Securing the Web with VACMAN® Enterprise

White Paper

SECURITY BEYOND e-MAGINATION

Securing the Web with VACMAN® Enterprise

Contents

Securing the Web with VACMAN® Enterprise

Web Security Challenges

Today's web security solutions must fulfill a basic function: They must make it easy for legitimate users to get the information they want, or to use the applications they need, while denying access to unauthorized users. But the best web security solution should also do more: it should deliver a positive user experience and make the web site easier to deploy, control, and manage.

Initially, "web security" was not considered a priority, because the web was designed to provide unfettered access to information – a simple, open, easy way to share data. The earliest web sites were open to all. Every user had the same access privileges. Any user with a browser could connect to any web server and make URL requests.

Second-generation web sites made it possible to host information more securely. Native web server tools could be used to constrain user access to documents and applications hosted on the web server, with constraints based on the IP address of the connecting machine.

Today, however, web portals must provide a much higher level of security. The reason? Many third-generation web sites host applications that have deep links into organizational processes and content. The portals also perform critical business functions, such as customer acquisition, customer retention, and customer relations. They play an essential role in boosting a company's efficiency, and increasing bottom line profits. With this increased level of sophistication, demands for web portal security have grown.

Third-generation web sites require an enterprise-class security solution that can provide or enable:

- **Strong security** – driven by user identity
- **Ease of use** – reducing or eliminating the need for repeated authentications, as authorized users move from application to application on the web site
- **A personalized user experience** – tailoring web site options and application responses to each user's profile or preferences

- **Manageability** – allowing delegated security, user account management, and other functions which let users manage aspects of their own accounts
- **Integration** – incorporating VACMAN Enterprise within the broader enterprise security context so that web sites do not become islands of security, requiring specialized knowledge and staff to secure them

The VACMAN Enterprise Solution

VACMAN Enterprise is an enterprise-class security solution, designed specifically for third-generation web sites and applications. Beyond providing "security for the web," or "single sign-on for the web," VACMAN Enterprise delivers a comprehensive solution that lets you deploy and manage web sites and enterprise portals ***as part of your overall security infrastructure.*** VACMAN Enterprise makes it possible to deploy a security solution with consistent policies and practices across all user-accessible network resources. It addresses all the most critical technical issues organizations face in securing their web sites and web portals – including:

Establishing user identity

VACMAN Enterprise can authenticate users through a wide variety of methods – digital certificates and smart cards, digital token devices, username / password and more. This flexibility lets you adjust the level of security based on the application involved. In addition, VACMAN Enterprise provides fine-grain access control over authenticated users, to ensure that users are given access only to the applications and data they are authorized to see.

Single sign-on

With the start of each session, VACMAN Enterprise grants authenticated users a secure, encrypted, digitally-signed enterprise credential which can then be used to provide access to any application within the VACMAN Enterprise framework – web or otherwise. This feature eliminates annoying requests for repeated authentication, as authorized users move from one application to another – greatly enhancing the user experience.

Web site personalization

VACMAN Enterprise helps you build strong one-to-one relationships with web users by securely passing user-specific information along to the applications they are authorized to use. This information can then be used by the application to customize its responses for each user. There's no need to retool or reprogram target applications to provide these personalization capabilities.

Dynamic user registration

Busy web sites often serve hundreds of thousands of active users or accounts. That can create an overwhelming management challenge – how to initiate and manage accounts for all those users, and keep them secure. VACMAN Enterprise tackles this challenge through Dynamic User Registration – a feature which enables authenticated users to self-register into the security framework, and then to self-manage many aspects of their account, including password recovery.

Integration with the corporate security infrastructure

VACMAN Enterprise is designed to protect your investment in legacy applications and in LDAP directory services. It can use existing LDAP directories without requiring changes to directory schemas. In addition, VACMAN Enterprise components can be installed to ensure that communications are encrypted end-to-end, from the user's browser (using the browser's native secure sockets layer support), to the web server, all the way to back-end application servers or other data sources.

VACMAN Enterprise Benefits

If your web site provides a window into corporate processes and information, it's smart to make the glass bulletproof. VACMAN Enterprise delivers – by providing the highest levels of security, without any of the application programming or modification required by other security products. With VACMAN Enterprise, your customers can be assured that their transactions and personal information are secure and confidential. VACMAN Enterprise provides configurable, full encryption of both communications and stored data, to protect the privacy and integrity of information.

The VACMAN Enterprise security solution delivers several key features and benefits, including:

- **Rapid deployment** to thousands of users through Dynamic User Registration technology
- **A scalable infrastructure** that can grow as your organization and security requirements change
- **High availability** – supported by replication and automatic fail-over technologies

- **Increased customer satisfaction** – by making it possible to personalize the web site experience, and by making it easier for authorized users to get the applications and files they need, regardless of the platform hosting the resources
- **Tighter security with less effort** – when you use VACMAN Enterprise to uniformly enforce security policies and rules throughout the enterprise
- **Reduced costs** – through account management features such as automated password recovery and user self-management of select aspects of their accounts
- Maximized return on investment – by allowing you to leverage existing resources, such as LDAP user directories, and by making it simple to deploy a comprehensive security infrastructure that can incorporate new access control and authentication mechanisms as your needs change
- **Increased user trust** – by providing tools to ensure data privacy and integrity

VACMAN Enterprise Technical Overview

VACMAN Enterprise is designed as a security plug-in for Netscape and Microsoft IIS web servers. This architecture simplifies deployment of the security solution. As a server-side only plug-in to the web server, VACMAN Enterprise does not remove, replace, or modify the web server's proprietary API. In addition, no software is required on the client desktop beyond a web browser (Note: The browser must be configured to accept cookies in order for VACMAN Enterprise to function properly).

With VACMAN Enterprise, you can secure all existing web-based applications, whether two-tier, three-tier, or multi-tier. VACMAN Enterprise gives you the ability to define security rules that govern access – both to individual resources on a machine (connection rules), and to individual objects maintained by those resources (object rules). Included in the security rules are constraints on:

- Who may gain access (identity specifications)
- The hosts from which access may be gained (location specifications)
- The periods during which access may be granted (time specifications)

VACMAN Enterprise maintains these rules in a distributed "master rule" database. In addition to the master rule database, VACMAN Enterprise uses a Security Repository, and a set of configuration files, to maintain information about a hierarchy of users, policies, groups, roles, and hosts. VACMAN Enterprise also provides transparent access to – and storage of – information in LDAP databases.

