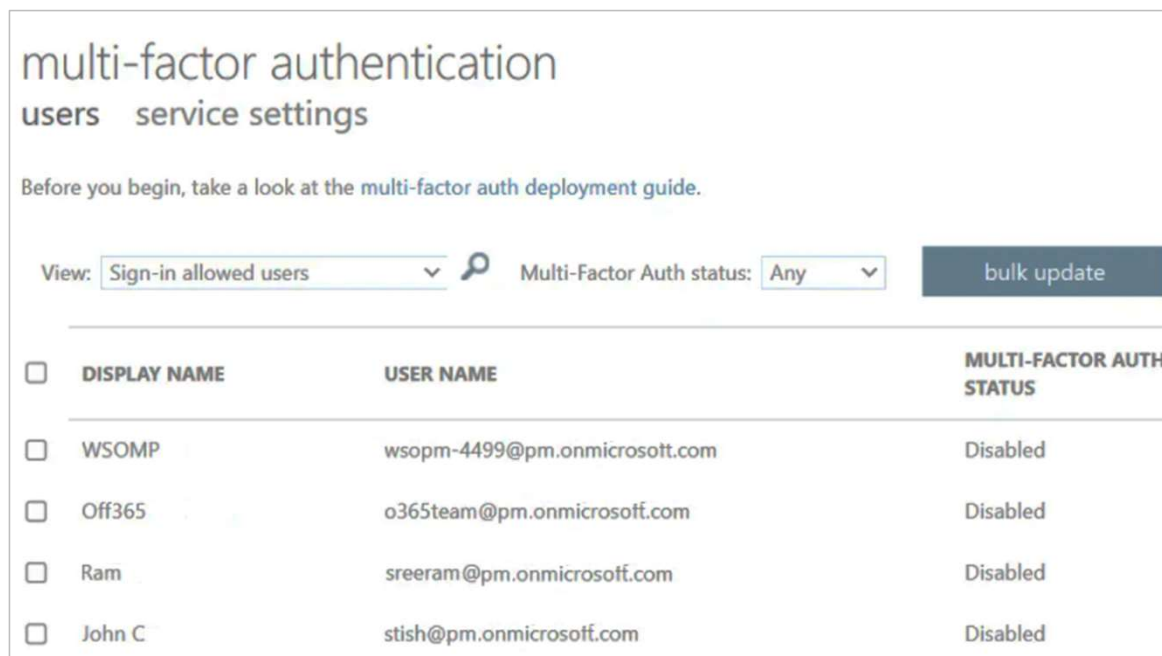


# Configuration Guide for Singtel Start Digital (Microsoft 365)

This quick-start configuration guide is for organisations using Microsoft 365 (M365) through Windows devices, without other servers. Some of the settings are to be configured at M365 (“@M365”), while others are to be configured at the Windows devices (“@Windows Device”). Windows 10 is used as the reference version for the steps and screenshots given.

## Configuration Guide for Singtel Start Digital (M365)

### 1. Enable Multi-Factor Authentication (MFA) for Administrators (@M365)



The screenshot shows the 'multi-factor authentication' configuration page for 'users' under 'service settings'. It includes a 'View' dropdown set to 'Sign-in allowed users', a 'Multi-Factor Auth status' dropdown set to 'Any', and a 'bulk update' button. Below is a table of users with their MFA status set to 'Disabled'.

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	WSOMP	wsopm-4499@pm.onmicrosoft.com	Disabled
<input type="checkbox"/>	Off365	o365team@pm.onmicrosoft.com	Disabled
<input type="checkbox"/>	Ram	sreeram@pm.onmicrosoft.com	Disabled
<input type="checkbox"/>	John C	stish@pm.onmicrosoft.com	Disabled

- Go to Users > Service Settings
- Under the Services Settings, enable MFA functionality for the selected administrator.
- Enable MFA for multiple users using a bulk update, or check the boxes next to the required user accounts and enable MFA for them.

#### Additional information:

- When users log in after the administrator has enabled MFA for them, they will be asked to set up verification details required to complete the MFA configuration.
- They can choose to receive the verification code through a text message, call, or push notification to the Microsoft Authenticator app.

## Configuration Guide for Singtel Start Digital (M365)

### 2. Strong Password Settings (@M365)

Property	Requirements
Characters allowed	<ul style="list-style-type: none"><li>• A - Z</li><li>• a - z</li><li>• 0 - 9</li><li>• @ # \$ % ^ &amp; * - _ ! + = [ ] { }   \ : ' , . ? / ` ~ " ( ) ;</li></ul>
Characters not allowed	<ul style="list-style-type: none"><li>• Unicode characters</li><li>• Spaces</li><li>• Cannot contain a dot character "." immediately preceding the "@" symbol"</li></ul>
Password restrictions	<ul style="list-style-type: none"><li>• A minimum of 8 characters and a maximum of 256 characters. *this is a recent change; the former maximum was 16 characters</li><li>• Requires three out of four of the following:<ul style="list-style-type: none"><li>- Lowercase characters</li><li>- Uppercase characters</li><li>- Numbers (0-9)</li><li>- Symbols</li></ul></li></ul>

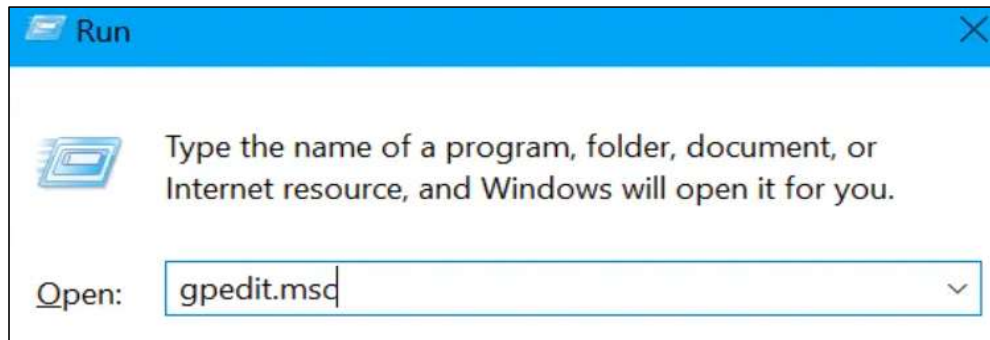
- Note: limited password options are available for M365 cloud-only users that do not have an Active Directory account
- In M365, the default minimum is 8 characters, with a combination of alphanumeric characters and special characters.

#### Additional information:

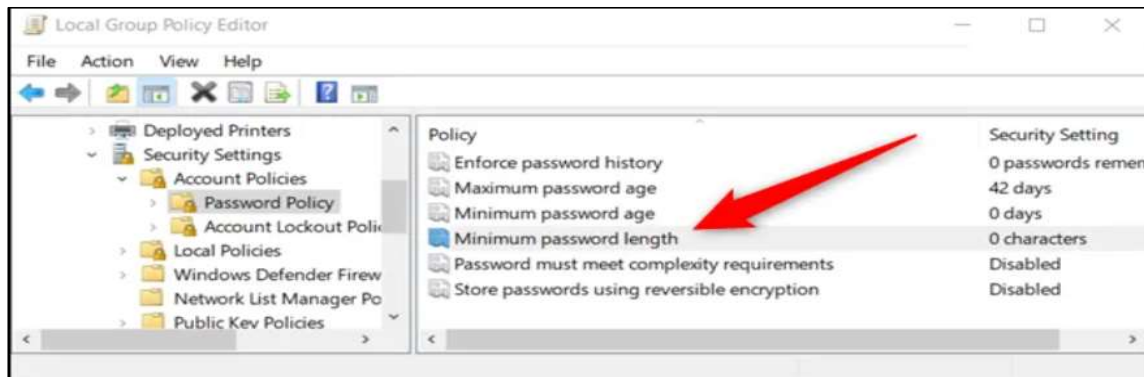
- Enforce a password history policy to ensure that employees do not reuse their previous passwords.
- Encourage users to use passphrases such as "Iwant2l@se10kg", which may be long and complex, yet easy to remember.
- Discourage users from using the same passwords across different systems.

