

ISE에서 사용자별 동적 액세스 제어 목록 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[ISE에서 새 사용자 지정 사용자 특성 구성](#)

[dACL 구성](#)

[사용자 지정 특성으로 내부 사용자 계정 구성](#)

[AD 사용자 계정 구성](#)

[AD에서 ISE로 특성 가져오기](#)

[내부 및 외부 사용자를 위한 권한 부여 프로파일 구성](#)

[권한 부여 정책 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 ID 저장소 유형에 있는 사용자에게 대한 사용자별 동적 액세스 제어 목록(dACL)의 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 ISE(Identity Services Engine)의 정책 컨피그레이션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

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.

배경 정보

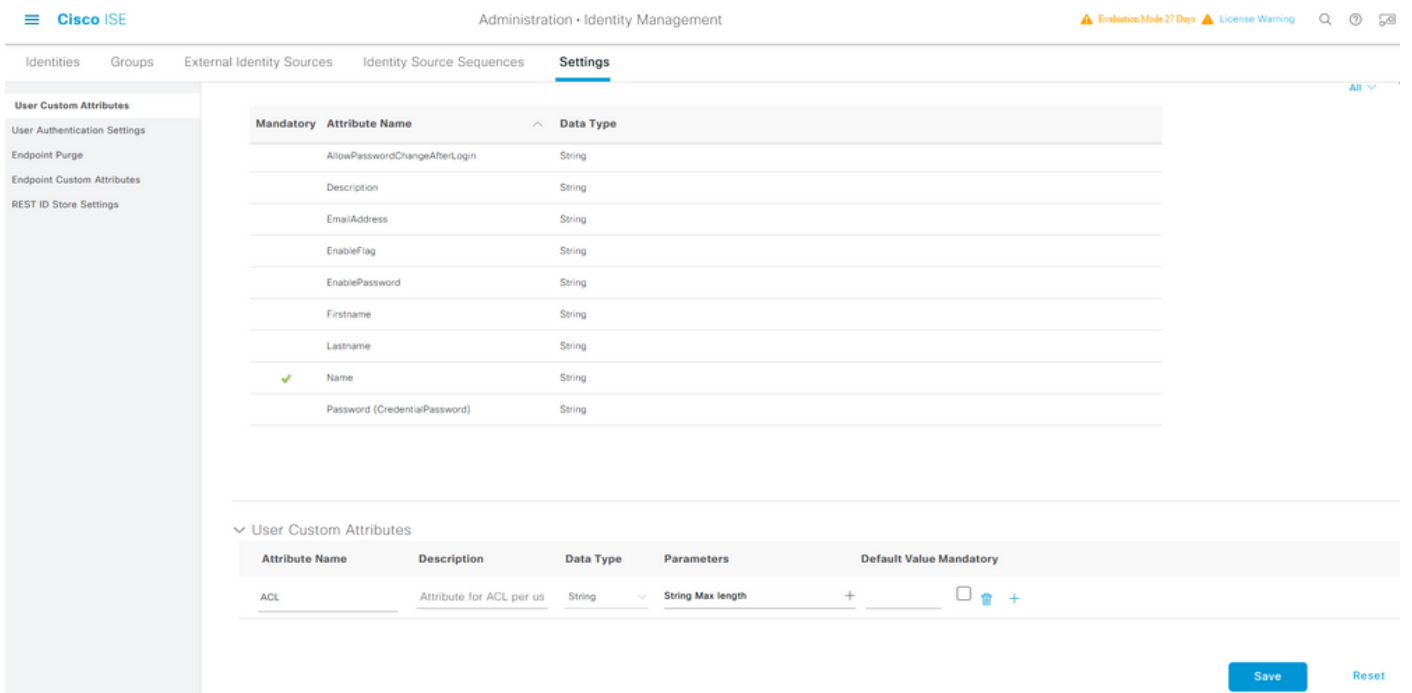
사용자별 동적 액세스 제어 목록의 컨피그레이션은 ISE 내부 ID 저장소 또는 외부 ID 저장소에 있는 사용자를 위한 것입니다.

구성

사용자 지정 사용자 특성을 사용하는 내부 저장소의 모든 사용자에게 대해 사용자별 dACL을 구성할 수 있습니다. AD(Active Directory)에 있는 사용자의 경우 문자열 유형의 특성을 사용하여 동일한 특성을 얻을 수 있습니다. 이 섹션에서는 ISE와 AD의 특성을 구성하는 데 필요한 정보와 이 기능이 작동하기 위해 ISE에 필요한 컨피그레이션을 제공합니다.

