

Configurar a autenticação externa RADIUS no DNA Center e no ISE 3.1

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

[Mais Funções](#)

Introdução

Este documento descreve como configurar a Autenticação externa RADIUS no Cisco DNA Center usando um servidor Cisco ISE executando a versão 3.1.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O Cisco DNA Center e o Cisco ISE já estão integrados e a integração está no status Ativo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do Cisco DNA Center 2.3.5.x.
- Cisco ISE versão 3.1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa 1. Faça login na GUI do Cisco DNA Center e navegue até System > Settings > Authentication and Policy Servers.

Verifique se o protocolo RADIUS está configurado e se o status do ISE é Ativo para o servidorTipo de ISE.

Settings / External Services

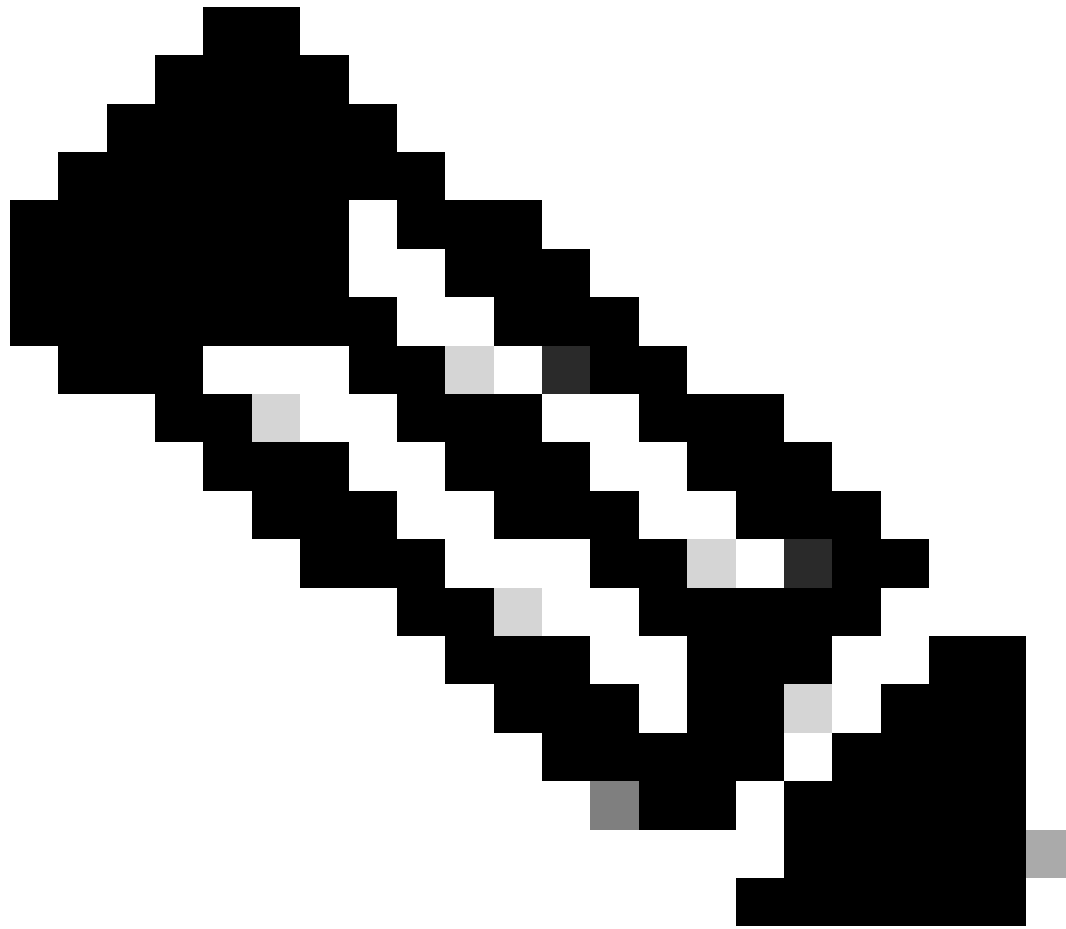
Authentication and Policy Servers

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	...



