Deploying EAP Chaining with AnyConnect NAM and Cisco ISE

Secure Access How -To Guides Series

Author: Aaron Woland

Date: August 2012

Table of Contents

Executive Summary

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 end-users 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 and 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

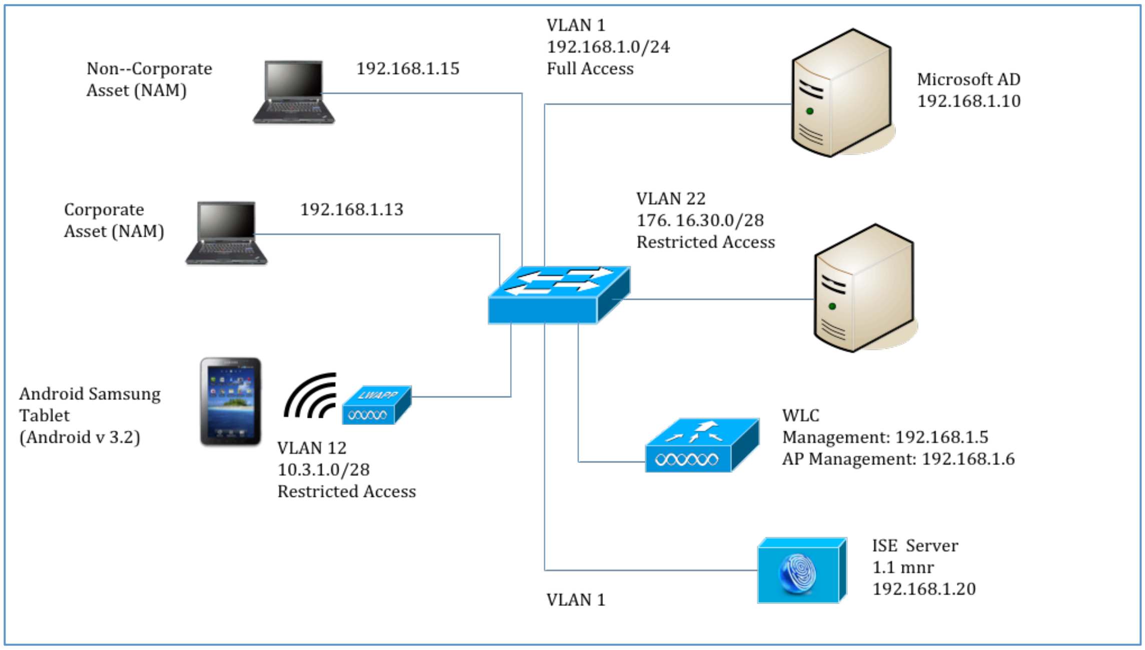


Figure 1. Architecture used in this document

Software/Hardware Requirements:

Client:

Laptop or desktop computer with an Ethernet NIC or WiFi NIC and one of the following operating systems:

- Windows 7 SP1 x 86 (32-bit) and x64 (64-bit)
- 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 ldentity-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.

Design Parameters

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

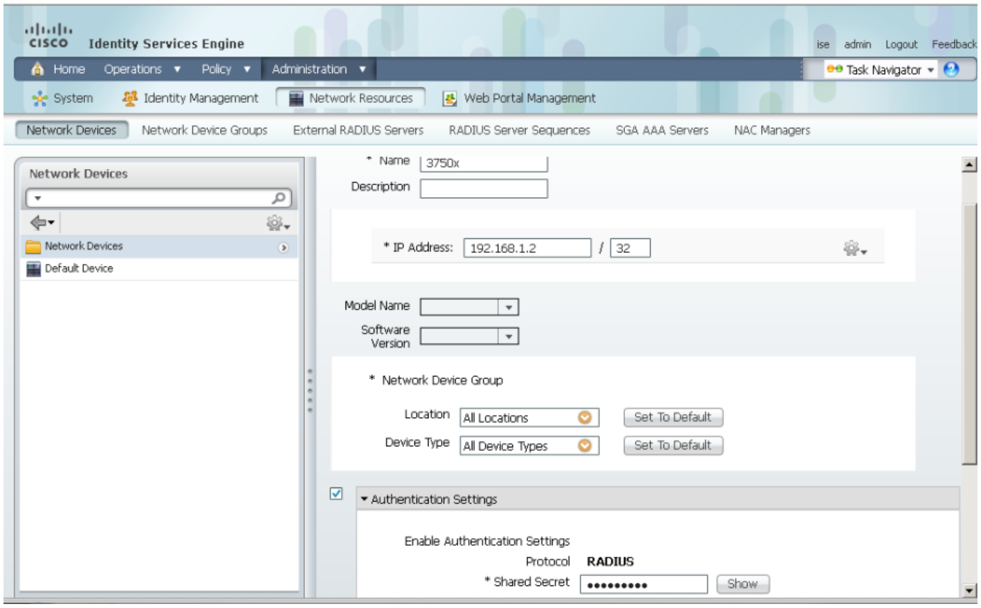
Configuring ISE

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

Adding Network Devices to ISE

Configure your WLC and switch for ISE and enable RADIUS.

Step 1 Select → Administration → Network Resources → Network Devices.
Step 2 Select → 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.



* Name: 3750x
Description:
* IP Address: 192.168.1.2 / 32
Model Name:
Software Version:
* Network Device Group
Location: All Locations
Device Type: All Device Types
☑ ▾ Authentication Settings
Enable Authentication Settings
Protocol: RADIUS
* Shared Secret: •••••••••

Figure 2. Example of the switch configuration

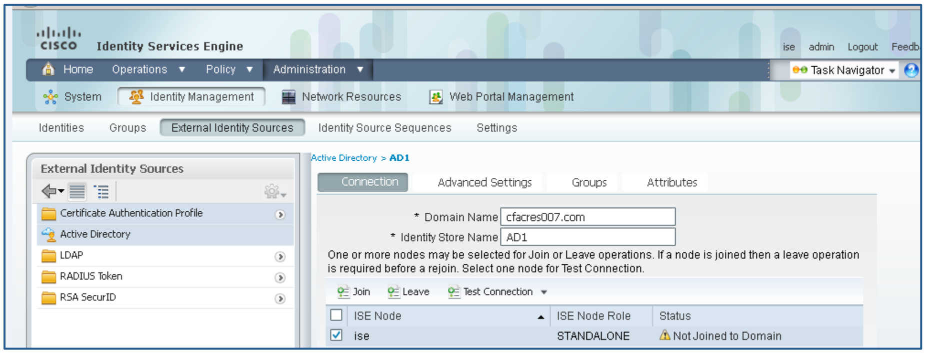
Add Microsoft Active Directory as the External Identity Store

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

Step 1 Select → Administration → Identity Management → External Identity Sources → Active Directory.
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.


Identity Services Engine
ise admin Logout Feedb
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > AD1
Connection Advanced Settings Groups Attributes
Join Leave Test Connection

* Domain Name cfacres007.com

* Identity Store Name AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

	ISE Node	ISE Node Role	Status
☑	ise	STANDALONE	⚠ Not Joined to Domain

Figure 3. Active Directory Setting

Procedure 3 Join the Active Directory Domain

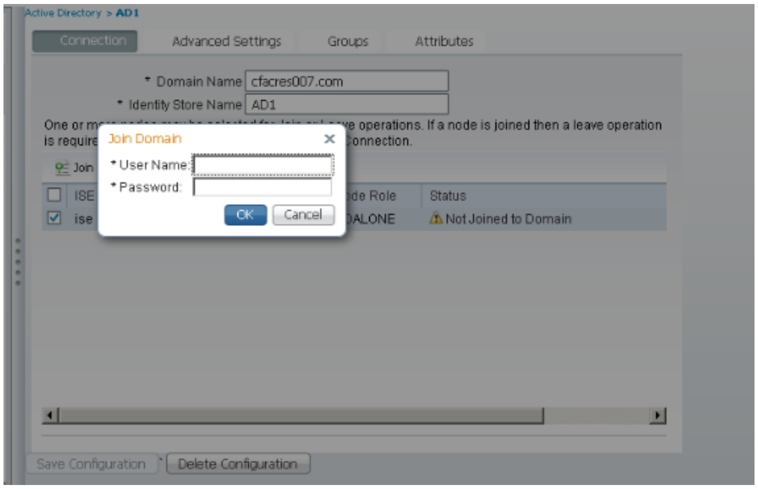
Each ISE node must join the AD domain.

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.
```

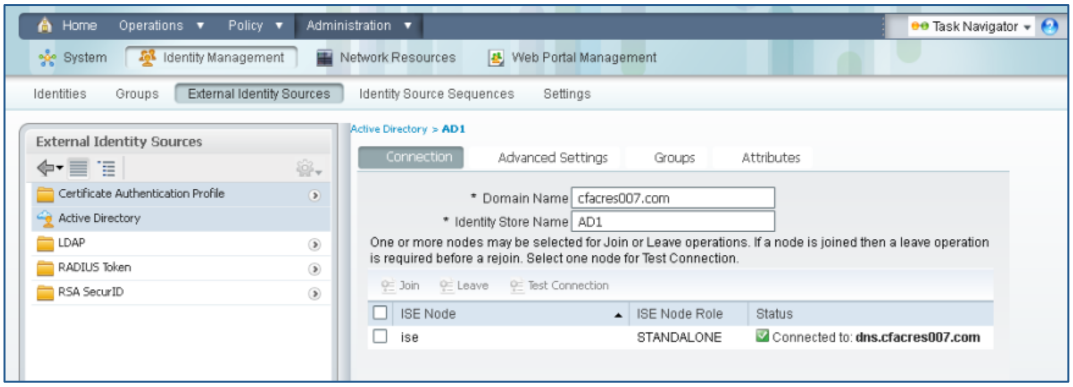

Active Directory > AD1
Connection Advanced Settings Groups Attributes
Join Domain
* User Name
* Password
OK Cancel
Join
Save Configuration Delete Configuration

* Domain Name cfacres007.com

* Identity Store Name AD1

	ISE	de Role	Status
☑	ise	ALONE	⚠ Not Joined to Domain

Figure 4. Prompt to join the domain


Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > AD1
Connection Advanced Settings Groups Attributes
Join Leave Test Connection

* Domain Name cfacres007.com

* Identity Store Name AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

	ISE Node	ISE Node Role	Status
□	ise	STANDALONE	✓ Connected to: **dns.cfacres007.com**

Figure 5. Results after the successful join to the domain

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 → Identity Management → External Identity Sources → 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'

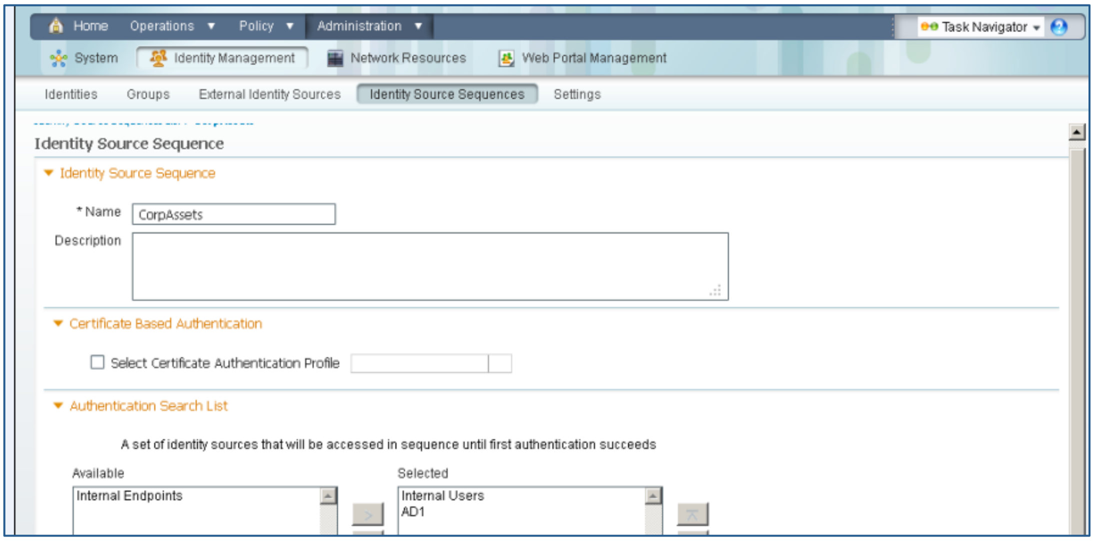
Defining the Identity Source Sequence

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 → Identity Management → 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



Identity Source Sequence

▼ Identity Source Sequence

* Name: CorpAssets

Description:

▼ Certificate Based Authentication

□ Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users AD1

Figure 6. Identity Source Sequence

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.

Enable EAP Chaining in the EAP-FAST Protocol

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

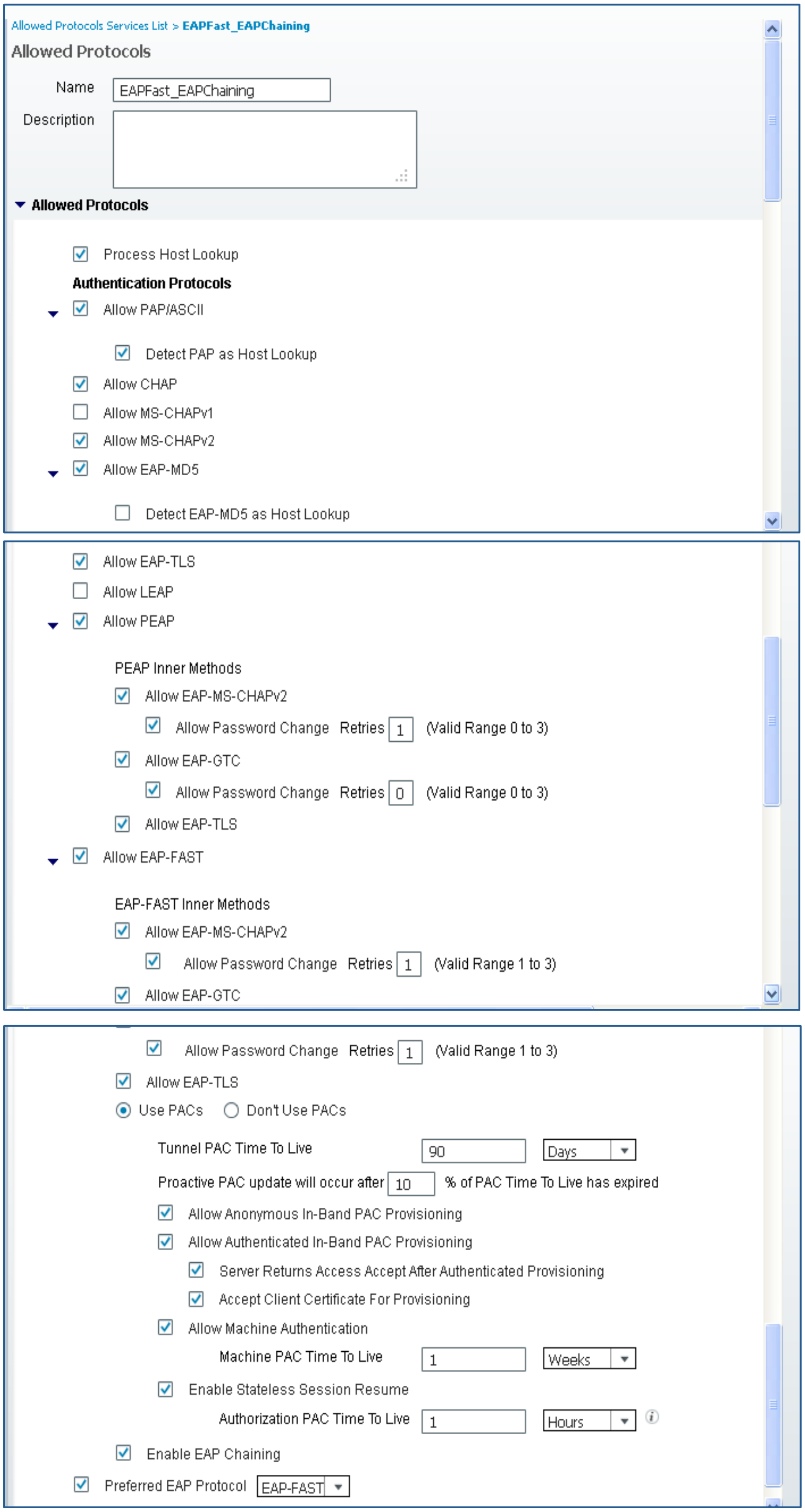
Step 1 Select Policy → Policy Elements → Results → Authentication → Authentication Protocols.
Step 2 Click Add.
Step 3 Enter the name of the Allowed Protocols.

```
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.



Allowed Protocols Services List > EAPFast_EAPChaining

Allowed Protocols

Name: EAPFast_EAPChaining

Description:

▼ Allowed Protocols

- ☑ Process Host Lookup

Authentication Protocols

- ☑ Allow PAP/ASCII
  - ☑ Detect PAP as Host Lookup
- ☑ Allow CHAP
- □ Allow MS-CHAPv1
- ☑ Allow MS-CHAPv2
- ☑ 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 EAP-GTC
    - ☑ Allow Password Change Retries 0 (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
    - 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

Figure 7. EAPFast_EAPChaining Allowed Protocols Definition

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 → 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 → Existing Conditions from library → Compound Condition .

Step 6 Choose Wireless_802.1X.

Step 7 Click on the cursor.

