Ramsys Head Office Evolution

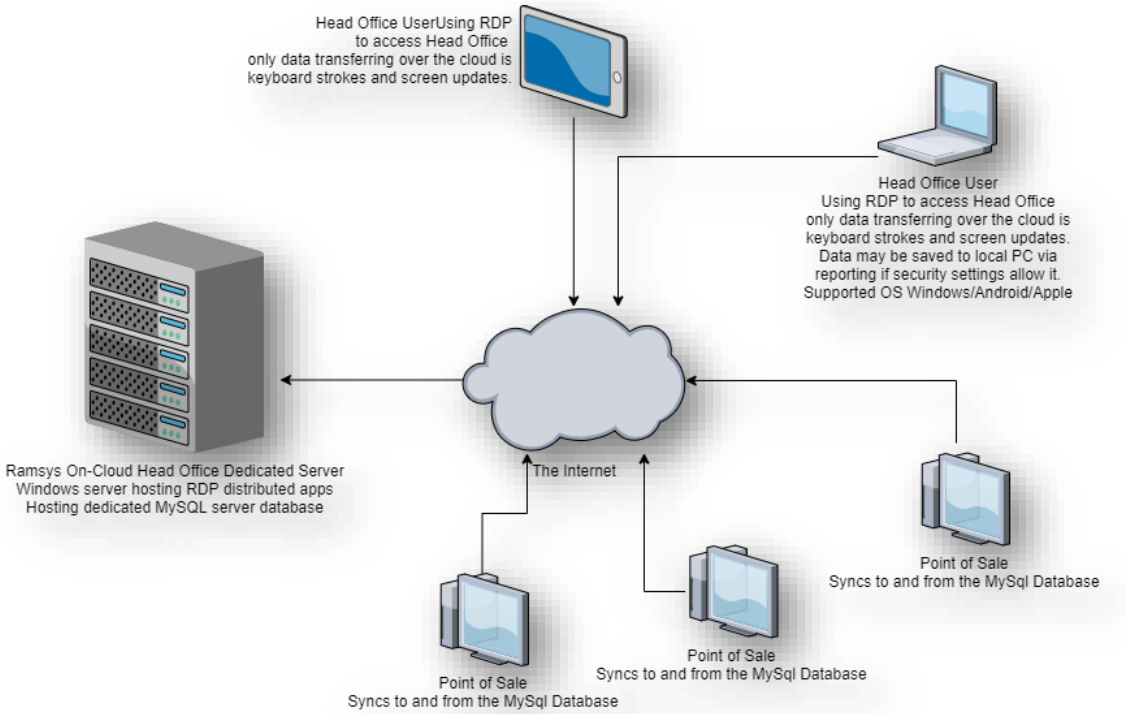
Cloud Security

Introduction

Ramsys Head Office Evolution is the most comprehensive Retail Management System available. It is generally and preferably installed on the cloud on servers provisioned and maintained by our very experienced technology partners Business IT on the BIT Cloud platform.

While the issue of Data Sovereignty is simple– You own your data, the security of your data is paramount to us and the approach is multilayered and taken very seriously by both BIT and Allspoke.

The following document outlines the basic standards and extra disciplines offered to increase security. As a cloud customer you will be assigned a dedicated server. This is not a shared server so there is no possibility of your operations being affected by another customer.



MySQL Database minimum restrictions

The Database used by Ramsys HO is MySQL Vsn 8 with the following minimum standards.

- Each store will access the server via a unique username and password
- Passwords are minimum length of 10 which must include letters (both upper and lower), numbers and at least 1 punctuation character. Passwords are not words found in a dictionary but a random sequence of the accepted characters
- Root or SA access will not be granted to anyone. At the customers request a superuser can be setup for the Ramsys Database.
- Data transmission uses a compressed protocol rather than text. Full SSH encryption is available if required but due to the overhead/risk factor not set by default
- Database privileges are strict and set to the minimum required to perform the required tasks of each application.
- The use of Symlinks to tables is disabled to prevent malicious file deletions
- Access to the database is only available by default to the secure compiled Ramsys applications. Application may be made to provide access to the company or third parties at the companies request. Procedures for making these requests are available on request.
- The database access credentials are held within Ramsys POS and HO they are encrypted using Triple Des cypher mode ECB with a 128bit key length. Encryption is performed in volatile RAM, decrypted credentials are never written to disk or other forms of non-volatile RAM.
- Due to the enhanced security capability available access to the server is only allowable via the Version 8 or higher drivers.
- All installation history and test databases are removed to prevent any possible exploitation regardless of how remote
- Features disabled to further tighten security include
    - Limited ability to the SHOW DATABASES command
    - Disabling of the LOAD DATA LOCAL INFILE command
    - At the customers request we will obfuscate the root account
    - At the customer request we can change the default port mapping (external ports are not set to the default)

ENHANCED SECURITY OPTIONS

It is possible to increase the protection provided with your data access to the MySQL database.

