FileWave Security

FileWave SSL Certificates

Using self-signed certificates should be avoided as much as possible in production environments; while it may make sense in some closed environments, using Globally trusted CAs is our recommended approach.

The FileWave Server and other FileWave Components (e.g. Clients, Web Console, IVS, etc.) use the MDM server SSL certificate to validate communication. This certificate needs to be uploaded into the SSL Certificate Management pane, in the General tab inside FileWave Admin Preferences. This validation check will ensure secure and trusted communication between your FileWave server and the various FileWave components in your environment. Even though a self-signed certificate is supported, having a root trusted certificate from a CA is the best and most recommend option.

- For more information on creating a root trusted certificate
- How your FileWave environment will be affected by have a self-signed certificate
- Let's Encrypt Setup for FileWave Server (Debian)

Security and FileWave

FileWave uses SSL, certificates, and secure tokens for much of its primary device and content management. Fileset technology is a patented, proprietary wrapper for content. Instead of sending a standard .pkg or .msi installer packages to the client, we wrap the content inside a Fileset. Because this is a proprietary container, the integrity of the delivered content is assured.

FileWave client security

Communications between the FileWave Client and either the Server or any Boosters is done through SSL.

The FileWave Client is tracked by device name in Inventory. Admin changes to Client configurations are either done through a specific Fileset, called a Superprefs Fileset, or through the Client Monitor. The contents of a Superprefs Fileset are secure from external packet sniffing, package viewer tools, and brute force access. The Client Monitor settings are protected by a unique password assigned by the FileWave Admin at the time of installation of the FileWave client. This password is not readily available to the device's local administrator.

FileWave Server security

The FileWave client communicates to the FileWave Server using SSL. The FileWave server supports multiple sub-administrators. The biggest concern is proper password and account management; but each sub-admin can be limited as to their level of access to clients, Filesets, and services.

- Securing FileWave Server on the Internet for Remote Device Management

Client tracking

A device can be tracked from FileWave Admin. Activating tracking involves setting the client state of the device to Normal and the current user of the device will receive a notification asking them to approve tracking (iOS and OS X only). Android devices will request that all client permissions be granted at installation, and Windows devices do not provide any user notification. Only devices on Wi-Fi will be tracked.

These tracking options can be disabled for any FileWave administrator account by modifying their permissions in the FileWave Admin. You can also have a global change on your FileWave license by requesting to disable Personal Data Collection. Keep in mind, disabling Personal Data Collection will not only prevent FileWave from gathering location data but also other personal data on the device.

Disaster recovery

Backup of both the server environment and end user data are critical areas of planning. Backup of your servers can be as simple as taking snapshots of the VMs at regular intervals. The FileWave server is running a database using SQL, and as such, you cannot use normal backup solutions to insure its safety. Use the information on the FileWave Support site to make sure you properly back up the server.

- Automated Backup

Revision #7
★Created 12 July 2023 01:37:59 by Josh Levitsky
✎Updated 23 April 2024 14:39:42 by Josh Levitsky