Retrieving Active Directory “Memberof” attribute from Identity source

You can return group information to a RADIUS client two ways;

1. Map to AD group. Years ago Frank Miller mapped User attributes to AD groups. The problem was when RSA does the group lookup, it returned the first AD group found as the RADIUS attribute, which **may be** functionally useless, because you cannot require that an AD User only belong to a single group. Apparently some Cisco devices may have a way to parse through group information. This is this document, KB a63481
2. Frank then wrote a practical solution that will map a Radius Attribute to a value that equals the user’s Group (though not a dynamic link to an AD group through the Identity Source), and return it in a RADIUS Profile assigned to the RADIUS Client. In effect we are not mapping to Active Directory, we’re simply re-creating the groups we know exist there, and assigning bunches of users to those Profiles. This is done in order to return that group attribute to the Radius Client for every user that logins on the RADIUS Client. This example uses the existing Standard Radius attribute #25 called Class. See KBa63480-RADIUSProfileReturnsToUserGroup.pdf

Purpose: to get “memberof” attribute from AD and pass the group name to a NAS using Radius with either a custom configured radius attribute or a standard Radius attribute like Class (25) or Filter-ID (11)**.**

Prerequisites: You need to have an Identity Source correctly configured.

Limitation: Does not work on Global catalog server. You must configure on Administrative Identity Source if you are using Global catalog server.

Patch Level: AM 7.1 SP4 server or 3.0.4 Appliance or later including AM 8.0.

On Appliance 3.0 you have to patch to 3.0.0.5.

Testing: Testing is done using NTRadPing, It’s available at: **http://www.novell.com/coolsolutions/tools/14377.html**

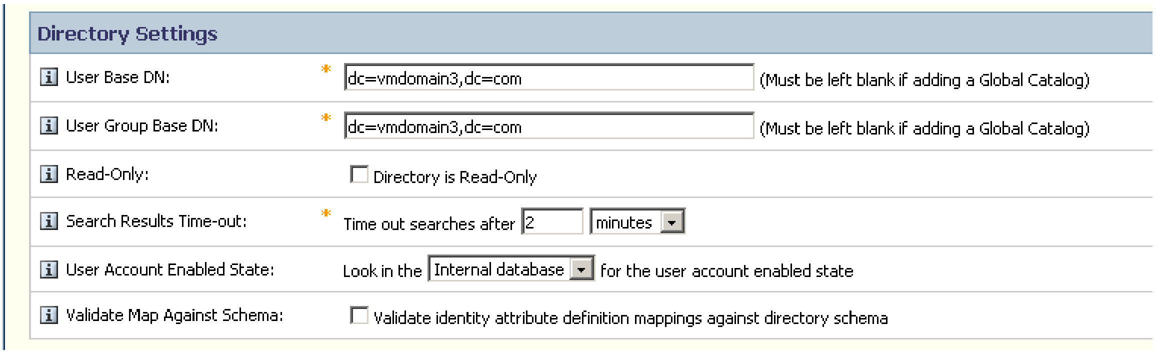
Setting Attributes: Pages 2 thru 3 are for setting the Identity attribute This will be used in both custom Radius attribute and the standard Radius attribute configuration.

Configuring a Custom Radius Attribute: pages 4 thru 6

Configuring a Standard Radius Attribute: Pages 7 thru 10

Setting up the Identity Attribute

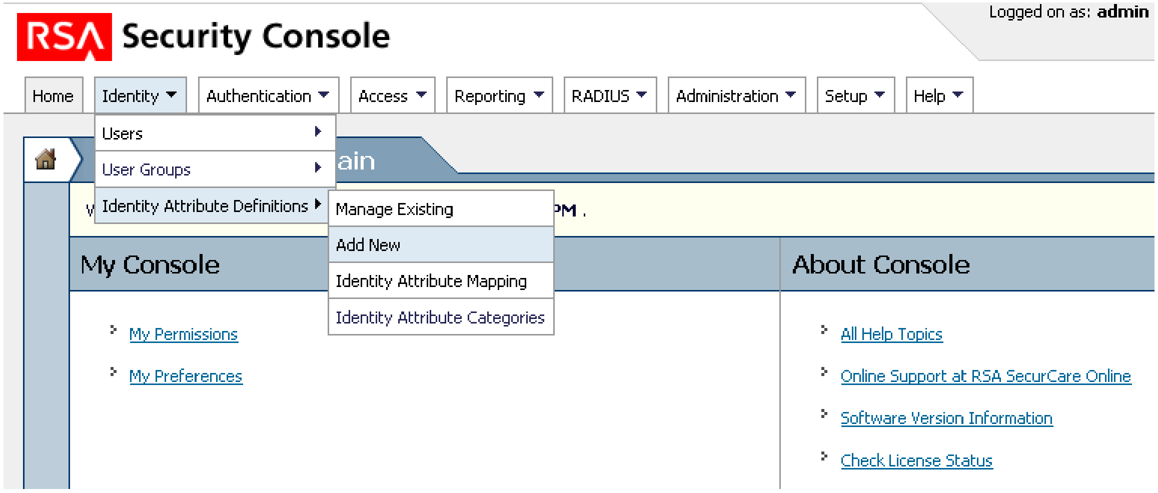
1) Go to your Operations Console and Manage Identity Source and pick edit of the identity Source that you are going to get Memberof from. In the edit window go to Map. You need to uncheck “Validate Identity Attribute…. And save it



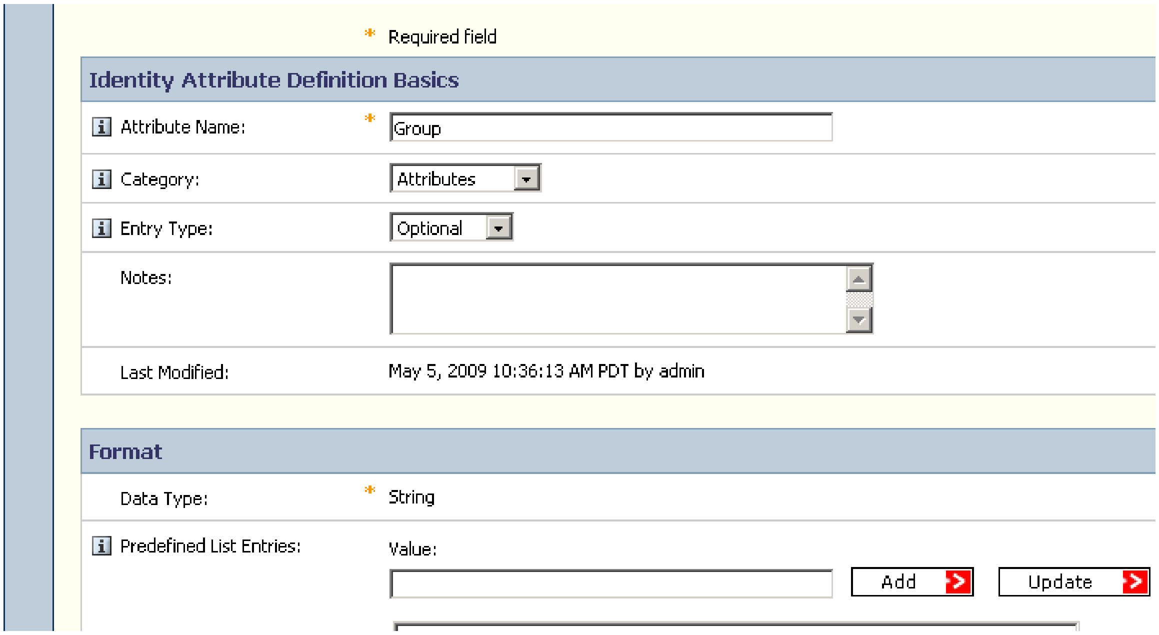
Directory Settings

User Base DN:	*	dc=vmdomain3,dc=com (Must be left blank if adding a Global Catalog)
User Group Base DN:	*	dc=vmdomain3,dc=com (Must be left blank if adding a Global Catalog)
Read-Only:		□ Directory is Read-Only
Search Results Time-out:	*	Time out searches after 2 minutes ▾
User Account Enabled State:		Look in the Internal database ▾ for the user account enabled state
Validate Map Against Schema:		□ Validate identity attribute definition mappings against directory schema

2) Next open the Security Console, and then go to Identity-> Identity Attribute Definitions->Add New.



3) **You need to configure an attribute. Give it a name (I used Group), Category= Attribute, Datatype=string.**



* Required field

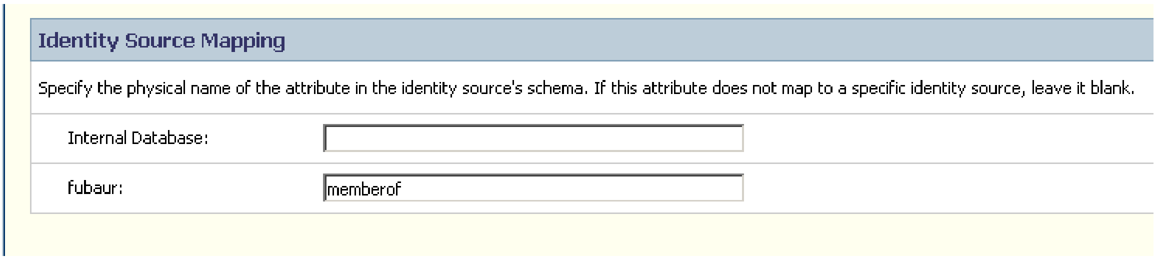
Identity Attribute Definition Basics

Attribute Name:	*	Group
Category:		Attributes
Entry Type:		Optional
Notes:		
Last Modified:		May 5, 2009 10:36:13 AM PDT by admin

Format

Data Type:	*	String
Predefined List Entries:		Value:

Pick your Identity Source and fill in the blank with “memberof”



Identity Source Mapping

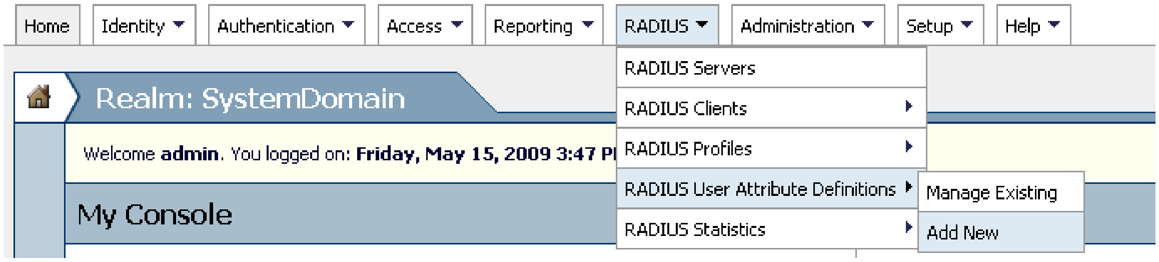
Specify the physical name of the attribute in the identity source's schema. If this attribute does not map to a specific identity source, leave it blank.