VACMAN Enterprise Web Architecture

The VACMAN Enterprise web plug-in is always installed on the web server it secures. The plug-in works in conjunction with other elements of the VACMAN Enterprise security framework to provide a full range of security features and functions.

Key elements of the security framework include:

VACMAN Enterprise Cell: A grouping of VACMAN Enterprise Servers, sharing a VACMAN Enterprise Security Repository, and controlled by a single VACMAN Enterprise host.

VACMAN Enterprise Security Repository: A repository of information about users, groups, hosts, and domains within a VACMAN Enterprise cell. The Repository uses a two-tier approach, combining LDAP user directories with its own encrypted and highly secure store of the environment's most sensitive elements. Although a cell may contain multiple copies of the Security Repository for replication, fail-over, and high availability, there is only one logical Repository in a cell. The Repository supports a highly flexible and granular internal security system that easily handles auditing and other management functions.

Authorization Server: A VACMAN Enterprise server that provides security services to one or more VACMAN Enterprise web plug-ins upon request. The Authorization Server authorizes (or refuses to authorize) both HTTP connections to the web server secured by the plug-in, and access to URLs and HTTP operations on the web server. The Authorization Server also gives the plug-in access to the Security Repository, to external authentication systems, and to other services such as LDAP databases and certificate authorities. Because the state of each client connection is stored in cookies, VACMAN Enterprise Web may be configured to use multiple Authorization Servers – to provide for load balancing and automatic fail-over.

VACMAN Enterprise Master Server, or Master: Houses the master rule database and configuration files for the local cell.

VACMAN Enterprise Console: The graphical user interface through which authorized VACMAN Enterprise administrators can access and manage the security framework.

VACMAN Enterprise Backup Server: The Backup Server can become the Master Server in the event that the primary Master fails or becomes unavailable. The VACMAN Enterprise Console on a VACMAN Enterprise Backup Server has remote read-only access to the master rule database and configuration files. However, it may acquire the lock necessary to write to these resources if the Master Console is not running on the Master host.

VACMAN Enterprise Slave Server: A VACMAN Enterprise Authorization Server that is limited to the creation and maintenance of object rules for the local host only. Each Slave Server maintains a read-only copy of the connection rules and its own set of local object rules.

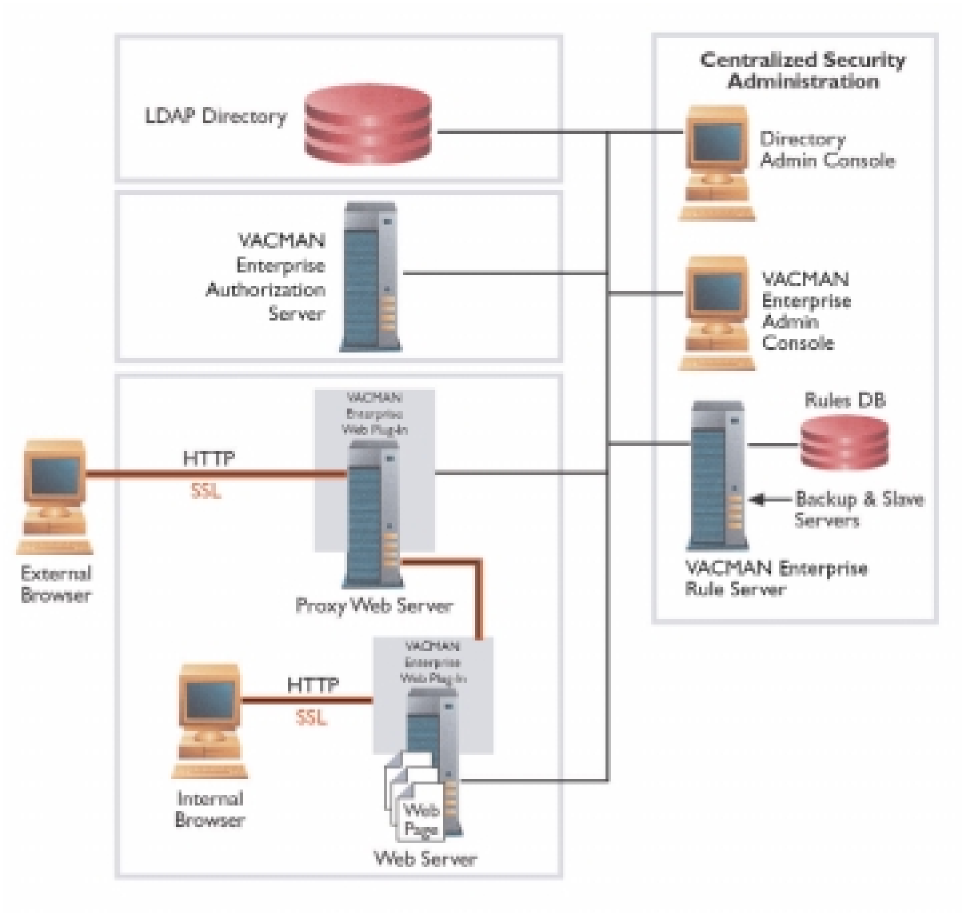

LDAP Directory
Centralized Security Administration
Directory Admin Console
VACMAN Enterprise Authorization Server
VACMAN Enterprise Admin Console
Rules DB
VACMAN Enterprise Web Plug-In
HTTP
SSL
Backup & Slave Servers
External Browser
Proxy Web Server
VACMAN Enterprise Rule Server
VACMAN Enterprise Web Plug-In
HTTP
SSL
Internal Browser
Web Page
Web Server

Figure 1.VACMAN Enterprise security architecture.

Web Access via the VACMAN Enterprise web plug-in

The VACMAN Enterprise web plug-in communicates with one or more VACMAN Enterprise Authorization Servers to mediate all HTTP interactions between each client and the web server – calling on VACMAN Enterprise for the security functions specified by the security administrator.

