EAP-TLS-verificatie configureren met ISE

Inhoud

Inleiding

Dit document beschrijft de eerste configuratie als een voorbeeld om EAP-TLS-verificatie (Extensible Verification Protocol-Transport Layer Security) te introduceren met Cisco Identity Services Engine (ISE). De belangrijkste focus ligt op de ISE-configuratie die kan worden toegepast op meerdere scenario's, zoals (maar niet beperkt tot) verificatie met een IP-telefoon/endpoint verbonden via bekabeld of draadloos.

Voor het toepassingsgebied van deze handleiding is het belangrijk om deze fasen van de ISE-verificatiestroom (RADIUS) te begrijpen:

- Verificatie - Identificeer en valideer de end-identiteits (machine, gebruiker enzovoort) die netwerktoegang aanvraagt.
- Vergunning - Bepaal welke toestemmingen/toegang de eindidentiteit op het netwerk zullen worden verleend.

- Accounting - Rapporteer en volg de netwerkactiviteit van de end-identiteit nadat netwerktoegang is bereikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van EAP- en RADIUS-communicatiestromen.
- Basiskennis van RADIUS-verificatie met op certificaten gebaseerde verificatiemethoden wat betreft de communicatiestroom.
- Inzicht in de verschillen tussen Dot1x en MAC-verificatie-omleiding (MAB).
- Basiskennis van Public Key Infrastructure (PKI).
- Bekendheid met het verkrijgen van ondertekende certificaten van een certificaatinstantie (CA) en het beheren van certificaten op de eindpunten.
- Configuratie van verificatie-, autorisatie- en accounting (AAA) (RADIUS)-instellingen op een netwerkapparaat (bekabeld of draadloos).
- Configuratie van supplicant (op eindpunt) voor gebruik met RADIUS/802.1x.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE-softwarerelease 3.x.
- CA - om certificaten uit te geven (kan Enterprise CA, externe/openbare CA zijn of het Certificate Provisioning Portal gebruiken).
- Active Directory (externe identiteitsbron) - van Windows Server; indien verenigbaar met ISE.
- Network Access Device (NAD) - kan Switch (bekabeld) of draadloze LAN-controller (WLC) (draadloos) zijn geconfigureerd voor 802.1x/AAA.
- Endpoint - certificaten die zijn afgegeven aan de configuratie van de (gebruikers)identiteit en de aanvrager en die zullen worden geverifieerd voor netwerktoegang via RADIUS/802.1x: Gebruikersverificatie. Het is mogelijk om een machinecertificaat te krijgen, maar het wordt niet gebruikt in dit voorbeeld.

> **Opmerking:** Aangezien deze handleiding gebruik maakt van ISE release 3.1, zijn alle documentatie referenties gebaseerd op deze versie. Dezelfde/soortgelijke configuratie is echter mogelijk en volledig ondersteund op eerdere releases van Cisco ISE.

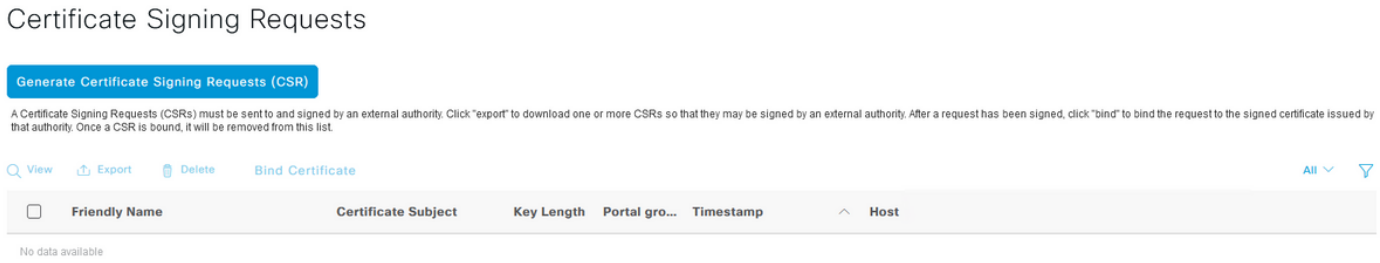
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Server- en clientcertificaten verkrijgen

Stap 1. Genereert een aanvraag voor certificaatondertekening van ISE

De eerste stap is het genereren van een certificaatondertekeningsaanvraag (CSR) van ISE en het indienen bij de CA (server) om het ondertekende certificaat te verkrijgen dat is afgegeven aan ISE, als systeemcertificaat. Dit certificaat wordt tijdens de EAP-TLS-verificatie door ISE gepresenteerd als een servercertificaat. Dit wordt uitgevoerd in de ISE-gebruikersinterface. Navigeer naar **Administration > System: Certificates > Certificate Management > Certificate Signing Requests**. Onder **Certificate Signing Requests**klikt u op **Generate Certificate Signing Requests (CSR)** zoals in deze afbeelding.



Voor certificaattypen zijn verschillende uitgebreide sleuteltoepassingen vereist. Deze lijst schetst welke uitgebreide belangrijkste toepassingen voor elk certificaattype worden vereist:

ISE-identificatiecertificaten

- Voor meervoudig gebruik (Admin, EAP, Portal, PxGrid) - client- en serververificatie
- Admin - serververificatie
- EAP-verificatie - serververificatie
- DTLS-verificatie (Datagram Transport Layer Security) - serververificatie
- Portal - Serververificatie
- PXGrid - client- en serververificatie
- Security Assertion Markup Language (SAML) - SAML-ondertekeningscertificaat
- ISE Messaging Service - Genereer een ondertekeningscertificaat of genereer een gloednieuw Messaging Certificate

Standaard is het systeemcertificaat "ISE Messaging Service" bedoeld voor gegevensreplicatie in elk ISE-knooppunt in de implementatie, de registratie van knooppunten en andere communicatie tussen knooppunten. Het certificaat wordt aangeboden en afgegeven door de interne ISE-certificeringsinstantie (CA)-server (intern voor ISE). Met dit certificaat hoeft geen actie te worden uitgevoerd.

Het systeemcertificaat "Admin" wordt gebruikt om elke ISE-knooppunt te identificeren, bijvoorbeeld wanneer de API die is gekoppeld aan de Admin UI (Beheer) wordt gebruikt, en voor bepaalde communicatie tussen knooppunten. Als u ISE voor het eerst wilt instellen, plaatst u het Systeemcertificaat "Admin". Die actie is niet direct gerelateerd aan deze configuratiehandleiding.

om IEEE 802.1x via EAP-TLS (op certificaten gebaseerde verificatie) uit te voeren, actie ondernemen voor het systeemcertificaat "EAP-verificatie", aangezien dit zal worden gebruikt als het servercertificaat dat tijdens de EAP-TLS-stroom aan het eindpunt/de client wordt voorgelegd; als het resultaat binnen de TLS-tunnel wordt beveiligd. Om aan de slag te gaan, maakt u een CSR om het systeemcertificaat EAP-verificatie te maken en geeft u dit aan het personeel dat de CA-server(s) in uw organisatie (of publieke CA-provider) beheert voor ondertekening. Het eindresultaat is het door CA ondertekende certificaat dat aan de CSR zal binden en bij ISE zal aansluiten.

Selecteer op het formulier Certificaatondertekeningsaanvraag (CSR) deze opties om de CSR in te vullen en de inhoud ervan te verkrijgen:

- **Certificaatgebruik**, kies bij dit configuratievoorbeeld **EAP Authentication**.

- Als u van plan bent een jokerteken in het certificaat te gebruiken, ***.example.com**, dan moet u ook de **Allow Wildcard Certificate** selectievakje. De beste locatie is het veld voor het certificaat van de alternatieve naam (SAN) voor compatibiliteit voor elk gebruik en voor meerdere verschillende typen besturingssystemen voor endpoints die in de omgeving aanwezig kunnen zijn.

- Als u er niet voor hebt gekozen om een verklaring met jokerteken in het certificaat te plaatsen, kies dan welke ISE-knooppunten u wilt koppelen aan het CA-ondertekende certificaat (na ondertekening). **Opmerking:** Wanneer u het door CA ondertekende certificaat dat de verklaring met jokerteken bevat, bindt aan meerdere knooppunten binnen de CSR, wordt het certificaat verdeeld naar elk ISE-knooppunt (of naar de geselecteerde knooppunten) in de ISE-implementatie, en kunnen de services opnieuw worden gestart. De herstart van de services wordt echter automatisch beperkt tot één knooppunt tegelijk. Controleer de herstart van de services via de **show application status ise** ISE-CLI-opdracht.Vervolgens moet u het formulier invullen om het **onderwerp** te kunnen definiëren. Dit omvat de gemeenschappelijke naam (CN), Organisatorische eenheid (OU), Organisatie (O), Stad (L), Staat (ST), en de gebieden van het Certificaat van het Land (C). De variabele *$FQDN$* is de waarde die staat voor het beheer van de volledig gekwalificeerde domeinnaam (hostname + domeinnaam) die is gekoppeld aan elk ISE-knooppunt.
- Het **Subject Alternative Name (SAN)** de velden moeten ook worden ingevuld om de vereiste en gewenste informatie op te nemen die moet worden gebruikt om vertrouwen te wekken. Als vereiste moet u de DNS-vermeldingen definiëren die verwijzen naar de FQDN van de ISE-knooppunten die aan dit certificaat worden gekoppeld nadat het certificaat is ondertekend.

- Zorg er ten slotte voor dat u het juiste "sleuteltype", "sleutellengte" en "verteren om te ondertekenen met" definieert, dat in overeenstemming is met de mogelijkheden van de CA-server(s) en met de juiste beveiligingspraktijken in het achterhoofd. Standaardwaarden zijn: RSA, 4096 bits en SHA-384 respectievelijk. Beschikbare keuzes en compatibiliteit worden op deze pagina binnen de ISE Admin UI weergegeven.

Dit is een voorbeeld van een ingevuld MVO formulier zonder het gebruik van een wildcard statement. Zorg ervoor dat u feitelijke waarden gebruikt die specifiek zijn voor de omgeving:

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)
$FQDN$

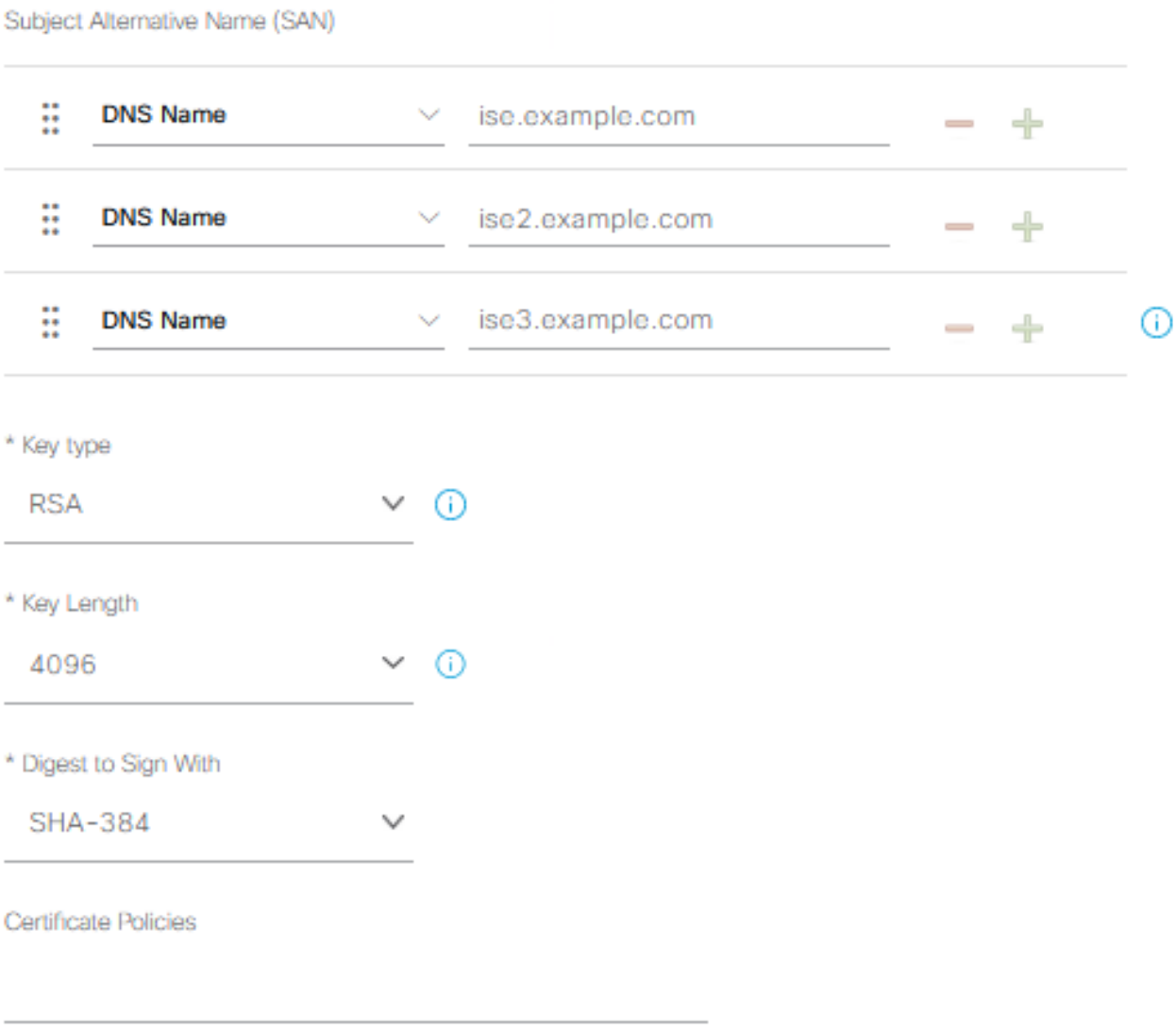
Organizational Unit (OU)

Organization (O)
Example Company

City (L)
San Jose

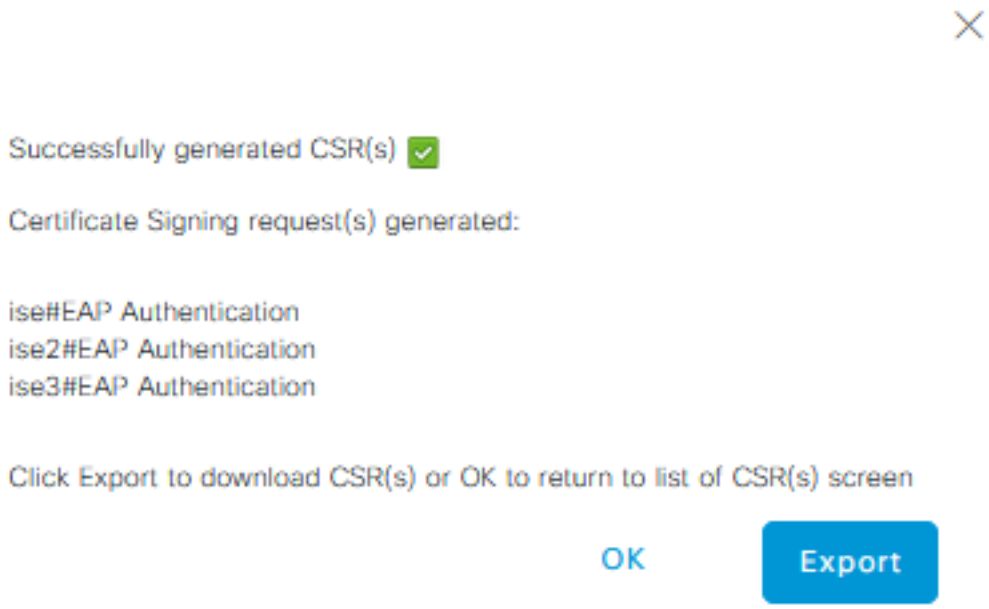
State (ST)
California

Country (C)
US



CSR-voorbeeld

Om de MVO op te slaan, klikt u op **Generate**. Klik **Export**, aan de rechteronderkant, om de CSR-bestanden vanaf deze prompt te exporteren:



Voorbeeld van MVO exporteren

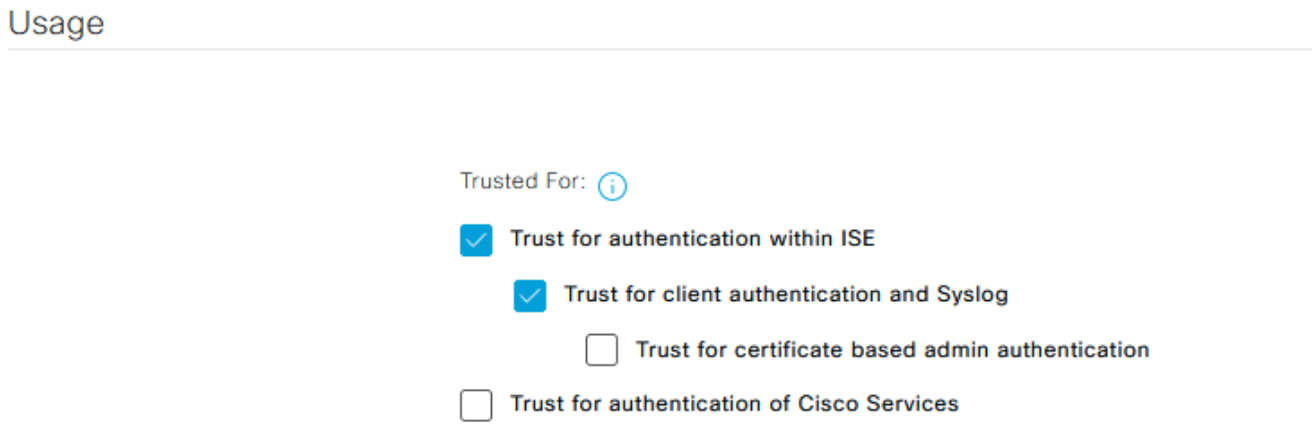
Meer informatie over certificaten voor gebruik met ISE kunt u vinden in de *beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Basis Setup > Certificaatbeheer in Cisco ISE* en installeer een door CA ondertekend certificaat van derden in ISE.

Stap 2. CA-certificaten importeren in ISE

Nadat de CA het ondertekende certificaat heeft teruggestuurd, zal het ook de volledige CA-keten omvatten die bestaat uit een basiscertificaat en één/meerdere tussenliggende certificaten. De ISE Admin UI dwingt u om eerst alle certificaten in de CA-keten te importeren, voorafgaand aan associatie of het uploaden van systeemcertificaten. Dit wordt gedaan om ervoor te zorgen dat elk systeemcertificaat correct is gekoppeld aan de CA-keten (ook bekend als vertrouwd certificaat) binnen de ISE-software.

Deze stappen zijn de beste manier om de CA-certificaten en het systeemcertificaat in ISE te importeren:

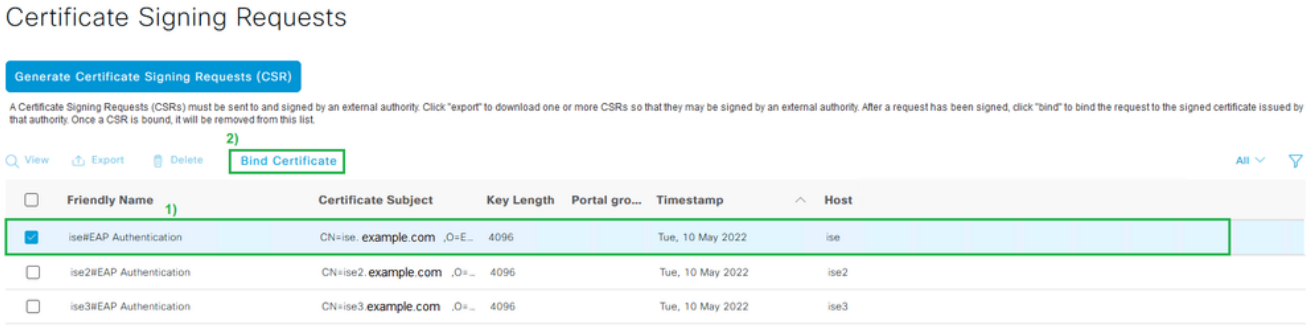
1. Om het basiscertificaat in ISE GUI te importeren, navigeer naar **Administration > System: Certificates > Certificate Management**. Onder **Trusted Certificates**klikt u op **Import** en controleer het certificaatgebruik **Trust voor verificatie binnen de** aanvinkvakjes **ISE** (Infrastructuur) en **Trust voor clientverificatie en Syslog** (Endpoints).



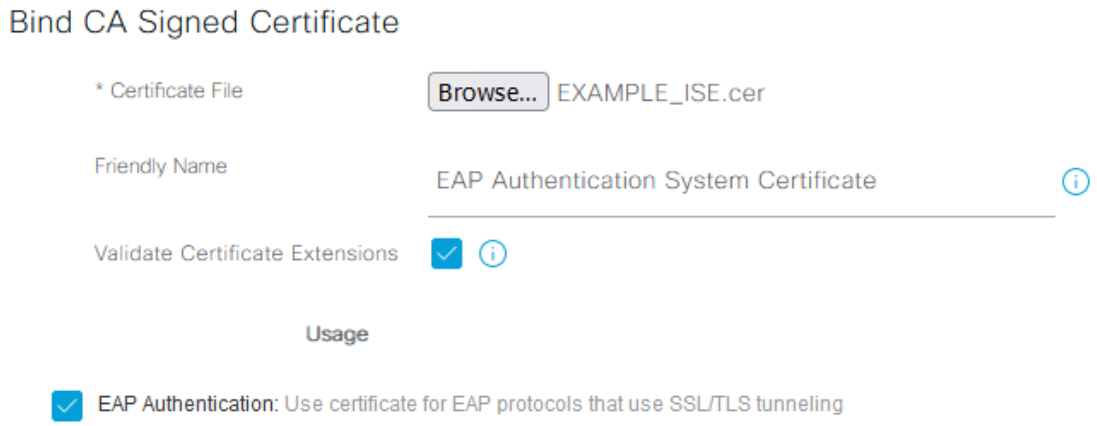
Certificaatgebruik voor CA-keten

2. Herhaal de voorgaande stap voor elk tussenliggend certificaat of tussenliggende certificaten als onderdeel van de CA-certificaatketen.

3. Wanneer alle certificaten, als onderdeel van de volledige CA-keten, zijn geïmporteerd in de Trusted Certificates-winkel in ISE, keert u terug naar de ISE GUI en bladert u naar **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. Zoek de CSR-vermelding onder **Vriendelijke naam** die overeenkomt met het ondertekende certificaat, klik op het aanvinkvakje van het certificaat en klik vervolgens op **Bind Certificate**.



*Certificaat binden aan MVO***Opmerking:** U moet één CA-ondertekend certificaat tegelijkertijd aan elke CSR binden. Herhaal dit voor alle resterende CSR's die tijdens de implementatie voor andere ISE-knooppunten zijn gemaakt.Klik op de volgende pagina **Browse** en kies het ondertekende certificaatbestand, definieer een gewenste vriendschappelijke naam en kies het (de) certificaatgebruik(en). Verzenden om de wijzigingen op te slaan.



Selecteer Certificaat om aan CSR te binden

4. Op dat moment wordt het ondertekende certificaat verplaatst naar de ISE GUI. Navigeer naar **Administration > System: Certificates > Certificate Management: System Certificates** en toewijzen aan

hetzelfde knooppunt waarvoor de MVO is gecreëerd. Herhaal dezelfde procedure voor andere knooppunten en/of andere certificaattoepassingen.

Stap 3. Clientcertificaat voor endpoint verkrijgen

Het is vereist om door een vergelijkbaar proces te navigeren op het eindpunt voor het maken van een clientcertificaat voor gebruik met EAP-TLS. Voor dit voorbeeld hebt u een clientcertificaat nodig dat is ondertekend en afgegeven aan de gebruikersaccount om de gebruikersverificatie met ISE uit te voeren. Een voorbeeld van hoe u een clientcertificaat voor het eindpunt kunt verkrijgen uit een Active Directory-omgeving, vindt u in: Begrijp en configureer EAP-TLS met behulp van WLC en **ISE > Configure >** Client voor EAP-TLS.

Vanwege de vele soorten endpoints en besturingssystemen, omdat het proces enigszins kan verschillen, worden er geen extra voorbeelden gegeven. Het totale proces is echter conceptueel hetzelfde. Een MVO genereren met alle relevante informatie die in het certificaat moet worden opgenomen en door de CA laten ondertekenen, of dat nu een interne server in de omgeving is of een publiek/extern bedrijf dat dit soort diensten aanbiedt.

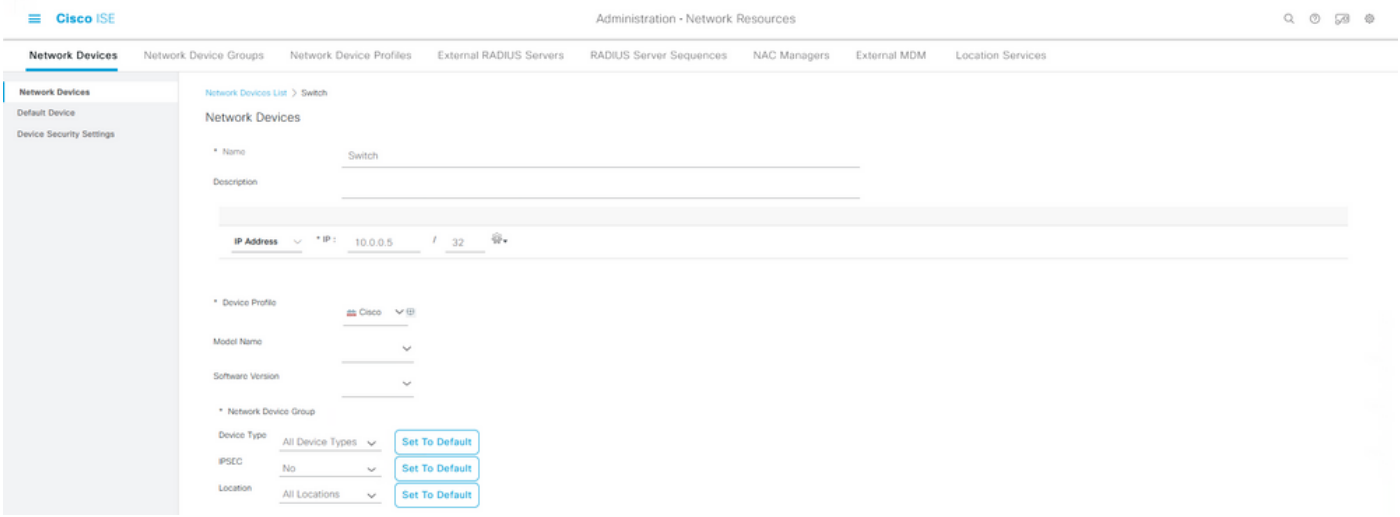
Bovendien bevatten de velden Common Name (CN) en Subjective Alternative Name (SAN) de identiteit die tijdens de verificatiestroom moet worden gebruikt. Dit bepaalt ook hoe de aanvrager voor EAP-TLS moet worden geconfigureerd wat de identiteit betreft: Machine- en/of gebruikersverificatie, systeemverificatie of gebruikersverificatie. In dit voorbeeld wordt alleen de gebruikersverificatie in de rest van dit document gebruikt.

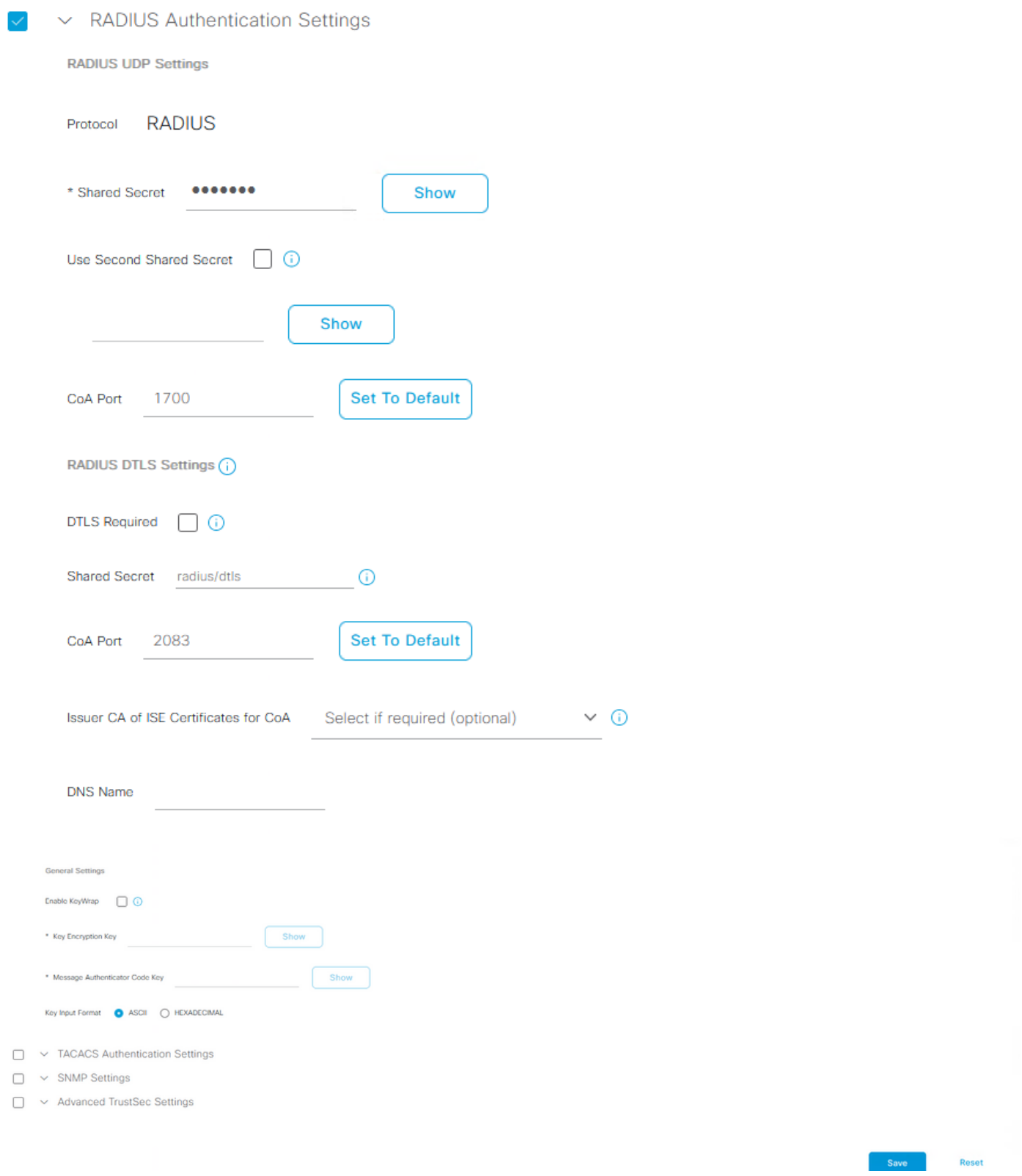
Netwerkapparaten

Stap 4. Voeg het netwerktoegangsapparaat toe in ISE

Het Network Access Device (NAD) waarmee een eindpunt is verbonden, wordt ook in ISE geconfigureerd, zodat RADIUS/TACACS+ (Device Admin) kan worden gecommuniceerd. Tussen de NAD en ISE wordt een gedeeld geheim/wachtwoord gebruikt voor vertrouwensdoeleinden.

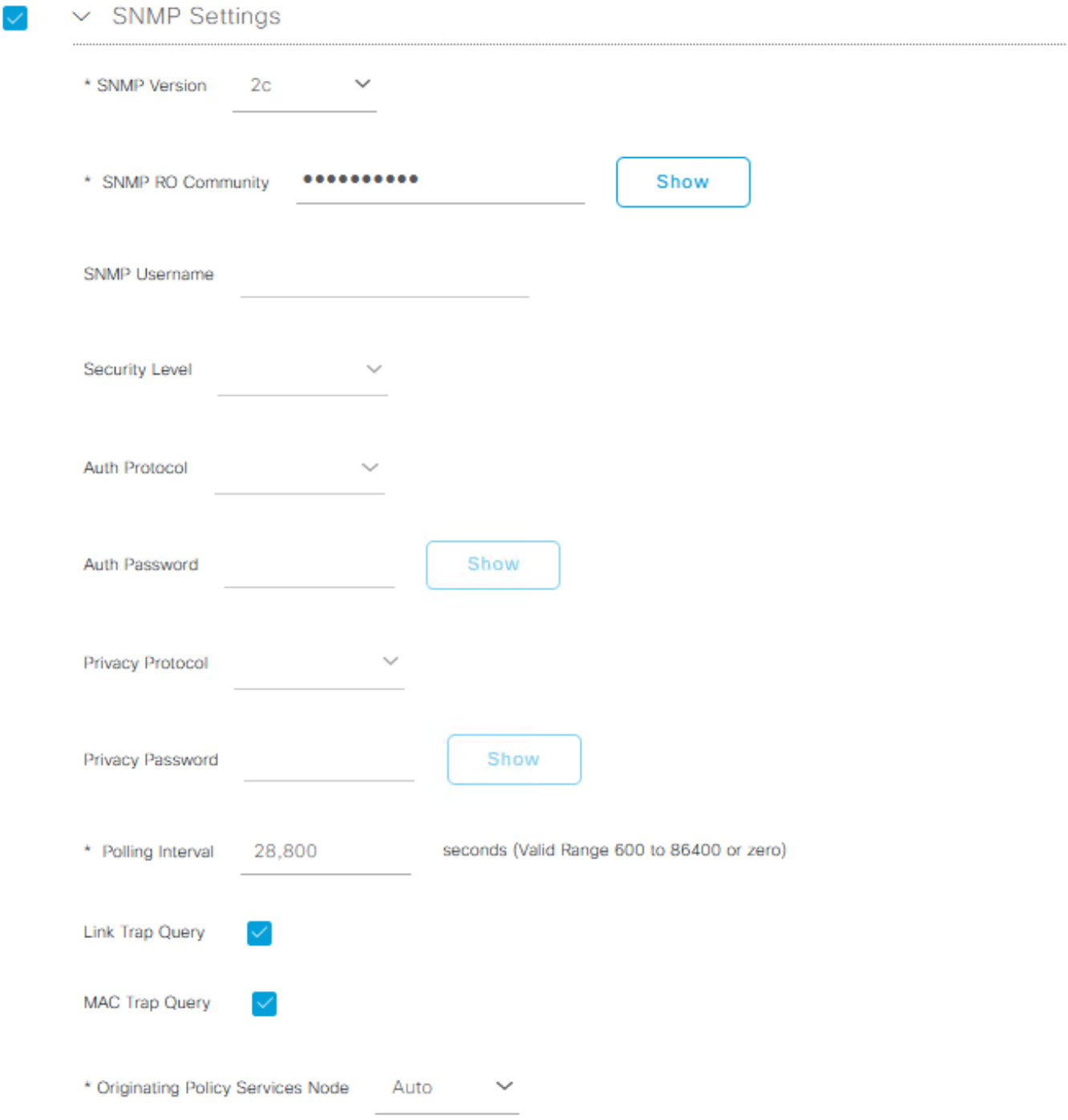
Als u een NAD via de ISE GUI wilt toevoegen, bladert u naar **Administration > Network Resources: Network Devices > Network Devices** en klik op **Add**, dat in deze afbeelding wordt weergegeven.





Voorbeeldconfiguratie van netwerkapparaten

Voor gebruik met ISE-profilering wilt u ook SNMPv2c of SNMPv3 (veiliger) configureren om het ISE Policy Service Node (PSN) in staat te stellen contact op te nemen met het NAD via SNMP-vragen die betrokken zijn bij het authenticeren van het eindpunt naar ISE om attributen te verzamelen voor het maken van nauwkeurige beslissingen over het gebruikte endpointtype. In het volgende voorbeeld wordt getoond hoe SNMP (v2c) op dezelfde pagina moet worden ingesteld als in het vorige voorbeeld:



Voorbeeld SNMPv2c-configuratie

Meer informatie is te vinden in de *beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Beveiligde toegang >* [Netwerkapparaten definiëren in Cisco ISE](#).

Op dit moment, als u dat nog niet hebt gedaan, moet u alle AAA-gerelateerde instellingen op de NAD configureren voor verificatie en autorisatie met Cisco ISE.

Beleidselementen

Deze instellingen zijn elementen die uiteindelijk bindend worden voor het verificatiebeleid of het autorisatiebeleid. In deze handleiding wordt vooral elk beleidselement gebouwd en vervolgens in kaart gebracht in het Verificatiebeleid of Autorisatiebeleid. Het is belangrijk om te begrijpen dat het beleid pas van kracht wordt als de binding aan het verificatie-/autorisatiebeleid met succes is voltooid.

Stap 5. Gebruik externe identiteitsbron

Een externe identiteitsbron is gewoon een bron waar de eindidentiteitsaccount (machine of gebruiker) zich bevindt die tijdens de ISE-verificatiefase wordt gebruikt. Active Directory wordt meestal gebruikt ter ondersteuning van Machine-verificatie met de computeraccount en/of Gebruikersverificatie met de eindgebruikersaccount in Active Directory. De interne endpoints-bron slaat de computeraccount/hostnaam niet op en kan daarom niet worden gebruikt bij de verificatie van de machine.

Hier worden de ondersteunde identiteitsbronnen met ISE en protocollen (verificatietype) getoond die met elke identiteitsbron kunnen worden gebruikt:

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

Mogelijkheden in Identity Store

Meer informatie over de beleidselementen kan worden gevonden in *Cisco Identity Services Engine Administrator Guide, release 3.1 > Hoofdstuk: Segmentatie >* [Beleidssets](#).

Active Directory-beveiligingsgroepen aan ISE toevoegen

Als u Active Directory-beveiligingsgroepen in ISE-beleid wilt gebruiken, moet u eerst de groep toevoegen aan het Active Directory-samenvoegpunt. Kies uit de ISE GUI **Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory**.

Raadpleeg dit document voor meer informatie en vereisten om ISE 3.x in Active Directory te integreren: *Active Directory-integratie met Cisco ISE 2.x*.

> **Opmerking:** De zelfde actie is van toepassing om veiligheidsgroepen aan een instantie toe te voegen LDAP. Kies uit ISE GUI **Administration > Identity Management: External Identity Sources > LDAP > *LDAP instance name* > tab: Groups > Add > Select Groups From Directory**.

Stap 6. Maak het certificaatverificatieprofiel aan

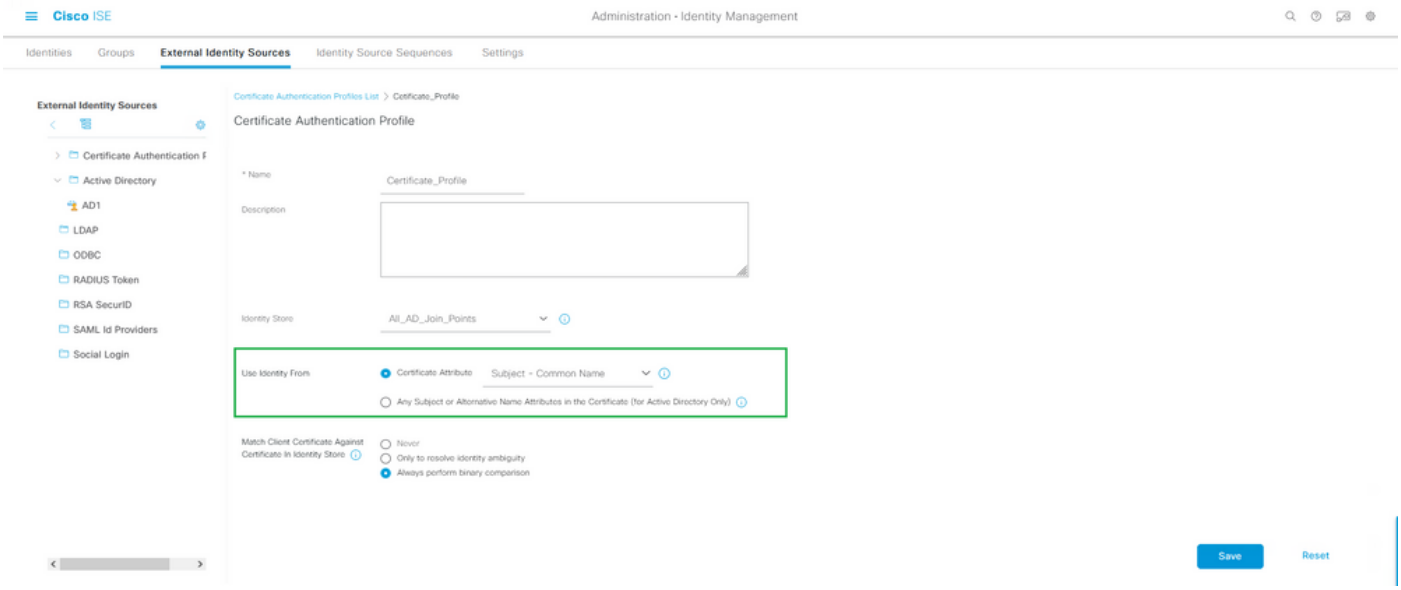
Het certificeringsverificatieprofiel heeft tot doel ISE te informeren welk certificaatveld de identiteit (machine of gebruiker) kan worden gevonden op het clientcertificaat (eindidentiteitscertificaat) dat tijdens EAP-TLS (ook tijdens andere op certificaten gebaseerde verificatiemethoden) aan ISE wordt aangeboden. Deze instellingen zijn gebonden aan het verificatiebeleid om de identiteit te verifiëren. Van ISE GUI, navigeer naar **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** en klik op **Add**.

Identity From gebruiken wordt gebruikt om het certificaatkenmerk te kiezen waaruit een specifiek veld van de identiteit kan worden gevonden. De keuzes zijn:

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

Als de identiteitsopslag moet worden gericht op Active Directory of LDAP (externe identiteitsbron), kan een functie genaamd Binaire Vergelijking worden gebruikt. Binaire vergelijking voert een raadpleging uit van de identiteit in Active Directory die uit het clientcertificaat wordt verkregen uit de selectie **Identity From gebruiken**, die tijdens de ISE-verificatiefase plaatsvindt. Zonder Binaire Vergelijking, wordt de identiteit eenvoudig verkregen van het cliëntcertificaat en niet opgezocht in Actieve Folder tot de fase van de Vergunning van ISE wanneer een Actieve Externe Groep van de Folder als voorwaarde, of andere voorwaarden wordt gebruikt die extern aan ISE zouden moeten worden uitgevoerd. Om Binaire Vergelijking te gebruiken, kies in de **Identity Store** de externe identiteitsbron (Active Directory of LDAP) waar de end-identiteits-account kan worden gevonden.

Dit is een configuratievoorbeeld wanneer de identiteit zich in het veld Common Name (CN) van het clientcertificaat bevindt, met Binaire vergelijking ingeschakeld (optioneel):



Certificaatverificatieprofiel

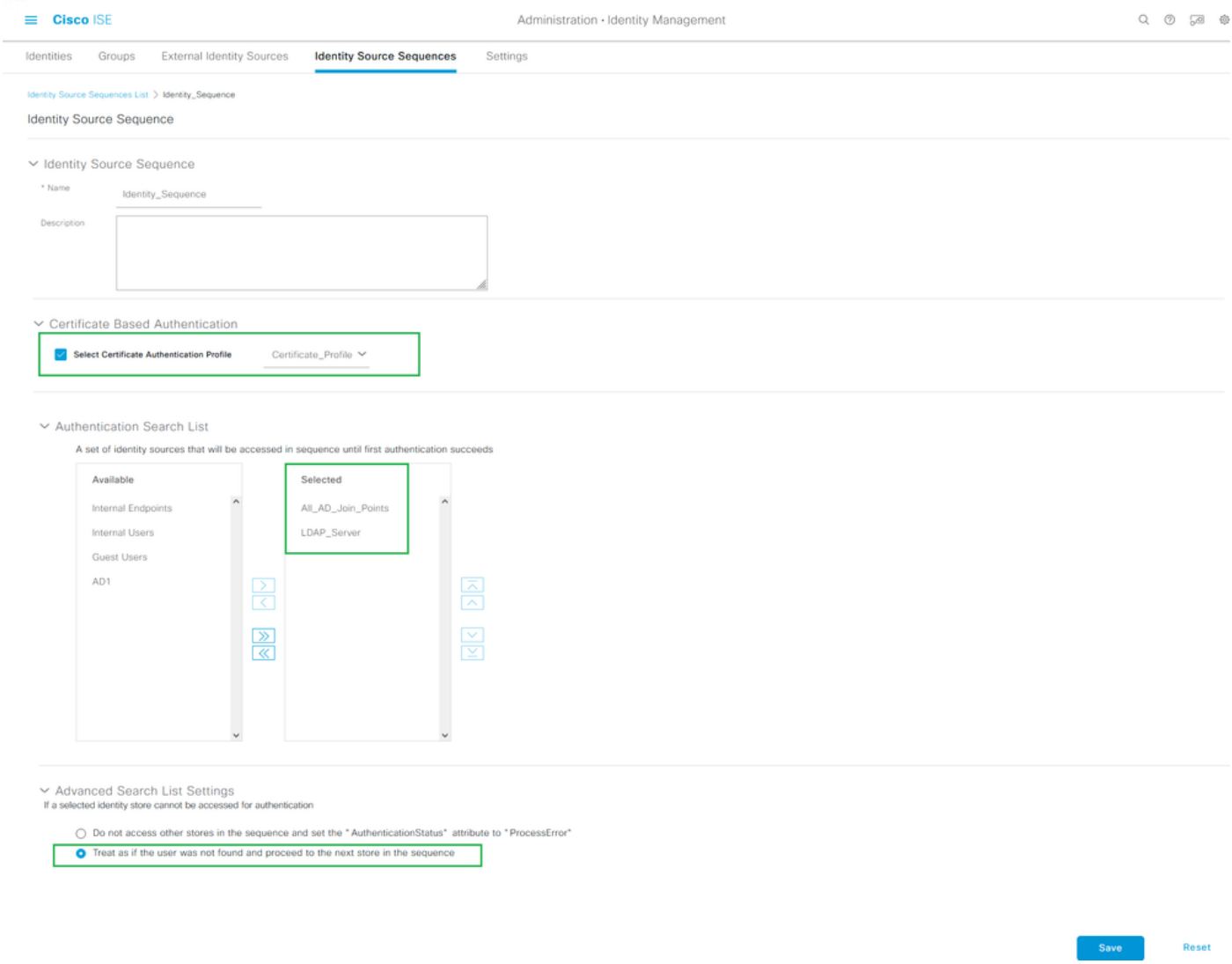
Meer informatie is te vinden in de *beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Basic Setup > Cisco ISE CA-service > Cisco ISE configureren voor het gebruik van certificaten voor het verifiëren van persoonlijke apparaten >* [*Een certificaatverificatieprofiel maken voor een op TLS gebaseerde verificatie*](#).

Stap 7. Voeg toe aan een identiteitsbronreeks

De Identity Source Sequence kan worden gemaakt vanuit de ISE GUI. Navigeer naar **Administration > Identity Management**. Onder **Identity Source Sequences** klikt u op **Add**.

De volgende stap is om het Certificaatverificatieprofiel toe te voegen aan een Identity Source Sequence die de mogelijkheid biedt om meerdere Active Directory-samenvoegingspunten of een combinatie van interne/externe identiteitsbronnen te omvatten, zoals gewenst, die vervolgens bindt aan het Verificatiebeleid onder de **Use** kolom.

Het voorbeeld zoals hier getoond staat toe de raadpleging eerst tegen Actieve Folder wordt uitgevoerd, dan als de gebruiker niet wordt gevonden, zal het omhoog op een server LDAP daarna kijken. Voor meerdere identiteitsbronnen. ervoor te zorgen dat **Treat as if the user was not found and proceed to the next store in the sequence** selectievakje ingeschakeld. Dit betekent dat elke identiteitsbron/server wordt gecontroleerd tijdens de verificatieaanvraag.



Identity Source Sequence

Anders kunt u ook alleen het certificaatverificatieprofiel aan het verificatiebeleid binden.

Stap 8. Bepaal de toegestane protocolservice

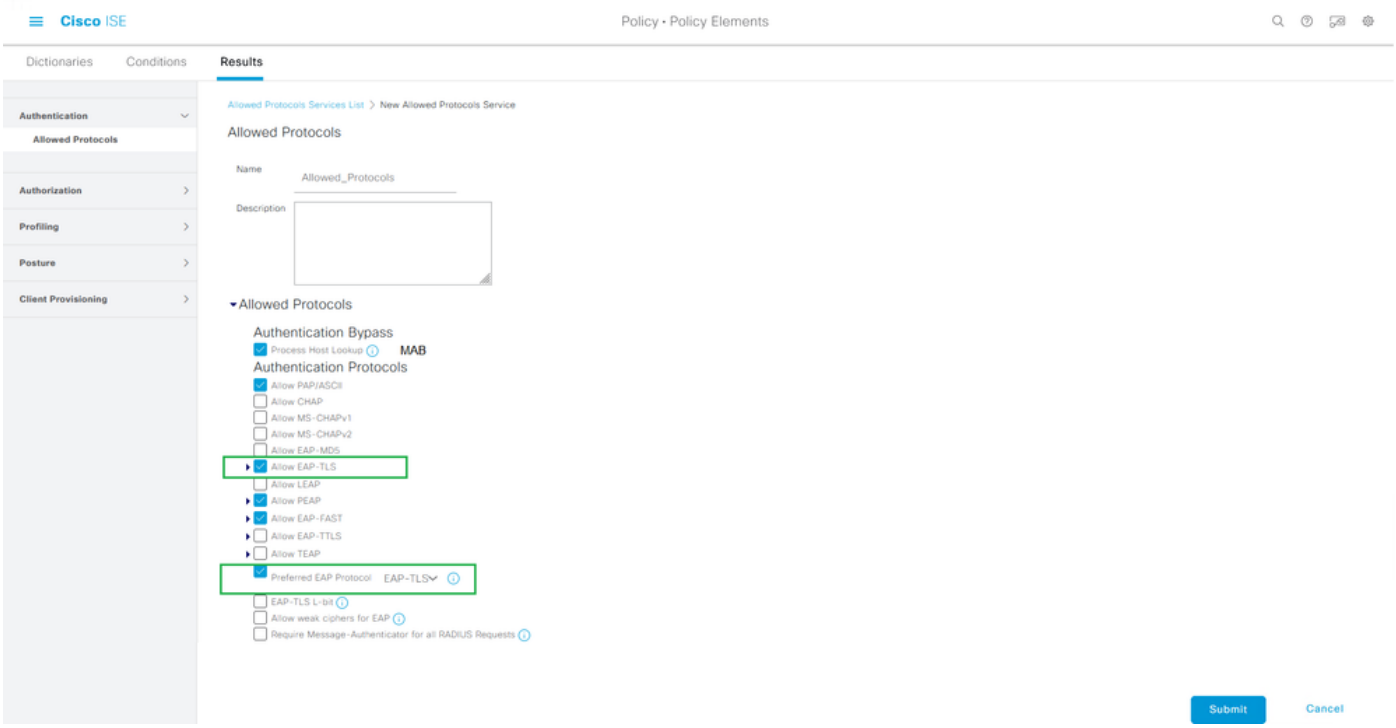
De Toegestane Dienst van Protocollen laat slechts dat authentificatiemethodes/protocollen toe die ISE tijdens de Verificatie van de RADIUS steunt. Ga om vanuit de ISE GUI te configureren naar **Policy > Policy Elements: Resultaten > Verificatie > Toegestane Protocollen** en vervolgens bindt het als een element aan het Verificatiebeleid.

> **Opmerking: Verificatie Omzeilen > Proces Host Lookup** heeft betrekking op MAB ingeschakeld op ISE.

Deze instellingen moeten hetzelfde zijn als wat wordt ondersteund en geconfigureerd op de aanvrager (op het eindpunt). Anders wordt over het verificatieprotocol niet onderhandeld zoals verwacht en kan RADIUS-communicatie mislukken. In een real-world ISE-configuratie wordt aanbevolen om elk verificatieprotocol dat in de omgeving wordt gebruikt in te schakelen, zodat ISE en de aanvrager kunnen onderhandelen en authenticeren zoals verwacht.

Dit zijn de standaardwaarden (samengevouwen) wanneer een nieuw exemplaar van de services van het toegestane protocol wordt gemaakt.

Opmerking: U moet minimaal **EAP-TLS** inschakelen aangezien ISE en onze aanvrager in dit configuratievoorbeeld via EAP-TLS verifiëren.



Protocollen om ISE toe te staan tijdens authenticatieaanvraag te gebruiken voor endpointaanvrager

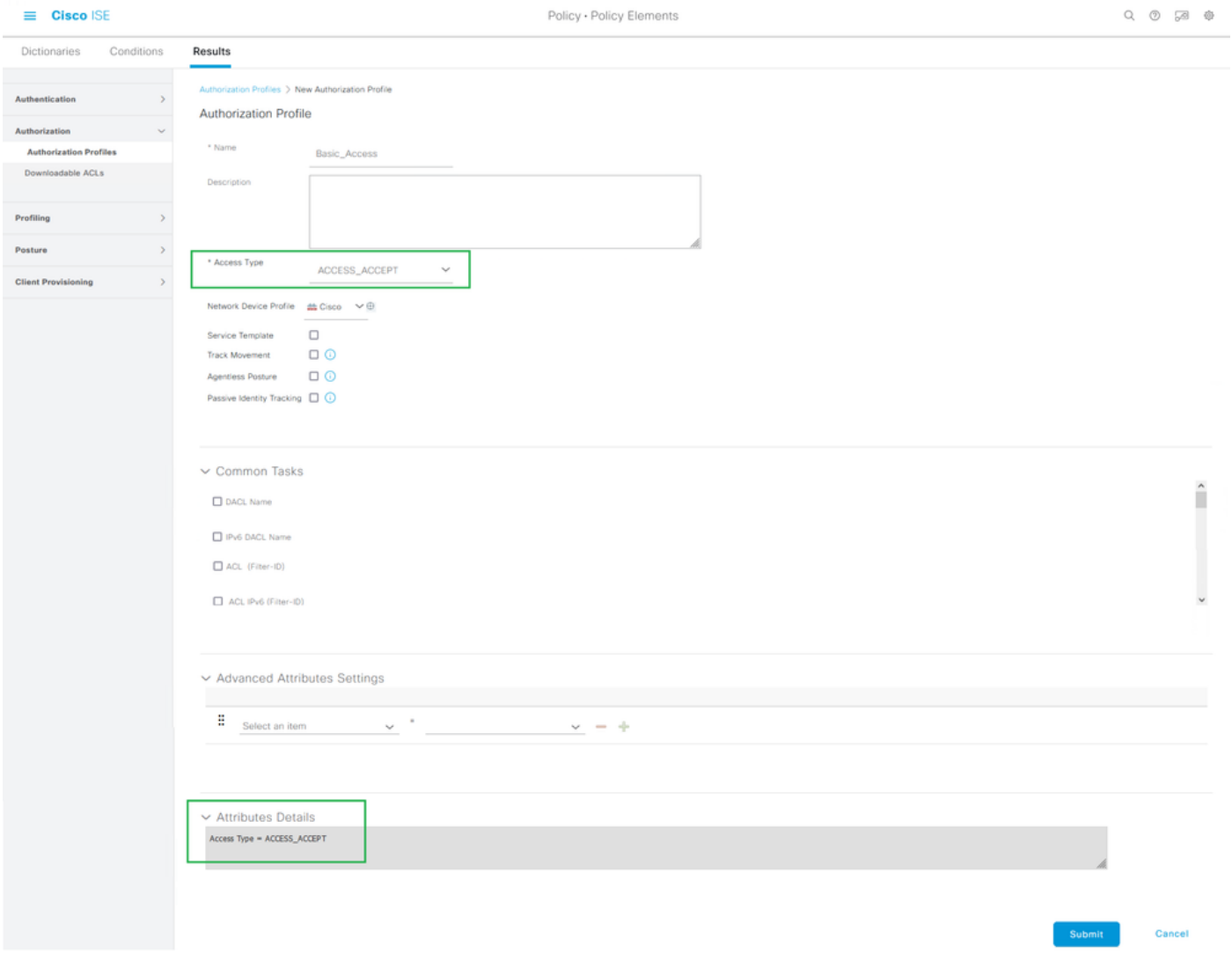
Opmerking: Het gebruik van "VoorkeursEAP-Protocol" ingesteld op de waarde "EAP-TLS" zal ervoor zorgen dat ISE het EAP-TLS-protocol aanvraagt als het eerste protocol dat aan de IEEE 802.1x-aanvrager voor endpoints wordt aangeboden. Deze instelling is handig als u vaak op de meeste endpoints die met ISE zullen worden geverifieerd, via EAP-TLS wilt verifiëren.

Stap 9. Maak het autorisatieprofiel aan

Het laatste beleidselement dat nodig is om te bouwen is het Autorisatieprofiel, dat bindt aan het Autorisatiebeleid en het gewenste toegangsniveau geeft. Het autorisatieprofiel is gebonden aan het autorisatiebeleid. Ga naar om het vanuit ISE GUI te configureren **Policy > Policy Elements: Results > Authorization > Authorization Profiles** en klik op **Add**.

Het autorisatieprofiel bevat een configuratie die resulteert in eigenschappen die worden doorgegeven van ISE naar de NAD voor een bepaalde RADIUS-sessie, waarin deze eigenschappen worden gebruikt om het gewenste niveau van netwerktoegang te bereiken.

Zoals hier getoond, gaat het eenvoudig RADIUS access-Accept over als het **toegangstype**, maar er kunnen extra items gebruikt worden bij de eerste verificatie. Opmerking **Kenmerkgegevens** helemaal onderaan, die de samenvatting van de kenmerken bevat die ISE naar het NAD stuurt wanneer het overeenkomt met een bepaald autorisatieprofiel.



Vergunningsprofiel - Beleidselement

Meer informatie over het ISE-autorisatieprofiel en -beleid vindt u in de *beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Segmentatie >* [*Autorisatiebeleid*](#).

Beveiligingsbeleid

Verificatie- en autorisatiebeleid worden gemaakt vanuit de ISE GUI, kies **Policy > Policy Sets**. Deze zijn standaard ingeschakeld op ISE 3.x. Wanneer u ISE installeert, is er altijd één Policy Set gedefinieerd, wat de standaard Policy Set is. De standaard Policy Set bevat vooraf gedefinieerde en standaardverificatie, autorisatie en uitzonderingsregels.

De beleidssets worden hiërarchisch geconfigureerd, zodat de ISE-beheerder gelijksoortig beleid in termen van de bedoeling kan groeperen in verschillende sets voor gebruik binnen een verificatieverzoek. Aanpassing- en groepsbeleid is vrijwel onbeperkt. Als zodanig kan één Policy Set worden gebruikt voor draadloze endpointverificatie voor netwerktoegang, terwijl een andere Policy Set kan worden gebruikt voor bekabelde endpointverificatie voor netwerktoegang; of op een andere unieke en differentiërende manier om het beleid te beheren.

Cisco ISE evalueert beleidssets en het beleid binnen gebruikt de top-down aanpak, om eerst een bepaalde beleidsset af te stemmen wanneer alle voorwaarden van die set waar blijken te zijn; waarop ISE het verificatiebeleid en het autorisatiebeleid binnen de beleidsreeks verder evalueert, als volgt:

1. Evaluatie van de beleidsreeks en de beleidsvoorwaarden
2. Verificatiebeleid binnen de overeenkomende beleidsset
3. Autorisatiebeleid - lokale uitzonderingen
4. Vergunningsbeleid - Algemene uitzonderingen
5. Vergunningsbeleid

Policy Exceptions bestaat globaal voor alle Policy Sets of lokaal binnen een specifieke Policy Set. Deze Policy Exceptions worden behandeld als deel van het Autorisatiebeleid, omdat ze betrekking hebben op welke machtigingen of resultaten worden gegeven voor netwerktoegang voor een bepaald tijdelijk scenario.

In de volgende paragraaf wordt beschreven hoe u de configuratie- en beleidselementen kunt combineren om aan het beleid voor ISE-verificatie en -autorisatie te binden om een eindpunt te verifiëren via EAP-TLS.

Stap 10. De beleidsset maken

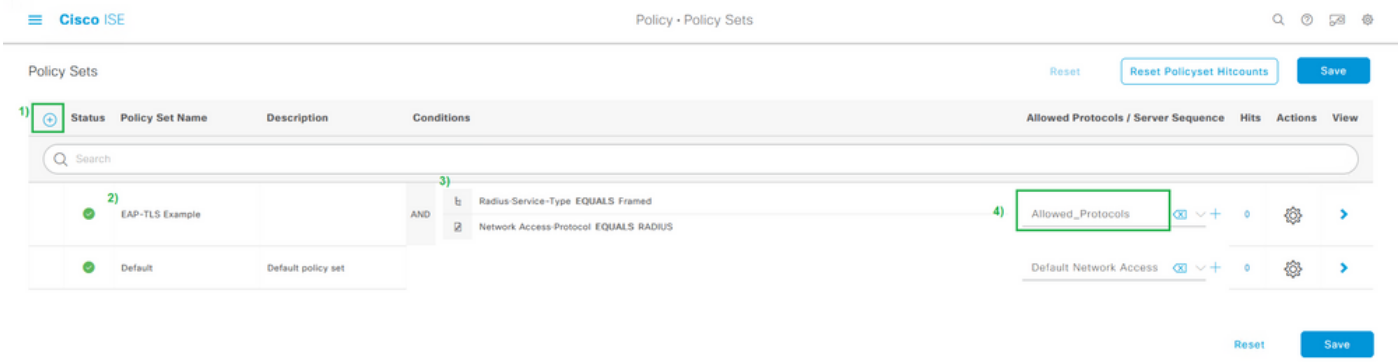
Een Policy Set is een hiërarchische container die bestaat uit een enkele, door de gebruiker gedefinieerde regel die de toegestane protocol- of serversequentie voor netwerktoegang aangeeft, evenals authenticatie- en autorisatiebeleid en beleidsuitzonderingen, die allemaal ook zijn geconfigureerd met door de gebruiker gedefinieerde voorwaarden.

Om een beleidsset te maken vanuit de ISE GUI, navigeer naar **Policy > Policy Set** en klik vervolgens op het plusteken (**+**) in de linkerbovenhoek, zoals in deze afbeelding.

Een nieuwe beleidsset toevoegen

De beleidsset zal dit eerder geconfigureerde beleidselement binden/combineren en wordt gebruikt om te bepalen welke beleidsset moet worden gekoppeld in een bepaalde RADIUS-verificatieaanvraag (access-request):

- Binden: Toegestane protocolservices



Vastgestelde voorwaarden en lijst met toegestane protocollen definiëren

In dit voorbeeld worden specifieke kenmerken en waarden gebruikt die in de RADIUS-sessie zouden worden weergegeven om IEEE 802.1x (framed attribuut) af te dwingen, ook al is het mogelijk dat het RADIUS-protocol moet worden versterkt. Om de beste resultaten te behalen, gebruikt u alleen unieke RADIUS-sessiekenmerken die van toepassing zijn op de gewenste

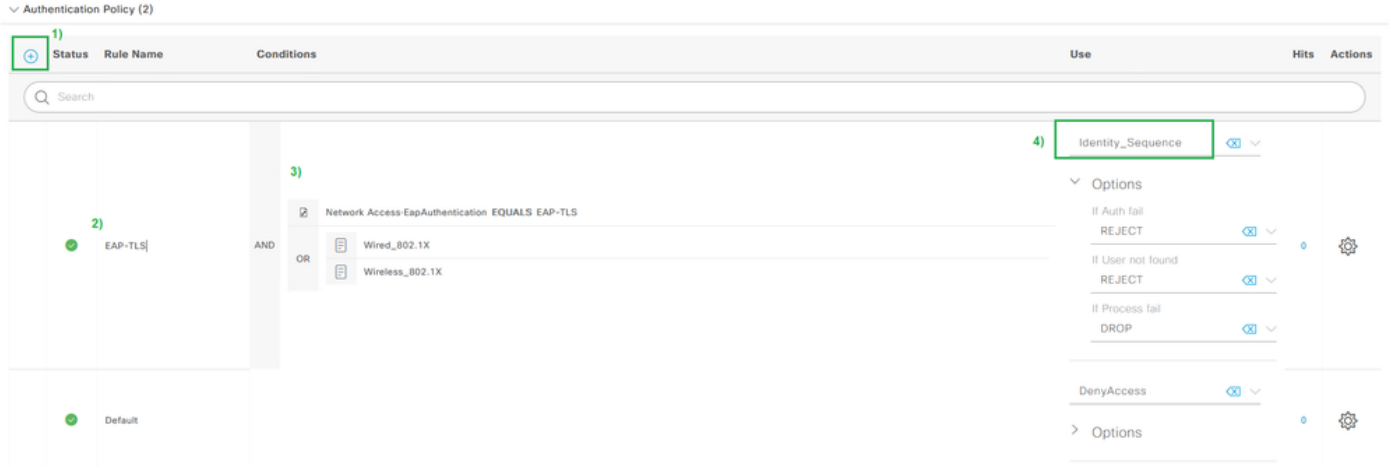
bedoeling, zoals Network Device Groepen of specifiek voor Wired 802.1x, Wireless 802.1x of zowel bekabeld 802.1x als Wireless 802.1x.

Meer informatie over Policy Sets on ISE kunt u vinden in de *beheerdershandleiding* van *Cisco Identity Services Engine. Release 3.1 > Hoofdstuk: Segmentatie >* [Beleidssets](), [Verificatiebeleid]() *en secties* [Autorisatiebeleid]().

Stap 1. Een verificatiebeleid maken

Binnen de beleidsset zal het verificatiebeleid deze beleidselementen die eerder zijn geconfigureerd om te worden gebruikt, verbinden/combineren met voorwaarden om te bepalen wanneer een verificatieregel moet worden aangepast.

- Binden: Certificaatverificatieprofiel of Identity Source Sequence.

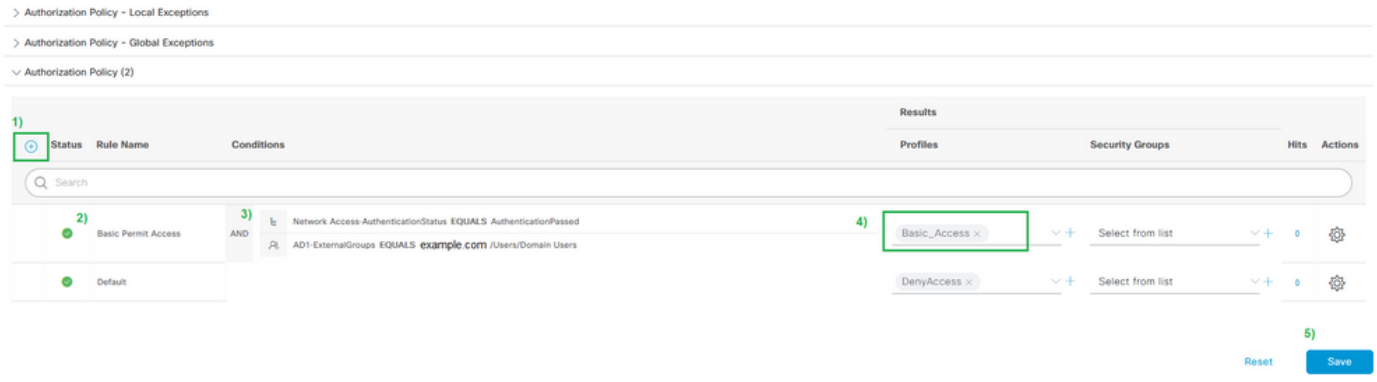


Voorbeeld van verificatiebeleidsregel

Stap 12. Maak het autorisatiebeleid aan

Binnen de Reeks van het Beleid, bindt het Beleid van de Vergunning/combineert deze die beleidselementen eerder worden gevormd om met voorwaarden worden gebruikt te bepalen wanneer een Regel van de Vergunning moet worden aangepast. Het voorbeeld hier is voor **Gebruikersverificatie** omdat de voorwaarden verwijzen naar de beveiligingsgroep **Domeingebruikers** in Active Directory.

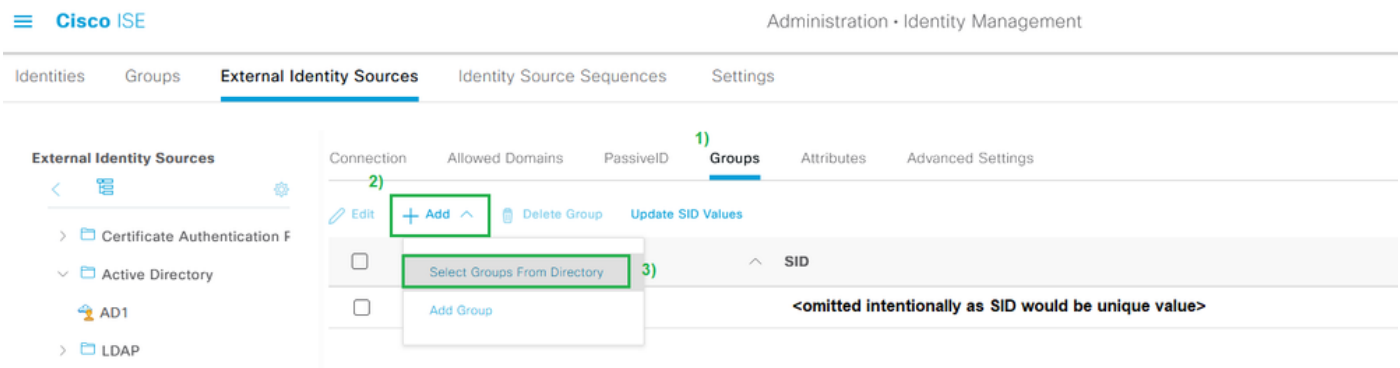
- Binden: Autorisatieprofiel



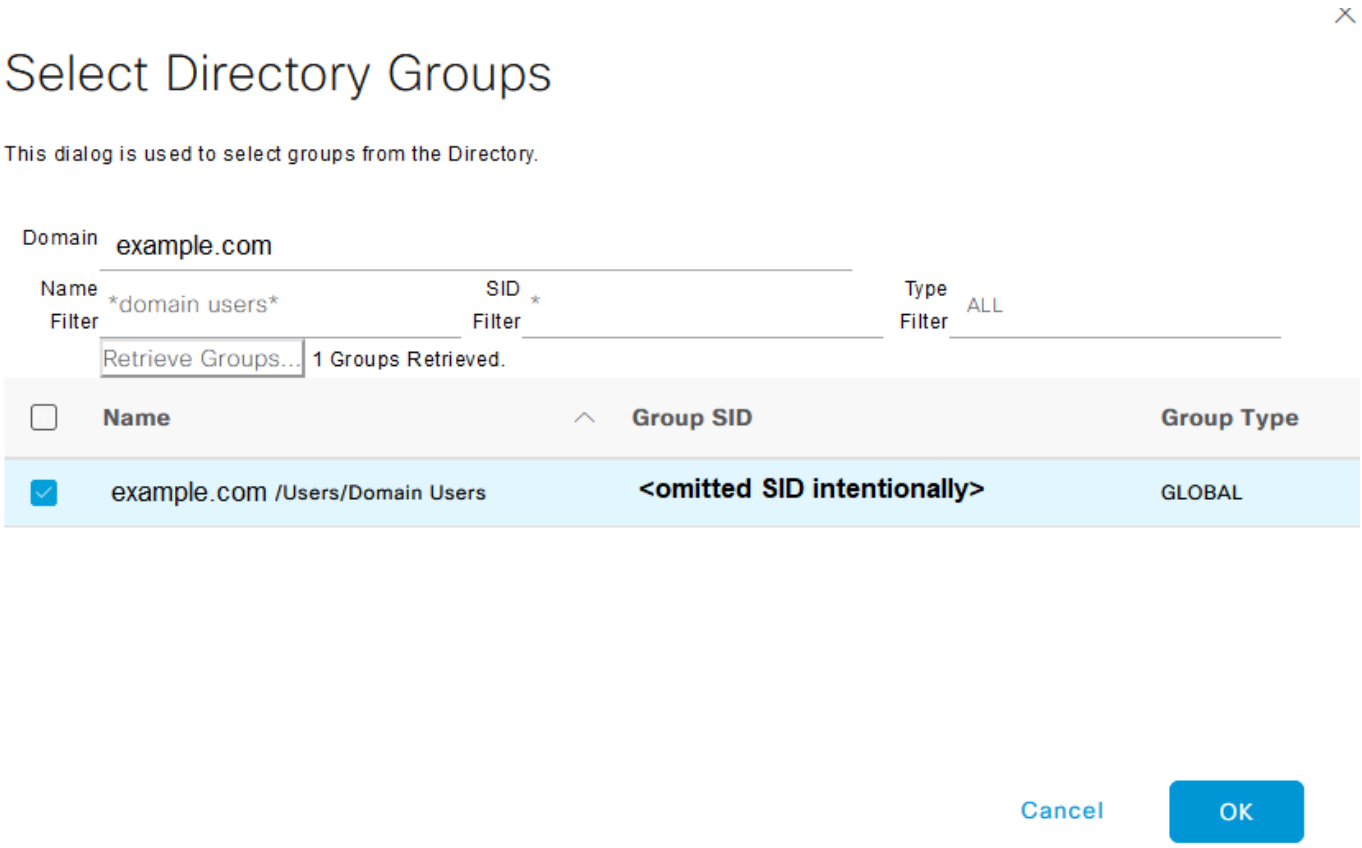
Voorbeeld van autorisatiebeleidsregel

Om een externe groep (zoals van Active Directory of LDAP) toe te voegen, moet u de groep toevoegen van de externe server instantie. In dit voorbeeld komt het van de ISE UI: **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups**. Kies op het

tabblad Groep **Add > Select Groups from Directory** en gebruik het "Name filter" om te zoeken naar alle groepen (*) of specifieke groepen, zoals Domeingebruikers (*domeingebruikers*) om groepen op te halen.



Om externe groepen te gebruiken in ISE-beleid, moet u groep toevoegen uit Directory



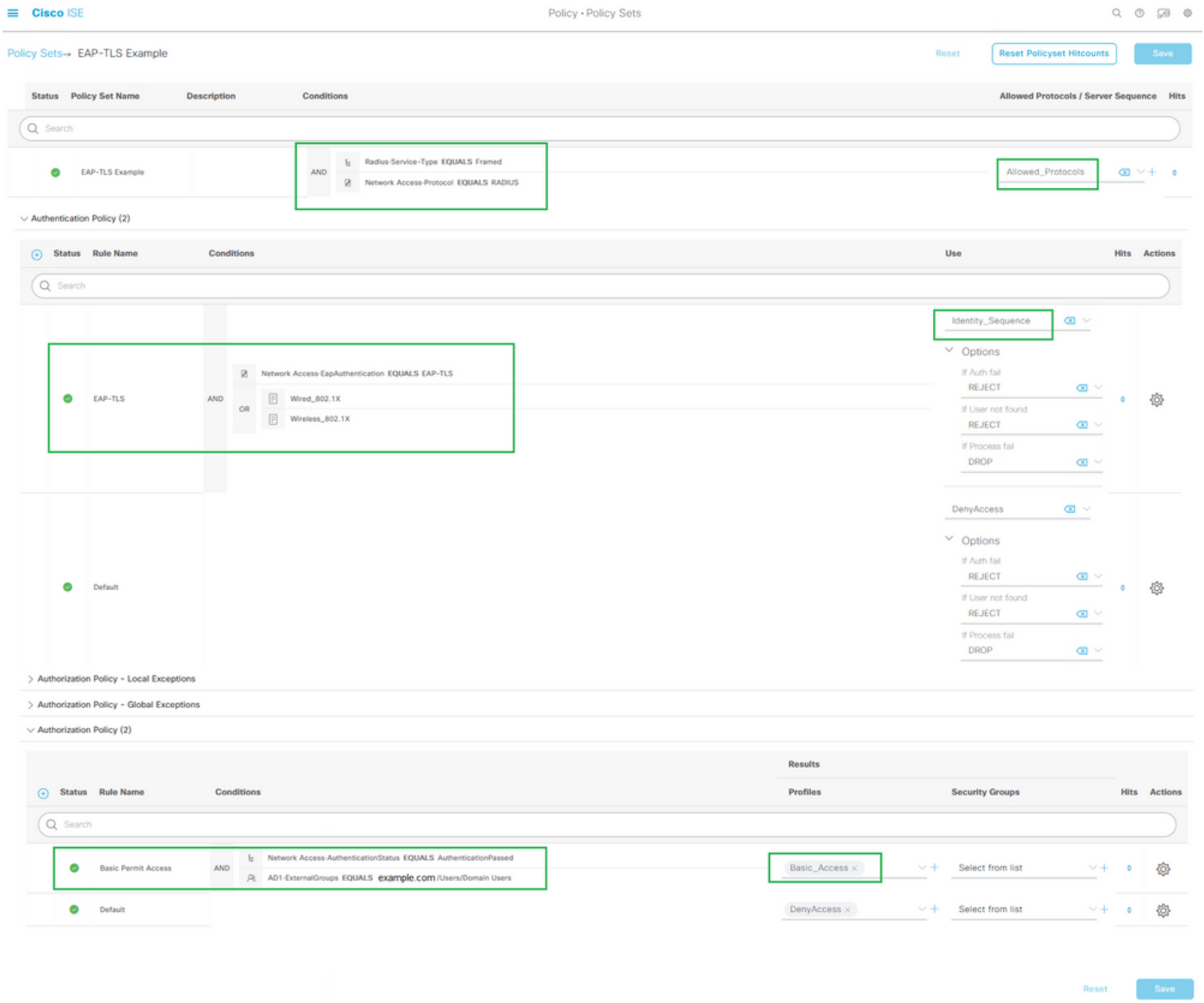
Zoeken in de externe map - Active Directory Voorbeeld

Nadat u het aanvinkvakje naast elke groep die u wilt gebruiken in het beleid binnen ISE aanvinkt, vergeet niet op **OK** en/of **Opslaan** te klikken om de wijzigingen op te slaan.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Zodra alle globale configuratie en beleidselementen de Policy Set binden, ziet de configuratie er voor de Gebruikersverificatie via EAP-TLS hetzelfde uit als dit beeld:

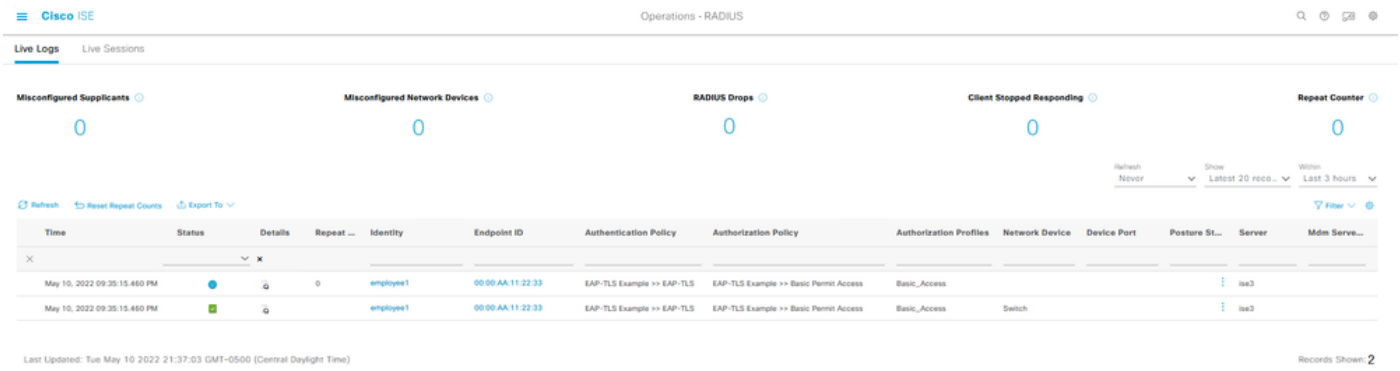


Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Wanneer de configuratie is voltooid, sluit u het eindpunt aan op verificatie. De resultaten zijn te vinden in de ISE GUI. Kiezen **Operations > Radius > Live Logs**, zoals in deze afbeelding wordt getoond.

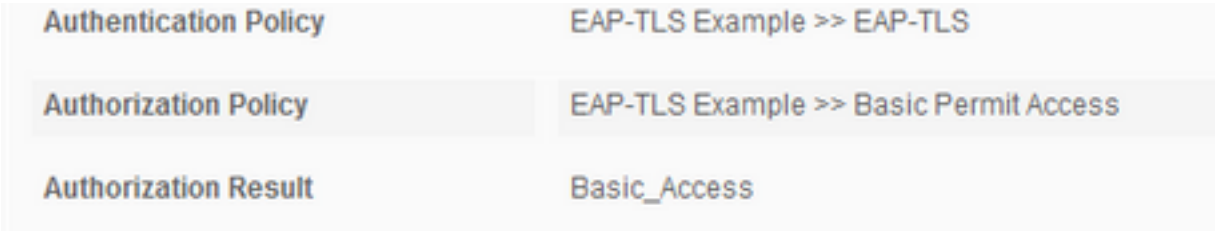
Voor bewustwording zijn de Live logs voor RADIUS en TACACS+ (Device Admin) beschikbaar voor de verificatiepogingen/activiteit tot de afgelopen 24 uur en voor de afgelopen 100 records. Als u dit type van rapporteringsgegevens na deze tijdspanne wenst te zien, dan zult u de rapporten moeten gebruiken, specifiek: **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications**.



Live logs" />*Voorbeeld van uitvoer vanuit straal > Live logs*

In de RADIUS Live Logs in ISE verwacht u informatie te vinden over de RADIUS-sessie, die sessiekenmerken omvat, en andere nuttige informatie om gedrag te diagnosticeren dat tijdens een verificatiestroom is waargenomen. Klik op de **details** pictogram om de gedetailleerde weergave van de sessie te openen om sessiekenmerken en gerelateerde informatie die specifiek is voor deze verificatiepoging te bekijken.

Om problemen op te lossen, is het belangrijk om ervoor te zorgen dat het juiste beleid wordt afgestemd. In dit configuratievoorbeeld wordt het gewenste verificatie- en autorisatiebeleid aangepast zoals verwacht, zoals in de afbeelding wordt getoond:



In de gedetailleerde weergave worden deze eigenschappen gecontroleerd om te verifiëren dat de verificatie zich gedraagt zoals verwacht wordt in het ontwerp als onderdeel van dit configuratievoorbeeld:

- **Gebeurtenis**
  Hierin staat of de verificatie is geslaagd.In een werkscenario is de waarde: **5200 verificatie geslaagd**.

- **Username**
  Dit omvat de end-identiteits die werd gehaald uit het clientcertificaat dat werd aangeboden aan ISE.In een werkscenario is dit de gebruikersnaam van de gebruiker die bij het eindpunt is ingelogd (namelijk worker1 uit de vorige afbeelding).

- **Endpoint-id**
  Voor bekabeld/draadloos is deze waarde het MAC-adres van de netwerkinterfacekaart (NIC) vanaf het eindpunt.In een werkscenario wordt dit het MAC-adres van het eindpunt tenzij de verbinding via VPN verloopt, in welk geval het IP-adres van het eindpunt kan zijn.

- **Verificatiebeleid**
  Toont het aangepaste verificatiebeleid voor de gegeven sessie op basis van sessiekenmerken die overeenkomen met de beleidsvoorwaarden.In een werkend scenario, is dit het verwachte authentificatiebeleid zoals gevormd.Als je naar een ander beleid kijkt,

betekent dat dat het verwachte beleid ten opzichte van de voorwaarden in het beleid niet als waar werd beoordeeld. In dit geval, herzie de zittingseigenschappen en zorg ervoor dat elk beleid verschillende maar unieke voorwaarden voor elk beleid bevat.

- Vergunningsbeleid
  Toont het afgestemde machtigingsbeleid voor de bepaalde sessie op basis van sessiekenmerken die overeenkomen met de beleidsvoorwaarden.In een werkscenario is dit het verwachte autorisatiebeleid zoals het is geconfigureerd.Als je naar een ander beleid kijkt, betekent dat dat het verwachte beleid ten opzichte van de voorwaarden in het beleid niet als waar werd beoordeeld. In dit geval, herzie de zittingseigenschappen en zorg ervoor dat elk beleid verschillende maar unieke voorwaarden voor elk beleid bevat.

- Resultaat van autorisatie
  Op basis van het overeenkomende autorisatiebeleid toont dit het autorisatieprofiel dat in de gegeven sessie is gebruikt.In een werkend scenario is dit dezelfde waarde als in het beleid. Het is goed om te controleren voor controledoeleinden en ervoor te zorgen dat het juiste autorisatieprofiel werd geconfigureerd.

- Beleidsserver
  Dit omvat de hostnaam van het ISE Policy Service Node (PSN) dat betrokken was bij de verificatiepoging.In een werkscenario ziet u alleen verificaties die naar de eerste PSN-knooppunt gaan zoals geconfigureerd op het NAD (ook bekend als randapparaat), tenzij dat PSN niet operationeel was of als failover is opgetreden, zoals vanwege een hogere latentie dan verwacht of als er een verificatietime-out optreedt.

- Verificatiemethode
  Toont de verificatiemethode die in de gegeven sessie is gebruikt. In dit voorbeeld ziet u de waarde als **dot1x**.In een werkscenario, gebaseerd op dit configuratievoorbeeld, ziet u de waarde als **dot1x**. Als u een andere waarde ziet, kan dit betekenen dat dot1x is mislukt of dat niet is geprobeerd.

- Verificatieprotocol
  Toont de verificatiemethode die in de gegeven sessie is gebruikt. In dit voorbeeld ziet u de waarde als "EAP-TLS".In een werkscenario dat is gebaseerd op dit configuratievoorbeeld, ziet u de waarde altijd als "EAP-TLS". Als u een andere waarde ziet, hebben de aanvrager en ISE niet met succes over EAP-TLS onderhandeld.

- Netwerkapparaat
  Toont de naam van het netwerkapparaat, zoals die in ISE is geconfigureerd, voor het NAD (ook bekend als het randapparaat) dat betrokken is bij de verificatiepoging tussen het eindpunt en ISE.In een werkscenario wordt deze naam altijd gegeven in ISE UI: **Administration > System: Network Devices.** Op basis van die configuratie wordt het IP-adres van de NAD (ook bekend als het randapparaat) gebruikt om te bepalen van welk netwerkapparaat de verificatie afkomstig is van waaruit het kenmerk **NAS IPv4-adressessie** is opgenomen.

Dit is in geen geval een volledige lijst van alle mogelijke sessiekenmerken die kunnen worden bekeken voor probleemoplossing of andere zichtbaarheidsdoeleinden, aangezien er andere nuttige kenmerken zijn die kunnen worden geverifieerd. Het wordt aanbevolen om alle sessiekenmerken te bekijken om bekend te worden met alle informatie. U kunt de rechterkant

onder de sectie **Stappen** zien omvatten, die de verrichtingen of het gedrag toont die door ISE worden genomen.

Gemeenschappelijke problemen en technieken voor probleemoplossing

Deze lijst bevat een aantal veelvoorkomende problemen en adviezen voor probleemoplossing en is geenszins bedoeld als een volledige lijst. In plaats daarvan, gebruik dit als gids en ontwikkel uw eigen technieken om problemen op te lossen wanneer ISE betrokken is.

Kwestie: Ontmoet een verificatiefout (**5400 verificatie mislukt**) of een andere niet-succesvolle verificatiepoging.

- Als er een verificatiefout wordt aangetroffen, klikt u op het pictogram **Details** met informatie over de reden van het mislukken van de verificatie en de stappen die zijn ondernomen. Dit omvat de reden van de storing en de mogelijke oorzaak van de storing.

- Aangezien ISE de beslissing neemt over het authenticatieresultaat, zal ISE de informatie hebben om te begrijpen waarom de authenticatiepoging niet succesvol was.

Kwestie: De verificatie wordt niet met succes voltooid en de reden voor de storing toont "5440 Endpoint verlaten EAP-sessie en gestart nieuwe" of "5411 Supplicant gestopt met reageren op ISE".

- Deze mislukkingsreden geeft aan dat de RADIUS-communicatie niet is voltooid voor de timing is verlopen. Aangezien EAP tussen het eindpunt en NAD ligt, moet u de onderbreking controleren die op NAD wordt gebruikt en ervoor zorgen dat het minstens vijf seconden wordt ingesteld.

- Als vijf seconden niet genoeg zijn om dit probleem op te lossen, raden we aan om het enkele malen met vijf seconden te verhogen en opnieuw te testen om te controleren of deze techniek dit probleem zal oplossen.

- Als het probleem niet uit de vorige stappen is opgelost, raden we aan ervoor te zorgen dat de authenticatie wordt verwerkt door dezelfde en juiste ISE-PSN-knooppunt en dat het algemene gedrag geen indicatie is van abnormaal gedrag, zoals een hogere latentie dan normaal tussen NAD- en ISE-PSN-knooppunt(en).

- Ook is het een goed idee om te controleren of het eindpunt het clientcertificaat via pakketopname verstuurt als ISE het clientcertificaat niet ontvangt. Het eindpunt (gebruikerscertificaten) vertrouwt dan mogelijk niet op het ISE EAP-verificatiecertificaat. Indien waar bevonden, importeer dan de CA-keten in de juiste certificaatwinkels (Root CA = Trusted Root CA | Intermediaire CA = Trusted Intermediary CA).

Kwestie: Verificatie is succesvol, maar komt niet overeen met het juiste verificatie- en/of autorisatiebeleid.

- Als u een verificatieverzoek tegenkomt dat succesvol is, maar niet voldoet aan de juiste verificatie- en/of autorisatieregels, raden we aan om sessiekenmerken te bekijken om ervoor te zorgen dat de gebruikte voorwaarden nauwkeurig zijn en aanwezig zijn in de RADIUS-

sessie.

- ISE evalueert dit beleid vanuit een top-down-benadering (met uitzondering van Posture Policies). U moet eerst bepalen of het beleid dat werd aangepast boven of onder het gewenste beleid was om aan te passen. Het verificatiebeleid wordt eerst en onafhankelijk van het autorisatiebeleid beoordeeld. Als het Verificatiebeleid correct wordt aangepast, dan heeft het "22037-verificatie doorgegeven" in de Verificatiedetails onder de rechtse sectie genaamd Stappen.

- Als het gewenste beleid boven het afgestemde beleid uitkomt, betekent dit dat de som van de voorwaarden voor het gewenste beleid niet waar is gebleken. Het herziet alle attributen en waarden in de conditie en op de sessie om ervoor te zorgen dat het bestaat en er geen spellingfout aanwezig is.

- Als het gewenste beleid onder het afgestemde beleid ligt, betekent dit dat er een ander beleid (boven) werd afgesproken in plaats van het gewenste beleid. Dit kan betekenen dat conditiewaarden niet specifiek genoeg zijn, de voorwaarden worden gedupliceerd in een ander beleid, of de volgorde van het beleid is niet correct. Terwijl het moeilijker wordt om problemen op te lossen, adviseren wij om beleid te beginnen te herzien om de reden te bepalen waarom het gewenste beleid niet werd aangepast. Dit helpt bij het identificeren van de volgende te nemen maatregelen.

Kwestie: De identiteit of gebruikersnaam die tijdens de verificatie wordt gebruikt, was niet de verwachte waarde.

- Als dit gebeurt, als het eindpunt het clientcertificaat verstuurt, gebruikt ISE waarschijnlijk niet het juiste certificaatveld in de certificaatverificatiemodule; die tijdens de verificatiefase wordt geëvalueerd.

- Bekijk het clientcertificaat om het exacte veld te vinden met de gewenste identiteit/gebruikersnaam en controleer of hetzelfde veld geselecteerd is uit: **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

Kwestie: Verificatie is niet succesvol bij storingsreden "12514 EAP-TLS mislukte SSL/TLS-handdruk vanwege een onbekende CA in de clientcertificaatketen".

- Dit kan voorkomen als het clientcertificaat een certificaat heeft in de CA-keten dat niet is vertrouwd op ISE UI: **Administration > System: Certificates > Trusted Certificates**.

- Dit kan doorgaans gebeuren wanneer het clientcertificaat (op het eindpunt) een CA-keten heeft die verschilt van de CA-keten van het certificaat die is ondertekend met ISE voor EAP-verificatie.

- Zorg er voor dat de CA-keten van het clientcertificaat op ISE wordt vertrouwd en de CA-keten van het ISE EAP-verificatieserver op het eindpunt wordt vertrouwd.
  - Ga voor Windows OS en Chrome naar **Start > Run MMC > Add/Remove Snap-In > Certificates > User**

Certificates.
- voor Firefox: Importeer de CA-keten (niet het end-identiteits certificaat) die moet worden vertrouwd op Web Server.

Gerelateerde informatie

- Cisco Identity Services Engine > Installatie- en upgrade-handleidingen
- Cisco Identity Services Engine > Configuratiehandleidingen
- Cisco Identity Services Engine > Compatibiliteitsinformatie
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Secure Access > Netwerkapparaten definiëren in Cisco ISE-software
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Segmentatie > Beleidssets
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Segmentatie > Verificatiebeleid
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Segmentatie > Autorisatiebeleid
- Cisco Identity Services Engine > Configuratiehandleidingen > Active Directory-integratie met Cisco ISE-lijnkaart 2.x
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Segmentatie > Netwerktoegangsservice > Netwerktoegang voor gebruikers
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Basisinstallatie > Certificaatbeheer in Cisco ISE
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.1 > Hoofdstuk: Basic Setup > Cisco ISE CA-service > Cisco ISE configureren voor het gebruik van certificaten voor het verifiëren van persoonlijke apparaten > Een certificaatverificatieprofiel maken voor een op TLS gebaseerde verificatie
- Cisco Identity Services Engine > Configuratievoorbeelden en TechNotes > ISE 2.0-portal voor certificaatprovisioning configureren
- Cisco Identity Services Engine > Configuratievoorbeelden en TechNotes > Installeer een CA-ondertekend certificaat van derden in ISE
- Draadloos LAN (WLAN) > Configuratievoorbeelden en TechNotes > EAP-TLS begrijpen en configureren met WLC en ISE
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.