- Limit access by IP address. While this requires the use of a Static IP by enabling this feature it is possible to only allow access from certain PC's.
- Increased password policy is available to suit the company's policy structure.

- A password policy that states that 2 incorrect logins will lock an account for 24hrs. Allspoke staff monitor this event. At the Customers request this may be made more stringent.

Server Access

Access to the on Cloud application is via secure Remote Desktop Protocol by Remote Distributed application. This can be on Premise for customers with a sloid infrastructure or on Cloud through our technology partners Business IT

ON PREMISE

Ramsys HO will be hosted by the company, Security, Backup, Access will be the responsibility of the company. Please ensure Allspoke staff have easy access to the server at any time for support and periodic maintenance.

ON CLOUD

The preferred method of Hosting Ramsys HO is on the cloud through our technology partners Business IT. This relationship stretches back to 2006 and has resulted in a strong, best of breed yet practical solution which balances security and availability with performance and ease of use.

Unlike other clouded solutions Ramsys is not provisioned via a browser thus exposing it to the limitations and risks browser based apps suffer from.

By using RDP distributed app virtualisation the application looks and operates as if it is installed on the users PC. There is however only a minimal configuration file. The user interface is displayed on the local PC while input from the user is transmitted to the server where the actual software execution takes place. In this way a very fast, secure connection is made between server and client. By default no direct access is allowed to the data or the server increasing the security against attack by magnitudes. RDP clients are available for Windows/MAC/Android. There is also a client for Unix although this has as yet been untested by Allspoke or BIT.

By default, Remote Desktop Services connections are encrypted at the highest level of security available. However, some older versions of the Remote Desktop Connection client (Depending on your version of Windows) do not support this high level of encryption. If your network contains such legacy clients, we can set the encryption level of the connection to send and receive data at the highest encryption level supported by the client.

Four encryption levels are available.

FIPS COMPLIANT - This level encrypts and decrypts data sent from the client to the server and from the server to the client by using Federal Information Process Standard (FIPS) 140-1 validated encryption methods. Clients that do not support this level of encryption cannot connect.

HIGH - This level encrypts data sent from the client to the server and from the server to the client by using 128-bit encryption. Use this level when the RD Session Host server is running in an environment containing 128-bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.

CLIENT COMPATIBLE - This is the default setting. This level encrypts data sent between the client and the server at the maximum key strength supported by the client. Use this level when the RD Session Host server is running in an environment containing mixed or legacy clients.

LOW - This level encrypts data sent from the client to the server by using 56-bit encryption. Data sent from the server to the client is not encrypted.

DEFAULT PASSWORD POLICY

The following is the default password policy, this is able to be customized if required to match customer policy.

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

FULL VIRTUAL ENVIRONMENT

It is possible to create at customer request to provide a full windows desktop to the server.

MULTI FACTOR AUTHENTICATION

As an option Business IT can provide a further layer of security by providing multi factor authentication using the Duo product (www.duo.com)

Duo is a world leader in Multi Factor Authorisation and is provided not by default but as an option for sites requiring a tighter security policy.

MONITORING

All servers are monitored using connect-wise automate and Liongard

Customer dashboards may be setup to provide customer specific KPI's on server health.

BIT are also subscribers to ID Agent which provides Channel-focused Dark Web monitoring and the most validated credential exposure data available. ID Agent's sophisticated intelligence allows customers to focus on their business with peace of mind (https://www.idagent.com/)

BACKUP

Backup is performed in 2 forms, your entire dedicated server is backed up using Datto backing up to a Sirus S4XE36E.

The Datto backup solution provides a wide range of powerful features integrated into a single data protection platform.

All-in-one solution – The Datto Agent, Datto Device and Datto Cloud are all proprietary Datto systems that work seamlessly together in a fully integrated platform. The solution is owned and maintained by Datto, and there are no third party vendors involved.

Image-based backups – Datto uses image-based backups to capture a complete snapshot of a protected server. The Datto Agent uses Microsoft's Volume Shadow Copy Service (VSS) to take copies of open files well as SQL databases and Exchange mailboxes. In a recovery situation, images of protected servers can be restored to new hardware (bare metal restore) or can be converted to HyperV or VMWare virtual machines.

Flexible Backup Schedules – The flexible scheduling tool on the Datto Device can be configured to perform backups from once a week to every 5 minutes. The scheduler allows the selection of hours of the day and days of the week, so backups are performed based on the customers business requirements.

