



GATEKEEPER

GateKeeper Client Reference Guide

Untethered Labs, Inc.
support@gkaccess.com

Contents

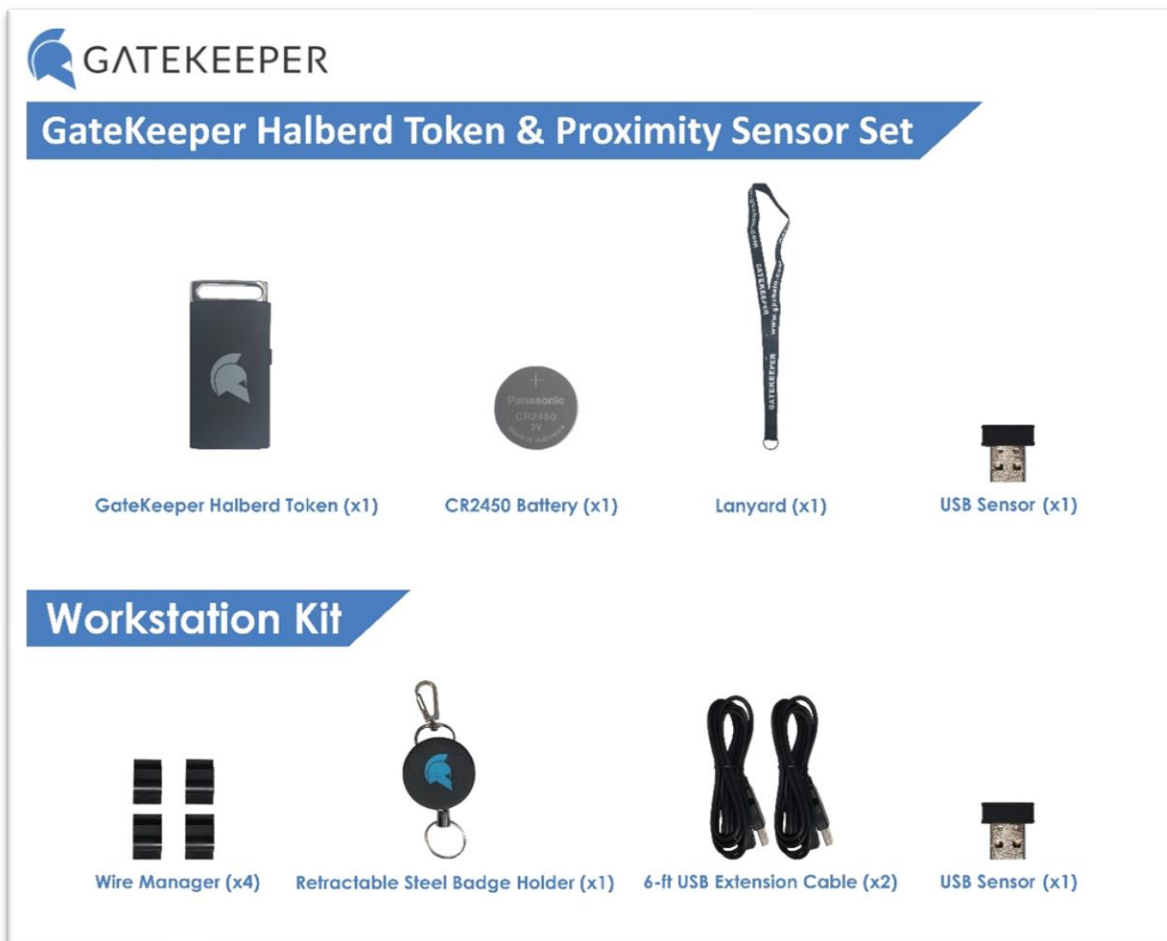
1	GateKeeper	2
1.1	What is GateKeeper?	2
1.2	What is the GateKeeper desktop application?	3
2	Supported Operating Systems	3
2.1	Windows 7 and Windows 10	3
2.2	Windows Embedded for Thin Clients.....	3
2.3	macOS 10.13 (High Sierra) and 10.14 (Mojave).....	3
3	GateKeeper Operation.....	4
3.1	Initial Setup	4
3.1.1	Bluetooth USB Proximity Sensor	4
3.1.2	Halberd Key (hardware token).....	4
3.1.3	Trident Application for Android Phones (software token)	5
3.2	Add New User	6
3.3	Connecting a User's token to the application.....	9
3.4	Credentials	10
3.5	Tokens	11
3.6	Settings.....	14
3.7	Help	19
3.8	About.....	20
4	Frequently Asked Questions	21
4.1	How can I download the GateKeeper desktop application?	21
4.2	How can I launch the GateKeeper application?.....	21
4.3	How can I verify my username and domain on Windows machines?	21
4.4	How many login credentials can be on a GateKeeper token?	21
4.5	Forgot the PIN to my GateKeeper token, can I recover it?.....	21
4.6	When I try to scan for tokens, why can't I select some?	22
4.7	Can I use my Mac's internal Bluetooth with GateKeeper?	22
4.8	My Mac is not locking when I walk away. Why?	22
4.9	Can I add multiple domain passwords to my GateKeeper token?	23

1 GateKeeper

1.1 What is GateKeeper?

GateKeeper is an access control system that authenticates users into computers and websites based on 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/passphrase again.

The GateKeeper comes with a wireless token (key fob), “Halberd”, that the users carry with them, a 3V CR2450 lithium coin cell battery, Bluetooth proximity USB sensor dongle (“receiver”) for the computer, and a lanyard. GateKeeper Enterprise users will also receive a workstation kit that includes 4 wire manager clips with adhesive backs, a retractable steel badge holder, two 6-ft. USB extension cables to optimally place your sensors, and one additional USB proximity sensor to maximize accuracy. These items are pictured below:



1.2 What is the GateKeeper desktop application?

The GateKeeper Client 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 authenticates (locks/unlocks) the computer based on the token's presence to the Bluetooth USB proximity sensor (dongle/receiver).

2 Supported Operating Systems

2.1 Windows 7 and Windows 10

The GateKeeper Client application fully supports Windows 7 and 10 operating systems. The client application can be installed on Windows computers using the MSI installer provided for that purpose. The client application can also be deployed through the command line and through Windows group policy.

2.2 Windows Embedded for Thin Clients

Thin clients with Windows Embedded 7 and 10 operating systems are also supported. The client application must be installed on the Windows Embedded Thin client or can be distributed by installing it on the Windows Embedded image. Furthermore, the thin clients requires USB CDC driver ([USBSE.SYS](http://USBSER.SYS)) to be installed. This driver can be added through the package manager for Windows Embedded. Finally, the "Always logged in mode" must be disabled for the thin client, and users logging on to the Thin client should be provided with Windows username and password either for the individual thin client, or as part of Active Directory.

2.3 macOS 10.13 (High Sierra) and 10.14 (Mojave)

The GateKeeper Client application package for macOS is available for download on our website. Only macOS versions 10.13 and 10.14 are currently supported. If your Mac has any operating system other than 10.13 or 10.14, please do not install the GateKeeper Client application. If you do, you will not be able to log in to your Mac.

3 GateKeeper Operation

3.1 Initial Setup

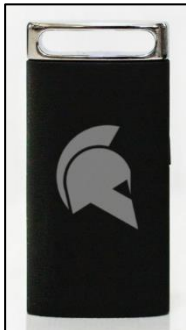
3.1.1 Bluetooth USB Proximity Sensor



The GateKeeper USB proximity sensor acts as the GateKeeper's Bluetooth SMART receiver and continuously scans for active GateKeeper tokens. The USB sensor should be placed in direct line of sight with the GateKeeper token (key) when you are working on your computer. We recommend using a USB extension cable to place it in the appropriate position. We also highly recommend using at least two sensors as this will increase range, coverage, and accuracy – resulting in a more optimal experience.



3.1.2 Halberd Key (hardware token)



To activate the Halberd token, slide open the battery cover and insert the battery by gently pressing it against the metal contact with the positive (+) 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.

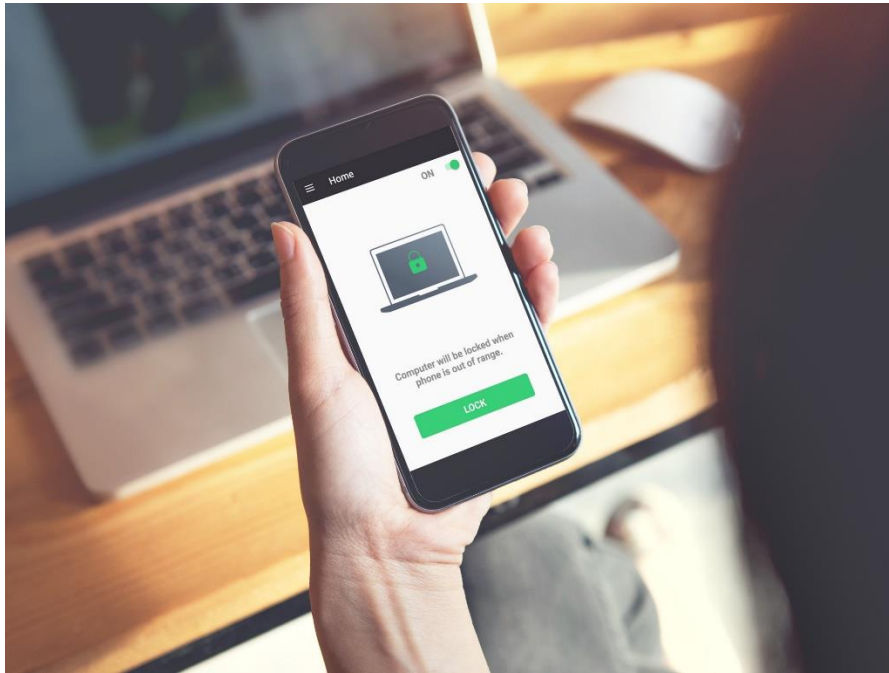


3.1.3 Trident Application for Android Phones (software token)



Download the [Android Trident](#) application from the Google Play Store. Install the Trident application on your phone, turn ON your phone's Bluetooth, then open the Trident app to make sure it is turned on. Remember, if your phone restarts for any reason, you must open the app to turn it back ON.





3.2 Add New User

To register a GateKeeper token with your computer's login credentials, go to the **New User** tab.

Step 1: Insert the CR-2450 battery into the token, plug the Bluetooth USB proximity sensor(s) into one of the front ports of the computer, touch the token to the USB proximity sensor, then click the **Scan Token** button.

GateKeeper Dashboard

ALEX LEE ANDROID 2 0 CONNECTED Search Knowledge Base

New User Setup

Step 1 Step 2 Step 3 Step 4

1. Pair GateKeeper Token

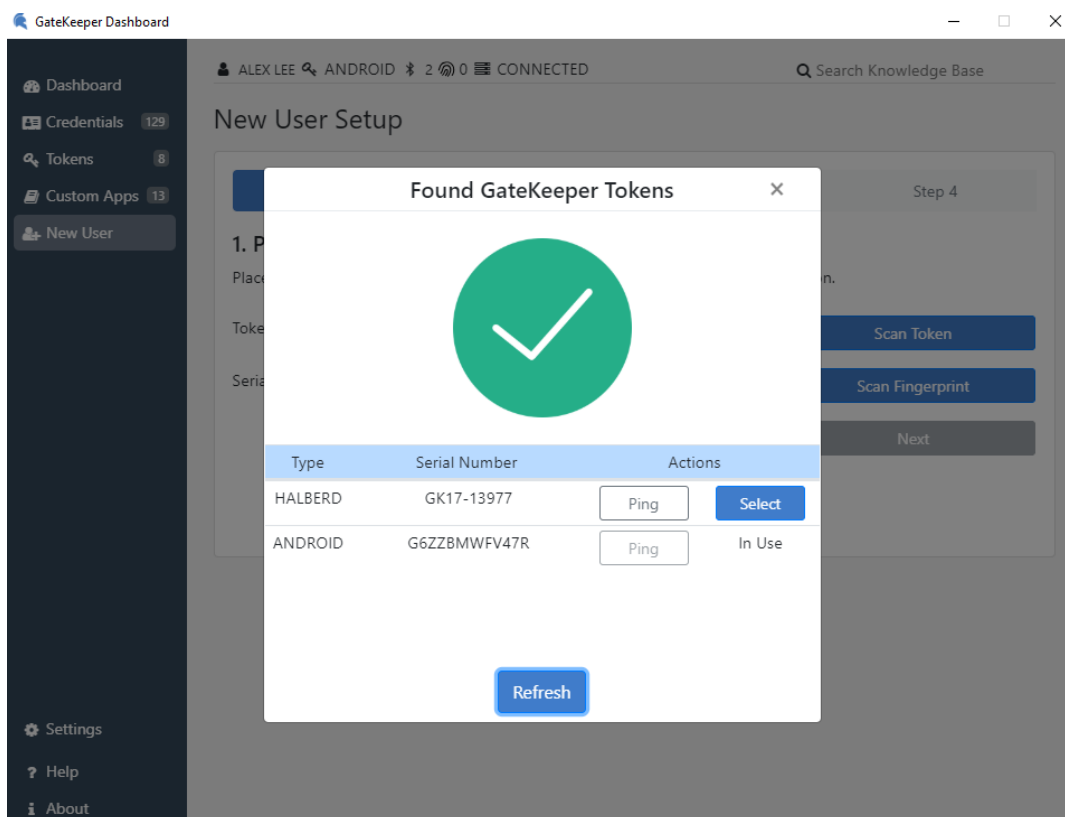
Place your GateKeeper token near the USB dongle and press the 'Scan Token' button.

