SmartHR SAAS delivery

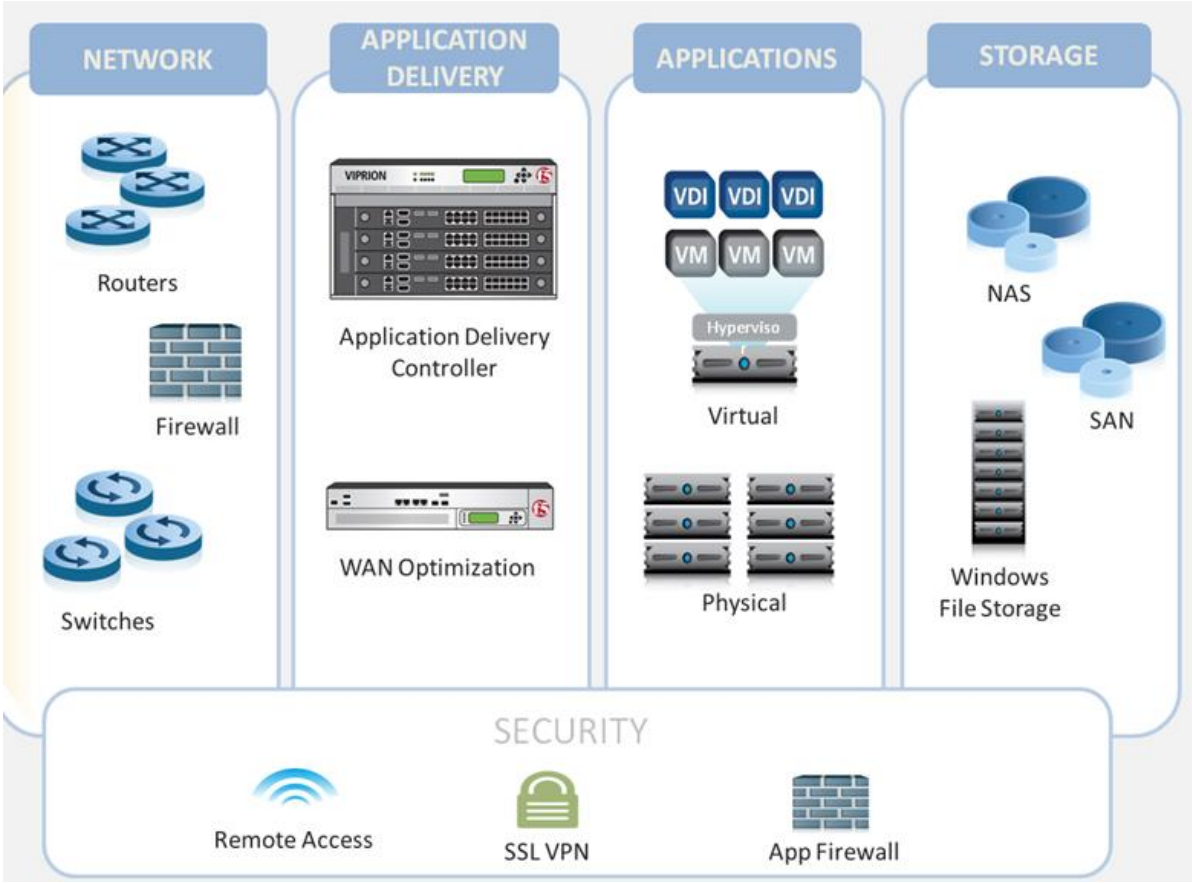
Overview

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

Introduction

At Smart City Systems (SCS), our cloud partners have built managed cloud hosting solution around our secure, high availability private cloud hosting architecture with professional accreditation such as ISO 27001:2013. We chose to build our shared servers on an "N+1" redundant architecture and data center infrastructure. That means there is redundancy in every component of the system from power and Internet delivery to the hardware and network components with no single point of failure in the system. Should any component fail, there are redundant components in place to maintain the server and Internet available.

Sample Application delivery architecture



Some of the key feature of SAAS cloud delivery model we offer to our clients

Our Data Center Facility and features

- **Multiple power source and power backup**

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

For an uninterrupted power supply to datacenter, we have both local power distribution and incase if there is a failure on that power distribution. This is equipped with generator backup apart from the backup UPS we have

- Precision cooled climate-controlled environment.
- 24-hour security, moisture, fire and power monitoring.
- Clean agent fire suppression system.

