

DNAC GUIの外部認証としてのISE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](#)

[はじめる前に](#)

[設定](#)

[\(オプション1\) RADIUSを使用したDNAC外部認証の設定](#)

[\(オプション1\) RADIUS用のISEの設定](#)

[\(オプション2\) TACACS+を使用したDNAC外部認証の設定](#)

[\(オプション2\) TACACS+用のISEの設定](#)

[確認](#)

[RADIUS設定の確認](#)

[TACACS+設定の確認](#)

[トラブルシューティング](#)

[参考資料](#)

はじめに

このドキュメントでは、Cisco DNA Center GUI管理の外部認証としてCisco Identity Services Engine(ISE)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。

- TACACS+およびRADIUSプロトコル。
- Cisco ISEとCisco DNA Centerの統合
- Cisco ISEポリシー評価

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 Identity Services Engine(ISE)バージョン3.4パッチ1。
- Cisco DNA Centerバージョン2.3.5.5

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。

はじめる前に

- System > Settings > External Services > Authentication and Policy Serversで、少なくとも1つのRADIUS認証サーバが設定されていることを確認します。
- DNACでSUPER-ADMIN-ROLE権限を持つユーザのみがこの手順を実行できます。
- 外部認証フォールバックを有効にします。

 注意:2.1.xより前のリリースでは、外部認証が有効な場合、AAAサーバに到達できないか、AAAサーバが未知のユーザ名を拒否すると、Cisco DNA Centerはローカルユーザにフォールバックします。現在のリリースでは、AAAサーバに到達できない場合、またはAAAサーバが未知のユーザ名を拒否した場合、Cisco DNA Centerはローカルユーザにフォールバックしません。外部認証フォールバックを有効にすると、外部ユーザとローカル管理者はCisco DNA Centerにログインできます。

外部認証フォールバックを有効にするには、Cisco DNA CenterインスタンスにSSHで接続し、次のCLIコマンドを入力します(magctl rbac external_auth_fallback enable)。

設定

(オプション1) RADIUSを使用したDNAC外部認証の設定

ステップ1: (オプション) カスタムロールを定義します。

要件を満たすカスタムロールを設定する代わりに、デフォルトのユーザロールを使用できます。これは、System > Users & Roles > Role Based Access Controlの順に選択することで実行できます。

手順

a.新しいロールを作成します。

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name*
DevOps-Role

Describe the role (optional)

2

Next

DevOpsロール名

b. アクセスを定義します。

Define the Access

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

1

Define the **DevOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

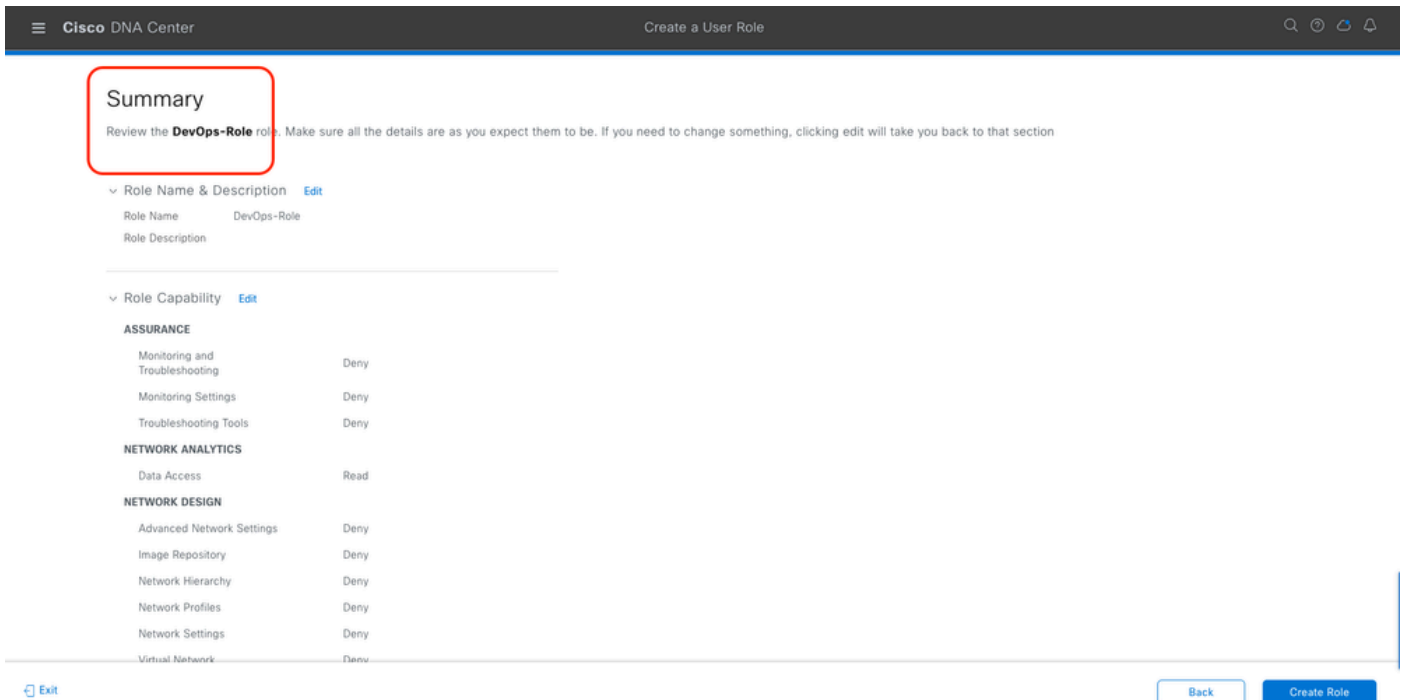
Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Manage and control secure access to the network.

2

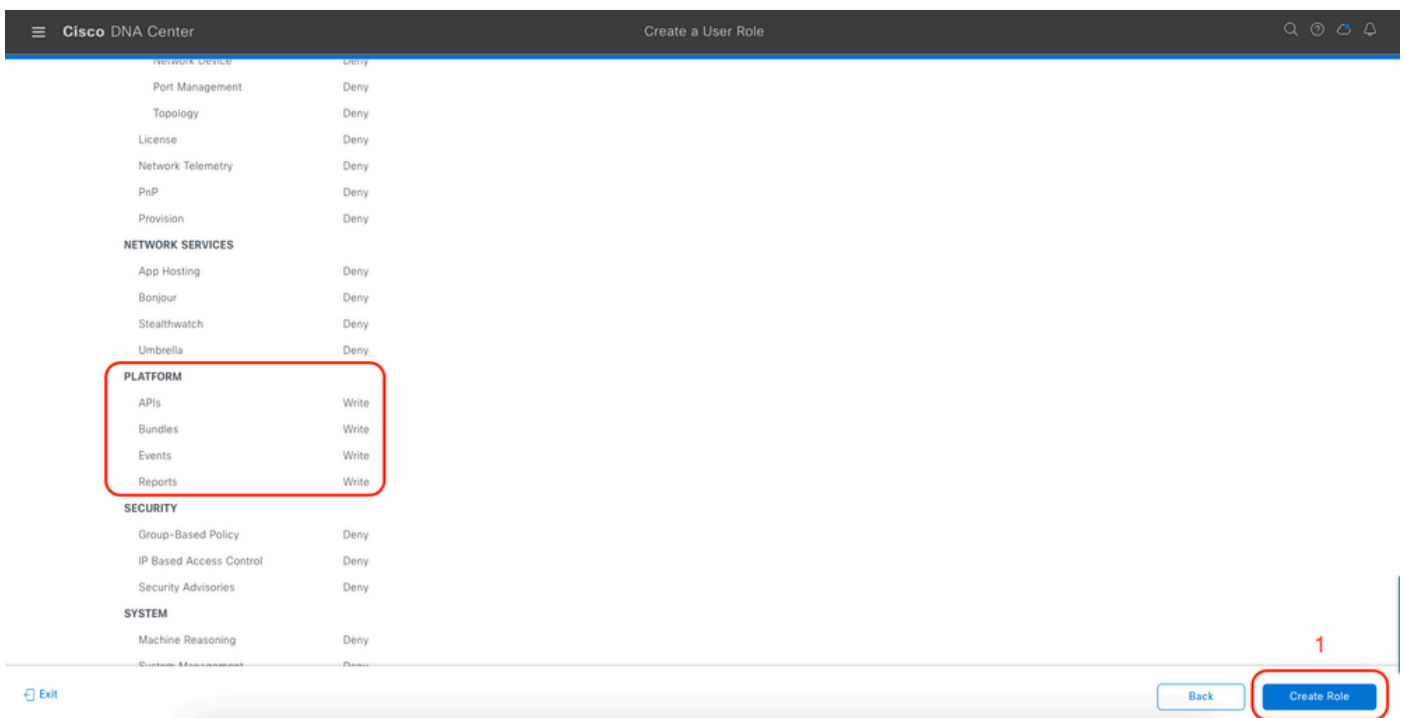
Next

DevOpsロールアクセス

c. 新しいロールを作成します。



DevOpsロールの概要



DevOpsロールのレビューと作成

ステップ 2 : RADIUSを使用して外部認証を設定する。

これは、System > Users & Roles > External Authenticationの順にタブから実行できます。

手順

a. Cisco DNA Centerで外部認証を有効にするには、Enable External Userチェックボックスにチェックマークを入れます。

b. AAA属性を設定します。

AAA attributesフィールドに、Cisco-AVPairと入力します。

c. (オプション) プライマリおよびセカンダリAAAサーバを設定します。

RADIUSプロトコルがプライマリAAAサーバで、少なくとも、またはプライマリとセカンダリの両方のサーバで有効になっていることを確認します。

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles'. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area is titled 'External Authentication' and contains the following configuration options:

- Enable External User:** A checkbox that is checked, highlighted with a red box and labeled 'a'.
- AAA Attribute:** A dropdown menu with 'Cisco-AVPair' selected, highlighted with a red box and labeled 'b'.
- AAA Server(s):** A section with two columns for 'Primary AAA Server' and 'Secondary AAA Server'. Both columns have 'IP Address' set to 'ISE Server 1 IP' and 'ISE Server 2 IP' respectively, and 'Authentication Port' set to '1812'. The 'RADIUS' protocol is selected for both, highlighted with a red box and labeled 'c'.

(RADIUS)外部認証の設定手順

(オプション1) RADIUS用のISEの設定

ステップ 1 : DNACサーバをISE上のネットワークデバイスとして追加します。

これは、タブAdministration > Network Resources > Network Devicesから実行できます。

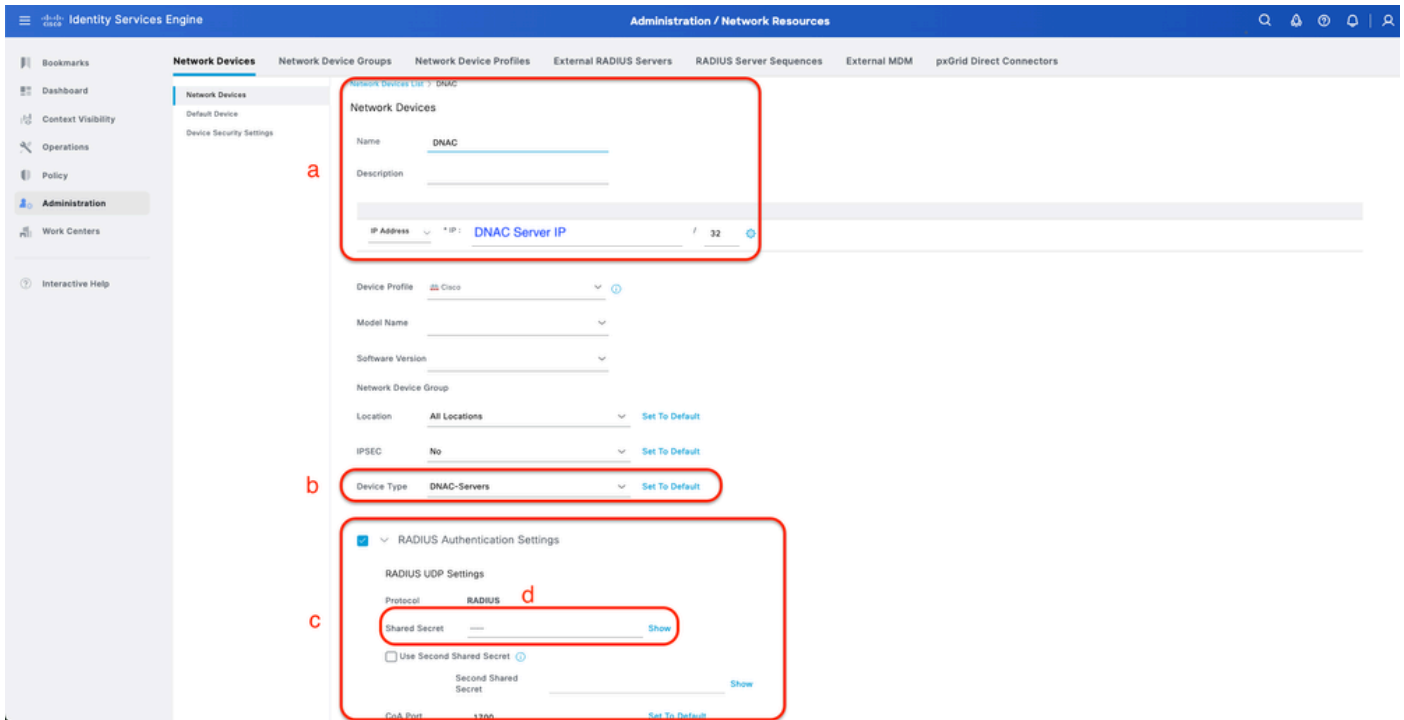
手順

a. (DNAC)ネットワークデバイス名とIPを定義します。

b. (オプション) ポリシーセット条件のデバイスタイプを分類します。

c. RADIUS認証設定を有効にします。

d. RADIUS共有秘密を設定します。



RADIUS用ISEネットワークデバイス(DNAC)

