Contents
1 GateKeeper ........................................................................................................................................... 2
  1.1 What is GateKeeper? ......................................................................................................................... 2
  1.2 What is the GateKeeper desktop application? .................................................................................. 3
2 GateKeeper Operation ........................................................................................................................................... 3
  2.1 Initial Setup ........................................................................................................................................... 3
    2.1.1 USB Proximity Sensor .................................................................................................................. 3
    2.1.2 Halberd Key (hardware token) ...................................................................................................... 3
    2.1.3 Trident Application for Android Phones (software token) ........................................................... 3
  2.2 Add New User ....................................................................................................................................... 4
  2.3 Connecting a User’s token to the application .................................................................................... 7
  2.4 Credentials .......................................................................................................................................... 8
  2.5 Tokens .................................................................................................................................................. 9
  2.6 Settings ............................................................................................................................................... 10
  2.7 Help ................................................................................................................................................... 13
  2.8 About ................................................................................................................................................. 14
3 Frequently Asked Questions ................................................................................................................................. 15
  3.1 How can I download the GateKeeper desktop application? ............................................................. 15
  3.2 How can I launch the GateKeeper application? .................................................................................. 15
  3.3 How can I verify my username and domain on Windows machines? ........................................... 15
  3.4 How many login credentials can be on a GateKeeper token? ............................................................ 15
  3.5 I don’t remember the PIN to my GateKeeper token, can I recover it? ........................................... 15
  3.6 When I try to Scan a token, why can’t I select it? ............................................................................... 16
  3.7 Can I use my Mac’s internal Bluetooth with GateKeeper? ............................................................... 17
  3.8 My Mac is not locking when I walk away. Why? ................................................................................. 17
  3.9 Can I add multiple domain credentials to my GateKeeper token? .................................................. 17
  3.10 What does ‘Server’ and ‘Scanning’ on the lower left of the application indicate? ........................... 17
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 again.

The GateKeeper comes with a wireless token (key), “Halberd”, that the users carry with them, a 3V CR2450 lithium coin cell battery, Bluetooth USB sensor dongle for the computer, and a lanyard. 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 USB proximity sensor (dongle/receiver).

2 GateKeeper Operation

2.1 Initial Setup

2.1.1 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.

2.1.2 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.

2.1.3 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.
2.2 Add New User

To register a GateKeeper token with your computer’s login credentials, click the New User tab, then follow the instructions below.

**Step 1:** Insert the battery into the token, plug the USB proximity sensor(s) into one of the front ports of the computer, touch the token to the USB sensor, then click the Scan Token button. Token will beep rapidly for 2 seconds and the token’s serial number will populate. Click Next.

The following image shows the initial screen after clicking ‘Scan Token’.

![Image of GateKeeper initial screen after scanning token]

After the token has been selected, the token’s MAC address and serial number will auto-populate.
If you would like 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: 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: Type in a secret PIN between four to eight digits. You can also click “Generate Random PIN” for the system to create a PIN for you (useful when registering for more than one user). Click Next to continue.

Step 4: Click Register New User.
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.

### 2.3 Connecting a User’s token to the application

To connect a user’s token to the application, go to Dashboard, click Connect Token, type in the PIN for the token, and click Connect.
2.4 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.

### 2.5 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.

To add a new Halberd key, touch it to the plugged-in USB sensor on the computer and then click on ‘+’.

To add your phone. Open the 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.

![Image of Token Management screen]

### 2.6 Settings

#### 2.6.1 Lock and Unlock Settings

**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.

- 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.

- 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.

- 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.

- Enable
- Disable

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

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

### 2.6.2 Advanced Settings

**‘Token Visibility Timeout’** sets a lock timer if no token (data packets) 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.

**‘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.

‘Windows username/password login’ 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.

‘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. We recommend setting this option to NEVER.

‘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.

‘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.

2.6.3 Hub 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 check the ‘Override registry parameters’ box and enter the new IP address.
2.7 Help

Help has 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.
2.8 About

The About tab shows the application version you are currently using. Please check with your GateKeeper administrator to see if you have the latest version.
3 Frequently Asked Questions

3.1 How can I download the GateKeeper desktop application?

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

Navigate to the Software section and select the appropriate OS version for your computer (Win or Mac) to download.

3.2 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.

3.3 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>

3.4 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.

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

The PIN for a 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 must restart the GateKeeper Service before you can register your token again.

### 3.6 When I try to scanned for tokens, why can’t I select some?

![GateKeeper Dashboard](image)

![Registered Ping Select](image)
The checkmark will be grayed out under “Select”. 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.

3.7 Can I use my Mac’s internal Bluetooth with GateKeeper?

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

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

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

3.9 Can I add multiple domain credentials 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.

3.10 What does ‘Server’ and ‘Scanning’ on the lower left of the application indicate?

The ‘Server’ notation with a checkmark indicates that the computer is connected to the GateKeeper Hub. An ‘x’ indicates the computer is not connected to the GateKeeper, please contact your administrator.

The ‘Scanning’ notation with a USB icon indicates that active GateKeeper tokens are in vicinity of the computer. An ‘x’ indicates there are no active GateKeeper keys around. But, if there are active tokens around, please verify that the USB sensor (dongle) is connecting properly. To verify, please go to Device Manager and check under Ports for TI CC2540 USB CDC Serial Port. If you don’t see the port, please contact your GateKeeper administrator.

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