Installieren eines Zertifizierungsstellenzertifikats eines Drittanbieters in der ISE

Inhalt

Einführung

In diesem Dokument wird die Installation eines signierten Zertifikats einer Zertifizierungsstelle eines Drittanbieters in der Cisco Identity Services Engine (ISE) beschrieben. Der Prozess ist unabhängig von der endgültigen Zertifikatrolle (EAP-Authentifizierung, Portal, Admin und pxGrid) identisch.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der grundlegenden Public Key-Infrastruktur zu verfügen.

Verwendete Komponenten

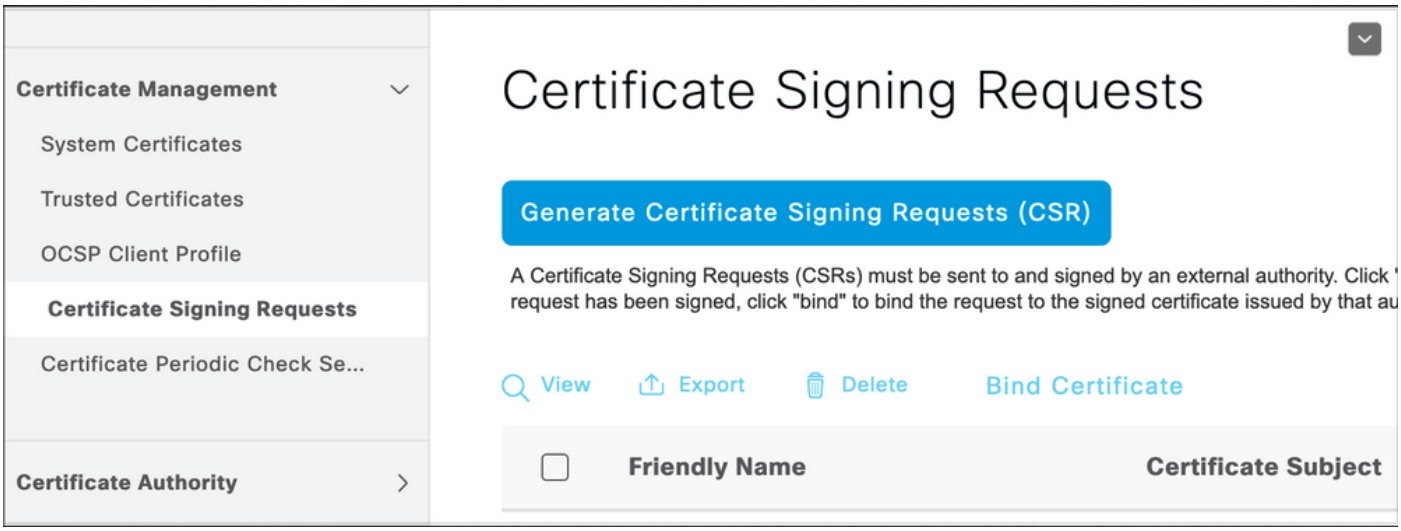
Die Informationen in diesem Dokument basieren auf der Cisco Identity Services Engine (ISE) Version 3.0. Dieselbe Konfiguration gilt für Version 2.x

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 potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Schritt 1: Erstellen einer Zertifikatssignaturanfrage (Certificate Signing Request, CSR).

Um den CSR zu generieren, navigieren Sie zu **Administration > Certificates > Certificate Signing Requests** und klicken Sie auf **Generate Certificate Signing Requests** (CSR).



1. Wählen Sie im Bereich Usage (Nutzung) die Rolle aus, die im Dropdown-Menü verwendet werden soll. Wenn das Zertifikat für mehrere Rollen verwendet wird, können Sie Multi-Use auswählen. Nach der Erstellung des Zertifikats können die Rollen ggf. geändert werden.

2. Wählen Sie den Knoten aus, für den das Zertifikat generiert wird.

3. Geben Sie die erforderlichen Informationen ein (Organisationseinheit, Organisation, Stadt, Bundesland und Land).

   Hinweis: Im Feld "Common Name" (CN) gibt die ISE automatisch den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Knotens ein.

Platzhalter:

- Wenn das Ziel darin besteht, ein Platzhalterzertifikat zu generieren, aktivieren Sie das Kontrollkästchen **Platzhalterzertifikate zulassen**.

