

ISEでのTLS/SSL証明書の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[サーバ証明書](#)

[ISE証明書](#)

[システム証明書](#)

[信頼できる証明書ストア](#)

[基本タスク](#)

[自己署名証明書の生成](#)

[自己署名証明書の更新](#)

[信頼できる証明書のインストール](#)

[CA署名付き証明書のインストール](#)

[証明書と秘密キーのバックアップ](#)

[トラブルシューティング](#)

[証明書の有効性の確認](#)

[証明書の削除](#)

[サブリカントが802.1x認証でISEサーバ証明書を信頼しない](#)

[ISE証明書チェーンは正しいが、エンドポイントが認証中にISEサーバ証明書を拒否する](#)

[よく寄せられる質問 \(FAQ\)](#)

[ISEが証明書がすでに存在するという警告をスローした場合の対処方法](#)

[ISEのポータルページが信頼できないサーバによって表示されることを示す警告がブラウザで表示されるのはなぜですか。](#)

[無効な証明書が原因でアップグレードが失敗した場合の対処方法](#)

[関連情報](#)

概要

このドキュメントでは、Cisco ISEのTLS/SSL証明書、ISE証明書の種類と役割、一般的なタスクの実行方法とトラブルシューティング、およびFAQへの回答について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

1. Cisco Identity Services Engine (ISE)
2. さまざまなタイプのISEおよびAAA導入を説明するために使用される用語。
3. RADIUSプロトコルとAAAの基礎
4. SSL/TLSおよびx509証明書

5. Public Key Infrastructure(PKI)の基本

使用するコンポーネント

このドキュメントの情報は、Cisco ISEリリース2.4 ~ 2.7のソフトウェアとハードウェアのバージョンに基づくものです。ISEのバージョン2.4から2.7までを対象としていますが、特に記載のない限り、他のISE 2.xソフトウェアリリースと類似または同一である必要があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

サーバ証明書

サーバ証明書は、サーバによって使用され、サーバのIDをクライアントに提示して信頼性を確保し、安全な通信チャネルを提供します。これらは、自己署名（サーバが自身に証明書を発行する場所）または認証局（組織の内部または有名なベンダーから）によって発行されます。

サーバ証明書は通常、サーバのホスト名またはFQDN（完全修飾ドメイン名）に対して発行されますが、ワイルドカード証明書(*.domain.com)。通常、発行先のホスト、ドメイン、またはサブドメインは、[Common Name(CN)]フィールドまたは[Subject Alternative Name(SAN)]フィールドに表示されます。

ワイルドカード証明書は、ワイルドカード表記（ホスト名の代わりにアスタリスクを使用）を使用して、同じ証明書を組織内の複数のホストで共有できるSSL証明書です。たとえば、ワイルドカード証明書のサブジェクト名のCN値またはSAN値は次のようになります *.company.com このドメインの任意のホストを保護するために使用できます server1.com、 server2.com,等。

証明書は通常、公開キー暗号化または非対称暗号化を使用します。

- 公開キー：公開キーは、いずれかのフィールドの証明書に存在し、デバイスが公開キーとの通信を試みると、システムによって公開キーが共有されます。
- 秘密キー：秘密キーはエンドシステムに対して秘密で、公開キーとペアになっています。公開キーで暗号化されたデータは、特定のペア化された秘密キーでのみ復号化できます。その逆も同様です。

ISE証明書

Cisco ISEは、パブリックキーインフラストラクチャ(PKI)に依存して、エンドポイント、ユーザ、管理者などとのセキュアな通信や、マルチノード環境におけるCisco ISEノード間のセキュアな通信を提供します。PKIは、x.509デジタル証明書を使用して、メッセージの暗号化と復号化のための公開キーを転送し、ユーザおよびデバイスから提示される他の証明書の信頼性を検証します。Cisco ISEには、通常使用される証明書のカテゴリが2つあります。

- システム証明書：クライアントに対してCisco ISEノードを識別するサーバ証明書です。各Cisco ISEノードには独自のローカル証明書があり、それぞれのローカル証明書はそれぞれの秘密キーとともにノードに保存されます。
- 信頼できる証明書ストア証明書：これは、さまざまな目的のためにISEに提示される証明書を検証するために使用される認証局(CA)証明書です。証明書ストア内のこれらの証明書は、プライマリ管理ノードで管理され、分散Cisco ISE環境の他のすべてのノードに複製されます。証明書ストアには、BYODを目的としたISEの内部認証局(CA)によってISEノード用に生成された証明書も含まれています。

