

FMC- en FTD externe verificatie configureren met ISE als RADIUS-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Externe verificatie voor VCC](#)

[Externe verificatie voor FTD](#)

[Netwerktopologie](#)

[Configureren](#)

[ISE-configuratie](#)

[FMC-configuratie](#)

[FTD-configuratie](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft een voorbeeld van externe verificatieconfiguratie voor Secure Firewall Management Center en Firewall Threat Defence.

Voorwaarden

Vereisten

Aanbevolen wordt kennis van deze onderwerpen te hebben:

- Cisco Secure Firewall Management Center - eerste configuratie via GUI en/of shell.
- Verificatie- en autorisatiebeleid configureren op ISE.
- Basiskennis van RADIUS.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- vFMC 7.2.5
- vFTD 7.2.5.
- ISE 3.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer u externe verificatie inschakelt voor beheer- en beheergebruikers van uw Secure Firewall-systeem, controleert het apparaat de gebruikersreferenties met een Lichtgewicht Directory Access Protocol (LDAP) of RADIUS-server zoals opgegeven in een extern verificatieobject.

Externe verificatieobjecten kunnen worden gebruikt door de FMC- en FTD-apparaten. U kunt hetzelfde object tussen de verschillende apparaten-/apparaattypen delen of afzonderlijke objecten maken.

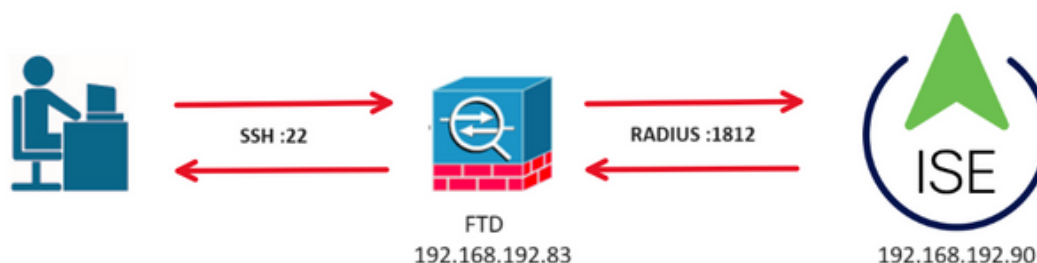
Externe verificatie voor VCC

U kunt meerdere externe verificatieobjecten configureren voor toegang tot de webinterface. Slechts één extern authenticatievoorwerp kan voor CLI of shell toegang worden gebruikt.

Externe verificatie voor FTD

Voor de FTD kunt u slechts één extern verificatieobject activeren.

Netwerktopologie



Configureren

ISE-configuratie



Opmerking: er zijn meerdere manieren om ISE-verificatie en -autorisatiebeleid voor Network Access Devices (NAD) zoals FMC in te stellen. Het voorbeeld dat in dit document wordt beschreven, is een referentiepunt waarin we twee profielen maken (een met beheerdersrechten en een ander alleen-lezen) en dat kan worden aangepast aan de basislijnen voor toegang tot uw netwerk. Op ISE kunnen een of meer machtigingsbeleidslijnen worden vastgesteld met terugkerende RADIUS-kenmerkwaarden aan het VCC die vervolgens worden toegewezen aan een lokale gebruikersgroep die in de beleidsconfiguratie van het VCC-systeem is gedefinieerd.

Stap 1. Voeg een nieuw netwerkapparaat toe. Navigeer naar het hamburgerpictogram linksboven >Beheer > Netwerkbronnen > Netwerkapparaten > +Add.



The screenshot shows the Cisco ISE Administration interface for Network Resources. The main navigation bar includes 'Administration - Network Resources' and search, help, and settings icons. Below the navigation bar, there are tabs for 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'More'. The 'Network Devices' tab is active. On the left, there is a sidebar with 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and shows a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. Above the table, there are action buttons: Edit, Add (highlighted with a red box), Duplicate, Import, Export, Generate PAC, and Delete. The table is currently empty, with 'Selected 0 Total 2' and a refresh icon.

Stap 2. Wijs een naam toe aan het object van het netwerkapparaat en voer het FMC IP-adres in.

Controleer het aanvinkvakje RADIUS en stel een gedeeld geheim in.

Dezelfde toets moet later worden gebruikt om het VCC te configureren.

Klik op Opslaan als u klaar bent.

The screenshot shows the configuration form for a Network Device in Cisco ISE. The main navigation bar is the same as in the previous screenshot. The 'Network Devices' tab is active. The left sidebar is the same. The main content area is titled 'Network Devices List > FMC' and 'Network Devices'. The form fields are: Name (FMC), Description, IP Address (192.168.192.60 / 32), Device Profile (Cisco), Model Name (vFMC), Software Version (7.2.5), Network Device Group, Location (All Locations), IPSEC (No), and Device Type (All Device Types). Below these fields, the 'RADIUS Authentication Settings' section is expanded, and the 'RADIUS' checkbox is highlighted with a red box. The 'RADIUS UDP Settings' section shows Protocol (RADIUS), Shared Secret (masked with dots), and a 'Show' button. There is also a checkbox for 'Use Second Shared Secret' and a 'Second Shared Secret' field with a 'Show' button.

Stap 2.1. Herhaal hetzelfde om de FTD toe te voegen.

Wijs een naam toe aan het object van het netwerkapparaat en voer het FTD IP-adres in.

Controleer het aanvinkvakje RADIUS en stel een gedeeld geheim in.

Klik op Opslaan als u klaar bent.

The screenshot shows the configuration page for a Network Device named 'FTD'. The IP Address is 192.168.192.83/32. The Device Profile is Cisco, Model Name is vFTD, and Software Version is 7.2.5. The RADIUS Authentication Settings section is expanded, showing the RADIUS UDP Settings with Protocol set to RADIUS and a Shared Secret field. The Shared Secret field is currently empty and has a 'Show' button next to it. There is also an option to 'Use Second Shared Secret' which is currently unchecked.

Stap 2.3. Controleer of beide apparaten worden weergegeven onder Netwerkkaparameters.

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

Stap 3. Maak de gewenste gebruikers-identiteitsgroepen. Navigeer naar het hamburgerpictogram linksboven >Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > + Toevoegen

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - Identity Management'. Below the navigation bar, there are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' tab is active. On the left, there is a sidebar for 'Identity Groups' with a search bar and a tree view showing 'Endpoint Identity Groups' and 'User Identity Groups'. The main area is titled 'User Identity Groups' and shows a table with columns 'Name' and 'Description'. Above the table, there are action buttons: 'Edit', '+ Add' (highlighted with a red box), 'Delete', 'Import', and 'Export'. The table currently shows no data, with 'Selected 0' and 'Total 11' indicated.

Stap 4. Geef elke groep een naam en sla afzonderlijk op. In dit voorbeeld maken we een groep voor beheerders en een groep voor alleen-lezen gebruikers. Maak eerst de groep voor de gebruiker met beheerdersrechten.

The screenshot shows the configuration page for an 'Identity Group'. The breadcrumb trail is 'User Identity Groups > FMC and FTD admins'. The page title is 'Identity Group'. There are two main fields: '* Name' with the value 'FMC and FTD admins' and 'Description' with the value 'FMC and FTD admins ISE local.'. At the bottom, there are two buttons: 'Save' (highlighted with a red box) and 'Reset'.

Stap 4.1. Maak de tweede groep voor de ReadOnly gebruiker.

The screenshot shows the configuration page for an 'Identity Group'. The breadcrumb trail is 'User Identity Groups > FMC and FTD ReadOnly'. The page title is 'Identity Group'. There are two main fields: '* Name' with the value 'FMC and FTD ReadOnly' and 'Description' with the value 'FMC and FTD ReadOnly.'. At the bottom, there are two buttons: 'Save' (highlighted with a red box) and 'Reset'.

Stap 4.2. Bevestig beide groepen onder de lijst Gebruikersidentiteitsgroepen. Gebruik het filter om deze gemakkelijk te vinden.

Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

- Endpoint Identity Groups
- User Identity Groups

User Identity Groups

Selected 0 Total 2

Edit + Add Delete Import Export Quick Filter

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

Stap 5. Maak lokale gebruikers en voeg ze toe aan hun correspondentengroep. Ga naar >Beheer > Identiteitsbeheer > Identiteiten > + Toevoegen.

Cisco ISE Administration · Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 0

Edit + Add Change Status Import Export Delete

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Adm
No data available							

Stap 5.1. Maak eerst de gebruiker met beheerdersrechten. Geef het een naam, wachtwoord en de FMC- en FTD-beheerders van de groep.

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_admin

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

	Password	Re-Enter Password	
* Login Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Users

Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD admins ▾ ⓘ +

Stap 5.2. Voeg de gebruiker met ReadOnly rechten toe. Wijs een naam, wachtwoord en de groep FMC en FTD ReadOnly toe.

