Understand ISE Stateful TLS Session Resume for EAP-PEAP

Contents

Introduction

This document describes the Transport Layer Security (TLS) Session Resumption in Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

- Knowledge of Transport Layer Security (TLS) handshake process.
- Knowledge of Protected Extensible Authentication Protocol (PEAP) flow
- Knowledge of Cisco Identity Services Engine

Components Used

The information in this document is based on these software and hardware versions

- Cisco Identity Services Engine 3.2
- ISE Virtual Machine (VM)
- Windows 10 PC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

TLS session resumption is a technique used to eliminate the overhead of the initial TLS handshake. It allows a client and server who have previously established a TLS session to resume that session without repeating the resource-intensive handshake process.

Advantages

- It reduces the latency by avoiding the resource-intensive steps of the initial handshake and the time required to do that.
- It also reduces the computational load on the server by skipping the intensive key exchange and certificate validation processes.

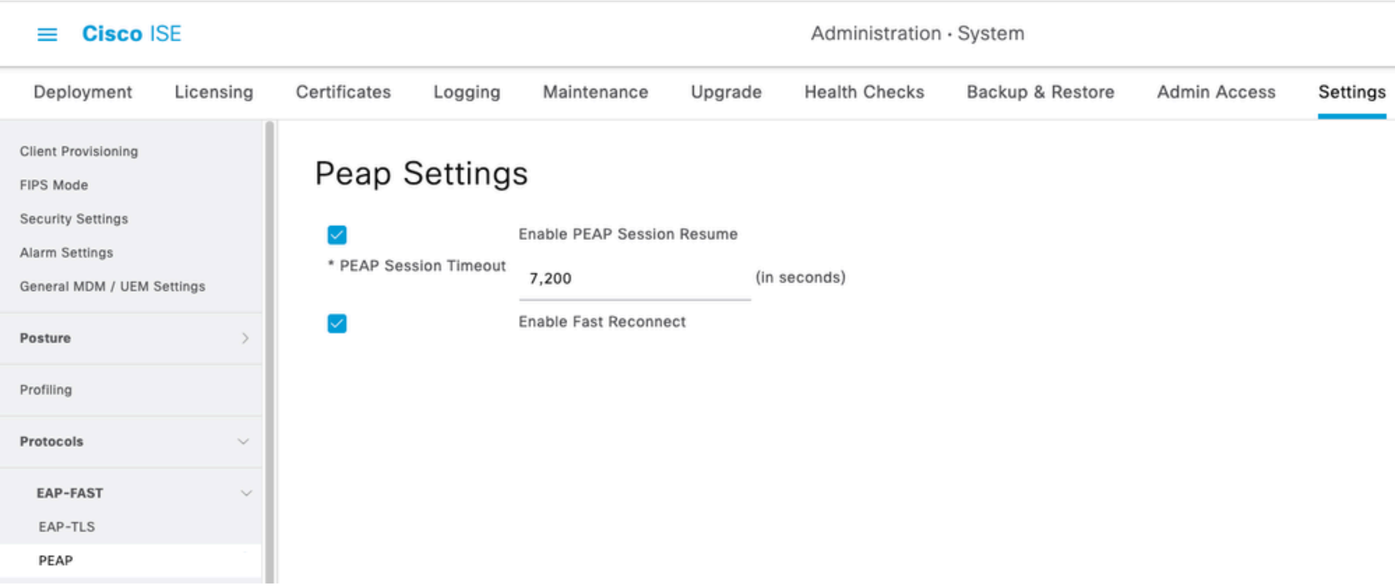
Configure

On ISE, to enable the TLS session, resume for PEAP:

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

By default, ISE holds the session for 7200 Seconds.

Optionally, you can enable the Enable Fast Reconnect, which in turns bypasses the inner method of PEAP and allows even faster reauthentication. It is desirable in applications such as wireless roaming.



