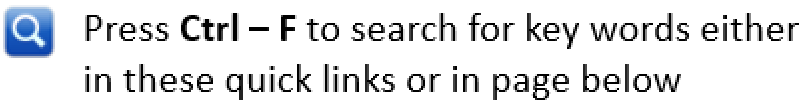
Duo Multi Factor Authentication

Common Issues - Quick Links



Press **Ctrl – F** to search for key words either in these quick links or in page below

- **A - I**
- Add secondary MFA method(s)
- Android Disk Encryption Error (FAQ #12)
- ***NEW:*** Blank authentication screen on iPhone (FAQ #31)
- Why no **D**esktop options for Duo MFA? (FAQ #5)
- Internet Explorer - SSO is broken (FAQ #28)
- ***NEW:*** What information does Duo collect? (FAQ #32)

- **J - R**
- *NEW*: Duo **Lockout** (FAQ #33)
- New phone enrollment, same phone number (FAQ #16)
- New phone enrollment, new phone number
- Order a Yubikey (FAQ #3)
- Cisco **P**olicy mandating MFA (FAQ #27)
- Re-activate Duo Mobile App Pairing (FAQ #16)

- **S - Z**
- Security Checkup - Recommended OS Version
- Too many logins (FAQ #6 & #7)
- Yubikey - Supported Browsers & Current Limitations (FAQ #3)
- Yubikey stops working, how to test (FAQ #30)
- Zeta app does not work with Android 6 (FAQ #29)

What is Duo MFA?

In August 2018, Cisco announced it's intent to acquire Duo Security and the acquisition closed at the end of September.

The Duo Security acquisition brings capabilities that will enable Cisco to extend our security perimeter beyond our firewall. The combination of Duo Security technologies and Cisco's existing ISE (Identity Services Engine) portfolio will provide an unprecedented level of visibility and control across our on-prem, off-prem, and hybrid workloads.

Duo MFA - Multi-factor Authentication - is a critical piece in realizing the above objectives.

Duo MFA is a strong authentication solution which enables users to authenticate to Cisco’s Web applications using multiple factors, in addition to traditional username/password. Even if a user's primary credentials (username/password) have been stolen or compromised, Duo MFA provides the added level of security to prevent unauthorized access. It has the right balance of ease of use needed by end users and the security and control needed for securing Cisco applications and data.

Duo MFA is now a Cisco product: the gateway to improving Cisco's security posture and enabling the new world of borderless security. As such, Duo MFA will completely replace the PingID multi-factor authentication technology.

Cisco’s Identity and Access Management team is rolling out Duo MFA capability to Cisco users, beginning with a pilot phase starting on November 19th.

What is Digital Login with Duo MFA?

Rather than the complicated one-time passcodes we are familiar with in banking and other secure institutional logins, Cisco’s Digital Login achieves the same security with ***just a simple approve button on your Apple or Android device***.

In addition to adding security to our web application login flow, we are equally focused on providing a ***better and easier user experience***.

Please note, if you prefer not or cannot use the app method on your mobile device for Digital Login, other methods are available, like:

- Security Key (Yubikey - see here for how to order: http://go2.cisco.com/yubikey)
- TouchID for compatible MacBook (Duo MFA with MacBook Touch ID - General Availability)
- SMS
  and
- Voice call - to either mobile phone, Cisco soft phone or landline

Why not stick with passwords?

The vulnerability of username/password credentials is a well-known fact. Compromised credentials mean sensitive data exposure, lost revenue and, worst of all, irreparable damage to Cisco’s brand.

Moving away from strictly username and password login is not something brand new. Username+password credentials alone are inherently vulnerable, vulnerable to getting hacked, shared, posted online, sold, etc. The move to additional factors of authentication needs to happen in order to maintain a needed level of security.

How do I get started?

In about 3 to 5 minutes of your time, you can register and pair your mobile device in order to make your first Digital Login experience as smooth as possible. Follow the guided instructions at:

https://disco.cisco.com/

Minimum Mobile Device Requirements - for Duo Mobile App Use

Please note:

- **Even if these minimum requirements are not met, you may still use the phone call or text message options on your mobile device.**
- The minimum OS requirements are enforced on ***access device*** as well. Meaning, if you are trying to access an application that requires login involving Duo MFA prompt on an old mobile device that does not meet the OS requirements below, then you will be blocked from logging in on that device. You will need to use a newer mobile device or your Cisco laptop to login and access SSO-protected applications.
- These differ from recommendations provided in 'Security Checkup' section of Duo Mobile app. Security Checkup provides optional recommendations. Below are the only mandatory requirements.
- Minimum Mobile Device Requirements are aligned necessarily with Cisco Mobility Team and Infosec.

1. The device should not be rooted or jailbroken.
2. The device must have the Screen lock enabled using Passcode, Touch ID or Face ID
3. If applicable, Secure Startup needs to be enabled (applies to certain Android models, e.g. Samsung, LG).
4. The device must have Cisco IT approved operating system (OS) version
    - iOS 11.2.6 or higher
    - Android 7 or higher

For more info: See the Cisco Mobility EC Page

Recommended for Duo MFA - Mobile Phone Registration Flow

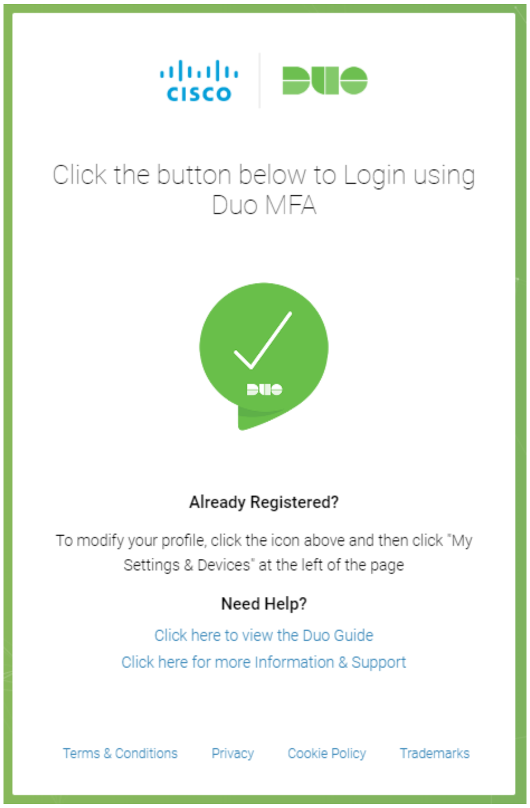
which automatically includes authentication via:

- Push notification in Duo Mobile App (certain minimum requirements apply)
- Passcode via SMS
- Accept via Voice Call

How can I pair my mobile device?

1. Start by accessing the enrollment flow for the first time - https://disco.cisco.com

Click the green DUO chat bubble to begin the enrollment flow.



Click the button below to Login using Duo MFA

Already Registered?

To modify your profile, click the icon above and then click "My Settings & Devices" at the left of the page

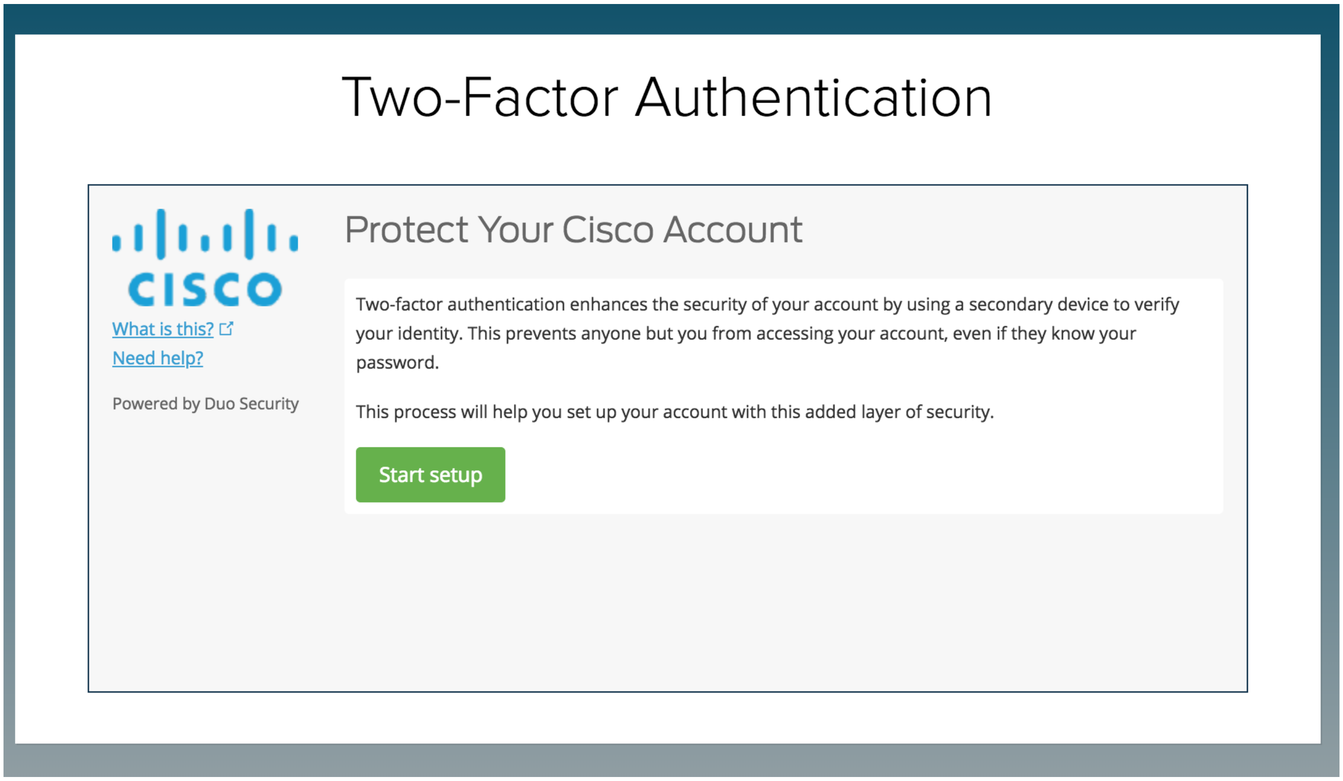
Need Help?

Click here to view the Duo Guide

Click here for more Information & Support

You will be prompted to walk through a self-registration process to register your device. Follow the steps to complete self-registration.

2. Click Start setup



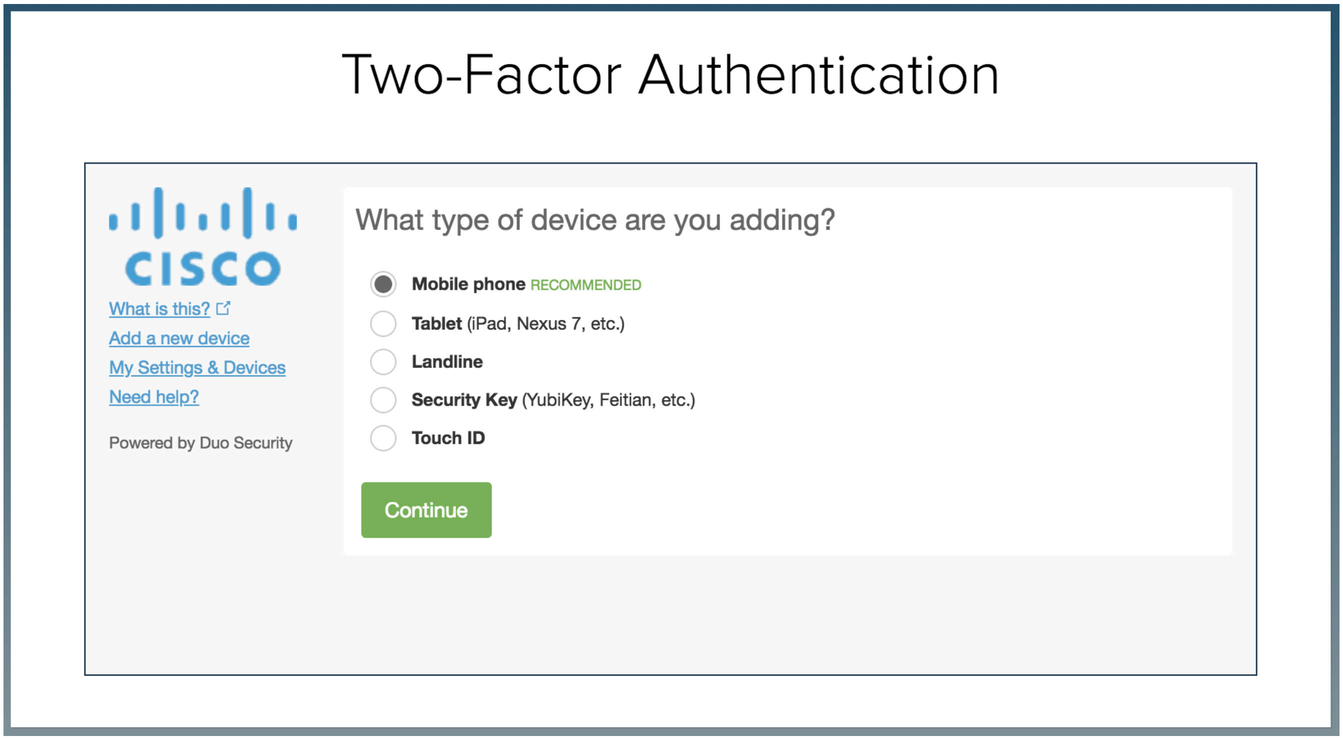
Two-Factor Authentication

Protect Your Cisco Account

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.

3. Choose Mobile phone option and click Continue

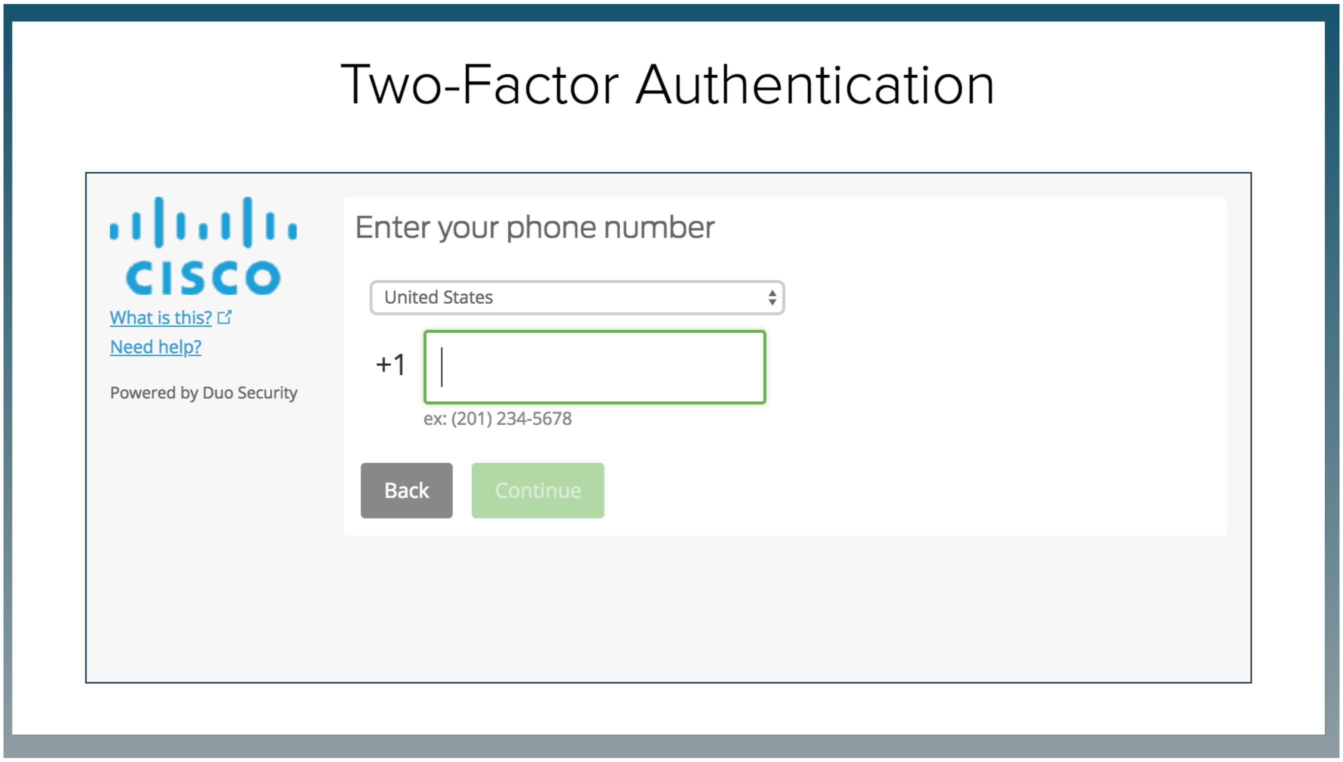


Two-Factor Authentication

What type of device are you adding?

- ● **Mobile phone** RECOMMENDED
- ○ **Tablet** (iPad, Nexus 7, etc.)
- ○ **Landline**
- ○ **Security Key** (YubiKey, Feitian, etc.)
- ○ **Touch ID**

4. Enter your phone number. Change the country code using drop down as needed. Click the check box to confirm the number you have typed is correct and click continue.



Two-Factor Authentication

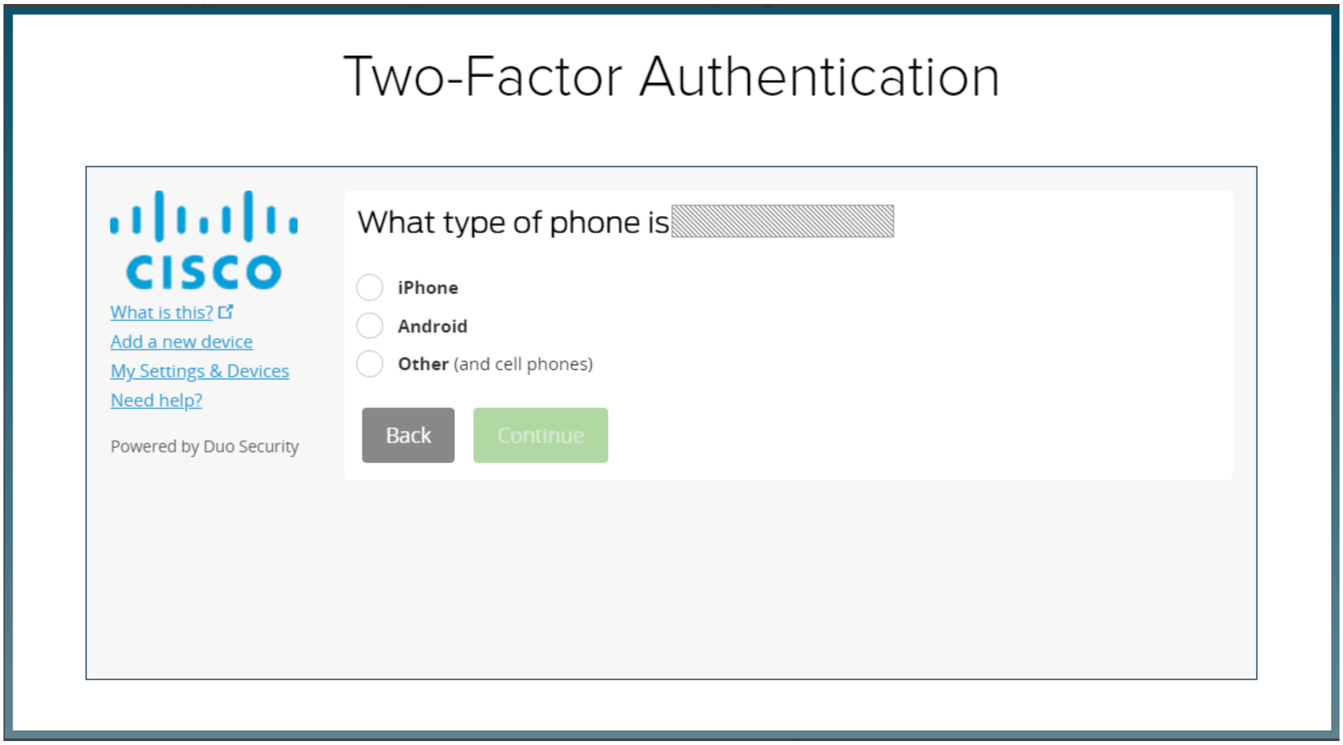
Enter your phone number

United States

+1

ex: (201) 234-5678

5. Select what type of phone it is and click Continue.



Two-Factor Authentication

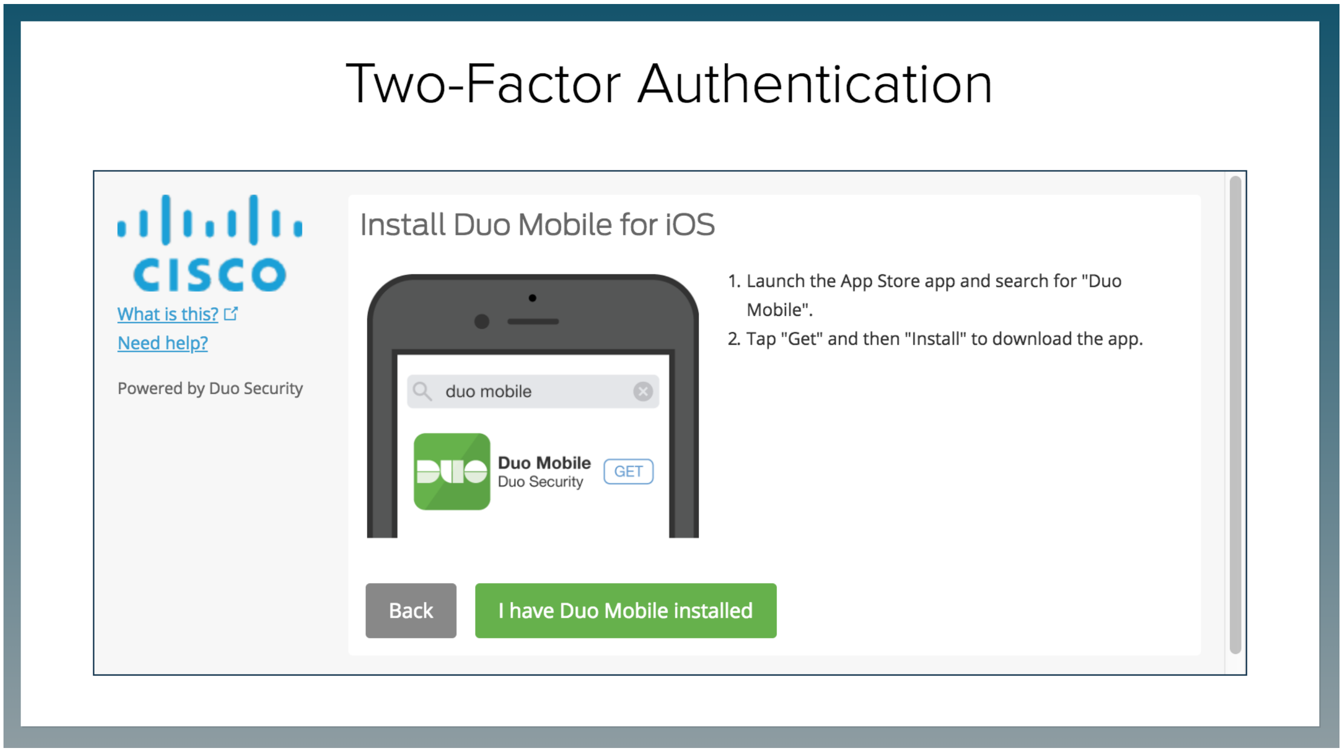
What type of phone is [redacted]

○ iPhone

○ Android

○ Other (and cell phones)

6. Launch the appropriate app store and search for "Duo Mobile" app and install it. Once it is installed, click on "I have Duo Mobile installed".

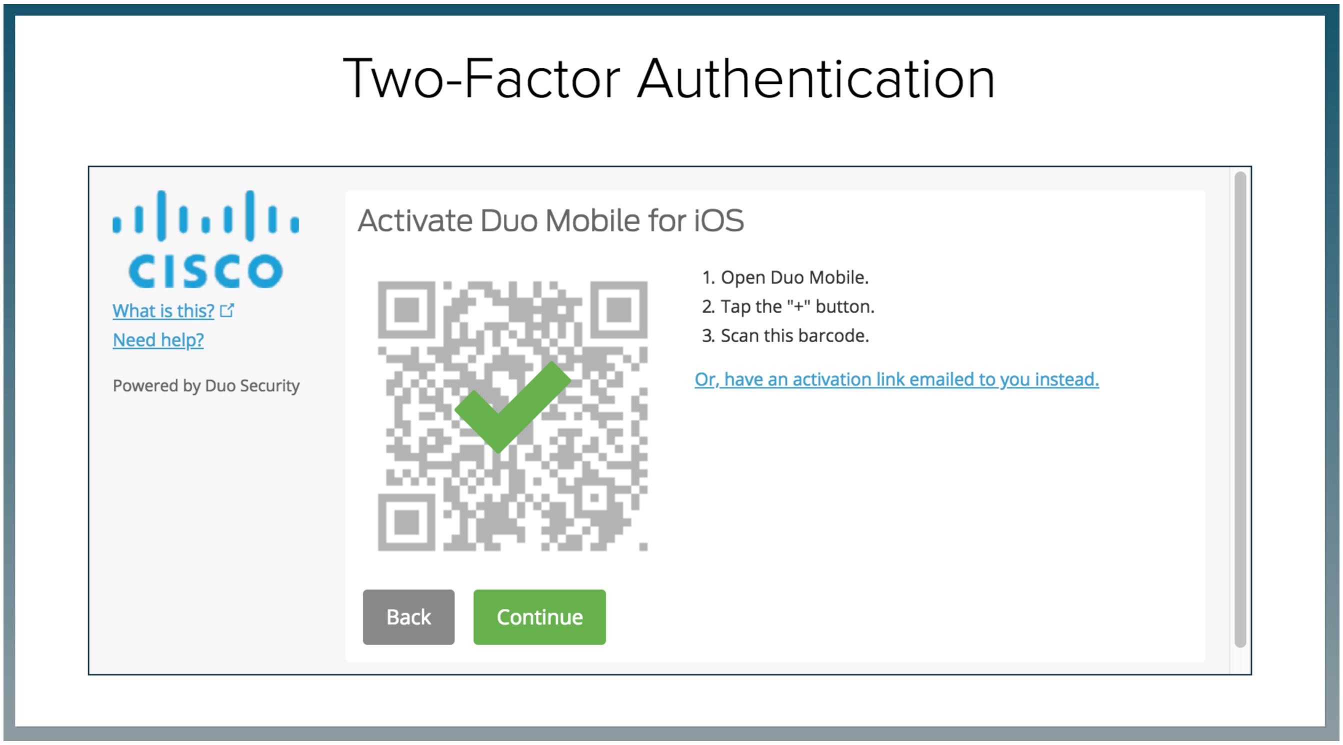


Two-Factor Authentication

Install Duo Mobile for iOS

1. Launch the App Store app and search for "Duo Mobile".
2. Tap "Get" and then "Install" to download the app.

7. Follow the instructions to scan the barcode and click continue.


Two-Factor Authentication

Activate Duo Mobile for iOS

1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.

Or, have an activation link emailed to you instead.

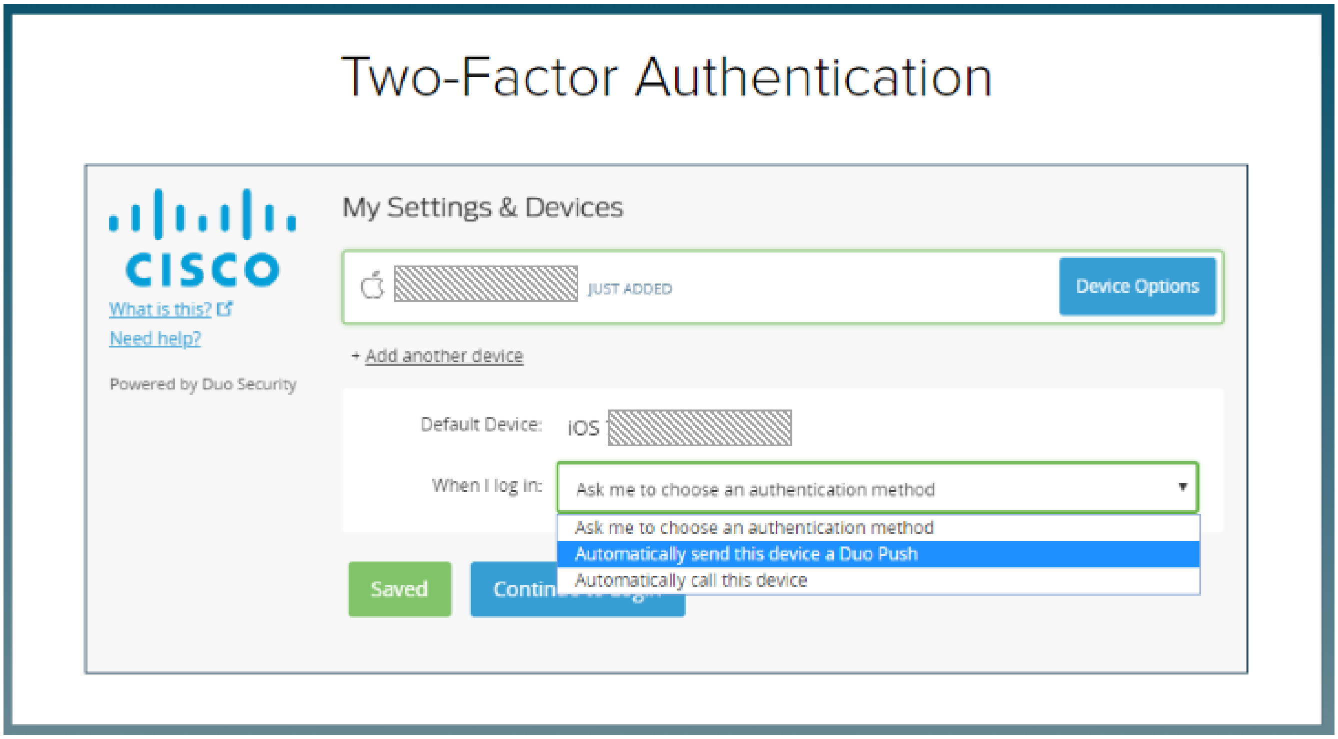
This completes the mobile app enrollment for push notifications.

