



MANNAI TRADING CO. WLL

Member of Mannai Corporation QPSC

Identity Service Engine

Use Case

Password + Smart Card Authentication with Cisco AnyConnect NAM

Submitted By

**MANNAI TRADING CO WLL
(Networking & ELV Division)**

MANNAI NETWORKING & ELV



1. OVERVIEW

1.1 Document Purpose

The purpose of this document is to demonstrate how ISE authenticate / authorize a user who uses a smartcard (PIN + Certificate) and password mechanism to login their system. This document describes the components used for this setup, configuration of ISE, settings of Cisco AnyConnect configuration.xml. The flow includes these steps:

- Domain users which is a part of AD group login to a domain machine with username and password. The protocols that supports authentication is EAP-FAST and MSCHAP-V2. ISE will validate the credentials against AD.
- Domain users which is a part of AD group login to a domain machine with smart card PIN. The protocols that supports authentication is EAP-FAST and EAP-TLS. PIN and certificate will be validated against two factor mechanism.
- Users will have a customized configuration.xml file which contains 2 profile that supports both password and smartcard authentication.
- ISE to be configured with protocols, identity source sequence (certificate and AD), authentication / authorization policies.

1.2 Components Used

Below are the list of devices that are used in this setup. ISE version compatibility needs to be validated before the setup.

- Cisco ISE 2.7
- NAD - Cisco 3850 switch
- Cisco AnyConnect NAM 4.9
- Certificate Authority (CA)
- Active Directory
- Endpoint: Microsoft Windows 10
- Gemalto 2FA

2. IDENTITY SERVICE ENGINE

2.1 ISE Overview

Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches.

- Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance.
- Provides for comprehensive guest access management for the Cisco ISE administrator, sanctioned sponsor administrators, or both.
- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing device posture for all endpoints that access the network, including 802.1X environment
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network.
- Enables consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed.
- Supports scalability to support a number of deployment scenarios from small office to large enterprise environment.

2.2 ISE Node, Roles and Personas

The persona or personas of a node determines the services provided by a node. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring. Below topic describes the personas of ISE.

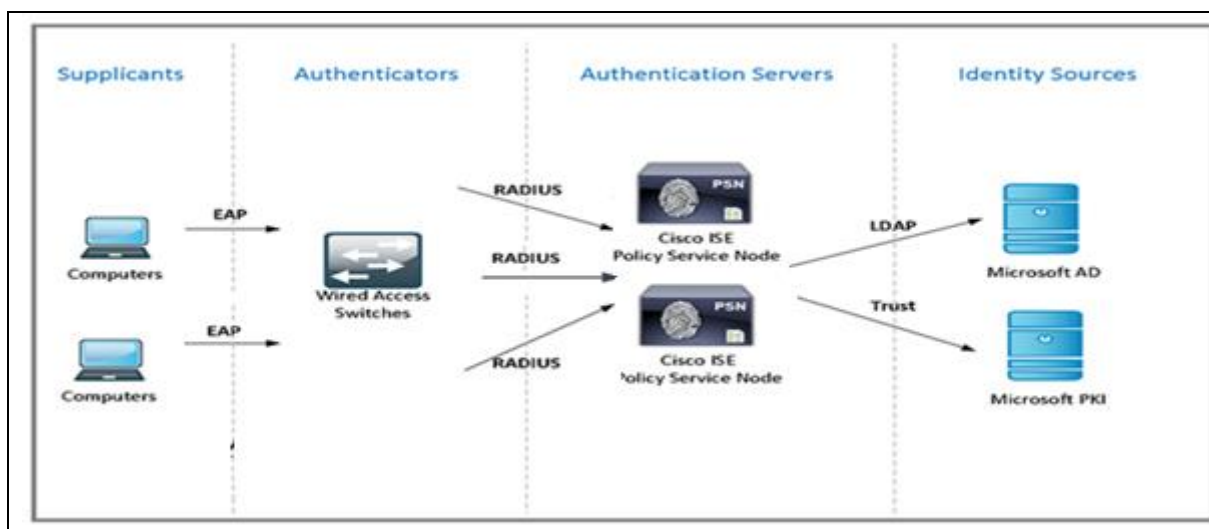
- Administration
- Monitoring
- Policy Service

3. NETWORK ARCHITECTURE

3.1 Network Infrastructure

Most ISE deployments are dependent on the existing infrastructure, as they need to be integrated into it. Hence, it is very important to verify that the network components, software versions and configurations meet the ISE requirements. The following are the dependencies that exist in the network infrastructure: Each network access devices should be configured with the ISE as RADIUS server for authentication and authorization

- Access switches



3.1.1 Supplicant

The supplicant is a piece of software on the device (workstation, laptop, etc.) that requests access to the switch or wireless services, and responds to requests from the authenticator (switch or WLC). The device must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows operating system. The client is the supplicant in the IEEE 802.1x specification.

3.1.2 Authenticator

The authenticator is a device such as a Catalyst switch that controls physical access to the network based on the authentication status of the client. The authenticator usually acts as an intermediary (proxy) between the client and the authentication server.

The authenticator requests identity information from the client via EAP, verifies that information with the authentication server via RADIUS, and then relays a response to the client based on the response from the authentication server.

When the switch receives EAP over LAN (EAPOL) frames and relays them to the authentication server, the Ethernet header and EAP frame are re-encapsulated into the RADIUS format.

3.1.3 Authentication Server

The authentication server performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the Switch whether or not the client is authorized to access the Switch. Because the switch acts as the proxy, the authentication server is transparent to the client. The RADIUS security system with EAP extensions is the only supported authentication server.

