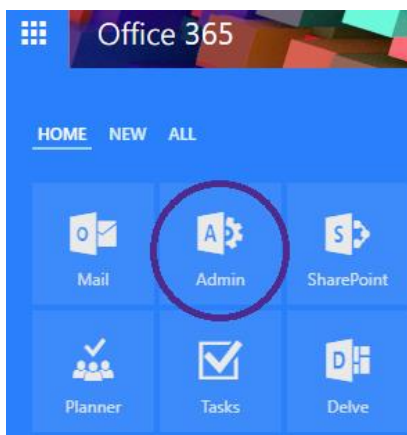


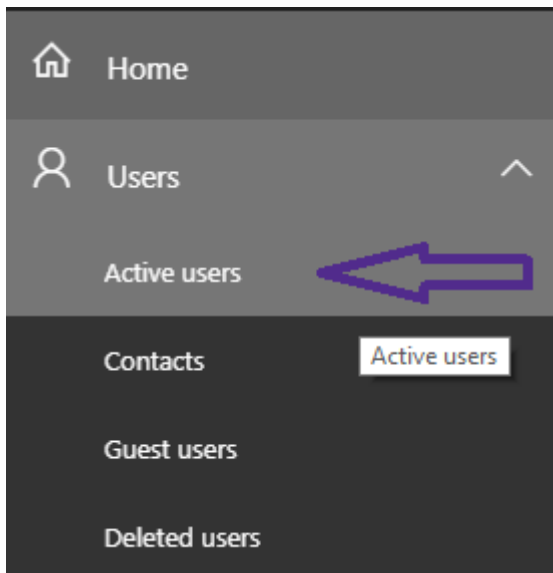
## How to set up modern Multi-Factor Authentication (MFA) with Office clients on Office 365

Set up MFA in Office 365 Admin Center

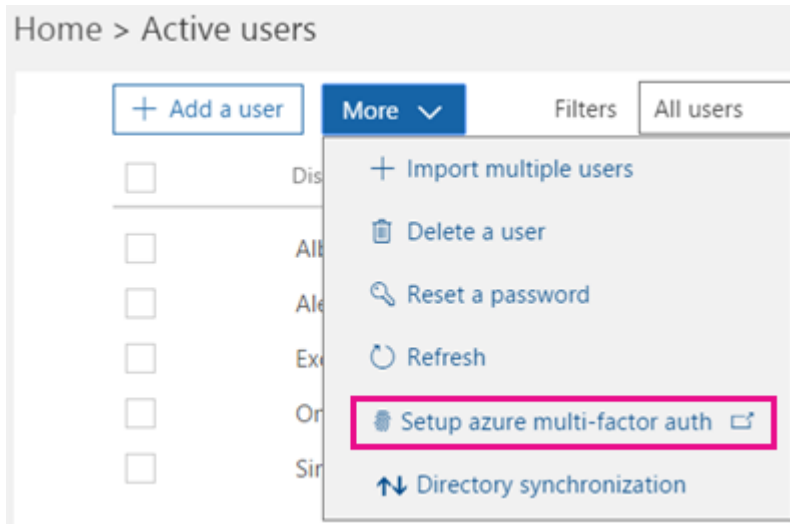
1. Sign in to Office 365 with your usual login and password
2. Go to the App Launcher (waffle) at top left and click on **Admin**



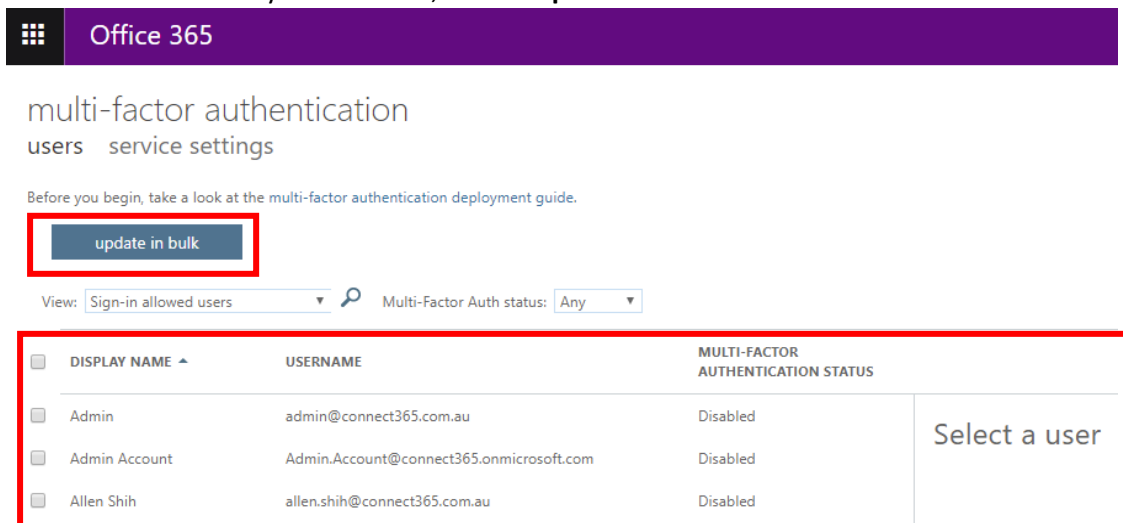
3. Navigate to **Users**, expand the menu by clicking on the arrow, then select **Active users**



