

# Konfigurieren der EAP-TLS-Authentifizierung mit der ISE

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Abrufen von Server- und Clientzertifikaten](#)

[Schritt 1: Erstellen einer Zertifikatsignierungsanforderung von der ISE](#)

[Schritt 2: Importieren von Zertifizierungsstellenzertifikaten in die ISE](#)

[Schritt 3: Clientzertifikat für Endpunkt abrufen](#)

[Netzwerkgeräte](#)

[Schritt 4: Netzwerkzugriffgerät der ISE hinzufügen](#)

[Richtlinienelemente](#)

[Schritt 5: Externe Identitätsquelle verwenden](#)

[Schritt 6: Erstellen des Zertifikats-Authentifizierungsprofils](#)

[Schritt 7: Zu einer Identitätsquellensequenz hinzufügen](#)

[Schritt 8: Definieren des Diensts für zulässige Protokolle](#)

[Schritt 9: Erstellen des Autorisierungsprofils](#)

[Sicherheitsrichtlinien](#)

[Schritt 10: Erstellen des Policy Sets](#)

[Schritt 11: Erstellen einer Authentifizierungsrichtlinie](#)

[Schritt 12: Erstellen der Autorisierungsrichtlinie](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Häufige Probleme und Verfahren zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird die Erstkonfiguration als Beispiel für die Einführung der EAP-TLS-Authentifizierung (Extensible Authentication Protocol-Transport Layer Security) mit der Cisco Identity Services Engine (ISE) beschrieben. Der Schwerpunkt liegt auf der ISE-Konfiguration, die auf mehrere Szenarien angewendet werden kann, wie z. B. (aber nicht beschränkt auf) die Authentifizierung mit einem IP-Telefon/Endpunkt, der über Wired oder Wireless verbunden ist.

Im Rahmen dieses Leitfadens sollten Sie die folgenden Phasen des ISE (RADIUS)-Authentifizierungsflusses verstehen:

- Authentifizierung - Identifiziert und validiert die End-Identität (Computer, Benutzer usw.), die den Netzwerkzugriff anfordert.

- Autorisierung - Bestimmen Sie, welche Berechtigungen/Zugriffe der End-Identität auf das Netzwerk gewährt werden sollen.
- Accounting - Dient zum Melden und Verfolgen der Netzwerkaktivität der End-Identität nach dem Netzwerkzugriff.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis des EAP- und RADIUS-Kommunikationsflusses
- Grundlegendes RADIUS-Authentifizierungswissen mit zertifikatbasierten Authentifizierungsmethoden hinsichtlich des Kommunikationsflusses.
- Verständnis der Unterschiede zwischen Dot1x und MAC Authentication Bypass (MAB).
- Grundlegendes Verständnis der Public Key Infrastructure (PKI)
- Vertrautheit mit dem Abrufen signierter Zertifikate von einer Zertifizierungsstelle (Certificate Authority, CA) und dem Verwalten von Zertifikaten auf den Endpunkten
- Konfiguration von Einstellungen im Zusammenhang mit Authentifizierung, Autorisierung und Abrechnung (AAA) (RADIUS) auf einem Netzwerkgerät (kabelgebunden oder Wireless).
- Konfiguration der Komponente (am Endpunkt) zur Verwendung mit RADIUS/802.1x

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE Version 3.x
- CA: Ausstellung von Zertifikaten (kann eine Enterprise-CA, eine Drittanbieter- oder öffentliche CA sein oder das [Zertifikatbereitstellungsportal](#) verwenden).
- Active Directory (externe Identitätsquelle) - von Windows Server; soweit [mit der ISE kompatibel](#).
- Netzwerkzugriffgerät (Network Access Device, NAD) - kann als Switch (kabelgebunden) oder [Wireless LAN Controller \(WLC\)](#) (Wireless) für 802.1x/AAA konfiguriert werden.
- Endpunkt - Zertifikate, die für die (Benutzer-)Identität und die Supplikant-Konfiguration ausgestellt werden, die für den Netzwerkzugriff über RADIUS/802.1x authentifiziert werden: Benutzerauthentifizierung. Es ist möglich, ein Computerzertifikat abzurufen, es wird in diesem Beispiel jedoch nicht verwendet.

**Anmerkung:** Da in diesem Leitfaden ISE Version 3.1 verwendet wird, basieren alle Dokumentationsverweise auf dieser Version. Dieselbe/eine ähnliche Konfiguration ist jedoch bei früheren Versionen der Cisco ISE möglich und wird vollständig unterstützt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Konfigurieren

## Abrufen von Server- und Clientzertifikaten

### Schritt 1: Erstellen einer Zertifikatsignierungsanforderung von der ISE

Der erste Schritt besteht darin, eine CSR-Anforderung (Certificate Signing Request) von der ISE zu generieren und an die Zertifizierungsstelle (CA) (Server) zu senden, um das signierte, an die ISE ausgestellte Zertifikat als Systemzertifikat zu erhalten. Dieses Zertifikat wird von der ISE während der EAP-TLS-Authentifizierung als Serverzertifikat angezeigt. Dies erfolgt über die ISE-Benutzeroberfläche. Navigieren Sie zu **Administration > System: Certificates > Certificate Management > Certificate Signing Requests**. Unter **Certificate Signing Requests**, klicken Sie auf **Generate Certificate Signing Requests (CSR)** wie in diesem Bild dargestellt.

#### Certificate Signing Requests



Zertifikatstypen erfordern unterschiedliche erweiterte Schlüsselverwendungen. In dieser Liste wird festgelegt, welche erweiterten Schlüsselverwendungen für jeden Zertifikatstyp erforderlich sind:

### ISE-Identitätszertifikate

- Mehrfachverwendung (Admin, EAP, Portal, pxGrid) - Client- und Serverauthentifizierung
- Admin - Serverauthentifizierung
- EAP-Authentifizierung - Serverauthentifizierung
- Datagram Transport Layer Security (DTLS)-Authentifizierung - Serverauthentifizierung
- Portal - Serverauthentifizierung
- pxGrid - Client- und Serverauthentifizierung
- Security Assertion Markup Language (SAML) - SAML-Signaturzertifikat
- ISE Messaging Service - Generieren eines Signaturzertifikats oder Generieren eines neuen Messaging-Zertifikats

Das Systemzertifikat des ISE Messaging Service ist standardmäßig für die Datenreplikation über alle ISE-Knoten in der Bereitstellung, in der Knotenregistrierung und in anderen Kommunikationen zwischen den Knoten vorgesehen und wird vom ISE Internal Certificate Authority (CA)-Server (intern für ISE) bereitgestellt. Für dieses Zertifikat ist keine Aktion erforderlich.

Das "Admin"-Systemzertifikat wird verwendet, um jeden ISE-Knoten zu identifizieren, z. B. wenn die der Admin-Benutzeroberfläche (Verwaltung) zugeordnete API verwendet wird, sowie für einige Kommunikation zwischen Knoten. Um die ISE zum ersten Mal einzurichten, legen Sie das "Admin"-Systemzertifikat fest. Diese Aktion steht nicht in direktem Zusammenhang mit diesem Konfigurationsleitfaden.

Um IEEE 802.1x über EAP-TLS (zertifikatbasierte Authentifizierung) auszuführen, müssen Sie Maßnahmen für das "EAP Authentication"-Systemzertifikat ergreifen, da dieses als Serverzertifikat verwendet wird, das dem Endpunkt/Client während des EAP-TLS-Flusses vorgelegt wird. da das

Ergebnis im TLS-Tunnel gesichert ist. Erstellen Sie zunächst einen CSR, um das Systemzertifikat für die "EAP-Authentifizierung" zu erstellen, und geben Sie es an die Mitarbeiter weiter, die den bzw. die CA-Server in Ihrer Organisation (oder den öffentlichen CA-Anbieter) für die Signatur verwalten. Das Endergebnis ist das CA-signierte Zertifikat, das an den CSR gebunden und mit diesen Schritten der ISE zugeordnet wird.


Wählen Sie im CSR-Formular (Certificate Signing Request) die folgenden Optionen aus, um die CSR-Anfrage auszufüllen und den Inhalt abzurufen:

- **Zertifikatverwendung**, wählen Sie für dieses Konfigurationsbeispiel **EAP Authentication**.
- Wenn Sie eine Platzhalteranweisung im Zertifikat verwenden möchten, **\*.example.com**, dann müssen Sie auch die **Allow Wildcard Certificate** Kontrollkästchen. Der beste Ort ist das Feld für das SAN-Zertifikat (Subject Alternative Name), das Kompatibilität für alle Verwendungen und für verschiedene Endpunkt-Betriebssysteme bietet, die möglicherweise in der Umgebung vorhanden sind.
- Wenn Sie keine Platzhalteranweisung im Zertifikat platzieren möchten, wählen Sie die ISE-Knoten aus, denen Sie das CA-signierte Zertifikat (nach dem Signieren) zuordnen möchten. **Anmerkung:** Wenn Sie das CA-signierte Zertifikat, das die Platzhalteranweisung enthält, an mehrere Knoten innerhalb des CSR binden, wird das Zertifikat an jeden ISE-Knoten (oder an die ausgewählten Knoten) in der ISE-Bereitstellung verteilt, und die Dienste werden möglicherweise neu gestartet. Der Neustart der Services wird jedoch automatisch auf jeweils einen Knoten beschränkt. Überwachen Sie den Neustart der Services über das **show application status ise** ISE CLI-Befehl. Als Nächstes müssen Sie das Formular ausfüllen, um den **Betreff** zu definieren. Dazu gehören die Zertifikatfelder Common Name (CN), Organizational Unit (OU), Organization (O), City (L), State (ST) und Country (C). Die **\$FQDN\$**-Variable ist der Wert, der den vollständig qualifizierten Verwaltungsdomänennamen (Hostname + Domänenname) darstellt, der jedem ISE-Knoten zugeordnet ist.
- Die Fehlermeldung **Subject Alternative Name (SAN)** Felder sind ebenfalls auszufüllen, um alle erforderlichen und gewünschten Informationen einzuschließen, die zur Vertrauensbildung verwendet werden sollen. Als Anforderung müssen Sie den DNS-Eintrag definieren, der auf den FQDN der ISE-Knoten verweist, die diesem Zertifikat zugeordnet werden, nachdem das Zertifikat signiert wurde.
- Stellen Sie abschließend sicher, dass Sie den richtigen "Key Type", "Key Length" und "Digest to Sign With" definieren, der den Funktionen des bzw. der CA-Server(s) und unter Berücksichtigung bewährter Sicherheitsverfahren entspricht. Die Standardwerte sind: RSA, 4096 Bit und SHA-384. Verfügbare Optionen und Kompatibilität werden auf dieser Seite in der ISE-Admin-Benutzeroberfläche angezeigt.

Dies ist ein Beispiel für ein ausgefülltes CSR-Formular ohne Verwendung einer Platzhalteranweisung. Stellen Sie sicher, dass Sie die tatsächlichen Werte für die Umgebung verwenden:

## Usage

Certificate(s) will be used for EAP Authentication 

Allow Wildcard Certificates  

## Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise	ise#EAP Authentication
<input checked="" type="checkbox"/> ise2	ise2#EAP Authentication
<input checked="" type="checkbox"/> 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

---

### Subject Alternative Name (SAN)

	DNS Name	▼	ise.example.com	—	+	
	DNS Name	▼	ise2.example.com	—	+	
	DNS Name	▼	ise3.example.com	—	+	

### \* Key type

RSA ▼ 

### \* Key Length

4096 ▼ 

### \* Digest to Sign With


SHA-384 ▼

### Certificate Policies

CSR - Beispiel

Um den CSR zu speichern, klicken Sie auf **Generate**. Klicken Sie auf **Export**, um die CSR-Datei(en) von dieser Eingabeaufforderung aus zu exportieren:



Successfully generated CSR(s) 

Certificate Signing request(s) generated:

ise#EAP Authentication  
ise2#EAP Authentication  
ise3#EAP Authentication

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

Beispiel

CSR exportieren -

Weitere Informationen zu Zertifikaten für die Verwendung mit der ISE finden Sie im *Cisco Identity Services Engine Administrator Guide, Release 3.1* > in folgendem Kapitel: *Grundlegende Einrichtung* > [Zertifikatsverwaltung in Cisco ISE](#) und [Installation eines von einer Zertifizierungsstelle signierten Zertifikats eines Drittanbieters in der ISE](#).

## Schritt 2: Importieren von Zertifizierungsstellenzertifikaten in die ISE

Nachdem die Zertifizierungsstelle das signierte Zertifikat zurückgibt, enthält sie auch die gesamte Zertifizierungsstellenkette, die aus einem Stammzertifikat und einem/mehreren Zwischenzertifikaten besteht. Die ISE-Admin-Benutzeroberfläche erzwingt den Import aller Zertifikate in der Zertifizierungsstellenkette vor der Zuordnung oder dem Hochladen von Systemzertifikaten. Auf diese Weise wird sichergestellt, dass jedes Systemzertifikat der Zertifizierungsstellenkette (auch als vertrauenswürdiges Zertifikat bezeichnet) innerhalb der ISE-Software richtig zugeordnet ist.

Diese Schritte sind die beste Möglichkeit, die Zertifizierungsstellenzertifikate und das Systemzertifikat in die ISE zu importieren:

1. Um das Stammzertifikat in die ISE-GUI zu importieren, navigieren Sie zu **Administration > System: Certificates > Certificate Management**. Unter **Trusted Certificates**, klicken Sie auf **Import** und aktivieren Sie die Kontrollkästchen **Trust for authentication in ISE (Infrastructure)** und **Trust for client authentication** und **Syslog (Endpoints)**.

Trusted For: ⓘ

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services

*Zertifikatverwendung für Zertifizierungsstellenkette*

2. Wiederholen Sie den vorherigen Schritt für alle Zwischenzertifikate, die Teil der Zertifizierungsstellen-Zertifikatskette sind.
3. Wenn alle Zertifikate als Teil der vollständigen Zertifizierungsstellenkette in den ISE-Speicher für vertrauenswürdige Zertifikate importiert wurden, kehren Sie zur ISE-GUI zurück, und navigieren Sie zu **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. Suchen Sie den CSR-Eintrag unter **Anzeigename**, der dem signierten Zertifikat entspricht, klicken Sie auf das Kontrollkästchen des Zertifikats, und klicken Sie dann auf **Bind Certificate**.

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

2)

View Export Delete Bind Certificate All

<input type="checkbox"/>	Friendly Name <sup>1)</sup>	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ise#EAP Authentication	CN=ise. example.com ,O=E...	4096		Tue, 10 May 2022	ise
<input type="checkbox"/>	ise2#EAP Authentication	CN=ise2. example.com ,O=...	4096		Tue, 10 May 2022	ise2
<input type="checkbox"/>	ise3#EAP Authentication	CN=ise3 example.com ,O=...	4096		Tue, 10 May 2022	ise3

*Zertifikat an CSR binden* **Anmerkung:** Sie müssen für jeden CSR jeweils ein CA-signiertes Zertifikat binden. Wiederholen Sie den Vorgang für alle verbleibenden CSRs, die für andere ISE-Knoten in der Bereitstellung erstellt wurden. Klicken Sie auf der nächsten Seite auf **Browse** und wählen Sie die signierte Zertifikatsdatei, definieren Sie einen gewünschten Anzeigenamen, und wählen Sie die Zertifikatsverwendung(en) aus. Senden, um die Änderungen zu speichern.

Bind CA Signed Certificate

\* Certificate File  EXAMPLE\_ISE.cer

Friendly Name  ⓘ

Validate Certificate Extensions  ⓘ

Usage

- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

*Zertifikat für Bindung an CSR auswählen*

4. Zu diesem Zeitpunkt wird das signierte Zertifikat in die ISE-GUI verschoben. Navigieren Sie



ZU **Administration > System: Certificates > Certificate Management: System Certificates** und weisen Sie ihn demselben Knoten zu, für den der CSR erstellt wurde. Wiederholen Sie den gleichen Vorgang für andere Knoten und/oder andere Zertifikatverwendungen.

### **Schritt 3: Clientzertifikat für Endpunkt abrufen**

Für die Erstellung eines Client-Zertifikats zur Verwendung mit EAP-TLS muss ein ähnlicher Prozess auf dem Endpunkt durchgeführt werden. Für dieses Beispiel benötigen Sie ein Clientzertifikat, das signiert und für das Benutzerkonto ausgestellt ist, um die Benutzerauthentifizierung mit ISE durchzuführen. Ein Beispiel, wie ein Clientzertifikat für den Endpunkt aus einer Active Directory-Umgebung abgerufen wird, finden Sie unter: Verständnis und Konfiguration von EAP-TLS mit WLC und ISE > **Configure > [Client für EAP-TLS](#)**.

Aufgrund der verschiedenen Endpunkt- und Betriebssystemtypen werden keine weiteren Beispiele angeführt, da der Prozess unterschiedlich sein kann. Der gesamte Prozess ist jedoch konzeptionell derselbe. Generieren Sie einen CSR, der alle relevanten Informationen enthält, die in das Zertifikat aufgenommen werden sollen, und lassen Sie ihn von der Zertifizierungsstelle signieren, unabhängig davon, ob es sich um einen internen Server in der Umgebung oder ein öffentliches oder Drittanbieter handelt, das diese Art von Service bereitstellt.

