Application Note

Setting up RADIUS authentication on Opengear devices using Windows 2003 Internet Authentication Service

Opengear devices can be set up to authenticate and get permission information via the RADIUS authentication protocol. This document describes how to set up an Opengear device, and Windows 2003 so that the Opengear can authenticate against existing Windows user accounts.

Configuring Windows 2003 server

To use Windows 2003 for RADIUS authentication, the **Internet Authentication Service (IAS)** needs to be installed. If it is installed, there will be an entry in the Administrative Tools menu.

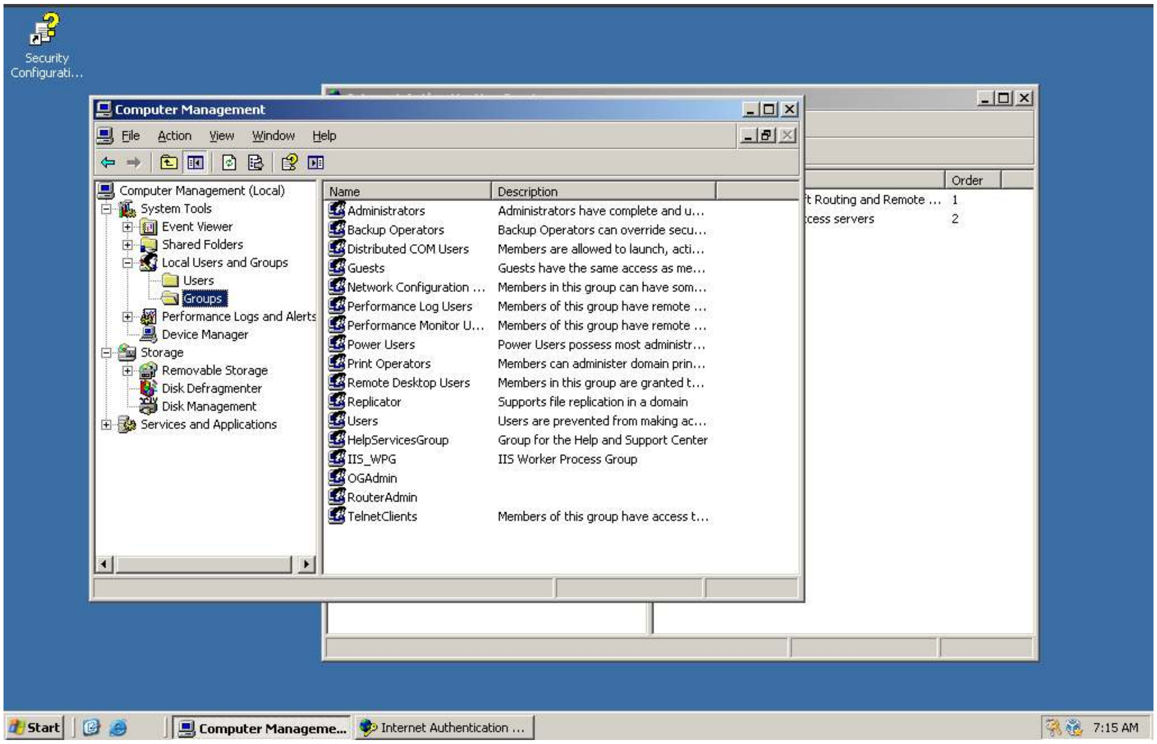
If it is not installed, you will need a Windows 2003 installation disc.

> Go to Control Panel, and click on Add/Remove Programs.
>
> Click on Add/Remove Windows Components, and then browse down to the Networking tick box, and tick it.
>
> When expanded, you should see a number of options such as DHCP/DNS etc, and Internet Authentication Service. Tick that, and click OK until Windows starts installing it.

In this App-Note, the Windows 2003 installation we are using does not have Active Directory installed. Active Directory will not affect the use of RADIUS, but the group and user configuration menus are different.

The example scenario that this Tech-Note covers, is creating a “Router Administration” Group, members of which will be able to get to the console of a Cisco Router connected to the Opengear device (in this case, the router is on console port 3).

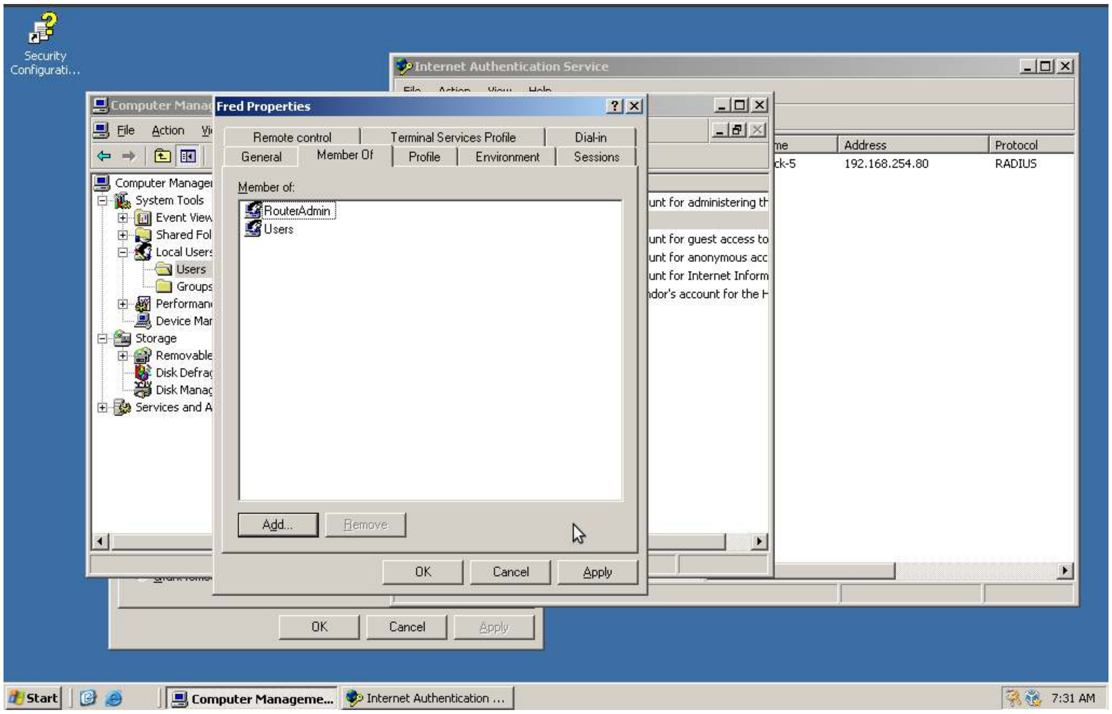
The first step is to create the *RouterAdmin* group. Of course, existing groups can be used for this.



Name	Description
Administrators	Administrators have complete and u…
Backup Operators	Backup Operators can override secu…
Distributed COM Users	Members are allowed to launch, acti…
Guests	Guests have the same access as me…
Network Configuration …	Members in this group can have som…
Performance Log Users	Members of this group have remote …
Performance Monitor U…	Members of this group have remote …
Power Users	Power Users possess most administr…
Print Operators	Members can administer domain prin…
Remote Desktop Users	Members in this group are granted t…
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac…
HelpServicesGroup	Group for the Help and Support Center
IIS_WPG	IIS Worker Process Group
OGAdmin	
RouterAdmin	
TelnetClients	Members of this group have access t…

In the above screen shot, you'll notice that a RouterAdmin group has been created.

Once the group is created, add any users that you wish to have access to port 3 on the Opengear to this group.