When users request a target on a web server protected with the VACMAN Enterprise web plug-in, they must provide the authentication specified in VACMAN Enterprise. Once authenticated, users are automatically logged into VACMAN Enterprise, and gain access to their individual user accounts in the VACMAN Enterprise Repository. This authentication and login process takes place ***before*** the original URL request (the one that led to the authentication challenge) is evaluated for authorization. Once identity is established through authentication and login, the user receives full identity and credentials (in the form of an encrypted and signed cookie) within the VACMAN Enterprise cell.

The user's VACMAN Enterprise identity and credentials are then used to determine that user's rights and privileges throughout the system's resources. VACMAN Enterprise evaluates the identity-based rules contained in the Security Repository and in the master rule database – and access is granted or denied accordingly.

Addressing Web Security Issues

The VACMAN Enterprise security framework can provide much more than a solution for basic authentication and authorization. If desired, the VACMAN Enterprise framework can be configured to provide Dynamic User Registration, secure single sign-on, and other valuable features.

Establishing User Identity – Authentication

Authentication is the process by which VACMAN Enterprise verifies the identity of a user requesting a protected target on a web server running the VACMAN Enterprise web plug-in. This illustration outlines the initial authentication process:

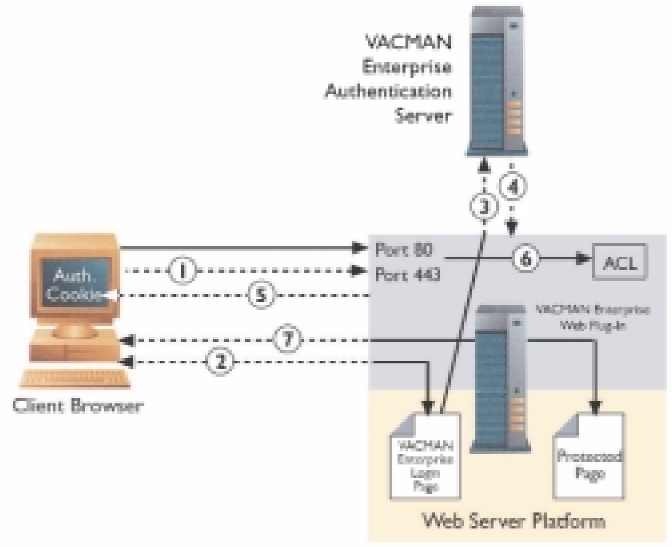


Figure 2. The process of an unauthenticated user trying to access a web page (or object) protected by the VACMAN Enterprises web plug-in.

1. A user launches a browser connection to a web server on Port 80 (HTTP) or Port 443 (HTTPS).
2. If the requested web page is protected, and if the user has not previously logged in (i.e., VACMAN Enterprise detects no valid cookie), the user is redirected to a secure login page which requests a login ID and a password (or other authentication methods, as configured by the system administrator).
3. The user ID and password are compared to data in the VACMAN Enterprise Authentication Server or to any designated external authentication source (LDAP, for example).
4. The Authentication Server returns a network-wide credential to the VACMAN Enterprise web plug-in.
5. The VACMAN Enterprise web plug-in sends a cookie to the client browser along with a redirect to the page originally requested. The cookie contains the cached user identity (no attributes), and is cryptographically sealed. The cookie can be linked to a specific client or to range of IP addresses. It can also be conveyed within an SSL session if needed.

6. The original user request is validated by the VACMAN Enterprise web plug-in, and may also be compared against a list of VACMAN Enterprise-protected URLs.

Multiple Authentication Mechanisms

VACMAN Enterprise integrates easily into web environments where multiple authentication mechanisms are in use. VACMAN Enterprise can unite the different authentication mechanisms used within an organization (both current and future), by mapping a successful authentication sequence to the user's global VACMAN Enterprise account and identity. This single network identity (or credential) is digitally signed and cannot be forged. It forms the basis for access to any VACMAN Enterprise-protected application or file.

Users can be authenticated to VACMAN Enterprise through a number of widely-used security mechanisms:

- VACMAN Enterprise password login
- X.509 digital certificate
- NT Domain
- UNIX
- RADIUS
- LDAP server
- RACF
- Tokens

VACMAN Enterprise password login (and all external authentication mechanisms except digital certificate) requires form-based authentication. The user follows the same process, regardless of which authentication mechanism is employed.

Speeding Deployment – Dynamic User Registration

Dynamic User Registration (DUR) lets you minimize the time-consuming (and often prohibitively expensive) process of installing security software and creating and managing user accounts. The DUR technology allows for the centralized configuration of policies and security information required for account creation and password management.

Through DUR, any web user can perform self-registration – that is, create an authorized account – quickly and easily. In some cases, it may be desirable to allow new users (e.g., those who do not have accounts in the Repository) to create individual accounts when they first contact the web server. For example, for a first transaction, you many want to allow customers to obtain a VACMAN Enterprise identity without administrative intervention. DUR can make it happen, simply and securely.

DUR can also be used to manage the account migration process for existing users who have a verifiable identity (e.g., an account or other information) within a legacy system. DUR can be used to create corresponding local accounts throughout the enterprise on NT, RACF, UNIX, database, or other target systems. In addition, the user can be issued an X.509 certificate, if desired.

DUR works by obtaining certain information from each connecting user (which may be used for record-keeping, verification, or for any purpose at all) – along with the username and password for the new account. Once the information is collected and verified, the new account is created, according to the characteristics and restrictions set by the VACMAN Enterprise Administrator. Any privileges associated with the new account can be managed in a variety of ways: They can be based on information provided by the registrant; on settings configured by the administrator; or on information gathered in a custom workflow arrangement implemented by the administrator.

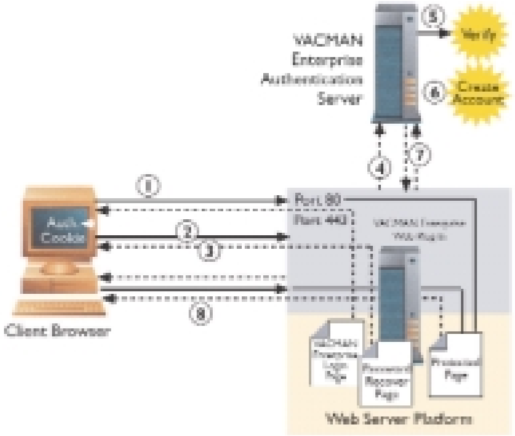


Figure 3. Dynamic User Registration.

