

# Integration des FireSIGHT-Systems mit der ISE für die RADIUS-Benutzerauthentifizierung

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[ISE-Konfiguration](#)

[Konfigurieren von Netzwerkgeräten und Netzwerkgerätegruppen](#)

[Konfigurieren der ISE-Authentifizierungsrichtlinie:](#)

[Hinzufügen eines lokalen Benutzers zur ISE](#)

[Konfigurieren der ISE-Autorisierungsrichtlinie](#)

[Konfiguration der Sourcefire-Systemrichtlinien](#)

[Externe Authentifizierung aktivieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument werden die Konfigurationsschritte beschrieben, die zur Integration eines Cisco FireSIGHT Management Center (FMC) oder eines FirePOWER Managed Device in die Cisco Identity Services Engine (ISE) für die Remote Authentication Dial In User Service (RADIUS)-Benutzerauthentifizierung erforderlich sind.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Erstkonfiguration von FireSIGHT-Systemen und verwalteten Geräten über GUI und/oder Shell
- Konfigurieren von Authentifizierungs- und Autorisierungsrichtlinien für die ISE
- Grundlegendes RADIUS-Wissen

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA v9.2.1

- ASA FirePOWER-Modul v5.3.1
- ISE 1.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konfiguration

### ISE-Konfiguration

**Tipp:** Es gibt mehrere Möglichkeiten, ISE-Authentifizierungs- und Autorisierungsrichtlinien zu konfigurieren, um die Integration mit Network Access Devices (NAD) wie Sourcefire zu unterstützen. Das nachfolgende Beispiel ist eine Möglichkeit, die Integration zu konfigurieren. Die Beispielkonfiguration ist ein Bezugspunkt und kann an die Anforderungen der jeweiligen Bereitstellung angepasst werden. Beachten Sie, dass die Autorisierungskonfiguration ein zweistufiger Prozess ist. Auf der ISE werden eine oder mehrere Autorisierungsrichtlinien definiert, wobei die ISE RADIUS-Attributwertpaare (av-pair) an das FMC oder das verwaltete Gerät zurückgibt. Diese Av-Paare werden dann einer lokalen Benutzergruppe zugeordnet, die in der Konfiguration der FMC-Systemrichtlinien definiert ist.

### Konfigurieren von Netzwerkgeräten und Netzwerkgerätegruppen

- Navigieren Sie in der ISE-GUI zu **Administration > Network Resources > Network Devices**. Klicken Sie auf **+Hinzufügen**, um ein neues Netzwerkzugriffsgerät (Network Access Device, NAD) hinzuzufügen. Geben Sie einen beschreibenden Namen und eine Geräte-IP-Adresse an. Das FMC wird im folgenden Beispiel definiert.

#### Network Devices

\* Name   
 Description

\* IP Address:  /

- Klicken Sie unter **Netzwerkgerätgruppe** auf den **orangefarbenen Pfeil** neben **Alle Gerätetypen**. Klicken Sie auf das  Symbol, und wählen Sie **Neue Netzwerkgerätegruppe erstellen aus**. Im folgenden Beispiel-Screenshot wurde der Gerätetyp Sourcefire konfiguriert. Auf diesen Gerätetyp wird in einem späteren Schritt in der Definition der Autorisierungsrichtlinie verwiesen. Klicken Sie auf **Speichern**.

Create New Network Device Group... ✕

### Network Device Groups

\* Parent

\* Name

Description

\* Type

- Klicken Sie erneut auf den **orangefarbenen Pfeil**, und wählen Sie die im obigen Schritt konfigurierte Netzwerkgerätegruppe aus.