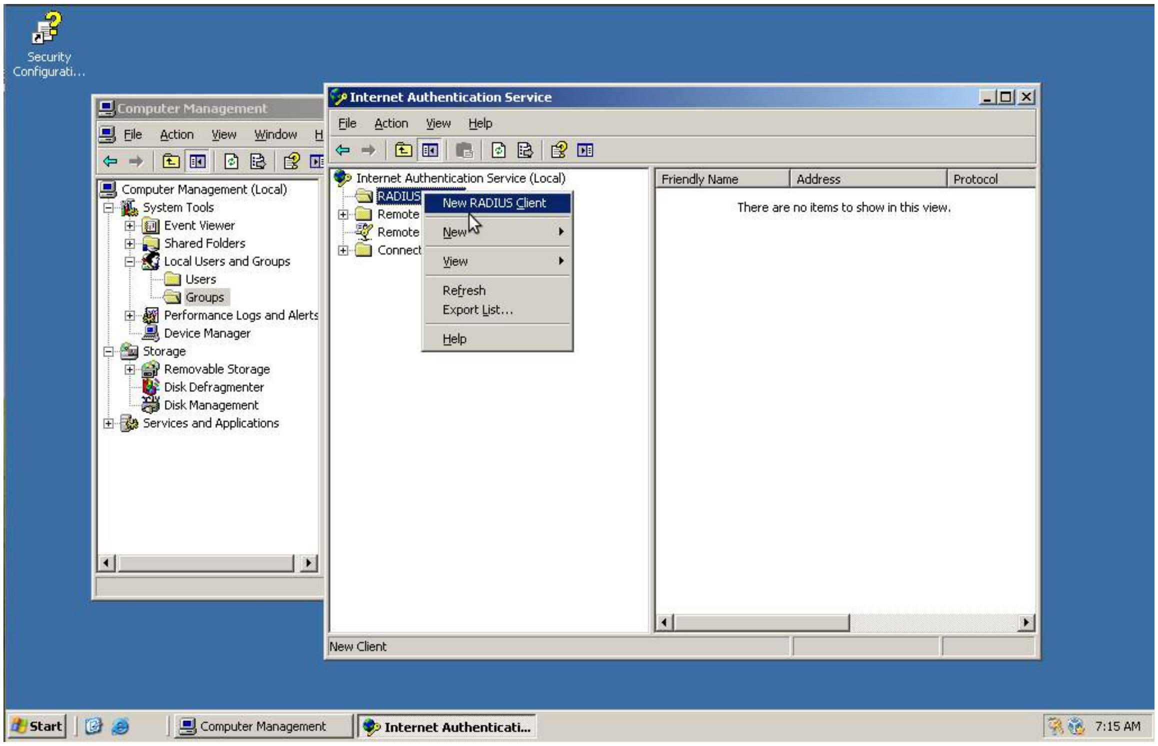
Member of:
RouterAdmin
Users

In the above screen shot, user "Fred" has been made a member of the "RouterAdmin" group.

The next step is to configure the RADIUS client.

Open up the Internet Authentication Service configuration app by going to Administrative Tools, and selection Internet Authentication Service.

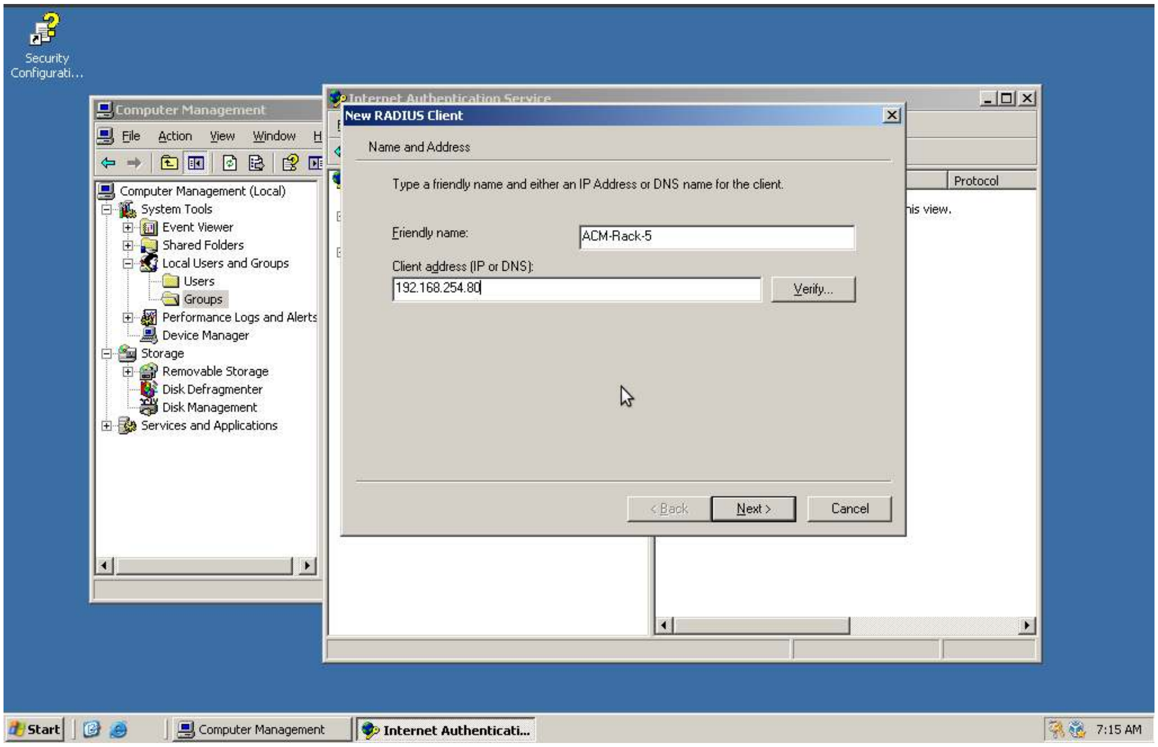
Right click on RADIUS Clients and select New RADIUS Client.



There are no items to show in this view.

The RADIUS client corresponds with the Opengear device, so fill in the IP address or DNS name of the Opengear device, and choose a simple name for the device. This name will be used later on in the Remote Access Policy, so choose something consistent if you multiple devices.

Once you have filled in these details, click Next.


New RADIUS Client

Name and Address

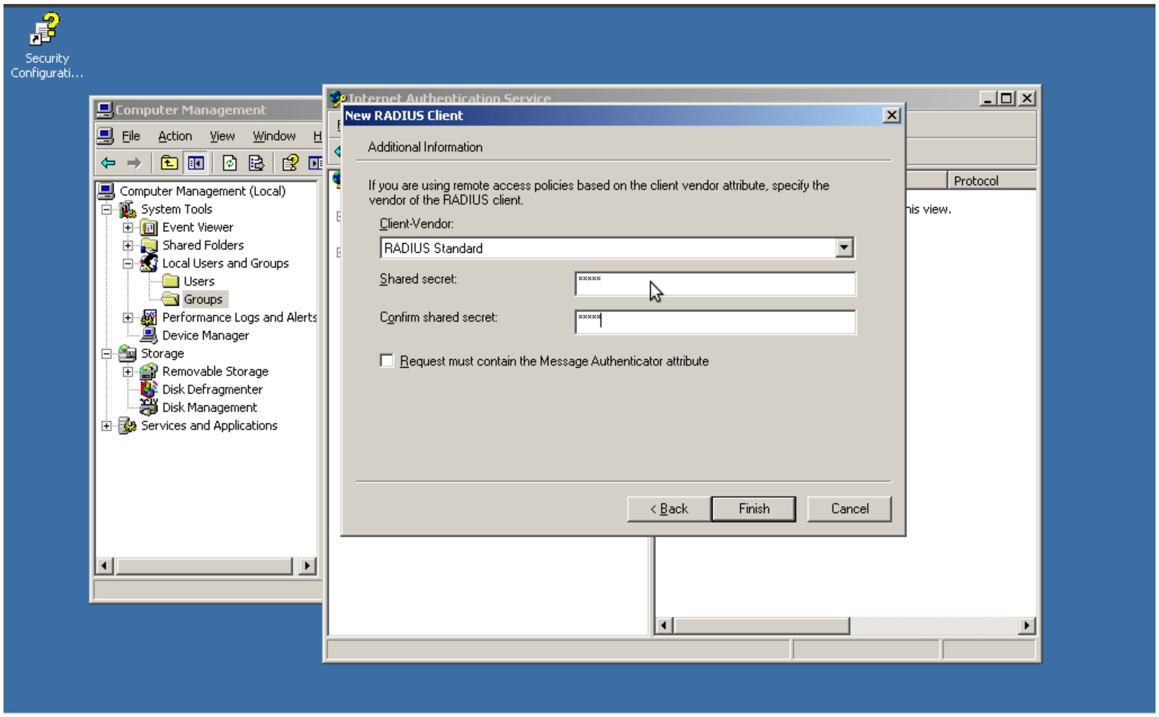
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: ACM-Rack-5

Client address (IP or DNS): 192.168.254.80

Now, choose a shared secret. This is the RADIUS password that is set on the Opengear device, and is used to encrypt all authentication traffic between the Opengear and the RADIUS server. Leave the “Request must contain Message Authenticator Attribute” tick box un-ticked.

When the shared secret is entered, click Finish.


New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

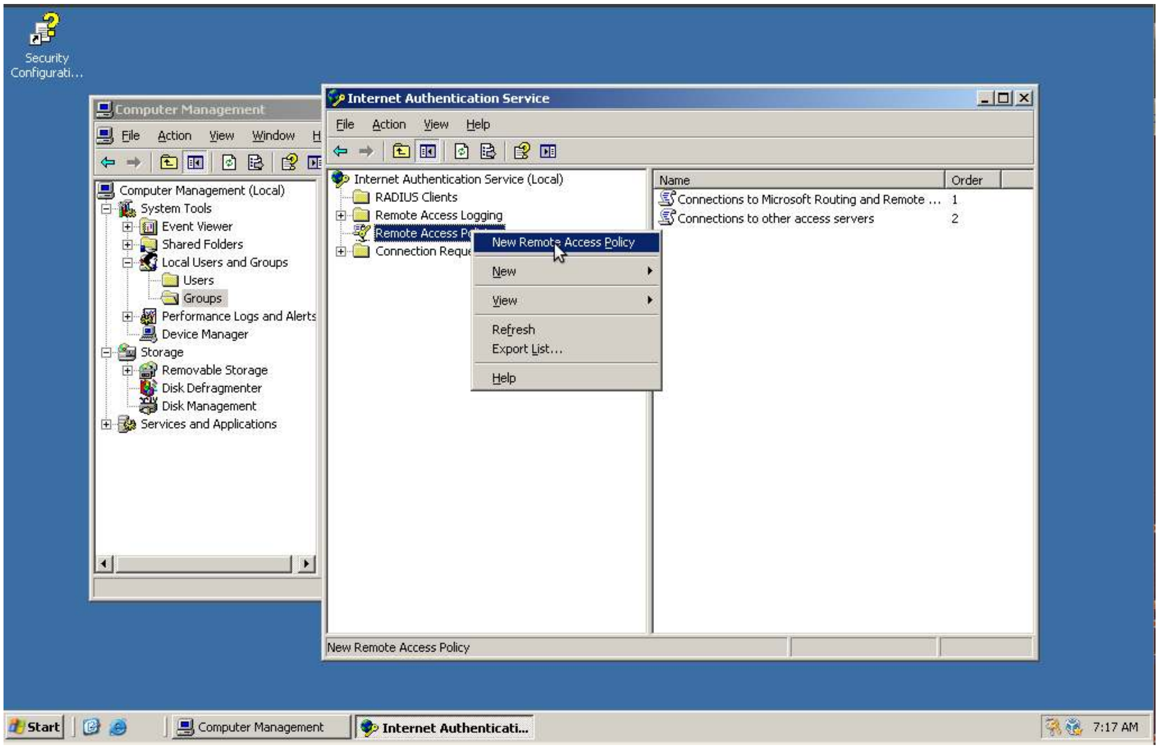
Shared secret: *****

Confirm shared secret: *****

☐ Request must contain the Message Authenticator attribute

Next, we create a new Remote Access Policy. These policies are used to evaluate incoming RADIUS Access Requests from RADIUS clients.

Right click on the Remote Access Policies folder, and then select New Remote Access Policy.

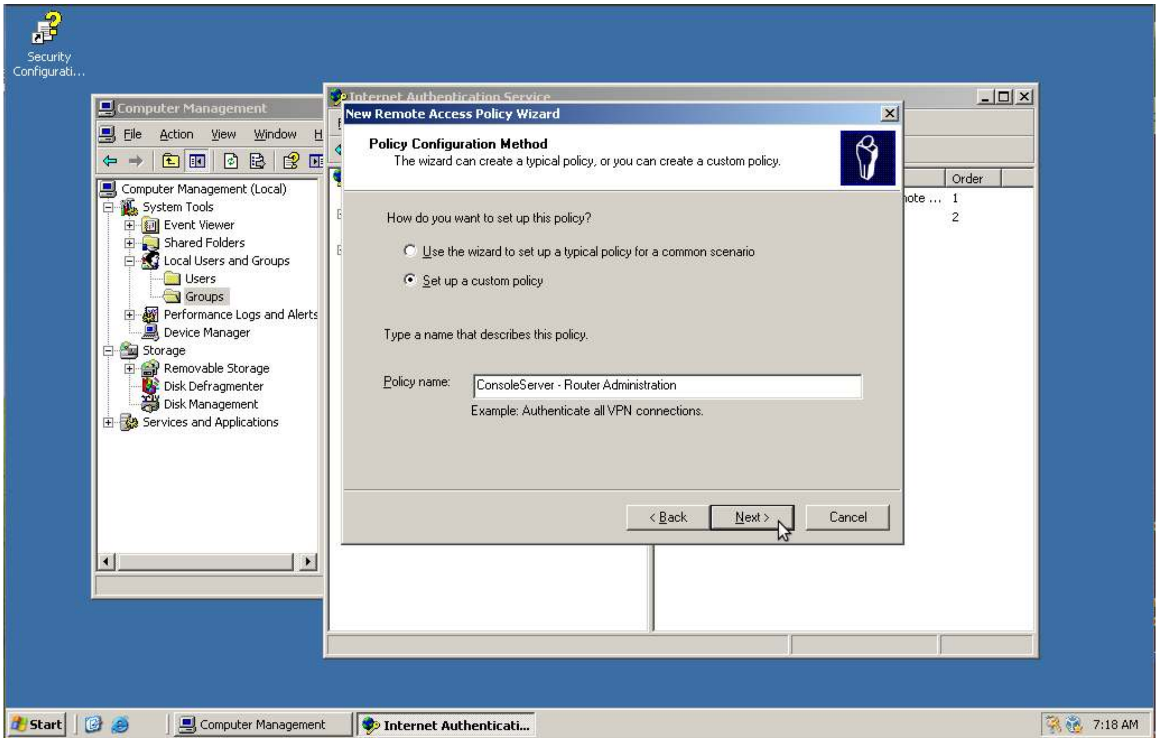


Name	Order
Connections to Microsoft Routing and Remote …	1
Connections to other access servers	2

New Remote Access Policy

Select “Set up a custom policy”, and then fill in the policy name. This is a descriptive name, and is not referenced anywhere else.

Once filled in, click Next



New Remote Access Policy Wizard

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

○ Use the wizard to set up a typical policy for a common scenario

● Set up a custom policy

Type a name that describes this policy.

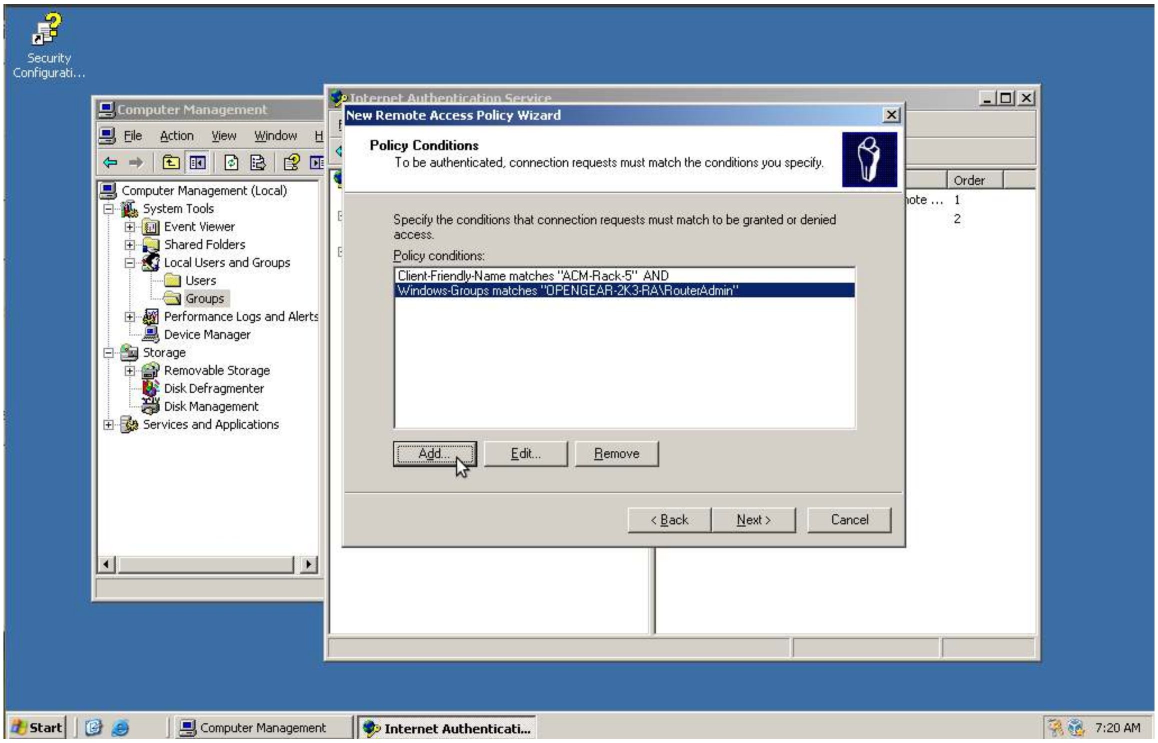
Policy name: ConsoleServer - Router Administration

Example: Authenticate all VPN connections.

Fill in the Remote Access Policy Conditions.

Incoming RADIUS requests are evaluated against these conditions, and if they match, then this policy is used to either Grant or Deny access. In this case, we are matching against two items; the “Client-Friendly-Name”, which is the name that was assigned to the Opengear in the RADIUS Client setup, and the “Windows-Group”, which will be set to the RouterAdmin group created earlier.

Use the Add button to add these conditions, and then click Next.



New Remote Access Policy Wizard

Policy Conditions

To be authenticated, connection requests must match the conditions you specify.

Specify the conditions that connection requests must match to be granted or denied access.

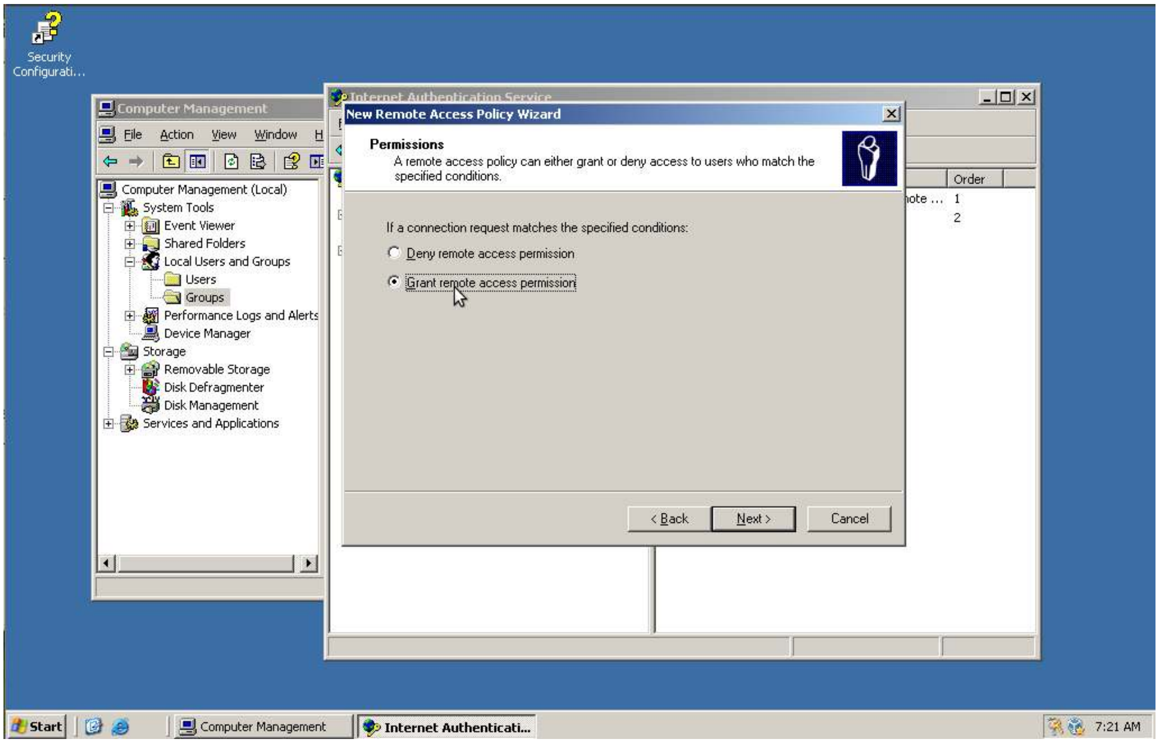
Policy conditions:

```
Client-Friendly-Name matches "ACM-Rack-5" AND
Windows-Groups matches "OPENGEAR-2K3-RA\RouterAdmin"
```

This screen determines what action will be taken if the incoming RADIUS request matches this policy.

Select Grant remote access permission, and click Next.

On the next screen, click Edit Profile



New Remote Access Policy Wizard

Permissions

A remote access policy can either grant or deny access to users who match the specified conditions.

If a connection request matches the specified conditions:

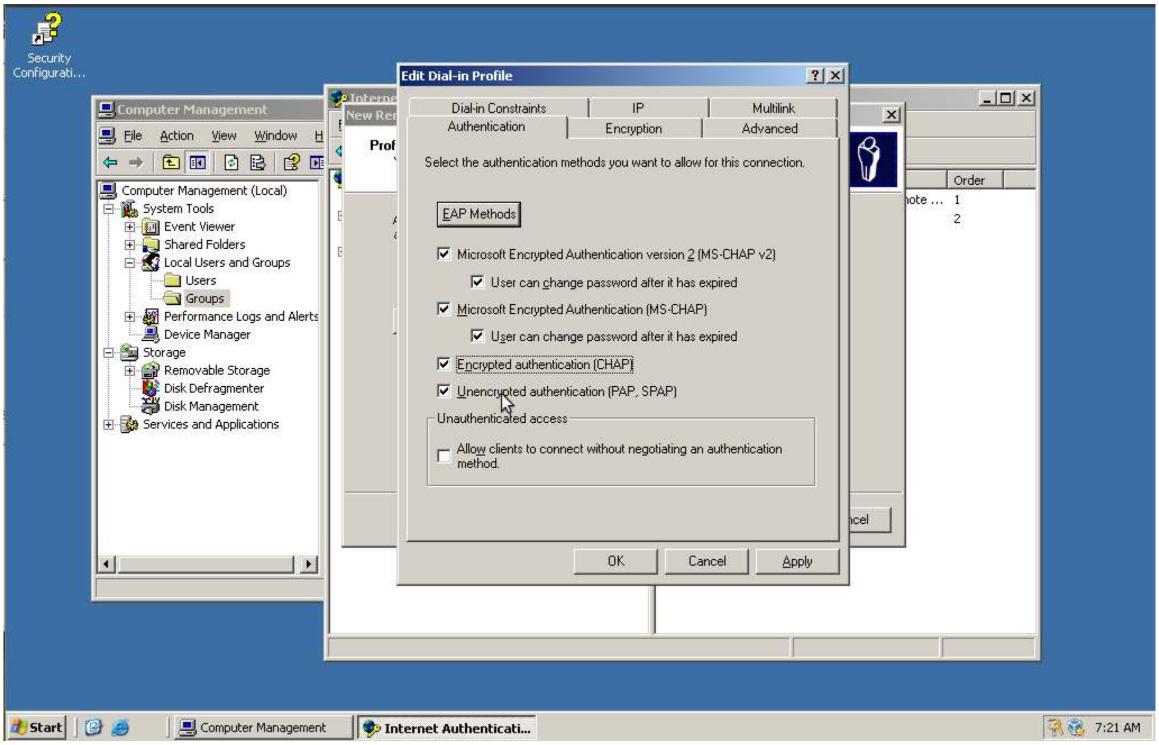
○ Deny remote access permission

● Grant remote access permission

To let the Opengear authenticate against the RADIUS server, click on the Authentication tab, and make sure Encrypted authentication (CHAP) and Unencrypted authentication (PAP,SPAP) are ticked.

In Dial-in networking, PAP is considered unsafe, but when used in RADIUS, any password data is encrypted using the RADIUS shared-secret, which means that PAP related security concerns do not apply.

When this is done, click Apply.



Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☑ User can change password after it has expired

☑ Encrypted authentication (CHAP)

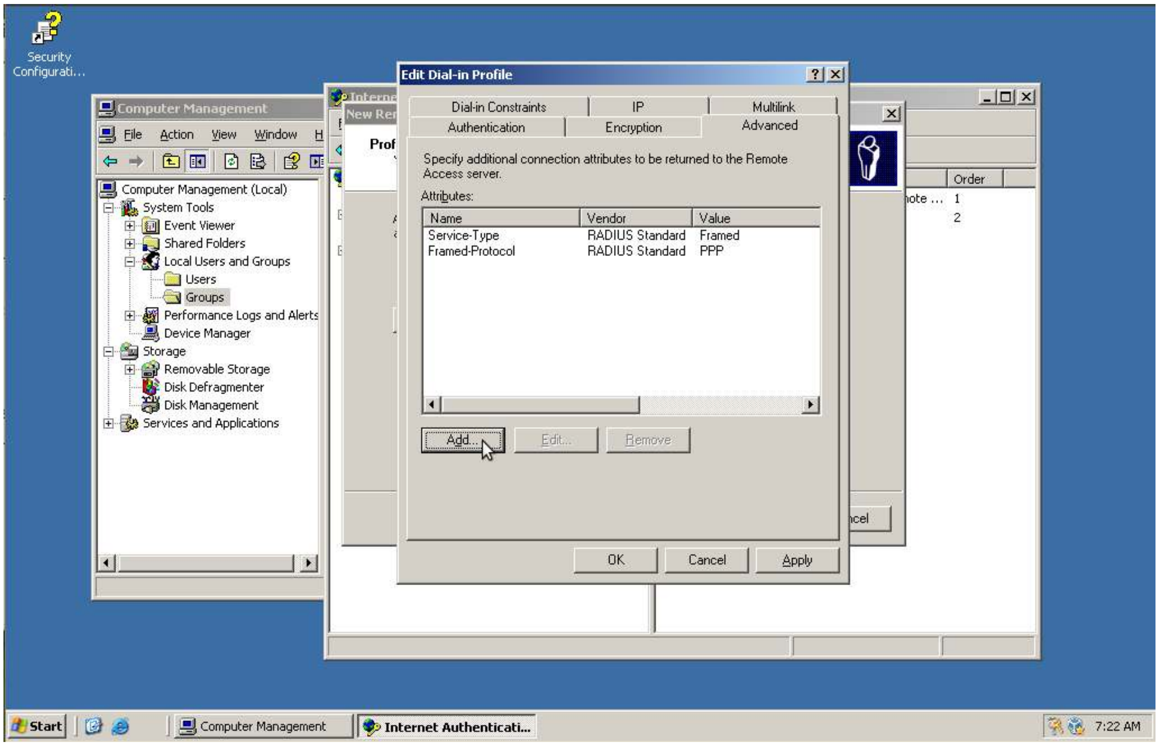
☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☐ Allow clients to connect without negotiating an authentication method.

Next, click on the Advanced Tab. This tab allows the user to specify which RADIUS attributes are sent back to the RADIUS client on successful authentication. The Opengear devices use the “Filter-ID” attribute to determine which groups the authenticated user should be a part of.

Click the Add button.



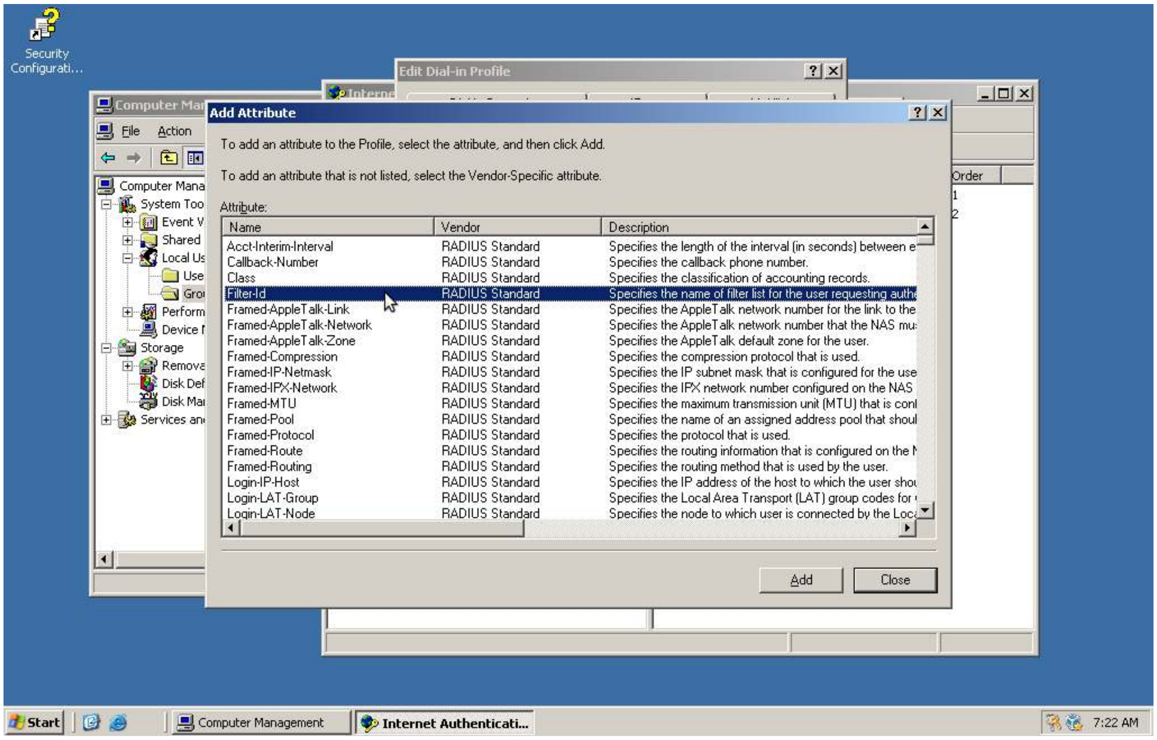
Edit Dial-in Profile

Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Framed-Protocol	RADIUS Standard	PPP

Select the Filter-ID attribute, and then click Add.



Add Attribute

To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Acct-Interim-Interval	RADIUS Standard	Specifies the length of the interval (in seconds) between e
Callback-Number	RADIUS Standard	Specifies the callback phone number.
Class	RADIUS Standard	Specifies the classification of accounting records.
Filter-Id	RADIUS Standard	Specifies the name of filter list for the user requesting authe
Framed-AppleTalk-Link	RADIUS Standard	Specifies the AppleTalk network number for the link to the
Framed-AppleTalk-Network	RADIUS Standard	Specifies the AppleTalk network number that the NAS mu
Framed-AppleTalk-Zone	RADIUS Standard	Specifies the AppleTalk default zone for the user.
Framed-Compression	RADIUS Standard	Specifies the compression protocol that is used.
Framed-IP-Netmask	RADIUS Standard	Specifies the IP subnet mask that is configured for the use
Framed-IPX-Network	RADIUS Standard	Specifies the IPX network number configured on the NAS
Framed-MTU	RADIUS Standard	Specifies the maximum transmission unit (MTU) that is con
Framed-Pool	RADIUS Standard	Specifies the name of an assigned address pool that shoul
Framed-Protocol	RADIUS Standard	Specifies the protocol that is used.
Framed-Route	RADIUS Standard	Specifies the routing information that is configured on the N
Framed-Routing	RADIUS Standard	Specifies the routing method that is used by the user.
Login-IP-Host	RADIUS Standard	Specifies the IP address of the host to which the user shou
Login-LAT-Group	RADIUS Standard	Specifies the Local Area Transport (LAT) group codes for
Login-LAT-Node	RADIUS Standard	Specifies the node to which user is connected by the Loc

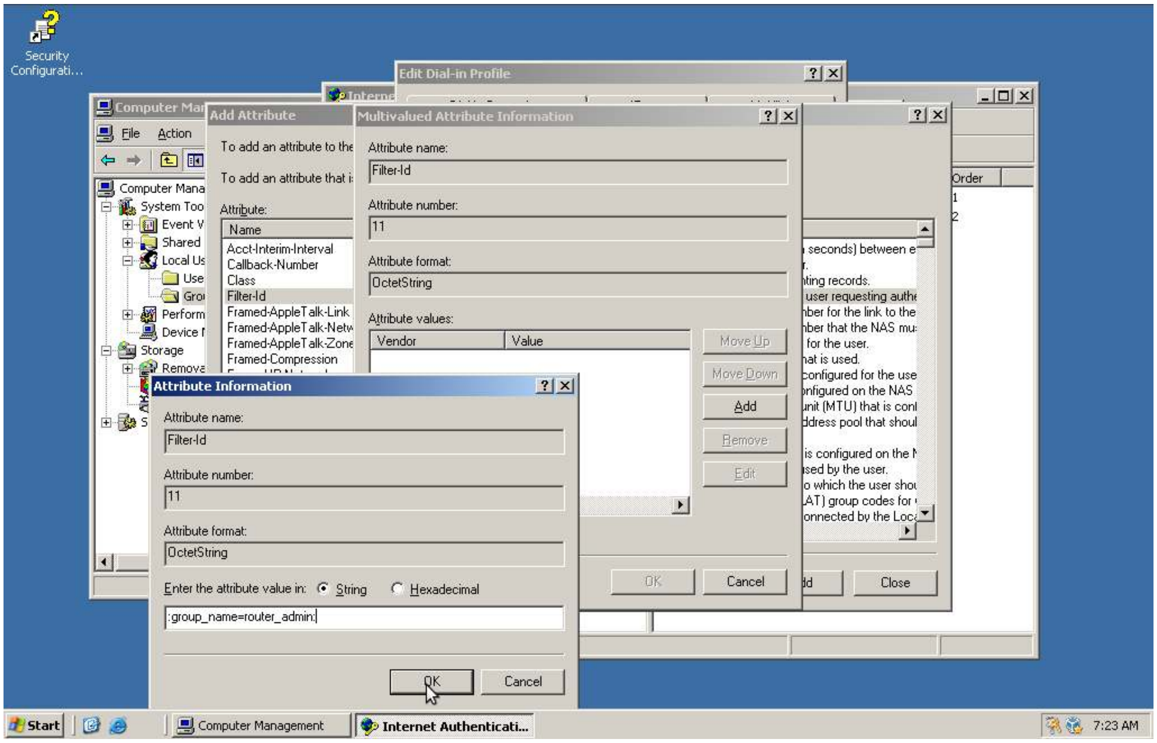
Click on Add again, and then fill in the group string. In this case, we’re going to create a group on the Opengear device called *router_admin*, so the group string is

:group_name=router_admin:

If you wish for these users to be part of more than one group on the Opengear, you can add more to this string. For example, if these users were to be part of the *firewall_admin* group as well, the group string would be

:group_name=router_admin,firewall_admin:

Fill in the group string, and click OK.



Attribute Information

Attribute name: Filter-Id

Attribute number: 11

Attribute format: OctetString

Enter the attribute value in: ● String ○ Hexadecimal

:group_name=router_admin:

Multivalued Attribute Information

Attribute name: Filter-Id

Attribute number: 11

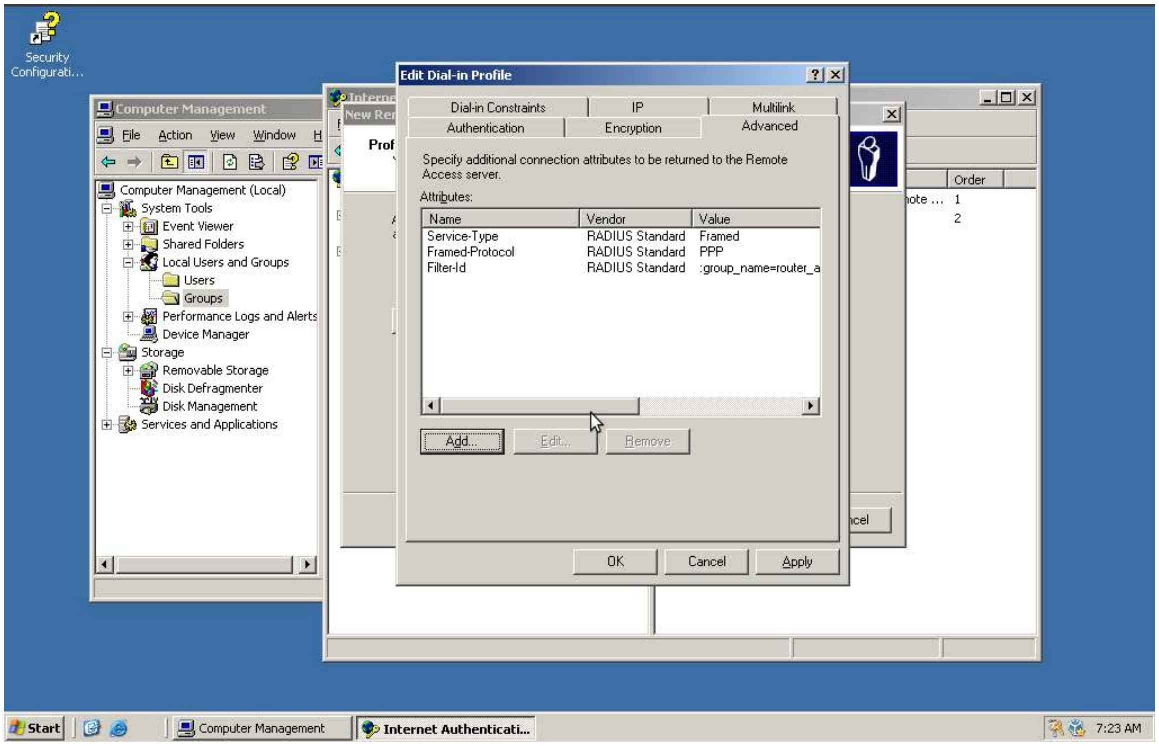
Attribute format: OctetString

Attribute values:

Vendor	Value

Once you've clicked OK, the Advanced tab should show the Filter-ID attribute as well as the others.

Click OK.



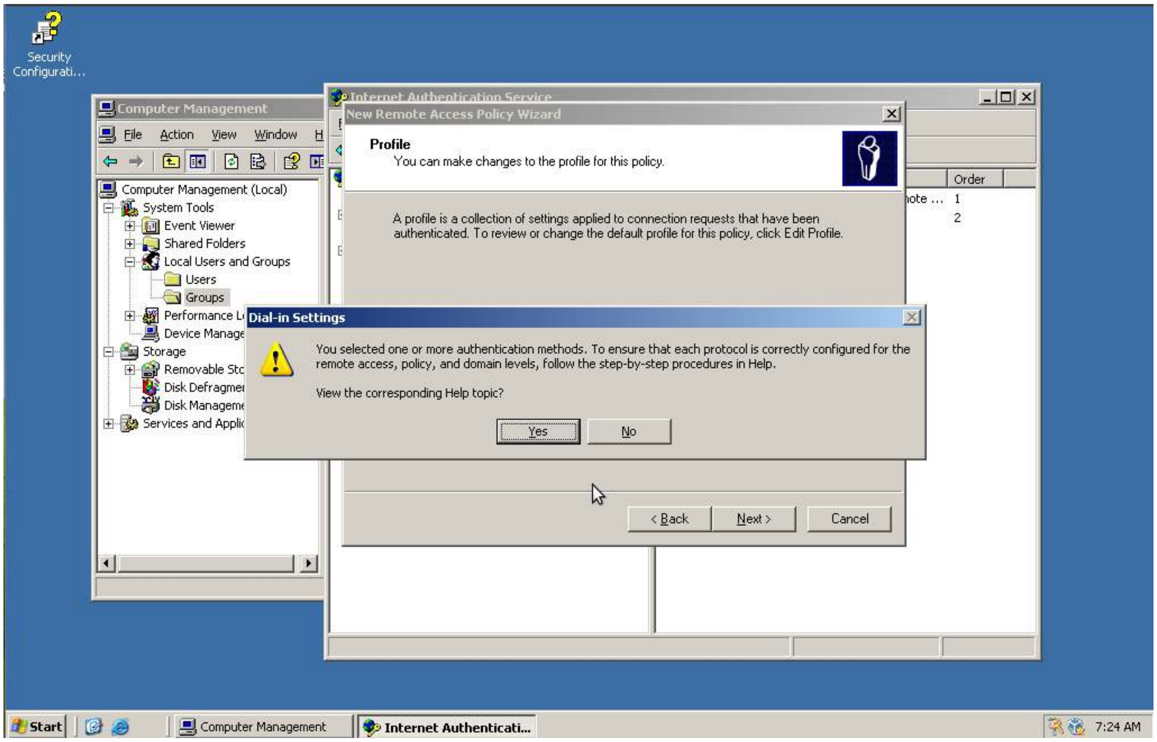
Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Framed-Protocol	RADIUS Standard	PPP
Filter-Id	RADIUS Standard	:group_name=router_a

Once you click ok, you may get this pop up message about Help Topics for authentication methods.

Click No, then click Next and Finish.



Profile

You can make changes to the profile for this policy.

A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.

You selected one or more authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

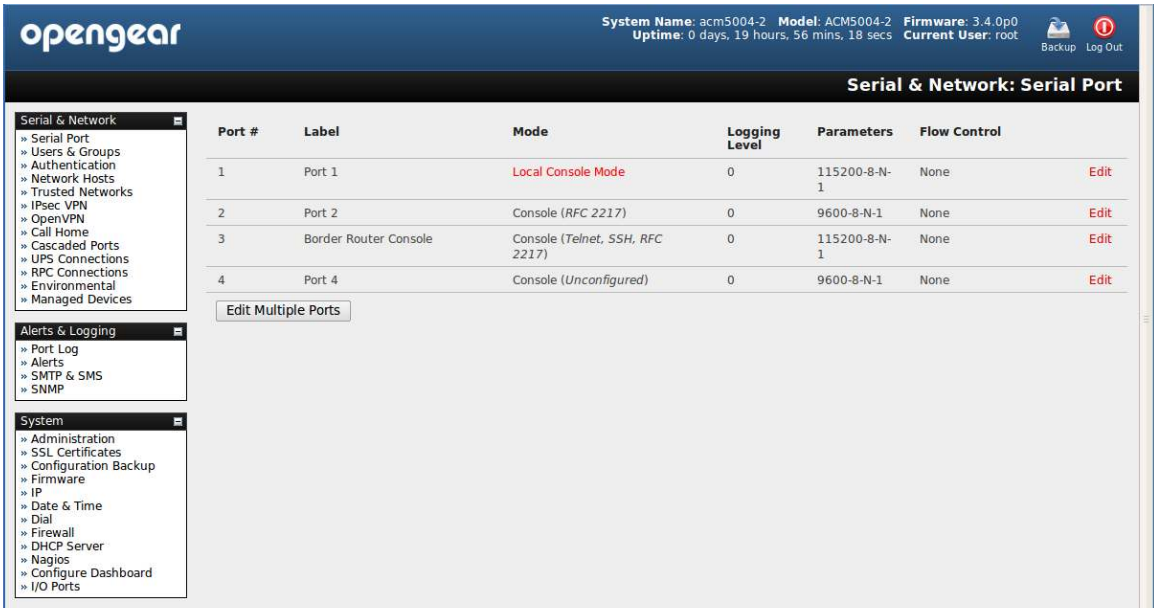
View the corresponding Help topic?

This concludes the set up required on the Windows 2003 server.

Configuring Opengear device

Connect the Web UI on the Opengear, and then navigate to the Serial Port entry.

In this example, we’ve configured port 3 to be connected to the console on the Border Router.



System Name: acm5004-2 **Model**: ACM5004-2 **Firmware**: 3.4.0p0
Uptime: 0 days, 19 hours, 56 mins, 18 secs **Current User**: root

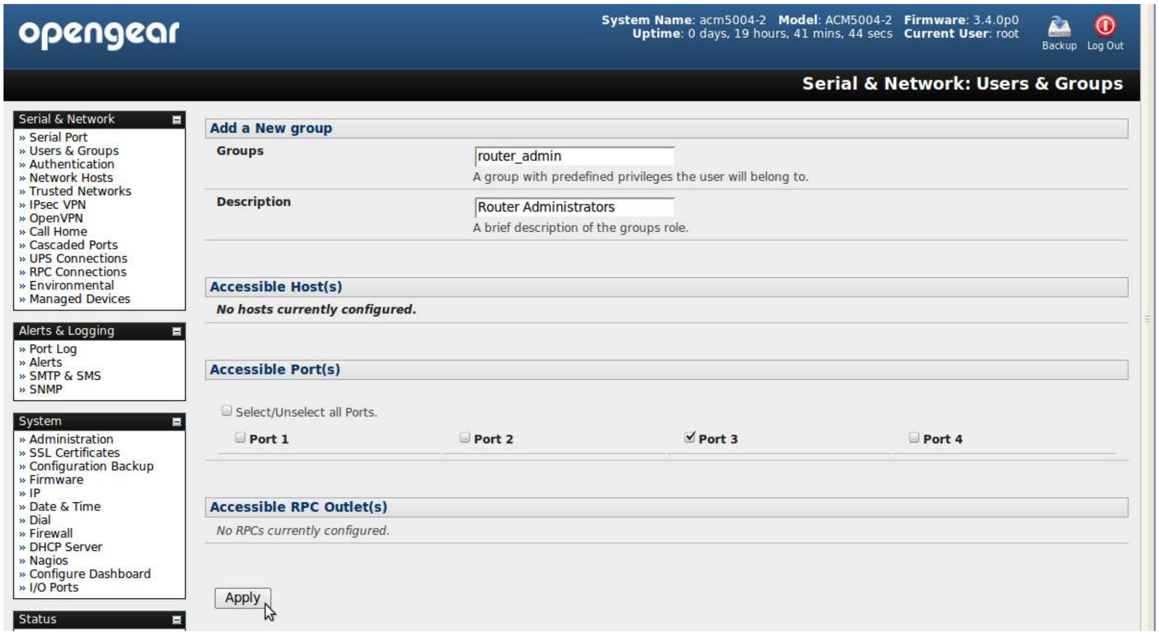
Serial & Network: Serial Port

Port #	Label	Mode	Logging Level	Parameters	Flow Control	
1	Port 1	Local Console Mode	0	115200-8-N-1	None	Edit
2	Port 2	Console (*RFC 2217*)	0	9600-8-N-1	None	Edit
3	Border Router Console	Console (*Telnet, SSH, RFC 2217*)	0	115200-8-N-1	None	Edit
4	Port 4	Console (*Unconfigured*)	0	9600-8-N-1	None	Edit

Navigate to the Users & Groups page, and click Add Group.