Token Address: Scan Token

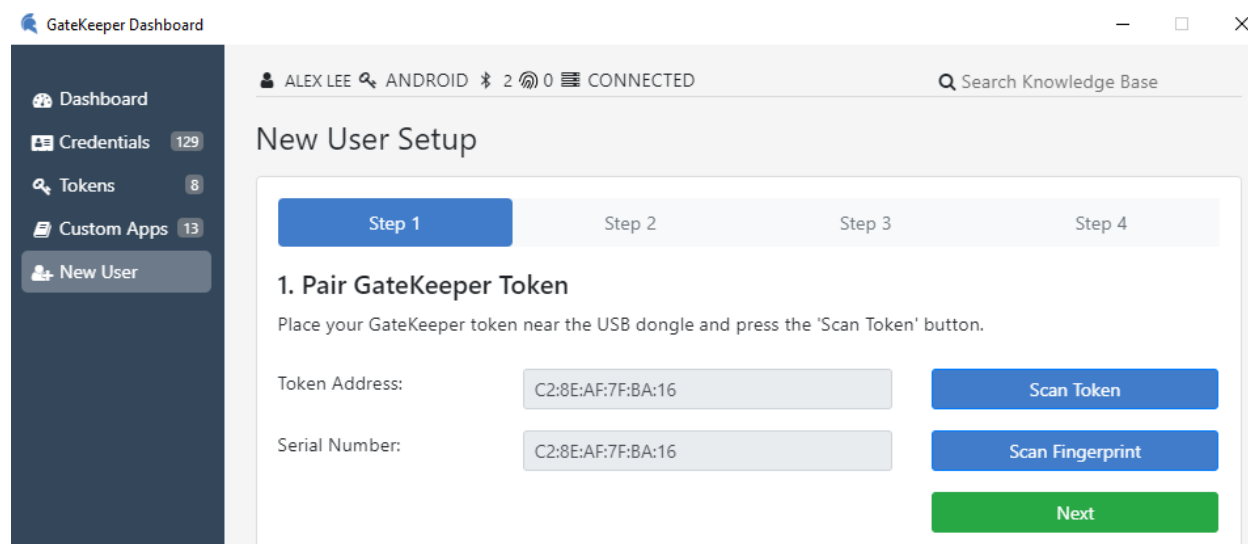
Serial Number: Scan Fingerprint

Next

The token's serial number will populate. "In Use" means that token is already registered and being used by someone. Click **"Select"** next to the token that you are registering.



After the token has been selected, the token's MAC address and serial number will auto-populate.



To use your smartphone as your key rather than the Halberd, please follow the same process above after [downloading](#), opening the GateKeeper Trident app and turning your phone's **Bluetooth ON**.

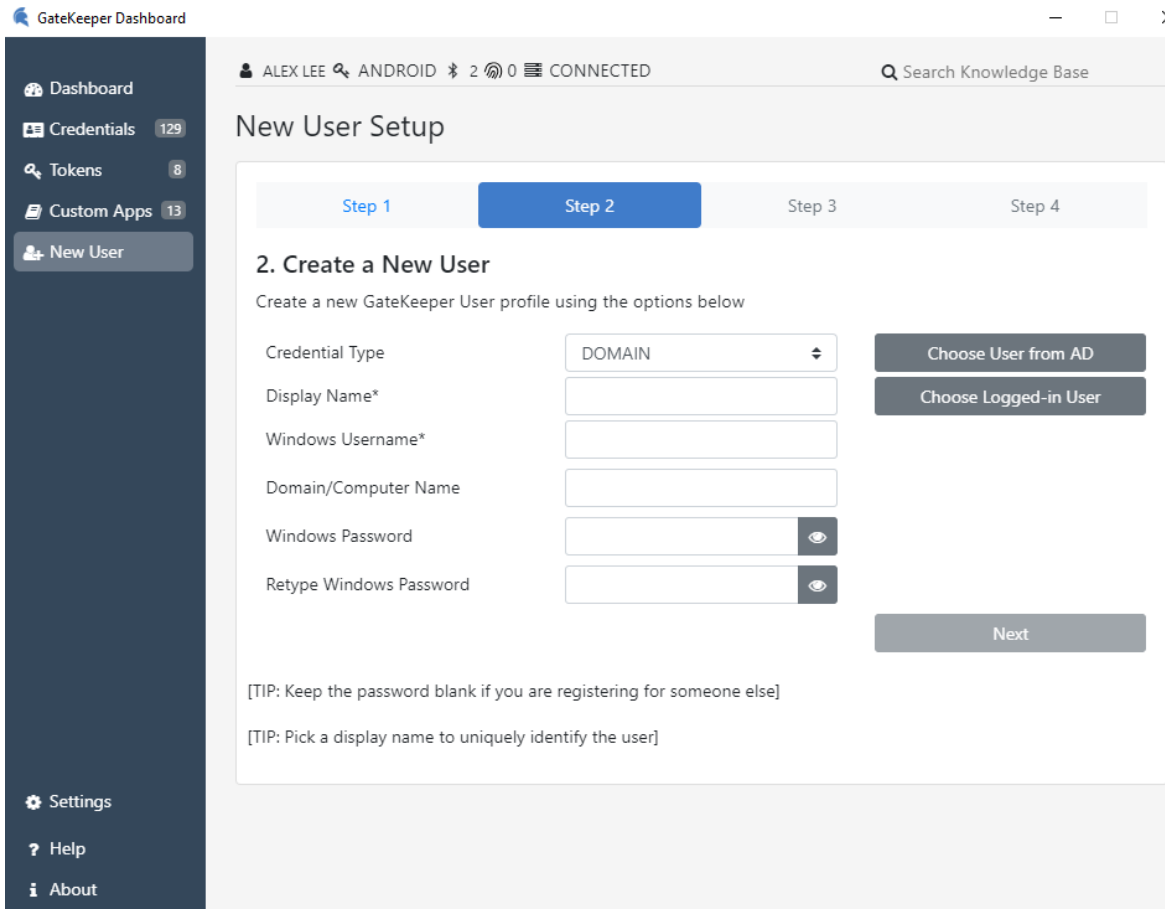
Step 2: If you are registering as a new user (or for a new user), you can simply click "**Choose Logged-in User**" to auto-fill the current user's profile that is logged in to Windows.