- **Multiple leased lines for links for redundancy**

We have a primary leased line from ISP for SAAS delivery and a second leased lines for the same capacity to maintain minimum down time.

- **Physical security in place and biometric access**

There are security guards to monitor and logs all in and out access to the premise, on top of that we have biometric access to the critical areas with specific access defined to various areas.

- **CCTV camera surveillance**

Premise is fitted with total surveillance and data is been stored over 60 days for review

- **Fail over server in UK and India**

SAAS data gets replicated to two geographical locations for redundancy, UK and India office. In case of any major down time using this data a failover setup will be populated with a minimum time frame.

- **Multiple Firewall with strict policy, Cisco products with L3 switches**

To protect our infrastructure from intrusion and penetration, we have a very well set of firewall with fail over and strict access policy in place

- **Dell and HP Servers with high-end spec.**

Our data center servers and backup solutions are standardized on Dell and HP products.

- **Security framework**

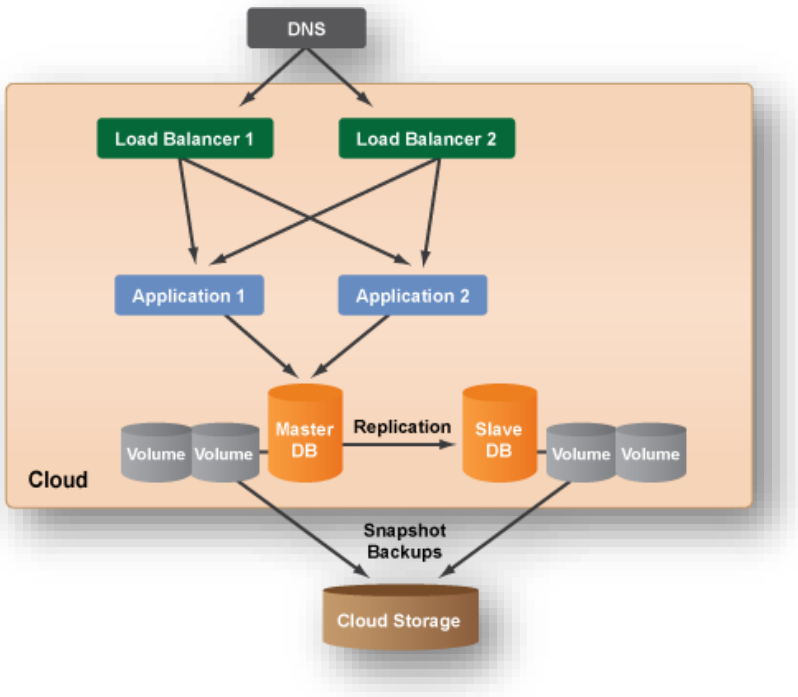
Compliance and security are top priorities to guarantee that your data is protected. Our DC is compliant with:

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

- **IT Security framework**
  - Security segregation done all layers, Gateway, DMZ, Network and Server
  - Active components are audited every 2 months
  - Logs at all layers are centralized and monitored
  - Security patches and service packs are updated on a regular basis
  - PT/VA process carried out on regular interval
  - AV products to protect servers from many of the threats
  - Snapshots been taken on a regular interval
  - MFA enabled for all access.

All the servers have got policy in place for external and internal access with user access restrictions and privileges.

Application delivery model



Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

- **Application server redundancy**

All the SAAS delivery servers work on fail over model with redundancy on servers and database.

- **Regular auditing**

Our team reviews the access logs against any discrepancies and gets escalated to L3 team to review if anything found**.** Penetration test is done on a period basis to evaluate the security aspects of the application and the IT infrastructure used for hosting the solution.

- **Database protection**

Encryption using TDE is enabled for database and physical database files such as data files, log files and database backup files. Database can be decrypted or restored only using the certificate and master key password.

- **Database security**

At SCS, we prioritize the security and privacy of customer data. To ensure the utmost protection, we employ a dedicated database system that guarantees the separation and non-sharing of data between clients. This means that your data is isolated and inaccessible to any other customer using our services.

Our data access control rules are designed to enforce strict segregation between customer databases within the same cluster. These rules prevent any unauthorized access or data leakage from one database to another. Rest assured that your data remains confidential and secure within your dedicated database.