1. When the browser connects to a protected resource (web page), the user is redirected to a secure login page which requests the user login ID and a password, or presents an opportunity to register.
2. The user selects the register option.
3. A form is returned to the user, asking for information that can be electronically verified along with the account name and new password.
4. The information supplied by the user (other than the password – e.g., mother's maiden name) is sent to the Authentication Server for verification.
5. The Authentication Server runs a customer-provided verification program.
6. If verification is successful, the Authentication Server may initiate account creation on one or more targets; may create host accounts; may create directory entries, etc.
7. The user is logged in and cookies are created.
8. Cookies are returned to the browser, which is re-directed to the original URL.

When a form-based authentication mechanism is in use, and DUR is enabled, any connecting user can be authenticated by creating and logging into a new VACMAN Enterprise account. Therefore, a verification script must be used to check the account name and password (or the registration information provided) against some external source before creating the new account.

A similar process is followed when X.509 certificate authentication is in use. If users authenticate by presenting a valid certificate that is not mapped to an existing account, they can then use DUR to create a new account to log into. Once the new account is created, the certificate used for authentication is automatically mapped to the new account until one or the other expires, or until the user chooses to destroy the mapping.

User registration information is also collected from users who must enable an existing VACMAN Enterprise account (Mandatory Account Enablement), or who want to reset the forgotten password of an existing account (Password Reset).

Easing Management Burdens – Mandatory Account Enablement (MAE)

The VACMAN Enterprise administrator may create a large number of new VACMAN Enterprise accounts at one time. Typically, this is done through a bulk import from an existing file into the VACMAN Enterprise Repository. However, other methods for bulk account creation are also available.

Usually, when computer accounts are created, the administrator provides the initial password, along with instructions to change it immediately. This process allows new users to log into the account the first time, and establish a secure password, with minimal assistance from the administrator.

However, when large numbers of accounts are created, it can be inconvenient to generate unique initial passwords and communicate them to all the users involved. On the other hand, if one widely-known initial password is used, it can create a security breach: If a user forgets to change his password on first use, or does not immediately use the account, anyone who knows the published initial password can use it to access the user's account.

VACMAN Enterprise addresses this issue through Mandatory Account Enablement (MAE). With MAE, users are required to complete two tasks when first logging into a new account: They must change the password (from the published initial password, to a secret individual one); and they must enter information in the required registration fields. The verification script then processes the registration information, thereby establishing the user’s authorization to access the account and change the password. Note that both tasks must be completed: the account cannot be used for login until the verification process takes place, and the password has been changed.

MAE also provides an opportunity to collect valuable information from users, even when a password change is not required. Say, for example, a number of user accounts are imported into the Repository with existing secret passwords intact. To learn the users e-mail addresses, the administrator can simply set mandatory enablement for the accounts, specifying “e-mail address” as a required field for registration. Then, when the users log in for the first time, they can be asked to provide a valid e-mail address as part of the account enablement process, rather than requiring them to re-set their established passwords.

MAE can be used to solve other administrative issues, too. For example, suppose that a group of RACF users is imported into the VACMAN Enterprise Repository. Their RACF passwords are not known to the administrator, and cannot be obtained in clear text. The MAE feature can be used to capture the passwords, and apply them to the new VACMAN Enterprise accounts. Here's how: The new VACMAN Enterprise accounts are assigned a hidden, unpublished password that is automatically provided by the login page. Then, when the users attempt to log in, the MAE feature requires them to register – including a request for the RACF password. This password is used to validate the user, and thereafter becomes the new password for the VACMAN Enterprise account.

Reducing Help Desk Costs – Password Reset

From time to time, web users may forget their passwords – a situation which is costly and time-consuming for the administrator to resolve. On the other hand, a security breach can be created if the administrator makes it possible for users to select new passwords without first entering the old ones.

VACMAN Enterprise tackles this challenge with a Password Reset feature. It allows users to select new passwords without entering existing passwords – but only if the users are also able to enter verifiable information in the mandatory fields of the registration form. The verification script then processes this information, to ensure that the user changing the password is in fact authorized to use the account.

Many sites collect information during the DUR and account enablement process, specifically to enable the password reset function. Typically, a user can select a security question such as "What is your mother's maiden name?" thereby providing a key that is difficult for unauthorized users to guess. This information can then be stored with the user's account in the Security Repository – and later, it can be collected from the user during the password reset process, as part of the verification procedure.

Controlling Access to Resources – Authorization

To simplify the creation, application, and management of rules governing connections and access to web server resources, VACMAN Enterprise organizes protected web servers into a simple hierarchy – consisting of cells, security domains, and hosts.

A VACMAN Enterprise **cell** is a grouping of VACMAN Enterprise protected devices, sharing a VACMAN Enterprise Security Repository and controlled by a single VACMAN Enterprise host. A **domain** is a logical grouping of VACMAN Enterprise-protected devices within a VACMAN Enterprise cell. A VACMAN Enterprise **host** is any machine that is running a VACMAN Enterprise Server.

VACMAN Enterprise user populations also are arranged into a hierarchy – segmented by roles, groups, and users.

A **user** is any individual making use of resources within the secured web environment. An authenticated, registered user has full privileges within the VACMAN Enterprise cell. A user **account** is an object in the Security Repository that identifies a user within the VACMAN Enterprise cell and controls many aspects of the user's activities. A **group** is an object in the Security Repository representing a collection of user accounts and conferring defined privileges on its members. Each user account must belong to a primary group, and can belong to an unlimited number of other sub-groups. A **role** is a collection of users and groups created to simplify authorization by sharing access privileges.