Peap Settings

☑ Enable PEAP Session Resume

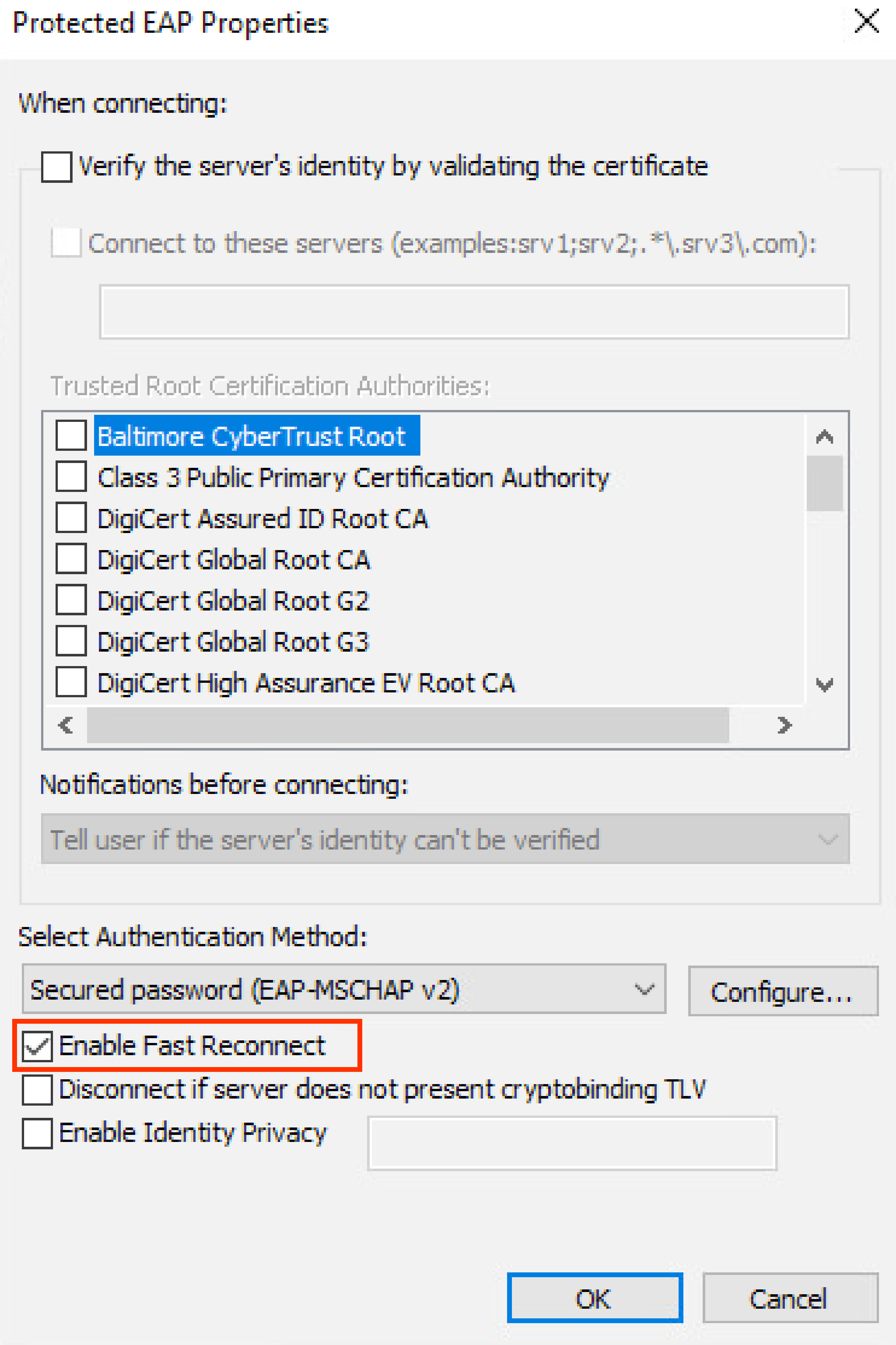
* PEAP Session Timeout 7,200 (in seconds)

☑ Enable Fast Reconnect

ISE PEAP Session Resume Config

The Fast Reconnect must also be enabled in the supplicant.

This configuration is for Windows native supplicant to enable Fast Reconnect.



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)

☑ Enable Fast Reconnect
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy