连接 Threat Grid 设备

2.0.3 版

最后更新时间： 2016 年 6 月 6 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。

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 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做出了其他担保，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。

《连接 Threat Grid 设备》包含《思科 AMP Threat Grid 设备管理员指南》中的“SSL 证书”部分

目录

目录 i

插图目录 i

SSL 证书和 THREAT GRID 设备 1
使用 SSL 的接口 1
支持的 SSL/TLS 版本 1
不支持 SSL 证书 1
SSL 证书 - 自签名的默认设置 1
为入站连接配置 SSL 证书 1
CN 验证 2
替换 SSL 证书 2
重新生成 SSL 证书 3
下载 SSL 证书 3
上传 SSL 证书 3
生成您自己的 SSL 证书 - 使用 OpenSSL 的示例 3
为出站连接配置 SSL 证书 5
配置 DNS 5
CA 证书管理 5
安全状态更新服务管理 5
将 ESA/WSA 设备连接到 Threat Grid 设备 6
到 ESA/WSA 文档的链接 6
在 Threat Grid 设备上激活新设备用户帐户。 7
将 Threat Grid 设备连接到思科 FireAMP 私有云 7
管理 Threat Grid 组织和用户 12

隐私和样本可见性 13
Threat Grid 设备上的隐私和可见性 13

插图目录

图 1 - SSL 证书配置页面 2
图 2 - 用户详细信息 (User Details) 页面 > 重新激活用户 7
图 3 - Threat Grid 设备上的隐私和可视性 14

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、FireAMP 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：

- **Clean** 接口，用于 Threat Grid 门户 UI 和 API，以及集成（ESA/WSA 设备、FireAMP 私有云安全状态更新服务等）
- **Admin** 接口，用于 **OpAdmin 门户**。

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：2.0.3 版通过允许客户导入其自己的受信任证书或 CA 证书来解决这些限制。

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。

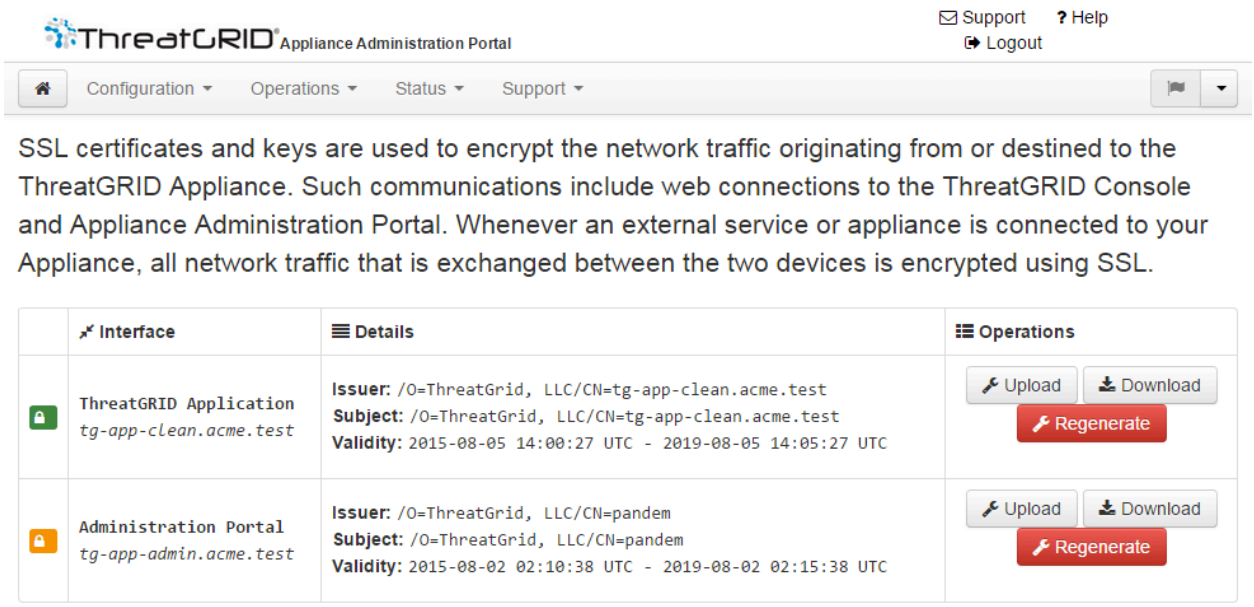
为入站连接配置 SSL 证书

其他思科产品（例如 ESA 和 WSA 设备以及 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，因此您需要将其从 TGA 导出（首先确保它在 CN 字段中使用正确的主机名，并在必要时重新生成或替换主机名），然后将其导入到集成设备或服务。

Threat Grid 设备上用于入站 SSL 连接的证书在 **SSL 证书配置 (SSL Certificate Configuration)** 页面中配置。**Clean** 接口和 **Admin** 接口的 SSL 证书可以独立配置。

