PortalGuard First Login Setup Steps

When first logging in to PortalGuard you will be presented with some extra steps that need to be completed.

1. Visit https://sso.imperial.edu
2. Enter in your current **IVC Email** and **Password**.
3. Click the **Login** button to start the initial Enrollment process.

IVC Email

jdoe12@students.imperial.edu

Password

•••••••••

Login   Set Passv

4. You will need to enroll a Personal Email Address in the next step (this is **REQUIRED**). Simply enter in a personal email address and click the **Continue** button (make sure you have quick access to your personal email account available when you do this to make this as quick as possible). One caveat here regarding the personal email address you use: issue reports have been made when a personal Yahoo email account has been used (the email doesn't arrive correctly due to Yahoo's more stringent blocks) and reports related to Hotmail have shown the message can arrive in the Junk Mail as well.

EMAIL ENROLLMENT

You must login using One Time Passcodes (OTP) sent to your email.

Please enter your current password and email address to enroll. A test OTP will be sent immediately for confirmation.

IVC Email   oramos1@students.imperial.edu

Password   •••••••••••••••

Email Address

Continue   Cancel

5. The next step requires that you have checked your personal email account and found the email from "IVC PortalGuard" that contains the One Time Passcode. Go ahead and copy/paste it in to the page, or type it in manually and click the **Login** button.

ONE TIME PASSCODE REQUIRED

A One Time Passcode (OTP) will be delivered as an email to:
oxxxxx@gmail.com

It could take 10 to 15 seconds to be delivered. Upon receipt, please enter the OTP below to continue.

IVC Email	oramos1@students.imperial.edu
Password	••••••••
One Time Passcode	

Problems with the OTP?

| Login | Cancel |

6. Next, we have two optional steps (and they also have the option for suppressing reminders for these too).

7. The first optional step is enrolling a mobile phone number which can be used for receiving a text when resetting your password. If you don't want to do this, simply click on the **Permanently Suppress Reminders** checkbox and then click on **Skip**.
If you do choose to set this up, please enter in your phone number and click on **Continue** and a text will be sent to the number that will need to be entered to confirm the mobile phone enrollment.

ENROLLMENT - MOBILE PHONE

Please enter your current password and your phone number to enroll. You may also be prompted to select a mobile phone carrier from a drop-down list. A test message will be sent immediately for confirmation. You can skip this enrollment but you will be asked to enroll again during your next login.

To **permanently** suppress reminders for this authentication type, check the box below before skipping. You can always enroll from the Account Management page.

IVC Email	oramos1@students.imperial.edu
Password	•••••••••••••••
Country	United States ▾
Phone Number	

☐ Enable Multi-Factor Login

☐ **Permanently Suppress Reminders**

| Continue | Skip |

8. The last optional step is the Mobile Authenticator enrollment. If you aren't familiar with what this is simply click on the **Permanently Suppress Reminders** checkbox and then click on **Skip**.

If you are interested in setting this up, IVC recommends using the Authy app
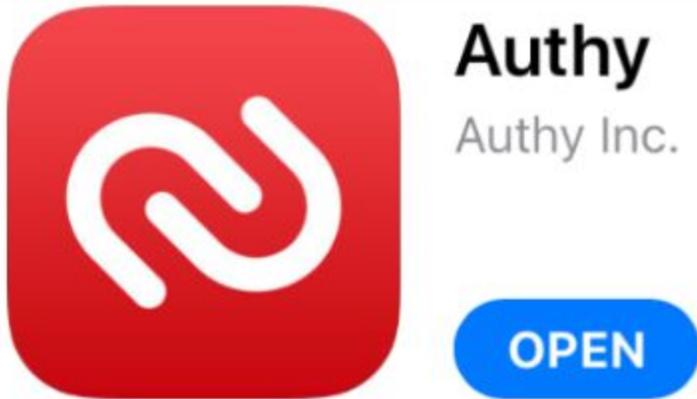
(https://authy.com/download/). You'll want to take some time to get the Authy app setup ahead of time using a personal email address (that way you can use Authy for IVC and other non-IVC services that use a mobile authenticator). Once you have the app setup, it'll have an option to Add in a new source. Once you hit **Continue** in the screenshot below you'll be presented with a QR code. This QR code will need to be scanned into the app and you should then see a One Time Passcode being generated every 30 seconds. You'll need to enter in the current code to confirm the mobile authenticator enrollment.


9. At this point, once you go to the next screen you should be able to see the PortalGuard Account Management page.
    a. You can come here to make further account adjustments in the future:
        i. Enable Disable Multi-Factor (2FA) for your account
        ii. Adjust the OTP Delivery Methods (default will be set to email, so you can change this to be Phone or Mobile Authenticator manually)
        iii. You can print out a list of backup one-time passcodes to use (without needing a phone/email/etc.)
        iv. You can remove your existing phone number and mobile authenticator settings and change your personal email address.

After Login:

1. After logging in you'll either be logged in to the service you were trying to get into or you will be taken to the PortalGuard "Jump Page" which has the links to the services you can login to via SSO:
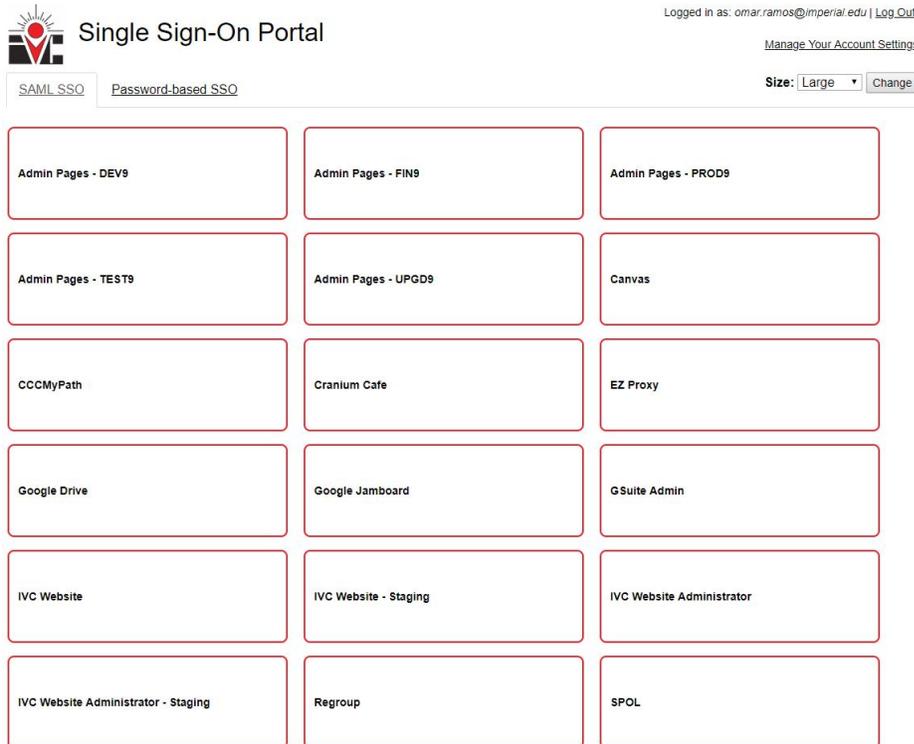
2. If you want to make any adjustments to your account (change the personal email address you used initially, update the phone number, turn on/off multi-factor authentication, enable/disable a mobile authenticator app, etc.) you can do so via the "Manage Your Account Settings" link in the top right corner of the Jump Page:

3. On the Account Settings/Management page you will be able to make any adjustments to those areas as needed (note, that there aren't any password reset/update options presented here since those are

only accessible on the login page prior to actually logging in):

Account Management

Account Details & Activity

Registered Email Address

Linked User Accounts

Enable/Disable Multi-Factor

OTP Delivery Methods

Registered Phones

Printed One Time Passcodes

Mobile Authenticator

Remembered Browser Sessions

Password Reset:

1. You can't reset your password from the Account Management page but now that you have done all of the initial setup work. If you logout and get back to the PortalGuard login page, you can enter in your IVC Email and Password again, but this time click on the **Set Password** button.
2. At this point PortalGuard will by default be sending an email with a one-time passcode to you, unless you have opted to use one of the other options (such as phone or mobile authenticator).
3. Once you've entered in that one-time passcode that was sent to you, it should let you set a new password.
4. At the end of the process it should show a success window showing that the password has been updated successfully.

Forgotten Password:

1. These follow a similar process as the Password Reset, except you click on the **Forgot Password?** button on the login page and you don't need to provide your current password. You will still be sent a One Time Passcode (via email by default, unless you've changed this to the Phone or Mobile Authenticator options and have those setup).

OTP Delivery Methods:

If you'd like to receive your One Time Passcodes via Phone or Mobile Authenticator, you'll need to be logged in and be on your Account Management page.

Expand the OTP Delivery Methods slider and you should have the option to change your OTP Delivery Method preferences:

OTP Delivery Methods

OTP Delivery Methods

Default OTP Methods

Action	Method	Modify
Website Login	Email	Change
Password Change	Email	
Account Unlock	Email	Change
Password Reset	Email	Change

Change Default OTP Method

Please choose the default One Time Passcode (OTP) method for **website login**.

OTP Method: Email

Phone
Email
Mobile Authenticator
Help Desk

Contin... | ...ancel

Future 2FA Requirements

Imperial Valley College will eventually be requiring that all users use what is called two factor authentication since this will help prevent unwanted access to accounts from attackers around the world that are constantly trying to get into accounts at higher education institutions and it is something that a lot of institutions have already started requiring.

In addition to your IVC Email and Password, two factor authentication means that you will also be required to receive a One Time Passcode (either via Email, Phone/SMS, or via a Mobile Authenticator app on your phone).

The most secure out of the three options is the Mobile Authenticator app and is the only option that does not require internet access once the initial setup has been completed (your phone can be in airplane mode and you'd still be able to get One Time Passcodes generated on the app).

To enable Two Factor Authentication for your account, from the **Account Management** page expand the **Enable/Disable Multi-Factor** slider and click on the **Enable Multi-Factor for my account** option.

Enabling Multi Factor Later from Account Page

You'll be prompted to confirm this is what you want to do:
I can hit "Enable Multi-Factor for my account" link:

After enabling Multi-Factor, it ends up utilizing the default "Email" method under the OTP Delivery Methods area unless you've already adjusted the settings to your preferred option.