As part of this enrollment, your phone number is also registered for SMS and voice call options.

You can also choose to Automatically send the mobile device a push notification by selecting the option in the dropdown.

Make sure to press 'Save' if you select a different default action.

You can Add another device as desired or click on 'Continue to Login' button.


Two-Factor Authentication

My Settings & Devices

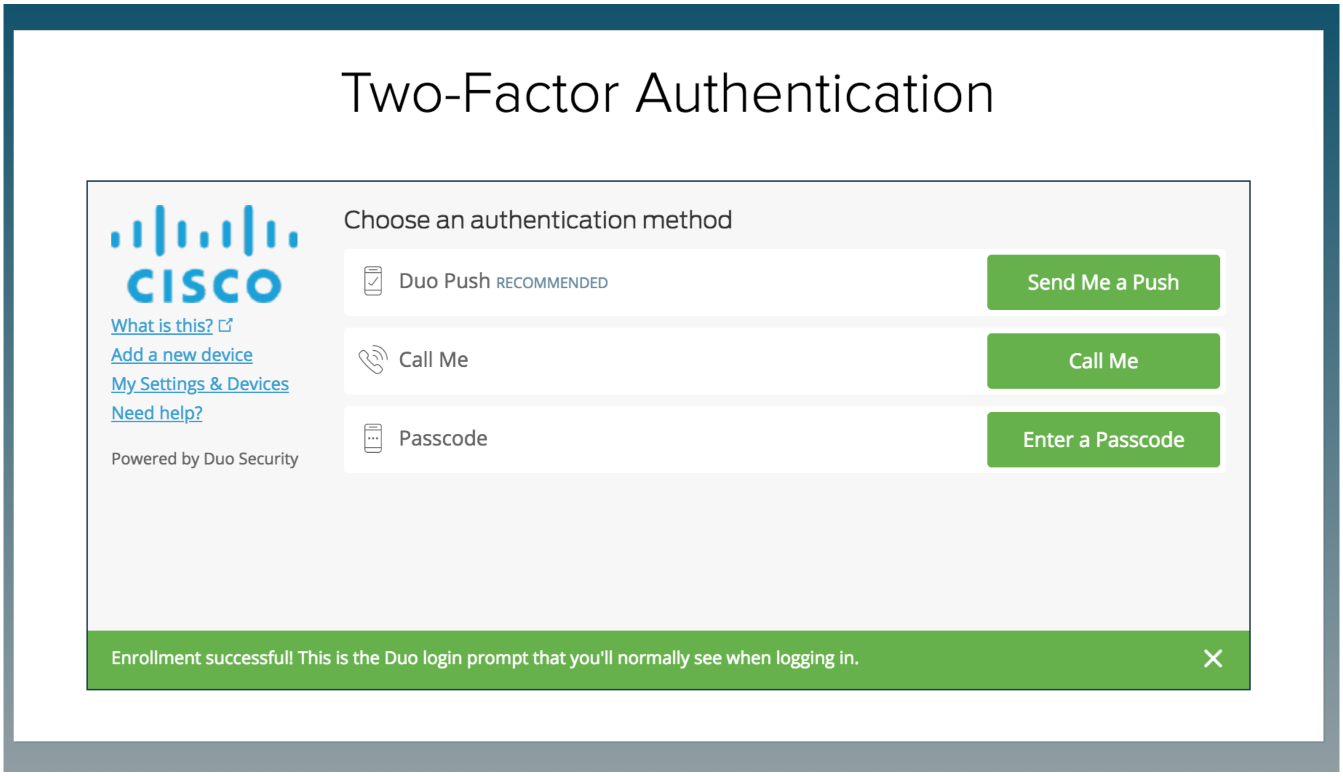
[redacted] JUST ADDED

Default Device: iOS [redacted]

When I log in: Ask me to choose an authentication method

- Ask me to choose an authentication method
- Automatically send this device a Duo Push
- Automatically call this device

8. Get yourself familiar with this screen as this is the screen you will see during login.



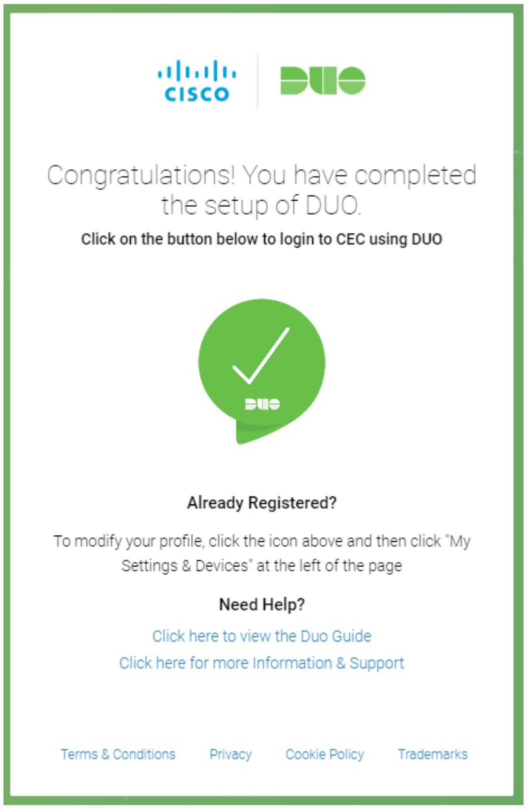
Two-Factor Authentication

Choose an authentication method

Enrollment successful! This is the Duo login prompt that you'll normally see when logging in.

9. Click on Send Me a Push to get the Duo notification on your phone.

10. Once you Approve the received Push notification, you will see the following enrollment confirmation.



Congratulations! You have completed the setup of DUO.

Click on the button below to login to CEC using DUO

Already Registered?

To modify your profile, click the icon above and then click "My Settings & Devices" at the left of the page

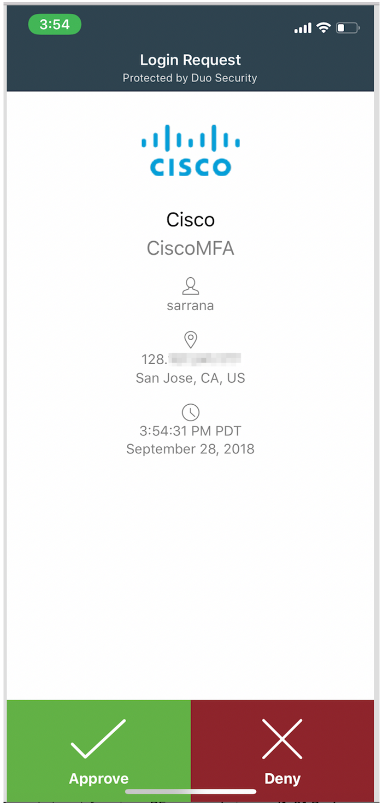
Need Help?

Click here to view the Duo Guide
Click here for more Information & Support
Terms & Conditions
Privacy
Cookie Policy
Trademarks

How can I get authenticated using the mobile application?

There are two ways to get authenticated

- If you are online, you can click on Approve in the Duo Mobile app upon receiving the push notification.
    - Alternatively, the notification can also be expanded/opened from the lock screen and approved from there. Device unlock (by passcode or Touch/Face ID) is still required to complete the authentication request.
        - Accept within Duo Mobile App



Login Request
Protected by Duo Security

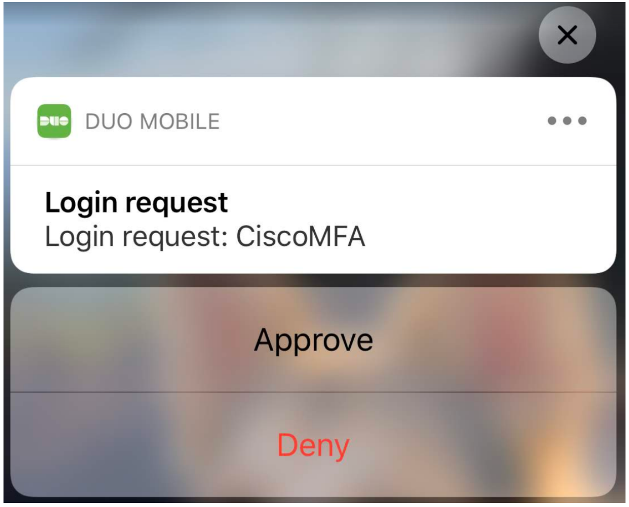
Cisco
CiscoMFA

sarrana

128.[redacted]
San Jose, CA, US

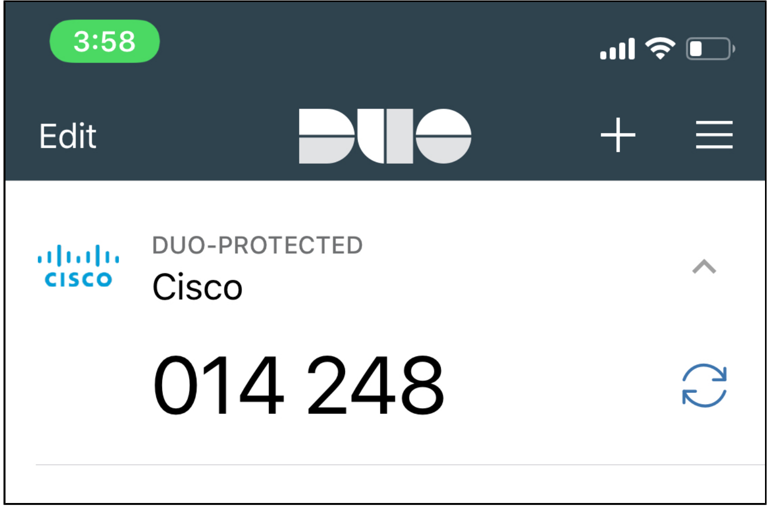
3:54:31 PM PDT
September 28, 2018

        - Or accept from lock screen:



Login request
Login request: CiscoMFA

- If your phone is not having any network connection - e.g. phone is in airplane mode or in an area of weak network signal - the “one-time passcode” continues to be generated in the Duo Mobile app and can be used for authentication.

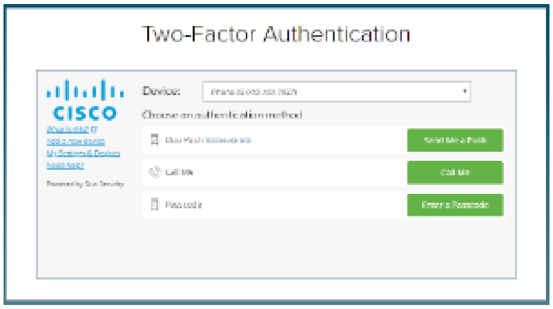


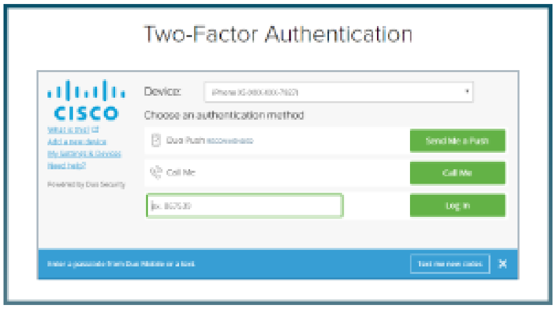
014 248

How do I authenticate using SMS?

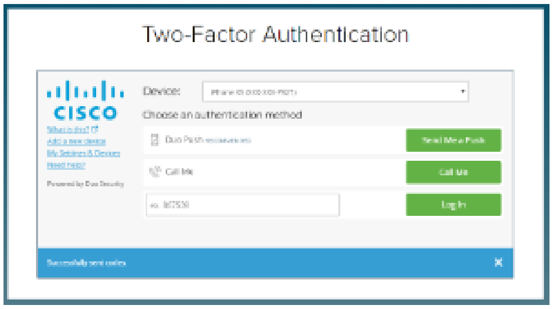
See screenshots below for step by step screens.

1) On Duo MFA prompt, click option to '**Enter a Passcode**'
2) Click button to '**Text me new codes**'
3) **Enter code** received by SMS into the provided field.
4) Click '**Log In**'

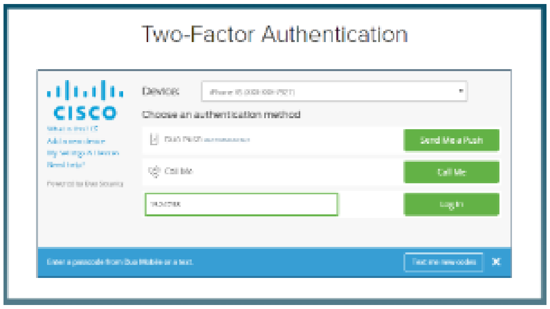




Enter a passcode from Duo Mobile or a text.



Successfully sent codes.



How do I authenticate using Yubikey?

Yubikey authentication only works in Chrome and Firefox browsers currently.

Please see FAQ #3 for more details.

Assuming you have completed the yubikey registration flow by using the 'Security Key' option in the setup or Add a new device flow, instructions below show you how to complete authentication.

