ISEを使用したEAP-TLS認証の設定

内容

はじめに

このドキュメントでは、Cisco ISEでExtensible Authentication Protocol-Transport Layer Security(EAP-TLS)認証を導入するための初期設定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。

- EAPおよびRADIUS通信フローの基本的な知識。
- 通信フローに関する、証明書ベースの認証方式に関する基本的なRADIUS認証の知識。

- Dot1xとMAC認証バイパス(MAB)の違いについて
- 公開キーインフラストラクチャ(PKI)の基本的な知識。
- 認証局(CA)から署名付き証明書を取得し、エンドポイントで証明書を管理する方法に精通していること。
- ネットワークデバイス(有線またはワイヤレス)での認証、許可、およびアカウンティング(AAA)(RADIUS)関連の設定。
- RADIUS/802.1xで使用するサプリカント（エンドポイント）の設定。

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。

- Identity Services Engine(ISE)リリース3.x
- CA：証明書を発行します(エンタープライズCA、サードパーティ/パブリックCAにすることも、証明書プロビジョニングポータルを使用することもできます)。
- Active Directory（外部IDソース）:Windows Serverから。ISEと互換性がある場合。
- ネットワークアクセスデバイス(NAD):802.1x/AAA用に設定されたスイッチ（有線）またはワイヤレスLANコントローラ(WLC)（ワイヤレス）です。
- エンドポイント – RADIUS/802.1x：ユーザ認証を介してネットワークアクセス用に認証できる（ユーザ）IDおよびサプリカント設定に対して発行される証明書。マシン証明書を取得することは可能ですが、この例では使用されていません。

注：このガイドではISEリリース3.1を使用しているため、すべてのドキュメント参照はこのバージョンに基づいています。ただし、以前のリリースのCisco ISEでは、同じ設定または同様の設定が可能であり、完全にサポートされています。

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。

背景説明

主な焦点は、有線またはワイヤレスで接続されたIPフォン/エンドポイントでの認証など（ただし、これに限定されない）複数のシナリオに適用できるISE設定です。

このガイドの対象範囲として、ISE(RADIUS)認証フローの次のフェーズを理解することが重要です。

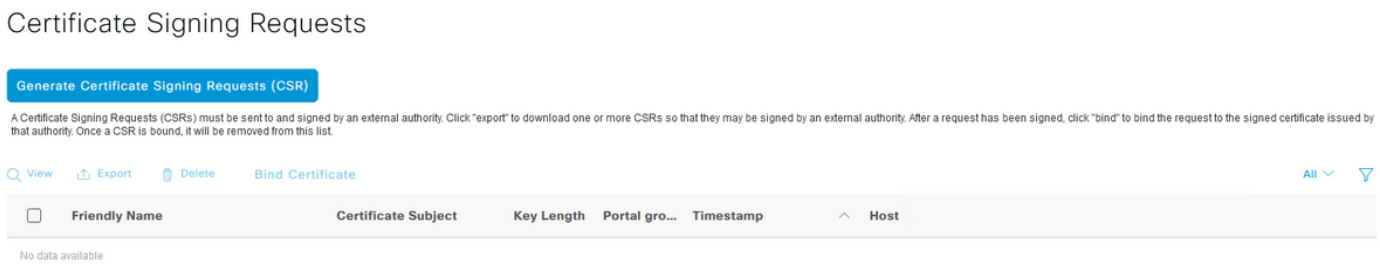
- 認証：ネットワークアクセスを要求するエンドアイデンティティ（マシン、ユーザなど）を特定し、検証します。
- 許可：ネットワークでエンドアイデンティティに付与できる権限とアクセスを決定します。
- アカウンティング：ネットワークアクセスが確立された後のエンドアイデンティティのネットワークアクティビティをレポートおよび追跡します。

設定

サーバ証明書とクライアント証明書の取得

ステップ 1：ISEからの証明書署名要求(CSR)の生成

最初のステップでは、ISEから証明書署名要求(CSR)を生成し、CA（サーバ）に送信して、ISEに発行された署名付き証明書をシステム証明書として取得します。この証明書は、Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)認証の際にISEによってサーバ証明書として提示されます。これはISE UIで実行されます。移動先 **Administration > System: Certificates > Certificate Management > Certificate Signing Requests**を参照。通常の **Certificate Signing Requests**をクリックし、 **Generate Certificate Signing Requests (CSR)** 以下の図に、出力例を示します。



証明書の種類には、異なる拡張キーの使用が必要です。次のリストは、各証明書タイプに必要な拡張キー使用法の概要を示しています。

ISE ID証明書

- 多用途(Admin、EAP、Portal、pxGrid) – クライアントおよびサーバ認証
- Admin：サーバ認証
- EAP認証 – サーバ認証
- Datagram Transport Layer Security(DTLS)認証 – サーバ認証
- ポータル – サーバ認証
- pxGrid – クライアントおよびサーバ認証
- Security Assertion Markup Language(SAML):SAML署名証明書
- ISEメッセージングサービス：署名証明書の生成または新しいメッセージング証明書の生成

デフォルトでは、ISEメッセージングサービスシステム証明書は、導入、ノード登録、およびその他のノード間通信における各ISEノード間のデータレプリケーション用であり、ISE内部認証局(CA)サーバ（ISEの内部）によって提示および発行されます。この証明書を使用して完了する必要のあるアクションはありません。

管理システム証明書は、管理UI（管理）に関連付けられたAPIが使用されるタイミングや、一部のノード間通信など、各ISEノードを識別するために使用されます。ISEを初めて設定するには、Admin System Certificateを配置します。この操作は、この設定ガイドに直接関連するものではありません。

EAP-TLS（証明書ベースの認証）を介してIEEE 802.1xを実行するには、EAP認証システム証明書がEAP-TLSフロー中にエンドポイント/クライアントに提示されるサーバ証明書として使用され

るため、EAP認証システム証明書に対してアクションを実行します。その結果、TLSトンネル内でセキュリティが確保されます。開始するには、CSRを作成してEAP認証システム証明書を作成し、組織内（またはパブリックCAプロバイダー）のCAサーバを管理する担当者に署名を依頼します。最終的に、CSRにバインドされ、次の手順でISEに関連付けられるCA署名付き証明書が作成されます。

証明書署名要求(CSR)フォームで、次のオプションを選択してCSRを完了し、その内容を取得します。

- この設定例では、Certificate Usageを選択します。 **EAP Authentication**を参照。
- 証明書でワイルドカード文を使用する場合は、 ***.example.com**を使用している場合は、 **Allow Wildcard Certificate** チェックボックスをオンにします。最適な場所は、環境内に存在する可能性がある複数の異なるタイプのエンドポイントオペレーティングシステム間での用途の互換性を確保するためのサブジェクト代替名(SAN)証明書フィールドです。
- 証明書にワイルドカードステートメントを配置しない場合は、CA署名付き証明書を関連付けるISEノード（署名後）を選択します。

  注:wildcard文を含むCA署名付き証明書をCSR内の複数のノードにバインドすると、証明書はISE導入環境内の各ISEノード（または選択したノード）に配布され、サービスを再起動できます。ただし、サービスの再起動は一度に1ノードに自動的に制限されます。サービスリスタートを監視するには、 **show application status ise** ISE CLIコマンドを使用します。

  次に、件名を定義するためのフォームに入力する必要があります。これには、共通名(CN)、組織単位(OU)、組織(O)、市(L)、州(ST)、および国(C)の証明書フィールドが含まれます。$FQDN$変数は、各ISEノードに関連付けられた管理完全修飾ドメイン名（ホスト名+ドメイン名）を表す値です。
- 「 Subject Alternative Name (SAN) また、信頼を確立するために必要な情報を入力する必要があります。要件として、証明書の署名後に、この証明書に関連付けられているISEノードのFQDNを指すDNSエントリを定義する必要があります。
- 最後に、CAサーバの機能に準拠し、優れたセキュリティ対策を念頭に置いて、適切なKey Type、Key Length、およびDigest to Sign Withを定義していることを確認します。デフォルト値は、それぞれRSA、4096ビット、SHA-384です。使用可能な選択肢と互換性は、ISE管理UI内のこのページに表示されます。

これは、ワイルドカード文を使用せずに完成したCSRフォームの例です。環境に固有の実際の値を使用していることを確認します。

Usage

Certificate(s) will be used for: EAP Authentication

Allow Wildcard Certificates: ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise	ise#EAP Authentication
☑ ise2	ise2#EAP Authentication
☑ ise3	ise3#EAP Authentication

Subject

Common Name (CN)
$FQDN$

Organizational Unit (OU)

