GATEKEEPER

Client Application Reference Guide For Windows and Mac

UNTETHERED LABS, INC.
support@gkaccess.com

Contents

1 What is GateKeeper?

GateKeeper is an access control system that authenticates users into computers and websites based on their proximity. GateKeeper provides secure and fast methods of locking and unlocking your computer while saving users the time spent typing long passwords. Companies benefit with reduced help desk calls and never a forgotten password again.

The GateKeeper comes with a wireless key, Halberd, that the users carry around with them, a 3V CR2450 lithium coin cell battery, USB dongle for the computer, lanyard, and instruction manual.

1.1 What is the GateKeeper desktop application?

The GateKeeper desktop application pairs the token to the user's domain/local and web credentials. Once connected to the user's token, the desktop application automatically locks/unlocks the computer based on the user's proximity.

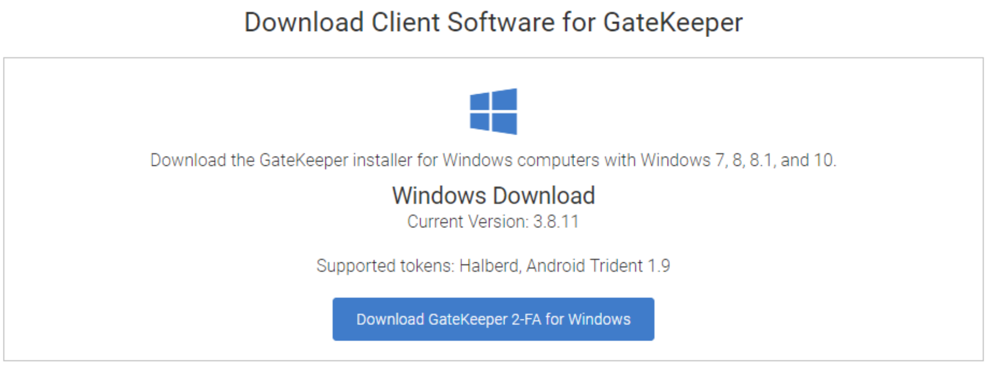
1.2 What is the GateKeeper Chrome extension?

The GateKeeper Chrome extension is the web password manager that installs along with the GateKeeper application and provides users secure access to their web login credentials. Its capabilities include auto-filling usernames and passwords, supports password generation, and two-factor authentication to generate OTPs which eliminates the need for apps such as Google Authenticator. It is also capable of capturing QR codes to generate OTP secrets.

2 GateKeeper Application Installation

To download the desktop application, go to our website https://gkaccess.com/downloads/ and click on the appropriate version for your computer (Win or Mac).

If you've downloaded the Windows version of the GateKeeper application, please find the installation instructions listed under Section 2.1. If you've downloaded the Mac version of the GateKeeper application, please go to Section 2.2 to find the installation instructions.



Download Client Software for GateKeeper

Download the GateKeeper installer for Windows computers with Windows 7, 8, 8.1, and 10.

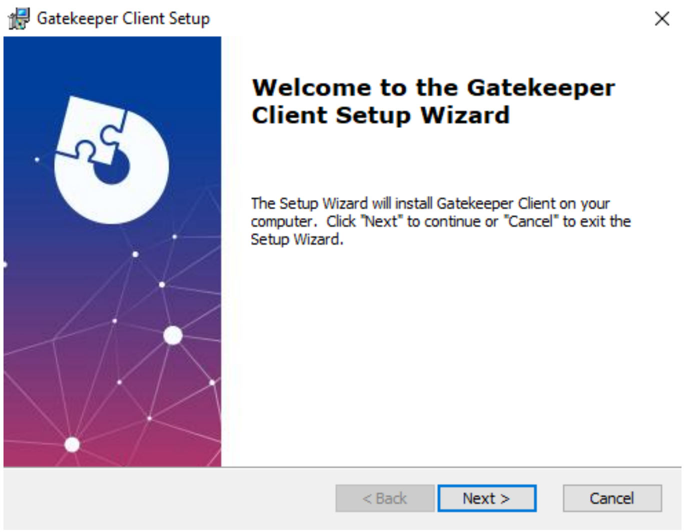
Windows Download

Current Version: 3.8.11

Supported tokens: Halberd, Android Trident 1.9

2.1 Windows Installation

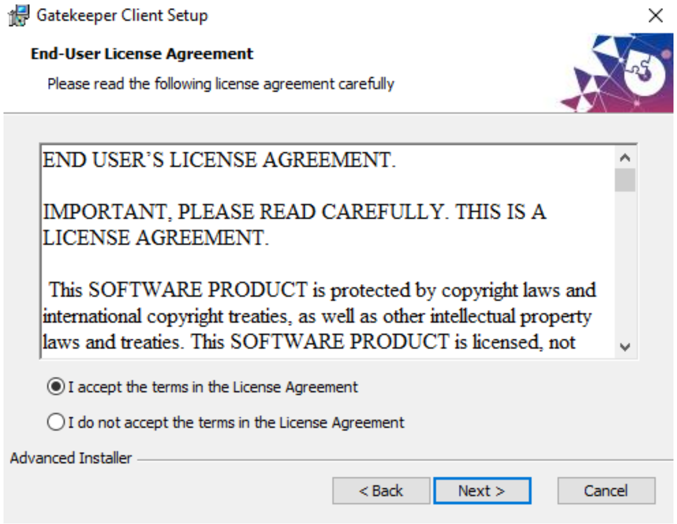
Run the downloaded application and click on **Next** to continue.



Welcome to the Gatekeeper Client Setup Wizard

The Setup Wizard will install Gatekeeper Client on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Accept the terms and conditions and click on **Next** to continue.



Gatekeeper Client Setup

End-User License Agreement

Please read the following license agreement carefully

END USER'S LICENSE AGREEMENT.

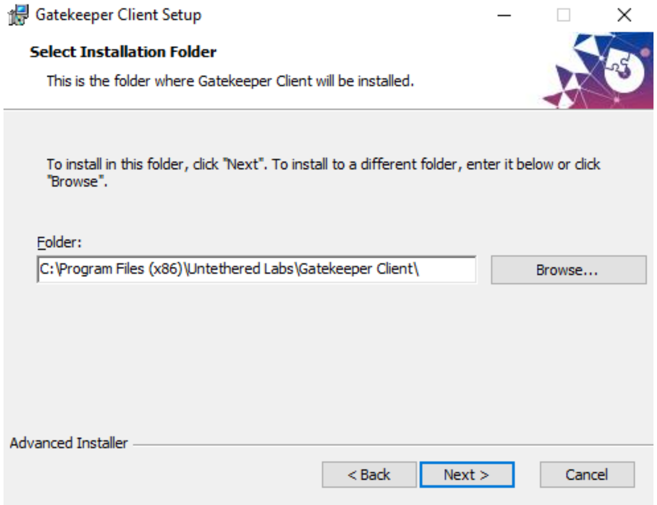
IMPORTANT, PLEASE READ CAREFULLY. THIS IS A LICENSE AGREEMENT.

This SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This SOFTWARE PRODUCT is licensed, not

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Select the location where you'd like to download the application and click on **Next** to continue.



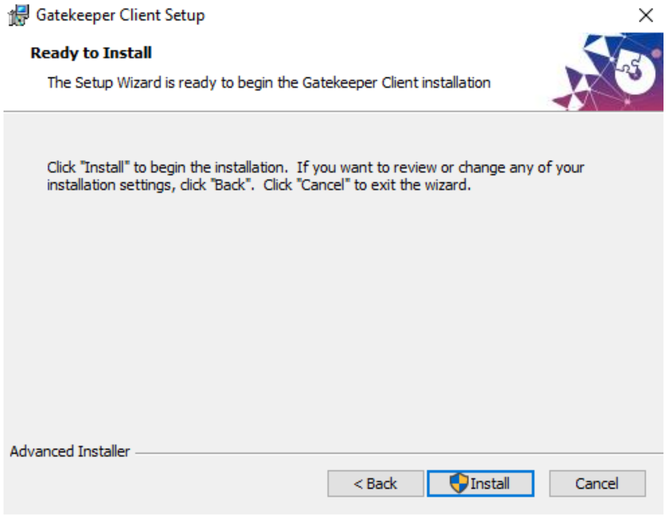
Gatekeeper Client Setup

Select Installation Folder

This is the folder where Gatekeeper Client will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\Untethered Labs\Gatekeeper Client\



Gatekeeper Client Setup

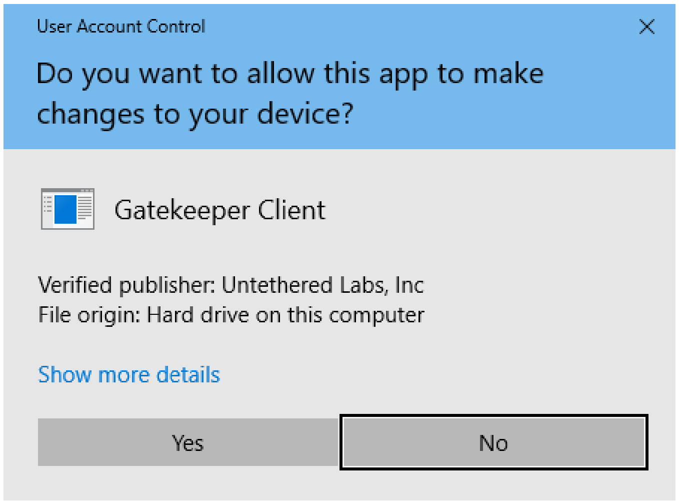
Ready to Install

The Setup Wizard is ready to begin the Gatekeeper Client installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Click on **Install** to start installing the application.

Click on **Yes** to allow the program to make changes to your computer.



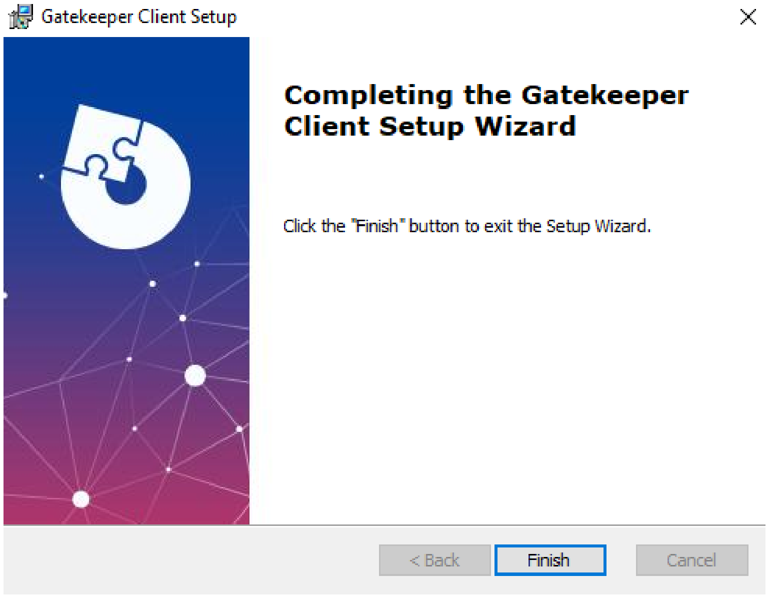
User Account Control

Do you want to allow this app to make changes to your device?

Gatekeeper Client

Verified publisher: Untethered Labs, Inc
File origin: Hard drive on this computer

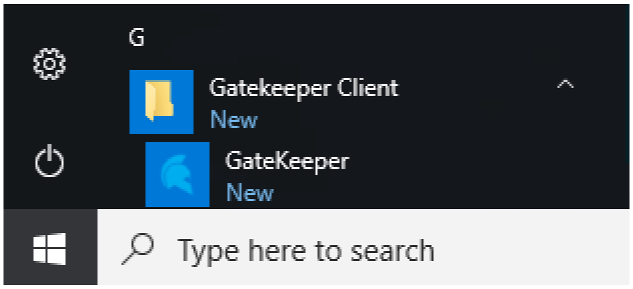
Please wait while the installation finishes. Then click on **Finish**.

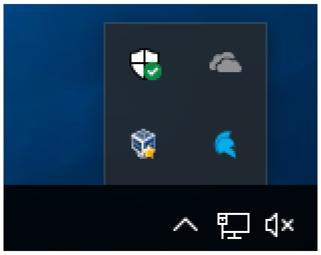


Completing the Gatekeeper Client Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

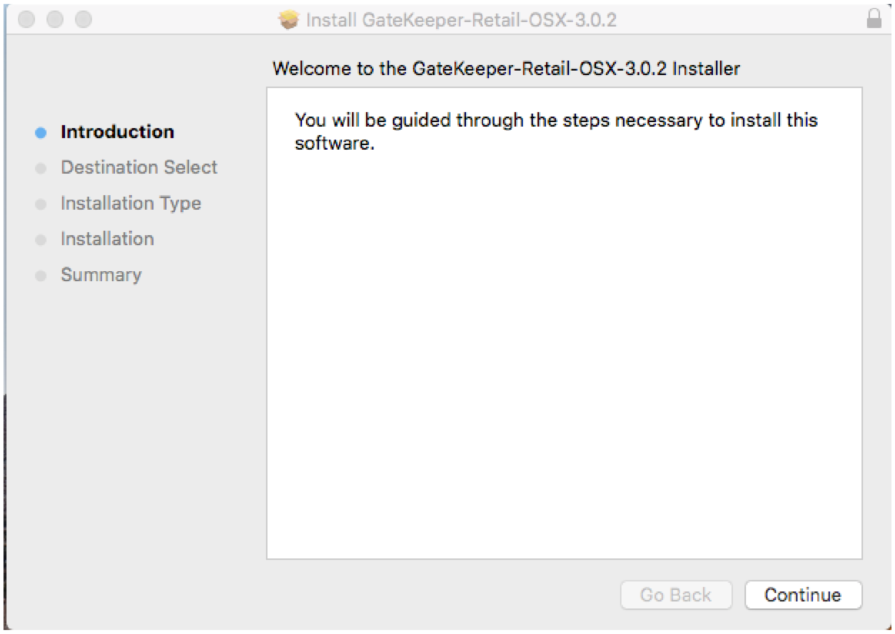
Launch the GateKeeper application from the **Start Menu** or by clicking on the GateKeeper icon on the taskbar.





2.2 GateKeeper macOS Installation

Download and run the macOS installer package on your Mac.

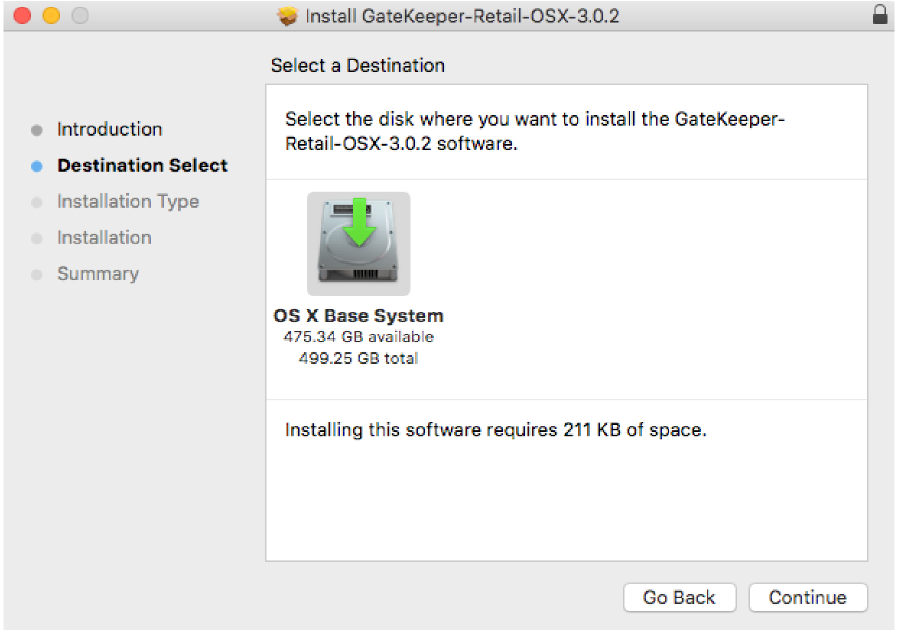


Install GateKeeper-Retail-OSX-3.0.2

Welcome to the GateKeeper-Retail-OSX-3.0.2 Installer

You will be guided through the steps necessary to install this software.

Click on **Continue**.



Install GateKeeper-Retail-OSX-3.0.2

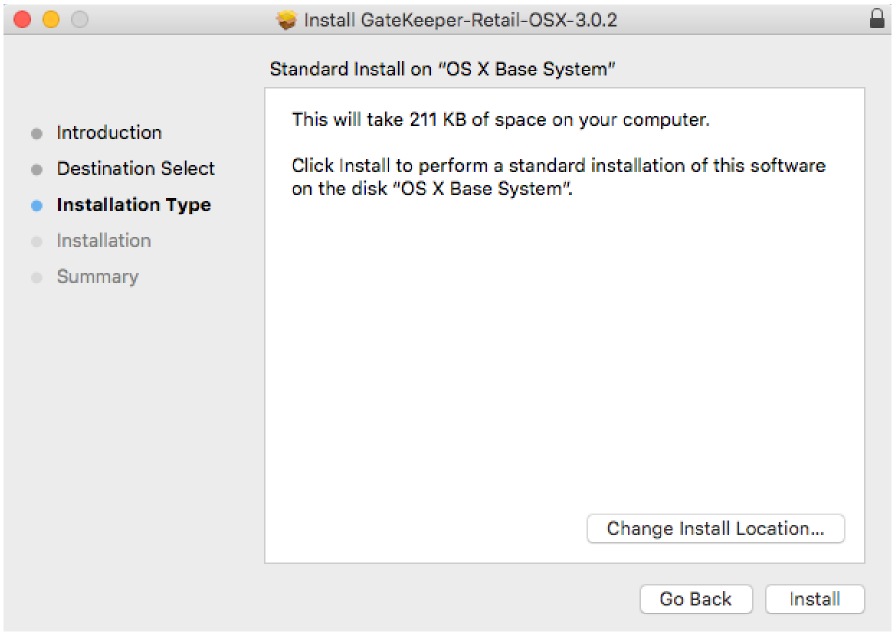
Select a Destination

Select the disk where you want to install the GateKeeper-Retail-OSX-3.0.2 software.

OS X Base System
475.34 GB available
499.25 GB total

Installing this software requires 211 KB of space.

Select the disk where you'd like to install the GateKeeper application and click on **Continue**.

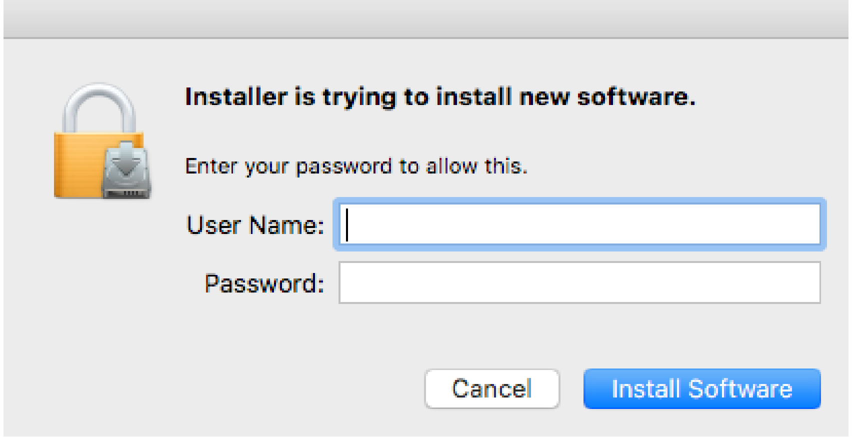


Standard Install on "OS X Base System"

This will take 211 KB of space on your computer.

Click Install to perform a standard installation of this software on the disk "OS X Base System".

Click on **Install** to begin the installation.

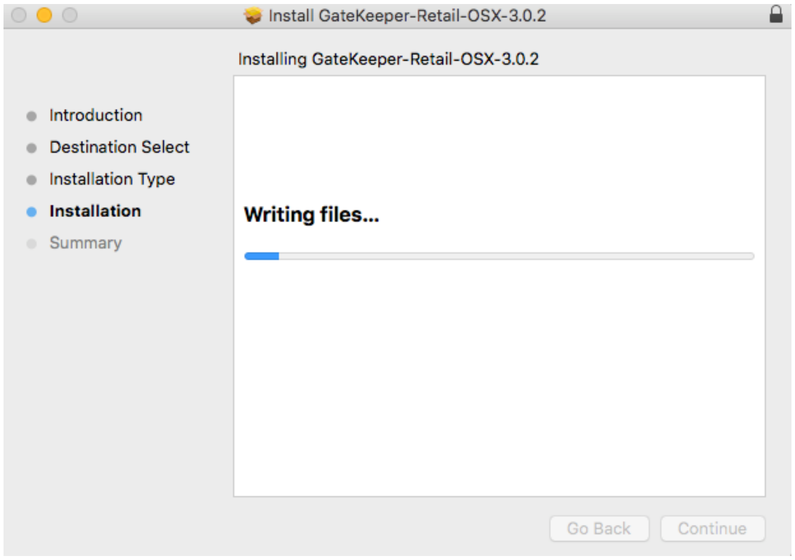


Installer is trying to install new software.

Enter your password to allow this.

Enter the credentials to install the software and click on **Install Software**.

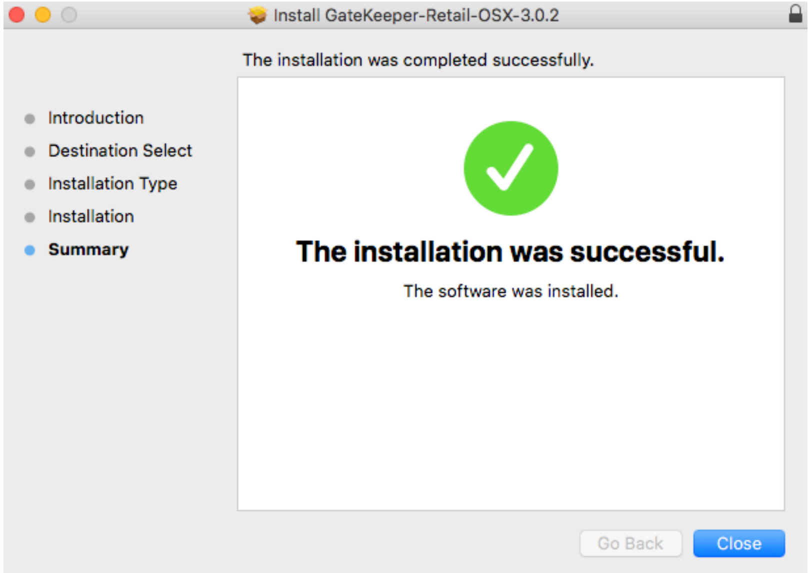
Please wait while the application installs. This may take a couple of minutes.



Installing GateKeeper-Retail-OSX-3.0.2

Writing files…

You’ll see a notification saying the installation was successful. Click on **Close**.

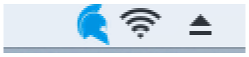


The installation was completed successfully.

The installation was successful.

The software was installed.

REBOOT your computer. Launch the GateKeeper application by clicking on the GateKeeper icon on the Menu Bar.



NOTE - If you’re going to use the GateKeeper to login to a domain account, please make sure you’ve logged in to the computer at-least once with the domain credentials.

3 GateKeeper Operation

3.1 Initial Setup

3.1.1 USB dongle

The GateKeeper USB dongle acts as the GateKeeper's Bluetooth sensor (receiver) and continuously scans for active GateKeeper tokens. The USB dongle should be placed in direct line of sight with the GateKeeper token (key) when you're working on your computer. We recommend using a USB extension cable to place it in the appropriate position.

3.1.2 Halberd key (hardware token) preparation

To activate the Halberd key, slide open the battery cover and insert the battery by gently pressing it against the metal contact with the '**+**' side facing up. Then press and hold the button on the side of the key until you hear a beeping sound with the LED lighting up green.