Observação: o tipo de protocolo RADIUS_TACACS funciona para este documento.














Aviso: caso o servidor ISE não esteja com status Ativo, é necessário corrigir a integração primeiro.

Etapa 2. No ISE Server, navegue para Administration > Network Resources > Network Devices, clique no ícone Filter, escreva o Cisco DNA Center IP Address e confirme se existe uma entrada. Se isso acontecer, vá para a Etapa 3.

Se a entrada estiver ausente, você deverá ver a mensagem No data available.

Network Devices

Selected 0 Total 0  

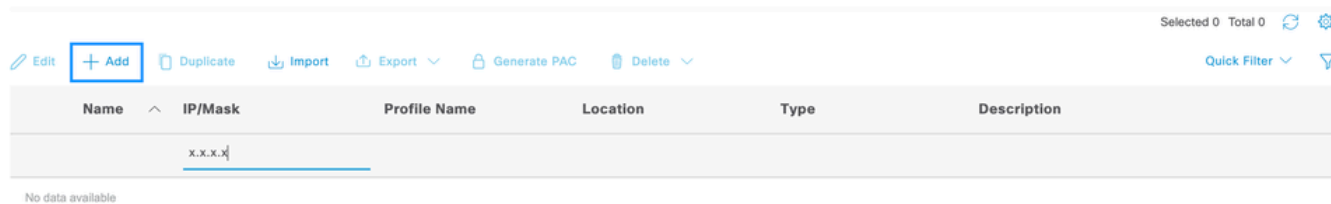
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

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

No data available

Nesse caso, você deve criar um dispositivo de rede para o Cisco DNA Center, então clique no botão Adicionar.

Network Devices



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



No data available

Configure o Nome, a Descrição e o Endereço IP (ou Endereços) do Cisco DNA Center; todas as outras configurações são definidas como Valores padrão e não são necessárias para a finalidade deste documento.

Network Devices

* Name

Description

 **IP Address** * IP : / 

* 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"/>

Role para baixo e ative as Configurações de autenticação RADIUS clicando em sua caixa de seleção e configure um segredo compartilhado.



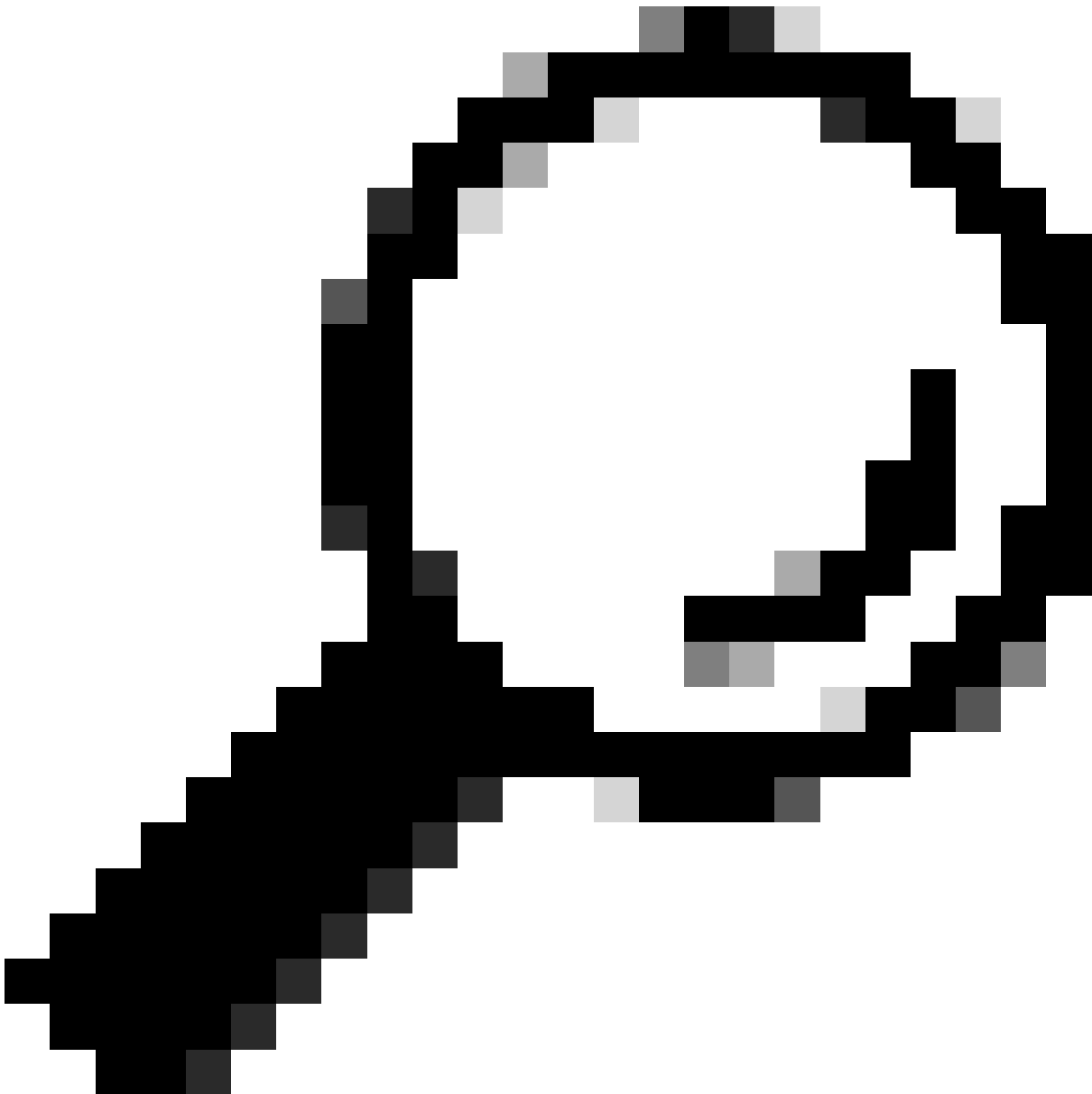
▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Show



Dica: esse segredo compartilhado será necessário posteriormente, portanto, salve-o em outro lugar.

Somente então, clique em Submit.

Etapa 3. No ISE Server, navegue para Policy > Policy Elements > Results, para criar o Authorization Profile.

Verifique se você está em Authorization > Authorization Profiles e selecione a opção Add.

The screenshot shows the Cisco ISE interface for 'Policy - Policy Elements' > 'Results'. The left sidebar has 'Authorization' > 'Authorization Profiles' selected. The main area displays a table of 'Standard Authorization Profiles'. The table has columns for Name, Profile, and Description. The 'Add' button is highlighted with a blue box and an arrow pointing to it.

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

Configure Name, adicione uma Description apenas para manter um registro do novo Perfil e certifique-se de que o Tipo de acesso esteja definido como ACCESS_ACCEPT.

The screenshot shows the 'New Authorization Profile' configuration form. The 'Name' field is 'DNAC_AUTH_PROFILE', the 'Description' field is 'External Authentication for Cisco DNA Center', and the 'Access Type' dropdown is set to 'ACCESS_ACCEPT'. The 'Network Device Profile' is set to 'Cisco'.

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: (i)

Agentless Posture: (i)

Passive Identity Tracking: (i)

Role para baixo e configure as Configurações avançadas de atributos.

Na coluna esquerda, procure a opção cisco-av-pair e selecione-a.

Na coluna da direita manualmente, digite Role=SUPER-ADMIN-ROLE.

Quando a imagem abaixo estiver parecida, clique em Submit.

Advanced Attributes Settings

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

Attributes Details

Access Type = ACCESS_ACCEPT

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

Etapa 4. No ISE Server, navegue para Work Centers > Profiler > Policy Sets, para configurar a Authentication & Authorization Policy.

