



Integrating ISE with Active Directory

Developers and Lab Proctors

This lab was created by Hakan Nohre.... And

Lab Overview

In the vast majority of 802.1X projects, Microsoft Active Directory is the Enterprise Directory for user and computer identity. It is therefore necessary for the ISE presales, consultant, engineer to have a fundamental understanding of key concepts and some powerful features of Microsoft Active Directory. It is specifically important to understand how Active Directory can provide automatic provisioning of client side certificates and configuration of client supplicants.

This lab is designed to help attendees gain an understanding of Microsoft Active Directory fundamentals and key Microsoft Active Directory features that will help in a 802.1X project.

This lab also introduces LDAP as a method for ISE to retrieve authorization data from Active Directory. Lab participants should be able to complete the lab within the allotted time of 3 hours.

Lab Exercises

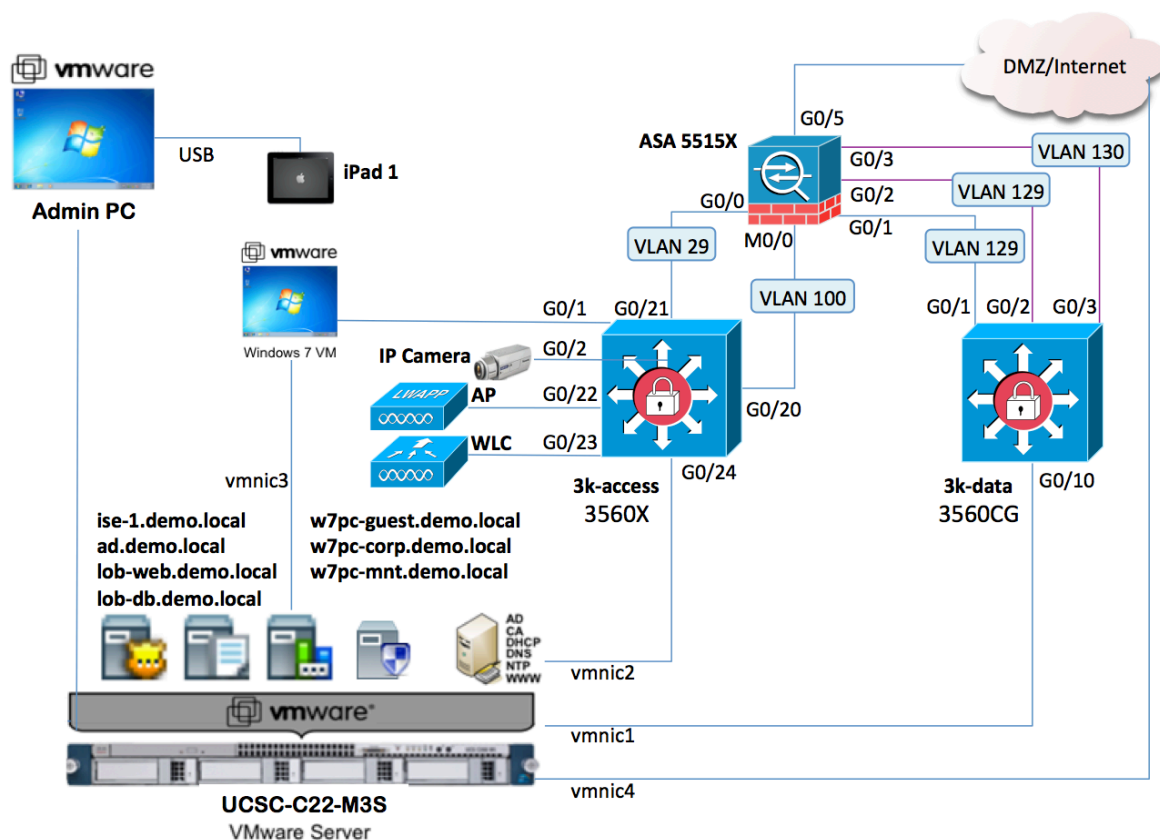
This lab guide includes the following exercises:

- Lab Exercise 1: Users and Computers, OUs and Groups.
- Lab Exercise 2: Creating Certificate Templates for Automatic Certificate Enrollment
- Lab Exercise 3: Creating Group Policies for Automatic Certificate Enrollment and Supplicant Configuration
- Lab Exercise 4: ISE interfacing with Active Directory using client certificates and LDAP
- Lab Exercise 5: ISE interfacing with Active Directory using client certificates and the AD identity store.

Product Overview: ISE

The Cisco Identity Services Engine (ISE) is an identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security and streamline their service operations. Its unique architecture allows enterprises to gather real-time contextual information from network, users and devices to make proactive governance decisions by tying identity back into various network elements including access switches, wireless controllers, VPN gateways, and datacenter switches. Cisco Identity Services Engine is a key component of the Cisco TrustSec™ Solution.

TrustSec Lab Topology



TrustSec Lab IP and VLANs

Internal IP Addresses

Device	Name/Hostname	IP Address
Access Switch (3560X)	3k-access.demo.local	10.1.100.1
Data Center Switch (3560CG)	3k-data.demo.local	10.1.129.3
Wireless LAN Controller (2504)	wlc.demo.local	10.1.100.61
Wireless Access Point (2602i)	ap.demo.local	10.1.90.x/24 (DHCP)
ASA (5515-X)	asa.demo.local	10.1.100.2
ISE Appliance	ise-1.demo.local	10.1.100.21
AD (AD/CS/DNS/DHCP)	ad.demo.local	10.1.100.10
NTP Server	ntp.demo.local	128.107.212.175
LOB Web	lob-web.demo.local	10.1.129.12
LOB DB	lob-db.demo.local	10.1.129.20
Admin (Management) Client (also FTP Server)	admin.demo.local ftp.demo.local	10.1.100.6
Windows 7 Client PC	w7pc-guest.demo.local	10.1.50.x/24 (DHCP)

Internal VLANs and IP Subnets

VLAN	VLAN Name	IP Subnet	Description
10	ACCESS	10.1.10.0/24	Authenticated users or access network using ACLs
20	MACHINE	10.1.20.0/24	Microsoft machine-authenticated devices (L3 segmentation)
(29)		10.1.29.0/24	Interconnect subnet between ASA and Access switch
30	QUARANTINE	10.1.30.0/24	Unauthenticated or non-compliant devices (L3 segmentation)
40	VOICE	10.1.40.0/24	Voice VLAN
50	GUEST	10.1.50.0/24	Network for authenticated and compliant guest users
90	AP	10.1.90.0/24	Wireless AP VLAN
100	Management	10.1.100.0/24	Network services (AAA, AD, DNS, DHCP, etc.)
129	WEB	10.1.129.0/24	Line-of-business Web servers
130	DB	10.1.130.0/24	Line-of-business Database servers

Note: Dedicated VLANs have been preconfigured for optional access policy assignments based on user identity, profiling, or compliance status. These VLANs include MACHINE, QUARANTINE, and GUEST. The labs will focus on the use of downloadable ACLs (dACLs) rather than VLAN assignment for policy enforcement.

Accounts and Passwords

Access To	Account (username/password)
Access Switch (3560X)	admin / ISEisC00L
Data Center Switch (3560X)	admin / ISEisC00L
Wireless LAN Controller (2504)	admin / ISEisC00L
ASA (5515-X)	admin / ISEisC00L
ISE Appliances	admin / ISEisC00L
AD (CS/DNS/DHCP/DHCP)	admin / ISEisC00L
Web Servers	admin / ISEisC00L
Admin (Management) Client	admin / ISEisC00L
Windows 7 Client (Local = W7PC-guest or W7PC-corp) (Domain = DEMO)	W7PC-guest\admin / ISEisC00L DEMO\admin / ISEisC00L DEMO\employee1 / ISEisC00L

Connecting to Lab Devices

Note: To access the lab, you must first connect to the Admin PC. The Admin PC provides a launching point for access to all the other lab components

Note: Admin PC access is through RDP, therefore you must have an RDP client installed on your computer

Connect to a POD

Step 1 Launch the Remote Desktop application on your system.

- In the LabOps student portal, click on the **Topology** tab
- Click on the **Admin PC**, and then click on the **RDP Client** option that appears.
- Clicking on this option should launch your RDP client and connect you to the Admin PC. Login as **admin / ISEisC00L**

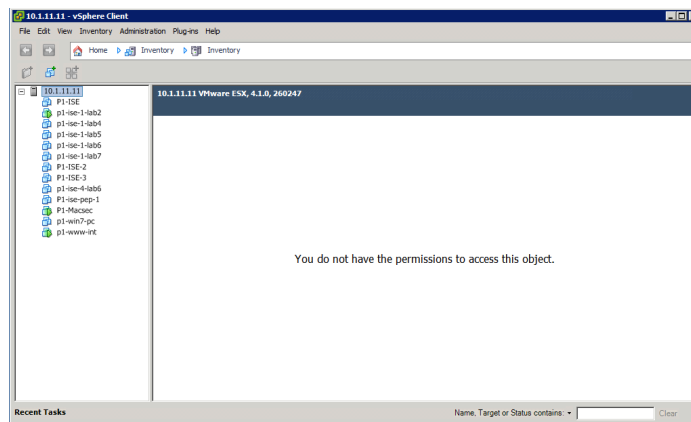
Note: All lab configurations can be performed from the Admin client PC.

Connect to ESX Server Virtual Machines

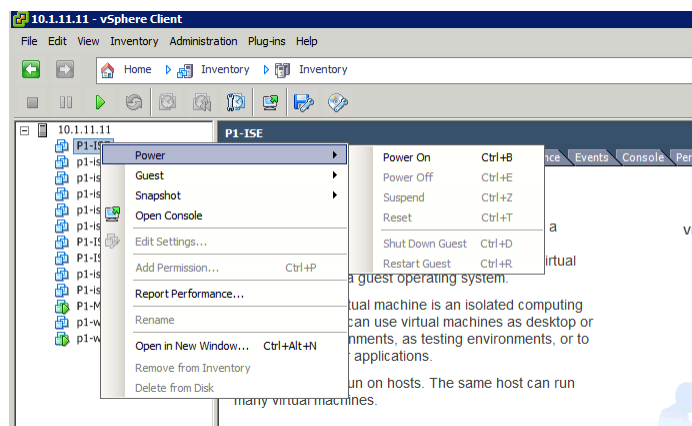
During the lab exercises, you may need to access and manage the computers running as virtual machines.