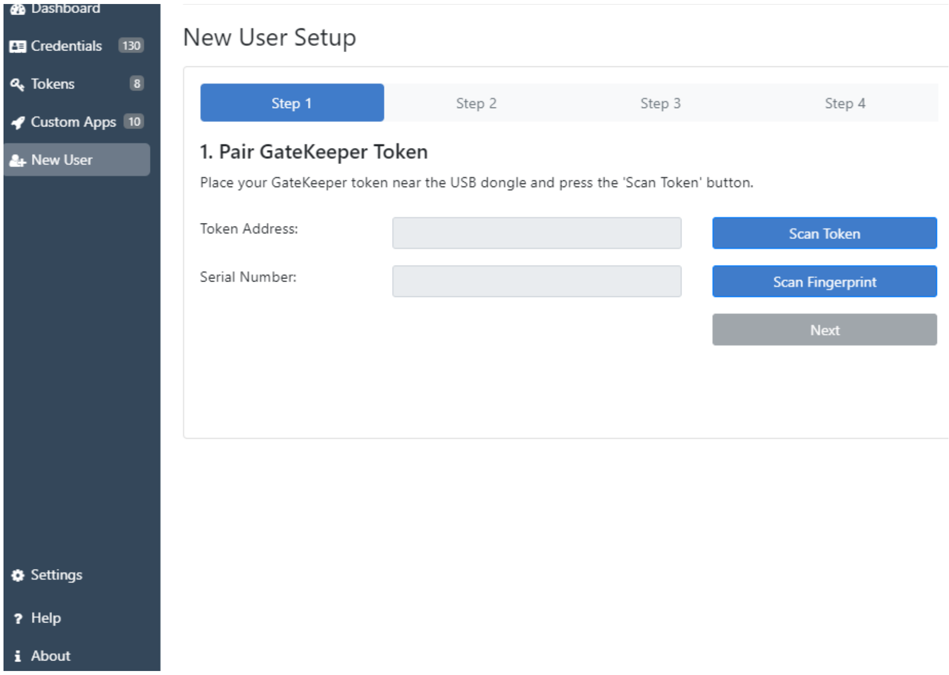
3.1.3 Trident app (software token) preparation

Download the Android Trident application from the Google Play Store. The GateKeeper iOS Trident application is available in iTunes.

Install the Trident application on your phone, turn on your phone's Bluetooth, then open the Trident app to make sure it's running.

3.2 Adding a User

To register the GateKeeper token with your computer's login credentials, click on the **Add User** tab, then follow the instructions below.



New User Setup

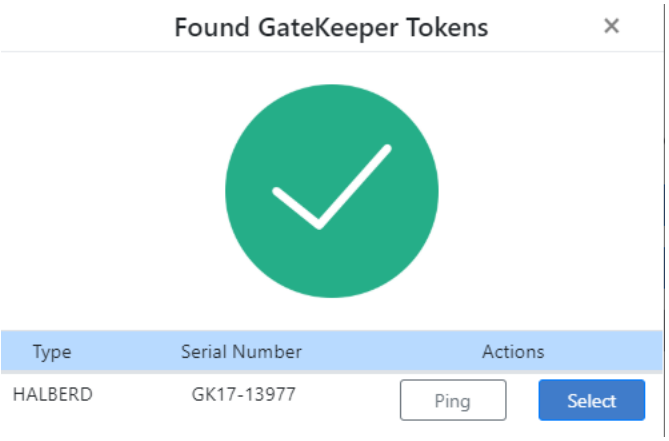
1. Pair GateKeeper Token

Place your GateKeeper token near the USB dongle and press the 'Scan Token' button.

Token Address:

Serial Number:

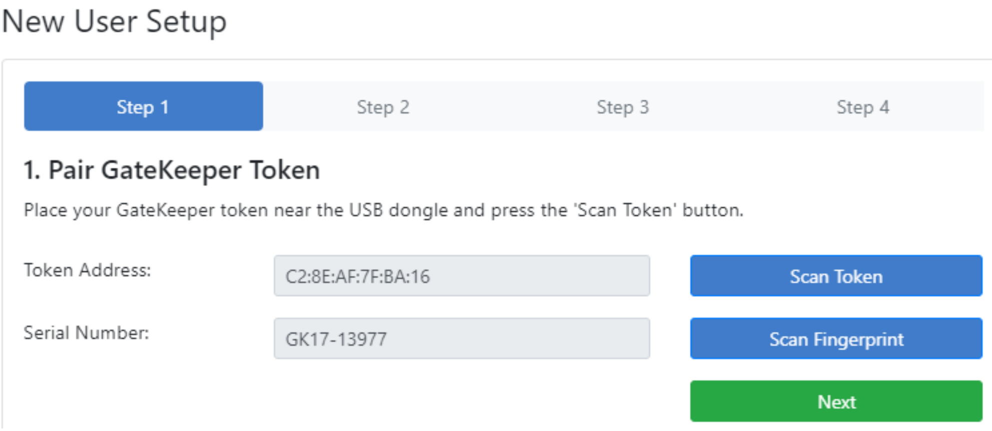
Step 1: Insert the battery into the token, plug the USB dongle into one of the front ports of the computer, touch the token to the USB dongle, then click on the **Scan** button. In a couple of seconds, the token will beep rapidly for 2 seconds and the token's serial number and address will populate on the screen. Click **Select** next to your token.



Found GateKeeper Tokens

Type	Serial Number	Actions
HALBERD	GK17-13977	Ping Select

If you would like to use your phone as your key rather than the Halberd, please follow the same process above after opening the GateKeeper Trident app and turning ON Bluetooth on your Android or iPhone.



New User Setup

Step 1 Step 2 Step 3 Step 4

1. Pair GateKeeper Token

Place your GateKeeper token near the USB dongle and press the 'Scan Token' button.

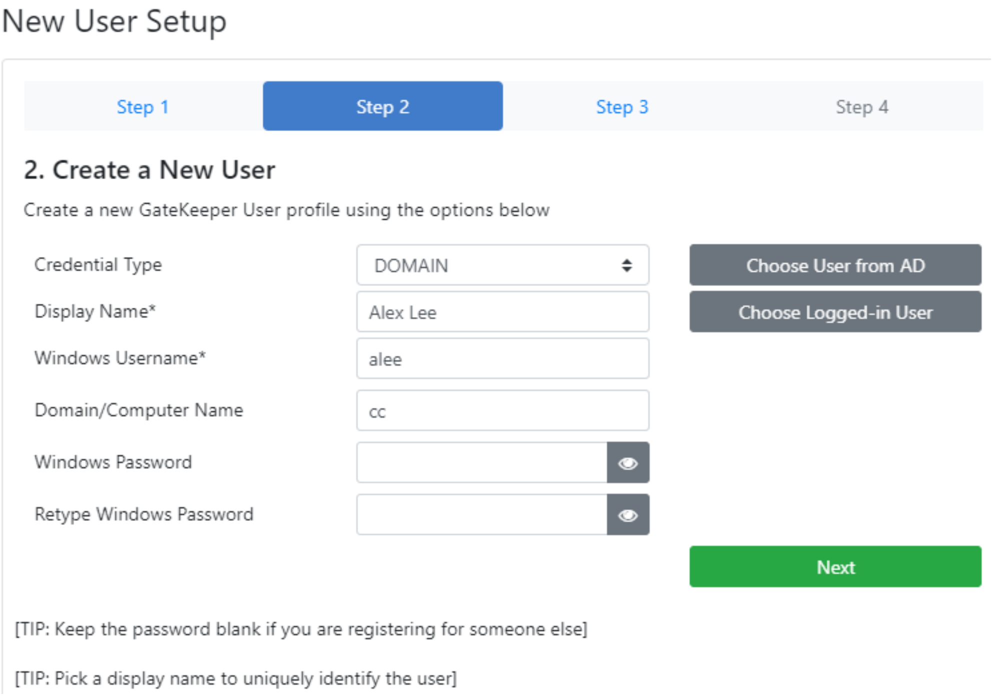
Token Address: C2:8E:AF:7F:BA:16

Serial Number: GK17-13977

Then click **Next**.

Step 2: In this step, you can either **Select Choose Logged-in User** if you're registering for yourself, type the username, domain, and display name or you can pick the user from the Active Directory by clicking on **Choose User from AD** and typing in the user's name. If you're registering the token for a different user, you can leave the password field blank. Click on **Next** to continue.

NOTE – If you want to register the token to the local Windows/Mac account, just leave the **Domain** field blank.



New User Setup

Step 1 Step 2 Step 3 Step 4

2. Create a New User

Create a new GateKeeper User profile using the options below

Credential Type: DOMAIN

Display Name*: Alex Lee

Windows Username*: alee

Domain/Computer Name: cc

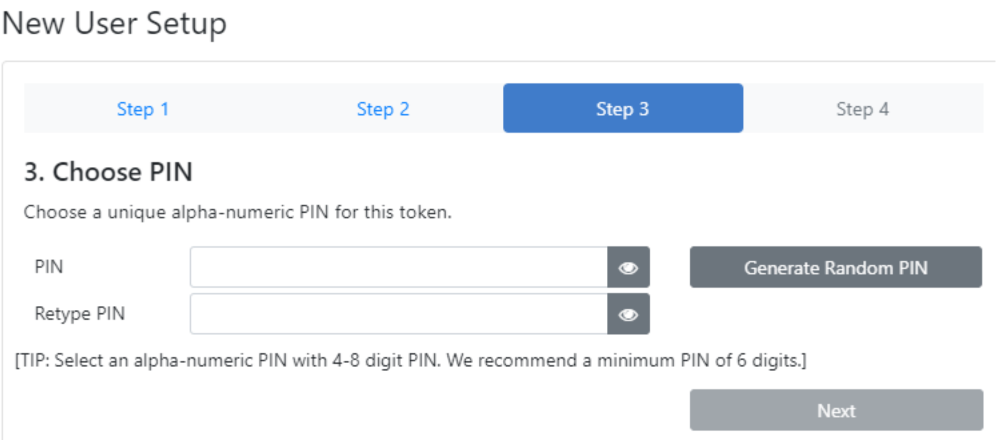
Windows Password:

Retype Windows Password:

[TIP: Keep the password blank if you are registering for someone else]

[TIP: Pick a display name to uniquely identify the user]

Step 3: Type in a secret PIN between four to eight digits. You can also click **Generate Random PIN** for the system to auto-generate. Click **Next** to continue.



New User Setup

Step 1 | Step 2 | Step 3 | Step 4

3. Choose PIN

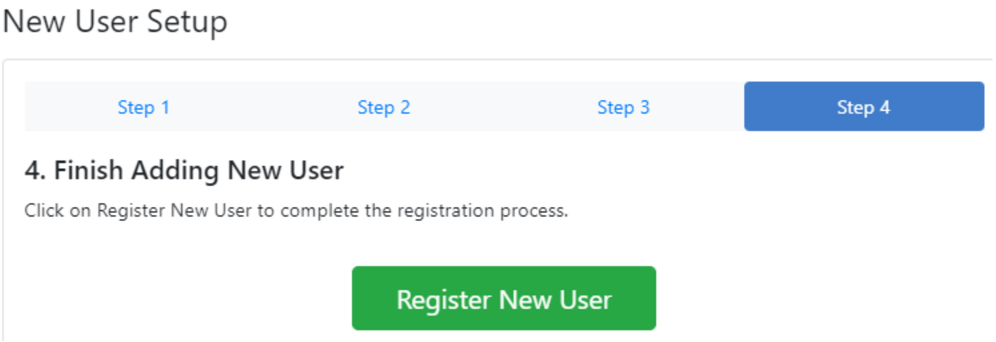
Choose a unique alpha-numeric PIN for this token.

PIN

Retype PIN

[TIP: Select an alpha-numeric PIN with 4-8 digit PIN. We recommend a minimum PIN of 6 digits.]

Step 4: Click **Register New User** to finish adding user.



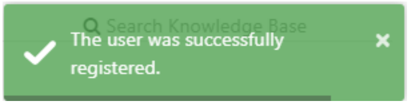
New User Setup

Step 1 | Step 2 | Step 3 | Step 4

4. Finish Adding New User

Click on Register New User to complete the registration process.

A notification will pop up stating that the user was successfully registered, and the application will generate a recovery code that can be used to recover all your web login credentials in case the GateKeeper token is lost. To save this code, click on **Copy**.

