Configuring Authentication, Roles and SSO on Cisco NAC Appliance

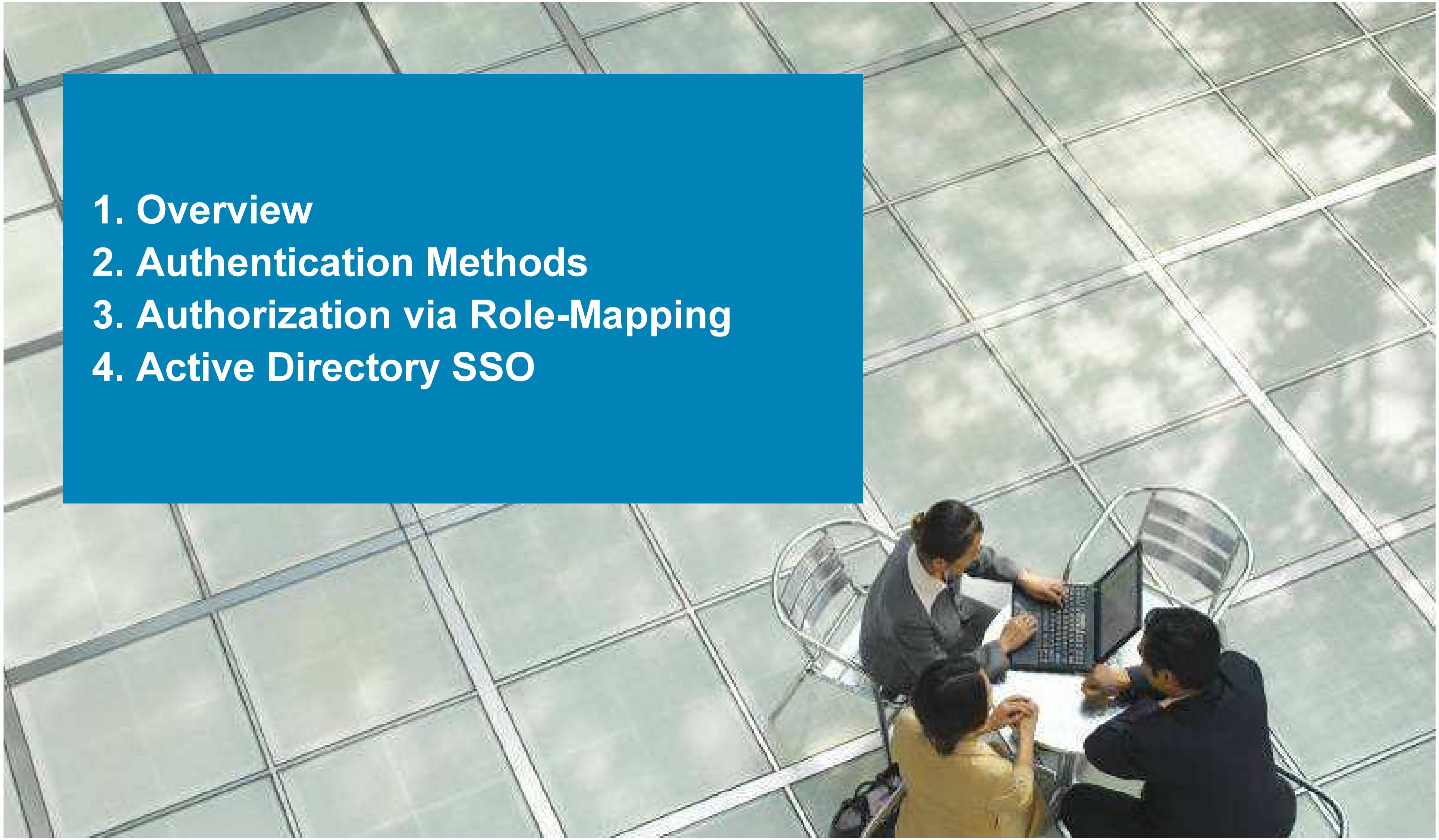
February 16 2007

Prem Ananthakrishnan

Technical Marketing Engineer

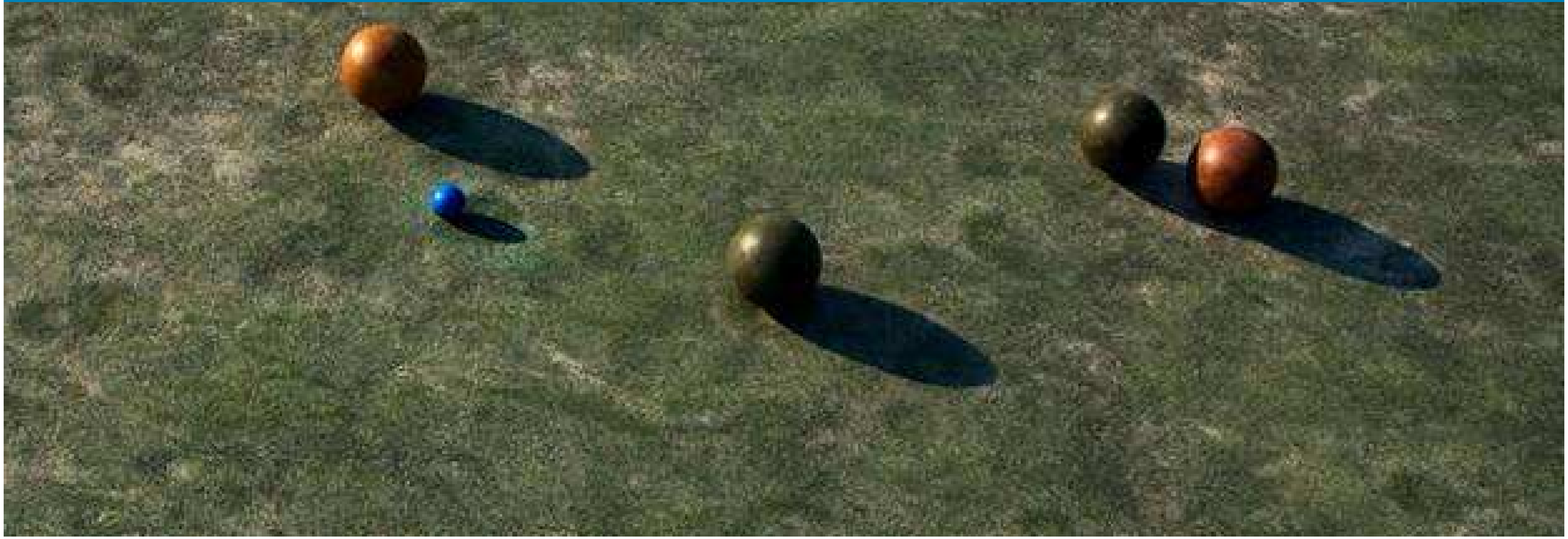
NAC Appliance

Agenda



1. Overview
2. Authentication Methods
3. Authorization via Role-Mapping
4. Active Directory SSO

Overview



Identity

- Identity is a crucial piece of any NAC solution.
- Identity confirms WHO YOU ARE, WHERE YOU ARE FROM and lets you enforce DIFFERENTIATED policies based on the same.
- Lets you leverage existing databases and information to achieve this.
- NAC without identity is not scalable and not dynamic
- At a high level, Identity is achieved through **Authentication** and **Authorization**

Authentication

- Basic authentication is achieved by communicating to an external database such as Radius, LDAP servers or a local database on the CAM
- Single Sign On can be used to leverage an existing authentication mechanism and hence avoid authenticating a second time to the NAC Appliance.

Authorization

- NAC Appliance achieves authorization by mapping users into Roles. This can be done dynamically through **ROLE MAPPING.**

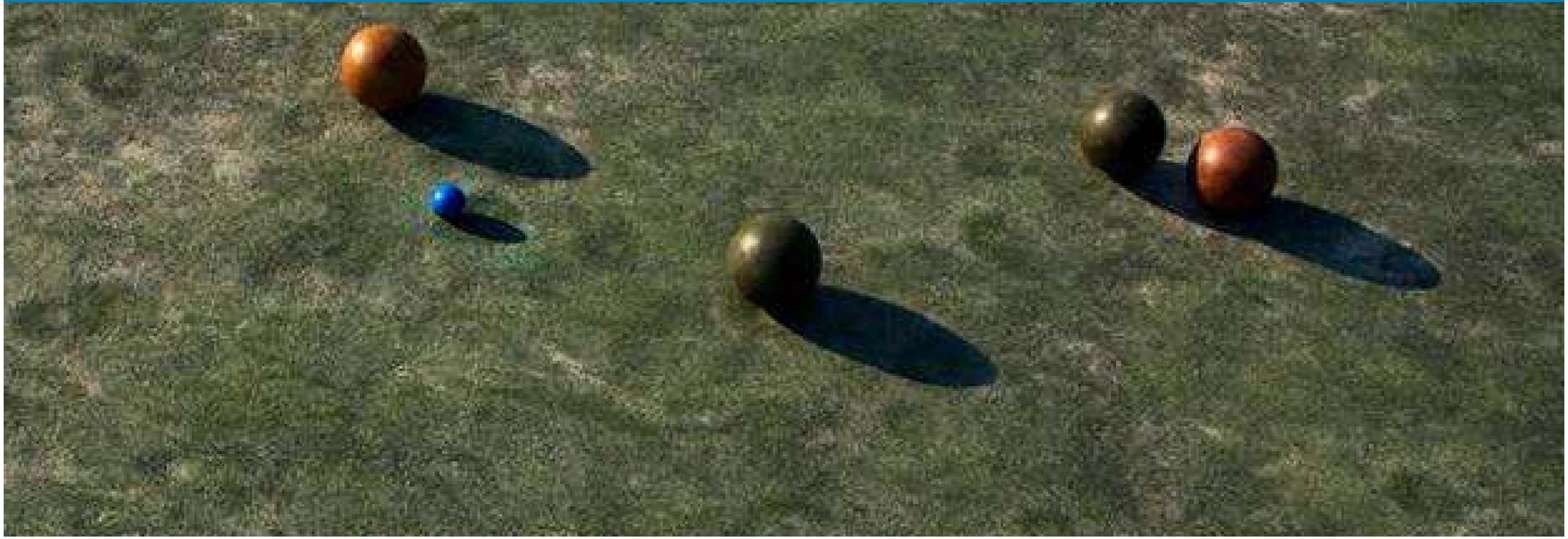
Placing users in different roles is a very important piece of NAC appliance solution.

- It helps provide differentiated enforcement like dynamic VLAN assignment (OOB), dynamic ACLs, dynamic Bandwidth control

- Role mapping helps us treat users differently and apply differentiated NAC Policies based on the source network, client OS, etc. Employers may be treated differently versus Contractors who get treated differently from Guests

Note: For OOB, dynamic ACLs and BW control apply only for the time the user is INLINE with the CAS (i.e during the time the user is on the Authentication VLAN)

Authentication Methods



Overview

Authentication mechanism and server is identified through Providers.

A new provider can be added by going to User Management >> Auth Server >> New

Providers:-

- Local authentication on the CAM - **Local DB**
- Generic LDAP support for Active Directory, iPlanet, eDirectory etc - **LDAP**
- Standards based support for ACS, Steelbelt, RSA (ACE), IAS, Freeradius etc - **Radius**
- Support for other methods like **Kerberos, NTLM**
- Single Sign On : **VPN SSO, AD SSO**
- Guest User authentication methods – Guest Button (One-click authentication), **Allow All** (Name/Email

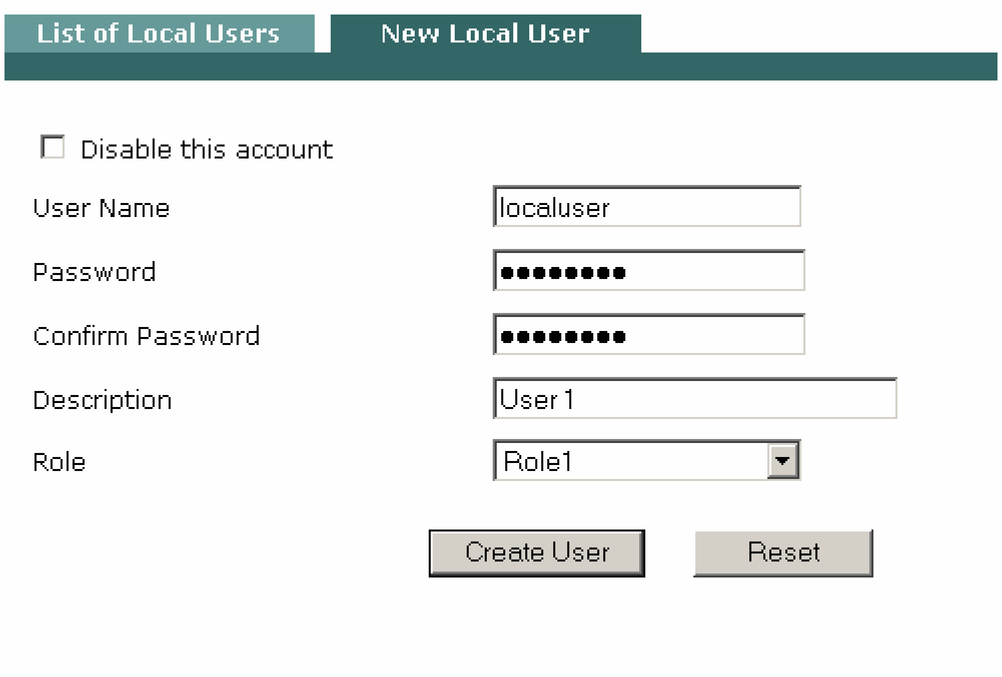
Note: For certain providers, It may be important to approve/select them on the User Pages section

Authentication methods

Local

Local Database

- Under User Management >> Local users , create a new user and associate the user to a Role

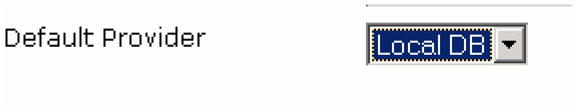


□ Disable this account

User Name	localuser
Password	●●●●●●●●●
Confirm Password	●●●●●●●●●
Description	User 1
Role	Role1

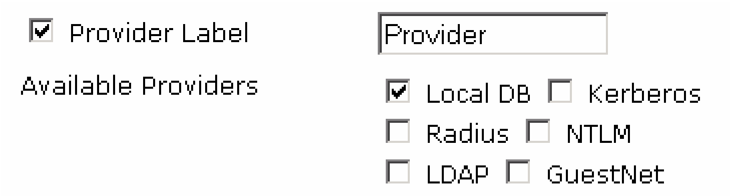
Add Provider to User Pages

- Ensure your provider is selected in the Administrator >> User Pages >>Content section in one of the following ways



Default Provider | Local DB ▾

By choosing your default Provider as the server you want to authenticate against. In this example, this is the provider called Local DB



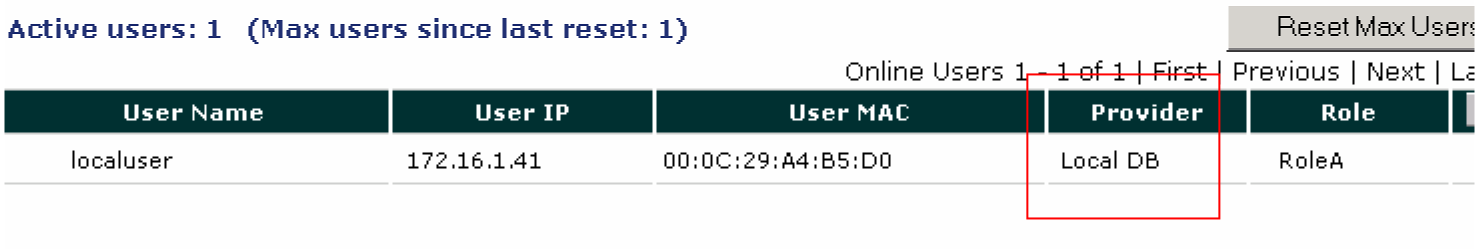
☑ Provider Label | Provider

Available Providers | ☑ Local DB ☐ Kerberos
☐ Radius ☐ NTLM
☐ LDAP ☐ GuestNet

By checking the option for Provider label and then selecting the available providers as shown. This option will be used when you have more than one external database to authenticate against. Users will pick the database they have to log into

Local Database

- User logs in and is seen on the Online User List with the Provider Name as Local DB



Active users: 1 (Max users since last reset: 1)

User Name	User IP	User MAC	Provider	Role
localuser	172.16.1.41	00:0C:29:A4:B5:D0	Local DB	RoleA

Authentication methods

LDAP

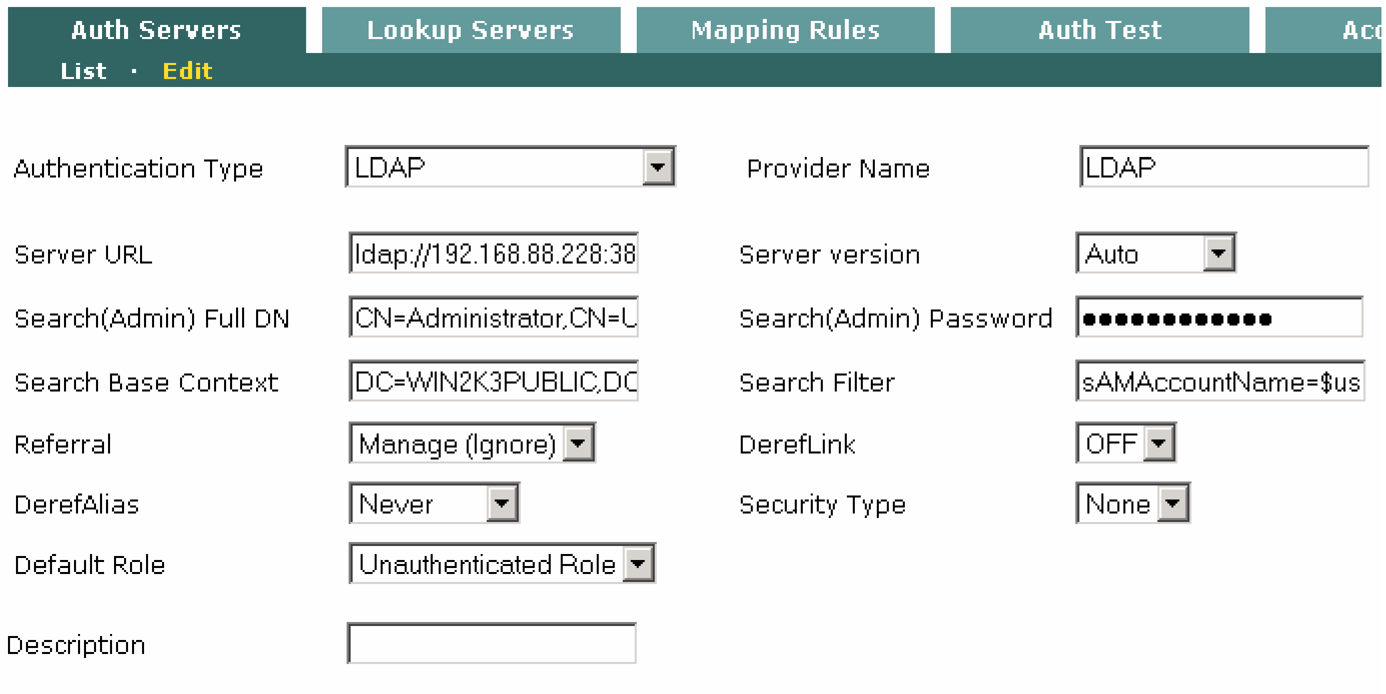
LDAP Basics

Lightweight Directory Access Protocol, or LDAP, is a networking protocol for querying and modifying directory services running over TCP/IP.

- Client-server architecture. LDAP Client talks to Directory Services Server such as Active Directory, e-Directory, iPlanet
- MS Active Directory services supports being queried by LDAP
- LDAP is **preferred method** for authentication and Authorization with AD
- **LDAP queries** are used to get attributes associated with a user such as group that he belongs to, shares he can access, email address, phone number etc.

Configure LDAP Provider

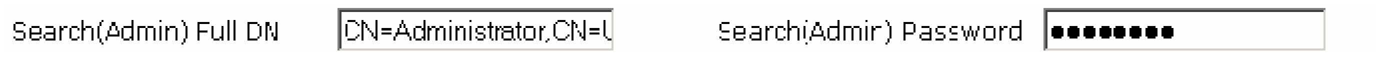
- User Management >> Auth Servers >> New - LDAP



Authentication Type	LDAP	Provider Name	LDAP
Server URL	ldap://192.168.88.228:38	Server version	Auto
Search(Admin) Full DN	CN=Administrator,CN=U	Search(Admin) Password	●●●●●●●●●●●●
Search Base Context	DC=WIN2K3PUBLIC,DC	Search Filter	sAMAccountName=$us
Referral	Manage (Ignore)	DerefLink	OFF
DerefAlias	Never	Security Type	None
Default Role	Unauthenticated Role		
Description			

How LDAP Query works

1) Admin Bind to connect



Search(Admin) Full DN CN=Administrator,CN=U

Search(Admin) Password ●●●●●●●●●

Search Admin DN is : CN=Administrator, CN=Users, DC=WIN2K3SERVER, DC=LOCAL

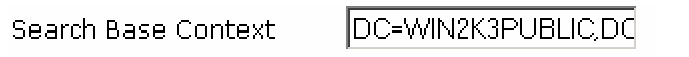
Password = xxxxxxx

- Server **cannot** allow anyone to just connect with LDAP and query it

  - So, we BIND to server by using the credentials for an Account that has privileges to Bind and Query.

2) Use Filters to search for user who is authenticating:-

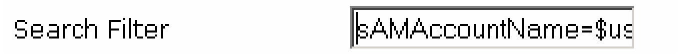
- Where to Start search – Search Base Context



Search Base Context DC=WIN2K3PUBLIC,DC

DC=WIN2K3SERVER, DC=LOCAL

- What naming attribute to search – Search Filter attribute



Search Filter sAMAccountName=$us

sAMAccountName=$userid$

3) Bind again now as that user:- Perform authentication with user provided password and fetch a list of all Attributes – **These will be then used for Mapping Users to Roles – (See Role Mapping later)**

Tips

Distinguished Name (DN): Means the complete path.

- Good analogy will be to think of DN as FQDN
- **Search Admin DN** is complete path to the Account used for initial bind (to begin search)

  In our example : Search Admin DN is : CN=Administrator, CN=Users, DC=WIN2K3PUBLIC, DC=LOCAL
- **Search Base Context (Base DN)** is complete Path to the part of the tree where you want to begin search.

  In our example: Base DN is: ***DC=WIN2K3PUBLIC, DC=LOCAL***

Search Filter Atrribute (Naming Attribute):

This is the attribute based on which the Search will be conducted.