Screenshot Verification – At the end of each day, the Datto Device automatically virtualises the last backup image and performs a test boot, separate from the real server. The Datto Device can check if a machine has booted successfully and send a screenshot email to Business IT for verification. Any failed tests are diagnosed and details sent to Business IT for rectification

Inverse Chain Technology – Datto's proprietary technology that allows the most recent back on the Datto Device to be a fully constructed image of the protected server. Traditional backup solutions perform an initial "full system" backup and then records the incremental changes in a linked list. Restores from traditional systems can be lengthy, as the backups are compressed sequentially to build the recovery image. Inverse chain technology maintains each backup point as a fully constructed image that can be used in minutes. 6

End-to-end Encryption – All data is protected by AES-256 encryption both in transit and while stored in the Datto Cloud. Data can also be encrypted locally on the Datto Device using a unique passphrase.

Instant Virtualisation – Using Datto's Inverse Chain Technology, the Datto Device can boot any snapshot of a protected server in minutes using the CPU and RAM on the Datto Device to host the virtual machine. The virtual machine will be available on the local network and normal business operations can continue with minimal disruption. Protected servers can also be virtualised in the Datto Cloud if the local Datto Device is not accessible.

Ransomware Detection – Datto has developed a multi-tier ransomware detection process that searches the backup images for file encryption, bulk file changes, and other key indicators that a system is infected. If ransomware is detected, an alert is created and sent to Business IT for action.

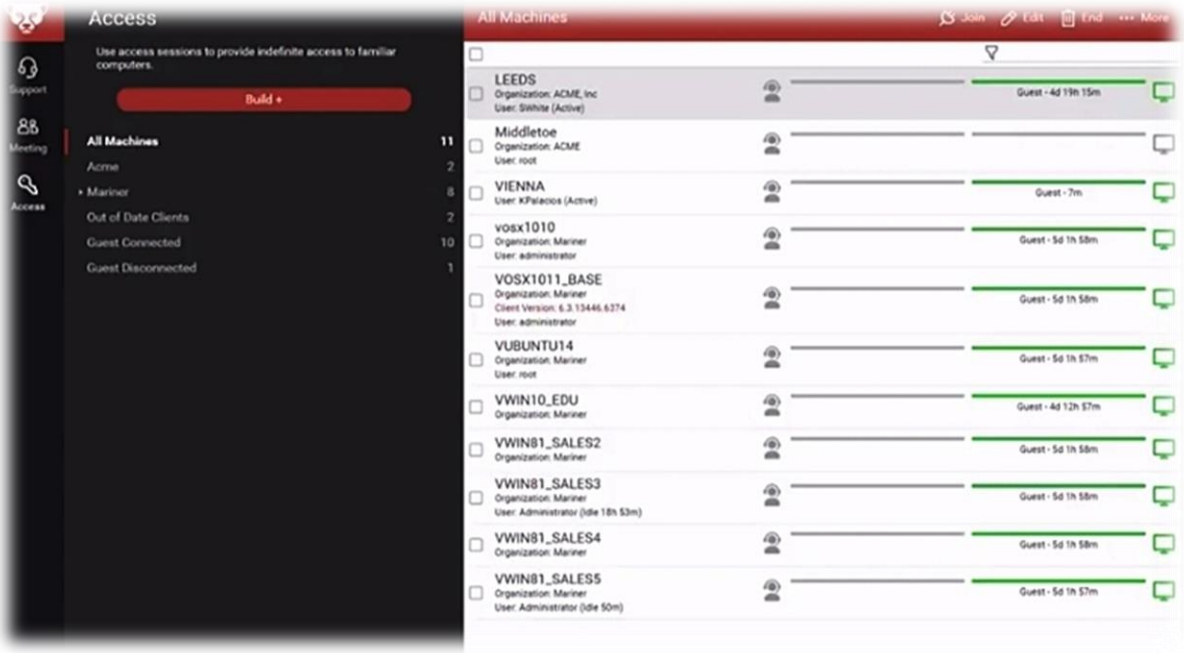
Customised Retention Periods – The Datto solution allows for flexible backup retention periods on the local Datto Device. Data retention has been set by Business IT to keep the local protected data until the storage capacity of the Datto Device is reached. The local retention rules are specified in Section 5. The retention rules in the Datto Cloud are based on the purchased plan and are also listed in Section 5.

MYSQL DUMP BACKUP

Your MySQL structure procedures and Data is also backed up overnight via SQL Dump and stored in an encrypted compressed file. This file is uploaded to a separate off site secure server. You may also request a copy is uploaded to a server of your choice as well Here at Allspoke we respect the fact that the data is YOUR data. This is performed at a set time each night in addition to the above backup regime.

User Support

Allspoke and if necessary, BIT are able to provide remote support services via the Connectwise client. Connectwise is a fast, secure remote support tool which is able to provide remote access with a much better piece of mind than products like VNC and Team Viewer.



BIT can provide approved customers and their agents with the same access by arrangement.

Ramsys Support options may be found at https://www.allspoke.nz/support

Other Applications

You may be able to host other applications on your server such as your accounting system, office etc. Please contact business IT directly to discuss.