UrbanUtilities

WaterTalk
Using Multi-Factor Authentication (MFA)

Securing your WaterTalk account access

July 2024

Overview

Multi-Factor Authentication (MFA) is coming to WaterTalk from 1 July 2024.

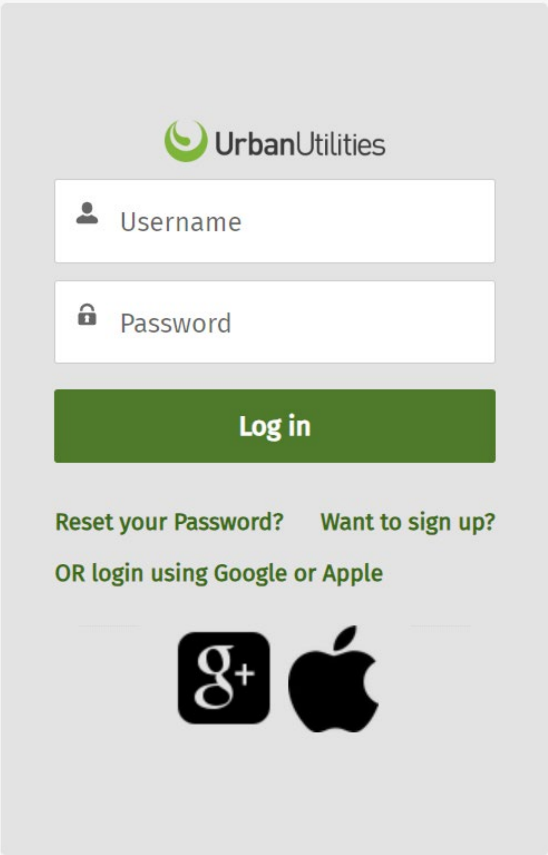
MFA enhances the security of the login process by requiring users to verify their identity with two or more pieces of evidence (or “factors”) to prove they are who they say they are.

The following information will guide you to set up your preferred option for extra cyber security.

WaterTalk is hosted on the Salesforce platform.

When you are setting up MFA, you will see messaging from salesforce (and not Urban Utilities).

The new Login experience to set up MFA



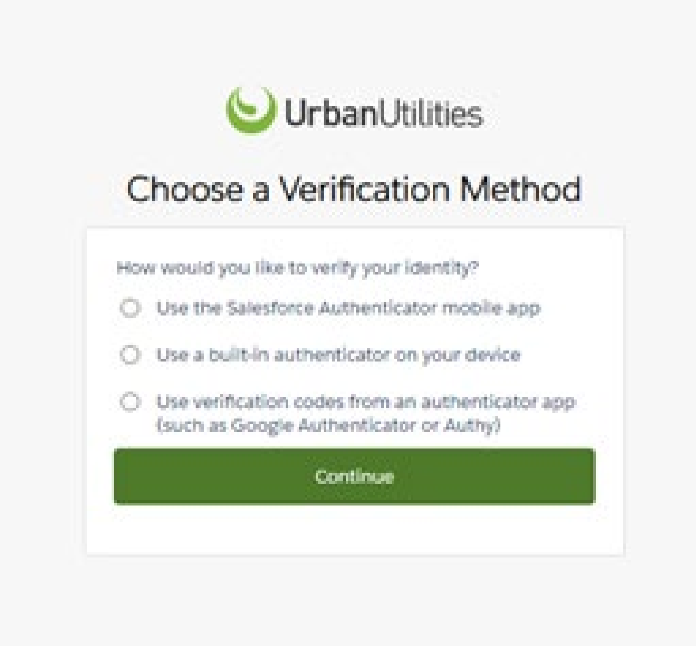
UrbanUtilities

Username

Password

Reset your Password? Want to sign up?

OR login using Google or Apple



UrbanUtilities

Choose a Verification Method

How would you like to verify your identity?

○ Use the Salesforce Authenticator mobile app

○ Use a built-in authenticator on your device

○ Use verification codes from an authenticator app (such as Google Authenticator or Authy)

Choosing your preferred MFA method

If you know which MFA you prefer to use, select it from the list below and start setting it up now.

If you're not yet sure, read through the following pages to see which method will suit you.

I would like to use the:

- Salesforce Authenticator app
- Third-Party authenticator app (eg Microsoft Authenticator, Authy, or Google Authenticator)
- Built in authenticator on my device (laptop, tablet, computer)

Using the Salesforce Authenticator app for MFA

Salesforce Authenticator

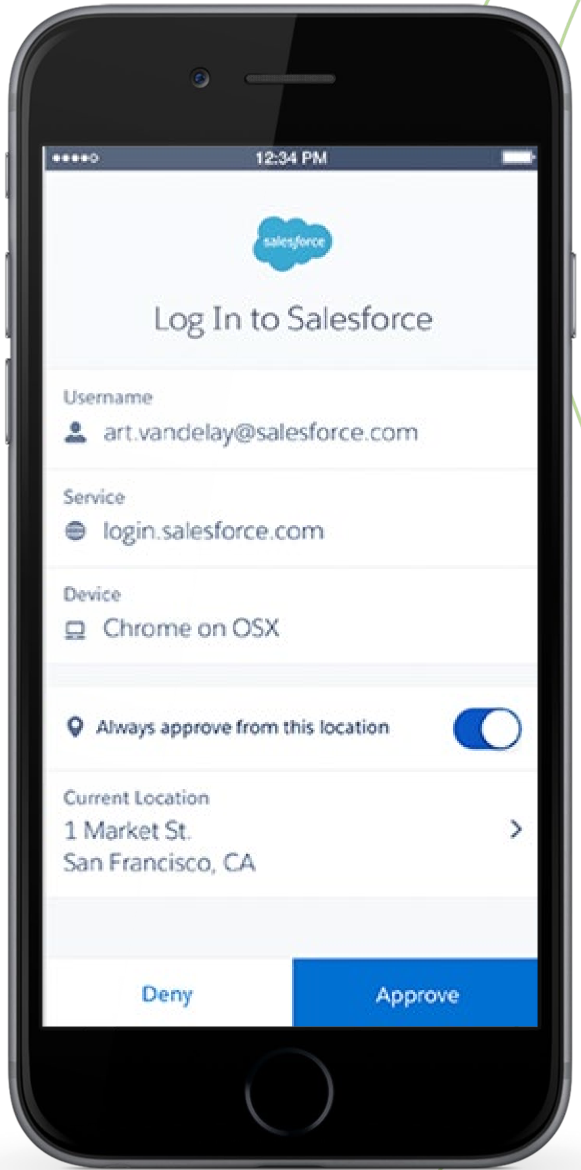
Fast, frictionless, free authentication

Salesforce Authenticator is a mobile app that can be used with MFA for the <<Developer Services Portal>>.

