

VACMAN RADIUS Middleware and Microsoft IAS (Internet Authentication Service)

White Paper



THE AUTHENTICATION COMPANY

VACMAN RADIUS Middleware and Microsoft IAS (Internet Authentication Service)

White Paper

Overview.....	3
Problem Description	3
Technical Concept/General Overview	3
Technical Concept/Special Features.....	5
Bulk assign mode.....	5
Automatic token assign.....	5
Dynamic User Registration	5
Grace Period.....	5
Technical Concept/Overview of IAS RADIUS Authentication with VRM	5
Overview of RADIUS IP and Port Settings.....	6
IAS Installation	7
IAS Configuration.....	9
VACMAN RADIUS Middleware Configuration.....	13



Overview

VASCO's Microsoft IAS (Internet Authentication Service) package is the result of the open market approach delivered through VACMAN Radius Middleware technology.

The solution provides the Microsoft's IAS server the ability to utilize the strength of the Digipass Token Family concept (One Time Password login as Time Based Response Only or Challenge/Response) into their solid existing technology.

VASCO has a long successful history of delivering strong authentication through our DIGIPASS Family of tokens that delivers the comfort of using One Time Passwords (OTP).

Problem Description

Since static passwords are generally known as non-secure and easy to compromise, the challenge was to introduce OTP's into the remote access market to strongly secure the corporate LAN. Additionally, it would be convenient to easily track and manage incoming users of the NAS/RAS devices.

The following pages present the DIGIPASS Authentication Mode as it is integrated in the RADIUS Server. There is also an overview on how to setup an easy configuration of the Steel Belted Radius Server.

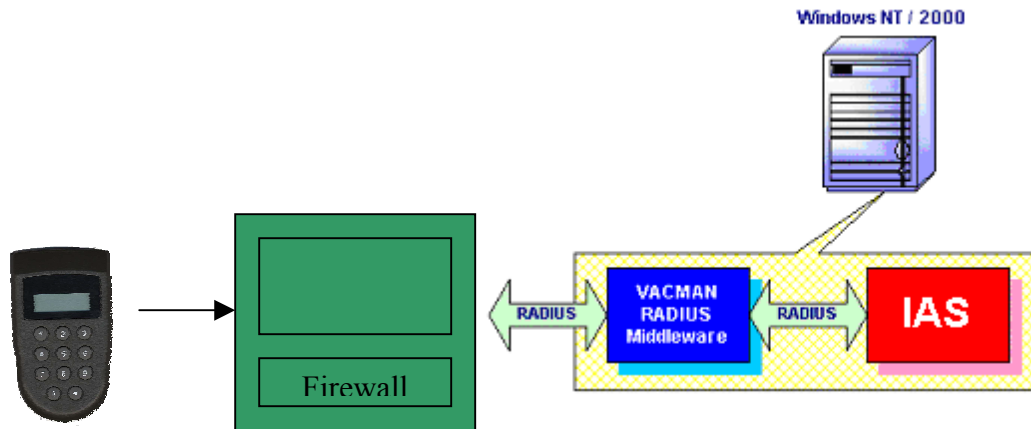
Technical Concept/General Overview

The concept is very easy: the VACMAN Radius Middleware is installed as back-end of the Steel Belted Radius server. (Fig. 1). This means that the VACMAN Plug-in will do each authentication on the SBR. The VACMAN Plug-in gives a yes/no back on the authentication request to the SBR who can do the next steps.

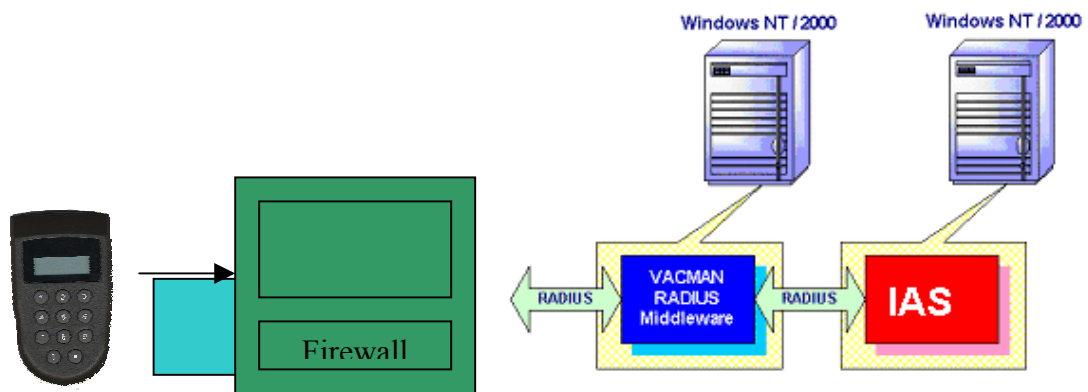
The Digipass Management Console gives the right interpretation (DUR, Autolearn) on each signal in combination with flexible Digipass™ management (Grace Period, Passthru,...).

