Configuring RADIUS Authentication for WebVPN

So we decided that we have too many users to keep track of locally on the ASA. What are some other options? There are a variety of AAA methods we can use. My personal favorite is RADIUS attached to a Microsoft/Windows IAS (Internet Authentication Server). In Server 2008 I believe it's called NPS (Network Policy Server) which we will hopefully cover how to configure at some point. Right now we are going to configure RADIUS with a 2003 domain controller for authentication. Another option would be LDAP but I'm not a huge fan of it; It seems to work well until it breaks, then it's a huge pain to troubleshoot and get working again. So let's get right into the configuration.

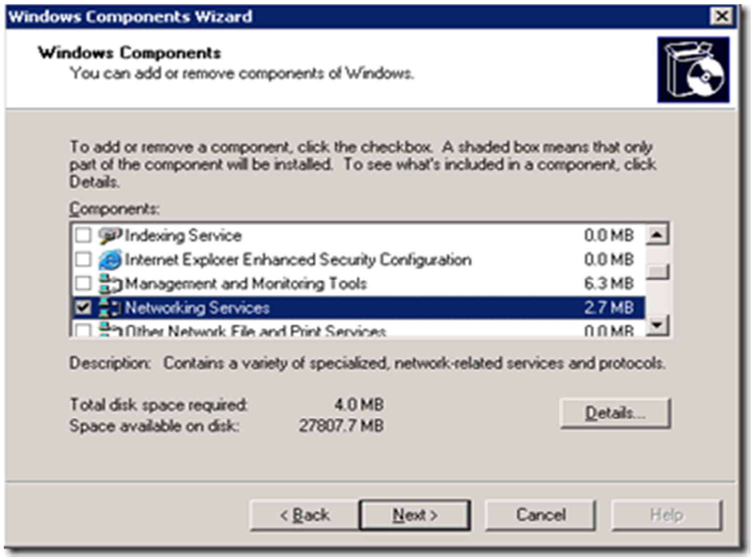
Notes
-Insert your relevant information between <>
-Console prompts are show in green
-Text in blue are variable names I made up, feel free to change them

Define an AAA server

```
ASA(config)# aaa-server WindowsIAS protocol radius
ASA(config-aaa-server-group)# aaa-server WindowsIAS host <IAS Server IP Address>
ASA(config-aaa-server-host)# key <IAS Key>
```

Configure RADIUS on the MS Server
The first thing we need is a server 2003 domain controller. Once we have that, we need to install IAS on top of it. IAS will do the RADIUS processing for us. In order to install IAS go to Control Panel, Add or Remove Programs, and select 'Add/Remove Windows Components' from the left-hand side bar. In the Windows Component Wizard scroll down to 'Networking Services' and double click on it.

Note: Prior to beginning this configuration I created two users in AD. One called marketing and one called sales. Additionally I have two groups configured SalesGroup and MarketingGroup. Each user is a member of their respective group. If you want to follow along with the example please add these users and groups now.



Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

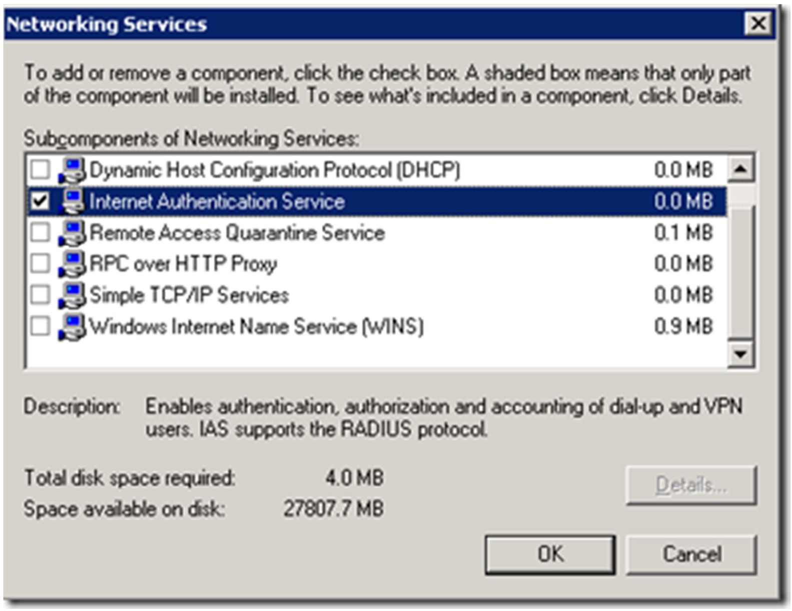
Components:

□ Indexing Service	0.0 MB
□ Internet Explorer Enhanced Security Configuration	0.0 MB
□ Management and Monitoring Tools	6.3 MB
☑ Networking Services	2.7 MB
□ Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 4.0 MB
Space available on disk: 27807.7 MB

Double clicking on ‘Networking Services’ should bring up a second window. On the second window find IAS and select the check box next to it. Then press OK to close the Networking Services window. Back on the Windows Components Wizard window press NEXT to begin the installation.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□ Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑ Internet Authentication Service	0.0 MB
□ Remote Access Quarantine Service	0.1 MB
□ RPC over HTTP Proxy	0.0 MB
□ Simple TCP/IP Services	0.0 MB
□ Windows Internet Name Service (WINS)	0.9 MB

Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

Total disk space required: 4.0 MB

Space available on disk: 27807.7 MB

Wait for the installation to complete.

