Integration of FireSIGHT System with ISE for RADIUS User Authentication

Contents

Introduction

This document describes the configuration steps required to integrate a Cisco FireSIGHT Management Center (FMC) or Firepower Managed Device with Cisco Identity Services Engine (ISE) for Remote Authentication Dial In User Service (RADIUS) user authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FireSIGHT System and Managed Device initial configuration via GUI and/or shell
- Configuring authentication and authorization policies on ISE
- Basic RADIUS knowledge

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

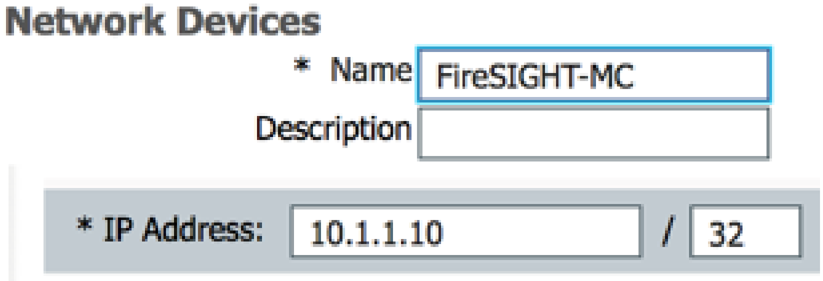
Configure

ISE Configuration

> **Tip**: There are multiple ways to configure ISE authentication and authorization policies to support integration with Network Access Devices (NAD) such as Sourcefire. The example below is one way to configure the intregration. The sample configuration is a point of reference and can be adapted to suit the needs of the specific deployment. Note that the authorization configuration is a two step process. One or more authorization policies will be defined on ISE with ISE returning RADIUS attribute value pairs (av-pairs) to the FMC or Managed Device. These av-pairs are then mapped to a local user group defined in the FMC system policy configuration.

Configuring Network Devices and Network Device Groups

- From the ISE GUI, navigate to **Administration > Network Resources > Network Devices**. Click **+Add** to add a new Network Access Device (NAD). Provide a descriptive name and device IP address. The FMC is defined in the example below.



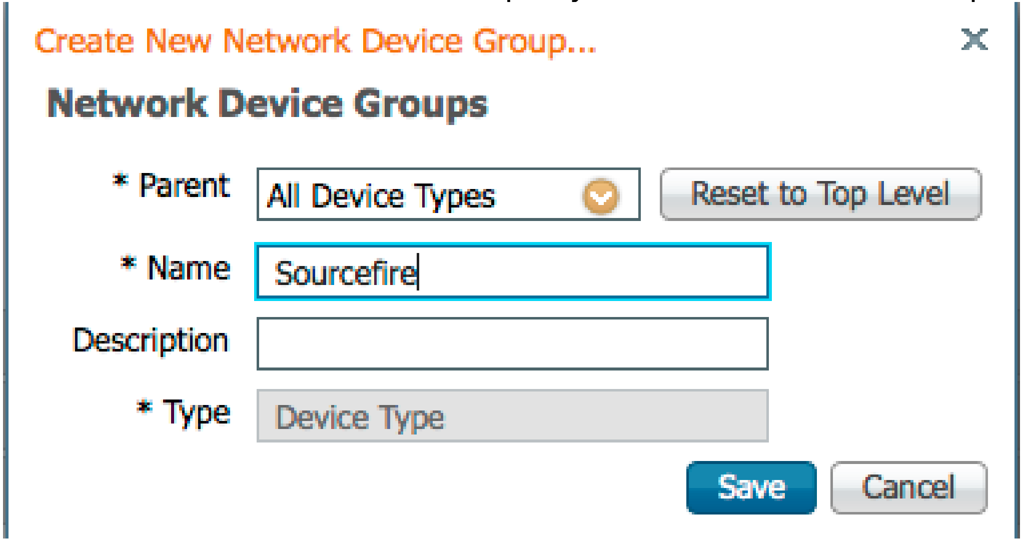
Network Devices

* Name FireSIGHT-MC

Description

* IP Address: 10.1.1.10 / 32

- Under **Network Device Group**, click on the **orange arrow** next to **All Device Types.** Click on the ⚙ icon and select **Create New Network Device Group**. In the example screenshot that follows, the Device Type Sourcefire has been configured. This Device Type will be referenced in the authorization policy rule definition in a later step. Click **Save**.



Create New Network Device Group...

Network Device Groups

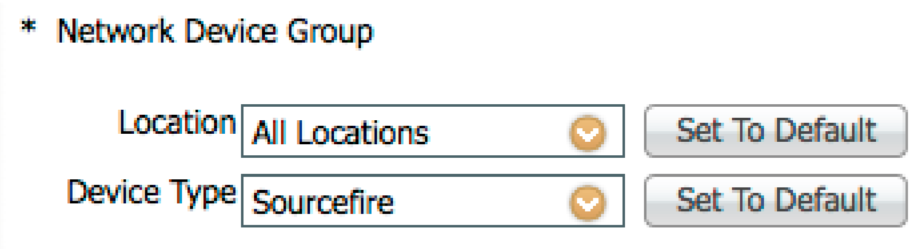
* Parent All Device Types

* Name Sourcefire

Description

* Type Device Type

- Click the orange arrow again and select the Network Device Group configured in the step above

