

# DNA CenterおよびISE 3.1でのRADIUS外部認証の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[その他のロール](#)

---

## はじめに

このドキュメントでは、3.1リリースを実行するCisco ISEサーバを使用して、Cisco DNA CenterでRADIUS外部認証を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco DNA CenterとCisco ISEはすでに統合されており、統合はアクティブステータスになっています。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco DNA Center 2.3.5.xリリース
- Cisco ISE 3.1リリース

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

ステップ 1： Cisco DNA CenterのGUIにログインし、System > Settings > Authentication and Policy Serversの順に選択します。

RADIUSプロトコルが設定されていて、ISE TypeサーバのISEステータスがActiveになっていることを確認します。

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] | <b>RADIUS</b> | <b>ISE</b> | <b>ACTIVE</b> | ...     |
| [REDACTED] | RADIUS        | AAA        | ACTIVE        | ...     |
| [REDACTED] | RADIUS        | AAA        | ACTIVE        | ...     |
| [REDACTED] | RADIUS_TACACS | AAA        | ACTIVE        | ...     |



注：このドキュメントでは、RADIUS\_TACACSプロトコルタイプが機能します。

---



警告:ISEサーバがアクティブステータスでない場合は、最初に統合を修正する必要があります。

ステップ 2 : ISEサーバで、Administration > Network Resources > Network Devicesの順に移動し、Filterアイコンをクリックし、Cisco DNA CenterのIPアドレスを記入して、エントリが存在するかどうかを確認します。増加している場合は、ステップ3に進みます。

エントリが見つからない場合は、「No data available」というメッセージが表示されます。

## Network Devices

Selected 0 Total 0  

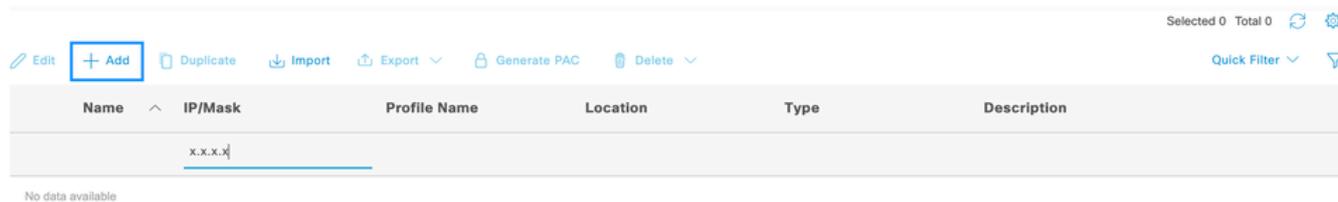
 Edit  + Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

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

No data available

この場合、Cisco DNA Center用のネットワークデバイスを作成する必要があるため、Addボタンをクリックします。

## 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

名前、説明、およびIPアドレス（またはアドレス）をCisco DNA Centerから設定します。その他の設定はすべてデフォルト値に設定されるため、このドキュメントの目的には必要ありません。

