Configuration de l'authentification EAP-TLS avec ISE

Contenu

Introduction

Ce document décrit la configuration initiale comme un exemple pour introduire l'authentification EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) avec Cisco Identity Services Engine (ISE). L'accent est mis sur la configuration ISE qui peut être appliquée à plusieurs scénarios, tels que (sans s'y limiter) l'authentification avec un téléphone IP/terminal connecté via un réseau filaire ou sans fil.

Pour la portée de ce guide, il est important de comprendre ces phases du flux d'authentification ISE (RADIUS) :

- Authentification - Identifiez et validez l'identité finale (ordinateur, utilisateur, etc.) qui demande l'accès au réseau.

- Autorisation : déterminez les autorisations/accès que l'identité finale recevra sur le réseau.
- Comptabilité : création de rapports et suivi de l'activité réseau de l'identité finale une fois l'accès au réseau obtenu.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du flux de communications EAP et RADIUS.
- Connaissances de base de l'authentification RADIUS avec méthodes d'authentification basées sur certificat en termes de flux de communication.
- Compréhension des différences entre Dot1x et MAC Authentication Bypass (MAB).
- Compréhension de base de l'infrastructure à clé publique (PKI).
- Connaissance de la manière d'obtenir des certificats signés auprès d'une autorité de certification (CA) et de gérer les certificats sur le ou les terminaux.
- Configuration des paramètres relatifs à l'authentification, l'autorisation et la comptabilité (AAA) (RADIUS) sur un périphérique réseau (filaire ou sans fil).
- Configuration du demandeur (sur le terminal) à utiliser avec RADIUS/802.1x.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE version 3.x.
- Autorité de certification : pour émettre des certificats (il peut s'agir d'une autorité de certification d'entreprise, d'une autorité de certification tierce/publique ou du portail d'approvisionnement de certificats).
- Active Directory (source d'identité externe) - depuis Windows Server ; où compatible avec ISE.
- Network Access Device (NAD) : peut être un commutateur (filaire) ou un contrôleur LAN sans fil (WLC) (sans fil) configuré pour 802.1x/AAA.
- Terminal : certificats délivrés à l'identité (utilisateur) et à la configuration du demandeur qui seront authentifiés pour l'accès au réseau via RADIUS/802.1x : Authentification utilisateur. Il est possible d'obtenir un certificat d'ordinateur, mais il n'est pas utilisé dans cet exemple.

> **Note**: Comme ce guide utilise ISE version 3.1, toutes les références de documentation sont basées sur cette version. Cependant, une configuration identique ou similaire est possible et entièrement prise en charge sur les versions antérieures de Cisco ISE.

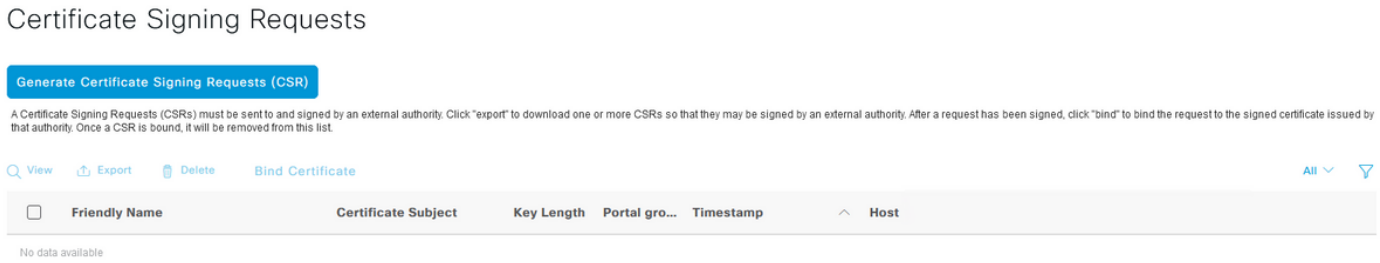
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

Obtenir des certificats serveur et client

Étape 1 : génération d'une demande de signature de certificat à partir d'ISE

La première étape consiste à générer une demande de signature de certificat (CSR) à partir d'ISE et à l'envoyer à l'autorité de certification (serveur) afin d'obtenir le certificat signé délivré à ISE, en tant que certificat système. Ce certificat sera présenté comme un certificat de serveur par ISE pendant l'authentification EAP-TLS. Cette opération est effectuée dans l'interface utilisateur ISE. Naviguez jusqu'à **Administration > System: Certificates > Certificate Management > Certificate Signing Requests.** Sous **Certificate Signing Requests**, cliquez sur **Generate Certificate Signing Requests (CSR)** comme le montre cette image.



Les types de certificats nécessitent différentes utilisations de clés étendues. Cette liste indique les utilisations de clés étendues requises pour chaque type de certificat :

Certificats d'identité ISE

- Multi-usage (Admin, EAP, Portal, pxGrid) - Authentification client et serveur
- Admin - Authentification du serveur
- Authentification EAP - Authentification serveur
- Authentification DTLS (Datagram Transport Layer Security) - Authentification serveur
- Portail - Authentification du serveur
- pxGrid - Authentification client et serveur
- Security Assertion Markup Language (SAML) - Certificat de signature SAML
- Service de messagerie ISE : générez un certificat de signature ou un nouveau certificat de messagerie

Par défaut, le certificat système « ISE Messaging Service » est destiné à la réplication des données sur chaque noeud ISE du déploiement, de l'enregistrement du noeud et d'autres communications entre noeuds. Il est présent et émis par le serveur de l'autorité de certification interne ISE (interne à ISE). Aucune action n'est requise avec ce certificat.

Le certificat système « Admin » est utilisé pour identifier chaque noeud ISE, par exemple lorsque l'API associée à l'interface utilisateur Admin (Gestion) est utilisée, et pour certaines communications entre noeuds. Afin de configurer ISE pour la première fois, mettez en place le certificat système « Admin ». Cette action n'est pas directement liée à ce guide de configuration.

Afin d'exécuter IEEE 802.1x via EAP-TLS (authentification basée sur certificat), prenez des mesures pour le certificat système "EAP Authentication" car il sera utilisé comme certificat de serveur présenté au point d'extrémité/client pendant le flux EAP-TLS ; le résultat sera sécurisé à l'intérieur du tunnel TLS. Pour commencer, créez un CSR pour créer le certificat système « Authentification EAP » et donnez-le au personnel qui gère le ou les serveurs AC dans votre organisation (ou le fournisseur AC public) pour signature. Le résultat final sera le certificat CA-Signed qui sera lié au CSR et associé à ISE avec ces étapes.

Dans le formulaire de demande de signature de certificat (CSR), choisissez ces options afin de compléter le CSR et d'obtenir son contenu :

- Utilisation du certificat, pour cet exemple de configuration, choisissez **EAP Authentication**.

- Si vous prévoyez d'utiliser une instruction générique dans le certificat, ***.example.com**, vous devez également vérifier la **Allow Wildcard Certificate** de l'Aide. Le meilleur emplacement est le champ de certificat Autre nom de l'objet (SAN) pour la compatibilité pour toute utilisation et sur plusieurs types différents de systèmes d'exploitation de terminaux qui peuvent être présents dans l'environnement.

- Si vous n'avez pas choisi de placer une instruction générique dans le certificat, choisissez les noeuds ISE auxquels vous souhaitez associer le certificat CA-Signed (après la signature). Note: Lorsque vous liez le certificat signé par l'autorité de certification qui contient l'instruction générique à plusieurs noeuds dans le CSR, le certificat est distribué à chaque noeud ISE (ou aux noeuds sélectionnés) dans le déploiement ISE et les services peuvent redémarrer. Cependant, le redémarrage des services sera automatiquement limité à un noeud à la fois. Surveillez le redémarrage des services via le **show application status ise** Commande ISE CLI.Vous devez ensuite remplir le formulaire afin de définir l'objet. Cela inclut les champs de certificat Nom commun (CN), Unité organisationnelle (OU), Organisation (O), Ville (L), État (ST) et Pays (C). La variable *$FQDN$* est la valeur qui représente le nom de domaine complet de gestion (nom d'hôte + nom de domaine) associé à chaque noeud ISE.
- Les **Subject Alternative Name (SAN)** les champs doivent également être remplis afin d'inclure toute information requise et souhaitée à utiliser pour établir la confiance. Vous devez obligatoirement définir l'entrée DNS qui pointe vers le nom de domaine complet du ou des noeuds ISE qui seront associés à ce certificat, une fois que le certificat aura été signé.

- Enfin, assurez-vous de définir le « type de clé », la « longueur de clé » et l'« empreinte à signer » appropriés qui sont conformes aux capacités du ou des serveurs de l'autorité de certification et qui tiennent compte des bonnes pratiques de sécurité. Les valeurs par défaut sont : RSA, 4 096 bits et SHA-384, respectivement. Les choix disponibles et la compatibilité s'affichent dans cette page de l'interface utilisateur d'administration d'ISE.

Ceci est un exemple de formulaire CSR rempli sans utiliser d'instruction générique. Veillez à utiliser les valeurs réelles spécifiques à l'environnement :

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)
$FQDN$

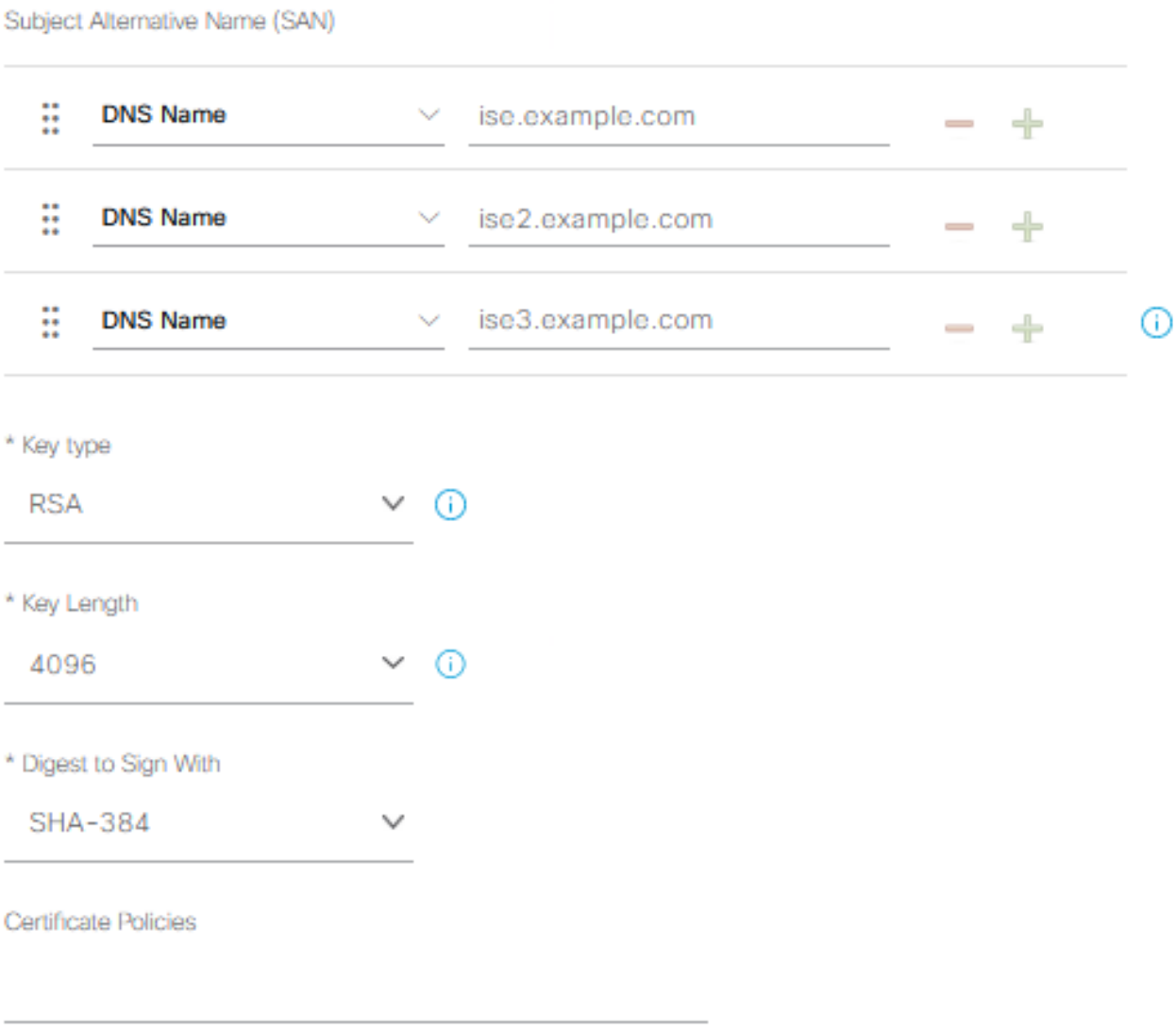
Organizational Unit (OU)

