quadient
Because connections matter.

V1.2 – January 2020

WTS Cloud

FAQ - IT Security

Where do you store customer's data? (Geographical localization)
Our WTS solution is hosted at Amazon Web Services (AWS) datacenter located in Europe (Dublin). AWS holds multiple certifications, especially ISO 27001 and SOC 2 certifications.

Does your organization have appropriate physical access controls in place to ensure only authorized staff have access to relevant systems?
AWS has its own policies and procedures that restrict physical access to the data facilities. AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.
We also restrict personnel access to all hypervisor management functions or administrative consoles on the principle of the least privilege.

Please provide an overview of your system / application architecture
Application server is hosted in a VPC (Virtual Private Cloud) at AWS segregated from unrelated hosts, access to database server is limited to requests only from that VPC.

What type of hardware, operating systems and user interface environment are supported on the desktop PCs or workstations?
WTS Cloud requires a PC with the following minimum features:

- Windows 7, Windows 8, Windows 8.1 or Windows 10

- 2 Ghz CPU, 32 or 64 bits
- 1 Gb RAM
- 50Mb free hard-disk space
- Microsoft .NET framework v4.0

WTS Cloud requires a web browser. The recommended and supported web browsers are Google Chrome, Mozilla Firefox and Microsoft Edge. It is recommended that you update your browser with the latest version to support the latest security fixes, performance improvements and internet standards. Microsoft Internet Explorer and Apple Safari are not recommended browsers and are not fully compatible with the WTS application.

WTS Cloud also requires a PDF reader Application to be set to look for updates automatically.

How is security handled by the application? E.g. authentication method, password controls, user access?

Our applications can only be accessed by registered users and their view depends on their privileges. Authentication is done with a user login and password.

If the application is web-based, does it support SSL/HTTPS? If yes, what encryption is supported?

Our web application has a standard RSA 2048-bit certificate to protect data in transit and supports TLS 1.0, 1.1, 1.2.

Does your platform have security protection against the OWASP Top Ten Web Application Vulnerabilities? This includes input validation, output escaping and SQL injection protection (e.g. parameterized queries)?

Our WTS solution uses NIST Cybersecurity Framework and the principles of OWASP. There are procedures in place to triage and to remedy reported bugs and security vulnerabilities for product and service offerings. We have the capability to rapidly patch vulnerabilities across all of our computing devices, applications and systems.

What measures do you have in place to provide assurance of the security of your products? E.g. application penetration test results, SSAE16 etc.?

The following intrusion detection solutions are in use: IPTABLES rules and Fail2Ban. Automated intrusion and security testing is conducted on software application periodically and prior to any software release.

Do you perform application penetration testing and vulnerability scanning? If not, do you permit external security tests to be conducted on behalf of your clients? Do you share the results?

Intrusion testing on WTS software are conducted periodically. We also encourage our customers to conduct their own security testing on WTS Cloud provided that they provide us with the report. If needed, we will deploy patches to cure any concerns within a reasonable time.

Do you have security incident response procedures in place to manage occurrences of incidents such as Denial of Service, website defacement, data breach and phishing?

We review applications for security vulnerabilities and address any issues prior to deployment to production.
Once an issue is identified, our process is to place issues into our current sprint for development. Once item has been developed it will be subject to peer code review and then will be passed to QA department that will review and test items. A hot-patch is generated for the solution in to our production environment for urgent patches.

Do you have malicious code protection (e.g. anti-virus, Intrusion detection systems)?

Application files regularly scanned against repository and synchronized to committed code. Expected content compared against application files, unexpected files quarantined and then removed if applicable and modified files are replaced if applicable.

Can you provide historical data concerning availability?

WTS Cloud committed uptime availability is 99,5%, on a monthly basis, excluding routine maintenance and downtime from interruption, termination, or failed operation of the Internet, private intranet, or of third-party telecommunication services and force majeure events.

What is your downtime plan (eg, service upgrade, patch, etc.)?

One week-end per quarter is reserved for service upgrade if necessary. Most of operations are done out of business hours.

How is client data protected?

Client data is stored in a secured sub network (MZ), which is not accessible from WAN, but only from web servers (DMZ).
Additionally, client Data is encrypted at rest at our data hosting location databases using AES256 encryption.
Direct access to database is restricted and can be done only by authorized staff.
Quadient guarantees and commits that customer data are not used for any business or any Marketing purposes.

How do you separate my customer data from other customers' data?

Customers' data are stored in a single database but data for each customer are logically segmented and encrypted so there is no risk of giving access inadvertently to another

customer's data. Access to each customer's data is available only through its unique account number.
As a chargeable option, we also offer our customers the ability to host their data in a dedicated database, out of the multi-tenant database.
Customer can also choose to have their own dedicated web server which is also a chargeable option, instead of sharing web server with other customers. Please note that sharing database server or web server does not represent any security threat as instances are created within separate processes that cannot share any information.

How is user access managed within your solution?

User can access only with their login and password. All requirements and trust levels for customers' access have been defined and documented.

What is end-user password policy?

Passwords are stored encrypted, hashed in SHA2.
Restrictions prevent users from using insecure passwords and reusing of old passwords.
Also, when a new user is created, she/he is required to change her/his password at first login.

What mechanisms are in place for clients to enter data in WTS Cloud?

Data entry related to packages and tracking information is performed manually through the application web site or using WTS mobile application.
Also, addresses and contacts can be imported manually or automatically via SFTP. And, WTS APIs are available that allow customer to transfer to and to query data securely from WTS Cloud.

What is data backup policy?

The WTS Cloud application server hosted on AWS is backed up nightly to an AWS snapshot.
WTS Cloud database backups also happen nightly and are transferred to an AWS file storage.
All backups are encrypted.

RTO (Recovery Time Objective) = 8 hours.
RPO (Recovery Point Objective) = 24 hours.

Do you have a rigorous testing and acceptance procedure for outsourced and packaged application code?

Each version is subject to code peer-reviews to detect security vulnerabilities and address any issues. We have controls in place to ensure that standards of quality are being met for all software development. Each version will be tested by our Software Quality Control team prior to deployment to production.

What about third-party apps (components) that you use in your services?

We only engage with 3rd parties and subcontractors who are compliant with necessary security and privacy laws. Each version is tested by our Software Quality Control team prior to deployment to production.

Will any third party, including government agencies, have access to my customers' data? If yes, under what conditions?

No, except if requested by law.

What data do you collect about my staff or other people related to my business operations (logs, etc.)? If data is collected, describe how and for how long it will be stored?

As the application gives the ability to track incoming and internal mail and parcels, we collect user, recipient, mail/parcel attributes information. We also keep logs when user makes changes to the packages as well as any notes related to the packages. These pieces of information can be used for support purposes such as bug fixing but are never used for any commercial purposes (marketing, stats, …).

Are there shared logs accessed by third parties with risk of revealing information about my staff and other related people?

No. Access to logs is strictly restricted to authorized staff. Log files are not shared with third parties. We keep only information about modification that each user has performed on the status of a package.

Also, all personal data is encrypted at rest at our data hosting location databases using AES256 encryption.

Do you have a high-level diagram documenting the information data flow of your application?

Yes. For WTS-Cloud we have the following high-level diagram with the schematic description of the data flow and the WTS Cloud architecture: