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

Contents

Introduction **Prerequisites** Requirements **Components Used Conventions Background Information** PAC PAC Provisoning Modes Configure **Network Diagram** Configurations Configure the WLC for EAP-FAST Authentication Configure the WLC for RADIUS Authentication through an External RADIUS Server Configure the WLAN for EAP-FAST Authentication Configure the RADIUS Server for EAP-FAST Authentication Create a User Database to Authenticate EAP-FAST Clients Add the WLC as AAA Client to the RADIUS Server Configure EAP-FAST Authentication on the RADIUS Server with Anonymous In-band PAC Provisioning Configure EAP-FAST Authentication on the RADIUS Server with Authenticated In-band PAC Provisioning Verify NAM profile configuration Test connectivity to SSID using EAP-FAST authentication. **ISE** authentication logs WLC side debug on succesfull EAP-FAST flow **Troubleshoot**

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 <u>Cisco Technical Tips Conventions</u> 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 <u>How EAP-FAST works</u> 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.
- 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.

cisco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u> (ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBAČK
Security	RADIUS Authenticat	ion Servers	s > New					
Security AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Advanced EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced	RADIUS Authenticat Server Index (Priority) Server IP Address(Ipv4/I Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default s Apply Cisco ACA Default Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Tunnel Proxy PAC Provisioning IPSec Cisco ACA	ion Servers	s > New 2 10.48.39.128 ASCII (Designed (Designed 1812 Enabled Enabled Enable	for FIPS custon	ners and requires a	a key wrap compl	liant RADI	IUS server)
• · · · · ·								

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.

،،ا،،،ا،، cısco	MONITOR WLANS	<u>C</u> ontroller W <u>i</u> reless <u>S</u>	ECURITY MANAGEMENT	C <u>O</u> MMANDS HELP <u>F</u> EEDBACK		
WLANs	WLANs					
VLANS	Current Filter: N	Ione [Change Filter] [Cle	ear Filter]		Create New 🛟 Go	
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
	1 WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]	
	2 WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]	

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

ahaha	,			Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER WIRELESS SECURITY MANAGEME	NT COMMANDS HELP FEEDBACK	🔒 <u>H</u> ome
WLANs	WLANs > New			< Back Apply
 ✓ WLANS WLANS ▶ Advanced 	Type Profile Name SSID ID	WLAN \$ eap_fast eap_fast 3 \$]	

- 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.
- 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.

LANs > E	dit 'eap_fa	st'			
General	Security	QoS	Policy-Mapping	g Advanced	
Profile Na	me	eap	_fast		
Туре		WL	AN		
SSID		eap	o_fast		
Status			Enabled		
Security I	Policies	[W	PA2][Auth(802.1)	()]	
		(Mo	difications done und	er security tab will ap	opear after applying the changes.)
Radio Pol	icy	All	\$		
Interface,	Interface Group	(G) vla	an1477 🛟		
Multicast	Vlan Feature		Enabled		
Broadcast	t SSID	e	Enabled		
NAS-ID		non	e		

 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.

LANs > E	dit 'eap_fa	ast'					
General	Security	QoS	Policy-Mapp	oing Adva	nced		
Layer 2	Layer 3	AAA Se	rvers				
Layer 2	Security 🧧 🚺 M4	VPA+WPA2 C Filtering					
Fast Trans	ition						
Fast Transit	ion	Disal	ole 🗘				
Protected	Management	Frame					
PMF		Disat	oled 🖨				
WPA+WPA	2 Parameter	S					
WPA Po	licy						
WPA2 P	olicy		_				
WPA2 E	ncryption	AES	🗌 ТКІР	CCMP256	GCMP128	GCMP256	
OSEN P	olicy		_				
Authentica	ation Key Man	agement ¹	9				
802.1X		Enable					
ССКМ		Enable	_				
PSK		Enable					
-							

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

neral S	Security	QoS	Policy-	Mapping	Advanced		
ayer 2	Layer 3	AAA S	ervers				
ADIUS Serv RADIUS Se	ervers belo v ers erver Overwa	w to over	r ride use (ce 🔲 Ena	o f default se bled	rvers on this V	VLAN	
Apply Cisco	o ISE Defaul	t Settings	🗌 Ena	bled			
Apply Cisco	O ISE Defaul	t Settings	Ena	Accounting	Servers		EAP P
Apply Cisco Server 1	Authentica	t Settings ation Serv 39.128, Po	ers	Accounting Content Enabled None	Servers	\	EAP P Ena
Apply Cisco Server 1 Server 2	Authentica Contraction Contra	t Settings ation Serv 39.128, Po	Ena rers rt:1812 \$	Accounting Contemporal Enabled None None	Servers	¢ \$	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3	Authentica Contraction Authentica Contraction Authentica Contraction Contract	t Settings ntion Serv 39.128, Po	Ena rers rt:1812 \$ \$ \$	Accounting Contractions Accounting Contractions Accounting None None None	Servers	 	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica Contraction Authentica Contraction Authentica Contraction Contraction None None None	t Settings ntion Serv 39.128, Po	Ena ers ert:1812 \$ \$ \$	Accounting Contractions Accounting Contractions Accounting Contractions None None None None	Servers	 <	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Constraints Authentica Constraints Constraints None None None None	t Settings ntion Serv 39.128, Po	Ena	Accounting Contempose	Servers	 <	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Authentica Control Enabled IP:10.48.2 None None None None None None	t Settings ntion Serv 39.128, Po	Ena	Accounting Enabled None None None None None None None	Servers	 <	EAP P Ena

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"



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"

dentity 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 Identities	ntity Sources Identity Source Sequences + Settings
(9
Users	Network Access User List > New Network Access User
Latest Manual Network Scan Results	Name eap_fast Status
	▼ Passwords
	Password Type: Internal Users 💌
	Password Re-Enter Password
	* Login Password Generate Password (j)
	Enable Password Generate Password
	▼ User Information
	First Name Test user
	Last Name Test user
	▼ Account Options
	Description
	Account Disable Policy
	Disable account if date exceeds 2019-04-23 (yyyy-mm-dd)
	✓ User Groups
	Employee 📀 — 🕂
	Submit Cancel
. User is created.	
F System ▼Identity Management F N	letwork Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC
✓Identities Groups External Identity S	Jources Identity Source Sequences + Settings
0	Network Access Users
Users	
Ladst Manual Network Scan Results	/ Edit 🗍 Add 🔀 Change Status • 🕼 Import 🕼 Export • 🗙 Delete • 🖓 Duplicate
E CONTRACTOR E CONTRA	Status Name Description First Name Last Name Email Address User Identity Groups Admin Image: Status Image: Status </td

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.



 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"

Identity Services Engine	Home	y → Operations → Policy	-Administration	Work Centers	
System Identity Management	- Network Resources > De	vice Portal Management pxGrid S	Services Feed Service	Threat Centric NAC	
Network Devices Network Device	Groups Network Device Prof	iles External RADIUS Servers	RADIUS Server Sequences	NAC Managers External MDM	Location Services
G					
Network Devices	Network Devices List > Network Devices	w Network Device			
Default Device	Network Devices	* Name WECEE20			
Device Security Settings		Description			
	IP Address	P: 10.48.71.20		/ 32	
	IPv6 is supported only	for TACACS, At least one IPv4 must	be defined when RADIUS i	is selected	
		* Device Profile 🚓 Cisco 👻 🕀			
		Model Name 👻	1		
	s	ioftware Version 🗸]		
			-		
	 Network Device Gro 	pup			
	Location LAB	Set To Defa	ult		
	IPSEC IS IPSE	C Device 🛇 Set To Defa	ult		
	Device Type WLC-la	b 📀 Set To Defa	ult		
	RADIUS Authent	ication Settings			
	RADIUS UDP S	ettings			
		_	Protocol RADIUS		
		' Share	ed Secret	Show	
			CoA Port 1700	Set To Default	
	RADIUS DTLS	Settings (j)			
		DTLS	Required 🗌 (i)		
		Share	ed Secret radius/dtls	۲	
			CoA Port 2083	Set To Default	
		Issuer CA of ISE Certificates	s for CoA Select if require	d (optional) *	
		D	NS Name		

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":

