

Configurazione dell'autenticazione esterna RADIUS su DNA Center e ISE 3.1

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Altri ruoli](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione esterna RADIUS su Cisco DNA Center utilizzando un server Cisco ISE con versione 3.1.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco DNA Center e Cisco ISE sono già integrati e l'integrazione è su Active Status.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco DNA Center versione 2.3.5.x.
- Cisco ISE versione 3.1.

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.

Configurazione

Passaggio 1. Accedere alla GUI di Cisco DNA Center e selezionare System > Settings > Authentication and Policy Server.

Verificare che il protocollo RADIUS sia configurato e che lo stato ISE sia Active per il server ISE Type.

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

IP Address	Protocol	Type	Status	Actions
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...
[REDACTED]	RADIUS	ISE	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...



Nota: il tipo di protocollo RADIUS_TACACS funziona per questo documento.



Avviso: se il server ISE non è nello stato Attivo, è necessario correggere prima l'integrazione.

Passaggio 2. Su ISE Server selezionare Administration > Network Resources > Network Devices, fare clic sull'icona Filter, scrivere l'indirizzo IP di Cisco DNA Center e verificare se è presente una voce. In caso affermativo, andare al passo 3.

Se la voce non è presente, è necessario visualizzare il messaggio Nessun dato disponibile.

Network Devices

Selected 0 Total 0  

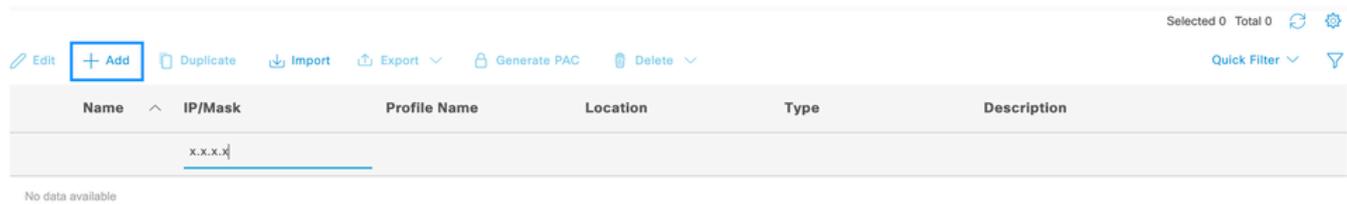
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

In questo caso, è necessario creare un dispositivo di rete per Cisco DNA Center, quindi fare clic sul pulsante Add (Aggiungi).

Network Devices



Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Configurare il nome, la descrizione e l'indirizzo IP (o gli indirizzi) di Cisco DNA Center. Tutte le altre impostazioni sono impostate sui valori predefiniti e non sono necessarie per le finalità di questo documento.

Network Devices

* Name

Description

IP Address

* Device Profile

Model Name

Software Version

* Network Device Group

Location	<input type="text" value="All Locations"/>	<input type="button" value="Set To Default"/>
IPSEC	<input type="text" value="Is IPSEC Device"/>	<input type="button" value="Set To Default"/>
Device Type	<input type="text" value="All Device Types"/>	<input type="button" value="Set To Default"/>

Scorrere verso il basso e abilitare le impostazioni di autenticazione RADIUS facendo clic sulla relativa casella di controllo e configurare un segreto condiviso.



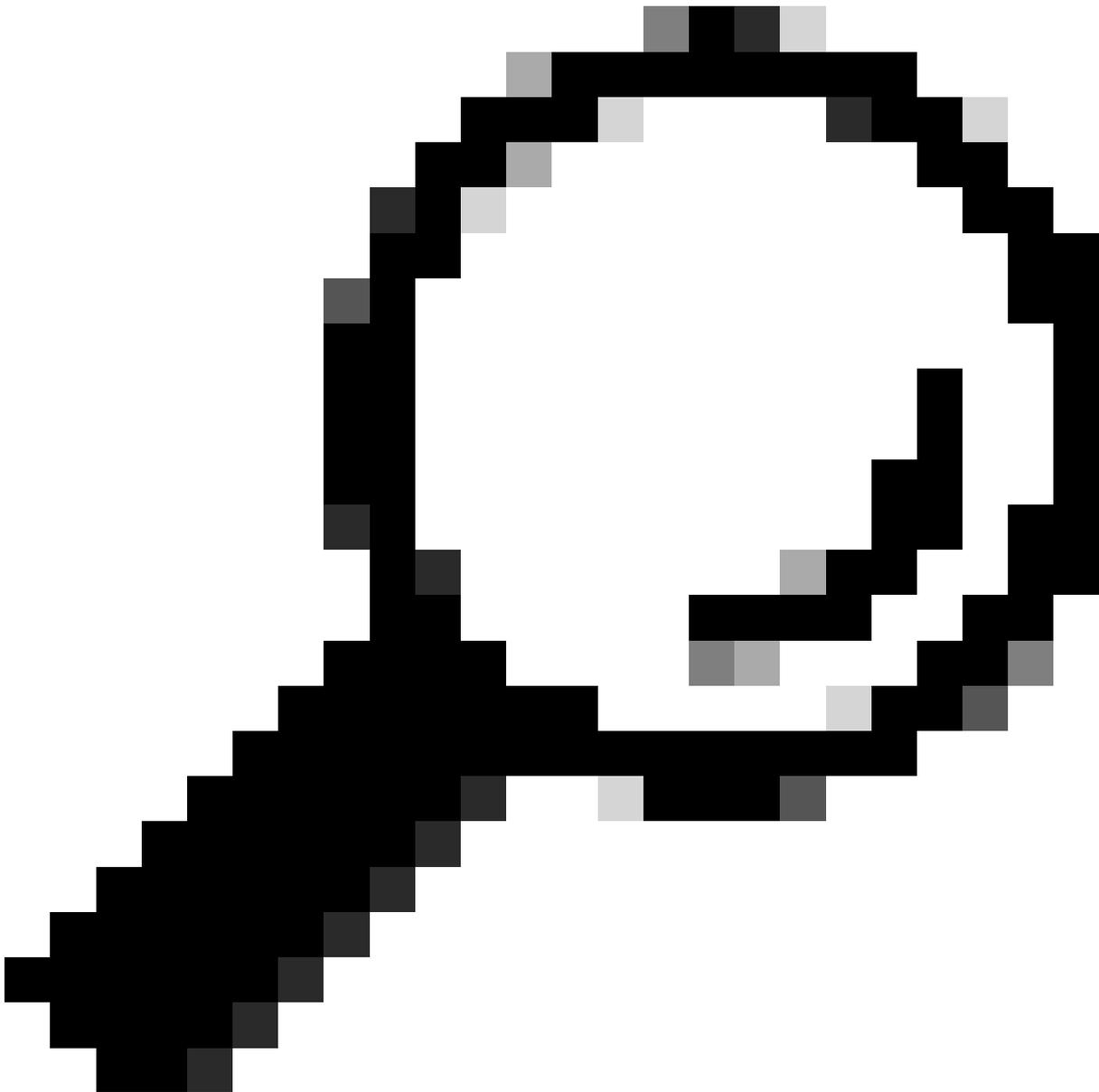
✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Show



Suggerimento: questo segreto condiviso sarà necessario in seguito, quindi salvalo altrove.

Solo in questo caso, fare clic su Submit (Invia).

Passaggio 3. Sul server ISE selezionare Policy > Policy Elements > Results (Policy > Elementi criteri > Risultati) per creare il profilo di autorizzazione.

Assicurarsi di essere in Autorizzazione > Profili di autorizzazione, quindi selezionare l'opzione Aggiungi.

Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 20

Name	Profile	Description
APs_19.5.0	Cisco	172_19_5_0-INFRA_VN
AuthTemplate	Cisco	
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the
CY_CAMPUS_MAC	Cisco	CY_CAMPUS_MAC
CY Guest profile	Cisco	CY Guest profile

Configurare Nome, aggiungere una Descrizione solo per conservare un record del nuovo Profilo e assicurarsi che il Tipo di accesso sia impostato su ACCES_ACCEPT.

Results

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: DNAC_AUTH_PROFILE

Description: External Authentication for Cisco DNA Center

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

Scorrere verso il basso e configurare le impostazioni avanzate degli attributi.

Nella colonna sinistra cercare l'opzione cisco-av-pair e selezionarla.

Nella colonna di destra digitare manualmente Role=SUPER-ADMIN-ROLE.

Una volta che l'immagine è simile a quella mostrata di seguito, fare clic su Submit (Invia).

Advanced Attributes Settings

Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = Role=SUPER-ADMIN-ROLE

Passaggio 4. Sul server ISE selezionare Work Centers > Profiler > Policy Sets (Centri di lavoro > Profiler > Set di criteri), per configurare i criteri di autenticazione e autorizzazione.

