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

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

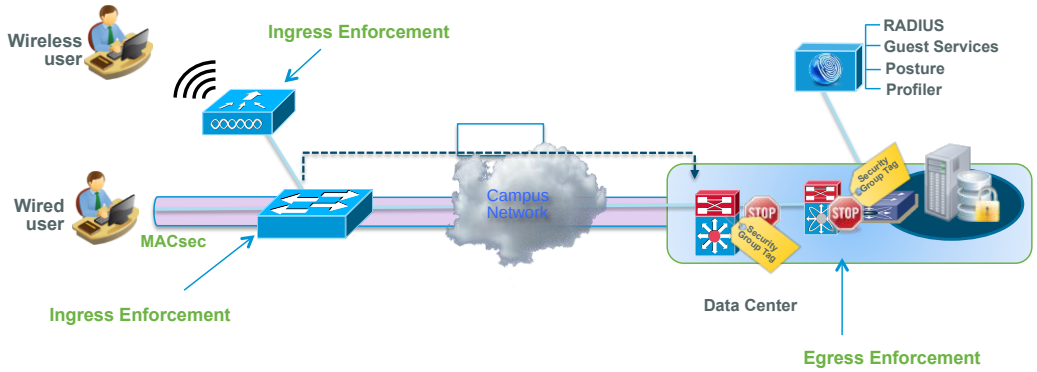
What Is the Cisco TrustSec System?

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

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

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

Figure 1: TrustSec Architecture Overview

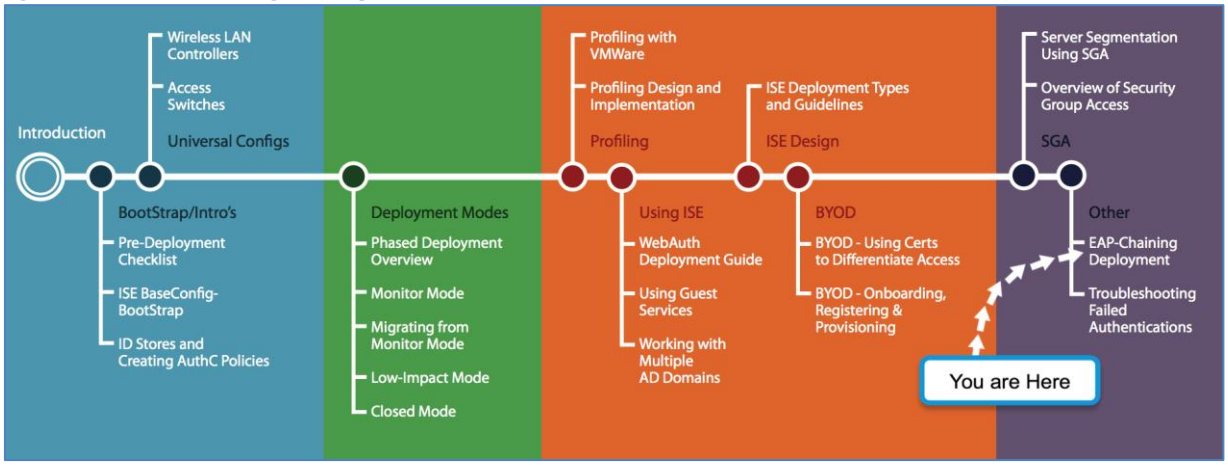


About the TrustSec How-To Guides

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

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

Figure 2: How-To Guide Navigation Map



What does it mean to be 'TrustSec Certified'?

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

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

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

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

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

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

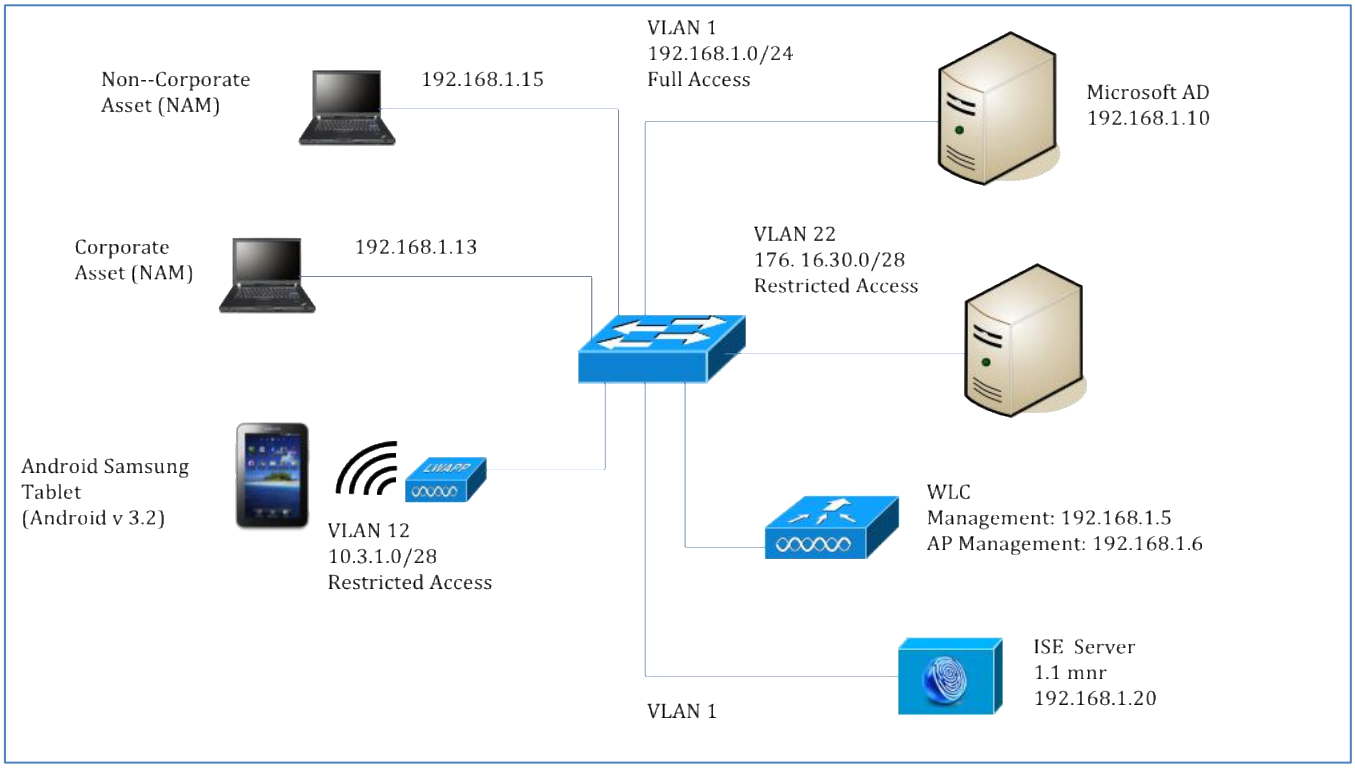
The Network Access Manager (NAM) will obtain both machine and user credentials from Windows (username/password) before the user logs in or when the user logs out- and after the user logs in, respectively. EAP Chaining will be enabled in the EAP-FAST authentication protocol, once the secure TLS tunnel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

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

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

Architecture

Figure 3 Architecture used in this document



Software/Hardware Requirements:

Client:

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

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

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

To accomplish EAP Chaining:

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

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

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

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

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

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

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

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

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

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.

Procedure 1 Adding Network Devices to ISE

Configure your WLC and switch for ISE and enable RADIUS

Step 1 Select → Administration → Network Resources → Network Devices

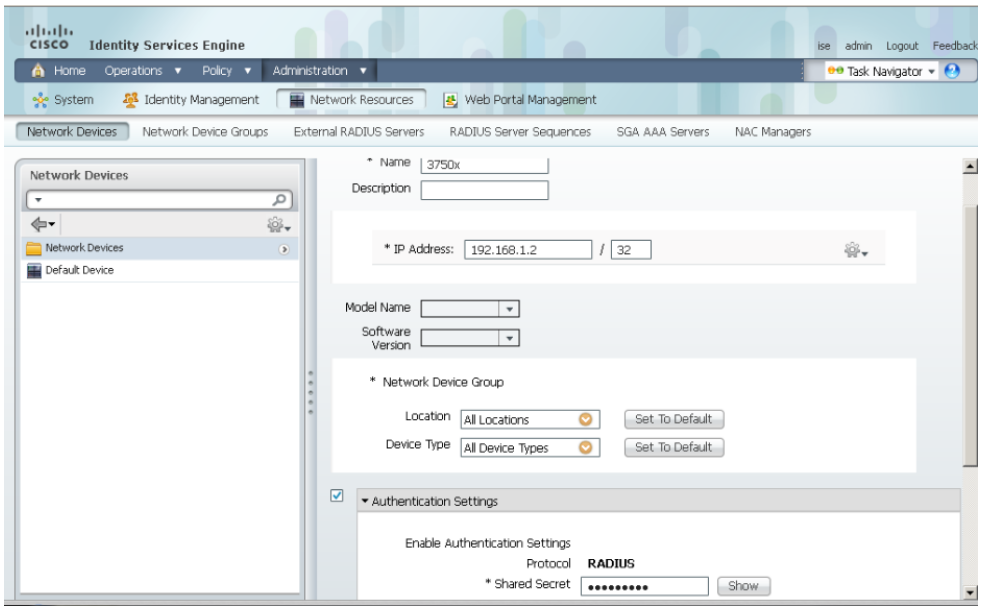
Step 2 Select → Add

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

Figure 4 an example of the switch configuration



Procedure 2 Add Microsoft Active Directory as the External Identity Store

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

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

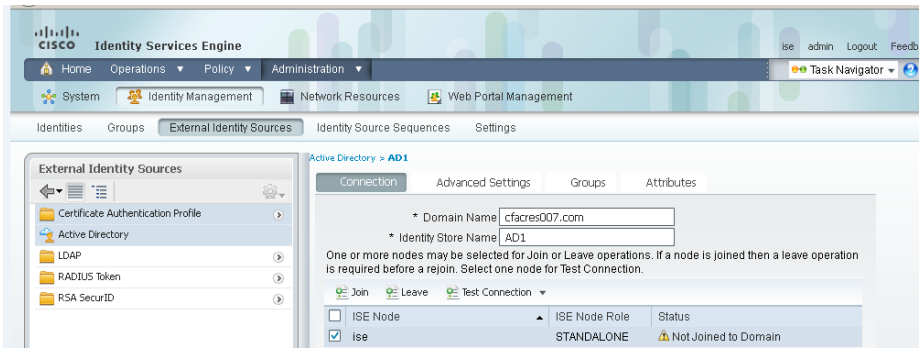
Step 2 Enter the Domain Name

```
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

Figure 5 Active Directory Setting



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

Each ISE node must join the AD domain.

Step 1 Select your ISE node

Step 2 Click Join

Step 3 Enter the user name credentials