ISE에서 새 사용자 지정 사용자 특성 구성

Administration(관리) > Identity Management(ID 관리) > Settings(설정) > User Custom Attributes(사용자 지정 특성)로 이동합니다. 이미지에 표시된 대로 + 버튼을 클릭하여 새 속성을 추가하고 변경 사항을 저장합니다. 이 예에서 사용자 지정 특성의 이름은 ACL입니다.



dACL 구성

다운로드 가능한 ACL을 구성하려면 Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Downloadable ACLs(다운로드 가능한 ACL)로 이동합니다. Add(추가)를 클릭합니다. dACL의 이름, 내용을 제공하고 변경 사항을 저장합니다. 이미지에 표시된 대로 dACL의 이름은 NotMuchAccess입니다.

Dictionary Conditions Results

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name NotMuchAccess

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

```
1234567 permit ip any any|
8910111
2131415
1617181
9202122
2324252
6272829
3031323
3343536
3738394
0414243
AAAAAAA
```

Check DACL Syntax ⓘ

Submit

사용자 지정 특성으로 내부 사용자 계정 구성

Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) > Add(추가)로 이동합니다. 사용자를 생성하고 권한 부여 시 사용자가 받아야 하는 dACL의 이름으로 사용자 지정 특성 값을 구성합니다. 이 예에서 dACL의 이름은 NotMuchAccess입니다.

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Name testuserinternal

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

> User Information

> Account Options

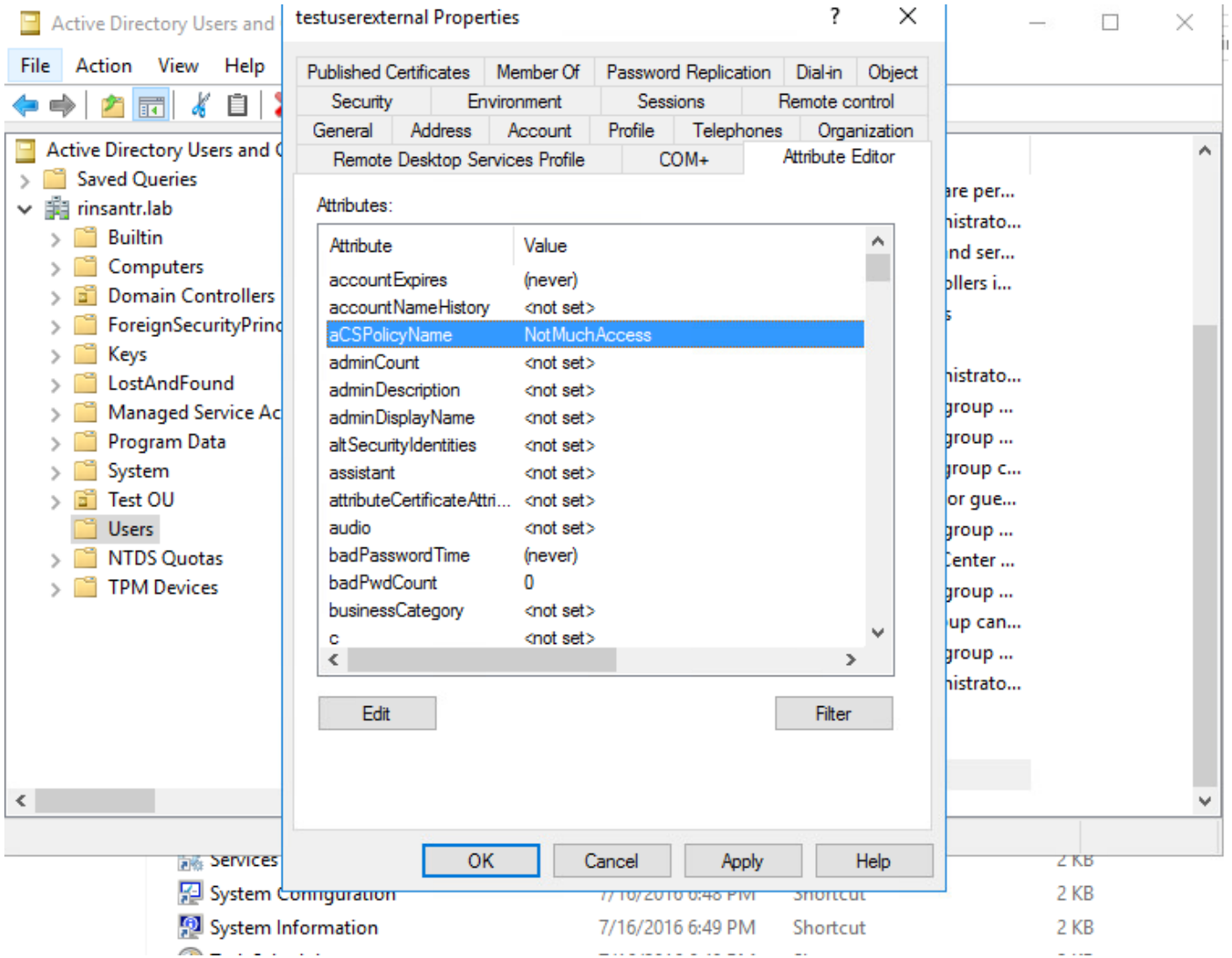
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

AD 사용자 계정 구성

Active Directory에서 사용자 계정 등록 정보로 이동한 다음 속성 편집기 탭으로 이동합니다. 이미지에 표시된 대로 aCSPolicyName은 dACL 이름을 지정하는 데 사용되는 특성입니다. 그러나 앞에서 언급한 것처럼 문자열 값을 수용할 수 있는 모든 특성도 사용할 수 있습니다.



AD에서 ISE로 특성 가져오기

AD에 구성된 특성을 사용하려면 ISE에서 해당 특성을 가져와야 합니다. 특성을 가져오려면 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory > [Join point configured](구성된 조인 지점) > Attributes(특성) 탭으로 이동합니다. Add(추가)를 클릭한 다음 Select Attributes From Directory(디렉토리에서 특성 선택)를 클릭합니다. AD에서 사용자 계정 이름을 제공한 다음 특성 검색을 클릭합니다. dACL에 대해 구성된 특성을 선택하고 OK(확인)를 클릭한 다음 Save(저장)를 클릭합니다. 그림에 표시된 것처럼 CSPolicyName은 특성입니다.

Directory Attributes

Only attributes selected below will be available for use as policy conditions in policy rules.

* Sample User or Machine

Account

testuserexternal



Retrieve Attributes...

| <input type="checkbox"/> | Name | Type | Example Value |
|-------------------------------------|-----------------------|--------|---|
| <input checked="" type="checkbox"/> | aCSPolicyName | STRING | NotMuchAccess |
| <input type="checkbox"/> | accountExpires | STRING | 9223372036854775807 |
| <input type="checkbox"/> | badPasswordTime | STRING | 0 |
| <input type="checkbox"/> | badPwdCount | STRING | 0 |
| <input type="checkbox"/> | cn | STRING | testuserexternal |
| <input type="checkbox"/> | codePage | STRING | 0 |
| <input type="checkbox"/> | countryCode | STRING | 0 |
| <input type="checkbox"/> | dSCorePropagationData | STRING | 16010101000000.0Z |
| <input type="checkbox"/> | displayName | STRING | testuserexternal |
| <input type="checkbox"/> | distinguishedName | STRING | CN=testuserexternal,CN=Users,DC=rinsantr,DC=lab |

Cancel OK

Cisco ISE Administration · Identity Management

External Identity Sources

- Certificate Authentication F
- Active Directory
 - RiniAD
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers
 - Social Login

Attributes

| Name | Type | Default | Internal Name |
|---------------|--------|---------|---------------|
| aCSPolicyName | STRING | | aCSPolicyName |

Save Reset

내부 및 외부 사용자를 위한 권한 부여 프로파일 구성

권한 부여 프로파일을 구성하려면 Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다. Add(추가)를 클릭합니다. 이름을 제공하고 내부 사용자의 dACL 이름을 InternalUser:<만든 사용자 지정 특성의

이름>으로 선택합니다. 이미지에 표시된 것처럼 내부 사용자의 경우 프로파일 InternalUserAttributeTest는 InternalUser:ACL로 구성된 dACL로 구성됩니다.

Cisco ISE Policy • Policy Elements

Dictionaryes Conditions **Results**

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name InternalUserAttributeTest

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name InternalUser:ACL

외부 사용자의 경우 <Join point name>:<attribute configured on AD>를 dACL 이름으로 사용합니다. 이 예에서 프로파일 ExternalUserAttributeTest는 RiniAD:aCSPolicyName으로 구성된 dACL로 구성되며, 여기서 RiniAD는 가입 포인트 이름입니다.

Dictionarys Conditions **Results**

- Authentication >
- Authorization ▾
 - Authorization Profiles**
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >


Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type ▾

Network Device Profile  Cisco ▾ ⊕

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

▾ Common Tasks

DACL Name ▾

권한 부여 정책 구성

권한 부여 정책은 외부 사용자가 AD에 있는 그룹 및 ISE 내부 ID 저장소의 사용자 이름을 기반으로 정책 > 정책 집합에서 구성할 수 있습니다. 이 예에서 testuserexternal은 그룹 rinsantr.lab/Users/Test Group에 있는 사용자이며 testuserinternal은 ISE 내부 ID 저장소에 있는 사용자입니다.