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_readuser

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

Users
Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

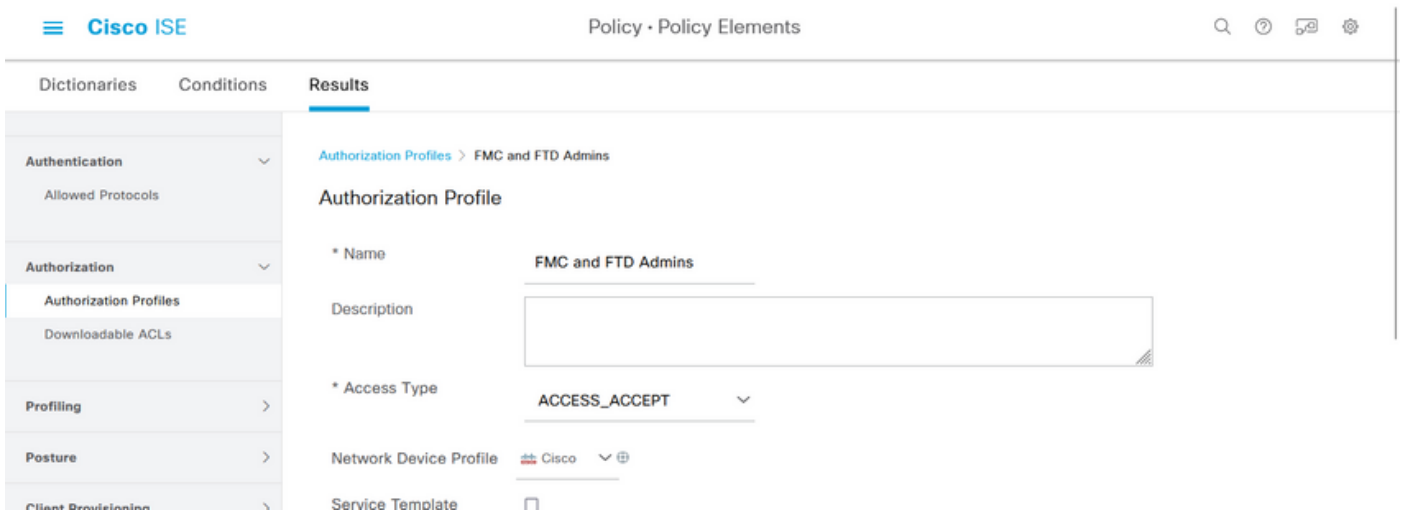
Stap 6. Maak het autorisatieprofiel aan voor de beheerder.

Navigeer naar



> Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen > +Add.

Definieer een naam voor het autorisatieprofiel, laat het toegangstype als ACCESS_ACCEPTEREN en voeg onder Geavanceerde Attributen-instellingen een straal > Klasse toe—[25] met de waarde Administrator en klik op Indienen.



Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

Stap 7. Herhaal de vorige stap om het autorisatieprofiel voor de alleen-lezen gebruiker te maken. Maak nu de Radius Class met de waarde ReadUser in plaats van Administrator.

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name FMC and FTD ReadUser

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Navigation: Dictionaries | Conditions | **Results**

Left sidebar menu:

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

Main content area:

Advanced Attributes Settings

⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Buttons: **Submit** (highlighted with a red box) | Cancel

Stap 8. Maak een beleidsset die overeenkomt met het IP-adres van het VCC. Dit om te voorkomen dat andere apparaten toegang verlenen aan de gebruikers.



Navigeer naar

> Beleidssets > pictogram aan de linkerbovenhoek >



Policy Sets

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
--------	-----------------	-------------	------------	-------------------------------------	------	---------	------

Search

	Default	Default policy set		Default Network Access	45		
--	---------	--------------------	--	------------------------	----	--	--

Reset

Save

Stap 8.1. Een nieuwe regel wordt bovenaan uw Policy Sets geplaatst.

Noem het nieuwe beleid en voeg een topvoorwaarde voor RADIUS NAS-IP-Adres-attribuut dat overeenkomt met het FMC IP-adres.

Voeg een tweede voorwaarde met OR combinatie toe om het IP-adres van de FTD op te nemen.

Klik op Gebruik om de wijzigingen te bewaren en de editor te verlaten.

Conditions Studio

Library

Search by Name

5G

Catalyst_Switch_Local_Web_Authentication

Source FMC

Switch_Local_Web_Authentication

Switch_Web_Authentication

Wired_802.1X

Wired_MAB

Wireless_802.1X

Wireless_Access

Editor

Radius-NAS-IP-Address

Equals 192.168.192.60

OR

Radius-NAS-IP-Address

Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

Stap 8.2. Klik op Opslaan als het proces is voltooid.

