

Azure Active Directory를 사용하여 ISE 3.0 REST ID 구성

목차

[소개](#)

[배경 정보](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[상위 레벨 플로우 개요](#)

[통합을 위한 Azure AD 구성](#)

[통합을 위한 ISE 구성](#)

[다양한 활용 사례에 대한 ISE 정책에](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[REST 인증 서비스 문제](#)

[REST ID 인증 문제](#)

[로그 파일 작업](#)

소개

이 문서에서는 REST ID 서비스를 통해 구현된 Cisco ISE 3.0과 Azure AD의 통합 및 리소스 소유자 암호 자격 증명에 대해 설명합니다.

배경 정보

이 문서에서는 ROPC(Resource Owner Password Credentials)를 통해 REST(Representational State Transfer) ID(Identity) 서비스를 통해 구현된 ISE(Identity Services Engine) 3.0과 Microsoft(MS) Azure AD(Active Directory)의 통합을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- ISE
- MS Azure AD

- ROPC 프로토콜 구현 및 제한 이해, [링크](#)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

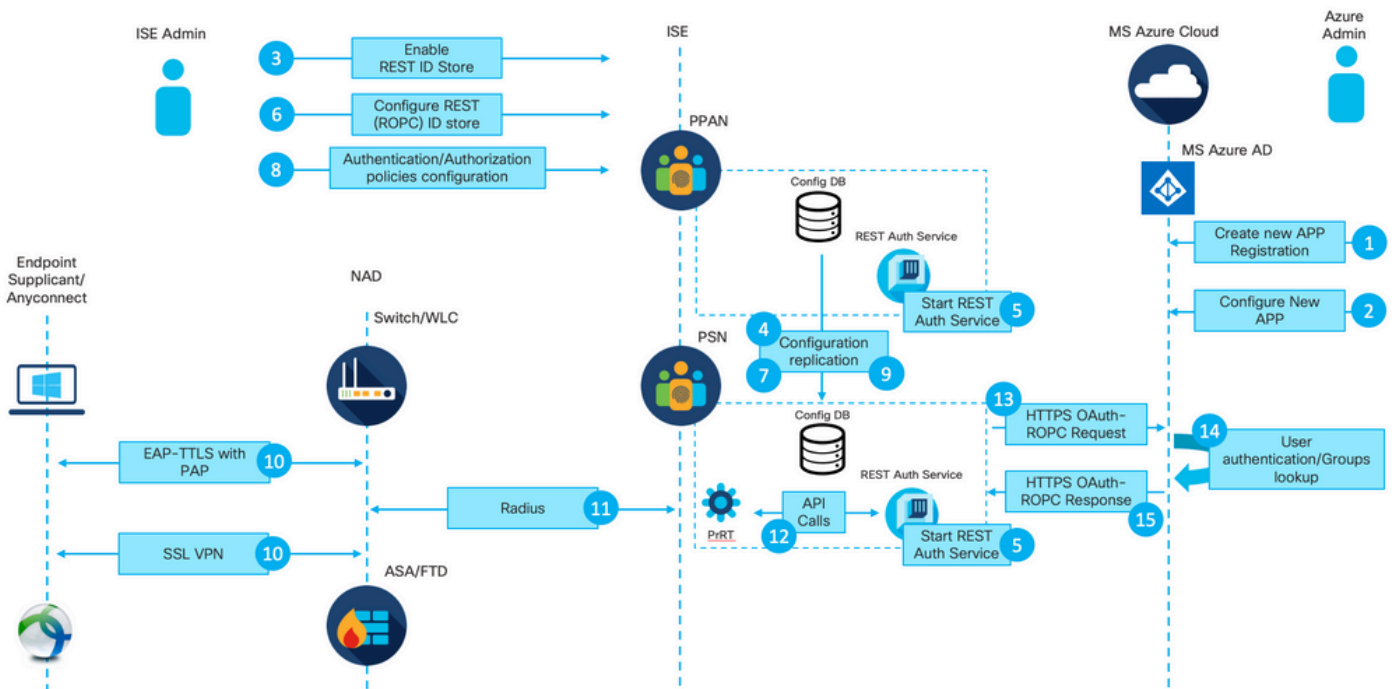
- Cisco ISE 버전 3.0
- MS Azure AD
- WS-C3850-24P(16.9.2 포함)
- ASAv(9.10 포함)(1)
- Windows 10.0.18363

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.

