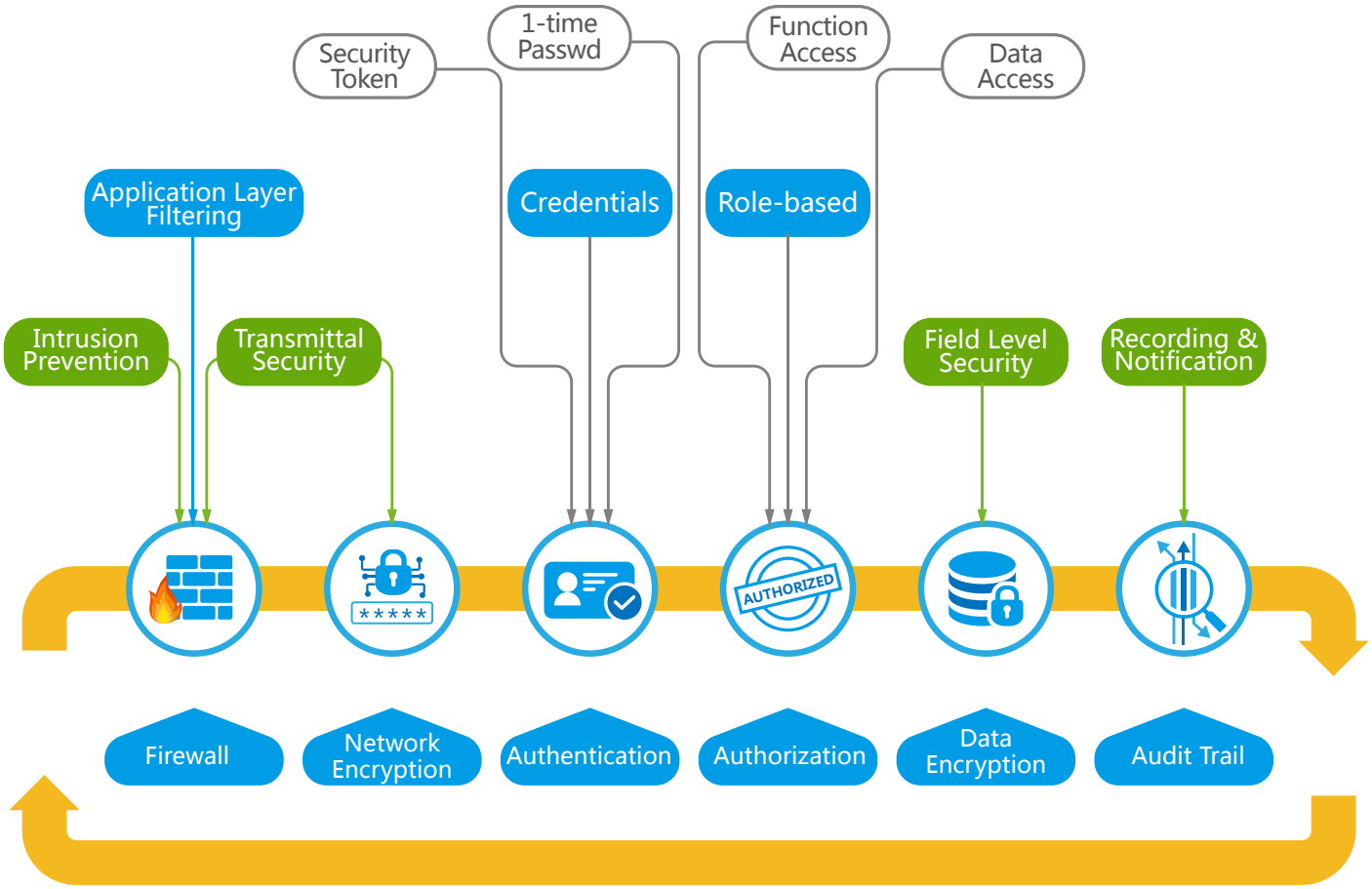
Security & Reliability

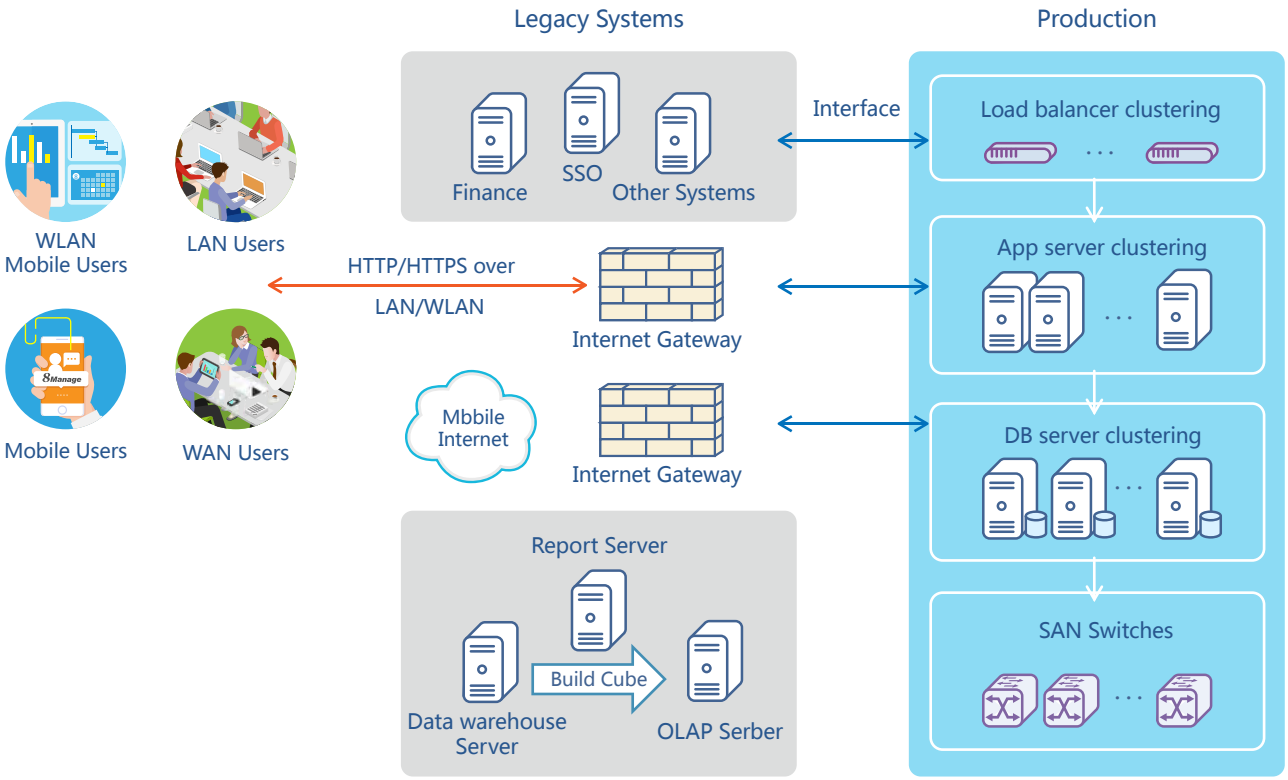


8Manage supports N-tier architecture which allows firewalls to be set up for packet inspection and application filtering to protect the servers in each layer against malware and intrusions. 8Manage uses HTTPS for transmittal security and supports Two-Factor Authentication (2FA) , separate role-based authorization for function and data, different methods for data encryption and provides the audit trail mechanism to log actions, detect unwanted behaviors and send out alerts.

• Network Security

Transmittal Encryption:

8Manage uses HTTPS for secure communication over computer networks. HTTPS is a mature technology that is widely used on Mobile Internet. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS), or formerly, its predecessor, Secure Sockets Layer (SSL).



