

Integrating Microsoft 365

<https://campus.barracuda.com/doc/96767914/>

Prerequisites

- Ensure you have enabled Audit Log Search. ([Microsoft docs](#))
- Register an application in Entra ID. ([Microsoft docs](#))
- Once application is registered, take note of the **Application (client) ID** and the **Directory (tenant) ID**.
- Configure app authentication in the **Certificates & Secrets** screen.
- Add API permissions and grant admin consent.
- Enter the **application id**, **directory id**, and **application secret** in **Barracuda XDR Dashboard**.

Enable Audit Logging For All Mailboxes in Microsoft 365

To enable audit logging for all mailboxes in Microsoft 365, do one of the following procedures:

- To enable audit logging through Admin Center (recommended)
- To enable audit logging via Powershell

To enable audit logging through Admin Center

You can use the **Security & Compliance Center** to turn on audit log search in Microsoft 365. It may take several hours after you turn on audit log search before you can return results when you search the audit log. You must be assigned the **Audit Logs** role in Exchange Online to turn on audit log search.

1. Navigate to `Portal.office.com`, and navigate to the **Admin center** on the left side.
2. On the left side, click **Show All**.
3. Click **Compliance** tab to open **Microsoft Purview**.
4. In **Microsoft Purview**, select **Audit**.
A banner is displayed saying that auditing must be turned on to record user and admin activity.
5. Click **Turn on auditing**.
The banner is updated to say the audit log is being prepared and may take a few hours, before taking full effect. (This could result in this integration not working right away.)

If you don't see the **Turn on auditing** banner at the top, that means auditing is already enabled.

Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

[Turn on auditing](#)

Search

[Clear](#)

Activities

Show results for all activities ▼

Start date

2019-09-23



00:00



End date

2019-10-01



00:00



Users

Show results for all users

File, folder, or site ⓘ

Add all or part of a file name, folder name, or URL.

Search

Results

Date ▼	IP address	User	Activity	Item
--------	------------	------	----------	------

To enable audit logging via Powershell

If you find any issues using the above instructions, you can also use Exchange Powershell to enable auditing for your tenant, .

