

Configuring MFA with Cloudwork





A little about me...

Consultant and Trusted Advisor

K-12 Technology Director

Risk and Compliance Executive

Reformed developer, sysadmin and
DBA

WHY
ARE WE
HERE?



Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Report

July to December 2021



Phishing remains the most common cause of cyber-related Notifiable Data Breaches



Australian Government
Office of the Australian Information Commissioner

Notifiable Data Breaches Report

July to December 2021




Phishing remains the most common cause of cyber-related Notifiable Data Breaches



Australian Government
Office of the Australian Information Commissioner

Notifiable Data Breaches Report

July to December 2021



Stolen credentials, obtained through unknown methods, many also likely through phishing, are the second most common cause of data breaches.

John Smith - Head of English

Urgent help please!

To: Sally Warren

Hi Sally,

Could you please help me? I've locked myself out of my computer and need urgent access to a file....

Can you click this link to send me the file I need?

<https://microsoft.office365helper.io/login?file=123AF-4341AS-54112-5213A>

Thanks!

John Smith
Head of English
Cloudwork School

John Smith - Head of English

Urgent help please!

To: Sally Warren

Hi Sally,

Could you please help me? I've locked myself out of my computer and need urgent access to a file....

Can you click this link to send me the file I need?

<https://microsoft.office365helper.io/login?file=123AF-4341AS-54112-5213A>

David Ralph

RESPONSE

To: Steven Jones

Hi Steven

Let me know if you are available. There is something I need you to do and also your confidentiality would be appreciated. Email me once you get this and let me have your personal email address to proceed.

David Ralph
Head of Junior School
Sent from mobile device

This email and any files transmitted with it are confidential and intended solely for the use of the individual entity to whom they are addressed. If you have received this email in error please inform the sender and delete it from your mailbox or any other storage mechanism. The school does not accept responsibility for loss or damage that may result from reliance on, or use of any information contained in this email or any attachment, unless it was clear that it was an official communication of the school and was intended to be relied upon by the recipient.



>99.9%

Less likely an account will be compromised by an automated attack with MFA enabled

Brute-force attack
(compromised credentials) 5%

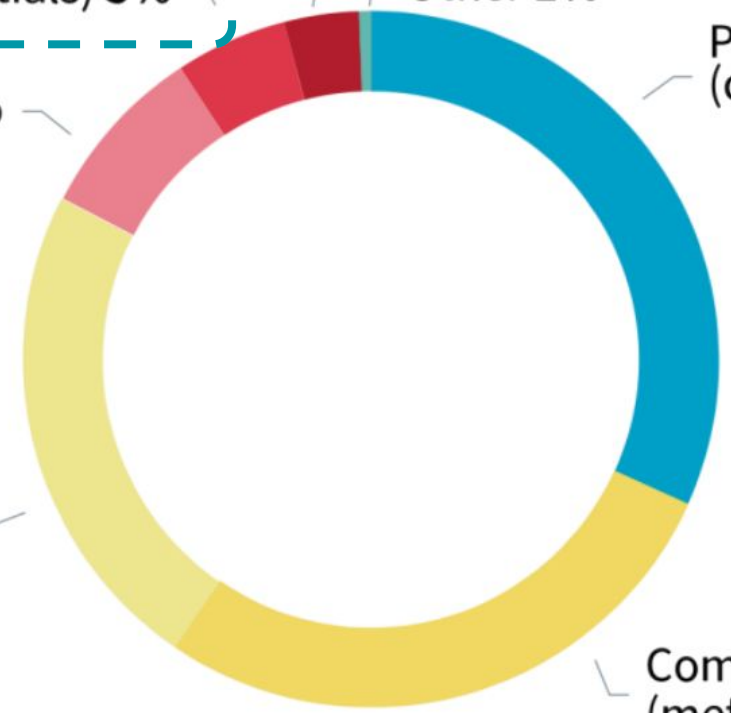
Malware 3%
Other 1%

Phishing
(compromised credentials) 32%

Hacking 8%

Ransomware 23%

Compromised or stolen credentials
(method unknown) 28%



MFA Configuration Options with Cloudwork

- Can be configured per user or per Org Unit
- Can use SMS tokens or an authenticator app (e.g. Google Authenticator)
- Can allow users to manage their own MFA settings
- Can allow users to trust devices
- Locations can be whitelisted so that MFA is not required from e.g. on campus



Per-user MFA configuration

Tom Teacher tteacher

[Change Password](#)
[Silent Inspection](#)
[Send Welcome Message](#)
[Delete User](#)

Account Details

Username	tteacher
Name	Tom Teacher
Primary Email	tteacher@school.nsw.edu.au
Other Email Addresses	
SIS ID	
Role	Teacher
Org Unit	/Domain Users/Staff
Account Status	Active
Password	Expires on 2022-02-22 16:33:18

Custom Attributes

There are no custom attributes for this user.

