ITmanager.net

Security White Paper

Our mobile apps are a thick client architecture, meaning most of the logic is inside the client app, for example when we perform SSH connections our client is using the libssh2 framework in order to perform an ssh connection directly from the mobile device to your target server. If the target server is located behind a firewall and your device is on a cellular connection, you have 3 connection options:

1) Use your own VPN client. This will disconnect you from the ITmanager.net Cloud Service. No information is relayed back to ITmanager.net
2) Expose your servers to the internet (highly not recommended)
3) Use our Enterprise Server to tunnel into your network. Benefit, install only once and you are always connected

Our Enterprise Server is a cloud hosted SSL VPN, it acts much like Gotomypc, logmein, BES or Dropbox. The goal of the Enterprise Server was to make it easier for users to setup VPN connections, without having to buy additional hardware or open any ports. The Enterprise Server's only role is to tunnel tcp connections from your mobile device to your servers, it connects to our cloud infrastructure using an SSL connection, then when your mobile device needs to make an internal connection the mobile device will first connect to our cloud infrastructure with SSL, then our infrastructure will match up your client connection with your Enterprise Server connection and tunnel the data. So for example if you're performing an SSH connection then the connections are encrypted twice, once by SSL by our tunnel and then again by SSH end to end from your mobile phone to your target SSH servers.

If your are managing other things such as Active Directory, VMware or others, then the connection is encrypted end to end with SSL as well as our tunnel SSL.

Your ITmanager.net account credentials are salted and hashed when stored on our servers, we do not store any credentials in plain text. All communication between our client and our servers is over SSL, and authentication follows the JWT spec. If you choose to store your connection profile passwords in order to sync them between devices, then they are also encrypted using a hash of your password as the secret key before storing them. (although saving them is entirely optional, you can be prompted every time you connect instead). We support 2 factor authentication in our apps and also support a keychain system in order to share credentials between many saved connection profiles.

We support touch ID on Android and Ios. We also support Face ID on iOS