Configurar Perfis de Segurança de Acesso Seguro API Avançado

Contents

Problema

Ao tentar configurar os Perfis de Segurança de Acesso Seguro da Cisco por meio da API pública, os usuários encontram limitações em que apenas a criação de perfil básico com configurações padrão é possível. A API não expõe opções de configuração granulares para recursos de segurança avançados, incluindo:

- Configurações de descriptografia TLS
- Controles de aplicação da categoria de ameaças
- Bloqueio e inspeção de tipo de arquivo
- Configurações de inspeção de malware

Os usuários relatam o recebimento de erros "403 Forbidden" ao tentar definir as configurações de descriptografia por meio de chamadas de API padrão. Os endpoints de API públicos documentados parecem não ter os parâmetros de configuração do perfil de segurança detalhado que estão disponíveis através da interface GUI, limitando os recursos de gerenciamento programático.

Ambiente

- Plataforma Cisco Secure Access
- Implementação da API de perfis de segurança
- Todas as versões de software afetadas
- Pontos de extremidade de documentação de API pública

Resolução

Os recursos avançados de configuração do perfil de segurança estão disponíveis por meio da API do Cisco Secure Access, mas exigem abordagens de implementação específicas e convenções de nomeação de campo que diferem dos exemplos de API pública documentados. Estas etapas de resolução abordam cada área de configuração:

Fluxo de Trabalho Básico de Criação de Perfil de Segurança

O fluxo de trabalho apropriado para a criação de perfis de segurança com configurações avançadas segue um processo de duas etapas:

Passo 1: Crie o perfil de segurança básico usando o POST.

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

Passo 2: Configure as opções avançadas usando PUT com a ID do perfil.

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

Inspeção de arquivo e configuração de bloqueio de tipo de arquivo

A inspeção de arquivo e o bloqueio de tipo de arquivo podem ser configurados usando estes nomes de campo de API na solicitação PUT:

- fileEngines - Controla os recursos de inspeção de arquivos.
- fileTypeControlStatus - Habilita ou desabilita o bloqueio de tipo de arquivo.

Exemplo de configuração para configurações de arquivo:

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

Configuração de descriptografia TLS

A configuração de descriptografia TLS requer a referência a uma ID de lista Não descriptografar, em vez de usar um endpoint dedicado de POST. A configuração é implementada através da solicitação da API PUT usando esta abordagem:

Passo 1: Identifique a ID da lista Não descriptografar da configuração existente.

Passo 2: Consulte a ID da lista na solicitação da API PUT.

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

Isso resolve o erro "403 Forbidden" que ocorre ao tentar configurar a descriptografia por outros métodos de API.

Configuração da categoria de ameaças

A configuração da categoria de ameaças está disponível por meio de um endpoint de API não documentado que se torna acessível após a configuração de descriptografia bem-sucedida. O ponto de extremidade permite o controle granular da categoria de ameaças, mas exige que o Perfil de segurança seja configurado corretamente primeiro com as configurações de descriptografia.

Referência do Nome do Campo da API

Esta tabela mapeia os recursos comuns do Perfil de segurança para os nomes de campo da API correspondente:

Recurso	Nome do campo de API	Descrição
Descriptografia TLS	definindoGroupBypassInspectionGroupID	As referências não descriptografam a ID da lista
Inspeção de arquivo	fileEngines	Controla os recursos de inspeção de arquivos
Bloqueio de tipo de arquivo	fileTypeControlStatus	Habilita restrições de tipo de arquivo

Causa

A limitação se deu principalmente devido à documentação incompleta da API e a convenções de nomenclatura de campo não intuitivas, em vez de restrições funcionais reais. Os recursos avançados de configuração do perfil de segurança existem dentro da API, mas são implementados usando:

- Nomes de campo não óbvios que diferem da terminologia da GUI
- Um fluxo de trabalho de duas etapas (POST para criação, PUT para configuração avançada)
- Dependências em objetos de configuração existentes (como listas Não descriptografar)
- Endpoints de API não documentados para determinados recursos

A documentação da API pública não expõe claramente esses detalhes de implementação, levando à percepção das limitações da API quando a funcionalidade está realmente disponível por meio de abordagens alternativas.

Conteúdo relacionado

- Documentação da API de perfis de segurança do Cisco Secure Access
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.