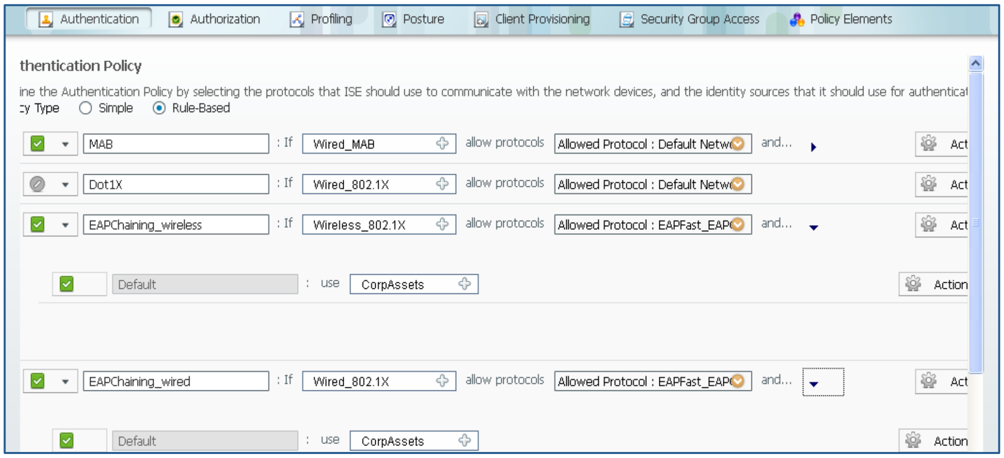
Step 8 Click Internal Users → and select your Identity Source.

```
In this example CorpAssets was used.
```

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

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

Step 11 Save the changes .



thentication Policy

ine the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authenticat

:y Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and... Act

Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw Act

☑ EAPChaining_wireless : If Wireless_802.1X allow protocols Allowed Protocol : EAPFast_EAP and... Act

☑ Default : use CorpAssets Action

☑ EAPChaining_wired : If Wired_802.1X allow protocols Allowed Protocol : EAPFast_EAP and... Act

☑ Default : use CorpAssets Action

Figure 8. Completed Authentication Policies

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

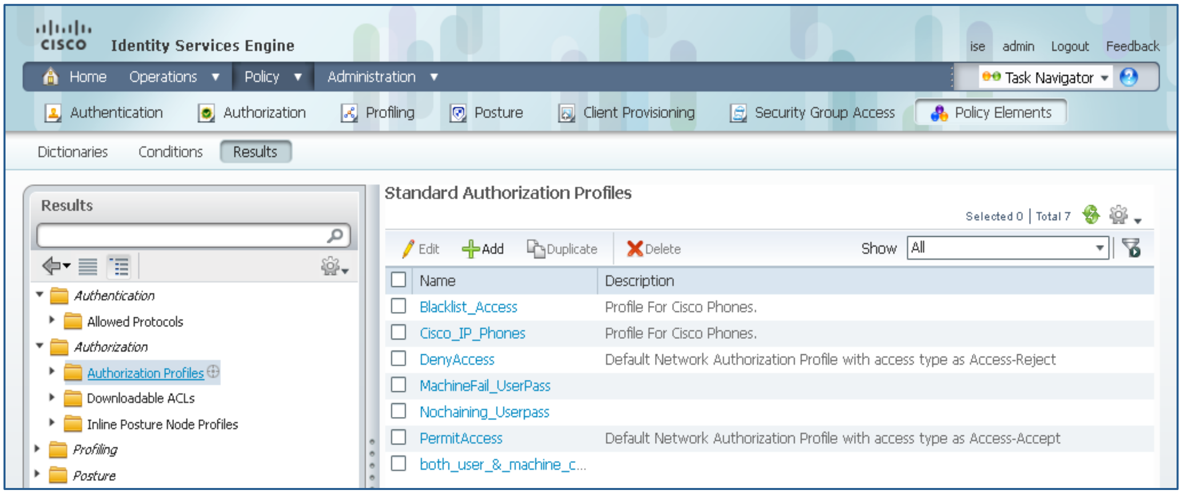
Define the Authorization Profiles

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.


Identity Services Engine
ise admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator ▼
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Allowed Protocols
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Selected 0 | Total 7
Edit Add Duplicate Delete Show All

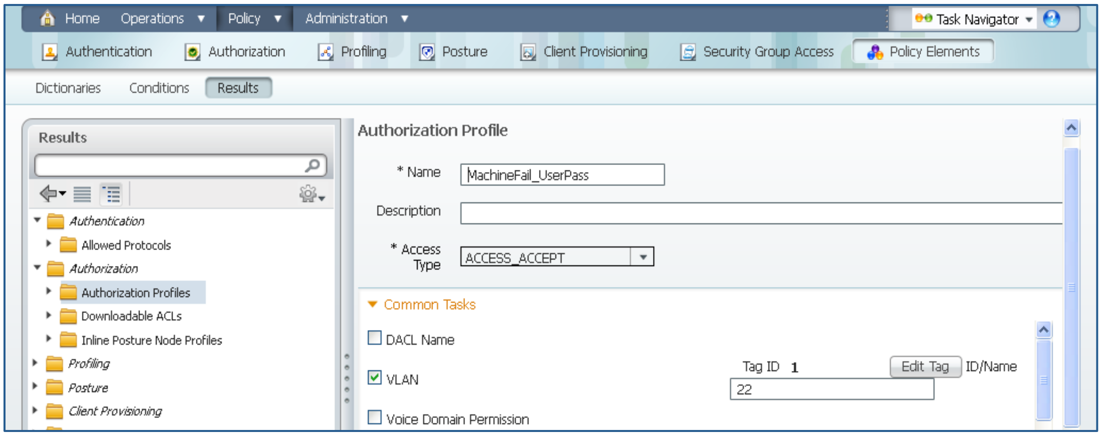
Standard Authorization Profiles

☐	Name	Description
☐	Blacklist_Access	Profile For Cisco Phones.
☐	Cisco_IP_Phones	Profile For Cisco Phones.
☐	DenyAccess	Default Network Authorization Profile with access type as Access-Reject
☐	MachineFail_UserPass	
☐	Nochaining_Userpass	
☐	PermitAccess	Default Network Authorization Profile with access type as Access-Accept
☐	both_user_&_machine_c...	

Figure 9. Completed Authorization Profiles

Define the Authorization Profile for 'MachineFail_UserPass'.

Step 1 Navigate to PolicyElements → Results → Authorization → 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.


Home Operations ▼ Policy ▼ Administration ▼
Task Navigator ▼
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Allowed Protocols
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Edit Tag

Authorization Profile

* Name: MachineFail_UserPass

Description:

* Access Type: ACCESS_ACCEPT

▼ Common Tasks

☐ DACL Name

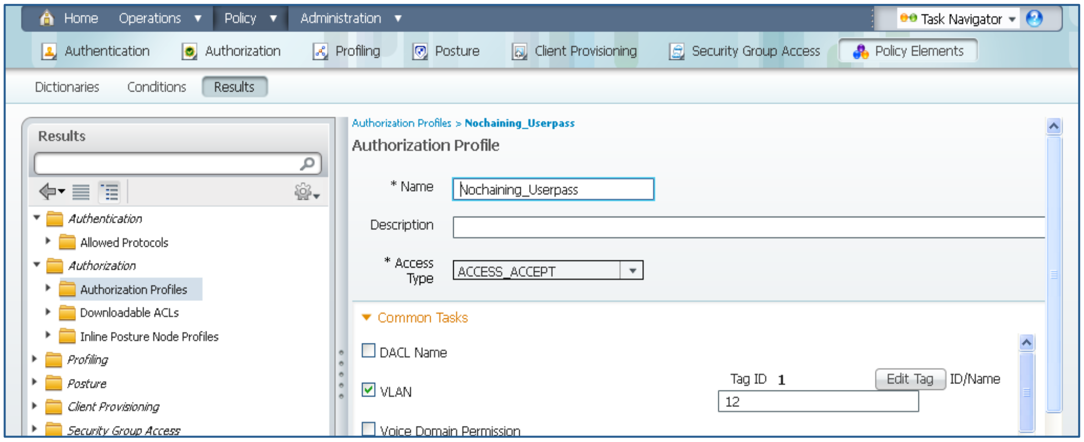
☑ VLAN Tag ID 1 ID/Name 22

☐ Voice Domain Permission

Figure 13. Authorization Profile for 'MachineFail_UserPass'

Define the Authorization Profile for 'NoChaining_UserPass'.

Step 1 Navigate to Policy → PolicyElements → Results → Authorization → 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.



Authorization Profiles > Nochaining_Userpass

Authorization Profile

* Name: Nochaining_Userpass

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☐ DACL Name

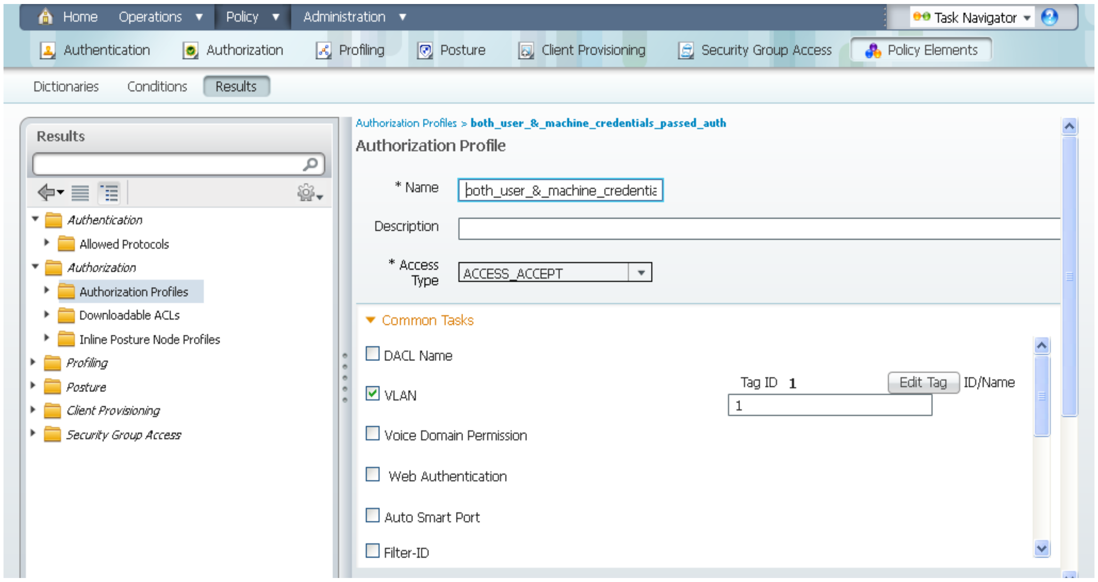
☑ VLAN — Tag ID 1 — ID/Name 12

☐ Voice Domain Permission

Figure 10. Authorization Profile for 'NoChaining_UserPass'

Define the Authorization Profile for 'both_user_&_machine_credentials_passed_auth'

Step 1 Navigate to Policy → PolicyElements → Results → Authorization → 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.



Authorization Profiles > both_user_&_machine_credentials_passed_auth

Authorization Profile

* Name: both_user_&_machine_credentia

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☐ DACL Name

☑ VLAN — Tag ID 1 — ID/Name 1

☐ Voice Domain Permission

☐ Web Authentication

☐ Auto Smart Port

☐ Filter-ID

Figure 11. Authorization Profile for 'both_user_&_machine_credentials_passed_auth'

Defining Authorization Condition Rules and Authorization Policies

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 → Policy Elements → Conditions → Authorization → Compound Conditions
Step 2 Add name, 'EAP-Chaining_UserPASS_MachinePASS.'

Step 3 Add description, this is optional.

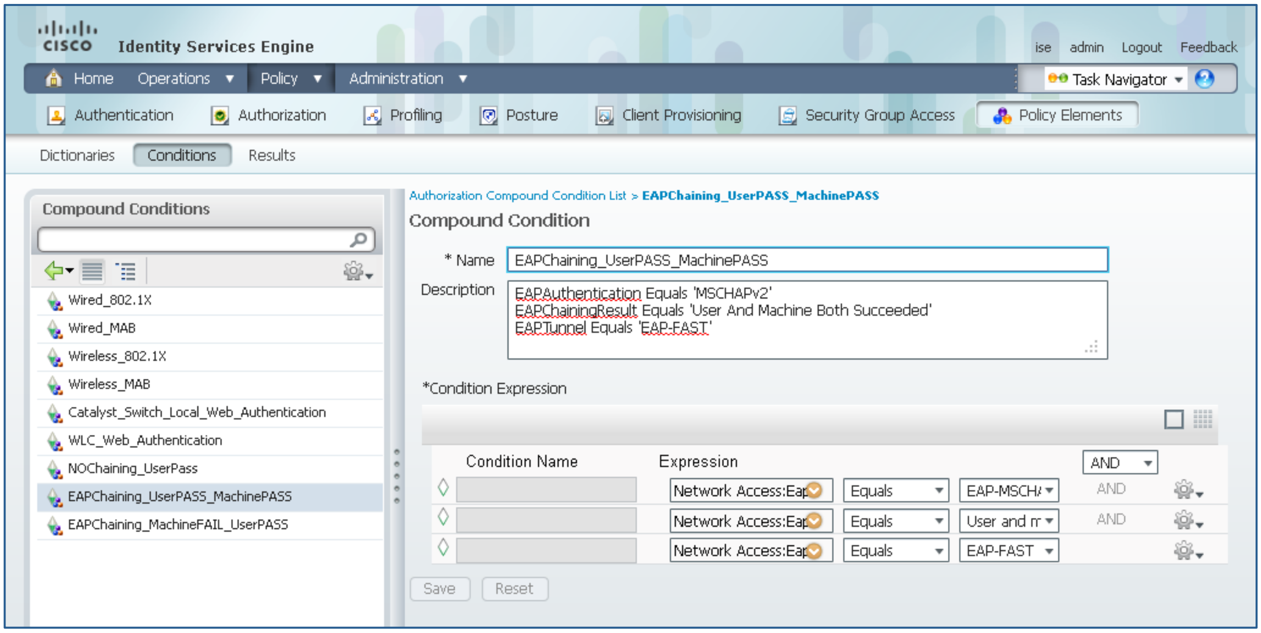
For **expressions**, select the following:

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.



* Name: EAPChaining_UserPASS_MachinePASS

Description:
EAPAuthentication Equals 'MSCHAPv2'
EAPChainingResult Equals 'User And Machine Both Succeeded'
EAPTunnel Equals 'EAP-FAST'

*Condition Expression

Condition Name	Expression			AND
	Network Access:Eap	Equals	EAP-MSCHA	AND
	Network Access:Eap	Equals	User and m	AND
	Network Access:Eap	Equals	EAP-FAST	

Figure 12. EAPChaining_UserPASS_MachinePASS Compound Condition

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.

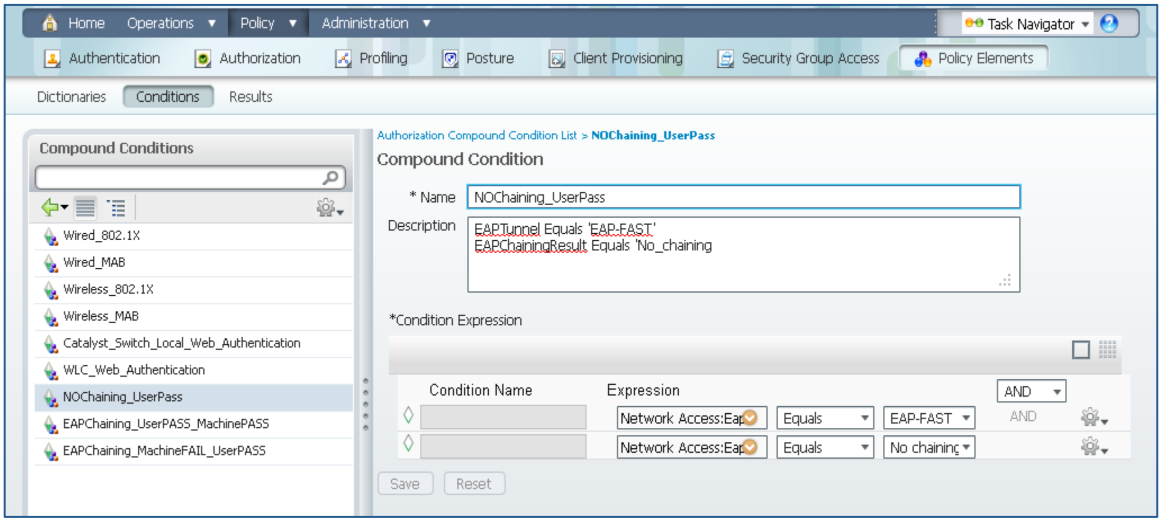
Step 1 Select Policy → Policy Elements → Conditions → Authorization → Compound Conditions.
Step 2 Add name, ‘NOChaining_UserPASS.’
Step 3 Add description, this is optional.

For expressions, select the following:

a. Network Access:EAPTunnel equals EAP-FAST

b. Network Access:EAP-ChainingResult equals No_chaining

Step 4 **Submit** the changes.



Authorization Compound Condition List > **NOChaining_UserPass**

Compound Condition

* Name: NOChaining_UserPass

Description:
EAPTunnel Equals 'EAP-FAST'
EAPChainingResult Equals 'No_chaining

*Condition Expression

Condition Name	Expression			AND
	Network Access:Eap	Equals	EAP-FAST	AND
	Network Access:Eap	Equals	No chaininc	

Figure 13. NOChaining_UserPass Compound Condition

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 → Policy Elements → Conditions → Authorization → Compound Conditions.
Step 2 Add name, ‘EAP-Chaining_MachineFAIL_UserPASS.’
Step 3 Add description, this is optional.

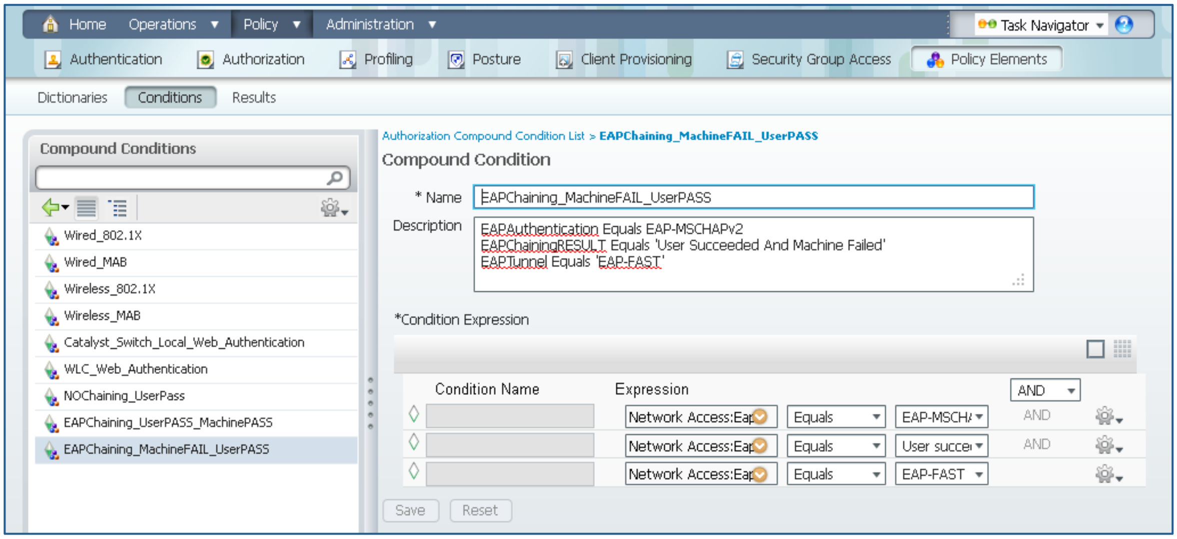
For expressions, select the following:

a. Network Access:EAPAuthentication equals EAP-MSCHAPv2

b. Network Access:EAP-ChainingResult equals User Succeeded and Machine Failed

c. Network Access: EAPTunnel equals EAP-FAST

Step 4 **Submit** the changes.



