

EメールセキュリティアプライアンスでのSAML認証の検索と表示

内容

[概要](#)

[背景説明](#)

[要件](#)

[使用するコンポーネント](#)

[ESAでSAMLログイン要求の認証ログを検索して表示するにはどうすればよいですか。](#)

[関連情報](#)

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)がSAML認証要求を処理する方法を示すログエントリを検索する方法について説明します。

背景説明

Cisco Eメールセキュリティアプライアンス(ESA)では、エンドユーザがスパム隔離にアクセスするためのSSOログインと、管理ユーザインターフェイスを使用する管理者がSAMLサポートを利用できません。SAMLサポートは、XMLベースのオープン標準のデータ形式で、管理者がアプリケーションにサインインした後に、定義された一連のアプリケーションにシームレスにアクセスできるようにします。

SAMLの詳細については、「[SAMLの一般情報](#)」を参照してください。

要件

- 外部認証が設定されたEメールセキュリティアプライアンス。
- 任意のアイデンティティプロバイダーへのSAML統合。

使用するコンポーネント

- Eメールセキュリティアプライアンス(ESA)からコマンドラインインターフェイス(CLI)へのアクセス。
- Guiログサブスクリプション
- SAML DevTools拡張。詳細については、次のサイトを参照してください。 [SAML Devtools for Chrome](#)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ESAでSAMLログイン要求の認証ログを検索して表示するにはどうすればよいですか。

認証ログサブスクリプションには、SAMLログイン要求に関する情報は表示されません。ただし、情報はGUIログに記録されます。

ログの名前は *gui_logs* で、ログタイプは *Http_logs* です。これは、 [System Administration] > [Log Subscriptions] > [gui_logs]。

次のログにアクセスできます。

コマンドラインを使用する場合：

- PuttyなどのSSHクライアントを使用します。ポート22/SSH経由でESAアプライアンスのCLIにログインします。
- コマンドラインからgrepを選択し、アクセスを要求したユーザの電子メールアドレスを検索します。

CLIがロードされたら、Email address次のコマンドで表示されます。

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

正常にログインすると、次の3つのエントリが表示されます。

1. ESAによって生成されるSAML要求。設定されたアイデンティティプロバイダーに認証および許可データを要求します。

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

2. 通知SAMLアサーションが正しく確立されました。

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

を選択します。SSO通知結果。

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

これら3つのエントリが表示されない場合、認証要求は成功せず、次のシナリオに関連しています。

シナリオ1:SAML要求のみがログに表示される場合。

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

ユーザがSAMLアプリケーションに割り当てられていないか、誤ったアイデンティティプロバイダーURLがESAに追加されていないため、アイデンティティプロバイダーは認証要求を拒否します。

シナリオ2：ログエントリの場合

```
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
```

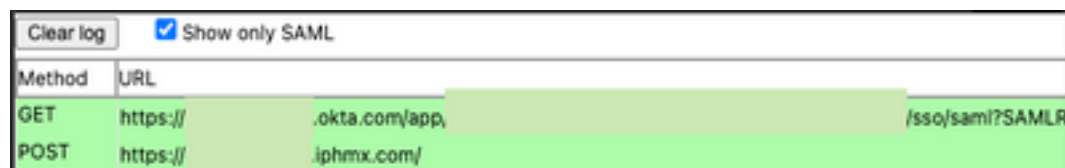
response ログに表示されます。

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.

アイデンティティプロバイダーの設定で、SAMLアプリケーションに割り当てられているユーザー権限とグループを確認します。

また、図に示すように、SAML DevTools拡張機能を使用して、Webブラウザから直接SAMLアプリケーション応答を取得することもできます。



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

関連情報

[『Cisco Secure Email Gateway User Guide』](#)

[SAML DevTools拡張機能](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。