ステップ 2 : RADIUS認可プロファイルを作成します。

これは、タブから実行できます Policy > Policy Elements > Results > Authorization > 認可プロファイル。

 注 : 各ユーザーロールに1つずつ、3つのRADIUS認可プロファイルを作成します。

手順

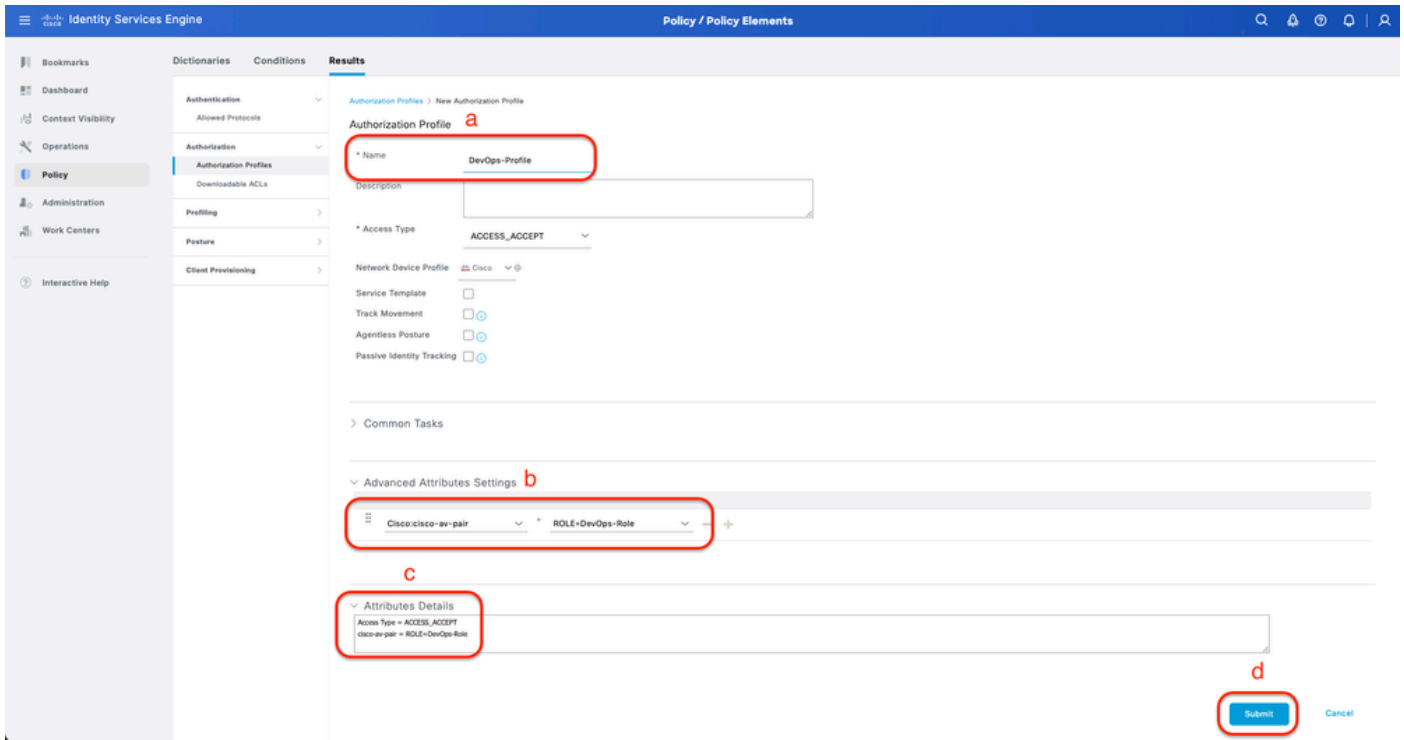
a. Addをクリックして、RADIUS許可プロファイル名を定義します。

b. Advanced Attributes SettingsでCisco:cisco-av-pairを入力し、正しいユーザーロールを入力します。

- (DecOps-Role)ユーザーロールに、ROLE=DevOps-Roleと入力します。
- (NETWORK-ADMIN-ROLE)ユーザーロールに、ROLE=NETWORK-ADMIN-ROLEと入力します。
- (SUPER-ADMIN-ROLE)ユーザーロールに、ROLE=SUPER-ADMIN-ROLEと入力します。

c. 属性の詳細を確認します。

d. Saveをクリックします。



認証プロファイルの作成

ステップ 3 : ユーザグループを作成します。

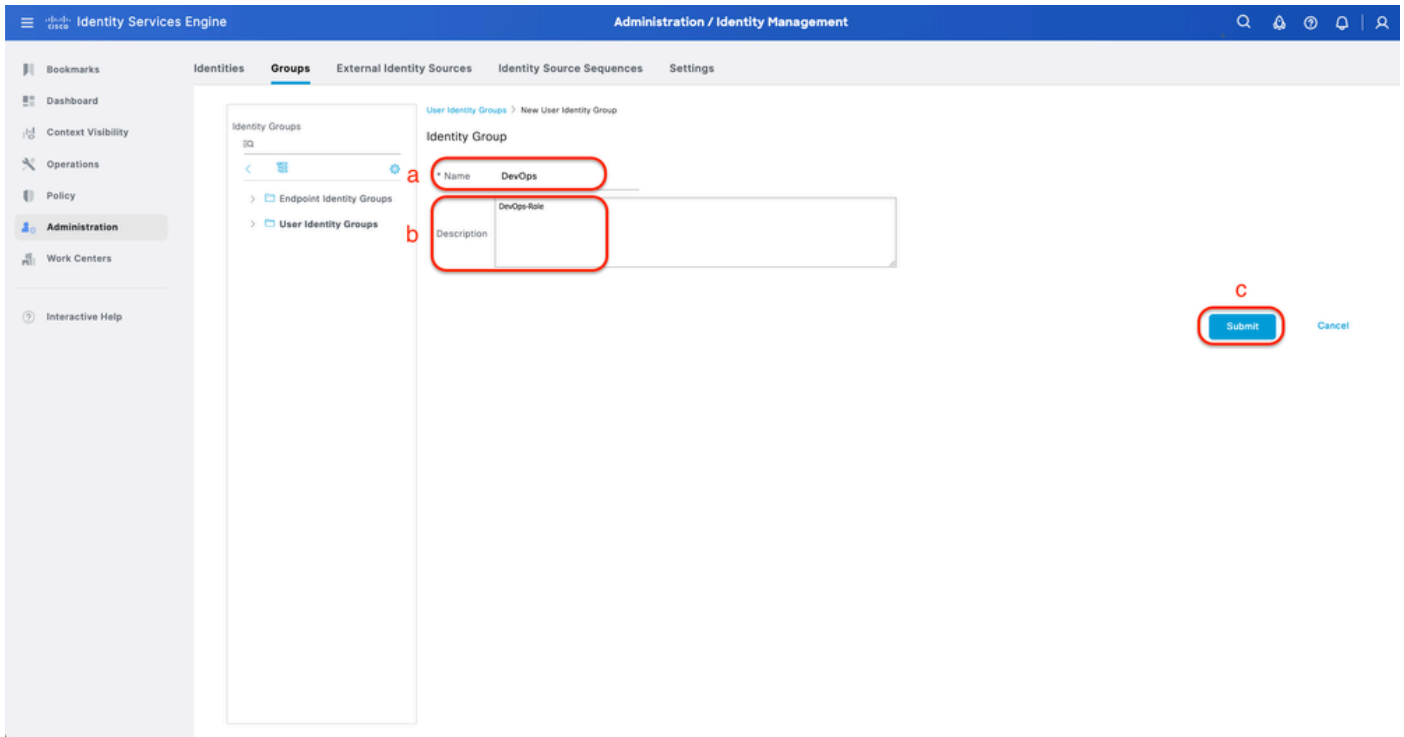
これは、タブ Administration > Identity Management > Groups > User Identity Groups から実行できます。

手順

a. Add をクリックして、ID グループ名を定義します

b. (オプション) 摘要を定義します。

c. Submit をクリックします。



ユーザIDグループの作成

ステップ 4 : ローカルユーザを作成します。

これは、タブ Administration > Identity Management > Identities > Users から実行できます。

手順

- a. Add をクリックして、ユーザ名を定義します。
- b. ログインパスワードを設定します。
- c. 関連するユーザグループにユーザを追加します。
- d. Submit をクリックします。

b. ポリシーセット名を定義します。

c. ポリシーセットConditionを、先ほど作成したSelect Device Type (ステップ1 > b) に設定します。

d. Allowedプロトコルを設定します。

e. Saveをクリックします。

f. (>) Policy Set Viewをクリックして、認証および認可ルールを設定します。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	DNAC - Policy		DEVICE Device Type EQUALS All Device Types@DNAC-Servers	Default Network Access	0	⚙️	>
●	Default	Default policy set		Default Network Access	0	⚙️	>

RADIUSポリシーセットの追加

手順 6 : RADIUS認証ポリシーを設定します。

これは、タブPolicy > Policy Sets > (>)をクリックすることで実行できます。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b. 認証ポリシー名を定義します。

c. 認証ポリシーの条件を設定し、前に作成したデバイスタイプを選択します (ステップ1 > b)。

d. アイデンティティソースの認証ポリシーUseを設定します。

e. Saveをクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main table displays the following information:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	DNAC - Policy		DEVICE Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0

Below this, the 'Authentication Policy(2)' section is expanded, showing a table of rules:

Status	Rule Name	Conditions	Use	Hits	Actions
●	DNAC - Authentication	DEVICE Device Type EQUALS All Device Types#DNAC-Servers	Internal Users	0	⚙️
●	Default		All_User_ID_Stores	2	⚙️

Red annotations in the image point to: 'b' (Rule Name), 'c' (Condition), 'd' (Use dropdown), and 'e' (Save button).

RADIUS認証ポリシーの追加

手順 7 : RADIUS許可ポリシーを設定します。

これは、タブPolicy > Policy Sets> Click (>)から実行できます。

各ユーザの役割の許可ポリシーを作成するには、次の手順を実行します。

- スーパー管理者ロール
- ネットワーク管理者ロール
- DevOpsロール

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.許可ポリシー名を定義します。

c.許可ポリシー条件を設定し、(ステップ3)で作成したユーザグループを選択します。

d.許可ポリシーの結果/プロファイルを設定し、(ステップ2)で作成した許可プロファイルを選択します。

e. Saveをクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a policy set. The main table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, a detailed view of a policy rule is shown with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. Red boxes and letters 'a' through 'e' highlight specific elements: 'a' is a gear icon for configuration, 'b' is the rule name, 'c' is the condition, 'd' is the profile selection, and 'e' is the 'Save' button.

許可ポリシーの追加

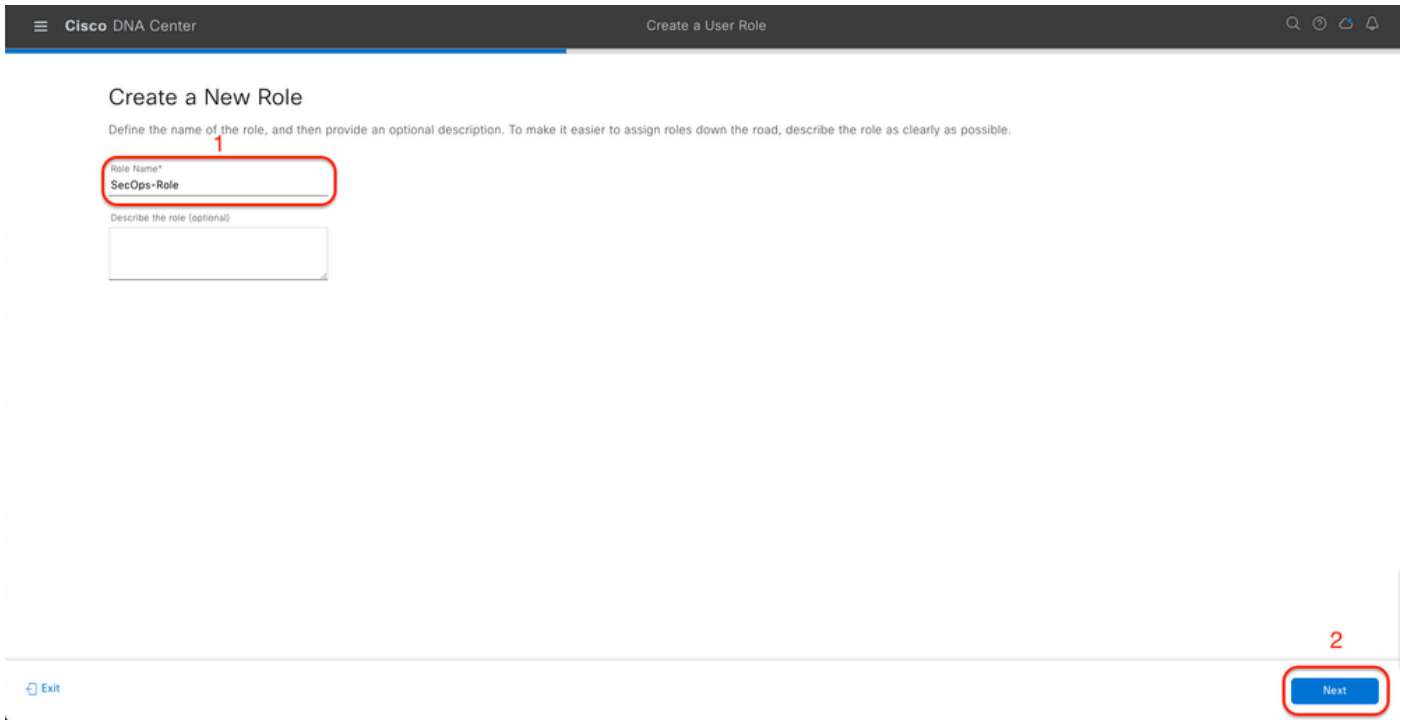
(オプション2) TACACS+を使用したDNAC外部認証の設定

ステップ1: (オプション) カスタムロールを定義します。

要件を満たすカスタムロールを設定する代わりに、デフォルトのユーザロールを使用できます。これは、System > Users & Roles > Role Based Access Controlの順に選択することで実行できます。

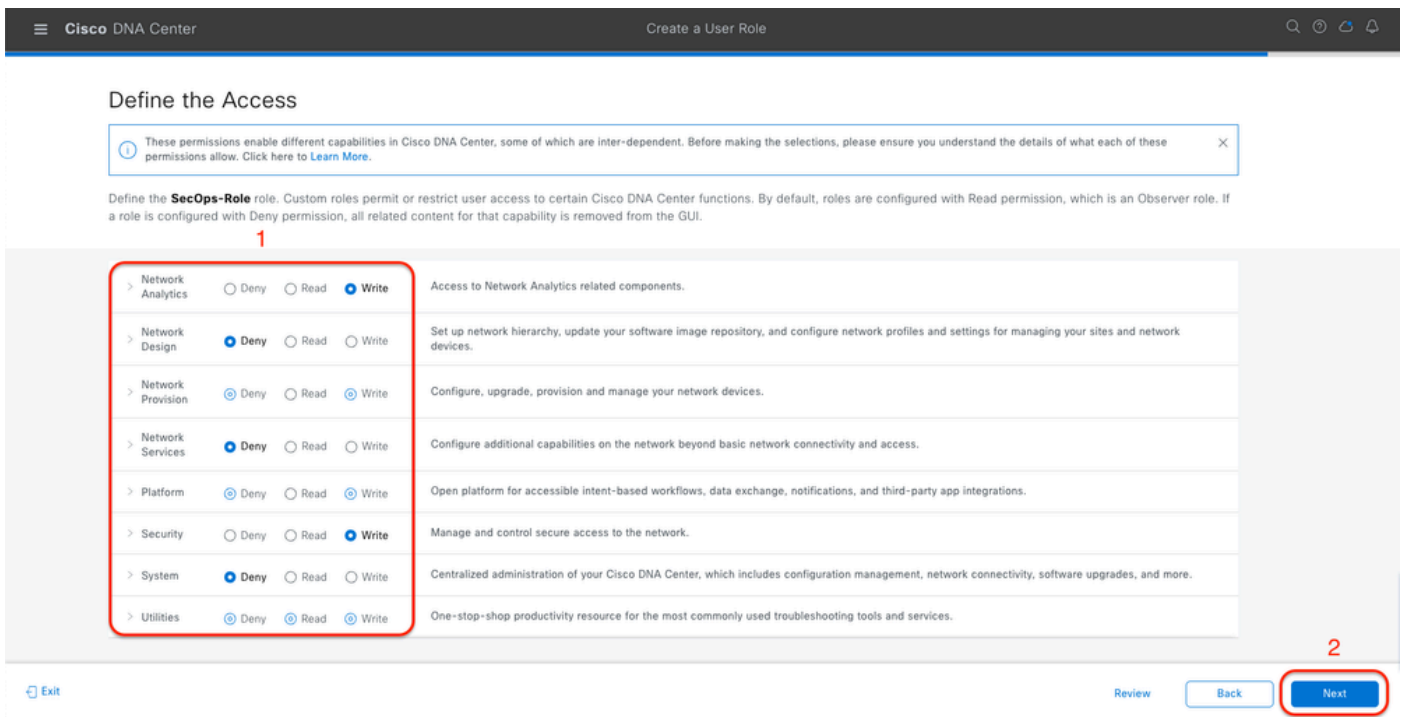
手順

a.新しいロールを作成します。



SecOpsロール名

b. アクセスを定義します。



SecOpsロールアクセス

c. 新しいロールを作成します。

Cisco DNA Center Create a User Role

Summary
Review the **SecOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section.

Role Name & Description [Edit](#)

Role Name	SecOps-Role
Role Description	

Role Capability [Edit](#)

ASSURANCE

Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny

NETWORK ANALYTICS

Data Access	Write
-------------	-------

NETWORK DESIGN

Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

[Exit](#) [Back](#) [Create Role](#)

SecOpsロールの概要

Cisco DNA Center Create a User Role

PnP	Deny
Provision	Deny

NETWORK SERVICES

App Hosting	Deny
Bonjour	Deny
Stealthwatch	Deny
Umbrella	Deny

PLATFORM

APIs	Write
Bundles	Deny
Events	Deny
Reports	Deny

SECURITY

Group-Based Policy	Write
IP Based Access Control	Write
Security Advisories	Write

SYSTEM

Machine Reasoning	Deny
System Management	Deny

UTILITIES

Audit Log	Deny
Event Viewer	Read
Network Reasoner	Read

[Exit](#) [Back](#) [Create Role](#) 1

SecOpsロールのレビューと作成

ステップ 2 : TACACS+を使用して外部認証を設定する。

これは、System > Users & Roles > External Authenticationの順にタブから実行できます。

a. Cisco DNA Centerで外部認証を有効にするには、Enable External Userチェックボックスにチェックマークを入れます。

b. AAA属性を設定します。

AAA attributesフィールドに、Cisco-AVPairと入力します。

c. (オプション) プライマリおよびセカンダリAAAサーバを設定します。

TACACS+プロトコルがプライマリAAAサーバで、少なくとも、またはプライマリとセカンダリの両方のサーバで有効になっていることを確認します。

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles'. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area is titled 'External Authentication' and contains the following sections:

- Enable External User:** A checkbox labeled 'Enable External User' is checked and circled in red with the letter 'a' next to it.
- AAA Attribute:** A dropdown menu labeled 'AAA Attribute' is set to 'Cisco-AVPair' and circled in red with the letter 'b' next to it.
- AAA Server(s):** A section containing two columns for 'Primary AAA Server' and 'Secondary AAA Server'. Both are set to 'ISE Server 1 IP' and 'ISE Server 2 IP' respectively. The 'Shared Secret' is masked with '*****'. The protocol is set to 'TACACS+' (selected with a radio button) and the port is '49'. This entire section is circled in red with the letter 'c' next to it.

(TACACS+)外部認証の設定手順

(オプション2) TACACS+用のISEの設定

ステップ 1 : Enable Device Admin Service.

これは、タブAdministration > System > Deployment > Edit (ISE PSN Node) > Check Enable Device Admin Serviceから実行できます。

The screenshot shows the 'Administration / System' page in Identity Services Engine. The 'Deployment' tab is active, showing various services and their status:

- Administration:** Enabled (checkbox checked).
- Monitoring:** Enabled (checkbox checked). Role is set to 'PRIMARY'. Other Monitoring Node is empty. Dedicated MNT is unchecked.
- Policy Service:** Enabled (checkbox checked).
 - Enable Session Services: Checked (checkbox checked).
 - Include Node in Node Group: None (dropdown).
 - Enable Profiling Service: Checked (checkbox checked).
 - Enable Threat Centric NAC Service: Unchecked (checkbox).
 - Enable SXP Service: Unchecked (checkbox).
 - Enable Device Admin Service:** Checked (checkbox checked) and circled in red with the number '1' next to it.
 - Enable Passive Identity Service: Unchecked (checkbox).
- pxGrid:** Enabled (checkbox checked).
 - Enable pxGrid Cloud: Unchecked (checkbox).

At the bottom right, the 'Save' button is circled in red with the number '2' next to it.

[デバイス管理サービスを有効にする (Enable Device Admin Service)]

ステップ 2 : DNACサーバをISE上のネットワークデバイスとして追加します。

これは、タブAdministration > Network Resources > Network Devicesから実行できます。

手順


- (DNAC)ネットワークデバイス名とIPを定義します。
- (オプション) ポリシーセット条件のデバイスタイプを分類します。
- TACACS+認証設定を有効にします。
- TACACS+共有秘密を設定します。

The screenshot shows the 'Network Devices' configuration page in the ISE Administration console. The page title is 'Administration / Network Resources'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'Network Devices' and shows a form for configuring a device. The form includes fields for Name (DNAC), Description, IP Address (DNAC Server IP), Device Profile (Cisco), Model Name, Software Version, Network Device Group, Location (All Locations), and IPSEC (No). The 'Device Type' dropdown is set to 'DNAC-Servers'. The 'TACACS Authentication Settings' section is expanded, showing a 'Shared Secret' field and a 'Retire' button. The 'SNMP Settings' section is collapsed.

