Configuring MFA with Cloudwork

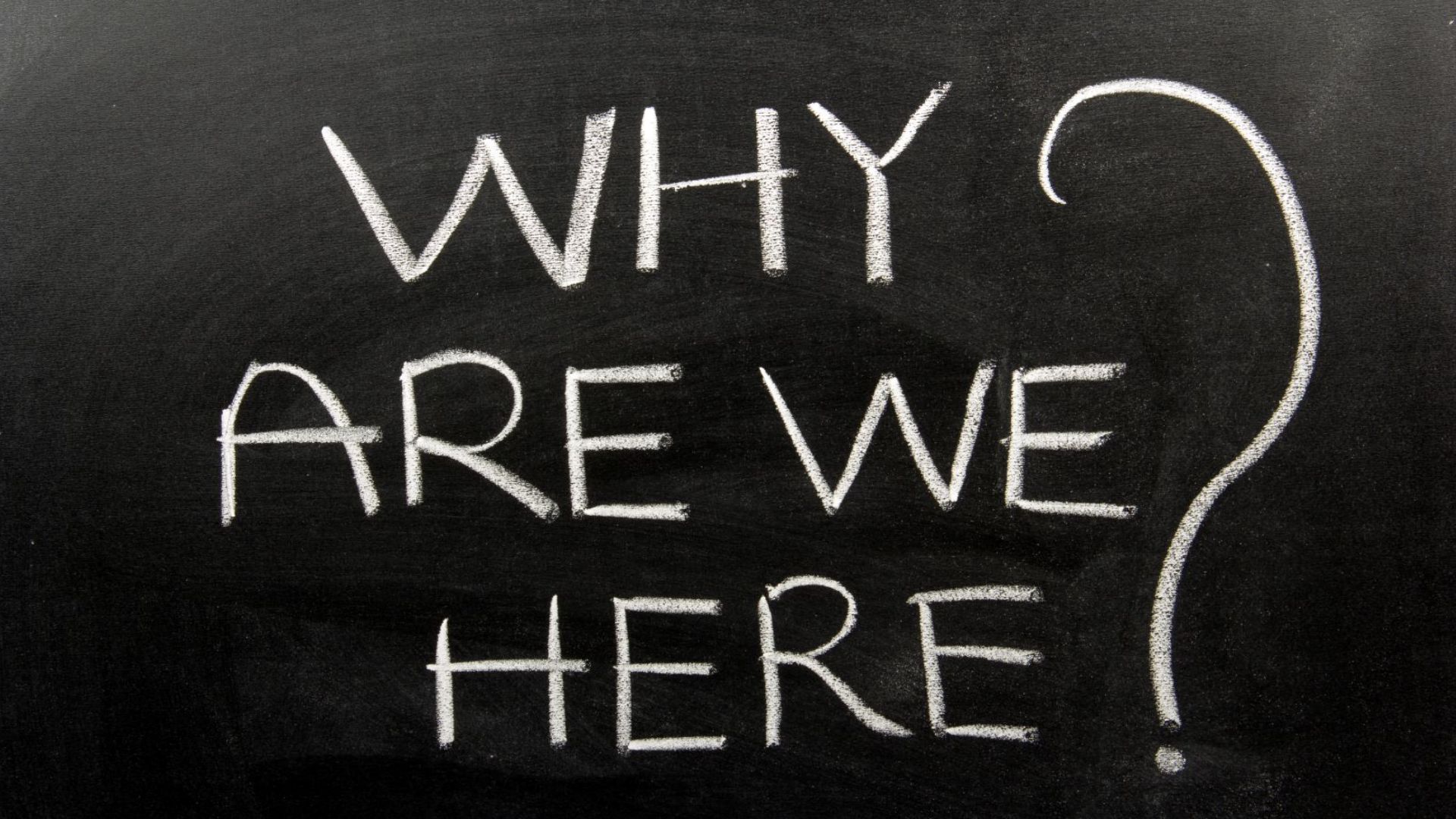
A little about me…

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

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 nd 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 nd 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

