Cisco Secure Firewallにおけるパブリックcaクライアント認証のEKUの変更の影響（セキュアな通信を実現するため、2026年5月より開始）

はじめに

このドキュメントでは、特にCisco Secure Firewall製品に関連する場合、Chromeルート証明書プログラムに準拠する認証局(CA)によって課される証明書発行基準への制限の影響について説明します。

バックグラウンド情報

一般に信頼されているTLS証明書は、証明書の発行と使用を規定する業界ポリシーに準拠する必要があるCAによって発行されます。

Googleが運営するChromeルートプログラムポリシーは、CAが証明書をGoogle Chromeブラウザによって信頼されるために従う必要がある要件を定義します。これらの要件は、業界全体で公的に信頼できる証明書を発行する方法に影響を与えます。進化するセキュリティ対策の一環として、Chromeルートプログラムは証明書の使用に関するより厳密なガイダンスを導入しています。

そのため、多くのパブリックCAは、クライアント認証EKUを含む証明書の発行から離れ、サーバ認証のみを目的とした証明書の発行に移行しています。 その結果、多くのパブリックCAから新しく発行された証明書には、サーバ認証EKUのみが含まれることが予想されます。

拡張キー使用法(EKU)は、デジタル証明書内の公開キーの目的の機能を定義する証明書の拡張です。許可されたアプリケーションの構造化されたセットを確立し、キーが特定の暗号操作にのみ使用されるようにします。 この機能は、オブジェクト識別子(OID)（コード署名、サーバ認証、クライアント認証、安全な電子メールなど、許可された各用途を分類する一意の数値識別子）によって制御されます。

認証が証明書ベースの場合、検証エンティティは証明書を確認して、EKU内のオブジェクト識別子(OID)を特定します。EKU拡張子を埋め込むことで、認証局(CA)は証明書の範囲を事前定義されたロールに制限し、指定された各目的は明示的にOIDにマップされます。

EKU属性の目的

・ 使用方法の定義：EKU属性は、証明書の実行が許可されている認証または暗号化のタイプを明確にします。

・ セキュリティの強化：EKUは、証明書を特定の用途に限定することで、誤用や意図しないアプリケーションの使用を防止します（たとえば、サーバ証明書をクライアント認証に使用することはできません）。

・ コンプライアンス：セキュリティポリシーと業界標準に従って証明書が使用されていることを確認します。

EKU属性の主な用途

1. TLS Webクライアント認証

・ サーバに対するユーザまたはデバイスの識別と認証に証明書を使用できるようにします。

・ OID:1.3.6.1.5.5.7.3.2

・ VPN、相互TLS、およびセキュアログインシナリオで使用されます。

2. TLS Webサーバ認証

・ サーバが証明書を使用して自身の身元をクライアントに証明することを許可します。

・ OID:1.3.6.1.5.5.7.3.1

・ HTTPS、SSL/TLS Webサーバ、およびセキュアAPIエンドポイントで使用されます。

3.コード署名

・ ソフトウェアまたは実行可能ファイルの署名に証明書を使用できることを示します。

・ OID:1.3.6.1.5.5.7.3.3

・ ソフトウェアの配布と整合性チェックで使用されます。

4. 電子メール保護

・ 電子メールメッセージの署名および暗号化に証明書を使用できるようにします。

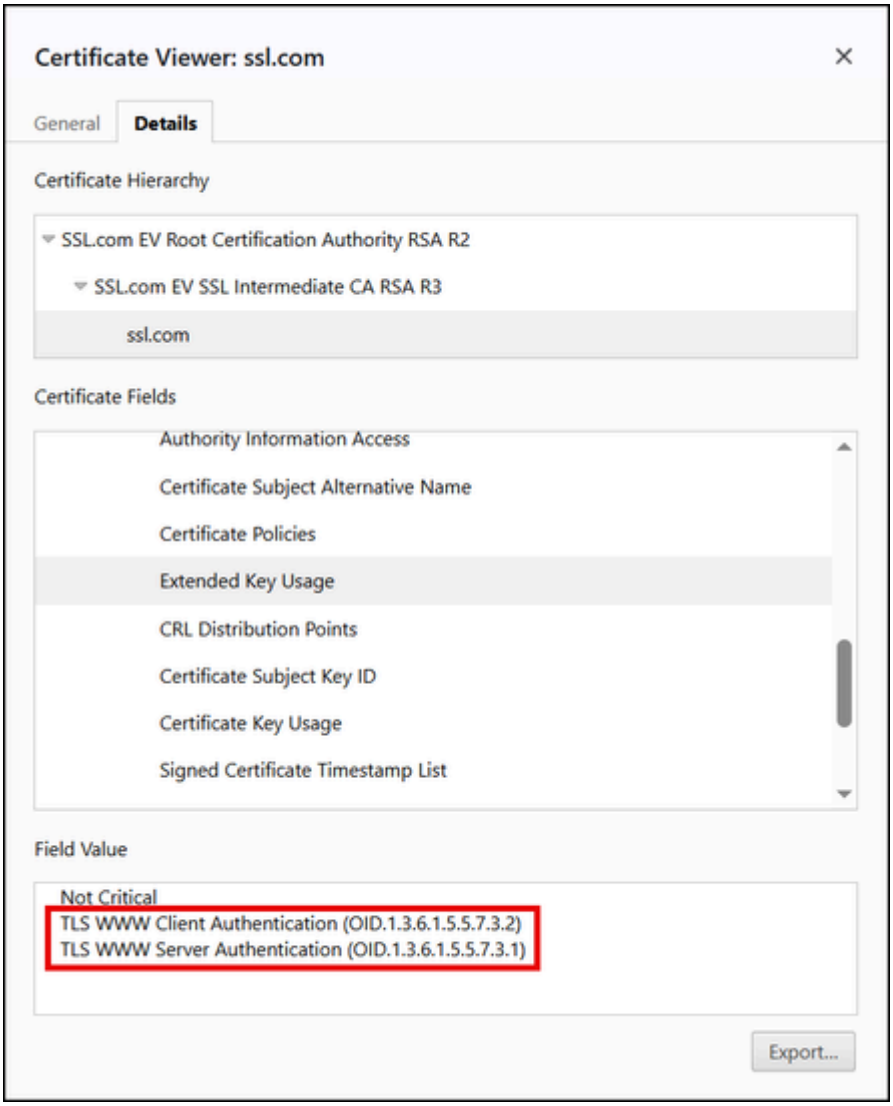
・ OID:1.3.6.1.5.5.7.3.4

・ S/MIME電子メールセキュリティで使用されます。

5.その他の目的

・ ドキュメントの署名、タイムスタンプ、スマートカードログオンなど、それぞれが独自のOIDを持つ。

ブラウザとサーバでは、HTTPSのセキュアな接続を確立するためにserverAuth EKUのみが必要ですが、歴史的に見ると、多くのTLSサーバ証明書には、serverAuthとclientAuth EKUの両方が含まれていました。このような証明書の例を次に示します。



サーバ証明書からクライアント認証EKUを削除する理由

- セキュリティとスコープ：パブリックTLS証明書は、Web上でサーバを認証するためだけに使用します。この削

除により、サーバとクライアントの機能が明確に分離されます。ClientAuth EKUは、相互TLS(mTLS)およびその他の認証シナリオを使用するマシンおよびユーザの認証に使用されます。

- 誤設定の防止：システムによっては、EKUが存在する場合、クライアント認証についてパブリックCAからのすべての証明書を信頼する場合があり、これはセキュリティリスクになる可能性があります。

- ブラウザの要件：主要なブラウザでは、Webサイトの証明書でclientAuth EKUを必要としたり、チェックしたりすることはありません。

- 簡素化されたPKIアーキテクチャ：使用法を分離することで、CAはサーバTLSと他の目的で異なる証明書階層を維持できます。

これは、Cisco Secure Firewall Adaptive Security Appliance(ASA)、Cisco Secure Firewall Threat Defense(FTD)、Cisco Secure Firewall Device Manager(FDM)、およびCisco Secure Firewall Management Center(FMC)などの製品で、ユースケースに応じて、TLS認証中にサーバまたはクライアントとして機能する可能性がある場合に特に重要です。

