

# RADIUS 사용자 인증을 위한 FireSIGHT 시스템 과 ISE 통합

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[ISE 컨피그레이션](#)

[네트워크 디바이스 및 네트워크 디바이스 그룹 구성](#)

[ISE 인증 정책 구성:](#)

[ISE에 로컬 사용자 추가](#)

[ISE 권한 부여 정책 구성](#)

[Sourcefire 시스템 정책 구성](#)

[외부 인증 사용](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 RADIUS(Remote Authentication Dial In User Service) 사용자 인증을 위해 Cisco FMC(FireSIGHT Management Center) 또는 Firepower Managed Device를 Cisco ISE(Identity Services Engine)와 통합하는 데 필요한 컨피그레이션 단계에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- GUI 및/또는 셸을 통한 FireSIGHT System 및 관리되는 디바이스 초기 구성
- ISE에서 인증 및 권한 부여 정책 구성
- 기본 RADIUS 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA v9.2.1
- ASA FirePOWER 모듈 v5.3.1
- ISE 1.2

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

## 구성

### ISE 컨피그레이션

**팁:** Sourcefire와 같은 NAD(Network Access Devices)와의 통합을 지원하도록 ISE 인증 및 권한 부여 정책을 구성하는 여러 가지 방법이 있습니다. 아래 예는 통합을 구성하는 한 가지 방법입니다. 샘플 컨피그레이션은 참조 지점이며 특정 구축의 필요에 맞게 조정할 수 있습니다. 인증 컨피그레이션은 2단계 프로세스입니다. ISE에서 RADIUS 특성 값 쌍(av 쌍)을 FMC 또는 관리 디바이스로 반환하는 권한 부여 정책이 하나 이상 ISE에 정의됩니다. 그런 다음 이러한 av-pair는 FMC 시스템 정책 컨피그레이션에 정의된 로컬 사용자 그룹에 매핑됩니다.


### 네트워크 디바이스 및 네트워크 디바이스 그룹 구성

- ISE GUI에서 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. +Add를 클릭하여 새 NAD(Network Access Device)를 추가합니다. 설명 이름과 장치 IP 주소를 제공 합니다. FMC는 아래 예에 정의되어 있습니다.

#### Network Devices

\* Name   
Description

\* IP Address:  /

- Network Device Group(네트워크 디바이스 그룹)에서 All Device Types(모든 디바이스 유형) 옆의 **주황색 화살표**를 클릭합니다. 아이콘을  클릭하고 Create New Network Device Group을 선택합니다. 다음 예제 스크린샷에서 Device Type Sourcefire가 구성되었습니다. 이 디바이스 유형은 나중에 권한 부여 정책 규칙 정의에서 참조됩니다. 저장을 클릭합니다.

#### Create New Network Device Group...

##### Network Device Groups

\* Parent  

\* Name

Description

\* Type

- **주황색 화살표**를 다시 클릭하고 위 단계에서 구성된 네트워크 디바이스 그룹을 선택합니다.

\* Network Device Group

Location

Device Type

- Authentication Settings(인증 설정) 옆의 **확인란**을 선택합니다. 이 NAD에 사용할 RADIUS 공유 비밀 키를 입력합니다. FireSIGHT MC에서 RADIUS 서버를 구성할 때 나중에 동일한 공유 비밀 키가 다시 사용됩니다. 일반 텍스트 키 값을 검토하려면 **표시** 단추를 클릭합니다. 저장을 클릭합니다.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

- GUI 및/또는 셸 액세스를 위해 RADIUS 사용자 인증/권한 부여가 필요한 모든 FireSIGHT MC 및 관리되는 디바이스에 대해 위의 단계를 반복합니다.

**ISE 인증 정책 구성:**

- ISE GUI에서 Policy(정책) > **Authentication(인증)**으로 이동합니다. Policy Sets(정책 집합)를 사용하는 경우 Policy(정책) > **Policy Sets(정책 집합)**로 이동합니다. 아래 예는 기본 인증 및 권한 부여 정책 인터페이스를 사용하는 ISE 구축에서 가져온 것입니다. 인증 및 권한 부여 규칙 논리는 컨피그레이션 방식과 상관없이 동일합니다.
- 기본 규칙(**일치하지 않는 경우**)은 사용 중인 방법이 MAB(MAC Authentication Bypass) 또는 802.1X가 아닌 NAD의 RADIUS 요청을 인증하는 데 사용됩니다. 기본적으로 구성된 대로 이 규칙은 ISE의 로컬 내부 사용자 ID 소스에서 사용자 계정을 찾습니다. 이 컨피그레이션은 Administration(관리) > Identity Management(ID 관리) > External Identity Sources(**외부 ID 소스**)에 정의된 대로 Active Directory, LDAP 등과 같은 외부 ID 소스를 참조하도록 수정할 수 있습니다. 이 예에서는 인증 정책을 더 이상 수정할 필요가 없도록 ISE에서 사용자 계정을 로컬로 정의합니다.

## Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type  Simple  Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access	and
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints		
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access	and
<input checked="" type="checkbox"/>	Default	: use Guest_Portal_Sequence		
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : Internal Users	

## ISE에 로컬 사용자 추가

- Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자)로 이동합니다. Add(추가)를 클릭합니다. 의미 있는 사용자 이름 및 비밀번호를 입력합니다. User Groups(사용자 그룹) 선택에서 기존 그룹 이름을 선택하거나 **녹색 + 기호**를 클릭하여 새 그룹을 추가합니다. 이 예에서는 사용자 "sfadmin"이 사용자 지정 그룹 "Sourcefire Administrator"에 할당됩니다. 이 사용자 그룹은 아래의 **Configuring ISE Authorization Policy(ISE 권한 부여 정책 구성)** 단계에 정의된 권한 부여 프로파일에 연결됩니다. 저장을 클릭합니다.

### Network Access User

\* Name

Status  Enabled ▾

Email

### Password

\* Password

Need help with password policy ? ⓘ

\* Re-Enter Password

### User Information

First Name

Last Name

### Account Options

Description

Change password on next login

### User Groups

▾ - +

## ISE 권한 부여 정책 구성

- Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다. 새 권한 부여 프로파일을 추가하려면 **녹색 + 기호**를 클릭합니다.
- Sourcefire Administrator와 같은 설명적인 이름을 제공합니다. **액세스 유형에 대해 ACCESS\_ACCEPT를 선택합니다.** Common Tasks(일반 작업)에서 아래쪽으로 스크롤하여 **ASA VPN** 옆의 상자를 선택합니다. **주황색 화살표**를 클릭하고 InternalUser:IdentityGroup을 선택합니다. 저장을 클릭합니다.

**팁:** 이 예에서는 ISE 로컬 사용자 ID 저장소를 사용하므로 InternalUser:IdentityGroup 그룹 옵션을 사용하여 컨피그레이션을 간소화합니다. 외부 ID 저장소를 사용하는 경우 ASA VPN 권한 부여 특성이 계속 사용되지만 Sourcefire 디바이스로 반환되는 값은 수동으로 구성됩니다. 예를 들어, ASA VPN 드롭다운 상자에 Administrator를 수동으로 입력하면 Class-25 av 쌍 값 Class = Administrator가 Sourcefire 디바이스로 전송됩니다. 그런 다음 시스템 정책 컨피그레이션의 일부로 sourcefire 사용자 그룹에 이 값을 매핑할 수 있습니다. 내부 사용자의 경우 두 컨피그레이션 방법을 사용할 수 있습니다.

내부 사용자 예

\* Name

Description

\* Access Type  ▼

Service Template

▼ Common Tasks

MACSEC Policy

NEAT

Web Authentication (Local Web Auth)

Airespace ACL Name

ASA VPN

▼

▼ Advanced Attributes Settings

▼ =  ▼ - +

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = InternalUser:IdentityGroup

외부 사용자 예

Advanced Attributes Settings

Select an item = [ ] - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

- Policy(정책) > Authorization(권한 부여)으로 이동하고 Sourcefire 관리 세션에 대한 새 권한 부여 정책을 구성합니다. 아래 예에서는 DEVICE:Device Type 조건을 사용하여 위의 **Configuring Network Devices and Network Device Groups(네트워크 디바이스 및 네트워크 디바이스 그룹 구성)** 섹션. 이 정책은 위에서 구성한 Sourcefire 관리자 권한 부여 프로파일과 연결됩니다. 저장을 클릭합니다.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Sourcefire Administrator	if DEVICE:Device Type EQUALS All Device Types#Sourcefire	then Sourcefire Administrator
✓	CWA-PSN1	if Network Access:ISE Host Name EQUALS ise12-psn1	then CWA-PSN1
✓	CWA-PSN2	if Network Access:ISE Host Name EQUALS ise12-psn2	then CWA-PSN2

### Sourcefire 시스템 정책 구성

- FireSIGHT MC에 로그인하고 **System > Local > User Management**로 이동합니다. Login **Authentication** 탭을 클릭합니다. + **Create Authentication Object(인증 개체 생성)** 버튼을 클릭하여 사용자 인증/권한 부여를 위한 새 RADIUS 서버를 추가합니다.
- Authentication Method(인증 방법)**에 대해 RADIUS를 선택합니다. RADIUS 서버를 설명하는 이름을 입력합니다. **Host Name/IP Address** 및 **RADIUS Secret Key**를 입력합니다. 비밀 키는 ISE에서 이전에 구성한 키와 일치해야 합니다. 선택적으로 백업 ISE 서버 **호스트 이름/IP 주소** (있는 경우)를 입력합니다.

## Authentication Object

Authentication Method

RADIUS

Name \*

ISE

Description

## Primary Server

Host Name/IP Address \*

10.1.1.254

Port \*

1812

RADIUS Secret Key

••••••••

## Backup Server (Optional)

Host Name/IP Address

Port

1812

RADIUS Secret Key

- **RADIUS Specific Parameters** 섹션 아래에서 GUI 액세스에 대해 매칭할 Sourcefire 로컬 그룹 이름 옆의 텍스트 상자에 Class-25 av-pair 문자열을 입력합니다. 이 예에서는 Class=User Identity Groups:Sourcefire Administrator 값이 Sourcefire Administrator 그룹에 매핑됩니다. ISE가 ACCESS-ACCEPT의 일부로 반환하는 값입니다. 선택적으로, Class-25 그룹이 할당되지 않은 인증된 사용자에게 대해 **Default User Role**을 선택합니다. Save(**저장**)를 클릭하여 컨피그레이션을 저장하거나 아래 Verify(확인) 섹션으로 이동하여 ISE와의 인증을 테스트합니다.



## RADIUS-Specific Parameters

Timeout (Seconds)	<input type="text" value="30"/>
Retries	<input type="text" value="3"/>
Access Admin	<input type="text"/>
Administrator	<input type="text" value="Class=User Identity&lt;br/&gt;Groups:Sourcefire Administrator"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text"/>
Security Analyst	<input type="text"/>
Security Analyst (Read Only)	<input type="text"/>
Security Approver	<input type="text"/>
Default User Role	<input type="text" value="Access Admin&lt;br/&gt;Administrator&lt;br/&gt;Discovery Admin&lt;br/&gt;External Database User"/>

- Shell Access Filter(셸 액세스 필터)에서 셸/SSH 세션을 제한할 사용자 목록을 쉼표로 구분하여 입력합니다.

## Shell Access Filter

Administrator Shell Access User List	<input type="text" value="user1, user2, user3"/>
--------------------------------------	--

## 외부 인증 사용

마지막으로 FMC에서 외부 인증을 활성화하려면 다음 단계를 완료하십시오.