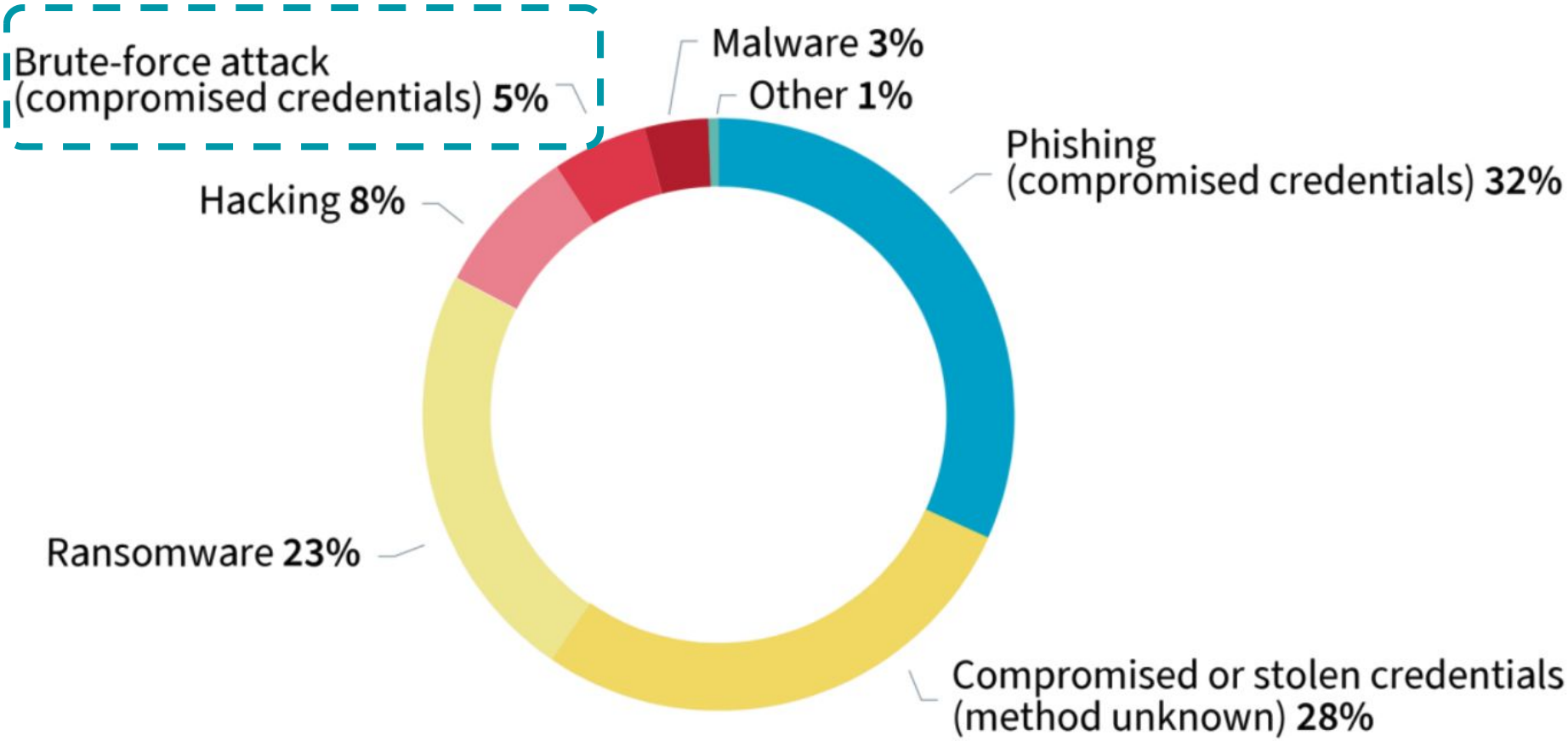
Hi Steven

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

>99.9%

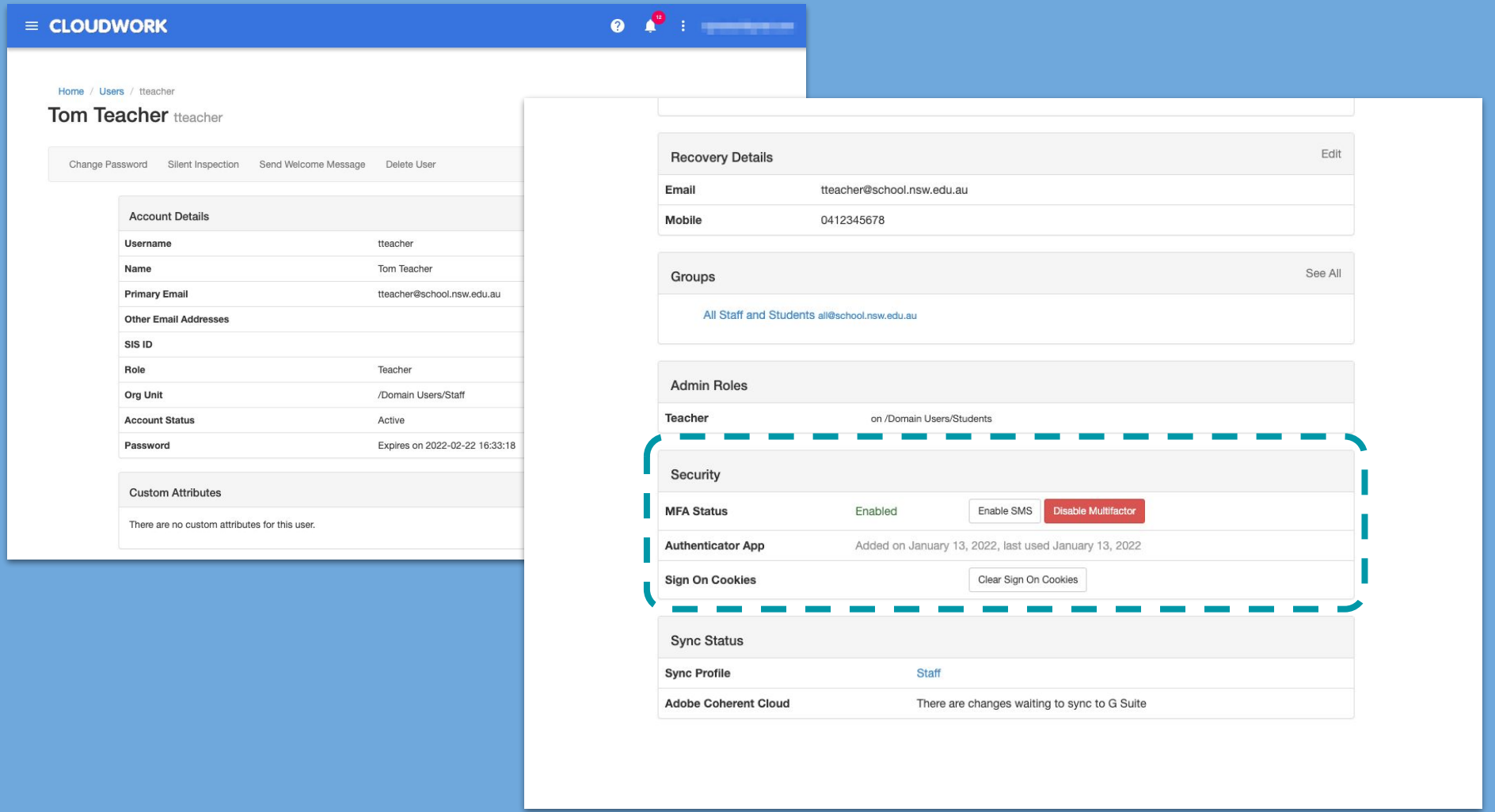
Less likely an account will be compromised by an automated attack with MFA enabled


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%

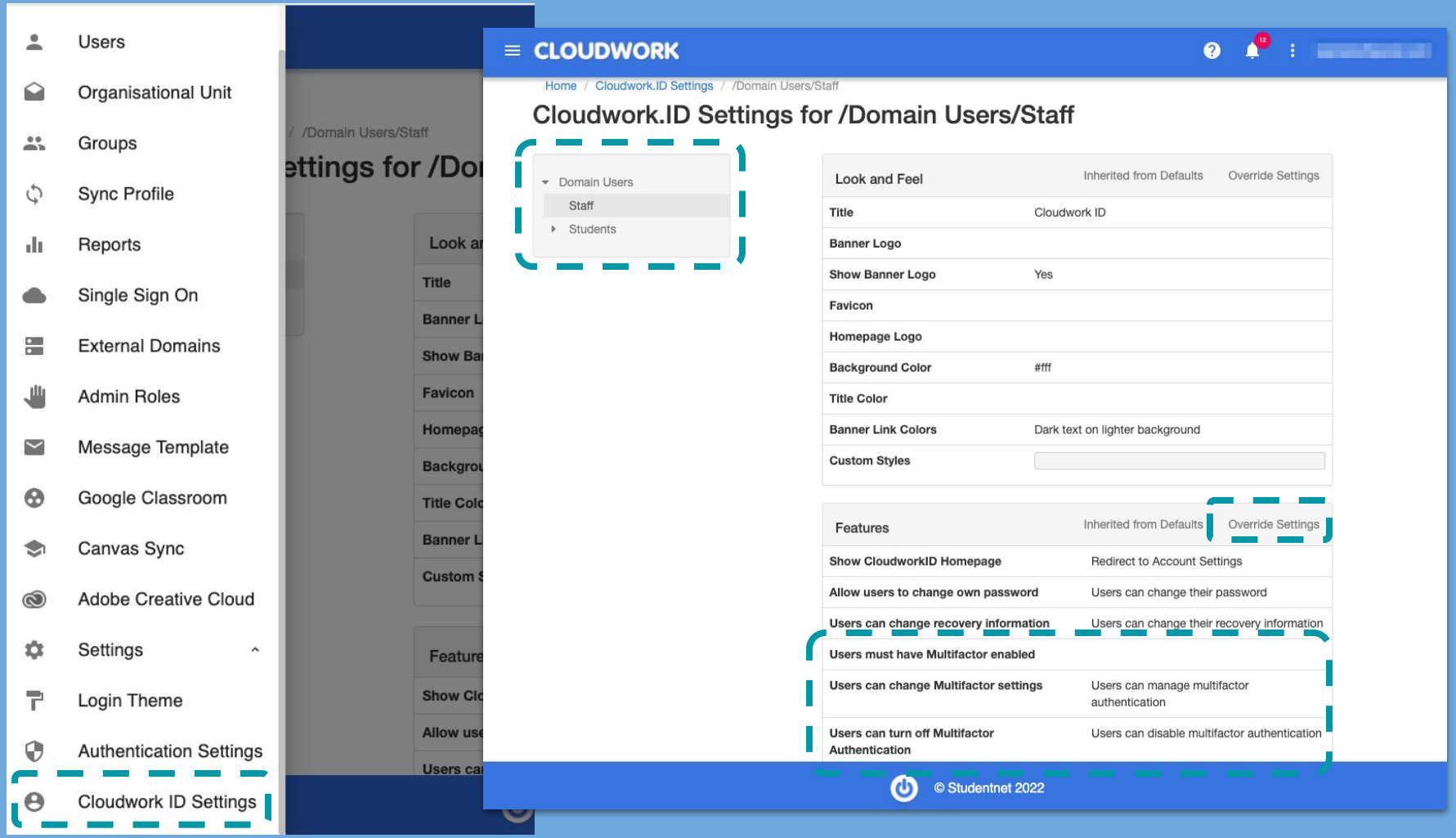
MFA Configuration Options with Cloudwork

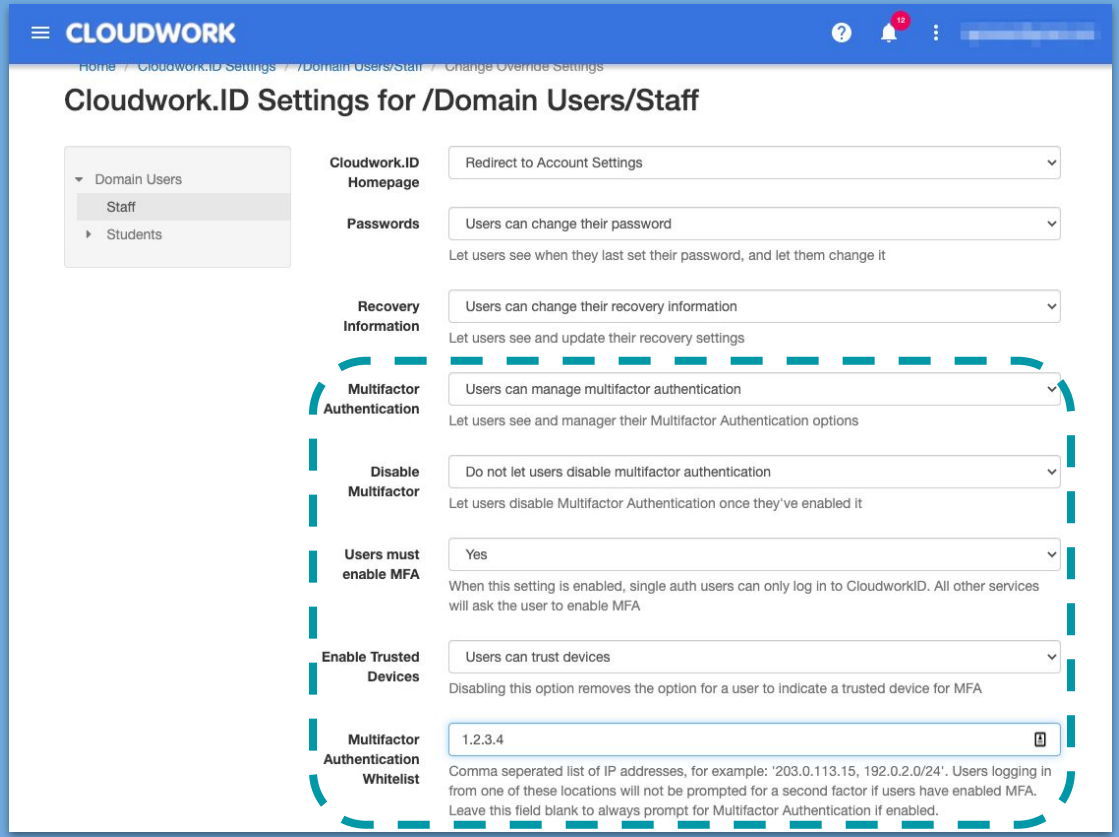
- Can be configured per user or per Org Unit
- Can use SMS tokens or an authenticator app (e.g. Google Authenticator)
- Can allow users to manage their own MFA settings
- Can allow users to trust devices
- Locations can be whitelisted so that MFA is not required from e.g. on campus