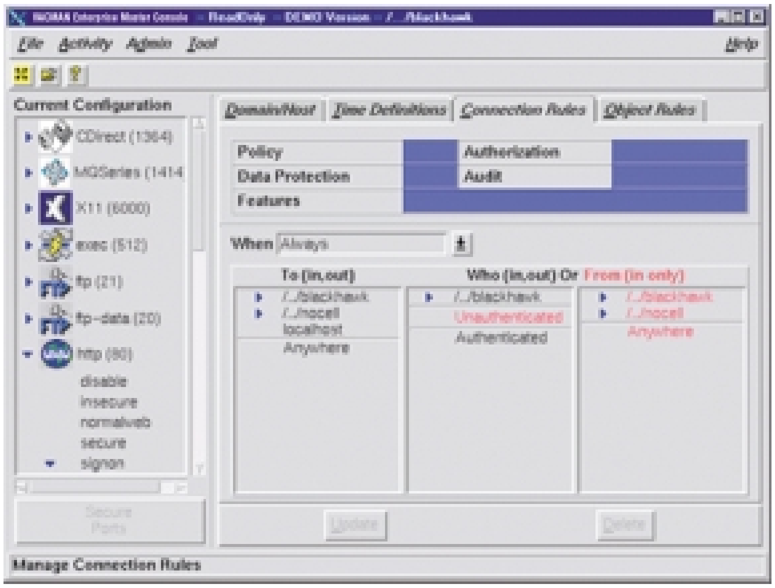
Rule Inheritance

Because VACMAN Enterprise supports a hierarchical naming and management system, an entire hierarchy of entities (a web server file system, for example, or an entire domain of web servers) can be protected with one set of rules at the top level of the system. Each subsequent level inherits rules from its closest ancestor in the hierarchy. VACMAN Enterprise supports such hierarchies when determining user access rights, object access rights, and machine / application access rights.

Connection Rules

Rules governing rights to connect to web servers (connection rules) can be defined for any level: cell, domain, or host. The most specific rule that applies is the one that is enforced (Example: A rule allowing a connection to a specific host for a given user supercedes a rule specified at the domain level denying connections for that user to machines in that domain).

VACMAN Enterprise uses connection rules to define the machines, identities, and time periods that can be used to access resources protected by VACMAN Enterprise. It also uses connection rules to define the properties that control the access to those servers and resources. Connection rules are applied by port number, and are configured in much the same way as packet filter rules are configured on a firewall — with one significant difference. Generally, firewall rules are stored and applied at only one central access point. In contrast, VACMAN Enterprise connection rules are ***managed*** centrally, but the rules databases are distributed to all VACMAN Enterprise authorization servers, which hold read-only copies for evaluating their own connection requests.



Policy	Authorization
Data Protection	Audit
Features	

When: Always

To (in,out)	Who (in,out) Or	From (in only)
/../blackhawk /../nocell localhost Anywhere	/../blackhawk Unauthenticated Authenticated	/../blackhawk /../nocell Anywhere

Figure 4. Connection rule editor.

Fine-grained Access Control

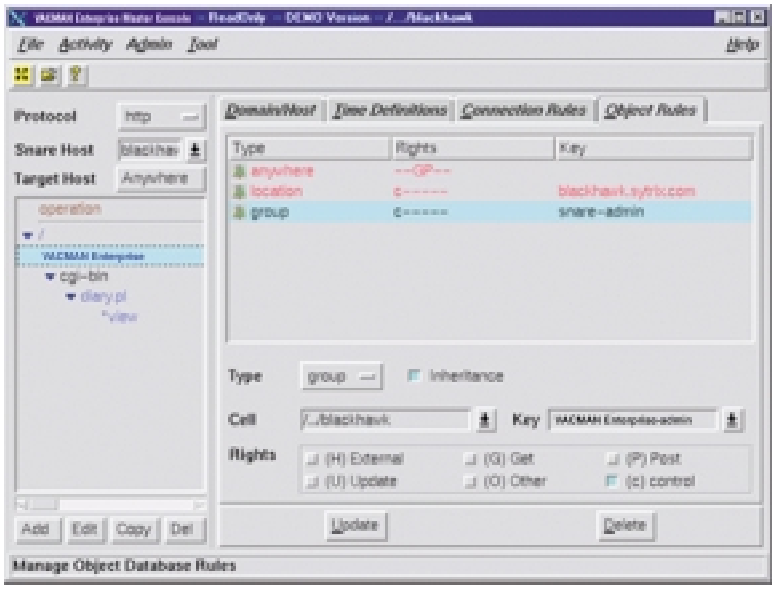
Users can be denied access to specific HTTP objects, such as URLs or directories, based on their VACMAN Enterprise identity or connecting location. In addition, users can be prevented from performing HTTP operations such as GET, POST, and PUT. VACMAN Enterprise can even secure URL requests that POST specific information from the user, thereby controlling the user's ability to make selections and respond to forms within an application.

Object Rules

A higher degree of access control is achieved through the use of VACMAN Enterprise object rules. Object rules govern access down to the level of a single object or transaction.

They control not only who is given access and when, but also what operations can be performed on the object (e.g., read, write, GET, POST, etc.). Object-type rules can also be applied in VACMAN Enterprise as Inheritance rules, simplifying the administration of access control.

The Inheritance feature makes it possible for a single access rule at the top of an object hierarchy (e.g., the root of a web server document directory) to automatically protect all directories and files lower in the hierarchy. However, rules placed on objects ***lower*** in the hierarchy can override any higher-level rules, since VACMAN Enterprise applies rules in order of most-specific to least-specific. Therefore, a rule could be set on a specific page allowing only administrators to view certain types of data. When non-admin users attempt to access this page or data item, they would be rejected when the specific rule for that object is evaluated. All pages above the requested URL would be open to all users (assuming that the root inheritance rule permits such access).



Protocol: http
Snare Host: blackhav
Target Host: Anywhere

operation
/
VACMAN Enterprise
cgi-bin
diary.pl
*view

Type	Rights	Key
anywhere	--GP--	
location	c------	blackhawk.syfrix.com
group	c------	snare-admin

Type: group ☑ Inheritance
Cell: /.../blackhawk Key: VACMAN Enterprise-admin
Rights: □ (H) External □ (G) Get □ (P) Post □ (U) Update □ (O) Other ☑ (c) control

Figure 5. Object rule editor.

Object Rule Transformations

Object Rule Transformations (or “transforms”) let you manipulate the browser/server data stream and perform special processing when a specific URL is requested. This is all accomplished without programming – a feature unique to VACMAN Enterprise among authentication and access control products.

Using transforms, you can:

- Change requested URLs (targets / destinations)
- Automatically fill out and POST forms (usually to perform transparent form-based login, including cookie management)
- Set and reset web server environment variables based on user profile information or using access control lists
- Set session time limits for requested targets
- Access user profile information stored in LDAP or the Repository by setting or adjusting HTTP headers, query strings or even POSTed data (as if simulating hidden fields)
- Automatically store information presented by the user (in an HTTP data stream such as an HTTP form) into the VACMAN Enterprise Security Repository or an LDAP database
- Rescind authentication status based on the need to perform secondary or additional authentication
- Automatically sign forms using certificates or tokens
- Specify explicit data, or use data derived from user information, either in the Security Repository or an LDAP-accessible directory, whenever information is inserted, replaced, or appended

The powerful combination of connection and object rules – including identity, location and time specifications, hierarchical rule evaluation, and strong authentication and encryption – lets you implement the security requirements of an entire enterprise with virtually no limitations.

Personalization

VACMAN Enterprise makes it possible to fine-tune access control and tailor application responses based on user profile information. When enabled, VACMAN Enterprise will:

- Securely pass user profile information to web applications
- Process user-submitted information before it is passed to its target application
- Shape application responses before passing them back to the user

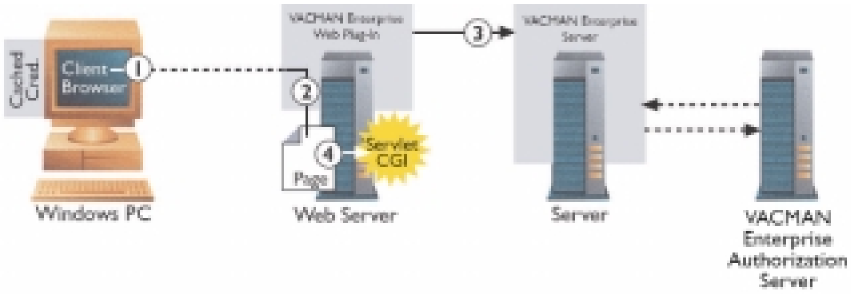


Figure 6. VACMAN Enterprise access control. 1) User's browser conducts a transaction which requires information to be sent by the middle tier to the application. 2) The VACMAN Enterprise plug-in can notify the CGI of user rights. 3) The plug-in can deny browser operations. 4) The plug-in can provide the user's credentials so that a servlet can make its own access control decisions or use the VACMAN Enterprise API to evaluate access control status.

Here are two examples showing how the personalization available through VACMAN Enterprise might enhance the user experience and / or system performance:

- You could provide a "live ticker" to account holders with more than $100,000 balance who have performed trades within the last month totaling more than $25,000
- You could determine if Bob Stanley, an Assistant Manager, is authorized to perform an international fund transfer from account 13579-1 to account 24680-1 for $1,000,000 on a legal holiday in the UK

VACMAN Enterprise access control provides for:

- Controlled access
- Multiple authentication methods
- Replicated authorization for load balancing, availability, and fail-over
- Single point of administration
- Flexible policy engine
- Personalization of content

Consistent Security Policies

A **policy** in VACMAN Enterprise is an object in the Security Repository containing a variety of settings that control the behavior of user accounts, such as password, account, and login restrictions. Once specified in VACMAN Enterprise, these policies are applied consistently throughout your web environments.

Password restrictions include lifespan, expiration date, minimum length, uniqueness, password age and history, and reminder of password expiration.

Account restrictions include lifespan, account idle, and idle activity.

Login restrictions include the time frame during which use of the account is permitted, as well as the number of invalid login attempts before rejection, or if unlimited login attempts are allowed.

Ensuring a Positive User Experience – Secure Single Sign-On

The VACMAN Enterprise secure single sign-on (SSSO) feature greatly enhances the web users' experience by allowing them to gain access to ***all*** the applications and data they are authorized to use with only a single log-on to the web site. VACMAN Enterprise SSSO encrypts all sign-on functions and network traffic. It securely stores and manages all passwords, even generating random passwords known only to the system, effectively taking the security burden off users, and eliminating password management burdens for Help Desk personnel. Beyond increased user satisfaction, the benefits of SSSO include enhanced productivity, improved security, and reduced costs.

Single Sign-On Credentials

Through authentication and registration to a VACMAN Enterprise Authorization Server, VACMAN Enterprise gives users a single enterprise identity. This identity allows them to be transparently logged in (re-authenticated) to all applications and hosts as required during the browser session, without transmitting unencrypted password information and without the user ever seeing login forms or authentication boxes.

Cookies as Credentials

Here's how it works: VACMAN Enterprise supplies the user's browser with a PAG (Process Authorization Group) cookie after authentication and login. This cookie contains the issuing (authenticating) authorization server's file-based (cached) credentials. Its contents are:

identifier@username@server_IP_address@encrypted_hash

The contents of this sequence are as follows, “identifier” is an 8-digit string identifying the credentials as stored on the server, “username” is the name of the VACMAN Enterprise account to which the user is logged in, “server_IP_address” is the IP address of the authorization server issuing the cookie, and “encrypted_hash” is a code derived from an MD5 hash of the IP address of the client on which the browser is running. This encrypted hash is critical: the cookie becomes invalid if it is stolen from its original machine and loaded onto another.

The PAG cookie is scoped to the DNS domain of the issuing server, with path set to / (root). Anonymous users, although not authenticated, do receive a PAG cookie, in which identifier is set to “00000000” and username is set to “anonymous”. The anonymous PAG cookie expires one hour after it is issued.

Credential (cookie) Expiration

The cookie issued by VACMAN Enterprise can be provided on either a per-session or persistent basis, depending on the web server configuration. If a per-session cookie is issued, it is held in memory by the client’s browser, but is not written to disk. It is therefore deleted when the browser session is terminated. If a persistent cookie is issued, it is written to disk by the client’s browser, and therefore exists beyond the end of the browser session. The VACMAN Enterprise administrator determines the lifespan of the credentials issued by the system. Either type of cookie (per-session or persistent) is always discarded when an object rule transformation forces logout, or when the user logs out.

Support for Multi-tier and Cross-domain Web Applications

Within multi-tier applications, VACMAN Enterprise can delegate credentials on the user’s behalf – both within the web server environment and beyond it (through outbound connections) for other purposes such as database access or remote file system access.

Once the user is authenticated, VACMAN Enterprise delegates the user credentials to CGI environments, as well as to NSAPI or ISAPI requests. The web server can use the user’s credentials in all authorization decisions. The cookie (and the associated user credential) is valid across all VACMAN Enterprise-protected web servers. When used with other VACMAN Enterprise products, these credentials can be passed securely to other components of the transaction. The same is true for web servers running in different, non-related DNS domains.

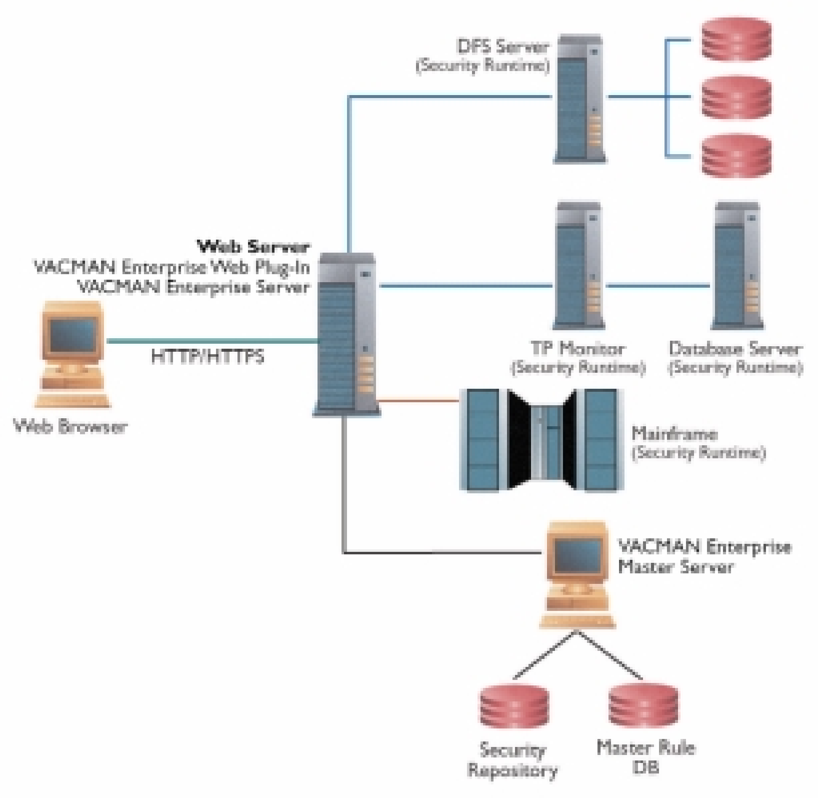


Figure 7. VACMAN Enterprise in a multi-tier environment.

To implement comprehensive SSSO, all applications that require authentication must accept the original authentication information, or other information made available with it, as proof of identity.

The ability to integrate other applications into a single sign-on system that distributes authentication information is key to achieving truly global secure single sign-on. VACMAN Enterprise achieves this goal without introducing any new application interfaces – and in most cases, without any programming! To do this, VACMAN Enterprises creates object rule transformations that instruct the plug-in to perform automatic login, or to provide other profile information to applications running on the web server.

Ensuring Privacy – Encryption

VACMAN Enterprise can actually boost your business, because a fully configurable, end-to-end encryption tool will boost customer / user confidence in your web site and encourage repeat visits.

To ensure bulletproof security, all VACMAN Enterprise internal databases are encrypted. Transmission of data from the front-end web servers to the back-end target application or database servers can be encrypted as well – via the installation of VACMAN Enterprise software (with proper rule configuration).

VACMAN Enterprise utilizes highly secure "secret key" technology for internal communications. The specific encryption method utilized is 3DES – a format which incorporates three separate DES 56-bit keys, to provide an accumulated 168-bit encryption.

Negotiation between the web servers and the VACMAN Enterprise authentication / authorization servers is implemented using an RSA BSafe exchange – with a 512-bit key length – to establish the 3DES key; or with Entrust Session providing 1024-bit keys.

Enhancing the User Experience – Fault-tolerance and High Availability

VACMAN Enterprise supports scalability and fail-over, by providing for replication of services. VACMAN Enterprise may be configured to use multiple authorization servers for security services. Although only one logical Security Repository may be stored in a cell, the cell may contain multiple copies of the Security Repository, distributed among the master and backup servers. This design makes it possible for any process failures to "fail-over" to functioning servers elsewhere in the network. If the master server fails, one of the backup servers can be promoted to "master" through a single button selection by the administrator.

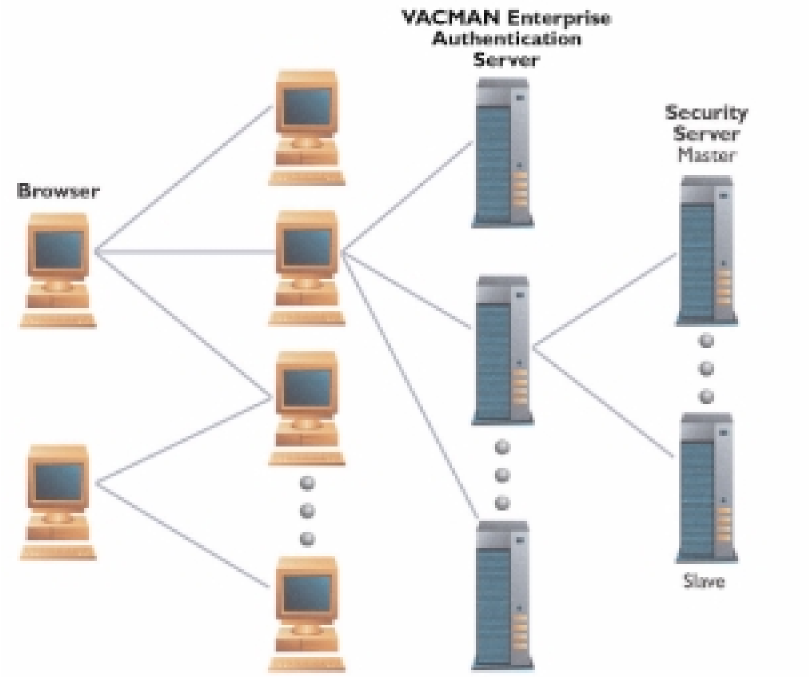


Figure 8. Scalability and availability (fail-over) via replication of services.