Step 1 From the Admin client PC, click the **VMware vSphere Client** icon on the desktop 

Step 2 Once logged in, you will see a list of VMs that are available on your ESX server:



Step 3 You have the ability to power on, power off, or open the console (view) these VMs. To do so, place the mouse cursor over VM name in the left-hand pane and right-click to select one of these options:



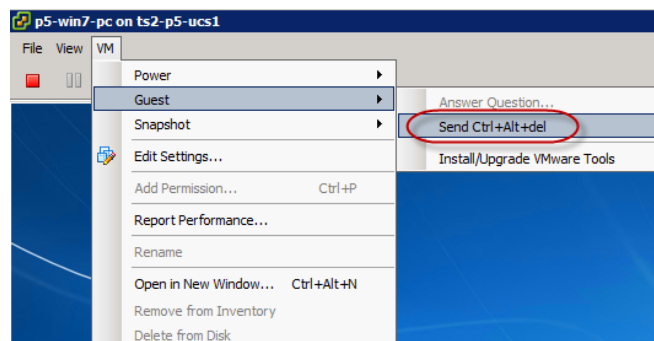
Step 4 For this lab ensure that the following VMs are up and running.

p###_ad
p###_admin
p###_ise-1-base
p###_lob-db
p###_lob-web
p###_w7pc-guest

refers to the pod number that you are assigned to. E.g., For POD 2, p##_ad would be p02_ad. The VM w7pc-guest may be power on manually during the exercises.

Step 5 To access the VM console, select **Open Console** from the drop-down.

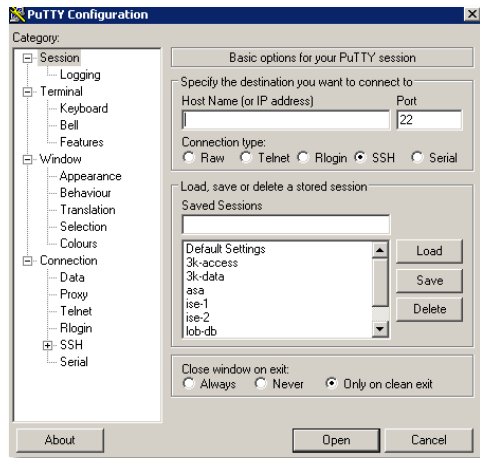
Step 6 To login to a Windows VM, select **Guest > Send Ctrl+Alt+del** from the VM Console menu:



Connect to Lab Device Consoles

Step 1 To access the lab switches and ISE servers using SSH:

- a. From the Admin client PC, right click on the **PuTTY** shortcut in the taskbar. Then, select **SSH, Telnet and Rlogin client** from the pop-up menu



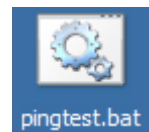
- b. Select the device that you'd like to log into and double click on it.
- c. If prompted, click **Yes** to cache the server host key and to continue login.
- d. Login using the credentials listed in the Accounts and Passwords table.

Pre-Lab Setup Instructions

Basic Connectivity Test

To perform a basic connectivity test for the primary lab devices, run the pingtest.bat script from the Windows desktop of the Admin client PC:

Verify that ping succeeds for all devices tested by the script.



Basic ISE Configuration

Step 1 Access the ISE administrative web interface.

- a. On **Admin PC**, launch Mozilla Firefox web browser. Enter this URL in the address bar:

<https://ise-1.demo.local/>

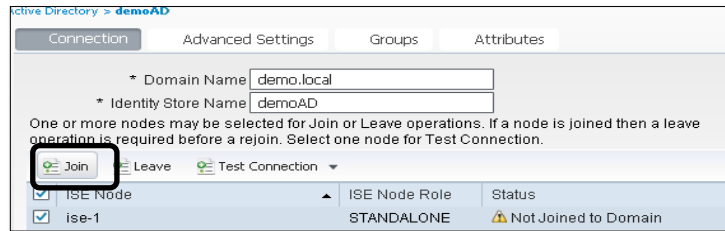
Note: Accept/Confirm any browser certificate warnings if present.



Login with username **admin** and password **ISEisC00L**

Step 2 Join to the Active Directory.

- Go to **Administration > Identity Management > External Identity Sources**.
- Pick **Active Directory** from the left-hand-side panel, and select **ise-1** in the right-hand-side **connection** tab.
- Click **Join** with AD domain admin credentials: **administrator / ISEisC00L**

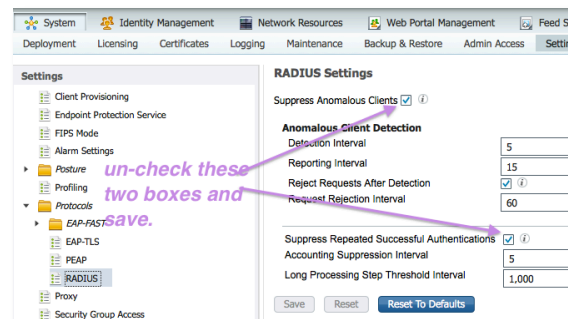


Note: If the join fails due to clock skew, use putty ssh to ise-1 admin CLI and issue **show ntp** and **show clock** to check if the ntp service is working. The ntp service may be corrected by a reload of ise-1 or a reset the VM.

Step 3 Disable log collection suppression

Starting from ISE 1.2, the log suppression is on by default to reduce monitoring data storage. In order to see all log entries during troubleshooting, the suppression can be disabled either globally or selectively per collection filters. In this lab, we will disable it globally, as shown in (a) below.

- Disable suppression globally
 - Go to **Administration > System > Settings**, expand on **Protocols**, and select **RADIUS**.
 - Un-toggle the checkboxes **Suppress Anomalous Clients** and **Suppress Repeated Successful Authentications**.



- Click **Save** when done.
- (For reference only)* Disable suppression per collection filter
 - Go to **Administration > System > Logging**, expand on **Collection Filters**, and click on **Add** for a new filter.
 - Select an attribute from the drop-down menu.
 - Enter a value to match the attribute in (ii).
 - Select **Disable Suppression** from the drop-down menu.
 - Click **Submit**.

Grant Client PC Access to AD Domain Controller

The client PC (w7pc-guest) initially has the default Windows configuration

- Wired 802.1X is turned off
- No client machine certificate
- No client user certificate

In order to obtain the appropriate settings including certificates, it must be able to communicate with the domain controller ad.demo.local. This “boot-strapping” of machines is something that has

to be taken into account in any wired 802.1X project. How can fresh machines get their configuration in a way that is seamless and automatic when the wired ports are closed down with 802.1X? Some solutions to this challenge include

- Using a separate location (switch port) where IT department may configure the PCs
- Using 802.1X with open mode, allowing all accesses to necessary configuration servers (e.g. domain controllers).
- Using 802.1X with MAB, giving only known devices in MAB database access to configuration servers (this requires that a MAB database of computers be kept).

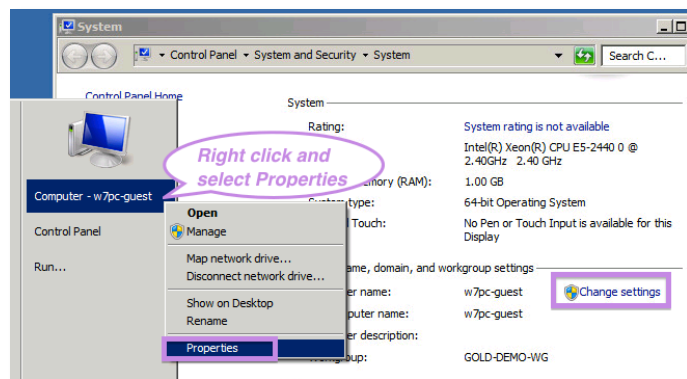
Step 1 Ensure that the PC has full access to the domain controller.

- 802.1X with open mode: Use Putty to SSH to the switch 3k-access. Issue “show run int g0/1” in exec mode to examine the running-configuration of the interface connecting the PC.
- At 3k-access CLI, issue “monitor terminal” in exec mode, to see debug messages at the current terminal session.
- At 3k-access CLI, issue “no shut” on interface gigabit 0/1 in the configuration mode.
- Log onto w7pc-guest via the vSphere console (username admin). This is a local administrator account.
- On **w7pc-guest**, double click on the desktop short-cut **w7pc-guest Network Connections**. Then, enable the **w7pc-guest-wired** connection by double-clicking on the icon.
- At 3k-access CLI, observe the debug messages or issue “show auth sessions int g0/1”, which should show auth failed. This is fine because of open mode.

Join Client PC to AD Domain

Step 1 Ensure that the PC is joined to the domain.

- Log onto w7pc-guest via the vSphere console (username admin). This is a local administrator account.
- Menu Start, then right click on **Computer – w7pc-guest** and select **Properties** from the context menu. Check under *Computer Name, Domain and Workgroup settings*. If it is not joined to demo.local, click change settings to join the computer to the domain demo.local.



- Click the change button, and enter the domain demo.local
- You will be prompted for credentials. Enter the domain administrator's credentials (administrator:ISEisC00L).
- After successfully joining the domain, you will have to restart the client w7pc-guest.
- Quiz: How did the client find a domain controller in the demo.local domain? Answer : DNS SRV records.

Lab Exercise 1: Users and Computers

Exercise Description

This exercise serves to familiarize the student with the Active Directory Users and Computers Console. Student should understand the following concepts

- Active Directory User
- Active Directory Computer
- Organizational Unit
- Security Groups and the MemberOf attribute.

Exercise Tasks

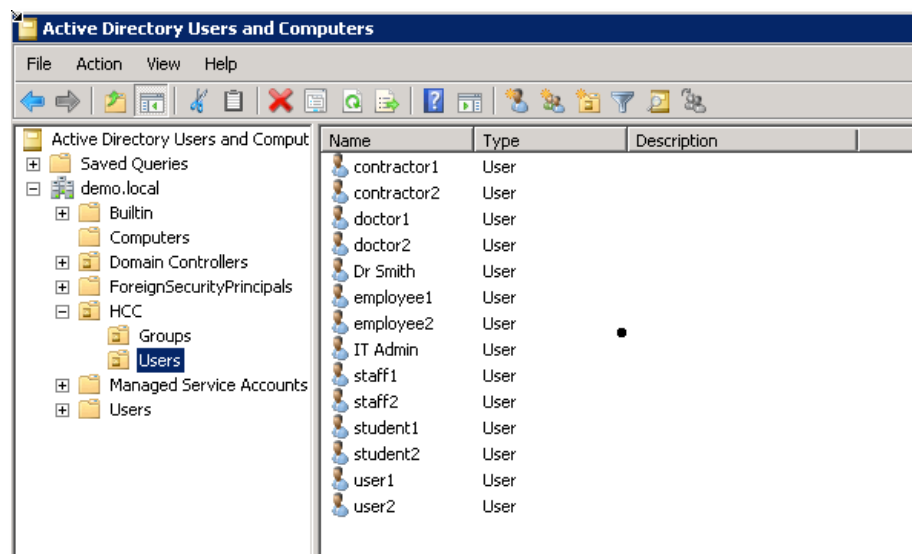
Step 1 From the admin PC, launch remote desktop (run mstsc.exe) to connect to the Domain Controller: ad.demo.local. Login with credentials for domain administrator.

Note: In an Microsoft Active Directory you may have both local accounts (local to a specific machine) and domain accounts (these credentials are validated by Domain Controllers but can be used from any computer in the domain).

To specify a domain account you can prepend the DOMAIN\ in front of the username, e.g. DEMO\administrator or DEMO\employee1. Alternatively you can specify the *user principal name*, administrator@demo.local

Step 2 Access the Active Directory Users and Computers console.

- a. On the DC, click Start Menu > Administrative Tools > Active Directory Users and Computers.



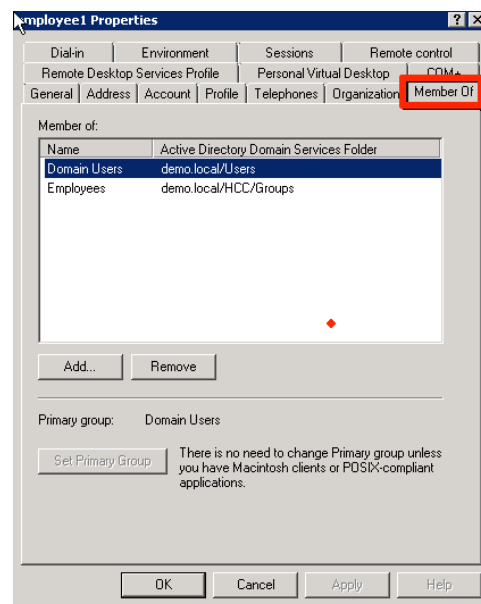
- b. Examine the structure of the domain demo.local. (**DO NOT CHANGE ANYTHING YET**). At the top level we have the domain demo.local. The domain is organized into subfolders. In the subfolder Computers where we find the computer objects (e.g. ISE). Note that the ISE itself appears here (as a result of ISE joining the domain). In the subfolder Domain Controllers we find ... you guessed it ... the domain controllers, in this case AD (which is ad.demo.local).

Note: In this lab environment there is only one domain controller per POD. In production environment you would need at least two for redundancy. It is important to understand that any changes to the Active Directory Domain (e.g. adding a user) are automatically replicated to all domain controllers in the domain. This is called Multi Master Replication, since there is no Primary Domain Controller: you can make the changes on any Domain Controller.

Locate the user accounts under subfolders HCC/Users. Here we find the users : employee1, employee2 etc.

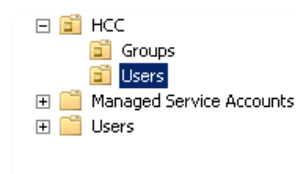
Right-click employee1 to examine its properties. Select the tab **Member Of**.

Here we see a list of the security groups that employee1 belongs to. A user (or computer) in the domain can be a member of many security groups. Typically being a member of the group brings certain security access rights, such as the right to administer the domain, the right to access a file. When working with ISE and Active Directory we often want to leverage the memberOf attribute to different network access rights depending on the memberships.



Locate the user administrator under the folder Users. Compare the Group memberships of administrator and employee1.

Note that some of the folders has a special square symbol (Like HCC, HCC:Groups and HCC:Users)

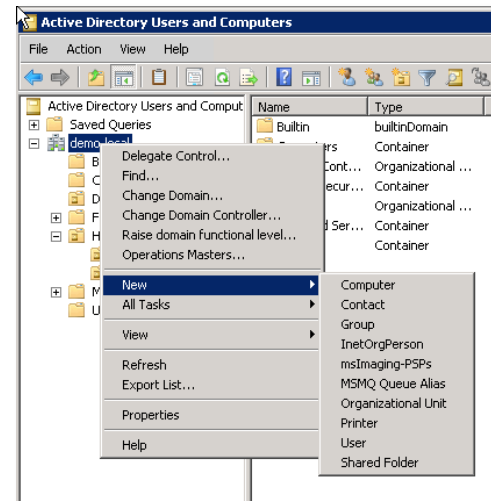


This signifies that the container is an **Organizational Unit, OU**. An OU is an important concept in Active Directory. There are two important things you should understand about OUs:

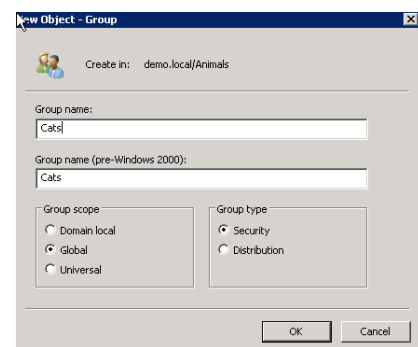
- You can delegate administrative control for an OU. This means you can delegate certain rights, such as creating users or resetting passwords, to another member of the domain who is not a domain administrator.
- You can apply **Group Policies Objects (GPOs)** to an OU. GPOs are the means by which administrators manage (mass-) configuration of client side computers and user attributes in a domain. You could also apply GPOs to the domain itself, but very often you want to limit the effects of a GPO to only some computers and users. We will cover GPOs in much more detail in exercise 4.

Step 3 Create a new OU with Groups and Members. Our objective in this step is to create a new OU (named Animals) in the domain. This OU should contain 4 groups: Rats, Cats, Mammals and AnimalsComputers. The Users are Itchy (member of Rats) and Scratchy (member of Cats). W7pc-guest is a member of AnimalsComputers.

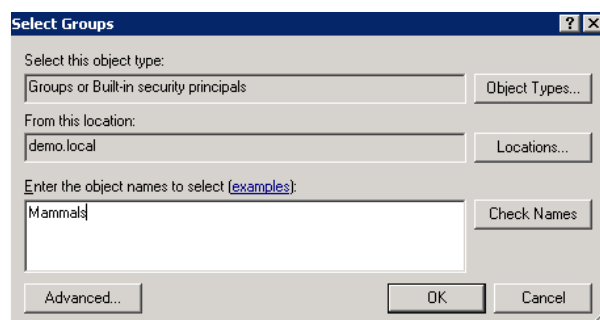
- a. In Active Directory Users and Computers, on the symbol for the domain (ad.demo.local) right-click and select New > Organizational Unit. Name the new OU Animals (it is just a name).



- b. Under the newly created OU, create a new security group called Cats. Right-Click on Animals, then select New Group. Name the group Cats and make this a Global Security Group (default options).



- c. Repeat step b. to create another Security Group named Rats.
- d. Repeat step b. to create another Security Group named Mammals. Change the scope of the group Mammals to Domain Local. (The difference between group scopes: Global, Domain local and universal scope is beyond the scope of this lab, but it is related to how the groups appear between different Active Directory domains).
- e. We now make both Cats and Rats members of the group Mammals. Right click group **Cats** and select **Add to a Group**, type Mammals. Repeat for group Rats.



Important Note: a user can be a member of a group, but that the group in turn can belong to another group (nested groups).

- f. Create a new user (itchy) in the OU. Right click the OU animals and select New User. Fill in the details as per below for itchy. Press Next, then specify the password ISEisC00L. Make sure the checkbox “User must change password at next login” is **NOT** selected.

- g. Right-click the newly created user and select properties. Under the General Tab, specify an email address for itchy (itchy@demo.local).

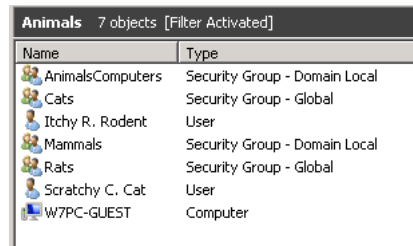
Specifying the email address is necessary for automatic provisioning of user certificates in a later exercise.

- h. Select Itchy's Member Of tab. Add Itchy to the group Rats.
- i. Repeat steps f-h to create a new user scratchy, who is a member of group Cats with an email address of scratchy@demo.local.
- j. Create a user iseLDAP with email address set to iseldap@demo.local to be used for LDAP binding in a later exercise. The user does not need added to another group.
- k. We will now move the computer object W7PC-guest from the domain Computers folder to our OU, animals. You can either drag and drop W7PC-guest or right click W7PC-guest and select move and then select the animals OU. Ignore the warning about moving objects to a different OU.

Note: Normally you would create separate OUs under the Animals OU to contain computers, but for simplicity we are mixing user and computer objects in the same container for this lab. The reason why we are moving W7PC-guest to the Animals OU is because we will later

create a Group Policy Object (GPO) applying to this OU. By applying a GPO to an OU we can limit the reconfigurations to the computers and users inside the OU (in case we don't want to apply the configuration to all computers/users in the domain). *Another reason why you want to create OUs is that you can delegate control to an OU to non domain administrators. As an example, we could allow members of the group cats to manage the OU, add and delete users, reset passwords, without them having the privilege to touch other OUs.*

- l. Add another security group (domain local), AnimalsComputers, to the OU Animals. Make W7PC-guest a member of that group.
- m. Examine your final configuration of the animals OU. It should look similar to figure below.



Name	Type
AnimalsComputers	Security Group - Domain Local
Cats	Security Group - Global
Itchy R. Rodent	User
Mammals	Security Group - Domain Local
Rats	Security Group - Global
Scratchy C. Cat	User
W7PC-GUEST	Computer

Step 4 Active Directory objects can be access via an LDAP interface (as we shall see in exercise 4). It can be very handy during development and troubleshooting to use a 3rd party LDAP browser to examine the LDAP structure, attributes and values of the Active Directory.

Install the free Softerra LDAP browser:

Download <http://tools.demo.local/admin/tools/ldapbrowser-4.5.10625.0-x64-eng.msi> to admin PC and install it.

Review Questions :

When a computer joins or logs into a domain, how does it find the (nearest) domain controller?

True or False : All the domain controllers in a domain share the same configuration of users and computers

Which of the following is NOT a typical reason to create an OU in Active Directory

- a) *To allow for delegation of administration (allow non-admins to manage the OU)*
- b) *To increase the number of objects (users and computers) Active Directory can handle*
- c) *Group Policies can be applied to an OU instead of the whole domain, to limit the effects of the Group Policy.*

True or False: A user in Active Directory can be a member of multiple groups

True or False: A group in Active Directory can be a member of another group.

☒ **End of Exercise: You have successfully completed this exercise. Proceed to next section.**

Lab Exercise 2: Configure Certificate Templates and the Certificate Authority for Automatic Certificate Enrollment

Exercise Description

This exercise will show how to leverage Active Directory Certificate Services to automatically provision client side certificates to computers and users in the OU animals.

Client certificates can be specific to a computer, or to a user that has logged on to the computer. It is possible for different users to have certificates on different computers.

In order to configure automatic certificate enrollment, we need to (in this lab exercise)

- Configure Certificate Templates that defines who can enroll and exactly what the certificate will contain.
- Tell the Certificate Authority server to use the new Certificate Templates.

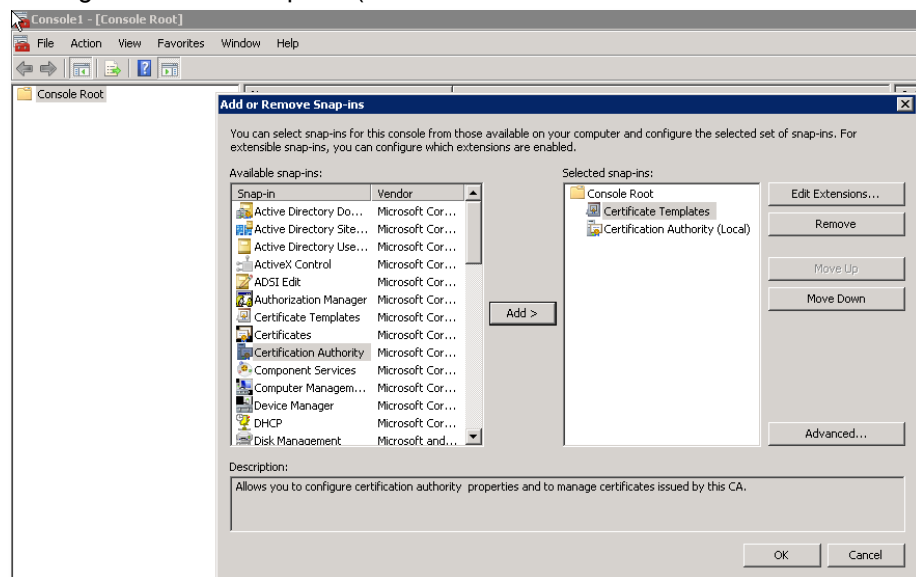
In order to activate the automatic enrollment we also need to (part of the next lab exercise 3)

- Apply a Group policy to the Users and/or Computers that enable automatic certificate enrollment.

Exercise Tasks

Step 1 Open the necessary consoles to manage certificates templates and the certificate authority.

- a. On the Domain Controller **ad.demo.local**, open the Microsoft Management Console (MMC) from Start > Run > MMC.
- b. On the MMC, choose File > Add Remove Snap-in to add configuration tools for Certificate Templates and Certificate Authority. For the Certificate Authority, use to manage the Local Computer (the CA is on same machine as the Domain Controller).



Step 2 Examine the Certificate Template Console. A Certificate Template contains the necessary information for the CA to issue certificates. In the certificate template we find information about which fields to populate in the certificates, renewal policies etc.

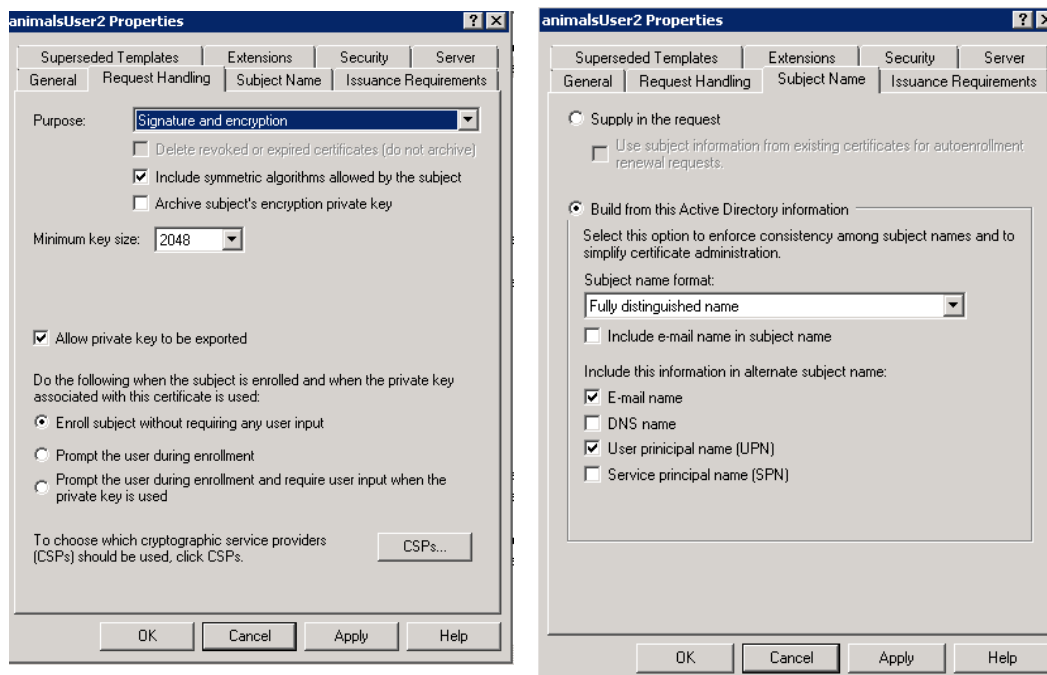
Step 3 Add a Certificate Template for Users. You **should not** change the preconfigured Certificate Templates, but instead duplicate them and apply changes to the duplicates. We are now creating two new templates, one for machine and one for users. Below the steps for the user certificate.

a. Duplicate the certificate template for User (choose the template and right-click). **Keep the Default Windows Server 2003 Enterprise.** Change the name to animalUser2.

b. Examine the tabs for Request Handling. Note the default to enroll without user input.

Examine the tab for Subject Name. Note that the default subject name in the user certificate is built from values in the Active Directory.

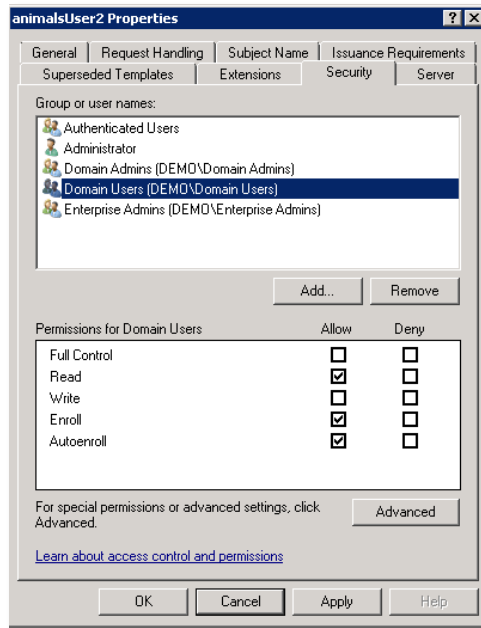
Ensure the Subject Name format is *Fully Distinguished Name*. Later we want to grab the subject name from the certificate to do an LDAP lookup for authorization, so it is important the Subject name has a format that will match the LDAP lookup we define in exercise 4.



User Certificate Template Subject Name Setting

Build from Active Directory Information	Selected
Subject Name format	Fully Distinguished Name
Include email name in subject name	Not Selected

- c. Go to the Security tab and change the settings for Domain Users. Ensure that Domain Users can Read, Enroll and Autoenroll. Click Apply/OK.

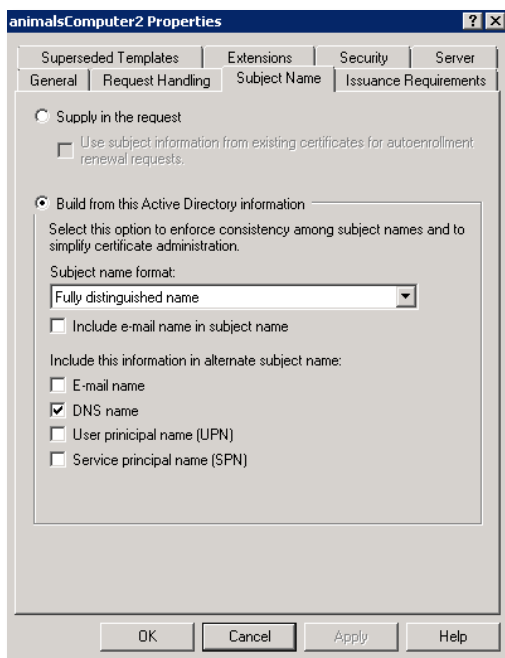


Domain User Permissions

Read	Allow
Enroll	Allow
Autoenroll	Allow

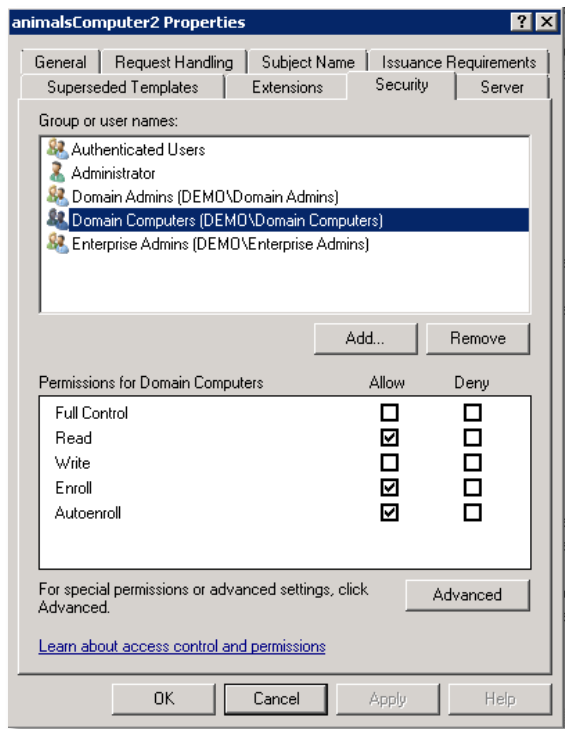
Step 4 Add a certificate template for computers. You should not change the preconfigured Certificate Templates, but instead duplicate them and apply changes to the duplicates. Below the step for the computer certificate template.

