



**fineDoc Number:** EDCS-<XXXXXX>  
**Last Revision Date:** February 3, 2011  
**Created by:** Steve Winters  
**Template Ver. Number:** EDCS-XXXX Rev X

**CAE**

**Virtual Network Management  
Center (VNMC)  
LDAP Integration with Active  
Directory White Paper**



## TABLE OF CONTENTS

<b>INTRODUCTION.....</b>	<b>3</b>
<b>1 VNMC - DEFINE LDAP PARAMETERS .....</b>	<b>3</b>
<b>2 VNMC - DEFINE AUTHORIZATION LOGIN SEQUENCE.....</b>	<b>5</b>
<b>APPENDIX A – ACTIVE DIRECTORY MODIFICATIONS TO SUPPORT LDAP AUTHENTICATION .....</b>	<b>7</b>
<b>AD Schema Tools: .....</b>	<b>7</b>
<b>Working with MMC Console files .....</b>	<b>7</b>
<b>Utility - "adsiedit" .....</b>	<b>7</b>
<b>UCS Documentation:.....</b>	<b>7</b>
<b>IANA Schema Standards link: .....</b>	<b>7</b>
<b>Full IANA CiscoAVPair Definition: .....</b>	<b>7</b>
<b>A. PREREQUISITES:.....</b>	<b>8</b>
<b>B. EXTENDING THE SCHEMA .....</b>	<b>9</b>
<b>Install MMC Schema SnapIn:.....</b>	<b>9</b>
<b>Download and Install adsiedit .....</b>	<b>12</b>
<b>Add the new CiscoAVPair attribute definition: .....</b>	<b>13</b>
<b>Modify “user Class” – add CiscoAVPair attribute .....</b>	<b>16</b>
<b>Modify CiscoAVPair attribute of a Domain User. ....</b>	<b>18</b>

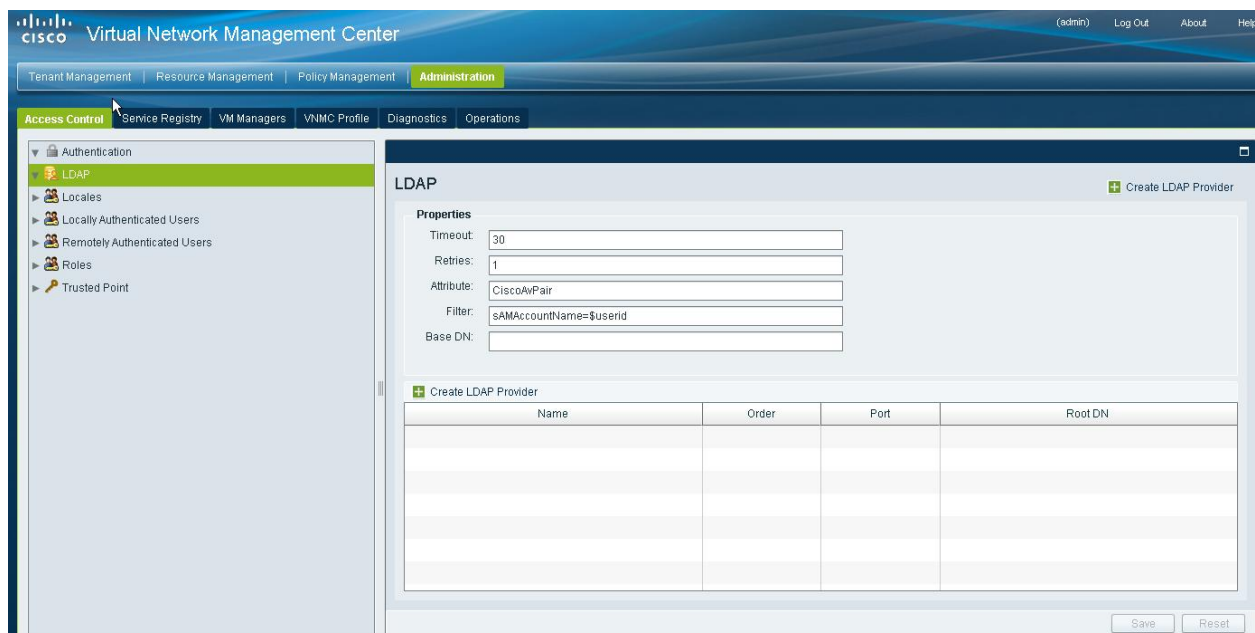
# Introduction

The purpose of this document is to describe how to integrate VNMC with Active Directory LDAP.

Please refer to Appendix A for the Active Directory modifications that are required for successful VNMC LDAP account authentication.

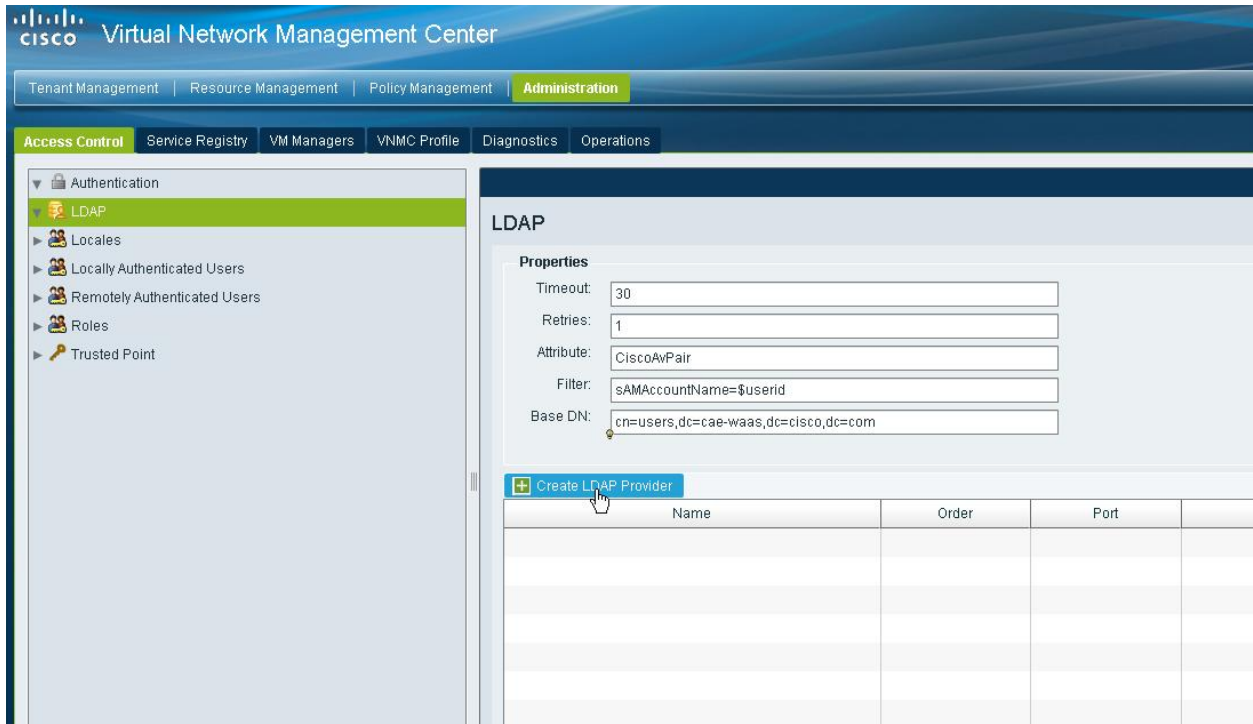
## 1 VNMC - Define LDAP Parameters

Log into the VNMC as admin and navigate to the Administration->Access Control Tab and select LDAP



Set the Base DN to: cn=users,dc=cae-waas,dc=cisco,dc=com (in this example, the FQDN of the active directory domain is cae-waas.cisco.com and we'll be looking for CiscoAVPair in the users schema).

