Platform security

At essensys we take security seriously. Our platform, network and voice services are built to keep you and your customers working in a safe and resilient environment 24/7.

A fail-proof platform

We understand that in today's digital economy, security is key to operating a successful business. That's why we have built in a variety of security solutions and processes to **safeguard your service delivery capabilities and customer data.**

Meeting security requirements

In today's flex-space market, occupier demands are soaring. With the influx of corporate tenants, IT and security requirements are a prime factor in winning or losing customers. Enterprise-grade technology and security purpose-built for multi-tenanted workspace environments are critical in meeting service demands of a wider market.

SaaS security

The essensys software platform is split across a tiered architecture: front-end application, secure API interface, and back-end database.

essensys ensures the **privacy and data integrity** through:

- TLS/SSL connections for all calls into the platform
- Dedicated secure management networks for communication between different platform components
- Secure encrypted interfaces provided by third parties for communication to third party internet-based platforms
- Secure fire walled environments
- Access is managed via individual username and password authentication
- The platform is closed and can only be accessed by an existing admin

audits

essensys undertakes regular audits on platform security and integrity. The most recent audit was finalised in **2019** and was conducted by an accredited third-party professional services partner.

Platform security

Network internet security

Our networks are connected to the public internet in order to provide ISP services and access to applications. To **protect the platform from any potential attacks**, several processes and solutions are in place:

- Firewalls to protect the essensys and customer infrastructure
- Network Address Translator is used for protection against non-initiated inbound traffic for those without public IP addresses
- essensys provides a powerful tenant VLAN solution for each customer provisioned on the platform to ensure tenant traffic only utilizes their assigned VLAN
- Guest wireless access is time limited and added through a shared guest VLAN

On-premise network security

essensys provide a powerful tenant VLAN solution for each customer network provisioned on the platform. This ensures **greater security and a better connectivity experience**

Wired Connectivity

- VLANs are provisioned based on port-allocation to each tenant
- All inter-VLAN traffic is denied
- Admins have the option to create a utilities network for communal services such as printing and scanning

Wireless Connectivity

essensys provide solutions for both residential, on-going end-users, short-term and guest access

- On-going residential end-users authenticate on the wireless LAN network via an individual username / password provided via Connect to gain network access.
- Authentication uses 802.1x, RADIUS, and permanently installed device certificates during the initial one-time configuration for each device.

Guest Wi-Fi

- Wireless LAN for guests is based on short-term access via a guest-portal
- Guests share a guest VLAN with no access to tenant VLAN traffic

Platform security

Enterprise-grade redundancy

We work in multiples - from data centers to internet providers - **to ensure we keep you and your customers online.**

Data centers

essensys operates from four Tier IV data centers located in the UK and USA, hosting our infrastructure, software and storage.

Our data centres are **SSAE16, ISO27001 and PCI-DSS accredited**, ensuring physical, network, data, and user security-based platforms

Voice services security

essensys operates a **hosted voice solution** from our secure data centres, delivering voice capabilities to end-users located on both operator premises and on the public Internet.

- The solution is based on the Session Initiation Protocol (SIP) for the majority of signalling between solution components.
- Secure WebRTC is also used for voice services provided to web-browser based clients.
- All non-WebRTC voice traffic runs on a separate secure VLAN across the essensys network, including on all operator premise.
- VLAN is accessible only via pre-configured MAC based admission. Non- authorised devices are not able to send or receive traffic on this VLAN.

The essensys solution supports the following devices: User desktop SIP phones; Communal area SIP conference phones; WebRTC based voice client; Analogue devices

Platform security

Voice services security

The essensys voice platform component is protected via a combination of **network firewall defences**:

- User Internet-based traffic is limited to encrypted secure WebRTC.
- The essensys Internet firewall protects the voice platform from all non-WebRTC traffic.
- The voice VLAN ensures that only devices with the correct pre-authorised MAC addresses are allowed to communicate with the voice platform.
- For communication with other voice carriers, traffic is via dedicated peering connections into the Data Centres.
- Utilization of voice fraud detection. essensys engineers are alerted to usage that may indicate potential fraudulent activity.

Voicemail & Call Recording
Part of the standard essensys voice offering, voicemail also provides specific security capabilities. Secure voicemail access is provided in two ways:

- Email attachment to an email address configured by the user in essensys Connect.
- Standard in-call mechanism provided by a PIN authentication.
- This PIN must meet minimum length and complexity requirements.
- A user will be locked out if the PIN is inserted wrong more than 3 times to prevent any potential breaches. This will be followed up by the essensys Support team.

essensys also provide an additional **call recording** capability for an extra monthly fee.

essensys administer client logins to enable clients to manage their own recording repositories. These **logins are specific to each client**, with no access available to recordings from other clients. When a client leaves essensys, their logins are removed. essensys regularly check the access capabilities of client login credentials.