



**Cloudwork® Best Practice
Security White Paper
February 2022**

**Nathan Mares
EdTech Consultant, Sydney**

Contents

About This Guide	1
Security Controls	1
1 Timely Revocation of Identities and Credentials	2
1.1 Configuration.....	2
1.2 Additional information.....	2
1.3 Supporting policies and procedures.....	2
2 Exception Alerting and Log Review	4
2.1 Configuration.....	4
2.2 Additional information.....	4
2.3 Supporting policy and procedures.....	5
3 Delegation of Least Privilege Access to Admin Users	6
3.1 Configuration.....	6
3.2 Additional information.....	6
4 Least Privilege Delegation for Sync Profile Accounts	7
4.1 Configuration.....	7
5 Rules to Restrict Access to Sensitive Systems	8
5.1 Configuration.....	8
5.2 Supporting policies and procedures.....	9
6 Multi-Factor Authentication	10
6.1 Configuration.....	10
6.2 Additional information.....	11
6.3 Supporting policies and procedures.....	12
7 Geoblocking	13
7.1 Configuration.....	13
7.2 Additional information.....	13
8 Customised Themes and User Awareness Training	14
8.1 Configuration.....	14
8.2 Supporting policies and procedures.....	14
9 Compromised Passwords, Minimum Password Length	15
9.1 Configuration.....	15
9.2 Additional information.....	15
9.3 Supporting policies and procedures.....	15
10 Key Additional Controls	16
Appendix A: Configuration Summaries	17
Contact Us	19

About This Guide

Schools are different to other organisations when it comes to technology use and cybersecurity. School IT teams support a significant number of users – Kindergarten to Year 12 students, staff and parents – sometimes numbering in the thousands, and with vastly different levels of technology competency and capacity.

The diversity of personal information, from basic contact information to sensitive healthcare and financial data is also different to many other organisations. Schools have a vested interest in maintaining a high degree of trust with their community. An effective cyber risk management program is essential, especially at a time when schools are increasingly finding themselves the target of cyber criminals.

This guide has been prepared for schools, particularly Cloudwork customers, with the aim of assisting them in improving their security posture. As the chosen provider of identity management and single sign on services for many leading schools, we are in a position to provide unique insights into what works when it comes to identity and security in the K-12 educational context.

This document has also been prepared by an experienced edtech leader, with wide experience in risk management and compliance. Security and usability are often seen as opposed, but our experience allows us to recommend a pragmatic approach which balances the impact on usability, and consequently student learning and organisational efficiency, which will work for the vast majority of schools.

The guide also builds on and references privacy and other legal obligations which typically apply to schools, as well as recognised cyber security frameworks, in particular the NIST Cybersecurity framework.¹ The NIST framework assists organisations in understanding and performing the various functions necessary to effectively manage cyber risk. These functions are: *Identify, Protect, Detect, Respond and Recover*.

While the scope of the NIST Framework extends beyond identity and single sign-on, the focus of the Cloudwork product, many aspects of the framework are helpful in illuminating the importance of the controls we recommend in this document.

Security Controls

The following sections detail recommended security controls for schools to implement in their Cloudwork environment. These controls include recommended configuration, as well as any supporting policies and procedures you should have in place in your organisation to support these controls.

Information security is not a task which is ever complete. Rather, it is a process requiring ongoing review and continuous improvement. Well thought-out policies and procedures, appropriately adapted to your environment, make it more likely the systems and structures to support excellent cyber security practises will be maintained over the long term.

No school is the same as another and Cloudwork does not take a one-size-fits-all approach to security. Additional information and considerations are also provided for some controls, which may be helpful as you plan to implement or adapt each recommendation to your school's unique context.

¹ <https://www.nist.gov/cyberframework>

1 Timely Revocation of Identities and Credentials

Ensuring the timely creation of accounts for new students, parents, staff and contractors is essential to delivering quality, efficient technology programs in schools. By enabling the automatic provisioning of user accounts for the many different groups of users in a typical school, this feature is one which has become highly valued by school technology teams.

While the majority of students, staff and parents commence and depart at defined times of year, many users come and go on an ad-hoc basis. Cloudwork provisioning features ensure consistent, timely access is provided with minimal effort and intervention.

Many schools now have effective processes and systems in place for provisioning accounts, but the same is not always true for *deprovisioning* accounts. Fortunately, Cloudwork functionality easily automates the revocation of access to staff, students and others as need arises. Obtaining agreement on a *consistent process for disabling accounts* and then configuring this in Cloudwork is a must-do task for Cloudwork customers.

1.1 Configuration

1. From the Dashboard, select Sync Profile.
2. Select each of your LDAP user sync profiles in turn.
3. Click Edit and review the value for “Action for deleted users”. Available options are:

Option	Description
Delete users	Delete the user from the Cloudwork Dashboard when the user is deleted from your LDAP directory.
Suspend users	Prevent the user from logging in to Cloudwork and linked services if they have been deleted from your LDAP directory.
Mark user as alumni	Change the user’s role to Alum but otherwise allow them to continue logging in.
Suspend user and mark as alumni	Prevent the user from logging into Cloudwork and linked services, and change the user’s role to Alum
Do nothing	<i>Not recommended</i>

4. Ensure a value *other than* “Do nothing” is selected.
5. If changes are made, click “Submit”.
6. Repeat for each LDAP user sync profile.

1.2 Additional information

1. When first configuring how Cloudwork should handle users deleted from your LDAP directory, you should implement *suspend users* rather than deleting them.
2. Where you have marked deleted student users as alumni but not suspend them, review authorisation rules to ensure that alumni cannot access internal systems which they should not be able to access. For example, your policy may be to provide former students with an ongoing email account, but that is the only service they should be able to access.

1.3 Supporting policies and procedures

- Data sourced from school management systems frequently governs when and who is provided an account, and when that access is revoked. Cloudwork staff will have worked with you during the initial setup of your school’s Cloudwork dashboard to determine the parameters and methods for extraction of this data from your school management system.

- The data in these systems is generally entered and maintained by staff who are not members of the IT team, e.g. enrolments officers and human resources staff. Difficulty is sometimes encountered when staff are unclear about their responsibilities or the procedures to enter data accurately into these systems.
- Technology teams should ensure staff are provided with clear, succinct procedures on the steps they must take to ensure accounts are provisioned and deprovisioned at the appropriate times, and regular training to limit the circumstances in which new users are not provided with timely access.
- Most school management systems include an “end date” field for student enrolment and staff employment. Some may also include a boolean “current” field. Preference should be given to using an “end date” field, rather than a “current” field when integrating your data source with Cloudwork, as this allows the *automated deprovisioning* of accounts without HR staff needing to take action.
- Seek input and agreement from senior management and human resources on when staff accounts should be deprovisioned. Frequently this will be employees’ last day of employment, although sometimes this will be a fixed period after the end date.
- Senior management will sometimes have good reasons for extending access for particular employees beyond the standard cutoff date. Where possible, procedures should be agreed with HR for these exceptions in advance, to ensure that such situations can be accommodated within the constraints of your user provisioning configuration. These procedures should include checks and/or reminders to ensure employees are terminated at the appropriate time in the source system.
- While most schools typically have well defined processes for regular staff, students and parent accounts, the same cannot always be said for casual staff, co-curricular coaches and contractors. Occasionally school IT staff are also called to hastily adapt systems for managing user access in order to respond to complex family relationships. *It is impossible to predict all complications that may arise, but it is important to spend some time preparing for the most likely complications that may arise in your school.*

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

2 Exception Alerting and Log Review

Exception alerting refers to the systems and processes for identifying the occurrence of events within a system which may indicate unusual or higher risk activity, such as an account compromise, and escalating information about such events to a decision-maker for review. The decision-maker will then assess whether or not an incident requires further investigation to determine whether a security incident has occurred.

Cloudwork includes features to enable exception alerting for certain high-risk events, with features for emailing administrators on the occurrence of predefined events.

While exception alerting does address one of the challenges of dealing with the sometimes overwhelming volume of data collected in system logs, procedures should also be established for regularly reviewing administrative and account activity logs on a recurring basis, e.g. weekly.

