关于 Cisco Secure Firewall Threat Defense REST API

您可以通过 HTTPS 使用 Cisco Secure Firewall Threat Defense 具象状态传输 (REST) 应用编程接口 (API) 利用客户端程序与 威胁防御 设备交互。REST API 使用 JavaScript 对象表示法 (JSON) 格式表示对象。

Secure Firewall 设备管理器 包括一个 API Explorer（该资源管理器对可供您编程使用的所有资源和 JSON 对象进行说明）。Explorer 提供有关各对象中属性值对的详细信息，您可以尝试不同的 HTTP 方法，确保了解使用各资源所需的编码。API Explorer 还提供各资源所需的 URL 示例。

您还可以在 https://developer.cisco.com/site/ftd-api-reference/上找到参考信息和示例。

API有其自己的版本号。无法保证设计用于一个API版本的客户端能够准确无误地用于将来的版本，且无需修改程序。

此编程指南的受众

本指南假设您对编程有基本认识并对REST API和JSON有特定理解。如果您不熟悉这些技术，请首先阅读有关 REST API 的一般指南。

支持的 HTTP 方法

仅可使用以下 HTTP 方法。不支持其他方法。

- GET - 从系统读取数据。

- POST - 创建新对象。
- PUT - 修改现有对象。使用 PUT 时，必须包含整个 JSON 对象。无法选择性地更新对象内的个别属性。
- DELETE - 删除用户定义的对象。

API 基准 URL

确定给定 威胁防御 设备基准 URL 的最简单方法是在 API Explorer 中尝试 GET 方法，且仅从结果中删除 URL 的对象部分。

例如，可执行 GET /object/networks，并在请求 URL 下的返回输出中看到与下面类似的内容：

```
https://ftd.example.com/api/fdm/v1/object/networks
```

URL 服务器名称部分是 威胁防御 设备的主机名或 IP 地址，因您的设备而不同，代替“ftd.example.com”。在本例中，从路径中删除 /object/networks 以获取基准 URL：

```
https://ftd.example.com/api/fdm/v1/
```

所有资源调用均将此 URL 作为请求 URL 的基础。

如果更改了 HTTPS 数据端口，则必须在 URL 中包含该自定义端口。例如，如果您将端口更改为 4443，则 URL 应为 https://ftd.example.com:4443/api/fdm/v1/

URL 中的“v”元素是 API 版本，通常随软件版本变化。例如，威胁防御 版本 6.3.0 的 API 版本是 v2，因此基准 URL 为：

```
https://ftd.example.com/api/fdm/v2/
```

注释 从 威胁防御 6.4 开始，可以在路径中使用 **latest** 代替 v 元素，从而无需在 API 调用中更新路径。例如，https://ftd.example.com/api/fdm/latest/。**latest** 别名将解析为设备支持的最新 API 版本。

在 API Explorer 中，如果滚动至页面底部，则可看到有关基准 URL（无服务器名称）和 API 版本的信息。

保护 REST API 的 SSL/TLS 通信

威胁防御设备附带自签证书，以便可以发起与设备的 HTTPS 通信。但是，由于证书并非由已知证书颁发机构 (CA) 签名，因此任何 SSL/TLS 访问尝试均将认为连接不安全。

使用浏览器进行连接时，系统会提示您接受自签证书，但 curl 等命令会拒绝该证书。对于 curl，可以通过添加 **--insecure** 关键字来避免证书检查失败。例如：

```
curl --insecure -X GET --header 'Accept: application/json'
'https://ftd.example.com/api/versions'
```

您应该做的第一件事是获取 威胁防御设备的 CA 签名设备证书。然后，使用 设备管理器 或 API 将此证书分配为管理证书。随后，SSL/TLS 证书检查应该不会失败，且无需在 API 调用中使用不安全的通信。

过程

步骤 1 使用 **POST /object/internalcertificates** 资源上传 CA 签名的设备证书。

步骤 2 使用 **PUT /devicesettings/default/webuicertificates/{objId}** 资源将此证书设置为管理证书。

使用 **GET /devicesettings/default/webuicertificates** 资源确定 Web UI 证书的对象 ID。

步骤 3 使用 **POST /operational/deploy** 资源部署更改。

确定支持的 API 版本

您可以使用 GET/api/versions (ApiVersions) 方法确定设备支持的 API 版本。此方法不需要身份验证，也不包括路径中的版本元素。例如：

```
curl -X GET --header 'Accept: application/json' 'https://ftd.example.com/api/versions'
```

“ftd.example.com”替换为 威胁防御 设备的主机名或 IP 地址。

此方法返回您可以使用的 API 版本的列表。例如：

```
{
    "supportedVersions":["v3", "latest"]
}
```

版本字符串与您在后续 API 调用的 URL 中使用的版本字符串相同。如果使用的是 **latest** 而不是特定版本标识符，则可避免为后续版本更新调用。但是，使用此方法无法克服更改调用中使用的对象模型的问题，这可能需要随着不同版本的发行而进行调整。

通常情况下，下一步是获取访问令牌，如使用 OAuth 对 REST API 客户端进行身份验证中所述。

API 版本向后兼容性

威胁防御 API 版本随 威胁防御 软件的每个主要版本而变化。新功能会影响要添加或更改的功能的 API 调用。

但是，许多功能在各版本之间不会发生变化。例如，与网络和端口对象相关的 API 在新版本中通常保持不变。

从 威胁防御 版本 6.7 开始，如果某项功能的 API 资源模型在各版本之间未更改，则 威胁防御 API 可以接受基于较早 API 版本的调用。即使功能模型发生了变化，如果有将旧模型转换为新模型的合理方法，旧的调用也仍然可用。例如，可以在 v6 系统上接受 v5 调用。如果在调用中使用“latest”作为版本号，则在此场景中，这些“较早”的调用将被解释为v6调用，因此，是否要利用向后兼容性取决于 API 调用的构建方式。

如果某个功能模型在API版本之间发生了更改，导致无法支持向后兼容，则您会收到一条错误消息，您需要检查这些错误并为这些特定调用更新代码。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。