

SENTRY™ Gatekeeper v5.6 User's Guide



911 Secure LLC
280 S. Lemon Ave. 2155 Walnut, CA 91788
Telephone: (213) 425-2050
E-Mail: info@911secure.com
Website: www.911Secure.com

Revision 10/15/2025

TABLE OF CONTENTS

Self-Registration and First-Time Login Process	4
Self-Registration and First-Time Login for Azure AD Users	5
Self-Registration and First-Time Login for Azure AD Users with SENTRY™ Cloud Enterprise	10
Self-Registration and First-Time Login for Azure AD Users with SENTRY™ Cloud Enterprise (with DIDs)	15
Self-Registration and First-Time Login for SENTRY™ Cloud Credentials Users	20
Self-Registration and First-Time Login for SENTRY™ Cloud Credentials Users with SENTRY™ Cloud Enterprise	26
Self-Registration and First-Time Login for SENTRY™ Cloud Credentials Users with SENTRY™ Cloud Enterprise (with DIDs)	32
Logging in with Azure AD Credentials	38
Logging in with SENTRY™ Cloud Credentials	39
SENTRY™ Gatekeeper v5.6 Users Guide	40
Selecting an Active Phone in SENTRY™ Gatekeeper	40
Setting a Remote Address Location in SENTRY™ Gatekeeper	43
Editing an Address in SENTRY™ Gatekeeper	51
Deleting an Address in SENTRY™ Gatekeeper	55
Setting an On Premise Location in SENTRY™ Gatekeeper – Location Services Enabled (Non-VDI)	56
Setting a Location in SENTRY™ Gatekeeper – Location Services Disabled (Non – VDI)	59
Remote	59
On-Premise	64
Other SENTRY™ Gatekeeper Features	68
SENTRY™ Gatekeeper v5.6 User’s Guide – VDI Enabled	74
Definitions	74
Enabling VDI Support for SENTRY™ Gatekeeper	75
Client Installation	75
Windows Registry / Group Policy	76
Setting an Address as a VDI Enabled Remote Worker	77
Without Location Services	77
With Location Services Using Client Location Redirection	86
Setting an Address as a VDI Enabled On-Premise User	89
Without Location Services	89
With Location Services Using Client Location Redirection	98

SENTRY™ Gatekeeper Troubleshooting Guide	101
SENTRY™ Cloud and SENTRY™ Gatekeeper Whitelisting URLs	105
Whitelisting Required SENTRY™ Cloud URLs	105
Whitelisting Required SENTRY™ Gatekeeper URLs	105

SELF-REGISTRATION AND FIRST-TIME LOGIN PROCESS

When launching the SENTRY™ Gatekeeper application for the first time, all users not preloaded by their SENTRY™ Cloud Administrator will go through a self-registration process. By completing this registration process, users will be able to sign into SENTRY™ Gatekeeper for the first time. This will negate the need to import a list of SENTRY™ Gatekeeper users and DIDs (or Extensions if your organization uses a SENTRY™ Cloud Enterprise solution) into SENTRY™ Cloud via the Users > Import function.



STOP! PLEASE NOTE: Unlike Remote DIDs and On Premise DIDs in SENTRY™ Cloud, **Cloud-sourced DIDs ARE capable of being overtaken by SENTRY™ Gatekeeper users.** We strongly recommend that remote workers dial 933 once they have set their information within SENTRY™ Gatekeeper. This will help ensure they are hearing a correct readback of their DID and address information.



STOP! PLEASE NOTE: If you utilize a **VPN**, you **MUST** follow the process to log into SENTRY™ Gatekeeper and set your address **BEFORE** connecting to your VPN. Failure to do so may result in the inability to fully complete the process for setting your address.



STOP! PLEASE NOTE: If you have more than one work email address, **choose one** to use consistently. Using two different email addresses can result in an inability to log in. If you are unsure which email address to use, please contact your administrator.



STOP! PLEASE NOTE: If your organization uses a **SENTRY™ Cloud Enterprise** solution, then users signing into SENTRY™ Gatekeeper for the first time will enter in their assigned **Extension**.



STOP! PLEASE NOTE: SENTRY™ Gatekeeper users who want to use Location Services for discovery must have **Location Services** and “**Let apps access your location**” enabled on their device under “**Privacy and security > Location**” for the SENTRY™ Gatekeeper application to function.

SELF-REGISTRATION AND FIRST-TIME LOGIN FOR AZURE AD USERS

The instructions detailed below will allow SENTRY™ Gatekeeper users from an organization authenticating against Azure Active Directory credentials to log into SENTRY™ Gatekeeper for the first time. In most cases, users will use their normal organizational login account.

1. Launch the SENTRY™ Gatekeeper application. Click on **“SIGN IN”**.

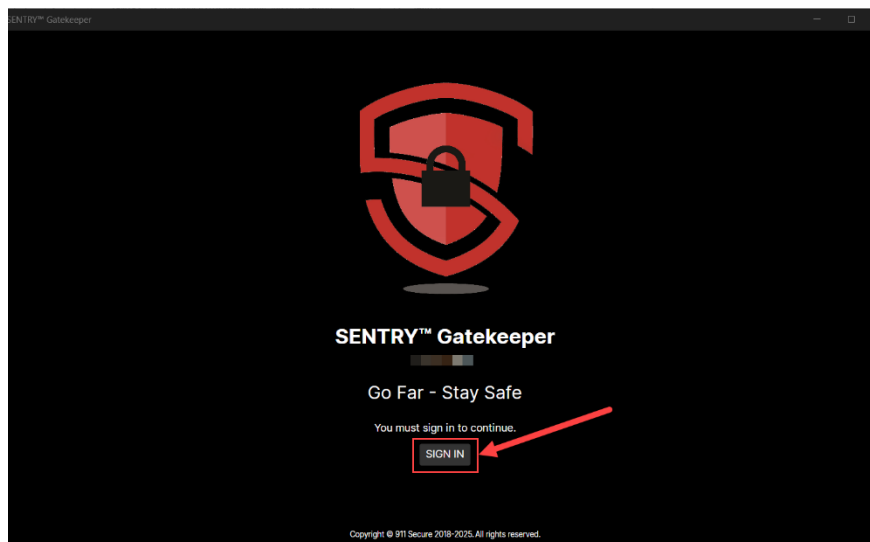


Figure 1

2. Click on **“Sign in with Azure AD credentials”**.

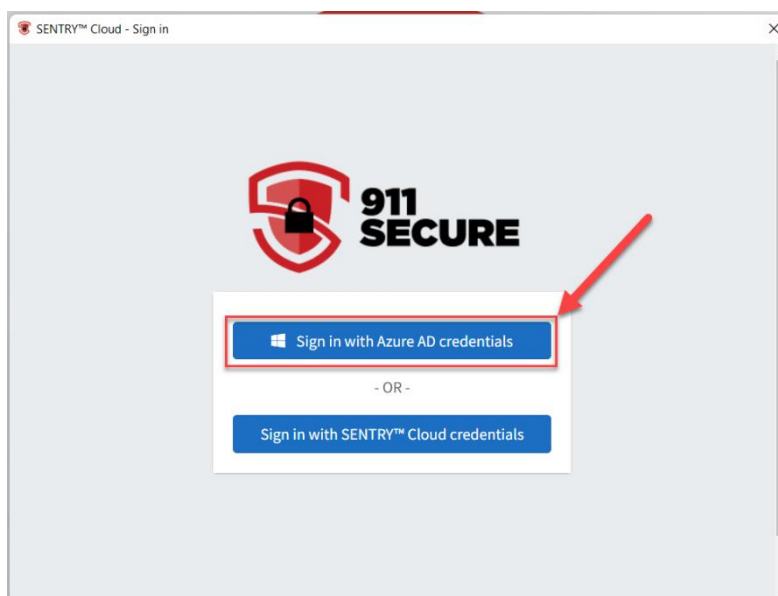


Figure 2

3. Enter your regular work email address and click **“Next”**.

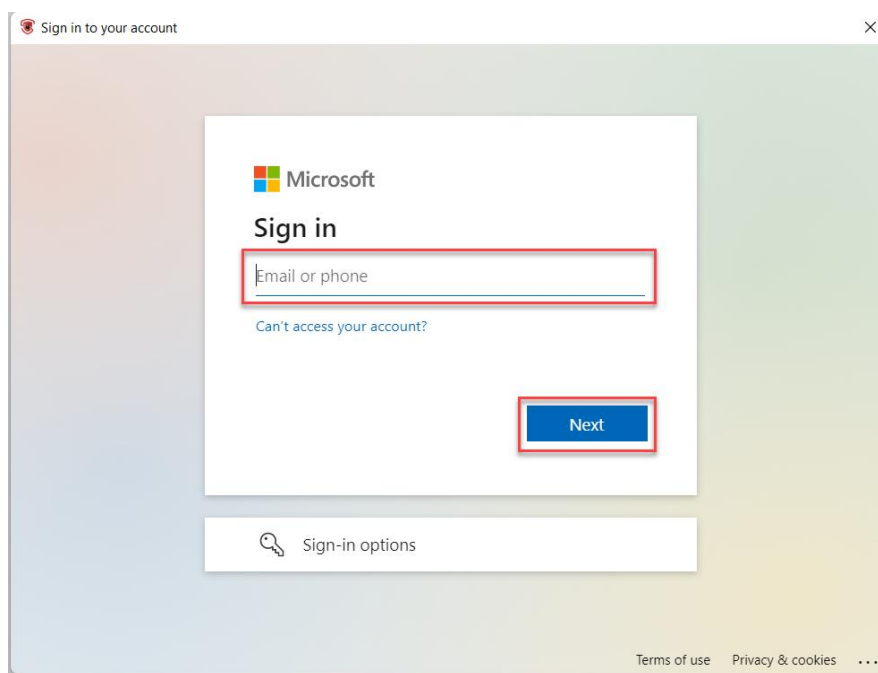


Figure 3

4. Enter in your corresponding work password and click **“Sign in”**.

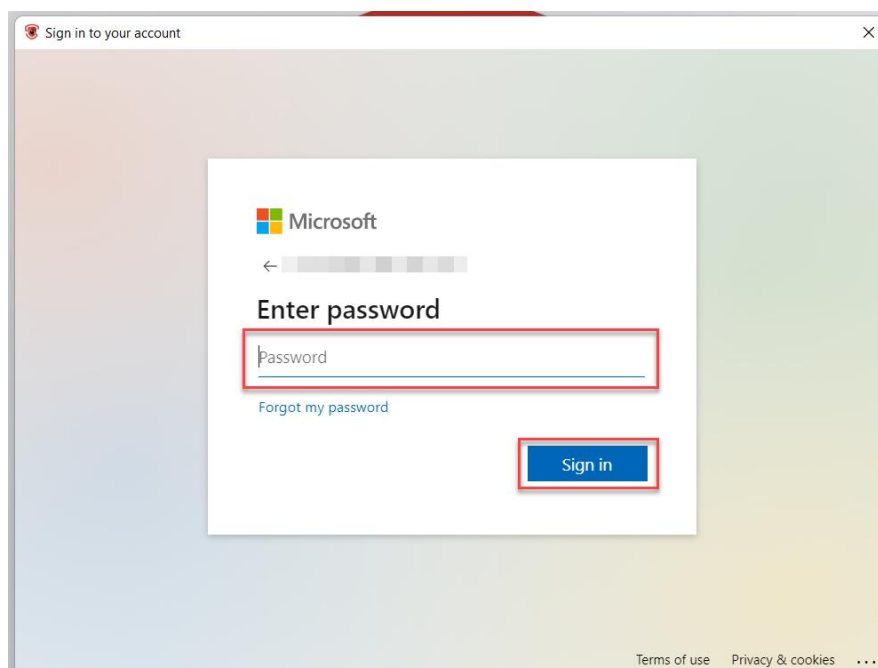
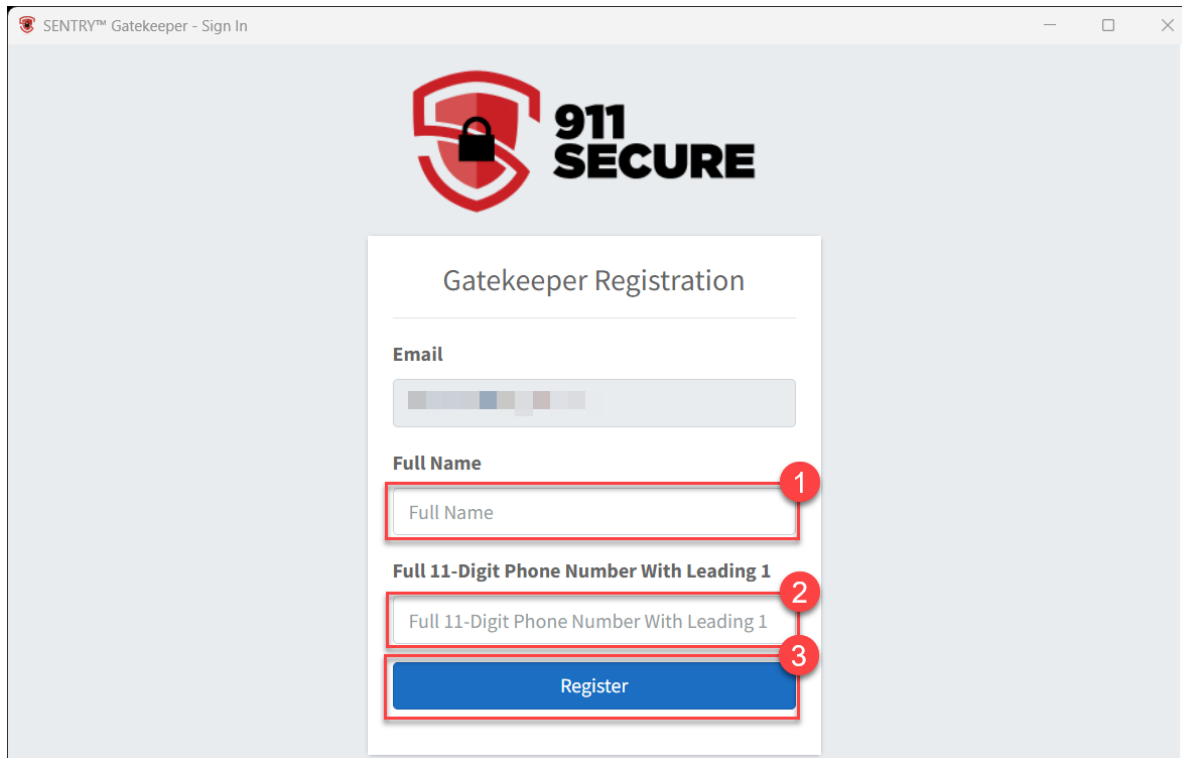


Figure 4

5. Enter in your **full name** and assigned **ELIN / DID** (i.e., the full 10-digit phone number used with your softphone device prepended with a leading “1” such as “15555552468”) into the appropriate fields. Once finished, click “**Register**” to complete the self-registration process.



SENTRY™ Gatekeeper - Sign In

**911
SECURE**

Gatekeeper Registration

Email

Full Name

Full 11-Digit Phone Number With Leading 1

Register

Figure 5

6. **PLEASE NOTE:** When logging into the application for the very first time, you will be met with a “**Gatekeeper User Acceptance**” window. Its purpose is to help end users understand why they must set their location and the importance of doing so. While the exact User Acceptance message may vary depending on the customer, the **default verbiage** is displayed below. Users must click the “**I have read and understand the above statement**” **checkbox**, then click on the “**OK**” button.

SENTRY™ Gatekeeper User Acceptance Default Message:

“SENTRY™ Gatekeeper is an application for keeping softphone users safe whenever they are working from a remote / offsite location. It requires users to provide accurate location information so any 911 call made from their softphone can be routed to the closest Public Safety Answering Point. By clicking the OK button below, I acknowledge that I will enter only accurate location information whenever my work location changes.”

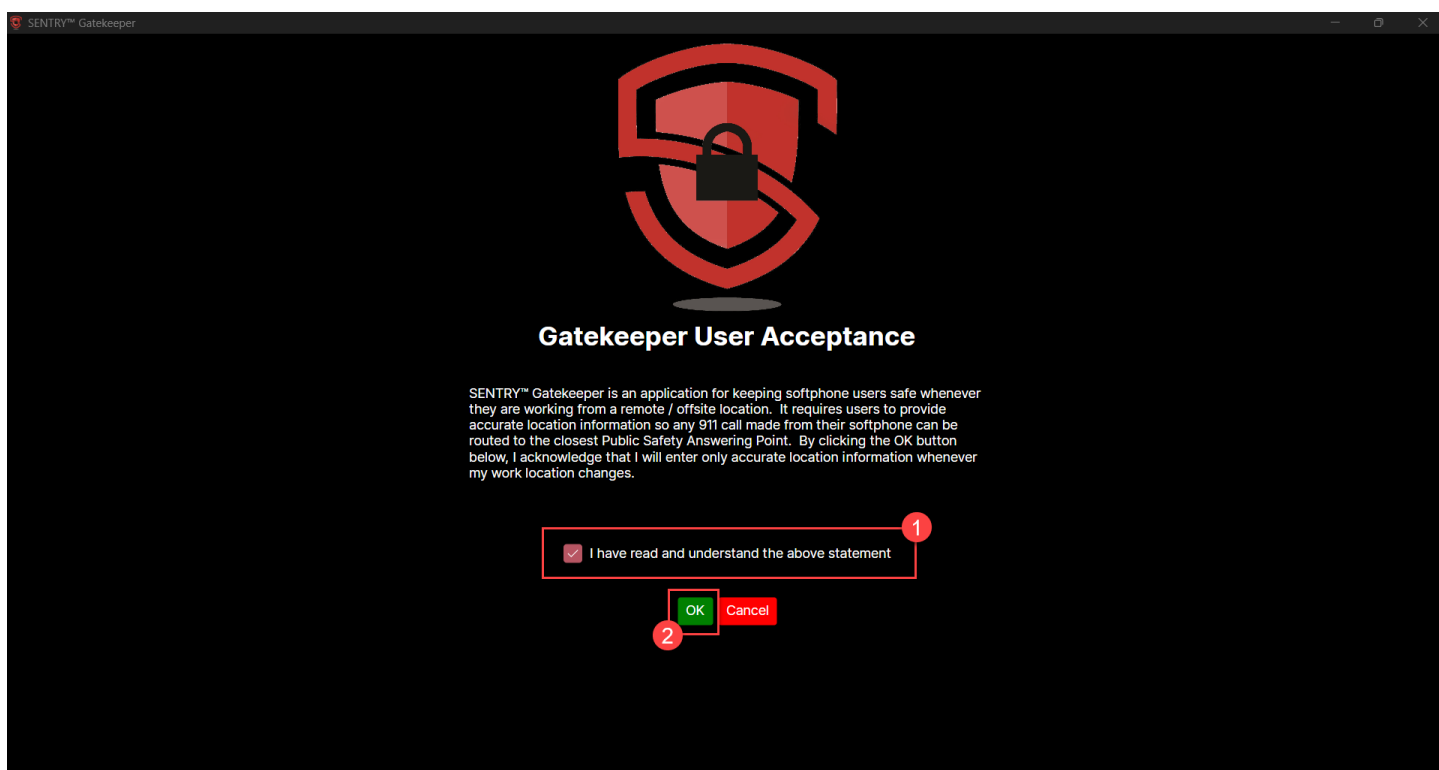


Figure 6

- Once you have signed in and clicked “OK” for the User Acceptance, you will be brought to the SENTRY™ Gatekeeper client screen and can begin the process of setting or selecting your address.

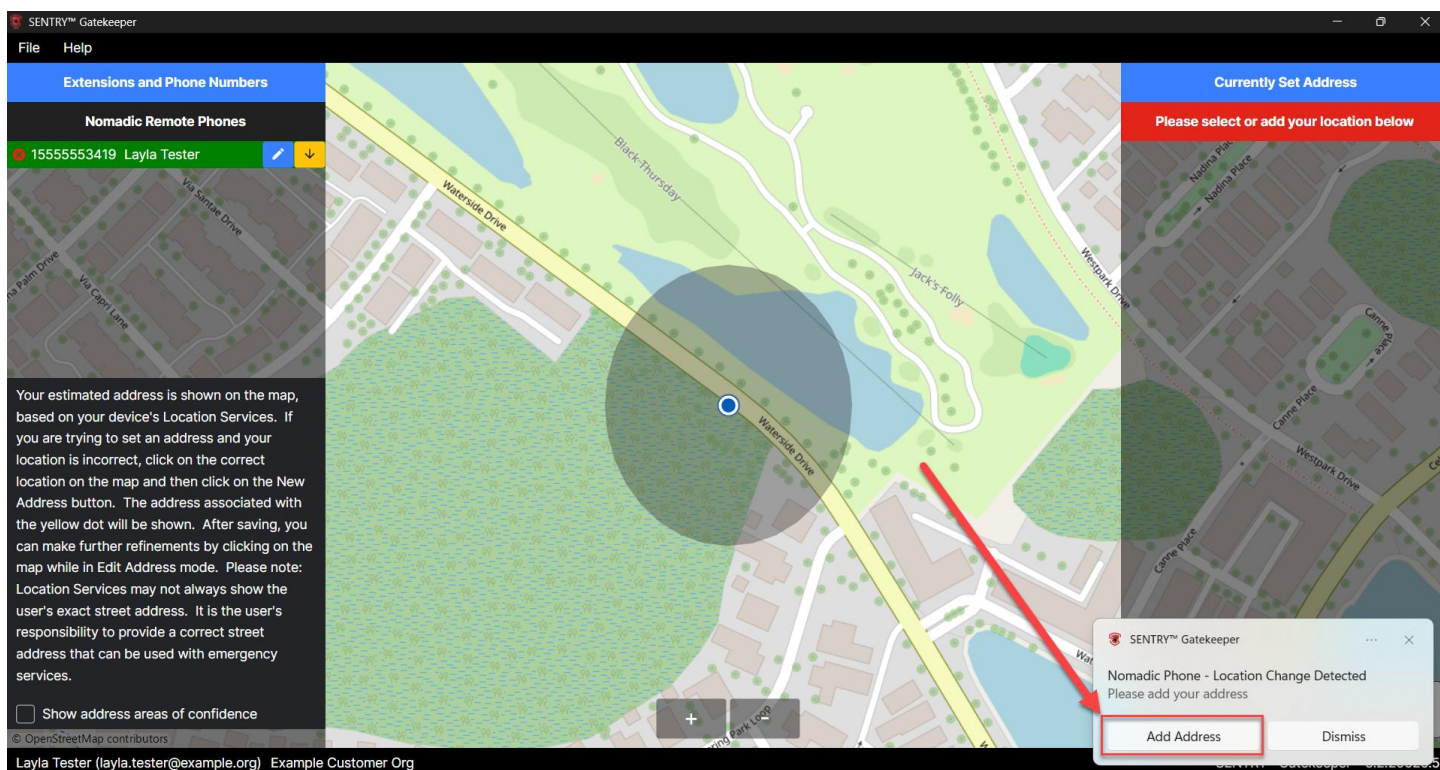


Figure 7

SELF-REGISTRATION AND FIRST-TIME LOGIN FOR AZURE AD USERS WITH SENTRY™ CLOUD ENTERPRISE

The instructions detailed below will allow SENTRY™ Gatekeeper users (using only their respective extensions) from an organization using SENTRY™ Cloud Enterprise and authenticating against Azure Active Directory credentials to log into SENTRY™ Gatekeeper for the first time. In most cases, users will use their normal organizational login account.

1. Launch the SENTRY™ Gatekeeper application. Click on **“SIGN IN”**.

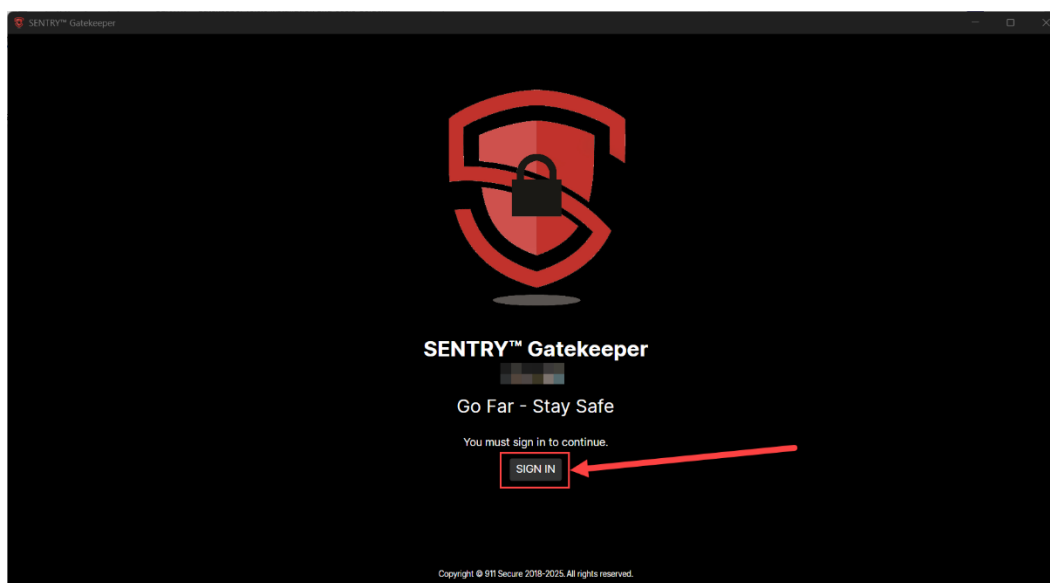


Figure 8

2. Click on **“Sign in with Azure AD credentials”**.

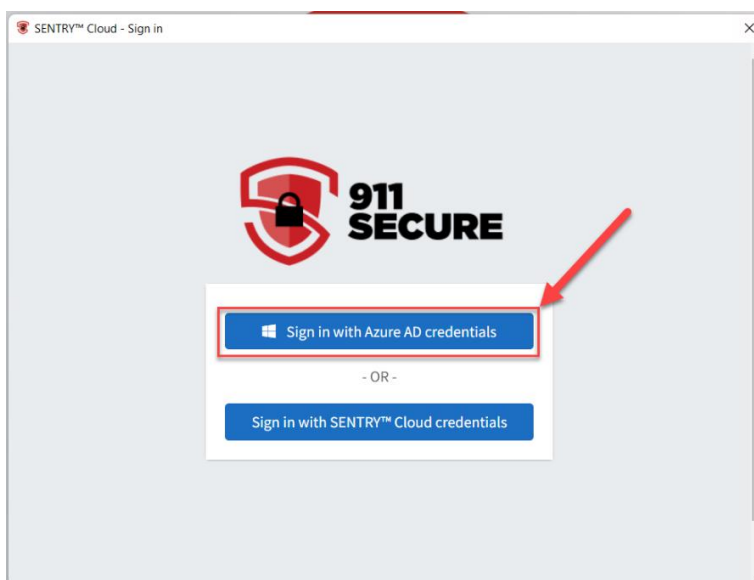


Figure 9

3. Enter your regular work email address and click **“Next”**.

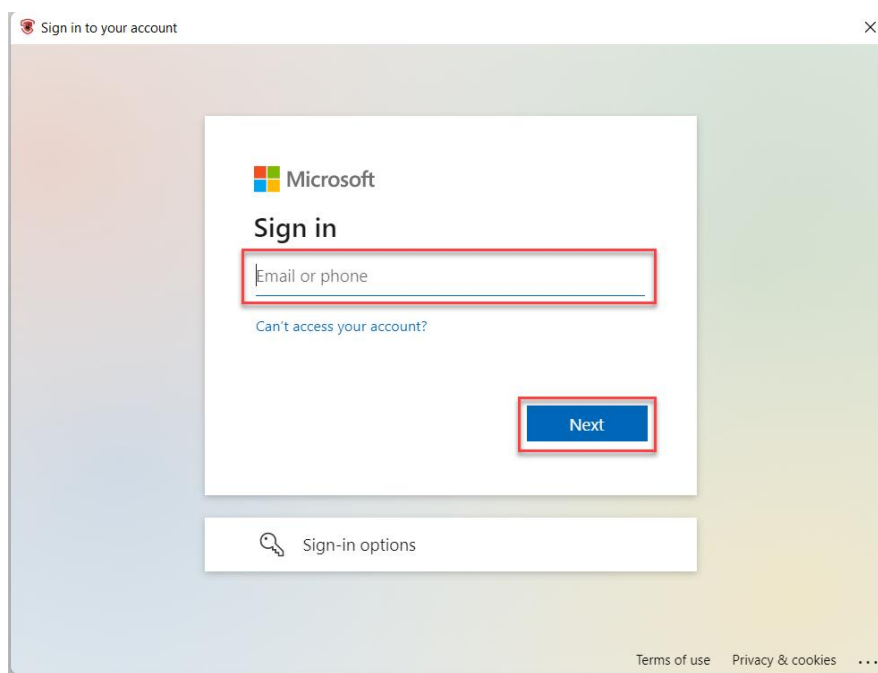


Figure 10

4. Enter in your corresponding work password and click **“Sign in”**.

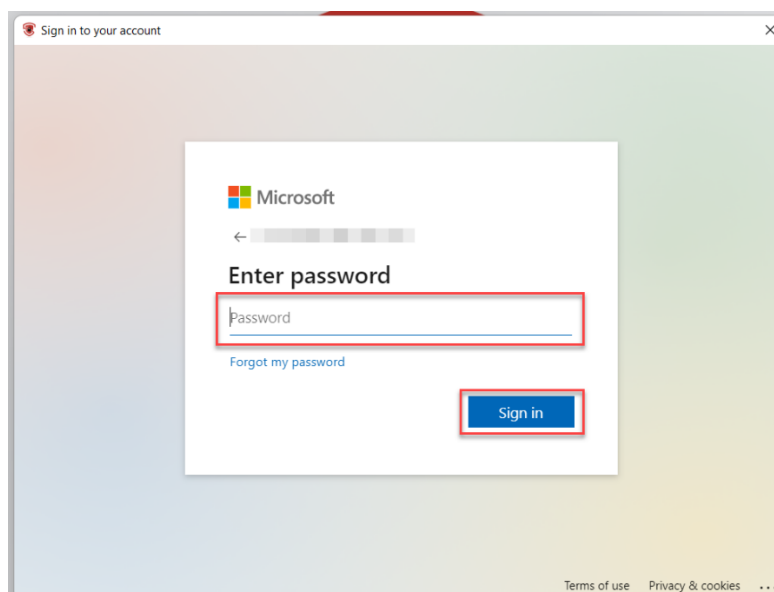
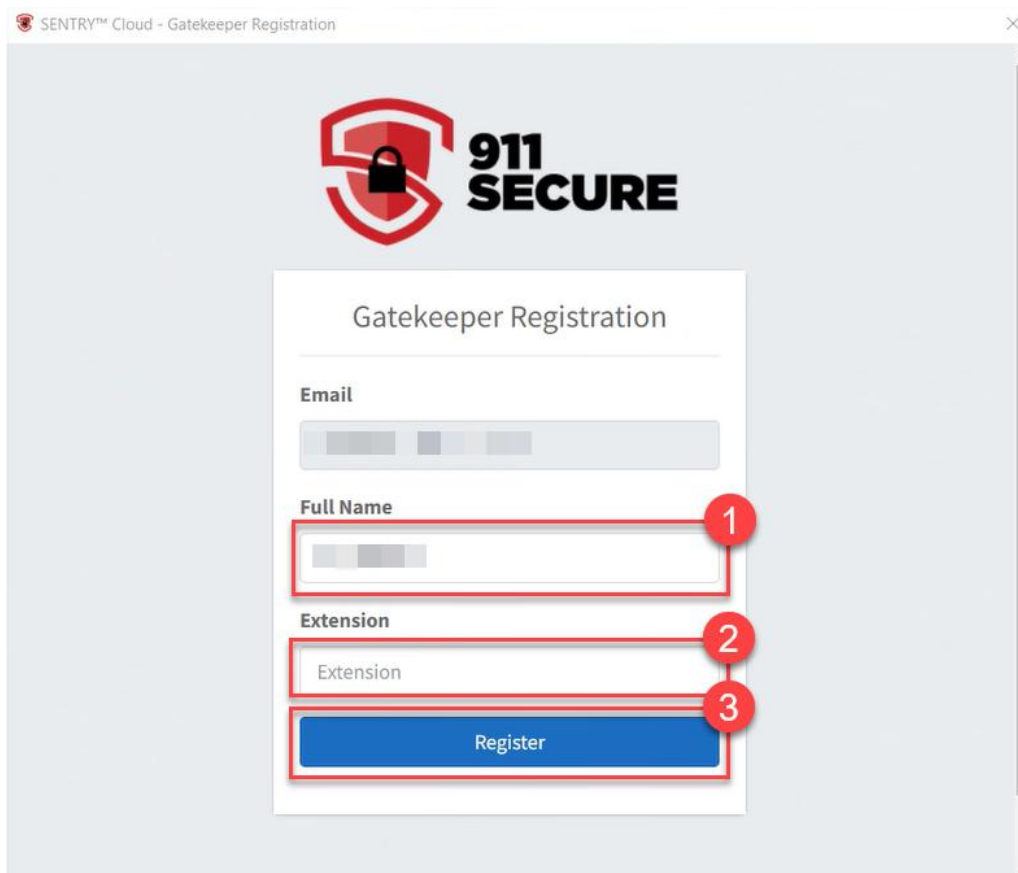



Figure 11

5. You will be presented with a “**Gatekeeper Registration**” screen with several fields to fill in. Enter in your **full name** and assigned **Extension** into the appropriate fields. Once finished, click “**Register**” to complete the self-registration process.



SENTRY™ Cloud - Gatekeeper Registration

 **911
SECURE**

Gatekeeper Registration

Email

Full Name 1

Extension 2

Register 3

Figure 12

6. **PLEASE NOTE:** When logging into the application for the very first time, you will be met with a “**Gatekeeper User Acceptance**” window. Its purpose is to help end users understand why they must set their location and the importance of doing so. While the exact User Acceptance message may vary depending on the customer, the **default verbiage** is displayed below. Users must click the “**I have read and understand the above statement**” checkbox, then click on the “**OK**” button.

SENTRY™ Gatekeeper User Acceptance Default Message:

“SENTRY™ Gatekeeper is an application for keeping softphone users safe whenever they are working from a remote / offsite location. It requires users to provide accurate location information so any 911 call made from their softphone can be routed to the closest Public Safety Answering Point. By clicking the OK button below, I acknowledge that I will enter only accurate location information whenever my work location changes.”

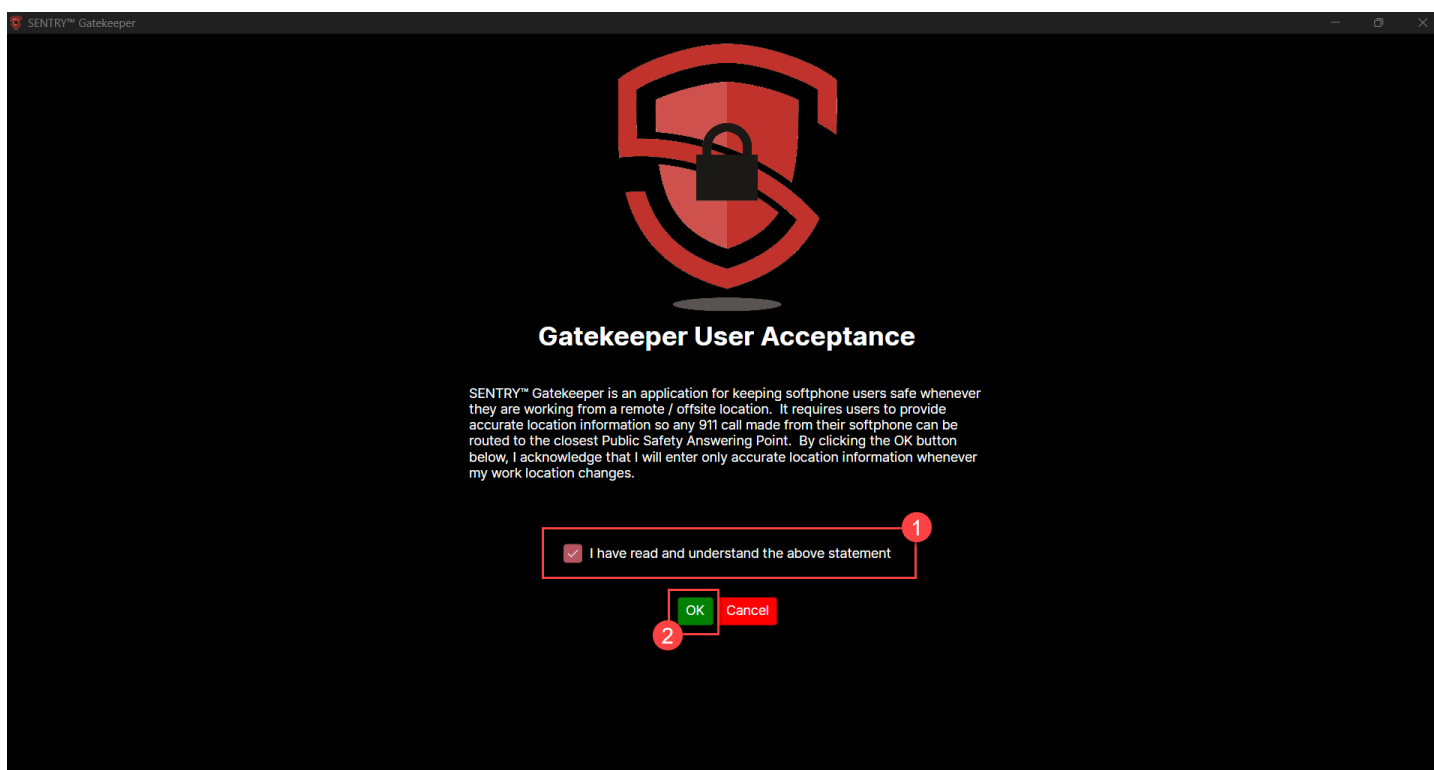


Figure 13

- Once you have signed in and clicked “OK” for the User Acceptance agreement, you will be brought to the SENTRY™ Gatekeeper client screen and can begin the process of setting or selecting your address.

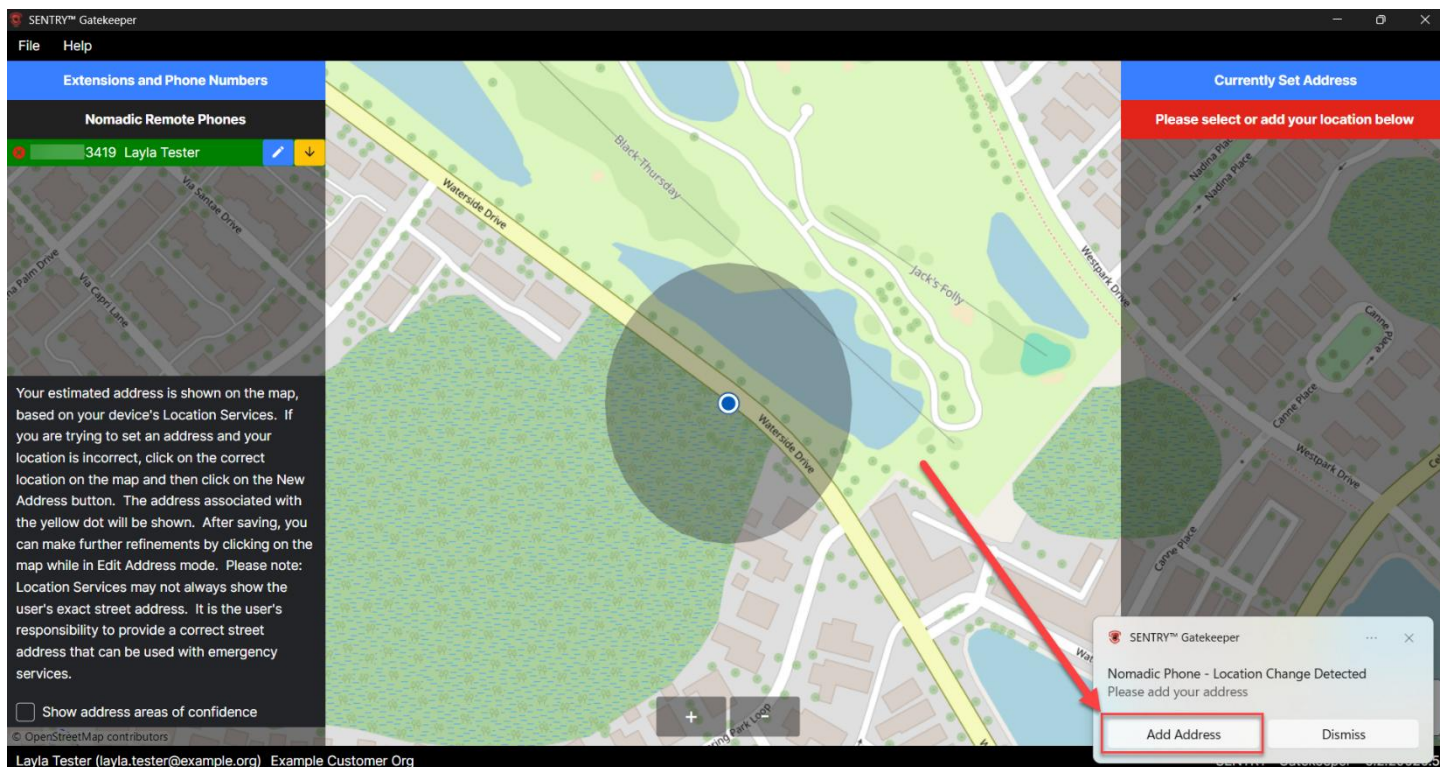


Figure 14

SELF-REGISTRATION AND FIRST-TIME LOGIN FOR AZURE AD USERS WITH SENTRY™ CLOUD ENTERPRISE (WITH DIDs)

The instructions detailed below will allow SENTRY™ Gatekeeper users (using either DIDs or their respective extensions) from an organization using SENTRY™ Cloud Enterprise and authenticating against Azure Active Directory credentials to log into SENTRY™ Gatekeeper for the first time. In most cases, users will use their normal organizational login account.

1. Launch the SENTRY™ Gatekeeper application. Click on **"SIGN IN"**.

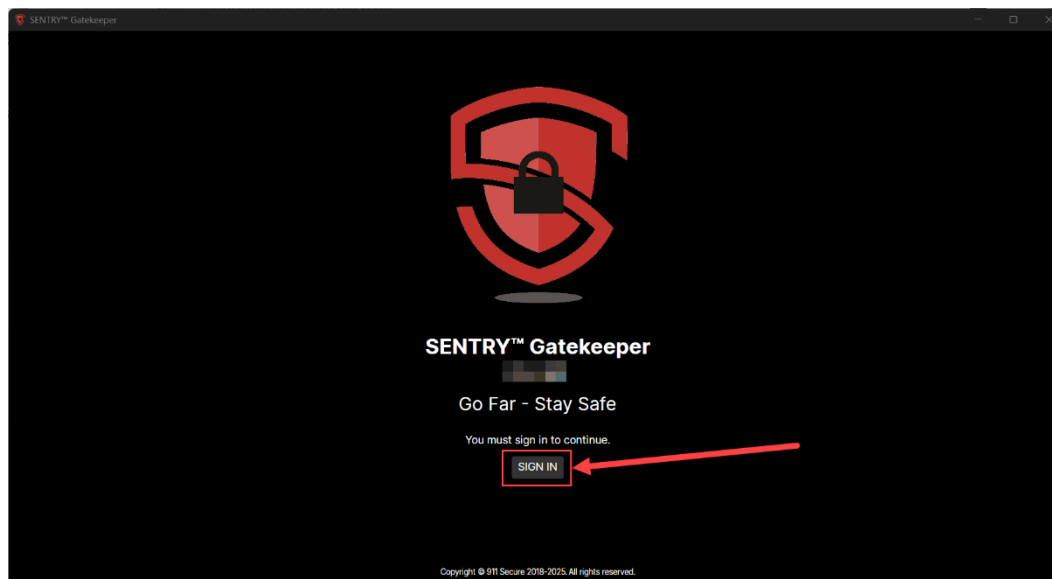


Figure 15

2. Click on **"Sign in with Azure AD credentials"**.

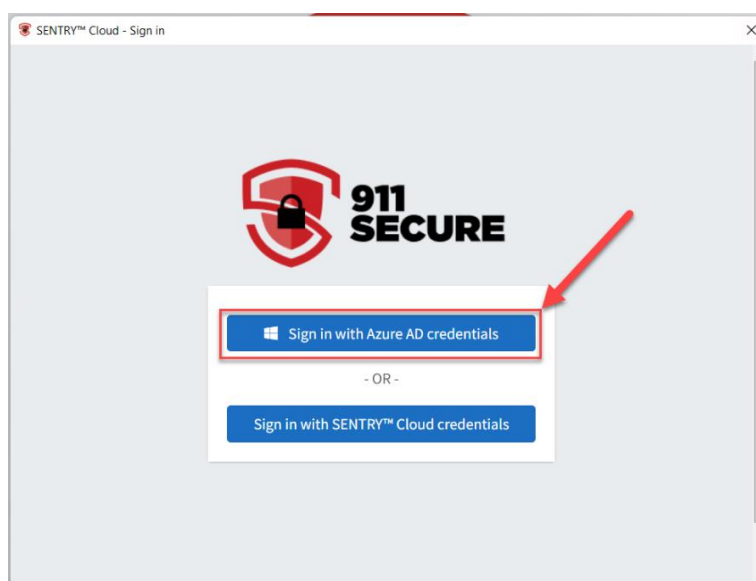


Figure 16

3. Enter your regular work email address and click **“Next”**.

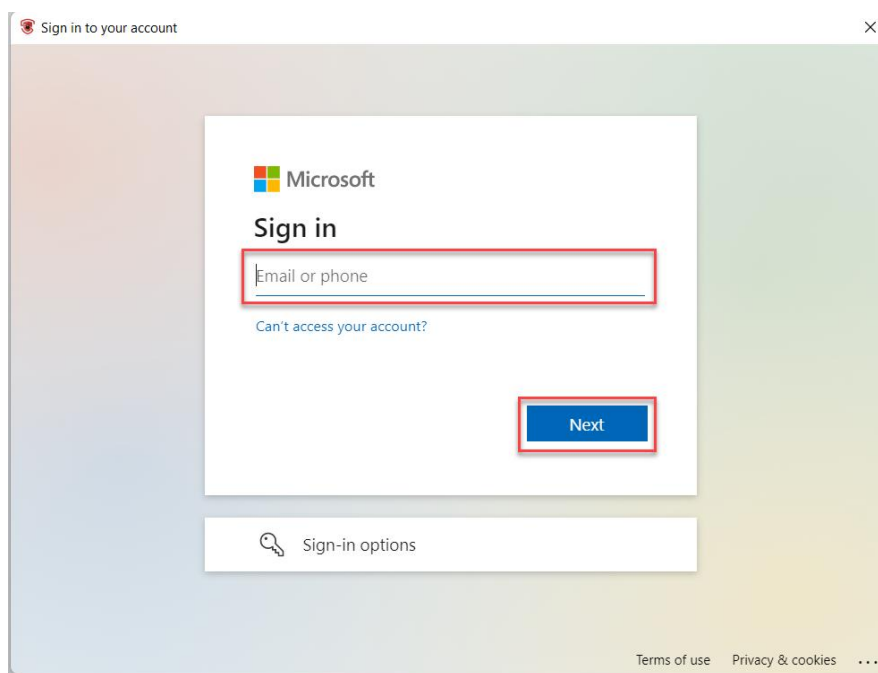


Figure 17

4. Enter in your corresponding work password and click **“Sign in”**.

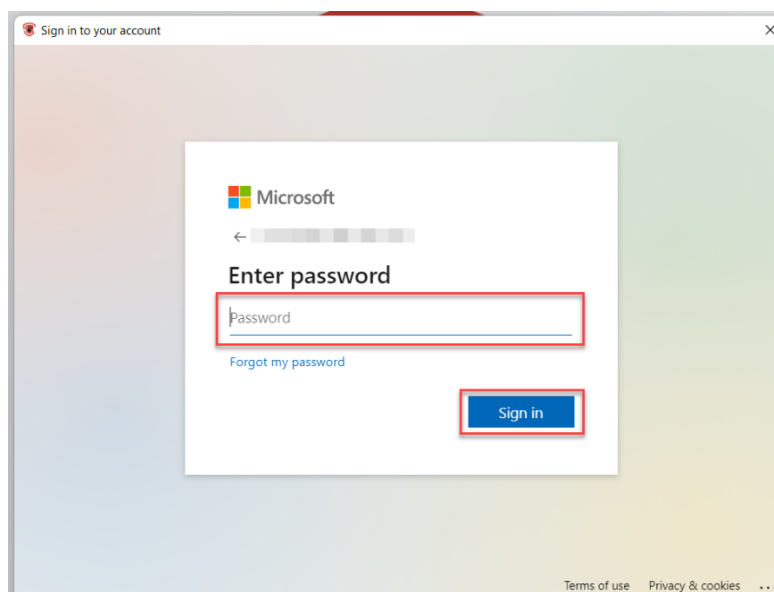



Figure 18

5. You will be presented with a “**Gatekeeper Registration**” screen with several fields to fill in. Enter in your **full name** and either your assigned **Extension** or assigned 11-digit **ELIN / DID** into the appropriate fields. If you have an assigned Extension, enter it into the **Extension** field and leave the “Full 11-Digit Phone Number With Leading 1” field blank. If you have been assigned an 11-digit **ELIN / DID** (i.e., the full 10-digit phone number used with your softphone device prepended with a leading “1” such as “15555552468”), enter that into the “**Full 11-Digit Phone Number With Leading 1**” field and leave the Extension field blank. Once finished, click “**Register**” to complete the self-registration process.



SENTRY™ Gatekeeper - Sign In


**911
SECURE**

Gatekeeper Registration

Email

Full Name

Full 11-Digit Phone Number With Leading 1

Extension

Register

Enter in your 10-digit DID with a leading "1" if you have your own DID assigned to you.

If you have an extension, but not your own DID, enter your extension.

Figure 19

6. **PLEASE NOTE:** When logging into the application for the very first time, you will be met with a “**Gatekeeper User Acceptance**” window. Its purpose is to help end users understand why they must set their location and the importance of doing so. While the exact User Acceptance message may vary depending on the customer, the **default verbiage** is displayed below. Users must click the “**I have read and understand the above statement**” **checkbox**, then click on the “**OK**” button.

SENTRY™ Gatekeeper User Acceptance Default Message:

“SENTRY™ Gatekeeper is an application for keeping softphone users safe whenever they are working from a remote / offsite location. It requires users to provide accurate location information so any 911 call made from their softphone can be routed to the closest Public Safety Answering Point. By clicking the OK button below, I acknowledge that I will enter only accurate location information whenever my work location changes.”

