Two-factor authentication for Apple ID

Two-factor authentication is an extra layer of security for your Apple ID designed to ensure that you're the only person who can access your account, even if someone knows your password.

How it works	Manage your account	What if I forget my password? and other questions

How it works

With two-factor authentication, your account can only be accessed on devices you trust, like your iPhone, iPad, or Mac. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information—your password and the six-digit verification code that's automatically displayed on your trusted devices. By entering the code, you're verifying that you trust the new device. For example, if you have an iPhone and are signing into your account for the first time on a newly purchased Mac, you'll be prompted to enter your password and the verification code that's automatically displayed on your iPhone.

Because your password alone is no longer enough to access your account, two-factor authentication dramatically improves the security of your Apple ID and all the personal information you store with Apple.

Once signed in, you won't be asked for a verification code on that device again unless you sign out completely, erase the device, or need to change your password for security reasons. When you sign in on the web, you can choose to trust your browser, so you won't be asked for a verification code the next time you sign in from that computer.

Trusted devices

A trusted device is an iPhone, iPad, or iPod touch with iOS 9 and later, or a Mac with OS X El Capitan and later that you've already signed in to using two-factor authentication. It's a device we know is yours and that can be used to verify your identity by displaying a verification code from Apple when you sign in on a different device or browser.

Trusted phone numbers

A trusted phone number is a number that can be used to receive verification codes by text message or automated phone call. You must verify at least one trusted phone number to enroll in two-factor authentication.

You should also consider verifying an additional phone number you can access, such as a home phone, or a number used by a family member or close friend. You can use this number if you temporarily can't access your primary number or your own devices.

Verification codes

A verification code is a temporary code sent to your trusted device or phone number when you sign in to a new device or browser with your Apple ID. You can also get a verification code from Settings on your trusted device.

A verification code is different from the device passcode you enter to unlock your iPhone, iPad, or iPod touch.

Set up two-factor authentication for your Apple ID

Two-factor authentication is available to iCloud and iTunes users with at least one device that's using the latest iOS or macOS. Learn more.

You can follow these steps on your iPhone, iPad, or iPod touch to turn on two-factor authentication.

① Turn on two-factor authentication in Settings

If you're using iOS 10.3 or later:

1. Go to Settings > [your name] > Password & Security.
2. Tap Turn On Two-Factor Authentication.
3. Tap Continue.

If you're using iOS 10.2 or earlier:

1. Go to Settings > iCloud.
2. Tap your Apple ID > Password & Security.
3. Tap Turn On Two-Factor Authentication.
4. Tap Continue.

You might be asked to answer your Apple ID security questions.
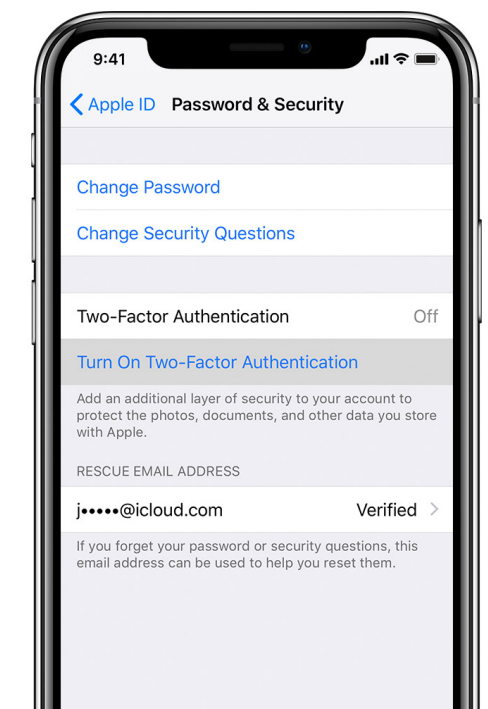
② Enter and verify your trusted phone number

Enter the phone number where you want to receive verification codes when you sign in. You can choose to receive the codes by text message or automated phone call.

When you tap Next, Apple sends a verification code to the phone number you provided.

Enter the verification code to verify your phone number and turn on two-factor authentication.

Follow these steps on your Mac with OS X El Capitan or later:
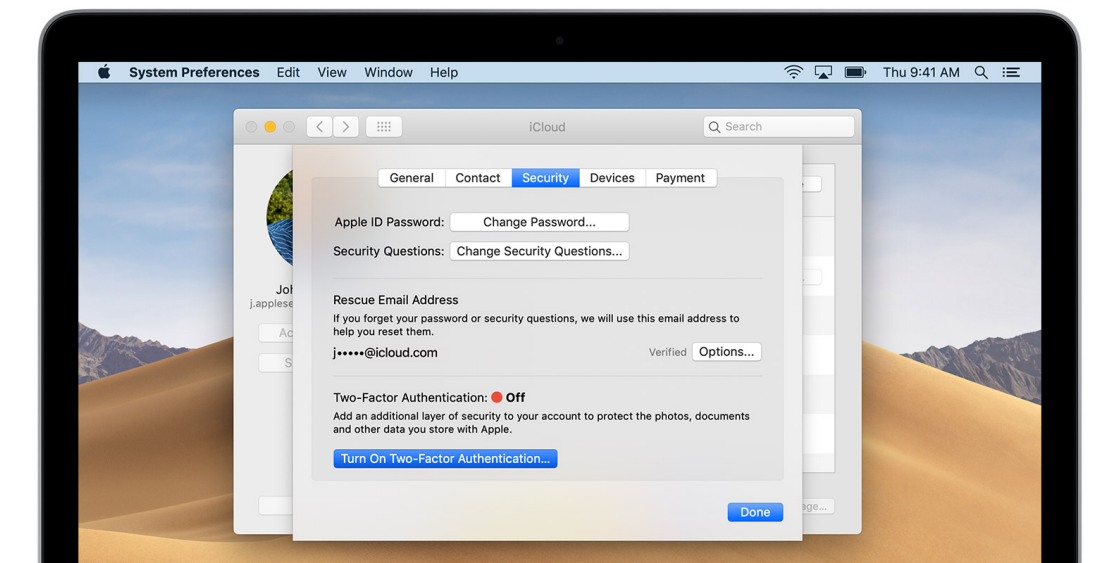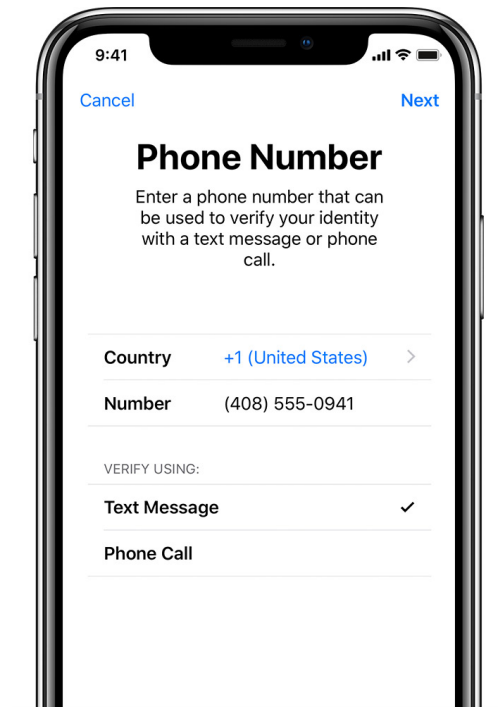
1. Go to Apple (🍎) menu > System Preferences > iCloud > Account Details.
2. Click Security.
3. Click Turn On Two-Factor Authentication.

Some Apple IDs created in iOS 10.3 or macOS 10.12.4 and later are protected with two-factor authentication by default. In this case, you see that two-factor authentication is already turned on.

If you already use two-step verification and want to update, turn it off, then turn on two-factor authentication.

If your account isn't eligible for two-factor authentication, you can still use two-step verification to protect your information.

What to remember when you use two-factor authentication

Two-factor authentication significantly improves the security of your Apple ID. After you turn it on, signing into your account will require both your password and access to your trusted devices or trusted phone number. To keep your account as secure as possible and help ensure you never lose access, there are a few simple guidelines you should follow:

- Remember your Apple ID password.
- Use a device passcode on all your devices.
- Keep your trusted phone number(s) up to date.
- Keep your trusted devices physically secure.

Manage your account

You can manage your trusted phone numbers, trusted devices, and other account information from your Apple ID account page.

Keep your trusted phone numbers up to date

To use two-factor authentication, you need at least one trusted phone number on file where you can receive verification codes. Consider verifying an additional trusted phone number other than your own phone number. If your iPhone is your only trusted device and it is missing or damaged, you will be unable to receive verification codes required to access your account.

You can update your trusted phone numbers when you follow these steps:

1. Go to your Apple ID account page.
2. Sign in with your Apple ID.
3. Go to the Security section and click Edit.

If you want to add a phone number, click Add a Trusted Phone Number and enter the phone number. Choose to verify the number with a text message or automated phone call, and click Continue. To remove a trusted phone number, click ⊗ next to the phone number you want to remove.

View and manage your trusted devices

You can view and manage a list of your trusted devices in the Devices section of your Apple ID account page.

1. Go to your Apple ID account page.
2. Sign in with your Apple ID.
3. Go to the Devices section.

The device list shows the devices that you're currently signed in to with your Apple ID. Select a device to view the model, serial number, and other useful information, including whether or not the device is trusted and can be used to receive Apple ID verification codes.

You can also remove a trusted device. Removing a trusted device will ensure that it can no longer display verification codes and that access to iCloud, and other Apple services on the device, is blocked until you sign in again with two-factor authentication. If you need to find or erase your device before you remove it from your trusted device list, you can use Find My iPhone.

Generate app-specific passwords

With two-factor authentication, you need an app-specific password to sign in to your account using third-party apps or services such as email, contacts, or calendar apps not provided by Apple. Follow these steps to generate an app-specific password:

1. Sign in to your Apple ID account page.
2. Click Generate Password below App-Specific Passwords.
3. Follow the steps on your screen.

After you generate your app-specific password, enter or paste it into the password field of the app as you would normally.

Frequently asked questions

Need help? You might find the answer to your question below.

What if I forget my password?

You can reset or change your password from your trusted device when you follow these steps.

On your iPhone, iPad, or iPod touch:

1. Go to Settings > [your name]. If you're using iOS 10.2 or earlier, go to Settings > iCloud > tap your Apple ID.
2. Tap Password & Security > Change Password.
3. Enter a new password.

On your Mac:

1. Go to > System Preferences > iCloud.
2. Choose Account Details. If you're asked to enter your Apple ID password, click Forgot Apple ID or password and follow the onscreen instructions. You can skip the steps below.
3. Click Security > Reset Password. Before you can reset your Apple ID password, enter the password used to unlock your Mac.

What if I can't access a trusted device or didn't receive a verification code?

If you're signing in and don't have a trusted device handy that can display verification codes, you can have a code sent to your trusted phone number via text message or an automated phone call instead. Click Didn't Get a Code on the sign in screen and choose to send a code to your trusted phone number. You can also get a code directly from Settings on a trusted device. Learn how to get a verification code.

If you use iOS 11.3 or later on your iPhone, you might not need to enter a verification code. In some cases, your trusted phone number can be automatically verified in the background on your iPhone. It's one less thing to do, and your account is still protected with two-factor authentication.

If I can't sign in, how do I regain access to my account?

If you can't sign in, access a trusted device, reset your password, or receive verification codes, you can request account recovery to regain access to your account. Account recovery is an automatic process designed to get you back in to your account as quickly as possible while denying access to anyone who might be pretending to be you. It might take a few days—or longer—depending on what specific account information you can provide to verify your identity.

Do I still need to remember any security questions?

No. With two-factor authentication, you don't need to remember any security questions. We verify your identity exclusively using your password and verification codes sent to your trusted devices and phone numbers. When you enroll in two-factor authentication, we keep your old security questions on file for two weeks in case you need to return your account to its previous security settings. After that, they're deleted.

Can Apple Support help me regain access to my account?

Apple Support can answer your questions about the account recovery process, but can't verify your identity or expedite the process in any way.

What are the system requirements for two-factor authentication?

For the best experience, make sure that you meet these system requirements on all of the devices you use with your Apple ID:

- iPhone, iPad, or iPod touch with iOS 9 and later
- Mac with OS X El Capitan and iTunes 12.3 and later
- Apple Watch with watchOS 2 and later
- Apple TV HD with tvOS
- Windows PC with iCloud for Windows 5 and iTunes 12.3.3 and later

Can Apple IDs created for children use two-factor authentication?

Yes. Any Apple ID that meets the basic system requirements can enroll in two-factor authentication. Learn more about who can use two-factor authentication.

What if I don't recognize the location shown in my sign in notification?

When you sign in on a new device, you'll get a notification on your other trusted devices that includes a map showing the approximate location of the new device. This is an approximate location based on the IP address the device is currently using, rather than the exact location of the device. The location shown might reflect the network you're connected to, and not your physical location.

If you know you're the person trying to sign in but you don't recognize the location shown, you can still tap Allow and continue signing in. However, if you ever see a notification that your Apple ID is being used to sign in on a new device and you're not the one signing in, tap Don't Allow to block the sign in attempt.

What if I use two-factor authentication on a device running older software?

If you use two-factor authentication with devices running older OS versions—like an Apple TV (2nd or 3rd generation)—you might be asked to add your six-digit verification code to the end of your password when signing in. Get your verification code from a trusted device running iOS 9 and later or OS X El Capitan and later, or have it sent to your trusted phone number. Then type your password followed by the six-digit verification code directly into the password field.

Can I turn off two-factor authentication after I've turned it on?

If you already use two-factor authentication, you can no longer turn it off. Certain features in the latest versions of iOS and macOS require this extra level of security, which is designed to protect your information. If you recently updated your account, you can unenroll for two weeks. Just open your enrollment confirmation email and click the link to return to your previous security settings. Keep in mind, this makes your account less secure and means that you can't use features that require higher security.

Is this different than Apple's current two-step verification feature?

Yes. Two-factor authentication is built directly into iOS, macOS, tvOS, watchOS, and Apple's web sites. It uses different methods to trust devices and deliver verification codes, and offers a more streamlined user experience. You need two-factor authentication to use certain features that require improved security.

The older two-step verification feature continues to work separately for users who are already enrolled.

Published Date: July 30, 2019

Helpful?   Yes   No   56% of people found this helpful.

Start a Discussion
in Apple Support Communities

Ask other users about this article

Submit my question to the community

See all questions on this article ›

Support   Two-factor authentication for Apple ID

See all questions on this article ›

Support   Two-factor authentication for Apple ID