

Buscar y ver autenticaciones SAML en el dispositivo de seguridad de correo electrónico

Contenido

[Introducción](#)

[Antecedentes](#)

[Requirements](#)

[Componentes Utilizados](#)

[¿Cómo puedo buscar y ver los registros de autenticación para una solicitud de inicio de sesión SAML en el ESA?](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo buscar entradas de registro que muestran cómo el dispositivo de seguridad de correo electrónico (ESA) procesa una solicitud de autenticación SAML.

Antecedentes

El dispositivo de seguridad Cisco Email Security Appliance (ESA) permite el inicio de sesión SSO para el acceso del usuario final a Spam Quarantine y los administradores que utilizan la interfaz de usuario de administración, con compatibilidad con SAML, un formato de datos estándar abierto basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones sin problemas después de iniciar sesión en una de esas aplicaciones.

Para obtener más información sobre SAML, consulte: [Información general sobre SAML](#)

Requirements

- Dispositivo de seguridad de correo electrónico con autenticación externa configurada.
- Integración de SAML con cualquier proveedor de identidad.

Componentes Utilizados

- Acceso del dispositivo de seguridad Email Security Appliance a la interfaz de línea de comandos (CLI).
- Suscripción a registros de Gui
- Extensión de SAML DevTools. Para obtener más información, consulte: [SAML Devtools for Chrome](#)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

¿Cómo puedo buscar y ver los registros de autenticación para una solicitud de inicio de sesión SAML en el ESA?

La suscripción al registro de autenticación no muestra información sobre las solicitudes de inicio de sesión SAML. Sin embargo, la información se registra en los registros de la GUI.

El nombre del registro es *gui_logs* y el tipo de registro es *Http_logs*. Puede ver esto en la **Administración del sistema > Suscripciones de registro > gui_logs**.

Puede acceder a estos registros:

Desde la línea de comandos:

- Utilice un cliente SSH como Putty. Inicie sesión en la CLI del dispositivo ESA a través del puerto 22/SSH.
- En la línea de comandos, elija `grep` para buscar la dirección de correo electrónico del usuario que solicitó el acceso.

Una vez que la CLI se ha cargado, puede buscar el `Email address`, como se muestra en este comando:

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

Para que el inicio de sesión se realice correctamente, verá tres entradas:

1. Solicitud SAML generada por ESA que solicita al proveedor de identidad configurado los datos de autenticación y autorización.

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

2. Se estableció correctamente una afirmación SAML de notificación.

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

3. Resultado de la notificación SSO.

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

Si no se muestran estas tres entradas, la solicitud de autenticación no es satisfactoria y está relacionada con estos escenarios:

Situación 1: si sólo se muestra la solicitud SAML en los registros.

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

El proveedor de identidad rechaza la solicitud de autenticación, ya que el usuario no está asignado a la aplicación SAML o no se ha agregado una URL de proveedor de identidad incorrecta al ESA.

Situación 2: si las entradas del registro

```
Authorization failed on appliance, While fetching user privileges from group mappingY An error occured during SSO authentication.
```

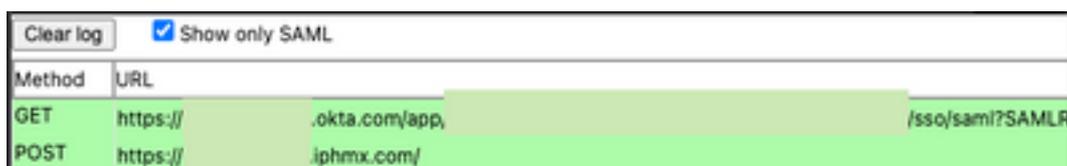
Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response **SE muestran en los registros.**

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.

Compruebe los permisos de usuario y los grupos asignados a la aplicación SAML en la configuración del proveedor de identidad.

Alternativamente, la extensión SAML DevTools se puede utilizar para recuperar las respuestas de la aplicación SAML del navegador web directamente, como se muestra en la imagen :



The image shows a screenshot of the SAML DevTools 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?SAML...' and a POST request to 'https://...iphmx.com/'.

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

Información Relacionada

[Guía del usuario de Cisco Secure Email Gateway](#)

[extensión SAML DevTools](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).