- **Application delivered through only https signed certificates**

SAAS gets delivered only through https certificate with end-to-end encryption; this makes data secure and hard to penetrate. Secure Sockets Layer (SSL) is a protocol for enabling data encryption on the Internet. SSL is used to protect communications between web browsers and servers. SSL certificate used is with 128-bit encryption. The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and RSA as key exchange mechanism.

- **Application Access Log**

Application keeps track of every user action upon login with detail information on the pages accessed, IP address, Access Device etc. Automatic security notification alert is send for any

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

unusual login activity or login attempt and the user has the option in employee self-service section to view account activity details.

- **Data protection and Encryption methods**

Transparent Database Encryption is applied to protect the physical media—including the entire database, log files and any backups or snapshots—from being read in the event of unauthorized access to the media.

SQL Server's **Cell-Level Encryption** is used to encrypt and protect information within a database that contain sensitive data; e.g.,

- Employee information (e.g., date of birth, contact details, username etc)

- Financial information (e.g., salary, benefits, payroll, bank details etc)

Attachments are stored encrypted in the database to prevent any physical file access.

- **SCS warrants 99% uptime for the hosted software and the server.**

All computers malfunction from time to time, whether due to software issues, hardware failure, or configuration issues. In addition, from time to time, planned maintenance and upgrades have to be carried out on server hardware and software, which can result in your software becoming unavailable. It is therefore impossible to keep a solitary web server up and running 100% of the time.

SCS do provide a 99% uptime warranty as part of the hosting service level agreement, but although problems are rare, we do not wish to imply that it will never go down! When problems arise, we always do our utmost to rectify them as soon as possible. We have a 24-hour network monitoring system in place which checks our servers every 3 minutes from 3 different locations and informs us if there is a problem.

Data storage, Backup and Security

- **Regular backup of data**

Servers are attached to a local backup solution and gets backed up every day. All data backup and to external devices are secured and encrypted, all of your data will be backed up every

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

night to ensure you have several points of recovery should an issue arise. Our team is available 24x7x365 to assist you with any server configuration need or restoration of data request.

- **Offsite backup**

One fully recoverable version of all DB Records will be stored in a secure, off-site location. An off-site location secure space in a separate from our data center building we have an offsite storage where we move one set of tape once in three days to a different location

- **Remote data backup and replication**

SAAS data gets replicated to three geographical locations for redundancy, UK, India and Dubai. In case of any major down time using this data a failover setup will be populated with a minimum time frame

In the unlikely event of a complete disaster where our data center is entirely down for an extended period, preventing failover to our local hot-standby (which has never occurred before and is considered the worst-case scenario), we have established the following objectives:

Recovery Point Objective (RPO) = 24 hours: This means that in the event of data loss that cannot be recovered, the maximum amount of work that could be lost is 24 hours. We achieve this by regularly backing up data and restoring the latest daily backup in case of a disaster.

Recovery Time Objective (RTO) = 24 hours: This is the timeframe within which we aim to restore the service in a different data center if a disaster occurs and a data center becomes completely unavailable. We have automated provisioning processes in place to swiftly deploy our services in a new hosting location.

To accomplish these objectives, we actively monitor our daily backups and replicate them in multiple locations across different continents. This ensures redundancy and availability of data. Our automated provisioning scripts enable us to quickly set up the services in a new location. Restoring the data from the previous day's backup can be completed within a few hours for the largest clusters, with priority given to paid subscriptions.

It is important to note that we routinely utilize both the daily backups and provisioning scripts for our daily operations. This ensures that both aspects of the disaster recovery procedure are tested regularly and are reliable in case of a real disaster.

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

We are committed to maintaining the integrity and availability of your data, and our disaster recovery procedures are designed to minimize any potential disruption or loss.

- **Security**

All backups are stored encrypted using AES_128 and cannot be decrypted without secure certificate and master key.

- **Staff Access**

At SCS, we understand the importance of privacy and data security. In certain cases, our helpdesk staff may need to sign into your account to access settings related to your support issue. However, please be assured that they use their own dedicated staff credentials and do not have access to your password.

This special staff access serves two important purposes: it enhances efficiency and ensures the security of your data. By signing into your account, our staff can immediately reproduce the problem you are experiencing, eliminating the need for you to share your password. Additionally, this access allows us to maintain a comprehensive audit trail and exercise strict control over staff actions.

Please rest assured that our helpdesk staff is committed to respecting your privacy to the highest degree possible. They will only access the files and settings necessary to diagnose and resolve your issue promptly. Your data security and confidentiality are of utmost importance to us, and we take every precaution to safeguard them throughout the support process.