Important: This option only works if the same user is already logged into the computer. For example, if you're registering Bill as a new user, then the IT admin would have to be on Bill's computer while Bill's user profile is logged in.

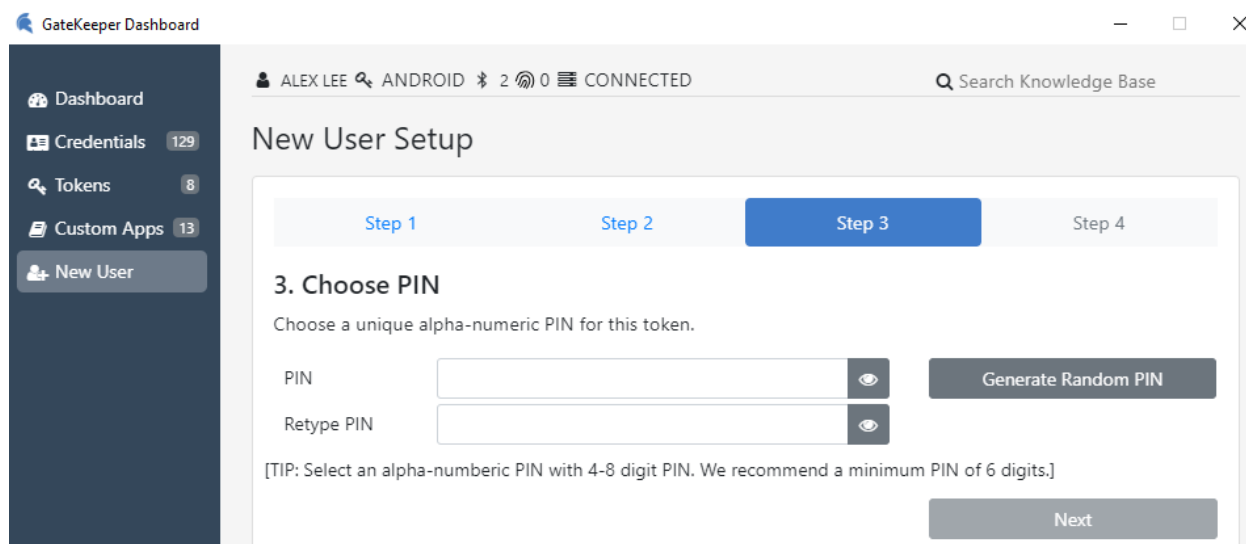
In this step, you can either type in the username, domain, and display name or you can pick the user from the Active Directory by clicking **Choose User from AD** and typing in the user's name.

If you're registering the token for a different user, you can leave the password field blank. Click **Next** to continue.

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

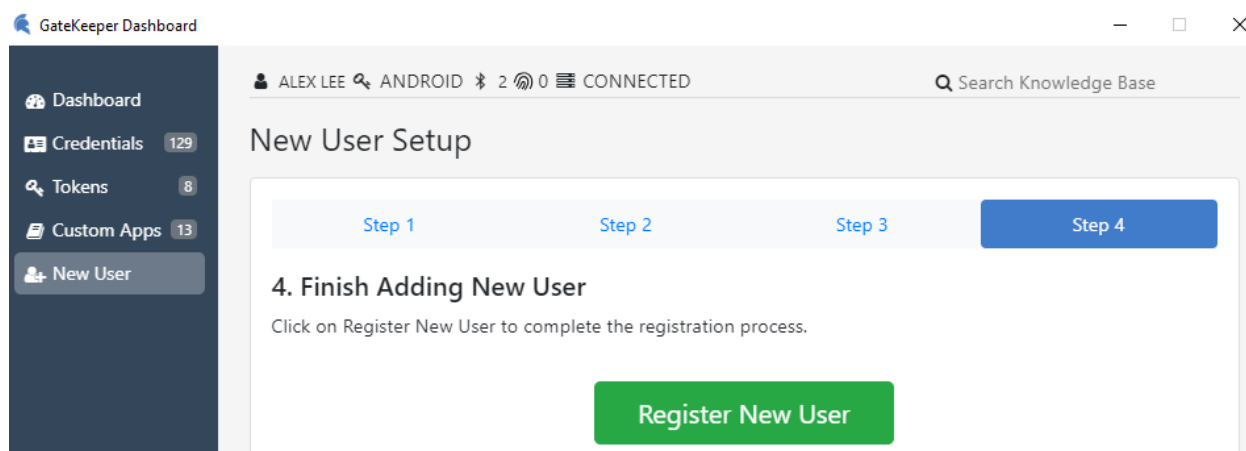


Step 3: Create a secret PIN between four to eight digits. You can also click **“Generate Random PIN”** (useful when registering for more than one user). Retype your PIN to confirm. Click **Next**.



The screenshot shows the GateKeeper Dashboard with a sidebar on the left containing links to Dashboard, Credentials (129), Tokens (8), Custom Apps (13), and New User. The main content area is titled 'New User Setup' and shows a progress bar with four steps: Step 1, Step 2, Step 3 (active), and Step 4. Step 3 is titled '3. Choose PIN' and instructs the user to 'Choose a unique alpha-numeric PIN for this token.' It features two input fields for 'PIN' and 'Retype PIN', each with a toggle for visibility. A 'Generate Random PIN' button is located to the right of the input fields. Below the input fields, a tip states: '[TIP: Select an alpha-numeric PIN with 4-8 digit PIN. We recommend a minimum PIN of 6 digits.]'. A 'Next' button is at the bottom right.

Step 4: Click Register New User.