Fig 1: Technical concept

VRM and IAS running on one machine



VRM and IAS running on two machines



Technical Concept/Special Features

Bulk assign mode

It is a batch process that allows you to simply manage the assignment operation. The Bulk Assign Function is available when using the "All free Users" or "All free Digipass" filter. It allows administrator to multi-select users and (if free DIGIPASS tokens are present in VASCO Database) to assign each DIGIPASS to the new auto-created user.

Automatic token assign

This mode will allow the user to auto-create his user account record in the VASCO Database and to self-auto assign his DIGIPASS. This can be done in Response Only and Challenge Response Mode. You need to send the Digipass serial number, the static password and the dynamic password to the server. From then on, you can start using Digipass tokens to authenticate.

Dynamic User Registration

You may select this option if you want any (successful) static authentication scheme to add automatically the user/password data into the VASCO Database.

In this case, the administrator will be able to easily assign DIGIPASS without having to manually create the user. This assignment is possible on a per user basis or in bulk mode.

Grace Period

When an administrator assigns a Digipass to a user, it does not imply that the user already possesses the Digipass.

The feature Grace Period allows to use the static password for a certain Grace Period of time even when a Digipass has already been assigned.

The Grace Period will end after the period has expired or at the first time within this period that the user uses the Digipass.

Technical Concept/Overview of IAS RADIUS Authentication with VRM

The following is a high-level description on the RADIUS authentication sequence:

1. A remote user initiates a (dial-up) connection to the NAS (Network Access Server).
2. NAS gathers the remote user's ID and password, and then submits a RADIUS authentication request to the VRM.
3. VRM performs its verification, and then proxies the request to IAS RADIUS server.
4. IAS server performs its verification and then returns the results.
5. VRM forwards the IAS server results to NAS.
6. The NAS takes an appropriate action based on returned RADIUS results from IAS Server via VRM.

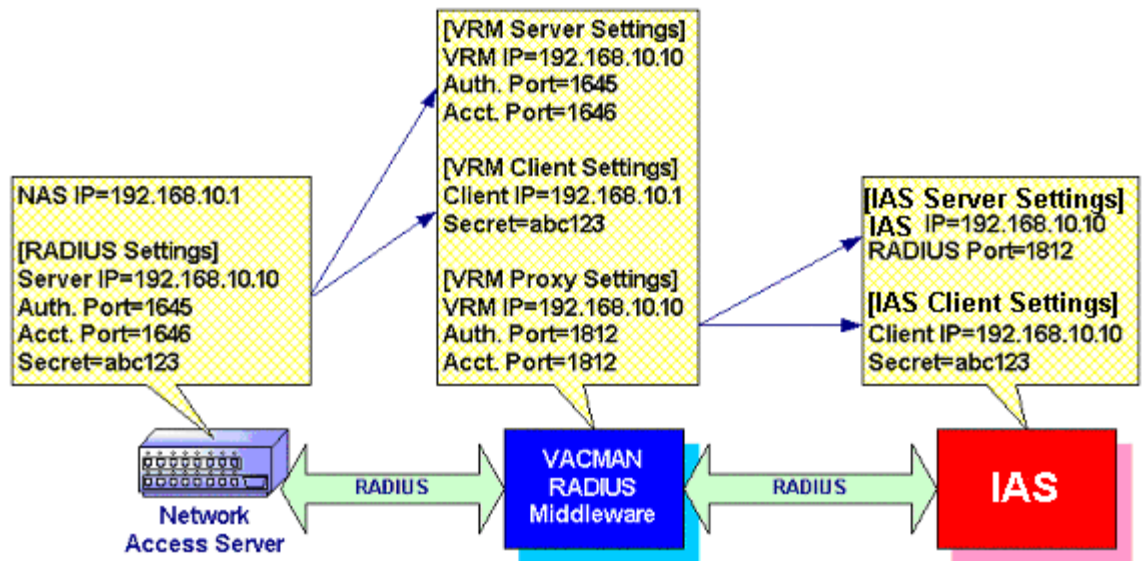
Overview of RADIUS IP and Port Settings

In most installations, only a few IAS RADIUS servers manage many NAS and firewall RADIUS clients. Therefore, the recommended setup is to change the limited number of VRM and IAS settings rather than the many RADIUS client settings. The alternate setup is to change those RADIUS clients to point to the VRM.

