# ISE 3.1 GUI 문제 해결 SAML SSO로 로그인

### 목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>디버그 사용</u> <u>로그 다운로드</u> <u>문제 1a: 액세스 거부됨</u> <u>원인/해결 방법</u> 문제 1b: SAML 응답의 여러 그룹(액세스 거부) 문제 2: 404 리소스를 찾을 수 없음 원인/해결 방법 문제 3: 인증서 경고 원인/해결 방법

## 소개

이 문서에서는 SAML GUI 로그인을 통해 ISE 3.1에서 관찰된 대부분의 문제에 대해 설명합니다. SAML 2.0 표준의 사용을 통해 SAML 기반 관리자 로그인은 ISE에 SSO(Single Sign-On) 기능을 추가합니다. Azure, Okta, PingOne, DUO Gateway와 같은 IdP(Identity Provider) 또는 SAML 2.0을 구현하는 IdP를 사용할 수 있습니다.

# 사전 요구 사항

#### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

**1.** Cisco ISE 3.1 이상

```
2. SAML SSO 설정의 기본 사항 이해
```

```
컨피그레이션과 <u>흐름에 대한</u> 자세한 내용은 SAML 컨피그레이션 및 <u>Azure AD를 통한 SAML을 통한 ISE 관리 로그인 흐름</u>에 대한 ISE<u>3.1</u> 관리 가이드를 참조
하십시오.
```

참고: ID 공급자 서비스에 대해 잘 알고 있어야 하며 서비스가 실행 중인지 확인해야 합니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• ISE 버전 3.1

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

#### 트러블슈팅을 시작하려면 먼저 아래에 설명된 대로 디버그를 활성화해야 합니다.

Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug Log Configuration(디버그 로그 컨피그레이션)으로 이동합니다. 다음 이 미지에 표시된 대로 Primary admin(기본) 노드를 선택하고 Edit(수정)를 클릭합니다.

| ≡ Cisco ISE                 |               |                         |                    |  |
|-----------------------------|---------------|-------------------------|--------------------|--|
| Diagnostic Tools            | Download Logs | Debug Wizard            |                    |  |
| Debug Profile Configuration | No            | do List                 |                    |  |
| Debug Log Configuration     | NO            | de List                 |                    |  |
|                             |               |                         |                    |  |
|                             | C/ Ed         | it 👌 🕁 Reset to Default |                    |  |
|                             |               | Node Name               | ∧ Replication Role |  |
|                             | ~             | ise-admin               | PRIMARY            |  |
|                             | 0             | ise-secondary           | SECONDARY          |  |
|                             |               |                         |                    |  |
|                             |               |                         |                    |  |

• 다음 구성 요소를 DEBUG **수준으로** 설정합니다.

| 구성 요소 이름 | 로그 레벨 | 로그 파일 이름    |
|----------|-------|-------------|
| 포털       | 디버그   | guest.log   |
| opensaml | 디버그   | ise-psc.log |
| SAML     | 디버그   | ise-psc.log |

참고: 문제 해결이 완료되면 노드를 선택하여 디버그를 재설정하고 "기본값으로 재설정"을 클릭합니다.

#### 로그 다운로드

문제가 재현되면 필요한 로그 파일을 확보해야 합니다.

1단계. Operations(운영) > Troubleshoot(문제 해결) > Download logs(로그 다운로드)로 이동합니다. '어플라이언스 노드 목록' > 디버그 로그에서 기본 관리 노 드를 선택합니다.

2단계. 게스트 및 ise-psc 상위 폴더를 찾아 확장합니다.

3단계. 다운로드 guest.log 및 ise-psc.log 파일.

문제 1a: 액세스 거부됨

- SAML 기반 관리자 로그인을 구성한 후
- Log in With SAML을 선택합니다.
- IdP 로그인 페이지로 리디렉션하면 예상대로 작동합니다.
- SAML/IdP 응답당 인증 성공

| ㆍ ldP는 그룹 특성을 | · 전송하고 ISE에 구성된 | 동일한 그룹/개체 ID를 | 볼 수 있습니다. |
|---------------|-----------------|---------------|-----------|
|---------------|-----------------|---------------|-----------|

• 그런 다음 ISE가 정책을 분석하려고 할 때, 스크린샷과 같이 "액세스 거부" 메시지를 발생시키는 예외가 발생합니다.

| 10 | cisco                      |  |
|----|----------------------------|--|
| -  | Identity Services Engine   |  |
|    | Intuitive network security |  |
|    | Access Denied              |  |
|    | Log In With SAML           |  |
|    | Log In With ISE            |  |
|    | English   日本語              |  |
|    | Problems logging in?       |  |

ise-psc.log에 로그인

2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse: IdP ID: TSDLAB\_DAG Subject: ise.test Group: null SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true SAML Status Message:null SAML email: SAML Exception:nullUserRole : NONE 2021-09-27 17:16:18,218 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - about to call authenticateSAMLUser messageCode:null subject: ise.test 2021-09-27 17:16:18,225 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::-Authenticate SAML User - result: PASSED 2021-09-27 17:16:18,390 INFO [admin-http-pool5][] pool5][] com.cisco.ise.util.RBACUtil -::::- Populating cache for external to internal group linkage. 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][] cpm.admin.infra.utils.PermissionEvaluationUtil -::::- Exception in login action java.lang.NullPointerException 2021-09-27 17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginAction -::::- In Login Action user has Menu Permission: false 2021-09-27 17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginAction -::::- In Login action, user has no menu permission 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][] cpm.admin.infra.action.LoginAction -::::- Can't save locale. loginSuccess: false 2021-09-27 17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginActionResultHandler -::::-

Redirected to: /admin/login.jsp?mid=access\_denied

#### 원인/해결 방법

IdP 구성의 그룹 클레임 이름이 ISE에 구성된 이름과 동일한지 확인합니다.

다음 스크린샷은 Azure 쪽에서 찍은 것입니다.

| Microsoft Azure   |  | ,> Search resources, services, an |
|---|--|-----------------------------------|
| Home > Enterprise applications   All applications > Attributes & Claims | SAML-based Sign-on > SAML              | -based Sign-on >                  |
| + Add new claim + Add a group claim == Columns   3                      | Got feedback?                          |                                   |
| Required claim  |  |                                   |
| Claim name  | Value                                  |                                   |
| Unique User Identifier (Name ID)  | user.userprincipalname [nameid-format: | emailAddre ***                    |
| Additional claims   |  |                                   |
| Claim name  | Value                                  |                                   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaila            | user.mail                              | ••••                              |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn            | user.givenname                         |                                   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name              | user.userprincipalname                 |                                   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surna             | user.sumame                            |                                   |
| Rom_Azure_Groups  | user.groups                            |                                   |

Advanced settings (Preview)

#### ISE Side의 스크린샷

| ≡ Cisc     | o ISE               |               |   |                          |                  |                  | Administration · |
|------------|---------------------|---------------|---|--------------------------|------------------|------------------|------------------|
| Identities | Groups              | External Ide  | ntity Sources                             | Identity Source Se       | quences Setti    | ngs              |                  |
| External   | Identity Source     | hentication F | Identity Provider<br>SAML Iden<br>General | List > tity Provider     | Donfig. Service  | e Provider Info. | Groups           |
|            | Active Director     | у             | Groups<br>Group M                         | s<br>embership Attribute | tom_Azure_Groups |                  |                  |
| 0<br>>     | DBC<br>RADIUS Token |               | + Add                                     | 🖉 Edit 📋 Delete          |                  |                  |                  |

#### 문제 1b: SAML 응답의 여러 그룹(액세스 거부)

이전 수정으로 문제가 해결되지 않으면 사용자가 둘 이상의 그룹에 속해 있지 않아야 합니다. 이 경우 ISE가 SAML 응답의 목록의 첫 번째 값(그룹 이름/ID)에만 일치하는 Cisco 버그 ID <u>CSCwa17470</u>을 발견해야 합니다. 이 버그는 3.1 P3에서 해결됩니다.



이전에 제공된 IdP 응답에 따라, 로그인이 성공하려면 iseadmins 그룹에 대한 ISE 매핑을 구성해야 합니다.

#### 문제 2:404 리소스를 찾을 수 없음



guest.log에 오류가 표시됩니다.

2021-10-21 13:38:49,308 ERROR [https-jsse-nio-10.200.50.44-8443-exec-3][] cpm.guestaccess.flowmanager.step.StepExecutor -::-Can not find the matched transition step on Step=id: 51d3f147-5261-4eb7-alc9-ce47ec8ec093, tranEnum=PROCEED\_SSO.

#### 원인/해결 방법

이 문제는 첫 번째 ID 저장소만 생성한 후에 발생합니다.

이 문제를 해결하려면 같은 순서로 다음을 시도하십시오.

1단계. ISE에서 새 SAML IdP를 생성합니다(현재 SAML IdP는 아직 제거하지 마십시오.).

2단계. 관리자 액세스 페이지로 이동하여 이 새 IdP에 관리자 액세스 권한을 할당합니다.

3단계. External Identity Providers(외부 ID 제공자) 페이지에서 기존 IdP를 삭제합니다.

4단계. 현재 IdP 메타데이터를 1단계에서 생성한 새 IdP로 가져오고 필요한 그룹 매핑을 수행합니다.

5단계. 이제 SAML 로그인을 시도합니다. 효과가 있을 겁니다

#### 문제 3: 인증서 경고

멀티 노드 구축에서 "Log In with SAML(SAML로 로그인)"을 클릭하면 브라우저에 신뢰할 수 없는 인증서 경고가 표시됩니다

| br | × +  |  |       |     | - | U      |
|----|--|--|-------|-----|---|--------|
| 3  | ▲ Not secure   https://*                           | t8443/portal/PortalSetup.action?portal=0715c4ba-3389-4049-8ce    | AN TO | 5⁄≡ | œ | disco. |
|    | Your connect                                       | ion isn't private  |       |     |   |        |
|    | Attackers might be tryin<br>passwords, messages, o | g to steal your information from (for example, or credit cards). |       |     |   |        |
|    | NET::ERR_CERT_COMMON_I                             | NAME_INVALID   |       |     |   |        |
|    | Advanced   | Go back  |       |     |   |        |

#### 원인/해결 방법

경우에 따라 pPAN은 사용자를 FQDN이 아닌 활성 PSN IP로 리디렉션합니다. 이로 인해 SAN 필드에 IP 주소가 없는 경우 일부 PKI 구축에서 인증서 경고가 발 생합니다.

해결 방법은 인증서의 SAN 필드에 IP를 추가하는 것입니다.

Cisco 버그 ID <u>CSCvz89415</u>. 3.1p1에서 해결됩니다.

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 번 역 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.