2.1 Configuration

1. From the Dashboard, select Reporting.
2. Click User Activity or Administrator Activity
3. Filter the relevant event log by one or more of the following events:

	User Activity	Administrator Activity
Recommended Minimum	Lockout Activated	Assign Admin Role Assign Admin Role to Group Silent Inspection Change Password Delete Alert Disable Alert
Optional	2FA Disabled Authentication Failed Authorize Failure Invalid Reset code Password Change Password Reset Started Password Reset Complete Update Password Recovery Details Username Recovery	Clear Lockout Delete Authorization Rules Disable Multifactor Edit Alert Edit Authentication Settings Edit CloudworkID Settings Remove Admin Role Remove Admin Role from Group Update User

4. Click Create Alert.
5. Enter an appropriate Description.
6. Either tick “Send alert to all super administrators” or one or more email addresses in the “Other recipients” field.
7. Click Submit.

2.2 Additional information

1. Depending on your environment and usage, Cloudwork may generate a large number of events corresponding to the event types above. The goal of exception alerting should always be to identify the highest risk events that are more likely to indicate a security incident has occurred. This means you may decide not to alert for event types you consider lower risk from the above list.
2. For some event types, you may wish to target alerts to particular users (for example, all members of the IT team who have higher levels of access, or contractor accounts) or to

particular services (e.g. the student management system, which contains sensitive data). Such decisions would usually be informed by a risk assessment.

2.3 Supporting policy and procedures

- Ensure responsibility for reviewing alerts is assigned to someone in your team. Responsibility for reviewing security incidents and conducting investigations should ideally be formally documented, at a high level and not just with respect to Cloudwork alerts, in one or more team member’s role description.
- Implement a checklist and/or basic pro-forma risk assessment for determining whether incidents should be investigated further, and how investigations should be conducted. For example, if an alert related to a highly privileged account, such as a staff member’s account, this would support a decision on whether to investigate.
- Ensure measures are in place for alerts to be reviewed and investigated when the team member ordinarily responsible for reviewing and investigating security incidents is unavailable, for example, on leave.
- While exception alerting allows teams to focus on higher risk events, regular log reviews should still form part of your security procedures. This practice ensures team members have a good understanding of what events are captured by the system, and enables them to build a picture of business-as-usual for when something does go wrong.

Security Framework

NIST Category	NIST Subcategory
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
	DE.AE-2: Detected events are analyzed to understand attack targets and methods
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors
	DE.AE-4: Impact of events is determined
	DE.AE-5: Incident alert thresholds are established
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability

3 Delegation of Least Privilege Access to Admin Users

The principle of *least privilege* means providing users and systems with only the level of access they need to perform their duties. In the context of the Cloudwork dashboard, this means giving admin users only the level of access they need to carry out their duties.

As a minimum you will have at least a few IT team members set up as admin users in the Dashboard. You may also have other staff within the school, for example year advisors, library assistants or class teachers, who have been given admin user access to reset passwords for select groups, e.g. students within their class.

3.1 Configuration

From the Dashboard, select Admin Roles. This will list all existing built-in and custom admin roles. Select one of the roles to view the users, groups and permissions attached to it.

3.1.1 Creating and modifying roles

Click “Add New Role” at the top of the Admin Roles page. Enter a name and select the required permissions for the role, and click Submit to create it. Permissions for existing roles (except some built-in roles) can be modified by selecting the role from the Admin Roles screen and clicking the “Edit Permissions” link.

Limit permissions to only those that are necessary. Only a small number of users would ordinarily be assigned to roles with permissions outside the “User permissions” category.

3.1.2 Assigning roles to users and groups

Roles can be assigned to users and groups (except the built-in Cloudwork Staff role). The assignment can be scoped to All Org Units or a single Org Unit (a subset of users in your Dashboard and probably corresponding to an Organizational Unit in your LDAP directory).

3.2 Additional information

- Assigning roles to *groups* is considered best practice, as it reduces the steps required (and room for error) to reassign access when IT and other admin users move on. e.g., instead of directly assigning a library assistant or year advisor to the Students “Org Unit” to allow them to reset passwords for students, create a “Student Password Reset” group, add those staff to this group, and assign the group to the Students Org Unit for the relevant role.
- When scoping role assignments, consistent with the principle of least privilege, preference should be given to assigning roles to a *subset* of Org Units rather than All Org Units. For example, if there was a desire for library staff to be able to reset passwords for students, the role assignment should be limited to the relevant Student Org Units only, to prevent those staff resetting passwords for other staff or parents.

