MeshCentral^2

Security Features

MeshCentral was architected from the start with both security and easy of use in mind. This document highlights the security features present in MeshCentral that makes it unique as an open source remote management server.

Two Factor Authentication. Passwords are not sufficient to protect users anymore. With support for two factor authentication, remotely managed assets are better protected against password disclosures.

Let's Encrypt Support. With built-in support for Let's Encrypt, MeshCentral can obtain a valid TLS certificate for the domain name and auto-renew the certificates making it easy to establish trust to users.

Strong Cryptography. By default, strong cryptography is used including SHA384, AES256 and RSA3072. This is a step above the industry and recommended good practice for quantum computer resistance.

Use of TLS 1.2. Strong security includes use of strong cryptographic transport protocols. MeshCentral makes use of TLS 1.2 on it's HTTPS port 443 and disables use of weaker generations of TLS on that port.

Strong Password Enforcement. By optionally requiring that users make use of strong passwords and requiring use of two-factor authentication, user accounts security can be improved.

Database Record Encryption. If enabled, MeshCentral will encrypt all sensitive fields before storing then in the database. This can be done in addition to database provided encryption for extra security.

HTTP Content Security. To secure against any possibility of unwanted cross-site scripting and other attacks, MeshCentral's HTTP headers includes browser instructions to limit the source of content that is loaded.

FIDO2 support. With built-in support for hardware authentication keys (Bluetooth, USB and NFC) administrator can setup an extra factor of authentication that defends against fishing attacks.

IP address token binding. All session tokens and cookies generated by MeshCentral are bound to the requester's source IP address making it impossible for malware stolen tokens to be reused at a different location.

Reverse Proxy Support. By supporting reverse proxies, MeshCentral can be installed in most modern data centers without having MeshCentral know the main HTTPS private certificate key.

HashiCorp Vault Support. MeshCentral can be configured to retrieve and store all configurations settings and secrets in Vault, making the server stateless and adding an extra layer of protection.

Strong Password Hashing. By default, MeshCentral account passwords are hashed using PBKDF2 with 12000 rounds of SHA384 and a 128 byte long salt providing security and dictionary attack resistance.

No software can be fully secure. For any security issues or concerns, contact the developers at:

MeshCommander.com/MeshCentral2