供应商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。

封面照片：美国拱门国家公园游客中心高高的山脊上怒放的红葡萄酒杯仙人掌花。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。版权所有 © 2015 年 Mary C. Ecsedy。保留所有权利。已获得使用许可。

思科 Threat Grid 设备管理员指南
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

目录

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

目录

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

图片清单

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

引言

思科 Threat Grid 设备 (TGA) 是一个全面的 Threat Grid 恶意软件分析平台，它可以安装在独立的思科 UCS 服务器（UCS C220-M3 或 UCS C220 M4）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。

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

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 设备及面向终端的 AMP 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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

使用入门

思科 Threat Grid 设备是一个 Linux 服务器，在出厂前已预装所有必要的样本分析组件。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*》、版本说明的格式化版本、集成指南等）可在 Cisco.com 网站的如下内部资源页面获取：*Threat Grid 设备产品文档页面*。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*》是本文档的配套文档。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 > 操作 > 更新设备 > 版本说明

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 > 帮助 > 版本说明

Threat Grid 门户在线帮助和 API 文档

您可以从 Threat Grid 门户的帮助主页访问 Threat Grid 门户的*使用 Threat Grid* 在线帮助、API 文档和其他信息：

Threat Grid 门户用户界面 > 导航栏 > 帮助

系统将显示**帮助**主页，其中包含文档的链接。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

ESA/WSA 设备文档

有关如何将 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”。

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

- 《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

您可以在 *OpAdmin 配置许可证*页面管理 Threat Grid 许可证：

配置 > 许可证

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。

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。

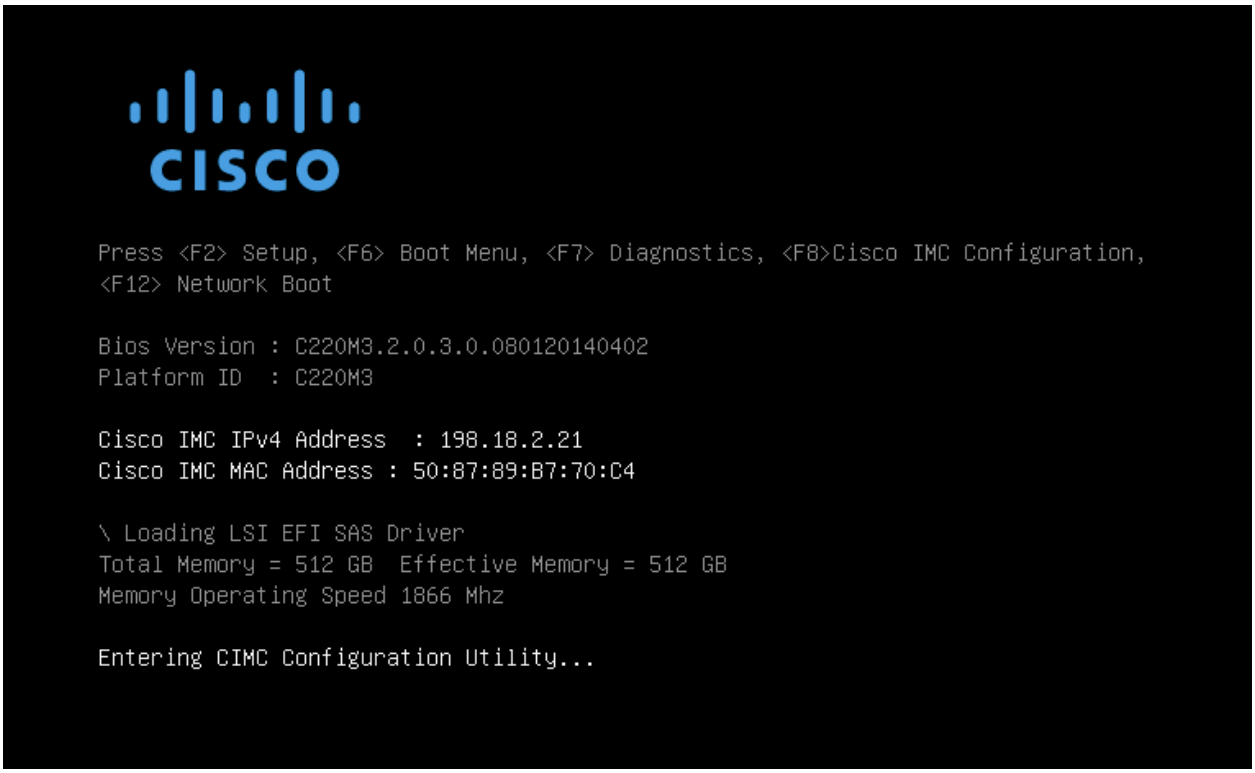
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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



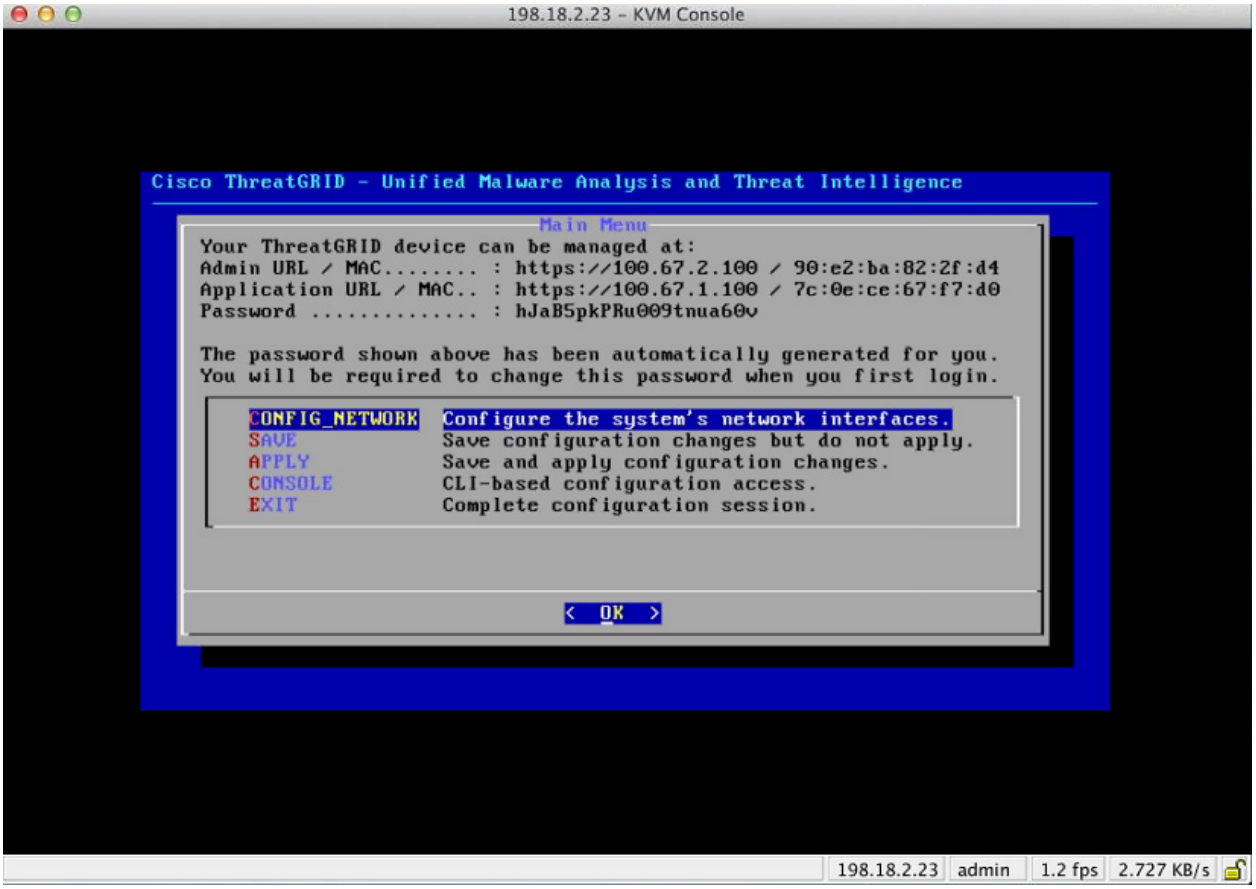
注意：如果您想要配置 CIMC 界面，请在内存检查完成后按 **F8**。

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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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。

注意：当有多名管理员时，可使用 LDAP 身份验证来登录 TGSH 对话和 OpAdmin。如果将设备配置为仅使用 LDAP 身份验证，那么在恢复模式下重置密码会将身份验证模式重新配置为允许使用系统密码登录。

如果丢失了管理员密码，无法登录到 OpAdmin，请完成以下步骤：

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

重新设置丢失的管理员密码

1. 重新启动设备。

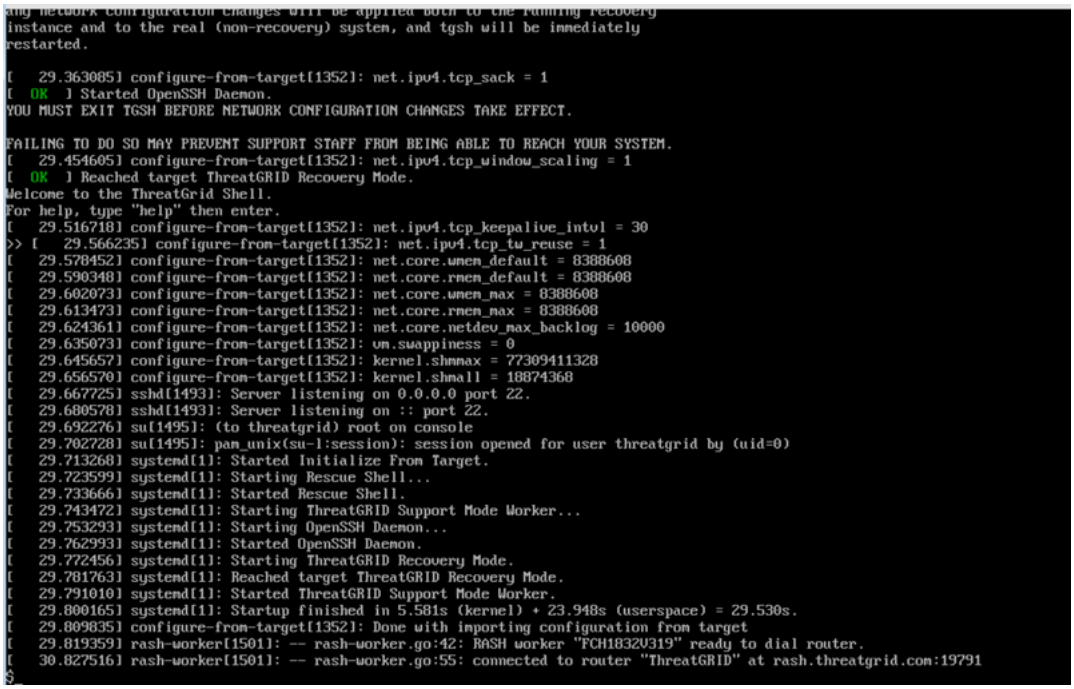
   在启动期间，系统会在一个短暂的时间里显示如下菜单，您可以在此期间选择“恢复模式”，如下所示：

图 3 - 启动菜单 - 恢复模式

系统将打开 Threat Grid Shell：

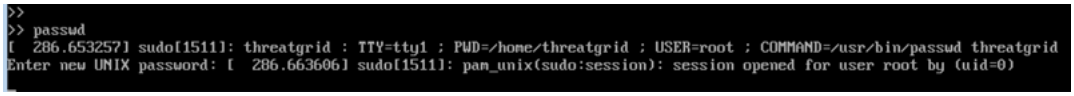
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

图 4 - 恢复模式下的 Threat Grid Shell



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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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低的版本，并且您希望安装更新，则必须先完成初始配置。请在完成所有设备配置之后再应用更新。

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。

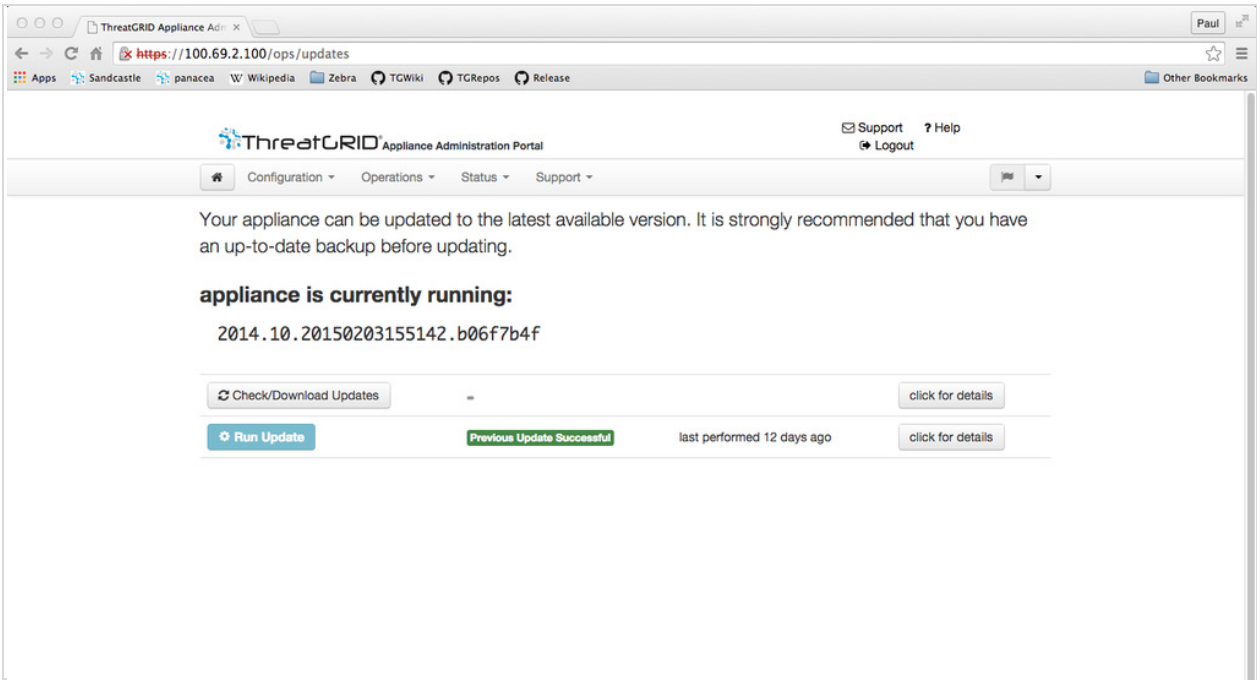
更新是不可逆的：在升级到最新版本后，您无法再将其恢复到先前版本。

要测试更新，请提交一个样本进行分析。

1. 从**操作**菜单中，选择**更新设备**。

   更新页面将打开，显示设备的当前版本：

图 6 – 设备版本号



本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

2. 点击**检查/下载更新**。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：下载过程可能需要一些时间：

   - 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. 更新下载完成后，点击**运行更新**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”页面上查看（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的对应关系：

内部版本号	版本	发布日期	说明
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；修复资源问题。
2016.05.20170308211223.c92516ee.rel	2.2mfg	2017 年 3 月 8 日	仅制造更改。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	存储迁移、修剪、Mask UI、多个处置更新。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

内部版本号	版本	发布日期	说明
2016.05.20170105200233.32f70432.rel	2.1.6	2017 年 1 月 5 日	增加 LDAP 身份验证。
2016.05.20161121134140.489f130d.rel	2.1.5	2016 年 11 月 21 日	ElasticSearch5；CSA 性能修复。
2016.05.20160905202824.f7792890.rel	2.1.4	2016 年 9 月 5 日	主要是制造上的更改。
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	2.1 更新的起点。您必须先升级到 2.0.4，然后才能更新为 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	
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 **注意：**此版本是版本 2.0 升级的起点。	2016 年 1 月 27 日	2.0.4 更新的起点。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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		
2014.10.20141125162s160+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		

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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*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 - 联系 Threat Grid

如需任何帮助，您可以通过以下多种方式请求 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。要打开思科支持案例管理器，请访问：https://mycase.cloudapps.cisco.com/case
- **电话。**思科联系信息：https://cisco.com/cisco/web/siteassets/contacts/index.html

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

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

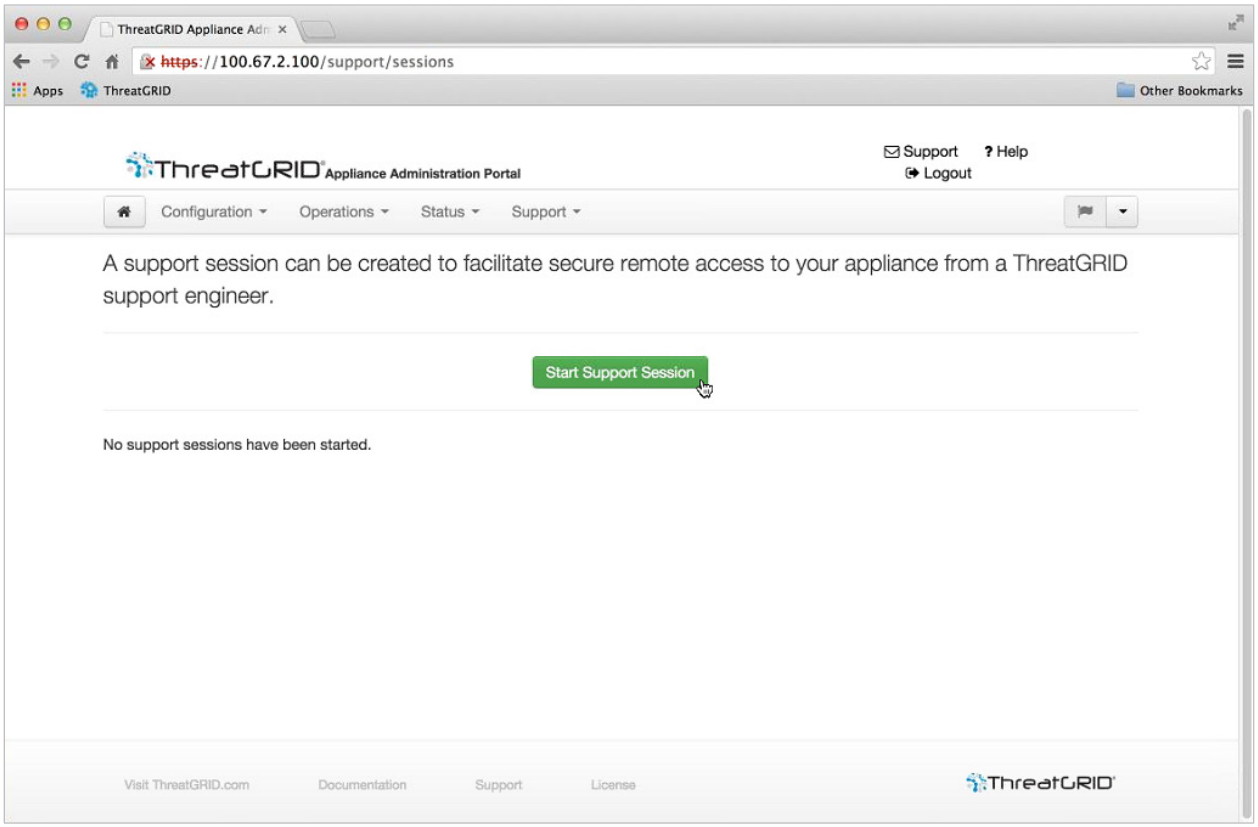
支持模式

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**。

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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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，帮助支持人员对任何问题进行故障排除。

1. 从**支持**菜单中，选择**支持快照**。
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，也可以按**提交**，使快照自动上传到 Threat Grid 快照服务器。

备份

在 OpAdmin 中，在“操作”>“备份”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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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。

您可以在 **TGSH 对话**和 **OpAdmin 门户**界面中管理 Threat Grid 设备配置。

Threat Grid 组织和用户帐户则通过 Threat Grid 门户 UI 进行管理（导航栏右上方的**欢迎**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*。

配置 TGSH 对话界面的操作

1. 登录 TGSH 对话。

   注意：如果您配置的是“仅 LDAP”身份验证，则只能使用 LDAP 登录 TGSH 对话。如果将身份验证模式设置为“系统密码或 LDAP”，则 TGSH 对话登录只允许系统登录。

2. 在 **TGSH 对话**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。

3. 根据需要进行更改。

   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. 将 Dirty 网络的 **DNS 名称**留空。

5. 更新网络设置后，按 Tab 键向下移动，并选择**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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

6. 选择**应用**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。

7. 点击**确定**。

   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“*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. 执行重新启动，等待系统显示启动菜单。该菜单只显示很短时间，因此请提前做好准备（请参阅上文“图 3 - 启动菜单 - 恢复模式”）。
2. 选择“恢复模式”。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：静态

   IP 地址：<CLEAN IP 地址>/<网络掩码>

   网关地址：<CLEAN 的网关>

   路由：<留为空白>

   对于最后一个问题，输入 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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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（包括面向终端的 AMP 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（面向终端的 AMP 私有云集成）
- LDAP 身份验证
- 第三方检测和增强服务（包括 ClamAV、OpenDNS、TitaniumCloud 和 VirusTotal）

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

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/

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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 > SSH

系统日志

除了可以将定期通知设置为通过邮件发送系统通知（在 OpAdmin 中的**配置 > 通知**下），您还可以配置一个远程系统日志服务器来接收系统日志消息和 Threat Grid 通知。

1. 在 OpAdmin 中，在**配置 > 系统日志**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. 点击**保存**，然后选中**验证**框执行 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）。

   如果不选中“验证”框，设备将接受任何名称（无论 DNS 是否有效）。
4. 点击**保存**。

编辑或删除：如果您需要更新系统日志 DNS，只需对其进行编辑或将其删除，然后点击**保存**。

为 OpAdmin 和 TGSH 对话配置 LDAP 身份验证

在版本 2.1.6 中，Threat Grid 设备增加了适用于 OpAdmin 登录和 TGSH 对话登录的 LDAP 身份验证和授权。过去，OpAdmin 和 TGSH 对话界面只有一个密码。如果您有多名设备管理员，他们之间必须共用该密码。这不仅非常不妥，而且很多思科客户都要求改善这种情况。为了解决这个问题，我们实施了 LDAP 身份验证。

现在，客户可以使用不同的凭证（在域控制器或 LDAP 服务器上进行管理）对多名设备管理员进行身份验证。LDAP 配置并非小事，因此我们建议谨慎采取此措施，务必在充分了解详情之后再进行设置。

身份验证模式包括：“仅系统密码”、“系统密码或 LDAP”和“仅 LDAP”。

系统提供三个 LDAP 协议选项：“LDAP”、“LDAPS”和“LDAP with STARTLS”。

请注意下列说明：

- 在设置 LDAP 时，为了避免意外将自己锁定在设备之外，需要采用“双”身份验证模式（**系统密码或 LDAP**）。请勿在初始配置时选择**仅 LDAP**；您必须先通过“双”模式确定其能够正常工作。完成初始配置后，您需要注销 OpAdmin，然后使用 LDAP 凭证重新登录，以便切换为**仅 LDAP**。
- 如果您配置的是“仅 LDAP”身份验证，则只能使用 LDAP 登录 TGSH 对话。如果将身份验证模式设置为“系统密码或 LDAP”，则 TGSH 对话登录只允许系统登录。
- 如果将设备配置为仅使用 LDAP 身份验证（**仅 LDAP**），则在恢复模式下重置密码会将身份验证模式重新配置为允许使用系统密码登录。

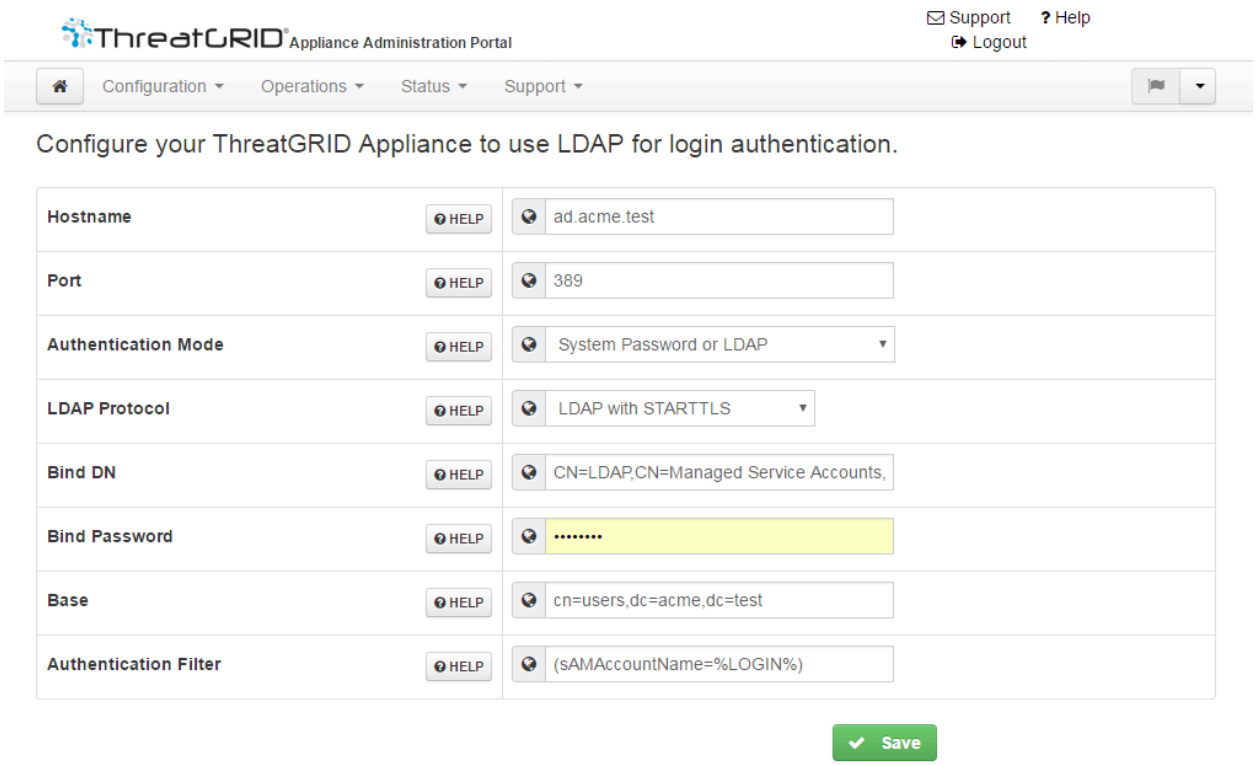
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

- 请务必设置身份验证过滤器，以限制成员身份。
- TGSH 对话和 OpAdmin 只有在**仅 LDAP** 模式下才需要使用 LDAP 凭证：如果配置的是“仅 LDAP”，TGSH 对话不会要求提供系统密码，而是会要求提供 LDAP 用户名/密码。
- 如果为身份验证配置的是**系统密码或 LDAP**，TGSH 对话仍将只会要求提供系统密码，而不会要求同时提供系统密码和 LDAP 凭证。
- LDAP 故障排除：如果 LDAP 出现故障，请在恢复模式下执行密码重置，以禁用 LDAP。
- 通过 SSH 访问 TGSH 对话：在“仅 LDAP”模式下通过 ssh 访问 tgsh-dialog 时，**除了需要 LDAP 凭证外**，还需提供系统密码或已配置的 SSH 密钥。
- LDAP 将 Clean 接口作为出站接口。

配置 LDAP 身份验证的步骤

1. 在 OpAdmin 中，依次选择**配置** > **LDAP**。系统将显示 LDAP 配置页面：

图 8 - LDAP 身份验证配置



本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

2. 填写各个字段。

   点击每个字段旁的**？（帮助）**按钮可获取详细说明和更多信息。

   再次提醒，首次配置 LDAP 身份验证时，必须选择“系统密码或 LDAP”，然后注销 OpAdmin，再使用 LDAP 凭证重新登录，以便将设置更改为**仅 LDAP**。

3. 点击**保存**。

现在，用户在登录 OpAdmin 或 TGSH 对话时，将看到以下内容：

图 9 – 仅 LDAP

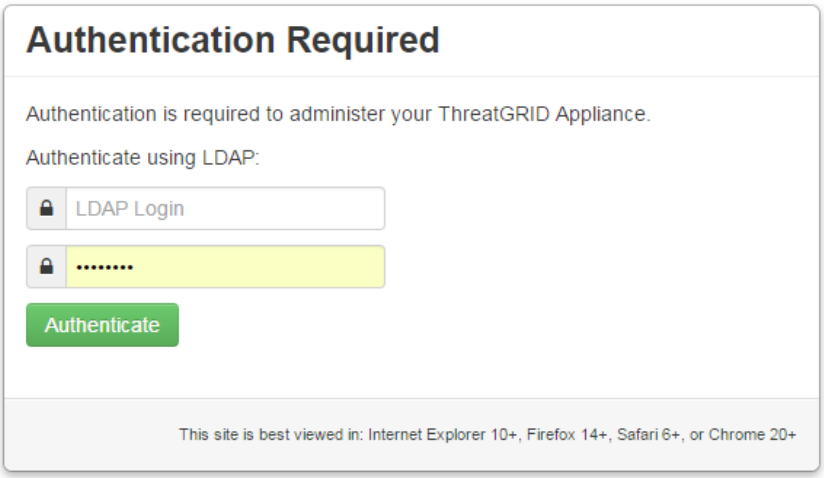
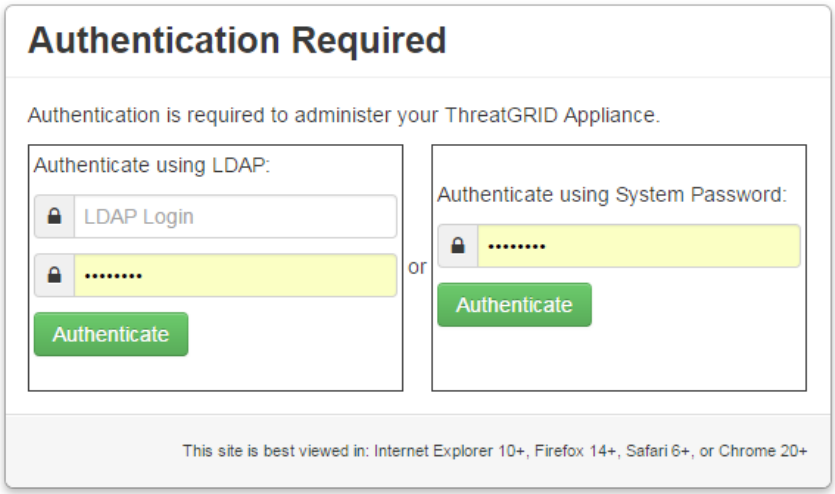


图 10 – 系统密码或 LDAP



本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

配置第三方检测和增强服务

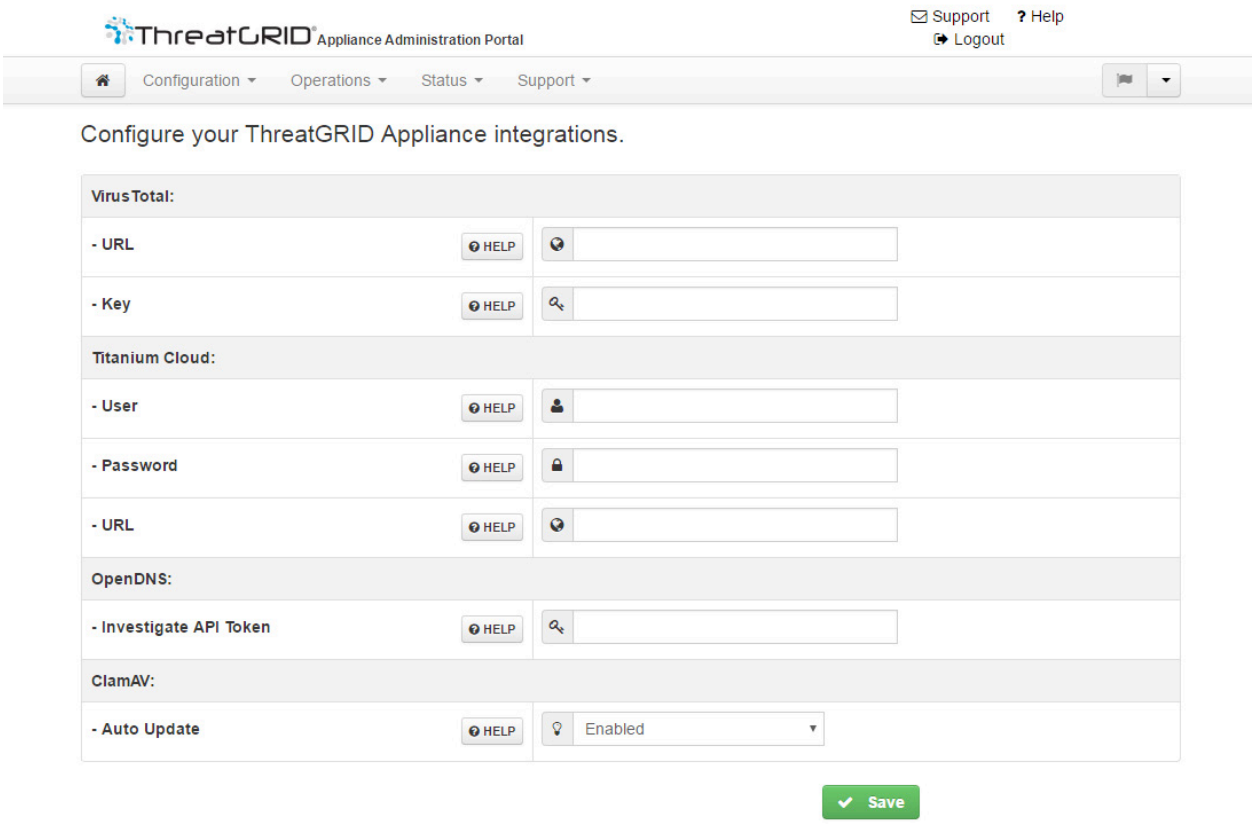
在版本 2.2 中，用户可以使用新的集成配置页面在设备上配置与多种第三方检测和增强服务（包括 OpenDNS、TitaniumCloud 和 VirusTotal）的集成。

在 **OpAdmin** 中，依次选择**配置 > 集成**打开集成配置页面：

输入所需的身份验证设置或其他值，然后点击**保存**。

OpenDNS：请注意，如果未配置 OpenDNS，则门户的分析报告中将不会显示*域*实体页面中的“whois”信息（在 UI 的 Mask 版本中）。

图 11 – 集成配置



ClamAV 签名默认每天自动更新

更新到版本 2.2 后，系统可以每天自动更新 ClamAV 签名。此功能默认启用，您可以通过新的“集成配置”页面（如上所示）将其禁用。

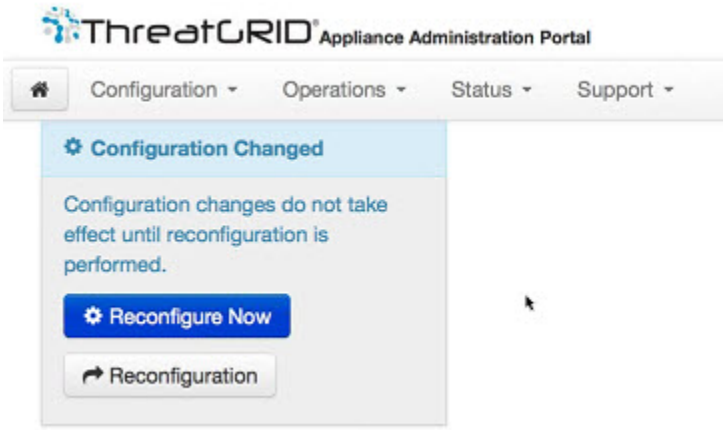
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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**。系统将显示**重新配置**对话框：

图 12 – 立即重新配置



2. 点击**重新配置**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。

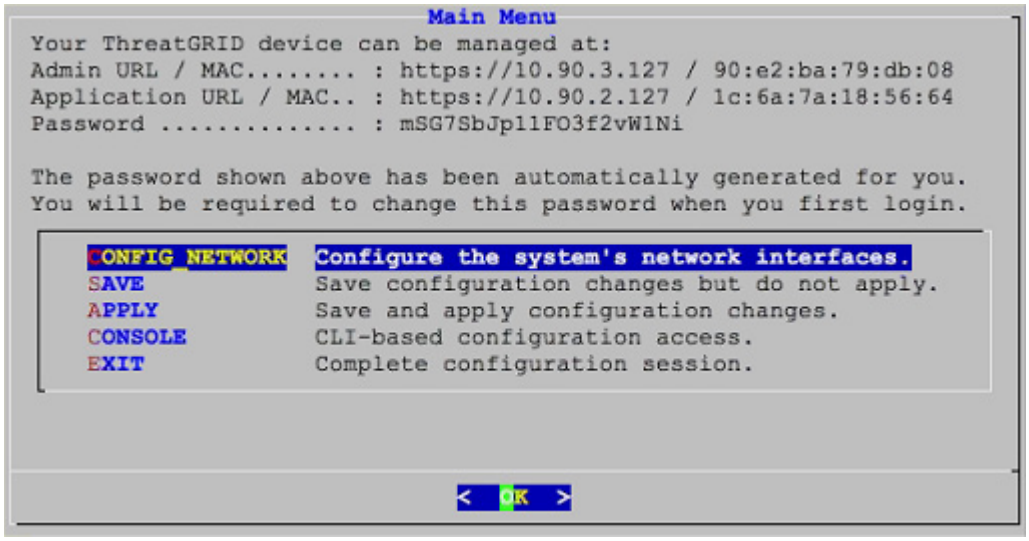
DHCP 的 IP 地址可能不会在您的设备启动后立即显示。请耐心等待！

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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 13 - TGSH 对话（连接到一个配置为使用 DHCP 的网络）



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

如果您计划永久使用 DHCP，则无需使用其他网络配置（除非您需要将“管理 IP”地址改为静态地址）。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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**。（尽管在“许可证”窗口中，**配置 > 网络**处于选中状态，但 DHCP 网络配置尚未完成。）

   系统将打开*网络配置*页面。

Clean

2. **IP 分配。**从下拉列表选择**静态**。
3. **IP 地址。**为 **CLEAN** 网络接口输入静态 IP 地址。
4. 根据需要填写**子网掩码**和**网关**。
5. 选中**验证 DNS 名称**，检查 DNS 是否已解析为您输入的 IP 地址。

Dirty

6. **IP 分配。**从下拉列表选择“静态”。
7. **IP 地址。**为 DIRTY 网络接口输入静态 IP 地址。
8. 根据需要填写**子网掩码**和**网关**。

Administration

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. 填写**主 DNS** 和**辅助 DNS** 服务器字段。

保存您的设置

10. 完成后，点击**下一步（应用配置）**保存您的网络配置设置。

SMTP/邮件

邮件配置可在*邮件*页面进行管理。

Time

NTP 服务器在*日期和时间*页面进行管理。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

应用 DHCP 配置

要应用您的 DHCP 配置设置，请点击**配置已更改**，然后点击**立即重新配置**。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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，提供以下信息有助于您完成设置 SSL 证书的步骤，从而支持 Threat Grid 设备与 ESA/WSA 设备、面向终端的 AMP 私有云和其他集成的连接。

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、面向终端的 AMP 私有云处置更新服务等）。
- **OpAdmin 门户**的 **Admin** 接口。

支持的 SSL/TLS 版本

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

支持客户提供的 CA 证书

从版本 2.0.3 起，Threat Grid 设备支持客户提供的 CA 证书，因此客户可以导入自己的受信任证书或 CA 证书。

SSL 证书 - 自签名的默认设置

Threat Grid 设备出厂时安装了一组自签名 SSL 证书和密钥。一组用于 **CLEAN** 接口，另一组用于 **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（公用名）是 *pandem*，有效期为 10 年。如果在配置期间向 Threat Grid 设备指定了不同的主机名，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 设备或者其他集成思科设备或服务预期的主机名匹配，因为很多客户端应用都需要 SSL 证书，其中证书内使用的 CN 必须与设备的主机名匹配。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

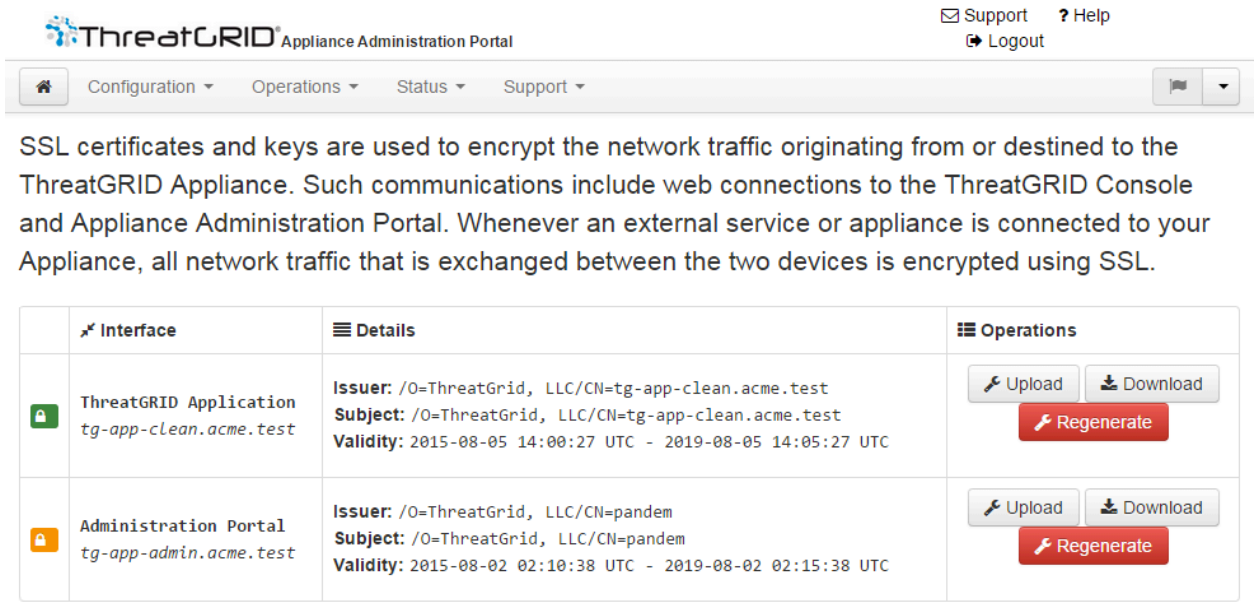
为入站连接配置 SSL 证书

其他思科产品（例如 ESA 和 WSA 设备以及面向终端的 AMP 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。

您可以在 **SSL 证书配置**页面上配置用于入站 SSL 连接的 Threat Grid 设备上的证书。**Clean** 接口和 **Admin** 接口的 SSL 证书可以独立配置。

依次选择 **OpAdmin > 配置 > SSL**。系统将打开“SSL 证书配置”页面：

图 14 - 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”页面中，彩色挂锁图标表示 Threat Grid 设备上 SSL 证书的状态。主机名必须与在 SSL 证书中使用的 CN（“公用名”）匹配。如果不匹配，则需要用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（“公用名”）匹配。
- 黄色挂锁图标是一个警告，表示 Admin 接口主机名与该 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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

替换 SSL 证书

由于各种原因，经常需要替换 SSL 证书。例如，证书到期或主机名更改。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。

在将 Threat Grid 设备与面向终端的 AMP 私有云集成在一起以使用其处置更新服务的情况下，需要安装面向终端的 AMP 私有云 SSL 证书，以便让 Threat Grid 设备能够信任连接。

有几种方式可以在 Threat Grid 设备上替换 SSL 证书。

- 重新生成新的 SSL 证书，该证书将使用 CN 的当前主机名。
- 下载 SSL 证书
- 上传新的 SSL 证书。这可以是商业或企业 SSL，或者您使用 OpenSSL 为自己生成的证书。
- 生成您自己的 SSL 证书 - 使用 OpenSSL 的示例

本文的后续各节将介绍这几种方式。

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，如下面的“生成您自己的 SSL 证书 - 使用 OpenSSL 的示例”一节所述。

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

在 **OpAdmin SSL 证书配置**页面上，点击**重新生成**。系统会在使用证书 CN 字段中的设备当前主机名的 Threat Grid 设备上生成新的自签名 SSL 证书。CN 验证挂锁图标为绿色。可以按下一节所述下载重新生成的证书（.cert 文件）并将其安装在集成设备上。

下载 SSL 证书

可以下载 Threat Grid SSL 证书，但不是密钥，然后将其安装在集成设备上，以便让设备能够信任来自 TG 设备的连接。此步骤您只需要 .cert 文件。

1. 在“OpAdmin SSL 证书配置”页面上，点击您希望获取的证书旁边的**下载。**系统将开始下载 SSL 证书。
2. 接着，像安装任何其他 SSL 证书一样，在 ESA/WSA 设备、FireAMP 公共云或其他集成思科产品上安装下载的 SSL 证书。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

上传 SSL 证书

如果您的组织内已拥有商业或公司 SSL 证书，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

另一种备选方法是手动生成您自己的 SSL 证书，例如在您的现场尚无 SSL 证书基础设施并且您无法通过其他方式获得证书时。然后，您可以按上述方法上传该证书。

以下示例说明为“Acme Company”生成新的自签名 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名证书而不是像通常那样生成证书签名请求，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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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 设备的主机名（我们的示例中为“tgapp”）以及附加到末尾的关联域名（“acmeco.com”）。

重要提示：您至少需要更改公用名，以匹配 Threat Grid 设备 CLEAN 接口的 FQDN。

新的 SSL 证书成功生成后，使用 SSL 页面的**上传**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）。

为出站连接配置 SSL 证书

Threat Grid 设备 2.0.3 版包含支持与面向终端的 AMP 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。如果由于 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（例如面向终端的 AMP 私有云）的主机名，则可以在 OpAdmin 中配置使用 Clean 接口的独立 DNS 服务器。

在 **OpAdmin** 中，依次选择**配置 > 网络**，再为 Dirty 和 Clean 网络填写 DNS 字段，然后点击**保存**。

CA 证书管理

版本 2.0.3 版的新增功能之一即面向*出站* SSL 连接的 CA 证书管理 Truststore 新页面，如此 TGA 便可信任面向终端的 AMP 私有云会向其发送有关已分析样本被视为恶意的通知。

在 **OpAdmin** 中，依次选择**配置 > CA 证书**。选择：

1. **从主机导入。**从服务器检索证书。系统将打开“从服务器检索证书”对话框。
2. 输入面向终端的 AMP 私有云的**主机**和**端口**，然后点击**检索**。系统将检索证书。

或

从剪贴板导入。从剪贴板粘贴 PEM，然后点击**添加证书**。

3. 点击**导入**。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

安全状态更新服务管理

此任务在 Threat Grid 门户用户界面内执行。

1. 从**我的帐户**下拉列表中选择**管理 FireAMP 集成**。系统将打开“处置更新服务”页面。
2. 输入 FireAMP 配置门户提供的**面向终端的 AMP 私有云 URL**、**管理员用户名**和**密码**，然后点击**配置**。

有关面向终端的 AMP 私有云设备集成的详细信息，请参阅后文中的将 Threat Grid 设备连接到思科。

将 ESA/WSA 设备连接到 Threat Grid 设备

其他思科产品（如 ESA/WSA 和其他设备、装置、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。

“CSA 集成”： ESA/WSA 设备与 Threat Grid 设备之间的集成通过思科沙盒 API（“CSA API”）实现，因此通常称为“CSA 集成”。

集成的 ESA/WSA 设备必须向 Threat Grid 设备注册后才能提交样本以供分析。ESA/WSA 管理员必须首先根据情况为其设备和网络环境设置 SSL 证书连接，然后才能向 Threat Grid 设备注册集成的 ESA/WSA 设备。

本部分介绍设置集成的 ESA/WSA 设备和其他思科产品以与 Threat Grid 设备通信所需执行的步骤。

到 ESA/WSA 文档的链接

有关 *“启用和配置文件信誉和分析服务”* 的说明，请参阅 ESA/WSA 的在线帮助或用户指南（在这些指南中，Threat Grid 设备通常称为“分析服务”或“私有云文件分析服务器”。）

- 《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

集成过程概述

准备工作： 本部分概述在 ESA/WSA 设备或其他 CSA 集成（入站）与 Threat Grid 设备之间建立连接的步骤。

本部分后面的表中包含每个步骤的更多详细说明。

Threat Grid 设备 SSL 证书 SAN 或 CN 必须与其当前主机名和 ESA/WSA 预期匹配：

Threat Grid 设备 SSL 证书 SAN（“使用者备用名称”- 如已定义）或 CN（“公用名”）需要与主机名和 ESA/WSA 预期匹配：要想与集成的 ESA/WSA 设备成功连接，此名称必须是集成的 ESA/WSA 设备用来标识 Threat Grid 设备所用的同一主机名。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

根据您的要求，您可能需要在 Threat Grid 设备上重新生成自签名的 SSL 证书，以便设备在 SAN/CN 字段中使用当前主机名，然后将其下载到您的工作环境，再上传并安装到集成的 ESA/WSA 设备中。

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 TGA SSL 证书。

有关详细说明，请参阅上文为入站连接配置 SSL 证书部分。

验证连接：

完成 SSL 证书设置后，下一步是验证 ESA/WSA 设备能否与 Threat Grid 设备通信。

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。（请参阅以上链接。）

完成 ESA/WSA 文件分析配置：

启用文件分析安全服务，并配置高级设置。

向 Threat Grid 设备注册思科 ESA/WSA/其他设备：

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。

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。如下一部分所述，必须由一名管理员激活该新设备用户帐户。

在 Threat Grid 设备上激活新 ESA/WSA 帐户：

当 ESA/WSA 设备或其他集成连接并向 Threat Grid 设备自行注册时，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”。与其他 Threat Grid 用户一样，必须由一名 Threat Grid 设备管理员手动激活该设备用户帐户，然后才能使用它来提交恶意软件样本以进行分析。

ESA/WSA 集成过程步骤

从 Threat Grid 设备的角度看，此连接是*传入*连接。

此集成使用 CSA API。

有关必须在此侧执行的任务的更多详细信息，请参阅 ESA 和 WSA 用户指南。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

步骤	Threat Grid 设备（“TGA”）	ESA/WSA/其他 CSA API 集成
1	如常设置和配置 Threat Grid 设备（“TGA”）（即尚未集成）。 检查更新。如果找到更新，则进行安装。	
2		如常设置和配置 ESA/WSA 设备（即尚未集成）。
3	**TGA SSL 证书 SAN 或 CN 必须与其当前主机名和 ESA/WSA 预期匹配** 如果要部署自签名 SSL 证书： 生成新的 SSL 证书（在“Threat Grid 应用”- Clean 接口上），以根据需要替换默认证书，然后将其下载并安装到 ESA/WSA 设备中。（TGA SSL 证书已在上文的“SSL 证书和 THREAT GRID 设备”部分作过介绍。） 请务必生成一个将 Threat Grid 设备的主机名作为 SAN 或 CN 的证书。来自 Threat Grid 设备的默认证书不起作用。 请使用主机名，而不要使用 IP 地址。	
4		**验证连接** 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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

步骤	Threat Grid 设备（“TGA”）	ESA/WSA/其他 CSA API 集成
5		**为 TG 设备集成配置 ESA/WSA 设备：** 有关完整的说明，请参阅 ESA/WSA 指南。以下步骤是针对 ESA 的步骤，因为 ESA 是目前最常见的集成类型 1. 依次选择**安全服务** > **文件信誉和分析**。 2. 点击**启用**。 3. 点击**编辑全局设置**。 默认情况下会启用文件分析。如果不取消选中**启用文件分析**，则在下次提交后将激活文件分析功能密钥。 4. 在**文件分析**部分中，选择要发送至云以供分析的文件类型。 5. 根据需要，按照 ESA 或 WSA 指南配置**文件分析的高级设置**： **文件分析服务器 URL：** 选择**私有云**。 **服务器：** 本地思科 Threat Grid 设备的 **URL**。 对于此值以及证书，请使用主机名，而不要使用 IP 地址。 **SSL 证书：** 上传从本地思科 Threat Grid 设备生成的自签名证书。 使用最近上传的自签名证书。无法访问在最新证书之前上传的证书；如有需要，请再次上传所需的证书。 6. 提交并确认更改。 请记录出现在页面底部的**文件分析客户端 ID**。此 ID 标识第 7 步中需要激活的“用户”。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

步骤	Threat Grid 设备（“TGA”）	ESA/WSA/其他 CSA API 集成
		向 Threat Grid 设备注册是自动操作 当您提交用于文件分析的配置时，系统将自动向 Threat Grid 设备注册邮件安全设备或 Web 安全设备。但是，您必须按照下文第 7 步中所述激活该注册。
7	**在 Threat Grid 设备上激活新设备用户帐户** 1. 请以管理员身份登录 Threat Grid 门户用户界面。 2. 从导航栏**欢迎**菜单中，选择**管理用户**。系统将打开 **Threat Grid 用户**页面。 3. 打开设备用户帐户的**用户详细信息**页面（可能需要使用“搜索”功能来查找）。 用户状态当前为“已停用”。 4. 点击**重新激活用户**。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**进行确认。	

ESA/WSA 或其他集成设备现在可以与 Threat Grid 设备连接。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

将 Threat Grid 设备连接到思科面向终端的 AMP 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面向终端的 AMP 私有云集成设置任务，尤其是当您在设置新设备的情况下。如果集成的是已设置和配置的设备，则顺序并不重要。

从 Threat Grid 设备的角度看，此连接是传出连接。此集成不使用 CSA API（“思科沙盒 API”）。

有关必须在另一端执行的任务的详细信息，请参阅面向终端的 AMP 私有云文档。

步骤	Threat Grid 设备（“TGA”）	面向终端的 AMP 私有云
1	如常设置和配置 Threat Grid 设备（“TGA”）（即尚未集成）。 检查更新。如果找到更新，则进行安装。	
2		如常设置和配置面向终端的 AMP 私有云（即尚未集成）。
3		**为 TGA 集成配置面向终端的 AMP 私有云：** 依次选择**集成 > Threat Grid** 并转到**连接到 Threat Grid** 部分。 要完成与 Threat Grid 设备的连接，您必须信任该设备。您需要其 DNS 主机名、SSL 证书和 API 密钥。 转至 TGA 列中的步骤 3.1 以找出此信息。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

步骤	Threat Grid 设备（“TGA”）	面向终端的 AMP 私有云
3.1	**SSL 证书：** 在 Threat Grid 设备 OpAdmin 界面中，依次选择**配置 > SSL** 重新生成新的 SSL 证书（在“Threat Grid 应用”- Clean 接口上），以根据需要替换默认证书，然后将其下载并安装到面向终端的 AMP 私有云设备中。（TGA SSL 证书已在“SSL 证书和 THREAT GRID 设备”部分作过介绍。） **主机名** 依次选择**配置 > 主机名** **API 密钥**： API 密钥可以在 Threat Grid Face 门户 UI 中用于集成的帐户的**用户详细信息**页面中找到： 1. 转到 **Threat Grid 门户 UI**。 2. 从右上方“欢迎”菜单（位于导航栏的右上角）中，选择**管理用户**。 3. 导航（如果需要可使用“搜索”）至集成的用户帐户的**用户详细信息**页面，并复制 **API 密钥**。注意，此操作不需要“admin”用户，但可以是在 Threat Grid 设备上专为此目的创建的其他用户。	

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

步骤	Threat Grid 设备（“TGA”）	面向终端的 AMP 私有云
3.2		完成**连接到 Threat Grid** 字段： 1. 输入 TGA 主机名 2. 输入即将用于集成的帐户的 Threat Grid API 密钥。 3. 选择 TGA SSL 证书文件。 4. 点击“保存配置”。 5. 点击“测试连接”。 6. 连接测试通过后，您将需要在面向终端的 AMP 私有云上运行“重新配置”以应用更改。 从技术上讲，这将允许 AMP 与 Threat Grid 设备通信，并且现在您可以向 TG 提交样本。但是，您必须完成余下的步骤来设置安全状态更新服务，以便向 TGA 报告处理结果。 （有关详细信息，请参阅面向终端的 AMP 私有云的用户文档。）
4	**设置安全状态更新服务** 以下步骤描述如何设置安全状态更新服务	

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

步骤	Threat Grid 设备（“TGA”）	面向终端的 AMP 私有云
4.1	**配置 DNS（如果需要）：** Clean 接口用于 FireAMP 集成。但是默认情况下，DNS 使用 Dirty 接口。如果在 Dirty 接口上无法解析面向终端的 AMP 私有云主机名，则可以在 OpAdmin 中配置一个使用 Clean 接口的独立 DNS 服务器。 在 OpAdmin 中，依次选择**配置> 网络**，再为 **Dirty** 和 **Clean** 网络填写 DNS 字段，然后点击**保存**。	
4.2	**CA 证书管理：** 下一步是将面向终端的 AMP 私有云 SSL 证书下载或复制/粘贴到 Threat Grid 设备，以便于它信任集成设备： 1. 在 OpAdmin 中，依次选择**配置 > CA 证书**。您可以选择一个 SSL 证书，以便从面向终端的 AMP 私有云主机导入或从剪贴板导入。 2. 选择要导入的证书并点击**从主机导入**。系统将打开**从服务器检索证书**对话框。输入 FireAMP 设备处置服务的**主机**和**端口**并点击**检索**。 3. 系统将检索证书。 4. 点击**导入**。 （或点击**从剪贴板导入**。从剪贴板粘贴 PEM，然后点击**添加证书**。）	

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

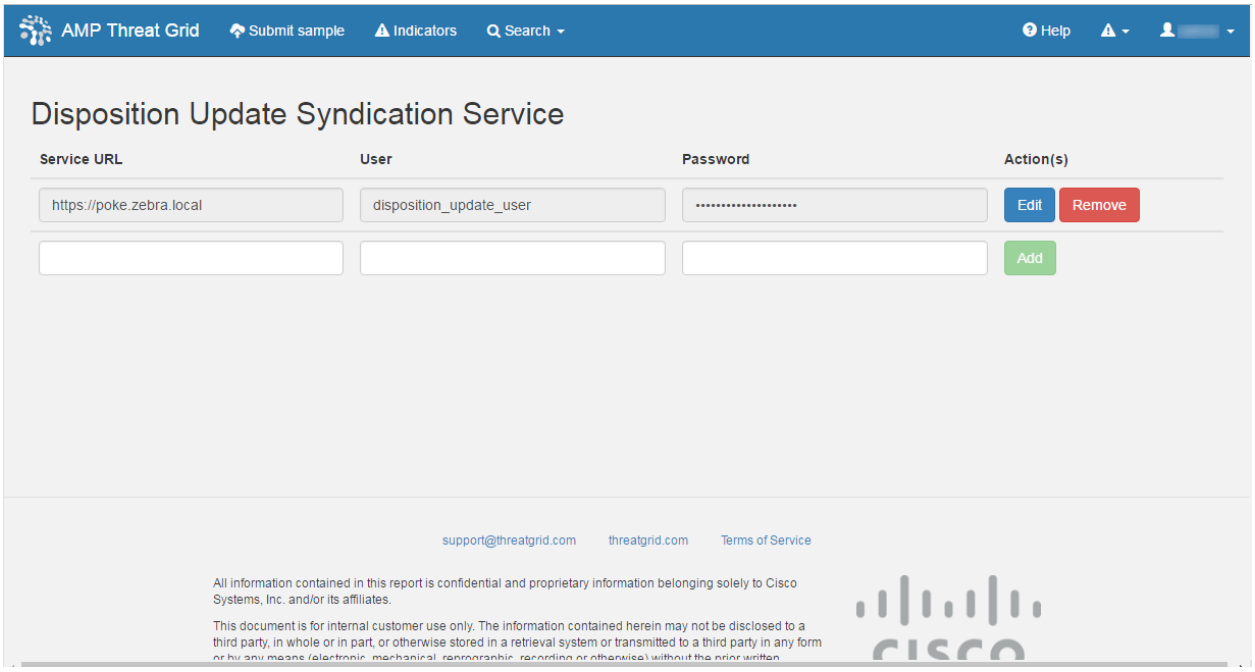
步骤	Threat Grid 设备（“TGA”）	面向终端的 AMP 私有云
4.3	**FireAMP 集成管理：** 在 Threat Grid Face 门户 UI 中，从右上方菜单中选择**管理 FireAMP 集成**。系统将打开“处置更新整合服务”窗口（如下所示）。 输入 AMP 处置更新服务 URL（您可以在 FireAMP 设备上找到它：依次选择**集成 > Threat Grid > 面向终端的 AMP 私有云详细信息**）。 输入您的**管理员用户名**和**密码**，并点击**配置**。	

管理处置更新整合服务

版本 2.2 中增加了为处置更新通知配置多个 URL 的支持（有时也称为“多 POKE”）。

可以通过新的“处置更新整合服务”页面添加、编辑和删除 URL：

图 15 – 处置更新整合服务页面



本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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**下拉链接，并选择**管理组织**。“组织”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**按钮。系统将打开“属性”对话框。
4. 所有字段均为必填字段。

   名称。添加一个组织名称（目前对名称没有大小限制）。

   行业。从“行业”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”，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”（从导航栏中依次选择“帮助”>“使用 Threat Grid 在线帮助”）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。从导航栏依次选择**帮助 > 使用 Threat Grid 在线帮助 > 管理用户**。

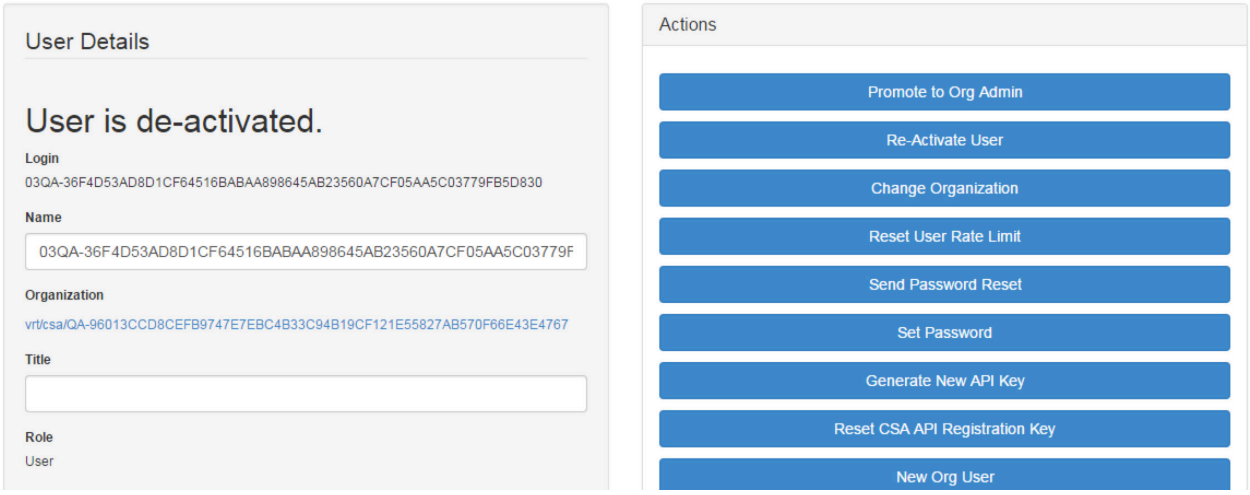
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

在 Threat Grid 设备上激活新设备用户帐户

当 ESA/WSA 设备或其他 CSA（“思科沙盒 API”）集成连接 Threat Grid 设备并向其注册时，系统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”。与其他 Threat Grid 用户一样，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 门户用户界面。
1. 从导航栏**欢迎**菜单中，选择**管理用户**。系统将打开 **Threat Grid 用户**页面。
2. 打开设备用户帐户的**用户详细信息**页面（可能需要使用“搜索”功能来查找）。用户状态当前为“已停用”：

图 16 - 用户详细信息页面 > 重新激活用户



3. 点击**重新激活用户**。会打开一个对话框要求您确认。
4. 在对话框中点击**重新激活**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。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

隐私和样本可见性

向 Threat Grid 设备提交样本进行分析时，需要考虑的一个重要问题是样本内容的隐私。如果提交敏感的文档或存档类型进行分析，则尤其需要考虑隐私问题，因为对那些具有 Threat Grid 设备访问权限的人而言，找到敏感材料会相对容易，特别是在使用搜索 API 的情况下。

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，否则提交者组织以外的用户将会看到这些样本。只有与提供样本的用户属于同一组织的 Threat Grid 用户才能看到*专用*样本。