Identificare il criterio predefinito e fare clic sulla freccia blu per configurarlo.

The screenshot shows the Cisco ISE interface for configuring Policy Sets. The breadcrumb navigation is Work Centers > Profiler > Policy Sets. The page title is "Work Centers - Profiler". The navigation menu includes Overview, Ext Id Sources, Network Devices, Endpoint Classification, Node Config, Feeds, Manual Scans, and More. The Policy Sets table has columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The 'Default' policy set is highlighted with a blue box, and a blue arrow points to its configuration icon.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙️	➔
⊗	MAB		Wired_MAB	Default Network Access	0	⚙️	➔
✅	Default	Default policy set		Default Network Access	180517	⚙️	➔

All'interno del set di criteri predefinito, espandere il criterio di autenticazione e nella sezione Default espandere le opzioni e verificare che corrispondano alla configurazione seguente.

Cisco ISE Work Centers - Profiler

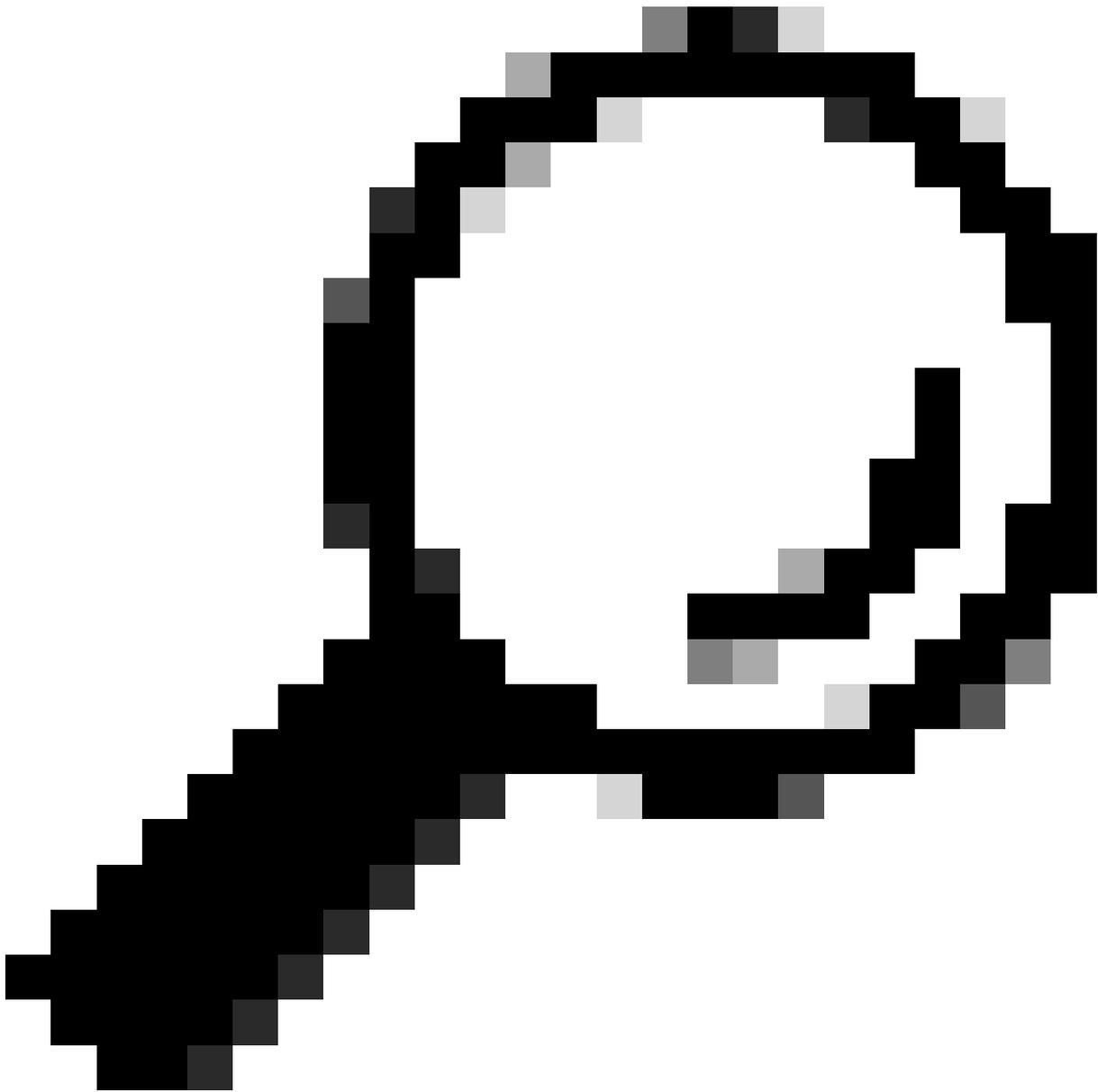
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	4556	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	⚙️



