

TrustSec How-To Guide: Deploying EAP Chaining with AnyConnect NAM and Cisco ISE

For Comments, please email: <u>howtoguides@external.cisco.com</u> Current Document Version: 3.0 August 27, 2012

Table of Contents

Table of Contents 2	2
Introduction 3 What Is the Cisco TrustSec System? 3 About the TrustSec How-To Guides 3 What does it mean to be 'TrustSec Certified'? 3	3 3
Executive Summary	5
Overview About This Document Scenario Overview Architecture Software/Hardware Requirements:	5 6 6
Technology Primer	3
Design Parameters	9
Configuring ISE	
Defining Authentication Policies and Authorization Profiles	ļ
Authentication Policies Defining the Authentication Policies Define the Authorization Profiles Defining Authorization Condition Rules and Authorization Policies Creating Authorization Policies	14 16
NAM Installation and Configuration	
Testing Procedure 33 TESTING PROCEDURE 33	
Detailed View of EAP Chaining	
Macintosh, iphone, Android, iPad Devices	2
Frequently Asked Questions	3
Appendix A: References 54 Cisco TrustSec System: 54 Device Configuration Guides: 54	54

What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX ArchitectureTM, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.



About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).



What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "TrustSec "certified". The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Overview

Personal computing devices, such as smartphones and tablets, are appearing in the office whether we want them to or not. These devices are convenient and end-users tend to trade up to newer versions of the devices faster than ever before. To some, these devices are a fashion statement just like jewelry.

Against this backdrop, corporate IT needs to develop real world strategies to cope. It is no longer enough to put out a policy that says no personal devices on the corporate network.

Employee-owned devices can be detected and given a special credential, such as a certificate, to access the network. However, deploying a second credential system is expensive and keeping track of which devices are currently in the endusers possession can be a challenge. An alternate approach would be to detect corporate devices and assume all others are non-corporate devices. The status of a corporate device is reasonably well known.

The crux of the problem is the credential systems that were originally deployed. Username / password, one-time password tokens, and smartcards are all examples of credential systems that can be used on any device. An end-user can just as easily type a username / password into a corporate laptop or into a personal smartphone.

To identify a device as a corporate or non-corporate device requires something, say a credential, which is locked to that particular device. While common wisdom suggests attaching a certificate to a non-corporate device, the more logical choice is to lock a credential to the corporate device and assume all other devices are non-corporate devices.

One solution is EAP Chaining which uses a machine certificate or a machine username / password locked to the device through the Microsoft domain enrollment process. When the device boots, it is authenticated to the network using 802.1X. When the user logs onto the device, the session information from the machine authentication and the user credentials are sent up to the network as part of the same user authentication. The combination of the two indicates that the device belongs to the corporation and the user is an employee.

If the device is not a member of the domain, then the machine authentication fails and the device is not a corporate device. If the device does not support EAP Chaining, then the device is also not a corporate device. In either case, the result would be to treat these devices differently than the corporate device. That could be limited access for employee owned devices and out to the Internet for non-employee devices depending on corporate policy.

About This Document

This document outlines how EAP Chaining can be used to differentiate a corporate Windows device, a personal Windows device, and a personal Android tablet coming onto the network using the same username and password authentication on all devices – corporate and non-corporate.

EAP Chaining requires both a supplicant on the client device and a RADIUS server that support the technology. For the purposes of this document, the Cisco AnyConnect Network Access Manager (NAM) Version 3.1 will be used as the supplicant on the corporate and personal Windows devices. The NAM supports EAP Chaining technology. The native supplicant will be used on the Android tablet. It does not support EAP Chaining technology. The Cisco Identity Services Engine (ISE) Version 1.1.1 also supports EAP Chaining and will be used as the RADIUS server. Detailed requirements are listed in the Software/Hardware Requirements section of this document.

EAP Chaining is enabled in the EAP-FAST protocol as defined on the ISE node (In this document ISE node ad ISE server will be used interchangeably). The NAM configuration profile is also setup to use EAP-FAST as the authentication method and is available for administratively defined networks only. In addition both machine and user connection types must be configured within the NAM configuration profile.

The corporate Windows device will gain full corporate access using the NAM. The personal Windows device will gain access to a restricted network using the same NAM configuration. The personal Android device will gain access to a second restricted showing the power and flexibility of this technology.

Scenario Overview

The Network Access Manager (NAM) will obtain both machine and user credentials from Windows (username/password) before the user logs in or when the user logs out- and after the user logs in, respectively. EAP Chaining will be enabled in the EAP-FAST authentication protocol, once the secure TLS tunnel is established, MS-CHAPv2 will be used for credential exchange between the ISE server and the client. EAP-TLS will not be used nor will X.509 certificates be required.

Figure 1 represents this simple configuration. In this network, there are 3 subnets defined to match three business cases:

- VLAN 1 provides full access to the network, pending successful authentication of both machine and user credentials, which represents and end-user logging into a corporate asset.
- VLAN 22 provides restricted access to the network, pending failure of machine credentials, and successful authentication of user credentials, which represents an end-user logging into a non-corporate device, such as a personal laptop.
- VLAN 12 also provides restricted access to the network representing mobile devices, that DO NOT support EAP Chaining and at the same time is a violation of the corporate security policy

Architecture

Figure 3 Architecture used in this document



Software/Hardware Requirements:

Client:

- Laptop or desktop computer with an Ethernet NIC or WiFi NIC and one of the following operating systems:
 - o Windows 7 SP1 x 86 (32-bit) and x64 (64-bit)
 - o Windows Vista SP2 x86 and x64
 - Windows XP SP3 x86
- Windows Server 2003 SP2 x86
- AnyConnect 3.1 or greater with the Network Access Manager Mobile installed
- AnyConnect 3.1 or greater Profile Editor

Authentication Server:

• Cisco Identity Services Engine (ISE) System 1.1.1 or greater

Network Infrastructure:

• Ethernet switch and /or WiFi access point configured for 802.1X

Technology Primer

EAP-FAST authentication occurs in two phases. In the first phase EAP-FAST employs a TLS handshake to provide and authenticate key exchanges using Type-Length-Values (TLV) objects to establish a protected tunnel. These TLV objects are used to convey authentication related data between the client and server. Once the tunnel is established, the second phase begins with the client and ISE node engaging in further conversations to establish the required authentication and authorization policies.

EAP Chaining employs an optional Identity-Type TLV at the start of the second phase of EAP-FAST authentication.

To accomplish EAP Chaining:

(Note: It is assumed that the PAC files have already been provisioned, and the secure TLS tunnel has been established)

- The ISE server sends the optional Identity-Type TLV, machine or user, and request identity to the client.
- The client responds back with either the same Identity-Type TLV, or proposes another identity-type.

For example, if the device is in Machine context (user has not logged in yet or logged out) and the client receives and Identity-Type TLV with the User identity type, it may respond with a Machine Identity-Type TLV.

The ISE server would recognize whether the client supports EAP Chaining by analyzing the response to the Identity-Type TLV request. If the response contains a matching Identity-Type TLV then the client supports EAP Chaining. In this document, we provide three examples. In the first example, the client matches both Machine and User Identity-Type TLV requests deeming it as a corporate device. This is defined by ISE's authorization compound condition expression "EAPChainingResult Equals User and Machine both succeeded". This will be used for creating an Authorization policy allowing users full network access when logging in with a corporate device. Log details can be found in the Detailed View of EAP Chaining section of this document.

If there is no Identity-Type TLV in the response then EAP Chaining is not supported by the client and normal processing for existing EAP-FAST v1 implementation applies. In the second example provided, the client, being an Android tablet, does not support EAP Chaining and continues with EAP-FAST authentication, deeming this as a non-corporate device. This is defined by ISE's authorization compound condition expression "EAPChainingResult Equals No Chaining" and will be used for creating ISE's authorization policy. Log details can be found in the Detailed View of EAP Chaining section of this document.

If the response Identity-Type TLV does not match the request, then the client does not process the requested credential type and the server can proceed with the proposed credential type authentication or proceed with requesting the next credential type as defined by the server policy.

For example, a Result TLV with failure can be sent immediately from the ISE Server to the client after a failure to negotiate a credential type required by the server policy.

During EAP Chaining the server may continue the inner EAP conversation to authenticate a new Identity-Type after a previously failed authentication. For instance, the user may fail machine authentication but the server decides to continue onto user authentication. Alternatively, the server may also decide to terminate the conversation after a failed authentication by sending a Result TLV with Success or Failure, pending the authorization policies.

In the final example, the client does not match the server's Machine Identity-Type TLV request, since this device is not enrolled in the corporate domain. Authentication continues and matches on the server's User Identity-Type TLV request, thus deeming it as a non-corporate device. This is defined by ISE's authorization compound condition expression "EAPChainingResult Equals User Succeeded and Machine Failed". This will be used for creating an Authorization policy for allowing users access restricted network access when logging on with a non-corporate device. Log details can be found in the Detailed View of EAP Chaining section of this document.

Identity Source / DATABASE

When deploying in a wired/wireless network and seeking an authentication protocol, it is common to use an existing database of user and machine authentication credentials. Typical databases are Windows Active Directory (AD), LDAP, or a One Time Password (OTP) database (i.e. RSA SecureID). All of these databases are compatible with the EAP-FAST protocol. When planning for deployment, there are compatibility requirements such as EAP Chaining which requires AD for machine and user validation. For the purpose of this document, AD will be used as the database. EAP Chaining will be enabled in the EAP-FAST protocol selection on the ISE node.

Encryption

EAP-TLS is a strong authentication method requiring server and client-based X.509 certificates that also need PKI for certificate deployment. Another strong authentication method EAP-FAST does not require X.509 certificates for mutual authentication, instead Protected Access Credential (PAC) files are used. PAC files can be provisioned either manually or automatically. In this document, the PAC files are automatically provisioned from the ISE server to the client if the client does not contain as existing PAC file. Anonymous PAC provisioning uses EAP-TLS with a Diffe Hellman Key Agreement protocol to establish a secure TLS tunnel. In addition, MSCHAPv2 is used to authenticate the client and prevent early MITM attack detection. Authenticated In-Band PAC provisioning uses TLS server-side authentication, requiring server certificates for establishing the secure tunnel. Unauthenticated PAC provisioning does not require server side validation, and thus has some security risks, such as allowing rogue authentications to mount a dictionary attack. In this document the NAM configuration profile will be configured for unauthenticated PAC provisioning for testing purposes only.

A PAC is a security credential generated by the ISE server that holds information specific to the client. These PAC files, machine tunnel (a.k.a. machine authentication), user authorization are all used to establish the secure TLS tunnel for securing inner method authentication exchanges. They also prove that the client and machine were authenticated prior and the current authentication process can be optimized and bypassed. PAC type 4 has been added to support EAP Chaining.

Configuring ISE

This section describes how to configure ISE starting with adding network devices, Active Directory configuration, and creating Authentication and Authorization Policies.

Procedure 1 Adding Network Devices to ISE

Configure your WLC and switch for ISE and enable RADIUS

Step 1 Select \rightarrow Administration \rightarrow Network Resources \rightarrow Network Devices

Step 2 Select \rightarrow Add

Step 3 Enter the name & IP address of your device

Step 4 Enable 'Authentication Settings' and enter your shared secret

Step 5 Submit the Changes

Figure 4 an example of the switch configuration

cisco Identity Services Engine		ise admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admini	stration 🔻	👓 Task Navigator 👻 🕗
🔆 System 🦉 Identity Management 📳	Network Resources 🛛 🛃 Web Portal Management	
Network Devices Network Device Groups Ext	ernal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers	
Network Devices	* Name 3750x Description	*
Aetwork Devices Default Device	* IP Address: 192.168.1.2 / 32	-
	Model Name v Software version v	
	* Network Device Group Location All Locations Set. To Default Device Type All Device Types Set. To Default	
	Authentication Settings Enable Authentication Settings	
	Protocol RADIUS * Shared Secret Show	•

Procedure 2 Add Microsoft Active Directory as the External Identity Store

Machine and user credentials will be validated against the AD domain and identified as an external identity source

Step 2 Enter the Domain Name

In this example, 'cfacres007.com' was used.