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

图 1 - 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，彩色的挂锁图标指示 TG 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。

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。为了支持在 Threat Grid 设备和其他思科设备与服务之间进行集成，可能还需要添加或替换 SSL 证书。

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 FireAMP 私有云集成在一起以使用其安全状态更新服务的情况下，需要安装 FireAMP 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 (SSL Certificate Configuration)** 页面中，点击**重新生成 (Regenerate)**。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”(SSL Certificate Configuration) 页面中，点击要获得的证书旁边的**下载 (Download)。**随即会下载 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。

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。

  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")。

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

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，并且还将其上传到 ESA/WSA 设备（仅 .cert）。

为出站连接配置 SSL 证书

Threat Grid 设备 2.0.3 版包含用于支持与 FireAMP 私有云安全状态更新服务进行集成的功能。

配置 DNS

默认情况下，DNS 使用 Dirty 接口。如果因为使用 Clean 接口进行集成而无法通过 Dirty 接口解析集成设备或服务（例如 FireAMP 私有云）的主机名，则可以在 OpAdmin 中配置一个使用 Clean 接口的单独 DNS 服务器。

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

CA 证书管理

2.0.3 版添加的其中一个功能是增加了一个面向*出站* SSL 连接的 CA 证书管理信任库 (truststore) 的新页面，因此 TGA 可以信任 FireAMP 私有云，以通知有关被视为恶意的分析样本的信息。

在 **OpAdmin** 中，依次选择**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)**，然后点击**检索 (Retrieve)**。系统将检索证书。

或

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

3. 点击**导入 (Import)**。

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 (My Account)** 下拉菜单选择**管理 FireAMP 集成 (Manage FireAMP Integration)**。“安全状态更新服务”(Disposition Update Service) 页面随即打开。
2. 输入 FireAMP 配置门户提供的 **FireAMP 私有云 URL (FireAMP Private Cloud URL)**、**管理员用户名 (admin user name)** 和**密码 (password)**，然后点击**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。思科沙盒 API（“CSA API”）支持在 Threat Grid 设备和 ESA/WSA 设备进行集成，通常称为“CSA 集成”。

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

集成设备必须向 Threat Grid 设备注册后才能提交样本以供分析。在集成 ESA/WSA 设备可以向 Threat Grid 设备注册前，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 设备以便与集成 ESA/WSA 设备和其他思科产品通信所需的步骤。

到 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. 主机名必须与 CN 和 ESA/WSA 预期匹配

   Threat Grid 设备 SSL 证书中的 CN 必须与其当前主机名匹配。要成功连接集成 ESA/WSA 设备，这也必须是集成 ESA/WSA 设备用于识别 TGA 的同一主机名。

   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 CN 字段中使用当前主机名，然后将其下载到您的工作环境，再上传并安装在集成 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：为入站连接配置 SSL 证书。

   完成 SSL 证书设置后，下一步就是验证 Threat Grid 设备和 ESA/WSA 设备是否可以彼此通信。

2. 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

   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。）

3. 向 Threat Grid 设备注册思科 ESA/WSA/其他设备。

   根据产品的文档配置的 ESA/WSA 设备会自动向 Threat Grid 设备自行注册。

4. 完成 ESA/WSA 文件分析配置。

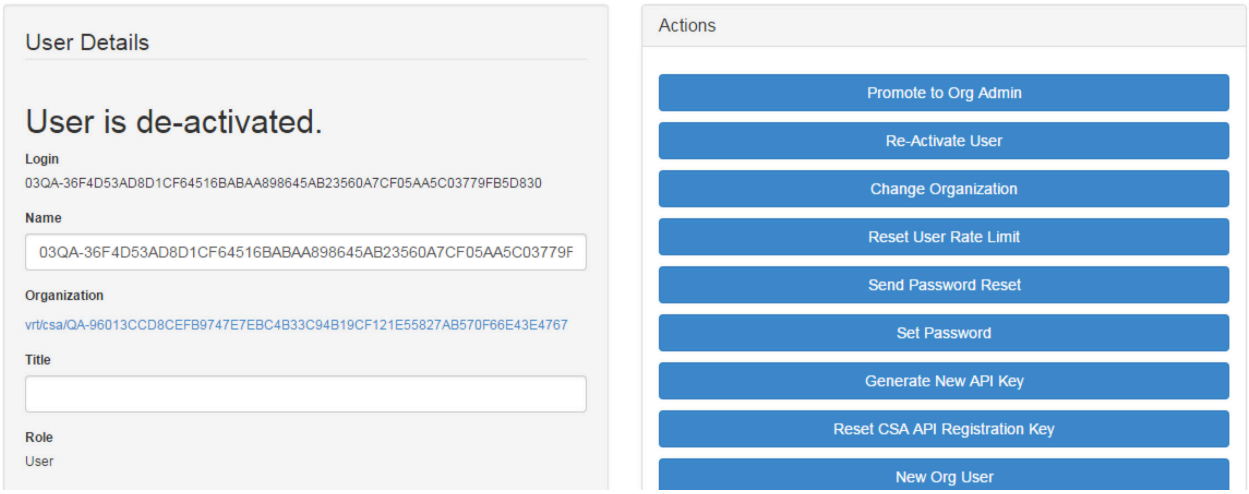
在连接设备注册后，会使用设备 ID 作为登录 ID 自动创建一个新的 Threat Grid 用户，同时会基于同一 ID 创建一个新组织。新的设备用户帐户必须由管理员激活，如下一节所述。