Darüber hinaus enthalten die Zertifikatfelder Common Name (CN) und Subject Alternative Name (SAN) die Identität, die während des Authentifizierungsflusses verwendet werden soll. Dies bestimmt auch, wie die Komponente für EAP-TLS hinsichtlich der Identität konfiguriert werden soll: Computer- und/oder Benutzerauthentifizierung, Computerauthentifizierung oder Benutzerauthentifizierung. In diesem Beispiel wird nur die Benutzerauthentifizierung im Rest dieses Dokuments verwendet.

## **Netzwerkgeräte**

### **Schritt 4: Netzwerkzugriffsgesetz der ISE hinzufügen**

Das Netzwerkzugriffsgesetz (Network Access Device, NAD), mit dem ein Endpunkt verbunden ist, wird ebenfalls in der ISE konfiguriert, sodass eine RADIUS/TACACS+-Kommunikation (Device Admin) stattfinden kann. Zwischen NAD und ISE wird ein gemeinsamer geheimer Schlüssel bzw. ein gemeinsames Kennwort zu Vertrauenszwecken verwendet.

Um ein NAD über die ISE-GUI hinzuzufügen, navigieren Sie zu **Administration > Network Resources: Network Devices > Network Devices** und klicke auf **Add**, die in diesem Bild angezeigt wird.

Network Devices

- Default Device
- Device Security Settings

Network Devices List > Switch

### Network Devices

\* Name:

Description:

---

IP Address:  /

---

\* Device Profile:

Model Name:

Software Version:

\* Network Device Group

Device Type:

IPSEC:

Location:

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

\* Shared Secret:

Use Second Shared Secret:

CoA Port:

RADIUS DTLS Settings

DTLS Required:

Shared Secret:

CoA Port:

Issuer CA of ISE Certificates for CoA:

DNS Name:

General Settings

Enable KeyWrap  ⓘ

\* Key Encryption Key \_\_\_\_\_ Show

\* Message Authenticator Code Key \_\_\_\_\_ Show

Key Input Format  ASCII  HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Save Reset

*Beispielkonfiguration für Netzwerkgeräte*

Für die Verwendung mit der ISE-Profilerstellung sollten Sie außerdem SNMPv2c oder SNMPv3 (sicherer) konfigurieren, damit der ISE Policy Service Node (PSN) den NAD über SNMP-Abfragen kontaktieren kann, die mit der Authentifizierung des Endpunkts bei der ISE verbunden sind, um Attribute zu sammeln und genaue Entscheidungen über den verwendeten Endpunkttyp zu treffen. Das nächste Beispiel zeigt, wie Sie SNMP (v2c) über dieselbe Seite wie im vorherigen Beispiel einrichten:



## SNMP Settings

\* SNMP Version

\* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

\* Polling Interval  seconds (Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

\* Originating Policy Services Node

Beispiel einer SNMPv2c-Konfiguration

Weitere Informationen finden Sie im *Cisco Identity Services Engine-Administratorhandbuch, Version 3.1*, > in diesem Kapitel: *Sicherer Zugriff* > [Definition von Netzwerkgeräten in der Cisco ISE](#).

Wenn dies noch nicht geschehen ist, müssen Sie alle AAA-bezogenen Einstellungen auf dem NAD konfigurieren, um sich über die Cisco ISE zu authentifizieren und zu autorisieren.

## Richtlinienelemente

Diese Einstellungen sind Elemente, die entweder an die Authentifizierungsrichtlinie oder die Autorisierungsrichtlinie gebunden werden. In diesem Leitfaden wird in erster Linie jedes Richtlinienelement erstellt und dann der Authentifizierungsrichtlinie oder Autorisierungsrichtlinie zugeordnet. Es ist wichtig zu wissen, dass die Richtlinie erst gültig ist, wenn die Bindung an die Authentifizierungs-/Autorisierungsrichtlinie erfolgreich abgeschlossen wurde.

## Schritt 5: Externe Identitätsquelle verwenden

Eine externe Identitätsquelle ist einfach eine Quelle, in der sich das Endidentitätskonto (Computer oder Benutzer) befindet, das während der ISE-Authentifizierungsphase verwendet wird. Active Directory wird normalerweise verwendet, um die Computerauthentifizierung für das Computerkonto und/oder die Benutzerauthentifizierung für das Endbenutzerkonto in Active Directory zu unterstützen. Die interne Quelle für interne Endpunkte speichert das Computerkonto bzw. den Hostnamen nicht und kann daher nicht mit der Computerauthentifizierung verwendet werden.

Hier sehen Sie die unterstützten Identitätsquellen mit ISE und Protokollen (Authentifizierungstyp), die mit jeder Identitätsquelle verwendet werden können:

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) <b>Note</b> 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

*Funktionen des Identitätsspeichers*

Weitere Informationen zu den Richtlinienelementen finden Sie im *Cisco Identity Services Engine-Administratorhandbuch, Version 3.1* > in folgendem Kapitel: *Segmentierung* > [Richtliniensätze](#).

## Hinzufügen von Active Directory-Sicherheitsgruppen zur ISE

Um Active Directory-Sicherheitsgruppen in ISE-Richtlinien zu verwenden, müssen Sie die Gruppe zuerst dem Active Directory-Verknüpfungspunkt hinzufügen. Wählen Sie in der ISE-GUI **Administration** > **Identity Management: Active Directory** > {select AD instance name / join point} > tab: **Groups** > **Add** > **Select Groups From Directory**.

Weitere Informationen und Anforderungen für die Integration von ISE 3.x in Active Directory finden Sie in diesem Dokument: [Active Directory-Integration in Cisco ISE 2.x](#).

**Anmerkung:** Die gleiche Aktion gilt für das Hinzufügen von Sicherheitsgruppen zu einer LDAP-Instanz. Wählen Sie in der ISE-GUI **Administration > Identity Management: External Identity Sources > LDAP > LDAP instance name > tab: Groups > Add > Select Groups From Directory**.

## Schritt 6: Erstellen des Zertifikats-Authentifizierungsprofils

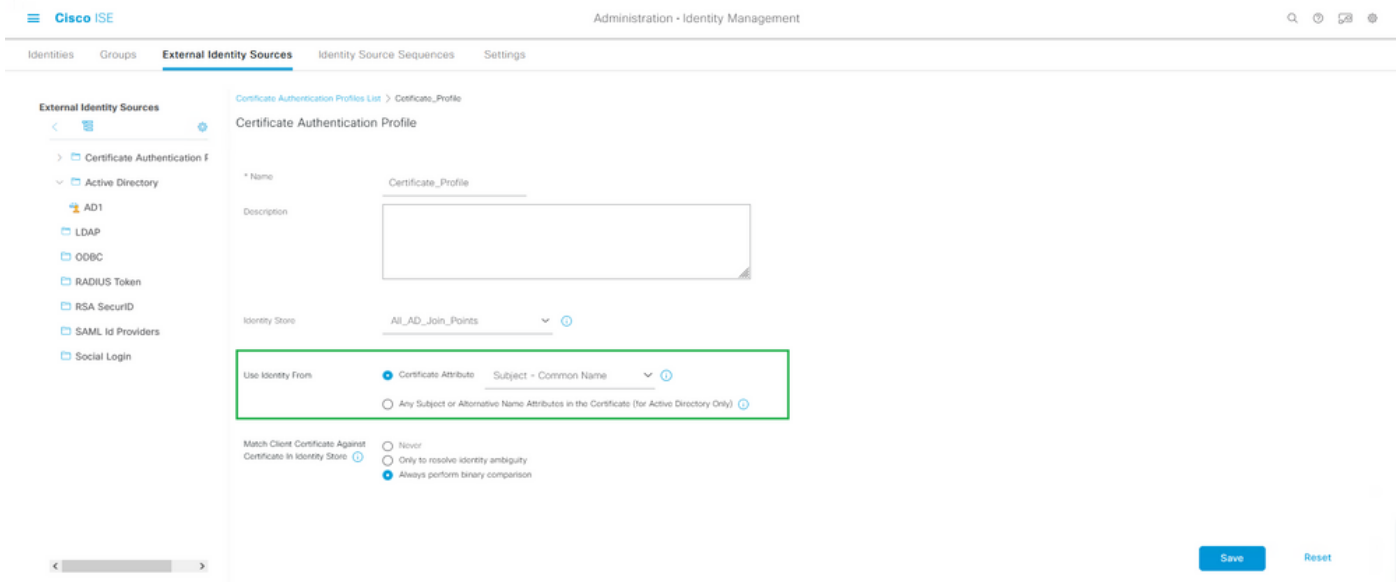
Der Zweck des Zertifikatauthentifizierungsprofils besteht darin, der ISE mitzuteilen, in welchem Zertifikatfeld sich die Identität (Computer oder Benutzer) auf dem Clientzertifikat (Endidentitätszertifikat) befindet, das der ISE während des EAP-TLS (auch bei anderen zertifikatbasierten Authentifizierungsmethoden) vorgelegt wird. Diese Einstellungen werden an die Authentifizierungsrichtlinie gebunden, um die Identität zu authentifizieren. Navigieren Sie über die ISE-GUI zu **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** und klicke auf **Add**.

