



# 思科 AMP Threat Grid 设备 管理员指南

1.4.5 版

最后更新日期：2015 年 12 月 10 日

思科系统公司 [www.cisco.com](http://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](http://www.cisco.com/go/offices)  
上列出了各办事处的地址、电话和传真。

## 目录

目录 .....	ii
图片清单 .....	v
前言 .....	vi
简介 .....	1
本指南的目标读者 .....	1
使用入门 .....	2
更新 .....	2
版本说明 .....	2
许可 .....	2
API 提交速率限制 .....	2
假定条件 .....	2
管理 .....	3
打开电源 .....	3
登录名和密码 - 默认 .....	5
Threat Grid 门户 UI 管理员 .....	5
TGA 管理员 - OpAdmin 和 threatgrid 用户 .....	5
CIMC (思科集成管理控制器) .....	5
恢复丢失的密码 .....	5
重新设置丢失的管理员密码 .....	5
安装更新 .....	7
更新端口 .....	7
设备内部版本号/版本查询表 .....	8
支持 - 与 Threat Grid 联系 .....	9
支持模式 .....	10
支持服务器 .....	10
支持快照 .....	11
备份 .....	11

配置 THREAT GRID 设备 .....	11
TGSH 对话 .....	11
网络接口配置更新 .....	12
重新连接到 TGSH 对话 .....	12
密码更新 .....	12
在恢复模式下设置网络连接 .....	12
OpAdmin 门户 .....	13
更新 OpAdmin 配置设置 .....	13
SSH 密钥 .....	14
系统日志 .....	14
重新配置 .....	14
使用 DHCP .....	15
DHCP 的显式 DNS .....	15
网络配置和 DHCP .....	15
应用 DHCP 配置 .....	16
SSL 证书和 THREAT GRID 设备 .....	17
使用 SSL 的接口 .....	17
支持的 SSL/TLS 版本 .....	17
SSL - 不支持 .....	18
主机名/CN 验证 .....	18
默认的自签名 SSL 证书 .....	18
下载 Threat Grid 设备 SSL 证书 .....	18
替换 SSL 证书 .....	18
如何将 ESA/WSA 设备连接到 THREAT GRID 设备 .....	19
方法 1: 重新生成新的 SSL 证书 .....	19
方法 2: 手动替换 SSL 证书 .....	21
管理 THREAT GRID 组织和用户 .....	22
创建新组织 .....	22
添加用户 .....	22
隐私和样本可见性 .....	22

Threat Grid 设备上的隐私和可见性 .....	23
擦除设备 .....	25
擦除选项.....	27
附录 - OPADMIN 菜单 .....	28
配置 (Configuration) 菜单 .....	28
操作 (Operations) 菜单 .....	29
状态 (Status) 菜单 .....	30
支持 (Support) 菜单 .....	31

## 图片清单

图 1 - 启动期间的 Cisco 屏幕 .....	3
图 2 - TGSN 对话 .....	4
图 3 - 启动菜单 - 恢复模式 (Recovery Mode) .....	6
图 4 - 恢复模式下的 Threat Grid 外壳 .....	6
图 5 - 输入新密码 .....	7
图 6 - 设备版本号 .....	8
图 7 - OpAdmin 启动一个实时支持会话 .....	10
图 8 - 立即重新配置 .....	14
图 9 - TGSN 对话（连接到一个配置为使用 DHCP 的网络） .....	15
图 10 - SSL 证书配置页面 .....	17
图 11 - 用户详细信息 (User Details) 页面 > 重新激活用户 .....	20
图 12 - Threat Grid 设备上的隐私和可视性 .....	24
图 13 - 擦除设备 .....	25
图 14 - 擦除选项 .....	26
图 15 - 擦除已完成 .....	27
图 16 - OpAdmin 配置菜单 .....	28
图 17 - OpAdmin 操作菜单 .....	29
图 18 - OpAdmin 状态菜单 .....	30
图 19 - OpAdmin 支持菜单 .....	31

## 前言

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，请与思科代表联系以获取副本。

思科所采用的 TCP 信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提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

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](http://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 AMP Threat Grid 设备设置和配置指南*

© 2015 Cisco Systems, Inc. 保留所有权利。

## 简介

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)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](#)》。

## 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。

## 版本说明

有关 Threat Grid 设备版本更新的详细信息，请参阅版本说明，该说明可从 **OpAdmin 门户 (OpAdmin Portal)** 的以下位置获取：

**操作 (Operations) > 更新设备 (Update Appliance) > 版本说明 (Release Notes)**。

Threat Grid 门户用户界面的版本说明位于 *帮助 (Help)* 页面：

**帮助 (Help) > 版本说明 (Release Notes)**

## 许可

应在 *OpAdmin 配置许可管理 (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](mailto:dedebeer@cisco.com) 与 Dean De Beer 联系

## API 提交速率限制

API 提交速率限制是许可证的一部分。（您还可以按照 Threat Grid 门户联机帮助文档中的说明限制单个用户的样本提交速率。）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 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