```
The results are shown in Figures 4 and 5.
```

Figure 6 Prompt to join the domain

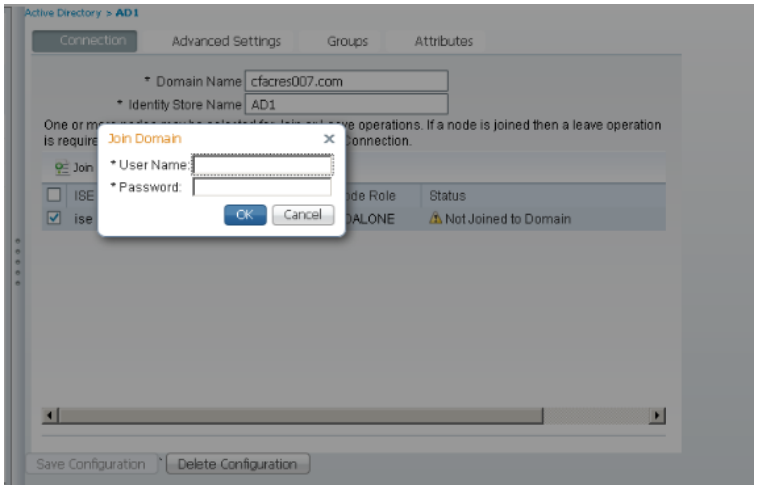
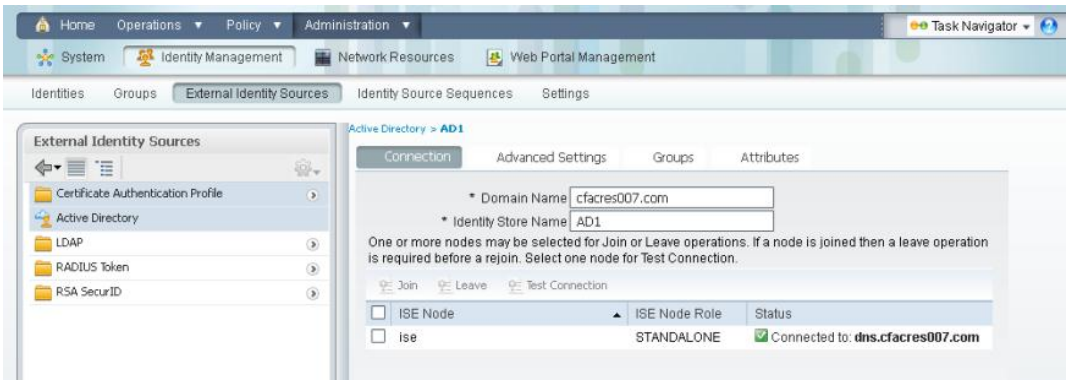


Figure 7 The results after the successful join to the domain



Procedure 4 Configuring Active Directory Groups

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

Step 1 Select Administration → 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'

Procedure 5 Defining the Identity Source Sequence

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

Step 1 Select Administration → Identity Management → Identity Source Sequences

Step 2 Click Add

Step 3 **Enter the name**

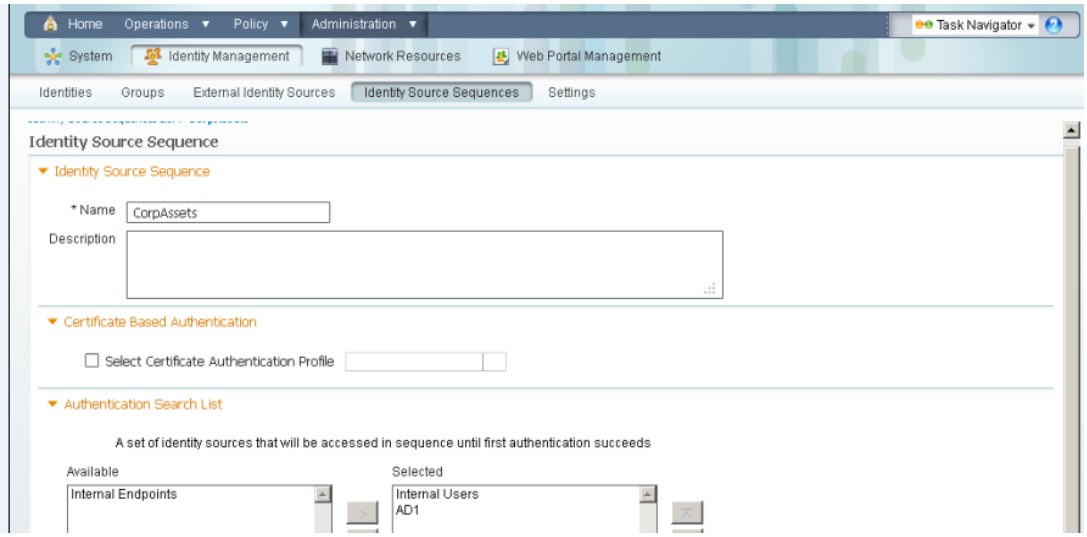
```
In this example, CorpAssets was used
```

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

Figure 8 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.

Procedure 6 Enable EAP Chaining in the EAP-FAST Protocol

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

Step 1 Select Policy → 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:

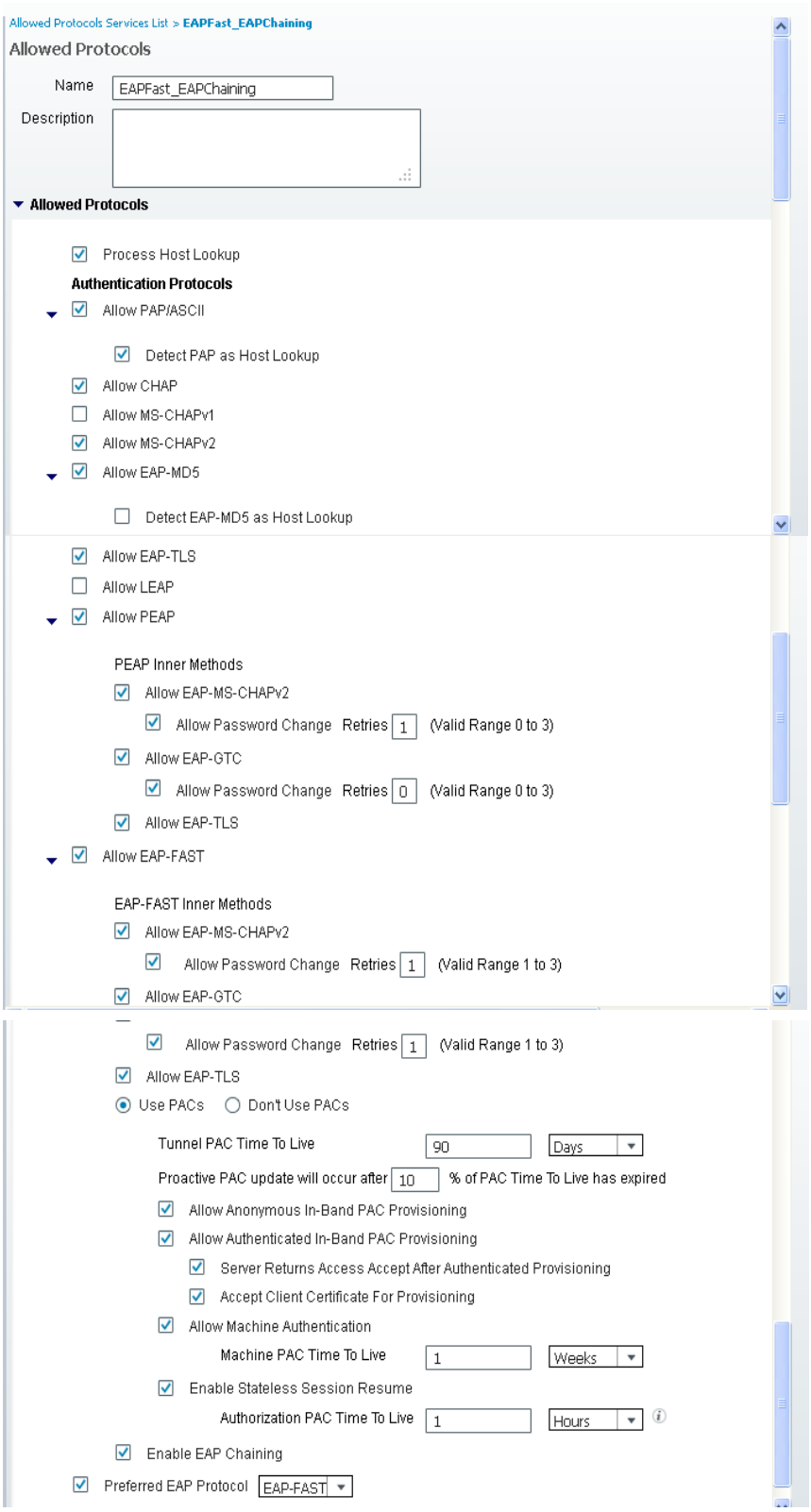
- `Server Returns Access Accept After Authenticated Provisioning`
- `Accept Client Certificate for Provisioning`

Step 7 Enable 'Allow Machine Authentication'

Step 8 Enable 'Stateless Session Resume'

Step 9 Click Submit

Figure 9 EAPFast_EAPChaining Allowed Protocols Definition



Procedure 7 Define the Authentication Policy

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

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

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

Step 2 Select **Polcy → 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

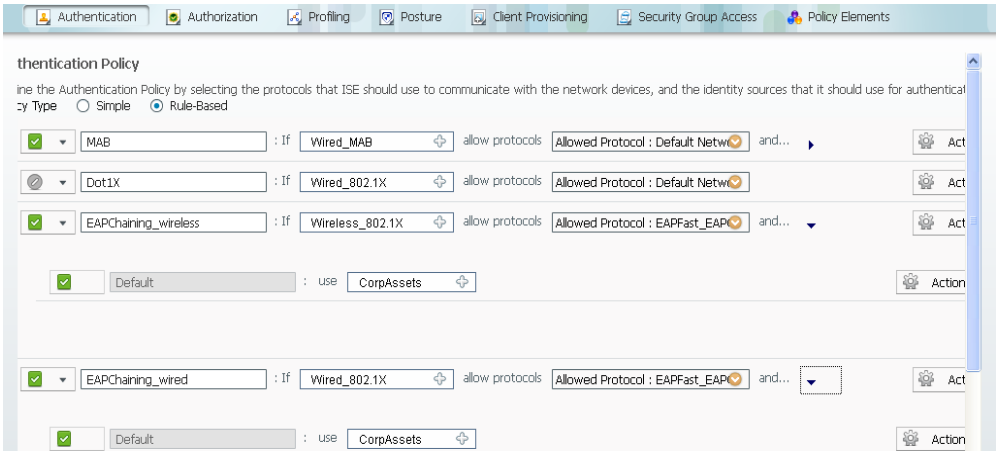
```
In this example CorpAssets was used.
```

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

Figure 10 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

Procedure 8 Define the Authorization Profiles

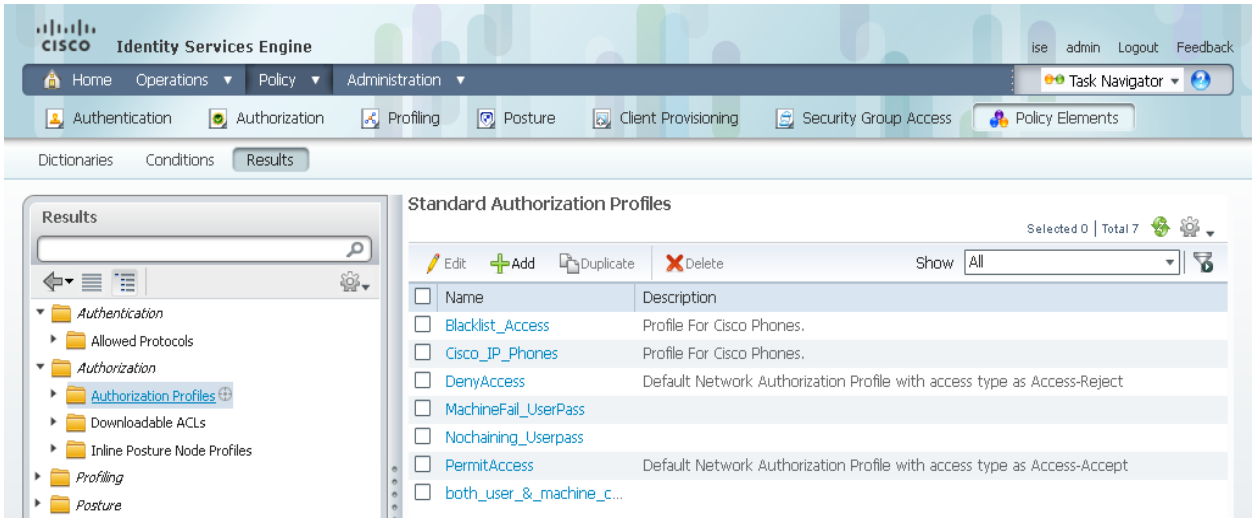
In this document, we will define, three Authorization Policies, based on the EAP Chaining results and then provide the appropriate level of access as defined by their corresponding authorization profiles.

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

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

The completed authorization profiles are shown below.

Figure 11 Completed Authorization Profiles



Procedure 9 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

Figure 12 Authorization Profile for 'MachineFail_UserPass'

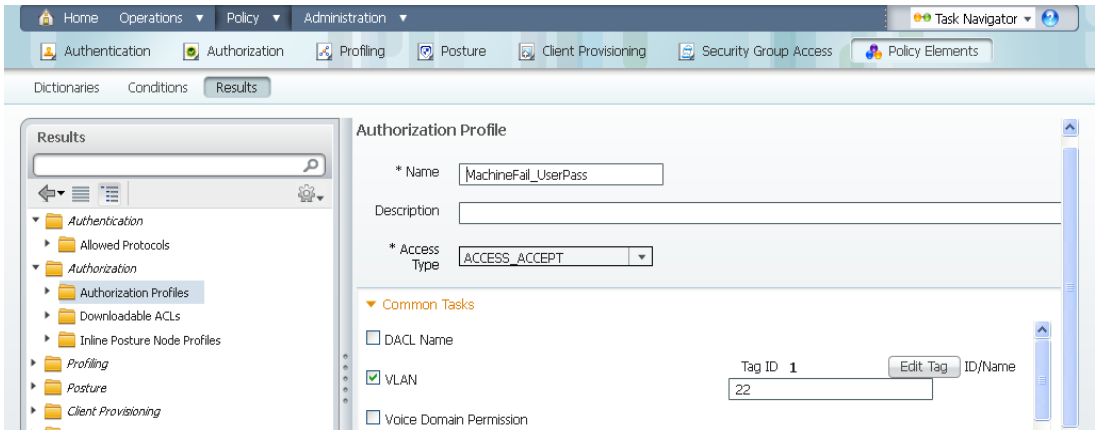


Figure 13

Procedure 10 Define the Authorization Profile for 'NoChaining_UserPass'.

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

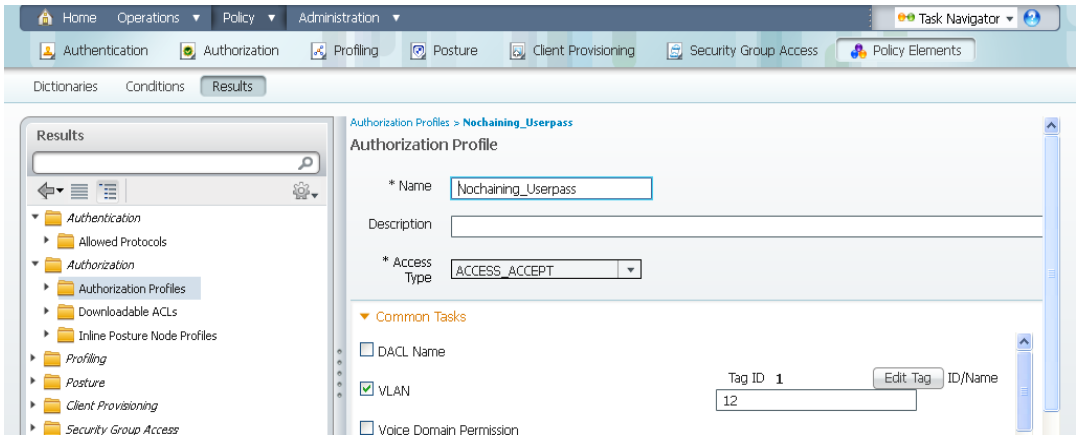
Step 2 Select **Add**

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

Figure 13 Authorization Profile for 'NoChaining_UserPass'



Procedure 11 Define the Authorization Profile for 'both_user_&_machine_credentials_passed_auth'

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

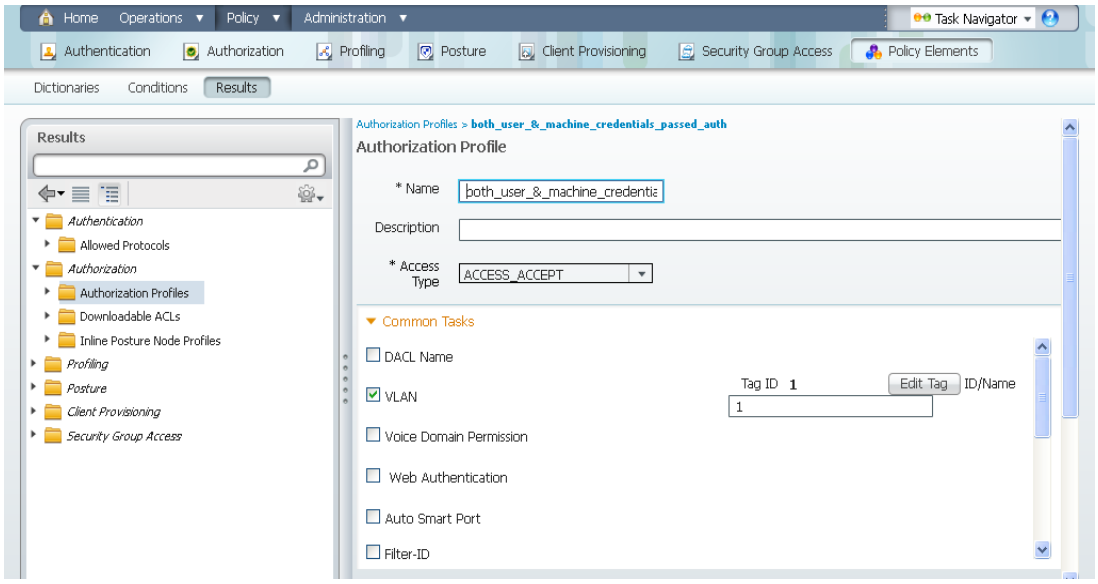
Step 2 Select **Add**

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

Figure 14 Authorization Profile for 'both_user_&_machine_credentials_passed_auth'



Defining Authorization Condition Rules and Authorization Policies

Procedure 12 Define the Authorization Condition for, “UserPASSED_MachinePASSED”:

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

Step 1 Navigate to Policy → Policy Elements → Conditions → Authorization → Compound Conditions

Step 2 Add name, ‘EAP-Chaining_UserPASS_MachinePASS’

Step 3 Add description, this is optional

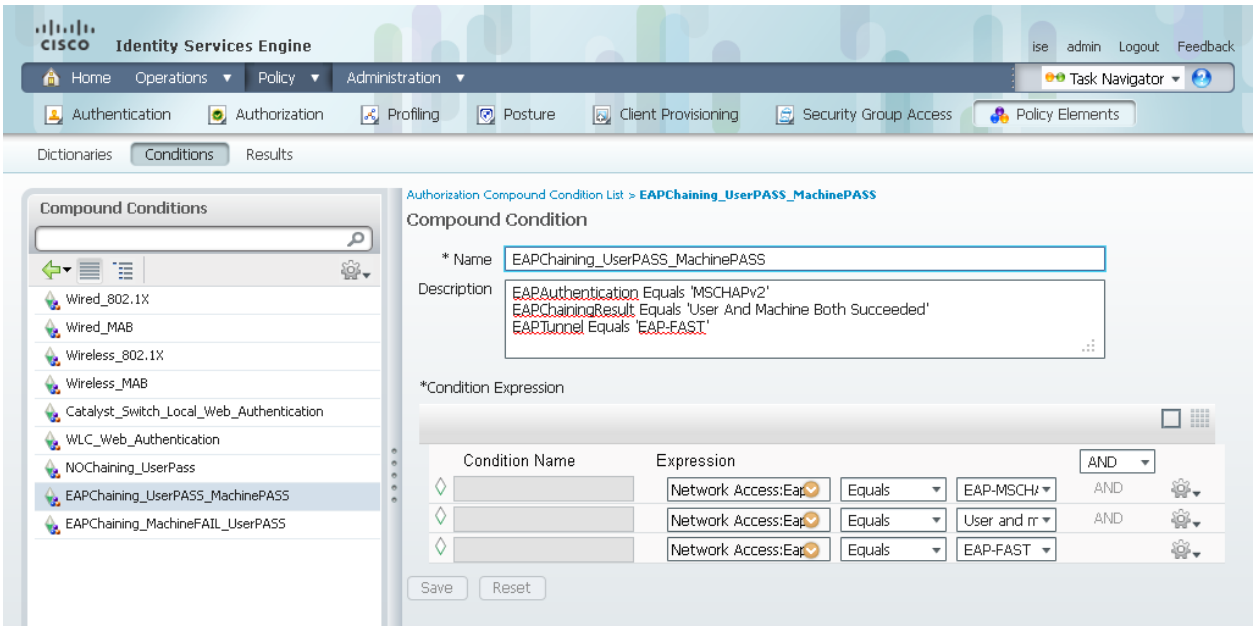
For **expressions**, select the following:

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

.

Figure 15 EAPChaining_UserPASS_MachinePASS Compound Condition