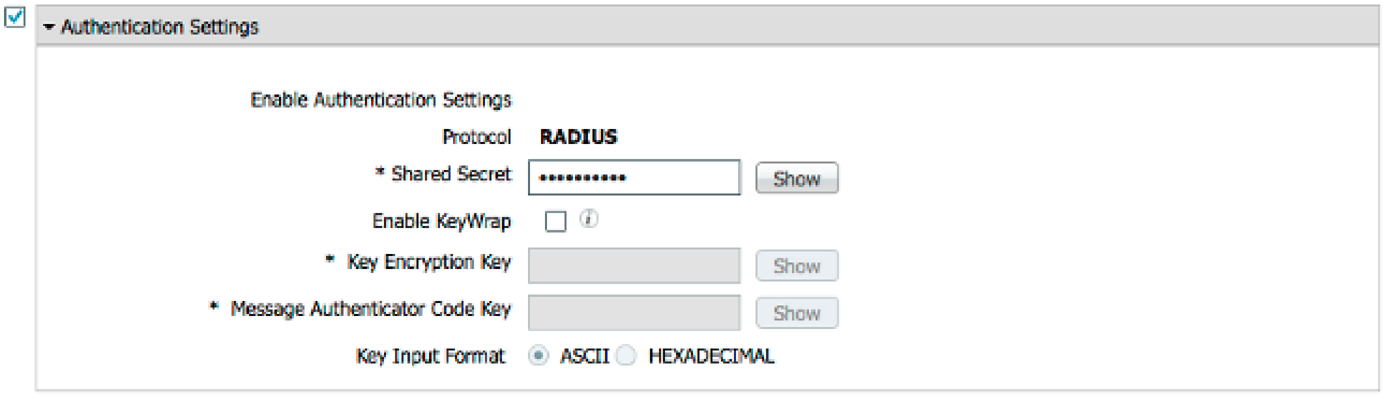


* Network Device Group

Location: All Locations — Set To Default

Device Type: Sourcefire — Set To Default

- Check the box next to **Authentication Settings**. Enter the RADIUS shared secret key that will be used for this NAD. Note the same shared secret key will be used again later when configuring the RADIUS server on the FireSIGHT MC. To review the plain text key value, click the **Show** button. Click **Save**.



☑ Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: ••••••••••• Show

Enable KeyWrap: □

* Key Encryption Key: Show

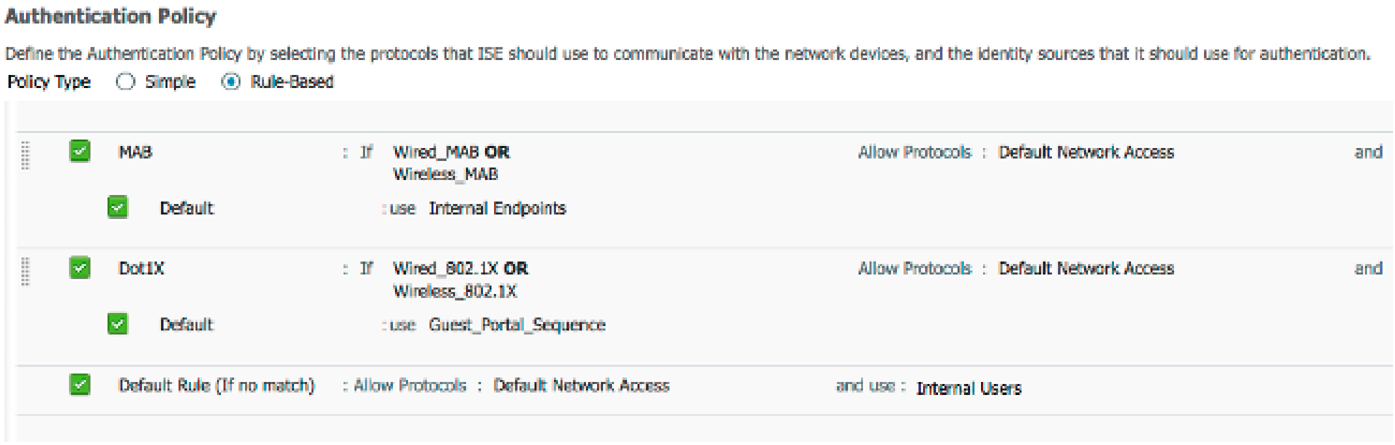
* Message Authenticator Code Key: Show

Key Input Format: ● ASCII ○ HEXADECIMAL

- Repeat the above steps for all FireSIGHT MCs and Managed Devices that will require RADIUS user authentication/authorization for GUI and/or shell access.

Configuring ISE Authentication Policy:

- From the ISE GUI, navigate to **Policy > Authentication**. If using Policy Sets, navigate to **Policy > Policy Sets**. The example below is taken from an ISE deployment that uses the default authentication and authorization policy interfaces. The authentication and authorization rule logic is the same regardless of the configuration approach.
- The **Default Rule (If no match)** will be used to authenticate RADIUS requests from NADs where the method in use is not MAC Authentication Bypass (MAB) or 802.1X. As configured by default, this rule will look for user accounts in ISE's local **Internal Users** identity source. This configuration can be modified to refer to an external identity source such as Active Directory, LDAP, etc as defined under **Administration > Identity Management > External Identity Sources**. For sake of simplciity, this example will define user accounts locally on ISE so no further modifications to the authentication policy are required.