1. Connect to **Exchange Online Powershell**.
2. Run the following Powershell command to turn on auditing.

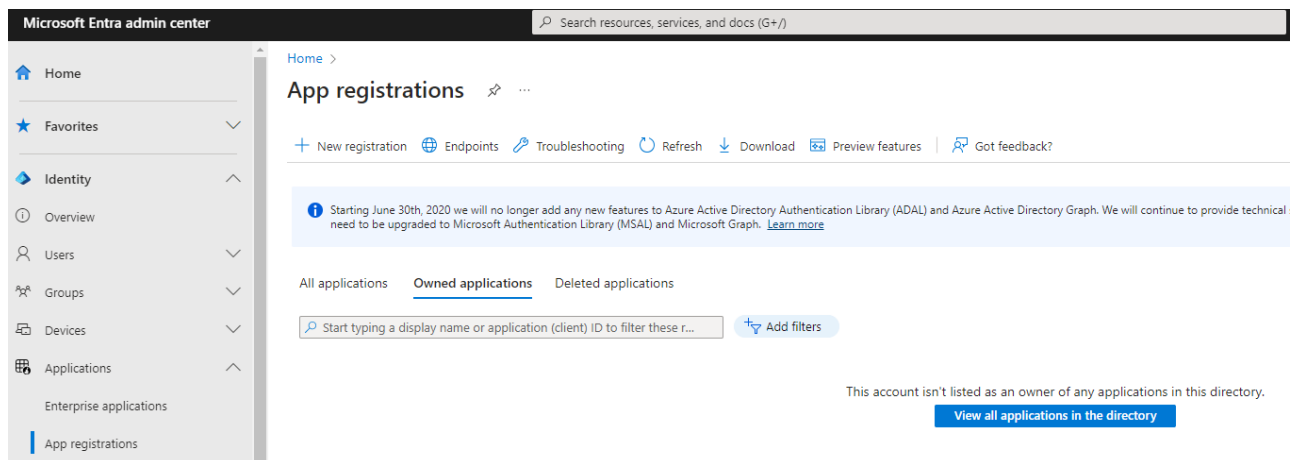
```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```
3. A message displays, saying that it may take up to 60 minutes for the changes to take effect.

You can find additional Powershell commands [here](#) .

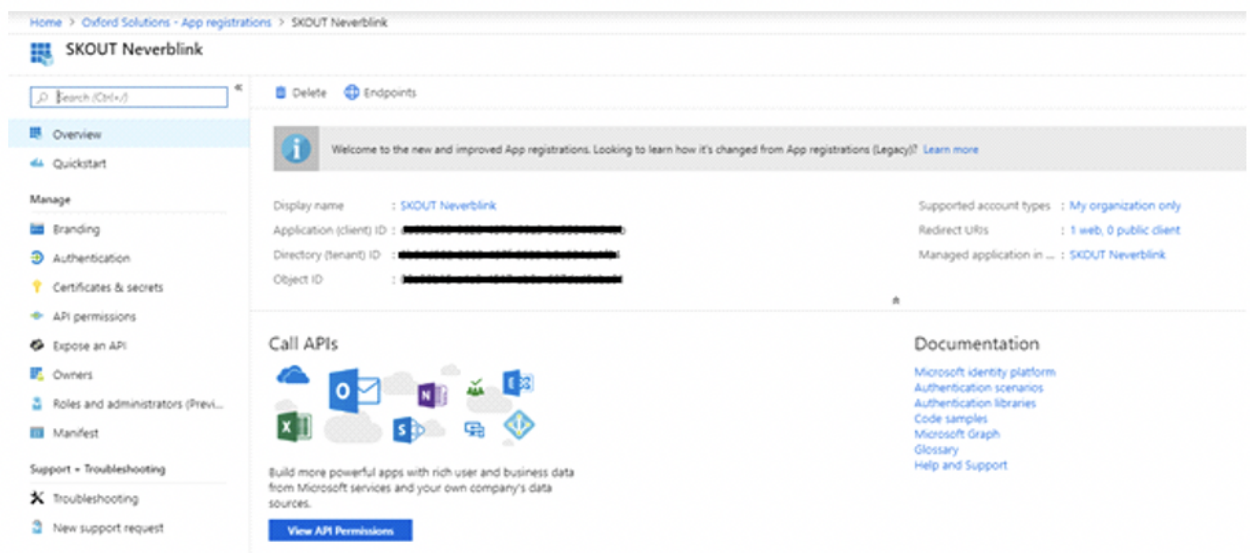
Configuring Microsoft 365

ALL steps require Microsoft 365/Azure Administrative privileges.

1. Log on to <https://portal.office.com/adminportal>
2. On the left side, click **Show All** and go to **Admin Center > Entra ID**.
3. Under **Favorites**, click **Entra ID**, and under **Manage Column**, navigate to **App Registrations**.



4. Click New Registration.
5. Fill in the Application Information::
 - In **Name**, enter SKOUTCYBERSECURITY.
 - Enable the **Accounts in this organizational directory only (domain - Single Tenant)** checkbox.
 - **Redirect URL** can be left blank.
6. You are redirected to another page. Copy the **Application ID** and **Directory (tenant) ID**, so you can input them into the **Security** dashboard once completed, or paste them in now without saving.



7. Under **Manage** on the left, click **API Permissions** > **Add a permission**.
8. From the list, select **Microsoft 365 Management API's** and open **Application permissions**.
9. From the list of **Application Permissions**, check all the options with **Read** privileges (those ending in .Read), then click **Add Permissions**.

The picture below may be different in your case, and will most likely have fewer permissions showing.

Home > Oxford Solutions - App registrations > SKOUT Neverlink - API permissions

SKOUT Neverlink - API permissions

Search: CH1x2

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up in grants/deny access.

[Add a permission](#)

API / PERMISSION NAME	TYPE	DESCRIPTION
Microsoft Graph (1)	Delegated	Sign in and read...

[View Read](#)

Grant consent

To consent to permissions that require admin consent, please sign in with an account that is an administrator.

[Grant admin consent for Oxford Solutions](#)

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

PowerApps Runtime Service
Powerful data storage, modeling, security and integration capabilities

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

Yammer
Access resources in the Yammer web interface (e.g. messages, users, groups etc.)

Request API permissions

[← All APIs](#)

Office 365 Management APIs

<https://manage.office.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[collapse all](#)