- a. Duplicate the certificate template for Computer. Choose the template and right-click. Change the name to animalComputer2.
- b. For the animalComputer2 certificate, under the Subject Name, ensure Format is Fully Distinguished Name. *ISE is going to use the field in the subject name for an LDAP lookup for authorization.*



Setting	Value
Subject Name Format	Fully Distinguished Name
Build from Active Dir information	Selected
Include email in subject name	Not Checked

- c. Go to the Security tab and change the settings for Domain Computers. Be sure that Domain Computers can Read, Enroll and Autoenroll. Click Apply/OK.



Domain Computers	Security Permissions
Read	Allow
Enroll	Allow
Autoenroll	Allow

Step 5 Now that we have created the Certificate Templates, we must instruct the Microsoft CA to issue certificates using these templates.

In the MMC, choose the Certificate Authority (Local) snap-in. Expand the tree to the left and select Certificate Templates. Right-Click **New Certificate Template to Issue**. Select our certificate templates, animalsComputer2 and animalsUser2.

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 3: Applying Group Policies

Exercise Description

In this exercise you will learn how to apply Group Policies Objects (GPOs) to computers and users. A GPO is a set of Group Policies. GPOs are a powerful tool in Microsoft Active Directory since they can be used to configure many client side aspects of computers and users. Of specific interest to an 802.1X project, is to configure the supplicant settings, and if EAP-TLS is used, to automatically provision certificates to the client machines.

Exercise Objective

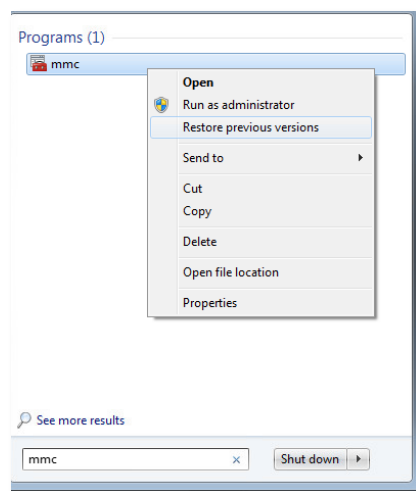
In this exercise, your goal is to complete the following tasks:

Configure a Group policy applied to the Animals OU that

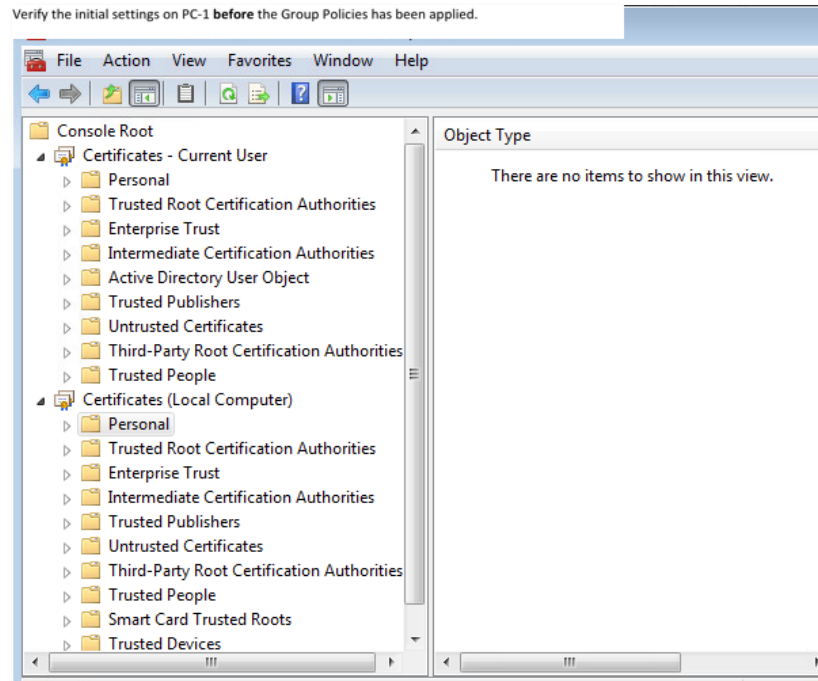
- Automatically enrolls the computer for a computer certificate
- Automatically enrolls the user with a user certificate
- Configures the 802.1X wired supplicant to run EAP-TLS with Computer or User authentication.

Exercise Tasks

- Step 1** Verify the initial settings on W7pc-guest **before** the Group Policies has been applied.
- a. Logon to W7pc-guest via the VMware console, username scratchy/ISEisC00L.
 - b. Verify the Wired Network Adapter Settings; 802.1X has not been enabled, (there is no authentication tab on network settings).
 - c. Open up the Microsoft Management Console as administrator. It is necessary to run with elevated administrator privileges to be able to examine all certificates on the computer (including the machine certificate). Start, and type MMC in the search text box. Right-click MMC select Run As Administrator. Username administrator Password is ISEisC00L.



- d. Add Snap-ins for certificates for the local computer account and my user account.

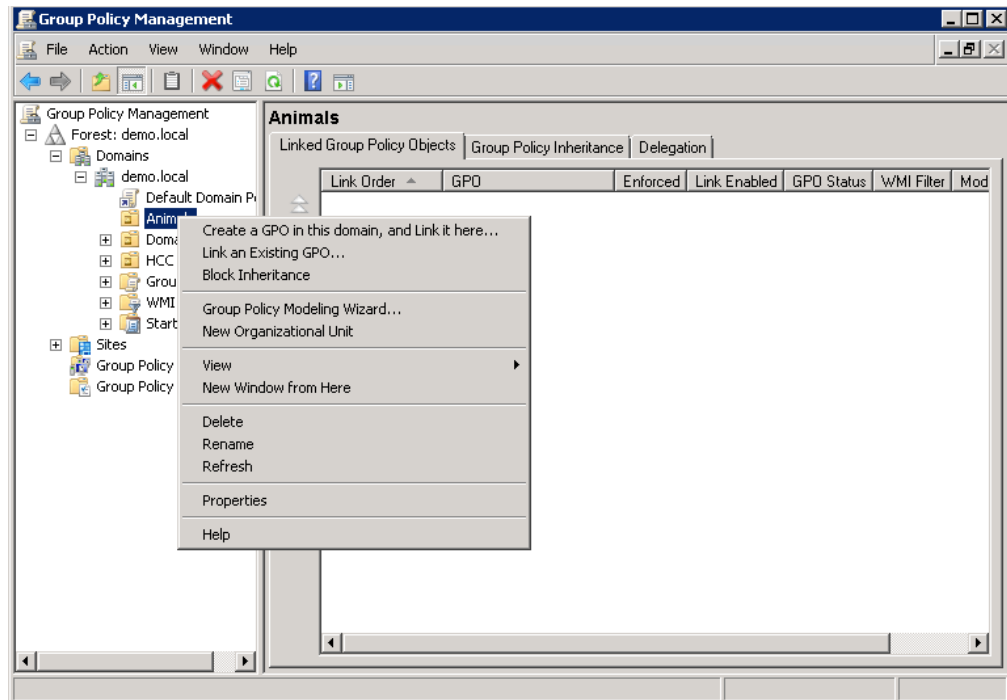


- e. Verify that there are no certificates for Current User or for the Local Computer (select each object and then the Personal Folder. This is as expected since we have not yet applied the Group Policy Object (GPO) that includes automatic certificate provisioning.
- f. Remember how to invoke the MMC console for examining client side certificates; you will need it in later exercises.

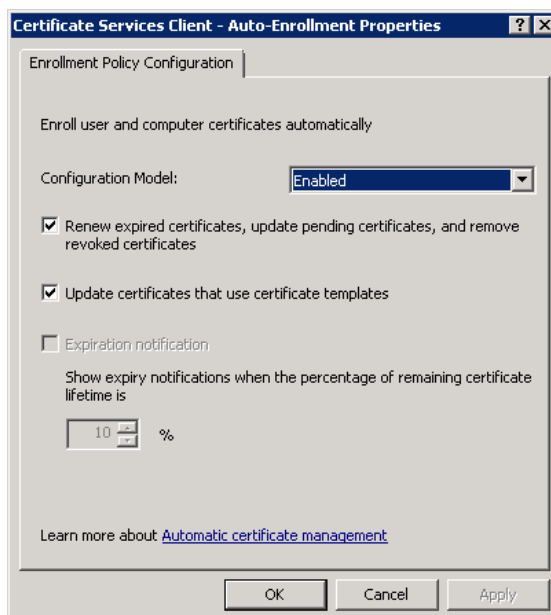
Step 2 Create a GPO to Apply Settings to Computers and Users in the Animals OU. The GPO should

- Automatically provision computer and user certificates
 - Configure the wired 802.1X supplicant to authenticate with certificates (EAP-TLS)
 - Configure the wired 802.1X supplicant for computer OR user authentication
- a. On the Active Directory Domain Controller, open up the Group Policy Management Console (Start Menu > Administrative Tools > Group Policy Management).
- b. In the Group Policy Management Console, select the OU Animals (that you created in Exercise 1), right click and select "Create a GPO in this Domain and Link it here".

Lab Exercise 3: Applying Group Policies



- c. Name it something meaningful, like “enrollCertsandConfigureDot1X”. Leave the field Source Starter GPO as none.
- d. Edit the GPO. Right Click the newly created GPO and click edit. The Group Policy Management Editor should open.
- e. Note that there are folders for Computer settings and folders for User Settings. Configure Automatic Certificate Enrollment for the Computer by opening up the folders Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies. Configure the Certificate Services Client – Autoenrollment Properties as per below.