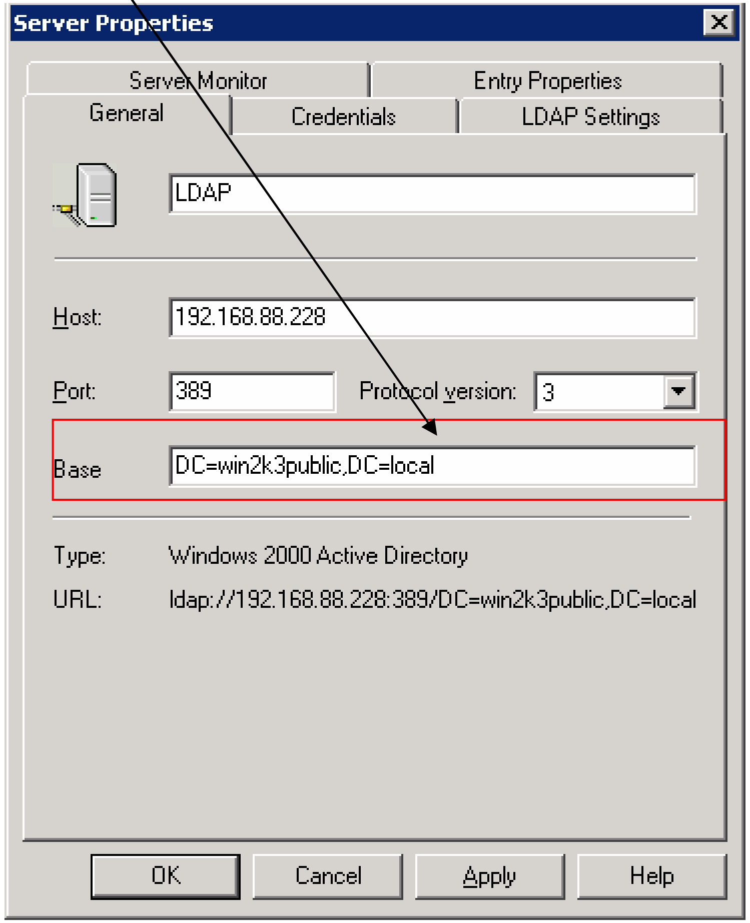
- This can be any attribute in the LDAP tree. Common examples are login names, display names, email-addresses, Phone etc
- The information user provides to authenticate will be used to search the directory. For .eg – If User provides username “test”, the query will search the LDAP tree for an account that has Filter-attribute value = test.
- Most common Search Filter Attribute for Windows AD is sAMAccountName. This attribute stores the login ID of user.

Use Tools such as ADSI Edit (Active Directory Support Tools) and LDAP browser

Use LDAP Browser (www.ldapbrowser.com)

Search Base Context

(Base DN)



LDAP

Host: 192.168.88.228

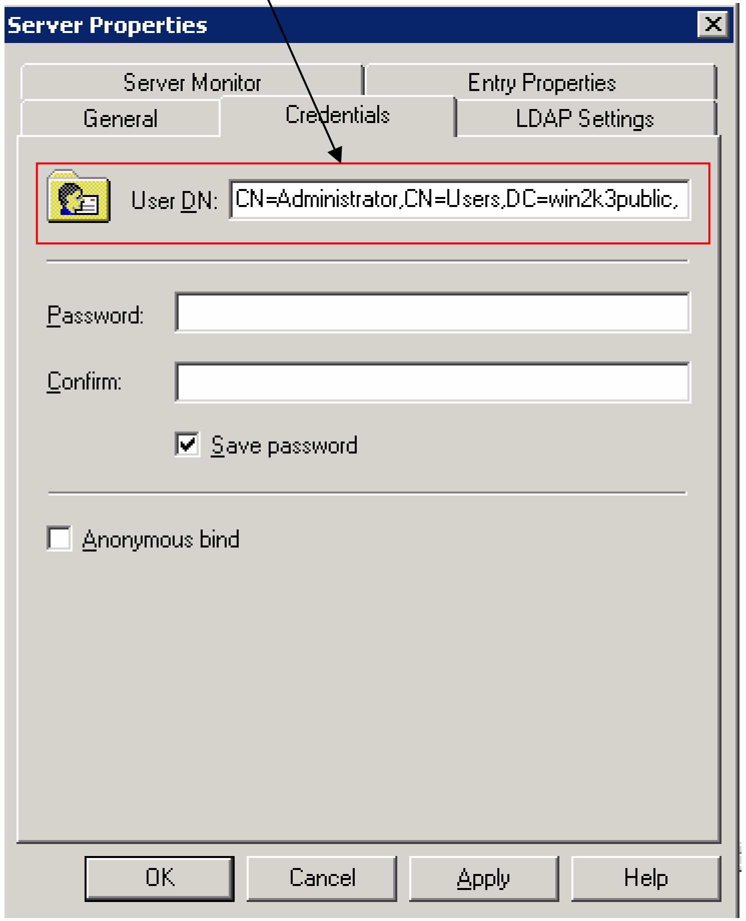
Port: 389 Protocol version: 3

Base DC=win2k3public,DC=local

Type: Windows 2000 Active Directory

URL: ldap://192.168.88.228:389/DC=win2k3public,DC=local

Search Admin DN



User DN: CN=Administrator,CN=Users,DC=win2k3public,

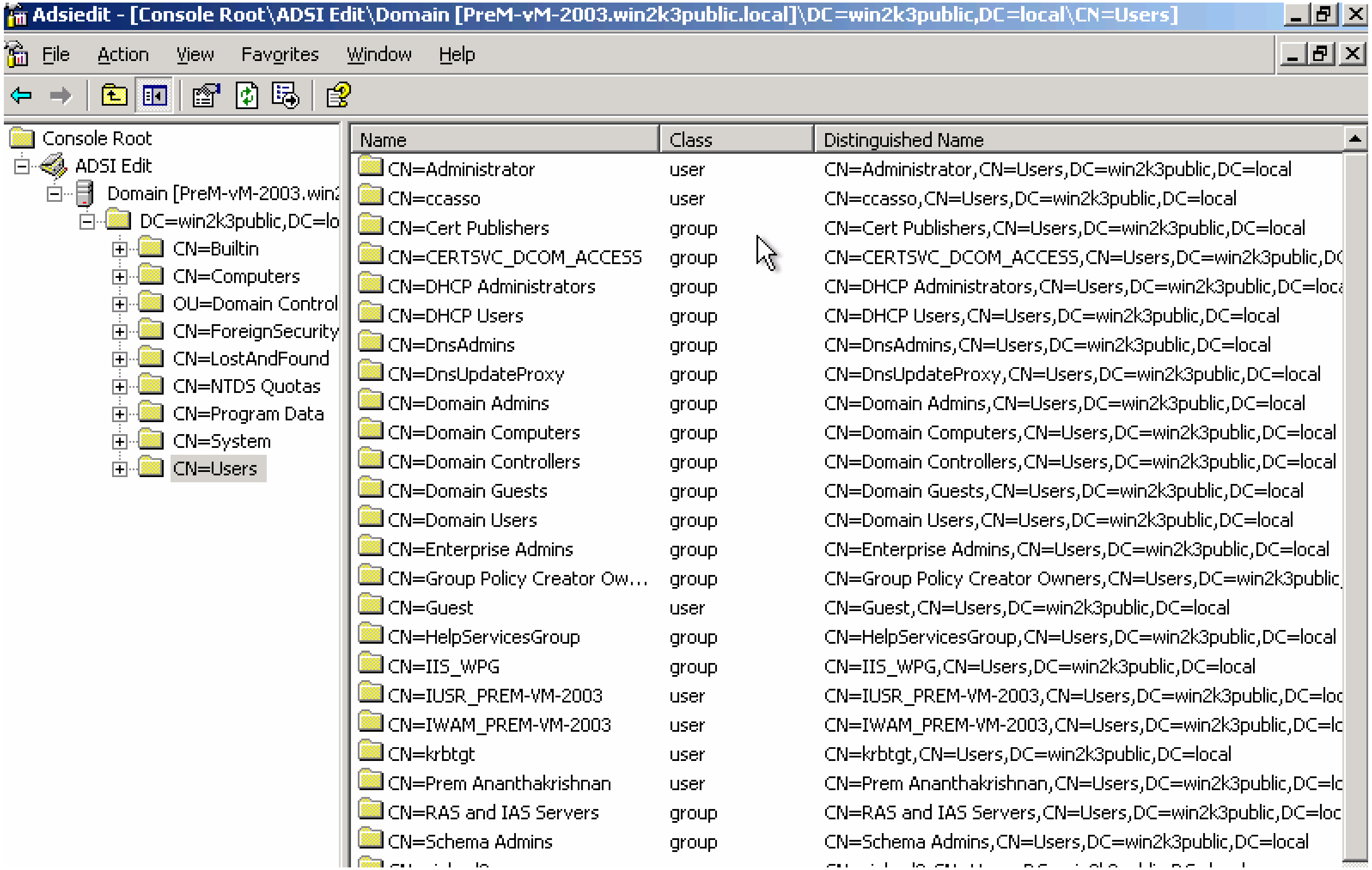
Password:

Confirm:

☑ Save password

☐ Anonymous bind

ADSI Edit to obtain Admin/Base DN

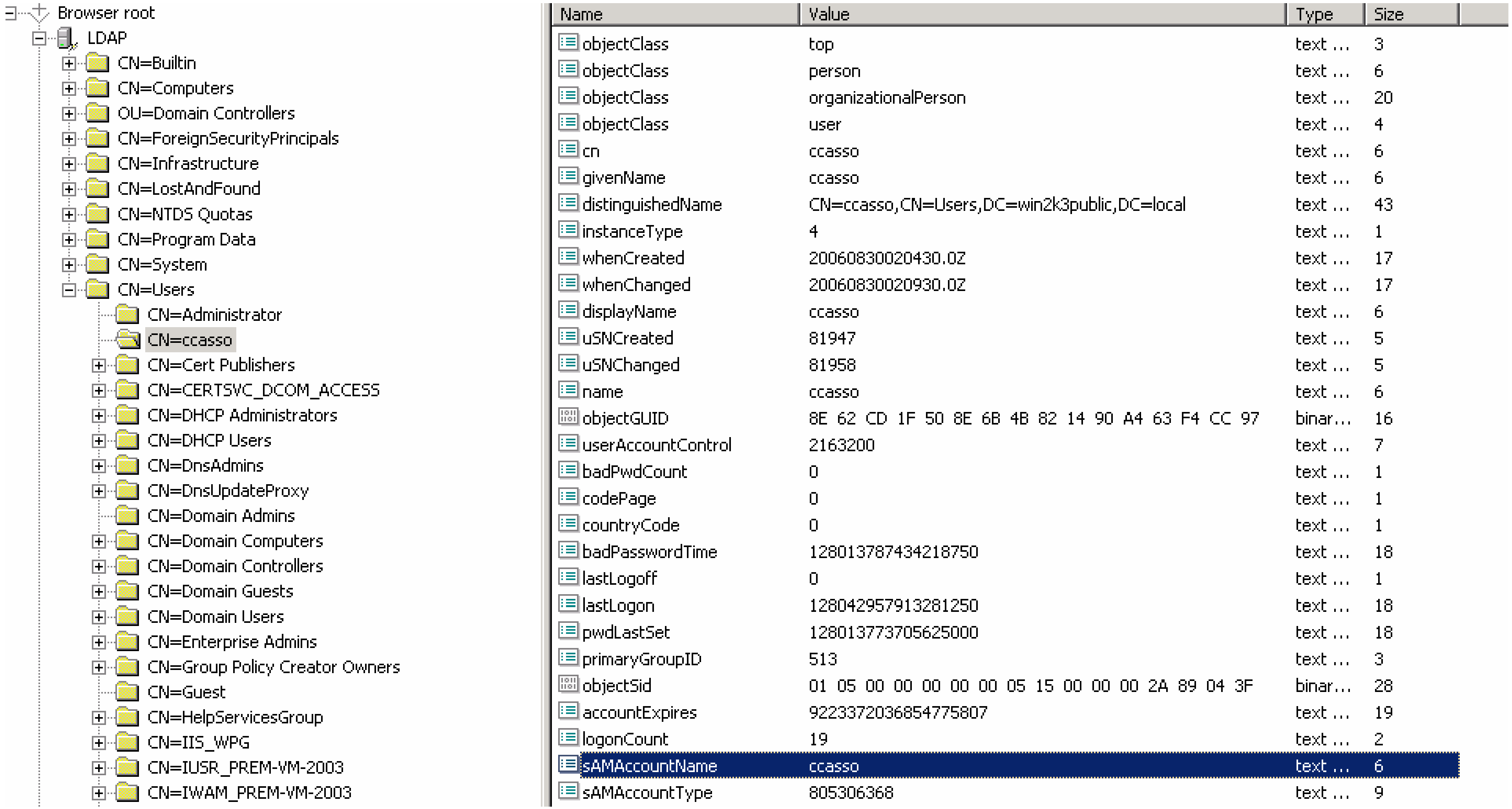


Adsiedit - [Console Root\ADSI Edit\Domain [PreM-vM-2003.win2k3public.local]\DC=win2k3public,DC=local\CN=Users]

- Console Root
  - ADSI Edit
    - Domain [PreM-vM-2003.win2
      - DC=win2k3public,DC=lo
        - CN=Builtin
        - CN=Computers
        - OU=Domain Control
        - CN=ForeignSecurity
        - CN=LostAndFound
        - CN=NTDS Quotas
        - CN=Program Data
        - CN=System
        - CN=Users

Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=win2k3public,DC=local
CN=ccasso	user	CN=ccasso,CN=Users,DC=win2k3public,DC=local
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=win2k3public,DC=local
CN=CERTSVC_DCOM_ACCESS	group	CN=CERTSVC_DCOM_ACCESS,CN=Users,DC=win2k3public,DC
CN=DHCP Administrators	group	CN=DHCP Administrators,CN=Users,DC=win2k3public,DC=loca
CN=DHCP Users	group	CN=DHCP Users,CN=Users,DC=win2k3public,DC=local
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=win2k3public,DC=local
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=win2k3public,DC=local
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=win2k3public,DC=local
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=win2k3public,DC=local
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=win2k3public,DC=local
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=win2k3public,DC=local
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=win2k3public,DC=local
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=win2k3public,DC=local
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=win2k3public
CN=Guest	user	CN=Guest,CN=Users,DC=win2k3public,DC=local
CN=HelpServicesGroup	group	CN=HelpServicesGroup,CN=Users,DC=win2k3public,DC=local
CN=IIS_WPG	group	CN=IIS_WPG,CN=Users,DC=win2k3public,DC=local
CN=IUSR_PREM-VM-2003	user	CN=IUSR_PREM-VM-2003,CN=Users,DC=win2k3public,DC=loc
CN=IWAM_PREM-VM-2003	user	CN=IWAM_PREM-VM-2003,CN=Users,DC=win2k3public,DC=lo
CN=krbtgt	user	CN=krbtgt,CN=Users,DC=win2k3public,DC=local
CN=Prem Ananthakrishnan	user	CN=Prem Ananthakrishnan,CN=Users,DC=win2k3public,DC=lo
CN=RAS and IAS Servers	group	CN=RAS and IAS Servers,CN=Users,DC=win2k3public,DC=loc
CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=win2k3public,DC=local

Attributes for Search Filter

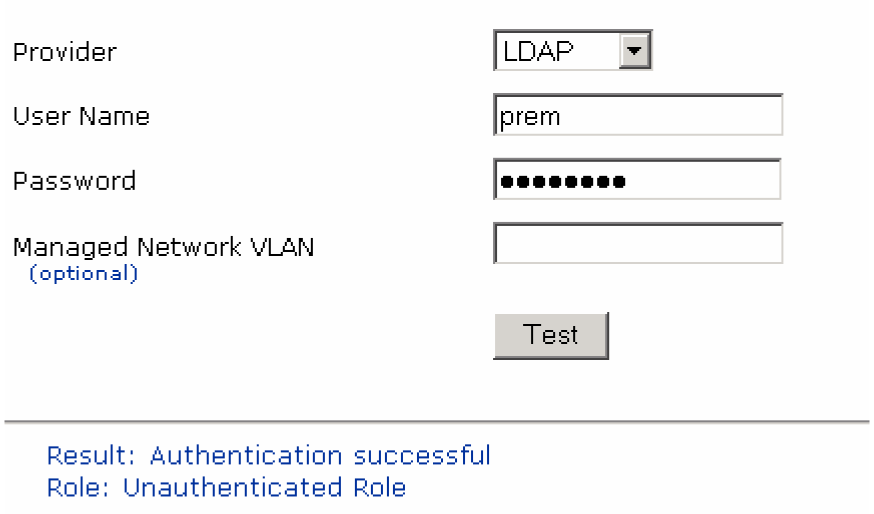


- Browser root
  - LDAP
    - CN=Builtin
    - CN=Computers
    - OU=Domain Controllers
    - CN=ForeignSecurityPrincipals
    - CN=Infrastructure
    - CN=LostAndFound
    - CN=NTDS Quotas
    - CN=Program Data
    - CN=System
    - CN=Users
      - CN=Administrator
      - CN=ccasso
      - CN=Cert Publishers
      - CN=CERTSVC_DCOM_ACCESS
      - CN=DHCP Administrators
      - CN=DHCP Users
      - CN=DnsAdmins
      - CN=DnsUpdateProxy
      - CN=Domain Admins
      - CN=Domain Computers
      - CN=Domain Controllers
      - CN=Domain Guests
      - CN=Domain Users
      - CN=Enterprise Admins
      - CN=Group Policy Creator Owners
      - CN=Guest
      - CN=HelpServicesGroup
      - CN=IIS_WPG
      - CN=IUSR_PREM-VM-2003
      - CN=IWAM_PREM-VM-2003

Name	Value	Type	Size
objectClass	top	text ...	3
objectClass	person	text ...	6
objectClass	organizationalPerson	text ...	20
objectClass	user	text ...	4
cn	ccasso	text ...	6
givenName	ccasso	text ...	6
distinguishedName	CN=ccasso,CN=Users,DC=win2k3public,DC=local	text ...	43
instanceType	4	text ...	1
whenCreated	20060830020430.0Z	text ...	17
whenChanged	20060830020930.0Z	text ...	17
displayName	ccasso	text ...	6
uSNCreated	81947	text ...	5
uSNChanged	81958	text ...	5
name	ccasso	text ...	6
objectGUID	8E 62 CD 1F 50 8E 6B 4B 82 14 90 A4 63 F4 CC 97	binar...	16
userAccountControl	2163200	text ...	7
badPwdCount	0	text ...	1
codePage	0	text ...	1
countryCode	0	text ...	1
badPasswordTime	128013787434218750	text ...	18
lastLogoff	0	text ...	1
lastLogon	128042957913281250	text ...	18
pwdLastSet	128013773705625000	text ...	18
primaryGroupID	513	text ...	3
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 2A 89 04 3F	binar...	28
accountExpires	9223372036854775807	text ...	19
logonCount	19	text ...	2
sAMAccountName	ccasso	text ...	6
sAMAccountType	805306368	text ...	9

Auth Test - LDAP

Perform Auth Test against the LDAP provider to confirm authentication works – User Management >> Auth Servers >> Auth Test



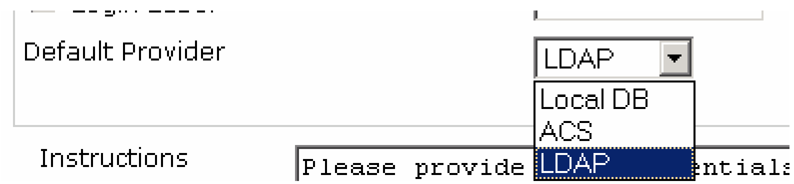
Provider	LDAP
User Name	prem
Password	●●●●●●●●●
Managed Network VLAN (optional)	

Result: Authentication successful
Role: Unauthenticated Role

If Auth Test fails, then go back and check your Admin DN, Search base context and search filter.