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

4 Least Privilege Delegation for Sync Profile Accounts

Sync Profiles manage the flow of information about users and groups to and from the Cloudwork Dashboard. Your Dashboard will likely have one or more LDAP User Sync Profiles, LDAP Group Sync Profiles or Active Directory Provisioning Profiles configured. You may also have another sync profile type configured for extracting data from your school’s student management system.

Each sync profile includes credentials for connecting to the relevant directory or data source. The credentials correspond to an account in the relevant source system with privileges necessary to read and manipulate data in that system. Frequently, school staff allocate an account for Cloudwork that has full access to all data in the system.

An example of this is a user account that is a member of the Domain Administrators group in Microsoft Active Directory. In keeping with the principle of least privilege, the service account used by a sync profile should instead have delegated access to only the organisational units in Active Directory which are being synced to or from the Cloudwork Dashboard.

Furthermore, the account should only have access to perform the actions required by Cloudwork. For example, if the relevant sync profile only reads data from Active Directory about users and groups and performs password resets, then the account should not have delegated access to modify other user attributes or delete user accounts or other objects in your Active Directory.

4.1 Configuration

Schools should consult the documentation for the systems they have integrated with Cloudwork to determine the correct steps to delegate access.

Information on delegating access in Active Directory can be found in [this article on the Microsoft website](#).

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

5 Rules to Restrict Access to Sensitive Systems

One or more SSO Services will be configured in your Dashboard, allowing users to seamlessly access other services at your school. Common services include email, cloud storage and collaboration platforms like Microsoft Office365 and Google Workspace/Apps, learning management systems like Canvas or Moodle, textbook platforms and the student management system. Authorization rules can be configured for each SSO service to allow or deny access, subject to attributes of the user or their connection. Authorization rules enable a graduated level of access corresponding to the level of potential risk.

To illustrate this, consider how the typical school management system contains a significant amount of personal and sensitive information about staff, students and families, including contact information, demographic data, medical conditions and histories, and financial information.

Contrast this with a digital textbook platform, which typically houses a very limited amount of personal information and generally no sensitive information. What limited personal information is contained within the digital textbook platform can generally only be accessed by the logged in user to which the personal information relates. These two systems, having vastly different risk profiles, will likely require different cyber-risk controls, which can be achieved in part through authorization rules for each SSO Service in the Dashboard.


5.1 Configuration

1. From the Dashboard, go to “Single Sign On”. SSO enabled services should be listed.
2. Select a service, then click the Authorization link at the top of the page.
3. The “Authorization Method” at the top of the page will have one of two values:
 - a. User must pass all rulesets to be able to access this service
 - b. User must pass at least one ruleset to be able to access this service
 - c. This can be changed from the “Change Authorization Method” link at the top.
4. Any existing rulesets will be shown in the rulesets table. Click “New ruleset” to create a new authorization rule.
5. Enter a description and name for the rule.
6. Select an “action”, which will be one of the following values:
 - a. Allow users matching at least one rule
 - b. Only allow users matching all rules
 - c. Deny users matching at least one rule
7. Configure and add rows to the “Rules” table to allow or deny access based on user or session attributes. Click Submit.

5.1.1 Examples




Allow students to login to the school management system from anywhere, while requiring staff to be onsite, or connected via the VPN.

1. Create two rulesets.
 - Staff ruleset:
 - All rules must be matched
 - IP address must match your school’s public IP address/default gateway
 - Org unit must match the organisational unit containing your staff accounts
 - Student ruleset:
 - Org unit must match the organisation unit containing your student accounts
2. Set the authorization method to “User must pass at least one ruleset”

Name * 


Helpful descriptor for this authorization ruleset

action

Rules	Attribute	Comparison	Match	
	<input type="text" value="IP Address"/>		<input type="text" value="1.2.3.4"/>	
	<input type="text" value="Orgunit"/>		<input type="text" value="/Domain Users/Staff"/>	
	<input type="text"/>	<input type="text" value="Exact"/>	<input type="text"/>	



Fields marked with * are required

New Filter

Name * 

Helpful descriptor for this authorization ruleset

action

Rules	Attribute	Comparison	Match	
	<input type="text" value="Groups"/>	<input type="text" value="Contains"/>	<input type="text" value="Staff"/>	
	<input type="text" value="IP Address"/>		<input type="text" value="1.2.3.4"/>	

Fields marked with * are required

5.2 Supporting policies and procedures

- Restricting access to systems to e.g. specific locations, will likely require the support and approval of senior leadership. Some effort will be required to clearly assess and articulate the need for such change, which can be supported by a risk assessment.