## Configuration Guide for Singtel Start Digital (M365)

### 2. Strong password settings (@Windows device)



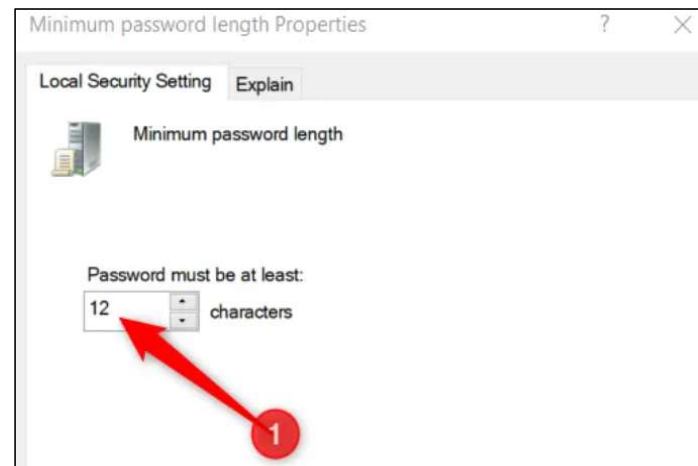
- Launch the group policy editor by pressing Windows+R.
- Type "gpedit.msc" and press Enter.



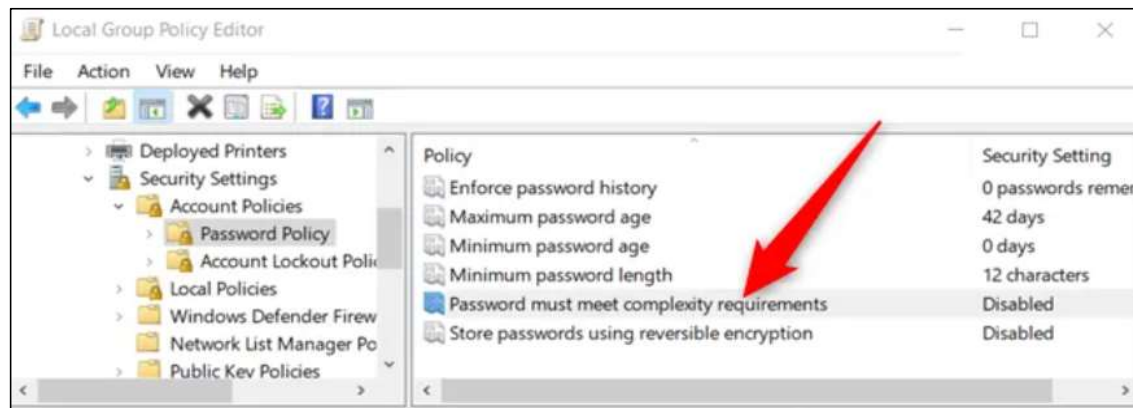
- Navigate to Computer configuration > Windows settings > Security settings > Account policies > Password policy.

## Configuration Guide for Singtel Start Digital (M365)

### 2. Strong password settings (@Windows device)



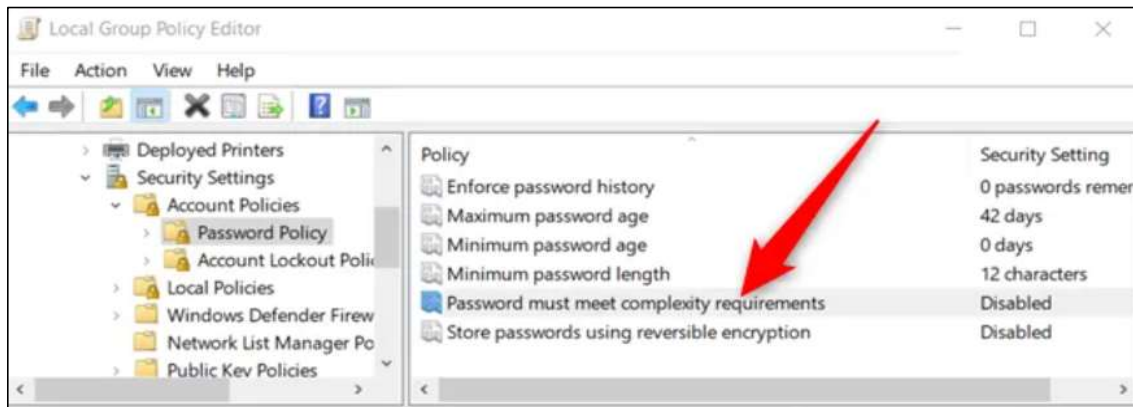
- d. Set the minimum password length to 12 characters.



- e. Enable password complexity requirements, to facilitate users in creating a secure password
- f. Restart your computer after making the policy changes.

## Configuration Guide for Singtel Start Digital (M365)

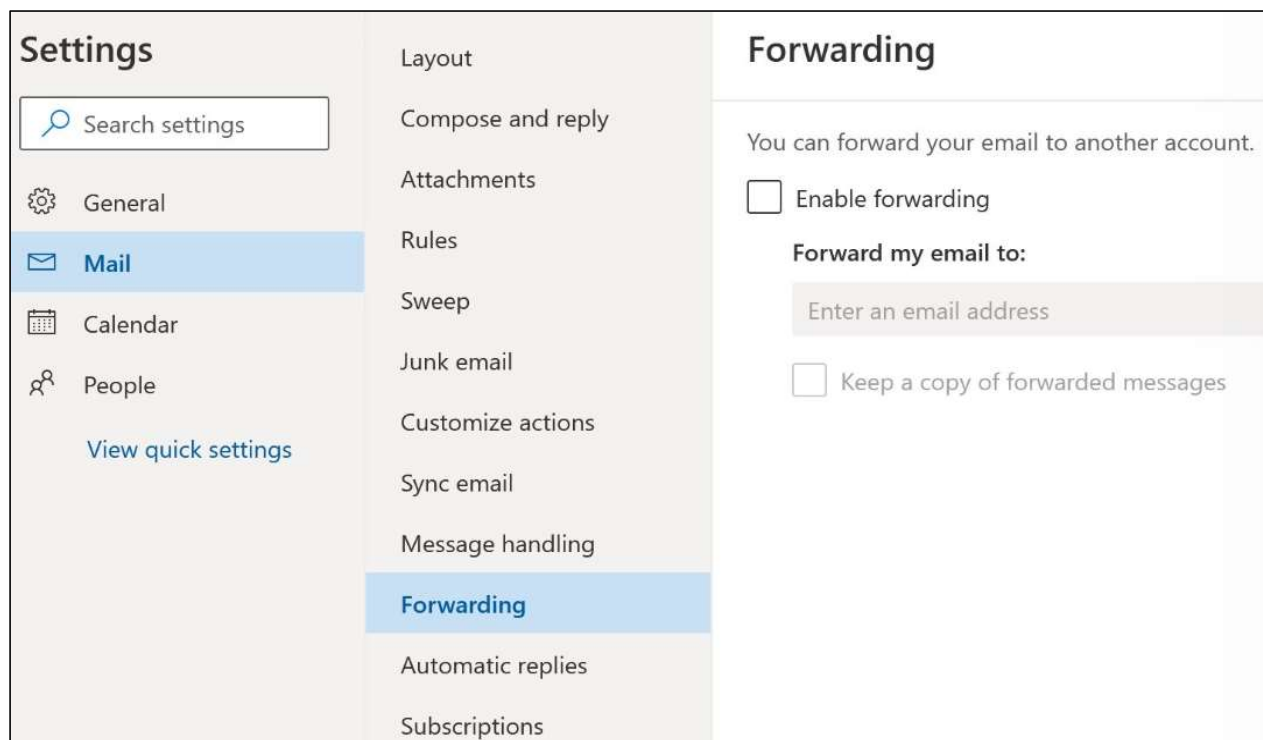
### 2. Strong password settings (@Windows device)



- g. Setting this to enabled means that Windows passwords
- do not contain the user account name or full name
  - be at least 6 characters in length and contain characters from at least 3 of the 4 following categories:
    - uppercase English letters (A-Z),
    - lowercase English letters (a-z),
    - base 10 digits (0-9), and
    - non-alphabetic characters (such as \$, !, %).
- h. Restart your computer after making the above policy changes.