Authentication Policy

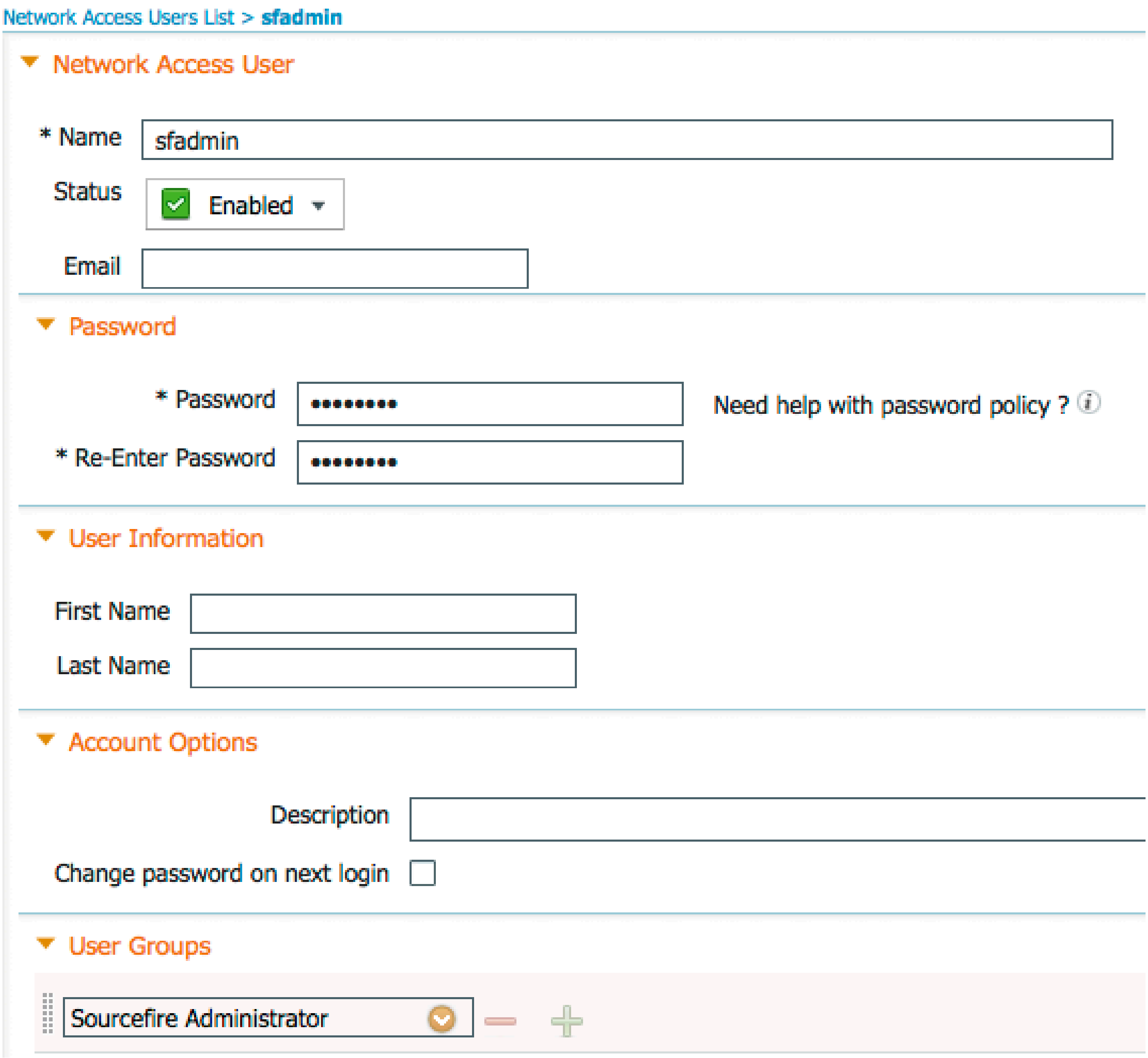
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB	: If	Wired_MAB **OR** Wireless_MAB	Allow Protocols :	Default Network Access	and
☑ Default	: use	Internal Endpoints			
☑ Dot1X	: If	Wired_802.1X **OR** Wireless_802.1X	Allow Protocols :	Default Network Access	and
☑ Default	: use	Guest_Portal_Sequence			
☑ Default Rule (If no match)	: Allow Protocols :	Default Network Access	and use :	Internal Users	

Adding a Local User to ISE

- Navigate to **Administration > Identity Management > Identities > Users**. Click **Add**. Enter a meaningful username and password. Under the **User Groups** selection, select an existing group name or click the **green + sign** to add a new group. In this example, the user "sfadmin" is assigned to the custom group "Sourcefire Administrator". This user group will be linked to the authorization profile defined in the **Configuring ISE Authorization Policy** step below. Click **Save**.



Network Access Users List > **sfadmin**

Network Access User

* Name: sfadmin

Status: ☑ Enabled

Email:

Password

* Password: •••••••••

* Re-Enter Password: •••••••••

Need help with password policy ?

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

User Groups

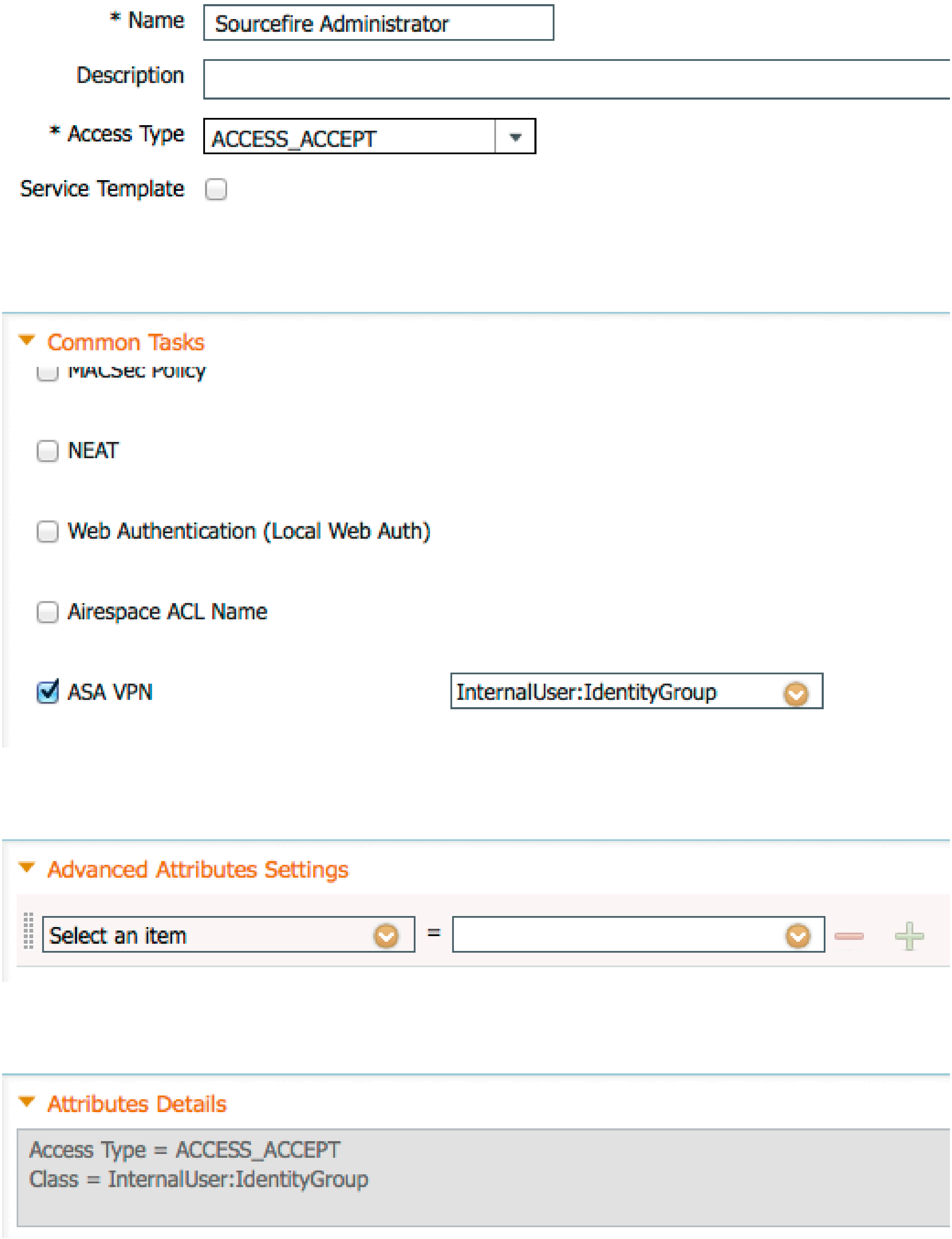
Sourcefire Administrator

Configuring ISE Authorization Policy

- Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Click the **green + sign** to add a new authorization profile.
- Provide a descriptive Name such as Sourcefire Administrator. Select **ACCESS_ACCEPT** for the **Access Type**. Under **Common Tasks**, scroll to the bottom and check the box next to **ASA VPN**. Click the **orange arrow** and select **InternalUser:IdentityGroup**. Click **Save**.