Internal Database:	
fubaur:	memberof

Leave all the rest at default and save it.

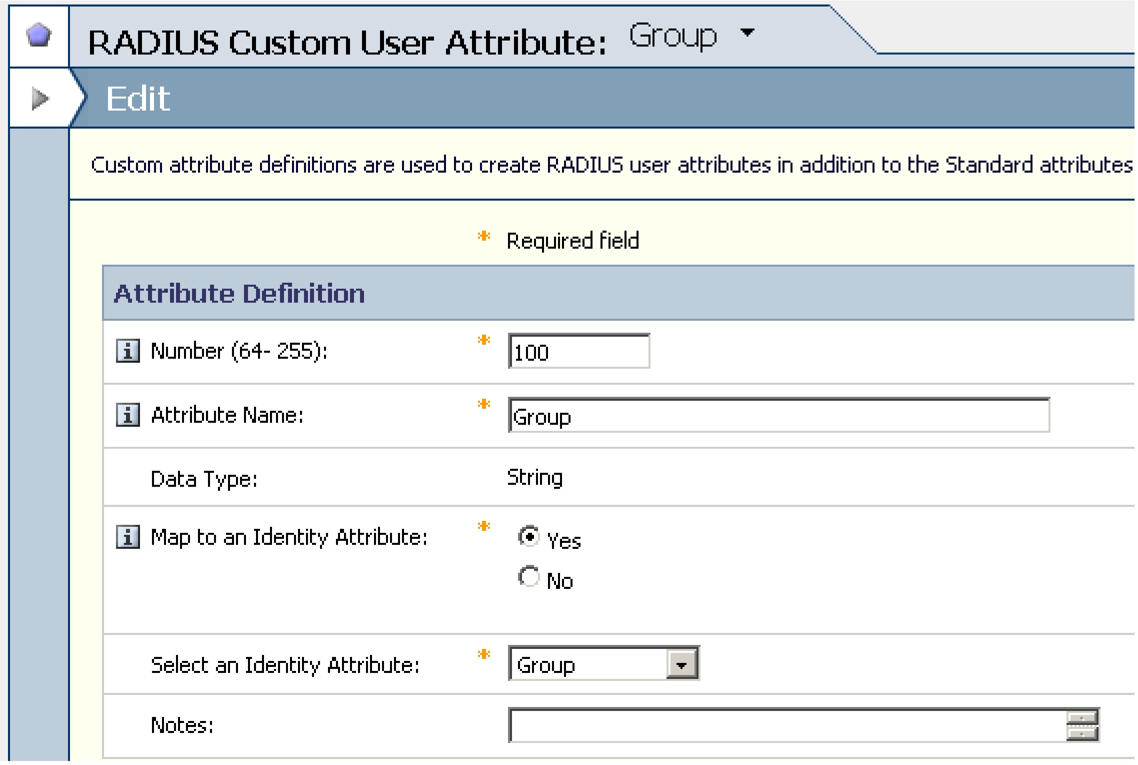
Setting up Radius to return a custom attribute (64-255)

1) From the Security Console go to Radius->Radius User Attribute Definitions->Add New



Welcome **admin**. You logged on: **Friday, May 15, 2009 3:47 P**

2) Define a Radius custom Attribute. Configure the number (I used 100), The Radius attribute name (I used Group), Map to an Identity check “yes” and select the identity attribute that you defined in previously (I also used Group for that one).