Authorization Compound Condition List > **EAPChaining_MachineFAIL_UserPASS**

Compound Condition

* Name: EAPChaining_MachineFAIL_UserPASS

Description:
EAPAuthentication Equals EAP-MSCHAPv2
EAPChainingRESULT Equals 'User Succeeded And Machine Failed'
EAPTunnel Equals 'EAP-FAST'

*Condition Expression

Condition Name	Expression			AND
	Network Access:Eap	Equals	EAP-MSCH/	AND
	Network Access:Eap	Equals	User succe	AND
	Network Access:Eap	Equals	EAP-FAST	

Figure 14. EAPChaining_MachineFAIL_UserPASS Compound Condition

Creating Authorization Policies

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

Create an Authorization Policy for 'UserPASSED_MachinePASSED'

Step 1 Navigate to Policy → 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 → Condition → 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 → Standard → both_user_&_machine_credentials_passed.
Step 8 **Save** the changes..

Create an Authorization Policy for 'NoCHAINING_UserPASSED'

Step 1 Navigate to Policy → 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
```

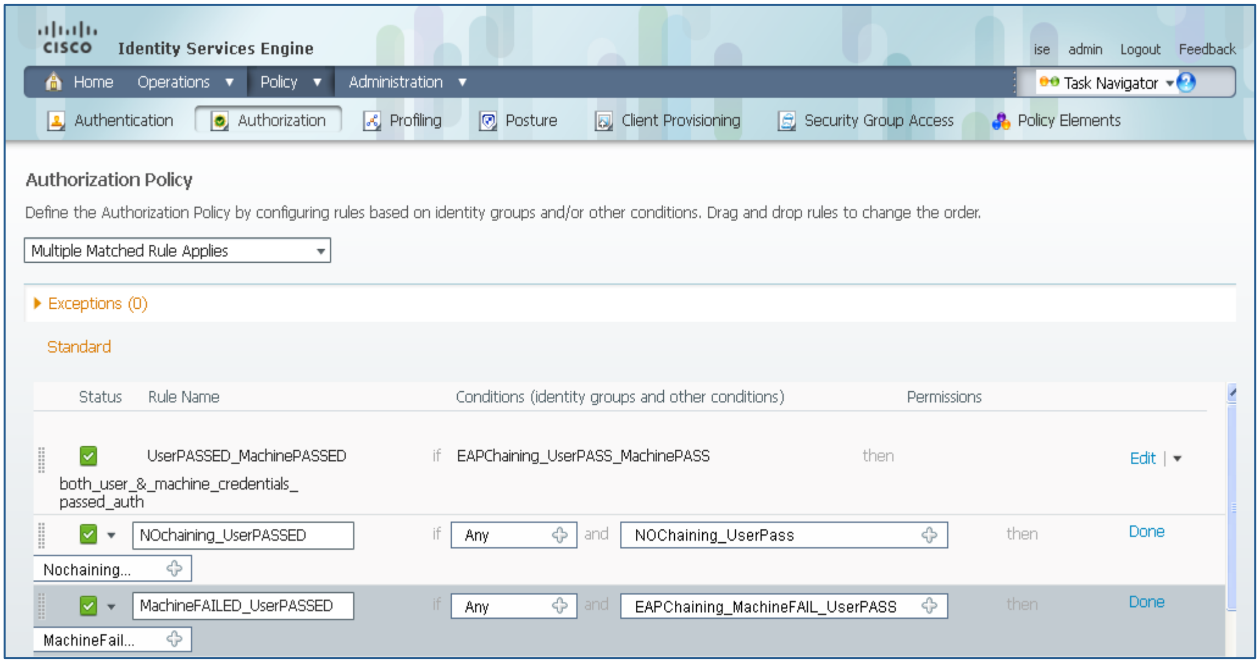
Step 4 Under Conditions Select 'Existing Condition from Library' → Condition → Compound Conditions → 'NoCHAINING_UserPASS.'
Step 5 Click on the '+' next to 'Authz Profile' and select your authorization profile. Select Item → Standard → 'NoCHAINING_USerPASS.'
Step 6 **Save** the changes.

Create an Authorization Policy for 'MachineFAILED_UserPASSED'

Step 1 Navigate to Policy → Authorization → 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 → Condition → Compound Conditions → 'EAP-Chaining_MachineFAIL_UserPASS.'
Step 4 Click on '+' next to 'Authz Profile' and select your authorization profile. Select Item → Standard → 'EAP-Chaining_MachineFAIL_UserPASS.'
Step 5 **Save** the changes.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

Multiple Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	UserPASSED_MachinePASSED	if	EAPChaining_UserPASS_MachinePASS	then	both_user_&_machine_credentials_passed_auth	Edit
☑	NOchaining_UserPASSED	if	Any and NOChaining_UserPass	then	Nochaining...	Done
☑	MachineFAILED_UserPASSED	if	Any and EAPChaining_MachineFAIL_UserPASS	then	MachineFail...	Done

Figure 15. The completed authorization policies.

NAM Installation and Configuration

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

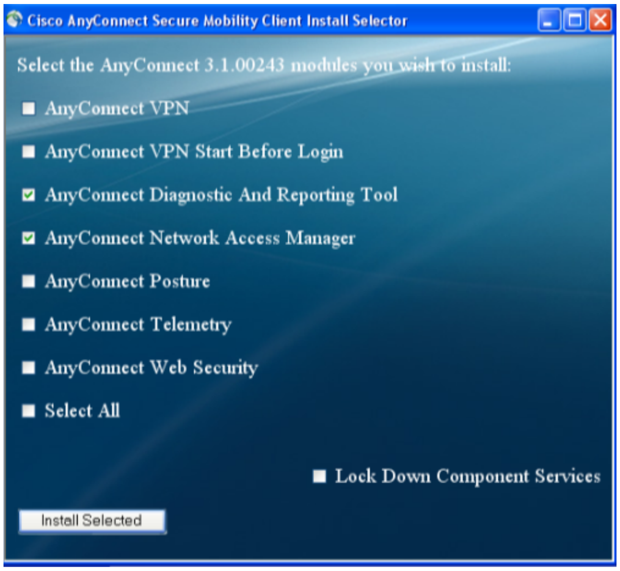
NAM Installation and Configuration

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 1 Enable AnyConnect Diagnostics and Reporting Tool .
Step 2 AnyConnect Network Access Manager.



Cisco AnyConnect Secure Mobility Client Install Selector

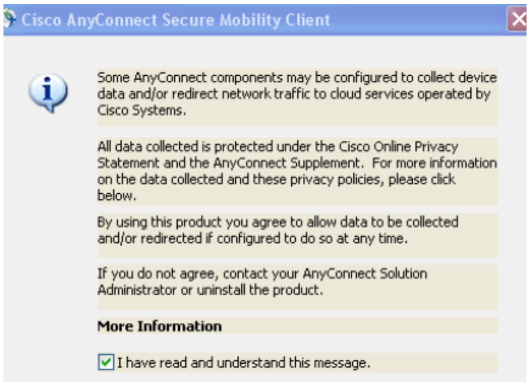
Select the AnyConnect 3.1.00243 modules you wish to install:

- □ AnyConnect VPN
- □ AnyConnect VPN Start Before Login
- ☑ AnyConnect Diagnostic And Reporting Tool
- ☑ AnyConnect Network Access Manager
- □ AnyConnect Posture
- □ AnyConnect Telemetry
- □ AnyConnect Web Security
- □ Select All

□ Lock Down Component Services

Figure 16. Installation Selectors

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.)



Cisco AnyConnect Secure Mobility Client

Some AnyConnect components may be configured to collect device data and/or redirect network traffic to cloud services operated by Cisco Systems.

All data collected is protected under the Cisco Online Privacy Statement and the AnyConnect Supplement. For more information on the data collected and these privacy policies, please click below.

By using this product you agree to allow data to be collected and/or redirected if configured to do so at any time.

If you do not agree, contact your AnyConnect Solution Administrator or uninstall the product.

More Information

☑ I have read and understand this message.

Figure 17. AnyConnect Quality Improvement Feature

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.

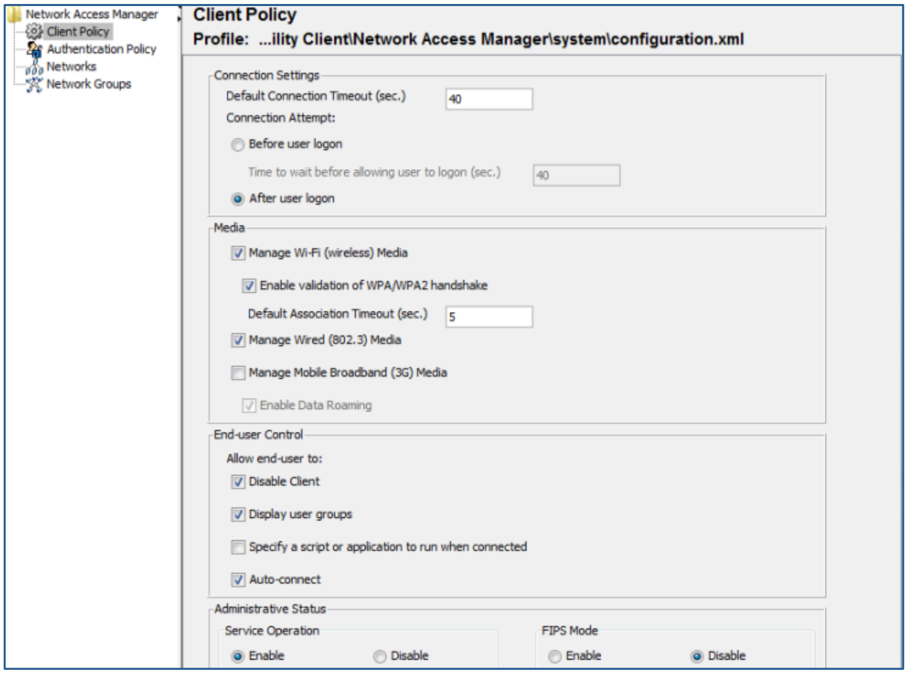
Note: Please note that the NAM configuration should be saved as ‘configuration.xml’, and saved to the ‘NewConfigFiles’ directory. Right-click on the AnyConnect GUI in the system tray, select ‘Network Repair’ . This will place the configuration.xml file into the NAM system directory.)

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

Step 2 Keep the defaults, and select → 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 1 NAM profile Editor



Client Policy

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Connection Settings

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:

☑ Disable Client

☑ Display user groups

□ Specify a script or application to run when connected

☑ Auto-connect

Administrative Status

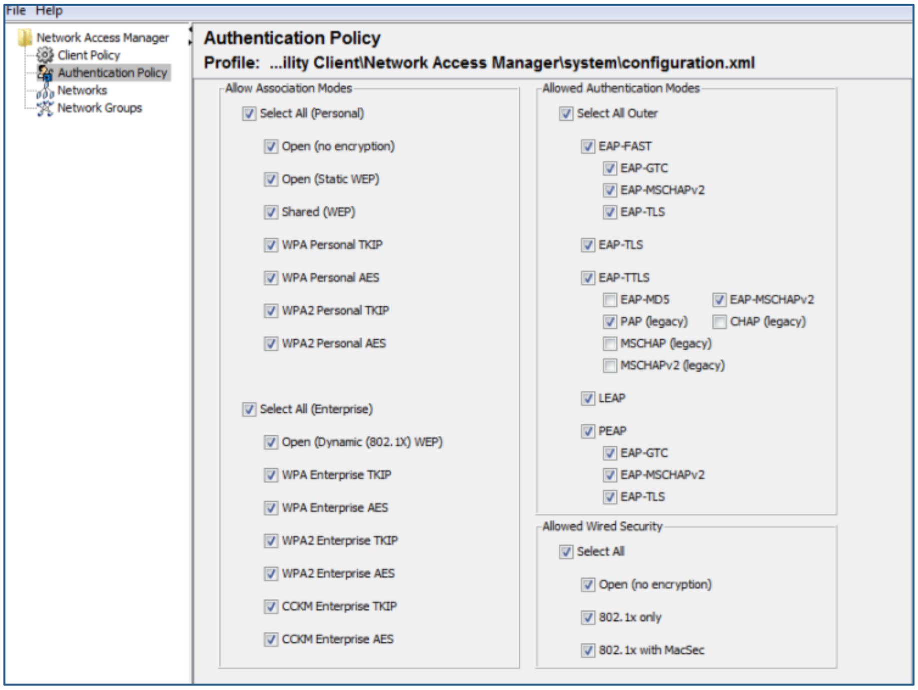
Service Operation: ● Enable ○ Disable

FIPS Mode: ○ Enable ● Disable

Figure 18. NAM profile Editor

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
```



Authentication Policy

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Allow Association Modes

☑ Select All (Personal)

☑ Open (no encryption)

☑ Open (Static WEP)

☑ Shared (WEP)

☑ WPA Personal TKIP

☑ WPA Personal AES

☑ WPA2 Personal TKIP

☑ WPA2 Personal AES

☑ Select All (Enterprise)

☑ Open (Dynamic (802.1X) WEP)

☑ WPA Enterprise TKIP

☑ WPA Enterprise AES

☑ WPA2 Enterprise TKIP

☑ WPA2 Enterprise AES

☑ CCKM Enterprise TKIP

☑ CCKM Enterprise AES

Allowed Authentication Modes

☑ Select All Outer

☑ EAP-FAST

☑ EAP-GTC

☑ EAP-MSCHAPv2

☑ EAP-TLS

☑ EAP-TLS

☑ EAP-TTLS

□ EAP-MD5 ☑ EAP-MSCHAPv2

☑ PAP (legacy) □ CHAP (legacy)

□ MSCHAP (legacy)

□ MSCHAPv2 (legacy)

☑ LEAP

☑ PEAP

☑ EAP-GTC

☑ EAP-MSCHAPv2

☑ EAP-TLS

Allowed Wired Security

☑ Select All

☑ Open (no encryption)

☑ 802.1x only

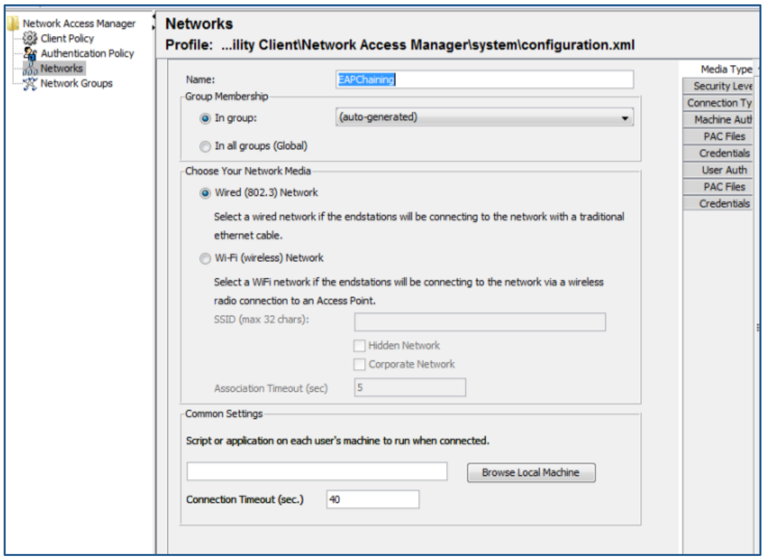
☑ 802.1x with MacSec

Figure 19. NAM Authentication Policy

Step 4 Define your network.

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

Step 5 Keep the defaults and **select Next.**



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name: EAPChaining

Group Membership

● In group: (auto-generated)

○ In all groups (Global)

Choose Your Network Media

● Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

○ Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

□ Hidden Network

□ Corporate Network

Association Timeout (sec) 5

Common Settings

Script or application on each user's machine to run when connected.

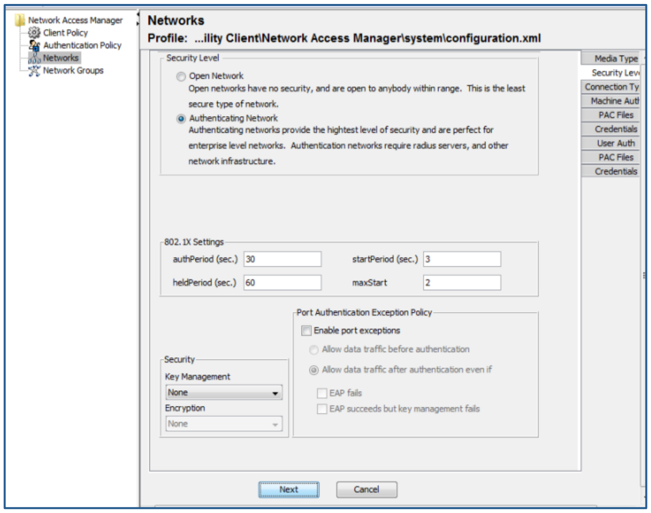
Connection Timeout (sec.) 40

Figure 20. Defining the Network

Step 6 Select Authenticating Network,

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



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Security Level

○ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

● Authenticating Network
Authenticating networks provide the hightest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) 30 startPeriod (sec.) 3

heldPeriod (sec.) 60 maxStart 2

Security

Key Management: None

Encryption: None

Port Authentication Exception Policy

□ Enable port exceptions

○ Allow data traffic before authentication

● Allow data traffic after authentication even if

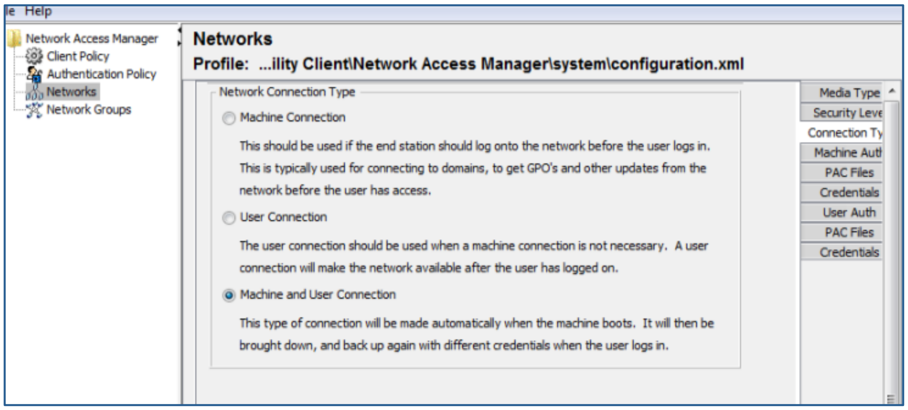
□ EAP fails

□ EAP succeeds but key management fails

Figure 21. Network Security Level

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

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



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

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

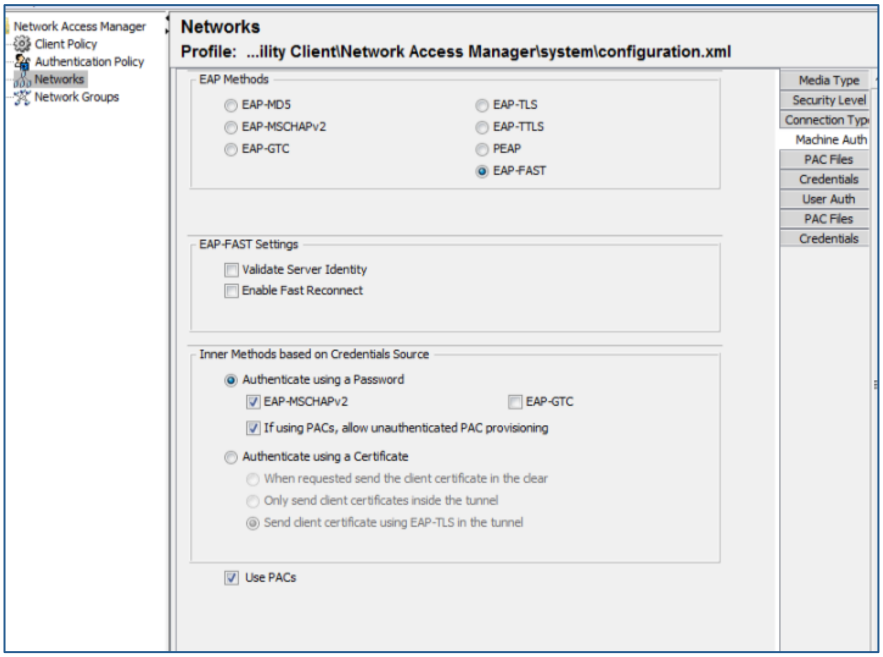
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Figure 22. Network Connection Type

