Vorbereitung der Identity Services Engine auf erweiterte Schlüsselverwendungsbeschränkungen in Zertifikaten, die von öffentlichen Zertifizierungsstellen ausgestellt wurden.

Inhalt

Einleitung

In diesem Dokument werden die Auswirkungen der angewendeten Einschränkungen

beschriebenzu den Kriterien für die Ausstellung der vonZertifizierungsstellen, die das Chrome Root Certificate-Programm in der Cisco Identity Services Engine (ISE) aktivieren.

Hintergrundinformationen

Digitale Zertifikate sind von Zertifizierungsstellen (Certification Authorities, CAs) ausgestellte elektronische Zertifikate, die die Kommunikation zwischen Servern und Clients schützen, indem sie Authentifizierung, Datenintegrität und Vertraulichkeit gewährleisten.
Extended Key Usage (EKU)-Felder sind Attribute, die den Zweck des öffentlichen Zertifikatschlüssels definieren.

Zwei der verfügbaren EKU-Werte sind:

- Serverauthentifizierungs-EKU (id-kp-serverAuth): Wird verwendet, wenn ein Server sein Zertifikat zum Identitätsnachweis vorlegt
- Clientauthentifizierungs-EKU (id-kp-clientAuth): Verwendung für gegenseitige TLS-Verbindungen (mTLS), bei denen sich beide Parteien gegenseitig authentifizieren

Ein einzelnes Zertifikat kann sowohl Server- als auch Client-Authentifizierungs-EKUs enthalten, sodass es für zwei Zwecke verwendet werden kann. Dies ist insbesondere für Produkte wie die ISE wichtig, die je nach Anwendungsfall entweder als Server oder Client fungieren.

Problemdefinition

Änderung der Chrome-Stammprogrammrichtlinie

Die Implementierung der EKU hängt von der CA ab, die das Zertifikat signiert. Die Verwendung von EKU für die Server- und die Clientauthentifizierung war eine gängige Praxis.

Im Rahmen der Chrome Root Program Policy Change setzen jedoch öffentliche Zertifizierungsstellen, die diese Zertifikatausstellungskriterien erfüllen, die Signierung von TLS-Zertifikaten ein, die die Client Authentication Extended Key Usage (EKU) enthalten. Neu ausgestellte Zertifikate enthalten nur die Serverauthentifizierungs-EKU.

Wichtige Richtlinienanforderungen

- Öffentliche Stammzertifizierungsstellen müssen nur die erweiterte Schlüsselverwendung (Extended Key Usage, EKU) für die Serverauthentifizierung (id-kp-serverAuth) geltend machen
- Das Zertifikat darf NUR die EKU für die Serverauthentifizierung enthalten.
- Das Einschließen von Clientauthentifizierungs-EKU in diese Zertifikate ist nicht zulässig.
- Stammzertifizierungsstellen, die weiterhin Zertifikate mit der Clientauthentifizierungs-EKU ausstellen, werden schließlich aus dem Chrome-Stammspeicher entfernt, was dazu führt,

dass solche Zertifikate vom Chrome-Browser als "Nicht vertrauenswürdig" gekennzeichnet werden

- Keine gemischten Stammzertifizierungsstellen mehr für TLS-Zertifikate für öffentliche Server
- Durchsetzungszeitleiste: März 2027.

Zeitplan

- Oktober 2025: CAs, die sich auf das Programm abstimmen (z. B. DigiCert, Sectigo usw.), haben standardmäßig mit der Ausgabe von Zertifikaten begonnen, die nur für Server bestimmt sind.
- Mai 2026: CAs, die sich auf das Programm abstimmen, stellen keine Client Authentication EKU-Zertifikate mehr aus
- März 2027: Chrome Root-Programm-Richtlinie wird voll wirksam

Auswirkungen auf die Cisco ISE

Betroffene Produkte

Alle Cisco ISE-Versionen sind betroffen:

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3.4
- ISE 3.5

Hinweis: Die erwähnte Änderung wirkt sich auf alle ISE-Versionen aus, einschließlich Versionen unter 3.x. Codeänderungen werden jedoch nur für die im vorherigen Abschnitt erwähnten Versionen freigegeben. Cisco empfiehlt ein Upgrade der ISE, um mögliche Auswirkungen zu vermeiden.