**Mit Identität verwenden** aus wird das Zertifikatattribut ausgewählt, aus dem ein bestimmtes Feld für die Identität gefunden werden kann. Sie können aus den folgenden Werten wählen:

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

Wenn der Identitätsspeicher auf Active Directory oder LDAP (externe Identitätsquelle) verweisen soll, kann eine Funktion namens [Binärvergleich](#) verwendet werden. Der Binärvergleich führt eine Suche nach der Identität in Active Directory durch, die aus dem Clientzertifikat der Auswahl **Identität verwenden** abgerufen wird. Dies geschieht während der ISE-Authentifizierungsphase. Ohne Binärvergleich wird die Identität einfach aus dem Clientzertifikat abgerufen und erst in der ISE-Autorisierungsphase in Active Directory nachgeschlagen, wenn eine externe Active Directory-Gruppe als Bedingung verwendet wird, oder wenn andere Bedingungen extern für ISE ausgeführt werden müssen. Um den Binärvergleich zu verwenden, wählen Sie im **Identitätsspeicher** die externe Identitätsquelle (Active Directory oder LDAP) aus, in der sich das Endidentitätskonto befindet.

Dies ist ein Konfigurationsbeispiel, wenn sich die Identität im Feld "Common Name (CN)" des Clientzertifikats befindet und der Binärvergleich aktiviert ist (optional):



Authentifizierungsprofil für Zertifikate

Weitere Informationen finden Sie im *Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1* > in diesem Kapitel: *Basic Setup* > *Cisco ISE CA Service* > *Configure Cisco ISE to Use Certificates for Authenticating Personal Devices* > [Create a Certificate Authentication Profile for TLS-Based Authentication](#).

## Schritt 7: Zu einer Identitätsquellensequenz hinzufügen

Die Identity Source Sequence kann über die ISE-GUI erstellt werden. Navigieren Sie zu **Administration > Identity Management**. Unter **Identity Source Sequences**, klicken Sie auf **Add**.

Der nächste Schritt besteht darin, das Zertifikatauthentifizierungsprofil zu einer Identitätsquellensequenz hinzuzufügen, die die Möglichkeit bietet, mehrere Active Directory-Verknüpfungspunkte einzuschließen oder eine Kombination aus internen und externen Identitätsquellen nach Bedarf zusammenzufassen, die dann an die Authentifizierungsrichtlinie unter **Use** Spalte.

Das hier gezeigte Beispiel erlaubt es, die Suche zuerst mit Active Directory durchzuführen. Wenn der Benutzer nicht gefunden wird, sucht er als Nächstes auf einem LDAP-Server. Für mehrere Identitätsquellen. Stellen Sie sicher, **Treat as if the user was not found and proceed to the next store in the sequence** ist aktiviert. Auf diese Weise wird jede Identitätsquelle/jeder Identitätsserver während der Authentifizierungsanforderung überprüft.

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > Identity\_Sequence

### Identity Source Sequence

Identity Source Sequence

Name: Identity\_Sequence

Description:

Certificate Based Authentication

Select Certificate Authentication Profile Certificate\_Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	All_AD_Join_Points
Internal Users	LDAP_Server
Guest Users	
AD1	

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

Save Reset

### Identitätsquellensequenz

Andernfalls können Sie auch nur das Zertifikatauthentifizierungsprofil an die Authentifizierungsrichtlinie binden.

### Schritt 8: Definieren des Diensts für zulässige Protokolle

Der Dienst für zulässige Protokolle aktiviert nur die Authentifizierungsmethoden/Protokolle, die von der ISE während der RADIUS-Authentifizierung unterstützt werden. Um die Konfiguration über die ISE-GUI durchzuführen, navigieren Sie zu **Policy > Policy Elements: Results > Authentication > Allowed Protocols** (Ergebnisse > Authentifizierung > zulässige Protokolle) und wird dann als Element an die Authentifizierungsrichtlinie gebunden.

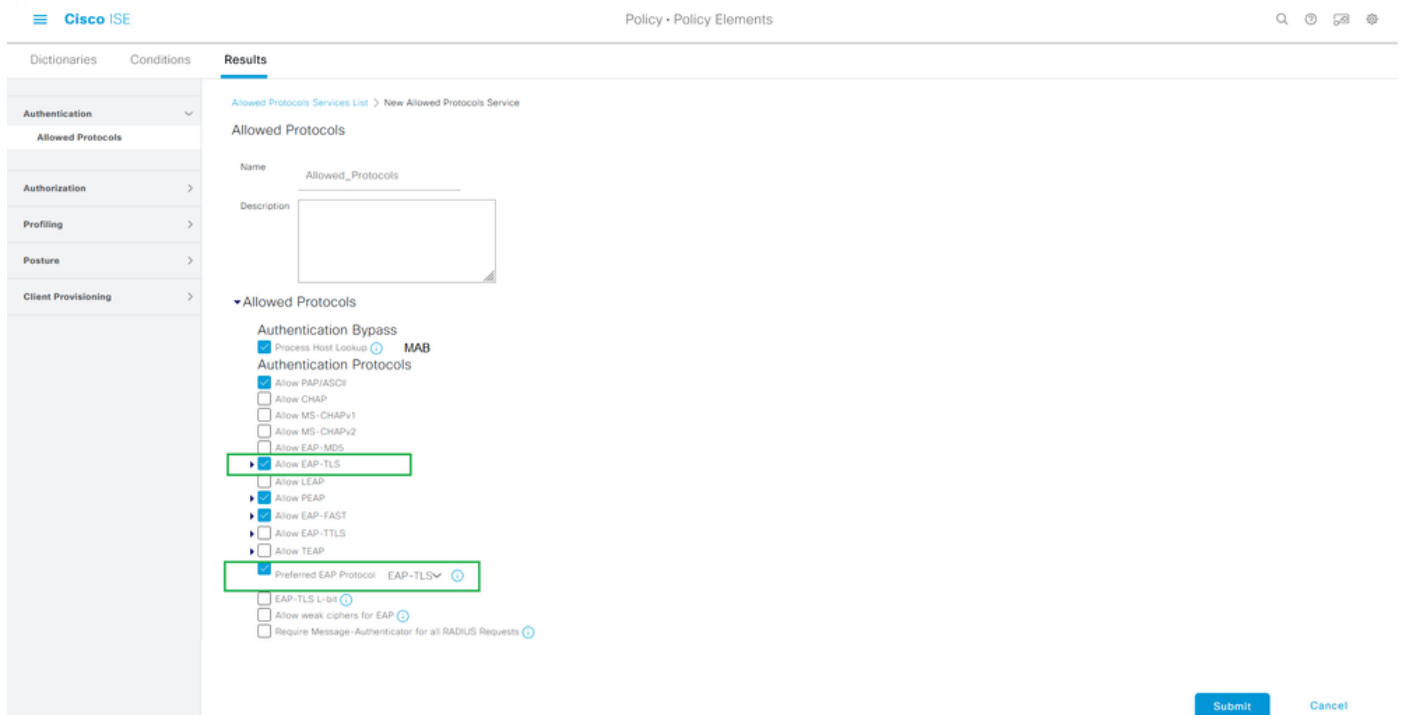
**Anmerkung: Die Authentifizierung Umgehung > Prozess-Host-Suche** bezieht sich auf die auf der ISE aktivierte MAB.

Diese Einstellungen müssen mit den Einstellungen übereinstimmen, die für die Komponente (auf dem Endgerät) unterstützt und konfiguriert werden. Andernfalls wird das Authentifizierungsprotokoll nicht wie erwartet ausgehandelt, und die RADIUS-Kommunikation schlägt möglicherweise fehl. In einer ISE-Konfiguration in der Praxis wird empfohlen, jedes Authentifizierungsprotokoll zu aktivieren, das in der Umgebung verwendet wird, damit ISE und Supplicant wie erwartet verhandeln und authentifizieren können.



Dies sind die Standardwerte (zusammengefasst), wenn eine neue Instanz der Dienste des zulässigen Protokolls erstellt wird.

**Anmerkung:** In diesem Konfigurationsbeispiel müssen Sie mindestens **EAP-TLS** aktivieren, da sich ISE und unsere Komponente über EAP-TLS authentifiziert.



