EAP-FAST Authentication with Wireless LAN Controllers and Identity Services Engine

Contents

Introduction

This document explains how to configure the wireless LAN controller (WLC) for Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST) authentication with the use of an external RADIUS server. This configuration example uses the Identity Services Engine (ISE) as the external RADIUS server to authenticate the wireless client.

This document focuses on how to configure the ISE for Anonymous and Authenticated In-Band (Automatic) Protected Access Credentials (PAC) provisioning to the wireless clients.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of the configuration of lightweight access points (LAPs) and Cisco WLCs
- Basic knowledge of CAPWAP protocol
- Knowledge of how to configure an external RADIUS server, such as the Cisco ISE
- Functional knowledge on general EAP framework
- Basic knowledge on security protocols, such as MS-CHAPv2 and EAP-GTC, and knowledge on digital certificates

Components Used

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

- Cisco 5520 Series WLC that runs firmware release 8.8.111.0Cisco 4800 Series APAnyconnect NAM.Cisco Secure ISE version 2.3.0.298Cisco 3560-CX Series Switch that runs version 15.2(4)E1

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, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The EAP-FAST protocol is a publicly accessible IEEE 802.1X EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1X EAP type that does not require digital certificates.

The EAP-FAST protocol is a client-server security architecture that encrypts EAP transactions with a Transport Level Security (TLS) tunnel. EAP-FAST tunnel establishment is based on strong secrets that are unique to users. These strong secrets are called PACs, which the ISE generates by using a master key known only to the ISE.

EAP-FAST occurs in three phases:

- **Phase zero (Automatic PAC provisioning phase)**—EAP-FAST phase zero, an optional phase is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access. **Providing a PAC to the end-user client is the sole purpose of phase zero**.**Note:** Phase zero is optional because PACs can also be manually provisioned to clients instead of using phase zero.See the PAC Provisioning Modes section of this document for details.
- **Phase one**—In phase one, the ISE and the end-user client establish a TLS tunnel based on the user's PAC credential. This phase requires that the end-user client has been provided a PAC for the user who is attempting to gain network access, and that the PAC is based on a

master key that has not expired. No network service is enabled by phase one of EAP-FAST.
- **Phase two**—In phase two, user authentication credentials are passed securely using an inner EAP method supported by EAP-FAST within the TLS tunnel to the RADIUS created using the PAC between the client and RADIUS server. EAP-GTC, TLS and MS-CHAP are supported as inner EAP methods. No other EAP types are supported for EAP-FAST.

Refer to How EAP-FAST works for more information.

PAC

PACs are strong shared secrets that enable the ISE and an EAP-FAST end-user client to authenticate each other and establish a TLS tunnel for use in EAP-FAST phase two. The ISE generates PACs by using the active master key and a username.

PAC comprises:

- **PAC-Key**—Shared secret bound to a client (and client device) and server identity.
- **PAC Opaque**—Opaque field that the client caches and passes to the server. The server recovers the PAC-Key and the client identity to mutually authenticate with the client.
- **PAC-Info**—At a minimum, includes the server's identity to enable the client to cache different PACs. Optionally, it includes other information such as the PAC's expiration time.

PAC Provisoning Modes

As mentioned earlier, phase zero is an optional phase.

EAP-FAST offers two options to provision a client with a PAC:

- **Automatic PAC provisioning (EAP-FAST Phase 0, or In-band PAC provisioning)**
- **Manual (Out-of-band) PAC provisioning**

In-band/Automatic PAC provisioning sends a new PAC to an end-user client over a secured network connection. Automatic PAC provisioning requires no intervention of the network user or an ISE administrator, provided that you configure the ISE and the end-user client to support automatic provisioning.

The latest EAP-FAST version supports two different in-band PAC provisioning configuration options:

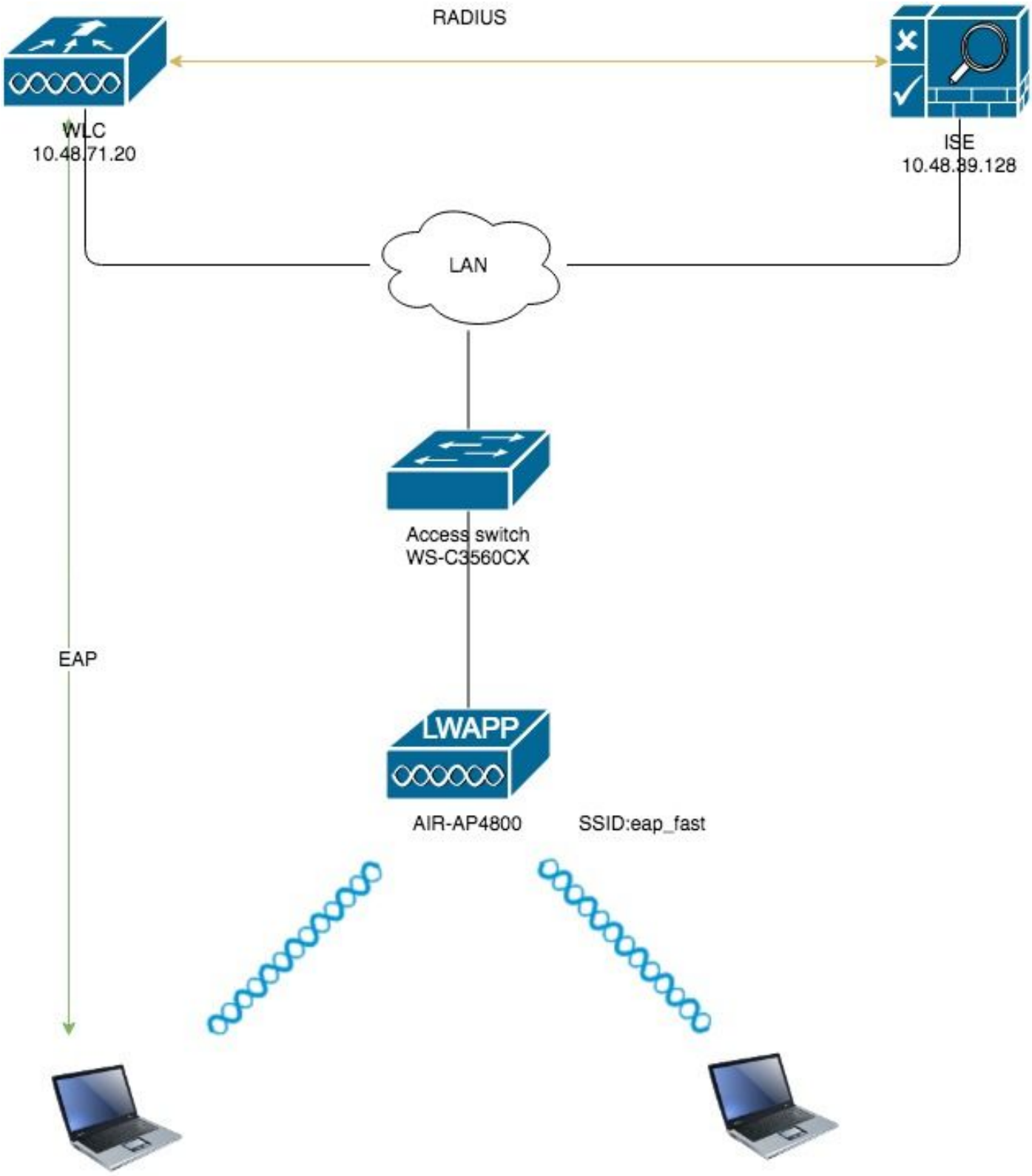
- **Anonymous In-band PAC provisioning**
- **Authenticated In-band PAC provisioning**

Note: This document discusses these in-band PAC provisioning methods and how to configure them.

Out-of-band/Manual PAC provisioning requires an ISE administrator to generate PAC files, which must then be distributed to the applicable network users. Users must configure end-user clients with their PAC files.

Configure

Network Diagram



Configurations

Configure the WLC for EAP-FAST Authentication

Perform these steps in order to configure the WLC for EAP-FAST authentication:

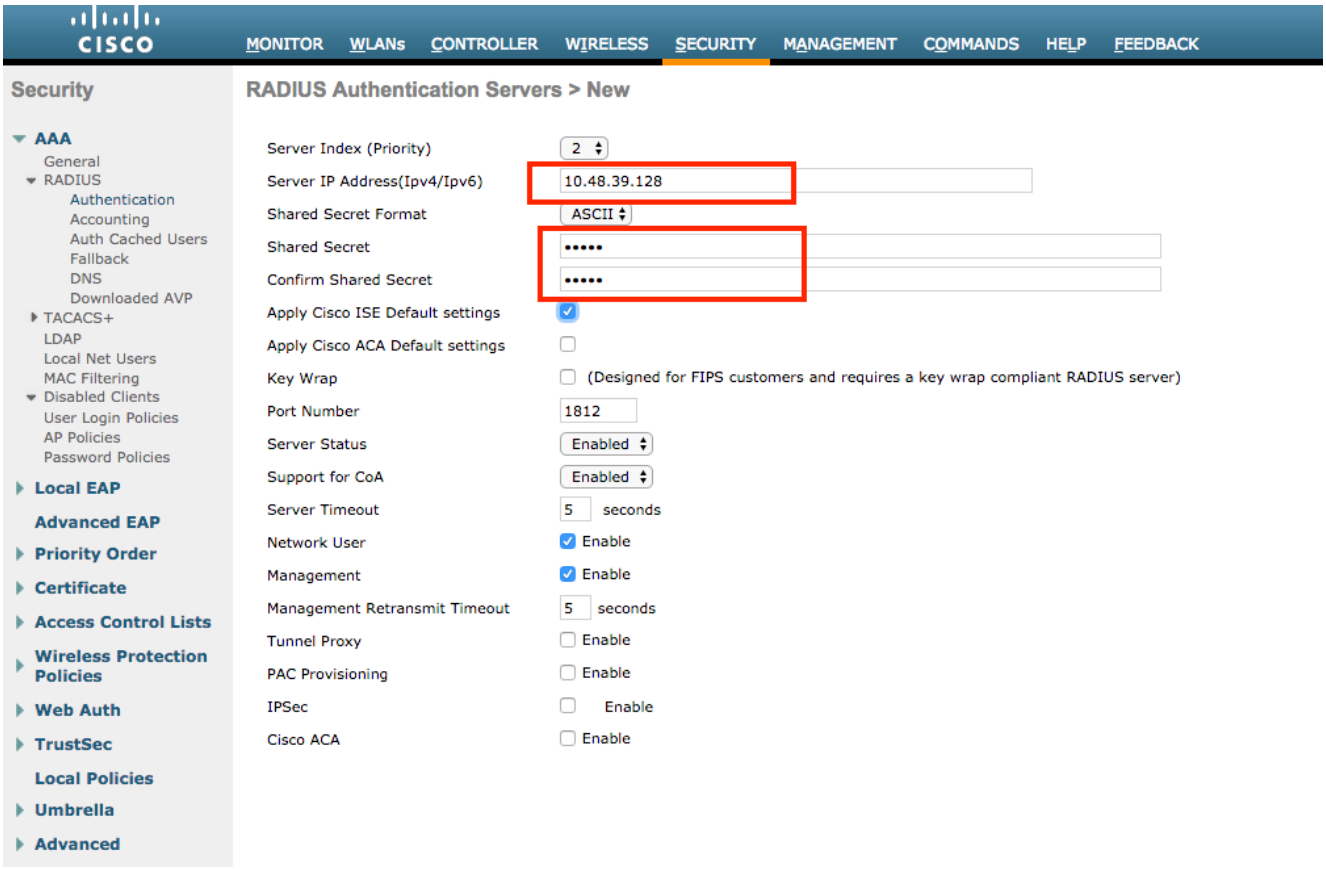
1. Configure the WLC for RADIUS Authentication through an External RADIUS Server
2. Configure the WLAN for EAP-FAST Authentication

Configure the WLC for RADIUS Authentication through an External RADIUS Server

The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials using EAP-FAST and provides access to the wireless clients.