- **Data Protection Privacy Policy**

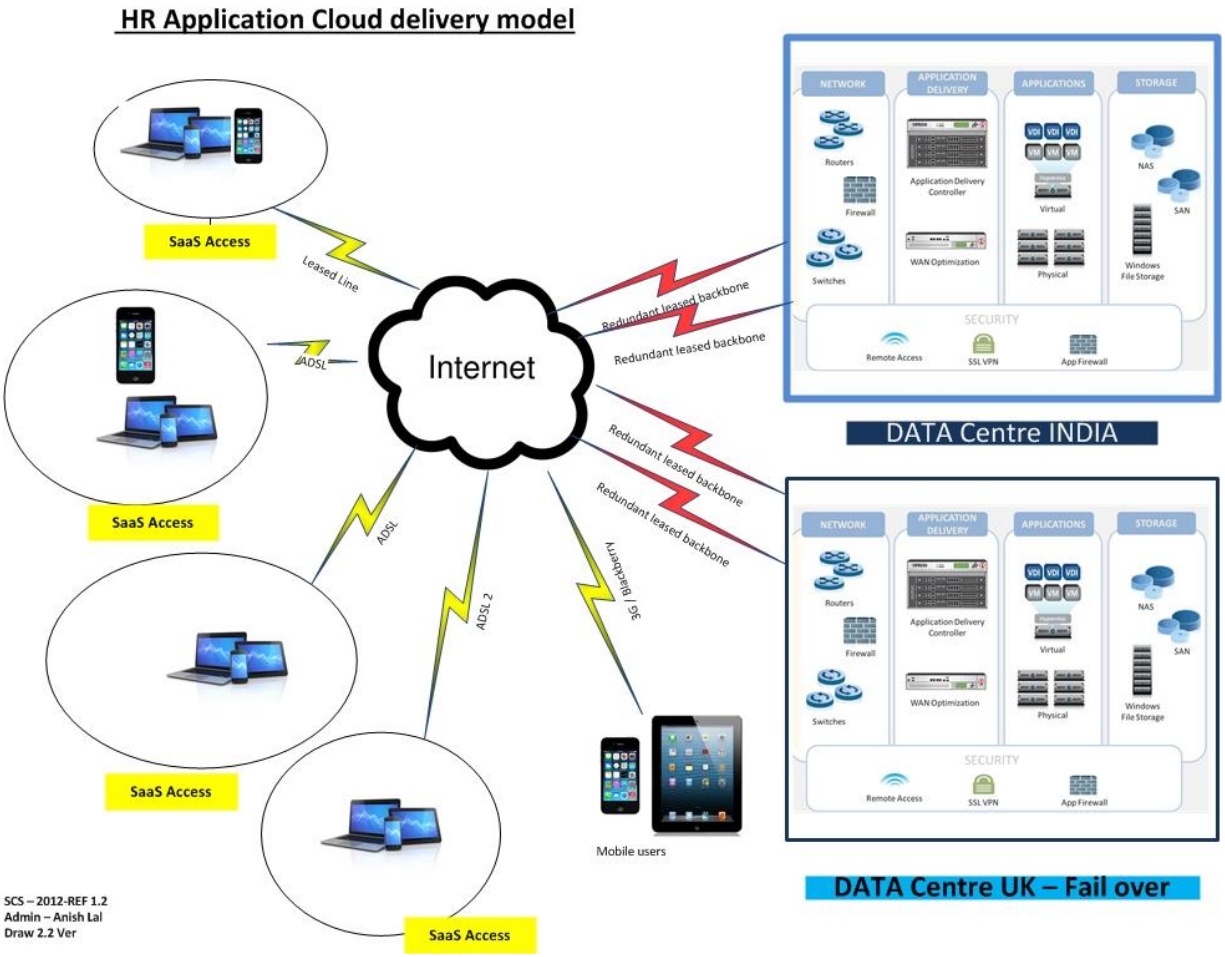
For more information on Data Protection Privacy Policy refer the documentation provided in the link https://www.smartcitysystems.com/privacy-policy.html

- **For further questions**

For questions related to this, please email us info@smartcitysystems.com

Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com

Birdseye view of SAAS delivery



Smart City Systems Software Services FZCO, IFZA Business Park, Dubai Silicon Oasis, Dubai, UAE
Tel: +971 4 2588814 Email: info@smartcitysystems.com