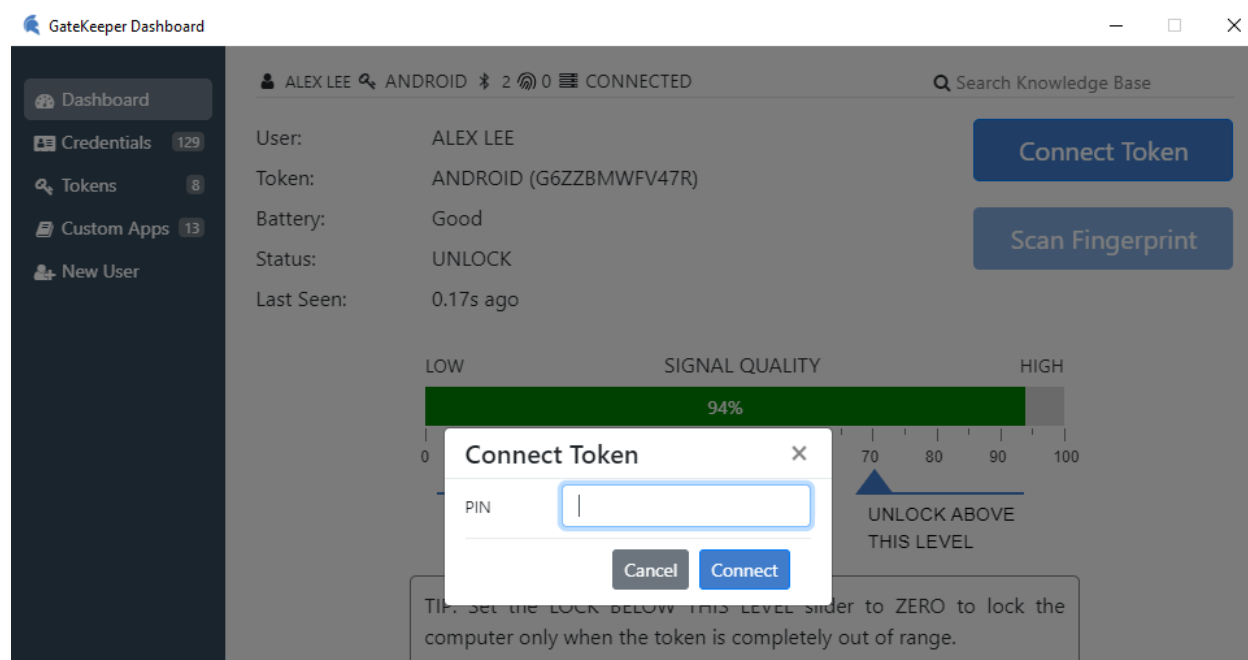
The screenshot shows the GateKeeper Dashboard with the same sidebar. The main content area is titled 'New User Setup' and shows a progress bar with four steps: Step 1, Step 2, Step 3, and Step 4 (active). Step 4 is titled '4. Finish Adding New User' and instructs the user to 'Click on Register New User to complete the registration process.' A large green 'Register New User' button is centered at the bottom.

A notification will pop up in the upper-right 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 **Copy**.

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

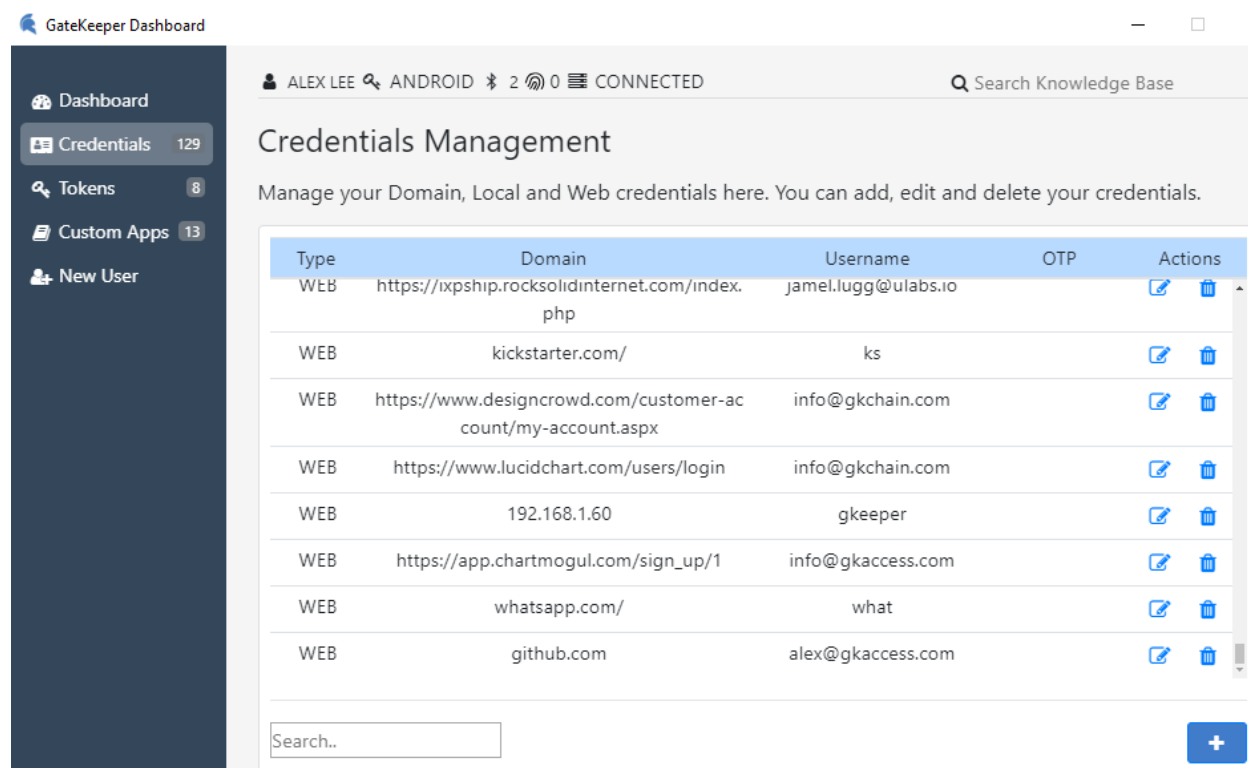
3.3 Connecting a User's token to the application

To connect a user's GateKeeper token to the computer, go to **Dashboard**, click **Connect Token**, type in the PIN for the token, and click **Connect**. (Make sure your admin put you in the same **Group** as this will give your user profile permission to access this computer).