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

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

Step 1 Select Policy → Policy Elements → Conditions → Authorization → Compound Conditions

Step 2 Add name, 'NOChaining_UserPASS'

Step 3 Add description, this is optional

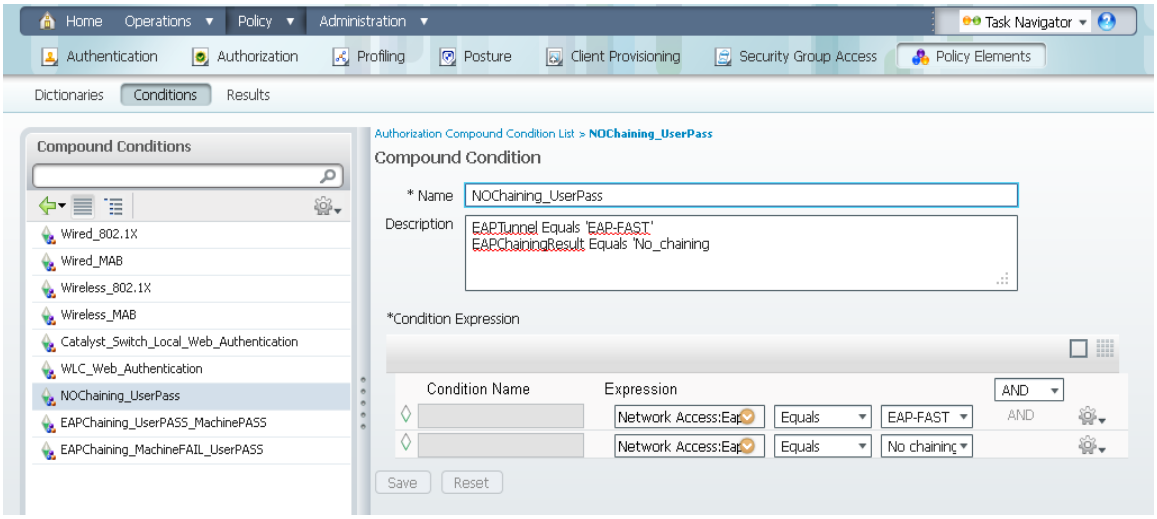
For expressions, select the following:

d. Network Access:EAPTunnel equals EAP-FAST

e. Network Access:EAP-ChainingResult equals No_chaining

Step 4 Submit the changes

Figure 16 NOChaining_UserPass Compound Condition



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

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

Step 1 Select Policy → 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:

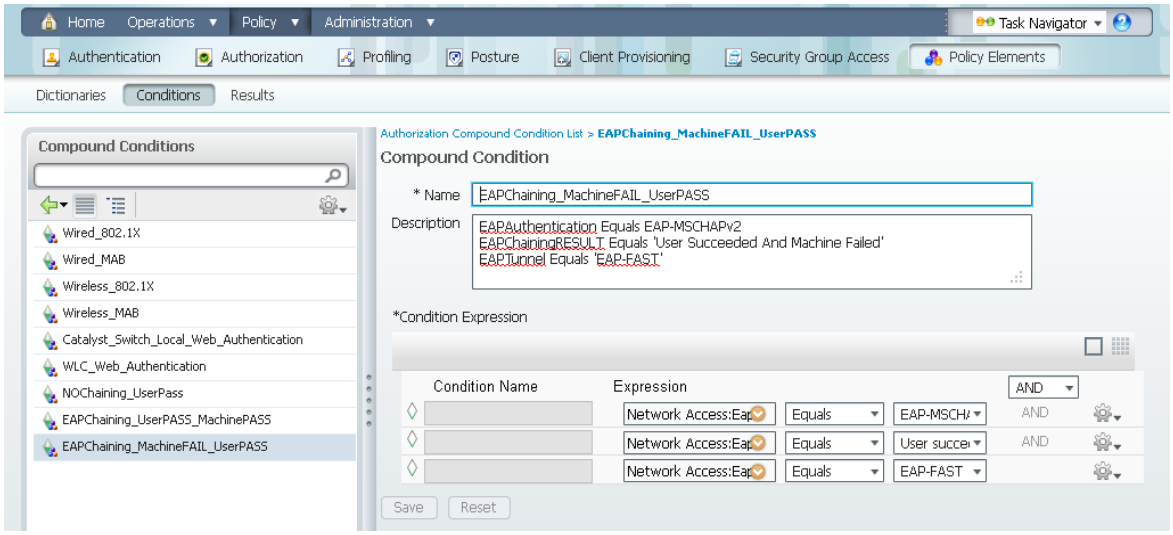
f. **Network Access:EAPAuthentication equals EAP-MSCHAPv2**

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

h. **Network Access: EAPTunnel equals EAP-FAST**

Step 4 Submit the changes

Figure 17 EAPChaining_MachineFAIL_UserPASS Compound Condition



Creating Authorization Policies

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

Procedure 15 Create an Authorization Policy for ‘UserPASSED_MachinePASSED’

Step 1 Navigate to Policy → 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

Procedure 16 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

Procedure 17 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

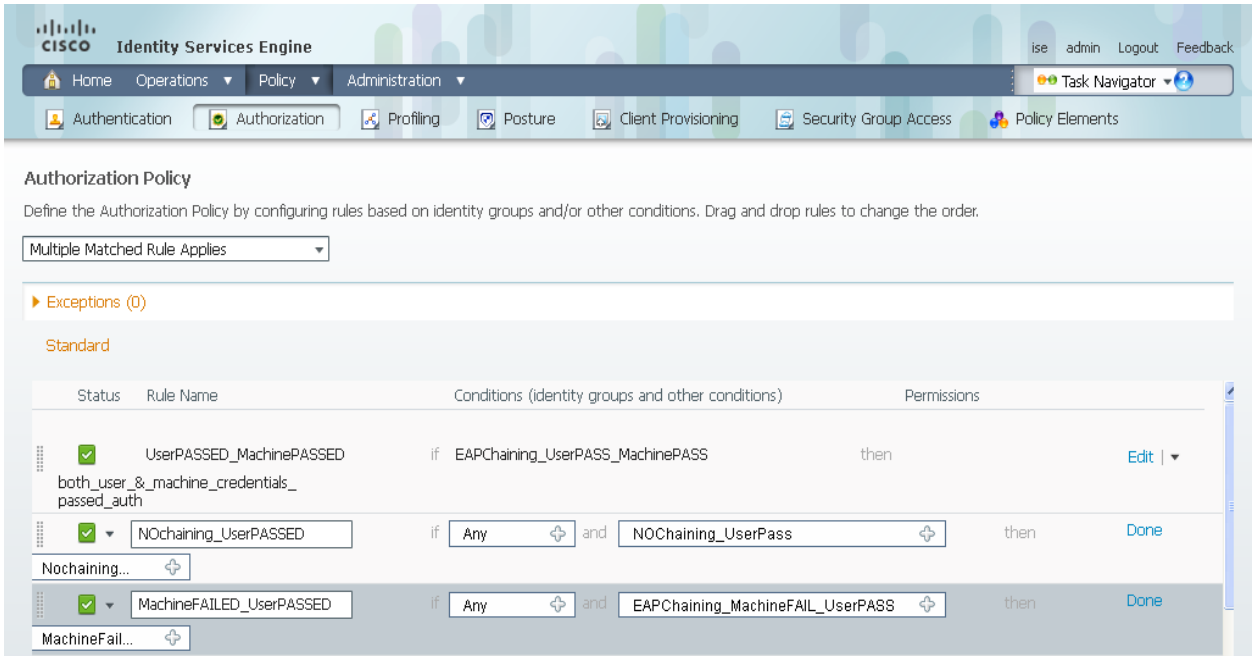
`In this example, 'MachineFAILED_UserPASSED' were used.`

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

Figure 18 - 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

Procedure 18 Installing AnyConnect NAM

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

Step 2 Run 'setup'

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

Step 3 Enable AnyConnect Diagnostics and Reporting Tool

Step 4 AnyConnect Network Access Manager

Figure 19 Installation Selector

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.)

Figure 20 AnyConnect Quality Improvement Feature

Procedure 19 Creating a NAM Profile with the Profile Editor

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

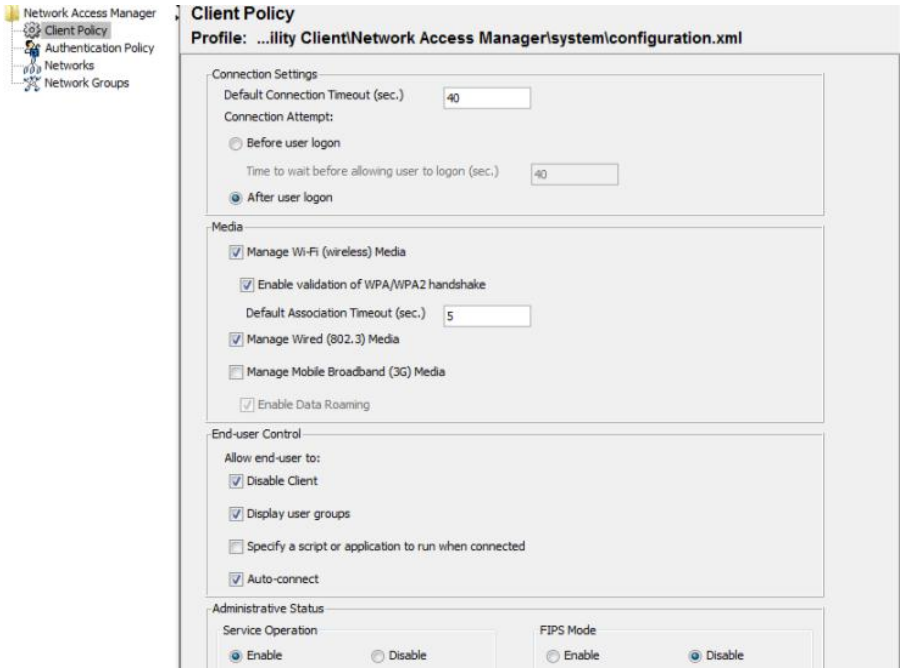
Note: Please note that the NAM configuration should be saved as 'configuration.xml', and saved to the 'NewConfigFiles' directory. Right-click on the AnyConnect GUI in the system tray, select 'Network Repair' . This will place the configuration.xml file into the NAM system directory.)

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

Step 2 Keep the defaults, and select → Authentication Policy

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

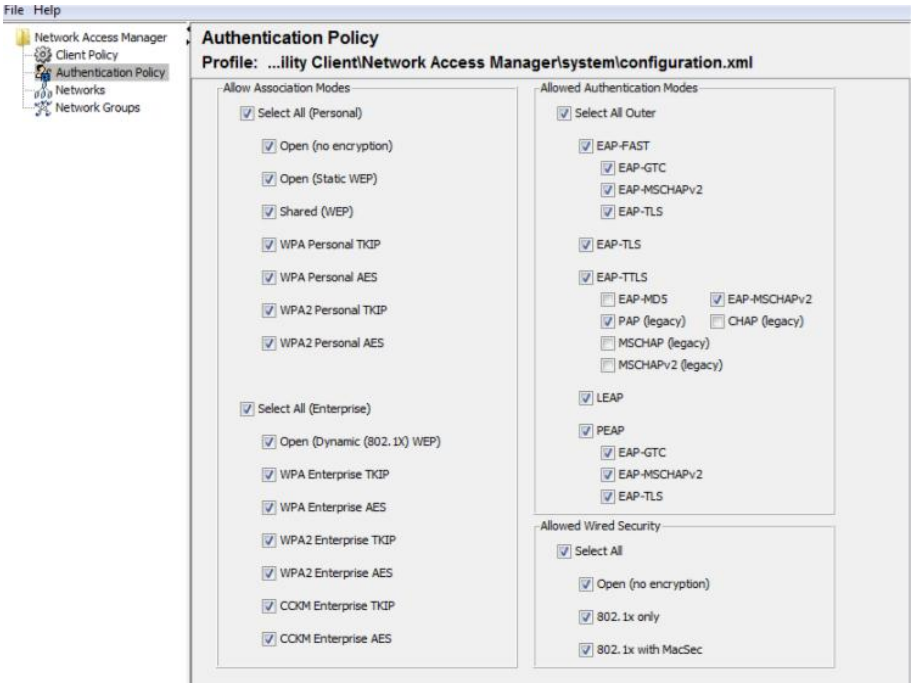
Figure 21 NAM profile Editor



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

Figure 22 NAM Authentication Policy

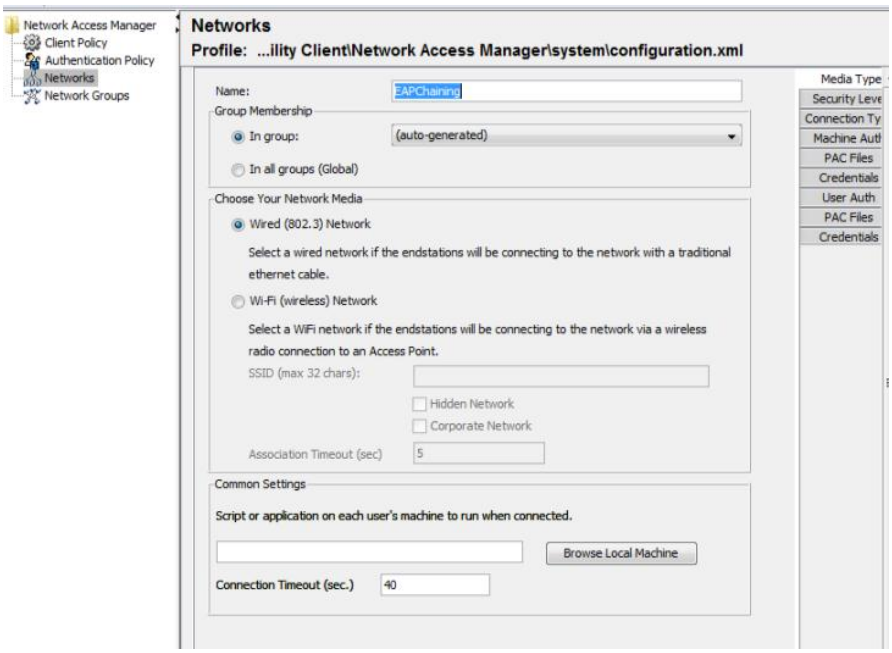


Step 4 **Define your network**

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

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

Figure 23 Defining the Network



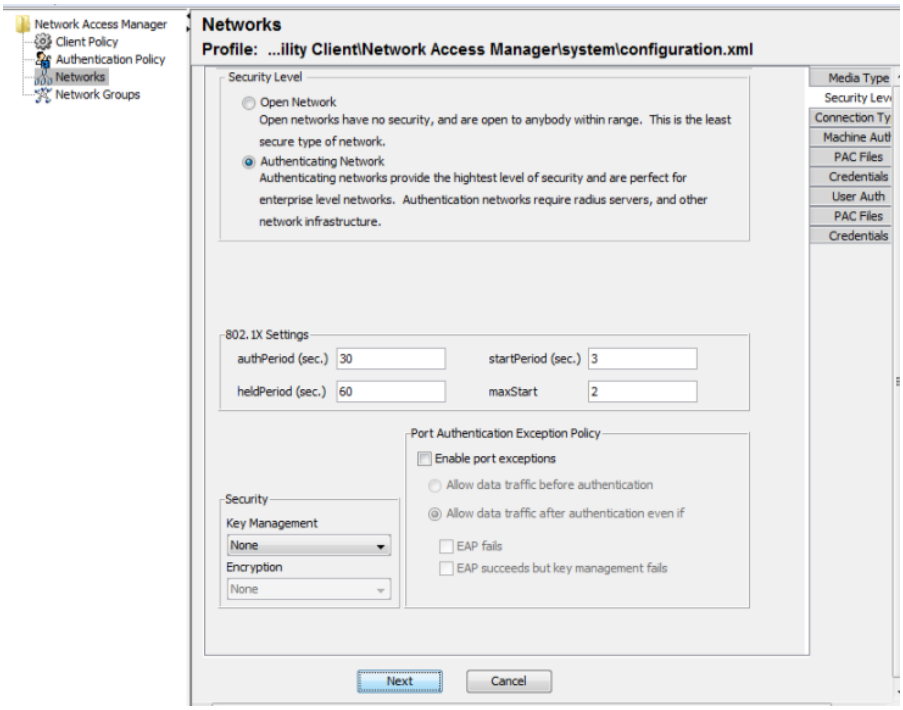
Step 6 Select Authenticating Network, as illustrated in Figure 22

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

Step 7 Keep the defaults

Step 8 **Click Next**

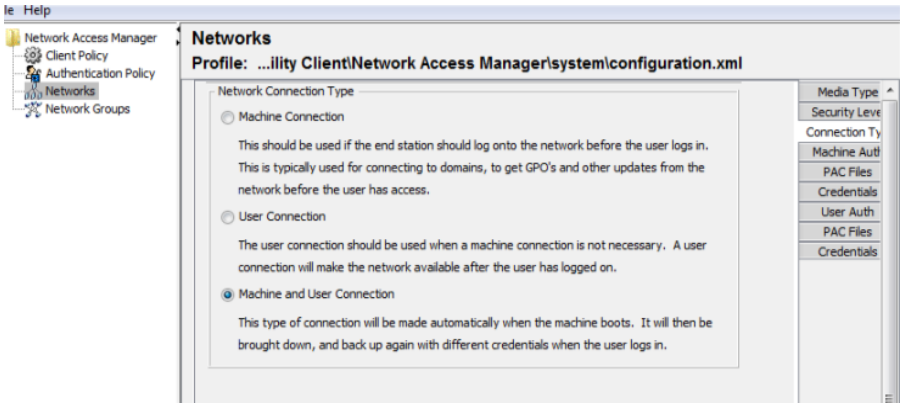
Figure 24 Network Security Level



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

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

Figure 25 Network Connection Type



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'

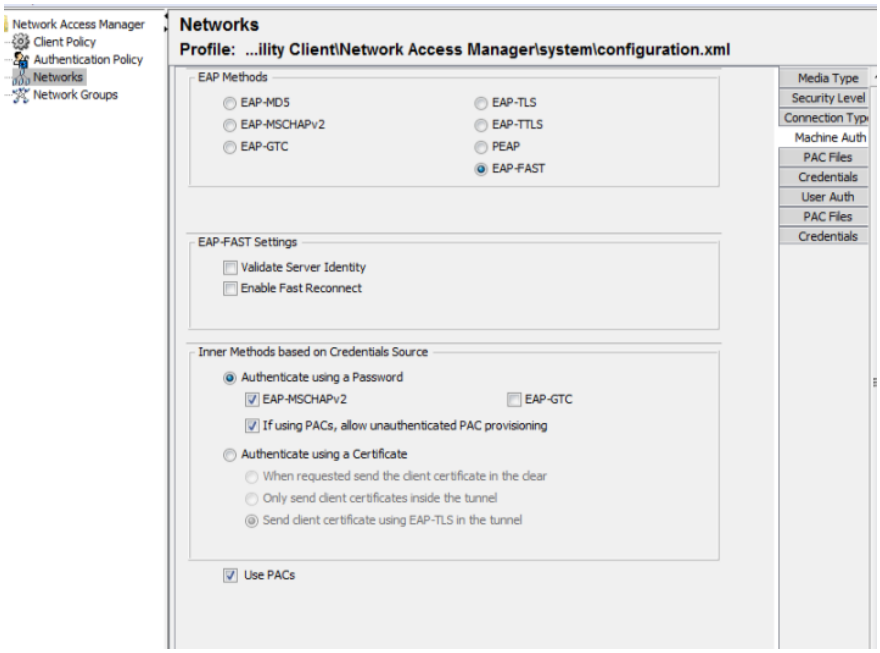
Step 14 Select'If using PACs

Step 15 Select 'Allow unauthenticated PAC provisioning'

Step 16 Select 'Use PACs'

Step 17 Click Next

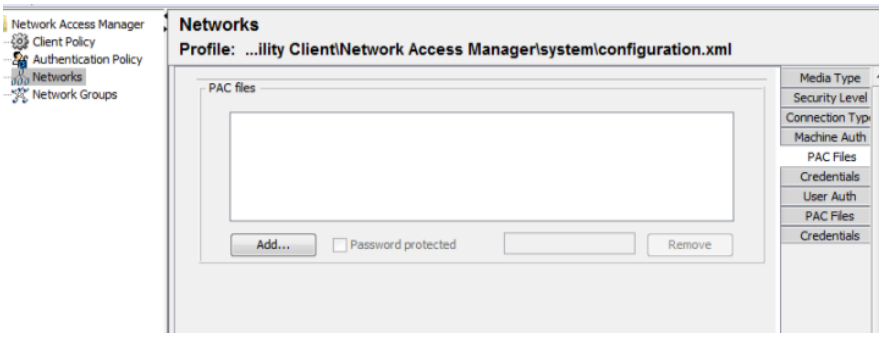
Figure 26 The Completed Configuration



