Updated 31 Mar 2022

# 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.

The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The PDPC and its members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

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

multi-factor authentication users service settings						
Before you begin, take a look at the multi-factor auth deployment guide.           View:         Sign-in allowed users <ul></ul>						
	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS			
	WSOMP	wsopm-4499@pm.onmicrosott.com Disabled				
	Off365 o365team@pm.onmicrosoff.com Disabled					
	Ram	sreeram@pm.onmicrosotf.com Disabled				
	Disabled					

- a. Go to Users > Service Settings
- b. Under the Services Settings, enable MFA functionality for the selected administrator.
- c. 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.

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

Property	Requirements
Characters allowed	<pre>• A - Z • a - z • 0 - 9 • @ # \$ % ^ &amp; *! + = [] { }   \:', .?/`~"();</pre>
Characters not allowed	• Unicode characters • Spaces • Cannot contain a dot character "." immediately preceding the "@" symbol"
Password restrictions	<ul> <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:</li> <li>Lowercase characters</li> <li>Uppercase characters</li> <li>Numbers (0-9)</li> <li>Symbols</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.

2. Strong password settings (@Windows device)

🖾 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	gpedit.msd	~

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



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

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.

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.

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

Settings	Layout	Forwarding
	Compose and reply Attachments Rules	You can forward your email to another account. <ul> <li>Enable forwarding</li> </ul> Forward my email to:
<ul> <li>Calendar</li> <li>R<sup>R</sup> People</li> <li>View quick settings</li> </ul>	Junk email Customize actions Sync email Message handling	Enter an email address
	Forwarding Automatic replies Subscriptions	

- 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

# 4. Review of User Accounts (@M365)

	Microsoft 365 admin center				0 🕸 ? 🛑
=		Add a user 🗄 User templates \cdots			¶Filter = ^
ଜ	Home	Display name 🏌		Username	
8	Users ^	R11		R11@01.onmicrosoft.	com
1	Active users	R12		R12@01.onmicrosoft.	com
	Contacts	<b>P14</b>		: P14@01 comissoroft	
	Guest users	R14		: KI4@01.onmicrosoft.	com
	Deleted users	R15		R15@01.onmicrosoft.	com
RR	Groups 🗸 🗸	R16	Q	R16@01.onmicrosoft.	com
Pa	Roles	R17		Anage product licenses	osoft.com
喝	Resources 🗸	R18		が Manage groups ■ Edit username	osoft.com
	Billing ~	R19		Delete user	osoft.com
		٢			>

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

5. Configure Folder Permissions (@M365 OneDrive)

+ New Y T Upload Y	G Sync 🥙 Automate Y	Send link	
My files		People you specify can edit >	
🗋 Name ~	Modified ~	To: Name, group or email	$\mathcal{O}$ $\sim$
C Ed Ed	January 19	$\Theta$ Please enter a name or an email address.	🖉 Can edit
الآن التحقيق ال التحقيق التحقيق ا	About a minute ago A few seconds ago	Message	Make any changes         Make any changes         Can view         Cannot make changes
			🐯 Link settings



#### To share a file/folder

- a. Select the file you want to share, and then select Share.
- b. 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

- a. Select Shared.
- b. Select a folder or file, and then select the **Information** icon.
- c. 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.



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



BitLocker Drive Encryption			- 0
🔶 🖃 🕆 🛧 🚱 Contro	I Panel + System and Security + BitLocker Drive Encryption	v 8	Ĵ.
ile Edit View Jools			
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protect		
	Operating system drive		
	Windows (C:) BitLocker off	I	0
	Fixed data drives		

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.

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





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

- a. Zip the local the local drive/folder/file that you wish to backup. Assign a password to the zipped file if necessary.
- b. At OneDrive, navigate to the target folder for the backup file.
- c. 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:

- a. Select the backed up (zip file) at M365 OneDrive.
- 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.

#### 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.

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

# To restore your entire OneDrive

Restore OneDrive to a previous time	4. Use the activity chart and activity feed to review the recent activities that you want to undo.  Restore your OneDrive	<ol> <li>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.</li> </ol>
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.	Reave Cancel	Note: Before you select <b>Restore</b> , 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.
1. Go to the OneDrive website. (Make sure you're signed in with the correct account.)		6. When you're reach, to restore your OpeDrive select <b>Pestore</b> . This action will undo all the activities you
2. If you're signed in with:		selected.
A personal account with a Microsoft 365 subscription, at the top of the page, select Settings 4 >	0	Your OneDrive will be restored to the state it was in before the first activity you selected.
Options, and then select Restore your OneDrive from the left navigation.	∧ Today - 5/10/2018 (56)	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.
<ul> <li>A work or school account, select Settings &gt; Restore your OneDrive.</li> </ul>		
Note: The Restore your OneDrive option isn't available in the classic experience of OneDrive for work		Limitations and troubleshooting
	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, it your OneDrive was inferred by makayare, your can hook for when it happened the state of the state of th	<ul> <li>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 where the setting of the setting o</li></ul>
3. On the Restore page, select a date from the dropdown list—such as Yesterday—or select Custom date	The activity feed shows individual file and folder operations in reverse chronological order. You can scroll	features.
and time. If you're restoring your files after automatic ransomware detection, a suggested restore date will be filled in for you.	down to see previous days, or move the slider below the daily activity chart to quickly move to a specific day.	<ul> <li>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</li> </ul>
Restore your OneDrive	Tip: Use the expand and collapse arrow next to each day in the activity feed to show or hide activities for that day.	view and restore those deleted items.
		<ul> <li>Albums are not restored.</li> </ul>
Select a date 🗡	<ol> <li>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.</li> </ol>	<ul> <li>If you upload a file or folder that you deleted, Files Restore will skip the restore operation for that file or folder.</li> </ul>
Yesterday One week ago Three weeks ago	Note: Before you select <b>Restore</b> , 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.	<ul> <li>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 trubleshoot any issues that may occur.</li> </ul>

Source: https://support.microsoft.com/en-us/office/restore-your-onedrive-fa231298-759d-41cf-bcd0-25ac53eb8a15

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

# To restore a selected file

Restore a previous version of a file	Version History			X 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
	Version Modified Date	Modified By	Size	you want and click <b>Restore</b> .
OneDrive for Business, SharePoint Server Subscription Edition, More	2.0 Jul 23, 2019 1.0 Jul 23, 2019	Nestar Wilke Jerri Frye	26.9 KB 34.4 KB	Car maintenance Open Edit
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.	Restore Open F Delete	Ja Version		New Print Share View online
Tip: You can also View previous versions of Office files in Office apps.	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 <b>Restore</b> .			
1. Sign in to OneDrive with your personal Microsoft account or your work or school account.	Version Histo	гу		previous version in the list.
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 <b>Version history</b> .	Delete All Versions		faditied By	<ul> <li>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.</li> </ul>
Note: In Classic view, select the document, then at the top, select More > Version History.	3.0 View 2.0 Restore		Jerri Frye Jerri Frye	<ul> <li>If you're baing Onebried as pair of sharehold serving you administration may have buried on bochment versioning. For more information about Sharehold 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?</li> </ul>
<ol> <li>In the Version History pane, do one of the following:</li> <li>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.</li> </ol>	1.0 Delete	<ul> <li>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.</li> </ul>		

Source: https://support.microsoft.com/en-us/office/restore-a-previous-version-of-a-file-stored-in-onedrive-159cad6d-d76e-4981-88ef-de6e96c93893

Updated 31 Mar 2022

# 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.

The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The PDPC and its members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

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

	Google Admin Q Search 1	or user	s, groups or settings			
Â	Security > 2-Step Verification					
₽ ₽ 0	Security Settings		Showing settings for u	sers in OrgA		
.⊂⊡ ::::	Organisational units		2-step verification			
0	Search for organisational units		Authentication Locally applied	Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. Learn more		
ılı	- OrgA		Allow users to turn on 2-Step Verification			
@	Groups	^		Enforcement <ul> <li>Off</li> </ul>		
۲	Customise settings for a group within an organisational unit. One group per organisational unit. Learn more			On On from Date		

# 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.

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

#### 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.

2. Strong password settings (@Windows device)

🖾 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	gpedit.msd	~

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



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

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.

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.

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

Ξ	Google Admin Q	Search for users, groups or setting	5	Ó Z Ø
â	Home	Apps > Google Workspace > Settings f	or Gmail > End user access	
	Dashboard		Showing settings for use	ers in OrgA
ő	Directory	Gmail		
	Devices		End user access	
· III	Apps	Groups		
	Overview	Organisational units	POP and IMAP access Applied at 'OrgA'	Enable IMAP access for all users: ON
	Google Workspace	Search for organisational units		Enable POP access for all users. UN
	Service status:	✓ OrgA	Google Workspace Sync	Enable Google Workspace Sync for Microsoft Outlook for my users: ON
	Calendar		Applied at 'OrgA'	
	Currents			
	Drive and Docs		Automatic forwarding Applied at 'OrgA'	Allow users to forward incoming email automatically to another address: <b>ON</b>
	Gmail			
	Google Chat and classic Hangouts		Image URL proxy allowlist Applied at 'OrgA'	Image URL patterns allowlist: OFF

- a. 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)

- Automatic forwarding
   Allow users to forward incoming email automatically to another address

   Applied at 'OrgA'
   Learn more

   Image: State of the state of
- c. Click on the pencil icon to edit.
- d. Uncheck the checkbox at the Automatic Forwarding section.

4. Review of User Accounts (@GWS)



=	Google Admin	Q Search f	or users, grou	ips or settings			?
â	Users						=
	Users   Showing a	all users A	dd new user	Bulk update users	Download users	More options 💌	
	+ Add a filter						
	□ Name ↑			Email	Status		
0	Edu	win		edwin'@orga.info	Active (Addec	recently)	
հ	lot (	hn Doe		johnd@orga.info	Active (Addec	recently)	
@	ST			kst@orga.info	Active (Addec	I recently)	
۲		5					5

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

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

6. Turn on Bitlocker disk encryption (@Windows device)



BitLocker Drive Encryption			- 0
Contro	5		
ile Edit Yiew Jools			
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protectin		
	Operating system drive		
	Windows (C:) BitLocker off		0
	Fixed data drives		

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.

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

4	Drive	٩
Ē+	Folder	
r A	File upload	]
<b>^</b>	Folder upload	
F	Google Docs	>
<b>H</b>	Google Sheets	>
	Google Slides	>
=	Google Forms	>
	More	>

#### 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.

🛆 Drive	Q Search in Drive		丰
- New	My Drive 👻		
▼ △ My Drive	Name 个	Owner	Last modified
• 🖿 A	014-10-15_19-06-30.png	me	Oct 15, 2022 I
ci	🗾 30.png	me	Oct 15, 2022 r
D DR	TechVendorReport.pdf	me	Aug 19, 2022

#### 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*.