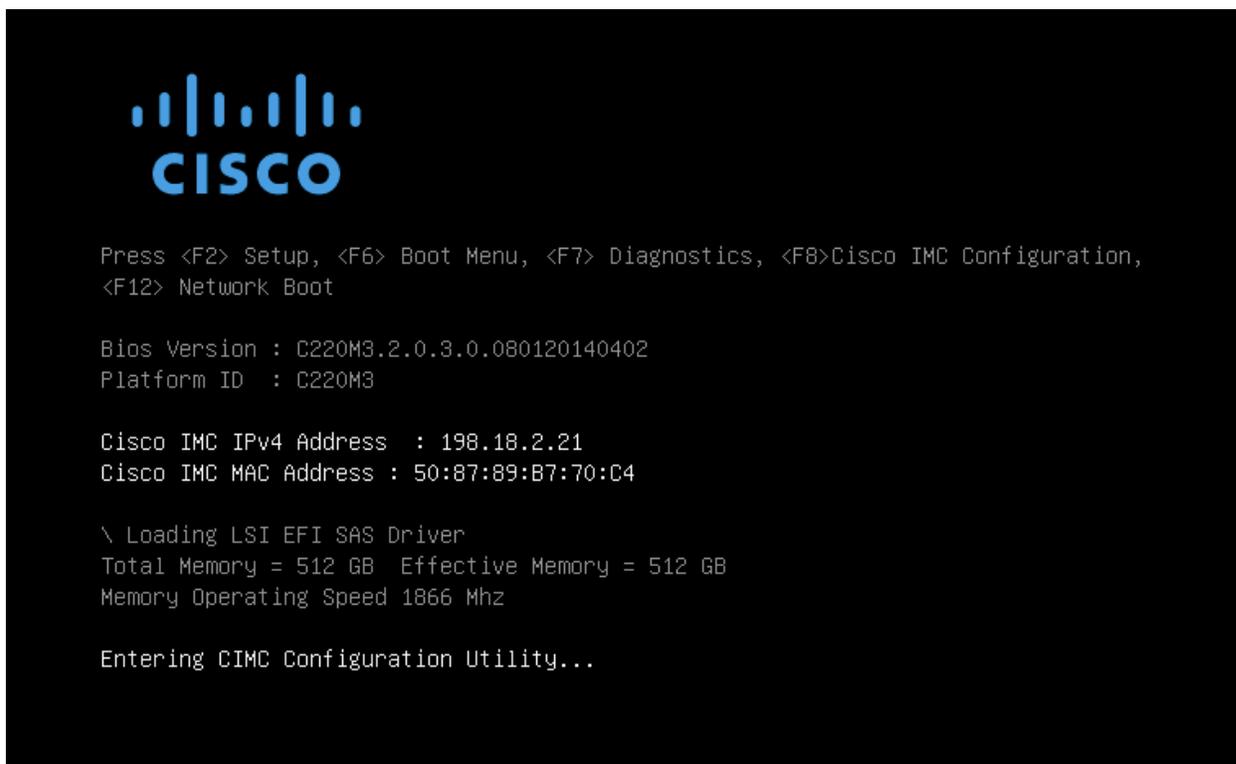
本指南假定，初始设置和配置步骤已经按《[Threat Grid 设备设置和配置指南](#)》中的说明完成，并且已成功提交并分析初始测试恶意软件样本。