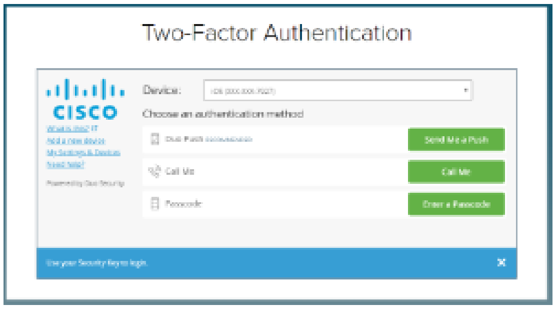
In Chrome browser:

1) Yubikey authentication can be done at any time once you see the 'Two-Factor Authentication' prompt. No need to specifically select your Yubikey device from the device drop-down.

2) You should see a ribbon at the bottom that says 'Use your Security Key to login.'.

3) Touch your Yubikey (make sure your finger makes contact with the metal receptor on your Yubikey).

4) Your authentication will be completed.


Two-Factor Authentication
CISCO
Device:
Choose an authentication method
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
Use your Security Key to login.

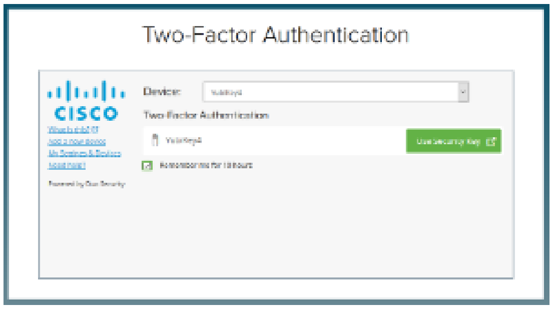
In Firefox browser:

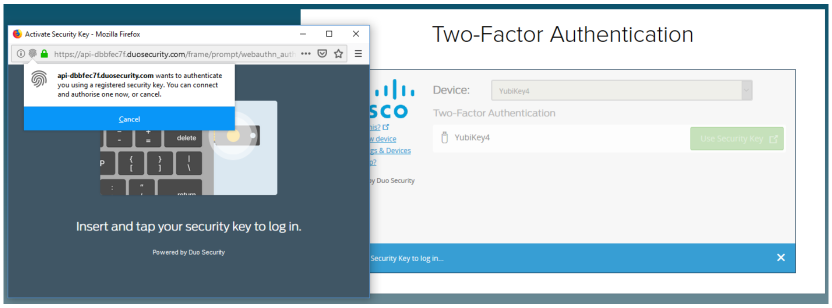
1) Your registered Yubikey device must be selected from the device drop-down.

2) Click the 'Use Security Key' button (if the popup window does not appear, make sure to allow pop-ups in your browser settings).

3) Touch your Yubikey (make sure your finger makes contact with the metal receptor on your Yubikey).

4) Your authentication will be completed.





Activate Security Key - Mozilla Firefox
https://api-dbbfec7f.duosecurity.com/frame/prompt/webauthn_auth
Cancel
delete
return
Two-Factor Authentication
sco
his?
w device
gs & Devices
p?
y Duo Security
Device:
YubiKey4
Use Security Key
Powered by Duo Security

api-dbbfec7f.duosecurity.com wants to authenticate you using a registered security key. You can connect and authorise one now, or cancel.

Insert and tap your security key to log in.

Two-Factor Authentication

YubiKey4

Security Key to log in...

Other Authentication Methods Available

Back to top

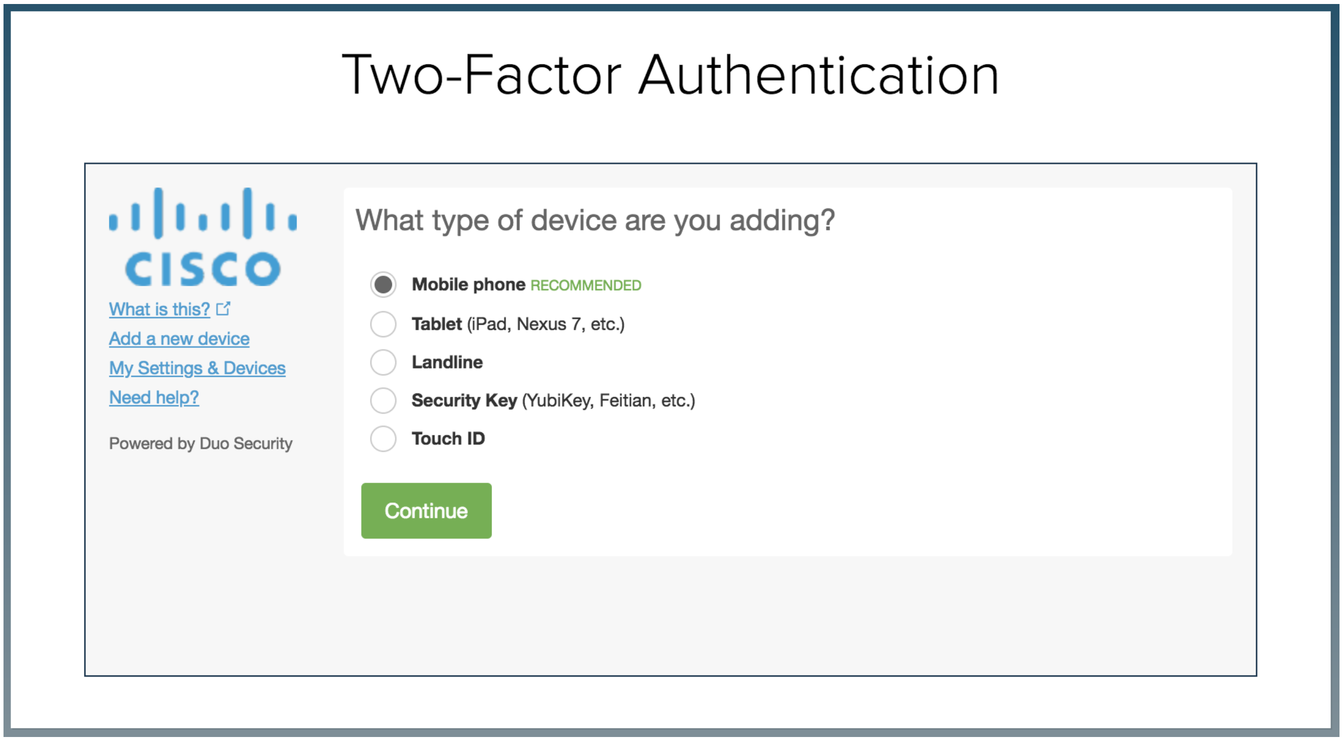
It is strongly recommended to have at least 2 different devices registered in your Duo MFA profile. This will save you from requiring admin intervention in case you have registered only 1 device and this device is unreachable, forgotten or lost.

If you have a ***new phone and new phone* number**, you may follow the instructions below to add it using the mobile phone option. ***Provided*** t hat you have some other means to authenticate in order to get access to the 'Add a new device' menu.

If you no longer have access to any of your existing Duo MFA methods, you will need to reach out for admin support: https://disco.cisco.com /teams

In order to add a different authentication method:

1) In a new browser tab, visit https://disco.cisco.com
2) Click green button in the middle
3) Enter username and password
4) **Important, *ignore*** this first Duo MFA prompt
5) Select 'Add a new device' option from left-hand side
6) Complete the Duo MFA authentication request that you see at this time
7) Next screen you should see is the options in screenshot below:



What type of device are you adding?

● **Mobile phone** RECOMMENDED
○ **Tablet** (iPad, Nexus 7, etc.)
○ **Landline**
○ **Security Key** (YubiKey, Feitian, etc.)
○ **Touch ID**

As with any Multi-Factor Authentication solution, **we highly recommend that you register at least 2 or more authentication methods.** In case one is not working, you have at least one other backup option to complete your authentication and access your desired application/data.

In order to register any of the options, select the radio button, 'Continue' and follow the on-screen instructions.

Mobile phone

Registration and use details provided above.

Automatically includes authentication via:

- Push notification in Duo Mobile App (certain minimum requirements apply)
- Passcode via SMS
- Accept via Voice Call

Tablet

- This option can be used to register only the Duo Mobile App method for push notifications or online/offline OTP (one-time password) code generation.
- This registration flow can either be used on a tablet device, or on a mobile phone (that meets the minimum requirements) to register strictly the Duo Mobile App option (i.e. not text or voice call to your mobile phone).

Landline

- This option can be used for voice call authentication to either a mobile phone number or any other landline phone number to which the user can reliably receive phone calls for authentication purposes.

Security Key

- **This option is currently only supported in Chrome and Firefox browsers** (Edge, Safari support is coming in the future but not currently available).
- This is for using hardware tokens (normally plugged into laptop via USB-A or USB-C port) that support U2F/Webauthn protocol for authentication.
- Please see FAQ concerning Yubikey for more information about this option.
- How to order a Yubikey through iProcurement

TouchID

- **This option is supported only in Chrome browser on a TouchID compatible MacBook.**
- In order to use Touch ID with Duo, make sure you have the following:
    - A MacBook Pro (2016 or later) or MacBook Air (2018) with a Touch ID button.
    - A fingerprint enrolled in Touch ID (see how to do this at the Apple Support site).
    - Chrome 70 or later. Safari and other browsers on macOS are not supported.

- Please see instructions here.

Back to top

Access Device Settings

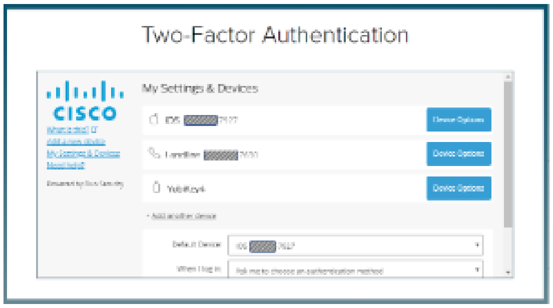
Back to top

Device Settings is where you can remove or add new devices, rename devices or reactivate a pairing with Duo Mobile app in case your pairing gets corrupted.

1) In a new browser tab, visit https://disco.cisco.com

In order to enroll and manage your devices for ***non-prod*** please visit https://disco-test.cisco.com

2) Click the green button in the middle
3) Enter your username/password
4) **Important, *ignore*** this first Duo MFA authentication request.
5) Click the 'My Settings & Devices' option on the left-hand side
6) At this point, you will need to complete a Duo MFA authentication in order to get to the settings screen shown below



Default Device: iOS [redacted] 7627

When I log in: Ask me to choose an authentication method

7) Device Options lets you remove/rename devices. Or 'Add another device' link for adding new devices.

How do I get support?

- https://disco.cisco.com/help - shortcut to this wiki page
- https://disco.cisco.com/case - ESP Case Support
- https://disco.cisco.com/teams - Webex Teams - Duo MFA Support Space
- https://disco.cisco.com/survey - Vovici Survey

Duo was acquired by Cisco in October. You can learn more here: https://wwwin.cisco.com/c/cec/news/global-employee-headlines/chitchat-with-our-newest-dynamic-duo.html. Chuck also specifically called out Duo as strategic to our security business in the quarterly earnings last week. If you have constructive feedback we would love to pass this along to the Duo Engineering team. They are incredibly responsive and thoughtful about all feedback. Deploying a product that touches every one of 100,000+ workforce on a daily basis is challenging to say the least, but it is also a great opportunity to help improve the product. The overwhelming majority of our workforce have expressed support of the user experience, but those that provide constructive feedback we take just as seriously.
Duo is very strategic to our security business as a company and it was imperative that we move our workforce to this product as soon as possible to show our customers how to utilize this product. With any transition between vendors/products, there will be pros/cons of each. We evaluated the gaps between Duo and PingID, and shared it with our executives. They supported our use of this product w/ the gaps, and committed that our workforce would adopt with the authentication methods that we have provided. With that said, anything can be improved. We are providing the feedback we get from this rollout, and sharing with the Duo product team to make the experience bette

Back to top

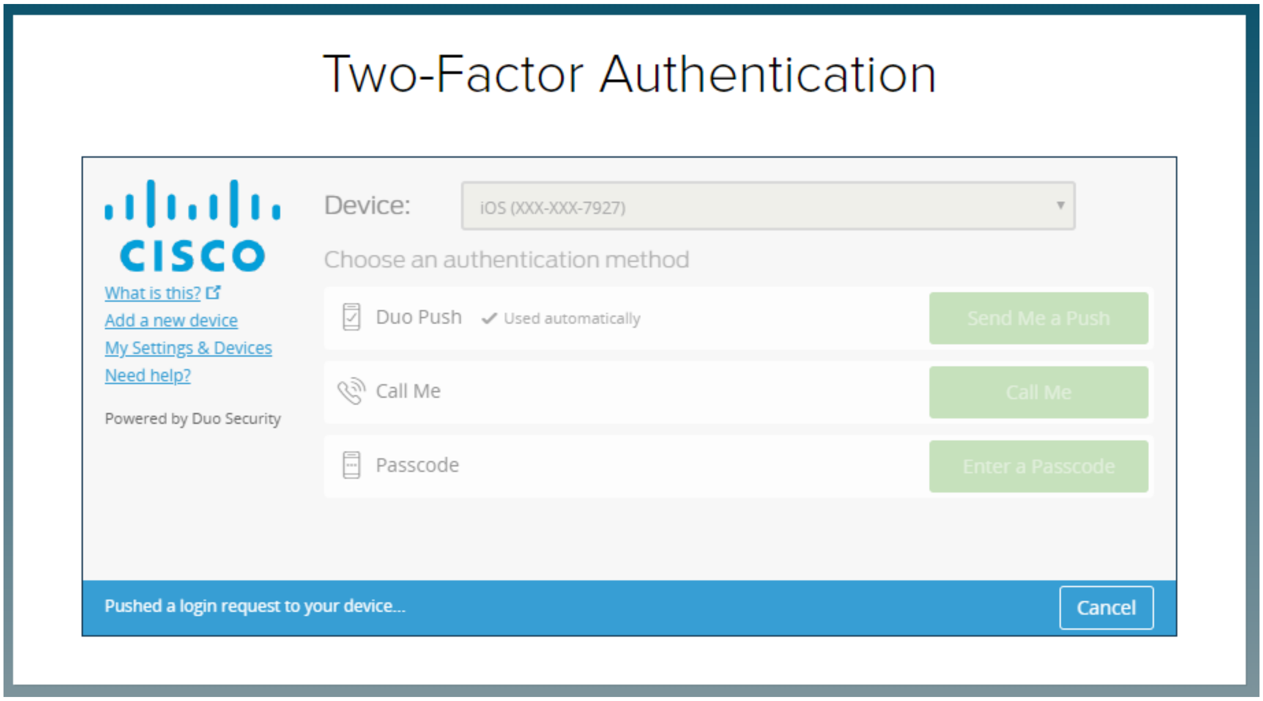
FAQs and Common Troubleshooting Scenarios

Back to top

1. **My phone completed enrollment but is not meeting minimum requirements so cannot be used for login. What do I do?**

   If you have an alternate method of authentication available to use (e.g. SMS text, voice call or U2F Security Key), there is a self-service resolution path to follow:
   Please note: If you used the 'Mobile phone' enrollment flow, SMS text and voice call options would have been registered as part of that flow.