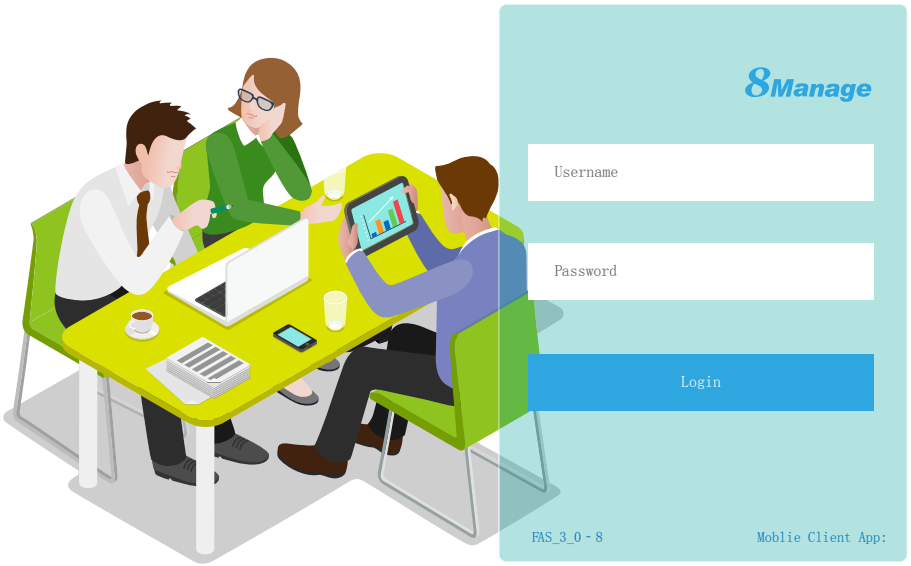
Device Address Access Control:

This is for the organizations who want to control who can access to the system by IP address, Network Segment or device access controlled by firewall.

• Authentication

Two-Factor Authentication (2FA):

8Manage supports different types of security tokens and password for 2FA. 2FA provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. 2FA has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.



Single Sign On (SSO) Integration:

8Manage supports the integration with SSO such as Windows Active Domain, LDAP, CAS, Open AM and Oracle OAM.

Third-party Authentication Integration:

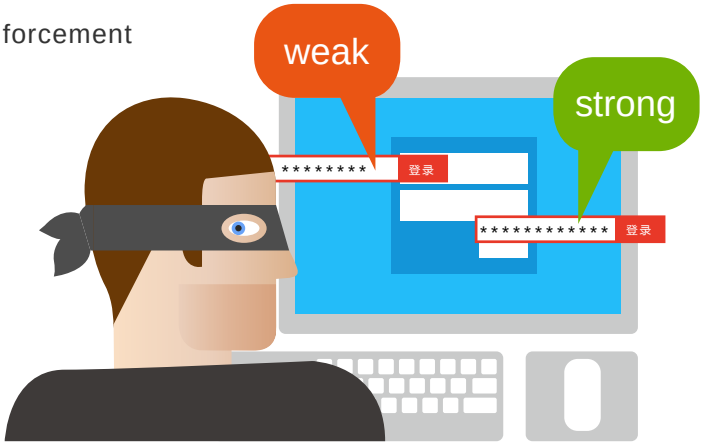
8Manage has the pre-built integration with i-Sprint Authentication Service.

• Password Security Management

Password Strength & Protection Policies:

8Manage allows the security officer to determine and set the following password strength and protection policies:

- Mandatory password change for initial user login
- Mandatory periodical user password change policy
- Password minimum length enforcement
- Password minimum number of alphabets enforcement
- Password minimum number of digits enforcement
- Password minimum number of special characters enforcement
- Word disallowed in password
- Number of repetitions of the password
- Login time control by roles/users
- Suspend inactive users
- Password age constraint



• Segregation of Duties

One of the key concepts in placing controls over functions and data of systems is segregation of duties. Segregation of duties serves the following 2 key purposes:

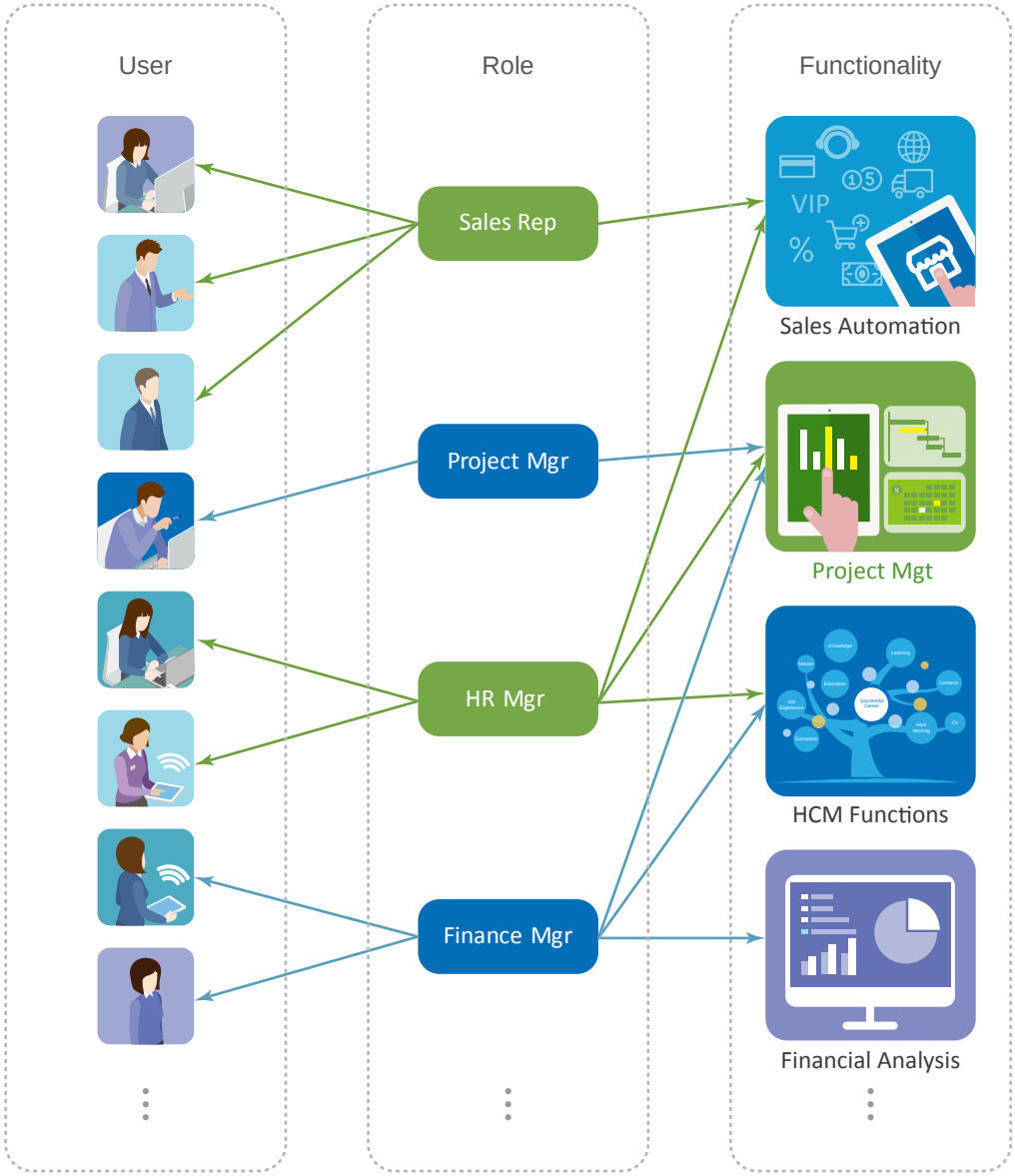
- Ensuring that there is oversight and review to catch errors
- Helping to prevent fraud or theft because it requires two people to collude in order to hide a transaction

8Manage supports segregation of duties and provides Role Based Access Control (RBAC) to control accesses by entitlement and/or authorization. In 8Manage, when the user is being assigned to or unassigned from a role, she will be automatically entitled to or debar from the access rights associated with that role. The user can also gain or lose additional access rights that are authorized to or removed from her by higher authority.