## 管理

### 打开电源

打开设备电源，等待设备启动。Cisco 屏幕会短暂显示：

图 1 - 启动期间的 Cisco 屏幕

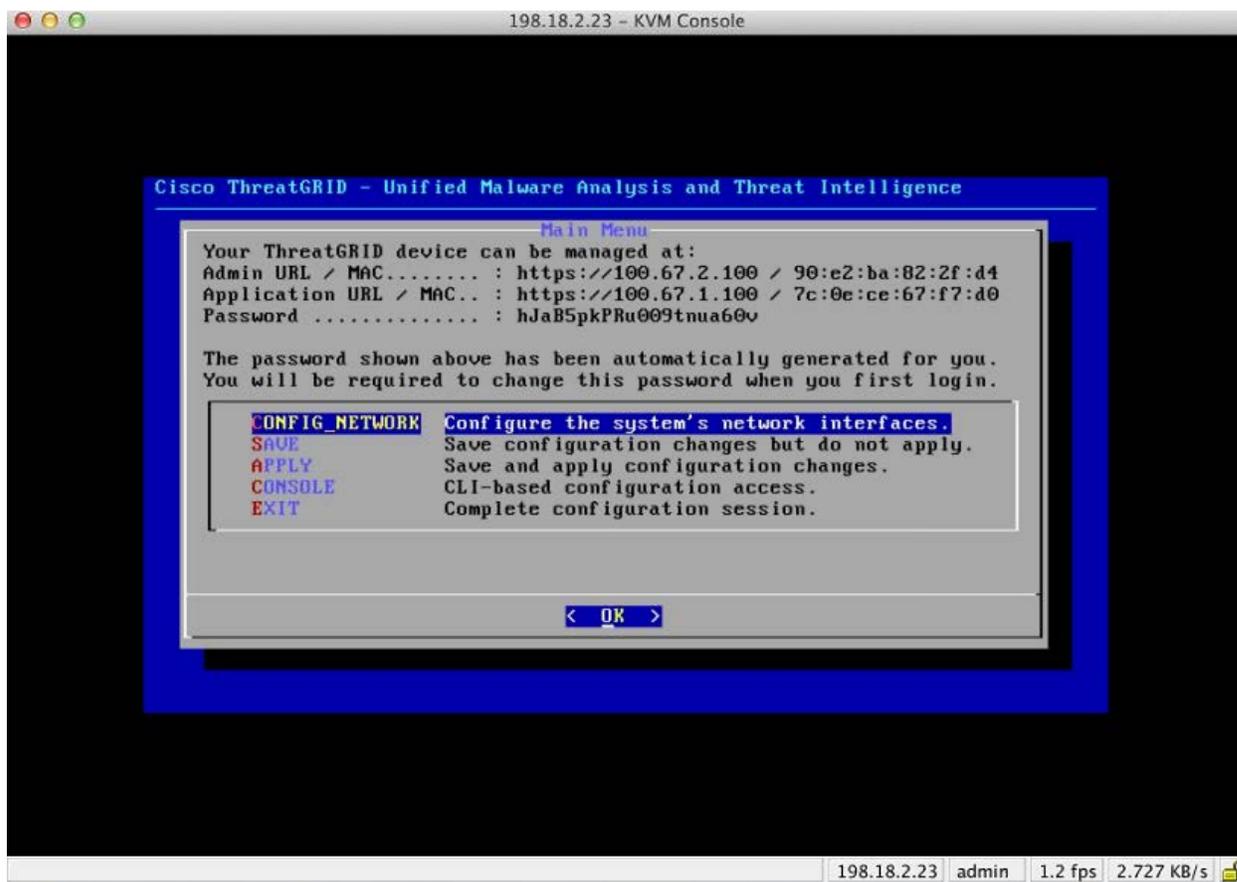


**注意：**如果您想要配置 CIMC 界面，请在内存检查完成后按 **F8**。

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“密码恢复”部分的相关说明。

## 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:** “changeme”

## 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 TGSN 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

```

any network configuration changes will be applied both to the running recovery
instance and to the real (non-recovery) system, and tgsd will be immediately
restarted.
[ 29.363085] configure-from-target[1352]: net.ipv4.tcp_sack = 1
[ OK ] Started OpenSSH Daemon.
YOU MUST EXIT TGSd BEFORE NETWORK CONFIGURATION CHANGES TAKE EFFECT.

FAILING TO DO SO MAY PREVENT SUPPORT STAFF FROM BEING ABLE TO REACH YOUR SYSTEM.
[ 29.454605] configure-from-target[1352]: net.ipv4.tcp_window_scaling = 1
[ OK ] Reached target ThreatGRID Recovery Mode.
Welcome to the ThreatGrid Shell.
For help, type "help" then enter.
[ 29.516718] configure-from-target[1352]: net.ipv4.tcp_keepalive_intvl = 30
>> [ 29.566235] configure-from-target[1352]: net.ipv4.tcp_tw_reuse = 1
[ 29.578452] configure-from-target[1352]: net.core.umem_default = 8388608
[ 29.590348] configure-from-target[1352]: net.core.rmem_default = 8388608
[ 29.602073] configure-from-target[1352]: net.core.umem_max = 8388608
[ 29.613473] configure-from-target[1352]: net.core.rmem_max = 8388608
[ 29.624361] configure-from-target[1352]: net.core.netdev_max_backlog = 10000
[ 29.635973] configure-from-target[1352]: vm.swappiness = 0
[ 29.645657] configure-from-target[1352]: kernel.shmmax = 77309411328
[ 29.656570] configure-from-target[1352]: kernel.shmall = 18874368
[ 29.667725] sshd[1493]: Server listening on 0.0.0.0 port 22.
[ 29.680578] sshd[1493]: Server listening on :: port 22.
[ 29.692276] su[1495]: (to threatgrid) root on console
[ 29.702728] su[1495]: pam_unix(su-l:session): session opened for user threatgrid by (uid=0)
[ 29.713268] systemd[1]: Started Initialize From Target.
[ 29.723599] systemd[1]: Starting Rescue Shell...
[ 29.733666] systemd[1]: Started Rescue Shell.
[ 29.743472] systemd[1]: Starting ThreatGRID Support Mode Worker...
[ 29.753293] systemd[1]: Starting OpenSSH Daemon...
[ 29.762993] systemd[1]: Started OpenSSH Daemon.
[ 29.772456] systemd[1]: Starting ThreatGRID Recovery Mode.
[ 29.781763] systemd[1]: Reached target ThreatGRID Recovery Mode.
[ 29.791010] systemd[1]: Started ThreatGRID Support Mode Worker.
[ 29.800165] systemd[1]: Startup finished in 5.581s (kernel) + 23.948s (userspace) = 29.530s.
[ 29.809835] configure-from-target[1352]: Done with importing configuration from target
[ 29.819359] rash-worker[1501]: -- rash-worker.go:42: RASH worker "FCH1832U319" ready to dial router.
[ 30.827516] rash-worker[1501]: -- rash-worker.go:55: connected to router "ThreatGRID" at rash.threatgrid.com:19791
$

```

2. 运行 `passwd` 以更改密码:

图 5 - 输入新密码

```
>>
>> passwd
[ 286.653257] sudo[1511]: threatgrid : TTY=ttty1 : PWD=/home/threatgrid : USER=root : COMMAND=/usr/bin/passwd threatgrid
Enter new UNIX password: [ 286.663606] sudo[1511]: pam_unix(sudo:session): session opened for user root by (uid=0)
```

**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。必须先安装许可证, 并完全配置设备, 才能下载设备更新。

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。

**重要提示:** 必须按顺序安装更新。要测试更新, 请提交一个样本进行分析。

## 更新端口

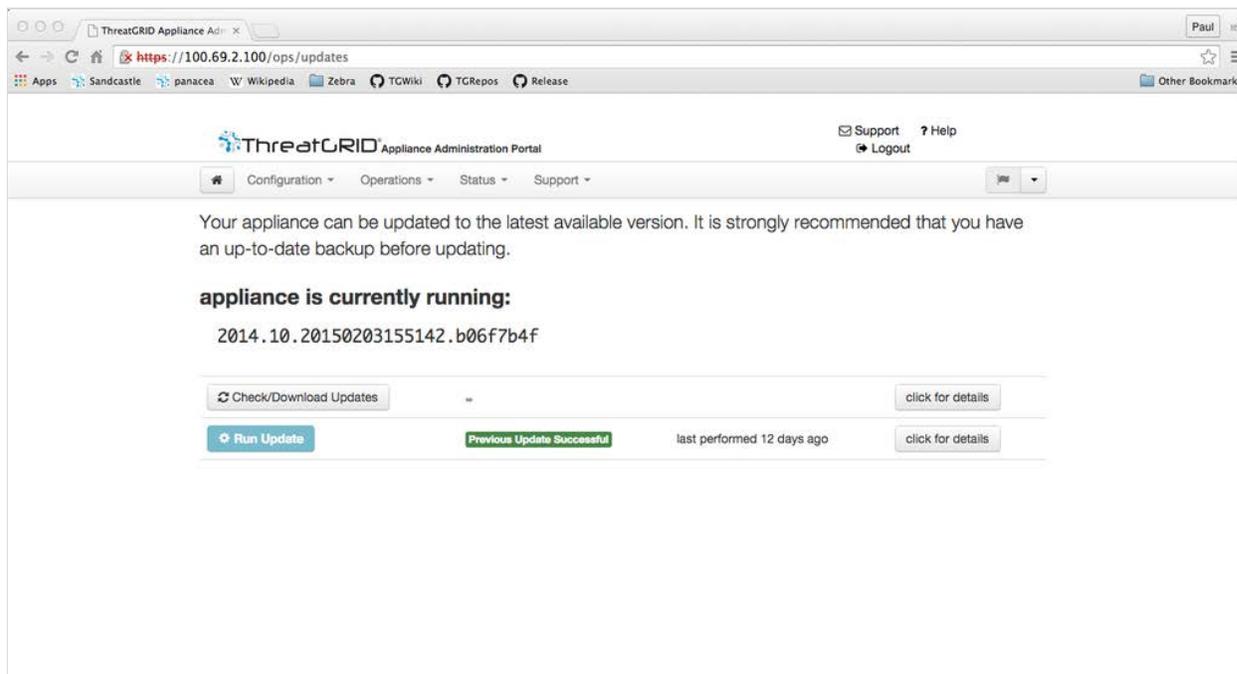
Threat Grid 设备通过 SSH、端口 22 下载版本更新。

- 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。

1. 从**操作 (Operations)** 菜单, 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