> **Tip**: Because this example uses the ISE local user identity store, the InternalUser:IdentityGroup group option is used to simplify the configuration. If using an external identity store, the ASA VPN authorization attribute is still used, however, the value to be returned to the Sourcefire device is manually configured. For example, manually typing Administrator in the ASA VPN drop down box will result in a Class-25 av-pair value of Class = Administrator being sent to the Sourcefire device. This value can then be mapped to a sourcefire user group as part of the system policy configuration. For internal users, either configuration method is acceptable.

Internal User Example



* Name: Sourcefire Administrator

Description:

* Access Type: ACCESS_ACCEPT

Service Template □

Common Tasks

□ MACSec Policy

□ NEAT

□ Web Authentication (Local Web Auth)

□ Airespace ACL Name

☑ ASA VPN: InternalUser:IdentityGroup

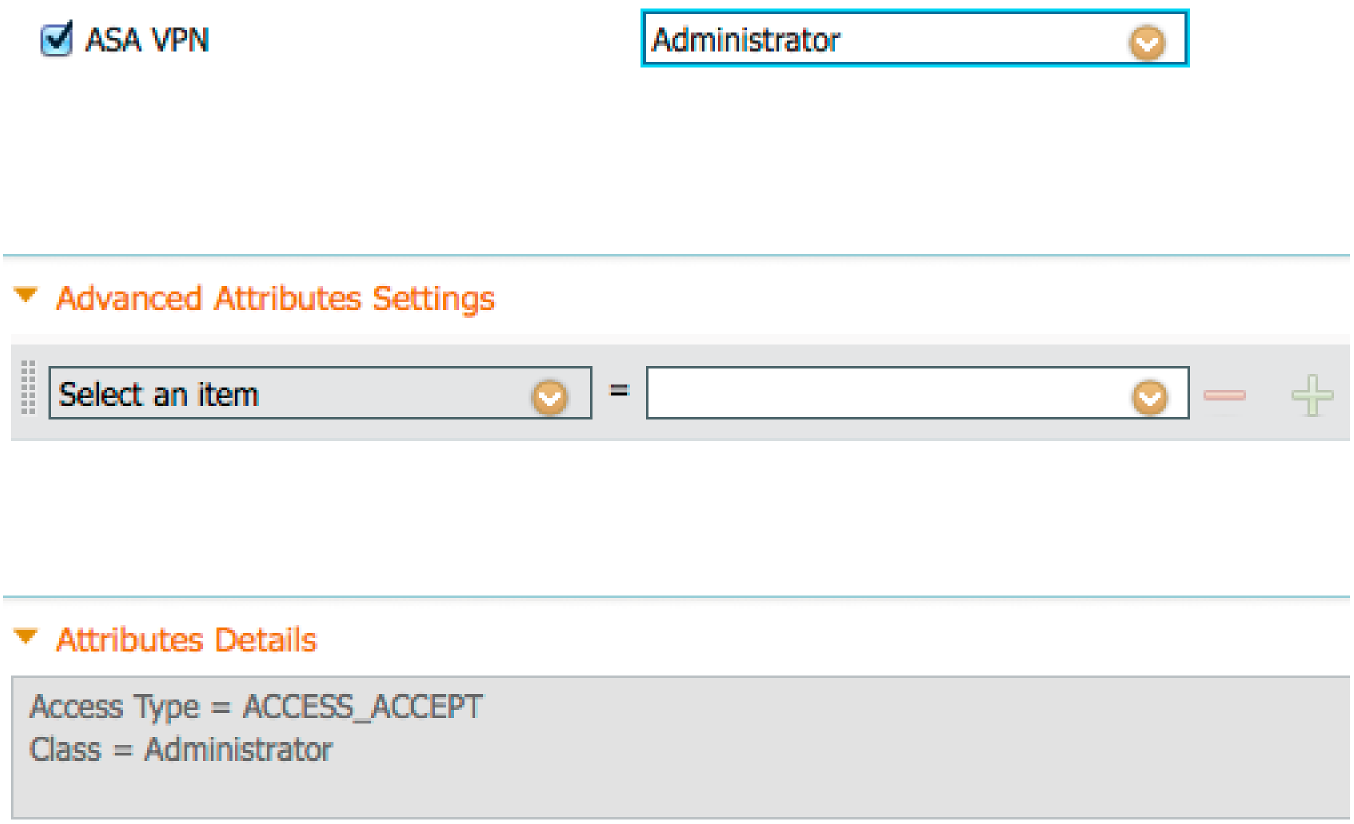
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = InternalUser:IdentityGroup

