

WLCとISEを使用したEAP-TLSの理解と設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[EAP-TLS フロー](#)

[EAP-TLS フローのステップ](#)

[設定](#)

[Cisco ワイヤレス LAN コントローラ](#)

[ISE と Cisco WLC](#)

[EAP-TLS 設定](#)

[ISE での WLC の設定](#)

[ISE での新しいユーザの作成](#)

[ISE での証明書の信頼確立](#)

[EAP-TLS 用のクライアント](#)

[クライアントマシン \(Windows デスクトップ \) へのユーザ証明書のダウンロード](#)

[EAP-TLS のワイヤレスプロファイル](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、802.1XとExtensible Authentication Protocol(EAP)EAP-TLSを使用して Wireless Local Area Network(WLAN)を設定する方法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。

- 802.1X認証プロセス
- 証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

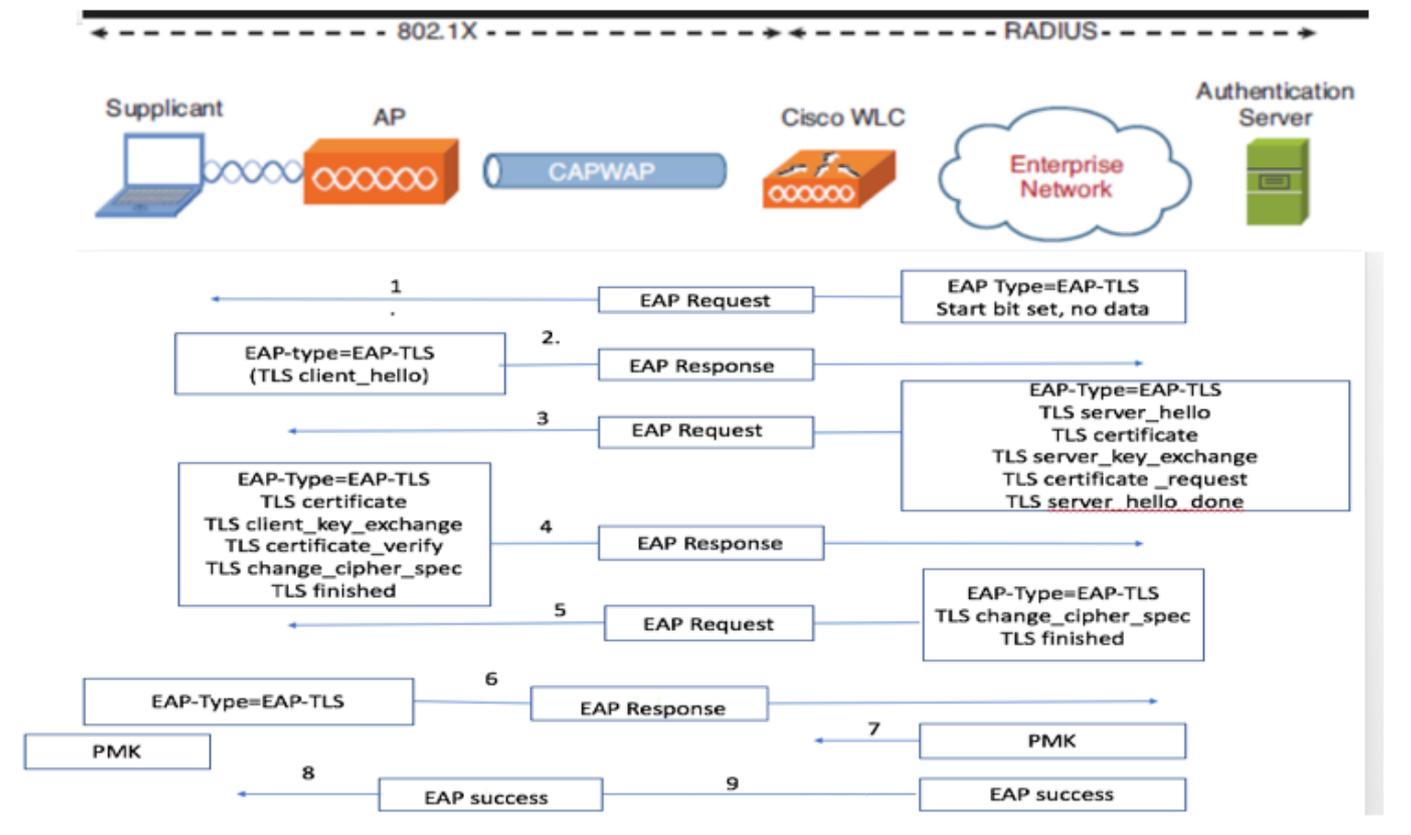
- WLC 3504 バージョン 8.10

- Identity Services Engine (ISE) バージョン 2.7

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。

背景説明

EAP-TLS フロー



EAP-TLS フローのステップ

1. ワイヤレスクライアントが、アクセスポイント (AP) に関連付けられます。APはこの時点ではクライアントによるデータの送信を許可せず、認証要求を送信します。サブリカントはEAP応答IDで応答します。WLCが、ユーザ ID 情報を認証サーバに送信します。RADIUSサーバが、EAP-TLS 開始パケットでクライアントに応答します。この時点で EAP-TLS カンバセーションが開始されます。
2. ピアは、NULLに設定された暗号である「client_hello」ハンドシェイクメッセージを含む EAP-Responseを認証サーバに返信します
3. 認証サーバが、次を含むアクセスチャレンジパケットで応答します。

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.