サーバ環境への影響

サーバ導入の大部分では、この変更による影響は小さいか、またはまったくないと考えられます。次の内容が予想されます。

- 標準Webサーバ(HTTPS):影響なし更新された証明書は正常に機能し続けます。

- 既存の証明書：カットオフの前に発行された証明書は、有効期限が切れるまで機能し続けます。

- 相互TLS(mTLS)およびクライアント証明書のシナリオ：クライアント認証にTLSサーバ証明書を使用している場合、別のソースからclientAuth EKUを使用して別の証明書を取得する必要があります。

- 両方のEKUを必要とするエンタープライズシステム：一部のレガシーシステムまたはエンタープライズシステムでは、両方のEKUを必要としていました。新しいルールに準拠するために更新が必要かどうかを確認する必要があります。

問題の説明

2026年5月以降、多くの公開証明機関(CA)は、クライアント認証の拡張キー使用法(EKU)を含むTransport Layer Security(TLS)証明書の発行を停止します。 新しく発行された証明書には、通常、サーバ認証EKUのみが含まれます。

その結果、パブリックCAによって発行された証明書が、更新されたCAポリシーに基づいて更新された後、Cisco Secure　Firewall製品に展開されると、クライアント認証EKUが必要なサービスは失敗します。影響を受ける具体的なサービスは次のとおりです。

- ASA、FTD、FDM、またはFMCがクライアントとして機能する場合(ISE(pxGrid)、RADIUS、LDAPS、Active DirectoryなどのIDプロバイダーや認証サーバに接続する場合など)、クライアント証明書がパブリックCAによって生成され、クライアント認証EKUが欠落していると、証明書ベースの認証が失敗する場合があります。このようなシナリオでは、認証サーバが必要なEKUなしで証明書を拒否すると、接続エラーが発生する可能性があります。

- Cisco Secure Client（以前のAnyConnect）は、証明書を使用してASAサーバまたはFTDサーバに対して認証できます。ただし、クライアント証明書がパブリックCAによって生成されたものであり、クライアント認証EKUが欠落している場合、リモートアクセスVPN(RAVPN)接続は失敗します。

- 証明書認証（RSAまたはECDSA）を使用して、FTDまたはASAがサイト間VPNトンネル（別のFTD、ASA、Ciscoルータ、またはサードパーティのVPNピアのいずれに対するものでも）を確立する場合、パブリックCAによって生成されたアイデンティティ証明書にクライアント認証EKU属性が欠落していると、トンネルに障害が発生します。これは、リモートVPNピアでは、ID証明書にクライアント認証EKUが含まれている必要があるためです。

Chromeルートプログラムポリシーの変更

EKUの実装は、証明書に署名するCAによって異なります。サーバ認証とクライアント認証のEKUの両方を使用するのが一般的でした。 ただし、Chromeルートプログラムポリシー変更の一部として、この証明書発行基準に合わせて、クライアント認証拡張キー使用法(EKU)を含むTLS証明書の署名を中止しています。　新しく発行された証明書には、サーバ認証EKUのみが含まれます。

主要なポリシー要件

- パブリックルートCAは、サーバー認証(id-kp-serverAuth)に対してのみ拡張キー使用法(EKU)をアサートする必要があります

- 証明書には、サーバ認証EKUのみが含まれている必要があります。

- これらの証明書にクライアント認証EKUを含めることは禁止されています

- クライアント認証EKUを使用して証明書を発行し続けるルートCAは、最終的にChromeルートストアから削除され、Chromeブラウザによって「信頼できない」などの証明書にフラグが付けられます

タイムライン

- 2025年9月、SSL.comからTLS証明書が発行されます。この証明書には、サーバ証明書のServerAuth EKU(ClientAuthは含みません)のみが含まれます。つまり、Webサイトまたはサーバの新しいSSL/TLS証明書は、明示的に「サーバ認証」のみを対象とします。

- 2025年10月：プログラムに連携するCA（DigiCert、Sectigoなど）は、デフォルトでサーバ専用証明書の発行を開始しました。

- 2026年5月：プログラムに合わせたCAは、クライアント認証EKU証明書の発行を停止します

- 2027年3月：Chromeルートプログラムポリシーが完全に発効

Cisco Secure Firewall製品への影響

公開CAが、発行された証明書にサーバ認証EKUのみを含めるようになると、これにより、次のCisco Secure Firewall製品のシナリオに次のような影響が及ぶ可能性があります。

- ASA、FTD、FDM、またはFMCがクライアントとして機能する場合(ISE(pxGrid)、RADIUS、LDAPS、Active DirectoryなどのIDプロバイダーや認証サーバに接続する場合など)、クライアント証明書がパブリックCAによって生成され、クライアント認証EKUが欠落していると、証明書ベースの認証が失敗する場合があります。このようなシナリオでは、認証サーバが必要なEKUなしで証明書を拒否すると、接続エラーが発生する可能性があります。

- Cisco Secure Client（以前のAnyConnect）は、証明書を使用してASAサーバまたはFTDサーバに対して認証できます。ただし、クライアント証明書がパブリックCAによって生成されたものであり、クライアント認証EKUが欠落している場合、リモートアクセスVPN(RAVPN)接続は失敗します。

- 証明書認証（RSAまたはECDSA）を使用して、FTDまたはASAがサイト間VPNトンネル（別のFTD、ASA、Ciscoルータ、またはサードパーティのVPNピアのいずれに対するものでも）を確立する場合、パブリックCAによって生成されたアイデンティティ証明書にクライアント認証EKU属性が欠落していると、トンネルに障害が発生します。これは、リモートVPNピアでは、ID証明書にクライアント認証EKUが含まれている必要があるためです。

注:pxGridを通じてFMCまたはFDMをISEと統合し、FMC/FDMにインストールされている証明書にクライアント認証EKU属性がない場合、このドキュメントおよび次のISEで提案されている回避策(FN74392)を確認し、公開証明機関によって発行された証明書の拡張キー使用制限についてIdentity Services Engineを準備します。

注:clientAuth　EKUをTLSサーバ証明書から削除することは、セキュリティを強化し、誤用を防ぐ業界全体のポリシー変更です。ほとんどのユーザにとって、目立った影響はありません。ただし、ClientAuth　EKUを利用する場合は、必要に応じて適切なタイプの証明書を取得するために予防的な手順を実行する必要があります。

該当製品

Cisco Secure Firewall製品	[Software Version]	影響を受けるシナリオ	修正
FTD	すべてのバージョン	がクライアントとして機能する場合(たとえば、ISE(pxGrid)、RADIUS、LDAPS、Active Directoryなどのアイデンティティプロバイダーや認証サーバに接続する場合)、クライアント証明書がパブリックCAによって生成され、クライアント認証EKUが欠落していると、証明書ベースの認証が失敗する可能性があります。このシナリオでは、認証サーバが必要なEKUなしで証明書を拒否すると、接続エラーが発生する可能性があります。	オプション 1クライアント認証にTLSサーバ証明書を使用している場合は、別のソースからClientAuth EKUを使用して証明書を取得する必要があります。 または オプション2: 組み合わせたEKU（ClientAuthおよびServerAuth）証明書を提供するパブリックルートCA（認証局）に切り替えます。 注：追加のオプションについては、このドキュメントの「回避策」のセクションを参照してください。
FDM	すべてのバージョン		
FMC	すべてのバージョン		
ASA	すべてのバージョン		
Cisco Secure Client（旧称AnyConnect）	すべてのバージョン	Cisco Secure Clientは、証明書を使用してASAサーバまたはFTDサーバに対して認証できます。ただし、クライアント証明書がパブリックCAによって生成され、クライアント	

		認証EKUが欠落している場合、リモートアクセスVPN(RAVPN)接続は失敗します。	
FTDまたはASA	すべてのバージョン	証明書認証（RSAまたはECDSA）を使用して、FTDまたはASAがサイト間（サイト間）VPNトンネル（別のFTD、ASA、Ciscoルータ、またはサードパーティのVPNピアのいずれに対するものでも）を確立する場合、パブリックCAによって生成されたアイデンティティ証明書にクライアント認証EKU属性が欠落していると、VPNトンネルに障害が発生します。これは、リモートVPNピアでは、ID証明書にクライアント認証EKUが含まれている必要があるためです。	