Type to search

Permission

Admin consent required

▼ **ActivityFeed (2)**

<input checked="" type="checkbox"/>	ActivityFeed.Read Read activity data for your organization ⓘ	Yes
<input checked="" type="checkbox"/>	ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ⓘ	Yes

▼ **ServiceHealth (1)**

<input checked="" type="checkbox"/>	ServiceHealth.Read Read service health information for your organization ⓘ	Yes
-------------------------------------	---	-----

Add permissions

Discard

10. Optionally, if you want to support remediation actions (disable user logins), add one more permission by doing the following.

1. Click **Add a permission** again.
2. Click **Microsoft Graph**.
3. Select **Application permissions (not delegated)**.
4. Select **User.ReadWrite.All**.
5. Click **Add permissions** to save the change.
6. If this is an update to a previously-configured app, make sure to click **Grant admin consent** after adding the new permission.

Request API permissions


[← All APIs](#)


Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

×

Permission	Admin consent required
> IdentityRiskyUser	
∨ User (1)	
<input checked="" type="checkbox"/> User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

11. You should now be back on the **API permissions Overview** page. Select **Grant admin consent for Domain**.

[All services](#) > [Skout Demo 2: Money Matters Accountants](#) > [SKOUT CYBERSECURITY](#)

SKOUT CYBERSECURITY | API permissions
✕

«
🔄 Refresh
💡 Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

📘

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

×

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+

Add a permission

✓ Grant admin consent for Skout Demo 2: Money Matters Accountants

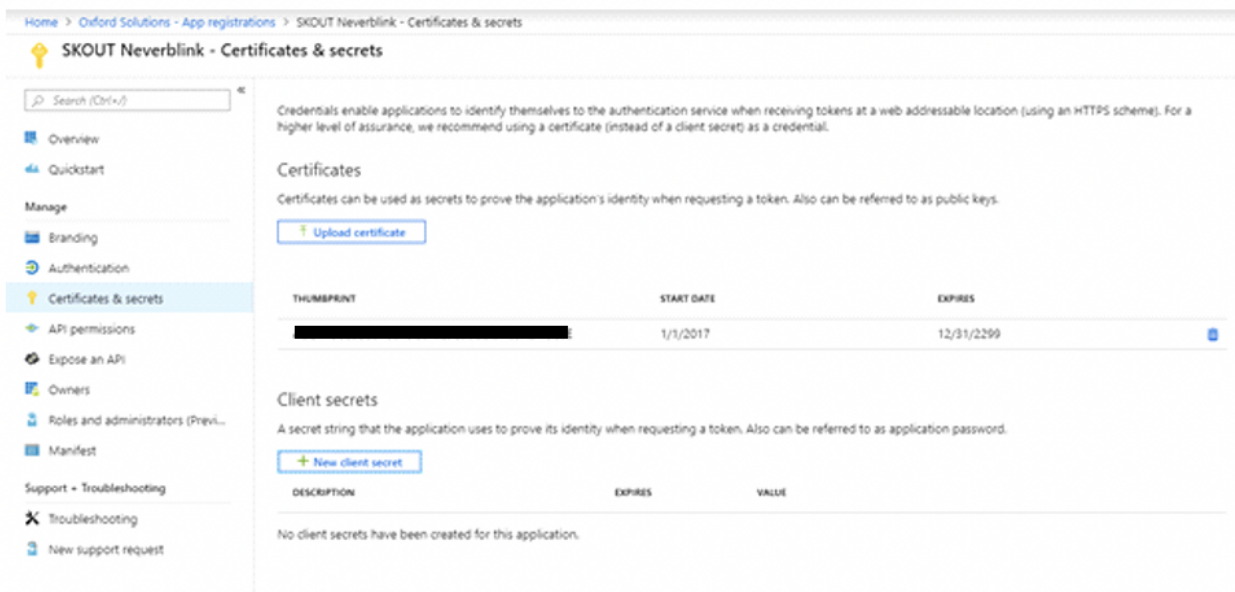
API / Permissions n...	Type	Description	Admin consent req...	Status
∨ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Skout Dem... ⋮
∨ Office 365 Managem...				
ActivityFeed.Read	Application	Read activity data for your ...	Yes	✓ Granted for Skout Dem... ⋮
ActivityFeed.ReadI	Application	Read DLP policy events incl...	Yes	✓ Granted for Skout Dem... ⋮
ServiceHealth.Reac	Application	Read service health inform...	Yes	✓ Granted for Skout Dem... ⋮

To view and manage permissions and user consent, try [Enterprise applications](#).

12. Click **Certificates & Secrets**.

Integrating Microsoft 365

6 / 10

13. Click **New Client Secret**.

Home > Oxford Solutions - App registrations > SKOUT Neverblink - Certificates & secrets

