Security

We take great care for data security and data privacy. There are two main security points to protect:

- from browser to Green Screens Service
- from Green Screens Service to IBM I.

For both segments we have enabled security measures to maximally protect sensitive data.

Green Screens Service

- Passwords encrypted in configuration files - all saved sensitive data in configuration files are encrypted.

Green Screens Service to IBM I

- SSL support - standard SSL certificate encryption is supported if SSL in configured on IBM I.
- Encrypted terminal sign-on - encrypted password exchange is used if bypass sing-on is enabled. IBM password exchange specification. (RFC 2877 sec. 5)
- Telnet exit program access control - during terminal connection handshake, terminal parameter PROXYIP containing client workstation IP (proxy mode - NGINX) and PRINCIPAL – Windows user will be sent to the IBM I. Values can be used in custom telnet exit programs to control workstation access.

Browser extensions

- Sensitive data is encrypted with non-exportable and non-shareable password.
- Cloud synchronization is disabled to protect saved macros with sensitive data.

External services usage

- We do not track user behavior or user location in any of our products
- We do not use any online analytics
- We do not exchange data in any form with any external services

Browser to Green Screens Service

- Protocol encryption on plain http - All data is encrypted with RSA and AES encryption keys at the browser side before they are sent over the network even SSL protocol is not used.
- Received terminal data is hashed and compressed with custom algorithm.
- SSL support - standard SSL certificate encryption is supported out of the box.
- SSL certificate access control - user certificate access can be controlled by certificate OU group if highly restrictive client SSL certificates are used.
- IP filtering engine - embedded IP filter engine to control access by IP address or IP ranges. Engine have features to allow or block specific addresses or to run in learning mode to log all remote IP addresses that are accessing the system.
- Browser fingerprint access control. Every browser session has unique ID based on browser properties. ID's are used to prevent generated web terminal URL address reuse.
- Web terminal URL parameters are encrypted with non-shareable instance based keys.
- Enforced bypass sign-on. If enabled, login page with encrypted password exchange use is mandatory instead of standard 5250 sign-on screens. This enables encrypted login on 5250 sign-on screens supported by IBM password exchange specification. (RFC 2877 sec. 5)

2FA – 2 Factor Authentication

- Fully compatibile with RFC 6238 - TOTP: Time-based One-time Password
- Requires OTP mobile application for verification
- Register and validate user against IBM I platform

FIDO Authentication

- Fully compatibile with FIDO2 standard
- WebAuthn standard for web terminal and web admin console
- Mobile biometric access control full support
- Hardware keys as Yubico or Google Titan are fully supported

2-Way authorization

- Web login through locally encrypted QR-Code requires Green Screens Mobile application for authorization.
- Prevents keyboard loggers to hijack sign-on username and password.
- Enable secure web terminal access from unsecured locations

Access control

- IP Filtering engine – IP filter support with wildcards and learning mode.
- Mobile filtering engine – mobile apps have unique ID for identifying installation. Used only by connected service to control device access. Stolen devices can be easily blocked from access.

Login access

- Through Green Screens login page – from browser
- Through Green Screens browser extension (Chrome, Firefox) – from browser
- Through Green Screens Web-API - from browser
- Through Green Screens Web without API (hastag use) – from browser
- Through Green Screens server-side-API (PHP sample on our GitHub) – from server side
- Through Green Screens Mobile application - directly from mobile application
- Through Green Screens QR-CODE bar-code - used by mobile app to request conenction
- Through Green Screens PDF-417 bar-code - used to easily configure mobile app

NOTE: Connection data is never sent unencrypted whichever mode is used. All listed methods will generate url link in format //SERVER:PORT/lite?d=***&k=***&v=*** where:

- d - dynamic AES encrypted JSON data with login parameters
- k – AES key encrypted with RSA public key (only server has temp. private key for decryption)