1. 다음으로 이동 시스템 > 로컬 > 시스템 정책.
2. 선택 외부 인증 왼쪽 패널에 표시됩니다.
3. Status(상태)를 사용 (기본적으로 비활성화됨)
4. 추가된 ISE RADIUS 서버를 활성화합니다.
5. 정책을 저장하고 어플라이언스에서 정책을 다시 적용합니다.

Access Control Preferences

Access List

Audit Log Settings

Dashboard

Database

DNS Cache

Email Notification

► External Authentication

Intrusion Policy Preferences

Language

Login Banner

Network Analysis Policy Preferences

SNMP

STIG Compliance

Time Synchronization

User Interface

Vulnerability Mapping

Save Policy and Exit Cancel

Status Enabled

Default User Role Administrator

Shell Authentication Disabled

CAC Authorization Disabled

Name	Description	Method	Server:Port	Encryption
ISE		RADIUS	10.1.1.254:1812	no

## 다음을 확인합니다.

- ISE에 대한 사용자 인증을 테스트하려면 Additional Test Parameters 섹션으로 아래로 스크롤 하여 ISE 사용자에게 대한 사용자 이름과 비밀번호를 입력합니다. 테스트를 클릭합니다. 테스트를 성공적으로 수행하면 녹색 성공이 발생합니다. 브라우저 창 상단에 테스트 완료 메시지가 표시됩니다.

Additional Test Parameters

User Name sfadmin

Password .....

\*Required Field

Save Test Cancel

- 테스트 인증 결과를 보려면 Test Output 섹션으로 이동하여 Show Details(세부 정보 표시) 옆의 검은색 화살표를 클릭합니다. 아래 예제 스크린샷에서 "radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|" 값이 ISE에서 수신되었습니다. 이 값은 위의 FireSIGHT MC에 구성된 로컬 Sourcefire 그룹과 연결된 Class 값과 일치해야 합니다. 저장을 클릭합니다.

## Test Output

Show Details

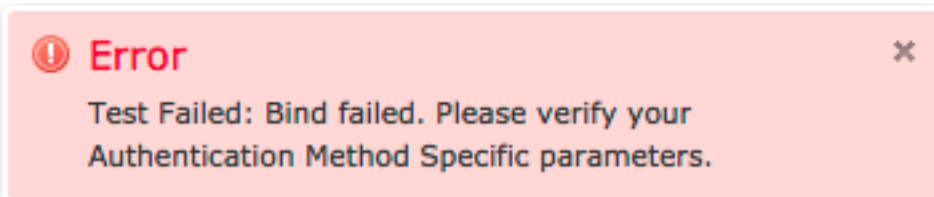
```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth - response: [Class=CACS:0ac9e8cb0000006539F4896:ise12-psn1/191969386/7]
"sfadmin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=User Identity Groups:Sourcefire Administrator] - [Class=User Identity Groups:Sourcefire Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```


- ISE 관리 GUI에서 **Operations(작업) > Authentications(인증)**로 이동하여 사용자 인증 테스트의 성공 또는 실패를 확인합니다.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2014-06-16 18:41:55.940	✓		0	sfadmin			Sourcefire3D-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:41:24.947	✗		0	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:41:10.088	✗		0	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:40:00.856	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:44:55.751	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:41:02.876	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:39:30.388	✗		0	sfadmin			SFR-DC			User Identity Groups...		ise12-psn1	Authentication f...

## 문제 해결

- ISE에 대한 사용자 인증을 테스트할 때 다음 오류는 RADIUS 암호 키 불일치 또는 잘못된 사용자 이름/비밀번호를 나타냅니다.



- ISE 관리 GUI에서 **Operations(작업) > Authentications(인증)**로 이동합니다. 빨간색 **이벤트**는 실패를 나타내는 반면 **녹색** 이벤트는 성공적인 인증/권한 부여/권한 변경을 나타냅니다. 인증 이벤트의 세부 정보를 검토하려면  아이콘을 클릭합니다.

## Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

## Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

## 관련 정보

[기술 지원 및 문서 - Cisco Systems](#)