   - You can use the 'My Settings & Devices' link on the left-hand side in order to remove the mobile phone pairing from your account.
     - Authentication is required in order to load the 'My Settings & Devices' page.
     - Then 'Device Options' beside the mobile phone option, and trash can symbol in order to remove the mobile phone pairing from your account.

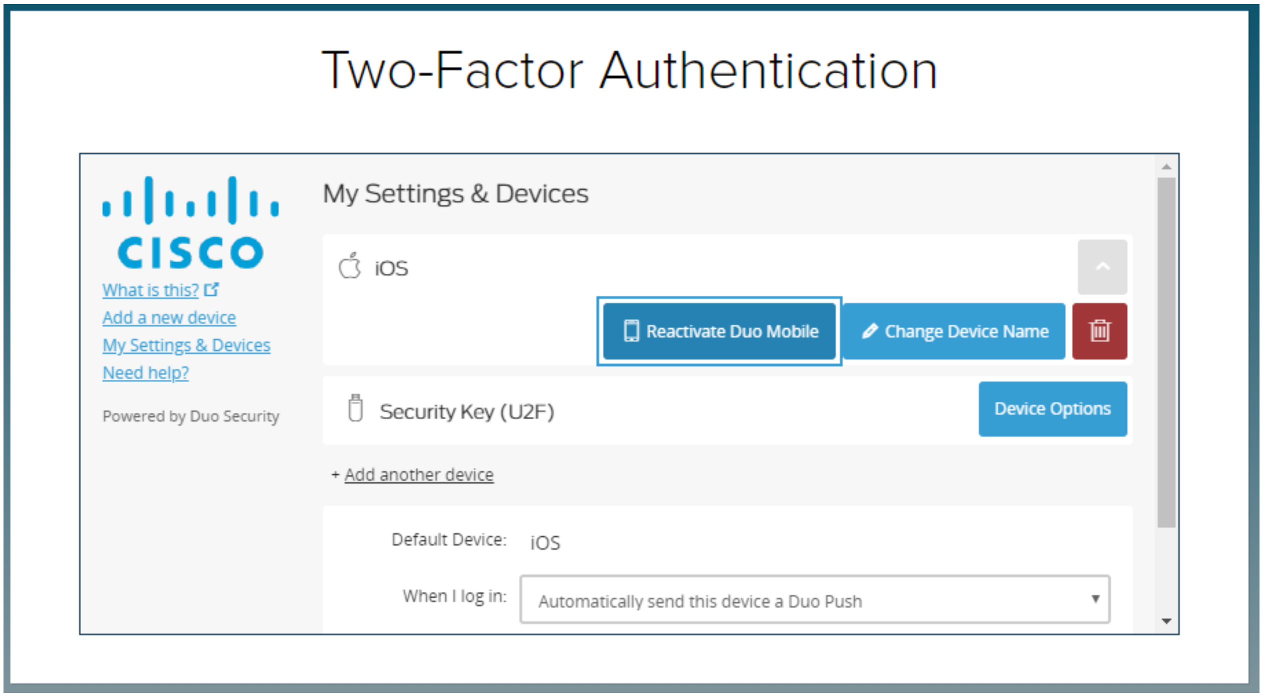


Two-Factor Authentication

Device: iOS (XXX-XXX-7927)

Choose an authentication method

Pushed a login request to your device...



Two-Factor Authentication

My Settings & Devices

Default Device: iOS

When I log in: Automatically send this device a Duo Push

If Duo Mobile App is your only authentication method registered (i.e. you used the 'Tablet' enrollment flow),

Please have your case escalated from Technical Support to Security Services Assignment Group for advanced assistance.

Admin intervention will be required in order to remove your mobile app pairing from your account and allow you to add an alternate working method of authentication.

Back to top

2. **Why do I have to enter my username/password with every login? With PingID, I was only entering username/password once a month.**

   With PingID MFA, there was a tight coupling with the first-factor (username/password) authentication layer which allowed for the use of a browser cookie between the 2 layers that allowed for the capability of only requiring username/password once in 30 days.

We are not currently able to enable the same behavior between Duo MFA and the first-factor authentication layer.
However, there is a short-term plan to re-enable kerberos for on-premise use cases. That is, when accessing protected applications while on Cisco network - wired, wireless or VPN.
When Kerberos is fully enabled and supported by the different browsers, on-prem users will not need to re-enter username /password for web SSO access once they have already logged into their Cisco-managed laptop.

3. **Can I use the same Yubikey I was using with PingID for Duo? How about the Yubikey I am using for admin access?**

For ordering a new Yubikey to use with Duo MFA - https://disco.cisco.com/yubikey

Yes - however they will be used differently compared to how you may be familiar with it for PingID.
The Yubikey, when used with Duo MFA, will not need to generate the long OTP passcode string.

Security keys that support U2F protocol or Webauthn standard, including the Yubikeys you may have been using for PingID and for admin access, can be used in Duo.

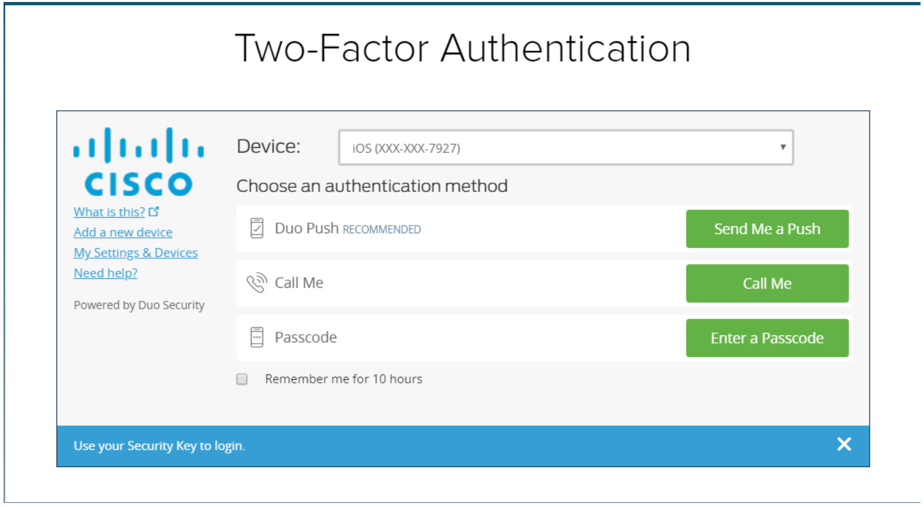
However, there are currently some limitations -
- Browser must support U2F or Webauthn. Then Duo MFA must support U2F/Webauthn authentication within the browser.
- **IE** will never support U2F/Webauthn since it is being decommissioned by Microsoft.
- **Safari and** (new Chromium-based) **Edge** should support U2F/Webauthn within the next 12 months.

Please note:
Several Cisco desktop applications launch the login flow within an embedded browser frame (**e.g. Desktop Webex Teams, Jabber, Desktop Webex Meetings, VPN EAP).**
This frame is based on the OS default browser - Edge or Safari.
Since Duo U2F/Webauthn authentication is not yet possible in Edge or Safari, an alternate Duo MFA method must be used for these applications - for example, mobile push notification, text message or voice call.

Working browsers:
- Duo MFA in Chrome supports security keys in both U2F and Webauthn mode.
- Duo MFA in Firefox supports security keys only in Webauthn mode.

If your Yubikey has been registered in Firefox first (Webauthn mode), you will need to go through the 'Add a new device' flow in Chrome and re-add your same Yubikey in order to enable the more seamless U2F experience in Chrome on your Yubikey. Registering your Yubikey in Chrome, automatically enables both U2F and Webauthn modes on your key.

U2F (Chrome) vs. Webauthn (Firefox) results in a signficantly different user **experience.**
Chrome (more seamless, better user experience):
As soon as Duo MFA prompt is displayed, Duo is automatically waiting for entry from any Security Key registered in U2F mode. Note the 'Use your Security Key to login.' banner along the bottom of the prompt.
You can tap your Yubikey at any time to complete successful login, regardless if Security Key device is not selected in the drop-down or if Duo MFA has been configured to automatically send a push notification to your phone. Push notification can be ignored as you tap your Yubikey to complete login since it is the most convenient method for the laptop experience.



Two-Factor Authentication

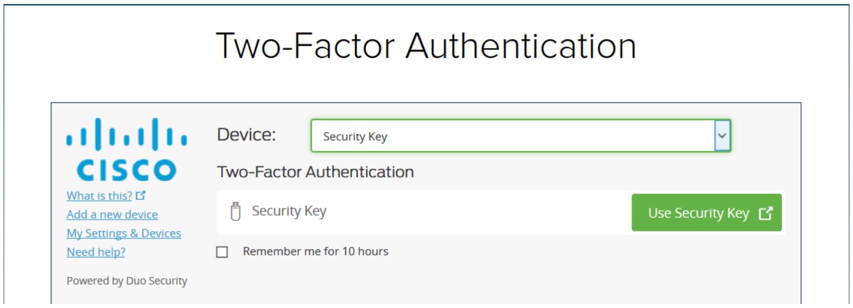
Device: iOS (XXX-XXX-7927)

Choose an authentication method

☐ Remember me for 10 hours

Use your Security Key to login.

Firefox (less seamless):
In Webauthn mode, Duo is currently unable to listen passively for Security Key input. In order to use your Yubikey in Firefox, 'Security Key' must be selected in the device drop-down menu,
then press 'Use Security Key'
Optionally, if Firefox is your primary browser and the large majority of your login access is via laptop (vs. mobile device), 'My Settings & Devices' can be used to set Security Key as your primary device.



Two-Factor Authentication

Device: Security Key

Two-Factor Authentication

Security Key

Use Security Key

□ Remember me for 10 hours

Support in Firefox/Webauthn mode is currently in beta mode so there are user experiences and messaging in the flow that we are working on improving with Duo Product team.

The Duo MFA enrollment and login prompt in any other browser (Safari, Edge, IE) will either not show the Security Key option at all, or show this as greyed out.

4. **I checked the 'Remember me' checkbox, however, I am still getting prompted for Duo on each login. Why?**

Please ensure that 3rd party cookies are enabled in your browser.

5. **I do not see e-mail or desktop app as available authentication options with Duo. How can I use those?**

E-mail is not a valid MFA method due to security concerns, as well as complications this creates when e-mail (Office 365) is moving to the cloud and requiring Duo MFA in order to access it.
Even in PingID, e-mail method was in the process of being removed due to the same reasons as above.
For these reasons, e-mail is not a method currently available in Duo MFA and is not considered to be added in the future.

Desktop App authentication method is also not currently available for Duo MFA due to security concerns.
Currently there is a security vulnerability concerning the ability to digitally copy/hack the desktop app installation and be able to use this on a laptop other than the one from which it was registered.
Even in PingID, desktop method was in the process of being re-implemented by the vendor in order to address this security concern.
Duo product team and our Infosec organization agree on roadmap toward supporting other built-in device options for secure MFA authn (e.g. biometric options built in to device), instead of investing efforts into implementing a desktop application method.

6. **Why do I have to log in multiple times a day?**

For anyone experiencing the multiple SSO login prompts, I would ask for some benefit of the doubt that our team is not intending this behavior, or intending a clearly unsatisfactory user experience in favor of security.

Expected SSO behavior is dependent on cookie handling.

Unfortunately, there’s no set recipe book that we can provide to all users to explain what is breaking in the end to end cookie flow causing a broken SSO experience.

Most of the time the “easier” explanations suffice –

- User is closing and re-opening browser
- Multiple logins across different desktop apps (e.g. Webex Teams, Jabber, Productivity Tools) – these embedded browser frames are not able to store/share cookies
- User is able to identify a known app that is logging them out/killing the SSO session
- Etc.

But several times, the troubleshooting does require a 1 on 1 session and a deeper dive into the cookie data or app(s) behavior that user is accessing.

If the easy explanations don’t cover it for you, please report it through our SSO service offering so we can take a deeper look:

https://cisco.service-now.com/sp?id=search&bt=t&q=*&filter_string=serviceoffering:%27Web%20Access%20Management%20-%20SSO,%20Authentication,%20Authorization%27

Note: Any broken SSO behavior is independent of either PingID or Duo as the MFA step.

For what it’s worth, here’s the experience I have that we hope most of our users can share as well:

- New work day - After laptop login, on first open of my default browser (Chrome) I am prompted for login to the first SSO-protected app. For the next 10 hours, I don’t see the SSO login prompt again. If I do see it, it is explained by some testing I am doing which has killed my SSO session. There is a small handful of web apps with a higher confidentiality rating that require login every time, but most of Cisco workforce are not accessing these, including myself.

    - It is in the active roadmap to eliminate SSO username/password with a valid Kerberos certificate tied to laptop login and Cisco on-prem status (VPN, blizzard or hardwire). There are factors and dependencies getting worked through to implement this successfully.

- Logins to desktop apps are separate and do prompt me for additional SSO logins. But for the main Cisco desktop apps (Webex Teams, Jabber, Productivity Tools), these have long-lived sessions and do not prompt me for login unless I explicitly sign out (which I don’t do).