RADIUS Custom User Attribute: Group

Edit

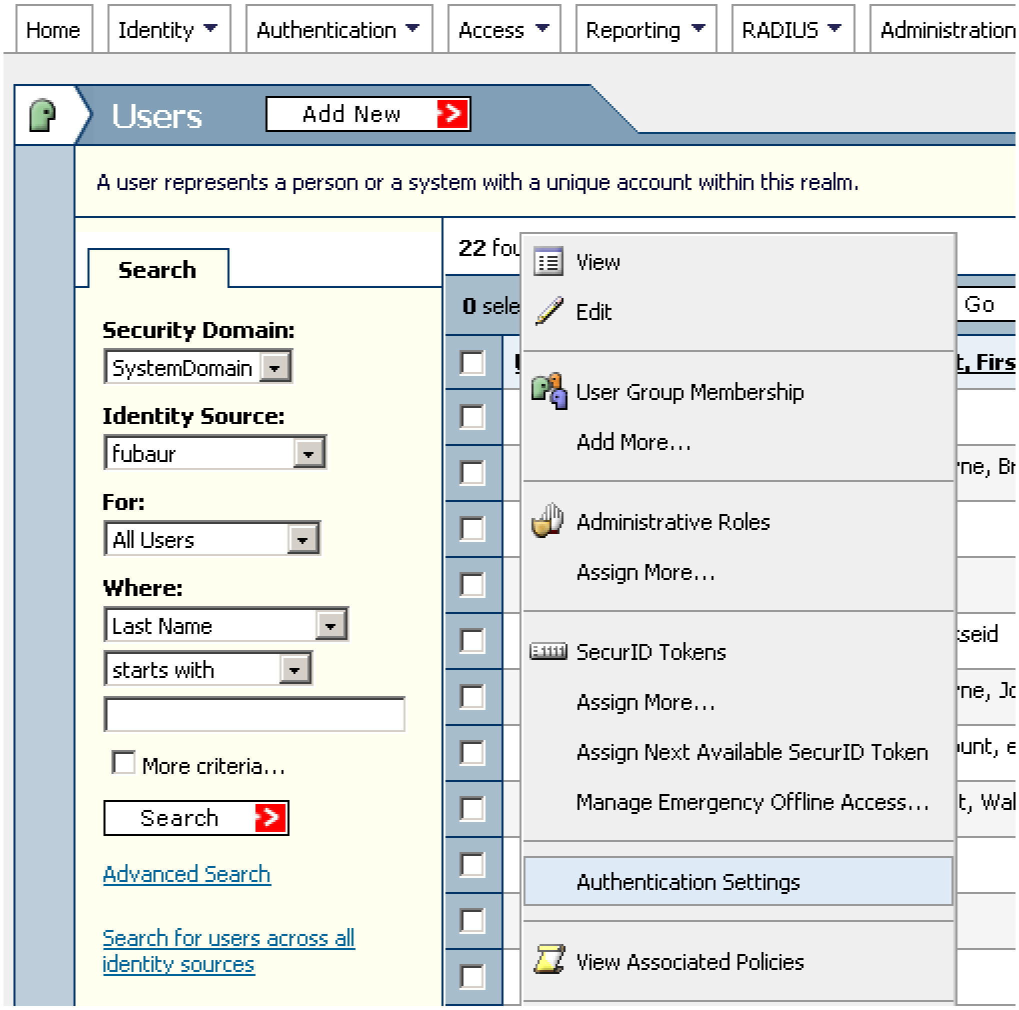
Custom attribute definitions are used to create RADIUS user attributes in addition to the Standard attributes

* Required field

Attribute Definition

Number (64- 255):	*	100
Attribute Name:	*	Group
Data Type:		String
Map to an Identity Attribute:	*	● Yes ○ No
Select an Identity Attribute:	*	Group
Notes:		

3) Now you have to enable this Attribute on the user. Go to Identity->Users->Manage existing and find the user to test with. Next go to the users pull down, and select Authentication settings



A user represents a person or a system with a unique account within this realm.

Security Domain: SystemDomain

Identity Source: fubaur

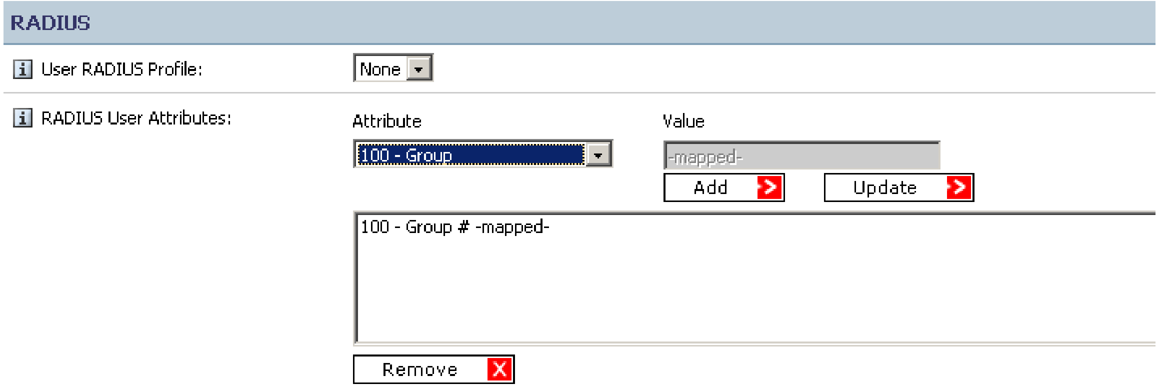
For: All Users

Where: Last Name

starts with

□ More criteria...

4) **Now you need to configure Radius. Go to Radius->Radius User Attributes. And select the custom attribute (I selected 100 – Group) and add it. Save it.**



