



Secure Mobile Gateway

Secure Mobile Gateway is an additional software component providing Web Access to existing Adroit graphics, giving you secure remote access on any device anywhere.

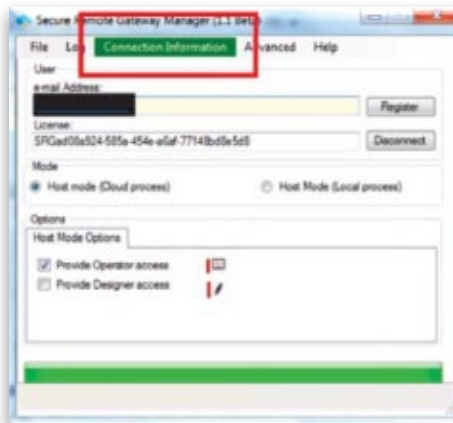
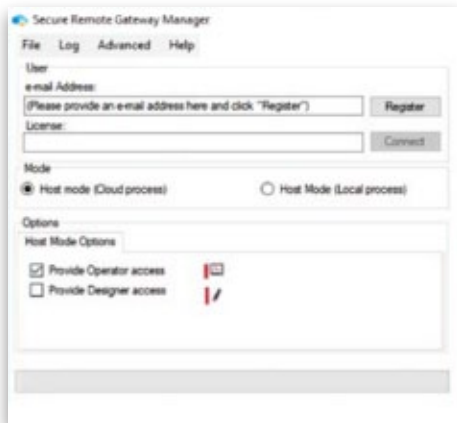
Key Features and Benefits

- Secure Mobile Gateway is an additional software component providing Web Access to existing Adroit mimics, giving you secure remote access on any device anywhere.
- Secure Mobile Gateway technology provides web browser (Edge, Firefox, Chrome, Opera, etc.) access from any device. User interface graphic forms can be designed for display on any device that supports an HTML 5 browser.
- Secure Mobile Gateway requires no open firewall ports.
- A secure channel is initiated from the client-side, preventing any direct exposure to sniffing, DDOS attacks, and hack attempts.
- Additional IT infrastructure changes or open inbound ports are not required (uses HTTPS). Direct HTML 5 representation of the operator is provided.
- The solution is application-specific and specifically designed and optimised for the operator.



- Secure Socket Layer (SSL 2.0) implemented (RFC 4419/4432/6594 compliant) - literally used by millions of organisations worldwide to provide secure communication channels.
- HTTPS and TLS (Transport Layer Security) to ensure secure web connectivity. (TLS 1.2, AES128 with SHA256)
- Provides optional 2FA (Two-Factor Authentication) - Can be used to provide additional security.

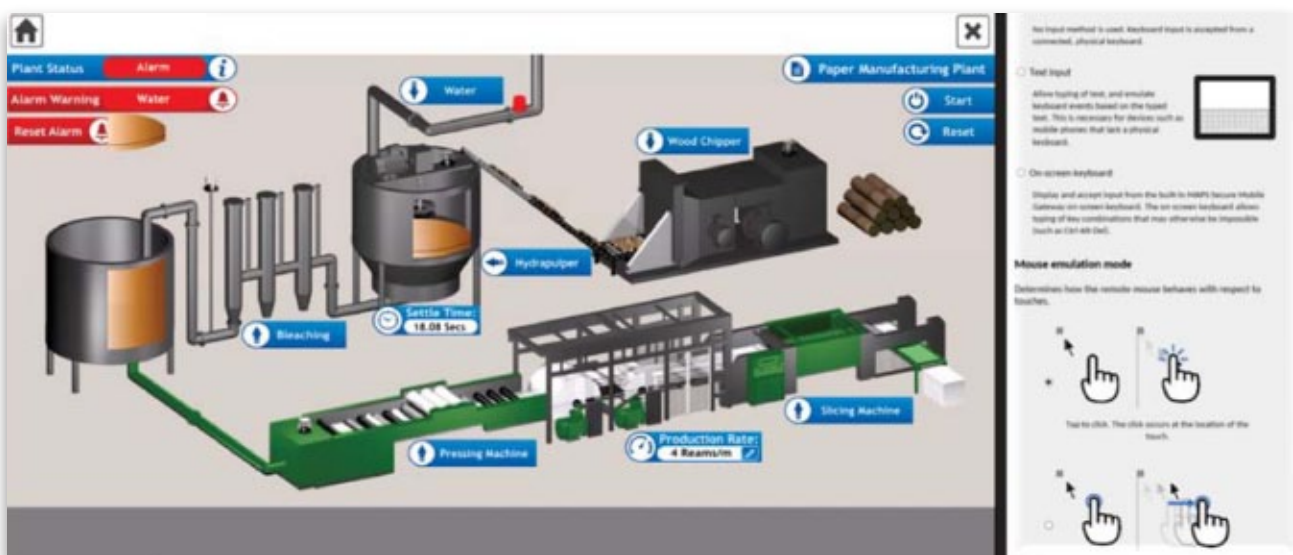
Architecture and Configuration

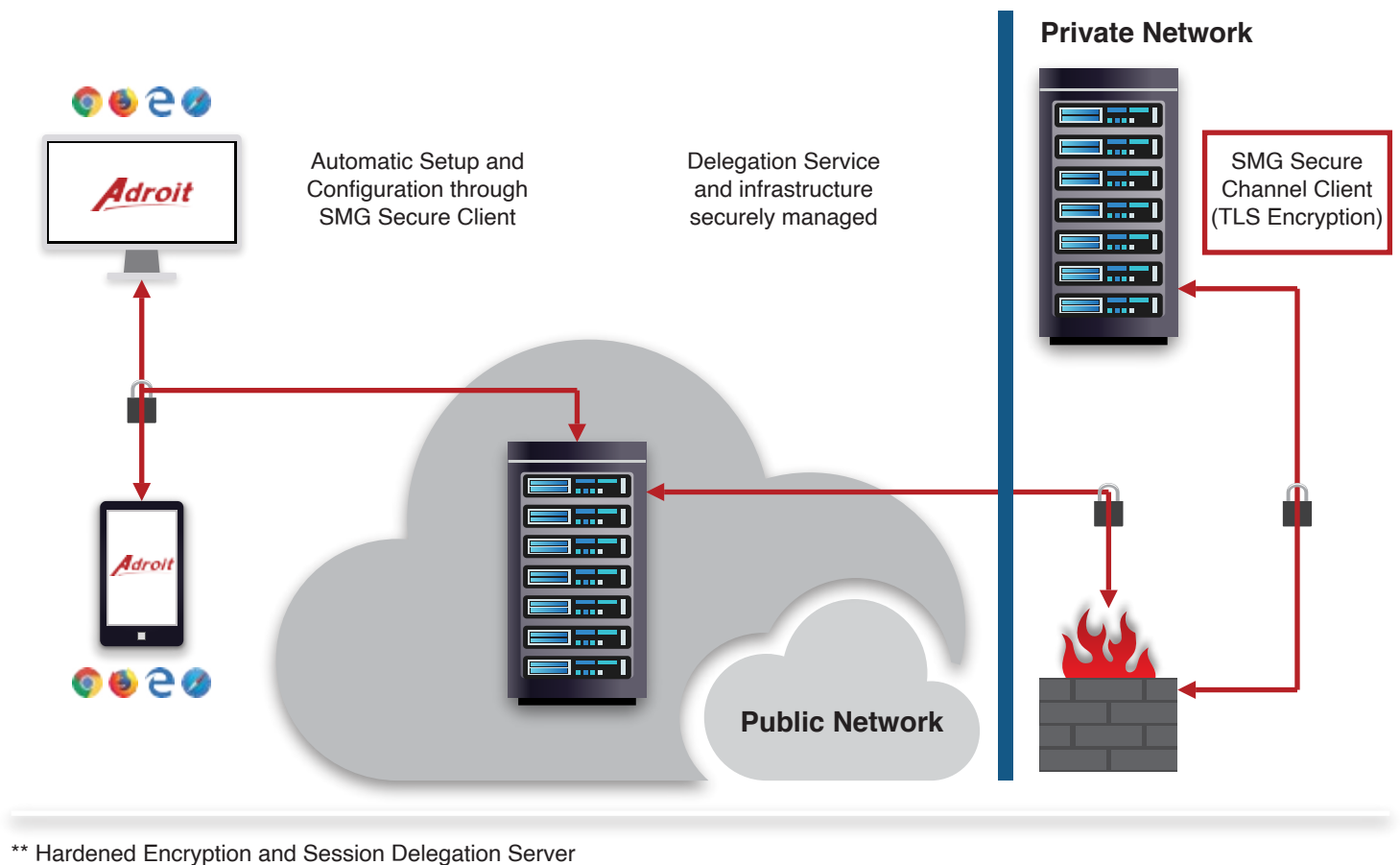


- By default, 2 simultaneous connections are supported for each registration. If more connections are required, please contact your salesperson.

PLEASE NOTE: A maximum of 10 simultaneous connections can be supported.

- An Adroit client license is required per Cloud operator.
- The Secure Gateway Client Manager determines whether a local Adroit Operator is installed. If found, it contacts the Secure Cloud Delegation Server and configures an Adroit Cloud Operator with the same encrypted credentials and connection information as the local Adroit Operator.
- An Internet connection of at least 2Mbps is recommended
- Operator scaling is configured for 1920 x 1080 (Full HD).
- Redesign of the project for Mobile devices is not required. However, this can sometimes be preferred if the current level of detail on the graphic forms is too much for smaller form factor devices.





Security

The Secure Gateway makes use of several mechanisms to ensure confidentiality and integrity:

Secure Shell SSH 2.0: SSH is a cryptographic network protocol for operating network services securely over an unsecured network. This protocol is used widely by commercial and governmental organisations to establish a cryptographic network channel and ensure the confidentiality of the underlying communication. The encryption protocol is used to establish an encrypted channel between the Secure Mobile Gateway Client Manager and a Cloud Delegation Server. The protocol implementation that forms part of the Secure Mobile Gateway will only connect to a trusted set of Cloud Delegation Servers as identified by their public/private key pairs.

HTTPS: Web-based access is provided via HTTPS only and all traffic is encrypted between the Browser and the Cloud Delegation Server.

Cloud-based process: If the “Cloud process” host mode is used, the actual Operator process does not run on the Host infrastructure, but rather in a protected sandbox environment on one of the trusted Cloud Delegation Servers.

Talk To Us

Website: www.adroittech.co.za
 Sales Enquires: sales@adroit.co.za
 Technical Support: support@adroit.co.za
 Contact Tel No: +27 11 658 8100