

Microsoft 365 / Entra ID Lab
Thomas McSherry
thomas.e.mcsherry@gmail.com

Objectives

For this project, I want to familiarize myself with Microsoft 365 concepts and practices. To facilitate this, I acquired a trial Microsoft 365 Business standard license. From there, I will set up users with Entra ID, assign appropriate groups and relevant privileges following best security practices. Then I will configure and test multi-factor authentication, configure outlook and shared files. Lastly, I will simulate a potential ticket one might receive in a help desk role and resolve it accordingly.

User/Groups Setup

To begin, I created a handful of accounts with appropriate display names and usernames as well as licenses:

Active users

Add a user	User templates	Add multiple users	Multi-factor authentication	Delete a user	Refresh	Reset password
Filter set: Commonly used						
<input type="checkbox"/> Display name ↑	Username	Licenses				
<input type="checkbox"/> Alicia Charming	: a.charming@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard				
<input type="checkbox"/> Computer Enthusiast	: c.enthusiast@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard				
<input type="checkbox"/> John Handsome	: j.handsome@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard				
<input type="checkbox"/> Normal Individual	: n.individual@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard				
<input type="checkbox"/> Regular Person	: r.person@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard				
<input type="checkbox"/> Thomas McSherry	: ThomasMcSherry@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard				



Alicia Charming

[Reset password](#) [Block sign-in](#) [Change photo](#)

Account Devices **Licenses and apps** Mail OneDrive

Select location *

United States

Licenses (2)

- Azure Active Directory Premium P1**
19 of 25 licenses available
- Microsoft 365 Business Standard**
19 of 25 licenses available

Entra ID Group/Role Management

In this case, I will have the Computer Enthusiast account be in an IT group and have some privileges, with the rest if the accounts being general users. In case of a potential compromise of a user, it's important to follow principles of least privilege to dampen potential damage.

Firstly, I assigned users to the RegularUsers group:

The screenshot shows the 'RegularUsers | Members' group page in the Azure portal. The left sidebar has 'Overview' and 'Diagnose and solve problems' under 'Manage'. The 'Members' tab is selected. The main area shows a search bar and a table of group members. The table has columns for Name, Type, and Email. The members listed are:

Name	Type	Email
AC Alicia Charming	User	a.charmin
JH John Handsome	User	j.hanson
NI Normal Individual	User	n.individu
RP Regular Person	User	r.person@

Then, I assigned the "Helpdesk Administrator" role to the IT Department security group. I chose this specific role as its scope of privilege is limited.

The screenshot shows the 'Assigned roles' section for the 'IT Department' group. On the left, there's a sidebar with links like 'Overview', 'Diagnose and solve problems', 'Properties', 'Members', 'Owners', 'Roles and administrators', and 'Administrative units'. The main area has a search bar and a table with columns 'Role' and 'Description'. One row is selected, showing the 'Helpdesk Administrator' role with the description: 'Can reset passwords for non-administrators and Helpdesk Administrators.'

Role	Description
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.

Multi Factor Authentication

Despite the default emphasis on the Microsoft Authenticator app for MFA, I want to configure a different layer as organizations can differ in standards and policy. To try this out, I enforced an SMS verification on the IT Department Group.

The screenshot shows the 'SMS settings' page. Under the 'Enable and Target' section, the 'Enable' toggle is turned on. The 'Target' dropdown is set to 'Select groups', and the 'IT Department' group is listed in the table below. The table has columns 'Name', 'Type', 'Use for sign-in', and 'Registration'. The 'IT Department' entry shows it is a 'Group' type, checked for 'Use for sign-in', and has 'Optional' selected for 'Registration'.

Name	Type	Use for sign-in	Registration
IT Department	Group	<input checked="" type="checkbox"/>	Optional

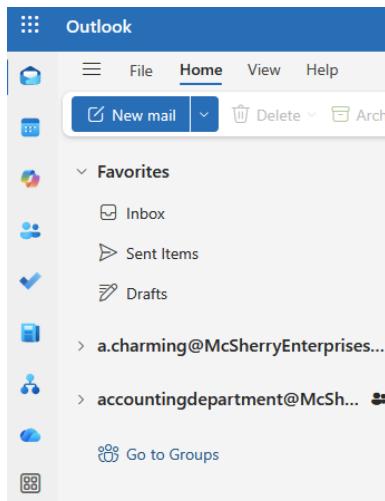
After assigning a phone number to the Computer Enthusiast account, I attempted logging in using the SMS code, which worked.