Protokolle, die die Verwendung von ISE während der Authentifizierungsanforderung an die Endpunktkomponente ermöglichen

**Anmerkung:** Die Verwendung des Werts "Preferred EAP Protocol" (Bevorzugtes EAP-Protokoll) von "EAP-TLS" veranlasst ISE, das EAP-TLS-Protokoll als erstes Protokoll anzufordern, das der Endpunkt-IEEE 802.1x-Komponente angeboten wird. Diese Einstellung ist nützlich, wenn Sie sich auf den meisten Endgeräten, die über die ISE authentifiziert werden, häufig über EAP-TLS authentifizieren möchten.

## Schritt 9: Erstellen des Autorisierungsprofils

Das letzte für die Erstellung erforderliche Richtlinienelement ist das Autorisierungsprofil, das an die Autorisierungsrichtlinie gebunden ist und die gewünschte Zugriffsebene bereitstellt. Das Autorisierungsprofil ist an die Autorisierungsrichtlinie gebunden. Um sie über die ISE-GUI zu konfigurieren, navigieren Sie zu **Policy > Policy Elements: Results > Authorization > Authorization Profiles** und klicke auf **Add**.

Das Autorisierungsprofil enthält eine Konfiguration, die zu Attributen führt, die für eine bestimmte RADIUS-Sitzung von der ISE an die NAD übergeben werden. Diese Attribute werden verwendet, um die gewünschte Netzwerkzugriffsstufe zu erreichen.

Wie hier gezeigt, wird RADIUS Access-Accept lediglich als **Zugriffstyp** übergeben, jedoch können bei der Erstauthentifizierung weitere Elemente verwendet werden. Beachten Sie die **Attributdetails** ganz unten. Diese enthalten die Zusammenfassung der Attribute, die ISE an den NAD sendet, wenn sie mit einem bestimmten Autorisierungsprofil übereinstimmt.

The screenshot displays the Cisco ISE configuration interface for a new Authorization Profile. The profile name is 'Basic\_Access'. The 'Access Type' is set to 'ACCESS\_ACCEPT'. The 'Attributes Details' section shows 'Access Type = ACCESS\_ACCEPT'. The interface includes a sidebar with navigation options like Authentication, Authorization, and Profiling, and a main content area with various configuration fields and sections like 'Common Tasks' and 'Advanced Attributes Settings'.

Autorisierungsprofil - Richtlinienelement

Weitere Informationen zum ISE-Autorisierungsprofil und den ISE-Richtlinien finden Sie im *Cisco Identity Services Engine Administrator Guide, Release 3.1 > Chapter: Segmentierung > [Autorisierungsrichtlinien](#)*.

## Sicherheitsrichtlinien

Die Authentifizierungs- und Autorisierungsrichtlinien werden über die ISE-GUI erstellt. Wählen Sie **Policy > Policy Sets**. Diese sind standardmäßig auf ISE 3.x aktiviert. Bei der Installation von ISE wird immer ein Policy Set definiert, der Standard-Policy Set. Der Standard-Richtliniensatz enthält vordefinierte und standardmäßige Authentifizierungs-, Autorisierungs- und Ausnahmerichtlinienregeln.

Die Policy Sets werden hierarchisch konfiguriert, sodass der ISE-Administrator ähnliche Policies nach Zielsetzung in verschiedenen Sets gruppieren kann, die in einer Authentifizierungsanfrage verwendet werden können. Die Anpassung und Gruppierung von Richtlinien ist praktisch grenzenlos. Daher kann ein Richtliniensatz für die Authentifizierung von Wireless-Endpunkten für den Netzwerkzugriff und ein anderer Richtliniensatz für die Authentifizierung von kabelgebundenen Endpunkten für den Netzwerkzugriff verwendet werden. oder für eine andere einzigartige und differenzierte Art der Richtlinienverwaltung.

Die Cisco ISE bewertet die Richtliniensätze und die darin enthaltenen Richtlinien anhand des Top-Down-Ansatzes, um zunächst einen bestimmten Richtliniensatz abzugleichen, wenn alle

Bedingungen des Satzes als wahr evaluieren. auf der die ISE die Authentifizierungsrichtlinien und Autorisierungsrichtlinien innerhalb des zugewiesenen Richtlinienatzes weiter auswertet. Dies geschieht wie folgt:

1. Evaluierung des Policy Sets und der Policy Set Conditions
2. Authentifizierungsrichtlinien innerhalb des zugeordneten Richtlinienatzes
3. Autorisierungsrichtlinie - Lokale Ausnahmen
4. Autorisierungsrichtlinie - Globale Ausnahmen
5. Autorisierungsrichtlinien

Richtlinienausnahmen sind global für alle oder lokal in einem bestimmten Richtlinienatz vorhanden. Diese Richtlinienausnahmen werden als Teil der Autorisierungsrichtlinien behandelt, da sie die Berechtigungen oder Ergebnisse für den Netzwerkzugriff für ein bestimmtes temporäres Szenario behandeln.

Im nächsten Abschnitt wird beschrieben, wie die Konfigurations- und Richtlinienelemente so kombiniert werden, dass sie an die ISE-Authentifizierungs- und Autorisierungsrichtlinien gebunden werden, um Endpunkte über EAP-TLS zu authentifizieren.

## Schritt 10: Erstellen des Policy Sets

Ein Richtlinienatz ist ein hierarchischer Container, der aus einer einzelnen benutzerdefinierten Regel besteht, die das zulässige Protokoll oder die zulässige Serversequenz für den Netzwerkzugriff angibt, sowie Authentifizierungs- und Autorisierungsrichtlinien und Richtlinienausnahmen, die alle ebenfalls mit benutzerdefinierten zustandsbasierten Regeln konfiguriert sind.

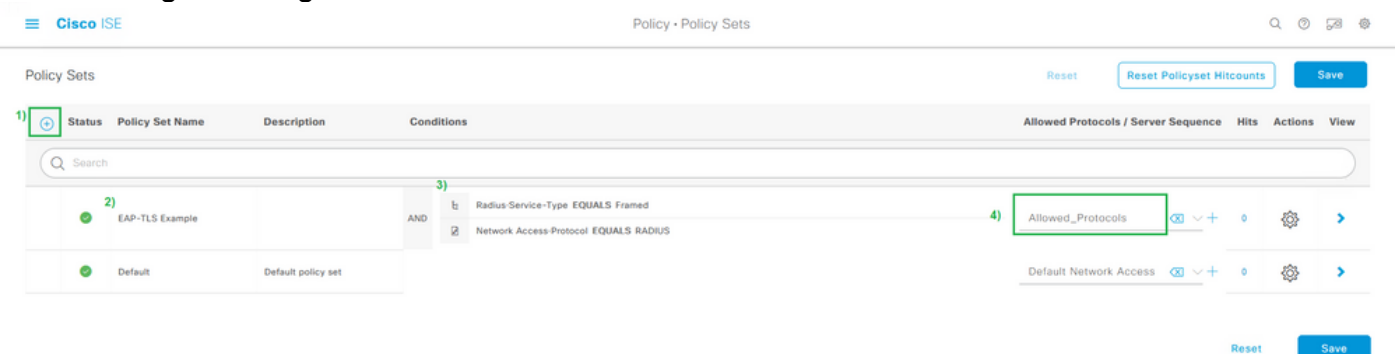
Um einen Richtlinienatz über die ISE-GUI zu erstellen, navigieren Sie zu **Policy > Policy Set** und dann auf das Plus-Symbol (+) in der linken oberen Ecke, wie in diesem Bild dargestellt.



*Hinzufügen eines neuen Policy Sets*

Das Policy Set bindet/kombiniert dieses zuvor konfigurierte Policy-Element und wird verwendet, um zu bestimmen, welcher Policy Set einer RADIUS-Authentifizierungsanforderung (Access-Request) zugeordnet werden soll:

- Bindung: Zulässige Protokolldienste



*Definieren der Bedingungen für den Richtlinienatz und der Liste der zulässigen Protokolle*

