

# مدختم ةقداصل مل ISE عم FireSIGHT ماظن جم د RADIUS

## تاوت حمل

[ةمدقملا](#)

[ةيساسألا تابلطت مل](#)

[تابلطت مل](#)

[ةمدختم مل تانوك مل](#)

[نئوكتلا](#)

[ISE نئوكت](#)

[ةكبشلا ةزهجأ تاعومجم وةكبشلا ةزهجأ نئوكت](#)

[ISE: ةقداصل مةسايس نئوكت](#)

[ISE ىلا ىلجم مدختم مةفاضا](#)

[ISE لئوخت جهن نئوكت](#)

[Sourcefire ماظن جهن نئوكت](#)

[ةچراخلا ةقداصل مل نئوكت](#)

[ةحصلا نم ققحتلا](#)

[اهالصال وءاطخألا فاشكتسا](#)

[ةلص تاذا تاملعم](#)

## ةمدقملا

زاهجلا وءا (FMC) FireSIGHT ةرادا زكرم جم دل ةبولطملا نئوكتلا تاوطخ دنتم مل اذه فصى ب ل ط ةقداصل مل (ISE) Cisco نم ةيوهلا تامدخ كرحم مادختسا اب Cisco نم FirePOWER رادملا (RADIUS) مدختم مل ةقداصل مةفاضا دع ب نع ةقداصل مل.

## ةيساسألا تابلطت مل

### تابلطت مل

ةيلاللا عيضاوملاب ةفرعم كئيدل نوكت نأ اب Cisco ي صوت:

- (GUI) ةيموسرلا مدختم مل ةهجاو ربع رادملا زاهجل لئولألا نئوكتلا وءا FireSIGHT System ةقبط وءا
- ISE ىل عضي وفتلا وءا ةقداصل مل تاسايس نئوكت
- ةيساسألا RADIUS ةفرعم

### ةمدختم مل تانوك مل

ةيلاللا ةيداملا تانوك مل او جم اربلا تارادصلا ىلا دنتم مل اذه يف ةدراولا تامولعملا دنتم:

- Cisco ASA V9.2.1
- ASA FirePOWER v5.3.1 ةيطمنلا ةدحو

- ISE 1.2

ةصاخ ةي لم عم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراولما تامولعملما ءاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالا عيمج تادب رما يال لمحتحملما ريثاتلل كمهف نم دكاتف ، ةرشابم كتكشب

## نيوكتلا

### ISE نيوكت

عم لم اكلتال معدل ISE ضيوفتو ةقداصم تاسايس نيوكتل ةددعتم قرط كانه :حيملت نيوكت قرط يدحا وه يلاتلا لاثملا Sourcefire لثم (NAD) ةكبشلا يلا لوصولا ةزهجا تاجايتحإ مئالتل اهفييكت نكميو ةي عجرم ةطقن نيوكتل ةنيغ لكشتو . ةكراشملا دي دحت متيس . ني توطخ يلع ةي لم عم وه ضيوفتلا نيوكت نا ظحال . ددحملما رشنلا RADIUS ةمس ةمي ق جاوزا عاچاراب ISE ماي ق عم ISE يلع رثكا وا ةدحاو ضيوفت ةسايس توصللا جاوزا نييغت متي كلذ دعبو . رادملا زاهجالا وا FMC يلا (AV ةمي قلا جاوزا) ماظن جهن نيوكت ي ف اهفي رعت متي نيي لحم ني مدختسم ةعومجم يلا هذه ويدي فالوا FMC.

### ةكبشلا ةزهجا تاعومجمو ةكبشلا ةزهجا نيوكت

- ةكبشلا ةزهجا > ةكبشلا دراوم > ةراداللا يلا لقتنا ، ISE ةي موسرلا مدختسملا ةهجاو نم ي ف فصو مسا ريفوت . (NAD) ةكبشلا يلا دي دج لوصولا زاهج ةفاضلا ةفاضلا + قوف رقنا يلاتلا لاثملا ي ف FMC دي دحت متي . زاهجاللا IP ناو نعو


#### Network Devices

\* Name

Description

\* IP Address:  /

- رقنا . ةزهجالا عاونأ عيمج راوجب **يلاق تربلا مهسلا** قوف رقنا ، ةكبشلا ةزهجا ةعومجم تحت

يذلا ةشاشلا ةطقنلا لاثملا ي ف . ةدي دج ةكبش ةزهجا ةعومجم ءاشنإ ددحو زمرلا  يلع في رعت ي ف اذه زاهجالا عون يلا ةراشلا متتس . Device Type Sourcefire نيوكت مت ، يلي ظفح ةقطق . ةقحالا ةوطخ ي ف ليوختلا جهن ةدعاق



وَأ (MAB) MAC ةقداصم ةزاجم تسيل ةمدختسملا ةقيرطلا نوكت شيح NAD نم RADIUS تاباسح نع ةدعاقلا هذه شحتس، يضارتفا لكشب اهنيوكت مت امكو .802.1X ليدعت نكمي . ISE ل نييلحملال نييلخالل نييمدختسملا ةيوه ردصم يف نييمدختسملا ددحم وه امك خلل، LDAP و Active Directory لثم يجراخ ةيوه ردصم ىلإ ةراشلل نيوكتلا اذه اذه موقيس، طيسبتلا لجا نم . ةيجراخلا ةيوهلا رداصم > ةيوهلا ةرادا > ةرادلا تحت تاليدعت يارمألا بلطتي ال تحت ISE ىلع ايلحمل نييمدختسملا تاباسح ديدحتب لاثملا ةقداصملا ةسايس ىلع ىرخأ.

#### 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	

#### ISE ىل ايلحمل ممدختسم ةفاضلا

- مسال خدأ (Add) ةفاضلا قوف رقنا . نييمدختسم > تايوه > ةيوهلا ةرادا > ةرادا ىل لقتنا دوجوم ةعومجم مسال ددح، نييمدختسملا تاعومجم ديدحت تحت . ىنعم يوذ رورم ةملاك و ممدختسم نييعت متي، لاثملا اذه يف . ةديدج ةعومجم ةفاضلا **ءارضخ + ةمالع** قوف رقنا وأ طبرم تي س "Sourcefire Administrator" ةصصخمل ةعومجملا ىل "sfadmin" ممدختسملا جهن نيوكت هاندأ ةوطخلال يف ددحمل ليوختلا فيرعت فلمب هذه نييمدختسملا ةعومجم ظفحة ققط . ISE ليوخت

### 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 لي وخت جهن ني وكت

- صي صخت تافل م > لي وخت لال > جئاتن لال > سايس لال رصان ع > سايس لال لال لقتنا . دي دج لي وخت في رعت فلم ة فاضال **رضخأ + ة مالع** لعل رقتنا . لي وخت لال
- تحت لوصول اعون ل ACCESS\_ACCEPT دح . Sourcefire لوؤسم لثم يفصو مساري فوت قوف رقتنا . ASA VPN ل رواج لال ع برمل دحو لفسأل لال ريرمت لال مق ، ة كرت شم لال ماهم لال ط فح ة ققط . InternalUser:IdentityGroup دحو **ل لاق ت ر ب لال مه س لال**

رايخ مادختسا متي ، ISE لي لحو لال مدختسا لال ة يوه نزخم مدختسا لال اذنه نأل : جي ملت ة يوه نزخم مدختسا تنك اذا . ني وكت لال طي سبت ل InternalUser:IdentityGroup ة وعومج يتي لال ة مي ق لال ني وكت متي ، كلذ عمو ، مدختسا لال ASA VPN لي وخت ة مس نإف ، جي راج لوؤسم لال ة باتك ي دؤتس ، لال لال لبي س لعل . اي ودي Sourcefire زا ه لال اه اراجرا متي س Class-25 AV-pair ة لال نم ة مي ق ثو دح لال ASA VPN لال دس نمل ع برمل لال ي ف اي ودي لال ة مي ق لال هذه ني يع ك لذ دع ب نكم وي . Sourcefire زا ه لال لوؤسم لال لال س را = ة لال ني مدختسا لال ة بس نل لال . ماظن لال جهن ني وكت نم عزجك Sourcefire مدختسا لال ة وعومج ة لوبقم ني وكت لال ة قيرط نوكت نأ اما ، ني لال خاد لال

يٰلخاد مدختسم لاثم

\* 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

يٰجراخ مدختسم لاثم

### Advanced Attributes Settings

Select an item = [ ] - +

### Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

- Sourcefire. قرادإ تاسلج ل ةديج ضيوفت ةسايس نيوكت و ضيوفت > جهن ىلإ لقتنا. هن نيوكت مت يذلا زاهجلا عون ةقباطم ل Device:Device Type طرش يلاتلا لاثملا مدختسي جهنلا اذه نارقإ متي مث . هالعأ ةكبشلا زهجا تاعومجم و ةكبشلا زهجا نيوكت مسق يف ظفح ةقطق . هالعأ هن نيوكت مت يذلا Sourcefire لوؤسم ليوخت فيرعت فلمب

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 ماطن جهن نيوكت

- قرادإ > يلجم > ماطنلا ىلإ لقتنا و FireSIGHT MC مكحتلا ةدحو ىلإ لوخدلا ليچستب مق **ءاشنإ +** رزلا قوف رقنا . لوخدلا ليچست ةقداصم بيوبتلا ةمالع ىلع رقنا . مدختسملا . مدختسملا ضيوفت/ةقداصم ل ديچ RADIUS مداخل ةفاضال ةقداصم نئاك .
- مسا لخدأ . RADIUS مداخل ايفصو امسا لخدأ . ةقداصملا بولسأل RADIUS دح عم يرسل اجاتفملا قباطتي نأ بجي . يرسل RADIUS اجاتفم و IP ناوع/افيضملا ISE مداخل فيضم مسا لخدأ ، يرايخ ل لكشبو . ISE ىلع اقبس م هن نيوكت مت يذلا اجاتفملا ادوجوم ناك اذا IP ناوع/يطايتحال افسنلل .

## 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

- ص ن ل ا ع ب ر م ي ف ي 25 av-pair ة ل س ل س ل خ د ا ، RADIUS ب ة ص ا خ ل ا ت ا م ل ع م ل ا م س ق ت ح ت ة ه ج ا و ل ل ا ل و ص و ل ل ا ه ت ق ب ا ط م م ت ي س ي ت ل ل Sourcefire ة ل ح م ل ا ة و م ج م ل ا م س ا ل ر و ا ج م ل ا ي ت ل ا ة م ي ق ل ل ا ي ه ه ذ ه . Sourcefire ل و و س م ة و م ج م ل ا ع ل ع Groups:Sourcefire Administrator value ي ض ا ر ت ف ا م د خ ت س م ر و د د د ح ، ا ي ر ا ي ت خ ا . Access-ACCEPT ن م ع ز ج ك ا ه ع ا ج ر ا ب ISE م و و ي ق و ف ر ق ن ا . ة ن ي ع م 25 ة ل ل ا ت ا ع و م ج م م ه ي د ل س ي ل ن ي ذ ل ا م ه ي ل ع ق د ا ص م ل ا ن ي م د خ ت س م ل ل ISE ع م ق د ا ص م ل ا ر ا ب ت خ ا ل ه ا ن د ا ق ق ح ت ل ا م س ق ل ل ا ل ق ت ن ا و ا ن ي و ك ت ل ا ظ ف ح ل ظ ف ح



## 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"/>

- نېم دځت سملل ډلصافب ډلصفنم ډمئاق لځدا، Shell لى لى لوصولا ډي فست لماع تحت  
ل Shell/SSH لمع تاسلج ديقتل

## Shell Access Filter

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



## 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:
```

User Test

- > تاي لم عمل الى لقتنا، ايراد ايصاخال (GUI) ةي موسرلا مدختسمل اةجاو نم . ه.لش ف و ا مدختسمل اةقداصم رابتخا اچن نم ققحتلل ققداصملا

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 f...
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 18:46:00.856	✓		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					ise12-psn1	Authentication f...

## اهحالص او ااطخال فاشكتسا

- حاتفم قباطت مدع الى ايلاتلا ااطخال ريشي، لباقم مدختسمل اةقداصم رابتخا دنع ة.ححص ريغ رورم ةم لك/مدختسمل مسا و ا يرسلل RADIUS

### Error

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

- ةقداصملا > تاي لم عمل الى لقتنا، ايراد ايصاخال (GUI) ةي موسرلا مدختسمل اةجاو نم . اچن الى ارضخال ا شذل ريشي امن ي لشف ا و ا شذل ريشي

ا شذل لي صافات ةع ارم ل زمرلا ا الى رونا .ضي و وف تال ريشي غت/ضي و وف تال/ةقداصملا ةقداصملا

## 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

قلم تاذ تامولعم

[تادنتس مل او ينقتلا مع دلا - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت  
ملاعلاء انء مچ م ف ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و  
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا ا م ا د ا د و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن تسمل ا