RADIUS

User RADIUS Profile: None

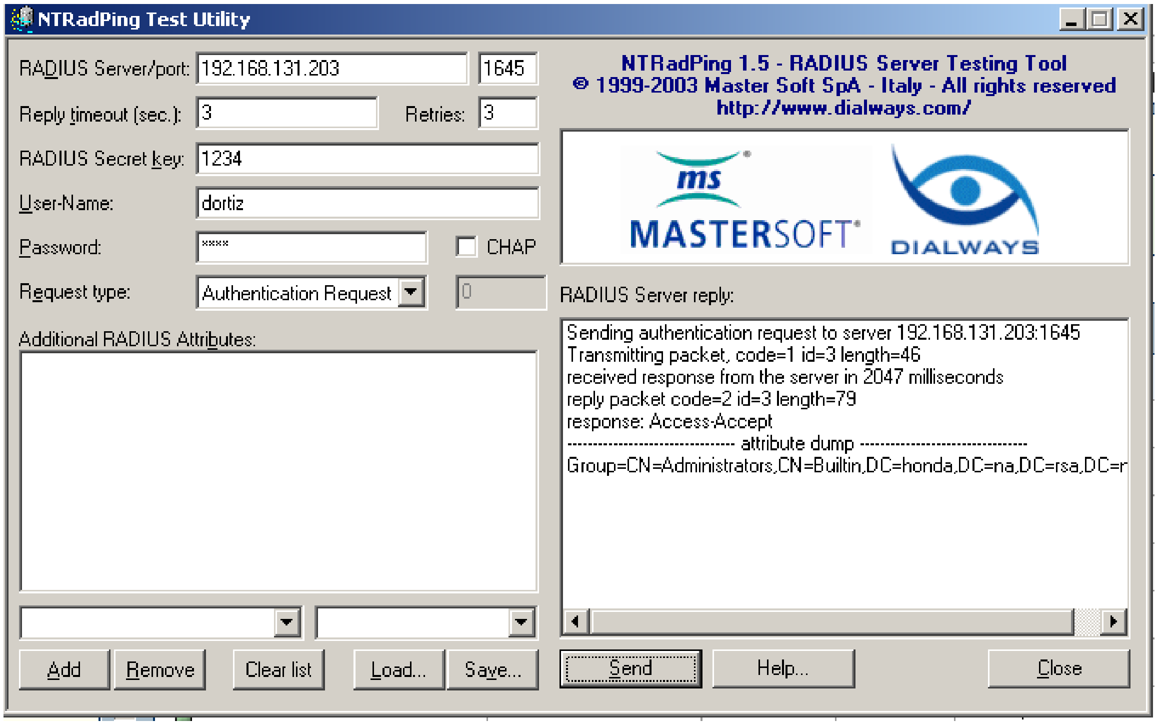
RADIUS User Attributes:

Attribute: 100 - Group

Value: -mapped-

100 - Group # -mapped-

Finally test with NTRadPing



NTRadPing Test Utility

RADIUS Server/port: 192.168.131.203 1645

Reply timeout (sec.): 3 Retries: 3

RADIUS Secret key: 1234

User-Name: dortiz

Password: ****

□ CHAP

Request type: Authentication Request 0

Additional RADIUS Attributes:

NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/

RADIUS Server reply:

```
Sending authentication request to server 192.168.131.203:1645
Transmitting packet, code=1 id=3 length=46
received response from the server in 2047 milliseconds
reply packet code=2 id=3 length=79
response: Access-Accept
-------------------------------- attribute dump --------------------------------
Group=CN=Administrators,CN=Builtin,DC=honda,DC=na,DC=rsa,DC=r
```

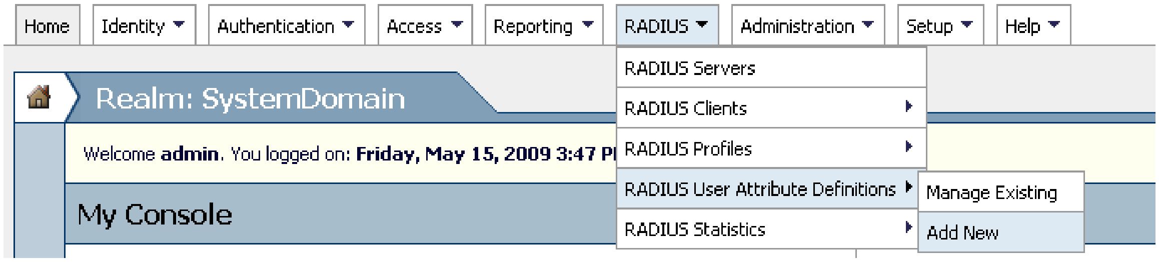
Your results might vary. I edited the radius dictionary that comes with NTRadPing to Correctly display the Custom attribute (Group) that I configured.

Configuring a standard Radius attribute to pass group information

My example will be the Class Attribute #25

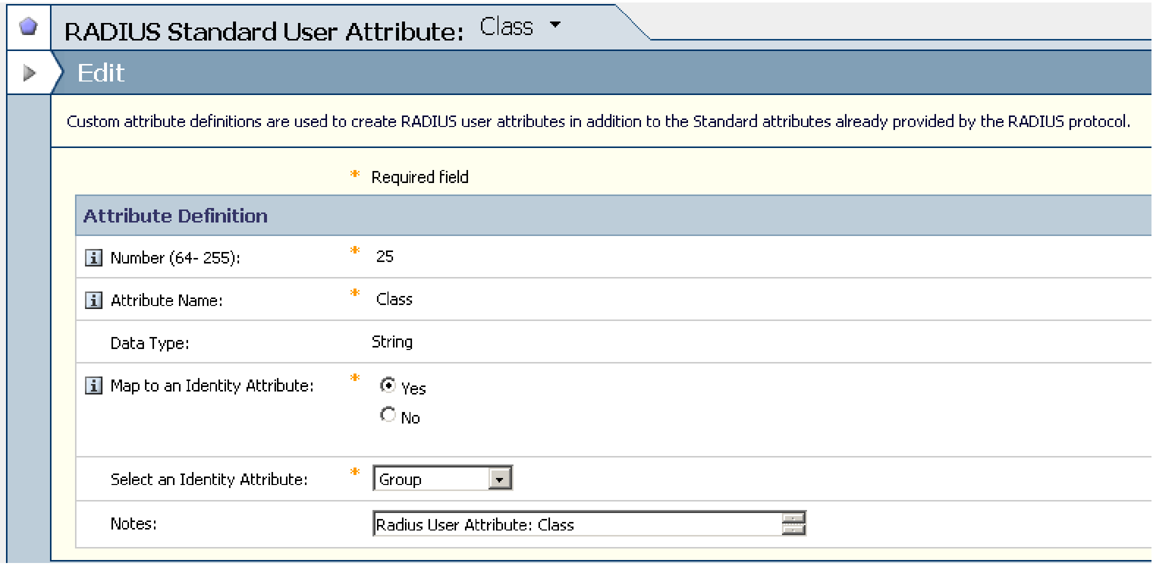
We will use the same attribute definition from page 3