Salesforce Authenticator tells you:

- What **action** needs to be approved
- What **user** is requesting the action
- From which **service** is the requested action coming
- What **device** the user is using
- From what **location** would the user approve or deny this request

With this information, you can simply tap the "Approve" or "Deny" button to execute the decision, completing authentication quickly as part of your login process.



Log In to Salesforce

Username
art.vandelay@salesforce.com

Service
login.salesforce.com

Device
Chrome on OSX

Always approve from this location

Current Location
1 Market St.
San Francisco, CA

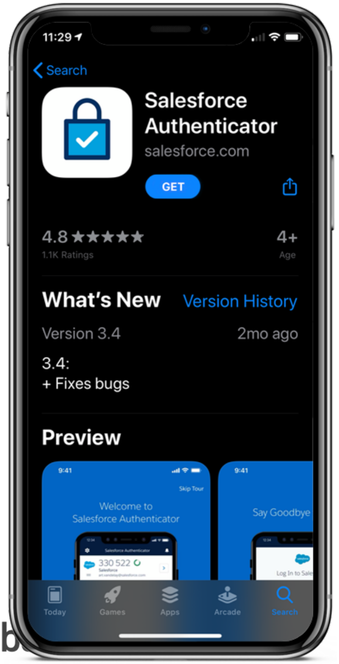
Salesforce Authenticator: Register the App

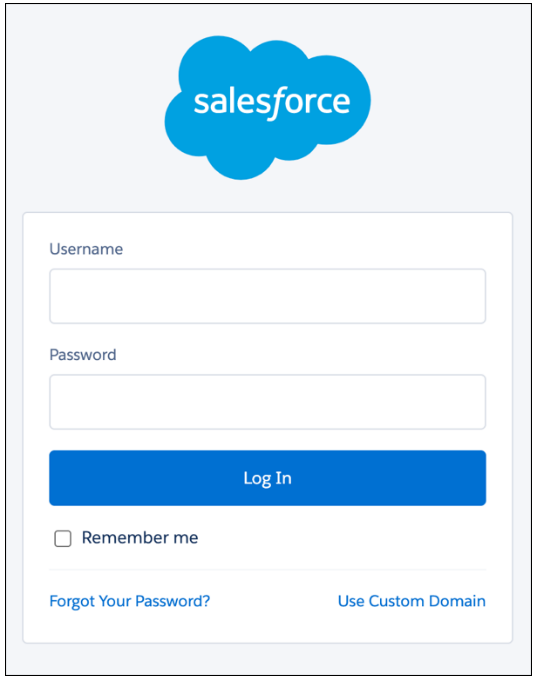
1. Install Salesforce Authenticator on your mobile device. It's available from the Apple App Store or Google Play.

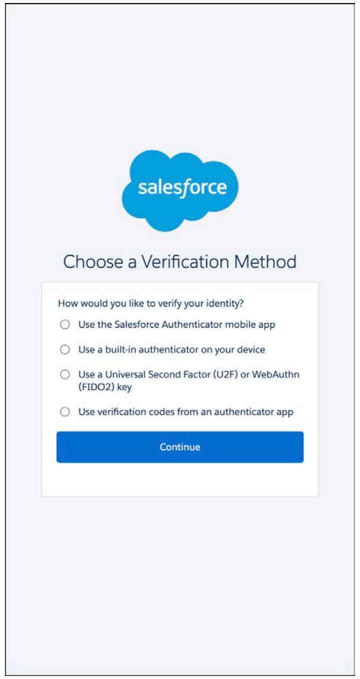
2. On your computer, log in to your account. You may be prompted to verify your identity with a one-time passcode via email or text message.

3. Select **Use the Salesforce Authenticator mobile app**.

4. The Connect Salesforce Authenticator screen displays.







Choose a Verification Method

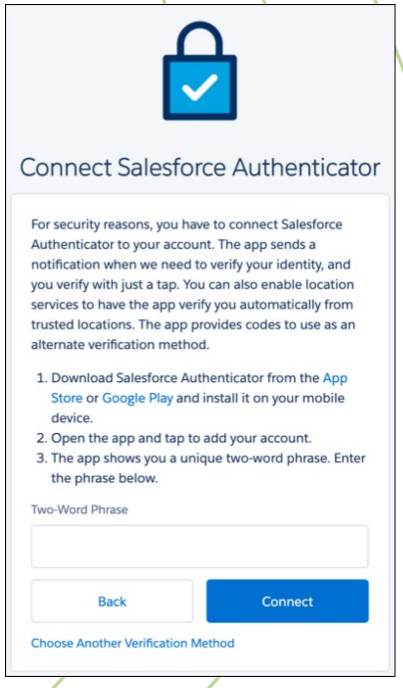
How would you like to verify your identity?

○ Use the Salesforce Authenticator mobile app

○ Use a built-in authenticator on your device

○ Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) key

○ Use verification codes from an authenticator app



Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the App Store or Google Play and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

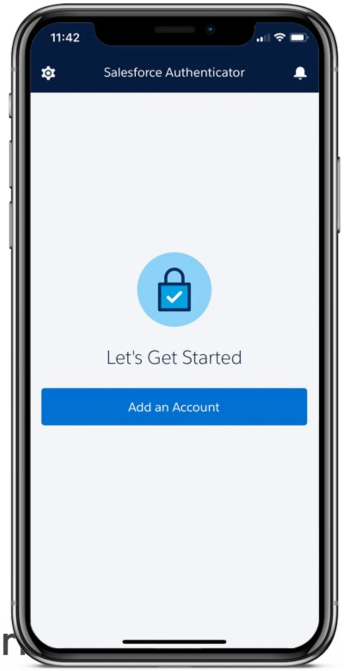
Salesforce Authenticator: Register the App *continued*

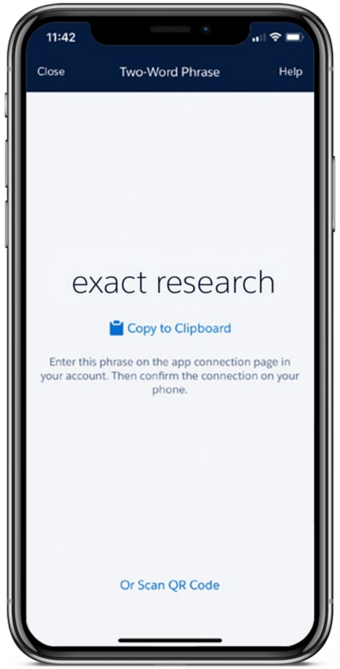
5. On your mobile device, open Salesforce Authenticator and tap **Add an Account**.

6. The app displays a two-word phrase.

7. On your computer, enter the phrase in the Two-Word Phrase field. Then click **Connect**.

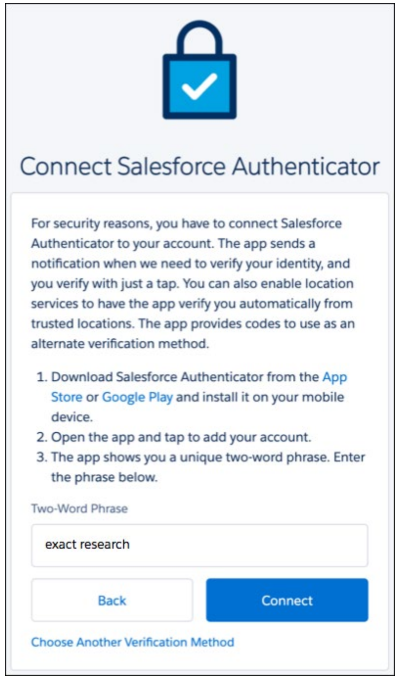
8. In Salesforce Authenticator, verify that the connection details are correct, then tap **Connect**.





exact research

Enter this phrase on the app connection page in your account. Then confirm the connection on your phone.

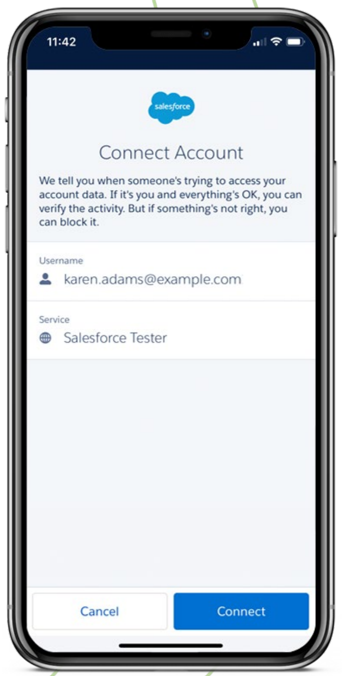


Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the App Store or Google Play and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase: exact research



Connect Account

We tell you when someone's trying to access your account data. If it's you and everything's OK, you can verify the activity. But if something's not right, you can block it.

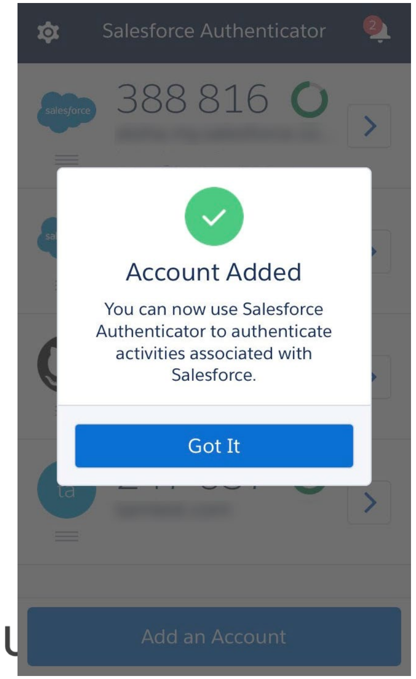
Username: karen.adams@example.com

Service: Salesforce Tester

Salesforce Authenticator: Register the App *continued*

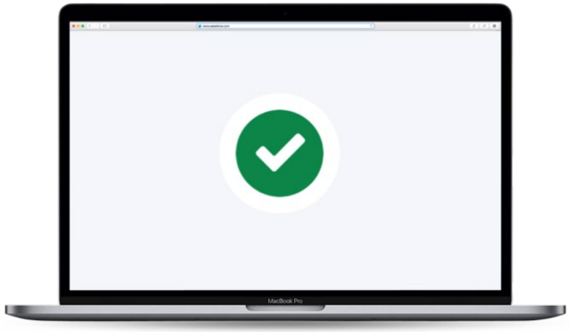
9. And that’s it! You’ve successfully connected Salesforce Authenticator to your account.

10. And you finish logging in.
Log out and log back in to use it for the first time.



Account Added

You can now use Salesforce Authenticator to authenticate activities associated with Salesforce.



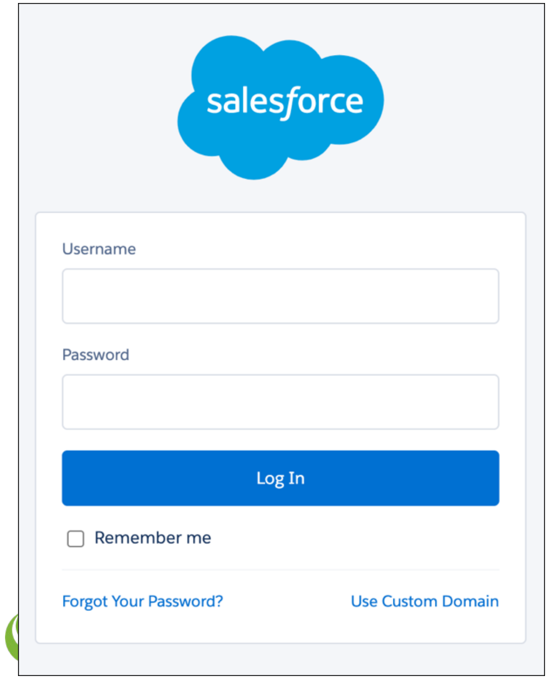
Salesforce Authenticator: Logging in

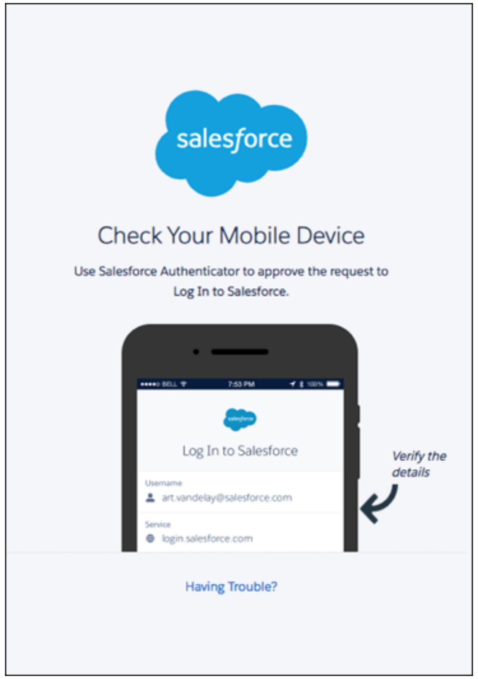
1. On the login screen, enter your username and password, as usual.

2. Salesforce prompts you to use Salesforce Authenticator to verify your identity.

3. On your mobile device, respond to the push notification to open Salesforce Authenticator.

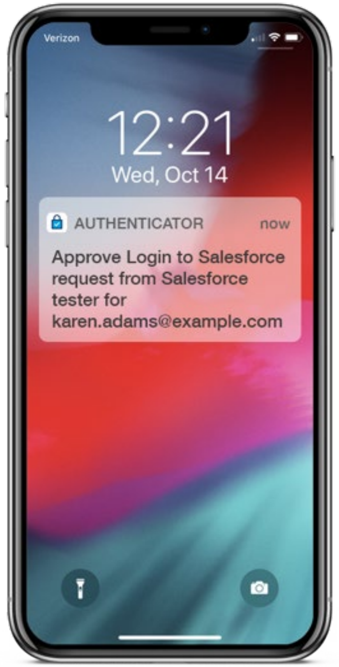
4. In Salesforce Authenticator, verify that the login request is from you, then tap **Approve**.



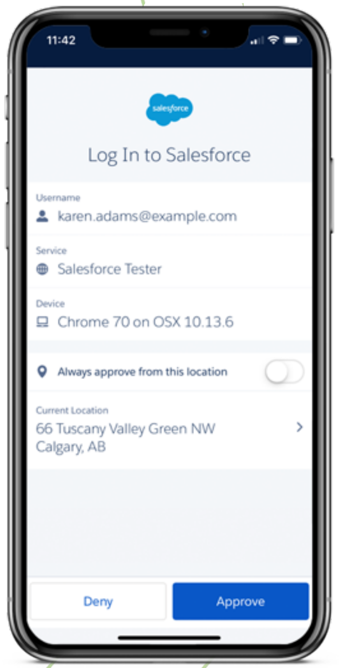


Check Your Mobile Device

Use Salesforce Authenticator to approve the request to Log In to Salesforce.



Approve Login to Salesforce request from Salesforce tester for karen.adams@example.com



Username: karen.adams@example.com

Service: Salesforce Tester

Device: Chrome 70 on OSX 10.13.6

Always approve from this location

Current Location: 66 Tuscany Valley Green NW Calgary, AB

Using the Third-Party Authenticator for MFA

UrbanUtilities

Third-Party Authenticator Apps

You can use any authenticator app that generates temporary codes based on the OATH time-based one-time password (TOTP) algorithms (specified in RFC 6238).

To log in with this type of verification method, get a code from the app, then enter that code during the login process.

TOTP apps don’t require a data or internet connection.

Widely-Used Apps

Microsoft Authenticator

Authy

Google Authenticator

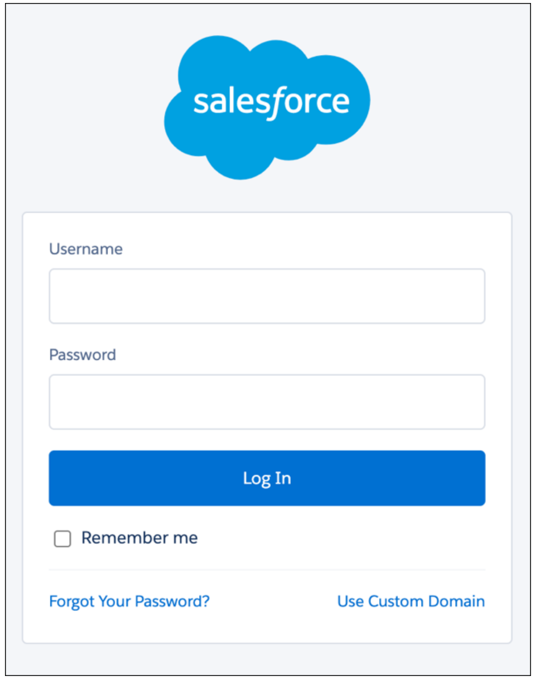
Third-Party Authenticator Apps: Register an App

1. Install a third-party authenticator on your mobile device. Apps are available from the Apple App Store or Google Play.

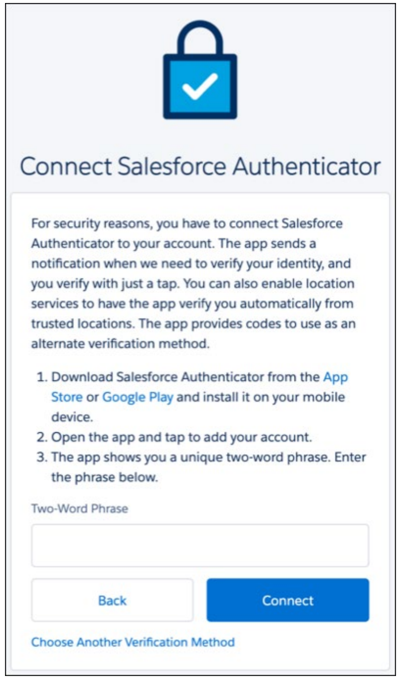
Download on the App Store

GET IT ON Google Play

2. On your computer, log in to your account. You may be prompted to verify your identity with a one-time passcode via email or text message.