システム証明書

システム証明書は、1つ以上のロールに使用できます。それぞれの役割は異なる目的を果たします。次に各役割について説明します。

- [Admin]:443(Admin GUI)を介したすべての通信のセキュリティ保護、およびレプリケーションに使用します。また、ここに記載されていないポートや使用状況に対しても使用します。
- ポータル：これは、集中型Web認証(CWA)ポータル、ゲスト、BYOD、クライアントプロビジョニング、ネイティブサブリカントプロビジョニングポータルなどのポータルを介したHTTP通信を保護するために使用されます。各ポータルは、ポータルグループタグ(デフォルトは[Default Portal Group Tag])にマッピングする必要があります。このタグは、特定のタグが付けられた証明書を使用するようにポータルに指示します。証明書の[Edit]オプションの[Portal Group Tag name]ドロップダウンメニューでは、新しいタグを作成したり、既存のタグを選択したりできます。
- EAP:802.1x認証のためにクライアントに提示される証明書を指定する役割です。証明書は、EAP-TLS、PEAP、EAP-FASTなどのほぼすべての可能なEAP方式で使用されます。PEAPやFASTなどのトンネリングEAP方式では、Transport Layer Security(TLS)を使用してクレデンシャル交換を保護します。クライアントのクレデンシャルは、このトンネルが確立されてセキュアな交換が行われるまで、サーバに送信されません。
- RADIUS DTLS：このロールは、ネットワークアクセスデバイス(NAD)とISE間のRADIUSトラフィックを暗号化するためのDTLS接続(UDP経由のTLS接続)に使用する証明書を指定します。この機能を使用するには、NADがDTLS暗号化対応である必要があります。
- SAML：サーバ証明書は、SAML Identity Provider(IdP)との通信を保護するために使用されます。SAML用に指定された証明書は、Admin、EAP認証などのその他のサービスには使用できません。
- ISEメッセージングサービス：2.6以降、ISEは従来のSyslogプロトコルの代わりにISEメッセージングサービスを使用してデータをログに記録します。これは、この通信を暗号化するために使用されます。
- PxGrid：この証明書は、ISE上のPxGridサービスに使用されます。

ISEをインストールすると、Default Self-Signed Server Certificate. デフォルトでは、これはEAP認証、Admin、Portal、およびRADIUS DTLSに割り当てられています。これらのロールを内部CAまたは既知のCA署名付き証明書に移動することをお勧めします。

Friendly Name	Used By	Portal group tag	Valid From	Expiration Date
OU=Certificate Services System Certificate, CN=hongkongise riverdale local#Certificate Services Endpoint Sub CA - hongkongise#00002	pxGrid	hongkongise riverdale local	Mon, 13 Apr 2020	Sun, 14 Apr 2030
OU=ISE Messaging Service, CN=hongkongise riverdale local#Certificate Services Endpoint Sub CA - hongkongise#00001	ISE Messaging Service	hongkongise riverdale local	Mon, 13 Apr 2020	Sun, 14 Apr 2030
Default self-signed saml server certificate - CN=SAML_hongkongise riverdale local	SAML	SAML_hongkongise riverdale local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
Default self-signed server certificate	Default Portal Certificate Group	hongkongise riverdale local	Tue, 14 Apr 2020	Wed, 14 Apr 2021

ヒント: ISEサーバのFQDNアドレスとIPアドレスの両方がISEシステム証明書のSANフィールドに追加されていることを確認することをお勧めします。一般に、Cisco ISEでの証明書認証が証明書駆動検証機能の小さな違いによる影響を受けないようにするため、ネットワークに導入されているすべてのCisco ISEノードで小文字のホスト名を使用します。

注: ISE証明書の形式は、Privacy Enhanced Mail (PEM) または Distinguished Encoding Rules (DER) である必要があります。

信頼できる証明書ストア

認証局の証明書は、次の場所に保存する必要があります。 Administration > System > Certificates > Certificate Store または IPv6 アドレスを Trust for client authentication ユースケースを使用して、ISE がこれらの証明書を使用して、エンドポイント、デバイス、または他の ISE ノードによって提示される証明書を検証することを確認します。

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2053
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2038
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA ...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Sun, 9 Aug 2099
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 2033
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034
Default self-signed server certificate	Enabled	Endpoints Infrastructure	5E 95 93 55 00 00 ...	hongkongise riverdale local	hongkongise riverdale local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
DigCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigCert Global Root CA	DigCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 2031
DigCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 0B...	DigCert High Assurance ...	DigCert High Assurance ...	Fri, 10 Nov 2006	Mon, 10 Nov 2031
DigCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C...	DigCert SHA2 High Assu...	DigCert High Assurance ...	Tue, 22 Oct 2013	Sun, 22 Oct 2028
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 00 ...	HydrantID SSL ICA G2	QuoVads Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023
QuoVads Root CA 2	Enabled	Cisco Services	05 09	QuoVads Root CA 2	QuoVads Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wed, 16 Jul 2036
VerSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VerSign Class 3 Public Pr...	VerSign Class 3 Public Pr...	Wed, 8 Nov 2006	Wed, 16 Jul 2036
VerSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VerSign Class 3 Secure ...	VerSign Class 3 Public Pr...	Mon, 8 Feb 2010	Fri, 7 Feb 2020