Suggerimento: anche REJECT configurato sulle 3 opzioni funziona

All'interno del set di criteri predefinito, espandere il criterio di autorizzazione e selezionare l'icona Aggiungi per creare una nuova condizione di autorizzazione.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 ▾ Authorization Policy (25)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
+							

Configurare un Nome regola e fare clic sull'icona Aggiungi per configurare la condizione.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 ▾ Authorization Policy (26)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
✓	DNAC-SUPER-ADMIN-ROLE		Select from list	Select from list			

Come parte della condizione, associarla all'indirizzo IP del dispositivo di rete configurato nel passo 2.

Conditions Studio

Library

Search by Name



- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CY_Campus
- CY_CAMPUS_MAC
- CY_Campus_voice
- CY_Guest
- EAP-MSCHAPv2
- ...

Editor

Network Access-Device IP Address

Equals 10.88.244.151

Set to 'Is not'

Duplicate Save

NEW | AND | OR

Close

Use

Fare clic su Save (Salva).

Salvarlo come nuova condizione della libreria e denominarlo come desiderato, in questo caso è denominato DNAC.



Save condition

Save as existing Library Condition (replaces current version and impact all policies that use this condition)

Select from list ▼

Save as a new Library Condition

DNAC

Description (optional)

Condition Description

Close

Save

Infine, configurare il profilo creato al passo 3.

The screenshot shows the Cisco ISE GUI for configuring a new condition. The 'Save as a new Library Condition' option is selected. The condition name is 'DNAC' and the description is 'Condition Description'. The 'Save' button is highlighted.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	DNAC-SUPER-ADMIN-ROLE	DNAC	DNAC_AUTH_PROFILE	Select from list		

Fare clic su Save.

Passaggio 5. Accedere alla GUI di Cisco DNA Center e selezionare System > Users & Roles > External Authentication.

Fare clic sull'opzione Enable External User (Abilita utente esterno) e impostare l'attributo AAA su

User Management

Role Based Access Control

External Authentication

External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisc attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

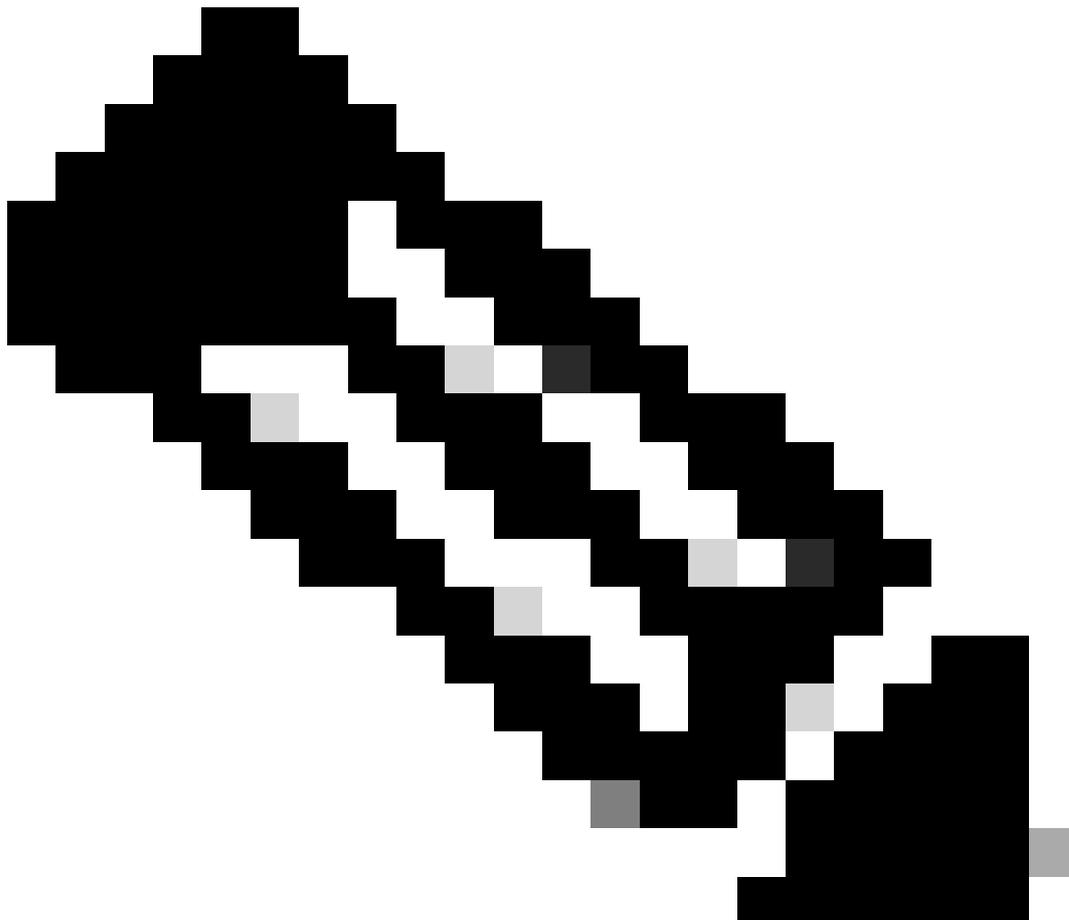
Enable External User ?