## Configuration Guide for Singtel Start Digital (M365)

### 3. Disable Email Auto forwarding (@Windows device)



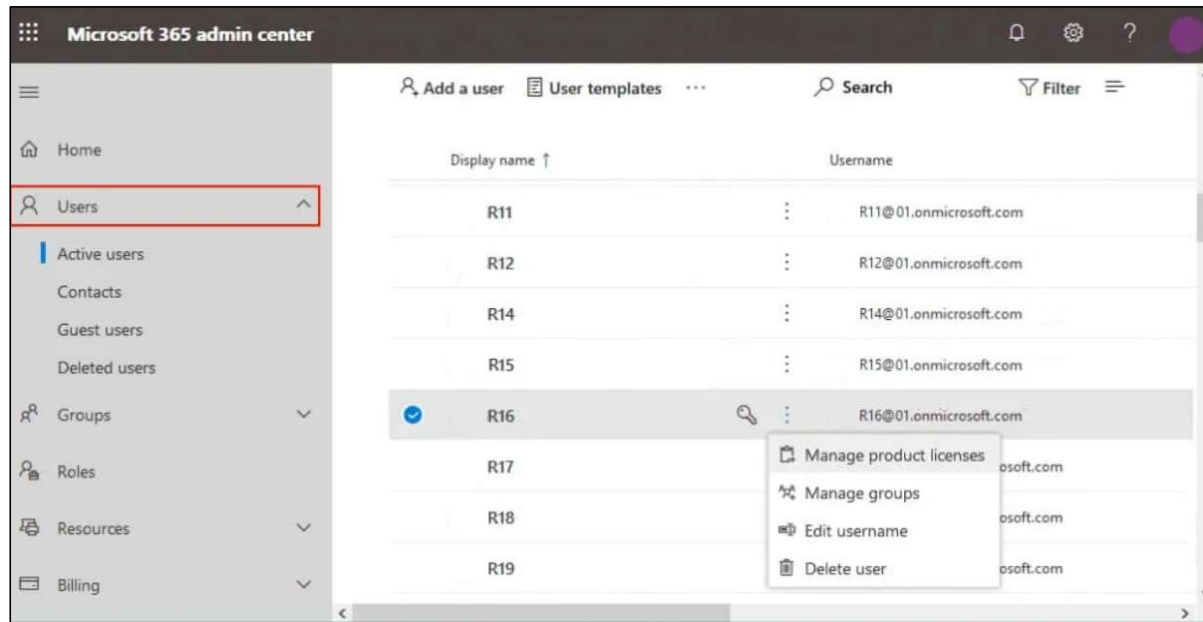
- Note: M365's current default setting is to disallow automatic forwarding to external email, for enhanced security.
- It is recommended to disallow automatic forwarding if the user's email account is often used for large amounts of personal data or personal data more likely to result in harm to individuals.

For more information:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide>

## Configuration Guide for Singtel Start Digital (M365)

### 4. Review of User Accounts (@M365)

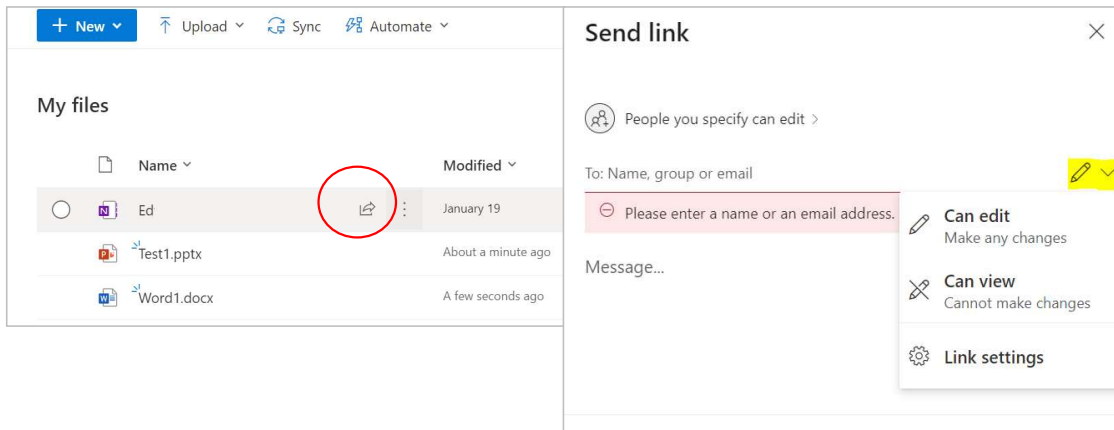


- Regularly conduct periodic review of user accounts to ensure that unused accounts are removed.



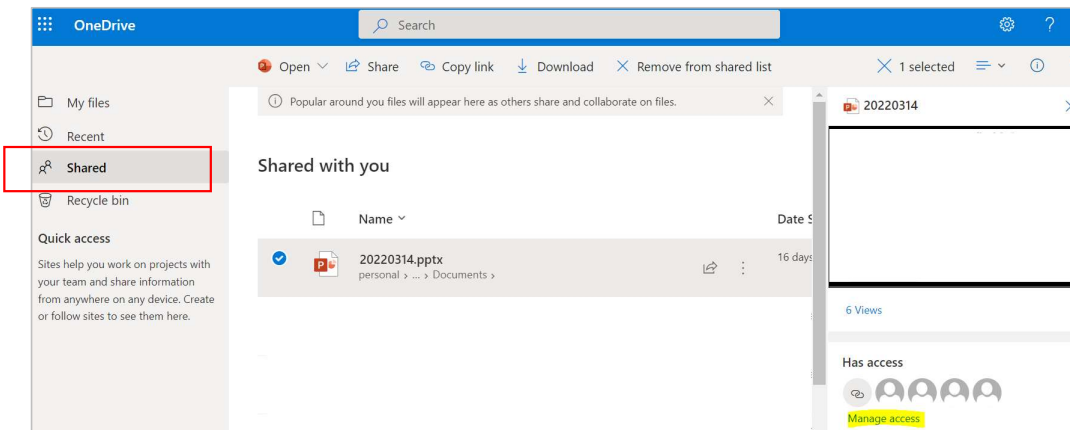
# Configuration Guide for Singtel Start Digital (M365)

## 5. Configure Folder Permissions (@M365 OneDrive)



### To share a file/folder

- Select the file you want to share, and then select Share.
- Specify the person(s) you want to share with. Click on the pencil icon to select the access permissions to be granted, i.e. view only or can edit.

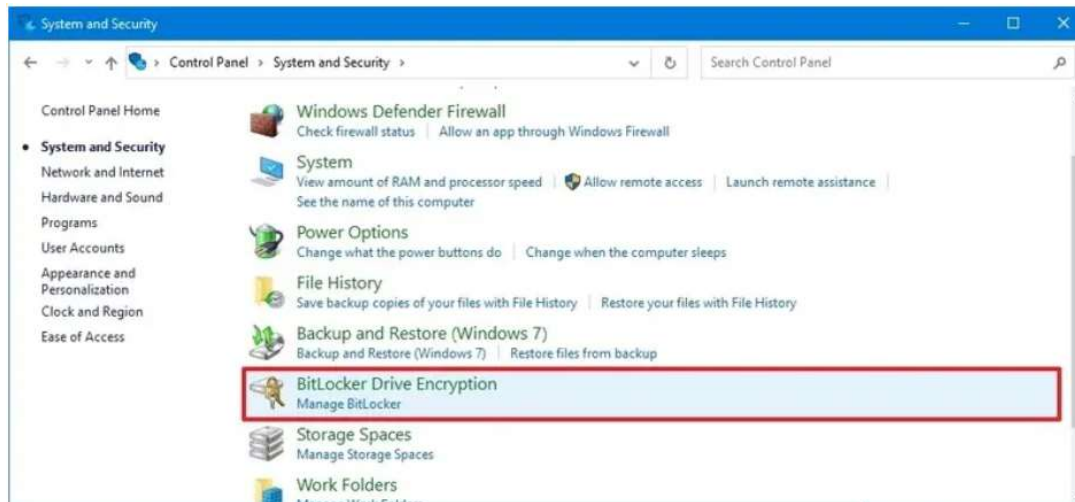


### To change sharing permissions

- Select **Shared**.
- Select a folder or file, and then select the **Information** icon.
- Do one of the following:
  - Select Add People to share with more people.
  - Select Manage access to change permissions.
  - Select the Can Edit or Can View dropdown to change permissions or Stop Sharing.
  - Select X to remove the link.