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

6 Multi-Factor Authentication

Multi-factor authentication (MFA) is now viewed as an essential control for internet-facing IT systems. It is referenced directly in various security frameworks, including the NIST Framework and Essential Eight. Insurance providers also increasingly expect that schools implement multi-factor authentication for internet-facing services, and may make coverage contingent on doing so, or reduce coverage where this has not been implemented.

Multi-factor authentication is viewed as a very effective control against a serious and very likely risk, which may have significant consequences for a school if or when it does eventuate. For these reasons, school boards and leadership teams are increasingly expecting their IT staff to implement MFA for internet-enabled services.

Cloudwork provides two methods for implementing multi-factor authentication for your users: *App authentication* and *SMS codes*.

Multi-factor authentication is configured and managed for each user from their user profile. Defaults can be configured during the user provisioning process. Contact Cloudwork Support to discuss your requirements. SSO-linked services can also be configured to only permit users with MFA enabled to access the relevant service.

6.1 Configuration

To enable MFA for a user

1. From the Dashboard, select Users and locate the user you wish to configure.
2. Review MFA configuration under “Security” for the selected user.
3. Select “Enable SMS” or “Enable App” for the chosen authentication method. Follow the prompts to complete the required configuration.

To enable MFA for an Org Unit, e.g. all staff or groups of students

1. From the Dashboard, expand the navigation menu (top left), expand Settings and click “Cloudwork.ID Settings”.
2. Expand the list of Org Units in the left hand pane and click the name of the Org Unit you wish to configure.
3. In the Features pane on the right, click “Override Settings”.
4. Review the message and click “Submit” to confirm you wish to override the default settings or inherited settings.
5. Review and configure the following fields, then click "Submit" to save changes:

Field	Explanation
Multifactor Authentication	Whether users should be allowed to manage their own multi-factor authentication settings.
Disable multifactor	Whether users can disable multi-factor authentication.
Users must enable MFA	Force users to enable multi-factor authentication before they can login to SSO Services.
Multifactor Authentication Whitelist	Public IP addresses or subnets from which users should not be prompted to provide an MFA code.

Users will occasionally need to re-setup multi-factor authentication because they have e.g. lost their phone or transferred to a new device. Click the “Disable multifactor” button on the user profile to disable and reconfigure.

To require that all users of a service have multi-factor authentication:

1. From the Dashboard, select Single Sign On and select the relevant Service.
2. Click Edit next to SAML config.
3. Set “Multifactor authentication” to “Only users who have Multifactor Authentication enabled can access this service”.

Users who do not have multi-factor authentication enabled will be prevented from logging into the relevant service and will instead be shown a message to contact their administrator.

6.2 Additional information

- The diverse range and capabilities of users in a school environment pose some unique challenges, especially with respect to implementing MFA. It will generally be inappropriate for younger students, as the degree of risk versus the impact on usability is too high. Other controls can however be considered for these groups of users, for example limiting access to services from external locations via authorization rules.
- Both SMS and App multi-factor authentication require access to a mobile phone, but student mobile phone policies may prevent student users accessing their phones except during break times. This may preclude your school from using MFA for student accounts.
- It may be desirable to stage the rollout of MFA in an order commensurate with the level of risk posed by user access to sensitive systems and data. A suggested order for roll out in a typical school is:
 - IT team members and all Cloudwork admin users
 - Executive and other senior leadership
 - Finance staff and payroll staff, nurses, school counsellors and psychologists, house masters/year advisors
 - Teaching staff and all remaining operational staff
 - Parents
- While SMS-based MFA is considered less secure than other methods due to the ease that tokens can be stolen, it offers a level of convenience and usability that may outweigh this risk in your environment and is certainly much better than not using multi-factor authentication at all.
- App authentication relies on the Time-based One-Time Password (TOTP) protocol. This protocol allows users to authenticate using a time-bound token generated using a shared secret known to both the server and the client (i.e. an app like Google Authenticator). App authentication does not require codes to be transferred between the client and server, except during initial setup, and so is not subject to the same security risks as SMS based authentication (e.g. interception or relaying). This also has the advantage of allowing authentication to occur where phone reception may be limited.
- Users planning to travel internationally, e.g. teaching staff during school holiday periods, should be encouraged to use app-based authentication to avoid the complications, unreliability or additional cost of international roaming when using SMS-based authentication while overseas.
- The Security Report in Dashboard > Reports lists the MFA status, enforcement level and methods (App or SMS) for all users in the organisation. This report may provide useful insights when checked as part of a regular security review.