注:pxGridを通じてFMCまたはFDMをISEと統合し、FMC/FDMにインストールされている証明書にクライアント認証EKU属性がない場合、このドキュメントおよび次のISEで提案されている回避策(FN74392)を確認し、公開証明機関によって発行された証明書の拡張キー使用制限についてIdentity Services Engineを準備します。

注:clientAuth　EKUをTLSサーバ証明書から削除することは、セキュリティを強化し、誤用を防ぐ業界全体のポリシー変更です。ほとんどのユーザにとって、目立った影響はありません。ただし、ClientAuth　EKUを利用する場合は、必要に応じて適切なタイプの証明書を取得するために予防的な手順を実行する必要があります。

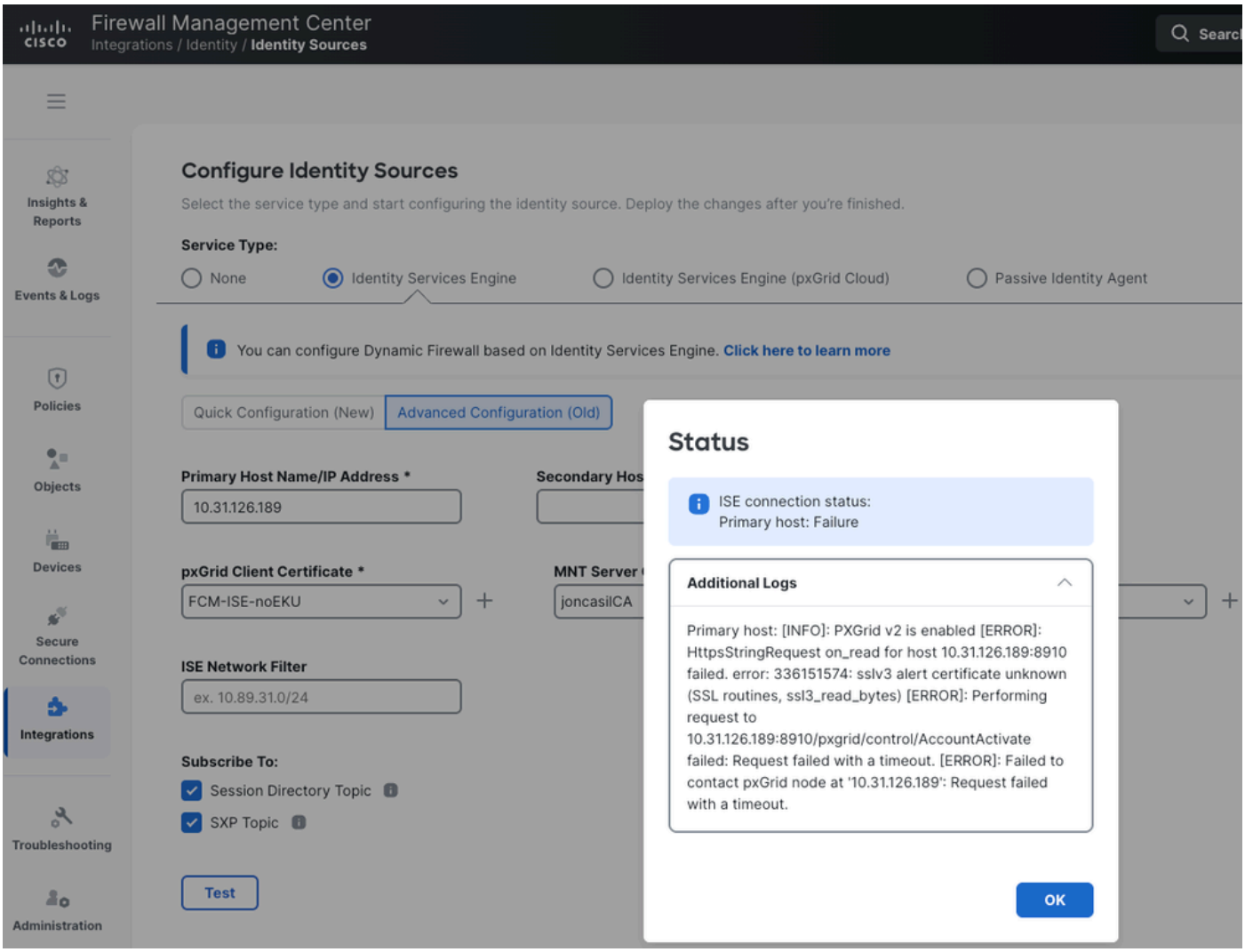
⚠ 注意:実稼働環境では、適切なEKU属性を持つ証明書を使用することを強くお勧めします。これにより、セキュリティ、互換性、および業界標準とベストプラクティスへの準拠が保証されます。EKU属性を持たない証明書は、一時的な回避策として、関連するリスクを明確に理解している場合にのみ考慮する必要があります。

問題1:FMC証明書にクライアント認証EKU属性がない場合の、FMCとISE間のpxGrid統合の問題

このシナリオでは、ISEとのpxGrid統合のためにFMCで使用される証明書にクライアント認証EKU属性がありません。その結果、ISEサーバはFMCによって提示される証明書にこの属性が存在することを予期しているため、pxGrid統合が失敗します。

トポロジ

FMC UIエラー：これは、FMCで使用される証明書に、ISEとのpxGrid統合のためのクライアント認証EKU属性が含まれていない場合に、FMCに表示されるエラーメッセージです。



FMC CLIエラー：同じエラーメッセージがFMC /var/log/messagesディレクトリにあります。

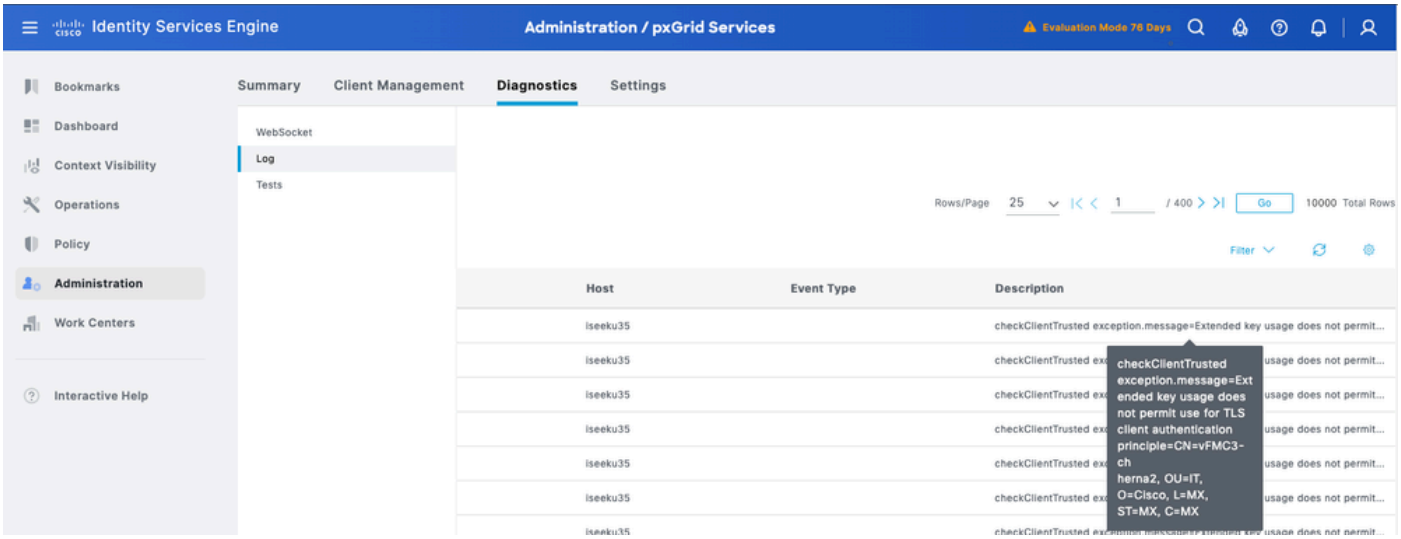
<#root>

```
HttpsStringRequest on_read for host 10.31.126.189:8910 failed. error: 336151574:

sslv3 alert certificate unknown


(SSL routines, ssl3_read_bytes)

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:HttpsEndpoint

[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService
```

```
[ERROR] pxgrid2_service was not created for 10.31.126.189. Reason - Request failed with a timeout.
```

```
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
```