In either case, the RADIUS settings must result in the following relationships as detailed below. Also, refer to the **VRM Configuration** and **IAS Configuration** sections in this document on how to configure these settings.

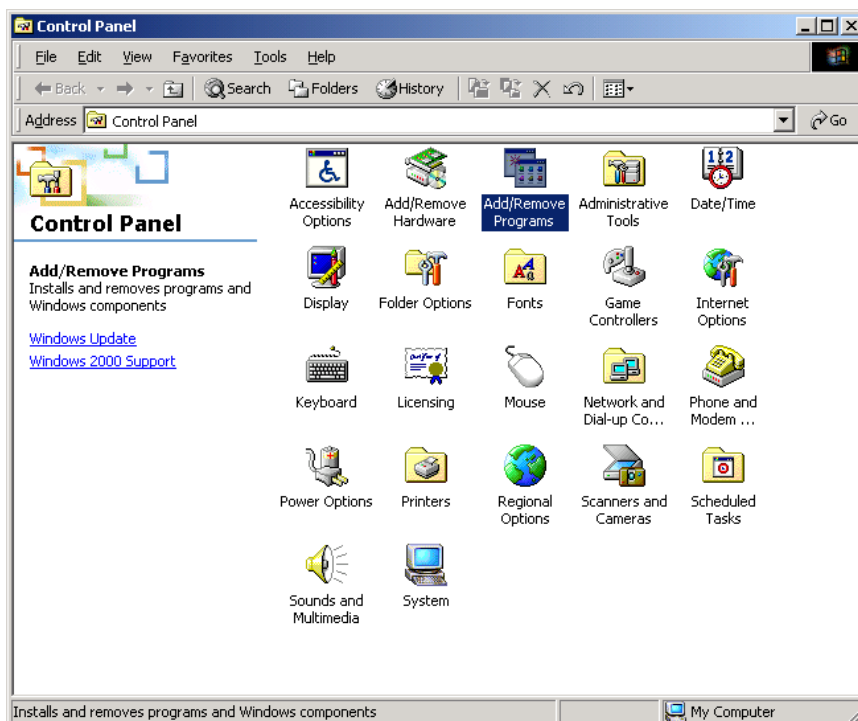
REQUIRED RADIUS SETTING RELATIONSHIPS		
NAS and Firewall RADIUS Clients	VRM	IAS
IP address	IP address in Server settings & IP address in Client settings	
Port numbers	Port numbers in Server settings	
Shared-Secret	Shared-Secret in Client settings	
	IP address in Proxy settings	IP address in Client settings IP address in Server settings
	Port numbers in Proxy settings	Port number in Server settings
	Shared-Secret in Proxy settings	Shared-Secret in Client settings

The following diagram shows actual RADIUS settings. (numbers are examples only)