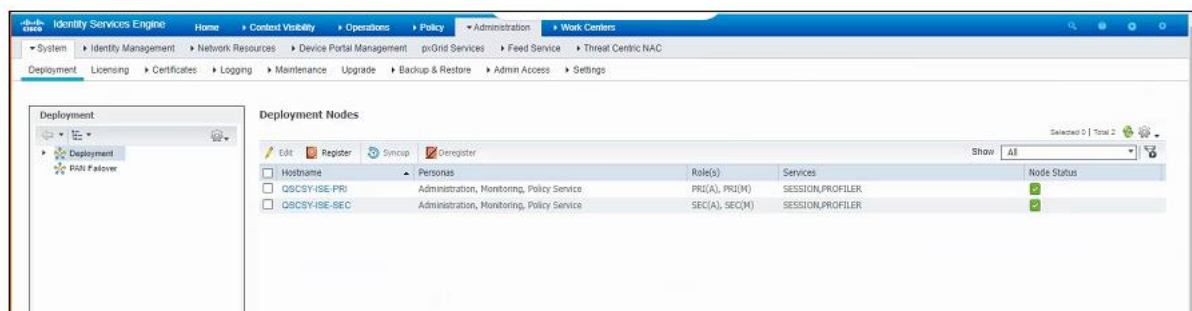
RADIUS uses a client-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

4. ISE Configuration

4.1 ISE Deployment

By default, an ISE appliance is configured in standalone mode. High availability can be configured between two ISE systems to provide fault tolerance.

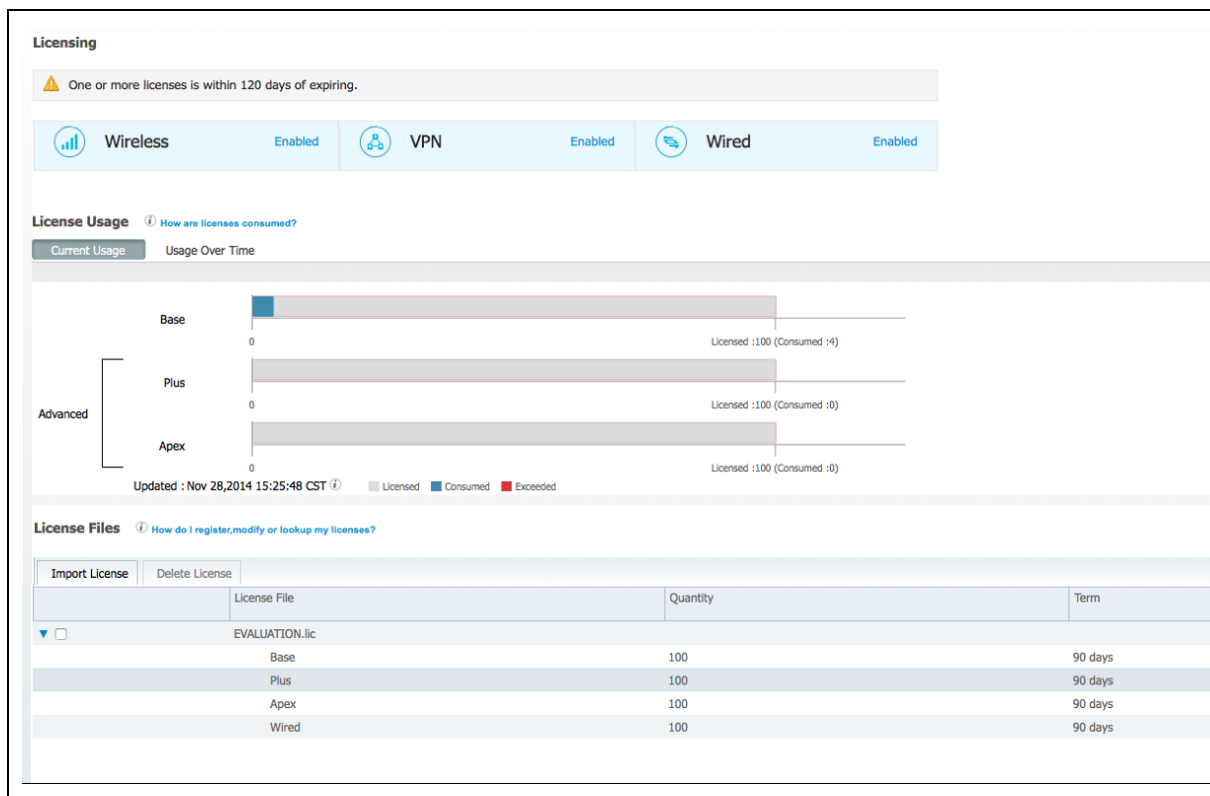
For this setup, two ISE nodes are configured as administration, monitoring and policy service enabled. In future Additional nodes can be registered by clicking Navigate to **Administration->Deployment** and then **Register** menu on primary node and then selecting the **Register** an ISE node. Before registering an ISE node, we need to have the DNS entry of the ISE nodes so that FQDN should be resolved.



4.2 ISE Licensing

Base license is required in ISE to execute this test. To install the license,

1. Navigate to Administration->Licensing
2. Import License.

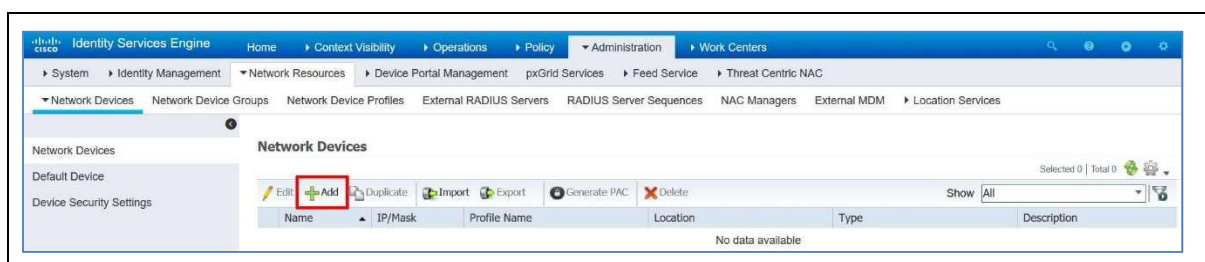


4.3 Add Switch to ISE as NAD

Network devices or NAD are devices in which endpoints directly connect to. These devices can be switches, access points etc. This POC will use switches for NADs. Below is a list of NADs and their information.