Add Provider to User Pages

- Ensure your provider is selected in the User Pages section in one of the following ways

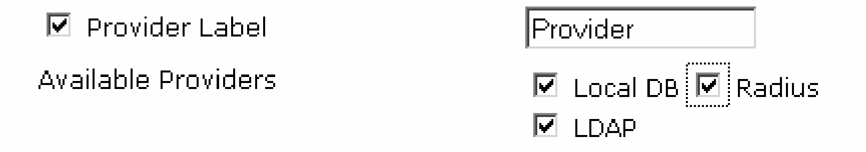


Default Provider LDAP

Local DB
ACS
LDAP

Instructions Please provide entials

By choosing your default Provider as the server you want to authenticate against. In this example, this is the provider called LDAP



☑ Provider Label Provider

Available Providers ☑ Local DB ☑ Radius ☑ LDAP

By checking the option for Provider label and then selecting the available providers as shown. This option will be used when you have more than one external database to authenticate against. Users will pick the database they have to log into

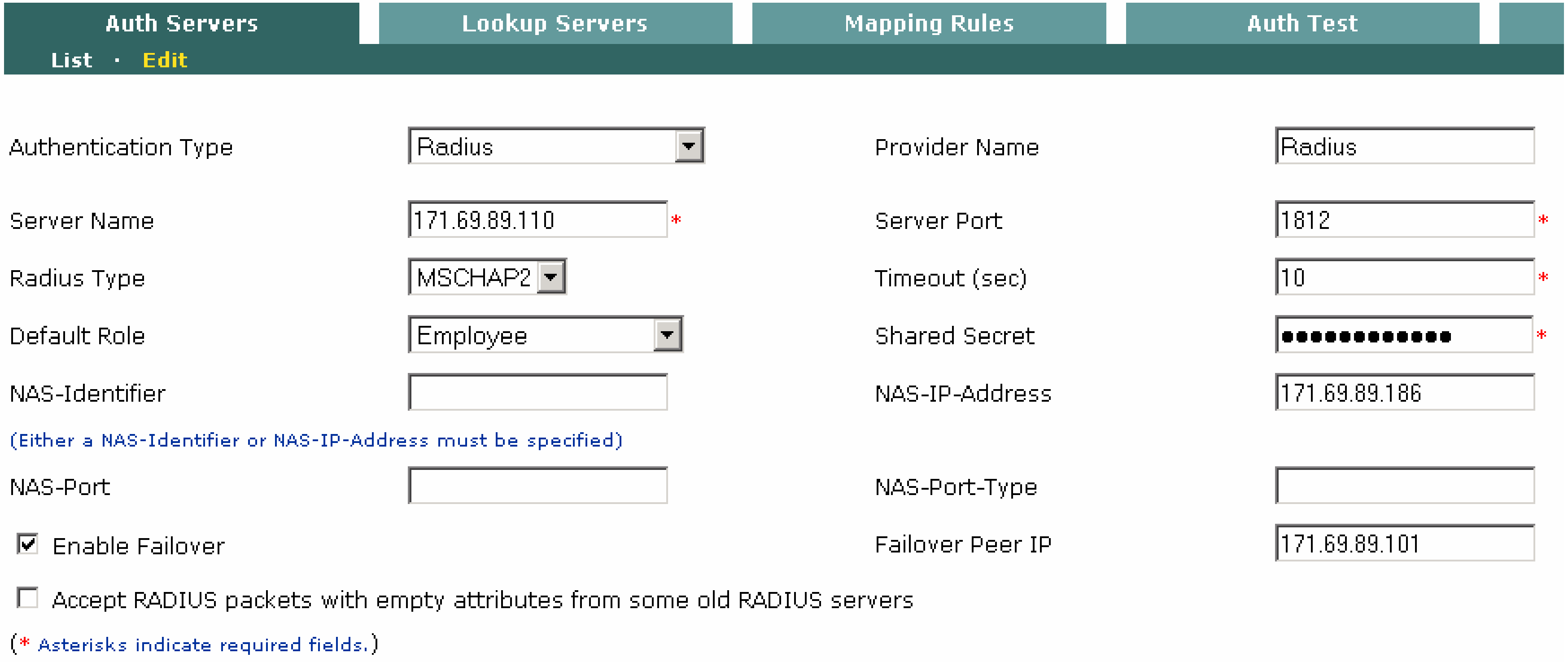
Authentication methods

Radius

Radius Authentication

- Multiple Radius servers can be specified for fallback
- Mapping can be done based on Radius Attributes (See Role Mapping later)

User Management >> Auth Servers >> New - Radius



Authentication Type	Radius	Provider Name	Radius
Server Name	171.69.89.110 *	Server Port	1812 *
Radius Type	MSCHAP2	Timeout (sec)	10 *
Default Role	Employee	Shared Secret	●●●●●●●●●●●● *
NAS-Identifier		NAS-IP-Address	171.69.89.186

(Either a NAS-Identifier or NAS-IP-Address must be specified)

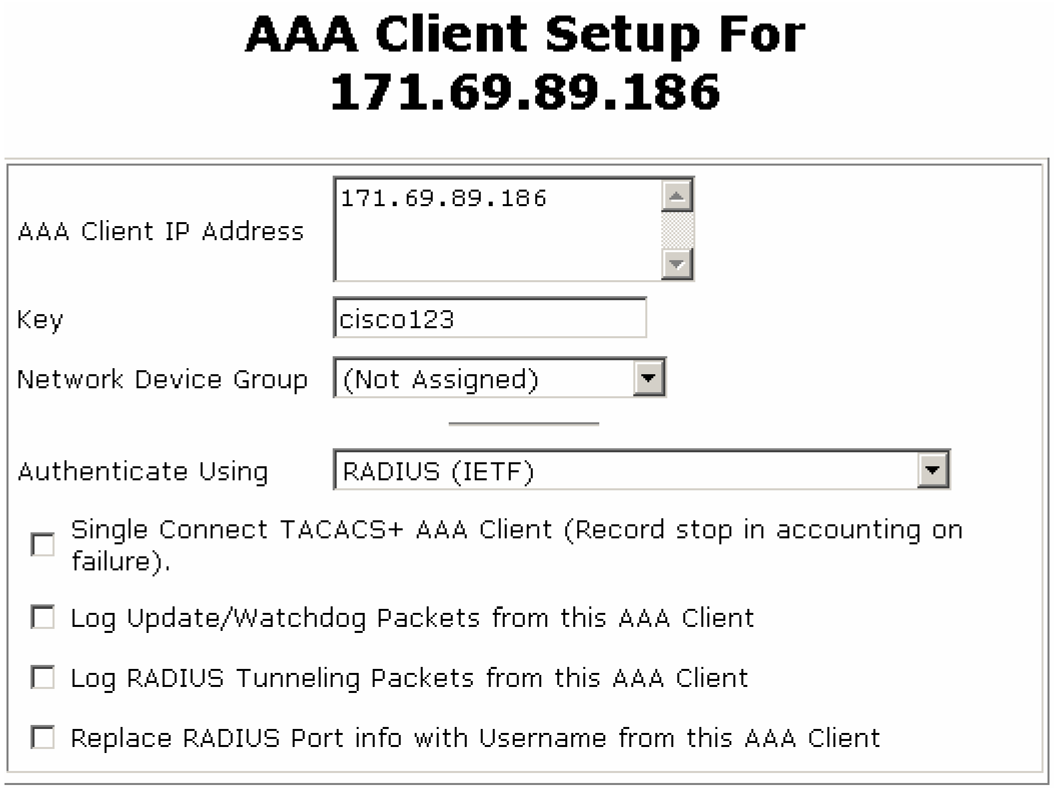
NAS-Port		NAS-Port-Type	
☑ Enable Failover		Failover Peer IP	171.69.89.101

□ Accept RADIUS packets with empty attributes from some old RADIUS servers

(* Asterisks indicate required fields.)

Radius Authentication

- Setup the CAM as NAS/AAA client on Radius server.



AAA Client Setup For 171.69.89.186

AAA Client IP Address: 171.69.89.186

Key: cisco123

Network Device Group: (Not Assigned)

Authenticate Using: RADIUS (IETF)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

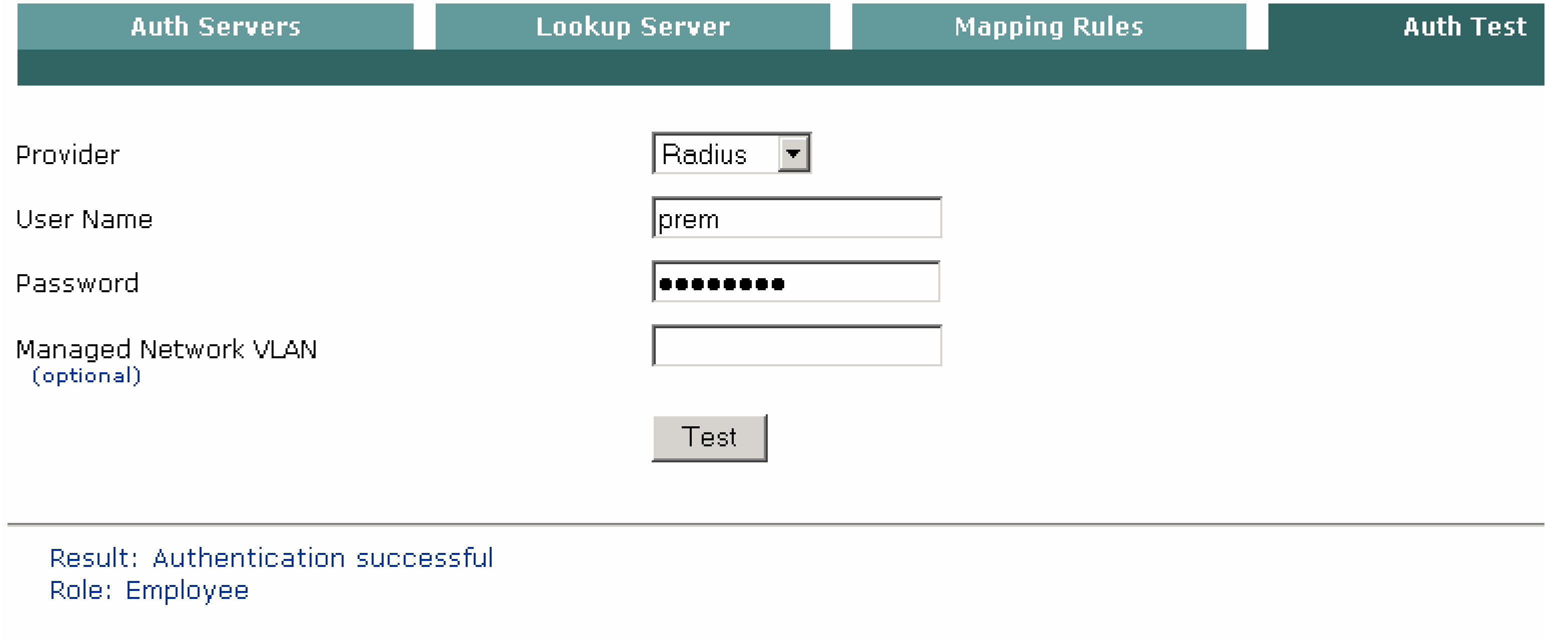
□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

Auth Test - Radius

Perform Auth Test against the Radius provider to confirm authentication/mapping works – User Management >> Auth Servers >> Auth Test



Provider: Radius

User Name: prem

Password: ●●●●●●●●●

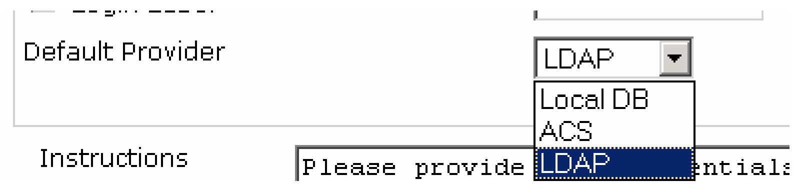
Managed Network VLAN (optional):

Result: Authentication successful
Role: Employee

If Auth Test fails, then go back and check your Shared secret, Radius server IP.

Add Provider to User Pages

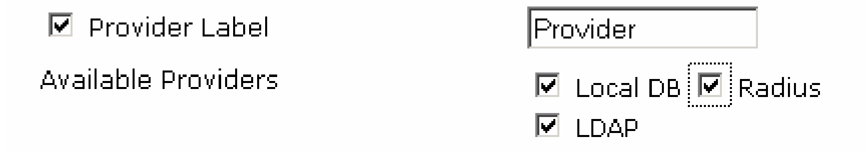
- Ensure your provider is selected in the User Pages section in one of the following ways



Default Provider LDAP

Instructions Please provide entials

By choosing your default Provider as the server you want to authenticate against. In this example, this is the provider called LDAP



☑ Provider Label Provider

Available Providers ☑ Local DB ☑ Radius ☑ LDAP

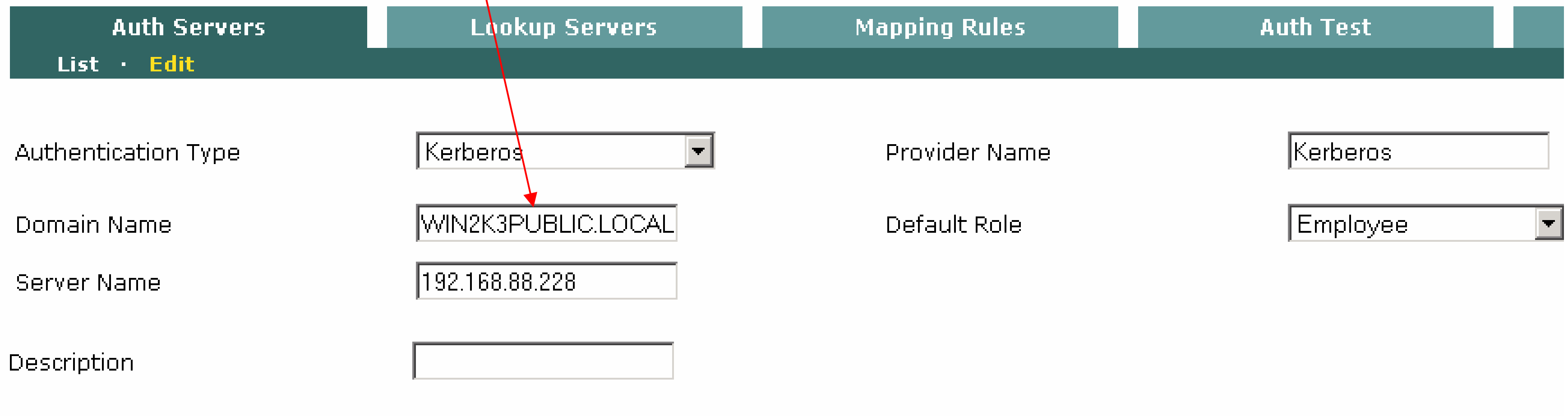
By checking the option for Provider label and then selecting the available providers as shown. This option will be used when you have more than one external database to authenticate against. Users will pick the database they have to log into

Authentication methods

Kerberos and NTLM

Kerberos

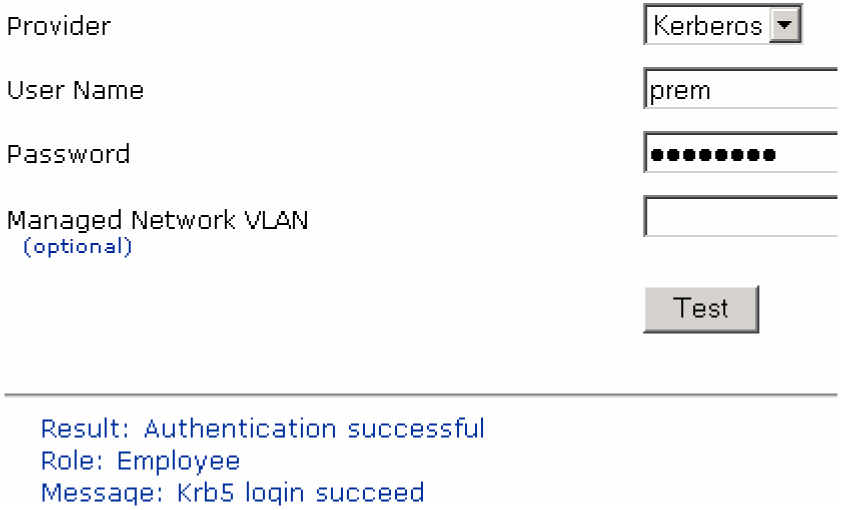
- Can be used against Active Directory or any Kerberos server
- Pure Authentication ONLY. Cannot perform **Attribute based** role mapping like LDAP/Radius. Hence not preferred.
- Make Sure Kerberos REALM is in CAPS



Authentication Type	Kerberos	Provider Name	Kerberos
Domain Name	WIN2K3PUBLIC.LOCAL	Default Role	Employee
Server Name	192.168.88.228		
Description			

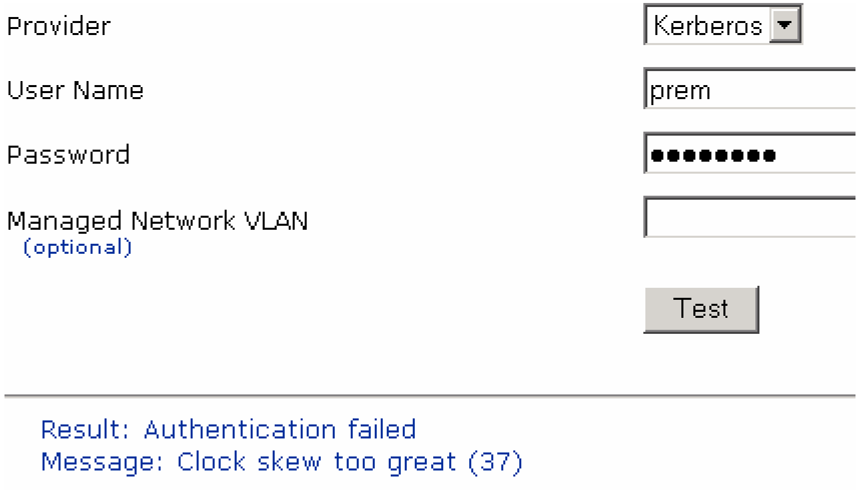
Auth Test - Kerberos

Perform Auth Test against Kerberos provider to confirm authentication works



Provider	Kerberos ▾
User Name	prem
Password	●●●●●●●●●
Managed Network VLAN (optional)	

Result: Authentication successful
Role: Employee
Message: Krb5 login succeed



Provider	Kerberos ▾
User Name	prem
Password	●●●●●●●●●
Managed Network VLAN (optional)	

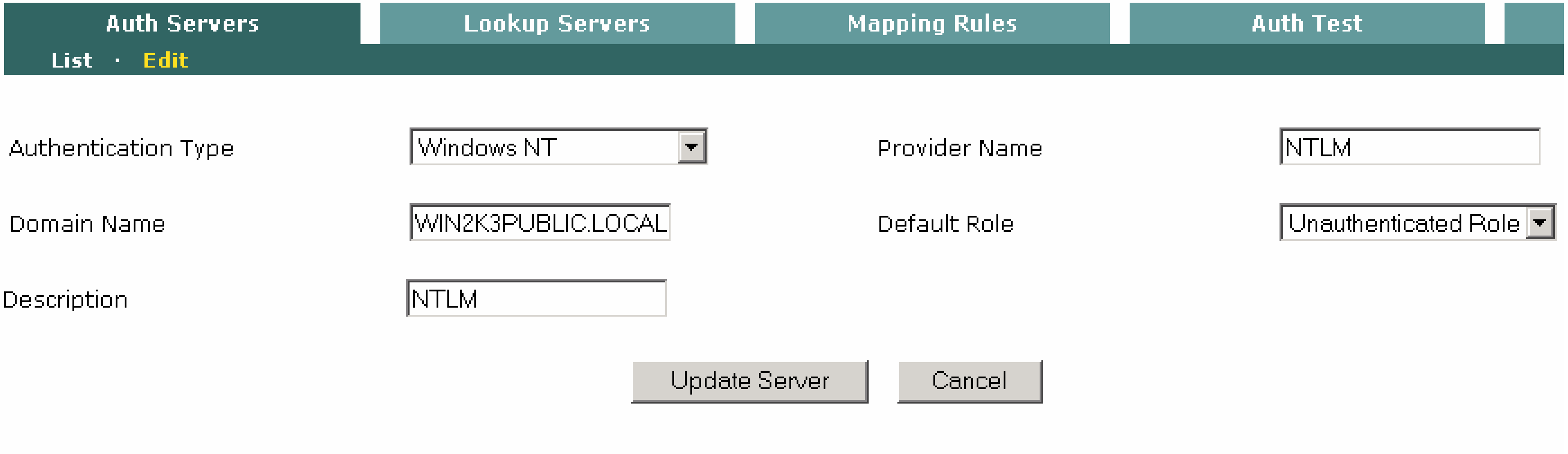
Result: Authentication failed
Message: Clock skew too great (37)

Kerberos is CLOCK sensitive. Make sure time on CAM is synchronized with Kerberos server (DC)

CAM can be synchronized with NTP server under CCA Manager >> System Time >> Time Servers

NTLM

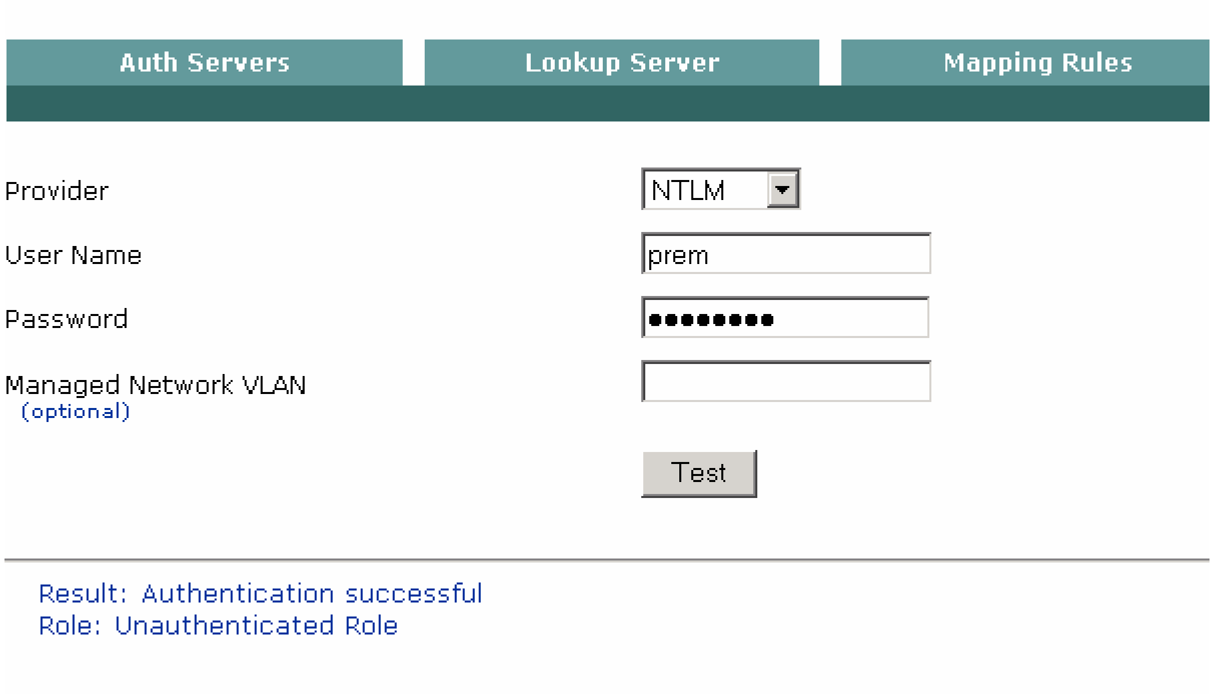
- Used with old Windows NT servers which do NOT support Active Directory
- Uses Netbios-Session for Authentication
- Pure Authentication ONLY. Cannot perform **Attribute based** role mapping like LDAP/Radius. Hence not preferred.



Authentication Type	Windows NT	Provider Name	NTLM
Domain Name	WIN2K3PUBLIC.LOCAL	Default Role	Unauthenticated Role
Description	NTLM		

Auth Test - NTLM

Perform Auth Test against the NTLM provider to confirm authentication/mapping works – User Management >> Auth Servers >> Auth Test



Provider: NTLM

User Name: prem

Password: ●●●●●●●●●

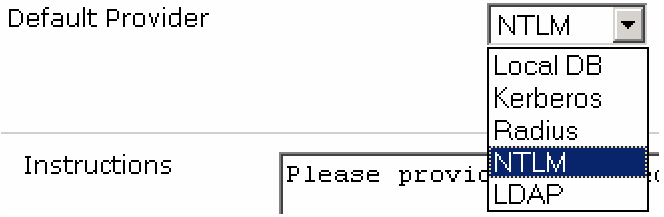
Managed Network VLAN (optional):

Result: Authentication successful

Role: Unauthenticated Role

Add Provider to User Pages

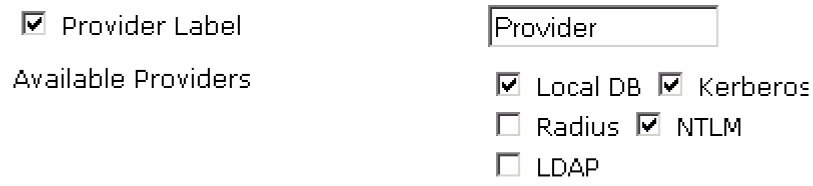
- Ensure your provider is selected in the User Pages section in one of the following ways



Default Provider NTLM

Instructions Please provid

By choosing your default Provider as the server you want to authenticate against. In this example, this is the provider called NTLM



☑ Provider Label Provider

Available Providers ☑ Local DB ☑ Kerberos ☐ Radius ☑ NTLM ☐ LDAP

By checking the option for Provider label and then selecting the available providers as shown. This option will be used when you have more than one external database to authenticate against. Users will pick the database they have to log into

Authentication methods

SSO (VPN and AD)

VPN and AD SSO

VPN SSO

- Uses Radius Accounting.
- Applies to both Agent and Agentless users

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a008074d641.shtml

AD SSO

- Based on Kerberos (Uses Windows Credentials to log you on to NAC Appliance
- Requires use of Clean Access Agent
- Covered in detail later in Section 4

Authentication methods

Guest

Guest Authentication Methods

Guest Button (One-Click Authentication)

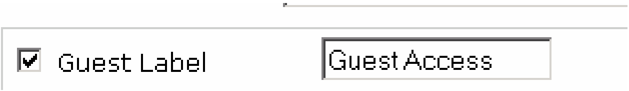
- User clicks “Guest” button on browser and gets authenticated.
- Placed in a Guest role automatically

Allow All (Email Address/Name based authentication)

- Can accept email/Name from user to allow login.
- Provides information for logging purposes.
- Uses the Allow All Provider to achieve this

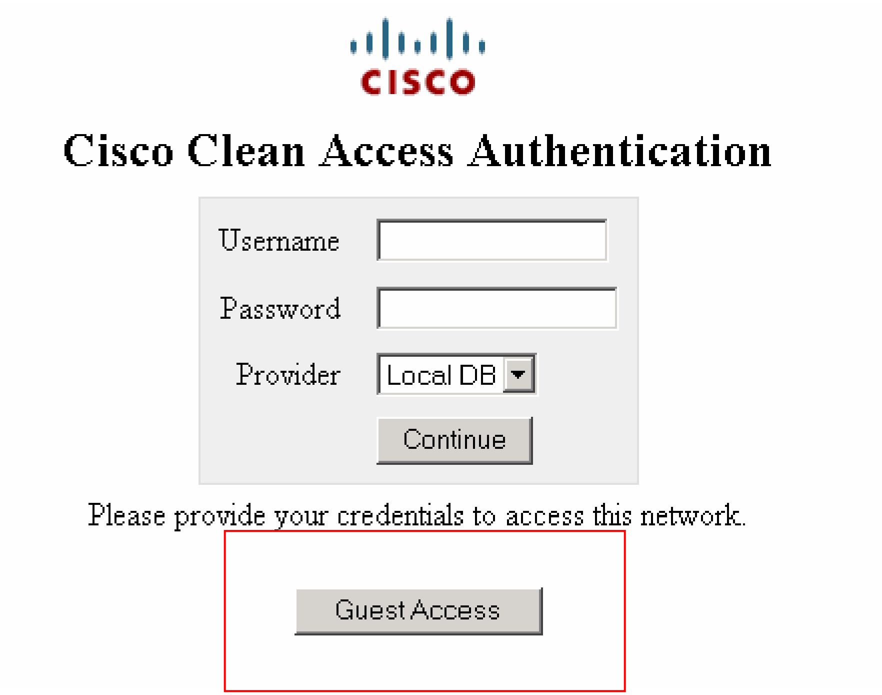
Guest Button: Configure User Pages

- Select the Guest Label under Administration >> User pages >> Edit >> Content



☑ Guest Label: Guest Access

- This will ensure that the Guest Button is displayed to the user when they open the browser as shown below



Cisco Clean Access Authentication

Username

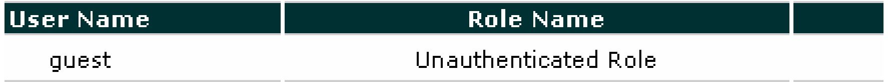
Password

Provider: Local DB

Please provide your credentials to access this network.

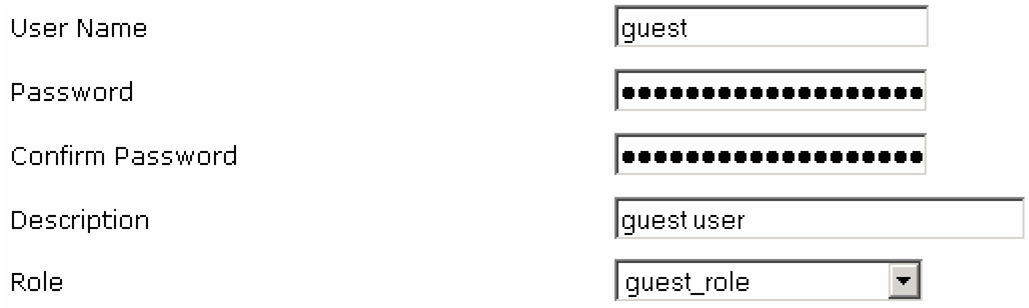
Guest Button: Create Guest Role

- There should be a default “LOCAL” account on the CAM with the username as “guest” and password as “guest”



User Name	Role Name	
guest	Unauthenticated Role	

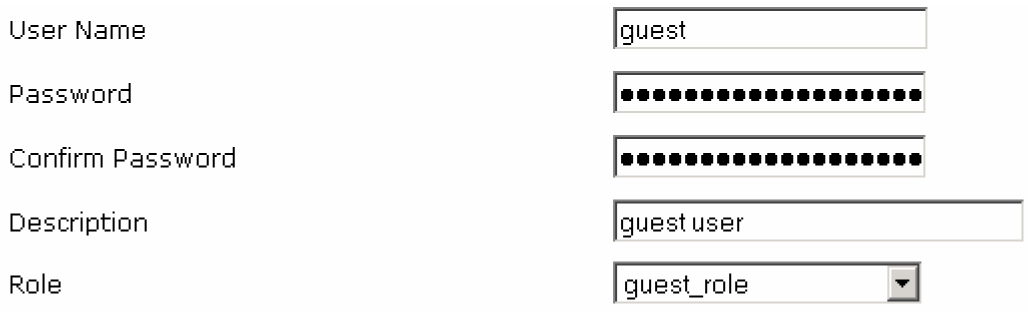
- The guest button uses this username and password in effect to login
- Create a new role for Guests say “guest_role” (User Management >> User Roles >> New role) and associate guest account to that role.



User Name	guest
Password	●●●●●●●●●●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●●●●●●●●●●
Description	guest user
Role	guest_role

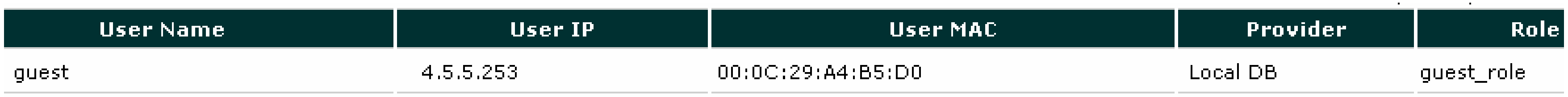
Guest Button: Create Role and Apply

- Create a new role for Guests say “guest_role” (User Management >> User Roles >> New role) and associate guest account to that role.



User Name	guest
Password	●●●●●●●●●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●●●●●●●●●
Description	guest user
Role	guest_role ▾

- You can apply ACLs, BW control, Guest VLAN*** on the guest_role so that it applies ONLY to guest users.
- Guest users show up on online user list as below

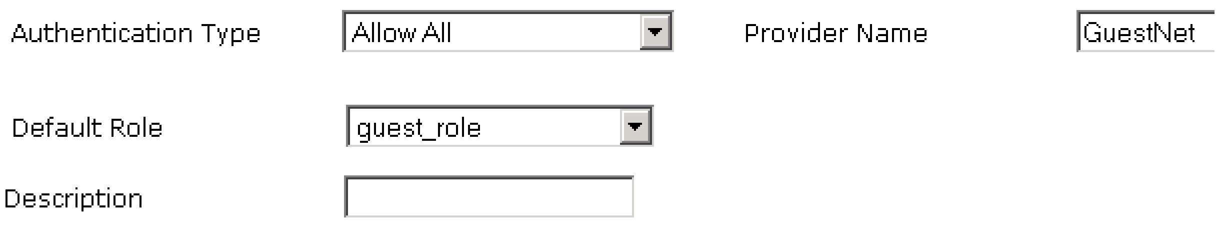


User Name	User IP	User MAC	Provider	Role
guest	4.5.5.253	00:0C:29:A4:B5:D0	Local DB	guest_role

Note: Dynamic guest VLAN applies to OOB only. ACLs, BW control on CAS apply only when traffic is passing through the CAS

Allow All: Configure Provider

- Add a new Auth Provider of the type "Allow All" and assign it to the guest role



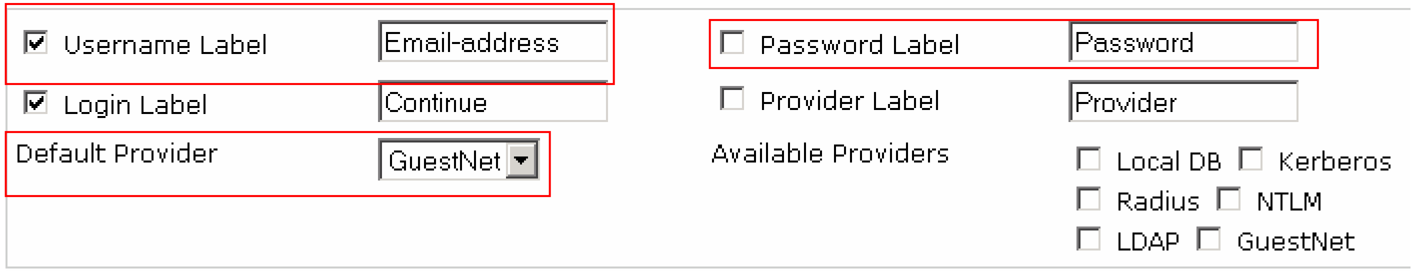
Authentication Type: Allow All

Provider Name: GuestNet

Default Role: guest_role

Description:

- On Administration>>User Pages>>Content, rename "Username Label" to E-mail-address as shown. Also, uncheck the Password Label box and pick the Default Provider as the Guestnet as configured above



☑ Username Label: Email-address

☑ Login Label: Continue

Default Provider: GuestNet

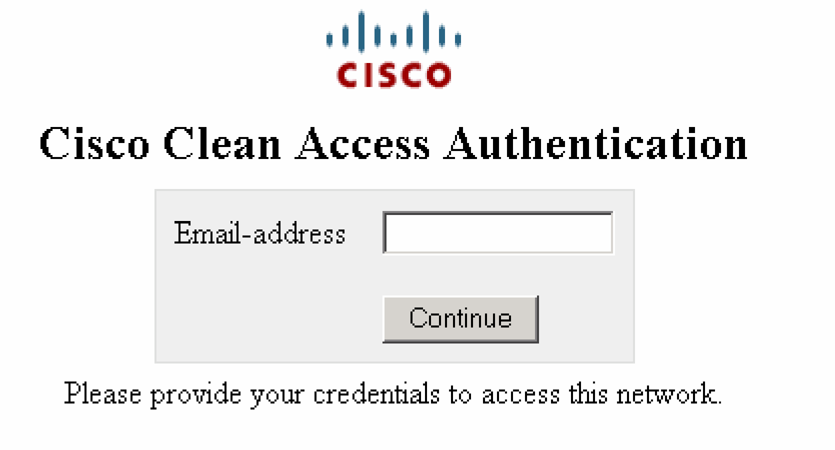
☐ Password Label: Password

☐ Provider Label: Provider

Available Providers: ☐ Local DB ☐ Kerberos ☐ Radius ☐ NTLM ☐ LDAP ☐ GuestNet

Allow All : User login Page

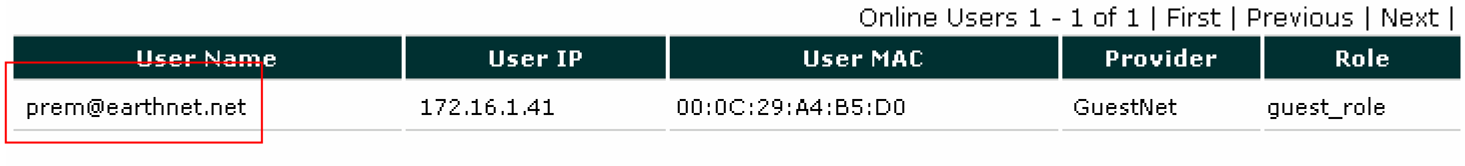
- The end user will now see a screen as follows when he opens up the browser



Cisco Clean Access Authentication

Please provide your credentials to access this network.

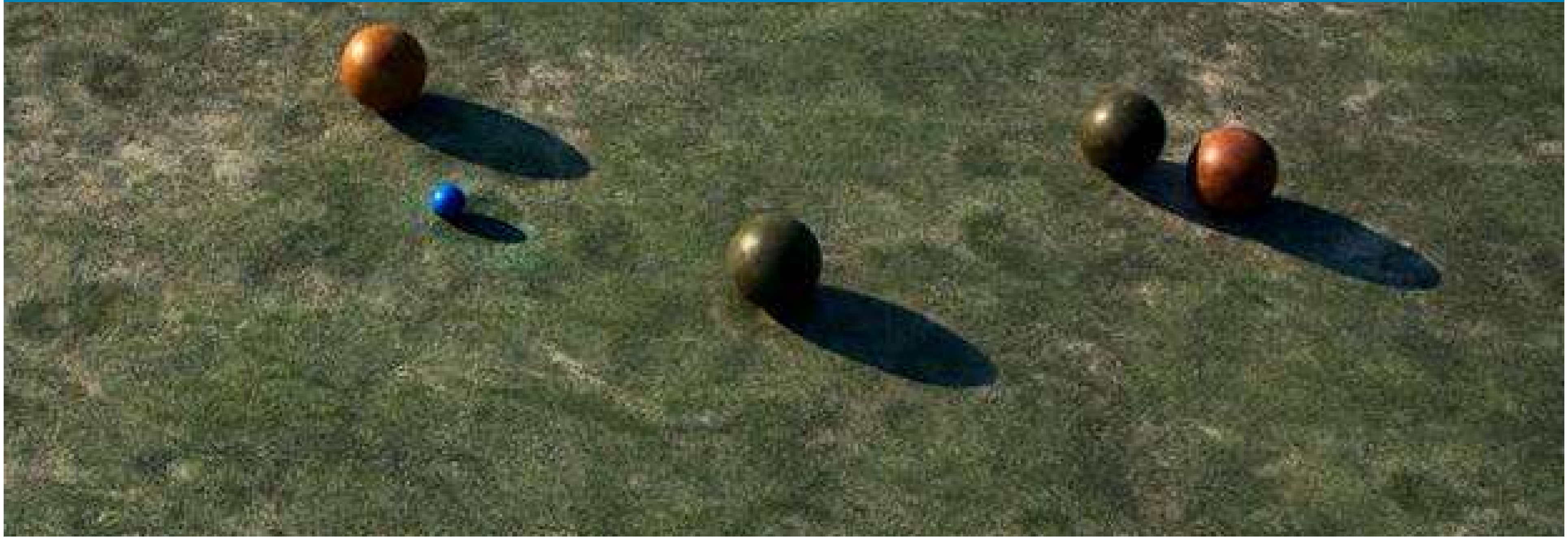
- User shows up in the online User list with the email address what was entered



Online Users 1 - 1 of 1 | First | Previous | Next |

User Name	User IP	User MAC	Provider	Role
prem@earthnet.net	172.16.1.41	00:0C:29:A4:B5:D0	GuestNet	guest_role

Authorization via Role Mapping



Authorization via Role Mapping

Types

Dynamic Role Mapping

- Dynamic Role mapping is a very important piece.
- Role mapping can be used to place users into different Roles based on whether they are an Employee OR Contractor OR Guests
- Authorization such as Dynamic VLAN assignment (OOB), Traffic Filters, Differentiated Policies (AV rules, Hotfixes etc) are applied based on the final Role the user is placed on
- There are 2 types of Dynamic Role mapping

  1) Source VLAN based Role Mapping

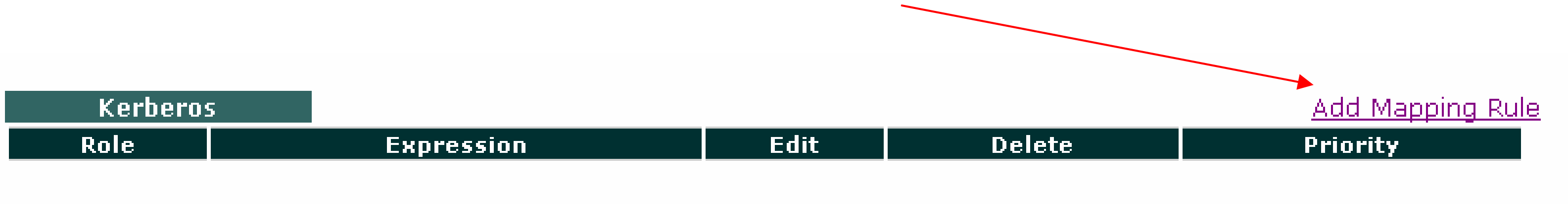
  2) Attribute based Role mapping (Radius/LDAP/SSO)

Authorization via Role Mapping

Source VLAN

Source VLAN based Role Mapping

- Applies to All Auth Providers
- Can place users into roles based on the Incoming or source VLAN of the traffic
- E.g. If the user is coming from Building A (VLAN 120 OR VLAN 230) place him in RoleA. If he is coming from Building B (Vlan 600), place him in RoleB.
- NAC Appliance will read the VLAN tag on the incoming packet and make a decision
- Under User Management >> Auth Server >> Mapping Rules, click on “Add mapping rule under your provider



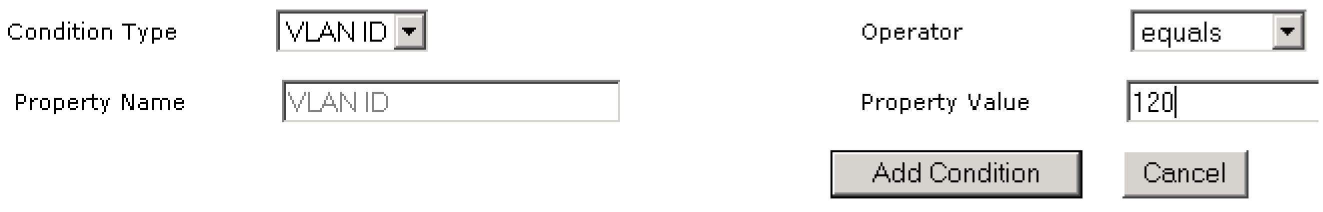
Kerberos

Add Mapping Rule

Role	Expression	Edit	Delete	Priority

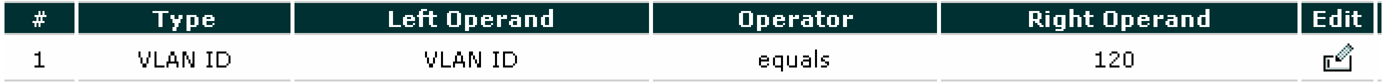
Add Condition

- Select Condition Type = VLAN ID and add the condition for Source VLAN=120 as follows



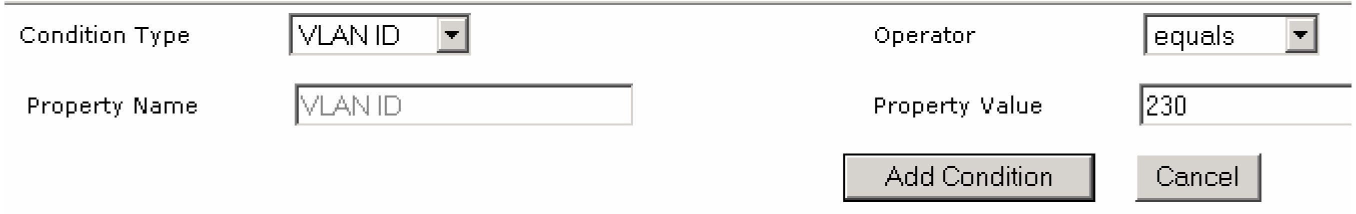
Condition Type	VLAN ID	Operator	equals
Property Name	VLAN ID	Property Value	120

- This condition appears below as follows



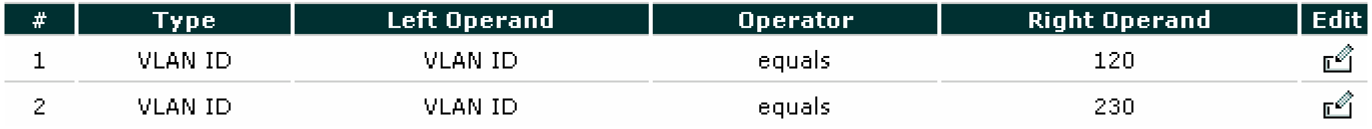
#	Type	Left Operand	Operator	Right Operand	Edit
1	VLAN ID	VLAN ID	equals	120	✎

- Similarly add a condition for VLAN 230



Condition Type	VLAN ID	Operator	equals
Property Name	VLAN ID	Property Value	230

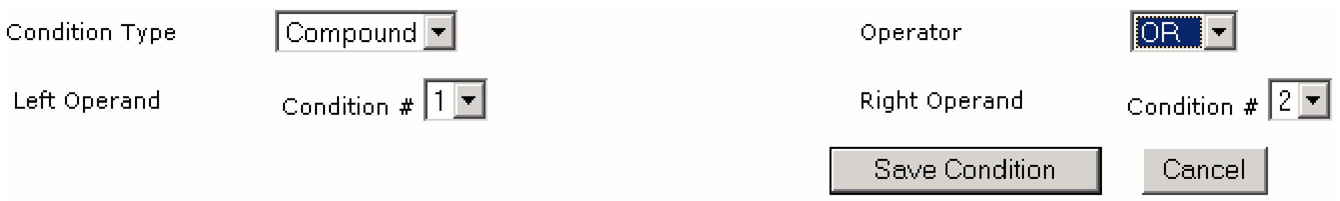
- Net result looks as below:



#	Type	Left Operand	Operator	Right Operand	Edit
1	VLAN ID	VLAN ID	equals	120	✎
2	VLAN ID	VLAN ID	equals	230	✎

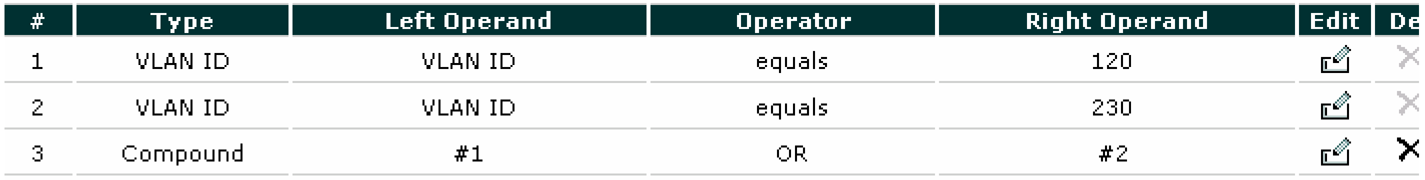
Compound conditions

- Now Use compound to combine the conditions



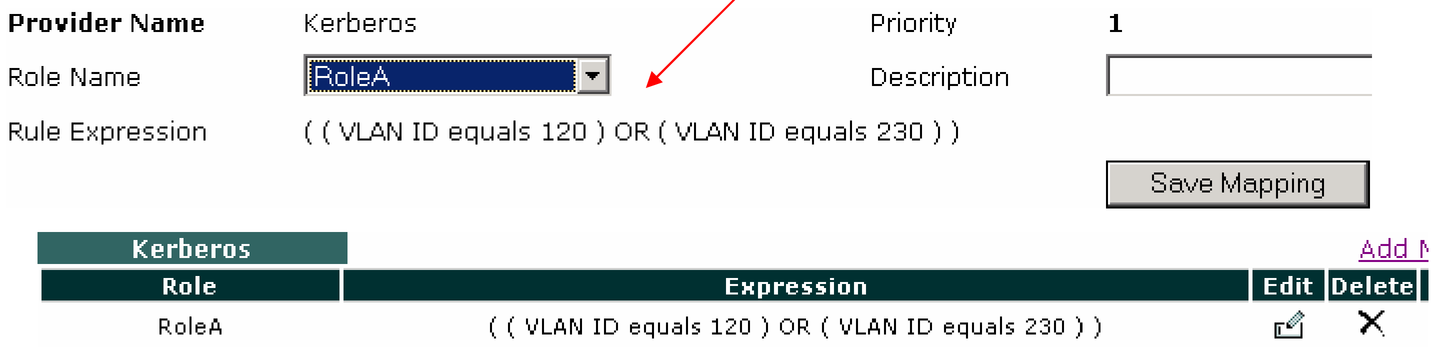
Condition Type	Compound ▾	Operator	OR ▾
Left Operand	Condition # 1 ▾	Right Operand	Condition # 2 ▾

- Compounded condition is as follows



#	Type	Left Operand	Operator	Right Operand	Edit	De
1	VLAN ID	VLAN ID	equals	120	✎	×
2	VLAN ID	VLAN ID	equals	230	✎	×
3	Compound	#1	OR	#2	✎	×

- Now pick the role you want to apply this to (RoleA) and click Add Mapping. Note the Rule Expression.

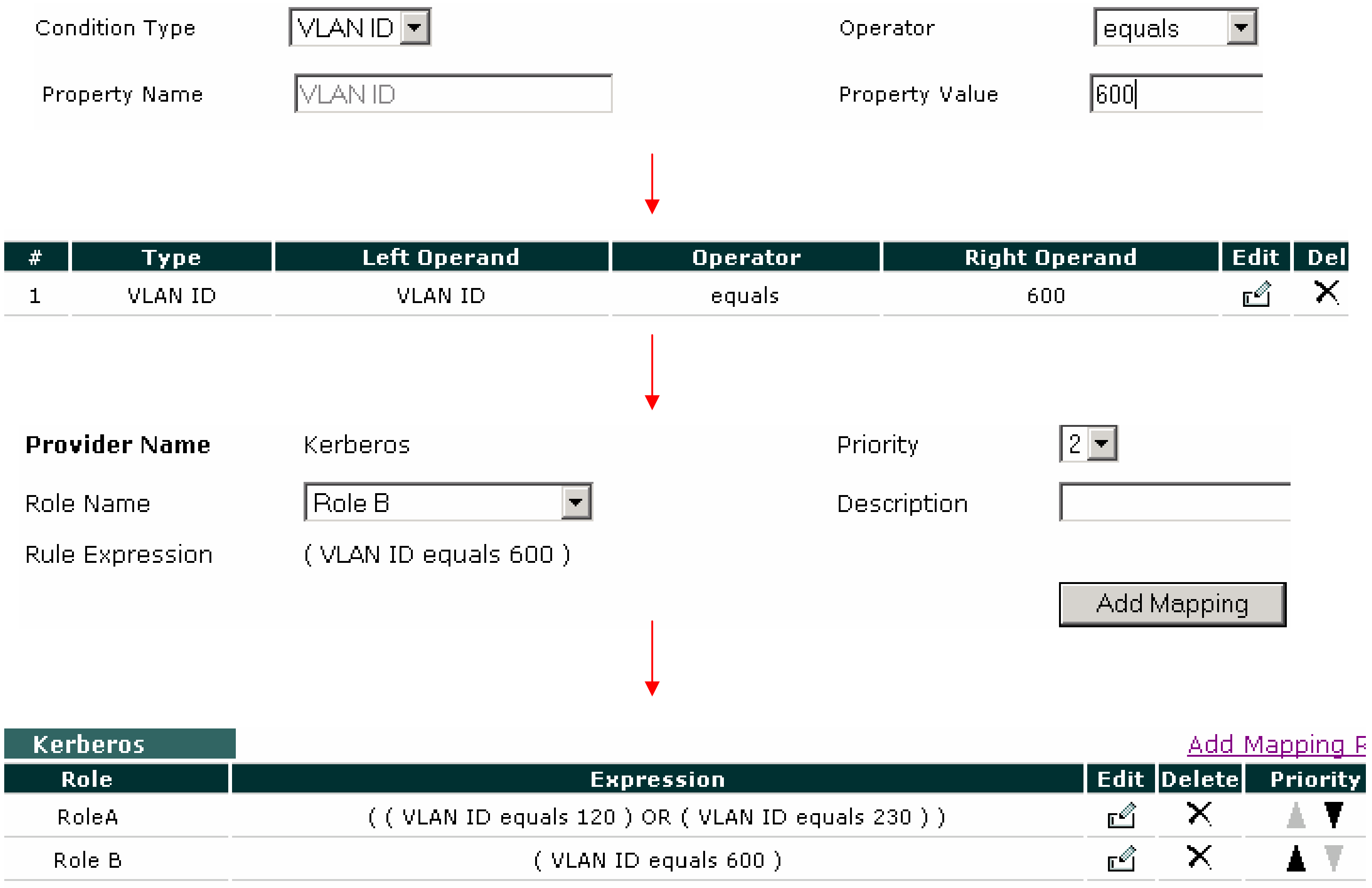


Provider Name	Kerberos	Priority	**1**
Role Name	RoleA ▾	Description	
Rule Expression	((VLAN ID equals 120) OR (VLAN ID equals 230))		

Role	Expression	Edit	Delete
RoleA	((VLAN ID equals 120) OR (VLAN ID equals 230))	✎	×

Multiple conditions

- Following similar steps for Role B, Source VLAN=600 as follows



Condition Type	VLAN ID	Operator	equals
Property Name	VLAN ID	Property Value	600

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	VLAN ID	VLAN ID	equals	600		✕

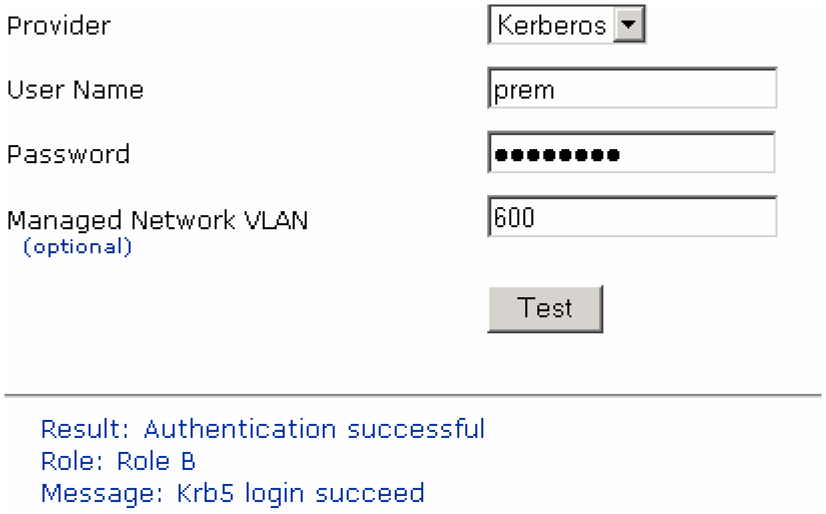
Provider Name	Kerberos	Priority	2
Role Name	Role B	Description	
Rule Expression	(VLAN ID equals 600)		

Kerberos

Role	Expression	Edit	Delete	Priority
RoleA	((VLAN ID equals 120) OR (VLAN ID equals 230))		✕	▲ ▼
Role B	(VLAN ID equals 600)		✕	▲ ▼

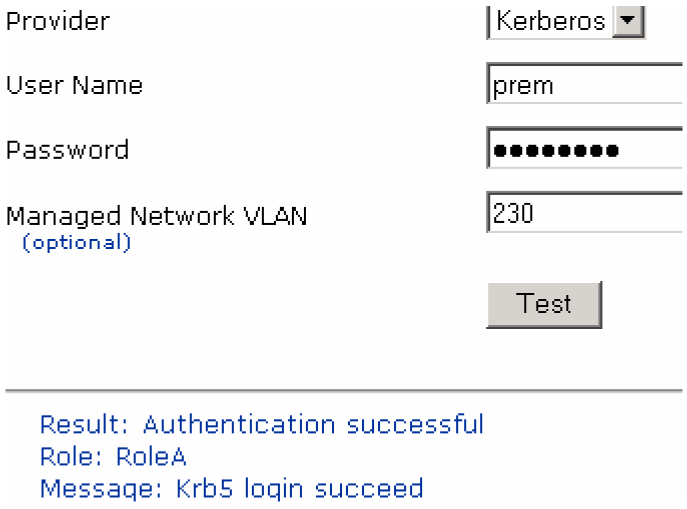
Confirm Mapping via Auth Test

- Perform Auth test by including the VLAN ID to confirm
- **Note: Success of Auth test (with VLAN ID) as shown below does not mean the mapping will succeed with real users. This is just a test from CAM. True result will be known when the CAS sees a 802.1Q VLAN tag on the incoming packet. For that, make sure your switch configuration is correct and tagging packets appropriately.**



Provider	Kerberos ▾
User Name	prem
Password	●●●●●●●●●
Managed Network VLAN (optional)	600

Result: Authentication successful
Role: Role B
Message: Krb5 login succeed

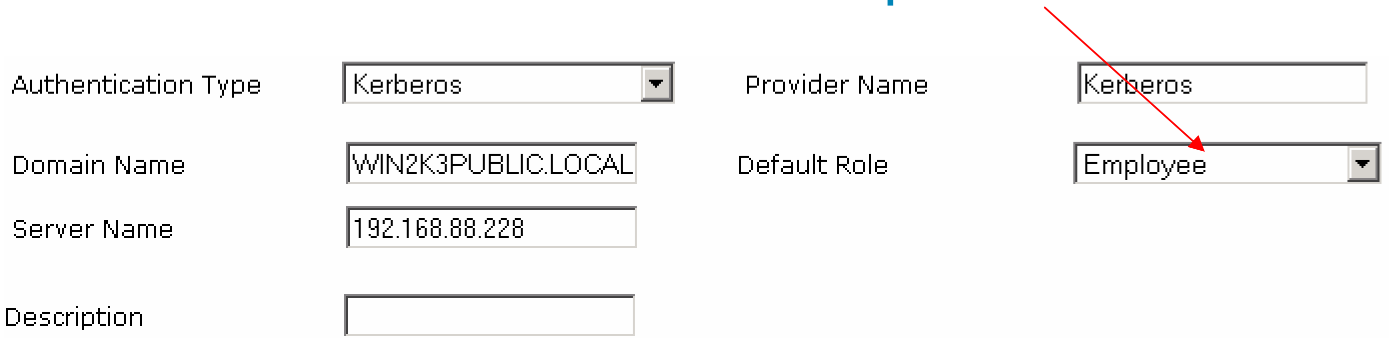


Provider	Kerberos ▾
User Name	prem
Password	●●●●●●●●●
Managed Network VLAN (optional)	230

Result: Authentication successful
Role: RoleA
Message: Krb5 login succeed

Default Role

- Mapping Conditions are parsed like Access Lists to look for the first match.
- If none of the mapping conditions are met, the user will be placed in the **Default Role** as defined on the Provider configurations page (Think of it as implicit policy on your ACL)
- In our example, if the source VLAN is NOT 120,230 or 600, then none of the mappings will match. Hence, user will be placed in the “Employee Role” as this is the default role on the Provider profile



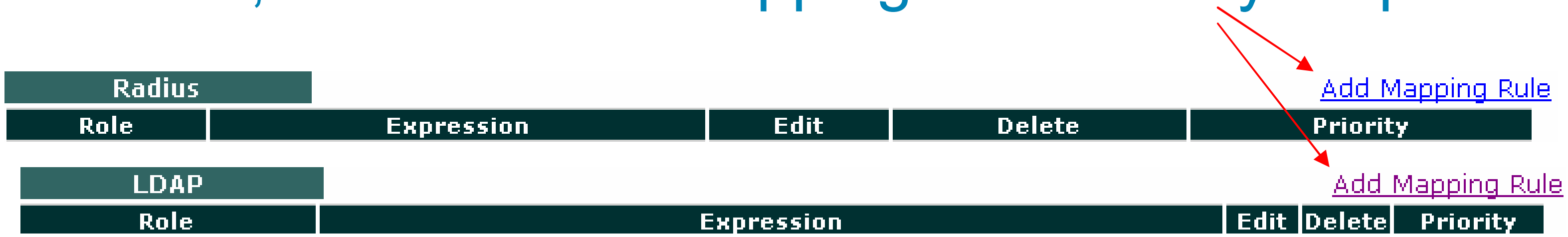
Authentication Type	Kerberos	Provider Name	Kerberos
Domain Name	WIN2K3PUBLIC.LOCAL	Default Role	Employee
Server Name	192.168.88.228		
Description			

Authorization via Role Mapping

Attribute Based

Attribute based Role Mapping

- Applies to Radius, SSO (VPN/AD) LDAP providers.
- Can place users into roles based on the value in a Radius or LDAP Attribute after authentication
- E.g. If the LDAP attribute “memberOf” has a value “Administrators”, place user in a “ITStaff” Role. If the value contains “Users”, place in “Employee” role.
- Similarly, If the Radius Class attribute has value “Contractor”, place user in “Restricted” role. Otherwise, default to “Employee” Role.
- Under User Management >> Auth Server >> Mapping Rules, click on “Add mapping rule under your provider



Radius

Add Mapping Rule

Role	Expression	Edit	Delete	Priority

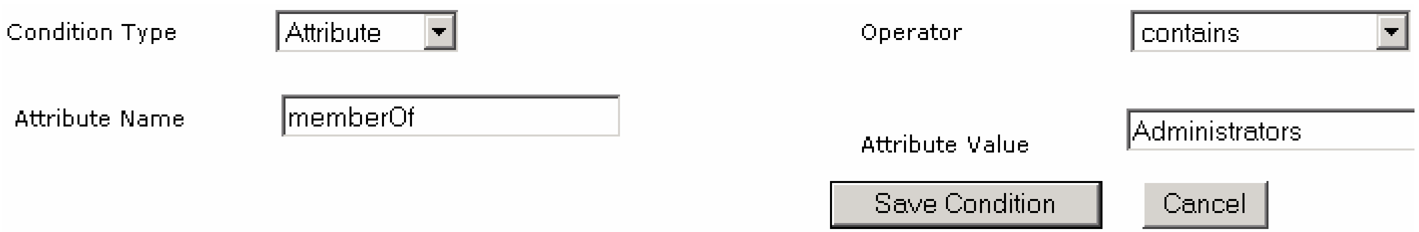
LDAP

Add Mapping Rule

Role	Expression	Edit	Delete	Priority

LDAP : Create Condition

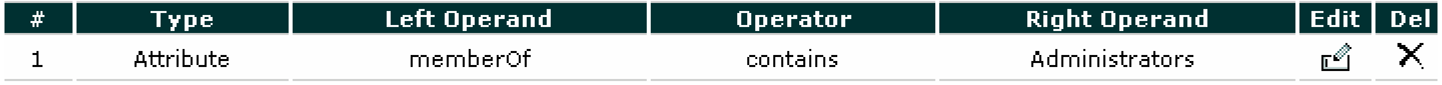
- Select Condition Type = Attribute and add the condition for memberOf Attribute as follows.



Condition Type	Attribute	Operator	contains
Attribute Name	memberOf	Attribute Value	Administrators

- Please note that the Attribute Name and Value are case sensitive

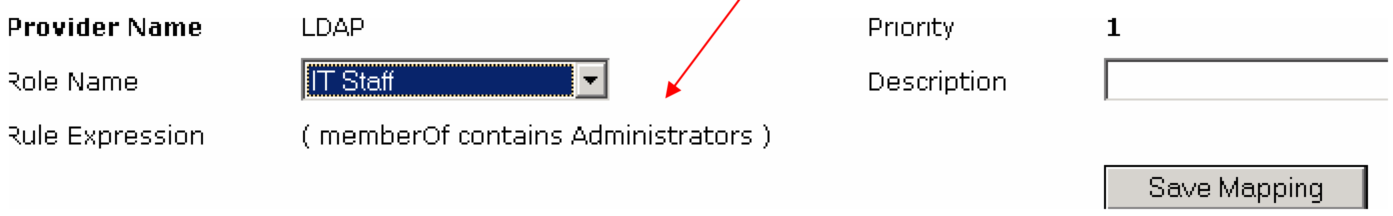
- This condition appears below as follows :



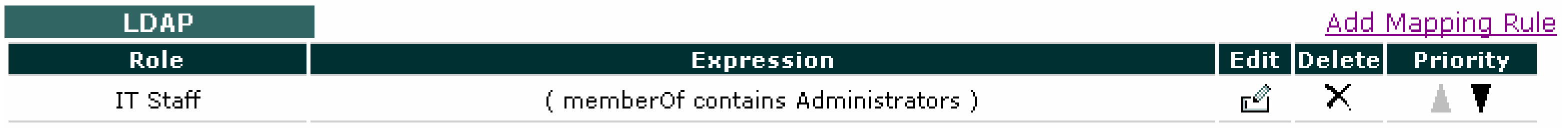
#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	memberOf	contains	Administrators	✎	✕

LDAP : Apply to Role

- Now pick the role you want to apply this to (IT Staff) and click Add Mapping. Note the Rule Expression



Provider Name	LDAP	Priority	**1**
Role Name	IT Staff	Description	
Rule Expression	(memberOf contains Administrators)		

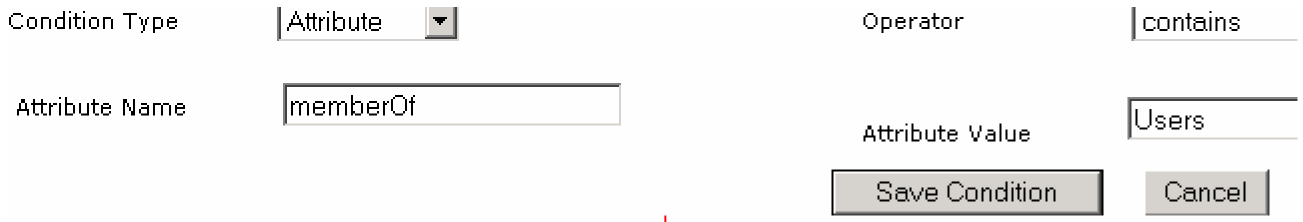


LDAP

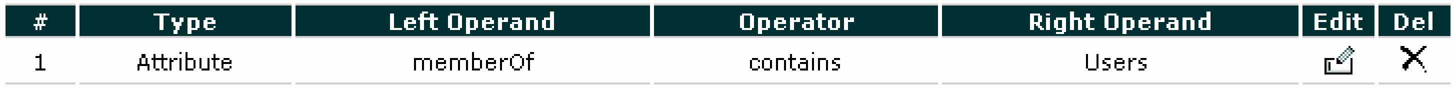
Role	Expression	Edit	Delete	Priority
IT Staff	(memberOf contains Administrators)	✎	✕	▲ ▼

LDAP : Create another mapping

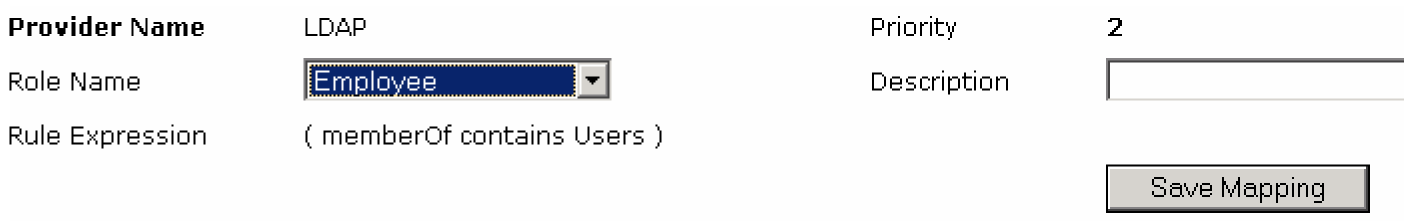
- Following similar steps for Employee Role, Attribute Value = Users as follows



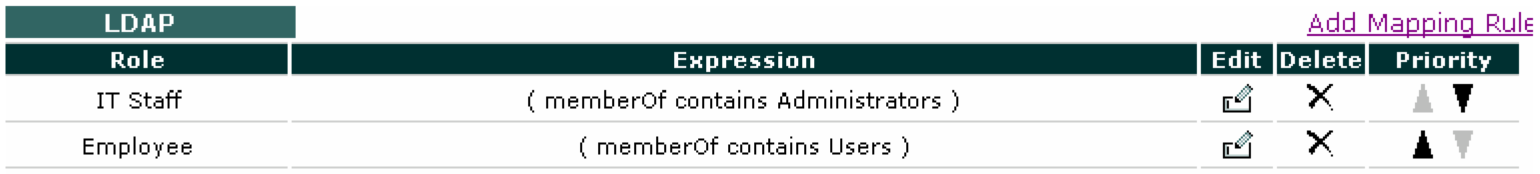
Condition Type	Attribute	Operator	contains
Attribute Name	memberOf	Attribute Value	Users



#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	memberOf	contains	Users	✎	✕



Provider Name	LDAP	Priority	2
Role Name	Employee	Description	
Rule Expression	(memberOf contains Users)		