구성

ISE REST ID 기능은 ISE 3.0 - REST 인증 서비스에 도입된 새 서비스를 기반으로 합니다. 이 서비스는 사용자 인증 및 그룹 검색을 수행하기 위해 OAuth(Open Authorization) ROPC 교환에서 Azure AD와의 통신을 담당합니다. REST 인증 서비스는 기본적으로 비활성화되어 있으며, 관리자가 활성화한 후에는 구축의 모든 ISE 노드에서 실행됩니다. 사용자 인증 시 REST Auth Service와 클라우드의 통신이 이루어지므로 경로의 지연이 발생하면 인증/권한 부여 플로우에 추가 레이턴시가 발생합니다. 이 레이턴시는 ISE 제어 범위를 벗어납니다. REST 인증의 구현은 다른 ISE 서비스에 영향을 주지 않도록 신중하게 계획하고 테스트해야 합니다.

상위 레벨 플로우 개요



1. Azure 클라우드 관리자가 새 응용 프로그램(앱) 등록을 만듭니다. 이 앱의 세부 정보는 나중에 Azure AD와의 연결을 설정하기 위해 ISE에서 사용됩니다.

2. Azure 클라우드 관리자는 다음 항목을 사용하여 앱을 구성해야 합니다.

- 클라이언트 암호 만들기
- ROPC 사용
- 그룹 클레임 추가
- API(Application Programming Interface) 권한 정의

3. ISE 관리자가 REST 인증 서비스를 켭니다. 이 작업은 다른 작업을 실행하기 전에 수행해야 합니다.

4. 변경 사항이 컨피그레이션 데이터베이스에 기록되고 전체 ISE 구축에 복제됩니다.

5. 모든 노드에서 REST 인증 서비스가 시작됩니다.

6. ISE 관리자는 2단계의 세부 정보로 REST ID 저장소를 구성합니다.

7. 변경 사항이 컨피그레이션 데이터베이스에 기록되고 전체 ISE 구축에 복제됩니다.

8. ISE 관리자가 새 ID 저장소 시퀀스를 생성하거나 이미 있는 ID 저장소 시퀀스를 수정하고 인증/권한 부여 정책을 구성합니다.

9. 변경 사항이 컨피그레이션 데이터베이스에 기록되고 전체 ISE 구축에 복제됩니다.

10. 엔드포인트가 인증을 시작합니다. ROPC 프로토콜 사양에 따라 사용자 비밀번호는 암호화된 HTTP 연결을 통해 일반 텍스트로 Microsoft ID 플랫폼에 제공되어야 합니다. 이러한 사실 때문에 현재 ISE에서 지원되는 유일한 인증 옵션은 다음과 같습니다.

- PAP(Password Authentication Protocol)를 내부 방법으로 사용하는 EAP-TTLS(Extensible Authentication Protocol-Tunneled Transport Layer Security)
- PAP를 사용한 AnyConnect SSL VPN 인증

11. Radius를 통해 ISE PSN(Policy Service Node)과 교환합니다.

12. PrRT(Process Runtime)가 내부 API를 통해 사용자 세부사항(사용자 이름/비밀번호)과 함께 REST ID 서비스에 요청을 보냅니다.

13. REST ID 서비스가 HTTPS(HyperText Transfer Protocol Secure)를 통해 Azure AD에 OAuth ROPC 요청을 보냅니다.

14. Azure AD는 사용자 인증을 수행하고 사용자 그룹을 가져옵니다.

15. 인증/권한 부여 결과가 ISE에 반환되었습니다.

포인트 15 후, 인증 결과 및 가져온 그룹은 PrRT로 반환되며, 이는 정책 평가 흐름과 관련이 있으며 최종 인증/권한 부여 결과를 할당합니다. 권한 부여 프로파일의 특성을 가진 Access-Accept 또는 Access-Reject가 네트워크 액세스 장치 (NAD)에 반환 됩니다.

통합을 위한 Azure AD 구성

1. 그림과 같이 AppRegistration Service를 찾습니다.