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

Note: PAC files will be provisioned from ISE

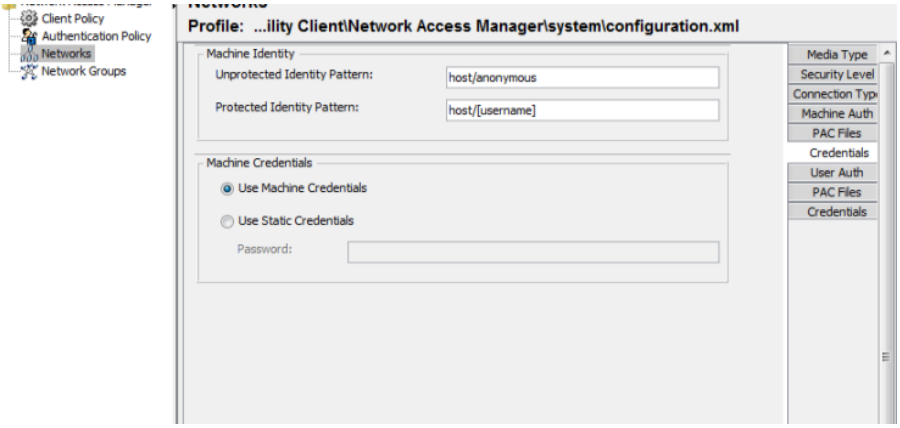
Figure 27 Leave PAC files as default (blank)



Step 19 Keep the defaults for Machine Identity

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

Figure 28 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.

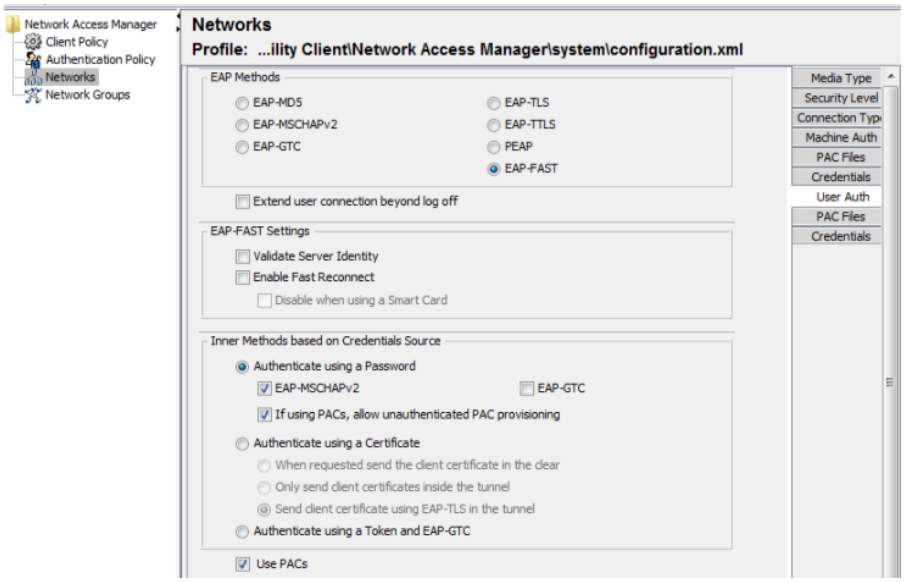
Step 23 Select EAP-MSCHAPv2

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

Step 25 Select Use PACs

Step 26 Click Next

Figure 29 Completed Configuration



Step 27 Leave the PAC file as empty

Note: PAC files will be provisioned from ISE

Step 28 Click Next

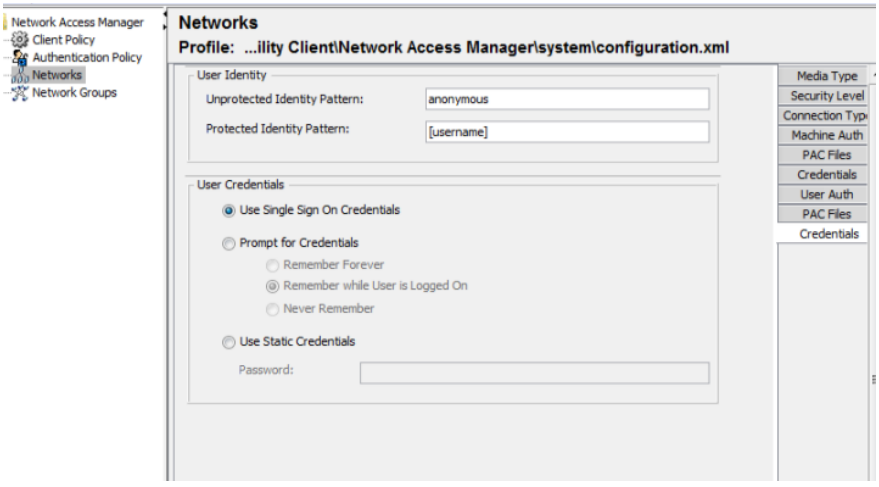
Step 29 Keep the defaults for the User Identity.

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’

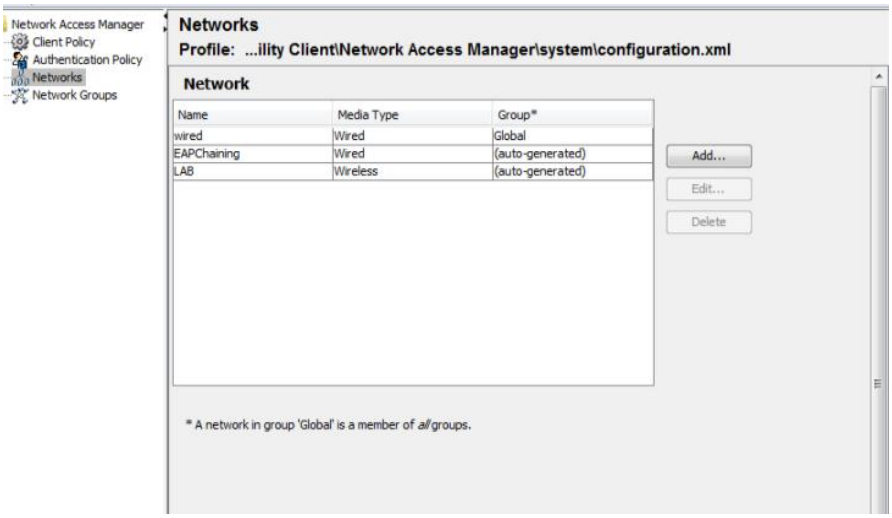
Step 31 Select Done

Figure 30 Completed User Authentication Configuration



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

Figure 31 Networks List



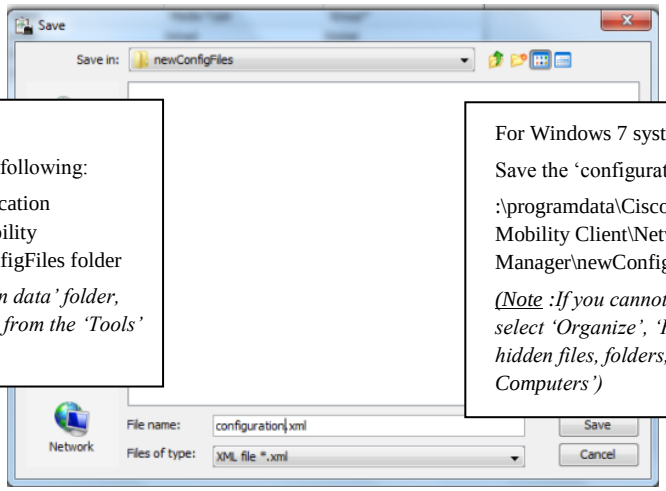
Step 32 From the drop-down File Menu, select 'Save-As'

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.

Figure 32 - Saving configuration.xml to the newConfigFiles directory



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')

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

Step 36 Select 'Network Repair'

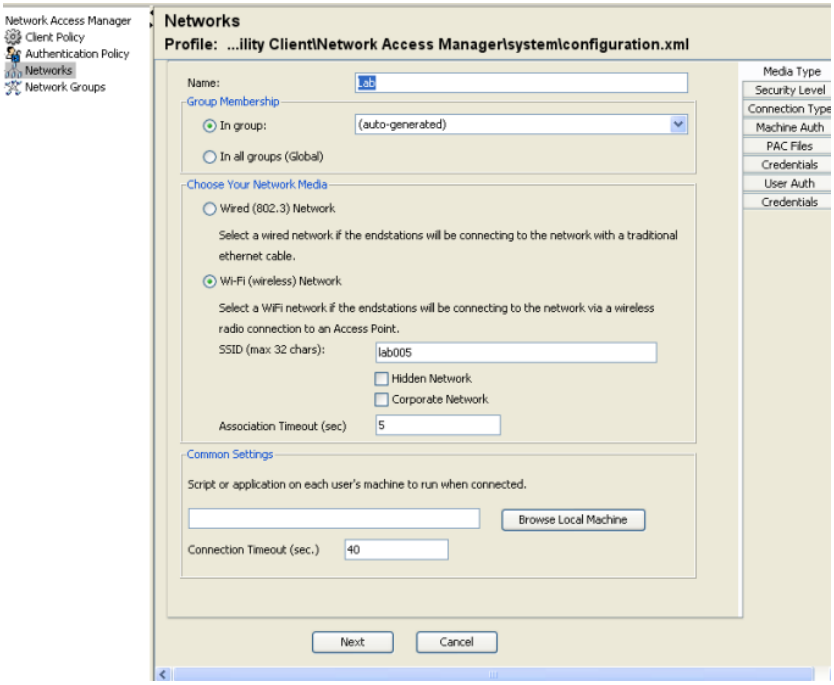
Procedure 20 Configuring Network Access Manager for Wireless Networks

Step 1 Provide a name for your wireless networks

Step 2 Define the SSID

Step 3 Click Next

Figure 33 Defining the Wireless Network

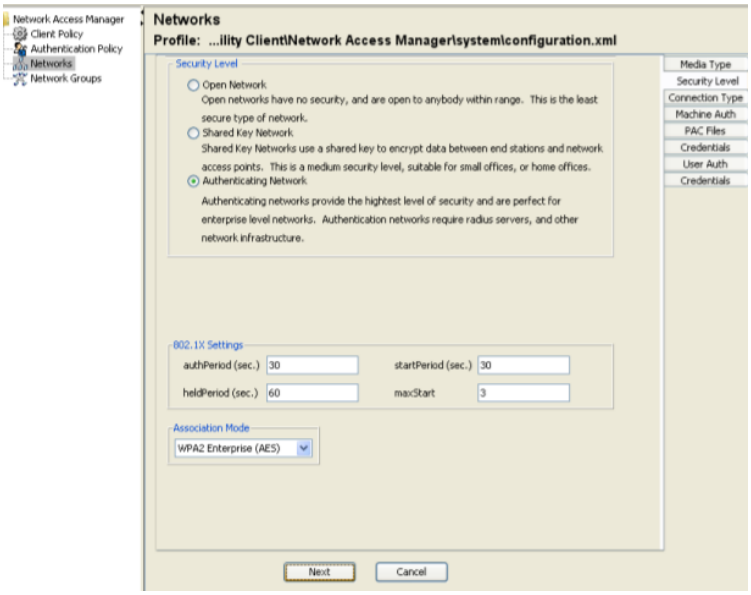


Step 4 Select 'Authenticating Network'

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

Step 6 Click Next

Figure 34 Wireless Network Settings for Steps 4 and 5

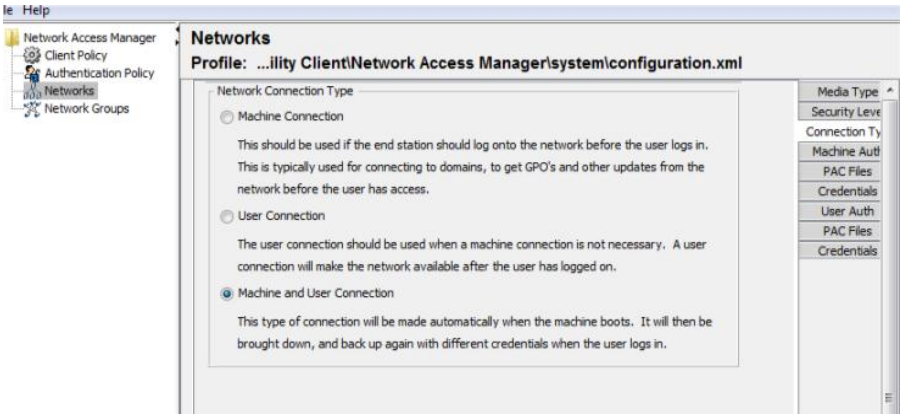


Step 7 Select 'Machine and User Connection'

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

Step 8 Click Next

Figure 35 Network Connection Type is Machine and User



Step 9 Select EAP-FAST

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

Step 10 Select EAP-FAST

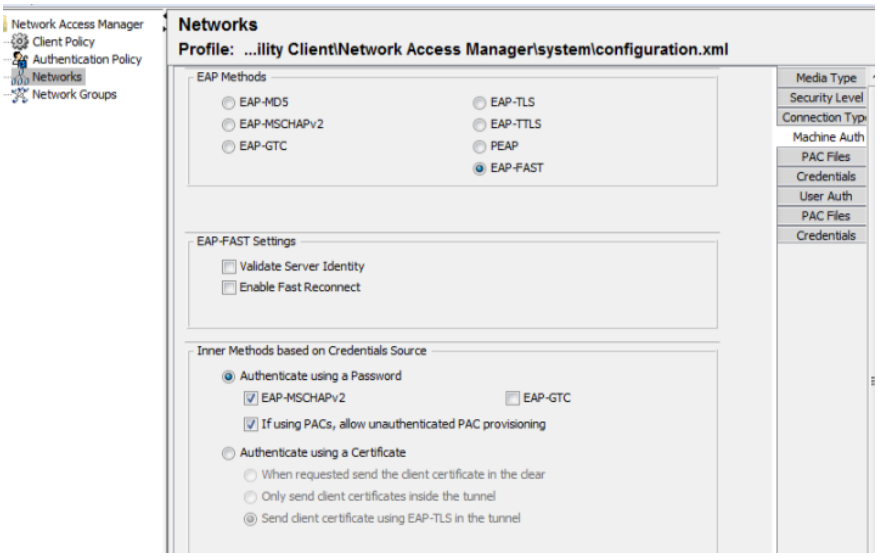
Step 11 Select 'Authenticate using a Password' in the 'Inner Methods based on Credentials Source' section.

Step 12 Select EAP-MSCHAPv2

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

Step 14 Select Use PACs

Figure 36 The Completed Configuration



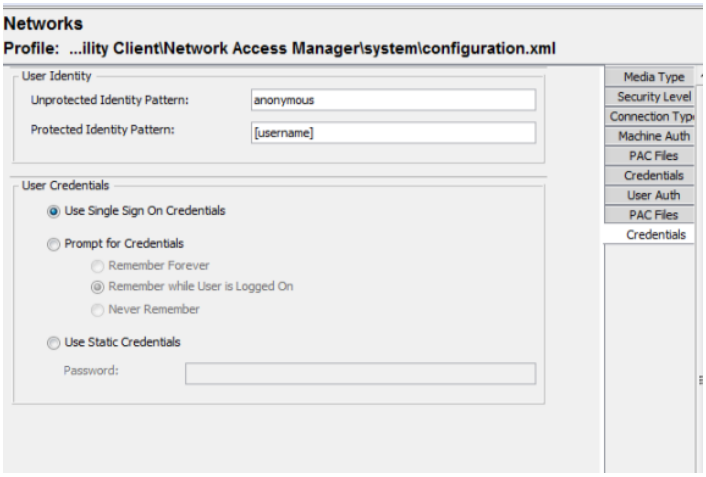
Step 15 Keep the defaults for the User Identity.

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

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

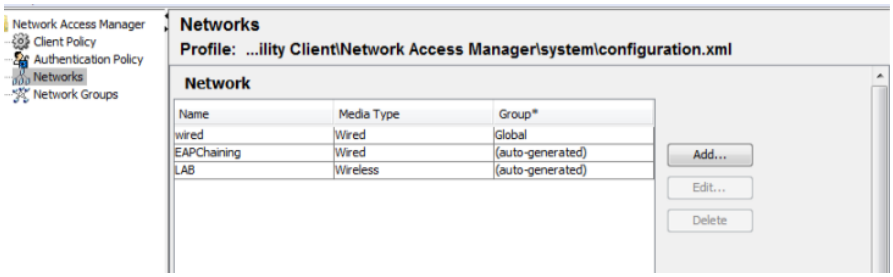
Step 17 Select Done

Figure 37 Completed Wireless User Authentication



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

Figure 38 List of Networks

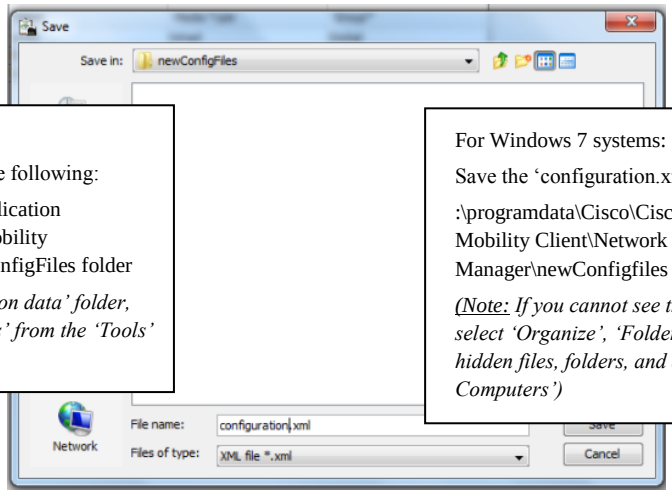


Step 18 From the drop-down File menu, select 'Save-As'

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

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

Figure 39 Saving the configuration.xml to the newConfigFiles directory



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')

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

Step 22 Select 'Network Repair'

TESTING PROCEDURE

EAP Chaining was tested with the following business cases:

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

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

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

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

Figure 40 AnyConnect User Interface

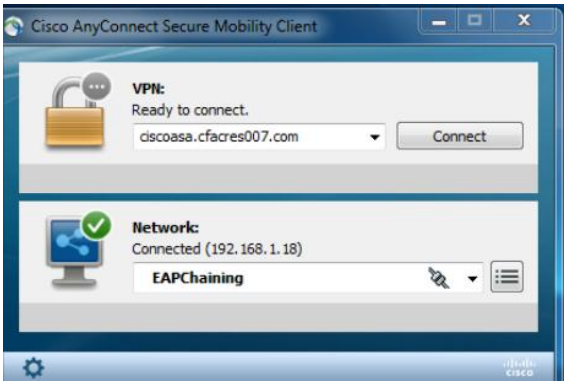
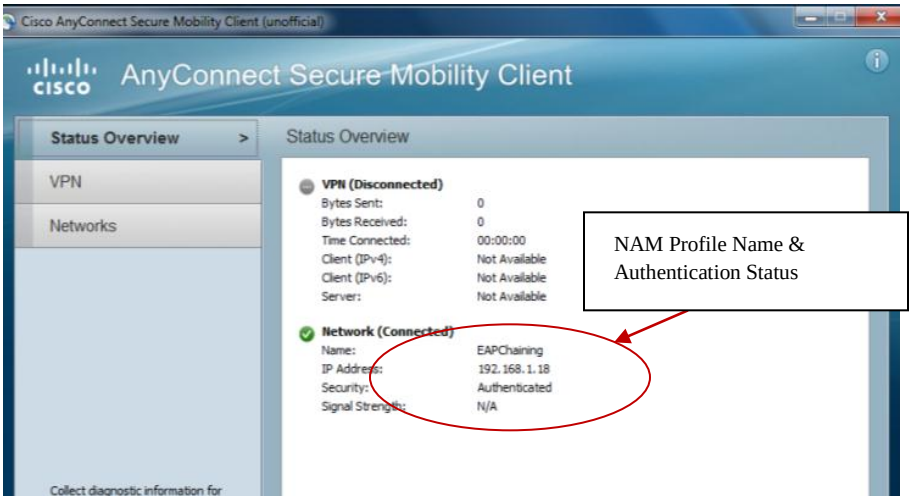


Figure 41 NAM Status



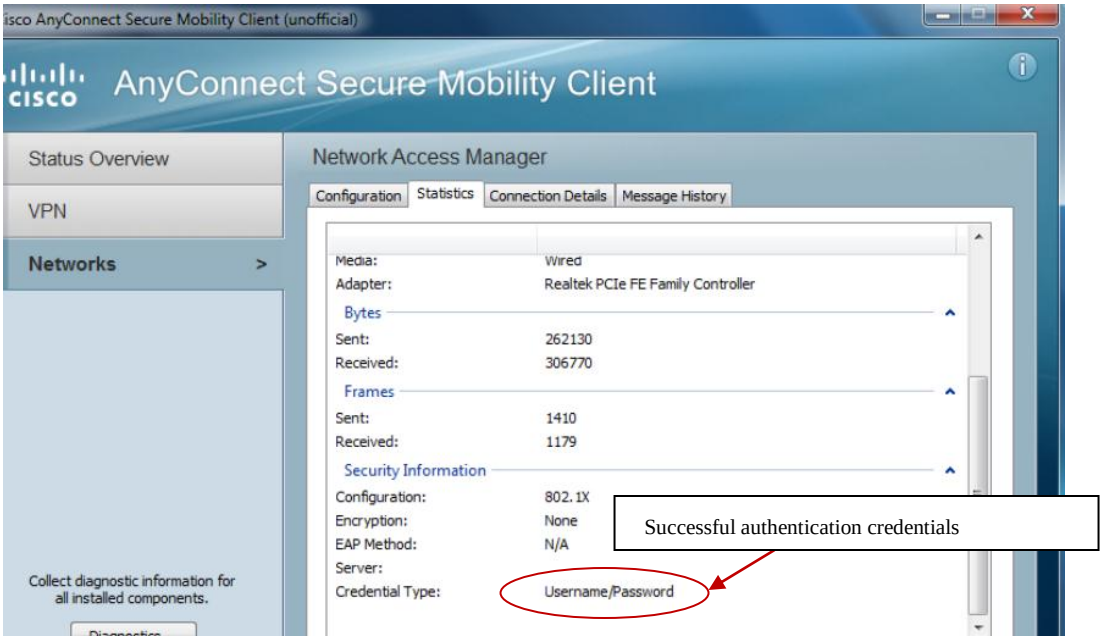


Figure 42 802.1X log information from the switch