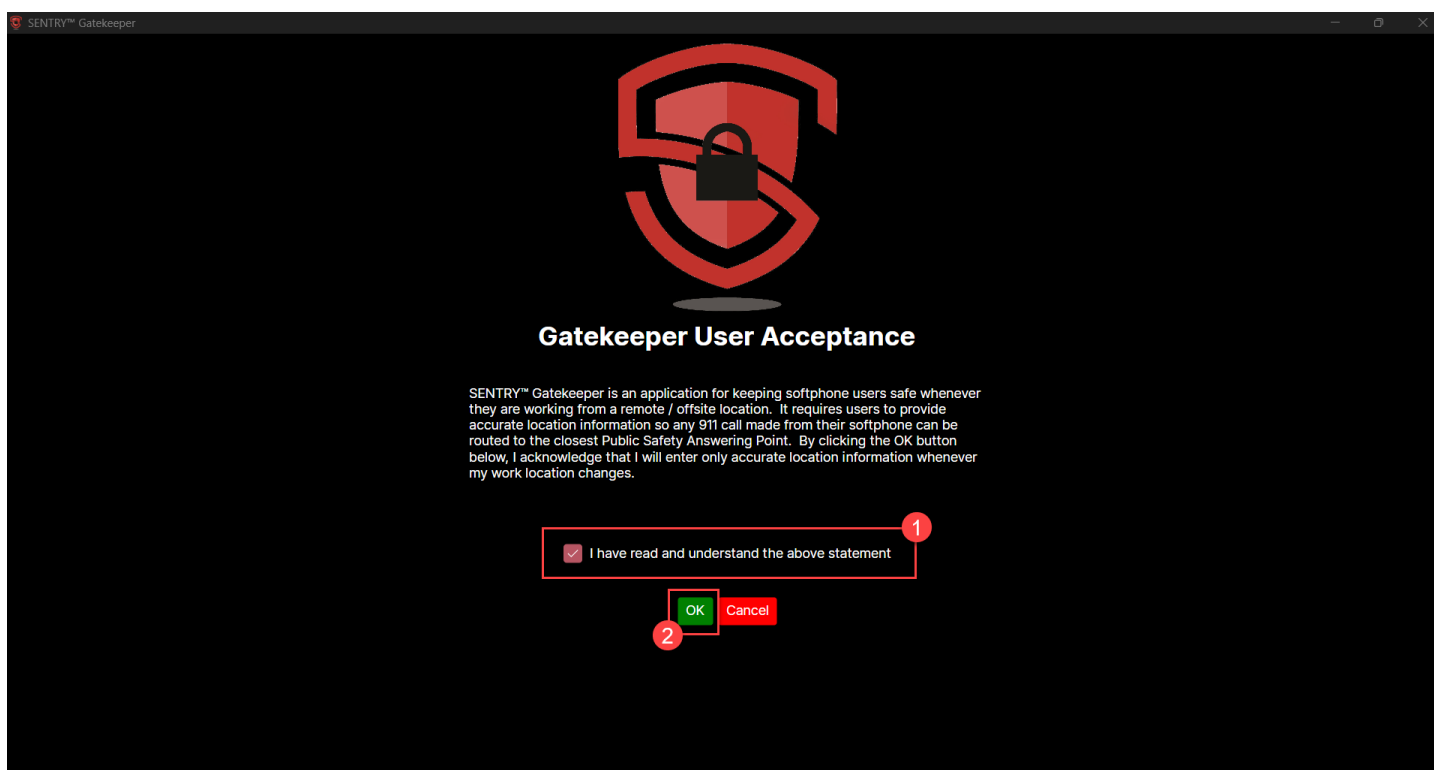


Figure 20

- Once you have signed in and clicked “OK” for the User Acceptance agreement, you will be brought to the SENTRY™ Gatekeeper client screen and can begin the process of setting or selecting your address.

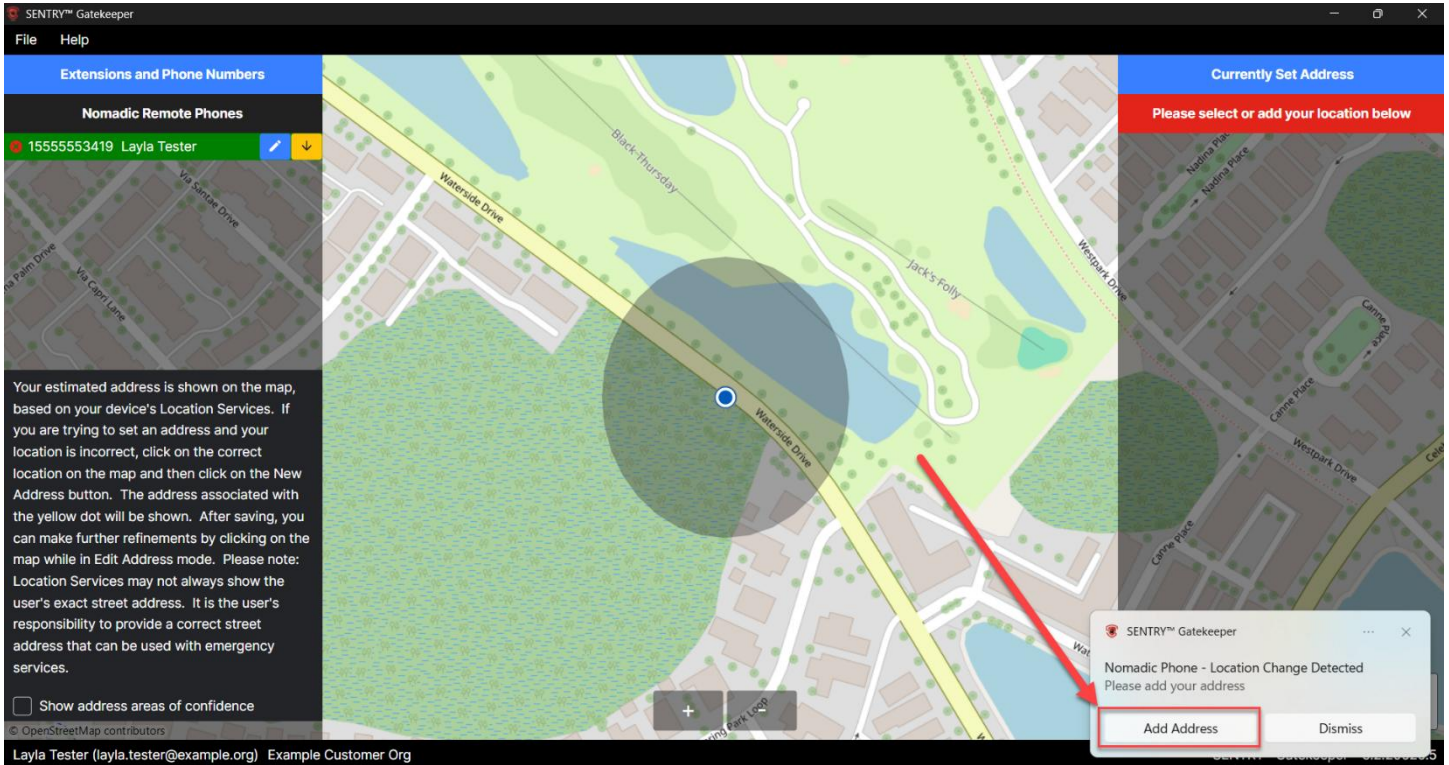


Figure 21

SELF-REGISTRATION AND FIRST-TIME LOGIN FOR SENTRY™ CLOUD CREDENTIALS USERS

The instructions detailed below will allow SENTRY™ Gatekeeper users from an organization NOT using Azure Active Directory credentials to set up a unique password and log into SENTRY™ Gatekeeper for the first time.

1. Launch the SENTRY™ Gatekeeper application. Click on “SIGN IN”.

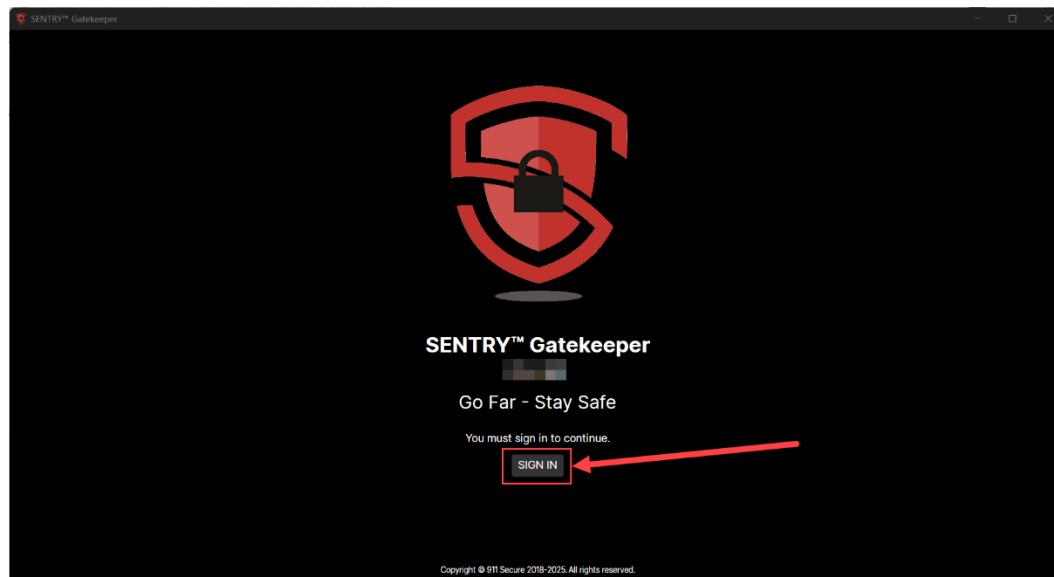


Figure 22

2. Click on “Sign in with SENTRY™ Cloud Credentials”.

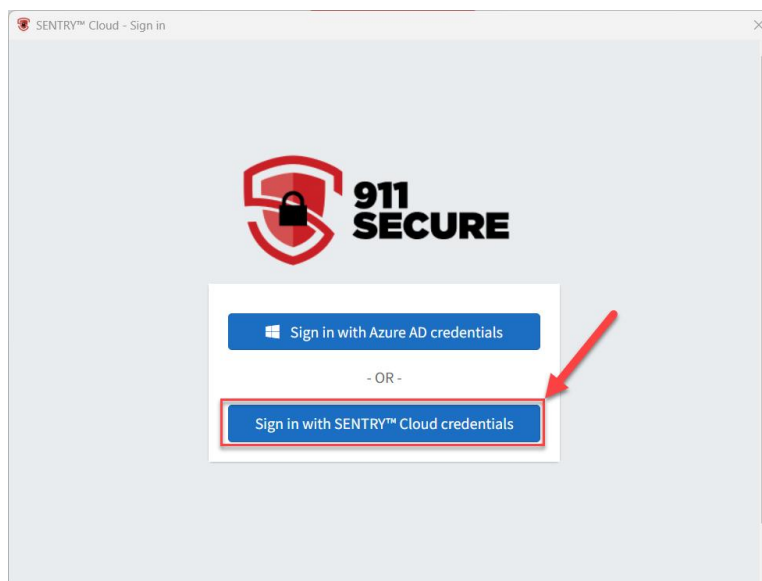


Figure 23

3. Click on **“First time registration”**.

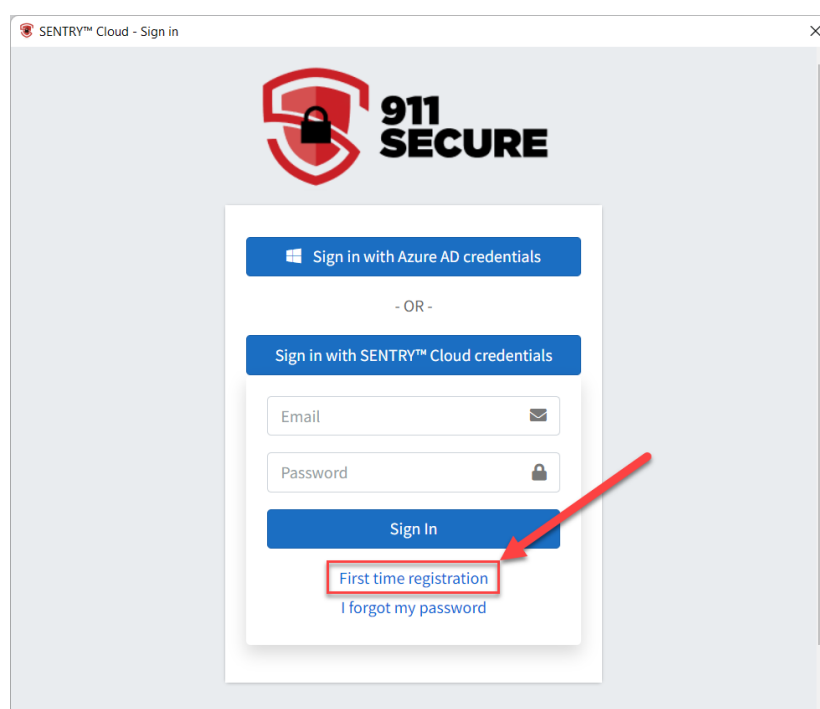


Figure 24

4. Enter in your **email address** used for work in the field provided, then click **“Submit”**.

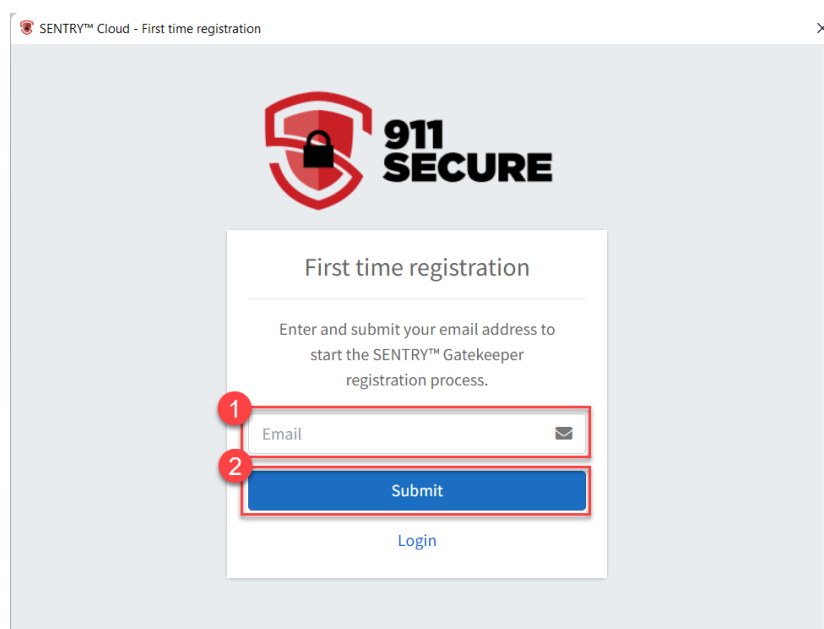


Figure 25

5. You will receive an email from alerts@911secure.com with a **registration code**. (**PLEASE NOTE:** Each registration code will be different. Below is an example.)

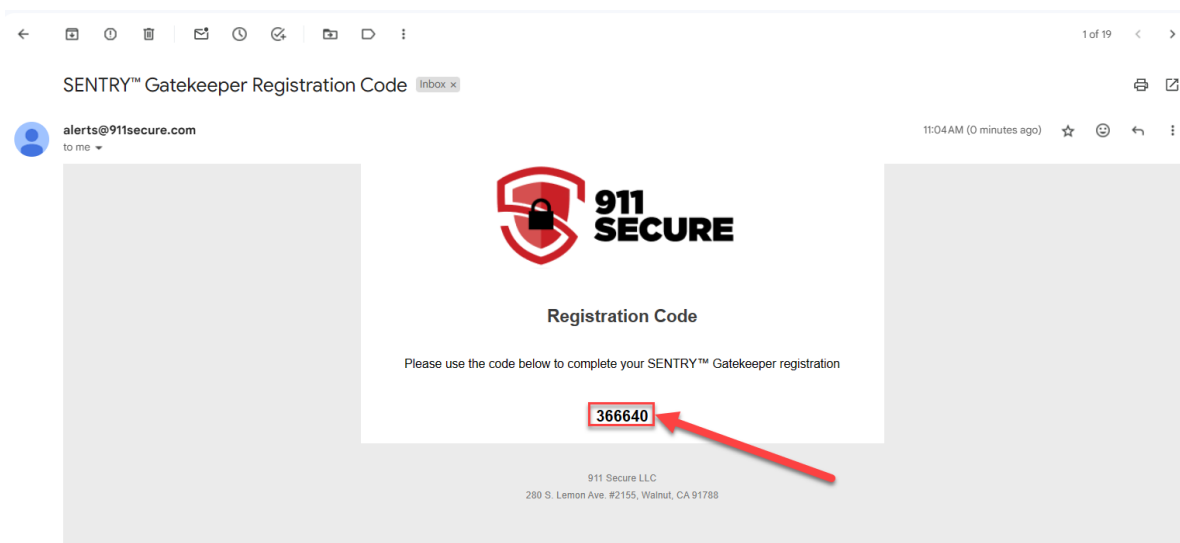


Figure 26

6. **Copy** the registration code and enter it into the **Registration code** field provided to complete your registration for SENTRY™ Gatekeeper. Click **“Submit”** once you have entered it. (**PLEASE NOTE:** If you don’t receive your registration code within five minutes, you can click **“Resend registration code”**. Make sure to check your Spam / Junk folder. If the issue of receiving the code persists, please reach out to **support@911secure.com**.)

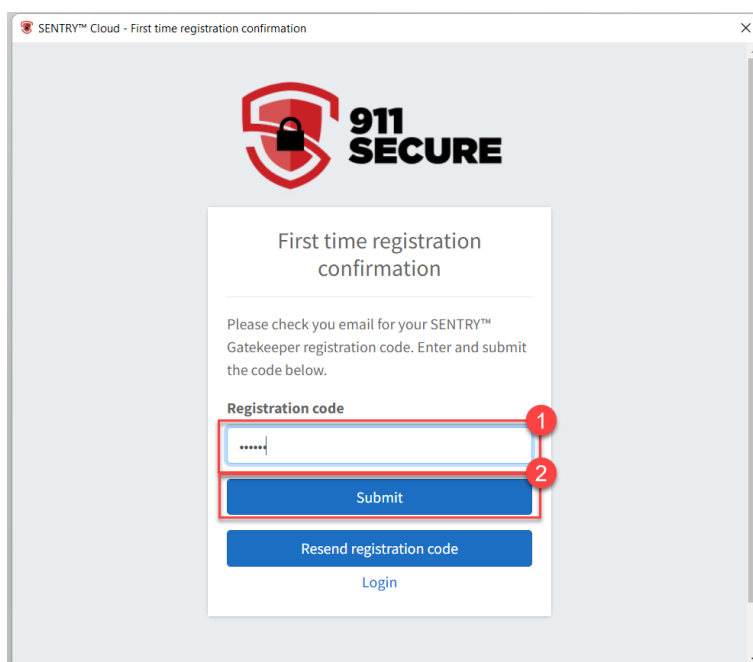
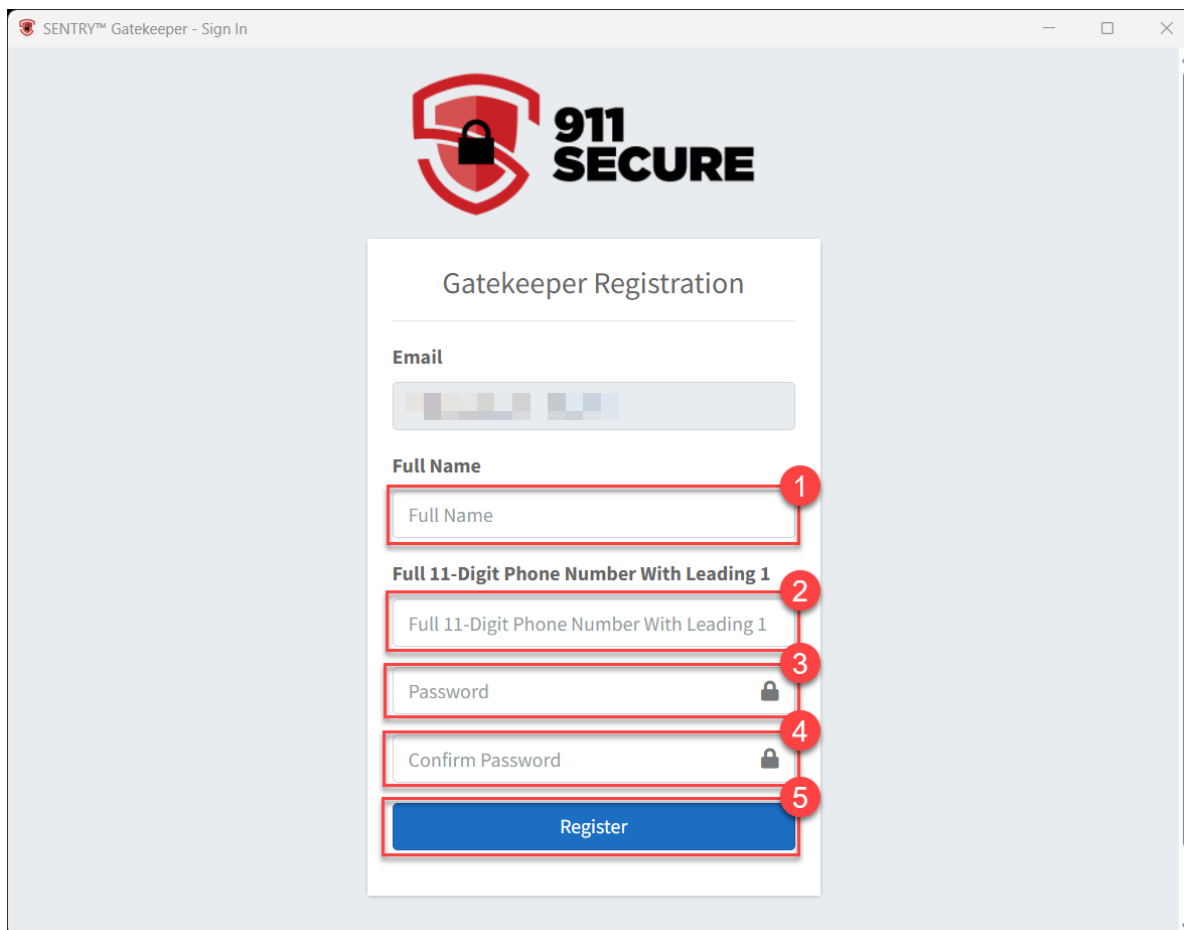



Figure 27

7. You can then enter your first and last name into the **“Full Name”** field, and your assigned 11-digit **ELIN / DID** (i.e., the full 10-digit phone number used with your softphone device prepended with a leading “1” such as “15555552468”) into the **“Full 11-Digit Phone Number With Leading 1”** field. You will also create a password to use when logging into SENTRY™ Gatekeeper in the future. Enter this created password into the **Password** and **Confirm Password** fields (indicated by the lock icons). Click **“Register”** once you have finished. This will sign you into SENTRY™ Gatekeeper.



SENTRY™ Gatekeeper - Sign In

 **911
SECURE**

Gatekeeper Registration

Email

Full Name

Full 11-Digit Phone Number With Leading 1

Password

Confirm Password

Register

Figure 28

8. **PLEASE NOTE:** When logging into the application for the very first time, you will be met with a “**Gatekeeper User Acceptance**” window. Its purpose is to help end users understand why they must set their location and the importance of doing so. While the exact User Acceptance message may vary depending on the customer, the **default verbiage** is displayed below. Users must click the “**I have read and understand the above statement**” **checkbox**, then click on the “**OK**” button.

SENTRY™ Gatekeeper User Acceptance Default Message:

“SENTRY™ Gatekeeper is an application for keeping softphone users safe whenever they are working from a remote / offsite location. It requires users to provide accurate location information so any 911 call made from their softphone can be routed to the closest Public Safety Answering Point. By clicking the OK button below, I acknowledge that I will enter only accurate location information whenever my work location changes.”

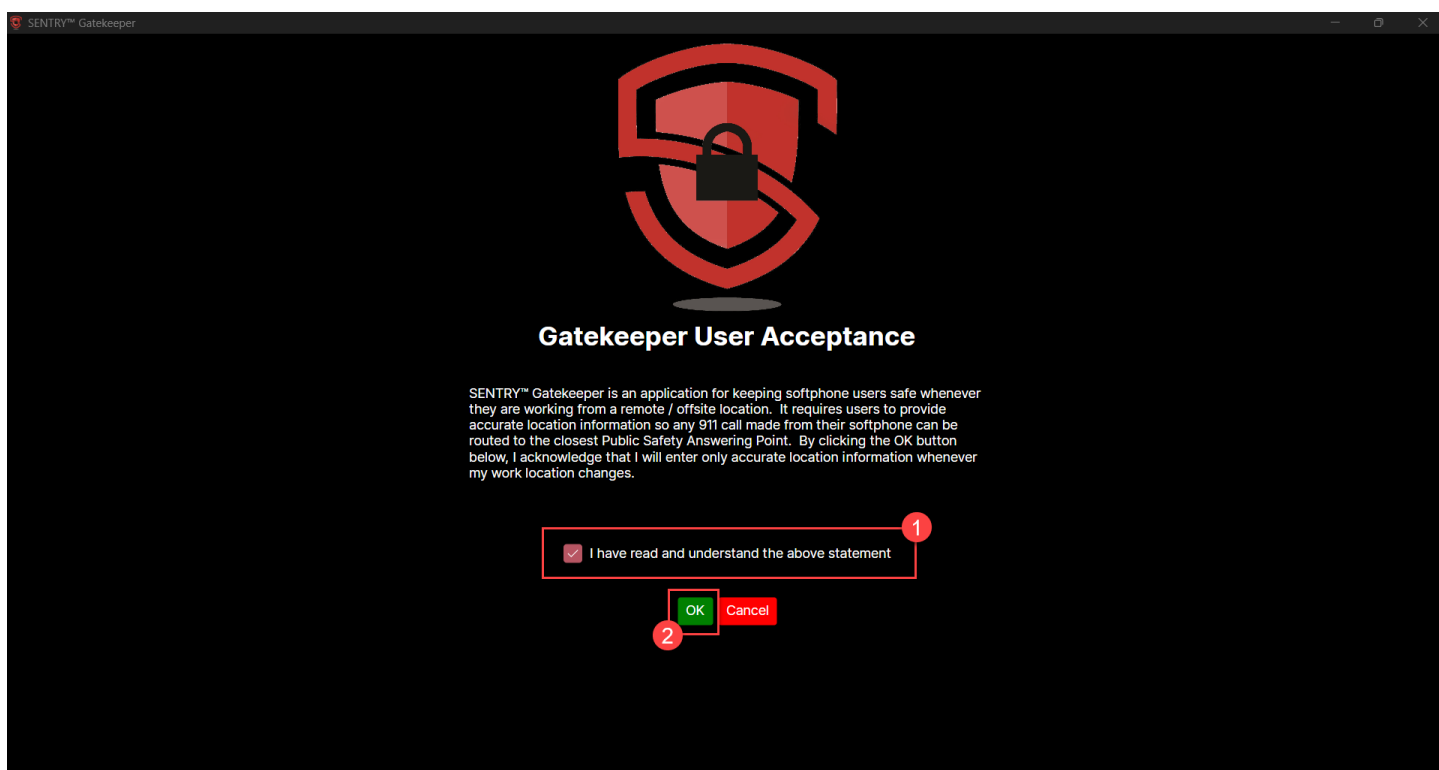


Figure 29

8. Once you have signed in and clicked “OK” for the User Acceptance agreement, you will be brought to the SENTRY™ Gatekeeper client screen and can begin the process of setting or selecting your address.

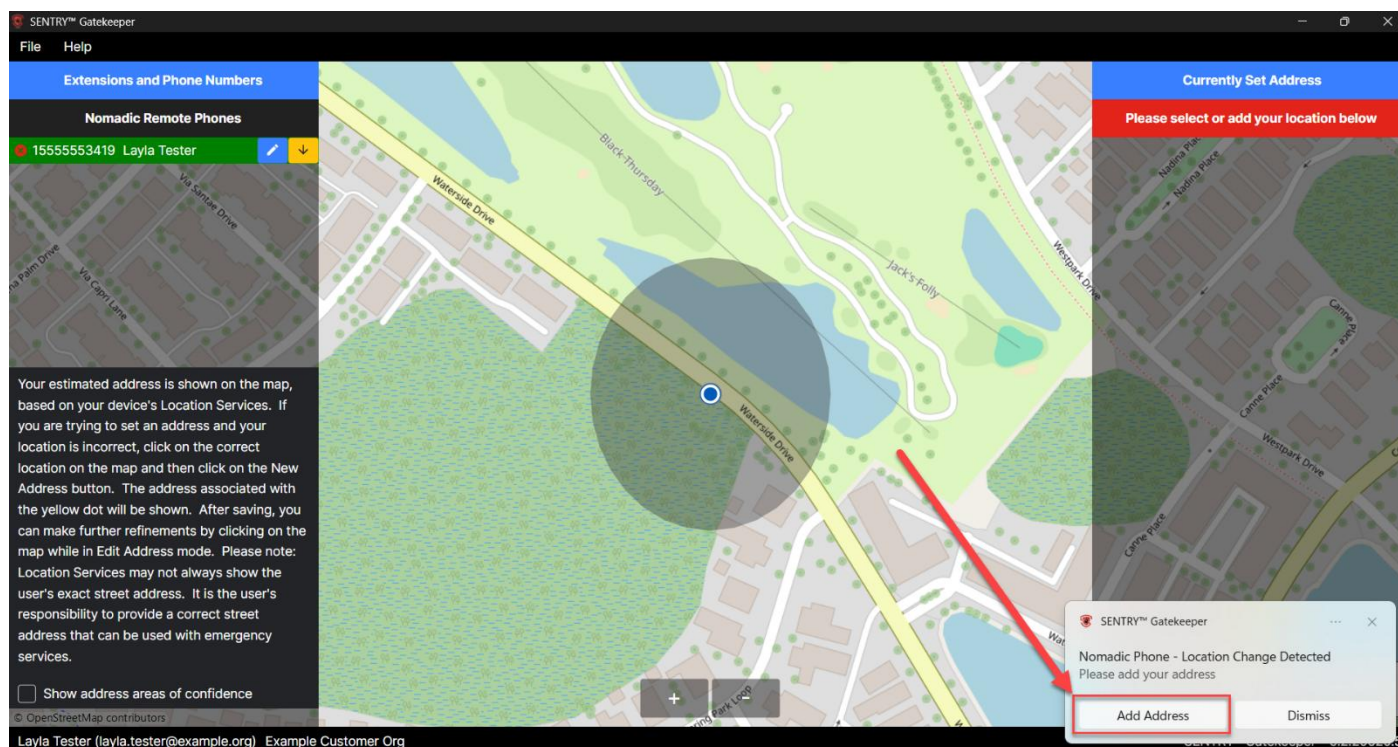


Figure 30

SELF-REGISTRATION AND FIRST-TIME LOGIN FOR SENTRY™ CLOUD CREDENTIALS USERS WITH SENTRY™ CLOUD ENTERPRISE

The instructions detailed below are specific to SENTRY™ Gatekeeper users (using only their respective extensions) from an organization using SENTRY™ Cloud Enterprise and NOT using Azure Active Directory credentials for login purposes. Follow the steps below to set up a unique password and log into SENTRY™ Gatekeeper for the first time.

1. Launch the SENTRY™ Gatekeeper application. Click on **"SIGN IN"**.

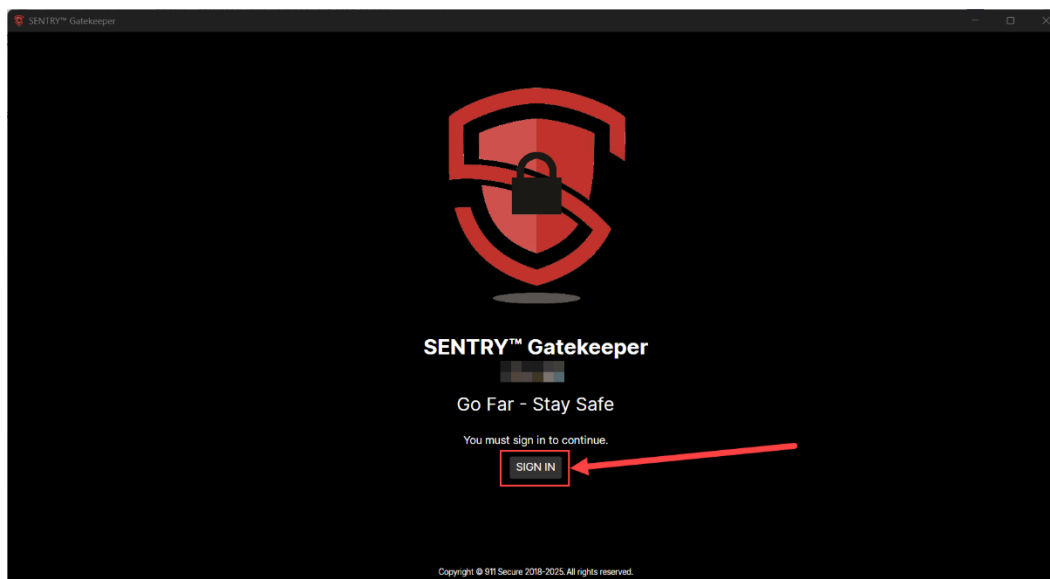


Figure 31

2. Click on **"Sign in with SENTRY™ Cloud credentials"**.

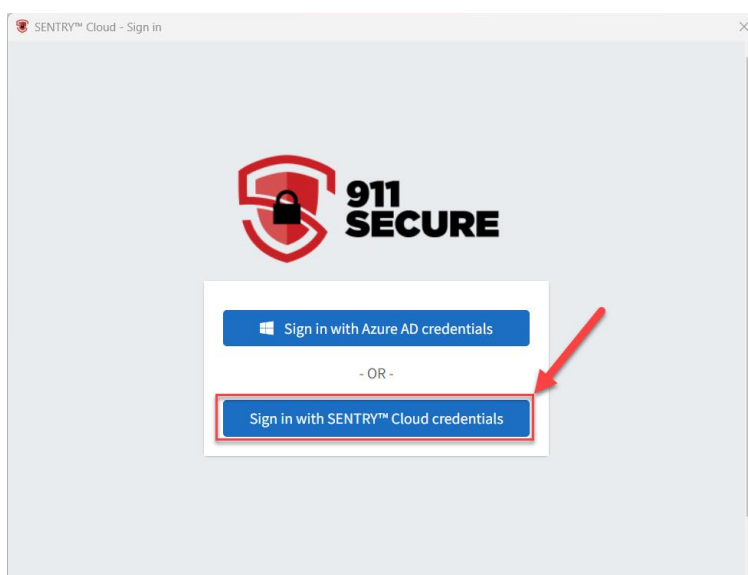


Figure 32

3. Click on “First time registration”.

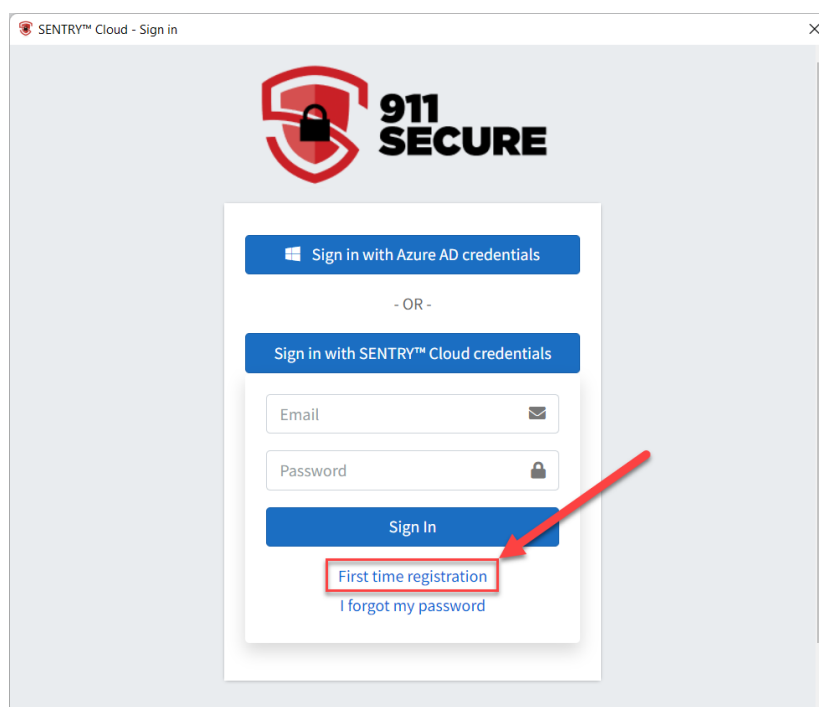


Figure 33

4. Enter in your **email address** used for work in the field provided, then click “Submit”.

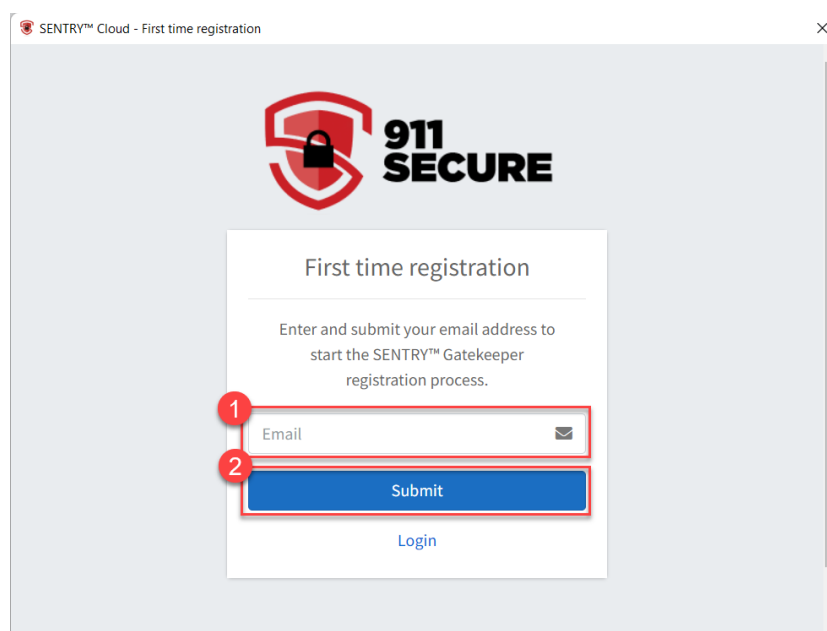


Figure 34

5. You will receive an email from alerts@911secure.com with a **registration code**. (**PLEASE NOTE:** Each registration code will be different. Below is an example.)

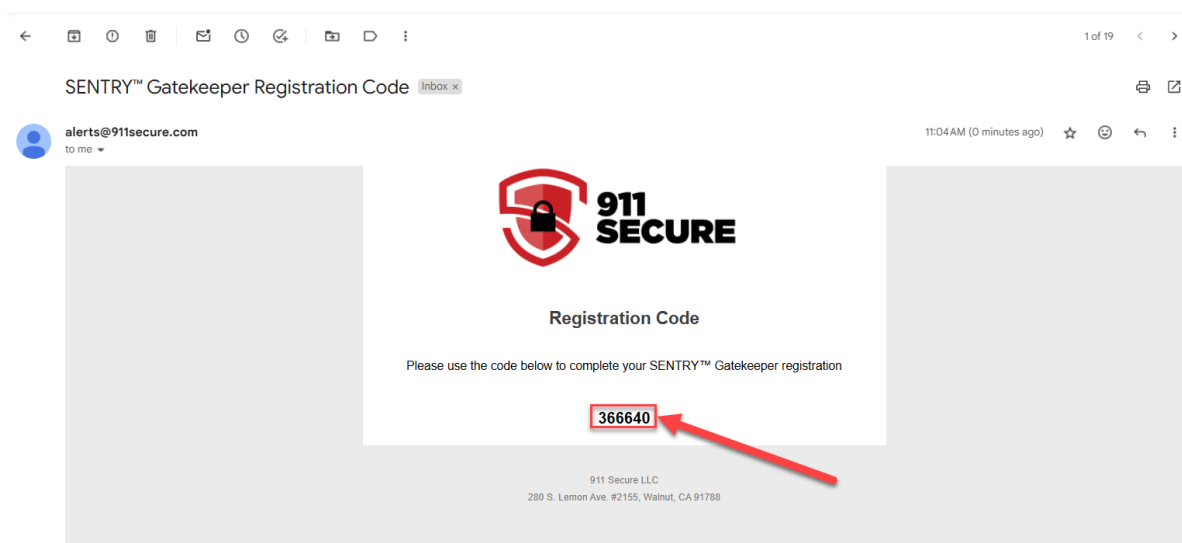


Figure 35

6. **Copy** the registration code and enter it into the **Registration code** field provided to complete your registration for SENTRY™ Gatekeeper. Click **“Submit”** once you have entered it. (**PLEASE NOTE:** If you don’t receive your registration code within five minutes, you can click **“Resend registration code”**. Make sure to check your Spam / Junk folder. If the issue of receiving the code persists, please reach out to support@911secure.com.)

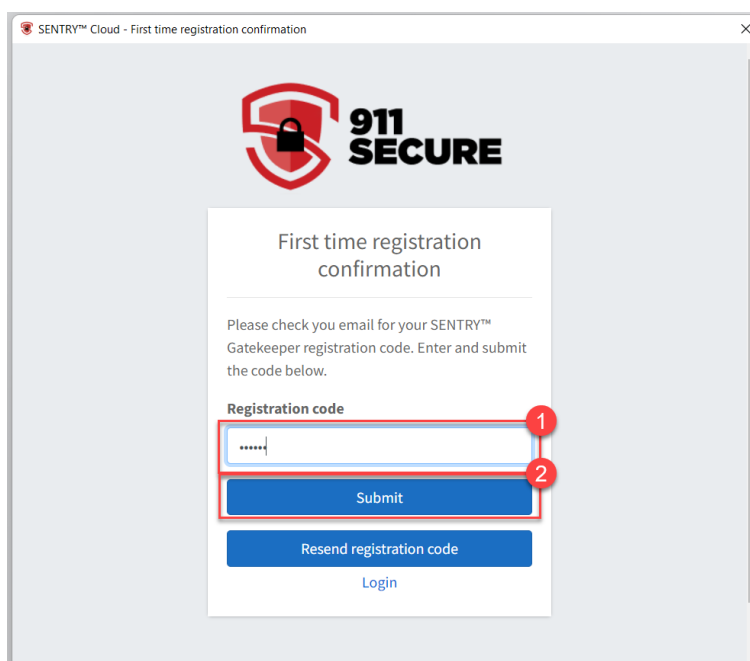
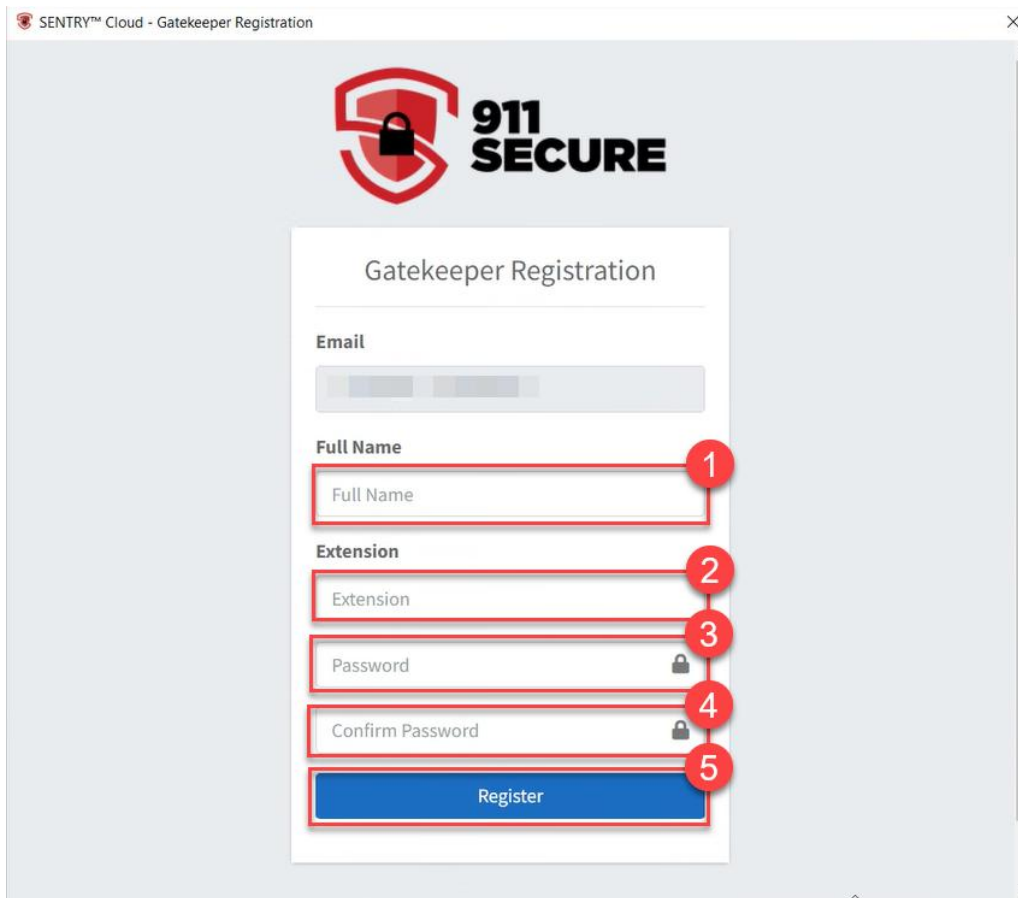



Figure 36

7. You will be presented with a “**Gatekeeper Registration**” screen with several fields to fill in. Enter in your **full name** and your assigned **Extension** into the appropriate fields. You will also create a password to use when logging into SENTRY™ Gatekeeper in the future. Enter this created password into the “**Password**” and “**Confirm Password**” fields (indicated by the lock icons). Once finished, click “**Register**” to complete the self-registration process.



SENTRY™ Cloud - Gatekeeper Registration

 **911
SECURE**

Gatekeeper Registration

Email

Full Name

Extension

Password

Confirm Password

Register

Figure 37

8. **PLEASE NOTE:** When logging into the application for the very first time, you will be met with a “**Gatekeeper User Acceptance**” window. Its purpose is to help end users understand why they must set their location and the importance of doing so. While the exact User Acceptance message may vary depending on the customer, the **default verbiage** is displayed below. Users must click the “**I have read and understand the above statement**” **checkbox**, then click on the “**OK**” button.

SENTRY™ Gatekeeper User Acceptance Default Message:

“SENTRY™ Gatekeeper is an application for keeping softphone users safe whenever they are working from a remote / offsite location. It requires users to provide accurate location information so any 911 call made from their softphone can be routed to the closest Public Safety Answering Point. By clicking the OK button below, I acknowledge that I will enter only accurate location information whenever my work location changes.”

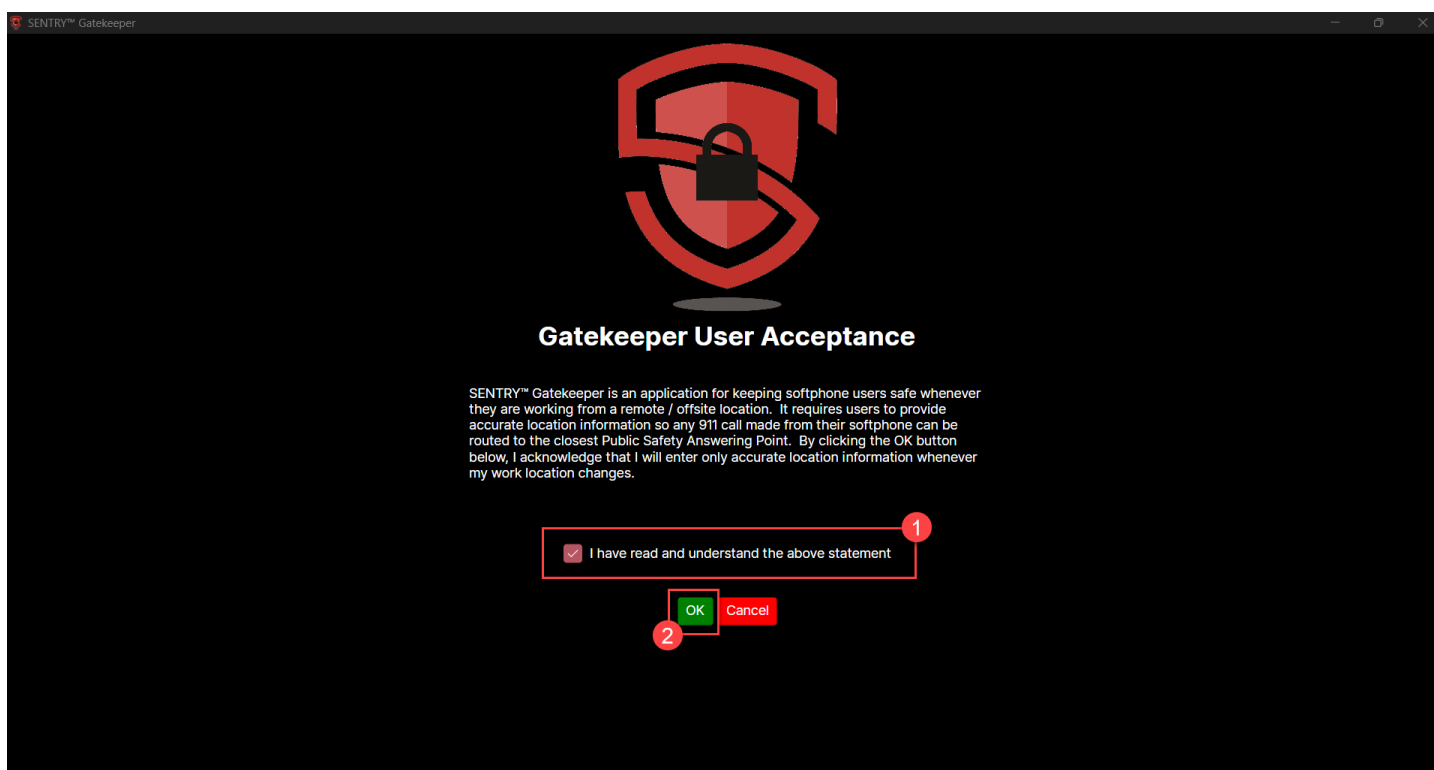


Figure 38

9. Once you have signed in and clicked “OK” for the User Acceptance agreement, you will be brought to the SENTRY™ Gatekeeper client screen and can begin the process of setting or selecting your address.

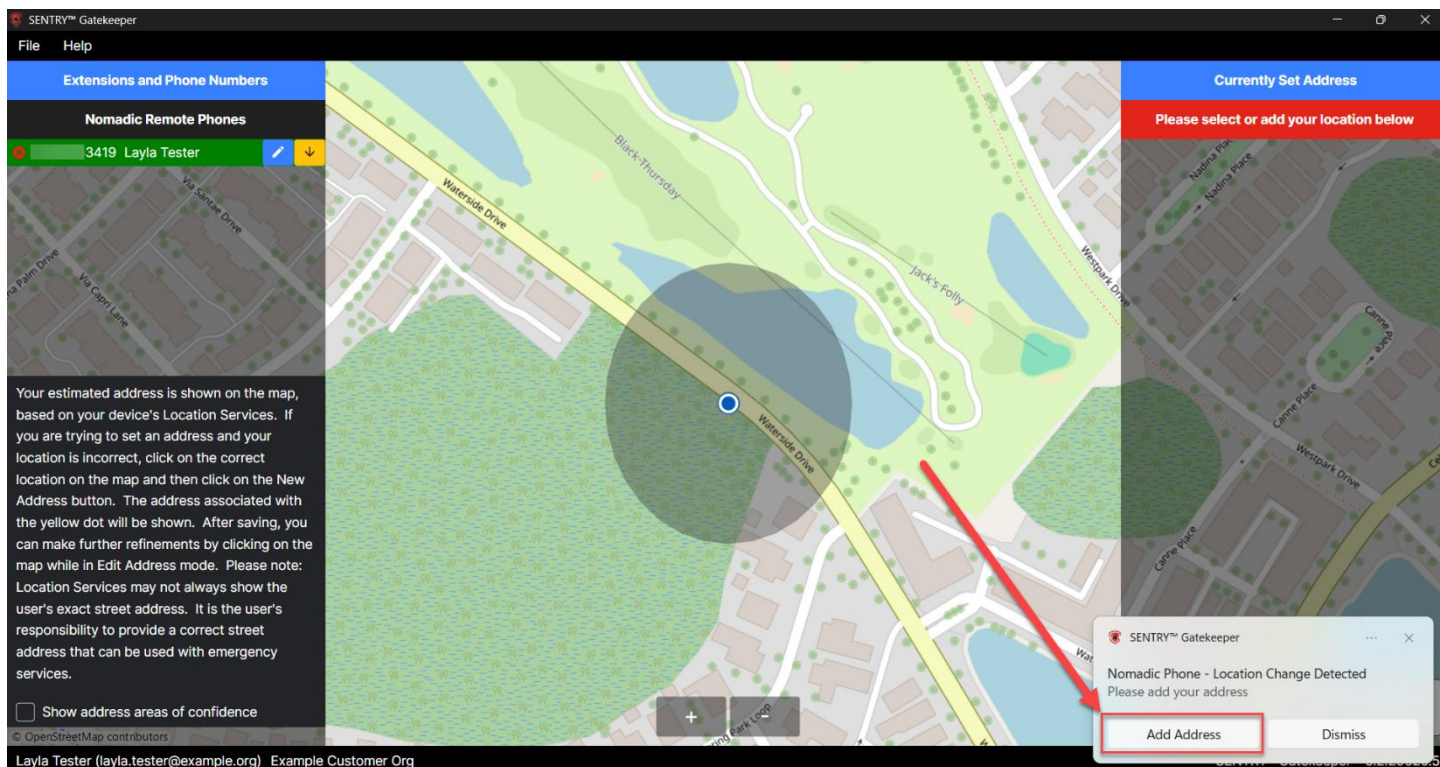


Figure 39

SELF-REGISTRATION AND FIRST-TIME LOGIN FOR SENTRY™ CLOUD CREDENTIALS USERS WITH SENTRY™ CLOUD ENTERPRISE (WITH DIDS)

The instructions detailed below are specific to SENTRY™ Gatekeeper users (using either DIDs or their respective extensions) from an organization using SENTRY™ Cloud Enterprise and NOT using Azure Active Directory credentials for login purposes. Follow the steps below to set up a unique password and log into SENTRY™ Gatekeeper for the first time.

1. Launch the SENTRY™ Gatekeeper application. Click on “SIGN IN”.

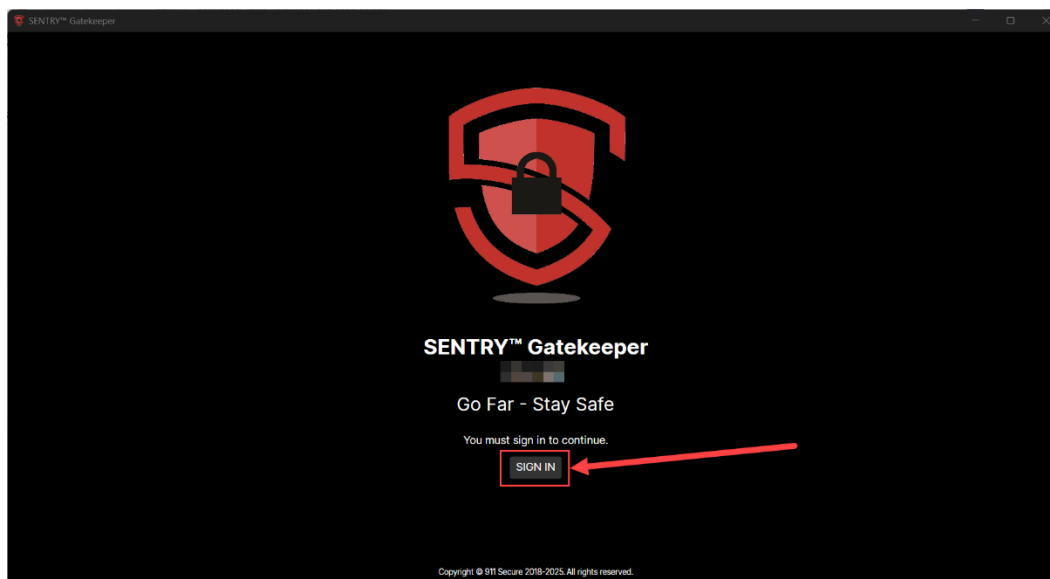


Figure 40

2. Click on “Sign in with SENTRY™ Cloud credentials”.

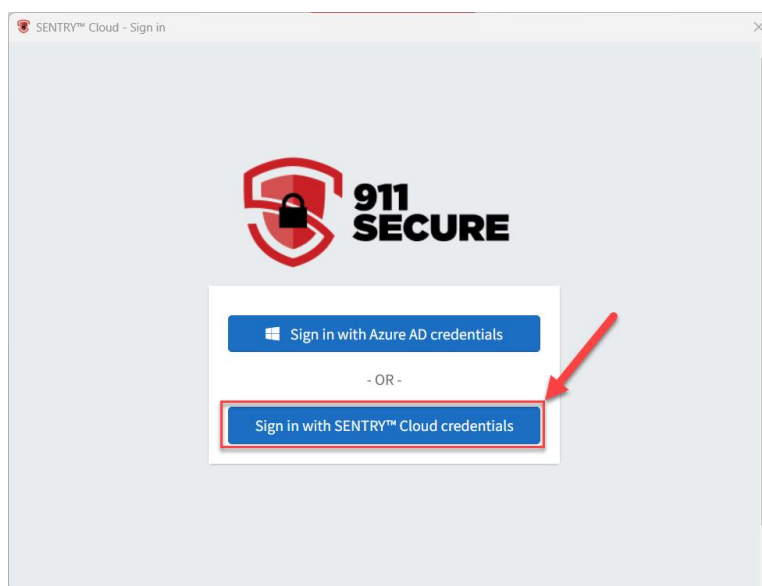


Figure 41

3. Click on “First time registration”.

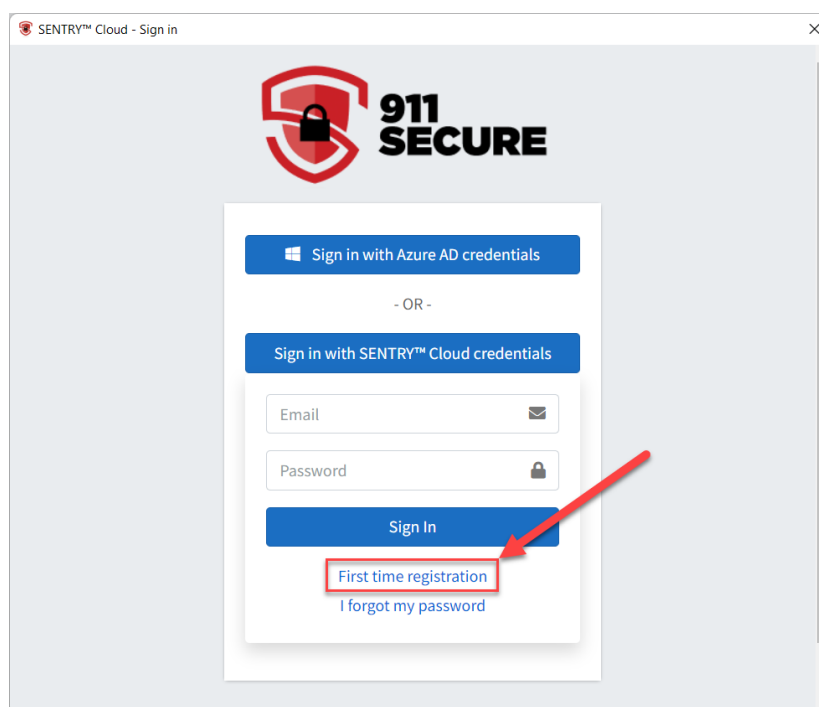


Figure 42

4. Enter in your **email address** used for work in the field provided, then click “Submit”.

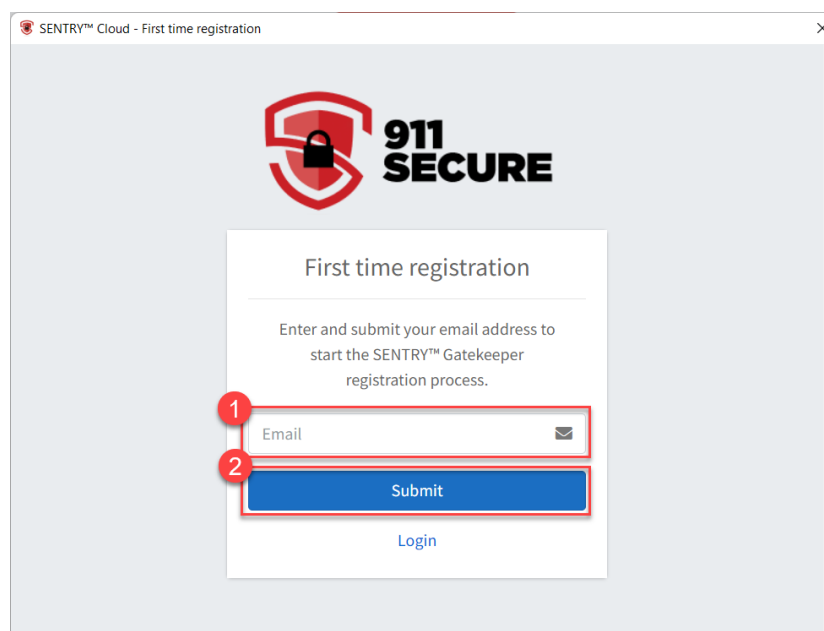


Figure 43

- You will receive an email from alerts@911secure.com with a **registration code**. (**PLEASE NOTE:** Each registration code will be different. Below is an example.)

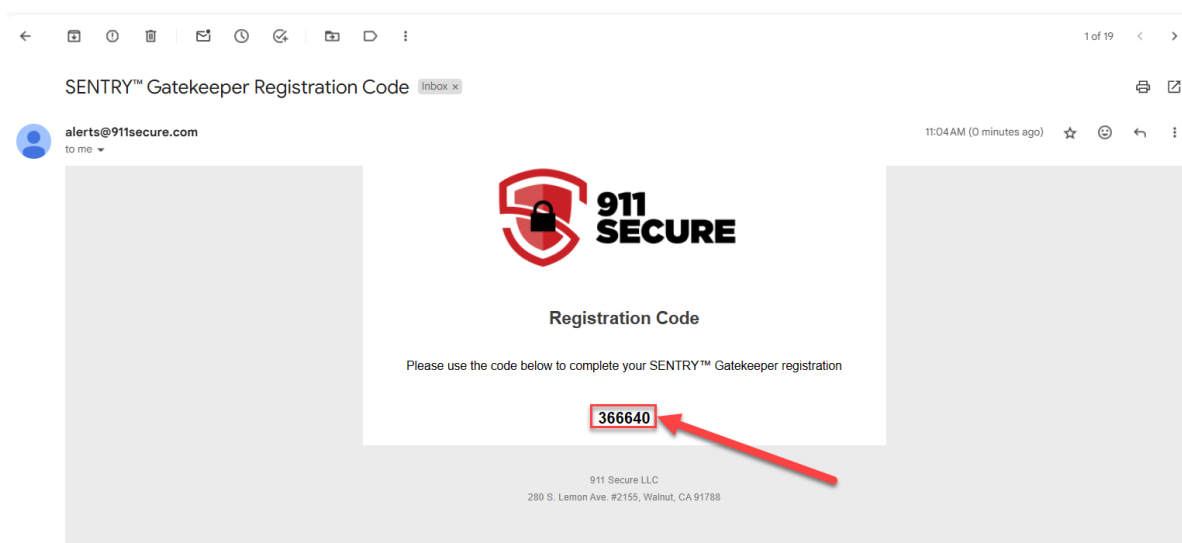


Figure 44

- Copy** the registration code and enter it into the **Registration code** field provided to complete your registration for SENTRY™ Gatekeeper. Click **“Submit”** once you have entered it. (**PLEASE NOTE:** If you don’t receive your registration code within five minutes, you can click **“Resend registration code”**. Make sure to check your Spam / Junk folder. If the issue of receiving the code persists, please reach out to support@911secure.com.)

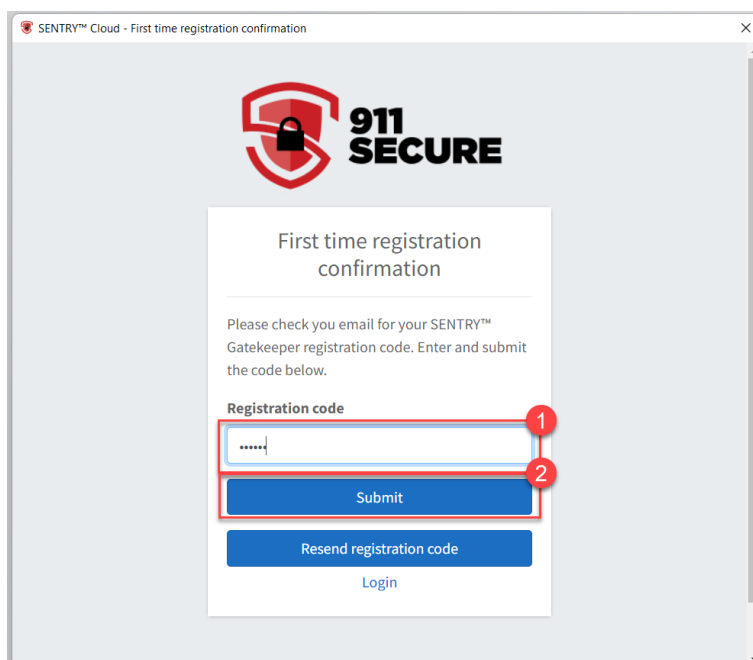
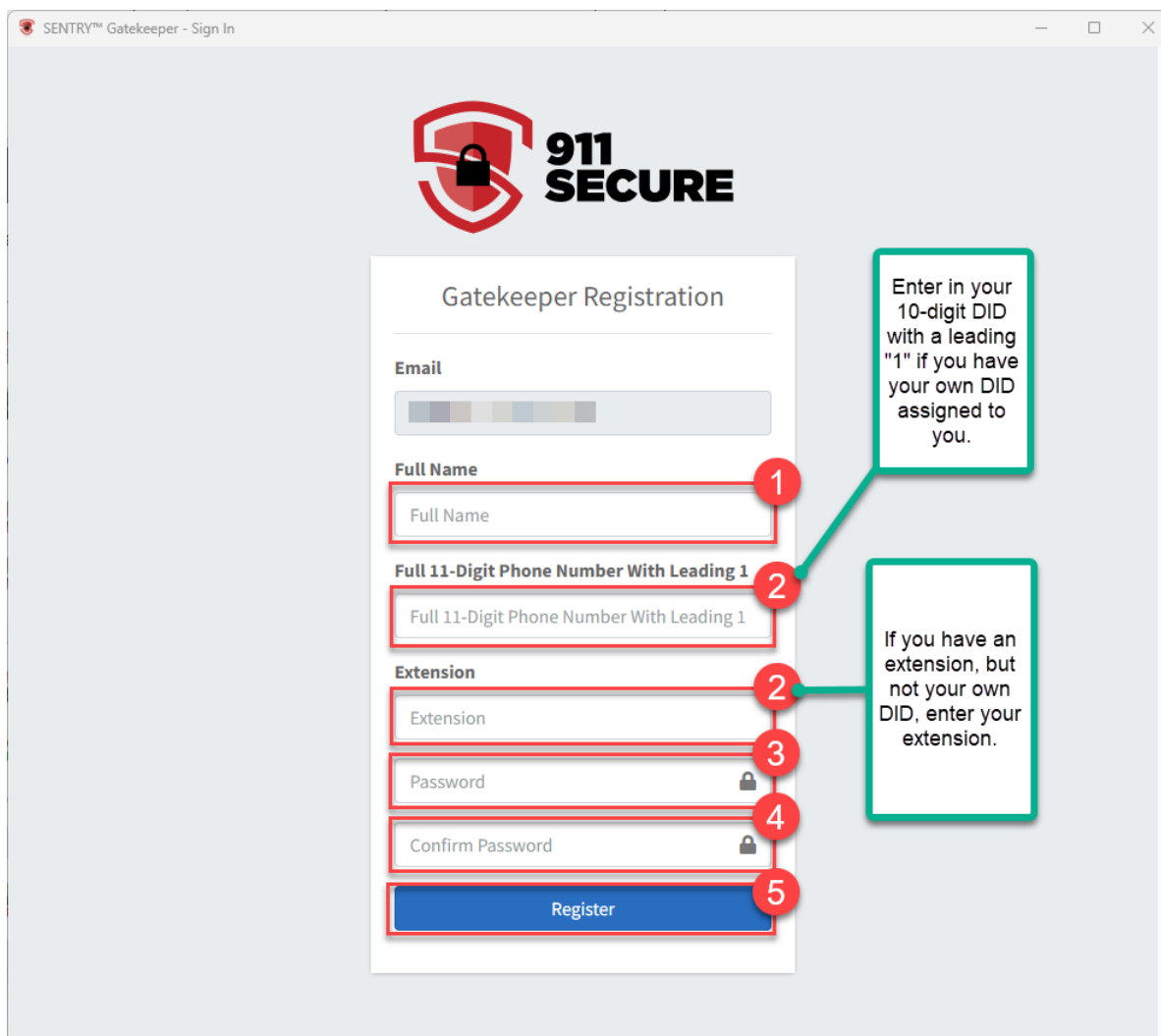


Figure 45

7. You will be presented with a “**Gatekeeper Registration**” screen with several fields to fill in. Enter your **full name** and either your assigned **Extension** or assigned 11-digit **ELIN / DID** into the appropriate fields. If you have an assigned Extension, enter it into the **Extension** field and leave the “Full 11-Digit Phone Number With Leading 1” field blank. If you have been assigned an 11-digit **ELIN / DID** (i.e., the full 10-digit phone number used with your softphone device prepended with a leading “1” such as “15555552468”), enter that into the “**Full 11-Digit Phone Number With Leading 1**” field and leave the Extension field blank. You will also create a password to use when logging into SENTRY™ Gatekeeper in the future. Enter this created password into the “**Password**” and “**Confirm Password**” fields (indicated by the lock icons). Once finished, click “**Register**” to complete the self-registration process.



The screenshot shows the SENTRY Gatekeeper Sign In page. The main heading is "Gatekeeper Registration". Below it are several input fields: "Email", "Full Name", "Full 11-Digit Phone Number With Leading 1", "Extension", "Password", "Confirm Password", and a "Register" button. Red circles with numbers 1 through 5 are placed next to the "Full Name", "Full 11-Digit Phone Number With Leading 1", "Extension", "Password", and "Confirm Password" fields respectively. Two green callout boxes provide additional instructions: one for the "Full 11-Digit Phone Number With Leading 1" field stating "Enter in your 10-digit DID with a leading '1' if you have your own DID assigned to you.", and another for the "Extension" field stating "If you have an extension, but not your own DID, enter your extension.".

Figure 46

8. **PLEASE NOTE:** When logging into the application for the very first time, you will be met with a “**Gatekeeper User Acceptance**” window. Its purpose is to help end users understand why they must set their location and the importance of doing so. While the exact User Acceptance message may vary depending on the customer, the **default verbiage** is displayed below. Users must click the “**I have read and understand the above statement**” **checkbox**, then click on the “**OK**” button.

SENTRY™ Gatekeeper User Acceptance Default Message:

“SENTRY™ Gatekeeper is an application for keeping softphone users safe whenever they are working from a remote / offsite location. It requires users to provide accurate location information so any 911 call made from their softphone can be routed to the closest Public Safety Answering Point. By clicking the OK button below, I acknowledge that I will enter only accurate location information whenever my work location changes.”

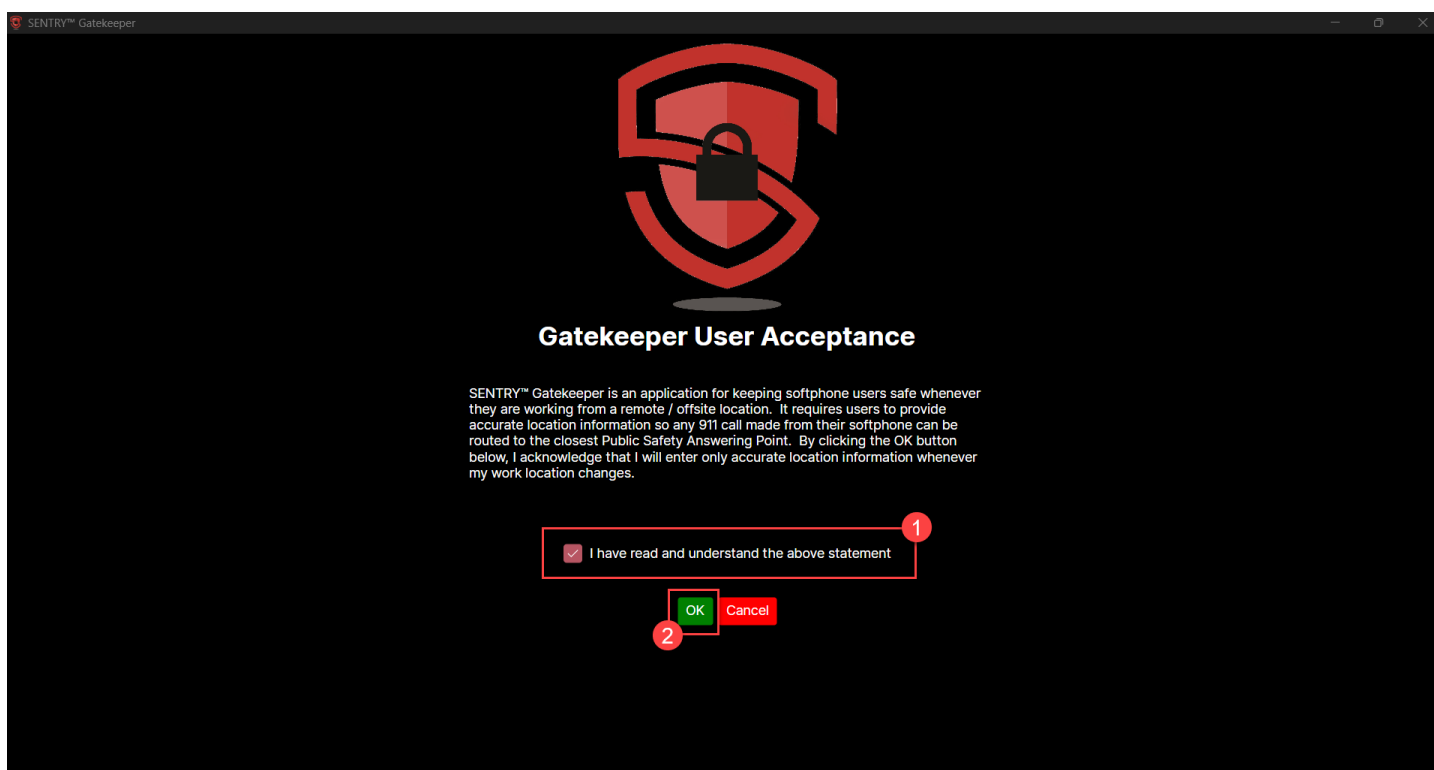


Figure 47

- Once you have signed in and clicked “OK” for the User Acceptance agreement, you will be brought to the SENTRY™ Gatekeeper client screen and can begin the process of setting or selecting your address.

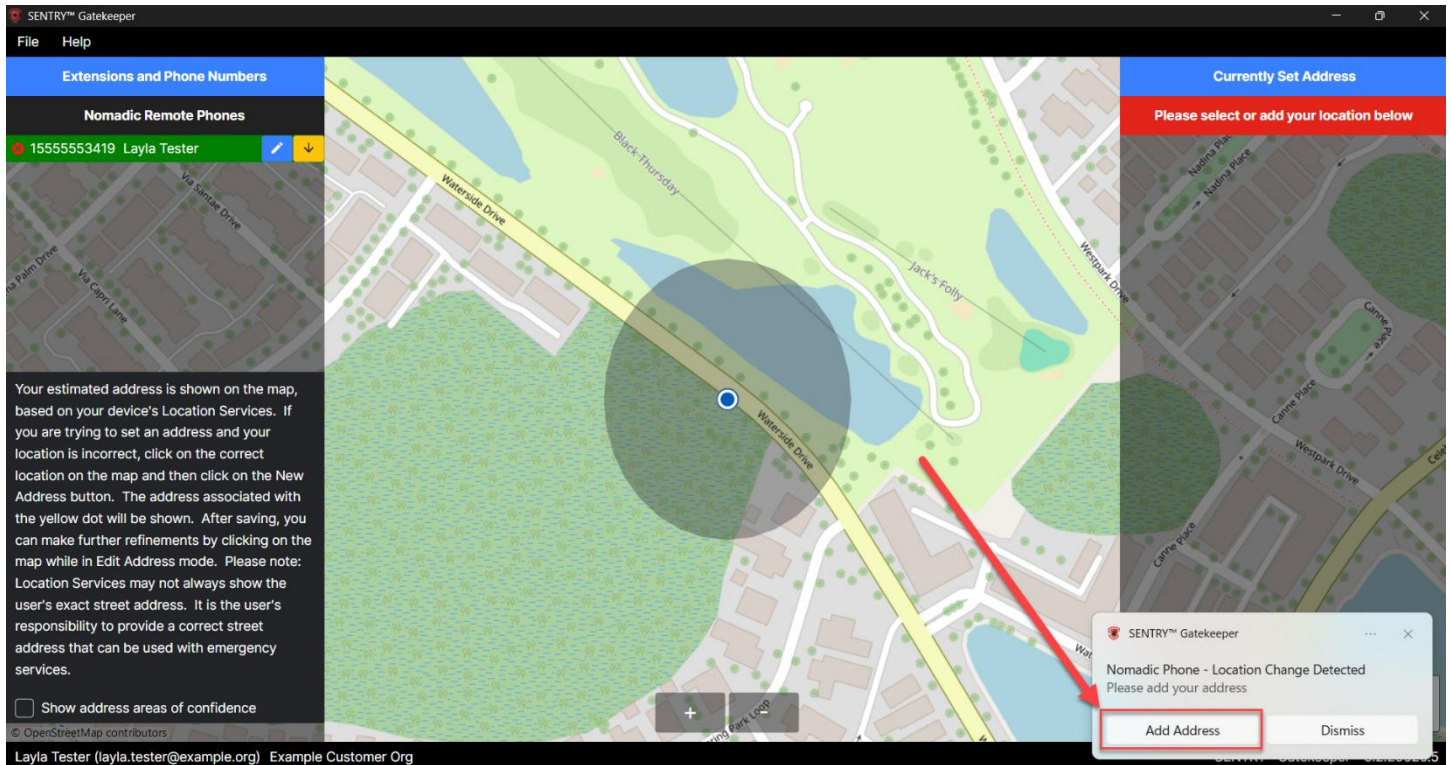


Figure 48

LOGGING IN WITH AZURE AD CREDENTIALS

Once you have finished the steps to complete Self-Registration and your first-time login, you can follow the steps below for all subsequent instances of logging into SENTRY™ Gatekeeper. When first starting SENTRY™ Gatekeeper, the user will be asked to log in using credentials set up by the SENTRY™ Cloud Administrator.

In most cases, users will use their normal organizational login account, using Azure Active Directory credentials. To log in:

1. Click **“Sign in with Azure AD credentials”**.

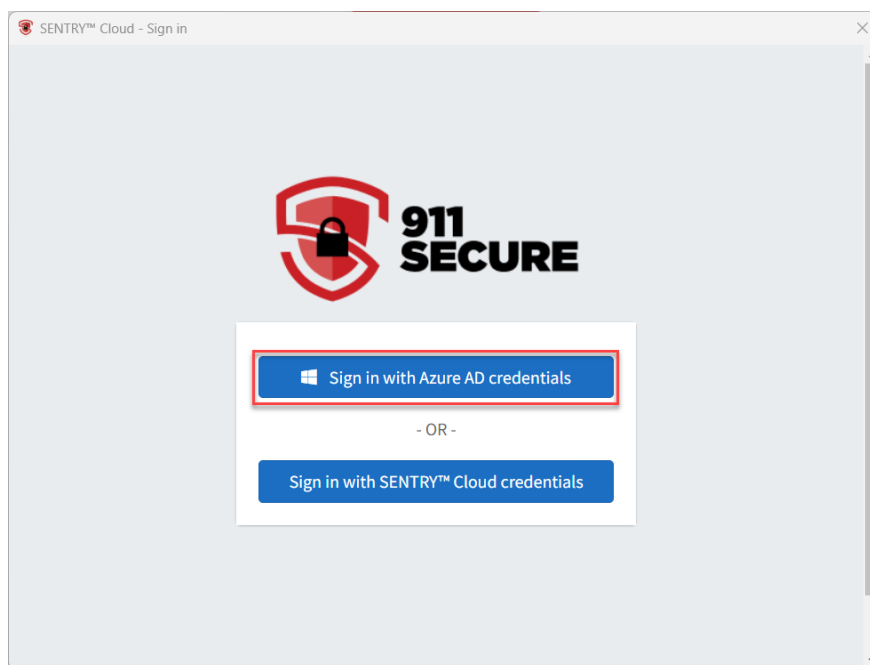


Figure 49

2. Enter your **email** address, then **password**. Then click **“Sign in”**.

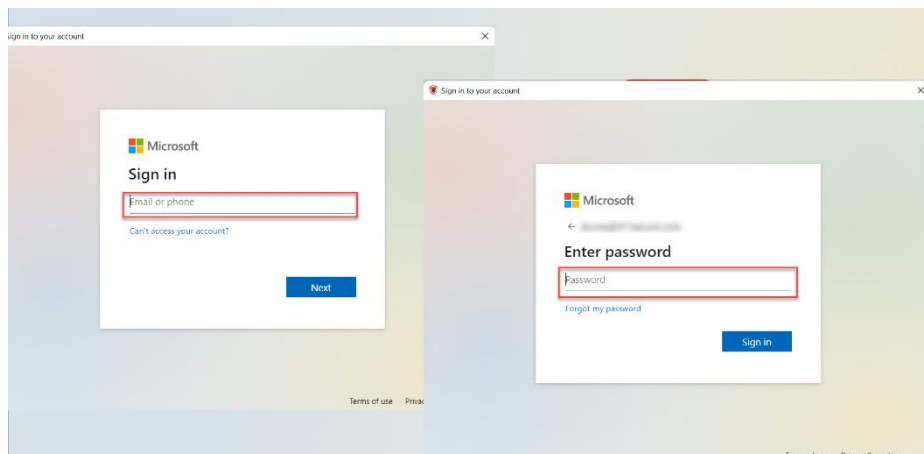


Figure 50

LOGGING IN WITH SENTRY™ CLOUD CREDENTIALS

In some cases where Azure Active Directory Authentication is not used by organizations, simple SENTRY™ Cloud credentials may be used instead. To log in:

1. Click “**Sign in with SENTRY™ Cloud credentials**”.

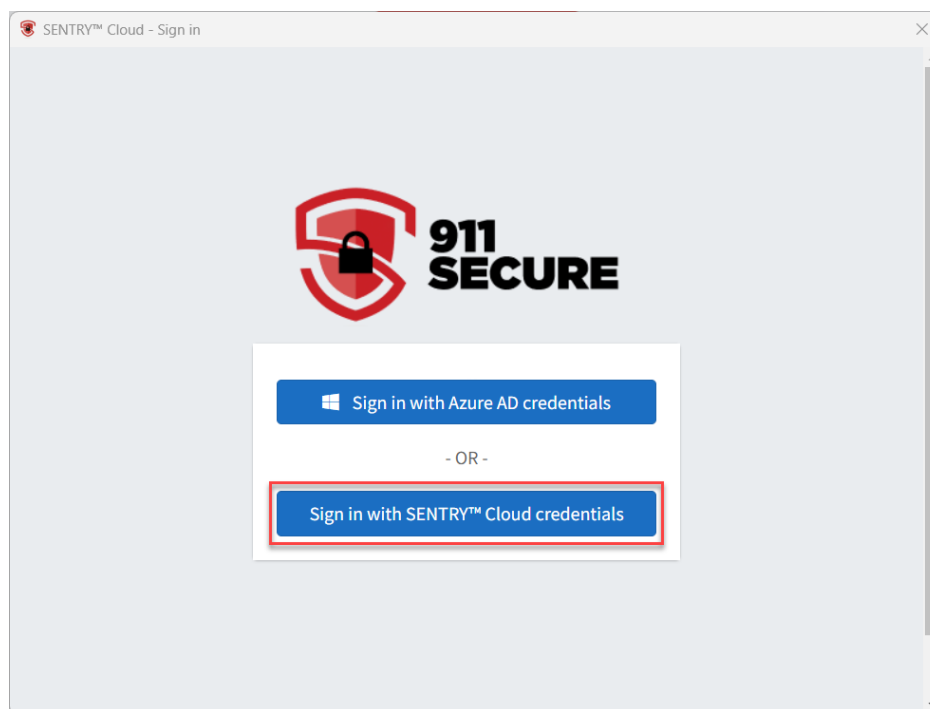


Figure 51

2. Enter your SENTRY™ Cloud **email** address and **password**, then click “**Sign In**”.

SENTRY™ GATEKEEPER v5.6 USERS GUIDE



STOP! PLEASE NOTE: Unlike Remote DIDs and On Premise DIDs, **Cloud-sourced ELINs / DIDs ARE capable of being overtaken by SENTRY™ Gatekeeper users.** We strongly recommend that remote workers dial 933 once they have set their information within SENTRY™ Gatekeeper. This will help ensure they are hearing a correct readback of their DID and address information.



STOP! PLEASE NOTE: **Captive internet** (seen at locations such as hotels) and **mobile hotspots with VPN** may lead to **inaccurate Location Services** results due to technical limitations. 911 Secure continues to investigate improvements regarding these limitations.

SELECTING AN ACTIVE PHONE IN SENTRY™ GATEKEEPER

After a user logs into SENTRY™ Gatekeeper for the first time, if they have more than one phone number / DID assigned to them, they will be presented with their personal **Phone List** where they can select which phone will be used currently for updating their E911 address.

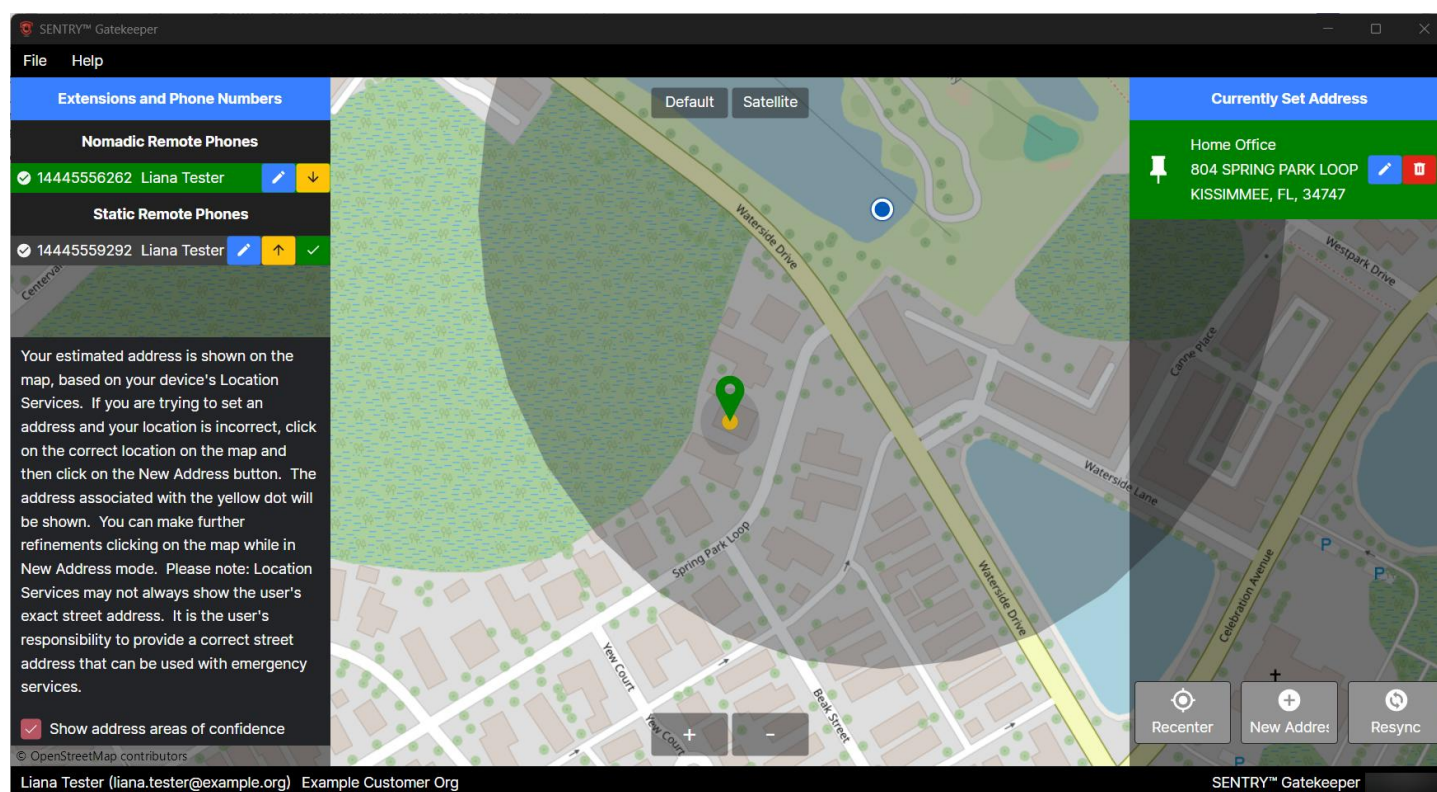


Figure 52

Users may return to this page at any time by selecting the green checkmark “**Select Phone**” button next to their name under the **Extensions and Phone Numbers** section of their client window to choose another phone for setting their E911 address. If a SENTRY™ Gatekeeper user has been assigned only a single phone number / DID in SENTRY™ Cloud, then that phone will be selected automatically. Users will simply show their one phone on the lefthand side of their screen (set as a Nomadic phone by default).

From this **Extensions and Phone Numbers** section, users can switch their remote phone from **NOMADIC** to **STATIC** and vice-versa by clicking the **yellow arrow button**. A **Nomadic** remote phone is one that can move around (i.e., a soft client on a PC) whereas a **Static** remote phone is one that is stationary and does not move (i.e., a corporate handset in one’s home office). Friendly names may be added for each phone number to identify them more easily by using the “**Edit phone**” **blue pencil button**.

The difference between the two is that if a change is detected in the Gatekeeper PC’s network location, then an assumption is made that all nomadic phone numbers have changed locations, but all static phone numbers have not. In this way, if a user had multiple soft clients running on their PC (Teams, Avaya IX Workplace, etc.) that all were set to Nomadic remote phones, when a user updated their E911 location, then all their E911 Addresses for their Nomadic phone numbers would be updated in SENTRY™ Cloud and their Static phone numbers would be left alone.

PLEASE NOTE: If a SENTRY™ Gatekeeper user uses a **Static** phone, then once the user sets a location for it, SENTRY™ Gatekeeper will **NOT** prompt the user to update that location again even if the user physically picks up and moves the phone. If a SENTRY™ Gatekeeper user uses a Static phone and moves it after setting an initial location for it, that user **MUST** update their SENTRY™ Gatekeeper address manually to reflect their new location. SENTRY™ Gatekeeper users may do this either by using the blue pencil “**Edit address**” button, then saving their changes, or by using the “**+New Address**” plus sign button then saving that address. Users can find both features at the bottom right-hand side of the SENTRY™ Gatekeeper client screen.

PLEASE NOTE: If you have more than one phone assigned to you as a SENTRY™ Gatekeeper user, please make sure to set an address for each corresponding DID / Extension representing those devices. If not, SENTRY™ Gatekeeper will continue to prompt you to set your location for which ever phone(s) do not have a location provisioned.

PLEASE NOTE: SENTRY™ Gatekeeper toast messages differ based on whether the user is remote or on-premise. In addition, they will also differ based on whether the user has a Nomadic phone versus a Static phone. Below are a few examples.

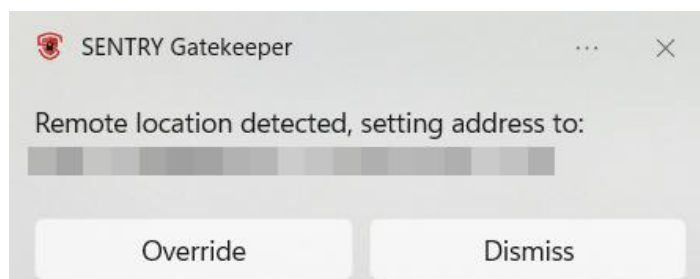


Figure 53

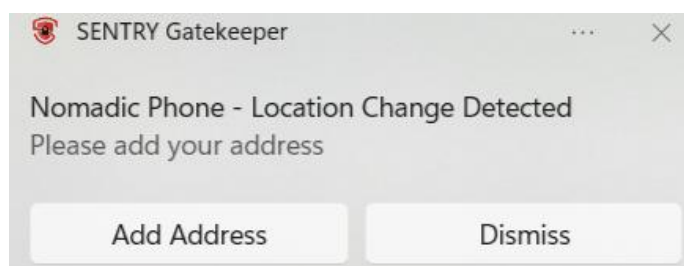


Figure 54

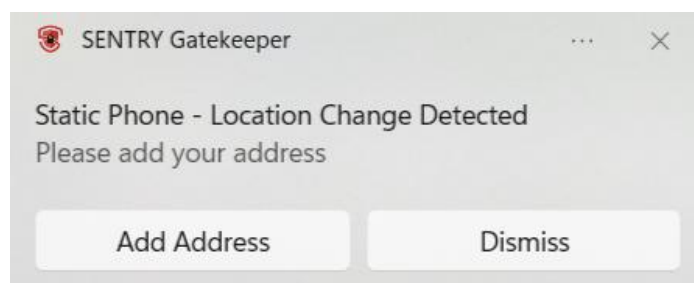


Figure 55

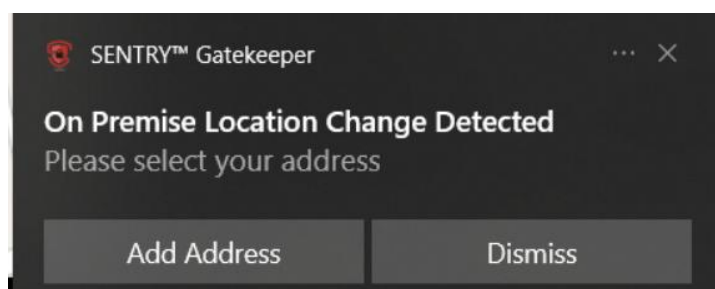


Figure 56

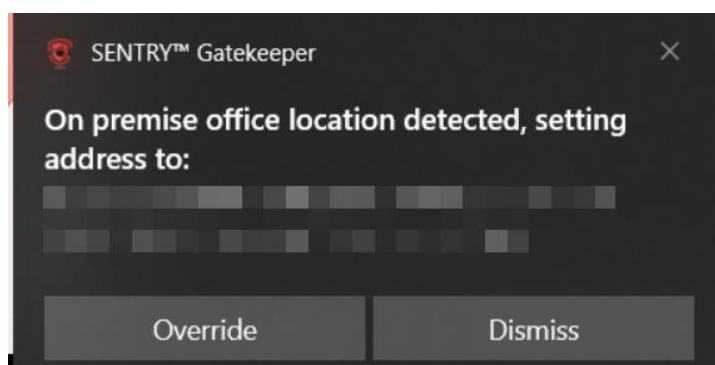


Figure 57

SETTING A REMOTE ADDRESS LOCATION IN SENTRY™ GATEKEEPER

For SENTRY™ Gatekeeper users working away from an office / corporate environment, they must indicate their accurate current address to remain protected. This ensures their correct location information gets outpulsed to their local serving PSAP (Public Safety Answering Point) as the time of a 911 call. The following steps cover how SENTRY™ Gatekeeper users can set the location when working remotely.

1. Once a user signs into SENTRY™ Gatekeeper for the first time, the user will receive a notification in the lower right-hand corner of the screen saying **“Nomadic Phone – Location Change Detected. Please add your address.”** They will also see a **blue dot** indicating where their device's **Location Services** thinks they are. If the **Location Services** estimation is accurate, users can then click on the **“Add Address”** button, as shown below. **PLEASE NOTE:** If **Location Services** is **NOT** accurate, please see the [“Editing an Address in SENTRY™ Gatekeeper”](#) section below.

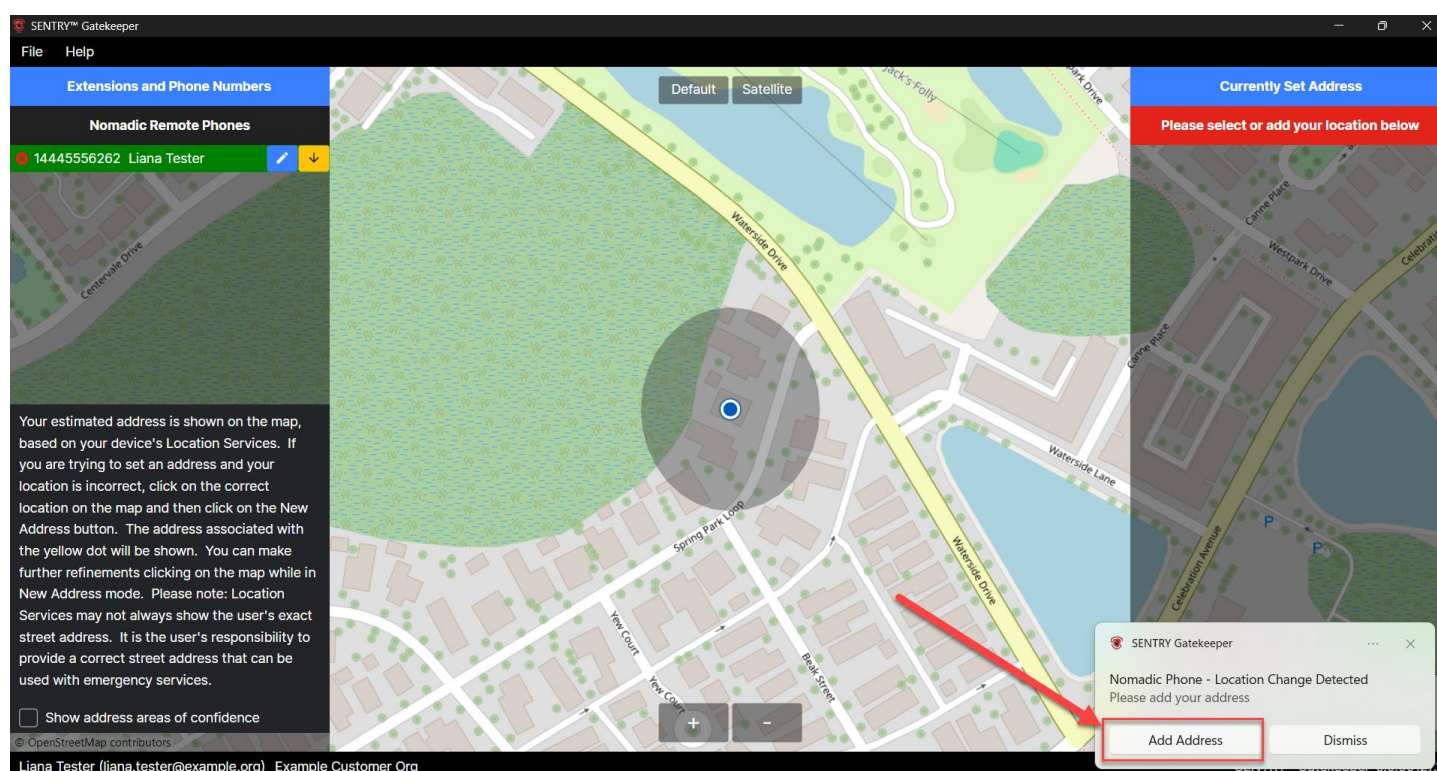


Figure 58

- With SENTRY™ Gatekeeper’s geolocation capabilities, the **best approximation of the user’s current address** will appear under the **Edit Address** panel on the right-hand side of the SENTRY™ Gatekeeper client window.

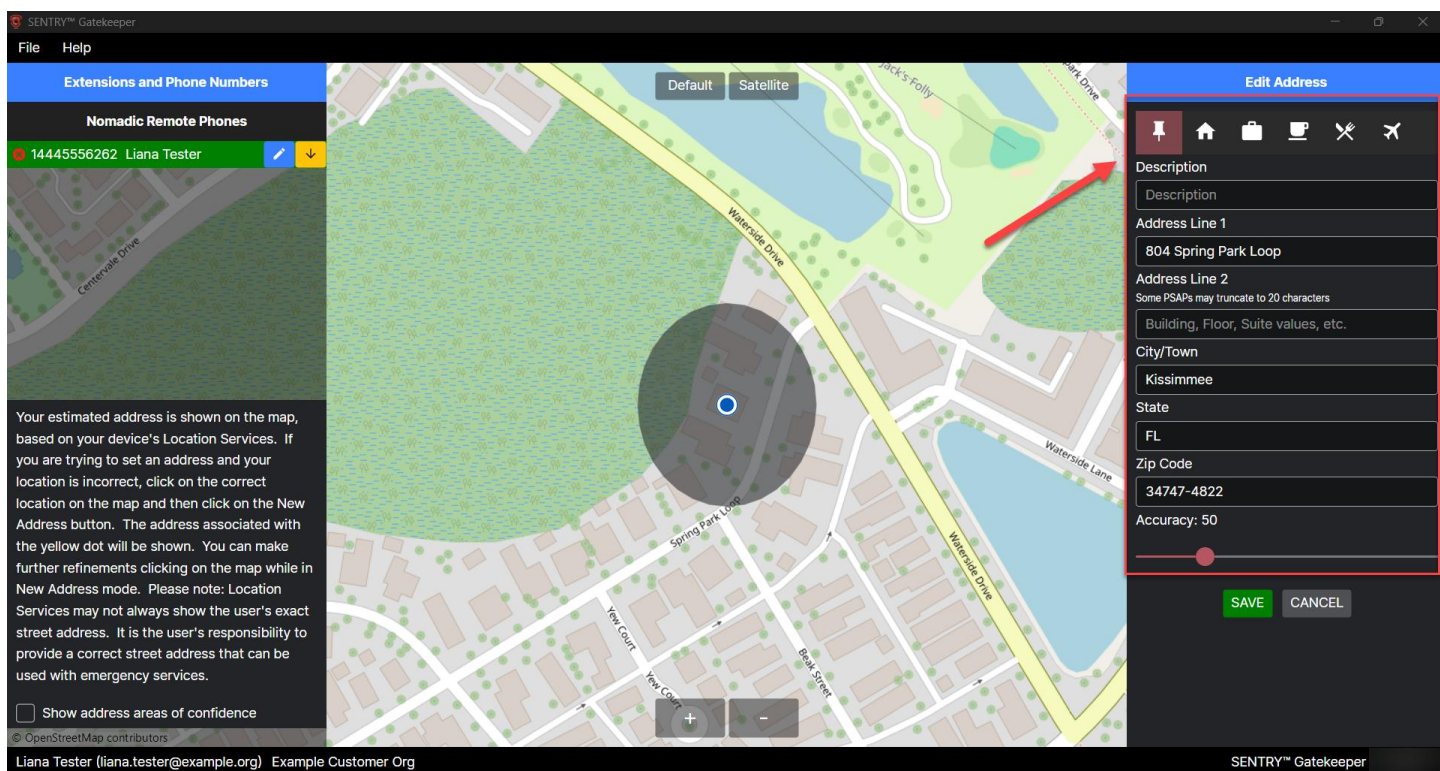


Figure 59

- If desired, the SENTRY™ Gatekeeper user can select an **icon** to represent their location. If not, a pushpin icon will display by default. The user can also enter a short description of their location in the **Description** field (such as “Office”, “Home”, “Library”, etc.). This Description is optional and will NOT get sent to the PSAP.

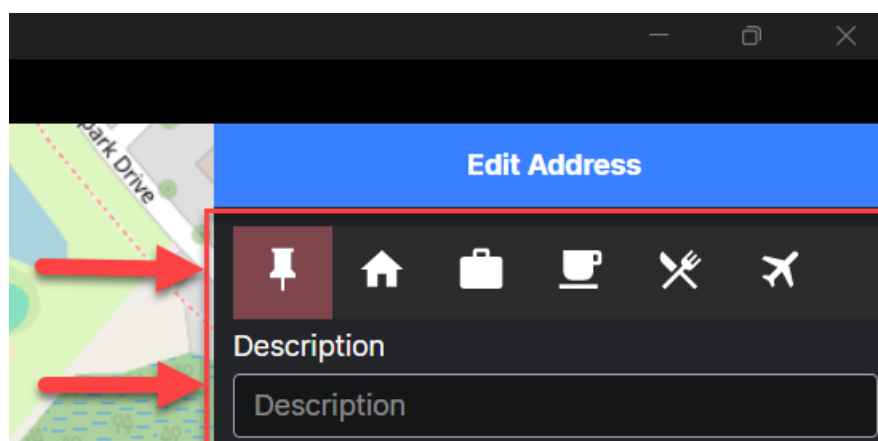


Figure 60

4. The user can then check over the address presented across **Address Line 1** (displaying the main street address of the location), along with the **City / Town**, **State**, and **Zip Code** information. If no adjustments are necessary, the user can leave those fields as is. **PLEASE NOTE:** If the presented address is not accurate, please see the [“Editing an Address in SENTRY™ Gatekeeper”](#) section below.

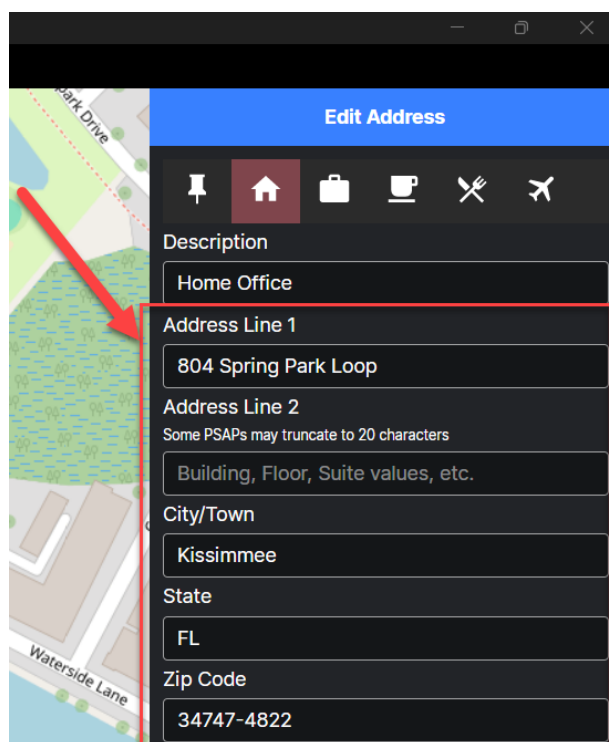


Figure 61

5. If the user lives in an apartment building, condominium complex, etc. where listing something such as a unit number, apartment number, and or floor number would help first responders know their exact location, the user can enter those details in the **Address Line 2** field. Any additional dispatchable location information belongs in Address Line 2, which is an **optional** field. **PLEASE NOTE:** Many PSAPs will truncate anything that exceeds 20 characters in limit.

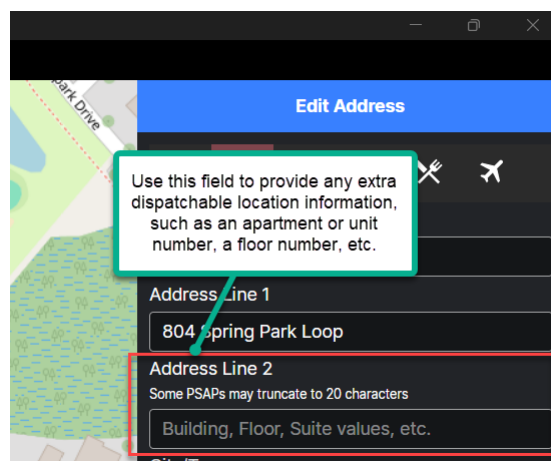


Figure 62

- Though optional, users can also adjust the **Accuracy** slider listed underneath the other **Edit Address** details. The Accuracy ring / area of confidence around the user's pin indicates the **level of estimated accuracy** of the user's location within the circumference displayed (in meters). The user can use the Accuracy slider to increase or decrease the circumference / distance of the ring. A larger area of confidence creates a larger possible area for the user to be located in. A smaller area of confidence indicates a more limited or precise area. **PLEASE NOTE:** This Accuracy / area of confidence does NOT get sent to the PSAP. **PLEASE NOTE:** You must have the “**Show address areas of confidence**” checked to see the results of the Accuracy slider.

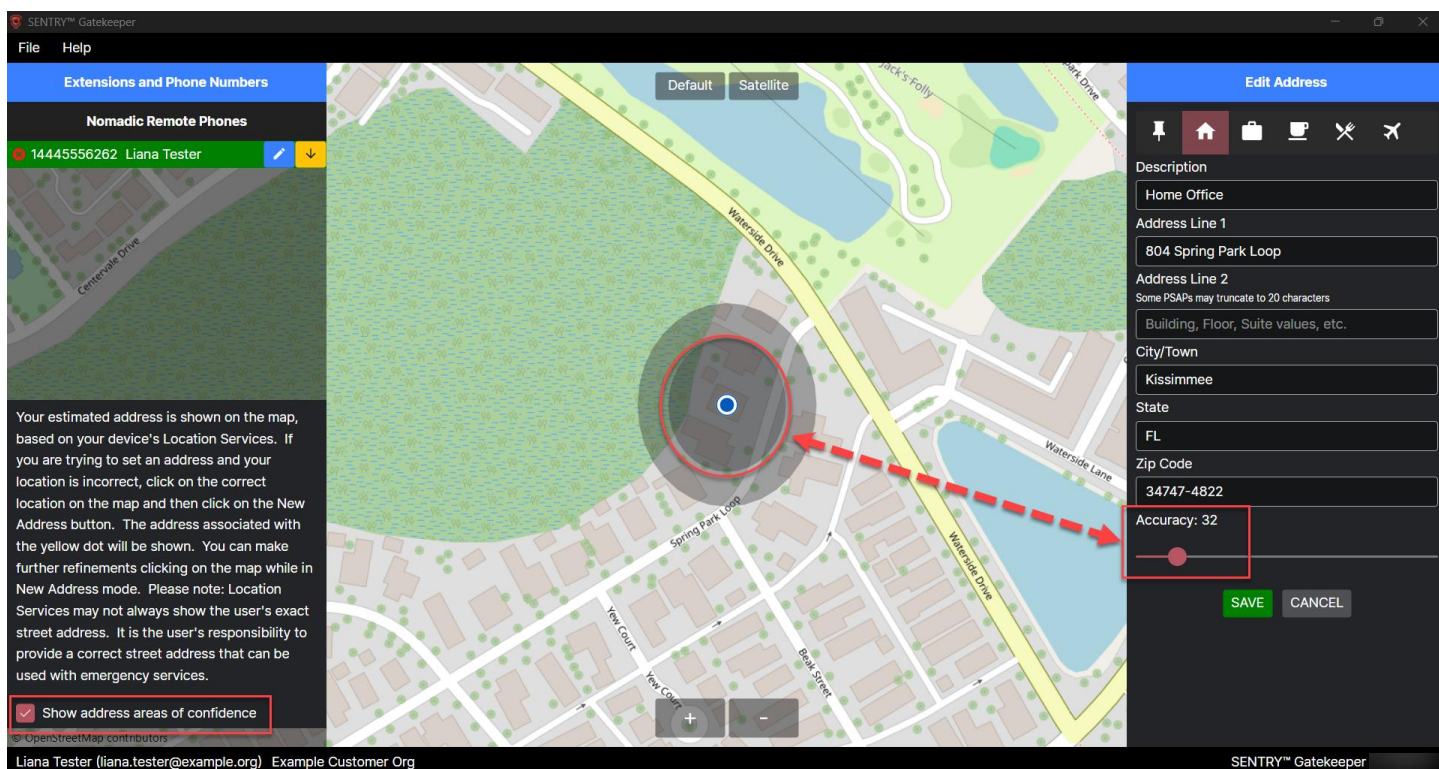


Figure 63

- After entering an address, select the **“Save”** button to verify and provision the address as a valid US Postal service address and in the Master Street Address Guide. If you receive an **“_ERR-JAB-0024: Address could not be validated”** message, see the **“SENTRY™ Gatekeeper Troubleshooting Guide”** section below.

If you receive “_ERR-JAB-0024: Address could not be validated”, this error indicates the address is not valid. This error can occur for many reasons. One such reason could be that a new location has not yet been verified as a valid US Postal service address and / or has not been entered into the Master Street Address Guide. Please make sure you have entered a valid address including the city, state, and zip code. It may be helpful to verify the address using <https://www.google.com/maps>. If you have verified the address is correct and valid but Gatekeeper will not accept it, please email support@911secure.com with details of the address. 911 Secure will follow up with the necessary research and get the address verified and entered into the Master Street Address Guide.

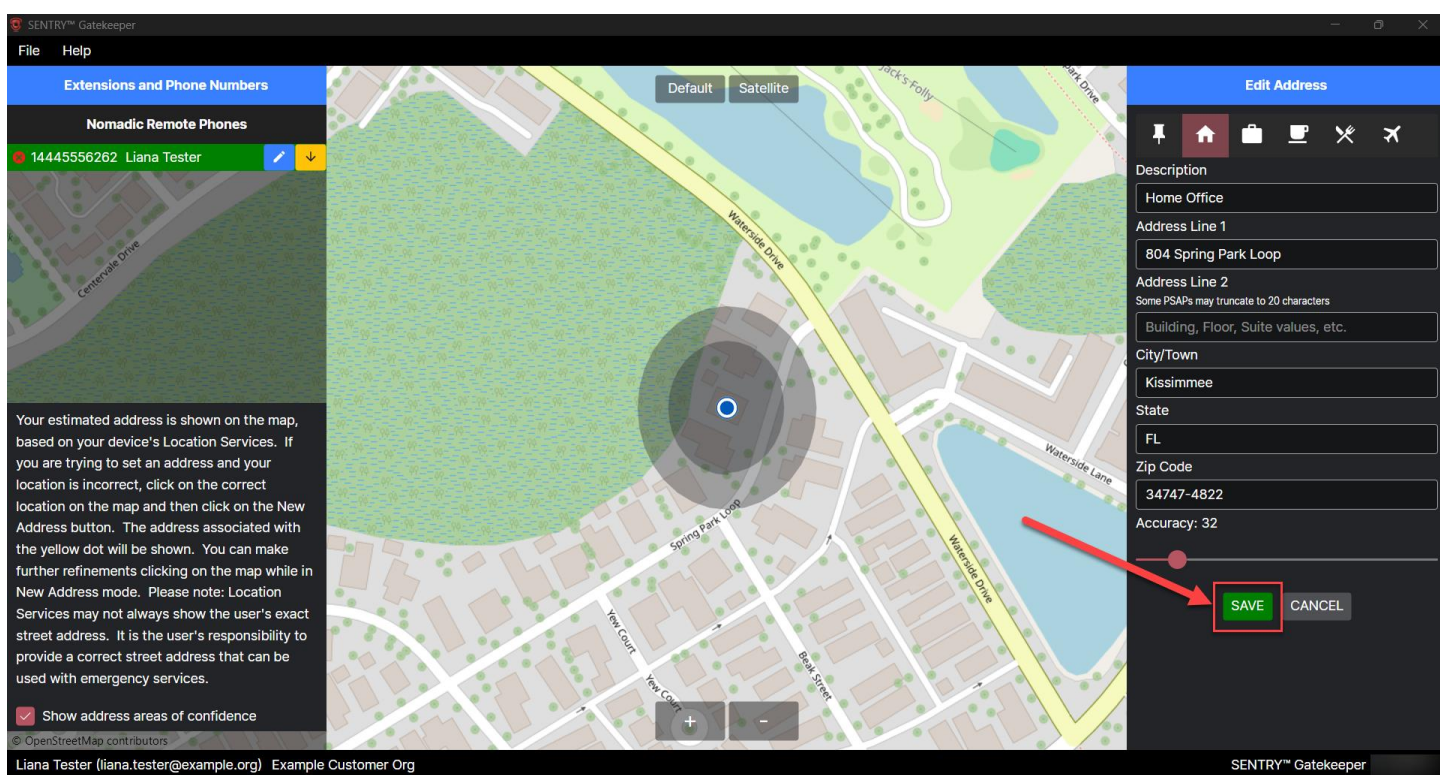


Figure 64

8. After clicking “Save”, the user will see their Currently Set Address bar turn entirely green and a toast message saying “**Saved Address created, setting to: [user’s saved address]. Override. Dismiss.**” will display. Users can click “Dismiss” or just wait for the toast message to retract. The user has officially set their location.

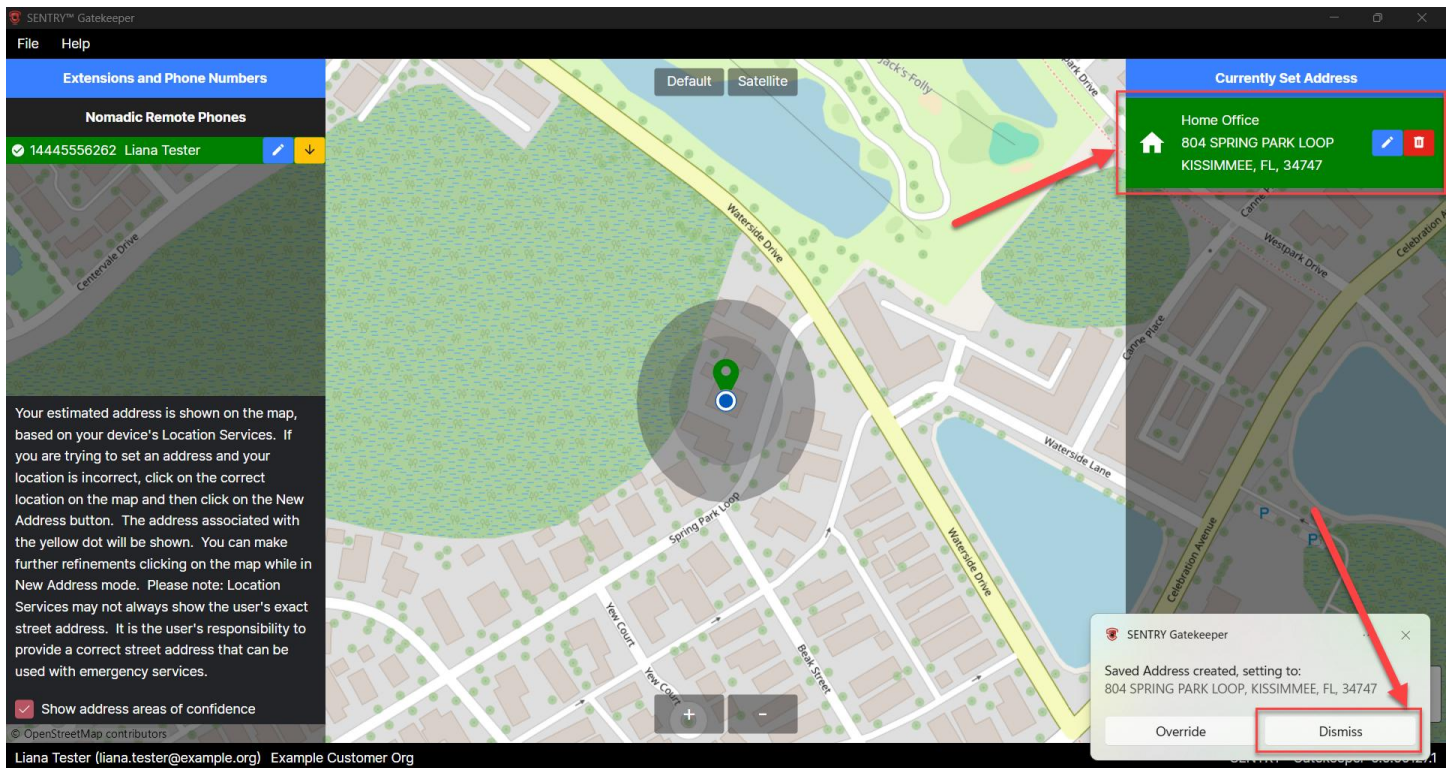


Figure 65

9. **PLEASE NOTE:** The left-hand side of the SENTRY™ Gatekeeper client window shows a disclaimer on the topic of editing / correcting address information. In addition, users can click the **“Show address areas of confidence”** checkbox to display the Accuracy area of confidence around their updated address pin, as shown in the screenshot below. A larger area of confidence creates a larger possible area for the user to be located in. A smaller area of confidence indicates a more limited or precise area. (The areas of confidence are more easily seen in the **“Default”** view mode as opposed to the **“Satellite”** mode.) **PLEASE NOTE:** Users will see one area of confidence generated by Location Services (which displays regardless of checking the **“Show address areas of confidence”** box), and a second one generated from their use of the Accuracy slider discussed in step 7 above.

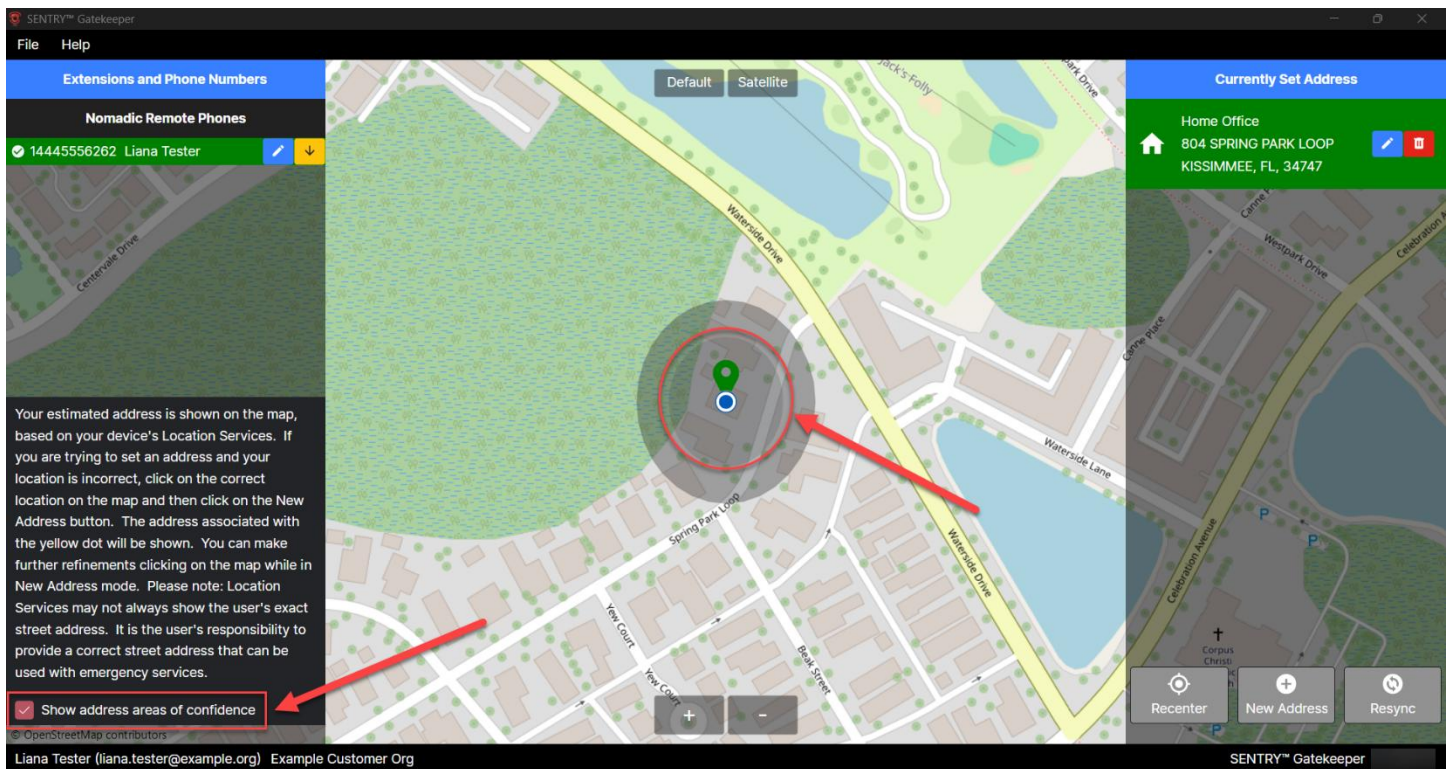


Figure 66

10. If a SENTRY™ Gatekeeper remote worker finds themselves working at a previously saved / provisioned location and is very close to another previously saved / previous location, they may be prompted to **select** which address they are truly located at. For instance, the screenshots below depict a remote worker stationed at a previous location. However, since the area of confidence overlaps with another previous location, SENTRY™ Gatekeeper prompts the user to confirm their correct location. When presented with this situation, the user can click the **green checkmark** to set and **provision** their correct location. Once the user clicks on their correct location option, a toast message saying **“Remote location detected, setting address to: [user’s location]. Override. Dismiss.”** will display. Users can click **“Dismiss”** or wait for the message to retract / disappear. The user’s location is now set.

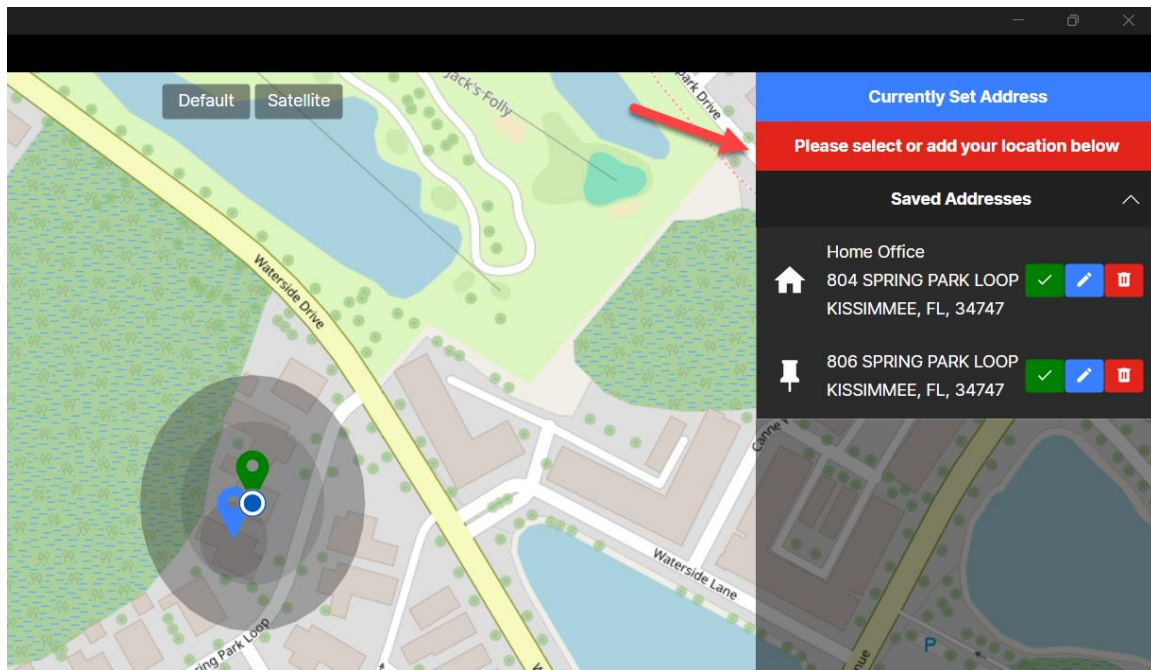


Figure 67

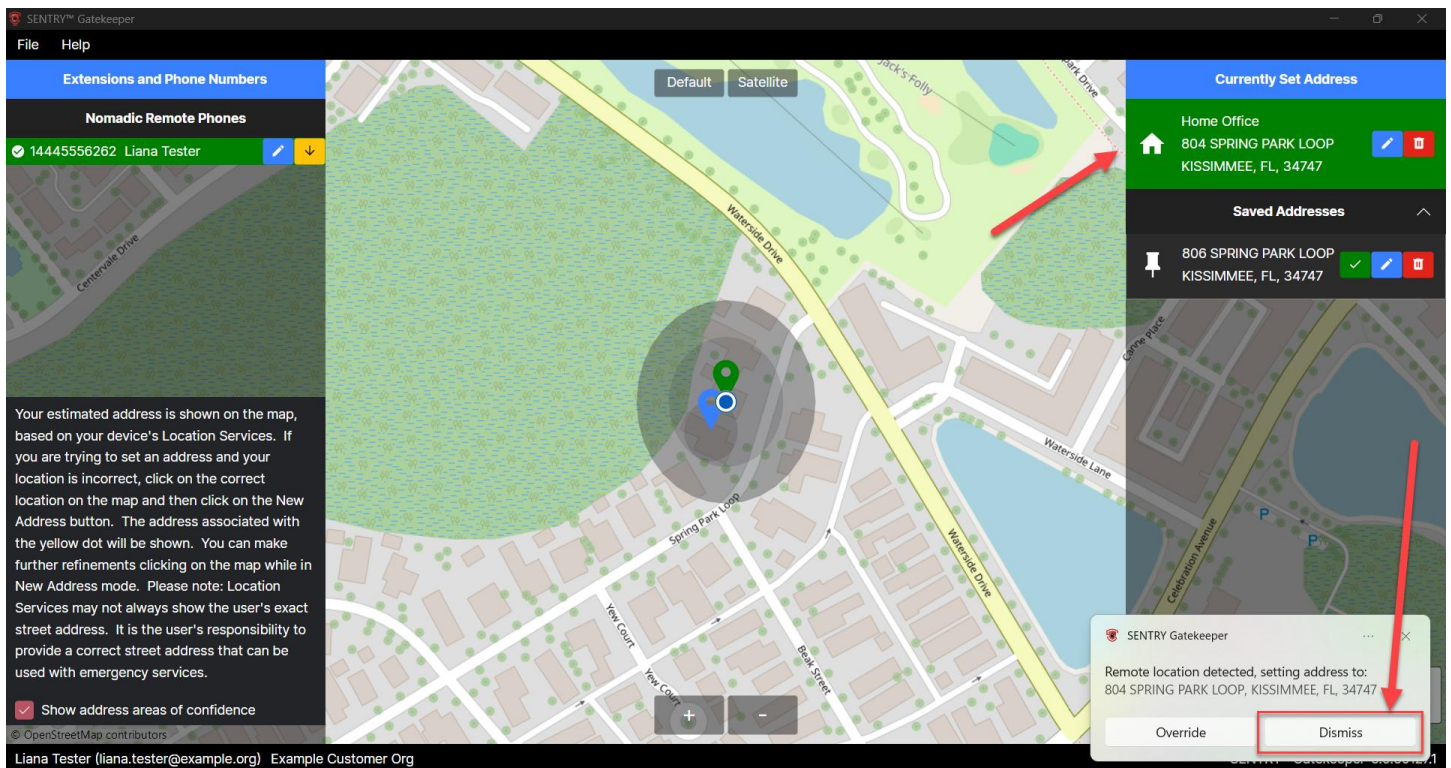


Figure 68

EDITING AN ADDRESS IN SENTRY™ GATEKEEPER

If the address presented to the SENTRY™ Gatekeeper end user when setting their remote location is inaccurate, the user can follow the steps outlined below. **PLEASE NOTE:** The estimated address initially shown on the SENTRY™ Gatekeeper map is based on the end user's device's Location Services. It is the end user's responsibility to provide a correct street address for emergency services.

PLEASE NOTE: SENTRY™ Gatekeeper users may notice that the **blue dot** indicating their initial pinpointed location will remain in its original place even after the user corrects and provisions their edited location. This is because the blue dot represents where the Location Services of the user's PC says where the user is. SENTRY™ Gatekeeper cannot and will not override what the user's Location Services indicates, but, as shown in the section above, it will allow users to provision the address they know is correct. If the SENTRY™ Gatekeeper user must edit their address for accuracy, they can rest assured that the adjusted provisioned address will output to the PSAP.

1. If a user must edit their address because their Location Services pinned them incorrectly, users can edit their address by **clicking on the map** with their cursor to change / update their position to its correct place. A **yellow dot** will appear, representing the user's click. Next, the user can click on the **“+New Address”** button in the bottom center of the **“Currently Set Address”** column. Users can then check and ensure that the address details under **“Edit Address”** are correct before clicking **“Save”**. The user will see the **address** information changes accordingly, and a **green map pin** will appear to indicate their updated set address. Click **“Dismiss”** or wait for the confirmation toast message to retract / disappear.

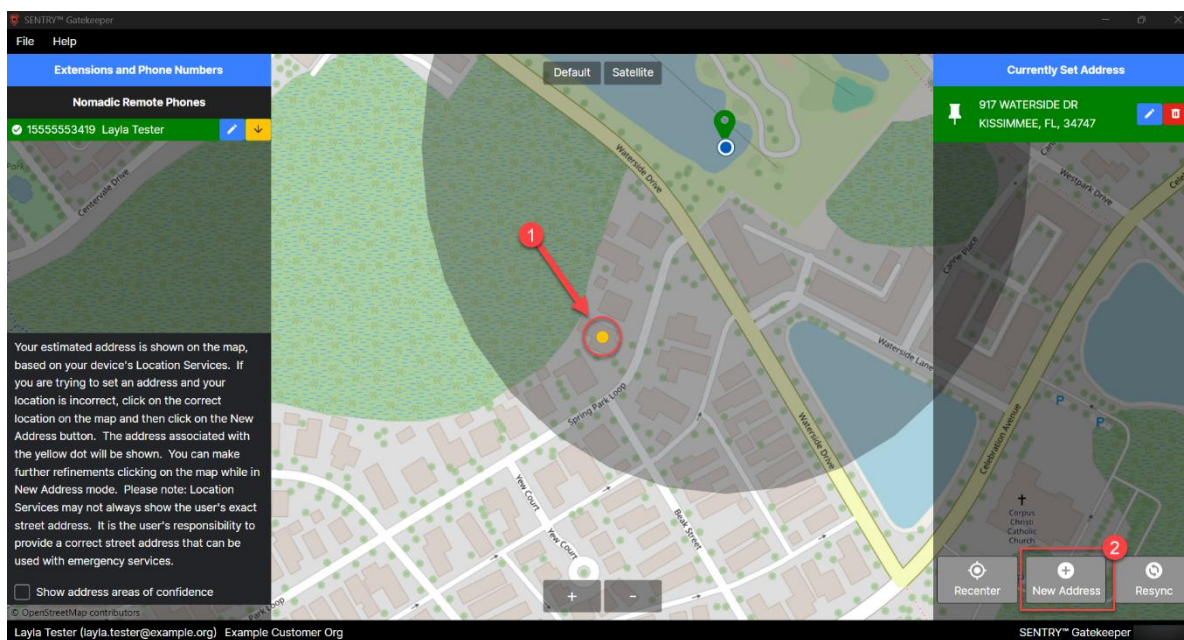


Figure 69

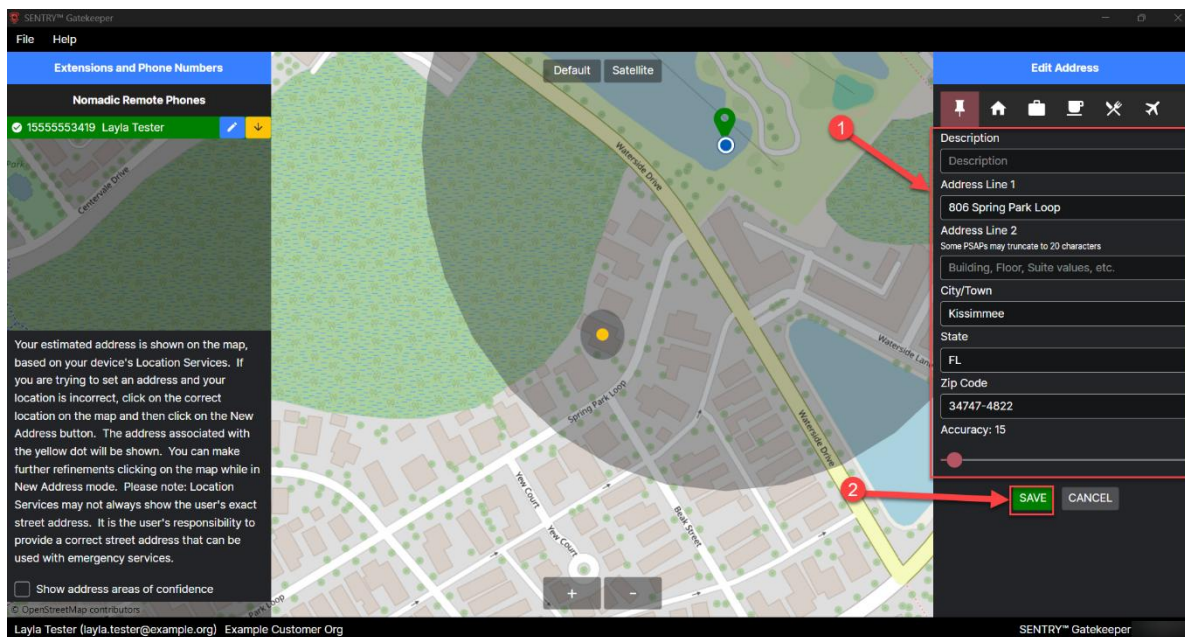


Figure 70

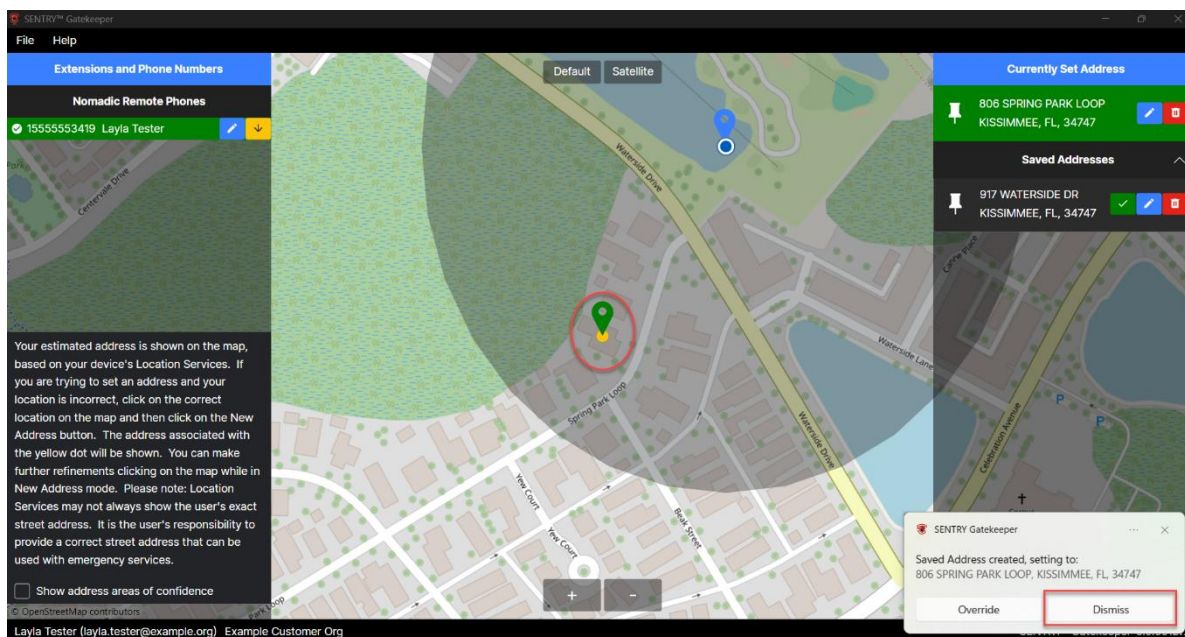


Figure 71

- If a user needs to update secondary or optional information such as their Address Line 2 information or the Description field, users can click on the blue pencil “**Edit**” icon, adjust or add the desired information, then click “**Save**”. In the example below, the user updates their address icon, their **Description**, their **Address Line 2** details, and their **Accuracy** slider. The user will see the **address** information change accordingly.

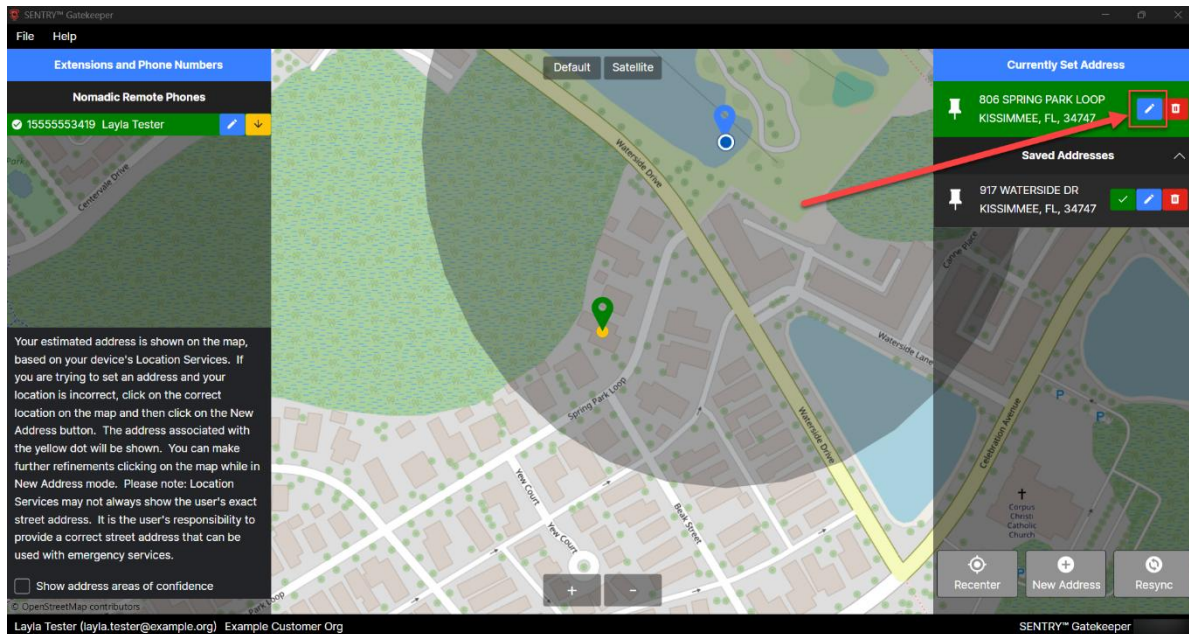


Figure 72

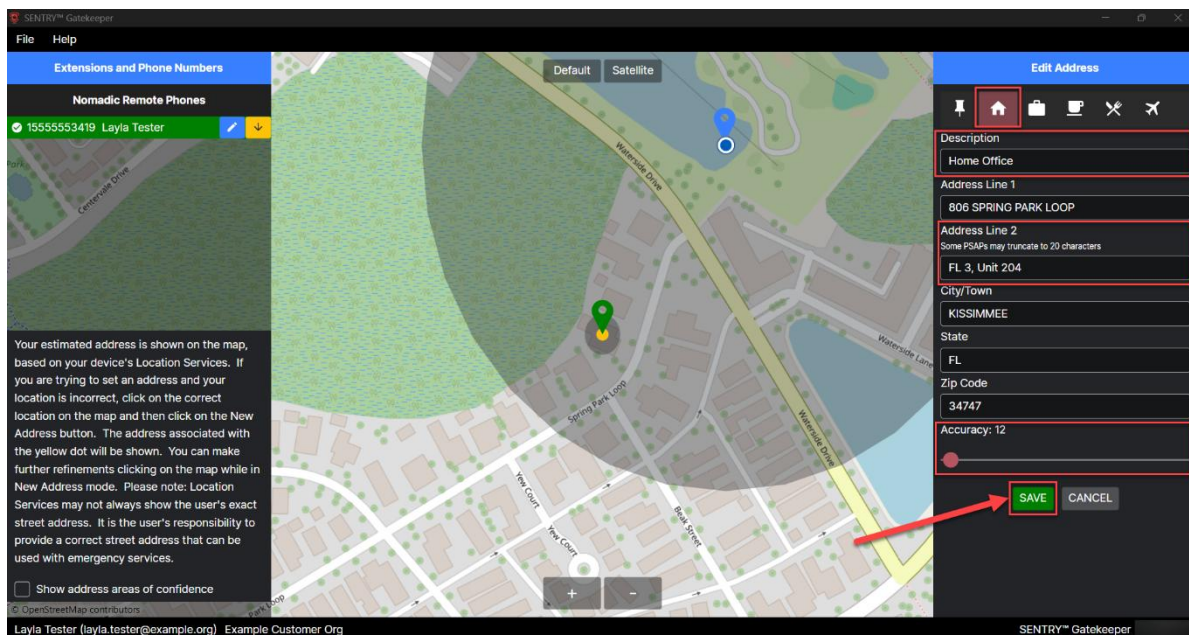


Figure 73

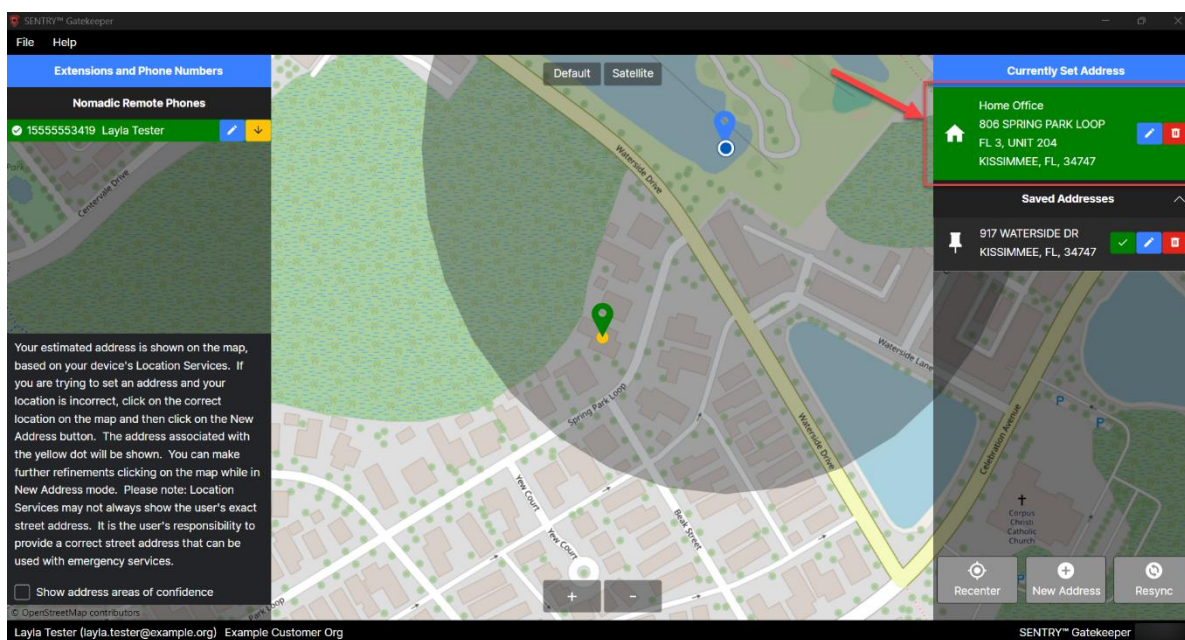


Figure 74

3. **PLEASE NOTE:** The left-hand side of the SENTRY™ Gatekeeper client window shows a disclaimer on the topic of editing / correcting address information. In addition, users can click the **“Show address areas of confidence”** checkbox to display the Accuracy area of confidence around their updated address pin, as shown in the screenshot below. A larger area of confidence creates a larger possible area for the user to be located in. A smaller area of confidence indicates a more limited or precise area. (The areas of confidence are more easily seen in the **“Default”** view mode as opposed to the **“Satellite”** mode.) **PLEASE NOTE:** Using the **Accuracy** slider is optional as it does **NOT** get sent to the PSAP.

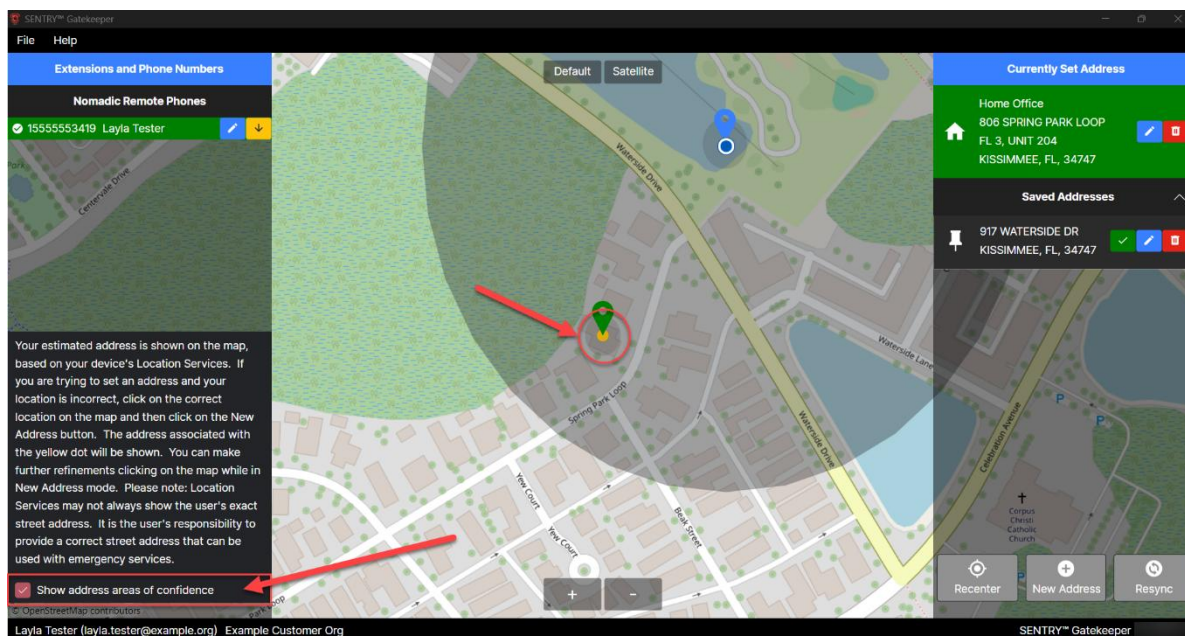


Figure 75

DELETING AN ADDRESS IN SENTRY™ GATEKEEPER

1. To **Delete** an address, click on the **red trash can** icon of the address to be edited, as shown in the figure below.

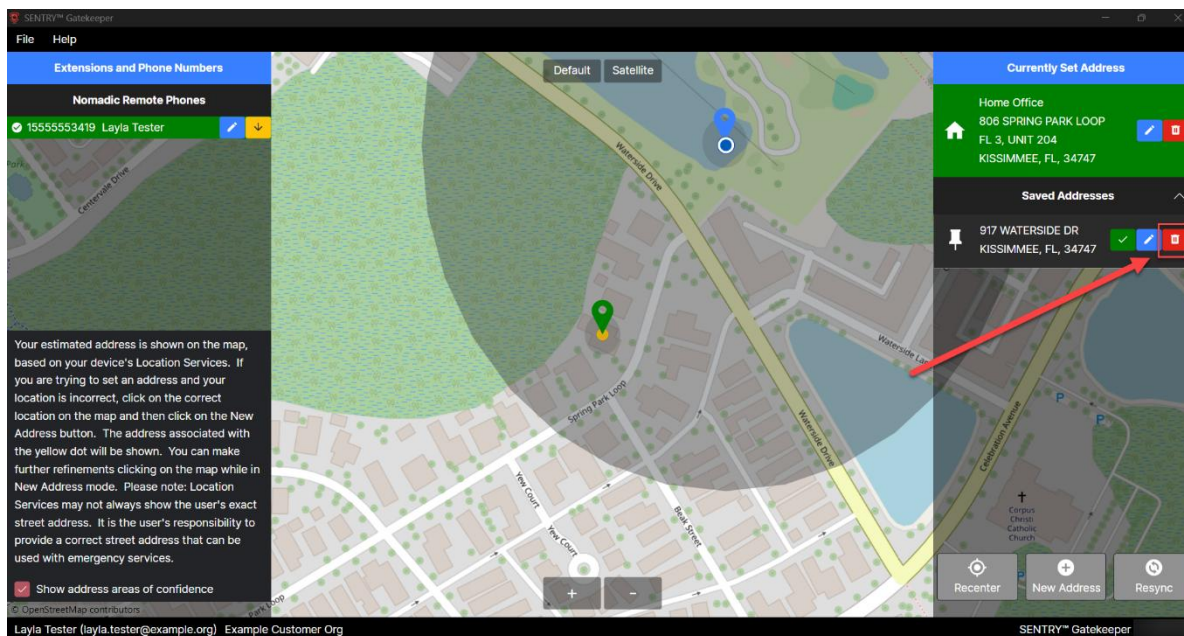


Figure 76

2. Users will be prompted to confirm with “**CONFIRM**” or “**CANCEL**”, as shown in the figure below. Click “**CONFIRM**” and the address will be deleted from SENTRY™ Gatekeeper.

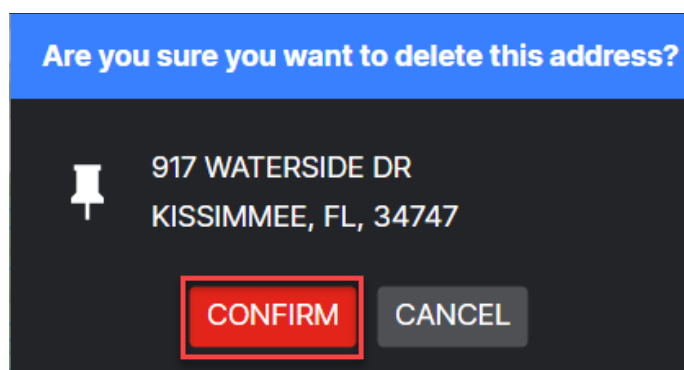


Figure 77

3. **PLEASE NOTE:** If users delete their current set address, SENTRY™ Gatekeeper will re-prompt them to set another address for their current location.

SETTING AN ON PREMISE LOCATION IN SENTRY™ GATEKEEPER – LOCATION SERVICES ENABLED (Non-VDI)

For SENTRY™ Gatekeeper users working on the premises in a dedicated office / corporate environment, they must indicate their accurate current address to remain protected. This ensures their correct location information gets outpulsed to their local serving PSAP (Public Safety Answering Point) as the time of a 911 call. The following steps cover how SENTRY™ Gatekeeper users can set the location when working on premise. **(PLEASE NOTE:** These instructions apply to a non-VDI, Location Services enabled environment.)

(PLEASE NOTE: When working on premise, SENTRY™ Gatekeeper users may see their location pin situated within a colored shape on the SENTRY™ Gatekeeper client screen map. This shape is called a Geofence. If the SENTRY™ Gatekeeper user's Accuracy ring falls within a Geofence, SENTRY™ Cloud will see the user as located within that Geofence. If the SENTRY™ Gatekeeper user does not see a Geofence, SENTRY™ Cloud will still discover the user via BSSID or IP Range. As a SENTRY™ Gatekeeper end user, do not worry about the presence (or lack thereof) of a Geofence. Geofences are managed by your Administrator.)

1. In many cases, when an on premise SENTRY™ Gatekeeper user logs in, their current accurate location will present itself automatically. SENTRY™ Gatekeeper will already have provisioned the location as well. As such, the user will see their **Currently Set Address** bar already showing entirely green and a toast message saying **"On premise office location detected, setting to: [user's on premise location]. Override. Dismiss."** will display. Users can click **"Dismiss"** or just wait for the toast message to retract. The user's location is now set.

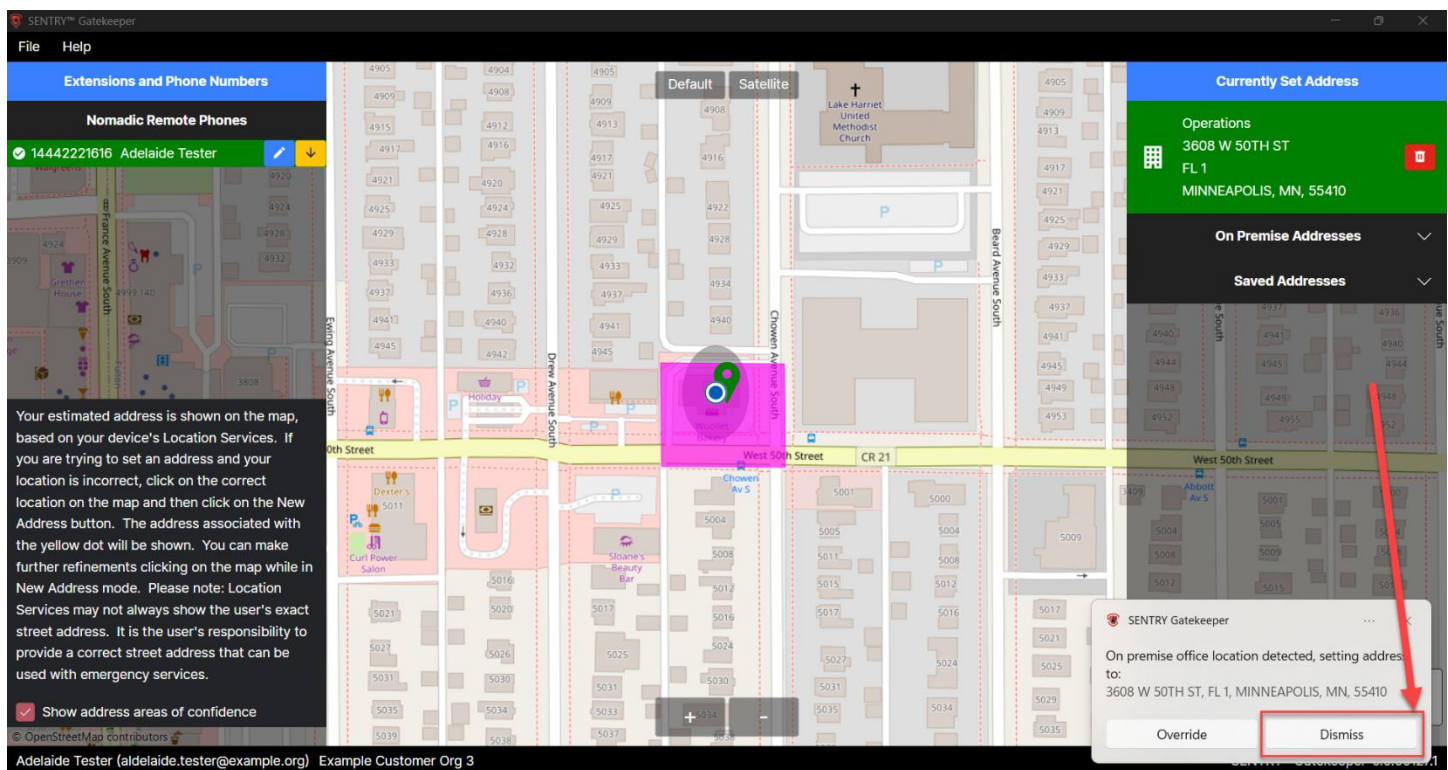


Figure 78

- In some cases, when an on premise SENTRY™ Gatekeeper user logs in, SENTRY™ Gatekeeper may present the end user with **multiple locations** to select from when setting their address (usually the same address, but with options to select from "FL1, FL 2, BLDG A", etc.). To set their location, the SENTRY™ Gatekeeper user will click the **green checkmark** for whichever option correlates to their current position within the on premise environment. (As they move around the environment, they will be prompted to re-select their location based on their updated position.)

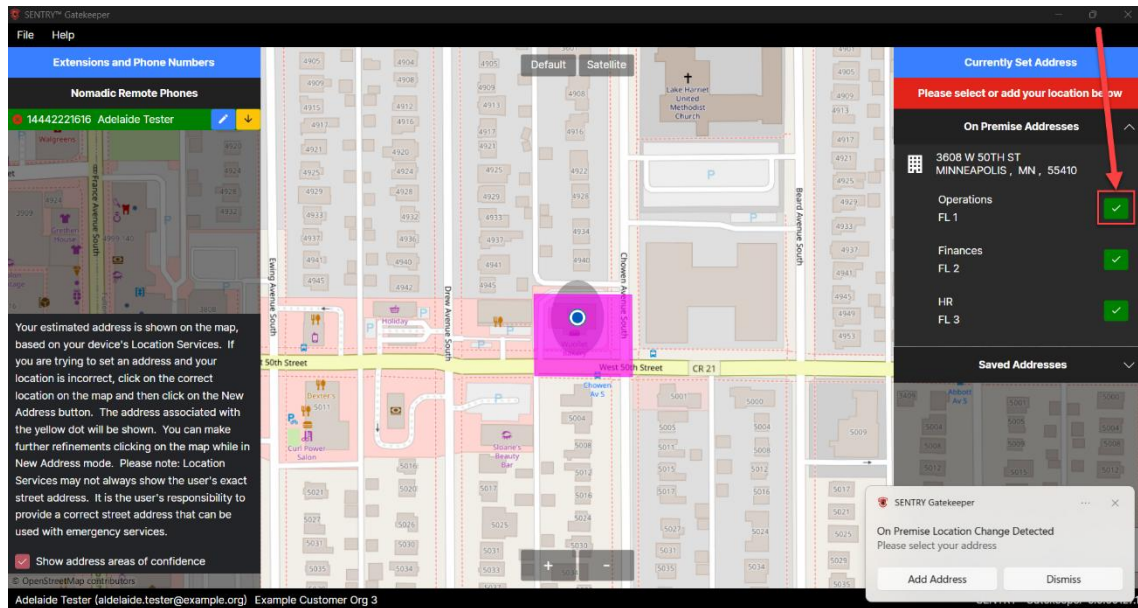


Figure 79

- Once the user clicks on their correct location option, a toast message saying **"On premise office location detected, setting address to: [user's on-premise location]. Override. Dismiss."** will display. Users can click **"Dismiss"** or wait for the message to retract / disappear. The user's location is now set.

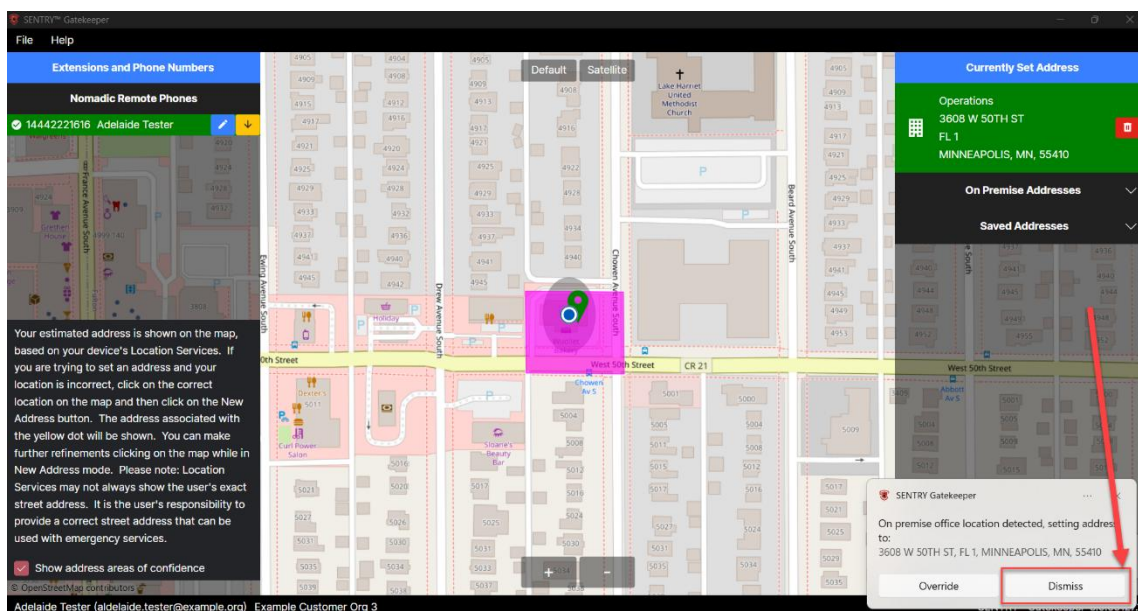


Figure 80

4. **PLEASE NOTE:** For cases where SENTRY™ Gatekeeper end users are located in their organization's on-premise environment and are being picked up by their organization's LIS (Location Information Server), the following message will display under the "Currently Set Address" column: **"Your location is being managed by your organization's 911 Location Information Service. Disregard this message if you are at an on-premise office location."** This indicates to on-prem end users that they **do not need to set an address**, as that is being managed for them by the SENTRY™ Sentinel portion of their organization's E911 solution. This statement is reflected in the **toast message** users receive as they move throughout their on-premise environment. (**PLEASE NOTE:** This applies to DLR customers that have on-premise SENTRY™ Gatekeeper users, they have SENTRY™ Sentinel as part of their solution, and also have SENTRY™ Sentinel Integration for wireless and or wired devices enabled.)

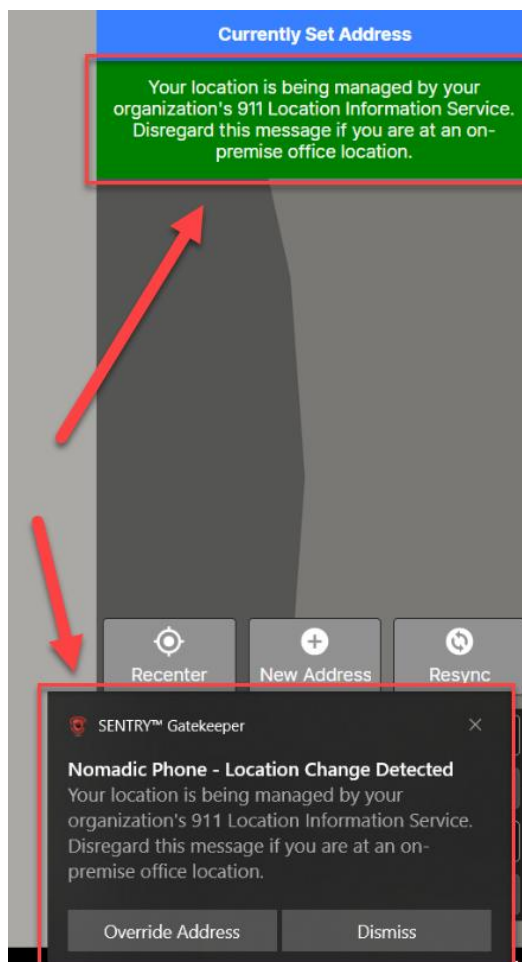


Figure 81

SETTING A LOCATION IN SENTRY™ GATEKEEPER – LOCATION SERVICES DISABLED (NON – VDI)

Whether working on-premise or remotely, some SENTRY™ Gatekeeper users belong to organizations without a VDI environment, but that do not allow for end users PCs to enable Location Services. Users from non-VDI environments with disabled Location Services can follow the guidance below for using SENTRY™ Gatekeeper.

REMOTE

For a non-VDI, no Location Services SENTRY™ Gatekeeper user working remotely and adding your address for the first time, adhere to the following instructions. Users will look to the “**Nomadic (or Static) Phone – Location Change Detected**” toast message. Users can then click “**Add Address**” to enter in their current remote location.

From the **New Address** panel, users must fill in information for the **Address Line 1**, **City**, **State**, and **Zip Code** fields. The user can select an **icon** at the top of the screen if desired, but it does not get sent to the PSAP. The user can also fill out the **Description** field to give their location a friendly name, but this will **NOT output to the PSAP**. In addition, the user can fill in the **Address Line 2** field to provide **extra information** to the PSAP, such as **floor or unit** numbers. Please note that this field has a general **20-character limit**, as some PSAPs truncate anything in this field that exceeds 20 characters. The user can also move the “**Accuracy**” slider, which will expand or shrink the **Area of Confidence** shaded circle around the user’s map pin, but this is up to the user if they would like to do this. It does **NOT** output to the PSAP. Click “**Save**” to finish setting and provisioning the location.

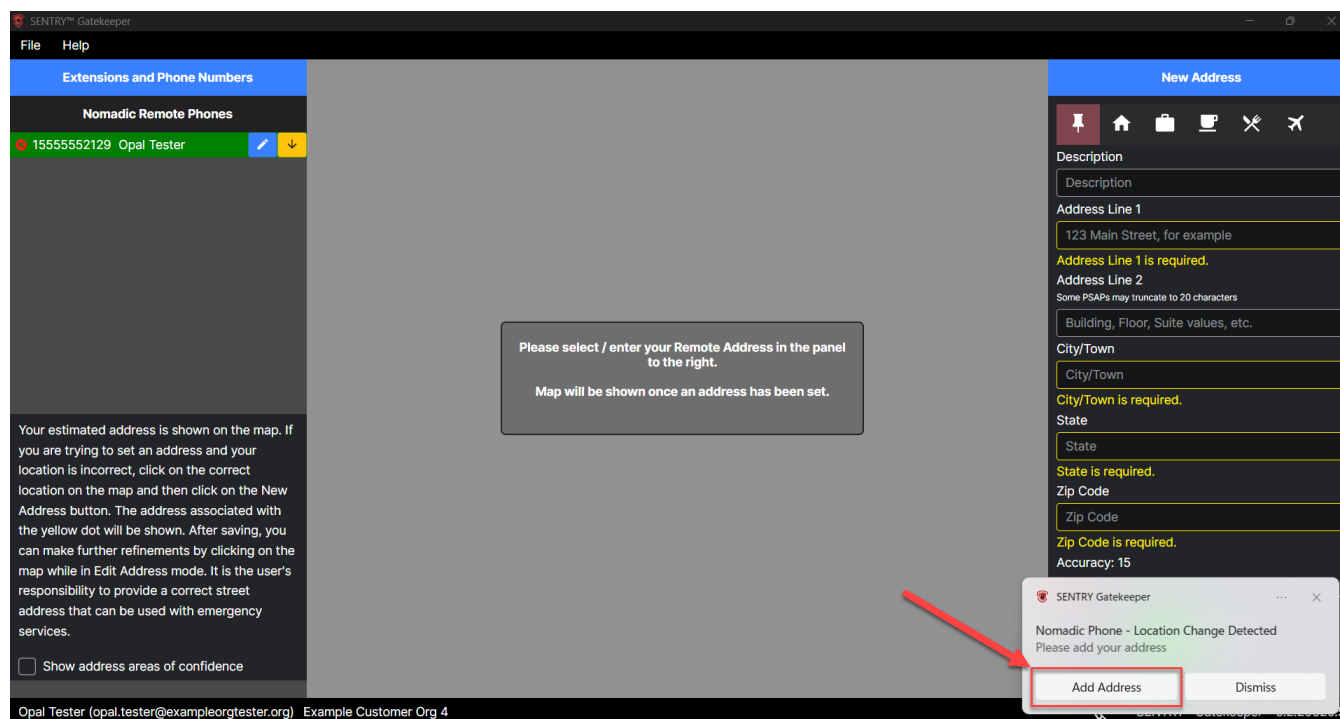


Figure 82

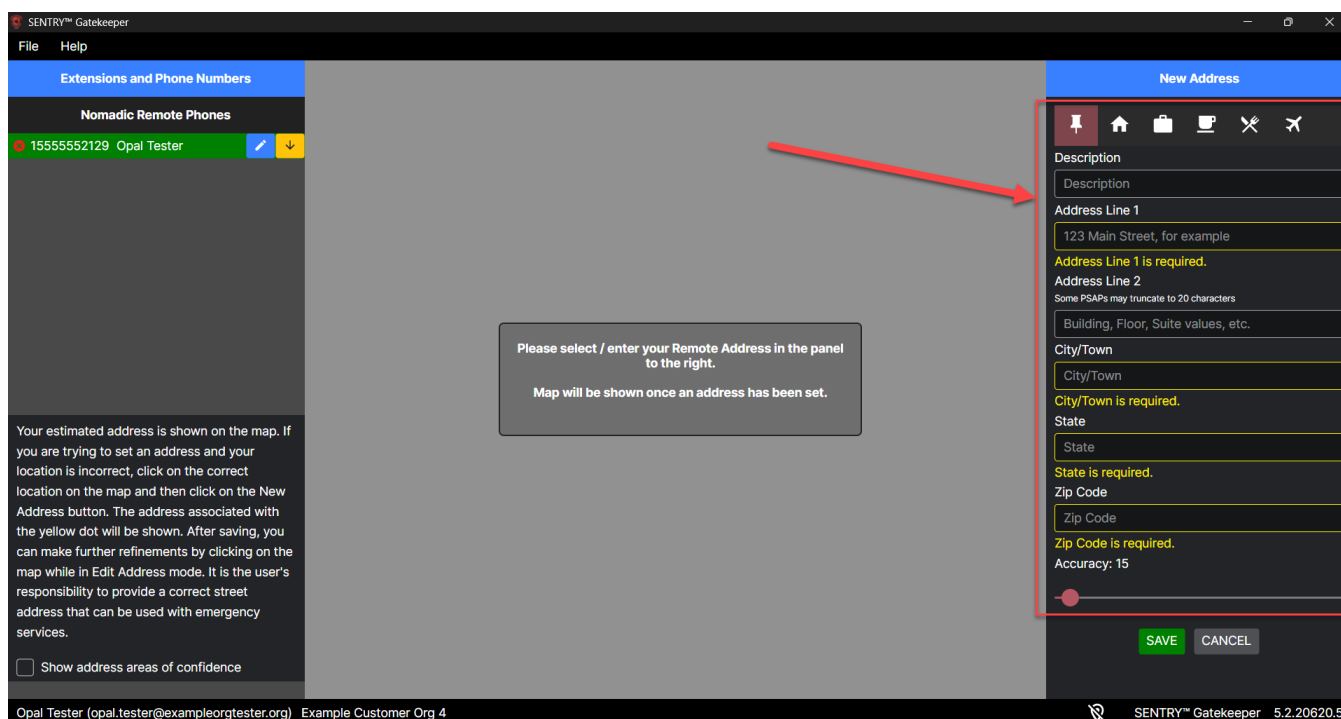


Figure 83

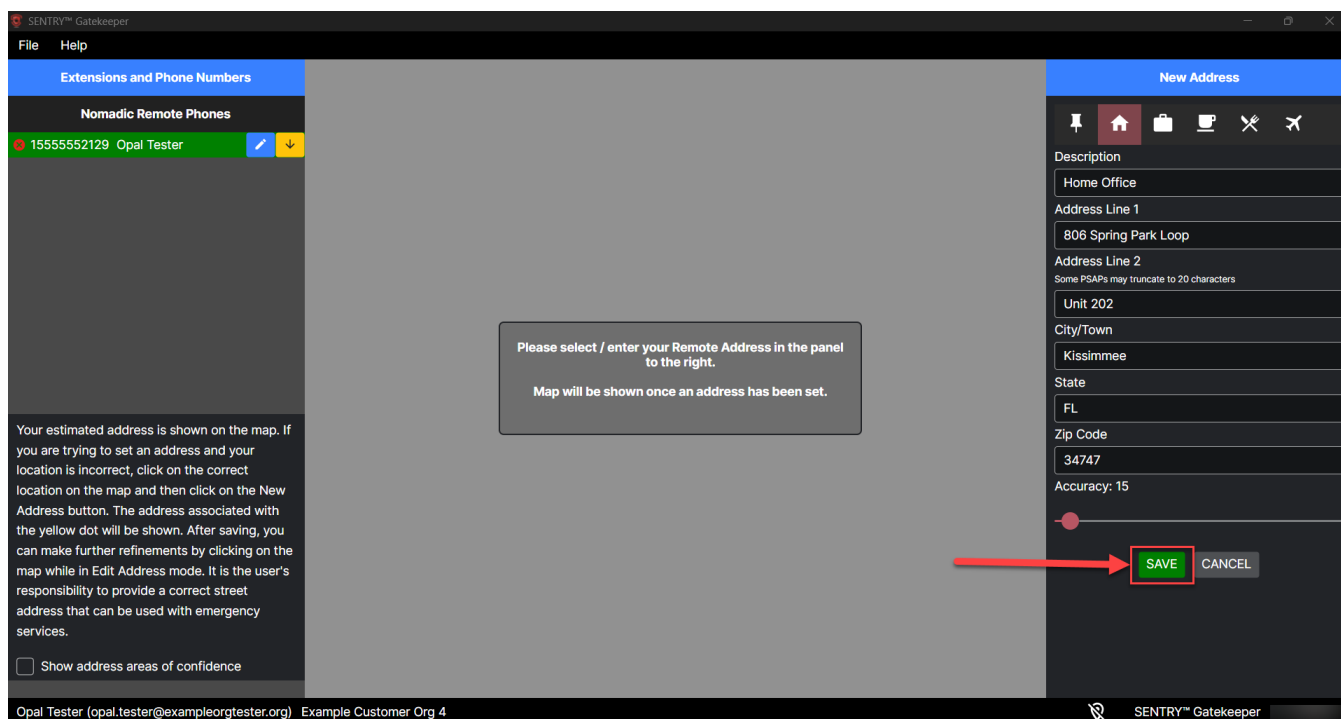


Figure 84

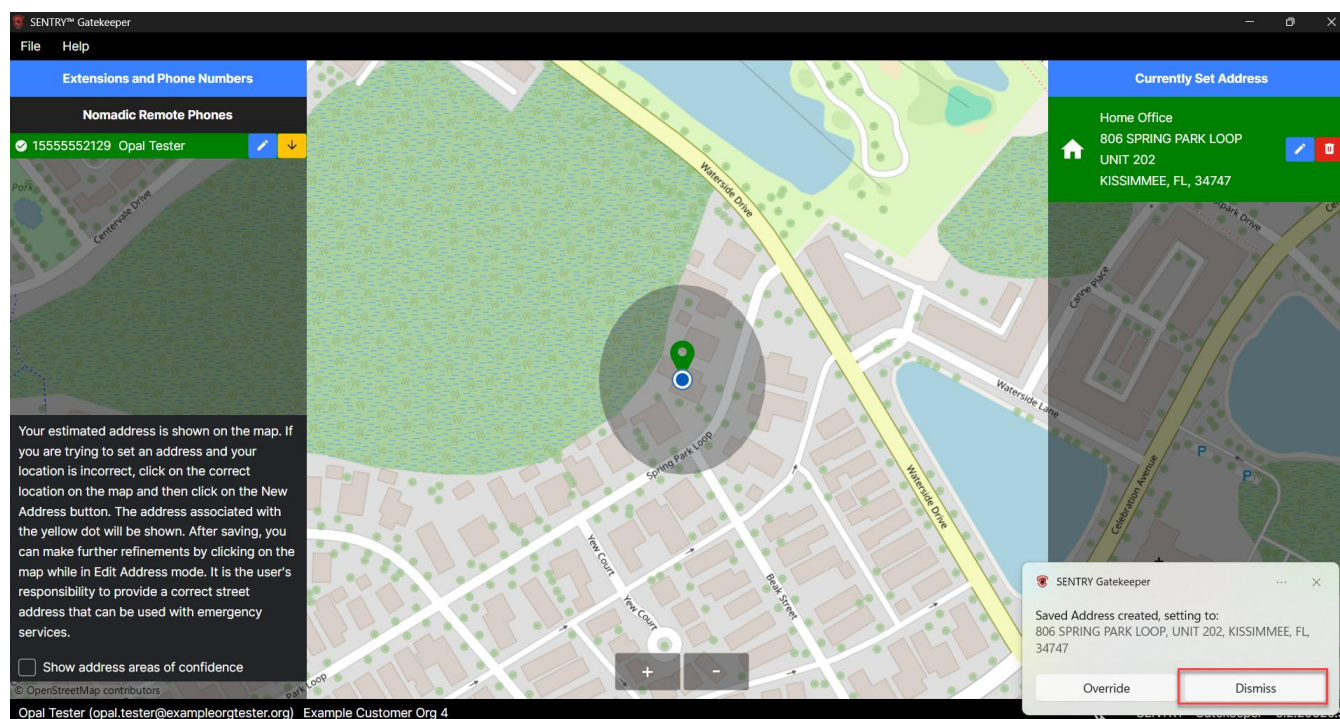


Figure 85

******PLEASE NOTE: A No Location Services SENTRY™ Gatekeeper user is responsible for updating their location whenever they move around, whether that be from one floor to another in the same building, or to a new building / site entirely. If a VDI-supported, No Location Services SENTRY™ Gatekeeper user moves to a new remote location throughout the day (from a home office to a coffee shop, for example), SENTRY™ Gatekeeper cannot detect that movement. As such, SENTRY™ Gatekeeper will not deprovision a user’s set address once they provision it. As such, the SENTRY™ Gatekeeper end user is responsible for updating their set address whenever they change locations. The user can do so using either the “Override” or “+New Address” method as desired.**

Upon startup, the last provisioned location will still be provisioned, but SENTRY™ Gatekeeper will provide the user with a toast message allowing the user to click “Override” and set a new address or click “x” or “Dismiss”, then use the “+New Address” button to set a new address.

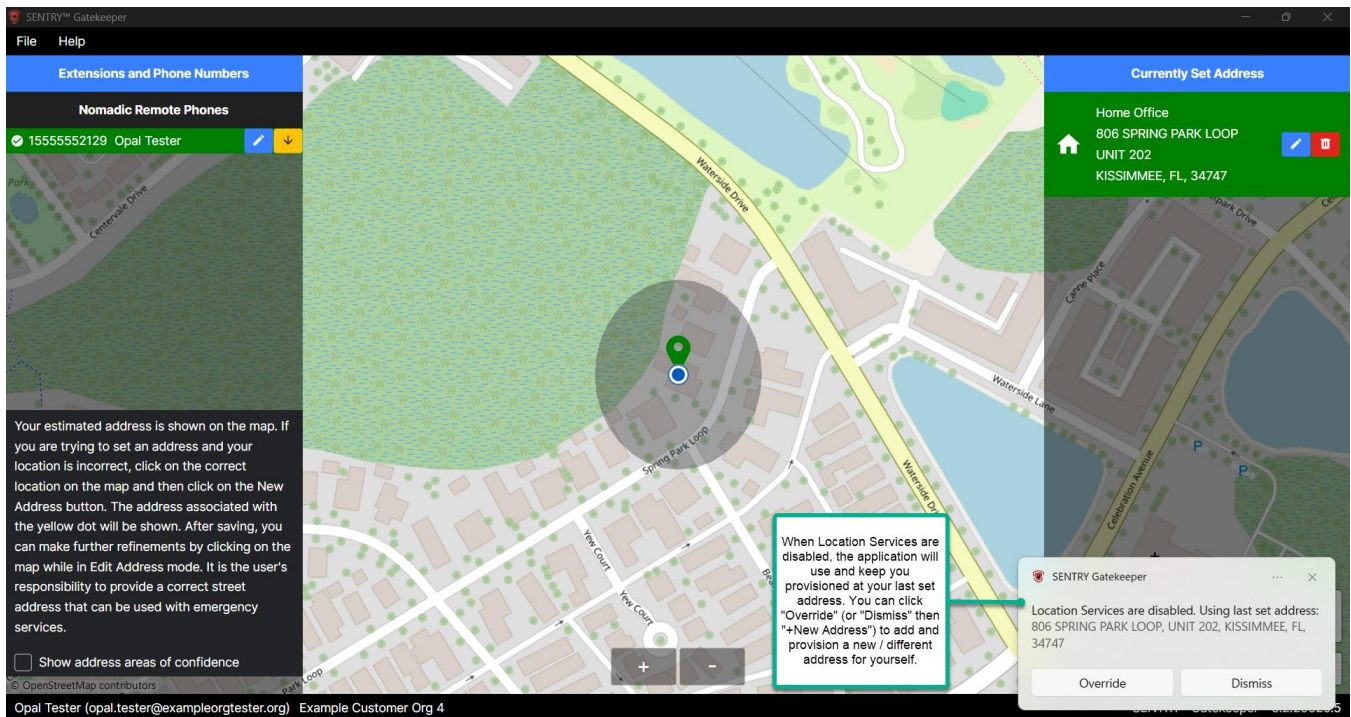


Figure 86



Figure 87

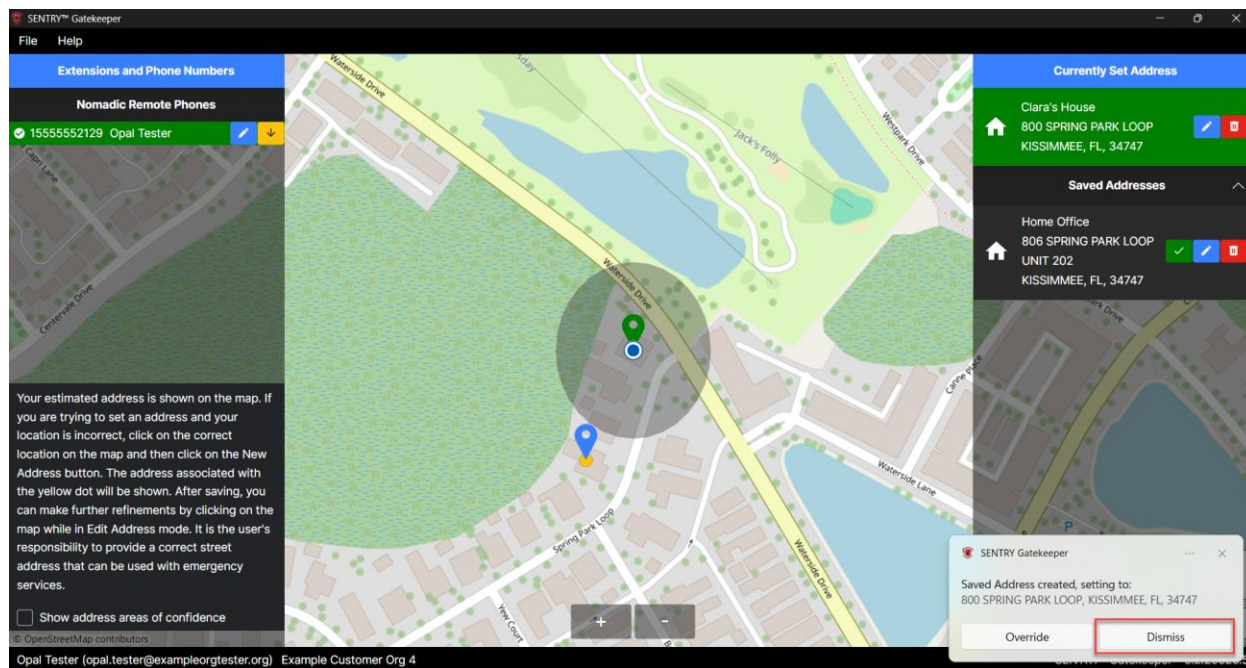


Figure 88

Once provisioned, the address will remain so until the user provisions a new or different location. **PLEASE NOTE:** Users can make use of the **Saved Addresses** list to re-provision themselves at a commonly frequented location. Users can use the **" +New Address"** button to create additional addresses to choose from. From the Saved Addresses list, users can click the **green checkmark** for whichever option applies to their current whereabouts to provision and update their location.

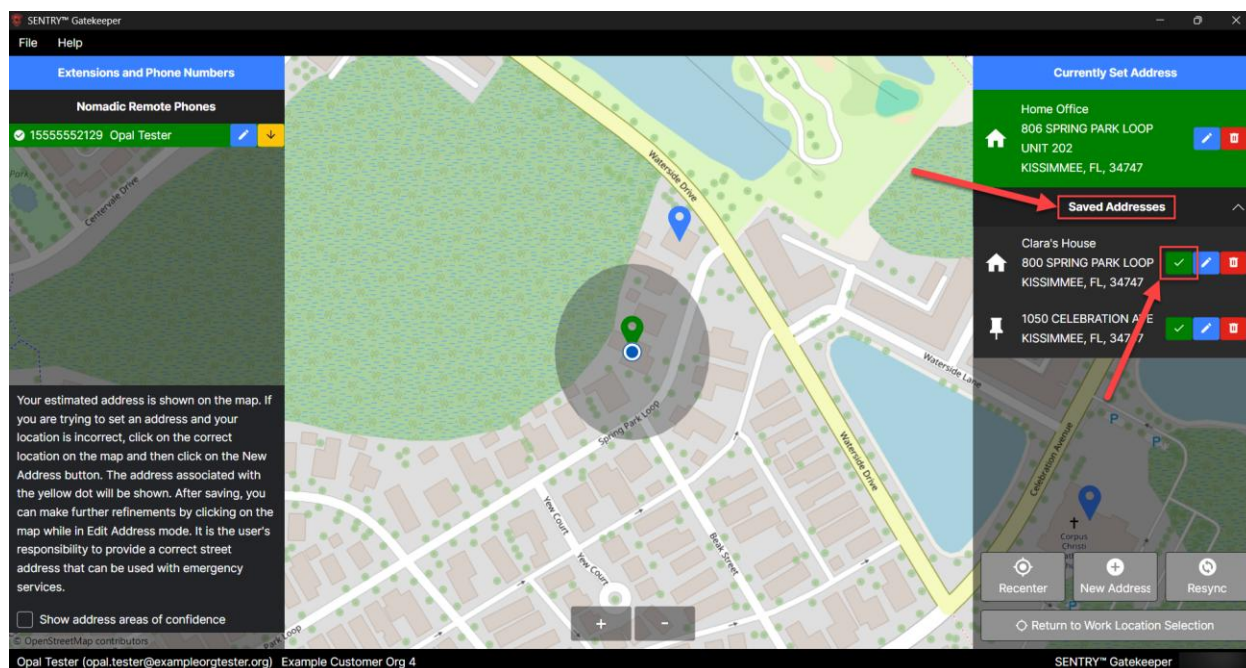


Figure 89

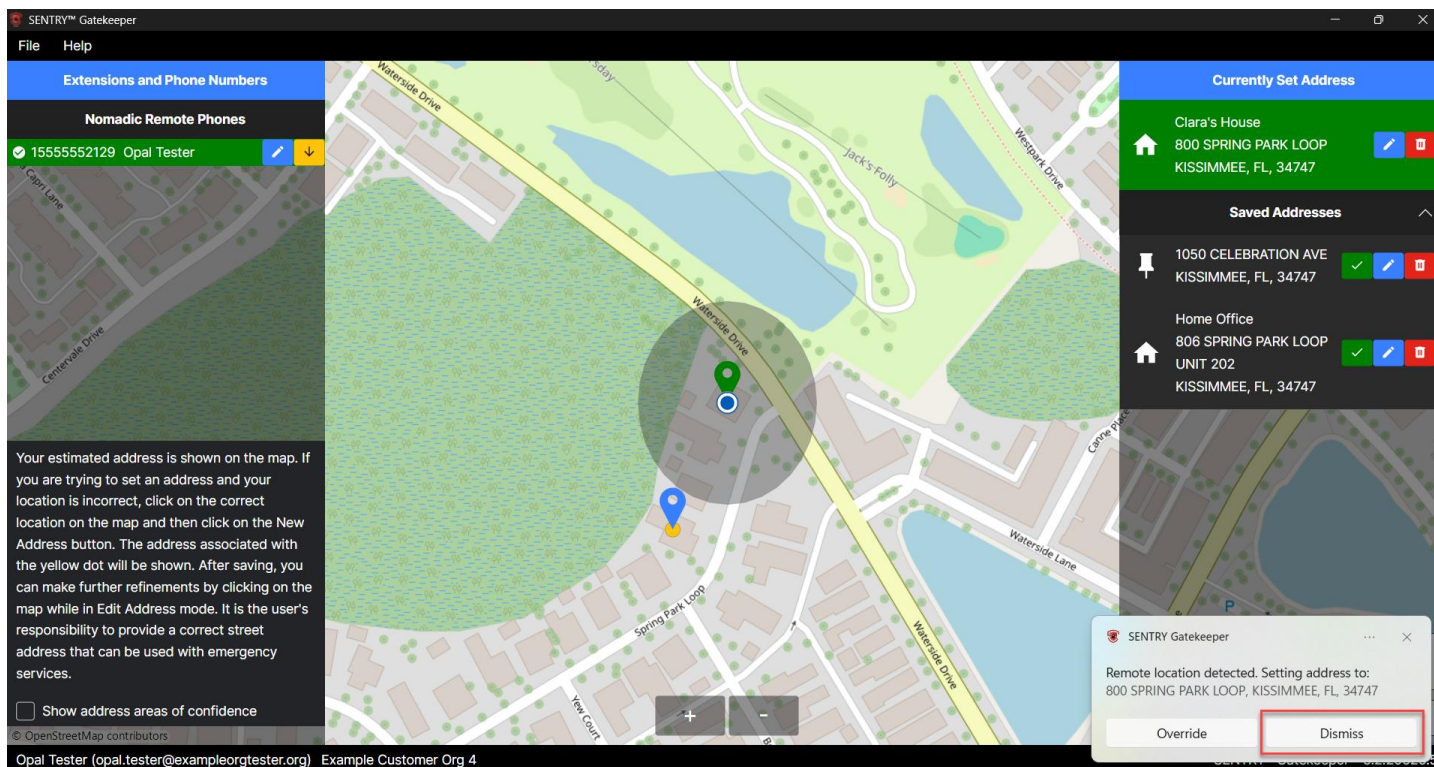


Figure 90

ON-PREMISE

For a non-VDI, no Location Services SENTRY™ Gatekeeper user working on-premise, the user's approach to setting their address will depend on whether their organization uses SENTRY™ Cloud Discovery (specifically via BSSIDs – IP Ranges will not work with a non-VDI, no Location Services setup). If a user's organization does NOT use SENTRY™ Cloud Discovery, then users would follow the same instructions outlined in the previous ["Remote"](#) section of this document, but instead of provisioning home or other remote addresses, they would provision their appropriate work address. If the user's organization DOES use SENTRY™ Cloud Discovery (specifically via BSSIDs), see the details below. (**PLEASE NOTE:** Even if customer organizations are using SENTRY™ Cloud Discovery with BSSIDs, the discovery may not work 100% of the time with Location Services disabled. End user experience may vary depending on if they are on Windows 10 versus Windows 11. See below for further details.)

If the SENTRY™ Gatekeeper application is unable to find the user via their BSSID, then when logging in for the first time, non-VDI and no Location Services users will see a **Work Location** box display like the one below when they first sign in. The end user can **select the name / title of their correct building, site, etc. from the text box presented** to them. The toast message stating **"Nomadic (or Static) Phone – Location Change Detected"** will also appear, with options to **"Add Address"** or **"Dismiss"**. The end user can either **ignore** this message or click **"Dismiss"** to get rid of the toast message. (Only VDI users working remotely instead on on-premise would click **"Add Address"** instead of ignoring or dismissing the message.) Once the user clicks on the correct building, site, etc., they can click **"Confirm Selection"**. **PLEASE NOTE:** No map view will display until the user selects their building / site and then clicks **"Confirm Selection"**. Once the user confirms their building / site selection, they will select the correct location within that building / site from the **On Premise Addresses** list on the right-hand side of the SENTRY™ Gatekeeper client window. Users will click the **green checkmark** to **finish setting and officially provision their address** and location within SENTRY™ Gatekeeper. In addition, once users

have provisioned their address location, they may click **“Dismiss”** on the SENTRY™ Gatekeeper toast message in the lower right-hand corner stating, **“Location Services are disabled. Using last set address: [address here] – Override – Dismiss”**.

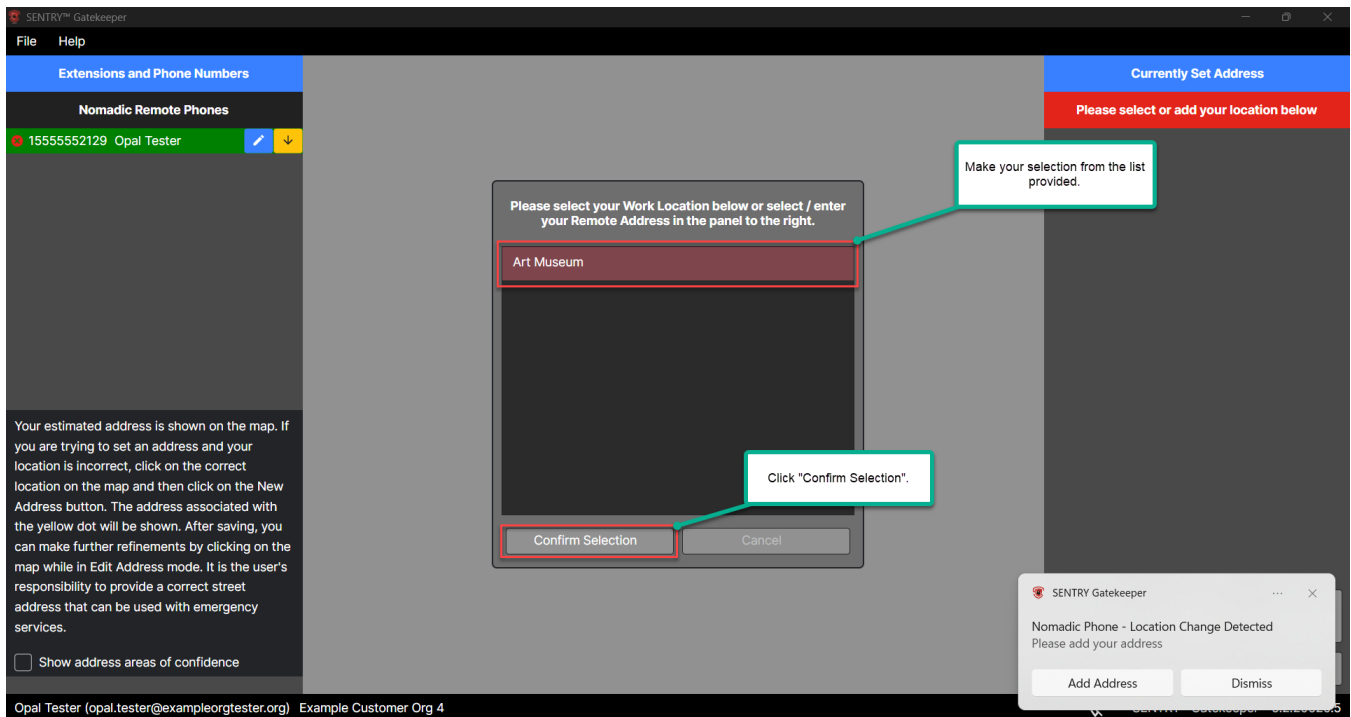


Figure 91

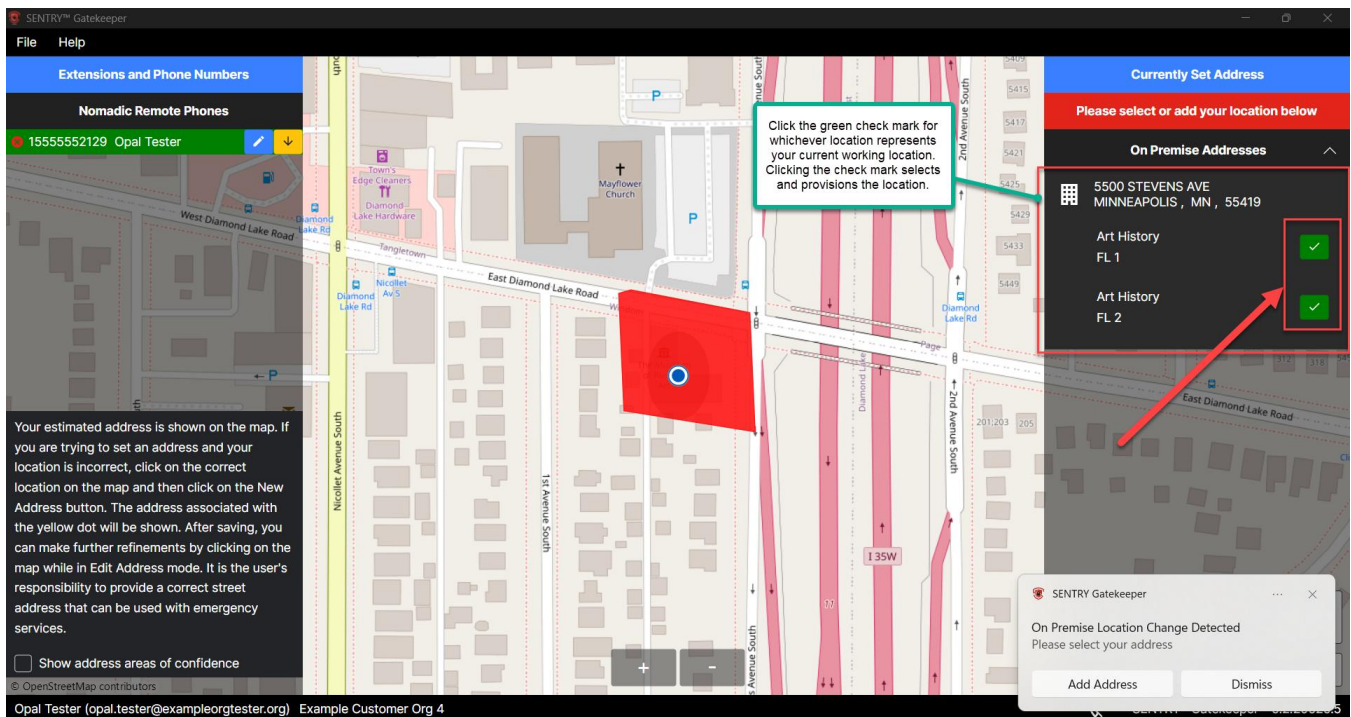


Figure 92

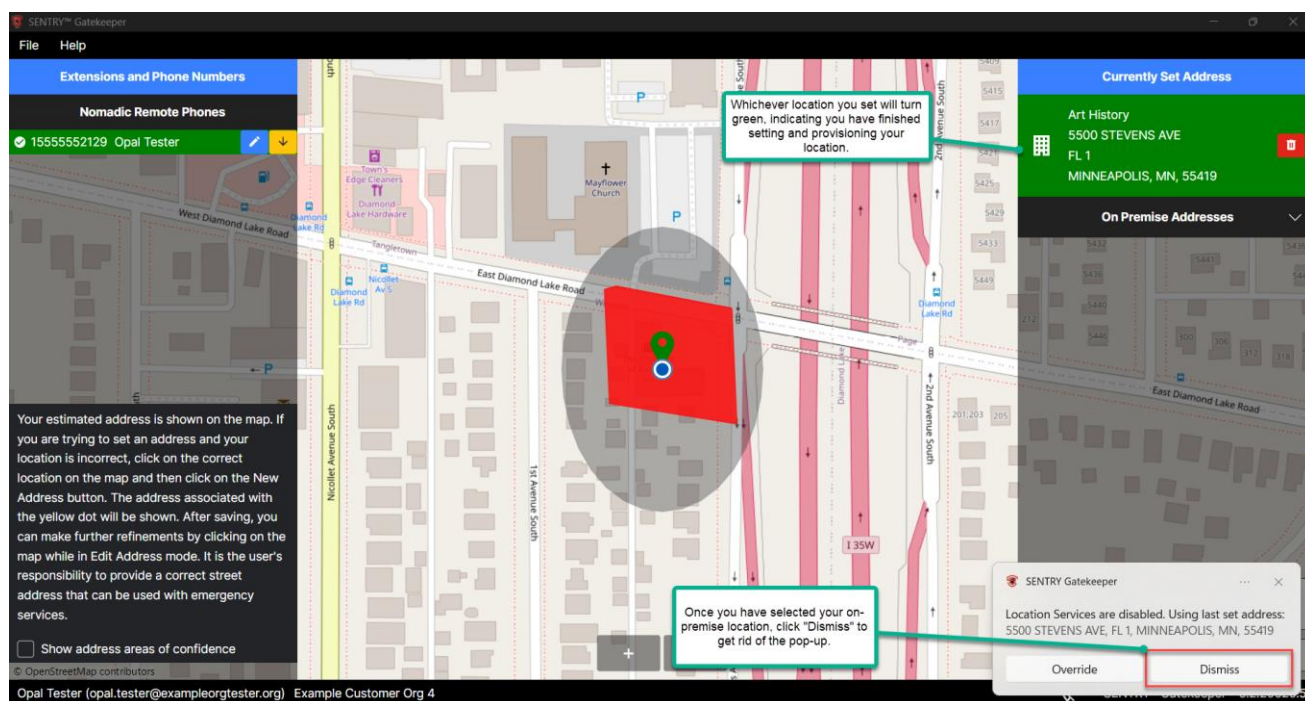


Figure 93

Upon next startup SENTRY™ Gatekeeper will have kept the user's last provisioned location as such UNLESS it can detect a change in the user's BSSID. If SENTRY™ Gatekeeper **CAN** detect a change in the user's **BSSID**, and the BSSID is one defined in SENTRY™ Cloud and associated to a defined Location, then SENTRY™ Gatekeeper will assign that Location as the user's address.

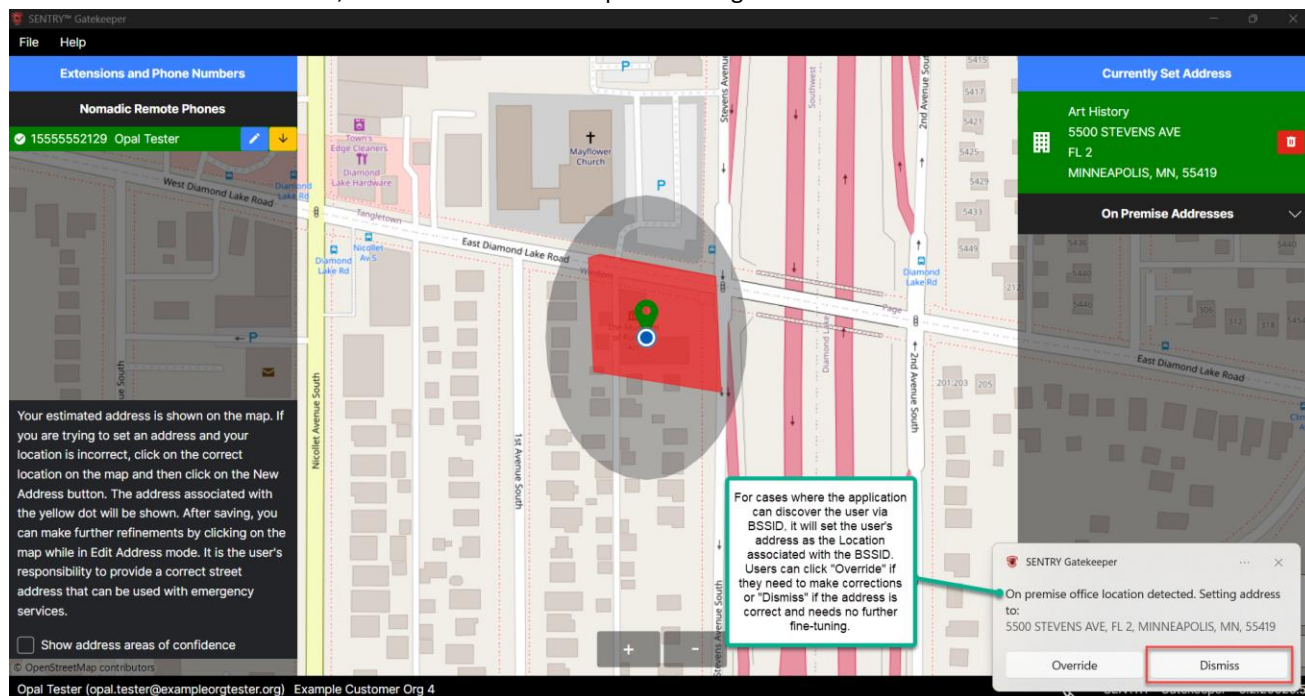


Figure 94

If SENTRY™ Gatekeeper **CANNOT** detect the user's **BSSID**, then it is up to the user to report any change in their address by clicking the **On Premise Addresses** list. Users can choose the correct on-premise address then click the **green check mark** of whichever granular option applies to where they moved (for example, a first-floor option, a second-floor option, etc.). Clicking the green checkmark will **update and provision their set address** to their new in-office location. This option will likely be the most convenient for the end user. Users could also click "Override" and provision their updated address manually. All of this information also applies to users moving around within their on-premise environment, not just for use cases where the user is starting up the application.

*****PLEASE NOTE:** The SENTRY™ Gatekeeper end user is responsible for updating their set address whenever they move throughout their workplace.

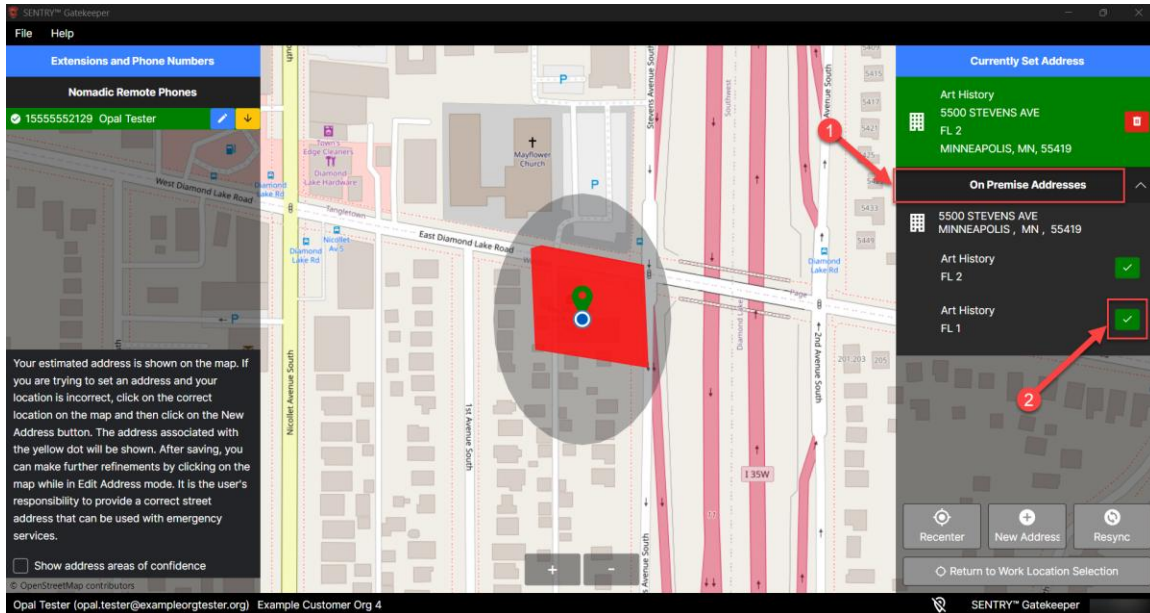


Figure 95

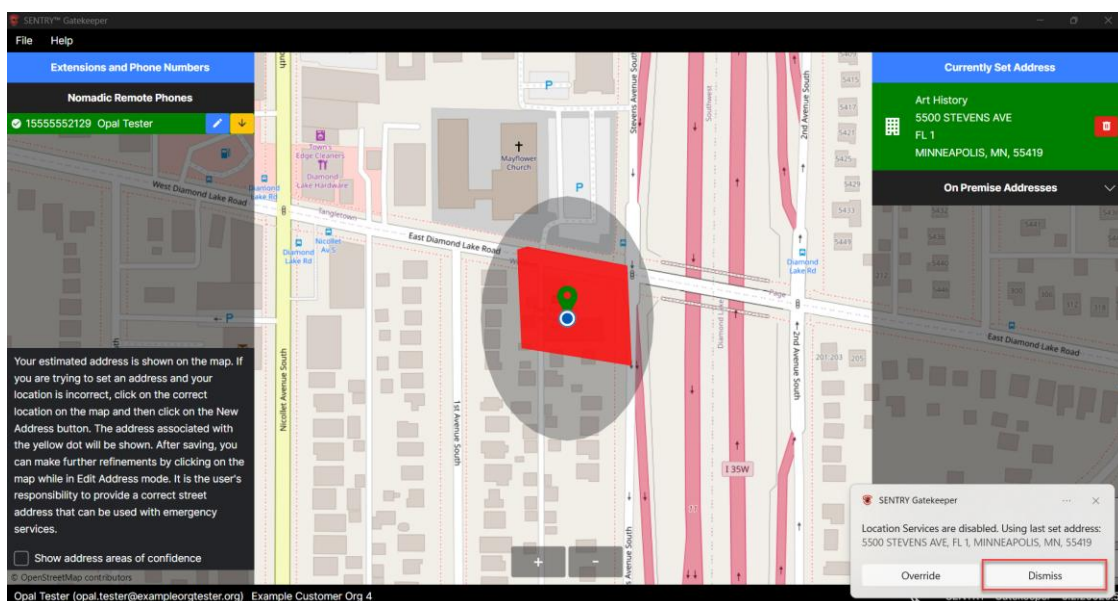


Figure 96

OTHER SENTRY™ GATEKEEPER FEATURES

1. SENTRY™ Gatekeeper users can select their map view to portray either a **Street** view or a **Satellite** view depending on their preference.

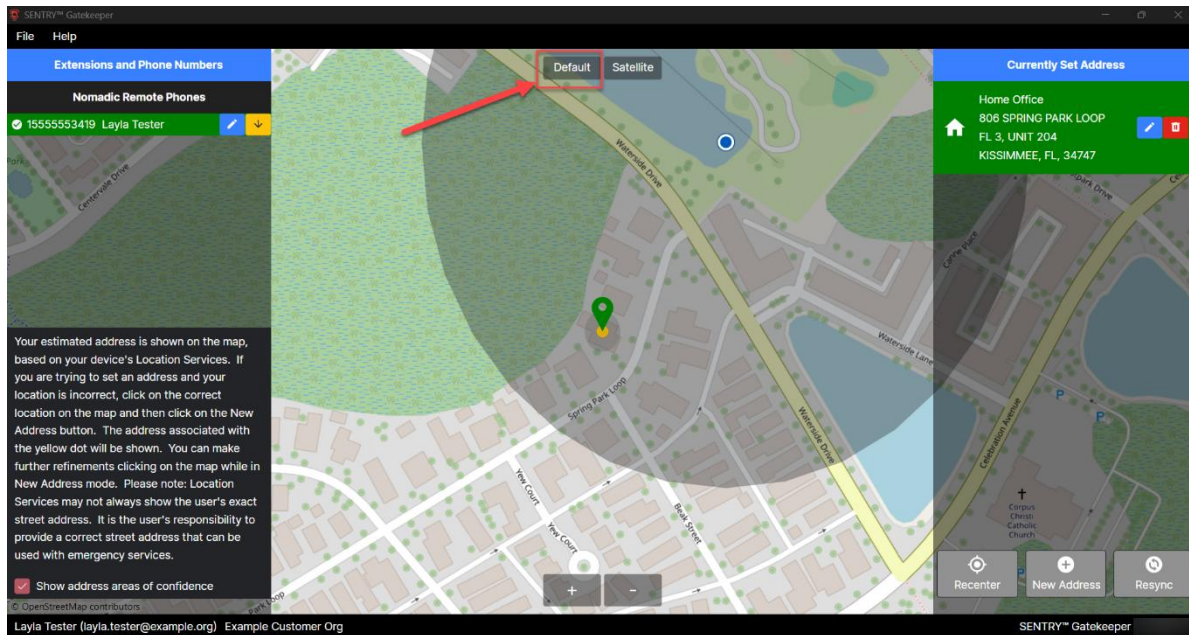


Figure 97

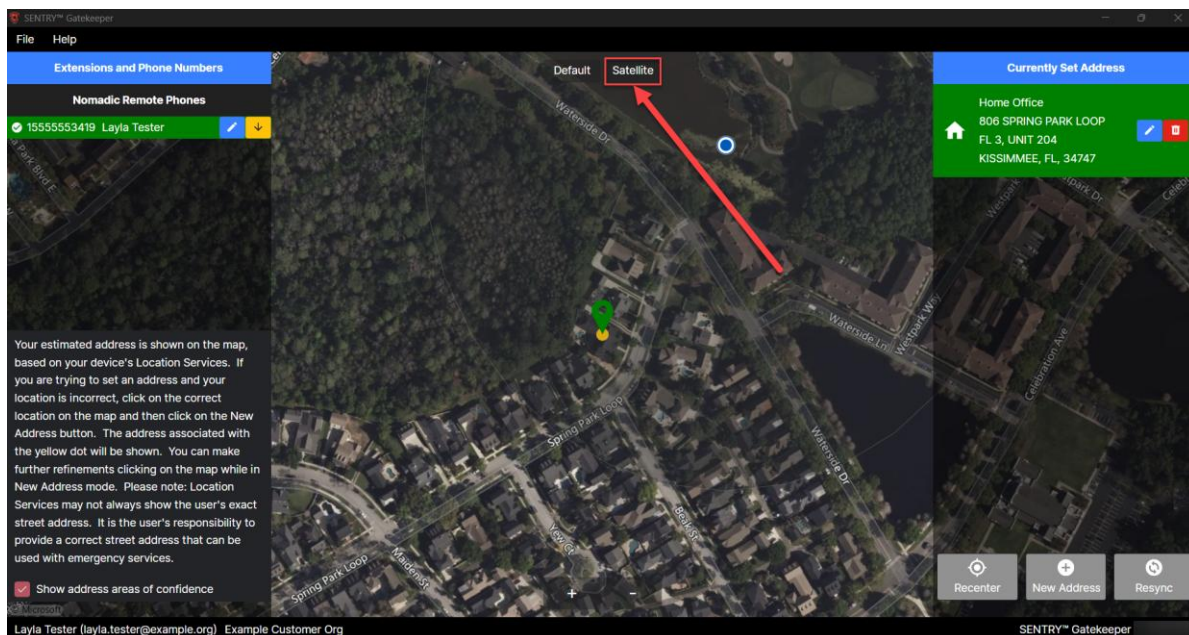


Figure 98

2. SENTRY™ Gatekeeper users can **center the map view** on their current location (as determined by their PC's **Location Services**), by clicking on the **target icon** / **"Recenter"** button in the lower right-hand corner of the SENTRY™ Gatekeeper client screen.

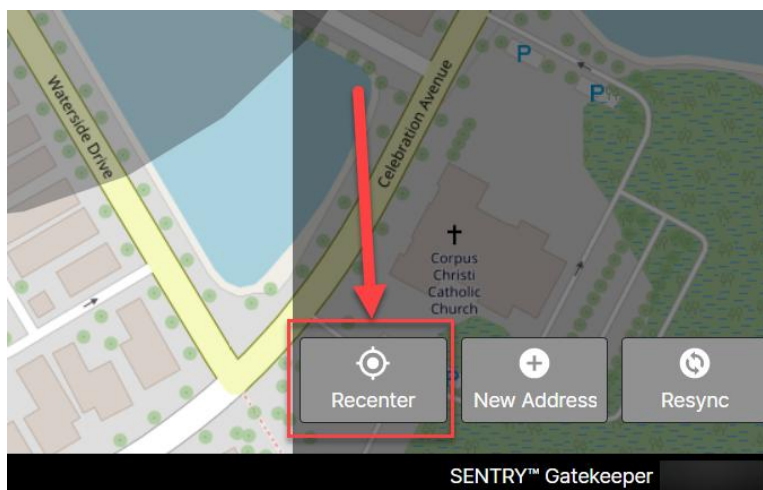


Figure 99

3. A SENTRY™ Gatekeeper user can manually fine-tune their estimated address by clicking on the map and using the **"New Address"** button featured in the lower right-hand corner of the SENTRY™ Gatekeeper client screen. For further details, see the ["Editing an Address in SENTRY™ Gatekeeper"](#) section of this document.

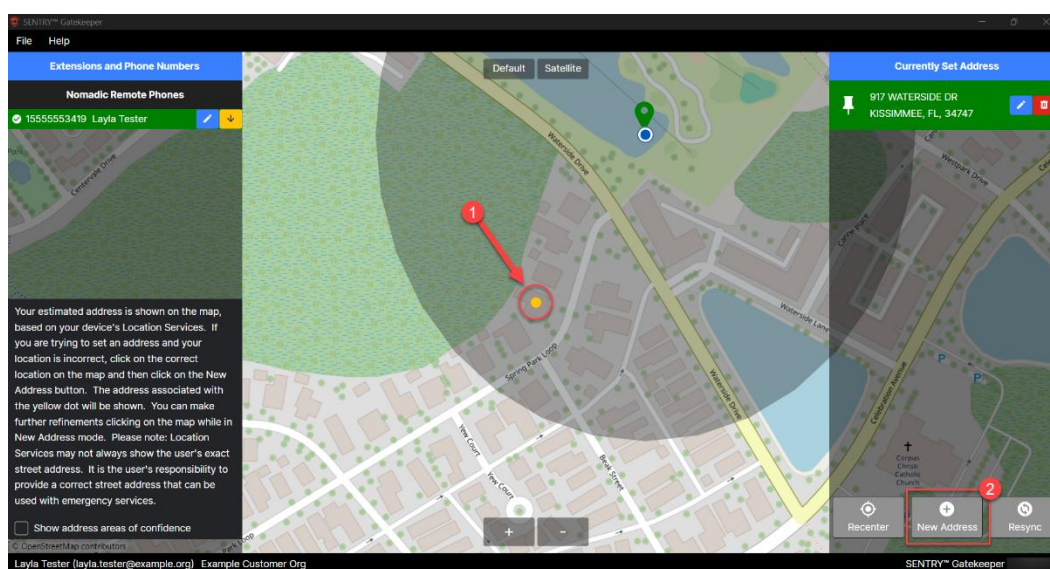


Figure 100

4. To refresh and resync the SENTRY™ Gatekeeper application, click the **“Resync”** button in the lower right-hand corner of the SENTRY™ Gatekeeper client screen.

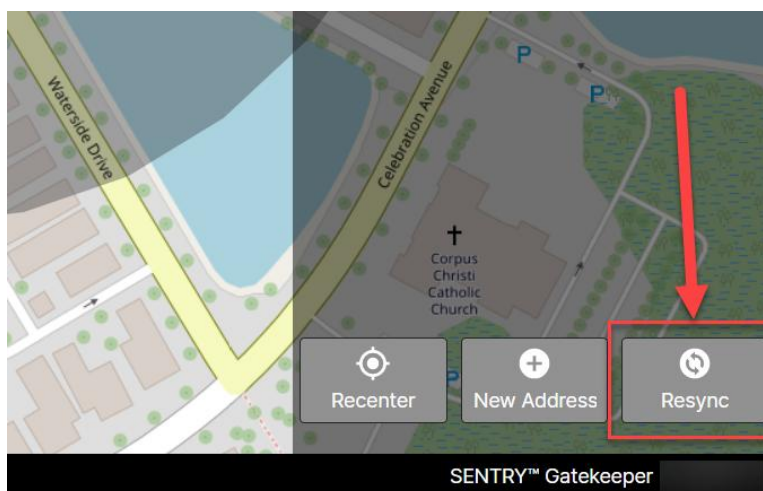


Figure 101

5. To log out of the SENTRY™ Gatekeeper application but not fully exit out and close the client window, click on **File > Log Out**. SENTRY™ Gatekeeper will present the user with a message reading, **"Are you sure you want to sign out? If you do and change locations, Emergency services will not be able to find you."** Click **“Yes”** to sign out or **“No”** to cancel.

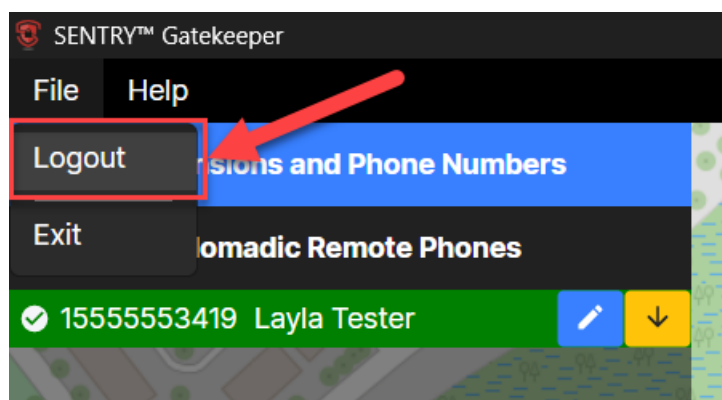


Figure 102

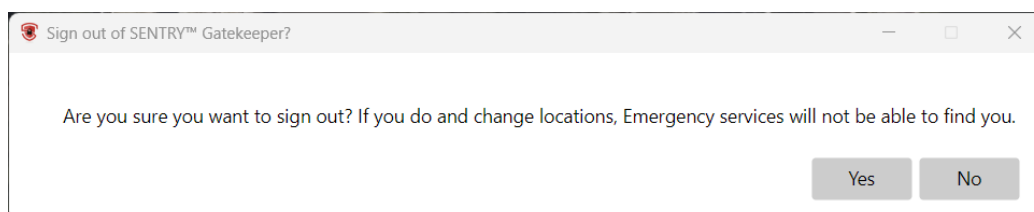


Figure 103

- To fully exit and quit out of the SENTRY™ Gatekeeper application, click on **File > Exit**. SENTRY™ Gatekeeper will present the user with a message reading, "Are you sure you want to exit? If you do and change locations, Emergency services will not be able to find you." Click "Yes" to exit out of the application or "No" to cancel.

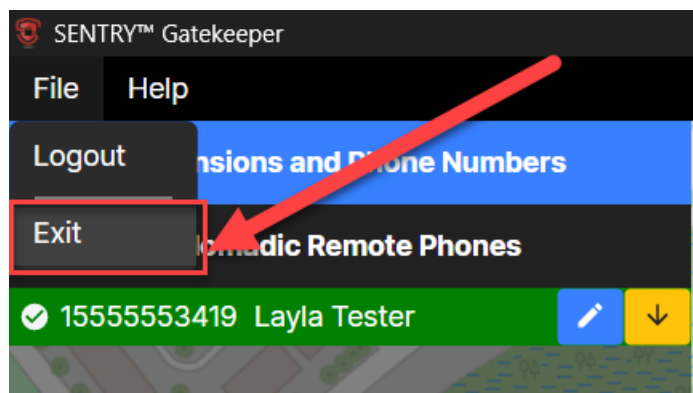


Figure 104

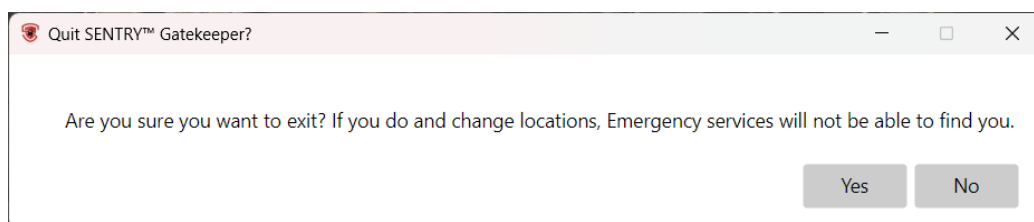


Figure 105

- Clicking on **Help > About** will result in a pop-up informational window (shown next page) displaying the official SENTRY™ Gatekeeper and 911 Secure logo along with the version number of the user's SENTRY™ Gatekeeper client, a link to the official 911 Secure website, and a copyright statement. Click the "x" button in the upper right-hand corner of the window to close it.

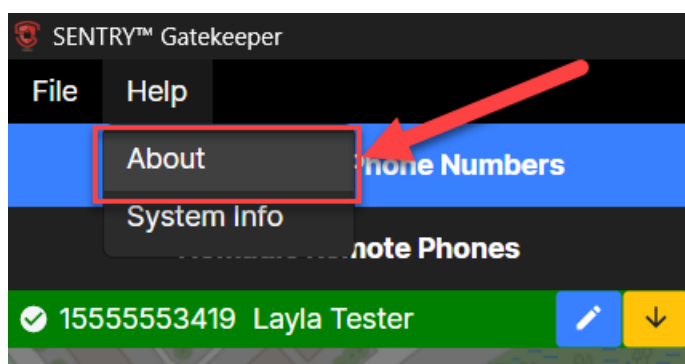


Figure 106



Figure 107

8. Clicking on **Help > System Info** will provide a snapshot of information about your device, including latitude and longitude details, the BSSID of your device, your IP Address, your device's connection type, and the area of accuracy of your Location Services. It can also show you the System Info for your last SENTRY™ Gatekeeper client and the System Info of the last time your device was discovered by SENTRY™ Cloud (pertinent only to those customers using a SENTRY™ Cloud Discovery setup). SENTRY™ Gatekeeper users will not need to reference this information often, if ever. 911 Secure Support personnel may ask for it for troubleshooting purposes.

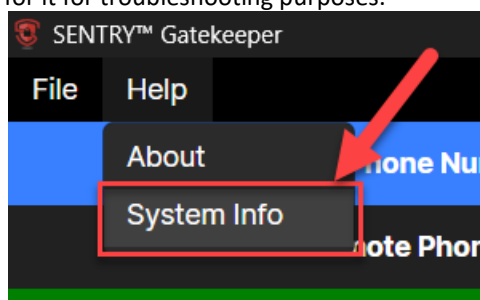


Figure 108

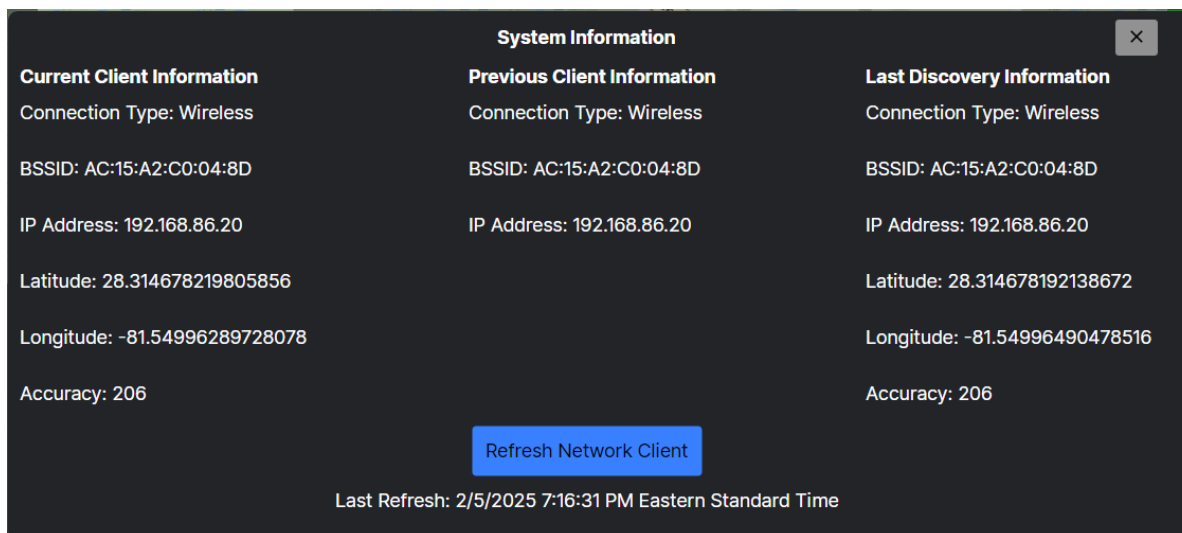


Figure 109

9. Click the **minimize button** to minimize the SENTRY™ Gatekeeper client window. Click the **minimize / maximize button** to shrink or expand the client window. Click the “x” button to **minimize** the SENTRY™ Gatekeeper application to the user’s **PC’s tray**. Open the tray and click the SENTRY™ Gatekeeper icon to bring the client window back up. Clicking the “x” does NOT exit the user out of the application. For that, the user must click File > Exit.

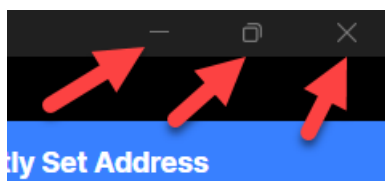


Figure 110

SENTRY™ GATEKEEPER v5.6 USER'S GUIDE – VDI ENABLED

Some SENTRY™ Gatekeeper customer organizations require support for VDI environments. Having a **VDI (or Virtual Desktop Infrastructure)** environment allows organizations to deliver desktops to their users, especially in the contact center space. Instead of applications running locally on a user's physical device, customers may instead "Remote control" a user's desktop instance hosted in a datacenter. With this type of environment, users can either connect from a standard PC with a full operating system or use a "dumb terminal" such as a Wyse terminal. A "dumb terminal" connects to the VDI server, but no applications are installed on the system. In most cases, multiple users have the same VDI "image" with all approved applications and associated configurations applied by an administrator. When a customer requires support for a VDI environment, **SENTRY™ Gatekeeper will not use a SENTRY™ Gatekeeper user's IP address, BSSID, or MAC address for the purpose of location discovery**, since only the customer's datacenter or cloud IP, BSSID, and or MAC address would present itself, not the end user's information. SENTRY™ Gatekeeper users that are part of a VDI environment must be flagged for VDI support, either via **client installation** (manual or silent installation), **organization settings** in SENTRY™ Cloud (set by a SENTRY™ Cloud Administrator), or by a **Windows registry / group policy**.

In addition, some customers do not allow enabling each SENTRY™ Gatekeeper end user's Location Services. In such "**No Location Services**" cases, SENTRY™ Gatekeeper v5.6 can support these customers. With Location Services disabled, SENTRY™ Gatekeeper will **not** use an end user's **Location Services** for **location discovery**.

DEFINITIONS

- **VDI – Virtual Desktop Infrastructure.** VDI is a software tool which allows users to access their organization's computer systems from any device with an internet connection. VDI operates by creating virtual desktops on a central server, which users access remotely. With the use of a remote display protocol, a VDI environment lets end users gain remote access to virtual desktops on a central server.
- **VDI Enabled** – An attribute assigned to a SENTRY™ Gatekeeper client possessing a VDI support "flag", which is set during installation or by the customer organization's existing Windows registry / group policy.
- **VDI Flag** – An indicator set for a SENTRY™ Gatekeeper client during installation (via either individual manual installation or via a script for silent installation) or set by a customer organization's existing Windows registry / group policy. To clarify, administrators can apply this VDI flag to their SENTRY™ Gatekeeper end users either through their SENTRY™ Cloud organization settings, through the SENTRY™ Gatekeeper configuration (manual or scripted silent installation), or through Windows registry settings. Whichever one is configured last wins and takes overriding precedence.
- **Windows Registry / Group Policy** – A database storing configuration settings for a customer organization's Windows operating system and applications that use it. In addition, the Windows registry / group policy can also act as a feature that allows administrators to manage and configure the settings for users and computers in a Microsoft Active Directory (AD) environment. By either definition, the Windows registry / group policy can act as a method for assigning the VDI Enabled attribute / VDI "flag" to SENTRY™ Gatekeeper clients.
- **No Locations Services** – A use case where SENTRY™ Gatekeeper cannot rely on an end user's latitude and longitude coordinates provided by their PC's Location Services for the purposes of location identification.

ENABLING VDI SUPPORT FOR SENTRY™ GATEKEEPER

As mentioned in the previous section, there are three ways to enable VDI support for SENTRY™ Gatekeeper users. See below for details.

CLIENT INSTALLATION

MANUAL INSTALLATION

When installing SENTRY™ Gatekeeper manually, an install screen will display saying, ***“Please enable this setting if Gatekeeper is being installed in a Virtual Desktop Infrastructure environment. If unsure, rely on the group policy registry setting”***. That same screen will then ask ***“Enable Vdi?”***, to which the user can select ***“Yes”***, ***“No”***, or ***“Rely on Group Policy/Organization Settings”***.

Selecting ***“Yes”*** will enable VDI support for the SENTRY™ Gatekeeper client.

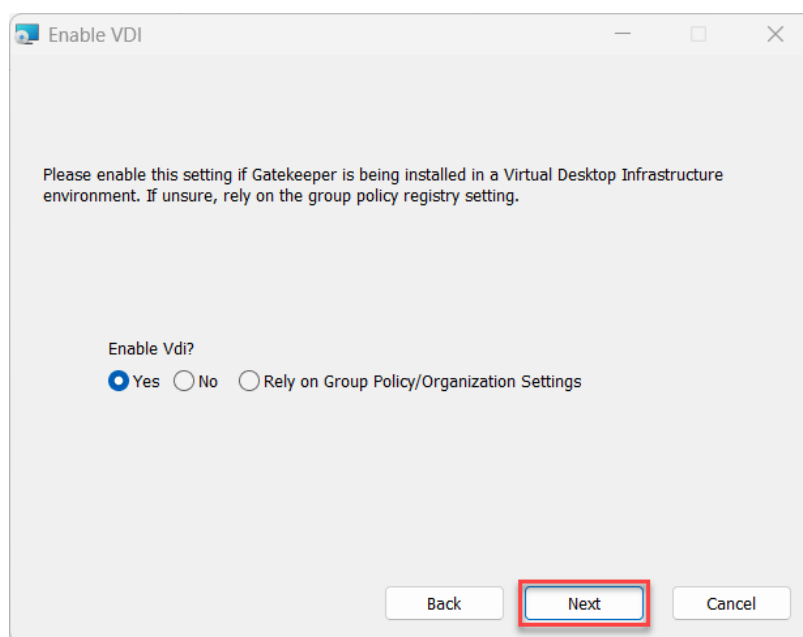


Figure 111

Selecting the third option (***“Rely on Group Policy/Organization Settings”***) means that SENTRY™ Gatekeeper will check against the customer’s Organization settings in SENTRY™ Cloud as they relate to VDI, and whether the organization has VDI support enabled. (It can also check against the organization’s existing Windows Group Policy should one exist.) If a customer has the “VDI Enabled” setting set to “Yes” in SENTRY™ Cloud, or if the customer’s Windows registry / group policy is set to provide SENTRY™ Gatekeeper users with the VDI flag, then selecting “Rely on Group Policy/Organization Settings” will enable VDI support for the SENTRY™ Gatekeeper client.

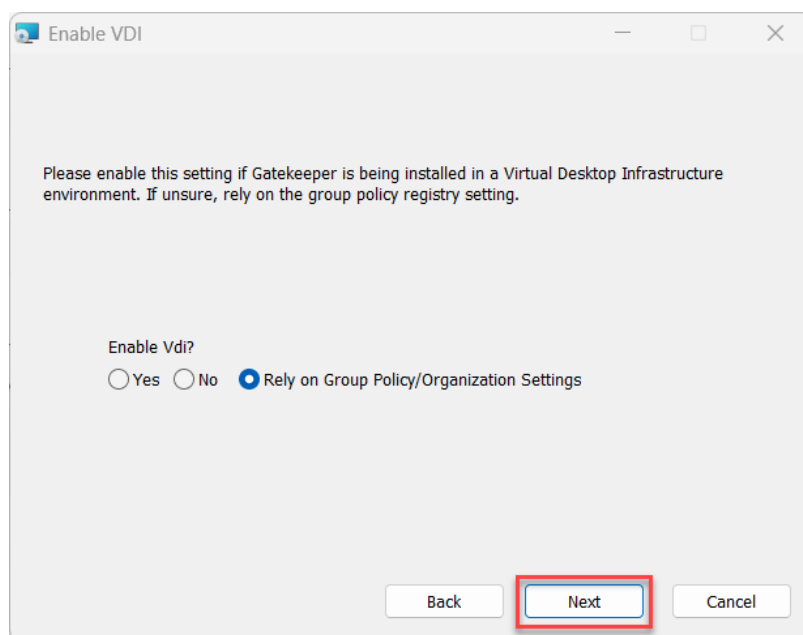


Figure 112

SILENT INSTALLATION / COMMAND PROMPT

To **override and enable VDI** support for a SENTRY™ Gatekeeper client via a silent installation command prompt, you can run the following.:

```
msiexec /i SentryGatekeeperSetup.msi /passive ENABLE_VDI="true"
```

WINDOWS REGISTRY / GROUP POLICY

A Windows registry / group policy, as described in the previous section, acts as a database storing configuration settings for a customer organization's Windows operating system and the applications that use it. It also lets administrators manage and configure the settings for users and computers in a Microsoft Active Directory (AD) environment. As such, customer administrators can use their Windows registry / group policy to attribute the VDI support "flag" to their SENTRY™ Gatekeeper end users.

SETTING AN ADDRESS AS A VDI ENABLED REMOTE WORKER

When a user from a VDI enabled uses SENTRY™ Gatekeeper to report their location while working remotely (i.e., not within a corporate environment building / site), they can follow the instructions below to set and provision their address. **PLEASE NOTE:** The SENTRY™ Gatekeeper client will behave with slight differences based on whether the end user's customer organization allows for the use of Location Services, or if administrators have Location Services disabled. The information below outlines both scenarios.

WITHOUT LOCATION SERVICES

Some SENTRY™ Gatekeeper users will belong to organizations that have **VDI Support**, but the users' PC's **Location Services** is **disabled**. For these users, when starting SENTRY™ Gatekeeper as a remote worker for the first time, they will **IGNORE** the **Work Location** text box (if it appears) and instead look to the **"Nomadic (or Static) Phone – Location Change Detected"** toast message. Users can then click **"Add Address"** to enter their current remote location.

From the **New Address** panel, users must fill in information for the **Address Line 1**, **City**, **State**, and **Zip Code** fields. The user can select an **icon** at the top of the screen if desired, but it does not get sent to the PSAP. The user can also fill out the **Description** field to give their location a friendly name, but this will **NOT output to the PSAP**. In addition, the user can fill in the **Address Line 2** field to provide **extra information** to the PSAP, such as **floor or unit** numbers. Please note that this field has a general **20-character limit**, as some PSAPs truncate anything in this field that exceeds 20 characters. The user can also move the **"Accuracy"** slider, which will expand or shrink the **Area of Confidence** shaded circle around the user's map pin, but this is up to the user if they would like to do this. It does **NOT** output to the PSAP. Click **"Save"** to finish setting and provisioning the location.

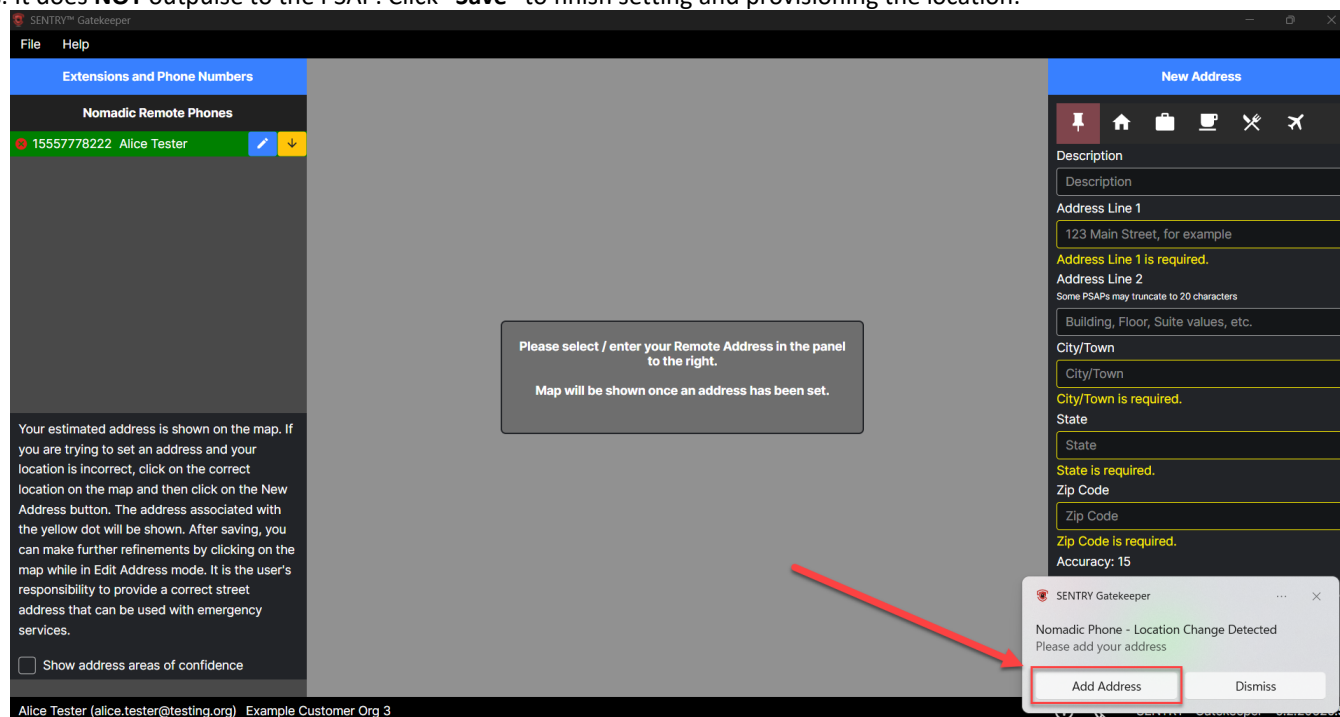


Figure 113



Figure 114

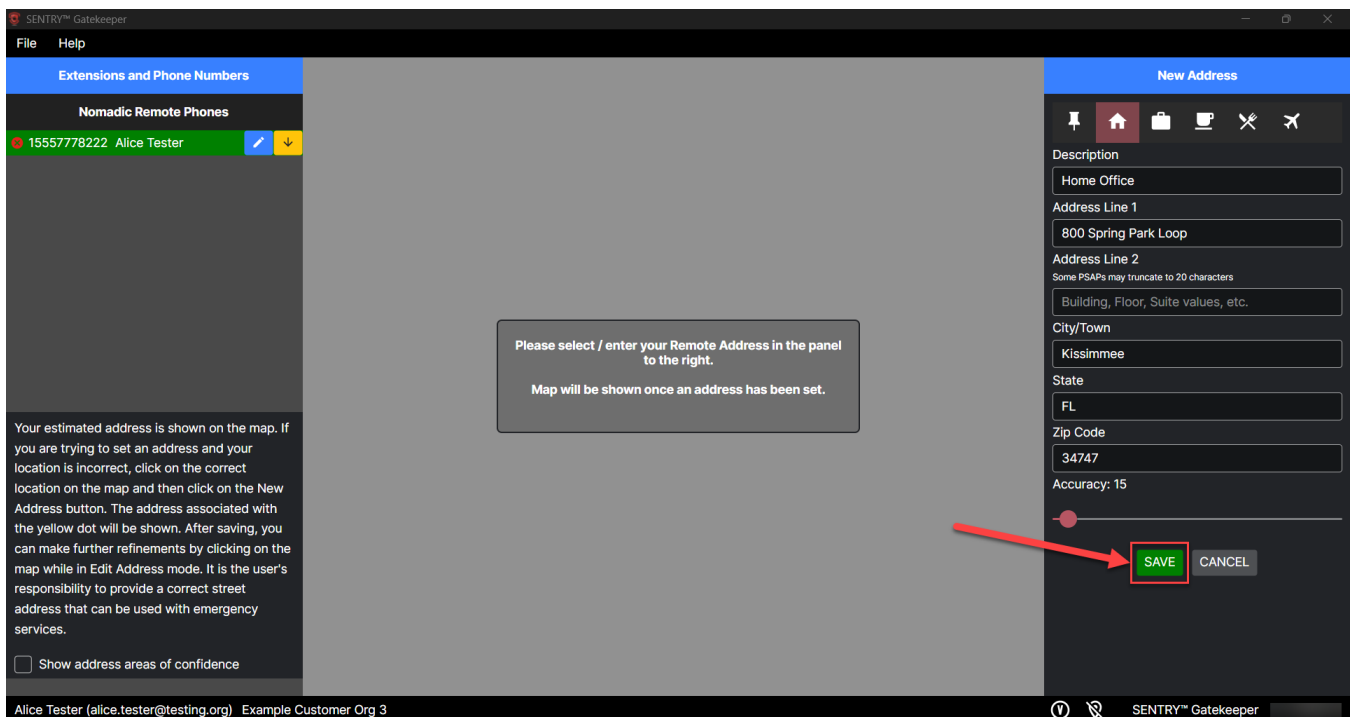


Figure 115

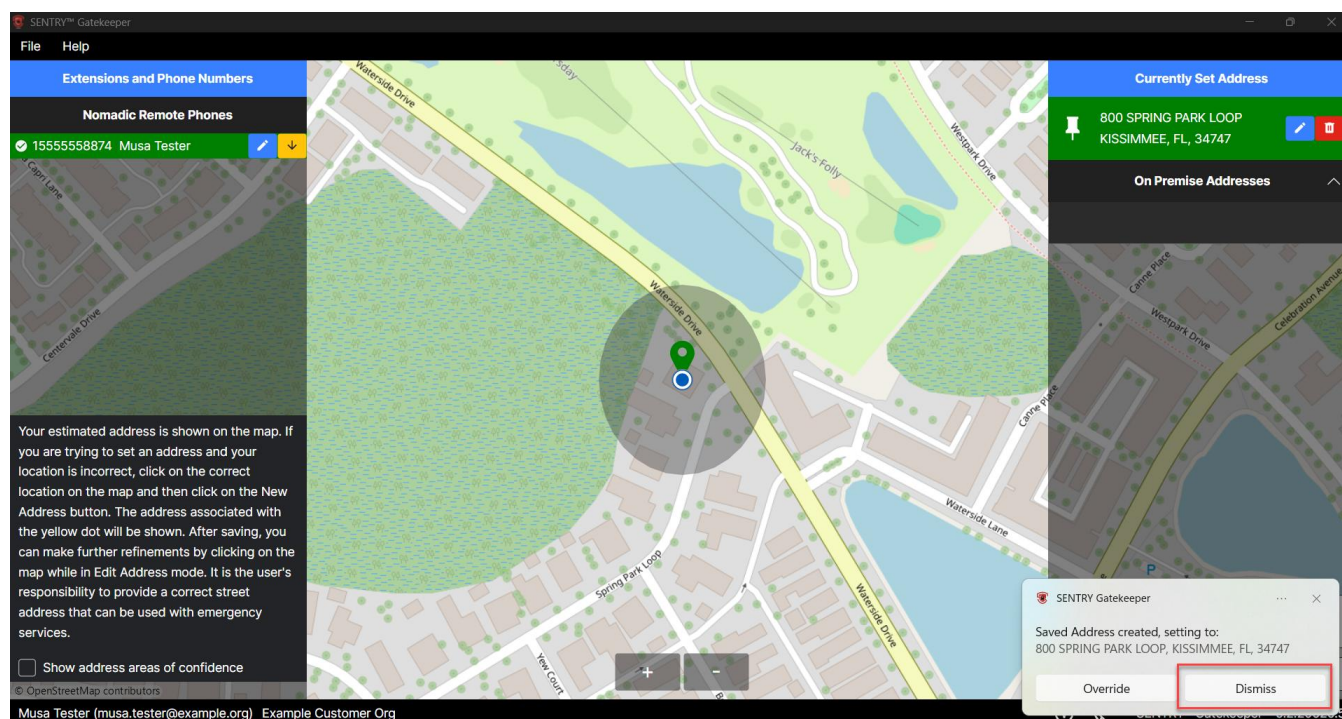


Figure 116

Those from an environment that employs the use of on-premise Geofences and Location definition will encounter a slightly different end user experience. When working from remotely instead of on-premise, users will still click **“Add Address”** to start setting an address or click **“the “x”** for the toast message or **“Dismiss”** and use the **“+New Address”** button to set a new address.

For the **“Add Address”** method, the user will click **“Add Address”** and follow the same instructions as described above. That is, they must at least fill in information for the **Address Line 1**, **City**, **State**, and **Zip Code** fields. Choosing an **icon**, adding a **Description**, and adding **Address Line 2** information remains optional. The user can also move the **“Accuracy”** slider, which will expand or shrink the **Area of Confidence** shaded circle around the user’s map pin, but this is up to the user if they would like to do this. It does **NOT** outpulse to the PSAP. Click **“Save”** to finish setting and provisioning the location.

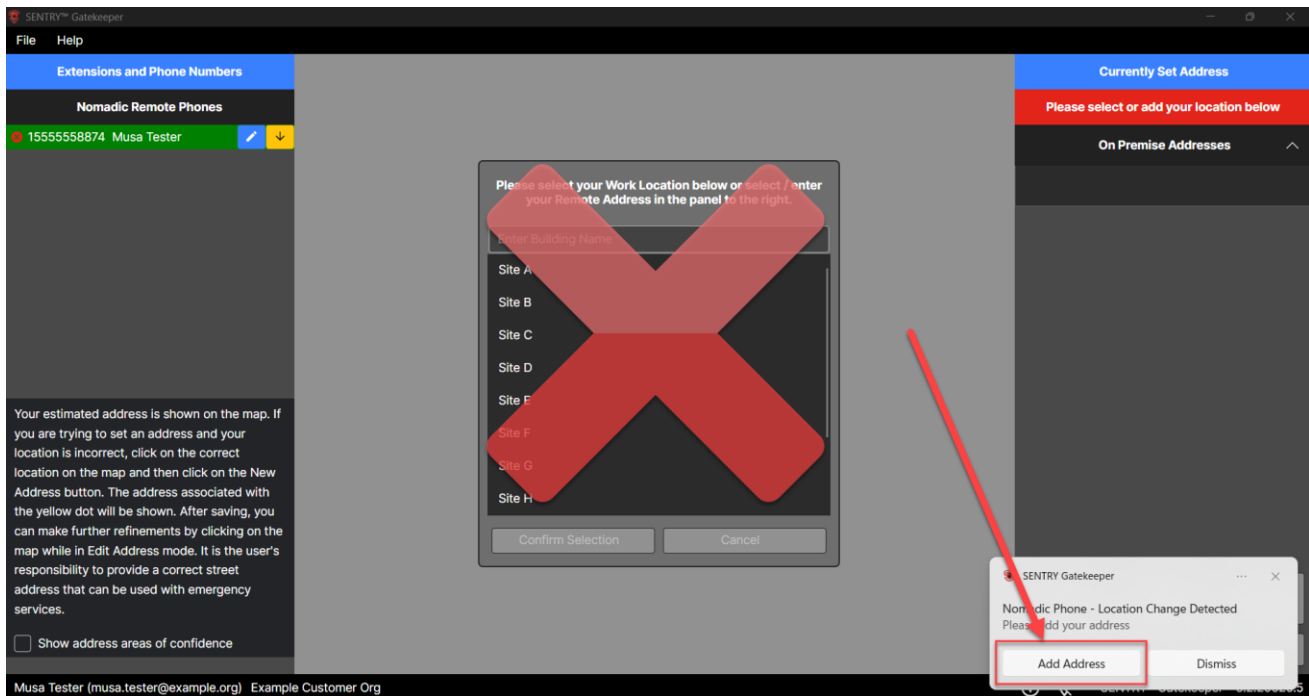


Figure 117

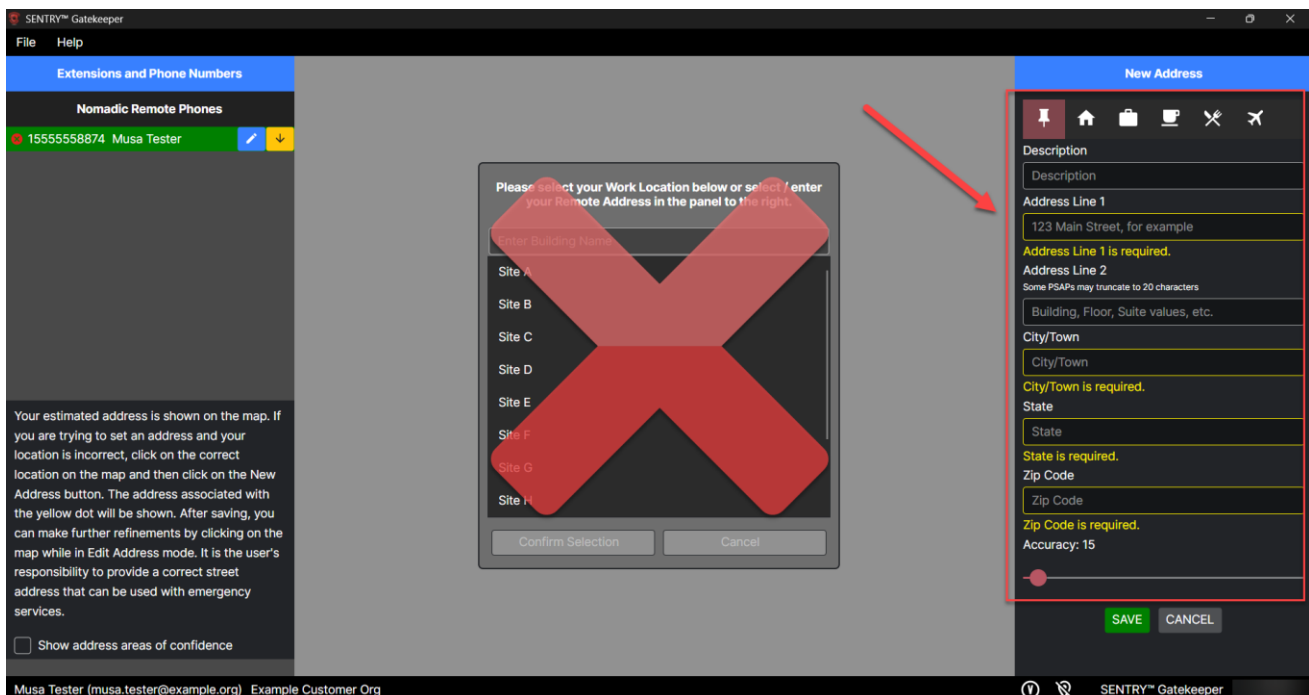


Figure 118



Figure 119

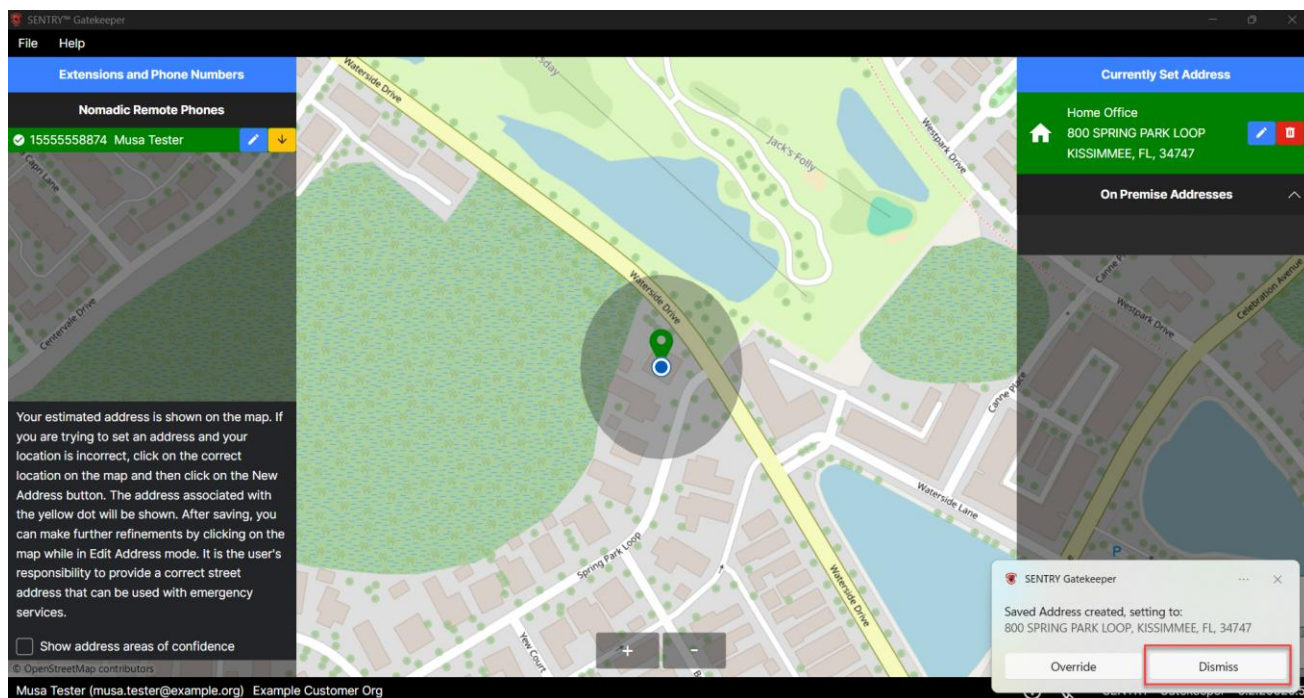


Figure 120

As an alternative method, the user could also click the “x” for the toast message or “Dismiss” and use the “+New Address” button to set a new address. After clicking “+New Address”, the user would follow the same steps for the “Override” method to enter and save their address, thus completing the process of provisioning it.

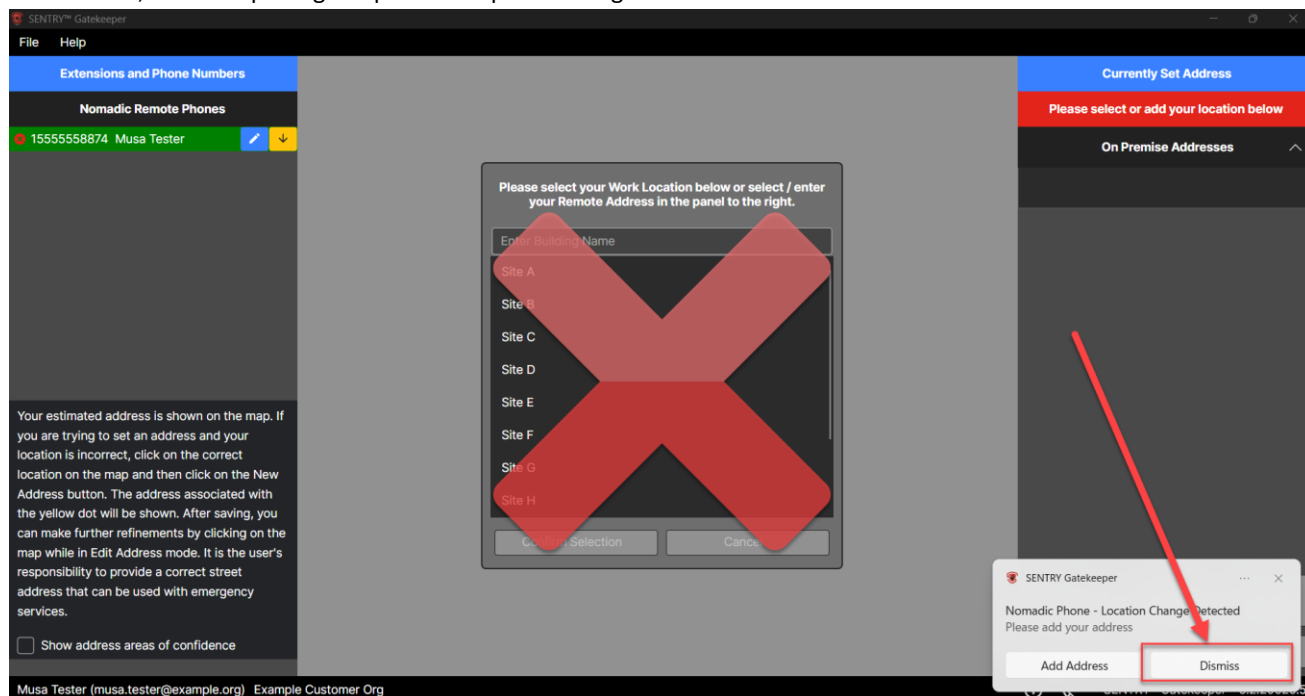


Figure 121



Figure 122



Figure 123

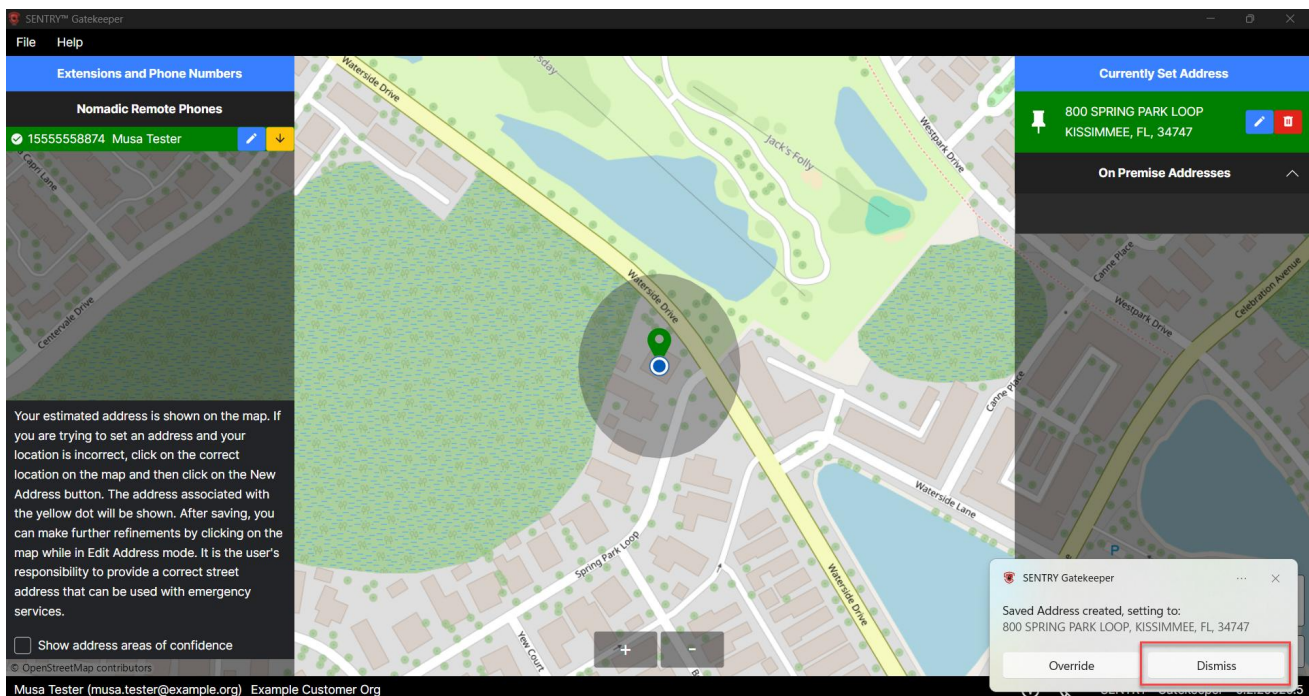


Figure 124

******PLEASE NOTE: A VDI-supported, No Location Services SENTRY™ Gatekeeper user is responsible for updating their location whenever they move** around, whether that be from one floor to another in the same building, or to a new building / site entirely. If a **VDI-supported, No Location Services SENTRY™ Gatekeeper** user moves to a new remote location throughout the day (from a home office to a coffee shop, for example), **SENTRY™ Gatekeeper cannot detect that movement**. As such, SENTRY™ Gatekeeper will not deprovision a user's set address once they provision it. As such, the **SENTRY™ Gatekeeper end user is responsible for updating their set address whenever they change locations**. The user can do so using either the **"Override"** or **"New Address"** method as desired.

Upon startup, the last provisioned location will still be provisioned, but SENTRY™ Gatekeeper will provide the user with a toast message allowing the user to click **"Override"** and set a new address or click **"x"** or **"Dismiss"**, then use the **"New Address"** button to set a new address as described above.

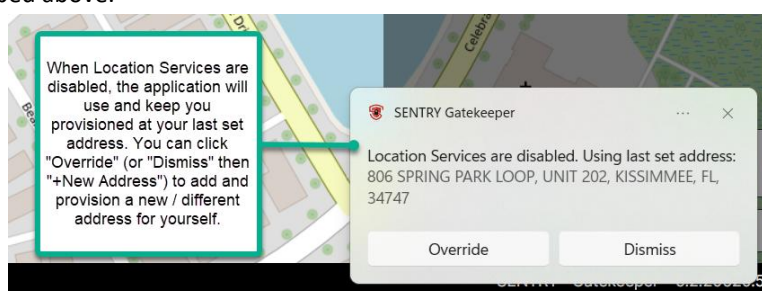


Figure 125

Once provisioned, the address will remain so until the user provisions a new or different location. **PLEASE NOTE:** Users can make use of the **Saved Addresses** list to re-provision themselves at a commonly frequented location. Users can use the **"New Address"** button to create additional addresses to choose from. From the Saved Addresses list, users can click the **green checkmark** for whichever option applies to their current whereabouts to provision and update their location.

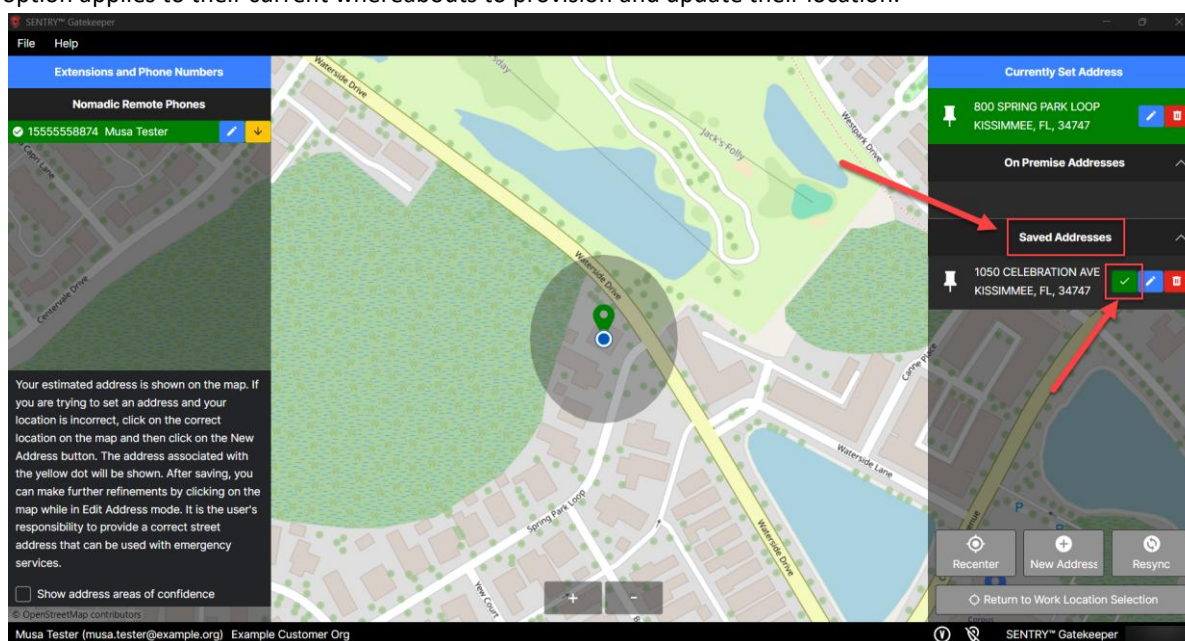


Figure 126

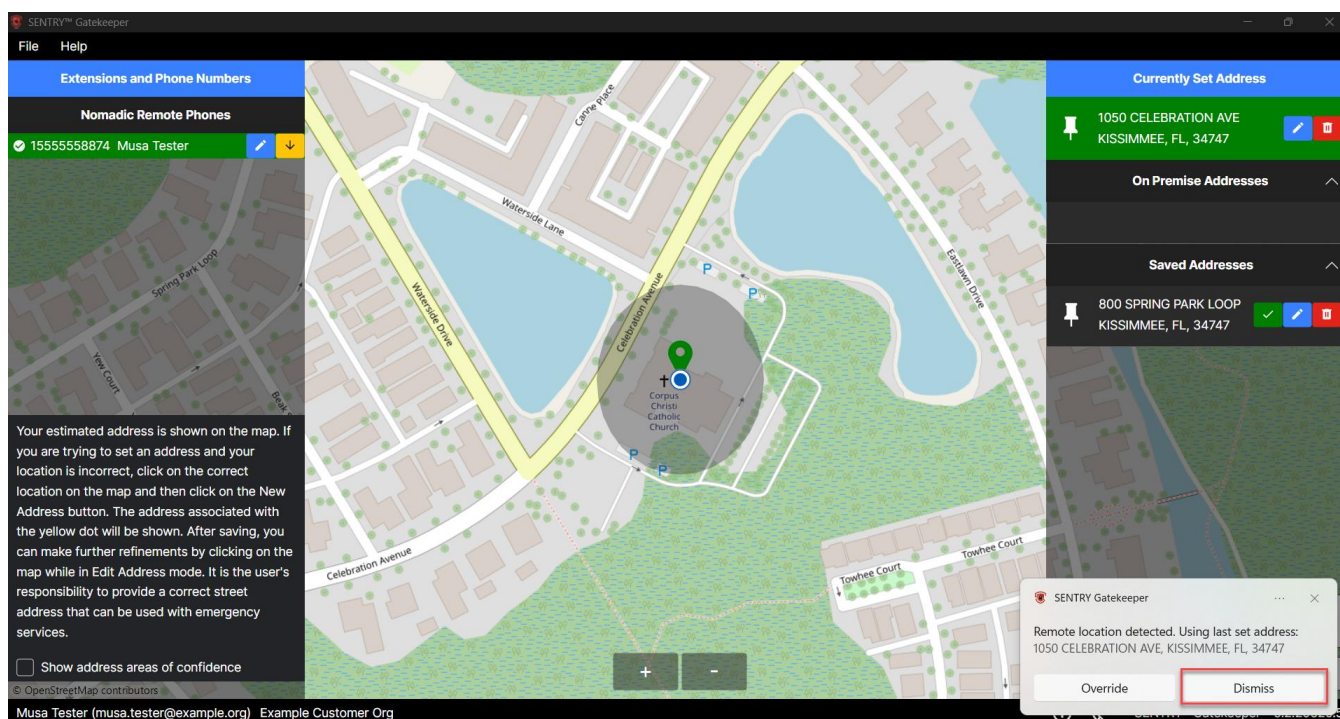


Figure 127

WITH LOCATION SERVICES USING CLIENT LOCATION REDIRECTION

Some SENTRY™ Gatekeeper users will belong to organizations that have **VDI Environments** and use **Client Location Redirection**, a configurable feature to pass the end user's device Location Services through the VDI Environment. **LIMITATION NOTE:** If Client Location Redirection is not enabled or not configured properly, the Location Services (though enabled on the user's device) input may return an incorrect location (e.g. the data center location). SENTRY™ Gatekeeper has no ability to distinguish or configure the different Location Services inputs. It can only be configured from the VDI Environment settings. When starting SENTRY™ Gatekeeper as a remote worker for the first time, users will look to the “**Nomadic (or Static) Phone – Location Change Detected**” toast message. Users can then click “**Add Address**” to enter their current remote location.

From the **New Address** panel, users will see their estimated address information populated in the **Address Line 1**, **City**, **State**, and **Zip Code** fields. If all the details are correct, the user can click “**Save**” to set and provision their address. However, the user can refine any details of the address that require correcting. Either way, users must have information filled in the **Address Line 1**, **City**, **State**, and **Zip Code** fields. The user can select an **icon** at the top of the screen if desired, but it does not get sent to the PSAP. The user can also fill out the **Description** field to give their location a friendly name, but this will **NOT output to the PSAP**. In addition, the user can fill in the **Address Line 2** field to provide **extra information** to the PSAP, such as **floor or unit** numbers. Please note that this field has a general **20-character limit**, as some PSAPs truncate anything in this field that exceeds 20 characters. The user can also move the “**Accuracy**” slider, which will expand or shrink the **Area of Confidence** shaded circle around the user's map pin, but this is up to the user if they would like to do this. It does **NOT** output to the PSAP. Click “**Save**” to finish setting and provisioning the location.

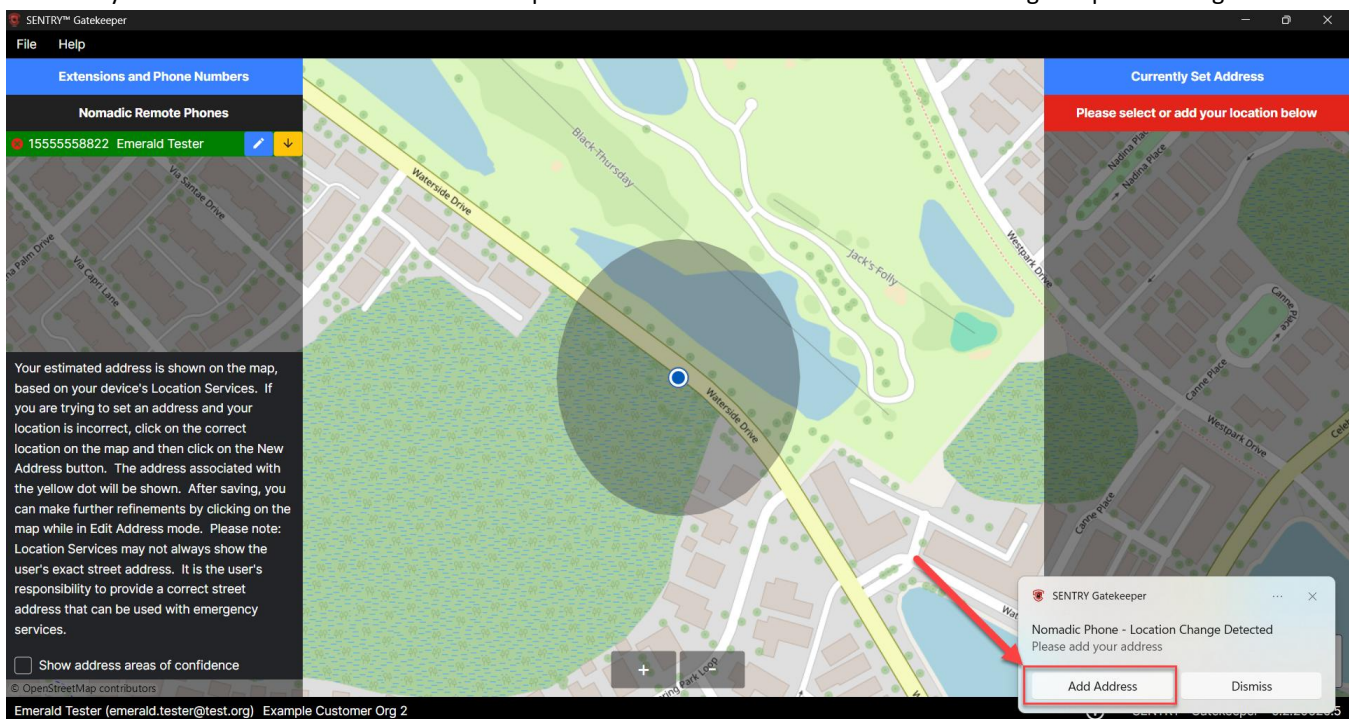


Figure 128

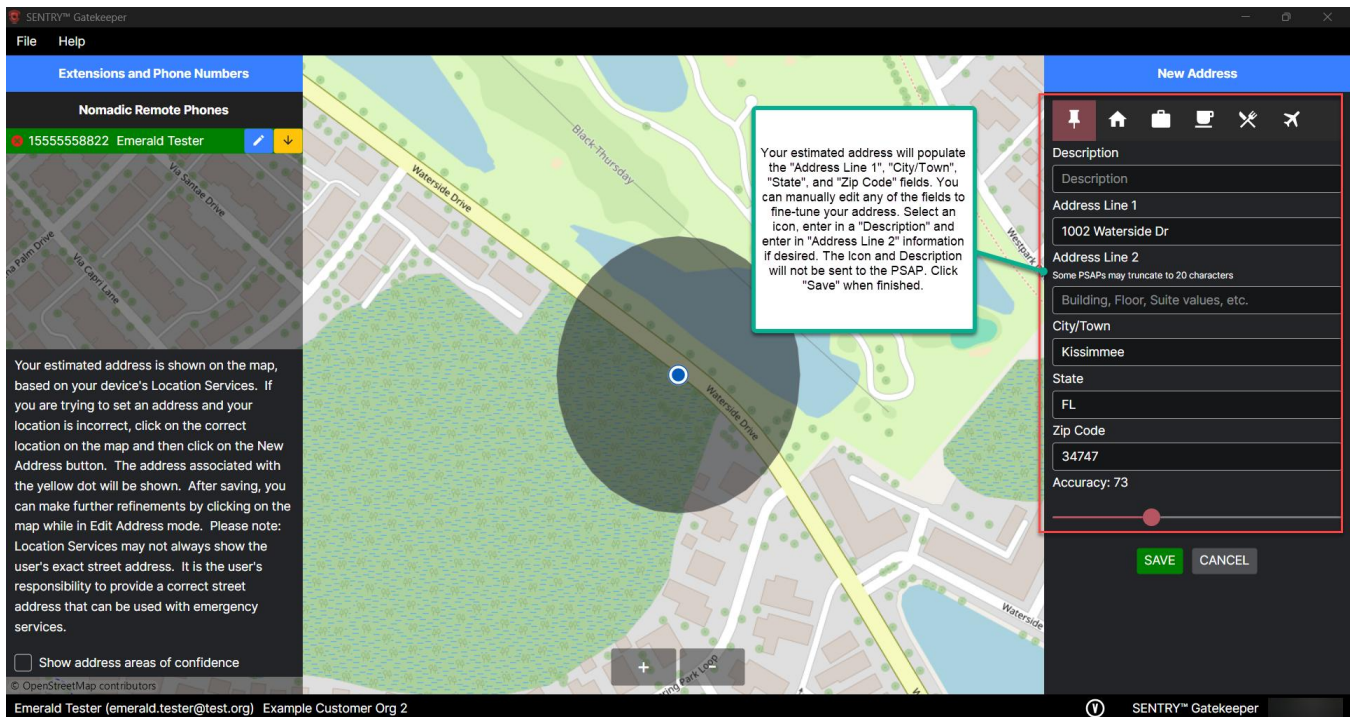


Figure 129

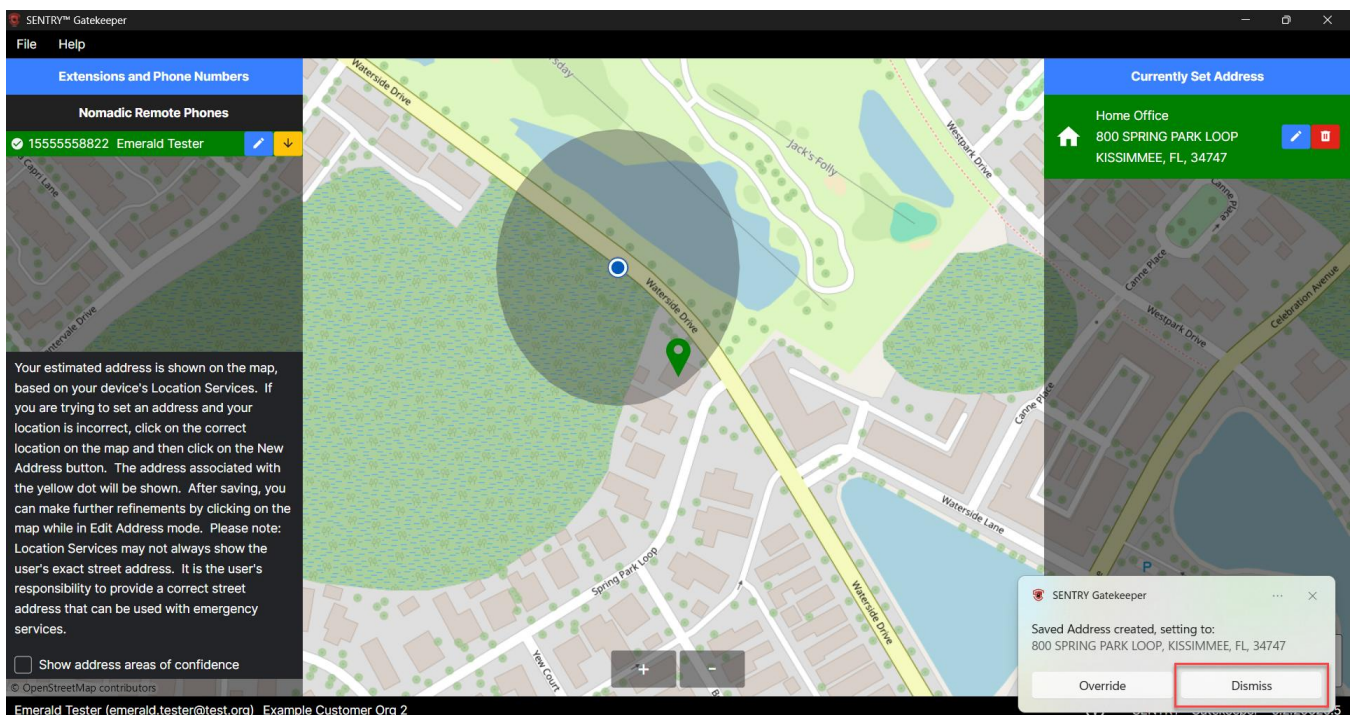


Figure 130

******PLEASE NOTE:** A VDI-supported, Location Services-enabled SENTRY™ Gatekeeper user is responsible for updating their location whenever they move around, whether that be from one floor to another in the same building, or to a new building / site entirely. If a VDI-supported, Location Services SENTRY™ Gatekeeper user moves to a new remote location throughout the day (from a home office to a coffee shop, for example), SENTRY™ Gatekeeper cannot use Location Services for movement discovery. As such, SENTRY™ Gatekeeper will not deprovision a user's set address once they provision it. As such, the SENTRY™ Gatekeeper end user is responsible for updating their set address whenever they change locations. The user can do so using either the "Override" or "+New Address" method as desired.

PLEASE NOTE: Users can make use of the **Saved Addresses** list to re-provision themselves at a commonly frequented location. Users can use the "+New Address" button to create additional addresses to choose from. From the Saved Addresses list, users can click the **green checkmark** for whichever option applies to their current whereabouts to provision and update their location.

The next time SENTRY™ Gatekeeper runs, it will remember the user's previously selected location, but SENTRY™ will still present the user with a toast message and a way to override the location should they desire to do so.

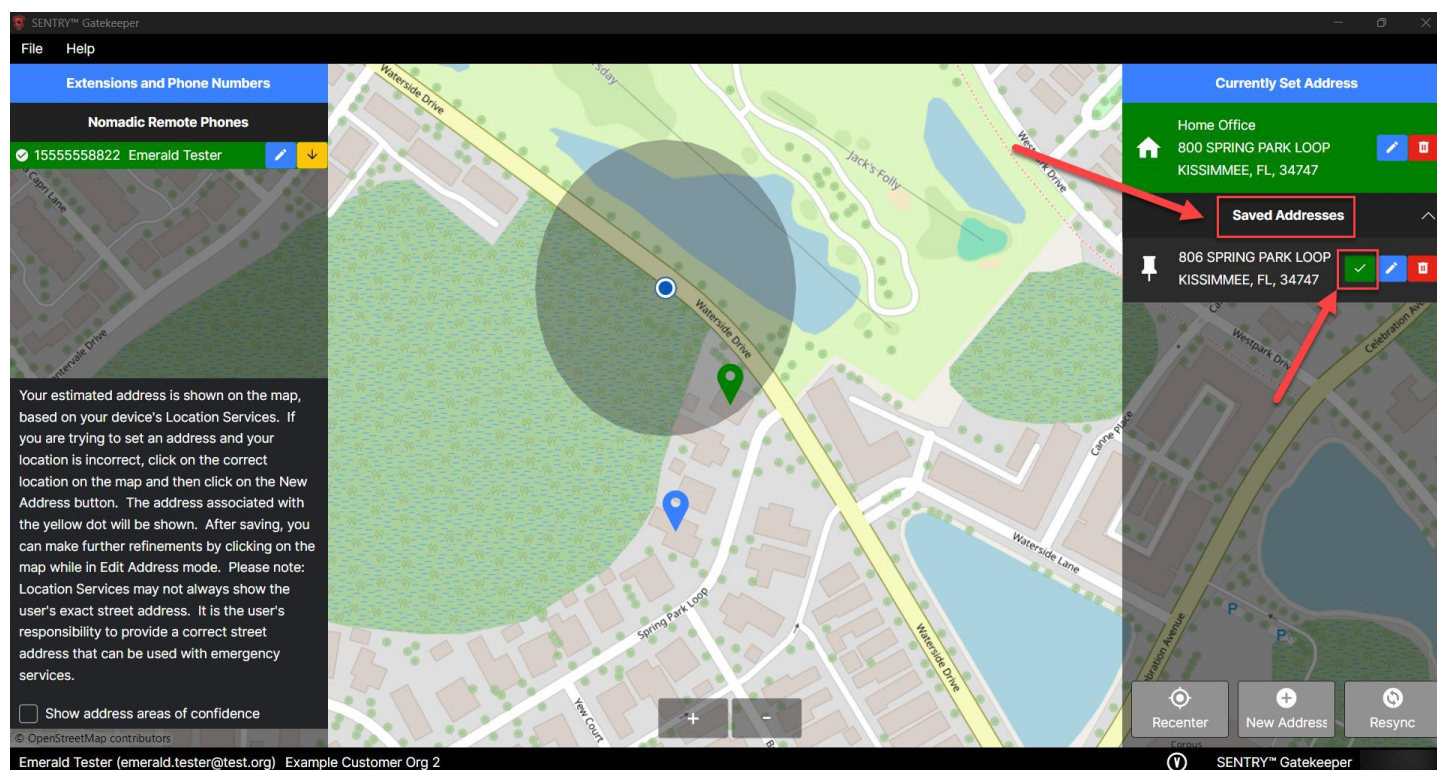


Figure 131

SETTING AN ADDRESS AS A VDI ENABLED ON-PREMISE USER

When a user from a VDI enabled environment uses SENTRY™ Gatekeeper to report their location while on-premise (i.e., physically at work), they can follow the instructions below to set and provision their address. Rather than manually typing in an address or specifying their location by clicking a map, these SENTRY™ Gatekeeper will present these end users with lists of on-premise locations to choose from. **PLEASE NOTE:** The SENTRY™ Gatekeeper client will behave with slight differences based on whether the end user's customer organization allows for the use of Location Services, or if administrators have Location Services disabled. The information below outlines both scenarios.

WITHOUT LOCATION SERVICES

Some SENTRY™ Gatekeeper users will belong to organizations that both have **VDI Support AND** their SENTRY™ Gatekeeper clients **are set to NOT rely on their PC's Location Services**. For these users, SENTRY™ Gatekeeper will present a list of Geofences (polygonal shapes drawn around a mapped area) for the user to pick from to specify their current location. These Geofences represent different sites, buildings, etc. from their organization. These Geofences will display with names or descriptions so that the SENTRY™ Gatekeeper end users will recognize them and select the correct site or building where they work from.

VDI-supported SENTRY™ Gatekeeper users with no Location Services will see a **Work Location** box display like the one below when they first sign in. The end user can **select the name / title of their correct building, site, etc. from the text box presented** to them. The toast message stating **"Nomadic (or Static) Phone – Location Change Detected"** will also appear, with options to **"Add Address"** or **"Dismiss"**. The end user can either **ignore** this message or click **"Dismiss"** to get rid of the toast message. (Only VDI users working remotely instead on on-premise would click **"Add Address"** instead of ignoring or dismissing the message.) Once the user clicks on the correct building, site, etc., they can click **"Confirm Selection"**. **PLEASE NOTE:** No map view will display until the user selects their building / site and then clicks **"Confirm Selection"**.

Once the user confirms their building / site selection, they will select the correct location within that building / site from the **On Premise Addresses** list on the right-hand side of the SENTRY™ Gatekeeper client window. Users will click the **green checkmark** to **finish setting and officially provision their address** and location within SENTRY™ Gatekeeper. In addition, once users have provisioned their address location, they may click **"Dismiss"** on the SENTRY™ Gatekeeper toast message in the lower right-hand corner stating, **"Location Services are disabled. Using last set address: [address here] – Override – Dismiss"**.

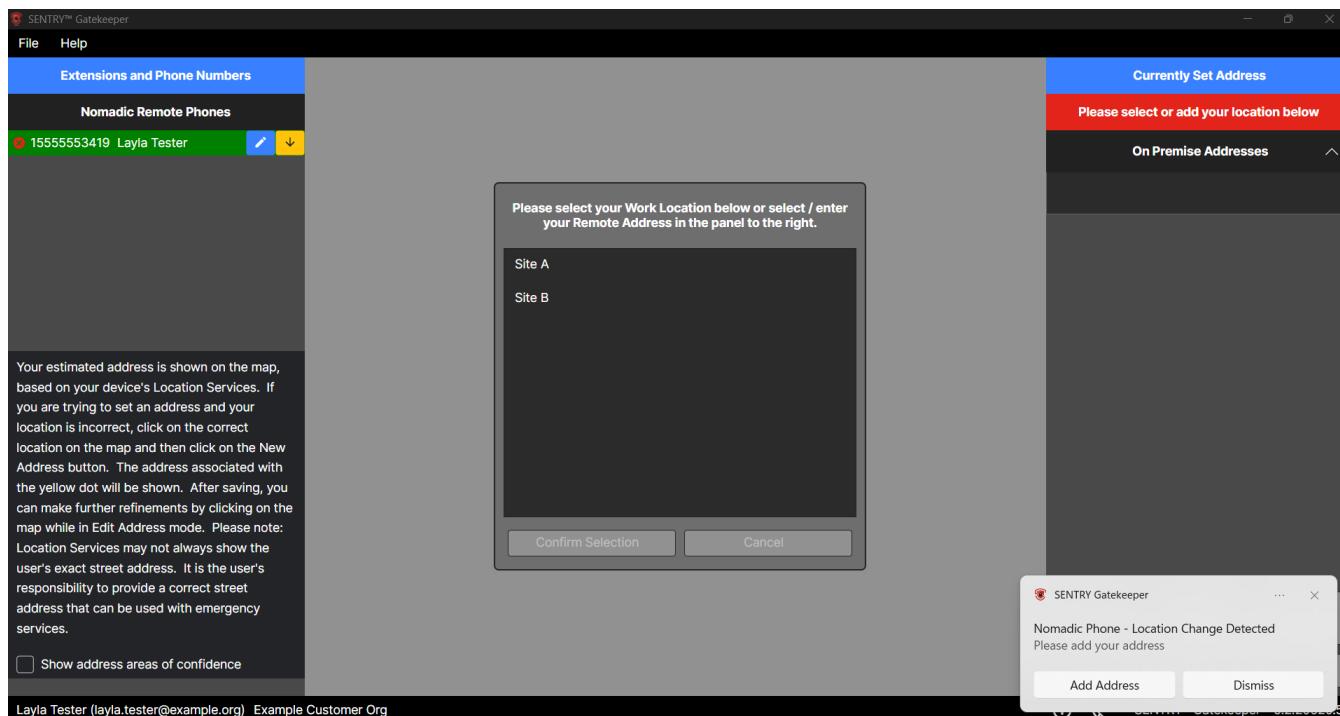


Figure 132

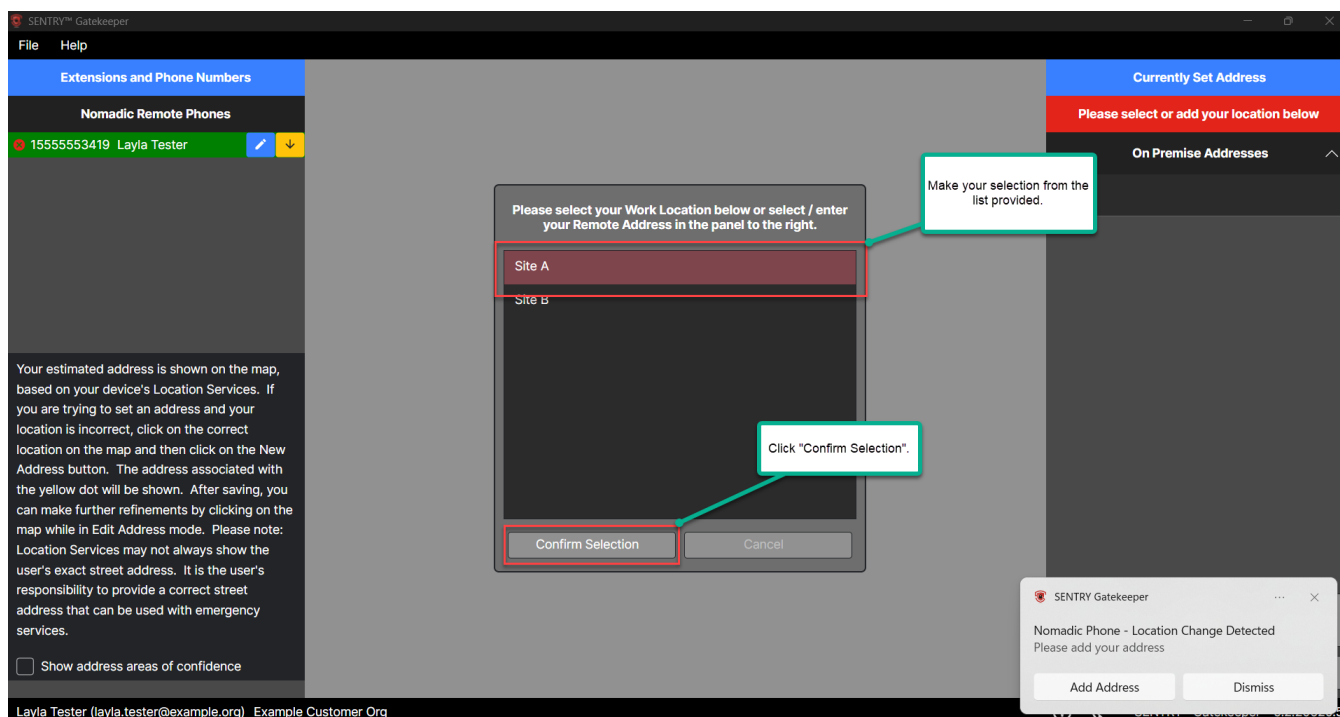


Figure 133

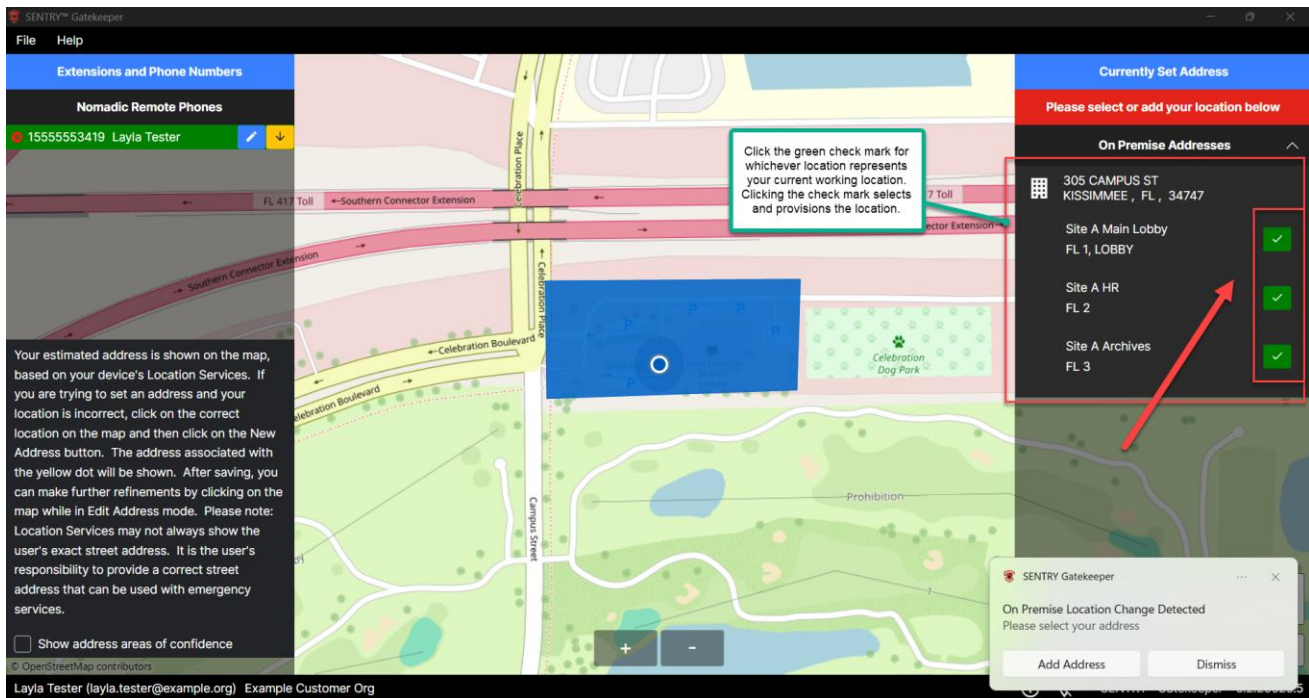


Figure 134

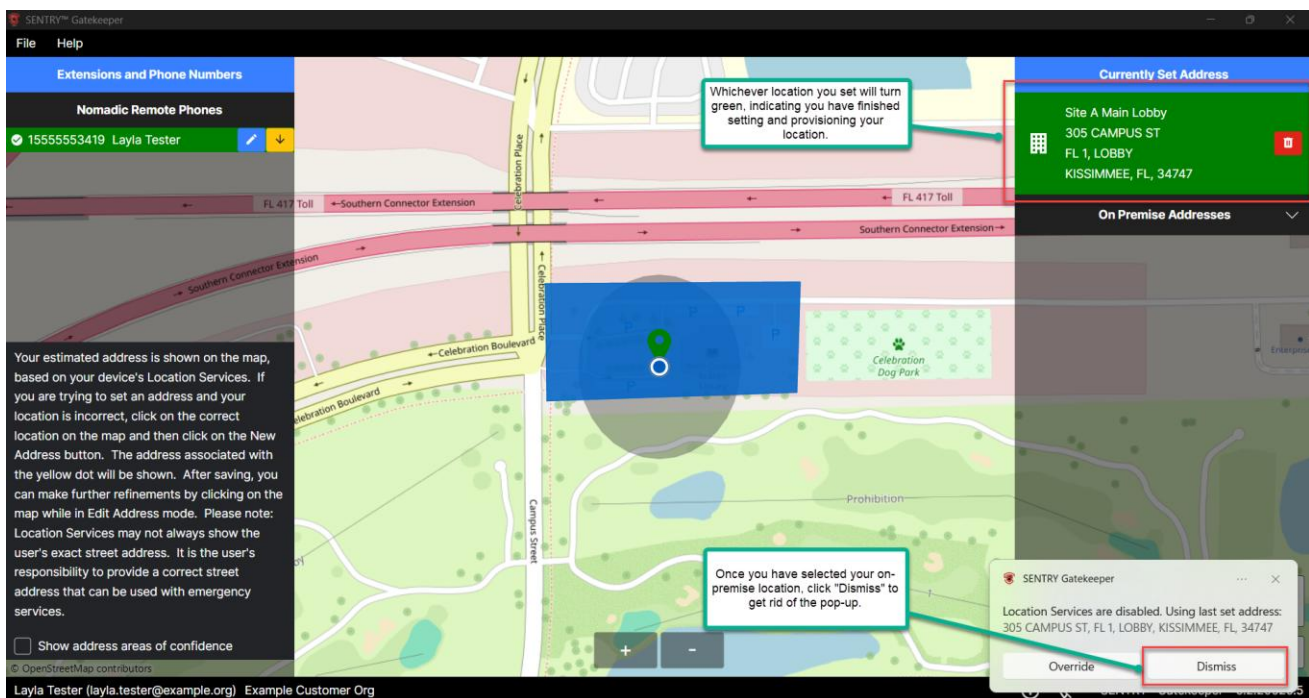


Figure 135

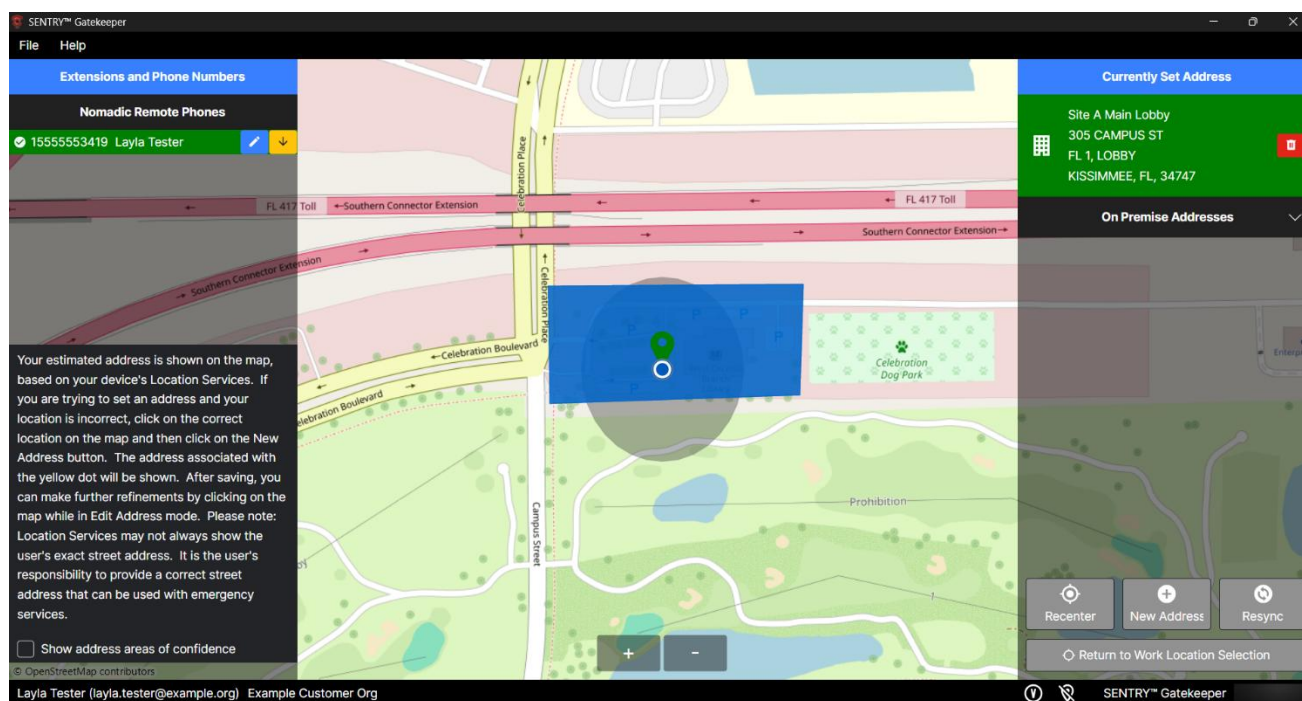


Figure 136

Depending on the length of the list of possible work buildings or sites for the user to select from, a **scroll bar** will present itself for easier searching. In addition, users can utilize a **search bar** with text reading (by default) **“Enter Building Name”**, as shown in the screenshots below. Users can search alphanumerically for the building / site appropriate to them, then **select their desired option** and click **“Confirm Selection”** to move forward with provisioning their location. (**PLEASE NOTE:** No map view will display until the user selects their building / site and then clicks **“Confirm Selection”**).

As stated above, users will then select the correct location within their on-premise appropriate building / site from the **On Premise Addresses** list on the right-hand side of the SENTRY™ Gatekeeper client window. Users will click the **green checkmark** to **finish setting and officially provision their address** and location within SENTRY™ Gatekeeper. In addition, once users have provisioned their address location, they may click **“Dismiss”** on the SENTRY™ Gatekeeper toast message in the lower right-hand corner stating, **“Location Services are disabled. Using last set address: [address here] – Override – Dismiss”**.

The next time SENTRY™ Gatekeeper runs, it will remember the user’s previously selected location, but SENTRY™ will still present the user with a toast message and a way to override the location should they desire to do so.

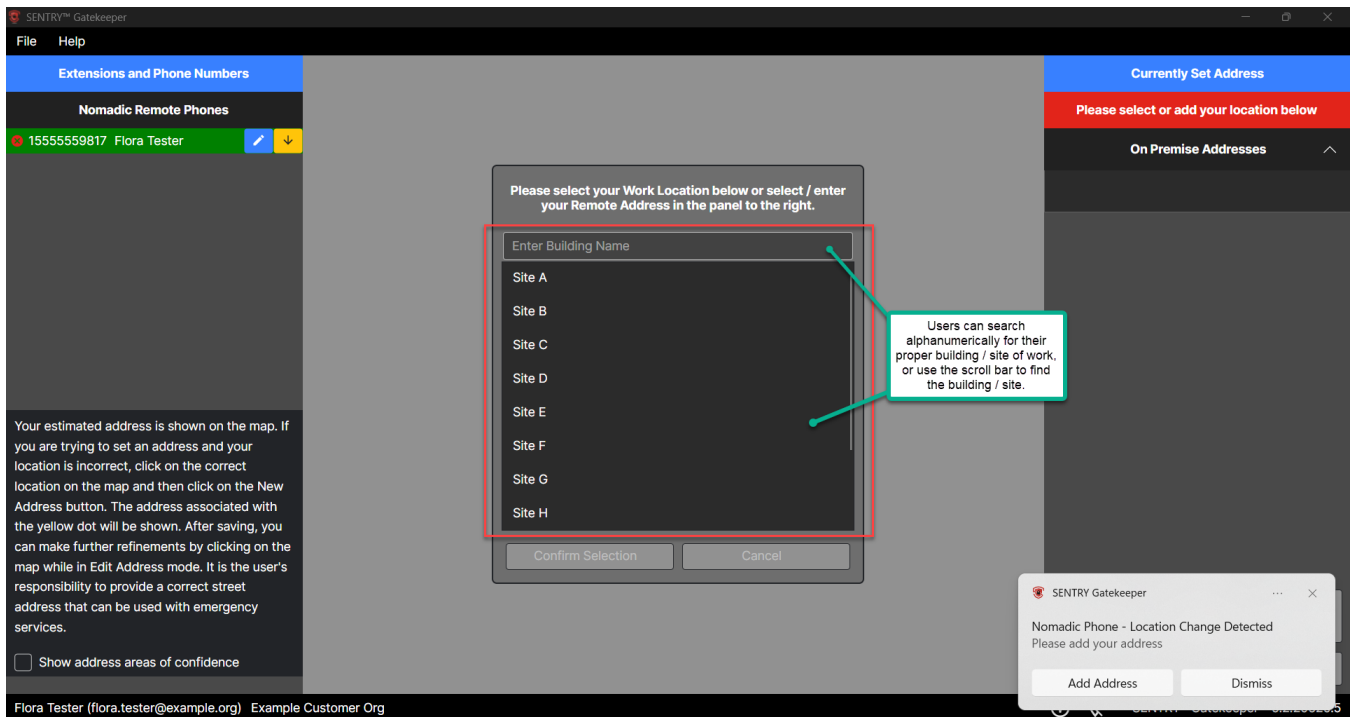


Figure 137

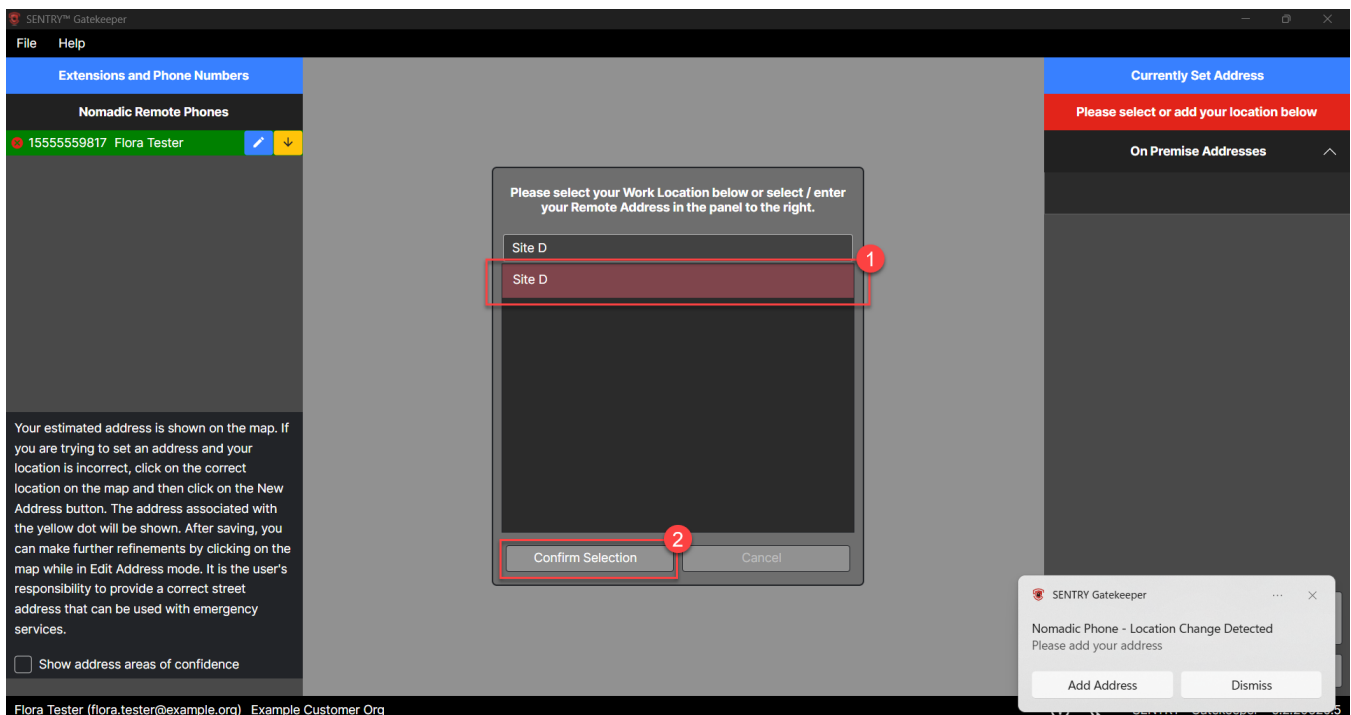


Figure 138

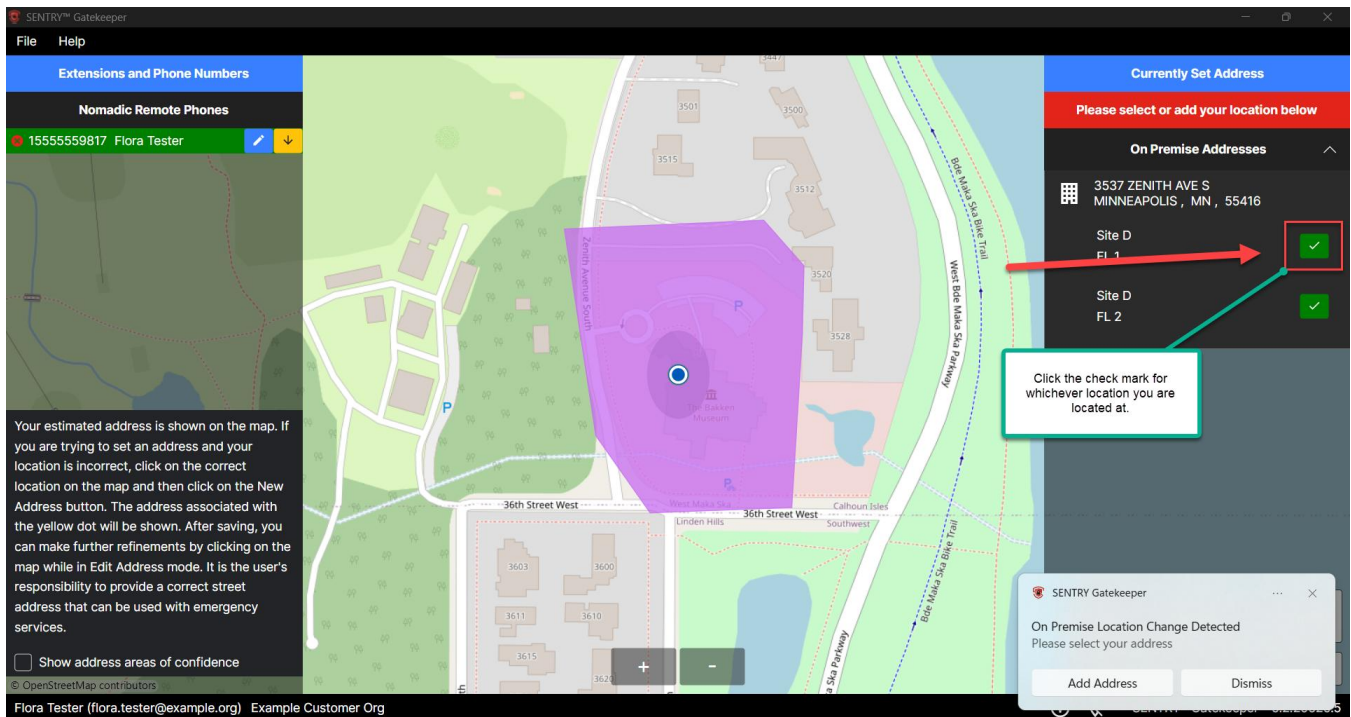


Figure 139

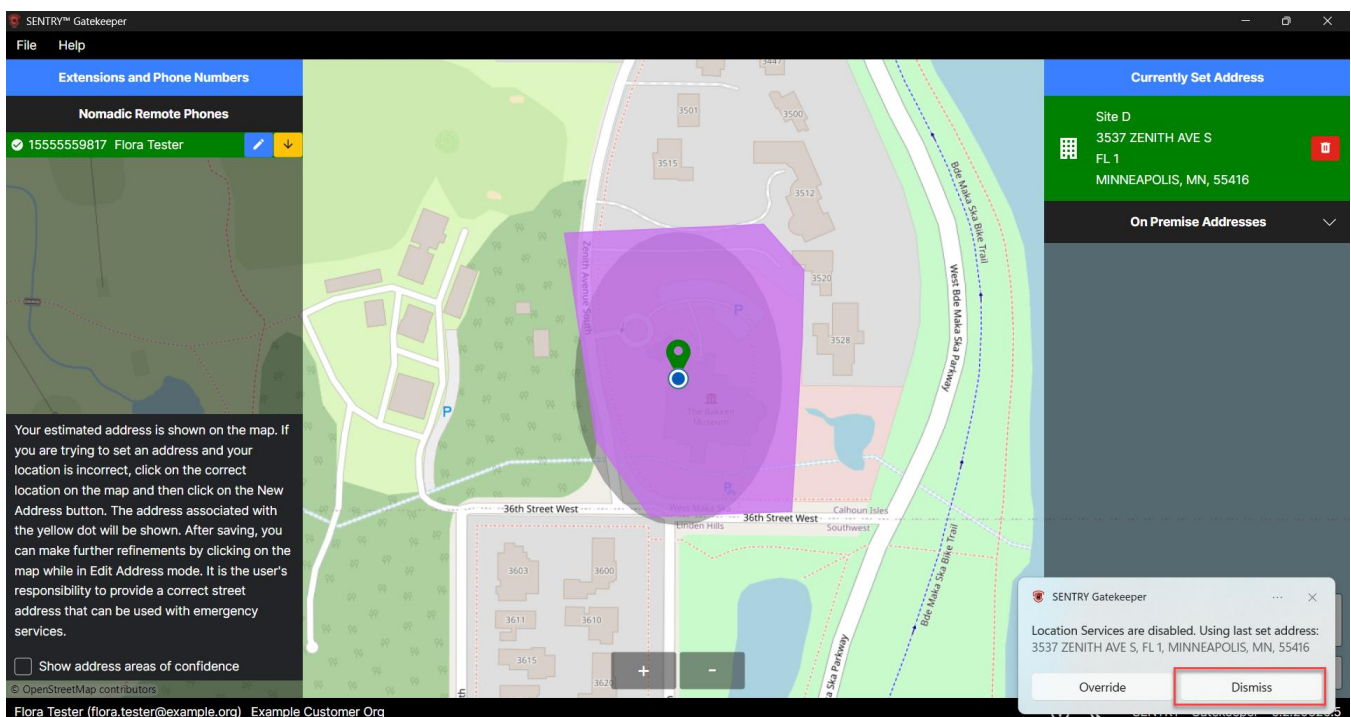


Figure 140

******PLEASE NOTE: A VDI-supported, No Location Services SENTRY™ Gatekeeper user is responsible for updating their location whenever they move** around, whether that be from one floor to another in the same building, or to a new building / site entirely. If a **VDI-supported, No Location Services SENTRY™ Gatekeeper** user moves to work at a new workspace throughout the same building of their on-premise work environment during their working hours, **SENTRY™ Gatekeeper cannot detect that movement**. As such, the **SENTRY™ Gatekeeper end user is responsible for updating their set address whenever they move** throughout their workplace. The user can do so in two ways.

The first option applies if the user moves throughout the same building or site within their workday. They can click on the “\On Premise Addresses header, then click the **green check mark** of whichever granular option applies to where they moved (for example, a first-floor option, a second-floor option, etc.). Clicking the green checkmark will **update and provision their set address** to their new in-office location. This option will likely be the most convenient for the end user.

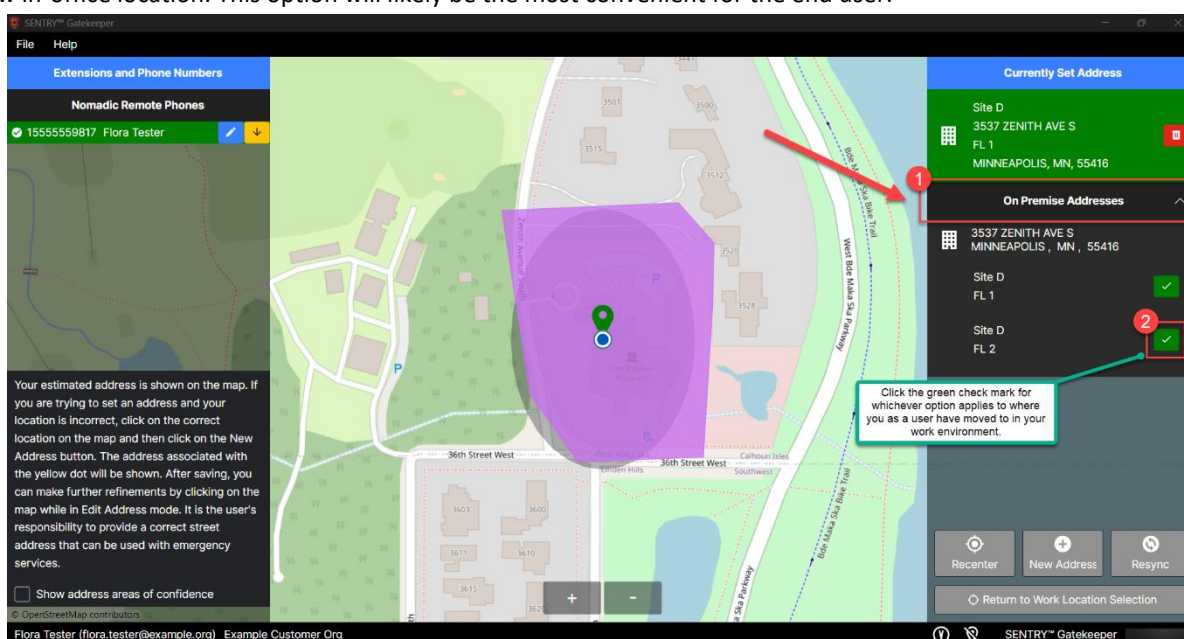


Figure 141

The second option will benefit those who have moved from one building to an entirely different building during their workday. (However, it can still apply for a user who changed working locations for the day but still operates out of the same building.) For this option, the user can click “**Return to Work Location Selection**” and SENTRY™ Gatekeeper will present the user with the **Work Location** box display so that they can scroll or search then select their new correct building / site location. Once they click “**Confirm Selection**” they can move forward with provisioning their address clicking the green check mark of whichever option best describes their new current location.

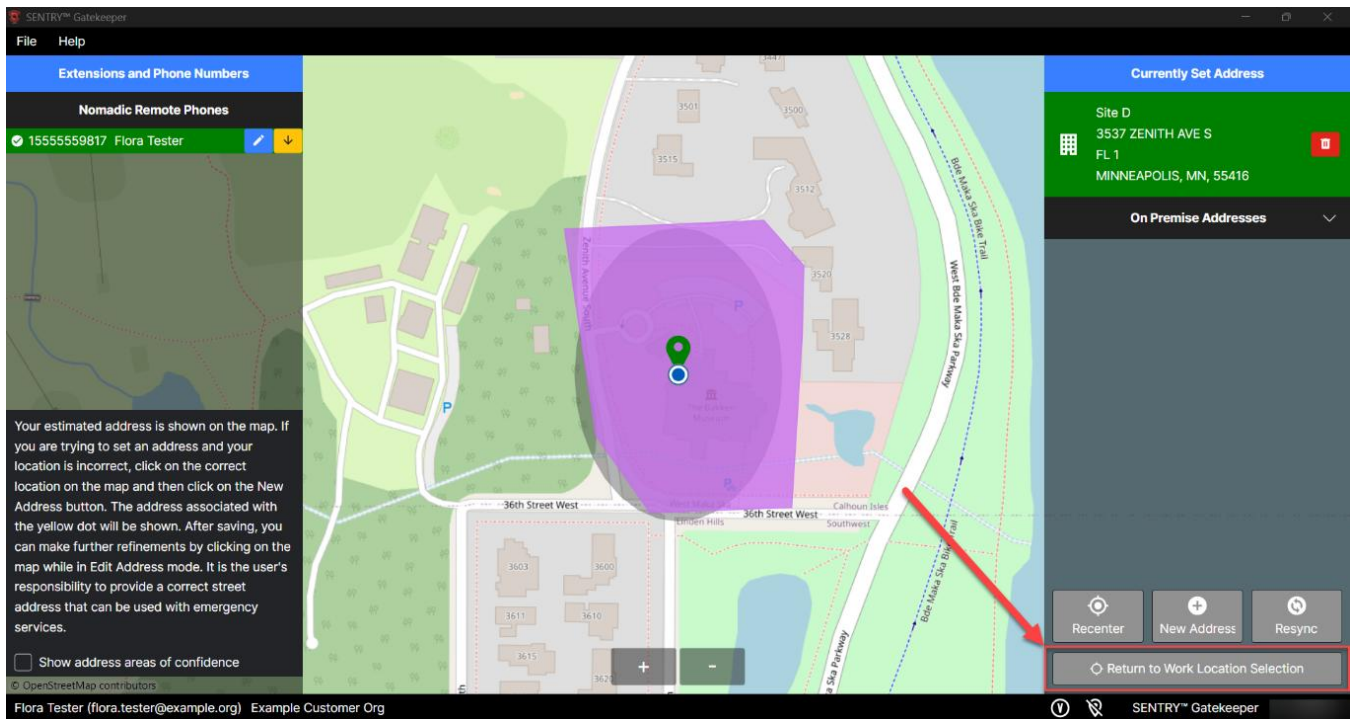


Figure 142

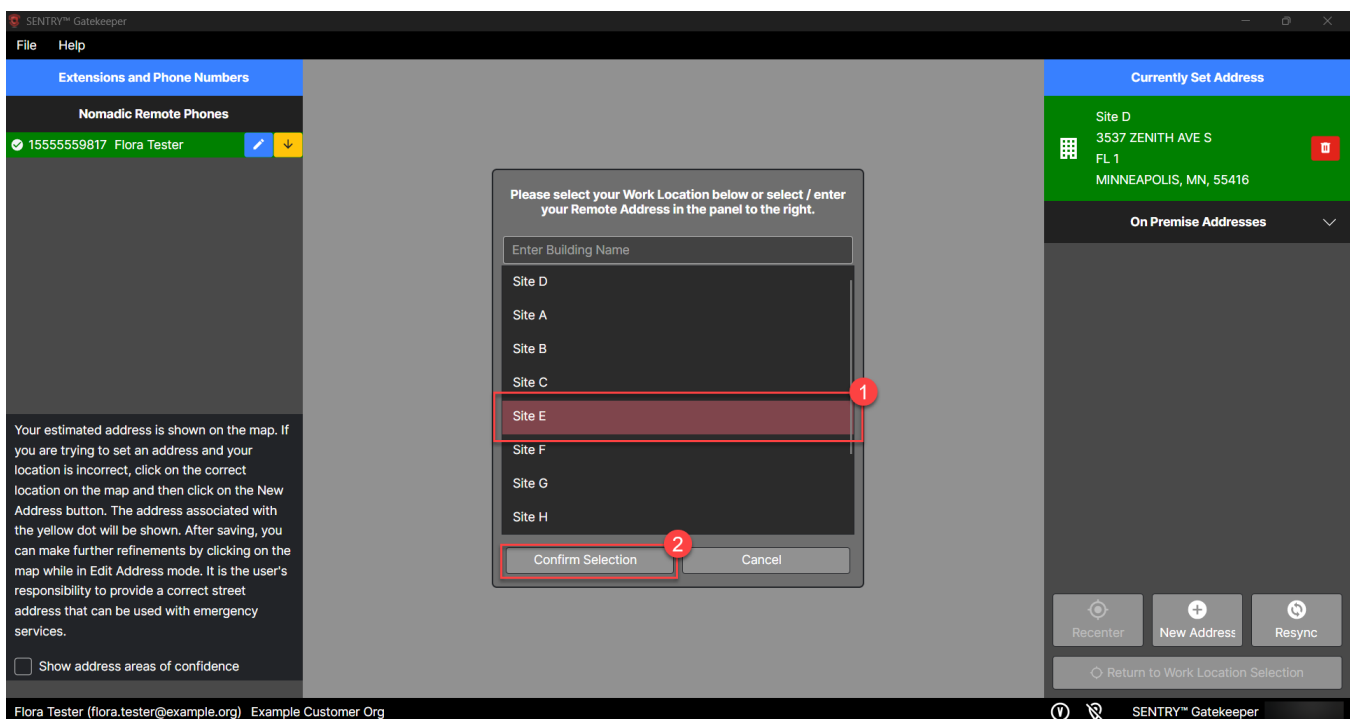


Figure 143

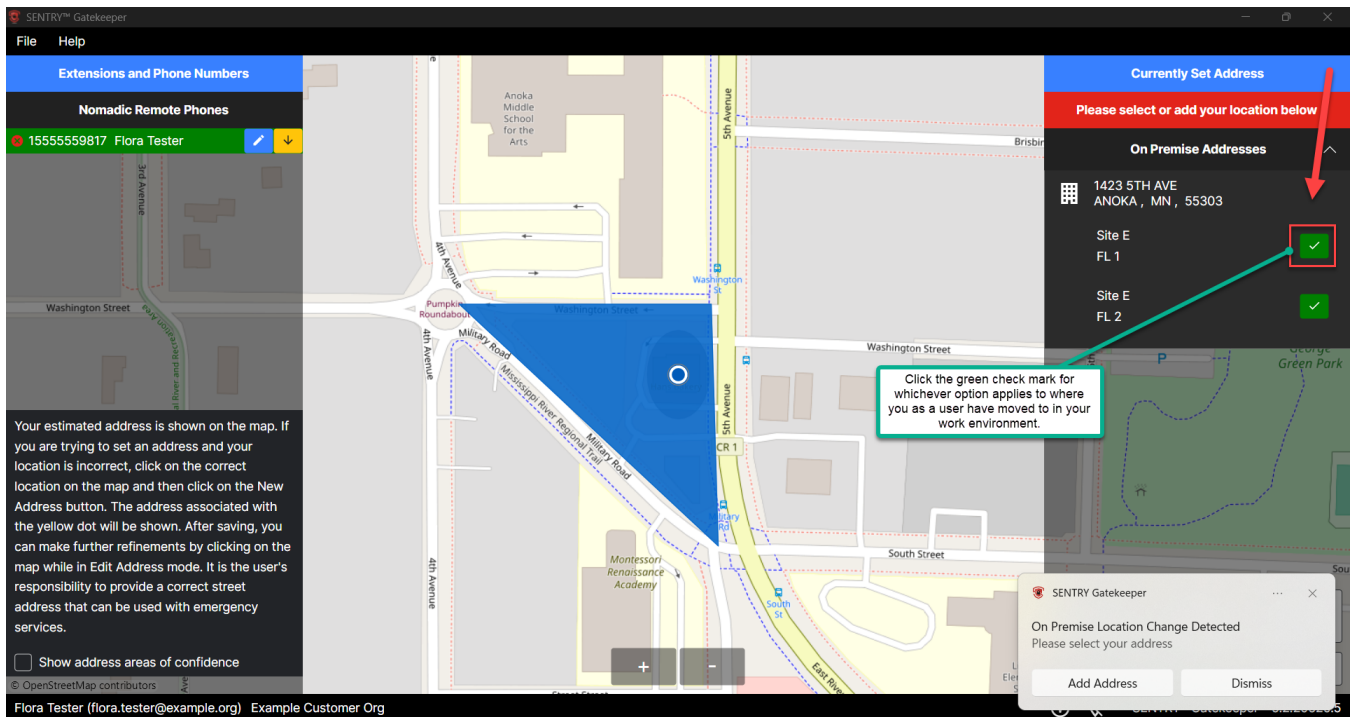


Figure 144

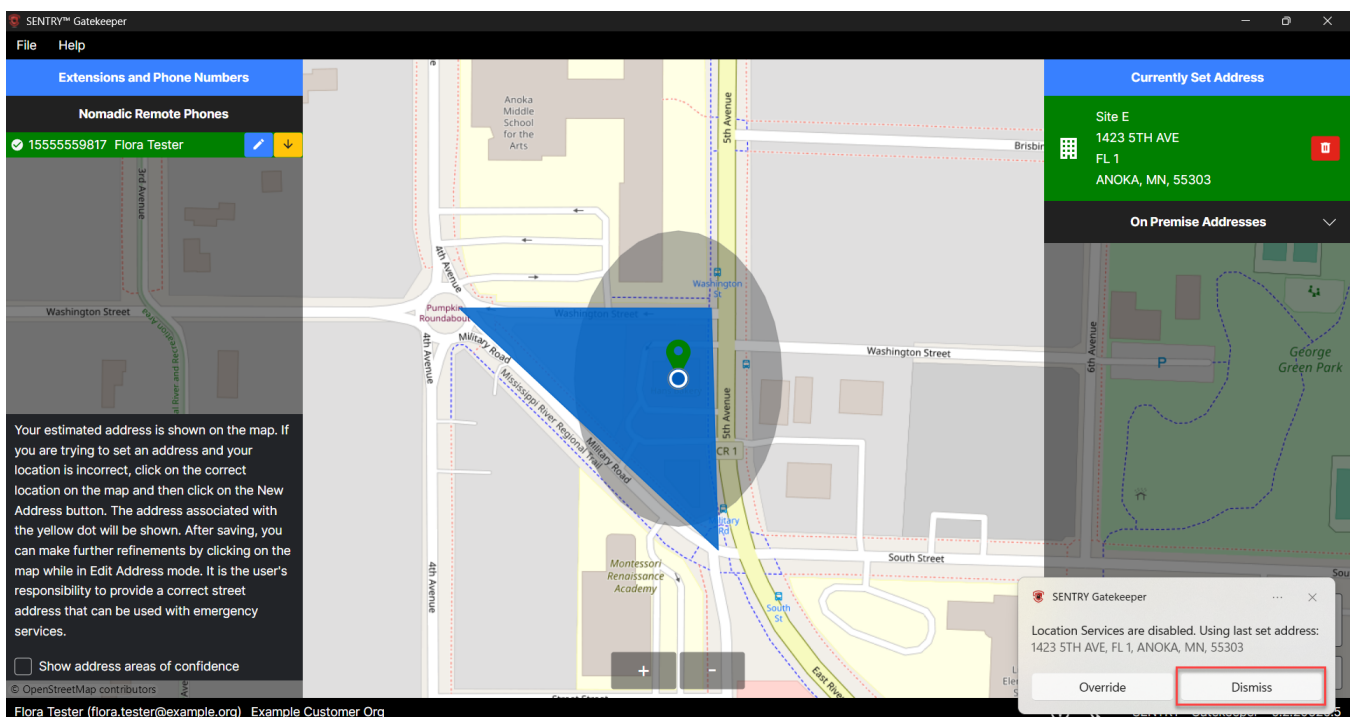


Figure 145

WITH LOCATION SERVICES USING CLIENT LOCATION REDIRECTION

Some SENTRY™ Gatekeeper users will belong to organizations that have **VDI Environments** and use **Client Location Redirection**, a configurable feature to pass the end user's device Location Services through the VDI Environment. **LIMITATION NOTE:** If Client Location Redirection is not enabled or not configured properly, the Location Services (though enabled on the user's device) input may return an incorrect location (e.g. the data center location). SENTRY™ Gatekeeper has no ability to distinguish or configure the different Location Services inputs. It can only be configured from the VDI Environment settings.

For these users, as SENTRY™ Gatekeeper initiates discovery for the user's location, SENTRY™ Gatekeeper will check the user's PC's Location Services pin to see if it falls within any of the Geofences (or specified geographical areas) defined by the organization's Administrators in SENTRY™ Cloud. If the user falls within one of these Geofences (each one usually represents a specific building or site belonging to their organization), then the **On Premise Addresses** list will present itself to the user. The On Premise Addresses list provides all options within that Geofence for the user to set as their current location. (The user could also enter their address manually with the **"Add Address"** button, should they choose.)

Users will then select the correct location within their on-premise appropriate building / site from the **On Premise Addresses** list on the right-hand side of the SENTRY™ Gatekeeper client window. Users will click the **green checkmark** to **finish setting and officially provision their address** and location within SENTRY™ Gatekeeper. In addition, once users have provisioned their address location, they may click **"Dismiss"** on the SENTRY™ Gatekeeper toast message in the lower right-hand corner stating, **"On premise office location detected. Using last set address: [address here] – Override – Dismiss"**.

The next time SENTRY™ Gatekeeper runs, it will remember the user's previously selected location, but SENTRY™ will still present the user with a toast message and a way to override the location should they desire to do so.

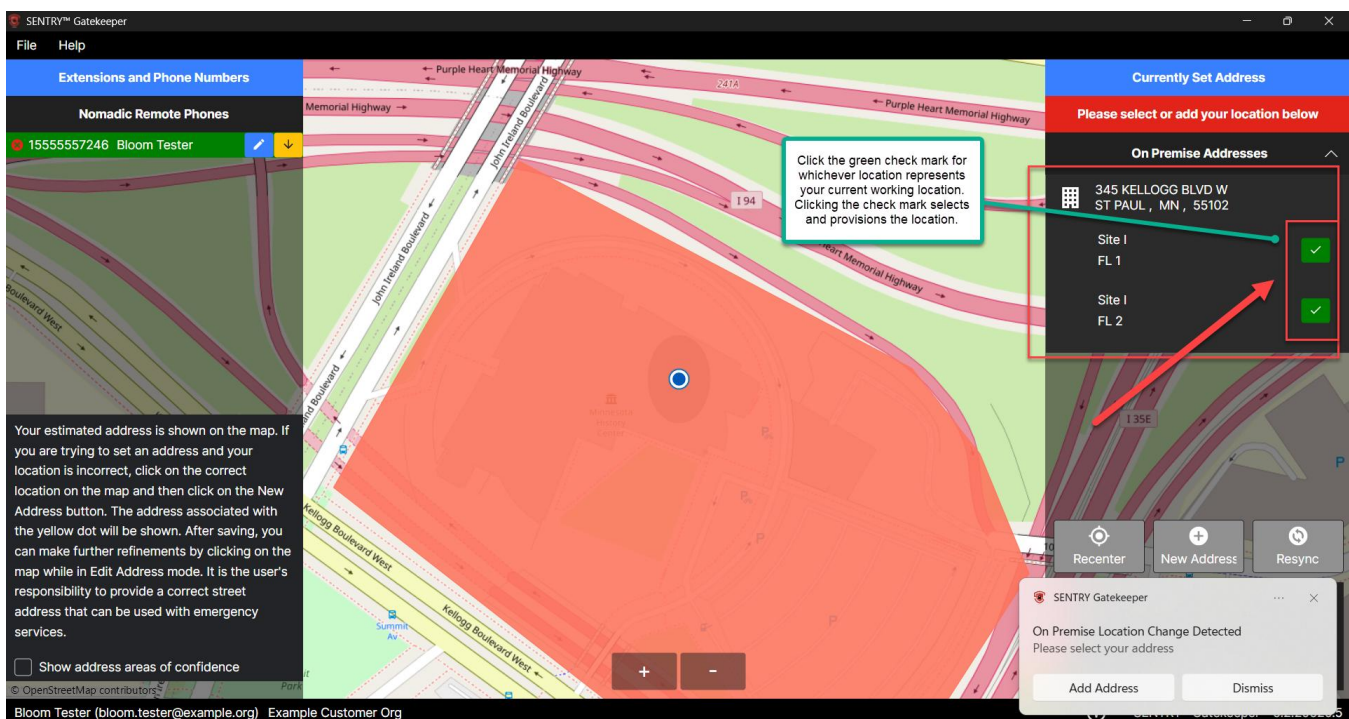


Figure 146

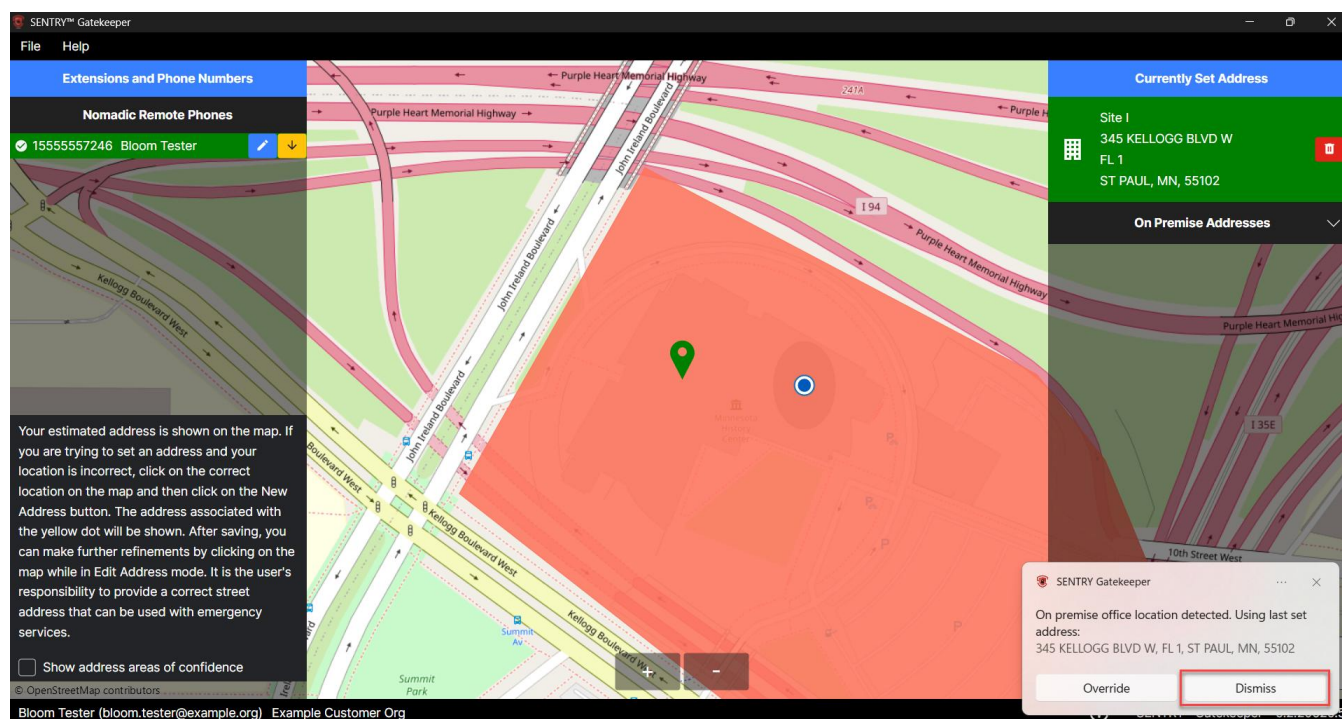


Figure 147

If a **VDI-supported SENTRY™ Gatekeeper user WITH Location Services** enabled moves to work at a new workspace throughout the same building of their on-premise work environment during their working hours, **SENTRY™ Gatekeeper will prompt the user to provision a new location**. The user can either select an option from the **On Premise Addresses** list which reflects their updated location within the building / site they are working in, OR they can click the **“Add Address”** button from the toast message and manually enter an updated address. (As long as the user remains within the same building / site, selecting an option from the **On Premise Addresses** list will likely be the most convenient and intuitive option.)

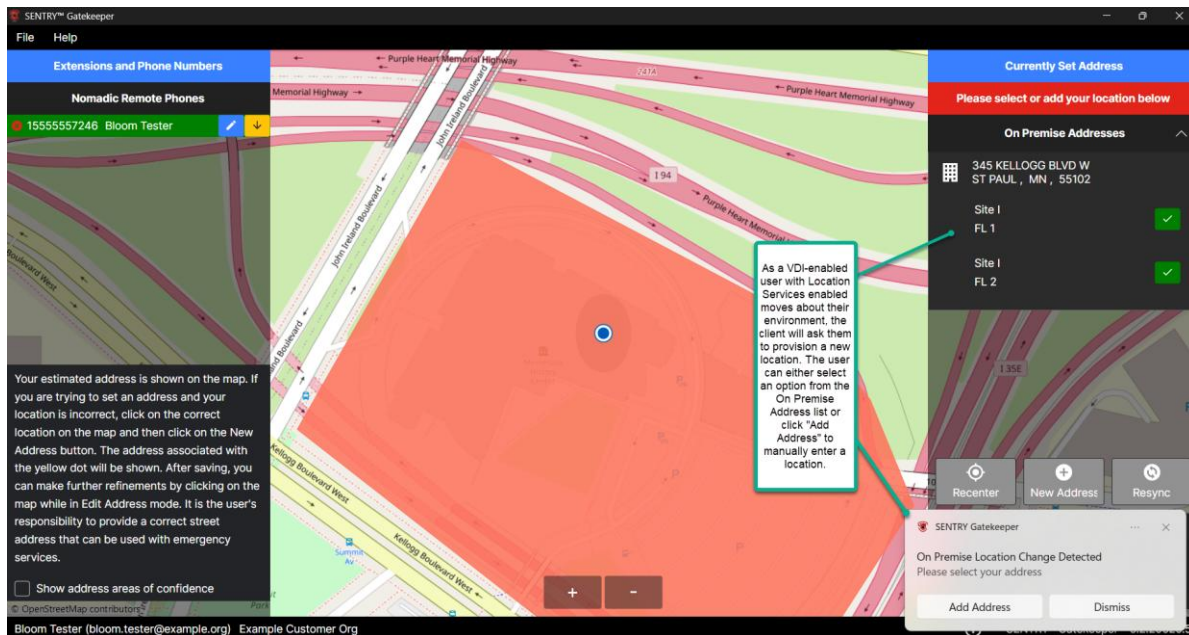


Figure 148

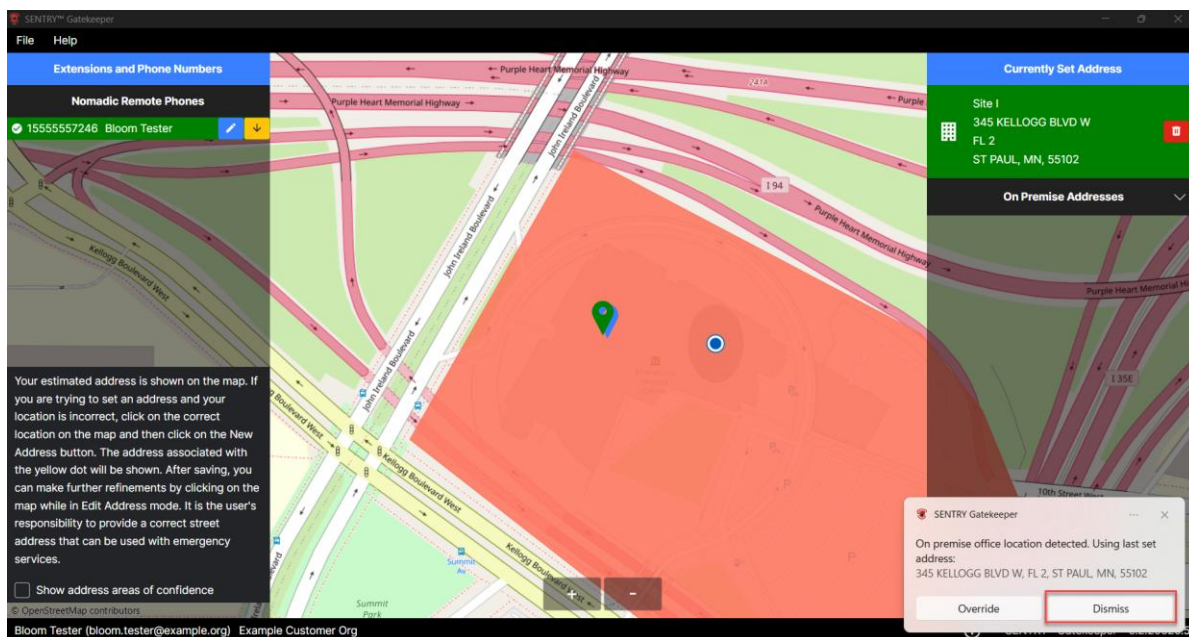


Figure 149

SENTRY™ GATEKEEPER TROUBLESHOOTING GUIDE

1. As a rule, SENTRY™ Gatekeeper users must have **Location Services** and **“Let apps access your location”** enabled on their device under **“Privacy and security > Location”** for the SENTRY™ Gatekeeper application to function.

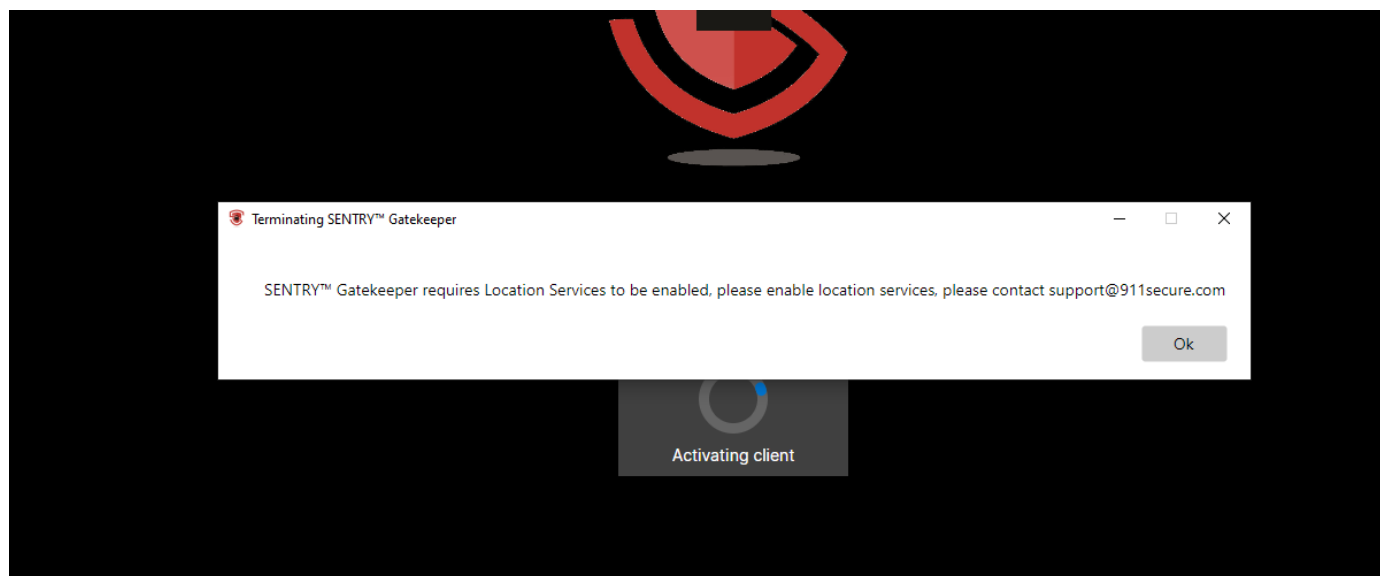


Figure 150

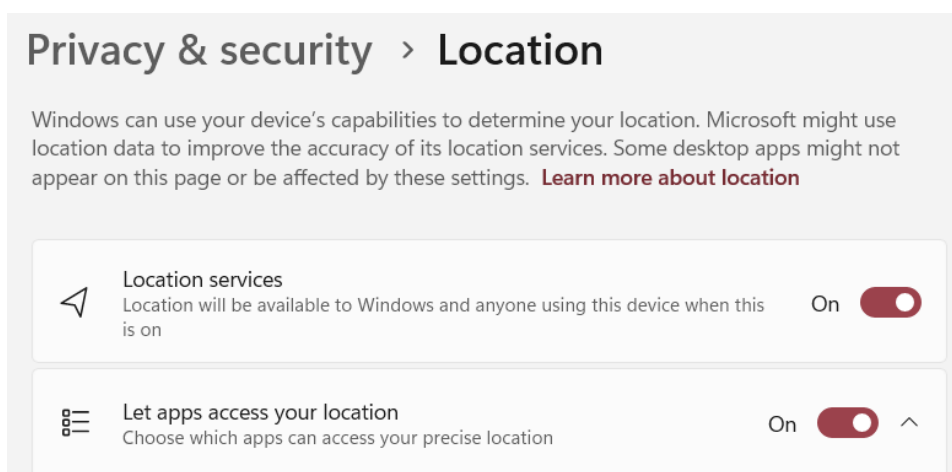


Figure 151

2. **“_ERR-JAB-0024: Address could not be validated.”** This error states that the address is not valid. This error can occur for many reasons such as a new location has not yet been verified as a valid US Postal service address and / or has not been entered into the Master Street Address Guide. Please make sure you have entered a valid address including the city, state, and zip code. It may be helpful to verify the address using <https://www.google.com/maps>. If you have verified the address is correct and valid but Gatekeeper will not accept it, please email support@911secure.com with details of the address. 911

Secure will follow up with the necessary research and get the address verified and added to the US Master Street Address Guide.

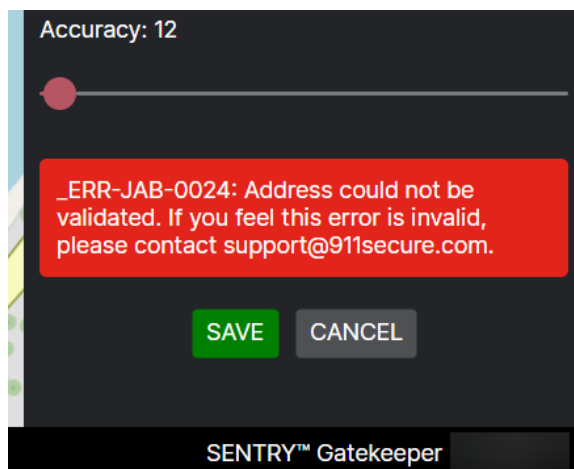


Figure 152

3. **Profile: Your user does not have the required SENTRY™ Gatekeeper license.** This error is stating that your user account has not been assigned a SENTRY™ Gatekeeper license. **Please contact your Administrator.**

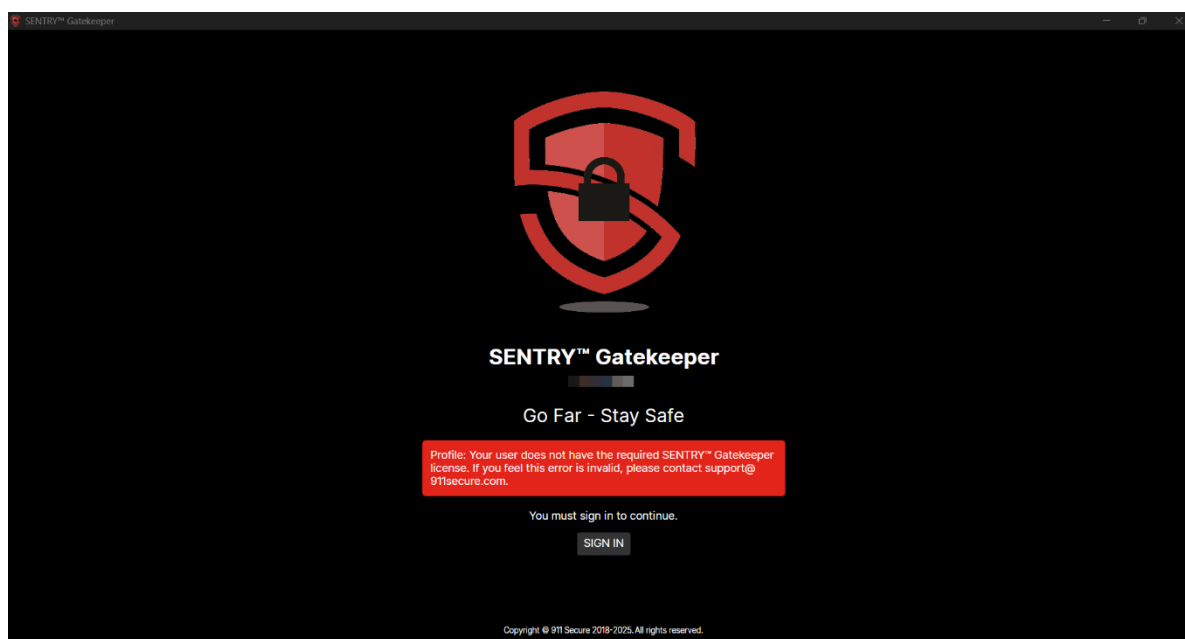


Figure 153

4. **Your ELIN / DID or Extension is incorrect.** If, for whatever reason, you see that your set DID (or Extension, if your organization uses SENTRY™ Cloud Enterprise) is incorrect, **please contact your Administrator.** (This may have resulted from accidentally entering in the wrong DID (or Extension) when completing the self-registration process.)

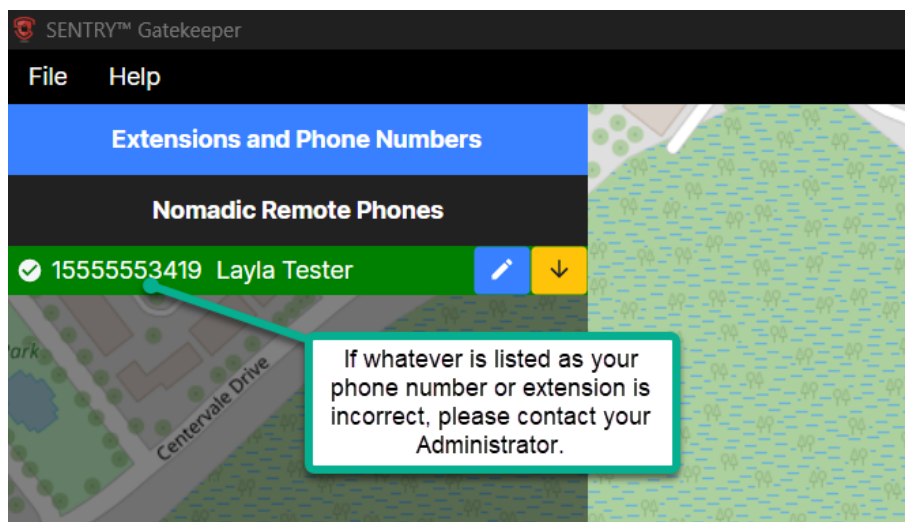


Figure 154

5. **ERR-MEL-5 – Invalid. Some inputs are missing or incorrect, please check your inputs and try again.** While this error is less common than the typical Geocode error, it can still occur. This error may present itself for several reasons, including counties being redrawn. When receiving this error, you may be able to validate your address, but not fully set/provision it. If you receive this error, please make sure you have entered a valid address including the city, state, and zip code. It may be helpful to verify the address using <https://www.google.com/maps>. If you have verified the address is correct and valid but Gatekeeper will not accept it, please email support@911secure.com with details of the address. 911 Secure will follow up with the necessary research and get the address verified and added to the US Master Street Address Guide (MSAG).
6. **You are prompted to load a license file.** The older version of SENTRY™ Gatekeeper (v1.3) required the use of a .json license file that SENTRY™ Gatekeeper v2 and up does not need. If you are ever prompted to load a license file, check to see if you still have an older version of Gatekeeper installed on your personal computer.

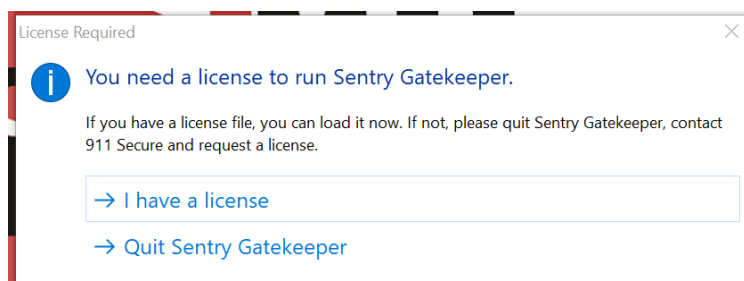


Figure 155

7. **You are re-prompted to agree to the User Acceptance terms.** – If the SENTRY™ Cloud Administrators of an organization make updates to the **User Acceptance** text, then the next time SENTRY™ Gatekeeper users log into the SENTRY™ Gatekeeper application, they must **read and re-accept the new terms** of the agreement prompt.

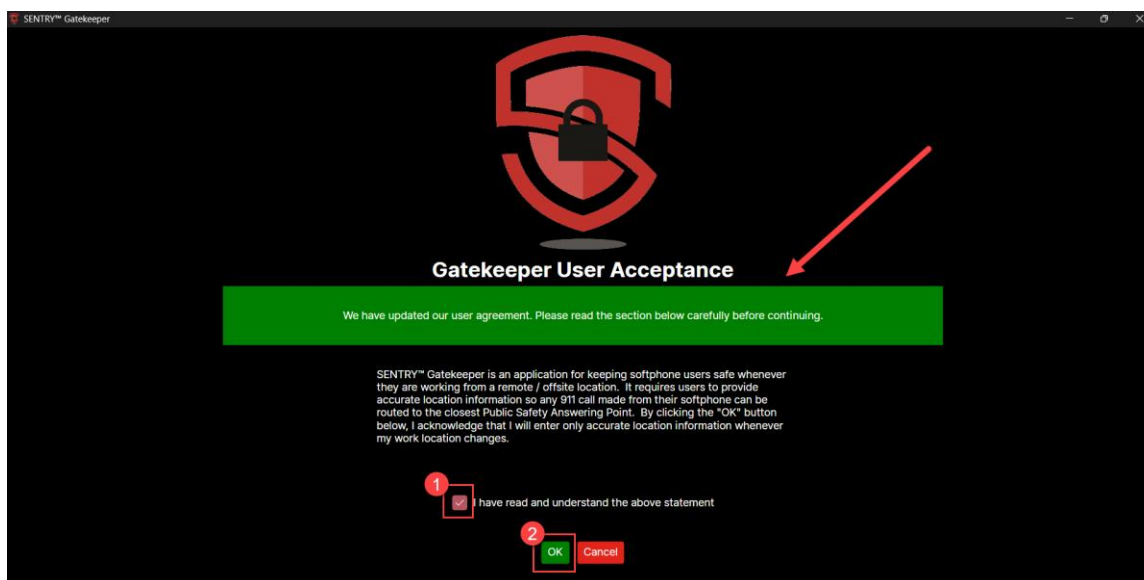


Figure 156

8. **SENTRY™ Gatekeeper requires DLR to be enabled for your organization, please contact support@911secure.com.** – If your organization does not use DLR (Dynamic Location Routing) as part of its E911 solution, then remote workers cannot use SENTRY™ Gatekeeper v5. Please contact support for further questions and details.

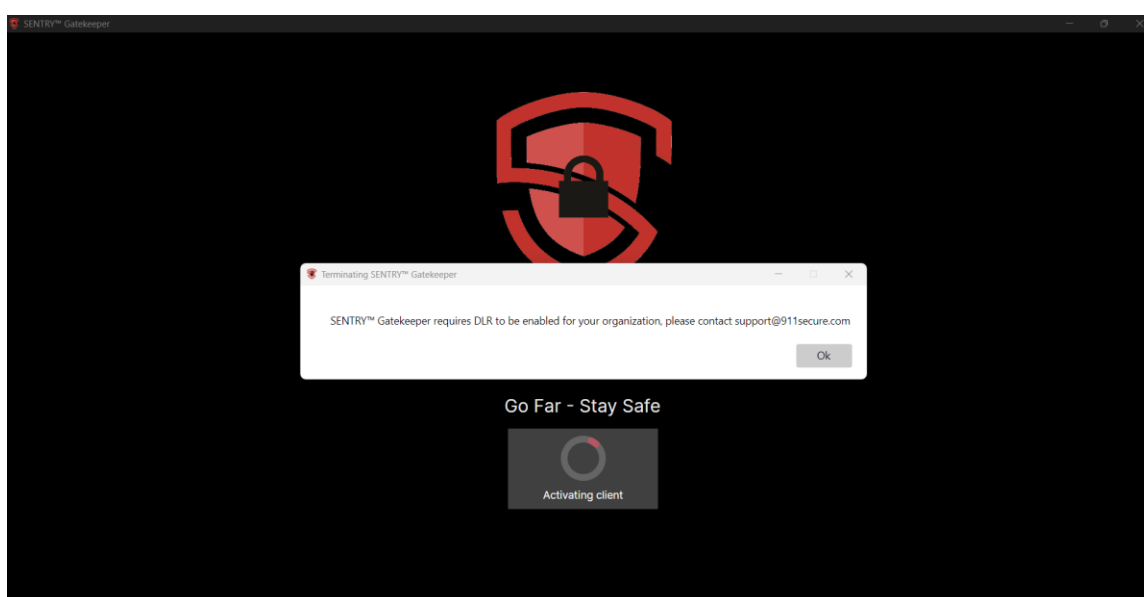


Figure 157

SENTRY™ CLOUD AND SENTRY™ GATEKEEPER WHITELISTING URLS

WHITELISTING REQUIRED SENTRY™ CLOUD URLS

For organizations using SENTRY™ Gatekeeper, please ensure that all **URLs** listed below are **whitelisted** and are not blocked by any type of security or firewalls. You do NOT need to “test” them by trying to open the URLs in a web browser. Additionally, please ensure that your environment does not block web sockets. If your environment blocks web sockets, you will not be able to properly access the data housed in **SENTRY™ Cloud**.

The URLs listed below are APIs used by **SENTRY™ Cloud** and are not meant to be, and cannot be, opened in a web browser.:

- <https://sentry-cloud.911secure.com/>
- <https://identity-sentry-cloud.911secure.com/>
- <https://sentrycloud911secure.blob.core.windows.net/>
- <https://api-sentry-cloud.911secure.com>
- <https://www.googleapis.com/geolocation/v1/geolocate>
- <https://maps.googleapis.com/maps/api/geocode/json>
- <https://developers.google.com/maps/gmp-domains>
- *.911secure.com/

The URLs listed below can be tested, as you can navigate to them to help check whether you are letting https calls pass through firewalls. A successful check will result in seeing a blank webpage populated only by the word “**Healthy**”.

- <https://api-sentry-cloud.911secure.com/health>
- <https://identity-sentry-cloud.911secure.com/health>
- <https://sentry-cloud.911secure.com/health>

WHITELISTING REQUIRED SENTRY™ GATEKEEPER URLS

To use the **SENTRY™ Gatekeeper** application, please ensure that all **URLs** listed below are **whitelisted** and are not blocked by any type of security or firewalls. You do NOT need to “test” them by trying to open the URLs in a web browser.

The URLs listed below are APIs used by SENTRY™ Gatekeeper and are not meant to be, and cannot be, opened in a web browser:

- <https://www.googleapis.com/geolocation/v1/geolocate>
- <https://maps.googleapis.com/maps/api/geocode/json>
- <https://developers.google.com/maps/gmp-domains>
- <https://tile.openstreetmap.org>
- https://*.tiles.virtualearth.net
- <https://atlas.microsoft.com/>

For additional information or assistance with the SENTRY™ applications, please contact 911 Secure via email at support@911secure.com, or via phone at (213) 425-2050.