ISEエラー：これは、ISEに表示されるエラーメッセージ「checkClientTrusted exception.message=Extended key usage does not permit use for TLS client authentication principal=CN=vFMC3-chherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX」です。



解決策：pxGridを介してFMCまたはFDMをISEと統合し、FMC/FDMにインストールされている証明書にクライアント認証EKU属性がない場合、このドキュメントおよび次のISEリファレンス「FN74392」および「Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates by Public Certification Grid Integration」を参照してください。

> 注:FMC pxGridクライアント証明書には、ClientAuth EKU属性を含めるか、クライアントまたはサーバのEKU属性をまったく含めないでください。

> 注:IMSではパブリックCA署名付き証明書の使用がサポートされていますが、ISE内部CA証明書を使用することをお勧めします。この通信は内部トランザクション専用であるためです。

問題 2.提示された証明書にクライアント認証のEKU属性がない、LDAPSサーバとのFTDまたはASA統合の問題

このシナリオでは、FTDまたはASAがクライアントとして機能し、証明書認証を使用してLDAPSサーバと統合します。FTDまたはASAで使用される証明書にクライアント認証EKU属性がない場合、LDAPSサーバではこの属性が証明書に含

まれている必要があるため、統合は失敗します。

トポロジ

LDAPSサーバエラー： 'TLS certificate verification: Error, unsupported certificate purpose'および'TLS trace: SSL3 alert write:fatal:unsupported certificate'

```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error in TLSv1.3 early d
ata
69ceb4f5.15b17eaa 0x7ff5522fc700 connection_get(15): got connid=1004
69ceb4f5.15b1b73f 0x7ff5522fc700 connection_read(15): checking for input on id=
1004
69ceb4f5.15b2bf05 0x7ff5522fc700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.15b4c6c3 0x7ff5522fc700 TLS certificate verification: depth: 0, err: 2
6, subject: /CN=asa-server-only,69ceb4f5.15b4e8de 0x7ff5522fc700  issuer: /CN=T
est-CA
69ceb4f5.15b4f367 0x7ff5522fc700 TLS certificate verification: Error, unsupport
ed certificate purpose
69ceb4f5.15b57df8 0x7ff5522fc700 TLS trace: SSL3 alert write:fatal:unsupported
certificate
69ceb4f5.15b5b557 0x7ff5522fc700 TLS trace: SSL_accept:error in error
69ceb4f5.15b66c36 0x7ff5522fc700 TLS: can't accept: error:1417C086:SSL routines
:tls_process_client_certificate:certificate verify failed (unsupported certific
ate purpose).
69ceb4f5.15b70391 0x7ff5522fc700 connection_read(15): TLS accept failure error=
-1 id=1004, closing
69ceb4f5.15b747ae 0x7ff5522fc700 connection_close: conn=1004 sd=15
```

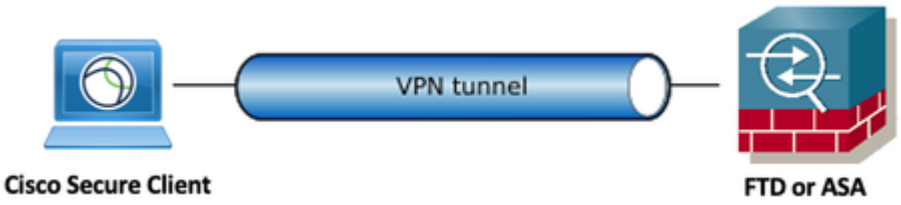
解決策：LDAPSサーバで証明書ベースの認証が正常に行われるように、FTDまたはASAが正しいID証明書（クライアント認証EKU属性を含む）を使用していることを確認するために、このドキュメントで提案されている内容を確認します。

問題3. Cisco Secure Client（以前のAnyConnect）では、クライアント証明書にClient Authentication EKU属性がない場

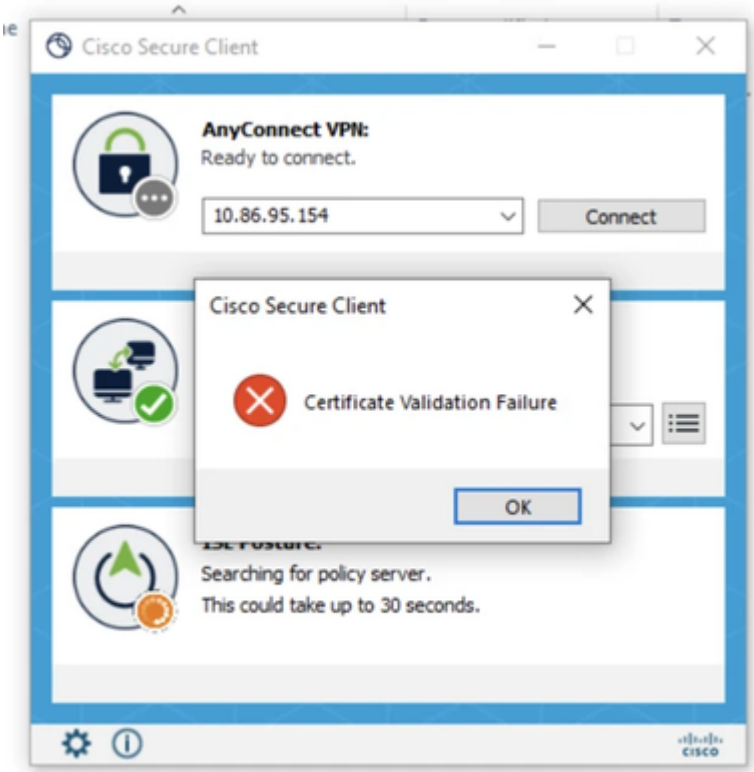
合、FTDまたはASAへの接続の問題が発生する場合があります

このシナリオでは、Cisco Secure Clientは証明書認証を使用して、FTDまたはASAへのRAVPNトンネルを確立します。ただし、クライアント証明書にクライアント認証EKU属性がない場合、ASAまたはFTDがこの属性をクライアント証明書に含める必要があるため、RAVPNセッションは失敗します。

トポロジ



Cisco Secure Clientのエラー：「Certificate Validation Failure」



Cisco Secure ClientのDARTエラー：DARTバンドル内のAnyConnectVPN.txtファイルからの次のログによって、FTD/ASAへのRAVPN証明書ベースの認証に使用される証明書がCisco Secure Clientによって拒否されたことが確認できますクライアント認証EKU属性が表示されないようにします(DARTバンドル内のAnyConnectVPN.txtファイルを見つけるには、Cisco Secure Client > AnyConnect VPN > Logs > AnyConnectVPN.txt.txtに移動します)。

<#root>

```
****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Error
Source : csc_vpnapi


Description : Function: CVerifyExtKeyUsage::compareEKUs


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\VerifyEx
Line: 330

EKU not found in certificate: 1.3.6.1.5.5.7.3.2



****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Information
Source : csc_vpnapi



Description : Function: CCertStore::GetCertificates


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\CertStor
Line: 225

Ignoring client certificate because it does not contain the required EKU extension.

 Certificate details:
Store: [Omitted Output]

****************************************
```

解決策：FTDまたはASAで証明書ベースの認証が成功するように、Cisco Secure Clientが正しい証明書（クライアント認証のEKU属性を含む）を使用していることを確認するために、このドキュメントで提示されている内容を確認します。

注：上記のDARTバンドルエラー「EKU not found in certificate: 1.3.6.1.5.5.7.3.2」では、この番号「1.3.6.1.5.5.7.3.2」がクライアント認証のEKU OIDに対応しています。

問題 4. ID証明書にクライアント認証EKU属性がない場合、証明書ベース認証を使用

したサイト間VPNトンネルは失敗します

IKEv2サイト間VPNトンネルに対する証明書ベースの認証を含むこのシナリオでは、FTD/ASA(1)がFTD/ASA(2)ピアへのトンネルを確立するために使用するID証明書に、クライアント認証EKU属性がありません。その結果、VPNトンネルを確立できません。これは、リモートピア(FTD/ASA (2))がこの属性を証明書に含める必要があるためです。