4.クライアントは、次の内容を含むEAP-Responseメッセージで応答します。

Certificate → Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify → Verifies the server is trusted

change_cipher_spec

TLS finished

5.クライアントが正常に認証されると、RADIUSサーバは「change_cipher_spec」と「handshake finished」メッセージを含むAccess-challengeで応答します。

6.これを受信すると、クライアントはRADIUSサーバを認証するためにハッシュを確認します。

7. TLSハンドシェイク中に新しい暗号キーがシークレットから動的に取得される

8/9.EAP：最終的にサーバからオーセンティケータに送信され、サブリカントに渡されます。

この時点で、EAP-TLS 対応のワイヤレスクライアントがワイヤレスネットワークにアクセスできます。

設定

Cisco ワイヤレス LAN コントローラ

ステップ1：最初のステップでは、Cisco WLCでRADIUSサーバを設定します。RADIUSサーバをWLCに追加するには、[セキュリティ (Security)] > [RADIUS] > [認証 (Authentication)] に移動します。図のように、[新規 (New)] をクリックします。

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The 'SECURITY' tab is selected, and the 'RADIUS Authentication Servers' page is displayed. The 'Authentication' sub-tab is active. The 'Auth Called Station ID Type' is set to 'AP Name:SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Colon'. The 'Framed MTU' is set to '1300'. A table lists the configured RADIUS servers:

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	138.77.0.84	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	138.77.0.83	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3	138.77.97.20	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	138.77.97.21	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5	172.27.1.71	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6	10.100.120.41	1812	Disabled	Enabled

ステップ2：ここで、ISE上のWLCを検証するために使用されるIPアドレスと共有秘密

<password>を入力する必要があります。図のように、[適用 (Apply)] をクリックして続行します。

The screenshot shows the 'RADIUS Authentication Servers > Edit' configuration page. The 'Shared Secret' and 'Confirm Shared Secret' fields are highlighted with a red box. The 'Apply' button is also highlighted with a red box. The configuration includes fields for Server Index (7), Server Address (10.106.35.67), Shared Secret Format (ASCII), and various other settings like Key Wrap, Port Number (1812), and Server Status (Enabled).

ステップ 3： RADIUS 認証用の WLAN を作成します。

ここで、新しい WLAN を作成できます。この WLAN を、WPA-enterprise モードを使用するように設定することで、認証に RADIUS を使用できるようになります。

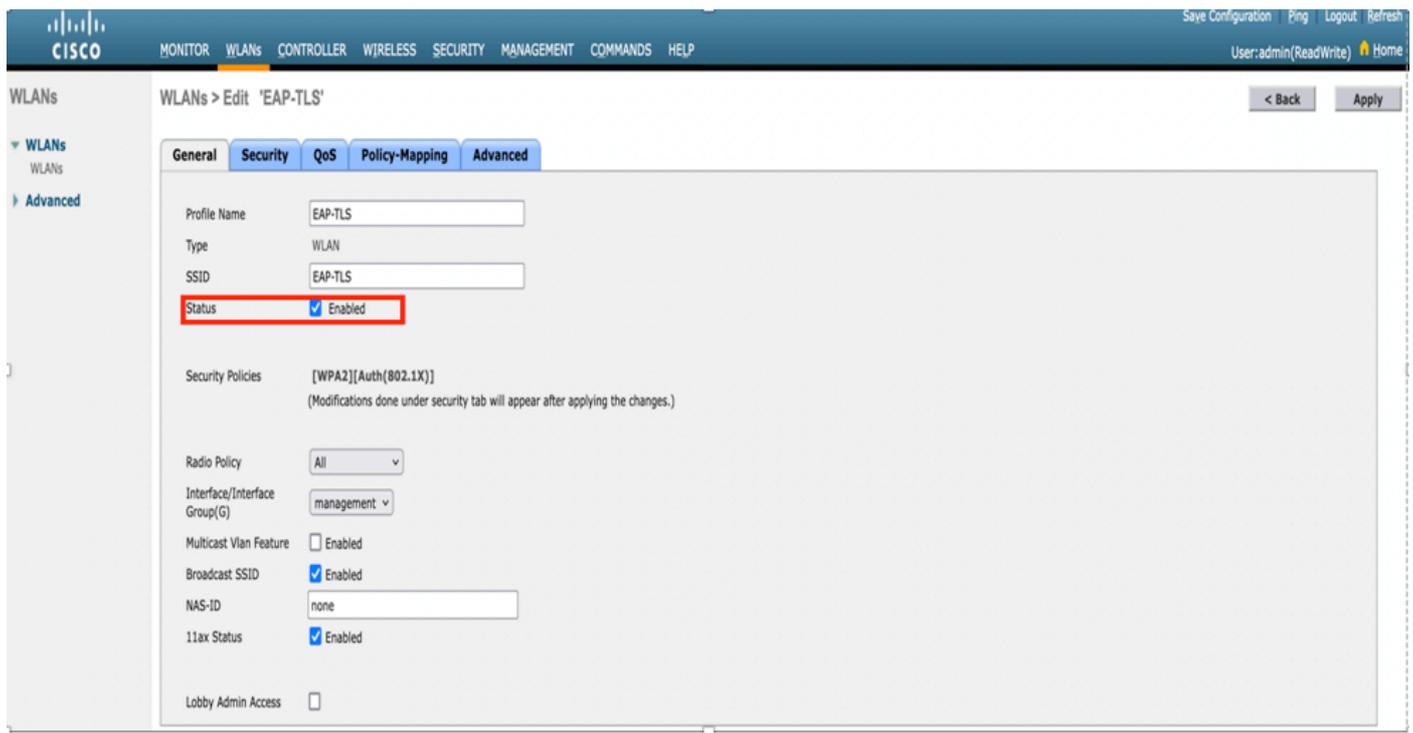
ステップ 4： 図のように、メインメニューから [WLAN (WLANs)] を選択し、[新規に作成 (Create New)] を選択して、[実行 (Go)] をクリックします。

The screenshot shows the 'WLANs' configuration page. The 'WLANs' menu item is highlighted with a red box. The 'Create New' button and the 'Go' button are also highlighted with red boxes. The page shows a table with columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies.

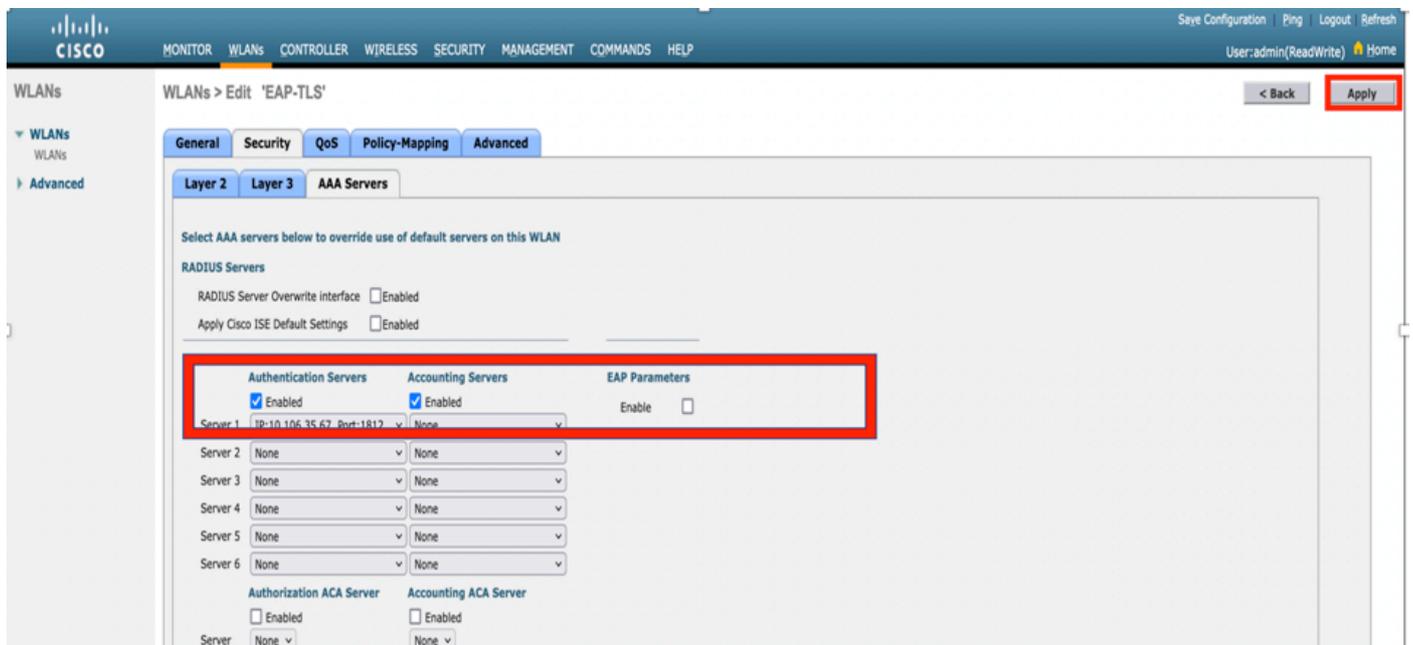
ステップ 5： 新しい WLAN に EAP-TLS という名前を付けます。図のように、[適用 (Apply)] をクリックして続行します。

The screenshot shows the 'WLANs > New' configuration page. The 'WLANs' menu item is highlighted with a red box. The 'Apply' button is also highlighted with a red box. The configuration includes fields for Type (WLAN), Profile Name (EAP-TLS), SSID (EAP-TLS), and ID (3).

ステップ6：[全般 (General)] をクリックし、[ステータス (Status)] が [有効 (Enabled)] であることを確認します。図のように、デフォルトのセキュリティポリシーは 802.1X 認証と WPA2 です。



ステップ7：次に、[Security] > [AAA Servers] タブに移動し、図に示すように、設定した RADIUSサーバを選択します。



注：先に進む前に、WLC から RADIUS サーバに到達できることを確認することをお勧めします。RADIUS は UDP ポート 1812 (認証用) を使用するため、このトラフィックがネットワークのどこにおいてもブロックされないようにする必要があります。

ISE と Cisco WLC

EAP-TLS 設定

ポリシーを作成するために、ポリシーで使用する許可プロトコルリストを作成する必要があります。dot1x ポリシーを作成するため、ポリシーの設定方針に基づいて許可される EAP タイプを指定します。

デフォルトを使用すると、特定のEAPタイプへのアクセスをロックダウンする必要がある場合に推奨されない、ほとんどのEAPタイプを認証に使用できます。

ステップ 1 : 図のように、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されるプロトコル (Allowed Protocols)] に移動し、[追加 (Add)] をクリックします。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit + Add Duplicate Delete

<input type="checkbox"/>	Service Name	Description
<input type="checkbox"/>	Default Network Access	Default Allowed Protocol Service

ステップ 2 : この[Allowed Protocol]リストで、リストの名前を入力できます。この場合、図のように、[EAP-TLSを許可 (Allow EAP-TLS)] チェックボックスをオンにして、他のチェックボックスをオフにします。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

Allowed Protocols Services List > New Allowed Protocols Service

Allowed Protocols

Name

Description

Allowed Protocols

Authentication Bypass

Process Host Lookup (i)

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)

Enable Stateless Session Resume

Session ticket time to live

Proactive session ticket update will occur after % of Time To Live has expired

Allow LEAP

Allow PEAP

PEAP Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)

Require cryptobinding TLV (i)

ISE での WLC の設定

ステップ 1： 図のように、ISE コンソールを開き、[管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [追加 (Add)] に移動します。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management (i) External Services Field Service Threat Center NAC

Network Devices Network Device Group Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Click here to do wireless setup and visibility setup. Do not close this again.