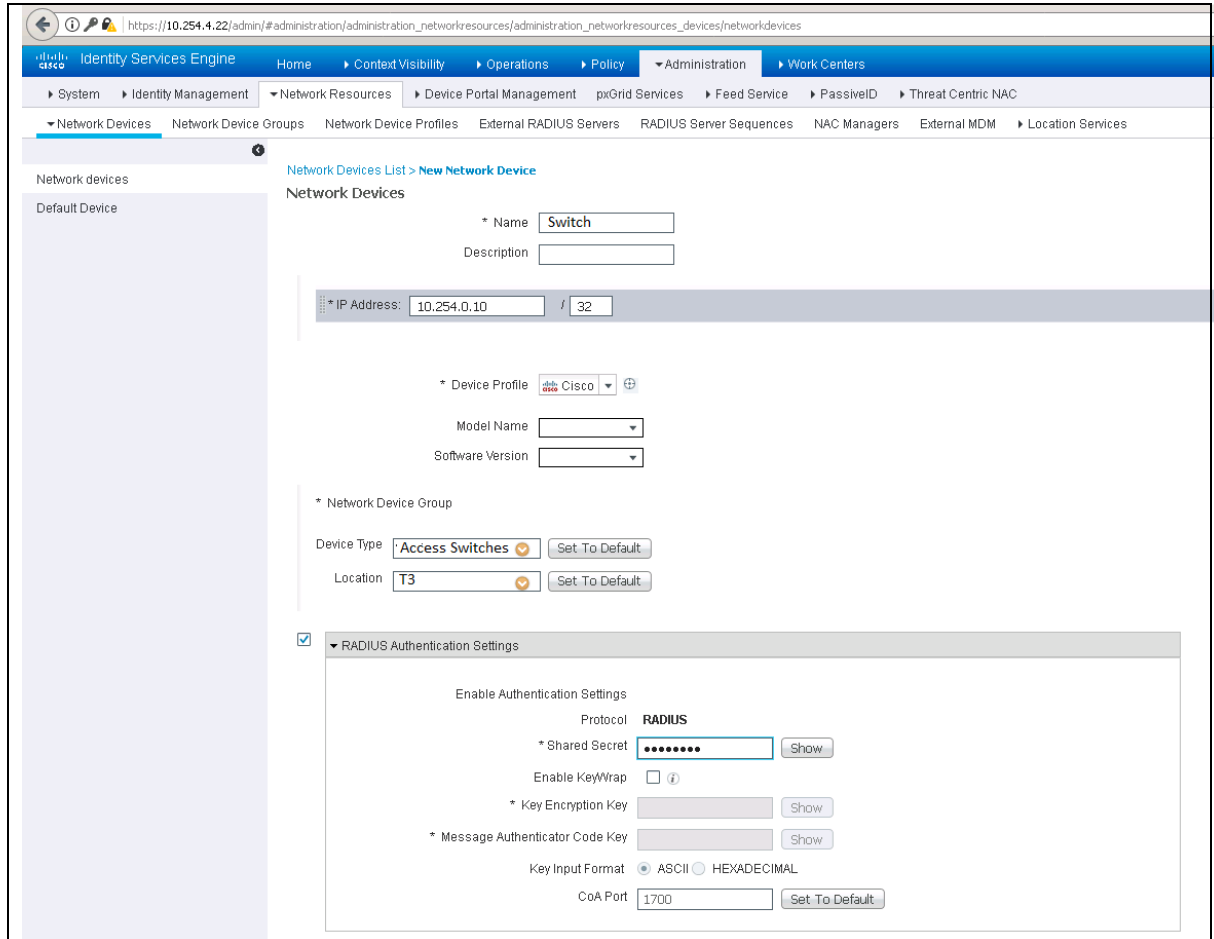
ISE offers the functionality to create Network Device Groups that allow a structured way to group the different NADs. Follow these steps to add two NADs to our ISE configuration:

1. Log in to ISE GUI by browsing to <http://<ISE PAN>>
2. Browse to Administration->Network Resources->Network Devices. In the Network Devices page, click the + Add button to add a network device:



3. Add the network devices for your switch with the Name, IP and Network Device groups. Location as shown in the following screenshot:

4. Enable RADIUS and on this NAD and set the shared secret for RADIUS to ISE.
5. Click Submit to save the Switch NAD configuration.



The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a Network Device. The page is titled "Network Devices List > New Network Device". The form includes the following fields and sections:

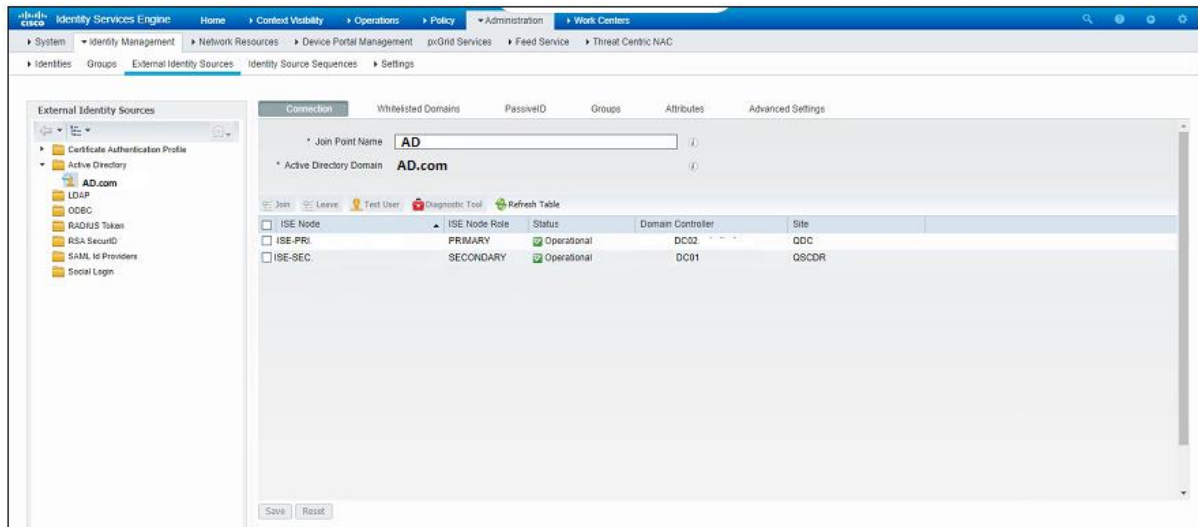
- Name:** Switch
- Description:** (empty)
- * IP Address:** 10.254.0.10 / 32
- * Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- * Network Device Group:** (empty)
- Device Type:** Access Switches (Set To Default)
- Location:** T3 (Set To Default)
- RADIUS Authentication Settings:**
 - Enable Authentication Settings:** (checked)
 - Protocol:** RADIUS
 - * Shared Secret:** (masked with dots) (Show)
 - Enable KeyWrap:** (unchecked)
 - * Key Encryption Key:** (masked with dots) (Show)
 - * Message Authenticator Code Key:** (masked with dots) (Show)
 - Key Input Format:** ASCII (selected), HEXADECIMAL
 - CoA Port:** 1700 (Set To Default)

4.4 Active Directory Integration

The Cisco Identity Services Engine (Cisco ISE) integrates with external identity sources to validate credentials in user authentication functions, and to retrieve group information and other attributes that are associated with the user for use in authorization policies. For Network Administration access, authentications will be validated against the Active Directory domain.

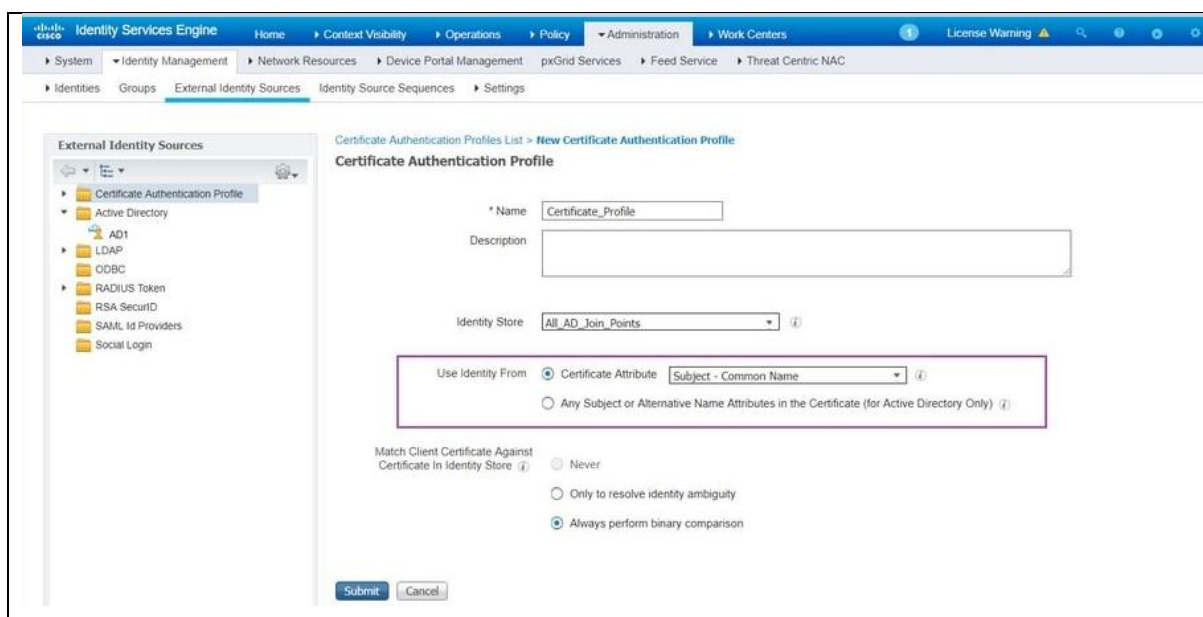
Joining Active Directory is configured on

1. Select **Administration->Identity Management->External Identity Sources->Active Directory->Connection** screen.
2. Click the join button and provide the service account information.
3. The screen shot below shows the Leave button because the screenshot was taken after the system joined Active Directory.