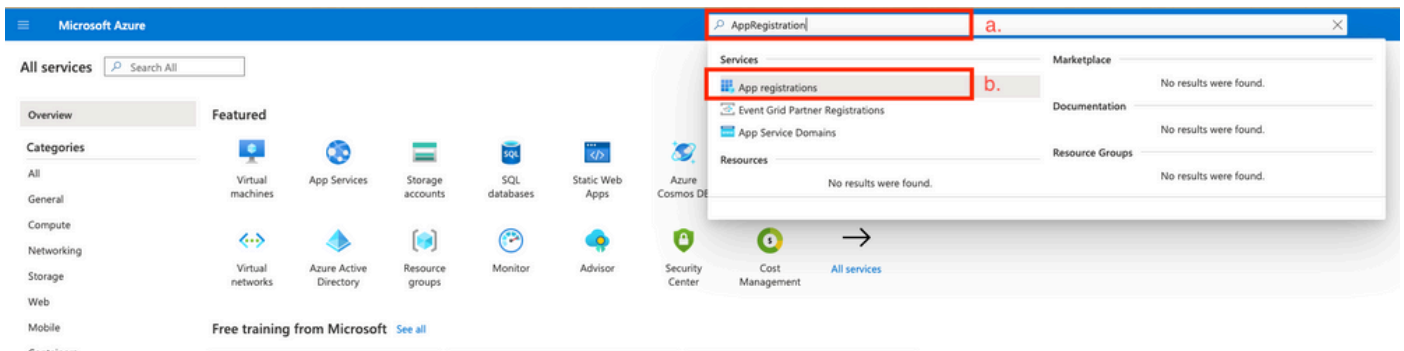


그림 2.

a. 글로벌 검색 표시줄에 AppRegistration을 입력합니다.

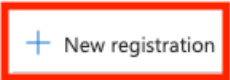
b. 애플리케이션 등록 서비스를 클릭합니다.

2. 새 앱 등록을 만듭니다.



All services >

App registrations

 [+ New registration](#)



[Endpoints](#)



[Troubleshooting](#)



[Download \(Preview\)](#)



[Got feedback?](#)



Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will con

All applications

Owned applications



Start typing a name or Application ID to filter these results

그림 3.

3. 새 앱을 등록합니다.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

 ✓

a.

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (DEMO only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

b.

[Help me choose...](#)


Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the [Microsoft Platform Policies](#)

c.

저장소에 추가하려면 [그룹 로드]를 누릅니다. 이 예에서는 관리자 환경이 어떻게 나타나는지 보여줍니다.

 참고: Cisco 버그 ID CSCvx00345의 결함으로 인해 그룹이 로드되지 않으므로 [이에](#) 유의하십시오. ISE 3.0 패치 2에서 결함이 수정되었습니다.

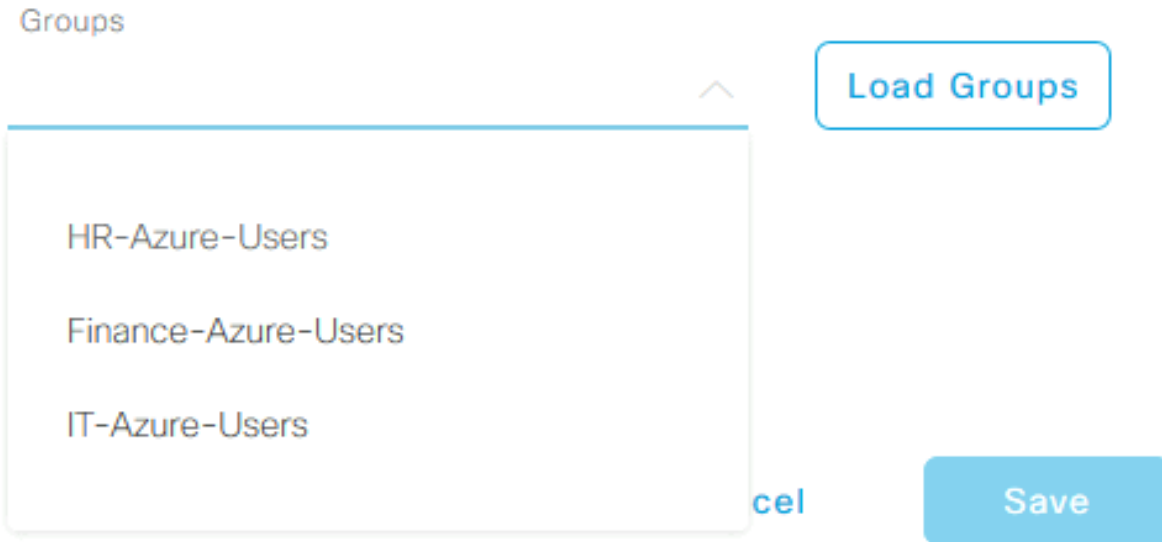


그림 23.

h. 변경 사항을 제출합니다.

5. 이 단계에서는 새로 생성된 REST ID 저장소를 포함하는 새 ID 저장소 시퀀스 생성을 고려합니다

6. 인증 정책에 할당된 REST ID 저장소 또는 ID 저장소 시퀀스가 포함된 REST ID 저장소 시퀀스가 있는 순간, 이미지에 표시된 대로 프로세스 실패에 대한 기본 작업을 DROP에서 REJECT로 변경합니다.

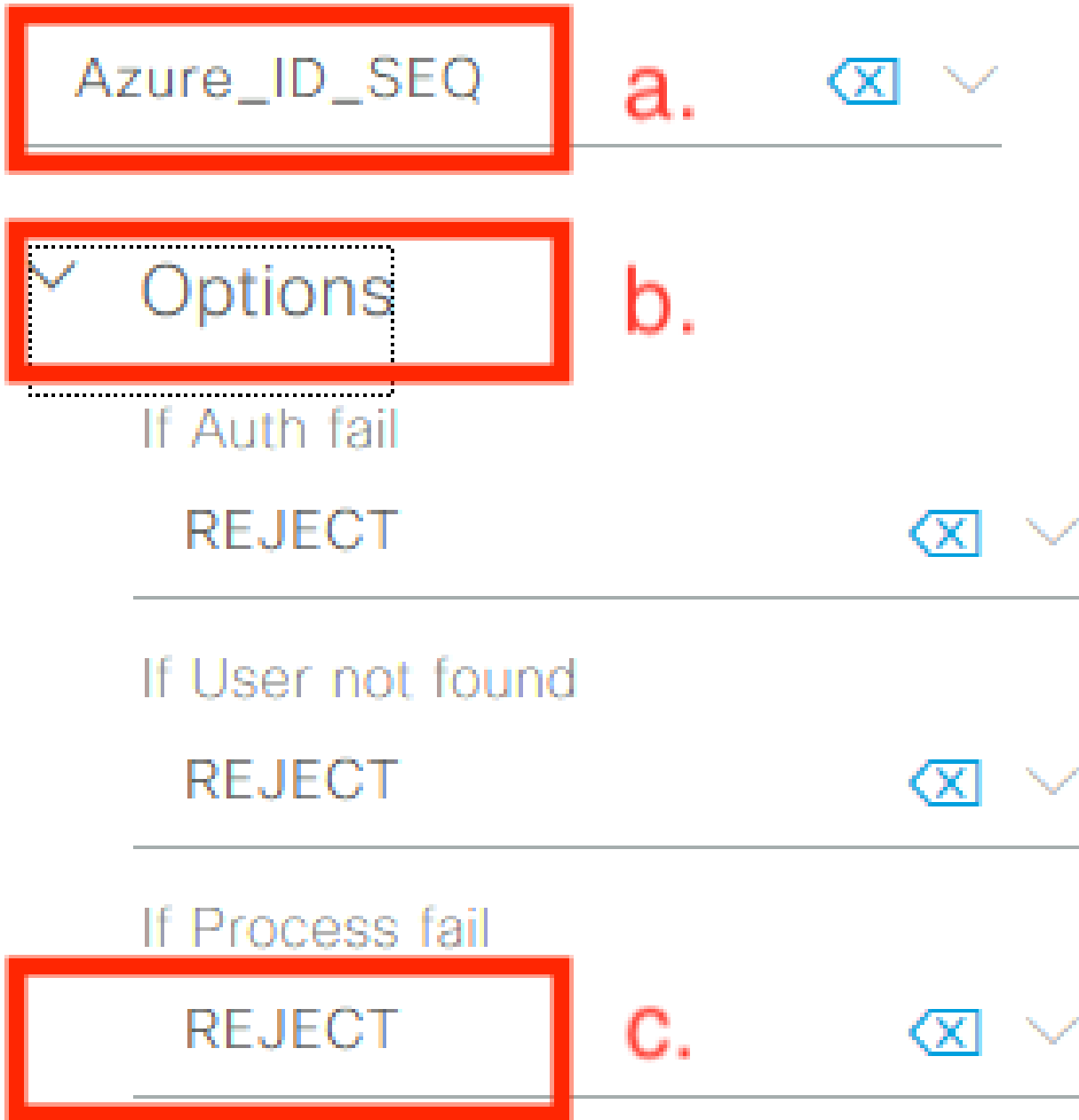


그림 24.

a. REST ID 저장소를 사용하는 인증 정책을 찾습니다.

b. 열기 옵션 드롭다운 목록

c. Process Failed(프로세스 실패)에 대한 기본 작업을 DROP(삭제)에서 REJECT(거부)로 변경합니다.

다음과 같이 REST ID 저장소 내에서 특정 오류가 발생하는 경우 NADs 측에서 dead로 표시된 PSN을 방지하기 위해 이 작업이 필요합니다.

- 사용자가 Azure AD에서 그룹의 구성원이 아닙니다.
- 사용자 비밀번호를 변경해야 합니다.

7. 권한 부여 정책에 REST ID 저장소 사전을 추가합니다.

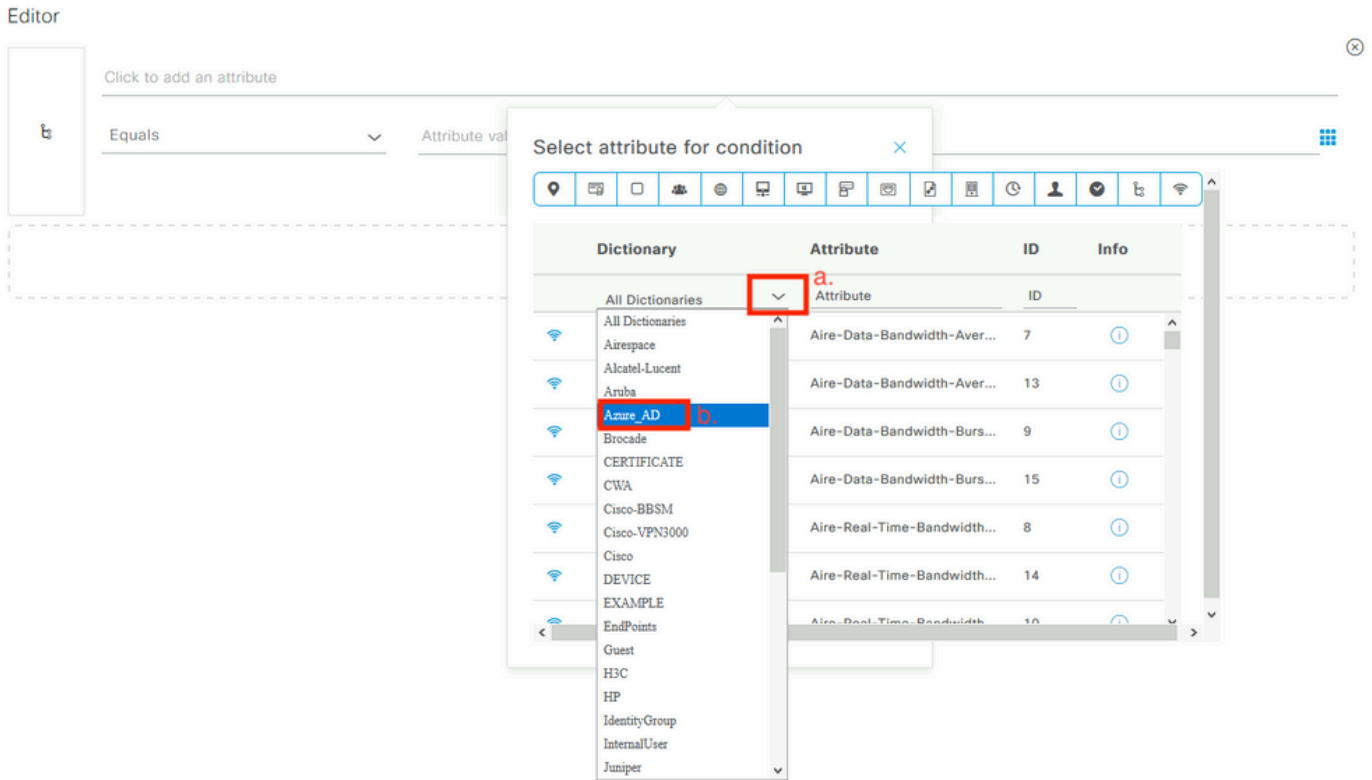


그림 25.

a. 모든 사전 열기 드롭다운 목록

b. REST ID 저장소와 같은 방법으로 이름이 지정된 사전을 찾습니다.

8. 외부 ID 그룹을 추가합니다(ISE 3.0부터 REST ID 저장소 사전에서 사용할 수 있는 유일한 특성은 외부 그룹임).

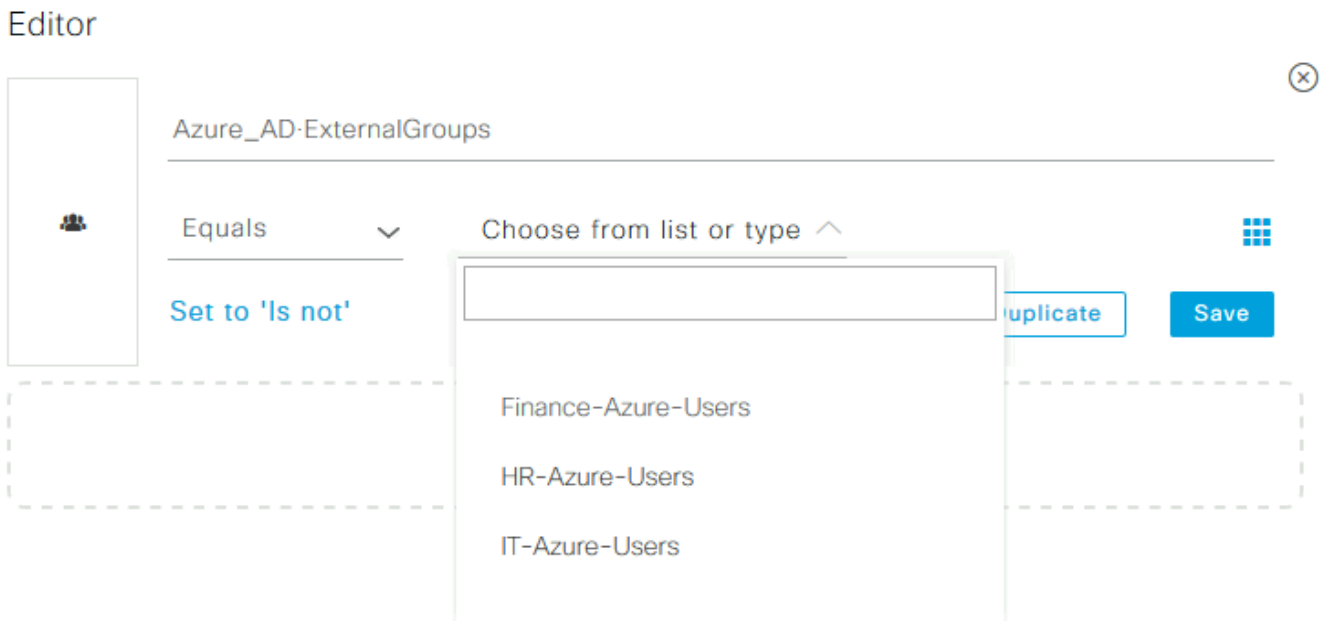


그림 26.

다양한 활용 사례에 대한 ISE 정책 예

Dot1x 인증의 경우 이미지에 표시된 대로 EAP-TTLS 시도에 매칭하려면 네트워크 액세스 사전의 EAP 터널 조건을 사용할 수 있습니다.