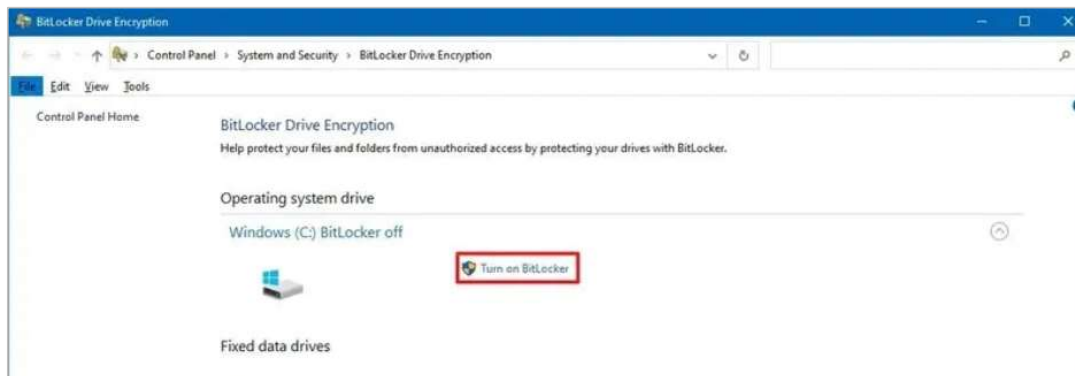
## Configuration Guide for Singtel Start Digital (M365)

### 6. Turn on Bitlocker Disk Encryption (@Windows device)



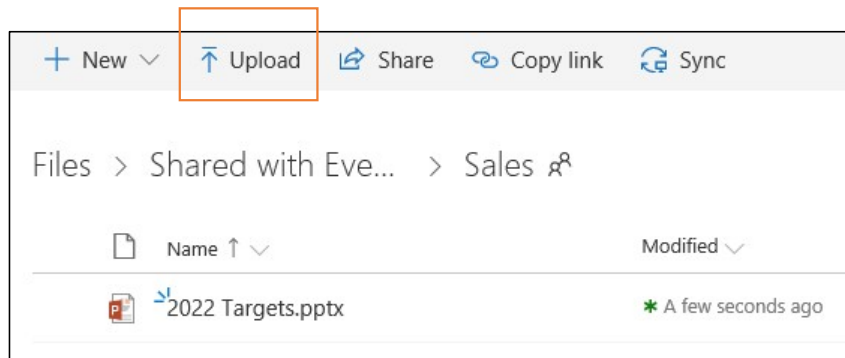
Note: For Windows 10, BitLocker is available on the Pro and Enterprise editions only.

- a. Open Start.
- b. Search for Control Panel and click the top result to open the app.
- c. Click on System and Security.
- d. Click on BitLocker Drive Encryption.
- e. Under the "Operating system drive" section, click the Turn on BitLocker option.



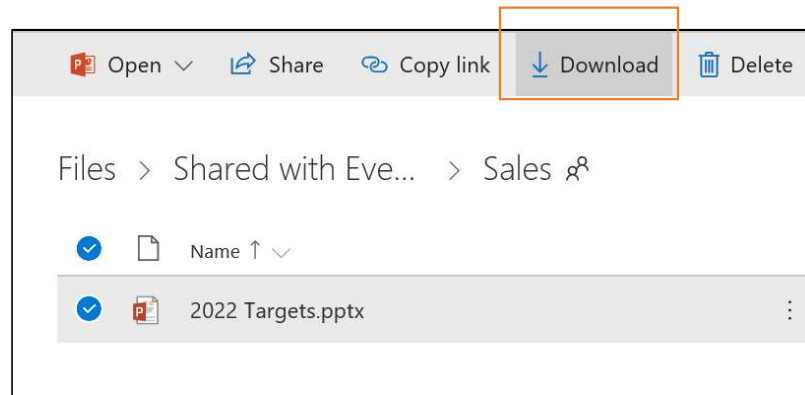
## Configuration Guide for Singtel Start Digital (M365)

### 7. Manual Backup of Local Files (from Windows device to M365 OneDrive)



#### To backup from a local device to M365 OneDrive:

- Zip the local the local drive/folder/file that you wish to backup. Assign a password to the zipped file if necessary.
- At OneDrive, navigate to the target folder for the backup file.
- Click on the **Upload** button in OneDrive. Select the file/zipped file from the previous step.



#### To restore from M365 OneDrive to a local device:

- Select the backed up (zip file) at M365 OneDrive.
- Click on **Download**
- Unzip the file if necessary and key in the password if necessary.
- Copy the file/folders to the target destination on your local device.

## **Configuration Guide for Singtel Start Digital (M365)**

### **8. Backup of Cloud Files (@M365 OneDrive)**

- All documents stored at OneDrive are automatically synchronised to another cloud location. This works like an automatic backup.
- For restoration of data from backup, you can either restore your OneDrive (select from a day within the last 30 days), or restore a previous version of the selected file.

# Configuration Guide for Singtel Start Digital (M365)

## 8. Backup of Cloud Files (@M365 OneDrive)

### To restore your entire OneDrive

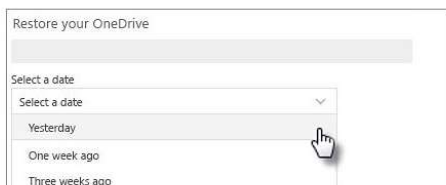
#### Restore OneDrive to a previous time

To restore your OneDrive, you'll need to have Microsoft 365. Otherwise, you'll be redirected to this article when you try to follow the steps below.

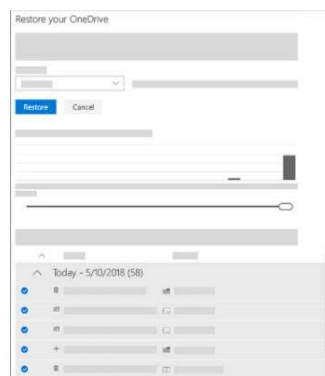
1. Go to the [OneDrive website](#). (Make sure you're signed in with the correct account.)
2. If you're signed in with:
  - A personal account with a Microsoft 365 subscription, at the top of the page, select **Settings** > **Options**, and then select **Restore your OneDrive** from the left navigation.
  - A work or school account, select **Settings** > **Restore your OneDrive**.

**Note:** The **Restore your OneDrive** option isn't available in the classic experience of OneDrive for work or school or without a Microsoft 365 subscription.

3. On the Restore page, select a date from the dropdown list—such as **Yesterday**—or select **Custom date and time**. If you're restoring your files after automatic ransomware detection, a suggested restore date will be filled in for you.



4. Use the activity chart and activity feed to review the recent activities that you want to undo.



The daily activity chart shows the volume of file activities in each day for the last 30 days. It gives you an overview of what has happened to your OneDrive over time and it can help you identify any unusual activities. For example, if your OneDrive was infected by malware, you can look for when it happened.

The activity feed shows individual file and folder operations in reverse chronological order. You can scroll down to see previous days, or move the slider below the daily activity chart to quickly move to a specific day.

**Tip:** Use the expand and collapse arrow next to each day in the activity feed to show or hide activities for that day.

5. If you selected **Custom date and time**, select the earliest activity that you want to undo. When you select an activity, all other activities that occurred after that are selected automatically.

**Note:** Before you select **Restore**, scroll to the top of the activity feed to review all the activities you are about to undo. When you pick a day in the activity chart, the more recent activities are hidden in the feed, but they're still selected when you select an activity.

5. If you selected **Custom date and time**, select the earliest activity that you want to undo. When you select an activity, all other activities that occurred after that are selected automatically.

**Note:** Before you select **Restore**, scroll to the top of the activity feed to review all the activities you are about to undo. When you pick a day in the activity chart, the more recent activities are hidden in the feed, but they're still selected when you select an activity.

6. When you're ready to restore your OneDrive, select **Restore**. This action will undo all the activities you selected.

Your OneDrive will be restored to the state it was in before the first activity you selected.

**Note:** If you change your mind about the restore you just did, you can undo the restore by running Files Restore again and selecting the restore action you just did.

#### Limitations and troubleshooting

- When version history is turned off, Files Restore can't restore files to a previous version. For information about versioning settings, see [Enable and configure versioning for a list or library](#). Files Restore uses version history and the recycle bin to restore OneDrive, so it's subject to the same restrictions as those features.
- You can't restore deleted files after they've been removed from the [site collection recycle bin](#)—either by manual delete or by emptying the recycle bin. A SharePoint site collection administrator may be able to view and restore those deleted items.
- Albums are not restored.
- If you upload a file or folder that you deleted, Files Restore will skip the restore operation for that file or folder.
- If some files or folders cannot be restored, a log file will be generated at the root folder of your OneDrive to capture the errors. The name of the file will begin with "RestoreLog" followed by an ID (for example, RestoreLog-e8b977ee-e059-454d-8117-569b380eed67.log). You can share the log file with our support team to troubleshoot any issues that may occur.

# Configuration Guide for Singtel Start Digital (M365)

## 8. Backup of Cloud Files (@M365 OneDrive)

### To restore a selected file

#### Restore a previous version of a file stored in OneDrive

OneDrive for Business, SharePoint Server Subscription Edition, [More...](#)

With version history, you can see and restore older versions of your files stored in OneDrive or SharePoint. Version history works with all file types, including Microsoft 365 files, PDFs, CAD files, photos, videos, and more. If you need to, you may be able to [restore deleted OneDrive files](#) or [restore deleted SharePoint items](#) from the recycle bin.