Complete these steps in order to configure the WLC for an external RADIUS server:

1. Choose **Security** and **RADIUS Authentication** from the controller GUI to display the RADIUS Authentication Servers page. Then, click **New** in order to define a RADIUS server.
2. Define the RADIUS server parameters on the **RADIUS Authentication Servers > New** page. These parameters include:RADIUS Server IP AddressShared SecretPort NumberServer StatusThis document uses the ISE server with an IP address of 10.48.39.128.



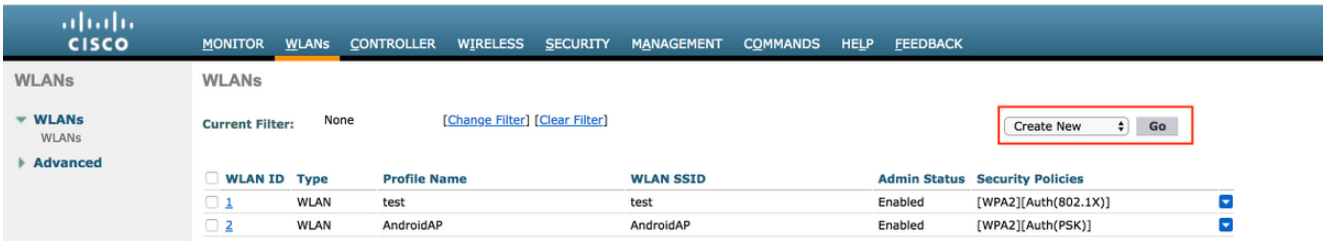
3. Click **Apply**.

Configure the WLAN for EAP-FAST Authentication

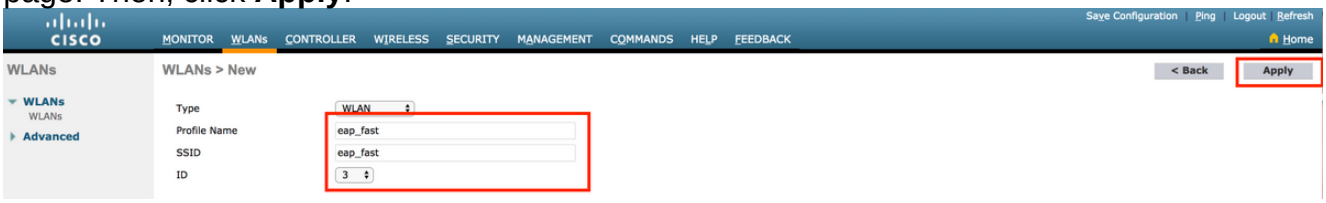
Next, configure the WLAN which the clients use to connect to the wireless network for EAP-FAST authentication and assign to a dynamic interface. The WLAN name configured in this example is **eap fast**. This example assigns this WLAN to the management interface.

Complete these steps in order to configure the **eap fast** WLAN and its related parameters:

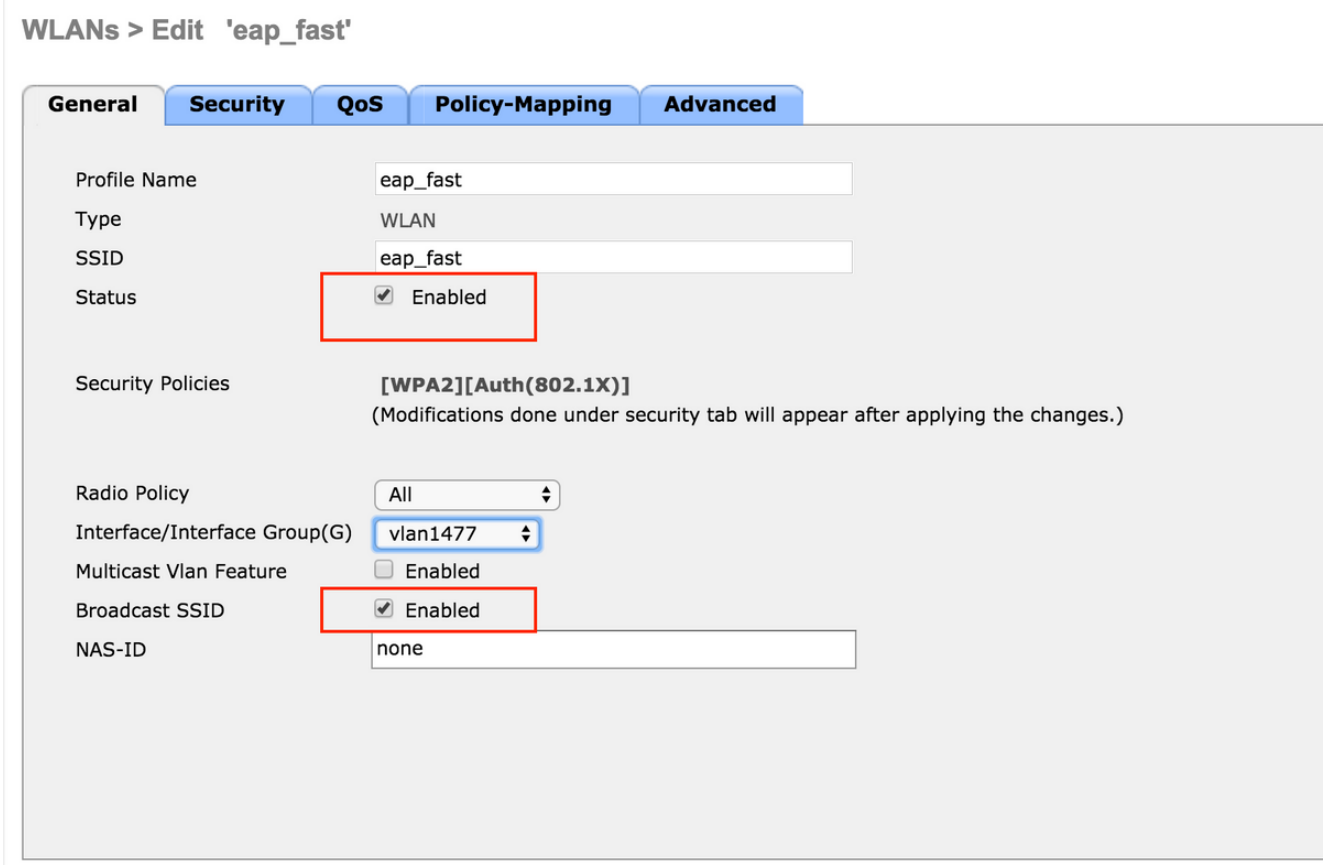
1. Click **WLANs** from the GUI of the controller in order to display the WLANs page.This page lists the WLANs that exist on the controller.
2. Click **New** in order to create a new WLAN.



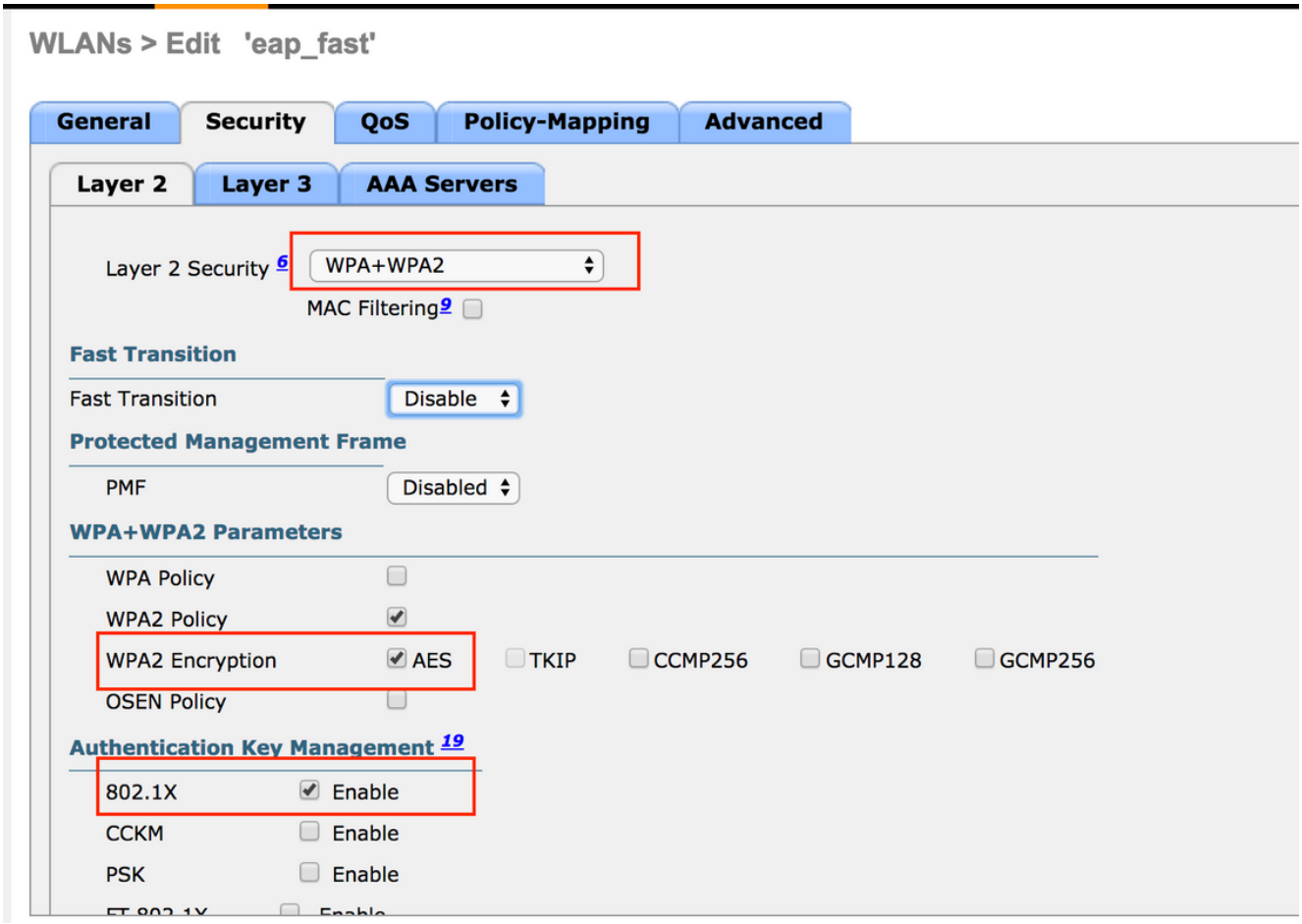
3. Configure the **eap_fast** WLAN SSID name, profile name and WLAN ID on the WLANs > New page. Then, click **Apply**.



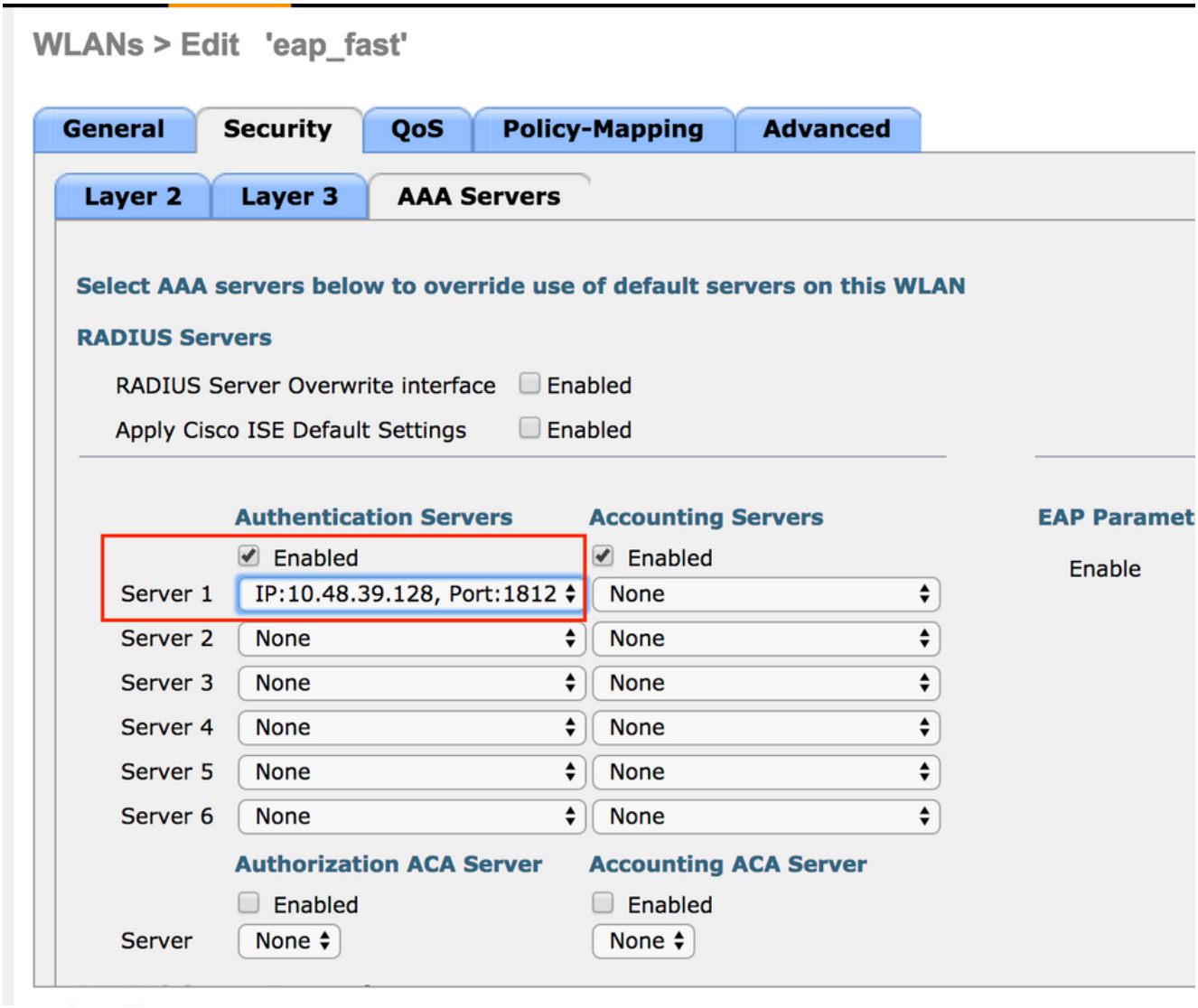
4. Once you create a new WLAN, the **WLAN > Edit** page for the new WLAN appears. On this page, you can define various parameters specific to this WLAN. This includes General Policies, RADIUS Servers, Security Policies, and 802.1x Parameters.
5. Check the **Admin Status** check box under **General Policies** tab in order to enable the WLAN. If you want the AP to broadcast the SSID in its beacon frames, check the **Broadcast SSID** check
box.



6. Under "**WLAN -> Edit -> Security -> Layer 2"** tab choose WPA/WPA2 parameters and select dot1x for AKM.
   This example uses WPA2/AES + dot1x as Layer 2 security for this WLAN. The other parameters can be modified based on the requirement of the WLAN network.



7. Under "**WLAN -> Edit -> Security -> AAA Servers"** tab choose the appropriate RADIUS server from the pull-down menu under RADIUS Servers.



8. Click **Apply**.**Note:** This is the only EAP setting that needs to be configured on the controller for EAP authentication. All other configurations specific to EAP-FAST need to be done on the RADIUS server and the clients that need to be authenticated.

Configure the RADIUS Server for EAP-FAST Authentication

Perform these steps in order to configure the RADIUS server for EAP-FAST authentication:

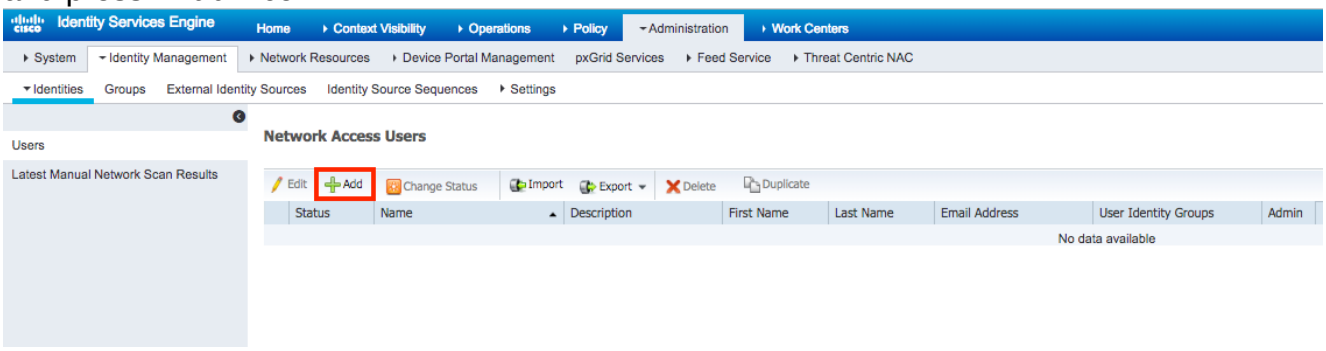
1. Create a User Database to Authenticate EAP-FAST Clients
2. Add the WLC as AAA Client to the RADIUS Server
3. Configure EAP-FAST Authentication on the RADIUS Server with Anonymous In-band PAC Provisioning
4. Configure EAP-FAST Authentication on the RADIUS Server with Authenticated In-band PAC Provisioning

Create a User Database to Authenticate EAP-FAST Clients

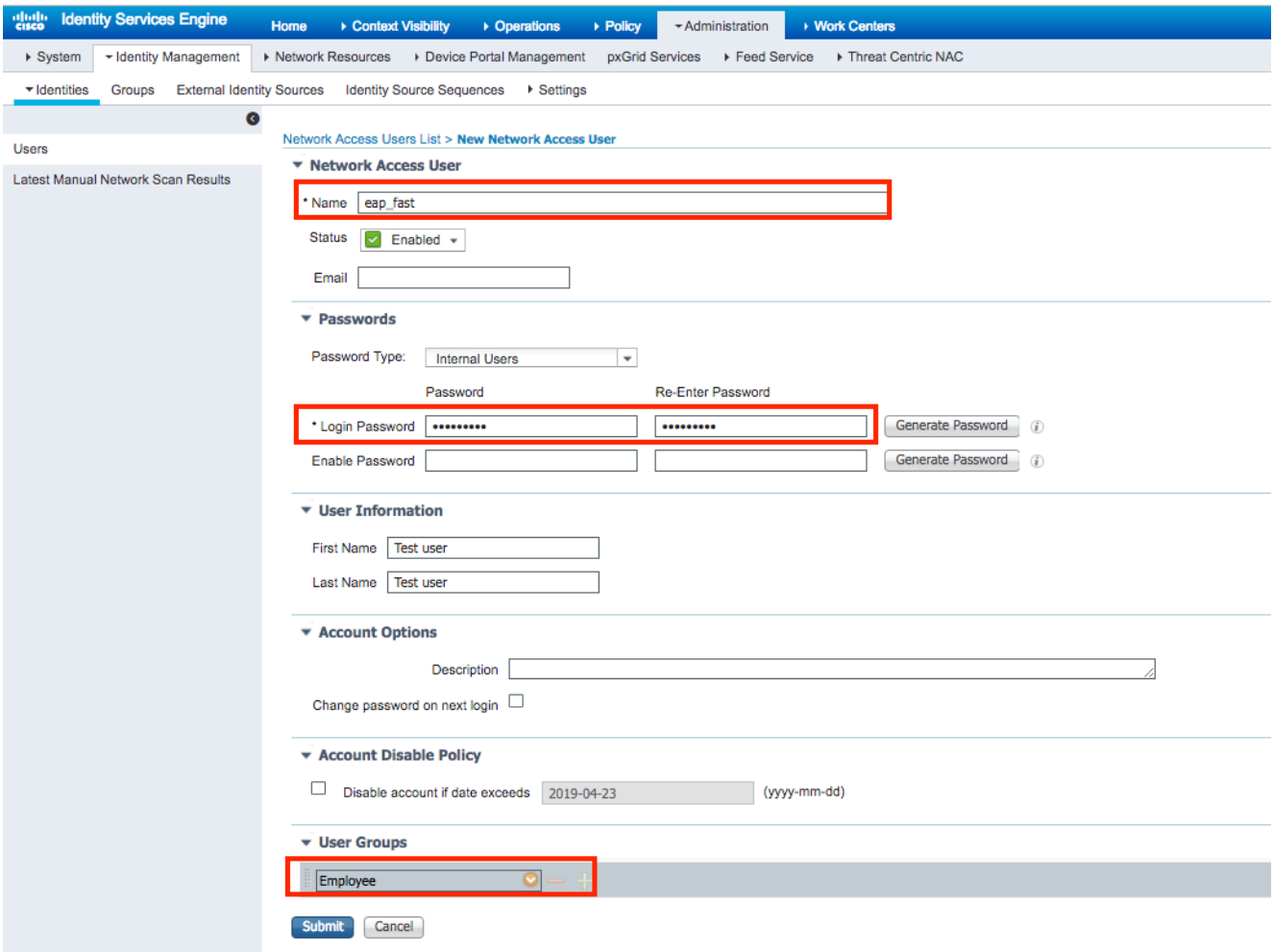
This example configures username and password of the EAP-FAST client as <*eap_fast*> and <*EAP-fast1*>, respectively.