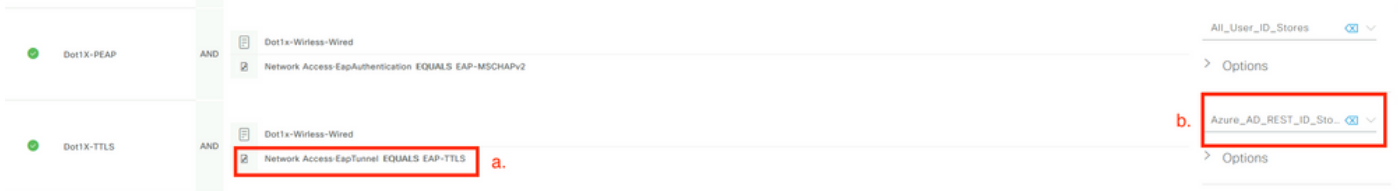


그림 27.

a. REST ID 저장소로 전달해야 하는 시도와 일치하도록 EAP-TTLS와 동일한 EAP 터널을 정의합니다.

b. REST ID 저장소에서 직접 선택하거나 [사용] 열에 포함된 [ID 저장소 시퀀스]를 선택합니다.

개별 권한 부여 정책 내에서 Azure AD의 외부 그룹을 EAP 터널 유형과 함께 사용할 수 있습니다.

✓	Dot1X-TTLS-Azure-Finance	AND	Dot1x-Wireless-Wired	Network Access-EapTunnel EQUALS EAP-TTLS	Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓	Dot1X-TTLS-Azure-HR	AND	Dot1x-Wireless-Wired	Network Access-EapTunnel EQUALS EAP-TTLS	Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓	Dot1X-TTLS-Azure-IT	AND	Dot1x-Wireless-Wired	Network Access-EapTunnel EQUALS EAP-TTLS	Azure_AD-ExternalGroups EQUALS IT-Azure-Users

그림 28.

VPN 기반 흐름의 경우, 터널 그룹 이름을 차별화 요소로 사용할 수 있습니다.

인증 정책:



권한 부여 정책:

✓ VPN-Azure-Finance	AND	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere	Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓ VPN-Azure-HR	AND	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere	Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓ VPN-Azure-IT	AND	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere	Azure_AD-ExternalGroups EQUALS IT-Azure-Users

그림 29.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. ISE 노드에서 REST 인증 서비스가 실행되는지 확인합니다.

이를 확인하려면 대상 ISE 노드의 SSH(Secure Shell) 셸에서 show application status ise 명령을 실행해야 합니다.

<#root>

```
skuchere-ise30-1/admin# show application status ise
```

```
ISE PROCESS NAME STATE PROCESS ID
-----
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
```

DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled

REST Auth Service running 63052

SSE Connector disabled

2. 인증 시 REST ID 저장소가 사용되는지 확인합니다(자세한 인증 보고서의 단계. 섹션 확인).

15013 Selected Identity Source - Azure_AD

25103 Perform plain text password authentication in external REST ID store server - Azure_AD a.

25100 Connecting to external REST ID store server - Azure_AD b.

25101 Successfully connected to external REST ID store server - Azure_AD (🕒 Step latency=1660 ms) c.

25104 Plain text password authentication in external REST ID store server succeeded - Azure_AD d.

25107 REST ID store server respond with groups - Azure_AD e.

25110 User groups inserted to session cache - Azure_AD f.

22037 Authentication Passed

a. PSN은 선택한 REST ID 저장소로 일반 텍스트 인증을 시작합니다.

b. Azure Cloud와 연결된 상태입니다.

c. 실제 인증 단계 - 여기에 제시된 레이턴시 값에 주목합니다. Secure Cloud의 모든 인증이 상당한 지연에서 어려움을 겪는 경우, 이는 다른 ISE 플로우에 영향을 미치며, 그 결과 전체 ISE 구축이 불안정해집니다.

d. 인증 성공 확인

e. 응답한 그룹 데이터의 확인

f. 사용자 그룹 데이터로 채워진 세션 컨텍스트 ISE 세션 관리 프로세스에 대한 자세한 내용은 이 문서 - 링크를 검토하십시오.

3. Expect Authentication/Authorization(인증/권한 부여 기대) 정책이 선택되었는지 확인합니다(자세

한 인증 보고서의 Investigate Overview(개요 조사) 섹션에 대해 확인).