Select "Create LDAP Provider":



Enter the Hostname or IP Address of the Active Directory server providing LDAP authentication  
Order number should be 1 (if this is the first in the LDAP provider lookup sequence)  
Key is the Active Directory “Administrator” account password  
Root DN should have the following: cn=Administrator,cn=users,dc=cae-waas,dc=cisco,dc=com (in this example, the FQDN of the active directory domain is cae-waas.cisco.com and Administrator is the AD account with Administrative privileges)  
Select OK

Create

## Create LDAP Provider

Hostname / IP Address: 172.18.217.235

Order: lowest-available (1-16, 0:lowest-available)

Key: \*\*\*\*\*

Root DN: cn=Administrator,cn=users,dc=cae-waas,dc=cisco,dc=com

Port: 389

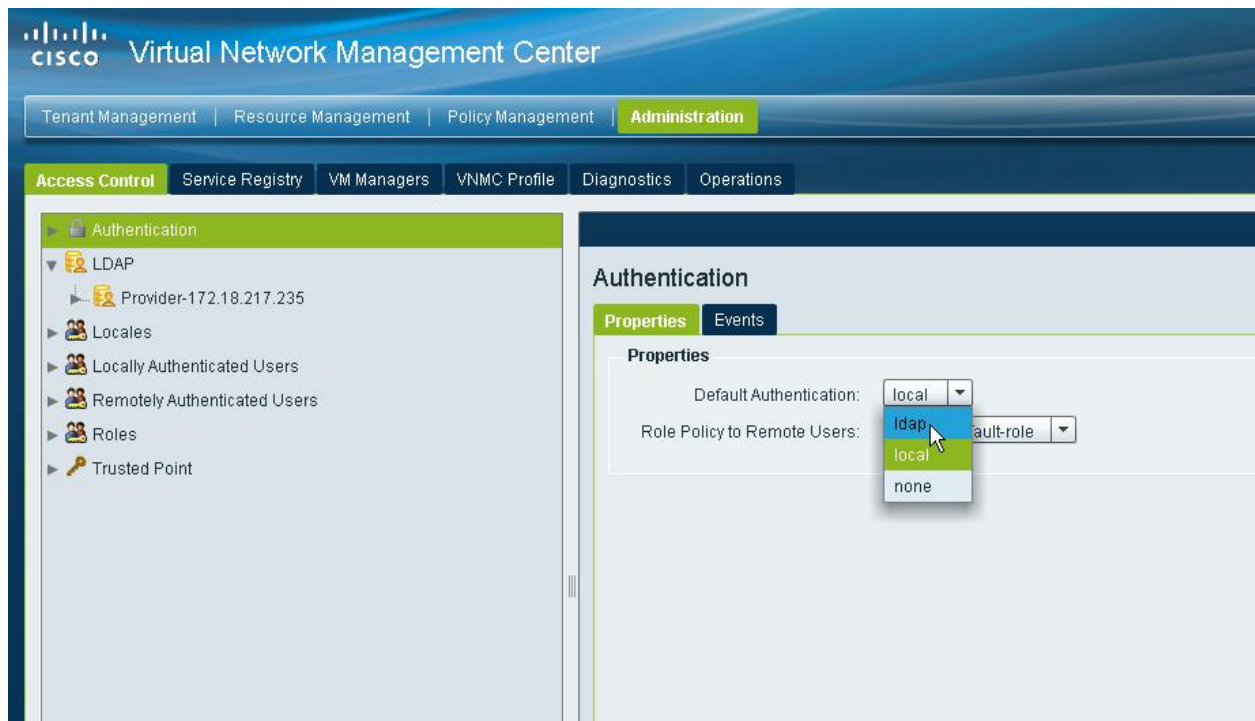
Enable SSL

OK Cancel

Then Save the provider configuration

## 2 VNMC - Define Authorization Login Sequence

Select Administration->Access Control Authorization and set the default VNMC login to be LDAP lookup:



Users identified in AD CiscoAVPair attribute mapping are ready to log into the VNMC

## Appendix A – Active Directory modifications to support LDAP Authentication

---

### References:

#### AD Schema Tools:

[http://technet.microsoft.com/en-us/library/cc757747\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc757747(WS.10).aspx)

#### Working with MMC Console files

[http://technet.microsoft.com/en-us/library/cc772621\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772621(WS.10).aspx)

#### Utility - "adsiedit"

[http://technet.microsoft.com/en-us/library/cc773354\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc773354(WS.10).aspx)

ADSI Edit is Microsoft Management Console (MMC) snap-in that uses the Lightweight Directory Access Protocol (LDAP). You can use ADSI Edit to view and modify directory objects in the Active Directory database. You can also use it to view schema directory partition objects and properties.

#### UCS Documentation:

The LDAP Authentication mechanism for VNMC is tightly coupled with the UCSM LDAP Authentication scheme; UCSM documentation can be found at:

[http://www.cisco.com/en/US/products/ps10281/tsd\\_products\\_support\\_configure.html](http://www.cisco.com/en/US/products/ps10281/tsd_products_support_configure.html)