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	Client Provisioning - Policy Elements
Dictionaries + Conditions - Resul	Its
G	- Ilow EAP-FAST
▼Authentication	
Allowed Protocols	EAP-FAST Inner Methods
Authorization	
▶ Profiling	
▶ Posture	Allow Password Change Retries 3 (Valid Range 0 to 3)
Client Provisioning	
	 Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)
	Use PACs O Don't Use PACs
	Tunnel PAC Time To Live
	Proactive PAC update will occur after 90 % of PAC Time To Live bas expired
	Allow Anonymous In-Band PAC Provisioning
	Allow Authenticated In-Band PAC Provisioning
	Server Returns Access Accest After Authenticated Provisioning
	Machine PAC Time To Live
	Enable Stateless Session Resume
	Authorization PAC Time To Live 1 Hourse
	Enable EAP Chaining

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:

- "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.

CISCO	Identity	Services	s Engine		Home)	Context Visibility	 Operations 	→ Policy	 Administration 	Work Centers
Policy S	Sets P	rofiling	Posture	Clie	nt Provisioning	→ Policy Elements	5			
Dictiona	aries	Conditio	ns ▼R	esults	•					
				0	→ 🗹	Allow EAP-FAST				
▼ Auther	tication									
Allowe	ed Protoc	ols				EAP-FAST Inner	Methods			
▶ Author	ization							Detries 2		2
▶ Profilin	na						Password Change	Retries 3	(valid Range 0 to 3	3)
						Allow EAP-				
▶ Postur	e					Allow I	Password Change	Retries 3	Valid Range 0 to 3	3)
Client	Provisio	ning				Allow EAP-	ILS			
						Allow	Authentication of	expired certific	ates to allow certificat	te renewal in Authorization Policy
						Use PACs	O Don't Use P/	Cs		
						Tunnel PA	C Time To Live		90	Days *
						Proactive	PAC update will o	occur after 90	% of PAC Time	e To Live has expired
						Allow	v Anonymous In-E	and PAC Pro	visioning	
						Allov	v Authenticated Ir	-Band PAC P	rovisioning	
							Server Returns A	ccess Accept	After Authenticated P	Provisioning
							Accept Client Ce	rtificate For Pr	rovisioning	
						Allow	v Machine Auther	tication		
							Machine PAC Tir	ne To Live	1	Weeks *
						Enat	ole Stateless Sess	sion Resume		
							Authorization PA	C Time To Live	e 1	Hours *
						Enable EAF	^o Chaining			

On ISE we also define simple authentication policy set for wireless users, below example is using as conidtion parameter device type and location and authentication type, authentication 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"

AnyConnect Profile Editor	- Network Access Manager	- 🗆 ×								
File Help										
Network Access Manager	Authentication Policy	Authentication Policy								
	Profile: Untitled									
	Allow Association Modes	Allowed Authentication Modes								
Setwork Groups	Select All (Personal)	Select All Outer								
	Open (no encryption)	EAP-FAST								
	Open (Static WEP)	✓ EAP-GTC ✓ EAP-MSCHAPv2								
	Shared (WEP)	EAP-TLS								
	WPA Personal TKIP	EAP-TLS								
	WPA Personal AES									
	WPA2 Personal TKIP	PAP (legacy) CHAP (legacy)								
	WPA2 Personal AES	MSCHAP (legacy)								
	Select All (Enterprise)	LEAP								
	Open (Dynamic (802.1X) WEP)	PEAP EAP-GTC								
	WPA Enterprise TKIP	EAP-MSCHAPv2								
	WPA Enterprise AES	EAP-TLS								
	WPA2 Enterprise TKIP	Allowed Wired Security								
	WPA2 Enterprise AES									
	CCKM Enterprise TKIP									
	CCKM Enterprise AES									
		≥ 802. 1x with MacSec								
	() Help									

3. "Add" a new network profile:

🕍 AnyConnect Profile Editor	- Network Access Ma	nager		_		×
File Help						
Network Access Manager	Networks Profile: Untit	led				
Networks	Network					^
55	Name	Media Type	Group*		_	
	WIEG	Wired	Giobai	Add		
				Edit		
				Delete		
	* A network in gr	oup 'Global' is a member of <i>all</i> gro	oups.			
						v
	<					>
		() Help				

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

🚰 AnyConnect Profile Editor - Network Access Manager File Help	-		×
Network Access Manager Client Policy Profile:ility Client\Network Access Manager\system\configuration.xml			
Name: eap_fast Group Membership Local networks In all groups (Global) Choose Your Network Media Owner Network (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethermet cable. Image: WiFin (wireless) Network Select a WiFin etwork if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): eap_fast Image: Hidden Network Corporate Network Association Timeout seconds Common Settings Script or application on each user's machine to run when connected. Image: Network 40 Next Cancel		Medi	a Typ ∧ y Lev
🚺 Help			

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

ork Access Manager Client Policy	Networks	
letworks letwork Groups	Security Level Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network. O Shared Key Network Shared Key Network use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices.	Media Type Security Lev Connection Ty
	Authenticating Network Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.	
	802.1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	
	802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3	

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

AnyConnect Profile Editor	- Network Access Manager —		ĸ
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml		
Networks Ketwork Groups	Network Connection Type Machine Connection This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. Image:	Media Type Security Lev Connection T User Auth Credentials	
	Help		

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.

letwork Access Manager Client Policy Authentication Policy	Networks Profile:ility Client\Netw	vork Access Manager\system\configuration	on.xml
Networks	EAP Methods		Media Type
🖏 Network Groups	O EAP-TLS	○ PEAP	Security Leve
			Connection Ty
	C EAP-TILS	() EAP-FAST	User Auth Crodentials
	OLEAP		Credentials
	Extend user connection	beyond log off	
	EAP-FAST Settings		
	Validate Server Identity		
	Enable Fast Reconnect		
	Disable when using a	a Smart Card	
	Inner Methods based on Creden	tials Source	
	 Authenticate using a Pas 	ssword	
	EAP-MSCHAPv2	EAP-GTC	
	If using PACs, allow	unauthenticated PAC provisioning	
	Authenticate using a Cer	rtificate	
	O When requested ser	nd the client certificate in the clear	
	Only send client cert	tificates inside the tunnel	
	 Send client certificat 	te using EAP-TLS in the tunnel	
	 Authenticate using a Tok 	ken and EAP-GTC	
	Use PACs		
	Ne	ext Cancel	

Note: in real production environment 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.

	×

_

AnyConnect Profile Editor - Network Access Mar	ager
--	------

works User Identity			 Media Type 4
vork Groups	entity Pattern:	anonymous	Security Leve
			Connection Ty
Protected Ident	ity Pattern:	[username]	 User Auth
			Credentials
User Credentials			
🔿 Use Singl	e Sign On Credentials		
Prompt for	or Credentials		
OF	Remember Forever		
a 🔘	Remember while User is	s Logged On	
0	lever Remember		
	r Credentials		
O use state			
Password	:		
	Dana	Canaal	
	Done	Cancel	

9. Save configured profile under respective NAM folder.

Test connectivity to SSID using EAP-FAST authentication.

1. Select respective profile from Anyconnect network list

S Cisco AnyCo	onnect Secure Mobility Client	_	· 🗆	X
	VPN: Verify your network connection.	~	Conne	ect
No Network C	onnectivity			
	Network: Authenticating eap_fast		الله 🖻	, ≡
	eap_fast		- 🖰 al	
			h, A h, A h, A h, A h, A	

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

Cisco AnyConnect		×
The server certificate failed validation. Do y	for the network you want to trus	k 'office_hq' has st it?
Certificate Name:	rmanchur-ise.	wlaaan.com@
Issued To:	rmanchur-ise.	wlaaan.com
Issued By:	rmanchur-ise.	wlaaan.com
Expiration Date:	2020-02-13 1	5:03:40 UTC
	Trust	Do Not Trust

4. Done

🕙 Cisco AnyC	onnect Secure Mobility Client	—		×
	VPN: Network error. Unable to lookup host r	names	s. Connect	
Limited Acces	s - DNS Failure			
	Network: Connected (192.168.77.34) eap_fast	8	atl 🗸 📰	

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-FAS1 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 successfully.

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 (g 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
40000	Despect of TLO 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)