Spezifische Anwendungsfälle

In Tabelle 1 sind die Services aufgeführt, die von den bevorstehenden Änderungen der Clientauthentifizierungs-EKU betroffen sind, sowie die erwarteten Auswirkungen für die einzelnen Services.

Service	Auswirkungen

pxGrid	ISE pxGrid Service erfordert Kommunikation zwischen den Knoten über den pxGrid-Kanal. Dies bedeutet, dass einige Knoten als Server und andere als Clients arbeiten. Für die Installation des pxGrid-Zertifikats sind daher sowohl Server Authentication EKU als auch Client Authentication EKU erforderlich. Daher ist die Installation neu ausgestellter öffentlicher Zertifizierungsstellenzertifikate, die nur die Server-Authentifizierungs-EKU enthalten, eingeschränkt. ⚠ Vorsicht: Der ISE pxGrid-Dienst führt eine Zertifikat-EKU-Validierung durch. Externe pxGrid-Clientzertifikate müssen die Clientauthentifizierungs-EKU enthalten, wenn mit der ISE kommuniziert wird oder die Verbindung abgelehnt wird. Cisco empfiehlt die Verifizierung von Zertifikaten mit Public-CA-Signatur, die in externen pxGrid-Clients verwendet werden, um die Integration nicht zu beeinträchtigen.
ISE Messaging Service (IMS)	ISE Messaging Services (IMS) ist ein sicherer Kanal für die Kommunikation zwischen Knoten. Daher ist für die Installation des IMS-Zertifikats sowohl die Serverauthentifizierungs-EKU als auch die Clientauthentifizierungs-EKU erforderlich. Daher ist die Installation neu ausgestellter öffentlicher Zertifizierungsstellenzertifikate, die nicht beide EKUs enthalten, eingeschränkt.
TC-NAC	Bei der Auswahl des TC-NAC-Anbieters Tenable Security Center: VA in Administration > Threat Centric NAC > Add a new TC-NAC connector is created. Nachdem der Connector für die Konfiguration bereit ist, kann die "Certificate Based Authentication" als Authentifizierungsmethode für den TC-NAC Connector ausgewählt und anschließend das "ISE Admin Certificate" ausgewählt werden. Die TC-NAC-Verbindung zwischen dem ISE PSN und der VA DB wird hergestellt, sodass das Admin-Zertifikat des jeweiligen PSN als Client-Zertifikat verwendet wird. Wenn strenge mTLS in Tenable aktiviert ist, ist die Clientauthentifizierungs-EKU erforderlich. Andernfalls wird die TLS-Verbindung unterbrochen.

LDAPs, sicheres Syslog, RADIUS-DTLs für CoA	Diese drei Dienste bieten die Möglichkeit, bestimmte Zertifikate als "Client-Zertifikate" für die TLS-Authentifizierung zu verwenden. Die ISE führt keine EKU-Validierung durch. Die Auswirkungen auf diese Services hängen daher vollständig von der Serverseite ab. Wenn die Zertifikat-EKU-Validierung auf dem Server erzwungen wird, erfordert das von der ISE verwendete Zertifikat die Client Authentication EKU, oder die TLS-Authentifizierung schlägt fehl.

Tabelle 1: Betroffene Services

Symptome

Wenn Sie versuchen, ein Zertifikat mit der Serverauthentifizierungs-EKU nur für Dienste mit bestimmten EKU-Anforderungen zu installieren, wird der in Abbildung 1 gezeigte Fehler generiert.

pxGrid und ISE Messaging Service (IMS) sind Dienste mit solchen EKU-Anforderungen.