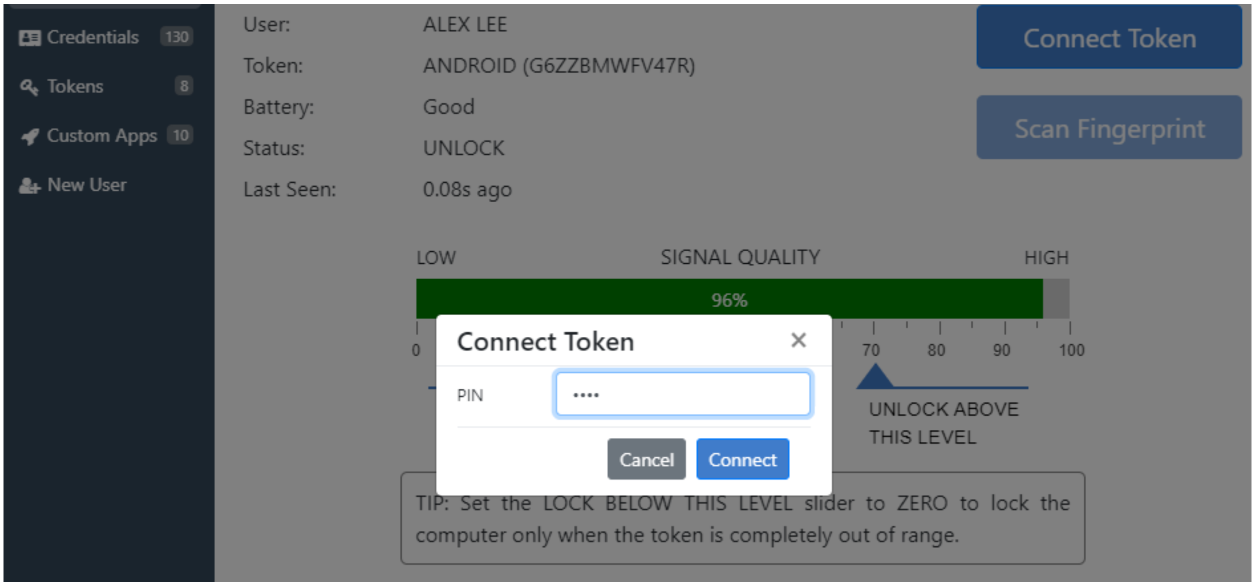


The user was successfully registered.

If you are not able to save this code now, you can always generate it later under the **Advanced** tab.

3.3 Connecting a User’s token to the application

To connect a user’s token to the application, go to the **App Settings** tab, click on **Connect User**, type in the PIN for the token, and click on **Connect**.



User: ALEX LEE
Token: ANDROID (G6ZZBMWFV47R)
Battery: Good
Status: UNLOCK
Last Seen: 0.08s ago

Connect Token

PIN ••••

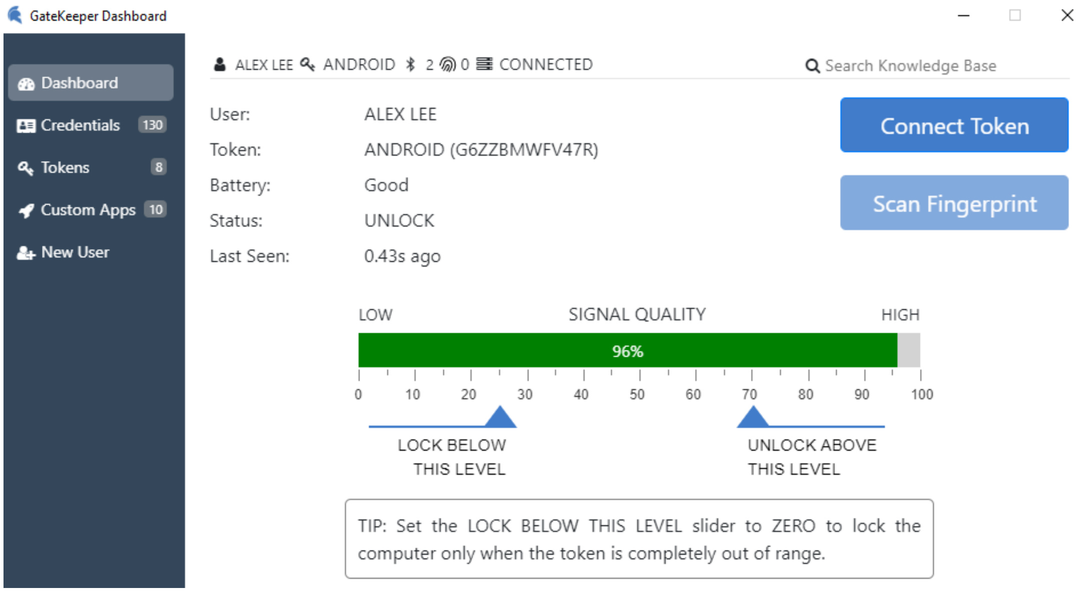
TIP: Set the LOCK BELOW THIS LEVEL slider to ZERO to lock the computer only when the token is completely out of range.

3.4 App Settings

This tab displays the user currently connected to the application, the lock/unlock options selected for the computer, along with **Advanced** settings.

3.4.1 User Info

This page displays the username, lock/unlock probability, battery status, and decision whether the computer is in 1) Lock state, 2) no change, or 3) Unlock state, with respect to how far the token is from the USB dongle.

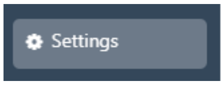


User: ALEX LEE
Token: ANDROID (G6ZZBMWFV47R)
Battery: Good
Status: UNLOCK
Last Seen: 0.43s ago

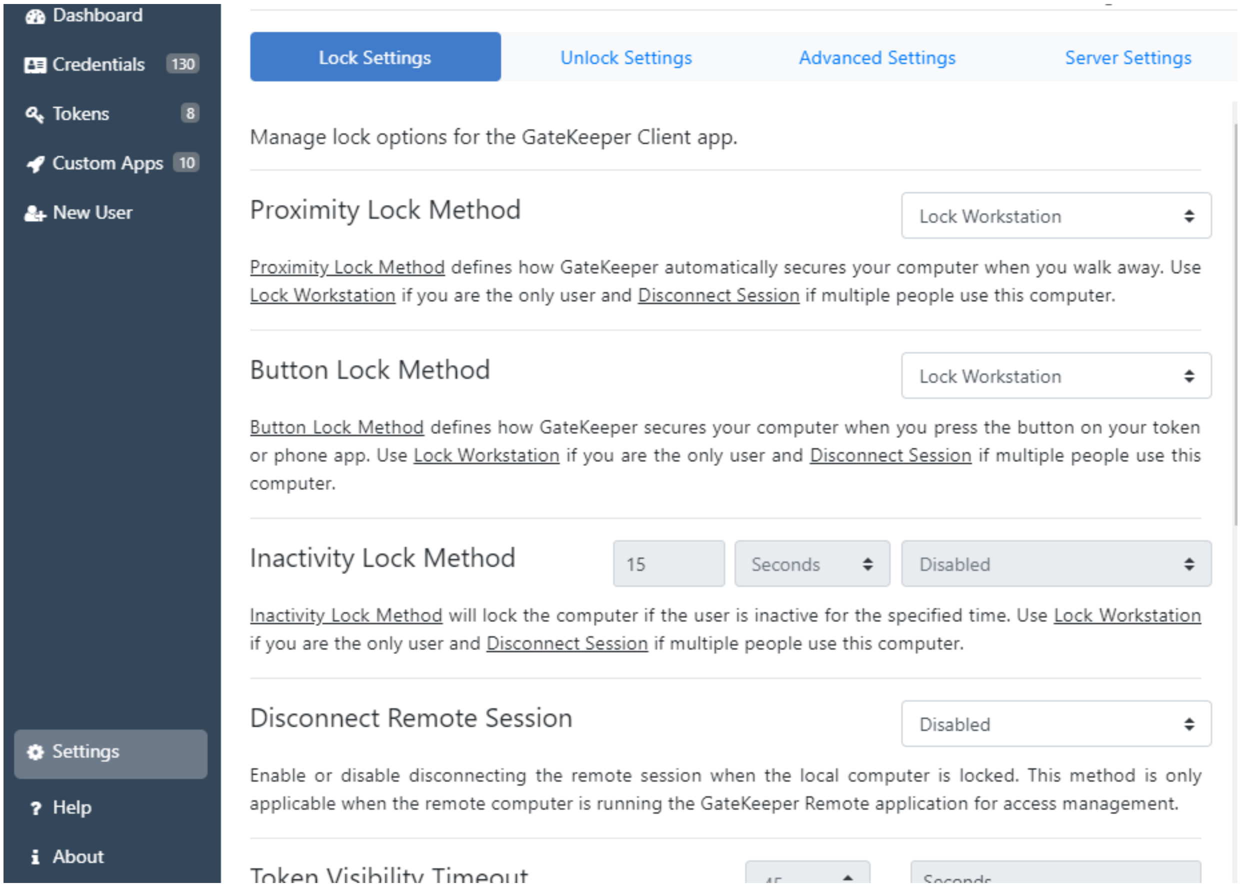
TIP: Set the LOCK BELOW THIS LEVEL slider to ZERO to lock the computer only when the token is completely out of range.

3.4.2 Lock Settings

Click **Settings**. Users can select how they want to lock/unlock their computers using their token.



You will see tabs for Lock Settings, Unlock Settings, Advanced Settings, and Server Settings.



Manage lock options for the GateKeeper Client app.

Proximity Lock Method: Lock Workstation

Proximity Lock Method defines how GateKeeper automatically secures your computer when you walk away. Use Lock Workstation if you are the only user and Disconnect Session if multiple people use this computer.

Button Lock Method: Lock Workstation

Button Lock Method defines how GateKeeper secures your computer when you press the button on your token or phone app. Use Lock Workstation if you are the only user and Disconnect Session if multiple people use this computer.

Inactivity Lock Method: 15 Seconds Disabled

Inactivity Lock Method will lock the computer if the user is inactive for the specified time. Use Lock Workstation if you are the only user and Disconnect Session if multiple people use this computer.

Disconnect Remote Session: Disabled

Enable or disable disconnecting the remote session when the local computer is locked. This method is only applicable when the remote computer is running the GateKeeper Remote application for access management.

Token Visibility Timeout: 45 Seconds

Proximity Lock Method defines how Gatekeeper automatically secures your computer when you walk away. Use Lock Workstation if you are the only user or **Disconnect Session (Switch User)** if multiple people use this computer. The user has the following Lock options available in the drop-down menu. Note 1: For macOS, **Lock Workstation** and **Logout** (sign out) options are not supported. Note 2: For Windows 7, it is recommended to use **Disconnect Session** instead of **Lock Workstation**.

- **Disabled**
- **Lock Workstation**
- **Disconnect Session (Switch User)**
- **Logout**

Button Lock Method defines how GateKeeper secures your computer when you press the action button on your token or phone app. Use **Lock Workstation** if you are the only user or **Disconnect Session (Switch**

User) if multiple people use this computer. The user has the following lock options available in the drop-down menu. Note 1: For macOS, **Lock Workstation** and **Logout** options are not supported. Note 2: For Windows 7, it is recommended to use **Disconnect Session (Switch User)** instead of **Lock Workstation**.

- **Disabled**
- **Lock Workstation**
- **Disconnect Session (Switch User)**
- **Logout**

Inactivity Lock Method will lock the computer if the user is inactive (no keyboard or mouse activity) for the specified time. Use Lock Workstation if you are the only user or **Disconnect Session (Switch User)** if multiple people use this computer. The user has the following Lock options available in the drop-down menu. Note 1: For macOS, **Lock Workstation** and **Logout** options are not supported. Note 2: For Windows 7, it is recommended to use **Disconnect Session (Switch User)** instead of **Lock Workstation**.

- **Disabled**
- **Lock Workstation**
- **Disconnect Session (Switch User)**
- **Logout**

Disconnect Remote Session allows user to enable or disable disconnecting remote session when the local computer is locked. This requires the client version to be 3.9 or higher, and the GateKeeper Remote application to be installed on the remote computer.