•

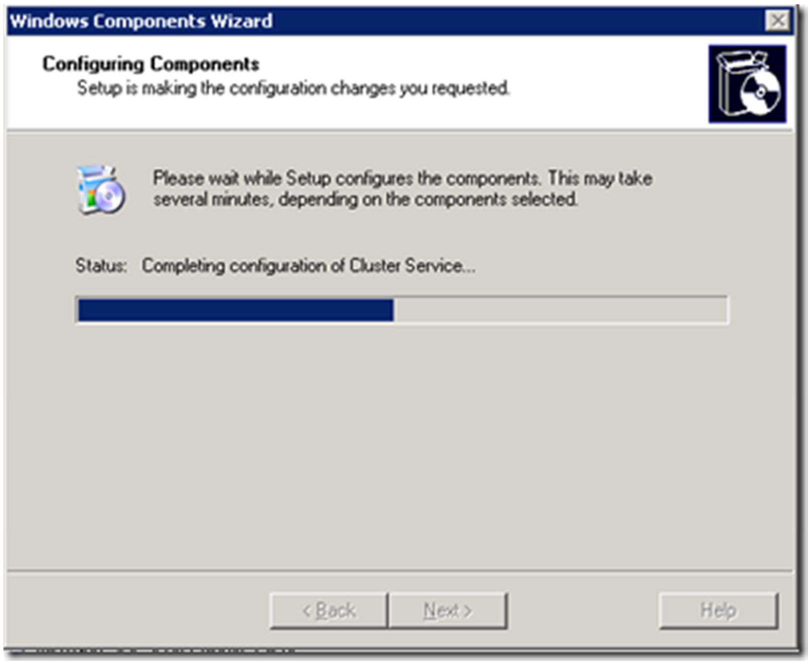
•

•

•

•

•



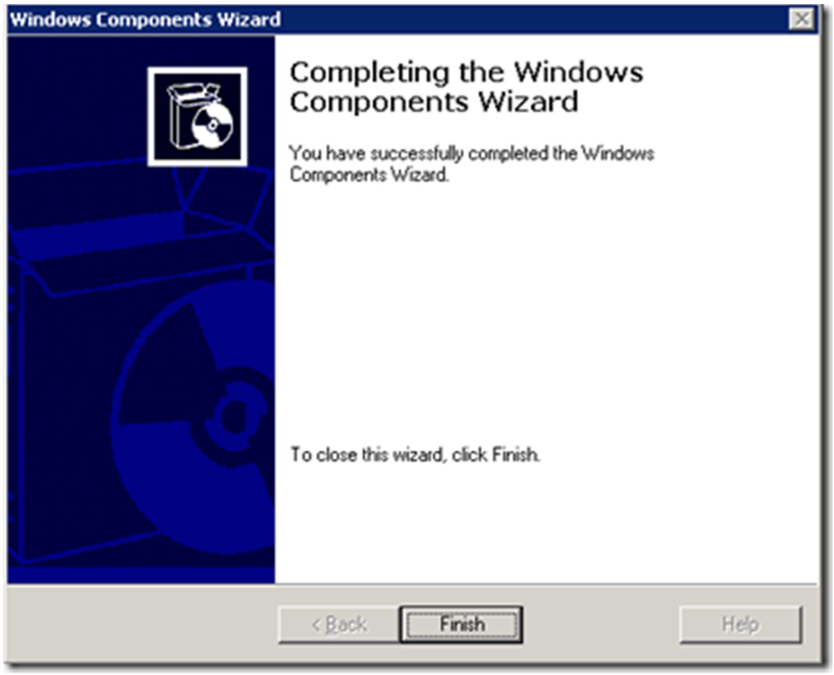
Configuring Components

Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Completing configuration of Cluster Service...

Once the installation is complete press FINISH and close Add/Remove programs.

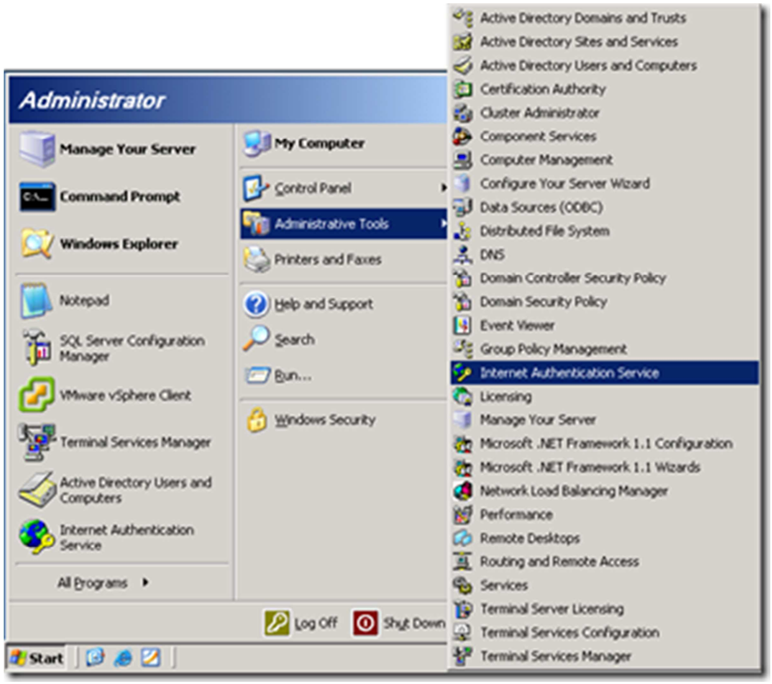


Completing the Windows Components Wizard

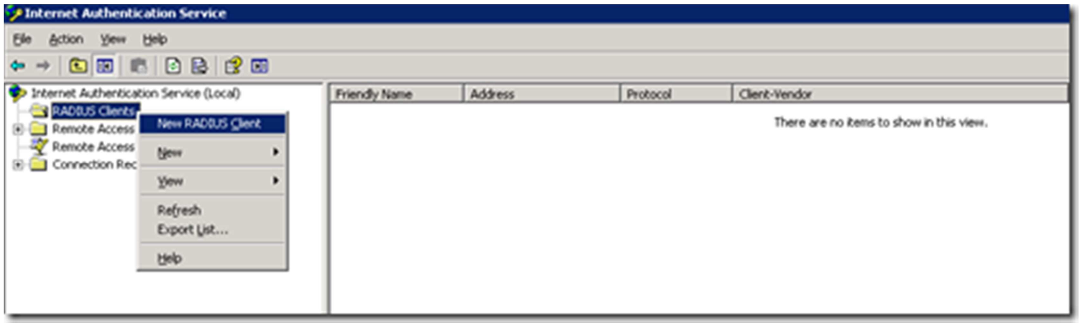
You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

Now that IAS is installed we can begin configuring it. To open IAS locate it under Administrative Tools.

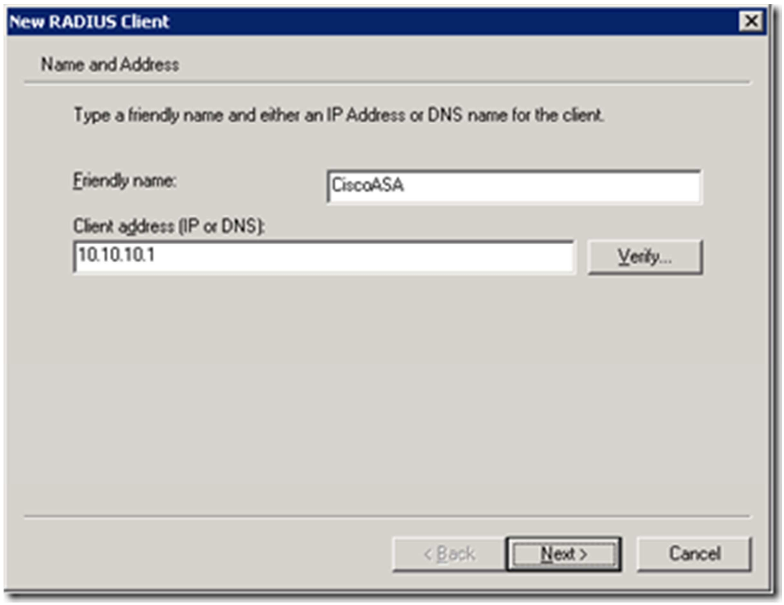

Administrator
Manage Your Server
Command Prompt
Windows Explorer
Notepad
SQL Server Configuration Manager
VMware vSphere Client
Terminal Services Manager
Active Directory Users and Computers
Internet Authentication Service
All Programs
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Windows Security
Log Off
Shut Down
Start
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Cluster Administrator
Component Services
Computer Management
Configure Your Server Wizard
Data Sources (ODBC)
Distributed File System
DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Group Policy Management
Internet Authentication Service
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktops
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager

The first thing to do is to configure a new RADIUS client. In our case this client will be the ASA. To configure the client right-click on RADIUS clients and select 'New RADIUS Client'



There are no items to show in this view.

On the New Radius Client window enter a name for the RADIUS client as well as the devices IP Address. Then press NEXT.



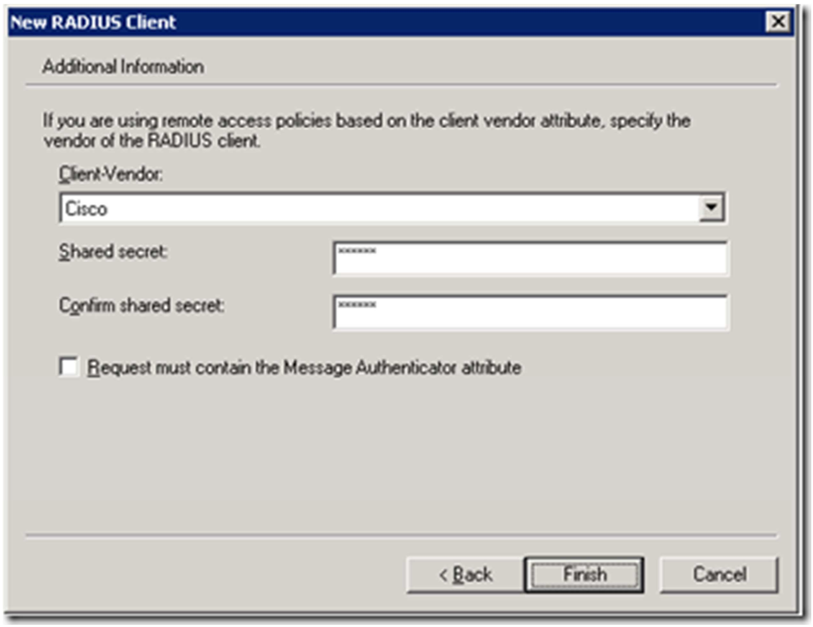
Name and Address

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

Friendly name: CiscoASA

Client address (IP or DNS): 10.10.10.1

On the next screen select ‘Cisco’ from the Client-Vendor drop down and then enter the secret you configured on the ASA when you defined the AAA server. Then press FINISH.



Additional Information

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

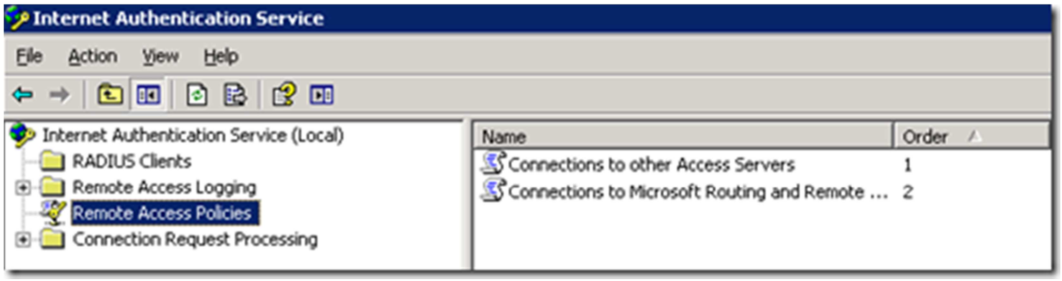
Client-Vendor: Cisco

Shared secret: ******

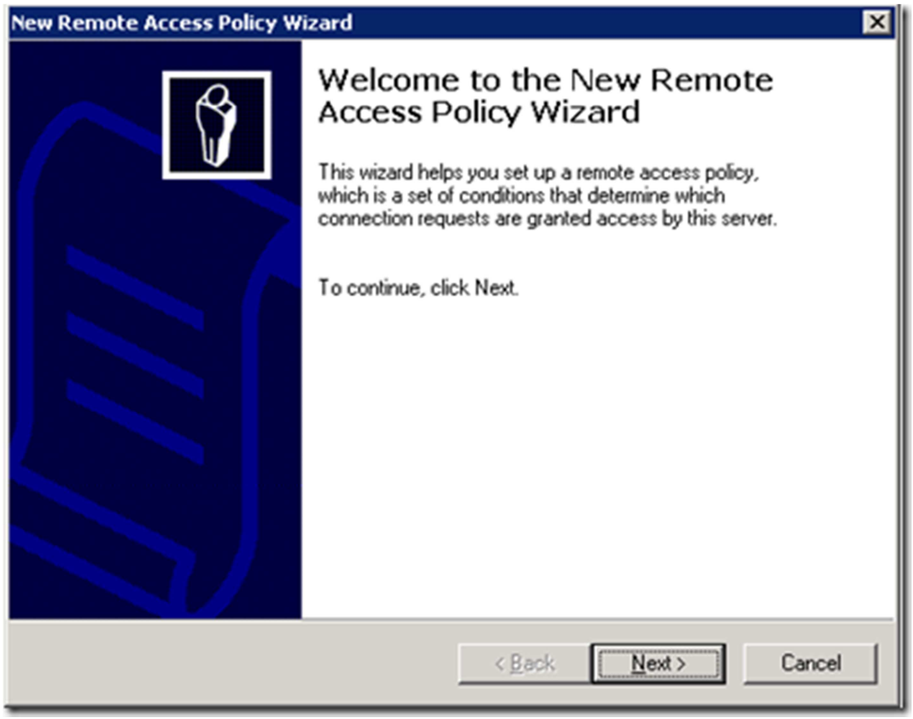
Confirm shared secret: ******

☐ Request must contain the Message Authenticator attribute

Technically the next step here would be to configure logging. I usually don’t configure logging beyond what’s configured in the default settings. All of the requests (approved and denied) are logged in the servers system event log. That’s usually good enough for me. So let’s jump right into configuring the remote access policy for our connection. Select ‘Remote Access Policies’ from the left-hand side bar. On the right you should see the two default policies. Let’s start from scratch; right-click on each and select DELETE. Then right-click on the Remote Access Policies and select ‘New Remote Access Policy’


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

Name	Order
Connections to other Access Servers	1
Connections to Microsoft Routing and Remote ...	2

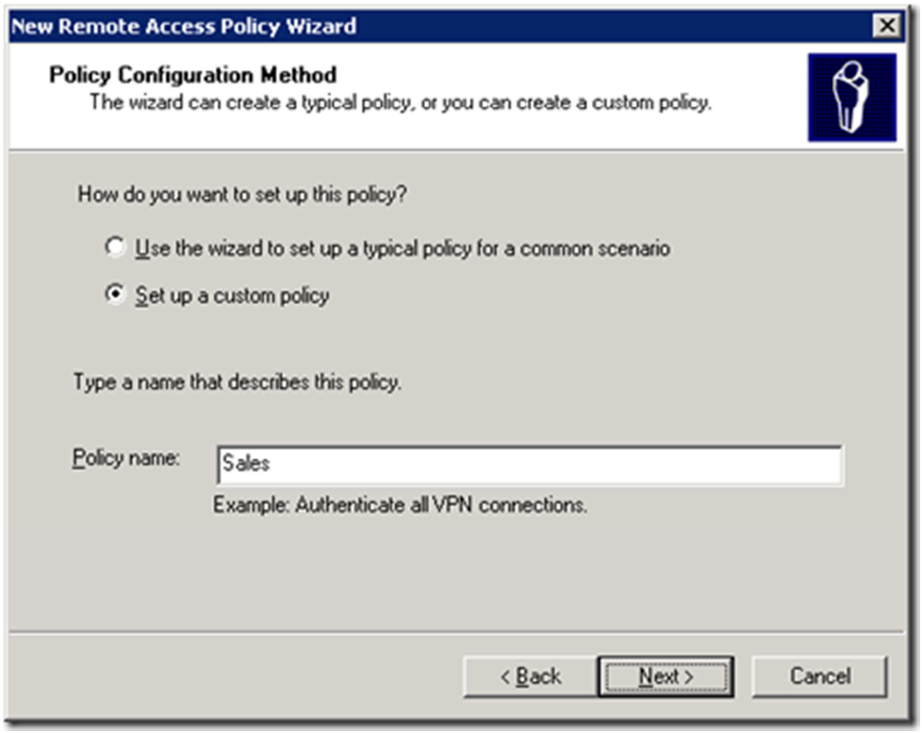


Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

On the next screen select the option for ‘Setup a custom policy’ and give it a name. Keeping with our example, I’ll call this policy ‘Sales’. Then press 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

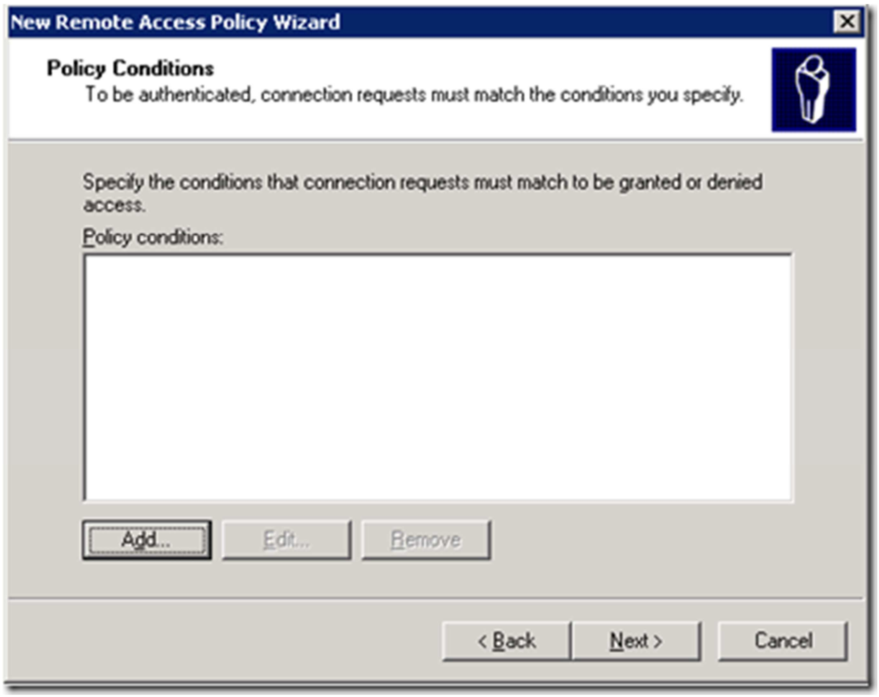
● Set up a custom policy

Type a name that describes this policy.

Policy name: Sales

Example: Authenticate all VPN connections.

On the next window press ADD to add a new policy condition



New Remote Access Policy Wizard

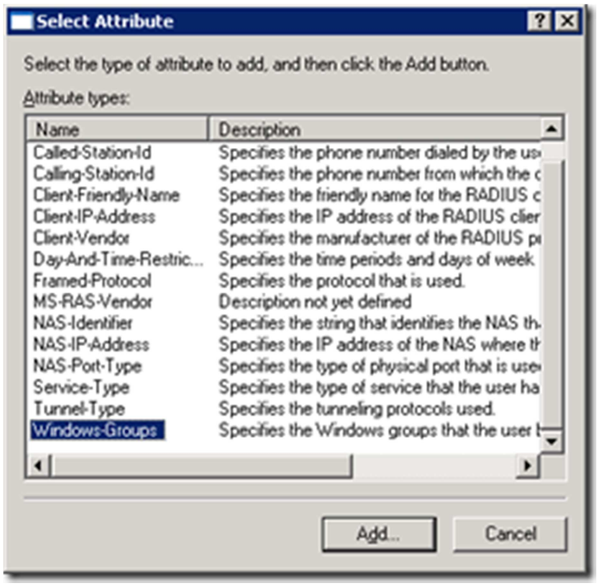
Policy Conditions

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:

In the Select Attribute window scroll down to ‘Windows Group’ and press ADD.

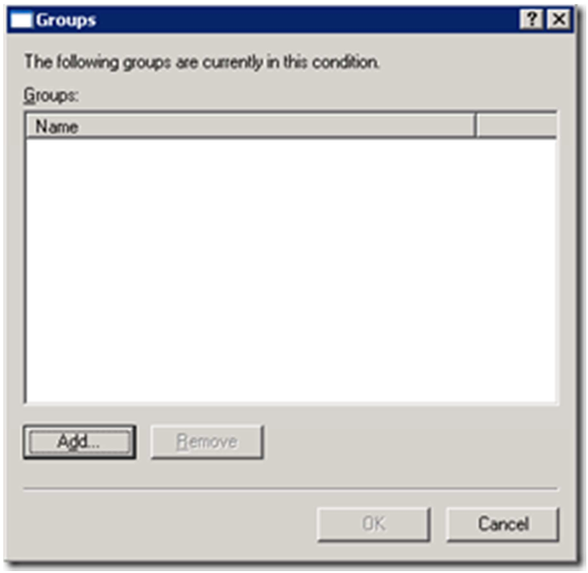


Select the type of attribute to add, and then click the Add button.

Attribute types:

Name	Description
Called-Station-Id	Specifies the phone number dialed by the us
Calling-Station-Id	Specifies the phone number from which the c
Client-Friendly-Name	Specifies the friendly name for the RADIUS c
Client-IP-Address	Specifies the IP address of the RADIUS clier
Client-Vendor	Specifies the manufacturer of the RADIUS pı
Day-And-Time-Restric...	Specifies the time periods and days of week
Framed-Protocol	Specifies the protocol that is used.
MS-RAS-Vendor	Description not yet defined
NAS-Identifier	Specifies the string that identifies the NAS th
NAS-IP-Address	Specifies the IP address of the NAS where tl
NAS-Port-Type	Specifies the type of physical port that is use
Service-Type	Specifies the type of service that the user ha
Tunnel-Type	Specifies the tunneling protocols used.
Windows-Groups	Specifies the Windows groups that the user t

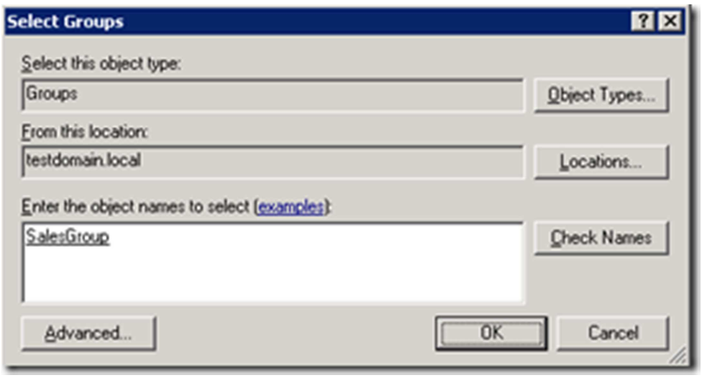
After you press ADD, a new window will pop up called ‘Groups’. Click the ADD button once again and select a windows security group from Active Directory.



The following groups are currently in this condition.

Groups:

Name	



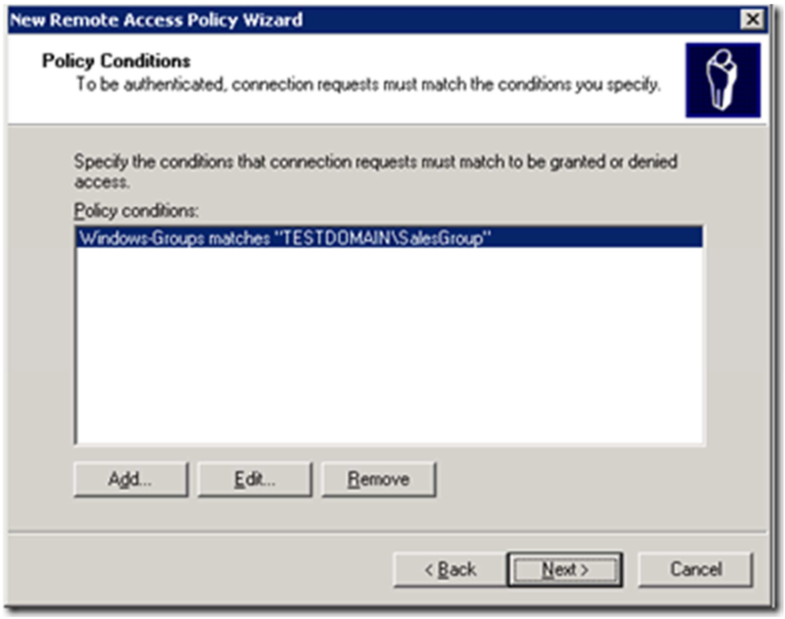
Select Groups

Select this object type: Groups

From this location: testdomain.local

Enter the object names to select (examples): SalesGroup

Press OK on the Select Groups window and OK on the Groups window to return to the New Remote Access Policy Wizard. You should now see your group listed in the Policy Conditions window as shown below. Press NEXT.



New Remote Access Policy Wizard

Policy Conditions

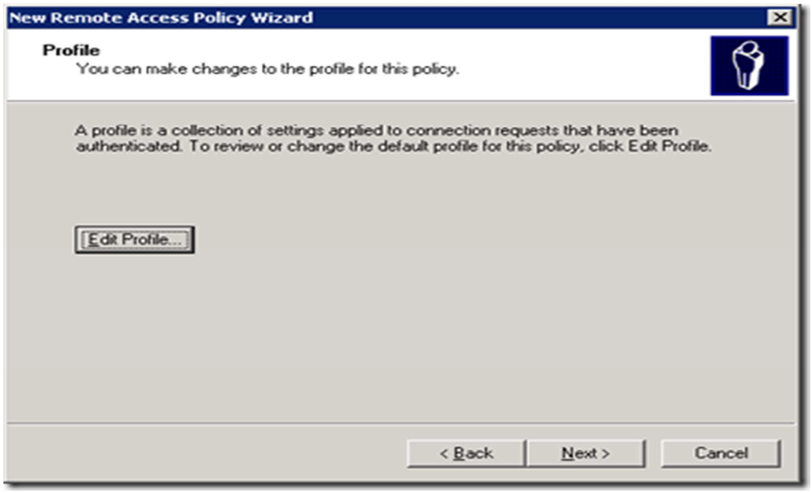
To be authenticated, connection requests must match the conditions you specify.

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

Policy conditions:

Windows-Groups matches "TESTDOMAIN\SalesGroup"

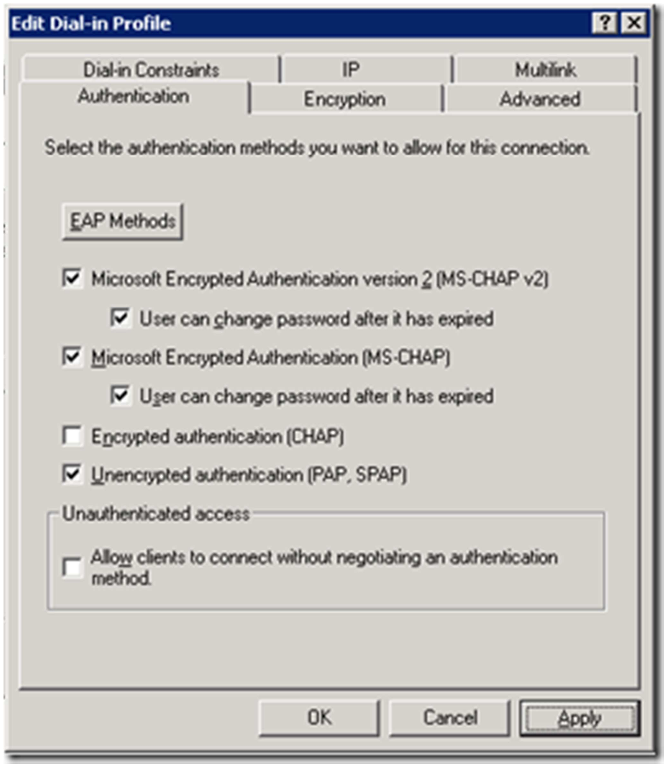
On the next screen press the EDIT PROFILE



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.

On the Edit Dial-in Profile window select the Authentication tab and ensure that 'Unencrypted authentication (PAP, SPAP)' is checked.



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

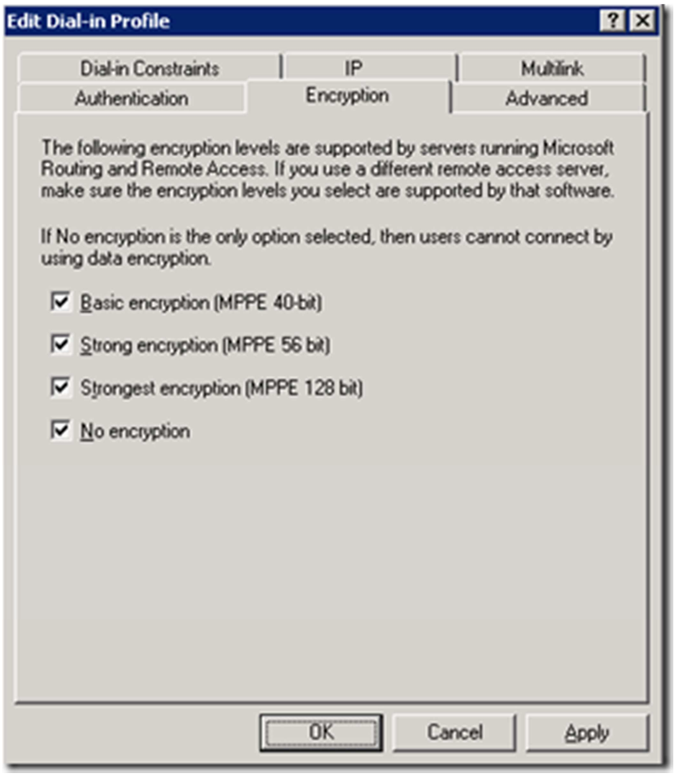
☐ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☐ Allow clients to connect without negotiating an authentication method.

Now select the Encryption tab and check the ‘No Encryption’ check mark. Then Press OK



The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you select are supported by that software.

If No encryption is the only option selected, then users cannot connect by using data encryption.

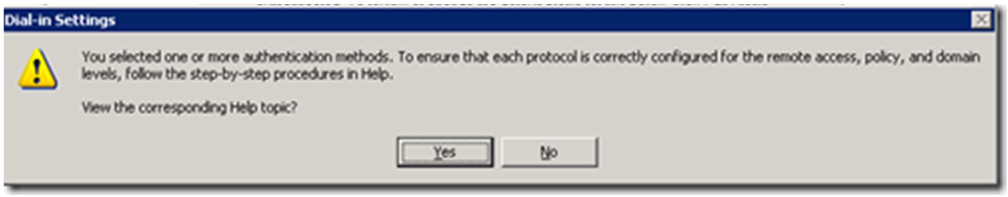
☑ Basic encryption (MPPE 40-bit)

☑ Strong encryption (MPPE 56 bit)

☑ Strongest encryption (MPPE 128 bit)

☑ No encryption

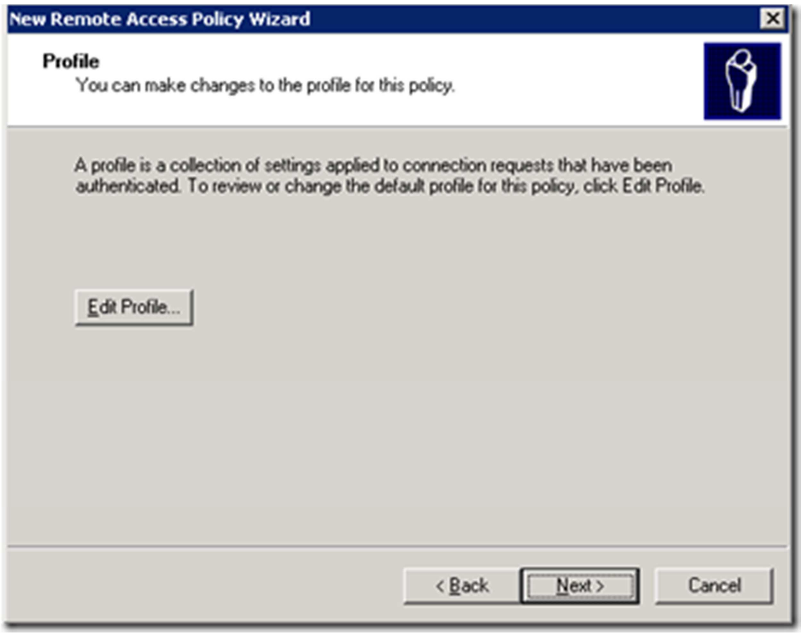
When you press OK, you will receive the following error message. Just press NO to return to the wizard.



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?

Press Next on the wizard window



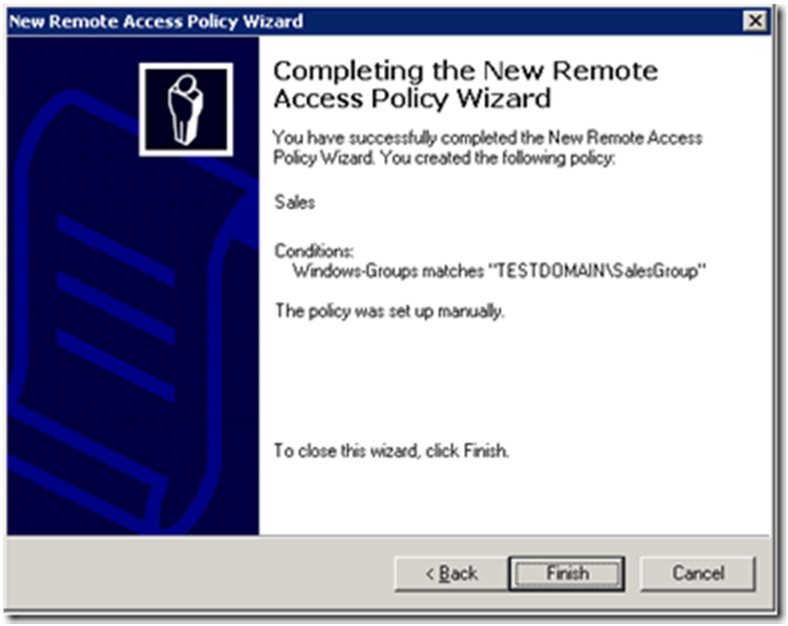
New Remote Access Policy Wizard

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.

Then press FINISH to create the policy



New Remote Access Policy Wizard

Completing the New Remote Access Policy Wizard

You have successfully completed the New Remote Access Policy Wizard. You created the following policy:

Sales

Conditions:
Windows-Groups matches "TESTDOMAIN\SalesGroup"

The policy was set up manually.

To close this wizard, click Finish.

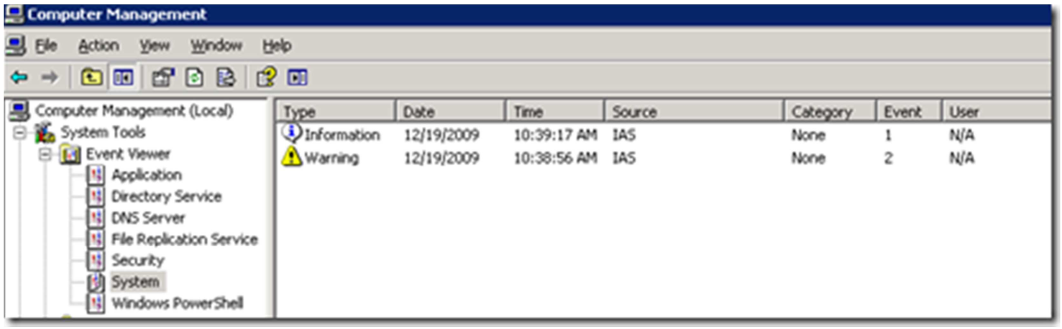
Now that we have successfully configured RADIUS let's test it on the ASA to ensure that it's working correctly.

Testing the RADIUS Configuration

```
ASA# test aaa-server authentication WindowsIAS username <username> password <password>
Server IP Address or name: <IP address of RADIUS Server that you defined>
INFO: Attempting Authentication test to IP address <IP you entered> (timeout: 12 seconds)
INFO: Authentication Successful
```

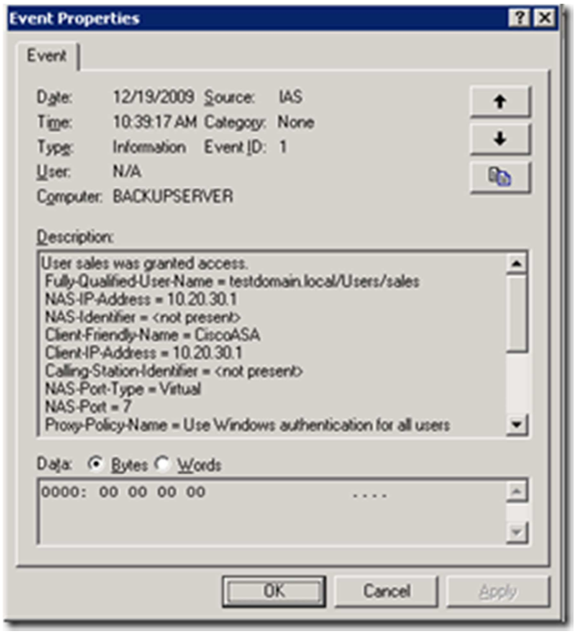
Checking the severs system log for IAS events

When you perform any sort of authentication (including the test we did above) against IAS it logs an event in the server's System log. Let's take a brief look at a couple of events that can appear in the log and I'll show you how easy it is to troubleshoot IAS/RADIUS issue. The below screen shot is of my system log.



Type	Date	Time	Source	Category	Event	User
Information	12/19/2009	10:39:17 AM	IAS	None	1	N/A
Warning	12/19/2009	10:38:56 AM	IAS	None	2	N/A

As you can see there are two events from IAS. Successful RADIUS authentication requests are logged as type informational and event ID 1. Failures are logged as type warning and event ID 2. Let's look at both of the actual events and see why the first one failed.



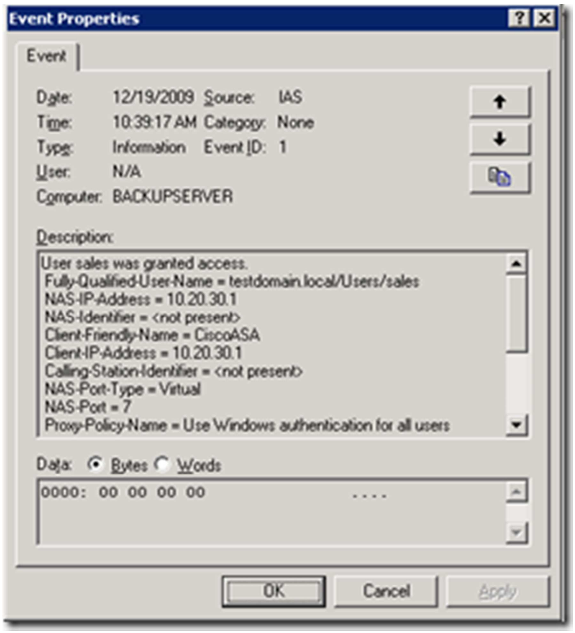
Date: 12/19/2009 Source: IAS
Time: 10:39:17 AM Category: None
Type: Information Event ID: 1
User: N/A
Computer: BACKUPSERVER

Description:

User sales was granted access.
Fully-Qualified-User-Name = testdomain.local/Users/sales
NAS-IP-Address = 10.20.30.1
NAS-Identifier = <not present>
Client-Friendly-Name = CiscoASA
Client-IP-Address = 10.20.30.1
Calling-Station-Identifier = <not present>
NAS-Port-Type = Virtual
NAS-Port = 7
Proxy-Policy-Name = Use Windows authentication for all users

Data: ● Bytes ○ Words

```
0000: 00 00 00 00          ....
```



Date: 12/19/2009 Source: IAS
Time: 10:39:17 AM Category: None
Type: Information Event ID: 1
User: N/A
Computer: BACKUPSERVER

Description:

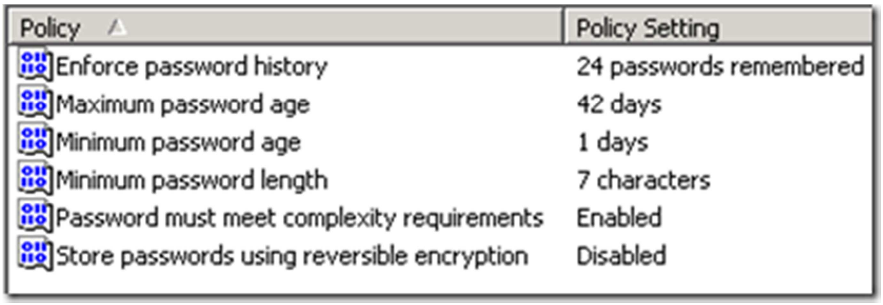
```
User sales was granted access.
 Fully-Qualified-User-Name = testdomain.local/Users/sales
 NAS-IP-Address = 10.20.30.1
 NAS-Identifier = <not present>
 Client-Friendly-Name = CiscoASA
 Client-IP-Address = 10.20.30.1
 Calling-Station-Identifier = <not present>
 NAS-Port-Type = Virtual
 NAS-Port = 7
 Proxy-Policy-Name = Use Windows authentication for all users
```

Data: ● Bytes ○ Words

```
0000:  00 00 00 00                    ....
```

The failure is shown on the left. To determine the cause of the failure, I scrolled down to the 'Reason' part of the event. I simulated this error by checking the 'User must change password at next logon' attribute underneath the users AD account settings. Once I unchecked the settings and ran the test on the ASA again, I got the event on the right. The first line indicates my user was grant access. Bottom line, if you are having IAS issues, check the system log. If there aren't any IAS events it's most likely a misconfig on the ASA or the IAS server. If there are events, it's usually pretty easy to determine the issue.

As I mentioned in my last post, an advantage of using RADIUS configured with a MS domain is that you get it's password policies along with it. For instance a default domain group policy on a 2003 MS Server requires that the password uses 'password' complexity'. In other words it has to meet certain standards such as containing a certain number of letters, numbers, and symbols. Additionally, you get the password expiration policy which forces the user to change their password every so often. The screen shot below shows the password policies that are available in the default domain policy on a MS Server. I'm not going to dig into configuring group policies on a MS server on this blog, but I will give you piece of advice: download the 'group policy management tool' if you are working in server 2003.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

However a problem does exist with this configuration. If you have RADIUS setup on the portal and you have some users defined in AD just for portal authentication, they might never logon to a windows PC (on the domain) to see warnings about their password expiring. At the very least, they wouldn't have the facilities to change the password. No fear, Cisco built this functionality into the ASA. One simple command enables password management that processes all of the warnings and errors to the user at the logon prompt. Password management is a function of a tunnel group.

Enable Password Management on the Logon page

```
ASA(config)# tunnel-group <Tunnel Group Name> general-attributes
ASA(config-tunnel-general)# password-management
OR
ASA(config-tunnel-general)# password-management password-expire-in-days <Days prior to expiration you want to warn the user>
```

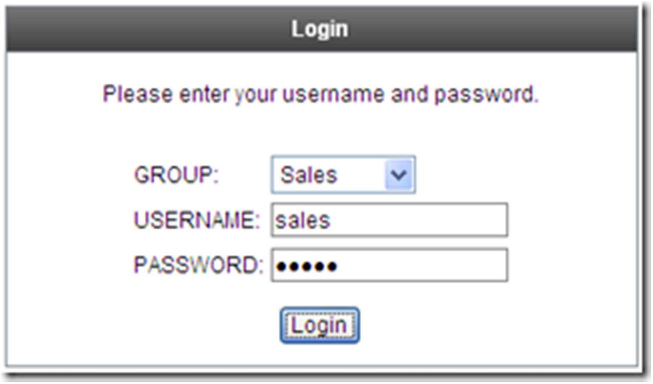
If you just enable password management by simply entering 'password-management', the 'password-expire-in-days' value is defaulted to a value of 14. If you want to warn the user on the day of expiration enter a value of 0 in the 'password-expire-in-days' value.

Now that we have all of this configured, let's configure our tunnel group to use RADIUS.

Modify your tunnel group to add the AAA server

```
ASA(config)# tunnel-group <Tunnel Group name> general-attributes
ASA(config-tunnel-general)# authentication-server-group WindowsIAS
```

Now let's browse externally to the ASA logon page and test it all out. I applied the AAA server to my sales tunnel group. Remember, AAA is defined per tunnel group. If you want all of your users to use RADIUS and have multiple tunnel groups you need to define RADIUS in each.



Login

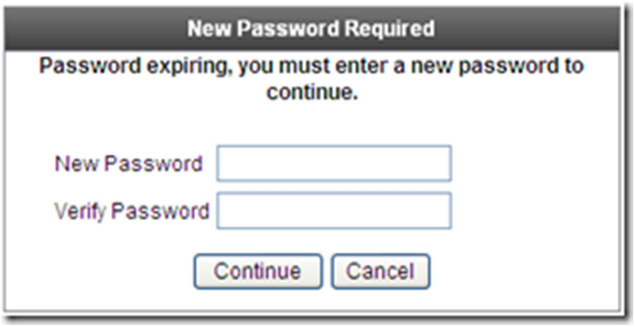
Please enter your username and password.

GROUP: Sales

USERNAME: sales

PASSWORD: •••••

After entering the credentials and clicking ‘Login’ I was able to successfully gain access to the portal page. A quick check of the IAS server’s system log confirmed that my RADIUS request was granted access. As a last note, try out the password management feature if you enabled it. Go into AD and check the ‘User must change password at next logon’ under the sales user’s account settings. Now let’s try logging in again.



New Password Required

Password expiring, you must enter a new password to continue.

The ASA caught onto the fact that the users password was expiring in AD and is giving us the opportunity to change it now. Additionally since it’s an AD password it needs to meet all of the AD password policies. Pretty slick huh? After I entered my new password, I confirmed that it changed on the AD side by logging in to a local computer on the domain with my new credentials. In the next post we’ll be talking about pulling attributes from AD and processing them during logon.