基本タスク

証明書には有効期限があり、取り消したり、ある時点で交換を要求したりできます。ISEサーバ証明書の期限が切れると、新しい有効な証明書に置き換えない限り、重大な問題が発生する可能性があります。

注：拡張認証プロトコル(EAP)に使用される証明書の有効期限が切れると、クライアントはISE証明書を信頼しなくなるため、クライアント認証が失敗する可能性があります。ポータルに使用される証明書の期限が切れると、クライアントとブラウザはポータルへの接続を拒否できます。管理使用証明書の期限が切れると、リスクはさらに大きくなり、管理者はISEにログインできなくなり、分散導入は本来の機能を停止する可能性があります。

自己署名証明書の生成

新しい自己署名証明書を生成するには、Administration > System > Certificates > System Certificates.ポリシーの横の [レポート (Report)] Generate Self Signed Certificate.

The screenshot shows the Cisco ISE Administration interface. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NA. Under Certificates, there are options for Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs'. Action buttons include Edit, Generate Self Signed Certificate (highlighted), Import, Export, Delete, and View. A table lists certificates with columns: Friendly Name, Used By, Portal group tag, and Issued To. One certificate is shown with the friendly name 'hongkongise' and a detailed description: 'OU=Certificate Services System Certificate, CN=hongkongise.riverdale.local#Certificate Services Endpoint Sub CA - hongkongise#00002'. The 'Used By' column shows 'pxGrid' and the 'Issued To' column shows 'hongkongise'.

このリストでは、[自己署名証明書の生成(Generate Self Signed Certificate)]ページのフィールドについて説明します。

自己署名証明書の設定フィールド名の使用方法のガイドライン：

- ノードの選択： (必須) システム証明書の生成に必要なノード。
- CN: (SANが指定されていない場合は必須) デフォルトでは、CNは自己署名証明書が生成されるISEノードのFQDNです。
- 組織単位(OU)：組織単位の名前 (例：エンジニアリング)。
- [組織(O)(Organization (O))]：組織名 (例：Cisco)。
- City (L): (省略形は使用しないでください) City name, example, San Jose.
- 都道府県(ST): (省略形を使用しない) 都道府県名 (例：California)。
- [国(C)(Country (C))]：国名2文字のISO国番号が必要です。たとえば、米国などです。
- SAN：証明書に関連付けられているIPアドレス、DNS名、またはUniform Resource Identifier(URI)。
- [Key Type]：公開キーの作成に使用するアルゴリズム (RSAまたはECDSA) を指定します。
- Key Length：公開キーのビットサイズを指定します。これらのオプションはRSA 512 1024 2048 4096で使用でき、これらのオプションはECDSA 256 384で使用できます。
- [署名するダイジェスト(Digest to Sign With)]：ハッシュアルゴリズムとしてSHA-1またはSHA-256のいずれかを選択します。

- [Certificate Policies] : 証明書が準拠する必要がある証明書ポリシーOIDまたはOIDのリストを入力します。OIDを区切るには、カンマまたはスペースを使用します。
- [Expiration TTL] : 証明書が期限切れになるまでの日数を指定します。
- [Friendly Name] : 証明書のわかりやすい名前を入力します。名前が指定されていない場合、Cisco ISEは自動的に次の形式で名前を作成します。値は次のとおりです。 は、一意の5桁の番号です。
- [Allow Wildcard Certificates] : 自己署名ワイルドカード証明書(サブジェクト内の任意のCNにアスタリスク(*)を含む証明書、およびSAN内のDNS名を生成するには、このチェックボックスをオンにします。たとえば、SANに割り当てられるDNS名は次のようになります。
*.domain.com.
- 使用法 : このシステム証明書を使用する必要があるサービスを選択します。使用可能なオプションは次のとおりです。

[管理 (Admin)]EAP AuthenticationRADIUS DTLSpXGridSAMLポータル

The screenshot displays the 'Generate Self Signed Certificate' configuration page in the Cisco Identity Services Engine (ISE) Administration console. The interface includes a navigation menu on the left and a main configuration area on the right.

