

Configurazione dell'autenticazione esterna di FMC in ambienti multidominio

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione di ISE](#)

[Aggiungi dispositivi di rete](#)

[Creare i gruppi di identità e gli utenti locali](#)

[Creare i profili di autorizzazione](#)

[Aggiungi nuovo set di criteri](#)

[Configurazione FMC](#)

[Aggiunta del server ISE RADIUS per l'autenticazione FMC](#)

[Verifica](#)

[Test di accesso tra domini](#)

[Test interni FMC](#)

[log ISE in tempo reale](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta l'implementazione della multitenancy (multidominio) nell'FMC Cisco e viene usata la tecnologia Cisco ISE per l'autenticazione RADIUS centralizzata.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione iniziale di Cisco Secure Firewall Management Center tramite GUI e/o shell.
- Privilegi di amministratore completi nel dominio globale della console centrale di gestione del sistema per creare sottodomini e oggetti di autenticazione esterna.
- Configurazione dei criteri di autenticazione e autorizzazione su ISE.
- Conoscenze base di RADIUS

Componenti usati

- Cisco Secure FMC: vFMC 7.4.2 (o versione successiva consigliata per la stabilità multidominio)
- Struttura dominio: Una gerarchia a tre livelli (Globale > Sottodomini di secondo livello).
- Cisco Identity Services Engine: ISE 3.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Negli ambienti aziendali su larga scala o negli scenari MSSP (Managed Security Service Provider), è spesso necessario segmentare la gestione della rete in confini amministrativi distinti. In questo documento viene descritto come configurare FMC per il supporto di più domini, in particolare per un esempio reale in cui un provider di servizi condivisi gestisce due client: Retail-A e Finance-B. Utilizzando l'autenticazione RADIUS esterna tramite Cisco ISE, gli amministratori possono garantire che gli utenti ricevano automaticamente la concessione dell'accesso solo ai rispettivi domini in base alle credenziali centralizzate.

Il sistema Cisco Secure Firewall utilizza i domini per implementare la multitenancy.

- Gerarchia dominio: La gerarchia inizia dal dominio globale. È possibile creare fino a 100 sottodomini in una struttura a due o tre livelli.
- Domini foglia: Si tratta di domini nella parte inferiore della gerarchia senza ulteriori sottodomini. È fondamentale che ciascun dispositivo FTD gestito sia associato esattamente a un dominio foglia.
- Attributo classe RADIUS (attributo 25): In un'installazione multidominio, il FMC utilizza l'attributo RADIUS Class restituito da ISE per mappare un utente autenticato a un dominio e a un ruolo utente specifici. Questo consente a un singolo server RADIUS di assegnare dinamicamente gli utenti a diversi segmenti di utenti (ad esempio, Retail-A e Finance-B) al momento dell'accesso.

Configurazione

Configurazione di ISE

Aggiungi dispositivi di rete

Passaggio 1. Passare a Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi.

The screenshot shows the 'Network Devices' section of the Cisco Identity Services Engine. The top navigation bar includes 'Administration / Network Resources'. The left sidebar has 'Administration' selected. The main area displays a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. A toolbar at the top provides options like Edit, Add, Duplicate, Import, Export, Generate PAC, Delete, and a search/filter section.

Passaggio 2. Assegnare un nome all'oggetto dispositivo di rete e inserire l'indirizzo IP del CCP.

Selezionare la casella di controllo RADIUS e definire un segreto condiviso. La stessa chiave deve essere utilizzata successivamente per configurare il CCP. Al termine, fare clic su Salva.

This screenshot shows the configuration details for a specific network device. The device name is set to 'fmc_10.225.86.50'. Under the 'Network Device Group' section, the 'Location' is set to 'All Locations'. In the 'RADIUS Authentication Settings' section, the 'Protocol' is set to 'RADIUS' and the 'Shared Secret' field contains a shared secret key. Other fields include 'Model Name', 'Software Version', and 'Device Type'.

Creare i gruppi di identità e gli utenti locali

Passaggio 3. Creare i gruppi di identità utente richiesti. Passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > Aggiungi.

The screenshot shows the 'Groups' section of the Cisco Identity Services Engine. The 'User Identity Groups' sub-section is displayed. The top navigation bar includes 'Administration / Identity Management'. The left sidebar has 'Administration' selected. The main area shows a table with columns: Name and Description. A toolbar at the top provides options like Edit, Add, Delete, Import, Export, and a search/filter section.

Passaggio 4. Assegnare un nome a ogni gruppo e salvare singolarmente. In questo esempio viene creato un gruppo per gli utenti Administrator. Creare due gruppi: Group_Retail_A e Group_Finance_B.

The screenshot shows the 'Groups' tab selected in the navigation bar. Under 'Identity Groups', a new group is being created. The 'Name' field contains 'Group_Retail_A' and the 'Description' field contains 'Cisco FMC Domain Retail-A'. The 'Save' button is visible at the bottom right.

The screenshot shows the 'Groups' tab selected in the navigation bar. Under 'Identity Groups', a new group is being created. The 'Name' field contains 'Group_Finance_B' and the 'Description' field contains 'Cisco FMC Domain Finance-B'. The 'Save' button is visible at the bottom right.

Passaggio 5. Creare gli utenti locali e aggiungerli al gruppo corrispondente. Passare a Amministrazione > Gestione delle identità > Identità > Aggiungi.

The screenshot shows the 'Identities' tab selected in the navigation bar. The main area displays the 'Network Access Users' list. The '+ Add' button, located in the top left of the user table, is highlighted with a red box. The table headers include Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin.

Passaggio 5.1. Creare innanzitutto l'utente con diritti di amministratore. Assegnare un nome al gruppo admin_retail, la password e il gruppo Group_Retail_A.

Identity Services Engine Administration / Identity Management

Identities

Bookmarks	Groups	External Identity Sources	Identity Source Sequences	Settings
-----------	--------	---------------------------	---------------------------	----------

* Username: admin_retail

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:
 With Expiration
 Never Expires

Password: Login Password: Re-Enter Password:

Enable Password:

User Information

Account Options

Account Disable Policy

User Groups

Group_Retail_A

Passaggio 5.2. Creare innanzitutto l'utente con diritti di amministratore. Assegnare un nome a admin_finance, la password e il gruppo Group_Finance_B.

Identity Services Engine Administration / Identity Management

Identities

Bookmarks	Groups	External Identity Sources	Identity Source Sequences	Settings
-----------	--------	---------------------------	---------------------------	----------

* Username: admin_finance

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:
 With Expiration
 Never Expires

Password: Login Password: Re-Enter Password:

Enable Password:

User Information

Account Options

Account Disable Policy

User Groups

Group_Finance_B

Creare i profili di autorizzazione

Passaggio 6. Creare il profilo di autorizzazione per l'utente Amministratore interfaccia Web di FMC. Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili autorizzazione > Aggiungi.

The screenshot shows the Cisco Identity Services Engine interface. In the top navigation bar, 'Identity Services Engine' and 'Policy / Policy Elements' are visible. On the left sidebar, under the 'Policy' section, there are links for Bookmarks, Dashboard, Context Visibility, Operations, Interactive Help, and Work Centers. The main content area is titled 'Standard Authorization Profiles'. It displays a table with columns 'Name' and 'Profile'. At the top of the table, there are buttons for 'Edit', '+ Add' (which is highlighted with a red box), 'Duplicate', and 'Delete'. A search bar at the bottom right shows 'Selected 0 Total 26'.

Assegnare un nome al profilo di autorizzazione e lasciare il campo Tipo di accesso impostato su ACCESS_ACCEPT.

In Impostazioni avanzate attributi (Advanced Attributes Settings), aggiungete Radius > Class—[25] con il valore e fate clic su Invia (Submit).

Passaggio 6.1. Profilo di vendita al dettaglio: In Impostazioni avanzate attributi aggiungere Radius:Class con il valore RETAIL_ADMIN_STR.



Suggerimento: Qui RETAIL_ADMIN_STR può essere qualsiasi cosa; accertarsi che anche il CCP abbia le stesse esigenze in termini di valore.