Cisco ISE

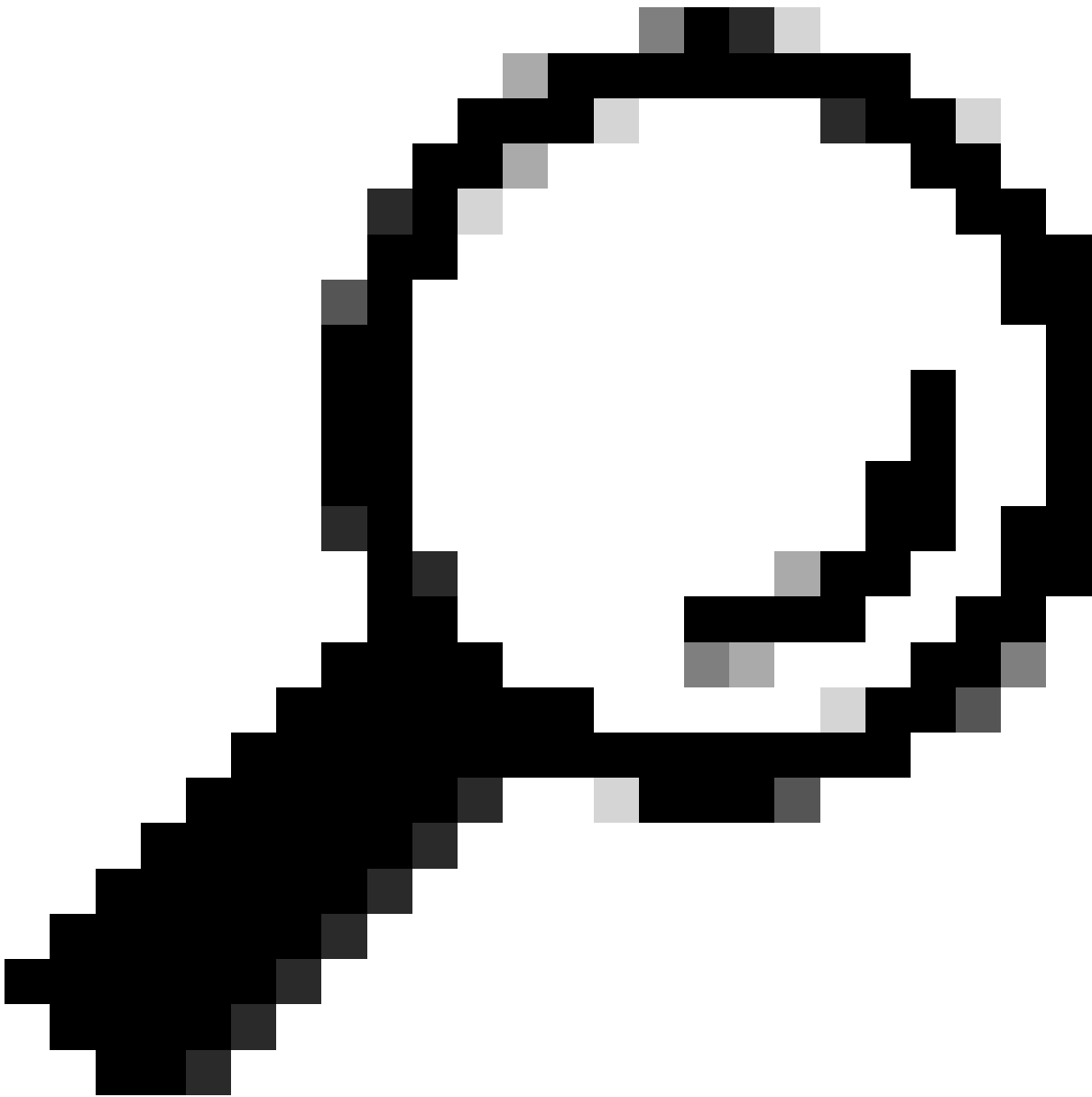
Policy > Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