Network devices

Default Device

Device Security Settings

Name	IP/Host	Profile Name	Location	Type	Description

Show [All]

ステップ 2： 図のように、値を入力します。

Identity Services Engine Administration Work Centers

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

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

* Name

Description

IP Address * IP: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings [?](#)

ISE での新しいユーザの作成

ステップ 1： 図のように、[管理 (Administration)] > [IDの管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [追加 (Add)] に移動します。

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Network Access Users

Latest Manual Network Scan Results

Status	Name	Description	First Name	Last Name	Email Address	User Identity Group	Admin
--------	------	-------------	------------	-----------	---------------	---------------------	-------

Show All

ステップ 2： 図のように、情報を入力します。

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

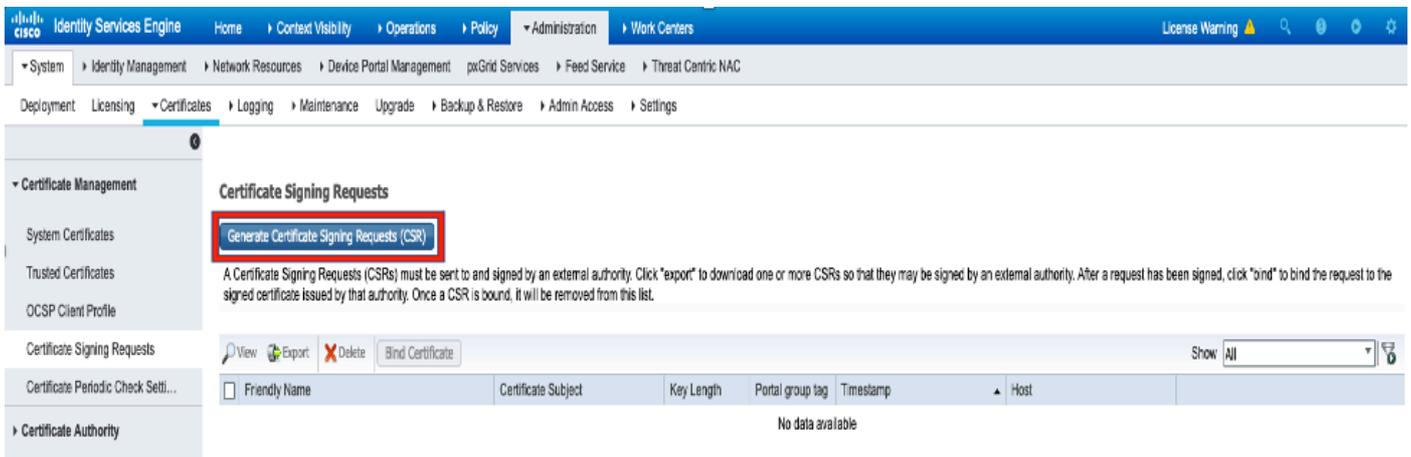
User Groups

ISE での証明書の信頼確立

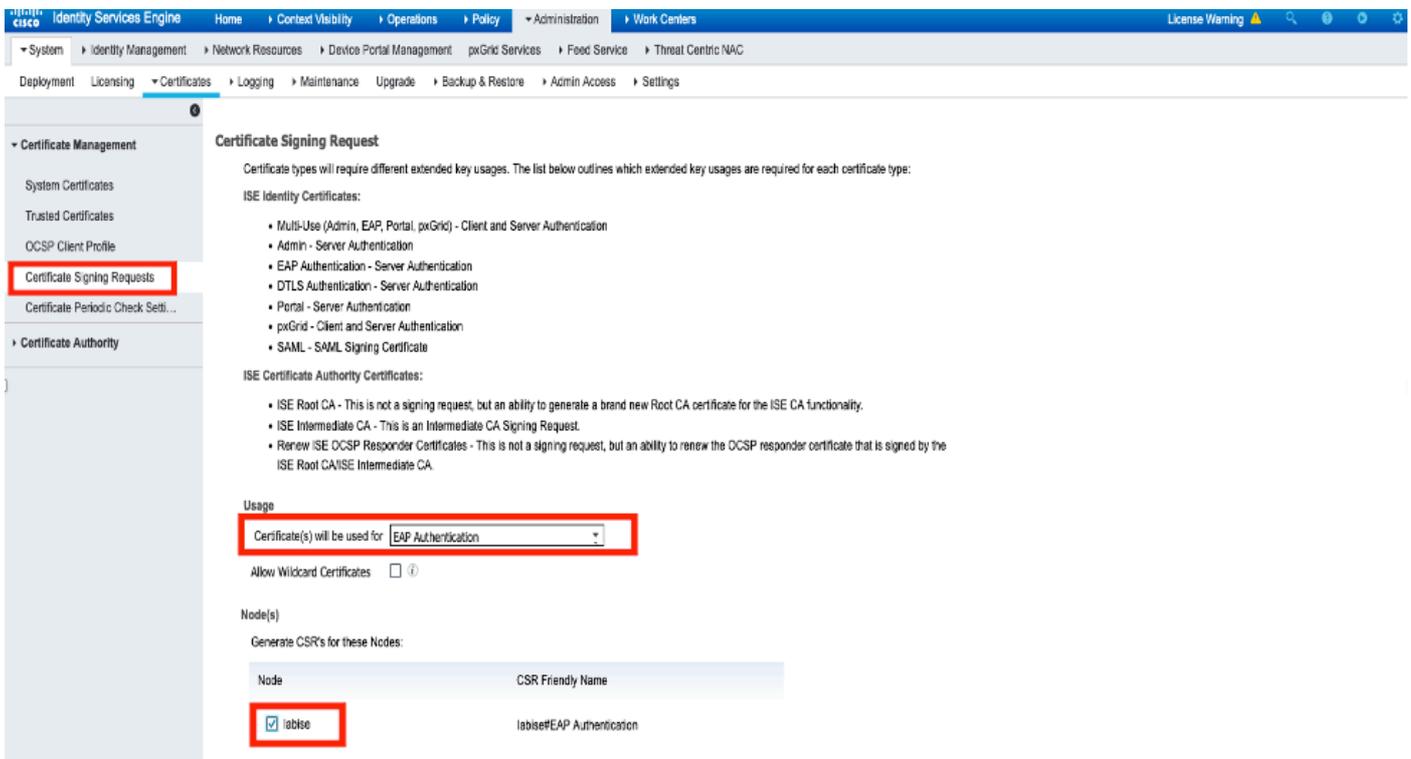
ステップ 1 : [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] に移動します。