Identifique a política Default e clique na seta azul para configurá-la.

The screenshot shows the Cisco ISE Work Centers - Profiler interface. The 'Policy Sets' section is active, displaying a table of policy sets. The 'Default' policy set is highlighted with a blue box, and a blue arrow points to its 'View' button.

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	⚙️	➔

Dentro do Default Policy Set, expanda a Authentication Policy e, na seção Default, expanda as Options e certifique-se de que elas correspondam à configuração abaixo.

Cisco ISE Work Centers - Profiler

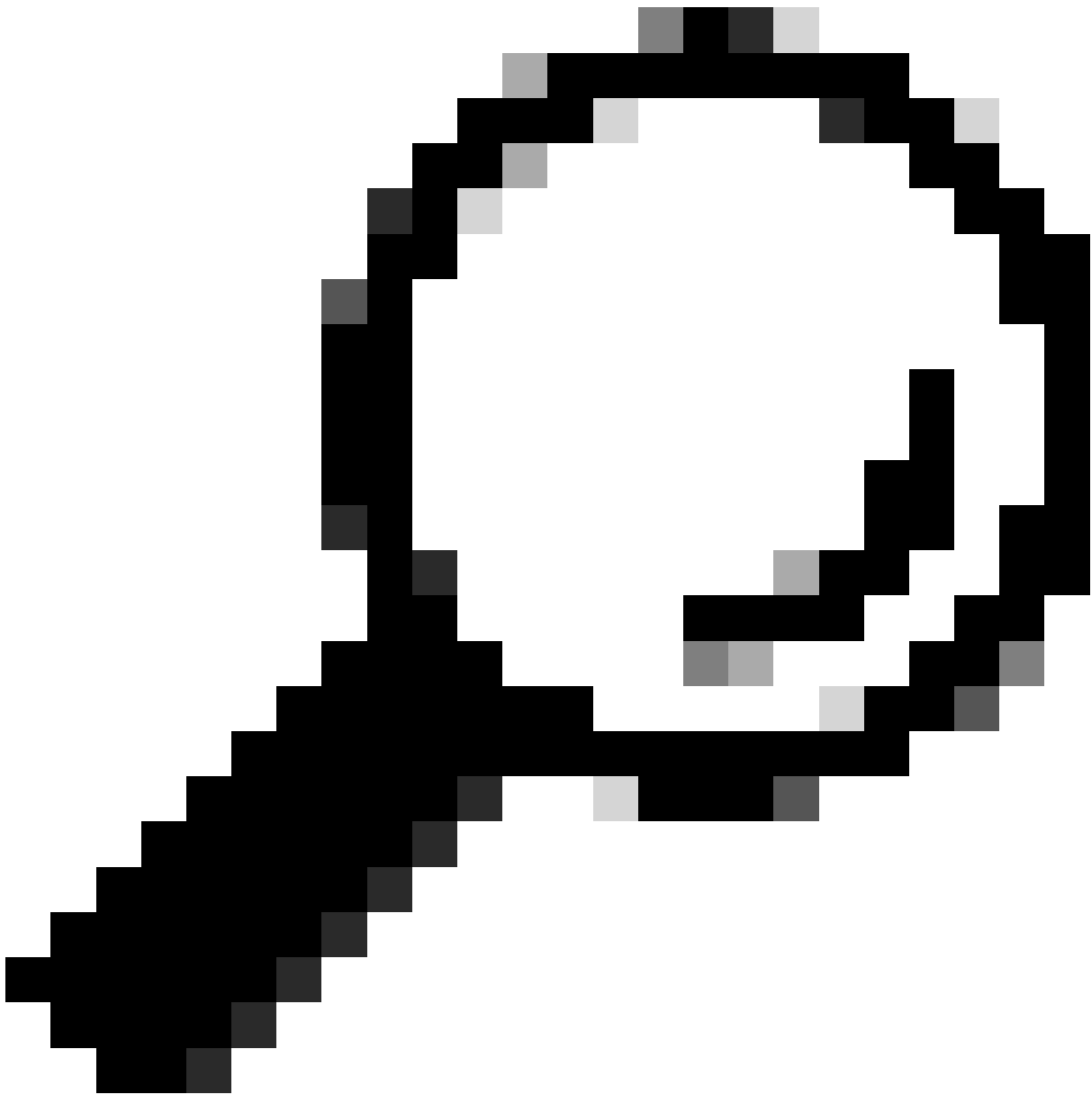
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