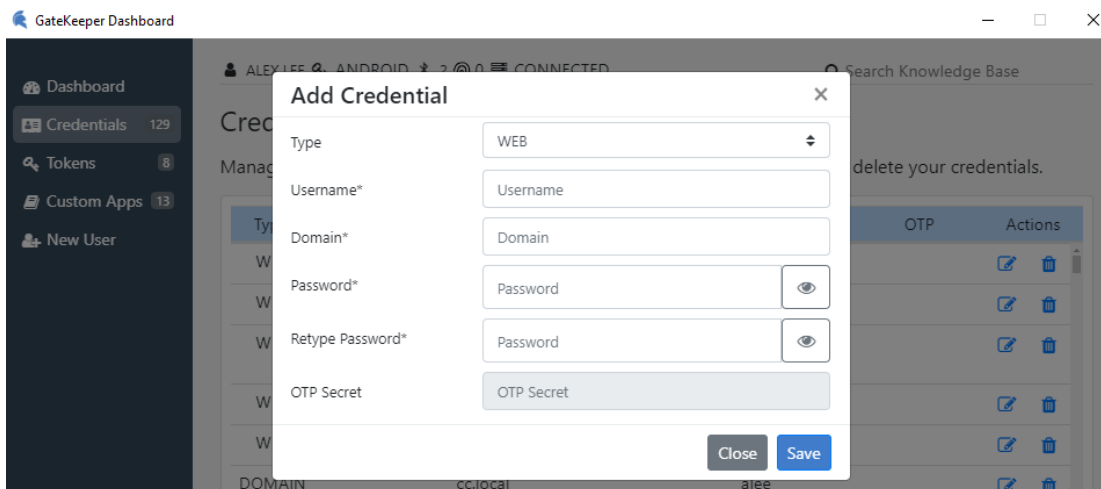


3.4 Credentials

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.

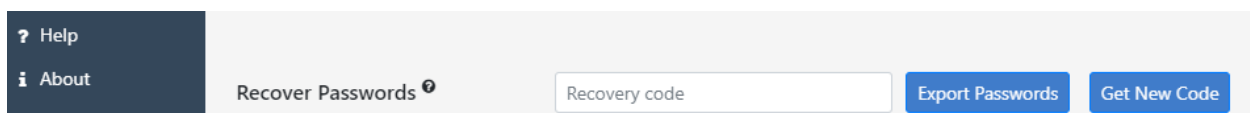


To add a new credential, click on '+'. Select the type of credential (Web/OTP/Winlocal/Maclocal/Domain), fill in the details, and click **Save Changes**. This will add the credential to the user's account, and then the user can log in with their token using these credentials.

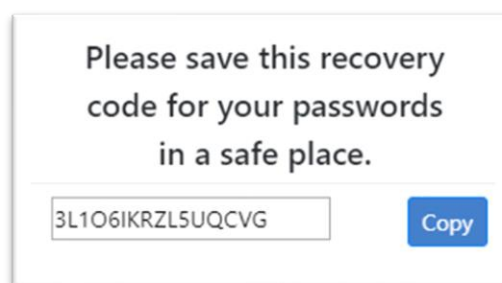


If you have misplaced your token, please use this function to recover your web login credentials.

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



After your PIN has been verified, the following screen will appear with a code.



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

To recover your web credentials, enter your code in the text box **Recover Credentials**, and click **Get Credentials**. This will save your credentials in a CSV file on your computer.

3.5 Tokens

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.

GateKeeper Dashboard

ALEX LEE ANDROID 2 0 CONNECTED Search Knowledge Base

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	E9:81:AD:F8:2A:ED	GK17-13374	-	✗	
HALBERD	ED:6A:22:96:A3:1E	GK17-18605		✗	
HALBERD	CF:19:A4:38:BA:80	GK17-10567		✗	
ANDROID	G6ZZBMWV47R	G6ZZBMWV47R		N/A	
ANDROID	1NU34MQS9CX7B	1NU34MQS9CX7B	-	N/A	
HALBERD	F7:B3:AF:64:D7:20	GK17-17429		✗	
ANDROID	52KXGTC6E3H3	52KXGTC6E3H3		N/A	
HALBERD	F1:6E:9B:1E:21:7E	GK17-10555		✗	

Search..


To add a new token key, touch it to the plugged-in USB proximity Bluetooth sensor on the computer and then click on '+'. To add your phone. Open the GateKeeper Trident app (software token) on your phone, make sure the phone's Bluetooth is **ON**, and then click '+'. The screen for scanning GateKeepers will appear. Select the token that you would like to add. Create a PIN for the token and click **Save**. This will add the token to the user's account and now the user can access all their computer and web credentials with this token (key) as well.