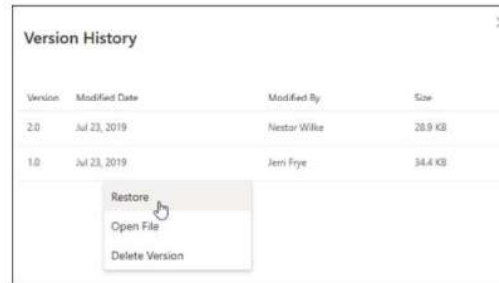
**Tip:** You can also [View previous versions of Office files](#) in Office apps.

1. Sign in to OneDrive with your personal Microsoft account or your work or school account.
2. Select the file that you want to restore to an earlier version (you can only restore one file at a time), right-click, then select **Version history**.

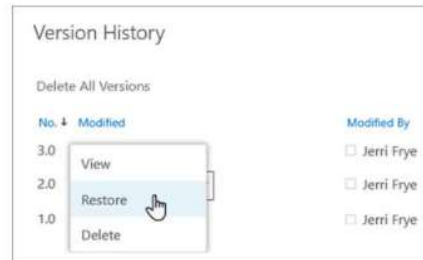
**Note:** In Classic view, select the document, then at the top, select **More > Version History**.

3. In the **Version History** pane, do one of the following:

If you're signed in to OneDrive or SharePoint with a work or school account (such as a Microsoft 365 account), select the ellipses (...) next to the version of the document that you want to restore, and then click **Restore**.

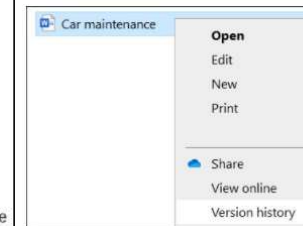


In Classic view or previous versions of SharePoint Server, select the arrow next to the version of the document that you want to restore, and then click **Restore**.



#### Use Version history in File Explorer

If you have the OneDrive [sync app](#) installed on your PC, right-click the file that you want to restore to an earlier version in File Explorer and select **Version history**. Then select the ellipses (...) next to the version you want and click **Restore**.



The document version you selected becomes the current version. The previous current version becomes the previous version in the list.

#### Notes:

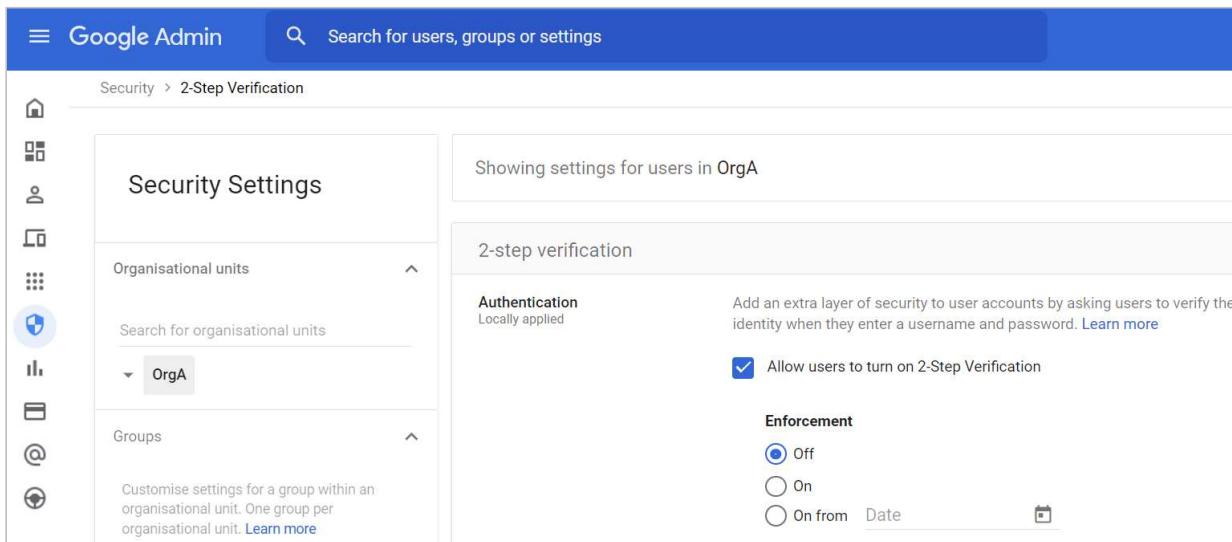
- If you sign in with a personal Microsoft account, you can retrieve the last 25 versions. If you sign in with a work or school account, the number of versions will depend on your [library configuration](#).
- If you're using OneDrive as part of SharePoint Server, your administrator may have turned off document versioning. For more information about SharePoint versioning settings (which also apply to OneDrive for work or school) see [Enable and configure versioning for a list or library](#) or [How does versioning work in a list or library?](#)
- If you're signed in to OneDrive with a Microsoft account, items in the recycle bin are automatically deleted 30 days after they're put there. If your recycle bin is full, the oldest items will be automatically deleted after three days. If you're signed in with a work or school account, items in the recycle bin are automatically deleted after 93 days, unless the administrator has changed the setting. See more information about [how long deleted items are kept](#) for work or school accounts.

# Configuration Guide for Singtel Start Digital (Google Workspace)

This quick-start configuration guide is for organisations using Google Workspace (GWS) through Windows devices, without other servers. Some of the settings are to be configured at GWS (“@GWS”), while others are to be configured at the Windows devices (“@Windows Device”). Windows 10 is used as the reference version for the steps and screenshots given.

# Configuration Guide for Singtel Start Digital (GWS)

## 1. Enable Multi-Factor Authentication (MFA) for Administrators (@GWS)



- Sign in to your Google Admin console.
- Sign in using an administrator account.
- From the Admin console Home page, go to Security and then 2-Step Verification.
- On the left, select an organizational unit or exception group.
- Let users turn on 2-Step Verification and use any verification method, but don't require 2-Step Verification yet.
- Check Allow users to turn on 2-Step Verification.
- Select Enforcement > Off.
- Click Save.

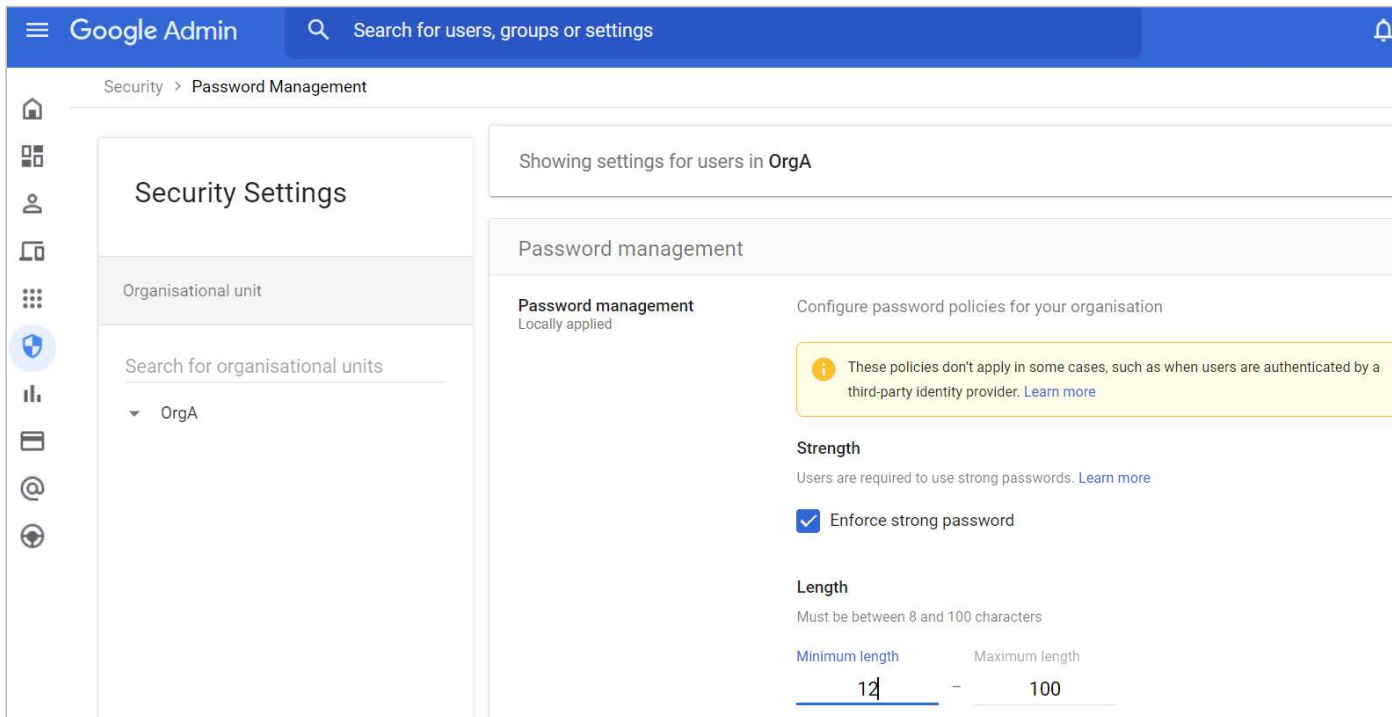
### Additional information:

- You can use the following for MFA:
  - Security keys
  - Google prompt
  - Google Authenticator app
  - Backup codes
  - Text message or phone call
- More Information can be found under this [link here](#).
- Google Workspace security checklist can be found under this [link here](#).



# Configuration Guide for Singtel Start Digital (GWS)

## 2. Strong password settings (@GWS)



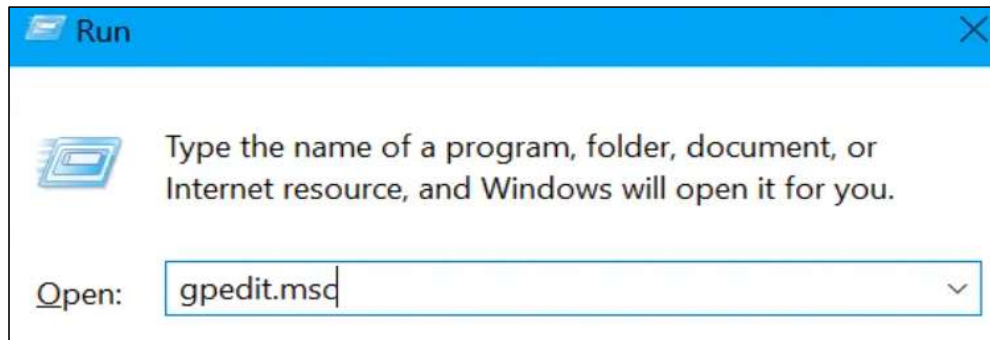
- a. Under Security > Password Management
- b. Configure the minimum to 12 characters

### Additional information:

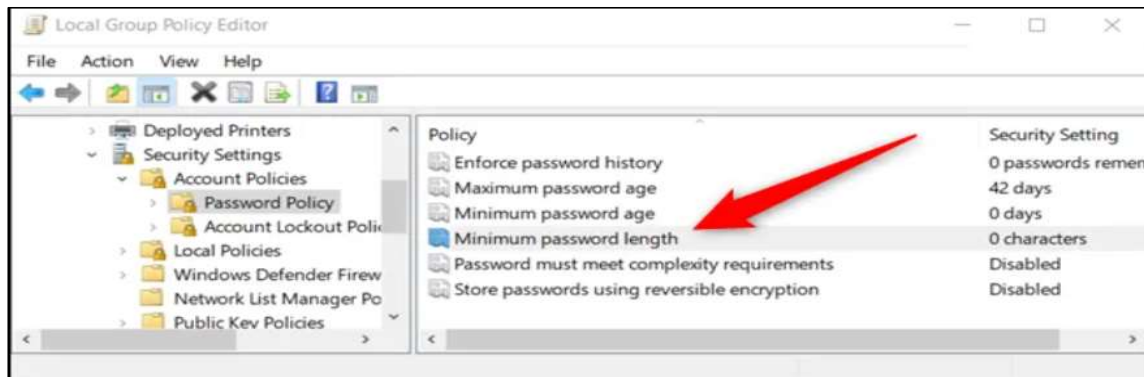
- Enforce a password history policy to ensure that employees do not reuse their previous passwords.
- Encourage users to use passphrases such as “Iwant2l@se10kg”, which may be long and complex, yet easy to remember.
- Discourage users from using the same passwords across different systems.

## Configuration Guide for Singtel Start Digital (GWS)

### 2. Strong password settings (@Windows device)



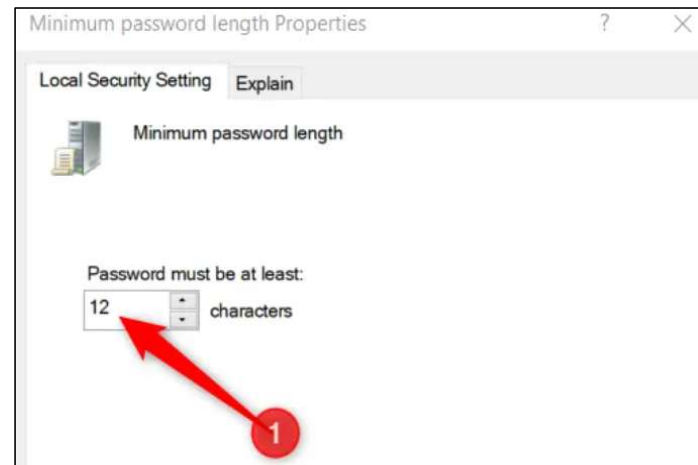
- a. Launch the group policy editor by pressing Windows+R.
- b. Type "gpedit.msc" and press Enter.



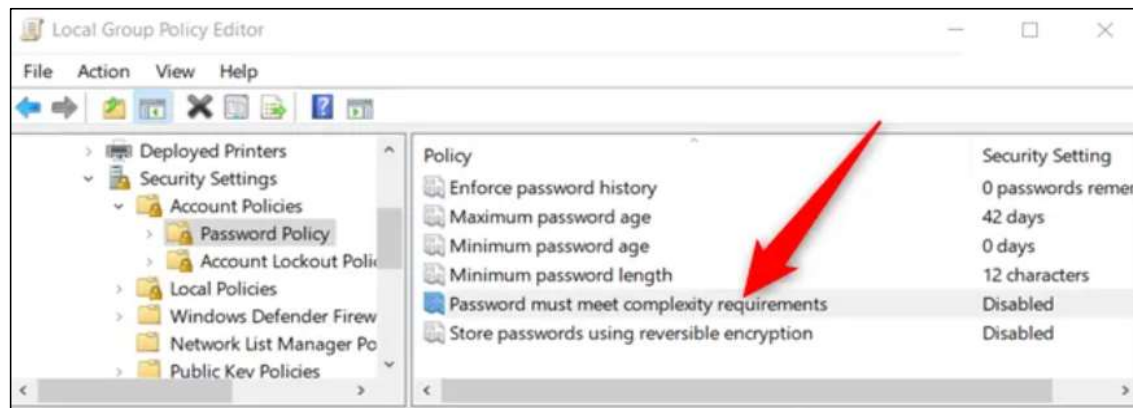
- c. Navigate to Computer configuration > Windows settings > Security settings > Account policies > Password policy.

## Configuration Guide for Singtel Start Digital (GWS)

### 2. Strong password settings (@Windows device)



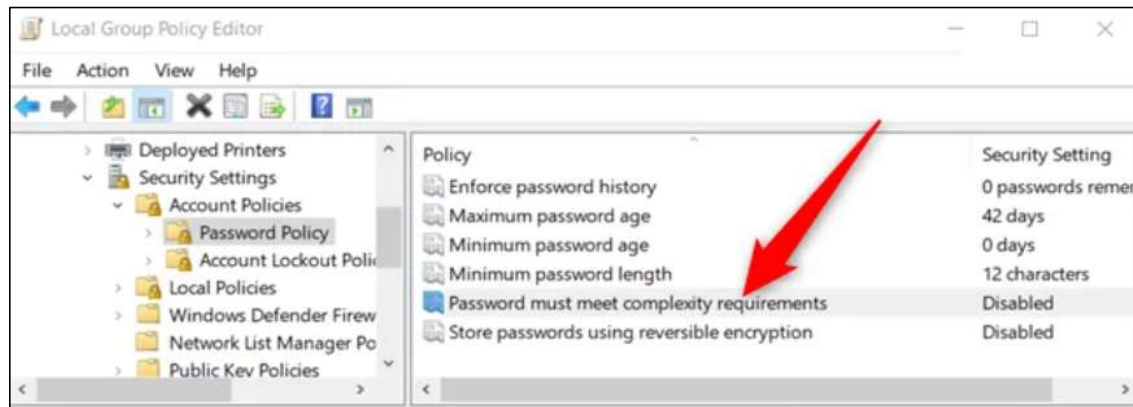
- d. Set the minimum password length to 12 characters.



- e. Enable password complexity requirements, to facilitate users in creating a secure password
- f. Restart your computer after making the policy changes.

## Configuration Guide for Singtel Start Digital (GWS)

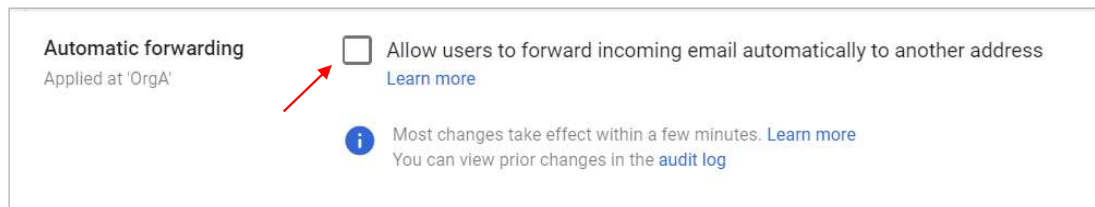
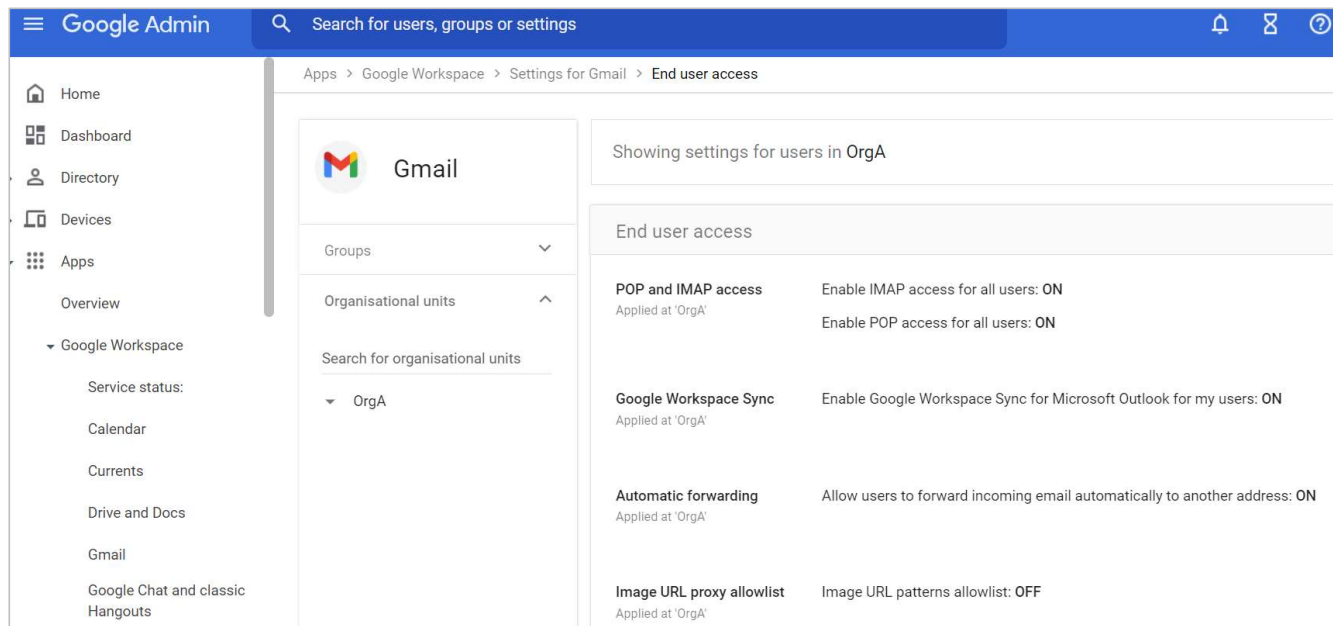
### 2. Strong password settings (@Windows device)



- g. Setting this to enabled means that Windows passwords
- do not contain the user account name or full name
  - be at least 6 characters in length and contain characters from at least 3 of the 4 following categories:
    - uppercase English letters (A-Z),
    - lowercase English letters (a-z),
    - base 10 digits (0-9), and
    - non-alphabetic characters (such as \$, !, %).
- h. Restart your computer after making the above policy changes.

## Configuration Guide for Singtel Start Digital (GWS)

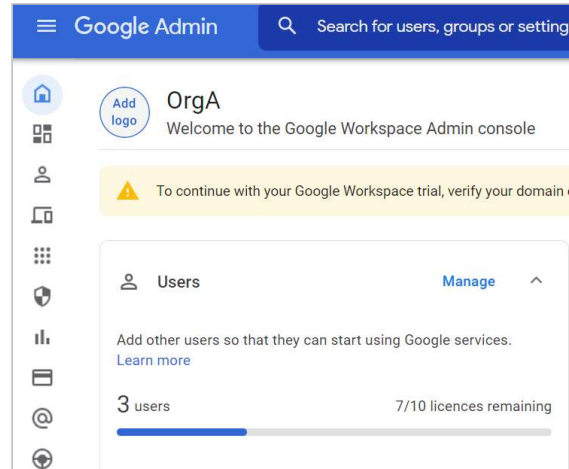
### 3. Disable Email Autoforwarding (@GWS)



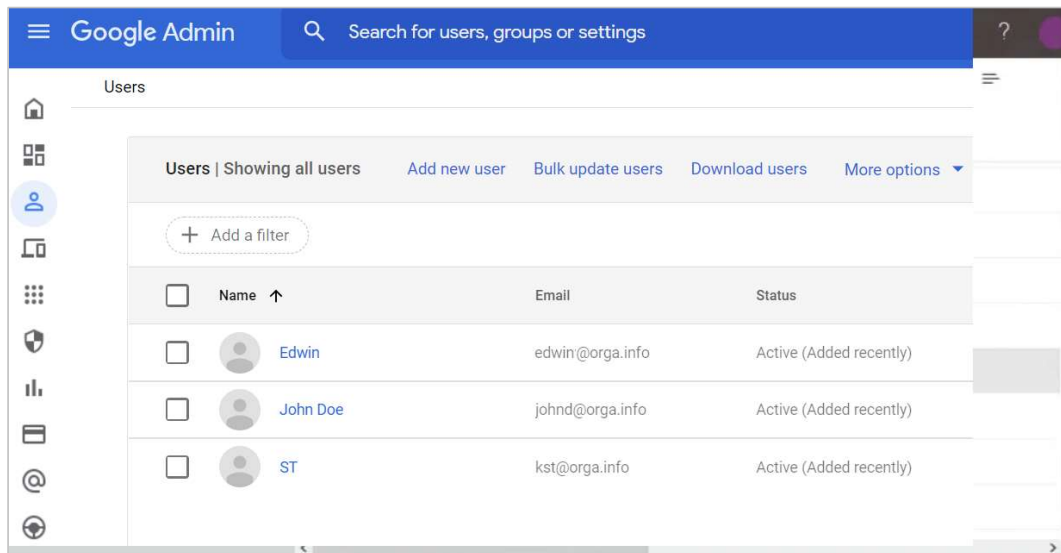
- Go to Apps> Google Workspace> Settings for Gmail> End user access
- Disable mail forwarding feature (i.e. if user is handling sensitive personal data in his/her daily work)
- Click on the pencil icon to edit.
- Uncheck the checkbox at the Automatic Forwarding section.

## Configuration Guide for Singtel Start Digital (GWS)

### 4. Review of User Accounts (@GWS)



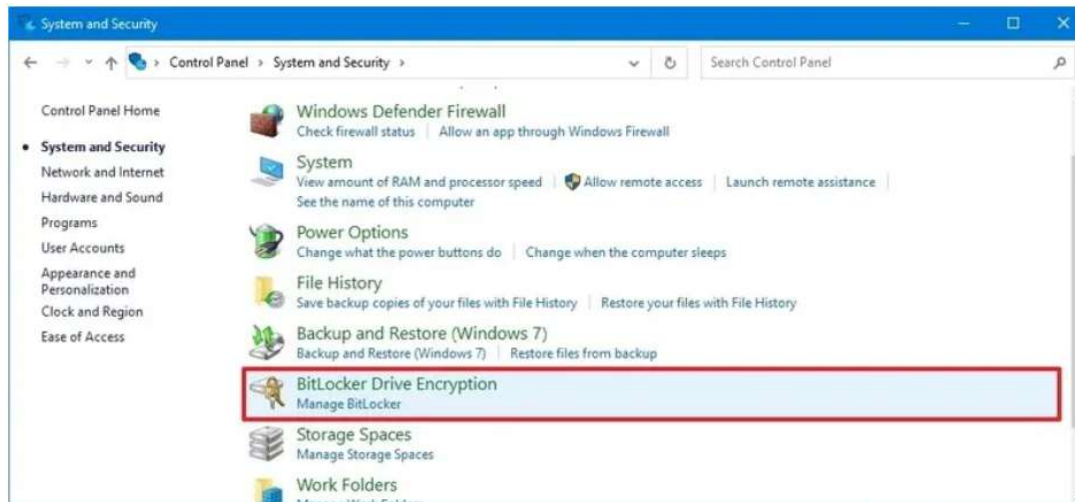
a. From the Google Admin Page, under Users > Manage



b. Regularly conduct periodic review of user accounts to ensure that unused accounts are removed.

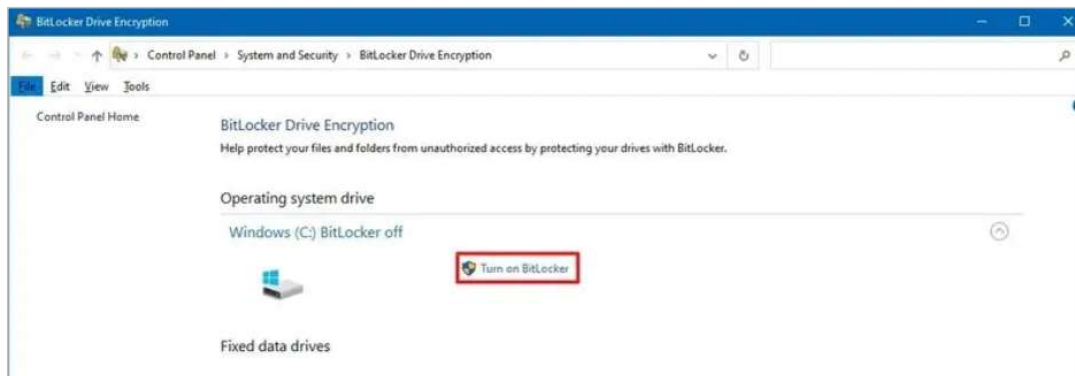
## Configuration Guide for Singtel Start Digital (GWS)

### 6. Turn on BitLocker disk encryption (@Windows device)



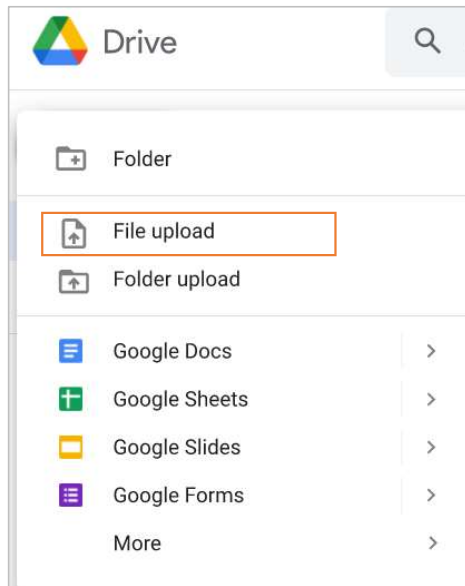
Note: For Windows 10, BitLocker is available on the Pro and Enterprise editions only.

- a. Open Start.
- b. Search for Control Panel and click the top result to open the app.
- c. Click on System and Security.
- d. Click on BitLocker Drive Encryption.
- e. Under the "Operating system drive" section, click the Turn on BitLocker option.



## Configuration Guide for Singtel Start Digital (GWS)

### 7. Manual Backup of Local Files (from Windows device to GWS)

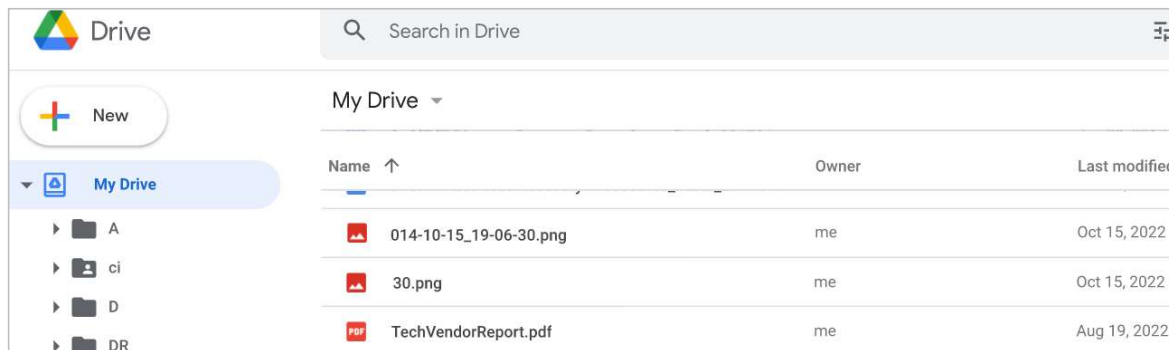


#### To backup from a local device to Google Drive:

- a. Zip the local the local drive/folder/file that you wish to backup.
- b. Assign a password to the zipped file if necessary.
- c. At Google Drive, navigate to the target folder for the backup file.
- d. Click on the **File Upload** option in Google Drive.
- e. Select the file/zipped file from the previous step.

#### To restore from Google Drive to a local device:

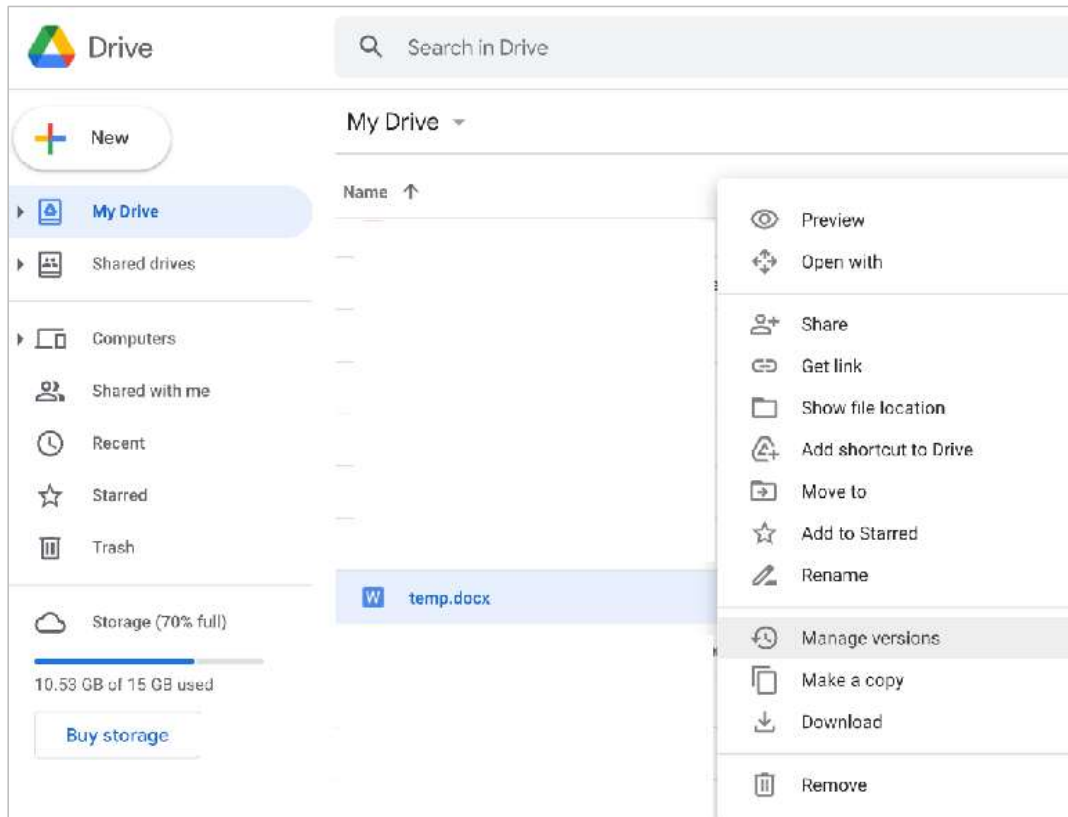
- a. Select the backed up (zip file) at Google Drive.
- b. Click on **Download**.
- c. Unzip the file if necessary and key in the password if necessary.
- d. Copy the file/folders to the target destination on your local device.





## Configuration Guide for Singtel Start Digital (GWS)

### 8. Backup of Cloud Files (@GWS)



#### To restore a selected file

- In Drive, click the file and at the top right, click *More > Manage versions*.
- To revert to an earlier version, find the version of the file, and click *Open*.