Step 3 Enter a name to be used in the Identity Store Name, in this example, the default "AD1" was used

Step 4 Select Save

Figure 5 Active Directory Setting



Procedure 3 Procedure 3 Join the Active Directory Domain specified in Procedure 2

Each ISE node must join the AD domain.

Step 1 Select your ISE node

Step 2 Click Join

Step 3 Enter the user name credentials

The results are shown in Figures 4 and 5.

Figure 6 Prompt to join the domain



Figure 7 The results after the successful join to the domain

🙆 Home Operations 🔻 Policy 🔻 Admin	istration 🔻		_	🕶 Task Navigator 👻 🌔
🔆 System 🦉 Identity Management 📄 🖬	letwork Resources 🛛 🛃 Web I	Portal Manage	ment	
Identities Groups External Identity Sources	Identity Source Sequences	Settings		
External Identity Sources	Active Directory > AD1			
∲• ≣`≣ ⊗ _*	Connection Advance	ed Settings	Groups	Attributes
Certificate Authentication Profile	* Domain Na	ame cfacres00	07.com	
Active Directory	* Identity Store N	ame AD1		
🚞 LDAP 💿				ns. If a node is joined then a leave operation
🚞 RADIUS Token 💿	is required before a rejoin. Sel	ectione node f	or Test Connection	
🚞 RSA SecurID 🛞	옆 Join 앞 Leave 앞 Tes	t Connection		
	ISE Node		ISE Node Role	Status
	ise ise		STANDALONE	Connected to: dns.cfacres007.com

Procedure 4 Configuring Active Directory Groups

In this procedure, you will configure active directory groups that will be available for authorization policy conditions

Step 1 Select Administration \rightarrow Identity Management \rightarrow External Identity Sources \rightarrow Active Directory

Step 2 Click on the Groups Tab

Step 3 Click Add

Note: If you leave the '*' by default, this will display all the AD groups (up to 100)

Step 4 Select any Active Directory Groups that you will use in your deployment.

Step 5 Click OK

Step 6 Click 'Save Configuration'

Procedure 5 Defining the Identity Source Sequence

Identity Source Sequences define the order in which the Cisco ISE will look for the validation of user and machine credentials in the different databases. Here we will configure ISE to look for Active Directory and Internal Users.

Step 1 Select Administration \rightarrow Identity Management \rightarrow Identity Source Sequences

Step 2 Click Add

Step 3 Enter the name

In this example, CorpAssets was used

Step 4 Under 'Authentication Search List' select 'Internal Users' and 'AD1' from Available, and then move over to selected list

Step 5 Under 'Advanced Search Listings Settings', leave the default values

Step 6 Click Submit

Figure 8 Identity Source Sequence

💧 Home	Operations 🔻 Policy 🔻 Administration 🔻	😝 Task Navigator 👻 😢
🔆 System	🦉 Identity Management 📲 Network Resources 🛃 Web Portal Management	
Identities	Groups External Identity Sources Identity Source Sequences Settings	
Identity Sou	Jarce Sequence	-
▼ Identity Sou	purce Sequence	
* Name	CarpAssets	
Description		
	ii.	
▼ Certificate	te Based Authentication	
🗆 Sel	elect Certificate Authentication Profile	
 Authentica 	cation Search List	
A	A set of identity sources that will be accessed in sequence until first authentication succeeds	
Available	e Selected	
Internal E	Endpoints Internal Users AD1	

Defining Authentication Policies and Authorization Profiles

Authentication Policies

Authentication policies define the conditions between the client and ISE node when 802.1X occurs. These policies define the radius attribute conditions and authentication protocols that are required for successful authentication and also for the external or internal database used for validation of machine and user credentials.

The Authentication policy consists of the following elements:

- Results- Define authentication protocols Configure the authentication method between ISE server and client. In this example we will enable EAP Chaining to occur in the EAP-FAST protocol.
- Conditions- Set the radius attributes to match on 802.1X-based radius authentication requests ISE ships with pre-defined 802.1X conditions that will be used when configuring our policies.
- Defining Identity Source Sequence- Authentication policy will use the identity source to validate the end-user and machine credentials. In this example, CorpAssets is used as the Identity source

Defining the Authentication Policies

In this document, we will define two policies: EAP-Chaining_Wired, and EAP-Chaining_Wireless, use EAP-FAST as the authentication protocol with EAP Chaining enabled, and use the CorpAssets sequence as the identity store for credential validation.

Procedure 6 Enable EAP Chaining in the EAP-FAST Protocol

The following illustrates the configuring EAP-Chaining in the EAP-FAST Protocol:

Step 1 Select Policy \rightarrow Policy Elements \rightarrow Results \rightarrow Authentication \rightarrow Authentication Protocols

Step 2 Click Add

Step 3 Enter the name of the Allowed Protocols

In this example, we use 'EAP-FAST_EAP-Chaining'

Step 4 Scroll down to the 'EAP-FAST' section and enable

Step 5 Under 'Authentication Protocols' enable MS-CHAPv2

Step 6 Enable 'Allow Anonymous In-band PAC Provisioning' and enable the following:

- Server Returns Access Accept After Authenticated Provisioning
- Accept Client Certificate for Provisioning

Step 7 Enable 'Allow Machine Authentication'

Step 8 Enable 'Stateless Session Resume'

Step 9 Click Submit

Figure 9 EAPFast_EAPChaining Allowed Protocols Definition

Allowed Protocol: Allowed Prot	s Services List > EAPFast_EAPChaining DTOCOIS	^
Name	EAPFast_EAPChaining	
Description		
 Allowed Pr 	otocols	
	Process Host Lookup	
	nentication Protocols	
	Allow PAP/ASCII	
	✓ Detect PAP as Host Lookup	
	Allow CHAP	
_	Allow MS-CHAPv1	
	Allow MS-CHAPv2	
→ <i></i>	Allow EAP-MD5	
	Detect EAP-MD5 as Host Lookup	~
✓	Allow EAP-TLS	
	Allow LEAP	
→ 🗹	Allow PEAP	
	PEAP Inner Methods	
	Allow EAP-MS-CHAPv2	
	Allow Password Change Retries 1 (Valid Range 0 to 3)	
	Allow Password Change Retries O (Valid Range 0 to 3)	
	Allow EAP-TLS	
- ⊻	Allow EAP-FAST	
	EAP-FAST Inner Methods	
	Allow EAP-MS-CHAPv2	
	Allow Password Change Retries 1 (Valid Range 1 to 3)	
	Allow EAP-GTC	~
	Allow Password Change Retries 1 (Valid Range 1 to 3)	
	Allow EAP-TLS Use PACs Don't Use PACs	
	Tunnel PAC Time To Live 90 Days V	
	Proactive PAC update will occur after 10 % of PAC Time To Live has expired	
	Allow Anonymous In-Band PAC Provisioning	
	Allow Authenticated In-Band PAC Provisioning	
	Server Returns Access Accept After Authenticated Provisioning	
	Accept Client Certificate For Provisioning	
	✓ Allow Machine Authentication	
	Machine PAC Time To Live 1 Weeks 💌	
	Enable Stateless Session Resume	
	Authorization PAC Time To Live 1 Hours 💌	
	Enable EAP Chaining	
	Preferred EAP Protocol EAP-FAST	

Procedure 7 Define the Authentication Policy

Two authentication policies need to be defined: EAP Chaining_wireless for wireless access and EAP Chaining for wired access, where in both cases EAP-FAST with EAP Chaining enabled is selected as the protocol, and CorpAssets for the identity store.

Note: The ISE default policies for Wireless_802.1X and Wired 802.1X were used in this document.

Step 1 Disable predefined Dot1X authentication rule by clicking on the down arrow next to the green check mark and select Disable, which is located on the left side of the Dot1X rule.

Step 2 Select Polcy \rightarrow Authentication

Step 3 Click on 'Actions' button on the row labeled 'MAB' and choose 'Insert new row below'

Note: This rule should be close to the top of your Authentication Policy.

Step 4 Provide a policy name

In this example, EAP-Chaining wireless was used

Step 5 Select Conditions \rightarrow Existing Conditions from library \rightarrow Compound Condition

Step 6 Choose Wireless 802.1X

Step 7 Click on the cursor

Step 8 Click Internal Users \rightarrow and select your Identity Source

In this example CorpAssets was used.

Step 9 In the next row, Select Actions \rightarrow Insert new row above, and create another policy for wired.

Step 10 The steps above are the same except, Select Existing conditions \rightarrow Compound Condition \rightarrow Wired_802.1X

Step 11 Save the changes

Figur	e 10 Comp	leted Authen	tication Po	licies						
	Authentication	🗴 Authorization	🛃 Profiling	Posture	😡 Client Prov	risioning [🗐 Security Group	Access	Policy Elements	
		Policy by selecting the p	protocols that ISE	should use to com	nmunicate with th	ne network de	evices, and the ide	entity sources t	that it should use fi	or authentical
	▼ MAB		: If VVired_M	\B ↔	allow protocols	Allowed Prot	:ocol : Default Net	w📀 and	•	🙀 Act
0	▼ Dot1X		: If Wired_80	12.1X 🔶	allow protocols	Allowed Prot	:ocol : Default Net	w		🖗 Act
	▼ EAPChainin	g_wireless	: If Wireless	_802.1X 🔶	allow protocols	Allowed Prot	:ocol : EAPFast_EA	and	•	🙀 Act
	✓ Defau	lit	: use	CorpAssets (A.					Action
	▼ EAPChainin	g_wired	: If Wired_80	12.1X 💠	allow protocols	Allowed Prot	:ocol : EAPFast_EA	אָ רְ⊘ and	•	🚔 Act
	🖌 Defau	lt	: use	CorpAssets (÷					🖗 Action

Define the Authorization Profiles

Authorization occurs once the end-user has successfully authenticated. Authorization policies provide the rules that must be met before the end-user is provided with full or restricted network access as determined by the associated authorization profile.

The authorization profile contains common data such as VLAN information and other RADIUS attributes.

The Authorization policy consists of the following elements:

• Authorization Profile- Defines full or restricted network access.

In this example, we will define three profiles to match the authorization conditions for: Corporate, Non-corporate, and End-Users with Mobile devices and associated VLANS.

• Conditions- Contain the authorization rules that determine the required network permissions or level of access:

In this example, these rules will be defined based on the EAP-Chaining results:

• If both user and machine both succeeded

- If user succeeded and machine failed
- No chaining is supported

Procedure 8 Define the Authorization Profiles

In this document, we will define, three Authorization Policies, based on the EAP Chaining results and then provide the appropriate level of access as defined by their corresponding authorization profiles.

In the table below, there are three profiles based on the results of the EAP-Chaining values:

Authorization Profiles	Results
both_user_&_machine_credentials_passed_auth	End-user placed in VLAN 1 and has full network access
MachineFail_UserPass	End-user placed in VLAN 22 and has restricted network access.
NoChaining_UserPass	End-user placed in VLAN 12 and has restricted network access.

The completed authorization profiles are shown below.

Figure 11 Completed Authorization Profiles

cisco Identity Services Engine		ise admin Logout Feedback
🍐 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻	😁 Task Navigator 👻 😢
🚨 Authentication 🛛 👩 Authorization 🧭	Profiling 👩 Posture 🗔 Clie	nt Provisioning 🔄 Security Group Access 🦳 🐥 Policy Elements
Dictionaries Conditions Results		
Results	Standard Authorization Prof	files Selected 0 Total 7 🛭 🍪 🖕
<u></u> ♦• ≡ च &	/ Edit 🕂 Add 🖻 Duplicate	XDelete Show All
	Blacklist_Access Cisco_IP_Phones	Description Profile For Cisco Phones. Profile For Cisco Phones. Default Network Authorization Profile with access type as Access-Reject
	Nochaining_Userpass	Default Network Authorization Profile with access type as Access-Accept

Procedure 9 Define the Authorization Profile for 'MachineFail UserPass'.

Step 1 Navigate to PolicyElements \rightarrow Results \rightarrow Authorization \rightarrow Authorization Profiles

Step 2 Select Add

- Step 3 Enter the profile name 'MachineFail_UserPass'
- Step 4 Enable VLAN- and enter the number, in this example 22 was used

Step 5 Submit the changes

Figure 12 Authorization Profile for 'MachineFail_UserPass'

🛕 Home Operations 🔻 Policy 🔻 Admir	istration 🔻	🤨 Task Navigator 👻 🕗 🔵
🔍 🔍 Authentication 🛛 🧕 Authorization 🔀	Profiling 💿 Posture 🛛 Client Provisioning 🚊 Security Group Access 🚺 🔒 Policy	Elements
Dictionaries Conditions Results		
Results Image: Constraint of the second s	Authorization Profile * Name MachineFai_UserPass Description * Access Type ACCESS_ACCEPT	
		: Tag ID/Name

Figure 13

Procedure 10 Define the Authorization Profile for 'NoChaining_UserPass'.

Step 1 Navigate to Policy \rightarrow PolicyElements \rightarrow Results \rightarrow Authorization \rightarrow Authorization Profiles

Step 2 Select Add

Step 3 Enter the profile name 'NoChaining_UserPass'.

Step 4 Enable VLAN- and enter the number, in this example 12 was used

Step 5 Submit the changes

Figure 13 Authorization Profile for 'NoChaining_UserPass'

🛕 Home Operations 🔻 Policy 🔻 Admin	stration 🔻 😜 😁 Task Navigator 👻	•
🚨 Authentication 💿 Authorization 🔗	Profiling 🛛 Posture 💫 Client Provisioning 🚊 Security Group Access 💦 Policy Elements	
Dictionaries Conditions Results		
Results	Authorization Profiles > Nochaining_Userpass Authorization Profile * Name Marchaining Licemass	
Authorization Profiles Downloadable ACLs Inine Posture Node Profiles	Common Tasks	
Frofiling Fosture	□ DACL Name Tag ID 1 Edit Tag ID/Name	Image: 1 to 1 t
 Client Provisioning Security Group Access 	Voice Domain Permission	



Step 1 Navigate to Policy \rightarrow PolicyElements \rightarrow Results \rightarrow Authorization \rightarrow Authorization Profiles

Step 2 Select Add

Step 3 Enter the profile name 'both user & machine credentials passed auth'

Step 4 Enable VLAN- and enter the number, in this example 1 was used

Step 5 Submit the changes

Figure 14 Authorization Profile for 'both_user_&_machine_credentials_passed_auth'

🛕 Home Operations 🔻 Policy 🔻 Admir	nistration 🔻 😶 Task Navigator	• 🕗 🛛
🛃 Authentication 🛛 💿 Authorization 🔀	Profiling 👩 Posture 👩 Client Provisioning 🚊 Security Group Access 🚺 Policy Elements	
Dictionaries Conditions Results		
Results	Authorization Profiles > both_user_&_machine_credentials_passed_auth Authorization Profile * Name poth_user_&_machine_credentials Description * Access Access_Accept * Common Tasks DACL Name VLAN Tag ID 1 Edit Tag ID/Name 1 Voice Domain Permission Web Authentication Auto Smart Port	
	Filter-ID	~

Defining Authorization Condition Rules and Authorization Policies

Procedure 12 Define the Authorization Condition for, "UserPASSED_MachinePASSED":

The EAP Chaining condition rule "UserPASSED_MachinePASSED" is defined as a trusted or corporate device when both machine and user credentials have been successfully authenticated.

Step 1 Navigate to Policy \rightarrow Policy Elements \rightarrow Conditions \rightarrow Authorization \rightarrow Compound Conditions

Step 2 Add name, 'EAP-Chaining_UserPASS_MachinePASS'

Step 3 Add description, this is optional

For expressions, select the following:

- a. Network Access: EAPAuthentication equals EAP-MSCHAPv2(inner method)
- b. Network Access: EAP-ChainingResult equals User and Machine Both Succeeded
- c. Network Access: EAPTunnel equals EAP-FAST

Step 4 Submit the changes

.

Figure 15 EAPChaining_UserPASS_MachinePASS Compound Condition

💧 Home Operations 🔻 Policy 🔻 Adr	ininistration 🔹 😌 Task Navigator 👻
🛓 Authentication 🛛 👩 Authorization	🛿 Profiling 💿 Posture 👵 Client Provisioning 📄 Security Group Access 🔒 Policy Elements
Dictionaries Conditions Results	
Compound Conditions	Authorization Compound Condition List > EAPChaining_UserPASS_MachinePASS Compound Condition
⟨] = := ::::::::::::::::::::::::::::::::	* Name EAPChaining_UserPASS_MachinePASS
€ Wired_802.1X	Description EAPAuthentication Equals 'MSCHAPv2'
💊 — — — — — — — — — — — — — — — — — — —	EAPChainingResult Equals 'User And Machine Both Succeeded' EAPTupnel Equals 'EAP-FAST'
💊 Wireless_802.1X	
🔬 Wireless_MAB	*Condition Expression
& Catalyst_Switch_Local_Web_Authentication	
& WLC_Web_Authentication	
💊 NOChaining_UserPass	Condition Name Expression AND -
🙀 EAPChaining_UserPASS_MachinePASS	Image: Image
🖕 EAPChaining_MachineFAIL_UserPASS	♦ Network Access:Ea℘ Equals ▼ User and m ▼ AND ŵ
	Network Access:Ea📀 Equals 🔻 EAP-FAST 👻
	Save Reset

Procedure 13 Define the Authorization Condition for, 'NOChaining_UserPASS':

The EAP Chaining condition rule "NOChaining_UserPASS" is defined as a device that does not support EAP Chaining such as a mobile device. The end-user credentials are valid and are also defined as a non-corporate device.

Step 1 Select Policy \rightarrow Policy Elements \rightarrow Conditions \rightarrow Authorization \rightarrow Compound Conditions

Step 2 Add name, 'NOChaining_UserPASS'

Step 3 Add description, this is optional

For expressions, select the following:

- d. Network Access:EAPTunnel equals EAP-FAST
- e. Network Access:EAP-ChainingResult equals No_chaining

Step 4 Submit the changes

Figure 16 NOChaining_UserPass Compound Condition

💧 Home Operations 🔻 Policy 🔻	Admini	stration 🔻				•	🤊 Task Navigator 👻 📀
🚨 Authentication 🛛 🧕 Authorization	K. 1	Profiling 🛛 💽	Posture	🔊 Client Provisioning	🚊 Security Group	Access 🔒 Policy	Elements
Dictionaries Conditions Results							
Compound Conditions	(م	Compound		lition List > NOChaining_UserPa N	355		
↓ · · · · · · · · · ·	£	* Name	NOChainin	ig_UserPass			
& Wired_802.1X		Description		el Equals 'EAP-EAST'			
wired_MAB			ESECTION	ngResult Equals 'No_chainir	Ig		
🗞 Wireless_802.1X							.::
🗞 Wireless_MAB		*Condition &	Expression				
💊 Catalyst_Switch_Local_Web_Authentication							
🗞 WLC_Web_Authentication							
💊 NOChaining_UserPass		Conc	ition Name	Expression			AND -
🗞 EAPChaining_UserPASS_MachinePASS		° 🔷		Network Acc	ess:Eap	▼ EAP-FAST ▼	AND 🊔 🗸
🗞 EAPChaining_MachineFAIL_UserPASS		\diamond		Network Acc	ess:Ea😰 Equals	▼ No chaining ▼	÷ġ.≁
		Save F	leset				

Procedure 14 Define the Authorization Condition for, 'EAP-Chaining_MachineFAIL-UserPASS'

The EAP Chaining condition rule 'MachineFail_UserPASS' which is defined as a non-corporate device when machine credential fails and the end-user credential is valid.

Step 1 Select Policy \rightarrow Policy Elements \rightarrow Conditions \rightarrow Authorization \rightarrow Compound Conditions

Step 2 Add name, 'EAP-Chaining_MachineFAIL_UserPASS'

Step 3 Add description, this is optional

For expressions, select the following:

- f. Network Access: EAPAuthentication equals EAP-MSCHAPv2
- g. Network Access: EAP-ChainingResult equals User Succeeded and Machine Failed
- h. Network Access: EAPTunnel equals EAP-FAST

Step 4 Submit the changes

Figure 17 EAPChaining_MachineFAIL_UserPASS Compound Condition

🛕 Home Operations 🔻 Policy 🔻	Administration 🔻) Task Naviga	itor 🕶 🕙 🔵
🚨 Authentication 🛛 🧕 Authorization	🛃 Profiling 🛛 💽	Posture [😡 Client Provisioning	🚊 Security Group /	Access 🔒 Policy	Elements	
Dictionaries Conditions Results							
Compound Conditions		d Condition EAPChaining EAPAuthenti EAPAuthenti	n List > EAPChaining_Machi _MachineFAIL_UserPASS icatione Equals EAP-MSCH SESULT Equals 'User Suc quals 'EAP-FAST'		ailed'	:	
💊 Wireless_MAB	*Condition	Expression					
Catalyst_Switch_Local_Web_Authentication							
WLC_Web_Authentication NOChaining_UserPass	Con	dition Name	Expression Network Acc	ess:Ear📀 Equals	▼ EAP-MSCH/▼		- ₩-
EAPChaining_UserPASS_MachinePASS EAPChaining_MachineFAIL_UserPASS			Network Acc	ess:Eap	User succer	AND	÷
	Save	Reset	Network Acc	ess:Ea‡ <mark>©</mark> Equals	▼ EAP-FAST ▼		÷≩∙

Creating Authorization Policies

Once these authorization profiles and authorization conditions have been configured, you can just select them in the Authorization policies.

Procedure 15 Create an Authorization Policy for 'UserPASSED MachinePASSED'

- Step 1 Navigate to Policy \rightarrow Authorization
- Step 2 Click on the down arrow next to 'Edit' and choose 'insert new rule above'
- Step 3 Replace the rule name 'Standard rule 1' with your rule name

In this example, 'UserPASSED MachinePASSED' were used.

- Step 4 Under Conditions, select Existing Condition from Library \rightarrow Condition \rightarrow Compound Conditions
- Step 5 Choose EAP-Chaining_UserPASS_Machine_PASS
- Step 6 Click on '+' next to 'Authz Profile' and select your authorization profile
- Step 7 Select Item \rightarrow Standard \rightarrow both_user_&_machine_credentials_passed

Step 8 Save the changes

Procedure 16 Create an Authorization Policy for 'NoCHAINING UserPASSED'

Step 1 Navigate to Policy \rightarrow Authorization

Step 2 Click on the down arrow next to 'Edit' and choose 'insert new rule above'

Step 3 Replace the rule name 'Standard rule 1' with your rule name,

In this example, 'NoCHAINING UserPASSED' were used

Step 4 Under Conditions Select 'Existing Condition from Library' \rightarrow Condition \rightarrow Compound Conditions \rightarrow 'NoCHAINING_UserPASS'

Step 5 Click on the '+' next to 'Authz Profile' and select your authorization profile. Select Item \rightarrow Standard \rightarrow 'NoCHAINING_USerPASS'

Step 6 Save the changes

Procedure 17 Create an Authorization Policy for 'MachineFAILED UserPASSED'

Step 1 Navigate to Policy \rightarrow Authorization \rightarrow click on the down arrow next to 'Edit' and choose 'insert new rule above'

Step 2 Replace the rule name 'Standard rule 1' with your rule name

In this example, 'MachineFAILED UserPASSED' were used.