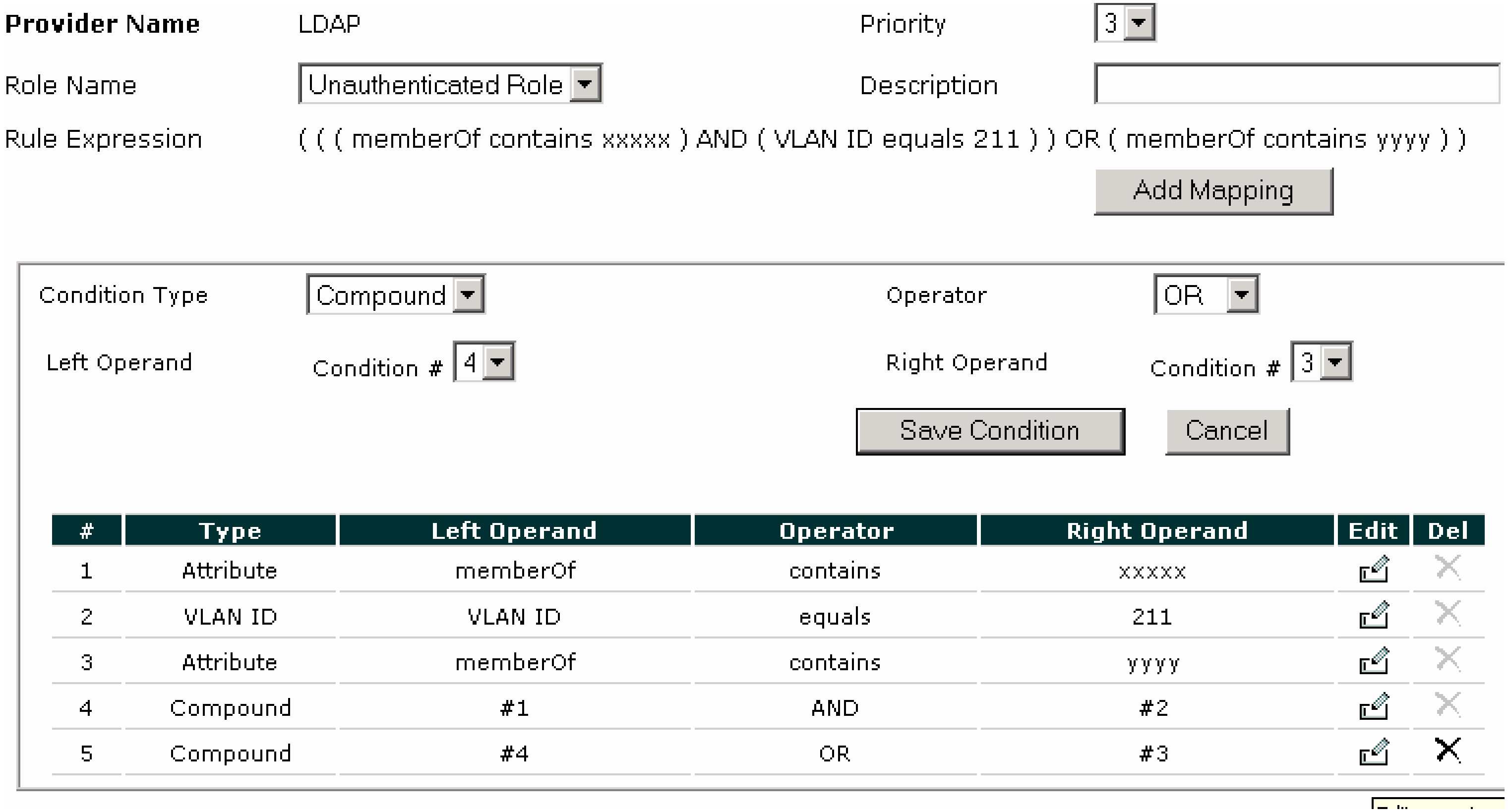


LDAP

Role	Expression	Edit	Delete	Priority
IT Staff	(memberOf contains Administrators)	✎	✕	▲ ▼
Employee	(memberOf contains Users)	✎	✕	▲ ▼

Compounds can be used again

- Please note that compound statements (AND/OR) between conditions can also be used IF necessary to achieve mappings



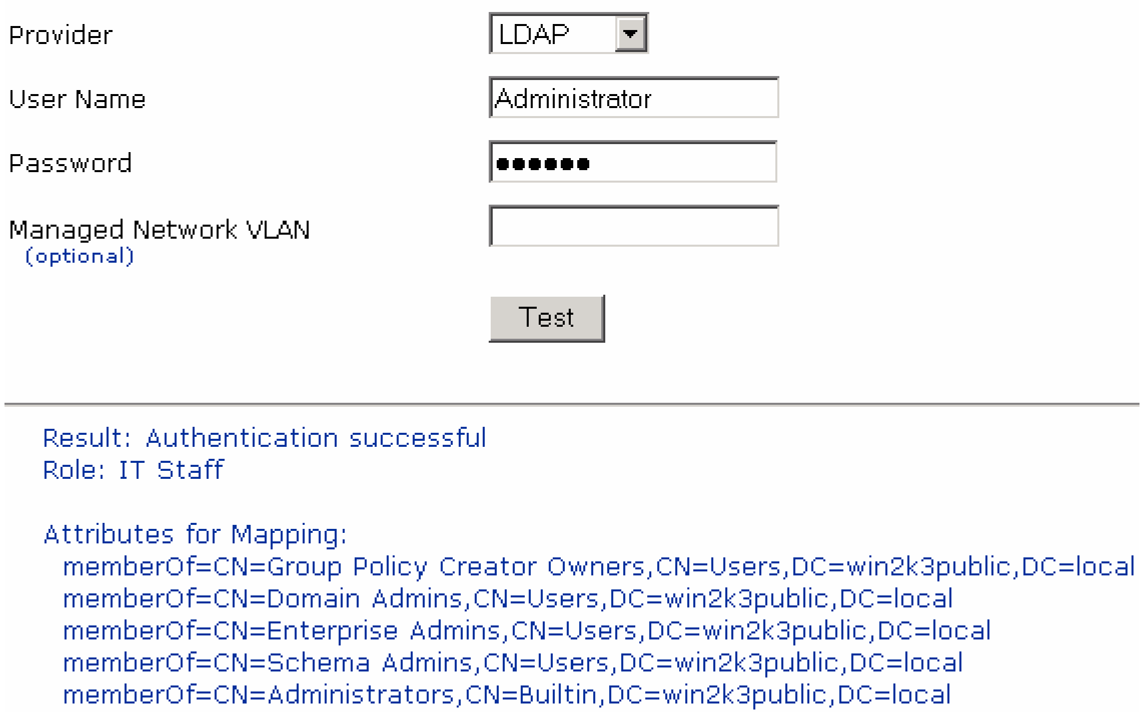
Provider Name	LDAP	Priority	3
Role Name	Unauthenticated Role	Description	
Rule Expression	(((memberOf contains xxxxx) AND (VLAN ID equals 211)) OR (memberOf contains yyyy))		

Condition Type	Compound	Operator	OR
Left Operand	Condition # 4	Right Operand	Condition # 3

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	memberOf	contains	xxxxx		×
2	VLAN ID	VLAN ID	equals	211		×
3	Attribute	memberOf	contains	yyyy		×
4	Compound	#1	AND	#2		×
5	Compound	#4	OR	#3		×

LDAP Auth Test - Administrator

- User “Administrator” is member of Administrators group in AD
- He is placed in “IT Staff” role based on mapping



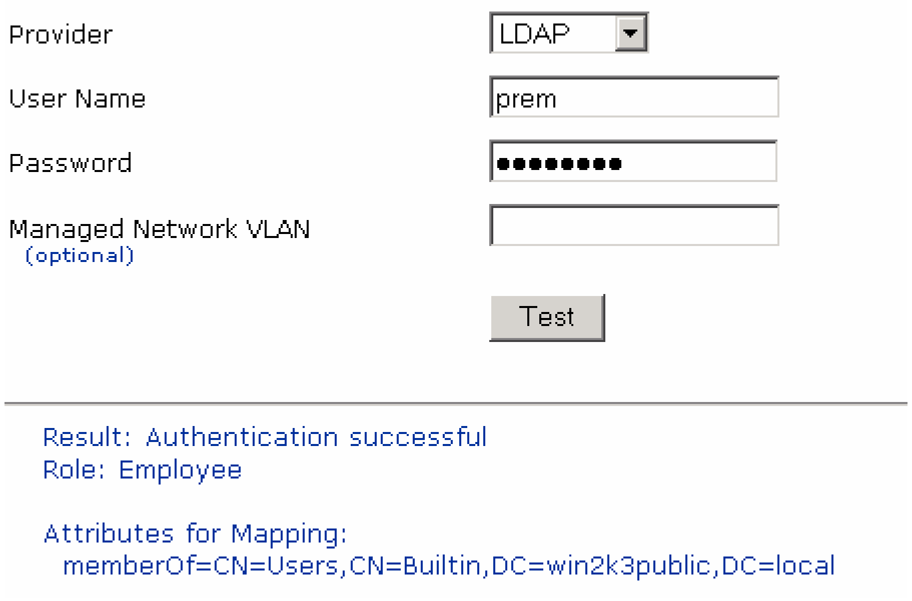
Provider	LDAP ▾
User Name	Administrator
Password	●●●●●●
Managed Network VLAN (optional)	

```
Result: Authentication successful
Role: IT Staff

Attributes for Mapping:
  memberOf=CN=Group Policy Creator Owners,CN=Users,DC=win2k3public,DC=local
  memberOf=CN=Domain Admins,CN=Users,DC=win2k3public,DC=local
  memberOf=CN=Enterprise Admins,CN=Users,DC=win2k3public,DC=local
  memberOf=CN=Schema Admins,CN=Users,DC=win2k3public,DC=local
  memberOf=CN=Administrators,CN=Builtin,DC=win2k3public,DC=local
```

LDAP Auth Test - User

- User “Prem” is a member of Users group in the Active Directory.
- Hence, this user is placed in the “Employee” role based on Role Mapping



Provider: LDAP

User Name: prem

Password: ●●●●●●●●●

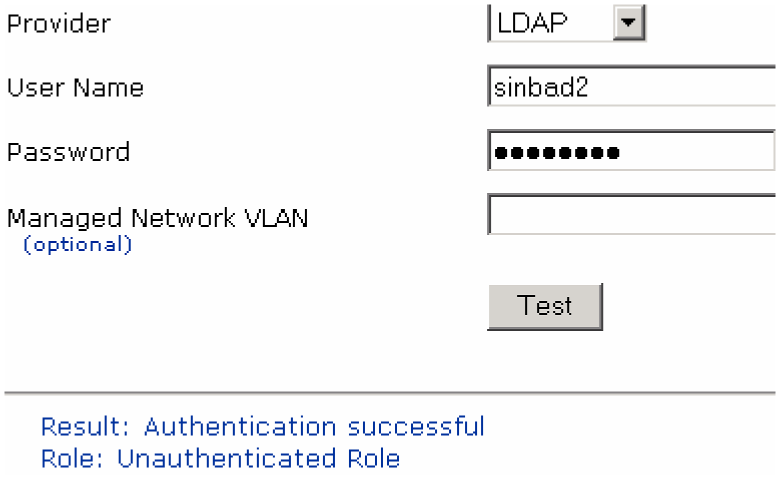
Managed Network VLAN (optional):

```
Result: Authentication successful
Role: Employee

Attributes for Mapping:
  memberOf=CN=Users,CN=Builtin,DC=win2k3public,DC=local
```

LDAP Default Role

- User sinbad2 is neither a part of Administrators group OR the Users group.
- Hence, based on the “Default Role” defined on the LDAP provider, he is placed in the “Unauthenticated Role”

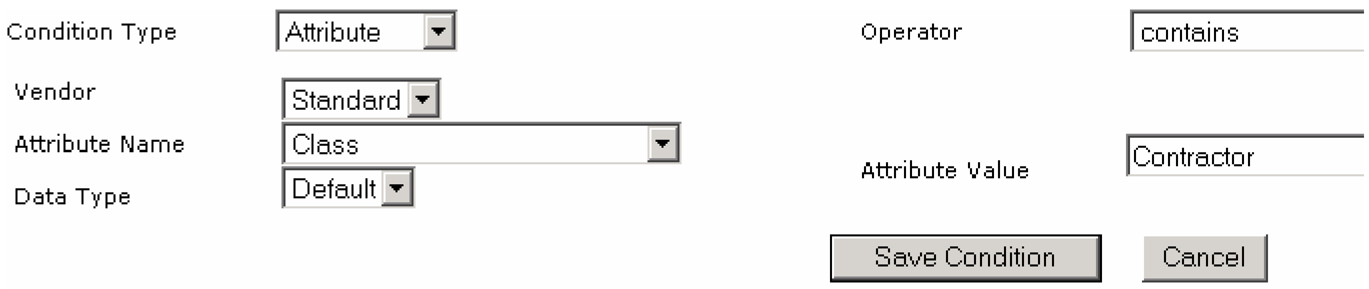


Provider	LDAP
User Name	sinbad2
Password	●●●●●●●●●
Managed Network VLAN (optional)	

Result: Authentication successful
Role: Unauthenticated Role

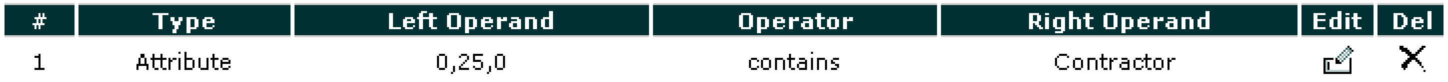
Radius : Create Condition

- Select Condition Type = Attribute and select a Standard (IETF), or Vendor specific Radius attribute.
- In this example we will use the “Class Attribute (25)”



Condition Type	Attribute	Operator	contains
Vendor	Standard		
Attribute Name	Class	Attribute Value	Contractor
Data Type	Default		

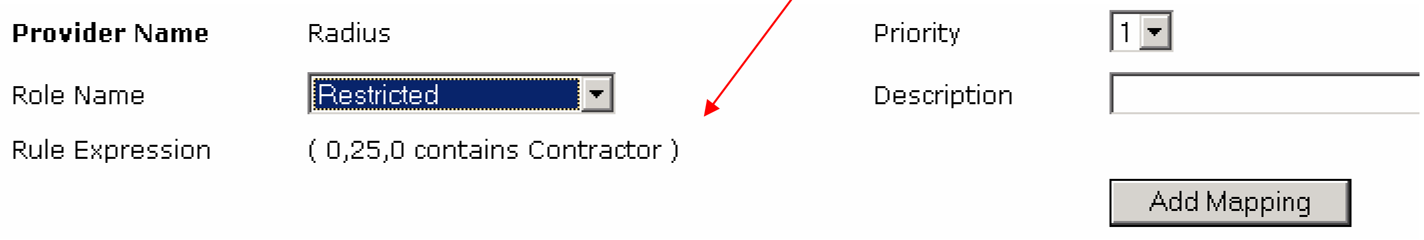
- CAM will look for this Attribute and corresponding value in the Radius Access-Accept packet. It will then be compared against what is configured on the CAM.
- This condition appears below as follows :



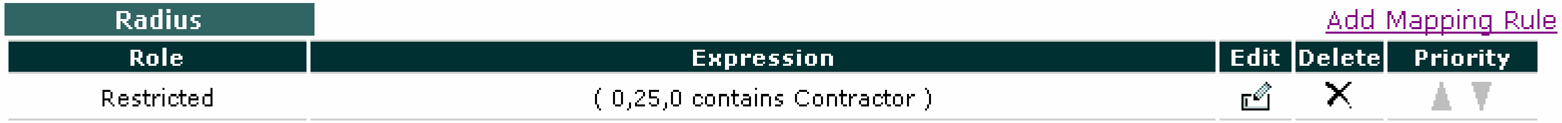
#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25,0	contains	Contractor	✎	✕

Radius : Apply to Role

- Now pick the role you want to apply this to (Restricted) and click Add Mapping. Note the Rule Expression



Provider Name	Radius	Priority	1
Role Name	Restricted	Description	
Rule Expression	(0,25,0 contains Contractor)		

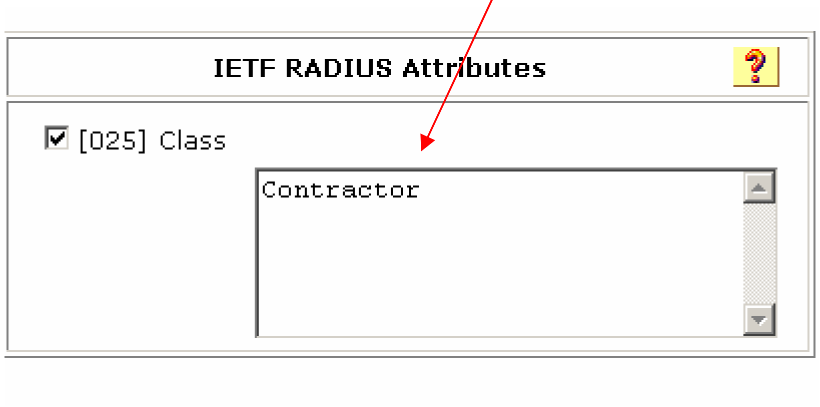


Radius

Role	Expression	Edit	Delete	Priority
Restricted	(0,25,0 contains Contractor)	✎	✕	▲ ▼

Radius: Auth Test

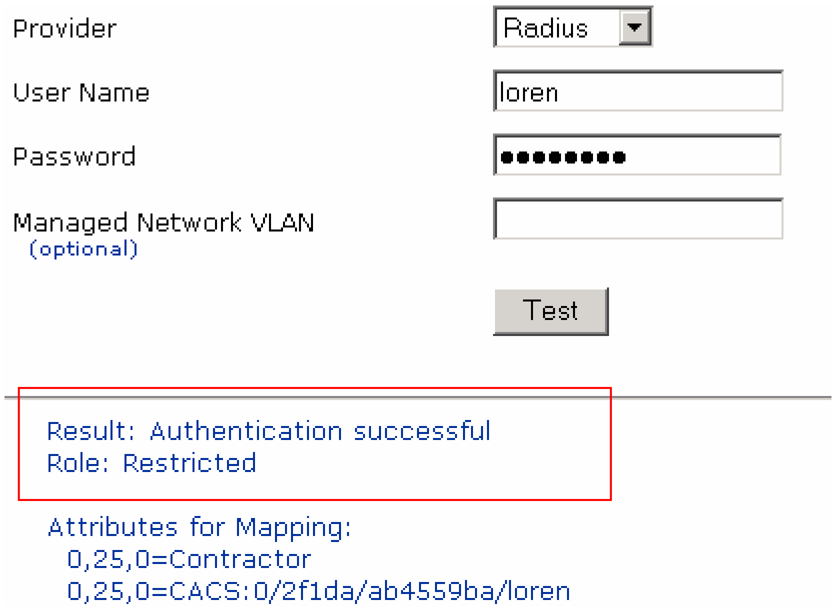
- On the Radius Server, Class Attribute is set on the "Contractors" group as shown



IETF RADIUS Attributes

☑ [025] Class

Contractor



Provider: Radius

User Name: loren

Password: ●●●●●●●●●

Managed Network VLAN (optional):

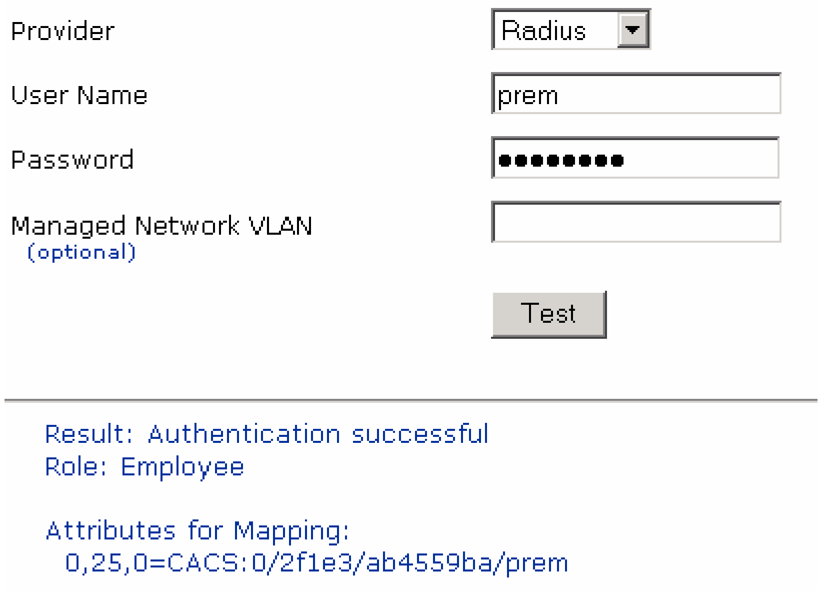
```
Result: Authentication successful
Role: Restricted

Attributes for Mapping:
  0,25,0=Contractor
  0,25,0=CACS:0/2f1da/ab4559ba/loren
```

- User "Loren" is a member of Contractors group
- Hence, this user is placed in the "Restricted" role based on Role Mapping

Radius : Default Role

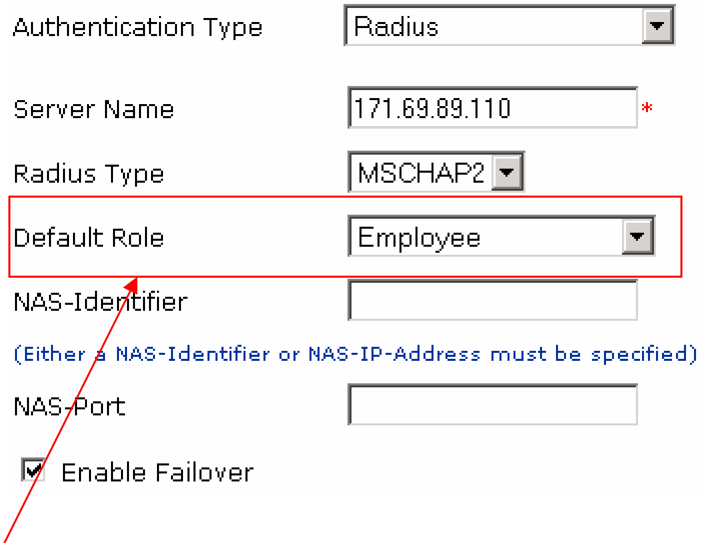
- User Prem is a regular Employee. There is NO class attribute set for Employees.