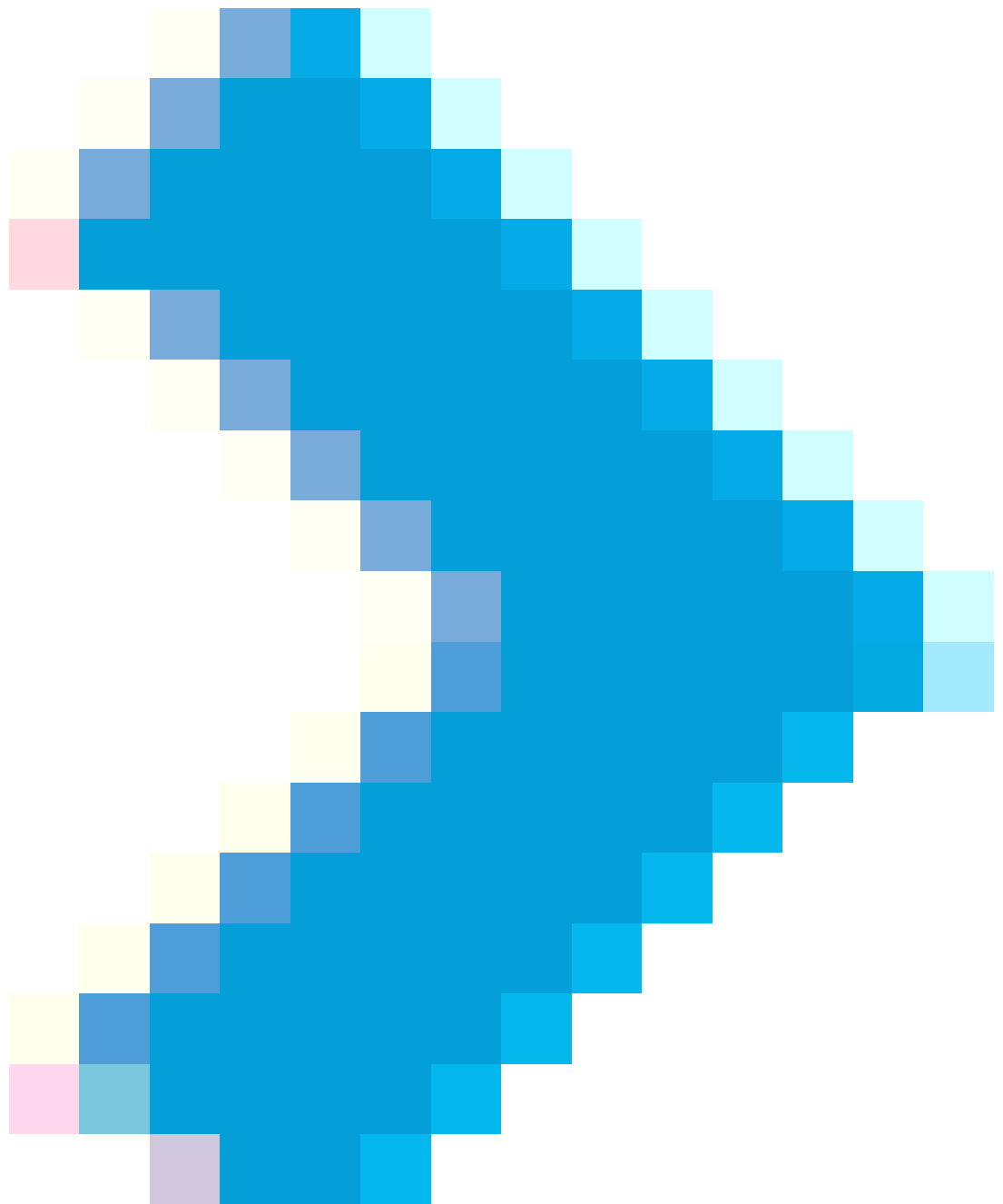
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save