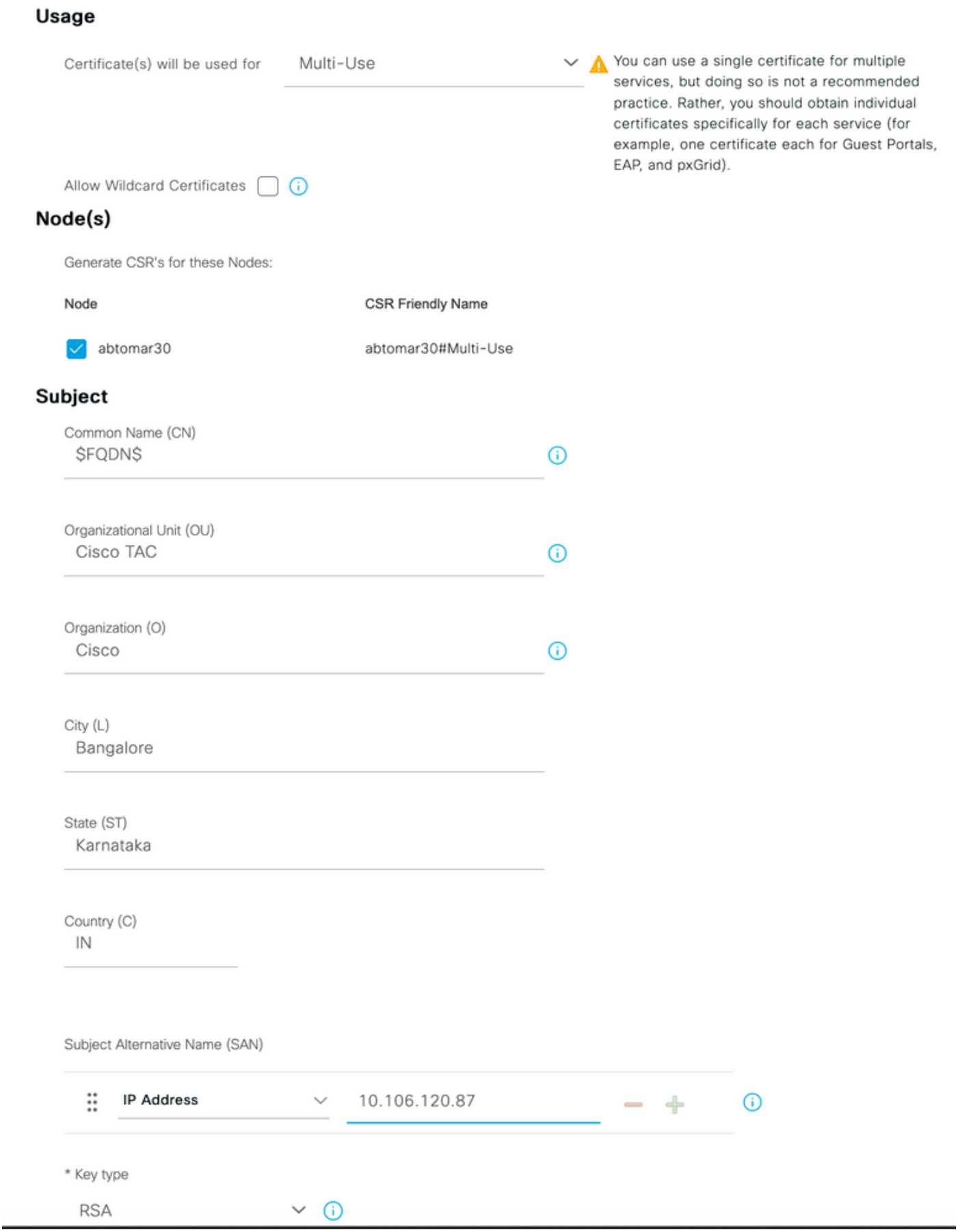
- Wenn das Zertifikat für EAP-Authentifizierungen verwendet wird, sollte das * Symbol nicht im Betreff-CN-Feld enthalten sein, da Windows-Supplicants das Serverzertifikat ablehnen.

- Selbst wenn die **Serveridentität validieren** für die Komponente deaktiviert ist, schlägt der SSL-Handshake möglicherweise fehl, wenn sich das *im CN-Feld befindet.