可以在更新 (Updates) 页面 (OpAdmin **操作 (Operations)** > **更新设备 (Update Appliance)**) 上查看设备的内部版本号, 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
2014.10.20151123133427.898f70c2	v1.4.5
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 <b>注意：</b> 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

## 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：

- **电子邮件。** 请将您的咨询发送电子邮件至 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)**
- 全面的服务状态（从外壳中读取的服务状态）
- 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

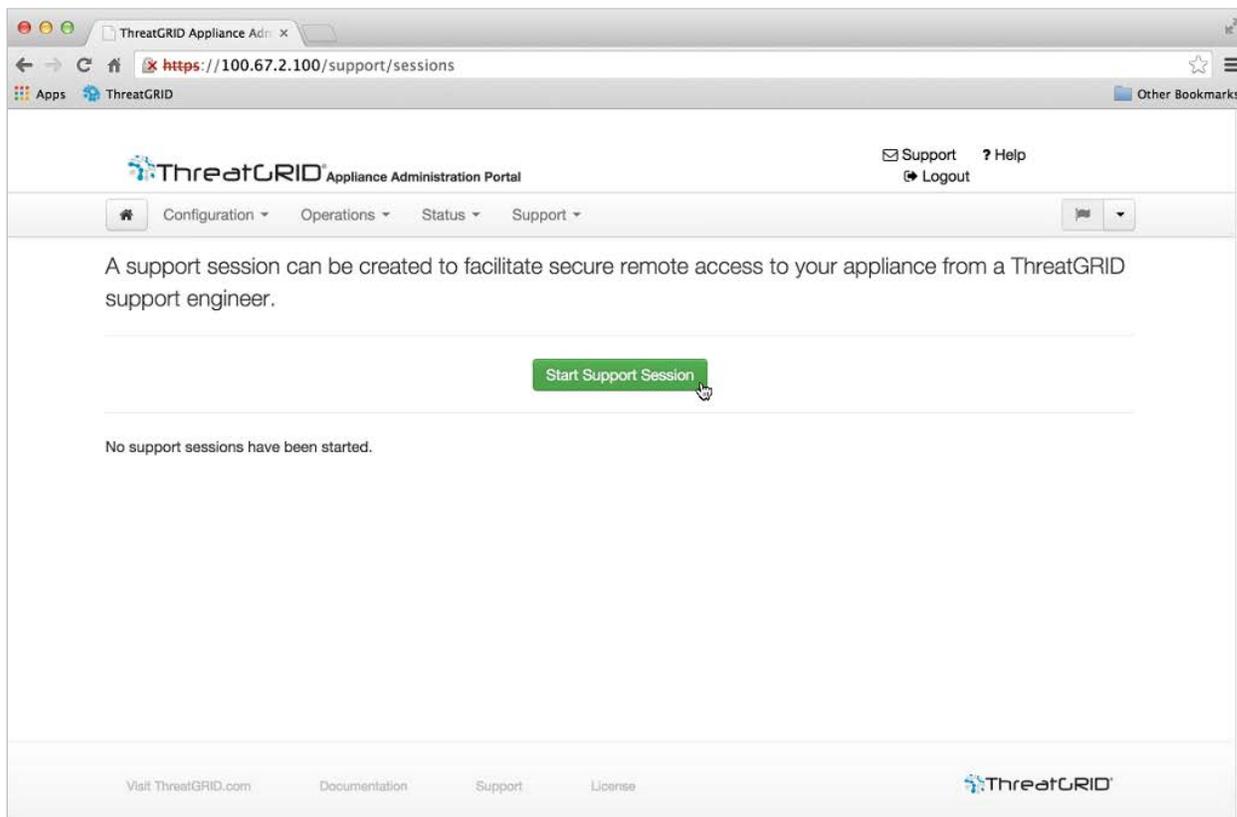
## 支持模式

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。可以通过 **OpAdmin 门户支持 (OpAdmin Portal Support)** 菜单完成此操作。（您还可以从 TGSN 对话启用支持模式。）

启动与 Threat Grid 技术支持的实时支持会话：

在 **OpAdmin** 中，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. 从**支持 (Support)** 菜单，请选择**支持快照 (Support Snapshots)**。
2. 拍摄快照。
3. 一经拍摄完快照后，您可以自己将其下载为 .tar .gz 文件，也可以按**提交 (Submit)**，这样会自动将快照上传到 Threat Grid 快照服务器。

## 备份

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 THREAT GRID 设备

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)** 界面中维护。

## TGSH 对话

TGSH 对话 (TGSH Dialog) 界面主要用于维护以下内容：

- 网络接口配置
- 显示 OpAdmin 管理员的密码
- 安装更新
- 启动支持模式
- 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*。

## 网络接口配置更新

1. 在 **TGSH 对话 (TGSH Dialog)** 界面中, 请选择 **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. 请将 **DIRTY** 网络 DNS 名称 (DNS Name) 留空。
4. 在您更新完网络设置后, 请向后移动选项卡, 然后选择**验证 (Validate)** 验证您的条目。  
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. 选择**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) 该对话框。

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。

## OpAdmin 门户

OpAdmin 门户是设备上的 Threat Grid 管理员的门户。它是一个 Web 接口，一经在 **Admin** 接口上配置了 IP 地址后，就可以使用该接口。

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的重要设备配置设置，包括：

- 管理员的密码 (OpAdmin 和 "threatgrid" 用户)
- Threat Grid 许可证和速率限制
- SMTP
- SSH
- SSL 证书
- DNS 服务器
- 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

## 更新 OpAdmin 配置设置

《[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。

**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 TGSN 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）为通过电子邮件提供系统通知，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)**。

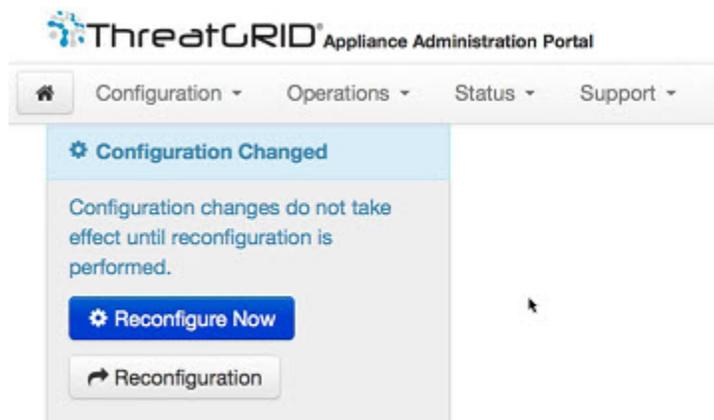
**编辑或删除：**如果需要更新系统日志 DNS，只需要编辑或删除它并点击**保存 (Save)**。

## 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)** 对话框将打开：

图 8 - 立即重新配置



2. 点击**重新配置 (Reconfigure)** 将更改应用到设备。

## 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）

```
Main Menu
Your ThreatGRID device can be managed at:
Admin URL / MAC..... : https://10.90.3.127 / 90:e2:ba:79:db:08
Application URL / MAC.. : https://10.90.2.127 / 1c:6a:7a:18:56:64
Password ..... : mSG7SbJp1lFO3f2vWlNi

The password shown above has been automatically generated for you.
You will be required to change this password when you first login.

CONFIG NETWORK  Configure the system's network interfaces.
SAVE            Save configuration changes but do not apply.
APPLY          Save and apply configuration changes.
CONSOLE        CLI-based configuration access.
EXIT           Complete configuration session.

< OK >
```

- **管理 URL (Admin 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 (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)** 是初始的管理员密码，在设备安装时随机生成。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，请点击**网络 (Network)**。（尽管在许可证窗口中选中了**配置 (Configuration) > 网络 (Network)**，但 DHCP 网络配置尚未完成。）

*网络配置(Network Configuration)* 页面打开。

#### 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. 完成**子网 (Subnet)** 掩码和**网关 (Gateway)**，如果需要。
5. 选中**验证 DNS 名称 (Validate DNS Name)**，验证 DNS 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. 完成**子网掩码 (Subnet mask)** 和**网关 (Gateway)**，如果需要。

#### 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/电子邮件

电子邮件配置是从**电子邮件 (Email)** 页面进行管理。

#### 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。

### 使用 SSL 的接口

在 Threat Grid 设备上有两个使用 SSL 的接口：

- UI/API 的 **CLEAN** 接口，以及集成（ESA/WSA 设备等）
- **OpAdmin 门户 (OpAdmin Portal)** 的 **Admin** 接口。

可独立地配置这两个证书。

在 **OpAdmin > 配置 (Configuration) > SSL** 中。**SSL** 页面将打开。

图 10 - SSL 证书配置页面



The screenshot shows the ThreatGRID Appliance Administration Portal interface. At the top, there are navigation tabs for Configuration, Operations, Status, and Support. The main content area displays a table of SSL certificates. The table has three columns: Interface, Details, and Operations. Two certificates are listed:

Interface	Details	Operations
ThreatGRID Application <i>tg-app-clean.acme.test</i>	Issuer: /O=ThreatGrid, LLC/CN=tg-app-clean.acme.test Subject: /O=ThreatGrid, LLC/CN=tg-app-clean.acme.test Validity: 2015-08-05 14:00:27 UTC - 2019-08-05 14:05:27 UTC	Upload, Download, Regenerate
Administration Portal <i>tg-app-admin.acme.test</i>	Issuer: /O=ThreatGrid, LLC/CN=pandem Subject: /O=ThreatGrid, LLC/CN=pandem Validity: 2015-08-02 02:10:38 UTC - 2019-08-02 02:15:38 UTC	Upload, Download, Regenerate

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

### 支持的 SSL/TLS 版本

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

## SSL - 不支持

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。

## 主机名/CN 验证

- 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。
- 黄色挂锁图标表示一个警告，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。请参阅下面的“*替换 SSL 证书*”。

## 默认的自签名 SSL 证书

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（通用名称）是 " *pandem* "，有效期为 10 年。在生产制造时不会知道客户在配置期间分配给 Threat Grid 设备的主机名。

某些客户端应用要求 SSL 证书中使用的 CN 与设备的主机名匹配。

证书中的主机名还必须与连接的 ESA 或 WSA 设备或其他集成思科设备或者服务上的比较证书中使用的主机名匹配。

## 下载 Threat Grid 设备 SSL 证书

可以下载 Threat Grid SSL 证书，而不是密钥。

1. 在 OpAdmin SSL 配置页面上，点击**下载 (Download)**。就会下载 SSL 证书。
2. 像安装任何其他 SSL 证书一样，在 ESA/WSA 设备或其他集成的思科产品上安装该证书。此步骤您只需要 .cert 文件。

## 替换 SSL 证书

有时候，经常会因各种原因需要替换 SSL 证书；证书过期，主机名变更，或者需要更改证书以支持与其他设备的集成。

例如，ESA/WSA 设备和其他 CSA 思科集成设备和服务可能需要 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。

有两种方式可以在 Threat Grid 设备上替换 SSL 证书。

- 方法 1：重新生成新的 SSL 证书：**SSL > 重新生成 (Regenerate)**
- 方法 2：手动替换 SSL 证书

下面的部分将介绍这两种方法。

## 如何将 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、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 设备和 ESA/WSA、其他设备以及思科产品之间的这些集成是由思科沙盒 API（“CSA API”）启用，通常称为“CSA 集成”。

为了 ESA/WSA 设备和其他集成可以连接到 Threat Grid 设备，Threat Grid 设备的 SSL 证书 CN 必须与其当前主机名匹配，必须是集成 ESA/WSA 预期的主机名。