集成的隐私和可见性

隐私和样本可见性模型在用于“集成”提交的样本的 Threat Grid 设备上进行修改。集成是指思科产品（例如 ESA/WSA 设备）与其他设备或第三方服务（您可能见过“CSA 集成”一词，它指通过思科沙盒 API 与 Threat Grid 设备集成 [即已注册] 的 ESA/WSA 及其他思科设备和其他服务）的集成。

默认情况下，Threat Grid 设备上的所有样本提交都是公开的，可供任何其他设备用户查看，包括集成设备用户（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。

Threat Grid 用户还可以向 Threat Grid 设备提交专用样本，只有与同一提交者位于相同组织的其他 Threat Grid 设备用户（包括集成设备用户）才能看到这些样本。

下表说明 Threat Grid 设备上的隐私和样本可见性模型：

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

图 17 - Threat Grid 设备上的隐私和可见性

	公开提交（默认）	私密提交	集成提交（默认为“公开”）
来自同一组织的用户	✔	✔	✔
来自其他组织的用户	✔	✖	✔
来自同一组织的集成	✔	✔	✔
来自其他组织的集成	✔	✖	✔

绿色复选标记表示用户对样本和分析结果具有完全访问权限。

红色“X”表示用户对样本或分析结果无权访问。

Threat Grid 设备与面向终端的 AMP 私有云的集成适用相同的基本隐私规则。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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。

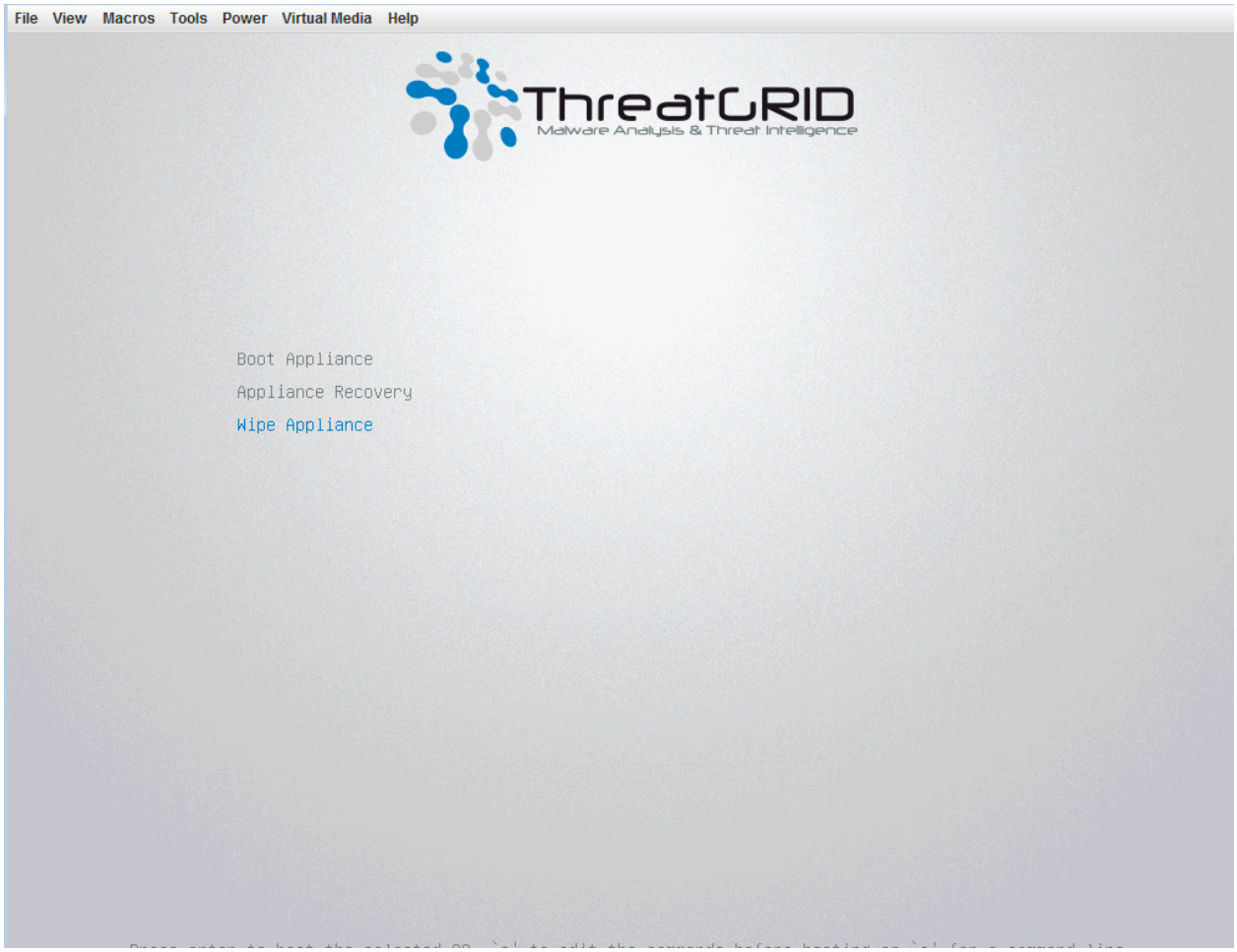
在停止使用设备或者将其返回给思科演示版本租借计划前，请使用“擦除设备”选项从设备删除所有数据。此过程有多种变体可用，某些过程执行其他通道，对使用高级技术进行数据检索的尝试提供安全防范。（请注意这些技术被视为对现代硬盘编码无效，因此即使最快的单通道擦除选项被视为安全和充分。）

重要信息：请注意，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映像。

1. 重新启动设备。

   在启动期间，设备将显示一个 4 秒钟的窗口，在这里您可以选择“擦除设备”：

图 18 - 擦除设备



本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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"

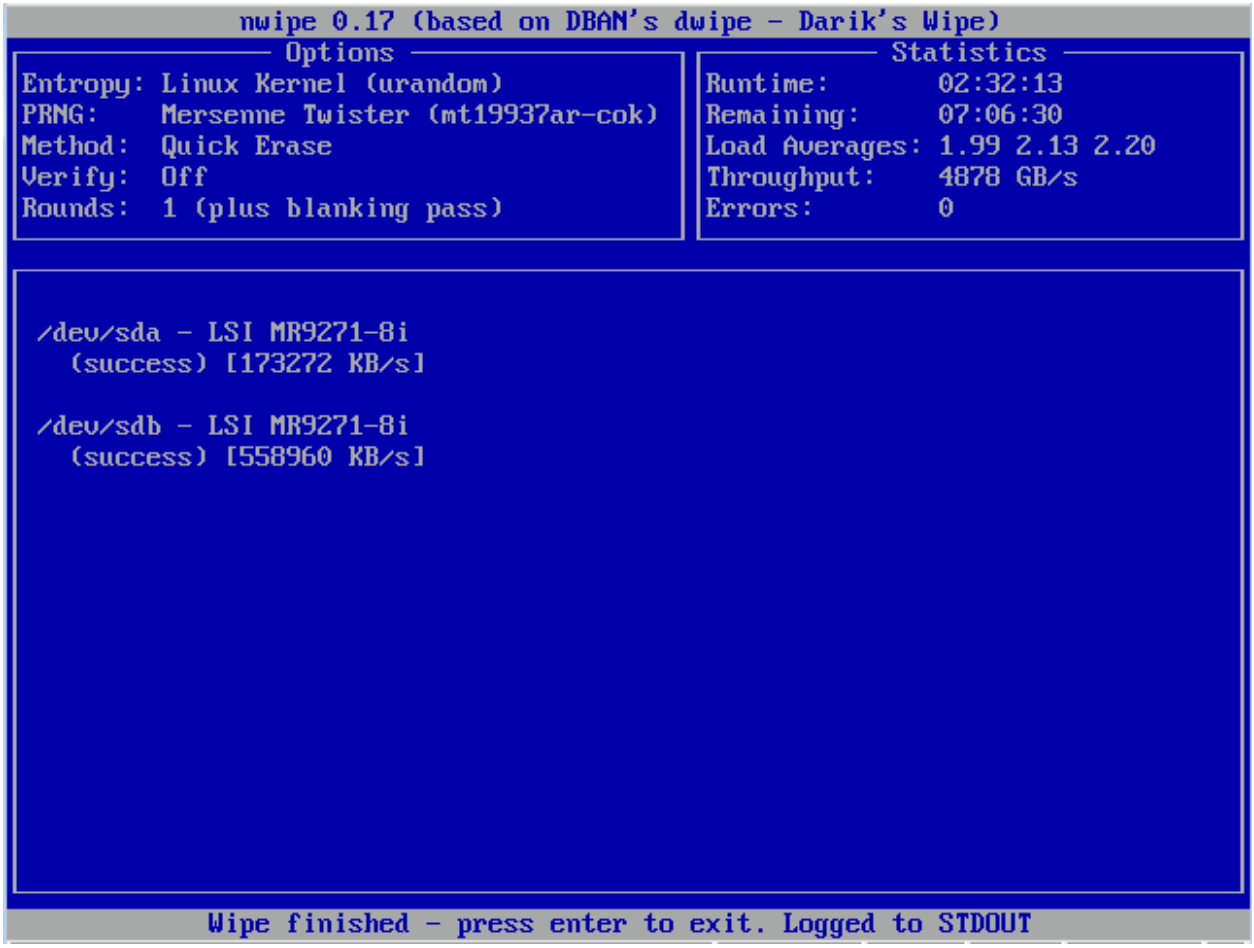
3. 接下来，选择一个擦除选项。请参阅“擦除选项”了解每个选项的大约运行时间。

图 19 - 擦除选项

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

4. 当擦除操作完成后，将显示**擦除已完成**屏幕：

图 20 - 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）	2.5 小时
擦除（3 通道 DOD 方法）	16 小时
擦除（随机覆盖）	12 小时

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

备份

版本 2.2.4 引入了备份功能。现在，Threat Grid 设备可以支持如下操作：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；重置为空数据库状态（可加载此类备份）。

请注意，重置与擦除设备擦除不同。当设备需要离开客户现场时，可使用擦除来避免信息泄漏。用于此目的的擦除流程存在于恢复引导加载程序中，因此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。

内容使用 gocryptfs（第三方开源产品）进行加密。

请注意，考虑到性能方面的原因，文件名加密被禁用。由于 Threat Grid 中的样本和其他内容在任何情况下都不是使用原始名称来存储的，因此这样不会泄漏客户拥有的数据。

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，请务必在使用备份功能之前仔细参考。有关其他技术信息和说明，请参阅*备份说明和常见问题*以及《*Threat Grid 设备设置和配置指南*》，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。

NFS 要求

- 必须运行基于 TCP 的 NFSv4 协议，并确保可以从设备的 Admin 接口进行访问。
- 配置的目录必须由 nfsnobody (UID 65534) 写入。
- NFSv4 服务器必须可以通过 Admin 10Gb 接口进行访问。
- 具有充足的存储空间。请参阅下面的备份存储要求部分了解详情。

下列安装参数可以无条件使用：`rw,sync,nfsvers=4,nofail`

如果 NFS 配置无效（或者配置导致服务指向配置不正确的 NFS 服务器），那么在应用配置时往往会失败。在 OpAdmin 中更正配置并重新应用即可成功。

您可以放心地暴露文件，以便 `nfsnobody` 执行写入操作。在 Threat Grid 设备上唯一能以 `nfsnobody` 身份运行或具有 `nfsnobody` 写入权限的进程就是负责数据加密的进程。例如：明文数据将按照最小特权原则，在不同的用户帐户下暴露给不同的子树；设备上的 PostgreSQL 服务无法访问 ElasticSearch 数据或 freezer；ElasticSearch 服务无法访问 PostgreSQL 或 freezer 数据。

使用 `nfsnobody` 帐户可以简化配置，而无需为每个客户站点都构建一个 `idmap.conf` 来映射本地和远程帐户名称。

备份存储要求

备份存储包括以下组件：

对象存储。在实际中，该存储通常是当前使用的批量存储。对于备份存储的批量存储组件，在数据保留方面应遵循当前使用的设备版本明确规定的策略和限制 - 对于 2.2.x 系列设备，适用的文档地址为 http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-data-retention-v2-2.pdf，此组件的最大存储使用量设为 4.1TB。

PostgreSQL 数据库存储。此存储包含 PostgreSQL 存储的两个完整备份以及一系列 WAL 日志（足以支持从保留的最早完整备份进行回放）。此存储的总容量应不足 500GB。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

ElasticSearch 快照存储。此存储的总容量应不足 1TB。

总存储。鉴于上述信息，备份存储所需的容量不应超过 **5.6TB**。

期望

包含在备份中 - Threat Grid 设备备份过程的初始版本包括以下客户拥有的批量数据：

- 示例
- 分析结果、工件、标记
- 应用层（非 OpAdmin）组织和用户帐户数据。
- 数据库（包括用户和组织）
- 在 Face 或 Mask 门户 UI 中完成的配置