4.5 Certificate Authentication Profile

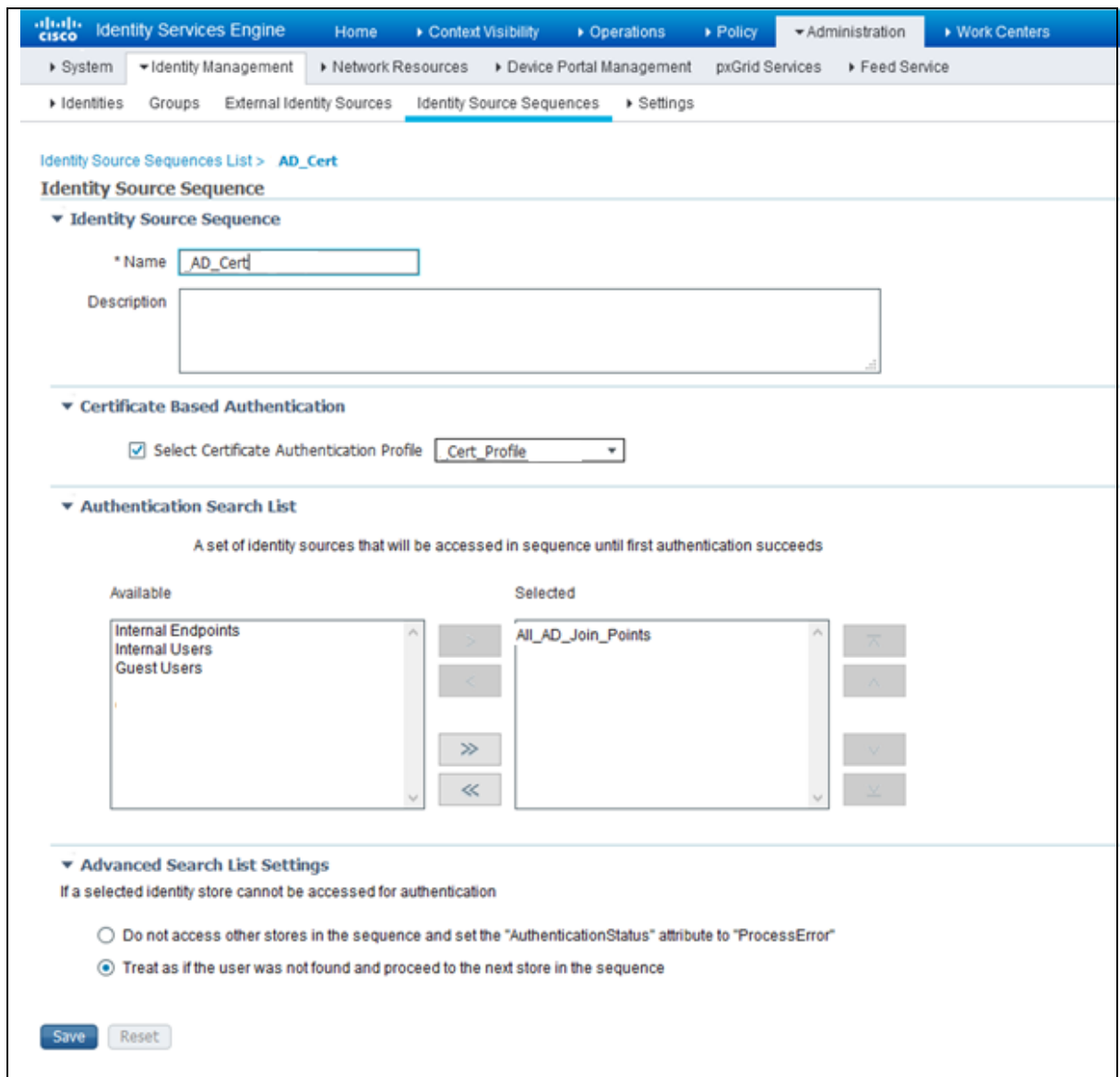
The purpose of the Certificate Authentication Profile is to inform ISE which certificate field the identity (machine or user) can be found on the client certificate (end-identity certificate) presented to ISE during EAP-TLS (also during other certificate-based authentication methods). These settings will be bound to the Authentication Policy to authenticate the identity; configured from ISE GUI, navigate to **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** and click on **Add**.



4.6 Identity Source Sequence

Identity Source Sequence can be created from ISE GUI, navigate to **Administration > Identity Management**, Under **Identity Source Sequences** and click on **Add**.

The next step is to add the Certificate Authentication Profile to an Identity Source Sequence which grants the ability to include multiple Active Directory (AD) join points or group a combination of internal/external identity sources together, as desired, which then binds to the Authentication Policy under the **Use** column.



Identity Source Sequence

Identity Source Sequence

* Name

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	>	All_AD_Join_Points
Internal Users	<	
Guest Users	>>	
	<<	

▼ Advanced Search List Settings

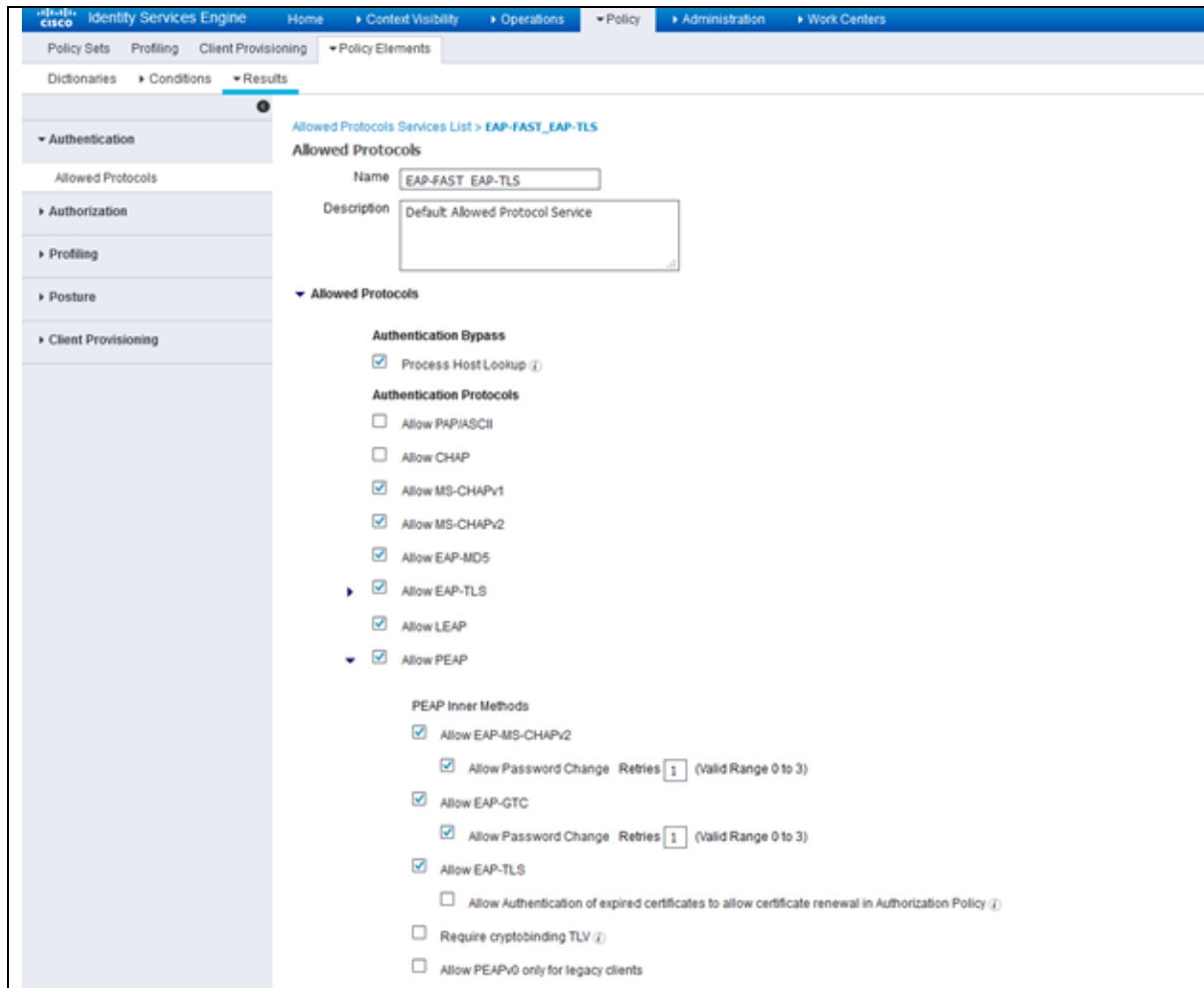
If a selected identity store cannot be accessed for authentication