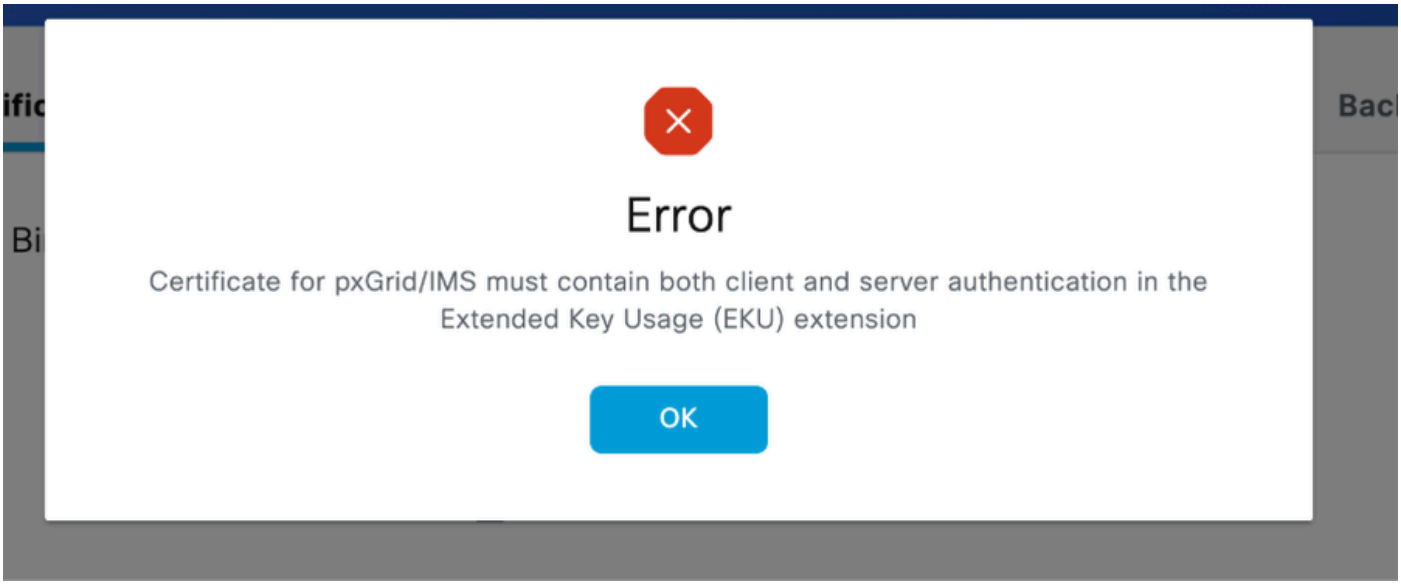

Image 1: Fehler bei der Installation eines Zertifikats, das nicht den EKU-Anforderungen entspricht

Empfehlungen

Prüfung von Zertifikaten mit potenziellen Auswirkungen und Befolgung der Empfehlungen

- In Tabelle 1 finden Sie die ISE-Services mit potenziellen Auswirkungen. Überprüfen Sie, welche der genannten Dienste auf von öffentlichen Zertifizierungsstellen signierten Zertifikaten basieren.

- Dokumentieren Sie die Zertifizierungsstellenkette für jedes Zertifikat, und validieren Sie, ob diese Zertifizierungsstelle die Änderungen der Ausstellungskriterien implementiert.
- Ablaufdatum überprüfen: Strategische Planung von Vertragsverlängerungen vor der Durchsetzung von Richtlinien Beachten Sie, dass die Clientauthentifizierungs-EKU je nach CA-Richtlinie eingeschränkt werden kann.
- Tabelle 2 enthält spezifische Empfehlungen für die Services, die von der Änderung der Ausstellungskriterien betroffen sind.