- Cloudwork logs a range of events concerning the configuration, use and enforcement of MFA. These events can be viewed in the User Activity log in Dashboard > Reports. Configuring alerts for higher-risk events, such as administrators disabling or resetting multi-factor authentication for a user, coupled with procedures for regularly reviewing reports should be considered when deploying multi-factor authentication at your school.

6.3 Supporting policies and procedures

- Many of your users should have some understanding of or experience with MFA, given its use by banks and government organisations. But unlike many other security controls, MFA has a noticeable impact on the user experience, so communication and change-management plans are essential to a successful rollout of this functionality.
- The approval and engagement of senior leadership will also be essential to implementing this security control. Consider asking your school principal to announce this change to all staff as a way to clearly communicate that this is a priority for your organisation. This should minimise any pushback you may get from otherwise reluctant users.
- An audit of the MFA status for key groups of users, for example, new staff and highly privileged users, should form part of your regular security reviews to detect, for example, a temporary configuration change by a service desk operator that has not been reverted.

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

7 Geoblocking

Geoblocking refers to the process of restricting access to a computer system to users in particular countries or geographic locations. The originating country or geographic location of internet traffic can be approximated with a fair degree of accuracy from the source IP address of an internet request.

By allowing schools to permit or block authentication requests from particular countries, Cloudwork allows them to reduce the risk posed by compromised accounts where attackers might reside in overseas jurisdictions.

7.1 Configuration

1. From the Dashboard, expand the menu (top left), select Settings > Authentication Settings.
2. Review configuration for “Country Blocking” at the bottom of the page. Set this field to either “Allow only specified countries” or “Block specified countries”.
 - a. If you select “Allow only specified countries”, add Australia and any other countries to the countries list which you know your users may be logging in from, including parents who may live overseas.
 - b. If you selected “Block specified countries”, add any countries you wish to block traffic from into the country list.
3. Click “Submit” to apply the configuration change.

7.2 Additional information

- While not all cyber attacks originate from botnets, a significant proportion do. The Spamhaus Project² maintains a number of “Top 10” lists for countries with significant numbers of spammers and bots. Consider using Cloudwork’s geoblocking features to block traffic from countries listed in the top 10 botnet infected countries listed on this page: <https://www.spamhaus.org/statistics/botnet-cc/>
- While geoblocking may provide some protection from credential attacks originating from overseas, the effectiveness of geoblocking as a security measure should not be overstated, as there have been many instances of credential attacks originating from botnets within Australia.

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)

² <https://www.spamhaus.org/>

8 Customised Themes and User Awareness Training

Tailoring the visual appearance of your Cloudwork login screen, and training your users to perform basic checks before providing their credentials to a website, are important steps to reduce the risk of account credentials being compromised through phishing attacks.

8.1 Configuration

1. From the Dashboard, expand the navigation menu (top left), expand Settings and click Login Theme.
2. Click General Settings.
3. Review and update login page settings, such as the text colour, background image and logo. Click Submit to save any changes.
4. Click Login Page Settings.
5. Review and update the textual messages that are presented to users on the login page. Click Submit to save any changes.