☐ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

☒ Treat as if the user was not found and proceed to the next store in the sequence

4.7 Define the Allowed Protocols Service.

The Allowed Protocols Service enables only that authentication methods/protocols which ISE supports during Radius Authentication. In order to configure from ISE GUI, navigate to **Policy > Policy Elements: Results > Authentication > Allowed Protocols** and then it binds as an element to the Authentication Policy.



Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services List > EAP-FAST_EAP-TLS

Allowed Protocols

Name: EAP-FAST EAP-TLS

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

☒ Process Host Lookup ⓘ

Authentication Protocols

☐ Allow PAPI/ASCII

☐ Allow CHAP

☒ Allow MS-CHAPv1

☒ Allow MS-CHAPv2

☒ Allow EAP-MD5

☒ 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: 1 (Valid Range 0 to 3)

☒ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

☐ Require cryptobinding TLV ⓘ

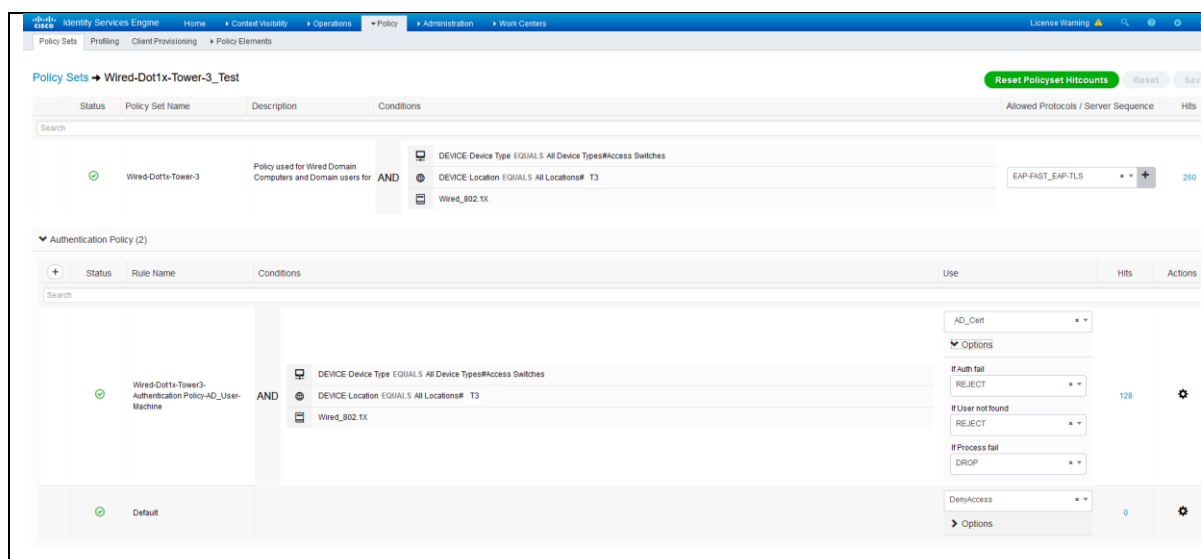
☐ Allow PEAPv0 only for legacy clients

4.8 ISE Policies

4.8.1 ISE Authentication Policy

Authentication policies define the protocols that Cisco ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. A policy is a set of conditions and a result. A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or operator.

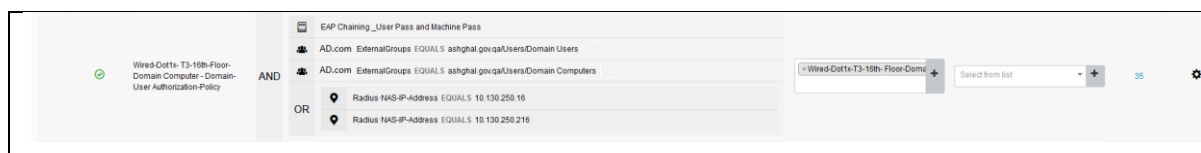
1. Enter a name for your authentication rule. This example uses **Wired 802.1x** which already exists by default on ISE.
2. Select the plus (+) icon in the condition field.
3. From the Conditions Studio drag **Wired_802.1x** in the Editor window and add **Device type** and **Device location** and click **Save**.
4. Use the Identity source sequence created before.
5. Click Options and Choose **Reject** from the If user not found a drop-down list.



4.8.2 ISE Authorization Policy

Authorization policies are a component of the Cisco ISE network authorization service that allows for defining authorization policies and configuring authorization profiles for specific users and groups of users that will access network resources.

1. Create a new rule, and enter a name.
2. From the Conditions Studio drag **EAPChaining_UserPass** and **MachinePass** and from AD external groups select domain computer and domain use and Save.
3. On the General Authorization page, choose respective authorization Profile under Results.