Overview

Event	5200 Authentication succeeded
Username	bob
Endpoint Id	ED:37:E1:08:57:15 ⊕

Endpoint Profile

Authentication Policy	SPRT-Policy-Set >> Azure-AD
Authorization Policy	SPRT-Policy-Set >> Azure-Finance

Authorization Result PermitAccess

그림 30.

문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 정보를 제공합니다.

REST 인증 서비스 문제

REST Auth Service의 문제를 해결하려면 ADE.log 파일 검토부터 시작해야 합니다. 지원 번들 위치 - /support/adeos/ade

REST 인증 서비스에 대한 검색 키워드는 - ROPC-control입니다.

다음 예에서는 REST 인증 서비스가 시작되는 방법을 보여 줍니다.

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

서비스가 시작되지 않거나 예기치 않게 다운되는 경우 문제가 되는 기간에 ADE.log를 검토하여 시작하는 것이 좋습니다.

REST ID 인증 문제

REST ID 저장소를 사용할 때 인증이 실패할 경우 항상 자세한 인증 보고서부터 시작해야 합니다. Other Attributes(기타 특성) 영역에는 Azure 클라우드에서 반환된 오류가 포함된 RestAuthErrorMsg 섹션이 표시됩니다.

```
RestAuthErrorMsg      Error Key - invalid_client | Error Description -
                        AADSTS7000218: The request body must contain the
                        following parameter: 'client_assertion' or 'client_secret.' Trace
                        ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID:
                        519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp:
                        2020-09-13 19:11:47Z | Error Codes - [7000218] | Error URI
                        - https://login.microsoftonline.com/error?code=7000218
```

그림 31.

로그 파일 작업

ISE 3.0에서는 REST ID 기능의 도입이 제어되어 기본적으로 디버그가 활성화됩니다. 모든 REST ID 관련 로그는 CLI를 통해 볼 수 있는 ROPC 파일에 저장됩니다.

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log
```

```
skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filte
```

설치된 패치가 있는 ISE 3.0에서 파일 이름이 ropc.log가 아니라 rest-id-store.log임을 확인합니다. 이전 검색 예에서는 폴더 이름이 변경되지 않았으므로 작업을 제공했습니다.

또는 이러한 파일은 ISE 지원 번들에서 추출할 수 있습니다.

다음은 다양한 작업 및 비작업 시나리오를 보여 주는 몇 가지 로그 예입니다.

1. Azure Graph가 ISE 노드에서 신뢰되지 않는 경우 인증서 오류가 발생합니다. 이 오류는 REST ID 저장소 설정에서 그룹이 로드되지 않을 때 표시됩니다.

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appl
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

이 문제는 Microsoft graph API 인증서가 ISE에서 신뢰하지 않는다는 것을 나타냅니다. ISE 3.0.0.458에는 신뢰할 수 있는 저장소에 설치된 DigiCert 글로벌 루트 G2 CA가 없습니다. 이것은 결함에 기록되어 있다

- Cisco 버그 ID [CSCv80297](https://cisco.com/cisco/webbugid/CSCv80297) 이 문제를 해결하려면 ISE 트러스트된 저장소에 DigiCert Global Root G2 CA를 설치하고 Cisco 서비스에 대해 트러스트된 것으로 표시해야 합니다.

인증서는 여기에서 다운로드할 수 있습니다. <https://www.digicert.com/kb/digicert-root-certificates.htm>

2. 신청 암호가 잘못되었습니다.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client s
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentity
```

3. 앱 ID가 잘못되었습니다.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4. 사용자가 없습니다.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error": "invalid_grant", "error_desc
```

```
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5. 사용자 암호가 만료되었습니다. 일반적으로 Office365에 로그인할 때 Azure 관리자가 정의한 암호를 변경해야 하므로 새로 만든 사용자에 대해 이 문제가 발생할 수 있습니다.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. 잘못된 API 권한으로 인해 그룹을 로드할 수 없습니다.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Stat
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. Azure 측에서 ROPC가 허용되지 않으면 인증에 실패합니다.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCCResponseErrorException: {"error":"invalid_client","error_des
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
```



```
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8. 사용자가 Azure 측의 어떤 그룹에도 속하지 않으므로 인증에 실패합니다.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. 성공적인 사용자 인증 및 그룹 검색

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

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.