#### IANA Schema Standards link:

<http://www.iana.org/assignments/enterprise-numbers>

#### Full IANA CiscoAVPair Definition:

```
CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: VNMC User Authorization Field
oMSyntax: 64
IDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

## A. Prerequisites:

---

- An Active Directory Server with a domain configured that VNMC can bind to.
- Microsoft Support Tools (Windows 2003)  
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en#Overview>
- 
- 2 Domain users:
  - i) One with sufficient privileges to bind to the AD server – any member of the “Domain Users” group will work.
  - ii) An admin user that is a member of “Domain Admins” or “Schema Admins” and has sufficient privileges to modify the Active Directory schema.
- Microsoft Schema modification tools:
  - i) MMC Schema snapin
  - ii) ADSIedit
- Wireshark – enables verification if LDAP bind handshake.
- Administrative access to VNMC



## B. Extending the Schema

---

### Install MMC Schema SnapIn:

Reference - Working with MMC Console files

**NOTE:**

*To perform this procedure, you must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority.*

**Procedure:**

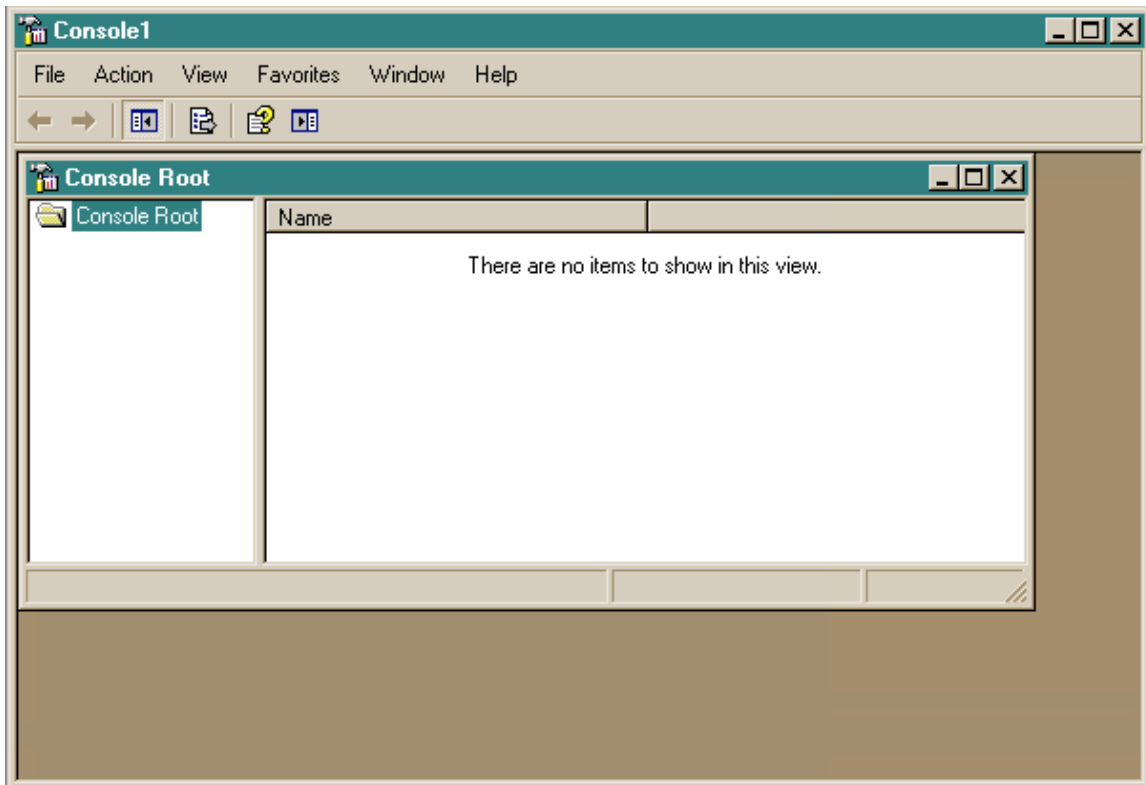
1. Open Command Prompt.

Type:

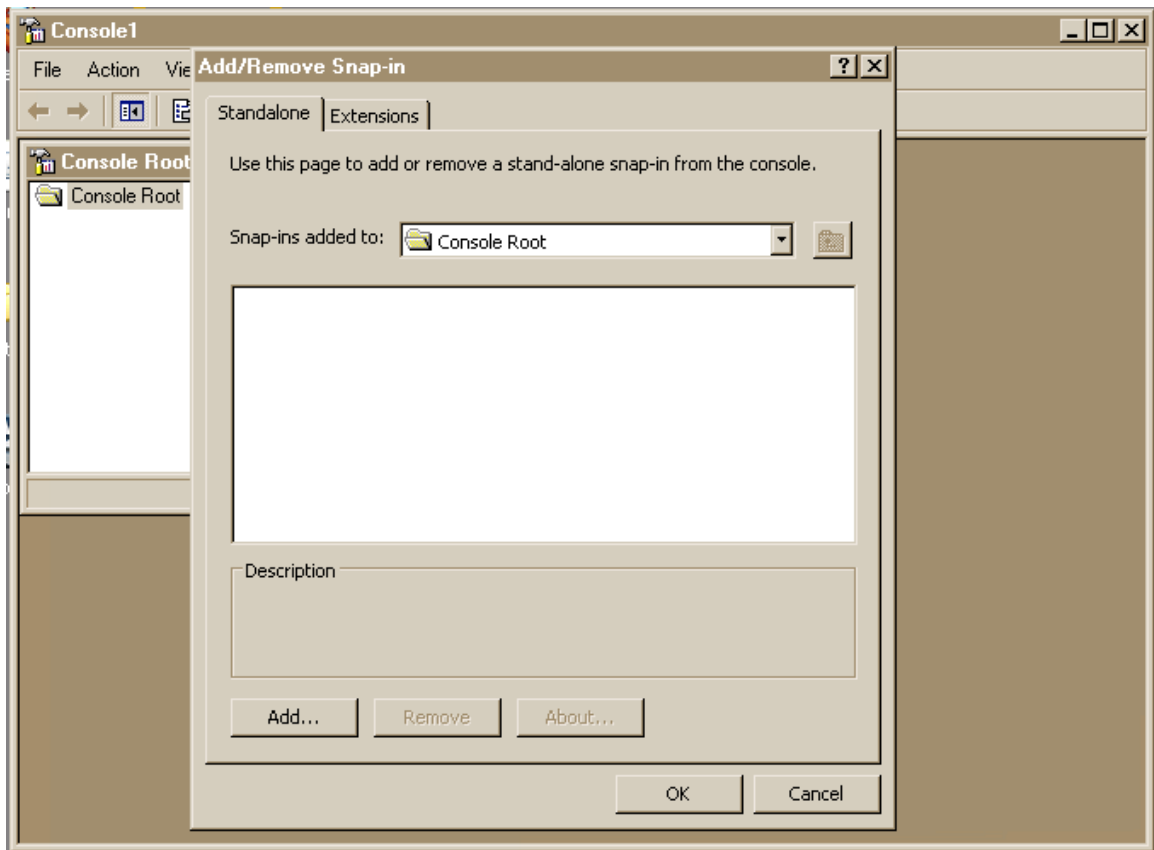
C:\regsvr32 schmmgmt.dll

*This command will register schmmgmt.dll on your computer*

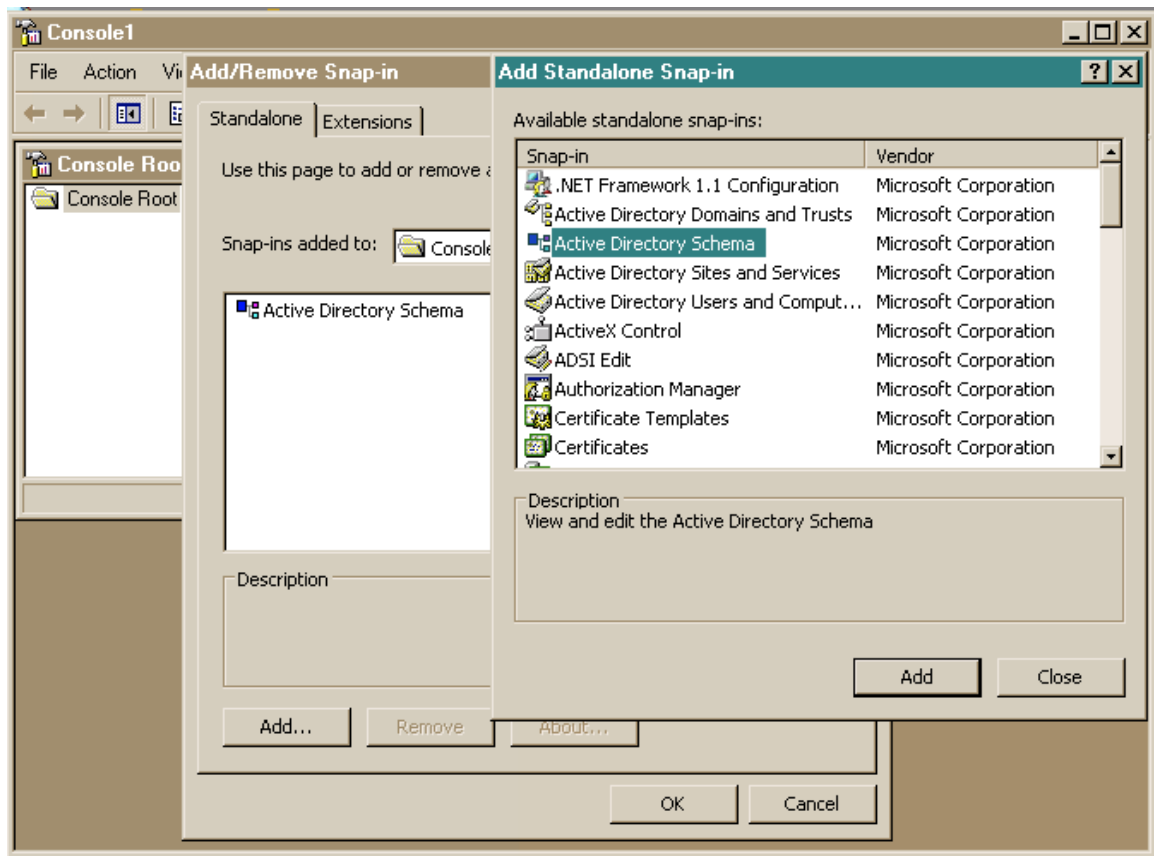
2. Click Start->Run, type "mmc /a" then click OK.



3. On the File menu, click Add/Remove Snap-in, and then click Add.



4. Under Available Standalone Snap-ins, double-click Active Directory Schema, click Close, and then click OK.



5. To save this console, on the File menu, click Save.
6. In Save in, place the snapin in the systemroot\system32 directory.
7. In File name, type schmmgmt.msc, and then click Save.

## Download and Install adsiedit

### Windows 2003:

To install ADSI Edit on computers running Windows Server 2003 or Windows XP operating systems, install Windows Server 2003 Support Tools from the Windows Server 2003 product CD or from the Microsoft Download Center:

<http://go.microsoft.com/fwlink/?LinkId=100114>

For more information about how to install Windows Support Tools from the product CD, see Install Windows Support Tools

<http://go.microsoft.com/fwlink/?LinkId=62270>

### Windows 2008:

On servers running Windows Server 2008 or Windows Server 2008 R2, ADSI Edit is installed when you install the Active Directory Domain Services (AD DS) role to make a server a domain controller.

#### NOTE:

*Adsiedit.msc will not run unless the Adsiedit.dll file is registered. This happens automatically if the support tools are installed. However, if the support tool files are copied instead of installed, you must run the regsvr32 command to register Adsiedit.dll before you run the Adsiedit.msc snap-in.*

#### To register:

Open Command Prompt.

Type:

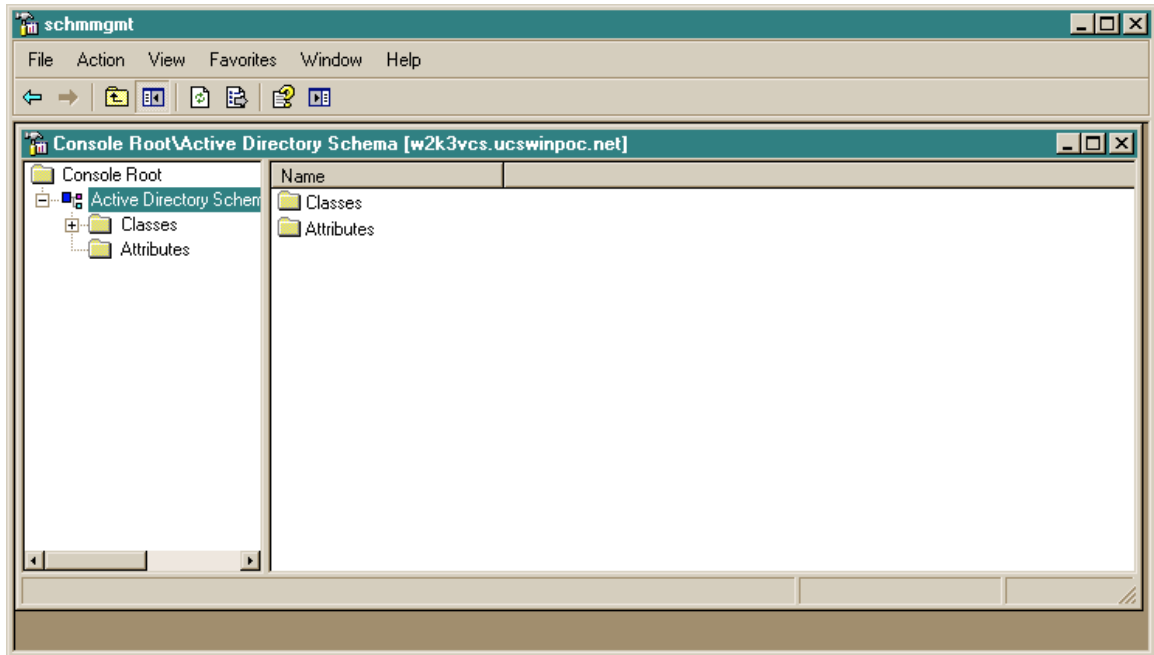
C:\regsvr32 adsiedit.dll