1. In ISE Web admin UI navigate under **"Administration -> Identity Management -> Users"**

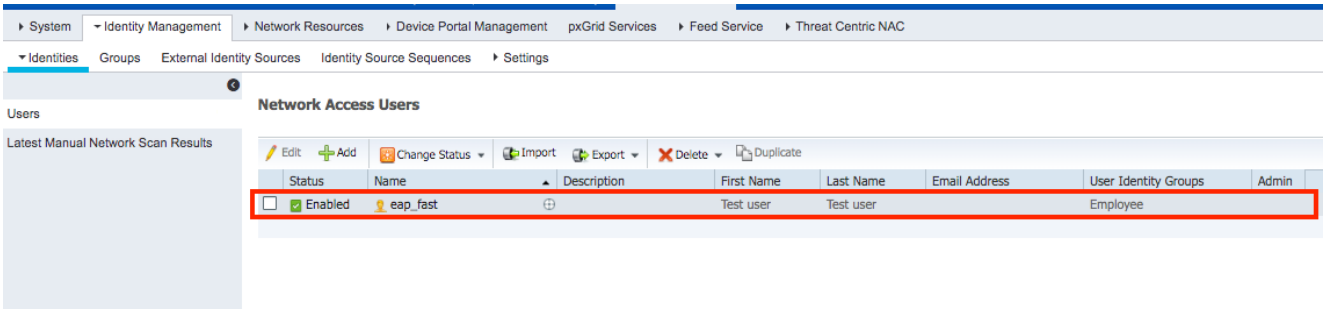
and press **"Add"** icon.



2. Fill in required forms for user to be created - "**Name**" and "**Login password**" and select **"User group"** from drop down list;[optionaly you can fill other information for the user account]
   Press "**Sumbit**"



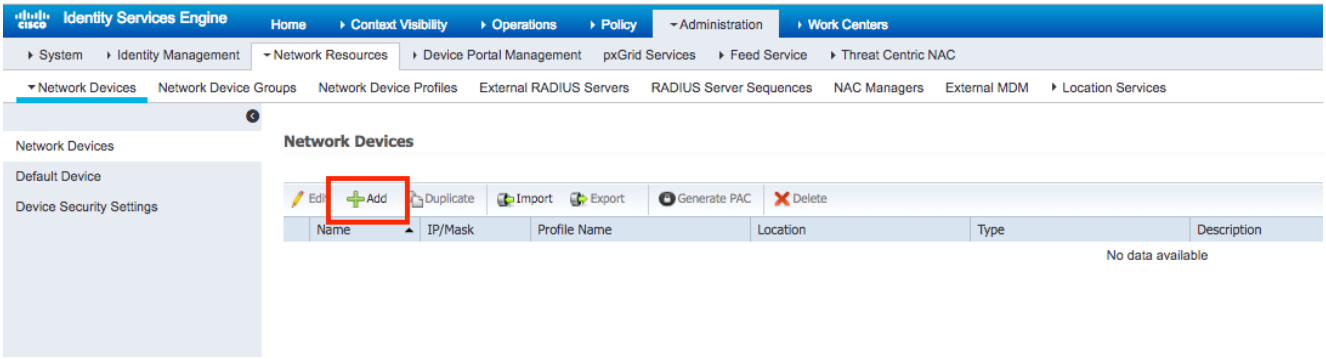
3. User is created.



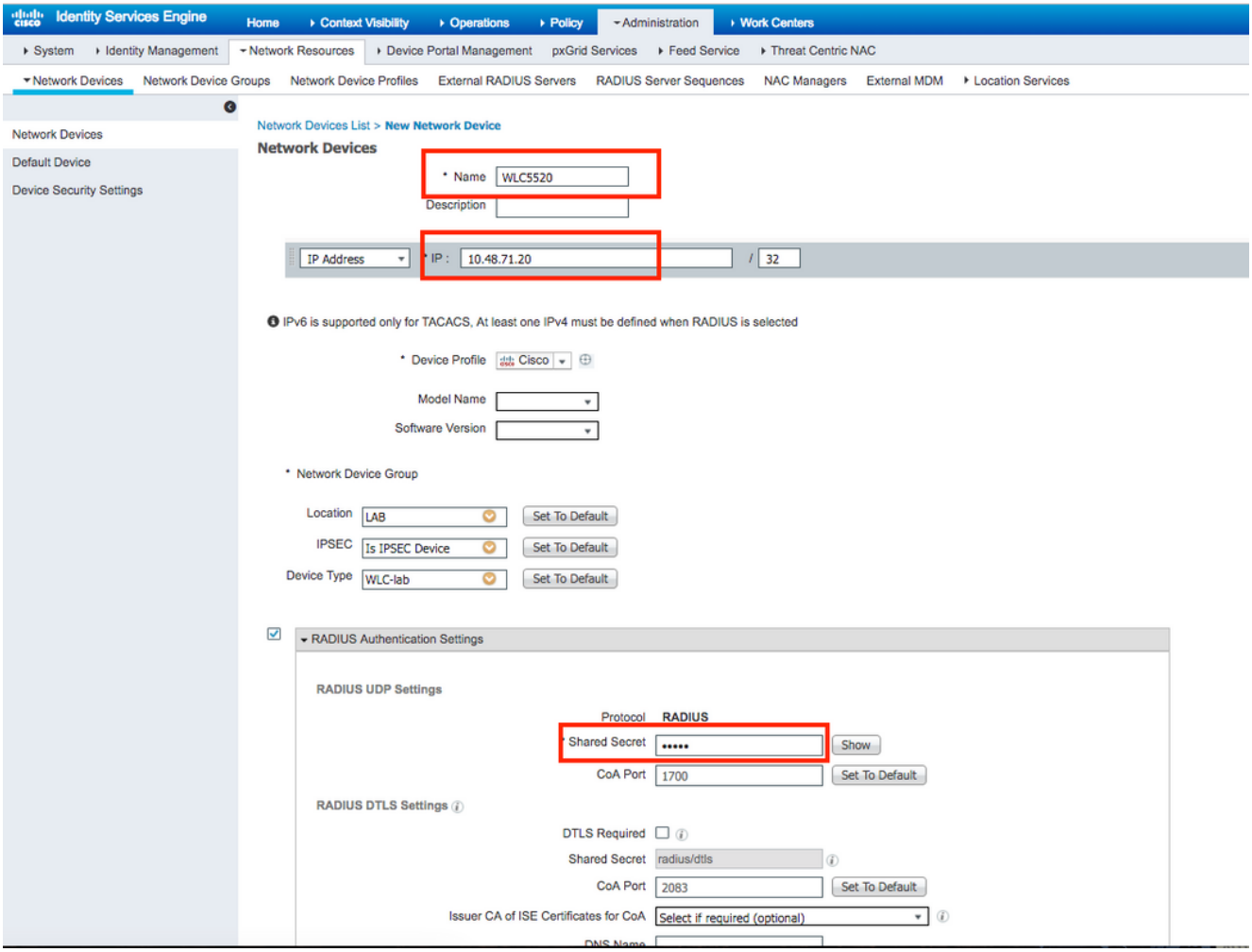
Add the WLC as AAA Client to the RADIUS Server

Complete these steps in order to define the controller as an AAA client on the ACS server:

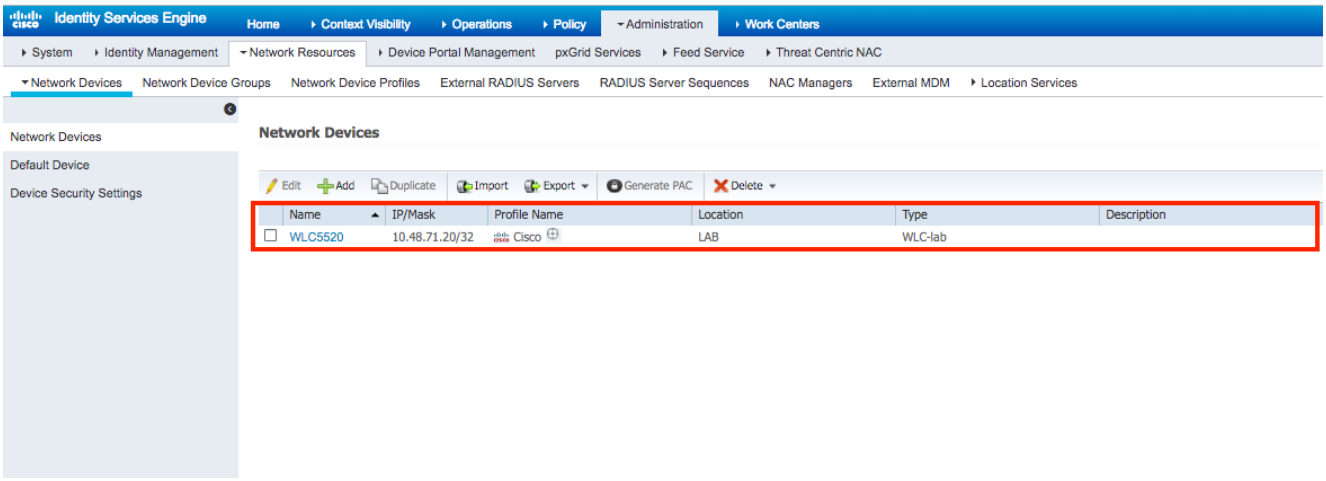
1. In ISE Web admin UI navigate under **"Administration -> Network Resources -> Network Devices"** and press **"Add"** icon.



2. Fill in required forms for device to be added - "**Name**", "**IP"** and configure same shared secret password, as we configured on WLC in earlier section, in "**Shared Secret**" form [optionaly you can fill other information for the device such as location, group, etc]. Press "**Sumbit**"