Due to the fact two managers of two different departments might need to have the same access rights to system functionality but different access rights to data (e.g., Manager A of department A needs to access department A' s data and manager B of department B needs to access department B' s data), 8Manage supports separation of access rights to system functionality and data (e.g., Manager A and manager B have the same rights to functionality but different data access rights to data).

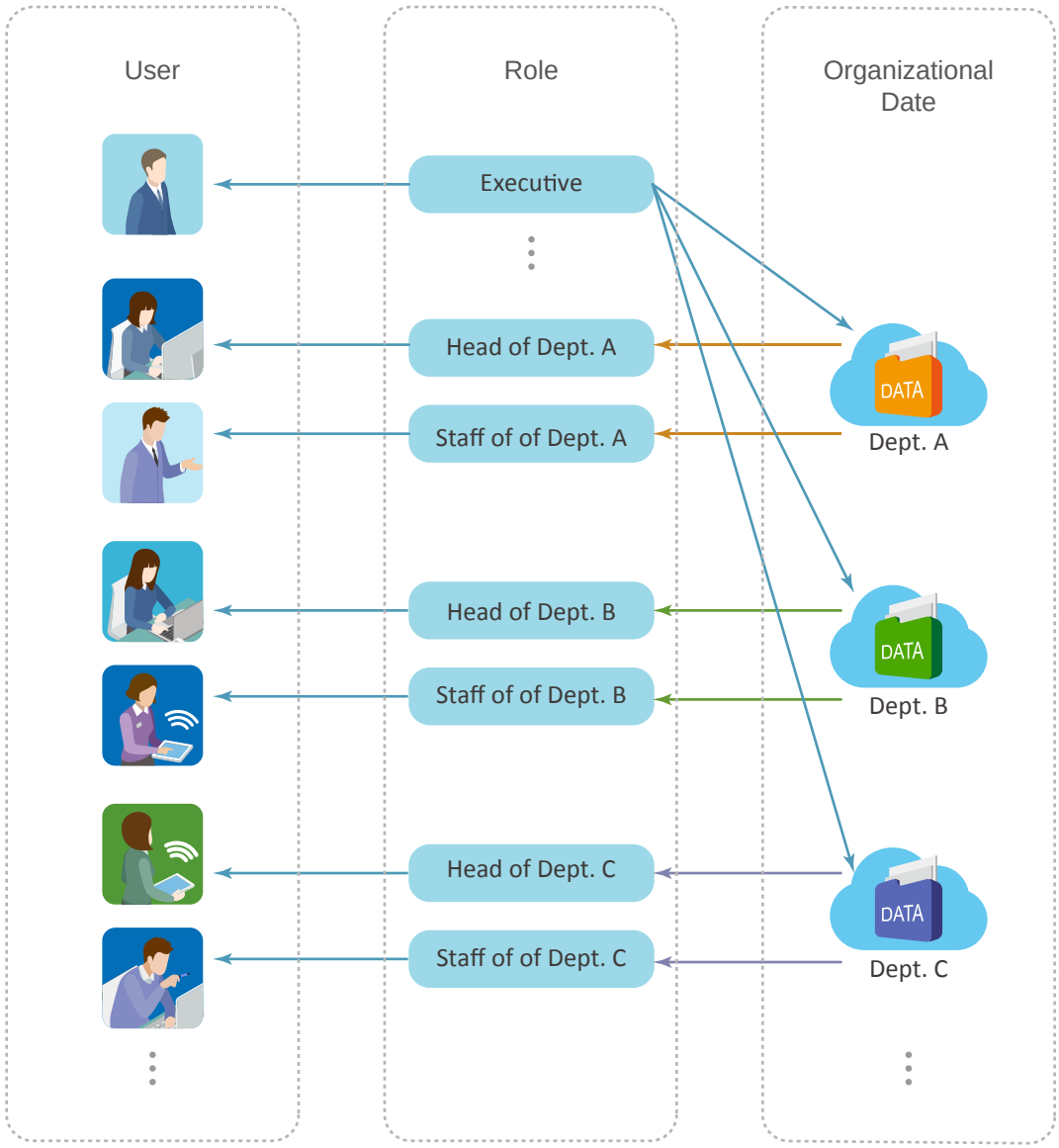
RBAC: Functional Access Entitlement

8Manage allows different roles (e.g., Sales Rep, Project Mgr., HR Mgr. and Financial Controller) to be defined and each user is assigned to one or multiple roles. The user' s functional access rights are determined by the roles assigned to her.



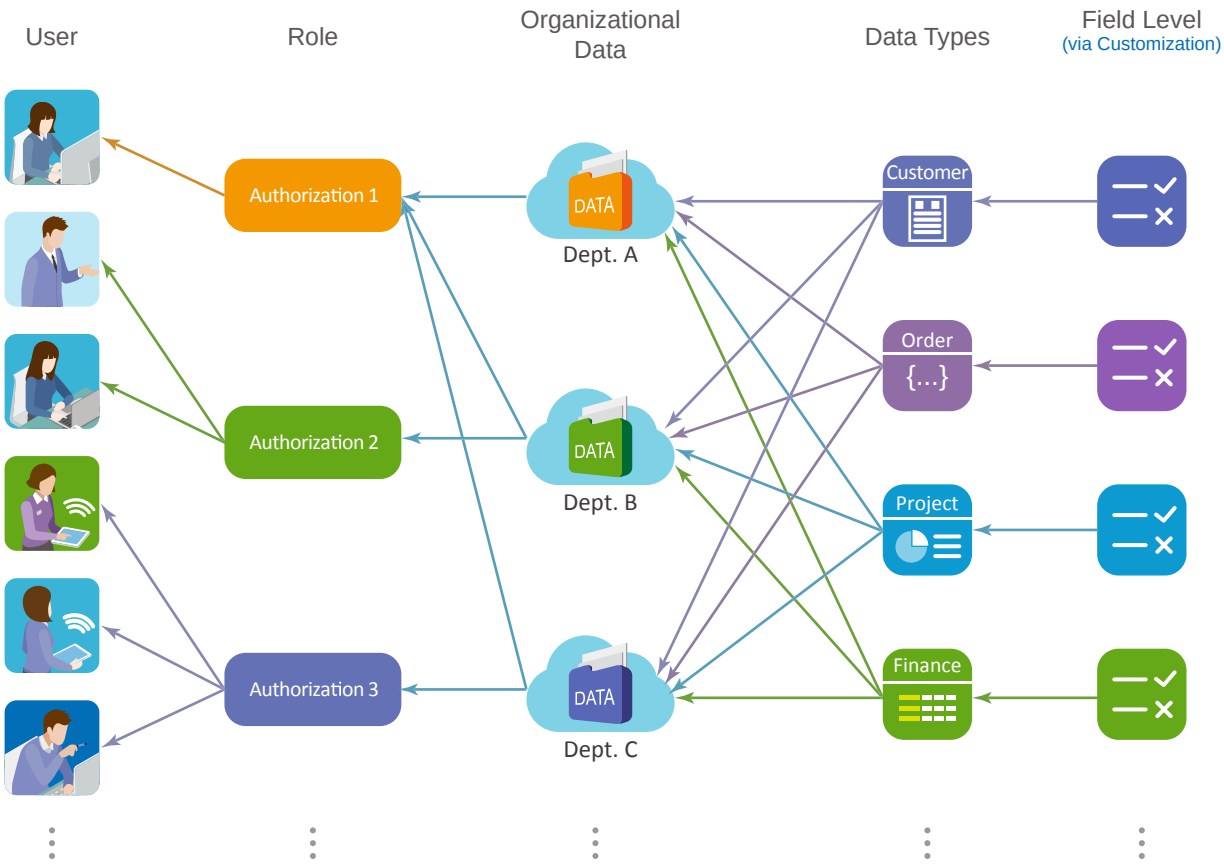
RBAC: Data Access Entitlement

8Manage allows different roles (e.g., Executive, Division Manager, Department Manager) to be defined and each user is usually assigned to one role. The user’ s data access rights are determined by the roles assigned to her.



RBAC: Data Access Authorization

8Manage supports authorizing users extra data access rights by the users (e.g., administrator) who have the authorization authority. The authorization can be done in the organization data level, data type level and field level.



• Audit Trail

8Manage provides Audit Trail which is a chronological record of everything that happens in your system. In addition to tracking all actions, interactions and transactions within your system, audit trails can be used for several other purposes such as:

- Identifying the user who performed the operation
- Time of operation
- Content of operation
- Data difference before and after the change

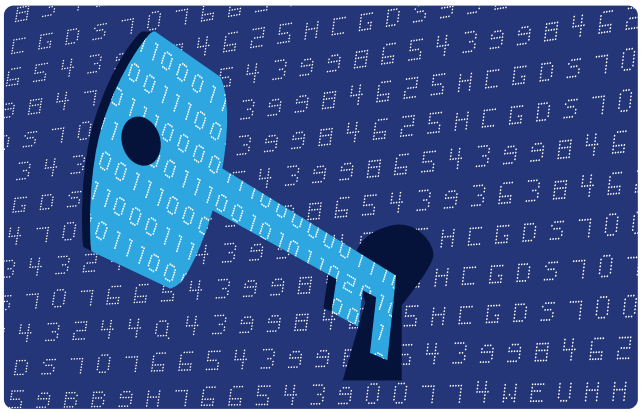
The log history of user action, interaction and transaction also includes the network address (IP) of the users.

