Security best practices

To keep your upKeeper environment to the highest standards and secure you should follow points outlined in this document. Diverting from this document should only be done if necessary and reason should be noted.

File sharing

- In an environment where computer clients and file distribution points (servers) using Microsoft Windows as operating system and belong to a common Microsoft Active Directory you should use system account for file share access instead of username and password.
- If username and password are used for accessing a distribution point. Rights for this user should be limited to read and only granted access to one specific distribution point.
- File sharing thru SMB should be replaced with HTTPS where suitable.

Configuration

- How long you can be logged in to upKeeper Manager can be adjusted. Default is set to ninety (90) days and should be adjusted to your organization needs. Maximum number of days recommended are five (5) days.

Administrators

- Users of upKeeper Manager environment should be configured with MFA (Multi Factor Authentication).
- User that can not use MFA should be limited to login from specific IP address.
- If users can not use MFA or IP address limitation extra complex password should be implemented.

Communication

- Communication with administration API should be configured with certificate for SSL traffic.
- Communication with client API should be configured with certificate for SSL traffic.

Redundancy

- upKeeper components should be separated on different server resources to maintain high availability and make update of underlying components possible, even under production.
- upKeeper client endpoint should be installed on dedicated server resources in upKeeper environments with large number of clients or where availability is of highest importance.

upKeeper update

- Communicate planned upgrades of upKeeper Manager to upKeeper Solutions so that support personal can be made available if needed.
- upKeeper Manager should be upgraded to latest version within six (6) month of release date.
- upKeeper Client components should be upgraded to the server version within six (6) months of the server upgrade.
- Certificate used in upKeeper environment should be updated not later than one (1) month before expiring.

Server environment

- upKeeper environment should be installed on server resources compliant to requirements specified for selected upKeeper version. Requirements is specified in “Installation prerequisites” document available with each new version.

- Server operating system and other server components should be updated with “Quality updates” according to Microsoft recommendation or established update policy.
- Server operating system and other server components should be upgraded with “Feature updates” according to Microsoft recommendation or to organization established update policy.
- Server resources used in a upKeeper environment should only have necessary server features activated.
- Firewalls on server resources should be configured and only admit traffic necessary for upKeeper Manager, server infrastructure and server maintenance.
- Users with access to server resources should be limited to users that need access for specific server resource and activity should be traceable.
- Password for users with access to server resources used by upKeeper should be complex and include MFA (Multi Factor Authentication).
- Users with access to server resources should be documented in a secure way.
- Users with access to server resources should be handled in your routine for users beginning and ending to work with the environment.

Computer clients

- Computer client should be locked down according to best practices by manufacture.
- Users on client computers should not direct or indirect belong to the local administrators group.
- Client computers should have a well-known and updated antivirus software.
- Firewalls on client computers should configured to only admit traffic necessary for these three scenarios: organization domain, private network, and public network.
- Client computers should be configured to get operating systems updates according to manufacture recommendation or to organisation established update policy.
- Client computers should be configured with finger or face recognition so that extra complex passwords can be used.