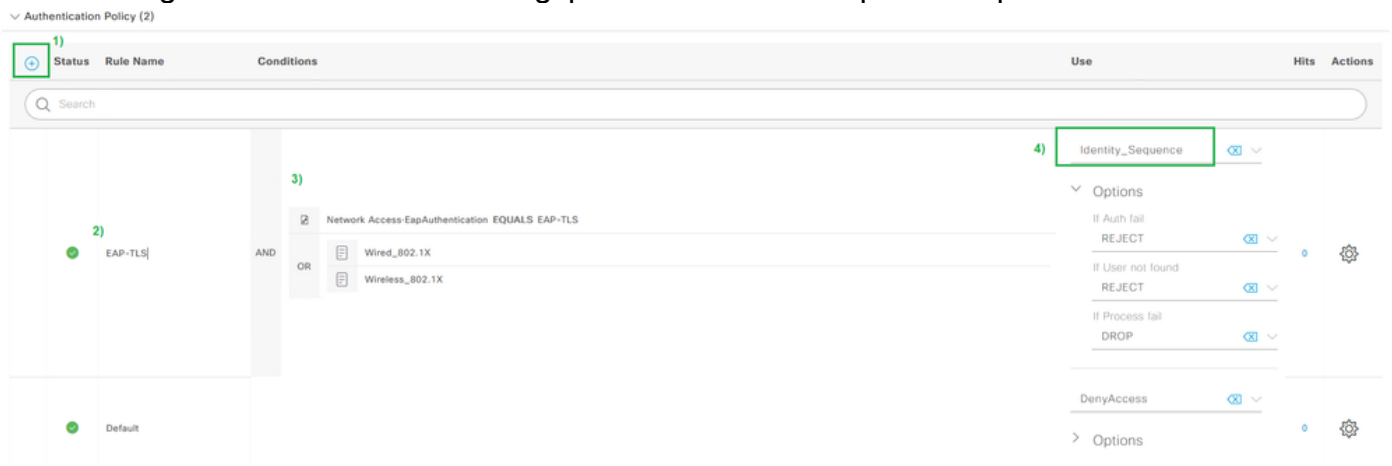
In diesem Beispiel werden bestimmte Attribute und Werte verwendet, die in der RADIUS-Sitzung angezeigt werden, um IEEE 802.1x (Framed-Attribut) durchzusetzen, auch wenn dies für die Durchsetzung des RADIUS-Protokolls möglicherweise redundant ist. Verwenden Sie nur eindeutige RADIUS-Sitzungsattribute, die für den gewünschten Zweck gelten, z. B. Netzwerk-Gerätegruppen oder spezielle Attribute für kabelgebundene 802.1x-, Wireless 802.1x- oder kabelgebundene 802.1x- und Wireless 802.1x-Netzwerke.

Weitere Informationen zu Richtlinienätzen für die ISE finden Sie im *Cisco Identity Services Engine-Administratorleitfaden, Version 3.1 > Kapitel: Segmentierung > [Richtliniensätze](#), [Authentifizierungsrichtlinien](#) und [Autorisierungsrichtlinien](#).*

### Schritt 11: Erstellen einer Authentifizierungsrichtlinie

Innerhalb des Richtlinienatzes bindet/kombiniert die Authentifizierungsrichtlinie diese Richtlinienelemente, die zuvor für die Verwendung mit Bedingungen konfiguriert wurden, um zu bestimmen, wann eine Authentifizierungsregel zugeordnet werden soll.

- Bindung: Zertifikatauthentifizierungsprofil oder Identitätssequenz.

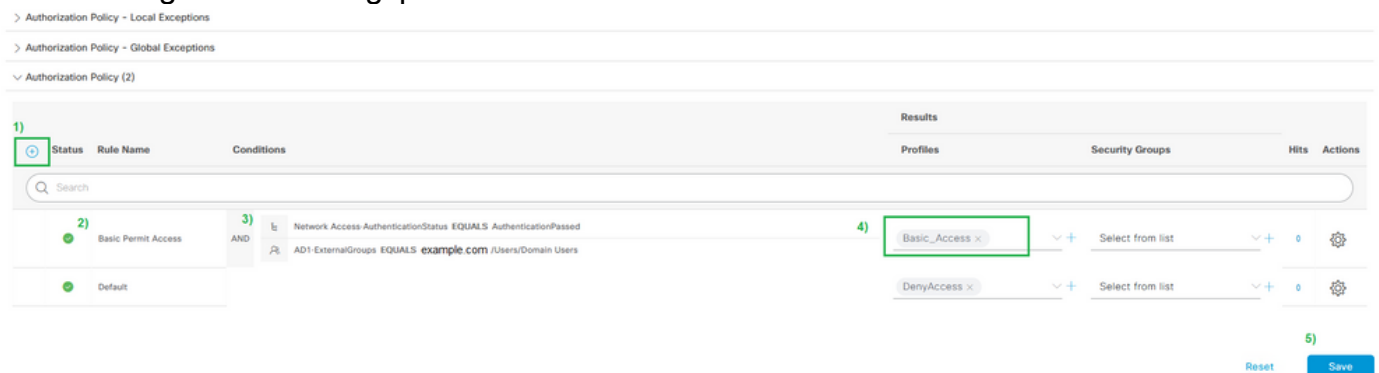


Beispiel für eine Authentifizierungsrichtlinie

### Schritt 12: Erstellen der Autorisierungsrichtlinie

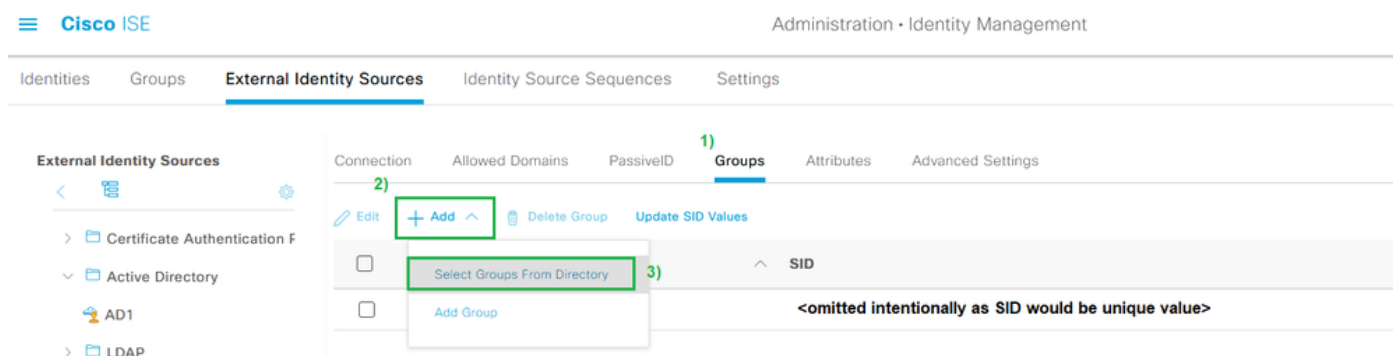
Innerhalb des Richtlinienatzes bindet/kombiniert die Autorisierungsrichtlinie diese Richtlinienelemente, die zuvor für die Verwendung mit Bedingungen konfiguriert wurden, um zu bestimmen, wann eine Autorisierungsregel zugeordnet werden soll. Das Beispiel hier bezieht sich auf die **Benutzerauthentifizierung**, da die Bedingungen auf die Sicherheitsgruppe **Domänenbenutzer** in Active Directory verweisen.

- Bindung: Autorisierungsprofil



Beispiel für eine Autorisierungsrichtlinienregel

Um eine externe Gruppe (z. B. von Active Directory oder LDAP) hinzuzufügen, müssen Sie die Gruppe von der externen Serverinstanz hinzufügen. In diesem Beispiel stammt er von der ISE-Benutzeroberfläche: **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups**. Wählen Sie auf der Registerkarte Gruppe **Add > Select Groups from Directory** und verwenden Sie den "Namensfilter", um nach allen Gruppen (\*) oder bestimmten Gruppen zu suchen, z. B. nach Domänenbenutzern (\*Domänenbenutzer\*), um Gruppen abzurufen.



Um externe Gruppen in ISE-Richtlinien zu verwenden, muss die Gruppe aus dem Verzeichnis hinzugefügt werden.

## Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name  SID  Type

Filter  1 Groups Retrieved.

<input type="checkbox"/>	Name	Group SID	Group Type
<input checked="" type="checkbox"/>	example.com /Users/Domain Users	<omitted SID intentionally>	GLOBAL

Suchen im externen Verzeichnis - Beispiel für Active Directory

Nachdem Sie das Kontrollkästchen neben jeder Gruppe aktiviert haben, die Sie in den Richtlinien innerhalb der ISE verwenden möchten, vergessen Sie nicht, auf **OK** und/oder **Speichern** zu klicken, um die Änderungen zu speichern.

## Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn alle globalen Konfigurations- und Richtlinienelemente an den Richtliniensatz gebunden sind, sieht die Konfiguration für die Benutzerauthentifizierung über EAP-TLS ähnlich aus wie im folgenden Bild:

The screenshot displays the Cisco ISE GUI for configuring a Policy Set. The main view is titled 'Policy Sets - Policy Sets' and shows a table of Policy Sets. The 'EAP-TLS Example' policy set is selected, and its configuration is shown in a detailed view. The configuration includes the following conditions:

- AND
  - Radius-Service-Type EQUALS Framed
  - Network Access Protocol EQUALS RADIUS

The 'Allowed Protocols / Server Sequence' section shows 'Allowed\_Protocols' and 'Identity\_Sequence'.