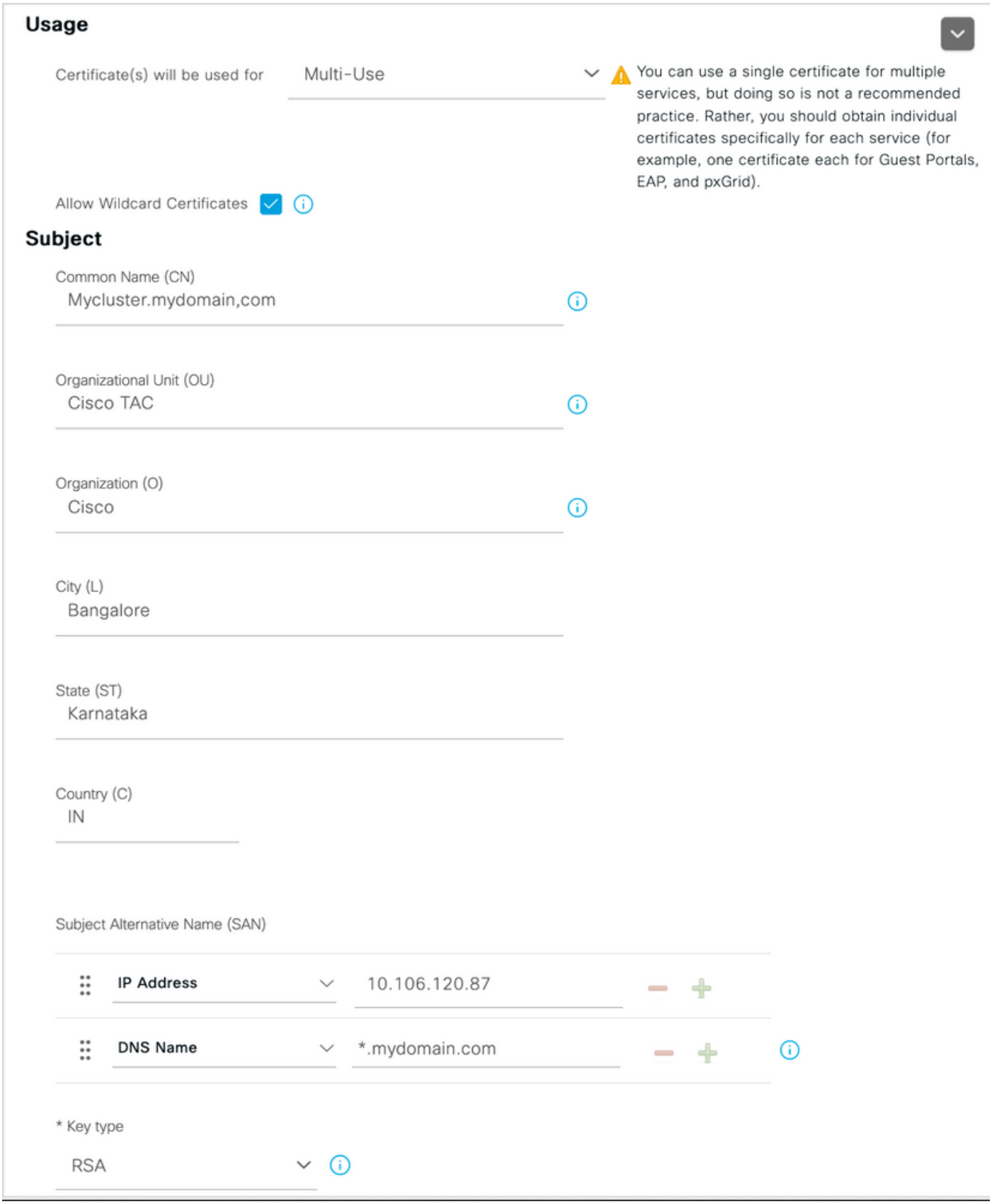
- Stattdessen kann im KN-Feld ein generischer FQDN verwendet werden, und dann kann die ***.domain.com** im Feld SAN-DNS-Name (Subject Alternative Name) verwendet werden.

  Hinweis: Einige Zertifizierungsstellen (Certificate Authorities, CA) können die Platzhalterkarte (*) automatisch in die CN des Zertifikats einfügen, auch wenn sie nicht im CSR vorhanden ist. In diesem Szenario ist eine spezielle Anfrage erforderlich, um diese Aktion zu verhindern.

CSR-Beispiel für einzelnes Serverzertifikat:

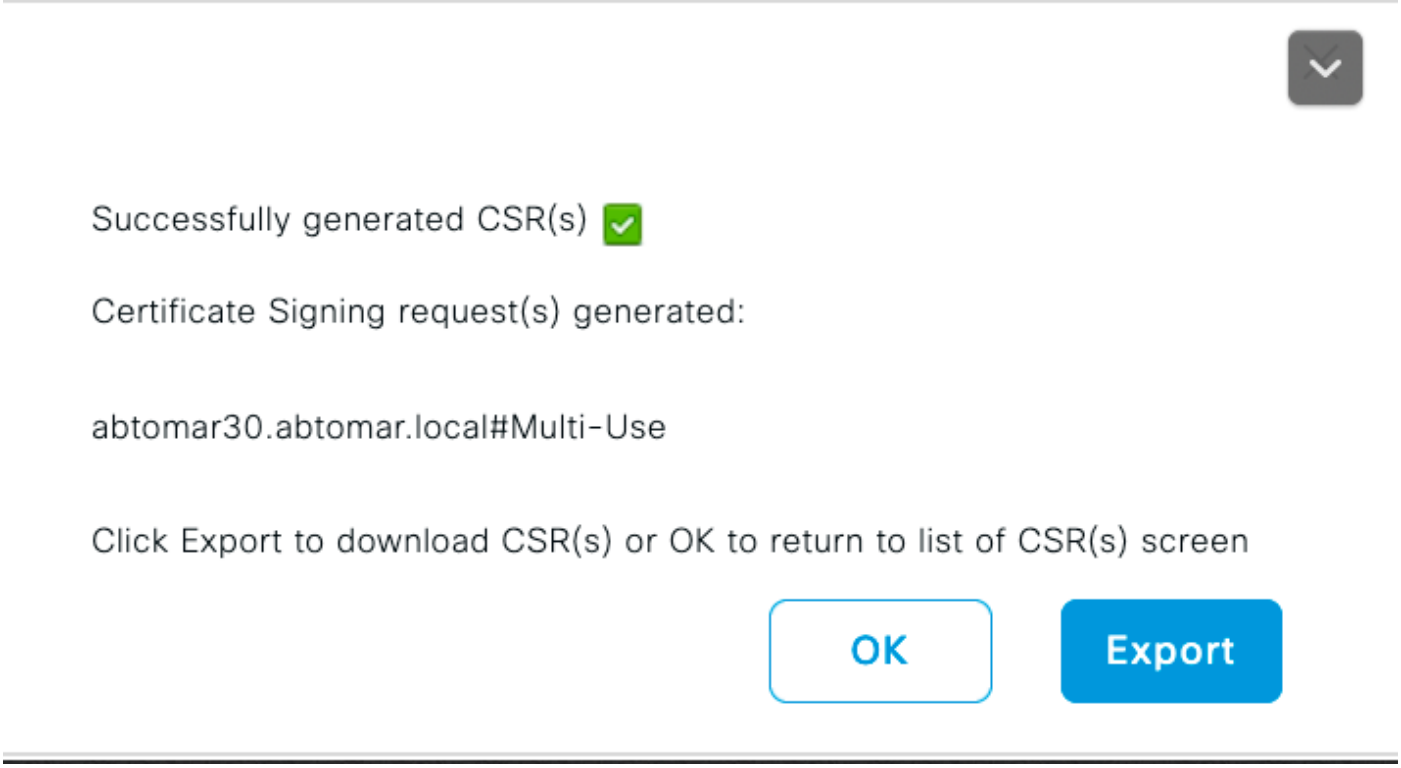


Wildcard CSR-Beispiel:



Hinweis: Die IP-Adresse jedes Bereitstellungsknotens kann dem SAN-Feld hinzugefügt werden, um eine Zertifikatwarnung beim Zugriff auf den Server über die IP-Adresse zu vermeiden.

Nach der Erstellung der CSR-Anfrage zeigt die ISE ein Popup-Fenster mit der Option zum Exportieren an. Nach dem Export sollte diese Datei zur Signierung an die CA gesendet werden.



Schritt 2: Importieren einer neuen Zertifikatskette.

Die Zertifizierungsstelle gibt das signierte Serverzertifikat zusammen mit der vollständigen Zertifikatkette (Root/Intermediate) zurück. Führen Sie nach dem Empfang die folgenden Schritte aus, um die Zertifikate in Ihren ISE-Server zu importieren:

1. Um von der CA bereitgestellte Root- und (oder) Zwischenzertifikate zu importieren, gehen Sie zu **Administration > Certificates > Trusted Certificates**.

2. Klicken Sie auf **Importieren**, wählen Sie dann das Root- und/oder Zwischenzertifikat aus, und aktivieren Sie die entsprechenden Kontrollkästchen für die Einreichung.
3. Um das Serverzertifikat zu importieren, navigieren Sie zu **Administration > Certificates > Certificate Signing Requests**.

