

How to Update or Change Your Multi-Factor Authentication Options

This guide will show you how to change your Multi-Factor Authentication options.



What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is a security method that helps keep your accounts safe by requiring more than just a password to log in.

Here's how it works:

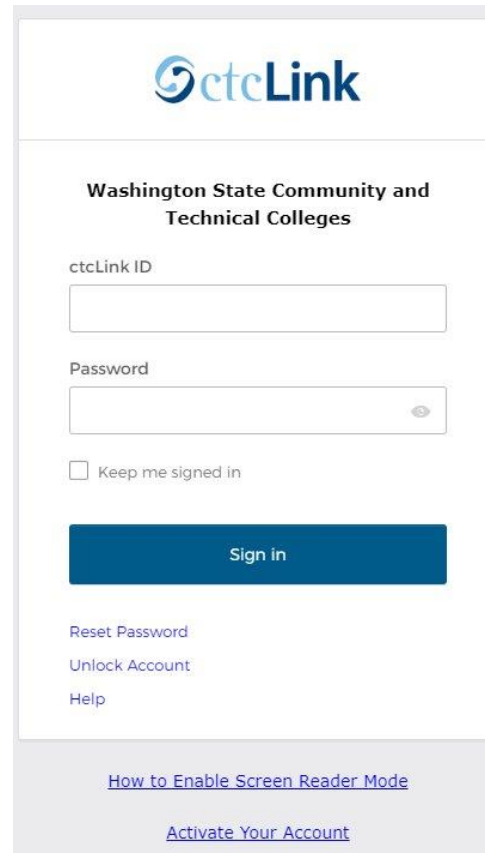
- **Something You Know:** This is usually your password. It's the first thing you use to access your account.
- **Something You Have:** After entering your password, you might need to use another device, like your smartphone. You could get a text message with a code that you have to enter.
- **Something You Are:** Some systems might use your fingerprint or face recognition to confirm your identity. (This step is optional for Peninsula College systems.)

So, even if someone steals your password, they can't get into your account without that second step, like the code sent to your phone. This makes your accounts much safer!



Proceed to ctclink:

1. Open web browser and go to gateway.ctclink.us.

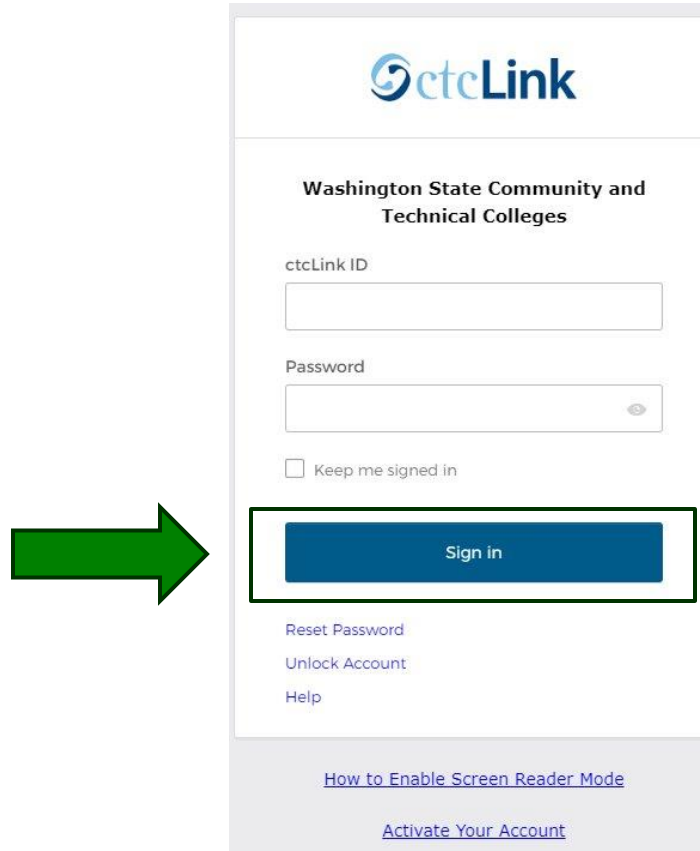


The screenshot shows the ctclink login interface. At the top is the ctclink logo. Below it, the text reads "Washington State Community and Technical Colleges". There are two input fields: "ctclink ID" and "Password". The password field has a toggle icon for visibility. Below the password field is a checkbox labeled "Keep me signed in". A blue "Sign in" button is centered below the checkbox. At the bottom of the form area are three links: "Reset Password", "Unlock Account", and "Help". Below the form area, there are two more links: "How to Enable Screen Reader Mode" and "Activate Your Account".



Enter ctcLink Credentials:

2. Enter your ctcLink ID and password, then click **Sign in**.




The screenshot shows the ctcLink login interface. At the top is the ctcLink logo. Below it, the text reads "Washington State Community and Technical Colleges". There are two input fields: "ctcLink ID" and "Password". Below the password field is a checkbox labeled "Keep me signed in". A blue "Sign in" button is highlighted with a black border and a green arrow points to it from the left. Below the button are links for "Reset Password", "Unlock Account", and "Help". At the bottom of the page are links for "How to Enable Screen Reader Mode" and "Activate Your Account".

Okta Portal:

3. On the ctcLink Gateway page, click on **Okta Portal** under Manage Okta Account Settings in the lower right-hand corner.

ctcLink My Institution View welcome betnary jennings-keily!


PENINSULA COLLEGE

Canvas

Student Homepage

Student Services Center

Advisor Homepage

Faculty Center

CS Staff Homepage

Your Gateway to ctcLink

Welcome!

You have arrived at the ctcLink Gateway for Washington's community and technical colleges. The links at the left should get you everywhere you need to go in ctcLink for your student, faculty or staff online work. Some of you will have links to applications across the top of the page as well.

Your ID is what drives access to all of these links and you will have this same ID forever. Whether you attend more than one Washington community college at a time, work at one or more throughout your career, or even if you go from student to employee or from employee to student, your user ID will never change.

How do I...?

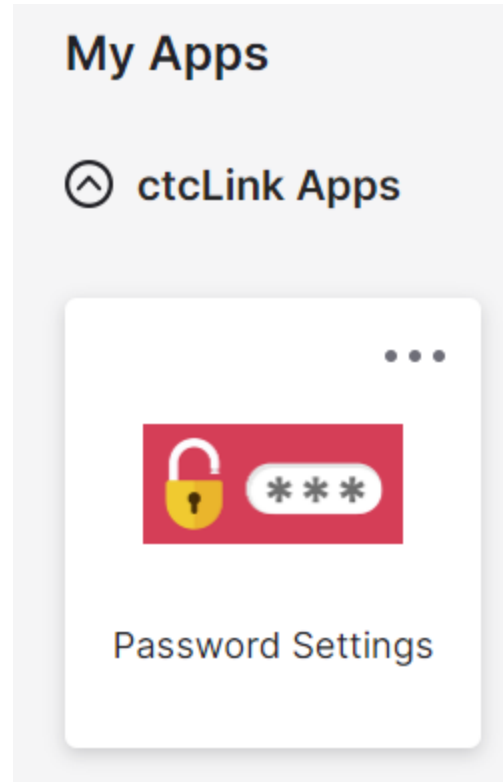
If you need to know how to use some of the ctcLink tools, check out the [ctcLink Training website](#). There you'll find Quick Reference Guides (QRG) and training exercises to get you on your way. More content will be added to the training website as materials are developed.

Manage Okta Account Settings

View the [Okta Portal](#) to manage account recovery details, view recent sign-in activity, and review/update multi-factor authentication settings.

Password Settings:

4. Click on **Password Settings**.



Verify Personal Information:

5. Verify the Personal Information is correct. If email is selected for the MFA option, a verification code will be sent to the 'Primary email' listed. If needed, click **Edit** and follow the prompts to update the primary email.

The screenshot shows the ctcLink user interface. On the left is a navigation sidebar with 'My Apps', 'ctcLink Apps', 'Add section', and 'Notifications'. The main content area is titled 'Account' and contains three sections: 'Personal Information', 'Display Language', and 'Security Methods'. The 'Personal Information' section has a dark header with an 'Edit' button, which is highlighted by a green arrow. Below the header are input fields for 'First name', 'Last name', 'Okta username', 'Primary email', 'Secondary email', and 'Mobile phone'. The 'Display Language' section shows 'Language' set to 'English' with a note that the default language has been automatically set. The 'Security Methods' section lists various authentication options with 'Set up' or 'Remove' buttons: Password (Reset), Okta Verify (Set up), Security Key or Biometric Authenticator (Set up), Google Authenticator (Set up), Phone (Set up another, Remove), and Security Question (Remove).

Update Security Methods:

6. Set up at least one security method for multi-factor authentication to your account. You can choose from the following options: Okta Verify, Google Authenticator, or Phone. After choosing a method, click **Set up**.


Note: We are unable to use Security Key or Biometric Authenticator at this time.

✓ Security Methods	
Security methods help your account security when signing in to Okta and other applications.	
Password	Reset
Okta Verify	Set up
Security Key or Biometric Authenticator	Set up
Google Authenticator	Set up
Phone	Set up another
	Remove



Option 1: Okta Verify

Select **Set up**. Download the Okta Verify app on your device. Scan the QR code.




ctcLink

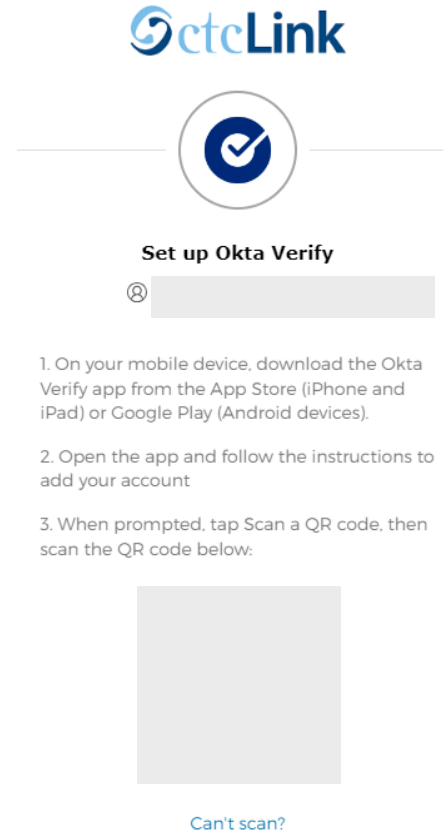
Set up security methods

Security methods help protect your ctcLink account by ensuring only you have access.

Set up required

-  **Okta Verify**
Okta Verify is an authenticator app, installed on your phone, used to prove your identity
Used for access

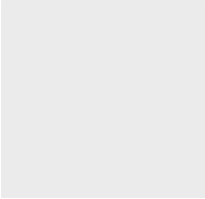
Set up



ctcLink

Set up Okta Verify

1. On your mobile device, download the Okta Verify app from the App Store (iPhone and iPad) or Google Play (Android devices).
2. Open the app and follow the instructions to add your account
3. When prompted, tap Scan a QR code, then scan the QR code below:



[Can't scan?](#)



Option 2: Google Authenticator

Select **Set up**. Download the Google Authenticator app on your device. Scan the QR code.

The image displays two sequential screenshots from the ctcLink account setup interface. The left screenshot, titled "Set up security methods", shows a user's email address in a greyed-out field. Below the field, it states "Security methods help protect your ctcLink account by ensuring only you have access." Under the heading "Set up required", there is a section for "Google Authenticator" with a small circular icon containing a 'G'. The text reads: "Enter a temporary code generated from the Google Authenticator app. Used for access". A green arrow points to a "Set up" button located at the bottom of this section. The right screenshot, titled "Set up Google Authenticator", shows the same email field. Below it, the text says "Scan barcode" and "Launch Google Authenticator, tap the '+' icon, then select 'Scan barcode'." A large grey square with a dashed line at the bottom represents the QR code area. Below this area is a "Can't scan?" link. At the bottom of the screen is a blue "Next" button.

Option 3: Phone Number

Select **Set up**. Select SMS or Voice call, choose country, and add your phone number. Click **Receive a code** and enter the code sent to your phone number.

The image shows two screenshots of the ctcLink user interface. The left screenshot is titled "Set up security methods" and shows a list of security options. The "Phone" option is highlighted with a blue circle and a phone icon. Below it, the text reads "Verify with a code sent to your phone" and "Used for access or recovery". A green arrow points to a "Set up" button. The right screenshot is titled "Set up phone authentication" and shows a form for entering a phone number. It includes a radio button for "SMS" (which is selected), a radio button for "Voice call", a "Country" dropdown menu set to "United States", and a "Phone number" input field containing "+1 360-123-4567". A green arrow points to a blue button labeled "Receive a code via SMS".

Success:

7. Done! Your Multi-Factor Authentication method has been updated.



If you have any questions or need further assistance contact the IT Help Desk at (360) 417-6565 or helpdesk@pencol.edu

