

Ricerca e visualizzazione delle autenticazioni SAML in Email Security Appliance

Sommario

[Introduzione](#)

[Premesse](#)

[Requisiti](#)

[Componenti usati](#)

[Come fare per cercare e visualizzare i log di autenticazione per una richiesta di accesso SAML sull'ESA?](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come cercare le voci di log che mostrano come Email Security Appliance (ESA) elabora una richiesta di autenticazione SAML.

Premesse

Cisco Email Security Appliance (ESA) consente l'accesso SSO per l'accesso dell'utente finale alla quarantena della posta indesiderata e agli amministratori che utilizzano l'interfaccia utente di amministrazione, con supporto SAML, un formato di dati open standard basato su XML che consente agli amministratori di accedere senza problemi a una serie definita di applicazioni dopo aver effettuato l'accesso a una di esse.

Per ulteriori informazioni su SAML, vedere: [Informazioni generali su SAML](#)

Requisiti

- Email Security Appliance con autenticazione esterna configurata.
- Integrazione SAML in qualsiasi provider di identità.

Componenti usati

- Email Security Appliance accede all'interfaccia della riga di comando (CLI).
- Sottoscrizione log GUI
- Estensione SAML DevTools. Per ulteriori informazioni, fare riferimento a: [SAML Devtools for Chrome](#)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Come fare per cercare e visualizzare i log di autenticazione per

una richiesta di accesso SAML sull'ESA?

La sottoscrizione del log di autenticazione non visualizza informazioni sulle richieste di accesso SAML. Tuttavia, le informazioni vengono registrate nei log GUI.

Il nome del log è *gui_logs* e il tipo di log è *Http_logs*. È possibile visualizzare questa finestra nel **Amministrazione sistema > Sottoscrizioni registro > gui_logs**.

È possibile accedere ai seguenti registri:

Dalla riga di comando:

- Usare un client SSH come Putty. Accedere alla CLI dell'appliance ESA tramite la porta 2/SSH.
- Dalla riga di comando, scegliere grep per cercare l'indirizzo e-mail dell'utente che ha richiesto l'accesso.

Una volta caricata la CLI, è possibile cercare il Email address, come visualizzato in questo comando:

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

Per un accesso corretto, vengono visualizzate tre voci:

1. Una richiesta SAML generata dall'ESA che richiede al provider di identità configurato i dati di autenticazione e autorizzazione.

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

2. Asserzione SAML di notifica stabilita correttamente.

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

3. Risultato della notifica SSO.

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

Se queste tre voci non vengono visualizzate, la richiesta di autenticazione ha esito negativo ed è correlata ai seguenti scenari:

Scenario 1: se nei log viene visualizzata solo la richiesta SAML.

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

Il provider di identità rifiuta la richiesta di autenticazione perché l'utente non è assegnato all'applicazione SAML o perché all'ESA non è stato aggiunto un URL del provider di identità errato.

Scenario 2: se le voci del log

```
Authorization failed on appliance, While fetching user privileges from group mappinge An error occured during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response vengono visualizzati nei registri.
```

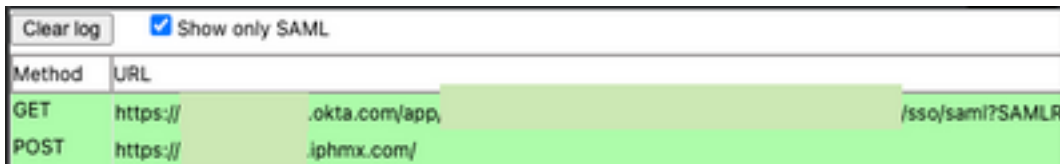
```
An error occured during SSO authentication. Details: User: usernamehere@cisco.com Authorization failed on appliance, While
```

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.

Verificare le autorizzazioni utente e i gruppi assegnati all'applicazione SAML nella configurazione del provider di identità.

In alternativa, è possibile utilizzare l'estensione SAML DevTools per recuperare le risposte dell'applicazione SAML direttamente dal browser Web, come mostrato nell'immagine:



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

Informazioni correlate

[Guida per l'utente di Cisco Secure Email Gateway](#)

[Estensione Strumenti di sviluppo SAML](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).