## Add the new CiscoAVPair attribute definition:

### Notes

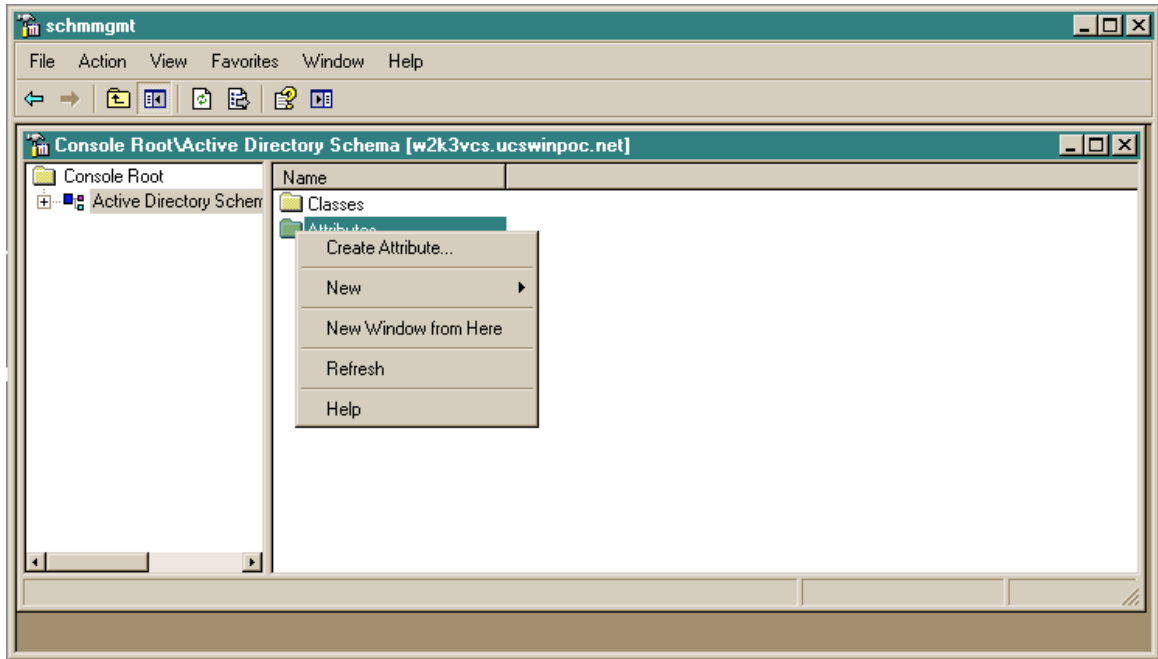
To modify the schema you must be a member of the Schema Admins group in Active Directory, or you must have been delegated the appropriate authority.

1. Open the Active Directory Schema snap-in.  
Run -> schmmgmt.msc
2. In the console tree, click Active Directory Schema.

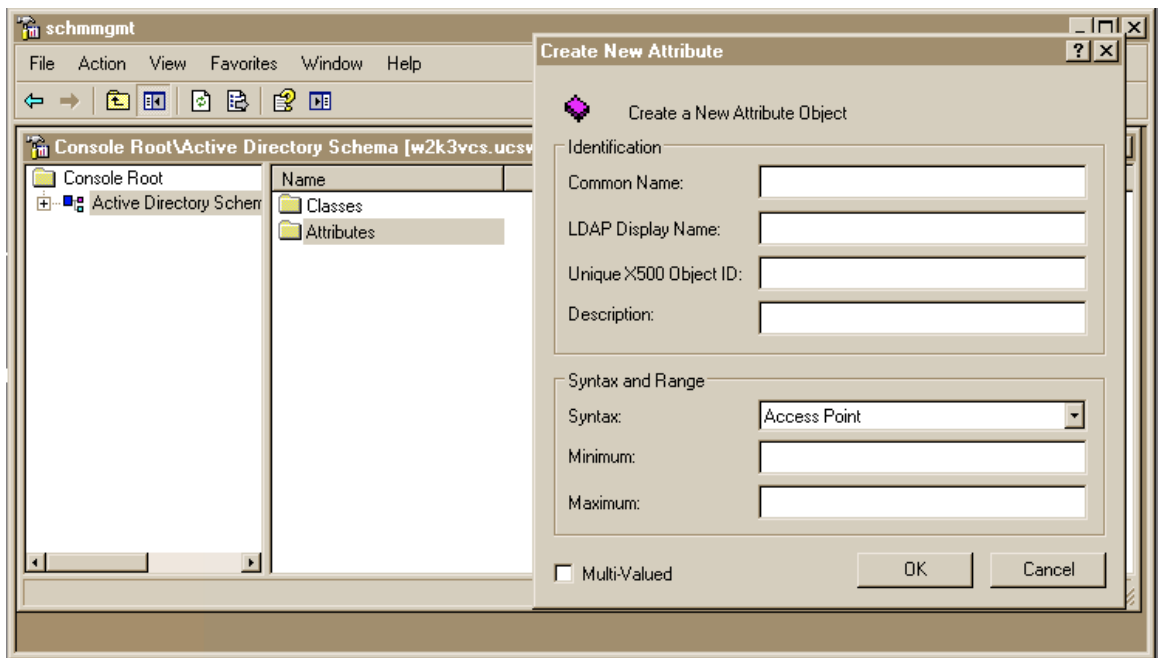


3. To add an attribute definition

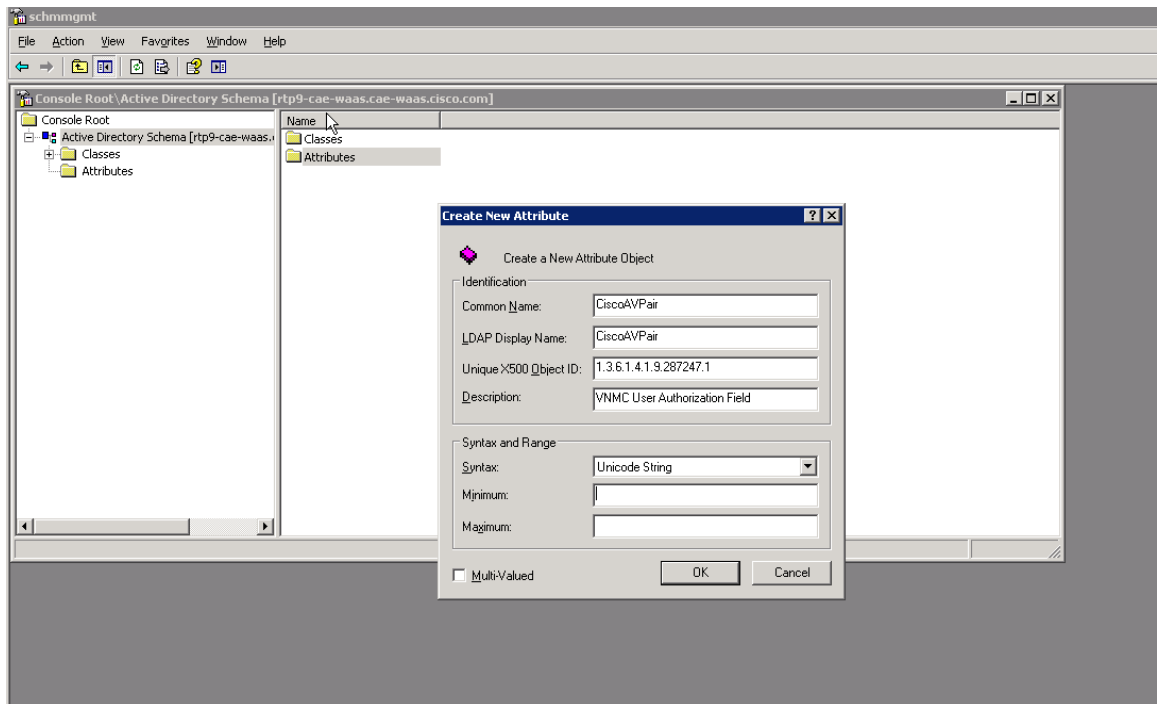
a) In the console tree, right-click Attributes



b) Click Create Attribute



c) Add CiscoAVPair to the schema.

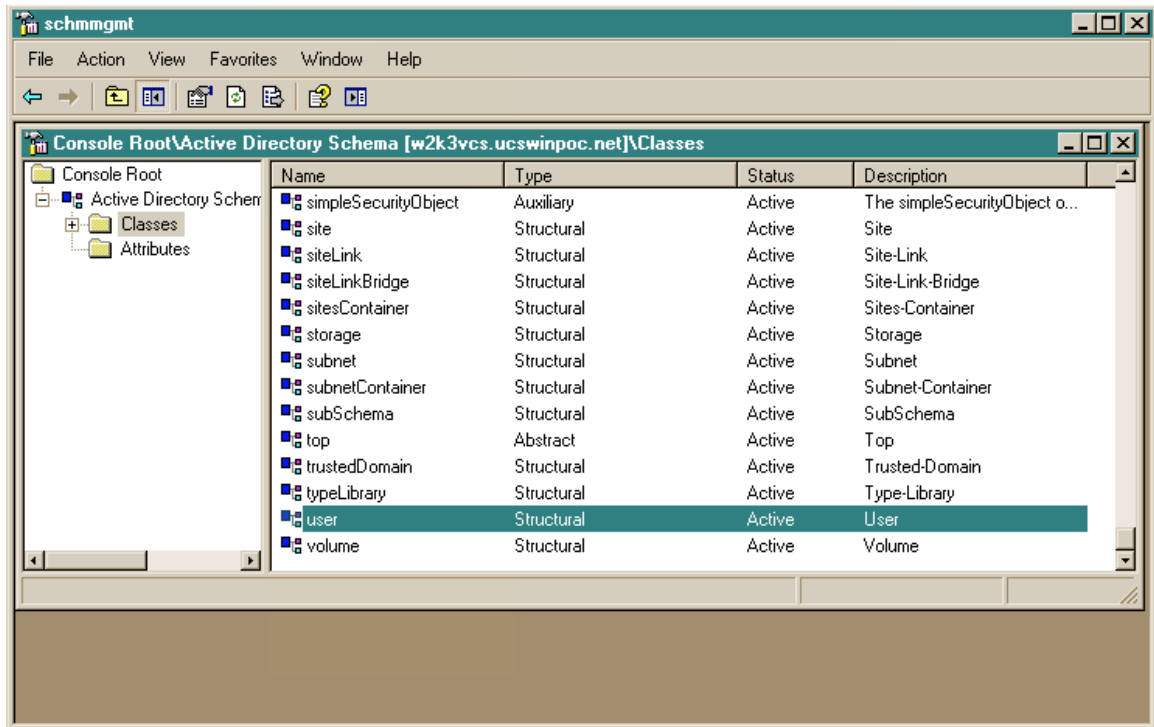


*Use the IANA values in the References section and identify as a "Unicode String"*

## Modify “user Class” – add CiscoAVPair attribute

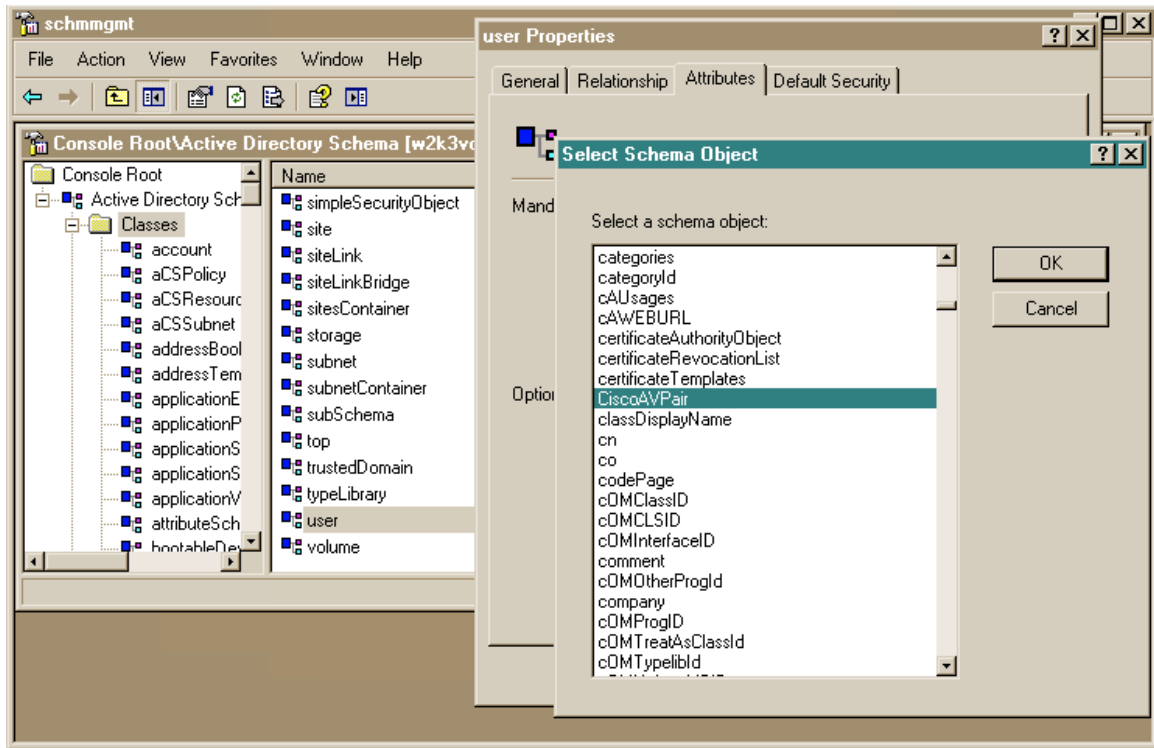
Once you have added the new attribute to the Schema you need to modify the “user” Class and add CiscoAVPair to it.

1. Open the Active Directory Schema snap-in.  
Run -> schmmgmt  
