

ISE 3.2およびWindowsの有線Dot1xの問題のトラブルシューティング

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](#)

[ネットワーク図](#)

はじめに

このドキュメントでは、Identity Services Engine(ISE)3.2およびWindowsネイティブサブリカント用の基本的な802.1X PEAP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。

- Protected Extensible Authentication Protocol (PEAP)
- PEAP 802.1x

使用するコンポーネント

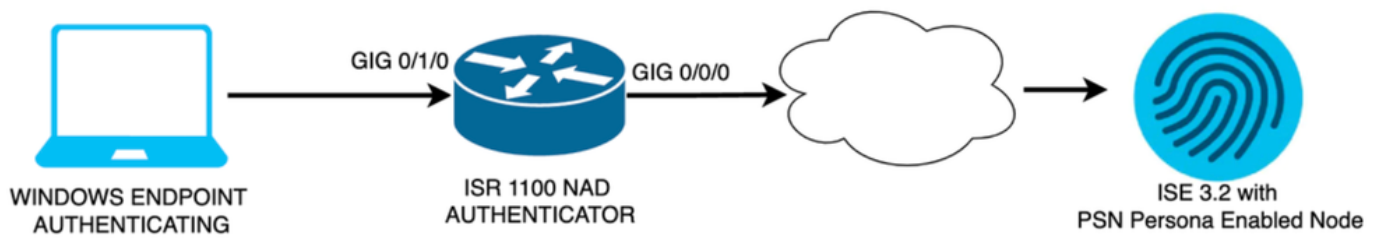
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine(ISE)バージョン
- Cisco C1117 Cisco IOS® XEソフトウェア、バージョン17.12.02
- Windows 10を使用するラップトップ

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

ネットワーク図



ネットワーク図

コンフィギュレーション

設定するには、次の手順を実行します。

ステップ 1 : ISR 1100ルータを設定します。

ステップ 2 : Identity Service Engine 3.2を設定します。

ステップ 3 : Windowsネイティブサブリカントを設定します。

ステップ 1 : ISR 1100ルータの設定

このセクションでは、dot1xを機能させるために少なくともNADが必要な基本設定について説明します。

注：マルチノードISE導入の場合、PSNペルソナが有効になっているノードのIPを設定します。これは、Administration > System > DeploymentタブでISEに移動することで有効にできます。

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
  key <Your shared secret>
```

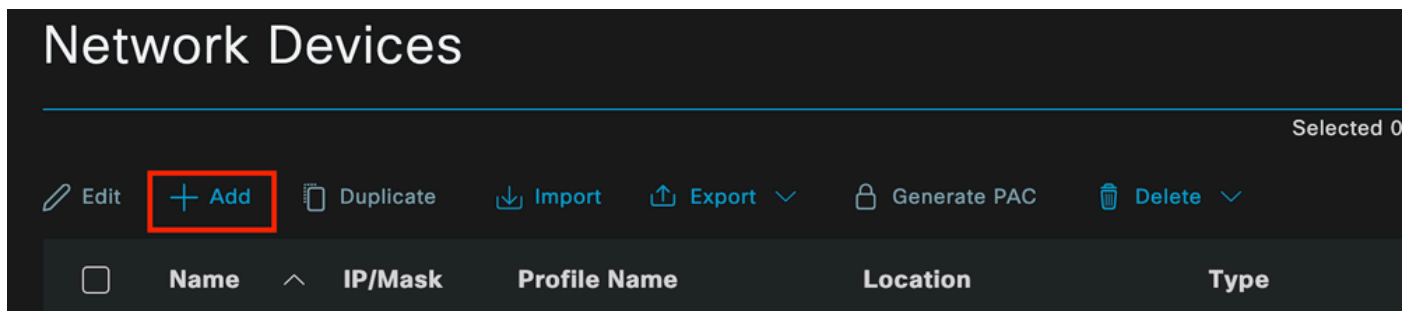
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication priority dot1x mab  
  authentication port-control auto  
  dot1x pae authenticator  
  spanning-tree portfast
```

ステップ 2 : Identity Service Engine 3.2を設定します。

2. a. 認証に使用するネットワークデバイスを設定し、追加します。

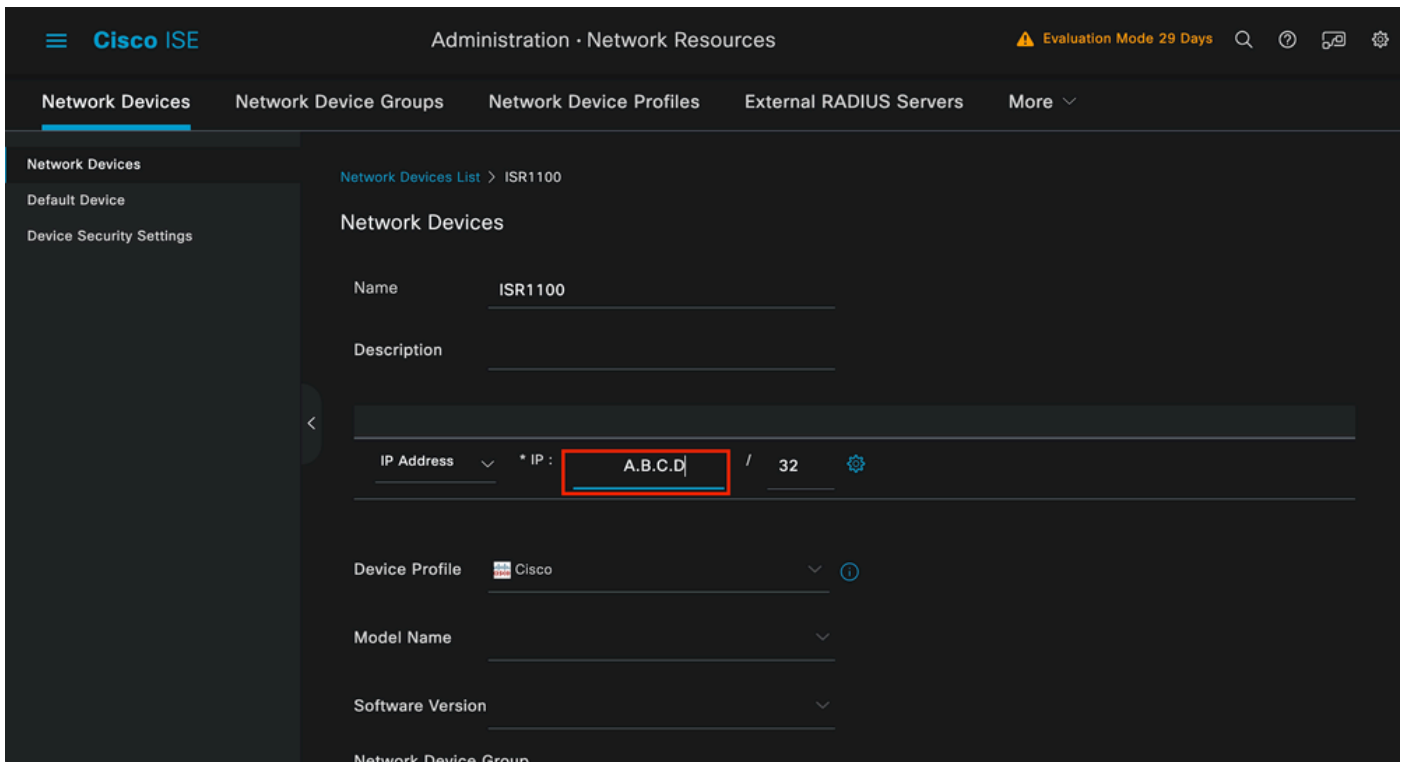
Add the Network Device to ISE Network Devicesセクション

Addボタンをクリックして起動します。



ISEネットワークデバイス

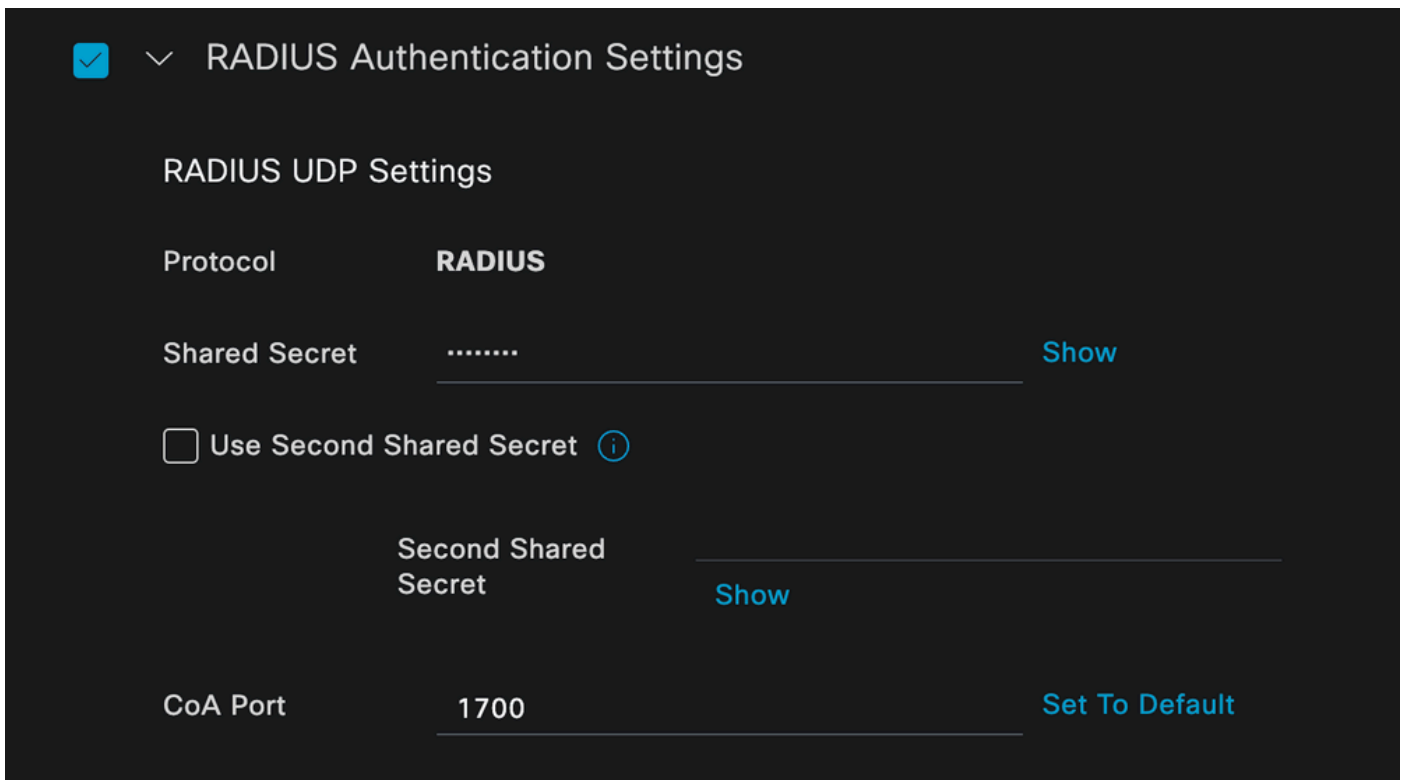
値を入力し、作成するNADに名前を割り当て、ネットワークデバイスがISEへの接続に使用するIPを追加します。