- **Enabled**
- **Disabled**

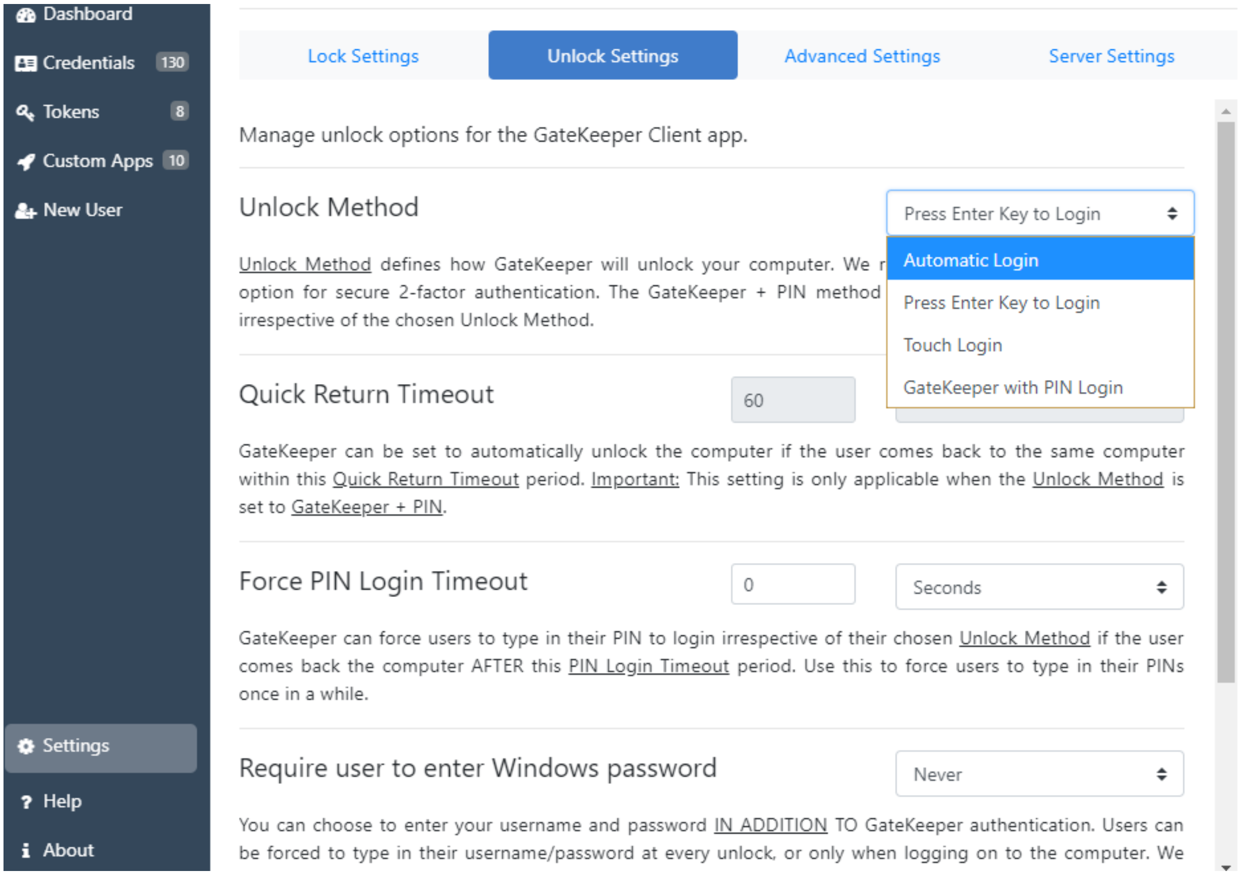
Token Visibility Timeout sets a lock timer if no token is detected within this time period – this is your backup locking mechanism if the proximity signal is not detected. 30 seconds is the default setting.

Lock Delay Timeout delays locking the computer after a lock decision has been made for this time period. Choose a value for this delay if you want to prevent the computer from locking immediately when you walk away. Important: This lock delay will only apply when the computer is locked due to proximity.

Operating System Timeout disables your screen saver from starting when your computer times out. Choose the appropriate option to keep enable or disable your screensaver timeout.

Motion Detection Sensitivity is useful for adapting your locking and unlocking experience in different environment. High level setting motion sensitivity will allow the computer to lock quicker. If the system is locking too much while you are sitting at your desk, reduce the motion sensitivity to the Low level.

3.4.3 Unlock Settings



Manage unlock options for the GateKeeper Client app.

Unlock Method: Press Enter Key to Login

- Automatic Login
- Press Enter Key to Login
- Touch Login
- GateKeeper with PIN Login

Unlock Method defines how GateKeeper will unlock your computer. We r option for secure 2-factor authentication. The GateKeeper + PIN method irrespective of the chosen Unlock Method.

Quick Return Timeout: 60

GateKeeper can be set to automatically unlock the computer if the user comes back to the same computer within this Quick Return Timeout period. Important: This setting is only applicable when the Unlock Method is set to GateKeeper + PIN.

Force PIN Login Timeout: 0 Seconds

GateKeeper can force users to type in their PIN to login irrespective of their chosen Unlock Method if the user comes back the computer AFTER this PIN Login Timeout period. Use this to force users to type in their PINs once in a while.

Require user to enter Windows password: Never

You can choose to enter your username and password IN ADDITION TO GateKeeper authentication. Users can be forced to type in their username/password at every unlock, or only when logging on to the computer. We

Unlock Method defines how GateKeeper will unlock your computer. We recommend **GateKeeper with PIN Login** option for secure 2-factor authentication (2FA).

Automatic Login	Unlocks automatically when you arrive at your computer with your GateKeeper token.
Press Enter Key to Login	Requires you to have your GateKeeper token and press the Enter Key. Great for shared locations so that computer can know which user's key to log in with.
Touch Login	Requires users to touch their GateKeeper token key fob (or phone) to the USB proximity sensor in order to log in.
GateKeeper with PIN Login	2FA: requires a user to have their GateKeeper token (possession factor) and to type in a secret PIN (knowledge factor). Most secure method.

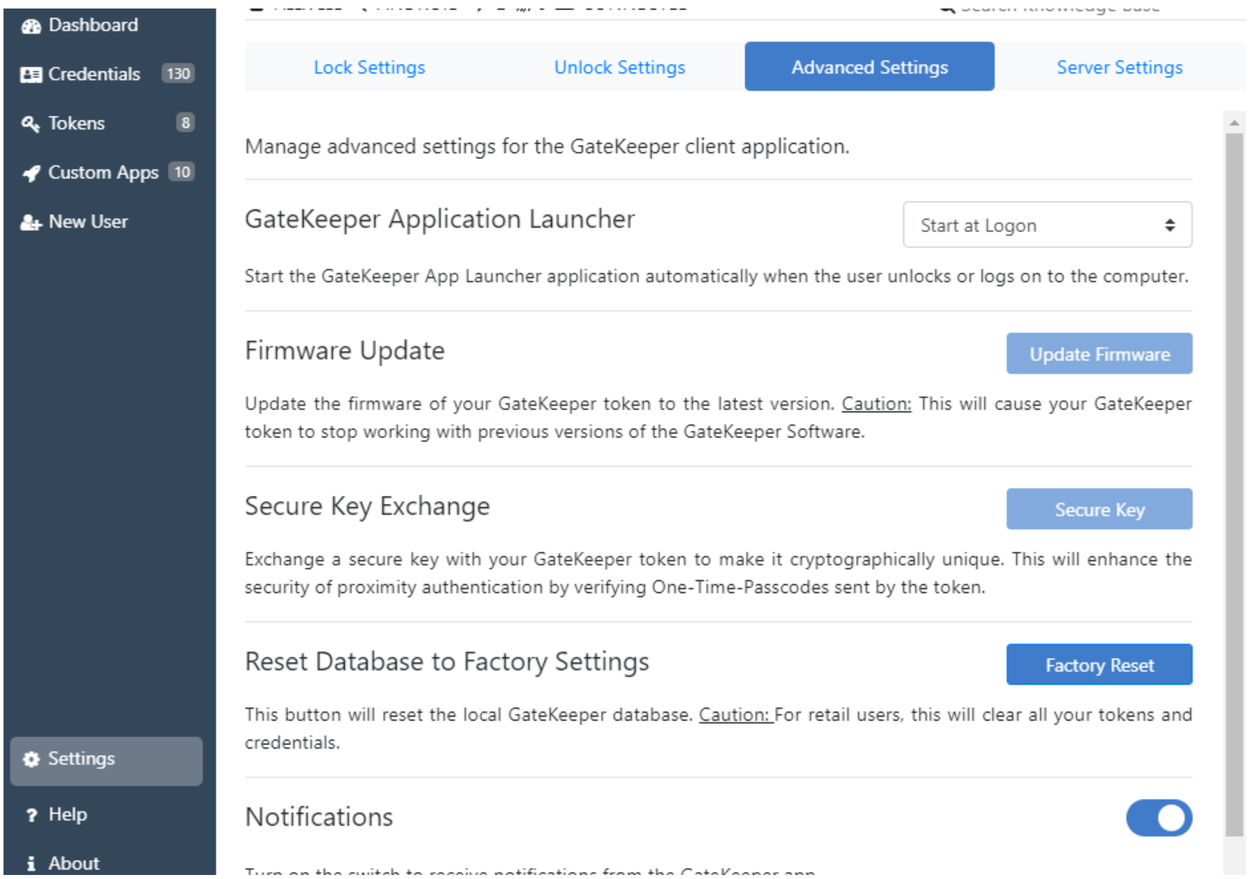
Quick Return Timeout allows the same returning user to automatically unlock the computer ONLY if the same user comes back to the same computer within this time period. Please keep in mind that this setting is only applicable when the **Unlock Method** is set to **GateKeeper with PIN Login**. Useful for the same person coming and going from the same computer in short intervals.

Force PIN Login Timeout forces users to type their PIN to login irrespective of their chosen **Unlock Method** if the user comes back the computer AFTER this predetermined PIN Login Timeout period. Use this to force users to type in their PINs at this predetermined interval for daily or weekly security checks.

Require user to enter Windows password option gives the user an option to enter their username and password IN ADDITION TO GateKeeper authentication. Users can be forced to type in their username/password at every unlock, or only when logging on to the computer. Recommend setting this option to NEVER.

Windows Standard Login enables/disables the standard Windows login method (username/password) for your computer. If you choose to disable the default login method, then you can ONLY access your computer with your GateKeeper. Please keep in mind that if you forget your PIN or lose your GateKeeper key, you will not be able to access your computer.

2.1.4 Advanced Settings



Manage advanced settings for the GateKeeper client application.

GateKeeper Application Launcher — Start at Logon

Start the GateKeeper App Launcher application automatically when the user unlocks or logs on to the computer.

Firmware Update

Update the firmware of your GateKeeper token to the latest version. Caution: This will cause your GateKeeper token to stop working with previous versions of the GateKeeper Software.

Secure Key Exchange

Exchange a secure key with your GateKeeper token to make it cryptographically unique. This will enhance the security of proximity authentication by verifying One-Time-Passcodes sent by the token.

Reset Database to Factory Settings

This button will reset the local GateKeeper database. Caution: For retail users, this will clear all your tokens and credentials.

Notifications

Turn on the switch to receive notifications from the GateKeeper app

GateKeeper Application Launcher allows users to choose programs to automatically launch either at startup or logon. EHRs, CRMs, Microsoft 365, Salesforce, and more can be auto-launched.

Firmware Update option allows users to update the firmware of their GateKeeper token to the latest version. Keep in mind, this will cause your GateKeeper token to stop working with previous versions of the GateKeeper software.

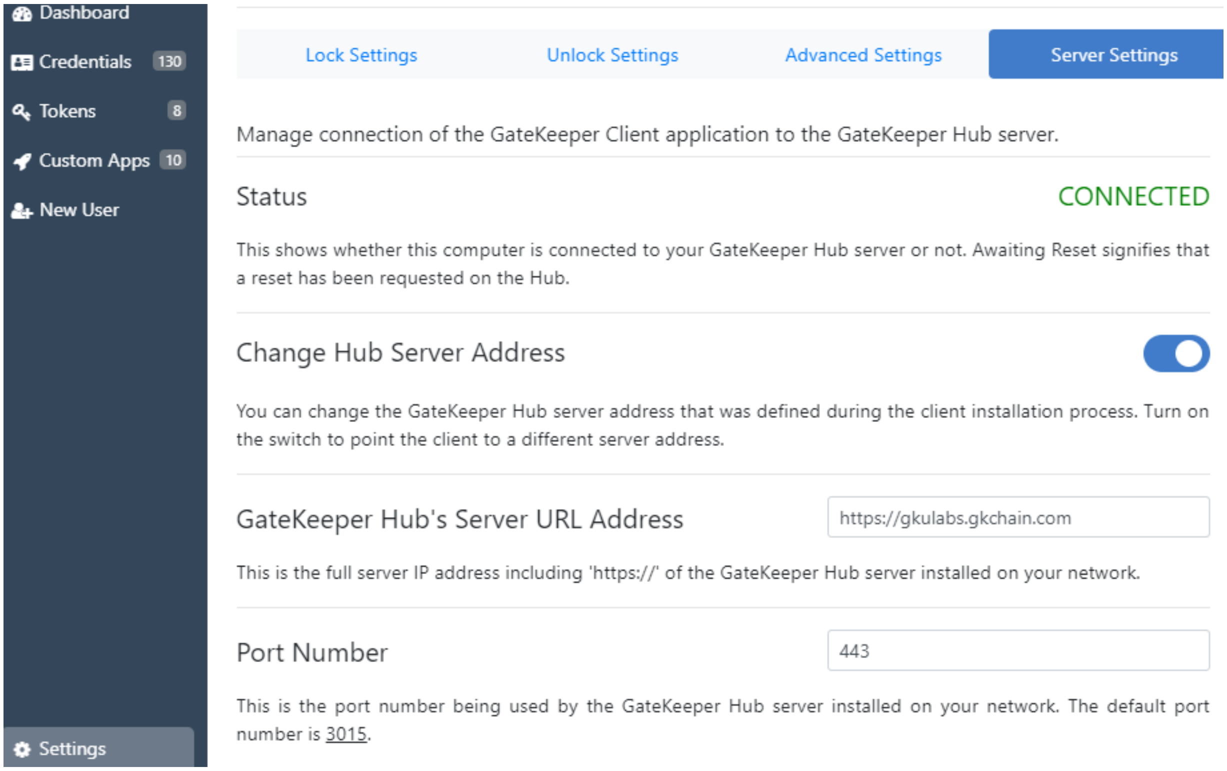
Secure Key Exchange option allows user to exchange a secure key with your GateKeeper token to make it cryptographically unique. This will enhance the security of proximity authentication by verifying One-Time-Passcodes sent by the token.

Reset Database to Factory Settings option will reset the local GateKeeper database. Keep in mind for individual users without the Hub, this will clear all your tokens and credentials.

Notifications allows you to receive notifications from GateKeeper via SMS, email, and/or the application.

2.1.5 Server Settings

This section displays the IP address of the machine where the GateKeeper Hub is installed, along with the port number. The correct IP address will indicate the **Status** as *Connected*. To change the IP address, please click the **'Change Hub Server Address'** switch and enter the new IP address.



Manage connection of the GateKeeper Client application to the GateKeeper Hub server.

Status CONNECTED

This shows whether this computer is connected to your GateKeeper Hub server or not. Awaiting Reset signifies that a reset has been requested on the Hub.

Change Hub Server Address

You can change the GateKeeper Hub server address that was defined during the client installation process. Turn on the switch to point the client to a different server address.

GateKeeper Hub's Server URL Address: https://gkulabs.gkchain.com

This is the full server IP address including 'https://' of the GateKeeper Hub server installed on your network.

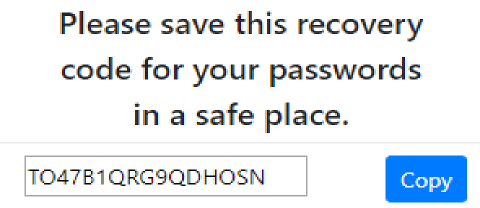
Port Number: 443

This is the port number being used by the GateKeeper Hub server installed on your network. The default port number is 3015.

3.4.4 Credentials Recovery

In case you have misplaced your token, please use this function to recover your web login credentials.

To generate the code, click on **Get New Code,** then enter your PIN.

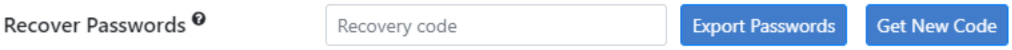


Please save this recovery code for your passwords in a safe place.

TO47B1QRG9QDHOSN

Click on **Copy** and save this code in a secure place.

To get your web credentials back, enter your code in the text box, and click on **Export Passwords.**

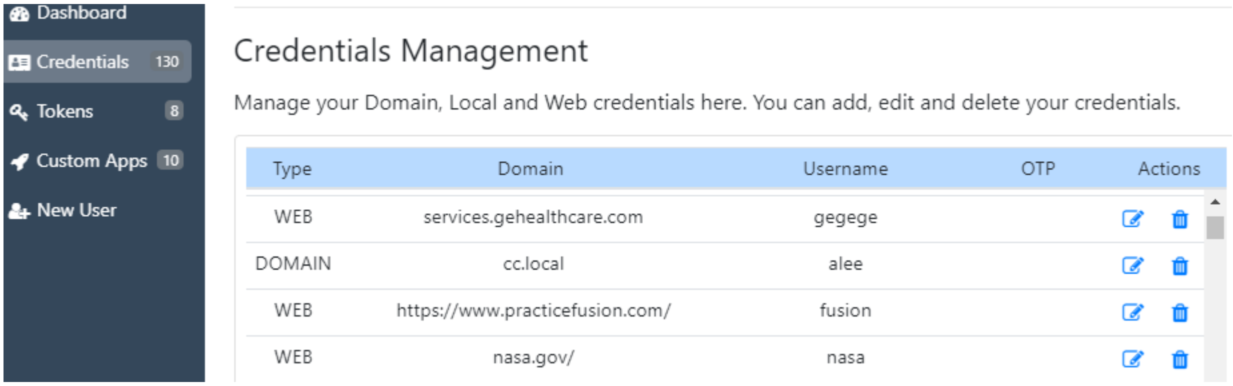


Recover Passwords

This will save your credentials in a CSV file on your computer.

3.5 Password and Token Management

The **Credentials** tab displays all the domain, local, and web credentials associated with the user connected to the application. You can edit/delete these credentials.



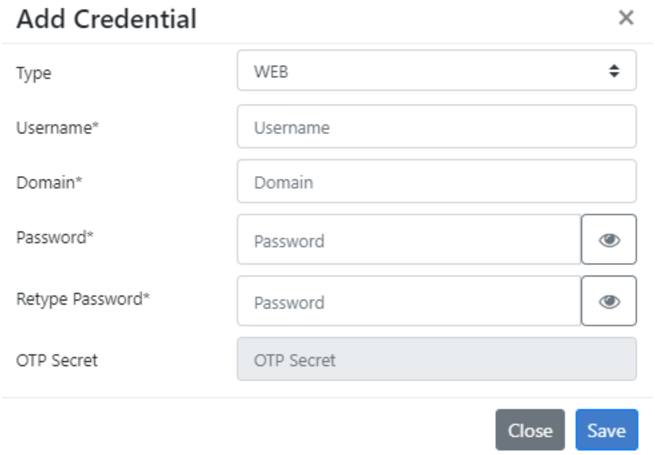
Credentials Management

Manage your Domain, Local and Web credentials here. You can add, edit and delete your credentials.

Type	Domain	Username	OTP	Actions
WEB	services.gehealthcare.com	gegege		✎ 🗑
DOMAIN	cc.local	alee		✎ 🗑
WEB	https://www.practicefusion.com/	fusion		✎ 🗑
WEB	nasa.gov/	nasa		✎ 🗑

3.5.1 Adding Credentials

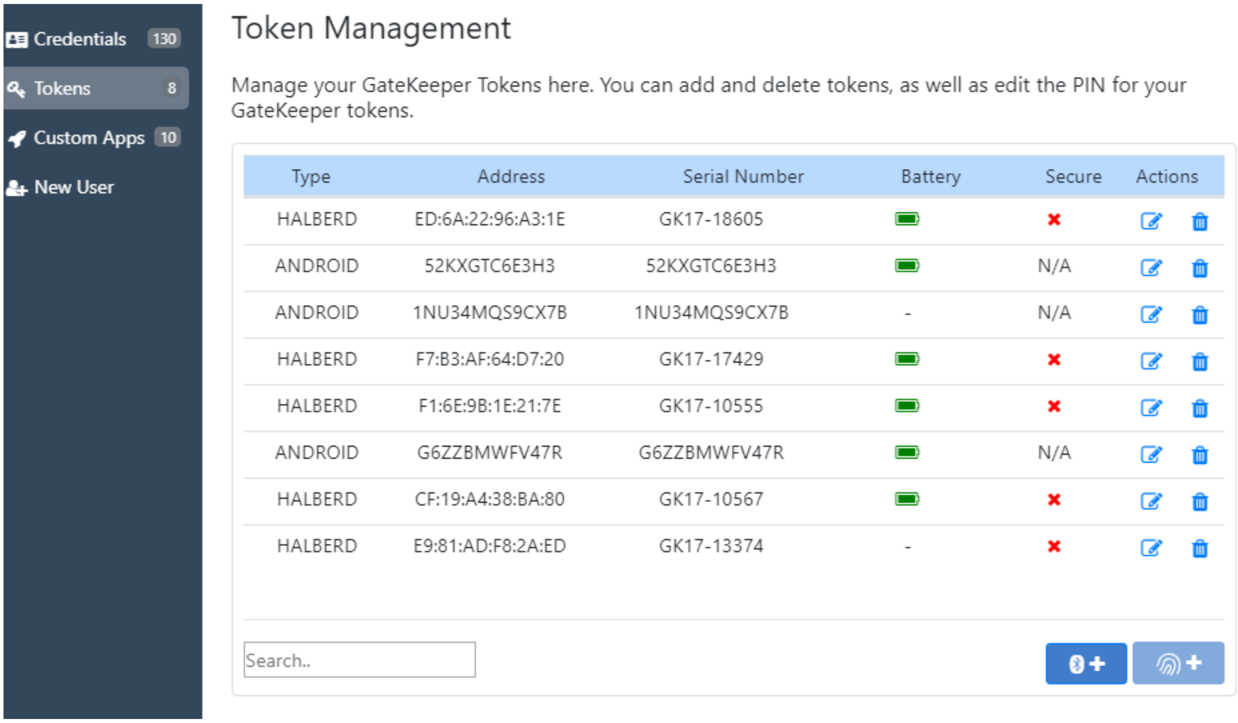
To add a new credential, click on '**+**'. Select the type of credential (web/local/domain/OTP), fill in the details, and click **Save**. This will add the credential to the user's account, and then the user can use their token to log in with these credentials.



Add Credential

Type	WEB
Username*	Username
Domain*	Domain
Password*	Password
Retype Password*	Password
OTP Secret	OTP Secret

The **Tokens** tab displays all the GateKeeper tokens associated with the currently connected user. You can edit/delete these tokens. The **Battery** status is only displayed for the currently connected token.



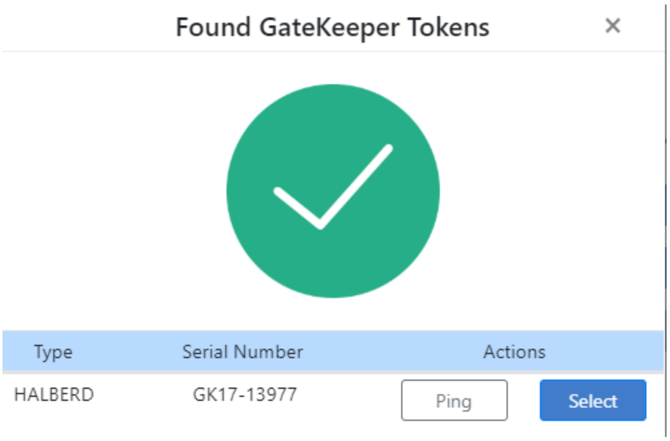
Token Management

Manage your GateKeeper Tokens here. You can add and delete tokens, as well as edit the PIN for your GateKeeper tokens.