Provider	Radius
User Name	prem
Password	●●●●●●●●●
Managed Network VLAN (optional)	

Result: Authentication successful
Role: Employee

Attributes for Mapping:
0,25,0=CACS:0/2f1e3/ab4559ba/prem



Authentication Type	Radius
Server Name	171.69.89.110 *
Radius Type	MSCHAP2
Default Role	Employee
NAS-Identifier	

(Either a NAS-Identifier or NAS-IP-Address must be specified)

NAS-Port	

☑ Enable Failover

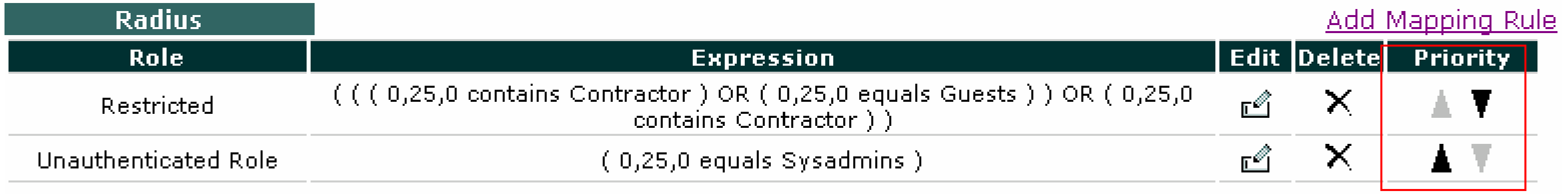
- Hence, based on the “Default Role” defined on the Radius provider, he is placed in the “Employee Role”

Compounds and Order of Processing

- Again, please note that multiple conditions and compound statements (AND/OR) between conditions can also be used IF necessary to achieve mappings

- The mappings are processed in the order or priority (just like ACLs).

- When a match is found – User is mapped into that Role.



Radius

Add Mapping Rule

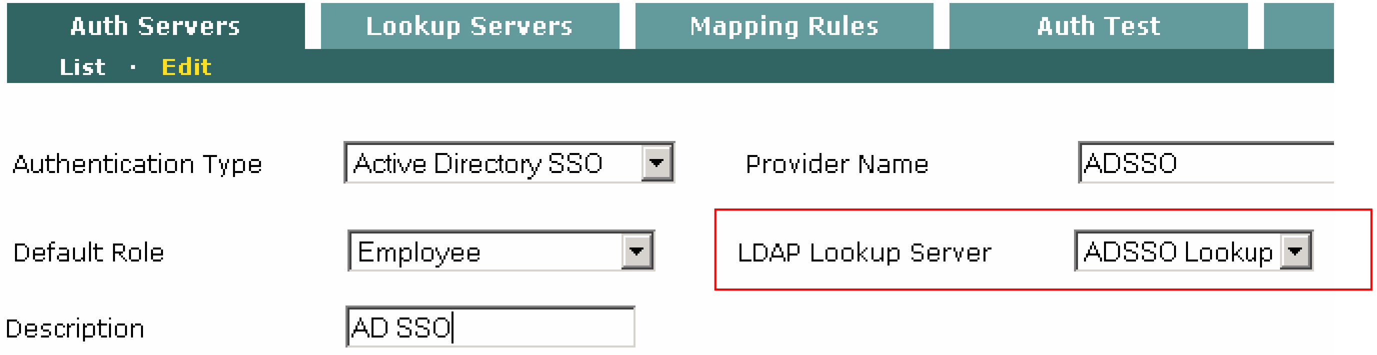
Role	Expression	Edit	Delete	Priority
Restricted	(((0,25,0 contains Contractor) OR (0,25,0 equals Guests)) OR (0,25,0 contains Contractor))	✎	✕	▲ ▼
Unauthenticated Role	(0,25,0 equals Sysadmins)	✎	✕	▲ ▼

- Priority can be changes by using the arrows

Role Mapping for AD SSO and VPN SSO

AD SSO

- Role Mapping for AD SSO is identical to that of LDAP.
- You will need to configure Lookup Servers under (Auth Servers >> Lookup Servers to do a lookup using LDAP). This lookup server will then be connected to AD SSO Provider



Authentication Type: Active Directory SSO

Provider Name: ADSSO

Default Role: Employee

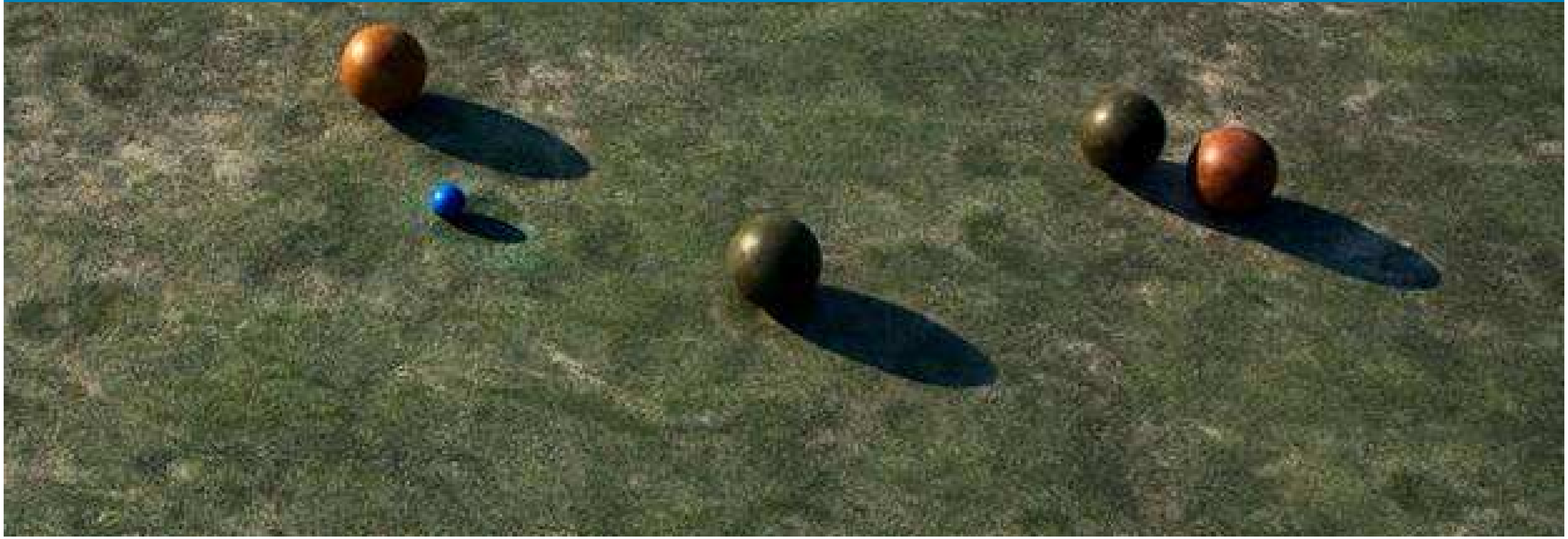
LDAP Lookup Server: ADSSO Lookup

Description: AD SSO

VPN SSO

Role Mapping for VPN SSO is identical to that of Radius.

Active Directory SSO



Windows AD SSO Overview

- Windows SSO is the ability for CCA to automatically authenticate users already authenticated to a backend Kerberos Domain Controller
- Supported on Clients running
  - Win2000 SP4
  - WinXP (Home/Pro), Win Vista (4.0.x) and later
- Support on Active Directory running
  - Win2000 SP4
  - Win2003 SP1 Standard and Enterprise Edition
  - Win2003 Enterprise R2
- **Requires the Clean Access Agent 4.0.0.1 or above**

Windows SSO Process

- Client and the CAS both have an account on the AD

    Client logs onto Windows AD (or cached credentials)

- Credentials are sent to the AD, AD authenticates and give a Ticket Granting Ticket (TGT) to the client

    The Clean Access Agent on the client asks the client for a Service Ticket (ST) with the CAS username to communicate with the CAS

    The client requests a ST from the AD. AD gives the ST to the client, the client give this ST to the agent

- The agent is now able to communicate with the CAS

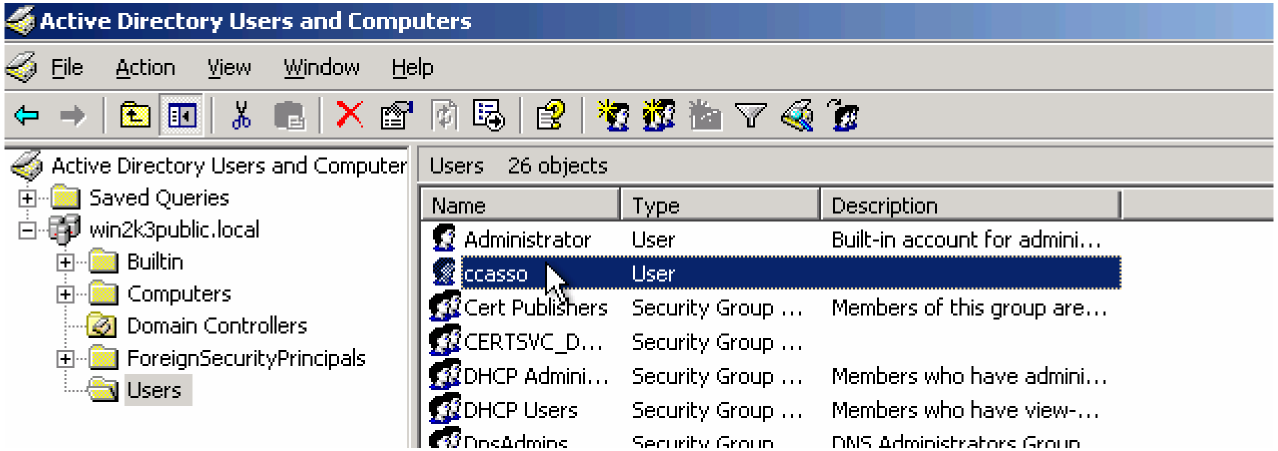
    The CAS sends back packets and mutually authenticates the client

- The client uses this information to sign the client onto Clean Access and hence SSO authentication takes place

- For additional user role mapping, configure a LDAP lookup server with attributes mapping

Get started

- Windows SSO is supported in AD environment only. Win NT environment is not supported.
- Setup CAS User account (ccasso) on Domain Controller. Basic user account is sufficient. No special rights required.For details refer to CAM Guide:- Pg 169-172 (7-23 through 7-27). In this case, username=ccasso, password=cisco123

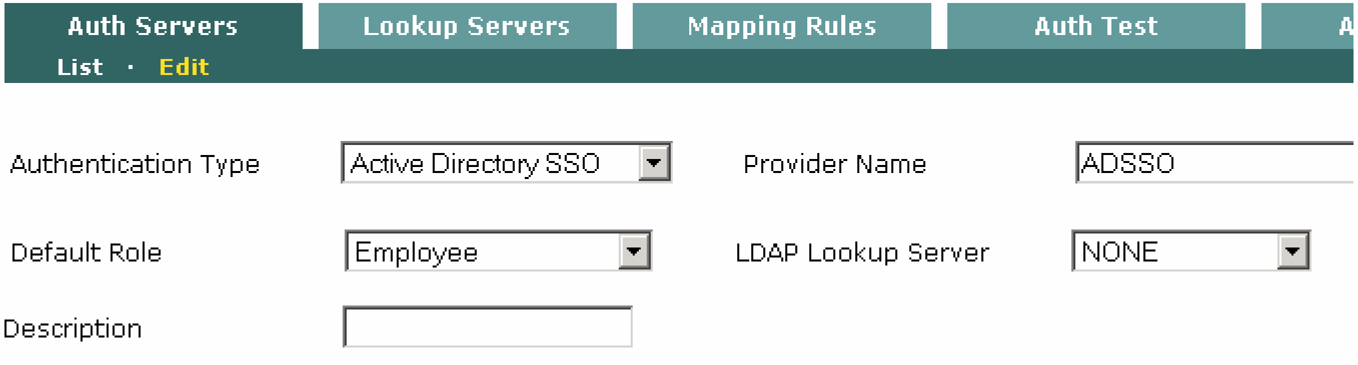


- Active Directory Users and Computer
  - Saved Queries
  - win2k3public.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Users

Users 26 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
ccasso	User	
Cert Publishers	Security Group ...	Members of this group are...
CERTSVC_D...	Security Group ...	
DHCP Admini...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group	DNS Administrators Group

Setup AD SSO provider



Authentication Type	Active Directory SSO	Provider Name	ADSSO
Default Role	Employee	LDAP Lookup Server	NONE
Description			

- The LDAP lookup server is needed only if they want to do Mapping rules for AD SSO, so that after ADSSO, the users will be placed in roles based on AD attributes. This is NOT needed to get basic SSO working (without Role mapping)

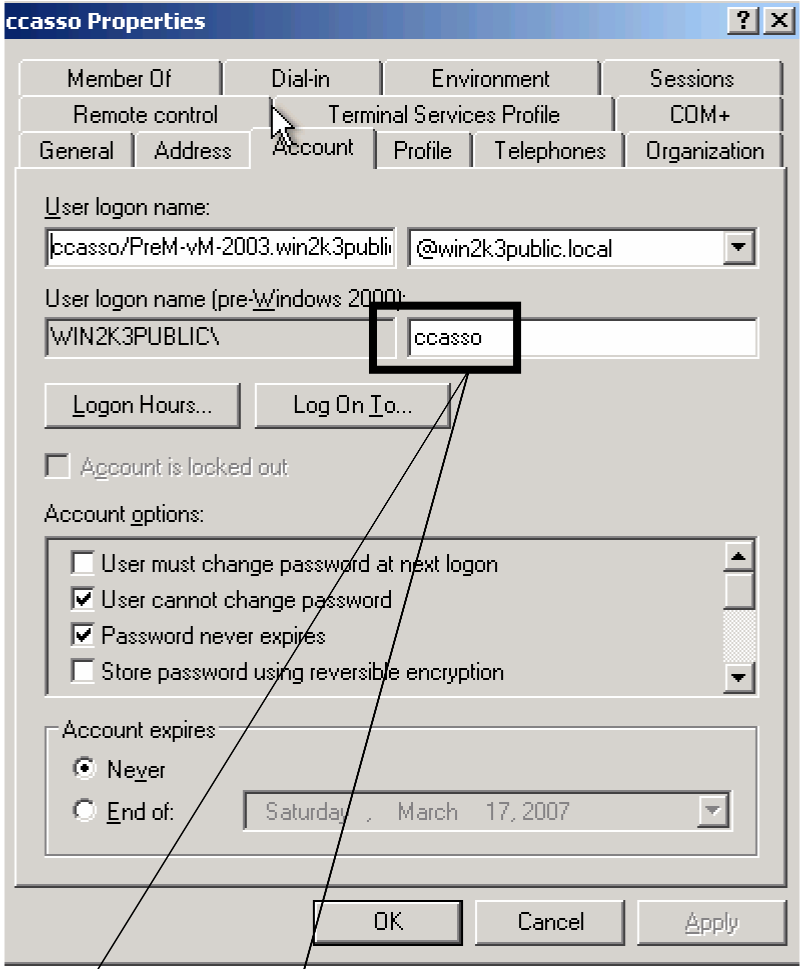
- You cannot do an Auth test to any SSO provider. Hence, testing must be done with a test PC

What is KTPASS?

- CAS need to provide a service called SSO.
- If CAS was a Windows Server, we would have created a Service Account
- Since CAS is running Linux, we need to establish KRB Pre-authentication between CAS and DC so that DC can trust the CAS
- Running KTPASS on DC is a step towards authenticating CAS to the DC so that CAS can start a domain based service called AD SSO.
- KTPASS.EXE is a FREE Microsoft provided tool available as a part of Windows 2K/2K3 support tools.

Coining the KTPASS command

User Account Properties



ccasso Properties

User logon name: ccasso/PreM-vM-2003.win2k3publi @win2k3public.local

User logon name (pre-Windows 2000): WIN2K3PUBLIC\ ccasso

□ Account is locked out

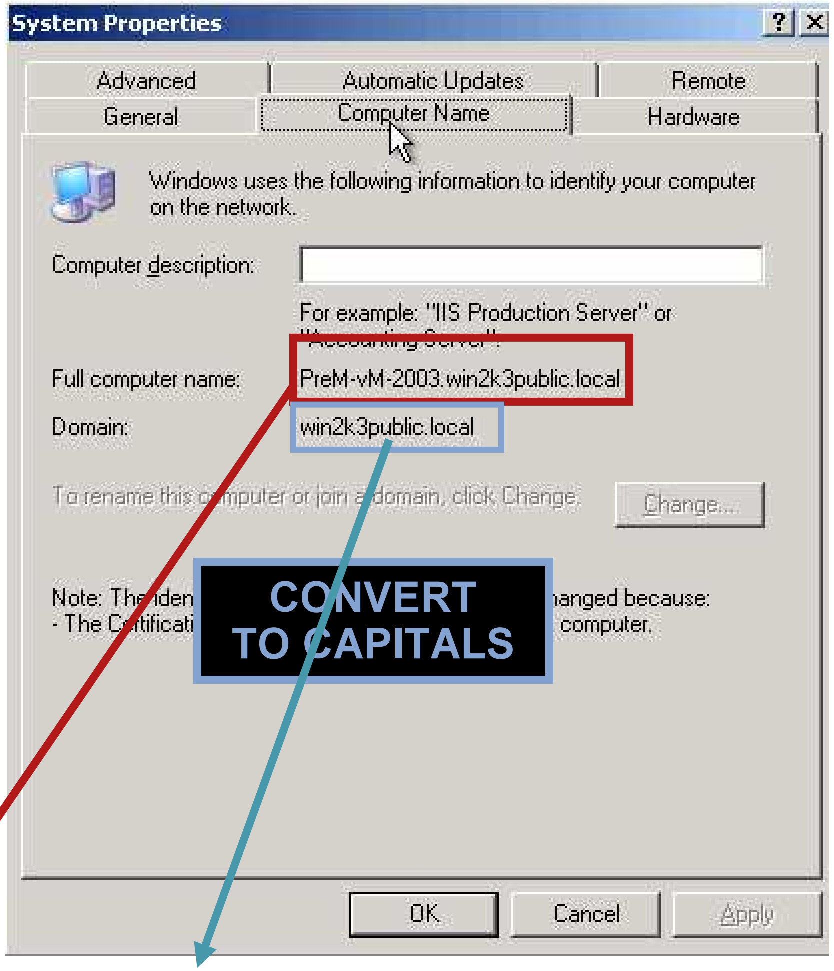
Account options:

- □ User must change password at next logon
- ☑ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Saturday , March 17, 2007

Control Panel -> System



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: PreM-vM-2003.win2k3public.local

Domain: win2k3public.local

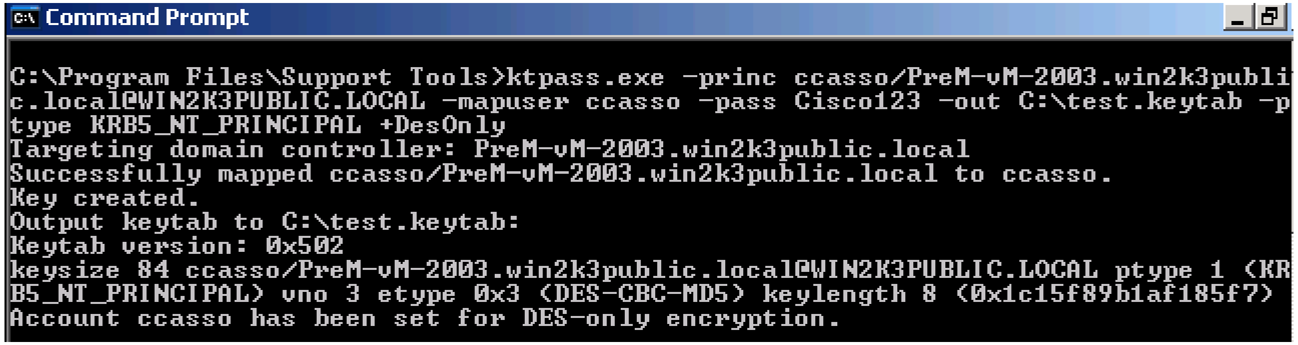
To rename this computer or join a domain, click Change.

Note: The iden... anged because:
- The Certificati... computer.

CONVERT TO CAPITALS

ktpass -princ ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL -mapuser ccasso –pass Cisco123 -out c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly

Run KTPass on the DC



```
C:\Program Files\Support Tools>ktpass.exe -princ ccasso/PreM-vM-2003.win2k3publi
c.local@WIN2K3PUBLIC.LOCAL -mapuser ccasso -pass Cisco123 -out C:\test.keytab -p
type KRB5_NT_PRINCIPAL +DesOnly
Targeting domain controller: PreM-vM-2003.win2k3public.local
Successfully mapped ccasso/PreM-vM-2003.win2k3public.local to ccasso.
Key created.
Output keytab to C:\test.keytab:
Keytab version: 0x502
keysize 84 ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL ptype 1 (KR
B5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0x1c15f89b1af185f7)
Account ccasso has been set for DES-only encryption.
```

C:\Program Files\Support Tools>ktpass.exe -princ ccasso/PreM-vM-2003.win2k3public.local**@WIN2K3PUBLIC.LOCAL** -mapuser ccasso -pass Cisco123 -out C:\test.keytab -p type KRB5_NT_PRINCIPAL +DesOnly

Targeting domain controller: PreM-vM-2003.win2k3public.local

Successfully mapped ccasso/PreM-vM-2003.win2k3public.local to ccasso.

Key created.

Output keytab to C:\test.keytab:

Keytab version: 0x502

keysize 84 ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0x1c15f89b1af185f7)

Account ccasso **has been set for DES-only encryption.**

Run KTPass on the DC

- When running ktpass it is important to note that the computer name that always falls between the "/" and the "@" highlighted in red below matches "CASE BY CASE" to the name of the DC as it would appear under Control Panel >> System >> Computer Name >> Full Computer Name on the DC
- Also, do make sure that the realm name that appears after @ highlighted in blue below is always in CAPITALS.

*C:\Program Files\Support Tools>ktpass.exe -princ ccasso/PreM-vM-2003.win2k3public.local@**WIN2K3PUBLIC.LOCAL** -mapuser ccasso -pass Cisco123 -out C:\test.keytab -p type KRB5_NT_PRINCIPAL +DesOnly*

- If the command is run incorrectly with wrong parameters, then please delete the "ccasso" account >> Recreate the account >> and run KTPASS all over again.

