VACMAN®
RADIUS Middleware

Easily Add Strong Authentication To Your Existing Remote Access Solution

Your Firewalls and RADIUS servers solve a lot of problems when it comes to providing remote access to the company's network. Are you concerned that non-authorized users may try to exploit your static passwords to their advantage? Do you want to increase your network protection, promote your users' productivity and do it without replacing or redesigning your remote access solution?

Now, you can. Simply choose VACMAN® RADIUS Middleware – the unique middleware product that enables strong authentication security, based on VASCO Digipass® technology.

Solid Security = Business Value

Remote Access is one of the most valuable – and most vulnerable – areas in a corporate network. Without remote access, productivity can grind to a halt. Consider what would happen, for example, if your sales people, telecommuting employees, or customers lost access to your central database or other network resources. Today, you also can't afford to leave valuable corporate data and systems unprotected. VACMAN RADIUS Middleware is the simple and cost-effective solution to help you positively identify the remote users who are requesting access to your network.

Powered by Digipass

Digipass technology is specifically designed to ensure that remote access doesn't become the weak link in your network security scheme. With a Digipass token in hand, your authorized users will be able to prove that they are who they say they are – quickly and easily. They simply use an individually assigned Digipass token to generate a one-time password and they're in business.

Easy to Integrate

VACMAN RADIUS Middleware makes things easy on the network administrator's end, too. This solution can be used to tighten the security for remote access in ANY RADIUS environment. It's designed to enforce Digipass' strong authentication technology in combination with any RADIUS server. But that's not all: VACMAN Middleware can also serve as a back-end authentication server to any RADIUS enabled firewall application. The secret? VASCO's unique software offers RADIUS-proxying capabilities, in addition to strong support for the RADIUS protocol and Digipass authentication devices.

VASCO

SECURITY BEYOND e-MAGINATION

Completely Compatible

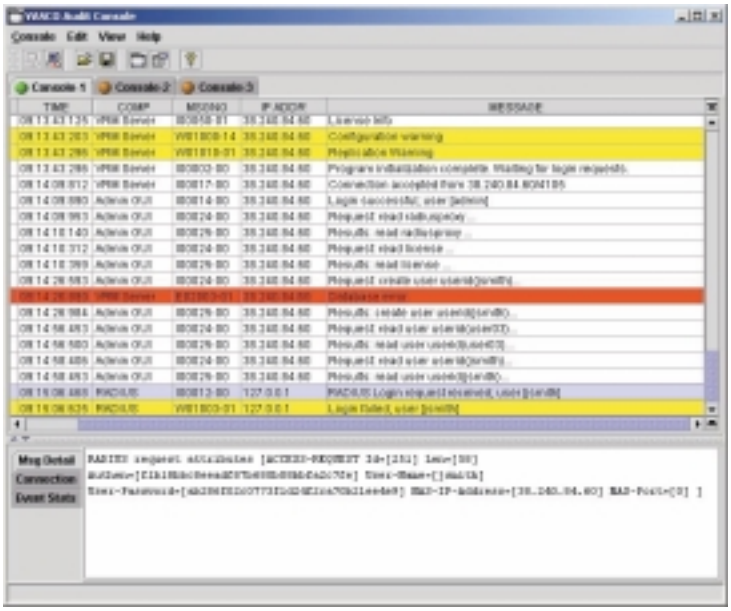

Figure 1: Audit Console

There are no hardware or software conflicts to worry about, because VACMAN Middleware uses a non-intrusive method of enabling Digipass authentication. Simply place VACMAN Middleware between the NAS and your existing RADIUS server – without affecting the performance of either.

Easy to Administer and Audit

VACMAN RADIUS Middleware fits seamlessly into any RADIUS environment without creating new management headaches. A single interface – the VACMAN Middleware Admin GUI (Figure 2) – lets you assign and manage the Digipass tokens you've distributed to authorized users, while automatically handling all strong authentication challenges and responses. This same tool also allows you to configure all the other features of VACMAN Middleware.

Once VACMAN Middleware is installed and configured, you can use the Audit Console to monitor incoming and outgoing RADIUS traffic (or any other events) on the VACMAN Middleware server. The Audit Console (Figure 1) presents all the statistical information you need to manage your remote access environment – providing details on events that have occurred since VACMAN Middleware started running, including:

- connection period
- number of information messages
- warnings
- errors and fatal errors

Both the Admin Graphical User Interface (GUI) and the Audit Console can be run remotely. Both are written in highly portable JAVA Swing-based code to fit future platform support.

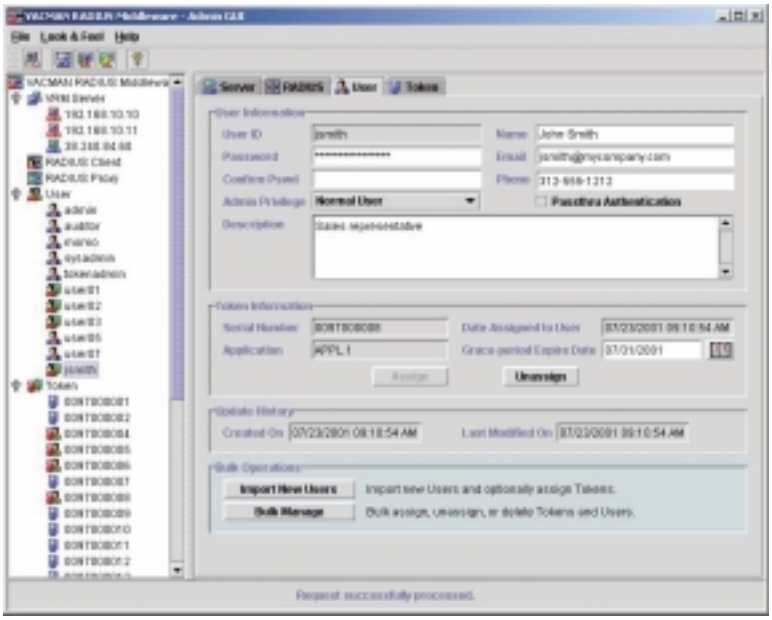

Figure 2: Admin Gui

Auto-Management

The VASCO solution is designed to be easy to administer, whether you're authenticating a few dozen remote users, or tens of thousands. By combining powerful features – such as Dynamic User Registration, Auto Token Assign, and Token Graceperiod – the VACMAN RADIUS Middleware technology automatically manages itself after the initial configuration.

VACMAN Middleware is extremely flexible, giving you many different ways to create users and assign tokens. In addition to the Auto-Management method, the technology allows you to:

- Import users and assign tokens from an input file
- "Bulk assign" users and tokens that have been loaded into the database
- Assign a token based on a user
- Assign a token based on a token
- Use command line interface (CLI) to create users and assign tokens (future)

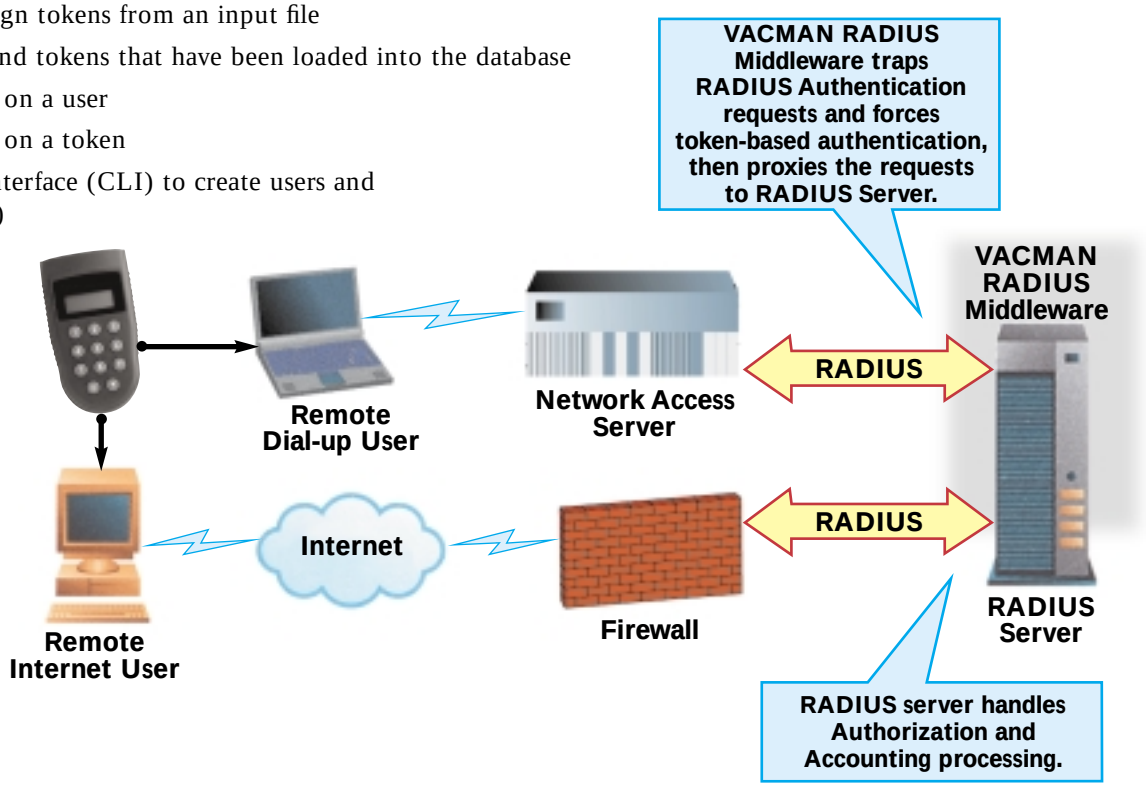

Figure 3: Network View of VACMAN RADIUS Middleware

Why Use VACMAN RADIUS Middleware?

- Strong, two-factor authentication – VACMAN Middleware and Digipass eliminate the weakest link in any security structure, the use of static passwords. It's a turnkey solution that can be up and running in minutes, not hours or weeks.
- Dynamic User Registration (DUR) – Refers to the automatic expansion of the VACMAN Middleware database to include users who are allowed to authenticate to the third party RADIUS Server. DUR creates the user in the database, if not already present, and the third party authenticates the user.
- Autolearn passwords – Automatically learned passwords is a feature that allows static user passwords, assigned to the user on the back-end RADIUS server, to be auto-stored in the database. Upon valid Digipass authentication in VACMAN Middleware, the "autolearned" user password is automatically played to the back-end RADIUS server.
- Token Auto Assign – An unassigned Digipass can automatically be assigned to a new user, whether the user was created by the Admin GUI or DUR. A logfile containing the assignment specific parameters (Serial Number, User-Id, User-Name, etc.) is then created.

VACMAN® RADIUS Middleware

- User Passthru – Digipass and static password authentication are supported simultaneously. Passthru allows a user to be authenticated by the back-end RADIUS server without any treatment on the VACMAN Middleware. This option can be activated globally, even to the user-level.
- Digipass Graceperiod – The user's static password is accepted (for a certain period of time) even when a Digipass has already been assigned. The Grace-period will end after the specified time has expired, OR at the first time the Digipass is used within this period.
- Admin GUI – This can also run from a remote location, and is used for:
  - Digipass management (Import, Assign, Unlock….)
  - User Administration (Create, Delete….)
  - Log-file configurations
  - General configuration settings (proxy, Passthru, TAA….)

Server Platforms Supported:

Windows NT Server 4.0
Windows 2000

SYSTEM REQUIREMENTS

Resource	Recommendation / Requirement
Processor	**CPU speed of Pentium 500MHz or faster is recommended.** **The following conditions increase the load on the CPU:** • **High number of RADIUS authentication/accounting requests** • **RADIUS requests are proxied to RADIUS servers** • **One or more Audit Consoles are active** • **ODBC Auditing is enabled** • **Server debug option is enabled**
Memory	**RAM capacity of 256 MB or greater is recommended.** **The following conditions increase the memory size requirement:** • **User cache is enabled with a large list of users. Every 10 cached users require approximately 1KB of RAM memory** • **Running JAVA based Admin GUI or Audit Console**
Disk Space	**Available disk space of 100 MB or greater is recommended.** **The following conditions increase the disk space requirement:** • **High number of user and token records. Each user and token records occupy approximately 1 KB of disk space** • **Audit log files that are not archived (backed up then deleted from the disk) frequently**
O/S	• **Windows 2000** • **Windows NT Server 4.0 with Service Pack 6 or above** • **Windows NT Workstation 4.0 with Service Pack 6 or above**
Winsock	**Version 2.0 or above**
ODBC Driver	**Microsoft Access database driver version 4.00.4403.02 or above.** **Microsoft Data Access Components (MDAC) 2.1 or later provides this driver and is included in the VRM installation media or can be downloaded from www.microsoft.com.**
JRE	**Version 1.2 or later. JRE is required for running the following JAVA based programs: Admin GUI and Audit Console.** **JRE 1.2 is included in the VRM installation media and it can be also downloaded from java.sun.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