トポロジ

FTDまたはASA CLIエラー：これらは、クライアント認証EKU属性を持たないFTD/ASA(1)のID証明書をIKEv2証明書ベースの認証時に拒否する場合に、FTD/ASA(2)で発生するエラーです。

<#root>

```
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certi. Peer certificate key usage is invalid,

 subject name: CN=ASAv3.cisco.com,OU=IT,O=Cisco,C=US,unstructuredName=ASAv3.cisco.com.
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorize

Apr 09 2026 15:59:50: %ASA-3-751006: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Certificate authentication failed.  Error: Certificate authentication failed

Apr 09 2026 15:59:50: %ASA-4-750003: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Negotiation aborted due to ERROR: Auth exchange failed

Apr 09 2026 15:59:50: %ASA-4-752012: IKEv2 was unsuccessful at setting up a tunnel.  Map Tag = CMAP.  M
Apr 09 2026 15:59:50: %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All configured
Apr 09 2026 15:59:55: %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.  Map Ta
Apr 09 2026 15:59:55: %ASA-5-750001: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:Unknown IKEv2 Rece
```

注：上記の例では、FTD/ASA(2)がClientAuthとServerAuthの両方のEKU属性を含むID証明書を使用しています。

注：上記の例では、FTD/ASA(2)をルータやサードパーティの物理またはクラウドベースのVPNコンセントレータに置き換えることもできます。その後、VPNピアでは、証明書ベースの認証を正常に行うために、FTD/ASA(1)で使用される証明書にクライアント認証EKU属性が存在している必要があるため、同じ問題が解決しません。

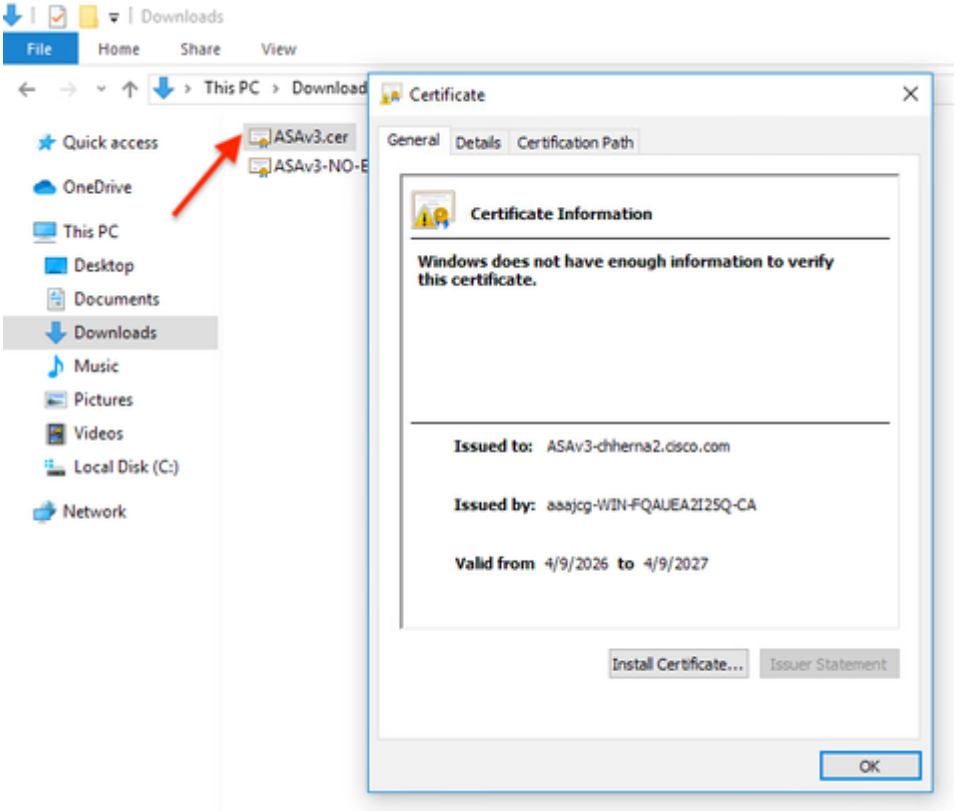
解決策：証明書ベースの認証を使用するサイト間VPNトンネルが成功する場合は、このドキュメントに記載されている推奨事項を見直して、FTD/ASA(1)が正しいID証明書（クライアント認証EKU属性を含む）を使用していることを確認します。

証明書にクライアント認証EKU属性が含まれていないかどうかを確認する手順

Windows Certificate Managerを使用した.cer証明書からのEKU属性の確認

次の手順に従い、Windows Certificate Managerを使用して.cer証明書のEKU属性を確認します。

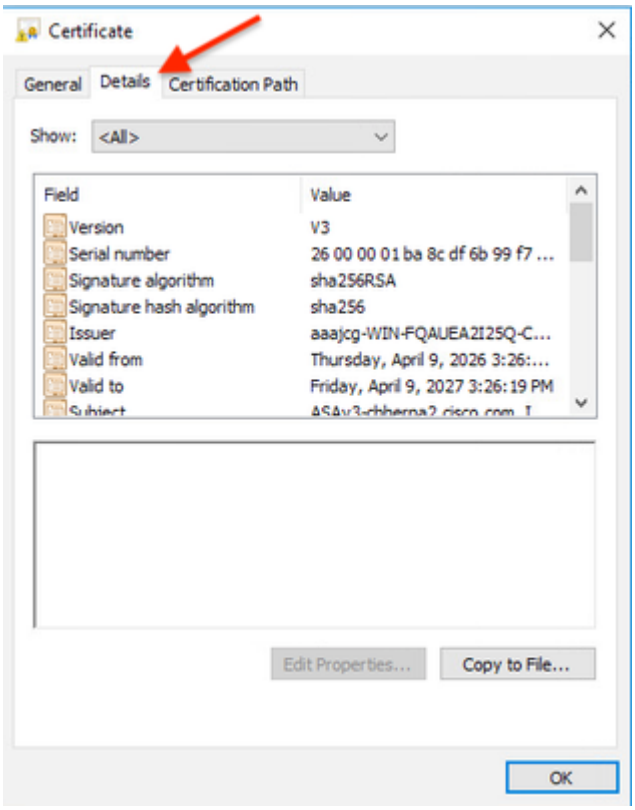
ステップ 1： .cerファイルをダブルクリックして、Windows証明書マネージャで開きます。



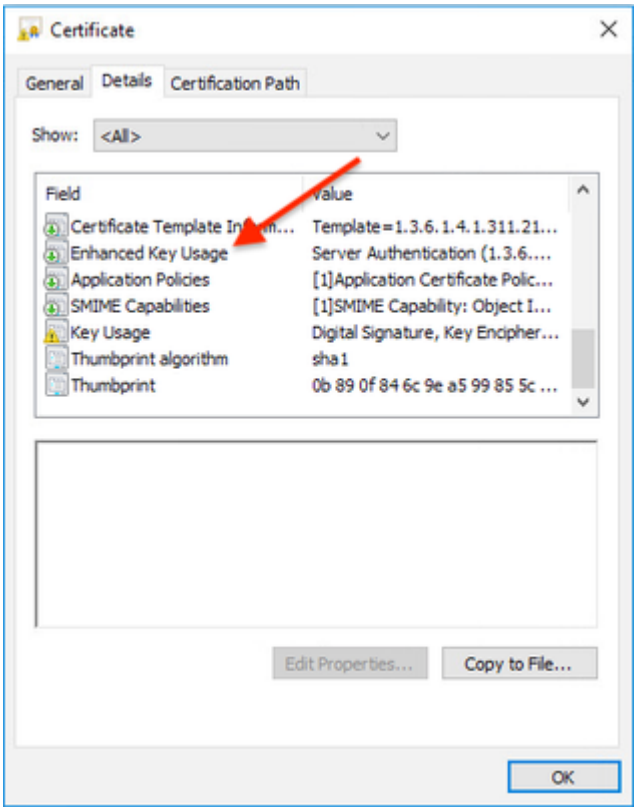
注：この方法で直接開くことができるのは.cerファイルだけです。証明書の拡張子が.pemの場合は、まず.cerまたは.crtに変更してください。