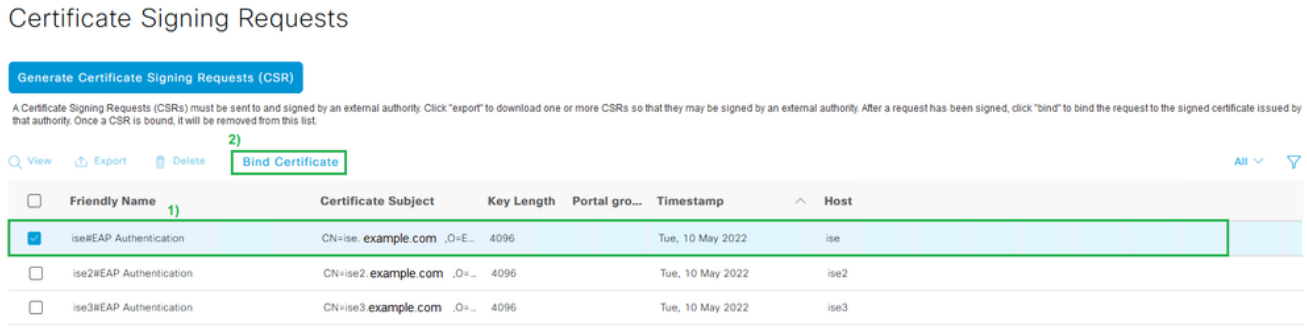
Organization (O)
Example Company

City (L)
San Jose

State (ST)
California

Country (C)
US

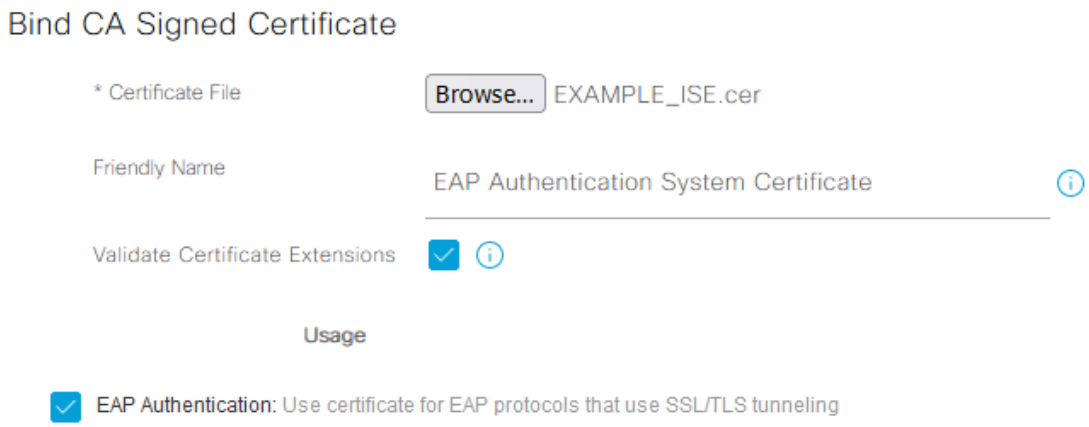
3. すべての証明書が完全なCAチェーンの一部としてISEの信頼できる証明書ストアにインポートされたら、ISE GUIに戻り、 **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**を参照。署名付き証明書に対応するFriendly Nameの下のCSRエントリを探し、証明書のチェックボックスをクリックして、 **Bind Certificate**を参照。



CSRへの証明書のバインド

注：各CSRに対して、一度に1つのCA署名付き証明書をバインドする必要があります。導入環境内の他のISEノード用に作成された残りのCSRに対して、この手順を繰り返します。

次のページで、 **Browse** 署名付き証明書ファイルを選択し、目的のフレンドリ名を定義し、証明書の使用法を選択します。送信して変更を保存します。



CSRにバインドする証明書の選択

4. この時点で、署名付き証明書がISE GUIに移動します。移動先 **Administration > System: Certificates > Certificate Management: System Certificates** CSRを作成したのと同じノードに割り当てます他のノードや他の証明書の使用についても、同じプロセスを繰り返します。

ステップ 3：エンドポイントのクライアント証明書の取得

EAP-TLSで使用するクライアント証明書を作成するには、エンドポイントで同様のプロセスを実行する必要があります。この例では、ISEでユーザ認証を実行するために、ユーザアカウントに

対して署名および発行されたクライアント証明書が必要です。Active Directory環境からエンドポイントのクライアント証明書を取得する方法の例については、「WLCとISEを使用したEAP-TLSの理解と設定」>「EAP-TLS用のクライアント」を参照してください。

エンドポイントとオペレーティングシステムのタイプが複数あるため、プロセスが多少異なる可能性があるため、追加の例は示されていません。ただし、プロセス全体は概念的には同じです。環境内の内部サーバであるか、このタイプのサービスを提供するパブリック/サードパーティ企業であるかにかかわらず、証明書に含めるすべての関連情報を含み、CAによって署名されたCSRを生成します。

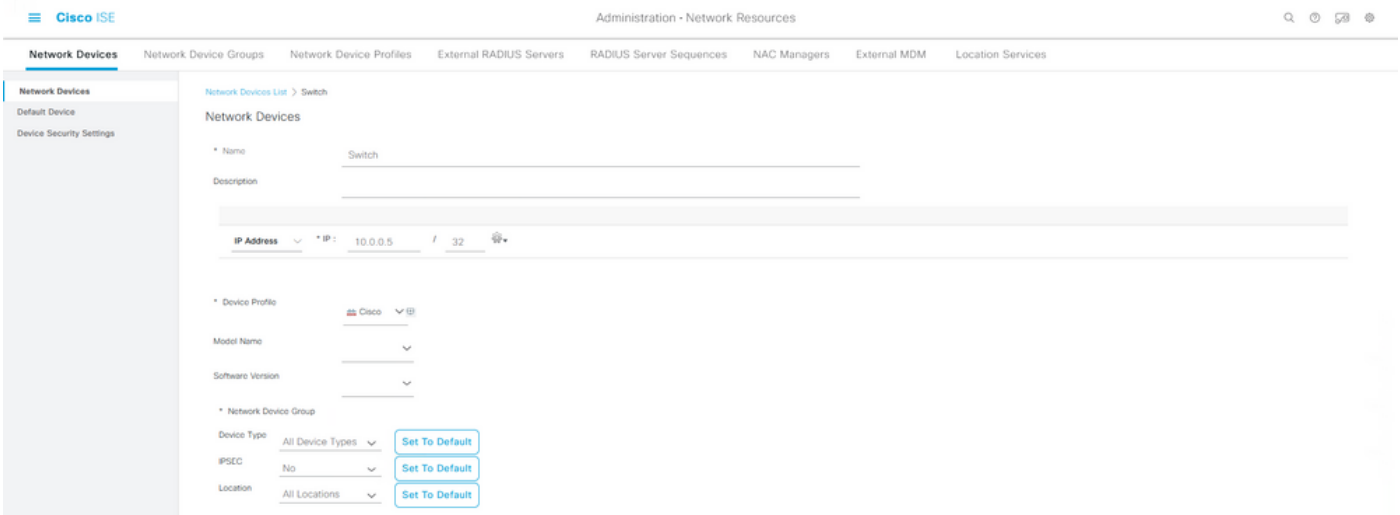
さらに、共通名(CN)証明書フィールドとサブジェクト代替名(SAN)証明書フィールドには、認証フローで使用するIDが含まれています。また、ID（マシン認証とユーザ認証、マシン認証、またはユーザ認証）の観点から、EAP-TLSに対してサプリカントを設定する方法も指定します。この例では、このドキュメントの残りの部分でユーザ認証のみを使用しています。

ネットワークデバイス

ステップ 4：ISEでのネットワークアクセスデバイスの追加

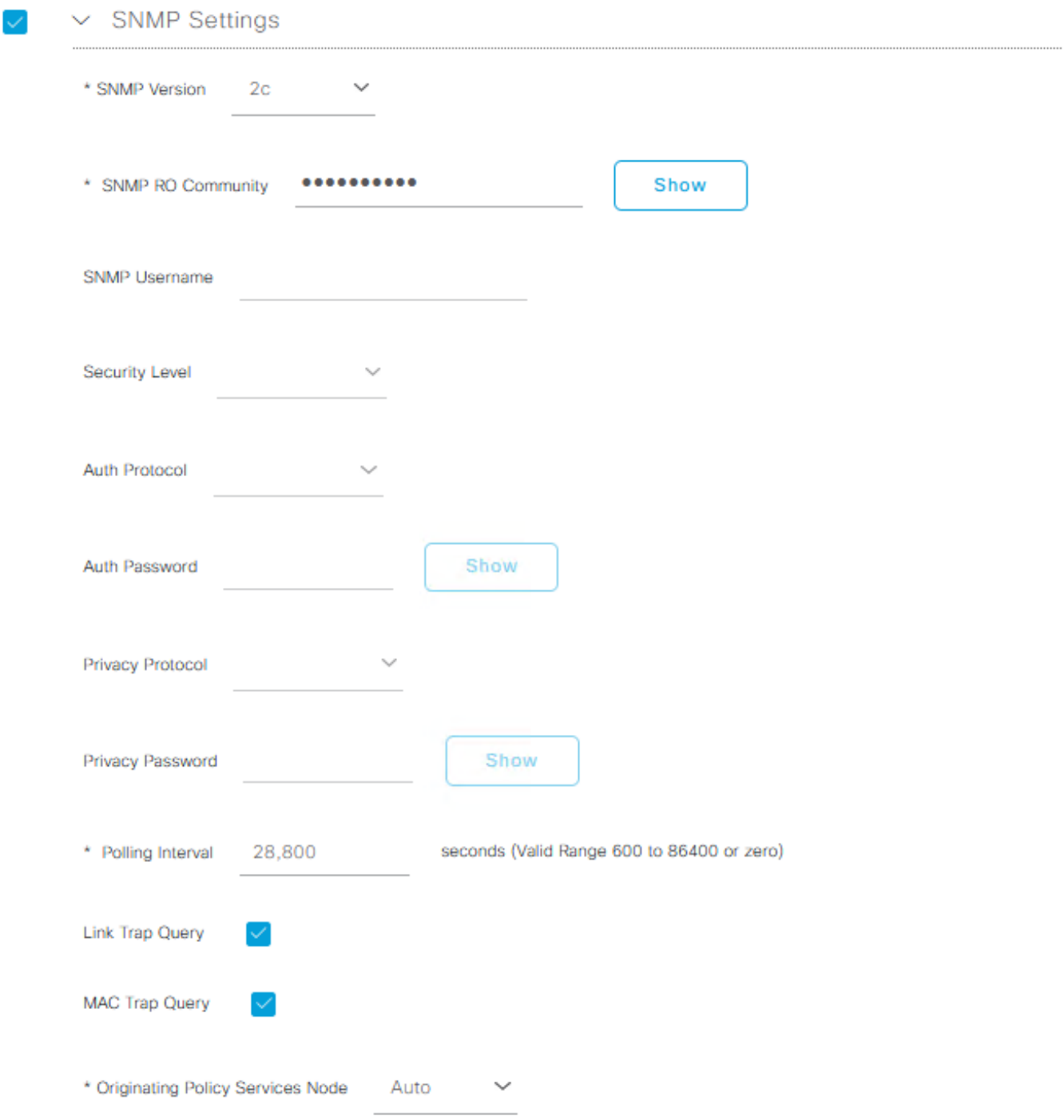
エンドポイントが接続されているネットワークアクセスデバイス(NAD)もISEで設定されるため、RADIUS/TACACS+（デバイス管理者）通信を行うことができます。NADとISEの間では、共有秘密/パスワードが信頼のために使用されます。