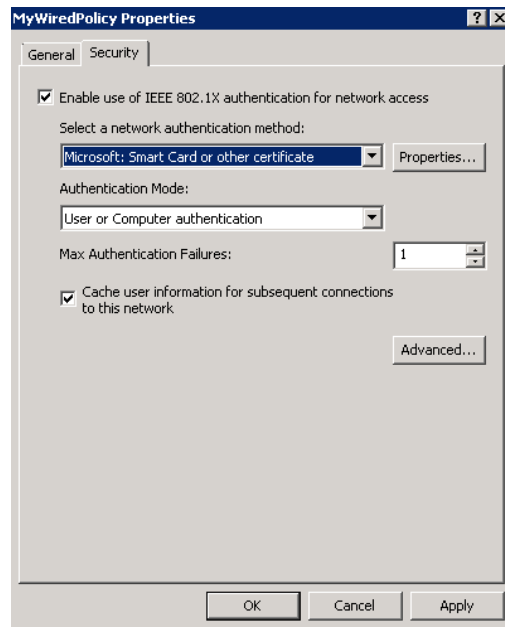


Value	Attribute
Configuration Model:	Enabled
Renew expired:	Checked
Update certificates:	Checked

- f. Configure the Computers wired 802.1X settings by opening up the folder Computer Configuration > Policies > Windows Settings > Security Settings > Wired Network (IEEE 802.3 Policies) > Create a New Wired Network Policy for Vista and Later Releases.

Under the general tab, give a name. Under the security tab,

- Enable Use of 802.1X
- Select a network authentication Method : Smart Card or Certificate
- Authentication Mode : User or Computer authentication.



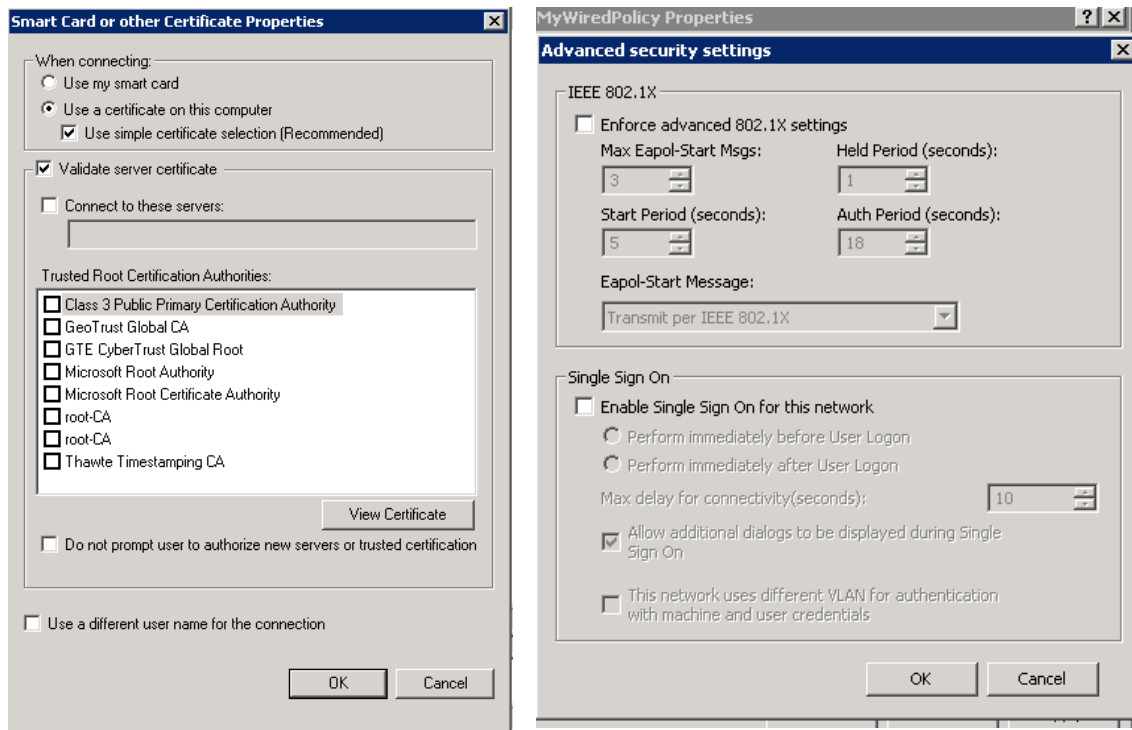
The Authentication Mode : User or Computer authentication will have Windows authenticate with machine credentials when no user is logged onto the machine. When a user logs on to the machine, the client will initiate a new EAP login with the user credentials.

The Authentication Mode: Computer will have Windows always use machine credentials, regardless of whether a user is logged onto the machine or not.

The Authentication Mode : User will have Windows only use the credentials of the currently logged on user. This is rarely used since with this option the machine may not be able to authenticate and gain access to the network unless a user is logged on. The Microsoft bootup process would suffer, since the machine attempts to contact the domain controller to apply GPOs even before any user has logged on.

Click on the Properties page next to Smart Card or Certificate. Note that it is possible to specify to which servers (RADIUS servers) to connect. The default is to connect to all servers with a certificate that the client trusts. Since ISE certificate has been issued by the demo.local CA server, and since the client trusts that CA server (that trust is automatically established when the client joins the domain) the client will trust the ISE certificate. Cancel out of the Smartcard or Certificates Properties dialog box.

Click on the Advanced button. Inspect the EAPOL parameters (timeouts, whether to send EAPOL-START etc). Cancel out of the Advanced dialog box.



Note : Students should recognize these settings from the settings of the network adapter on a Microsoft Windows Computer running Vista or later. However, the big advantage of using a GPO to configure these settings is that you can use central management that takes precedence over any local configuration of the client

- g. Wired 802.1X supplicant requires that the Wired AutoConfig Service is started. Configure this setting with the Group Policy Management Editor. Open up the Computer Configuration > Policies > Windows Settings > Security Settings > System Services and double-click or right click to open up the service configuration.

☒ Define this policy setting

Select service startup mode: Automatic.

- h. Configure the User settings for Automatic Certificate Enrollment with the Group Policy Management Editor. Open up the User Configuration > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto Enrollment. Right-click and click properties.

Choose Configuration Model Enabled

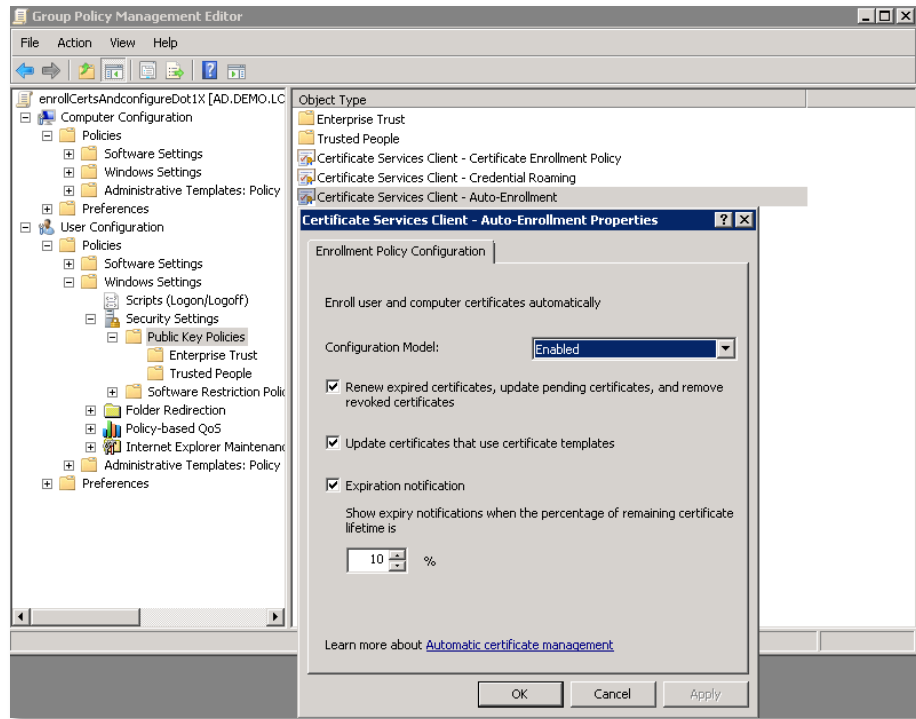
Renew expired certificates: checked

Update certificates that use certificates templates

Expiration notification

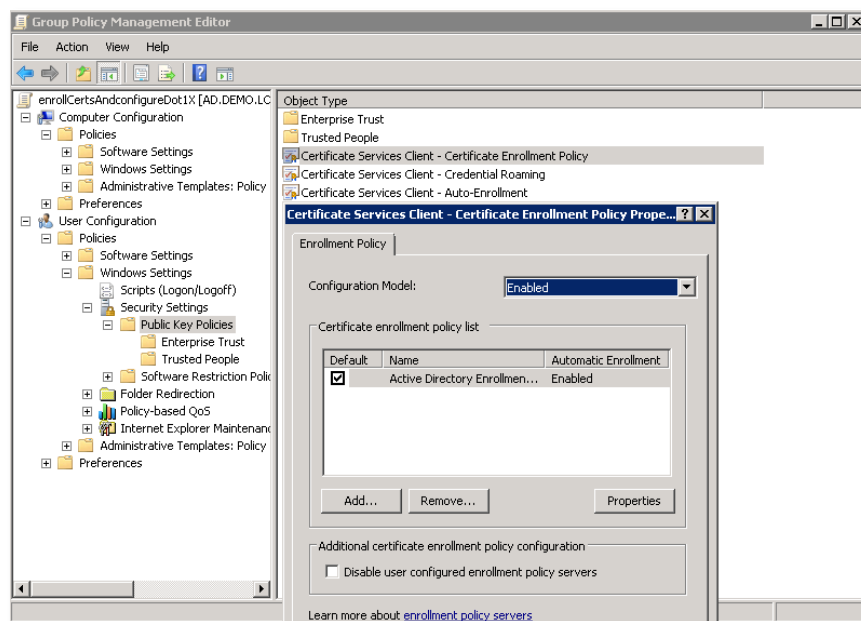
10%

Lab Exercise 3: Applying Group Policies

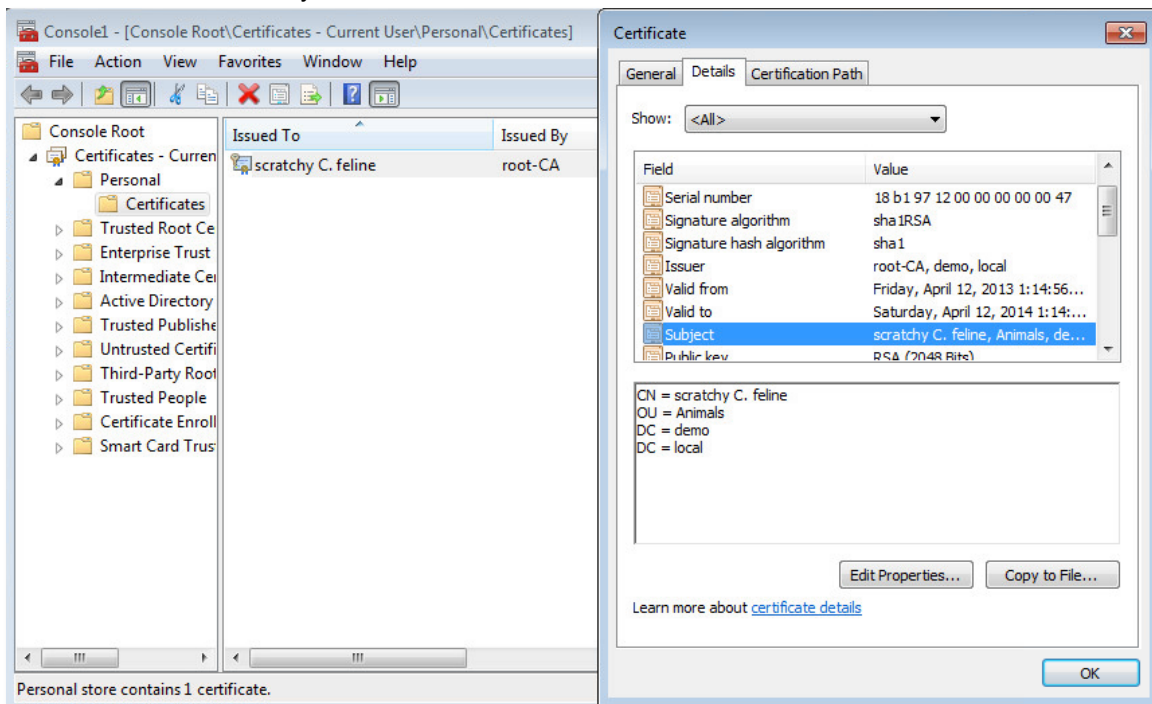


Configure the Certificate Services Client – Certificate Enrolment Policy.

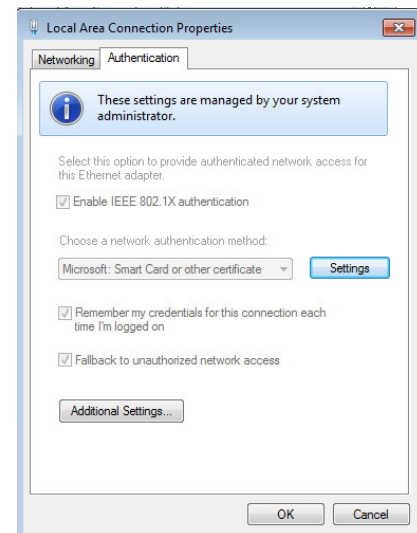
Attribute	Value
Configuration Model	Enabled
Certificate Enrollment Policy List	Use default (Active Directory Enrollment)



- Step 3 Apply the Group Policies on W7pc-guest machine. Computer GPOs are applied at the next restart of the computer. User GPOs are applied at the next user login. You can also force immediate refresh of GPOs by running `gpupdate /force` from the command prompt (you need to be administrator to refresh computer GPOs.).
- On W7pc-guest, issue a restart from the start menu (start menu > restart).
 - Login to W7pc-guest with DEMO\scratchy account.
 - Open up MMC console to examine both the user certificate and the computer certificate (you need to run MMC as administrator to see computer store). What are the subject names and why?



- Open up the wired network adapter properties and verify there is now an authentication tab (Wired Autoconfig process has started). Verify that 802.1X configuration uses client side certificate or smartcard, and Machine or User authentication. Note that you can not change these settings on the client since they are configured by the GPO.



☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

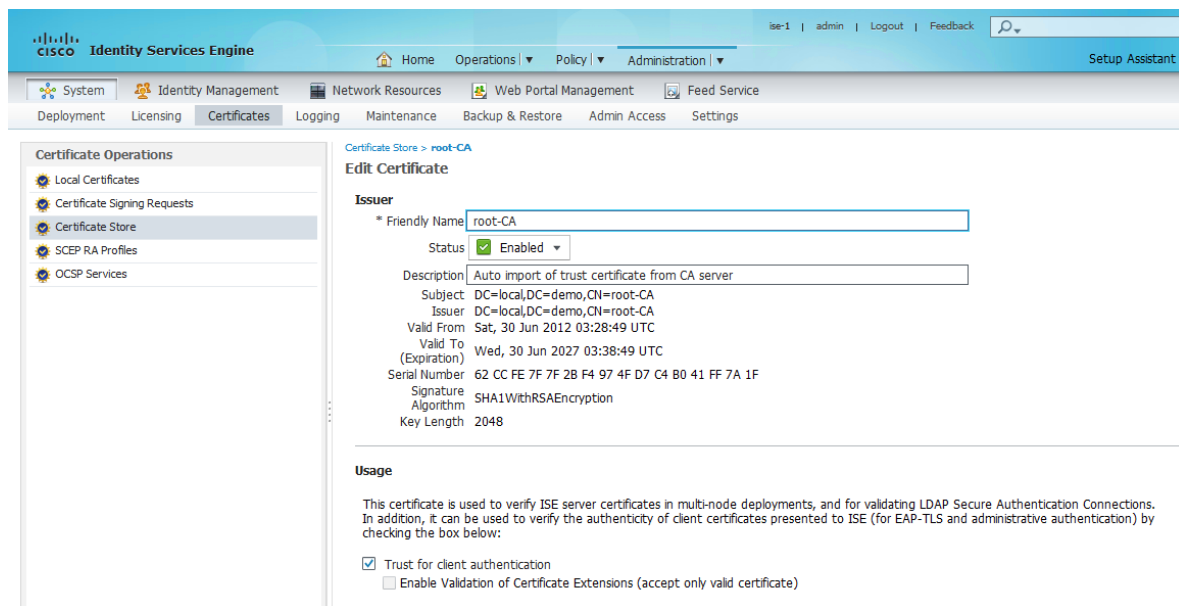
Lab Exercise 4: Configure and Test ISE for Client Certificate Authentication and Authorization via LDAP

Exercise Description

We will now configure ISE to allow for client side certificate authentication with EAP-TLS, and subsequent authorization via LDAP lookup. Note that instead of using LDAP lookup we could use ISE native Active Directory connection (AD identity store) for authorization lookup. The reason we use LDAP in this lab exercise is because to show an alternative to the native Active Directory connection that may be useful in certain scenarios. (One such scenario is when you have multiple Active Directory Forests without trust. Here using LDAP may support more than one domain connection).

Exercise Tasks

- Step 1** Logon to <https://ise1.demo.local> with your browser. Username admin and password ISEisC00L.
- Step 2** Verify that ISE trusts the client certificates issued by the root-CA (this should already have been configured. Go to Administration > System > Certificates > Certificate Store and examine the root-CA certificate. Ensure that **Trust for client authentication** is checked.



- Step 3** Configure an LDAP connection under ISE > Administration > Identity Management > External Identity Sources > LDAP.
- Under the General tab, give the name demoLDAP and the schema ActiveDirectory. Choose the Active Directory Schema template, but modify the attribute for Subject Name to contain **distinguishedName**. (Changing this will change the Schema template name to Custom).

Using the default value, userPrincipalName will not work with our certificates, since we have configured the computer and user certificates to have the Subject Name populated with the Fully Distinguished Name. The attribute in LDAP that contains the Fully Distinguished Name is called distinguishedName. (Bonus Exercise: verify this with your Softerra LDAP Browser).

LDAP Identity Sources List > demoLDAP

LDAP Identity Source

General Connection Directory Organization Groups Attributes

* Name: demoLDAP

Description:

Schema: Custom

* Subject Objectclass: Person

* Subject Name Attribute: distinguishedName

* Group Objectclass: Group

* Group Map Attribute: memberOf

Certificate Attribute: userCertificate

☒ Subject Objects Contain Reference To Groups

☐ Group Objects Contain Reference To Subjects

Subjects In Groups Are Stored In Member Attribute As: Distinguished Name

- b. Under Connection tab, specify the host ad.demo.local, and the credentials with which ISE will bind to the LDAP server (iseldap@demo.local, password ISEisC00L. Note that it is best practice to use a low privilege account such as iseldap and not the administrator account. Test the configuration so far by pressing “Test Bind to Server”.

LDAP Identity Sources List > demoLDAP

LDAP Identity Source

General Connection Directory Organization Groups Attributes

Primary Server

* Hostname/IP: ad.demo.local

* Port: 389

Access: ☒ Authenticated Access

Admin DN: iseldap@demo.local

Password: *****

Secure Authentication: ☐ Enable Secure Authentication

Root CA: VeriSign Class 3 Public Primar

* Server Timeout: 10 Seconds

* Max. Admin Connections: 20

Test Bind to Server

Secondary Server

☐ Enable Secondary Server

Hostname/IP:

Port: 389

Access: ☐ Anonymous Access

Admin DN:

Secure Authentication: ☐ Enable Secure Authentication

Root CA: VeriSign Class 3 Public Primar

Server Timeout: 10 Seconds

Max. Admin Connections: 20

Test Bind to Server

non-domain-admin user with email address iseldap@demo.local

- c. Under the Directory Organization tab, specify the subject and group search base as dc=demo,dc=local. (We could also limit the search to only search the animals OU).

LDAP Identity Sources List > demoLDAP

LDAP Identity Source

General Connection Directory Organization Groups

* Subject Search Base: DC=demo,DC=local

* Group Search Base: DC=demo,DC=local

Search for MAC Address in Format: xx-xx-xx-xx-xx-xx

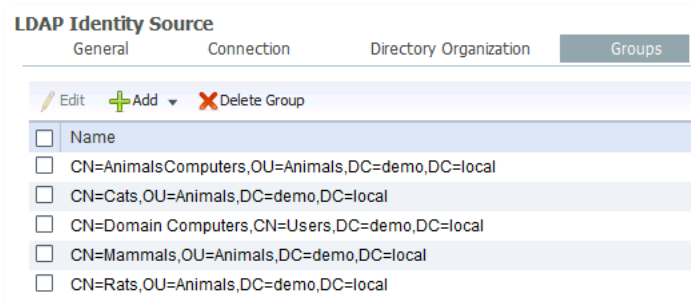
☐ Strip start of subject name up to the last occurrence of the separator \

☐ Strip end of subject name from the first occurrence of the separator

- d. Under Groups Tab, select Add and Retrieve groups from Directory. Make sure to select the following groups corresponding to the 5 groups:

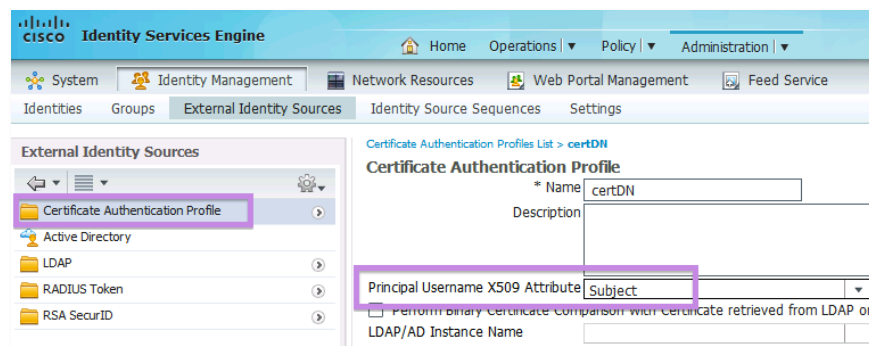
Domain Computers
AnimalsComputers
Cats
Rats
Mammals

- e. Make sure you save the LDAP configuration by pressing Save Button.