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	⚙️



Dica: REJECT configurado nas 3 opções também funciona

Dentro do Default Policy Set, expanda a Authorization Policy e selecione o ícone Add para criar uma nova Authorization Condition.

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			
⊕							

Configure um Nome da Regra e clique no ícone Adicionar para configurar a Condição.

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			

Como parte da condição, associe-a ao endereço IP do dispositivo de rede configurado na etapa 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

Clique em Salvar.

Salve-a como uma nova condição de biblioteca e nomeie-a como desejar; nesse caso, é nomeada como 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

Por fim, configure o Perfil criado na Etapa 3.

The screenshot shows the Cisco ISE GUI for configuring a new profile. 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		

Clique em Save.

Etapa 5. Faça login na GUI do Cisco DNA Center e navegue para Sistema > Usuários e funções > Autenticação externa.

Clique na opção Enable External User e defina o AAA Attribute como Cisco-AVPair.

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 cisco 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".

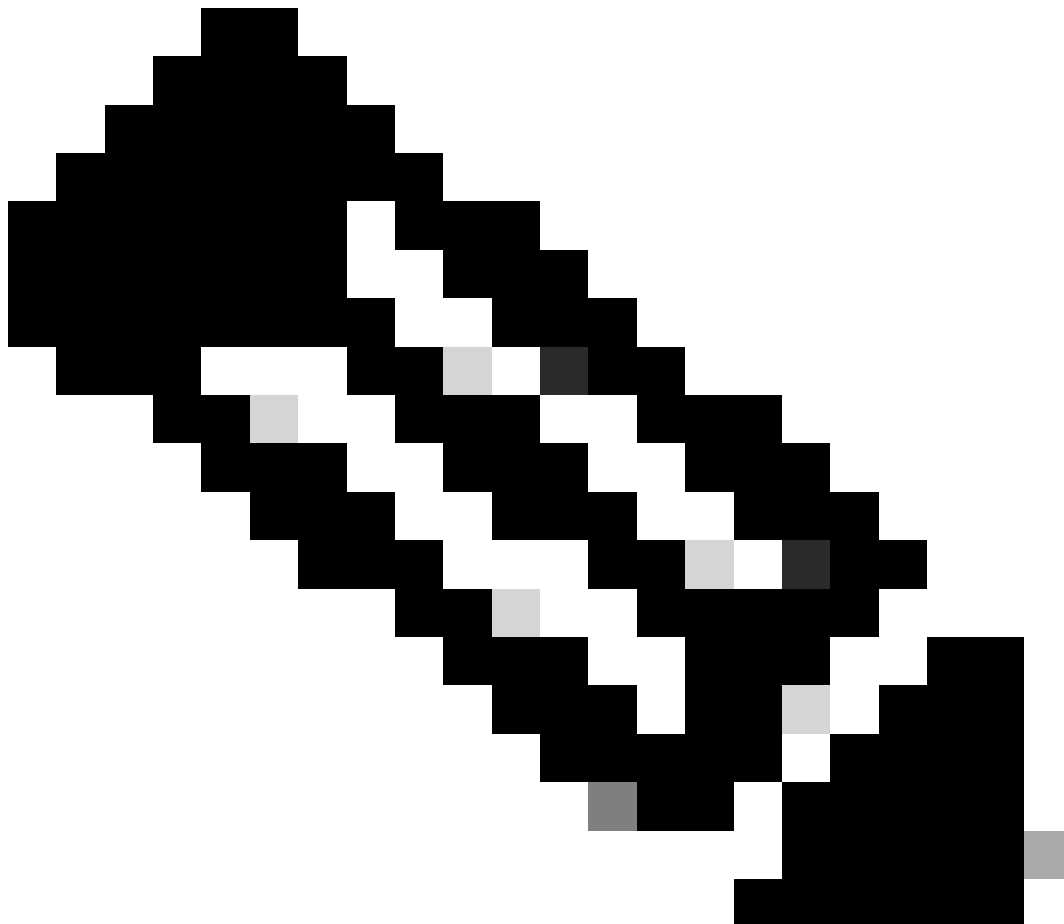
Enable External User ?