3. Device is added to ISE Network access device list. (NAD)

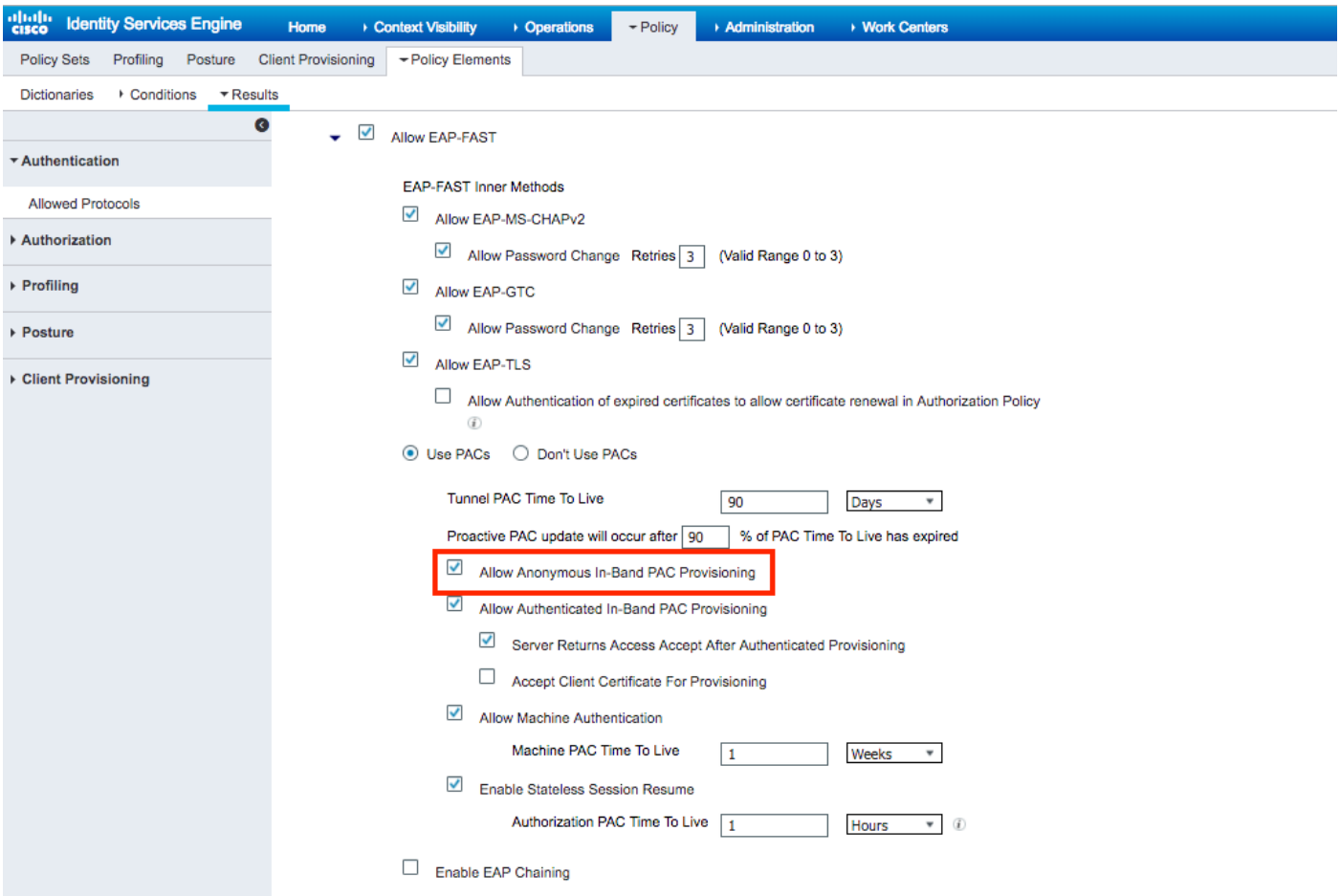


Configure EAP-FAST Authentication on the RADIUS Server with Anonymous In-band PAC Provisioning

Generally one would like to use this type of method in case they don't have PKI infrastructure in their deployment.

This method operates inside an Authenticated Diffie-HellmanKey Agreement Protocol (ADHP) tunnel before the peer authenticates the ISE server.

To support this method we need to enable ""**Allow Anonymous In-band PAC Provisioning**" on ISE under the "**Authentication Allowed Protocols**":



Note: Ensure you have allowed password type authetnication, like EAP-MS-CHAPv2 for EAP-FAST inner method, since obviously with Anonymous In-band Provisioning we can't use any

certificates.

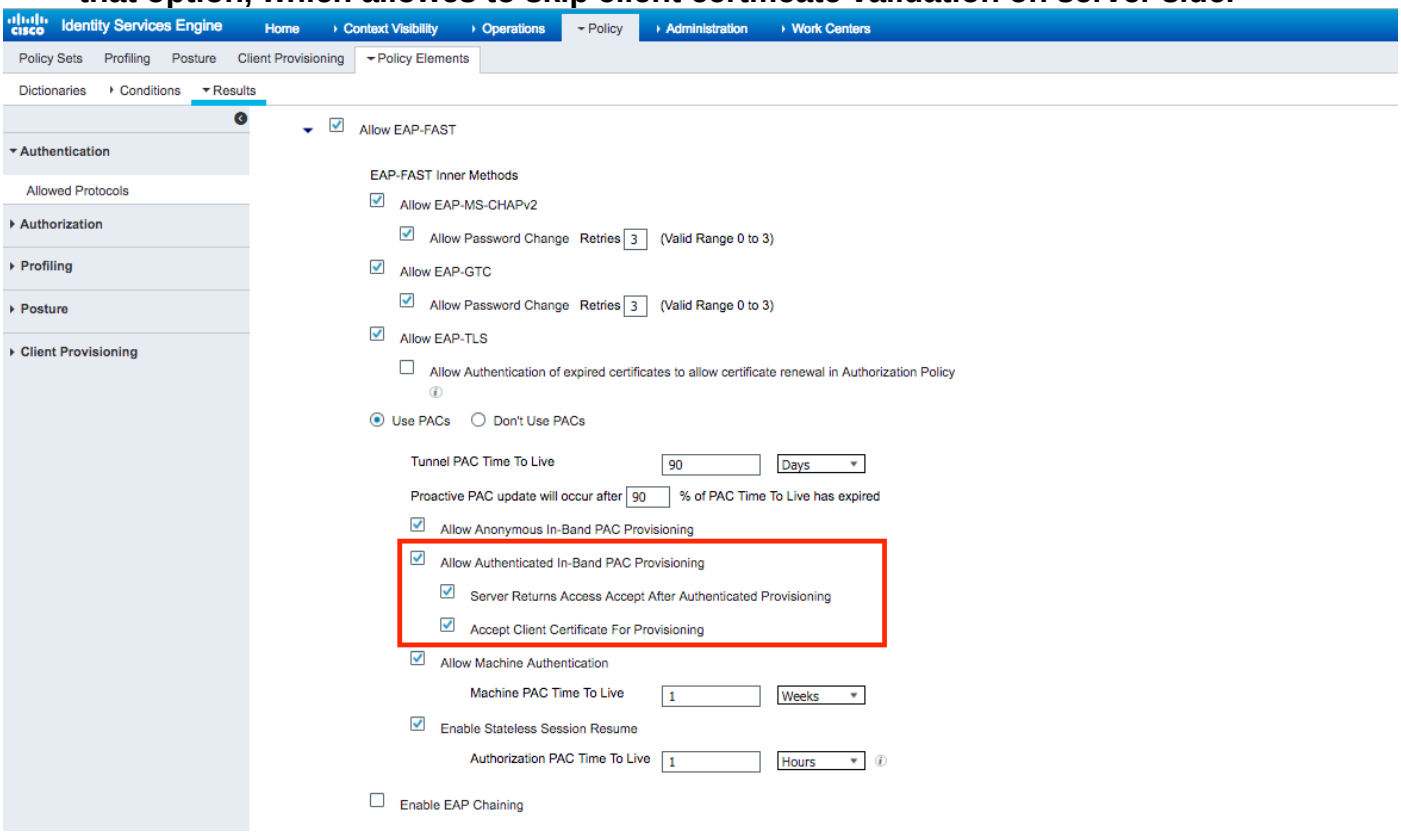
Configure EAP-FAST Authentication on the RADIUS Server with Authenticated In-band PAC Provisioning

This is the most secure and recommended option. The TLS tunnel is built based on the server certificate which is validated by the supplicant and cleint certificate is validated by ISE (default).

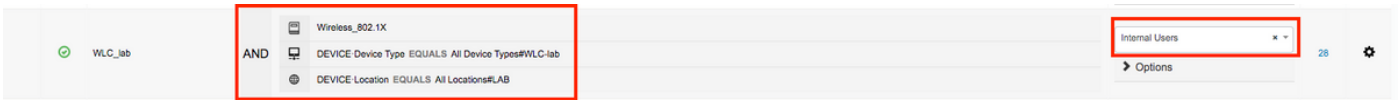
That option requires to have PKI infrastructure for client and server, though it may be limitted to server side only or skipped on both sides.

On ISE there are two additional options for Authenticated In-band provisioning:

1. **"Server Returns Access Accept After Authenticated Provisioning**" - Normally, after PAC provisioning, an Access-Reject should be sent forcing the supplicant to reauthenticate using PACs. However since PAC provisioning is done in authenticated TLS tunnel we can immeditelly respond with Access-Accept to minimize authentication time. (in such case make sure that you have trusted certificates on cleint and server side).
2. **"Accept Client Certificate For Provisioning" - if one doesn't want to provide PKI infrastructure to client devices and only have trusted certificate on ISE, then enable that option, which allowes to skip client certificate validation on server side.**



On ISE we also define simple authentication policy set for wireless users, below example is using as conidtion parameter device type and location and authenticaiton type, authenticaiton flow matching that condition will be validated against internal user database.



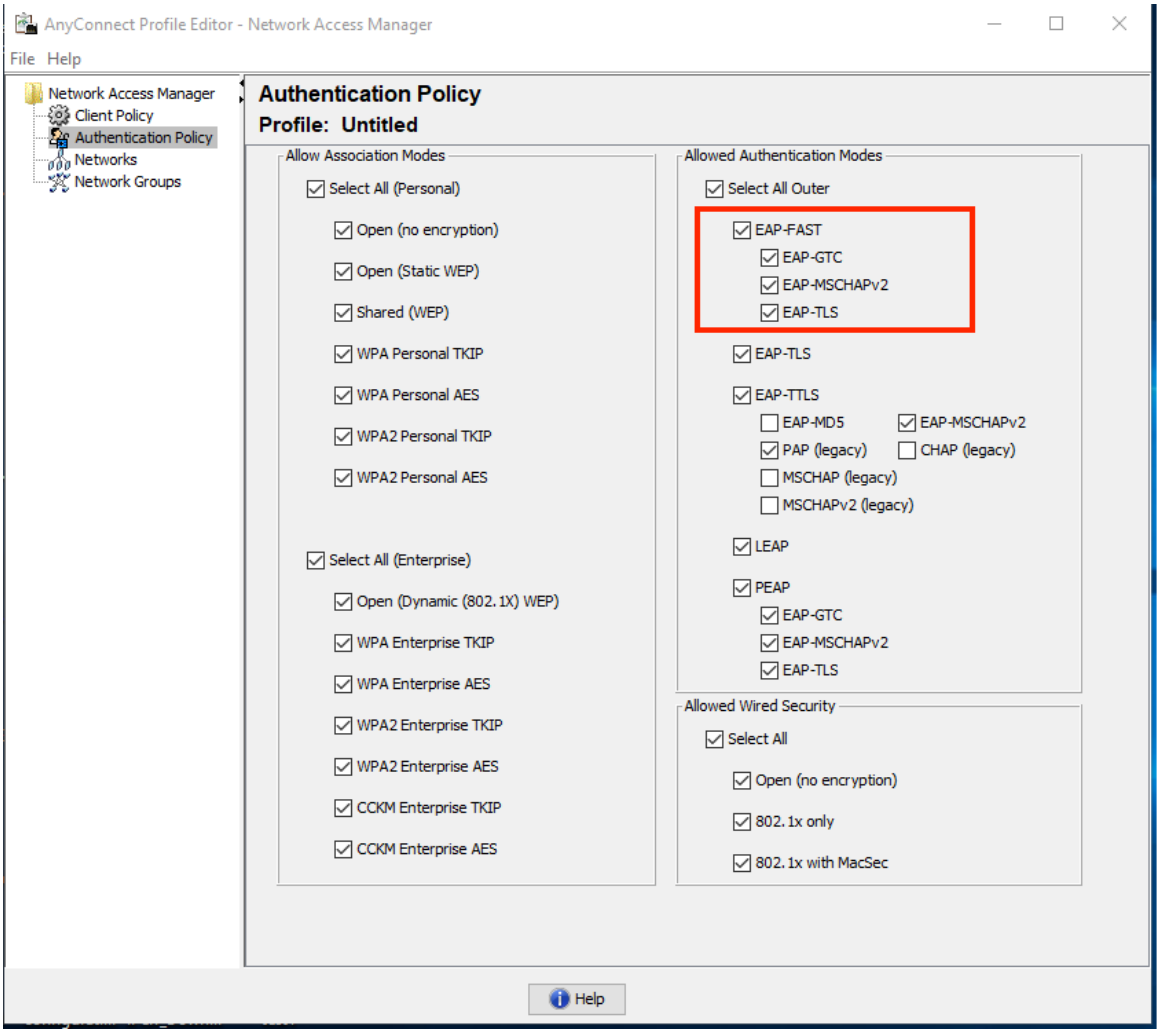
Verify

This example will show Authenticated In-band PAC Provisioning flow andNetwork Access Manager(NAM) configuration settings along with respective WLC debugs.