```
*Mar  3 03:29:27.830: %AUTHMGR-5-START: Starting 'dot1x' for client (f0de.f194.6
59c) on Interface Gi1/0/15 AuditSessionID C0A80102000000540B0C7B91
*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 C0A80102000000540B0C7B91
*Mar  3 03:30:56.833: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (f0
de.f194.659c) on Interface Gi1/0/15 AuditSessionID C0A80102000000540B0C7B91
```

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

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

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

Figure 43 Successful Authentication

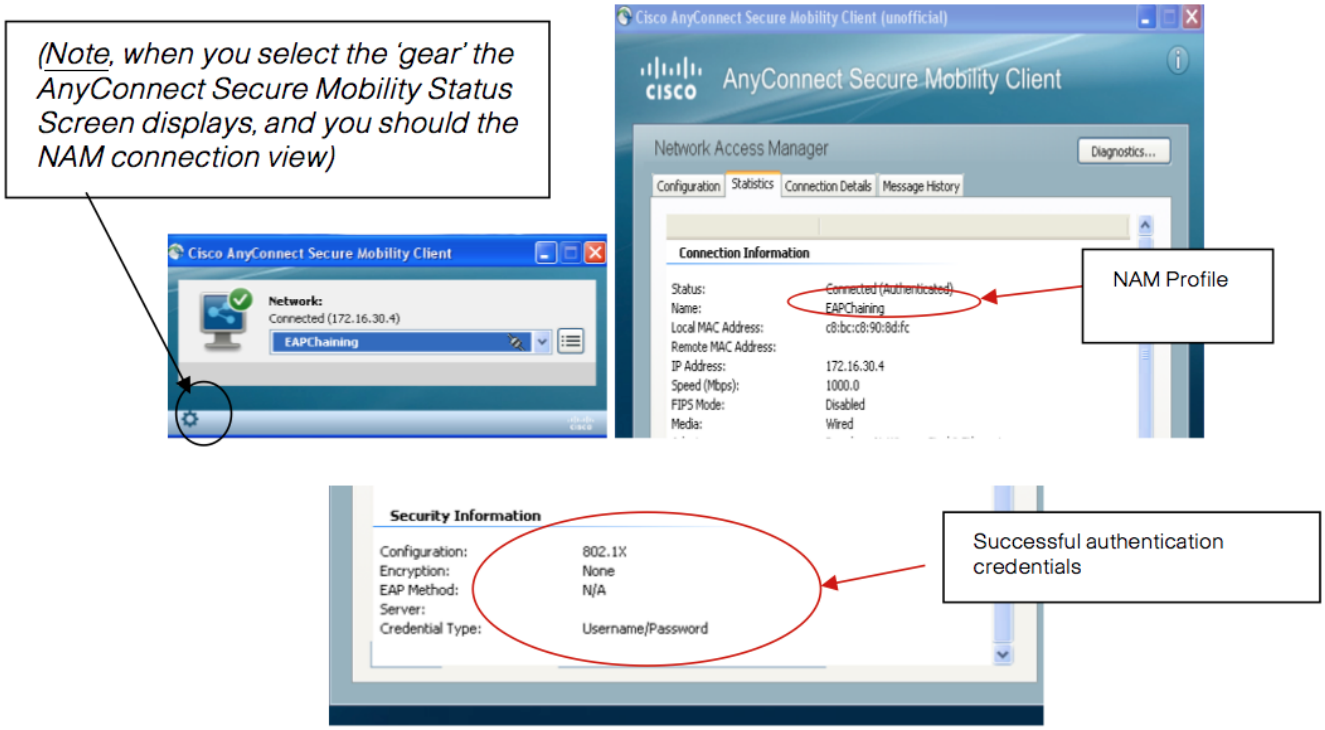


Figure 44 802.1X log information from the switch

```
Switch#
*Mar  3 04:21:11.699: %AUTHMGR-5-START: Starting 'dot1x' for client (c8bc.c890.8
dfc) on Interface Gi1/0/15 AuditSessionID C0A801020000000550B3BD8F0
*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 C0A801020000000550B3BD8F0
*Mar  3 04:21:13.234: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (c8
bc.c890.8dfc) on Interface Gi1/0/15 AuditSessionID C0A801020000000550B3BD8F0
*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
```

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

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

The Samsung Android Tablet settings are as follows:

```
EAP-Method = FAST,
Provisioning = 1
Phase 2 Authentication = MSCHAPv2
Identity = Username (i.e. employee1)
Anonymous Identity = username (i.e employee1)
Password = password  (i.e. cisco123)
```

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

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

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

Figure 45 EAP-FAST selection

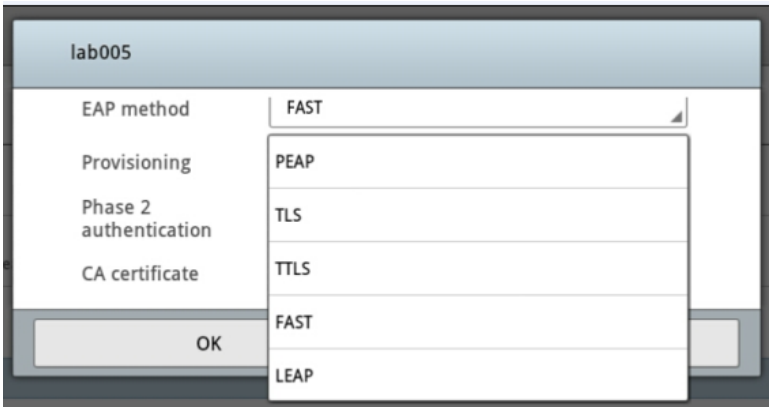


Figure 46 Provisioning set to "1"

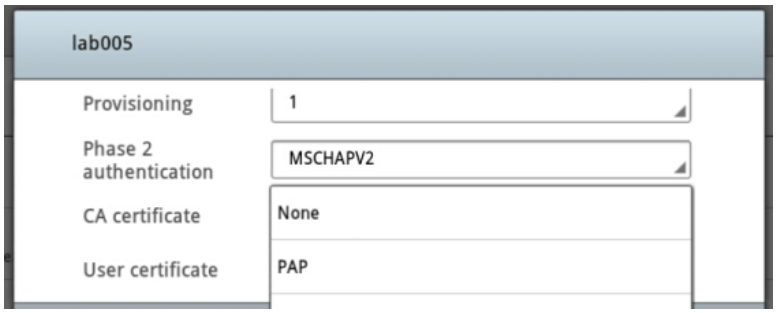


Figure 47 Phase-2 Authentication = MSCHAPv2

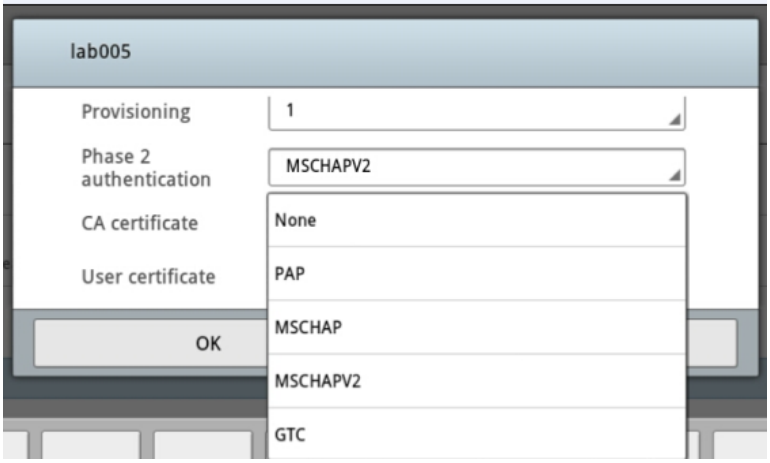


Figure 48 Cisco Wireless LAN Controller - showing successful authentication

Detailed View of EAP Chaining

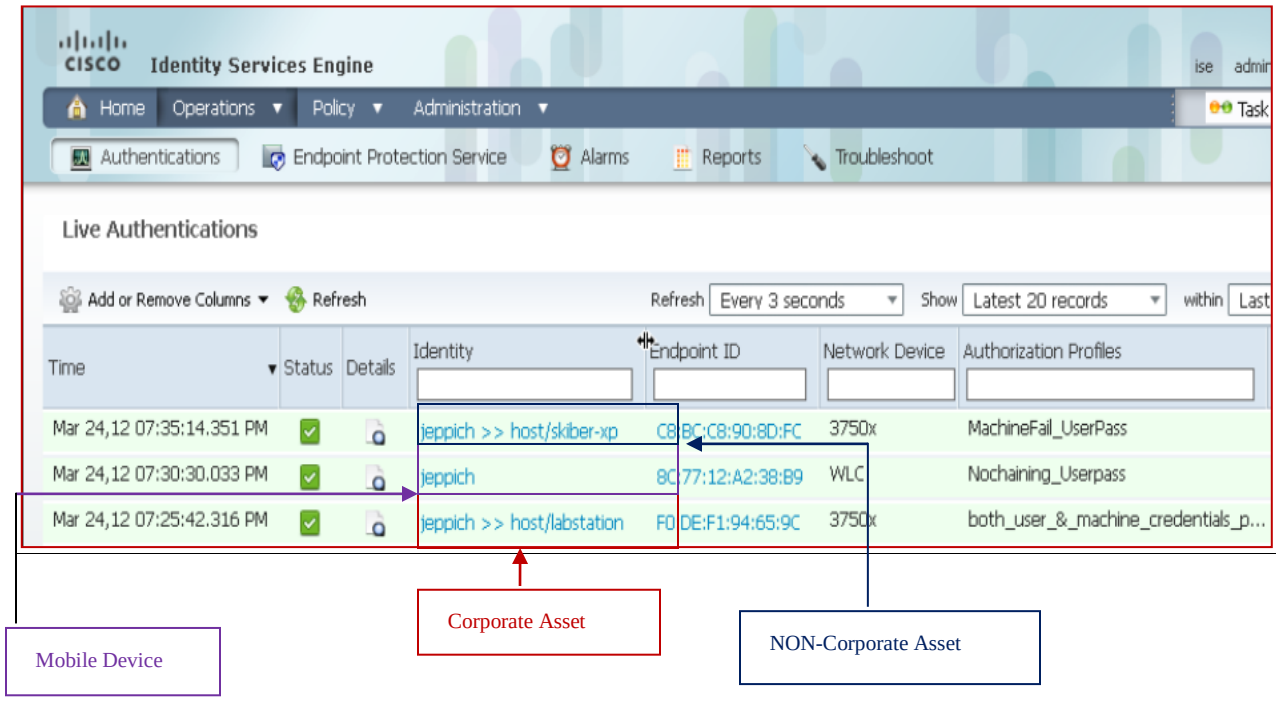
Detailed View of EAP Chaining

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.

Procedure 24 Access the Live Authentications menu

Step 1 Select Operations → Authentications

Figure 49 Live Authentications Log

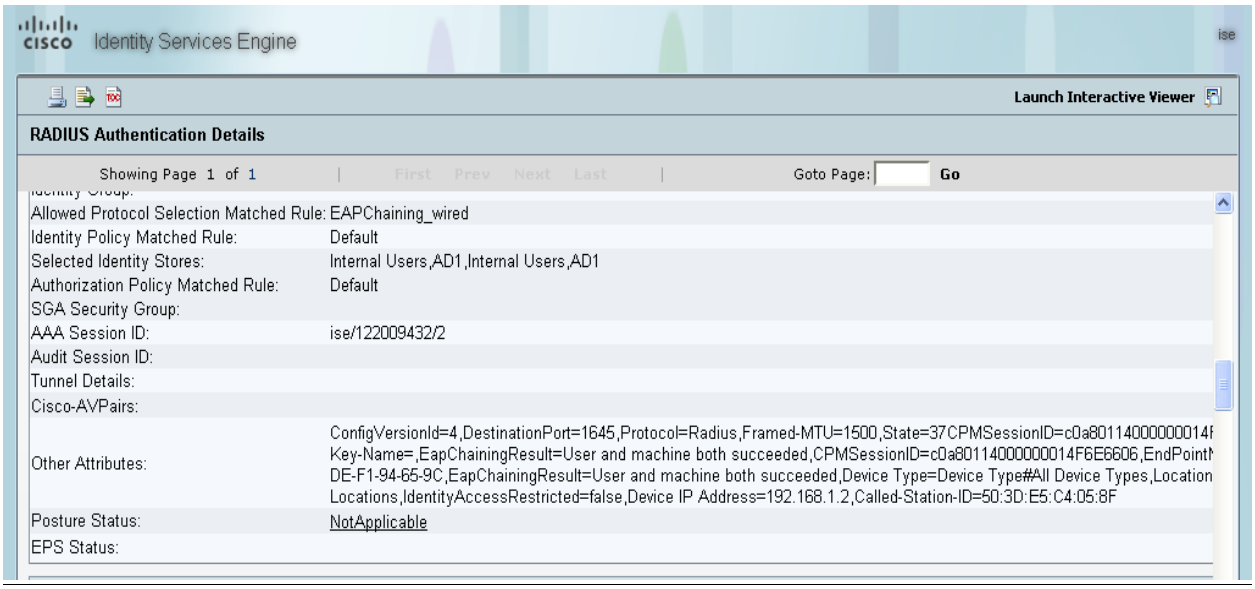


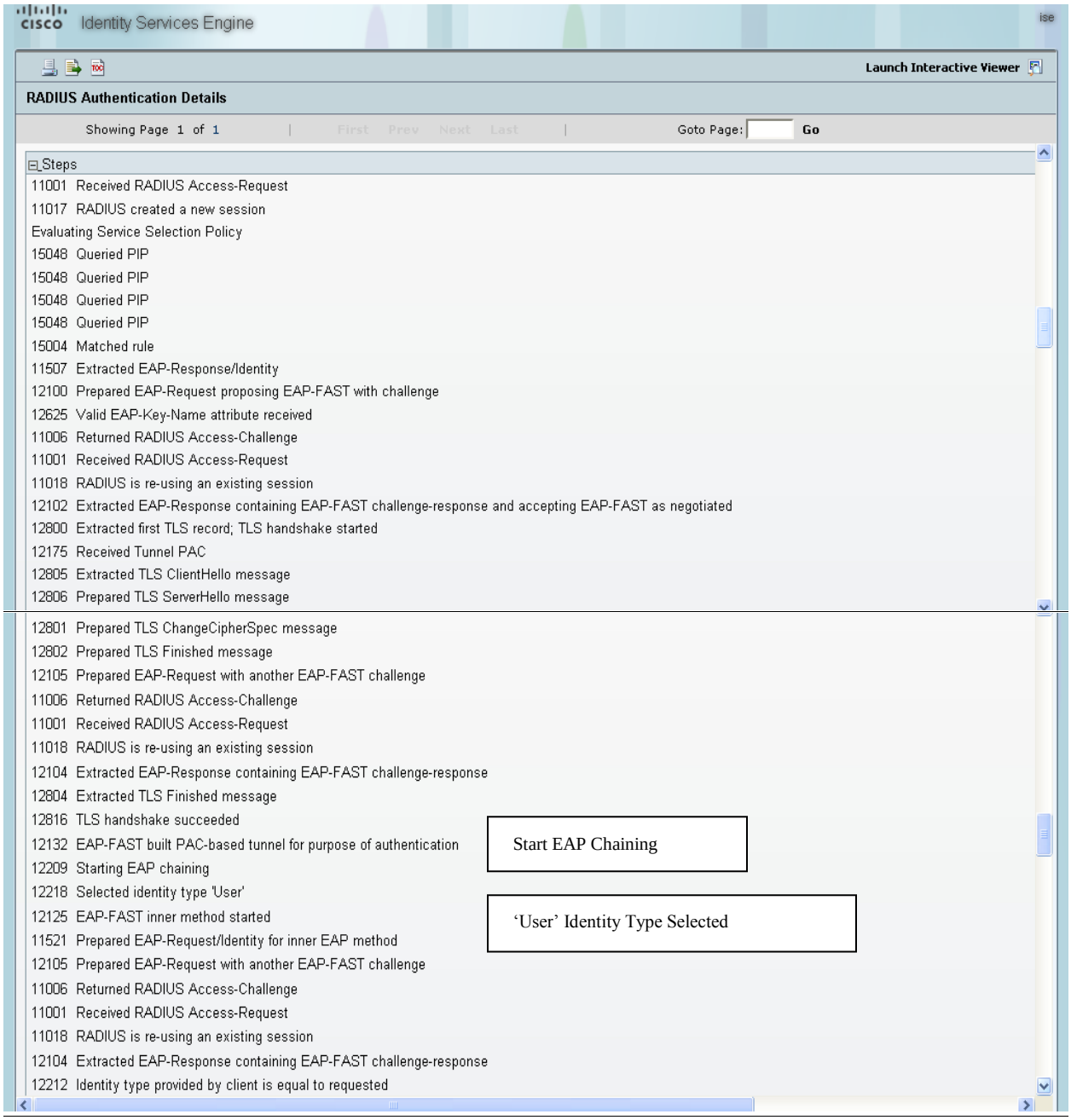
Procedure 25 Log Details of an End-User Logging in from a Corporate Device

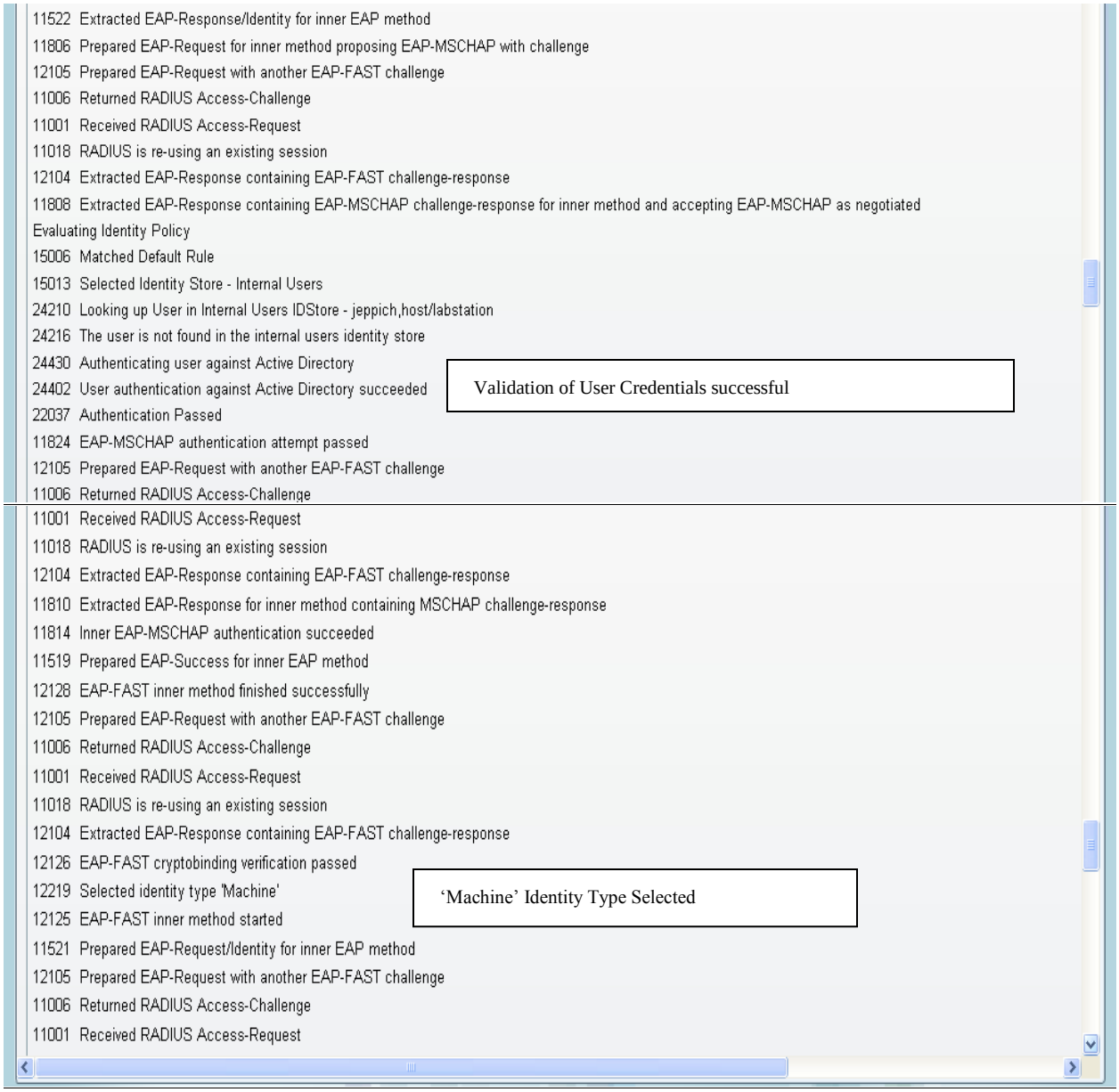
User Logging on from a Corporate laptop, both machine and user credentials successfully validated

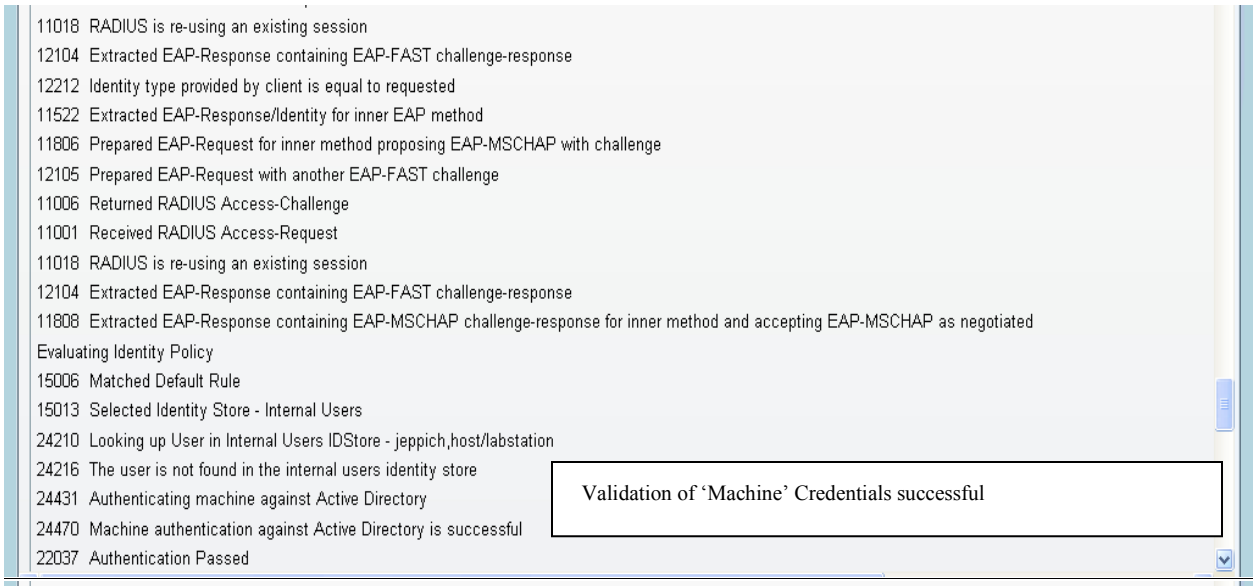
Machine and User credentials are tied to a corporate device. Both credentials are passed an EAP transaction. Below are the RADIUS Authentication Details and detailed EAP transaction logs of the authentication as illustrated in the figures below.

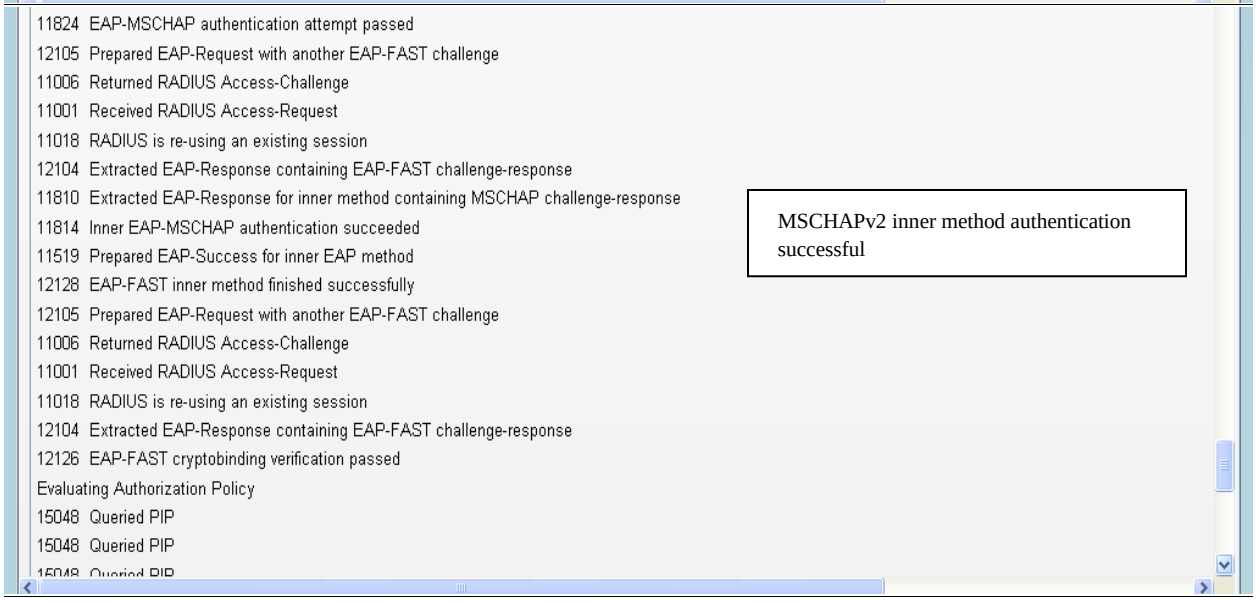
Figure 50 End-User placed in VLAN 1

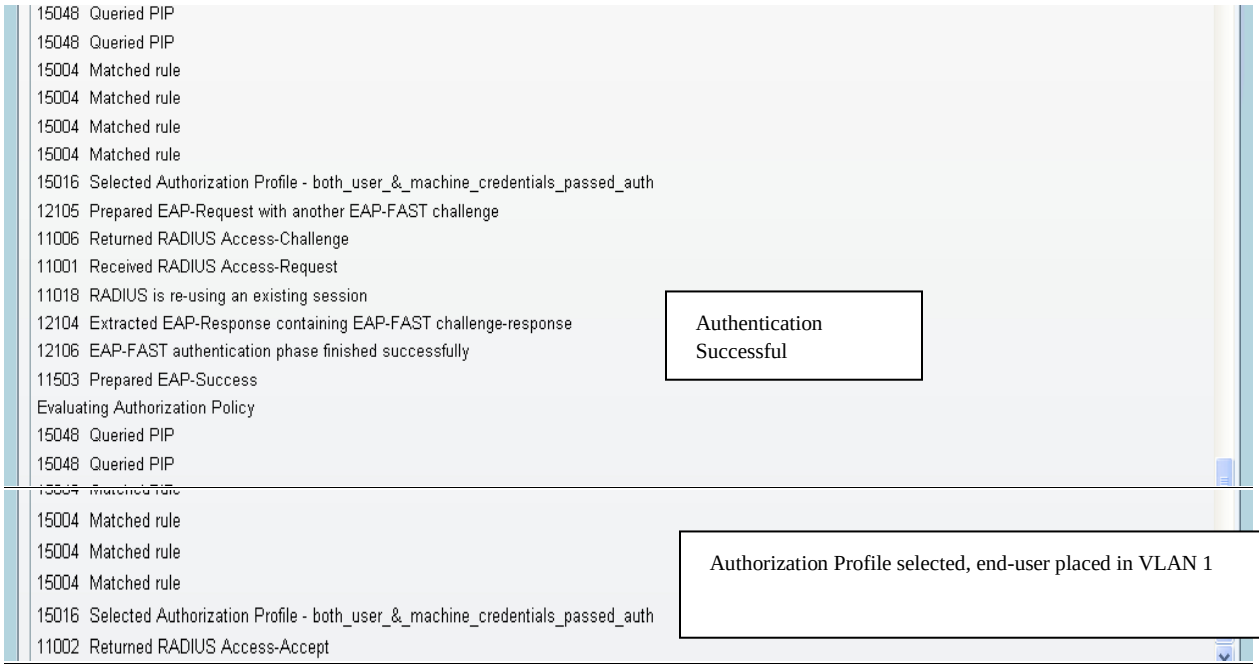

Identity Services Engine
ise
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1
First Prev Next Last
Goto Page:
Go
Allowed Protocol Selection Matched Rule: EAPChaining_wired
Identity Policy Matched Rule: Default
Selected Identity Stores: Internal Users,AD1,Internal Users,AD1
Authorization Policy Matched Rule: Default
SGA Security Group:
AAA Session ID: ise/122009432/2
Audit Session ID:
Tunnel Details:
Cisco-AVPairs:
Other Attributes: ConfigVersionId=4,DestinationPort=1645,Protocol=Radius,Framed-MTU=1500,State=37CPMSessionID=c0a80114000000014
Key-Name=,EapChainingResult=User and machine both succeeded,CPMSessionID=c0a80114000000014F6E6606,EndPoint
DE-F1-94-65-9C,EapChainingResult=User and machine both succeeded,Device Type=Device Type#All Device Types,Location
Locations,IdentityAccessRestricted=false,Device IP Address=192.168.1.2,Called-Station-ID=50:3D:E5:C4:05:8F
Posture Status: NotApplicable
EPS Status:


Identity Services Engine
ise
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1
First Prev Next Last
Goto Page:
Go
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
Start EAP Chaining
'User' Identity Type Selected


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/labstation
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
Validation of User Credentials successful
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'
'Machine' Identity Type Selected
12125 EAP-FAST inner method started
11521 Prepared EAP-Request/Identity for inner EAP method
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request

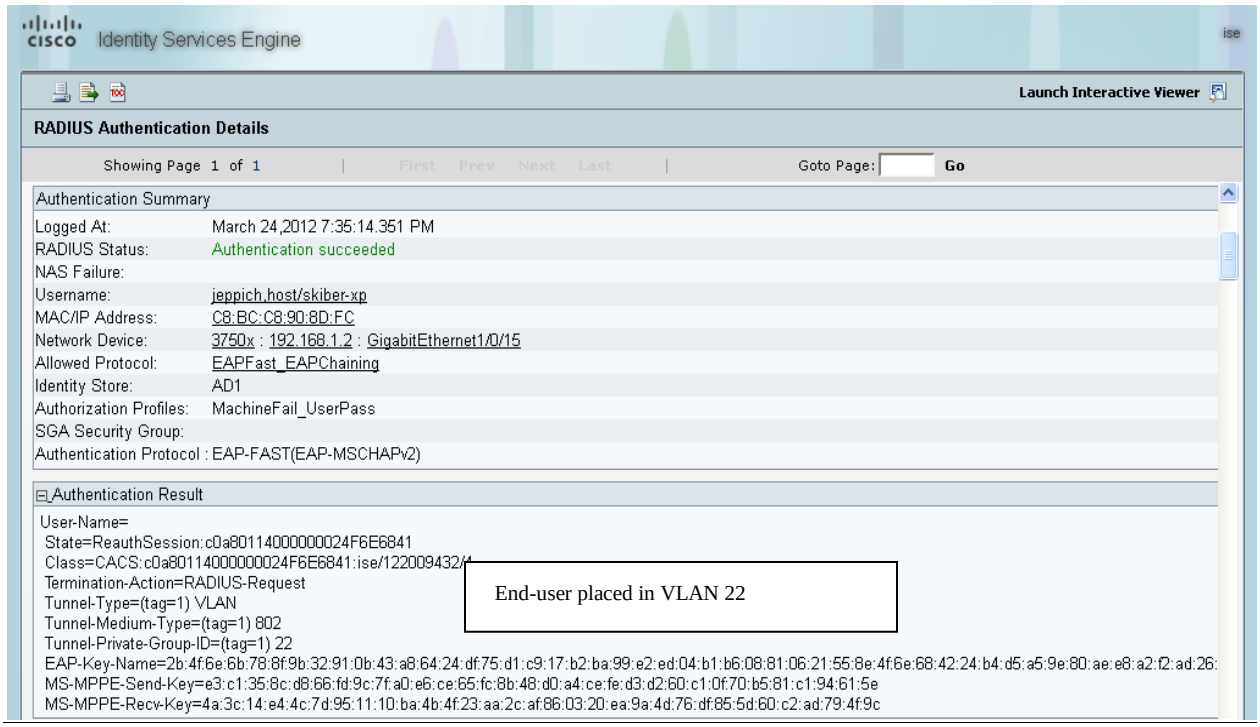

11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12212 Identity type provided by client is equal to requested
11522 Extracted EAP-Response/Identity for inner EAP method
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with 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/labstation
24216 The user is not found in the internal users identity store
24431 Authenticating machine against Active Directory
24470 Machine authentication against Active Directory is successful
22037 Authentication Passed
Validation of 'Machine' Credentials successful

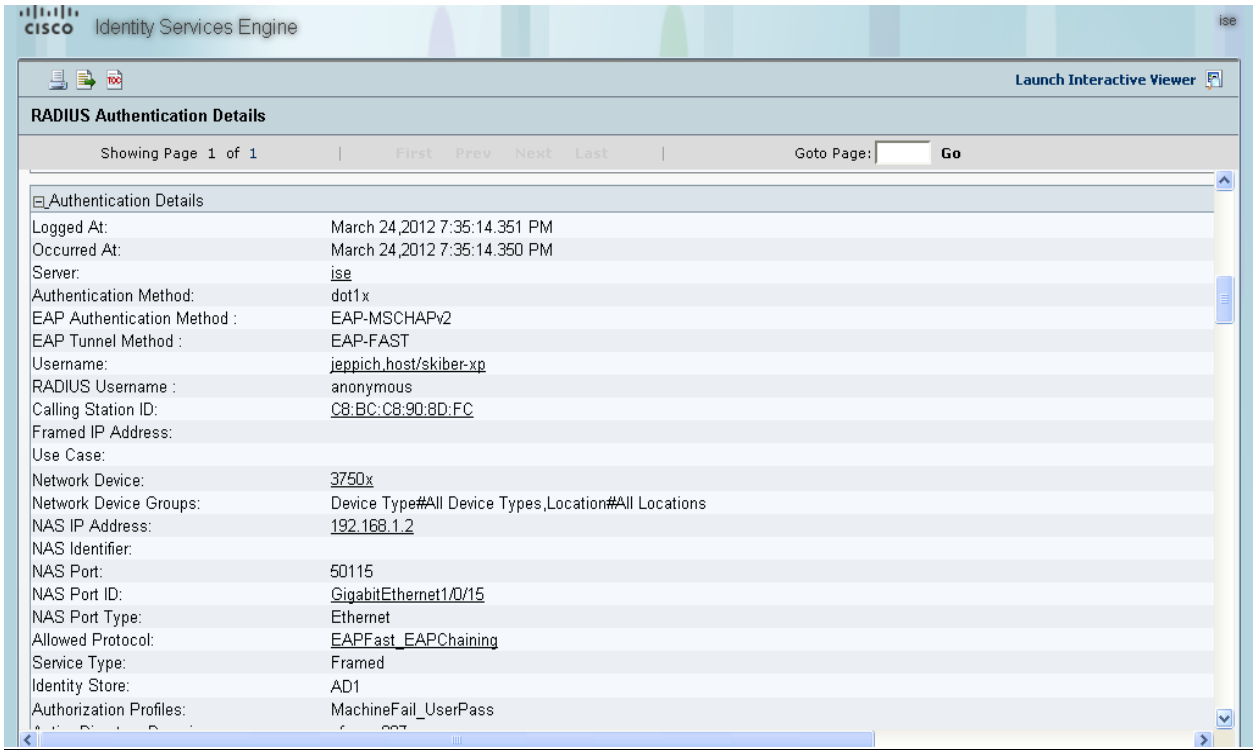

11824 EAP-MSCHAP authentication attempt passed
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
11810 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
Evaluating Authorization Policy
15048 Queried PIP
15048 Queried PIP
MSCHAPv2 inner method authentication successful

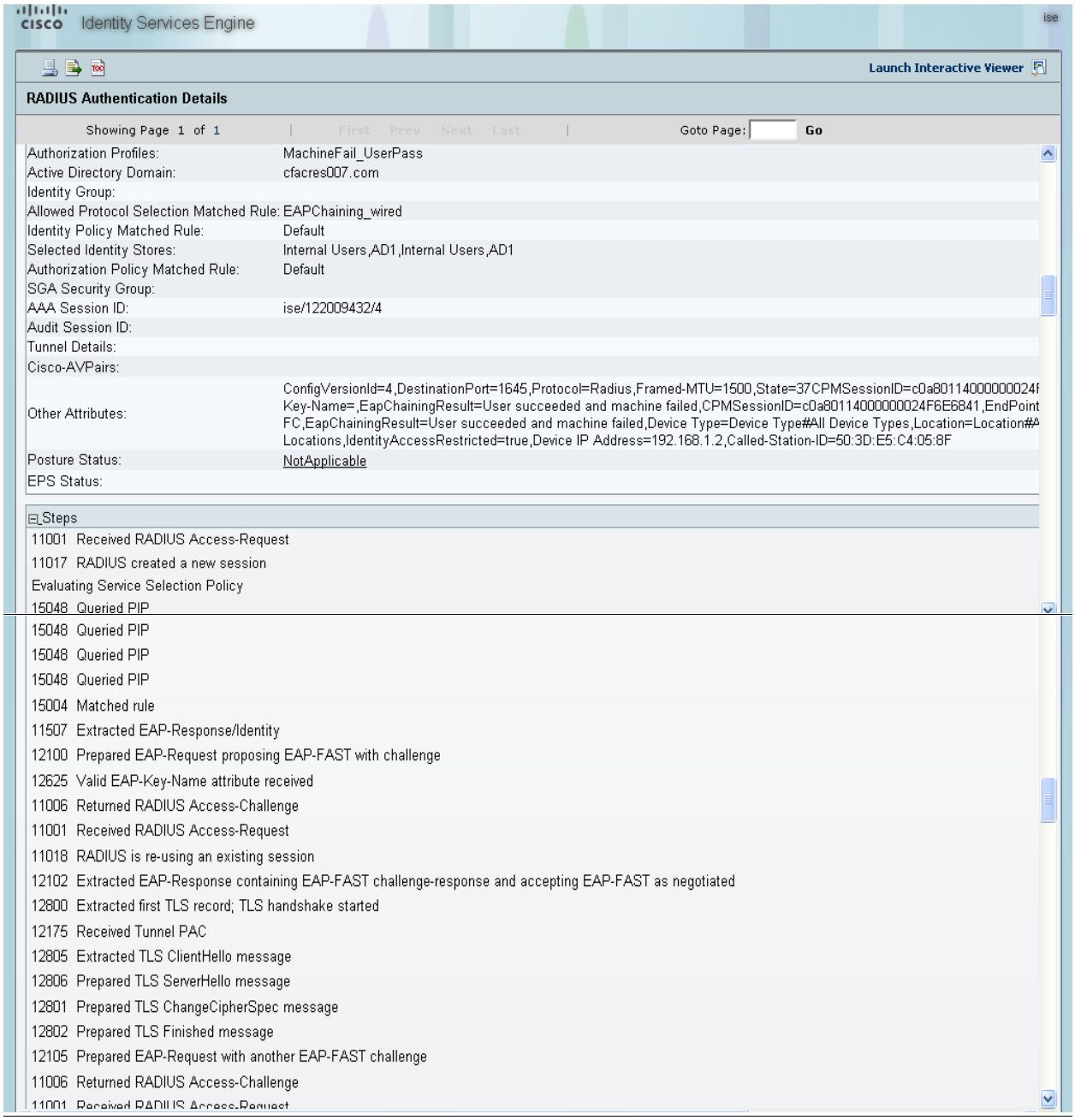

15048 Queried PIP
15048 Queried PIP
15004 Matched rule
15004 Matched rule
15004 Matched rule
15004 Matched rule
15016 Selected Authorization Profile - both_user_&_machine_credentials_passed_auth
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12106 EAP-FAST authentication phase finished successfully
11503 Prepared EAP-Success
Evaluating Authorization Policy
15048 Queried PIP
15048 Queried PIP
15004 Matched rule
15004 Matched rule
15004 Matched rule
15016 Selected Authorization Profile - both_user_&_machine_credentials_passed_auth
11002 Returned RADIUS Access-Accept
Authentication Successful
Authorization Profile selected, end-user placed in VLAN 1

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

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