Recovery Details Edit

Email	tteacher@school.nsw.edu.au
Mobile	0412345678

Groups See All

[All Staff and Students](#) all@school.nsw.edu.au

Admin Roles

Teacher on /Domain Users/Students

Security

MFA Status	Enabled	<input type="button" value="Enable SMS"/> <input type="button" value="Disable Multifactor"/>
Authenticator App	Added on January 13, 2022, last used January 13, 2022	
Sign On Cookies	<input type="button" value="Clear Sign On Cookies"/>	

Sync Status

Sync Profile	Staff
Adobe Coherent Cloud	There are changes waiting to sync to G Suite

Per-Org Unit MFA configuration

- Users
- Organisational Unit
- Groups
- Sync Profile
- Reports
- Single Sign On
- External Domains
- Admin Roles
- Message Template
- Google Classroom
- Canvas Sync
- Adobe Creative Cloud
- Settings
- Login Theme
- Authentication Settings
- Cloudwork ID Settings

Cloudwork.ID Settings for /Domain Users/Staff

- Domain Users
 - Staff
 - Students

Look and Feel	Inherited from Defaults	Override Settings
Title	Cloudwork ID	
Banner Logo		
Show Banner Logo	Yes	
Favicon		
Homepage Logo		
Background Color	#fff	
Title Color		
Banner Link Colors	Dark text on lighter background	
Custom Styles		

Features	Inherited from Defaults	Override Settings
Show CloudworkID Homepage	Redirect to Account Settings	
Allow users to change own password	Users can change their password	
Users can change recovery information	Users can change their recovery information	
Users must have Multifactor enabled		
Users can change Multifactor settings	Users can manage multifactor authentication	
Users can turn off Multifactor Authentication	Users can disable multifactor authentication	

Cloudwork.ID Settings for /Domain Users/Staff

- ▾ Domain Users
- ▾ Staff
- Students

Cloudwork.ID

Homepage

Passwords

Let users see when they last set their password, and let them change it

Recovery Information

Let users see and update their recovery settings

Multifactor Authentication

Let users see and manager their Multifactor Authentication options

Disable Multifactor

Let users disable Multifactor Authentication once they've enabled it

Users must enable MFA

When this setting is enabled, single auth users can only log in to CloudworkID. All other services will ask the user to enable MFA

Enable Trusted Devices

Disabling this option removes the option for a user to indicate a trusted device for MFA

Multifactor Authentication Whitelist

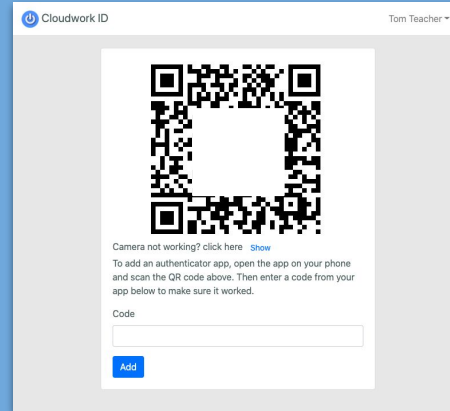
Comma seperated list of IP addresses, for example: '203.0.113.15, 192.0.2.0/24'. Users logging in from one of these locations will not be prompted for a second factor if users have enabled MFA. Leave this field blank to always prompt for Multifactor Authentication if enabled.

Cloudwork School

Multifactor Authentication is Required

To access this service, you must have Multifactor Authentication enabled.

[Click here to enable Multifactor Authentication](#)



Password

Your password was last changed on January 11, 2022 

Recovery Settings

Email: tteacherrecovery@gmail.com Verified

Phone: 0410245678 Verified

[Update Recovery Settings](#)

Multifactor Authentication

You have not enabled Multifactor Authentication

[Add Authenticator App](#) [Add a phone](#)

Cloudwork School

2-Step Verification

A text message with a verification code was sent to **** *
480

692427

I trust this device, don't ask again

Sign in

[Choose another option](#)

Cloudwork® Copyright © 2021 [Studentnet®](#) | Powered by [Coherent Cloud®](#)

MFA Technology Choices



SMS tokens

- Less secure - SIM swapping, SMS mirroring
- Convenience - pushed codes
- Familiarity



Time-based One-Time Passcode (Authenticator apps)

- More secure
- More reliable

Monitoring Compliance - Security Report

[Home](#) / [Reports](#)

Security Report

- Summary
- User Activity
- Security**
- Administrator Activity
- Provisioning
- Manage Alerts

For Org Unit:

For Role:

For Account Status:

Username	Primary Email	MFA Status	App Enabled	SMS Enabled	MFA Enforced	Is Admin	Status
ngmares_cwkadmin	[REDACTED]	No	Not Enabled	Not Enabled	No	Yes	active
sallys22	[REDACTED]	Yes	Feb 4 12:12	Feb 4 12:11	No	No	active
studentnetsupport	[REDACTED]	No	Not Enabled	Not Enabled	No	Yes	administrator
toms22	[REDACTED]	No	Not Enabled	Not Enabled	No	No	active
teacher	[REDACTED]	Yes	Not Enabled	Apr 4 20:50	Yes	Yes	active

[Load More](#)



Monitoring Compliance - Activity Reports and Alerting

Home / Reports

User Activity Report

Summary

- User Activity
- Security
- Administrator Activity
- Provisioning
- Manage Alerts

From: Oct 05 2021 07:54

To: Apr 05 2022 07:54

For User:

For SSO Service:

For Event:

- 2FA Disabled x
- 2FA Verification x
- Add App Second Factor x
- Add Mobile Second Factor x
- Enable 2FA x
- Remove App Second Factor x
- Remove Mobile Second Factor x

Update Download Create Alert

Event	IP Address	Date
tteacher (Tom Teacher) used second factor ██████████ to log in	██████████	Apr 4 20:50
tteacher (Tom Teacher) added ██████████ for Multifactor Authentication	██████████	Apr 4 20:50
tteacher (Tom Teacher) enabled Multifactor Authentication	██████████	Apr 4 20:50
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Feb 8 11:40
tteacher (Tom Teacher) used second factor Authenticator App to log in	██████████	Jan 13 14:15
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Jan 13 14:15
tteacher (Tom Teacher) used second factor Authenticator App to log in	██████████	Jan 13 09:18
tteacher (Tom Teacher) added Authenticator App for Multifactor Authentication	██████████	Jan 13 09:17
tteacher (Tom Teacher) enabled Multifactor Authentication	██████████	Jan 13 09:17
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Jan 13 08:17
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Jan 13 08:02
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Jan 13 08:01
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Jan 12 14:24
sallys22 (Sal Student) used second factor Authenticator App to log in	██████████	Jan 12 14:16
sallys22 (Sal Student) added Authenticator App for Multifactor Authentication	██████████	Jan 12 14:14
sallys22 (Sal Student) enabled Multifactor Authentication	██████████	Jan 12 14:14

[Load More](#)

Monitoring Compliance - Activity Reports and Alerting

For Event:

- 2FA Disabled x
- Remove App Second Factor x
- Remove Mobile Second Factor x

[Update](#) [Download](#)

[Create Alert](#)

ORK ? 12 ⋮

[Home](#) / [Reports](#) / [Alerts](#)

Manage Alerts

- Summary
- User Activity
- Administrator Activity
- Provisioning
- Manage Alerts

Description			
Weekly Cloudwork usage report	Disable	Delivery Settings	
User logged into Moodle	Enable	Delivery Settings	View Report
Silent inspection alert	Disable	Delivery Settings	View Report
Multifactor disabled	Disable	Delivery Settings	View Report

Preparing for deployment

Which users?

Timelines?

Communications plan

End user education - Why and how?

Who will launch it?

Which technology will you use? SMS or TOTP or a mix?

How will you monitor compliance? Reporting and alerts

What training will your team need?



Where to begin?



Cloudwork Best Practice
Security White Paper
February 2022

1. Get leadership on board
2. Implement for your team
3. Refine frequency of MFA prompts
4. Train your team
5. Launch with your wider staff group
6. Support and monitor compliance

Questions?

