

Active Directory Integration with GateKeeper

Manage AD Accounts with GateKeeper Enterprise.



GateKeeper Proximity – Active Directory

GateKeeper is a proximity based two-factor authentication solution that uses Bluetooth tokens in combination with a PIN to provide secure access to domain joined computers for an organization.

Why would this feature be useful to me?

By integrating GateKeeper Hub with the organization's Active Directory, admins can manage AD accounts directly from the GateKeeper Hub website.

1. Admins can use the AD management feature to set complex passwords for AD users, without even telling the users what their AD password are.
2. Since the users are using GateKeeper for authentication, they don't need to know their AD passwords at all.
3. Finally, revoking access for employees leaving the organization is simplified because now you can not only remove the GateKeeper tokens from a user's profile, but you can also disable the user's AD account through the Hub.



How does GateKeeper work with Active Directory?

With GateKeeper Hub, admins can make instantly update users, PCs, passwords, and tokens the on-premise Active Directory (AD). Once a user is added to the Hub, the admin can fetch the AD credential for that user. Then the admin can make changes to the user's AD profile through the Hub, such as reset their password, unlock their account, or disable account. This allows admins to on-board new employees by giving them AD accounts and assigning them GateKeeper tokens simultaneously.