TACACS+用ISEネットワークデバイス(DNAC)

ステップ 3 : 各DNACロールのTACACS+プロファイルを作成します。


これは、タブWork Centers > Device Administration > Policy Elements > Results > TACACS Profilesから実行できます。

 注 : ユーザロールごとに1つずつ、3つのTACACS+プロファイルを作成します。

手順

- Addをクリックして、TACACS Profileの名前を定義します。
- Raw Viewタブをクリックします。
- Cisco-AVPair=ROLE=と入力し、正しいユーザロールを入力します。
 - (SecOps-Role)ユーザロールに、Cisco-AVPair=ROLE=SecOps-Roleと入力します。

- (NETWORK-ADMIN-ROLE)ユーザロールに、Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLEと入力します。
- (SUPER-ADMIN-ROLE)ユーザロールに、Cisco-AVPair=ROLE=SUPER-ADMIN-ROLEと入力します。

 注:AVPair値(Cisco-AVPair=ROLE=)は大文字と小文字が区別されることを覚えておき、DNACユーザロールに一致していることを確認してください。

d. Saveをクリックします。

TACACSプロファイルの作成(SecOps_Role)

ステップ 4 : ユーザグループを作成します。

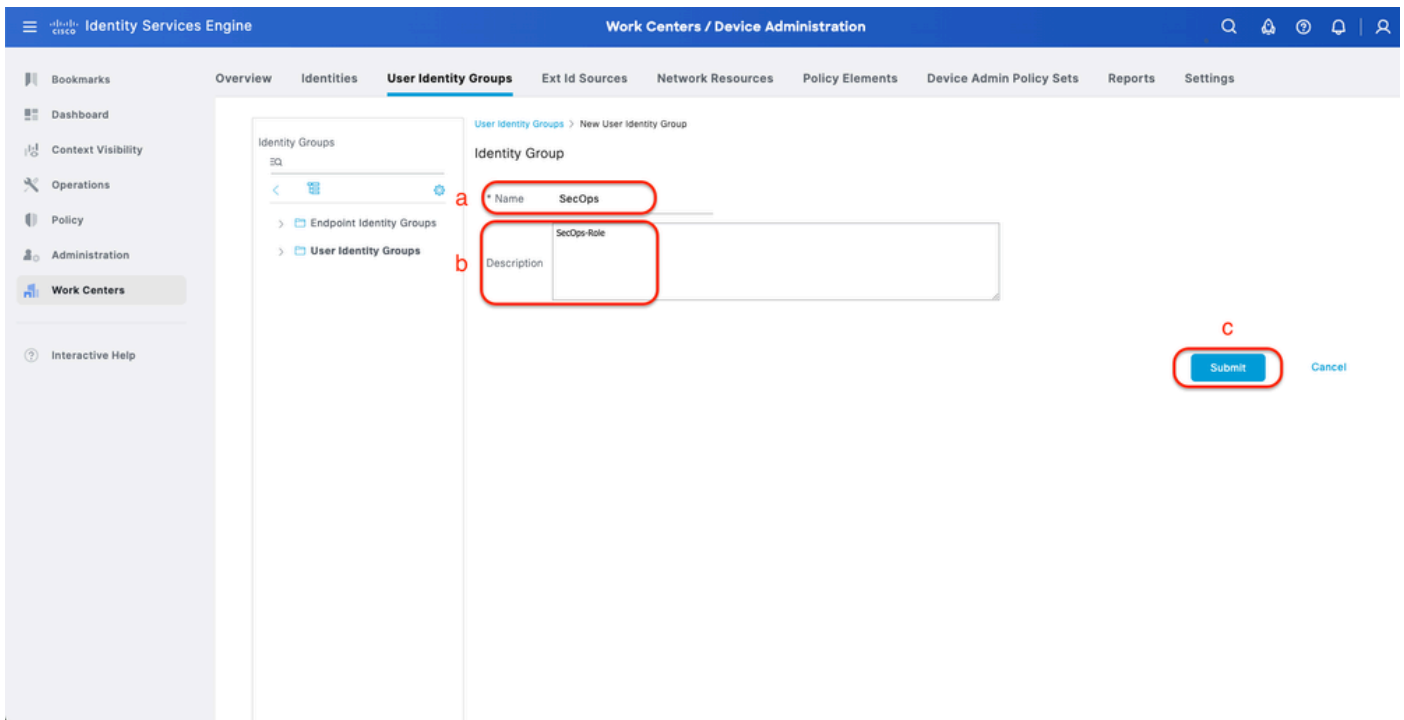
これは、タブWork Centers > Device Administration > User Identity Groupsから実行できます。

手順

a. Addをクリックして、IDグループ名を定義します。

b. (オプション) 摘要を定義します。

c. Submitをクリックします。



ユーザIDグループの作成

ステップ 5 : ローカルユーザを作成します。

これは、タブWork Centers > Device Administration > Identities > Usersから実行できます。

手順

- a. Addをクリックして、ユーザ名を定義します。
- b. ログインパスワードを設定します。
- c. 関連するユーザグループにユーザを追加します。
- d. Submitをクリックします。

ローカルユーザの作成1-2

ローカルユーザの作成2-2

ステップ6: (オプション) TACACS+ポリシーセットを追加します。

これは、タブWork Centers > Device Administration > Device Admin Policy Setsから実行できます。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

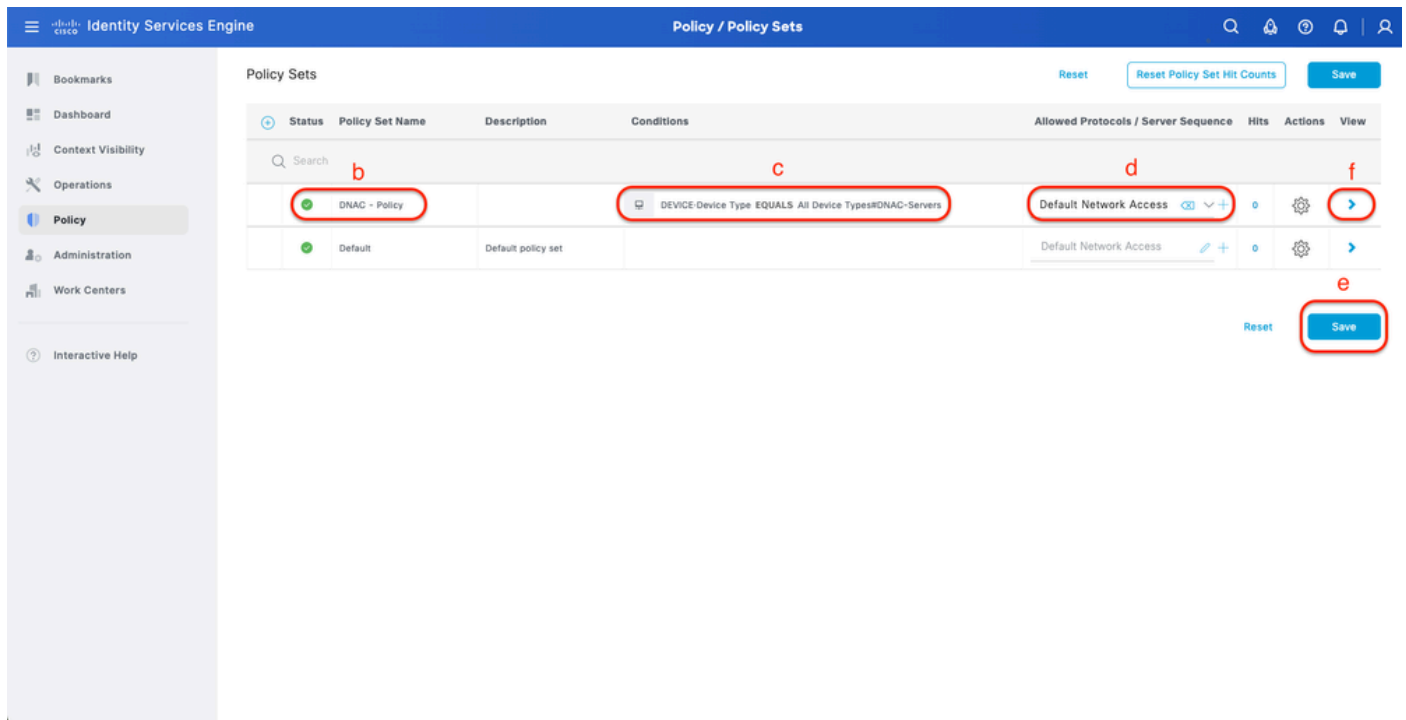
b. ポリシーセット名を定義します。

c. ポリシーセットConditionを、先ほど作成したSelect Device Type (ステップ2 > b) に設定します。

d. Allowedプロトコルを設定します。

e. Saveをクリックします。

f. (>) Policy Set Viewをクリックして、認証および認可ルールを設定します。



TACACS+ポリシーセットの追加

手順 7 : TACACS+認証ポリシーを設定します。

これを行うには、タブWork Centers > Device Administration > Device Admin Policy Sets >(>) をクリックします。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b. 認証ポリシー名を定義します。

