

Search and View SAML Authentications in the Email Security Appliance

Contents

[Introduction](#)

[Background Information](#)

[Requirements](#)

[Components Used](#)

[How do I Search and View the authentication logs for a SAML login request on the ESA?](#)

[Related Information](#)

Introduction

This document describes how to search for log entries that show how the Email Security Appliance (ESA) processes a SAML Authentication request.

Background Information

The Cisco Email Security Appliance (ESA) enables SSO login for end user access to Spam Quarantine and Administrators who use the administration user interface, with SAML support, an XML-based open standard data format that enables administrators to access a defined set of applications seamlessly after the sign into one of those applications.

To learn more about SAML, refer to: [SAML General Information](#)

Requirements

- Email Security Appliance with external authentication configured.
- SAML integration to any Identity Provider.

Components Used

- Email Security Appliance access to the Command Line Interface (CLI).
- Gui logs subscription
- SAML DevTools extension. For more information, refer to : [SAML Devtools for 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. If your network is live, ensure that you understand the potential impact of any command.

How do I Search and View the authentication logs for a SAML login request on the ESA?

The Authentication log subscription does not display information about SAML login requests.

However, the information is recorded in GUI logs.

The name of the log is *gui_logs* and the log type is *Http_logs*. You can see this in the **System Administration > Log Subscriptions > gui_logs**.

You can access these logs:

From the command line:

- Use a SSH client like Putty. Log in to the CLI of the ESA appliance via port 22/SSH.
- From the command line, choose grep to search for the Email address of the user who requested the access.

Once the CLI has loaded, you can search for the Email address, as displayed in this command:

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

For a successful login, you see three entries:

1. A SAML request generated by the ESA which asks the configured Identity Provider for the authentication and authorization data.

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

2. A notification SAML assertion was established correctly.

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

3. SSO notification result.

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

If these three entries are not displayed, the authentication request is not successful and it is related to these scenarios:

Scenario 1 : If only the SAML request is displayed in the logs.

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

The identity provider rejects the authentication request, due to the user is not assigned to the SAML application or an incorrect Identity Provider URL is not added to the ESA.

Scenario 2 : If the log entries

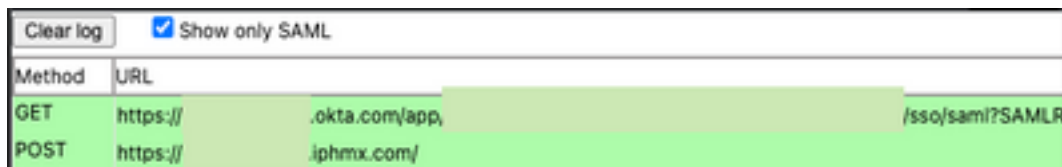
Authorization failed on appliance, While fetching user privileges from group mapping and An error occurred during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response are displayed in the logs.

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.

Check the user permissions and groups assigned to the SAML application in the Identity Provider configuration.

Alternatively, SAML DevTools extension can be used to retrieve SAML application responses from the web browser directly, as shown in the image :



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/

Related Information

[Cisco Secure Email Gateway User Guide](#)

[SAML DevTools extension](#)