The 'Authentication Policy' section shows a table of Authentication Policies. The 'EAP-TLS' policy is selected, and its configuration is shown in a detailed view. The configuration includes the following conditions:

- AND
  - Network Access EapAuthentication EQUALS EAP-TLS
  - OR
    - Wired\_802.1X
    - Wireless\_802.1X

The 'Authorization Policy' section shows a table of Authorization Policies. The 'Basic Permit Access' policy is selected, and its configuration is shown in a detailed view. The configuration includes the following conditions:

- AND
  - Network Access AuthenticationStatus EQUALS AuthenticationPassed
  - AD1-ExternalGroups EQUALS example.com/Users/Domain Users

The 'Results' section shows a table of Results. The 'Basic\_Permit\_Access' result is selected, and its configuration is shown in a detailed view. The configuration includes the following profiles and security groups:

- Basic\_Permit\_Access
  - Select from list
- DenyAccess
  - Select from list

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Wenn die Konfiguration abgeschlossen ist, verbinden Sie den Endpunkt mit der Testauthentifizierung. Die Ergebnisse finden Sie in der ISE-GUI. Auswählen **Operations > Radius > Live Logs**, wie in diesem Bild dargestellt.

Zur Erkennung stehen die Live-Protokolle für RADIUS und TACACS+ (Device Admin) für Authentifizierungsversuche/Aktivitäten bis zu den letzten 24 Stunden und für die letzten 100 Datensätze zur Verfügung. Wenn diese Art von Berichtsdaten über diesen Zeitraum hinaus angezeigt werden soll, müssen Sie die Berichte verwenden. Dies gilt insbesondere für: **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications**.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Posture St...	Server	Mdm Serve...
May 10, 2022 09:35:15.460 PM	<span style="color: blue;">●</span>		0	employee1	00:00:AA:11:22:33	EAP-TLS Example >> EAP-TLS	EAP-TLS Example >> Basic Permit Access	Basic_Access				ise3	
May 10, 2022 09:35:15.460 PM	<span style="color: green;">●</span>		0	employee1	00:00:AA:11:22:33	EAP-TLS Example >> EAP-TLS	EAP-TLS Example >> Basic Permit Access	Basic_Access	Switch			ise3	

## Live Logs" />Beispielausgabe von Radius > Live Logs

Bei RADIUS Live Logs in der ISE erwarten Sie Informationen über die RADIUS-Sitzung, die Sitzungsattribute sowie andere hilfreiche Informationen zur Diagnose des Verhaltens während eines Authentifizierungsflusses enthalten. Klicken Sie auf **details** um die Detailansicht der Sitzung anzuzeigen, in der Sitzungsattribute und zugehörige Informationen zu diesem Authentifizierungsversuch angezeigt werden.

Für die Fehlerbehebung muss sichergestellt werden, dass die richtigen Richtlinien zugeordnet werden. Für dieses Konfigurationsbeispiel werden die gewünschten Authentifizierungs- und Autorisierungsrichtlinien wie erwartet zugeordnet, wie im Bild gezeigt:

<b>Authentication Policy</b>	EAP-TLS Example >> EAP-TLS
<b>Authorization Policy</b>	EAP-TLS Example >> Basic Permit Access
<b>Authorization Result</b>	Basic_Access

In der Detailansicht werden diese Attribute überprüft, um zu überprüfen, ob sich die Authentifizierung im Rahmen dieses Konfigurationsbeispiels wie erwartet verhält:

- **Veranstaltung**

Enthält, ob die Authentifizierung erfolgreich war oder nicht. In einem Arbeitsszenario hat dies folgende Vorteile: **5200 Authentifizierung erfolgreich.**

- **Benutzername**

Dazu gehört auch die End-Identität, die aus dem Client-Zertifikat abgerufen wurde, das der ISE vorgelegt wurde. In einem Arbeitsszenario ist dies der Benutzername des Benutzers, der am Endpunkt angemeldet ist (d. h. employee1 aus dem vorherigen Bild).

- **Endpunkt-ID**

Bei kabelgebundenen/Wireless-Netzwerken ist dieser Wert die MAC-Adresse der Netzwerkkarte (NIC) des Endpunkts. In einem Arbeitsszenario wird dies zur MAC-Adresse des Endpunkts, es sei denn, die Verbindung erfolgt über VPN. In diesem Fall kann es sich um die IP-Adresse des Endpunkts handeln.

- **Authentifizierungsrichtlinie**

Zeigt die zugeordnete Authentifizierungsrichtlinie für die angegebene Sitzung basierend auf Sitzungsattributen an, die den Richtlinienbedingungen entsprechen. In einem funktionierenden Szenario ist dies die erwartete Authentifizierungsrichtlinie, wie konfiguriert. Wenn Sie eine

andere Richtlinie sehen, bedeutet dies, dass die erwartete Richtlinie im Vergleich zu den Bedingungen in der Richtlinie nicht als wahr bewertet wurde. Überprüfen Sie in diesem Fall die Sitzungsattribute, und stellen Sie sicher, dass jede Richtlinie unterschiedliche, aber eindeutige Bedingungen für jede Richtlinie enthält.

- **Autorisierungsrichtlinie**

Zeigt die zugeordnete Autorisierungsrichtlinie für die angegebene Sitzung basierend auf Sitzungsattributen an, die den Richtlinienbedingungen entsprechen. In einem funktionierenden Szenario ist dies die erwartete Autorisierungsrichtlinie, wie konfiguriert. Wenn Sie eine andere Richtlinie sehen, bedeutet dies, dass die erwartete Richtlinie im Vergleich zu den Bedingungen in der Richtlinie nicht als wahr bewertet wurde. Überprüfen Sie in diesem Fall die Sitzungsattribute, und stellen Sie sicher, dass jede Richtlinie unterschiedliche, aber eindeutige Bedingungen für jede Richtlinie enthält.

- **Autorisierungsergebnis**

Basierend auf der entsprechenden Autorisierungsrichtlinie wird das Autorisierungsprofil angezeigt, das in der angegebenen Sitzung verwendet wurde. In einem Arbeitsszenario entspricht dieser Wert der Konfiguration in der Richtlinie. Es empfiehlt sich, die Konfiguration zu Prüfzwecken und zur Sicherstellung des korrekten Autorisierungsprofils zu überprüfen.

- **Richtlinienserver**

Dies schließt den Hostnamen des ISE Policy Service Node (PSN) ein, der am Authentifizierungsversuch beteiligt war. In einem funktionierenden Szenario werden nur Authentifizierungen angezeigt, die an den ersten PSN-Knoten gehen, wie er für das NAD konfiguriert wurde (auch als Edge-Gerät bezeichnet), es sei denn, dieser PSN war nicht betriebsbereit oder es ist ein Failover aufgetreten, z. B. aufgrund einer höheren Latenz als erwartet oder wenn ein Timeout für die Authentifizierung auftritt.

- **Authentifizierungsmethode**

Zeigt die Authentifizierungsmethode an, die in der angegebenen Sitzung verwendet wurde. In diesem Beispiel sehen Sie den Wert als **dot1x**. In einem Arbeitsszenario wird der Wert basierend auf diesem Konfigurationsbeispiel als **dot1x** angezeigt. Wenn Sie einen anderen Wert sehen, kann dies bedeuten, dass entweder dot1x fehlgeschlagen ist oder nicht versucht wurde.

- **Authentifizierungsprotokoll**

Zeigt die Authentifizierungsmethode an, die in der angegebenen Sitzung verwendet wurde. Für dieses Beispiel sehen Sie den Wert als "EAP-TLS". In einem Arbeitsszenario wird der Wert basierend auf diesem Konfigurationsbeispiel immer als "EAP-TLS" angezeigt. Wenn ein anderer Wert angezeigt wird, haben der Supplicant und die ISE EAP-TLS nicht erfolgreich ausgehandelt.

- **Netzwerkgerät**

Zeigt den Netzwerkgerätenamen, wie in ISE konfiguriert, für die NAD (auch als Edge-Gerät bezeichnet) an, die an dem Authentifizierungsversuch zwischen dem Endpunkt und der ISE beteiligt ist. In einem Arbeitsszenario wird dieser Name immer in der ISE-Benutzeroberfläche angegeben: **Administration > System: Network Devices**. Basierend auf dieser Konfiguration wird die IP-Adresse des NAD (auch als Edge-Gerät bezeichnet) verwendet, um zu bestimmen, von



welchem Netzwerkgerät die Authentifizierung stammt, das im **NAS-IPv4-Adress**sitzungsattribut enthalten ist.

Dies ist keinesfalls eine vollständige Liste aller möglichen Sitzungsattribute, die zur Fehlerbehebung oder für andere Transparenzzwecke überprüft werden können, da es andere nützliche Attribute gibt, die überprüft werden müssen. Es wird empfohlen, alle Sitzungsattribute zu überprüfen, um sich mit allen Informationen vertraut zu machen. Sie können die rechte Seite unter dem Abschnitt **Schritte** einschließen, der die von der ISE durchgeführten Vorgänge und Verhaltensweisen zeigt.