c. 認証ポリシーの条件を設定し、前に作成したデバイスタイプを選択します (ステップ2 > b)。

d. アイデンティティソースの認証ポリシーUseを設定します。

e. Saveをクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Work Centers / Device Administration'. The left sidebar contains 'Work Centers'. The main content area is titled 'Policy Sets -> DNAC - Policy'. It features a table with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, there is a section for 'Authentication Policy(2)' with a table for Status, Rule Name, Conditions, Use, Hits, and Actions. The 'DNAC - Authentication' rule is highlighted with a red box labeled 'b'. Its condition is 'DEVICE-Device Type EQUALS All Device Types#DNAC-Servers', highlighted with a red box labeled 'c'. The 'Use' column for this rule shows 'Internal Users', highlighted with a red box labeled 'd'. A red box labeled 'a' highlights the 'Save' button in the top right corner.

TACACS+認証ポリシーの追加

ステップ 8 : TACACS+認可ポリシーを設定します。

これを行うには、タブWork Centers > Device Administration > Device Admin Policy Sets >(>)の順にクリックします。

各ユーザの役割の許可ポリシーを作成するには、次の手順を実行します。

- スーパー管理者ロール
- ネットワーク管理者ロール
- SecOpsロール

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.許可ポリシー名を定義します。

c.許可ポリシー条件を設定し、(ステップ4)で作成したユーザグループを選択します。

d. (ステップ3)で作成した認可ポリシーシェルフファイルと選択 TACACSプロファイルを設定します。

e. Saveをクリックします。

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Search

DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC Default Device Admin

> Authentication Policy(2)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
v Authorization Policy(1)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
+	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE	0	+
+	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE	0	+
+	SecOps	IdentityGroup-Name EQUALS User Identity Groups:SecOps	Select from list	SecOps_Role	0	+
+	Default		DenyAllCommands	Deny All Shell Profile	0	+

Reset Save

許可ポリシーの追加

確認

RADIUS設定の確認

1- DNAC – 外部ユーザの表示システム>ユーザとロール>外部認証>外部ユーザ
RADIUSから初めてログインした外部ユーザのリストを表示できます。表示される情報には、ユーザ名とロールが含まれます。

Cisco DNA Center System / Users & Roles

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 delete AAA Servers. The AAA Attribute here 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 chooses to change it to any other AAA attribute, 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=role!". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA 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
Cisco-AVPair

Reset to Default Update

AAA Server(s)

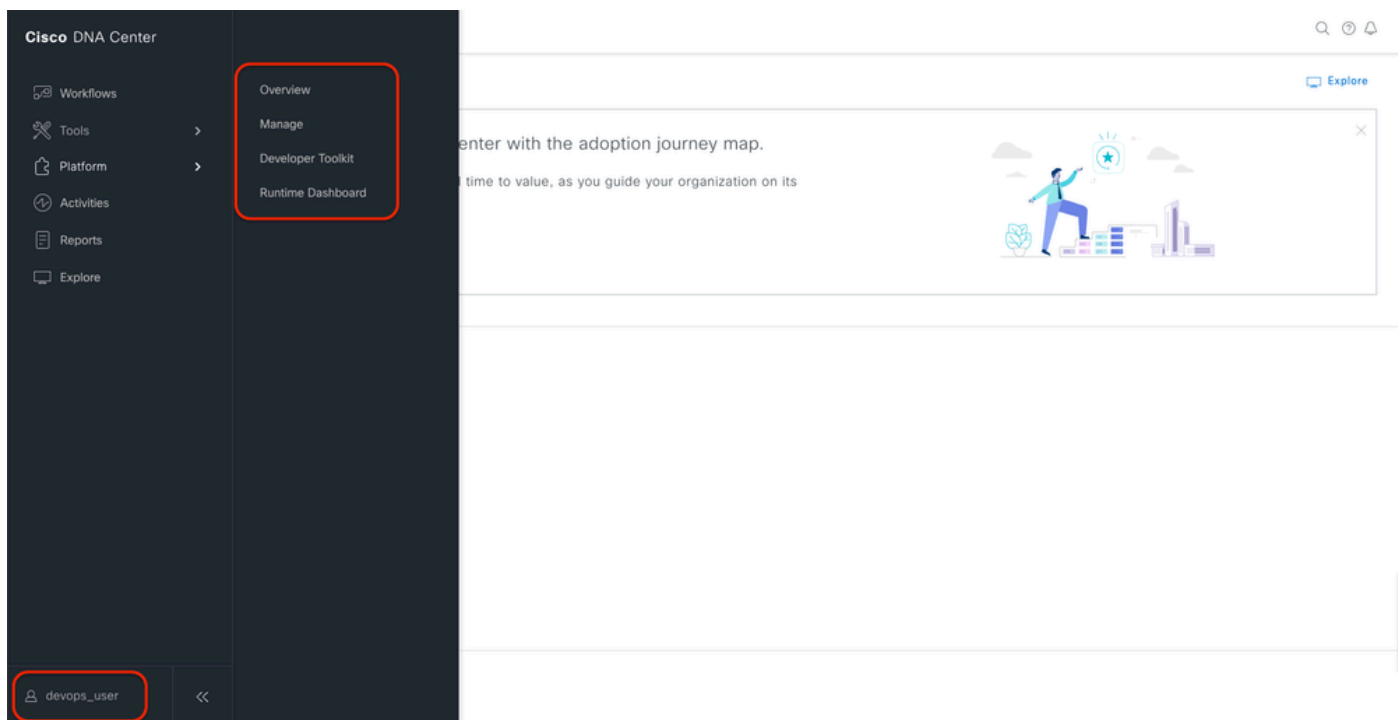
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

