

SAML-verificaties zoeken en bekijken in de e-mail security applicatie

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Hoe zoek en bekijk ik de verificatielogboeken voor een SAML-inlogaanvraag op de ESA?](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u kunt zoeken naar logitems die laten zien hoe de E-mail security applicatie (ESA) een SAML-verificatieaanvraag verwerkt.

Achtergrondinformatie

De Cisco Email Security Applicatie (ESA) maakt SSO-aanmelding mogelijk voor toegang van eindgebruikers tot spamquarantaine en beheerders die de gebruikersinterface voor beheer gebruiken, met SAML-ondersteuning, een op XML gebaseerde open standaard dataformaat dat beheerders in staat stelt om naadloos toegang te krijgen tot een gedefinieerde set toepassingen na het ondertekenen in een van die toepassingen.

Voor meer informatie over SAML, raadpleegt u: [SAML General Information](#)

Vereisten

- E-mail security applicatie met externe verificatie geconfigureerd.
- SAML-integratie met een Identity Provider.

Gebruikte componenten

- E-mail security applicatie toegang tot de Command Line Interface (CLI).
- Gui-logboekabonnement
- SAML DevTools extensie. Raadpleeg voor meer informatie: [SAML Devtools for Chrome](#)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Hoe zoek en bekijk ik de verificatielogboeken voor een SAML-inlogaanvraag op de ESA?

Het logabonnement voor verificatie geeft geen informatie weer over de inlogaanvragen van SAML. De informatie wordt echter opgeslagen in GUI-logboeken.

De naam van het log is *gui_logs* en het logtype is *Http_logs*. U kunt dit zien in de **Systeembeheer > Log abonnementen > gui_logs**.

U hebt toegang tot deze logbestanden:

Vanaf de opdrachtregel:

- Gebruik een SSH client zoals Putty. Log in op de CLI van het ESA apparaat via poort 22/SSH.
- Kies in de opdrachtregel `grep` om te zoeken naar het e-mailadres van de gebruiker die om de toegang heeft gevraagd.

Nadat de CLI is geladen, kunt u zoeken naar de `Email address`, zoals weergegeven in deze opdracht:

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

Voor een succesvolle login, ziet u drie ingangen:

1. Een door de ESA gegenereerd SAML-verzoek dat de geconfigureerde Identity Provider vraagt om de authenticatie- en autorisatiegegevens.

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

2. Er is een correct bericht voor SAML-bewering opgesteld.

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

3. Resultaat van melding op SSO.

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

Als deze drie vermeldingen niet worden weergegeven, is het verificatieverzoek niet geslaagd en is het gerelateerd aan deze scenario's:

Scenario 1: Als alleen het SAML-verzoek in de logbestanden wordt weergegeven.

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

De identiteitsprovider wijst de verificatieaanvraag af omdat de gebruiker niet is toegewezen aan de SAML-toepassing of omdat er geen onjuiste URL voor de identiteitsprovider is toegevoegd aan de ESA.

Scenario 2: Indien de loggegevens

```
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 worden weergegeven in de logbestanden.

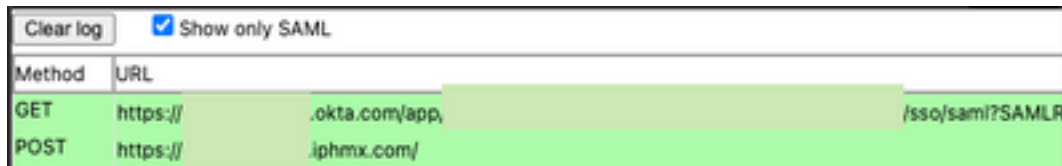
```
An error occurred during SSO authentication. Details: User: usernamehere@cisco.com Authorization failed on appliance, While fetching user privileges from group mapping.
```

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

Attributes values from IDP response.

Controleer de gebruikerstoestemmingen en groepen die aan de SAML-toepassing zijn toegewezen in de configuratie van de Identity Provider.

U kunt ook de extensie SAML DevTools gebruiken om direct de toepassingsreacties van SAML uit de webbrowser op te halen, zoals wordt getoond in de afbeelding:



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

Gerelateerde informatie

[Gebruikershandleiding voor Cisco Secure Email Gateway](#)

[extensie SAML DevTools](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.