Per-user MFA configuration


CLOUDWORK
Home / Users / tteacher
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
Enable SMS
Disable Multifactor
Authenticator App Added on January 13, 2022, last used January 13, 2022
Sign On Cookies
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
Home / Cloudwork.ID Settings / /Domain Users/Staff
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
© Studentnet 2022

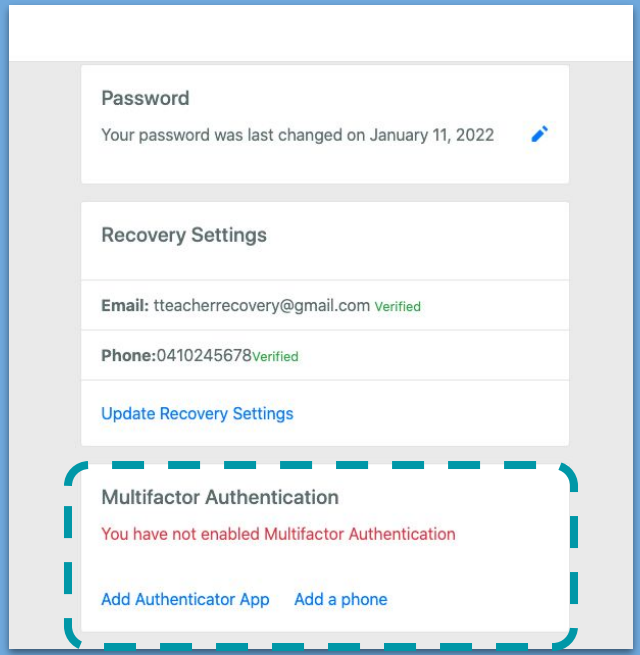

CLOUDWORK
Home / Cloudwork.ID Settings / /Domain Users/Staff / Change Override Settings
Cloudwork.ID Settings for /Domain Users/Staff
Domain Users
Staff
Students
Cloudwork.ID Homepage
Redirect to Account Settings
Passwords
Users can change their password
Let users see when they last set their password, and let them change it
Recovery Information
Users can change their recovery information
Let users see and update their recovery settings
Multifactor Authentication
Users can manage multifactor authentication
Let users see and manager their Multifactor Authentication options
Disable Multifactor
Do not let users disable multifactor authentication
Let users disable Multifactor Authentication once they've enabled it
Users must enable MFA
Yes
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
Users can trust devices
Disabling this option removes the option for a user to indicate a trusted device for MFA
Multifactor Authentication Whitelist
1.2.3.4
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