Per 10 hour work day –

- Laptop login at start of day and any time I need to lock
- 1 SSO login per browser window
- Plus SSO login per desktop app (which is rarely required in my experience)

More detailed list of reasons why you may be prompted for a new SSO login:

a) Cookies are disabled in your browser.
The existence and validity of SSO sessions are tracked via browser cookies. If you have disabled the creation or storying of cookies in your browser, then you will be prompted for credentials on every attempt to access an SSO-protected resource.

b) Brand new browser window
Best to keep your browser window open for your whole work day if possible. Closing and re-opening your browser window will require a new authentication.

c) Different browser (i.e. switching from Chrome to Firefox)
Each new browser window will require a login.

d) New Desktop Application login
When desktop applications (e.g. Webex Teams, Desktop Webex Meetings, Jabber, etc.) prompt for login inside an embedded browser frame inside the application, this browser frame does not have access to create/use saved cookies similar to full browser windows.
Unfortunately, no workaround to this. However, these applications should also require login very infrequently. Unless a user explicitly signs out or "resets" the application.

e) No SSO activity on cisco.com domain for 10 hours or more (new: recently extended from 4 to 10 hours to cover a standard work day)
Please note: Continuous activity on certain popular websites like WebEx, Jive, Smartsheet and Box will not count as SSO activity because they are not hosted on cisco.com.
Initial login to these sites uses the common login page and communicates with Cisco SSO server. However, once login is complete, continued activity on the site no longer communicates with Cisco SSO servers.

f) After using 'Logout' button on Cisco websites and applications which have implemented a global logout action, i.e. logout that kills your SSO session.
Note: This varies between application.
Logout from CEC, www.cisco.com, Oracle EBS (iProc), applications kills your SSO session.
Logout from Box does not kill your SSO session.

g) Also, note that some applications are not integrated with centralized SSO. These may require CEC credentials to log in, but these handle login and/or validity of login sessions independently.
For example, eman.cisco.com, onramp.cisco.com, cdanalytics.cisco.com and others.

If you don't find SSO is working for you as described above, please open a case via At Your Service and our support team can help investigate and resolve problems if required.

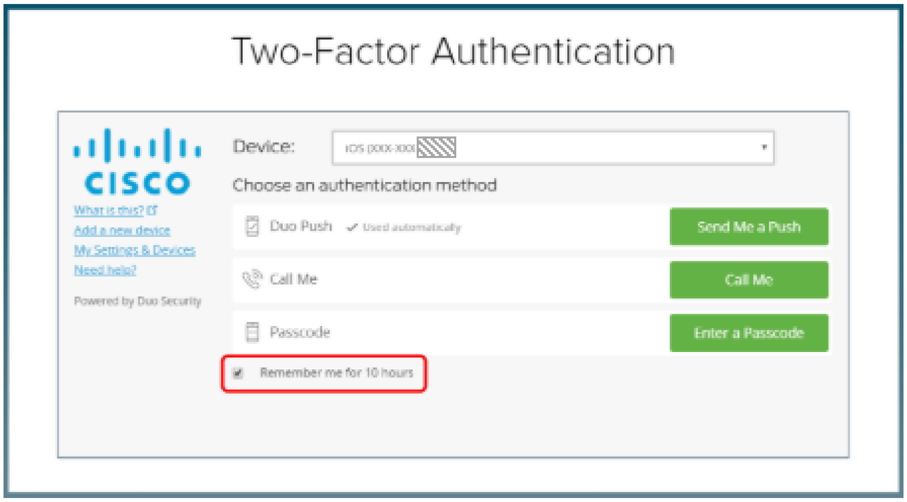
7. **Can I reduce the number of times I need to enter username/password or do Duo MFA?**

If you log in once at the start of your day and use that same browser window for the rest of the day, you should not be prompted to log in again for 10 hours. Browser can be minimized if working on other things. But as long as window stays open and you just close /open new tabs, SSO session stays valid. Please see above FAQ #6 for reasons why SSO session could be killed despite browser window staying open.

Username/Password - It is on our short-term roadmap to enable Kerberos validation as part of the Web SSO login flow. Kerberos validation is a combination of validating a certificate on your device and location on Cisco network.
If Kerberos validation is successful, Web SSO login will not require username/password entry.

Duo MFA - Make sure to check the 'Remember me' checkbox on Duo MFA prompt screen.
Please note: You may need to cancel the automatic push notification in order to see/check this box. But you should only need to do this once at the start of your day, per browser.
'Remember me' capability also requires the use of browser cookies. So if cookies are disabled, or deleted for whatever reason, or you are switching between different browsers (e.g. chrome vs. firefox), you will be prompted again for Duo MFA.

The setting of this box being checked is stored as a persistent cookie in your browser. If cookies have not been cleared, then the box should remain checked automatically for the following days, as long as the persistent cookie is still there.



Two-Factor Authentication

Device: iOS (XXX-XXX[redacted]

Choose an authentication method

☑ Remember me for 10 hours

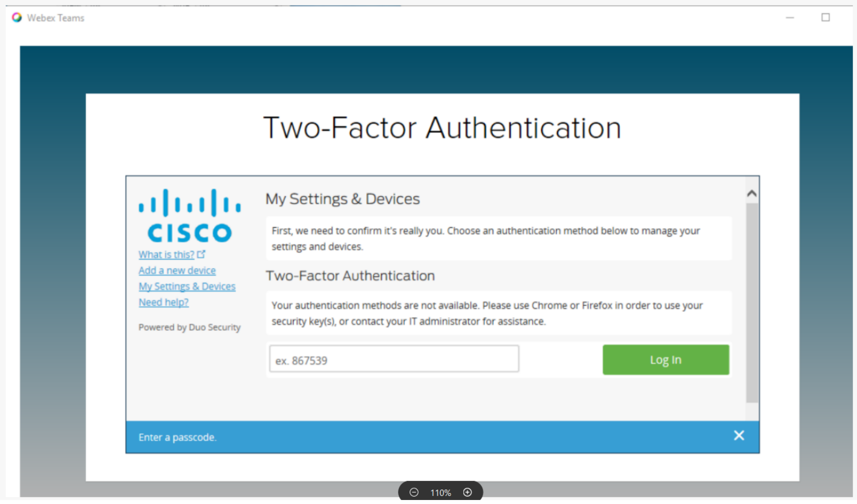
8. **Attention: Developers and anyone accessing non-production websites and resources -**
   I have enrolled for Duo MFA using https://disco.cisco.com , but now I am being prompted to enroll again. Or I am not seeing Duo MFA when accessing a non-prod resource. Why??

   As per Infosec requirements, our production and non-production environments are protected by independent SSO infrastructure. As such, we have a Cisco Duo MFA tenant dedicated to non-prod, and a separate tenant dedicated to production.

   In order to enroll and manage your devices for ***non-prod*** please visit https://disco-test.cisco.com

   In order to enroll and manage your devices for ***prod*** please visit https://disco.cisco.com

9. **Your authentication methods are not available. Please use Chrome or Firefox in order to use your security key(s), or contact your IT administrator for assistance.**



Two-Factor Authentication

My Settings & Devices

First, we need to confirm it's really you. Choose an authentication method below to manage your settings and devices.

Two-Factor Authentication

Your authentication methods are not available. Please use Chrome or Firefox in order to use your security key(s), or contact your IT administrator for assistance.

ex. 867539

Enter a passcode.

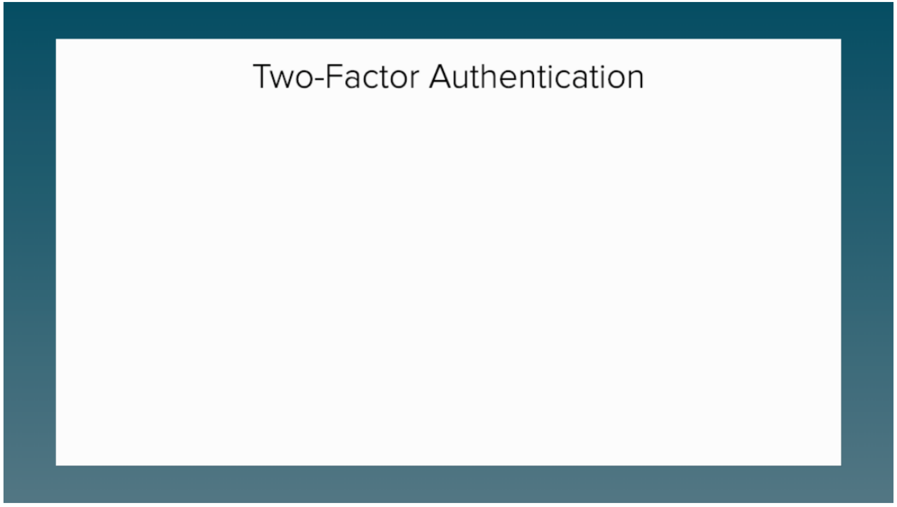
You may run into this scenario because you have registered your security key in Chrome or Firefox and are now being prompted for a login in some other browser (i.e. Edge or Safari).
This is likely to happen if you are logging into a desktop app (e.g. Webex Teams) that uses the OS default browser (Edge or Safari) for the embedded login flow.

In order to be able to use Edge or Safari based login flows, please do the following:
Use Chrome or Firefox to access https://disco.cisco.com
Click the green button
Click the 'My Settings & Devices' link on the left
Authenticate using your Security Key
Add a method which is available for Duo MFA use in Edge/Safari - i.e. text message, voice call (landline) or Duo Mobile App

10. **Duo enrollment flow and data privacy concerns.**

    We are working with Duo in terms of adding an in-line privacy statement during the enrollment flow.
    Also, for more information, please see this article What data does Duo collect?

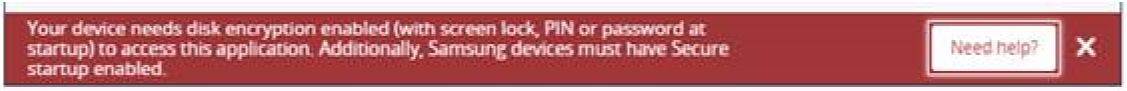
11. **I am using Chrome and the Duo MFA authentication prompt is showing blank.**


Two-Factor Authentication

    Please check if you are using a 'Privacy Badger' add-on in Chrome. If so, please disable the add-on or otherwise allow the Duo MFA prompt in the add-on settings.

12. **I successfully enrolled my Android device. But why is it now showing as unencrypted when trying to authenticate using push notification?**

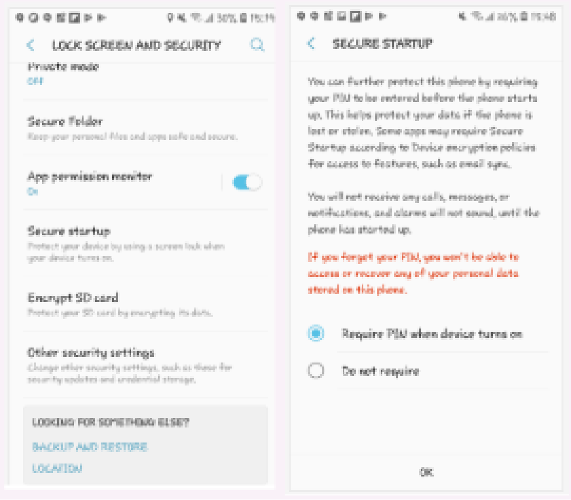
    You may be seeing the following error message on login attempt:
    "Your device needs disk encryption enabled (with screen lock, PIN, or password at startup) to access this application. Additionally, Samsung devices must have Secure startup enabled."


Your device needs disk encryption enabled (with screen lock, PIN or password at startup) to access this application. Additionally, Samsung devices must have Secure startup enabled.

    The 'Need help?' link provides helpful step-by-step for resolving this issue.

    In order to properly enable encryption, please enable the following 2 settings.
    If enabling screen lock alone does not resolve the problem,
    then please also make sure to enable 'Secure Startup'. (Applicable on only certain Android devices, e.g. Samsung and possibly Motorola)

    (1) Enable screen lock on your android device using the following instructions: https://help.duo.com/s/article/2280?language=en_US
    (2) Enable 'Secure Startup' on your device. Make sure 'Require PIN when device turns on' is selected and saved.
    Depending on Device Model and Android Version, the Secure Startup option may appear under different menus. Easiest is to search for 'Secure Startup' in the 'Settings' menu.



LOCK SCREEN AND SECURITY

Private mode
Off

Secure Folder
Keep your personal files and apps safe and secure.

App permission monitor
On

Secure startup
Protect your device by using a screen lock when your device turns on.

Encrypt SD card
Protect your SD card by encrypting its data.

Other security settings
Change other security settings, such as those for security updates and credential storage.

LOOKING FOR SOMETHING ELSE?
BACKUP AND RESTORE
LOCATION

SECURE STARTUP

You can further protect this phone by requiring your PIN to be entered before the phone starts up. This helps protect your data if the phone is lost or stolen. Some apps may require Secure Startup according to Device encryption policies for access to features, such as email sync.

You will not receive any calls, messages, or notifications, and alarms will not sound, until the phone has started up.

If you forget your PIN, you won't be able to access or recover any of your personal data stored on this phone.

● Require PIN when device turns on

○ Do not require

OK

In some cases, you may also need to disable then re-enable your screen lock in order for the encryption flag on your device to be properly set as activated.

13. **I enrolled for Duo but I'm still seeing PingID challenge in certain cases.**

2 things are required in order to see Duo for SSO login instead of PingID:
1) Enrollment in Duo MFA (via https://disco.cisco.com or via mandatory in-line enrollment during login flow)
2) Membership in the specific DSX group that allows us to determine, during the login flow, whether you should be sent to PingID branch or Duo MFA branch.

If you received a specific invite and communication regarding participation in Duo MFA rollout, then you are already added to the DSX group.

If you have not received any communication and would like to add yourself to the DSX group, please visit and complete the login flow at https://disco.cisco.com/pilot .

For those officially invited:
There are a very small handful of use cases where it is expected behavior that you may see a PingID challenge during the first week of your invite even after enrolling in Duo - e.g. off-prem login to Office 365, login to applications such as SWIMS, Streamline or eProxy.
Once you are in the 2nd week after being invited, your status changes to mandatory enrollment phase, and you will start to see Duo MFA even for the above use cases.

14. **I cannot log in to Concur mobile app on my Android**

Both my team and the Cisco business owner of Concur deployment at Cisco have been looped into this discussion which was first brought up a few months ago.

SAP Concur's stance at the time: they do not support MFA in the login flow.
The reason for the broken user experience is because the Concur mobile app has not been updated to properly support Android 8.0 and higher. As of Android 8.0, Google has implemented Background Execution Limits which automatically kills "background" apps in order to save battery life.
In terms of MFA login experience, as soon as a user switches to the MFA app to accept the authentication (regardless of MFA app, e.g. PingID or Duo MFA), the Concur app gets killed which breaks the login flow.

There is well documented resources to enable mobile app developers to properly update their app (if required) such that it is not killed when it goes to background.

We have it documented here, including links to the official Android documentation on this:

Please scroll to "*Why is authentication failing on Android 8.x+ devices?*"

https://apps.na.collabserv.com/wikis/home?lang=en-us#!/wiki/W8b53af71169c_418b_91ea_a8b7b4e2f9f3/page/Mobile%20Authentication%20Framework%20-%20Frequently%20Asked%20Questions

Workaround:
If the Duo MFA or PingID request is actioned/approved from the notification itself, the login flow should succeed. (Since user is not switching applications, causing Concur app to go into the background.)

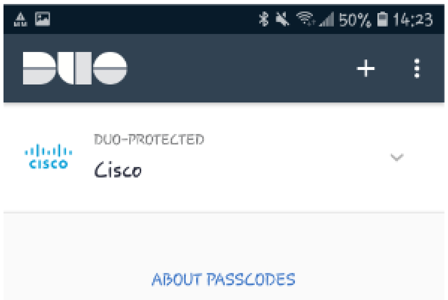
Depending on model and version of your Android, there may be different ways to expand the options on the notification and see the 'Approve' option - e.g. pull down on notification or swipe left/right.

We will continue to work with the Cisco business owners of Concur and will update our FAQ as we get new developments.

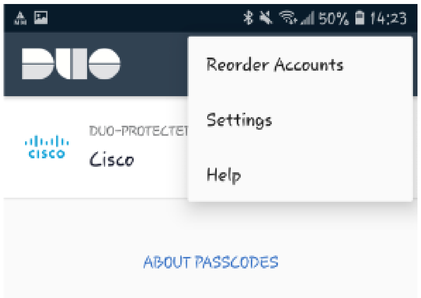
In the meantime, unfortunately, as long as Concur mobile app goes into background the login experience will be broken on Android 8.0.

15. **Android - Duo Mobile App Troubleshooting - How can I take screenshots of the Duo Mobile app screens on my phone?**

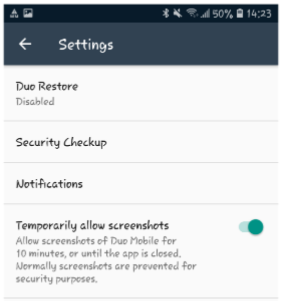
    I have an Android phone. When I try to take a screenshot in Duo Mobile App I get the message: "Can't take screenshot due to security policy."
    Screenshots can be temporarily enabled for Duo Mobile App on Android -
    (1) Open Duo Mobile App



    (2) Click the 3 dots at the top right of the app screen
    (3) 'Settings'



    (4) Toggle on 'Temporarily allow screenshots'



Duo Restore
Disabled

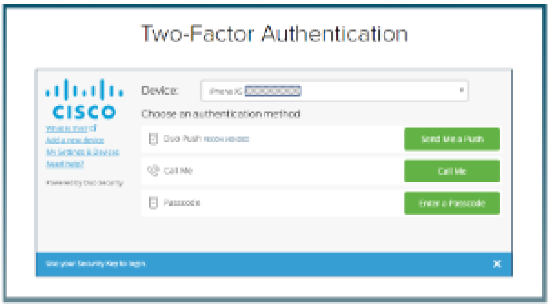
Security Checkup

Notifications

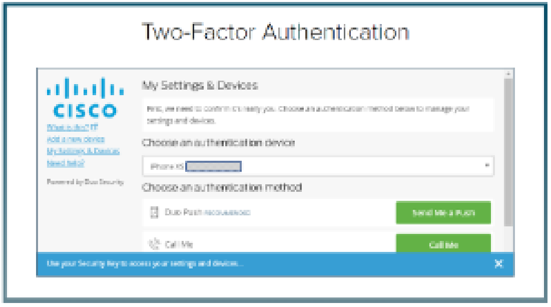
Temporarily allow screenshots
Allow screenshots of Duo Mobile for 10 minutes, or until the app is closed. Normally screenshots are prevented for security purposes.

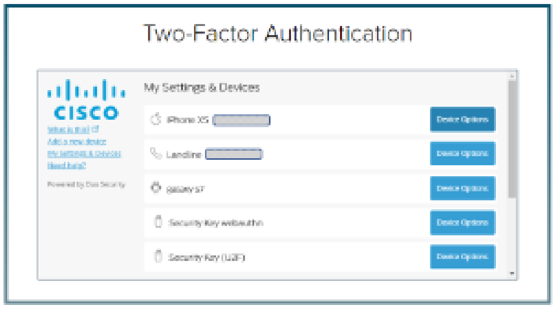
16. **In some scenarios, Duo Mobile App may no longer work and need to be re-activated. For example:**
    (1) New phone, same phone number, need to re-scan QR code to re-pair in Duo mobile app.
    (2) New phone, Duo Mobile App is restored from a backup and push notification attempts result in error.
    (3) Push notification attempts give this error on phone: "There was an error completing this request. If this problem persists, contact an administrator."

    Please follow these steps to re-activate your Duo Mobile App:
    (1) Visit https://disco.cisco.com. Click green button. Enter credentials to get to Duo MFA prompt screen. ***Ignore initial authentication request.*** Select 'My Settings & Devices' from left-side options.

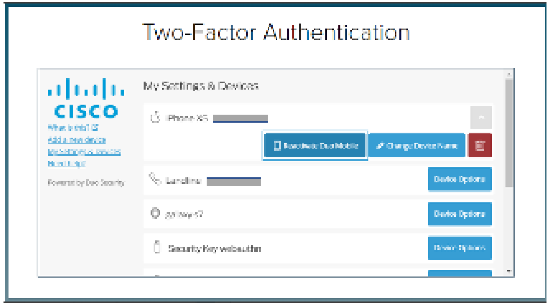


(2) After selecting 'My Settings & Devices', complete the authentication requested at that point.
If you enrolled your phone, and only Duo Mobile App is not working, you may still authenticate using the text message or voice call options with your enrolled mobile phone. If you have a security key registered with your account and are in Firefox or Chrome, you may use this to authenticate as well.


Two-Factor Authentication
CISCO
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security
My Settings & Devices
First, we need to confirm it's really you. Choose an authentication method below to manage your settings and devices.
Choose an authentication device
Choose an authentication method
Duo Push
Send Me a Push
Call Me
Call Me
Use your Security Key to access your settings and devices...
X



(3) Click 'Device Options' beside your mobile phone.



(4) Follow the instructions on the subsequent screens in order to reactivate Duo Mobile App for your account.

17. **I have a new YubiKey 5 Series security key. When I try to register or use in Chrome, I get an "Unable to register." error during the update step.**

1/18/2019 UPDATE - Fix released and validated. Yubikey 5 series should work fine now in both Firefox and Chrome (browser should be on latest GA version). Please use the support options below to report otherwise.

This is currently a known bug. Affecting only the "update" step in Chrome that is trying to register webauthn mode of the key in Chrome.
Target fix date from Duo product team: mid-January 2019.
Once we receive the fix from Duo, we will deploy in the Cisco Duo tenant as soon as possible.

Temporary workaround:
(1) Register your YubiKey 5 Series in an up-to-date version of Firefox browser.
(2) This will register your key in webauthn mode.
(3) Return to Chrome. Register key in Chrome again. This registers the key for U2F mode. The initial attempts to register would have

failed because of the bug error in "update" / webauthn step in Chrome. Since the webauthn mode was already activated in Firefox in (1), the "update" step in Chrome should no longer appear during registration or login.
(4) You should now be able to use your key in U2F mode (seamless entry without selecting in drop-down) in Chrome without being prompted for the update step.

See FAQ #3 above for details on how security key behavior differs currently in Chrome and Firefox.

18. **I forgot/lost my phone and it is the only device I registered in Duo MFA. What can I do?**
    Below applies to all situations where user is "locked out" of Duo MFA due to single registered device being incorrect or unavailable.

    Reach out to IAM support team via Teams (https://disco.cisco.com/teams - Duo MFA Pilot Support Space).
    Support team can help troubleshoot and validate what path forward is available.

    For the future, please make sure to have at least 2 different Duo MFA devices registered among the current options of
    (1) mobile phone (push, text or voice call), yubikey,
    (2) text or voice call to alternate mobile phone or
    (3) voice call to Cisco phone number or personal home number.

    So, if one method is forgotten, lost or stolen, there is a secondary method available for a self service route of going to https://disco.cisco.com and either authenticating for login or authenticating to modify your devices or settings.

19. **Different Duo tenants in Cisco -**
    Cisco Enterprise IT / GIS-IAM (Identity and Access Management) manages the Duo MFA tenant being used for Cisco Enterprise SSO. This wiki page and the below support options are administered by Cisco IT.
    I am having a Duo MFA issue. Is Cisco IT / Identity and Access Management the right team to support me?

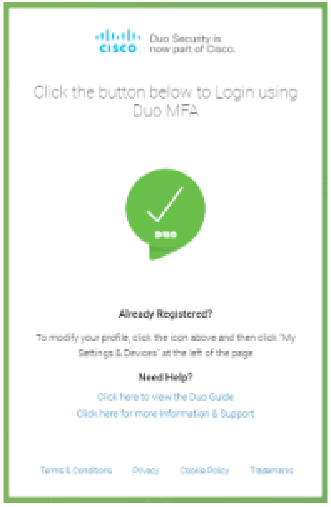
    Dating back before Cisco's acquisition of Duo, other Cisco BUs have purchased and set up their own standalone tenants of Duo MFA.
    This wiki page and support options provided through this page are intended for users seeing Duo MFA as part of Cisco Enterprise SSO login flow.

    If you are logging into applications and websites hosted by these other BUs listed below and are seeing a different UI than the screenshots provided below, then please look for a 'Need help?' link provided on your specific login flow and/or reach out to the direct support team from within that specific Cisco BU.

    Other Cisco BUs having their own Duo MFA tenant:

    AppDynamics
    OpenDNS
    Broadsoft
    Meraki
    GTTS - BU for federal acccounts
    Cisco IoT (Jasper)
    Cisco Talos

    Screenshots for Cisco Enterprise SSO login flow and Cisco IT Duo MFA tenant:



Duo Security is now part of Cisco.

Click the button below to Login using Duo MFA

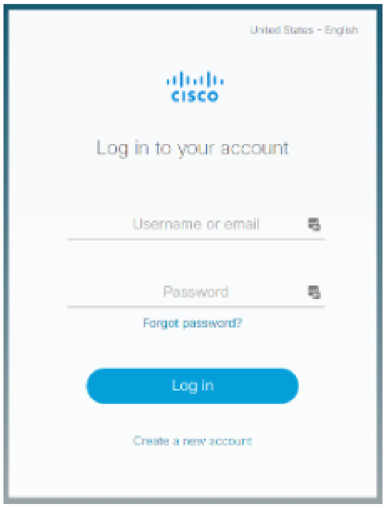
Already Registered?

To modify your profile, click the icon above and then click 'My Settings & Devices' at the left of the page

Need Help?

Click here to view the Duo Guide
Click here for more Information & Support

Terms & Conditions Privacy Cookie Policy Trademarks



United States - English

Log in to your account

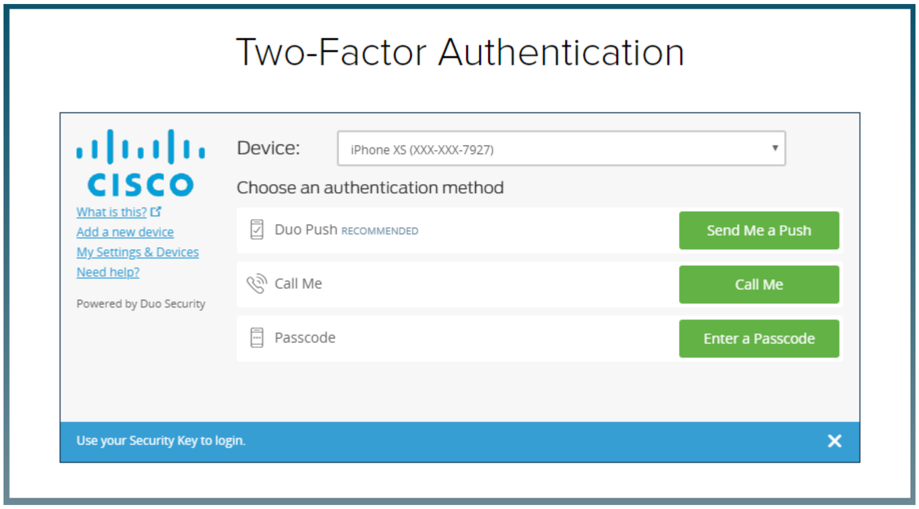
Username or email

Password

Forgot password?

Log in

Create a new account



Two-Factor Authentication

What is this?

Add a new device

My Settings & Devices

Need help?

Powered by Duo Security

Device: iPhone XS (XXX-XXX-7927)

Choose an authentication method

Duo Push RECOMMENDED — Send Me a Push

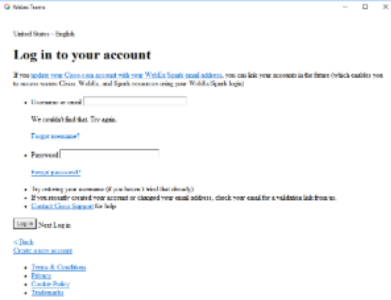
Call Me — Call Me

Passcode — Enter a Passcode

Use your Security Key to login.

20. **I am a Windows user and my 'Two-Factor Authentication' screen is blank. (see screenshots below, click on image to maximize)**

    If your login screens look mal-formatted like the below screenshots, please try the solution provided below.
    You may encounter the below screens in IE, Edge or Windows desktop applications (e.g. Webex Teams, Jabber, AnyConnect, Webex Meetings, etc.) which launch the login flow using an embedded IE/Edge browser frame.



Webex Teams

United States - English

Log in to your account

If you update your Cisco.com account with your WebEx/Spark email address, you can link your accounts in the future (which enables you to access secure Cisco, WebEx, and Spark resources using your WebEx/Spark login)

- Username or email

We couldn't find that. Try again.

Forgot username?

- Password

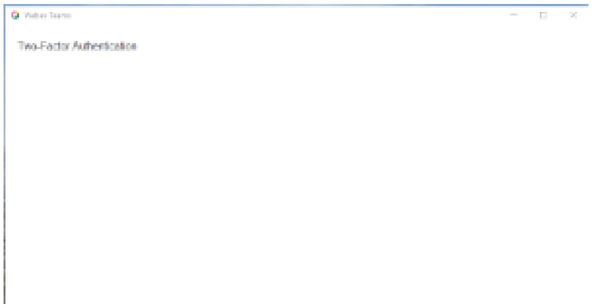
Forgot password?