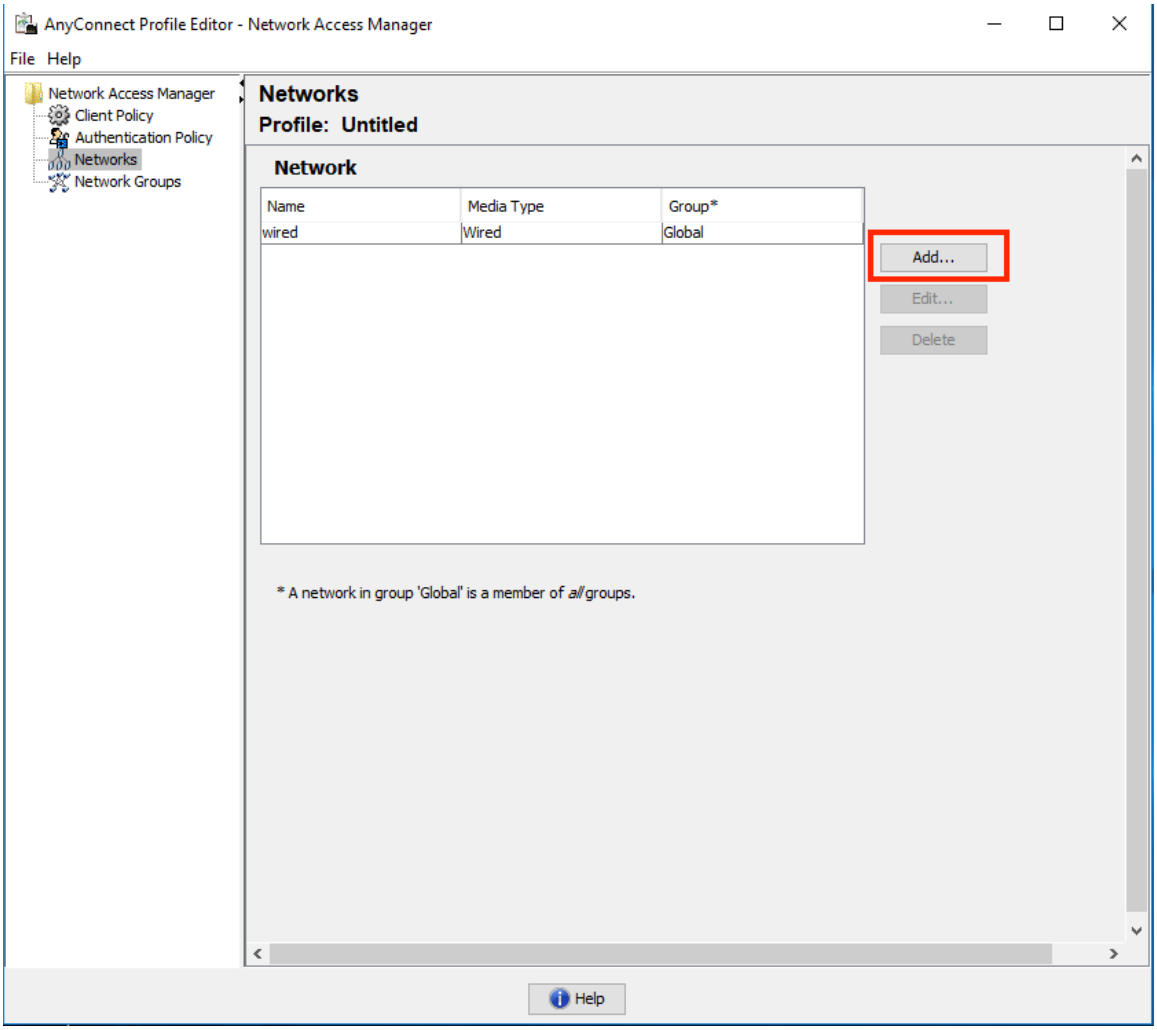
NAM profile configuration

Following steps need to be done in order to configure Anyconnect NAM profile to authenticate user session against ISE using EAP-FAST:

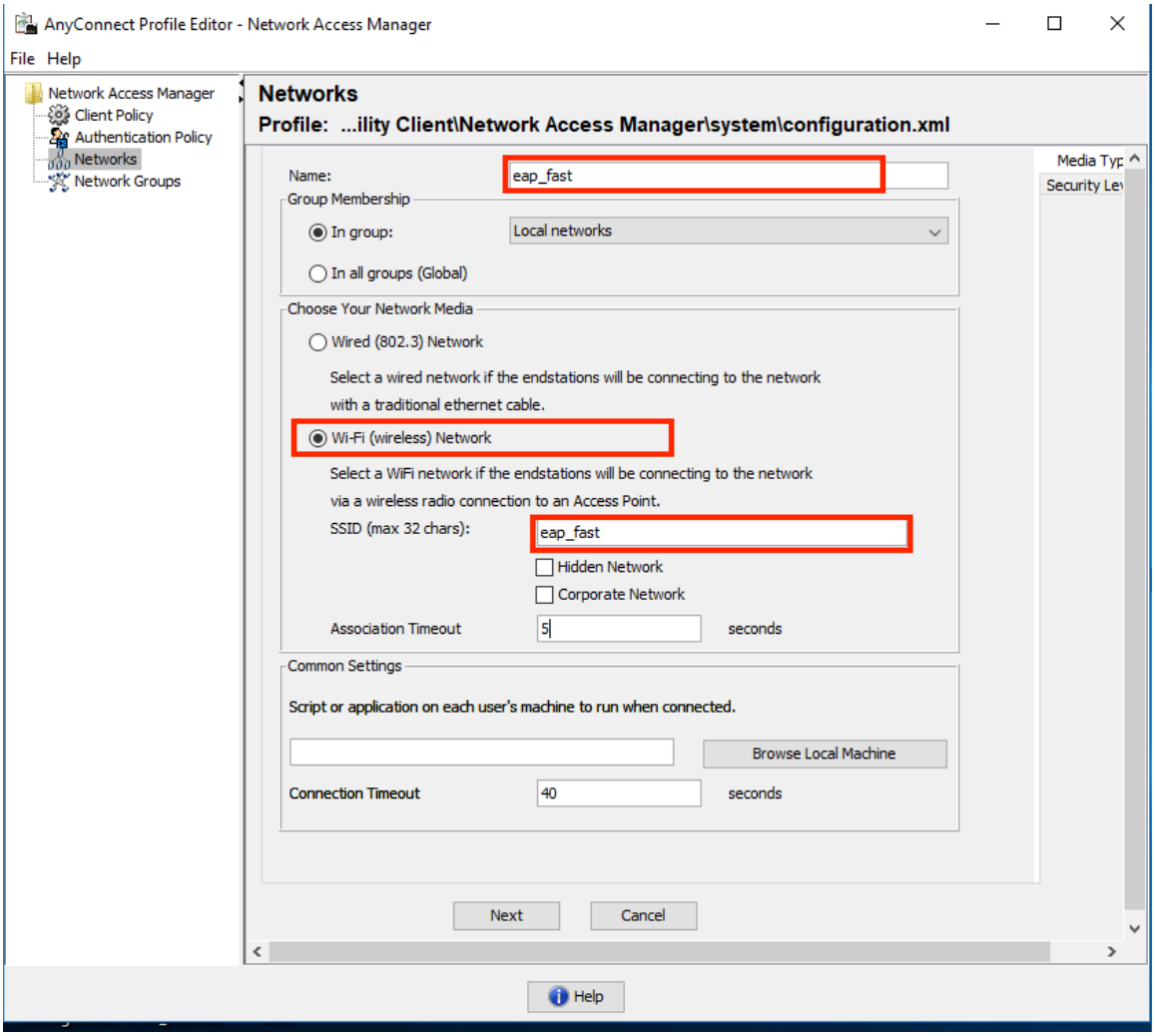
1. Open Network Access Manager Profile Editor and load current configuration file.
2. Make sure that "**EAP-FAST**" is enabled under **"Allowed Authentication Modes"**



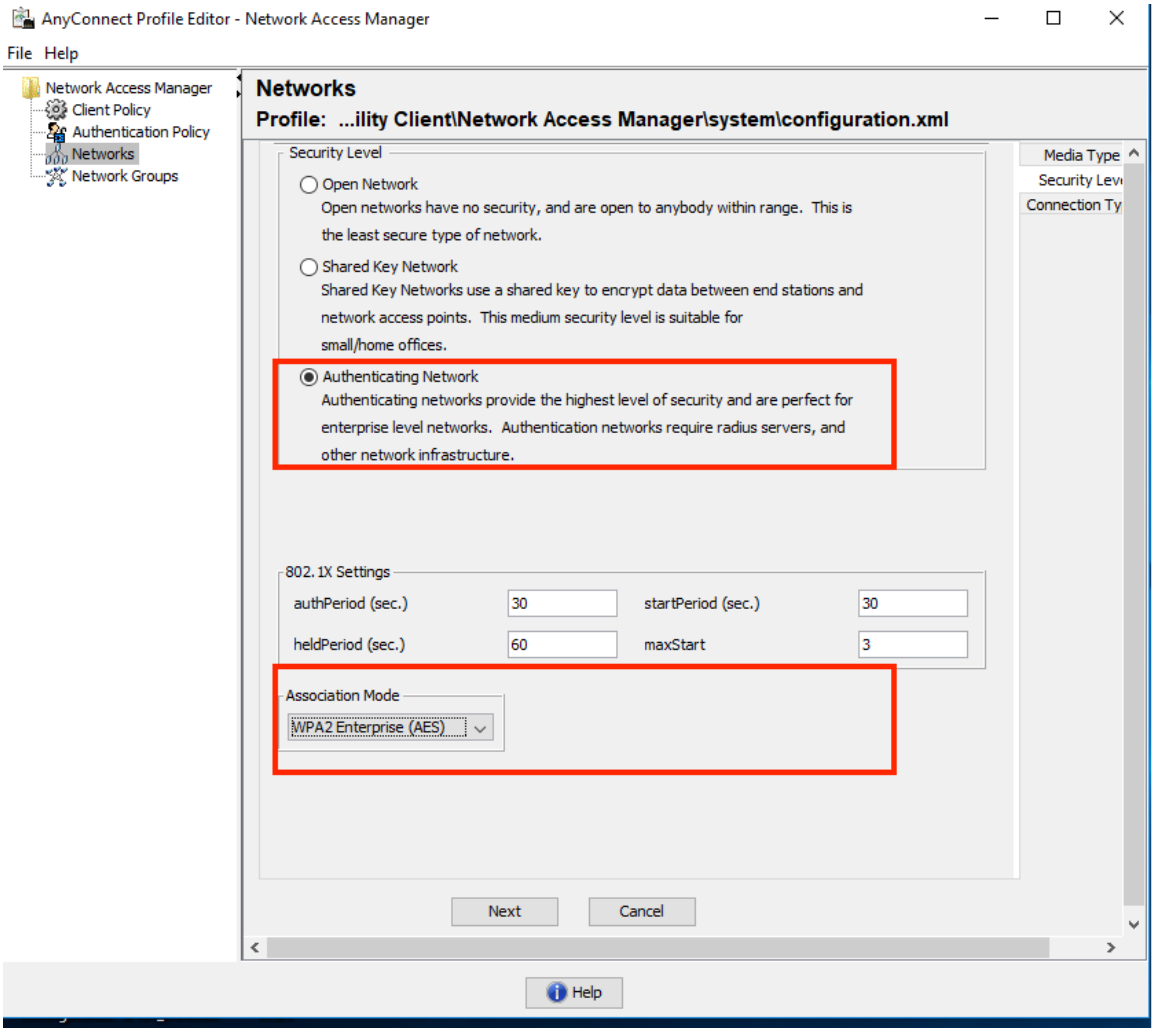
3. "**Add"** a new network profile:



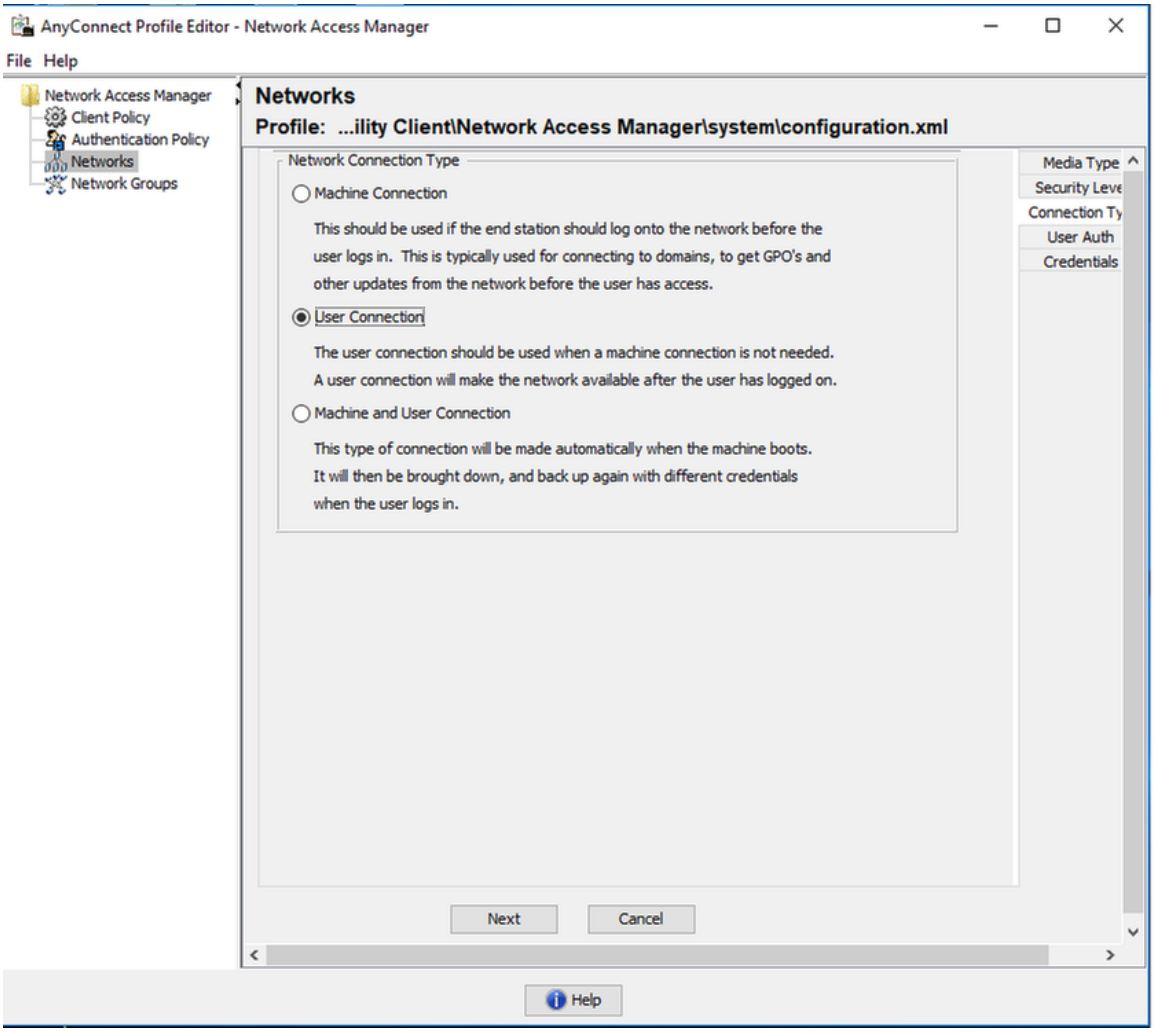
4. Under **"Media type"** configuration section define profile "**Name**", wireless as your media network type and specify SSID name.



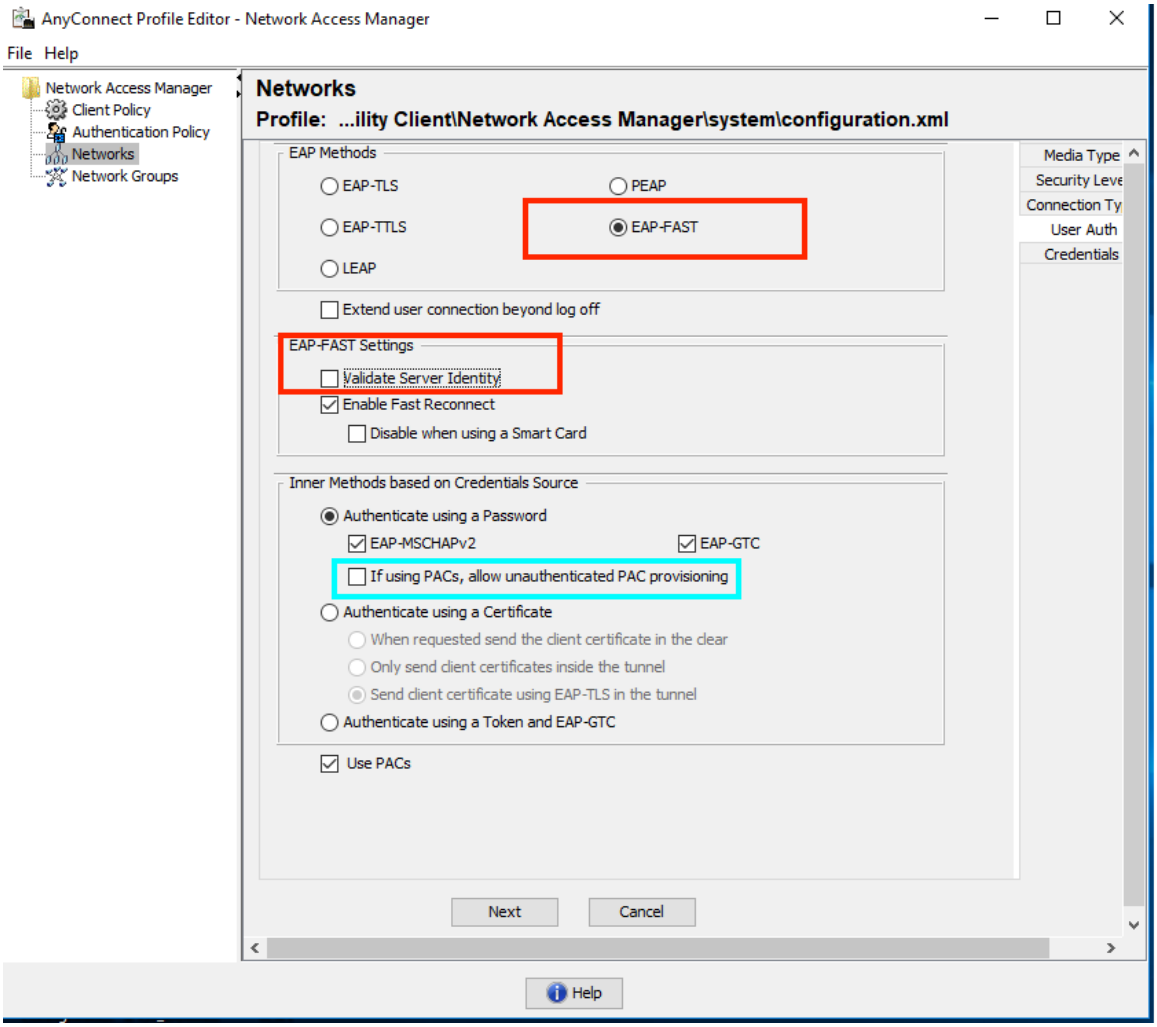
5. Under "**Security Level**" configuration tab select "Authenticating Network" and specify association mode as WPA2 Enterprise (AES)



6. In this example we are using user type authentication, therefor under next tab "**Connection type**" select "**User Connection"**

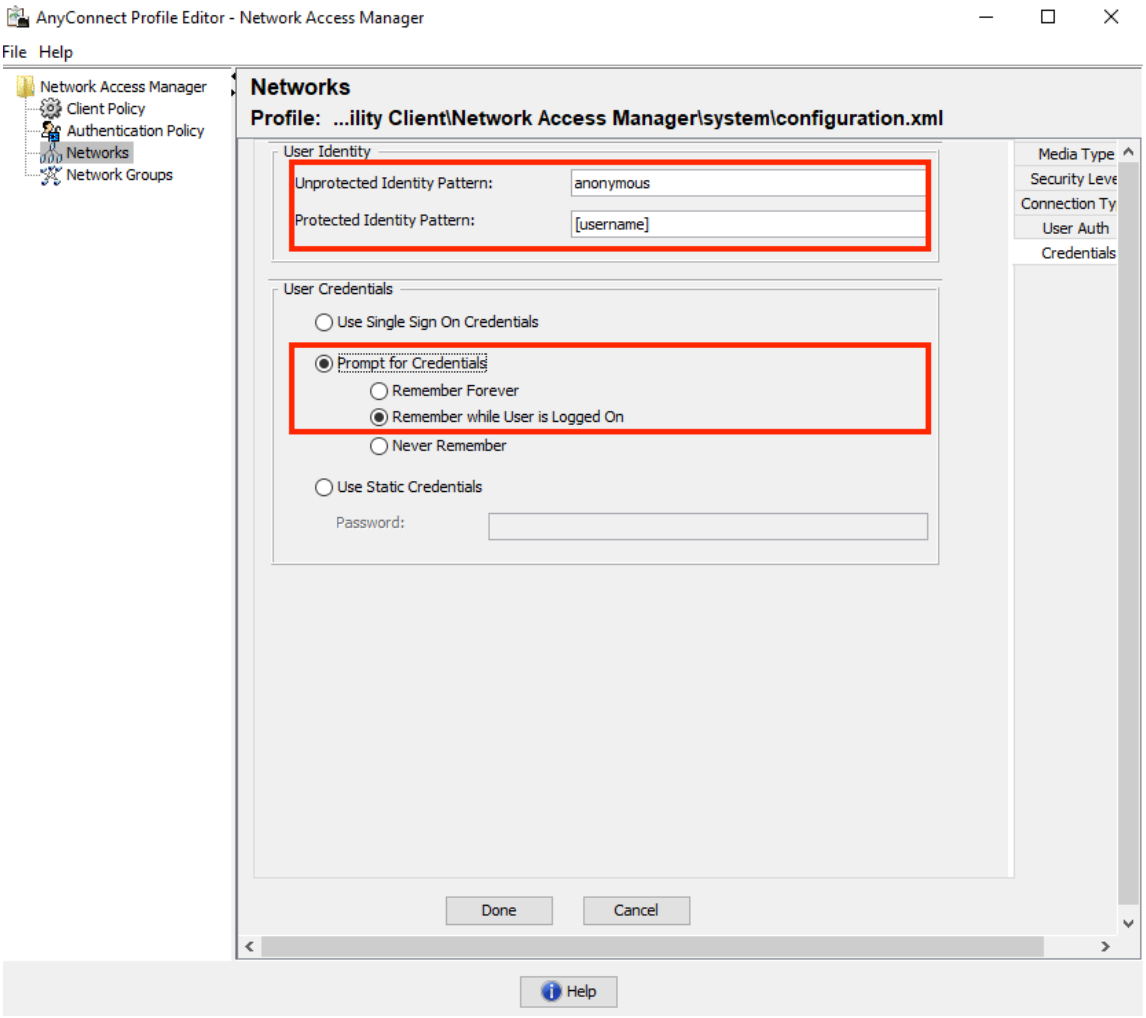


7. Under "**User Auth**" tab specify EAP-FAST as allowed authentication method and disable server certificate validation, since we aren't using trusted certificates in this example.



Note: in real production enviroment ensure that you have trusted certificate installed on ISE and keep server certificate validation option enabled in NAM settings.
Note: option "If using PACs, allow unauthenticated PAC provisioning" has to be selected only in case of Anonymous In-band PAC Provisioning.

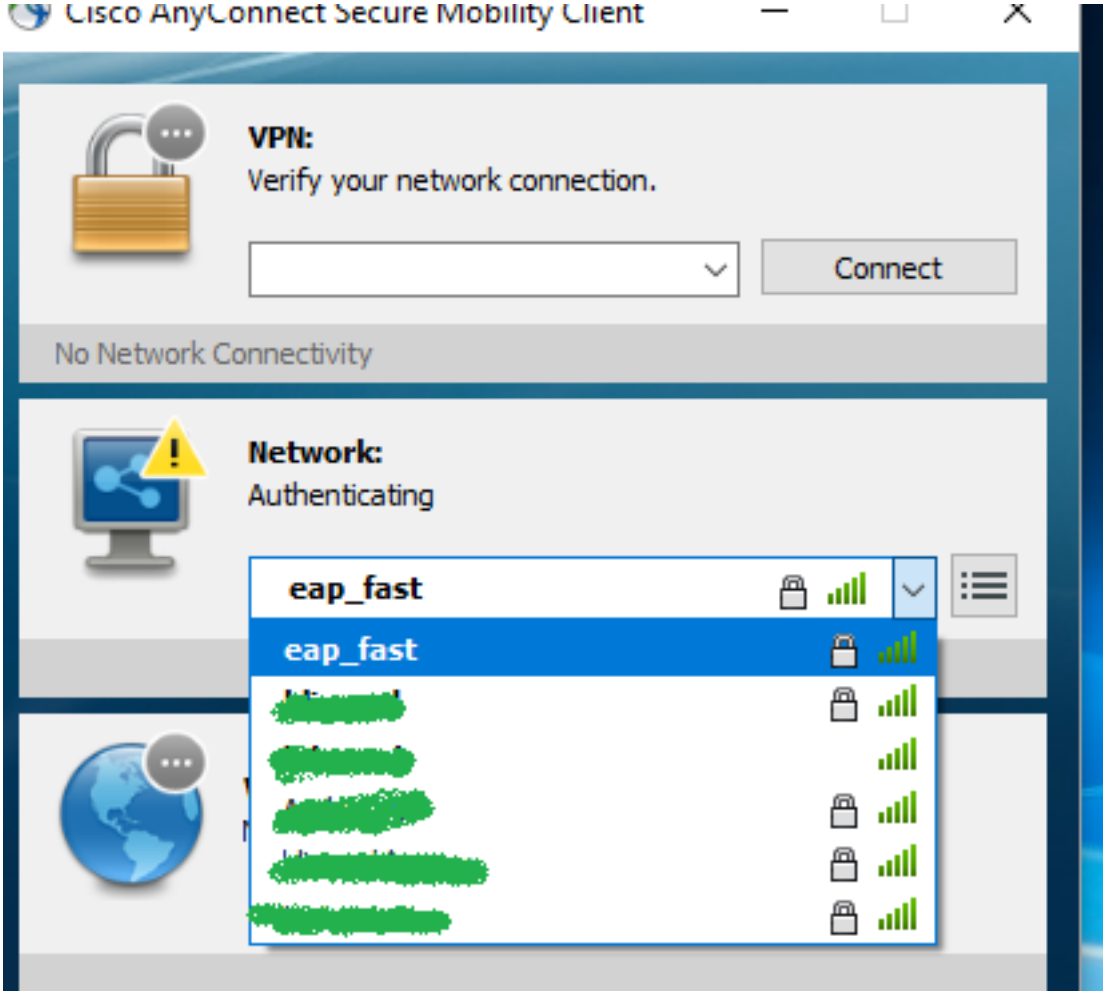
8. Define user credentials, either as SSO in case you willing to use same credentials as used for login, or select "Prompt for credentials" in case you want user to be asked for credentials while connecting to network, or define static credentials for that access type. In this example we are prompting user for credentials at connection attempt to network.



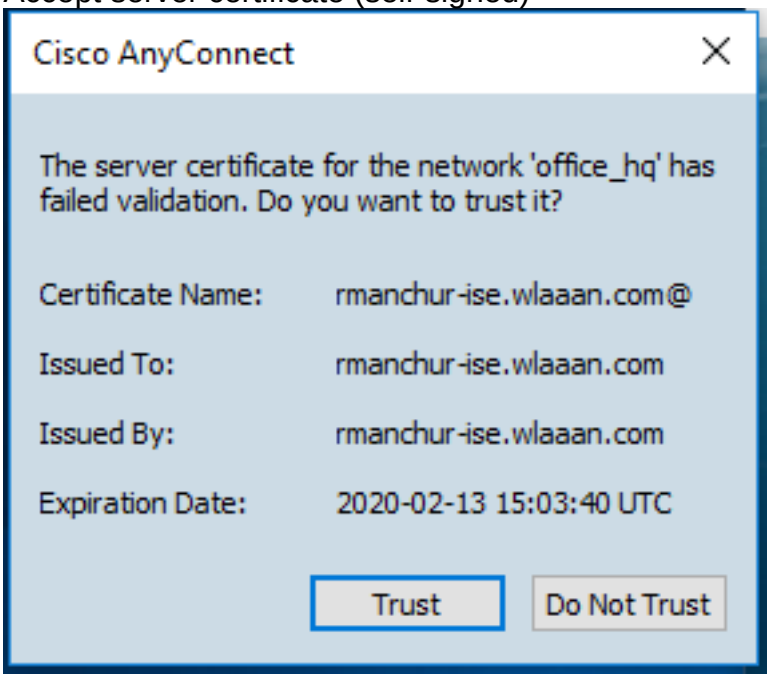
9. Save configured profile under respective NAM folder.

Test connectivity to SSID using EAP-FAST authentication.

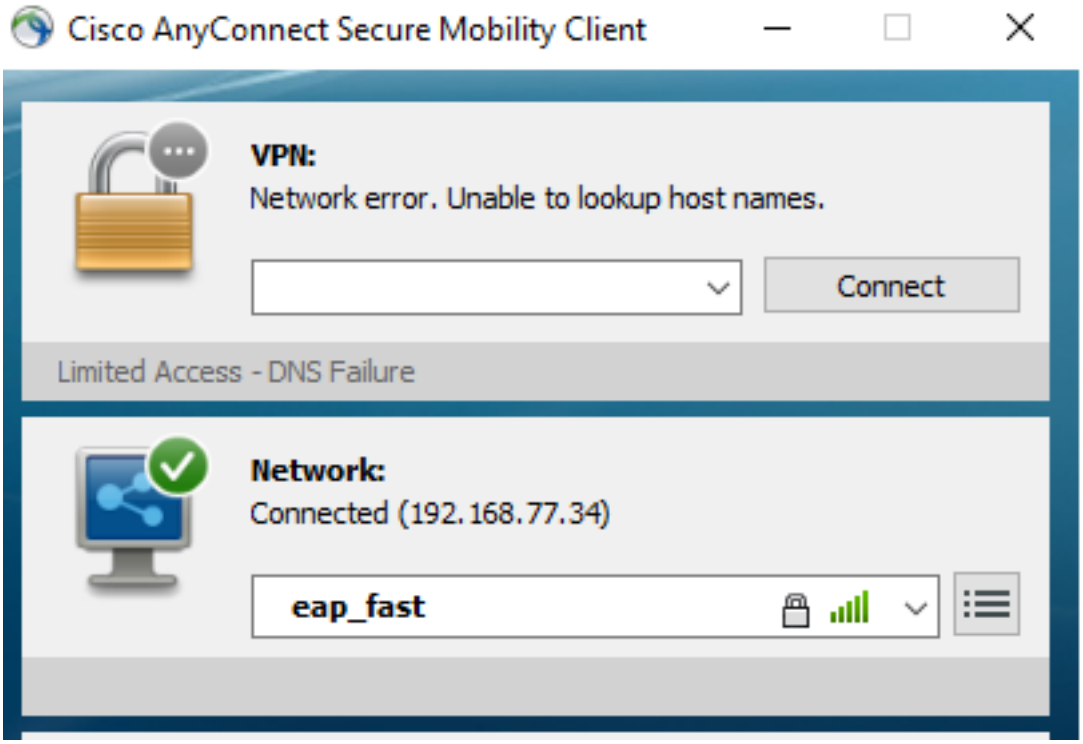
1. Select respective profile from Anyconnect network list



2. Enter username and password required for authentication
3. Accept server certificate (self-signed)



4. Done



ISE authentication logs

ISE authentication logs showing EAP-FAST and PAC provisioning flow can be seen under "**Operations -> RADIUS -> Live Logs**" and can be looked in more details using "**Zoom**" icon:

1. Client has started authentication and ISE was proposing EAP-TLS as authenticaiton method, but client rejected and proposed EAP-FAST instead, that was the method both client and ISE agreed on.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. TLS handshake started between client and server to provided protected enviroment for PAC exchange and was completed succcesfully.

12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12810 Prepared TLS ServerDone message
12811 Extracted TLS Certificate message containing client certificate
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request (⏰ Step latency=13317 ms)
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded

3. Inner authentication started and user credentials were validated successfully by ISE using MS-CHAPv2 (username / password based authentication)