• Data Encryption

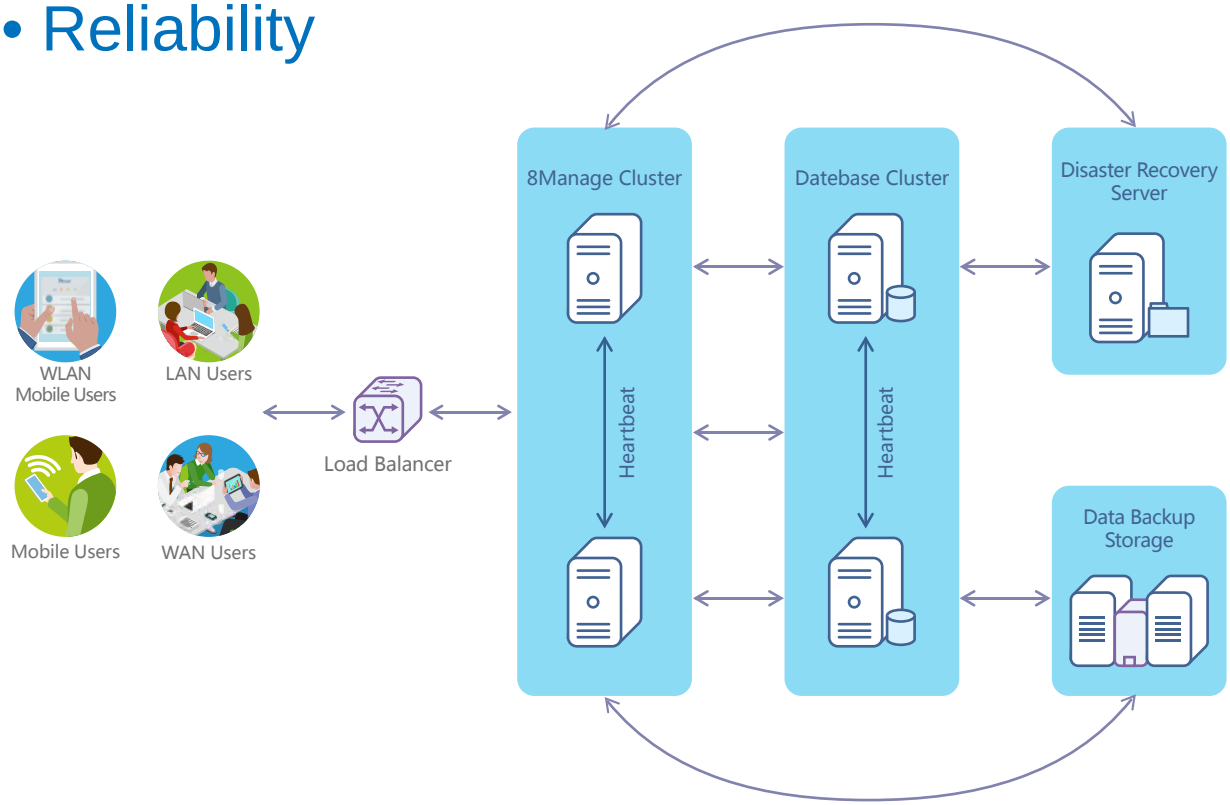
8Manage supports the following methods for data encryptions:

- Hash Encryption (MD5 128-bit) for user passwords
- PGP Encryption (1024-bit) for Database storage

The names and contents of the uploaded files will be encrypted (DES 64-bit) before storing in the file system.



• Reliability



8Manage supports the following levels of recovery to maximize the availability (uptime) of the system and minimize data loss even if a system crash or site diaster occurs :

Data Backup & Re-install:

Periodical backup of data to secondary storage automatically to minimize data loss if a system crash occurs.

Hot failover:

8Manage supports different modes of hot failover such as Active-Standby mode and Active-Active modes to minimize system downtime or unavailability.

- In Active-Standby mode, the active server will be online and synchronize data to the standby server. At the same time, the standby server will monitor the status of active server and active itself when the active server crashes.
- In Active-Active mode, both servers are online and provide the same services, it improves performance of the whole system and provides load balancing function.

Disaster Recovery :

8Manage supports replication of data to an off-site location to overcome the need to restore the data (only the systems then need to be restored or synchronized).

www.8manage.com

Wisage Technology is an international software product company with clients in many countries and regions, including the U.S., Canada, China mainland, Dubai, Hong Kong, Macau, Philippines, Taiwan, Malaysia and Singapore. All its products are mobile internet ready and can be accessed with IE, Firefox, Safari and Chrome browsers and we also provide different apps on Android and iOS. It offers SaaS and perpetual licenses for all regions for the following products:

8Manage CRM : Mobile Internet CRM
8Manage SRM : Supplier Management, e-Procurement & e-Tender
8Manage Simple PM : Simple to Start & Extend PM
8Manage PM : Advanced Tool for Project Planning & Execution
8Manage PMO : High Performance PMO
8Manage HCM : Human Capital Management
8Manage OA : New Generation Office Automation
8Manage FAS : Enterprise Management Full Automation Suite

8Manage e-Expense : Web & Smartphone Expense Report System
8Manage e-Leave : e-Leave & Leave Management
8Manage e-Timesheet : Web & App Timesheet System
8Manage e-DMS : e-Document Management

Emailing info@wisagetech.com , or calling +852-6969-6665 or +86-20-3873 2922 .