## 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"/> |

スクロールダウンして、RADIUS Authentication Settingsのチェックボックスをクリックしてイネーブルにし、共有秘密を設定します。



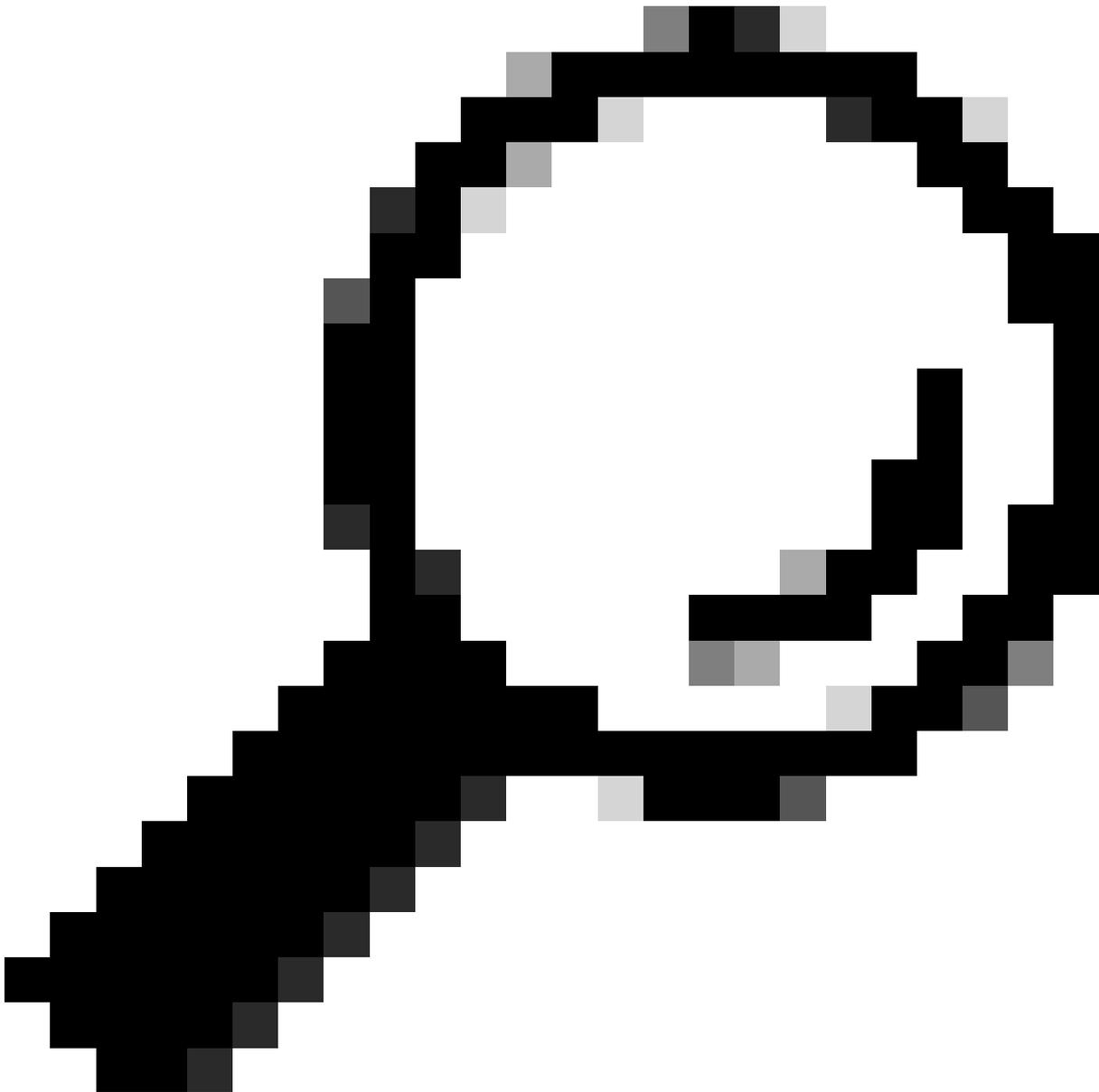
## ✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret .....

Show



ヒント：この共有秘密は後で必要になるので、他の場所に保存してください。

その後で、Submitをクリックします。

ステップ 3：ISEサーバで、Policy > Policy Elements > Resultsの順に移動し、認可プロファイルを作成します。

Authorization > Authorization Profilesの順に選択し、Addオプションを選択します。

The screenshot shows the Cisco ISE interface for Policy Elements > Results. The left sidebar has 'Authorization' selected, with 'Authorization Profiles' highlighted. 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 the table.

| <input type="checkbox"/> | Name                      | Profile | Description  |
|--------------------------|---------------------------|---------|--|
| <input type="checkbox"/> | APs_19.5.0                | Cisco   | 172_19_5_0-INFRA_VN  |
| <input type="checkbox"/> | AuthTemplate              | Cisco   |  |
| <input type="checkbox"/> | Blackhole_Wireless_Access | Cisco   | Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the |
| <input type="checkbox"/> | CY_CAMPUS_MAC             | Cisco   | CY_CAMPUS_MAC  |
| <input type="checkbox"/> | CY_Quart_profile          | Cisco   | CY_Quart_profile   |

Nameを設定し、Descriptionを追加して新しいプロファイルの記録を保存し、Access TypeがACCES\_ACCEPTに設定されていることを確認します。

The screenshot shows the 'New Authorization Profile' form in the Cisco ISE interface. The form fields are as follows:

- 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)