[インポート (Import)]をクリックして ISE に証明書をインポートします。WLC を追加し、ISE でユーザを作成したら、ISE で証明書の信頼を確立するという EAP-TLS の最も重要な部分を実行する必要があります。そのために、CSR を生成する必要があります。

ステップ 2 : 図のように、[管理 (Administrauon)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] > [証明書署名要求 (CSR) の生成 (Generate Certificate Signing Requests (CSR))] に移動します。

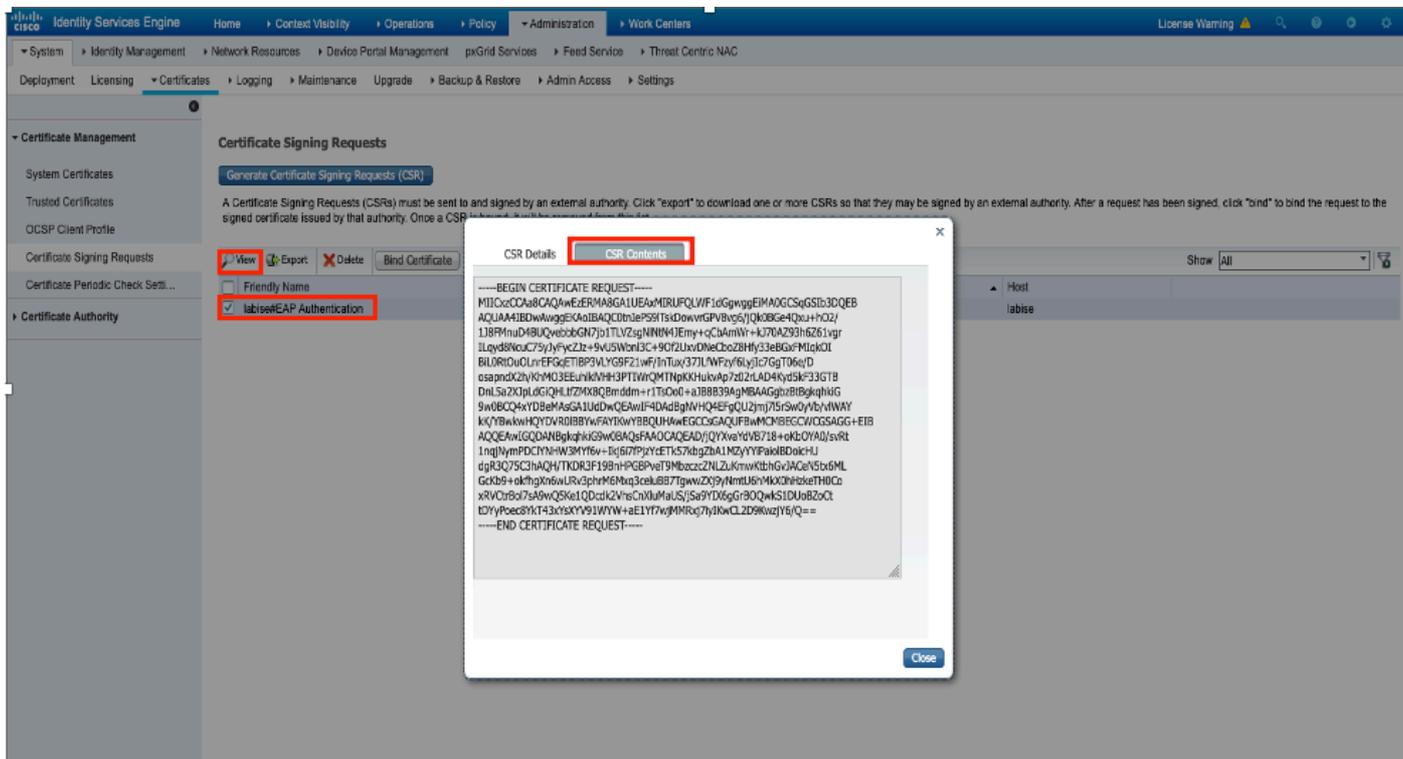


ステップ3:CSRを生成するには、[Usage] に移動し、[Certificate(s) are used for] ドロップダウンオプションから[EAP Authentication] を選択します (図を参照) 。

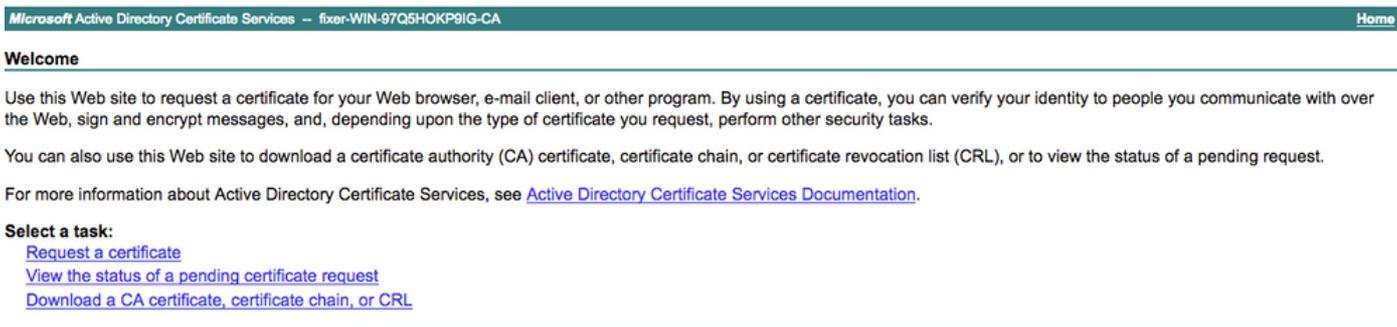


ステップ4:ISEで生成されたCSRを表示できます。図のように、[表示 (View)] をクリックします

。



ステップ5:CSRが生成されたら、図に示すように、CAサーバを参照し、[Request a certificate] をクリックします。



ステップ6：証明書を要求すると、[User Certificate] と [advanced certificate request] のオプションが表示されます。次の図に示すように、[advanced certificate request] をクリックします。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

