

**VACMAN RADIUS Middleware  
for Interlink Networks AAA  
RADIUS Server**



THE AUTHENTICATION COMPANY

# VACMAN RADIUS Middleware for Interlink Networks AAA RADIUS Server

---

## Contents

Contents .....	2
VRM Must Run Between the RADIUS Clients and AAA Server .....	3
Overview of RADIUS Authentication With VRM Installed.....	3
Overview of RADIUS IP and Port Settings.....	3
Interlink AAA Installation.....	5
Interlink AAA Configuration .....	5
VACMAN® RADIUS Middleware Configuration.....	5
Migration Steps.....	8
Delaying the Migration Until Ready.....	8
Creating Users in VRM Database .....	9
Determining Whether to Keep the AAA Server Running .....	9
About VASCO Data Security .....	10
General.....	10
Digipass product range .....	11
Digipass Pro:.....	11
Digipass GO:.....	11
Digipass Desk: .....	11
VACMAN product range .....	12

## VRM Must Run Between the RADIUS Clients and AAA Server

In order for VRM to transparently integrate into the AAA's RADIUS environment, it has to be positioned in between the RADIUS clients such as NAS and firewall and the AAA's RADIUS daemon program as shown below. More details on how to properly configure the RADIUS IP, Port, and Shared-Secret settings are discussed later.



## Overview of RADIUS Authentication With VRM Installed

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 AAA RADIUS server.
4. The Interlink AAA RADIUS server performs its verification, and then returns the results.
5. VRM forwards the AAA server results to NAS.
6. The NAS takes an appropriate action based on returned RADIUS results from AAA Server via VRM.

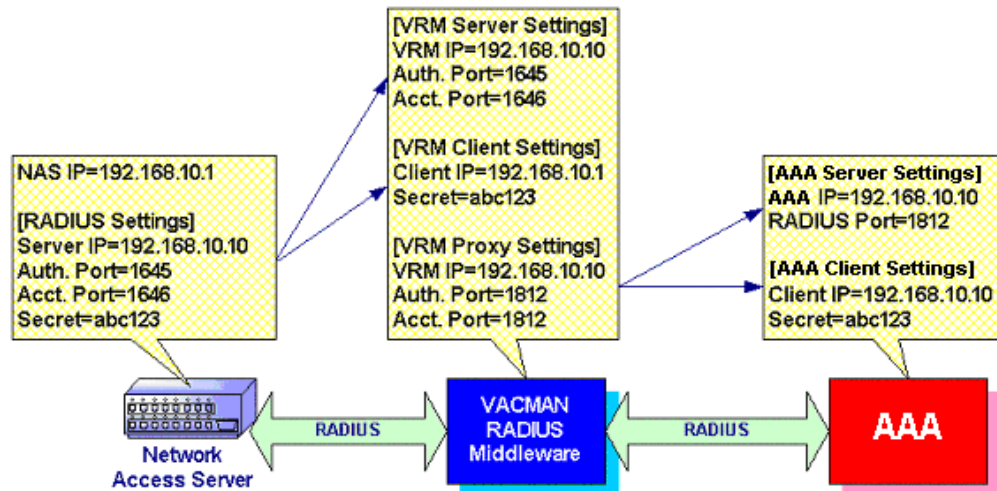
## Overview of RADIUS IP and Port Settings

In most installations, only a few AAA RADIUS servers manage many NAS and firewall RADIUS clients. Therefore, the recommended setup is to change the limited number of VRM and AAA 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, see **VRM Configuration** and **Interlink AAA Server Configuration** sections in this document on how to configure these settings.

Required RADIUS Setting Relationships		
NAS & Firewall RADIUS Clients	VRM	AAA
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. (These numbers are examples!)



## Interlink AAA Installation

Look for the tarball (\*.tar.gz file) of the Interlink AAA server. The place of this file depends on the way you received the file (probably CDROM), and copy it to /tmp and unpack it:

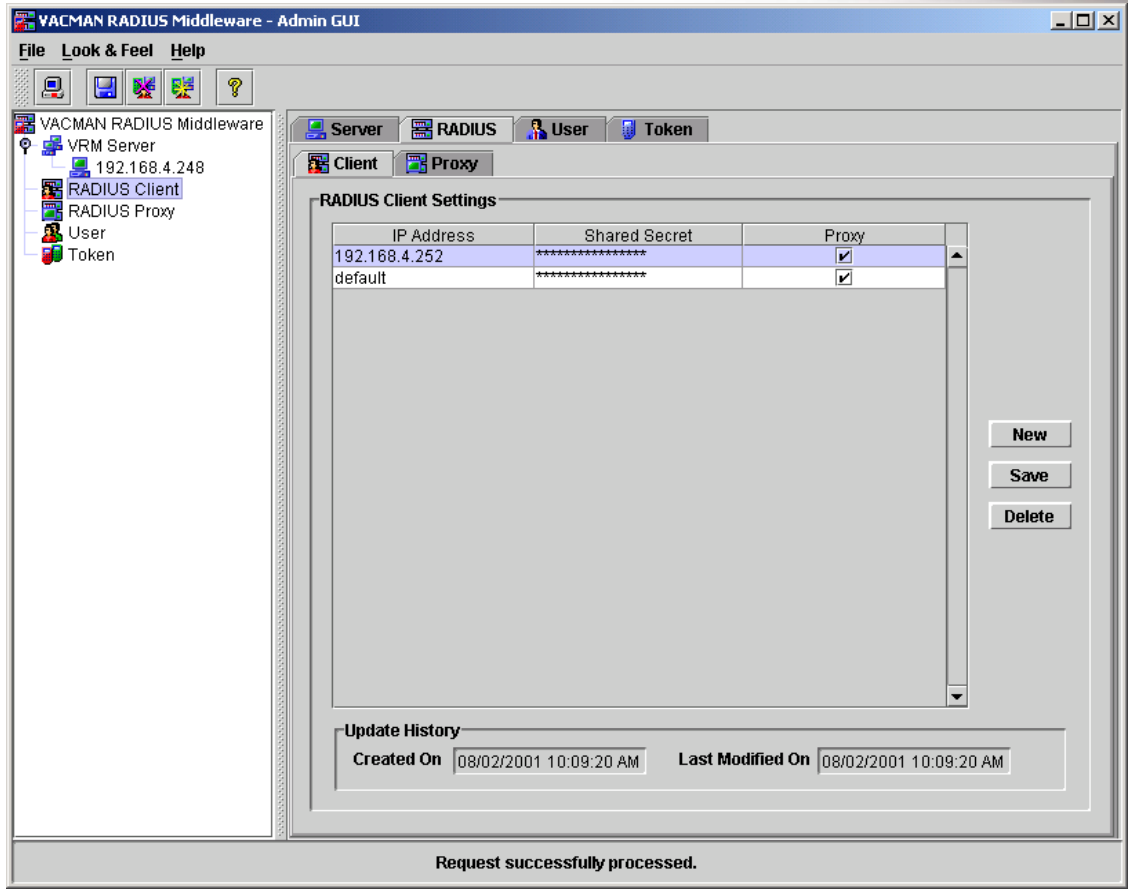
```
cp AAA.4.4TW.linux.tar.gz /tmp
cd /tmp
tar -xvfz AAA.4.4TW.linux.tar.gz
cd aaa-4.4TW-linux/
./aaainstall all
cd /usr/private/etc
```

## Interlink AAA Configuration

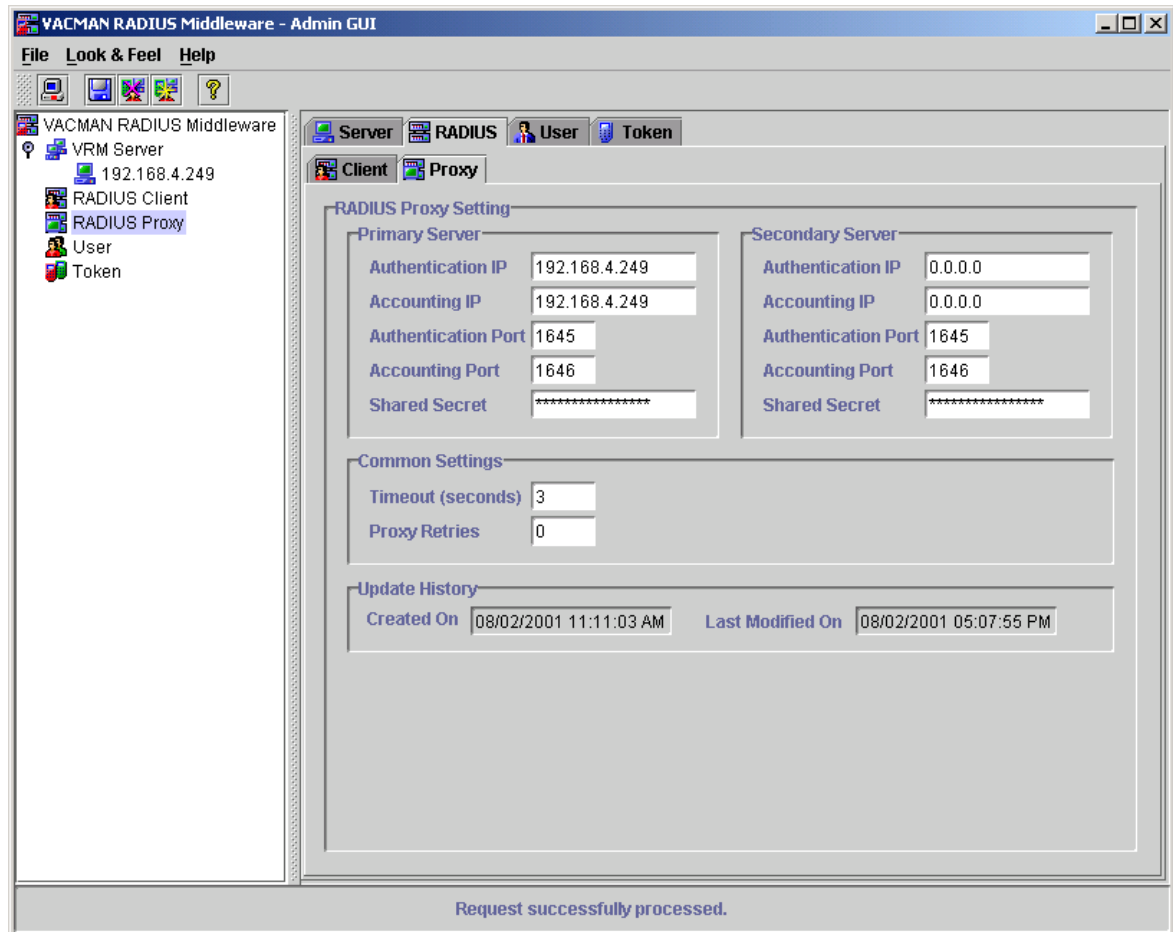
- in raddb/clients add a clientline for the middleware server:  
<client IP or name> <shared secret> type=none:proxy
- be sure to start radiusd with the same port as specified in the VRM configuration, you can OR change radiusd ports to 1645/1646 or you can change VRM configuration to connect to the standard AAA radiusd ports 1812/1813. For example:  
./radiusd -p 1645 -q 1646

## VACMAN® RADIUS Middleware Configuration

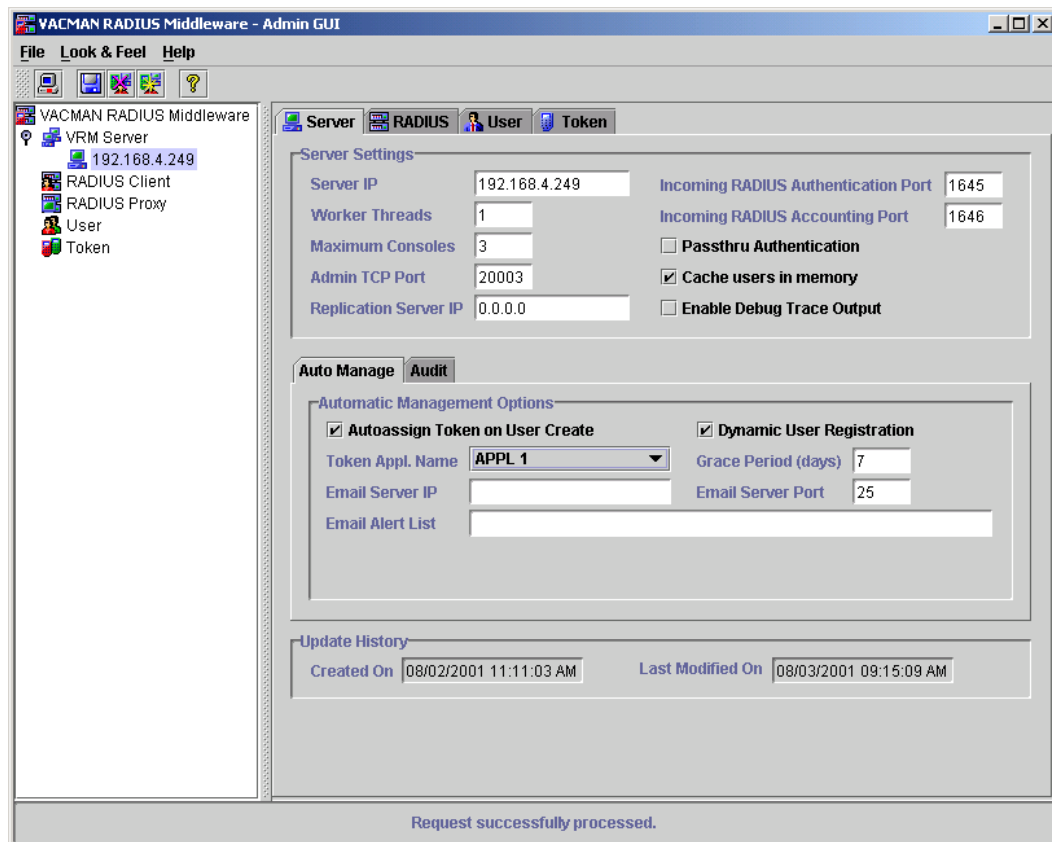
- Install VACMAN® RADIUS Middleware - be sure to have JAVA Runtime Environment installed (JRE 1.2 or 1.3)
- Reboot
- Configure the VACMAN® RADIUS Middleware
- Open the Admin GUI (The first time - Log in as admin with no password)
- In the left field click "RADIUS Client", then click new
- In the new line, type as IP the IP of your RAS/NAS server
- Fill in the shared secret between the Middleware and RAS/NAS
- Check the proxycheckbox



- 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 AAA and VRM
- change the port numbers ( Authentication and Accounting ports) to the ones radius is listening to (see above)



- 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 (see also VRM manual)



## Migration Steps

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

### Delaying the Migration Until Ready

If there is a need to delay the migration, enable the **PASSTHRU** option in the **VRM Server** settings to suppress VRM's authentication and only to authenticate at AAA. See the **Server Object** section in the *VACMAN® RADIUS Middleware Administration Guide* on how to set this option.

## *Creating Users in VRM Database*

Enable **Dynamic User Registration (DUR)** and disable **PASSTHRU** in the **VRM Server** settings. During this time, VRM transparently forwarded all RADIUS authentication requests to IAS without performing any authentication. With DUR enabled, and PASSTHRU disabled, all users that authenticate successfully to the AAA will be automatically created in the VRM database.

Using the DUR option is strongly recommended, but alternatively, users can be manually created using the VRM's **Admin GUI** or **admutil** command line interface.

## *Determining Whether to Keep the AAA Server Running*

Once all users have been migrated to the VRM database and are assigned Digipass tokens, a decision has to be made on the following:

- Continue to use VRM and AAA together.
- Only use VRM and remove AAA.
- Use VRM with another RADIUS server.

RADIUS is based on the triple A disciplines: Authentication, Authorization, and Accounting.

From a RADIUS client's perspective, devices such as Network Access Servers (NAS) require a RADIUS server that supports all three disciplines to manage them. On the other hand, RADIUS clients such as firewalls usually only require support for RADIUS authentication and not the RADIUS authorization nor accounting.

From a RADIUS server's perspective, VRM only handles the RADIUS authentication requests and relies on a third-party RADIUS server to provide the RADIUS authorization or accounting support.

VRM is primarily a Digipass authentication server that uses RADIUS authentication protocol. VRM separates the token authentication from the rest of the RADIUS processing. By doing so, VRM enables Digipass authentication with virtually no disruption to the existing RADIUS environment.

If AAA is no longer going to be used, ensure that there are no other AAA clients, besides the RADIUS authentication, that need the AAA's presence.

## About VASCO Data Security

### General

VASCO Data Security International, Inc. (VDSI) designs, develops, markets and supports open standards-based software and hardware security products, which manage and secure access to information and financial assets. Securing trust, securing value is the company's creed. VASCO's range of enterprise-wide products secure Internet, client/server, and mainframe-based applications, and provide end-to-end security through RADIUS, LAN and Web security, PKI and LDAP enablement, web portal and application security, strong user authentication, access control, user administration and encryption.

VASCO's products are used by more than 7 million users, by over 180 financial institutions and by hundreds of blue-chip corporations and governments, spanning over 50 countries. VASCO is a global company with headquarters in the United States.

Company:	VASCO Data Security International
NASDAQ NM/NASDAQ EU.:	VDSI
Founded:	1997
Web:	www.VASCO.com
CEO:	Ken Hunt
President and COO:	Jan Valcke
Employees:	80
Worldwide Headquarters:	1901 South Meyers Road, Suite 210, Oakbrook Terrace, Illinois, USA
European Headquarters:	Koningin Astridlaan 164, B-1780 Wemmel, Belgium
VASCO Product Range:	<i>VACMAN</i> : Authentication, Authorization, Administration, AAA Security <i>Digipass</i> : Encryption, Remote Access, Corporate Access, Hard- & software tokens

VASCO's roots are in cryptography. It was the first company in the world to port the DES and RSA algorithms to a chip and also the first to develop a software product to authenticate and digitally sign e-banking and online brokerage services. Now, VASCO secures the enterprise from the mainframe to the Internet with infrastructure solutions that enable secure e-business and e-commerce, while protecting sensitive information and safeguarding the identity of users. The company's family of Digipass® and VACMAN® products offer end-to-end security through strong authentication and digital signature, enterprise Single Sign-On, and LAN security, while sharply reducing the time and effort required to deploy and manage security.

## **Digipass product range**

DIGIPASS® provides financial institutions and companies with a secure means of customer or employee identification and authentication for remote access to their computer systems and networks.

Digipass stands for three ranges:

### ***Digipass Pro:***

Digipass Pro includes Digipass models for professional use, offering dynamic password and digital signature functionality.

- Digipass Pro 300 is ideally suited for large public banking applications such as telebanking, home banking, PC banking, phone banking and Internet banking where authentication and e-signatures are key requirements.
- Digipass Pro 550 combines strong authentication, e-signatures and a modern design with integrated hardcover.
- Digipass Pro 600 grants physical access to buildings as well as secure remote network access.
- Digipass Pro 700 offers sophisticated and yet user-friendly strong authentication services with extended digital signature capability.
- Digipass Pro 800 is used by several top tier banking institutions
- worldwide and is strongly appreciated by the banks and their clients for securing full access to financial applications on the existing banking network via an existing smart card, in a flexible, easy to use and cost-effective way.

### ***Digipass GO:***

Digipass GO can be used Anywhere, Anyhow and Anytime. It is e-security that fits in your pocket, clips on your belt, hangs around your neck, on a key ring.

- Digipass GO 1 is the first-born in the "GO" range. GO 1 is an ultra-portable, smoothly designed token that outsmarts all others and is much safer than any static password.
- Digipass GO 10 is a software Digipass for GSM's, integrated on the SIM card.

### ***Digipass Desk:***

The Desk-range contains highly user friendly Digipass models to be used on a professional's desk.

- Digipass Desk 300 is a large-scale security device designed for managers and executives. It features remote access and authentication features and its larger size makes it very suitable for use in the office.
- Digipass Desk 850 can future-proof an existing smart card system, increase a network's security and leverage investment in a public key infrastructure (PKI) solution. This

advanced e-wallet/PKI device provides ultimate versatility and security, supporting strong authentication and e-signatures for the customers authorized to carry your smart cards.

- Digipass Desk 3000 is a software Digipass for laptop & desktop.

### **VACMAN product range**

VACMAN Controller integrates smoothly into existing applications that require remote access.

VACMAN RADIUS Middleware enables strong authentication security without replacing or redesigning your remote access solution(s).

VACMAN Server is a cross platform authentication engine designed to provide strong and seamless user authentication and access control for remote, local and web-based users. The product supports RADIUS, LAN and Web functionality.

- *VACMAN Server for RADIUS* is a standard compliant server designed to provide AAA services.
- *VACMAN Server for Networks* provides strong user authentication and access control management for RADIUS and LAN environments in a fully integrated system.
- *VACMAN Server for Web* delivers access control to Web enabled applications, whether Internet, extranet or intranet based.