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



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-MD5
○ EAP-MSCHAPv2
○ EAP-GTC
○ EAP-TLS
○ EAP-TTLS
○ PEAP
● EAP-FAST

EAP-FAST Settings

□ Validate Server Identity
□ Enable Fast Reconnect

Inner Methods based on Credentials Source

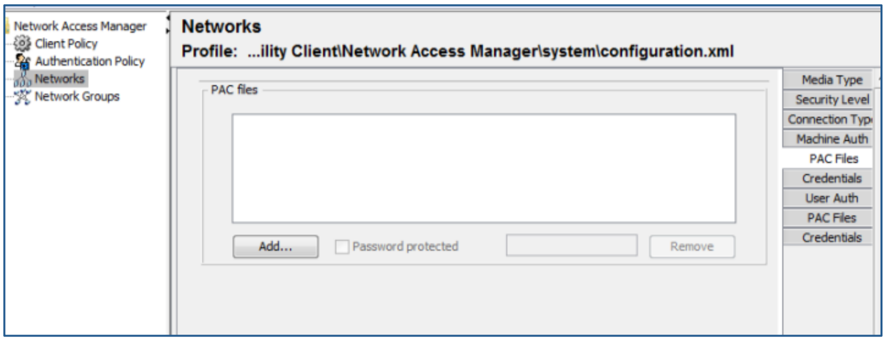
● Authenticate using a Password
☑ EAP-MSCHAPv2 □ EAP-GTC
☑ If using PACs, allow unauthenticated PAC provisioning
○ Authenticate using a Certificate
○ When requested send the client certificate in the clear
○ Only send client certificates inside the tunnel
● Send client certificate using EAP-TLS in the tunnel

☑ Use PACs

Figure 23. The Completed Configuration

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

Note: PAC files will be provisioned from ISE



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

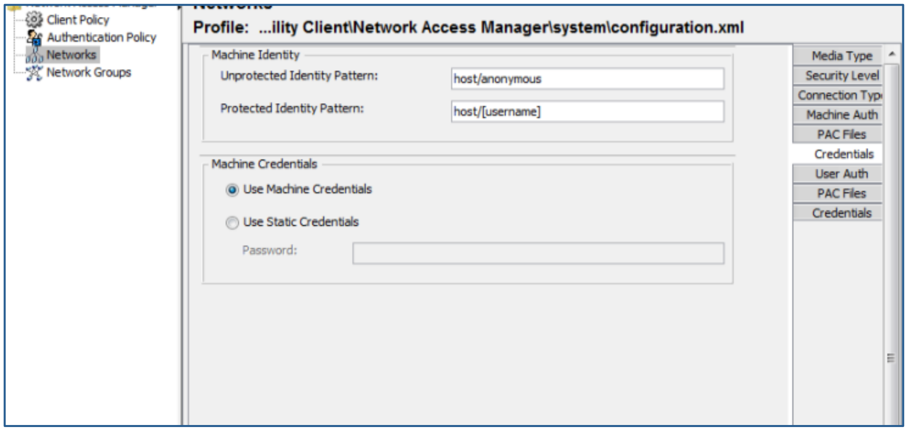
PAC files

□ Password protected

Figure 24. Leave PAC files as default (blank)

Step 19 Keep the defaults for Machine Identity.

Note: Machine identity specifies the machine credentials sent to the ISE server for validation



Profile: ...ility Client\Network Access Manager\system\configuration.xml

Machine Identity

Unprotected Identity Pattern: host/anonymous

Protected Identity Pattern: host/[username]

Machine Credentials

● Use Machine Credentials

○ Use Static Credentials

Password:

Figure 25. Machine Identity

Step 20 Click Next.

Step 21 Select EAP-FAST.

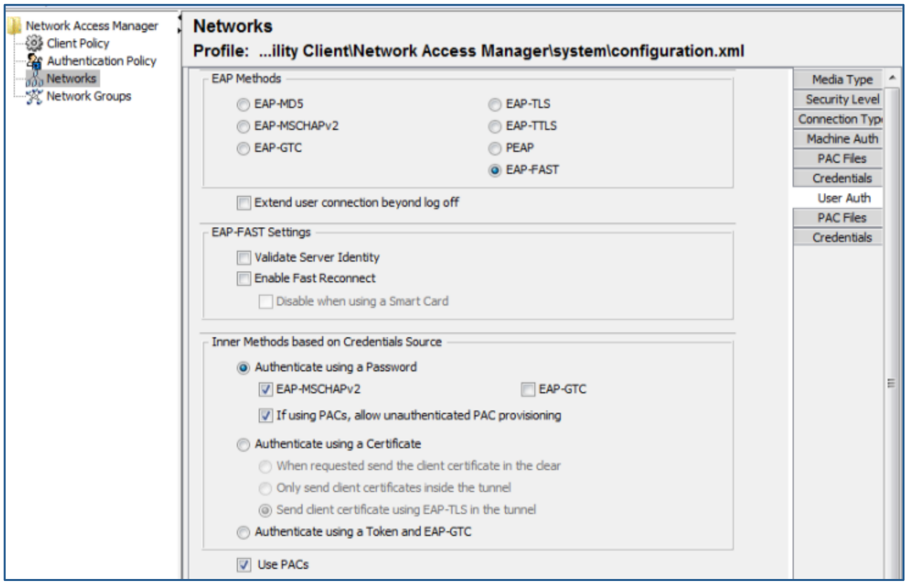
Step 22 Select ‘Authenticate using a Password’ in the ‘Inner Methods based on Credentials Source’ section.

Step 23 Select EAP-MSCHAPv2.

Step 24 Select ’If using PACs, allow unauthenticated PAC provisioning.’

Step 25 Select Use PACs.

Step 26 Click Next.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-MD5 ○ EAP-TLS
○ EAP-MSCHAPv2 ○ EAP-TTLS
○ EAP-GTC ○ PEAP
● EAP-FAST

□ Extend user connection beyond log off

EAP-FAST Settings

□ Validate Server Identity
□ Enable Fast Reconnect
□ Disable when using a Smart Card

Inner Methods based on Credentials Source

● Authenticate using a Password
☑ EAP-MSCHAPv2 □ EAP-GTC
☑ If using PACs, allow unauthenticated PAC provisioning
○ Authenticate using a Certificate
○ When requested send the client certificate in the clear
○ Only send client certificates inside the tunnel
● Send client certificate using EAP-TLS in the tunnel
○ Authenticate using a Token and EAP-GTC

☑ Use PACs

Figure 26. Completed Configuration

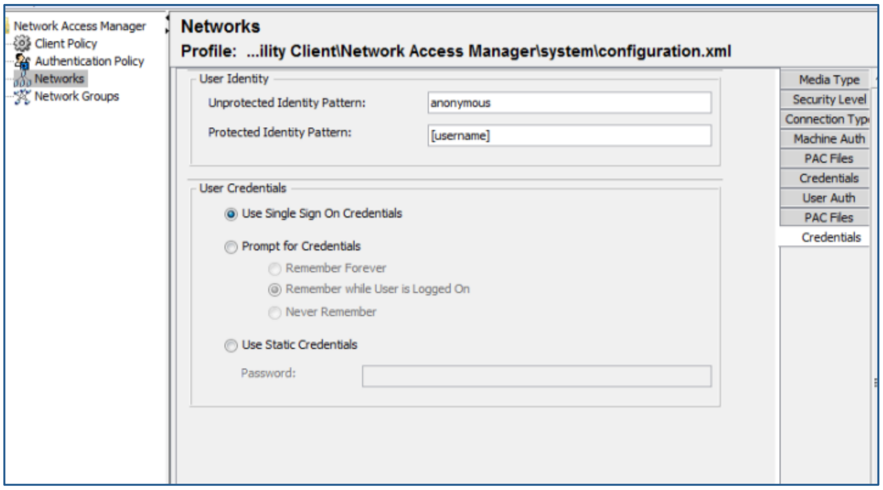
Step 27 Leave the PAC file as empty.

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.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]

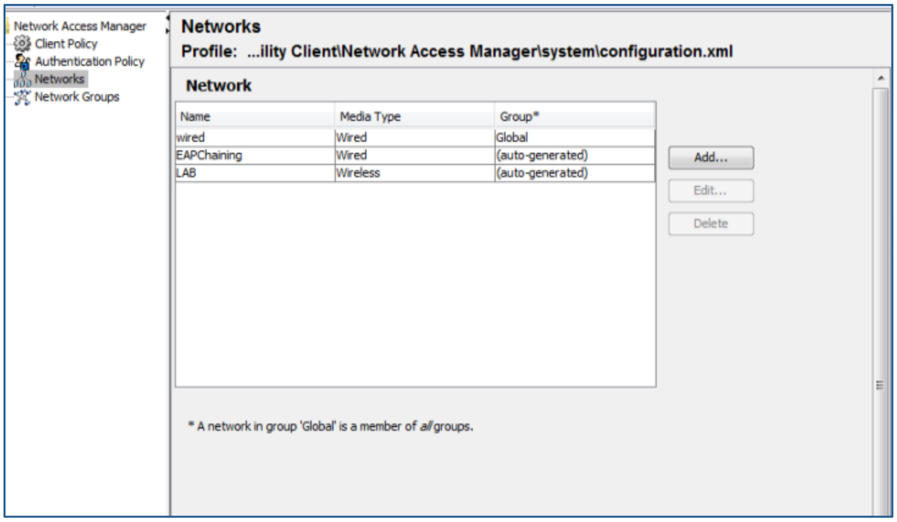
User Credentials

● Use Single Sign On Credentials
○ Prompt for Credentials
○ Remember Forever
● Remember while User is Logged On
○ Never Remember
○ Use Static Credentials

Password:

Figure 27. Completed User Authentication Configuration

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



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Network

Name	Media Type	Group*
wired	Wired	Global
EAPChaining	Wired	(auto-generated)
LAB	Wireless	(auto-generated)

* A network in group 'Global' is a member of *all* groups.

Figure 28. Networks List

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.

For Windows XP systems:

Save the ‘configuration.xml’ file to the following:

```
:\documents and settings\all users\application data\cisco\cisco anyconnect secure mobility
client\network access manager\newConfigFiles folder
```

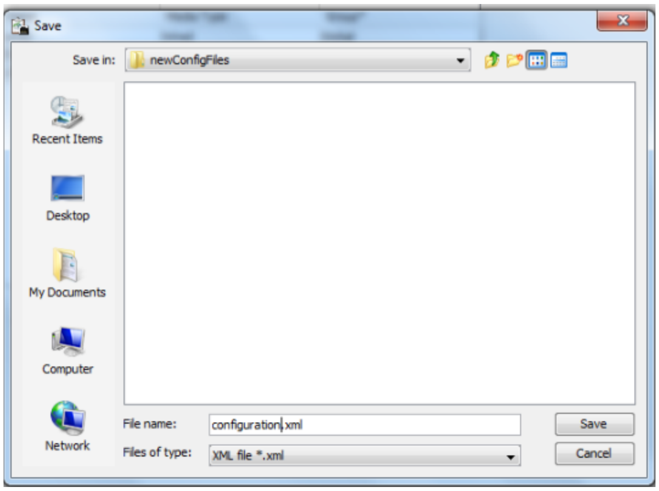
Note: If you cannot see the ‘application data’ folder, please enable ‘hidden files and folders’ from the ‘Tools’ dropdown in Control Panel.

For Windows 7 systems:

Save the ‘configuration.xml’ file to the following:

```
:\programdata\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigfiles
folder
```

Note :If you cannot see the ‘programdata’ folder, select ‘Organize’, ‘Folder and Search Options’, ‘Show hidden files, folders, and drives’, under ‘My Computers’)



Save

Save in: newConfigFiles

File name: configuration.xml

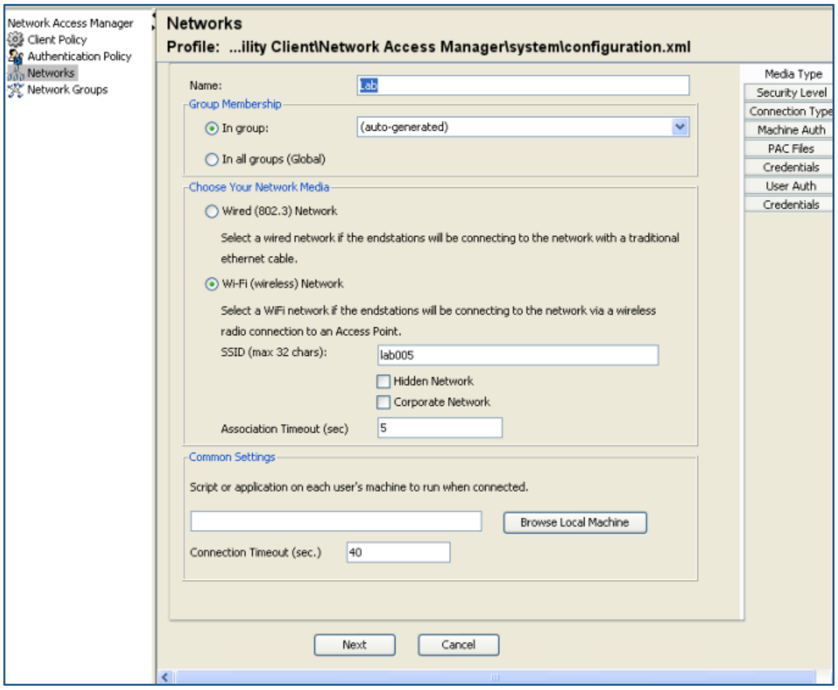
Files of type: XML file *.xml

Figure 29. Saving configuration.xml to the newConfigFiles directory

Step 35 {Right Click} on the AnyConnect GUI in the system tray
Step 36 Select 'Network Repair'

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.



Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name: Lab

Group Membership
- ● In group: (auto-generated)
- ○ In all groups (Global)

Choose Your Network Media
- ○ Wired (802.3) Network

  Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.
- ● Wi-Fi (wireless) Network

  Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

  SSID (max 32 chars): lab005

  □ Hidden Network
  □ Corporate Network

  Association Timeout (sec) 5

Common Settings

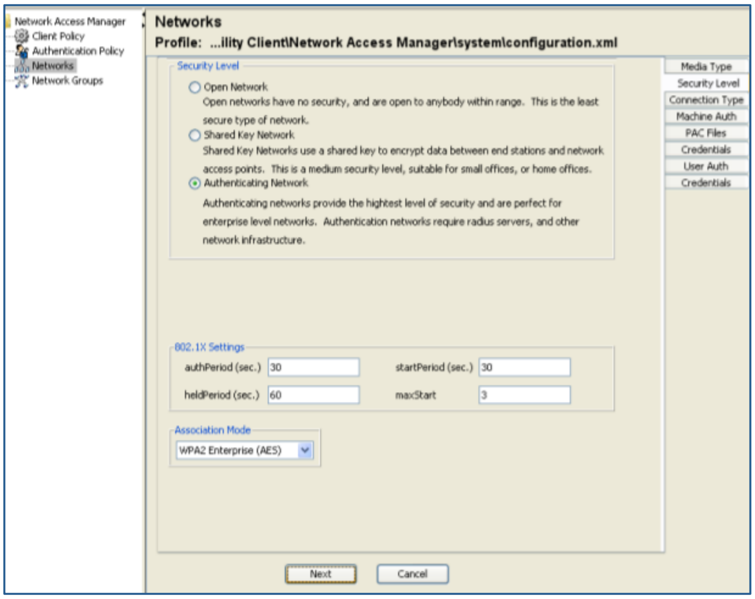
Script or application on each user's machine to run when connected.

Connection Timeout (sec.) 40

Figure 30. Defining the Wireless Network

Step 4 Select 'Authenticating Network.'
Step 5 Under Association Mode, choose the correct encryption level for your network.

Step 6 Click Next.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Security Level

○ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

○ Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This is a medium security level, suitable for small offices, or home offices.

● Authenticating Network
Authenticating networks provide the hightest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) 30
startPeriod (sec.) 30
heldPeriod (sec.) 60
maxStart 3

Association Mode

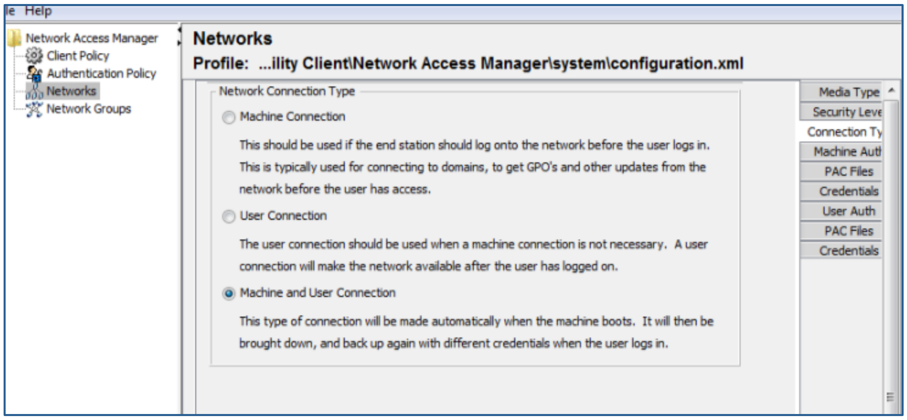
WPA2 Enterprise (AES)

Figure 31. Wireless Network Settings for Steps 4 and 5

Step 7 Select 'Machine and User Connection.'

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

Step 8 Click Next.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

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.

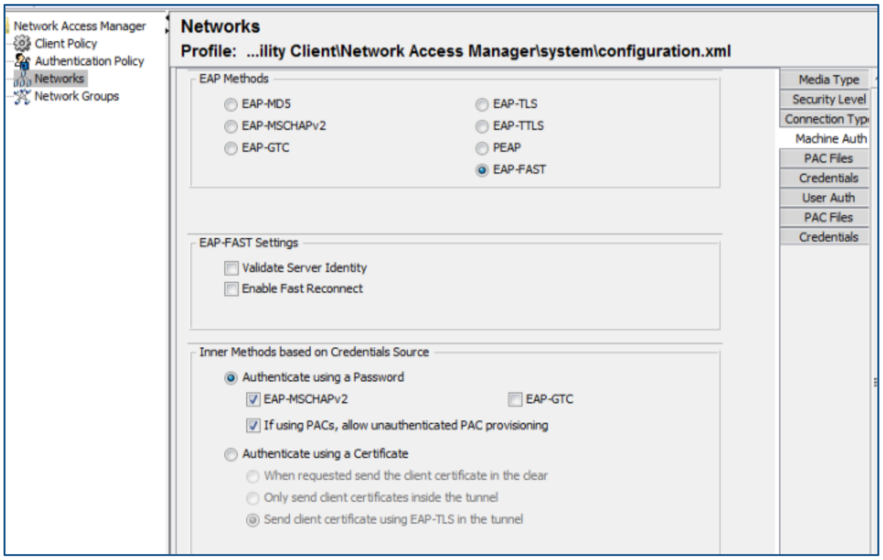
○ User Connection
The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.

● 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.

Figure 32. Network Connection Type is Machine and User

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

Step 9 Select EAP-FAST
Step 10 Select 'Authenticate using a Password' in the 'Inner Methods based on Credentials Source' section.
Step 11 Select EAP-MSCHAPv2
Step 12 Select 'If using PACs, allow unauthenticated PAC provisioning'
Step 13 Select Use PACs



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-MD5 ○ EAP-TLS
○ EAP-MSCHAPv2 ○ EAP-TTLS
○ EAP-GTC ○ PEAP
● EAP-FAST

EAP-FAST Settings

□ Validate Server Identity
□ Enable Fast Reconnect

Inner Methods based on Credentials Source

● Authenticate using a Password
☑ EAP-MSCHAPv2 □ EAP-GTC
☑ If using PACs, allow unauthenticated PAC provisioning

○ Authenticate using a Certificate
○ When requested send the client certificate in the clear
○ Only send client certificates inside the tunnel
● Send client certificate using EAP-TLS in the tunnel

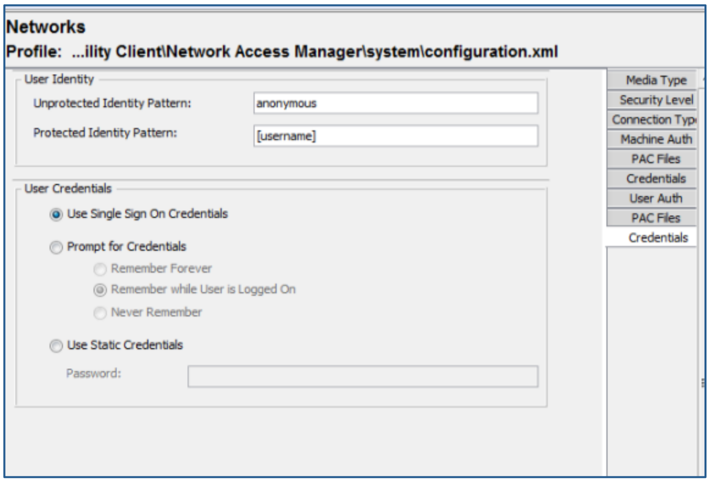
Figure 33. The Completed Configuration

Step 14 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 15 Keep the default value ‘Use Single Sign on Credentials’ for ‘User Credentials’

Step 16 Select Done



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]

User Credentials

● Use Single Sign On Credentials

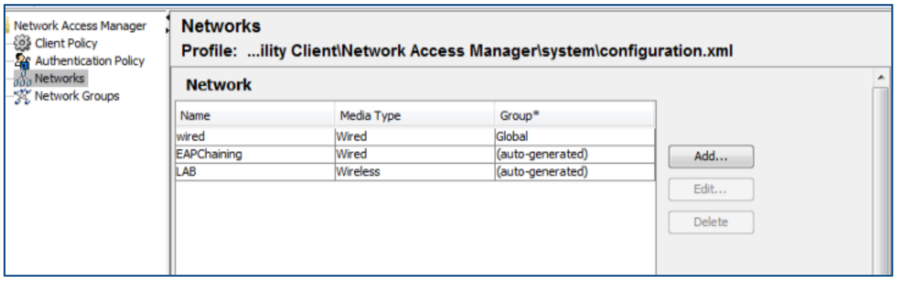
○ Prompt for Credentials
○ Remember Forever
● Remember while User is Logged On
○ Never Remember

○ Use Static Credentials

Password:

Figure 34. Completed Wireless User Authentication

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



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Network

Name	Media Type	Group*
wired	Wired	Global
EAPChaining	Wired	(auto-generated)
LAB	Wireless	(auto-generated)

Figure 35. List of Networks

Step 17 From the drop-down File menu, select ‘Save-As’
Step 18 Name the file ‘configuration.xml’ (this MUST be the file name)
Step 19 Save the file into the .. \newConfigFiles folder as illustrated

For Windows XP systems:

Save the ‘configuration.xml’ file to the following:

```
:\documents and settings\all users\application data\cisco\cisco anyconnect secure mobility
client\network access manager\newConfigFiles folder
```

Note: If you cannot see the ‘application data’ folder, please enable ‘hidden files and folders’ from the ‘Tools’ dropdown in Control Panel.

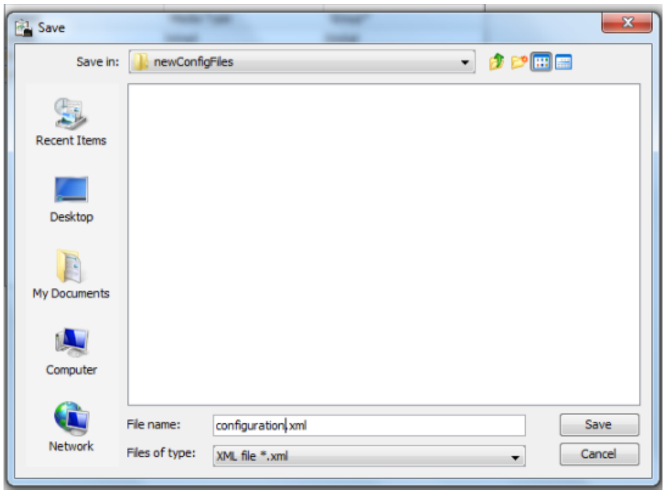
For Windows 7 systems:

Save the ‘configuration.xml’ file to the following:

```
:\programdata\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigfiles
folder
```

Note :If you cannot see the ‘programdata’ folder, select ‘Organize’, ‘Folder and Search Options’, ‘Show hidden files, folders, and drives’, under ‘My Computers’)

Figure 2 Saving the configuration.xml to the newConfigFiles directory



Save in: newConfigFiles

File name: configuration.xml

Files of type: XML file *.xml

Figure 36. Saving the configuration.xml to the newConfigFiles directory

Step 20 Click on the AnyConnect GUI in the system tray

Step 21 Select ‘Network Repair’

Testing Procedure

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.

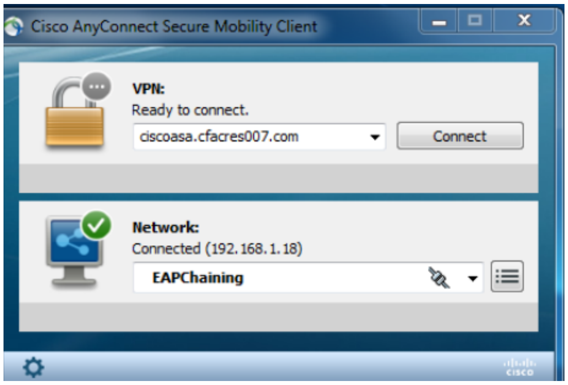
End-User logs into a non-corporate device with their personal laptop, machine domain credentials are not available and fail validation, however, their user credentials have been successfully validated placed in VLAN 22 and receive restricted network access.

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.

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.

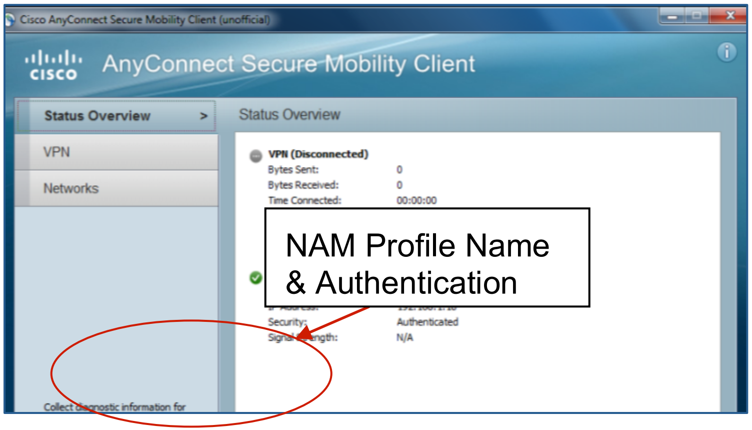


Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.
ciscoasa.cfacres007.com

Network:
Connected (192.168.1.18)
EAPChaining

Figure 37. AnyConnect User Interface

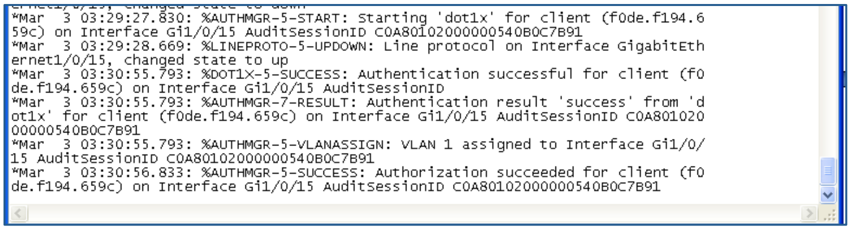

Cisco AnyConnect Secure Mobility Client (unofficial)
AnyConnect Secure Mobility Client
Status Overview >
VPN
Networks
Status Overview

VPN (Disconnected)
Bytes Sent: 0
Bytes Received: 0
Time Connected: 00:00:00
Security: Authenticated
Signal Strength: N/A

Collect diagnostic information for

NAM Profile Name & Authentication

Figure 38. NAM Status



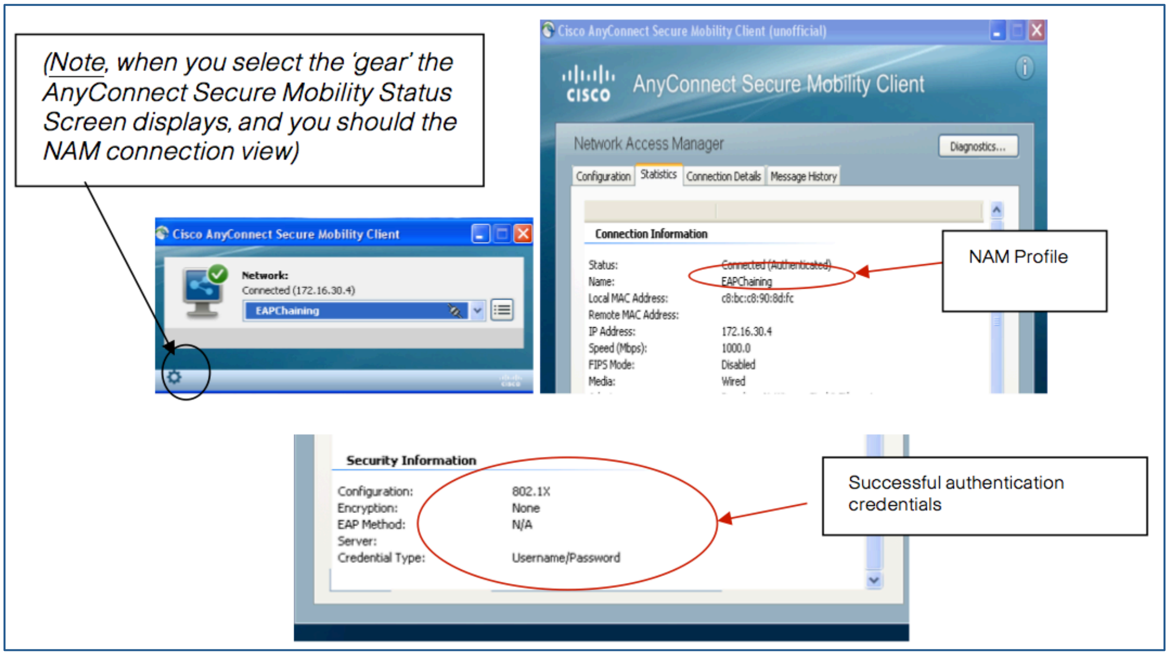
```
ernet1/0/15, changed state to down
*Mar  3 03:29:27.830: %AUTHMGR-5-START: Starting 'dot1x' for client (f0de.f194.6
59c) on Interface Gi1/0/15 AuditSessionID C0A8010200000540B0C7B91
*Mar  3 03:29:28.669: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/15, changed state to up
*Mar  3 03:30:55.793: %DOT1X-5-SUCCESS: Authentication successful for client (f0
de.f194.659c) on Interface Gi1/0/15 AuditSessionID
*Mar  3 03:30:55.793: %AUTHMGR-7-RESULT: Authentication result 'success' from 'd
ot1x' for client (f0de.f194.659c) on Interface Gi1/0/15 AuditSessionID C0A801020
00000540B0C7B91
*Mar  3 03:30:55.793: %AUTHMGR-5-VLANASSIGN: VLAN 1 assigned to Interface Gi1/0/
15 AuditSessionID C0A8010200000540B0C7B91
*Mar  3 03:30:56.833: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f0
de.f194.659c) on Interface Gi1/0/15 AuditSessionID C0A8010200000540B0C7B91
```

Figure 39. 802.1X log information from the switch

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.



(Note, when you select the 'gear' the AnyConnect Secure Mobility Status Screen displays, and you should the NAM connection view)

Connection Information

Status: Connected (Authenticated)
Name: EAPChaining
Local MAC Address: c8:bc:c8:90:8d:fc
Remote MAC Address:
IP Address: 172.16.30.4
Speed (Mbps): 1000.0
FIPS Mode: Disabled
Media: Wired

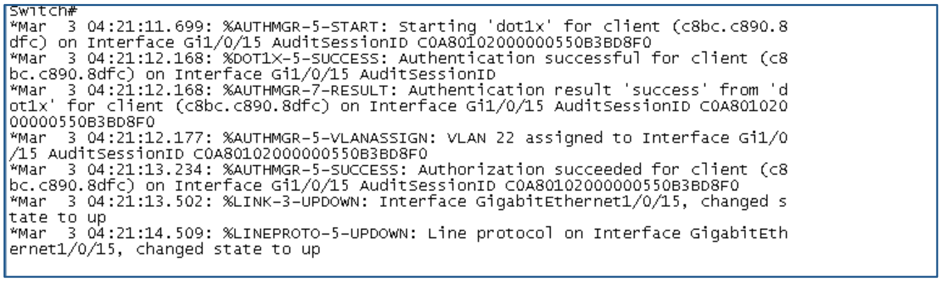
NAM Profile

Security Information

Configuration: 802.1X
Encryption: None
EAP Method: N/A
Server:
Credential Type: Username/Password

Successful authentication credentials

Figure 40. Figure 3 Successful Authentication



```
Switch#
*Mar  3 04:21:11.699: %AUTHMGR-5-START: Starting 'dot1x' for client (c8bc.c890.8
dfc) on Interface Gi1/0/15 AuditSessionID C0A80102000000550B3BD8F0
*Mar  3 04:21:12.168: %DOT1X-5-SUCCESS: Authentication successful for client (c8
bc.c890.8dfc) on Interface Gi1/0/15 AuditSessionID
*Mar  3 04:21:12.168: %AUTHMGR-7-RESULT: Authentication result 'success' from 'd
ot1x' for client (c8bc.c890.8dfc) on Interface Gi1/0/15 AuditSessionID C0A801020
00000550B3BD8F0
*Mar  3 04:21:12.177: %AUTHMGR-5-VLANASSIGN: VLAN 22 assigned to Interface Gi1/0
/15 AuditSessionID C0A80102000000550B3BD8F0
*Mar  3 04:21:13.234: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (c8
bc.c890.8dfc) on Interface Gi1/0/15 AuditSessionID C0A80102000000550B3BD8F0
*Mar  3 04:21:13.502: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/15, changed s
tate to up
*Mar  3 04:21:14.509: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/15, changed state to up
```