ステップ 2セキュリティ警告がある場合は処理します。セキュリティ警告のプロンプトが表示されたら、[開く]をクリックして続行します。

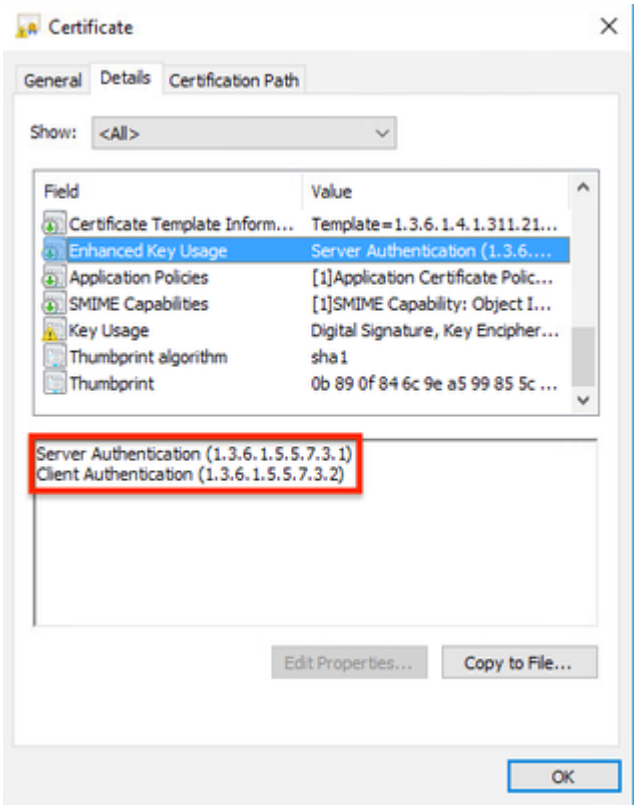
ステップ 3 [Certificate] ウィンドウで、[Details] タブをクリックします。



ステップ 4 フィールドのリストをスクロールして、[Enhanced Key Usage]（または[Extended Key Usage]）を選択します。

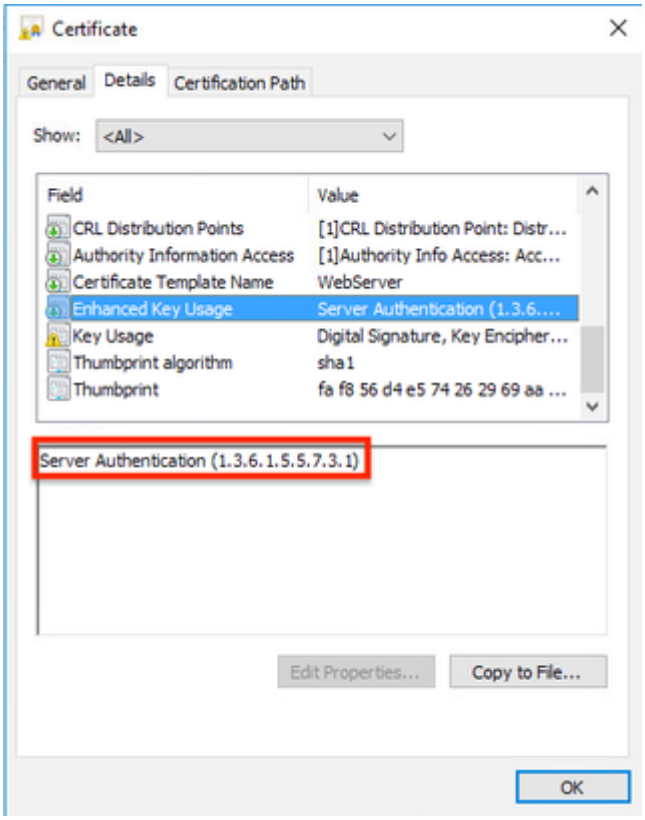


ステップ 5EKU属性を確認します。証明書にEKU値が含まれていることを示す「Server Authentication」や「Client Authentication」などのエントリが表示されることがあります。

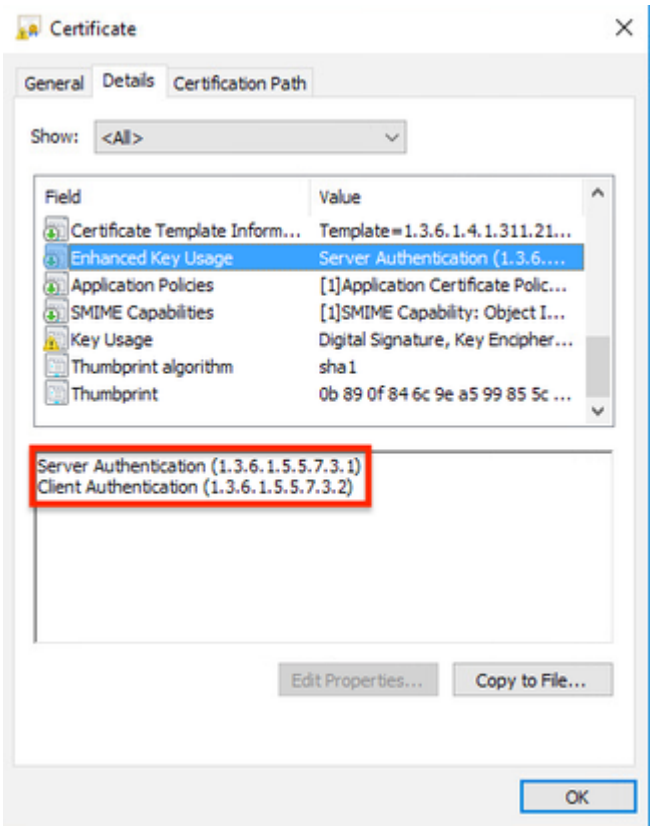


ステップ 6確認後、OKをクリックして証明書ウィンドウを閉じます。

例1：この.cer証明書にはクライアント認証EKU属性がなく、サーバ認証EKU属性のみが含まれています。



例2：この.cer証明書には、EKU属性としてサーバ認証とクライアント認証の両方が含まれています。



OpenSSLを使用したPKCS#12、PEM、および.cer証明書からのEKU属性の確認

次の手順に従って、.p12(PKCS#12)、.pem(PEM)、および.cer証明書のEKU属性を確認します。

ステップ 1： チェックする必要のある証明書を探し、.p12(PKCS#12)、.pem(PEM)、または.cer形式でエクスポートします。

.p12(PKCS#12)証明書の場合は、opensslを使用して.p12(PKCS#12)ファイルから証明書を抽出します。.p12(PKCS#12)ファイルには、秘密キー、証明書、およびCA証明書が含まれる場合があります。

次のコマンドを使用して、.p12(PKCS#12)ファイルから.pem(PEM)ファイルに（秘密キーまたはCAチェーンを使用せずに）証明書を抽出します。

```
openssl pkcs12 -in yourfile.p12 -nokeys -clcerts -out cert.pem
```

- yourfile.p12：実際のファイル名で置き換えます。
- .p12ファイルのパスワードを入力する必要がある場合があります。
- cert.pem:（秘密キーまたはCAチェーンなしで）抽出された証明書は.pem(PEM)形式です。

ステップ 2次のopensslコマンドを使用して、証明書の詳細とEKU属性を表示します。

a) .pemファイルの場合は、次のopensslコマンドを使用して、証明書の詳細とEKU属性を表示します。

```
openssl x509 -in cert.pem -text -noout
```

- cert.pem：実際のファイル名で置き換えます。

b) .cerファイルの場合は、次のopensslコマンドを使用して、証明書の詳細とEKU属性を表示します。

```
openssl x509 -in yourfile.cer -text -noout
```

- yourfile.cer：実際のファイル名で置き換えます。

ステップ 3 次に、出力のX509v3Extended Key Usageセクションを探すと、「TLS Web Server Authentication」や「TLS Web Client Authentication」などのエントリが表示され、証明書にEKU値が示されていることがあります。

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

またはEKU属性OID（オブジェクト識別子）:

```
X509v3 Extended Key Usage:
1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2
```