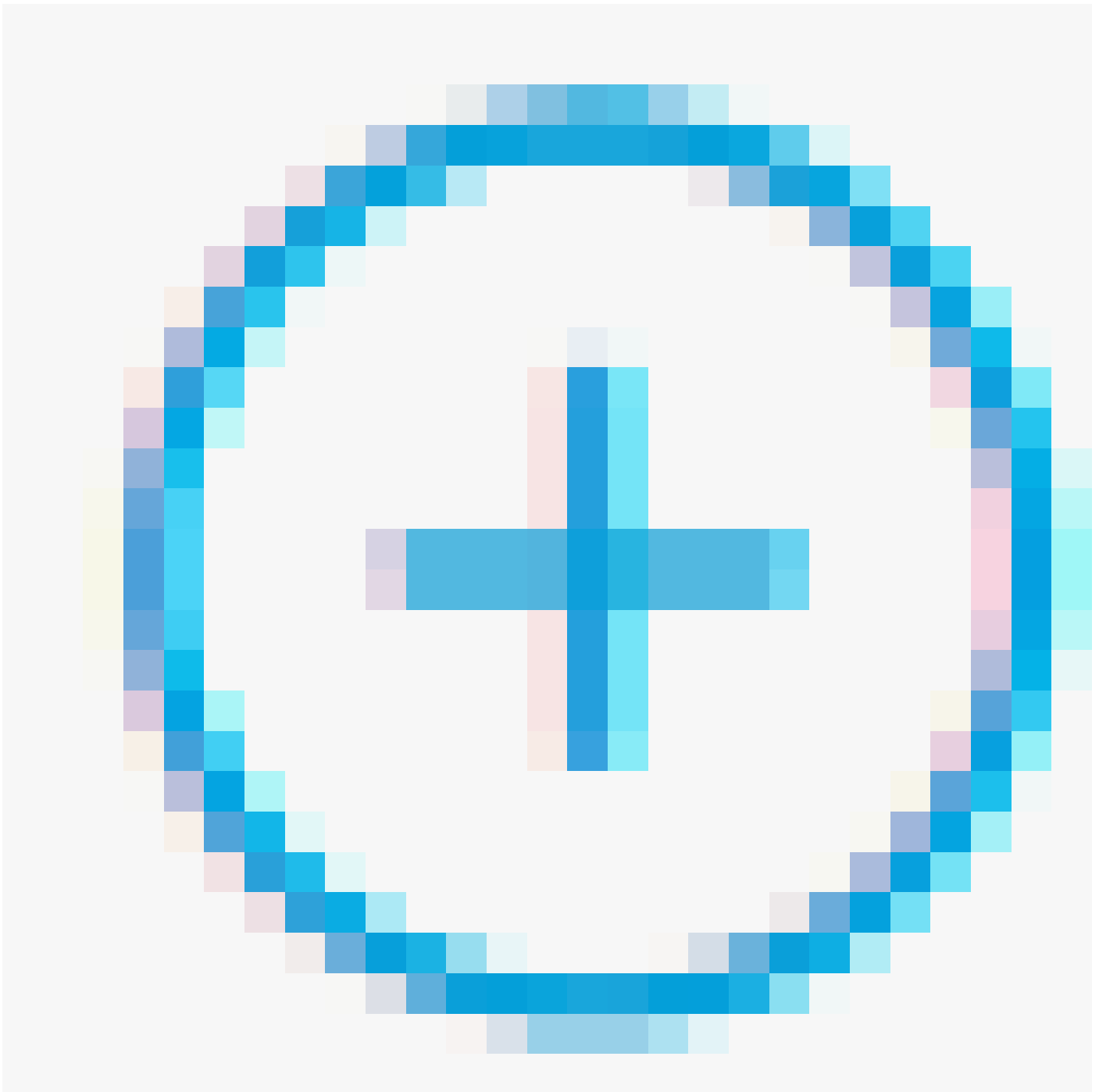
Tip: voor deze oefening hebben we de lijst Default Network Access Protocols toegestaan. U kunt een nieuwe lijst maken en deze indien nodig beperken.

Stap 9. Bekijk de nieuwe Policy Set door op het



pictogram aan het einde van de rij te drukken.

Breid het menu Autorisatiebeleid uit en druk op het



pictogram om een nieuwe regel toe te voegen om de toegang tot de gebruiker met beheerdersrechten toe te staan.

Geef het een naam.

Stel de voorwaarden in om de Dictionary Identity Group met Attribute Name gelijk te stellen aan User Identity Groups: FMC- en FTD-beheerders (de groepsnaam die in Stap 4 is gemaakt) en klik op Use.

Geef het een naam.

Stel de voorwaarden in om de Dictionary Identity Group af te stemmen op de naam van het kenmerk Gelijk aan gebruikersgroepen: FMC en FTD ReadOnly (de groepsnaam die in stap 4 is gemaakt) en klik op Use.

Conditions Studio

Conditions Studio interface showing the configuration of a condition. The condition is set to 'IdentityGroup-Name' equals 'User Identity Groups:FMC and FTD ReadOnly'. The 'Use' button is highlighted.

Stap 11. Stel de autorisatieprofielen voor elke regel in en druk op Opslaan.

Policy Sets configuration page showing the 'FMC and FTD Access' policy set. The table below shows the configuration for the 'Authorization Policy (3)' section, including the 'FMC and FTD read user access' rule.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	FMC and FTD Access	Management Access	OR • Radius-NAS-IP-Address EQUALS 192.168.192.60 • Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	FMC and FTD read user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly	FMC and FTD ReadUser	Select from list	0	⚙️
✓	FMC and FTD admin user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins	FMC and FTD Admins	Select from list	0	⚙️
✓	Default		DenyAccess	Select from list	0	⚙️

FMC-configuratie

Stap 1. Maak het externe verificatie object onder System > Gebruikers > Externe verificatie > + Add Externe verificatie object.

Stap 2. Selecteer RADIUS als verificatiemethode.

Geef onder Externe verificatie object een naam aan het nieuwe object.

Plaats vervolgens in de instelling Primary Server het ISE-IP-adres en dezelfde RADIUS Secret Key die u in stap 2 van uw ISE-configuratie hebt gebruikt.

Stap 3. Plaats de waarden van de RADIUS-klasse die zijn geconfigureerd in stap 6 en 7 van ISE Configuration: Administrator en ReadUser voor respectievelijk firewall_admin en firewall_readuser.

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

To specify the default user role if user is not found in any group



Opmerking: Het tijdsbereik is anders voor de FTD en de FMC. Als u dus een object deelt en de standaardwaarde van 30 seconden wijzigt, moet u ervoor zorgen dat u het kleinere tijdsbereik (1-300 seconden) voor FTD-apparaten niet overschrijdt. Als u de timeout op een hogere waarde instelt, werkt de Threat Defense RADIUS configuratie niet.

Stap 4. Bevolk de beheerder CLI Access User List onder CLI Access Filter met de gebruikersnamen die CLI-toegang kunnen verkrijgen.

Klik op Opslaan als u klaar bent.

CLI Access Filter

(For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

Stap 5. Schakel het nieuwe object in. Stel dit in als de Shell-verificatiemethode voor FMC en klik op Opslaan en Toepassen.

Firewall Management Center
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ? admin | Cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE_Radius) + Add External Authentication Object

Name	Method	Enabled	
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>	

FTD-configuratie

Stap 1. In FMC GUI navigeer je naar Apparaten > Platform-instellingen. Bewerk uw huidige beleid of maak een nieuwe als u geen toegewezen aan het FTD hebt u toegang tot nodig hebt. Schakel de RADIUS-server in onder Externe verificatie en klik op Opslaan.

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 🟢 ⚙️ ? admin | Cisco SECURE

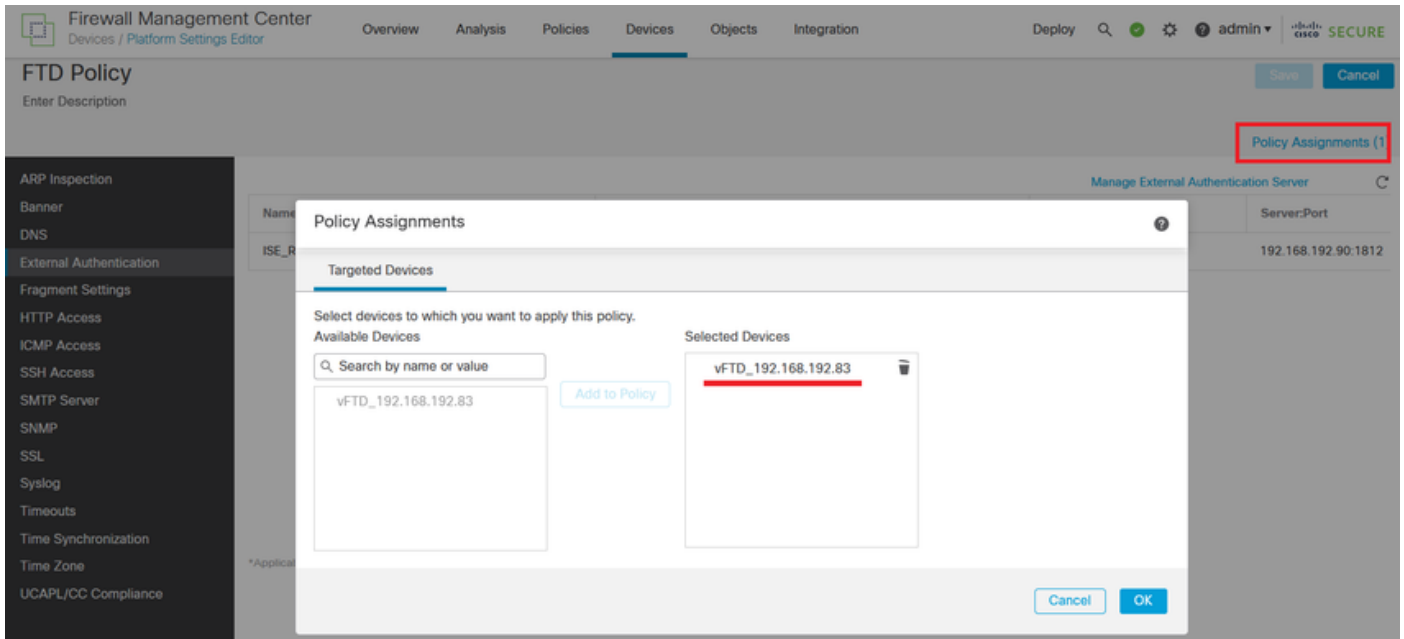
FTD Policy Enter Description You have unsaved changes