ステップ7：生成されたCSRを [Base-64エンコード証明書要求 (Base-64 encoded certificate request)] に貼り付けます。図のように、[証明書テンプレート： (Certificate Template:)] ドロップダウンオプションから [Webサーバ (Web Server)] を選択し、[送信 (Submit)] をクリックします。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

Additional Attributes:

Attributes:

ステップ8:[Submit] をクリックすると、証明書のタイプを選択するオプションが表示されます。次に、[Base-64 encoded] を選択し、[Download certificate chain] をクリックします (図を参照)。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

ステップ9:ISEサーバの証明書のダウンロードが完了します。証明書を抽出できます。証明書には、1つのルート証明書と他の中間証明書の2つの証明書が含まれています。ルート証明書は、図のように、[管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted certificates)] > [インポート (Import)] を選択してインポートできます。

Identity Services Engine License Warning

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

Click here to do wireless setup and visibility setup Do not show this again.

Certificate Management

System Certificates

Trusted Certificates

Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
---------------	--------	-------------	---------------	-----------	-----------	------------	-----------------

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

Import a new Certificate into the Certificate Store

* Certificate File No file chosen

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

ステップ10:[Submit] をクリックすると、信頼できる証明書リストに証明書が追加されます。また、図のように、CSR にバインドするには中間証明書が必要です。

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 Signing Requests

[Generate Certificate Signing Requests \(CSR\)](#)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/> ise#EAP Authentication	CN=ise.c.com	2048		Mon, 9 Jul 2018	ise

Created by Paint X

ステップ11:[Bind certificate] をクリックすると、デスクトップに保存されている証明書ファイルを選択するオプションがあります。図のように、中間証明書を選択し、[送信 (Submit)] をクリックします。

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

Bind CA Signed Certificate

* Certificate File No file chosen

Friendly Name

Validate Certificate Extensions

Usage

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

ステップ12：証明書を表示するには、図に示すように、[Administration] > [Certificates] > [System

Certificates] に移動します。

The screenshot shows the 'System Certificates' page in the Identity Services Engine. The page has a navigation menu on the left and a main content area. The main content area contains a table of certificates. The table has the following columns: Friendly Name, Used By, Portal group tag, Issued To, Issued By, Valid From, and Expiration Date. There are two rows of certificates. The first row is 'Default self-signed saml server certificate - CN=SAML_ise.c.com' with 'SAML' as the Used By, 'SAML_ise.c.com' as Issued To and Issued By, 'Wed, 11 Jul 2018' as Valid From, and 'Thu, 11 Jul 2019' as Expiration Date. The second row is 'Intermediate' with 'EAP Authentication, Admin, Portal' as Used By, 'Default Portal Certificate Group (j)' as Portal group tag, 'ise.c.com' as Issued To, 'fixer-WIN-97Q5HOKP9IG-CA' as Issued By, 'Fri, 13 Jul 2018' as Valid From, and 'Sun, 12 Jul 2020' as Expiration Date. A red box highlights the second row.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
Default self-signed saml server certificate - CN=SAML_ise.c.com	SAML		SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019
Intermediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group (j)	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020

EAP-TLS 用のクライアント

クライアントマシン (Windows デスクトップ) へのユーザ証明書のダウンロード

ステップ 1 : EAP-TLS を使用してワイヤレスユーザを認証するには、クライアント証明書を生成する必要があります。サーバにアクセスできるように、Windows コンピュータをネットワークに接続します。Web ブラウザを開き、次のアドレスを入力します : <https://sever ip addr/certsrv:>

ステップ2:CAは、ISE用に証明書をダウンロードしたCAと同じである必要があります。

そのために、サーバ用の証明書のダウンロードに使用した CA サーバにアクセスする必要があります。同じ CA で以前と同じように [証明書を要求する (Request a certificate)] をクリックしますが、今回は、図のように、[証明書テンプレート (Certificate Template)] で [ユーザ (User)] を選択する必要があります。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJryaF4l2aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUIIweOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgRdD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX-----END CERTIFICATE REQUEST-----
-------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

ステップ3 : 次に、先にサーバで行ったように、[download certificate chain] をクリックします。

証明書を取得したら、次の手順に従って証明書を Windows ラップトップにインポートします。

ステップ4 : 証明書をインポートするには、Microsoft 管理コンソール (MMC) から証明書にアクセスする必要があります。

1. MMC を開くには、[スタート (Start)] > [ファイル名を指定して実行 (Run)] > [MMC] に移動します。
2. [ファイル (File)] > [スナップインの追加と削除 (Add / Remove Snap In)] に移動します。
3. [証明書 (Certificates)] をダブルクリックします。
4. [コンピューターアカウント (Computer Account)] を選択します。
5. [ローカルコンピューター (Local Computer)] > [完了 (Finish)] を選択します。
6. [OK] をクリックして[スナップイン (Snap-In)] ウィンドウを終了します。
7. [証明書 (Certificates)] の横にある [+] をクリックし、[個人 (Personal)] > [証明書 (Certificates)] を選択します。
8. [証明書 (Certificates)] を右クリックし、[すべてのタスク (All Tasks)] > [インポート (Import)] を選択します。
9. [next] をクリックします。