Organization (O)
Example Company

City (L)
San Jose

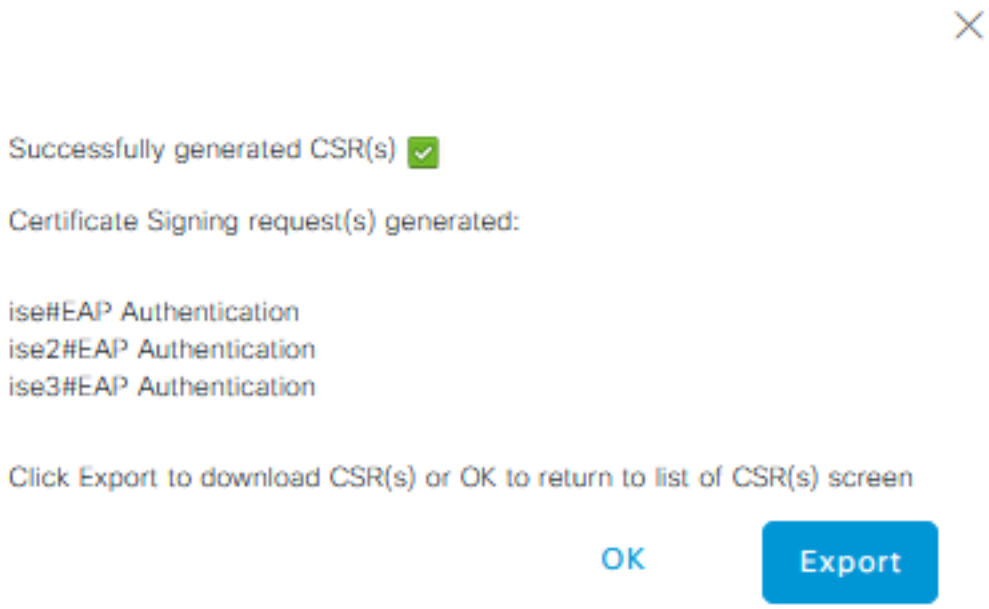
State (ST)
California

Country (C)
US



Exemple CSR

Afin d'enregistrer le CSR, cliquez sur **Generate**. Cliquer **Export**, situé en bas à droite, afin d'exporter le ou les fichiers CSR à partir de cette invite :



Exporter un exemple CSR

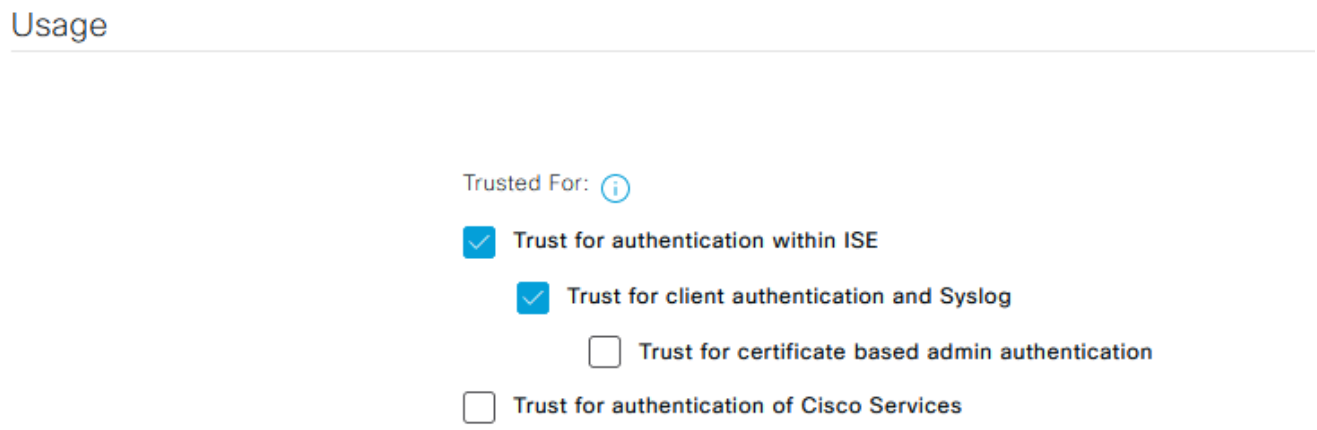
Pour plus d'informations sur les certificats à utiliser avec ISE, consultez le *Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Configuration de base > Gestion des certificats dans Cisco ISE* et installation d'un certificat CA tiers signé dans ISE.

Étape 2. Importation de certificats CA dans ISE

Une fois que l'autorité de certification renvoie le certificat signé, elle inclut également la chaîne complète de l'autorité de certification composée d'un certificat racine et d'un ou de plusieurs certificats intermédiaires. L'interface utilisateur d'administration d'ISE vous oblige à importer tous les certificats de la chaîne d'autorité de certification avant de les associer ou de les télécharger. Cela permet de s'assurer que chaque certificat système est correctement associé à la chaîne CA (également appelée certificat sécurisé) dans le logiciel ISE.

Les étapes suivantes constituent le meilleur moyen d'importer les certificats CA et le certificat système dans ISE :

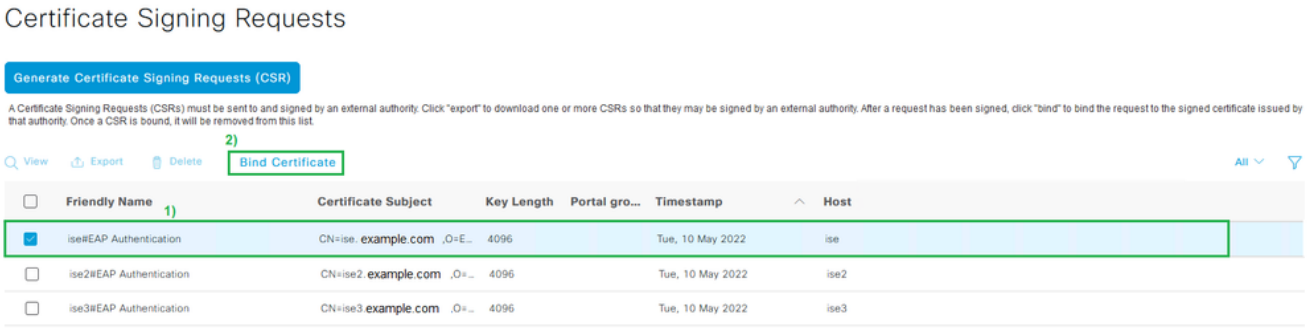
1. Afin d'importer le certificat racine dans l'interface utilisateur graphique ISE, accédez à **Administration > System: Certificates > Certificate Management**. Sous **Trusted Certificates**, cliquez sur **Import** et cochez les cases **Trust for authentication within ISE** (Infrastructure) et **Trust for client authentication et Syslog** (Endpoints).



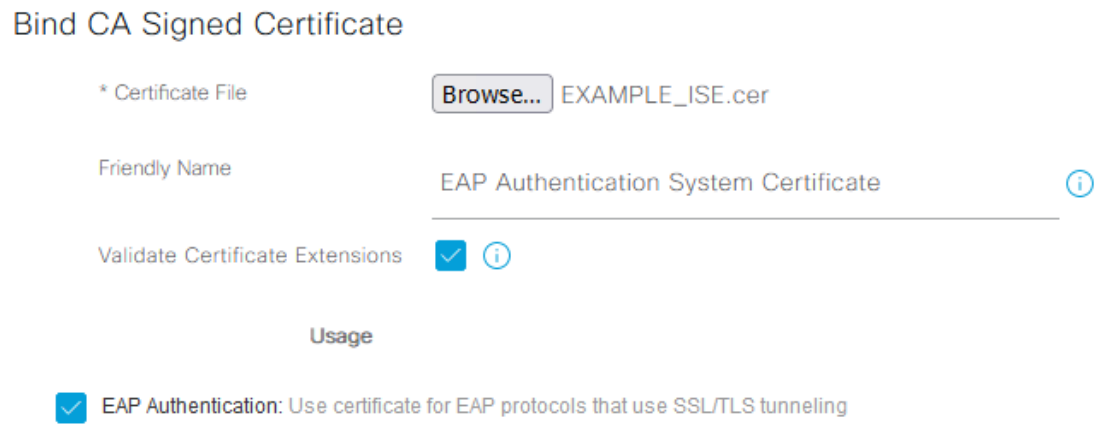
Utilisation du certificat pour la chaîne CA

2. Répétez l'étape précédente pour chaque certificat intermédiaire faisant partie de la chaîne de certificats de l'autorité de certification.

3. Une fois que tous les certificats, dans le cadre de la chaîne d'autorité de certification complète, sont importés dans le magasin de certificats de confiance dans ISE, revenez à l'interface utilisateur graphique ISE et accédez à **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. Recherchez l'entrée CSR sous **Friendly Name** qui correspond au certificat signé, cliquez sur la case à cocher du certificat, puis cliquez sur **Bind Certificate**.



*Lier le certificat à CSR***Note**: Vous devrez lier un seul certificat CA-Signed à chaque CSR, un par un. Répétez cette procédure pour tous les CSR restants créés pour d'autres noeuds ISE dans le déploiement.Sur la page suivante, cliquez sur **Browse** et choisissez le fichier de certificat signé, définissez un nom convivial souhaité et choisissez la ou les utilisations de certificat. Soumettre pour enregistrer les modifications.



Sélectionner le certificat à lier à CSR

4. Àce stade, le certificat signé est déplacé vers l'interface utilisateur graphique ISE. Naviguez

jusqu'à **Administration > System: Certificates > Certificate Management: System Certificates** et l'attribuer au même noeud pour lequel le CSR a été créé. Répétez le même processus pour les autres noeuds et/ou les autres utilisations de certificats.

Étape 3. Obtention du certificat client pour le terminal

Il est nécessaire de naviguer dans un processus similaire sur le terminal pour créer un certificat client à utiliser avec EAP-TLS. Dans cet exemple, vous devez signer un certificat client et l'émettre vers le compte utilisateur pour effectuer l'authentification utilisateur avec ISE. Vous trouverez un exemple d'obtention d'un certificat client pour le terminal à partir d'un environnement Active Directory dans : Comprendre et configurer EAP-TLS en utilisant WLC et **ISE > Configurer >** [Client pour EAP-TLS](#).

En raison des différents types de terminaux et de systèmes d'exploitation, le processus pouvant être quelque peu différent, aucun exemple supplémentaire n'est fourni. Cependant, le processus global est conceptuellement le même. Générez un CSR qui contient toutes les informations pertinentes à inclure dans le certificat et faites-le signer par l'autorité de certification, qu'il s'agisse d'un serveur interne dans l'environnement ou d'une société publique/tierce qui fournit ce type de service.