AAA Attribute

AAA Attribute
Cisco-AVPair

Reset to Default

Update



Observação: o ISE Server usa o atributo Cisco-AVPair no back-end, portanto, a

configuração na Etapa 3 é válida.

Role para baixo para ver a seção de configuração de servidor(es) AAA. Configure o endereço IP do servidor ISE na etapa 1 e o segredo compartilhado configurado na etapa 3.

Em seguida, clique em View Advanced Settings (Exibir configurações avançadas).

∨ AAA Server(s)

Primary AAA Server

IP Address

10.10.10.10



Shared Secret

SHOW

Info

View Advanced Settings

Update

Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

SHOW

Info

View Advanced Settings

Update

Verifique se a opção RADIUS está selecionada e clique no botão Update em ambos os servidores.

▼ AAA Server(s)

Primary AAA Server

IP Address

10.10.10.10



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

10.10.10.11



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

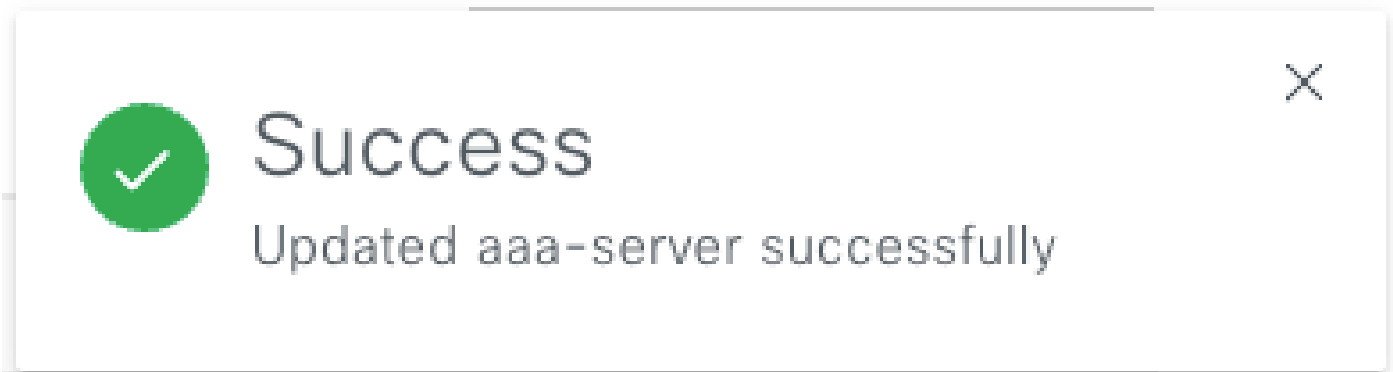
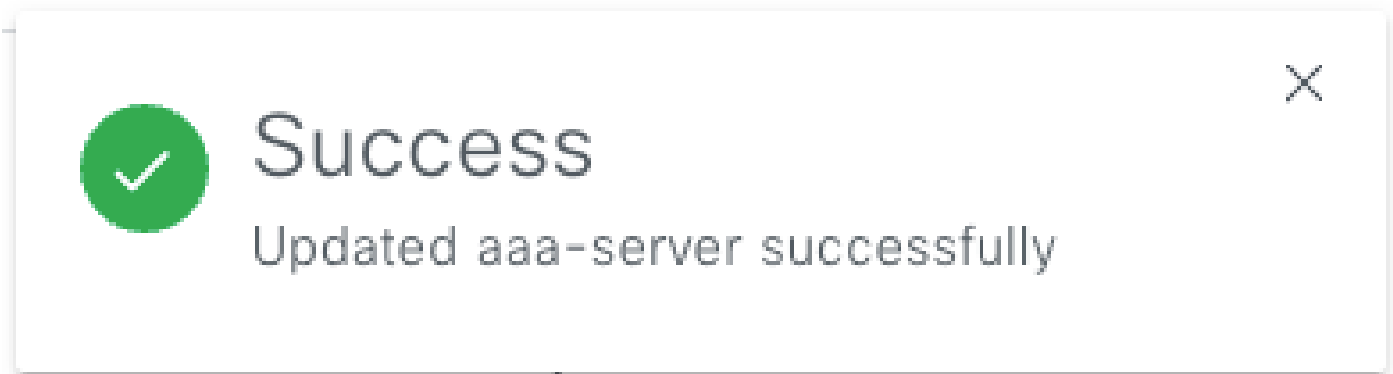
Timeout (seconds)