Cloudwork School

2-Step Verification

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

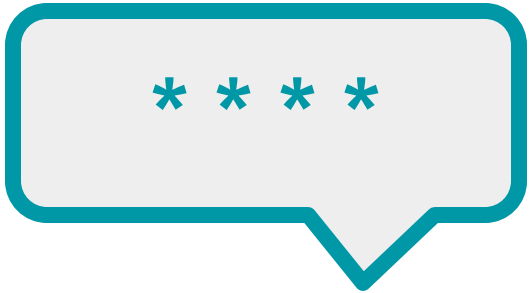
692427

I trust this device, don't ask again

Sign in

Choose another option

MFA Technology Choices



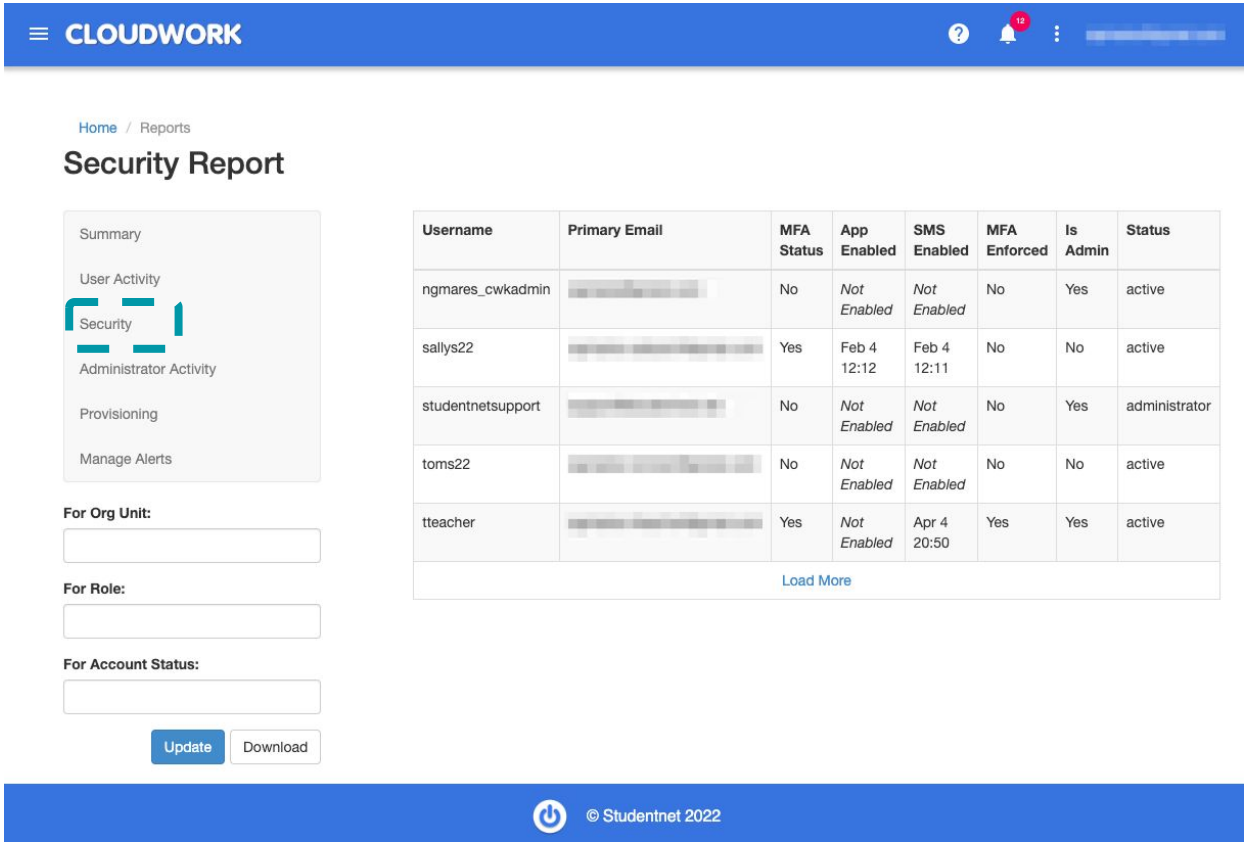
SMS tokens

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

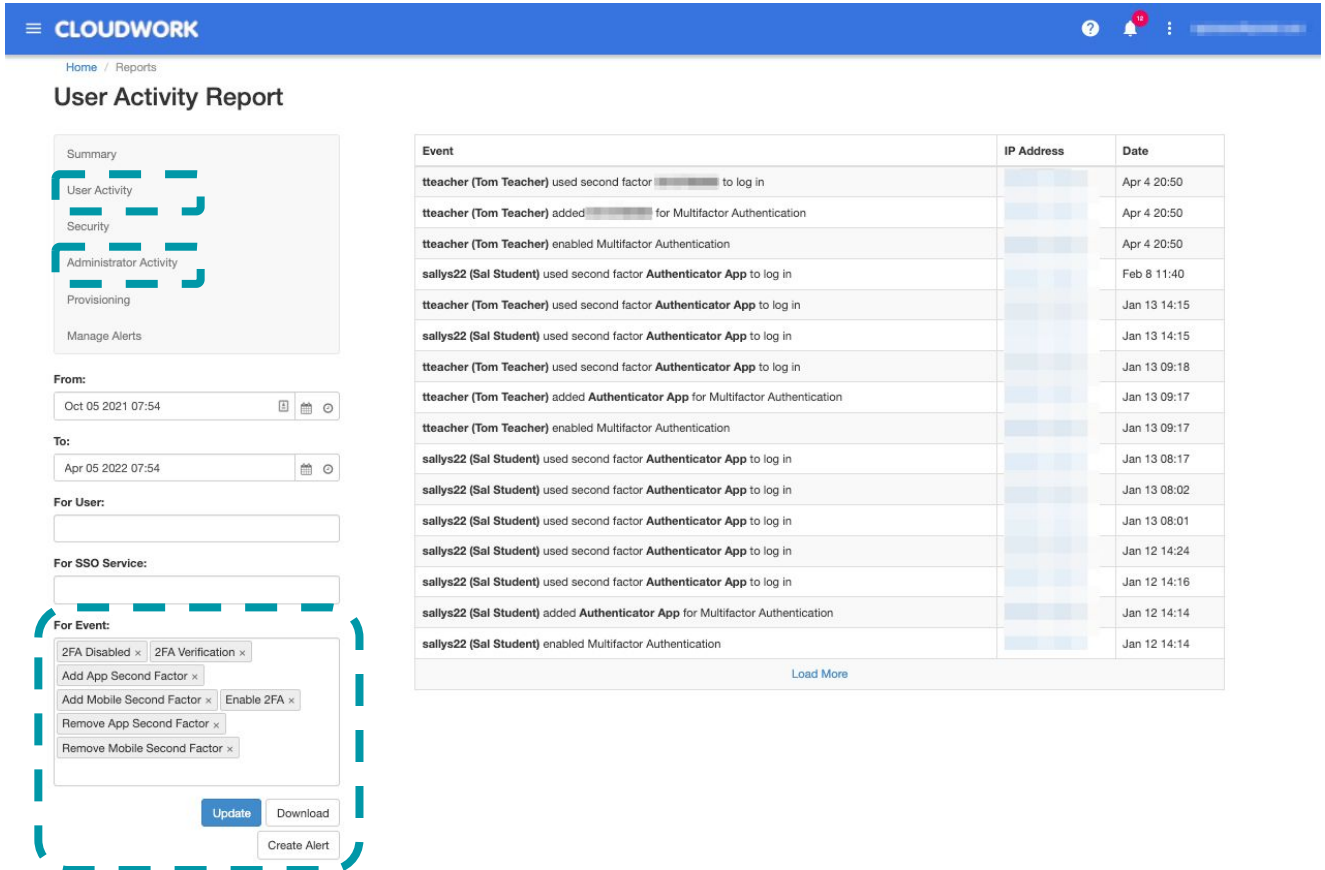
Time-based One-Time Passcode (Authenticator apps)