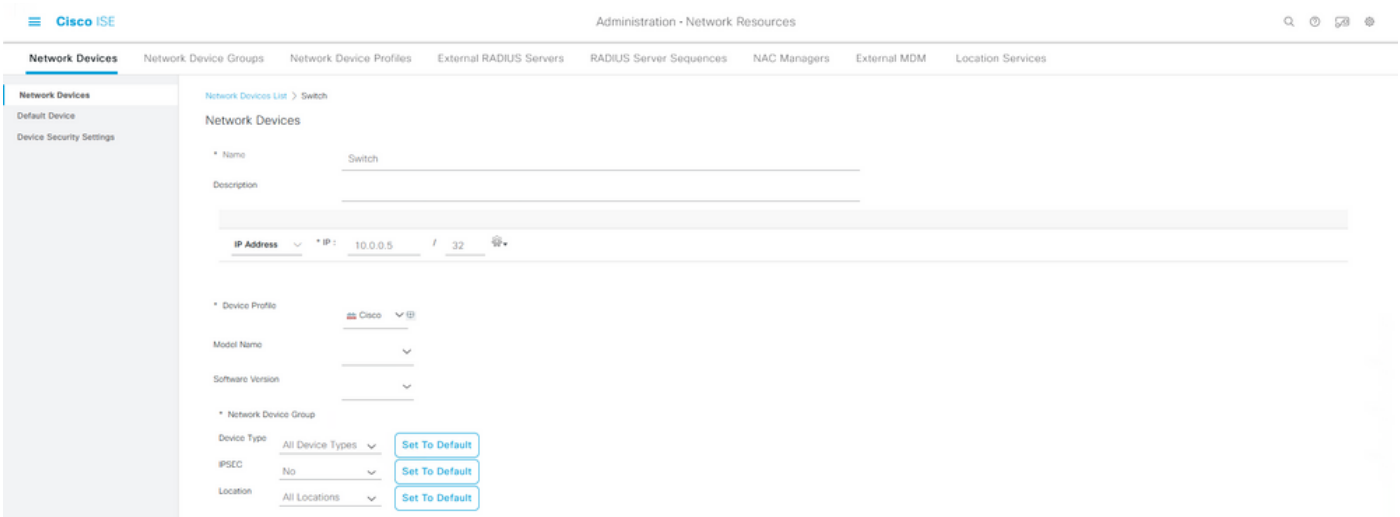
En outre, les champs de certificat Common Name (CN) et Subject Alternative Name (SAN) incluent l'identité à utiliser pendant le flux d'authentification. Cela détermine également la manière dont le demandeur doit être configuré pour EAP-TLS en termes d'identité : Authentification de la machine et/ou de l'utilisateur, Authentification de la machine ou Authentification de l'utilisateur. Cet exemple utilise uniquement l'authentification utilisateur dans le reste de ce document.

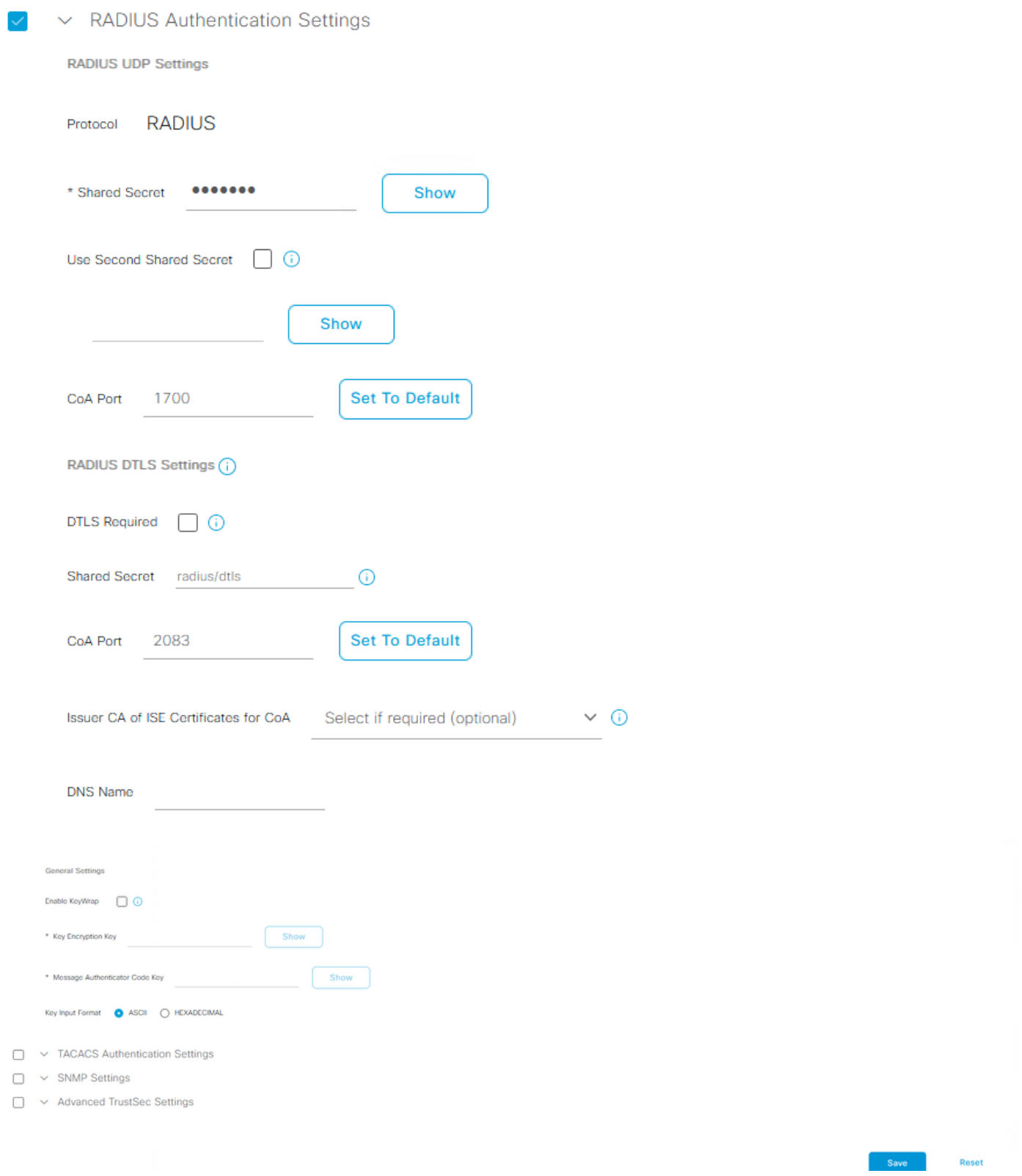
Périphériques réseau

Étape 4. Ajout du périphérique d'accès réseau dans ISE

Le périphérique d'accès réseau (NAD) auquel un point d'extrémité est connecté est également configuré dans ISE afin que la communication RADIUS/TACACS+ (Device Admin) puisse avoir lieu. Entre NAD et ISE, un mot de passe/secret partagé est utilisé à des fins de confiance.

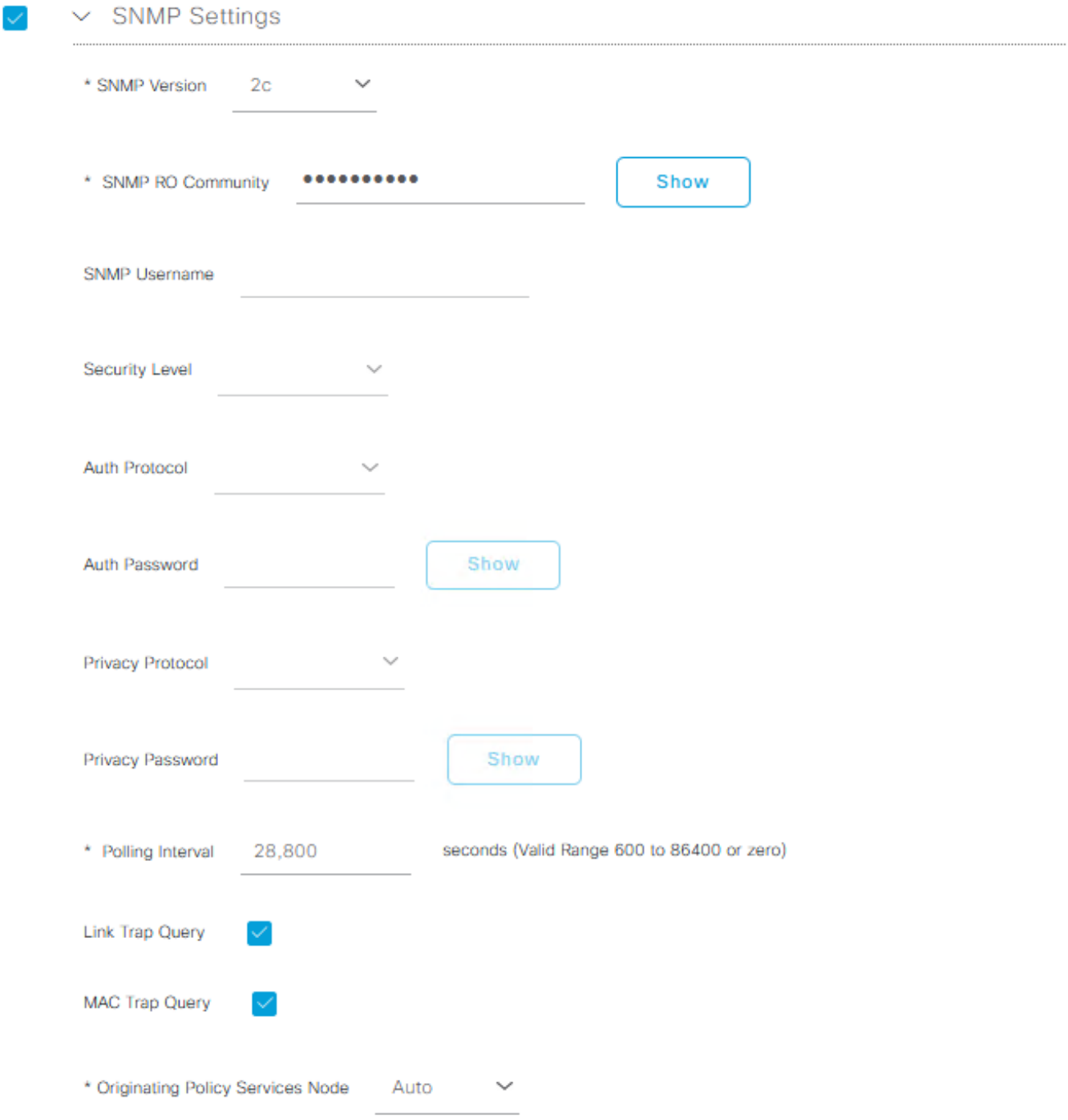
Afin d'ajouter un NAD via l'interface utilisateur graphique ISE, accédez à **Administration > Network Resources: Network Devices > Network Devices** et cliquez sur **Add**, qui est représenté sur cette image.





Exemple de configuration de périphérique réseau

Pour une utilisation avec le profilage ISE, vous voudrez également configurer SNMPv2c ou SNMPv3 (plus sécurisé) pour permettre au noeud de service de stratégie ISE (PSN) de contacter le NAD via des requêtes SNMP impliquées dans l'authentification du terminal à ISE afin de collecter des attributs pour prendre des décisions précises sur le type de terminal utilisé. L'exemple suivant montre comment configurer SNMP (v2c), à partir de la même page que dans l'exemple précédent :



Exemple de configuration SNMPv2c

Pour plus d'informations, consultez le *Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Accès sécurisé >* [*Définition des périphériques réseau dans Cisco ISE*].