4

Update

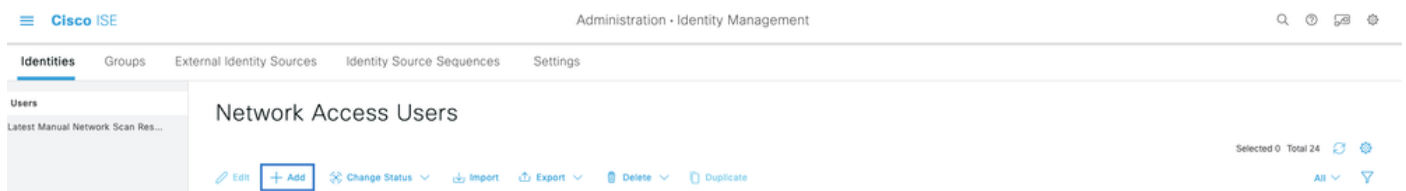
Update

Você deve ver uma mensagem de êxito para cada um.



Agora você poderá fazer login com qualquer Identidade do ISE criada no menu ISE > Administração > Gerenciamento de identidades > Identidades > Usuários.

Caso você não tenha nenhum criado, faça login no ISE, navegue até o caminho acima e adicione um novo usuário de acesso à rede.



Verificar

Carregar a GUI do Cisco DNA Center e faça login com um usuário das identidades do ISE.



Cisco DNA Center

The bridge to possible

✓ Success!