Type	Address	Serial Number	Battery	Secure	Actions
HALBERD	ED:6A:22:96:A3:1E	GK17-18605	🟩	✗	✎ 🗑
ANDROID	52KXGTC6E3H3	52KXGTC6E3H3	🟩	N/A	✎ 🗑
ANDROID	1NU34MQS9CX7B	1NU34MQS9CX7B	-	N/A	✎ 🗑
HALBERD	F7:B3:AF:64:D7:20	GK17-17429	🟩	✗	✎ 🗑
HALBERD	F1:6E:9B:1E:21:7E	GK17-10555	🟩	✗	✎ 🗑
ANDROID	G6ZZBMWFV47R	G6ZZBMWFV47R	🟩	N/A	✎ 🗑
HALBERD	CF:19:A4:38:BA:80	GK17-10567	🟩	✗	✎ 🗑
HALBERD	E9:81:AD:F8:2A:ED	GK17-13374	-	✗	✎ 🗑

3.5.2 Adding Tokens

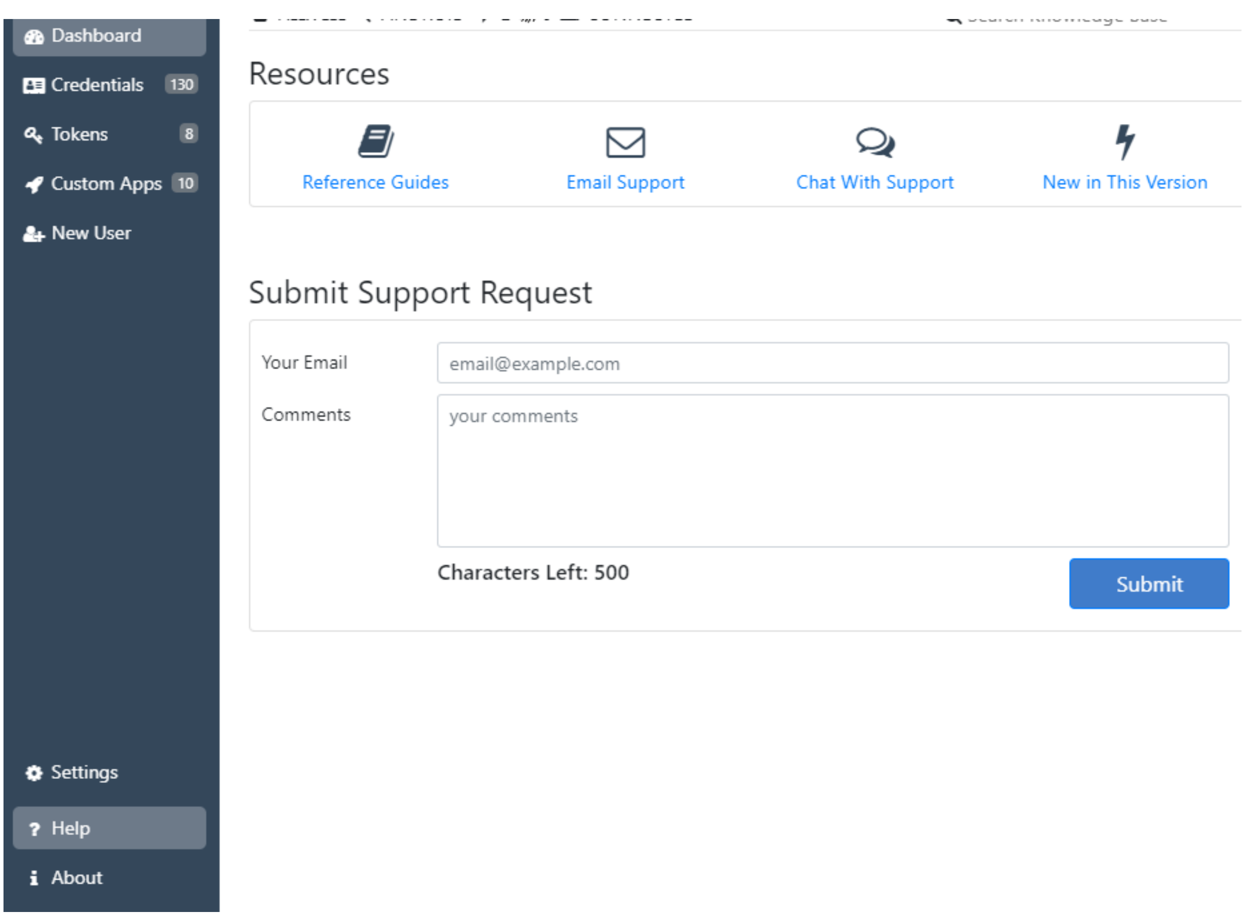
To add a new Halberd key (hardware token), touch it to the plugged in USB dongle on the computer and then click on '**+**'. To add your phone, open the Trident app (software token), turn ON the phone's Bluetooth, and then click on '**+**'. Enter a PIN for the token and click on **Save**. This will add the token to the user's account and now the user can access all their computer and web credentials using this token as well.



Found GateKeeper Tokens

Type	Serial Number	Actions
HALBERD	GK17-13977	Ping Select

3.6 Help



Resources

Submit Support Request

Your Email	email@example.com
Comments	your comments

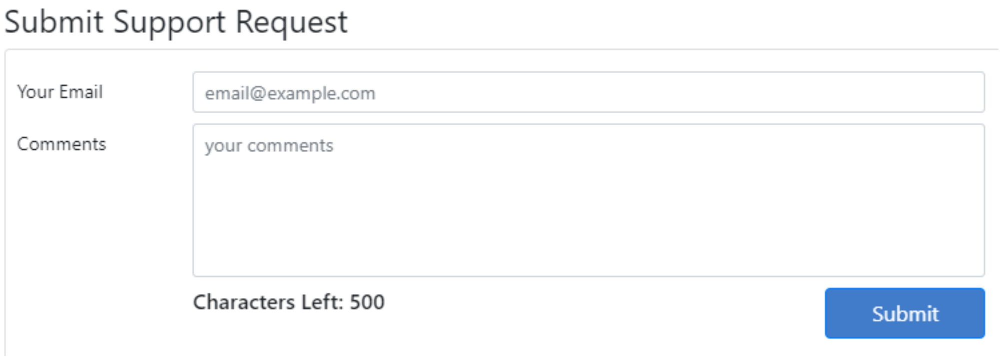
Characters Left: 500

This tab has links to download the Reference Guide for this client application and the instructions on how to disable the group policy of the Ctrl+Alt+Del screen for Windows users.

Use this tab to reach out to our support team through Live Chat or Email. You can also access the online store from here. For additional assistance or inquiries, please email us at info@gkaccess.com.

3.7 Feedback

Please use this tab inform us about any issues you may be experiencing with the application. Make sure you include your email and a brief description of the issue/incident and click **Send**. This will grab the GateKeeper logs from the application and send it to us for diagnosis.



Submit Support Request

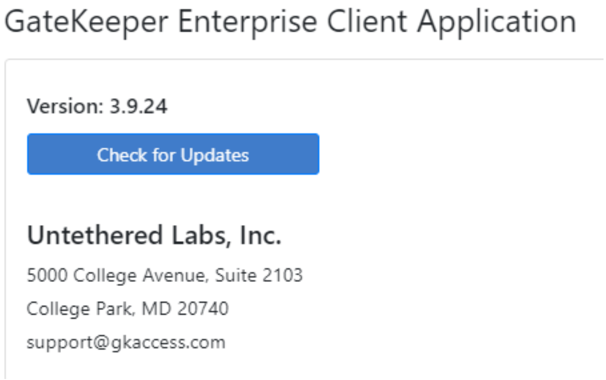
Your Email: email@example.com

Comments: your comments

Characters Left: 500

3.8 About

This tab shows the application version you're currently using. Please check with your GateKeeper administrator to see if you're using the latest version.



GateKeeper Enterprise Client Application

Version: 3.9.24

Untethered Labs, Inc.
5000 College Avenue, Suite 2103
College Park, MD 20740
support@gkaccess.com

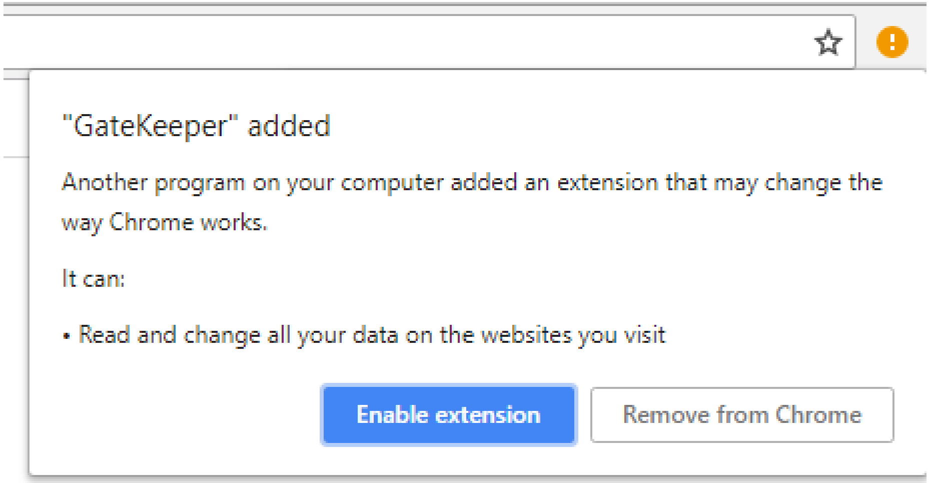
4 GateKeeper Chrome Extension

The GateKeeper Chrome Extension password manager connects to your GateKeeper token through the desktop application and stores the encrypted passwords securely in your GateKeeper account. We ***DO NOT*** store any information on the Chrome extension itself, instead we provide a more secure (and faster) means of accessing your web credentials. The passwords are encrypted by the desktop application using military-grade AES-256 encryption.

Chrome

4.1 Installation

Open Google Chrome and enable the GateKeeper Chrome extension.



"GateKeeper" added

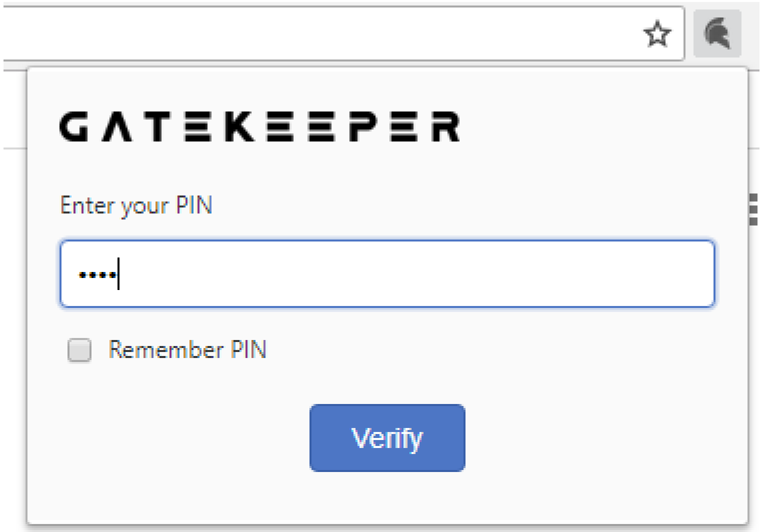
Another program on your computer added an extension that may change the way Chrome works.

It can:

- Read and change all your data on the websites you visit

1.1 How to log in to Chrome using my GateKeeper token?

Click on the GateKeeper Chrome extension and type in the PIN to your GateKeeper token. Click on **Verify** to connect your token.

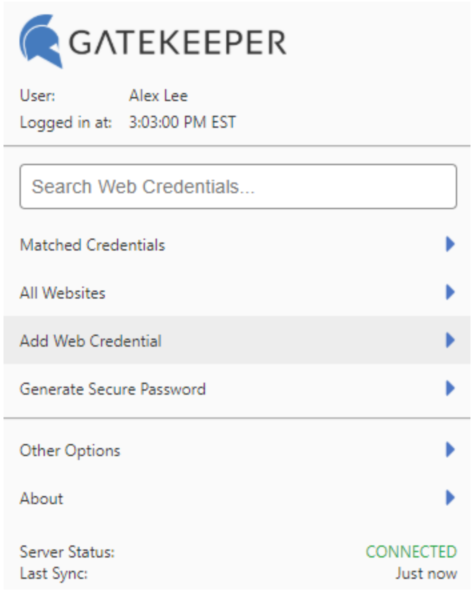


Enter your PIN

••••

□ Remember PIN

If you want to connect to the Chrome extension automatically after logging into your computer with your GateKeeper token, click on **Other Options** and check the box for **Skip PIN Verification**.

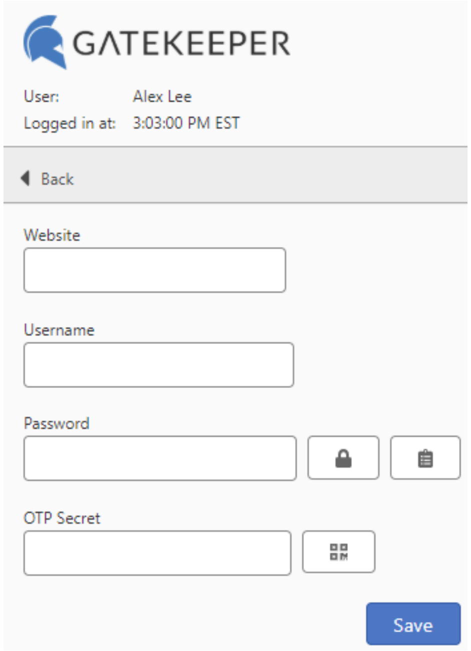


User: Alex Lee
Logged in at: 3:03:00 PM EST

Server Status: CONNECTED
Last Sync: Just now

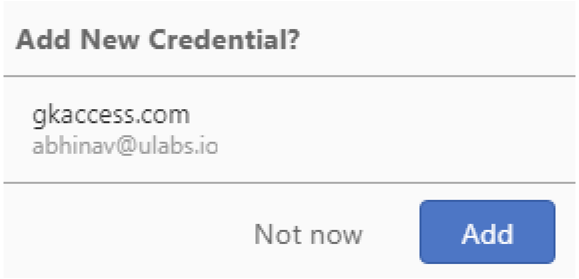
4.2 Adding a web credential

To add a web credential, click on **Add Web Credential**. Enter the website address, username, password, and then click on **Save**. You can also create a new password by clicking on 🔒. To copy this password, click on 📋.



