

Transparent, Strong Authentication Using Auto-managed **VACMAN[®] RADIUS Middleware**

White Paper



SECURITY BEYOND e-MAGINATION

Transparent, Strong Authentication Using Auto-managed VACMAN[®] RADIUS Middleware

Contents

Overview	2
Why Use VACMAN RADIUS Middleware	2
Problem Description	3
Concept	4
Technical Description	5
Client Server Authentication Model	6
Special Features	7
Admin GUI	9
Audit Console GUI	10
Admin Utility – Command Line Interface	12
Product Configurations	13
Full RADIUS Support (AAA) – Single Server Machine	13
Full RADIUS Support (AAA) – Two Server Machines	14
RADIUS Authentication Only	15
Full RADIUS Support (AAA) – Proxy Servers	16
System Requirements	17

Transparent, Strong Authentication Using Auto-managed VACMAN® RADIUS Middleware

Overview

Strong user authentication, based on VASCO Digipass® technology, is now easy and affordable thanks to VACMAN® RADIUS Middleware. This RADIUS security middleware product helps you manage and secure remote access to your corporate IT environment.

With dozens of different entry points to consider, and almost as many different platforms and technologies to manage, it's not easy to provide secure remote access to today's corporate computing networks. VACMAN RADIUS Middleware ("VRM") bridges this security gap by bringing seamless strong user authentication to your RADIUS environment.

Many companies already use RADIUS servers and/or firewalls to provide a way to centrally manage all remote connections to the corporate IT infrastructure. In most cases, these RADIUS-based solutions perform very well. But they're simply not designed to provide strong user authentication. VRM solves this dilemma by bringing strong user authentication to the RADIUS environment, while seamlessly integrating with other current infrastructure technology. With VRM installed, network administrators are always able to positively identify the remote users who request access to the network.

Why Use VACMAN RADIUS Middleware?

- **Transparently Enables Strong User Authentication** using Digipass to the existing RADIUS environment while preserving the existing network infrastructure and investments made in them.
- **Seamless and Non-intrusive Interoperability with all RADIUS Servers** that conform to the industry standard RADIUS protocol specifications.
- **Turnkey Solution** that is simple and quick to install, configure, and activate.
- **Automated Management** feature automates the user registration, token assignment, and email distribution.

- **Token Graceperiod** feature permits static-password logins after the token is assigned to compensate for the time lag required to make physical distribution of tokens to users.
- **Bulk Management** feature allow administrators to quickly administer thousands of users and tokens through a single mouse click.
- **High Performance Engine** can easily handle high number of authentication requests of a large remote access network. There is even an option to cache user information in memory.
- Provides **Full Redundancy** through the use of one or more backup servers.
- **Admin GUI** is a highly intuitive GUI where authorized administrators can perform sophisticated administration tasks.
- **Audit Console** is a highly intuitive GUI where authorized administrators can perform realtime monitoring of audit events such as RADIUS authentication, accounting, and VRM administration. These audit events are also centrally recorded on the server's machine.
- **Admin Utility** is a comprehensive command line interface (CLI) designed to enable VRM administration from a third-party program.

Problem Description

Most of today's corporate computing networks provide remote access to authorized users through RADIUS servers, firewalls, or similar remote access solutions. These solutions provide central management of all Authentication, Authorization and Accounting (AAA) services for remote users. In most cases, remote access solutions follow the industry-standard RADIUS protocol as a carrier for the AAA services they provide. RADIUS-based solutions are known to be very solid and cost effective. However, as a rule, they do not provide Strong User Authentication. Instead, security is typically based on pairing User-Ids with static Passwords as a means of identifying the persons trying to access proprietary information on the corporate LAN or Intra/Extranet. VRM is designed to close the potential gap in network security, by providing a proven, cost-effective way to verify the identity of any remote user who requests access to corporate data resources.

VRM delivers strong user authentication through the VASCO Digipass family of tokens—special devices that are programmed to generate One Time Passwords (OTP's). With VRM installed, OTP's can be used to provide secure access to remote users, through the company's existing AAA servers and firewalls.

Concept

VRM is a fast, highly configurable, simple to use, turnkey Digipass authentication server solution, designed to work in any RADIUS-based environment. VRM makes it possible to secure an enterprise network, through strong (two-factor) user authentication, without replacing or reconfiguring existing RADIUS servers and firewalls. Logically, VRM is installed between the RADIUS client (NAS, RAS, or firewall) and the RADIUS server. Once installed, VRM functions transparently, adding strong (two-factor) authentication without otherwise affecting the operation of the server or other network components. VRM fills the security gap present in most of current RADIUS solutions. It's designed to give companies a simple and cost-effective way to "install, configure and run" a full-featured security solution – one that delivers the maximum level of security and flexibility, while requiring a minimal amount of management. The following illustration shows how VRM achieves its objectives.

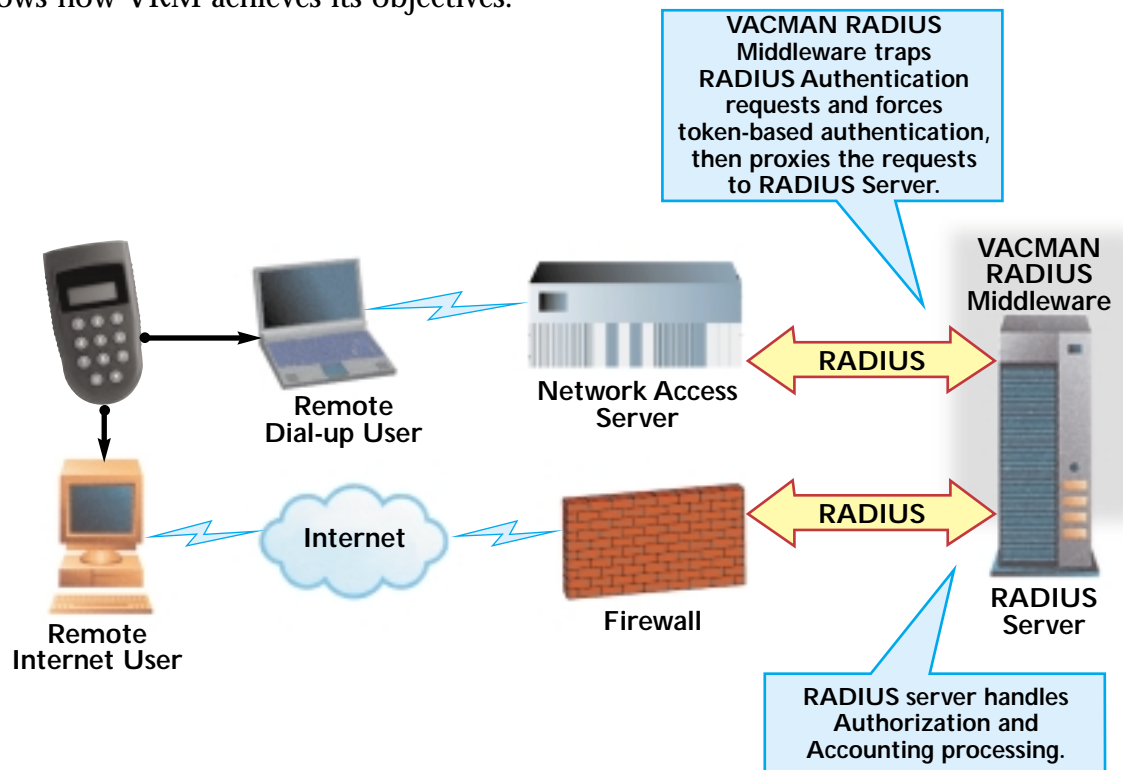


Figure 1. The global goal: Secure any RADIUS environment with Digipass strong user authentication.

Technical Description

VRM integrates seamlessly into the RADIUS environment, whether a RAS or a firewall is used to connect remote users to the corporate IT infrastructure. Therefore, we will first explore how VRM fits into these environments, before we provide technical detail on how the solution works.

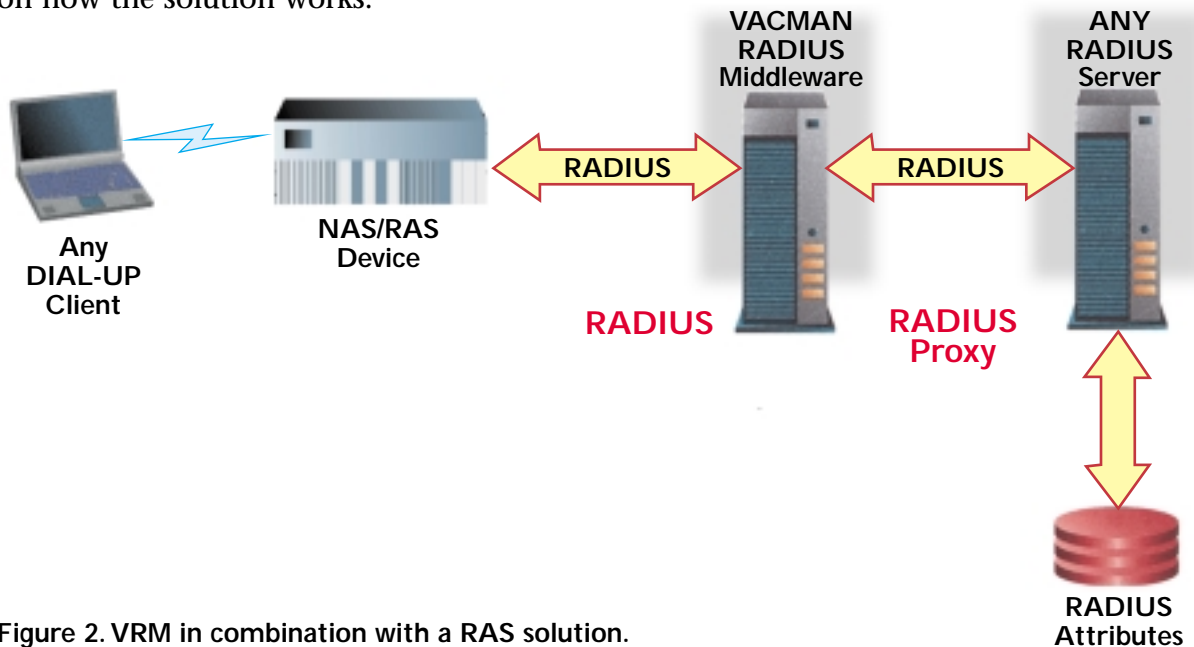


Figure 2. VRM in combination with a RAS solution.

As shown in Figure 2, VRM is installed logically between the back-end RADIUS server and the NAS/RAS (Network Access Server/Remote Access Server) device.

Physically, VRM can be installed on any machine (that meets VRM's system requirements) on the network that has both IP connectivity and a connection to the NAS and the RADIUS server. In most cases, VRM can be installed on the same machine as the RADIUS server application, if it is running on Windows NT 4.x or 2000.

Client Server Authentication Model

The following illustration shows how VRM enforces strong Digipass authentication in a typical scenario. (Please note: the presence of a RADIUS server is mandatory in this situation if you require full AAA services in your environment.)

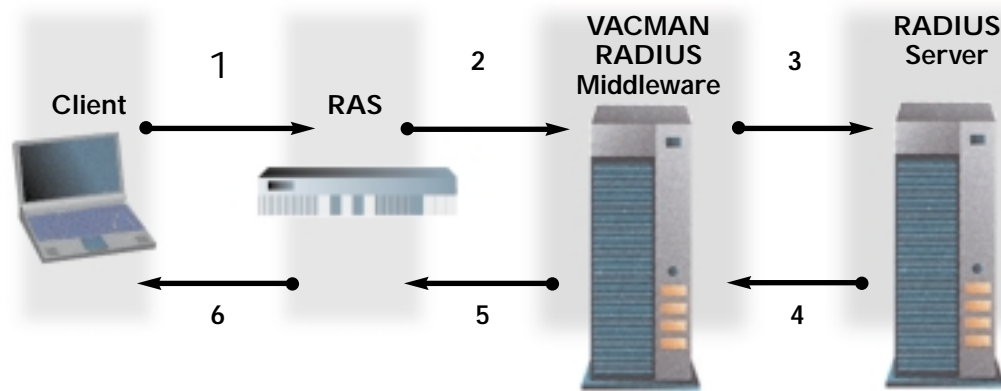


Figure 3. Client Server Authentication Model (Time Based Response Only mode).

Each time a user tries to log on to the corporate network, the following steps occur:

1. User attempts a dialup connection to the NAS device from a Windows O/S using the default dialup client.
2. NAS collects the user ID and password entered by the remote dialup user and submits a RADIUS authentication request to VRM. Note that this password can be static-password, Digipass OTP, or both.
3. VRM performs the following:
 - 3.1. The login request is denied by VRM and an login-denied result is sent back to the NAS in the following conditions:
 - 3.1.1. Either the Dynamic User Registration (DUR) is not enabled or RADIUS proxy is not setup and the user did not exist in the VRM database
 - 3.1.2. Either the DUR is not enabled or RADIUS proxy is not setup and the existing user fails the VRM's password and/or OTP verification
 - 3.2. The login request is forwarded to the third-party RADIUS server in the following conditions:
 - 3.2.1. DUR is enabled and RADIUS proxy is setup and the user did not exist in the VRM database. This is an attempt to DUR the user into the VRM database.

- 3.2.2. DUR is enabled and RADIUS proxy is setup and the user exists in the VRM database but the static-password did not match. This is an attempt to autolearn the password.
 - 3.2.3. PASSTHRU is enabled and RADIUS proxy is setup. VRM is not involved in the authentication in this mode.
4. VRM performs the following:
 - 4.1 If the proxied login request is accepted by the third-party RADIUS server:
 - 4.1.1. The user is created into the VRM database if it corresponds to the 3.2.1 condition.
 - 4.1.2. The user's static-password is updated if it corresponds to the 3.2.2 condition.
 - 4.1.3. In all other cases, the login-accepted result is sent back to the NAS.
 - 4.2 If the proxied login request is denied by the third-party RADIUS server:
 - 4.2.1. The login-denied result is sent back to the NAS and VRM performs no other processing.
5. NAS performs the following:
 - 5.1. If the login request is accepted, NAS uses the returned RADIUS authorization attributes as a guideline to establish the dialup connection.
 - 5.1.1. If the login request denied, NAS rejects the connection request.
6. The remote user's connection request is either established or dropped.

Special Features

- **Response Only and Challenge-Response Digipass Authentication**

VRM is specifically designed to support the Digipass Token family on RADIUS servers. This means that the entire range of security settings supported by the Digipass tokens are now available to secure RADIUS-based remote-access environments. Administrators can choose from a variety of login features such as Time-Based-Response-Only and Challenge-Response.
- **Dynamic User Registration (DUR)**

The DUR feature can automatically create users in the VRM database after they have been authenticated by the third-party RADIUS server. (NOTE: The DUR feature requires a third-party RADIUS server with existing users.)

- **AutoLearn Passwords**

This feature allows static user passwords, assigned to new users on the back-end RADIUS server, to be auto-stored in the VRM database. After a valid Digipass authentication is received in VRM, the “autolearned” user password is automatically played back to the back-end RADIUS Server. (NOTE: The AutoLearn feature requires a third-party RADIUS server with existing users.)

- **Token Auto Assign**

If desired, VRM can be configured to automatically assign a ‘Free’ Digipass to a newly created user – whether the user was created through the Admin GUI, Admin Command Line Utility, or through the DUR feature. When a Digipass is assigned to a user, the VRM automatically writes a record containing all the account-specific parameters (Serial Number, User-Id, User-Name, etc.) to a log file and can also send out email notifications.

- **Passthru**

VRM supports both Digipass and Static Password authentication simultaneously. The Passthru feature allows a user to be authenticated by the back-end RADIUS server without any intervention from VRM. This option can be applied either globally; or at the individual user level. (NOTE: The AutoLearn feature requires a third-party RADIUS server with existing users.)

- **Digipass Graceperiod**

The Graceperiod enables VRM Administrators to assign Digipass tokens to users and delay the enforcement of Digipass authentication for a certain number of days. The Graceperiod feature allows the continued use of an existing static password until the Graceperiod expires or until the user successfully authenticates with the token. The length of the Graceperiod is configurable by the VRM Administrator.

- **Database Replication**

A built-in database replication feature can be used to provide realtime replication of the VRM database to one or more back VRM servers.

The Admin GUI is a standalone JAVA application, which requires JAVA Runtime Environment 1.2.2 or higher to run. This highly intuitive yet powerful interface allows authorized administrators to perform complete administrative tasks.

Feature Summary

- Run on the same machine as VRM server or remotely from another machine.
- Requires authentication and proper administration privilege to activate.
- Can dynamically switch between JAVA, Windows, and Motif look and feel at runtime.
- Create, Read, Update, and Delete all objects such as VRM Server, RADIUS Client, RADIUS Proxy, User, and Token.
- Perform conditional query and display the results in the tree view section.
- Select a specific object to display in the detail view in the tabbed section.
- Assign a token application to a user, or a user to a token application.
- Test, reset, and unlock each token application.
- Bulk manage one or thousands of users and token applications through a single mouse click.
- Import user and token records from an external file.
- View VRM product license with realtime user counts.

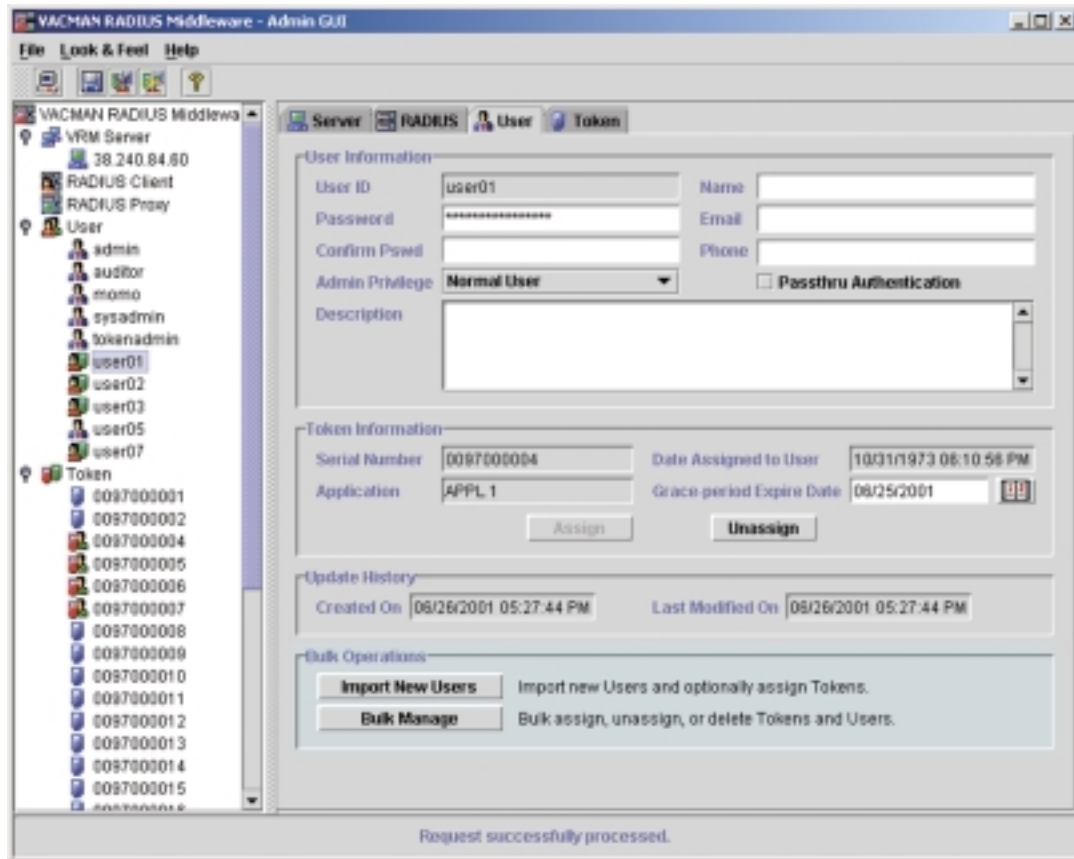


Figure 4. The VRM Admin GUI.

Audit Console GUI

The Audit Console is a standalone JAVA application, which requires a JAVA Runtime Environment 1.2.2 or higher to run. This is a highly intuitive, yet powerful interface that allows authorized administrators to monitor RADIUS requests, VRM administrative tasks, and VRM server activities in realtime.

Feature Summary

- Runs on the same machine as VRM server or remotely from another machine.
- Requires authentication and proper administration privilege to activate.
- Can dynamically switch between a JAVA, Windows, or Motif look and feel at runtime.
- Monitor up to three VRM servers simultaneously per each Audit Console program instance.
- Displays structure audit messages that contain Date/Time, Component ID, Message Number, Origination IP address, Summary Message, and Detail Message.
- Realtime total audit-event statistic counts.
- Customize audit-filtering on VRM components and message levels.
- Customize display coloring based on message levels.
- Able to read and format archived audit-events from a flat-file.

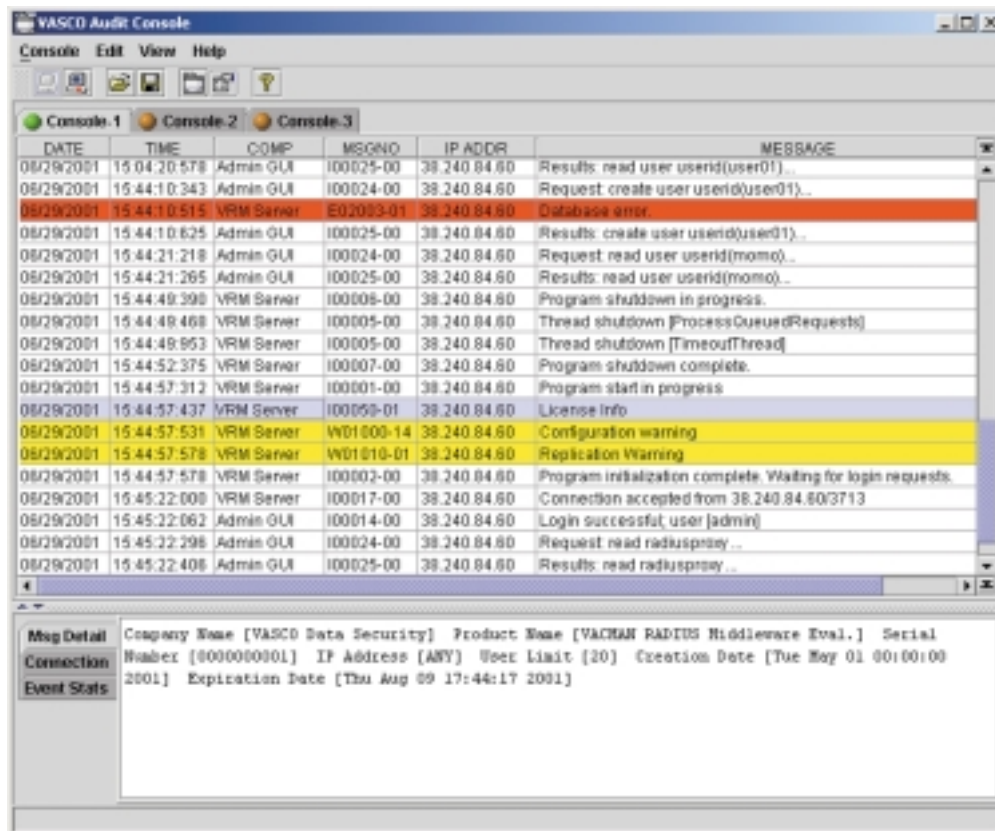


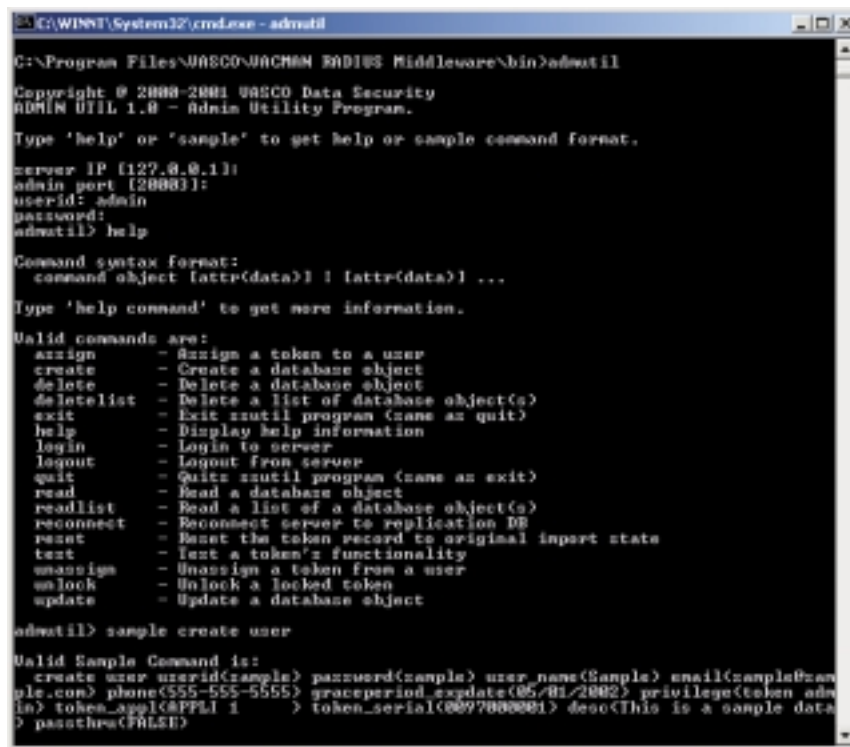
Figure 5. The VRM Audit Console.

Admin Utility – Command Line Interface

The Admin Utility (util.exe) is a command line interface, CLI, which is a highly intuitive, yet powerful interface that allows authorized administrators and third-party programs to perform complete administrative tasks similar to the Admin GUI.

Feature Summary

- Runs on the same machine as VRM server or remotely from another machine.
- Requires authentication and proper administration privilege to activate.
- Can perform almost all administrative tasks that Admin GUI can.
- Help and sample commands are structured, which allows quick navigation down to the necessary details.
- Can be used to enable VRM administration from a third-party program.



```
C:\WINDOWS\System32\cmd.exe - admutil
C:\Program Files\VASCO\WACHMAN RADIOS Middleware\bin>admutil
Copyright © 2000-2001 VASCO Data Security
ADMIN UTIL 1.0 - Admin Utility Program.
Type 'help' or 'sample' to get help or sample command format.
server IP [127.0.0.1]:
admin port [2000]:
userid: admin
password:
admutil> help
Command syntax format:
  command object [attr(data)] | [attr(data)] | ...
Type 'help command' to get more information.
Valid commands are:
  assign - Assign a token to a user
  create - Create a database object
  delete - Delete a database object
  deletelist - Delete a list of database object(s)
  exit - Exit admutil program (name as quit)
  help - Display help information
  login - Login to server
  logout - Logout from server
  quit - Quit admutil program (name as exit)
  read - Read a database object
  readlist - Read a list of a database object(s)
  reconnect - Reconnect server to replication DE
  reset - Reset the token record to original input state
  test - Test a token's functionality
  unassign - Unassign a token from a user
  unlock - Unlock a locked token
  update - Update a database object
admutil> sample create user
Valid Sample Command is:
  create user userid(sample) password(sample) user_name(Sample) email(sample@sam
  ple.com) phone(555-555-5555) graceperiod_expirydate(05/01/2002) privilege(token adm
  in) token_appl(APPL1 1) token_serial(0097000001) desc(This is a sample data)
  passthru(FALSE)
```

Figure 6. The VRM Admin Utility.

VRM is a fast, highly configurable, simple to use, turnkey Digipass authentication server solution, designed to work in any RADIUS-based environment. Where full AAA services are being used, VRM provides strong authentication while acting as a conduit for authorization and accounting services that are provided by an existing RADIUS server. VRM can also be used where only RADIUS authentication is needed, for example, in conjunction with a firewall. In addition, VRM can have RADIUS authentication requests proxied to it by other RADIUS servers. The following discussion summarizes the different configurations in which VRM can be used.

Full RADIUS Support (AAA) – Single Server Machine

Application

In this configuration, VRM is installed on the same machine as the existing RADIUS server. Logically, it sits between the NAS devices and the RADIUS server. It is configured to accept RADIUS authentication and accounting requests on the same ports as the RADIUS server was previously accepting them on, and the RADIUS server configuration is modified to accept requests on different ports. This configuration requires no changes in the configuration of the NAS devices, which is ideal if there are many of them.

In this configuration user management can be done only on the RADIUS server. VRM can dynamically register (DUR) the RADIUS server's users, can "AutoLearn" their passwords and can automatically assign Digipass tokens.

When an authentication request is received from a NAS, VRM authenticates the Digipass One-Time-Password (OTP). If this is successful, the request is modified, replacing the OTP with the user's static password, which was autolearned during DUR. The request is then proxied to the RADIUS server. The result of this proxy request is received by VRM and then sent back to the NAS. The result will typically contain RADIUS authorization attributes if the authentication succeeded.

If accounting is enabled in the NAS, the NAS will send an accounting record following successful authentication. VRM does not act upon accounting records. It simply proxies them to the RADIUS server and the results it receives are sent back to the NAS.

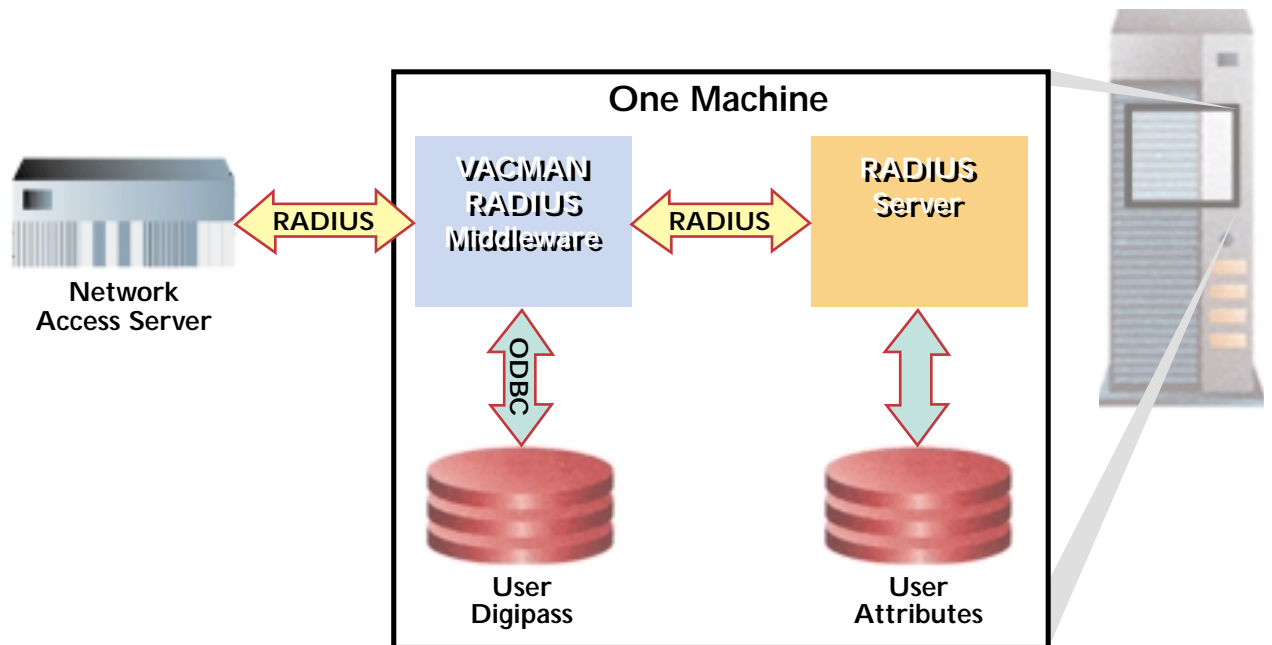


Figure 7.
Schematic Overview

Full RADIUS Support (AAA) – Two Server Machines

Application

In this configuration, VRM is installed on a machine different than the RADIUS server. Logically and operationally, there is no difference between this configuration and the previous one in which both the RADIUS server and VRM were on the same machine.

This configuration may be necessary if the RADIUS server's authentication and accounting ports cannot be modified and it is not desirable to reconfigure the NAS devices (because there is a large number of them). The machine with VRM installed must be configured to have the IP address that the NAS devices will be sending their requests to, and the machine with the RADIUS server must have its IP address changed.

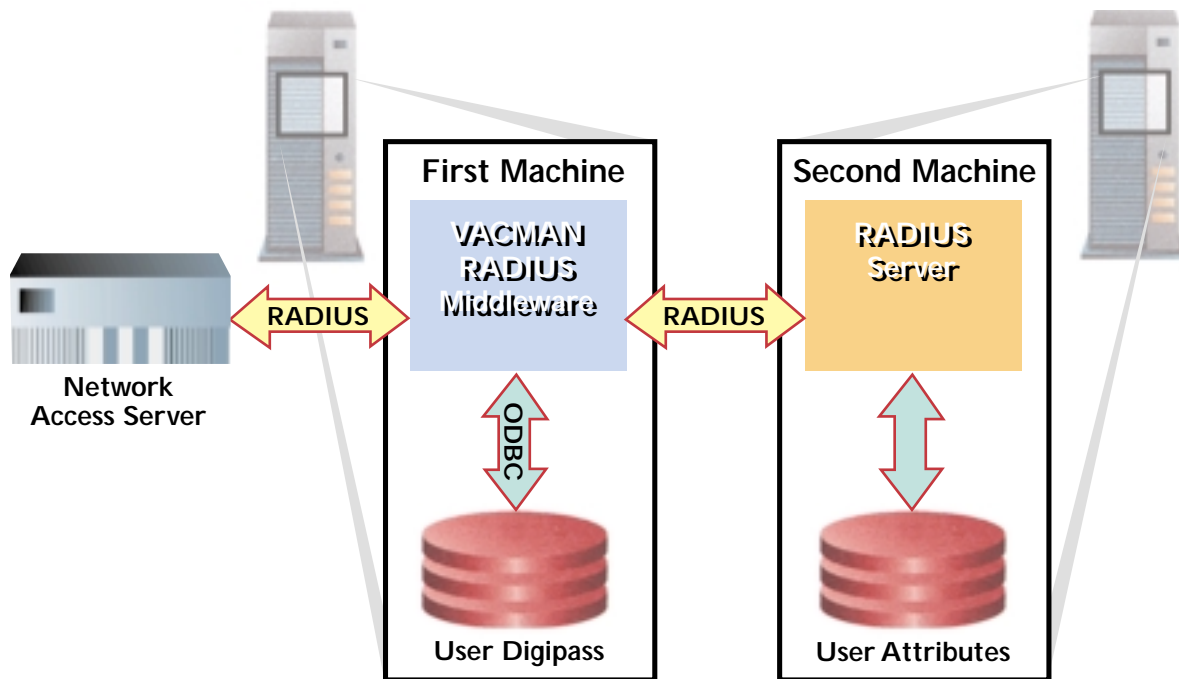


Figure 8.
Schematic Overview

RADIUS Authentication Only

Application

In the RADIUS Authentication Only configuration, VRM can be used in conjunction with applications that only require RADIUS authentication. This includes firewalls, such as CheckPoint FireWall I or ORACLE RDBMS.

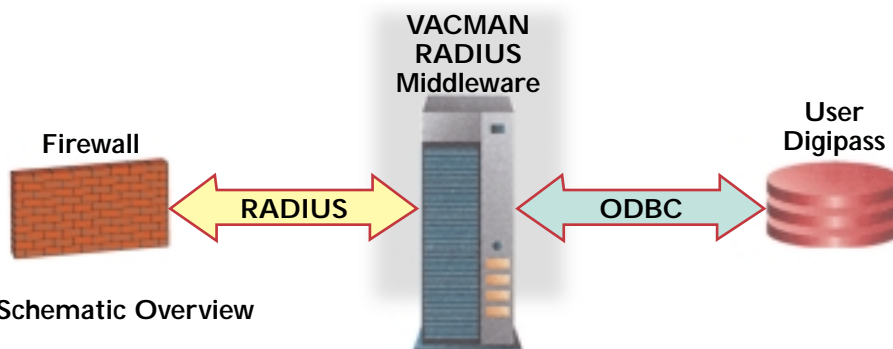


Figure 9. Schematic Overview

In this case, the Firewall will be set up to use external RADIUS Authentication. VRM, which contains the User database and corresponding information about the Digipass assigned to each user, will perform this authentication task.

In this configuration, user management will be accomplished manually using the ADMIN GUI. Since there is no RADIUS server in the configuration, DUR and AutoLearning of passwords cannot be performed by VRM.

Full RADIUS Support (AAA) – Proxy Servers

Application

In all of the examples above, VRM was positioned in between the RADIUS clients and RADIUS server, but VRM can also be positioned so that it can receive proxied requests. In this case, an existing authentication server (supporting RADIUS, TACACS, XTACACS protocol) cannot directly authenticate the user because it cannot verify Digipass tokens. Therefore, it proxies authentication requests to VRM. Upon successful authentication, the authentication server will reply to the NAS with any appropriate authorization attributes and will handle accounting requests.

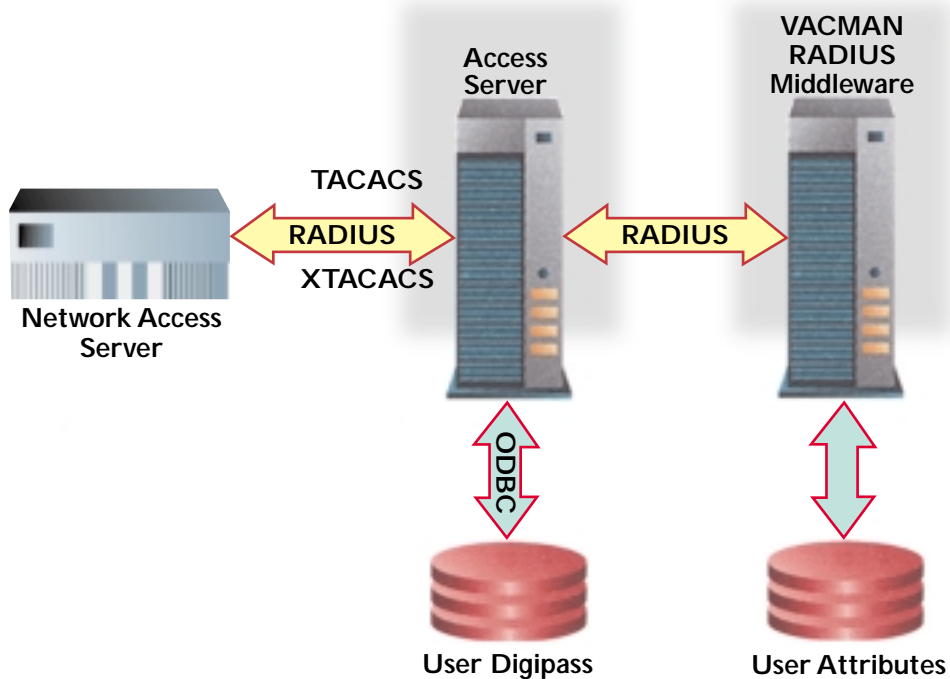


Figure 10. Schematic Overview

System Requirements

CPU	Pentium 350 MHz or above
Memory	<ul style="list-style-type: none">• Minimum of 128 MB, but recommend 256 MB or more• VRM requires 1 KB or RAM (if cached) per 10 user accounts
Hard Drive	<ul style="list-style-type: none">• 100 MB or above• Each user record requires approximately 1 KB of space.• Each token token requires approximately 1.5 KB of space.• Note that the audit logs can consume a lot of hard drive space if there are high number of authentication and administration processing.
O/S	<ul style="list-style-type: none">• Windows NT 4.0 Workstation or Server with patch 4 or above• Windows 2000
Winsock	2.0 or above
ODBC Drive	Microsoft access database driver number 4.00.4403.02. MDAC 2.1 provides this driver and is bundled with the VRM installation CD, and it also can be downloaded from www.microsoft.com .
JAVA Runtime	JAVA Runtime Environment 1.2.2_008. This is bundled in the VRM installation CD, but can also be downloaded from www.sun.com

About VASCO

VASCO secures the enterprise from the mainframe to the Internet with infrastructure solutions that enable secure e-business and e-commerce, protect sensitive information, and safeguard the identity of users. The company's Digipass® and VACMAN® product families offer end-to-end security through strong authentication and electronic signature, true and secure single sign-on, access control, and web portal security, while sharply reducing the time and effort required to deploy and manage security. VASCO's customers include hundreds of financial institutions, blue-chip corporations, and government agencies in more than 50 countries. More information is available at www.vasco.com.

For regional offices or to learn more about us, visit our web site at www.vasco.com



SECURITY BEYOND e-MAGINATION

AMERICAS HQ

VASCO Data Security, Inc.
1901 Meyers Road, Suite 210
Oakbrook Terrace, Illinois 60181, USA
phone: +1.630.932.8844
fax: +1.630.932.8852
e-mail: info_usa@vasco.com

EMEA HQ

VASCO Data Security nv/sa
Koningin Astridlaan 164
B-1780 Wemmel, Belgium
phone: +32.2.456.98.10
fax: +32.2.456.98.20
e-mail: info_europe@vasco.com

APAC HQ

VASCO Data Security Asia-Pacific Pte Ltd.
#15-03 Prudential Tower, 30 Cecil Street
049712 Singapore
phone: +65.232.2727
fax: +65.232.2888
email: info_asia@vasco.com

All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for any infringement of patents or other rights of third parties resulting from its use.