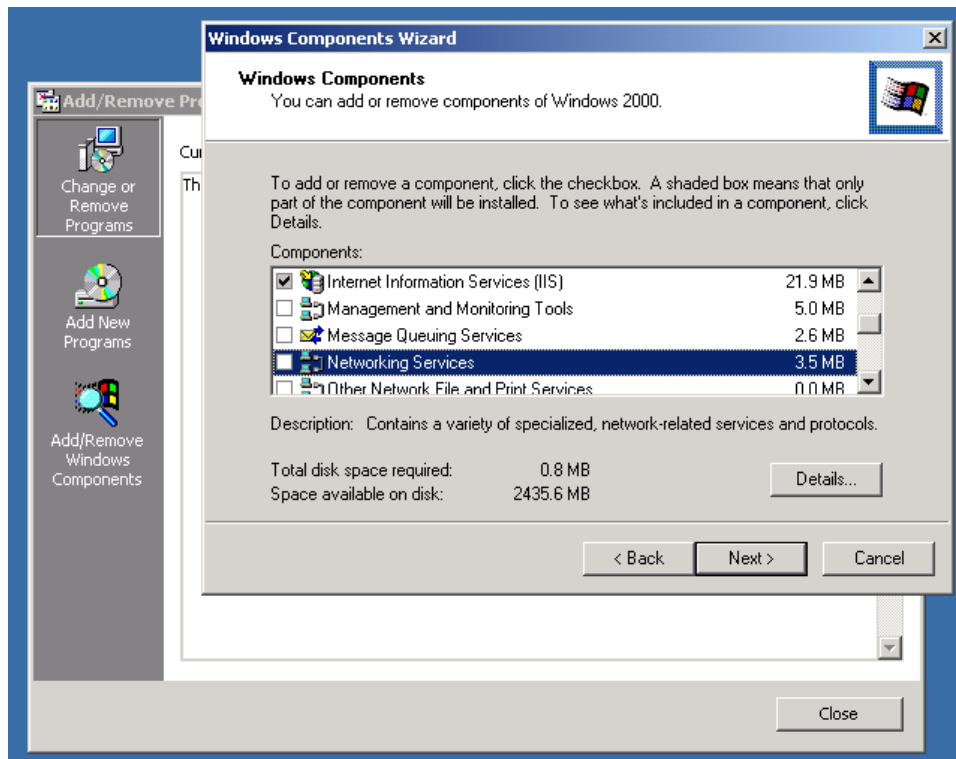


IAS Installation

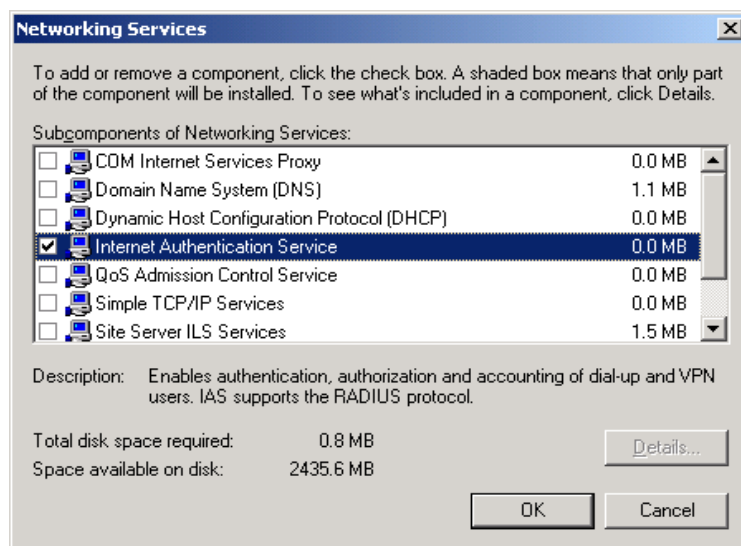
IAS (Internet Authentication Service) is a part of Windows 2000. To install it, go to the control panel and click on Add/Remove Software:



Next, select Add/Remove Windows Components and look for Networking Services. Then, click on details:



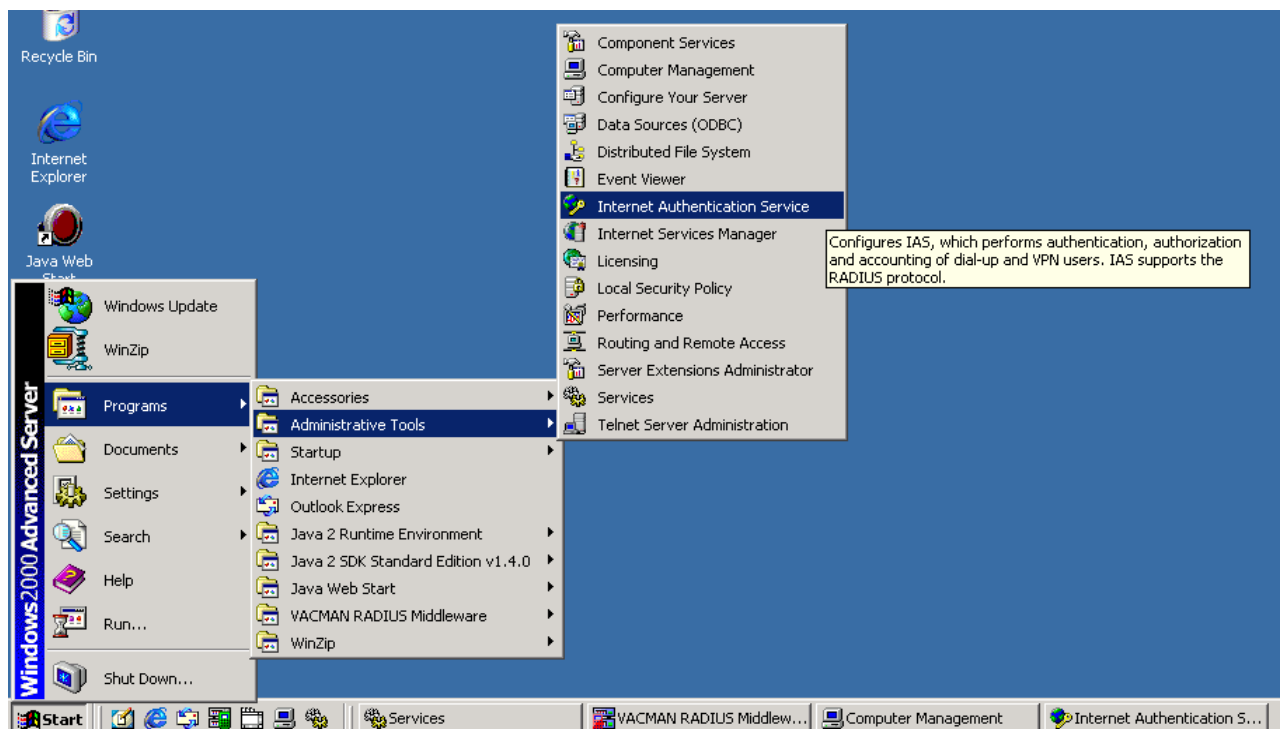
Select Internet Authentication Services from the list



Insert your W2K CDROM, click “OK”, click next...
Now go on to the next section to configure your IAS

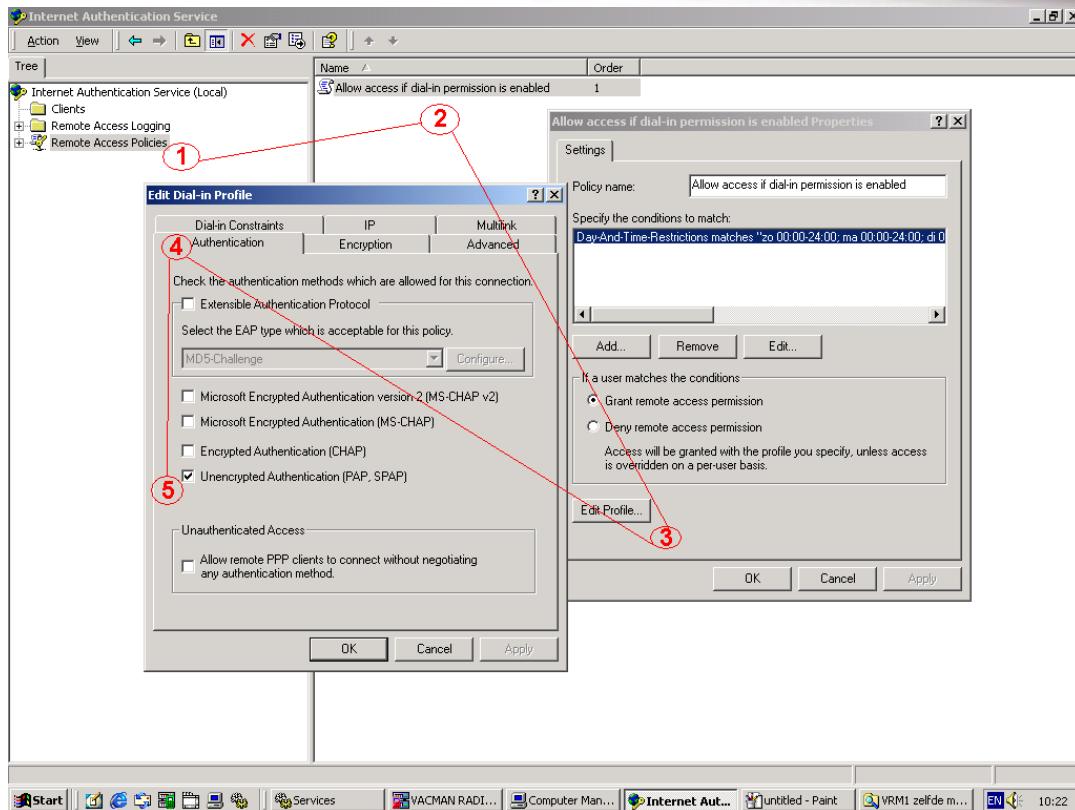
IAS Configuration

First you have to change the policy so the IAS accepts PAP as an authentication method
START -> admin tools -> Internet Authentication Server



- Click on REMOTE access policy's (1)
- Select your policy and open it's properties (2)
- Click on "edit profile" (3)
- Authentication tab (4)
- Enable PAP authentication (5)
- Apply/ok

Remark: You should change your policies. This is very site specific.



Second, add the machine that will run the Middleware as a client in IAS

- START -> admin tools -> Internet Authentication Server (Fig 1)
- Click on clients and add a new client
- Choose a friendly name
- Click next

Add Client

Name and Protocol
Assign a name and protocol for the client.

Type a friendly name and protocol for the client.

Friendly name: VRM

Protocol: RADIUS

< Back Next > Cancel

- As IP choose the Middleware-server-to-be (this can be the same or different machine)
- Fill in the shared secret between the VACMAN Radius Middleware and your IAS server
- Apply

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS): 192.168.4.251 Verify...