1) From the Security Console go to Radius->Radius User Attribute Definitions->Manage Existing



Welcome **admin**. You logged on: **Friday, May 15, 2009 3:47 PI**

2) Select the Standard Attributes tab, then select Class and edit Next go to Map of Identity Attribute and select Yes, then select The identity attribute that you configured on page 3 (I used Group). Save



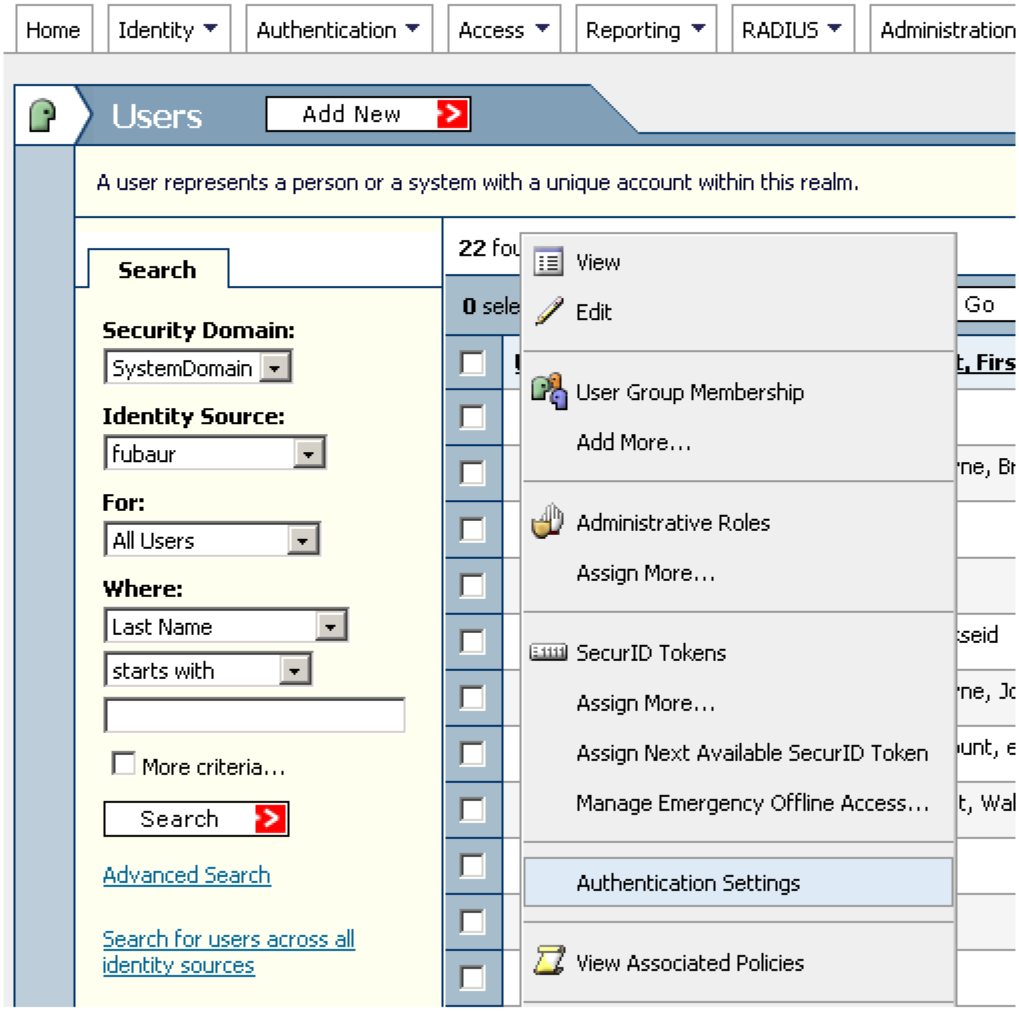
Custom attribute definitions are used to create RADIUS user attributes in addition to the Standard attributes already provided by the RADIUS protocol.

* Required field

Attribute Definition

Number (64- 255): *	25
Attribute Name: *	Class
Data Type:	String
Map to an Identity Attribute: *	● Yes ○ No
Select an Identity Attribute: *	Group
Notes:	Radius User Attribute: Class

3) Now you have to enable this Attribute on the user. Go to Identity->Users->Manage existing and find the user to test with. Next go to the users pull down, and select Authentication settings



A user represents a person or a system with a unique account within this realm.