在集成的 ESA/WSA 或其他设备可以向 Threat Grid 设备提交样本以进行分析前，它必须在 Threat Grid 设备处已注册。

在集成的 ESA/WSA 或其他设备可以在 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。

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，提供了以下信息，协助您完成设置 Threat Grid 设备的顺序步骤，以便与 ESA/WSA 设备和其他 CSA 集成通信。

处理 Threat Grid 设备 SSL 证书的方法有两种：

- 方法 1：重新生成新的 SSL 证书
- 方法 2：手动替换 SSL 证书

### 方法 1：重新生成新的 SSL 证书

**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。

1. 在 **OpAdmin SSL** 页面中，点击**重新生成 (Regenerate)**。会使用证书的 CN 字段中的设备当前主机名生成 Threat Grid 设备的新自签 SSL 证书。挂锁图标为绿色。
2. 点击**下载 (Download)** 下载新的 SSL 证书。
3. 在 ESA/WSA 设备上安装新的 SSL 证书。

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>
4. 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。

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

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。

5. 将思科 ESA/WSA/其他设备注册到 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。

6. 完成 ESA/WSA 文件分析配置。

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。

7. 在 Threat Grid 设备上激活新设备用户帐户。

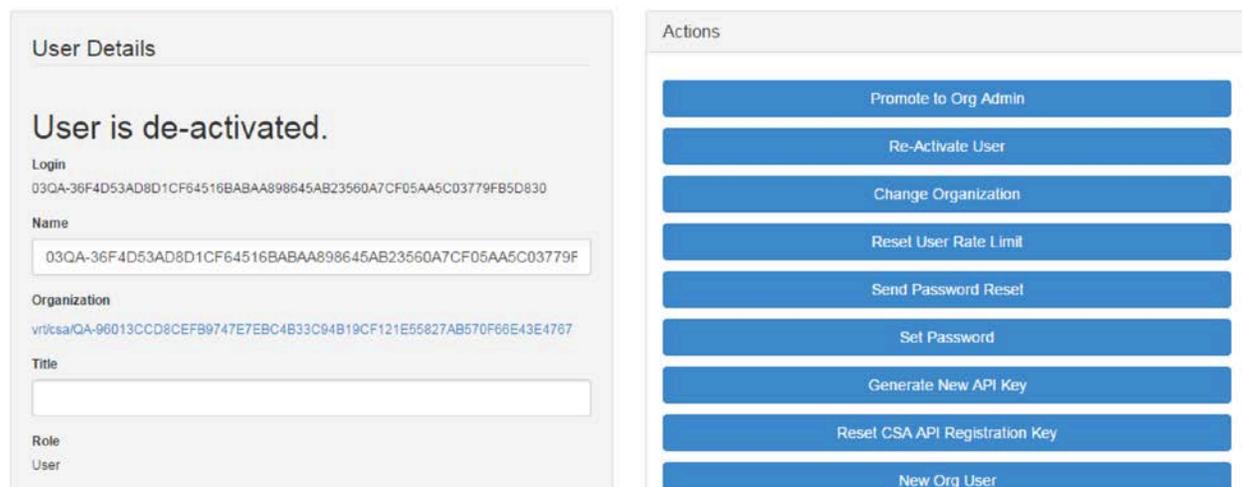
根据那些自动注册到 TG 设备的产品的说明文档配置 ESA/WSA。

在连接设备注册后，会使用设备 ID 作为登录 ID 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。

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。此帐户的初始状态为“已停用”（de-activated）。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，就像其他用户一样。

8. 作为管理员登录到 Threat Grid 用户界面，从**欢迎 (Welcome)** 菜单中选择**管理用户 (Manage Users)**，然后打开设备用户帐户的**用户详细信息 (User Details)** 页面。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



9. 点击**重新激活用户 (Re-Activate User)**。会打开一个对话框要求您确认。

10. 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。

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（相关内容将在下面介绍）。

## 方法 2：手动替换 SSL 证书

如果您的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，在 ESA/WSA 设备上使用 CA 证书。

仅在您的现场尚无 SSL 证书基础设施，并且您希望手动生成新的 SSL 证书时，以下信息才适用。

### 1. 生成您自己的 SSL 证书 - 使用开放 SSL 的示例。

以下示例说明了为“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：**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)** 按钮将其上载到 Threat Grid 设备, 并且还将其上传到 ESA/WSA 设备 (仅 .cert)。
- 按照上面的方法 1 的步骤 3 到步骤 10。

## 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。

**注意:** 组织一经在此界面中创建后, 无法删除, 因此请仔细安排此任务。

- 请以管理员身份登录 Threat Grid 门户。
- 点击位于左上角的**欢迎 (Welcome)** 下拉链接, 然后选择**管理组织 (Manage Orgs)**。组织 (Organizations) 页面打开, 列出设备上的所有组织。
- 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。
- 所有字段均为必填字段。

添加一个组织名称 (目前对名称没有大小限制)。

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。

优先级 (Priority) 字段消失; 现在请输入 " 50 "。

- 点击**创建 (Create)**。现在创建了新的组织, 并且在组织列表中可以看到。

## 添加用户

有关管理用户帐户 (包括集成思科 ESA/WSA 设备和其他设备的帐户) 的完整说明和文档 - 请参阅 Threat Grid **帮助 (Help) > 管理用户 (Managing Users)**。

## 隐私和样本可见性

如果提交敏感文档或存档类型进行分析, 则隐私尤为重要。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。

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。

## 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。

<b>CSA 集成</b>	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。
<b>Threat Grid 用户 - 公共</b>	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。
<b>Threat Grid 用户 - 专用</b>	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：			
当样本由以下人员提交时：	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	全	全	全	全
Threat Grid 用户 - 专用	全	无	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	全	全	全	全

## 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：**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. 此选项要求输入以下文本作为密码：