8.2 Supporting policies and procedures

- Communicate any changes about the appearance of your login page to your users, preferably in advance, and ideally with screenshots so that they become familiar with the appearance of the Cloudwork login page.
- Suggest to staff that they contact the IT team before entering their school-issued credentials into a login page that varies from the appearance of your Cloudwork login page.
- Your Cloudwork site has a custom domain name which references your school. Train your users to always look for that domain name before entering their credentials.
- Your Cloudwork site is also protected by an SSL certificate. Train your users to look for the lock symbol when providing their credentials to login to any website.

Security Framework

NIST Category	NIST Subcategory
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained

9 Compromised Passwords, Minimum Password Length

Subject to your configuration, Cloudwork may allow users to change their own passwords, either through the *forgot my password* workflow, or *change password* link. Before updating a user's password, Cloudwork can check that a proposed new password is not in a database of compromised passwords, and can also enforce complexity and minimum password length.

9.1 Configuration

1. Expand Navigation menu (top left), expand Settings, click "Cloudwork.ID Settings".
2. Optionally expand and select an Org Unit to configure in the left pane.
3. Click "Edit" or "Override Settings" in the Features pane. If overriding, you will be prompted to confirm you wish to override settings to the selected Org Unit.
4. Then follow either a) or b) below.

a) Prevent the use of compromised passwords:

1. Ensure "Reject Compromised Passwords" is set to "Yes".
2. Ensure "Compromised Password Threshold" is set to a sufficiently low number. The default value for this field is 100, but a lower number will make it even less likely a user will be able to use a compromised password when changing their password.
3. Click "Submit" to save any changes.

b) Configure password length and complexity settings:

1. Set appropriate values for "Minimum Password Length" and "Require Complexity".
2. Click "Submit" to save any changes.

9.2 Additional information

1. It may be appropriate to vary password length and complexity requirements for different groups of users in accordance with their capacity and the availability of other security measures. Schools can use the override settings feature in the Cloudwork.ID settings page to differentiate password policies for these groups.
2. The latest password use guidance from NIST advises organisations to focus on password *length* over complexity. Forced password changes after e.g. 90 days are *no longer recommended*. When users are forced to change passwords regularly, the majority typically make only small variations, by e.g. incrementing a number. These changes are easy for attackers to guess, and offer little protection relative to the frustration and inconvenience experienced by your users.

9.3 Supporting policies and procedures

- Ensure staff and students are provided with appropriate guidance at induction and on a recurring basis around how to select secure passwords. Review the latest guidance on password security from e.g. NIST to develop your training in this area.

Security Framework

NIST Category	NIST Subcategory
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

10 Key Additional Controls

Implementing the configuration, policies and procedures outlined in earlier sections will enable Cloudwork organisations to move towards an optimal security posture in alignment with the NIST Cybersecurity Framework. The following section outlines additional controls which are included out-of-the-box for all Cloudwork Customers:

NIST Category	NIST Subcategory	Explanation
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-4: Adequate capacity to ensure availability is maintained	Cloudwork implements highly available, load balancing technologies to maintain system availability at times of peak load.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-4: Backups of information are conducted, maintained, and tested	Cloudwork application code and server configurations are automatically backed up on a regular basis. Backup restorations are also performed on a regular basis.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	In addition to load balancing for managing load, Cloudwork has arrangements with third-party providers to mitigate the risk of DDOS attacks.

Appendix A: Configuration Summaries

1 Timely Revocation of Identities and Credentials

1. From the Dashboard, select Sync Profile.
2. Select each of your LDAP user sync profiles in turn.
3. Click Edit and review the value for “Action for deleted users”.
4. Ensure a value *other than* “Do nothing” is selected.
5. If changes are made, click “Submit”.
6. Repeat for each LDAP user sync profile.

2 Exception Alerting and Log Review

1. From the Dashboard, select Reporting.
2. Click User Activity or Administrator Activity.
3. Filter the relevant event log by one or more of the events.
4. Click Create Alert.
5. Enter an appropriate Description.
6. Either tick “Send alert to all super administrators” or one or more email addresses in the “Other recipients” field.
7. Click Submit.

3 Delegation of Least Privilege Access to Admin Users

1. From the Dashboard, select Admin Roles.
2. Click “Add New Role” or “Edit Permissions” at the top of the Admin Roles page.
3. Enter a name and select the required permissions.
4. Click Submit.