下にスクロールして、Advanced Attributes Settingsを設定します。

左側の列でcisco-av-pairオプションを検索して選択します。

右列の手動で「Role=SUPER-ADMIN-ROLE」と入力します。

次の図のように表示されたら、Submitをクリックします。

### Advanced Attributes Settings

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

### Attributes Details

Access Type = ACCESS\_ACCEPT

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

ステップ 4 : ISEサーバで、Work Centers > Profiler > Policy Setsの順に移動し、認証および認可ポリシーを設定します。

Defaultポリシーを特定し、青い矢印をクリックして設定します。

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 green checkmark in the 'Status' column. A blue arrow points from the 'Default' row to the 'View' button in the 'Actions' column. The table has the following data:

| 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 | ⚙️      | ➔    |

Default Policy Set内でAuthentication Policyを展開し、Defaultセクションの下でOptionsを展開して、これらが次の設定と一致していることを確認します。

Cisco ISE Work Centers - Profiler

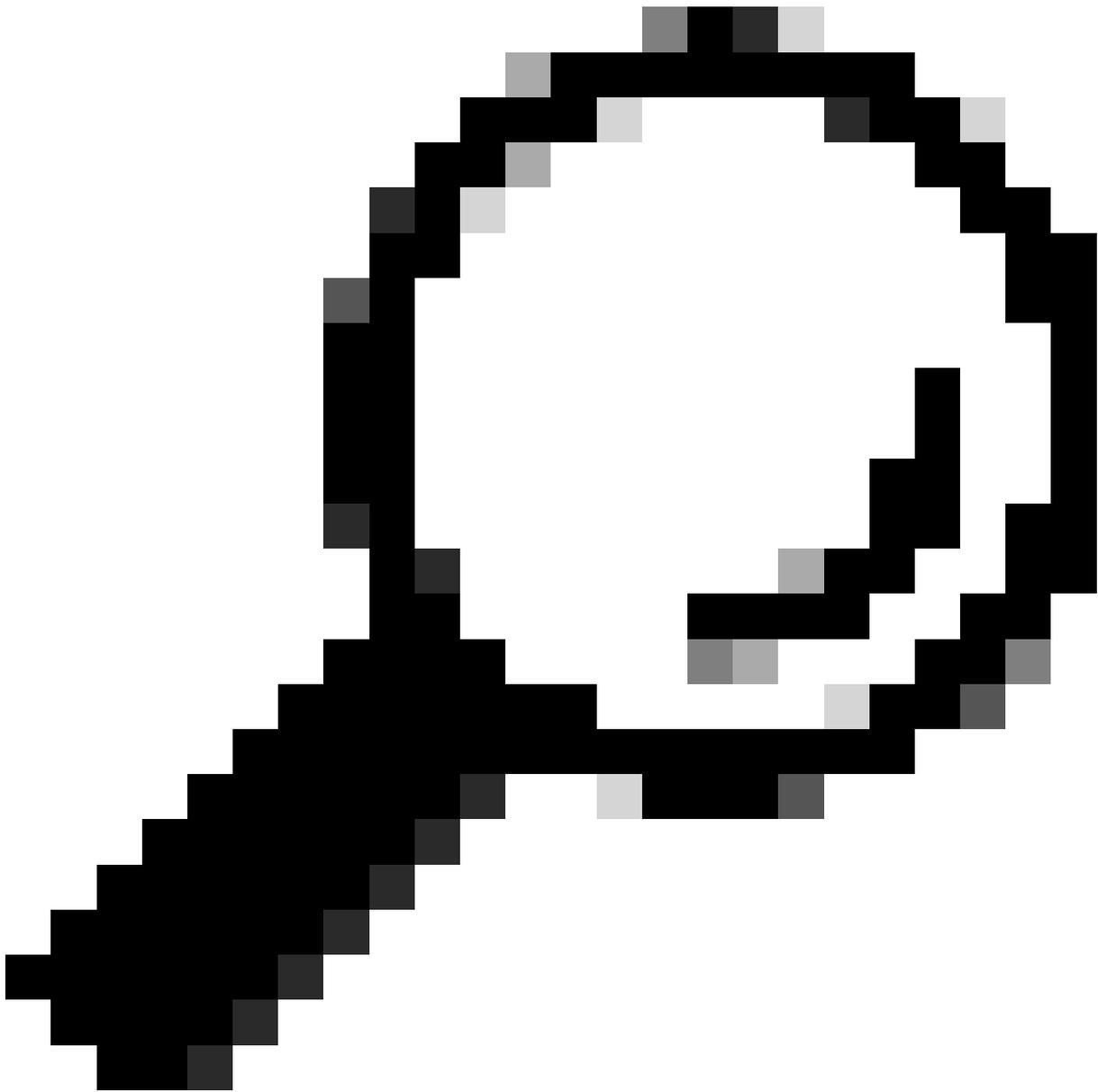
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

