

# Pesquisar e exibir autenticações SAML no aplicativo de segurança de e-mail

## Contents

[Introduction](#)

[Informações de Apoio](#)

[Requirements](#)

[Componentes Utilizados](#)

[Como faço para pesquisar e exibir os logs de autenticação de uma solicitação de login SAML no ESA?](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como pesquisar entradas de log que mostram como o Email Security Appliance (ESA) processa uma solicitação de Autenticação SAML.

## Informações de Apoio

O Cisco Email Security Appliance (ESA) permite o login do SSO para o acesso do usuário final à Quarentena de spam e administradores que usam a interface de usuário de administração, com suporte a SAML, um formato de dados padrão aberto baseado em XML que permite aos administradores acessar um conjunto definido de aplicativos sem interrupções após o login em um desses aplicativos.

Para saber mais sobre SAML, consulte: [Informações Gerais de SAML](#)

## Requirements

- Email Security Appliance com autenticação externa configurada.
- Integração SAML com qualquer Provedor de Identidade.

## Componentes Utilizados

- Acesso do Email Security Appliance à CLI (Command Line Interface, interface de linha de comando).
- Assinatura de logs de GUI
- Extensão do SAML DevTools. Para obter mais informações, consulte: [Devtools SAML para Chrome](#)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Como faço para pesquisar e exibir os logs de autenticação de uma solicitação de login SAML no ESA?

A inscrição no log de autenticação não exibe informações sobre solicitações de logon SAML. No entanto, as informações são registradas em logs da GUI.

O nome do log é *gui\_logs* e o tipo de log é *Http\_logs*. Você pode ver isso no **Administração do sistema > Inscrições de log > gui\_logs**.

Você pode acessar estes logs:

Da linha de comando:

- Use um cliente SSH como Putty. Faça login na CLI do dispositivo ESA através da porta 22/SSH.
- Na linha de comando, escolha `grep` para procurar o endereço de e-mail do usuário que solicitou o acesso.

Depois que o CLI for carregado, você poderá procurar o `Email address`, conforme exibido neste comando:

```
(Machine esa.cisco.com) (SERVICE)> grep "username@cisco.com" gui_logs
```

Para um login bem-sucedido, você verá três entradas:

1. Uma solicitação SAML gerada pelo ESA que solicita ao provedor de identidade configurado os dados de autenticação e autorização.

```
GET /login?action=SAMLRequest
```

2. Uma declaração SAML de notificação foi estabelecida corretamente.

```
Destination:/ Username:usernamehere@cisco.com Privilege:PrivilegeTypeHere session:SessionIdHere Action: The HTTPS session has been established successfully.
```

3. Resultado da notificação de SSO.

```
Info: SSO authentication is successful for the user: username@cisco.com.
```

Se essas três entradas não forem exibidas, a solicitação de autenticação não será bem-sucedida e estará relacionada a estes cenários:

Cenário 1: se apenas a solicitação SAML for exibida nos logs.

```
GET /login?action=SAMLRequest
```

O provedor de identidade rejeita a solicitação de autenticação, pois o usuário não está atribuído ao aplicativo SAML ou uma URL incorreta do provedor de identidade não foi adicionada ao ESA.

Cenário 2: Se as entradas de log

```
Authorization failed on appliance, While fetching user privileges from group mapping@ An error occurred during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response SÃO
```

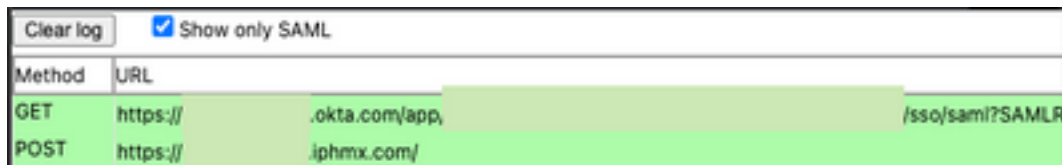
exibidos nos logs.

An error occurred during SSO authentication. Details: User: usernamehere@cisco.com Authorization failed on appliance, While fetching user privileges from group mapping.

An error occurred during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response.

Verifique as permissões de usuário e os grupos atribuídos ao aplicativo SAML na configuração do Provedor de identidade.

Como alternativa, a extensão SAML DevTools pode ser usada para recuperar respostas de aplicativos SAML diretamente do navegador da Web, como mostrado na imagem :



The image shows a screenshot of the SAML DevTools extension interface. At the top, there is a 'Clear log' button and a checked checkbox labeled 'Show only SAML'. Below this is a table with two columns: 'Method' and 'URL'. The table contains two entries: a GET request to 'https://...okta.com/app, .../sso/saml?SAMLR' and a POST request to 'https://...iphmx.com/'.

Method	URL
GET	https://...okta.com/app, .../sso/saml?SAMLR
POST	https://...iphmx.com/

## Informações Relacionadas

[Guia do usuário do Cisco Secure Email Gateway](#)

[Extensão do SAML DevTools](#)

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.