ISE GUIを使用してNADを追加するには、 **Administration > Network Resources: Network Devices > Network Devices** をクリックして **Add**を参照してください。



ネットワークデバイスの設定例

ISEプロファイリングで使用する場合は、使用されるエンドポイントタイプを正確に決定するための属性を収集するために、ISEへのエンドポイントの認証に関与するSNMPクエリを介してISEポリシーサービスノード(PSN)がNADに接続できるように、SNMPv2c（よりセキュア）またはSNMPv3（よりセキュア）も設定する必要があります。次の例では、前の例と同じページからSNMP(v2c)を設定する方法を示します。



SNMPv2cの設定例

詳細については、『Cisco Identity Services Engine管理者ガイド、リリース3.1』の第3章「セキュアアクセス」 > 「Cisco ISEでのネットワークデバイスの定義」を参照してください。

この時点で、まだ行っていない場合は、Cisco ISEで認証および認可するために、NADですべてのAAA関連の設定を行う必要があります。

ポリシー要素

これらの設定は、認証ポリシーまたは認可ポリシーにバインドされる要素です。このガイドでは、主に各ポリシー要素が作成され、認証ポリシーまたは認可ポリシーにマッピングされます。認証/認可ポリシーへのバインドが正常に完了するまで、ポリシーは有効にならないことを理解する

ことが重要です。

ステップ 5：外部アイデンティティソースの使用

外部アイデンティティソースは、ISE認証フェーズで使用されるエンドアイデンティティ（マシンまたはユーザ）アカウントが存在するソースです。Active Directoryは通常、コンピュータアカウントに対するマシン認証や、Active Directoryのエンドユーザアカウントに対するユーザ認証をサポートするために使用されます。内部エンドポイント（内部）ソースにはコンピュータアカウント/ホスト名が保存されないため、マシン認証では使用できません。

次に、ISEでサポートされるアイデンティティソースと、各アイデンティティソースで使用できるプロトコル（認証タイプ）を示します。

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, or EAP-TTLS) LEAP	Yes	Yes	No	No
EAP-MD5 CHAP	Yes	No	No	No
EAP-TLS PEAP-TLS (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No

Identity Storeの機能

ポリシー要素の詳細については、『Cisco Identity Services Engine管理者ガイド、リリース3.1』の章「セグメンテーション」>「ポリシーセット」を参照してください。

ISEへのActive Directoryセキュリティグループの追加

ISEポリシーでActive Directoryセキュリティグループを使用するには、まずグループをActive

Directory参加ポイントに追加する必要があります。ISEのGUIで、 **Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory**を参照。

ISE 3.xとActive Directoryを統合するための詳細と要件については、Active Directory Integration with Cisco ISE 2.xを参照してください。

注：セキュリティグループをLDAPインスタンスに追加する場合も同じアクションを適用できます。ISEのGUIで、 **Administration > Identity Management: External Identity Sources > LDAP > *LDAP instance name* > tab: Groups > Add > Select Groups From Directory**を参照。

手順 6：証明書認証プロファイルの作成

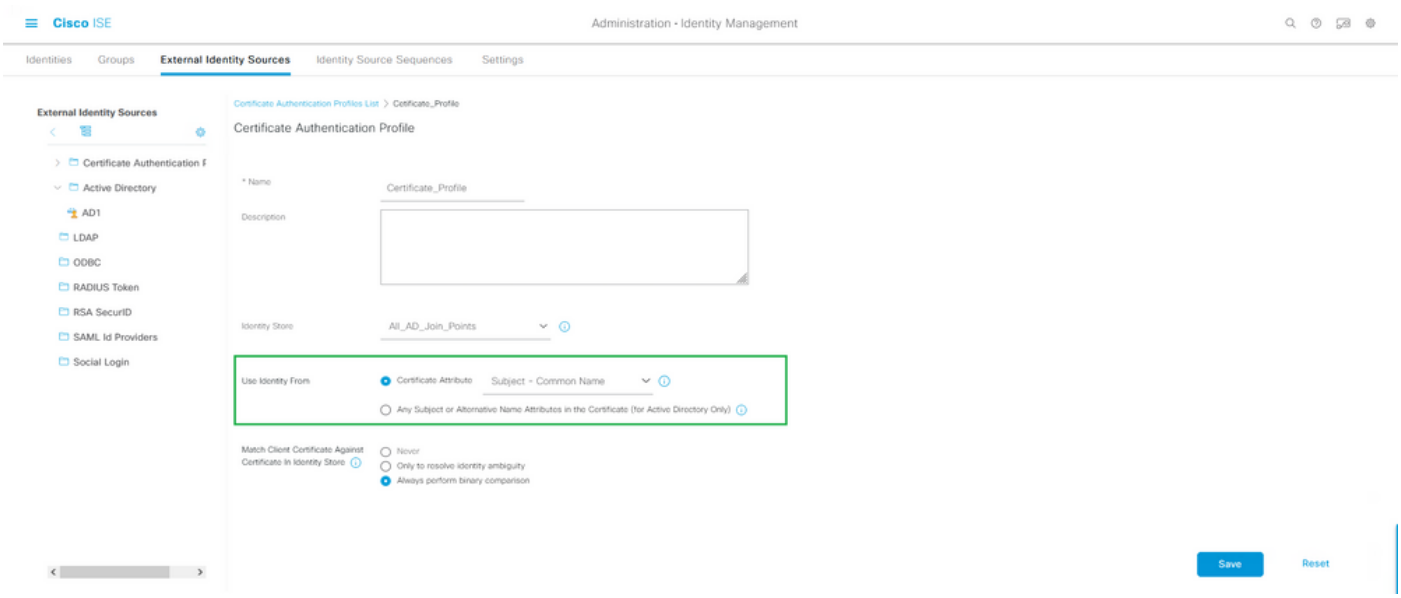
証明書認証プロファイルの目的は、EAP-TLS中（他の証明書ベースの認証方式の間も）にISEに提示されるクライアント証明書（エンドアイデンティティ証明書）でID（マシンまたはユーザ）を検出できる証明書フィールドをISEに通知することです。これらの設定は、IDを認証するために認証ポリシーにバインドされます。ISE GUIから、次の順に移動します **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** をクリックして **Add**を参照。

Use Identity Fromは、IDを検索できる特定のフィールドの証明書属性を選択するために使用します。選択できる基準は、次のとおりです。

> Subject - Common Name
> Subject Alternative Name
> Subject - Serial Number
> Subject
> Subject Alternative Name - Other Name
> Subject Alternative Name - EMail
> Subject Alternative Name - DNS

IDストアがActive Directory(AD)またはLDAP（外部IDソース）をポイントしている場合は、バイナリ比較と呼ばれる機能を使用できます。バイナリ比較は、ISE認証フェーズで行われるUse Identity From選択からクライアント証明書から取得したActive Directory内のIDのルックアップを実行します。バイナリ比較を使用しない場合、IDはクライアント証明書から取得され、Active Directory外部グループが条件として使用されるISE認証フェーズまたはISEに対して外部で実行する必要があるその他の条件まで、Active Directoryで検索されません。バイナリ比較を使用するには、IDストアで、エンドIDアカウントを検索できる外部アイデンティティソース（Active DirectoryまたはLDAP）を選択します。

次に、バイナリ比較を有効にして（オプション）、クライアント証明書のCommon Name(CN)フィールドにIDがある場合の設定例を示します。



証明書認証プロファイル

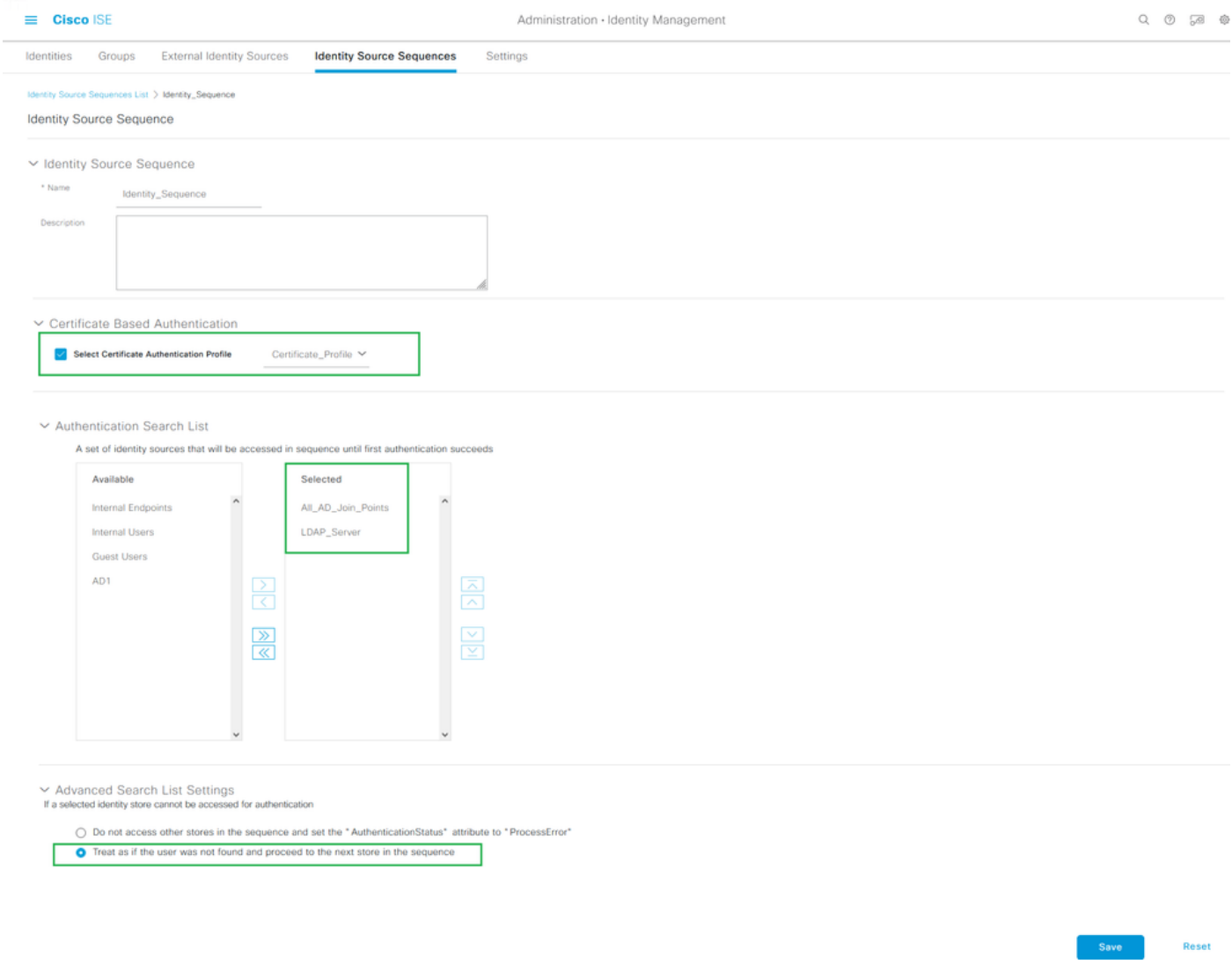
詳細については、『Cisco Identity Services Engine管理者ガイド、リリース3.1』 >章：基本設定> Cisco ISE CAサービス>個人所有デバイスの認証に証明書を使用するためのCisco ISEの設定> TLSベース認証の証明書認証プロファイルの作成を参照してください。

手順 7：アイデンティティソースシーケンスへの追加

IDソースシーケンスは、ISE GUIから作成できます。移動先 **Administration > Identity Management**を参照。通常の **Identity Source Sequences** をクリックし、 **Add**を参照。

次の手順では、証明書認証プロファイルをアイデンティティソースシーケンスに追加します。これにより、複数のActive Directory結合ポイントを含めたり、内部/外部アイデンティティソースの組み合わせを必要に応じてグループ化したりすることができ、アイデンティティソースシーケンスの下の認証ポリシーにバインドできます **Use** カラム.

次に示す例では、最初にActive Directoryに対してルックアップを実行し、ユーザが見つからない場合は次にLDAPサーバを検索します。複数のアイデンティティ・ ソースの場合は、必ず **Treat as if the user was not found and proceed to the next store in the sequence** チェックボックスをオンにします。これにより、認証要求中に各アイデンティティソース/サーバがチェックされます。



アイデンティティソースシーケンス

それ以外の場合は、証明書認証プロファイルだけを認証ポリシーにバインドすることもできます。

ステップ 8：許可されるプロトコルサービスの定義

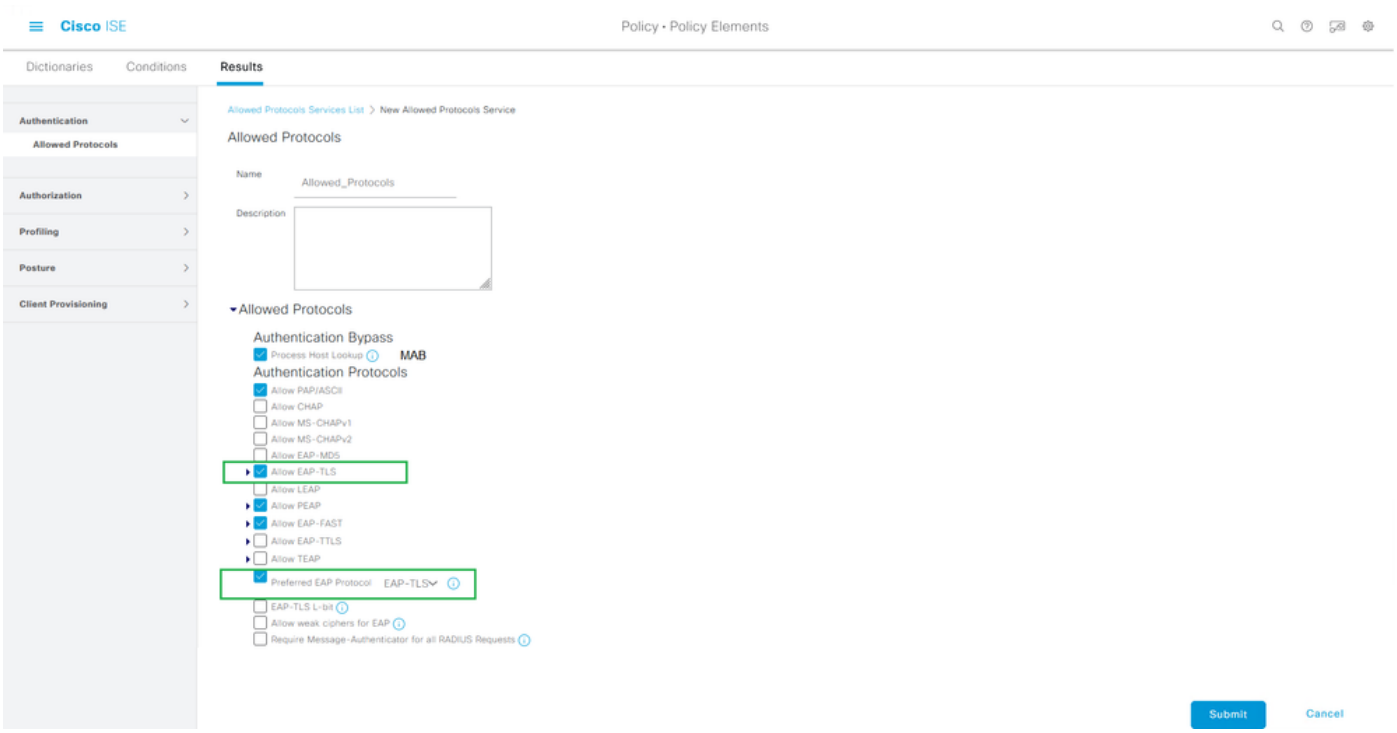
Allowed Protocols Serviceは、RADIUS認証中にISEがサポートする認証方式/プロトコルのみを有効にします。ISE GUIから設定するには、Policy > Policy Elements: Results > Authentication > Allowed Protocolsの順に移動し、要素として認証ポリシーにバインドします。

注:「認証バイパス> Process Host Lookup」は、ISEで有効にされたMABに関連しています。

これらの設定は、サプリカント（エンドポイント）でサポートおよび設定されているものと同じである必要があります。そうしないと、認証プロトコルが期待どおりにネゴシエートされず、RADIUS通信が失敗する可能性があります。実際のISE設定では、ISEとサプリカントがネゴシエートして期待どおりに認証できるように、環境で使用されている任意の認証プロトコルを有効にすることが推奨されます。