3. The Connect Salesforce Authenticator screen displays by default. Click **Choose Another Verification Method**.

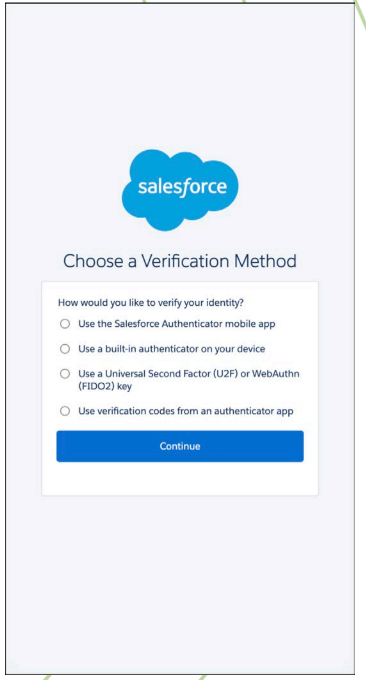

Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the App Store or Google Play and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase

4. Select **Use verification codes from an authenticator app**.



Choose a Verification Method

How would you like to verify your identity?

○ Use the Salesforce Authenticator mobile app

○ Use a built-in authenticator on your device

○ Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) key

○ Use verification codes from an authenticator app

UrbanUtilities

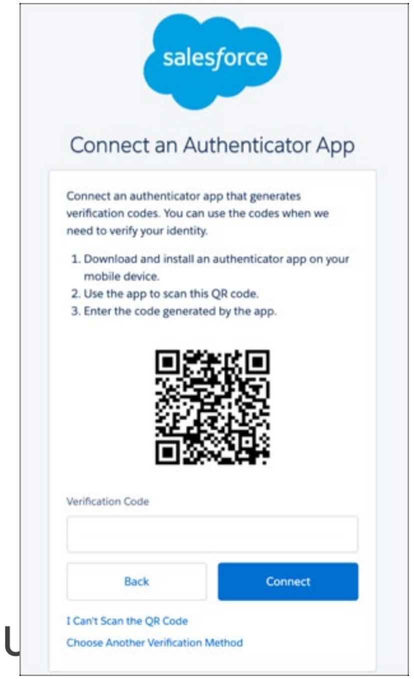
Third-Party Authenticator Apps: Register an App *continued*

5. The Connect an Authenticator app screen displays.

6. On your mobile device, open your authenticator app and select to add a new account.

7. Use the authenticator app to scan the QR barcode that's displayed on your computer.

8. The authenticator app is connected to your account. The app automatically starts generating time-based one-time passcodes.

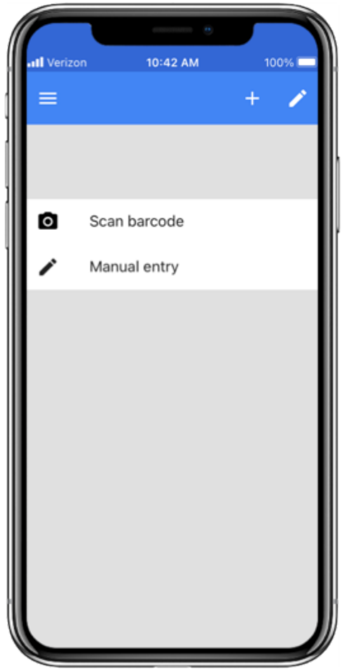


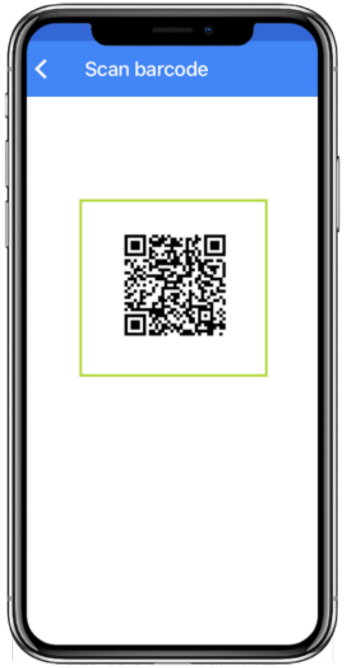
Connect an Authenticator App

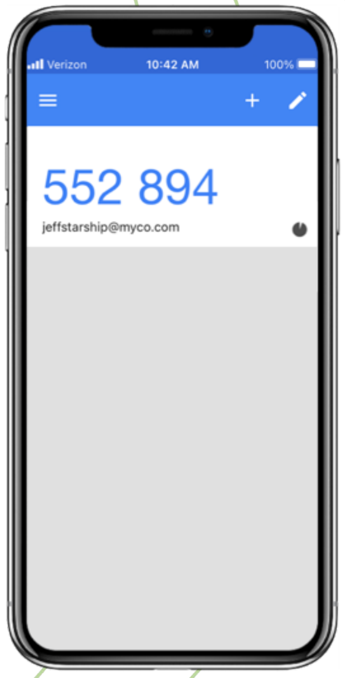
Connect an authenticator app that generates verification codes. You can use the codes when we need to verify your identity.

1. Download and install an authenticator app on your mobile device.
2. Use the app to scan this QR code.
3. Enter the code generated by the app.

Verification Code



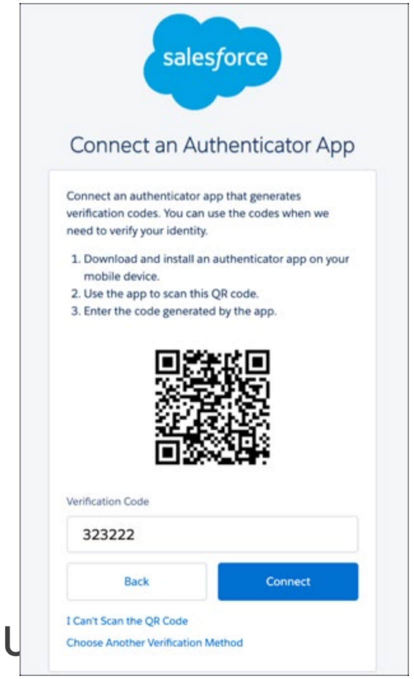




Third-Party Authenticator Apps: Register an App *continued*

9. On your computer, enter a code generated by the authenticator app in the Verification Code field, then click **Connect**.