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”(de-activated)。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。
2. 从导航栏**欢迎 (Welcome)** 菜单选择**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（可能需要使用“搜索”[Search] 来查找）。用户状态当前为“已停用”(de-activated)。

图 2 - 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

必须按以下顺序在设备上执行 Threat Grid 设备安全状态更新服务和 FireAMP 私有云集成设置任务，尤其是在设置新设备时。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。

有关必须在此侧执行的任务的详细信息，请参阅 FireAMP 私有云的文档。

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
1	如常设置和配置 Threat Grid 设备（“TGA”）（即尚未集成）。	
2		如常设置和配置 FireAMP 私有云（“TGA”）（即尚未集成）。
3		**为 TGA 集成配置 FireAMP 私有云：** 依次选择**集成 (Integrations) > Threat Grid**，然后转至**到 Threat Grid 的连接 (Connection to 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。

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
3.1	**SSL 证书：** 在 Threat Grid 设备 OpAdmin 界面中，依次选择**配置 (Configuration) > SSL**。如有需要，重新生成新的 SSL 证书以替换默认证书，然后下载该证书并安装在 FireAMP 私有云上。（在“SSL 证书和 THREAT GRID 设备”中说明了 TGA SSL 证书。） **主机名** 依次选择**配置 (Configuration) > 主机名 (Hostname)** **API 密钥**： 或许可以在 Threat Grid Face 门户用户界面中，于即将用于集成的帐户的**用户详细信息 (User Details)** 页面内找到 API 密钥： 1. 转至 **Threat Grid 门户用户界面**。 2. 从右上角的“欢迎”(Welcome) 菜单（位于导航栏的右上角），选择**管理用户 (Manage Users)**。 3. 导航（如有必要，使用“搜索”[Search]）至集成用户帐户的**用户详细信息 (User Details)** 页面，然后复制 **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。	

步骤	Threat Grid 设备（“TGA”）	FireAMP 私有云
3.2		完成**到 Threat Grid 的连接 (Connection to 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”(Save Configuration)。 5. 点击“测试连接”(Test Connection)。 6. 连接测试通过后，您将需要在 FireAMP 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 FireAMP 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	

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。但是默认情况下，DNS 使用 Dirty 接口。如果无法通过 Dirty 接口解析 FireAMP 私有云主机名，则可以在 OpAdmin 中配置一个使用 Clean 接口的单独 DNS 服务器。 在 OpAdmin 中，依次选择**配置 (Configuration) > 网络 (Network)**，再为 **Dirty** 和 **Clean** 网络填写 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，以便其可以信任集成设备： 1. 在 OpAdmin 中，依次选择**配置 (Configuration) > CA 证书 (CA Certificates)**。您可以选择一个 SSL 证书以从 FireAMP 私有云主机导入，或从剪贴板导入。 2. 选择要导入的证书，然后单击**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 设备安全状态服务的**主机 (Host)** 和**端口 (Port)**，然后点击**检索 (Retrieve)**。 3. 系统将检索证书。 4. 点击**导入 (Import)**。 （或者点击**从剪贴板导入 (Import from Clipboard)**。从剪贴板粘贴 PEM，然后点击**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 门户用户界面中，从右上角菜单选择**管理 FireAMP 集成 (Manage FireAMP Integration)**。“处理更新服务”(Disposition Update Service) 窗口随即打开。 输入 AMP 安全状态更新服务 URL（您可以在 FireAMP 设备中找到此 URL：依次选择**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)**，然后点击**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。

有关管理组织的信息，请参阅《*Threat Grid 设备管理员指南*》，可以在 Cisco.com 上的**“Threat Grid 安装和升级”页面**中找到该指南。

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）的说明和文档，请参阅 Threat Grid 门户用户界面的联机帮助。从导航栏依次选择**帮助 (Help) > 使用 Threat Grid 联机帮助 (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，则隐私问题尤为重要。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。如果将样本提交到现场 Threat Grid 设备而不是提交到 Threat Grid 云，则此问题也不算什么，但是了解隐私和样本可见性的基础知识对 TGA 管理员而言仍然非常有必要。

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 3 - 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应用于 Threat Grid 设备与 FireAMP 私有云的集成。