Synergita - Security FAQ

Synergita - Security FAQ

Security

Where Synergita is hosted & how secure is that environment?

Synergita is hosted in Amazon cloud environment. The infrastructure is secured by the following means.

- ISO 27001 certification for security
- Level 1 PCI compliance
- Successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- SOC1 & SOC2 Type 2 audit reports are published by Amazon Web Services

How do you ensure the data security?

By deploying industry standard security measures, Synergita ensures end-to-end security and privacy for tenants. All sensitive data are encrypted and stored in the database and also the access to database servers is highly restricted. The data is also protected by the implementation of multiple levels of data backup and disaster recovery strategy, which makes it possible to recover the data, during unforeseen failures.

Synergita performs security testing frequently & Application & network level securities are put in place to protect the software against the security threats like Distributed Denial Of Service (DDoS) Attacks, Packet sniffing, etc.

How do you protect the data from intruders?

Data-in-transit is protected by the implementation of SSL protocol to encrypt & transfer data between server and browser. The complex levels of encryption make it impossible for the intruders to decode & access the data. So your data is absolutely safe when you access Synergita over internet.

Will other customers be able to access my data?

Synergita product architecture ensures tenant data isolation in all the layers (View, Services, and Data). This architecture and our development practices automatically ensure that the tenant data do not mix-up between multiple tenant / tenant hierarchy. Data layer conducts additional validations to ensure the data retrieved belongs to the tenant of logged-in user. So you own your data and only you have access to your data.

Synergita - Security FAQ

1

How can I manage the data security and access privileges within my Organization?

Roles & Privileges - Using access control lists (ACLs) to determine who can access data in the application and what they can do with it. (For example, Employee Salary information will be visible only for few people in the organization – employee self, manager, HR manager and whoever is provided relevant access, e.g. CEO).

All the features are controlled by role based privileges and for each privilege, scope of data under consideration can also be configured. (For example, Department head can view the salaries of employees from his department only & not from other departments)

What happens to my data in-case if I decide to stop using Synergita?

Upon termination, Synergita will retain your data to a maximum of 60 days for your backup purposes. Later to that, Synergita will remove the data from the server and destroy the data.

1