## Häufige Probleme und Verfahren zur Fehlerbehebung

Diese Liste enthält einige häufig auftretende Probleme und Tipps zur Fehlerbehebung und ist keinesfalls als vollständige Liste gedacht. Nutzen Sie diese Informationen stattdessen als Leitfaden, und entwickeln Sie eigene Verfahren zur Fehlerbehebung bei ISE-Problemen.

Problem: Authentifizierungsfehler (**5400-Authentifizierung fehlgeschlagen**) oder ein anderer nicht erfolgreicher Authentifizierungsversuch.

- Wenn bei der Authentifizierung ein Fehler auftritt, klicken Sie auf das Symbol **Details**, das Informationen darüber enthält, warum die Authentifizierung fehlgeschlagen ist, und welche Schritte unternommen wurden. Dazu gehören der Fehlergrund und die mögliche Ursache.
- Da die ISE die Entscheidung über das Authentifizierungsergebnis trifft, verfügt sie über die Informationen, um den Grund für den fehlgeschlagenen Authentifizierungsversuch zu ermitteln.

Problem: Die Authentifizierung wurde nicht erfolgreich abgeschlossen, und der Fehlergrund lautet: "5440 Endpoint brach die EAP-Sitzung ab und begann neu" oder "5411 Supplicant reagierte nicht mehr auf ISE".

- Dieser Fehlergrund zeigt an, dass die RADIUS-Kommunikation vor dem Timeout nicht abgeschlossen wurde. Da sich EAP zwischen dem Endpunkt und NAD befindet, müssen Sie das Timeout für das NAD überprüfen und sicherstellen, dass es für mindestens fünf Sekunden festgelegt ist.
- Wenn fünf Sekunden nicht ausreichen, um dieses Problem zu lösen, empfehlen wir, es einige Male um fünf Sekunden zu erhöhen und erneut zu testen, ob dieses Problem durch dieses Verfahren behoben wird.
- Wenn das Problem mit den vorherigen Schritten nicht behoben wurde, empfehlen wir, sicherzustellen, dass die Authentifizierung vom selben und richtigen ISE-PSN-Knoten durchgeführt wird und das Gesamtverhalten kein Anzeichen für ein abnormales Verhalten ist, z. B. eine Latenz, die höher ist als die normale Latenz zwischen NAD- und ISE-PSN-Knoten.
- Außerdem sollte überprüft werden, ob der Endpunkt das Client-Zertifikat über die Paketerfassung sendet, wenn ISE das Client-Zertifikat nicht empfängt. Der Endpunkt (Benutzerzertifikate) kann dem ISE-EAP-Authentifizierungszertifikat möglicherweise nicht vertrauen. Wenn der Wert true lautet, importieren Sie die Zertifizierungsstellenkette in die richtigen Zertifikatspeicher (Stammzertifizierungsstelle = vertrauenswürdige

Stammzertifizierungsstelle). | Intermediäre CA = vertrauenswürdige Intermediäre CA).

Problem: Die Authentifizierung war erfolgreich, entspricht jedoch nicht den richtigen Authentifizierungs- und/oder Autorisierungsrichtlinien.

- Wenn eine Authentifizierungsanforderung erfolgreich ist, aber nicht den richtigen Authentifizierungs- und/oder Autorisierungsregeln entspricht, empfehlen wir, die Sitzungsattribute zu überprüfen, um sicherzustellen, dass die verwendeten Bedingungen korrekt sind und in der RADIUS-Sitzung vorhanden sind.
- Die ISE bewertet diese Richtlinien anhand eines Top-Down-Ansatzes (mit Ausnahme von Statusrichtlinien). Sie müssen zunächst ermitteln, ob die gefundene Richtlinie über oder unter der gewünschten abzugleichenden Richtlinie lag. Die Authentifizierungsrichtlinie wird zuerst und unabhängig von den Autorisierungsrichtlinien ausgewertet. Wenn die Authentifizierungsrichtlinie richtig zugeordnet ist, wird im rechten Abschnitt **"Steps"** unter den Authentifizierungsdetails **"22037 Authentication Passed" (Authentifizierung bestanden) angezeigt.**
- Liegt die gewünschte Policy über der entsprechenden Policy, bedeutet dies, dass die Summe der Bedingungen auf der gewünschten Policy nicht als wahr bewertet wurde. Es überprüft alle Attribute und Werte in der Bedingung und in der Sitzung, um sicherzustellen, dass es existiert und kein Rechtschreibfehler vorliegt.
- Liegt die gewünschte Policy unter der entsprechenden Policy, bedeutet dies, dass eine andere Policy (oben) anstatt der gewünschten Policy durchgeführt wurde. Dies kann bedeuten, dass Bedingungswerte nicht spezifisch genug sind, dass die Bedingungen in einer anderen Richtlinie dupliziert werden oder dass die Reihenfolge der Richtlinie nicht korrekt ist. Auch wenn die Fehlerbehebung schwieriger wird, empfehlen wir, Richtlinien zu überprüfen, um den Grund zu ermitteln, warum die gewünschte Richtlinie nicht übereinstimmt. So können Sie leichter erkennen, welche Maßnahmen als Nächstes zu ergreifen sind.

Problem: Die bei der Authentifizierung verwendete Identität oder der Benutzername entsprach nicht dem erwarteten Wert.

- Wenn der Endpunkt das Client-Zertifikat sendet, verwendet die ISE in diesem Fall höchstwahrscheinlich nicht das richtige Zertifikatfeld in der Zertifikatauthentifizierungsvorlage, die während der Authentifizierungsphase ausgewertet wird.
- Überprüfen Sie das Client-Zertifikat, um das genaue Feld zu finden, in dem die gewünschte Identität/der Benutzername vorhanden ist, und stellen Sie sicher, dass das gleiche Feld ausgewählt ist aus: **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

Problem: Die Authentifizierung ist nicht erfolgreich. Fehlerursache: **"12514 EAP-TLS fehlgeschlagener SSL/TLS-Handshake aufgrund einer unbekanntes Zertifizierungsstelle in der Client-Zertifikatskette".**

- Dies kann auftreten, wenn das Clientzertifikat ein Zertifikat in der Zertifizierungsstellenkette hat, das auf der ISE-Benutzeroberfläche nicht vertrauenswürdig ist: **Administration > System: Certificates > Trusted Certificates.**
- Dies kann in der Regel dann der Fall sein, wenn das Clientzertifikat (auf dem Endpunkt) eine Zertifizierungsstellenkette aufweist, die sich von der Zertifizierungsstellenkette des Zertifikats unterscheidet, das zur EAP-Authentifizierung bei der ISE signiert ist.
- Stellen Sie zur Problembeseitigung sicher, dass die Zertifikatskette des Clientzertifikats auf der ISE vertrauenswürdig und die Zertifikatskette des ISE EAP-Authentifizierungsservers auf dem Endpunkt vertrauenswürdig ist.
  - Navigieren Sie für Windows OS und Chrome zu **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates.**
  - Für Firefox: Importieren Sie die Zertifizierungsstellenkette (nicht das Endidentitätszertifikat), die für den Webserver als vertrauenswürdig gelten soll.

## Zugehörige Informationen

- Cisco Identity Services Engine > [Installations- und Upgradeleitfäden](#)
- Cisco Identity Services Engine > [Konfigurationsleitfäden](#)
- Cisco Identity Services Engine > [Kompatibilitätsinformationen](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Sicherer Zugriff > [Definition von Netzwerkgeräten in der Cisco ISE](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Segmentierung > [Richtliniensätze](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Segmentierung > [Authentifizierungsrichtlinien](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Segmentierung > [Autorisierungsrichtlinien](#)
- Cisco Identity Services Engine > Konfigurationsanleitungen > [Active Directory-Integration mit Cisco ISE 2.x](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Segmentierung > Netzwerkzugriffsservice > [Netzwerkzugriff für Benutzer](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Grundlegende Einrichtung > [Zertifikatsverwaltung in der Cisco ISE](#)
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1 > Kapitel: Grundlegende Einrichtung > Cisco ISE CA Service > Konfigurieren der Cisco ISE zur Verwendung von Zertifikaten für die Authentifizierung privater Geräte > [Erstellen eines Zertifikats-Authentifizierungsprofils für die TLS-basierte Authentifizierung](#)
- Cisco Identity Services Engine > Konfigurationsbeispiele und technische Hinweise > [ISE 2.0-Zertifikatsbereitstellungsportal konfigurieren](#)
- Cisco Identity Services Engine > Konfigurationsbeispiele und technische Hinweise > [Installieren eines von einer Zertifizierungsstelle signierten Zertifikats eines Drittanbieters in der ISE](#)
- Wireless LAN (WLAN) > Konfigurationsbeispiele und technische Hinweise > [EAP-TLS mit WLC und ISE verstehen und konfigurieren](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.