The screenshot shows the 'Authorization Profile' configuration page for 'FMC_GUI_Retail'. The 'Name' field is set to 'FMC_GUI_Retail'. The 'Access Type' dropdown is set to 'ACCESS_ACCEPT'. Under 'Network Device Profile', 'Cisco' is selected. In the 'Attributes Details' section, it shows 'Access Type = ACCESS_ACCEPT' and 'Class = RETAIL_ADMIN_STR'.

Passaggio 6.2 Finanza profilo: In Impostazioni avanzate attributi aggiungere Radius:Class con il valore FINANCE_ADMIN_STR.



Suggerimento: Qui FINANCE_ADMIN_STR può essere qualsiasi cosa; assicurarsi che lo stesso valore sia inserito anche sul lato FMC.

The screenshot shows the 'Policy / Policy Elements' section of the Cisco Identity Services Engine. On the left, there's a navigation bar with links like Bookmarks, Dashboard, Context Visibility, Operations, Policy (which is selected), Administration, Work Centers, and Interactive Help. The main area is titled 'Authorization Profiles > FMC_GUI_Finance'. It shows an 'Authorization Profile' with a name 'FMC_GUI_Finance' and a description. Under 'Access Type', it's set to 'ACCESS_ACCEPT'. A 'Network Device Profile' dropdown is set to 'Cisco'. Below that, 'Service Template', 'Track Movement', 'Agentless Posture', and 'Passive Identity Tracking' are listed with checkboxes. A 'Common Tasks' section follows, then an 'Advanced Attributes Settings' section. At the bottom, under 'Attributes Details', it says 'Access Type = ACCESS_ACCEPT' and 'Class = FINANCE_ADMINISTRATOR'.

Aggiungi nuovo set di criteri

Passaggio 7. Creare un set di criteri corrispondente all'indirizzo IP del CCP. In questo modo si impedisce ad altre periferiche di concedere l'accesso agli utenti. Passare a Criterio > Set di criteri > Icona del segno più nell'angolo superiore sinistro.

The screenshot shows the 'Policy / Policy Sets' section. The left sidebar is identical to the previous one. The main area is titled 'Policy Sets' and contains a table with columns for Status, Policy Set Name, Description, and Conditions. A search bar is at the top of the table. To the right of the table are buttons for 'Reset', 'Reset Policyset Hitcounts', 'Save', and 'Allowed Protocols / Server Sequence Hits Actions View'. A red box highlights the '+' icon in the top-left corner of the table header.

Passaggio 8.1. Una nuova riga viene posizionata all'inizio dei set di criteri.

Assegnare un nome al nuovo criterio e aggiungere una condizione superiore per l'attributo RADIUS NAS-IP-Address corrispondente all'indirizzo IP della console centrale di gestione. Fate clic su Usa (Use) per mantenere le modifiche e uscire dall'editor.

The screenshot shows the 'Conditions Studio' interface. The left sidebar includes a 'Library' section with various icons. The main area has a 'Editor' section where a condition is being defined. The condition is for 'Radius-NAS-IP-Address' with the operator 'Equals' and the value '10.225.86.50'. Below the condition, there's a link 'Set to "Is not"' and a 'Save' button. A red box highlights the 'Save' button.

Passaggio 8.2. Al termine, fare clic su Save (Salva).

Passaggio 9. Visualizzare il nuovo set di criteri facendo clic sull'icona set situata alla fine della riga.

Espandere il menu Criteri di autorizzazione e fare clic sull'icona con il segno più per aggiungere una nuova regola che consente l'accesso all'utente con diritti di amministratore. Dagli un nome.

Impostare le condizioni in modo che corrispondano al gruppo di identità del dizionario con nome attributo uguale a e scegliere Gruppi di identità utente. In Criteri di autorizzazione creare le regole seguenti:

- Regola 1: Se Gruppo di identità utente è uguale a Gruppo_Retail_A, assegnare il profilo Retail.
- Regola 2: Se Gruppo di identità utente è uguale a Group_Finance_B, assegnare la funzione Contabilità profilo.

Passaggio 10. Impostare i profili di autorizzazione rispettivamente per ogni regola e fare clic su Salva.