Client-Vendor: RADIUS Standard

Client must always send the signature attribute in the request

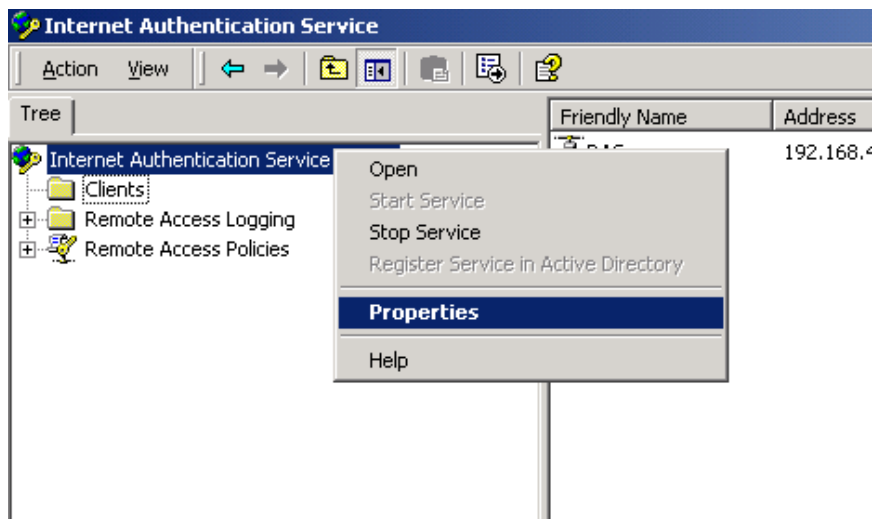
Shared secret: xxxxxx

Confirm shared secret: xxxxxx

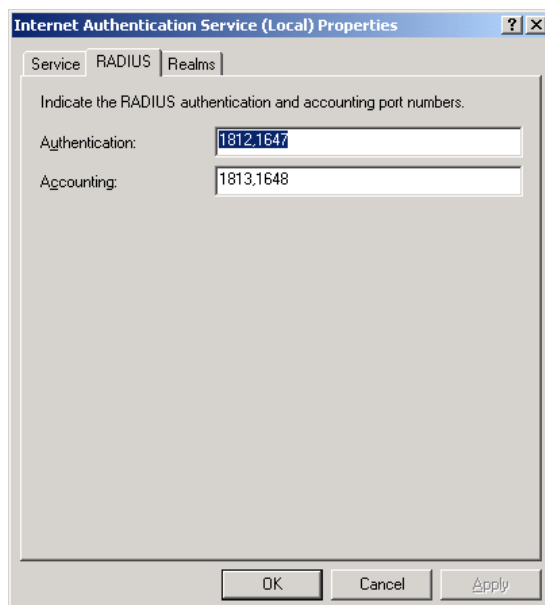
< Back Finish Cancel

NOTE: If you are installing VRM and IAS on the same machine, you have to alter the port settings of your IAS server

- START -> admin tools -> Internet Authentication Server
- Right-click on "Internet Authentication Service (local)" and open properties

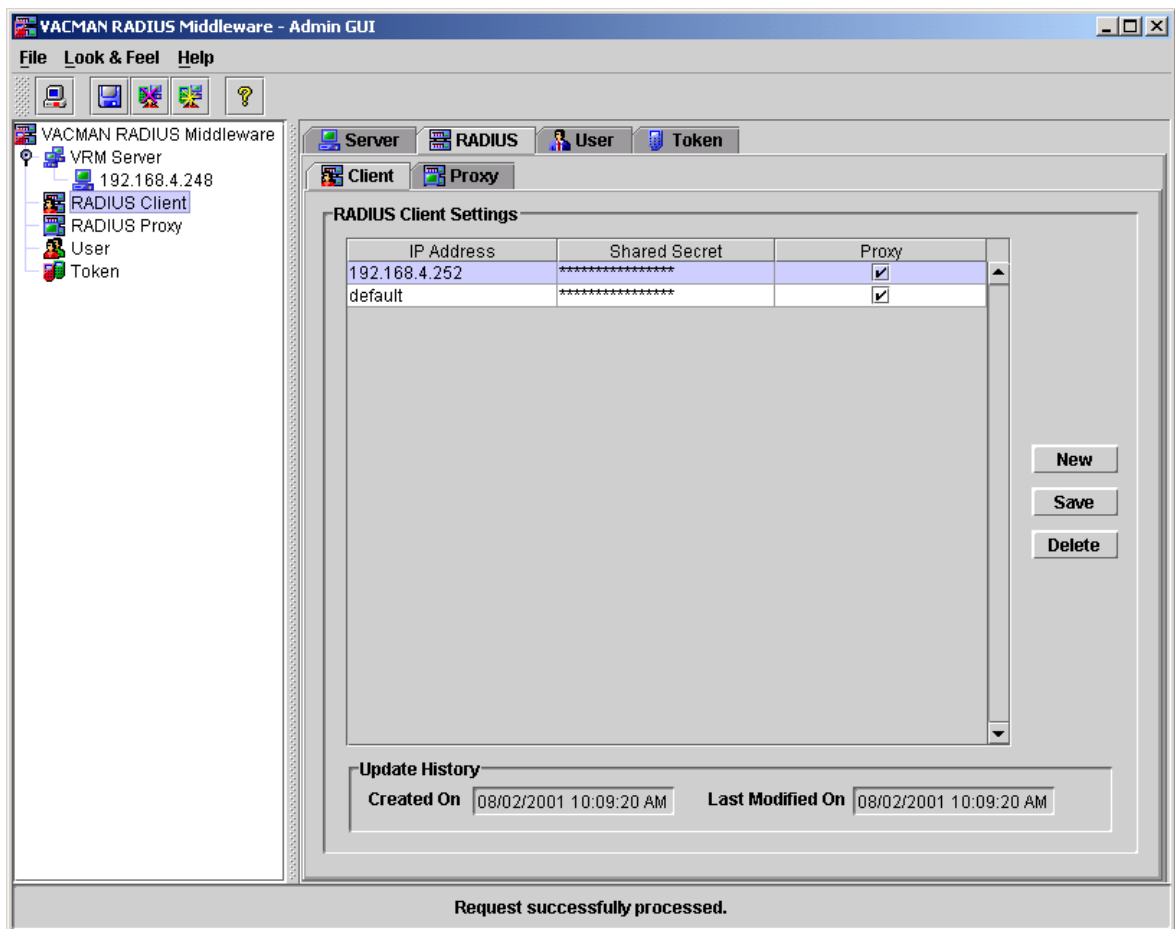


- Click on the RADIUS field and change the port settings to something else then the default RADIUS ports
- These ports should be unused UDP port numbers, (in the example: 1647, 1648)