Àce stade, si vous ne l'avez pas encore fait, vous devez configurer tous les paramètres AAA associés sur le NAD pour l'authentification et l'autorisation avec Cisco ISE.

Éléments de stratégie

Ces paramètres sont des éléments qui finissent par se lier à la stratégie d'authentification ou à la stratégie d'autorisation. Dans ce guide, chaque élément de stratégie est principalement construit, puis mappé dans la stratégie d'authentification ou la stratégie d'autorisation. Il est important de comprendre que la stratégie n'est pas en vigueur tant que la liaison à la stratégie d'authentification/d'autorisation n'est pas terminée avec succès.

Étape 5. Utiliser la source d'identité externe

Une source d'identité externe est simplement une source où réside l'identité finale (ordinateur ou utilisateur) utilisée pendant la phase d'authentification ISE. Active Directory est généralement utilisé pour prendre en charge l'authentification de l'ordinateur par rapport au compte de l'ordinateur et/ou l'authentification de l'utilisateur par rapport au compte de l'utilisateur final dans Active Directory. La source des terminaux internes (internes) ne stocke pas le compte/nom d'hôte de l'ordinateur. Par conséquent, elle ne peut pas être utilisée avec l'authentification de l'ordinateur.

Voici les sources d'identité prises en charge avec ISE et les protocoles (type d'authentification) qui peuvent être utilisés avec chaque source d'identité :

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

Fonctionnalités du magasin d'identités

Pour plus d'informations sur les éléments de stratégie, reportez-vous au *Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Segmentation >* [*Jeux de stratégies*].

Ajouter des groupes de sécurité Active Directory à ISE

Pour utiliser les groupes de sécurité Active Directory dans les stratégies ISE, vous devez d'abord ajouter le groupe au point de jointure Active Directory. Dans l'interface utilisateur graphique ISE, sélectionnez **Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory**.

Pour plus d'informations sur l'intégration d'ISE 3.x à Active Directory et sur les conditions requises, consultez ce document en détail : *Intégration d'Active Directory avec Cisco ISE 2.x*.

> **Note**: La même action est applicable pour ajouter des groupes de sécurité à une instance LDAP. Dans l'interface utilisateur graphique ISE, sélectionnez **Administration > Identity Management: External Identity Sources > LDAP > *LDAP instance name* > tab: Groups > Add > Select Groups From Directory**.

Étape 6. Création du profil d'authentification de certificat

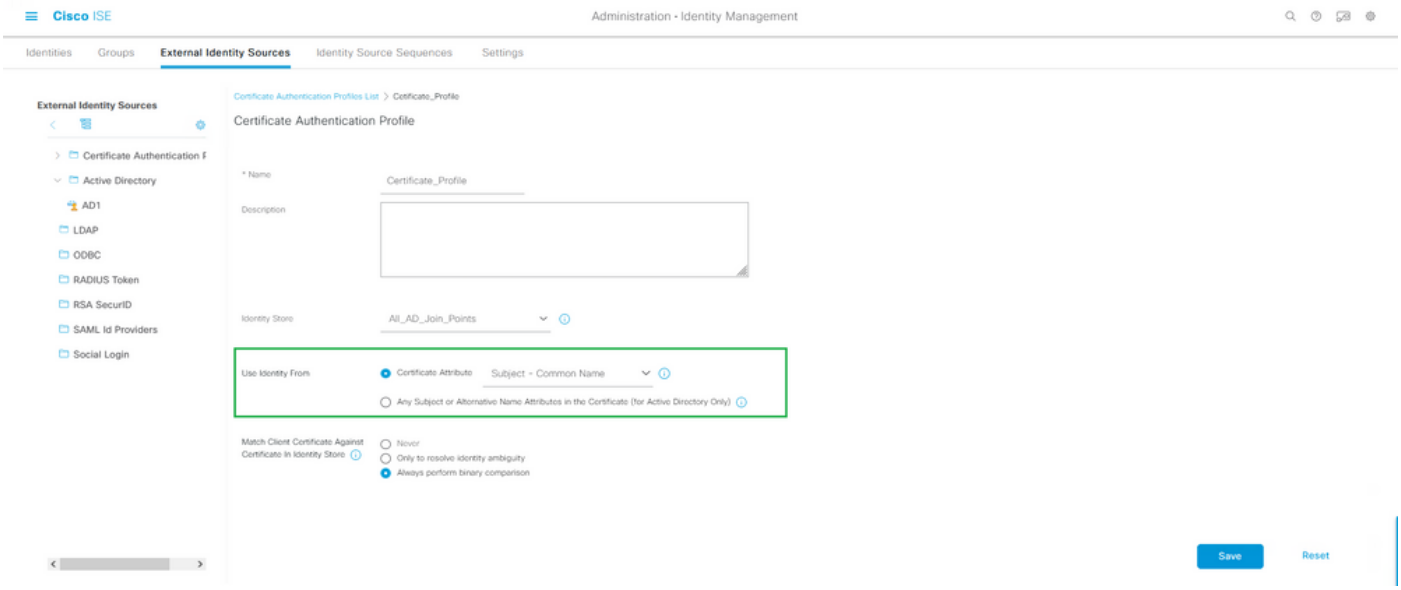
L'objectif du profil d'authentification de certificat est d'informer ISE du champ de certificat dans lequel l'identité (ordinateur ou utilisateur) peut être trouvée sur le certificat client (certificat d'identité finale) présenté à ISE pendant EAP-TLS (également pendant d'autres méthodes d'authentification basées sur les certificats). Ces paramètres seront liés à la stratégie d'authentification pour authentifier l'identité. Dans l'interface utilisateur graphique ISE, accédez à **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** et cliquez sur **Add**.

Utiliser l'identité de est utilisé pour choisir l'attribut de certificat à partir duquel un champ spécifique de l'identité peut être trouvé. Les choix sont les suivants :

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

Si le magasin d'identités doit être pointé vers Active Directory ou LDAP (source d'identité externe), alors une fonctionnalité appelée Comparaison binaire peut être utilisée. La comparaison binaire effectue une recherche de l'identité dans Active Directory obtenue à partir du certificat client à partir de la sélection **Utiliser l'identité de** , qui se produit pendant la phase d'authentification ISE. Sans comparaison binaire, l'identité est simplement obtenue à partir du certificat client et n'est pas recherchée dans Active Directory jusqu'à la phase d'autorisation ISE lorsqu'un groupe externe Active Directory est utilisé comme condition, ou toute autre condition qui devrait être exécutée en externe à ISE. Afin d'utiliser la comparaison binaire, dans le **magasin d'identités** choisissez la source d'identité externe (Active Directory ou LDAP) où le compte d'identité de fin peut être trouvé.

Il s'agit d'un exemple de configuration lorsque l'identité est située dans le champ Common Name (CN) du certificat client, avec la comparaison binaire activée (facultatif) :



Profil d'authentification du certificat

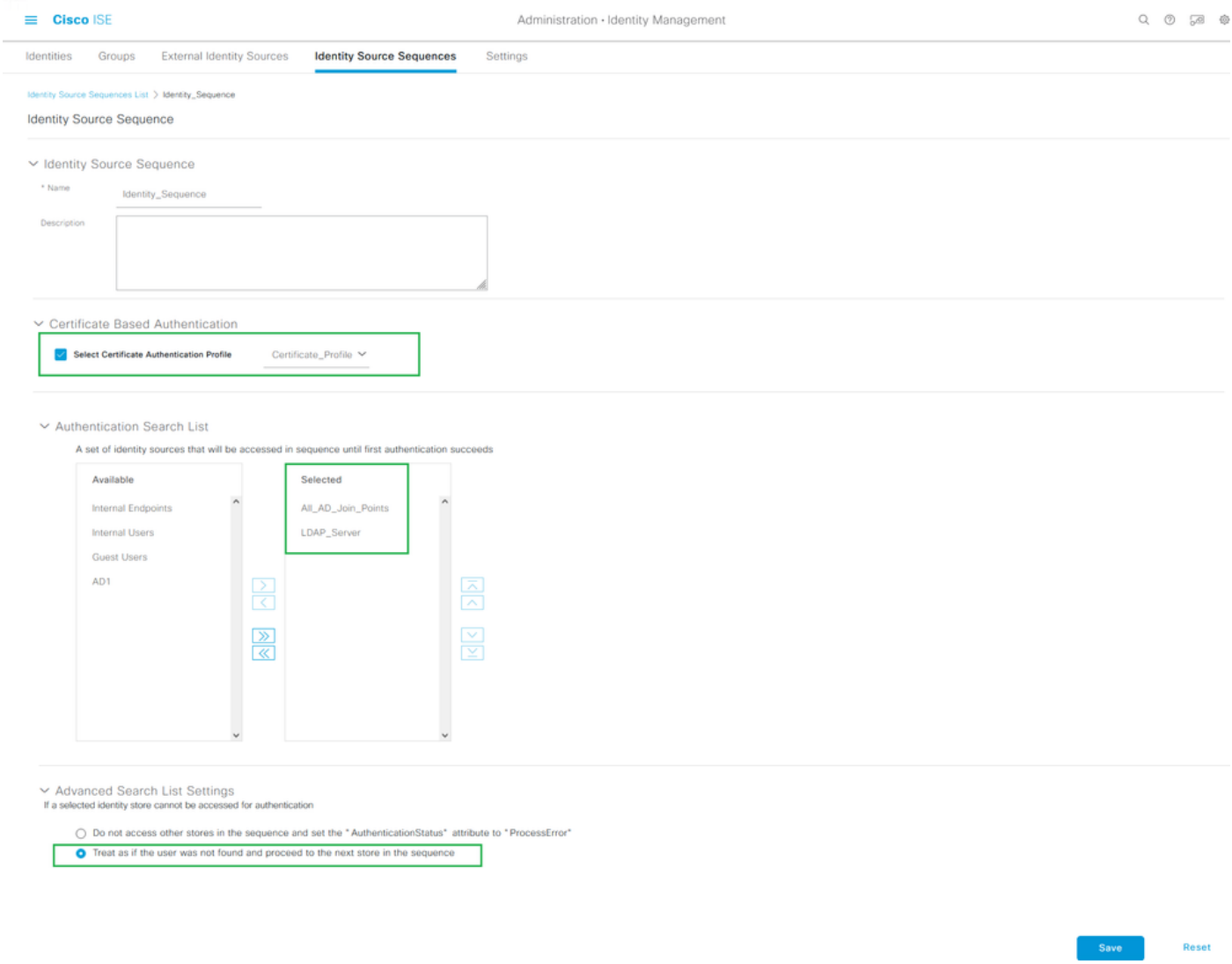
Pour plus d'informations, consultez le *Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Configuration de base > Service Cisco ISE CA > Configurer Cisco ISE pour utiliser des certificats pour authentifier les périphériques personnels >* [*Créer un profil d'authentification de certificat pour l'authentification basée sur TLS*]().

Étape 7. Ajout à une séquence source d'identité

La séquence source d'identité peut être créée à partir de l'interface utilisateur graphique ISE. Naviguez jusqu'à **Administration > Identity Management**. Sous **Identity Source Sequences** , cliquez sur **Add**.

L'étape suivante consiste à ajouter le profil d'authentification de certificat à une séquence de sources d'identité qui permet d'inclure plusieurs points de jointure Active Directory ou de regrouper une combinaison de sources d'identité internes/externes, selon les besoins, qui se lie ensuite à la stratégie d'authentification sous la **Use** colonne.

