

Configurar Inclusão e Exclusão de Política DLP

Contents

Introdução

Este documento descreve como usar as opções de inclusão e exclusão nas políticas DLP para adaptar as regras de prevenção de perda de dados a identidades específicas.

Overview

As opções de inclusão e exclusão nas políticas DLP permitem definir com precisão quais identidades são cobertas pelas suas regras de prevenção contra perda de dados. Você pode incluir ou excluir usuários ou grupos específicos, fornecendo um controle mais granular sobre a aplicação da política.

Utilizar opções de inclusão e exclusão de políticas de DLP

Regras DLP em tempo real

- No painel Umbrella ou Secure Access, crie ou edite uma regra DLP em Tempo Real.
- Vá para a seção Destino.
 - Agora você pode incluir e excluir identidades (usuários ou grupos) da mesma lista.
- Isso permite aplicar ações DLP somente às identidades especificadas ou isentar determinadas identidades, conforme necessário.

Identities

Select identities to add them to this rule.

Select identities

All Identities

☐	AD Groups	8 >
☐	AD Users	32 >
☐	Tunnels	2 >
☐	Networks	10 >
☐	Roaming Computers	4 >

0 Selected for Exclusion

None selected.

You may add identities by selecting items on the left.

☒ Select identities for exclusion

Select identities

All Identities

☐	AD Groups	8 >
☐	AD Users	32 >
☐	Tunnels	2 >
☐	Networks	10 >
☐	Roaming Computers	4 >

0 Selected for Exclusion

None selected.

You may add identities by selecting items on the left.

Regras de API DLP do SaaS

- Na configuração de regra de DLP da API SaaS, vá para a seção Incluir e Excluir.
 - Aqui, você pode especificar quais usuários do Ative Directory (AD) e grupos do AD devem ser incluídos ou excluídos ao mesmo tempo.
- Isso permite aplicar políticas DLP em identidades selecionadas ou impedir que as políticas sejam aplicadas a determinados usuários ou grupos.

Encontre mais informações

Consulte a documentação do Umbrella e do Secure Access para obter instruções passo a passo:

Guarda-chuva:

- [Adicionar uma Regra em Tempo Real à Política de Prevenção de Perda de Dados](#)
- [Adicionar uma regra de API de SaaS à política de prevenção de perda de dados](#)

Acesso seguro:

- [Adicionar uma Regra em Tempo Real à Política de Prevenção de Perda de Dados](#)
- [Adicionar uma regra de API de SaaS à política de prevenção de perda de dados](#)

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.