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<br>Wired_MAB<br>Wireless_MAB       | Internal Endpoints<br>> Options   | 4556  | ⚙️      |
| ✓      | Dot1X     | OR<br>Wired_802.1X<br>Wireless_802.1X | All_User_ID_Stores<br>> Options   | 0     | ⚙️      |
| ✓      | Default   |                                       | All_User_ID_Stores<br>Options<br>If Auth fail<br>REJECT<br>If User not found<br>REJECT<br>If Process fail<br>DROP | 62816 | ⚙️      |



ヒント:3つのオプションで設定されたREJECTも機能します

---

Default Policy Set内でAuthorization Policyを展開し、Addアイコンを選択して新しいAuthorization Conditionを作成します。

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 |      |         |
|   |        |           |            |          |                 |      |         |

ルール名を設定し、Addアイコンをクリックして条件を設定します。

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 < > + |      |         |

条件の一部として、ステップ2で設定したネットワークデバイスのIPアドレスに関連付けます。

# 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

[Save] をクリックします。

新しいLibrary Conditionとして保存し、必要に応じて名前を付けます。この場合は、DNACという名前です。



# 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

最後に、ステップ3で作成したプロファイルを設定します。

The screenshot shows the Cisco ISE GUI for the Profiler work center. The breadcrumb is 'Policy Sets → Default'. There are buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. A table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The 'Default' policy set is shown with a description of 'Default policy set' and 'Default Network Access' protocols, with 180617 hits. Below this, several authentication and authorization policies are listed. At the bottom, a detailed view of the 'DNAC-SUPER-ADMIN-ROLE' rule is shown, with a dropdown menu set to 'DNAC\_AUTH\_PROFILE' and a 'Select from list' button.

[Save] をクリックします。

ステップ 5 : Cisco DNA CenterのGUIにログインし、System > Users & Roles > External Authenticationの順に移動します。

Enable External Userオプションをクリックして、AAA AttributeをCisco-AVPairに設定します。

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".

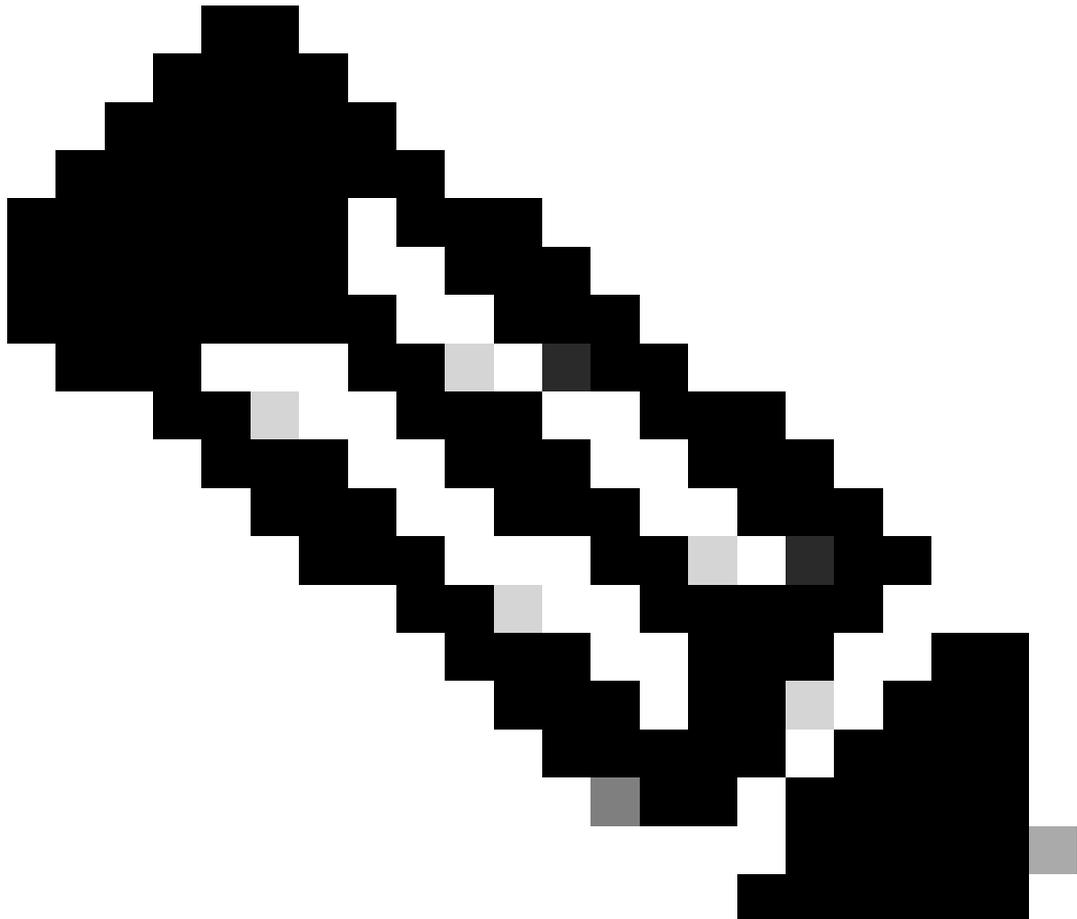
Enable External User ?