L'exemple ci-dessous permet d'effectuer la recherche dans Active Directory en premier, puis, si l'utilisateur est introuvable, il recherche ensuite sur un serveur LDAP. Pour plusieurs sources d'identité. assurez-vous toujours que **Treat as if the user was not found and proceed to the next store in the sequence** est cochée. Ainsi, chaque source/serveur d'identité est vérifié lors de la demande d'authentification.



Séquence source d'identité

Sinon, vous pouvez également lier uniquement le profil d'authentification de certificat à la stratégie d'authentification.

Étape 8. Définition du service de protocoles autorisés

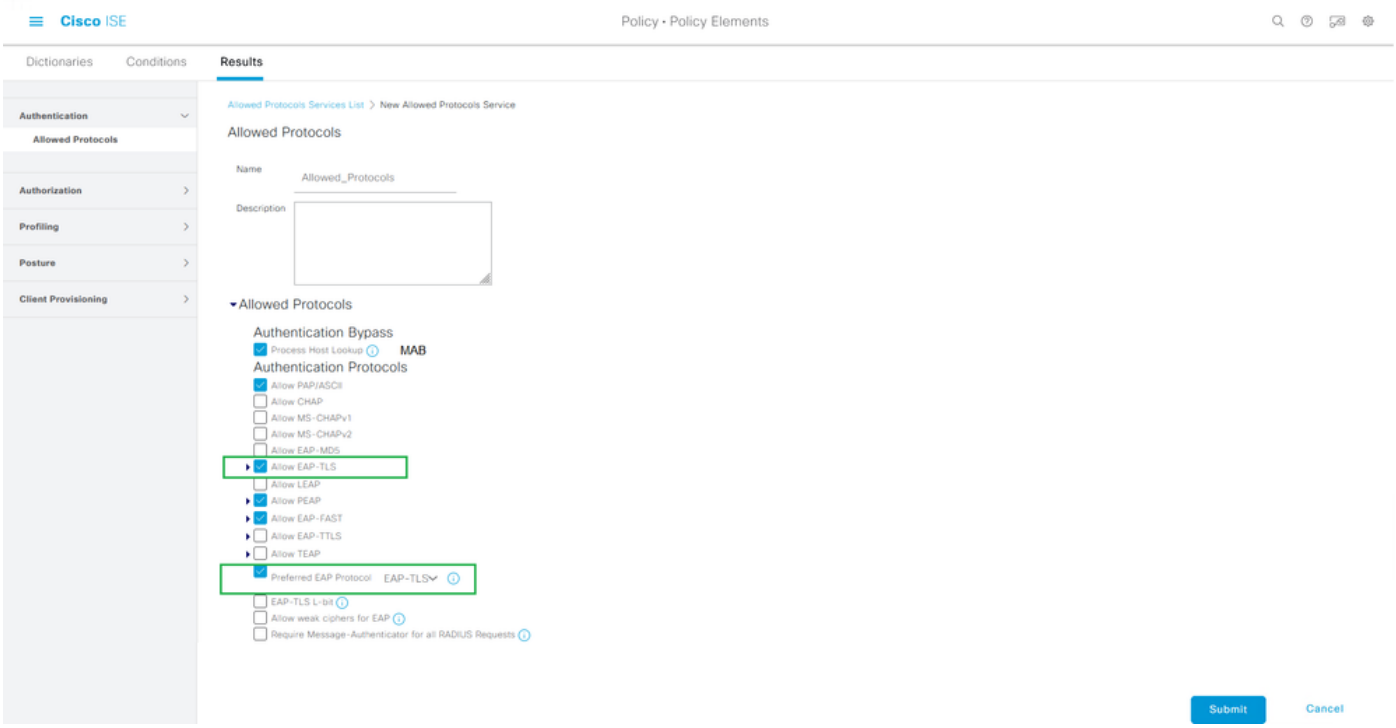
Le service de protocoles autorisés active uniquement les méthodes/protocoles d'authentification pris en charge par ISE pendant l'authentification RADIUS. Afin de configurer à partir de l'interface utilisateur graphique ISE, naviguez vers **Policy > Policy Elements : Results > Authentication > Allowed Protocols**, puis il se lie en tant qu'élément à la politique d'authentification.

> **Note**: **Authentication Bypass > Process Host Lookup** se rapporte à MAB activé sur ISE.

Ces paramètres doivent être identiques à ceux pris en charge et configurés sur le demandeur (sur le terminal). Sinon, le protocole d'authentification n'est pas négocié comme prévu et la communication RADIUS risque d'échouer. Dans une configuration ISE réelle, il est recommandé d'activer tout protocole d'authentification utilisé dans l'environnement afin qu'ISE et le demandeur puissent négocier et authentifier comme prévu.

Il s'agit des valeurs par défaut (réduites) lorsqu'une nouvelle instance des services du protocole autorisé est créée.

Note: Au minimum, vous devez activer **EAP-TLS** puisque ISE et notre demandeur s'authentifient via EAP-TLS dans cet exemple de configuration.



Protocoles permettant à ISE d'utiliser pendant la demande d'authentification au demandeur de point d'extrémité

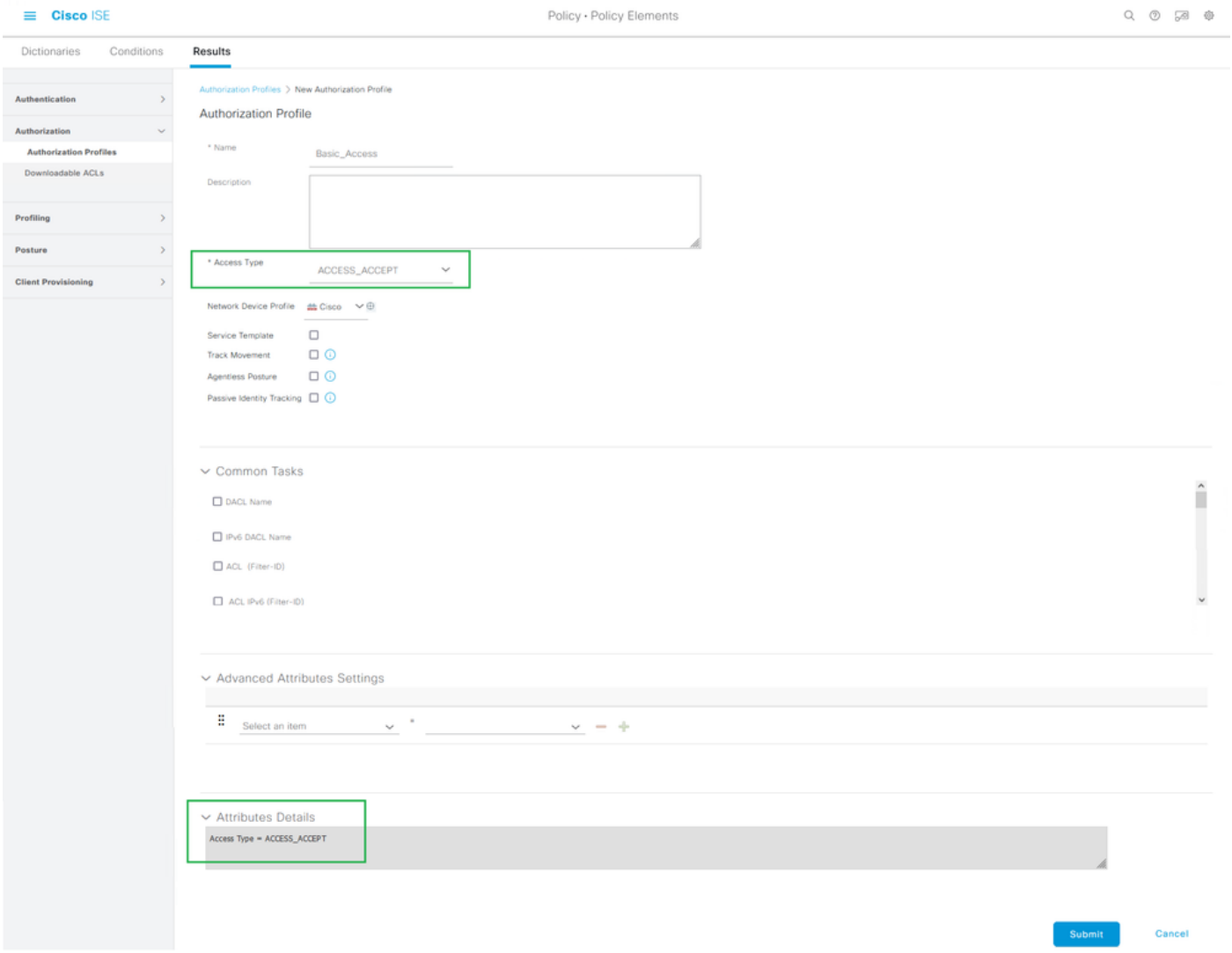
Note: L'utilisation du « Preferred EAP Protocol » défini sur la valeur « EAP-TLS » amènera ISE à demander le protocole EAP-TLS comme premier protocole offert au demandeur IEEE 802.1x du point d'extrémité. Ce paramètre est utile si vous envisagez de vous authentifier via EAP-TLS souvent sur la plupart des terminaux qui seront authentifiés avec ISE.

Étape 9. Créer le profil d'autorisation

Le dernier élément de stratégie nécessaire à la création est le profil d'autorisation, qui se lie à la stratégie d'autorisation et donne le niveau d'accès souhaité. Le profil d'autorisation est lié à la stratégie d'autorisation. Afin de le configurer à partir de l'interface utilisateur graphique ISE, accédez à **Policy > Policy Elements: Results > Authorization > Authorization Profiles** et cliquez sur **Add**.

Le profil d'autorisation contient une configuration qui génère des attributs qui sont transmis d'ISE au NAD pour une session RADIUS donnée, dans laquelle ces attributs sont utilisés pour atteindre le niveau d'accès réseau souhaité.

Comme illustré ici, il passe simplement RADIUS Access-Accept comme **Access Type**, cependant, des éléments supplémentaires peuvent être utilisés lors de l'authentification initiale. Notez les **détails d'attribut** en bas, qui contiennent le résumé des attributs qu'ISE envoie au NAD lorsqu'il correspond à un profil d'autorisation donné.



Profil d'autorisation - Élément de stratégie

Pour plus d'informations sur le profil et la politique d'autorisation ISE, reportez-vous au *Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Segmentation > Stratégies d'autorisation*.

Stratégies de sécurité

Les politiques d'authentification et d'autorisation sont créées à partir de l'interface utilisateur graphique ISE, sélectionnez **Policy > Policy Sets**. Ils sont activés par défaut sur ISE 3.x. Lorsque vous installez ISE, un jeu de stratégies est toujours défini, c'est-à-dire le jeu de stratégies par défaut. Le jeu de stratégies par défaut contient des règles d'authentification, d'autorisation et d'exception prédéfinies et par défaut.

Les ensembles de stratégies sont configurés de manière hiérarchique, ce qui permet à l'administrateur ISE de regrouper des stratégies similaires, en termes d'intention, dans différents ensembles pour une utilisation dans une demande d'authentification. Les stratégies de personnalisation et de regroupement sont pratiquement illimitées. Ainsi, un ensemble de stratégies peut être utilisé pour l'authentification des points d'extrémité sans fil pour l'accès au réseau, tandis qu'un autre ensemble de stratégies peut être utilisé pour l'authentification des points d'extrémité filaires pour l'accès au réseau ; ou pour tout autre moyen unique et différenciant de gérer les politiques.