Management

The VACMAN Enterprise Console is the tool used by administrators to perform remote, graphical installation, configuration, and security management functions for all of the VACMAN Enterprise components in the network. The VACMAN Enterprise Console supports a fully secure delegation of these management tasks.

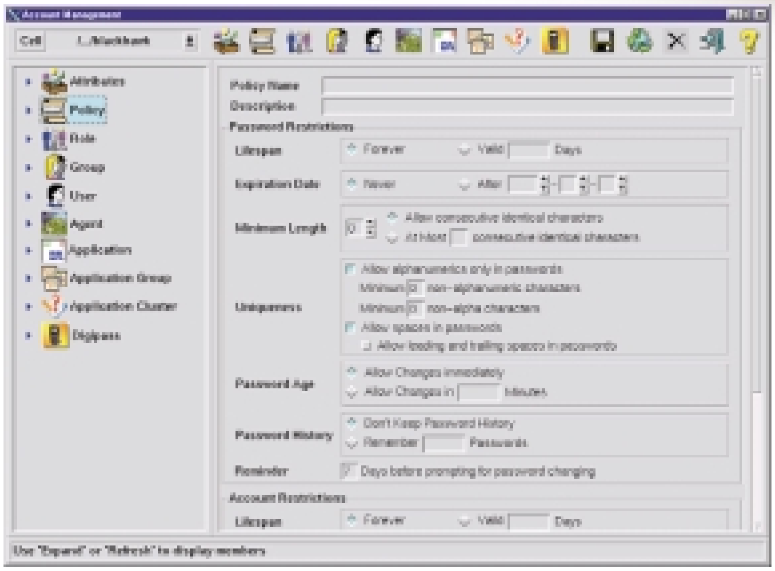
VACMAN Enterprise Console

The Console allows administrators to configure and maintain the web security framework and policies. Administrators can use it to add, delete, and rearrange hosts, domains, and cells; to create and modify the connection and object rules that secure web sites; and to secure connections between those machines and the non-VACMAN Enterprise machines and remote cells that are part of your configuration. The VACMAN Enterprise Console also provides access to a number of other VACMAN Enterprise administrative functions and tools.

Using the Console's Time Definitions Editor, administrators can configure Time Specifications. These specifications, along with hosts and domains, are used in the Connection Rule Editor to create connection rules (e.g., "business hours" or "off-hours") which are stored in the Connection Rule Database (CRDB). The CRDB is maintained centrally and distributed to each node.

Using the Object Rule Editor, individual object rules can be defined to protect any object supported by a specific service (such as HTTP or FTP), on a specific web server, anywhere in the network. The object rules are stored in the Object Rule Database (ORDB). The ORDB can be maintained centrally or locally.

The Console's User Account Manager enables administrators to create, modify, and delete users, groups, and roles within the VACMAN Enterprise framework. The Account Manager also manages security attributes and system security behavior profiles (e.g., configuring password length, history, number of failed attempts before lockout, and other password strength settings).



Policy Name
Description

Password Restrictions

Lifespan ○ Forever ○ Valid Days

Expiration Date ○ Never ○ After

Minimum Length 0 ○ Allow consecutive identical characters ○ At Most consecutive identical characters

Uniqueness ☑ Allow alphanumerics only in passwords
Minimum 0 non-alphanumeric characters
Minimum 0 non-alpha characters
☑ Allow spaces in passwords
□ Allow leading and trailing spaces in passwords

Password Age ○ Allow Changes immediately ○ Allow Changes in Minutes

Password History ○ Don't Keep Password History ○ Remember Passwords

Reminder 7 Days before prompting for password changing

Account Restrictions

Lifespan ○ Forever ○ Valid Days

Use "Expand" or "Refresh" to display members

Figure 9. VACMAN Enterprise Administration Console Account Manager showing Policy settings.

(Note: Some available policy settings, such as additional account restrictions and login restrictions, are not visible in this image).

Web Administration Tool

VACMAN Enterprise also provides a multi-functioned web-based administration tool for use with VACMAN Enterprise. The Web Admin tool allows administrators to delegate many common day-to-day activities – such as re-setting passwords, adding and deleting users, re-mapping group memberships, or account lockout.

Designed for easy-to-use, browser-based access, and with a focus on user account management, the Web Admin tool makes an ideal Help Desk companion. Although Web Admin does not provide all of the configuration tools available with the VACMAN Enterprise Console, the Web Admin software can be easily customized to meet the needs of any installation.

User Account Self-management

With VACMAN Enterprise, administrators can allow users to self-manage many aspects of their accounts, including:

- Viewing account information
- Viewing and discarding credentials
- Logout
- Application password mappings
- Password change
- Digital certificate functions

Summary

VACMAN Enterprise helps you reduce the time and costs associated with maintaining effective web security, while improving overall security performance and enhancing your customers / users' confidence in the security of your web site. VACMAN Enterprises delivers several key capabilities:

- **Dynamic User Registration and Mandatory Account Enablement** – speeds deployment to thousands of users while dramatically reducing administrator involvement
- **Secure single sign-on** – significantly improves the users' experience by eliminating the need for repeated authentication, even when the application accesses resources outside of the web environment
- **Automated password reset** – reduces the administrative burden on Help Desk personnel, freeing them up to perform other, higher-value tasks
- **Cross-platform, centralized management of security rules and policies** – eases management for large, complex web sites
- **Fine-grain control of connections to (and requests for) web site servers and online resources** – maximizes the value of information resources by making them as open as possible, while also providing an adequate level of security and protection
- **Personalization of web application responses and web pages** – improves the user experience and encourages return visits
- **Multiple authentication methods** – provides the ultimate flexibility in managing your security environment

VACMAN Enterprise is designed to integrate seamlessly with your existing web applications – whether two-tier, three-tier, or multi-tier. VACMAN Enterprise can securely and easily incorporate back-end client / server and legacy systems into your web infrastructure, all under a single security management framework. These capabilities combine to make VACMAN Enterprise the industry's premier choice for managing security on enterprise-class web sites.

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 digital 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.