10. And that's it! You've successfully connected your third-party authenticator app to your account, and you finish logging in.



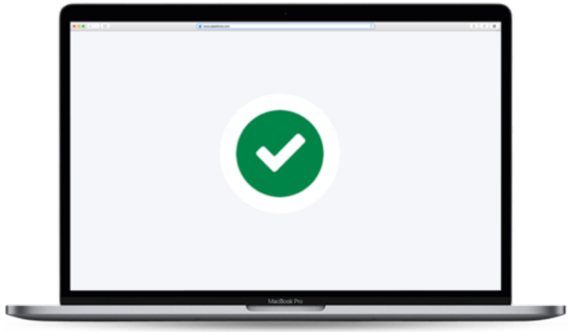
Connect an Authenticator App

Connect an authenticator app that generates verification codes. You can use the codes when we need to verify your identity.

1. Download and install an authenticator app on your mobile device.
2. Use the app to scan this QR code.
3. Enter the code generated by the app.

Verification Code

323222



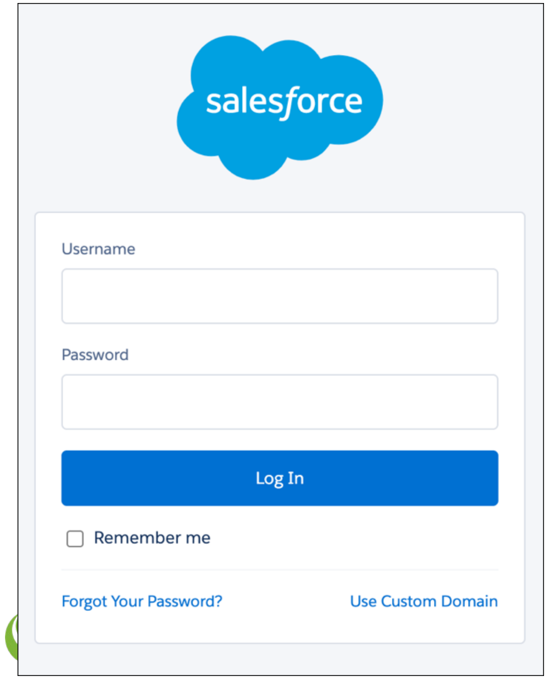
Third-Party Authenticator Apps: Logging in

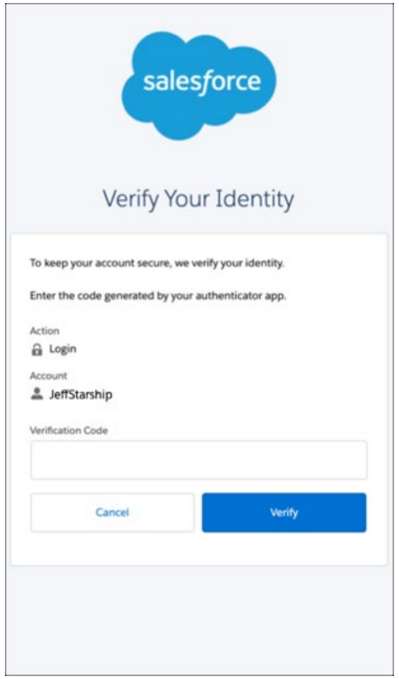
1. On the login screen, enter your username and password, as usual.

2. You’re prompted to enter a code from your authenticator app to verify your identity.

3. On your mobile device, open your authenticator app to get a time-based one-time passcode.

4. On your computer, enter the code generated by the authenticator app, then click **Verify**. You’re successfully logged in to your account.





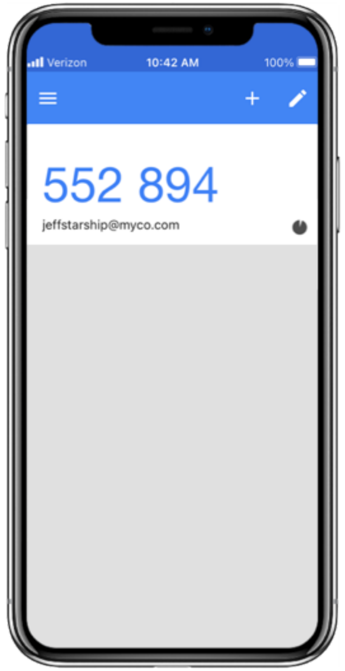
To keep your account secure, we verify your identity.

Enter the code generated by your authenticator app.

Action: Login

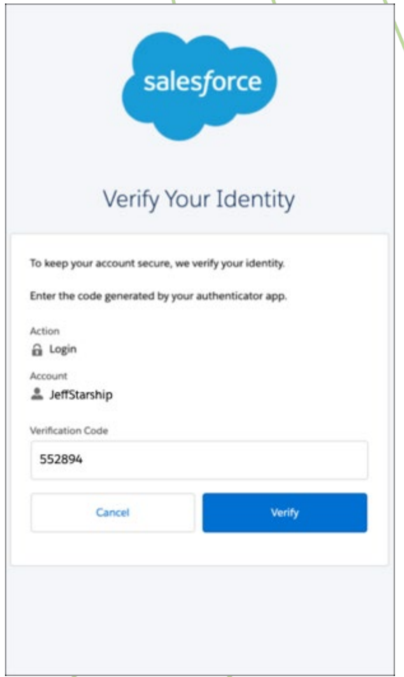
Account: JeffStarship

Verification Code:



552 894

jeffstarship@myco.com



To keep your account secure, we verify your identity.

Enter the code generated by your authenticator app.