AAA Attribute

AAA Attribute  
Cisco-AVPair

Reset to Default

Update



注: ISEサーバはバックエンドで属性Cisco-AVPairを使用するため、ステップ3の設定は有

効です。

スクロールダウンして、「AAAサーバ」設定セクションを表示します。ステップ1でISEサーバからIPアドレスを設定し、ステップ3で設定した共有秘密を設定します。

次に、View Advanced Settingsをクリックします。

### AAA Server(s)

#### Primary AAA Server

IP Address

██████████



Shared Secret

.....

SHOW

Info

View Advanced Settings

Update

#### Secondary AAA Server

IP Address

██████████



Shared Secret

.....

SHOW

Info

View Advanced Settings

Update

RADIUSオプションが選択されていることを確認し、両方のサーバでUpdateボタンをクリックします。

▼ 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

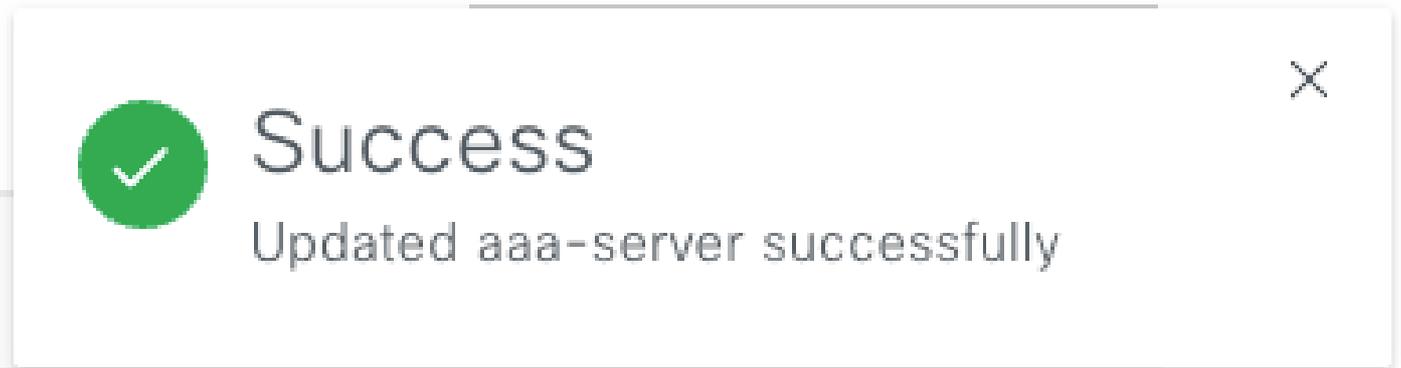
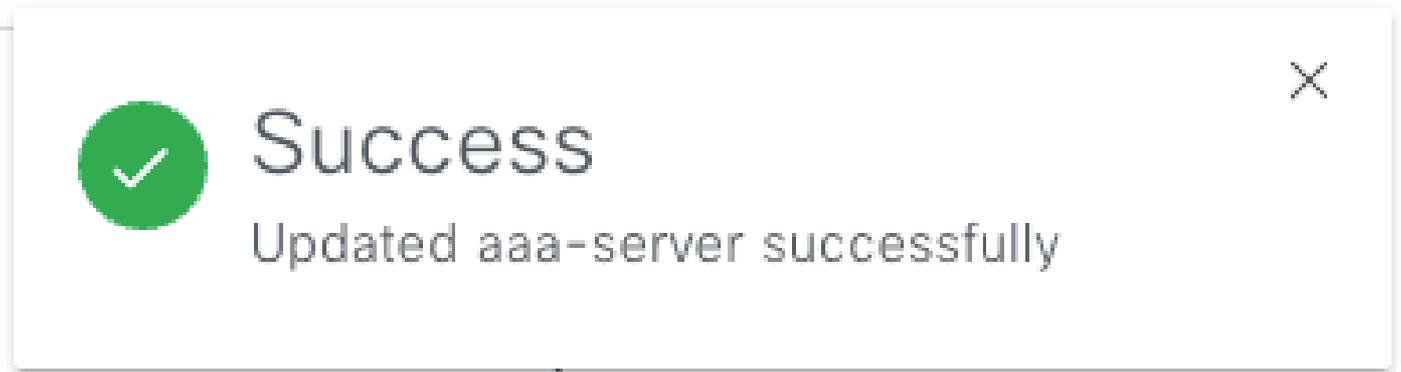
Timeout (seconds)