Step 3 Under Conditions, Select Existing Condition from Library \rightarrow Condition \rightarrow Compound Conditions \rightarrow 'EAP-Chaining_MachineFAIL_UserPASS'

Step 4 Click on '+' next to 'Authz Profile' and select your authorization profile. Select Item \rightarrow Standard \rightarrow 'EAP-Chaining_MachineFAIL_UserPASS'

Step 5 Save the changes

Figure 18 - The completed authorization policies.

cisco Identity Services Engine			0	ise admin Lu	ogout Feedback
💧 Home Operations 🔻 Policy 🔻 Admini	stration 🔻			\varTheta Task Navig	jator 📲 🕘
Authentication 🧕 Authorization 🛃	Profiling 💽 Posture	🔊 Client Provisioning	🚊 Security Group Access	🔒 Policy Elements	
Authorization Policy Define the Authorization Policy by configuring rules bas Multiple Matched Rule Applies	ed on identity groups and/or	r other conditions. Drag and	l drop rules to change the orde	er.	
Exceptions (0) Standard					
Status Rule Name	Conditions (identity	y groups and other conditio	ns) Permission	าร	4
UserPASSED_MachinePASSED both_user_&_machine_credentials_ passed_auth	if EAPChaining_UserF	PASS_MachinePASS	then		Edit 🕶
Nochaining_UserPASSED	if Any 🔶	and NOChaining_User	°ass 🔶	then	Done
MachineFAILED_UserPASSED	if Any 💠	and EAPChaining_Mach	nineFAIL_UserPASS 🔶		Done

In this section we will go over installing Cisco's AnyConnect Network Access Manager (NAM)

NAM Installation and Configuration

Procedure 18 Installing AnyConnect NAM

Step 1 Extract the contents of the AnyConnect ISO image to a folder

Step 2 Run 'setup'

Note: Please note that you will require local admin rights during the installation.

Step 3 Enable AnyConnect Diagnostics and Reporting Tool

Step 4 AnyConnect Network Access Manager



Note: You will see the message in Figure 20 after a completed install of the AnyConnect Secure Mobility Client. As part of the core install, the AnyConnect Quality Improvement feature is enabled by default. This feature provides Cisco with customer installed AnyConnect modules, and enabled features. Crash dumps may also be included. This feature can be completely disabled via the Profile Editor or just for disabling crash dumps. Corporate privacy is maintained by hashing the machine name, however crash dumps may contain personal information, and hence the displayed EULA license.)



Procedure 19 Creating a NAM Profile with the Profile Editor

Profiler Editor will also be required to configure the Network Access Manager configuration profile for EAP-FAST authentication.

Note: Please note that the NAM configuration should be saved as 'configuration.xml', and saved to the 'NewConfigFiles' directory. Right-click on the AnyConnect GUI in the system tray, select 'Network Repair'. This will place the configuration.xml file into the NAM system directory.)

Step 1 Open the profile editor, and access the current system configuration.

Step 2 Keep the defaults, and select \rightarrow Authentication Policy

```
The Client Policy as illustrated in Figure 19 determines what types of media will be managed, allow end-users to disable NAM client, and use the native Windows supplicant, allow end-users to see the admin configured groups in their NAM profile, and other admin-defined options.
```

Figure 21 NAM profile Editor

Networks Network Groups	Connection Settings		
needore of output	Default Connection Timeout (sec.) 40		
	Connection Attempt:		
	Before user logon		
	Time to wait before allowing user to logon (sec.)	40	
	After user logon		
	Media		
	💟 Manage Wi-Fi (wireless) Media		
	Enable validation of WPA/WPA2 handshake		
	Default Association Timeout (sec.) 5	-	
	Manage Wired (802.3) Media		
	Manage Mobile Broadband (3G) Media		
	📝 Enable Data Roaming		
	End-user Control		
	Allow end-user to:		
	V Disable Client		
	V Display user groups		
	Specify a script or application to run when connect	cted	
	V Auto-connect		
	and the second se		
	Administrative Status		
	Administrative Status Service Operation	FIPS Mode	

Step 3 Keep the defaults, and select 'Networks'

The Authentication policy as illustrated in Figure 20 sets the methods of authentication for user-created networks

File Help Network Access Manager Authentication Policy Client Policy Profile: ...ility Client\Network Access Manager\system\configuration.xml Allow Association Modes Allowed Authentication Modes Networks Select All (Personal) Select All Outer EAP-FAST Open (no encryption) EAP-GTC Open (Static WEP) EAP-MSCHAPv2 Shared (WEP) EAP-TLS WPA Personal TKIP EAP-TLS WPA Personal AES EAP-TTLS EAP-MD5 EAP-MSCHAPv2 WPA2 Personal TKIP PAP (legacy) CHAP (legacy) WPA2 Personal AES MSCHAP (legacy) MSCHAPv2 (legacy) LEAP Select All (Enterprise) PEAP ✓ Open (Dynamic (802.1X) WEP) EAP-GTC VPA Enterprise TKIP EAP-MSCHAPv2 EAP-TLS WPA Enterprise AES Allowed Wired Security WPA2 Enterprise TKIP Select All WPA2 Enterprise AES V Open (no encryption) CCKM Enterprise TKIP 302.1x only CCKM Enterprise AES 802. 1x with MacSec

Step 4 Define your network

Figure 22 NAM Authentication Policy

In this example, this was defined as 'EAP-Chaining' as illustrated in Figure 21

Step 5 Keep the defaults and select Next

Figure 23 Defining the Network

tworks		271270700000000		- 1 · · ·	Media Type
twork Groups	Name:	EAPChaining			Security Leve
	Group Membership				Connection Ty
	In group:	(auto-generated)		•	Machine Aut
					PAC Files
	In all groups (Global)				Credentials
	Choose Your Network Media				User Auth
	Wired (802.3) Network				PAC Files
					Credentials
		he endstations will be connect	ing to the network with a traditio	inal	
	ethernet cable.				
	Wi-Fi (wireless) Network				
			ig to the network via a wireless		
	radio connection to an Acc	ess Point.			
	SSID (max 32 chars):				
		Hidden Network			
		Corporate Network			
	Association Timeout (sec)	5			
	Common Settings				
	conner occurgo				
	Script or application on each use	r's machine to run when conne	cted.		
			Browse Local Machine		
	Connection Timeout (sec.)	90			

Step 6 Select Authenticating Network, as illustrated in Figure 22

Authenticating Network settings contain the 802.1X settings that contain MACSec configuration settings, and also 802.1X network connectivity settings.

Step 7 Keep the defaults

Step 8 Click Next

Figure 24 Network Security Level

Networks Network Groups	Security Level					Media Type
rk Groups	Open Network					Security Leve
	Open network	ks have no sec	urity, and are	open to anybody w	ithin range. This is the least	Connection Ty
	secure type o	of network.				Machine Auth
	 Authenticatin 	PAC Files				
	Authenticating	Credentials				
	enterprise lev	User Auth				
	network infra	PAC Files				
						Credentials
			🔄 Enable p	tication Exception Po port exceptions data traffic before a		
	Security					
	Key Management		(a) Allow	data traffic after au	thentication even if	
	None	•	EAP	fails		
	Encryption			succeeds but key m	nanagement fails	
				buccus buccus ,		
	None	-				

Step 9 Select 'Machine and User Connection', as illustrated in Figure 23

Note: Machine and User Connection, determine the network connection types

Figure 25 Network Connection Type

Network Access Manager Client Policy Authentication Policy	Networks Profile:ility Client\Network Access Manager\system\configuration.xml	
高いための形成 一次 Network の に いて いて の いて の いて の いて の いて の い の い の い の	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. User Connection The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on. Machine and User Connection This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.	Media Type Security Leve Connection Ty Machine Auth PAC Files Credentials User Auth PAC Files Credentials

Step 10 Click Next

Step 11 Select EAP-FAST

Note: EAP-FAST will be the method of Authentication, and EAP-MSCHAPv2 will be the inner method

Step 12 Select Authenticate Using a Password

Step 13 Select EAP-MSCHAPv2 Under 'Inner Methods based on Credentials Source'

Step 14 Select'If using PACs

Step 15 Select 'Allow unauthenticated PAC provisioning'

Step 16 Select 'Use PACs'

Step 17 Click Next

EAP Methods		Media Type				
k Groups © EAP-MD5	C EAP-TLS	Security Level				
C EAP-MSCHAPv2	C EAP-TTLS	Connection Typ				
© EAP-GTC	PEAP	Machine Auth				
	EAP-FAST	PAC Files				
		Credentials				
		User Auth				
		PAC Files Credentials				
EAP-FAST Settings		Credentials				
Validate Server Id	dentity					
Enable Fast Recor	nnect					
	Inner Methods based on Credentials Source (in Authenticate using a Password					
	-					
EAP-MSCHAP	v2 EAP-GTC					
If using PACs,	If using PACs, allow unauthenticated PAC provisioning					
 Authenticate using 	Authenticate using a Certificate					
When request	ted send the client certificate in the clear					
 Only send die 	ent certificates inside the tunnel					
③ Send client ce	③ Send client certificate using EAP-TLS in the tunnel					
Use PACs						

Step 18 Choose the defaults under PAC Files, and click Next.

Note: P	AC files will be provisioned from ISE	
Figure 27 Leave F	PAC files as default (blank)	
Network Access Manager 	Networks Profile:ility Client/Network Access Manager/system/configuration.xml PAC files Add Password protected Remove Remove	Media Type Security Leve Connection Typ Machine Auth PAC Files Credentials User Auth PAC Files Credentials

Step 19 Keep the defaults for Machine Identity

Client Policy Authentication Policy	-	k Access Manager\system\configur	
works	Machine Identity		Media Type
work Groups	Unprotected Identity Pattern:	host/anonymous	Security Level
	Protected Identity Pattern:		Connection Type
	Protected Identity Pattern.	host/[username]	Machine Auth
			PAC Files
	- Machine Credentials		Credentials
			User Auth
	 Use Machine Credentials 		PAC Files
	O Use Static Credentials		Credentials
	Password:		

Step 20 Click Next

Step 21 Select EAP-FAST

Step 22 Select 'Authenticate using a Password' in the 'Inner Methods based on Credentials Source' section.

Step 23 Select EAP-MSCHAPv2

Step 24 Select 'If using PACs, allow unauthenticated PAC provisioning'

Step 25 Select Use PACs

Step 26 Click Next

Figure 29 Completed Configuration

EAP Methods				
	EAP-TLS		Security Level	
	EAP-TTLS		Connection Type	
	PEAP		Machine Auth	
	EAP-FAST		PAC Files Credentials	
nection beyond log off			User Auth	
inclusion beyond log off			PAC Files	
			Credentials	
Identity				
onnect				
n using a Smart Card				
Credentials Source				
ing a Password				
Pv2	EAP-GTC			
s, allow unauthenticated	PAC provisioning			
ing a Certificate				
ested send the client cert	ificate in the clear			
lient certificates inside th	e tunnel			
certificate using EAP-TLS	in the tunnel			
ing a Token and EAP-GTO	C			

Step 27 Leave the PAC file as empty

Note: PAC files will be provisioned from ISE

Step 28 Click Next

Step 29 Keep the defaults for the User Identity.

Note: User identity specifies the types of user credentials that will be sent to the ISE server for validation

Step 30 Keep the default value 'Use Single Sign on Credentials' for 'User Credentials'

Step 31 Select Done

Figure 30 Completed User Authentication Configuration

User Identity	User Identity				
Unprotected Identity Pattern:	anonymous		Security Level		
Protected Identity Pattern:			Connection Type		
Protected addrivery Partern.	[username]		Machine Auth		
			PAC Files		
User Credentials			Credentials		
Use Single Sign On Credentia	le l		User Auth		
			PAC Files Credentials		
Prompt for Credentials			Credentials		
Remember Forever					
@ Remember while Use	r is Logged On				
Never Remember					
Use Static Credentials					
Password:					

At this point, you should see the network added to the NAM profile as illustrated in Figure 29.

Figure 31 Networks List

Network Access Manager Client Policy Authentication Policy Networks Network Groups	Networks Profile:ility Client/Network Access Manager/system/configuration.xml				
	Network				
	Name	Media Type	Group*		
	wired	Wired	Global		
	EAPChaining	Wired	(auto-generated)	Add	
	LAB	Wireless	(auto-generated)		
				Edit	
				Delete	
	h				
	* A network in grou	up 'Global' is a member of al/gro	oups,		

Step 32 From the drop-down File Menu, select 'Save-As'

Step 33 Name the file 'configuration.xml'

```
Note: this MUST be the file name. No variations will work.
```

Step 34 Save the file into the ..\newConfigFiles folder, as illustrated in Figure 30.

Figure 32 - Saving configuration.xml to the newConfigFiles directory

	🔁 Save	×
	Save in: 🔐 newConfigFiles	
For Windows XP systems: Save the 'configuration.xml' file to the fo	ollowing:	For Windows 7 systems: Save the 'configuration.xml' file to the following:
:\documents and settings\all users\applic: data\cisco\cisco anyconnect secure mobi client\network access manager\newConf	lity	:\programdata\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigfiles folder
(<u>Note:</u> If you cannot see the 'application please enable 'hidden files and folders' J dropdown in Control Panel.		(<u>Note</u> : If you cannot see the 'programdata' folder, select 'Organize', 'Folder and Search Options', 'Show hidden files, folders, and drives', under 'My
	File name: configuration[xm] Network Files of type: XML file *.xml	Computers')

Step 35 {Right Click} on the AnyConnect GUI in the system tray

Step 36 Select 'Network Repair'

Procedure 20 Configuring Network Access Manager for Wireless Networks

Step 1 Provide a name for your wireless networks

Step 2 Define the SSID

Step 3 Click Next

Figure 33 Defining the Wireless Network

Network Access Manager	Networks Profile:ility Client\Net	twork Access Manager\system\configuration.xml	
A Networks		ab	Media Type
🔆 Network Groups	Name:	Lab	Security Level
	-Group Membership		Connection Type
	 In group: 	(auto-generated)	Machine Auth
	 In all groups (Global) 		PAC Files
		Credentials	
	Choose Your Network Media-	User Auth Credentials	
	Wired (802.3) Network		Credentials
	Select a wired network i	f the endstations will be connecting to the network with a traditional	
	ethernet cable.		
	 Wi-Fi (wireless) Network 		
	Select a WiFi network if		
	radio connection to an A	Access Point.	
	SSID (max 32 chars): lab005		
		Hidden Network	
		Corporate Network	
	Association Timeout (se	c) 5	
	Common Settings Script or application on each u Connection Timeout (sec.)	ser's machine to run when connected.	

Step 4 Select 'Authenticating Network'

Step 5 Under Association Mode, choose the correct encryption level for your network.

Step 6 Click Next

```
Figure 34 Wireless Network Settings for Steps 4 and 5
```

Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml				
🔏 Networks	Security Level			Media Type	
😤 Network Groups	O Open Network			Security Level	
		ecurity, and are open to anybody v	ithin range. This is the least	Connection Type	
	secure type of network.			Machine Auth	
	Shared Key Network			PAC Files	
	Shared Key Networks use	Credentials			
	access points. This is a m	edium security level, suitable for sm	all offices, or home offices.	User Auth	
	 Authenticating Network 			Credentials	
	network infrastructure. - 602.1X Settings authPeriod (sec.) 30 heidPeriod (sec.) 60 - Association Mode (wPA2 Enterprise (AES) V	startPeriod (sec.) macStart	3		
		lext Cancel			

Step 7 Select 'Machine and User Connection'

Note: Machine and User Connection, determine the network connection types

Step 8 Click Next



Step 9 Select EAP-FAST

Note: EAP-FAST will be the method of Authentication, and EAP-MSCHAPv2 will be the inner method

Step 10 Select EAP-FAST

Step 11 Select 'Authenticate using a Password' in the 'Inner Methods based on Credentials Source' section.

Step 12 Select EAP-MSCHAPv2

Step 13 Select 'If using PACs, allow unauthenticated PAC provisioning'

Step 14 Select Use PACs

Figure 36 The Completed Configuration

Network Access Manager	Networks Profile:ility Client\Network Access Manager\s	ystem\configuration.xml
- Wetwork Groups	EAP-Methods EAP-MDS EAP-MDS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-FAST EA	Media Type Security Level Connection Typ Machine Auth PAC Files Credentials User Auth PAC Files Credentials
	Inner Methods based on Credentials Source Authenticate using a Password	GTC

Step 15 Keep the defaults for the User Identity.

Note: User identity specifies the types of user credentials that will be sent to the ISE server for validation

Step 16 Keep the default value 'Use Single Sign on Credentials' for 'User Credentials'

Step 17 Select Done

Figure 37 Completed Wireless User Authentication

User Identity		Media Type
Unprotected Identity Pattern:	anonymous	Security Level
		Connection Typ
Protected Identity Pattern:	[username]	Machine Auth
		PAC Files
User Credentials		Credentials
		User Auth
O Use Single Sign On Credentia	IS	PAC Files
Prompt for Credentials		Credentials
Remember Forever		
 Remember while Use 	r is Logged On	
Never Remember		
Use Static Credentials		
Password:		

You should see the network added to the NAM profile as illustrated.

Vetwork Access Manager	Networks Profile:ility Client/Network Access Manager/system/configuration.xml				
	Network				
	Name	Media Type	Group*		
	wired	Wired	Global		
	EAPChaining	Wired	(auto-generated)	Add	
	LAB	Wireless	(auto-generated)		
				Edit	
				Delete	

Step 18 From the drop-down File menu, select 'Save-As'

Step 19 Name the file 'configuration.xml' (this MUST be the file name)

Step 20 Save the file into the .. \newConfigFiles folder as illustrated

Figure 39 Saving the configuration.xml to the newConfigFiles directory



Step 21 {Right Click} on the AnyConnect GUI in the system tray

Step 22 Select 'Network Repair'

TESTING PROCEDURE

EAP Chaining was tested with the following business cases:

- End-User logs into a corporate device, both machine and user credentials have been successfully validated, placed in VLAN 1 and receive full network access.
- End-User logs into a non-corporate device with their personal laptop, machine domain credentials are not available and fail validation, however, their user credentials have been successfully validated placed in VLAN 22 and receive restricted network access.
- End-User logs into a non-corporate device using their mobile device, such as an Android Samsung tablet. EAP Chaining is not supported, however, their user credentials have been successfully validated and are placed in VLAN 12 and receive restricted network access.

Procedure 21 End-User Logs on to Corporate Network with Corporate Device

The end-user logs into the corporate device, machine and user credentials are tied to the trusted device. Upon successful authentication the trusted device is placed into VLAN 1, as determined by the ISE authorization profile.

The figures below show the AnyConnect NAM UI & Statistics screen after a successful authentication.

Figure 40 AnyConnect User Interface



Figure 41 NAM Status



PN	Configuration Statistics C	Connection Details Message History	
works >	Media: Adapter: Bytes	Wired Realtek PCIe FE Family Controller	_
	Sent: Received: Frames	262130 306770	- • □
	Sent: Received: Security Information - Configuration: Encryption:	1410 1179 802.1X	- •
lect diagnostic information for all installed components.	EAP Method: Server: Credential Type:	None Successful authentication crede	ntials

Procedure 22 End-User Logs on to corporate network with their personal laptop.

The end-user brings in their personal laptop and logs on their corporate network with limited access. They are placed in VLAN 22 with restricted access.

The figures below depict the AnyConnect NAM UI & Statistics screen after successful authentication.



Procedure 23 End-User Logs on to corporate network with their mobile device.

The end-user brings in their Samsung Android tablet and accesses the network. They are given restricted access and are placed in VLAN 12

The Samsung Android Tablet settings are as follows:

```
EAP-Method = FAST,

Provisioning = 1

Phase 2 Authentication = MSCHAPv2

Identity = Username (i.e. employee1)

Anonymous Identity = username (i.e employee1)

Password = password (i.e. cisco123)
```

Note: Both identity & anonymous should use the same MS Windows username that has been successfully validated against AD

Note: Leave settings for both CA Certificate and User Certificates set for "unspecified", also check to ensure you are running Android version 3.2 or above.

Listed below are screenshots from the Samsung Android Tablet, EAP- Method Setup:

Figure 45 EAP-FAST selection

lab005	
EAP method	FAST
Provisioning	PEAP
Phase 2 authentication	TLS
CA certificate	TTLS
ОК	FAST
	LEAP

Figure 46 Provisioning set to "1"

lab005		
Provisioning	1	
Phase 2 authentication	MSCHAPV2]
CA certificate	None	
User certificate	PAP	

Figure 47 Phase-2 Authentication = MSCHAPv2

lab005		
Provisioning	1	
Phase 2 authentication	MSCHAPV2	
CA certificate	None	
User certificate	PAP	
ОК	MSCHAP	
	MSCHAPV2	
	GTC	
Figure 48 Cisco Wireless LAN Controller - showing successful authentication

սիսիս					tion <u>P</u> ing Lo <u>q</u> out <u>R</u> efi
CISCO	MONITOR WLANS CON	TROLLER WIRELESS	SECURITY MANAGEMEN	NT C <u>O</u> MMANDS HE <u>L</u> P	EEEDBACK
onitor	Clients > Detail			< Back	Link Test Remove
Summary					
Access Points	Client Properties			AP Properties	
Cisco CleanAir	MAC Address	8c:77:12:a2:38:b9		AP Address	00:19:a9:e0:f5:60
Statistics	IP Address	10.3.1.12		AP Name	AP001a.2f6d.f868
CDP	Client Type	Regular		АР Туре	802.11g
Rogues	User Name	jeppich		WLAN Profile	lab005
lients	Port Number	1		Status	Associated
Multicast	Interface	vlan12		Association ID	1
	VLAN ID	12		802.11 Authentication	Open System
	CCX Version	CCXv4		Reason Code	1
	E2E Version	Not Supported		Status Code	0
	Mobility Role	Local		CF Pollable	Not Implemented
	Mobility Peer IP Address	N/A		CF Poll Request	Not Implemented
	Policy Manager State	RUN		Short Preamble	Implemented
	Management Frame Protection	No		PBCC	Not Implemented
	UpTime (Sec)	251		Channel Agility	Not Implemented
	Power Save Mode	ON		Re-authentication timeout	1566
	Current TxRateSet	54.0		Remaining Re- authentication	0
	Data RateSet	1.0,2.0,5.5,11.0,6.0,9.0 ,24.0,36.0,48.0,54.0	,12.0,18.0	timeout WEP State	WEP Enable

Detailed View of EAP Chaining

The Live Authentications view as illustrated in Figure 57, represent the identities and the authorization profiles of the three business cases outlined in this document. Detailed logs also accompany the business cases.

Procedure 24 Access the Live Authentications menu

Step 1 Select Operations \rightarrow Authentications

Figure 49 Live Authentications Log

	li.ili. Lisco Identity Servi	ces En	gine					ise admir
	🔒 Home Operations י	 Poli 	icy 🔻	Administration 🔻				😶 Task
	Mathentications	🔊 Endpo	oint Prote	ction Service 🛛 💆 Alarms	👖 Reports	💊 Troubleshoot		
L	ive Authentications							
S.	🚡 Add or Remove Columns 🔻	🛞 Ref	resh		Refresh Every 3 se	econds 🔻 Sho	ow Latest 20 records 🔹 🔻	within Last
Tin	ne 🔹	Status	Details	Identity	+HEndpoint ID	Network Device	Authorization Profiles	
Ma	ar 24,12 07:35:14.351 PM	~	Q	jeppich >> host/skiber-xp	C8:BC:C8:90:8D:FC	3750x	MachineFail_UserPass	
Ma	ar 24,12 07:30:30.033 PM	~	<u>a</u>	jeppich	8C 77:12:A2:38:B9	WLC	Nochaining_Userpass	
Ma	ar 24,12 07:25:42.316 PM		à	jeppich >> host/labstation	F0 DE:F1:94:65:90	3750x	both_user_&_machine_cre	dentials_p
Mot	pile Device			Corporate Asset	NO	DN-Corporate Ass	set	

Procedure 25 Log Details of an End-User Logging in from a Corporate Device

User Logging on from a Corporate laptop, both machine and user credentials successfully validated

Machine and User credentials are tied to a corporate device. Both credentials are passed an EAP transaction. Below are the RADIUS Authentication Details and detailed EAP transaction logs of the authentication as illustrated in the figures below.

블 🖹 🗟	Launch Interactive Viewer
RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next Last Goto Page: Go
⊟_Authentication Result User-Name=	
State=ReauthSession:c0a8011400 Class=CACS:c0a80114000000014 Termination-Action=RADIUS-Reque Tunnel-Type=(tag=1) VLAN Tunnel-Medium-Type=(tag=1) 802	F6E6606;ise/122009432/2
MS-MPPE-Send-Key=4c:89:b1:94:	61:f4:a1:90:a5:fb:c6:0c:0b:b8:9f:14:83:d5:0a:2d:1b:99:dc:a0:c5:83:86:cb:89:60:4f:4f.6e:66:06:34:7c:13:4c:5b:00:d9:40:5f:d5:2f.92:a 90:a0:6d:e5:13:ef.7d:5f:80:5d:64:d4:81:89:c9:d2:13:ee:e7:7c:cc:6a:69:15:93:0a:78:c2 5b:08:01:8c:1b:54:67:4f:fa:55:25:65:ba:17:b9:75:99:61:cd:05:e5:26:32:54:5b:2c:78:a2
- · · -	
Identity Services Engin	e Launch Interactive Viewer
RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next Last Goto Page: Go
□_Authentication Details	
E_Authentication Details	
Loggod At:	March 24 2012 7:25:42 216 DM
	March 24,2012 7:25:42:316 PM March 24,2012 7:25:42:315 PM
Occurred At:	March 24,2012 7:25:42:315 PM
Occurred At: Server:	March 24,2012 7:25:42.315 PM ise
Occurred At: Server: Authentication Method:	March 24,2012 7:25:42.315 PM <u>ise</u> dot1x
Occurred At: Server: Authentication Method: EAP Authentication Method :	March 24,2012 7:25:42.315 PM <u>ise</u> dot1x EAP-MSCHAPv2
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method :	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Jsername:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Jsername: RADIUS Username :	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Jsername: RADIUS Username : Calling Station ID:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation
Decurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Jsername: RADIUS Username : Calling Station ID: Framed IP Address:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous F0:DE:F1:94:65:9C
Decurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Jsername: AADIUS Username : Calling Station ID: Framed IP Address: Jse Case: Network Device:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C
Decurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Jsername: RADIUS Username : Calling Station ID: Framed IP Address: Jse Case: Vetwork Device: Network Device Groups:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device Groups: NAS IP Address:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device Groups: NAS IP Address: NAS IP Address:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous F0:DE:F1:94:65:9C
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device Groups: NAS IP Address: NAS IP Address: NAS Identifier: NAS Port:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous F0:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations 192.168.1.2 50115
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device: NAS IP Address: NAS IP Address: NAS IP Address: NAS IP Address: NAS IP Address: NAS IP Address: NAS Port: NAS Port ID:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous F0:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations 192.168.1.2 50115 GigabitEthemet1/0/15
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device: NAS IP Address: NAS IP Address: NAS IP Address: NAS Port: NAS Port ID: NAS Port ID: NAS Port Type:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations 192.168.1.2 50115 GigabitEthernet1/0/15 Ethernet
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device Groups: NAS IP Address: NAS IP Address: NAS IP Address: NAS Port: NAS Port ID: NAS Port ID: NAS Port Type: Allowed Protocol:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations 192.168.1.2 50115 GigabitEthemet1/0/15 Ethernet EAPFast_EAPChaining
Logged At: Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device: NAS IP Address: NAS IP Address: NAS IP Address: NAS IP Address: NAS Port : NAS Port : NAS Port : NAS Port ID: NAS Port Type: Allowed Protocol: Service Type:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations 192.168.1.2 50115 GigabitEthemet1.70/15 Ethernet EAPFast_EAPChaining Framed
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device Groups: NAS IP Address: NAS IP Address: NAS IP Address: NAS Port: NAS Port: NAS Port ID: NAS Port ID: NAS Port Type: Allowed Protocol: Service Type: Identity Store:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous F0.DE:F1:94:65:9C 375Dx Device Type#All Device Types,Location#All Locations 192.168.1.2 50115 GigabitEthernet1/0/15 Ethernet EAPFast_EAPChaining Framed AD1
Occurred At: Server: Authentication Method: EAP Authentication Method : EAP Tunnel Method : Username: RADIUS Username : Calling Station ID: Framed IP Address: Use Case: Network Device: Network Device Groups: NAS IP Address: NAS IP Address: NAS IP Address: NAS Port: NAS Port ID: NAS Port ID: NAS Port Type: Allowed Protocol: Service Type:	March 24,2012 7:25:42.315 PM ise dot1x EAP-MSCHAPv2 EAP-FAST jeppich.host/labstation anonymous FD:DE:F1:94:65:9C 3750x Device Type#All Device Types,Location#All Locations 192.168.1.2 50115 GigabitEthemet1.70/15 Ethernet EAPFast_EAPChaining Framed

cisco Identity Services Engine	ise
≞ ≧ ⊠	Launch Interactive Viewer 🛐
RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next Last Goto Page: Go
Allowed Protocol Selection Matched Ru	le: EAPChaining wired
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users,AD1,Internal Users,AD1
Authorization Policy Matched Rule:	Default
SGA Security Group:	
AAA Session ID:	ise/122009432/2
Audit Session ID:	
Tunnel Details:	
Cisco-AVPairs:	
Other Attributes:	ConfigVersionId=4,DestinationPort=1645,Protocol=Radius,Framed-MTU=1500,State=37CPMSessionID=c0a80114000000014f Key-Name=,EapChainingResult=User and machine both succeeded,CPMSessionID=c0a80114000000014F6E6606,EndPoint DE-F1-94-65-9C,EapChainingResult=User and machine both succeeded,Device Type=Device Type#All Device Types,Location Locations,IdentityAccessRestricted=false,Device IP Address=192.168.1.2,Called-Station-ID=50:3D:E5:C4:05:8F
Posture Status:	NotApplicable
EPS Status:	

불 💺 🖻			Launch Interactive Viewer
ADIUS Authentication Details			
Showing Page 1 of 1 First Prev Next	Last	Goto Page: Go	
Steps			
1001 Received RADIUS Access-Request			
1017 RADIUS created a new session			
Evaluating Service Selection Policy			
5048 Queried PIP			
5004 Matched rule			
1507 Extracted EAP-Response/Identity			
2100 Prepared EAP-Request proposing EAP-FAST with challenge			
2625 Valid EAP-Key-Name attribute received			
1006 Returned RADIUS Access-Challenge			
1001 Received RADIUS Access-Request			
1018 RADIUS is re-using an existing session			
2102 Extracted EAP-Response containing EAP-FAST challenge-response	and accepting EAP-FAST	as negotiated	
2800 Extracted first TLS record; TLS handshake started			
2175 Received Tunnel PAC			
2805 Extracted TLS ClientHello message			
2806 Prepared TLS ServerHello message			
2801 Prepared TLS ChangeCipherSpec message			
2802 Prepared TLS Finished message			
2105 Prepared EAP-Request with another EAP-FAST challenge			
1006 Returned RADIUS Access-Challenge			
1001 Received RADIUS Access-Request			
1018 RADIUS is re-using an existing session			
2104 Extracted EAP-Response containing EAP-FAST challenge-response			
2804 Extracted TLS Finished message			
2816 TLS handshake succeeded			
2132 EAP-FAST built PAC-based tunnel for purpose of authentication	Start EAP Chainin	g	
2209 Starting EAP chaining			
2218 Selected identity type 'User'			_
2125 EAP-FAST inner method started	'User' Identity Ty	ne Selected	
1521 Prepared EAP-Request/Identity for inner EAP method	eser haentity ry	pe selected	
2105 Prepared EAP-Request with another EAP-FAST challenge			_
1006 Returned RADIUS Access-Challenge			
1001 Received RADIUS Access-Request			
1018 RADIUS is re-using an existing session			
1018 RADIUS is re-using an existing session 2104 Extracted EAP-Response containing EAP-FAST challenge-response			

	11522	Extracted EAP-Response/Identity for inner EAP method	
	11806	Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge	
	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	
		Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated	
	Evaluat	ating Identity Policy	
	15006	Matched Default Rule	
		Selected Identity Store - Internal Users	≣
		Looking up User in Internal Users IDStore - jeppich,host/labstation	-
		The user is not found in the internal users identity store	
		Authenticating user against Active Directory	
		User authentication against Active Directory succeeded Validation of User Credentials successful	
		Authentication Passed	
		EAP-MSCHAP authentication attempt passed	
		Prepared EAP-Request with another EAP-FAST challenge	
	-	Returned RADIUS Access-Challenge Received RADIUS Access-Request	
		RADIUS is re-using an existing session	
		Extracted EAP-Response containing EAP-FAST challenge-response	
		Extracted EAP-Response for inner method containing MSCHAP challenge-response	
		Inner EAP-MSCHAP authentication succeeded	
		Prepared EAP-Success for inner EAP method	
		EAP-FAST inner method finished successfully	
		Prepared EAP-Request with another EAP-FAST challenge	
	11006	Returned RADIUS Access-Challenge	
		Received RADIUS Access-Request	
	11018	RADIUS is re-using an existing session	
	12104	Extracted EAP-Response containing EAP-FAST challenge-response	=
	12126	EAP-FAST cryptobinding verification passed	
	12219	Selected identity type 'Machine' 'Machine' Identity Type Selected	
	12125	EAP-FAST inner method started	
	11521	Prepared EAP-Request/Identity for inner EAP method	
	12105	Prepared EAP-Request with another EAP-FAST challenge	
	11006	Returned RADIUS Access-Challenge	
	11001	Received RADIUS Access-Request	
	<		>
1			