Navigation Menu:

- System
 - Identity Management
 - Network Resources
 - Device Portal Management
 - pxGrid Services
 - Feed Service
 - Threat Centric NAC
- Deployment
- Licensing
- Certificates**
 - Logging
 - Maintenance
 - Upgrade
 - Backup & Restore
 - Admin Access
 - Settings

Generate Self Signed Certificate Configuration:

- * Select Node: hongkongise
- Subject**
 - Common Name (CN): SFODNS
 - Organizational Unit (OU): Security
 - Organization (O): IT
 - City (L): Kolkata
 - State (ST): West Bengal
 - Country (C): IN
- Subject Alternative Name (SAN)**: IP Address, 10.127.196.248
- * Key type: RSA
- * Key Length: 2048
- * Digest to Sign With: SHA-256
- Certificate Policies: (Empty field)

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSF Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Subject Alternative Name (SAN) IP Address 10.127.196.248

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

Certificate Policies

* Expiration TTL 10 years

Friendly Name

Allow Wildcard Certificates

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Submit Cancel

注:RSAとECDSAの公開キーは、同じセキュリティレベルに対して異なるキー長を持つことができます。パブリックCA署名付き証明書を取得する場合、またはFIPS準拠のポリシー管理システムとしてCisco ISEを導入する場合は、[2048]を選択します。

自己署名証明書の更新

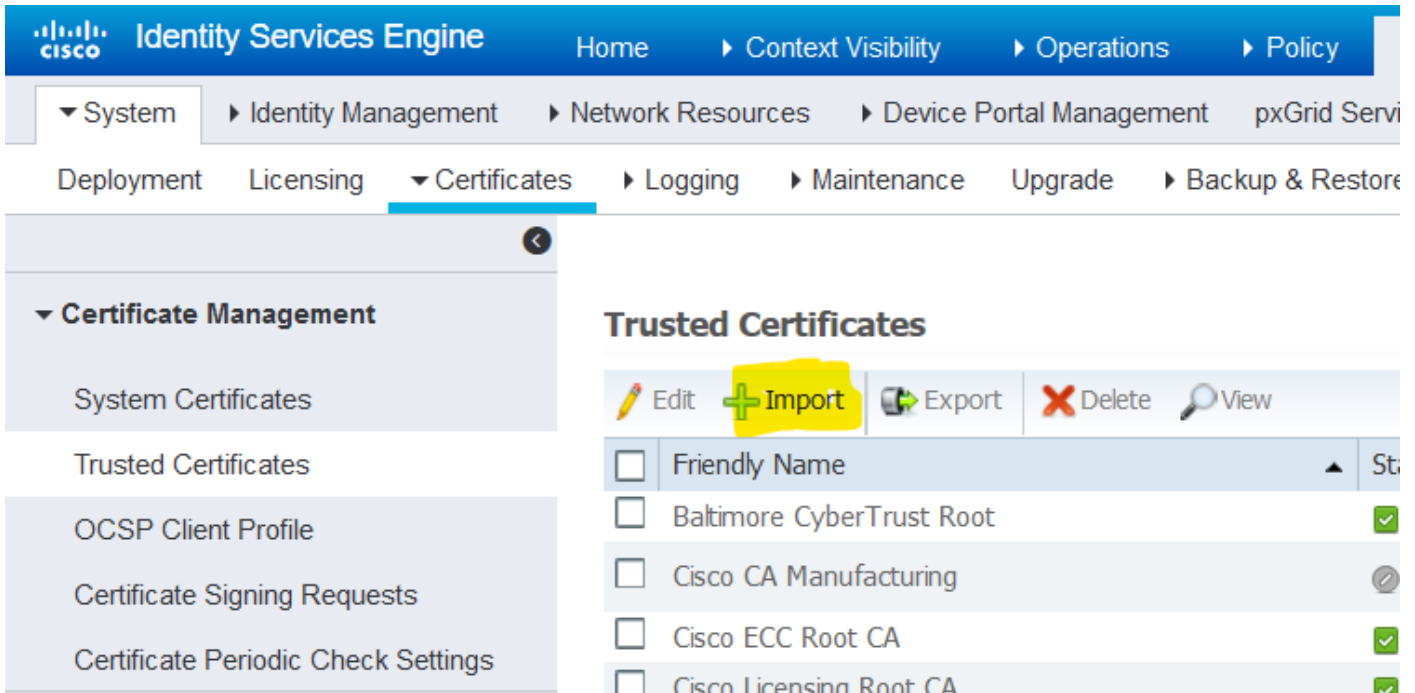
存在する自己署名証明書を表示するには、Administration > System > Certificates > System Certificates ISEコンソールで行います。同じISEサーバFQDNに指定されている場合は、[Issued To]と[Issued By]を持つ証明書は自己署名証明書です。この証明書を選択し、Edit.

通常の Renew Self Signed Certificate をチェックし、Renewal Period ボックスに入力し、必要に応じて [Expiration TTL] を設定します。最後に、 Save.