4. Wählen Sie den zuvor erstellten CSR aus, und klicken Sie auf **Bind Certificate**.

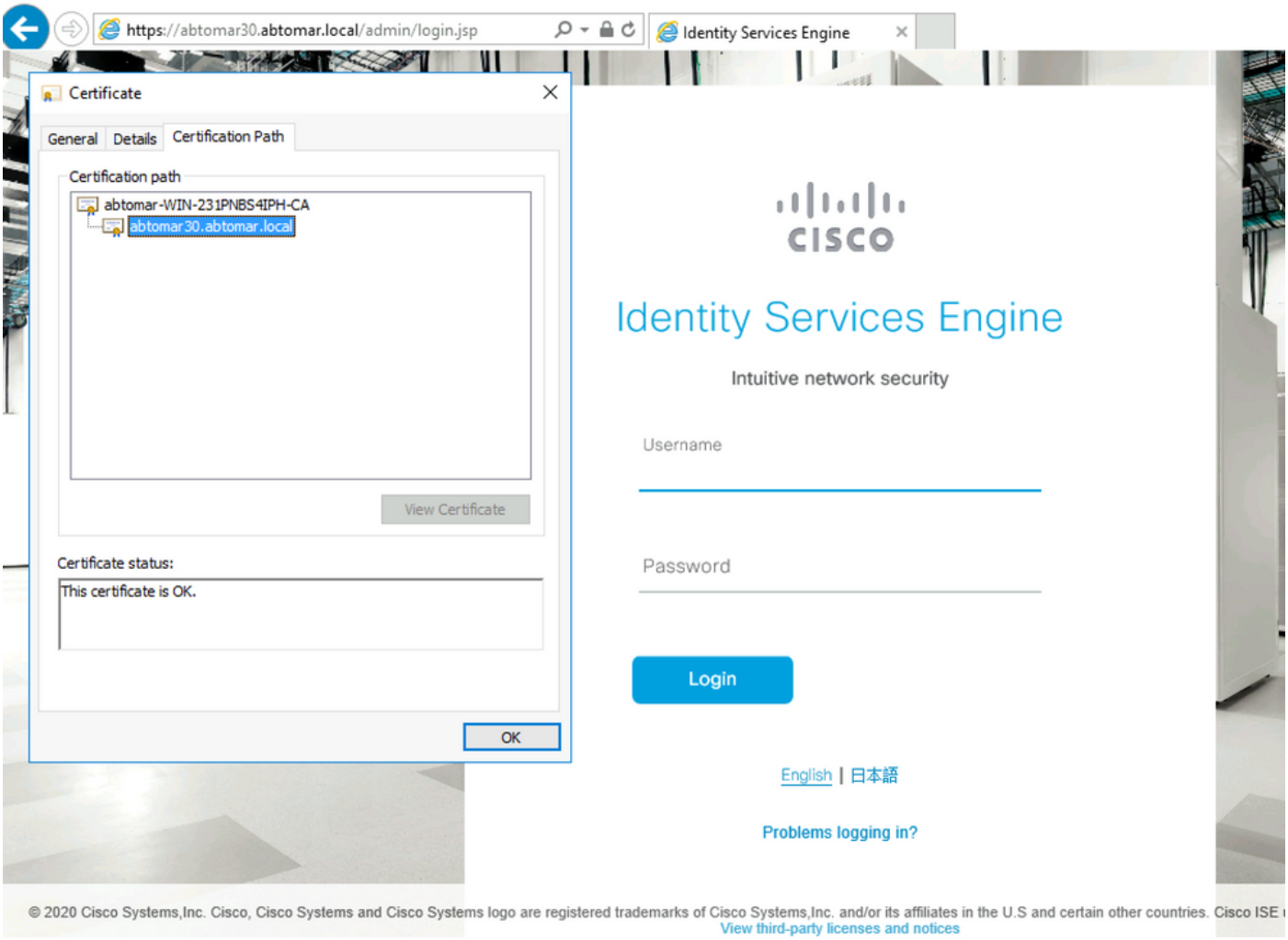
5. Wählen Sie den neuen Zertifikatsspeicherort aus, und die ISE bindet das Zertifikat an den privaten Schlüssel, der in der Datenbank erstellt und gespeichert wird.

   Hinweis: Wenn die Administratorrolle für dieses Zertifikat ausgewählt wurde, wird der spezielle ISE-Serverdienst neu gestartet.

   Vorsicht: Wenn das importierte Zertifikat für den primären Administrationsknoten der Bereitstellung bestimmt ist und die Administratorrolle ausgewählt ist, werden die Dienste auf allen Knoten nacheinander neu gestartet. Dies ist zu erwarten, und es wird eine Ausfallzeit empfohlen, um diese Aktivität durchzuführen.

Überprüfung

Wenn die Administratorrolle während des Zertifikatsimports ausgewählt wurde, können Sie überprüfen, ob das neue Zertifikat vorhanden ist. Laden Sie dazu die Administratorseite in den Browser. Der Browser sollte dem neuen Admin-Zertifikat vertrauen, solange die Kette korrekt erstellt wurde und die Zertifikatskette vom Browser vertrauenswürdig ist.



Um eine zusätzliche Überprüfung durchzuführen, wählen Sie im Browser das Sperrsymbol aus, und überprüfen Sie unter dem Zertifikatspfad, ob die vollständige Kette vorhanden und vom Computer vertrauenswürdig ist. Dies ist kein direkter Indikator dafür, dass der Server die gesamte Kette korrekt weitergegeben hat, sondern ein Indikator für den Browser, der das Serverzertifikat basierend auf seinem lokalen Vertrauensspeicher vertrauenswürdig machen kann.

Fehlerbehebung

Supplicant vertraut bei einer 802.1x-Authentifizierung nicht auf das ISE Local Server Certificate

Überprüfen Sie, ob die ISE während des SSL-Handshake-Prozesses die gesamte Zertifikatkette übergibt.

Wenn EAP-Methoden verwendet werden, für die ein Serverzertifikat (d. h. PEAP) erforderlich ist und **die Serveridentität validieren** ist, validiert der Supplicant die Zertifikatkette anhand der Zertifikate, die er im lokalen Vertrauensspeicher im Rahmen des Authentifizierungsprozesses besitzt. Im Rahmen des SSL-Handshake-Prozesses präsentiert die ISE ihr Zertifikat sowie alle Root- und (oder) Zwischenzertifikate, die in ihrer Kette vorhanden sind. Die Komponente kann die