Cisco ISE évaluera les ensembles de politiques et les politiques au sein de utilise l'approche

descendante, pour d'abord faire correspondre un ensemble de politiques donné lorsque toutes les conditions dudit ensemble s'avèrent vraies ; sur lequel ISE évalue en outre les stratégies d'authentification et d'autorisation dans ce qui correspond à l'ensemble de stratégies, comme suit :

1. Évaluation de l'ensemble de règles et des conditions de cet ensemble
2. Stratégies d'authentification dans l'ensemble de stratégies correspondant
3. Stratégie d'autorisation - Exceptions locales
4. Politique d'autorisation - Exceptions globales
5. Stratégies d'autorisation

Les exceptions de stratégie existent globalement pour tous les ensembles de stratégies ou localement dans un ensemble de stratégies spécifique. Ces exceptions de stratégie sont traitées dans le cadre des stratégies d'autorisation, car elles traitent des autorisations ou des résultats donnés pour l'accès au réseau dans un scénario temporaire donné.

La section suivante explique comment combiner les éléments de configuration et de stratégie à lier aux stratégies d'authentification et d'autorisation ISE pour authentifier un terminal via EAP-TLS.

Étape 10. Création de l'ensemble de stratégies

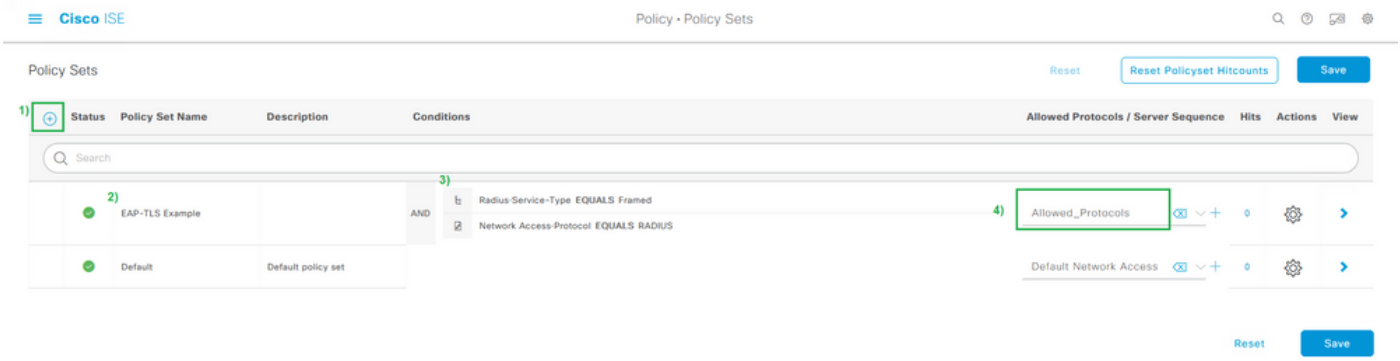
Un ensemble de stratégies est un conteneur hiérarchique constitué d'une seule règle définie par l'utilisateur qui indique le protocole ou la séquence de serveurs autorisés pour l'accès au réseau, ainsi que les stratégies d'authentification et d'autorisation et les exceptions de stratégie, tous également configurés avec des règles basées sur des conditions définies par l'utilisateur.

Afin de créer un ensemble de politiques à partir de l'interface utilisateur graphique ISE, accédez à **Policy > Policy Set** puis cliquez sur l'icône plus (**+**) dans le coin supérieur gauche, comme illustré dans cette image.

Ajout d'un nouvel ensemble de stratégies

L'ensemble de stratégies lie/combine cet élément de stratégie précédemment configuré et est utilisé pour déterminer quel ensemble de stratégies doit correspondre dans une demande d'authentification RADIUS donnée (Access-Request) :

- Lier : Services de protocoles autorisés



Définition des conditions des ensembles de stratégies et de la liste des protocoles autorisés

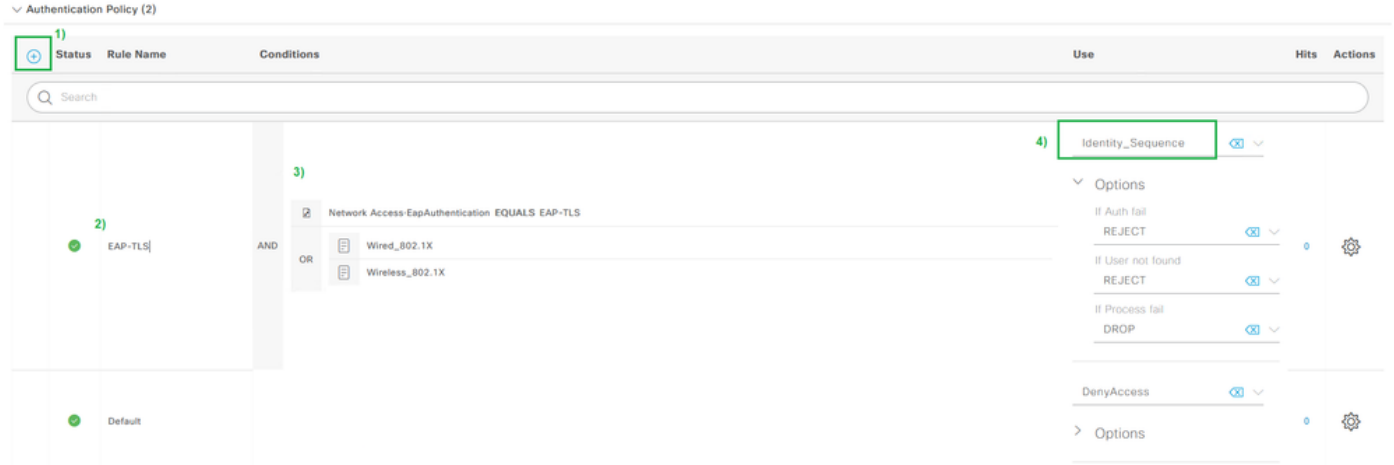
Cet exemple utilise des attributs et des valeurs spécifiques qui apparaîtraient dans la session RADIUS pour appliquer la norme IEEE 802.1x (attribut tramé), même s'il est possible qu'elle soit redondante pour appliquer à nouveau le protocole RADIUS. Afin d'obtenir les meilleurs résultats, utilisez uniquement des attributs de session RADIUS uniques qui sont applicables à l'intention souhaitée, tels que les groupes de périphériques réseau ou spécifiques pour les réseaux filaires 802.1x, sans fil 802.1x, ou les réseaux filaires 802.1x et sans fil 802.1x.

Pour plus d'informations sur les ensembles de stratégies sur ISE, consultez le *Guide de l'administrateur de Cisco Identity Services Engine, Version 3.1 > Chapitre : Segmentation > Ensembles de stratégies, Stratégies d'authentification et Stratégies d'autorisation.*

Étape 11. Créer une stratégie d'authentification

Dans l'ensemble de stratégies, la stratégie d'authentification lie/combine ces éléments de stratégie précédemment configurés pour être utilisés avec des conditions afin de déterminer quand une règle d'authentification doit être mise en correspondance.

- Lier : Profil d'authentification de certificat ou séquence source d'identité.

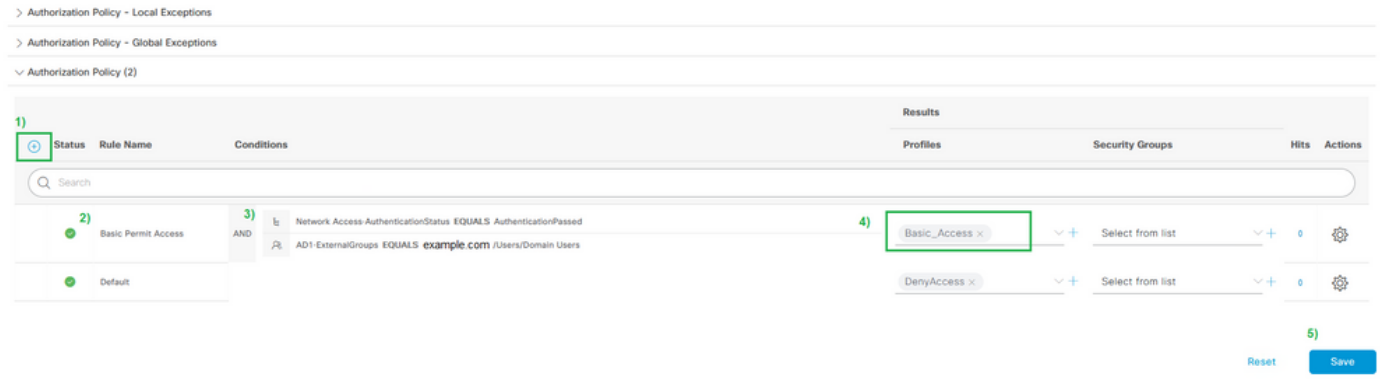


Exemple de règle de stratégie d'authentification

Étape 12. Création de la stratégie d'autorisation

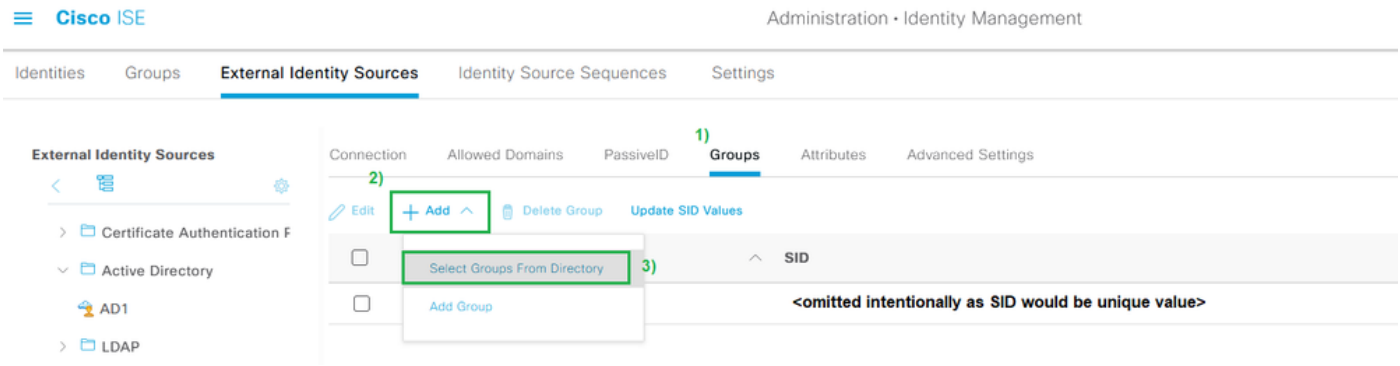
Dans l'ensemble de stratégies, la stratégie d'autorisation lie/combine ces éléments de stratégie précédemment configurés pour être utilisés avec des conditions pour déterminer quand une règle d'autorisation doit être mise en correspondance. L'exemple ici est pour **Authentification utilisateur** puisque les conditions pointent vers le groupe de sécurité **Utilisateurs du domaine** dans Active Directory.