- Try entering your username (if you haven't tried that already)
- If you recently created your account or changed your email address, check your email for a validation link from us.
- Contact Cisco Support for help

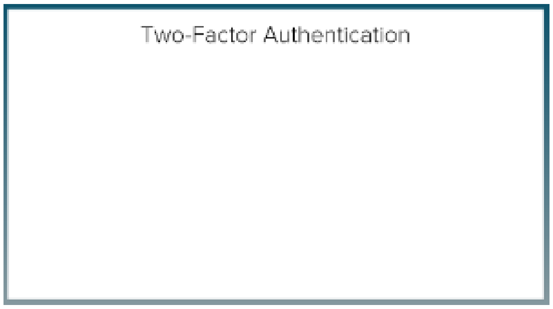
Log in Next Log in

< Back
Create a new account

- Terms & Conditions
- Privacy
- Cookie Policy
- Trademarks



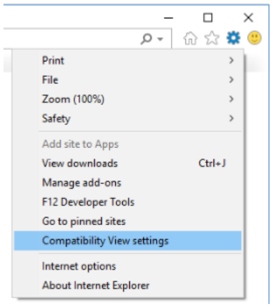
Two-Factor Authentication

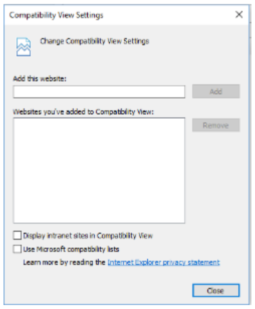


Two-Factor Authentication

Probable Solution:
Every now and then, updates get pushed through Windows Desktop management which inadvertently enable compatibility view in Internet Explorer. Which prevents Cisco SSO login page and Two-Factor Authentication screens from displaying properly, and prevents users from completing login.
The steps below will disable compatibility view again, as it should be.

(click on screenshots below to maximize)
(1) Open Internet Explorer   Click the gear icon   Click 'Compatibility View settings'
(2) If 'cisco.com' appears in the website list, please remove it.
(3) If 'Display intranet sites in Compatibility View' is checked, please uncheck it.
(4) Close the window and close Internet Explorer to make sure the changes are applied.





Compatibility View Settings

Change Compatibility View Settings

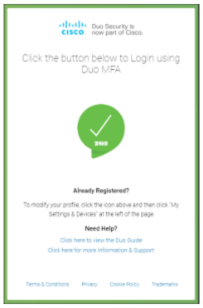
Add this website:

Websites you've added to Compatibility View:

☐ Display intranet sites in Compatibility View
☐ Use Microsoft compatibility lists
Learn more by reading the Internet Explorer privacy statement

21. **The Yubikey product is being used by at least 2 different programs in Cisco IT -**
(1) Access Key program for Admins (Admin Token replacement) and
(2) Duo MFA.
Please see screenshots below to determine if you need help from Duo MFA support channels provided on this wiki page.
For Access Key help, please refer to the Access Key home page.

Duo MFA screenshots:


Duo Security is now part of Cisco.

Click the button below to Login using Duo MFA

Already Registered?

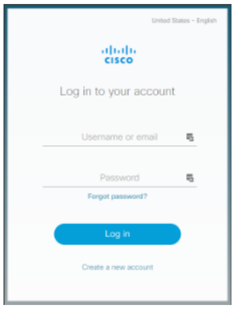
To modify your profile, click the icon above and then click 'My Settings & Devices' at the left of the page

Need Help?

Click here to view the Duo Guide

Click here for more information & Support

Terms & Conditions Privacy Cookie Policy Trademarks


United States - English

Log in to your account

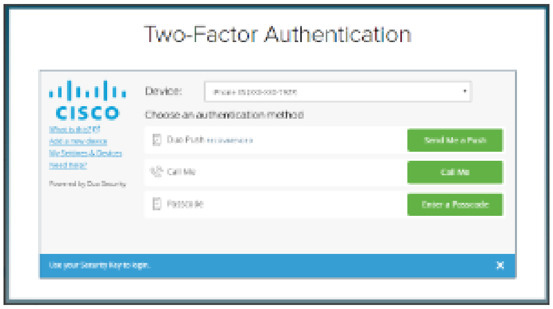
Username or email

Password

Forgot password?

Log in

Create a new account


Two-Factor Authentication

What is this?

Add a new device

My Settings & Devices

Need help?

Powered by Duo Security

Device:

Choose an authentication method

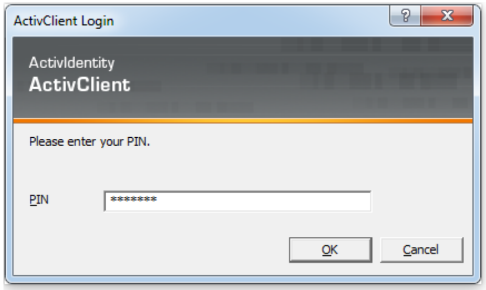
Duo Push — Send Me a Push

Call Me — Call Me

Passcode — Enter a Passcode

Use your Security Key to login.

Access Key screenshots:

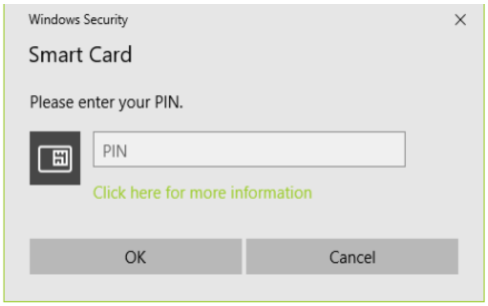

ActivClient Login

ActivIdentity
ActivClient

Please enter your PIN.

PIN *******

OK Cancel


Windows Security

Smart Card

Please enter your PIN.

PIN

Click here for more information

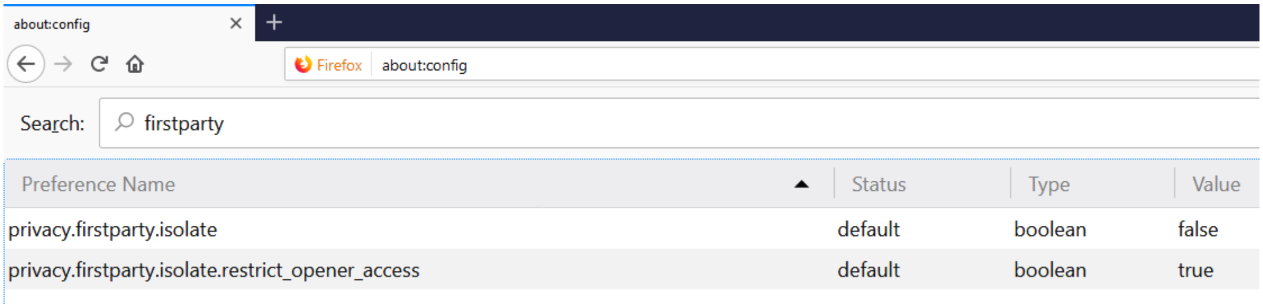
OK Cancel

22. **Duo MFA authentication in Firefox via Yubikey does not work.**
    I select 'Security Key' from device drop-down, then press 'Use Security Key', then touch my Yubikey when prompted. But then authentication does not complete.

    If you have changed some advanced settings in Firefox related to cookie isolation and restricting cookie access, this may be causing your issue.
    Default settings shown in screenshot below will allow authentication to work normally.

    If both values are set to 'true', authentication will fail.

    Authentication will still work if 'isolate' is set to 'true' and 'restrict_opener_access' is set to 'false'.



firstparty

Preference Name	Status	Type	Value
privacy.firstparty.isolate	default	boolean	false
privacy.firstparty.isolate.restrict_opener_access	default	boolean	true

23. **How do I disable automatic submit of YubiKey one-time password (OTP)?**

    YubiKey - Disable OTP Auto Submit

24. **I'm enrolled and using Duo MFA during SSO login. Can I delete the PingID app from my phone now?**

    As long space is not critical on your phone, better to keep PingID on your phone for now until it is completely out of our SSO environment.
    For some unexpected scenario of still getting PingID which may require troubleshooting, better to not have the extra hassle of re-installing at that point.

25. **I don't have access to Google Play store to download Duo Mobile app.**

    Please use the following link to download the .apk directly: https://help.duo.com/s/article/2094?language=en_US

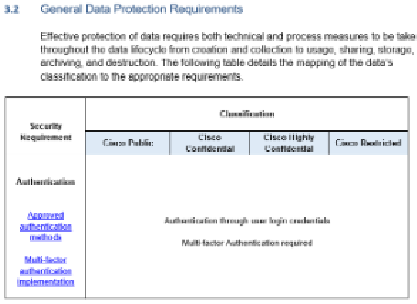
26. **I am having trouble receiving or approving Duo MFA notifications on my mobile phone.**

    Android troubleshooting: https://help.duo.com/s/article/2050?language=en_US

    iOS troubleshooting: https://help.duo.com/s/article/2051?language=en_US

27. **Does Cisco have a policy mandating Multi-Factor Authentication (MFA)?**

    Yes. According to the Data Protection Standard set by Cisco Security & Trust Organization, MFA is required in order to adequately protect all levels of Cisco data.
    Link to full document: https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-806757&ver=approved
    Excerpt (**click for full-size view)** regarding MFA:



3.2 General Data Protection Requirements

Effective protection of data requires both technical and process measures to be taken throughout the data lifecycle from creation and collection to usage, sharing, storage, archiving, and destruction. The following table details the mapping of the data's classification to the appropriate requirements.

Security Requirement	Classification			
	Cisco Public	Cisco Confidential	Cisco Highly Confidential	Cisco Restricted
Authentication				
Approved authentication methods	Authentication through user login credentials			
Multi-factor authentication implementation	Multi-factor Authentication required			

As for Duo MFA as our enterprise MFA solution:

Duo Security was acquired by Cisco in October 2018.
You can learn more here: https://wwwin.cisco.com/c/cec/news/global-employee-headlines/chitchat-with-our-newest-dynamic-duo.html.

During earnings calls, Chuck Robbins has called out Duo as very strategic to our security business as a company. It was imperative that we move our workforce to this product as soon as possible to show our customers how to utilize this product.
With any transition between vendors/products, there are pros/cons of each. The gaps between Duo and PingID were evaluated and shared with executives. Executives supported our use of this product with the gaps, and committed that our workforce would adopt the authentication methods currently provided.
In parallel, we continue to work on improvements. All feedback from the Duo MFA rollout is being considered and shared with the Duo product team in order to continually strive for a better user experience.

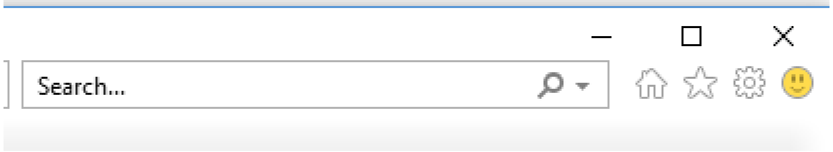
28. **Internet Explorer - SSO is broken. I do successful SSO login - Username/Password/Duo MFA. But then new tab to other Cisco protected website keeps asking for a new login.**

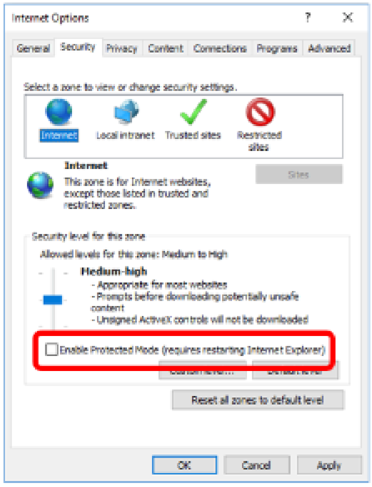
    This is a known issue related to a configuration specific to Internet Explorer.
    Currently does not affect other browsers, to our knowledge.

    How to fix:

    (1) In Internet Explorer, click the "gear" icon at the top right (screenshots below)
    (2) Internet options
    (3) Security tab
    (4) For the 3 zones - "Internet", "Local intranet", "Trusted sites" - make sure "Enable Protected Mode" checkbox is **un**checked
    (5) Close and restart Internet Explorer

    This box does sometimes get re-checked on its own after certain Desktop Windows updates.
    If the problem behavior re-starts, please check this setting again for these 3 zones.
    It is okay to leave checked for "Restricted sites" zone. All other 3 zones should have this unchecked.




Internet Options

Select a zone to view or change security settings.

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone
Allowed levels for this zone: Medium to High
Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

29. To use ZETA App, we need to login to it by using Cisco credentials. After Duo-authentication is put in place, I am not able to login to ZETA App with my Android 6.

Zeta app uses Cisco login credentials and it subject to these checks.

If you are using your mobile device to access an application within Cisco, in this case the Zeta app, then your device is also checked for minimum device standards using Duo. We give more information on this here: https://wiki.cisco.com/display/GISIAM/Duo+Multi+Factor+Authentication#DuoMultiFactorAuthentication-MinimumMobileDeviceRequirements-forDuoMobileAppUse The minimum device standards enforced by Duo are same that are required for Cisco mobile device standards: https://apps.na.collabserv.com/wikis/home?lang=en-us#!/wiki/W4e448aed9990_4e86_a9db_b6dad8282500/page/Compatible%20Devices.

This minimum device standard check is no different than what exists for your laptop. Your laptop is continuously checked that it meets minimum standards and you as the owner/user are expected to remediate any deficiencies, or automated processes will do that for you. If issues are not remediated, then you will eventually be prevented from accessing Cisco resources until action is taken.

Since this is a personal device, the same expectation exists, but you are responsible for remediation. It is your choice to not upgrade your device, but it is a privilege that Cisco allows you to use personal device. If your device does not pass a minimum check, you will be prevented from using it to access Cisco applications, whether they are internally hosted or in the cloud.   You will see this more as we continue to strengthen our security posture at Cisco.

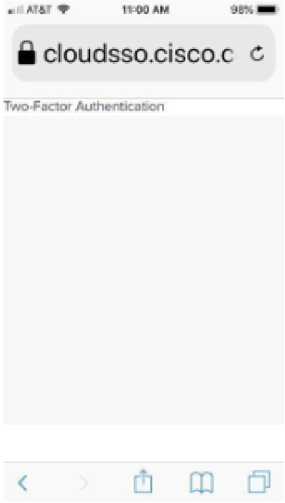
30. How to test Yubikey

If your Yubikey stops working, use these steps to determine if Yubikey is still functioning:

https://support.yubico.com/support/solutions/articles/15000008691-basic-yubikey-troubleshooting

https://support.yubico.com/support/solutions/articles/15000008592-testing-u2f

31. I am seeing a blank authentication screen on my iPhone when I try to authenticate. How do i fix?



The fix involves changing the content restrictions on your iPhone. Please follow these instructions from Duo: https://help.duo.com/s/article/3710?language=en_US

32. What information does Duo collect?

Read more about what Duo collects here: https://help.duo.com/s/article/2939?language=en_US

33. My account has been locked out due to excessive login failures. What do I do?

The lockout will expire in 15 minutes. You can try to login again at that time. No action is required by the Duo team.