Figure 41. 802.1X log information from the switch

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

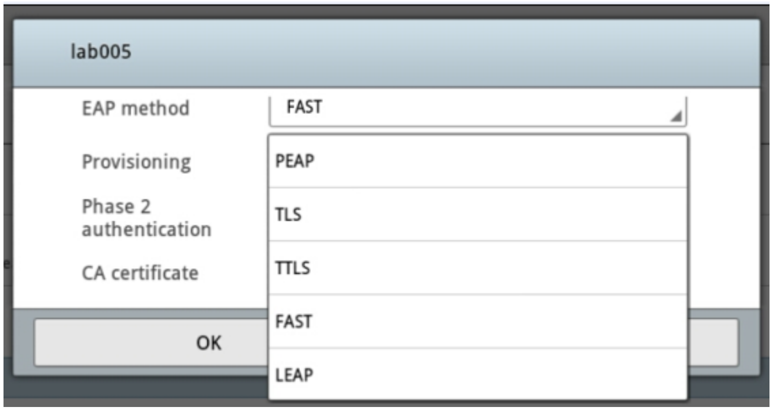
The Samsung Android Tablet settings are as follows:

```
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:



lab005

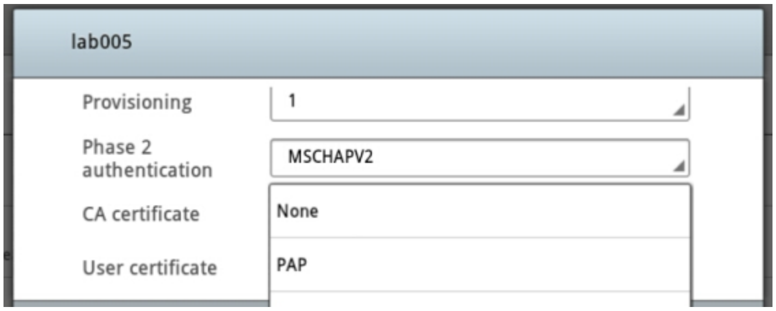
EAP method FAST

Provisioning

Phase 2 authentication

CA certificate

Figure 42. EAP-FAST selection



lab005

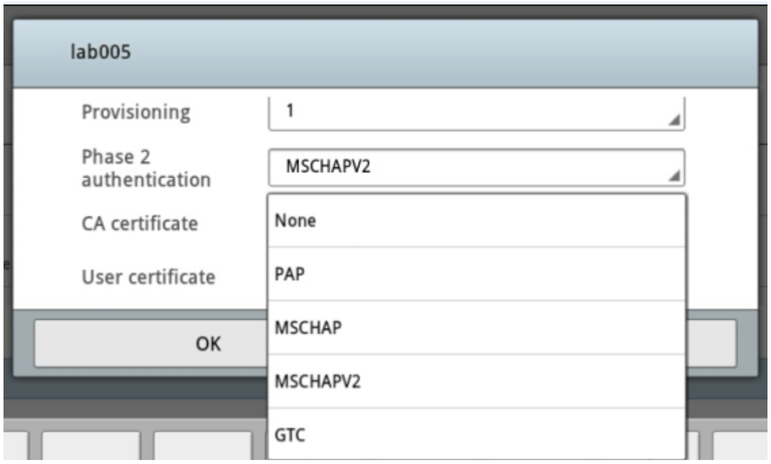
Provisioning 1

Phase 2 authentication MSCHAPV2

CA certificate

User certificate

Figure 43. Provisioning set to "1"



lab005

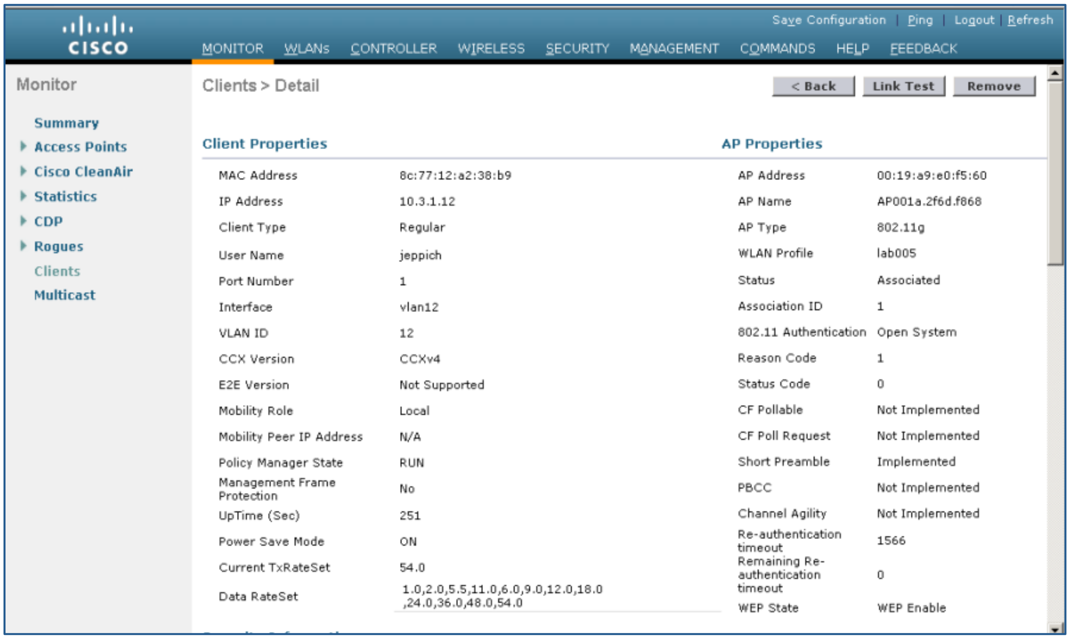
Provisioning 1

Phase 2 authentication MSCHAPV2

CA certificate

User certificate

Figure 44. Phase-2 Authentication = MSCHAPv2



Clients > Detail

Client Properties

MAC Address	8c:77:12:a2:38:b9
IP Address	10.3.1.12
Client Type	Regular
User Name	jeppich
Port Number	1
Interface	vlan12
VLAN ID	12
CCX Version	CCXv4
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	251
Power Save Mode	ON
Current TxRateSet	54.0
Data RateSet	1.0,2.0,5.5,11.0,6.0,9.0,12.0,18.0 ,24.0,36.0,48.0,54.0

AP Properties

AP Address	00:19:a9:e0:f5:60
AP Name	AP001a.2f6d.f868
AP Type	802.11g
WLAN Profile	lab005
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	1566
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Figure 45. Cisco Wireless LAN Controller - showing successful authentication

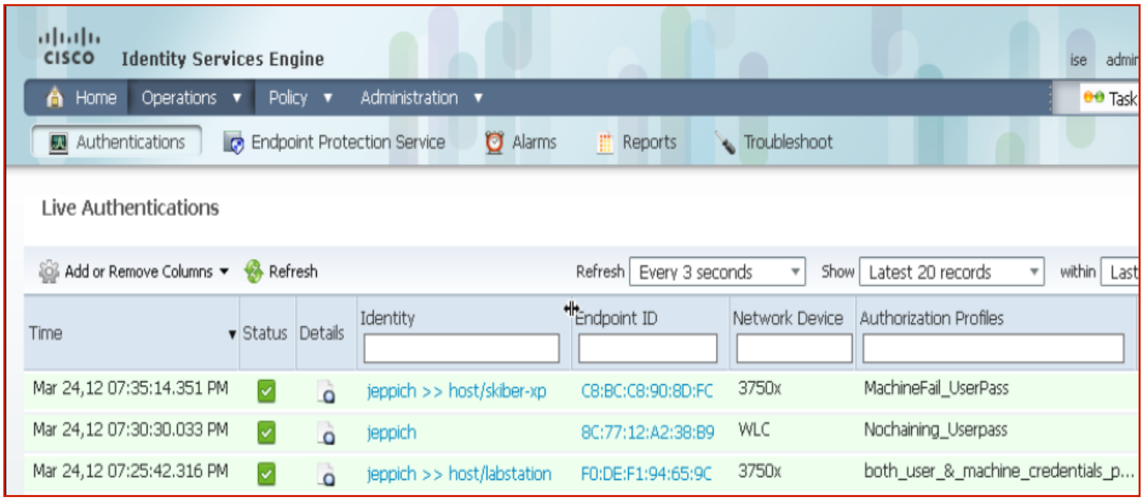
Detailed View of EAP Chaining

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.

Access the Live Authentications menu

Step 1 Select Operations → Authentications



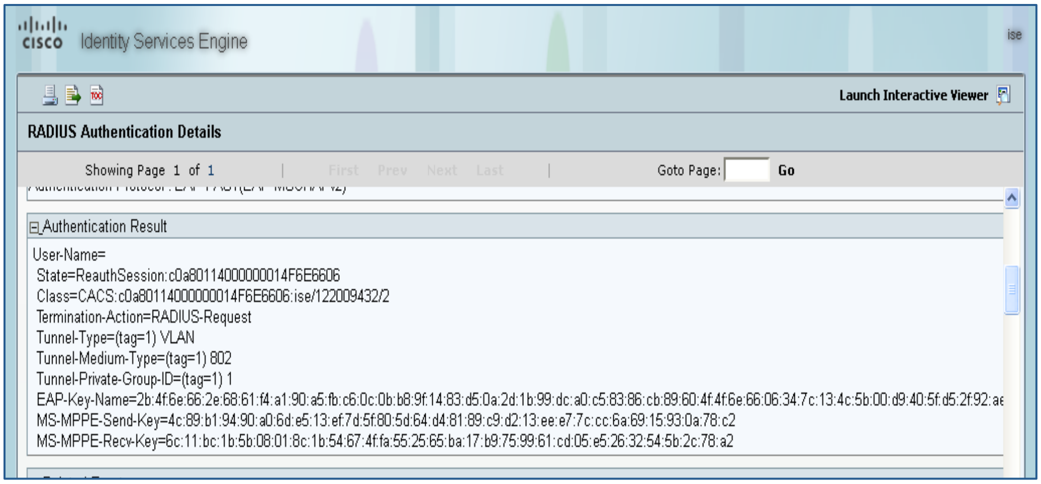
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles
Mar 24,12 07:35:14.351 PM	✓		jeppich >> host/skiber-xp	C8:BC:C8:90:8D:FC	3750x	MachineFail_UserPass
Mar 24,12 07:30:30.033 PM	✓		jeppich	8C:77:12:A2:38:B9	WLC	Nochaining_Userpass
Mar 24,12 07:25:42.316 PM	✓		jeppich >> host/labstation	F0:DE:F1:94:65:9C	3750x	both_user_&_machine_credentials_p...

Figure 46. Live Authentications Log

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.



RADIUS Authentication Details

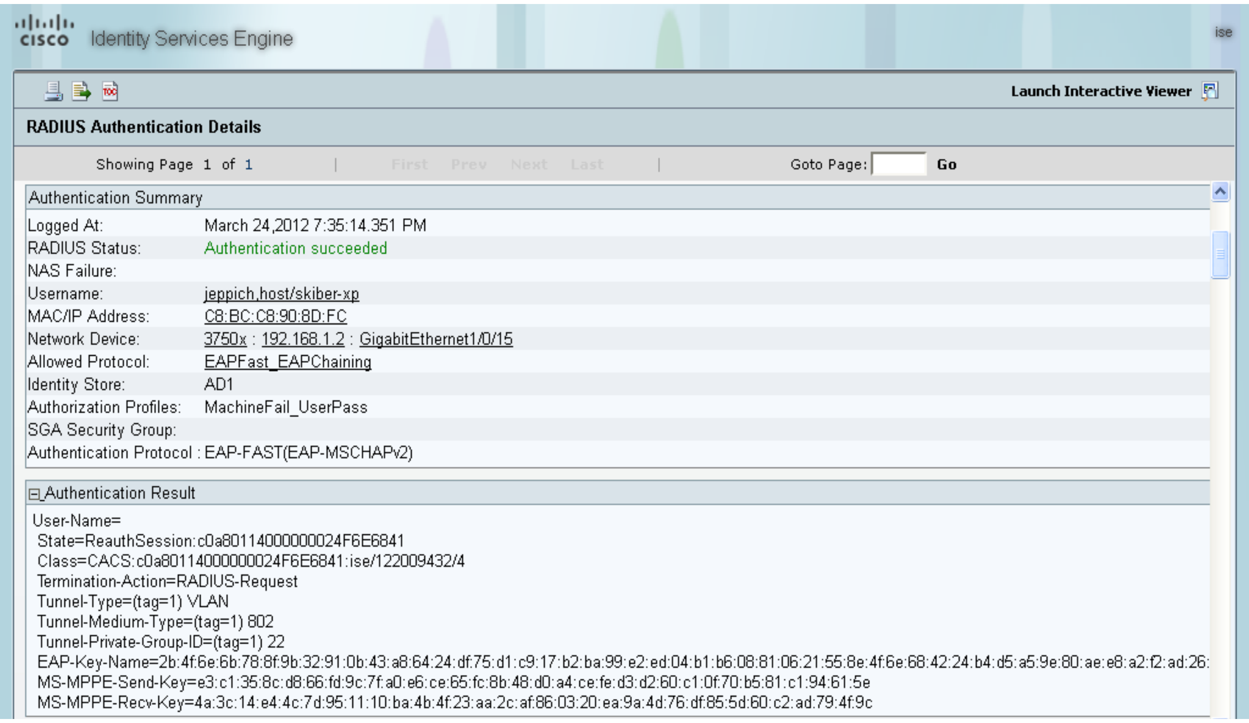
Authentication Result

```
User-Name=
 State=ReauthSession:c0a80114000000014F6E6606
 Class=CACS:c0a80114000000014F6E6606:ise/122009432/2
 Termination-Action=RADIUS-Request
 Tunnel-Type=(tag=1) VLAN
 Tunnel-Medium-Type=(tag=1) 802
 Tunnel-Private-Group-ID=(tag=1) 1
 EAP-Key-Name=2b:4f:6e:66:2e:68:61: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:ae
 MS-MPPE-Send-Key=4c:89:b1:94:90: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
 MS-MPPE-Recv-Key=6c:11:bc:1b: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
```

Figure 47. End-User placed in VLAN 1

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.

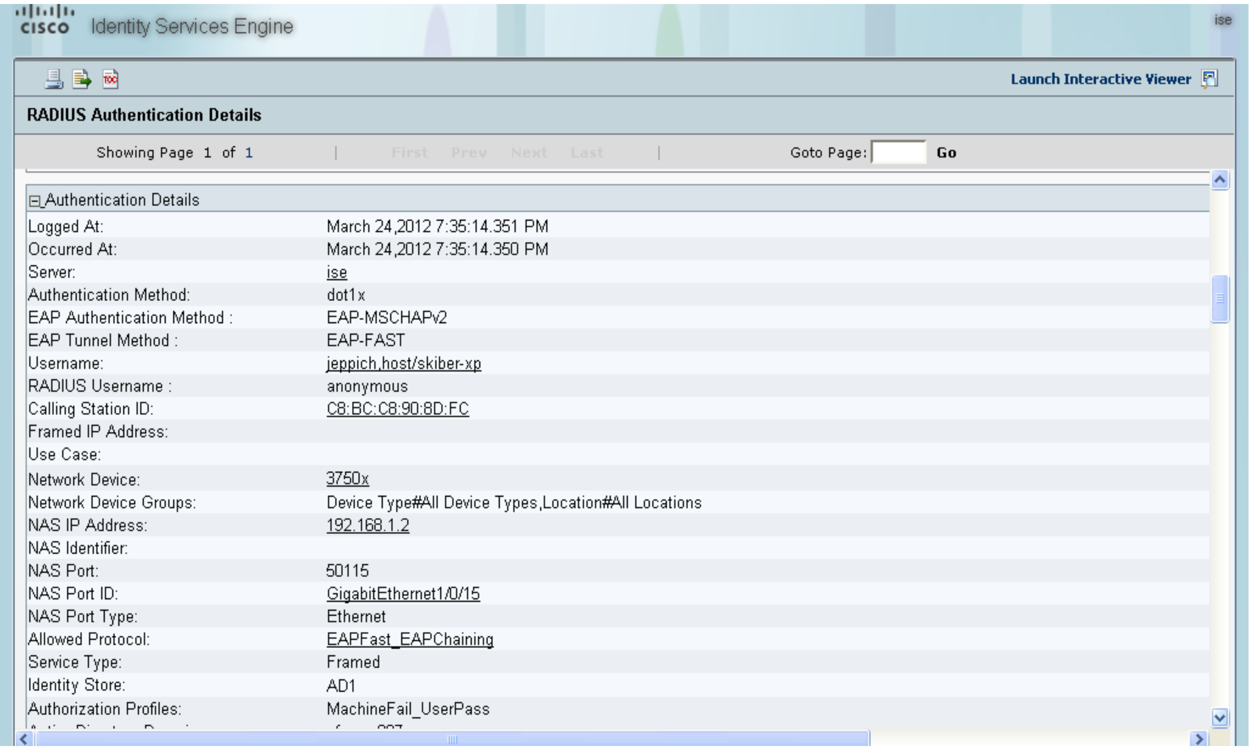


Authentication Summary

Logged At:	March 24,2012 7:35:14.351 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	jeppich,host/skiber-xp
MAC/IP Address:	C8:BC:C8:90:8D:FC
Network Device:	3750x : 192.168.1.2 : GigabitEthernet1/0/15
Allowed Protocol:	EAPFast_EAPChaining
Identity Store:	AD1
Authorization Profiles:	MachineFail_UserPass
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

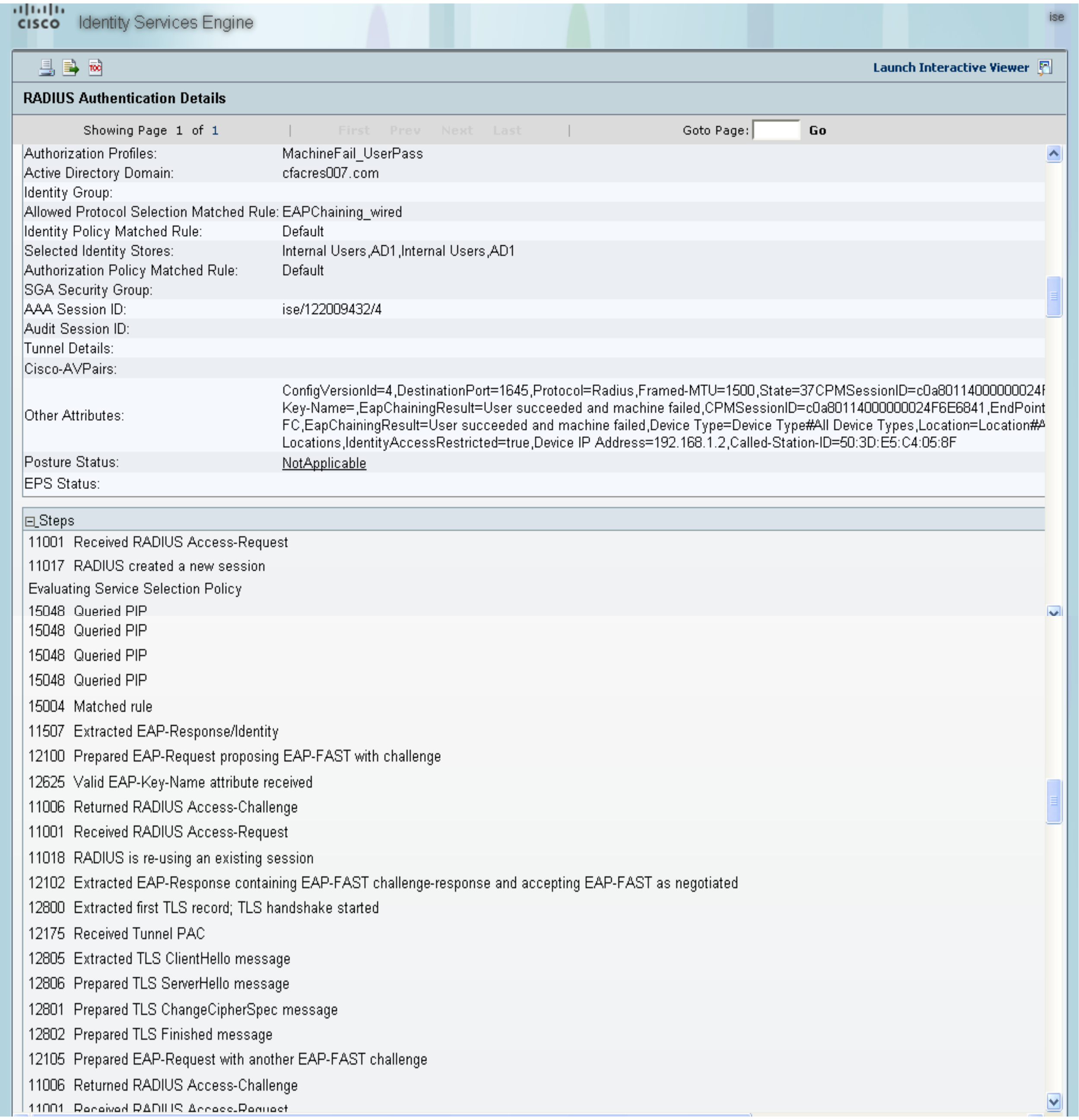
⊟ Authentication Result

```
User-Name=
 State=ReauthSession:c0a80114000000024F6E6841
 Class=CACS:c0a80114000000024F6E6841:ise/122009432/4
 Termination-Action=RADIUS-Request
 Tunnel-Type=(tag=1) VLAN
 Tunnel-Medium-Type=(tag=1) 802
 Tunnel-Private-Group-ID=(tag=1) 22
 EAP-Key-Name=2b:4f:6e:6b:78:8f:9b:32:91:0b:43:a8:64:24:df:75:d1:c9:17:b2:ba:99:e2:ed:04:b1:b6:08:81:06:21:55:8e:4f:6e:68:42:24:b4:d5:a5:9e:80:ae:e8:a2:f2:ad:26:
 MS-MPPE-Send-Key=e3:c1:35:8c:d8:66:fd:9c:7f:a0:e6:ce:65:fc:8b:48:d0:a4:ce:fe:d3:d2:60:c1:0f:70:b5:81:c1:94:61:5e
 MS-MPPE-Recv-Key=4a:3c:14:e4:4c:7d:95:11:10:ba:4b:4f:23:aa:2c:af:86:03:20:ea:9a:4d:76:df:85:5d:60:c2:ad:79:4f:9c
```



⊟ 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
Username:	jeppich,host/skiber-xp
RADIUS Username :	anonymous
Calling Station ID:	C8:BC:C8:90:8D:FC
Framed IP Address:	
Use Case:	
Network Device:	3750x
Network Device Groups:	Device Type#All Device Types,Location#All Locations
NAS IP Address:	192.168.1.2
NAS Identifier:	
NAS Port:	50115
NAS Port ID:	GigabitEthernet1/0/15
NAS Port Type:	Ethernet
Allowed Protocol:	EAPFast_EAPChaining
Service Type:	Framed
Identity Store:	AD1
Authorization Profiles:	MachineFail_UserPass



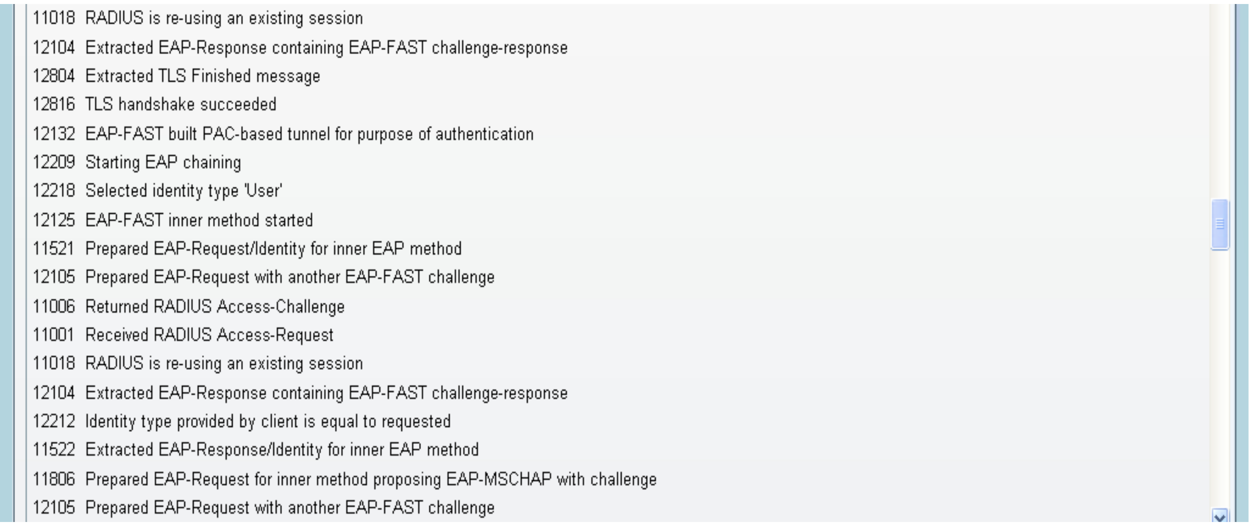
RADIUS Authentication Details

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

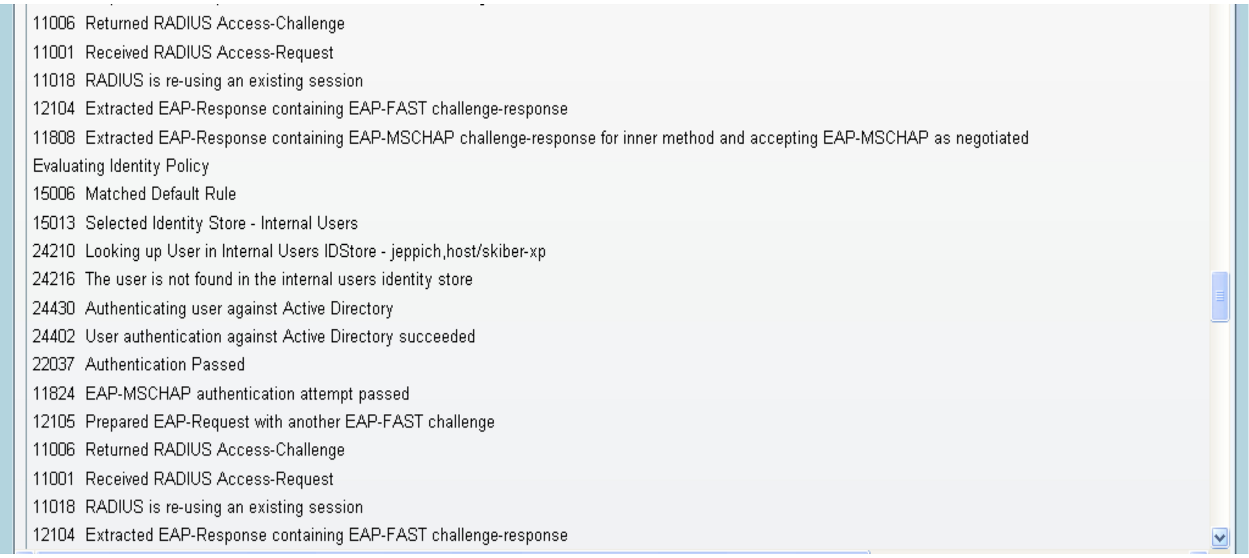
Authorization Profiles:	MachineFail_UserPass
Active Directory Domain:	cfacres007.com
Identity Group:	
Allowed Protocol Selection Matched Rule:	EAPChaining_wired
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users,AD1,Internal Users,AD1
Authorization Policy Matched Rule:	Default
SGA Security Group:	
AAA Session ID:	ise/122009432/4
Audit Session ID:	
Tunnel Details:	
Cisco-AVPairs:	
Other Attributes:	ConfigVersionId=4,DestinationPort=1645,Protocol=Radius,Framed-MTU=1500,State=37CPMSessionID=c0a80114000000024F Key-Name=,EapChainingResult=User succeeded and machine failed,CPMSessionID=c0a80114000000024F6E6841,EndPoint FC,EapChainingResult=User succeeded and machine failed,Device Type=Device Type#All Device Types,Location=Location#A Locations,IdentityAccessRestricted=true,Device IP Address=192.168.1.2,Called-Station-ID=50:3D:E5:C4:05:8F
Posture Status:	NotApplicable
EPS Status:	

⊟ Steps

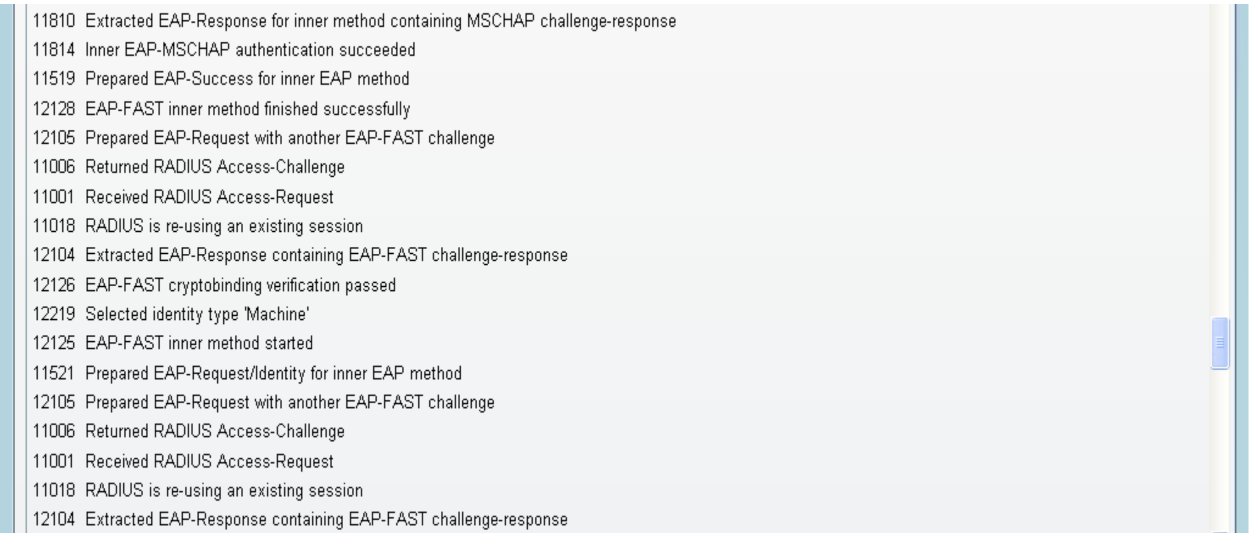
```
11001  Received RADIUS Access-Request
11017  RADIUS created a new session
Evaluating Service Selection Policy
15048  Queried PIP
15048  Queried PIP
15048  Queried PIP
15048  Queried PIP
15004  Matched rule
11507  Extracted EAP-Response/Identity
12100  Prepared EAP-Request proposing EAP-FAST with challenge
12625  Valid EAP-Key-Name attribute received
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12175  Received Tunnel PAC
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message
12802  Prepared TLS Finished message
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
```



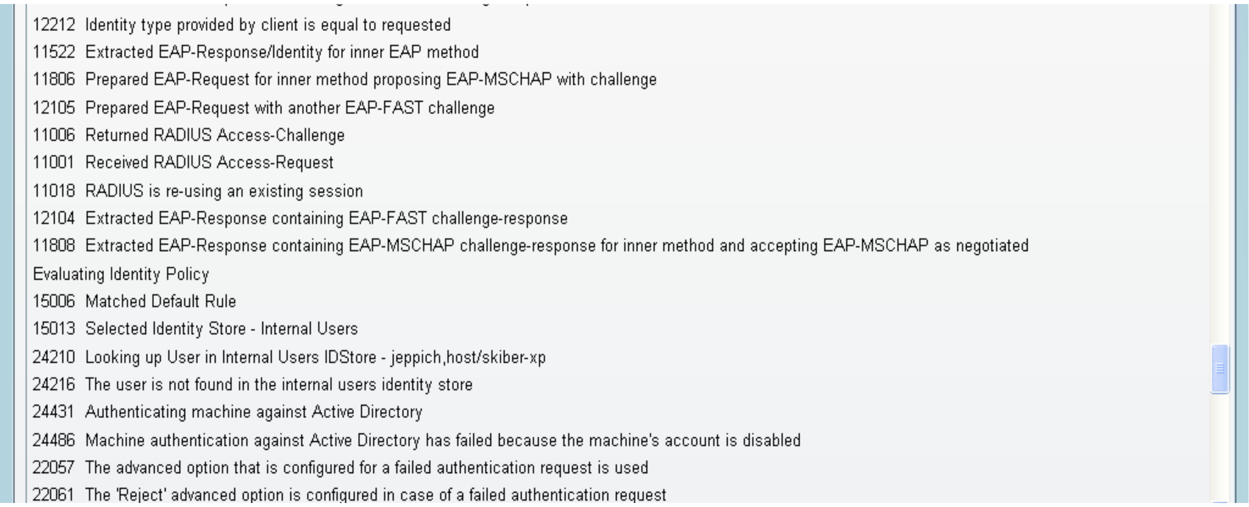
```
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
12804  Extracted TLS Finished message
12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
12209  Starting EAP chaining
12218  Selected 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
11018  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
```



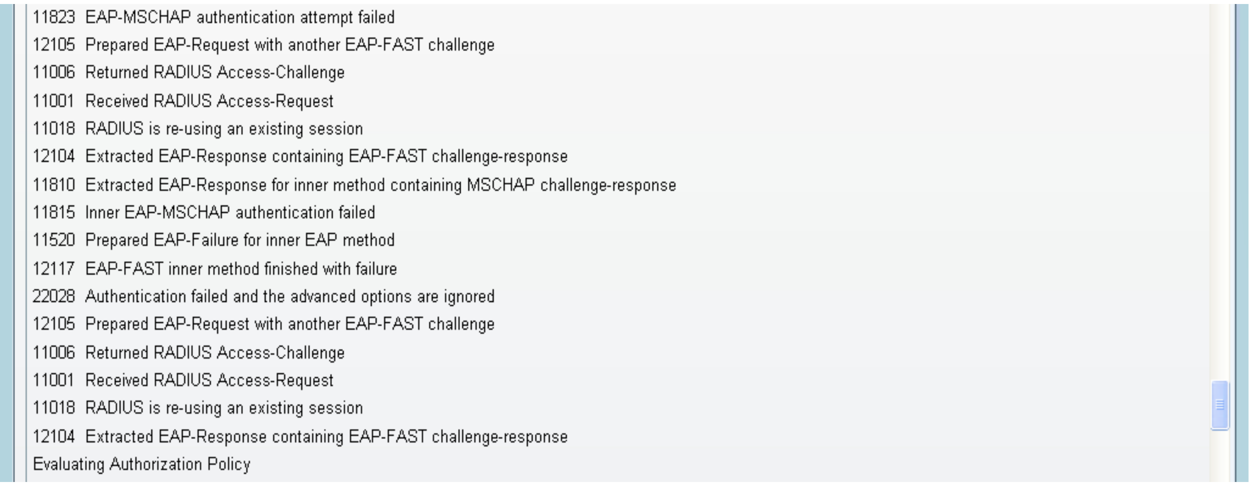
```
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
11808  Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP 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
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
```



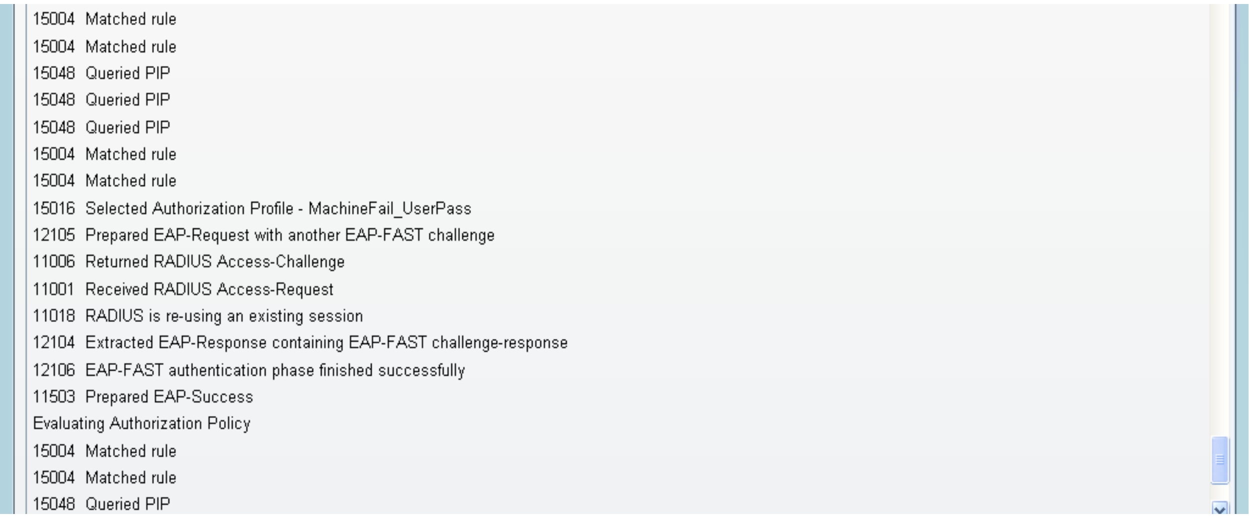
```
11810  Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814  Inner EAP-MSCHAP authentication succeeded
11519  Prepared EAP-Success for inner EAP method
12128  EAP-FAST inner method finished successfully
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
12126  EAP-FAST cryptobinding verification passed
12219  Selected identity type 'Machine'
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
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
```



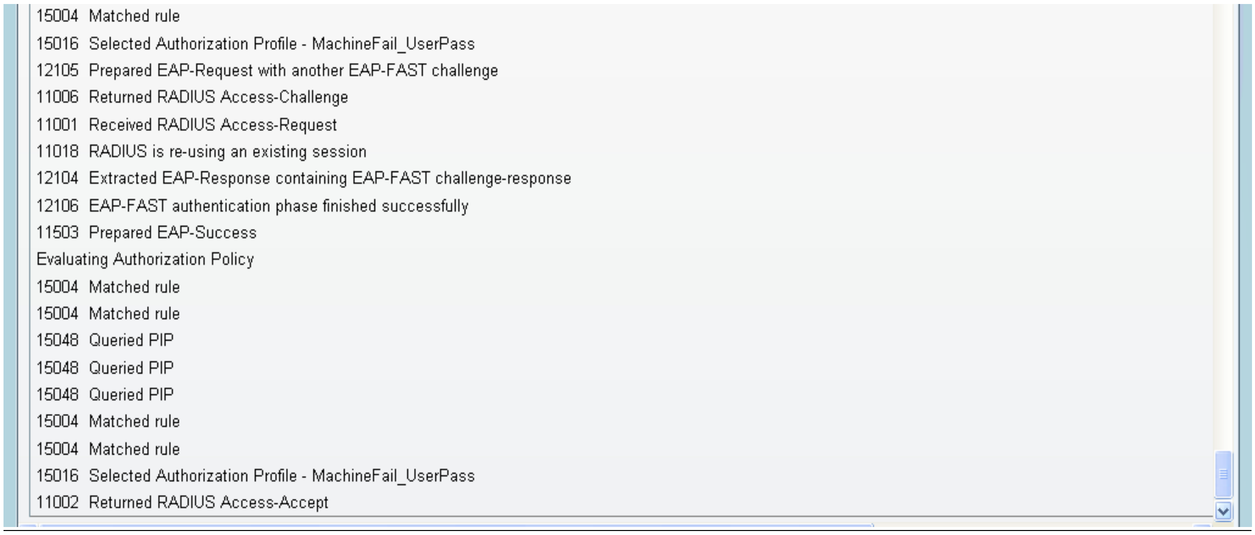
```
12212  Identity type provided by client is equal to requested
11522  Extracted EAP-Response/Identity for inner EAP method
11806  Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
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 disabled
22057  The advanced option that is configured for a failed authentication request is used
22061  The 'Reject' advanced option is configured in case of a failed authentication request
```



```
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
```



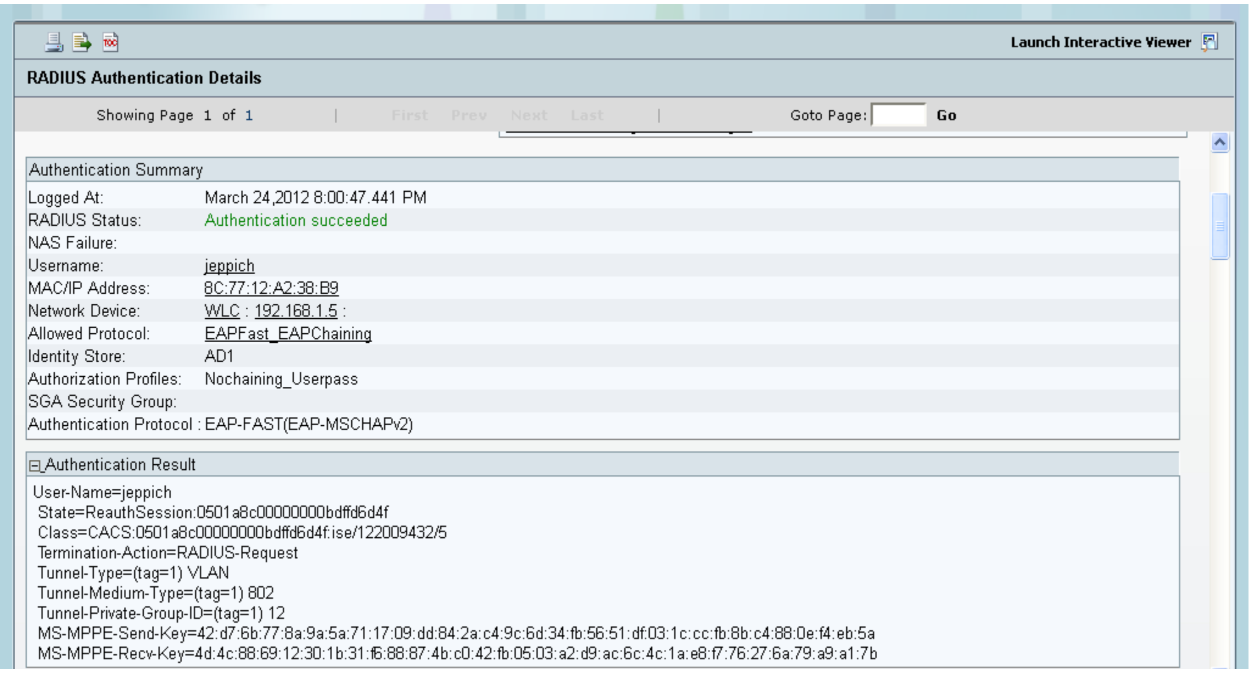
```
15004  Matched rule
15004  Matched rule
15048  Queried PIP
15048  Queried PIP
15048  Queried PIP
15004  Matched rule
15004  Matched rule
15016  Selected Authorization Profile - MachineFail_UserPass
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
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
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
11002  Returned RADIUS Access-Accept
```

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.



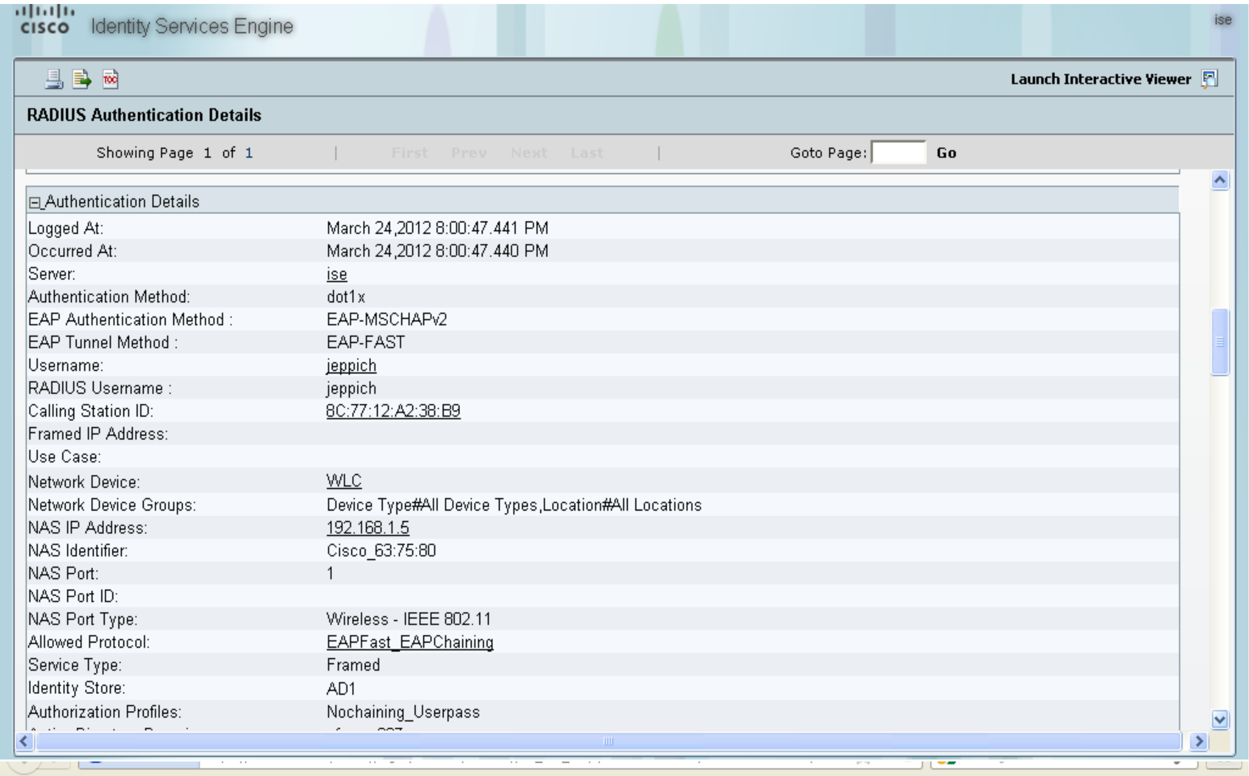
RADIUS Authentication Details

Authentication Summary

Logged At:	March 24,2012 8:00:47.441 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	jeppich
MAC/IP Address:	8C:77:12:A2:38:B9
Network Device:	WLC : 192.168.1.5 :
Allowed Protocol:	EAPFast_EAPChaining
Identity Store:	AD1
Authorization Profiles:	Nochaining_Userpass
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

⊟ Authentication Result

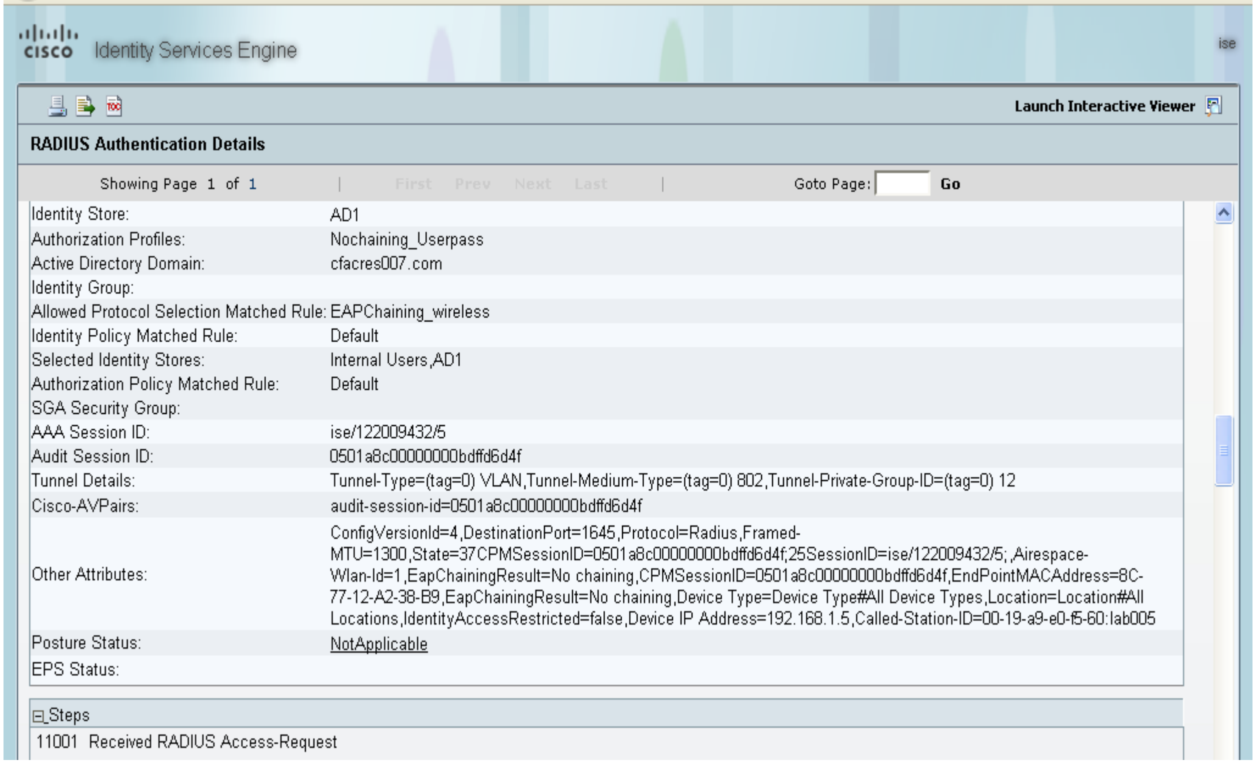
```
User-Name=jeppich
 State=ReauthSession:0501a8c00000000bdffd6d4f
 Class=CACS:0501a8c00000000bdffd6d4f:ise/122009432/5
 Termination-Action=RADIUS-Request
 Tunnel-Type=(tag=1) VLAN
 Tunnel-Medium-Type=(tag=1) 802
 Tunnel-Private-Group-ID=(tag=1) 12
 MS-MPPE-Send-Key=42:d7:6b:77:8a:9a:5a:71:17:09:dd:84:2a:c4:9c:6d:34:fb:56:51:df:03:1c:cc:fb:8b:c4:88:0e:f4:eb:5a
 MS-MPPE-Recv-Key=4d:4c:88:69:12:30:1b:31:f6:88:87:4b:c0:42:fb:05:03:a2:d9:ac:6c:4c:1a:e8:f7:76:27:6a:79:a9:a1:7b
```



RADIUS Authentication Details

⊟ Authentication Details

Logged At:	March 24,2012 8:00:47.441 PM
Occurred At:	March 24,2012 8:00:47.440 PM
Server:	ise
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
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 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

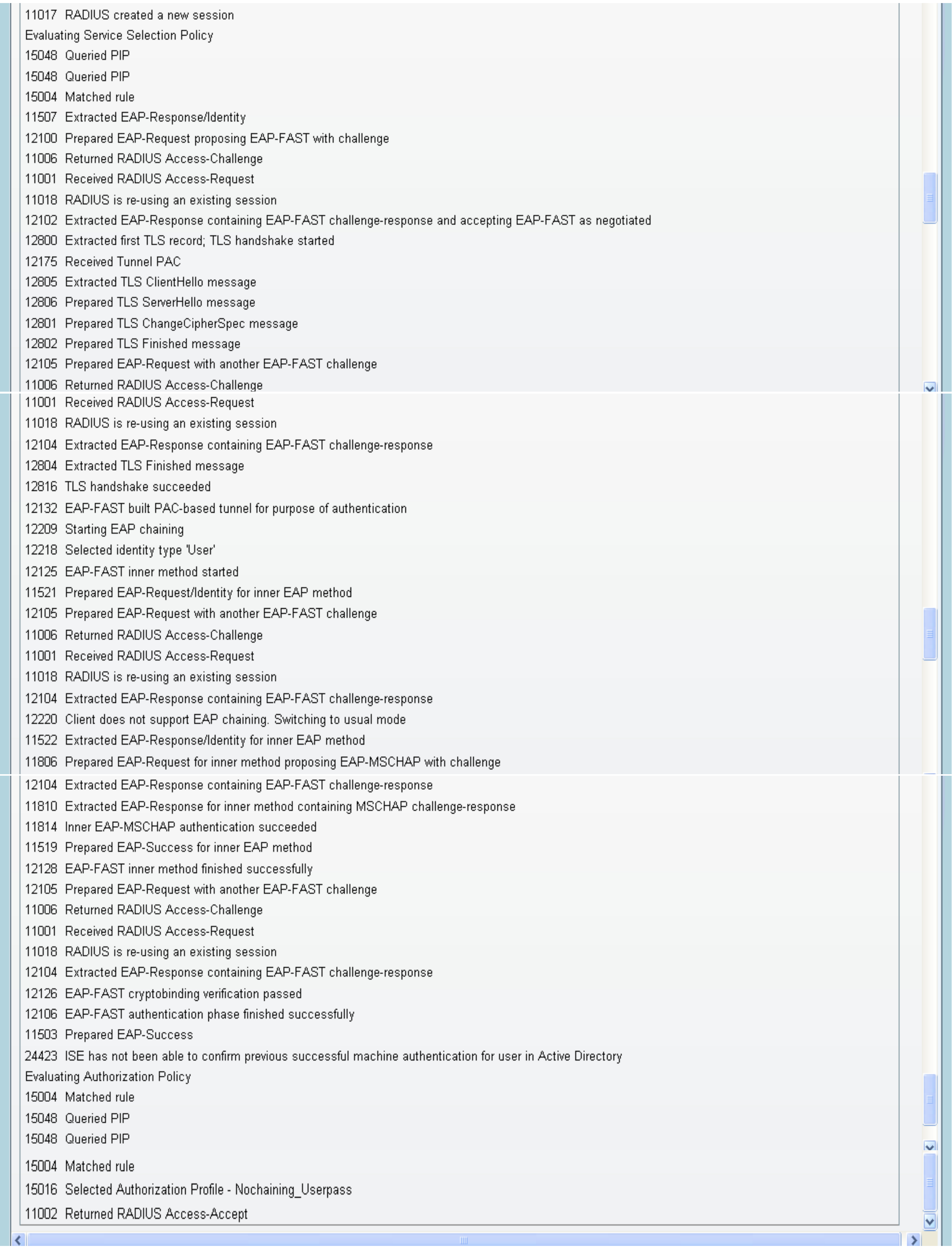


RADIUS Authentication Details

Identity Store:	AD1
Authorization Profiles:	Nochaining_Userpass
Active Directory Domain:	cfacres007.com
Identity Group:	
Allowed Protocol Selection Matched Rule:	EAPChaining_wireless
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users,AD1
Authorization Policy Matched Rule:	Default
SGA Security Group:	
AAA Session ID:	ise/122009432/5
Audit Session ID:	0501a8c00000000bdffd6d4f
Tunnel Details:	Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0) 12
Cisco-AVPairs:	audit-session-id=0501a8c00000000bdffd6d4f
Other Attributes:	ConfigVersionId=4,DestinationPort=1645,Protocol=Radius,Framed-MTU=1300,State=37CPMSessionID=0501a8c00000000bdffd6d4f;25SessionID=ise/122009432/5;,Airespace-Wlan-Id=1,EapChainingResult=No chaining,CPMSessionID=0501a8c00000000bdffd6d4f,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-f5-60:lab005
Posture Status:	NotApplicable
EPS Status:	

⊟ Steps

11001 Received RADIUS Access-Request



```
11017  RADIUS created a new session
Evaluating Service Selection Policy
15048  Queried PIP
15048  Queried PIP
15004  Matched rule
11507  Extracted EAP-Response/Identity
12100  Prepared EAP-Request proposing EAP-FAST with challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12175  Received Tunnel PAC
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message
12802  Prepared TLS Finished message
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
12804  Extracted TLS Finished message
12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
12209  Starting EAP chaining
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
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
11522  Extracted EAP-Response/Identity for inner EAP method
11806  Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12104  Extracted EAP-Response containing EAP-FAST challenge-response
11810  Extracted EAP-Response for inner method containing MSCHAP challenge-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-Response containing EAP-FAST challenge-response
12126  EAP-FAST cryptobinding verification passed
12106  EAP-FAST authentication phase finished successfully
11503  Prepared EAP-Success
24423  ISE has not been able to confirm previous successful machine authentication for user in Active Directory
Evaluating Authorization Policy
15004  Matched rule
15048  Queried PIP
15048  Queried PIP
15004  Matched rule
15016  Selected Authorization Profile - Nochaining_Userpass
11002  Returned RADIUS Access-Accept
```

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.

Frequently Asked Questions

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 (http://tools.ietf.org/html/draft-zhou-emu-eap-fastv2-00).

Appendix A: References

Cisco TrustSec System:

- http://www.cisco.com/go/trustsec
- 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: http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- 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: http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- 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: http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- For Cisco Wireless LAN Controllers: http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.htmlAdding Identity Stores and Creating Authentication Policies