I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION

3. 接下来，选择一个擦除选项。请参阅下面部分介绍的擦除选项，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

```

nwipe 0.17 (based on DBAN's dwipe - Darik's Wipe)
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseme Twister (mt19937ar-cok)
Method: Quick Erase
Verify: Off
Rounds: 1 (plus blanking pass)

----- Statistics -----
Runtime: 02:32:13
Remaining: 07:06:30
Load Averages: 1.99 2.13 2.20
Throughput: 4878 GB/s
Errors: 0

/dev/sda - LSI MR9271-8i
(success) [173272 KB/s]

/dev/sdb - LSI MR9271-8i
(success) [558960 KB/s]

Wipe finished - press enter to exit. Logged to STDOUT
    
```

- 按 **Enter** 键退出。

### 擦除选项

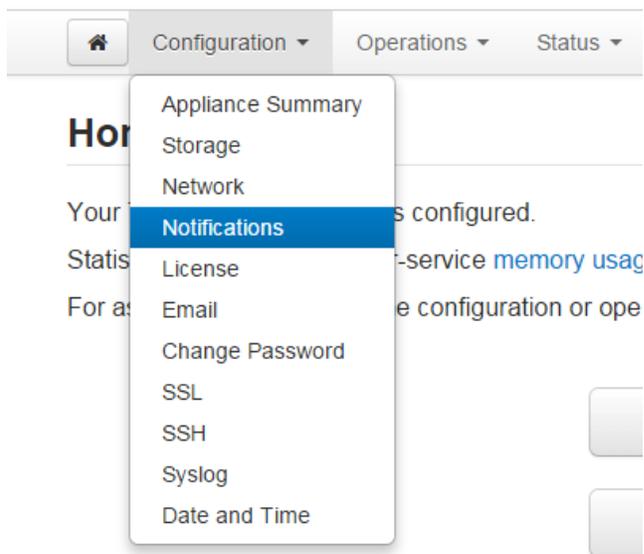
擦除选项	大约运行时间
擦除 (快速: 零磁盘) (Wipe (Fast: Zero Disks))	2.5 小时
擦除 (3 通道 DOD 方法) (Wipe (3-pass DOD method))	16 小时
擦除 (随机覆盖) (Wipe (Random Overwrite))	12 小时

## 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

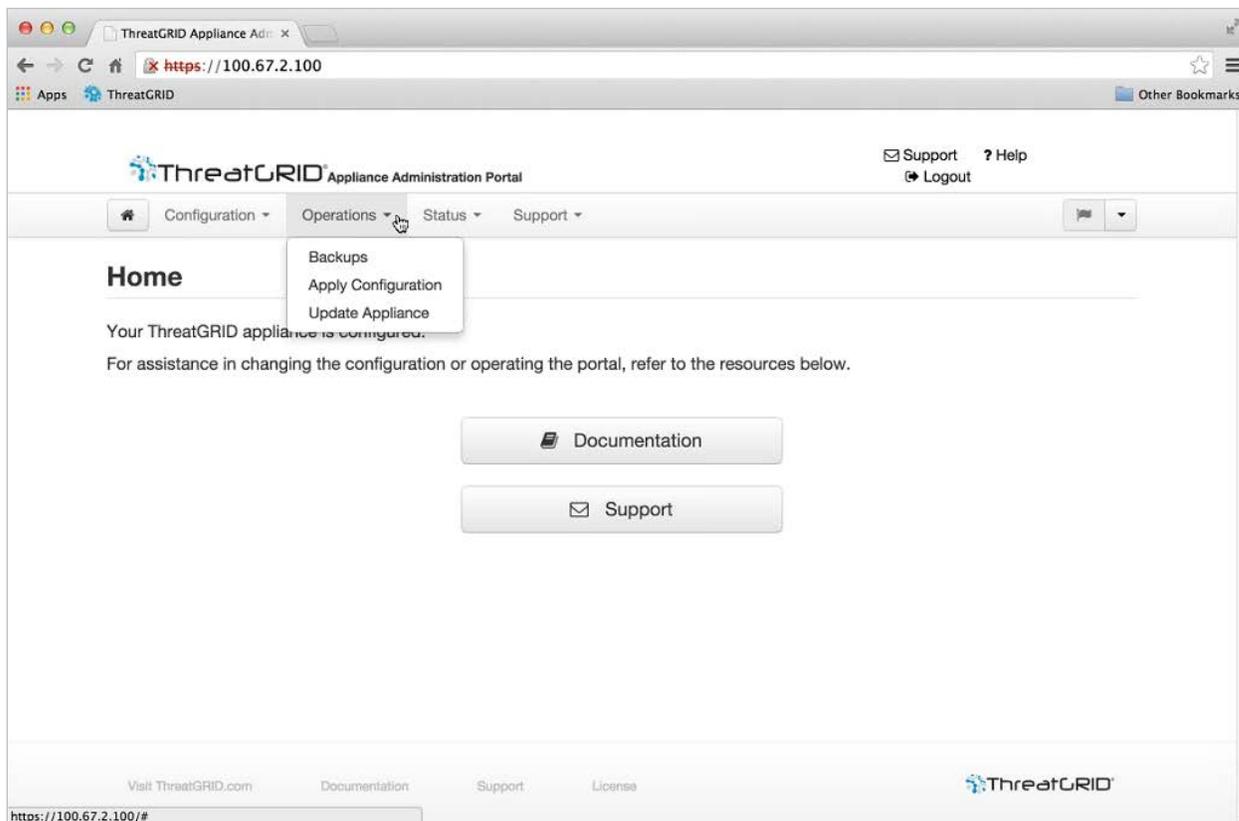
图 16 - OpAdmin 配置菜单



**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

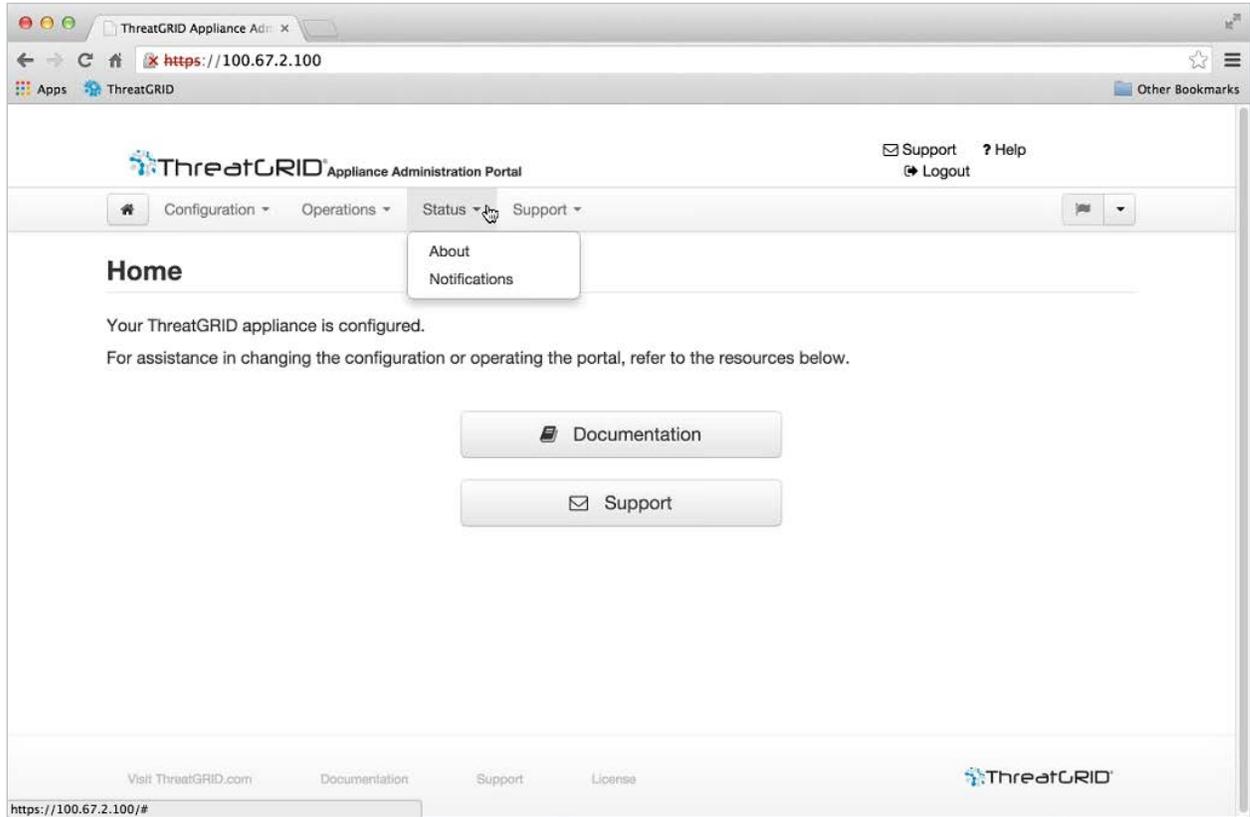
图 17 - OpAdmin 操作菜单



**注意：**选择**更新设备 (Update Appliance)** 查看发行说明。

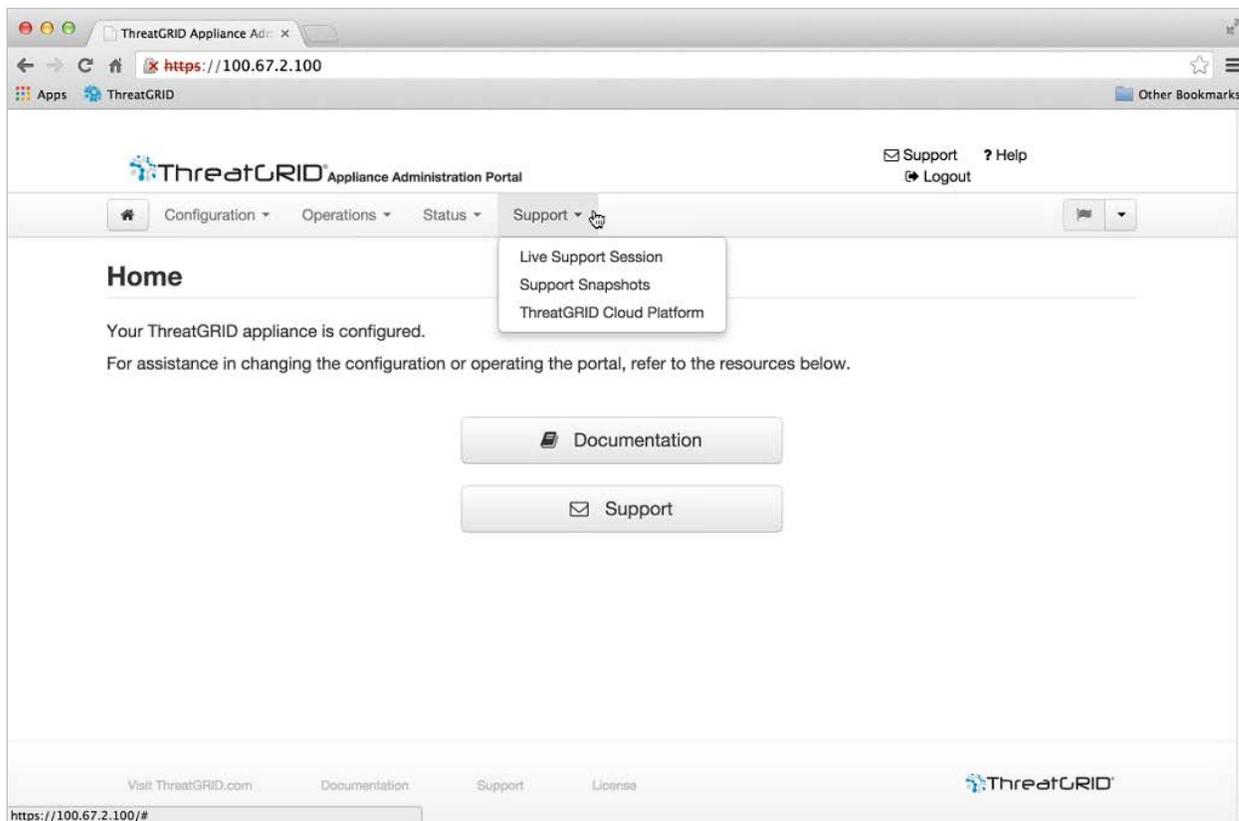
## 状态 (Status) 菜单

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。