External User Example



☑ ASA VPN

Administrator

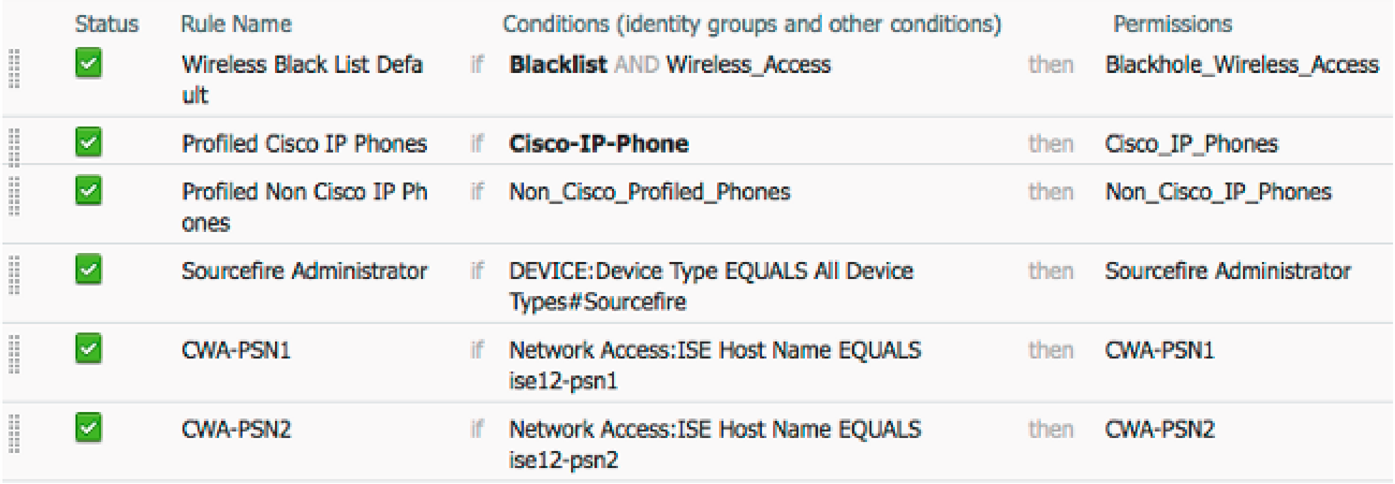
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

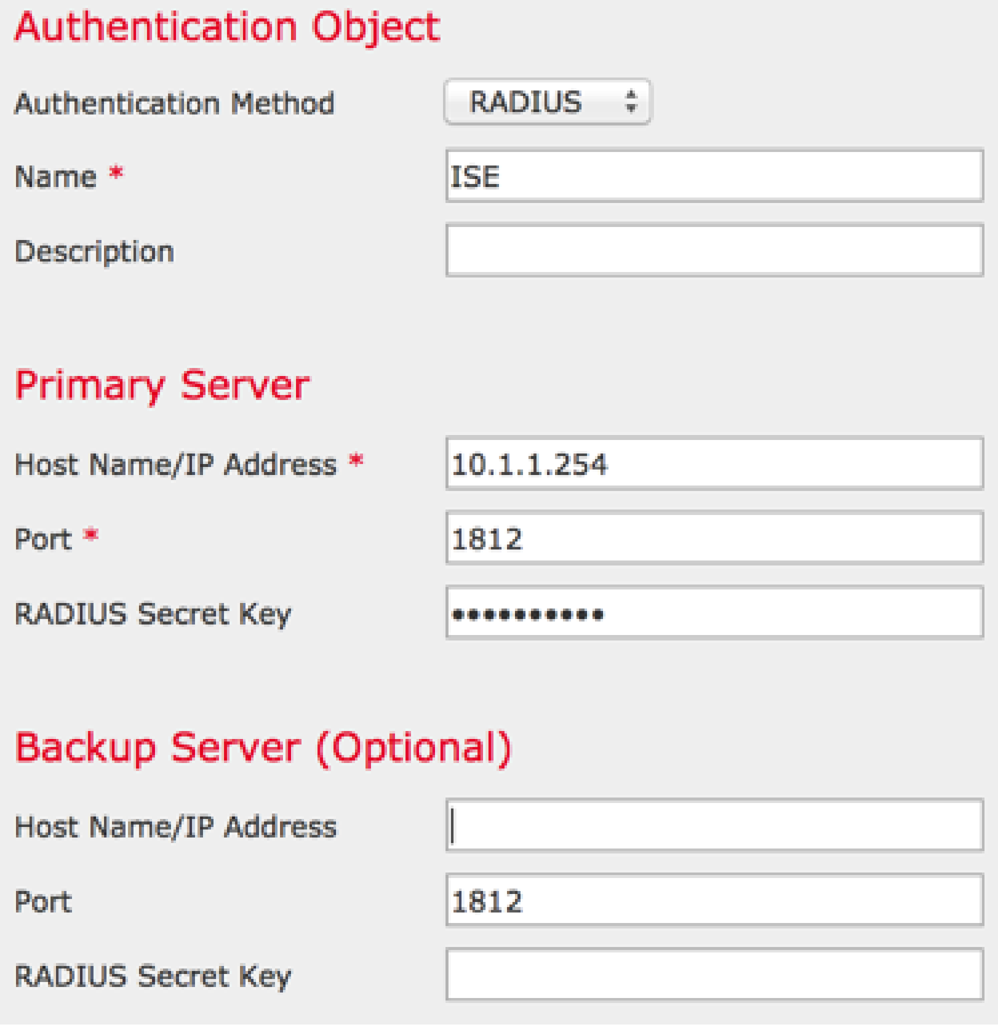
- Navigate to **Policy > Authorization** and configure a new authorization policy for the Sourcefire administration sessions. The example below uses the **DEVICE:Device Type** condition to match the device type configured in the **Configuring Network Devices and Network Device Groups** section above. This policy is then associated with the Sourcefire Administrator authorization profile configured above. Click **Save**.



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	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 System Policy Configuration

- Login to the FireSIGHT MC and navigate to **System > Local > User Management**. Click on the **Login Authentication** tab. Click the **+ Create Authentication Object** button to add a new RADIUS server for user authentication/authorization.
- Select **RADIUS** for the **Authentication Method**. Enter a descriptive name for the RADIUS server. Enter the **Host Name/IP Address** and **RADIUS Secret Key**. The secret key should match the key previously configured on ISE. Optionally enter a backup ISE server **Host Name/IP address** if one exists.