Action: Login

Account: JeffStarship

Verification Code: 552894

Using the
Built in Authenticator
for MFA

UrbanUtilities

Built-In Authenticators

Easy MFA verification using a desktop or mobile device’s built-in authenticator service, such as Windows Hello, Touch ID, or Face ID

- Verify identity with fingerprint, iris, or facial recognition scan
- No apps needed
- Strong public-key cryptography that’s unique to the user’s account
- Resistant to malware, phishing, and man-in-the-middle attacks

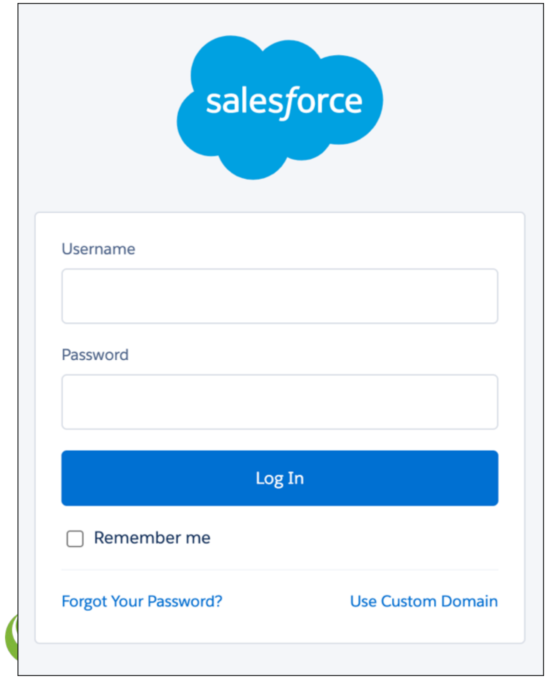
Logging in with this type of verification method is easy!

1. Enter a username and password
2. Use your built-in authenticator to provide your biometric identifier, PIN, or password

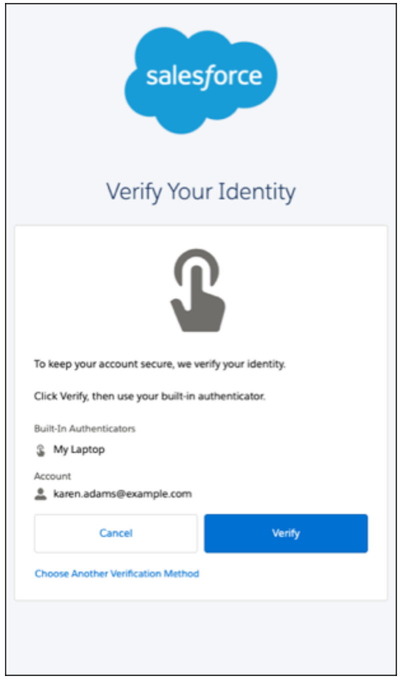
- User’s device, operating system, and browser must support the FIDO2 WebAuthn standard.
- Built-in authenticator service must be enabled and set up to verify a user’s identity via a biometric, PIN, or password.
- For biometric authentication, user’s device must include a supported fingerprint, iris, or facial scanner.
- Works only for logins to the device where the built-in authenticator exists.

Built-In Authenticators: Logging In

1. In a supported browser, go to the login screen and enter your username and password, as usual.



2. When you see the Verify Your Identity screen, click **Verify**.



Verify Your Identity

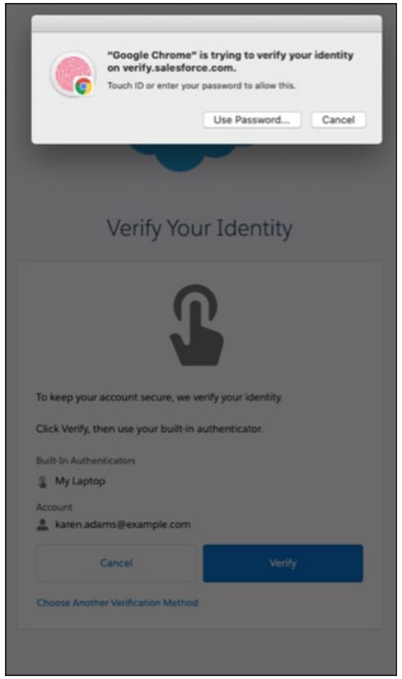
To keep your account secure, we verify your identity.

Click Verify, then use your built-in authenticator.

Built-In Authenticators: My Laptop

Account: karen.adams@example.com

3. When prompted, enter the identifier that you set up for your built-in authenticator, such as a fingerprint, facial scan, or PIN.



"Google Chrome" is trying to verify your identity on verify.salesforce.com.

Touch ID or enter your password to allow this.

Verify Your Identity

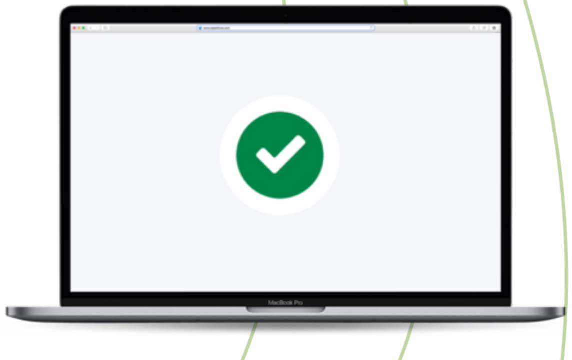
To keep your account secure, we verify your identity.

Click Verify, then use your built-in authenticator.

Built-In Authenticators: My Laptop

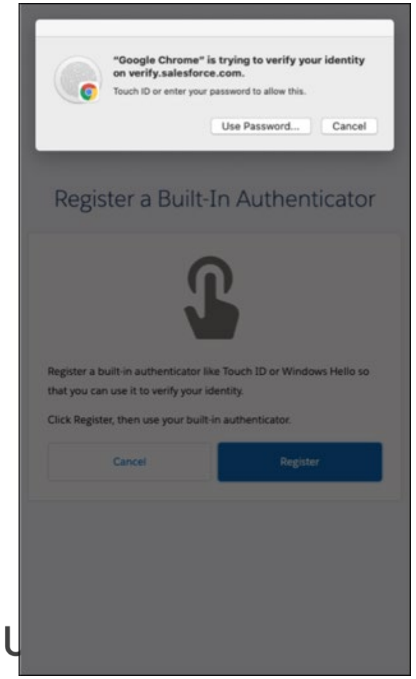
Account: karen.adams@example.com

4. You're successfully logged in.



Built-In Authenticators: Register an Authenticator *continued*

5. When prompted, enter the identifier that you set up for your built-in authenticator, such as a fingerprint, facial scan, or PIN.



"Google Chrome" is trying to verify your identity on verify.salesforce.com.

