

# Email Security Appliance에서 SAML 인증 검색 및 보기

## 목차

[소개](#)

[배경 정보](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[ESA에서 SAML 로그인 요청에 대한 인증 로그를 검색하고 보려면 어떻게 해야 하나요?](#)

[관련 정보](#)

## 소개

이 문서에서는 ESA(Email Security Appliance)에서 SAML 인증 요청을 처리하는 방법을 보여 주는 로그 항목을 검색하는 방법에 대해 설명합니다.

## 배경 정보

Cisco ESA(Email Security Appliance)는 스팸 격리에 대한 최종 사용자 액세스 및 관리 사용자 인터페이스를 사용하는 관리자를 위해 SSO 로그인을 지원하며, SAML은 관리자가 정의된 애플리케이션 세트에 액세스할 수 있도록 하는 XML 기반 개방형 표준 데이터 형식으로, 이러한 애플리케이션 중 하나에 로그인한 후에 해당 애플리케이션에 원활하게 액세스할 수 있도록 합니다.

SAML에 대한 자세한 내용은 SAML [일반](#) 정보를 [참조하십시오](#).

## 요구 사항

- 외부 인증이 구성된 Email Security Appliance.
- 모든 ID 공급자에 대한 SAML 통합.

## 사용되는 구성 요소

- CLI(Command Line Interface)에 대한 이메일 보안 어플라이언스 액세스.
- Gui 로그 서브스크립션
- SAML DevTools 확장입니다. 자세한 내용은 SAML Devtools [for Chrome](#)을 [참조하십시오](#).

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## ESA에서 SAML 로그인 요청에 대한 인증 로그를 검색하고 보려면 어떻게 해야 하나요?

인증 로그 서브스크립션은 SAML 로그인 요청에 대한 정보를 표시하지 않습니다. 그러나 이 정보는

GUI 로그에 기록됩니다.

로그의 이름은 *gui\_logs*이고 로그 유형은 *Http\_logs*입니다. 이 내용은 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) > gui\_logs**를 선택합니다.

다음 로그에 액세스할 수 있습니다.

명령줄에서

- Putty와 같은 SSH 클라이언트를 사용합니다. 포트 22/SSH를 통해 ESA 어플라이언스의 CLI에 로그인합니다.
- 명령줄에서 `grep`를 선택하여 액세스를 요청한 사용자의 이메일 주소를 검색합니다.

CLI가 로드되면 `Email address`, 이 명령에 표시된 대로

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

성공적인 로그인을 위해 다음과 같은 세 가지 항목을 볼 수 있습니다.

1. 구성된 ID 공급자에게 인증 및 권한 부여 데이터를 묻는 ESA에서 생성되는 SAML 요청.

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

2. 알림 SAML 어설션이 올바르게 설정되었습니다.

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

3. SSO 알림 결과.

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

이 세 가지 항목이 표시되지 않으면 인증 요청이 성공하지 못하며 다음 시나리오와 관련이 있습니다.

시나리오 1: SAML 요청만 로그에 표시되는 경우

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

사용자가 SAML 애플리케이션에 할당되지 않았거나 잘못된 ID 제공자 URL이 ESA에 추가되지 않았기 때문에 ID 제공자가 인증 요청을 거부합니다.

시나리오 2: 로그 항목인 경우

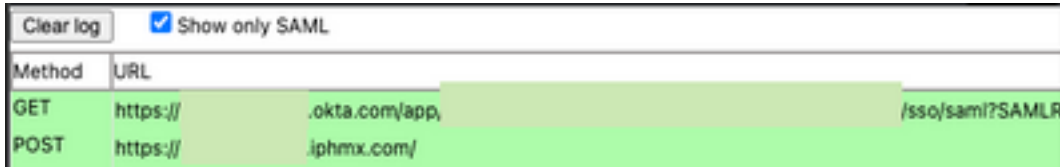
```
Authorization failed on appliance, While fetching user privileges from group mapping 및 An error occurred during SSO authentication. Details: Please check the configured Group Mapping values, it does not match the Attributes values from IDP response 로그에 표시됩니다.
```

```
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.
```

ID 공급자 컨피그레이션에서 SAML 애플리케이션에 할당된 사용자 권한 및 그룹을 확인합니다.

또는 SAML DevTools 확장을 사용하여 이미지에 표시된 대로 웹 브라우저에서 직접 SAML 애플리케이션 응답을 검색할 수 있습니다.



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

## 관련 정보

[Cisco Secure Email Gateway 사용 설명서](#)

[SAML DevTools 확장](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.