ネットワークデバイス作成ページ

同じページで、スクロールダウンしてRadius Authentication Settingsを探します。次の図に示すように、

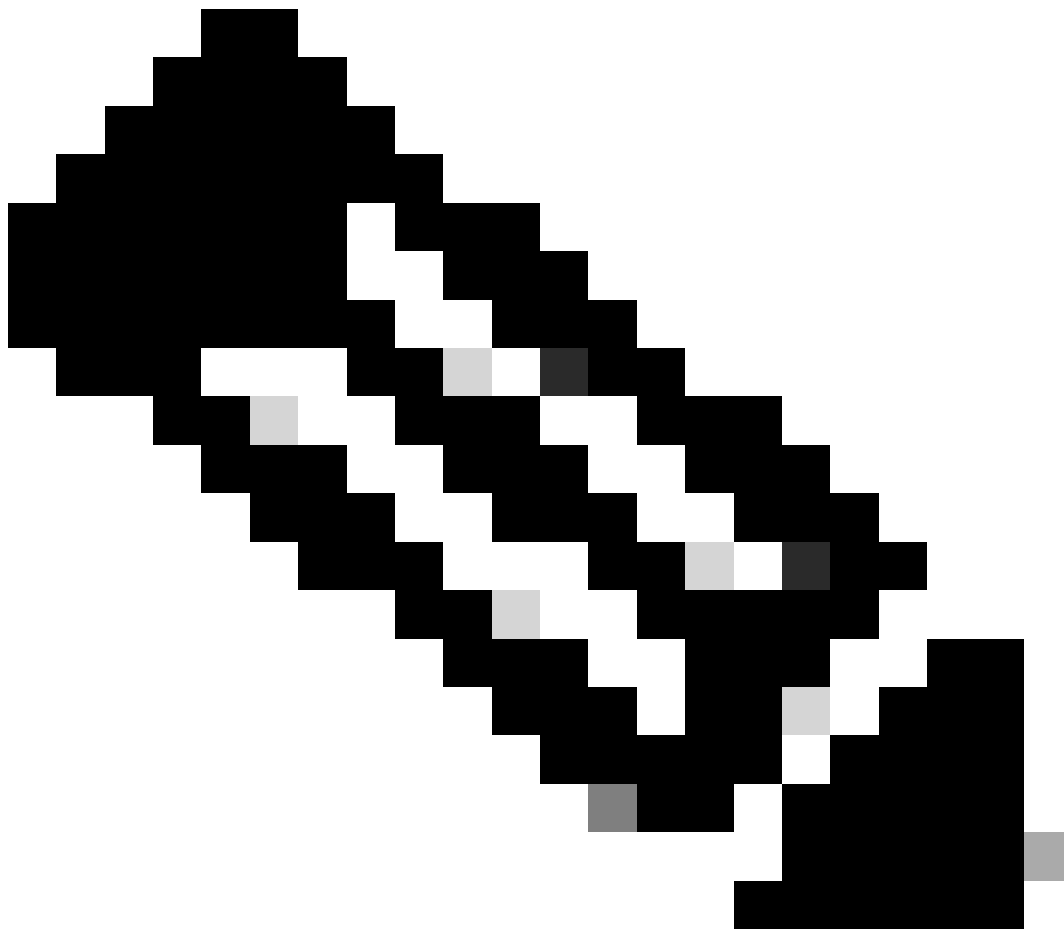
NAD設定で使用した共有秘密を追加します。



RADIUSの設定

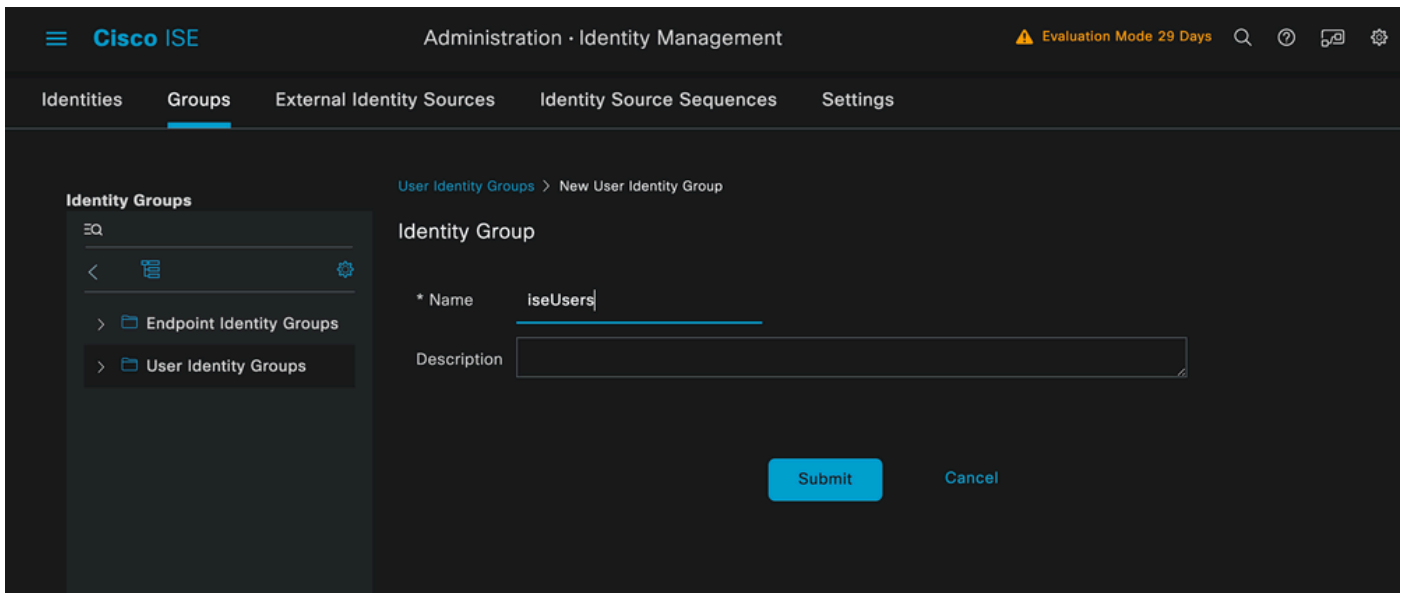
変更を保存します。

2. b.エンドポイントの認証に使用されるIDを設定します。



注：この設定ガイドを保持するために、単純なISEローカル認証が使用されます。

Administration > Identity Management > Groupsタブに移動します。グループとIDを作成します。
このデモンストレーション用に作成したグループはiseUsersです。

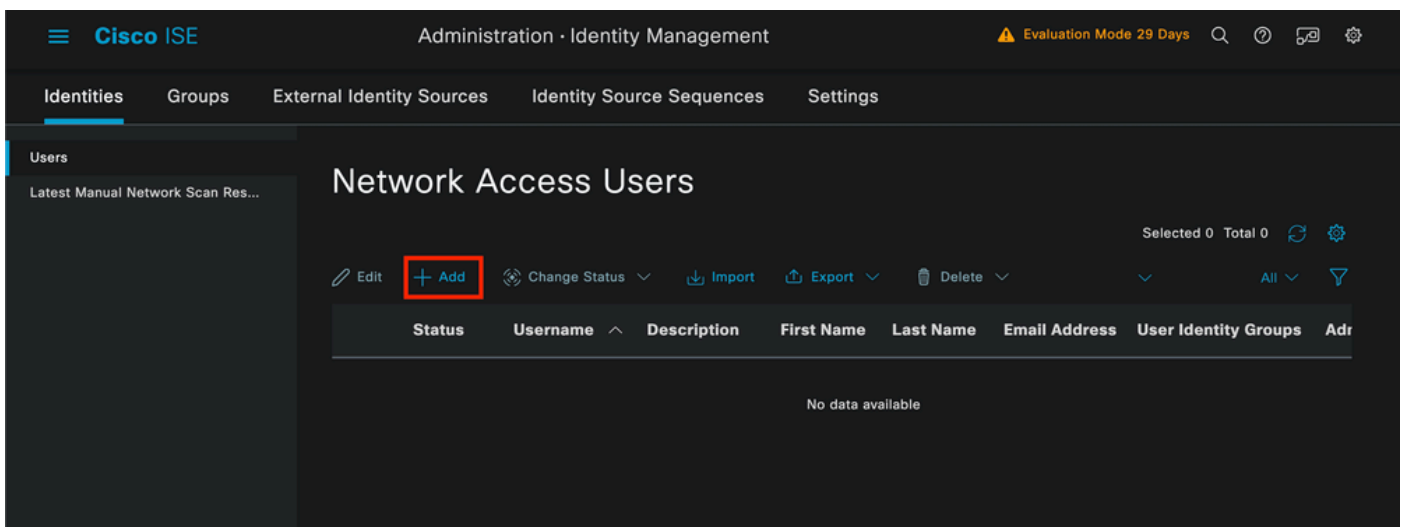


IDグループの作成ページ

Submitボタンをクリックします。

次に、Administration > Identity Management > Identity タブに移動します。

[Add] をクリックします。



ユーザー作成ページ

必須フィールドの一部として、ユーザの名前で始まります。この例では、ユーザ名iseiscoolを使用しています。

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

ユーザ名に割り当てられた名前

次に、作成したユーザ名にパスワードを割り当てます。このデモンストレーションでは、VainillaISE97を使用します。

Passwords

Password Type: ▼

Password Lifetime:

- With Expiration ⓘ
Password will expire in 60 days
- Never Expires ⓘ

Password

Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

パスワードの作成

ユーザをiseUsersグループに割り当てます。

User Groups

ⓘ

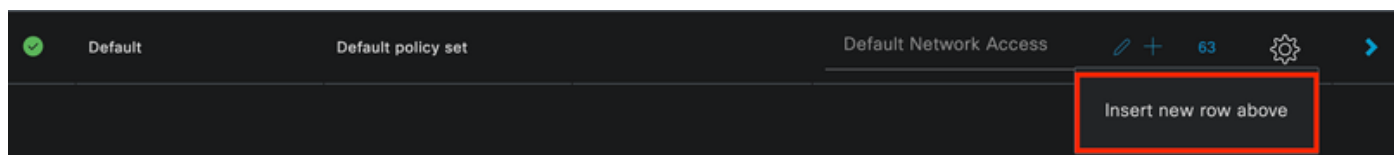
ユーザグループの割り当て

2. c. ポリシーセットの設定

ISEメニュー>ポリシー>ポリシーセットに移動します。

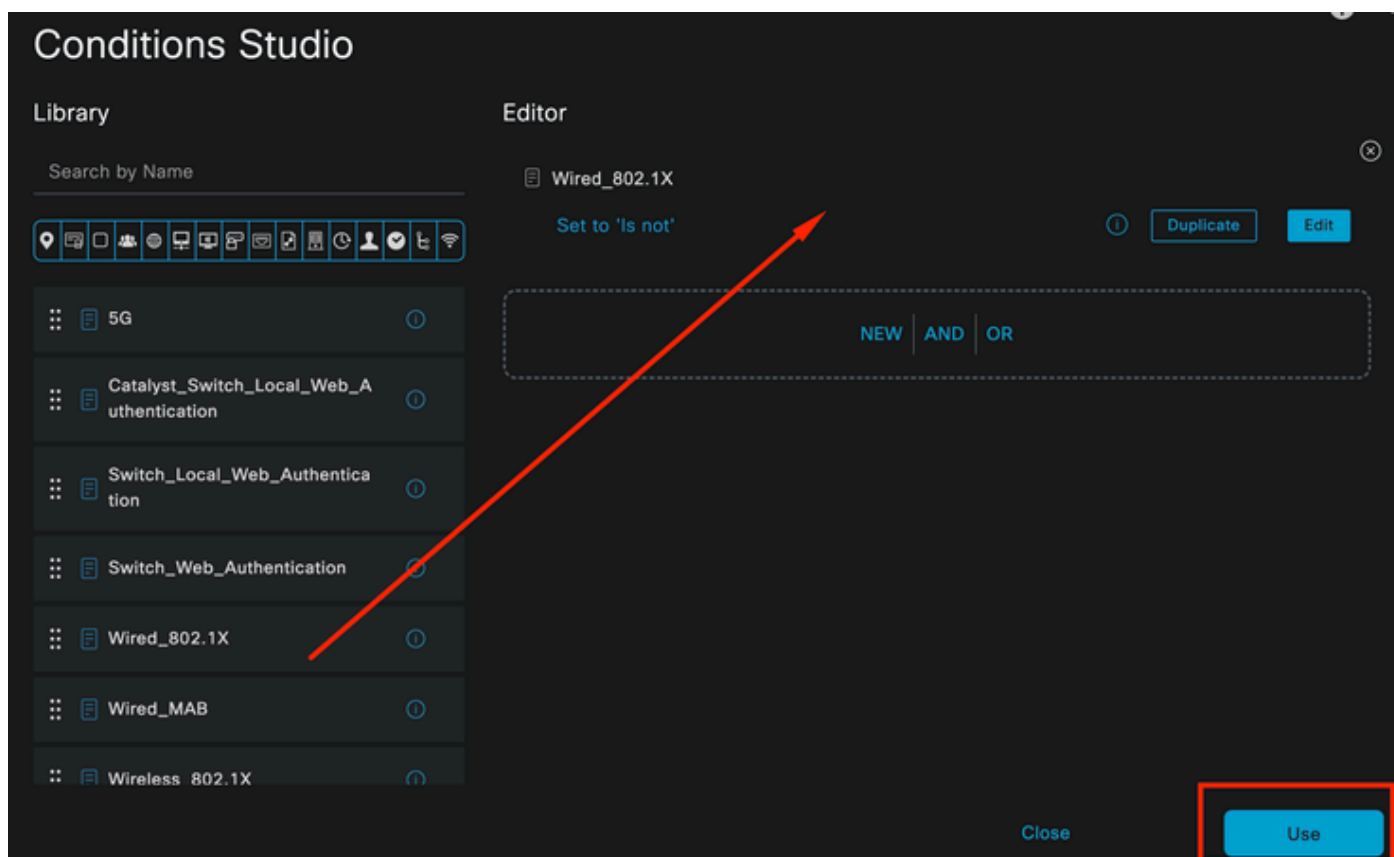
デフォルトのポリシーセットを使用できます。ただし、この例ではポリシーセットが作成され、名前はWiredになっています。ポリシーセットの分類と区別は、トラブルシューティングに役立ちます。

追加アイコンまたはプラスアイコンが表示されていない場合は、任意のポリシーセットの歯車アイコンをクリックできます。歯車アイコンを選択し、[上に新しい行を挿入]を選択します。



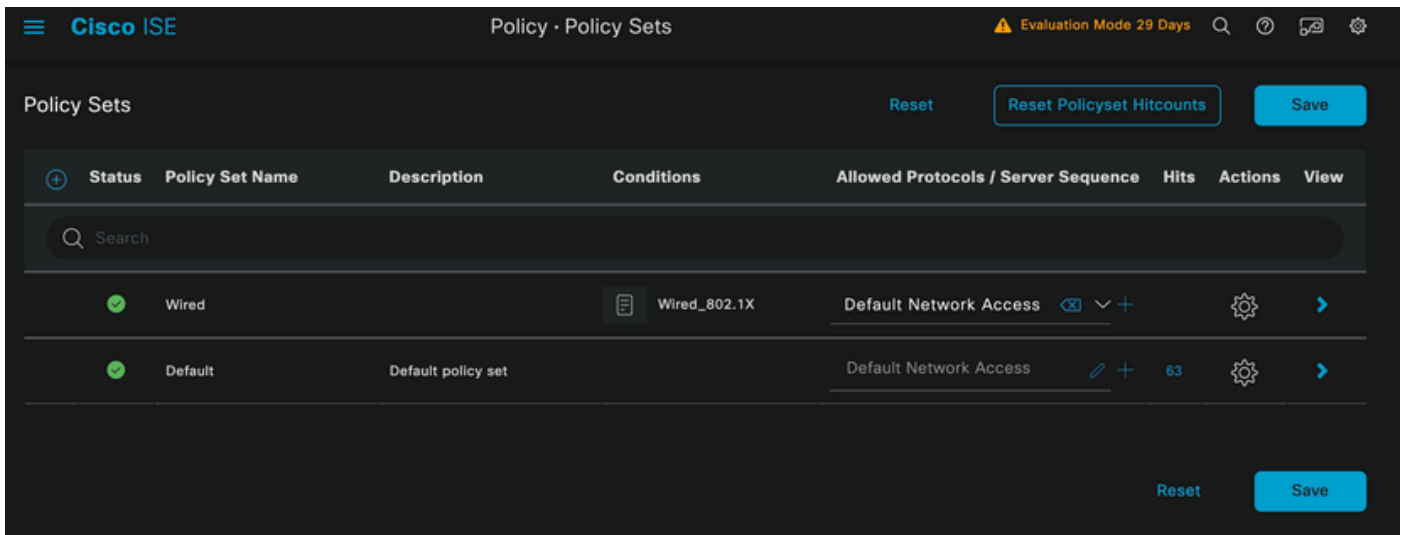
ポリシーの作成

この例で設定される条件は有線802.1xで、これはISEの新規導入で事前に設定された条件です。これをドラッグして、Useをクリックします。



条件スタジオ

最後に、Default Network Access preconfigured allowed protocols serviceを選択します。

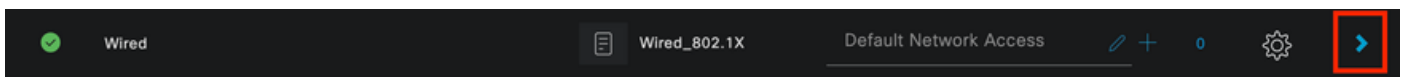


ポリシーセットビュー

[Save] をクリックします。

2. d. 認証および認可ポリシーの設定

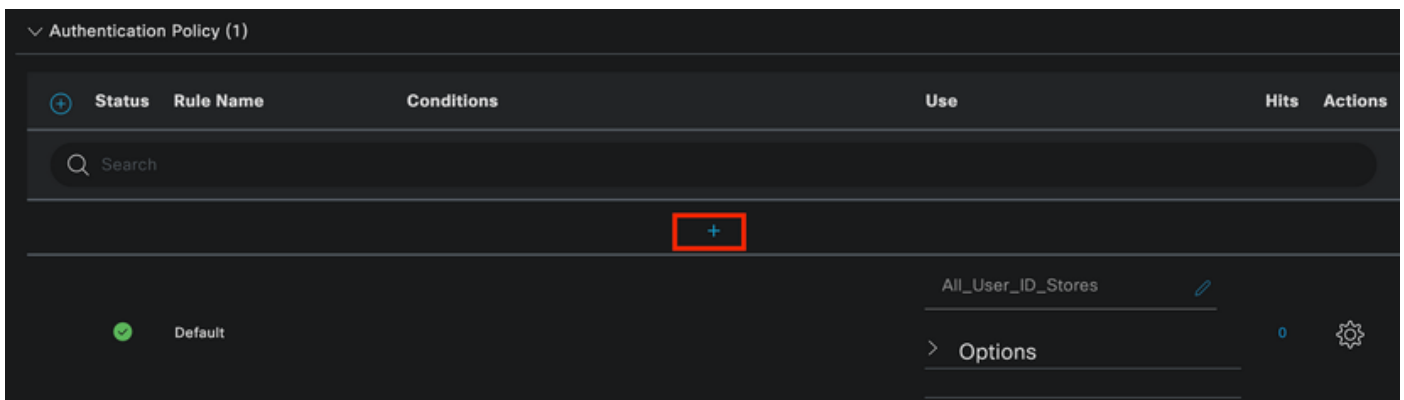
作成したポリシーセットの右側にある矢印をクリックします。



有線ポリシーセット

認証ポリシーの展開

+アイコンをクリックします。



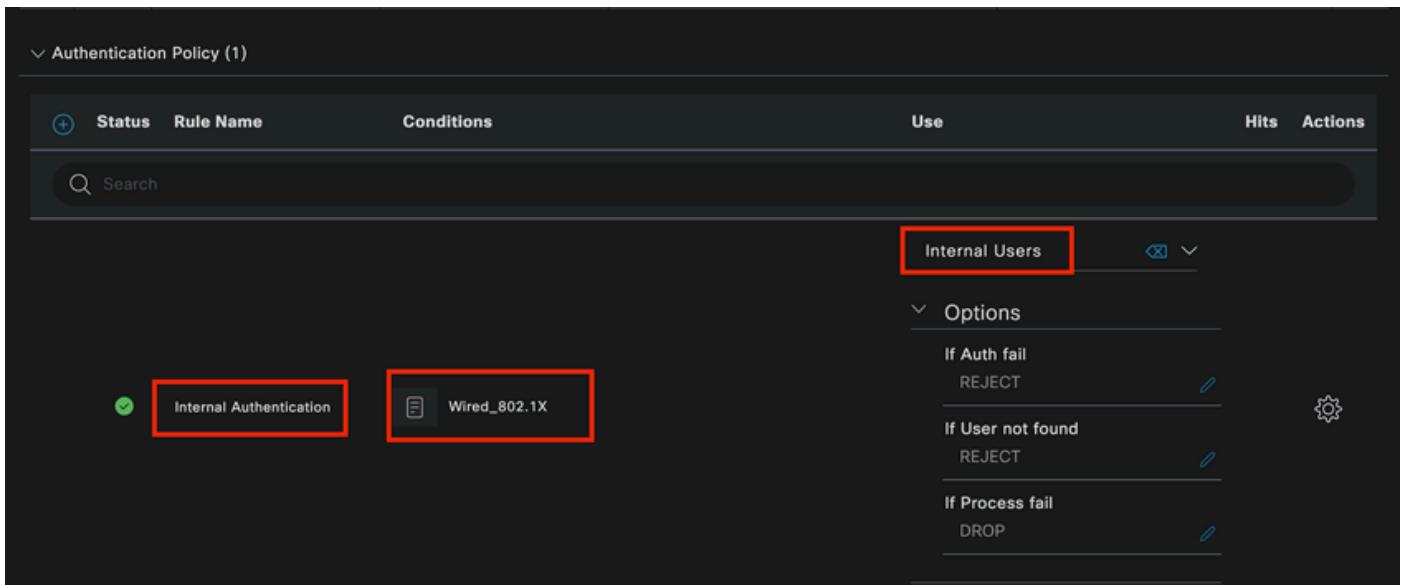
認証ポリシーの追加

認証ポリシーに名前を割り当てます。この例では、内部認証が使用されています。

この新しい認証ポリシーの条件列で+アイコンをクリックします。

Wired Dot1x ISEに付属の事前設定された条件を使用できます。

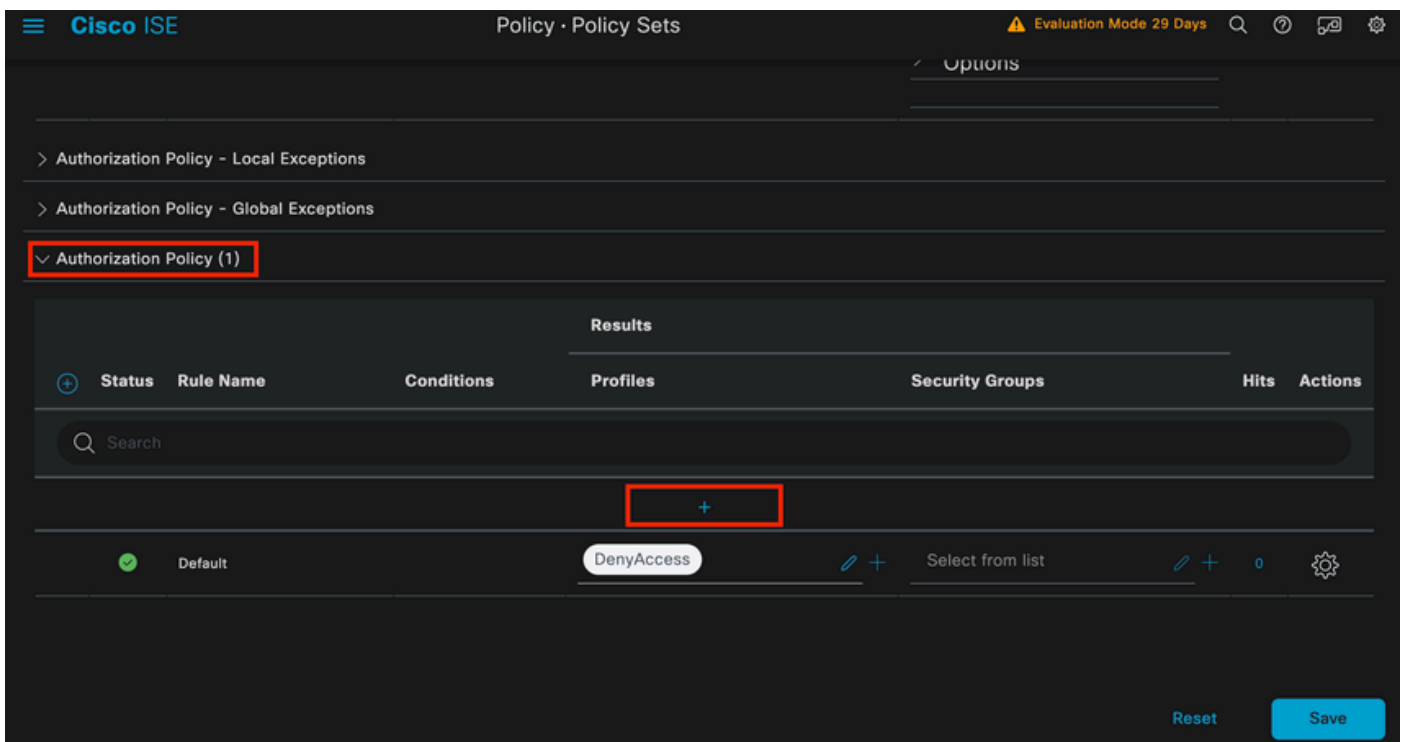
最後に、Use列で、ドロップダウンリストからInternal Usersを選択します。



認証ポリシー

認可ポリシー

Authorization Policyセクションは、ページの下部にあります。これを展開して、+アイコンをクリックします。



認可ポリシー

追加した認可ポリシーに名前を付けます。この設定例では、Internal ISE Usersという名前が使用されています。

この認可ポリシーの条件を作成するには、Conditions列にある+アイコンをクリックします。

以前に作成したユーザはIseUsersグループの一部です。

エディタが開いたら、Click to add an attributeセクションをクリックします。

IDグループアイコンを選択します。

ディクショナリから、Identity Group属性に付属するInternalUserディクショナリを選択します。

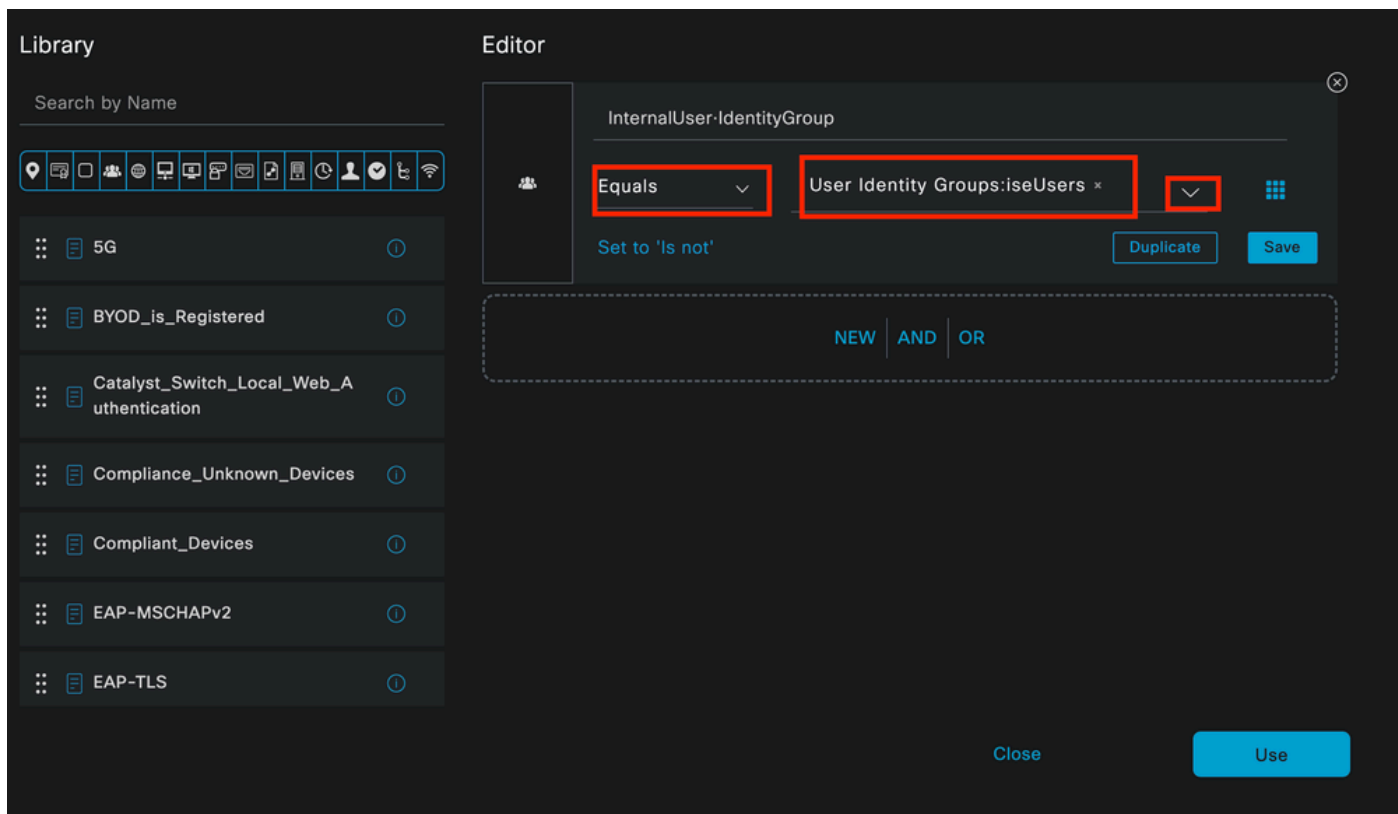
The screenshot shows the Cisco ISE configuration interface. On the left is the 'Library' pane with a search bar and a list of dictionaries. On the right is the 'Editor' pane, which is currently displaying a 'Select attribute for condition' dialog. The dialog title is 'InternalUser-IdentityGroup'. Below the title is a toolbar with various icons, and a table of available attributes. The 'InternalUser' dictionary and its 'IdentityGroup' attribute are highlighted with a red box.