GateKeeper Dashboard

ALEX LEE ANDROID 2 0 0 CONNECTED Search Knowledge Base



Token Management

Touch GateKeeper Token to USB Dongle




Type	Serial Number	Actions

Refresh

Add new GateKeeper token  

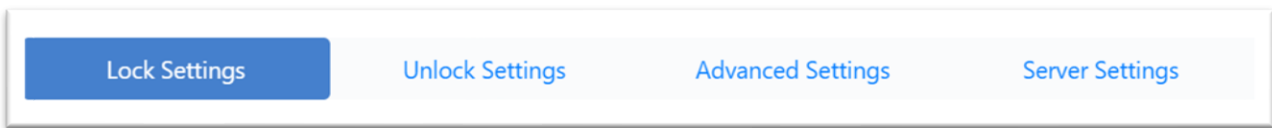
Found GateKeeper Tokens



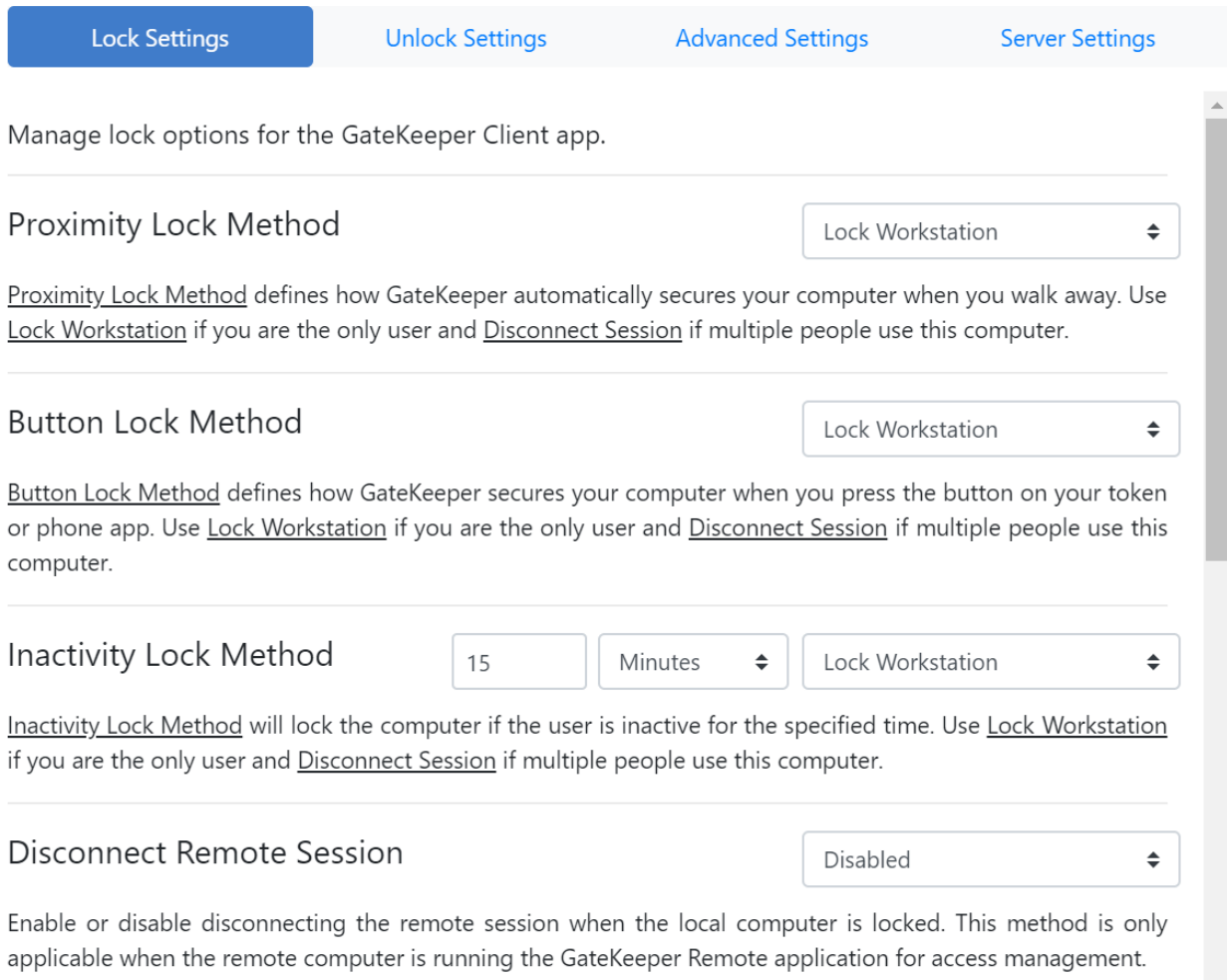
Type	Serial Number	Actions
ANDROID	G6ZZBMWFV47R	<div>Ping</div> <div>In Use</div>
HALBERD	C2:8E:AF:7F:BA:16	<div>Ping</div> <div>Select</div>

Refresh

3.6 Settings



3.6.1 Lock 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 Minutes Lock Workstation

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.

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 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 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 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.

3.6.2 *Unlock Settings*

[Lock Settings](#)**Unlock Settings**[Advanced Settings](#)[Server Settings](#)

Manage unlock options for the GateKeeper Client app.

Unlock Method

Press Enter Key to Login ▾

Unlock Method defines how GateKeeper will unlock your computer. We recommend the GateKeeper + PIN option for secure 2-factor authentication. The GateKeeper + PIN method will always allow a user to log in irrespective of the chosen Unlock Method.

Quick Return Timeout

60

Seconds ▾

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

Unlock Method defines how GateKeeper will unlock your computer. We recommend GateKeeper with PIN 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 + PIN. 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.

3.6.3 *Advanced Settings*

[Lock Settings](#)[Unlock Settings](#)[Advanced Settings](#)[Server Settings](#)

Manage advanced settings for the GateKeeper client application.

GateKeeper Application Launcher

Disabled

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

Firmware Update

Update Firmware

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

Secure Key

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

Factory Reset

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

Notifications

GateKeeper Application Launcher allows users to choose programs to automatically launch either at startup or login.

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.

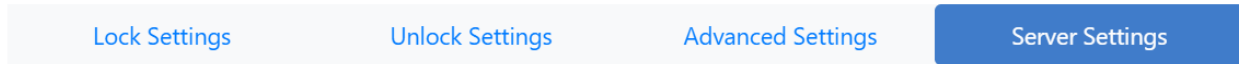
Secure Key Exchange option allows user to exchange a secure key with your GateKeeper token to make it cryptographically unique. This will enhance the security of proximity authentication by verifying One-Time-Passcodes sent by the token.

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.

3.6.4 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

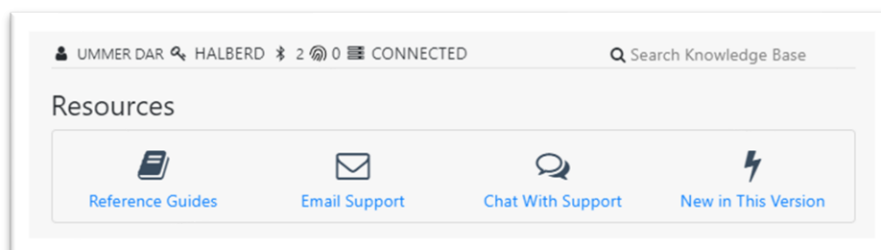
This is the full server IP address including 'https://' of the GateKeeper Hub server installed on your network.

Port Number

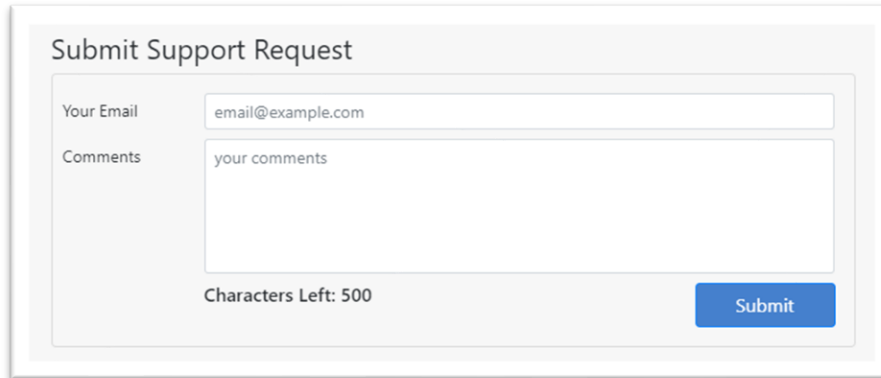
This is the port number being used by the GateKeeper Hub server installed on your network. The default port number is 3015.

3.7 Help

Links to download Reference Guides, contact support, and live chat. Also, learn about the latest updates by clicking **New in This Version**.