信頼できる証明書のインストール

ルートCA、中間CA、または信頼に必要なホストからBase 64でエンコードされた証明書を取得します。

1. ISEノードにログインし、 Administration > System > Certificate > Certificate Management > Trusted Certificates をクリックし、 Import,以下の図に、出力例を示します。



2.次のページで、取得したCA証明書を（前述と同じ順序で）アップロードします。追跡を続けるために、証明書の目的を説明する分かりやすい名前と説明を割り当てます。

必要に応じて、次の横のチェックボックスをオンにします。

- Trust for authentication within ISE : これは、同じ信頼できるCA証明書が信頼できる証明書ストアにロードされている場合に、新しいISEノードを追加することです。
- [Trust for client authentication and Syslog] : 証明書を使用して、EAPを使用してISEに接続するエンドポイントの認証や、セキュアSyslogサーバの信頼を行うには、これを有効にします。
- Trust for authentication of Cisco Services : これは、フィードサービスなどの外部シスコサービスを信頼する場合にのみ必要です。

3.最後に、 Submit.これで、証明書が信頼できるストアに表示され、すべてのセカンダリISEノード（導入環境の場合）に同期される必要があります。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSF Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Import a new Certificate into the Certificate Store

* Certificate File CA certificate.cer

Friendly Name

Trusted For:

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

CA署名付き証明書のインストール

ルートCAおよび中間CA証明書が信頼できる証明書ストアに追加されると、証明書署名要求 (CSR)を発行し、CSRに基づいて署名された証明書をISEノードにバインドできるようになります。

1.これを行うには、 Administration > System > Certificates > Certificate Signing Requests をクリックし、 **Generate Certificate Signing Requests (CSR)** CSRを生成します。

2.表示されるページの[Usage]セクションで、ドロップダウンメニューから使用するロールを選択します。

証明書が複数のロールに使用されている場合は、[Multi-Use]を選択します。証明書が生成されてからも、必要に応じてロールを変更できます。ほとんどの場合、証明書は[Used For]ドロップダウンで[Multi-use]に設定できます。これにより、すべてのISE Webポータルで証明書を使用できるようになります。

3. ISEノードの横にあるチェックボックスをオンにして、証明書を生成するノードを選択します。

4.ワイルドカード証明書のインストールまたは生成を目的とする場合は、 **Allow Wildcard Certificates** ボックス。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:


ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - This is not a signing request, but an ability to generate a brand new Messaging certificate.

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for  You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).


Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input type="checkbox"/> hongkongise	hongkongise#Multi-Use

Usage

Certificate(s) will be used for  You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input type="checkbox"/> hongkongise	hongkongise#Multi-Use

5. ホストまたは組織の詳細 (組織単位、組織、都市、州、および国) に基づいてサブジェクト情報を入力します。

6. これを完了するには、Generate をクリックし、Export ポップアップが表示されます。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

▼ Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

▶ Certificate Authority

hongkongise hongkongise#Multi-Use

Subject

Common Name (CN) \$FQDN\$ ⓘ

Organizational Unit (OU) Security ⓘ

Organization (O) IT ⓘ

City (L) Kolkata

State (ST) West Bengal

Country (C) IN

Subject Alternative Name (SAN) IP Address 10.127.196.248 - + ⓘ

* Key type RSA ⓘ

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

Certificate Policies

Generate Cancel

Country (C) IN

Subject Alternative Name (SAN) ⓘ

- DNS Name
- IP Address
- Uniform Resource Identifier
- Directory Name

* Key type RSA

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

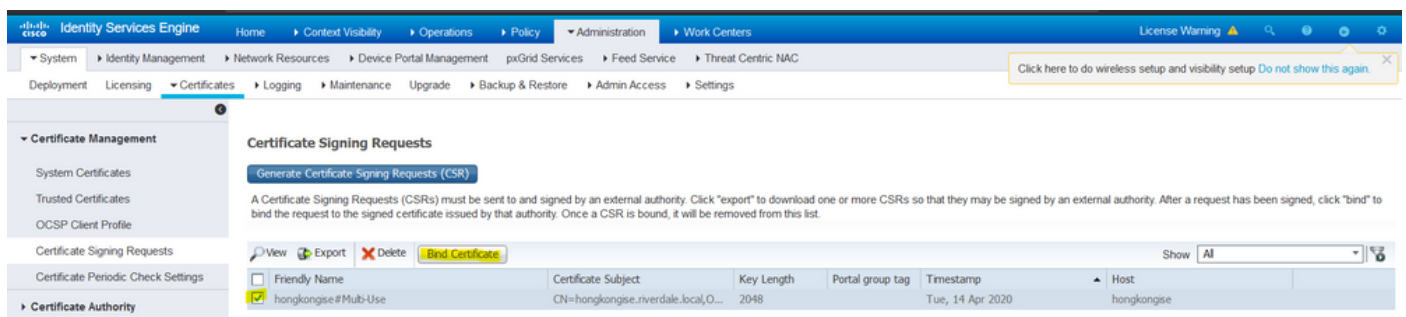
これにより、作成したばかりのBase 64でエンコードされたCertificate Request (CSR ; 証明書要求) 要求がダウンロードされます。このPEMファイルは、署名のためにCAに送信し、結果として得られる署名付き証明書CERファイル (Base 64でエンコード) を取得する必要があります。

注:[CN]フィールドの下で、ISEはノードのFQDNを自動的に入力します。

注:ISE 1.3および1.4では、少なくともpxGridを使用するために2つのCSRを発行する必要があります。1つはpxGrid専用で、もう1つは残りのサービス専用です。2.0以降では、これらはすべて1つのCSRに対して行われます。

注：証明書がEAP認証に使用される場合、Windowsサブリカントはサーバ証明書を拒否するため、「*」記号を[Subject CN]フィールドに含めることはできません。サブリカントでValidate Server Identityが無効になっている場合でも、*がCNフィールドにあるとSSLハンドシェイクが失敗する可能性があります。代わりに、汎用FQDNをCNフィールドで使用し、*.domain.com [SAN DNS Name]フィールドで使用できます。一部の認証局(CA)は、CSRにワイルドカード(*)が存在しない場合でも、証明書のCNにワイルドカードを自動的に追加できます。このシナリオでは、このアクションを防ぐために特別な要求を発行する必要があります。

7.証明書がCAによって署名された(ビデオに示すようにCSRから生成された、[Microsoft CAを使用している場合](#)はここ)場合は、ISE GUIに戻り、[Administration] > [System] > [Certificates] > [Certificate Management] > [Certificate Signing Request] に移動し、前に作成したCSRの横のチェックボックスをオンにして、[Bind Certificate] ボタンをクリックします。



The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The navigation pane on the left includes 'Certificate Management' with sub-items like 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', 'Certificate Periodic Check Settings', and 'Certificate Authority'. The main content area is titled 'Certificate Signing Requests' and contains a 'Generate Certificate Signing Requests (CSR)' button. Below this, there is a table of existing CSR requests. The table has columns for 'Friendly Name', 'Certificate Subject', 'Key Length', 'Portal group tag', 'Timestamp', and 'Host'. One entry is shown with a checked checkbox in the 'Friendly Name' column.

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/> hongkongse# Multi-Use	CN=hongkongse.nverdale.local,O=...	2048		Tue, 14 Apr 2020	hongkongse

8.次に、受信した署名付き証明書をアップロードし、ISEのフレンドリ名を指定します。次に、証明書の必要に応じて、[Usage]の横にあるボックス ([Admin]、[EAP authentication]、[Portal]など) を選択し、Submit次の図に示すように、

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Bind CA Signed Certificate

* Certificate File certnew(1).cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

* Portal group tag ⓘ

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

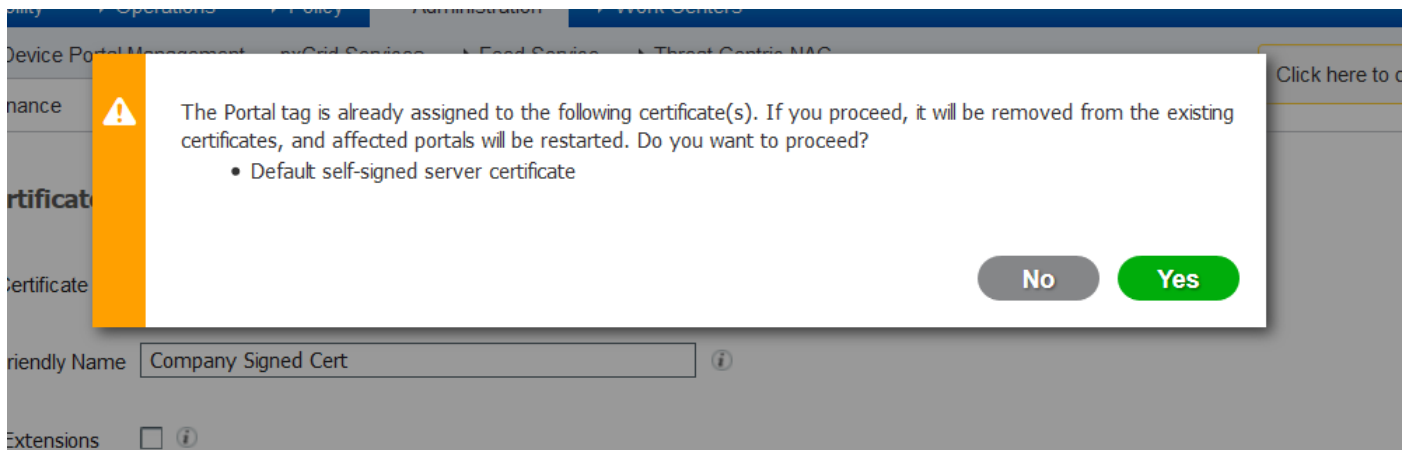
この証明書に管理者ロールが選択されている場合、ISEノードはサービスを再起動する必要があります。VMに割り当てられたバージョンとリソースによっては、10 ~ 15分かかります。アプリケーションのステータスを確認するには、ISEコマンドラインを開き、`show application status ise` コマンドが表示されない場合もあります。

Warning dialog box:

Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

Friendly Name ⓘ



証明書のインポート時に管理者ロールまたはポータルロールが選択された場合は、ブラウザの管理者ページまたはポータルページにアクセスしたときに新しい証明書が配置されていることを確認できます。ブラウザでロックシンボルを選択し、証明書の下で、パスは完全なチェーンが存在し、マシンによって信頼されていることを確認します。チェーンが正しく構築されていて、証明書チェーンがブラウザによって信頼されている限り、ブラウザは新しい管理者またはポータル証明書を信頼する必要があります。

注：現在のCA署名付きシステム証明書を更新するには、新しいCSRを生成し、同じオプションで署名付き証明書をバインドします。アクティブになる前に新しい証明書をISEにインストールすることは可能なので、古い証明書が期限切れになる前に新しい証明書をインストールすることを計画します。古い証明書の有効期限と新しい証明書の開始日の間のこの重複期間は、証明書を更新し、ダウンタイムがほとんどまたはまったくない状態で交換を計画する時間を提供します。開始日が古い証明書の失効日より前である新しい証明書を取得します。この2つの日付の間の期間が移行期間です。新しい証明書が有効な日付範囲に入ったら、必要なプロトコル(Admin/EAP/Portal)を有効にします。Admin usageが有効になっている場合は、サービスが再起動されることに注意してください。

ヒント：管理者証明書とEAP証明書には社内CAを使用し、ゲスト/スポンサー/ホットスポット/その他のポータルには公開署名証明書を使用することをお勧めします。その理由は、ユーザまたはゲストがネットワークに接続し、ISEポータルがゲストポータルに対してプライベート署名付き証明書を使用する場合、証明書エラーが発生するか、ポータルページからのアクセスがブラウザによってブロックされる可能性があるためです。これらをすべて回避するには、ポータルで使用する公開署名証明書を使用して、より優れたユーザエクスペリエンスを確保します。また、各導入ノードのIPアドレスをSANフィールドに追加して、IPアドレスを介してサーバにアクセスする際の証明書の警告を回避する必要があります。

証明書と秘密キーのバックアップ

次のファイルをエクスポートすることをお勧めします。

1.すべてのシステム証明書（展開内のすべてのノードから）とその秘密キー（再インストールするために必要）を安全な場所に保存します。証明書の設定（証明書が使用されたサービス）をメモしておきます。

2.プライマリ管理ノードの信頼された証明書ストアからのすべての証明書。証明書の設定（証明書が使用されたサービス）をメモしておきます。

3.すべての認証局証明書。

これを行うには

1. 移動先 Administration > System > Certificates > Certificate Management > System Certificates. 証明書を選択し、
Export. 選択 Export Certificates および[Private Keys]オプションボタンを選択します。秘密キーの
パスワードを入力し、パスワードを確認します。クリック Export.
2. 移動先 Administration > System > Certificates > Certificate Management > Trusted Certificates. 証明書を選択し、
Export. クリック Save File 証明書をエクスポートします。
3. 移動先 Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. 証明書を選
択し、 Export. 選択 Export Certificates および[Private Keys]オプションボタンを選択します。
[Private Key Password]と[Confirm Password]を入力します。クリック Export. クリック Save
File 証明書をエクスポートします。

トラブルシューティング

証明書の有効性の確認

Cisco ISEの信頼できる証明書またはシステム証明書ストア内のいずれかの証明書が期限切れになると、アップグレードプロセスが失敗します。[Trusted Certificates]ウィンドウと[System Certificates]ウィンドウ(Administration > System > Certificates > Certificate Management)にアクセスし、必要に応じてアップグレードの前に更新します。

また、[CA Certificates]ウィンドウ(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)にアクセスし、必要に応じてアップグレードの前に更新します。

証明書の削除

ISEの証明書が期限切れまたは未使用の場合は、削除する必要があります。削除する前に、証明書を (該当する場合は秘密キーとともに) エクスポートしてください。

期限切れの証明書を削除するには、 Administration > System > Certificates > Certificate Management. をクリック
します。 System Certificates Store. 期限切れの証明書を選択し、 Delete.

信頼できる証明書ストアと認証局(CA)証明書ストアについても同じ説明を参照してください。

サブリカントが802.1x認証でISEサーバ証明書を信頼しない

ISEがSSLハンドシェイクプロセスの完全な証明書チェーンを送信するかどうかを確認します。

サーバ証明書を必要とするEAP方式 (つまり、PEAP) で、クライアントOS設定で[Validate Server Identity]が選択されている場合、サブリカントは、認証プロセスの一部として、ローカルの信頼ストアにある証明書を使用して証明書チェーンを検証します。SSLハンドシェイクプロセスの一部として、ISEは自身の証明書と、そのチェーン内に存在するルート証明書または中間証明書 (あるいはその両方) を提示します。チェーンが不完全な場合、またはサブリカントがその信頼ストアにこのチェーンを含まない場合、サブリカントはサーバIDを検証できません。

証明書チェーンがクライアントに戻されたことを確認するには、ISE(Operations > Diagnostic Tools > General Tools > TCP Dump)または認証時のエンドポイントでのWiresharkキャプチャ。キャプチャを開き、フィルタを適用します ssl.handshake.certificates Wiresharkでアクセスの課題を見つけます。

選択したら、に移動します。 Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

チェーンが不完全な場合、ISEに移動します Administration > Certificates > Trusted Certificates ルート証明書や中間証明書が存在することを確認します。証明書チェーンが正常に渡された場合は、チェーン自体が有効であることを、ここで説明する方法で確認する必要があります。

各証明書 (サーバ、中間、およびルート) を開き、各証明書のSubject Key Identifier(SKI)と、チェーン内の次の証明書のAuthority Key Identifier(AKI)が一致するように、信頼のチェーンを確認します。

ISE証明書チェーンは正しいが、エンドポイントが認証中にISEサーバ証明書を拒否する

ISEがSSLハンドシェイク用の完全な証明書チェーンを提示し、サブリカントが証明書チェーンを拒否している場合、次の手順は、ルート証明書または中間証明書がクライアントのローカル信頼ストアにあることを確認することです。

これをWindowsデバイスから確認するには、 mmc.exe (Microsoft管理コンソール) に移動し、 File > Add-Remove Snap-in.[使用可能なスナップイン]列から、 Certificates をクリックし、 Add.次のいずれかを選択します My user account または Computer account 使用している認証タイプ (ユーザまたはマシン) に基づいて、 OK .

コンソールビューで、 [Trusted Root Certification Authorities]および[Intermediate Certification Authorities]を選択して、ローカル信頼ストアにルート証明書と中間証明書が存在することを確認します。

これがサーバIDチェックの問題であることを確認する簡単な方法は、サブリカントプロファイル設定で[Validate Server Certificate]をオフにして、もう一度テストすることです。

よく寄せられる質問 (FAQ)

ISEが証明書がすでに存在するという警告をスローした場合の対処方法

このメッセージは、ISEがまったく同じOUパラメータを持つシステム証明書を検出し、重複する証明書をインストールしようとしたことを意味します。重複したシステム証明書はサポートされていないため、新しい証明書が異なっていることを確認するために、市/州/部署の値を少し異なる値に変更することを推奨します。

ISEのポータルページが信頼できないサーバによって表示されることを示す警告がブラウザで表示されるのはなぜですか。

これは、ブラウザがサーバのID証明書を信頼していない場合に発生します。

最初に、ブラウザに表示されるポータル証明書が予想どおりであり、ポータル用にISEで設定されていることを確認します。

次に、FQDNを使用してポータルにアクセスします。使用中のIPアドレスの場合は、FQDNとIPアドレスの両方が証明書のSANフィールドまたはCNフィールドに含まれていることを確認します。

最後に、ポータル証明書チェーン (ISEポータル、中間CA、ルートCA証明書) がクライアントOSまたはブラウザソフトウェアにインポートされ、信頼されていることを確認します。

注:iOS、Android OS、およびChrome/Firefoxブラウザの一部の新しいバージョンでは、証明書に対して厳密なセキュリティ要件があります。これらのポイントが満たされていても、ポータルCAと中間CAがSHA-256より小さい場合は、接続を拒否できます。

無効な証明書が原因でアップグレードが失敗した場合の対処方法

Cisco ISEの信頼できる証明書またはシステム証明書ストア内のいずれかの証明書が期限切れになると、アップグレードプロセスが失敗します。[Trusted Certificates]ウィンドウと[System Certificates]ウィンドウ(Administration > System > Certificates > Certificate Management)にアクセスし、必要に応じてアップグレードの前に更新します。

また、[CA Certificates]ウィンドウ(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)にアクセスし、必要に応じてアップグレードの前に更新します。

ISEをアップグレードする前に、内部CA証明書チェーンが有効であることを確認します。

移動先 Administration > System > Certificates > Certificate Authority Certificates. 展開の各ノードで、[Friendly Name]列の[Certificate Services Endpoint Sub CA]で証明書を選択します。クリック View [Certificate Status]が正常なメッセージで、表示されているかどうかを確認します。

証明書チェーンが破損している場合は、Cisco ISEのアップグレードプロセスを開始する前に問題を修正してください。この問題を解決するには、 Administration > System > Certificates > Certificate Management > Certificate Signing Requestsを選択し、ISEルートCAオプション用に生成します。

関連情報

- [ISE 2.7証明書および証明書ストアの設定の管理](#)
- [ISEでのデジタル証明書の実装](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

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。