

# Public

- [Office 365 MFA User Setup](#)
- [Response to Compromised or Breach Email \(in progress\)](#)
- [Bulk Contact migration on iPhones](#)

# Office 365 MFA User Setup

Summary: This article provides url for 2Factor,2FA,MFA,Microsoft,O365,Email,Prompt

<https://aka.ms/mfasetup>

Click Above

Sign in to your account

If multiple users use the email provided add more then one multiple factor authentication method  
IE. Cell Phone for User1

Office Phone for User2

MultiFactor Authentication App like Authy, Microsoft Authenticator or other

Note: If using Authy or something besides Microsoft you have to click "Use Verification Code" then select the link Configure app without notifications

Microsoft

## 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 ▼

United States (+1) ▼

Invalid phone number. Please provide a phone number in following format: 999 999 9999

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.

©2022 Microsoft Legal | Privacy

Turn on for everyone

entra.microsoft.com/#view/Microsoft\_AAD\_IAM/TenantOverview.ReactView?Microsoft\_AAD\_IAM\_legacyAADRedirect=true

Microsoft Entra admin center

Home >

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity governance

External Identities

Show more

Protection

Learn & support

Home >

Add Manage tenants What's new Preview features Got feedback?

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview Monitoring **Properties** Recommendations Tutorials

Name

Country or region United States

Data location United States datacenters

Notification language English

Tenant ID 36735f41-bd13-4774-a6e1-27fae1a7a45d

Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

Angel Support (angelsupport@cohassetgifts.com) can manage access to all Azure subscriptions and management groups in this tenant. [Learn more](#)

No

Security defaults

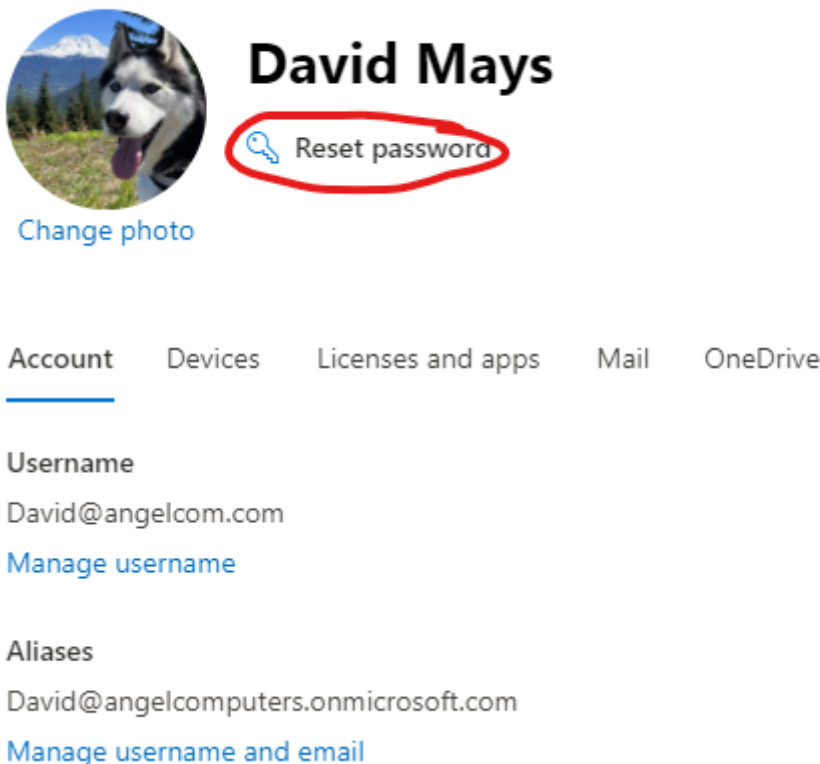
Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators can manage security defaults. [Learn more](#)

✓ Your organization is protected by security defaults. [Manage security defaults](#)

# Response to Compromised or Breach Email (in progress)

If a user has their email and/or password compromised, please follow the instructions below as quickly as possible to secure the account.

1. Reset User Password in the Office 365 admin page, [Admin Portal](#) Users>Active Users



**David Mays**

[Reset password](#)

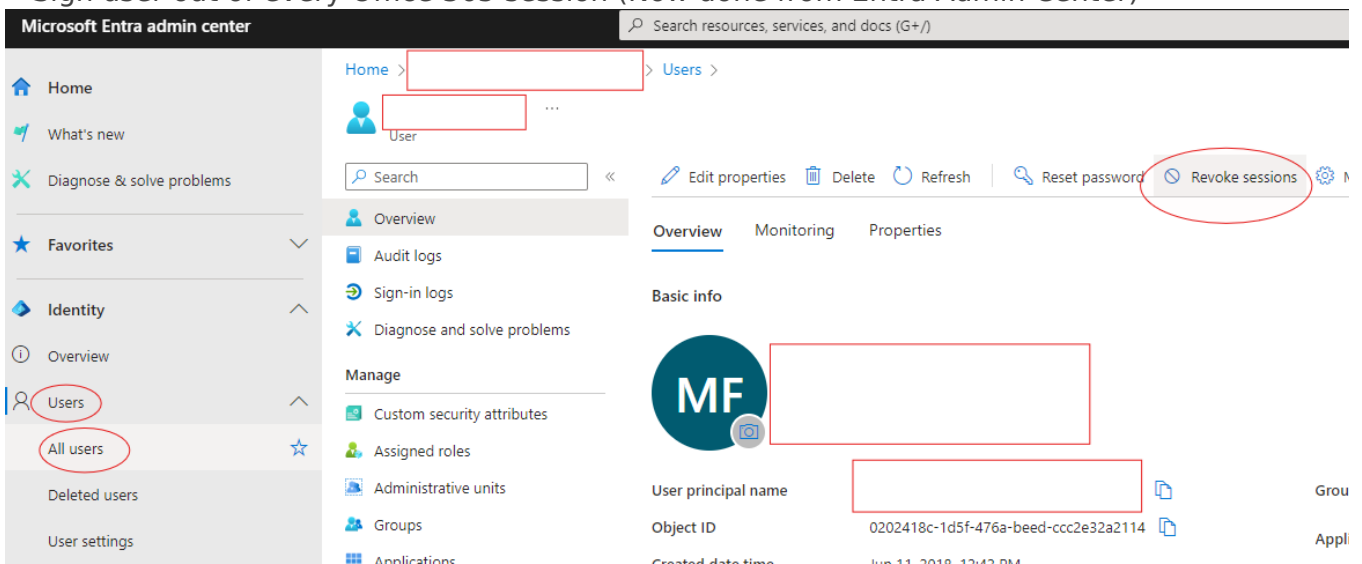
[Change photo](#)

[Account](#) [Devices](#) [Licenses and apps](#) [Mail](#) [OneDrive](#)

**Username**  
David@angelcom.com  
[Manage username](#)

**Aliases**  
David@angelcomputers.onmicrosoft.com  
[Manage username and email](#)

2. Sign user out of every Office 365 session (Now done from Entra Admin Center)



**Microsoft Entra admin center**

Search resources, services, and docs (G+/J)

Home > [redacted] > Users >

User

Search

Edit properties Delete Refresh Reset password **Revoke sessions**

Overview Monitoring Properties

**Basic info**

MF [redacted]

User principal name [redacted] Group

Object ID 0202418c-1d5f-476a-beed-ccc2e32a2114 Appli

Created date time Jun 11, 2018, 12:42 PM

### 3. Setup MFA

### 4. Reset MFA if it was already setup (Do this through Endpoint Manager)

\*\*If endpoint manager is not available through 365 admin, going incognito and signing into entra.microsoft.com will bring you to the area below as well\*\*

Dashboard > Users > Kavita Rama

User

## Authentication methods

« Save Discard Reset password Require re-register MFA Revoke MFA sessions Got feedback?

Switch to the new user authentication methods experience! Click here to use it now. →

Authentication methods are the ways you users sign into Azure AD. Here, you can set the phone numbers and email addresses that users use to perform multi-factor authentication and self-service password reset, and reset a user's password.

### Authentication contact info

Phone

Alternate phone

Email

Alternate email is now managed on the [Profile](#) page

Diagnose and solve problems

Manage

- Profile
- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

Troubleshooting + Support

- New support request

5. Look at sign in logs and take note of irregular locations. Export data and format into a neat excel workbook and name it "Summary of Breach for [user's name]". We want to make this a report that the user's manager can document since banks (or some vendors) will require some of this info and action plans from our clients to restore access.

Dashboard > Users > Kavita Rama

User

## Sign-in logs

« Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date: Last 24 hours Show dates as: Local User contains 8e6837b2-687a-4047-904d-a79892a7e8b4 Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User	Application	Status	IP address	Location	Conditional Access	Authentication re...
4/8/2022, 10:30:04 AM	1f55c071-9644-4a7d-...	Kavita Rama	My Access	Success	50.208.200.93	Snohomish, Washing...	Not Applied	Multi-factor authentic...
4/8/2022, 10:30:01 AM	9f232c63-dd00-4e85-...	Kavita Rama	Microsoft Account Co...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:59 AM	df16cf39-008a-4a1e-a...	Kavita Rama	My Profile	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:56 AM	27386062-a1f1-4cde-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:56 AM	e44fc109-7844-43f5-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:56 AM	9e68d09a-62d2-42ee-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:56 AM	7d969ede-0145-41a1-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:56 AM	d10176bb-f163-4c31-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Snohomish, Washing...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:52 AM	d902568b-f4f6-4f3b-...	Kavita Rama	OfficeHome	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:29:49 AM	07590d10-49bf-426a-...	Kavita Rama	OfficeHome	Interrupted	50.208.200.93	Snohomish, Washing...	Not Applied	Multi-factor authentic...
4/8/2022, 10:28:42 AM	9e68d09a-62d2-42ee-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:28:42 AM	81e4fa3b-1652-4384-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:28:42 AM	d82856ec-cad7-4c4d-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:28:39 AM	2120fcca-c635-4e7d-...	Kavita Rama	OfficeHome	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...
4/8/2022, 10:25:32 AM	021d4b24-f4f6-4285-...	Kavita Rama	Office 365 Exchange ...	Failure	102.89.32.77	NG	Not Applied	Single-factor authenti...
4/8/2022, 10:24:01 AM	a3ed0926-c9c4-4cae-...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Snohomish, Washing...	Not Applied	Multi-factor authentic...
4/8/2022, 10:24:01 AM	a568f977-1f03-4af6-8...	Kavita Rama	Office365 Shell WCSS...	Success	50.208.200.93	Seattle, Washington, ...	Not Applied	Multi-factor authentic...

6. Look in Outlook OWA (or access individual mailbox through exchange admin center) for any odd rules redirecting emails or deleting emails.
  7. In Exchange Admin Center, pull a message trace for any email sent by that user for a timeframe that covers the whole breach. Export those results into a second page in the excel workbook that you started and format it with relevant columns and make it easy for the user to read.
  8. Look for any Registered devices in Azure that aren't good devices
  9. If user is a Global Admin go to next section
  10. Send an email to the relevant manager of that user with the user CC'd with a small summary of what kind of compromise it was (session hijack/user provided access, or something else?) and attach the summary workbook. That will give them the info of when the bad guy got access and what emails they were able to send and to whom. I am attaching an example email to this documentation with sensitive data removed but will show what the client should see.
  11. If you're fully satisfied that the account is secured again, remove the user from "Restricted Entities" if they're still there: <https://security.microsoft.com/restrictedusers>
- 

#### Was the User a Global Admin?

1. Verify if the user needs to be a Global Admin
2. Remove all unnecessary Global Admins
3. Look for any outbound connectors in Exchange that don't belong
4. Look for any rules in Exchange that don't belong
5. Verify all users have MFA enabled

There is also this company that specializes in digital investigations and stuff, called Asceris. I am putting their name down here as a potential partner in the future  
<https://www.asceris.com/bec> if clients ever need a investigation specialist type service that is more indepth than our own stuff (I don't even know if they're more in-depth yet)

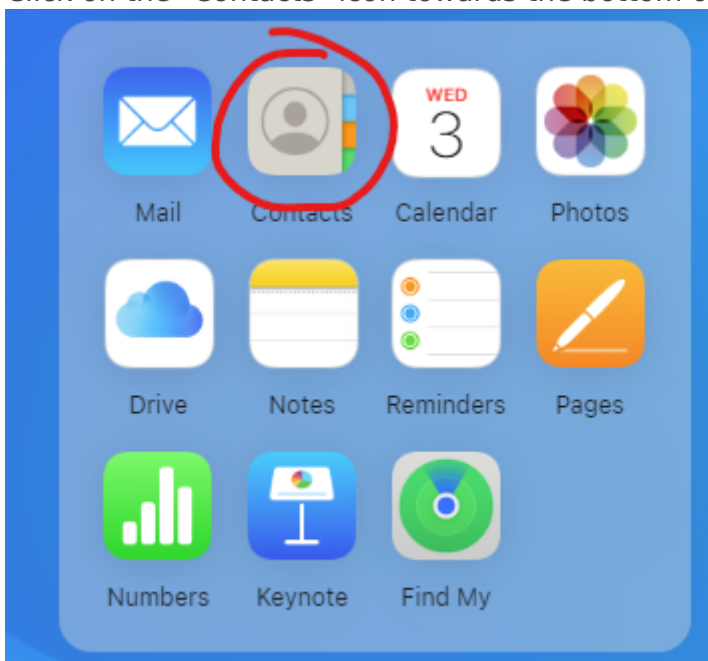
# Bulk Contact migration on iPhones

## Problem:

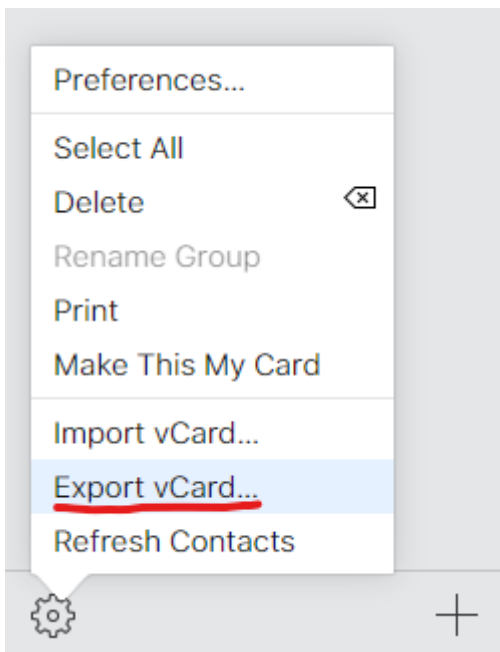
Apple iPhone's do not have a built in bulk contact export function programmed into them. Rather they expect that you can share 1 contact at a time, or that you would log into another iPhone with your iCloud account if you needed all of your contacts. However, there is a way to get a single vCard file that contains any or all of your contacts. Please follow the instructions below for this process. As always, please reach out if further assistance is needed, thank you!

## Resolution:

1. Ensure that your current (old) iPhone has its contacts synced to your iCloud account  
You can check this by going to Settings > click on your name at the top > iCloud > Show All and then make sure "Contacts" is switched on
2. Go to <https://icloud.com> and login to your iCloud account
3. Click on the "Contacts" icon towards the bottom of the page



4. Select all of the contacts that you would like to move over to the new phone. You can do this by holding "Ctrl" and selecting multiple contacts, or by holding Shift and selecting the last contact to highlight ALL contacts.
5. On the bottom left of the screen, click on the gear icon and then select "Export vCard..."



6. The file that downloads can then be emailed to the new phone (or anyone else) and opened. At that point, the iPhone will ask if you'd like to import all of the contacts in the file.

This will allow you to move any number of contacts from one iPhone to another without a shared iCloud account. Have a wonderful day!