- In the Office 365 Admin Center, click **More**, then select **Set up azure multi-factor auth** (without ticking to select any users). This will open a new browser window.



- Select the users from your users list, or click **update in bulk** to enable for all users.



6. Once users are selected, click **Enable** on the right side of the page

## multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

**bulk update**

View:  Multi-Factor Auth status:

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	365SG Accounts	accounts@365solutionsgroup.com.au	Enabled
<input type="checkbox"/>	365sg admin	administrator@365solutionsgroupau.onmicrosoft.com	Enabled
<input type="checkbox"/>	365SG Admin	admin@365solutionsgroup.com.au	Enabled
<input type="checkbox"/>	365SG Michael Andrew Ferrer	michael@365solutionsgroup.com.au	Enabled
<input type="checkbox"/>	365SG Sales	sales@365solutionsgroup.com.au	Enabled
<input type="checkbox"/>	365SG Support	support@365solutionsgroup.com.au	Enabled
<input type="checkbox"/>	Hardeep Brar	hardeep.brar@365solutionsgroup.com.au	Enforced
<input type="checkbox"/>	Kim Brian	kim.brian@365solutionsgroup.com.au	Enforced
<input checked="" type="checkbox"/>	Mohammad Norouzzadeh	Norouzzadeh.M@365solutionsgroup.com.au	Disabled
<input type="checkbox"/>	Tristram Morgan	tristram.morgan@365solutionsgroup.com.au	Enforced

**Mohammad Norouzzadeh**

Norouzzadeh.M@365solutionsgroup.com.au  
Level 15, 97 Creek St  
1300 228 744

quick steps

**Enable** ←

Manage user settings

7. After enabling MFA, users will need to log out and back in to Office 365, at which point they will be required to set up their additional security verification method, with the options being a phone call or text message.



## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

### Step 1: How should we contact you?

Authentication phone

Australia (+61)

Method

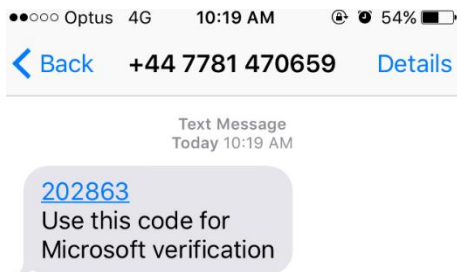
Send me a code by text message

Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

8. In this example, we will select the first method **Send me a code by text message**
9. Enter your mobile number and select the first option, then click **Next**

10. You will receive a code from Microsoft on your phone.



11. Enter the code you receive into the text field, then click “Verify”.

### Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

**Step 2: We've sent a text message to your phone at +61 0481755920**

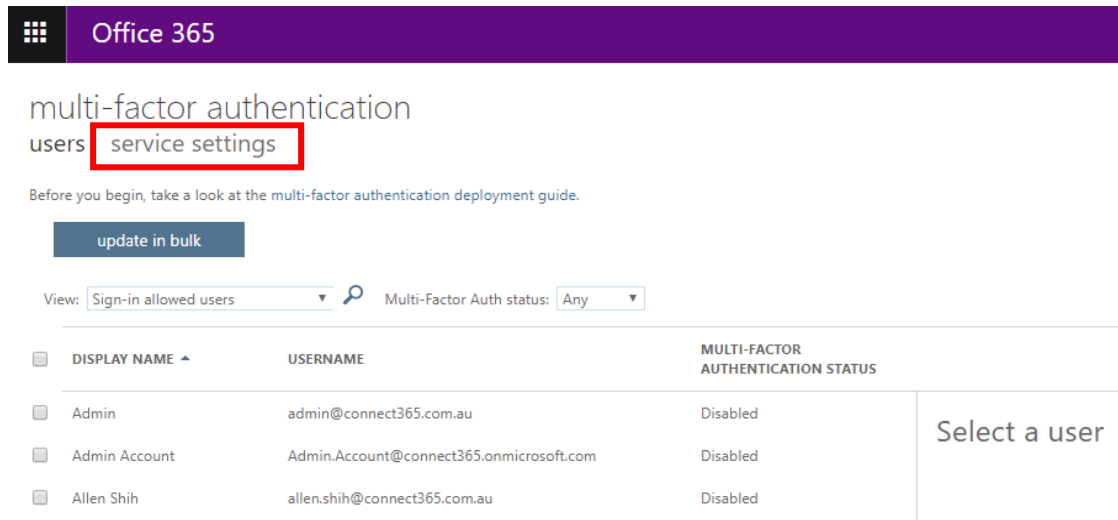
When you receive the verification code, enter it here