- サーバ認証EKU OID:1.3.6.1.5.5.7.3.1
- クライアント認証EKU OID:1.3.6.1.5.5.7.3.2

例1：この.pem(PEM)証明書にはクライアント認証EKU属性がなく、サーバ認証EKU属性のみが

含まれています。

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b7:e7:90:48:d6:f9:41:d3:54:00:01:00:00:01:b7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 27 00:31:40 2026 GMT
            Not After : Mar 26 00:31:40 2028 GMT
        Subject: C=MX, ST=MX, L=MX, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:a8:a0:ff:dd:34:73:7d:46:86:85:05:b6:0c:
                    5e:32:8c:6f:6f:88:52:03:58:63:c6:89:d8:fc:55:
                    c5:58:ba:eb:45:88:b2:21:9e:c5:d8:67:57:39:0f:
                    91:a5:41:61:fa:94:b1:ad:9e:71:26:87:b6:30:ae:
                    a7:f6:89:b1:6d:61:ce:fa:47:7f:2a:d8:e8:4d:26:
                    4f:a7:d3:eb:5a:69:16:46:71:c7:55:cf:87:b4:10:
                    96:f2:10:6b:c0:a7:3d:3c:49:9d:ee:77:8c:b5:95:
                    9b:69:81:e0:2d:a0:6e:5c:78:73:22:5a:38:d0:74:
                    38:b2:ba:e0:ab:c5:44:eb:e1:3c:52:86:b8:2a:4e:
                    37:44:9c:34:d8:d8:6c:ae:3e:df:12:57:0e:28:52:
                    57:dc:6d:62:ea:b6:ec:19:4e:90:8f:3f:2c:23:1b:
                    e2:39:f0:ba:07:08:9a:0b:97:96:05:2e:69:fe:9a:
                    b2:b2:74:9a:ba:06:25:bc:38:1c:94:87:8e:2a:dc:
                    2f:0b:a6:31:6c:bf:11:96:2a:71:b3:87:e5:f5:cb:
                    88:f1:73:cf:88:d7:30:78:24:77:7c:b7:2c:7c:83:
                    6d:69:5b:bd:d4:21:b9:ee:19:c4:02:be:7b:44:a2:
                    55:d6:b2:95:11:46:bf:db:3e:4f:9a:8c:d4:ad:8d:
                    82:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0D:8E:DA:07:6D:49:EA:51:D2:C7:EF:50:CE:CE:2B:8E:7C:DF:A6:8D
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
```

```
X509v3 Extended Key Usage:

        <--------- "EKU SECTION"


TLS Web Server Authentication


  <--------- "Server Authentication EKU Attribute Included"
    Signature Algorithm: sha256WithRSAEncryption
         2f:27:cd:95:7d:5c:40:fa:29:64:df:75:7d:7a:87:9b:b0:94:
         0e:6b:07:4d:d2:7e:83:da:03:08:f3:50:0d:5b:05:8c:1f:54:
         46:fe:53:f3:e2:d4:0a:ba:37:4f:cd:a4:49:04:74:79:09:23:
         d6:06:af:69:d2:7b:f5:bc:ec:fe:ce:e4:c9:07:31:d7:85:45:
         55:78:d3:42:45:f9:ce:cd:bf:43:53:b4:8e:4c:af:64:4b:a6:
         dc:47:d0:16:4e:73:62:fd:c8:5e:37:74:cb:68:48:29:7d:f9:
         41:b3:d1:46:56:24:83:23:5c:bd:b0:e3:7c:f9:8a:af:da:09:
         d0:c2:7d:4a:e6:24:0f:e6:fc:6e:0d:65:8c:96:8c:af:21:b2:
         7f:4b:bb:1c:17:33:b1:db:00:f3:12:e3:53:39:d0:e7:6a:48:
         4c:c6:4f:29:6f:74:ff:2d:a7:e5:ea:e8:89:fe:a4:2b:cd:e3:
         61:6a:9e:11:52:15:57:f2:b8:e8:fa:78:31:20:49:d9:50:f9:
         70:3f:1e:aa:9c:1a:bb:0b:59:66:1e:85:bd:76:e7:73:6f:ec:
         86:30:b0:dd:86:3c:b3:a0:7b:fb:b7:74:5d:38:88:82:3d:a3:
         2d:8c:a5:e4:db:37:eb:be:7f:62:bc:87:7c:35:17:32:fc:52:
         c5:d3:c5:8f
```

例2：この.pem(PEM)証明書には、クライアント認証とサーバ認証の両方のEKU属性が含まれています。

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b6:74:fc:b4:1e:99:be:7a:10:00:01:00:00:01:b6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 26 23:44:58 2026 GMT
            Not After : Mar 26 23:44:58 2027 GMT
        Subject: C=MX, ST=AD, L=AD, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:aa:67:4e:55:19:3b:38:6c:33:2e:ba:fd:19:
                    56:e7:68:f8:f7:e9:53:95:1f:53:b4:f1:ce:94:c8:
                    ca:41:f1:52:15:eb:a5:35:9f:07:95:9f:c3:8a:5e:
                    62:d6:e1:5c:04:c5:c0:27:1c:84:ed:3d:1b:42:50:
                    91:4a:a6:86:90:e0:6e:26:7e:37:fd:17:0c:2f:bb:
                    fe:58:81:ec:3b:9d:0b:fc:dd:8c:6b:dd:ab:d3:96:
                    74:23:0d:78:d7:09:53:61:f9:b0:29:c6:7c:e2:9c:
                    2f:74:30:42:0f:45:47:cd:16:59:ed:53:62:8f:60:
```

```
                    75:f8:24:f5:1f:77:fb:89:85:4b:49:ad:93:43:04:
                    6e:4a:b3:59:fc:eb:75:70:39:67:71:60:be:b3:b7:
                    86:f7:c5:53:28:1e:bf:8f:b2:52:ec:79:d6:12:b0:
                    33:9c:6d:46:7a:9c:5d:53:a5:44:24:da:4b:36:7d:
                    c2:ec:61:d7:a0:01:c3:d2:bc:0a:df:a8:f6:0c:82:
                    48:30:fb:c6:3e:4a:48:a9:01:13:f5:4e:f2:03:24:
                    38:ee:aa:d9:60:78:30:45:ed:3b:76:16:fd:7a:d3:
                    b0:16:10:28:75:fc:41:32:e6:6d:cb:c3:96:58:77:
                    9e:11:0a:9b:33:c7:92:8d:75:1f:e5:30:29:a4:a5:
                    ba:7d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DF:62:25:17:DB:72:31:D8:D2:D0:41:CB:FB:DD:00:FF:38:BD:BB
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....^..9...
...b.../ ...R...Z..d...


X509v3 Extended Key Usage:

          <-------- "EKU SECTION"


TLS Web Server Authentication, TLS Web Client Authentication


  <----- "Server & Client EKU Attributes Included"
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
            S/MIME Capabilities:
......0...+....0050...*.H..
..*.H..
    Signature Algorithm: sha256WithRSAEncryption
         3f:66:b1:35:7e:05:b4:69:f1:81:95:b8:18:90:f2:20:bd:8d:
         ff:03:5a:59:ca:02:ba:2d:1d:e0:8d:3f:63:e9:fe:71:3c:9a:
         11:15:5c:3b:fc:62:e4:cf:15:25:4c:74:5e:ad:3f:09:e9:3b:
         d5:08:95:7d:97:7a:ef:c1:16:6d:e0:7a:0b:21:81:46:bc:15:
         c3:76:8c:fe:fb:14:94:36:92:0d:3b:4a:c9:8f:6a:bd:dc:4b:
         0b:24:c3:32:35:27:e7:aa:23:95:85:e4:a9:64:71:f0:98:9e:
         33:aa:6e:bd:7c:dd:dc:4b:cf:dd:0e:a7:ea:e8:aa:61:8f:67:
         84:da:5b:be:8e:05:75:c8:eb:46:13:6f:14:4d:fe:4e:57:3c:
         29:27:cc:0b:5b:25:87:37:24:12:79:b1:c3:78:c8:94:fe:df:
         3c:77:aa:fc:f2:ee:ae:9b:ab:88:29:f9:ee:04:c2:48:5f:21:
         9e:1c:25:cc:c9:c5:9c:23:8f:af:87:76:5e:46:74:ac:73:57:
         01:ba:71:ae:46:e1:87:3c:94:6c:19:f7:fe:8e:66:9d:c7:1f:
```

```
b0:87:4b:65:e2:fc:d6:10:7c:44:57:56:5d:68:bb:df:f0:36:
0e:07:c5:8a:be:56:86:97:3d:a7:1c:8b:86:df:0b:51:b5:97:
cc:67:09:8e
```

回避策

管理者は、次のいずれかの回避策を選択できます。

オプション 1結合されたEKU証明書を提供するパブリックルートCAに切り替える

DigiCertやIdentrustなどの一部のパブリックルートCAは、代替ルートからEKUタイプ（サーバ証明書とクライアント証明書）を組み合わせた証明書を発行しますが、これはChromeルートストアには含まれない場合があります。CAプロバイダーと連携してこれらの証明書の可用性をチェックし、証明書を展開する前に、証明書を提示するサーバと、証明書を使用するクライアントの両方が、対応するルートCAを信頼していることを確認します。

このアプローチにより、Chromeルートプログラムポリシーによって強制されるクライアント認証EKUのサンセットを軽減するためにサーバソフトウェアをアップグレードする必要性が軽減されます。

次の表は、パブリックルートCAおよびEKUタイプの例を示していますが、すべてを網羅しているわけではなく、説明のみを目的としています。

CAベンダー	EKUタイプ	ルートCA	発行側/下位CA
Identrust	clientAuth +サーバ認証	Identrustパブリックセクタルート CA 1	Identrust Public Sector Server CA 1
Identrust	クライアント認証	Identrustパブリックセクタルート CA 1	TrustID RSA ClientAuth CA 2
Identrust	serverAuth（ブラウザは信頼済み）	Identrust商用ルートCA 1	HydrantIDサーバCA O1
デジタル証明書	clientAuth +サーバ認証	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2
デジタル証明書	クライアント認証	DigiCert Assured ID Root G2	DigiCert Assured IDクライアントCA G2
デジタル証明書	serverAuth（ブラウザは信頼済み）	DigiCertグローバルルート G2	DigiCertグローバルG2 TLS RSA SHA256

オプション 2現在の証明書を更新して有効期間を延長

2026年5月より前に公開ルートCAによって発行され、サーバ認証とクライアント認証の両方のEKUを持つ証明書は、その期間が満了するまで保持されます。ただし、ポリシーのサンセットが発生する前に、結合されたEKU証明書を更新することをお勧めします。

- パブリックCAポリシーと実装日は、ベンダーによって異なる場合があります。
- CAに確認し、それに応じて証明書の更新を計画します。
- 2026年3月15日以降、公開されているCA発行の証明書は200日間のみ有効です。
- 一部のパブリックCAが複合EKU証明書の発行を停止していることを考慮してください。

オプション 3プライベートPKIに移行し、組み合わせたEKU（サーバおよびクライアント）証明書を発行する

Private Public Key Infrastructure(PKI)への移行の実現可能性を評価し、EKUを組み合わせた1つの証明書（必要なEKUを持つサーバ証明書とクライアント証明書）を発行するようにプライベートCAを設定します。

証明書を発行または展開する前に、証明書を提示するサーバと、証明書を使用するすべてのクライアントの両方が、対応するルートCAを信頼していることを確認してください。

オプション 4.クライアント認証EKUのみを使用して、一般に信頼されている証明書を取得する

SSL.comなどの一部のCAは、専用のクライアント認証証明書を提供します。 これらはTLS証明書とは別のもので、通常はエンタープライズ認証に使用されます。

⚠ 注意:実稼働環境では、適切なEKU属性を持つ証明書を使用することを強くお勧めします。これにより、セキュリティ、互換性、および業界標準とベストプラクティスへの準拠が保証されます。EKU属性を持たない証明書は、一時的な回避策として、関連するリスクを明確に理解している場合にのみ考慮する必要があります。

よく寄せられる質問（FAQ）

Q1.プライベートPKIを使用する場合、この点を考慮する必要がありますか。

A:プライベートCAによって適用されるポリシーは、各組織によって決定されます。証明書からクライアント認証EKU属性を削除するなど、プライベートCAが同じ発行基準を採用している場合は、このドキュメントで説明するガイドラインが適用されます。

Q2.既存の証明書を引き続き使用できますか。

A：はい。EKUを組み合わせた有効な証明書を有効期限まで使用できます。

Q3. FMC/FDMにインストールされている証明書にクライアント認証EKU属性がない場合、pxGridを使用してFMCまたはFDMをISEと統合するにはどのようなオプションを使用できますか。

A：このドキュメントで提示されている回避策に加えて、次のISEリファレンスを確認することを強くお勧めします。

- フィールド通知： FN74392 - Cisco Identity Services Engine: 2026年5月に開始されるパブリックCAクライアント認証EKU変更からのセキュア通信への影響 – 回避策を提供
- 公開されている証明機関によって発行された証明書のキーの拡張使用制限に対するIdentity Services Engineの準備

注:IMSではパブリックCA署名付き証明書の使用がサポートされていますが、ISE内部CA証明書を使用することをお勧めします。この通信は内部トランザクション専用であるためです。

Q4.「クライアント認証」EKUとは何ですか。また、証明書に含まれていたのはなぜですか。

A: 「クライアント認証」EKUは、クライアントがサーバへの認証に使用できる証明書を示します。一部のCAでは、以前はデフォルトでTLS証明書に含まれていましたが、通常のWebサイトセキュリティには必要とされていませんでした。

質問5現在のTLS証明書の「Extended Key Usage」の下に「Client Authentication」と表示されています。今は無効ですか？

A：いいえ。引き続き有効です。すぐに交換する必要はありません。更新すると、新しい証明書にはclientAuth EKUが含まれなくなります。

Q6証明書にclientAuth EKUが含まれているかどうかを確認するにはどうすればよいですか。

A:OpenSSL、PowerShell、またはGUIのツールを使用して証明書の詳細を調べ、拡張キー使用法の拡張を確認できます。

Q7.それでも、クライアント認証EKUのみを含む、一般に信頼されている証明書を取得できます

か。

A: SSL.comなどの一部のCAは、専用のクライアント認証証明書を提供します。 これらはTLS証明書とは別のもので、通常はエンタープライズ認証に使用されます。

Q8これは、他のEKUまたは証明書タイプ（コード署名、電子メールなど）に影響しますか。

A：いいえ、この変更はTLSサーバ証明書に固有です。コード署名と電子メール証明書には、独自のEKU要件があります。

Q9.この変更に関する正式な要件はどこで確認できますか。

A: Google Chromeルートプログラムポリシーには、TLSサーバ証明書でのclientAuth EKUの禁止に関するガイドラインが記載されています。

Q10.クライアントおよびサーバのEKU属性のない証明書を実稼働環境で使用しても安全ですか。

A：実稼働環境では、適切なEKU属性を持つ証明書を使用することを強くお勧めします。これにより、セキュリティ、互換性、および業界標準とベストプラクティスへの準拠が保証されます。EKU属性を持たない証明書は、一時的な回避策として、関連するリスクを明確に理解している場合にのみ考慮する必要があります。

関連情報

- 詳細については、Cisco Technical Assistance Center(TAC)にお問い合わせください。 有効なサポート契約が必要です。シスコワールドワイドサポートの連絡先です。
- Cisco Support & Downloads:Cisco Technical Support & Downloads

関連するバグ

- CSCwt94492 ENH:FMCは、pxGrid統合に使用されるクライアント証明書にクライアント認証EKU属性が含まれることを検証する必要があります
- CSCwt94509 ENH:pxGrid統合に使用するクライアント証明書にクライアント認証EKU属性が必要であることを示すメッセージがFMCに表示されます

- CSCwt61767 2026年5月EKUサーバのみの変更：EKUが不適切な場合はASA設定に関する警告を発行してください

- CSCws83036 EKU:ISEでのClientAuth EKU適用のインパクトアセスメント

Cisco ISEリファレンス

- フィールド通知： FN74392 - Cisco Identity Services Engine: 2026年5月に開始されるパブリックCAクライアント認証EKU変更からのセキュア通信への影響 – 回避策を提供

- 公開されている証明機関によって発行された証明書のキーの拡張使用制限に対するIdentity Services Engineの準備

外部参照

- Chromeルートプログラムポリシー

- Identrustポータル

- SSL - TLSサーバ証明書からのクライアント認証EKUの削除 – 知っておくべきこと

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。