- More secure
- More reliable

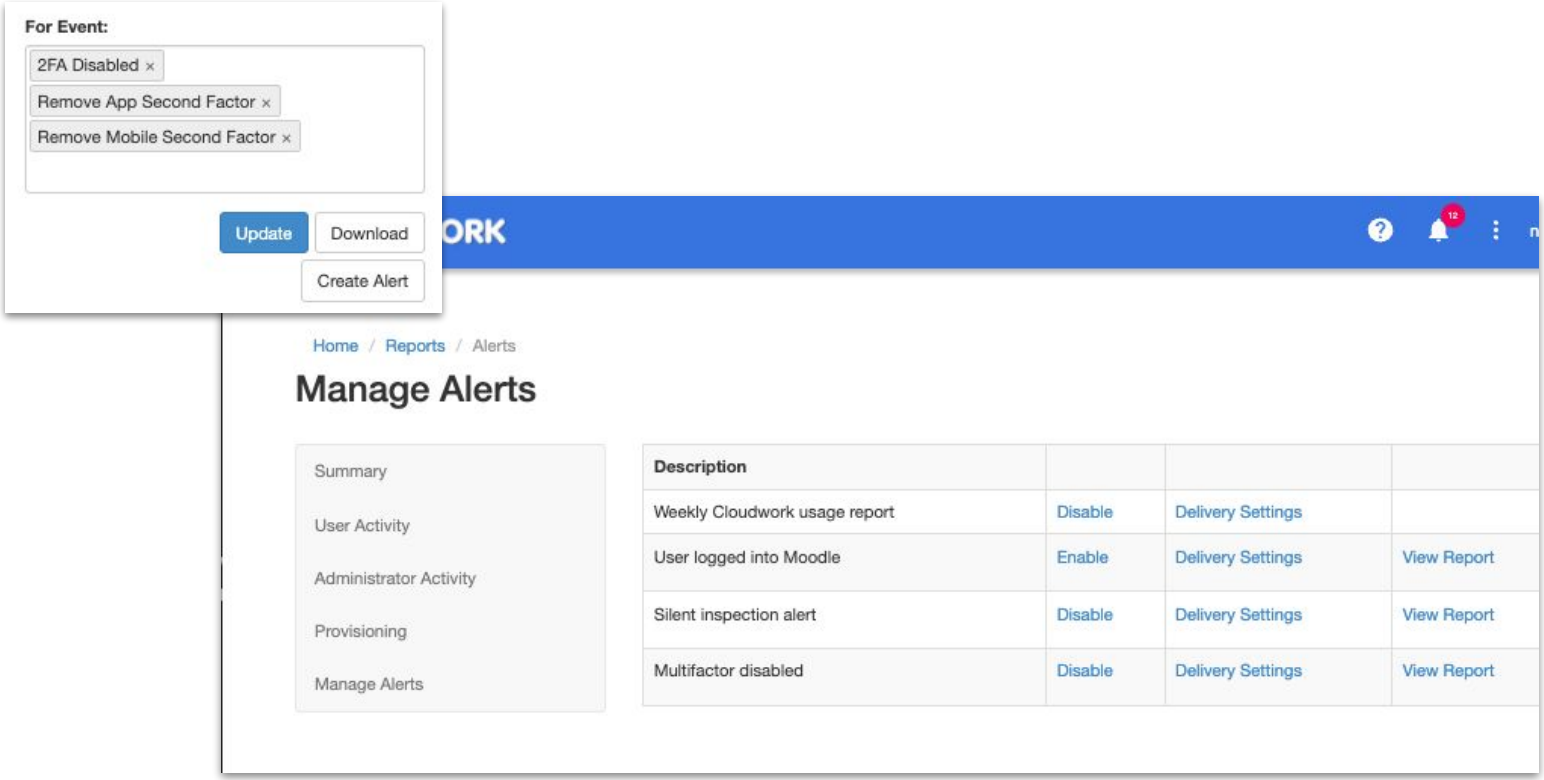
Monitoring Compliance - Security Report



Monitoring Compliance - Activity Reports and Alerting



Monitoring Compliance - Activity Reports and Alerting



Preparing for deployment

Which users?

Timelines?

Communications plan

End user education - Why and how?

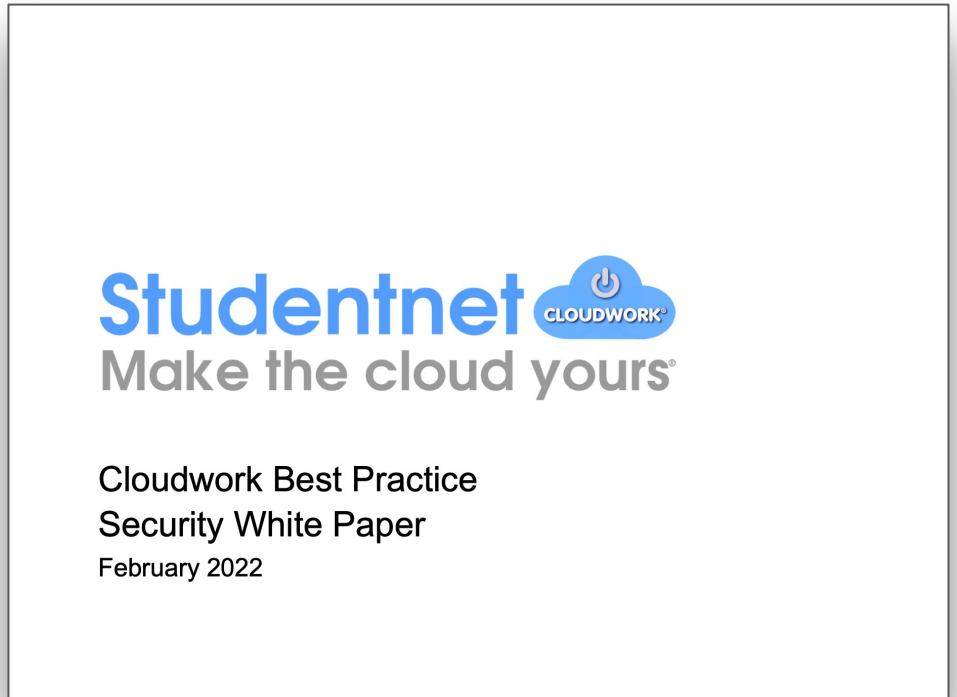
Who will launch it?

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?



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?