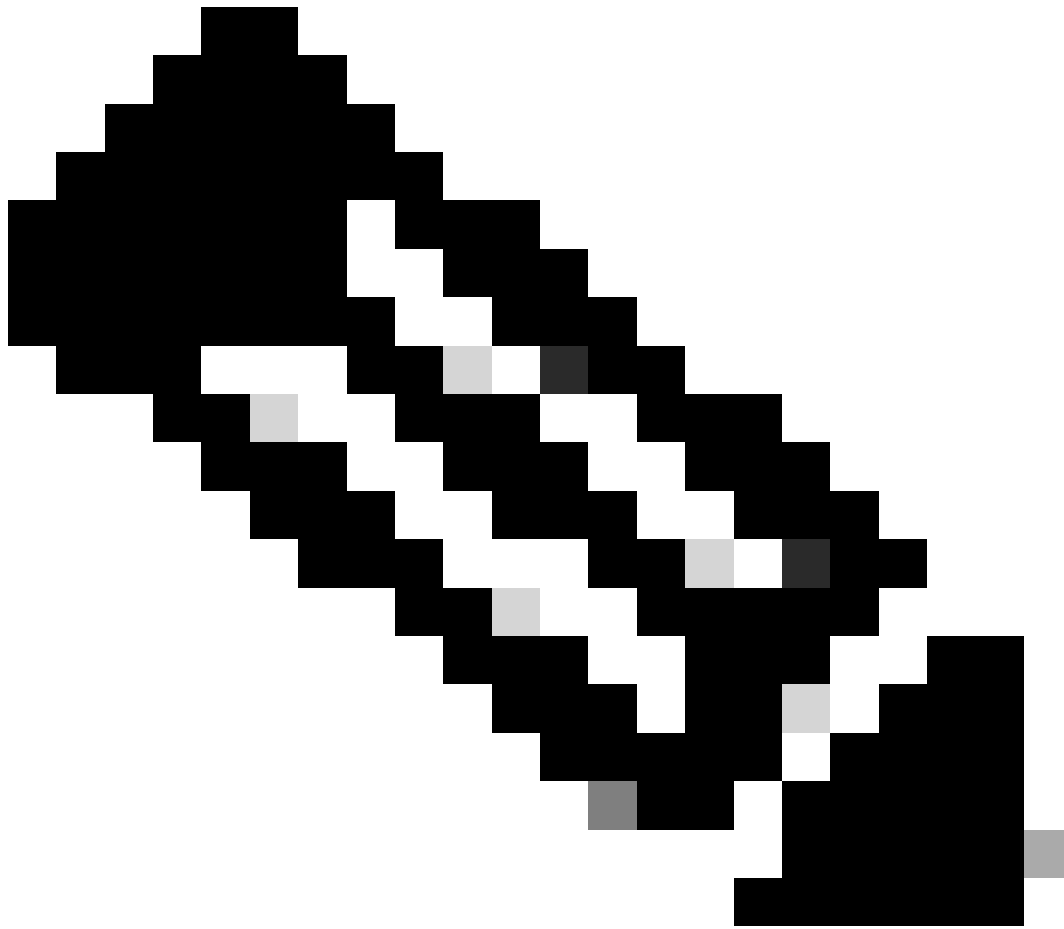
Username

test

Password

.....

Log In



Observação: qualquer usuário em identidades do ISE pode fazer login agora. Você pode adicionar mais granularidade às regras de autenticação no ISE Server.

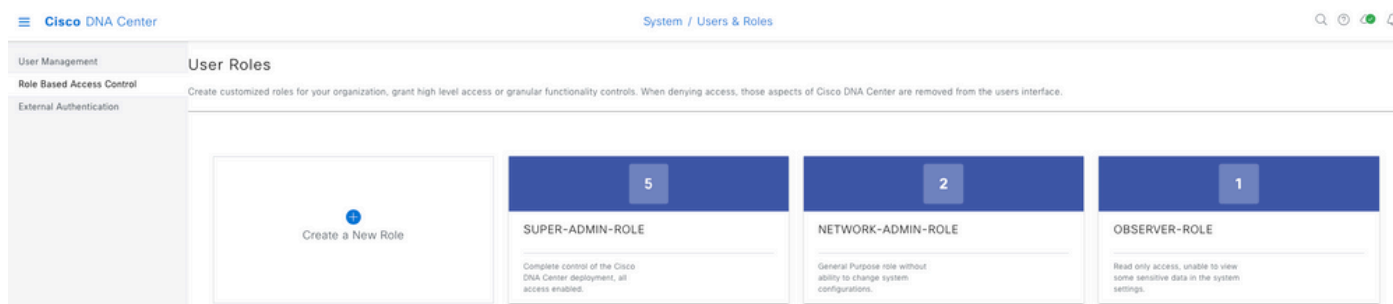
Após o login bem-sucedido, o nome de usuário é exibido na GUI do Cisco DNA Center

Welcome, test

Tela de boas-vindas

Mais Funções

Você pode repetir essas etapas para cada função no Cisco DNA Center, como padrão temos: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE e OBSERVER-ROLE.



Neste documento, usamos o exemplo de função SUPER-ADMIN-ROLE; no entanto, você pode configurar um perfil de autorização no ISE para cada função no Cisco DNA Center. A única consideração é que a função configurada na Etapa 3 precisa corresponder exatamente (diferencia maiúsculas de minúsculas) ao nome da função no Cisco DNA Center.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.