Step 4 Configure a Certificate Authentication Profile that extracts the Fully Distinguished Name from the certificate and uses this field as the username.

- a. ISE > Administration > Identity Management > External Identity Stores > Certificate Authentication Profiles. Add a profile called certDN that selects Subject as the Principal Username X509 Attribute.



Step 5 Use certDN for DOT1X authentication: Navigate to Policy > Authentication. Update DOT1X Authentication Policy rule below to use certDN.



Step 6 Create four Authorization Profiles. We can use the same RADIUS attributes – a simple ACCESS-ACCEPT – in all of them. The purpose of these authorization policies is to test our configuration. At a later stage in the project, animals could enforce more granular control with different VLANs or dACLs in the different Authorization Profiles.

Authorization Profile	Value
TLS_Domain_Computers	ACCESS-ACCEPT
TLS_Mammals	ACCESS-ACCEPT
TLS_Rats	ACCESS-ACCEPT
TLS_Cats	ACCESS-ACCEPT

Step 7 Create authorization policies to catch the following conditions.

Rule Name	Condition	Authorization Profile
<i>TLS Corp Computers</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=AnimalsComputers,.....	TLS-Domain-Computers
<i>TLS Mammals</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=Mammals,.....	TLS-Mammals
<i>TLS Cats</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=Cats,.....	TLS-Cats
<i>TLS Rats</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=Rats,.....	TLS-Rats

Note that the first condition checks for the client belonging to the group AnimalsComputers. You can try to check for membership of the group Domain Computers, but that check will not work with the LDAP check since it is the primary group. This should not be an issue in real life deployment, since you can use another group to check that this is a “corporate” computer. Also, using client side certificates may be used to proof that it is a corporate computer.

✓	TLS Corp Computers	if (Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=AnimalsComputers,OU=Animals,DC=demo,DC=local)	then TLS_Domain_Computers
✓	TLS Mammals	if (Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=Mammals,OU=Animals,DC=demo,DC=local)	then TLS_Mammals
✓	TLS Cats	if (Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=Cats,OU=Animals,DC=demo,DC=local)	then TLS_Cats
✓	TLS Rats	if (Network Access:EapAuthentication EQUALS EAP-TLS AND demoLDAP:ExternalGroups EQUALS CN=Rats,OU=Animals,DC=demo,DC=local)	then TLS_Rats

Step 8 Test our configuration. We will test a sequence of events that should exercise our configuration and also show the behavior of Microsoft Windows 7 supplicant when configured for Computer OR User authentication.

- Restart w7pc-guest (Use the Windows Start Panel > Restart).
- Logon as domain user scratchy
- Logout (Use the Windows Start Panel > Logoff)
- Logon as domain user itchy.

Step 9 Verify the ISE authentication logs. You should see (in chronological order) 4 different logons with the results corresponding to the actions in the previous step.

- TLS-Domain-Computers (client has restarted as authenticates as machine)
- TLS-Cats (scratchy logs in to the client)
- TLS-Domain-Computers (scratchy logs off, note that this generates a machine authentication).
- TLS-Rats (Itchy logs on).

Show Live Sessions Add or Remove Columns Refresh Refresh Every 10 seconds Show Latest 20 records within Last 24 hours							
Time	Status	Details	Repeat Count	Identity	Authorization Profiles	Event	Session ID
2013-08-24 22:30:29.167			0	CN=Itchy R. Rodent,OU=Animals,DC=demo,DC=local		Session State is Authorized	0A016401000000C4767E3D70
2013-08-24 22:30:27.122				CN=Itchy R. Rodent,OU=Animals,DC=demo,DC=local	TLS_Rats	Authentication succeeded	0A016401000000C4767E3D70
2013-08-24 22:30:11.836				CN=W7PC-GUEST,OU=Animals,DC=demo,DC=local	TLS_Domain_Comp...	Authentication succeeded	0A016401000000C4767E3D70
2013-08-24 22:30:02.020				CN=Scratchy C. Cat,OU=Animals,DC=demo,DC=local	TLS_Cats	Authentication succeeded	0A016401000000C4767E3D70
2013-08-24 22:29:35.078				CN=W7PC-GUEST,OU=Animals,DC=demo,DC=local	TLS_Domain_Comp...	Authentication succeeded	0A016401000000C4767E3D70

Note that we did not get a match on the 2nd authorization profile TLS-Mammals. This checks for a membership in the Group CN=Mammals, the Group-in-Group or Nested Group we configured in Exercise 1. ISE LDAP lookup does not lookup groups in groups. (This is different from when using the Active Directory Identity Store defined in ISE seen by next exercise.).

End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 5: Configure and Test ISE for Client Certificate Authentication and Authorization via Active Directory Identity Store

Exercise Description

We will now configure ISE to allow for client side certificate authentication with EAP-TLS, and subsequently authorize using the ISE native Active Directory interface, the Active Directory Identity Store.

Exercise Tasks

Step 1 You have already configured ISE for client certificate authentication and for extracting the Full Distinguished Name for username. All we have to do is to modify Authorization Policy with conditions to test group membership using the Active Directory Identity Store.

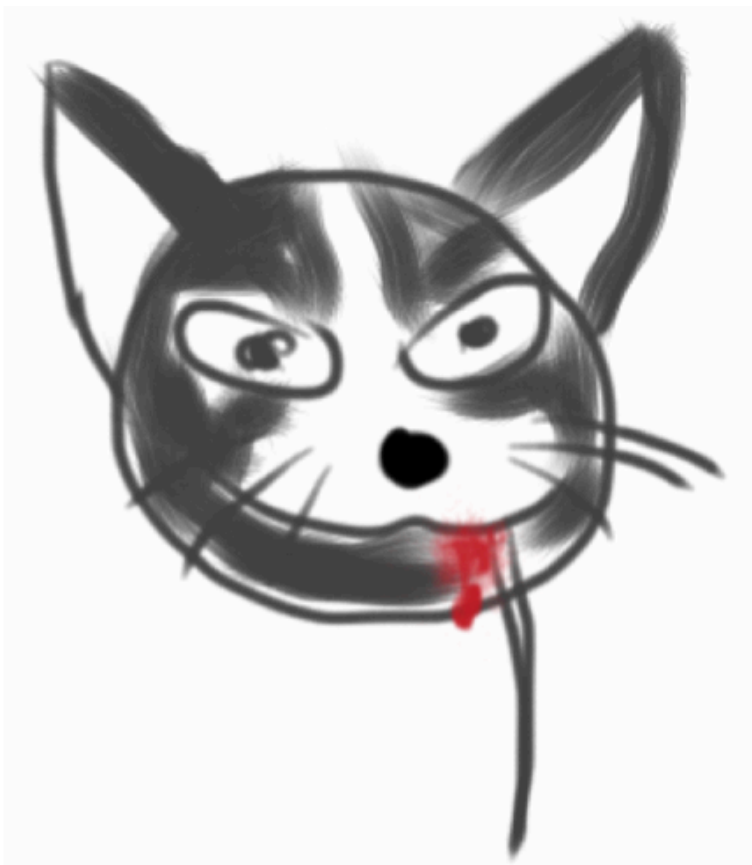
<i>Rule Name</i>	<i>Condition</i>	<i>Authorization Profile</i>
<i>TLS Corp Computers</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoAD:ExternalGroups EQUALS AnimalsComputers	TLS-Domain-Computers
<i>TLS Mammals</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoAD:ExternalGroups EQUALS Mammals	TLS-Mammals
<i>TLS Cats</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoAD:ExternalGroups EQUALS Cats.	TLS-Cats
<i>TLS Rats</i>	Network Access:EapAuthentication EQUALS EAP-TLS AND demoAD:ExternalGroups EQUALS Rats	TLS-Rats

Step 2 Test our configuration. We will test a sequence of events that should exercise our configuration and also show the behavior of Microsoft Windows 7 supplicant when configured for Computer OR User authentication.

- e. Restart w7pc-guest (Use the Windows Start Panel > Restart).
- f. Logon as domain user scratchy
- g. Logout (Use the Windows Start Panel > Logoff)
- h. Logon as domain user itchy.

Step 3 Verify the result with the ISE authentication logs. The result is the same, with the difference that the Mammals condition was matched, because ISE-AD integration supports nested groups.

Time	Status	Details	Repeat Count	Identity	Authorization Profiles	Event	Session ID
2013-08-24 22:37:54.824			0	CN=Itchy R. Rodent,OU=Animals,DC=demo,DC=local		Session State I...	0A016401000000C5768513F8
2013-08-24 22:37:52.764				CN=Itchy R. Rodent,OU=Animals,DC=demo,DC=local	TLS_Mammals	Authentication...	0A016401000000C5768513F8
2013-08-24 22:37:38.915				CN=W7PC-GUEST,OU=Animals,DC=demo,DC=local	TLS_Domain_Comp...	Authentication...	0A016401000000C5768513F8
2013-08-24 22:37:30.721				CN=Scratchy C. Cat,OU=Animals,DC=demo,DC=local	TLS_Mammals	Authentication...	0A016401000000C5768513F8
2013-08-24 22:37:13.113				CN=W7PC-GUEST,OU=Animals,DC=demo,DC=local	TLS_Domain_Comp...	Authentication...	0A016401000000C5768513F8



☒ **End of Exercise:** You have successfully completed this exercise and the whole lab. Please Note that no animals were injured during this lab.