不包括 -

- 系统日志
- 以前下载和安装的更新
- 此版本不包括在设备 OpAdmin 界面中完成的配置，包括 SSL 密钥和 CA 证书

PostgreSQL - 每 24 小时进行一次 PostgreSQL 基础备份。数据库备份无法恢复，系统会显示一条警告，直到至少成功完成一次恢复。

ElasticSearch - ElasticSearch 备份以增量方式进行，每 5 分钟备份一次。

Freezer - Freezer 备份持续进行，在每 24 小时后执行一项作业来处理持续备份遗漏的任何对象。

生成新密钥 - 生成新密钥将创建一个新的独立备份存储。同原始备份存储一样，新存储在按 24 小时周期进行基础备份之后才有效。

备份数据保留

PostgreSQL - 对于 PostgreSQL，保留自执行备份以来的最后两个成功备份和所有 WAL 数据分段。

ElasticSearch - 对于 ElasticSearch，保留最后两个 5 分钟的快照。

批量存储 - 对于批量存储，为共享存储应用与单个设备执行和记录的相同保留策略。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

备份过程概述

Threat Grid 设备上的备份过程包括以下步骤。

步骤 1 根据以上 NFS 要求创建备份目标目录。

步骤 2 在 OpAdmin 中完成安装向导的“NFS 配置”页面。（有关说明，请参阅*配置 Threat* Grid 设备以使用 NFS。）

步骤 3 下载完成 NFS 配置后生成的加密密钥。

重要说明：客户负责备份和安全存储加密密钥！

Threat Grid 不会保留副本。

没有该密钥，就无法进行备份！

步骤 4 重置备份恢复目标。（有关说明，请参阅*将 Threat Grid 设备重置为备份恢复目标*。）

步骤 5 恢复备份数据。（您需要使用步骤 3 中的加密密钥。有关说明，请参阅*恢复备份内容*。）

有关详细说明，请参阅以下各节。

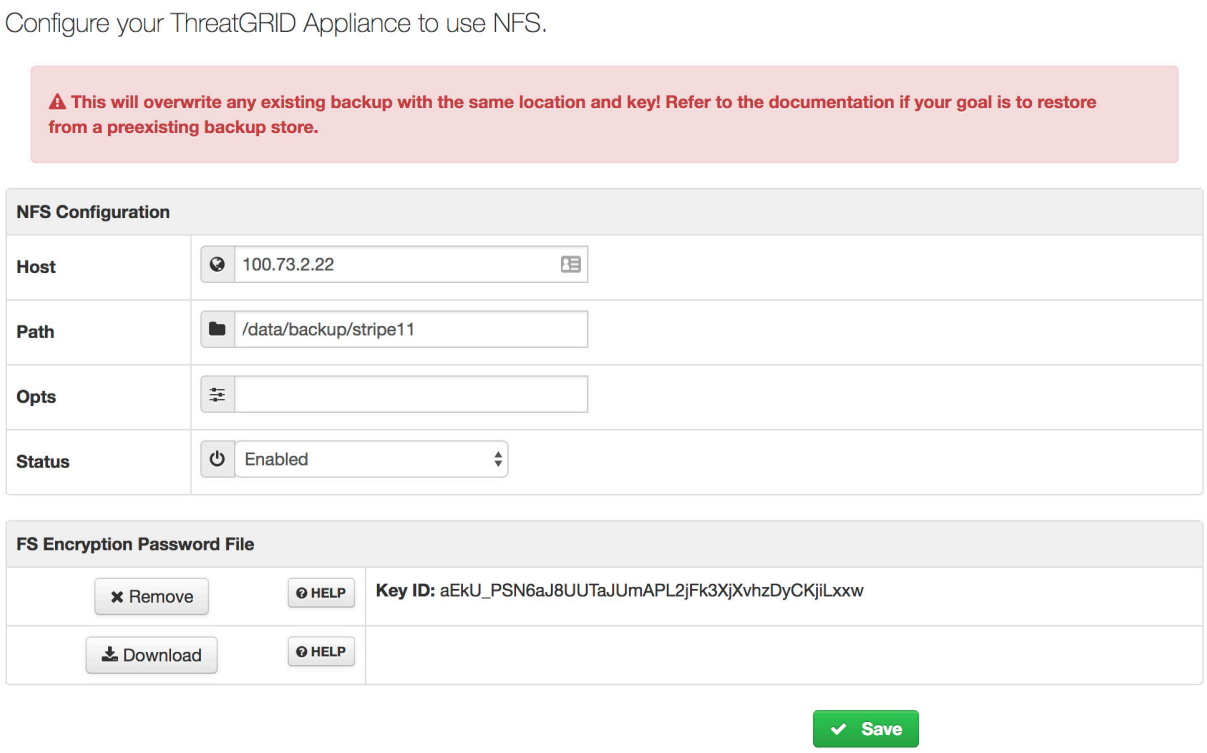
配置 Threat Grid 设备以使用 NFS

NFSv4（非 v3）是 Threat Grid 设备备份的必备要求。（有关详细信息，请参阅 NFS 要求。）NFS 配置通过安装向导中新增的步骤在 OpAdmin 界面中完成。该界面中新增了一个菜单项，可用于以后访问 NFS 配置。

1. 在 OpAdmin 中打开安装向导的“NFS 配置”页面（**配置 > NFS**）。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

图 21 - NFS 配置



2. 按如下方式配置页面：

   主机 - 用于存储设备备份数据的 NFSv4 服务器的地址

   路径 - 指向主机服务器备份目录的路径

   选项 - NFS 安装选项

   状态 - 从下拉列表中选择“启用”（密钥待定）。

3. 点击**保存**。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，没有加密密钥，就无法恢复备份。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

4. 照常完成安装向导的其余部分。

   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 datastore 的过程。

备份频率

对于批量存储的样本、工件和报告，内容将连续备份。另外，还会执行传递以查找和传输 24 小时周期遗漏的内容。

对于 PostgreSQL 数据库，每 24 小时会创建一个基础备份，此后一旦新写入数据库的内容达到 16MB 的阈值，或不少于每 5 分钟创建一次，就会不断添加增量内容。

对于 ElasticSearch 数据库，内容以 5 分钟的周期逐步增加到备份存储中。

备份频率无法得以控制或调整。因为调整这些值需要估计存储使用率、恢复过程时间和无效性能开销，所以目前还不能进行调整。

将 Threat Grid 设备重置为备份恢复目标

注意！使用此过程会破坏客户拥有的数据！所以，请务必小心谨慎！在执行任何任务之前，请通读所有文档。

在可以将设备用作恢复目标之前，设备必须处于预配置状态。设备以这种状态出厂。不过，在设备完成配置后再将其恢复到预配置状态需要显式管理操作。（有关详细信息，请参阅*将 Threat Grid 设备重置为备份恢复目标*。）

注意：重置与恢复模式下可用的安全擦除不同；在将计算机运到 DLP 重新映像中心之前，只有恢复模式下的安全擦除可以从计算机中完全删除客户拥有的数据。恢复模式下的安全擦除不能替代此重置功能：安全擦除会重新映像设备无法使用的单元，而重置是让设备准备好恢复备份。

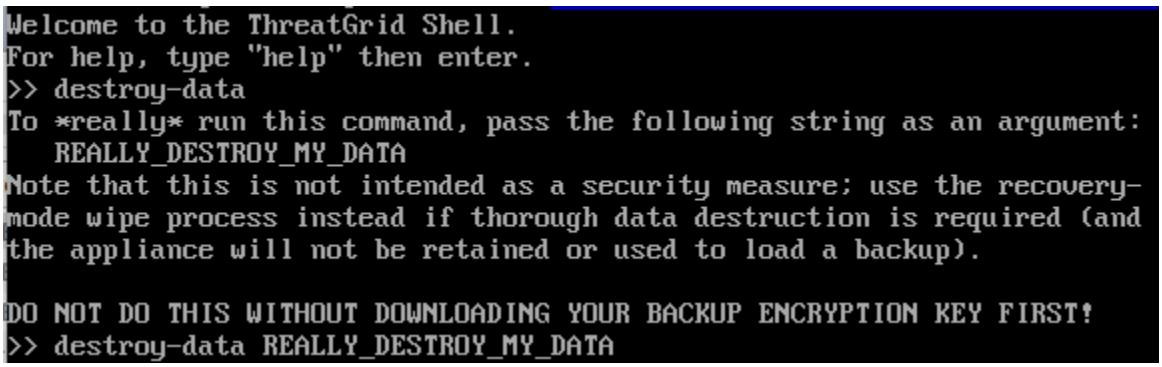
1. **如果不恢复到生产的系统初始状态：**

   必须通过清除系统中已有的数据和 NFS 相关配置，使恢复目标设备恢复预配置状态：

   - 通过设备的 TTY 或通过 SSH 访问 `tgsh-dialog` 配置界面。
   - 选择 `CONSOLE` 选项以输入 tgsh。（请注意，这种情况不适合通过恢复模式输入 tgsh。）
   - 在 `tgsh` 提示符后，输入命令 `destroy-data`。认真阅读提示符提供的说明并遵照操作。
   - 注意此命令不可*撤消*:

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

图 2 - destroy-data REALLY_DESTROY_MY_DATA 命令和参数



以下数据将被销毁：

- 上面***错误!未找到引用源。***下列出的所有数据
- NFS 配置和凭证。
- 用于 NFS 的本地加密密钥副本。

2. **如果另一系统正在主动写入要恢复的备份：**

   （例如，如果是测试恢复生产中主动使用的第二个主设备写入的内容。）

   生成一个一致的可写入 datastore 副本，使执行测试恢复的设备指向此可写入副本，而不是正在连续写入的存储。

一旦设备处于预配置状态，它即可作为备份存储的目标运行，如下一节中所述。

恢复备份内容

重要说明：在恢复过程中，系统不可用来提交样本。

要求：加密密钥。

上传备份加密密钥：

在 OpAdmin 中，在安装向导的“NFS 配置”页面（**配置 > NFS**）中点击**上传**，检索以前在配置用于创建备份的服务器时生成的备份密钥。

- 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。
- 安装向导会检查与备份密钥匹配的目录，如果找到，则会开始将数据恢复到该位置。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

- 所需时间：恢复数据所需的时间取决于备份的大小及其他因素。在测试中，1.2GB 的恢复轻而易举即可完成，而 1.2TB 的恢复则需要 16 个小时以上。
- 注意：恢复过程中不显示进度栏，所以耗时较长的恢复看起来像是安装已挂起；请耐心等待。OpAdmin 会报告恢复成功，而设备将会启动。
- 恢复的数据看起来与原始数据类似。

备份恢复说明

在恢复过程中，样本提交不可用。

只能从安装向导中恢复备份。

通过与原过程相同的过程设置与以前所用相同的 NFS 存储和加密密钥。

将设备设置为使用先前 NFS 存储和加密密钥的行为会触发恢复。

重要说明：一次只能激活一个使用特定备份存储数据运行的服务器。

要在不同的 Threat Grid 设备上测试恢复过程，同时使主设备仍保持运行，请保留一份一致的备份存储快照副本，并使新设备（已上传加密密钥）指向该副本。

备份相关服务通知

未安装网络存储。检查用作后端的网络文件系统是否完全可用，并尝试通过 opadmin 重新应用配置或重新启动设备。

网络存储不工作。检查用作后端的网络文件系统是否完全可用；如果系统在纠正 NFS 服务器的任何问题后 15 分钟内未恢复正常，请尝试重新启动设备。

备份文件系统访问失败。请联系客户支持代表。

找不到 PostgreSQL 备份 - 在已配置备份存储之时到进行第一次基础备份（每 24 小时自动执行）期间，这属于正常情况。请注意，在完成此备份之前，备份属于不完整状态，无法恢复。*在且仅在*此消息持续显示超过 48 小时的情况下，请联系客户支持代表。

最新 PostgreSQL 基础备份超过两天 - 这表明系统尚未成功地为 PostgreSQL 生成新的基础备份。如果未加补救，可能会导致备份存储使用量不受控制（用于保留从越来越早的备份时间点进行恢复所需的完整系列写入内容），并且进行恢复所需的处理时间会非常长。请联系客户支持代表。

备份创建消息： - 这些消息反映启动或触发备份时检测到的错误。

ES 备份（创建）不活动 - 表示启动 ElasticSearch 时，备份存储不可用。通过重新启动设备或（如果 NFS 和加密服务现在在正常运行）登录 tgsh 并运行命令 `service restart elasticsearch.service` 可纠正此问题。

备份维护消息： - 这些消息反映检查以前创建的备份状态时检测到的错误。

ES 备份（维护）快照 (...) 状态“失败” - 这表示最近一次尝试更新 ElasticSearch 数据库的备份时，无法成功写入任何索引。检查 NFS 服务器是否正常工作并有可用空间；如果无法找出问题的起因且该问题仍然存在，请联系客户支持代表。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

ES 备份（维护）快照 (...) 状态“不兼容” - 应仅会在设备升级安装新版 ElasticSearch 后出现；在备份存储升级到与此新版本兼容的版本之前会一直显示。从不兼容的备份中恢复可能需要客户服务协助，否则在这种状态下将会发生故障。

ES 备份（维护）快照 (...) 状态“部分” - 正文中包含两条消息之一：*No prior successful backups seen, so retaining*（如果我们要保留部分备份，总比没有好）；或 *Prior successful backups exist, so removing.*（如果我们要丢弃该部分备份并打算日后重试）。

ES 备份（维护）- 备份需要 (...) ms - 如果备份所需时间超过 60 秒，则屏幕上会显示此消息。这不一定是错误：ElasticSearch 会执行定期维护，由此可能导致大量写入负载（即使是在空闲系统上）。但是，如果在低负载期间仍持续显示该消息，请调查存储性能或联系客户服务代表寻求帮助。

ES 备份（维护）- 无法查询 ElasticSearch 快照状态 - 无法与 ElasticSearch 通信；此故障发生在成功启动备份创建之后。通常，此错误会与其他设备故障一起出现，而补救应侧重于这些问题。如果在设备完全正常运行时出现此错误，并且此错误不自行消失，请联系客户支持代表。

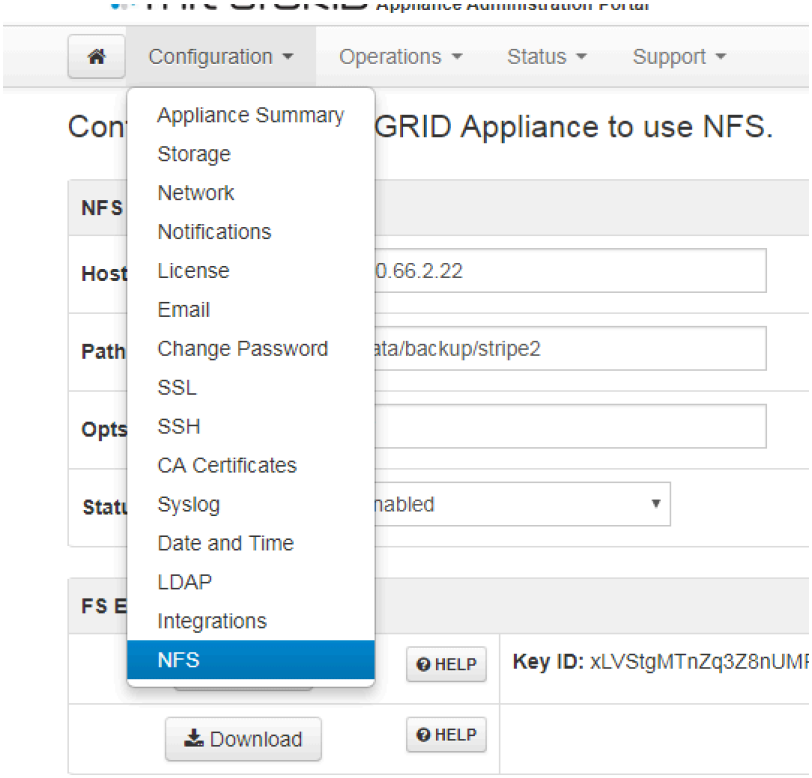
本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

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：

配置菜单

图 22 - OpAdmin 配置菜单

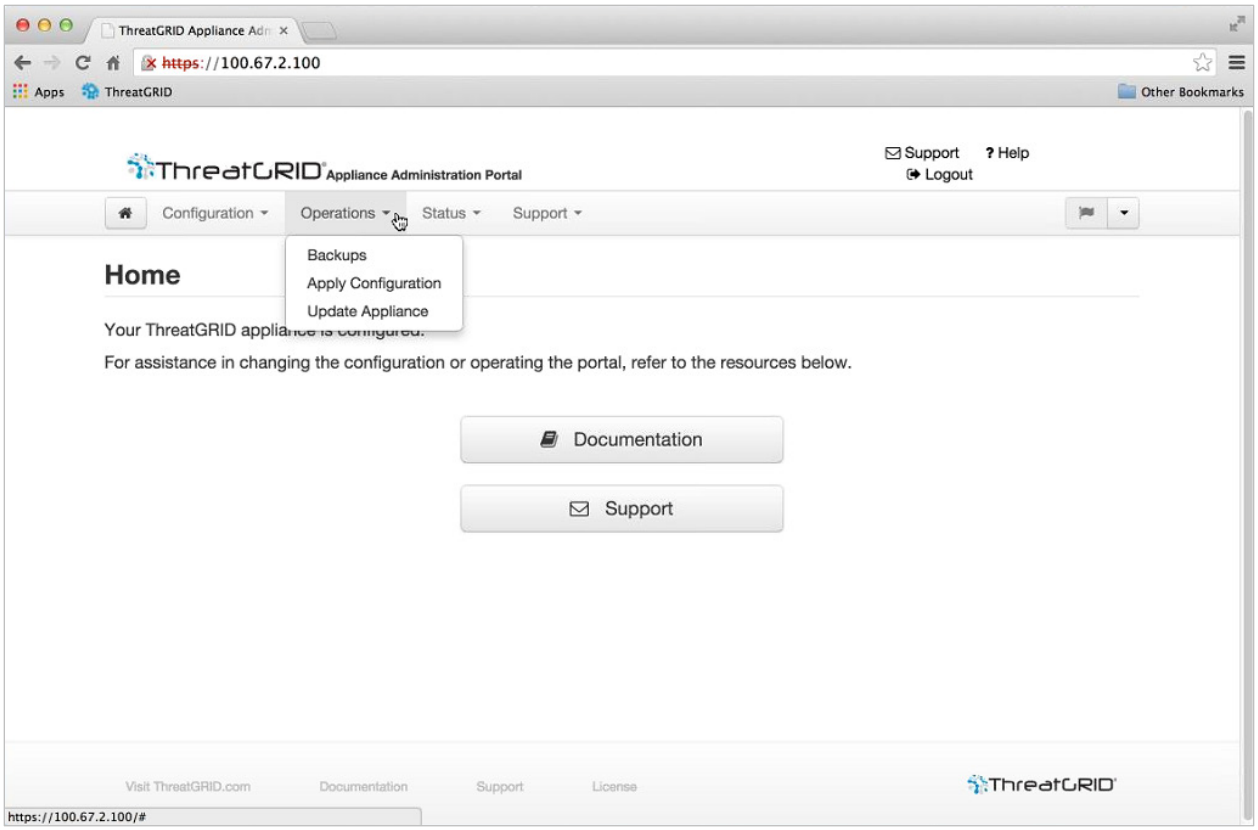


注意：如果您未来需要对您的 OpAdmin 配置设置进行更改，则必须从“配置”菜单访问这些设置以进入编辑模式。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

操作菜单

图 23 - OpAdmin 操作菜单

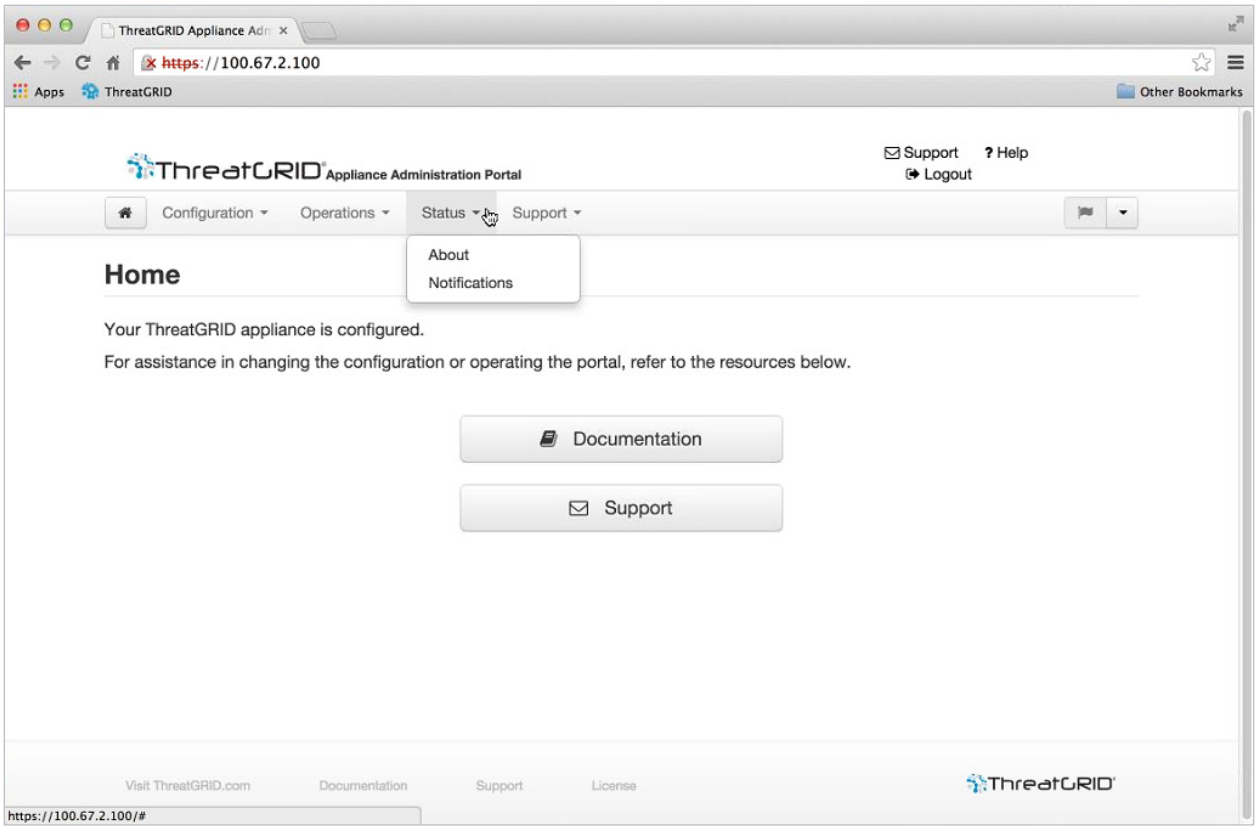


注意：请选择**更新设备**来查看版本说明。

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

状态菜单

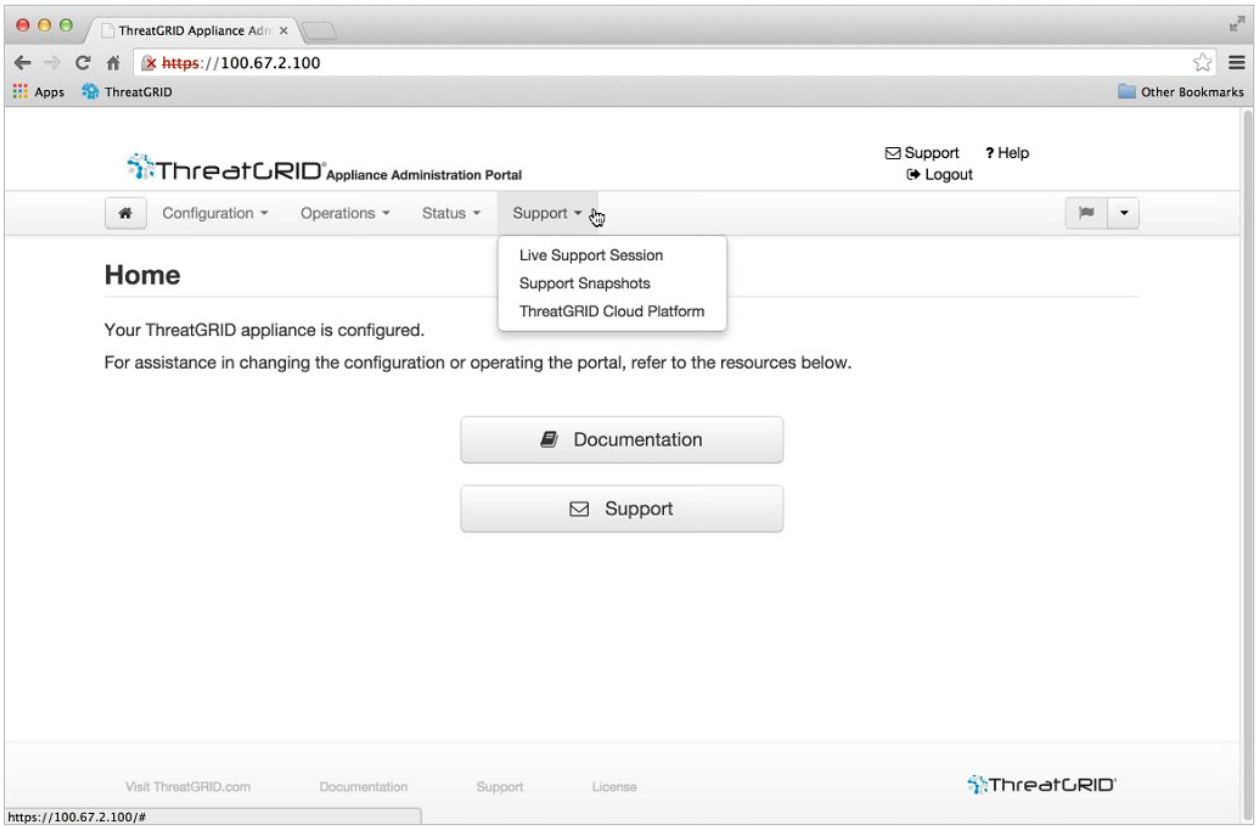
图 24 - OpAdmin 状态菜单



本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。

支持菜单

图 25 - OpAdmin 支持菜单



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

本文所有内容版权所有 © 2015-2017 思科系统公司和/或其附属公司。保留所有权利。