Authorization Policy (3)

| | | | | Results | |
|--------|--|------------|---|------------------------------|------------------|
| Status | Rule Name | Conditions | | | |
| | | | Profiles | Security Groups | |
| + | Search | | | | |
| ✓ | Basic Authenticated Access Internal User | AND | <ul style="list-style-type: none"> Network Access-AuthenticationStatus EQUALS AuthenticationPassed Radius-User-Name EQUALS testuserinternal | InternalUserAttributeTe... x | Select from list |
| ✓ | Basic Authenticated Access External User | AND | <ul style="list-style-type: none"> Network Access-AuthenticationStatus EQUALS AuthenticationPassed RiniAD-ExternalGroups EQUALS rinsantr.lab/Users/Test Group | ExternalUserAttributeT... x | Select from list |
| ✓ | Default | | DenyAccess x | Select from list | |

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 작동하는지 확인합니다.

사용자 인증을 확인 하기 위해 RADIUS 라이브 로그를 확인 합니다.

내부 사용자:

| | | | | | | | |
|----------------------------|---|---|------------------|-------------------|--------------|--------------|---------------|
| Jan 18, 2021 03:27:11.5... | ✓ | 🔒 | #ACSACL#-IP-... | | | | |
| Jan 18, 2021 03:27:11.5... | ✓ | 🔒 | testuserinternal | B4:96:91:26:E0:2B | Intel-Device | New Polic... | InternalUs... |


외부 사용자:

| | | | | | | | |
|----------------------------|---|---|------------------|-------------------|--------------|--------------|---------------|
| Jan 18, 2021 03:39:33.3... | ✓ | 🔒 | #ACSACL#-IP-... | | | | |
| Jan 18, 2021 03:39:33.3... | ✓ | 🔒 | testuserexternal | B4:96:91:26:E0:2B | Intel-Device | New Polic... | ExternalUs... |

성공적인 사용자 인증에서 돋보기 아이콘을 클릭하여 요청이 자세한 라이브 로그의 Overview(개요) 섹션에서 올바른 정책에 부합하는지 확인합니다.


내부 사용자:

Overview

| | |
|-----------------------|---|
| Event | 5200 Authentication succeeded |
| Username | testuserinternal |
| Endpoint Id | B4:96:91:26:E0:2B  |
| Endpoint Profile | Intel-Device |
| Authentication Policy | New Policy Set 1 >> Authentication Rule 1 |
| Authorization Policy | New Policy Set 1 >> Basic Authenticated Access Internal User |
| Authorization Result | InternalUserAttributeTest |

외부 사용자:

Overview

| | |
|-----------------------|---|
| Event | 5200 Authentication succeeded |
| Username | testuserexternal |
| Endpoint Id | B4:96:91:26:E0:2B  |
| Endpoint Profile | Intel-Device |
| Authentication Policy | New Policy Set 1 >> Authentication Rule 1 |
| Authorization Policy | New Policy Set 1 >> Basic Authenticated Access External User |
| Authorization Result | ExternalUserAttributeTest |

자세한 라이브 로그의 Other Attributes 섹션에서 사용자 특성이 검색되었는지 확인합니다.

내부 사용자:

| | |
|-----------------|------------------|
| EnableFlag | Enabled |
| ACL | NotMuchAccess |
| RADIUS Username | testuserinternal |



외부 사용자:

| | |
|-----------------|------------------|
| aCSPolicyName | NotMuchAccess |
| RADIUS Username | testuserexternal |

자세한 라이브 로그의 Result 섹션을 확인하여 dACL 특성이 Access-Accept의 일부로 전송되는지 확인합니다.

| | |
|---------------|--|
| cisco-av-pair | ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-NotMuchAccess-60049cbb |
|---------------|--|

또한 RADIUS 라이브 로그를 확인하여 사용자 인증 후 dACL이 다운로드되었는지 확인합니다.

| | | | |
|----------------------------|---|---|--|
| Jan 18, 2021 03:39:33.3... |  |  | #ACSACL#-IP-NotMuchAccess-60049cbb |
|----------------------------|---|---|--|

성공적인 dACL 다운로드 로그에서 돋보기 아이콘을 클릭하고 Overview(개요) 섹션을 확인하여 dACL 다운로드를 확인합니다.

Overview

| | |
|----------------------|------------------------------------|
| Event | 5232 DACL Download Succeeded |
| Username | #ACSACL#-IP-NotMuchAccess-60049cbb |
| Endpoint Id | |
| Endpoint Profile | |
| Authorization Result | |

dACL의 내용을 확인하려면 이 세부 보고서의 Result(결과) 섹션을 확인하십시오.

cisco-av-pair

ip:inacl#1=permit ip any any

문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

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.