\* Network Device Group

Location

Device Type

- Aktivieren Sie das Kontrollkästchen neben **Authentifizierungseinstellungen**. Geben Sie den für diese NAD verwendeten gemeinsamen geheimen Schlüssel für den RADIUS ein. Beachten Sie, dass der gleiche geheime Schlüssel später erneut verwendet wird, wenn der RADIUS-Server auf dem FireSIGHT MC konfiguriert wird. Um den Wert für den Nur-Text-Schlüssel zu überprüfen, klicken Sie auf die Schaltfläche **Anzeigen**. Klicken Sie auf **Speichern**.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

- Wiederholen Sie die oben genannten Schritte für alle FireSIGHT MCs und Managed Devices, die eine RADIUS-Benutzerauthentifizierung bzw. -autorisierung für den Zugriff auf die Benutzeroberfläche und/oder die Shell erfordern.

### Konfigurieren der ISE-Authentifizierungsrichtlinie:

- Navigieren Sie in der ISE-GUI zu **Richtlinien > Authentifizierung**. Wenn Sie Policy Sets verwenden, navigieren Sie zu **Policy > Policy Sets (Richtlinien > Richtlinienätze)**. Das nachfolgende Beispiel stammt von einer ISE-Bereitstellung, die die Standardschnittstellen für

Authentifizierung und Autorisierung verwendet. Die Authentifizierungs- und Autorisierungsregellogik ist unabhängig vom Konfigurationsansatz identisch.

- Die **Standardregel (falls keine Übereinstimmung vorliegt)** wird zur Authentifizierung von RADIUS-Anfragen von NADs verwendet, bei denen die verwendete Methode nicht MAC Authentication Bypass (MAB) oder 802.1X ist. Wie standardmäßig konfiguriert, sucht diese Regel nach Benutzerkonten in der lokalen **internen Benutzer**-Identitätsquelle der ISE. Diese Konfiguration kann so geändert werden, dass sie auf eine externe Identitätsquelle wie Active Directory, LDAP usw. verweist, wie unter **Administration > Identity Management > External Identity Sources** definiert. Aus Gründen der Einfachheit werden in diesem Beispiel Benutzerkonten lokal auf der ISE definiert, sodass keine weiteren Änderungen an der Authentifizierungsrichtlinie erforderlich sind.

#### 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	

#### Hinzufügen eines lokalen Benutzers zur ISE

- Navigieren Sie zu **Administration > Identity Management > Identities > Users**. Klicken Sie auf **Hinzufügen**. Geben Sie einen aussagekräftigen Benutzernamen und ein Kennwort ein. Wählen Sie unter der Auswahl **Benutzergruppen** einen vorhandenen Gruppennamen aus, oder klicken Sie auf das **grüne + Zeichen**, um eine neue Gruppe hinzuzufügen. In diesem Beispiel wird der Benutzer "sfadmin" der benutzerdefinierten Gruppe "Sourcefire Administrator" zugewiesen. Diese Benutzergruppe wird mit dem Autorisierungsprofil verknüpft, das im nachfolgenden Schritt **Konfigurieren der ISE-Autorisierungsrichtlinie** definiert wurde. Klicken Sie auf **Speichern**.

▼ 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

▼ - +

## Konfigurieren der ISE-Autorisierungsrichtlinie

- Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**. Klicken Sie auf das **grüne +-Zeichen**, um ein neues Autorisierungsprofil hinzuzufügen.
- Geben Sie einen beschreibenden Namen wie Sourcefire Administrator ein. Wählen Sie **ACCESS\_ACCEPT** als **Zugriffstyp aus**. Scrollen Sie unter "**Allgemeine Aufgaben**" zum unteren Rand, und aktivieren Sie das Kontrollkästchen neben **ASA VPN**. Klicken Sie auf den **orangefarbenen Pfeil**, und wählen Sie **InternalUser:IdentityGroup** aus. Klicken Sie auf **Speichern**.

