Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Business Continuity in a Box

Guidance: Continuity of Communications

Content Complexity

SIMPLE ●○○

cyber.gov.au

Contents

Disclaimer

The information herein is being provided "as is" for information purposes only. The authors do not endorse or favour any commercial entity, product, company, or service, including any entities, products, or services linked or otherwise referenced within this document.

Introduction

Purpose

In modern organisations, email is the most common function for internal and external communications. In the case of a systems outage during a cyber incident, email (and other communications) functionality is often lost. To ensure business continuity and coordinate an effective response to the incident, organisations must rapidly re-establish basic internal and external communications.

Continuity of Communications focuses on keeping communications flowing during a cyber incident by assisting organisations to establish basic communications functions quickly and securely. It provides guidance to organisations on how to deploy a Microsoft 365 tenant, create a 'catch-all' email inbox, and manually configure Exchange Online security features when core systems, such as user directory and email, become unusable or unavailable.

> ⓘ **NOTE:** We do not recommend the Continuity of Communications package for existing Microsoft 365 of Google Workspace customers. In the event existing customers are impacted by a cyber incident, we recommend contacting the relevant Microsoft or Google incident response service available to them as part of their subscription. Doing so may provide for a more tailored solution than is offered in this guidance.

Overview

Business Continuity in a Box – developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) with contributions from the United States Cybersecurity and Infrastructure Security Agency (CISA) – is an interim solution to be deployed by either the organisation or its Managed Service Provider (MSP). Successful implementation of Continuity of Communications entails provisioning and configuring of a Microsoft 365 Business Standard tenant and requires a basic level of computing knowledge.

The implementation steps within this guidance will enable an organisation to provision a trial Microsoft 365 Business Standard tenant which includes Microsoft Entra ID (formerly Azure Active Directory), Exchange Online, and associated security services. The guidance also steps through the establishment of a 'catch-all' email inbox, and how to manually configure Microsoft 365 security features. These are established as priorities to ensure critical communications sent to an organisation can continue to be received while other communications systems are unavailable.

Once the Microsoft 365 tenant has been provisioned, the guidance steps through how to deploy the accompanying automation tool – preconfigured system configurations via PowerShell scripts.

The tool automates the configuration of the Microsoft 365 tenant by:

- Applying settings to the Microsoft 365 tenant to secure the organisation and its users.
- Creating a temporary 'catch-all' mailbox to ensure all emails sent to the organisation's email address are captured.
- Creating an emergency account which should be used in situations where existing administrators are unable to log into their accounts.Users will then be guided through how to manually configure Microsoft 365 security features.

The configuration provides a secure foundation for organisations to expand on as needed. This may include enabling additional Microsoft 365 services or provisioning additional cloud capabilities to enable restoration of other business services such as financial management or human resource management (see: Business Continuity in a Box - Guidance: Continuity of Applications).

What is Microsoft 365?

Microsoft 365 is a suite of cloud-based productivity tools and services. It includes several online services and capabilities required for business activities. Access to these services and capabilities is dependent on the licence type. This guidance focuses on the Microsoft 365 Business Standard plan. Microsoft offers a range of other plans depending on an organisation's requirements, size and type. For a comprehensive comparison of all Microsoft 365 plans see:

- Microsoft 365 and Office 365 Plan Options at learn.microsoft.com/en-au/office365/servicedescriptions/office-365-platform-service-description/office-365-plan-options

The Continuity of Communications package uses the following Microsoft 365 services:

- **Microsoft Entra ID** provides centralised Identity and Access Management capabilities for an organisation to secure systems, identities, and data.
- **Exchange Online** provides an organisation with enterprise email and calendar capabilities. Access to Exchange Online can be via a traditional desktop email client or via Outlook Web Access through the user's internet browser.
- **Microsoft Defender** is an integrated security solution across the Microsoft 365 suite, which offers protection against phishing emails, malware and other threats across Office 365 applications, Exchange Online, SharePoint Online and managed devices.

The following Microsoft 365 services are out of scope of the Continuity of Communications package:

- **Office Applications** are the online versions of the equivalent desktop applications. These include Word, Excel, PowerPoint and OneNote.
- **SharePoint Online** and **OneDrive for Business** offer document management and collaboration capabilities.
- **Teams** provides a platform for unified communications and collaboration.

How to use this document

This document is divided into five consecutive stages. It is recommended that the reader reviews the document in its entirety before commencing Stage 1.

This document uses the below callout boxes to highlight various information.

> **NOTE:** Information to assist the reader in understanding the document, including justification for a particular decision, key considerations, and other important details.

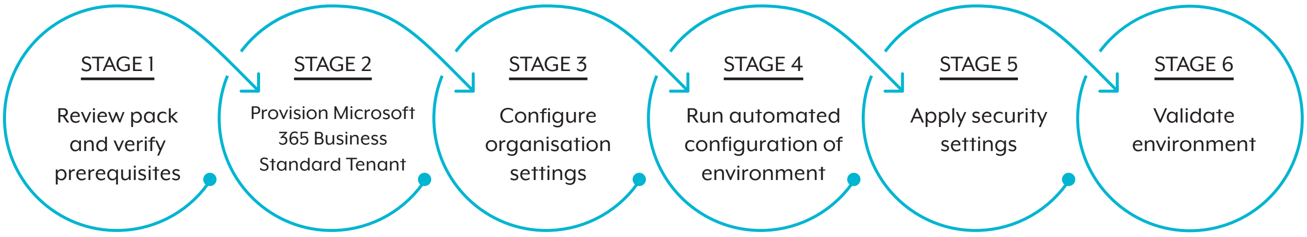
> **WARNING:** Highlights information that requires careful attention, such as implementation of a change or configuration that may impact users or the organisation's information technology operations.

Guidance

Stage 1: Review Pack and Verify Prerequisites

This document forms one component of the Continuity of Communications implementation guidance. An additional repository containing the automation tool and associated configuration files is also required to make full use of the guidance. Before continuing with this guidance, review all the content in this document, ensuring to prepare and verify additional prerequisites for each stage.

This document is divided into six consecutive stages. The term 'operator' refers to the person responsible for implementation of the Business Continuity in a Box solution within their organisation. The below diagram represents the staged process and the prerequisites for each stage.


STAGE 1
Review pack and verify prerequisites
STAGE 2
Provision Microsoft 365 Business Standard Tenant
STAGE 3
Configure organisation settings
STAGE 4
Run automated configuration of environment
STAGE 5
Apply security settings
STAGE 6
Validate environment

Computer

This guidance assumes the operator will use a Microsoft Windows-based personal computer (PC) running Windows 10 or Windows 11 using the Microsoft Edge browser to perform the steps. Instructions within this guidance can be completed using alternative solutions. However, the operator will need to interpret the steps for the specific operating system and browser.

Business Continuity in a Box is designed for use during a cyber incident that has affected access to or trust of an organisation's systems. The selected PC must therefore be independent from the organisation's IT environment, including network and Internet connection.

The automation tool within this guidance uses the command-line shell scripting language and configuration management framework called PowerShell. Configuration of the automation tool is done via supplied configuration files which have the '.config' file extension.

Phone

During the setup process, Microsoft will either text or call a verification code to a phone. Voice over internet protocol (VOIP) systems generally do not allow the receiving of the verification phone call. Microsoft recommends not using a VOIP phone number for the verification process.

Email

During the setup process, Microsoft will email an account confirmation to the email address provided during the setup process. To receive the confirmation email, the operator must have access to the email account.

NOTE: Whilst ordinarily it would be preferred to avoid use of a personal email account, the nature of the cyber incident may restrict alternatives. If the operator does not have access to an appropriate email account, the operator could choose to sign up for a new email account using providers such as Microsoft Outlook or Google Mail.

WARNING: Do not use an email address associated with the affected organisation.

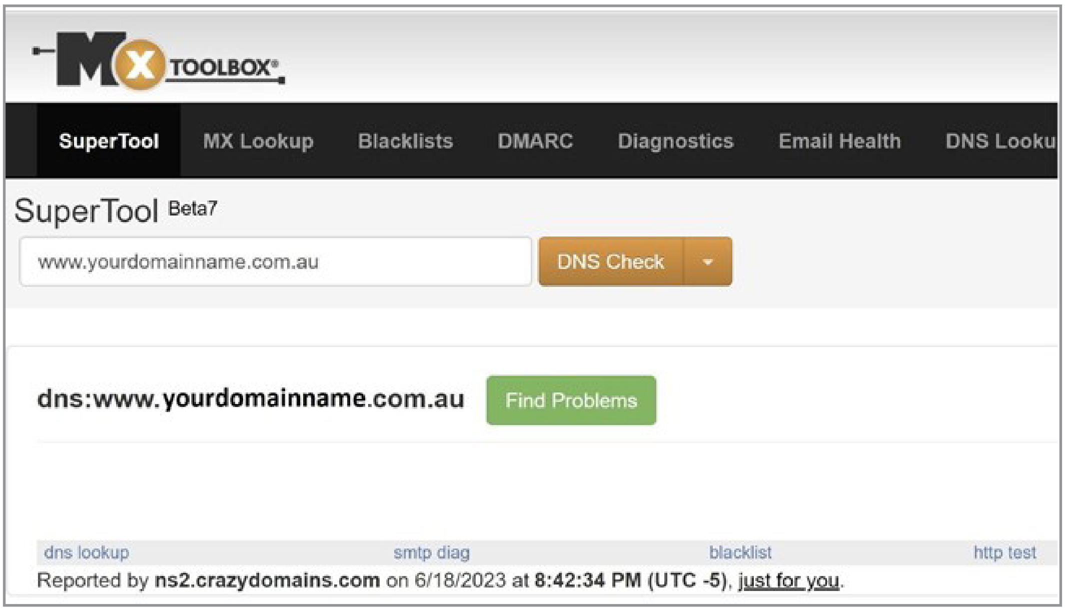
Organisation Information

Continuity of Communications will provision and configure Exchange Online to enable an organisation to capture all incoming emails to their existing domain name. To redirect emails to Exchange Online, the operator will require access to the organisation's public Domain Name Service (DNS) hosting provider in order to modify the text (TXT) and mail exchange (MX) records.

NOTE: Given the scenario in which Business Continuity in a Box should be used, we do not recommend creating new domain records. To receive email messages sent to the organisation's existing email addresses, only the relevant domain(s) for those email addresses should be modified to update the TXT and MX records.

WARNING: Incorrectly configuring, adding or removing an organisation's DNS records can result in further impacts to the availability of a system.

Configuration steps for modifying DNS records vary depending on the hosting provider. The organisation will be required to supply the operator with the appropriate credentials to access the hosting platform. If the organisation cannot provide the necessary credentials, they must contact their hosting provider prior to proceeding further. If the hosting provider cannot be located, a DNS lookup using a free service such as www.mxtoolbox.com depicted in the image below may assist.



SuperTool Beta7

www.yourdomainname.com.au

dns:www.yourdomainname.com.au

Reported by **ns2.crazydomains.com** on 6/18/2023 at **8:42:34 PM (UTC -5)**, just for you.

Financial Delegation

The Microsoft 365 Business Standard plan is valid as a free trial for 30 days. Registration requires an organisation to provide valid credit card credentials. Microsoft will automatically bill the credit card after the trial period if the organisation does not cancel the subscription beforehand. For full terms and conditions regarding Microsoft billing, please refer to:

- Microsoft Business Subscriptions and Billing Documentation at learn.microsoft.com/en-au/microsoft-365/commerce

Stage 2: Provision Microsoft 365 Business Standard Tenant

Overview

This stage walks through the process for setting up a trial Microsoft 365 Business Standard tenant and redirecting emails to the new tenant.

> ⓘ
>
> **NOTE:**
> This stage of the guidance provisions a trial Microsoft 365 Business Standard tenant.
>
> The trial provides up to 25 user licences for 30 days.
>
> Microsoft allows a one-time extension of the trial period for an additional 30 days within 15 days of the trial expiry date.
>
> A paid Microsoft 365 Business Standard plan allows for the provision of up to 300 user licences.
>
> If the 25-user licence limit offered by the trial plan is insufficient for an organisation's needs, the organisation can, at any time, convert the trial to a paid subscription to gain access to the full user licence allowance.

Stage Prerequisites

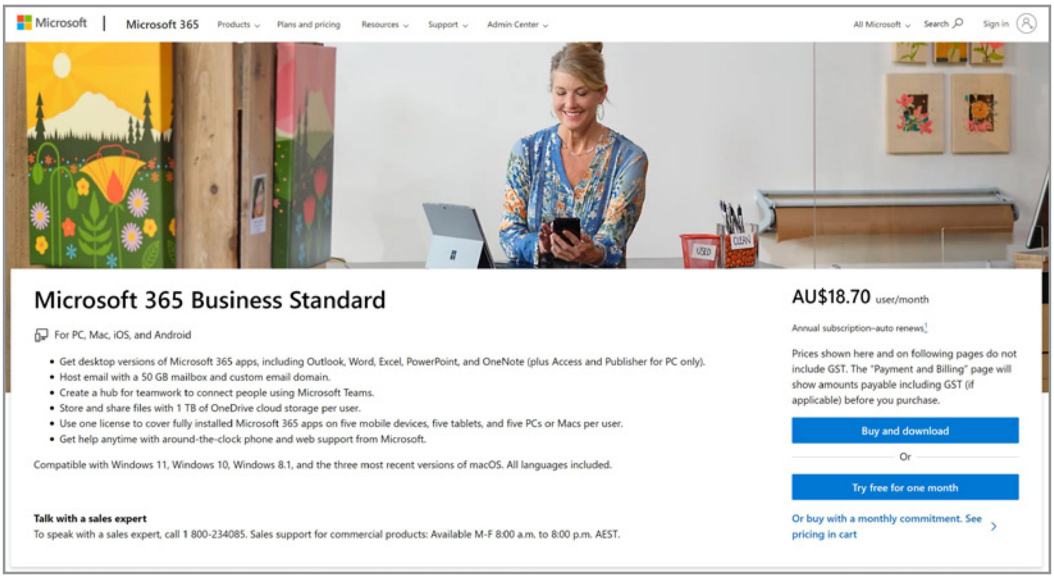
The operator completing this stage will require:

1. PC with a connection to the Internet
2. Up-to-date web browser
3. Valid email address to use during the registration process (must not be associated with or hosted on the network experiencing disruption)
4. Phone that can receive a phone call or a SMS verification code (non-VOIP)
5. Valid credit card

Process

1. Navigate to the Microsoft 365 Business Standard Sales Portal at microsoft.com/en-au/microsoft-365/business/microsoft-365-business-standard

2. Select **'Try free for one month'.**



Microsoft 365 Business Standard

For PC, Mac, iOS, and Android

- Get desktop versions of Microsoft 365 apps, including Outlook, Word, Excel, PowerPoint, and OneNote (plus Access and Publisher for PC only).
- Host email with a 50 GB mailbox and custom email domain.
- Create a hub for teamwork to connect people using Microsoft Teams.
- Store and share files with 1 TB of OneDrive cloud storage per user.
- Use one license to cover fully installed Microsoft 365 apps on five mobile devices, five tablets, and five PCs or Macs per user.
- Get help anytime with around-the-clock phone and web support from Microsoft.

Compatible with Windows 11, Windows 10, Windows 8.1, and the three most recent versions of macOS. All languages included.

Talk with a sales expert
To speak with a sales expert, call 1 800-234085. Sales support for commercial products: Available M-F 8:00 a.m. to 8:00 p.m. AEST.

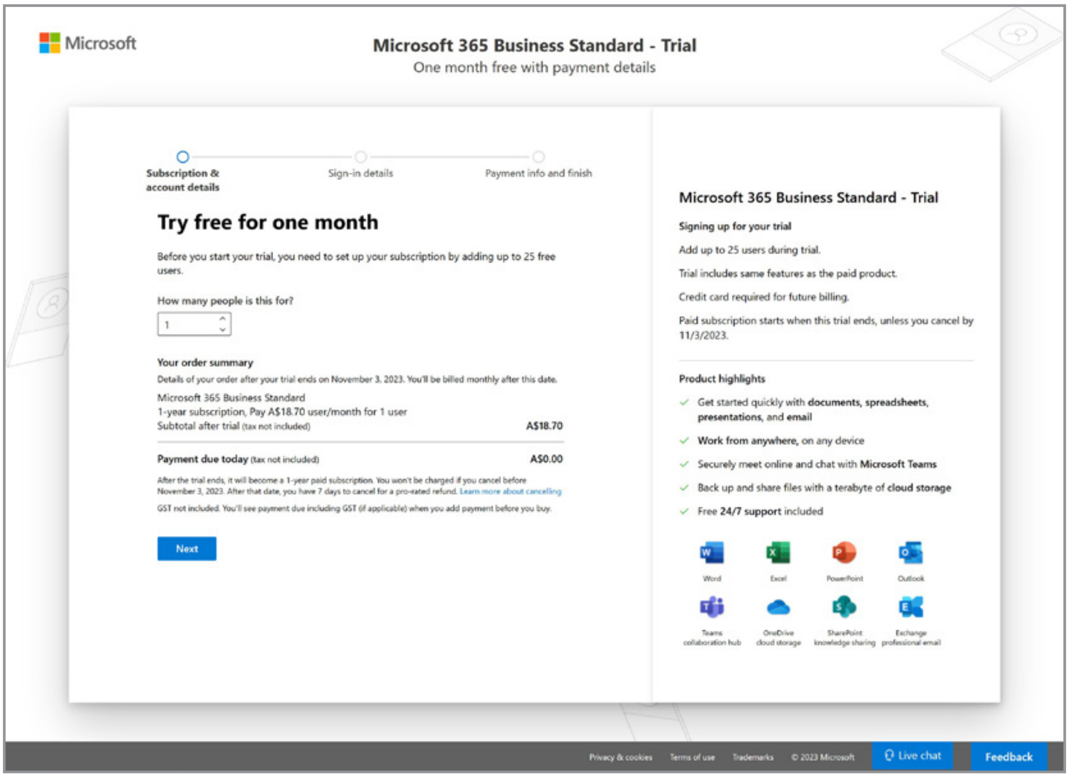
AU$18.70 user/month

Annual subscription–auto renews[1]

Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

3. In the next screen, ensure that only one person is selected and click '**Next**'.

NOTE: Selecting one user at this stage does not restrict the number of users that an organisation can add to the tenant. The trial allows for an additional 24 users. Selecting one user at this stage will simplify the setup and configuration process until the organisation has configured the remainder of the Microsoft 365 tenant.



Microsoft 365 Business Standard - Trial
One month free with payment details

Try free for one month

Before you start your trial, you need to set up your subscription by adding up to 25 free users.

How many people is this for?
1

Your order summary
Details of your order after your trial ends on November 3, 2023. You'll be billed monthly after this date.

Microsoft 365 Business Standard
1-year subscription, Pay A$18.70 user/month for 1 user
Subtotal after trial (tax not included) A$18.70

Payment due today (tax not included) A$0.00

After the trial ends, it will become a 1-year paid subscription. You won't be charged if you cancel before November 3, 2023. After that date, you have 7 days to cancel for a pro-rated refund. Learn more about cancelling

GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

Microsoft 365 Business Standard - Trial

Signing up for your trial

Add up to 25 users during trial.

Trial includes same features as the paid product.

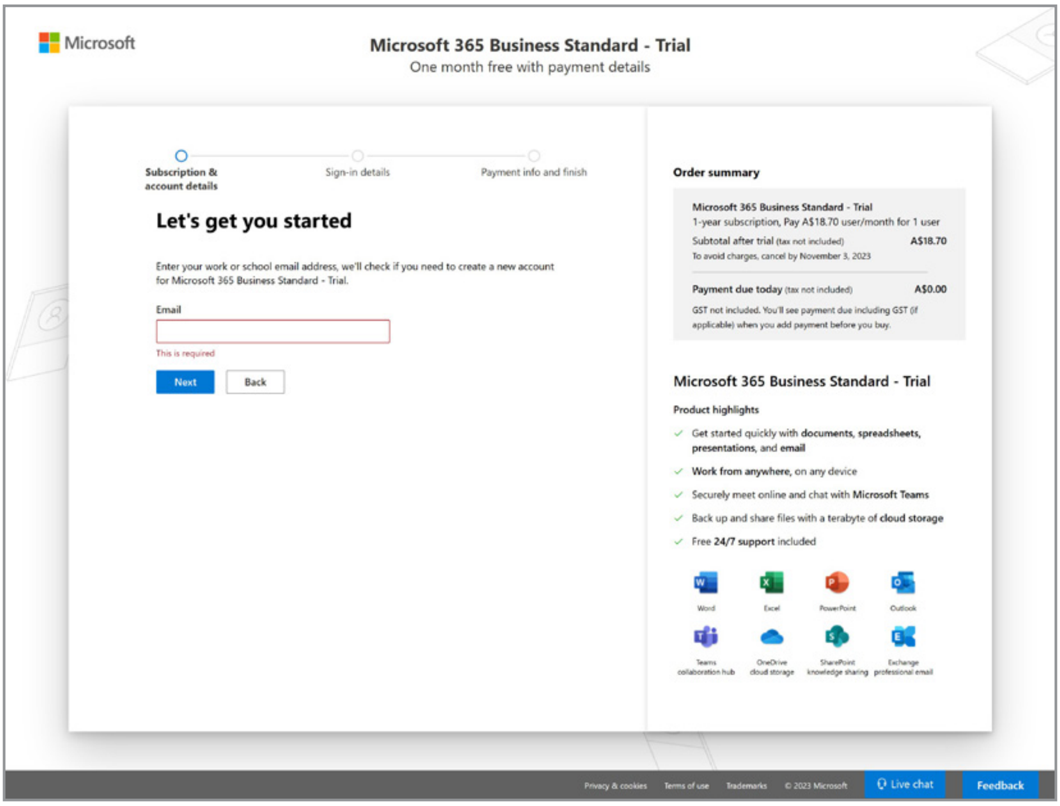
Credit card required for future billing.

Paid subscription starts when this trial ends, unless you cancel by 11/3/2023.

Product highlights

- ✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**
- ✓ **Work from anywhere,** on any device
- ✓ Securely meet online and chat with **Microsoft Teams**
- ✓ Back up and share files with a terabyte of **cloud storage**
- ✓ Free **24/7 support** included

4. In the next screen, enter an email address to use for account verification and click **'Next'.**



Microsoft 365 Business Standard - Trial

One month free with payment details

Let's get you started

Enter your work or school email address, we'll check if you need to create a new account for Microsoft 365 Business Standard - Trial.

Email

This is required

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user

Subtotal after trial (tax not included)	A$18.70
To avoid charges, cancel by November 3, 2023	
Payment due today (tax not included)	A$0.00

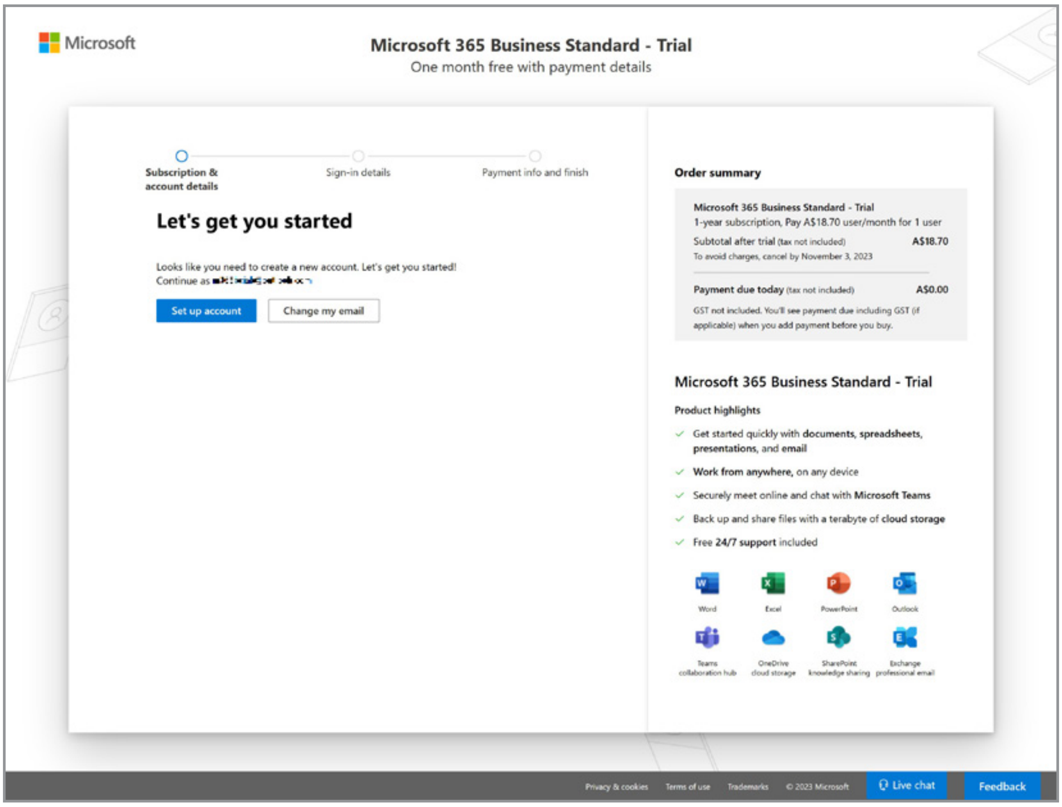
GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with documents, spreadsheets, presentations, and email
- ✓ Work from anywhere, on any device
- ✓ Securely meet online and chat with Microsoft Teams
- ✓ Back up and share files with a terabyte of cloud storage
- ✓ Free 24/7 support included

5. Click **'Set up account'.**



Microsoft 365 Business Standard - Trial

One month free with payment details

Let's get you started

Looks like you need to create a new account. Let's get you started!
Continue as [redacted]

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user

Subtotal after trial (tax not included)	A$18.70
To avoid charges, cancel by November 3, 2023	
Payment due today (tax not included)	A$0.00

GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

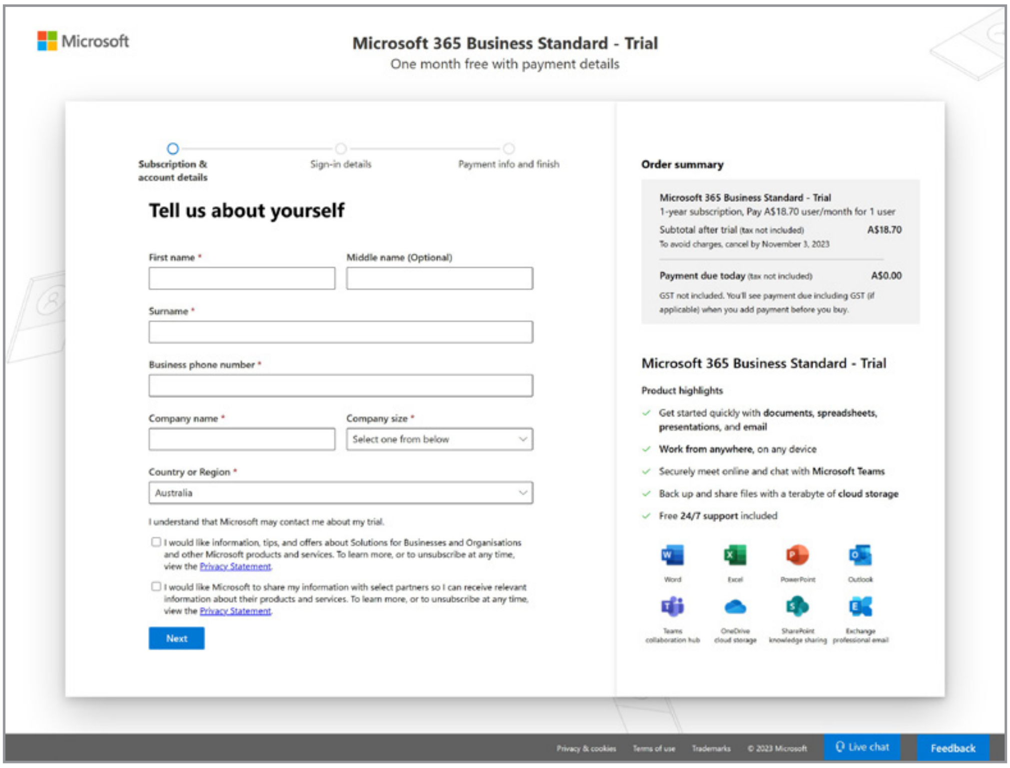
Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with documents, spreadsheets, presentations, and email
- ✓ Work from anywhere, on any device
- ✓ Securely meet online and chat with Microsoft Teams
- ✓ Back up and share files with a terabyte of cloud storage
- ✓ Free 24/7 support included

6. Enter the required information and click '**Next**'.

> **NOTE:** The country or region selected on this screen will determine the data centre region for data storage. Set this entry to the appropriate country or region to meet your data storage requirements.



Microsoft

Microsoft 365 Business Standard - Trial

One month free with payment details

○ **Subscription & account details** — ○ Sign-in details — ○ Payment info and finish

Tell us about yourself

First name *

Middle name (Optional)

Surname *

Business phone number *

Company name *

Company size * Select one from below

Country or Region * Australia

I understand that Microsoft may contact me about my trial.

□ I would like information, tips, and offers about Solutions for Businesses and Organisations and other Microsoft products and services. To learn more, or to unsubscribe at any time, view the Privacy Statement.

□ I would like Microsoft to share my information with select partners so I can receive relevant information about their products and services. To learn more, or to unsubscribe at any time, view the Privacy Statement.

Next

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user

Subtotal after trial (tax not included) A$18.70
To avoid charges, cancel by November 3, 2023

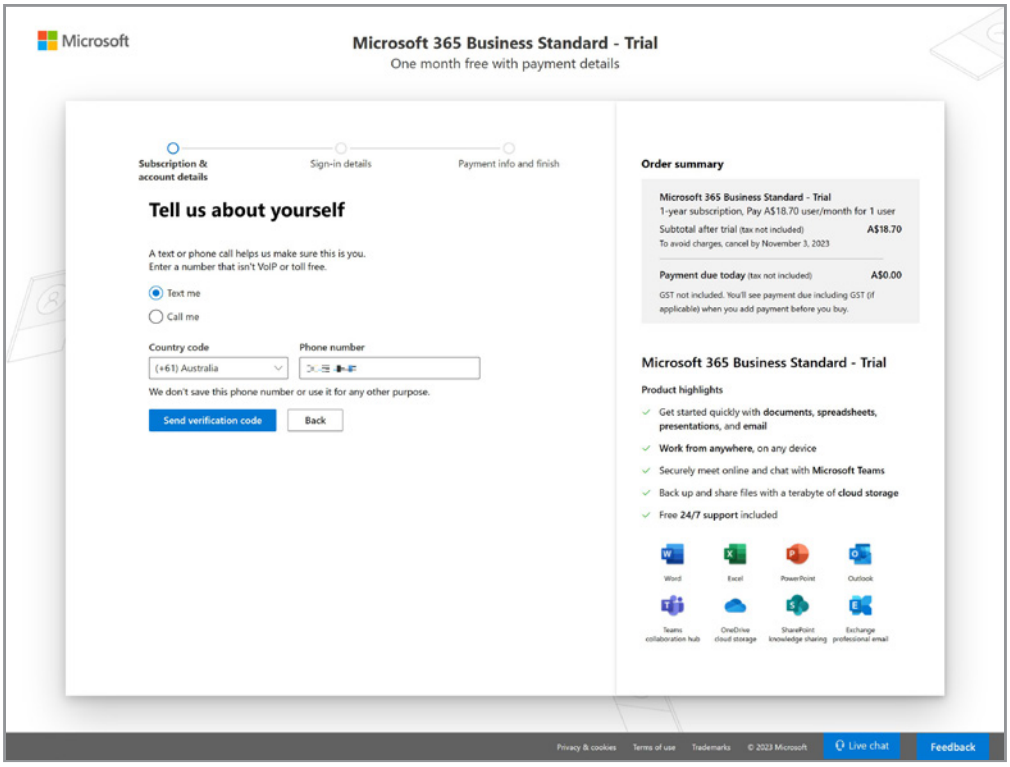
Payment due today (tax not included) A$0.00
GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**
- ✓ **Work from anywhere,** on any device
- ✓ Securely meet online and chat with **Microsoft Teams**
- ✓ Back up and share files with a terabyte of **cloud storage**
- ✓ Free **24/7 support** included

7. Enter a phone number that can receive a phone call or SMS verification code and click '**Send verification code**'.



Microsoft

Microsoft 365 Business Standard - Trial

One month free with payment details

○ **Subscription & account details** — ○ Sign-in details — ○ Payment info and finish

Tell us about yourself

A text or phone call helps us make sure this is you.
Enter a number that isn't VoIP or toll free.

● Text me

○ Call me

Country code (+61) Australia

Phone number [redacted]

We don't save this phone number or use it for any other purpose.

Send verification code Back

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user

Subtotal after trial (tax not included) A$18.70
To avoid charges, cancel by November 3, 2023

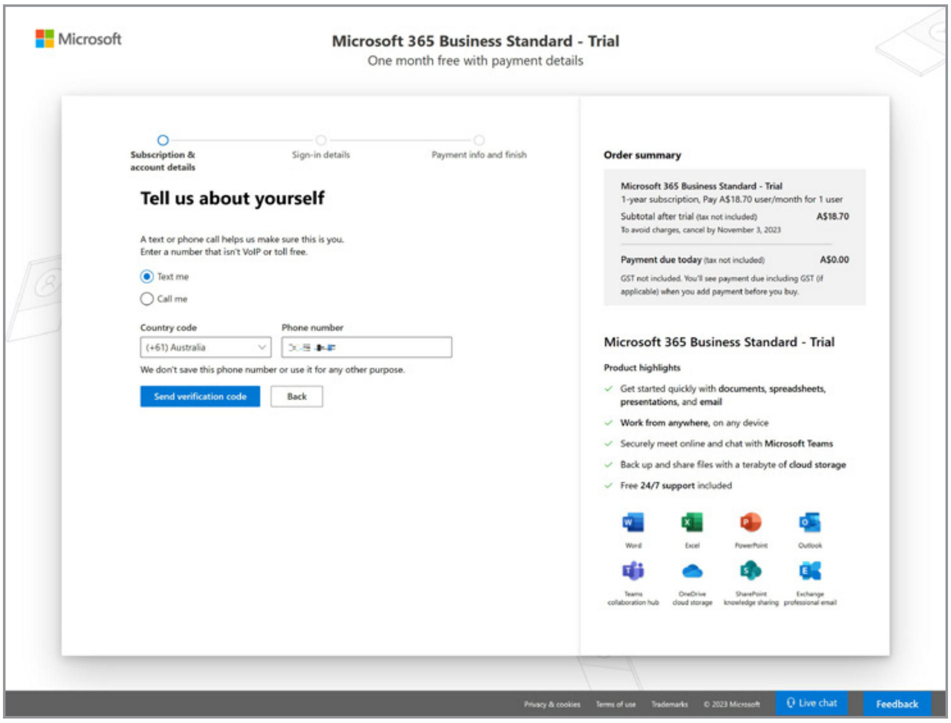
Payment due today (tax not included) A$0.00
GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**
- ✓ **Work from anywhere,** on any device
- ✓ Securely meet online and chat with **Microsoft Teams**
- ✓ Back up and share files with a terabyte of **cloud storage**
- ✓ Free **24/7 support** included

8. Enter the code received into the text box and click ‘**Verify**’.



Microsoft 365 Business Standard - Trial
One month free with payment details

Subscription & account details — Sign-in details — Payment info and finish

Tell us about yourself

A text or phone call helps us make sure this is you.
Enter a number that isn't VoIP or toll free.

● Text me
○ Call me

Country code: (+61) Australia
Phone number: [redacted]

We don't save this phone number or use it for any other purpose.

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user
Subtotal after trial (tax not included) A$18.70
To avoid charges, cancel by November 3, 2023

Payment due today (tax not included) A$0.00
GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

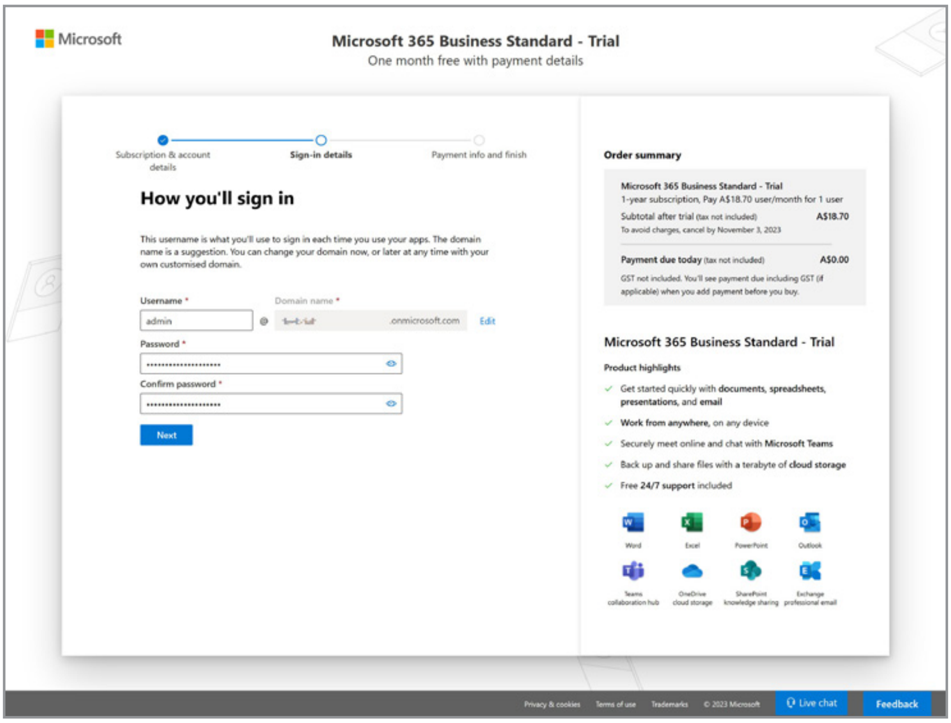
Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**
- ✓ **Work from anywhere,** on any device
- ✓ Securely meet online and chat with **Microsoft Teams**
- ✓ Back up and share files with a terabyte of **cloud storage**
- ✓ Free **24/7 support** included

9. Enter a username, domain name and password, and then click ‘**Next**’. This will create a ‘Global Administrator’ account with the chosen username and password required in later stages of this guidance.

> **NOTE:** Username: The username on this screen will be the primary administrator account to gain access to the Microsoft 365 administration portal.
>
> Domain Name: Microsoft requires initial use of ‘.onmicrosoft.com’. After setup, the organisation’s own domain name can replace this.



Microsoft 365 Business Standard - Trial
One month free with payment details

Subscription & account details — Sign-in details — Payment info and finish

How you'll sign in

This username is what you'll use to sign in each time you use your apps. The domain name is a suggestion. You can change your domain now, or later at any time with your own customised domain.

Username *: admin @ Domain name *: [redacted] .onmicrosoft.com Edit
Password *: ••••••••••••••••••••
Confirm password *: ••••••••••••••••••••

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user
Subtotal after trial (tax not included) A$18.70
To avoid charges, cancel by November 3, 2023

Payment due today (tax not included) A$0.00
GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**
- ✓ **Work from anywhere,** on any device
- ✓ Securely meet online and chat with **Microsoft Teams**
- ✓ Back up and share files with a terabyte of **cloud storage**
- ✓ Free **24/7 support** included

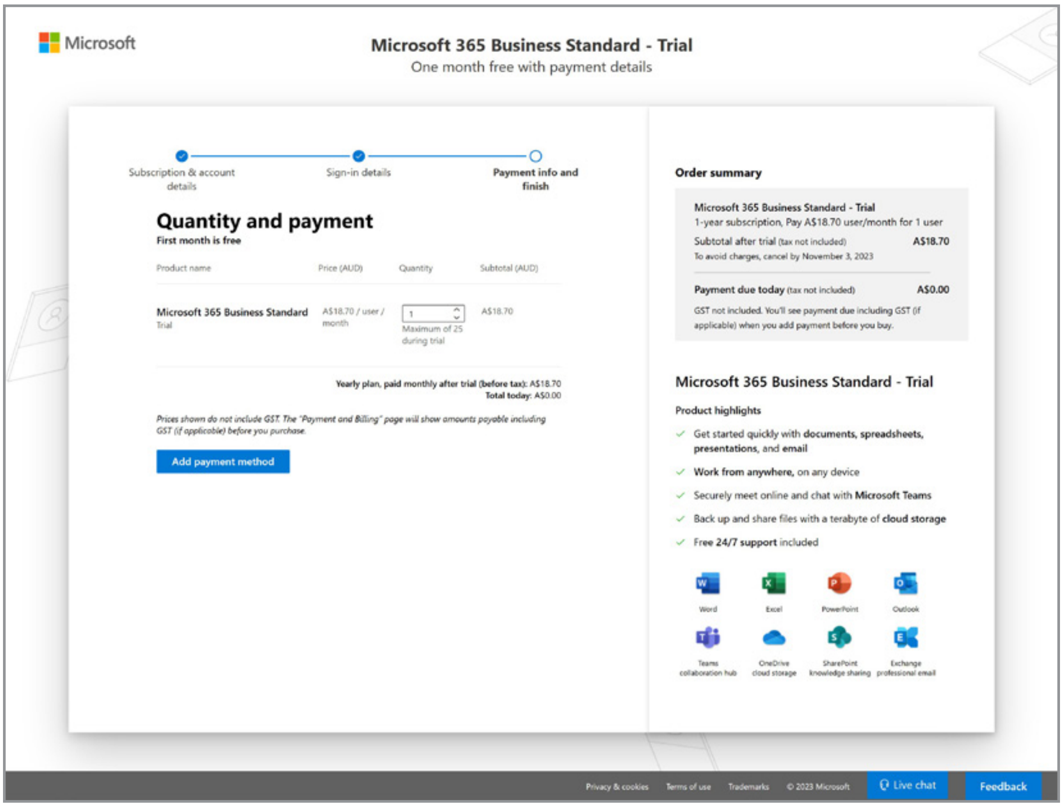
WARNING: Ensure to record the username, domain name and password in a secure location (location must not be associated with or hosted on the network experiencing disruption). Until additional users are added to the tenant with appropriate access permissions, loss of the credentials will result in an inability to access the Microsoft 365 environment.

10. Microsoft requires a valid credit card to register a Business Standard subscription, click '**Add Payment method**', complete the payment information, and click '**Save**'.

NOTE: Microsoft will not bill the credit card within the trial period. However, Microsoft will verify the validity of the card and create a billing account. The billing account is used to manage account settings, invoices, update payment methods and purchases. For more information about billing accounts, see:

- Understand Billing Accounts at learn.microsoft.com/en-us/microsoft-365/commerce/manage-billing-accounts

At the end of the free trial period, the trial subscription will automatically convert to a paid subscription, defaulting to the same plan selected for the trial period. Charges to the credit card will not be incurred if the trial subscription is cancelled prior to the end of the free trial period. The trial will automatically expire at the end of the 30-day period and the credit card will not be charged.



Microsoft 365 Business Standard - Trial
One month free with payment details

Quantity and payment
First month is free

Product name	Price (AUD)	Quantity	Subtotal (AUD)
Microsoft 365 Business Standard Trial	A$18.70 / user / month	1 Maximum of 25 during trial	A$18.70

Yearly plan, paid monthly after trial (before tax): A$18.70
Total today: A$0.00

Prices shown do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

Order summary

Microsoft 365 Business Standard - Trial
1-year subscription, Pay A$18.70 user/month for 1 user

Subtotal after trial (tax not included)	**A$18.70**
To avoid charges, cancel by November 3, 2023	
Payment due today (tax not included)	**A$0.00**

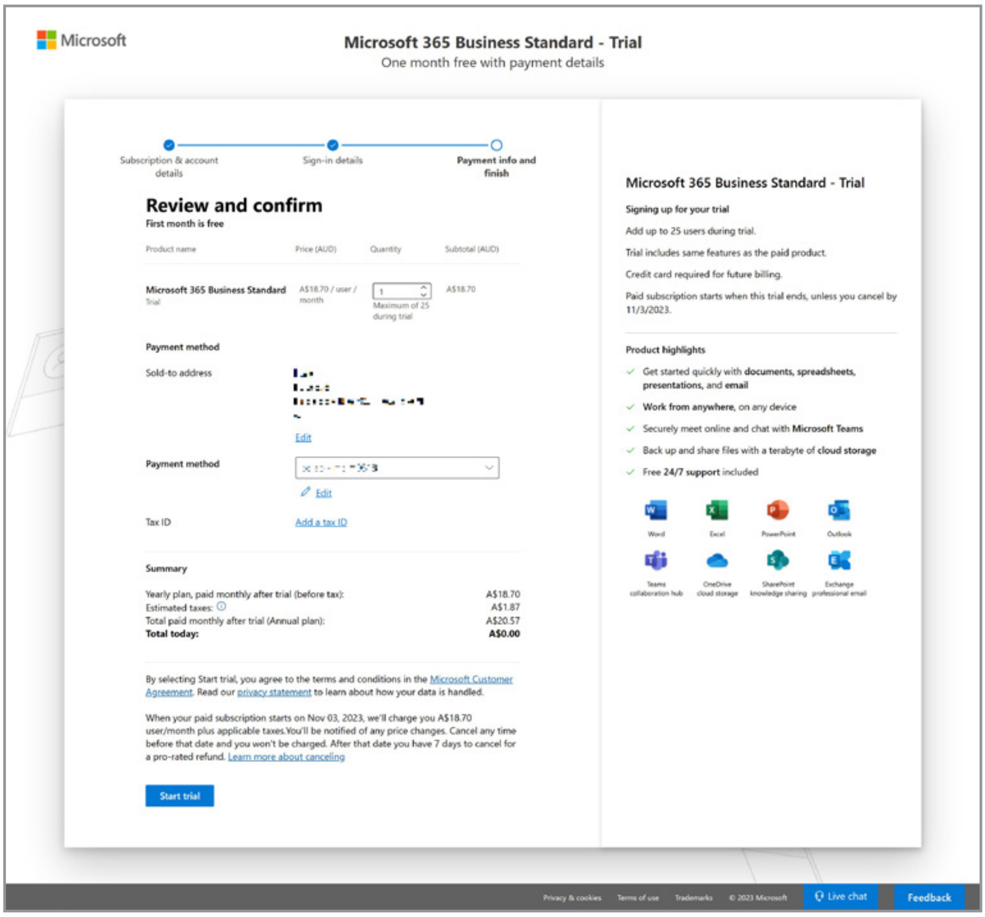
GST not included. You'll see payment due including GST (if applicable) when you add payment before you buy.

Microsoft 365 Business Standard - Trial

Product highlights

- ✓ Get started quickly with **documents, spreadsheets, presentations**, and **email**
- ✓ **Work from anywhere,** on any device
- ✓ Securely meet online and chat with **Microsoft Teams**
- ✓ Back up and share files with a terabyte of **cloud storage**
- ✓ Free **24/7 support** included

11. Review the information and click ‘**Start trial**’.



Microsoft 365 Business Standard - Trial

One month free with payment details

Review and confirm

First month is free

Product name	Price (AUD)	Quantity	Subtotal (AUD)
Microsoft 365 Business Standard Trial	A$18.70 / user / month	1 Maximum of 25 during trial	A$18.70

Payment method

Sold-to address [redacted]

Edit

Payment method [redacted]

Edit

Tax ID Add a tax ID

Summary

Yearly plan, paid monthly after trial (before tax):	A$18.70
Estimated taxes: ⓘ	A$1.87
Total paid monthly after trial (Annual plan):	A$20.57
Total today:	**A$0.00**

By selecting Start trial, you agree to the terms and conditions in the Microsoft Customer Agreement. Read our privacy statement to learn about how your data is handled.

When your paid subscription starts on Nov 03, 2023, we'll charge you A$18.70 user/month plus applicable taxes.You'll be notified of any price changes. Cancel any time before that date and you won't be charged. After that date you have 7 days to cancel for a pro-rated refund. Learn more about canceling

Microsoft 365 Business Standard - Trial

Signing up for your trial

Add up to 25 users during trial.

Trial includes same features as the paid product.

Credit card required for future billing.

Paid subscription starts when this trial ends, unless you cancel by 11/3/2023.

Product highlights

✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**

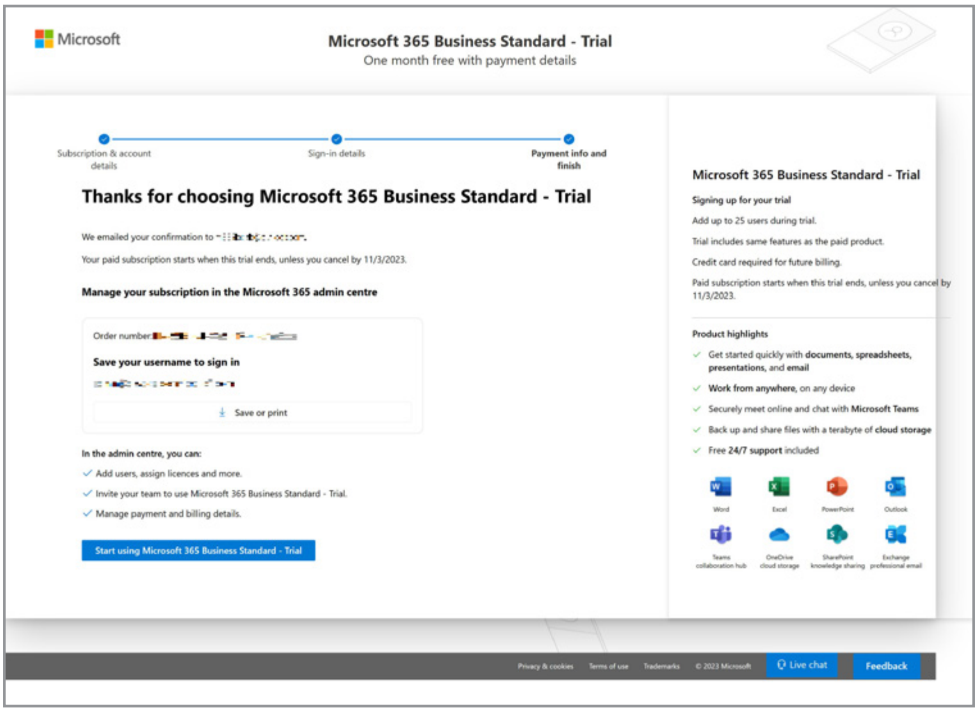
✓ **Work from anywhere,** on any device

✓ Securely meet online and chat with **Microsoft Teams**

✓ Back up and share files with a terabyte of **cloud storage**

✓ Free **24/7 support** included

12. After a short period, the screen will update to show a confirmation that the Microsoft 365 Business Standard subscription process is active. Ensure the information is saved to a location where it can be accessed in the future (location must not be associated with or hosted on the network experiencing disruption), and then click ‘**Start using Microsoft 365 Business Standard**’.



Microsoft 365 Business Standard - Trial

One month free with payment details

Thanks for choosing Microsoft 365 Business Standard - Trial

We emailed your confirmation to [redacted]

Your paid subscription starts when this trial ends, unless you cancel by 11/3/2023.

Manage your subscription in the Microsoft 365 admin centre

Order number [redacted]

Save your username to sign in

[redacted]

In the admin centre, you can:

✓ Add users, assign licences and more.

✓ Invite your team to use Microsoft 365 Business Standard - Trial.

✓ Manage payment and billing details.

Microsoft 365 Business Standard - Trial

Signing up for your trial

Add up to 25 users during trial.

Trial includes same features as the paid product.

Credit card required for future billing.

Paid subscription starts when this trial ends, unless you cancel by 11/3/2023.

Product highlights

✓ Get started quickly with **documents, spreadsheets, presentations,** and **email**

✓ **Work from anywhere,** on any device

✓ Securely meet online and chat with **Microsoft Teams**

✓ Back up and share files with a terabyte of **cloud storage**

✓ Free **24/7 support** included

13. The Microsoft 365 Business Standard trial is now active.

Stage 3: Configure Organisation Settings

Overview

This step configures the organisation's existing DNS information to point to the new Microsoft 365 Business Standard tenant, enabling email routing.

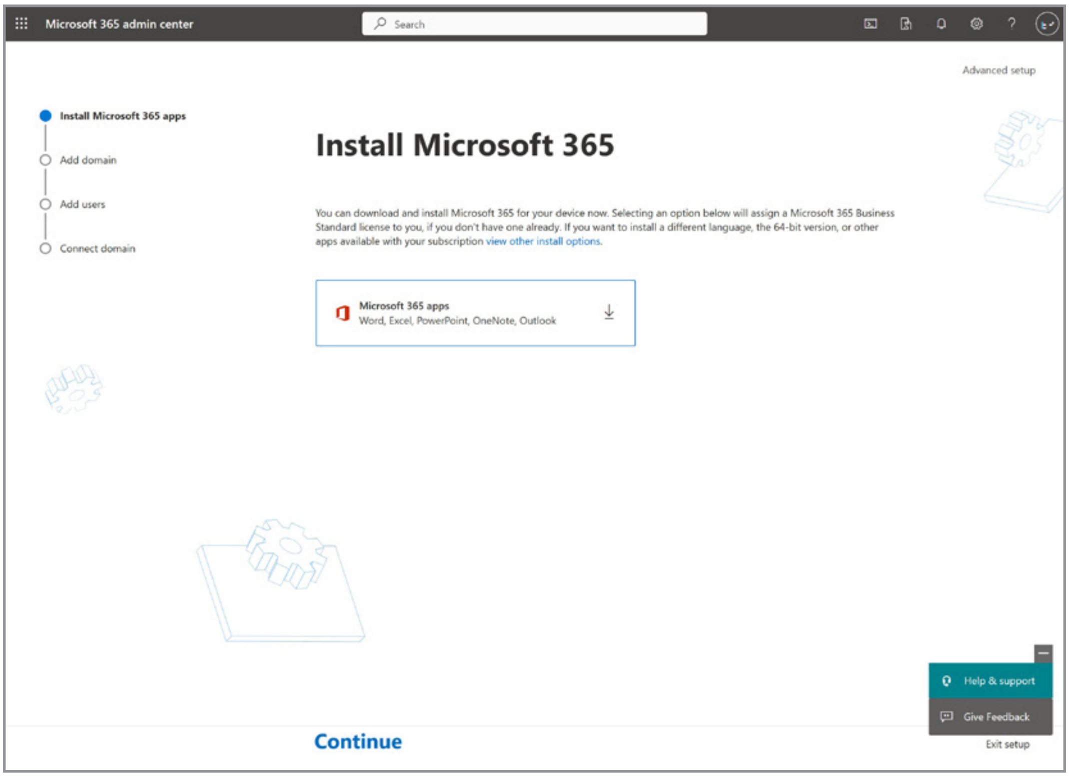
Stage Prerequisites

The operator completing this stage will require:

1. PC with a connection to the Internet
2. Up-to-date web browser
3. Access to and ability to edit the organisation's DNS settings in the provider portal

Process

1. Continuing from Stage 2, the operator will have the opportunity to install Microsoft 365 desktop applications. Installation and operation of the desktop applications are not in scope for this guidance, so click '**Continue**'.

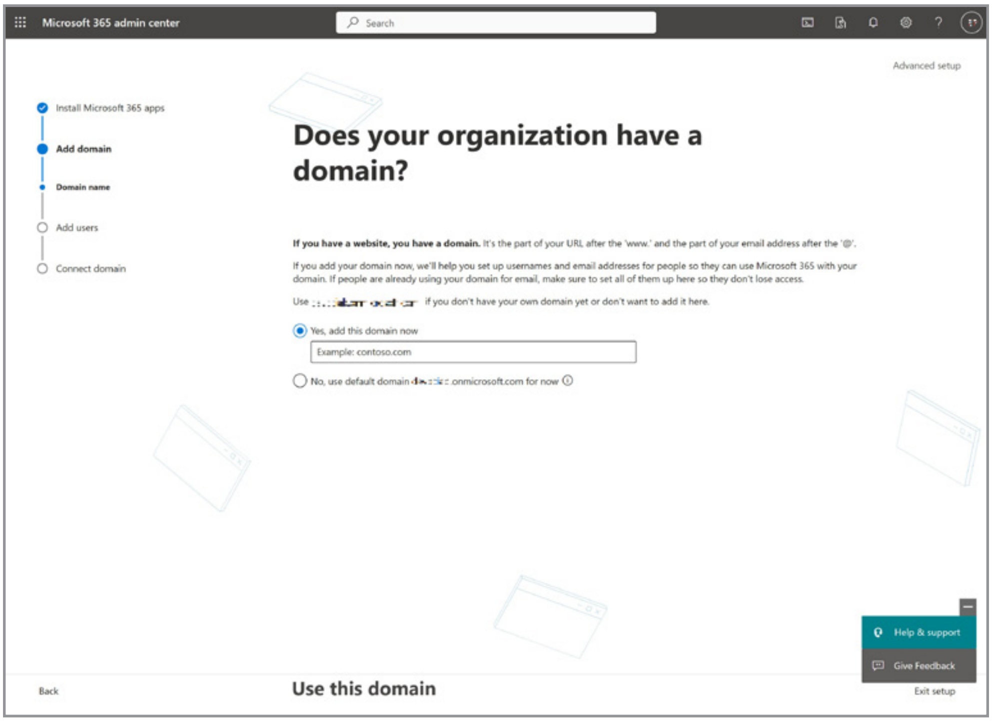


Install Microsoft 365

You can download and install Microsoft 365 for your device now. Selecting an option below will assign a Microsoft 365 Business Standard license to you, if you don't have one already. If you want to install a different language, the 64-bit version, or other apps available with your subscription view other install options.

Microsoft 365 apps
Word, Excel, PowerPoint, OneNote, Outlook

2. To enable creation of the catch-all mailbox, the organisation's existing DNS records need to be updated to point to the new Microsoft 365 Exchange Online endpoints for the organisation. In the available text box enter the organisation's domain name and click '**Use this domain**'.



Does your organization have a domain?

If you have a website, you have a domain. It's the part of your URL after the 'www.' and the part of your email address after the '@'.

If you add your domain now, we'll help you set up usernames and email addresses for people so they can use Microsoft 365 with your domain. If people are already using your domain for email, make sure to set all of them up here so they don't lose access.

Use [redacted] if you don't have your own domain yet or don't want to add it here.

● Yes, add this domain now

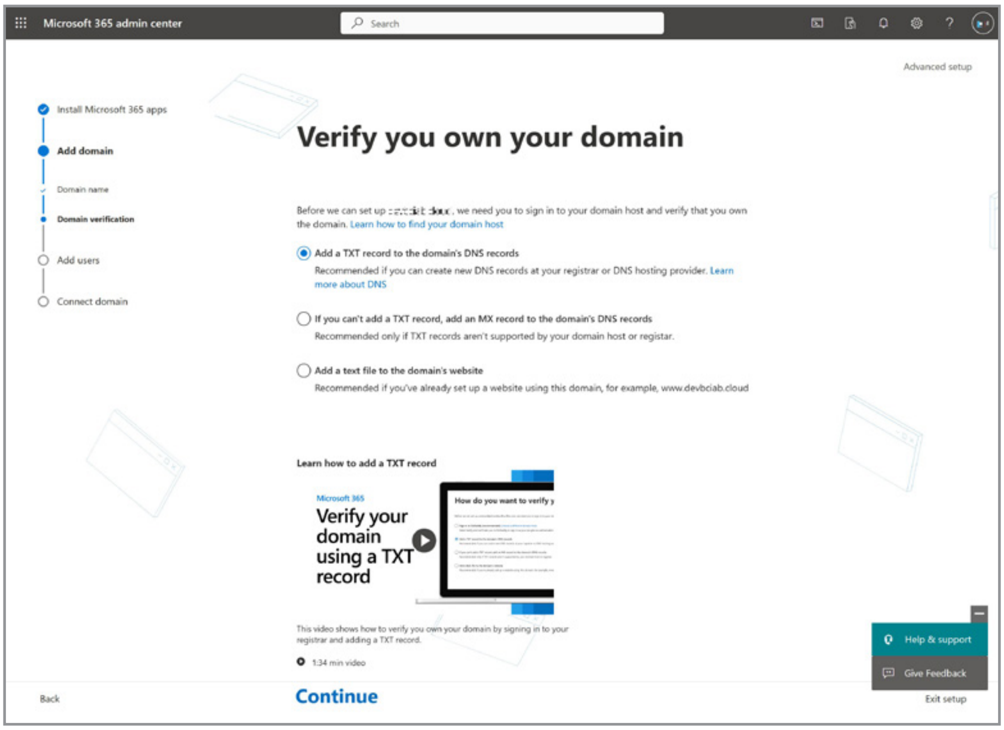
Example: contoso.com

○ No, use default domain [redacted].onmicrosoft.com for now ⓘ

Use this domain

3. To verify ownership of the domain, Microsoft requires the addition of a TXT record or an MX record to the DNS settings. This guidance uses the first option, 'Add a TXT record to the domain's DNS records', but the processes for adding an MX record is similar. Click 'Continue' after selecting the desired option.

> ⓘ **NOTE:** Microsoft allows for the upload of a text file to the organisation's website. However, this guidance assumes that the website is not available.



Verify you own your domain

Before we can set up [redacted], we need you to sign in to your domain host and verify that you own the domain. Learn how to find your domain host

● Add a TXT record to the domain's DNS records
Recommended if you can create new DNS records at your registrar or DNS hosting provider. Learn more about DNS

○ If you can't add a TXT record, add an MX record to the domain's DNS records
Recommended only if TXT records aren't supported by your domain host or registar.

○ Add a text file to the domain's website
Recommended if you've already set up a website using this domain, for example, www.devbciab.cloud

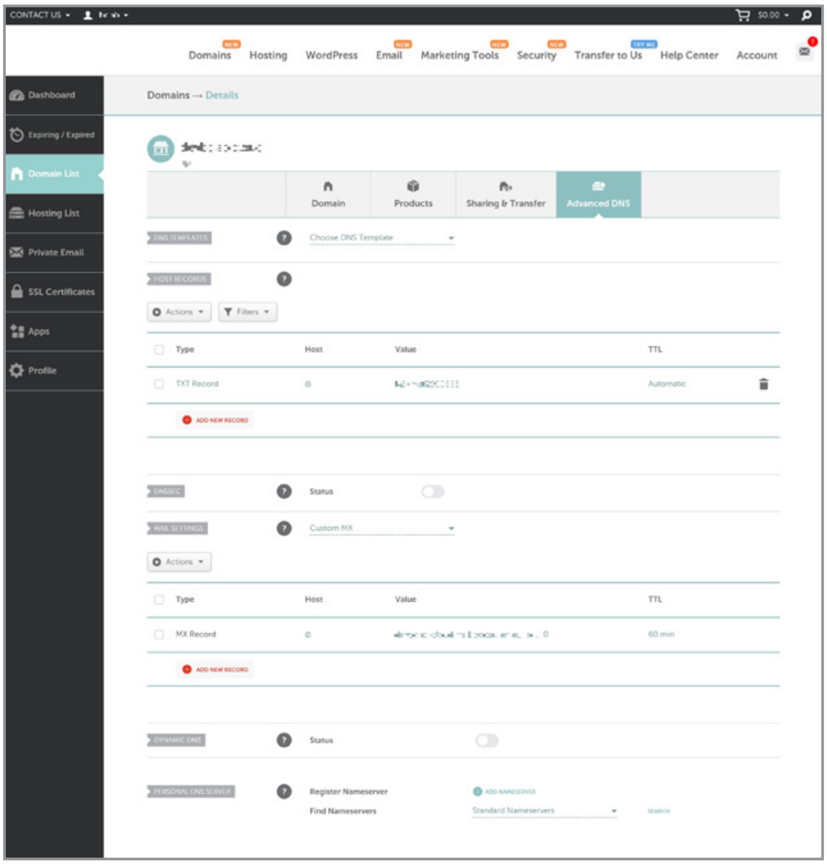
Learn how to add a TXT record

This video shows how to verify you own your domain by signing in to your registrar and adding a TXT record.

1:34 min video

Continue

4. Microsoft will attempt to identify the DNS hosting provider. If known, they will provide the steps to edit the DNS records or a link to the DNS provider's guidance documentation. To continue with this step, in a separate internet browser window or tab, go to the organisation's DNS hosting provider portal and add the identified TXT record information. After editing the DNS record information on the hosting provider portal, return to the Microsoft 365 page and click '**Verify**'.

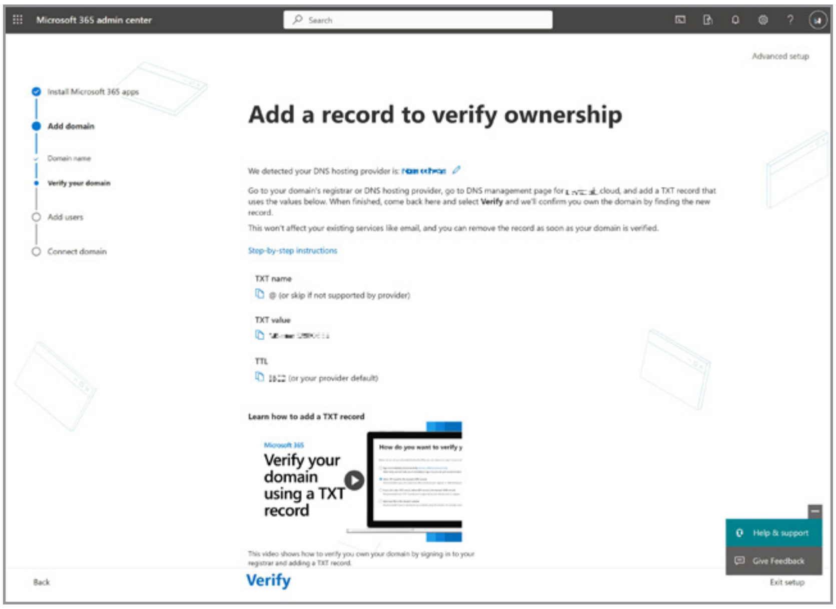


Type	Host	Value	TTL
TXT Record	@		Automatic

Type	Host	Value	TTL
MX Record	@		60 min

WARNING: It is important not to edit existing records at this stage. The DNS record entry is to be added to existing entries only.

Changes to DNS record information can take some time for Microsoft to find. If Microsoft cannot find the new DNS record after clicking '**Verify**', keep retrying. Depending on the DNS hosting provider, changes can generally take anywhere from a few minutes to 48 hours.



Add a record to verify ownership

We detected your DNS hosting provider is:

Go to your domain's registrar or DNS hosting provider, go to DNS management page for , and add a TXT record that uses the values below. When finished, come back here and select **Verify** and we'll confirm you own the domain by finding the new record.

This won't affect your existing services like email, and you can remove the record as soon as your domain is verified.

TXT name
@ (or skip if not supported by provider)

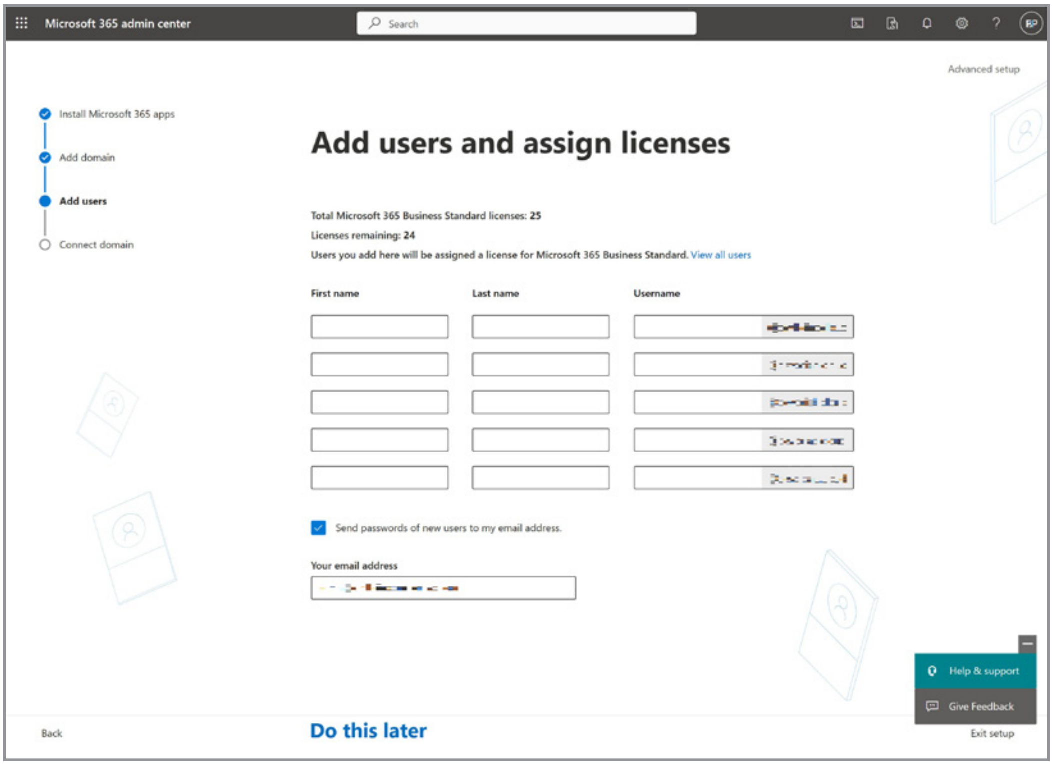
TXT value

TTL
(or your provider default)

Learn how to add a TXT record

This video shows how to verify you own your domain by signing in to your registrar and adding a TXT record.

5. Once Microsoft successfully verifies the domain, the page will automatically update to enable the adding of users and assigning of licences. By default, the initial account created during Stage 2 will have all relevant licences assigned and will be assigned the role of Global Administrator, see learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles. It is not necessary to create any additional users at this stage of the setup. Click '**Do this later**'.



Add users and assign licenses

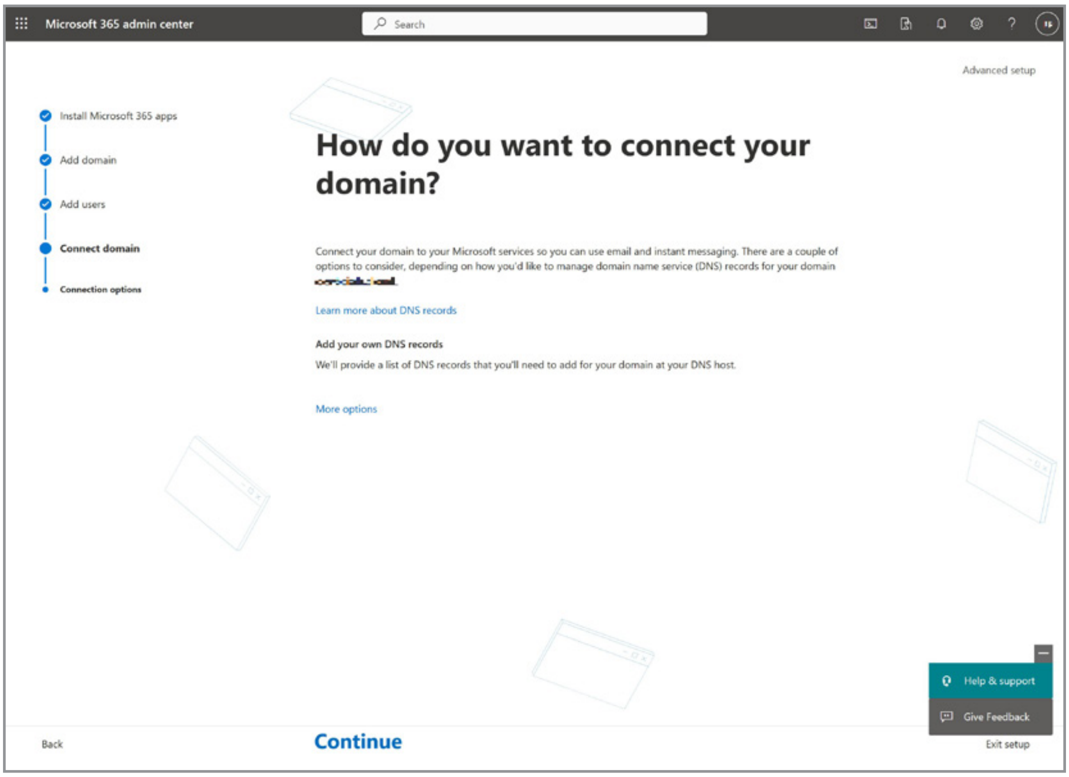
Total Microsoft 365 Business Standard licenses: 25
Licenses remaining: 24
Users you add here will be assigned a license for Microsoft 365 Business Standard. View all users

First name	Last name	Username
		[redacted]
		[redacted]
		[redacted]
		[redacted]
		[redacted]

☑ Send passwords of new users to my email address.

Your email address: [redacted]

6. To connect Microsoft 365 to the organisation's domain, the DNS records require modification in the DNS hosting provider portal. Click the default option '*Add your own DNS records*'. Click '**Continue**'.



How do you want to connect your domain?

Connect your domain to your Microsoft services so you can use email and instant messaging. There are a couple of options to consider, depending on how you'd like to manage domain name service (DNS) records for your domain [redacted]

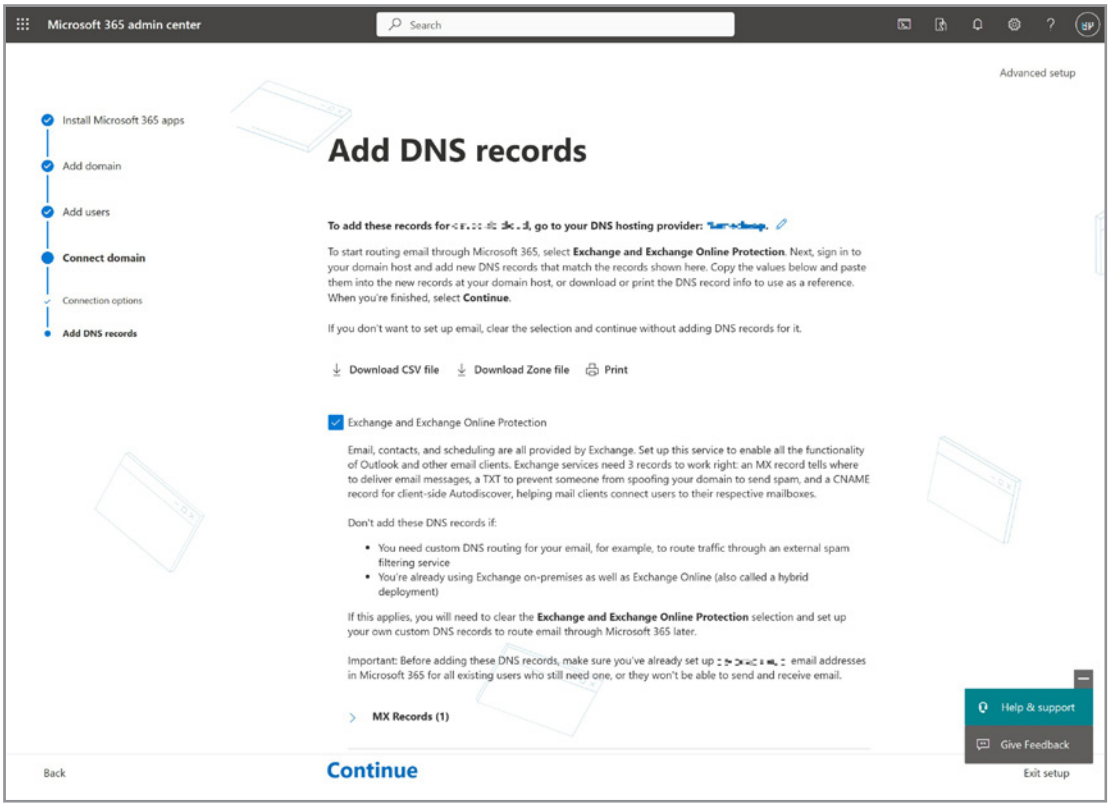
Learn more about DNS records

Add your own DNS records
We'll provide a list of DNS records that you'll need to add for your domain at your DNS host.

More options

7. The next screen provides the DNS record information to implement in the DNS hosting provider portal. Follow the guidance provided on this page and within the organisation DNS hosting provider guidance to add the DNS records. Once complete click ‘**Continue**’.

> ⚠ **WARNING:** The changes made at this stage will cause all emails sent to the organisation domain to be re-routed to the new Microsoft 365 tenant. Ensure a backup of the DNS information in the hosting provider portal is made to enable the organisation to switch back to the enterprise email solution when possible.
>
> If the organisation can receive emails during the cyber security incident, it is recommended not to proceed with this step until the catch-all mailbox is configured within Exchange Online to minimise the risk of lost email messages during the change.
>
> As with Step 4, changes to DNS record information can take some time for Microsoft to verify. If Microsoft cannot find the new DNS record, keep retrying. Depending on the DNS hosting provider, changes can take anywhere from a few minutes to 48 hours.



Add DNS records

To add these records for [redacted], go to your DNS hosting provider: [redacted].

To start routing email through Microsoft 365, select **Exchange and Exchange Online Protection**. Next, sign in to your domain host and add new DNS records that match the records shown here. Copy the values below and paste them into the new records at your domain host, or download or print the DNS record info to use as a reference. When you're finished, select **Continue**.

If you don't want to set up email, clear the selection and continue without adding DNS records for it.

Download CSV file Download Zone file Print

☑ Exchange and Exchange Online Protection

Email, contacts, and scheduling are all provided by Exchange. Set up this service to enable all the functionality of Outlook and other email clients. Exchange services need 3 records to work right: an MX record tells where to deliver email messages, a TXT to prevent someone from spoofing your domain to send spam, and a CNAME record for client-side Autodiscover, helping mail clients connect users to their respective mailboxes.

Don't add these DNS records if:

- You need custom DNS routing for your email, for example, to route traffic through an external spam filtering service
- You're already using Exchange on-premises as well as Exchange Online (also called a hybrid deployment)

If this applies, you will need to clear the **Exchange and Exchange Online Protection** selection and set up your own custom DNS records to route email through Microsoft 365 later.

Important: Before adding these DNS records, make sure you've already set up [redacted] email addresses in Microsoft 365 for all existing users who still need one, or they won't be able to send and receive email.

> **MX Records (1)**

Continue

8. Once the DNS record information is configured and Microsoft can verify the updates, the setup will finish. The DNS record information is now pointing to the new Microsoft 365 Business Standard tenant.

Stage 4: Run Automated Configuration of Environment

Overview

This stage applies system configuration settings to the newly provisioned Microsoft 365 tenant via the automation tool, which comprises a collection of PowerShell scripts.

The automation tool will perform the following actions:

1. Install required Microsoft modules from the PowerShell gallery
2. Create a connection to the Microsoft 365 tenant
3. Create an emergency 'break glass' administration account
4. Create a 'catch-all' mailbox, associated group, and mail transport rules
5. Close the connection to the Microsoft 365 tenant

ⓘ **NOTE:** For instances where the use of an automated tool may not be suitable, guidance on how to manually implement the 'catch-all' mailbox can be found at Appendix B.

⚠ **WARNING:** The 'catch-all' mailbox created by the automation tool is not supported by Microsoft due to its lesser filtering capability and resultant increased risk of spam and undetected phishing attempts.

Access to the catch-all mailbox should therefore be restricted and closely monitored to reduce the likelihood of an unskilled operator accessing a potentially malicious email message.

Where practical, the catch-all mailbox should be provisioned for as short a period as possible. Once all users have been created within the new Microsoft 365 tenant, or business operations are restored, the mailbox should be removed.

To minimise the impact to the Microsoft 365 tenant in the event of accessing a malicious email message held within the catch-all mailbox, a separate user account should be created with minimal access permissions to the remainder of the Microsoft 365 tenant. Ideally, this user should be the only user to access the catch-all mailbox. However, given the limited availability of user licences within the trial tenant and the cost of an additional user licence, this is something organisations will need to individually determine based on their own risk assessment.

Additionally, the Microsoft 365 Business Standard subscription only allows each user up to 50 GB of mailbox storage per user. Given the nature of the catch-all mailbox, once this size limit is reached, additional mail may be rejected.

Stage Prerequisites

The operator completing this stage will require:

1. PC with a connection to the Internet
2. Up-to-date web browser
3. The Business Continuity in a Box PowerShell module available from: cyber.gov.au/resources-business-and-government/essential-cyber-security/smallbusiness/business-continuity-box
4. Username and password of an account with the Global Administrator role

> **NOTE:** If continuing from previous stages within this guidance, the account created in Stage 2 of the document has the necessary Global Administrator permissions.

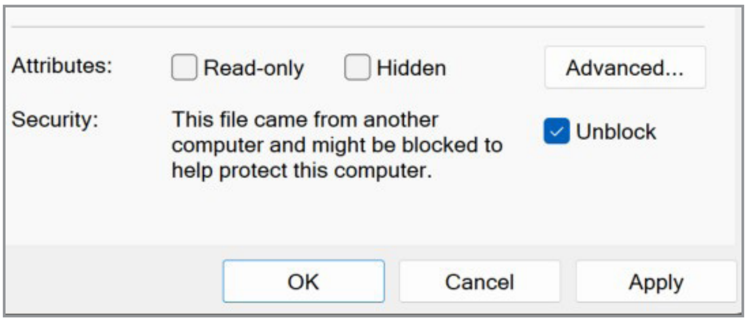
Process

Step 1: Preparation

1. Navigate to cyber.gov.au/resources-business-and-government/essential-cyber-security/smallbusiness/business-continuity-box and download the automation tool compressed folder, then open File Explorer and navigate to the download location of the folder.
   a. Press the Windows Key on the keyboard or click the Windows button on the Taskbar.
   b. In the "Search for apps, settings and documents" textbox, type "File Explorer" and click '**Open**'.
   c. Navigate to the folder where the automation tool folder was extracted (e.g., Downloads).
2. Extract the contents of the package to a nominated location.

> ⚠ **WARNING:** Before performing the following steps, ensure the downloaded automation tool folder is from cyber.gov.au/resources-business-and-government/essential-cyber-security/smallbusiness/business-continuity-box.

   a. Right click on the file and select '**Properties**'.
   b. In the pop-up window that appears locate the '**Unblock**' checkbox in the bottom right corner and place a tick in the checkbox to select the item.



Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. ☑ Unblock

   c. Click '**OK**' to return to Windows Explorer.
   d. Right click on the file again and select '**Extract All...**'.
   e. In the pop-up window that appears select the desired location to extract the files.
   f. Click '**Extract**'.

NOTE: Access to the Microsoft 365 tenant is dependent on the account that is used to sign in. As such, there is no configuration required for the script to apply the default configuration settings.

More specific configuration of the Microsoft 365 tenant is possible by editing the configuration settings within the associated configuration files. This guidance does not cover customised tenant configuration.

Step 2: Run the Automation Tool

1. The automation tool can be run using either a Windows Normal User or Windows Administrator account.
2. To run the automation tool with the currently logged-in user, open the extracted package in File Explorer.
   a. Press the Windows Key on the keyboard or click the Windows button on the Taskbar.
   b. In the 'Search for apps, settings, and documents' textbox, type 'File Explorer' and then click '**Open**'.
   c. Navigate to the folder where the automation tool folder was extracted and open the folder.
3. Locate the file BCiaB.bat and double click the file to begin implementation.
4. A window will appear.
5. Early in the implementation, the operator will be presented with a prompt that displays the credentials of the Emergency Administrator account. Ensure that these credentials are written down and stored appropriately.
6. The automation tool will provide feedback to the operator on the process currently running. Do not exit the open applications or shutdown the computer until the tool has finished.
7. Once the automation tool has finished, the user will be presented with a completion screen with a report summarising the process and the changes, which can be used to troubleshoot any unexpected issues.
8. The new Microsoft 365 Business Standard trial tenant is now configured.

NOTE: Some settings may take time to be activated by background Microsoft processes. Microsoft advises that configuration can take up to 24 hours for certain features and capabilities.

Stage 5: Apply Security Settings

This stage outlines the security settings that should be applied to achieve a minimum secure baseline for the Microsoft 365 tenant. Organisations should assess their own requirements and adjust the below to suit their context. Please note, these settings are designed to meet the baseline security requirements of a temporary system.

The tables listed below are categorised according to Microsoft 365 services: Entra ID, Exchange Online and Defender. They are listed in order of recommended criticality.

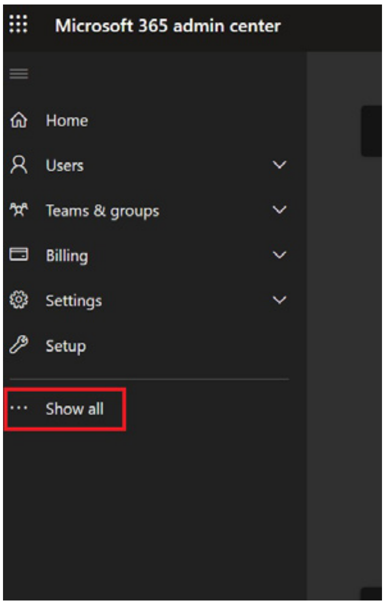
Note: Business Continuity in a Box is designed to be a temporary solution for organisations experiencing a cyber incident. Depending on the situation, organisations may need to use the Microsoft 365 tenant for a longer duration than initially expected. In such circumstances, organisations may wish to use an alternative license type in order to access additional security features. Additional security features available at alternative licence tiers can be found at Appendix C.

Microsoft Entra ID

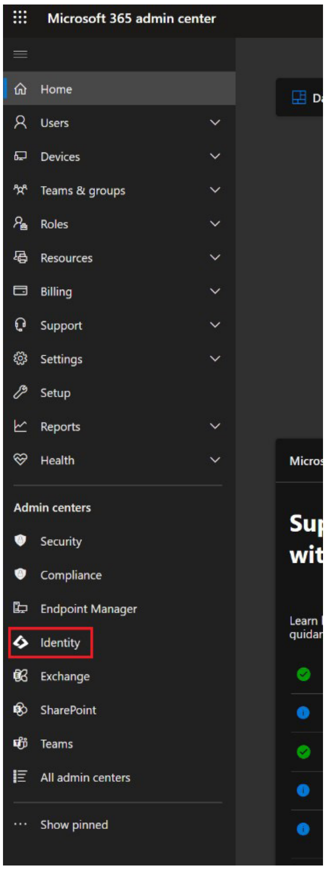
How to get to Microsoft Entra ID:

1. Go to the Microsoft admin portal by typing 'admin.microsoft.com' into the search bar.

2. In the navigation menu on the left-hand side, locate and click '**Show all**'.



3. Click on ‘**Identity**’. This should take you the Entra ID portal.



Critical Settings:

Security Setting	Description	Reference	Where to change this
Apply principles of least privilege, paying special attention to admin accounts	Use separate admin accounts and RBAC roles to limit admin privileges; grant only the roles required for job function	Best practices for Microsoft Entra roles	Roles and administrators - Microsoft Entra admin centre
Observe Microsoft’s guidance for emergency access accounts	Cloud-only accounts configured with extra-long password; excluded from Conditional access policies	Manage emergency access accounts	N/A
Configure authentication methods	At a minimum, configure the Microsoft Authenticator mobile app, Temporary Access Pass (TAP), and email OTP	Manage authentication methods	Authentication methods - Microsoft Entra admin centre
Enable Self-service password reset (SSPR) for all users	Admins are set up this way by default; allow users to reset their own passwords using a second factor	Deployment considerations for self-service password reset	Password reset - Microsoft Entra admin centre

Recommended Settings:

Security Setting	Description	Reference	Where to change this
Configure the password expiration policy	Ensure that your password expiration is in alignment with corporate policy	Set the password expiration policy for your organization	Settings > Org settings > Security & Privacy > Password expiration - Microsoft 365 admin centre
Follow best practices for security groups	Assign licenses, apps and policies to well-named security groups rather than individual users; avoid nesting groups	Manage Microsoft Entra groups and group membership	N/A
Configure Device settings, e.g. Microsoft Entra Join, Enterprise State Roaming, and local administrator settings	Prepare for Company-owned devices joined to Microsoft Entra	Plan your Microsoft Entra join implementation	Devices > Device settings - Microsoft Entra admin centre
Configure user settings in Microsoft Entra ID	For higher sensitivity environments it is recommended to disable user App registration and tenant creation	Default user permissions in Microsoft Entra ID	Users > User settings - Microsoft Entra admin centre
Manage application consent and permissions	By default, all users are able to grant permissions to apps or add-ins; we have options to restrict this capability	Overview of user and admin consent	User consent settings - Microsoft Entra admin centre
Trust claims from other Entra ID tenants	Trust MFA claims and managed devices that have already been verified by another Entra ID tenant	To change inbound trust settings for MFA and device claims	External Identities > Cross-tenant access settings - Microsoft Entra admin centre
Require MFA for guests	Enforce conditional access controls for guest and external users	Require MFA for guest users with Conditional Access	Conditional Access - Microsoft Entra admin centre
Configure external collaboration settings	By default, external collaboration features are fairly open (this is an organisational decision)	Microsoft Entra B2B best practices	External Identities > External collaboration settings - Microsoft Entra admin centre
Configure SSO for enterprise applications	Entra ID can manage and provide SSO for third-party apps as well as Microsoft	App Integration Tutorials for use with Microsoft Entra ID	Enterprise applications - Microsoft Entra admin centre

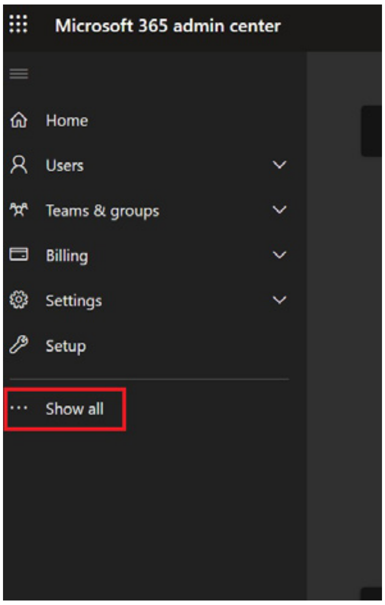
Optional Settings:

Security Setting	Description	Reference	Where to change this
Configure company branding login	Corporate branding on the login page reduces likelihood of phishing via look-a-like pages	Add your company branding to the Microsoft 365 sign-in page	Company Branding - Microsoft Entra admin centre
Add your organisation's privacy info	Add a privacy contact and privacy statement for internal employees and guests to review	Add your organization's privacy info	Overview > Properties - Microsoft Entra admin centre
Enable hybrid support (if applicable)	Plan for Entra ID Connect and Cloud Sync (and any associated items)	Microsoft Entra Hybrid Identity Documentation	N/A
Additional considerations for applications and resources	Plan for access to legacy systems, applications, printer and files shares, etc.	Understand considerations for applications and resources	N/A

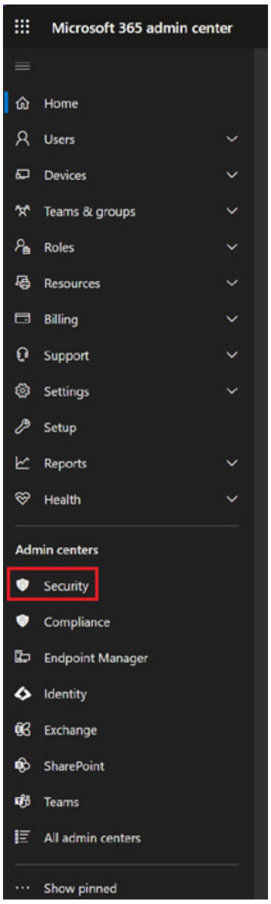
Microsoft Exchange Online and Defender

How to get to Microsoft Exchange Online and Defender:

1. Go to the Microsoft admin portal by typing 'admin.microsoft.com' into the search bar.
2. In the navigation menu on the left-hand side, locate and click '**Show all**'.

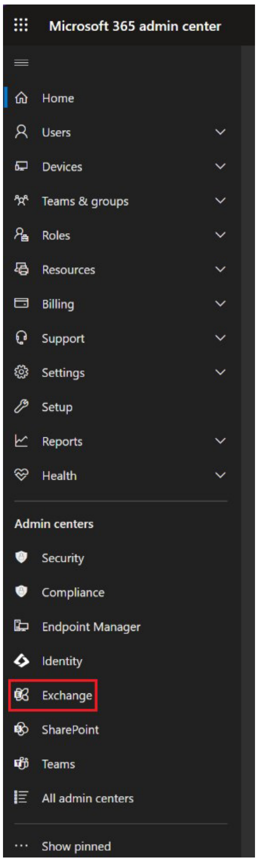


3. Click on ‘**Security**’. This should take you to the Defender portal.



4. Repeat steps 1 and 2 for Microsoft Exchange.

5. Click on ‘**Exchange**’. This should take you to the Exchange portal.



Critical Settings:

Security Setting	Description	Reference	Where to change this
Block legacy authentication	Most legacy authentication should be blocked by default, however, you should still be able to take steps to block SMTP auth.	Disable Basic authentication in Exchange Online	Admin centre > Settings > Org settings > Modern authentication
Block sign-in for all shared mailboxes	Shred mailboxes are often easy targets with weak passwords and no MFA	Block user's sign in	Admin centre > Users > Active users
Implement pre-set security policies (or equivalent)	Microsoft publishes two pre-configured templates for email protection; recommended to use Standard protection	Pre-set security policies	Defender portal > Policies & rules > Threat policies > Pre-set security policies

Recommended Settings:

Security Setting	Description	Reference	Where to change this
Configure Email authentication (SPF, DKIM and DMARC)	Prove that your email really comes from you and prevent spoofing attempts by publishing records in DNS	Email authentication in Microsoft 365	External DNS provider
Deploy the Report Phishing add-in	Not every bad message will be caught and blocked by your security policies, so let users flag messages that slip by	How-to deploy and configure the report message add-in	Admin centre > Settings > Integrated apps
Modify the default value for Retain Deleted Items	By default, deleted items will be purged after 14 days; this is extendable to 30; set on all mailboxes and the mailbox plan	Change how long permanently deleted items are kept for an Exchange Online mailbox	See Set-DeletedItemsRetention.ps1
Migrate to Microsoft 365 groups	Look for opportunities to migrate from legacy Distribution Lists and Public Folders to Microsoft 365 Groups	Upgrade distribution lists to Microsoft 365 Groups	Exchange admin centre > recipients > groups

Optional Settings:

Security Setting	Description	Reference	Where to change this
Disable consumer storage locations in Outlook on the Web	By default, users can work with consumer storage locations such as DropBox, Gsuites and OneDrive (personal)	Set up OneDrive file storage and sharing - Enable or disable third-party storage services	See Block-ConsumerStorageOWA.ps1

Stage 6: Validate Environment

Overview

This stage walks through the process of verifying that the previous stages have been implemented correctly. The operator will log into the new Microsoft 365 tenant, send an email from an external email service to the new tenant, and then send an email from the new tenant to an external email address.

Process

1. Open an internet browser and navigate to Microsoft Outlook https://outlook.com.
2. Click '**Sign in**', using the username and password of the Global Administrator account created in Stage 2.
3. Microsoft Outlook will open to the user mailbox.
4. Add the catch-all mailbox to the available folders:
   a. Right click '**Folders**' in the left-hand navigation pane.
   b. Click '**Add shared folder or mailbox**'.
   c. Type the email address of the catch-all mailbox in the dialog box and select '**Add**'. The catch-all mailbox email address will be 'catch-all@<domain>' where <domain> is the organisation domain not the initial 'onmicrosoft.com' domain.
5. Open a new internet browser tab and navigate to the email account used for account verification in Stage 1 or another email account not associated with the new Microsoft 365 tenant.
6. Send an email to the Global Administrator email address.
7. Send an email to 'info@<domain>' where <domain> is the organisation domain not the 'onmicrosoft.com' domain.

> ⓘ **NOTE**: It is recommended you do not setup any email addresses before this stage, as doing so may potentially create a new mailbox within Exchange Online. If the Microsoft 365 tenant already has an 'info' mailbox, replace 'info@<domain>' with an alternative email address that does not exist to test that all email messages sent to the organisation are captured within the catch-all mailbox.

8. Return to the tab opened in step 1 of this Stage.
9. Verify receipt of the email from step 6 within the Global Administrator mailbox.
10. Verify receipt of the email sent to 'info@<domain>' from step 7 by selecting the catch-all mailbox in the available folders.
11. Create a new email within Outlook and send to the email account used in step 5 of this Stage.
12. Return to the email account in step 5 and verify receipt of the email from the Global Administrator.

Contact

For any enquiries concerning this guidance or to provide feedback, please navigate to cyber.gov.au/about-us/about-asd-acsc/contact-us. Select 'General enquiry or feedback', and choose 'Business Continuity in a Box' from the drop-down menu under 'Your enquiry/feedback type'.

If you or your organisation are victim of a data breach or cyber incident, follow relevant cyber incident response and communication plans, as appropriate.

Australian organisations impacted by, or requiring assistance relating to, a cyber incident can contact ASD's ACSC via 1300 CYBER1 (1300 292 371), or by using ReportCyber at cyber.gov.au/report-and-recover/report.

United States organisations may report cyber incidents to CISA's 24/7 Operations Center at report@cisa.dhs.gov, cisa.gov/report, or (888) 282-0870. When available, please include information regarding the incident: date, time and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organisation; and a designated point of contact.

Appendix A: acronyms, abbreviations and definitions

This document uses the following acronyms and abbreviations:

Acronym or Abbreviation	Definition
DNS	Domain Name Service
Microsoft Entra ID	Formerly Azure Active Directory
MX	Mail Exchange DNS record
Operator	The person responsible for implementation of the Business Continuity in a Box solution for an organisation.
PC	Personal Computer
TXT	Text DNS record
VOIP	Voice over Internet Protocol

Appendix B: manual steps to establish 'catch-all' mailbox

Prerequisites

To implement this guidance, users require:

1. PC with a connection to the Internet.

2. Up-to-date web browser.

3. Username and password of a Microsoft 365 account with active tenant and Global Administrator role.

> ⚠ **WARNING:** The 'catch-all' mailbox created via the below steps is not supported by Microsoft due to its lesser filtering capability and resultant increased risk of spam and undetected phishing attempts.
>
> Access to the catch-all mailbox should therefore be restricted and closely monitored to reduce the likelihood of an unskilled operator accessing a potentially malicious email message.

Where practical, the catch-all mailbox should be provisioned for as short a period as possible. Once all users have been created within the new Microsoft 365 tenant, or business operations are restored, the mailbox should be removed.

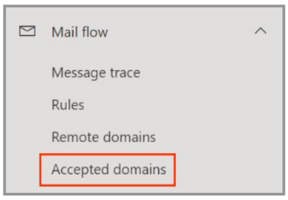
Step 1: Change Domain Status

This step involves changing the domain status of the Microsoft 365 tenant so that it accepts messages to recipients that do not exist within the organisation directory.

1. Open a browser and navigate to https://admin.exchange.microsoft.com/. If prompted, enter the username and password created in Stage 2 of Continuity of Communications.

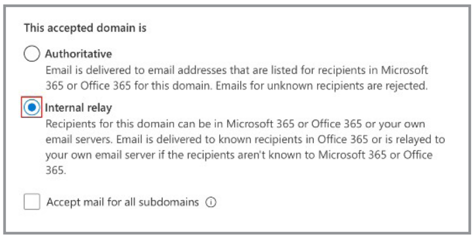
> ⓘ **NOTE:** The first time accessing any of the Microsoft 365 administration portals will present the operator with various hints. It is beneficial to spend some time to navigate through the tips, which are presented to learn the location of items to enable ongoing administration.

2. In the left-hand menu on the portal, select '**Mail flow**' to expand the list, and then click '**Accepted domains**'. The accepted domains window will appear.



3. Click on the name of the organisation's domain name in the list of available domains.

4. On the right-hand side of the screen a new panel will appear. Select '**Internal relay**' and then click '**Save**'.



This accepted domain is

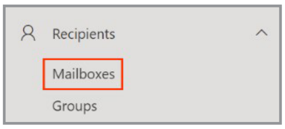
○ Authoritative
Email is delivered to email addresses that are listed for recipients in Microsoft 365 or Office 365 for this domain. Emails for unknown recipients are rejected.

● Internal relay
Recipients for this domain can be in Microsoft 365 or Office 365 or your own email servers. Email is delivered to known recipients in Office 365 or is relayed to your own email server if the recipients aren't known to Microsoft 365 or Office 365.

□ Accept mail for all subdomains ⓘ

Step 2: Add Shared Mailbox

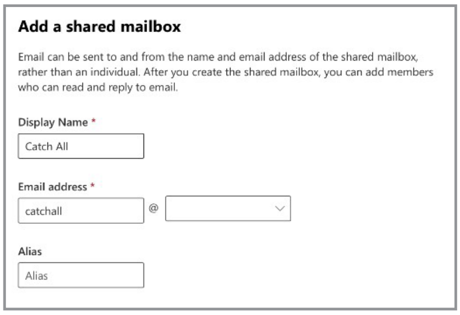
1. Still within the Exchange Online administration portal, in the menu on the left-hand side, select '**Recipients**' and then '**Mailboxes**'.



2. Click '**Add a shared mailbox**' and enter the below information in the panel on the right-hand side:

Display name: Name presented to recipients if sending email from this mailbox.

Email address: Enter '**catchall**' in the first textbox and select the organisation domain from the dropdown list.



Add a shared mailbox

Email can be sent to and from the name and email address of the shared mailbox, rather than an individual. After you create the shared mailbox, you can add members who can read and reply to email.

Display Name *
Catch All

Email address *
catchall @

Alias
Alias

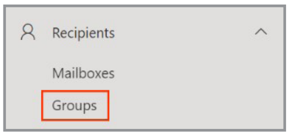
3. Click '**Create**'. A success message will display.

> ⓘ **NOTE:** It may take up to 30 minutes for the catch-all mailbox to become available.

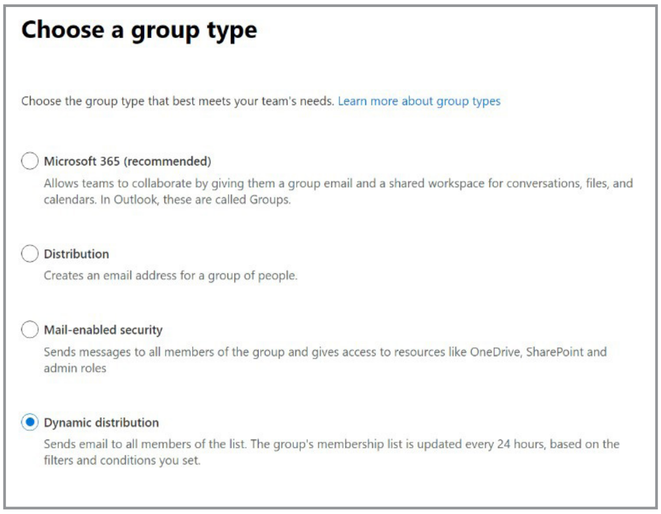
Step 3: Create Dynamic Distribution Group

> ⓘ **NOTE:** A Dynamic Distribution Group automatically changes based on configured rules. The rules within this step are configured so that as users are added to the Microsoft 365 tenant, their email stops being captured by the catch-all mailbox and will instead route to their new mailbox.

1. From the Exchange Online administration portal left-hand menu, select ‘**Recipients**’ and then select ‘**Groups**’.



2. Click ‘**Add a group**’, which will present the associated wizard screen.
3. Select the option for ‘**Dynamic distribution**’ and click ‘**Next**’.



Choose a group type

Choose the group type that best meets your team's needs. Learn more about group types

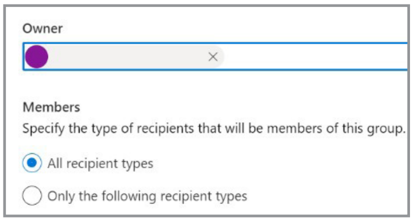
○ Microsoft 365 (recommended)
Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars. In Outlook, these are called Groups.

○ Distribution
Creates an email address for a group of people.

○ Mail-enabled security
Sends messages to all members of the group and gives access to resources like OneDrive, SharePoint and admin roles

● Dynamic distribution
Sends email to all members of the list. The group's membership list is updated every 24 hours, based on the filters and conditions you set.

4. In the ‘**Name**’ text box, type ‘**allusers**’ and select ‘**Next**’.
5. Click into the ‘**Owner**’ text box and select the email address for the currently signed-in administrator. Under the ‘**Members**’ heading, select ‘**All recipient types**’ and then click ‘**Next**’.

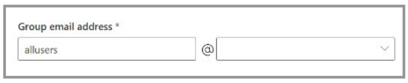


Owner

Members
Specify the type of recipients that will be members of this group.

● All recipient types
○ Only the following recipient types

6. Enter ‘**allusers**’ within the first box for the ‘**Group email address**’ and then select the organisation domain in the drop down on the right-hand side. Click ‘**Next**’.

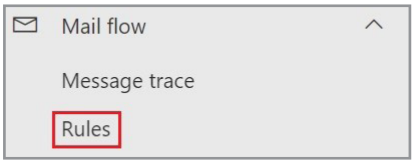


Group email address *
allusers @

7. Verify the details on the screen, and then click ‘**Create group**’. Once created, the system will present a success message.

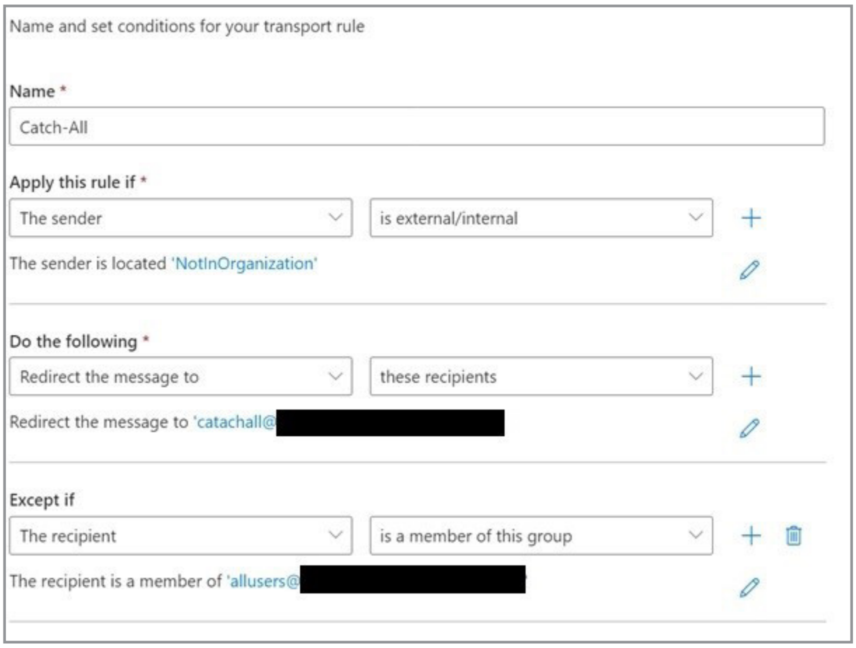
Step 4: Create Mail Flow Rule

1. From the Exchange Online administration portal left-hand menu, select ‘**Mail flow**’ and then select ‘**Rules**’.



2. Select ‘**Add a rule**’ from the popup menu, which will open a new right-hand side panel to configure the rule conditions.

3. In the ‘**Set rule conditions**’ panel configure the below settings and then click ‘**Next**’.
   a. Name: Catch-All
   b. Under ‘**Apply this rule if**’, select ‘**The sender**’ and in the second drop down box select ‘**is external/internal**’.
   c. Another panel will appear to ‘**Select sender location**’. Select ‘**Outside the organization**’ and then click ‘**Save**’.
   d. Under ‘**Do the following**’, select ‘**Redirect the message to**’ and in the second drop down box select ‘**these recipients**’.
   e. In the ‘**Select members**’ panel, select the catch-all mailbox created in Step 2 and the click ‘**Save**’.
   f. Under ‘**Except if**’, select ‘**the recipient**’, then select ‘**is a member of this group**’.
   g. In the ‘**Select members**’ panel that appears, select the ‘**All Users**’ dynamic distribution list created in Step 3 and then click ‘**Save**’.



Name and set conditions for your transport rule

Name *

Catch-All

Apply this rule if *

The sender | is external/internal

The sender is located 'NotInOrganization'

Do the following *

Redirect the message to | these recipients

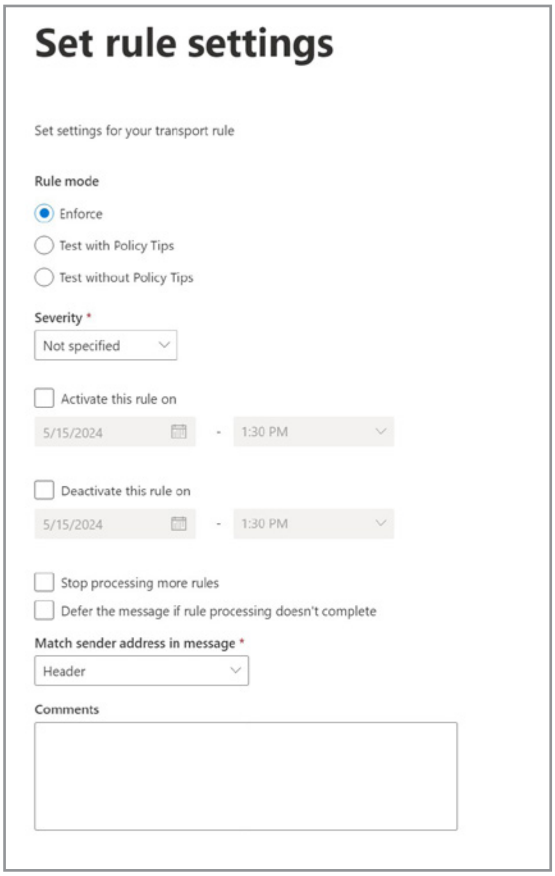
Redirect the message to 'catachall@[redacted]

Except if

The recipient | is a member of this group

The recipient is a member of 'allusers@[redacted]

4. Unless otherwise required, the default settings in the '**Set rule settings**' panel should be sufficient. Ensure the '**Rule mode**' is set to '**Enforce**' and then click '**Next**'.



Set rule settings

Set settings for your transport rule

Rule mode

● Enforce

○ Test with Policy Tips

○ Test without Policy Tips

Severity *

Not specified

□ Activate this rule on

5/15/2024 - 1:30 PM

□ Deactivate this rule on

5/15/2024 - 1:30 PM

□ Stop processing more rules

□ Defer the message if rule processing doesn't complete

Match sender address in message *

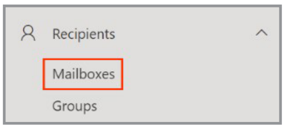
Header

Comments

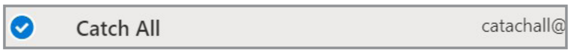
5. Review the created rule and then click '**Save**'.

Step 5: Manage Mailbox Delegation

1. From the Exchange Online administration portal left-hand menu, select '**Recipients**' and then select '**Mailboxes**'.

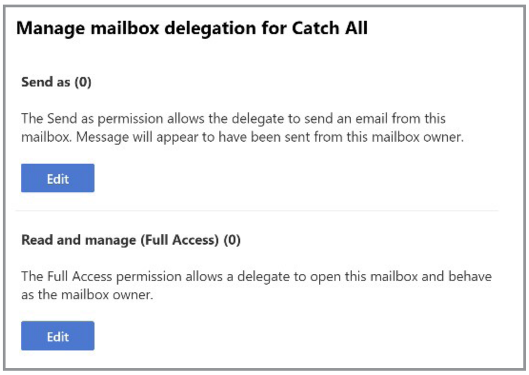


2. Select the radio button next to the '**Catch All**' mailbox.



3. In the menu that appears at the top, click '**Mailbox delegation**'.

4. In the ‘**Manage mailbox delegation for Catch All**’ panel that appears, click ‘**Edit**’ under ‘**Read and manage (Full Access)**’.



Manage mailbox delegation for Catch All

Send as (0)

The Send as permission allows the delegate to send an email from this mailbox. Message will appear to have been sent from this mailbox owner.

Edit

Read and manage (Full Access) (0)

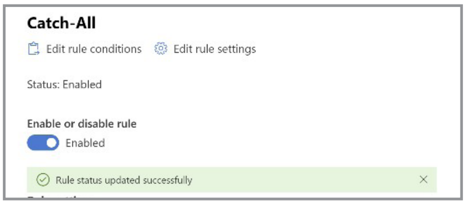
The Full Access permission allows a delegate to open this mailbox and behave as the mailbox owner.

Edit

5. Select ‘**Add members**’ and then select the administration user to add the user to the read and manage permissions for the catch-all mailbox. Click ‘**Save**’ and then ‘**Confirm**’ to apply the change.

Step 6: Enable the Mail Flow Rule

1. From the Exchange Online administration portal left-hand menu, select ‘**Mail flow**’ and then select ‘**Rules**’.
2. The Rules window will display again. This time, the ‘**Catch All**’ rule should appear in the table with its status set to ‘**Disabled**’. Click on the ‘Catch All’ rule name to open the rule properties.
3. Under ‘**Enable or disable rule**’ click on the toggle switch so that it shows as ‘**Enabled.**’ After a brief period, a message will display to say the rule status has updated successfully.



Catch-All

Edit rule conditions   Edit rule settings

Status: Enabled

Enable or disable rule

Enabled

Rule status updated successfully

4. The catch-all mailbox is now active. However, it may take up to 24 hours for all changes to take effect within the environment.
5. The configuration can be tested by sending two emails from an external email solution.
   a. The first email should go to the Administrator email address.
   b. The second email should go to a non-existent email address within the organisation.
   c. The email to the Administrator email address should be available within the Administrator’s individual mailbox, while the second email should go to the shared catch-all mailbox.

Appendix C: additional security settings

Business Continuity in a Box is designed to be used with a Business Standard Microsoft 365 licence to allow for rapid deployment using a trial licence. The security settings listed below were assessed as useful, though require an additional Entra P1 licence (included as part of a Business Premium licence). Organisations should assess their own operating context and add these licences to their tenant if required.

Microsoft Entra ID

Security Setting	Description	Reference	Where to change this
Set up Conditional Access to replace Security Defaults following best practices	Enable Multi-factor authentication for admin roles and standard users	Require MFA for all users	Conditional Access - Microsoft Entra admin centre
Secure the security info registration page	Deploy a Conditional Access policy to secure the process of registering your authentication methods	Control security information registration with Conditional Access	Conditional Access - Microsoft Entra admin centre
Require MFA to register or join devices	Require MFA in order to complete device registration or join operation	Require multifactor authentication for Intune device enrollments	Conditional Access - Microsoft Entra admin centre
Require Terms of Use	Require users to accept terms on an annual or semi-annual basis	Terms of use in Microsoft Entra ID	Conditional Access > Terms of Use - Microsoft Entra admin centre

Microsoft Exchange Online

Security Setting	Description	Reference	Where to change this
Enable Unified audit log	The activity log is not recording audit log data across all services by default; it needs to be enabled	Turn auditing on or off	Defender portal > Settings > Endpoints > Advanced features
Configure Alert policies	The alert policies can send notifications regarding suspicious events, or be leveraged to monitor other activities	Microsoft 365 alert policies	Defender portal > Policies & rules > Alert policy
Configure outbound spam policy, including block auto forward	Adversaries will often compromise mailboxes and set up forwarding rules to outside accounts	Configure outbound spam policies	Defender portal > Policies & rules > Threat policies > Anti-spam (outbound policy)

Security Setting	Description	Reference	Where to change this
Configure Audit log retention	By default, the audit log age limit is set to 90 days; if you have an E5 licensing, consider raising it (e.g. to 365 days)	Manage audit log retention policies	See Configure-Auditing.ps1
Email Encryption branding	Customise email encryption (OME) settings including branding	Add your brand to encrypted messages	PowerShell: see this article
Other settings for email encryption	Enable PDF encryption, check automatic decryption options (e.g. download attachments, journal reports etc.)	Manage Purview Message Encryption	See options for Set-IRM Configuration
Conditional Access (block attachment download)	Enable 'App enforced restrictions' to block attachment	Conditional Access in Outlook on the web for Exchange Online	See Block-UnmanagedDownload.ps1
Enable Auto-Expanding Archive	The default archive mailbox size is 100 GB; this can auto-expand the personal archive up to 1 TB	Enable auto-expanding archiving	See Setup-ArchiveLegalHold.ps1
Enable personal archive mailbox	The archive mailbox can store older messages, and policies can sweep aged items into the archive automatically	Enable archive mailboxes	See Setup-ArchiveLegalHold.ps1
Enable Litigation hold	Litigation hold will preserve all mailbox items for eDiscovery (even if deleted)	Create a Litigation hold	See Setup-ArchiveLegalHold.ps1

Microsoft Intune

Checklist Item	Description	Reference	Where to change this
Deploy App Protection Policies (a.k.a. MAM) for personally owned devices	Protect data inside mobile applications, and enable remote wipe capability (MAM)	Mobile Application Management (MAM) for unenrolled devices	Apps > App Protection policies
Configure Device enrolment restrictions	Blocks unsupported devices from enrolling, and limits the number of devices per user	Overview of enrolment restrictions	Devices > Enrolment > Device platform restriction OR Device limit restriction
Review the enrolment guides for each platform you intend to support	Choose which enrolment method(s) will work best for your organisation	Device enrolment guides for Microsoft Intune	N/A
Get an Apple Push Notification Certificate	You must setup a Push notification certificate through Apple (renewed annually)	Get an Apple MDM Push certificate for Intune	Devices > Enrolment > Apple

Checklist Item	Description	Reference	Where to change this
Prepare for Android enrolment	Block Android Device administrator and enable Android enterprise by connecting a Managed Google Play account	Android device enrolment guide for Microsoft Intune	Devices > Enrolment > Android
Prepare for Windows enrolment	Review auto-enrolment, Windows Hello, Enrolment Status Page, and Autopilot settings	Windows device enrolment guide for Microsoft Intune	Devices > Enrolment > Windows
Turn on Enrolment notifications	Turn on email notifications for enrolling new devices	Set up enrolment notifications in Intune	Each platform's enrolment page
Require MFA for Intune enrolment	Require MFA to complete Intune enrolment request (with every time sign-in frequency configured)	Require multifactor authentication for Intune device enrolment	Endpoint Security > Conditional access
Enrol devices	MAM devices do not need to be enrolled, MDM devices should enrol using the appropriate method	Device enrolment guides for Microsoft Intune	N/A
Set up Security groups	User-based groups is usually preferred unless there is a need for device-based	Add groups to organize users and devices in Microsoft Intune	Groups
Configure Windows Update for Business software Rings and Driver updates	Define Windows update rings to apply automatic updates; defer updates slightly for non-pilot users	Learn about using Windows Update for Business in Microsoft Intune	Devices > Windows 10 and later updates
Deploy Microsoft 365 Apps on Windows	Microsoft 365 apps will be auto-installed on devices (third party app may be deployed if preferred)	Add Microsoft 365 Apps to Windows devices using Microsoft Intune	Apps > All apps > Add
Configure Security Baselines	Harden Microsoft Windows, Edge, and Office apps with security baselines, or individual baseline policies	Learn about Windows security baselines you can deploy with Microsoft Intune	Endpoint Security > Security Baselines
Avoid conflicts between Security baseline, Device Configuration, and Endpoint Security	Conflicts mean that the setting will not be applied. Intune will not choose a "winner"	Avoid conflicts with Windows security baselines	N/A
Configure the Default Compliance policy settings	Devices without an assigned compliance policy should be marked as 'non-compliant'	Compliance Policy Settings	Devices > Compliance > Policies
Configure Device Compliance policies	Each type of device under management should have a compliance policy for use with Conditional access	Device compliance policies	Devices > Compliance > Policies

Checklist Item	Description	Reference	Where to change this
Enable Device-based Conditional access	Non-compliant devices will be unable to access company apps and data	Set up device-based Conditional Access policies with Intune	Devices > Conditional access
Use filters for more granular targeting	Filters can help target specific policies, by including or excluding device properties	Create filters in Microsoft Intune	Tenant administration > Filters
Control mobile experiences with App configuration policies	Control in-app experiences, based on managed apps (e.g. outlook) or managed devices (e.g. Work profile for Android)	App configuration policies for Microsoft Intune	Apps > App configuration policies
Customise Company portal	Configure branding, privacy URL, and define the support contact displayed in the Company Portal	How to configure the Intune Company Portal apps, Company Portal website, and Intune app	Tenant administration > Customization
Create the Company terms and conditions	Skip this step is you are using Conditional access for Terms of Use	Set terms and conditions in Microsoft Intune	Tenant administration > Terms and conditions
Configure device clean-up	Delete devices based on the last check-in date (e.g. 60-90 days)	Automatically delete devices with clean-up rules	Devices > Device clean-up rules
Use policy sets to simplify management	Group compliance policies, configuration profiles, app assignments and more into a single, assignable policy	Policy sets in Microsoft Intune	Devices > Policy sets > Policy sets

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre