

VACMAN[®] Middleware 3.0

DIGIPASS[®] authentication service middleware

VACMAN Middleware is a software suite for organizations of all sizes that need to authenticate remote users for access to enterprise networks and its applications. This state-of-the art VASCO product is used to verify authentication requests and to centrally administer user authentication policies. VACMAN Middleware and VASCO's DIGIPASS authenticators provides affordable strong authentication and secure access to web applications, business applications and virtual private networks.

You've invested considerable time and energy protecting your network from unauthorized remote users by implementing password based security. Raise your level of protection and eliminate your exposure to password abuse without the costly replacement or redesign of your existing remote access solution. VACMAN Middleware is based on VASCO DIGIPASS technology and provides strong authentication security which can be easily integrated into your current infrastructure.

Remote access is one of the most valuable – and most vulnerable – features in a corporate network. Today you simply cannot afford to leave your systems and valuable corporate data unprotected. VACMAN Middleware is the simple and cost-effective solution to help you authenticate remote users requesting access to your network. Using an individually assigned DIGIPASS authenticator, your remote users will be able to prove their claimed identity quickly and easily through a dynamically generated one-time password.

VACMAN Middleware simplifies things for the network administrator, also. This solution can elevate remote access security in any radius and web environment by enforcing DIGIPASS strong authentication technology. But there's more ... VACMAN Middleware can also provide back-end server authentication for any RADIUS/IIS enabled firewall application.

FUNCTIONS

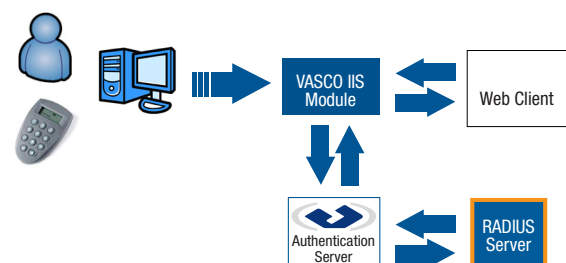
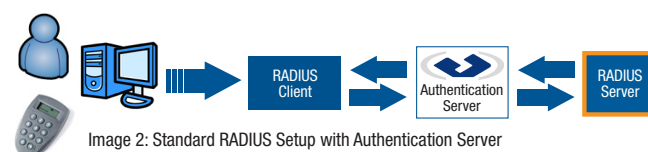
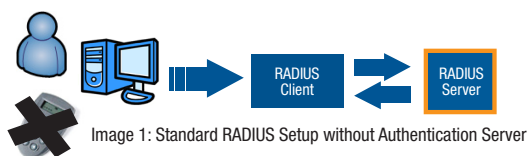
- Verification of authentication requests
- Central administration of users, DIGIPASS authenticators and authentication policies

FEATURES

- Strong DIGIPASS based two-factor authentication
- Support of radius and web server environments
- Policy based authentication
- Bulk management and auto management
- Flexible DIGIPASS assign procedures
- Active directory integration
- ODBC database support
- Dynamic user registration
- Password auto learning
- DIGIPASS authenticator auto assign
- Comprehensive audit system
- Support of multiple authentication server environments

BENEFITS

- Strong authentication without the hassles
- Designed to fit the needs of any size organization
- 'Out-of-the-box' solution
- Easy to integrate, administer and audit
- No software installation on client PCs
- Seamless solution; easy to use
- Extremely low 'total cost of ownership'



Multiple DIGIPASS authentication products may be deployed simultaneously to meet your company's specific requirements



STRONG, TWO FACTOR AUTHENTICATION

The combination of VACMAN Middleware and DIGIPASS authenticators provides a much more reliable form of user authentication than reusable static passwords and can be easily implemented. It's a turnkey solution that can be up and running in hours; not days or weeks.

ACTIVE DIRECTORY INTEGRATION

The main authentication instance in a VACMAN Middleware enabled infrastructure remains the Active Directory service. The storage of the DIGIPASS related data is linked with the users in the Active Directory. This scalable approach provides optimal support for multiple domains and delegated administration.

ODBC COMPLIANT DATABASE SUPPORT

VACMAN Middleware supports ODBC compliant databases, such as Oracle 9i, Microsoft SQL server 2000 and 2005, IBM DB2 8.1, Sybase Adaptive Server Anywhere 9.0 and PostgreSQL 8.0 and 8.1.

VACMAN Middleware comes standard with PostgreSQL.

AUDITING AND REPORTING

The audit console monitors incoming and outgoing radius and web traffic (or any other events) on the VACMAN Middleware server. Informational statistics gathered by the audit console provide critical details necessary to easily manage your remote access environment including:

- Connection period
- Number of information messages
- Warnings
- Errors and fatal

INTEROPERABILITY

Hardware or software conflicts are not a concern as VACMAN Middleware uses a non-intrusive method of enabling DIGIPASS authentication. Simply position VACMAN Middleware between the Network Access Server and your existing radius server; the performance will be unaffected.

COMPLIANCE TO STANDARDS

RADIUS

- RFC 2865 and 2866

AUTHENTICATION

- DIGIPASS
- OATH

SYSTEM REQUIREMENTS

OPERATING SYSTEM

- Windows 2000 with SP4 or above
- Windows XP Professional (32bit version only) with SP 2 and above
- Windows Server 2003 (32bit version only) with SP 1 and above

PROCESSOR

- Pentium 600 MHz or faster (2 GHz recommended)

The following conditions may increase the load of the CPU:

- High number of RADIUS authentication / accounting requests
- RADIUS request proxied to RADIUS server
- One or more audit consoles active
- ODBC auditing enabled
- Server debug option enabled

MEMORY

- RAM capacity of 512 MByte or greater recommended

Following conditions may increase memory size requirements:

- User cache enabled with a large number of users to be cached
- JAVA based Admin GUI or Audit Console active

DISK SPACE

- Disk space of 200 MB free space or greater
- Recommended at least 500 MB free space

The following conditions may increase disk space requirements:

- High number of user and token records
- For authentication rates of hundreds or more per day, allow additional disk space for audit logs

NETWORK CARD

- Minimum 100 Mb

WINSOCK

- Version 2.0 or above

About VASCO

VASCO designs, develops and supports patented "Strong User Authentication" products for the financial world, secure network access, e-business and e-commerce. VASCO's user authentication technology is carried by the end-user on its DIGIPASS products which exist in hard & software format.

At the server side, VASCO's VACMAN products guarantee that only the designated DIGIPASS user gets access to the application. VASCO's target markets are the applications and their several hundred million users using fixed password as security. VASCO's time-based system generates e-signatures and a "one-time" password that changes with every use, and is virtually impossible to hack or break. With tens of million of DIGIPASS products sold, VASCO has established itself as a world leader in strong authentication for e-banking and for network access for blue-chip corporations and governments worldwide.

WWW.VASCO.COM

	<p>Belgium (Brussels) phone: +32.2.609.97.00 email: info_europe@vasco.com</p>	<p>The Netherlands ('s-Hertogenbosch) phone: +31 73 691 88 88 email: info_europe@vasco.com</p>	<p>USA (Boston) phone: +1 508.366.3400 email: info_usa@vasco.com</p>
	<p>Australia (Sydney) phone: +61 2 8920 9666 email: info_australia@vasco.com</p>	<p>Singapore (Singapore) phone: +65 6323 0906 email: info_asia@vasco.com</p>	<p>China (Shanghai) phone: +86 21 6443 2697 email: info_asia@vasco.com</p>