4

Update

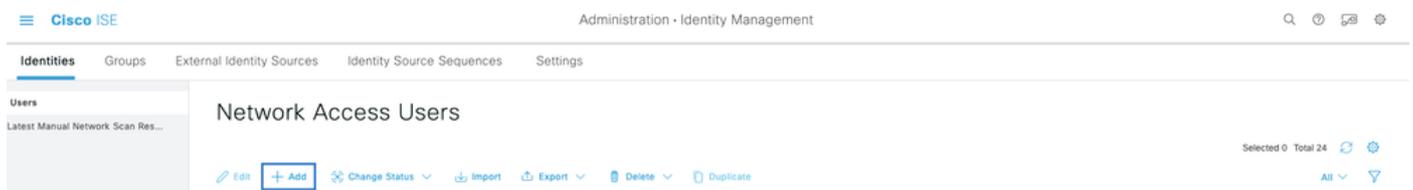
Update

それぞれの成功メッセージが表示されます。



これで、ISEメニュー> Administration > Identity Management > Identities > Usersで作成された任意のISE IDを使用してログインできるようになりました。

を作成していない場合は、ISEにログインし、上記のパスに移動して、新しいネットワークアクセスユーザを追加します。



## 確認

Cisco DNA Center GUIのロード ISE IDからユーザでログインします。



# Cisco DNA Center

The bridge to possible

✓ Success!

