

EAP-PEAPのためのISEステートフルTLSセッション再開について

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[初期認証](#)

[再認証中](#)

[よく寄せられる質問 \(FAQ\)](#)

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)でのTransport Layer Security(TLS)セッションの再開について説明します。

前提条件

要件

- Transport Layer Security(TLS)ハンドシェイクプロセスに関する知識
- Protected Extensible Authentication Protocol(PEAP)フローの知識
- Cisco Identity Services Engine(ISE)に関する知識

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。

- Cisco Identity Services Engine 3.2
- ISE仮想マシン(VM)
- Windows 10 PC

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、クリアな（デフォルト）設定で作業を開始しています。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

TLSセッション再開は、初期TLSハンドシェイクのオーバーヘッドを排除するために使用される手法です。これにより、以前にTLSセッションを確立したクライアントとサーバは、リソースを大量に消費するハンドシェイクプロセスを繰り返すことなく、そのセッションを再開できます。

長所

- 最初のハンドシェイクでリソースを大量に消費する手順と、その手順の実行に必要な時間を回避することで、遅延を低減します。
- また、集中的なキー交換および証明書検証プロセスを省略することで、サーバの計算負荷を軽減します。

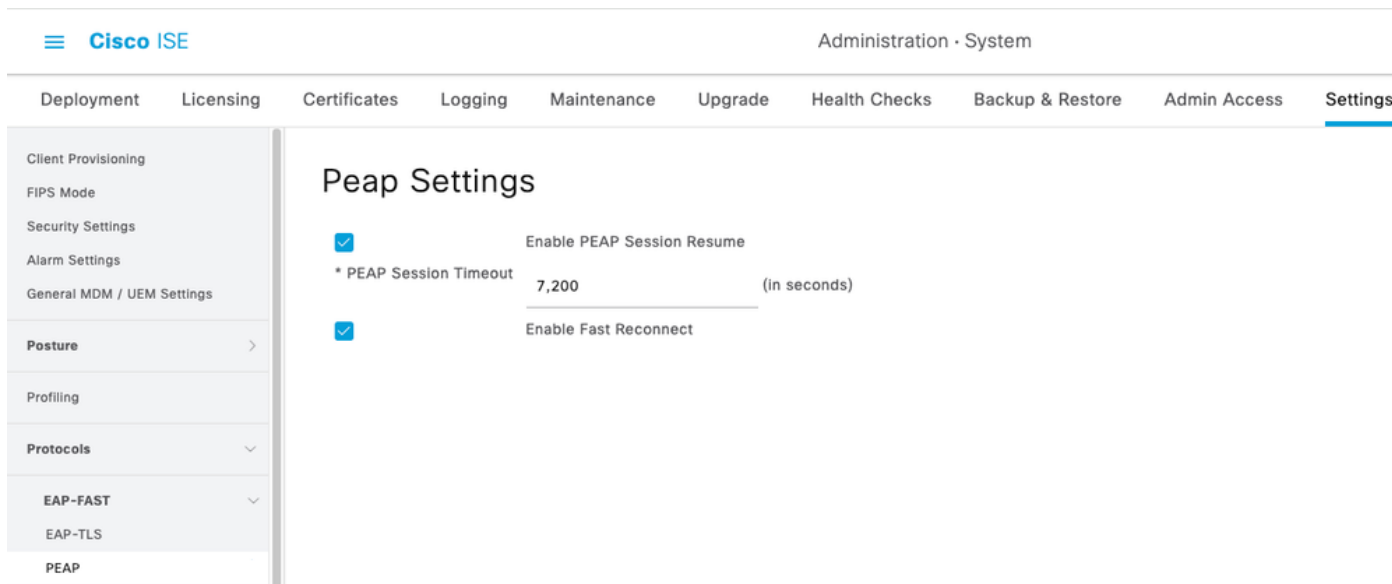
設定

ISEで、TLSセッションを有効にするには、PEAP用に再開します。

Administration > System > Settings > Protocols > PEAP > check the Enable PEAP Session Resume

デフォルトでは、ISEは7200秒間セッションを保持します。

オプションで、Enable Fast Reconnectを有効にできます。これにより、PEAPの内部方式がバイパスされ、さらに高速な再認証が可能になります。これは、ワイヤレスローミングなどのアプリケーションで望ましい動作です。



ISE PEAPセッション再開設定

サブリカントでも高速再接続を有効にする必要があります。

この設定は、高速再接続を有効にするWindowsネイティブサブリカント用です。

Protected EAP Properties



When connecting:

☐ Verify the server's identity by validating the certificate

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

Trusted Root Certification Authorities:

- ☐ Baltimore CyberTrust Root
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA
- ☐ DigiCert Global Root G2
- ☐ DigiCert Global Root G3
- ☐ DigiCert High Assurance EV Root CA



Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)



Configure...

☒ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK

Cancel

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。