**Under Active Directory Schema choose “Classes”, on the right-hand side select “user”**





2. Right-Click “user” -> Select Properties -> Attributes Tab -> Select “CiscoAVPair” -> Ok



You are done and ready to modify Domain Users to allow remote authorization.

## Modify CiscoAVPair attribute of a Domain User.

CiscoAVPair is used to assign VNMC roles and locales to an AD Domain User. Without the CiscoAVPair attribute or if it is unset, a remotely authenticated user will have read only access to VNMC. You can use the default roles or create custom roles within VNMC.

### Default VNMC Roles:

- admin
- aaa
- network
- operations
- read-only

### CiscoAVPair Syntax:

Locales:

- Single locale
  - shell:locales="locale1"
- Multiple locales, more locales can be added by separating with spaces.
  - shell:locales="locale1 locale2"

Roles:

- Single role
  - shell:roles="role1"
- Multiple roles, more roles can be added by separating with spaces.
  - shell:roles="role1 role2"

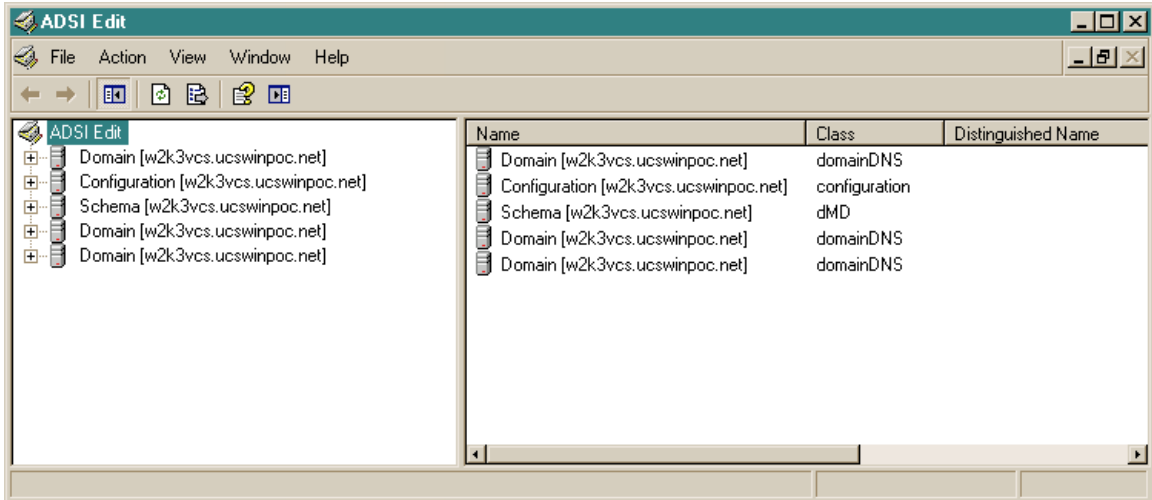