Security Domain: SystemDomain

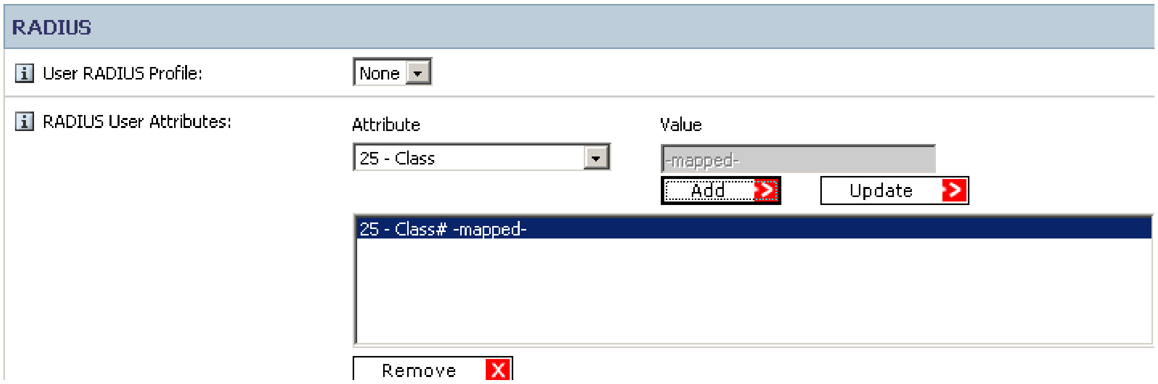
Identity Source: fubaur

For: All Users

Where: Last Name, starts with

□ More criteria...

4) Next the user has to be configured to use the Mapped Class Attribute. Select the Class attribute and add.



RADIUS

User RADIUS Profile: None

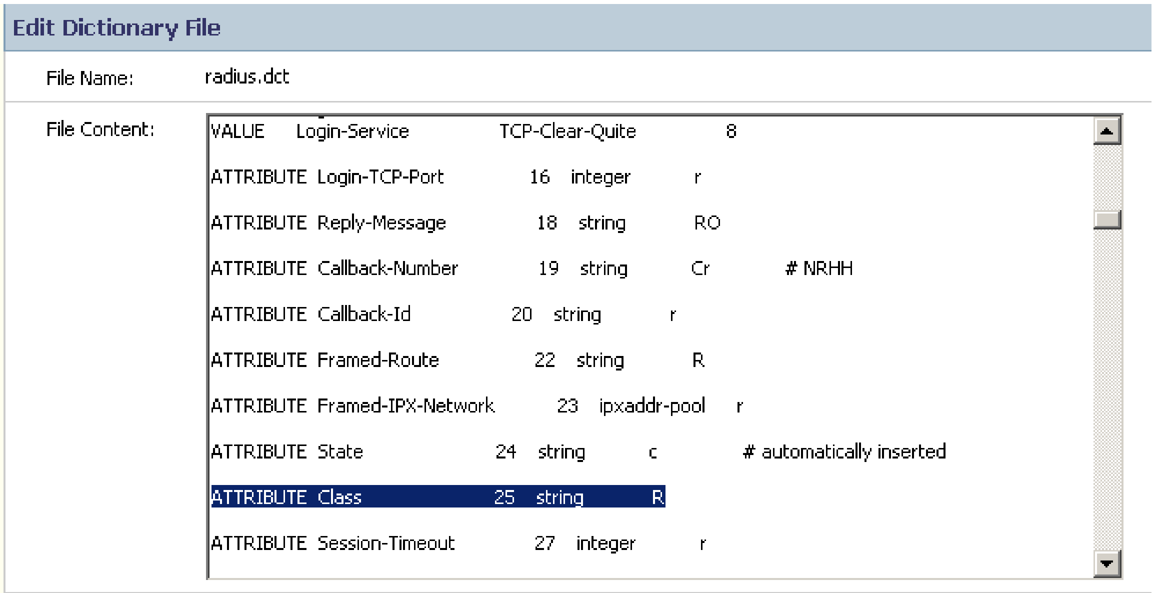
RADIUS User Attributes:

Attribute: 25 - Class

Value: -mapped-

25 - Class# -mapped-

In order to make this work properly, you must edit the Radius dictionary radius.dct You can do this from the Operations Console. Go to Deployment Configuration-> Radius->Manage Existing. There you can Manage your radius server. Go to Edit server configuration files, Select Dictionary files, then find Radius.dct and edit it. You need to find the class attribute and at the end is a lower case "r". You need To change it to an upper case "R". save it