4 Least Privilege Delegation for Sync Profile Accounts

1. Schools should consult the documentation for the systems they have integrated with Cloudwork to determine the correct steps to delegate access.

5 Rules to Restrict Access to Sensitive Systems

1. From the Dashboard, go to “Single Sign On”. SSO enabled services should be listed.
2. Select a service, then click the Authorization link at the top of the page.
3. The “Authorization Method” at the top of the page will have one of two values:
 1. User must pass all rulesets to be able to access this service
 2. User must pass at least one ruleset to be able to access this service
 3. This can be changed from the “Change Authorization Method” link at the top.
4. Any existing rulesets will be shown in the rulesets table. Click “New ruleset” to create a new authorization rule.
5. Enter a description and name for the rule.
6. Select an “action”, which will be one of the following values:
 1. Allow users matching at least one rule

2. Only allow users matching all rules
3. Deny users matching at least one rule
7. Configure and add rows to the “Rules” table to allow or deny access based on user or session attributes. Click Submit.

6 Multi-Factor Authentication

1. From the Dashboard, expand the navigation menu (top left), expand Settings and click “Cloudwork.ID Settings”.
2. Expand the list of Org Units in the left hand pane and click the name of the Org Unit you wish to configure.
3. In the Features pane on the right, click “Override Settings”.
4. Review the message and click “Submit” to confirm you wish to override the default settings or inherited settings.
5. Review and configure the fields, then click “Submit” to save changes.
6. To re-setup MFA for a new device, click the “Disable multifactor” button on the user profile to disable and reconfigure.
7. To require that all users of a service have multi-factor authentication:
 - a) From the Dashboard, select Single Sign On and select the relevant Service.
 - b) Click Edit next to SAML config.
 - c) Set “Multifactor authentication” to “Only users who have Multifactor Authentication enabled can access this service”.

7 Geoblocking

1. From the Dashboard, expand the menu (top left), select Settings > Authentication Settings.
2. Review configuration for “Country Blocking” at the bottom of the page. Set this field to either “Allow only specified countries” or “Block specified countries”.
 - a) If you select “Allow only specified countries”, add Australia and any other countries to the countries list which you know your users may be logging in from, including parents who may live overseas.
 - b) If you selected “Block specified countries”, add any countries you wish to block traffic from into the country list.
3. Click “Submit” to apply the configuration change.

8 Customised Themes and User Awareness Training

1. From the Dashboard, expand the navigation menu (top left), expand Settings and click Login Theme.
2. Click General Settings.
3. Review and update login page settings, such as the text colour, background image and logo. Click Submit to save any changes.
4. Click Login Page Settings.
5. Review and update the textual messages that are presented to users on the login page. Click Submit to save any changes.

9 Compromised Passwords, Minimum Password Length

1. Expand Navigation menu (top left), expand Settings, click “Cloudwork.ID Settings”.
2. Optionally expand and select an Org Unit to configure in the left pane.
3. Click “Edit” or “Override Settings” in the Features pane. If overriding, you will be prompted to confirm you wish to override settings to the selected Org Unit.
4. **Then follow either (a) or (b) below.**
 - a. Prevent the use of compromised passwords:**
 1. Ensure “Reject Compromised Passwords” is set to “Yes”.
 2. Ensure “Compromised Password Threshold” is set to a sufficiently low number. The default value for this field is 100, but a lower number will make it even less likely a user will be able to use a compromised password when changing their password.
 3. Click “Submit” to save any changes.
 - b. Configure password length and complexity settings:**
 1. Set appropriate values for “Minimum Password Length” and “Require Complexity”.
 2. Click “Submit” to save any changes.

Contact Us

Studentnet has been working with schools since 1996. We are dedicated to the needs of educators, students, parents, IT staff and school communities, and are committed to providing the highest possible levels of security and privacy. Please feel free to contact us to discuss this document or your school's requirements.

Tel: +612 9281 1626 Email: info@studentnet.net

Postal Address: Suite 1, 89 Jones St, Ultimo NSW Australia 2007

Studentnet®, the Studentnet® logo, Cloudwork®, Make the Cloud Yours® and Isonet® are registered trade marks of Twin-K Computers Pty Ltd, ABN 90 001 966 892. This document is Commercial-in-Confidence © Studentnet 2022.