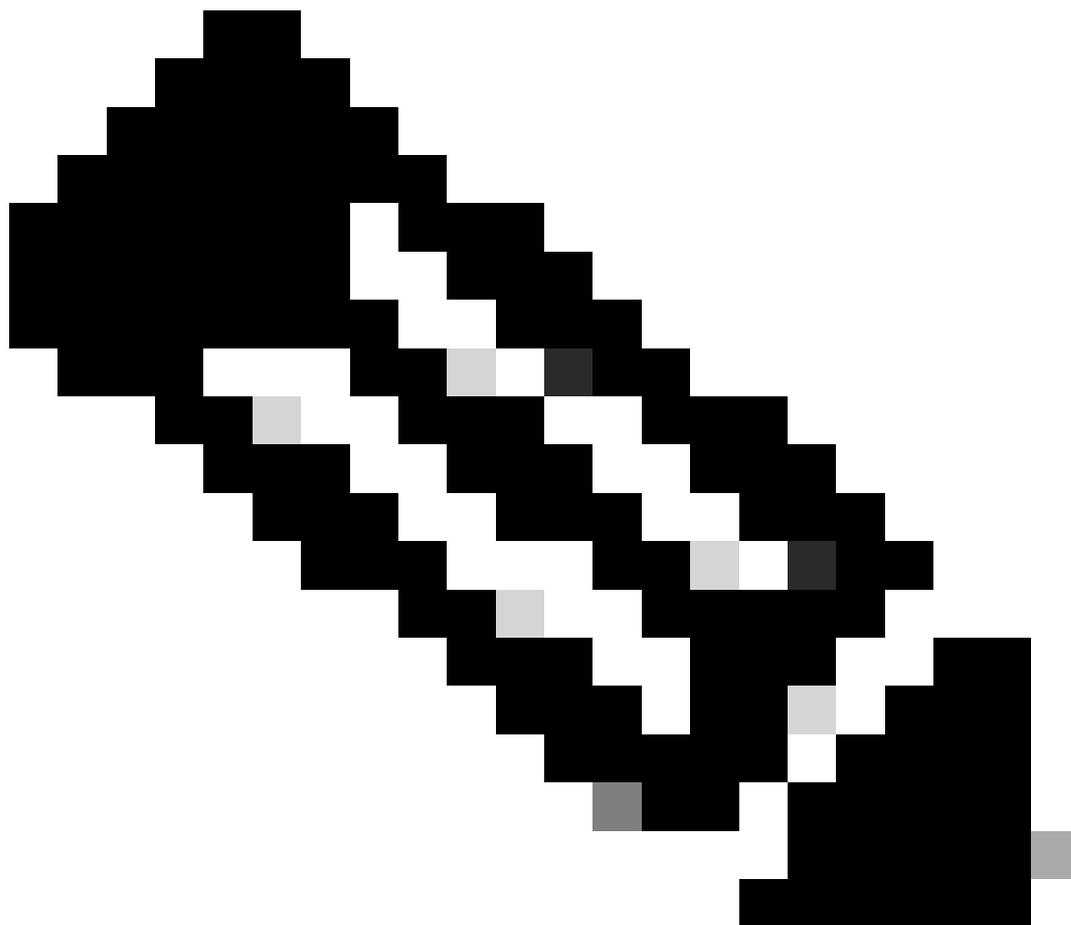
Username

test

Password

.....

Log In



注:ISE IDを持つすべてのユーザがログインできるようになりました。ISEサーバの認証ルールをより細かく設定できます。

---

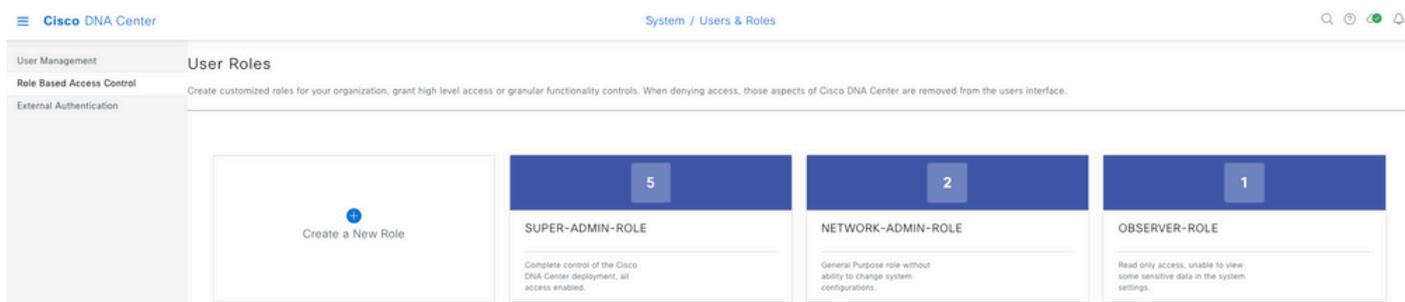
ログインが成功すると、ユーザ名がCisco DNA Center GUIに表示されます

## Welcome, test

ウェルカム画面

### その他のロール

Cisco DNA Centerのすべてのロールに対して、デフォルトでSUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE、およびOBSERVER-ROLEの手順を繰り返すことができます。



このドキュメントでは、SUPER-ADMIN-ROLEロールの例を使用しますが、ISEではCisco DNA Centerのすべてのロールに対して1つの認可プロファイルを設定できます。唯一の考慮事項は、ステップ3で設定したロールがCisco DNA Centerのロール名と正確に（大文字と小文字を区別して）一致する必要があることです。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。