12. The process of enabling MFA is now complete, and you will be redirected to your Office 365 landing page. You will be required to use MFA each time you log in once it is enabled, unless you choose to whitelist certain IP addresses. For example, you may wish to enforce MFA for all logins except when users are directly connected to your network, i.e. in the office.

## Skip multi-factor authentication from your intranet

1. Repeat steps 1. to 4. as above. Click on **service settings**.



The screenshot shows the Office 365 administration interface. At the top, there is a purple header with the Office 365 logo and the text "Office 365". Below this, the page title is "multi-factor authentication users" with "service settings" highlighted in a red box. A link "update in bulk" is visible. Below that, there are filters for "View: Sign-in allowed users" and "Multi-Factor Auth status: Any". A table lists users with columns for "DISPLAY NAME", "USERNAME", and "MULTI-FACTOR AUTHENTICATION STATUS". All listed users have a status of "Disabled". A "Select a user" button is on the right side of the table.

<input type="checkbox"/>	DISPLAY NAME ^	USERNAME	MULTI-FACTOR AUTHENTICATION STATUS
<input type="checkbox"/>	Admin	admin@connect365.com.au	Disabled
<input type="checkbox"/>	Admin Account	Admin.Account@connect365.onmicrosoft.com	Disabled
<input type="checkbox"/>	Allen Shih	allen.shih@connect365.com.au	Disabled

6. Tick the option under **trusted IPs**, insert your company IP address subnets, then click **save**. You can also enable devices to remain authenticated without needing MFA for a period of up to 60 days.

## multi-factor authentication

users **service settings**

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27  
192.168.1.0/27  
192.168.1.0/27

verification options [\(learn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app

remember multi-factor authentication [\(learn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust  
Days before a device must re-authenticate (1-60):

save

Manage advanced settings and view reports [Go to the portal](#)

7. Easy way to find the company's IP address is to go to a web site such as <http://www.whatsmyip.org/> or <http://www.howtofindmyipaddress.com/>. The IP address should be in the format of aaa.bbb.ccc.ddd (e.g. 192.168.0.1).

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

1 error(s) found. Place cursor on the red highlighted lines for more information.

Invalid IP address subnet: **Please verify that it's using CIDR notation.**

192.168.0.1

To match the CIDR notation, add /32 to the end of the IP address in order for the system to accept it (e.g. 192.168.0.1/32). Click **save** in the bottom to update.

trusted ips [\(learn more\)](#)

