配置安全访问安全配置文件API高级

目录

问题

当尝试通过公共API配置思科安全访问安全配置文件时，用户会遇到限制，即只能使用默认设置创建基本配置文件。API不公开高级安全功能的精细配置选项，包括：

- TLS解密设置
- 威胁类别实施控制
- 文件类型阻止和检查
- 恶意软件检测设置

用户报告在尝试通过标准API调用配置解密设置时收到“403 Forbidden”错误。记录的公共API终端似乎缺少可通过GUI界面提供的详细安全配置文件配置参数，从而限制了编程管理功能。

环境

- 思科安全接入平台
- 安全配置文件API实施
- 所有受影响的软件版本
- 公共API文档端点

分辨率

高级安全配置文件配置功能可通过思科安全访问API获得，但需要特定的实施方法和不同于已记录的公共API示例的字段命名约定。这些解决步骤针对每个配置区域：

基本安全配置文件创建工作流程

使用高级设置创建安全配置文件的正确工作流程分为两步：

步骤 1：使用POST创建基本安全配置文件。

```
POST /api/v1/security-profiles
{
  "name": "profile_name",
  "description": "profile_description"
}
```

步骤 2：使用PUT和配置文件ID配置高级选项。

```
PUT /api/v1/security-profiles/{profile_id}
{
  "advanced_settings": {
    "decryption_settings": {...},
    "file_settings": {...},
    "threat_settings": {...}
  }
}
```

文件检查和文件类型阻止配置

可以在PUT请求中使用以下API字段名称配置文件检查和文件类型阻止：

- fileEngine — 控制文件检查功能。
- fileTypeControlStatus — 启用或禁用文件类型阻止。

文件设置的配置示例：

```
{
  "fileEngines": "enabled",
  "fileTypeControlStatus": "active",
  "blockedFileTypes": ["exe", "zip", "rar"]
}
```

TLS解密配置

TLS解密配置需要引用Do Not Decrypt列表ID，而不是使用专用POST终端。通过以下方法通过PUT API请求实现配置：

步骤 1：从现有配置中识别Do Not Decrypt list ID。

步骤 2：引用PUT API请求中的列表ID。

```
{
  "seetingGroupBypassInspectionGroupID": "do_not_decrypt_list_id",
  "decryptionEnabled": true
}
```

这解决了尝试通过其他API方法配置解密时发生的“403 Forbidden”错误。

威胁类别配置

威胁类别配置可通过未记录的API终端提供，该终端在成功解密配置后可访问。终端允许精细的威胁类别控制，但要求首先使用解密设置正确配置安全配置文件。

API字段名称参考

下表将常见的安全配置文件功能映射到其对应的API字段名称：

功能	API字段名称	描述
TLS解密	settingGroupBypassInspectionGroupID	引用不解密列表ID
文件检查	文件引擎	控制文件检查功能
文件类型阻止	fileTypeControlStatus	启用文件类型限制

原因

限制主要是因为API文档不完整以及字段命名规则不直观，而不是实际功能限制。高级安全配置文件配置功能存在于API中，但通过以下方式实施：

- 与GUI术语不同的非明显字段名称
- 两步工作流（POST用于创建，PUT用于高级配置）
- 依赖现有配置对象（例如Do Not Decrypt列表）
- 针对某些功能的未记录的API终端

公共API文档没有清楚地显示这些实施细节，因此当通过替代方法实际提供功能时，会感觉到API限制。

相关内容

- 思科安全访问安全配置文件API文档
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。