これらは、許可されたプロトコルのサービスの新しいインスタンスが作成されたときのデフォルト値（折りたたまれた）です。

注：この設定例では、ISEとサプリカントがEAP-TLS経由で認証を行うため、少なくともEAP-TLSを有効にする必要があります。



エンドポイントサプリカントへの認証要求中にISEが使用できるようにするプロトコル

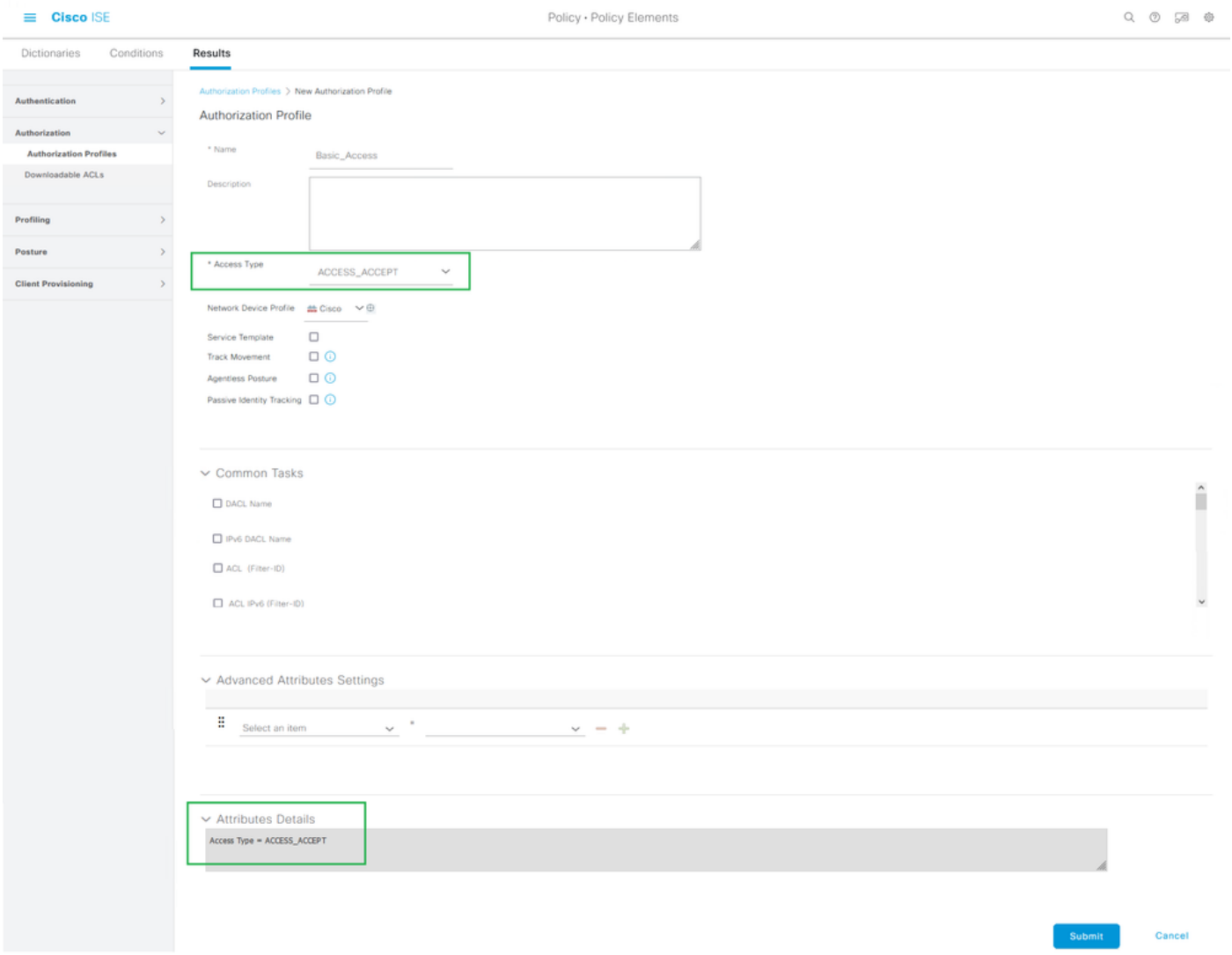
注:EAP-TLSの値に設定された優先EAPプロトコルを使用すると、ISEはエンドポイントIEEE 802.1xサプリカントに提供される最初のプロトコルとしてEAP-TLSプロトコルを要求します。この設定は、ISEで認証されるほとんどのエンドポイントでEAP-TLSを使用して頻繁に認証する場合に役立ちます。

ステップ 9：許可プロファイルの作成

構築する必要がある最後のポリシー要素は認可プロファイルです。認可プロファイルは認可ポリシーにバインドされ、必要なアクセスレベルを提供します。認可プロファイルは認可ポリシーにバインドされます。ISE GUIから設定するには、 **Policy > Policy Elements: Results > Authorization > Authorization Profiles** をクリックして **Add**を参照。

許可プロファイルには、特定のRADIUSセッションのためにISEからNADに渡される属性を生成する設定が含まれており、これらの属性は必要なレベルのネットワークアクセスを実現するために使用されます。

ここに示すように、これは単にアクセスタイプとしてRADIUS Access-Acceptを渡すだけですが、初期認証の際に追加の項目を使用できます。一番下にあるAttribute Detailsには、特定の認可プロファイルに一致したときにISEがNADに送信する属性の要約が含まれています。



許可プロファイル – ポリシー要素

ISE認可プロファイルおよびポリシーの詳細については、『Cisco Identity Services Engine管理者ガイド、リリース3.1』の「章：セグメンテーション」>「認可ポリシー」を参照してください。

セキュリティポリシー

認証ポリシーと認可ポリシーはISE GUIから作成され、 **Policy > Policy Sets**を参照。これらはISE 3.xではデフォルトで有効になっています。ISEをインストールする際には、常に1つのポリシーセット（デフォルトのポリシーセット）が定義されています。デフォルトのポリシーセットには、事前定義されたデフォルトの認証、許可、および例外のポリシールールが含まれています。

ポリシーセットは階層的に設定されるため、ISE管理者は、意図的に類似のポリシーをグループ化して、認証要求内で使用できるように異なるセットを作成できます。カスタマイズとグループ化のポリシーは事実上無制限です。そのため、1つのポリシーセットをネットワークアクセス用のワイヤレスエンドポイント認証に使用し、別のポリシーセットをネットワークアクセス用の有線エンドポイント認証に使用したり、ポリシーを管理する独自の差別化された方法に使用したりできます。

Cisco ISEはポリシーセットを評価でき、内部のポリシーはトップダウンアプローチを使用して、特定のポリシーセットのすべての条件がTrueであると評価された場合に、最初に特定のポリシー

セットに一致します。ISEは次のように、さらにポリシーセットに一致した内部の認証ポリシーと認可ポリシーを評価します。

1. ポリシー・セットおよびポリシー・セットの条件の評価
2. 一致したポリシーセット内の認証ポリシー
3. 許可ポリシー – ローカルの例外
4. 許可ポリシー – グローバル例外
5. 許可ポリシー

ポリシー例外は、すべてのポリシーセットに対してグローバルに、または特定のポリシーセット内でローカルに存在します。これらのポリシー例外は、許可ポリシーの一部として処理されます。これは、特定の一時的なシナリオでネットワークアクセスに与えられる許可または結果を処理するためです。

次のセクションでは、ISE認証および認可ポリシーにバインドしてEAP-TLS経由でエンドポイントを認証するための設定およびポリシー要素を組み合わせる方法について説明します。

ステップ 10：ポリシーセットの作成

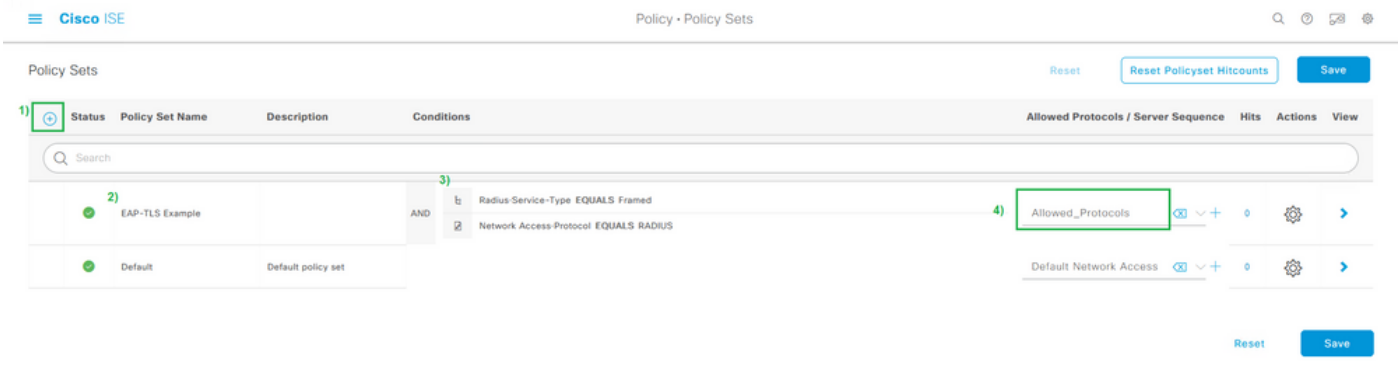
ポリシーセットは、ネットワークアクセスに許可されるプロトコルまたはサーバーの順序を示す単一のユーザー定義ルール、および認証ポリシー、承認ポリシー、ポリシー例外で構成される階層コンテナです。これらはすべて、ユーザー定義の条件ベースのルールで構成されます。

ISE GUIからポリシーセットを作成するには、 **Policy > Policy Set** 次の図に示すように、左上隅のプラス(+) アイコンをクリックします。

新しいポリシーセットの追加

ポリシーセットは、以前に設定されたこのポリシー要素をバインド/結合でき、特定のRADIUS認証要求(Access-Request)でどのポリシーセットが一致するかを決定するために使用されます。

- バインド：許可されたプロトコルサービス



ポリシーセットの条件と許可されるプロトコルリストの定義

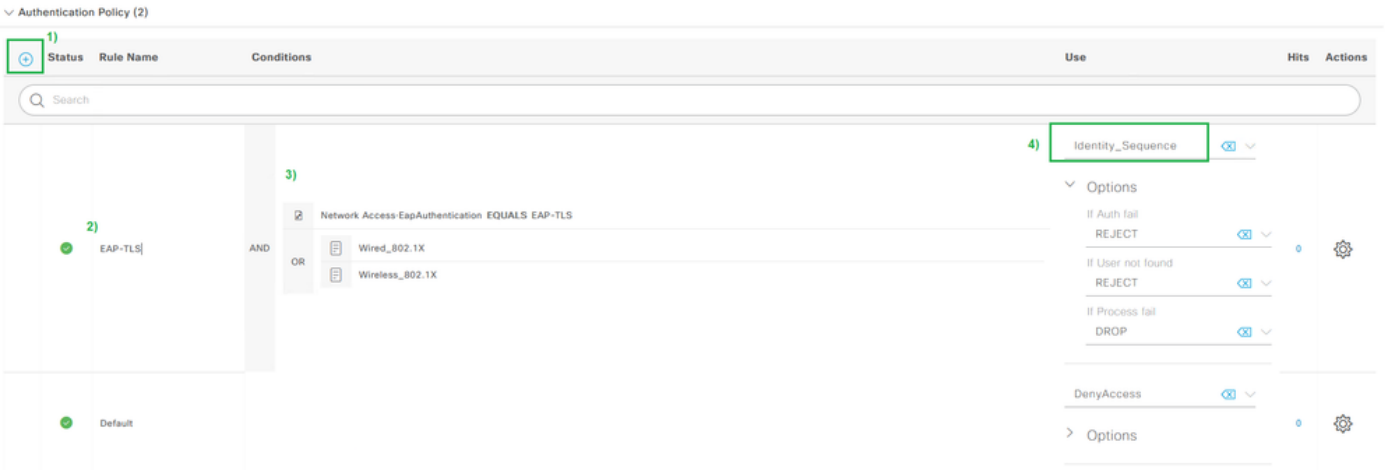
この例では、RADIUSプロトコルを再適用するために冗長性が確保されている可能性がある場合でも、RADIUSセッションに表示される特定の属性および値を使用してIEEE 802.1x（フレーム化属性）を適用します。最適な結果を得るには、ネットワークデバイスグループや有線802.1x、ワイヤレス802.1x、または有線802.1xとワイヤレス802.1xの両方に固有のものなど、目的に適した一意のRADIUSセッション属性のみを使用します。

ISEのポリシーセットの詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.1』の「Chapter: Segmentation > Policy Sets」、「Authentication Policies」、および「Authorization Policies」の各セクションを参照してください。

ステップ 11認証ポリシーの作成

ポリシーセット内で、認証ポリシーは、以前に使用するように設定されたこれらのポリシー要素を条件とバインド/結合して、認証ルールが一致するタイミングを決定します。

- バインド：証明書認証プロファイルまたはアイデンティティソースシーケンス。

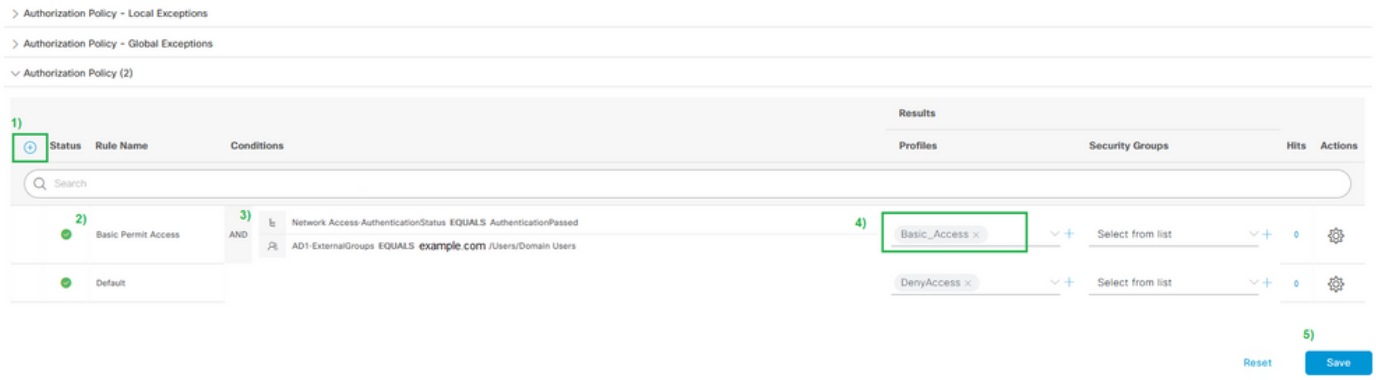


認証ポリシールールの例

ステップ 12認可ポリシーの作成

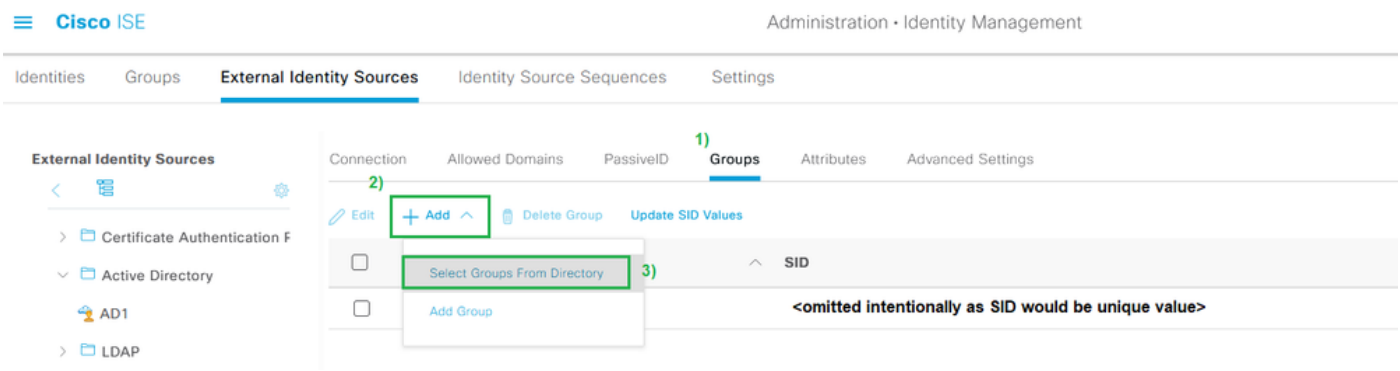
ポリシーセット内で、許可ポリシーは、以前に使用するように設定されたこれらのポリシー要素を条件とバインド/結合して、許可ルールが一致するタイミングを決定します。次の例では、Active DirectoryのDomain Usersセキュリティグループが条件で指定されているため、ユーザ認証が行われています。

- バインド：許可プロファイル

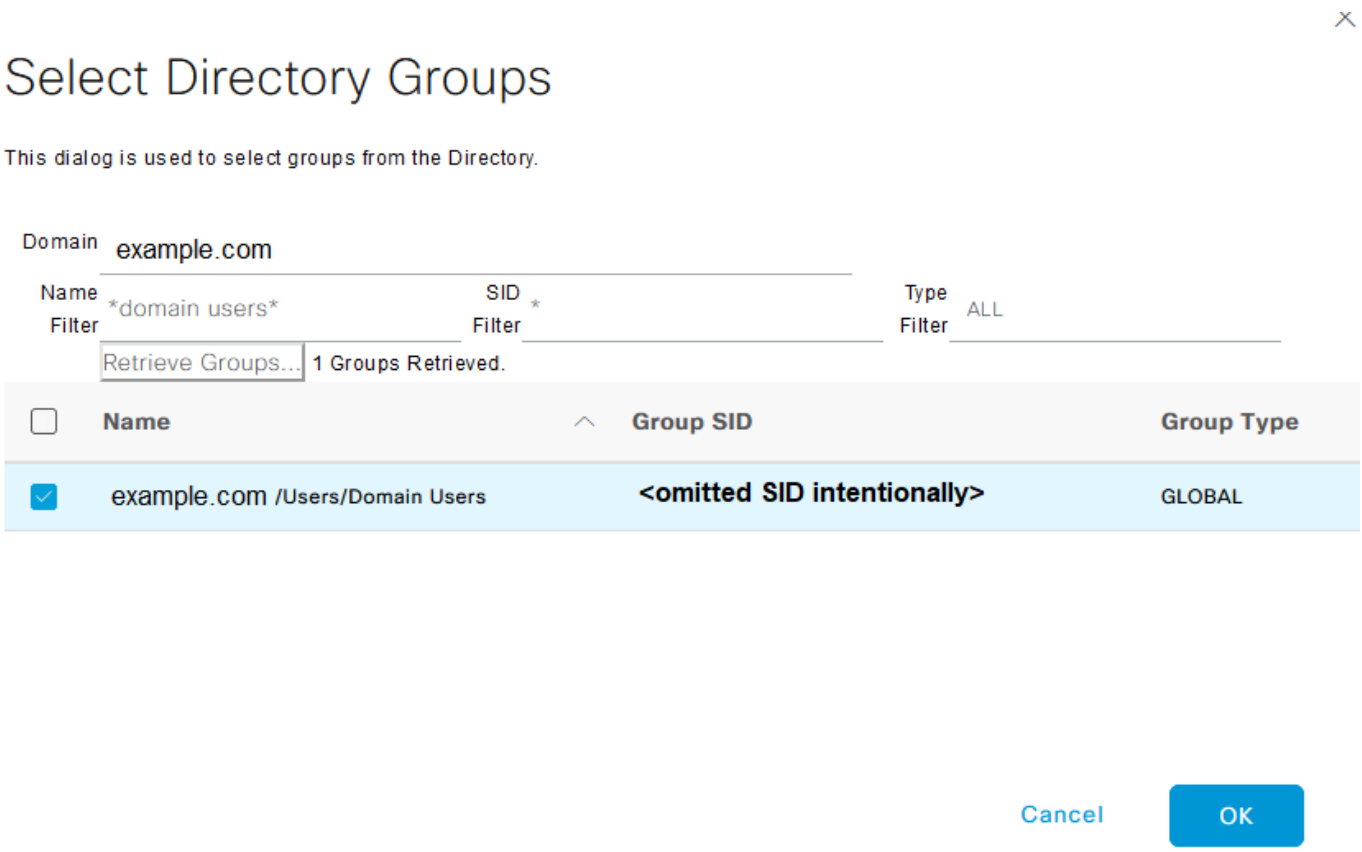


許可ポリシールールの例

（Active DirectoryやLDAPなどから）外部グループを追加するには、外部サーバインスタンスからグループを追加する必要があります。この例では、ISE UIから取得します。 **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups**を参照。Groupタブから、次のコマンドを選択します。 **Add > Select Groups from Directory** 名前フィルタを使用して、すべてのグループ(*)または特定のグループ(グループを取得するドメインユーザ(*domain users*)など)を検索します。



ISEポリシーで外部グループを使用するには、ディレクトリからグループを追加する必要があります



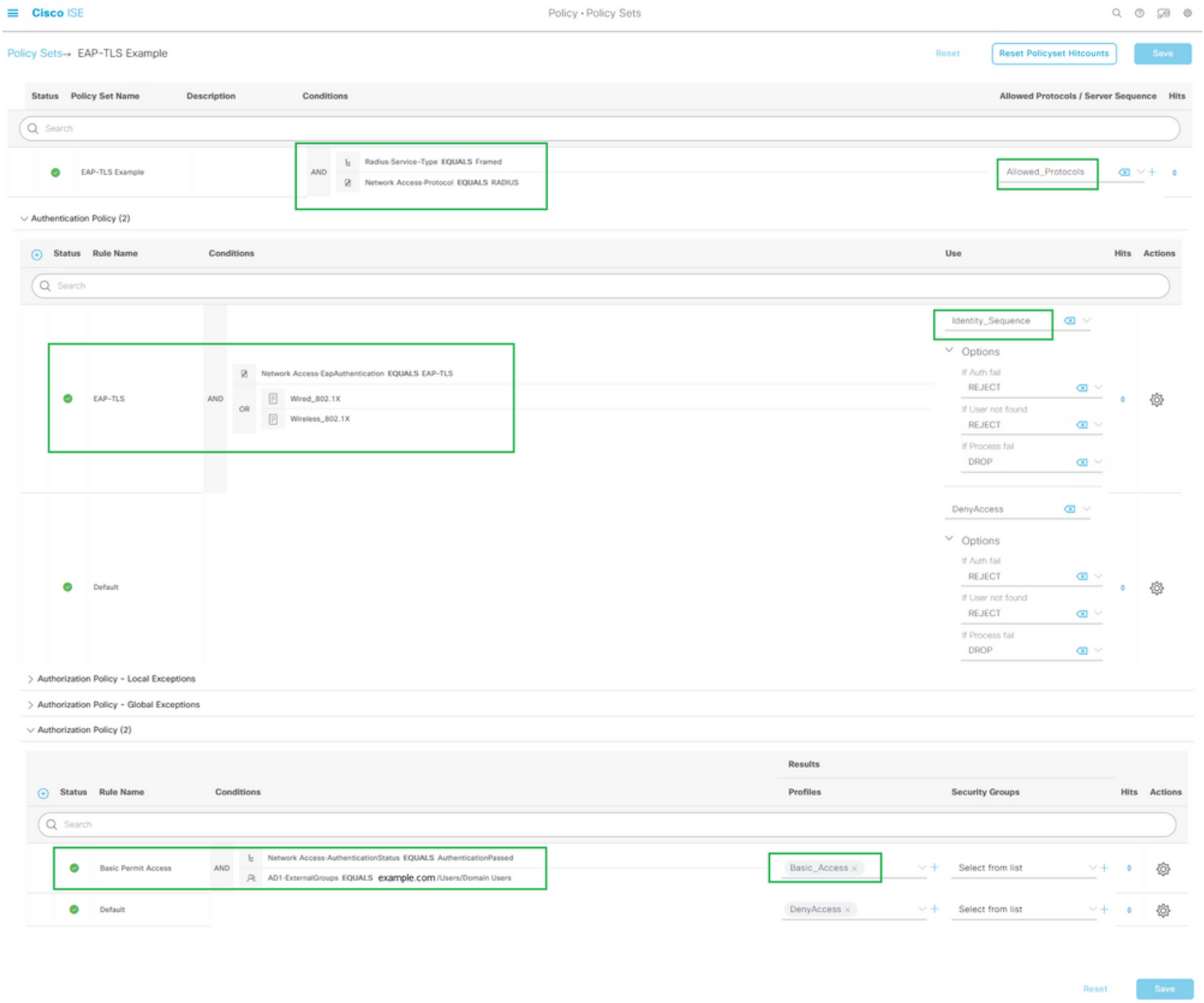
外部ディレクトリ内の検索 – Active Directoryの例

各グループの横にあるチェックボックスをオンにすると、ISE内のポリシーで使用されます。変更を保存するために、必ずOkまたはSave（あるいはその両方）をクリックしてください。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

すべてのグローバル設定とポリシー要素がポリシーセットをバインドすると、設定はEAP-TLSを介したユーザ認証の次の図のようになります。

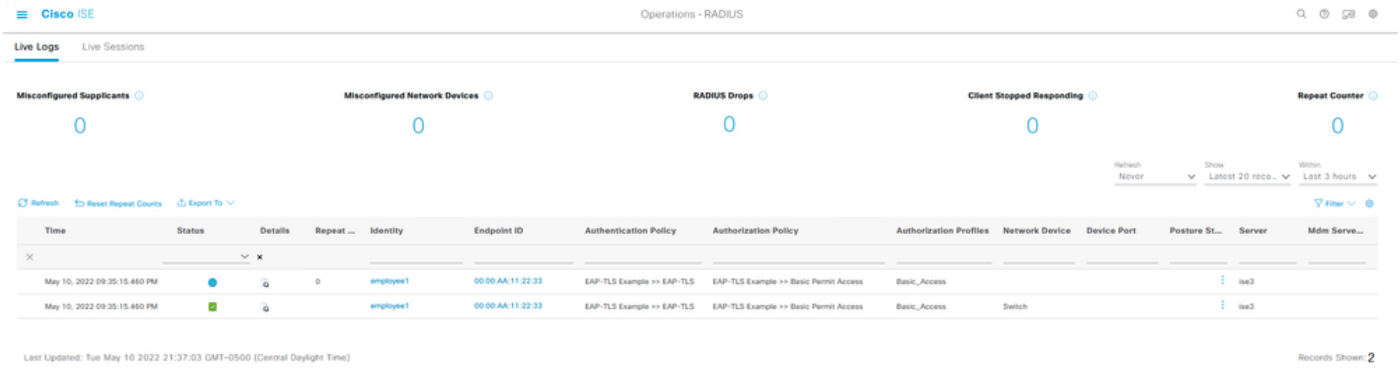


トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

設定が完了したら、エンドポイントを接続して認証をテストします。結果はISE GUIで確認できます。選択 **Operations > Radius > Live Logs**,以下の図に、出力例を示します。

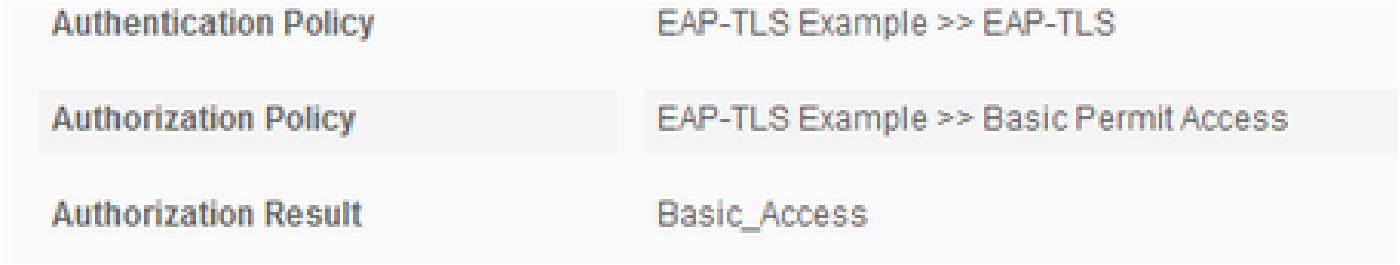
RADIUSおよびTACACS+（デバイス管理者）のライブログは、過去24時間までの認証の試行とアクティビティ、および過去100件のレコードについて確認できます。このタイプのレポートデータをこの時間枠を超えて表示する場合は、レポートを使用する必要があります。具体的には、次の手順を実行します。 **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications**を参照。



Radius >ライブログからの出力例

ISEのRADIUSライブログには、RADIUSセッションに関する情報が記録されています。これには、セッション属性や、認証フロー中に観察される動作を診断するのに役立つその他の情報が含まれています。ポリシーの横の [レポート（Report）] **details** アイコンをクリックすると、セッションの詳細ビューが開き、この認証試行に固有のセッション属性と関連情報が表示されます。

トラブルシューティングを行うには、正しいポリシーが一致していることを確認することが重要です。次の図に示すように、この設定例では、目的の認証ポリシーと認可ポリシーが予想どおりに照合されます。



詳細ビューでは、次の設定例の一部として、認証が設計に従って期待どおりに動作することを確認するために、これらの属性がチェックされます。

- [Event]
  - これには、認証が成功したかどうかが含まれます。
  - 実際のシナリオでは、値は「5200 Authentication succeeded」です。

- ユーザ名
  - これには、ISEに提示されたクライアント証明書から取得されたエンドIDが含まれます。
  - 実際のシナリオでは、これはエンドポイントにログインしているユーザのユーザ名（つまり、前の図のemployee1）です。

- エンドポイントID
  - 有線/ワイヤレスの場合、この値はエンドポイントからのネットワークインターフェイスカード(NIC)のMACアドレスです。
  - 実際のシナリオでは、接続がVPN経由でない限り、これはエンドポイントのMACアドレスになります。VPN経由の場合は、エンドポイントのIPアドレスになります。

- 認証ポリシー
  - ポリシー条件に一致するセッション属性に基づいて、特定のセッションで一致した認証ポリシーを表示します。
  - 実際のシナリオでは、これは設定されている想定される認証ポリシーです。
  - 別のポリシーが表示される場合は、ポリシーの条件と比較したときに予期されたポリシーがtrueと評価されなかったことを意味します。この場合は、セッション属性を確認し、各ポリシーに異なる一意の条件が含まれていることを確認します。

- 認可ポリシー
  - ポリシー条件に一致するセッション属性に基づいて、特定のセッションで一致した認可ポリシーを表示します。
  - 実際のシナリオでは、これは設定されている予想される認可ポリシーです。
  - 別のポリシーが表示される場合は、ポリシー内の条件と比較した際に予想されるポリシーがtrueとして評価されなかったことを意味します。この場合は、セッション属性を確認し、各ポリシーに異なる一意の条件が含まれていることを確認します。

- 許可結果
  - 一致した認可ポリシーに基づいて、特定のセッションで使用された認可プロファイルが表示されます。
  - 稼働中のシナリオでは、これはポリシーで設定された値と同じです。監査の目的で確認し、正しい許可プロファイルが設定されていることを確認することをお勧めします。

- ポリシーサーバ
  - これには、認証の試行に関与したISEポリシーサービスノード(PSN)のホスト名が含まれます。
  - 稼働中のシナリオでは、PSNが動作していなかったり、フェールオーバーが発生したりした場合（予想より長い遅延が原因で発生した場合や、認証タイムアウトが発生した場合など）を除き、NAD（エッジデバイスとも呼ばれる）で設定された最初のPSNノードに送信される認証だけが表示されます。

- 認証メソッド
  - 特定のセッションで使用された認証方法を表示します。この例では、値はdot1xです。
  - この設定例に基づく実際のシナリオでは、値はdot1xと表示されます。別の値が表示される場合は、dot1xが失敗したか、試行されなかったことを意味している可能性があります。

- 認証プロトコル
  - 特定のセッションで使用された認証方法を表示します。この例では、値はEAP-TLSです。
  - この設定例に基づく実際のシナリオでは、値は常にEAP-TLSと表示されます。別の値が表示された場合、サプリカントとISEはEAP-TLSを正常にネゴシエートしませんでした。

- ネットワークデバイス
  - エンドポイントとISEの間の認証の試行に関係するNAD（エッジデバイスとも呼ばれ

る）のネットワークデバイス名を、ISEで設定したとおりに表示します。
    - 作業シナリオでは、ISE UIに常に次の名前が付けられます。 **Administration > System: Network Devices**. この設定に基づいて、NADのIPアドレス（エッジデバイスとも呼ばれる）を使用して、NAS IPv4アドレスセッション属性に含まれる認証の発信元ネットワークデバイスが決定されます。

これは、トラブルシューティングやその他の可視性の目的で確認する可能性のあるすべてのセッション属性の完全なリストではなく、検証が必要なその他の有用な属性もあります。すべてのセッション属性を確認して、すべての情報に慣れ始めることをお勧めします。ISEが実行する操作や動作を示すセクション「Steps」の下に右側が含まれていることがわかります。

トラブルシューティングのための一般的な問題とテクニック

このリストには、一般的な問題とトラブルシューティングのアドバイスが含まれており、完全なリストを意図したものではありません。代わりに、これをガイドとして使用し、ISEが関与する場合の問題をトラブルシューティングするための独自の手法を開発します。

問題：認証エラー(5400認証に失敗)またはその他の認証の失敗が発生しました。

- 認証の失敗が発生した場合は、detailsアイコンをクリックして、認証が失敗した理由と実行した手順に関する情報を表示します。これには、障害の原因と考えられる根本原因が含まれます。

- ISEは認証結果に基づいて決定を行うため、認証の試行が失敗した理由を理解するための情報を提供します。

問題：認証が正常に完了せず、エラーの理由は「5440エンドポイントがEAPセッションを放棄し、新たに開始した」または「5411サプリカントがISEに応答しなくなった」と表示されます。

- このエラーの理由は、タイムアウトする前にRADIUS通信が完了しなかったことを示します。EAPはエンドポイントとNADの間で行われるため、NADで使用されているタイムアウトを確認し、5秒以上にわたって設定されていることを確認する必要があります。

- この問題を解決するのに5秒では不十分な場合は、この手法でこの問題が解決するかどうかを確認するために、5秒ずつ数回増やして再テストすることを推奨します。

- 前の手順で問題が解決されない場合は、認証が同じ正しいISE PSNノードで処理され、全体的な動作がNADとISE PSNノード間の通常の遅延よりも大きいなどの異常な動作を示していないことを確認することをお勧めします。

- また、ISEがクライアント証明書を受信しない場合、エンドポイント（ユーザ証明書）はISE EAP認証証明書を信頼できないため、エンドポイントがパケットキャプチャを使用してクライアント証明書を送信するかどうかを確認することをお勧めします。trueであることが判明した場合は、正しい証明書ストア（ルートCA =信頼されたルートCA）にCAチェーンをインポートします | 中間CA =信頼された中間CA)。

問題：認証は成功するが、正しい認証または認可ポリシーに一致しない。

- 認証リクエストが成功しても、正しい認証または認可ルールに一致しない場合は、セッション属性を確認して、使用されている条件が正確で、RADIUSセッションに存在することを確認することをお勧めします。

- ISEは、これらのポリシーをトップダウンアプローチから評価します（ポスチャポリシーを除く）。最初に、一致したポリシーが、一致させる目的のポリシーよりも上または下であるかどうかを判断する必要があります。認証ポリシーは、最初に、認可ポリシーとは独立して評価されます。認証ポリシーが正しく一致している場合は、右側の「Steps」というセクションの「Authentication Details」に「Authentication Passed」22037示されています。

- 目的のポリシーが一致したポリシーより上にある場合、これは目的のポリシーの条件の合計が真と評価されなかったことを意味します。条件とセッションのすべての属性と値を確認して、存在し、スペルの間違いがないことを確認します。

- 目的のポリシーが一致したポリシーの下にある場合は、目的のポリシーの代わりに別のポリシー（上記）が一致したことを意味します。これは、条件値が十分に特定されていない、条件が別のポリシーで重複している、またはポリシーの順序が正しくないことを意味します。トラブルシューティングがより困難になる一方で、目的のポリシーが一致しなかった理由を判断するために、ポリシーのレビューを開始することをお勧めします。これは、次に行うアクションを特定するのに役立ちます。

問題：認証中に使用されたIDまたはユーザ名が予期された値ではありませんでした。

- これが発生した場合、エンドポイントがクライアント証明書を送信すると、ISEが証明書認証テンプレートで正しい証明書フィールドを使用しない可能性があります。証明書認証テンプレートは認証フェーズで評価されます。

- クライアント証明書を確認して、目的のIDまたはユーザ名が存在する正確なフィールドを見つけ、同じフィールドが次の中から選択されていることを確認します。 **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy)**を参照。

問題：クライアント証明書チェーンに不明なCAが存在す12514ため、EAP-TLSがSSL/TLSハンドシェイクに失敗するという失敗の理由で認証が成功しません。

- これは、ISE UIで信頼されていない証明書がクライアント証明書のCAチェーンにある場合に発生する可能性があります。 **Administration > System: Certificates > Trusted Certificates**を参照。

- これは通常、（エンドポイント上の）クライアント証明書に、EAP認証用にISEに署名された証明書CAチェーンとは異なるCAチェーンがある場合に発生します。

- 解決するには、クライアント証明書CAチェーンがISEで信頼され、ISE EAP認証サーバ証明書CAチェーンがエンドポイントで信頼されていることを確認します。

- Windows OSおよびChromeの場合は、 **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates**を参照。
- Firefoxの場合：Webサーバに対して信頼されるCAチェーン（エンドアイデンティティ証明書ではない）をインポートします。

関連情報

- Cisco Identity Services Engine >インストールおよびアップグレードガイド
- Cisco Identity Services Engine >設定ガイド
- Cisco Identity Services Engine >互換性情報
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：セキュアアクセス> Cisco ISEでのネットワークデバイスの定義
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：セグメンテーション>ポリシーセット
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：セグメンテーション>認証ポリシー
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：セグメンテーション>許可ポリシー
- Cisco Identity Services Engine > Configuration Guides > Active DirectoryとCisco ISE 2.xの統合
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：セグメンテーション>ネットワークアクセスサービス>ユーザのネットワークアクセス
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：基本設定> Cisco ISEでの証明書管理
- Cisco Identity Services Engine管理者ガイド、リリース3.1 >章：基本設定> Cisco ISE CAサービス>個人デバイスの認証に証明書を使用するためのCisco ISEの設定> TLSベース認証の証明書認証プロファイルの作成
- Cisco Identity Services Engine > Configuration Examples and TechNotes > ISE 2.0証明書プロビジョニングポータルの設定
- Cisco Identity Services Engine >設定例とテクニカルノート> ISEでのサードパーティCA署名付き証明書のインストール
- ワイヤレスLAN(WLAN) >設定例とテクニカルノート> WLCとISEを使用したEAP-TLSの理解と設定
- テクニカル サポートとドキュメント - Cisco Systems

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。