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
AD	ExternalGroups		ⓘ
CWA	CWA_ExternalGroups		ⓘ
IdentityGroup	Description		ⓘ
IdentityGroup	Name		ⓘ
InternalUser	IdentityGroup		ⓘ
PassiveID	PassiveID_Groups		ⓘ

認可ポリシーの条件スタジオ

Equals演算子を選択します。

User Identity Groupsドロップダウンリストから、グループIseUsersを選択します。



許可ポリシーの条件が完了しました

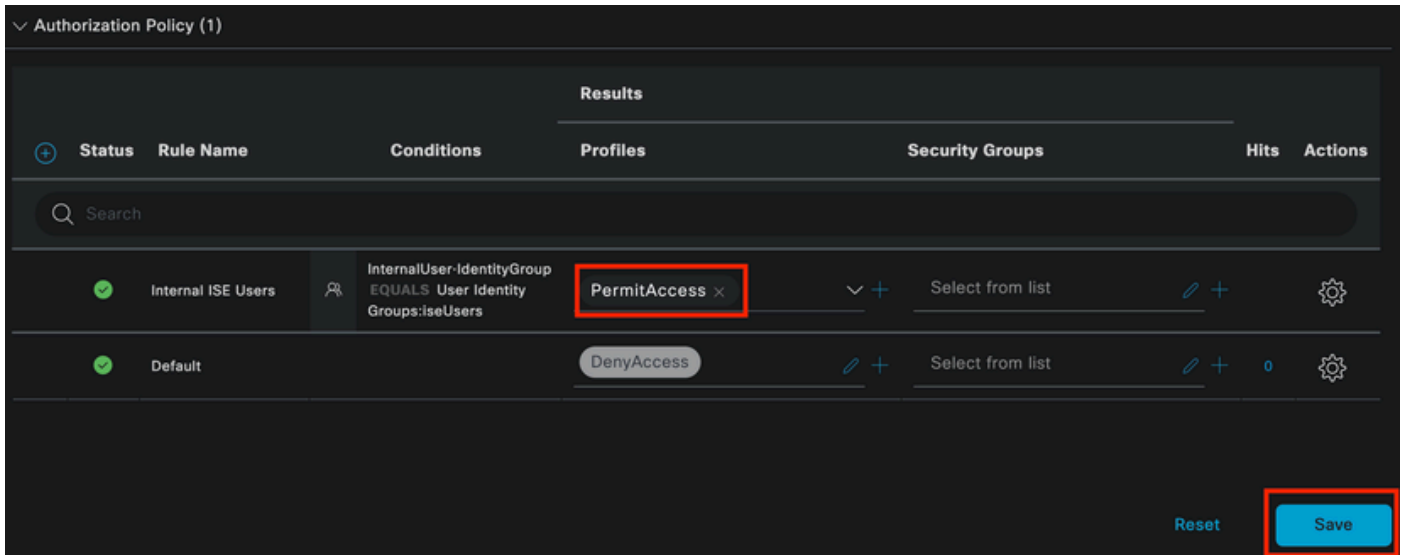
Useをクリックします。

最後に、このIDグループの認証部分を受信する結果認可プロファイルを選択します。



注：ISEに到達した認証が、ユーザIDグループISEUsersに属していないこの有線Dot1xポリシーセットにヒットしていることに注目してください。この時点で、デフォルトの許可ポリシーにヒットします。これは、プロファイル結果DenyAccessを持ちます。

ISEには、許可アクセスプロファイルが事前に設定されています。これを選択します。



承認ポリシーが完了しました

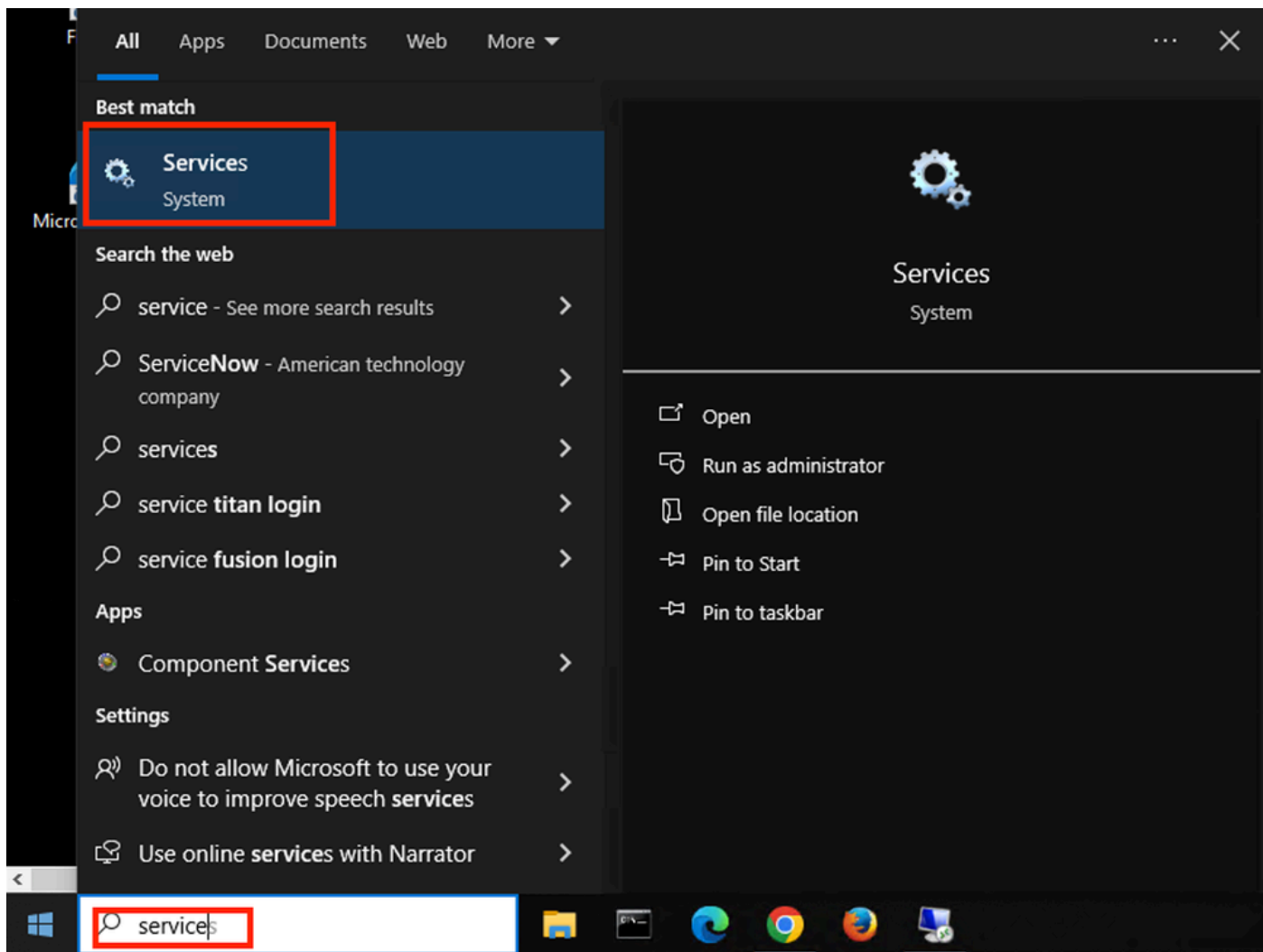
[Save] をクリックします。

ISEの設定が完了しました。

ステップ 3 : Windowsネイティブサブリカントの設定

3. a. Windowsで有線dot1xを有効にします。

Windowsの検索バーからServicesを開きます。



Windows検索バー

サービスリストの下部で、Wired Autoconfigを見つけます。

Wired AutoConfigで右クリックして、Propertiesを選択します。

Wired AutoConfig Properties (Local Computer)



General Log On Recovery Dependencies

Service name: dot3svc

Display name: Wired AutoConfig

Description: responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X

Path to executable:

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Manual

Service status: Stopped

Start

Stop

Pause

Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK

Cancel

Apply



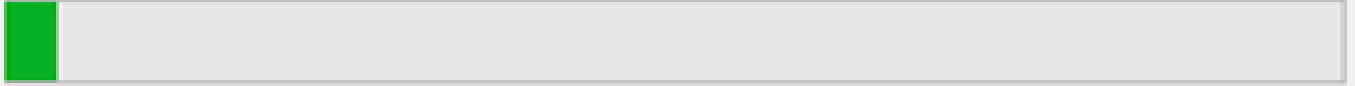
注:Wired AutoConfig(DOT3SVC)サービスは、イーサネットインターフェイスでIEEE 802.1X認証を実行します。

Manual起動タイプが選択されています。

サービスステータスがStoppedであるため。[Start (スタート)] をクリックします。

Windows is attempting to start the following service on Local Computer...

Wired AutoConfig



Close

サービス制御

次に、OKをクリックします。

この後、サービスは実行されています。

Windows Update	Enables the ...	Running	Manual (Trig...	Local System...
Windows Update Medic Service	Enables rem...		Manual	Local System...
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired A...	Running	Manual	Local System...
WLAN AutoConfig	The WLANS...		Manual	Local System...
WMI Performance Adapter	Provides pe...		Manual	Local System...
Work Folders	This service ...		Manual	Local Service

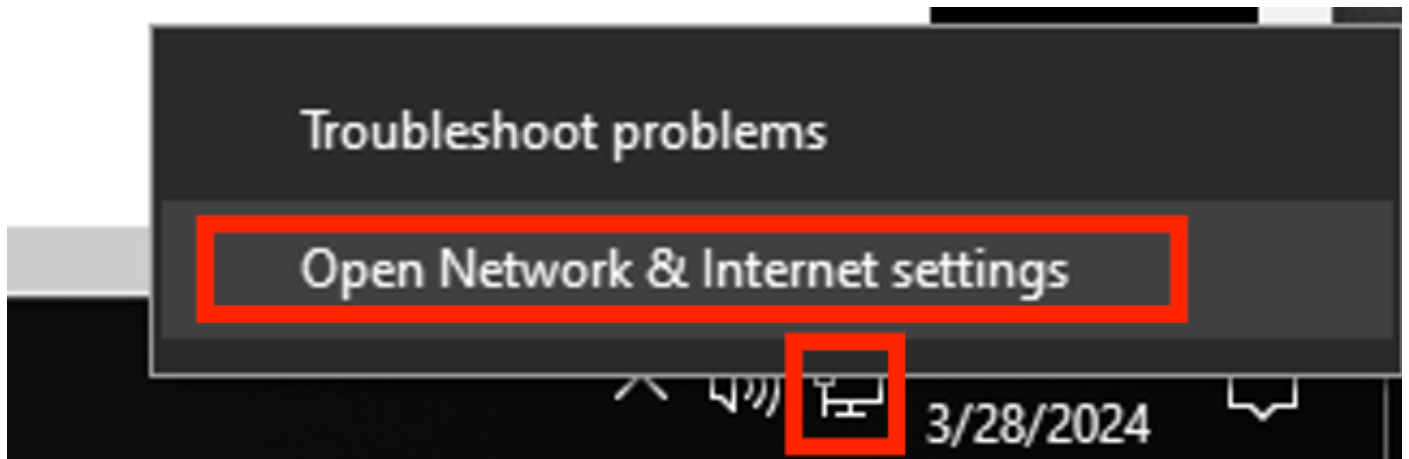
有線AutoConfigサービス

3. b. NADオーセンティケーター(ISR 1100)に接続されているWindowsラップトップインターフェイスを設定します。

タスクバーから右側の角を見つけ、コンピュータアイコンを使用します。

コンピュータのアイコンをダブルクリックします。

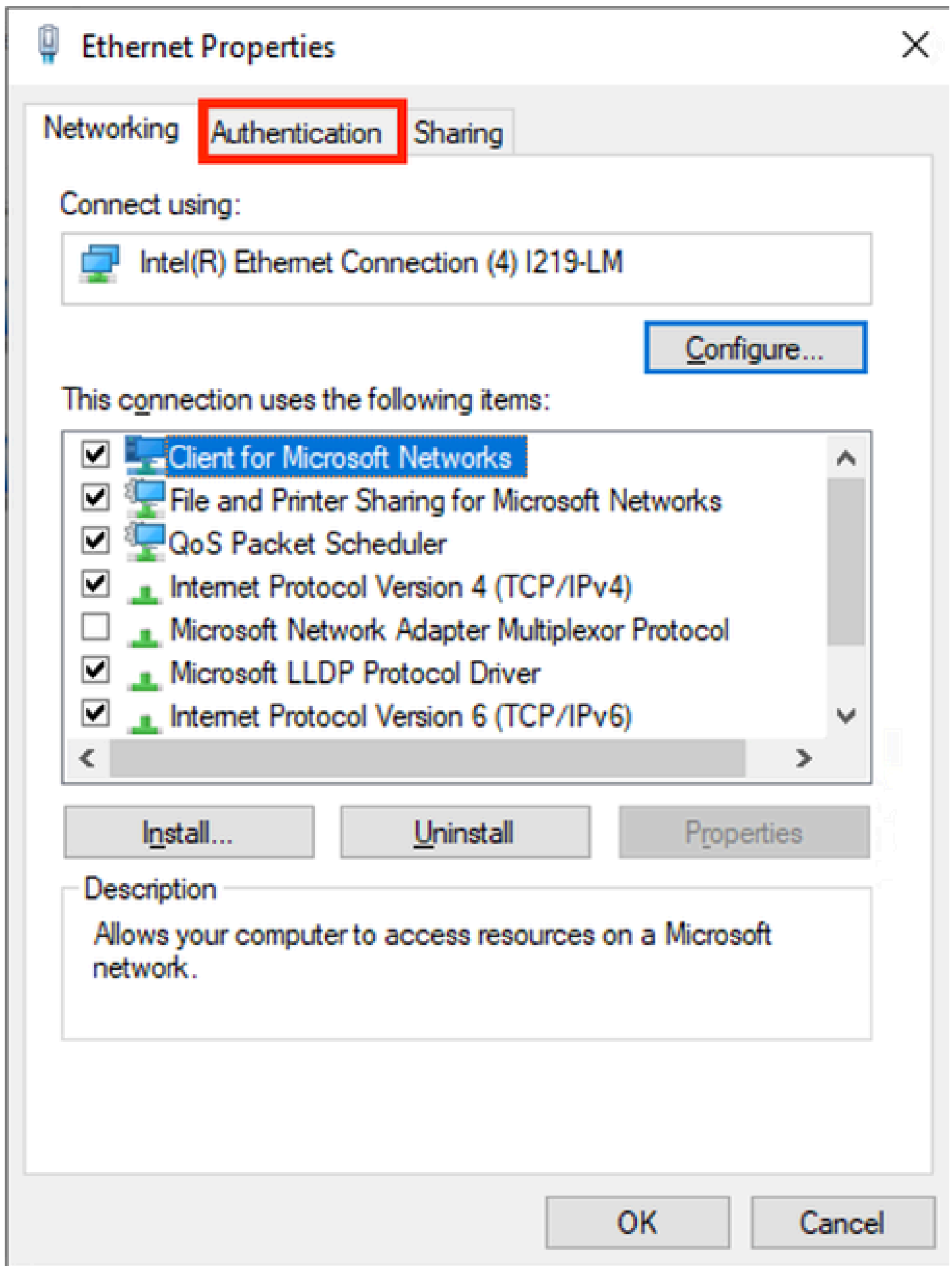
Open Network & Internet Settingsを選択します。



Windowsタスクバー

Network Connectionsウィンドウが開いたら、ISR Gig 0/1/0に接続されているイーサネットインターフェイスで右クリックします。Propertiesオプションをクリックします。

[Authentication] タブをクリックします。



インターフェイスイーサネットプロパティ

Enable IEEE 802.1X authentication チェックボックスを選択します。



Ethernet Properties



Networking

Authentication

Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) ▾

Settings

Remember my credentials for this connection each time I'm logged on

Fallback to unauthorized network access

Additional Settings...

OK

Cancel

Protected EAP (PEAP)を選択します。

Remember my credentials for this connection every time I'm logged onオプションをオフにします。

[Setting] をクリックします。

Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;. *\.srv3\.com):

Trusted Root Certification Authorities:

- AAA Certificate Services
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

Interface: GigabitEthernet0/1/0
IIF-ID: 0x08767C0D
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool <----- The username configured for Windows Native Supplicant
Status: Authorized <----- An indication that this session was authorized by the PSN
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C83E28461
Acct Session ID: 0x00000003
Handle: 0xc6000002
Current Policy: POLICY_Gi0/1/0

Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:

Method status list:

Method	State
dot1x	Authc Success <----- An indication that dot1x is used for this authentication

Router#

ISEログ

Operations > Radius > Live logsタブに移動します。

ユーザ名IDでフィルタリングします。この例では、ユーザ名iseiscoolが使用されます。

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (1), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the summary cards, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 3 hours). There are also buttons for 'Reset Repeat Counts' and 'Export To'. The main table has columns: 'Time', 'Status', 'Details', 'Repea...', 'Identity', 'Endpoint ID', 'Endpoint...', 'Authentication Policy', and 'Authc'. Two rows of log entries are visible, with the 'Identity' and 'Authentication Policy' columns highlighted in red. The first row shows 'iseiscool' and 'Wired >> Internal Authentication'. The second row shows 'iseiscool' and 'Wired >> Internal Authentication'. At the bottom, it says 'Last Updated: Thu Mar 28 2024 01:29:12 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

ISEのLivelogs

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (1), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the summary cards, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 3 hours). There are also buttons for 'Reset Repeat Counts' and 'Export To'. The main table has columns: 'Authorization Policy', 'Authoriz...', 'IP Address', 'Network De...', 'Device Port', 'Identity Group', 'Posture ...', and 'Server'. Two rows of log entries are visible, with the 'Authorization Policy', 'IP Address', 'Network De...', 'Device Port', 'Identity Group', and 'Server' columns highlighted in red. The first row shows 'Wired >> Internal ISE Users', 'PermitAcc...', 'ISR1100', 'GigabitEthernet0/1/0', 'User Identity Groups:iseUsers', and 'PSN01'. The second row shows 'Wired >> Internal ISE Users', 'PermitAcc...', 'ISR1100', 'GigabitEthernet0/1/0', 'User Identity Groups:iseUsers', and 'PSN01'. At the bottom, it says 'Last Updated: Thu Mar 28 2024 01:34:19 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

ISEのLivelogs

このクイックビューから、ライブログが重要な情報を提供していることに注目してください。

- 認証のタイムスタンプ。
- IDが使用されました。
- エンドポイントMACアドレス。
- アクセスされたポリシーセットと認証ポリシー。
- アクセスされたポリシーセットと許可ポリシー。
- 許可プロファイルの結果。
- ISEにRADIUS要求を送信するネットワークデバイス。
- エンドポイントが接続されているインターフェイス。
- 認証されたユーザのIDグループ。
- 認証を処理したポリシーサーバーノード(PSN)。

トラブルシューティング

1: ISEライブログの詳細の読み取り

Operations > Radius > Live logsの順に移動し、Auth status: Failedでフィルタリングするか、使用されているユーザ名、MACアドレス、または使用されているネットワークアクセスデバイスでフィルタリングします。

Operations > Radius > Live logs > Desired authentication > Live logの順に選択して、詳細を表示します。

同じページで、認証をフィルタリングしたら、Searchアイコンをクリックします。

最初のシナリオ：ユーザはユーザ名を入力するときに入力ミスを行いました。

Time	Status	Details	Repea...	Identity	Endpoint...	Endpoint...	Authentication Policy	Authoriz...	Authoriz...	IP Address	Network De
Apr 19, 2024 11:54:53.2...	Failed			iselscoool	8C:16:4...		Wired >> Internal Authentication	Wired			ISR1100

ライブログの詳細を開く

ライブログの詳細を開くと、認証に失敗したユーザ名と、使用されたユーザ名が表示されていることがわかります。

Overview

Event	5400 Authentication failed
Username	iseiscool
Endpoint Id	<ENDPOINT MAC ADDRESS>#
Endpoint Profile	
Authentication Policy	Wired >> Internal Authentication
Authorization Policy	Wired
Authorization Result	

概要セクション

次に、同じライブログの詳細（「認証の詳細」セクション）で、エラーのエラーの原因、根本原因、および解決策を確認できます。

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resolution settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).
Username	iseiscool

認証の詳細

このシナリオで認証が失敗する原因は、ユーザ名に誤りがあることです。ただし、ユーザがISEで作成されていない場合、またはISEがユーザが他のアイデンティティストア（LDAPやADなど）に存在することを検証できなかった場合は、これと同じエラーが表示されます。

Stepsセクション

```
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users ←
24210 Looking up User in Internal Users IDStore - iseiscoool ←
24216 The user is not found in the internal users identity store ←
22056 Subject not found in the applicable identity store(s) ←
22058 The advanced option that is configured for an unknown
user is used
22061 The 'Reject' advanced option is configured in case of a
failed authentication request ←
11815 Inner EAP-MSCHAP authentication failed ←
11520 Prepared EAP-Failure for inner EAP method
22028 Authentication failed and the advanced options are
ignored
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-
response
61025 Open secure connection with TLS peer
12307 PEAP authentication failed ←
11504 Prepared EAP-Failure
11003 Returned RADIUS Access-Reject ←
```

Live Log Details Stepセクション

手順のセクションでは、RADIUSカンバセーション中にISEが実行したプロセスについて詳しく説

明します。

次のような情報が表示されます。

- 会話の開始方法。
- SSLハンドシェイクプロセス。
- ネゴシエートされたEAP方式。
- EAP方式プロセス。

この例では、ISEがこの認証の内部IDをチェックインしたことがわかります。ユーザが見つからなかったため、ISEは応答としてアクセス拒否を送信しました。

2番目のシナリオ:ISE管理者は、ポリシーセット許可プロトコルからPEAPを無効にしました。

2 – 無効なPEAP

セッション障害のライブログの詳細を開くと、「PEAP is not allowed in the Allowed Protocols」というエラーメッセージが表示されます。

Event	5400 Authentication failed
Failure Reason	12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols
Resolution	Ensure that the PEAP protocol is allowed by ISE in Allowed Protocols.
Root cause	The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols.
Username	iseiscool

ライブログ詳細レポート

このエラーは簡単に解決できます。解決するには、Policy > Policy Elements > Authentication > Allowed Protocolsの順に移動します。 オプションAllow PEAPが無効になっているかどうかを確認します。

The screenshot shows the Cisco ISE configuration interface for a policy element named 'Allow EAP-TLS'. The left sidebar contains navigation tabs: Dictionaries, Conditions, and Results (selected). Under 'Results', the 'Allowed Protocols' section is expanded. A red box highlights the 'Allow PEAP' checkbox, which is currently unchecked. Other visible settings include 'Allow LEAP' (unchecked), 'PEAP Inner Methods' (with 'Allow EAP-MS-CHAPv2' checked), 'Allow EAP-GTC' (checked), and 'Allow EAP-TLS' (checked). The 'Session ticket time to live' is set to 2 hours, and 'Proactive session ticket update will occur after 90 % of Time To Live has expired'.

Allowed Protocolsセクション

3番目のシナリオ：エンドポイントがISE証明書を信頼しないため、認証が失敗します。

ライブログの詳細に移動します。失敗した認証のレコードを検索し、ライブログの詳細を確認します。

Authentication Details

Source Timestamp 2024-04-20 04:37:42.007

Received Timestamp 2024-04-20 04:37:42.007

Policy Server ISE PSN

Event 5411 Supplicant stopped responding to ISE

Failure Reason 12934 Supplicant stopped responding to ISE during PEAP tunnel establishment

Resolution Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page (Administration > System > Certificates > Local Certificates). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.

Root cause PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

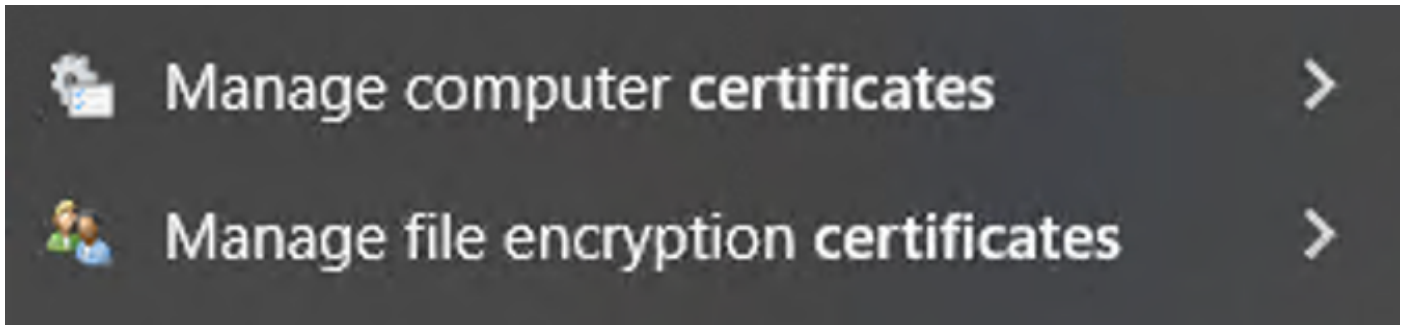
Username iseiscool

ライブログの詳細

エンドポイントが、PEAPトンネルの確立に使用する証明書を拒否しています。

この問題を解決するには、問題が発生したWindowsエンドポイントで、ISE証明書に署名したCAチェーンがWindowsセクションManage User Certificates > Trusted Root Certification AuthoritiesまたはManage Computer Certificates > Trusted Root Certification Authoritiesにあることを確認します。

Windowsの検索バーで検索すると、Windowsデバイス上でこの構成セクションにアクセスできません。

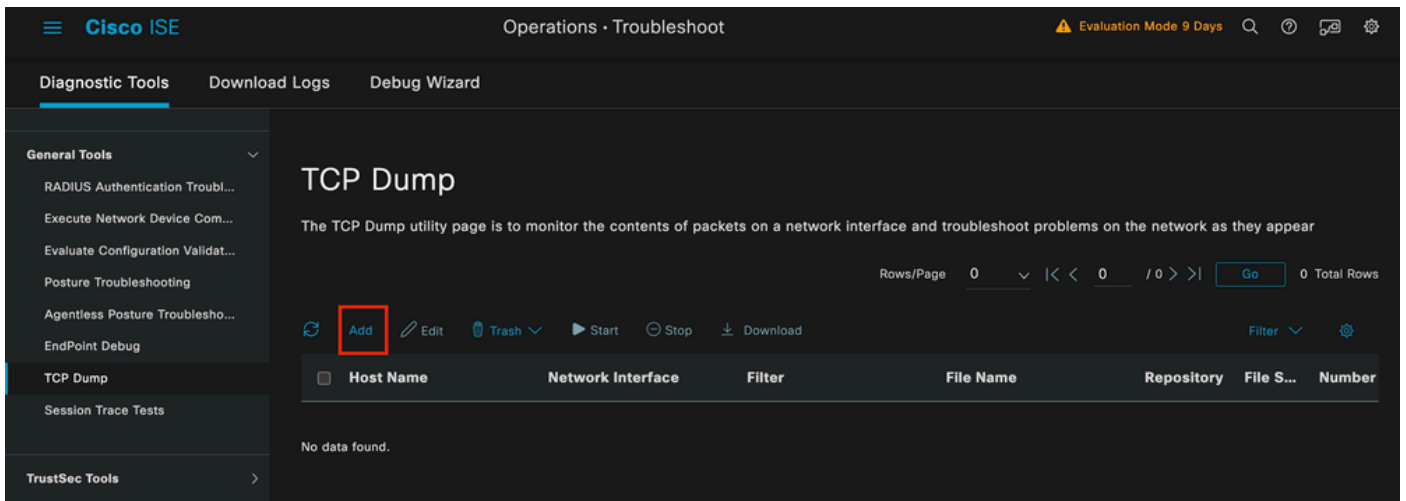


Windows検索バーの結果

3:ISE TCPダンプツール (パケットキャプチャ)

トラブルシューティングでは、パケットキャプチャ分析が不可欠です。ISEから直接パケットキャプチャを、すべてのノードおよびノードの任意のインターフェイスで取得できます。

このツールにアクセスするには、Operations > Diagnostic Tools > General Tools > TCP Dumpの順に選択します。



TCP Dumpセクション

pcapの設定を開始するには、Addボタンをクリックします。

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*

ISE PSN





Network Interface*

GigabitEthernet 0 [Up, Running]



Filter



E.g: ip host 10.77.122.123 and not
10.177.122.119

File Name

ISEPCAP

TCPダンプの作成

Repository

File Size
10
Mb

Limit to
1
File(s)

Time Limit
5
Minute(s)

Promiscuous Mode

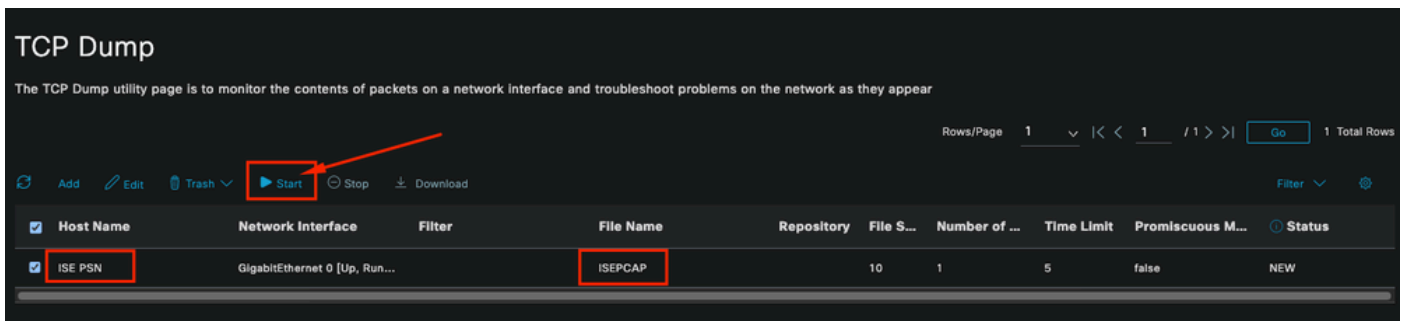
Cancel Save Save and Run

TCP Dumpセクション

ISEでpcapを作成するには、次のデータを入力する必要があります。

- pcapを取得する必要があるノードを選択します。
- pcapに使用されるISEノードインターフェイスを選択します。
- 特定のトラフィックをキャプチャする必要がある場合は、フィルタを使用します。ISEではいくつかの例を示します。
- pcapに名前を付けます。このシナリオでは、ISEPCAPを使用しました。
- リポジトリを選択します。リポジトリが選択されていない場合、キャプチャはISEローカルディスクに保存され、GUIからダウンロードできます。
- また、必要に応じて、pcapファイルのサイズを変更します。
- 必要に応じて複数のファイルを使用するため、pcapがファイルサイズを超えると、その後新しいファイルが作成されます。
- 必要に応じて、pcapのトラフィックのキャプチャ時間を延長します。

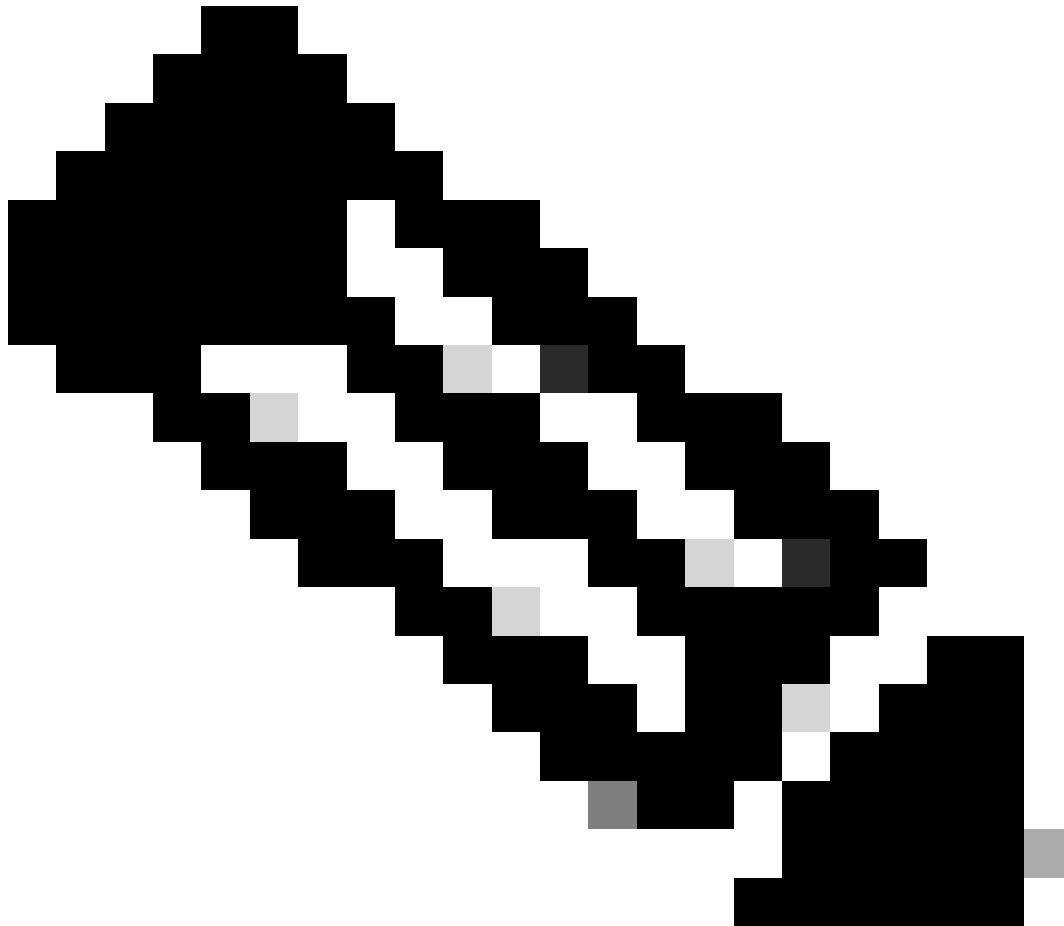
最後に、Saveボタンをクリックします。



TCP Dumpセクション

準備ができたなら、pcapを選択し、Startボタンをクリックします。

Startをクリックすると、Status列がRUNNING状態に変わります。



注:PCAPがRUNNING状態のときに、障害の発生しているシナリオやキャプチャする必要がある動作を複製します。完了すると、RADIUSの詳細、カンバセーションがPCAPに表示されます。

PCAPの実行中に必要なデータをキャプチャしたら、pcapコレクションを終了します。もう一度選択して、Stopをクリックします。

3 - 1 ISEレポート

より詳細な分析が必要な場合、ISEは過去のイベントを調査するための有用なレポートを提供します。

これらを見つけるには、Operations > Reports > Reports > Endpoints and Usersの順に移動します。

The screenshot displays the Cisco ISE interface. The top right corner shows 'Operations · Reports'. The left sidebar contains a navigation menu with 'Reports' and 'Endpoints and Users' highlighted with red boxes. The main content area is titled 'RADIUS Authentications' and shows a table of authentication events. The table has columns for 'Logged At', 'RADIUS Status', 'Details', and 'Identity'. The data shows four failed authentication attempts for the user 'iseiscool' on 2024-04-20.

Logged At	RADIUS Status	Details	Identity
× Last 7 Days ×	↓		Identity
2024-04-20 05:10:59.176	×	👤	iseiscool
2024-04-20 05:00:59.153	×	👤	iseiscool
2024-04-20 04:50:59.135	×	👤	iseiscool
2024-04-20 04:40:59.097	×	👤	iseiscool

ISEレポートセクション

Endpoints and Users



Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname
State: current UP, duration 2876s, previous duration 0s
Dead: total time 0s, count 0

Platform State from SMD: current UP, duration 2876s, previous duration 0s
SMD Platform Dead: total time 0s, count 0

Platform State from WNCN (1) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (2) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (3) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (4) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (5) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (6) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (7) : current UP, duration 3015s, previous duration 0s
Platform State from WNCN (8) : current UP, duration 3015s, previous duration 0s

WNCN Platform Dead: total time 0s, count 0

Quarantined: No

Authen: request 11, timeouts 0, failover 0, retransmission 0

Response: accept 1, reject 0, challenge 10
Response: unexpected 0, server error 0, incorrect 0, time 33ms
Transaction: success 11, failure 0
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
Dot1x transactions:

Response: total responses: 11, avg response time: 33ms
Transaction: timeouts 0, failover 0
Transaction: total 1, success 1, failure 0

MAC auth transactions:
Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0

Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0
MAC author transactions:

Response: total responses: 0, avg response time: 0ms
Transaction: timeouts 0, failover 0
Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
Request: start 1, interim 0, stop 0
Response: start 1, interim 0, stop 0

Response: unexpected 0, server error 0, incorrect 0, time 27ms
Transaction: success 2, failure 1
Throttled: transaction 0, timeout 0, failure 0
Malformed responses: 0
Bad authenticators: 0

```
Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

```
Consecutive Response Failures: total 0
  SMD Platform : max 0, current 0 total 0
  WNCN Platform: max 0, current 0 total 0
  IOSD Platform : max 0, current 0 total 0
```

```
Consecutive Timeouts: total 3
  SMD Platform : max 0, current 0 total 0
  WNCN Platform: max 0, current 0 total 0
  IOSD Platform : max 3, current 0 total 3
```

```
Requests per minute past 24 hours:
  high - 0 hours, 47 minutes ago: 4
  low  - 0 hours, 45 minutes ago: 0
  average: 0
```

Router>

8-2ポートのステータス、詳細、セッションに適用されているACL、認証方法、さらに役立つ情報を表示するには、show authentication sessions interface <interface where the laptop is attached> detailsコマンドを使用します。

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A00000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0
```

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
```

```
Server Policies:
```

```
Method status list:
Method State
dot1x Authc Success
```

Router#

8-3グローバルコンフィギュレーションにaaaに必要なすべてのコマンドがあることを確認するには、show running-config aaaを実行します。

```
Router#sh run aaa
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
client <A.B.C.D> server-key Cisc0123
!
!
radius server COHVSRAISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRAISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4もう一つの便利なコマンドは、test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacyです。

```
Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy
User was successfully authenticated.
```

```
Router#
```

9 – ネットワークデバイス関連のデバッグ

- debug dot1x all : すべてのdot1x EAPメッセージを表示します
- debug aaa authentication:AAAアプリケーションからの認証デバッグ情報を表示します
- debug aaa authorization:AAA認可のデバッグ情報を表示します
- debug radius authentication : 認証用に、プロトコルレベルのアクティビティに関する詳細情報を提供します

- debug radius : プロトコルレベルのアクティビティに関する詳細情報を提供します

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

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。