essensys

Platform security

Contents

Overview 3
Platform security 3
Audits 3
Data Centres 3
SaaS Security 4
Network Internet Security 4
Operator Premise Network Security 5
Voice Services Security 5

Overview

essensys provide software and technology platforms specifically designed for operators, to help you manage your business from lead to cash and everything in-between.

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.

We look at security from a platform, network, voice and SaaS perspective.

Platform security

Audits

essensys undertakes regular audits on platform security and integrity:

- Upon every major release for SaaS (Software as a service) platform component
- Approximately every 18 months for ISP (Internet Service Provider), Network and Voice platform components

The most recent audit was finalised in December 2015 / January 2016. It was conducted by an accredited third-party professional services partner, specialising in penetration testing, software security analysis, and white-hat-hacking.

The audit was conducted in two parts:

- Audit of essensys ISP services
- Audit of essensys SaaS, network, and voice services

The audit was conducted from two different locations to test the security and integrity of our systems against attacks and uncover any vulnerabilities:

1) Off-net – from the public Internet, simulating an outside attack
2) On-net – from an operator premise, simulating an attack launched from a customer site

The audit found no critical or major issues for resolution. All minor issues across all audit scopes have since been remedied. All platform components are regularly patched and updated in line with vendor recommendations.

Data Centres

essensys operates from four Tier IV data centres located in the UK and USA for co-location, interconnects, and hosting of our infrastructure, software, and storage. The data centres are SSAE16, ISO27001 and PCI-DSS accredited, ensuring physical, network, data, and user security.

SaaS Security

The essensys software platform is split across a tiered architecture comprising of:

- front-end application
- secure API interface
- back-end database

essensys ensures the privacy and data integrity through:

- TLS/SSL connections for all calls into the platform
- Dedicated secure management network for communication between different platform components
- Secure encrypted interfaces provided by third parties for communication to third party Internet-based platforms
- Secure firewalled environment

Access to the platform is managed through username and password authentication. The platform is closed, meaning that access can only be granted by an existing administrator.

Upon invitation, users set their own password. This password is held in a hashed encrypted state within the platform database. Invalid login attempts force an account logout in order to protect against brute-force account compromise attempts.

essensys logs all changes made by customers that use the essensys - Connect - platform, to ensure that all customer action is traceable.

Network Internet Security

Our networks are connected to the public Internet in order to provide ISP services and access to applications. In order to protect the platform from a variety of potential attacks, several processes and solutions are in place:

- Firewalls are put in place in order to protect both the essensys and customer infrastructure
- For customers who have not purchased unique public IP addresses, a Network Address Translator (NAT) function on the firewall platform is used for protection against non-initiated inbound traffic
- No-access policy for management capabilities from the public Internet – secure VPN connectivity must be used
- Monitoring solution and traffic black-hole capability for detecting and minimising impact of Denial of Service (DOS) attacks, against either the essensys infrastructure or customer networks.

Operator Premise Network Security

essensys provides a powerful tenant VLAN solution for each customer network provisioned on the platform. This ensures that tenant traffic only utilises their provisioned VLAN.

For wired access, these VLANs are provisioned based on port allocation to each tenant. All inter-VLAN traffic is denied, with the option to create a utilities network for communal services such as printing and scanning.

For wireless LAN connectivity, essensys provides solutions for both residential ongoing end-users, or short-term guest access. Ongoing residential end-users authenticate onto the wireless LAN network via username / passwords provided via essensys Connect to enable access to the wireless network, and to gain access to their tenant VLAN. Authentication uses 802.1x, RADIUS, and permanently installed device certificates during the initial one-time configuration for each device.

Guest wireless LAN access is based on short-term access via a guest-portal mechanism. Access duration is time limited. Guests are added to a shared guest VLAN, with no access to tenant VLAN traffic.

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. This 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 types of end-user "devices":

- User desktop SIP phones

User desktop SIP phones authenticate directly to the essensys platform using a username (based on the full national number) and pre-assigned unique password combination. Access to the configuration settings on the device is not provided to the end user, and cannot be altered. The SIP phone traffic is carried exclusively on the secure voice VLAN.

- Communal area SIP conference phones

Communal area SIP conference phones communicate securely with the essensys platform via a secure hard-configured interface and hard-coded authentication. These devices also run exclusively in the secure voice VLAN. Access to the configuration settings on the device is not provided to the end user.

- WebRTC based voice client

For remote voice service away from the user's desk, a WebRTC based voice client is provided via the essensys – Connect - platform, which runs in a web-browser interface. This traffic is encrypted WebRTC, to enable secure communication from the client to the essensys platform over the Public Internet. Authentication for the voice services in essensys Connect is provided by the user's essensys Connect login credentials.

- Analogue devices

Analogue devices via an Analogue Terminal Adaptor (ATA). The ATA communicates securely with the essensys platform via a secure hard-configured interface from its location in the secure operator comms room, and runs in the voice VLAN.

The essensys voice platform component is protected via a combination of network firewall defences combined with user-interface and network-interface Session Border Controllers (SBC).

- User Internet-based traffic is limited to encrypted secure WebRTC. The essensys Internet firewall protects the voice platform from all non-WebRTC traffic.
- For traffic from customer premises, the voice VLAN ensures that only devices with the correct pre-authorised MAC addresses are allowed to communicate with the voice platform. A firewall and SBC further protect the voice platform from any other traffic types.
- For communication with other voice carriers, traffic is via dedicated peering connections into the Data Centres. This traffic traverses both the essensys carrier firewall, as well as the SBC. Voice traffic to other carriers can route unencrypted over the public internet should a primary connection to another voice carrier fail.

To further protect, and detect, any unauthorised usage of the voice services, we utilise voice fraud detection in the platform, and via our voice interconnect carrier providers.

essensys engineers are alerted to usage that may indicate potential fraudulent use of services, enabling further investigation into the legitimacy of this traffic.

Voicemail is also part of the standard voice service offering, and also provides specific security capabilities. Secure voice mail access is provided via two mechanisms:

- Delivery of voice mail as an email attachment to an email address configured by the user in essensys Connect.
- Voice mail retrieval by a standard in-call mechanism. This is provided by a PIN based mechanism for authentication.
    - PINs must meet minimum length and complexity requirements (i.e. avoiding concurrent digits, repetition of digits, etc). As essensys do not supply a default PIN, even if a user does not change it, authentication is still secure.
    - Inserting a wrong PIN more than 3 times will lock the user out to prevent any potential breaches. essensys support receives an email is someone gets locked out so that we identify any attacks.

The functionality for setting up call forward from in the voice mail platform has been disabled in order to de-risk fraud potential.

essensys also provide an additional optional call recording capability for an additional monthly fee. When coupled with the relevant processes, our clients can meet FSA requirements as outlined on their website.

Businesses that require call recording under FSA policy need to ensure their end-to-end processes meet guidelines for their business type. The essensys voice platform has not been certified as PCI DSS compliant.

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.