Configurazione FMC

Aggiunta del server ISE RADIUS per l'autenticazione FMC

Passaggio 1. Definizione della struttura di dominio:

- Accedere al dominio globale FMC.
- Passare a Amministrazione > Domini.
- Fare clic su Aggiungi dominio per creare Retail-A e Finance-B come sottodomini di Global.

Firewall Management Center
System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin cisco SECURE

Domain configuration is up to date. Save Cancel Add Domain

Name	Description	Devices
Global		
Finance-B		
Retail-A		 1 Device*

Passaggio 2.1. Configurare l'oggetto autenticazione esterna nel dominio su Retail-A

- Passare il dominio a Retail-A.
- Selezionare Sistema > Utenti > Autenticazione esterna.
- Selezionare Add External Authentication Object (Aggiungi oggetto autenticazione esterno) e scegliere RADIUS.
- Immettere l'indirizzo IP di ISE e il segreto condiviso configurato in precedenza.
- Immettere i parametri specifici di RADIUS > Amministratore > classe=RETAIL_ADMIN_STR



Suggerimento: Utilizzare lo stesso valore per class configurato in Authorization Profiles of ISE (Profili di autorizzazione di ISE).

Firewall Management Center
System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin cisco SECURE

Domain configuration is up to date.

Filter domains

Name	Description
Global	
Finance-B	
Retail-A	

Global
Finance-B
Retail-A

User Preferences

Theme: Light Dusk Classic

Log Out

Last login from 10.227.192.57 on 2020-02-11 02:17:27

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FMC

Description: RADIUS Auth for FMC

Primary Server

Host Name/IP Address: 10.197.243.183
ex. IP or hostname

Port: 1812

RADIUS Secret Key: ****

Backup Server (Optional)

Host Name/IP Address:

Port: 1812
ex. IP or hostname

RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator: Class=RETAIL_ADMIN_STR

Passaggio 2.2. Configurare l'oggetto autenticazione esterna nel dominio su Finance-B

- Passare Domain a Finance-B.
- Selezionare Sistema > Utenti > Autenticazione esterna.
- Selezionare Add External Authentication Object (Aggiungi oggetto autenticazione esterno) e scegliere RADIUS.
- Immettere l'indirizzo IP di ISE e il segreto condiviso configurati in precedenza.
- Immettere i parametri specifici di RADIUS > Amministratore > class=FINANCE_ADMIN_STR



Suggerimento: Utilizzare lo stesso valore per class configurato in Authorization Profiles of ISE (Profili di autorizzazione di ISE).

Firewall Management Center

System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin SECURE

Name	Description
Global	
Finance-B	
Retail-A	

Domain configuration is u

Filter domains

Global

Finance-B

Retail-A

User Preferences

Theme: Light

Last login from 10.227.192.57 on 2026-02-11 02:17:27

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FMC

Description: RADIUS Auth for FMC

Primary Server

Host Name/IP Address: 10.197.243.183
Port: 1812
RADIUS Secret Key: ****

Backup Server (Optional)

Host Name/IP Address:
Port: 1812
RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30
Retries: 3
Access Admin:
Administrator: Class=FINANCE_ADMIN_STR

Passaggio 3. Attiva autenticazione: Abilitare l'oggetto e impostarlo come metodo di autenticazione shell. Fare clic su Save and Apply (Salva e applica).

Verifica

Test di accesso tra domini

- Tentare di accedere all'interfaccia Web di FMC utilizzando admin_retail. Verificare che il Dominio corrente visualizzato nella parte superiore destra dell'interfaccia utente sia Retail-A.



Suggerimento: Quando si accede a un dominio specifico, utilizzare il formato nome_utente nome_dominio\radius_user_mapped_with_that_domain.

Ad esempio, se l'utente amministratore di Retail deve eseguire l'accesso, il nome utente deve essere Retail-A\admin_retail e la password corrispondente.

Summary Dashboard (switch_dashboard)

Provides a summary of activity on the appliance

Network Threats Intrusion Events Status Geolocation QoS Zero Trust +

Unique Applications over Time

Top Web Applications Seen

Top Client Applications

User Preferences

Theme: Light, Dusk, Classic

Last login from 10.110.212.21 on 2026-02-11 10:03:51

No Data

No Data

- Uscire e accedere come admin_financial. Verificare che l'utente sia limitato al dominio Finance-B e che non sia in grado di visualizzare i dispositivi Retail-A.

The screenshot shows the FMC interface with the 'Devices' tab selected. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. A right-hand sidebar shows 'User Preferences' with themes 'Light', 'Dusk', and 'Classic' selected. The main content area shows a table with columns: Name, Model, Version, Chassis, Licenses, Access Control Policy, and Auto. A search bar at the top says 'Filter domains' and shows 'Finance-B'.

Test interni FMC

Passare alle impostazioni del server RADIUS nel FMC. Utilizzare la sezione Parametri di test aggiuntivi per immettere un nome utente e una password di test. Se il test ha esito positivo, deve essere visualizzato un messaggio verde di operazione riuscita.

Additional Test Parameters

User Name	admin_financial
Password	*****

Test Output

```

Show Details ▾
check_auth_radius: szUser: admin_financial
RADIUS config file: /var/tmp/roCPmVujOv/radiusclient_0.conf
radiusauth - response: |User-Name=admin_financial|
radiusauth - response: |Class=FINANCE_ADMIN_STR|
User Test
radiusauth - response: |Class=CACS:0ac5f3b7m0vFormvHHyC_lgO13NsO1DZN6QciDbrC0cwlaYWHMto:eagle/556377151/553|
"admin_financial" RADIUS Authentication OK
check_is_radius_member attrib match found: |Class=FINANCE_ADMIN_STR| ~ |Class=FINANCE_ADMIN_STR| *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:

```

*Required Field

[Cancel](#) [Test](#) [Save](#)

log ISE in tempo reale

- In Cisco ISE, selezionare Operations > RADIUS > Live Log.

The screenshot shows the Cisco ISE Operations / RADIUS interface. The left sidebar includes 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations' (selected), 'Policy', 'Administration', 'Work Centers', and 'Interactive Help'. The main area has tabs for 'Live Logs' (selected) and 'Live Sessions'. It displays metrics for 'Misconfigured Suplicants', 'Misconfigured Network Devices', 'RADIUS Drops' (30), 'Client Stopped Responding', and 'Repeat Counter'. Below is a table of log entries:

Time	Status	Details	Reape...	Identity	Endpoint ID	Endpoint...	Authentica...	Authorization Policy	Authorization Profiles	IP Address
Feb 11, 2026 10:10:43.2...	0	0	0	admin_financial	FMC Domain ...	FMC Domain Login >> Finance Domain	FMC_GUI_Finance			
Feb 11, 2026 10:09:38.3...	0	0	0	admin_financial	FMC Domain ...	FMC Domain Login >> Finance Domain	FMC_GUI_Finance			
Feb 11, 2026 10:08:12.9...	0	0	0	admin_retail	FMC Domain ...	FMC Domain Login >> Retail Domain	FMC_GUI_Retail			

- Confermare che le richieste di autenticazione mostrino uno stato di superamento e che il profilo di autorizzazione corretto (e la stringa della classe associata) sia stato inviato nel pacchetto RADIUS Access-Accept.

Overview

Event	5200 Authentication succeeded
Username	admin_finance
Endpoint Id	
Endpoint Profile	
Authentication Policy	FMC Domain Login >> Default
Authorization Policy	FMC Domain Login >> Finance Domain
Authorization Result	FMC_GUI_Finance

Authentication Details

Source Timestamp	2026-02-11 16:40:43.275
Received Timestamp	2026-02-11 22:10:43.275
Policy Server	eagle
Event	5200 Authentication succeeded
Username	admin_finance
User Type	User
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Group_Finance_B

Result

Class	FINANCE_ADMIN_STR
Class	CACS:0ac5f3b7m0vFomvHHyC_igO13NsO1DZN6QciDbrc0cwl aYWHMto:eagle/556377151/553

Informazioni correlate

Configurazione dell'autenticazione esterna FMC e FTD con ISE come server RADIUS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuracy di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).