Prepare Cisco ISE for Client Auth EKU Sunset in Public CA Certificates

Contents

Introduction

This document describes the impact on ISE services due to upcoming changes to TLS Certificates Issued by Public Certificate Authorities with Client Authentication EKU.

Background Information

Digital certificates are electronic credentials issued by trusted Certificate Authorities (CAs) that secure communication between servers and clients by ensuring authentication, data integrity, and confidentiality. These certificates contain Extended Key Usage (EKU) fields that define their purpose:

- **Server Authentication EKU** (id-kp-serverAuth): Used when a server presents its certificate to prove identity
- **Client Authentication EKU** (id-kp-clientAuth): Used in mutual TLS (mTLS) connections where both parties authenticate each other

Traditionally, a single certificate could contain both Server and Client Authentication EKUs, allowing it to serve dual purposes. This is particularly important for products like Cisco ISE that act as both server and client in different connection scenarios.

Problem Definition

Chrome Root Program Policy Change

Beginning May 2026, many Public Certificate Authorities (CAs) will discontinue issuing Transport Layer Security (TLS) certificates that include the Client Authentication Extended Key Usage (EKU). Newly issued certificates will typically include Server Authentication EKU only.

Key Policy Requirements

- Public Root CAs must assert Extended Key Usage (EKU) ONLY for Server Authentication (id-kp-serverAuth)
- Certificates must include ONLY Server Authentication EKU.
- Including Client Authentication EKU in these certificates are prohibited
- Root CAs that continue to issue certificates with Client Authentication EKU are eventually removed from the Chrome Root Store
- No more mixed-use root CAs for public server TLS certificates
- Enforcement Timeline: March 2027.

Public CA Response Timeline

- October 2025: Many public CAs (DigiCert, Sectigo, SSL) began issuing server-only certificates by default.
- May 2026: Many Public CA servers stop issuing Client Authentication EKU certifications
- March 2027: Chrome Root Program Policy becomes fully effective

Note: This policy applies only to certificates issued by public CAs. Private PKI and self-signed certificates are not affected by this policy.

How It Impacts Cisco ISE

Affected Products

All Cisco ISE releases are affected:

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

Note: Cisco ISE 2.x versions are also affected; however, no fix is planned because these releases have reached end of life (EOL).

Dual Role of Cisco ISE

ISE act as both server and client in various connection scenarios, requiring certificates with **both Server and Client Authentication EKUs**.

Cisco ISE as a Server **(Server Authentication EKU required)**:

- PxGrid
- ISE Messaging Service

Cisco ISE as a Client **(Client Authentication EKU required)**:

- TC-NAC
- Secure Syslog
- LDAPS
- Radius DTLS

Specific Affected Use Cases

The table below summarizes the Cisco ISE services that may be affected by the upcoming Client Authentication EKU changes, along with the expected impact for each service.

Service	**Impact**
pxGrid	pxGrid certificates are used for communication between ISE nodes and external pxGrid integrations. While external pxGrid integrations require only **Server Authentication EKU**, Cisco ISE currently requires imported pxGrid certificates to contain both **Server Authentication EKU** and **Client Authentication EKU** due to a UI restriction. As a result, Public CA–issued pxGrid certificates are commonly deployed with both EKUs.
ISE Messaging Service (IMS)	IMS is used for backend communication between internal ISE services. Cisco ISE currently requires IMS certificates to contain both **Server Authentication EKU** and **Client Authentication EKU**. Certificates renewed by a Public CA with **Server**

	Authentication EKU only cannot be used for IMS, which can result in failures in internal ISE communication.
TC-NAC	If the **Admin certificate** contains **Server Authentication EKU only**, certificate-based authentication for **TC-NAC** may be impacted when **FIPS mode** is enabled or when **Tenable is configured with mTLS** (Introduced in ISE versions 3.4P3 and 3.5).
Secure Syslog	
LDAPs	
RADIUS DTLS	

⚠ **Caution**: Customers should verify the certificate type used by any **external pxGrid clients**. Upon renewal, Public CA–signed certificates may **no longer include Client Authentication EKU**. External pxGrid client integrations **must include the Client Authentication EKU** when communicating with ISE or the connection will be rejected.

Problem Symptoms

After deployment of **Server Authentication EKU only** certificates in Cisco ISE, customers will observe certificate import failures in the Cisco ISE GUI when attempting to upload **pxGrid** or **ISE Messaging Service (IMS)** certificates that do not meet the current Extended Key Usage (EKU) requirements for the selected service.

An example of the error message displayed in the GUI is shown below.

Recommendations

Audit Current Certificates (MANDATORY FIRST STEP)

- Prepare an inventory of all public TLS certificates to identify which certificates contain the Client Authentication EKU
- Document certificate usage: Identify which certificates are used as per the table above that are signed with Public-CA.
- Verify CA and root information: Document which CA and root issued each certificate
- Check expiration dates: Plan renewals strategically before policy enforcement

Suggestions for Services that require Client EKU

The table below provides recommended actions for Cisco ISE services and integrations that rely on certificates containing Client Authentication EKU.

Service	**Recommended actions**
TC-NAC	• When **Tenable** is used, **strict EKU validation can be disabled on the Tenable side to maintain connectivity.**
Secure Syslog	
LDAPs	
RADIUS DTLS	
PxGrid Clients (CatC, FMC...etc)	
EAP-TLS	

Short-Term Workarounds (Before June 2026)

Administrators can choose from one of these workaround options:

Option 1: Switch to Public Root CAs Providing Combined EKU Certificates

Some Public Root CAs (such as DigiCert and IdenTrust) issue certificates with combined EKU from an alternative root, which can not be included in the Chrome browser trust store.

Examples of Public Root CAs and EKU Types:

CA Vendor	**EKU Type**	**Root CA**	**Issuing/Sub CA**
IdenTrust	clientAuth + serverAuth	IdenTrust Public Sector Root CA 1	IdenTrust Public Sector Server CA 1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

Prerequisites for this approach:

- Coordinate with your CA provider to check the availability of such certificates.
- Before deploying certificates, ensure that both the server presenting the certificate and all clients consuming it trust the corresponding Root CA.
- Exchange root certificate information with communication peers.
- This approach avoids immediate need for software upgrades.

Certificate Management References:

- Cisco Identity Services Engine Administrator Guide, Release 3.3
- Configure Certificate Renewals on ISE

Option 2: Renew Current Certificates to Extend Their Validity

Certificates issued by Public Root CAs before May 2026 that have both Server and Client Authentication EKU continue to be honored until their term expires.

Renewal Strategy

General recommendations are:

- Renew combined EKU certificates before policy sunsetting occurs
- For maximum certificate validity, plan to renew certificates before March 15, 2026.
- After this date, Public CA-issued certificates are valid only for 200 days.
- Cisco strongly recommends that you renew your certificates before this date if you wish to pursue this option.
- Public CA policy and implementation dates can vary.
- Some Public CAs have stopped issuing combined EKU certificates and can not provide one by default.
- To generate a certificate with a combined EKU, work with your CA authority and use a special profile provided by Public CAs.

Option 3: Evaluate and Migrate to Alternative CA Providers

Private PKI Approach

- Evaluate the feasibility of transition to private PKI
- Set up a private CA to issue single certificates with combined EKU (server and client certificates with the required EKUs)
- When issuing a private CA-signed certificate, you need to share root certificate information with the peer.
- Before issuing or deploying a certificate, ensure that both the server presenting the certificate and all clients consuming it trust the corresponding Root CA.
- Private CAs are not subject to Chrome Root Program Policy
- Provides long-term control over certificate policies

Long-Term Solution (Software Upgrade Required)

Customers should upgrade Cisco ISE to a patch release that introduces updated certificate handling to support certificates issued under the new CA policies.

The following patch releases address this issue planned for 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

Behaviour After Patch Installation

PxGrid Certificate

After installing the patch release:

- The current UI requirement that enforces both Server Authentication EKU and Client Authentication EKU for pxGrid certificates will be removed.
- Cisco ISE will allow the import of pxGrid certificates containing **Server Authentication EKU only**, **both Server and Client Authentication EKUs**, or **no EKU extension**.
- Certificates containing **Client Authentication EKU only** will not be accepted.

ISE Messaging Service (IMS) Certificate

For ISE 3.1, 3.2 and 3.3

There is **no change in behavior** after installing the patch. The ISE Messaging Service will continue to require a certificate with both client and server EKU. Customers should plan to use an **ISE Internal CA certificate** once the current certificate expires.

For ISE 3.4 and 3.5

IMS now supports **Public CA certificates containing Server Authentication EKU only**. However, because IMS is used only for internal Cisco ISE communication, Cisco recommends using the **ISE Internal CA certificate** when the certificate is renewed.

Decision Tree

START: Do you use Public CA certificates on Cisco ISE?

```
│
├── NO: Private PKI or Self-Signed
│   └── No action required - Not affected by policy
│
└── YES: Public CA certificates in use
    │
    ├── Are they used for any of the services mentioned in the "Specific Affected Use Cases" section?
```

```
│ │
│ ├─ Services when ISE acts as TLS Client
│ │  └─ Review "Suggestions for Services that require Client EKU" section.
│ │
│ └─ Services when ISE acts as TLS Server (PxGrid OR IMS)
│    │
│    └─ Choose YOUR approach:
│       │
│       ├─ Option A: Switch to Alternative Root CA
│       │  ├─ Contact CA provider for combined EKU from alternative root
│       │  ├─ Ensure all peers trust new root
│       │  └─ No immediate software upgrade needed
│       │
│       ├─ Option B: Renew Certificates Before Deadlines
│       │  ├─ This will help release the urgency of patching Cisco ISE
│       │  │
│       │  ├─ For maximum validity: Renew before Mar 15, 2026
│       │  └─ Buys time until certificate expiry
│       │
│       ├─ Option C: Migrate to Private PKI
│       │  ├─ Set up private CA infrastructure
│       │  ├─ Issue combined EKU certificates
│       │  ├─ Install the new CA in ISE Trusted Store
│       │  └─ Long-term control
│       │
│       └─ Option D : Plan Software Upgrade
│          ├─ Apply the required ISE patch release (Available starting April 2026)
```

Frequently Asked Questions (FAQ)

General Questions

Q: Do I need to worry about this if I use private PKI?

A: No. This policy only affects certificates issued by Public Root CAs. Private PKI and self-signed certificates are not impacted.

Q: Can I continue using my existing certificates?

A: Yes, existing certificates with combined EKU remain valid until they expire. The issue arises when you need to renew. They work for both TLS and mTLS connections until expiry.

Q: How do I know if I am using mTLS or standard TLS?

A: Review ***Specific Affected Use Cases*** section.

Upgrade Questions

Certificate Management

Timeline Questions

Q: What happens on June 15, 2026?

A: Chrome stops trusting public TLS certificates containing both Server and Client Authentication EKUs. Services using such certificates can fail.

Q: Why do I have to I renew before March 15, 2026?

A: After March 15, 2026, certificate validity is reduced from 398 days to 200 days. Renewing before this date gives you maximum certificate lifetime.

Q: What is the deadline for action?

A: There are multiple deadlines:

- March 15, 2026: Certificate validity reduced to 200 days
- May 2026: Most public CAs stop issuing combined EKU entirely
- March 2027: Chrome policy fully enforced

Additional Resources

- Cisco bug ID: CSCws83036- Impact assesment of ClientAuth EKU enforcement in ISE

External References

- Chrome Root Program Policy

Certificate Authority Resources

- IdenTrust Portal

Conclusion

The sunsetting of Client Authentication EKU in public CA certificates represent a significant security policy shift that impacts Cisco ISE deployments using mTLS connections. While this is an industry-wide change, the impact rating is CRITICAL and immediate action is required to prevent service disruptions.