AAA Attribute

AAA Attribute
Cisco-AVPair

Reset to Default

Update



Nota: ISE Server usa l'attributo Cisco-AVPair sul back-end, quindi la configurazione al punto 3 è valida.

Scorrere verso il basso per visualizzare la sezione di configurazione dei server AAA. Configurare l'indirizzo IP del server ISE nel passaggio 1 e il segreto condiviso configurato nel passaggio 3.

Quindi fai clic su Visualizza impostazioni avanzate.

▼ AAA Server(s)

Primary AAA Server

IP Address

192.168.1.1



Shared Secret

SHOW

Info

[View Advanced Settings](#)

[Update](#)

Secondary AAA Server

IP Address

192.168.1.1



Shared Secret

SHOW

Info

[View Advanced Settings](#)

[Update](#)

Verificare che l'opzione RADIUS sia selezionata e fare clic sul pulsante Aggiorna su entrambi i server.

▼ AAA Server(s)

Primary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

Secondary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

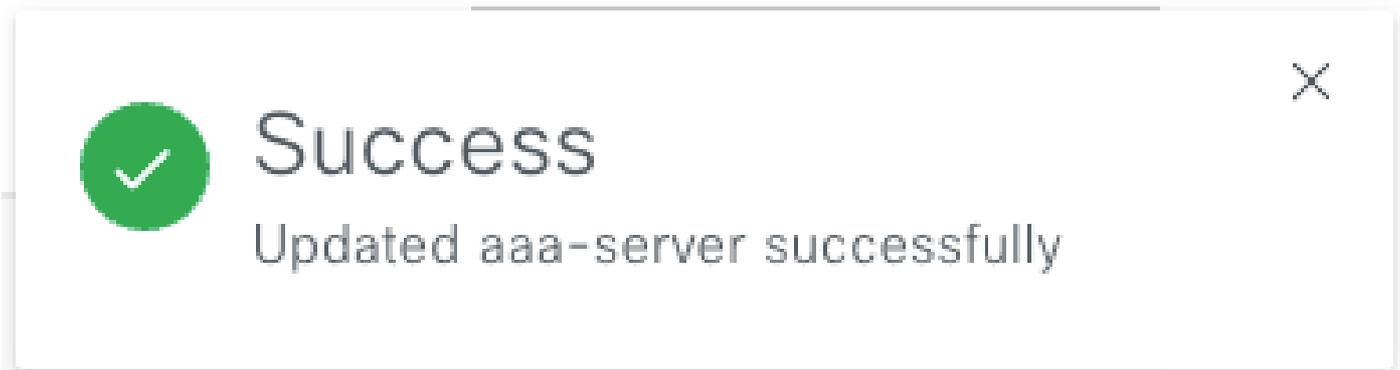
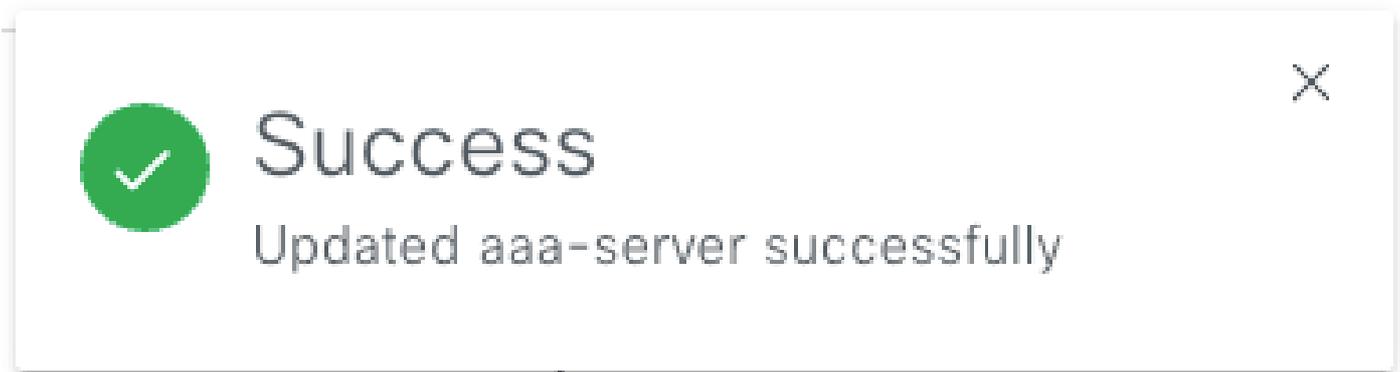
Timeout (seconds)