User: Alex Lee
Logged in at: 3:03:00 PM EST

If you're logging into a website for the first time while connected to the extension, you'll see a notification asking whether you'd like to save those credentials. Click on **Add** to save it to the application or **Not now** if you don't want to save it right now.

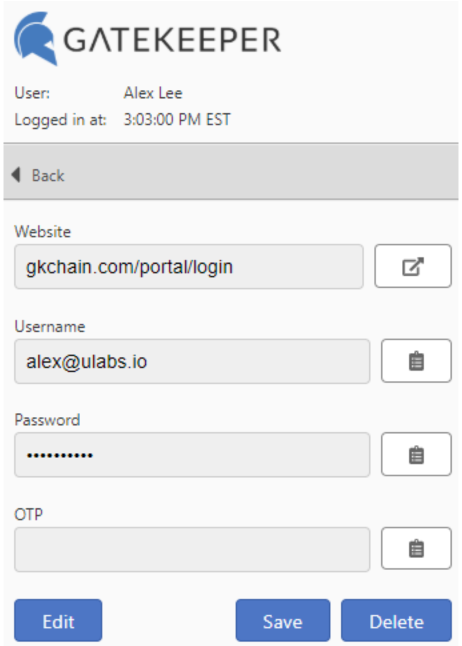


Add New Credential?

gkaccess.com
abhinav@ulabs.io

4.3 Editing/Deleting an existing web credential

To change the username/password on an existing web credential, go to **All Websites**, and select the credential you'd like to edit. Click on **Edit** to update the username/password and click on **Save**. Click on **Delete** to remove the saved credential.



User: Alex Lee
Logged in at: 3:03:00 PM EST

Website: gkchain.com/portal/login

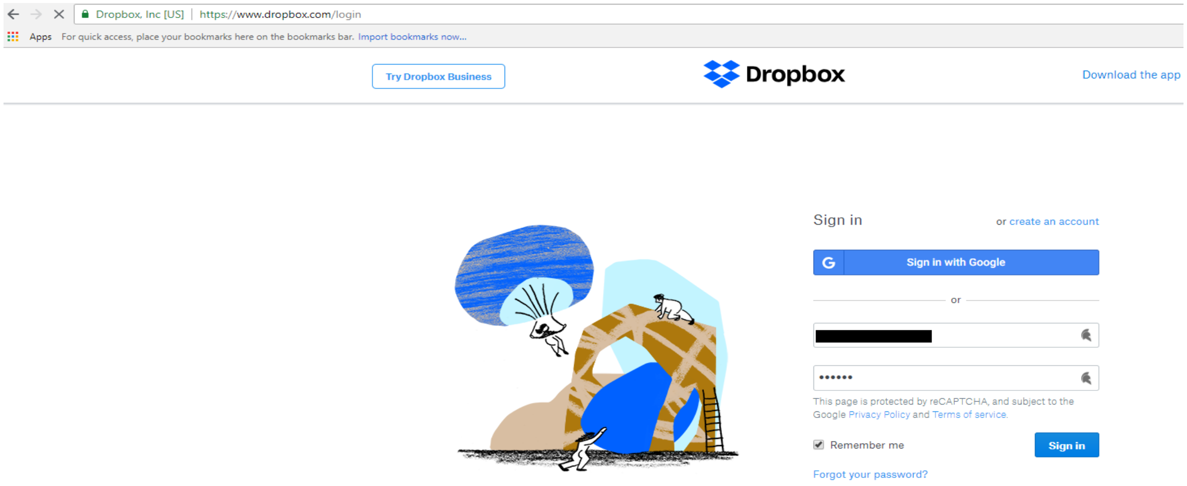
Username: alex@ulabs.io

Password: ••••••••••

OTP:

4.4 Using the Chrome extension

Once you've added a web credential to your GateKeeper account, the next time you visit the same website, the username and password will be populated automatically, and you'll be able to log in in with a single click – no usernames or passwords to remember anymore.



Dropbox, Inc [US] | https://www.dropbox.com/login

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Sign in or create an account

[redacted]

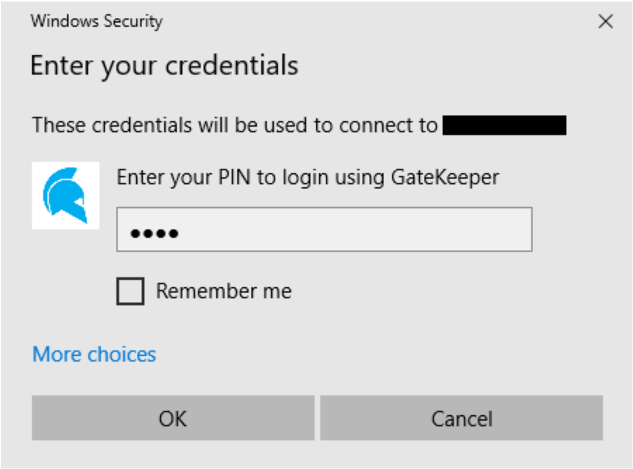
••••••

This page is protected by reCAPTCHA, and subject to the Google Privacy Policy and Terms of service.

☑ Remember me

5 Remote Desktop Connection Authentication

The GateKeeper client application also authenticates users into Remote Desktop sessions. To use this feature, please launch the **Windows Remote Desktop Connection** app from the Start Menu and type in the IP address to connect to the computer. Make sure you're on the same network as the remote computer.



Windows Security

Enter your credentials

These credentials will be used to connect to [redacted]

Enter your PIN to login using GateKeeper

••••

☐ Remember me

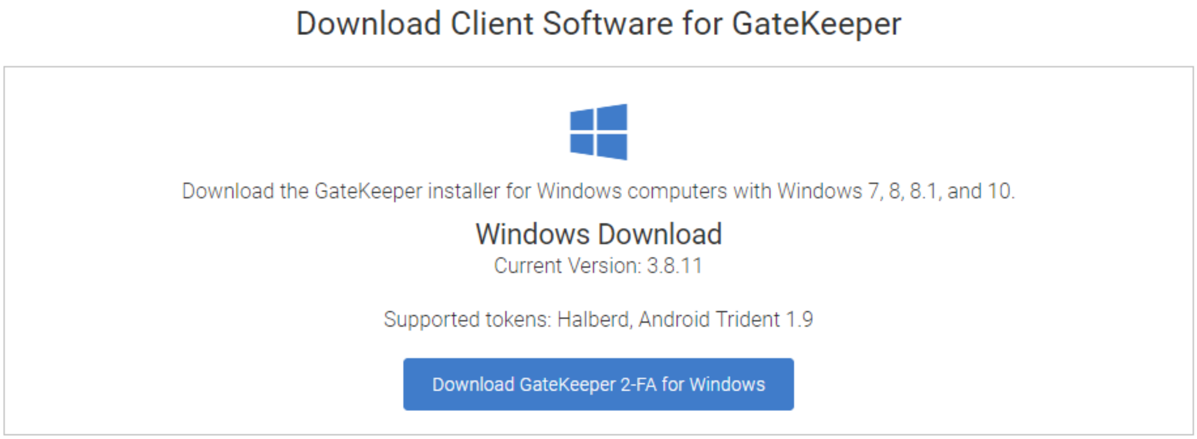
Type in the PIN for the GateKeeper token that has access to the credentials you're using to log in to the remote computer, then click **OK** to log in to your session.

6 Frequently Asked Questions

6.1 How can I download the GateKeeper Desktop Application?

To download the desktop application, go to our website https://gkaccess.com/downloads/.

Click on the appropriate version for your computer (Win or Mac).



Download Client Software for GateKeeper

Download the GateKeeper installer for Windows computers with Windows 7, 8, 8.1, and 10.

Windows Download

Current Version: 3.8.11

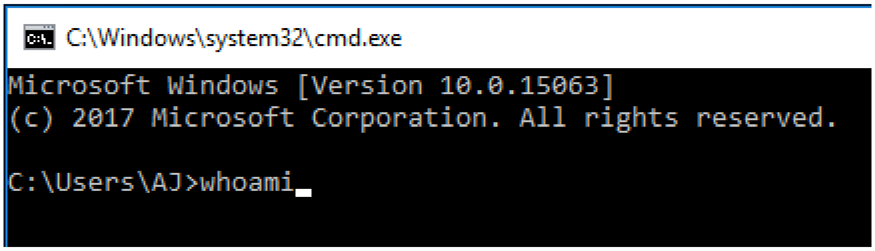
Supported tokens: Halberd, Android Trident 1.9

6.2 How can I launch the GateKeeper application?

The GateKeeper application can be found as a tray icon on your taskbar for Windows and the top taskbar for Mac. Click on the icon to launch it.

6.3 How can I verify my username and domain on Windows machines?

On the **Start Menu** enter 'cmd' and hit enter. On the command prompt window type 'whoami' and hit enter. This will return you the domain and username in the format <domain-name>/<username>



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\AJ>whoami_
```

6.4 How many login credentials can be on a GateKeeper token?

The GateKeeper token can manage as many credentials as you like. To add more credentials, connect your token to the application and add them on the **Credentials** tab.

6.5 I don't remember the PIN to my GateKeeper token, can I reset it?

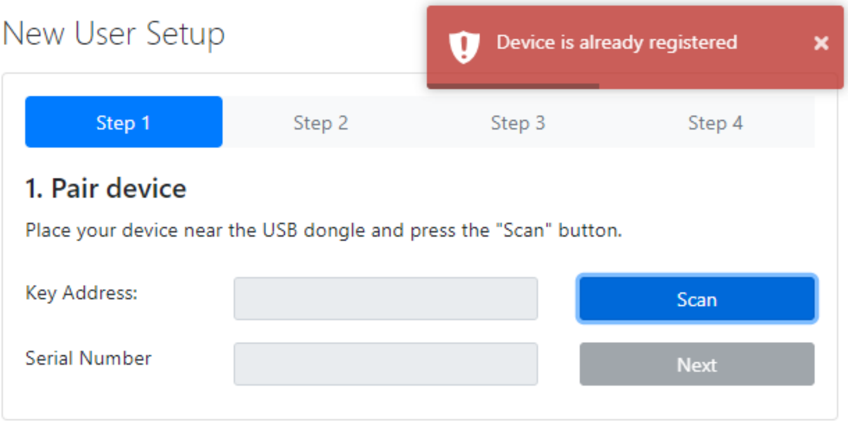
The PIN on the GateKeeper token cannot be recovered in any from as a security precaution. It is saved after hashing it with your Windows password.

If you have forgotten your PIN, please first recover your stored credentials, and then delete the GateKeeper database located at:

```
Windows:

c:\programdata\GateKeeper\gkdb_6.db

Mac:

/Library/Application\ Support/GateKeeper/GateKeeper.Service.App/Contents/Resources/gkdb_6.db
```

You will need to restart the GateKeeper Service before you can register your token again.

6.6 When I try to Scan a token, why does it say, 'Token is already registered'?



New User Setup

Device is already registered

1. Pair device

Place your device near the USB dongle and press the "Scan" button.

Key Address:

Serial Number

This means the token has already been registered with your user account in the past. If you don't remember the PIN for the token, follow the instructions given in the previous section.

6.7 Can I use my Mac's internal Bluetooth with GateKeeper?

No. Currently we only support the GateKeeper USB dongle on all Mac computers.

6.8 My Mac is not locking when I walk away. Why?

Restart your Mac after installing the software. After that, the Mac will lock when you walk away.

6.9 Can I add multiple domain credentials to my GateKeeper key?

Yes, to add more domain credentials to your token, please refer to section 2.5.1. Once you've added more domain credentials, the next time you try to unlock the computer, you'll see on the lock screen a drop-down menu listing all the domain credentials available. Select the username you want to log in with and hit Enter.

Questions? Concerns? Please email us at info@gkaccess.com.