Passing both roles and locales:

Include both in the same field separated by a space  
[ shell:roles="role1" shell:locales="locale1 locale2" ]

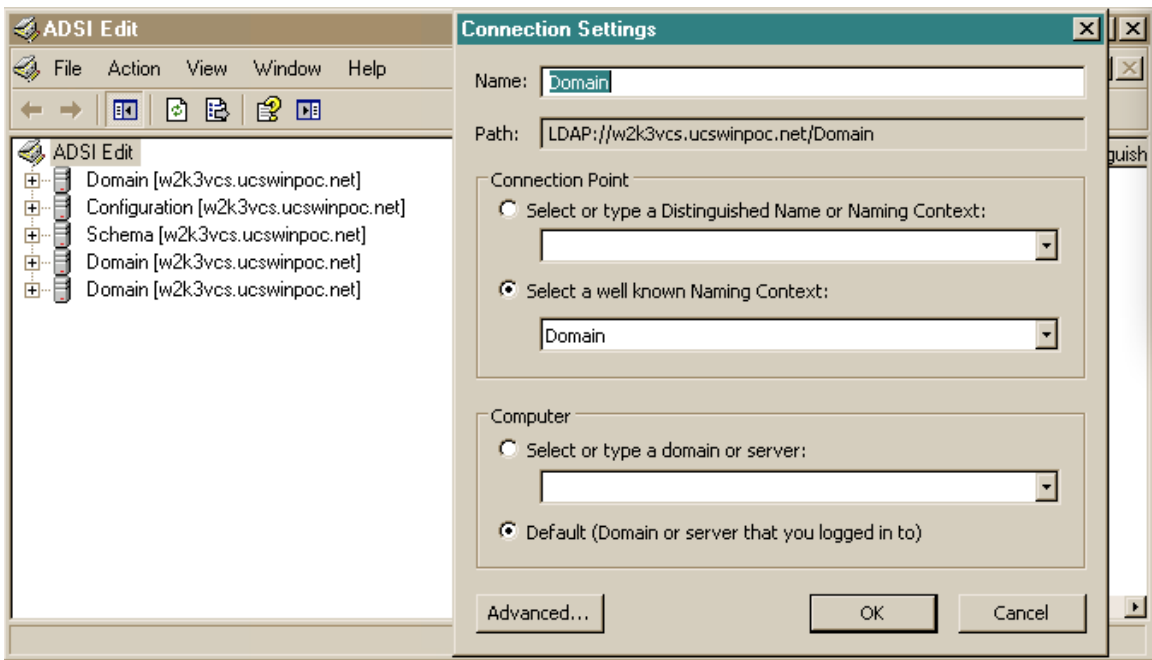
### Notes:

- The "root dn" can't have spaces in the name – the bind from VNMC will fail (*fixed in 1.0.1f*)
- All Domain Users will have "read only" access to VNMC if they are able to access the GUI/CLI/API.

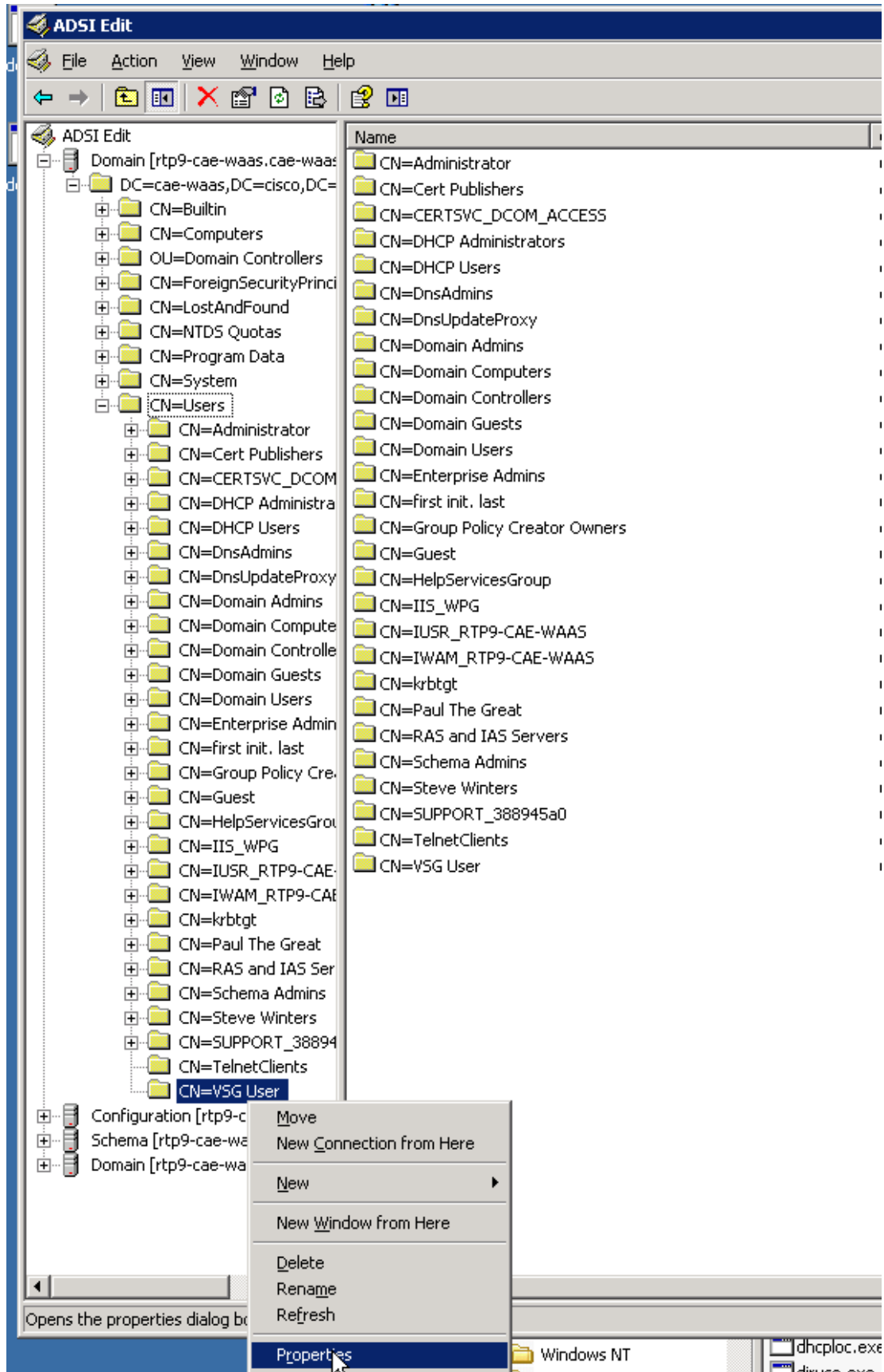
1. Run "adsiedit.msc" to bring up the utility to edit user attributes. (Note: "adsiedit.msc" is located under "C:\Program Files\Support Tools".)



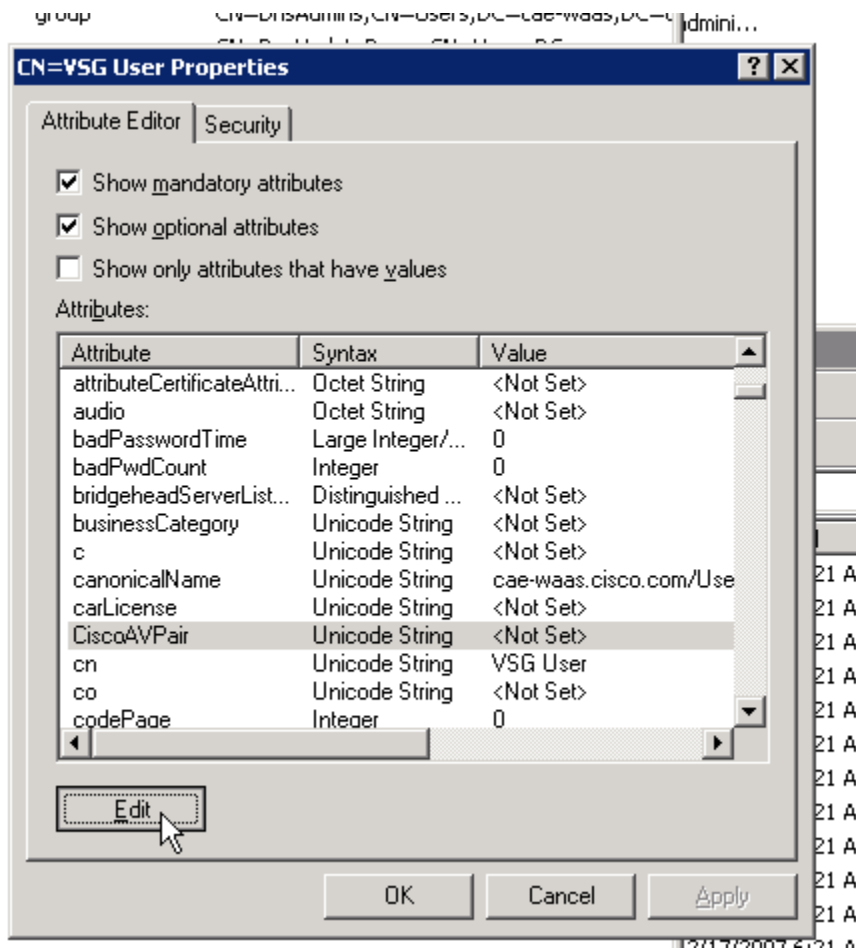
2. You need to connect to the Domain. Right-click “ADSI Edit” – Connect To - Ok

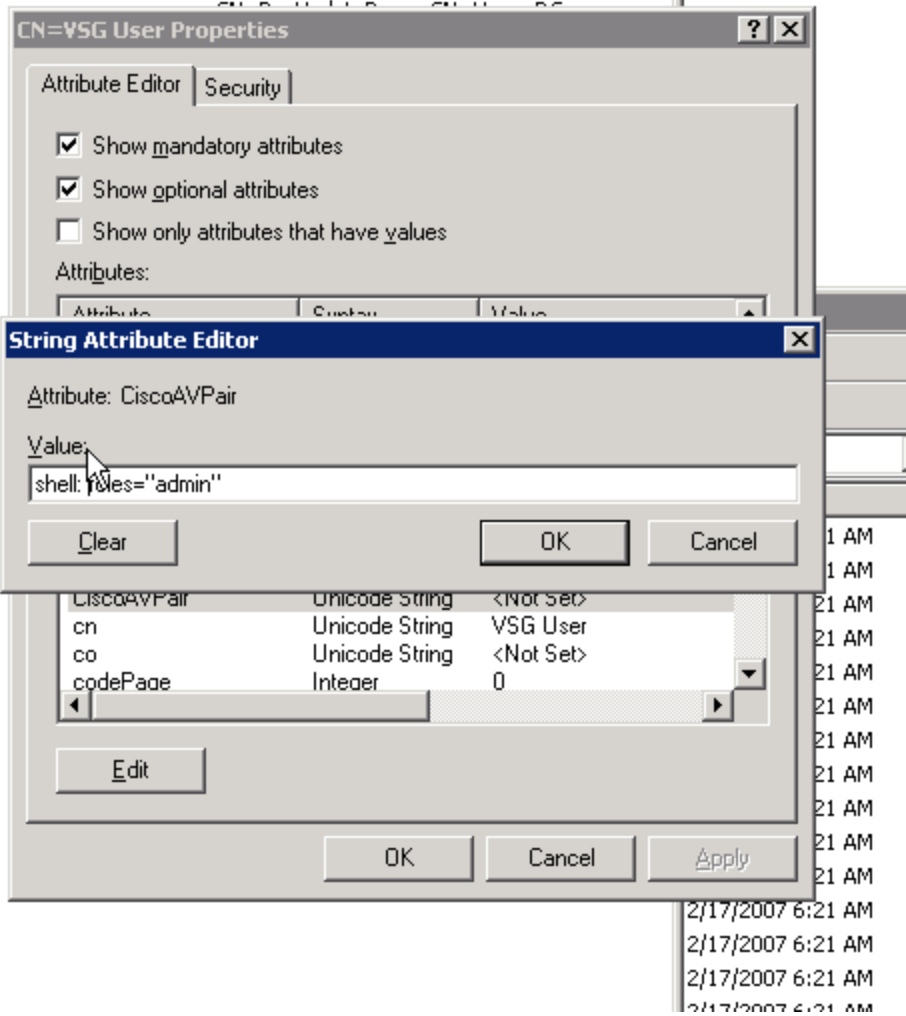


**3. Select the domain, find the user you want to edit, Right-Click -> Properties -> edit**



4. When you select “edit” you are presented with the dialogue to add roles and locales





**5. Example of adding a role and a locale:**