4

Update

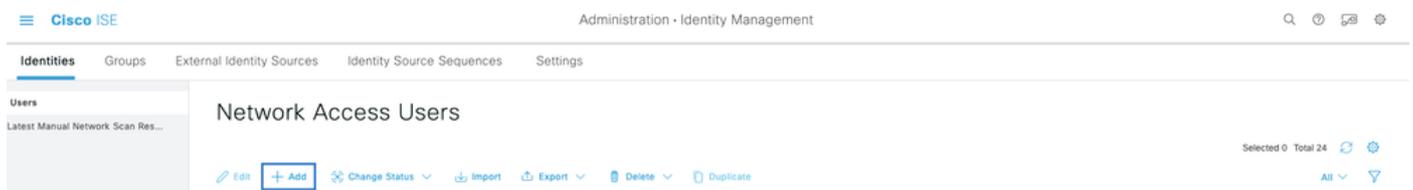
Update

È necessario visualizzare un messaggio di operazione completata per ogni elemento.



Ora è possibile eseguire il login con qualsiasi identità ISE creata con il menu ISE > Amministrazione > Gestione delle identità > Identità > Utenti.

Nel caso in cui non sia stato creato alcun utente, effettuare il login ad ISE, selezionare il percorso indicato sopra e aggiungere un nuovo utente di accesso alla rete.



Verifica

Caricamento dell'interfaccia utente di Cisco DNA Center e accedere con un utente dalle identità ISE.



Cisco DNA Center

The bridge to possible

✓ Success!