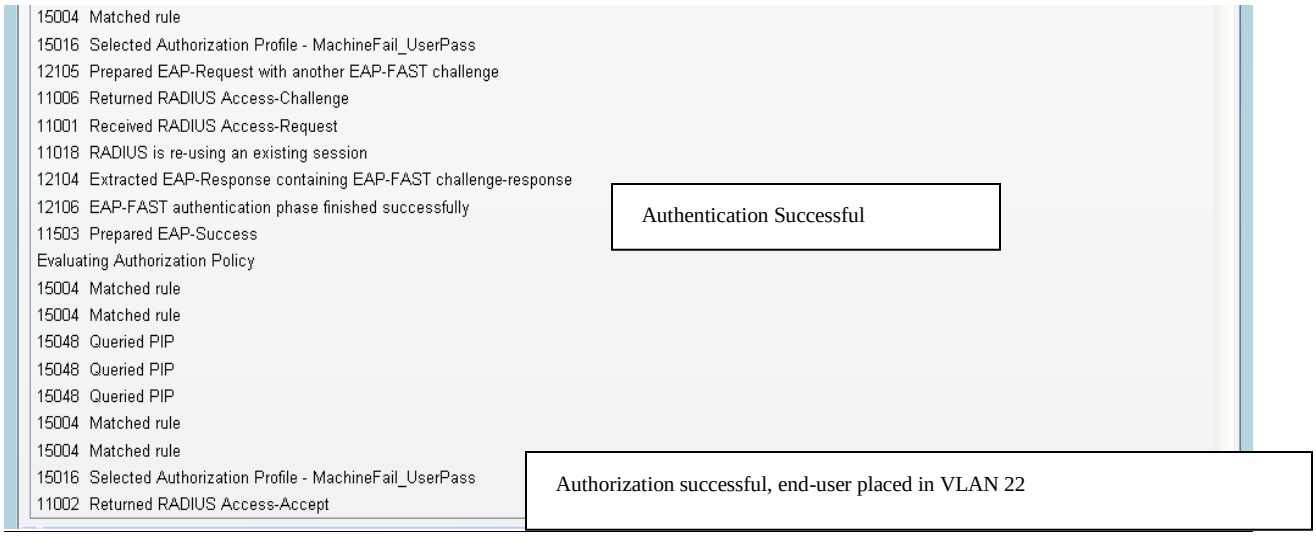





Identity Services Engine
ise
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1
First Prev Next Last
Goto Page: Go
Authorization Profiles: MachineFail_UserPass
Active Directory Domain: cfacres007.com
Identity Group:
Allowed Protocol Selection Matched Rule: EAPChaining_wired
Identity 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

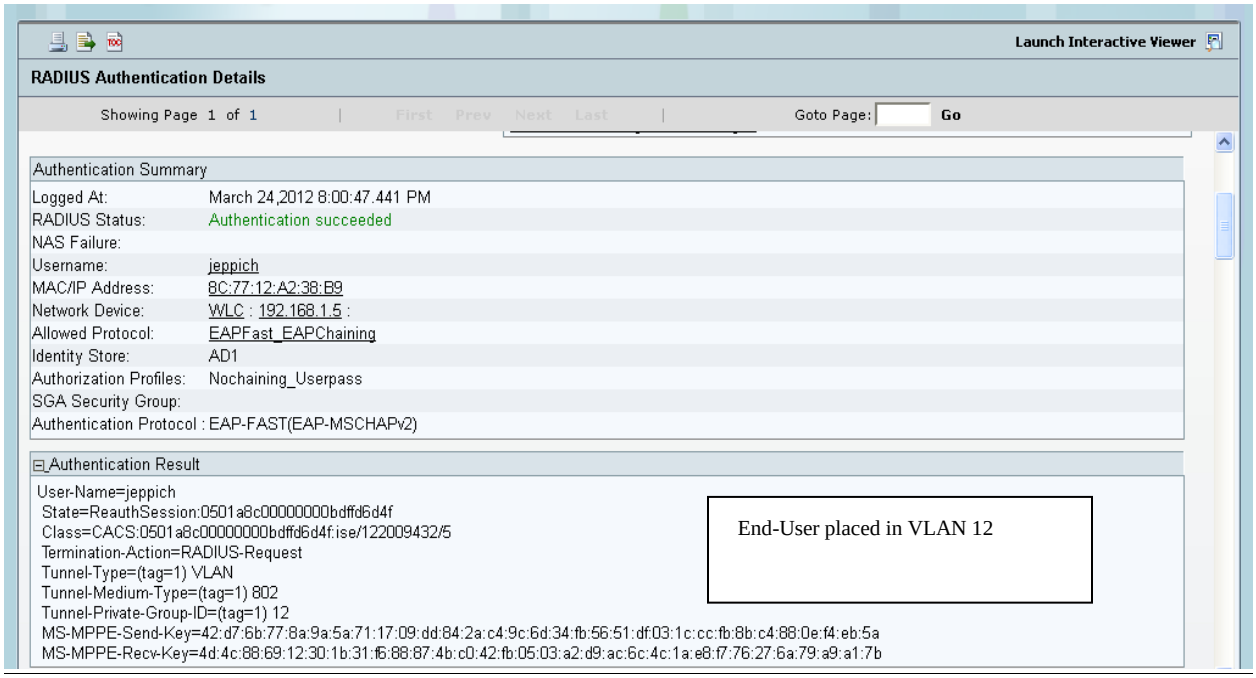

11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12804 Extracted TLS Finished message
12816 TLS handshake succeeded
12132 EAP-FAST built PAC-based tunnel for purpose of authentication
12209 Starting EAP chaining
12218 Selected identity type '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
Start EAP Chaining
'User' Identity Type Selected
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
Validating 'User ' Credentials
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
'Machine' Identity Type Selected

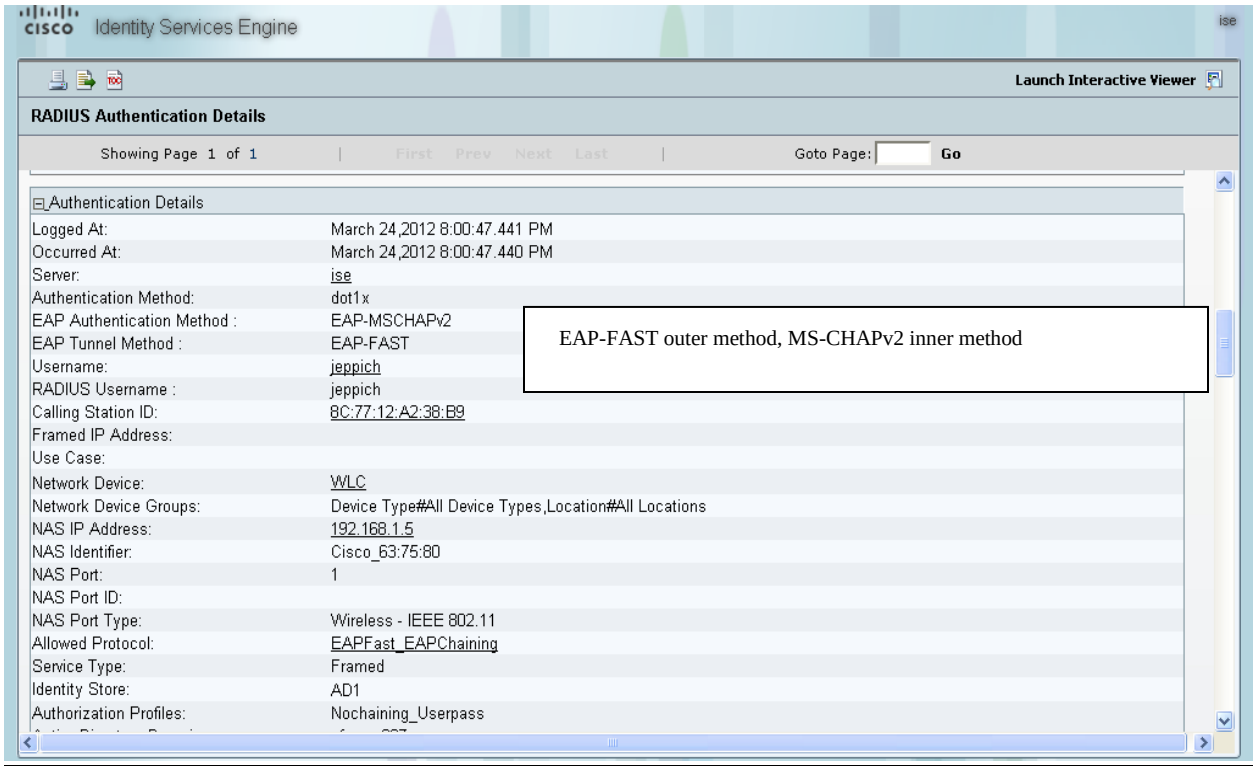

12212 Identity type provided by client is equal to requested
11522 Extracted EAP-Response/Identity for inner EAP method
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 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 disab
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
Failed 'Machine' Authentication, simulate personal laptop
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
Authorization Profile Selected 'Machine Fail_UserPass'
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

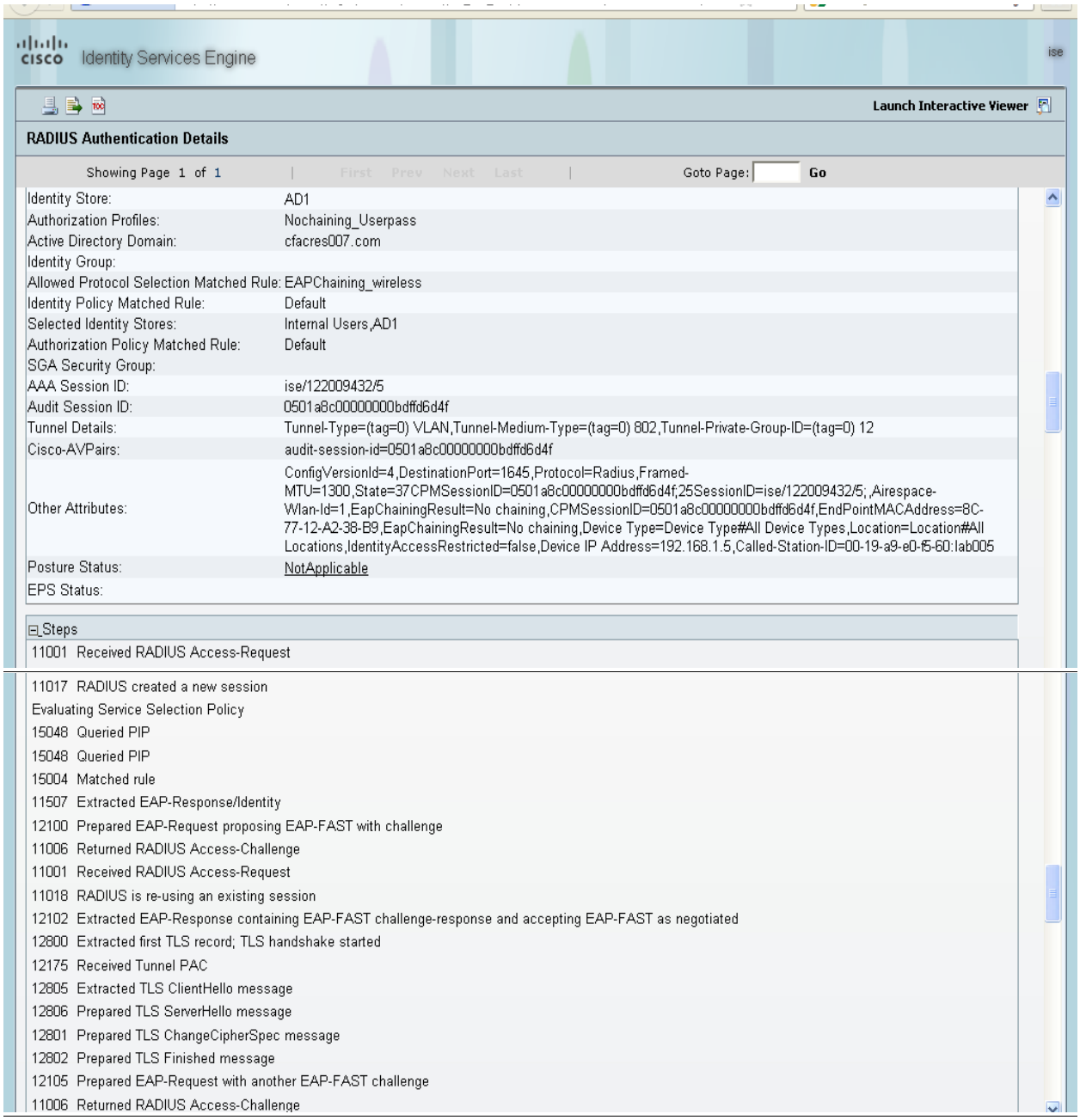


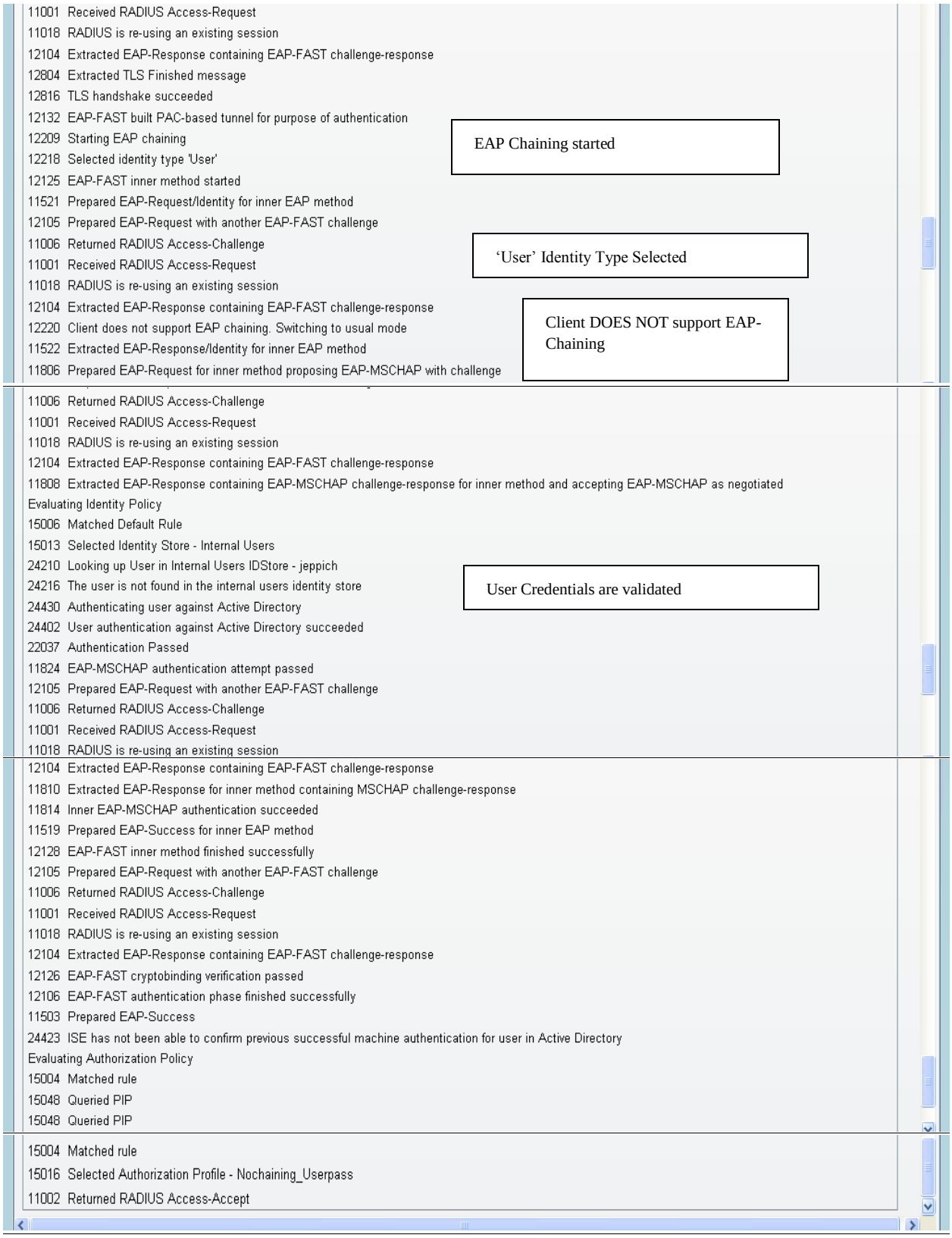
Procedure 27 Log Details of an End-User Logging in from a Mobile Device

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




Identity Services Engine
ise
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1
First Prev Next Last
Goto Page: Go
Authentication Details
Logged At: March 24,2012 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
EAP-FAST outer method, MS-CHAPv2 inner method


Identity Services Engine
ise
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1
First Prev Next Last
Goto Page: Go
Identity Store: AD1
Authorization Profiles: Nochaining_Userpass
Active Directory Domain: cfacres007.com
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
EAP Chaining started
'User' Identity Type Selected
Client DOES NOT support EAP-Chaining
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
Evaluating Identity Policy
15006 Matched Default Rule
15013 Selected Identity Store - Internal Users
24210 Looking up User in Internal Users IDStore - jeppich
24216 The user is not found in the internal users identity store
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
User Credentials are validated
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.html