Service	Empfehlungen für Maßnahmen
pxGrid	Wenn das pxGrid-Zertifikat auf der ISE von einer öffentlichen Zertifizierungsstelle ausgestellt wird und eine Verlängerung oder Migration zu einer öffentlichen Zertifizierungsstelle geplant ist, wird die folgende Vorgehensweise empfohlen: 1.- Überprüfen Sie, ob derzeit die Serverauthentifizierungs-EKU und die Clientauthentifizierungs-EKU im Zertifikat vorhanden sind und ob beide je nach Zertifizierungsstellenrichtlinie beibehalten werden können. 2.- Wenn die Zertifizierungsstellenrichtlinie das Vorhandensein beider EKUs nicht zulässt, empfehlen wir die Migration des Zertifikats zur Signatur durch die interne ISE-Zertifizierungsstelle. Gehen Sie zu: Administration > System > Certificates > System Certificates > Select the certificate issued by the ISE internal CA of the specific node you want to modification > Edit > Check the pxGrid box under the usage section > Click on Save. Wenn kein von der internen ISE-Zertifizierungsstelle ausgestelltes Zertifikat vorhanden ist, müssen Sie ein Zertifikat generieren. Verwenden Sie das nächste Video als Hilfestellung bei der Erstellung des Zertifikats.
ISE Messaging-Zertifikat (IMS)	Wenn das ISE Messaging Service-Zertifikat derzeit von einer öffentlichen Zertifizierungsstelle signiert ist und eine Verlängerung oder Migration zu einer öffentlichen Zertifizierungsstelle geplant ist, wird die folgende Vorgehensweise empfohlen: 1.- Überprüfen Sie, ob die öffentliche Zertifizierungsstelle, zu der Sie migrieren oder die Sie für die Verlängerung verwenden, die Verwendung von EKUs für die Serverauthentifizierung und die Clientauthentifizierung akzeptiert. 2.- Wenn die öffentliche Zertifizierungsstelle dies nicht zulässt, migrieren Sie das ISE-Messaging-Zertifikat, um die interne ISE-Zertifizierungsstelle zu verwenden. Gehen Sie dazu zu Administration > System > Certificates > Certificate Signing Request > Generate Certificate Signing Request (CSR) > Wählen Sie im

	Dropdown-Menü "Certificate(s) will be used for" (Zertifikate werden verwendet für) die Option "ISE Messaging Service Certificate regenerieren > die Schaltfläche "ISE Messaging Service Certificate generieren" rechts unten im Bildschirm aus. Ein Neustart des Service ist nicht erforderlich. Stellen Sie sicher, dass alle ISE-Knoten in Betrieb und erreichbar sind. Dies geschieht aus der Perspektive des PAN an den Ports 12001 und 443, sodass die Zertifikatänderung ordnungsgemäß an alle Knoten propagiert wird.
TC-NAC	Der TC-NAC-Dienst verlässt sich für die mTLS-Authentifizierung auf das spezifische ISE-Admin-Zertifikat des Knotens. Wenn das Zertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt wird und eine Verlängerung oder Migration zu einer öffentlichen Zertifizierungsstelle geplant ist, wird Folgendes empfohlen: 1.- Überprüfen Sie, ob derzeit die Serverauthentifizierungs-EKU und die Clientauthentifizierungs-EKU im Zertifikat vorhanden sind und ob beide je nach Zertifizierungsstellenrichtlinie beibehalten werden können. 2.- Überprüfen, ob "strict mTLS" auf Tenable aktiviert ist Wenn Sie die strikte mTLS deaktivieren, kann nur ein Zertifikat mit der Serverauthentifizierungs-EKU verwendet werden.
LDAPs, sicheres Syslog, RADIUS-DTLs für CoA	Die ISE führt keine EKU-Validierung für die Clientzertifikate dieser Dienste durch. Wenn eine Verlängerung oder Migration zu einer öffentlichen Zertifizierungsstelle geplant ist, sollten Sie überprüfen, ob die EKU des Zertifikats nach der Verlängerung/Migration geändert wird und ob dies mit der TLS-Richtlinie auf Serverseite in Konflikt steht.