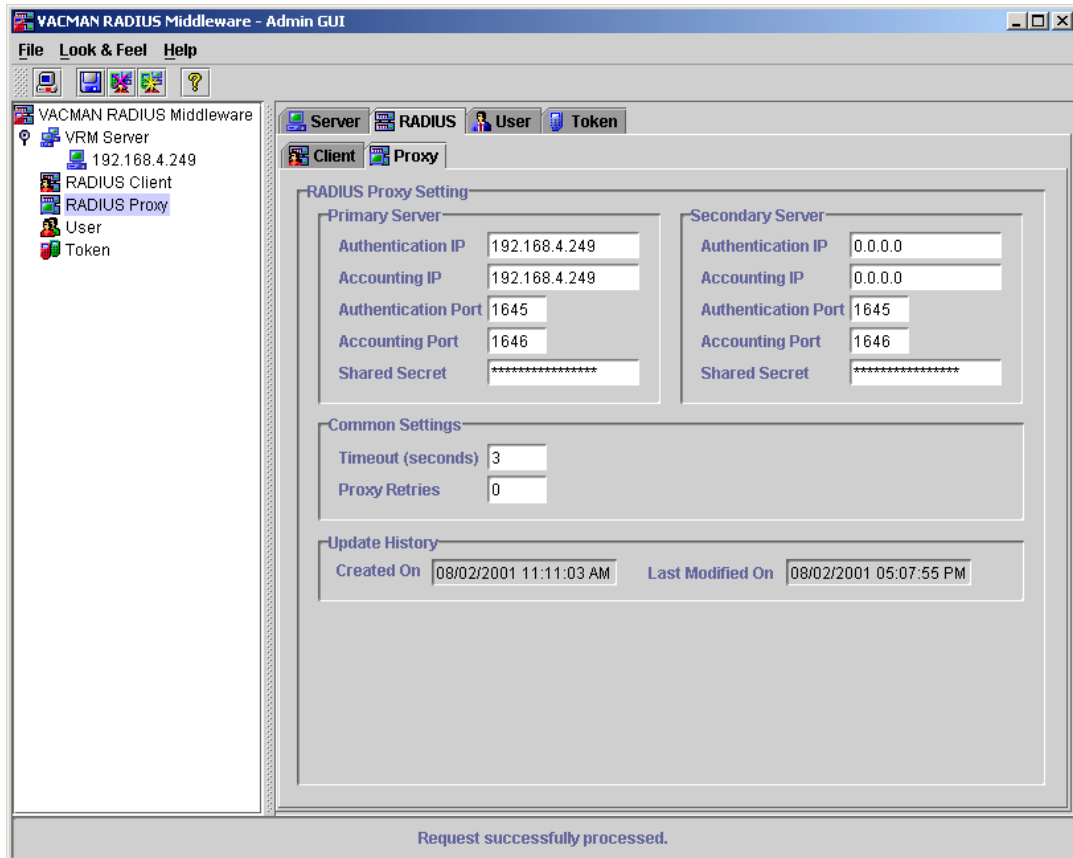
VACMAN RADIUS Middleware Configuration

- Install VACMAN RADIUS Middleware (this can be the same machine, see below)
- Be sure to have JAVA Runtime Environment installed (JRE 1.2 or 1.3)
- Reboot
- Configure the VACMAN RADIUS Middleware
- Open the Admin GUI
 - First Time? Log in as Admin with no password
- In the left field click "RADIUS Client", then click new
 - In the new line, type as IP the IP of your RAS/NAS server
 - Fill in the shared secret between the Middleware and RAS/NAS
 - Check the proxy checkbox
 - SAVE

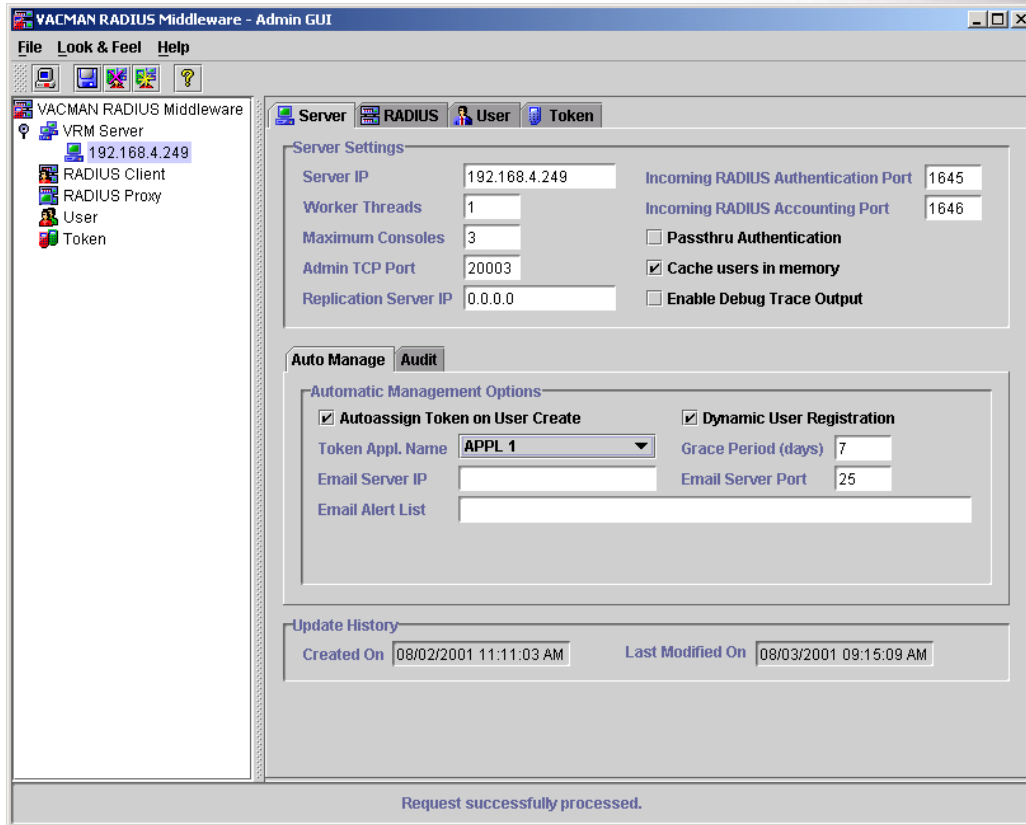


- In the left field click RADIUS PROXY

- Change the IP of the proxy to the IP of your IAS server
- Change the shared secret to the secret between your IAS and Middleware
- Change the port numbers (Authentication and Accounting ports). If you run this VRM on the same machine as the IAS? use the port numbers you assigned to IAS



- In the server window, check the Dynamic user registration and Autoassign token
- Choose the appropriate application name for the autoassigned tokens
- Don't forget to import your tokens (refer to VRM manual)



At this point, the RADIUS clients, VRM and IAS should be properly configured and running.