Authentication Object

Authentication Method	RADIUS
Name *	ISE
Description	

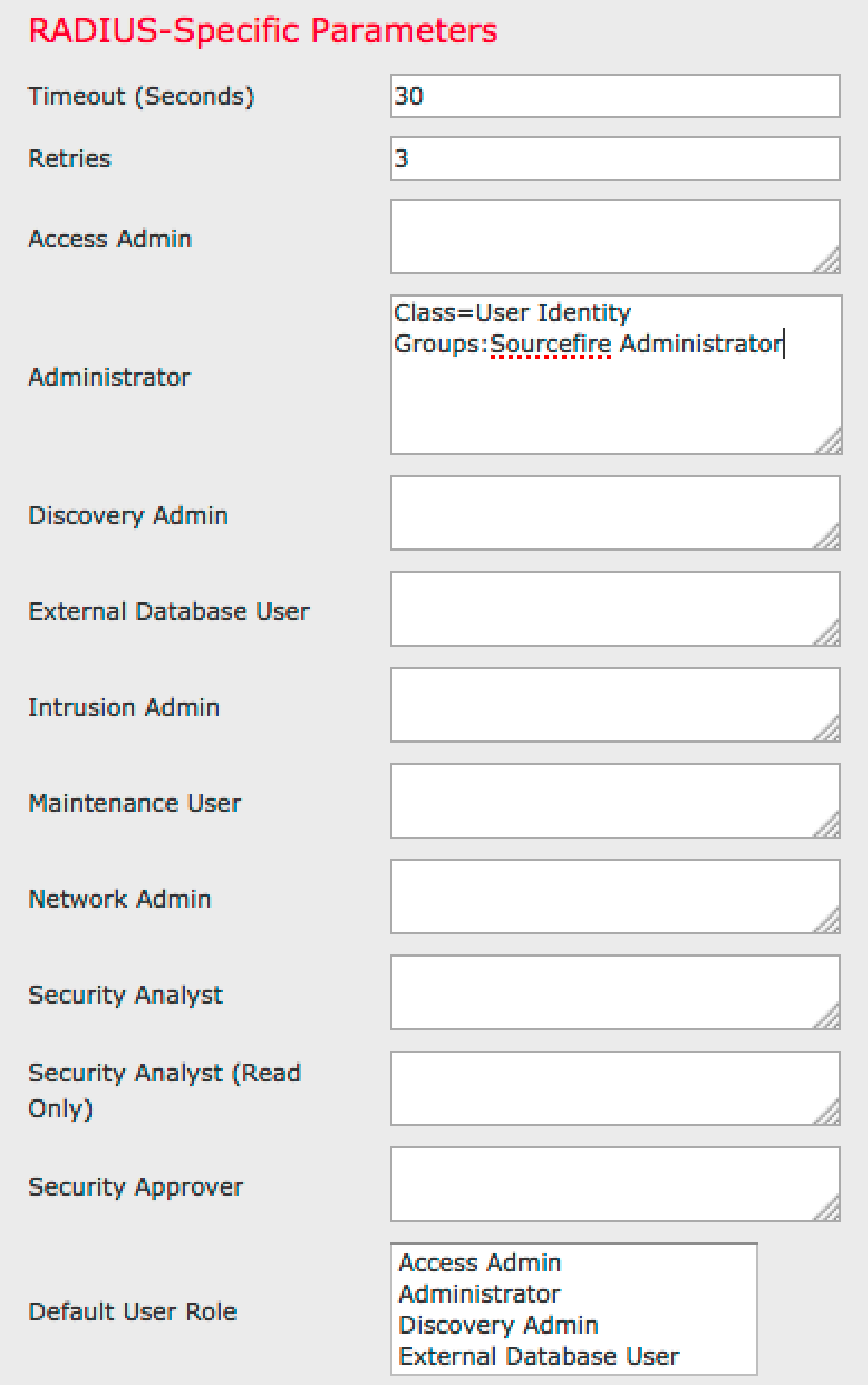
Primary Server

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	

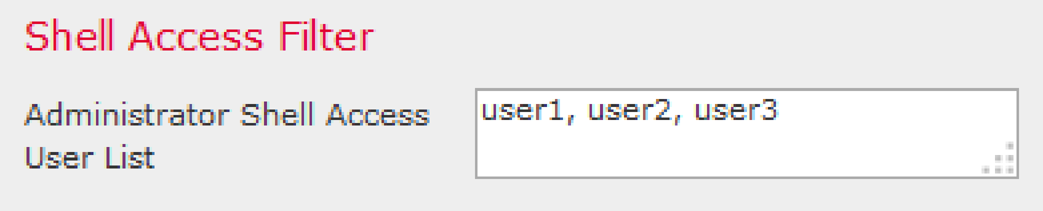
- Under the **RADIUS-Specific Parameters** section, enter the Class-25 av-pair string in the text box next to the Sourcefire local group name to be matched for GUI access. In this example, the Class=User Identity Groups:Sourcefire Administrator value is mapped to the Sourcefire Administrator group. This is the value that ISE returns as part of the ACCESS-ACCEPT. Optionally, select a **Default User Role** for authenticated users who do not have Class-25 groups assigned. Click **Save** to save the configuration or proceed to the Verify section below to test authentication with ISE.



RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=User Identity Groups:Sourcefire Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Default User Role	Access Admin Administrator Discovery Admin External Database User

- Under **Shell Access Filter**, enter a comma separated list of users to restrict shell/SSH sessions.



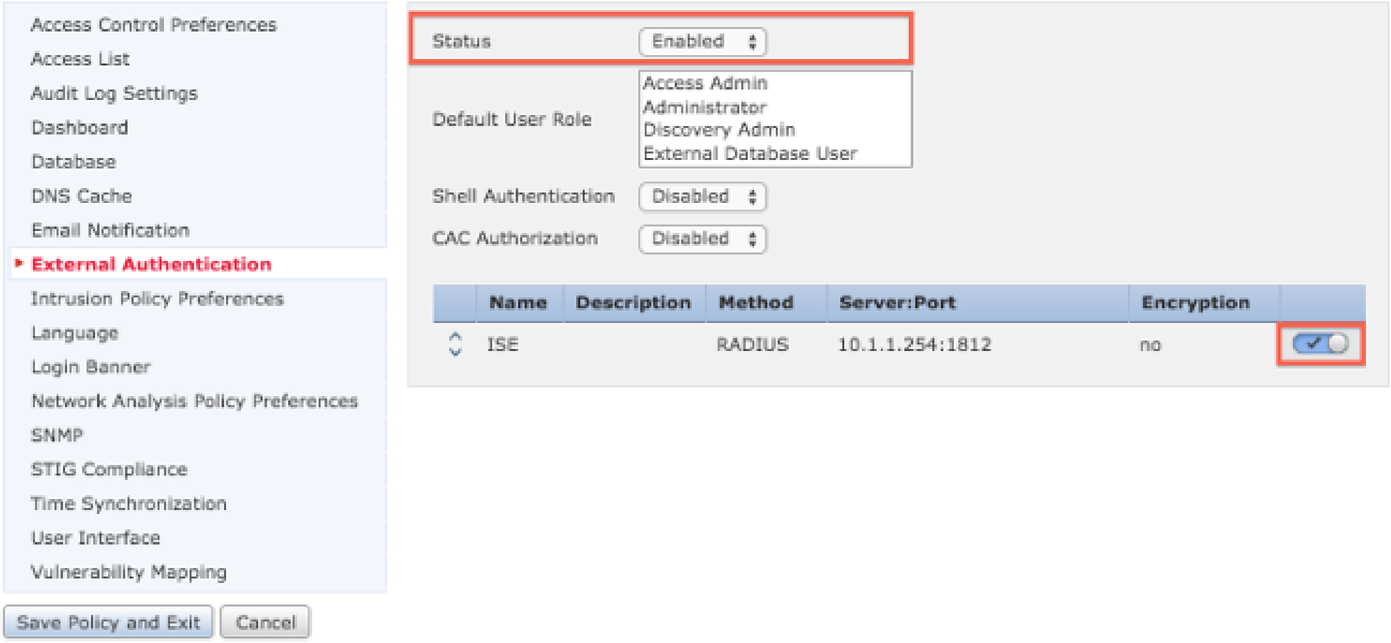
Shell Access Filter

Administrator Shell Access User List	user1, user2, user3

Enable External Authentication

Finally, complete these steps in order to enable external authentication on the FMC:

Navigate to **System** > **Local** > **System Policy**.Select **External Authentication** on the left panel.Change the *Status* to **Enabled** (disabled by default).Enable the added ISE RADIUS server.Save the policy and reapply the policy on the appliance.



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

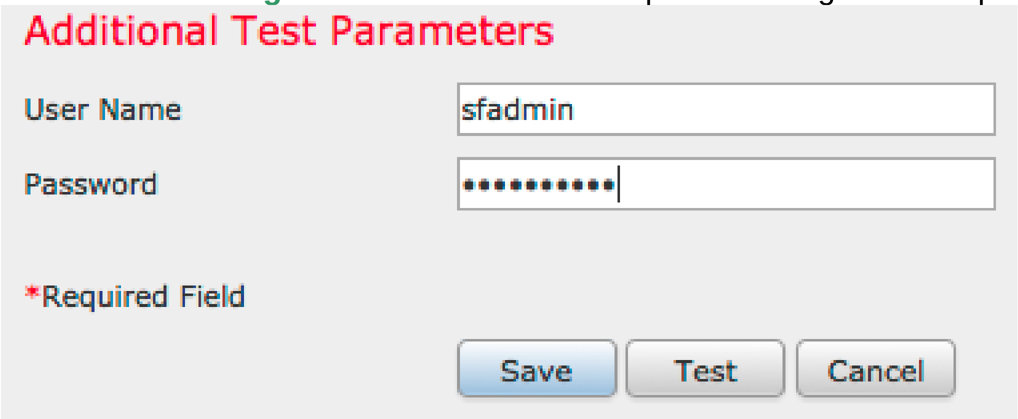
Save Policy and Exit | Cancel

Status	Enabled
Default User Role	Access Admin Administrator Discovery Admin External Database User
Shell Authentication	Disabled
CAC Authorization	Disabled

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

Verify

- To test user authentication against ISE, scroll down to the **Additional Test Parameters** section and enter a username and password for the ISE user. Click **Test.** A successfull test will result in a **green** Success: Test Complete message at the top of the browser window.

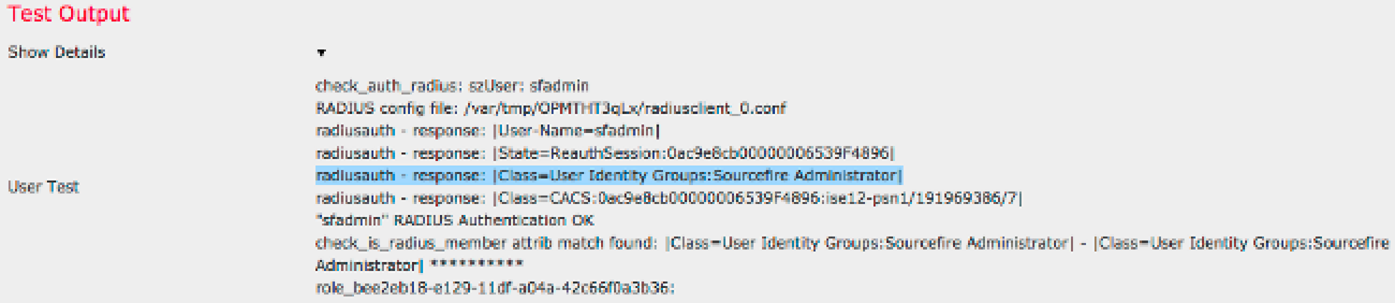


Additional Test Parameters

User Name	sfadmin
Password	••••••••••

*Required Field

- To view the results of the test authentication, go to the **Test Output** section and click the **black** arrow next to **Show Details**. In the example screenshot below, note the "radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|" value received from ISE. This should match the Class value associated with the local Sourcefire group configured on the FireSIGHT MC above. Click **Save**.



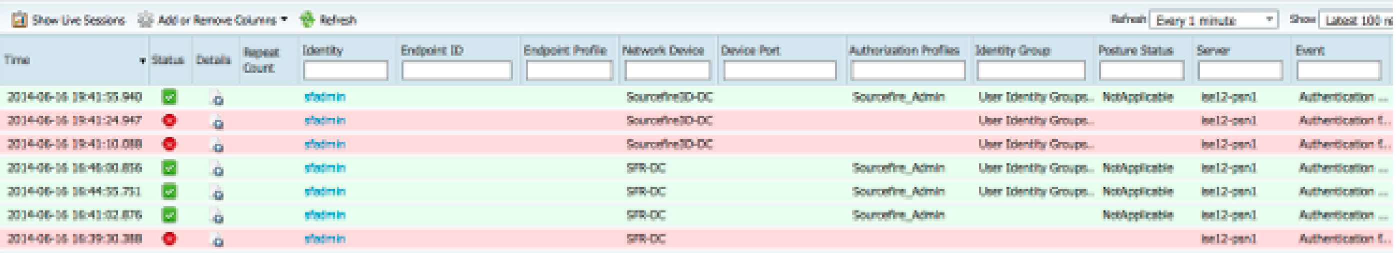
Test Output

Show Details ▾

User Test

```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTHT3qLx/radiusclient_0.conf
radiusauth - response: |User-Name=sfadmin|
radiusauth - response: |State=ReauthSession:0ac9e8cb00000006539F4896|
radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|
radiusauth - response: |Class=CACS:0ac9e8cb00000006539F4896: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:
```

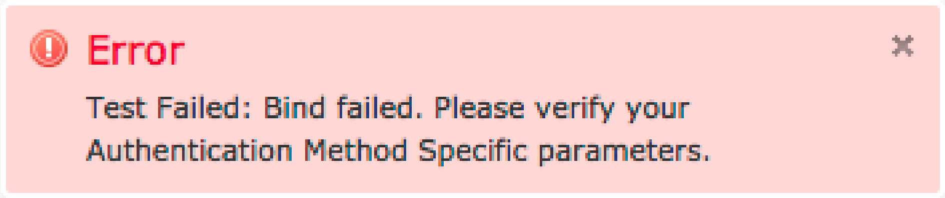
- From the ISE Admin GUI, navigate to **Operations > Authentications** to verify the success or failure of the user authentication test.



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 19:41:55.940	✓	🔍		sfadmin			SourcefireID-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 19:41:24.947	●	🔍		sfadmin			SourcefireID-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 19:41:10.088	●	🔍		sfadmin			SourcefireID-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 16:46:00.856	✓	🔍		sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 16:44:55.751	✓	🔍		sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 16:41:02.876	✓	🔍		sfadmin			SFR-DC		Sourcefire_Admin		NotApplicable	ise12-psn1	Authentication ...
2014-06-16 16:39:30.388	●	🔍		sfadmin			SFR-DC					ise12-psn1	Authentication f...

Troubleshoot

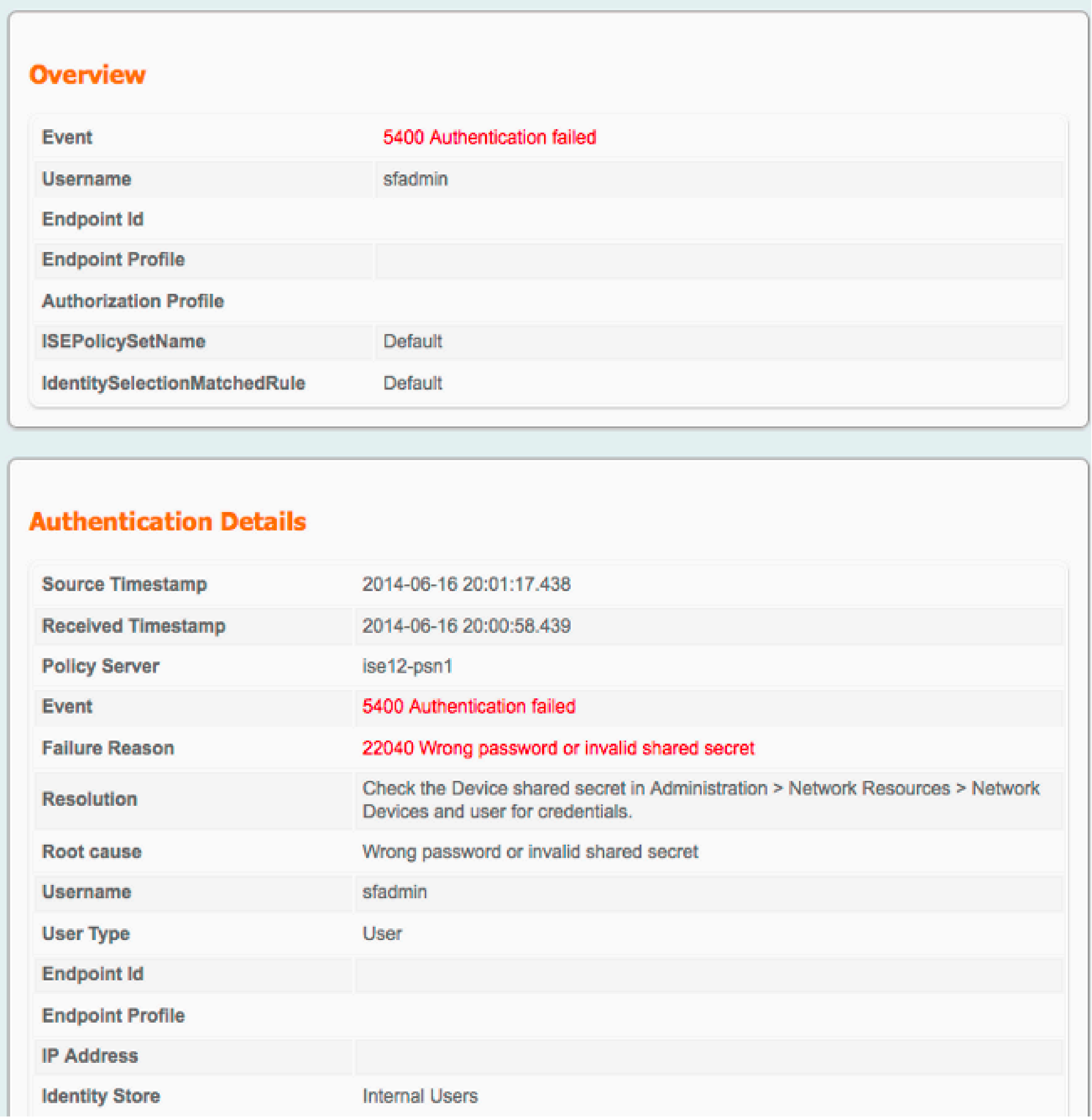
- When testing user authentication against ISE, the following error is indicative of a RADIUS Secret Key mismatch or an incorrect username/password.



Error

Test Failed: Bind failed. Please verify your Authentication Method Specific parameters.

- From the ISE admin GUI, navigate to **Operations > Authentications**. A **red** event is indicative of a failure while a **green** event is indicative of a successful authentication/authorization/Change of Authorization. Click on the 🔍 icon to review the details of the authentication event.



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

Related Information

Technical Support & Documentation - Cisco Systems