

Yardi Voyager Security

Advanced, Comprehensive, and Integrated Application Security

Yardi Voyager Security Overview	2
Multi-Level Security	3
Advanced Auditing Capabilities	3
Security Validation	3
Security with Auxiliary Services	4
Network Security	4
Data Encryption	4

YARDI VOYAGER SECURITY OVERVIEW

Yardi Voyager™ features a sophisticated and comprehensive security system that allows system administrators to apply granular security settings to internally defined security classes and groups. Yardi Voyager™ includes a front-end administrative tool that sets levels of security and privilege at the user and group levels. With this tool, system administrators can easily define flexible access, resource, and privilege assignments, thereby providing a mechanism that allows only relevant, authorized information and tasks to be accessed by the user. Data security can easily be set by the client's system administrator to define multiple levels of access (e.g., read only, read/write, etc.) for users or groups of users. The following table details the various layers of security that are either standard or optional with Yardi Voyager™. Security is addressed at both the application and network level.

Layer	Optional	Feature	Description
1	Standard	Cisco PIX Firewalls	Firewalls control the type of information coming and going through the servers.
2	Standard	RDBMS Authentication	Database access is limited to name-encrypted databases related to individual clients.
3	Optional	Workstation Authentication	Users can only log in from machines that have been authenticated by the system administrator.
4	Standard	Application Authentication	Application requires valid user name and password combination.
5	Standard	User-Defined Access	System administrators can assign access to program features.
6	Standard	User-Defined Timeouts	User sessions will be disconnected from Yardi ASP servers after 30 minutes of inactivity to minimize possible misuse of connected workstations left unattended.
7	Optional	Secure Sockets Layer	Certificates (either Yardi-provided or third-party vendor-provided) are employed for network encryption and authentication along with public key and private key encryption techniques between browser and server.
8	Optional	Point-to-Point Virtual Private Networks	Only authorized users can access the network and data cannot be intercepted.

Yardi Voyager™ includes standard login and password protection in addition to workstation authentication security, which can be optionally implemented. Security for the application is set up in a security table in the Yardi Voyager™ database. A comprehensive and sophisticated security system of passwords and permissions is used to control access to data based on both individual user and user group roles. Yardi Voyager™ provides field- and function-level security for most commonly used functions. Access can be controlled at multiple levels.

MULTI-LEVEL SECURITY

Yardi Voyager™ security includes the following five levels: Portfolio, Menu, Function, Field (View Only, Edit, or Mask Out), and Accounting Period. Yardi Voyager™ provides field- and function- level security for most commonly used functions. Security can be established on menu sets, with one user, or groups of users, having predefined access to multiple menu sets. Furthermore, different users within the same group can have different security permissions. System administrators can change the experience of users based on their role in the organization and have ultimate control of viewable fields and read/ write capabilities.

Menus and permissions are set up on a group level. This defines what functions, data, and reports each group can access. Before the request is processed, the system validates that the particular user has access to the requested item. The system administrator can also define whether the given group has read-only access to a given item.

ADVANCED AUDITING CAPABILITIES

The system provides standard audit reports of user activity that clients can utilize to monitor accessed functions. System administrators can track user activity on a variety of different levels. Each login session is tracked, including login and logout time, IP address, and last request. Updates to the database can optionally be tracked on a per user/per statement level. Performance statistics for each request can optionally be tracked on a per user/per request level. The system can be configured to audit all database updates, inserts and deletes by user, and user logins with date and time stamps. It stamps every financial transaction with the user name, date, and time it was created and modified.

SECURITY VALIDATION

Yardi recognizes that our clients' confidential information is one of their greatest assets. We adhere to rigid confidentiality compliance regulations mandated by Sarbanes-Oxley and HIPAA.

System logins occur over a secure sockets connection. User logins and passwords are validated against an encrypted database table. Once a user is validated, an encrypted cookie is set. The login cookie is a session cookie which never gets stored on the client machine but is passed between the server and the client. The cookie string is validated against the database before each request. After each request is processed, the system updates a last activity date and time.

Users are automatically logged out if their session has expired due to inactivity (the length of which is set by the system administrator). Minimum password length and password expiration can be set up and monitored by the system administrator. Users can also be marked as inactive, which automatically disallows logins. Individual users can be marked as "Authenticated Machine" users. In this mode, the user can only log in from workstations that have been authenticated by the system administrator. Machines are authenticated through a process initiated through the Yardi Voyager™ Administration program.

SECURITY WITH AUXILIARY SERVICES

Access to peripheral devices is controlled by the Windows operating system. Yardi Voyager™ uses Secure Sockets Layer (SSL) technology for remote access and mobile devices. The system also supports machine authentication to support remote access control.

NETWORK SECURITY

With our Yardi-hosted (ASP) solutions, client data resides behind a sophisticated Cisco firewall along with password protection allowing only authorized users access to data. For another layer of security, data is backed up nightly and moved off-site for extra protection. Other security layers include Secure Sockets Layer (SSL), virtual private networks (VPNs), and other encryption standards, which may be deployed at the discretion of the client. Yardi ASP Hosting Services include the following security features:

- Battery backups and a fully automatic fail-over standby generator to ensure performance in the event of a power failure
- Weekly server maintenance and back-up of all data
- Cisco firewall
- 128-bit encryption over the Internet
- Redundancy/co-locations
- Physical site security
- Daily and/or up-to-the-minute backups

DATA ENCRYPTION

User passwords are encrypted and stored in the database. Future plans include a conversion to public/private, 128-bit encryption. System logon is form-based. X.509 certificates are optionally required for clients wishing to use SSL. All data transfers, including login, are protected using SSL. Certificate Authorities (CAs) typically provide X.509 certificates; Yardi is not limited to any set of CAs.