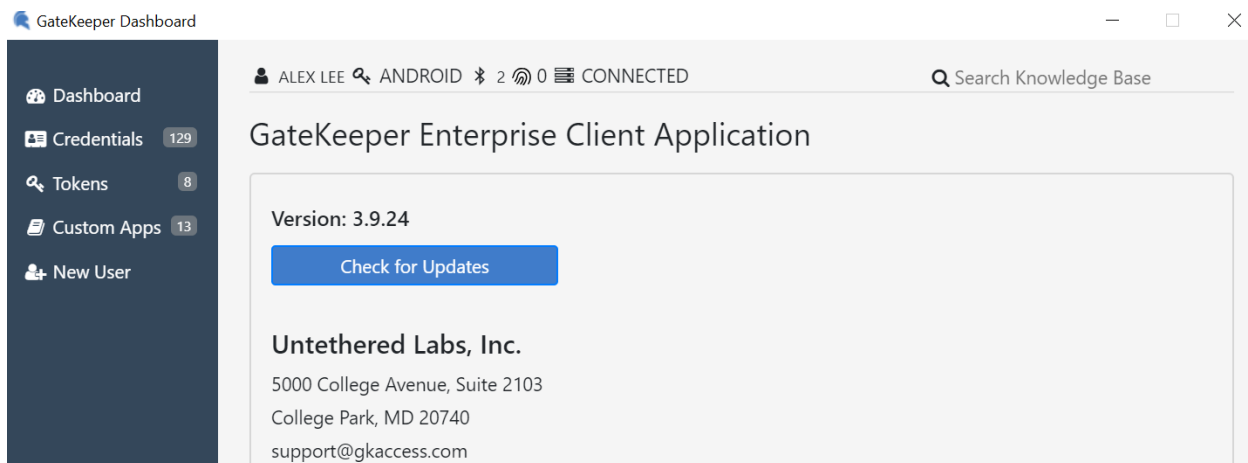
Users can reach out to our support team by using the **Submit Support Request** form in the application or emailing support@gkaccess.com. For additional assistance or inquiries, please email us at info@gkaccess.com.



The image shows a 'Submit Support Request' form. It has a title bar at the top. Below the title, there are two input fields: 'Your Email' with the value 'email@example.com' and 'Comments' with the value 'your comments'. Below the 'Comments' field, it says 'Characters Left: 500'. At the bottom right, there is a blue 'Submit' button.

3.8 About

Shows the application version you are currently using.



4 Frequently Asked Questions

4.1 How can I download the GateKeeper desktop application?

To download the GateKeeper Client desktop application, go to our website <https://gkaccess.com/portal> and log in to your customer portal account.

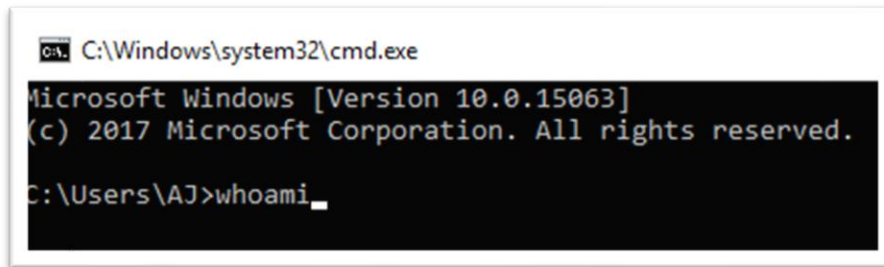
Navigate to **Software** and click the appropriate OS version of your computer (Win or Mac) to download.

4.2 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 the icon to launch it.

4.3 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 the domain and username in the format <domain-name>/<username>



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Users\AJ>whoami_
```

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

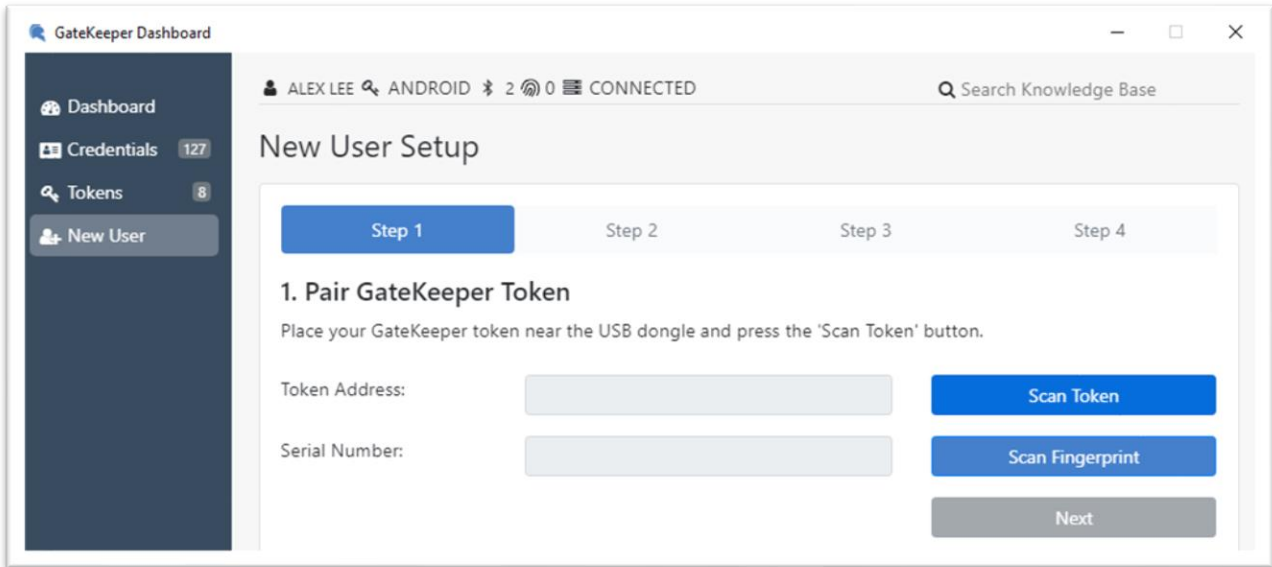
The GateKeeper token can manage an unlimited number of credentials. To add more credentials, log in with your GateKeeper and add them on the **Credentials** tab.





4.5 Forgot the PIN to my GateKeeper token, can I recover it?

The PIN for a GateKeeper token cannot be recovered in any form as a security precaution.

If you have forgotten your PIN, please first recover your stored credentials, then clear the local database by using the Factory Reset option. For enterprise users, the Hub administrator can reset your PIN.:

4.6 When I try to scan for tokens, why can't I select some?



Registered	Ping	Select
Yes		
Yes		

If after scanning and finding nearby GateKeeper tokens or Trident app, the checkmark under the select option is grayed out, then it means the token has already been registered. If you don't remember the PIN for the token, follow the instructions given in the previous section.

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

Currently, we only support the GateKeeper Bluetooth USB sensor on Mac computers.

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

Please restart your Mac after installing the software. Then the Mac will lock when you walk away.

4.9 Can I add multiple domain passwords to my GateKeeper token?

Yes, to add more domain credentials to your token. 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 support@gkaccess.com.