Fill in the group name as *router_admin* (as set in the attribute), and then select which ports this group has access to. In our case, that is port 3.

Click Apply



System Name: acm5004-2 **Model**: ACM5004-2 **Firmware**: 3.4.0p0
Uptime: 0 days, 19 hours, 41 mins, 44 secs **Current User**: root

Serial & Network: Users & Groups

Add a New group

Groups: router_admin
A group with predefined privileges the user will belong to.

Description: Router Administrators
A brief description of the groups role.

Accessible Host(s)

No hosts currently configured.

Accessible Port(s)

□ Select/Unselect all Ports.

□ **Port 1** □ **Port 2** ☑ **Port 3** □ **Port 4**

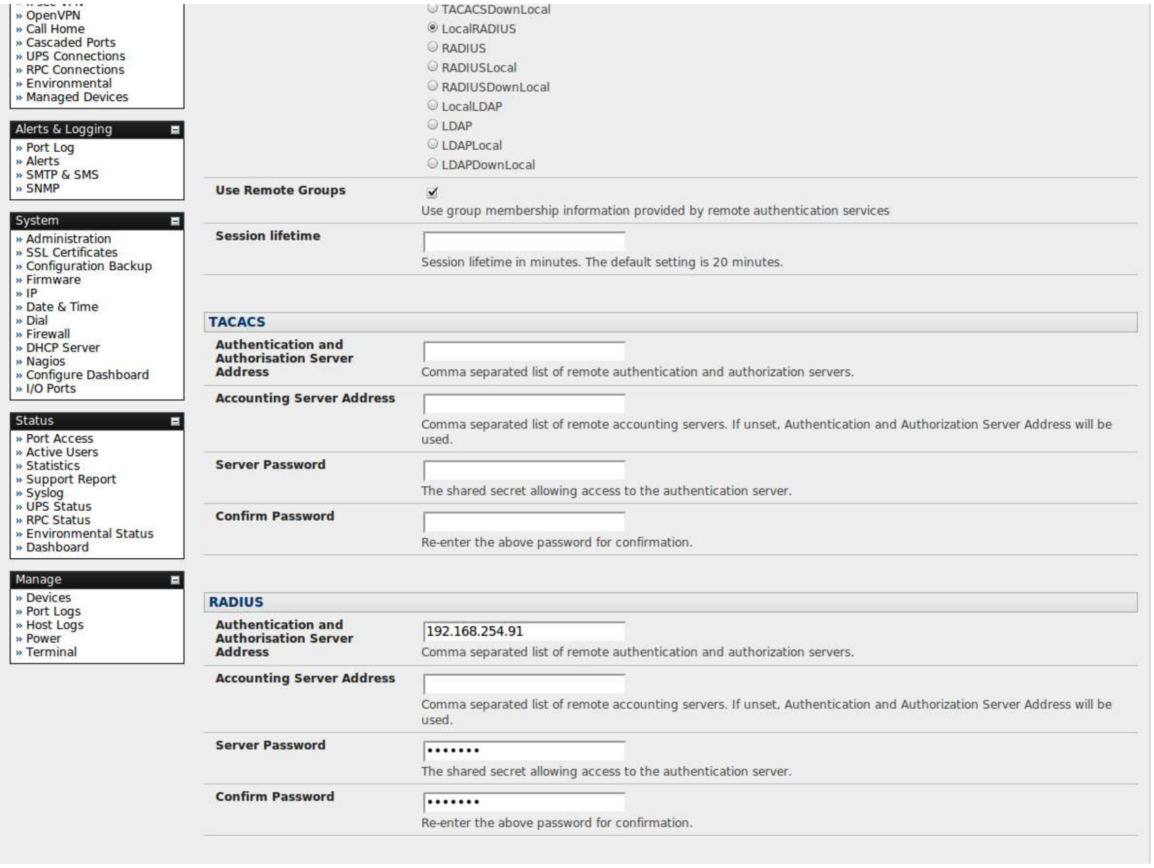
Accessible RPC Outlet(s)

No RPCs currently configured.

Navigate to the Authentication Page.

Select LocalRADIUS (this allows both local users and RADIUS users to connect, with local users being evaluated first), tick the Use Remote Groups tick box, and then fill in your RADIUS server details. The server password is the shared secret you entered when you set up the RADIUS Client during the IAS configuration.

Once this is done, click Apply at the bottom of the page.



- » OpenVPN
- » Call Home
- » Cascaded Ports
- » UPS Connections
- » RPC Connections
- » Environmental
- » Managed Devices

Alerts & Logging
- » Port Log
- » Alerts
- » SMTP & SMS
- » SNMP

System
- » Administration
- » SSL Certificates
- » Configuration Backup
- » Firmware
- » IP
- » Date & Time
- » Dial
- » Firewall
- » DHCP Server
- » Nagios
- » Configure Dashboard
- » I/O Ports

Status
- » Port Access
- » Active Users
- » Statistics
- » Support Report
- » Syslog
- » UPS Status
- » RPC Status
- » Environmental Status
- » Dashboard

Manage
- » Devices
- » Port Logs
- » Host Logs
- » Power
- » Terminal

○ TACACSDownLocal
● LocalRADIUS
○ RADIUS
○ RADIUSLocal
○ RADIUSDownLocal
○ LocalLDAP
○ LDAP
○ LDAPLocal
○ LDAPDownLocal

Use Remote Groups ☑
Use group membership information provided by remote authentication services

Session lifetime
Session lifetime in minutes. The default setting is 20 minutes.

TACACS

Authentication and Authorisation Server Address
Comma separated list of remote authentication and authorization servers.

Accounting Server Address
Comma separated list of remote accounting servers. If unset, Authentication and Authorization Server Address will be used.

Server Password
The shared secret allowing access to the authentication server.

Confirm Password
Re-enter the above password for confirmation.

RADIUS

Authentication and Authorisation Server Address 192.168.254.91
Comma separated list of remote authentication and authorization servers.

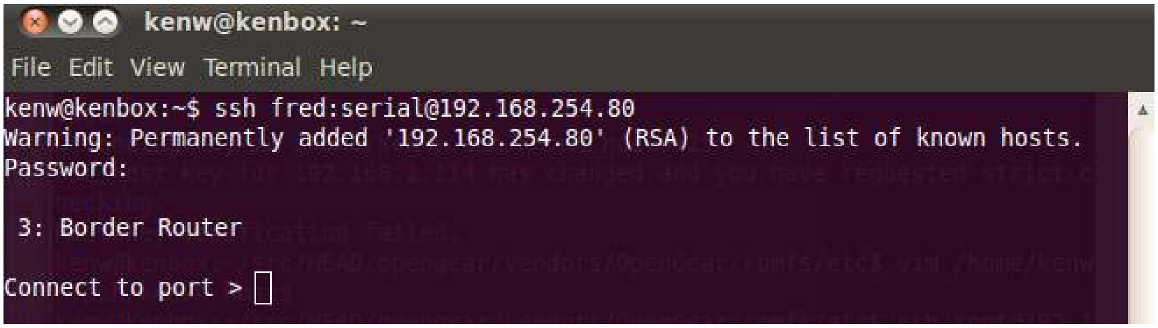
Accounting Server Address
Comma separated list of remote accounting servers. If unset, Authentication and Authorization Server Address will be used.

Server Password •••••••
The shared secret allowing access to the authentication server.

Confirm Password •••••••
Re-enter the above password for confirmation.

Now, you can test your RADIUS configuration.

Using SSH, try to connect in as a Windows User, who is a member of the RouterAdmin group.



```
kenw@kenbox:~$ ssh fred:serial@192.168.254.80
Warning: Permanently added '192.168.254.80' (RSA) to the list of known hosts.
Password:

 3: Border Router

Connect to port > 
```