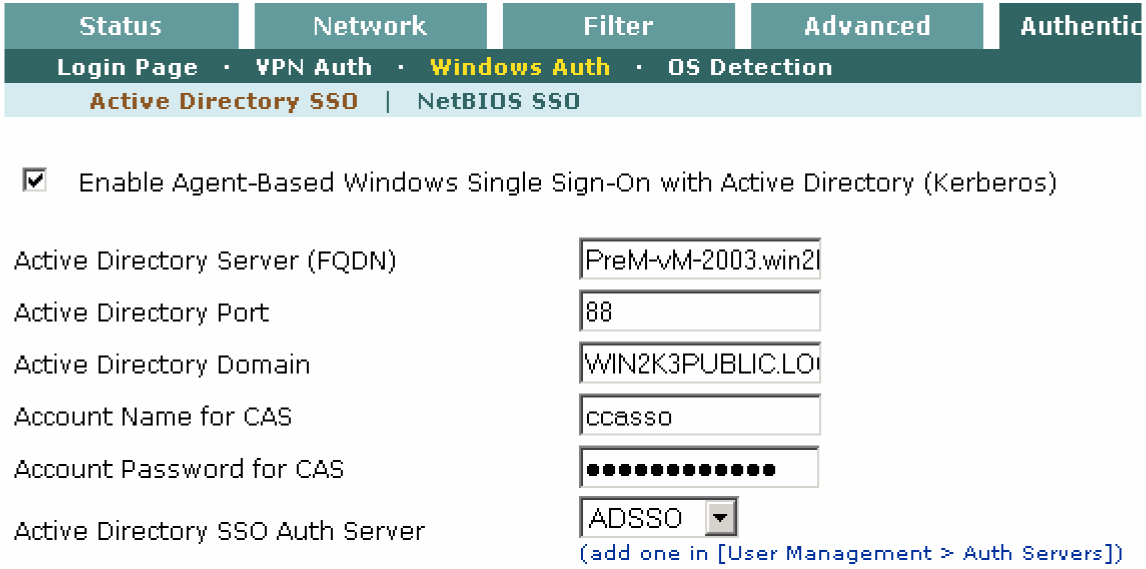
SSO Configuration on the CAS:-

CCA Servers>>Manage>>Authentication>>Windows Auth>>Active Directory SSO

1) Active Directory Domain = WIN2K3PUBLIC.LOCAL = Needs to be in CAPITALS

2) Make sure FQDN matches CASE by CASE **as it appears under under** "Control Panel > System > Computer Name | Full computer name **on the AD server machine (DC)"**

3) Active Directory Server (FQDN) – Please make sure that CAS can resolve this name via DNS. This field cannot be an IP address. In this example, log on to CAS via SSH and do "nslookup prem-vm-2003.win2k3public.local" and make sure it resolves successfully

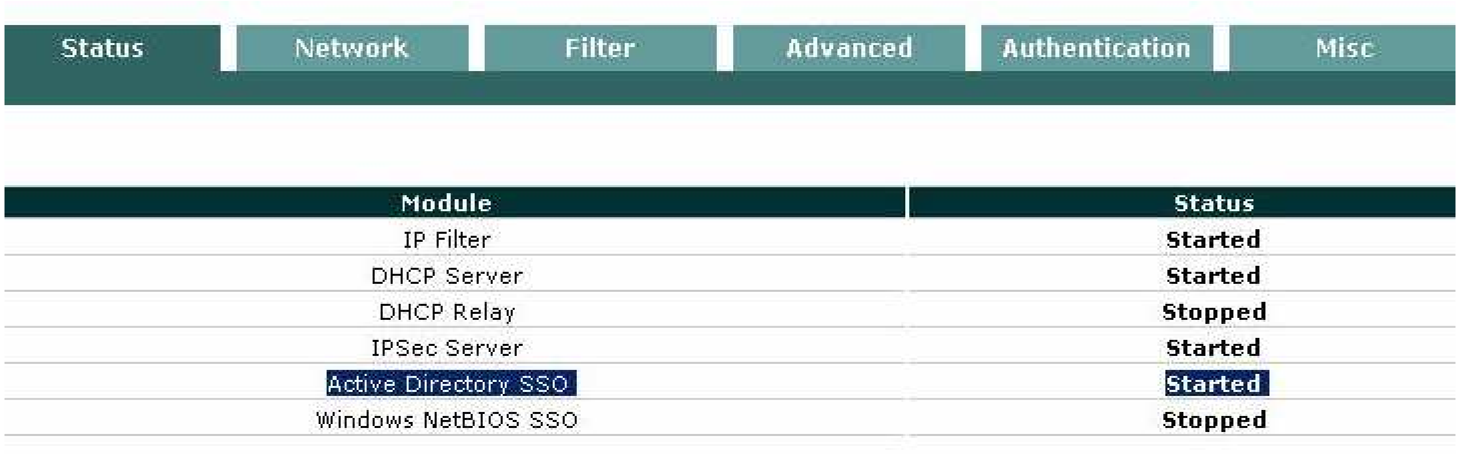

Status
Network
Filter
Advanced
Authentic
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO

☑ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Active Directory Server (FQDN)	PreM-vM-2003.win2l
Active Directory Port	88
Active Directory Domain	WIN2K3PUBLIC.LO(
Account Name for CAS	ccasso
Account Password for CAS	●●●●●●●●●●●●●
Active Directory SSO Auth Server	ADSSO ▾ (add one in [User Management > Auth Servers])

SSO Service started

- Please confirm that SSO service has been started as shown under CCA Servers>>Manage>>Status



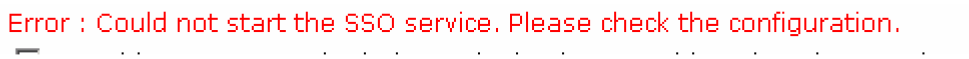
Module	Status
IP Filter	Started
DHCP Server	Started
DHCP Relay	Stopped
IPSec Server	Started
Active Directory SSO	Started
Windows NetBIOS SSO	Stopped

Also confirm that the CAS is now listening on TCP 8910 (Used for Windows SSO)

- [root@cs-ccas02 ~]# netstat -a | grep 8910

```
tcp        0      0 *:8910                        *:*
LISTEN
```

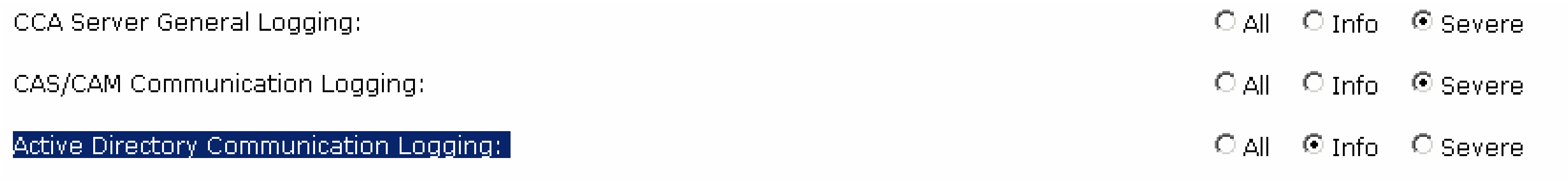
Could not start the SSO service



Error : Could not start the SSO service. Please check the configuration.

- Starting of SSO service is purely based on communication between CAS-DC. Nothing to troubleshoot on client PC
- Check to make sure KTPass has been run correctly. Important to check the fields as mentioned earlier. If KTpass was run incorrectly, delete the account and create a new account on AD and run KTPass again
- Make sure time on CAS is synchronized with the DC. This can be done by pointing them both to the same time server OR by just pointing the CAS to the DC itself (DC runs Windows time). Kerberos is sensitive to clock and skew cannot be greater than 5 minutes (300 secs)
- Make sure Active Directory Domain is in CAPS and CAS can resolve FQDN in DNS.

Could not start the SSO service



CCA Server General Logging: ○ All ○ Info ● Severe

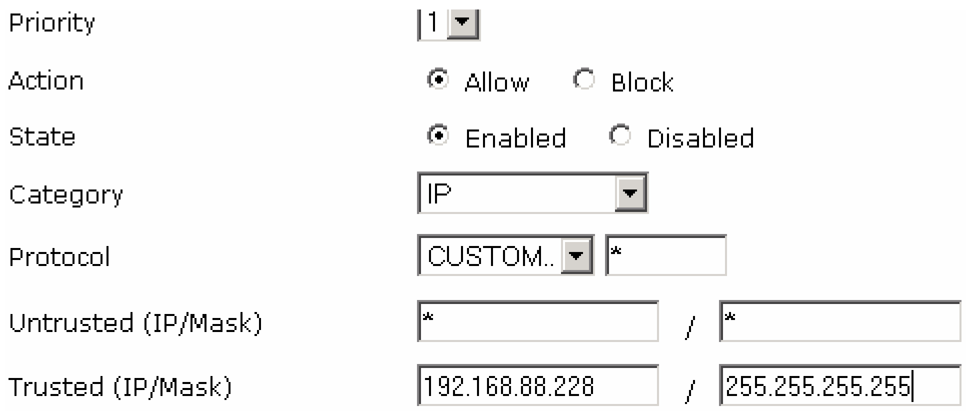
CAS/CAM Communication Logging: ○ All ○ Info ● Severe

Active Directory Communication Logging: ○ All ● Info ○ Severe

- Login to CAS directly as https://<CAS-IP>/admin. Then click on Support Logs and change the logging level for Active Directory communication logging to “INFO”. Recreate problem and download support logs.
- Take a look at the /perfigo/logs/perifgo-redirect-log0.log.0 log file.
- This should give you error info.

Open Ports to DC

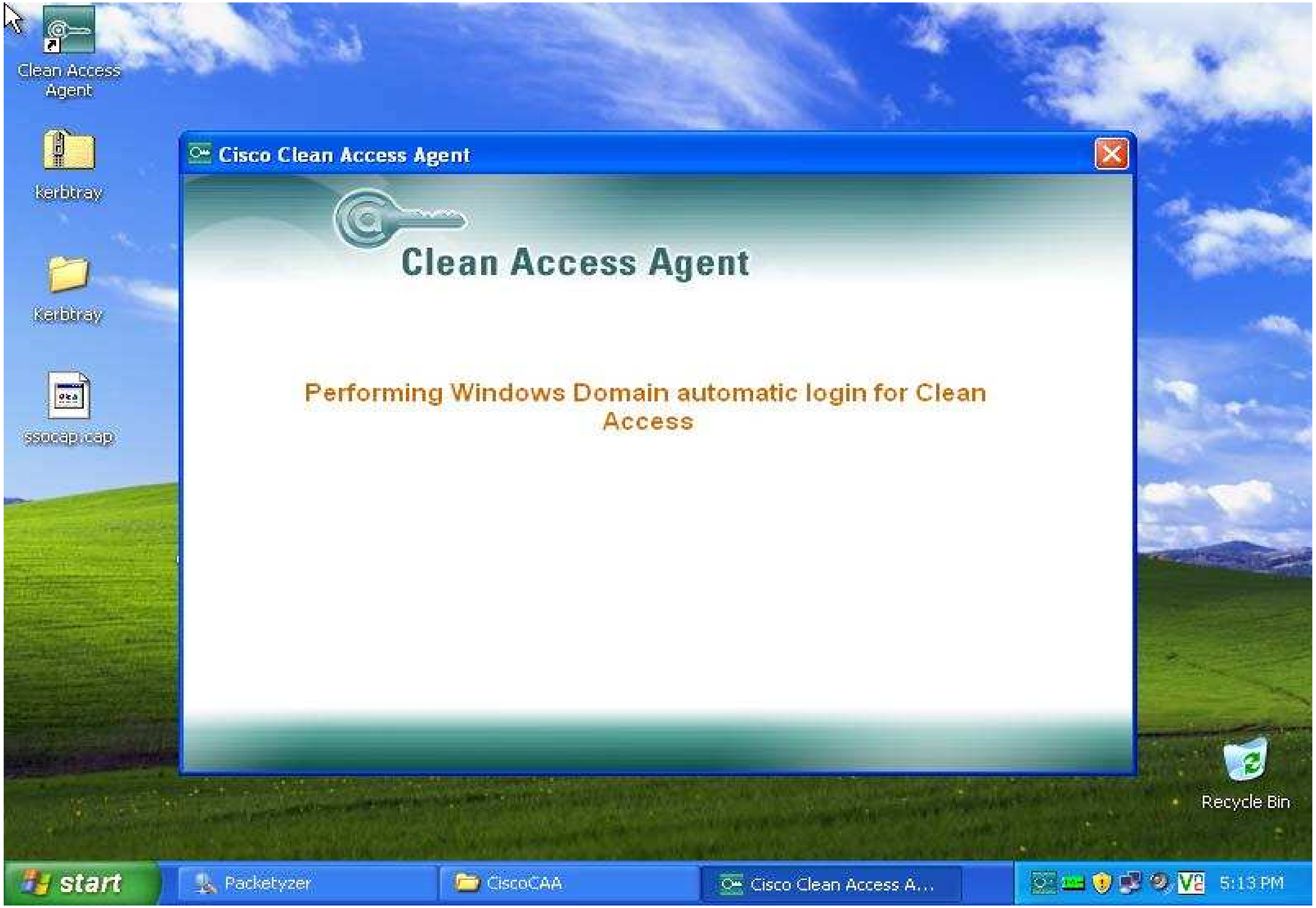
- Open appropriate ports to the DC
- For testing, always open complete access to DC. Then, once you get SSO working you can tie it down to specific ports



Priority	1
Action	● Allow ○ Block
State	● Enabled ○ Disabled
Category	IP
Protocol	CUSTOM.. *
Untrusted (IP/Mask)	* / *
Trusted (IP/Mask)	192.168.88.228 / 255.255.255.255

- Specific ports for AD SSO that need to be opened in the unauthenticated role are indicated in the CAM Administrator Guide.
- Login into the PC using Windows domain credentials.
- Make sure you are logging into the domain (not Local Account)

Client sees Agent performing SSO

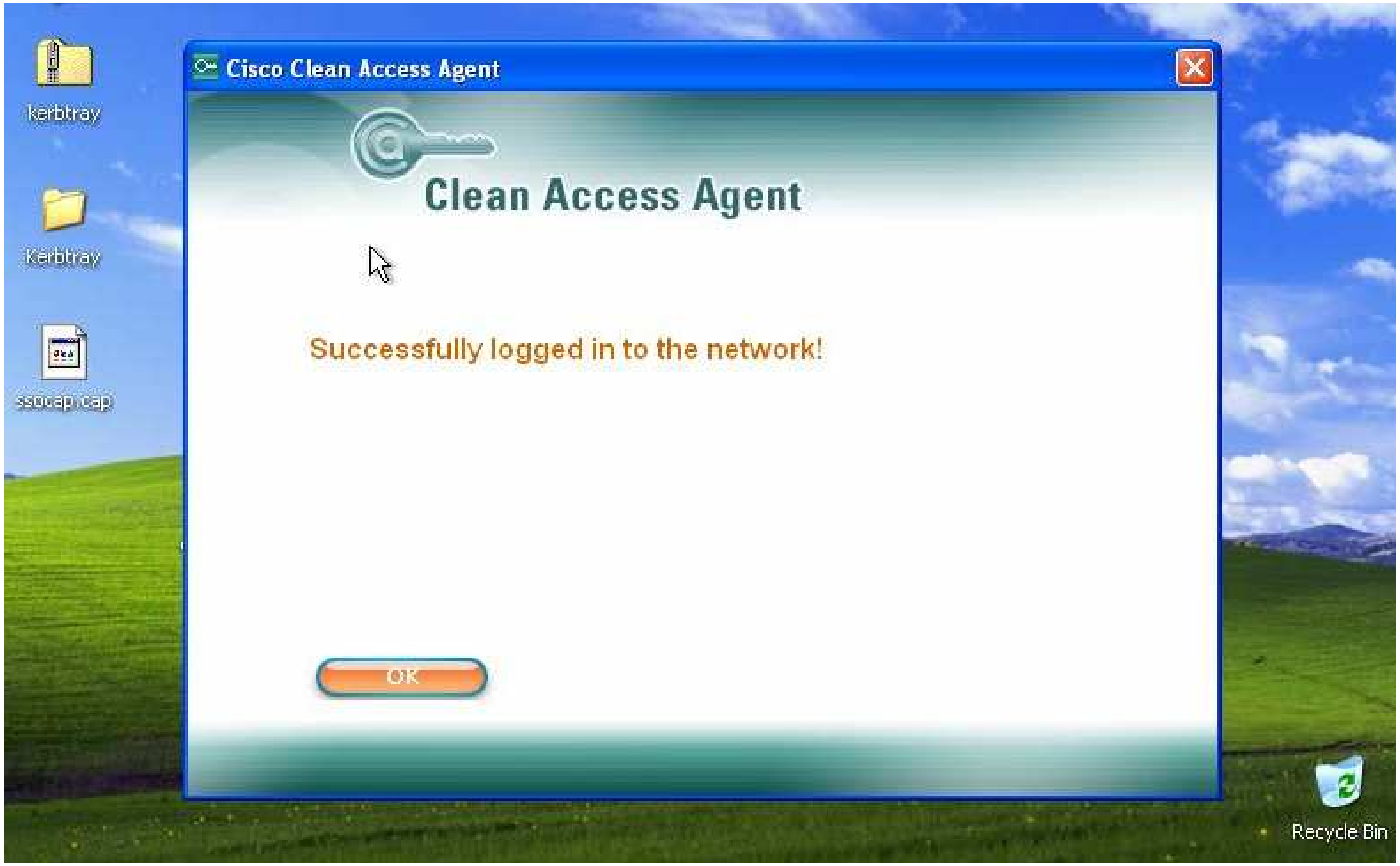


Cisco Clean Access Agent

Clean Access Agent

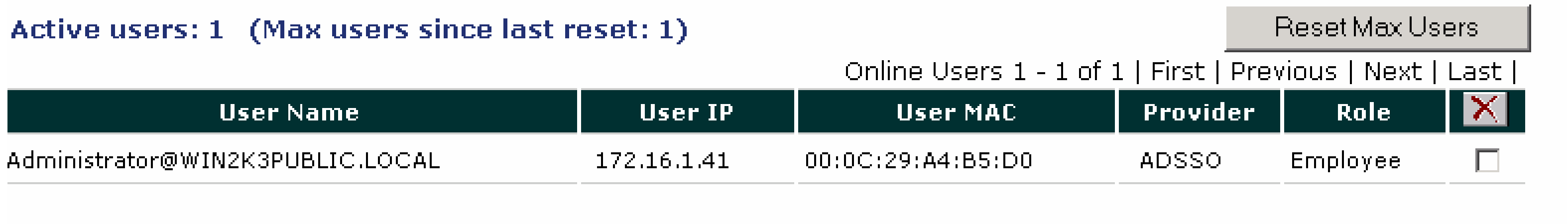
Performing Windows Domain automatic login for Clean Access

SSO completed



Successfully logged in to the network!

SSO User seen on Online User list



Active users: 1 (Max users since last reset: 1)

Online Users 1 - 1 of 1 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	☒
Administrator@WIN2K3PUBLIC.LOCAL	172.16.1.41	00:0C:29:A4:B5:D0	ADSSO	Employee	□

SSO Service is started, but client is not doing SSO

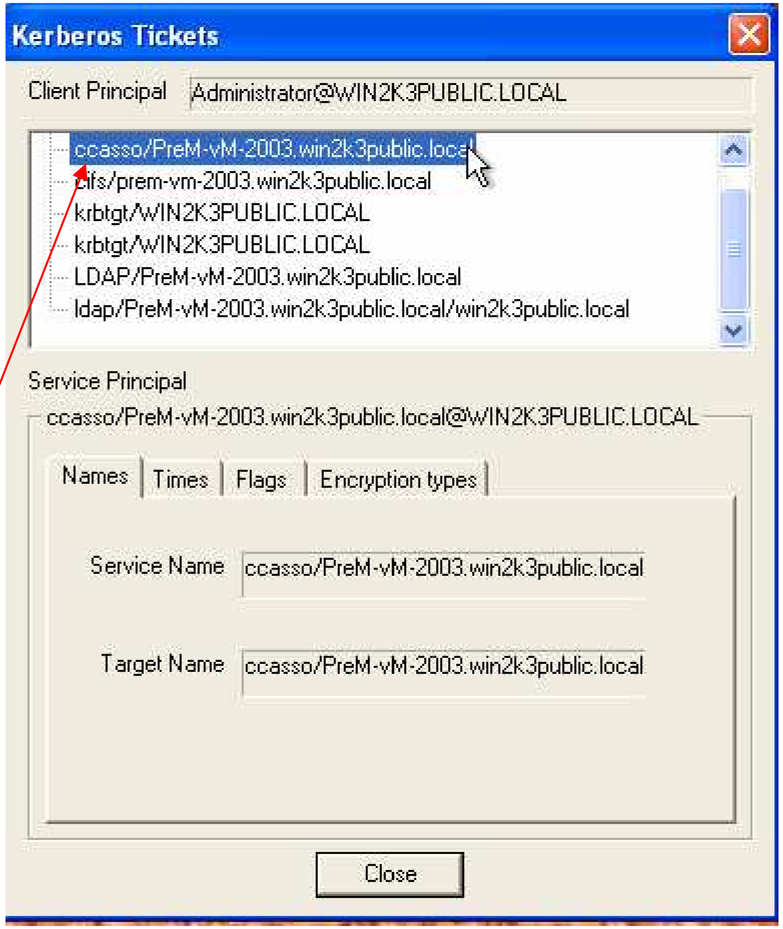
- This is usually due to some communication issue between the DC/client PC or between client PC and the CAS
- Make sure are client does have Kerberos keys –i.e confirm that you are logged into domain
- Confirm that ports are open to the DC so that the client can connect.
- Get agent logs, Get logs on the CAS and work with TAC
- Also confirm CAS is listening on port 8910. An sniffer trace on the client PC will also help
- Make sure CCA Agent is 4.0.0.1 or higher.
- Make sure the user is actually logged in using the domain account and not using the local account.

Kerbtray

Kerbtray can be used to
Confim that the client has
Obtained the Kerberos
Tickets (TGT and ST)
Our concern is the ST
Also known as Service
Ticket, which is for the
CAS Account that we created
On the DC

Kerbtray is a free tool available
From Microsoft Support tools. It
Can also be used to purge the Kerberos
Tickets on a client machine.

A green Kerbtray Icon on the system
Tray indicated that client has active Kerberos
Tickets. However, u need to check to see
If that ticket is correct (valid) for CAS account



Kerberos Tickets

Client Principal Administrator@WIN2K3PUBLIC.LOCAL

- ccasso/PreM-vM-2003.win2k3public.local
- cifs/prem-vm-2003.win2k3public.local
- krbtgt/WIN2K3PUBLIC.LOCAL
- krbtgt/WIN2K3PUBLIC.LOCAL
- LDAP/PreM-vM-2003.win2k3public.local
- ldap/PreM-vM-2003.win2k3public.local/win2k3public.local

Service Principal
ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL

Service Name ccasso/PreM-vM-2003.win2k3public.local

Target Name ccasso/PreM-vM-2003.win2k3public.local

Additional Resources:

Web: http://www.cisco.com/go/nac/appliance
Email: cca-questions@cisco.com