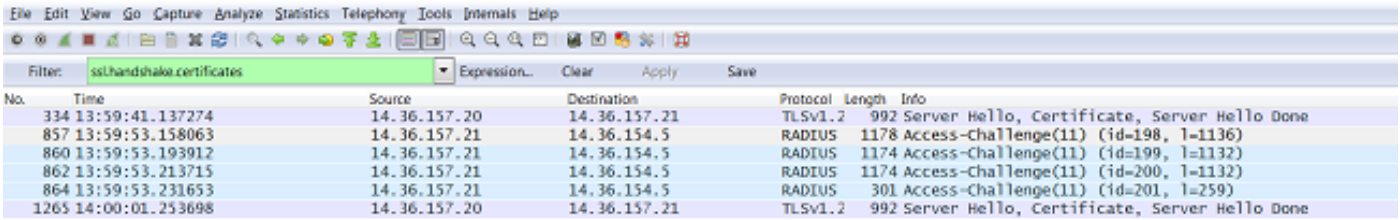
Serveridentität nicht überprüfen, wenn die Kette unvollständig ist. So überprüfen Sie, ob die Zertifikatskette an den Client zurückgegeben wird:

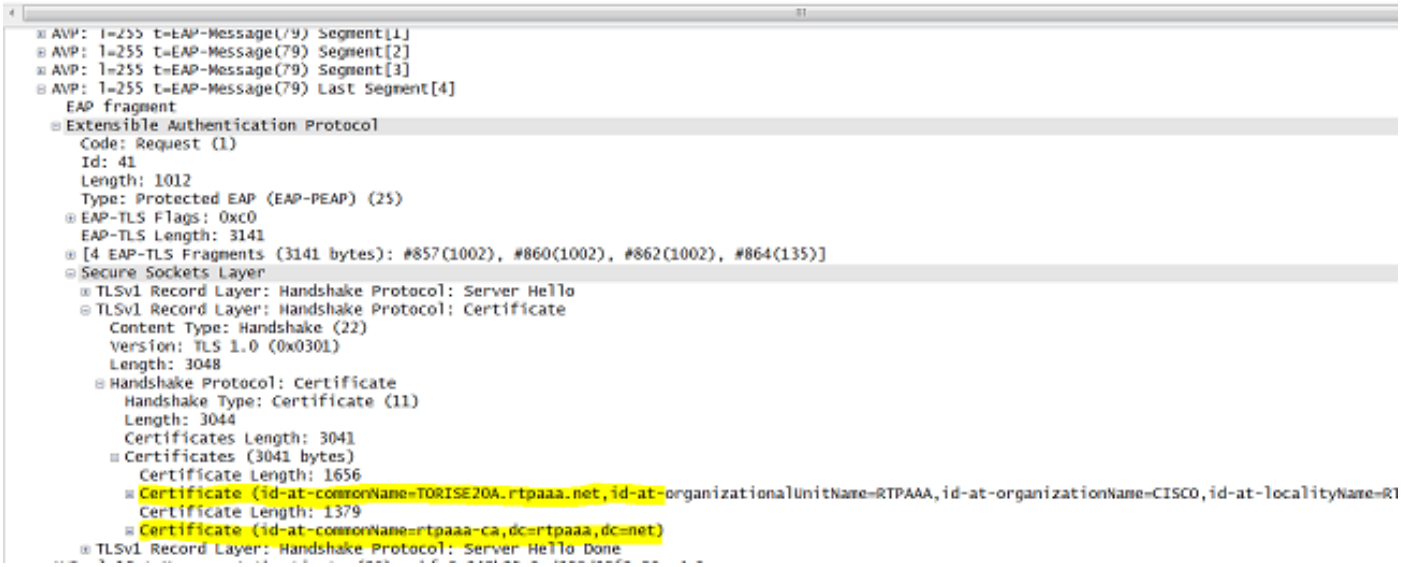
1. Um während der Authentifizierung eine Erfassung von der ISE (TCPDump) durchzuführen, navigieren Sie zu **Operations > Diagostic Tools > General Tools > TCP Dump**.

2. Laden Sie die Erfassung herunter/öffnen Sie sie, und wenden Sie den Filter **ssl.handshake.Certificates** in Wireshark an, um eine Zugriffs-Herausforderung zu finden.

3. Navigieren Sie nach der Auswahl zu **Erweitern Sie Radius Protocol > Attribute Value Paares > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates**.

Zertifikatskette in der Erfassung.

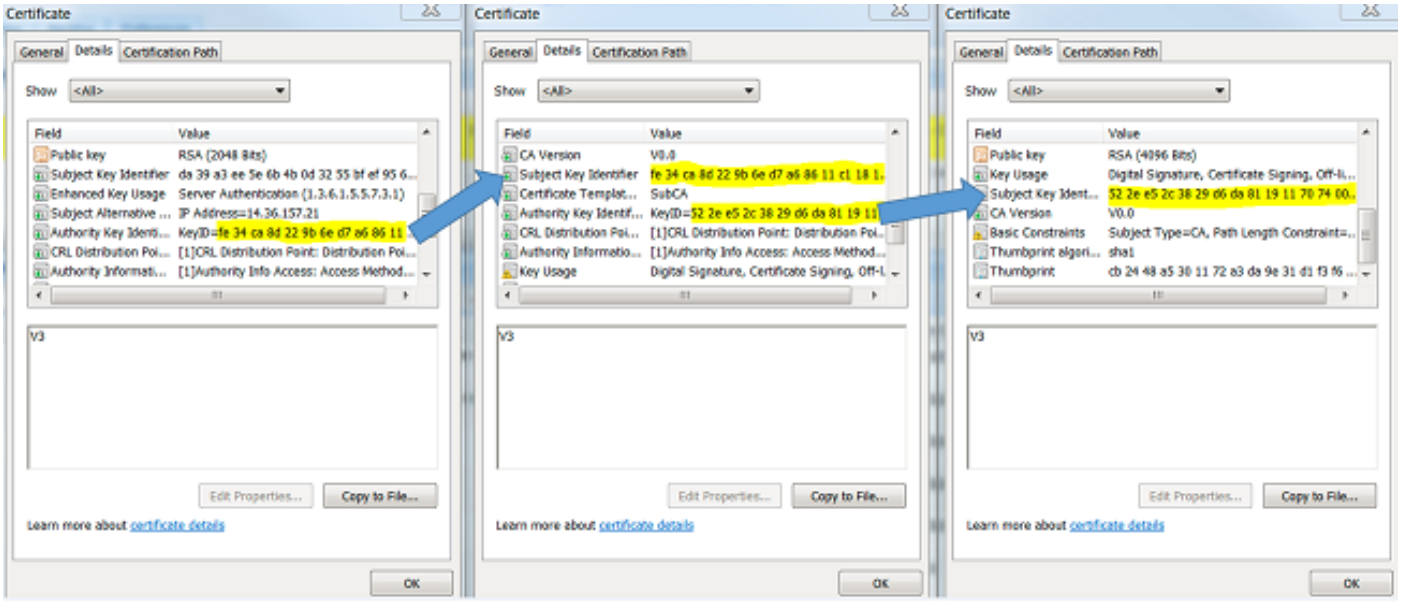




Wenn die Kette unvollständig ist, navigieren Sie zu **ISE Administration > Certificates > Trusted Certificates (ISE-Verwaltung > Certificates > Trusted Certificates),** und überprüfen Sie, ob die Root-Zertifikate und (oder) Zwischenzertifikate vorhanden sind. Wenn die Zertifikatskette erfolgreich übergeben wurde, sollte die Kette selbst mithilfe der hier beschriebenen Methode als gültig überprüft werden.

Öffnen Sie jedes Zertifikat (Server, Zwischengerät und Root), und überprüfen Sie die Vertrauenskette, indem Sie den Betreffschlüssel-Identifier (SKI) jedes Zertifikats mit dem Authority Key Identifier (AKI) des nächsten Zertifikats in der Kette abgleichen.

Beispiel einer Zertifikatskette.

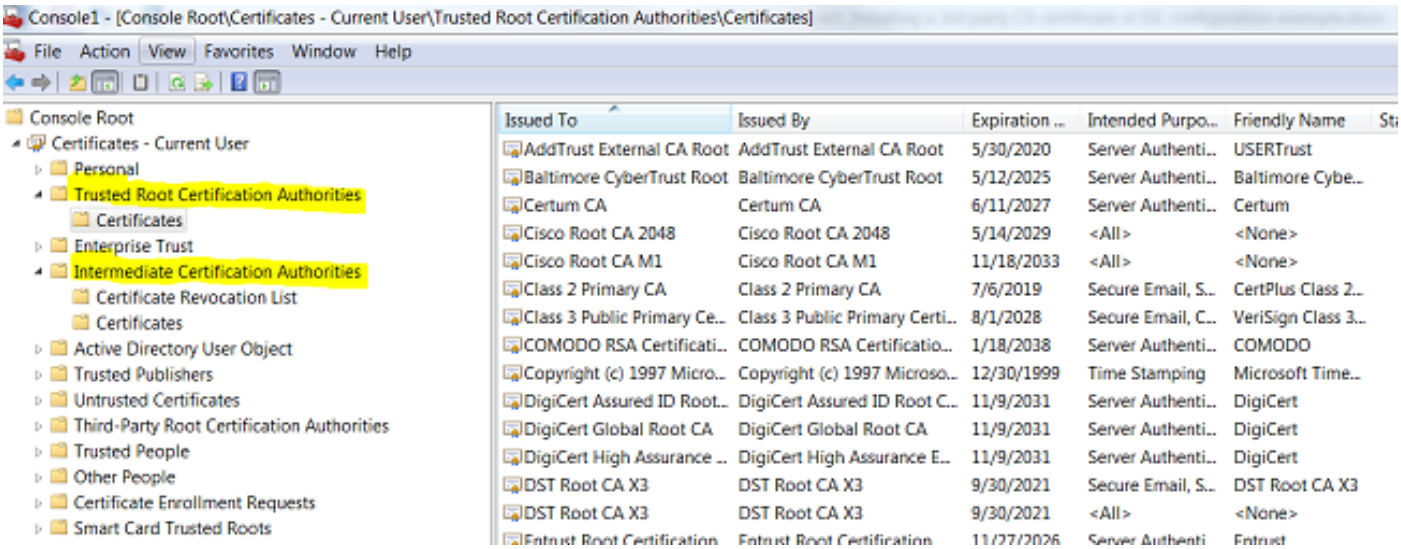


Die ISE-Zertifikatkette ist korrekt, aber der Endpunkt lehnt das ISE-Serverzertifikat während der Authentifizierung ab

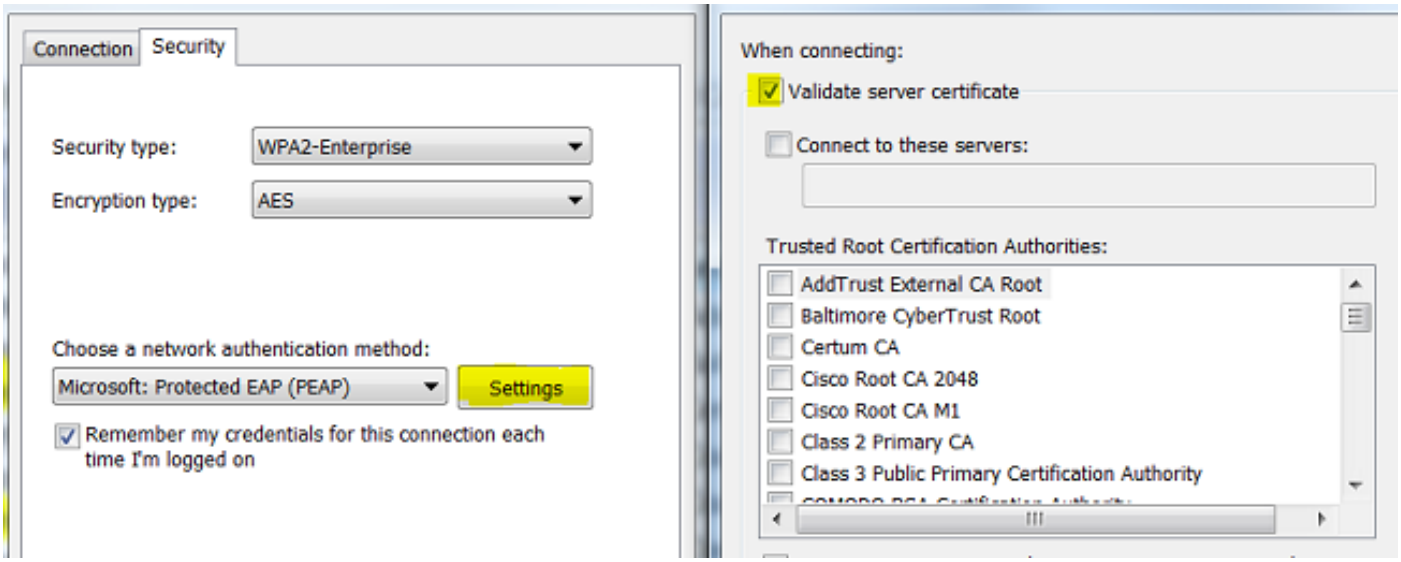
Wenn die ISE während des SSL-Handshakes die gesamte Zertifikatkette vorlegt und der Supplicant die Zertifikatskette weiterhin ablehnt, Im nächsten Schritt wird überprüft, ob sich die Root- und/oder Zwischenzertifikate im lokalen Client-Trust-Store befinden.

Um dies von einem Windows-Gerät aus zu überprüfen, navigieren Sie zu **mmc.exe** File **> Add-Remove Snap-In**. Wählen Sie in der Spalte Verfügbare Snap-Ins die Option **Zertifikate aus**, und klicken Sie auf **Hinzufügen**. Wählen Sie je nach verwendetem Authentifizierungstyp (Benutzer oder Computer) entweder **Mein Benutzerkonto** oder **Computerkonto** aus, und klicken Sie dann auf **OK**.

Wählen Sie in der Konsolenansicht **Trusted Root Certification Authorities** and **Intermediate Certification Authority (Vertrauenswürdige Root-Zertifizierungsstellen** und **Erweiterte Zertifizierungsstellen)** aus, um das Vorhandensein von Root and Intermediate Certificate im lokalen Trust Store zu überprüfen.



Eine einfache Methode, um zu überprüfen, ob es sich um ein Problem mit der Serveridentitätsprüfung handelt, deaktivieren Sie **Validate Server Certificate** unter der Komponentenprofilkonfiguration, und testen Sie es erneut.



Zugehörige Informationen

- Administratoranleitung für Cisco Identity Services Engine, Version 3.0
- Technischer Support und Dokumentation für Cisco Systeme