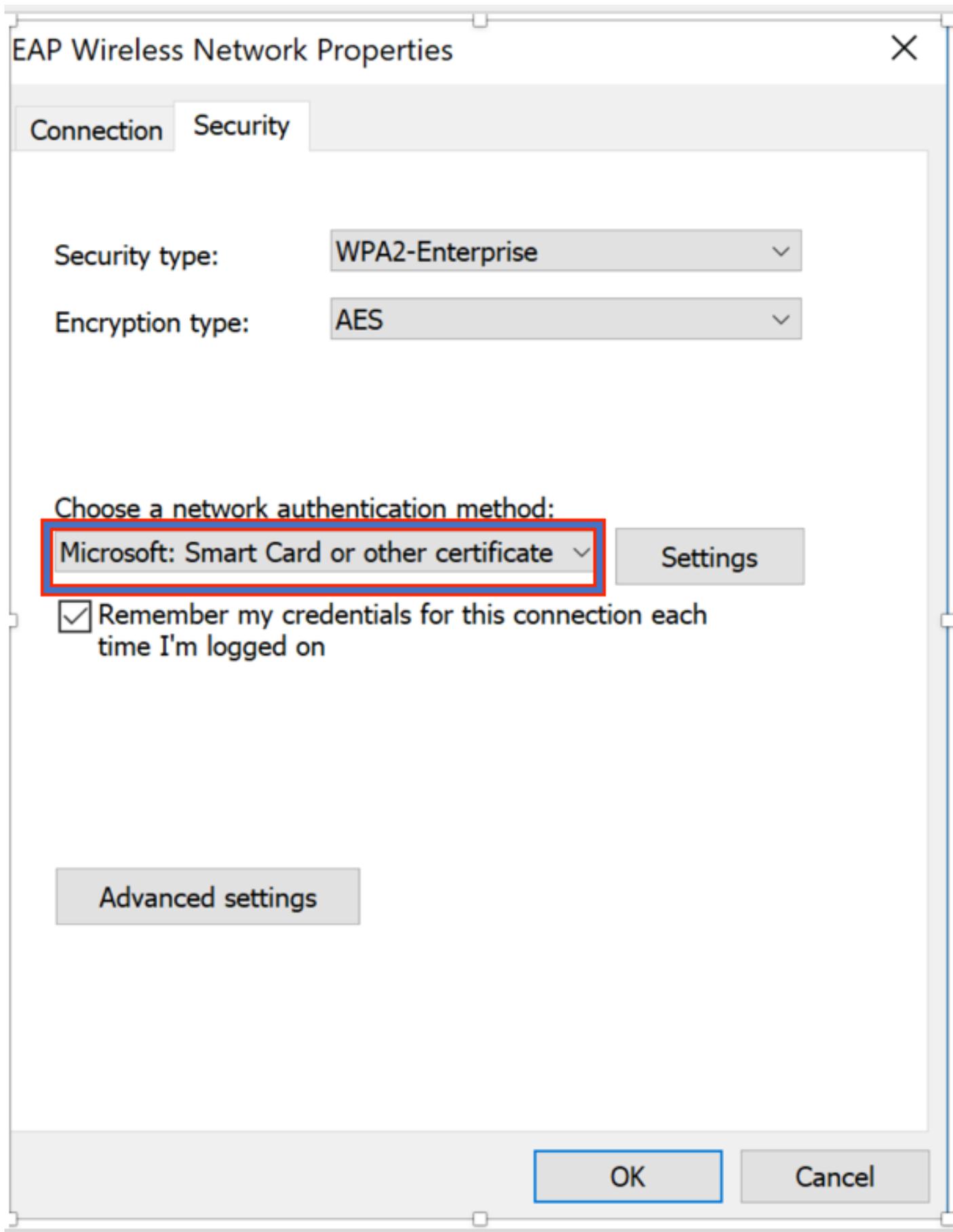
10. [Browse] をクリックします。
11. インポートする .cer、.crt、または .pfx ファイルを選択します。
12. [Open] をクリックします。
13. [next] をクリックします。
14. [証明書の種類に基づいて、自動的に証明書ストアを選択する (Automatically select the certificate store based on the type of certificate)] を選択します。
15. [完了 (Finish)]、[OK] の順にクリックして完了。

証明書のインポートが完了したら、ワイヤレスクライアント (この例では Windows デスクトップ) を EAP-TLS 用に設定する必要があります。

EAP-TLS のワイヤレスプロファイル

ステップ 1 : Protected Extensible Authentication Protocol (PEAP) の代わりに EAP-TLS を使用するために、PEAP 用に以前に作成されたワイヤレスプロファイルを変更します。EAP ワイヤレスプロファイルをクリックします。

ステップ 2 : 図のように、[Microsoft : スマートカードまたはその他の証明書 (Microsoft: Smart Card or other certificate)] を選択し、[OK] をクリックします。



ステップ 3 : [設定 (Settings)] をクリックし、図のように、CA サーバから発行されたルート証明書を選択します。

Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Advanced

Use simple certificate selection (Recommended)

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1; srv2; *.srv3.com):

Trusted Root Certification Authorities:

Entrust.net Certification Authority (2048)

Equifax Secure Certificate Authority

fixer-WIN-97Q5HOKP9IG-CA

GeoTrust Global CA

GeoTrust Primary Certification Authority

GeoTrust Primary Certification Authority - G3

GlobalSign

GlobalSign

GlobalSign Root CA

View Certificate

ステップ 4 : [詳細設定 (Advanced Settings)] をクリックし、図のように、[802.1x設定 (802.1x settings)] タブで [ユーザまたはコンピュータ認証 (User or computer authentication)] を選択します。

Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

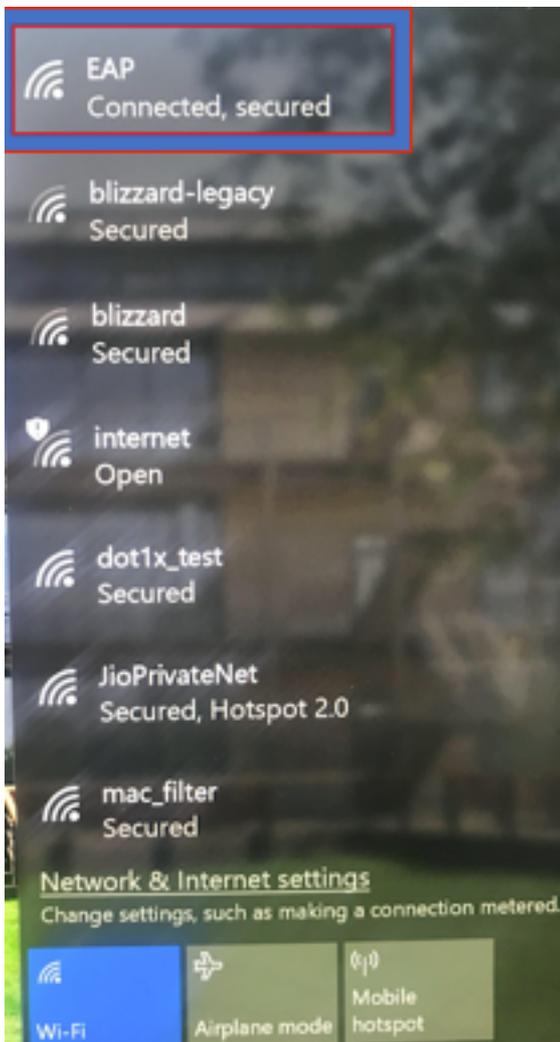
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

ステップ5 : ここで、ワイヤレスネットワークへの接続を再試行し、正しいプロファイル (この例ではEAP) を選択して、**Connect**をクリックします。図のように、ワイヤレスネットワークに接続されます。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ1：クライアントポリシーマネージャの状態が**RUN**と表示されている必要があります。これは、クライアントが、認証を完了し、IP アドレスを取得して、図に示されているトラフィックを渡す準備ができていることを意味します。

Monitor

Clients > Detail

Max Number of Records Clear AVC Stats

General **AVC Statistics**

Client Properties		AP Properties	
MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
IPv6 Address	fe80::2818:15a4:65f9:842,	AP Type	802.11bn
		AP radio slot Id	0
		WLAN Profile	EAP
		WLAN SSID	EAP
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
Client Type	Simple IP	Reason Code	1
User Name	Administrator	Status Code	0
Port Number	1	CF Pollable	Not Implemented
Interface	management	CF Poll Request	Not Implemented
VLAN ID	32	Short Preamble	Not Implemented
Quarantine VLAN ID	0	PBCC	Not Implemented
CCX Version	CCXv1	Channel Agility	Not Implemented
E2E Version	Not Supported	Re-authentication timeout	1682
Mobility Role	Local	Remaining Re-authentication timeout	0
Mobility Peer IP Address	N/A	WEP State	WEP Enable
Mobility Move Count	0		
Policy Manager State	RUN		
Management Frame Protection	No		
UpTime (Sec)	146		

Lync Properties	
Lync State	Disabled
Audio Qos Policy	Silver

ステップ2：また、図に示すように、クライアントの詳細ページでWLCの正しいEAP方式を確認します。

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Auth Key Mgmt	802.1x
Encryption Cipher	CCMP (AES)
EAP Type	EAP-TLS
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied	Unavailable

ステップ3 : コントローラのCLIからのクライアントの詳細を次に示します (出力を省略) 。

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... 00:d7:8f:52:db:a0
AP Name..... Alpha2802_3rdfloor
AP radio slot Id..... 0
Client State..... Associated
Wireless LAN Id..... 5
Wireless LAN Network Name (SSID)..... EAP
Wireless LAN Profile Name..... EAP
Hotspot (802.11u)..... Not Supported
BSSID..... 00:d7:8f:52:db:a4
Connected For ..... 48 secs
Channel..... 1
IP Address..... 10.106.32.239
Gateway Address..... 10.106.32.1
Netmask..... 255.255.255.0
Policy Manager State..... RUN
Policy Type..... WPA2
Authentication Key Management..... 802.1x
```

Encryption Cipher..... CCMP-128 (AES)
Protected Management Frame No
Management Frame Protection..... No
EAP Type..... EAP-TLS

ステップ4 : 図に示すように、ISEで[Context Visibility] > [End Points] > [Attributes] に移動します。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Endpoints' section is active, showing the MAC address 34:02:86:96:2F:B7. Below this, the endpoint details are listed: MAC Address: 34:02:86:96:2F:B7, Username: Administrator@fixer.com, Endpoint Profile: Intel-Device, Current IP Address, and Location. The 'Attributes' tab is selected, displaying 'General Attributes' and 'Other Attributes'. The 'General Attributes' section includes: Description, Static Assignment (false), Endpoint Policy (Intel-Device), Static Group Assignment (false), and Identity Group Assignment (Profiled). The 'Custom Attributes' section is empty, with a 'Filter' button and a settings icon. The 'Other Attributes' section lists: AAA-Server (ise), AKI (88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd), Airespace-Wlan-Id (5), AllowedProtocolMatchedRule (Dot1X), AuthenticationIdentityStore (Internal Users), and AuthenticationMethod (x509 .PKI). The 'AllowedProtocolMatchedRule' attribute is highlighted with a red box.

Attribute Name	Attribute Value
Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled
AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	5
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509 .PKI

BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_svr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11...

トラブルシューティング

現在、この設定のトラブルシューティングに使用できる特定の情報はあります。

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。