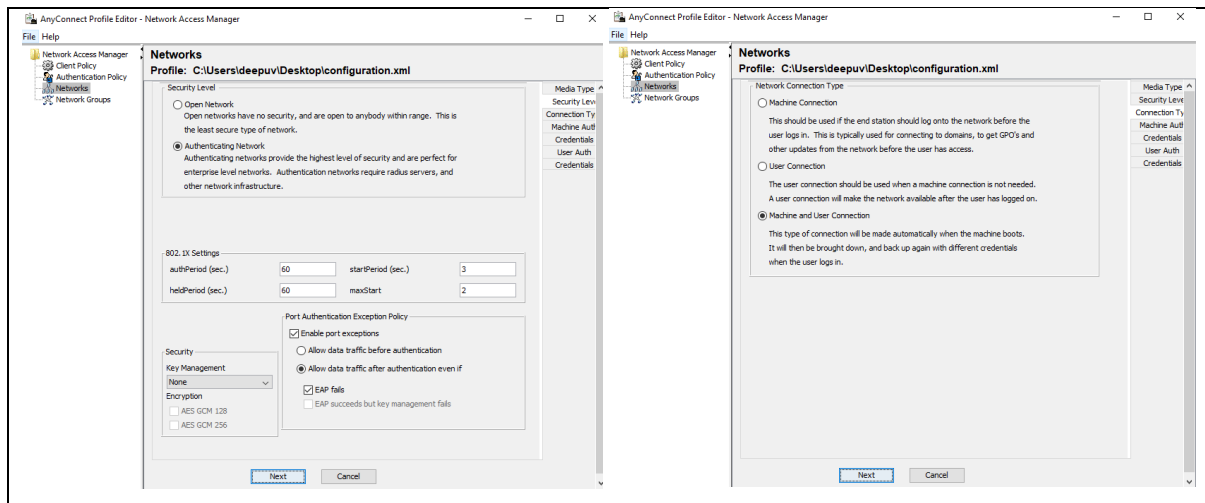
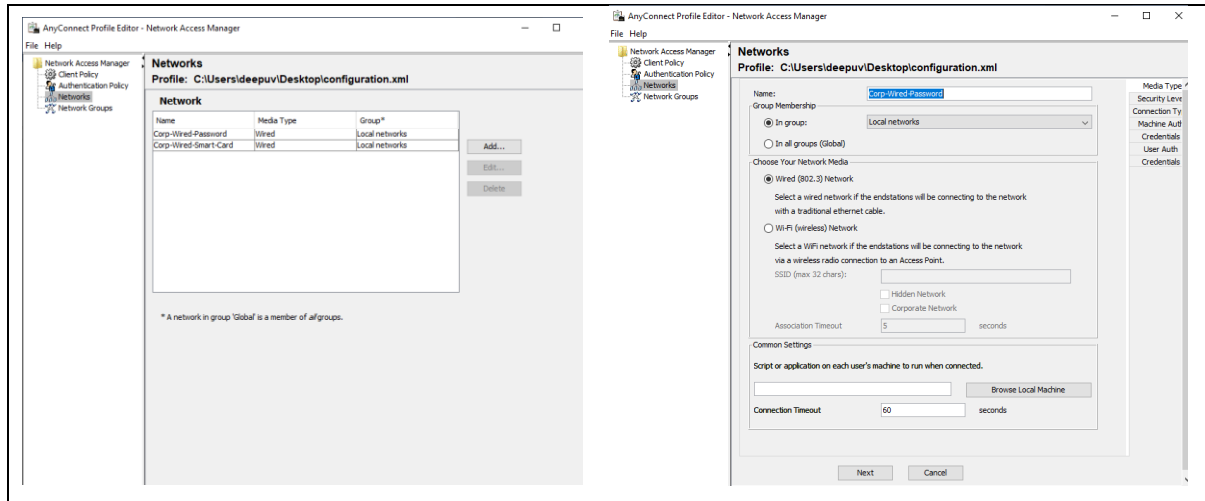


4. Create an authorization policy for domain computers.



5. AnyConnect XML Configuration

Below snaps shots shows the supported configuration.xml created from a Cisco AnyConnect profile editor shows a password-based authentication for user and machine. EAP-FAST is the EAP method and MSCHAPV2 is the inner method based on credential source used for this method.



AnyConnect Profile Editor - Network Access Manager

File Help

Network Access Manager

Client Policy

Authentication Policy

Networks

Network Groups

Networks

Profile: C:\Users\deepuv\Desktop\configuration.xml

EAP Methods

☐ EAP-MD5
☐ EAP-TLS
☐ EAP-MSCHAPv2
☐ 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
☐ 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

Media Type

Security Level

Connection Ty

Machine Aut

Credentials

User Auth

Credentials

Next Cancel

AnyConnect Profile Editor - Network Access Manager

File Help

Network Access Manager

Client Policy

Authentication Policy

Networks

Network Groups

Networks

Profile: C:\Users\deepuv\Desktop\configuration.xml

Machine Identity

Unprotected Identity Pattern: host/anonymous

Protected Identity Pattern: host/{username}

Machine Credentials

☒ Use Machine Credentials
☐ Use Static Credentials

Password:

Media Type

Security Level

Connection Ty

Machine Aut

Credentials

User Auth

Credentials

Next Cancel

AnyConnect Profile Editor - Network Access Manager

File Help

Network Access Manager

Client Policy

Authentication Policy

Networks

Network Groups

Networks

Profile: C:\Users\deepuv\Desktop\configuration.xml

EAP Methods

☐ EAP-MD5
☐ EAP-TLS
☐ EAP-MSCHAPv2
☐ EAP-TTLS
☐ PEAP
☒ EAP-FAST

EAP-FAST Settings

☐ Extend user connection beyond log off
☐ Validate Server Identity
☐ Enable Fast Reconnect
☐ Disable when using a Smart Card

Inner Methods based on Credentials Source

☒ Authenticate using a Password
☐ EAP-MSCHAPv2
☐ 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

Media Type

Security Level

Connection Ty

Machine Aut

Credentials

User Auth

Credentials

Next Cancel

AnyConnect Profile Editor - Network Access Manager

File Help

Network Access Manager

Client Policy

Authentication Policy

Networks

Network Groups

Networks

Profile: C:\Users\deepuv\Desktop\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:

Media Type

Security Level

Connection Ty

Machine Aut

Credentials

User Auth

Credentials

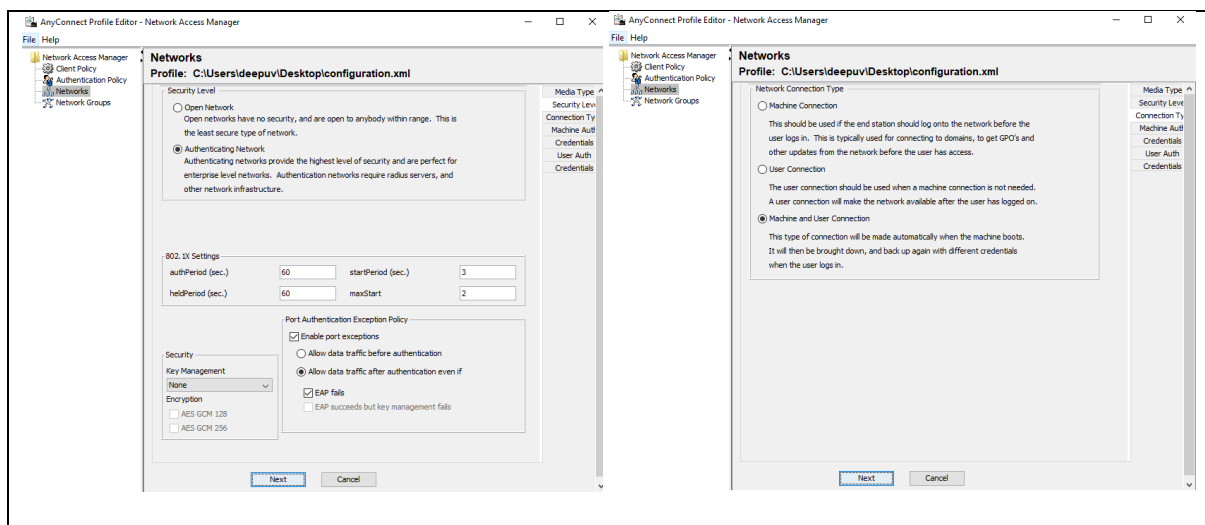
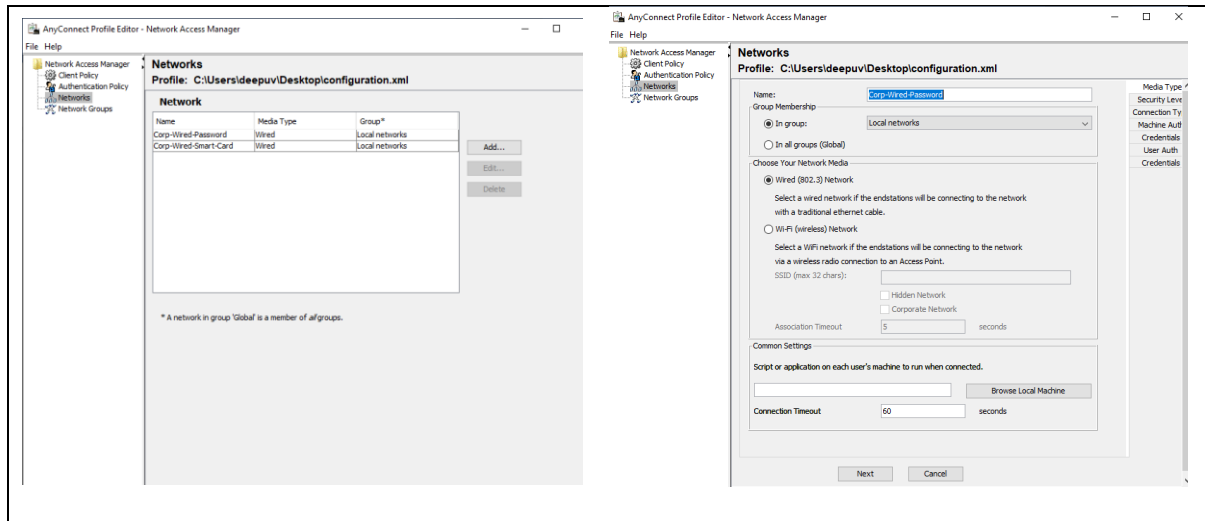
Done Cancel

Page | 14

ISE for Multi Authentication

Confidential

Below snaps shots shows the supported configuration.xml created from a Cisco AnyConnect profile editor shows a smart card (PIN+ Certificate) based authentication for user and machine. EAP-FAST is the EAP method and EAP-TLS is to authenticate using certificate as inner method based on credential source used for this method.



AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Networks
Profile: C:\Users\deepuv\Desktop\configuration.xml

EAP Methods
EAP-MSD
EAP-MSCHAPv2
EAP-GTC
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
Media Type
Security Level
Connection Ty
Machine Aut
Credentia
User Auth
Credentia

EAP-FAST Settings
Validate Server Identity
Enable Fast Reconnect

Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
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
Next
Cancel

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Networks
Profile: C:\Users\deepuv\Desktop\configuration.xml

Machine Identity
Unprotected Identity Pattern: host/anonymous
Protected Identity Pattern: host/[username]
Machine Credentials
Use Machine Credentials
Use Static Credentials
Password:
Media Type
Security Level
Connection Ty
Machine Aut
Credentia
User Auth
Credentia

Next
Cancel

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Networks
Profile: C:\Users\deepuv\Desktop\configuration.xml

EAP Methods
EAP-MSD
EAP-MSCHAPv2
EAP-GTC
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
Media Type
Security Level
Connection Ty
Machine Aut
Credentia
User Auth
Credentia

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
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
Next
Cancel

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups

Networks
Profile: C:\Users\deepuv\Desktop\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:
Media Type
Security Level
Connection Ty
Machine Aut
Credentia
User Auth
Credentia

Done
Cancel

-----End of Document-----