Configuring a Shared Mailbox

To simulate a common task, I created a shared mailbox for the “Finance Department”, and delegate specific permissions to mirror real-world applications.

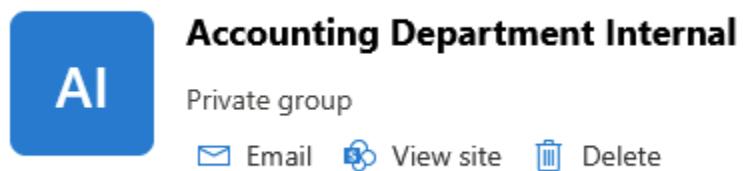


To verify my steps were correct, I logged into the Alicia Charming account on Outlook and added the shared mailbox, through SMS authentication.



Sharepoint / Teams

A big part of the Microsoft 365 suite is allowing collaboration between members in a business. To facilitate this teams and sharepoint are used. First, I'm going to create a Microsoft 365 group based on the Accounting department.



I then navigated to SharePoint and then configured it appropriately.

The screenshot shows the "Site Information" configuration page for the "Accounting Department Internal" site. The page includes the following fields:

- Site name ***: Accounting Department Internal
- Site description**: Accounting Department Internal
- Hub site association**: A dropdown menu currently showing a single option.
- Privacy settings**: Set to "Private - only members can access this..." with a dropdown arrow.
- View all site settings**: A blue link at the bottom of the configuration area.
- Delete site**: A button with a trash can icon at the bottom of the page.

[Site sharing settings](#)

Control how things in this site can be shared and how request access works.

Sharing permissions

- Site owners and members can share files, folders, and the site. People with Edit permissions can share files and folders.
- Site owners and members, and people with Edit permissions can share files and folders, but only site owners can share the site.
- Only site owners can share files, folders, and the site.

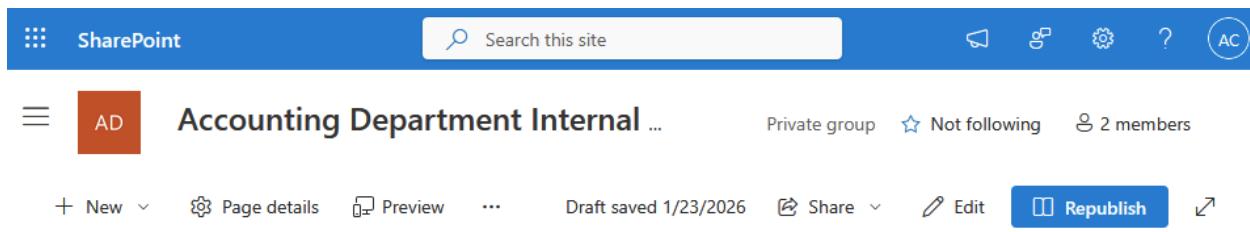
Access requests

Allow access requests  On

Choose who will receive access requests for this site:

- Accounting Department Internal Owners
- Specific email

I then created a sample Documents library, and tested it on my Alicia Charming account to confirm access.



Then I followed the site, so it would show up in the end-user's homepage.

Conclusion

The scope of this lab covered configuring and testing Microsoft 365 + Entra ID services/applications to reflect common tasks, while reinforcing foundational concepts. The creation of users and group assignment reflected common tasks such as onboarding, assigning role based access control as well as how cybersecurity fundamentals such as IAM are used. The configuration of SMS-based MFA within Entra ID allowed a grasp of how MFA is used to follow best security practices, as well as showing steps for potential troubleshooting tasks. The deployment of an Outlook Shared mailbox and a Teams-based sharepoint site exposed how groups and users from 365 / Entra ID translate to applications within the 365 suite. Testing these configurations from an end-user perspective reinforced troubleshooting skills to resolve issues governing access and permission.