

SAML-Authentifizierungen in der E-Mail Security Appliance suchen und anzeigen

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Wie kann ich die Authentifizierungsprotokolle für eine SAML-Anmeldeanforderung auf der ESA durchsuchen und anzeigen?](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie nach Protokolleinträgen suchen, die zeigen, wie die E-Mail Security Appliance (ESA) eine SAML-Authentifizierungsanfrage verarbeitet.

Hintergrundinformationen

Die Cisco E-Mail Security Appliance (ESA) ermöglicht die SSO-Anmeldung für den Endbenutzerzugriff auf die Spam-Quarantäne sowie Administratoren, die die Administrations-Benutzeroberfläche verwenden, mit SAML-Unterstützung, einem XML-basierten offenen Standarddatenformat, das es Administratoren ermöglicht, nach der Anmeldung bei einer dieser Anwendungen nahtlos auf einen definierten Satz von Anwendungen zuzugreifen.

Weitere Informationen zu SAML finden Sie unter: [Allgemeine Informationen zu SAML](#)

Anforderungen

- Email Security Appliance mit konfigurierter externer Authentifizierung
- SAML-Integration in jeden Identity Provider.

Verwendete Komponenten

- E-Mail Security Appliance-Zugriff auf die Kommandozeile (CLI)
- Abonnement für Gui-Protokolle
- SAML DevTools-Erweiterung. Weitere Informationen finden Sie unter: [SAML Devtools for Chrome](#)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Wie kann ich die Authentifizierungsprotokolle für eine SAML-

Anmeldeanforderung auf der ESA durchsuchen und anzeigen?

Das Authentifizierungsprotokollabonnement zeigt keine Informationen über SAML-Anmeldeanforderungen an. Die Informationen werden jedoch in GUI-Protokollen aufgezeichnet.

Der Name des Protokolls lautet *gui_logs*, und der Protokolltyp lautet *Http_logs*. Sie können dies im **Systemverwaltung > Protokoll-Subscriptions > gui_logs**.

Sie können auf folgende Protokolle zugreifen:

Über die Befehlszeile:

- Verwenden Sie einen SSH-Client wie Putty. Melden Sie sich über Port 22/SSH an der CLI der ESA-Appliance an.
- Wählen Sie in der Befehlszeile `grep` aus, um nach der E-Mail-Adresse des Benutzers zu suchen, der den Zugriff angefordert hat.

Nachdem die CLI geladen wurde, können Sie nach dem `Email address`, wie in diesem Befehl angezeigt:

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

Für eine erfolgreiche Anmeldung werden drei Einträge angezeigt:

1. Eine von der ESA generierte SAML-Anforderung, die den konfigurierten Identity Provider nach den Authentifizierungs- und Autorisierungsdaten fragt.

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

2. Eine SAML-Assertion für Benachrichtigungen wurde korrekt erstellt.

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

3. Ergebnis der SSO-Benachrichtigung.

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

Wenn diese drei Einträge nicht angezeigt werden, ist die Authentifizierungsanforderung nicht erfolgreich und hängt mit folgenden Szenarien zusammen:

Szenario 1: Wenn nur die SAML-Anfrage in den Protokollen angezeigt wird.

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

Der Identitätsanbieter lehnt die Authentifizierungsanforderung ab, da der Benutzer nicht der SAML-Anwendung zugewiesen wurde oder der ESA keine falsche Identitätsanbieter-URL hinzugefügt wurde.

Szenario 2: Wenn die Protokolleinträge

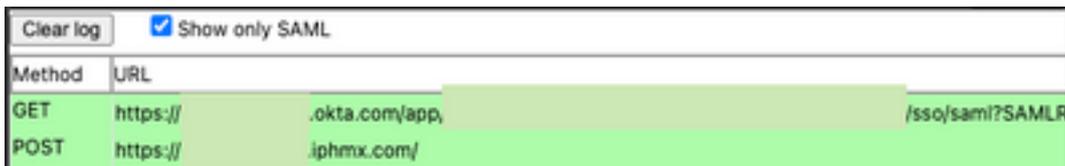
Authorization failed on appliance, While fetching user privileges from group mappingund An error occurred during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response werden in den Protokollen angezeigt.

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.

Überprüfen Sie die Benutzerberechtigungen und Gruppen, die der SAML-Anwendung in der Identity Provider-Konfiguration zugewiesen sind.

Alternativ kann die SAML DevTools-Erweiterung verwendet werden, um die Antworten der SAML-Anwendung direkt vom Webbrowser abzurufen, wie in der Abbildung dargestellt:



Method	URL
GET	https://[redacted].okta.com/app/[redacted]/sso/saml?SAMLRequest=[redacted]
POST	https://[redacted].iphmx.com/[redacted]

Zugehörige Informationen

[Benutzerhandbuch zu Cisco Secure Email Gateway](#)

[SAML DevTools-Erweiterung](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.