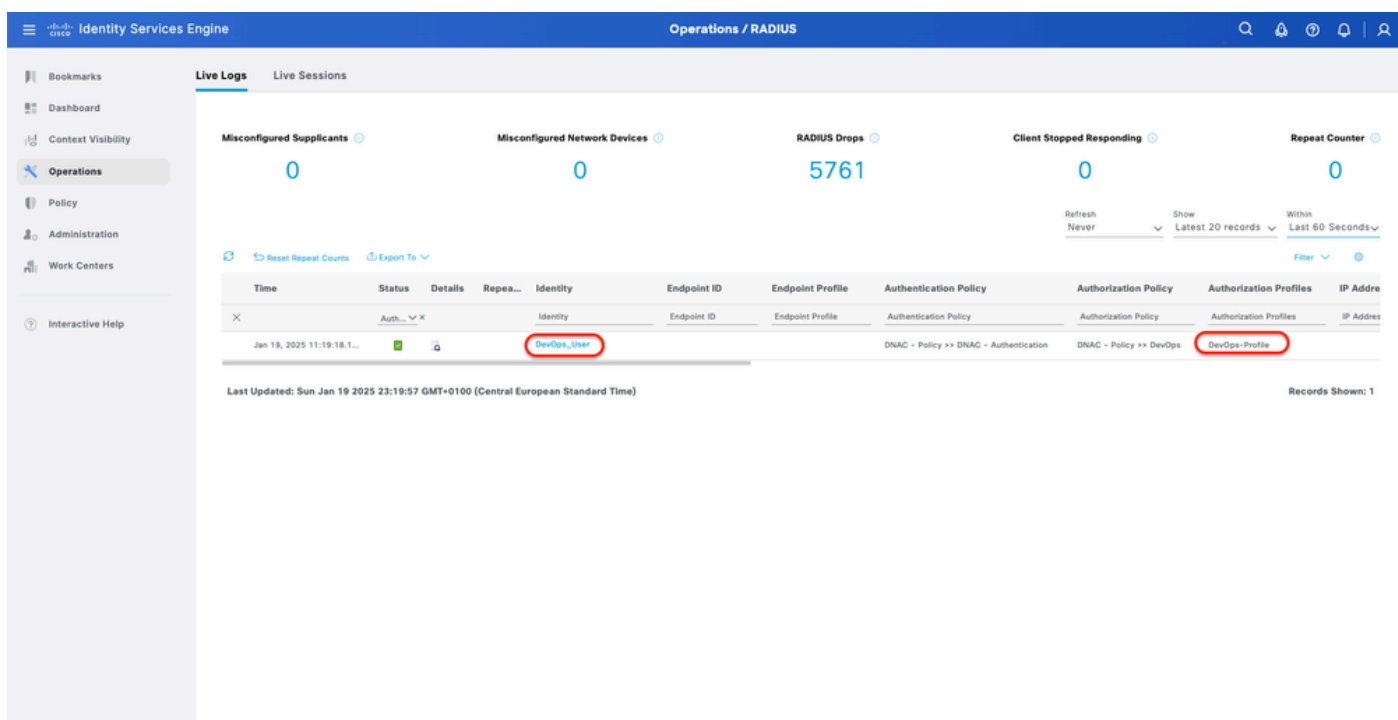
外部ユーザ

2. DNAC – ユーザアクセスを確認します。



制限付きユーザアクセス

3.a ISE:RADIUSライブログ操作> RADIUS >ライブログ。



RADIUSライブログ

3.b ISE:RADIUSライブログ操作> RADIUS >ライブログ>認証ログの (詳細) をクリックします。

Cisco ISE

Overview

Event: 5200 Authentication succeeded

Username: DevOps_User

Endpoint Id:

Endpoint Profile:

Authentication Policy: DNAC - Policy >> DNAC - Authentication

Authorization Policy: DNAC - Policy >> DevOps

Authorization Result: DevOps-Profile

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
22037	Authentication Passed	1
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

Authentication Details

Source Timestamp: 2025-01-19 23:19:18.156

Received Timestamp: 2025-01-19 23:19:18.156

Policy Server: ise34

Event: 5200 Authentication succeeded

Username: DevOps_User

User Type: User

Authentication Identity Store: Internal Users

Identity Group: User Identity Groups:DevOps

Authentication Method: PAP_ASCII

Authentication Protocol: PAP_ASCII

Network Device: DNAC

Device Type: All Device Types#DNAC-Servers

Location: All Locations

RADIUS詳細ライブログ1-2

Cisco ISE

IdentityPolicyMatchedRule: DNAC - Authentication

AuthorizationPolicyMatchedRule: DevOps

ISEPolicySetName: DNAC - Policy

IdentitySelectionMatchedRule: DNAC - Authentication

TotalAuthnLatency: 35

ClientLatency: 0

DTLSSupport: Unknown

Network Device Profile: Cisco

Location: Location#All Locations

Device Type: Device Type#All Device Types#DNAC-Servers

IPSEC: IPSEC#Is IPSEC Device#No

Name: User Identity Groups:DevOps

EnableFlag: Enabled

RADIUS Username: DevOps_User

Device IP Address:

CPMSessionID: 0a301105095d4kCbV7kMBCoFkesRrFcdXec0uEqPP8RtG/WY

CiscoAVPair: AuthenticationIdentityStore=Internal Users, FQSubjectName=92731e30-8c01-11e6-996c-525400b48521#devops_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5ea5dedf467

Result

Class: CACS:0a301105095d4kCbV7kMBCoFkesRrFcdXec0uEqPP8RtG/WY:ise34/528427220/15433

Cisco-av-pair: ROLE=DevOps-Role

RADIUS詳細ライブログ2-2

TACACS+設定の確認

1- DNAC – 外部ユーザの表示システム>ユーザとロール>外部認証>外部ユーザ
 TACACS+から初めてログインした外部ユーザのリストを表示できます。表示される情報には、ユーザ名とロールが含まれます。

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

Primary AAA Server Secondary AAA Server

IP Address IP Address

Shared Secret Shared Secret

View Advanced Settings View Advanced Settings

Update Update

External Users

Filter

Username	Role	Action
secops_user	SecOps-Role	Delete

Showing 1 of 1

外部ユーザ

2. DNAC – ユーザアクセスを確認します。

Cisco DNA Center

Policy >
Workflows >
Tools >
Platform >
Activities >
Explore

Group-Based Access Control
IP & URL Based Access Control

Network Bug Identifier
Identify bugs in the network

secops_user

制限付きユーザアクセス

3.a ISE:TACACS+ライブログワークセンター>デバイス管理>概要> TACACS LiveLog。

Identity Services Engine Operations / TACACS

Live Logs

Refresh Never Show Latest 20 records Within Last 60 Seconds

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#AII Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#AII Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 2

TACACSライブログ

3.b ISE : 詳細なTACACS+ライブログワークセンター>デバイス管理>概要> TACACS Livelog > (詳細) をクリックして認証ログを表示します。

Cisco ISE

Overview

Request Type: Authorization
 Status: Pass
 Session Key: ise34/526427220/13958
 Message Text: Device-Administration: Session Authorization succeeded
 Username: SecOps_User
 Authorization Policy: DNAC - Policy >> SecOps
 Shell Profile: SecOps_Role
 Matched Command Set
 Command From Device

Authorization Details

Generated Time: 2025-01-19 17:12:43.368 +1:00
 Logged Time: 2025-01-19 17:12:43.368
 Epoch Time (sec): 1737303163
 ISE Node: ise34
 Message Text: Device-Administration: Session Authorization succeeded
 Failure Reason
 Resolution
 Root Cause
 Username: SecOps_User
 Network Device Name: DNAC

Steps

Step ID	Description	Latency (ms)
13005	Received TACACS+ Authorization Request	
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	4
15041	Evaluating Identity Policy	7
15013	Selected Identity Source - Internal Users	5
24210	Looking up User in Internal Users IDStore	1
24212	Found User in Internal Users IDStore	4
22037	Authentication Passed	0
15036	Evaluating Authorization Policy	0
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
15017	Selected Shell Profile	2
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	0
13034	Returned TACACS+ Authorization Reply	0

TACACS+の詳細なライブログ1-2

Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;13=1;14=0;15=0
TotalAuthenLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco-AVPair=ROLE+SecOps-Role; }

TACACS+の詳細なライブログ2-2

トラブルシューティング

現在のところ、この設定に関する特定の診断情報はありません。

参考資料

- [Cisco Identity Services Engine管理者ガイドリリース3.4 >デバイス管理](#)
- [Cisco DNA Center管理者ガイド、リリース2.3.5](#)
- [Cisco DNA Center：外部認証によるロールベースアクセスコントロール](#)

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。