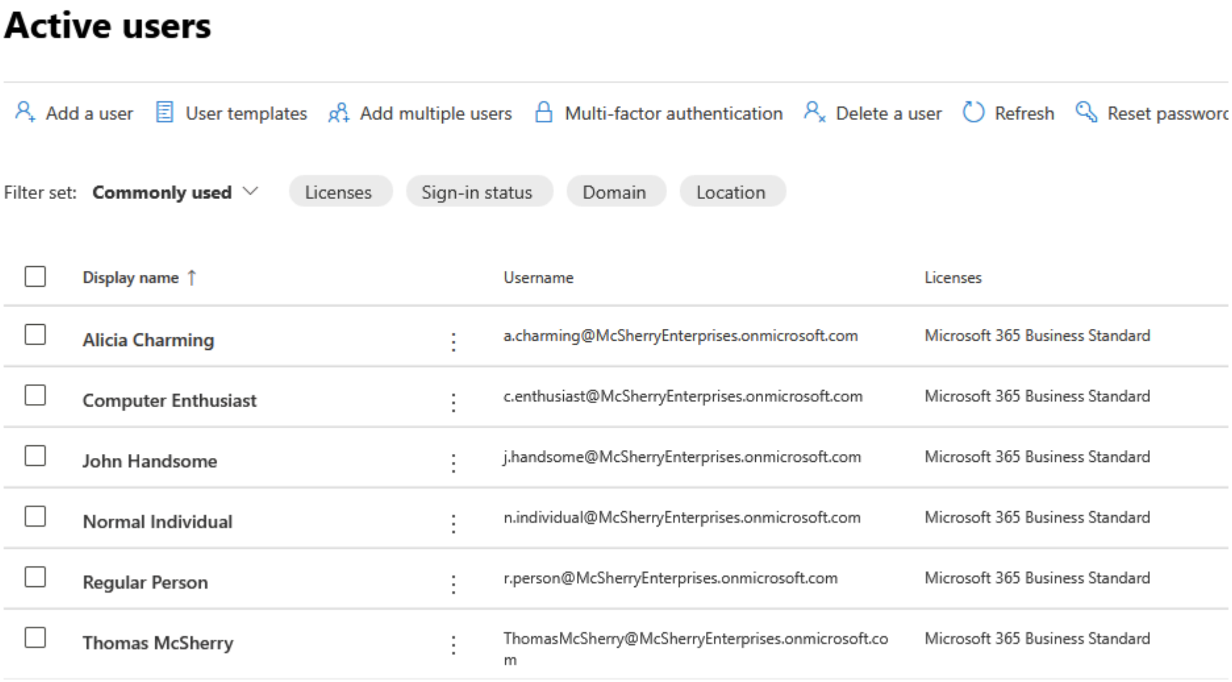
Microsoft 365 / Azure Entra ID Lab
Thomas McSherry
thomas.e.mcsherry@gmail.com

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

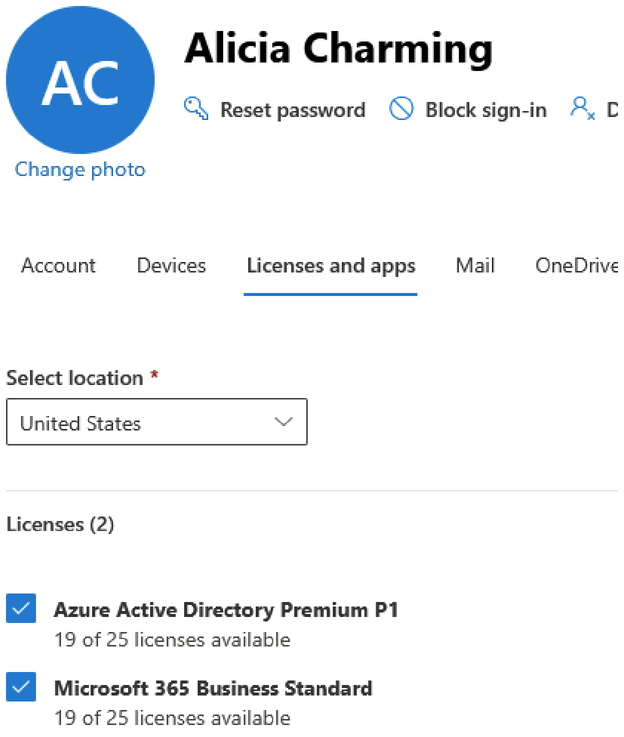
To begin, I created a handful of accounts with appropriate display names and usernames as well as licenses:



Active users

Filter set: **Commonly used**

☐	Display name ↑	Username	Licenses
☐	Alicia Charming	a.charming@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard
☐	Computer Enthusiast	c.enthusiast@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard
☐	John Handsome	j.handsome@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard
☐	Normal Individual	n.individual@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard
☐	Regular Person	r.person@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard
☐	Thomas McSherry	ThomasMcSherry@McSherryEnterprises.onmicrosoft.com	Microsoft 365 Business Standard



Alicia Charming

Select location *

United States

Licenses (2)

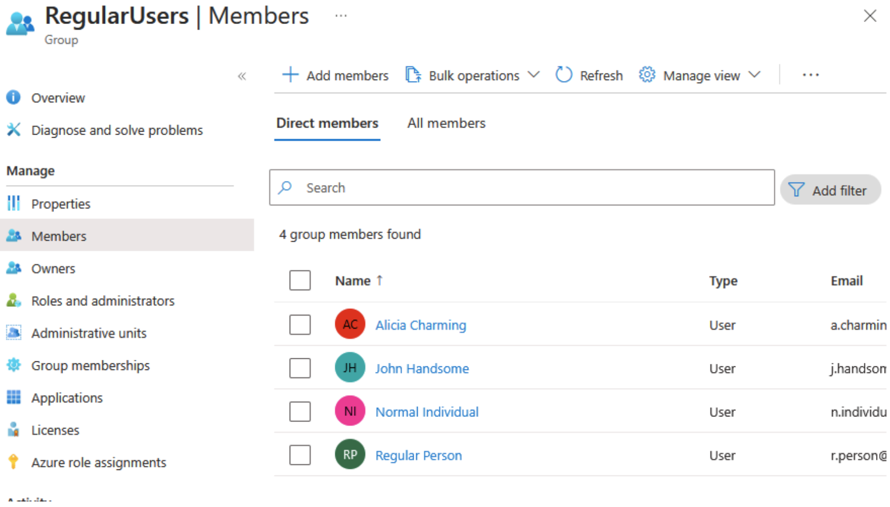
☑ **Azure Active Directory Premium P1**
19 of 25 licenses available

☑ **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.

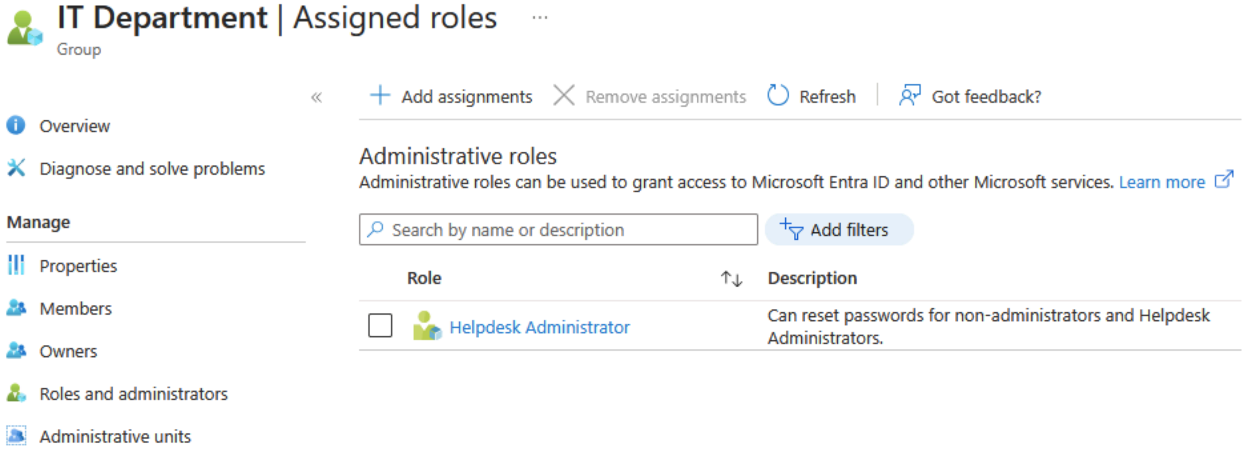
Firstly, I assigned users to the RegularUsers group:



4 group members found

Name ↑	Type	Email
AC Alicia Charming	User	a.charmin
JH John Handsome	User	j.handson
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.



IT Department | Assigned roles

Group

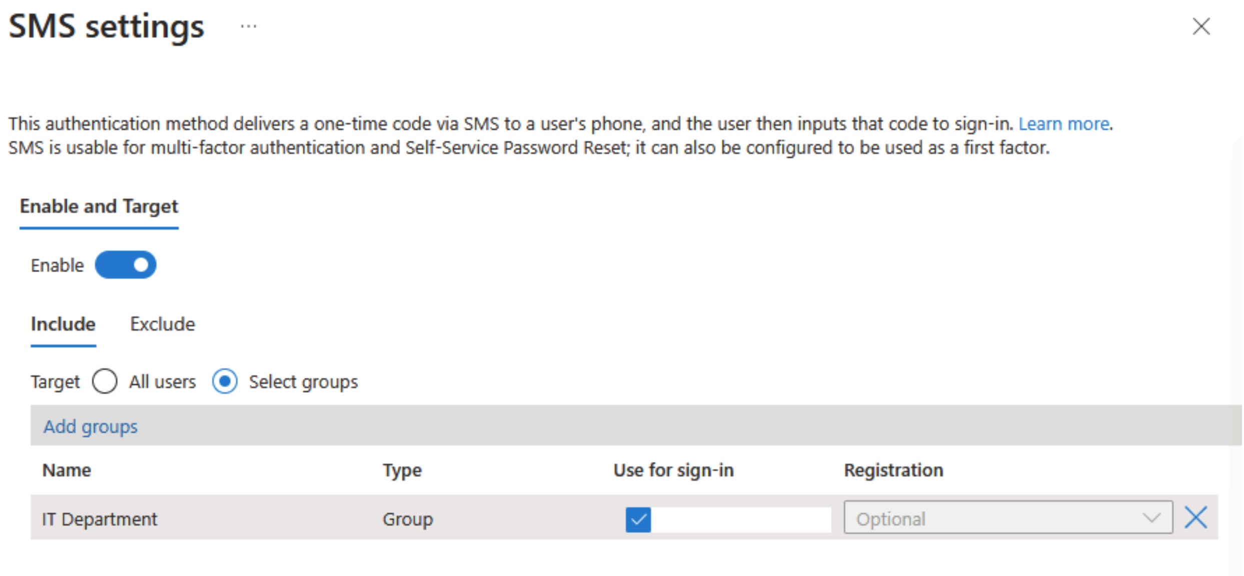
Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

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

Multi Factor Authentication

Despite the default emphasis on the Microsoft Authenticator act 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.



SMS settings

This authentication method delivers a one-time code via SMS to a user's phone, and the user then inputs that code to sign-in. Learn more.
SMS is usable for multi-factor authentication and Self-Service Password Reset; it can also be configured to be used as a first factor.

Enable and Target

Enable: On

Include | Exclude

Target ○ All users ● Select groups

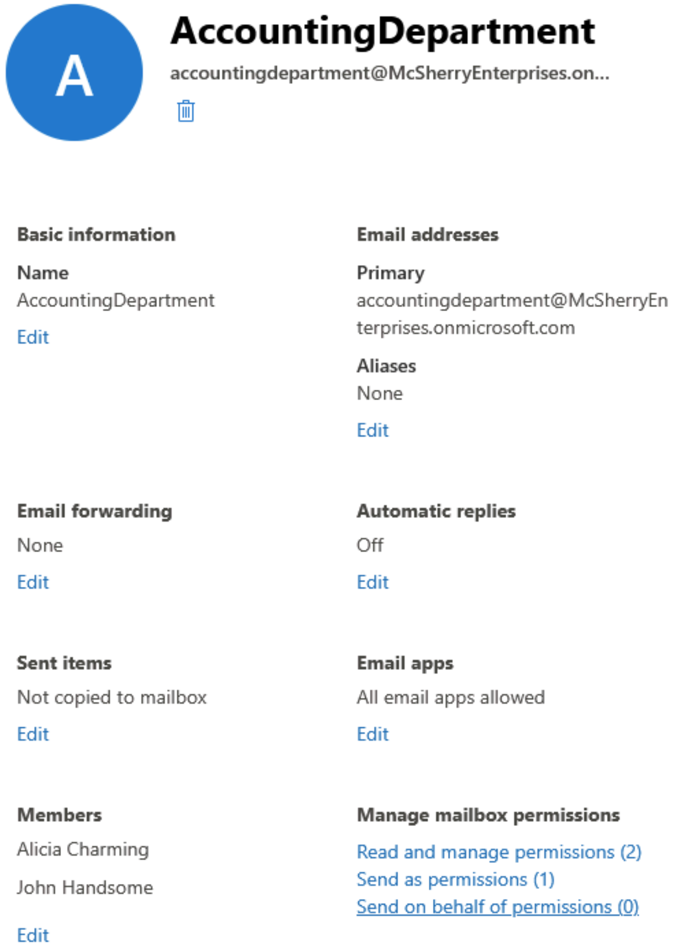
Add groups

Name	Type	Use for sign-in	Registration
IT Department	Group	☑	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.



AccountingDepartment

accountingdepartment@McSherryEnterprises.on...

Basic information

Name
AccountingDepartment
Edit

Email addresses

Primary
accountingdepartment@McSherryEnterprises.onmicrosoft.com

Aliases
None
Edit

Email forwarding

None
Edit

Automatic replies

Off
Edit

Sent items

Not copied to mailbox
Edit

Email apps

All email apps allowed
Edit

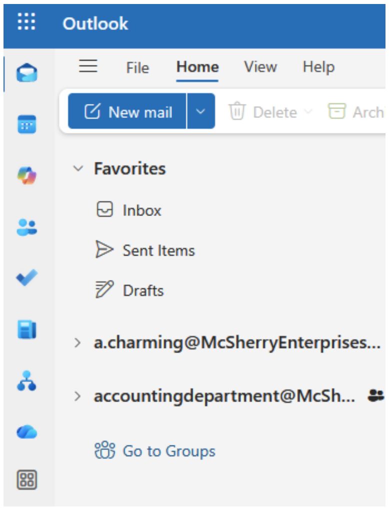
Members

Alicia Charming
John Handsome
Edit

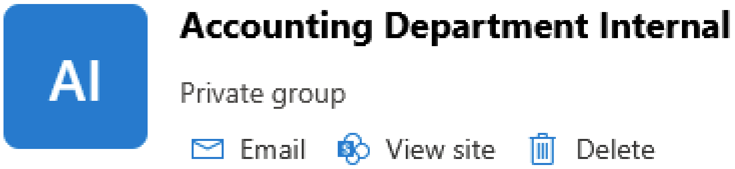
Manage mailbox permissions

Read and manage permissions (2)
Send as permissions (1)
Send on behalf of permissions (0)

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



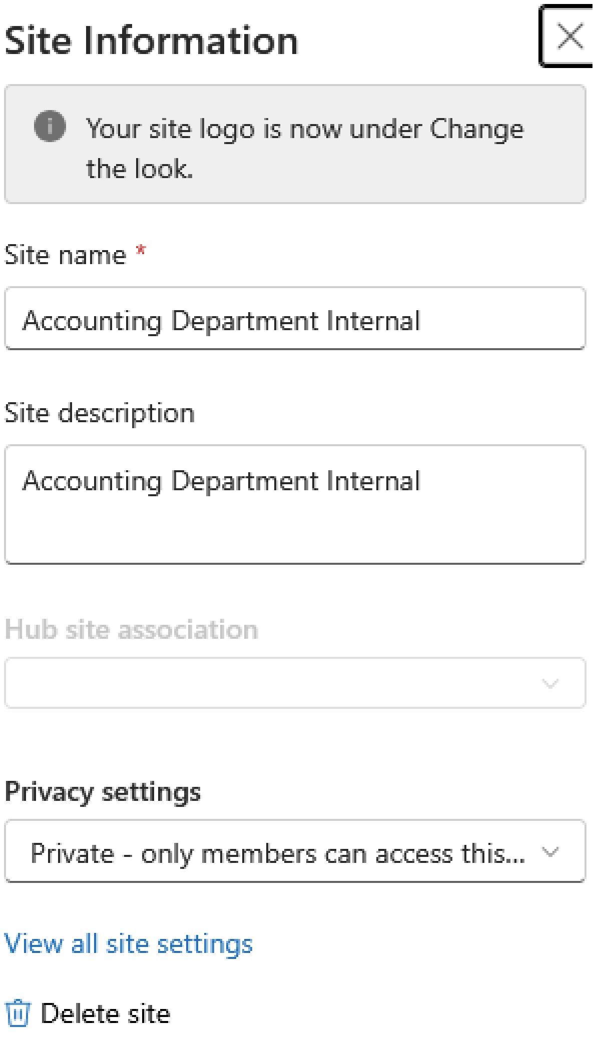
Sharepoint / Teams
A big part of the Microsoft 365 suite is allowing collaboration between members in a business. To facilitate this teams and sharepoint are used. First, I'm going to create a Microsoft 365 group based on the Accounting department.



Accounting Department Internal

Private group

I then navigated to SharePoint and then configured it appropriately.


Site Information

Your site logo is now under Change the look.

Site name *

Accounting Department Internal

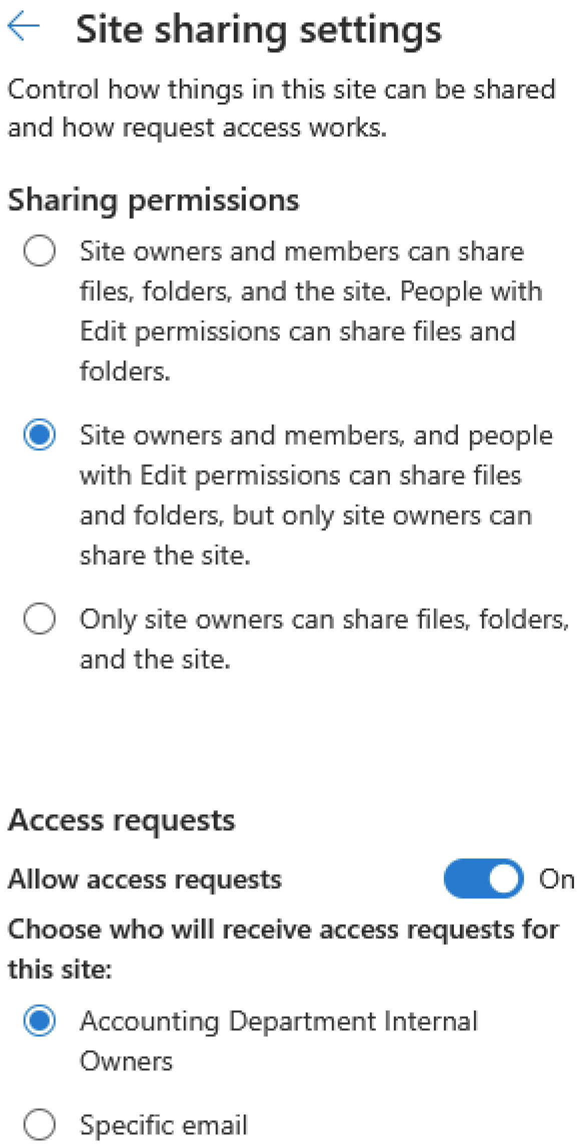
Site description

Accounting Department Internal

Hub site association

Privacy settings

Private - only members can access this...



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

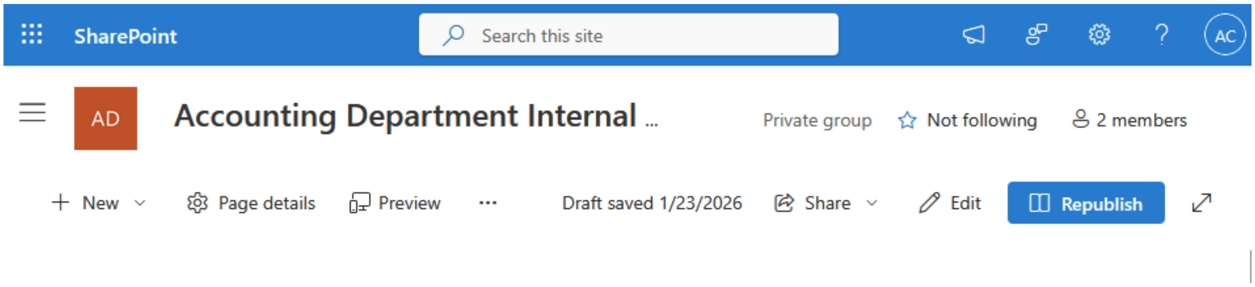
Allow access requests On

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.