Edit Dictionary File

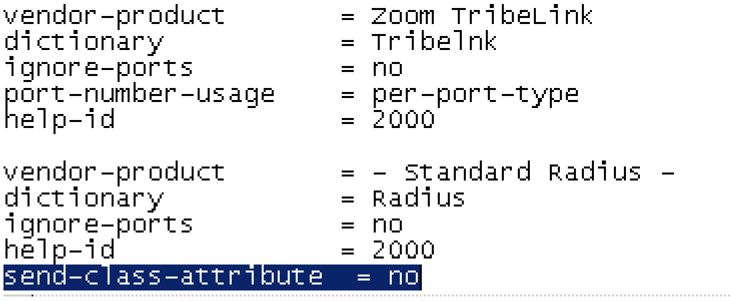
File Name: radius.dct

File Content:

```
VALUE     Login-Service          TCP-Clear-Quite          8
ATTRIBUTE  Login-TCP-Port          16   integer        r
ATTRIBUTE  Reply-Message           18   string         RO
ATTRIBUTE  Callback-Number         19   string         Cr          # NRHH
ATTRIBUTE  Callback-Id           20   string         r
ATTRIBUTE  Framed-Route            22   string         R
ATTRIBUTE  Framed-IPX-Network        23   ipxaddr-pool     r
ATTRIBUTE  State                24   string        c           # automatically inserted
ATTRIBUTE  Class                25   string        R
ATTRIBUTE  Session-Timeout         27   integer        r
```

You will need to stop and restart Radius in order for this to work. You can do this from the operations console. If you have replicas, this edit needs to be done on them too along with a stop and start of Radius.

To prevent multiple class attributes from being sent you need edit the vendor.ini File. You need to put send-class-attribute = no in the last line of the file.

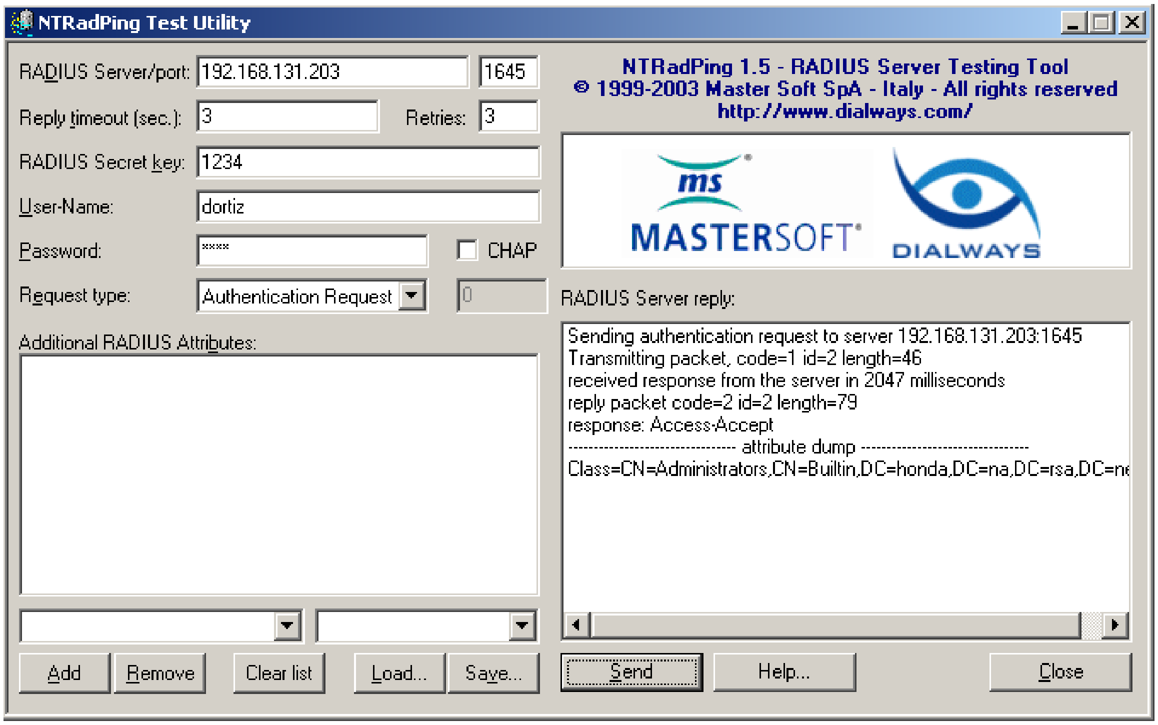


```
vendor-product         = Zoom TribeLink
dictionary             = Tribelnk
ignore-ports           = no
port-number-usage      = per-port-type
help-id                = 2000

vendor-product         = - Standard Radius -
dictionary             = Radius
ignore-ports           = no
help-id                = 2000
send-class-attribute   = no
```

After the edit you will need to stop and start Radius. You can do this from the Operations Console. If you have replicas, this edit needs to be done on them too along with a stop and start of Radius.

Finally test with NTRadPing



NTRadPing Test Utility
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
ms MASTERSOFT
DIALWAYS
Additional RADIUS Attributes:
Add
Remove
Clear list
Load...
Save...
Send
Help...
Close

RADIUS Server/port: 192.168.131.203 1645

Reply timeout (sec.): 3 Retries: 3

RADIUS Secret key: 1234

User-Name: dortiz

Password: **** □ CHAP

Request type: Authentication Request 0

RADIUS Server reply:

```
Sending authentication request to server 192.168.131.203:1645
Transmitting packet, code=1 id=2 length=46
received response from the server in 2047 milliseconds
reply packet code=2 id=2 length=79
response: Access-Accept
------------------------------ attribute dump ------------------------------
Class=CN=Administrators,CN=Builtin,DC=honda,DC=na,DC=rsa,DC=ne
```

There is one limitation. If the user is a member of multiple groups, Radius will only pickup the first one sent to it by Active Directory