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

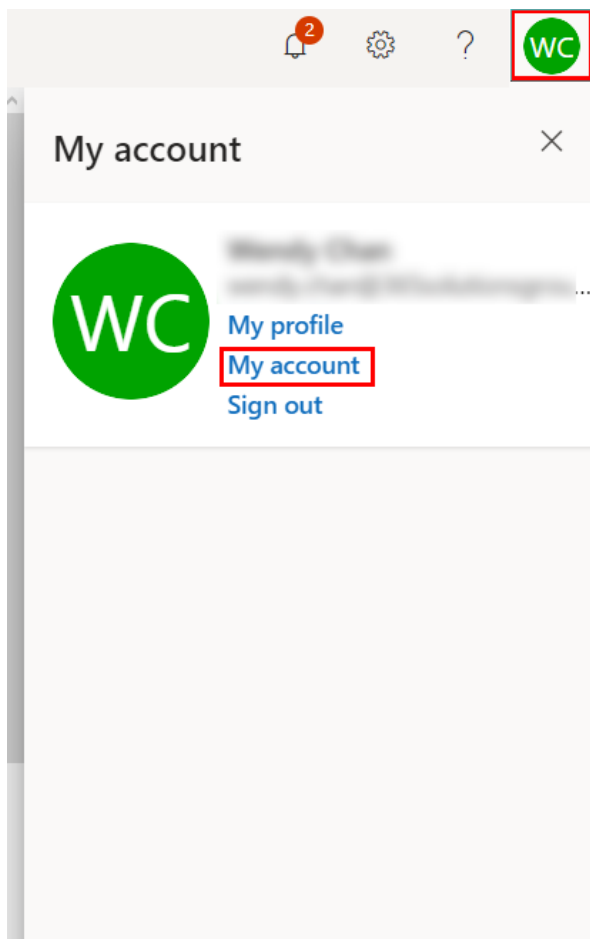
192.168.0.1/32



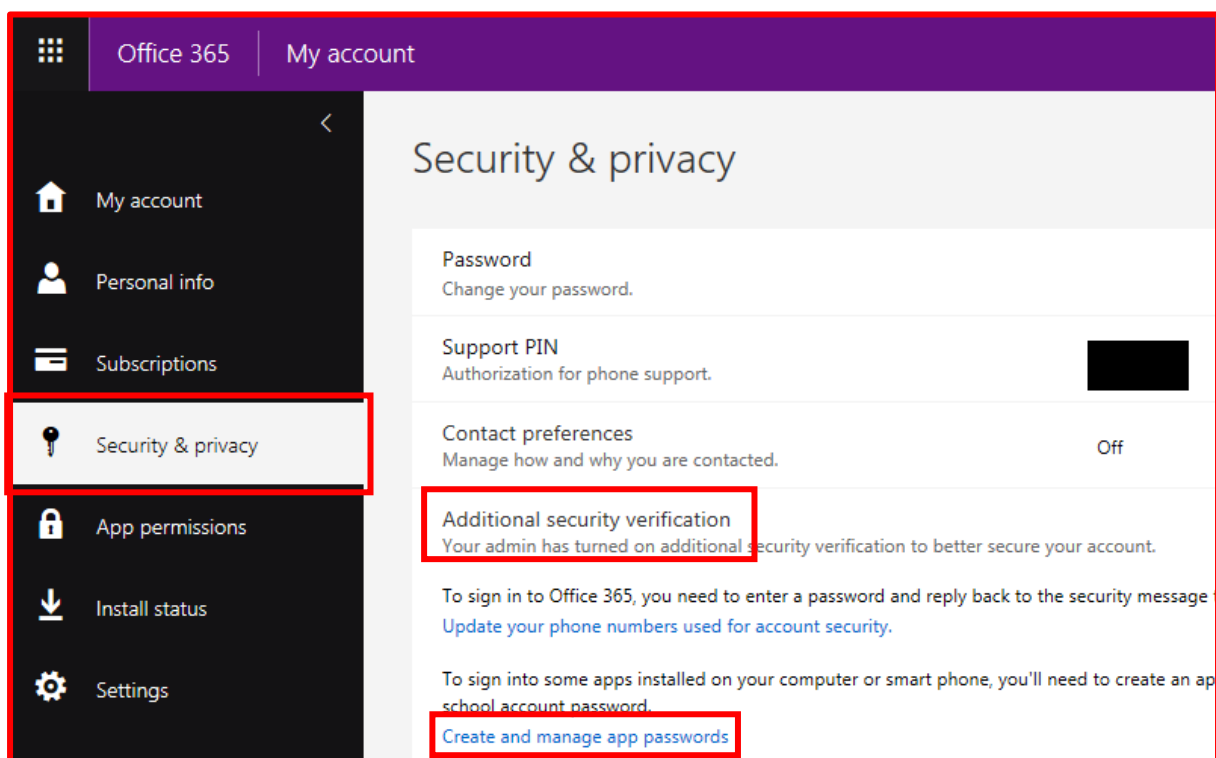
**NOTE!** This solution (adding the /32) only works when you are connecting to the internet through a modem. If you are connecting to the internet through a router, please seek advice from your IT department.

8. After setting up the MFA, some apps, such as Skype for Business or mail apps on some smartphones, ask for an app password. This is not the same password that is used to sign in to the Office 365 environment.

To create an app password first sign into your office online environment <https://www.office.com>. Then on the main site click on the **My account** icon on the top right corner and from the menu that appears, click on **My account** just below 'My profile'.



From the next page click on **Security & privacy** from the left menu and then click on **Additional security verification**. From the two options that appear, click on the bottom one: **Create and manage app passwords**.



On the next page click on **create**. Give the app password a name e.g. 'Skype'. The next window will show you the created app password. Make sure that you copy the password before you close this window, because once you close it, you won't be able to see it again and have to create another password. Once you have copied the password you can close the window.