1	11018 RADIUS is re-using an existing session
1	12104 Extracted EAP-Response containing EAP-FAST challenge-response
1	12212 Identity type provided by client is equal to requested
1	11522 Extracted EAP-Response/Identity for inner EAP method
1	11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
1	12105 Prepared EAP-Request with another EAP-FAST challenge
1	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
	11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
	Evaluating Identity Policy
	15006 Matched Default Rule
	15013 Selected Identity Store - Internal Users
	24210 Looking up User in Internal Users IDStore - jeppich,host/labstation
	24216 The user is not found in the internal users identity store
2	24431 Authenticating machine against Active Directory Validation of 'Machine' Credentials successful
2	24470 Machine authentication against Active Directory is successful
2	22037 Authentication Passed 🛛 🖸
	11824 EAP-MSCHAP authentication attempt passed
	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
1	11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response
1	11814 Inner EAP-MSCHAP authentication succeeded MSCHAPv2 inner method authentication
1	11519 Prepared EAP-Success for inner EAP method successful
1	12128 EAP-FAST inner method finished successfully
1	12105 Prepared EAP-Request with another EAP-FAST challenge
1	11006 Returned RADIUS Access-Challenge
1	11001 Received RADIUS Access-Request
1	11018 RADIUS is re-using an existing session
1	12104 Extracted EAP-Response containing EAP-FAST challenge-response
	12126 EAP-FAST cryptobinding verification passed
	Evaluating Authorization Policy
	15048 Queried PIP
	15048 Queried PIP
	ISUAR Outpited DID
<	
1	15048 Queried PIP
1	15048 Queried PIP
1	15004 Matched rule
1	15004 Matched rule
1	15004 Matched rule
	15004 Matched rule
	15016 Selected Authorization Profile - both_user_&_machine_credentials_passed_auth
	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 Authentication
	12106 EAP-FAST authentication phase finished successfully Successful
	11503 Prepared EAP-Success
	Evaluating Authorization Policy 15048 Queried PIP
	15048 Queried PIP
	15004 Matched rule
	15004 Matched rule Authorization Profile selected, end-user placed in VLAN 1
1	15004 Matched rule
1	15016 Selected Authorization Profile - both_user_&_machine_credentials_passed_auth
1	11002 Returned RADIUS Access-Accept

Procedure 26 Log Details of an End-User Logging in from a personal laptop

Machine credentials fail and user credentials have been successfully validated. Below are the RADIUS Authentication Details and detailed EAP transaction logs of the authentication as illustrated below

르 🚔 🖻	Launch Interactive	: Yiewer 🛐
RADIUS Authenticatio	ion Details	
Showing Page	ge 1 of 1 First Prev Next Last Goto Page: Go	
Authentication Summa	ary	<u> </u>
Logged At:	March 24,2012 7:35:14,351 PM	
RADIUS Status:	Authentication succeeded	
NAS Failure:		
Username:	jeppich,host/skiber-xp	
MAC/IP Address:	<u>C8:BC:C8:90:8D:FC</u>	
Network Device:	<u>3750x : 192.168.1.2 : GigabitEthernet1/0/15</u>	
Allowed Protocol:	EAPFast_EAPChaining	
Identity Store:	AD1	
Authorization Profiles:		
SGA Security Group:		
Authentication Protoco	ol : EAP-FAST(EAP-MSCHAPv2)	
□_Authentication Resu	ult	
User-Name=		
	on:c0a8011400000024F6E6841	
	114000000024F6E6841:ise/122009432/	
Termination-Action=R.		
Tunnel-Type=(tag=1) Tunnel-Medium-Type=		

블 🚔 🖻			Launch Interactive Viewer
RADIUS Authentication Details			
Showing Page 1 of 1	First Prev Next Last	Goto Page: Go	
⊡_Authentication Details			
Logged At:	March 24,2012 7:35:14.351 PM		
Occurred At:	March 24,2012 7:35:14.350 PM		
Server:	ise		
Authentication Method:	dot1x		
EAP Authentication Method :	EAP-MSCHAPv2		
EAP Tunnel Method :	EAP-FAST		
Jsername:	jeppich,host/skiber-xp		
RADIUS Usemame :	anonymous		
Calling Station ID:	C8:BC:C8:90:8D:FC		
Framed IP Address:			
Use Case:			
Network Device:	<u>3750x</u>		
Network Device Groups:	Device Type#All Device Types,Location#All Locations		
NAS IP Address:	<u>192.168.1.2</u>		
NAS Identifier:			
NAS Port:	50115		
NAS Port ID:	<u>GigabitEthernet1/0/15</u>		
NAS Port Type:	Ethernet		
Allowed Protocol:	EAPFast EAPChaining		
Service Type:	Framed		
dentity Store:	AD1		
Authorization Profiles:	MachineFail_UserPass		
provide a second			

트 🖹 🖹	Launch Interactive Viewer
RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next Last Goto Page: Go
Authorization Profiles:	MachineFail_UserPass
Active Directory Domain:	cfacres007.com
dentity Group:	
llowed Protocol Selection Matched R	ule: EAPChaining_wired
lentity Policy Matched Rule:	Default
elected Identity Stores:	Internal Users,AD1,Internal Users,AD1
uthorization Policy Matched Rule:	Default
GA Security Group:	
AA Session ID: .udit Session ID:	ise/122009432/4
unnel Details:	
cimer Details. Sisco-AVPairs:	
ISCO-AVE allS.	Confect/ansignated a Destinction Dest=1645 Destance/Destino Exercised MTL = 1500 State=37.0DMS.acaiaelDes0.00011400000000
Other Attributes:	ConfigVersionId=4, DestinationPort=1645, Protocol=Radius, Framed-MTU=1500, State=37CPMSessionID=c0a8011400000002. Key-Name=,EapChainingResult=User succeeded and machine failed,CPMSessionID=c0a80114000000024F6E6841,EndF FC,EapChainingResult=User succeeded and machine failed,Device Type=Device Type#All Device Types,Location=Location# Locations,IdentityAccessRestricted=true,Device IP Address=192.168.1.2,Called-Station-ID=50.3D:E5:C4:05:8F
Posture Status:	NotApplicable
EPS Status:	
1_Steps	
11001 Received RADIUS Access-Rec	luest
11017 RADIUS created a new sessio	n
Evaluating Service Selection Policy	
15048 Queried PIP	
15048 Queried PIP	
15048 Queried PIP	
15048 Queried PIP	
15004 Matched rule	
11507 Extracted EAP-Response/Iden	tity
12100 Prepared EAP-Request propos	ing EAP-FAST with challenge
12625 Valid EAP-Key-Name attribute	
11006 Returned RADIUS Access-Cha	
	•
11001 Received RADIUS Access-Rec	•
11018 RADIUS is re-using an existing	·
12102 Extracted EAP-Response cont	aining EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800 Extracted first TLS record; TLS) handshake started
12175 Received Tunnel PAC	
12805 Extracted TLS ClientHello mes	sage
12806 Prepared TLS ServerHello mes	•
	•
12801 Prepared TLS ChangeCipherSp	•
12802 Prepared TLS Finished messa	× ·
12105 Prepared EAP-Request with ar	nother EAP-FAST challenge
44000 D / L DADIUD A OL	
11006 Returned RADIUS Access-Cha	allenge

11018	RADIUS is re-using an existing session		
12104	Extracted EAP-Response containing EAP-FAST challenge-response		
	Extracted TLS Finished message		
12818	i TLS handshake succeeded		
12132	EAP-FAST built PAC-based tunnel for purpose of authentication		
	Starting EAP chaining		
	Selected identity type 'User'	Start EAP Chaining	
	EAP-FAST inner method started		
	Prepared EAP-Request/Identity for inner EAP method		
	Prepared EAP-Request with another EAP-FAST challenge		
	Returned RADIUS Access-Challenge	'User' Identity Type Selected	
	Received RADIUS Access-Request		
	RADIUS is re-using an existing session		
	Extracted EAP-Response containing EAP-FAST challenge-response		
	Identity type provided by client is equal to requested		
	Extracted EAP-Response/Identity for inner EAP method		
	Prepared EAP-Request for inner method proposing EAP-MSCHAP with the second s	th challenge	
	Prepared EAP-Request with another EAP-FAST challenge		
			~
	Returned RADIUS Access-Challenge		
	Received RADIUS Access-Request		
	I RADIUS is re-using an existing session		
	Extracted EAP-Response containing EAP-FAST challenge-response Extracted EAP-Response containing EAP-MSCHAP challenge-response	non far inner method and according EAD MCCUAD on possilisted	
	ating Identity Policy	ise for inner method and accepting EAP-MISCHAP as negotiated	
	i Matched Default Rule		
	I Selected Identity Store - Internal Users I Looking up User in Internal Users IDStore - jeppich,host/skiber-xp		
	The user is not found in the internal users identity store		
	Authenticating user against Active Directory	Validatina (Ulan) Cardantiala	=
	Vserreincening door against Active Directory Secretary	Validating 'User ' Credentials	-
	Authentication Passed		
	EAP-MSCHAP authentication attempt passed		
	Prepared EAP-Request with another EAP-FAST challenge		
	Returned RADIUS Access-Challenge		
	Received RADIUS Access-Request		
	RADIUS is re-using an existing session		
	Extracted EAP-Response containing EAP-FAST challenge-response		
11810	Extracted EAP-Response for inner method containing MSCHAP chal		
	Inner EAP-MSCHAP authentication succeeded	engenesponse	
	Prepared EAP-Success for inner EAP method		
	EAP-FAST inner method finished successfully		
	Prepared EAP-Request with another EAP-FAST challenge		
	i Returned RADIUS Access-Challenge		
	-		
	Received RADIUS Access-Request RADIUS is re-using an existing session		
	 Extracted EAP-Response containing EAP-FAST challenge-response 		
	EAP-FAST cryptobinding verification passed		
	I Selected identity type 'Machine' EAP-FAST inner method started		
	Prepared EAP-Request/Identity for inner EAP method	'Machine' Identity Type Selected	
	Prepared EAP-Request/identity for inner EAP method L Prepared EAP-Request with another EAP-FAST challenge		
	Returned RADIUS Access-Challenge		
	Received RADIUS Access-Request		
	RADIUS is re-using an existing session		
12104	Extracted EAP-Response containing EAP-FAST challenge-response		

	12212 Identity type provided by client is equal to requested	
	11522 Extracted EAP-Response/Identity for inner EAP method	
	11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge	
	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	
	11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated	
	Evaluating Identity Policy	
	15006 Matched Default Rule	
	15013 Selected Identity Store - Internal Users	
	24210 Looking up User in Internal Users IDStore - jeppich,host/skiber-xp	
	24216 The user is not found in the internal users identity store	
	24431 Authenticating machine against Active Directory	
	24486 Machine authentication against Active Directory has failed because the machine's account is disable Failed 'Machine' Authentication.	
	22057 The advanced option that is configured for a failed authentication request is used simulate personal laptop	
	22061 The 'Reject' advanced option is configured in case of a failed authentication request	
Ť	11823 EAP-MSCHAP authentication attempt failed	
	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	
	11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response	
	11815 Inner EAP-MSCHAP authentication failed	
	11520 Prepared EAP-Failure for inner EAP method	
	12117 EAP-FAST inner method finished with failure	
	22028 Authentication failed and the advanced options are ignored	
	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	
	Evaluating Authorization Policy	
Ť	15004 Matched rule	
	15004 Matched rule	
	1504 Matched Ne	
	15048 Queried PIP	
	15048 Queried PIP	
	15004 Matched rule Authorization Profile Selected 'Machine Fail UserPass'	
	15004 Matched rule	
	15016 Selected Authorization Profile - MachineFail_UserPass	
	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	
	12106 EAP-FAST authentication phase finished successfully	
	11503 Prepared EAP-Success	
	Evaluating Authorization Policy	
	15004 Matched rule	
	15004 Matched rule	
	15048 Queried PIP	

15004 Matched rule								
15016 Selected Authorization Profile - MachineFail_UserPass								
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								
12106 EAP-FAST authentication phase finished successfully	Authentication Successful							
11503 Prepared EAP-Success								
Evaluating Authorization Policy								
15004 Matched rule								
15004 Matched rule								
15048 Queried PIP								
15048 Queried PIP								
15048 Queried PIP								
15004 Matched rule								
15004 Matched rule								
15016 Selected Authorization Profile - MachineFail_UserPass	Authorization successful, end-user placed in VLAN 22							
11002 Returned RADIUS Access-Accept	······································							

Procedure 27 Log Details of an End-User Logging in from a Mobile Device

The mobile devices not support 'EAP Chaining', and falls back to EAP-FAST authentication, even though the user is authenticated. Below are the RADIUS Authentication Details and detailed EAP transaction logs of the authentication as illustrated below

📙 🚔 📾								Laur	ich Interactive Vie
RADIUS Authenticatio	n Details								
Showing Page	1 of 1			Next	Last	_		Goto Page: Go	
Authentication Summa	ry								
Logged At:	March 24,2012 8:00:	47.441 PM							
RADIUS Status:	Authentication succe	eeded							
NAS Failure:									
Username:	jeppich								
MAC/IP Address:	8C:77:12:A2:38:B9								
Network Device:	WLC : 192.168.1.5 :								
Allowed Protocol:	EAPFast_EAPChain	ning							
Identity Store:	AD1								
Authorization Profiles:	Nochaining_Userpas	s							
SGA Security Group:									
Authentication Protocol	: EAP-FAST(EAP-MS	CHAPv2)							
□_Authentication Resul	t								
User-Name=jeppich									
State=ReauthSession:0501a8c0000000bdffd6d4f									
Class=CACS:0501a8c0000000bdffd6d4f:ise/122009432/5					End-User placed in VLAN 12				
Termination-Action=RADIUS-Request									
Tunnel-Type=(tag=1) VLAN Tunnel-Medium-Type=(tag=1) 802									
Tunnel-Private-Group-									
		:71:17:09:do	1:84:2a:c4	4:9c:6d:3	4:fb:56:51	l:df:03:1c	c:ci	cc:fb:8b:c4:88:0e:f4:eb:5a	
								e8:f7:76:27:6a:79:a9:a1:7b	

블 🖹 🗟				Launch Interactive Viewe	er 🦻		
RADIUS Authentication Details							
Showing Page 1 of 1	First Prev No	ext Last	Goto Page: Go				
⊡Authentication Details					-		
Logged At:	March 24,2012 8:00:47.441	PM					
Occurred At:	March 24,2012 8:00:47.440						
Server:	ise .						
Authentication Method:	dot1x						
EAP Authentication Method :	EAP-MSCHAPv2						
EAP Tunnel Method :	EAP-FAST	EAP-FAST outer method	, MS-CHAPv2 inner 1	nethod			
Username:	jeppich						
RADIUS Username :	jeppich						
Calling Station ID:	8C:77:12:A2:38:B9						
Framed IP Address:							
Use Case:							
Network Device:	WLC						
Network Device Groups:	Device Type#All Device Type	Device Type#All Device Types,Location#All Locations					
NAS IP Address:	192.168.1.5						
NAS Identifier:	Cisco_63:75:80						
NAS Port:	1						
NAS Port ID:							
NAS Port Type:	Wireless - IEEE 802.11						
Allowed Protocol:	EAPFast_EAPChaining						
Service Type:	Framed						
Identity Store:	AD1						
Authorization Profiles:	Nochaining_Userpass				•		

≞ ≥	Launch Interactive Viewe
RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next Last Goto Page: Go
Identity Store:	AD1
Authorization Profiles:	Nochaining_Userpass
Active Directory Domain:	cfacres007.com
dentity Group:	
Allowed Protocol Selection Matched R	tule: EAPChaining_wireless
dentity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users,AD1
Authorization Policy Matched Rule:	Default
GA Security Group:	
AA Session ID:	ise/122009432/5
Audit Session ID:	0501a8c000000bdffd6d4f
unnel Details:	Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0) 12
Cisco-AVPairs:	audit-session-id=0501a8c0000000bdffd6d4f
Other Attributes:	ConfigVersionId=4, DestinationPort=1645, Protocol=Radius, Framed- MTU=1300, State=37 CPMSessionID=0501 a8c000000000bfffd6d4f;25SessionID=ise/122009432/5; ,Airespace- Wlan-Id=1, EapChainingResult=No chaining, CPMSessionID=0501 a8c00000000bdffd6d4f, EndPointMACAddress=8C- 77-12-A2-38-B9, EapChainingResult=No chaining, Device Type=Device Type#All Device Types, Location=Location#All Locations, IdentityAccessRestricted=false, Device IP Address=192.168.1.5, Called-Station-ID=00-19-a9-e0-65-60:1ab005
Posture Status:	NotApplicable
EPS Status:	
⊒_Steps	
11001 Received RADIUS Access-Re	auact
11017 RADIUS created a new sessio	un die
Evaluating Service Selection Policy	
15048 Queried PIP	
15048 Queried PIP	
15004 Matched rule	
11507 Extracted EAP-Response/Ider	ntity
12100 Prepared EAP-Request propos	sing EAP-FAST with challenge
11006 Returned RADIUS Access-Ch	allenge
11001 Received RADIUS Access-Re	-
11018 RADIUS is re-using an existing	taining EAP-FAST challenge-response and accepting EAP-FAST as negotiated
*	
12102 Extracted EAP-Response con	
12102 Extracted EAP-Response con 12800 Extracted first TLS record; TLS	
12102 Extracted EAP-Response con 12800 Extracted first TLS record; TLS 12175 Received Tunnel PAC	S handshake started
12102 Extracted EAP-Response con 12800 Extracted first TLS record; TLS 12175 Received Tunnel PAC 12805 Extracted TLS ClientHello mes	S handshake started
12102 Extracted EAP-Response con 12800 Extracted first TLS record; TLS 12175 Received Tunnel PAC 12805 Extracted TLS ClientHello mes 12806 Prepared TLS ServerHello mes	S handshake started ssage ssage
12102 Extracted EAP-Response con 12800 Extracted first TLS record; TLS 12175 Received Tunnel PAC 12805 Extracted TLS ClientHello mee 12806 Prepared TLS ServerHello mee 12801 Prepared TLS ChangeCipherS	S handshake started ssage ssage pec message
12102 Extracted EAP-Response con 12800 Extracted first TLS record; TLS 12175 Received Tunnel PAC 12805 Extracted TLS ClientHello mes 12806 Prepared TLS ServerHello mes 12801 Prepared TLS ChangeCipherS 12802 Prepared TLS Finished messa	S handshake started ssage spec message age
 12800 Extracted first TLS record; TLS 12175 Received Tunnel PAC 12805 Extracted TLS ClientHello mes 12806 Prepared TLS ServerHello mes 12801 Prepared TLS ChangeCipherS 	S handshake started ssage spec message age inother EAP-FAST challenge

	11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session		
	12104 Extracted EAP-Response containing EAP-FAST challenge-response		
	12804 Extracted TLS Finished message		
	12816 TLS handshake succeeded		
	12132 EAP-FAST built PAC-based tunnel for purpose of authentication		
	12209 Starting EAP chaining	EAP Chaining started	
	12218 Selected identity type 'User'		
	12125 EAP-FAST inner method started		
	11521 Prepared EAP-Request/Identity for inner EAP method		
	12105 Prepared EAP-Request with another EAP-FAST challenge		
	11006 Returned RADIUS Access-Challenge		
	11001 Received RADIUS Access-Request	'User' Identity Type Selected	
	11018 RADIUS is re-using an existing session		
	12104 Extracted EAP-Response containing EAP-FAST challenge-response		
	12220 Client does not support EAP chaining. Switching to usual mode	Client DOES NOT support EAP-	
	11522 Extracted EAP-Response/Identity for inner EAP method	Chaining	
	11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with cl	hallenge	
	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		
	11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response	for inner method and accepting EAP-MSCHAP as negotiated	
	Evaluating Identity Policy		
	15006 Matched Default Rule		
	15013 Selected Identity Store - Internal Users		
	24210 Looking up User in Internal Users IDStore - jeppich		
	24216 The user is not found in the internal users identity store	User Credentials are validated	
	24430 Authenticating user against Active Directory		
	24402 User authentication against Active Directory succeeded		
	22037 Authentication Passed 11824 EAP-MSCHAP authentication attempt passed		
	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		
	11810 Extracted EAP-Response for inner method containing MSCHAP challeng	e-response	
	11814 Inner EAP-MSCHAP authentication succeeded		
	11519 Prepared EAP-Success for inner EAP method		
	12128 EAP-FAST inner method finished successfully		
	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 Because containing EAP-EAST challenge response		
	12104 Extracted EAP-Response containing EAP-FAST challenge-response 12126 EAP-FAST cryptobinding verification passed		
	12126 EAP-FAST cryptobinding ventication passed 12106 EAP-FAST authentication phase finished successfully		
	11503 Prepared EAP-Success		
	24423 ISE has not been able to confirm previous successful machine authentica	ation for user in Active Directory	
	Evaluating Authorization Policy		
	15004 Matched rule		
	15048 Queried PIP		
	15048 Queried PIP		
	15004 Matched rule		
	15004 Matched fore 15016 Selected Authorization Profile - Nochaining_Userpass		
	11002 Returned RADIUS Access-Accept		
1	<		>

Macintosh, iphone, Android, iPad Devices

EAP Chaining is meant for corporate devices and not for personal devices, EAP chaining does not need to be supported on the latest hot device out on the market. However, as these newer devices become corporate devices controlled by IT, they need to have full access to the corporate network.

Today, EAP Chaining is limited to Windows on the client side. EAP Chaining is new technology and it has not made its way into the operating system clients as yet. Windows has enough hooks in the operating system so a separate client can operate on its own whereas many of the other operating systems do not have the necessary hooks.

Another approach is required to permit these newer devices to gain full access to the corporate network until the native operating systems support EAP Chaining. The traditional method to identify corporate devices has been certificates. Certificates can be locked to most devices and permit the identification of corporate devices.

Certificates are not recommended for personal devices, just for corporate devices. Personal devices tend to change more often and change without notice. Changing without notice leads to a potential exposure of corporate data as the old device gets sold off and a savvy buyer looks for existing configuration data on the old personal device.

EAP Chaining permits users to continue with their username / password credential they have today for their corporate Windows device on personal devices

Q: Is EAP Chaining only supported on EAP-FAST?

A: Today, EAP Chaining is only supported on EAP-FAST. As adoption grows in the coming years, we expect other EAP types to incorporate EAP-Chaining. This will depend on the authors of the various EAP types updating the respective specifications in the IETF.

Q: Is EAP Chaining supported on ACS?

A: No, EAP-Chaining is only supported on the Identity Services Engine (ISE) version 1.1 MnR or greater.

Q: How does EAP Chaining compare to Machine Access Restriction (MAR) on ACS?

A: MAR is a supplicant and EAP-type agnostic. EAP Chaining requires a supplicant and a server that both support the technology. MAR requires a machine authentication followed by a user authentication on the same access point or switch. EAP Chaining requires both a machine authentication and a user authentication but the two authentications need not be on the same access point or switch. EAP Chaining makes the transition from Ethernet to Wi-Fi and back again much easier than MAR.

Q: Is EAP Chaining a standards-based implementation or proprietary to Cisco?

A: Yes, EAP Chaining is a standards-based implementation, it is part of the EAP-FAST v2 specification (<u>http://tools.ietf.org/html/draft-zhou-emu-eap-fastv2-00</u>).

Cisco TrustSec System:

- <u>http://www.cisco.com/go/trustsec</u>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing DesignZone TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides: http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches: http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches: <u>http://www.cisco.com/en/US/products/ps7077/products installation and configuration guides list.html</u>
- For Cisco Catalyst 3000-X series switches: http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches: <u>http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.ht</u> <u>ml</u>
- For Cisco Catalyst 6500 series switches: http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers: <u>http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html</u>
- For Cisco Wireless LAN Controllers: <u>http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html</u>