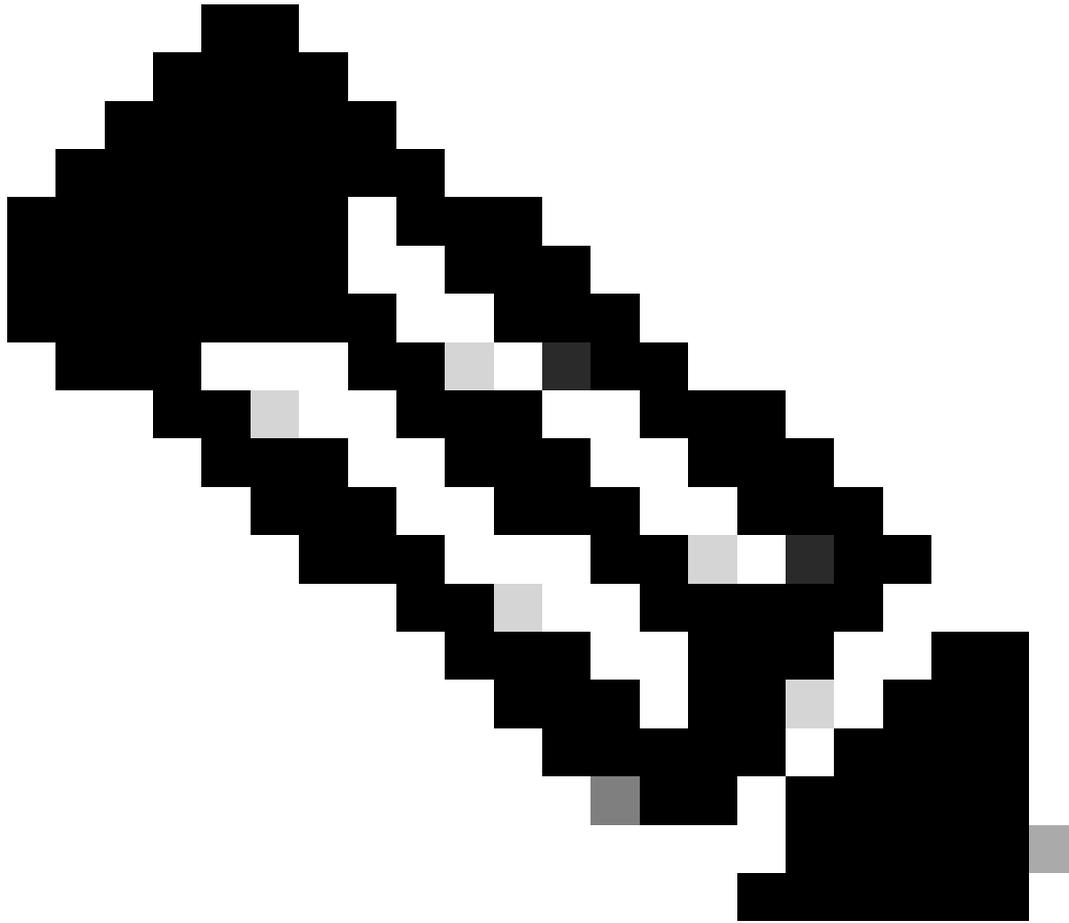
Username

test

Password

.....

Log In



Nota: qualsiasi utente con identità ISE può accedere ora. È possibile aggiungere maggiore granularità alle regole di autenticazione su ISE Server.

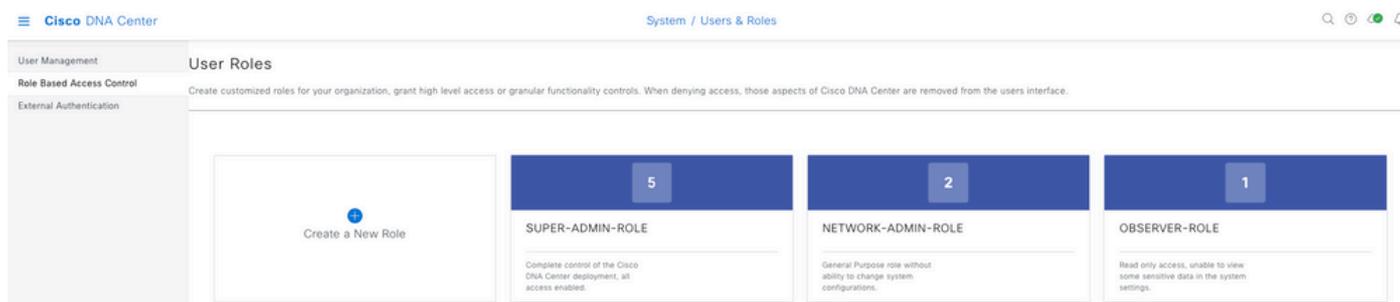
Dopo l'accesso riuscito, il nome utente viene visualizzato sull'interfaccia utente di Cisco DNA Center

Welcome, test

Schermata iniziale

Altri ruoli

È possibile ripetere questi passaggi per ogni ruolo in Cisco DNA Center, come predefinito: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE e OBSERVER-ROLE.



In questo documento viene utilizzato l'esempio del ruolo SUPER-ADMIN-ROLE. Tuttavia, è possibile configurare un profilo di autorizzazione per ISE per ogni ruolo su Cisco DNA Center. L'unica considerazione è che il ruolo configurato nel passaggio 3 deve corrispondere esattamente (con distinzione tra maiuscole e minuscole) al nome del ruolo su Cisco DNA Center.

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'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).