**Tipp:** Da in diesem Beispiel der lokale ISE-Benutzeridentitätsspeicher verwendet wird, wird die Option InternalUser:IdentityGroup verwendet, um die Konfiguration zu vereinfachen. Wenn ein externer Identitätsdatenspeicher verwendet wird, wird das ASA VPN-Autorisierungsattribut verwendet. Der an das Sourcefire-Gerät zurückzugebende Wert wird jedoch manuell konfiguriert. Wenn Sie beispielsweise Administrator manuell in das ASA VPN-Dropdown-Feld eingeben, wird ein Class-25-av-pair-Wert von Class = Administrator an das Sourcefire-Gerät gesendet. Dieser Wert kann dann einer Sourcefire-Benutzergruppe als

Teil der Systemrichtlinienkonfiguration zugeordnet werden. Für interne Benutzer ist jede Konfigurationsmethode zulässig.

#### Beispiel für internen Benutzer

\* 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

## Beispiel für externen Benutzer

ASA VPN

Administrator

### Advanced Attributes Settings

Select an item = [ ] - +

### Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

- Navigieren Sie zu **Richtlinien > Autorisierung**, und konfigurieren Sie eine neue Autorisierungsrichtlinie für die Sourcefire-Verwaltungssitzungen. Im folgenden Beispiel wird die Bedingung **DEVICE:Device Type (GERÄT:Gerätetyp)** verwendet, um dem im Abschnitt **"Konfigurieren von Netzwerkgeräten und Netzwerkgerätegruppen"** weiter oben. Diese Richtlinie wird dann dem oben konfigurierten Sourcefire Administrator-Autorisierungsprofil zugeordnet. Klicken Sie auf **Speichern**.

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

## Konfiguration der Sourcefire-Systemrichtlinien

- Melden Sie sich beim FireSIGHT MC an, und navigieren Sie zu **System > Local > User Management**. Klicken Sie auf die Registerkarte **Login Authentication** (Anmeldenauthentifizierung). Klicken Sie auf die Schaltfläche **+ Create Authentication Object (Authentifizierungsobjekt erstellen)**, um einen neuen RADIUS-Server für die Benutzerauthentifizierung/-autorisierung hinzuzufügen.

- Wählen Sie **RADIUS** als **Authentifizierungsmethode** aus. Geben Sie einen beschreibenden Namen für den RADIUS-Server ein. Geben Sie den **Hostnamen/die IP-Adresse** und den **geheimen RADIUS-Schlüssel** ein. Der geheime Schlüssel muss mit dem zuvor auf der ISE konfigurierten Schlüssel übereinstimmen. Geben Sie optional einen Backup-ISE-Server-**Hostnamen/eine IP-Adresse** ein, falls vorhanden.

**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:

- Geben Sie im Abschnitt **RADIUS-spezifische Parameter** die Zeichenfolge Class-25 av-pair in das Textfeld neben dem lokalen Gruppennamen von Sourcefire ein, der für den GUI-Zugriff zugeordnet werden soll. In diesem Beispiel wird der Wert Class=User Identity Groups:Sourcefire Administrator der Sourcefire Administrator-Gruppe zugeordnet. Dies ist der Wert, den die ISE im Rahmen der ACCESS-ACCEPT zurückgibt. Wählen Sie optional eine **Standardbenutzerrolle** für authentifizierte Benutzer aus, denen keine Class-25-Gruppen zugewiesen sind. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern, oder fahren Sie mit dem Abschnitt Überprüfen unten fort, um die Authentifizierung mit der ISE zu testen.

## 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"/>

- Geben Sie unter **Shell Access Filter (Shell-Zugriffsfiler)** eine kommasetrennte Liste von Benutzern ein, um Shell/SSH-Sitzungen zu beschränken.

## Shell Access Filter

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

## Externe Authentifizierung aktivieren

Führen Sie abschließend die folgenden Schritte aus, um die externe Authentifizierung auf dem FMC zu aktivieren:

1. Navigieren zu **System > Lokal > Systemrichtlinie**.
2. Auswählen **Externe Authentifizierung** auf der linken Seite.
3. Ändern Sie den *Status* in **Aktiviert** (Standardmäßig deaktiviert).
4. Aktivieren Sie den hinzugefügten ISE RADIUS-Server.
5. Speichern Sie die Richtlinie, und wenden Sie die Richtlinie erneut auf die Appliance an.

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

## Überprüfung

- Um die Benutzerauthentifizierung mit der ISE zu testen, scrollen Sie nach unten zum Abschnitt **Zusätzliche Testparameter** und geben Sie einen Benutzernamen und ein Kennwort für den ISE-Benutzer ein. Klicken Sie auf **Test**. Ein erfolgreicher Test führt zu einer **grünen** Meldung: Test abgeschlossen am oberen Rand des Browserfensters.

**Additional Test Parameters**

User Name: sfadmin

Password: .....

\*Required Field

Save Test Cancel

- Um die Ergebnisse der Testauthentifizierung anzuzeigen, gehen Sie zum Abschnitt **Testausgabe**, und klicken Sie auf den **schwarzen** Pfeil neben **Details anzeigen**. Beachten Sie im folgenden Beispielbildschirm den Abschnitt "radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|" -Wert, der von der ISE empfangen wurde. Dies muss mit dem Class-Wert übereinstimmen, der der lokalen Sourcefire-Gruppe zugeordnet ist, die oben

im FireSIGHT MC konfiguriert wurde. Klicken Sie auf **Speichern**.

### Test Output

Show Details

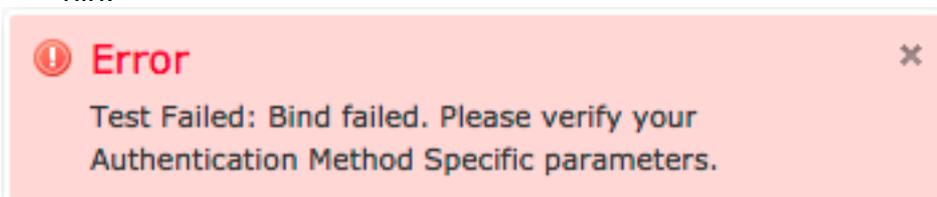
```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth - response: [Class=CACS:0ac9e8cb0000006539F4896:ise12-pn1/191969386/7]
"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:
```

- Navigieren Sie in der ISE Admin-GUI zu **Operations > Authentications (Vorgänge > Authentifizierungen)**, um den Erfolg oder Misserfolg des Benutzerauthentifizierungstests zu überprüfen.

Time	Status	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2014-06-16 18:41:25.940	Success	1	sfadmin			Sourcefire3D-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-pn1	Authentication f...
2014-06-16 18:41:24.947	Failure	1	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-pn1	Authentication f...
2014-06-16 18:41:10.088	Failure	1	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-pn1	Authentication f...
2014-06-16 18:46:00.856	Success	1	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-pn1	Authentication ...
2014-06-16 18:44:35.751	Success	1	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-pn1	Authentication ...
2014-06-16 18:41:02.876	Success	1	sfadmin			SFR-DC		Sourcefire_Admin		NotApplicable	ise12-pn1	Authentication ...
2014-06-16 18:39:30.388	Failure	1	sfadmin			SFR-DC					ise12-pn1	Authentication f...

## Fehlerbehebung

- Beim Testen der Benutzerauthentifizierung mit ISE deutet der folgende Fehler auf eine RADIUS Secret Key-Dismatch oder einen falschen Benutzernamen/ein falsches Kennwort hin.



- Navigieren Sie in der Administratorbenutzeroberfläche der ISE zu **Operations > Authentications (Vorgänge > Authentifizierungen)**. Ein **rotes** Ereignis weist auf einen Ausfall hin, während ein **grünes** Ereignis auf eine erfolgreiche Authentifizierung/Autorisierung/Autorisierungsänderung hinweist. Klicken Sie auf das  Symbol, um die Details des Authentifizierungsereignisses anzuzeigen.

## 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

## Zugehörige Informationen

[Technischer Support und Dokumentation für Cisco Systeme](#)