Tabelle 2: Empfohlene Maßnahmen zur Vermeidung von Beeinträchtigungen bestimmter Services

Kurzfristige Lösungen (vor Juni 2026)

Administratoren können aus einer der folgenden Workaround-Optionen wählen:

Option 1: Wechseln zu öffentlichen Stammzertifizierungsstellen mit kombinierten EKU-Zertifikaten

Einige Public Root-CAs (wie DigiCert und IdenTrust) stellen Zertifikate mit kombinierter EKU von einem alternativen Root aus aus aus, die nicht in den Chrome-Browser-Vertrauensspeicher aufgenommen werden können.

Beispiele für öffentliche Stammzertifizierungsstellen und EKU-Typen:

CA-Anbieter	EKU-Typ	Stamm-CA	Issuing/Sub-CA
IdenTrust	clientAuth + serverAuth	IdenTrust Stammzertifizierungsstelle für den öffentlichen Sektor 1	IdenTrust Public Sector Server CA 1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

Voraussetzungen für diesen Ansatz:

- Wenden Sie sich an Ihren Zertifizierungsstellenanbieter, um die Verfügbarkeit solcher Zertifikate zu überprüfen.
- Stellen Sie vor der Bereitstellung von Zertifikaten sicher, dass sowohl der Server, der das Zertifikat präsentiert, als auch alle Clients, die es verwenden, der entsprechenden Stammzertifizierungsstelle vertrauen.
- Wenn die Zertifizierungsstellenkette nicht vorinstalliert ist, installieren Sie sie bei Bedarf.
- Auf diese Weise können Software-Upgrades vermieden werden.

Verweise auf die Zertifikatsverwaltung:

- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3
- Zertifikatverlängerungen auf der ISE konfigurieren

Option 2: Verlängerung der aktuellen Zertifikate, um ihre Gültigkeit zu verlängern

Zertifikate, die von öffentlichen Stammzertifizierungsstellen vor Mai 2026 ausgestellt wurden und über eine EKU für die Server- und Clientauthentifizierung verfügen, werden bis zum Ablauf ihrer Laufzeit weiterhin anerkannt.

Erneuerungsstrategie

Allgemeine Richtlinien:

- Erneuern Sie kombinierte EKU-Zertifikate, bevor die Richtlinie außer Kraft gesetzt wird.
- Nach dem 15. März 2026 sind von einer öffentlichen Zertifizierungsstelle ausgestellte Zertifikate nur noch 200 Tage gültig.
- Die Richtlinien für öffentliche Zertifizierungsstellen und die Implementierungsdaten können variieren.
- Einige öffentliche Zertifizierungsstellen stellen keine kombinierten EKU-Zertifikate mehr aus.

Option 3: Evaluierung und Migration zu alternativen Zertifizierungsstellenanbietern

Allgemeine Richtlinien:

- Migrieren Sie zu einer alternativen Zertifizierungsstelle, sodass sowohl die Server- als auch die Clientauthentifizierungs-EKU vorhanden ist.
- Bietet langfristige Kontrolle über Zertifikatrichtlinien
- Wenn Sie ein privates CA-signiertes Zertifikat ausstellen, müssen Sie dem Peer Stammzertifikatinformationen zur Verfügung stellen.
- Stellen Sie vor der Ausstellung oder Bereitstellung eines Zertifikats sicher, dass sowohl der Server, auf dem das Zertifikat ausgestellt wird, als auch alle Clients, die es verwenden, der entsprechenden Zertifizierungsstellenkette vertrauen.

Langfristige Lösung (Software-Upgrade erforderlich)

Kunden können die ISE auf eine Patch-Version aktualisieren, die eine aktualisierte Zertifikatbehandlung zur Unterstützung von Zertifikaten ermöglicht, die im Rahmen der neuen Zertifizierungsstellenrichtlinien ausgestellt wurden.

Die nächsten Patch-Versionen enthalten Verhaltensänderungen, um die ISE an die neuen Einschränkungen anzupassen. Geplantes Veröffentlichungsdatum ist April 2026:

Cisco ISE-Version	Patch-Version
ISE 3.1	Patch 11
ISE 3.2	Patch 10
ISE 3.3	Patch 11
ISE 3.4	Patch 6
ISE 3.5	Patch 3

Verhalten nach der Patch-Installation

⚠ Vorsicht: Dieser Patch führt Verhaltensänderungen in der Zertifikatverwaltungslogik ein. Vor der Installation des Patches sollten Sie ein Backup des ISE pxGrid-Zertifikats und des IMS-Zertifikats erstellen. Ein mögliches Störungsszenario besteht darin, den Patch zu installieren, mit der Installation von Zertifikaten nur mit der Serverauthentifizierungs-EKU fortzufahren und den Patch dann zurückzusetzen. In diesem Szenario werden die Zertifikate vom System ignoriert, das sich auf die spezifischen Funktionen auswirkt.

PxGrid-Zertifikat

Nach der Installation der Patch-Version:

- Der Import von pxGrid-Zertifikaten, die nur Server-Authentifizierungs-EKUs, sowohl Server- als auch Clientauthentifizierungs-EKUs enthalten, oder keine EKU-Erweiterung ist zulässig.
- Zertifikate, die nur die Clientauthentifizierungs-EKU enthalten, werden abgelehnt.

ISE Messaging Service (IMS)-Zertifikat

ISE 3.1, 3.2 und 3.3

Nach der Installation des Patches wird keine Verhaltensänderung vorgenommen. Der ISE Messaging Service erfordert ein Zertifikat mit der Client- und Server-EKU. Kunden müssen die Migration zu einem ISE Internal CA-signierten Zertifikat planen, sobald das aktuelle Zertifikat abläuft.

ISE 3.4 und 3.5

Nach der Patch-Installation ist die Verwendung eines öffentlichen, von einer Zertifizierungsstelle signierten Zertifikats zulässig, das nur die Serverauthentifizierungs-EKU enthält.

Anmerkung: Die Verwendung einer von einer öffentlichen Zertifizierungsstelle signierten Zertifizierung wird für IMS unterstützt. Cisco empfiehlt die Verwendung des ISE Internal CA-Zertifikats, da diese Kommunikation nur für interne Transaktionen verwendet wird.

Häufig gestellte Fragen

Allgemeine Fragen

F: Muss ich mir darüber Gedanken machen, wenn ich eine private PKI verwende?

A: Die von privaten Zertifizierungsstellen durchgesetzte Richtlinie wird von jeder Organisation definiert. Wenn Ihre private Zertifizierungsstelle die gleichen Ausstellungskriterien erfüllt, können die Richtlinien für dieses Dokument verwendet werden.

F: Kann ich meine vorhandenen Zertifikate weiterhin verwenden?

A : Ja, vorhandene Zertifikate mit kombinierter EKU bleiben bis zu ihrem Ablauf gültig. Das Problem tritt auf, wenn eine Verlängerung erforderlich ist. Sie funktionieren sowohl für TLS- als auch für mTLS-Verbindungen bis zum Ablauf.

F: Woher weiß ich, ob ich mTLS oder Standard-TLS verwende?

A : Lesen Sie den Abschnitt "Spezifische betroffene Anwendungsfälle".

Zusätzliche Ressourcen

- Cisco Bug-ID CSCws83036- Auswirkungsanalyse der ClientAuth EKU-Durchsetzung in ISE

Externe Referenzen

- Richtlinie für Chrome-Stammprogramm

Ressourcen der Zertifizierungsstelle

- IdenTrust-Portal

Schlussfolgerung

Die Einstellung der EKU für die Client-Authentifizierung in öffentlichen Zertifizierungsstellenzertifikaten stellt eine erhebliche Änderung der Sicherheitsrichtlinien dar, die sich auf Cisco ISE-Bereitstellungen mit mTLS-Verbindungen auswirkt. Zwar handelt es sich hierbei um eine branchenweite Änderung, die Auswirkungsbewertung ist jedoch ENTSCHEIDEND, und es sind sofortige Maßnahmen erforderlich, um Serviceunterbrechungen zu vermeiden.

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.