- Lier : Profil d'autorisation

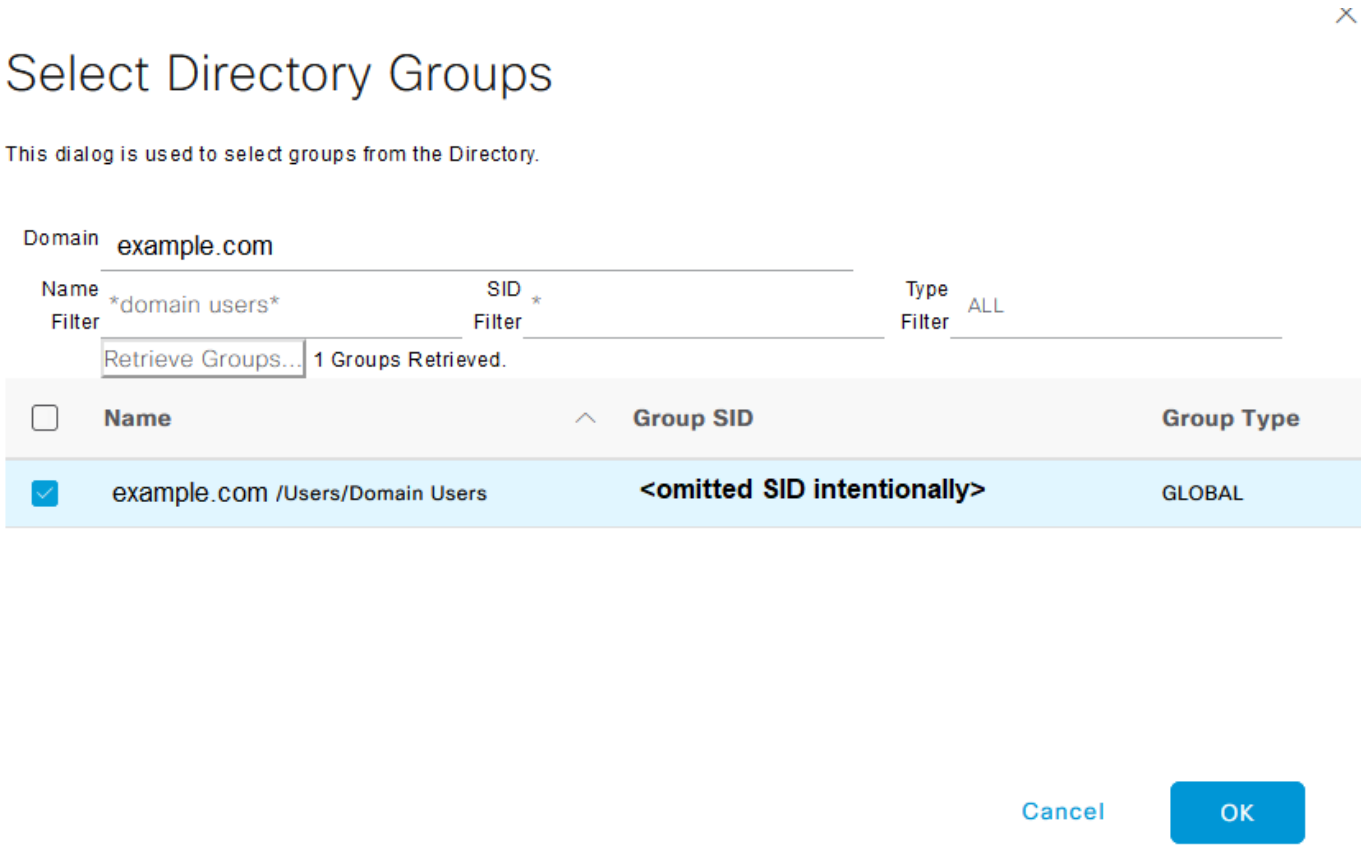


Exemple de règle de stratégie d'autorisation

Pour ajouter un groupe externe (depuis Active Directory ou LDAP, par exemple), vous devez ajouter le groupe à partir de l'instance de serveur externe. Dans cet exemple, il sera extrait de l'interface utilisateur ISE : **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups**. Dans l'onglet Groupe, sélectionnez **Add > Select Groups from Directory** et utilisez le filtre Nom pour rechercher tous les groupes (*) ou des groupes spécifiques, tels que les utilisateurs du domaine (*utilisateurs du domaine*) pour récupérer des groupes.



Pour utiliser des groupes externes dans les stratégies ISE, vous devez ajouter un groupe à partir du répertoire



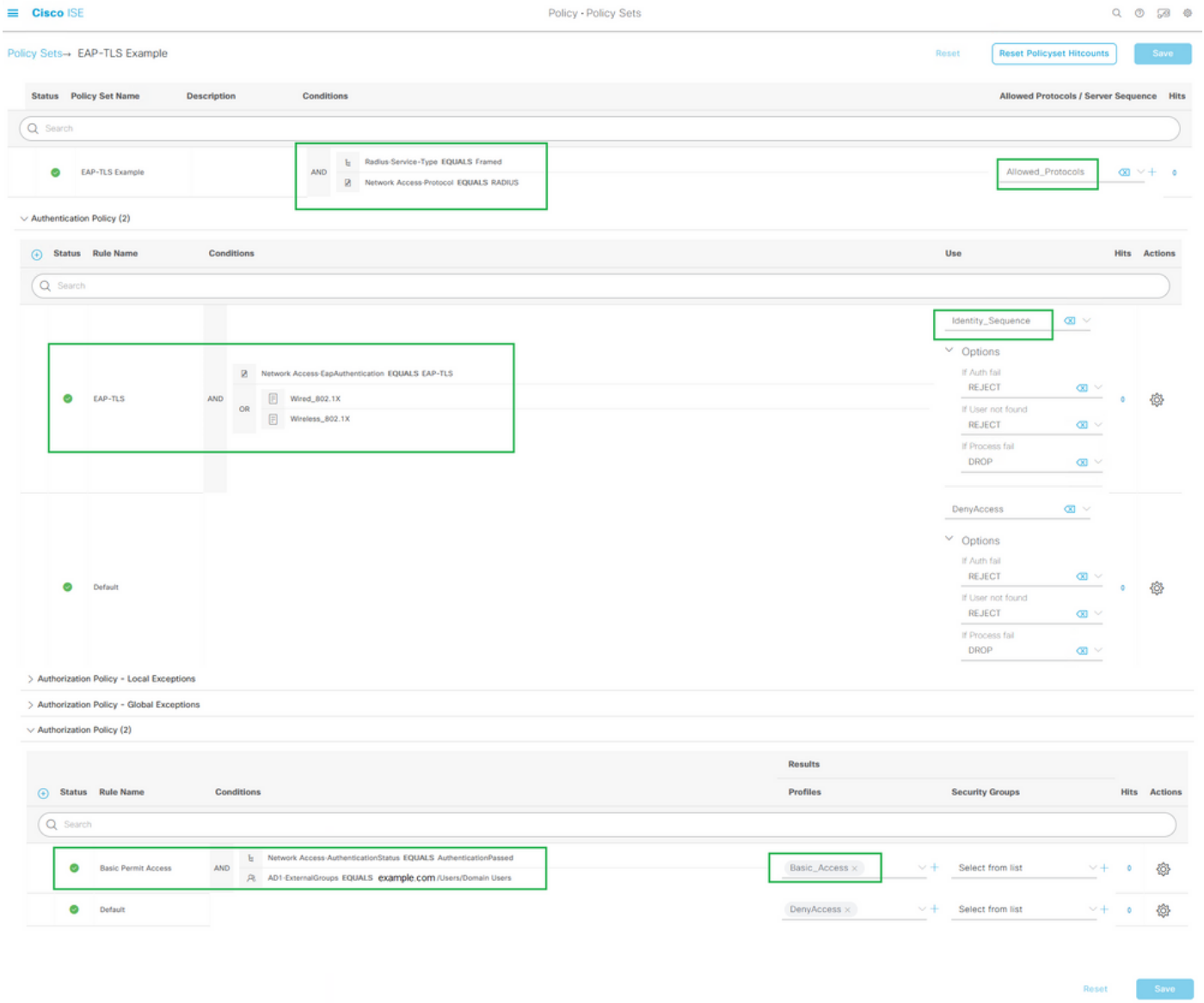
Exemple de recherche dans le répertoire externe - Active Directory

Après avoir coché la case à côté de chaque groupe que vous souhaitez utiliser dans les stratégies dans ISE, n'oubliez pas de cliquer sur **Ok** et/ou **Enregistrer** afin d'enregistrer les modifications.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Une fois que tous les éléments de configuration globale et de stratégie lient le jeu de stratégies, la configuration ressemble à cette image pour l'authentification de l'utilisateur via EAP-TLS :

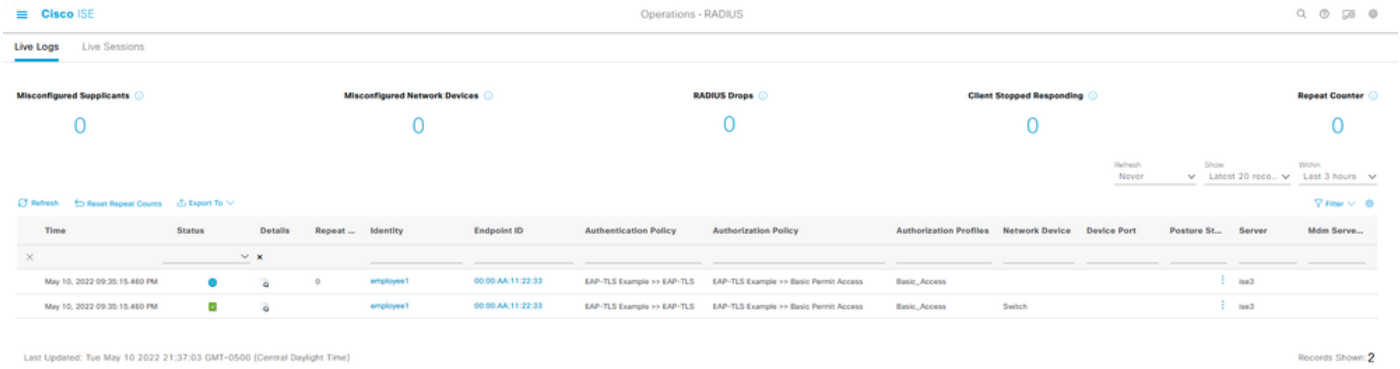


Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Une fois la configuration terminée, connectez le terminal pour tester l'authentification. Les résultats sont disponibles dans l'interface utilisateur graphique ISE. Choisir **Operations > Radius > Live Logs**, comme le montre cette image.

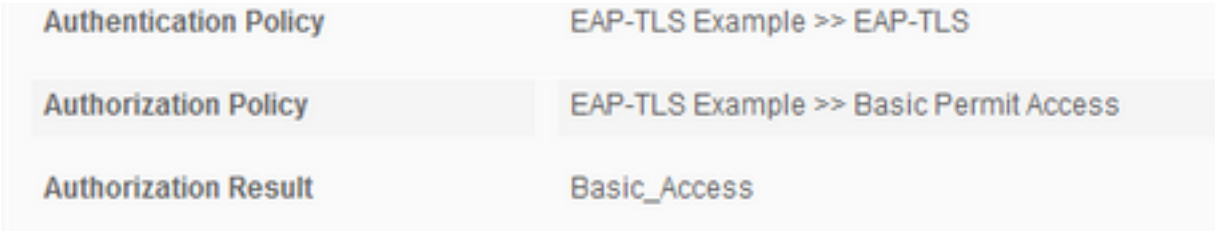
Pour la reconnaissance, les journaux actifs pour RADIUS et TACACS+ (Device Admin) sont disponibles pour les tentatives/activités d'authentification jusqu'aux dernières 24 heures et pour les 100 derniers enregistrements. Si vous souhaitez voir ce type de données de rapport au-delà de cette période, vous devrez utiliser les rapports, en particulier : **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications**.



Live Logs" />*Exemple de sortie de Radius > Live Logs*

Dans les journaux RADIUS Live Logs dans ISE, vous vous attendez à trouver des informations sur la session RADIUS, qui incluent des attributs de session, et d'autres informations utiles pour diagnostiquer le comportement observé pendant un flux d'authentification. Cliquez sur le bouton **details** pour ouvrir la vue détaillée de la session afin d'afficher les attributs de session et les informations associées spécifiques à cette tentative d'authentification.

Afin de résoudre les problèmes, il est important de s'assurer que les stratégies correctes sont respectées. Pour cet exemple de configuration, les stratégies d'authentification et d'autorisation souhaitées sont mises en correspondance comme prévu, comme indiqué dans l'image :



Dans la vue détaillée, ces attributs sont vérifiés afin de vérifier que l'authentification se comporte comme prévu selon la conception dans cet exemple de configuration :

- **Événement**
  Indique si l'authentification a réussi ou non.Dans un scénario de travail, la valeur est : **Authentification 5200 réussie**.

- **Nom d'utilisateur**
  Cela inclut l'identité finale qui a été extraite du certificat client qui a été présenté à ISE.Dans un scénario de travail, il s'agit du nom d'utilisateur de l'utilisateur connecté au point d'extrémité (à savoir, employee1 de l'image précédente).

- **ID du terminal**
  Pour les réseaux filaires et sans fil, cette valeur correspond à l'adresse MAC de la carte réseau du point d'extrémité.Dans un scénario de travail, il s'agit de l'adresse MAC du point d'extrémité, sauf si la connexion s'effectue via un réseau privé virtuel, auquel cas il peut s'agir de l'adresse IP du point d'extrémité.

- **Stratégie d'authentification**
  Affiche la stratégie d'authentification correspondante pour la session donnée en fonction des attributs de session qui correspondent aux conditions de la stratégie.Dans un scénario de travail, il s'agit de la stratégie d'authentification attendue telle que configurée.Si vous voyez

une autre stratégie, cela signifie que la stratégie attendue par rapport aux conditions de la stratégie n'a pas été évaluée comme vraie. Dans ce cas, vérifiez les attributs de session et assurez-vous que chaque stratégie contient des conditions différentes mais uniques pour chaque stratégie.

- **Politique d'autorisation**
  Affiche la stratégie d'autorisation correspondante pour la session donnée en fonction des attributs de session qui correspondent aux conditions de la stratégie.Dans un scénario de travail, il s'agit de la stratégie d'autorisation attendue telle que configurée.Si vous voyez une autre stratégie, cela signifie que la stratégie attendue par rapport aux conditions de la stratégie n'a pas été évaluée comme vraie. Dans ce cas, vérifiez les attributs de session et assurez-vous que chaque stratégie contient des conditions différentes mais uniques pour chaque stratégie.

- **Résultat d'autorisation**
  En fonction de la stratégie d'autorisation correspondante, le profil d'autorisation qui a été utilisé dans la session donnée s'affiche.Dans un scénario de travail, il s'agit de la même valeur que celle configurée dans la stratégie. Il est conseillé de vérifier les informations à des fins d'audit et de s'assurer que le profil d'autorisation correct a été configuré.

- **Serveur de stratégie**
  Cela inclut le nom d'hôte du noeud de service de stratégie ISE (PSN) qui a été impliqué dans la tentative d'authentification.Dans un scénario de travail, vous ne voyez que les authentifications qui vont au premier noeud PSN tel que configuré sur le NAD (également connu sous le nom de périphérique de périphérie), sauf si ce PSN n'était pas opérationnel ou si un basculement s'est produit, par exemple en raison d'une latence plus élevée que prévu ou si un délai d'attente d'authentification se produit.

- **Méthode d'authentification**
  Affiche la méthode d'authentification utilisée dans la session donnée. Dans cet exemple, la valeur est **dot1x**.Dans un scénario de travail, basé sur cet exemple de configuration, vous voyez la valeur **dot1x**. Si vous voyez une autre valeur, cela peut signifier que dot1x a échoué ou n'a pas été tenté.

- **Protocole d'authentification**
  Affiche la méthode d'authentification utilisée dans la session donnée. Dans cet exemple, la valeur est « EAP-TLS ».Dans un scénario de travail, basé sur cet exemple de configuration, vous voyez toujours la valeur "EAP-TLS". Si vous voyez une autre valeur, cela signifie que le demandeur et ISE n'ont pas réussi à négocier EAP-TLS.

- **Périphérique réseau**
  Affiche le nom du périphérique réseau, tel que configuré dans ISE, pour le NAD (également appelé périphérique de périphérie) impliqué dans la tentative d'authentification entre le point d'extrémité et ISE.Dans un scénario de travail, ce nom est toujours donné dans l'interface utilisateur ISE : **Administration > System: Network Devices.** Sur la base de cette configuration, l'adresse IP du NAD (également appelé périphérique de périphérie) est utilisée pour déterminer le périphérique réseau d'où provient l'authentification qui est inclus dans l'attribut de session **Adresse IPv4 NAS**.

Il ne s'agit en aucun cas d'une liste complète de tous les attributs de session possibles à examiner à des fins de dépannage ou de visibilité, car il existe d'autres attributs utiles à vérifier. Il est recommandé de passer en revue tous les attributs de session pour commencer à se familiariser avec toutes les informations. Vous pouvez voir inclure le côté droit sous la section **Étapes**, qui montre les opérations ou le comportement pris par l'ISE.

Problèmes courants et techniques de dépannage

Cette liste inclut des problèmes courants et des conseils de dépannage et ne constitue en aucun cas une liste complète. Utilisez plutôt ce guide et développez vos propres techniques pour résoudre les problèmes liés à l'ISE.

Problème : Rencontrez un échec d'authentification (**échec de l'authentification 5400**) ou toute autre tentative d'authentification infructueuse.

- Si un échec d'authentification est rencontré, cliquez sur l'icône **details** qui donne des informations sur la raison de l'échec d'authentification et les étapes suivies. Cela inclut la raison de l'échec et la cause première possible.

- Étant donné qu'ISE prend la décision relative au résultat de l'authentification, elle dispose des informations nécessaires pour comprendre la raison pour laquelle la tentative d'authentification a échoué.

Problème : L'authentification ne s'effectue pas correctement et la raison de l'échec indique « 5440 Endpoint a abandonné la session EAP et a démarré une nouvelle session » ou « 5411 Supplicant a cessé de répondre à ISE ».

- Ce motif d'échec indique que la communication RADIUS ne s'est pas terminée avant l'expiration du délai. EAP étant situé entre le point d'extrémité et NAD, vous devez vérifier le délai d'attente utilisé sur le NAD et vous assurer qu'il est défini pendant au moins cinq secondes.

- Si cinq secondes ne suffisent pas pour résoudre ce problème, nous vous recommandons de l'augmenter de cinq secondes plusieurs fois et de procéder à un nouveau test afin de vérifier si cette technique permettra de résoudre ce problème.

- Si le problème n'est pas résolu à partir des étapes précédentes, nous vous recommandons de vous assurer que l'authentification est gérée par le même noeud PSN ISE correct et que le comportement global n'indique pas un comportement anormal, tel qu'une latence supérieure à la normale entre NAD et le ou les noeuds PSN ISE.

- En outre, il est conseillé de vérifier si le point de terminaison envoie le certificat client par capture de paquets si ISE ne reçoit pas le certificat client, alors le point de terminaison (certificats utilisateur) peut ne pas faire confiance au certificat d'authentification EAP ISE. S'il est vrai, importez la chaîne d'autorités de certification dans les magasins de certificats corrects (Autorité de certification racine = Autorité de certification racine de confiance | CA intermédiaire = CA intermédiaire de confiance).

Problème : L'authentification a réussi, mais ne correspond pas à la stratégie d'authentification

et/ou d'autorisation correcte.

- Si vous rencontrez une demande d'authentification qui a réussi, mais ne correspond pas aux règles d'authentification et/ou d'autorisation correctes, nous vous recommandons de vérifier les attributs de session afin de vous assurer que les conditions utilisées sont exactes et présentes dans la session RADIUS.

- ISE évalue ces politiques à partir d'une approche descendante (à l'exception des politiques de posture). Vous devez d'abord déterminer si la stratégie qui a été mise en correspondance était supérieure ou inférieure à la stratégie souhaitée. La stratégie d'authentification est évaluée en premier et indépendamment des stratégies d'autorisation. Si la stratégie d'authentification correspond correctement, alors "22037 Authentication Passed" apparaît dans les détails d'authentification sous la section de droite intitulée **Steps.**

- Si la stratégie souhaitée est supérieure à la stratégie correspondante, cela signifie que la somme des conditions de la stratégie souhaitée n'a pas été évaluée comme vraie. Il passe en revue tous les attributs et valeurs de la condition et de la session afin de s'assurer qu'il existe et qu'aucune faute d'orthographe n'est présente.

- Si la stratégie souhaitée est inférieure à la stratégie recherchée, cela signifie qu'une autre stratégie (ci-dessus) a été recherchée au lieu de la stratégie souhaitée. Cela peut signifier que les valeurs de condition ne sont pas suffisamment spécifiques, que les conditions sont dupliquées dans une autre stratégie ou que l'ordre de la stratégie n'est pas correct. Bien qu'il soit plus difficile de résoudre les problèmes, nous vous recommandons de commencer par examiner les stratégies afin de déterminer la raison pour laquelle la stratégie souhaitée n'a pas été mise en correspondance. Cela permet d'identifier les actions à entreprendre ensuite.

Problème : L'identité ou le nom d'utilisateur utilisé lors de l'authentification n'était pas la valeur attendue.

- Dans ce cas, si le point d'extrémité envoie le certificat client, alors il est très probable qu'ISE n'utilise pas le champ de certificat correct dans le modèle d'authentification de certificat ; qui est évaluée pendant la phase d'authentification.

- Vérifiez le certificat client pour localiser le champ exact où se trouve l'identité/le nom d'utilisateur souhaité et assurez-vous que le même champ est sélectionné parmi : **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

Problème : Échec de l'authentification avec la raison de l'échec « **12514 EAP-TLS a échoué la connexion SSL/TLS en raison d'une autorité de certification inconnue dans la chaîne de certificats client** ».

- Cela peut se produire si le certificat client a un certificat dans la chaîne CA qui n'est pas approuvé sur l'interface utilisateur ISE : **Administration > System: Certificates > Trusted Certificates.**

- Cela peut généralement se produire lorsque le certificat client (sur le point d'extrémité) a une chaîne CA différente de la chaîne CA de certificat qui est signée à ISE pour l'authentification

EAP.

- Pour la résolution, assurez-vous que la chaîne CA du certificat client est approuvée sur ISE et que la chaîne CA du certificat du serveur d'authentification ISE EAP est approuvée sur le point d'extrémité.
  - Pour Windows OS et Chrome, accédez à **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates**.
  - Pour Firefox : Importez la chaîne d'autorité de certification (et non le certificat d'identité finale) à approuver pour le serveur Web.

Informations connexes

- Cisco Identity Services Engine > Guides d'installation et de mise à niveau
- Cisco Identity Services Engine > Guides de configuration
- Cisco Identity Services Engine > Informations de compatibilité
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Accès sécurisé > Définition des périphériques réseau dans Cisco ISE
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Segmentation > Jeux de politiques
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Segmentation > Stratégies d'authentification
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Segmentation > Stratégies d'autorisation
- Cisco Identity Services Engine > Guides de configuration > Intégration d'Active Directory avec Cisco ISE 2.x
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Segmentation > Network Access Service > Accès réseau pour les utilisateurs
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Configuration de base > Gestion des certificats dans Cisco ISE
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1 > Chapitre : Configuration de base > Service Cisco ISE CA > Configurer Cisco ISE pour utiliser des certificats pour authentifier les périphériques personnels > Créer un profil d'authentification de certificat pour l'authentification basée sur TLS
- Cisco Identity Services Engine > Exemples de configuration et TechNotes > Configurer le portail d'approvisionnement de certificats ISE 2.0
- Cisco Identity Services Engine > Exemples de configuration et TechNotes > Installation d'un certificat CA tiers dans ISE
- LAN sans fil (WLAN) > Exemples de configuration et notes techniques > Comprendre et configurer EAP-TLS à l'aide de WLC et ISE
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.