Policy Assignments (1)

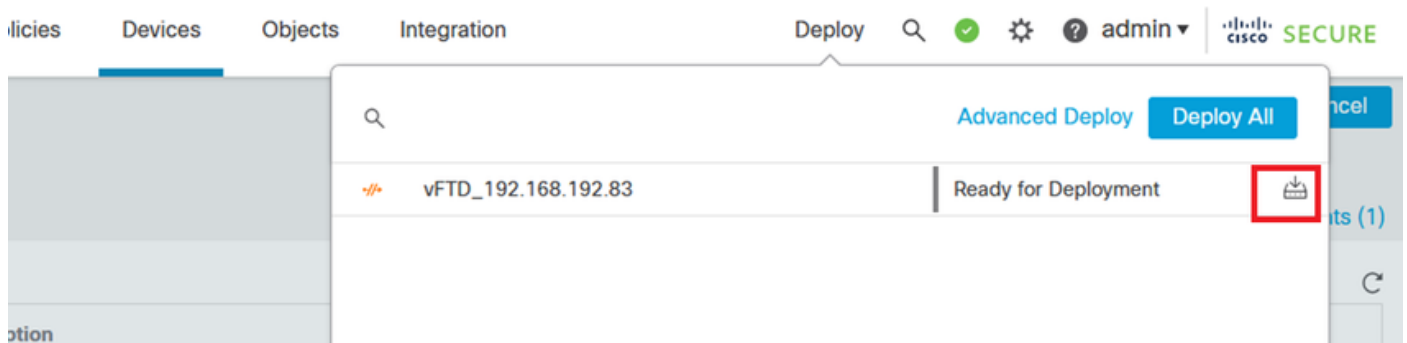
Manage External Authentication Server

Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

Stap 2. Zorg ervoor dat de FTD die u moet bereiken, wordt vermeld onder Beleidstoe wijzingen als geselecteerd apparaat.

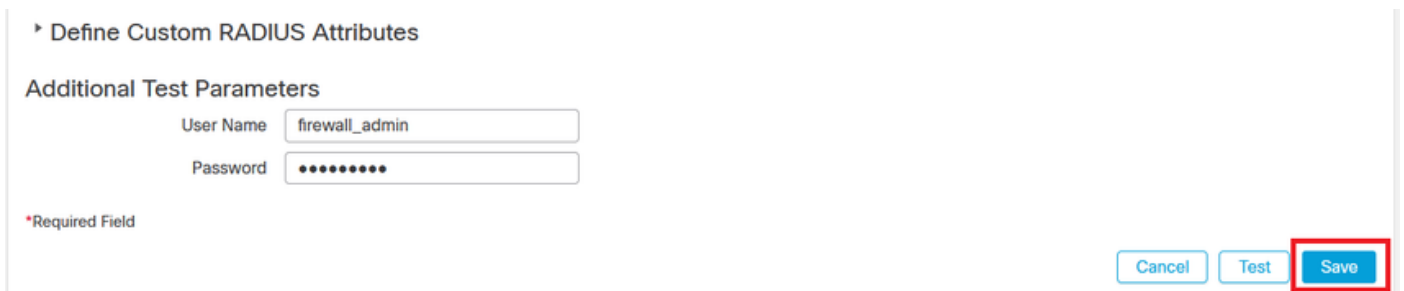


Stap 3. Voer de wijzigingen in.



Verifiëren

- Test of uw nieuwe implementatie goed werkt.
- Navigeer in de FMC GUI naar de RADIUS-serverinstellingen en blader naar beneden naar de sectie Aanvullende testparameters.
- Voer een gebruikersnaam en wachtwoord in voor de ISE-gebruiker en klik op Test.



- Een succesvolle test toont een groen Success Test Compleet bericht boven in het browservenster.



Success
Test Complete.

External Authentication Object

Authentication Method

Name *

- U kunt de Details onder de Test-uitgang uitvouwen voor meer informatie.

Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.