SKOUT Neverblink - Certificates & secrets

Search (Ctrl+K)

Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previous version)
Manifest
Support > Troubleshooting
Troubleshooting
New support request

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

THUMBPRINT	START DATE	EXPIRES
[REDACTED]	1/1/2017	12/31/2299

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[New client secret](#)

DESCRIPTION	EXPIRES	VALUE
-------------	---------	-------

No client secrets have been created for this application.

14. In **Description**, type Barracuda XDR .15. In **Expires**, select **24 months**, then click **Add**.

All services > Skout Demo 2: Money Matters Accountants > SKOUT CYBERSECURITY

SKOUT CYBERSECURITY | Certificates & secrets

Search (Ctrl+ /)

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Credentials enable confidential access to an addressable location (using an OAuth 2.0 client secret) as a credential.

Certificates

Certificates can be used as secret keys.

Upload certificate

Thumbprint

No certificates have been added

Client secrets

A secret string that the application uses as a password.

New client secret

Description

No client secrets have been created

Add a client secret

Description

SKOUT

Expires

24 months

Add

Cancel

All services > Skout Demo 2: Money Matters Accountants > SKOUT CYBERSECURITY

SKOUT CYBERSECURITY | Certificates & secrets

Search (Ctrl+/) << Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators | Preview
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
SKOUT	10/18/2023	bx17Q~Ao3UWcZPf2Nue6...	9dfc3d5a-5e1d-4028-bd2...

16. Save the value to your notes. You'll need to paste it into the **Barracuda XDR Dashboard** setup screen.

To verify connection and permissions

1. In **Barracuda XDR Dashboard**, click **Administration > Integrations**.
2. On the **Microsoft 365** card, click **Setup**.
 If you have already set up the integration, click **Update**.
3. Paste the **application ID**, **directory ID**, and **secret** value that you saved from the above steps.
4. Click the **Test** button to verify connection & permissions.
5. Click **Save**.

It may take some time for Microsoft's changes to take effect. If the test function says there's no data yet, try saving the settings anyway.

Figures

1. 1.png
2. Screenshot 1.png
3. setup.o365.4copyIds.png
4. setup.o365.5selectApi.png
5. setup.o365.6apiPermissions.png
6. setup.o365.user-read-write-all.png
7. capture1.png
8. setup.o365.8newSecret.png
9. capture2.png
10. capture3.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.