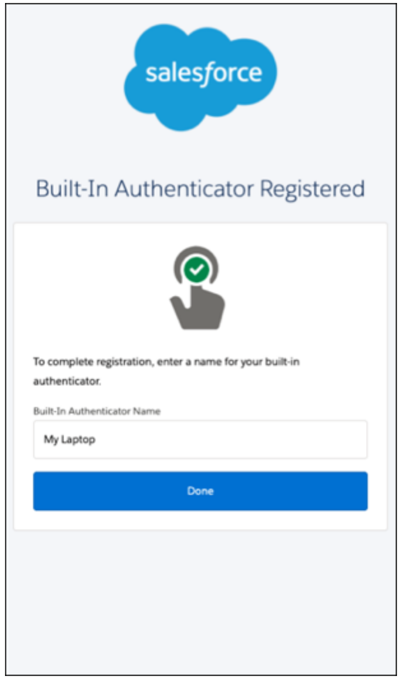
Touch ID or enter your password to allow this.

Register a Built-In Authenticator

Register a built-in authenticator like Touch ID or Windows Hello so that you can use it to verify your identity.

Click Register, then use your built-in authenticator.

6. Assign a name to your built-in authenticator, then click **Done.** And that's it! You've connected your built-in authenticator and you finish logging in.



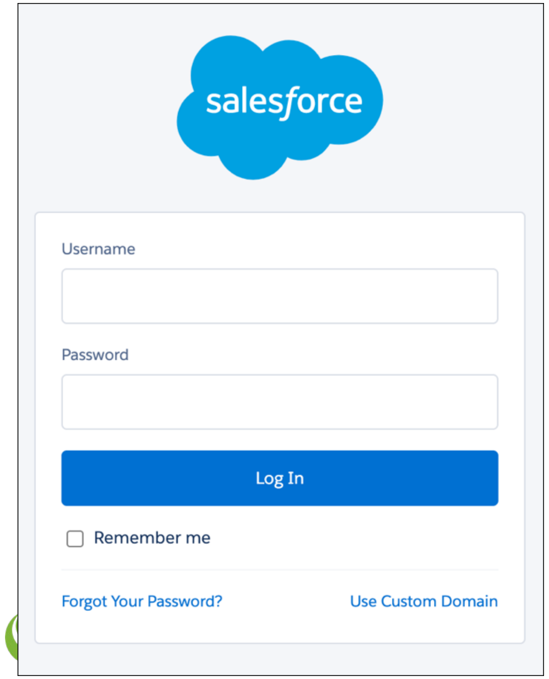
Built-In Authenticator Registered

To complete registration, enter a name for your built-in authenticator.

Built-In Authenticator Name: My Laptop

Built-In Authenticators: Logging In

1. In a supported browser, go to the login screen and enter your username and password, as usual.



Username

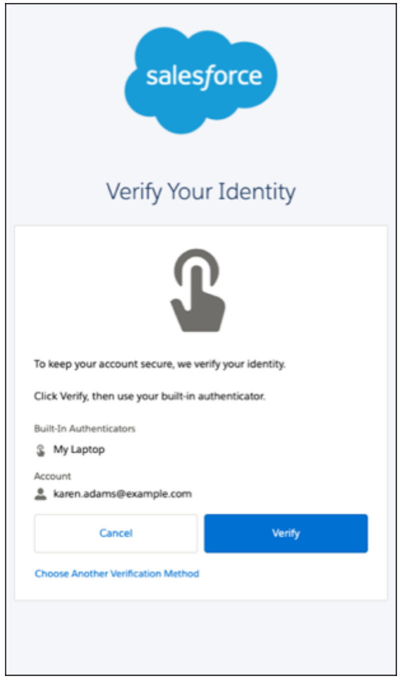
Password

Log In

□ Remember me

Forgot Your Password? Use Custom Domain

2. When you see the Verify Your Identity screen, click **Verify**.



Verify Your Identity

To keep your account secure, we verify your identity.

Click Verify, then use your built-in authenticator.

Built-In Authenticators

My Laptop

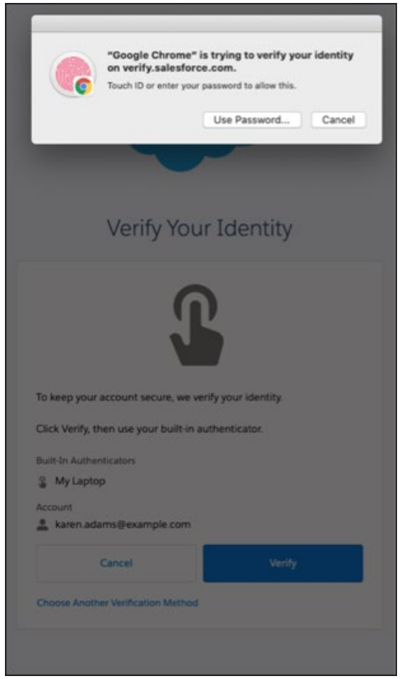
Account

karen.adams@example.com

Cancel Verify

Choose Another Verification Method

3. When prompted, enter the identifier that you set up for your built-in authenticator, such as a fingerprint, facial scan, or PIN.



"Google Chrome" is trying to verify your identity on verify.salesforce.com.

Touch ID or enter your password to allow this.

Use Password... Cancel

Verify Your Identity

To keep your account secure, we verify your identity.

Click Verify, then use your built-in authenticator.

Built-In Authenticators

My Laptop

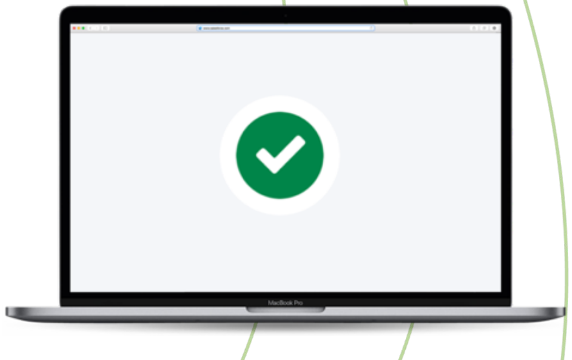
Account

karen.adams@example.com

Cancel Verify

Choose Another Verification Method

4. You're successfully logged in.



Experiencing difficulties?

Contact the WaterTalk team on

WaterTalk@urbanutilities.com.au

UrbanUtilities