Netsurion®

Integration Guide

Integrate Microsoft 365 with Netsurion Open XDR

Publication Date

September 22, 2023

Abstract

This guide provides instructions to configure and integrate Microsoft 365 with Netsurion Open XDR to retrieve its logs via API and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Microsoft 365 (E3, E5, F3 licenses for Enterprise; Basic, Standard, Premium licenses for Business; G3, G5 licenses for Government Community Cloud (GCC), GCC High and Department of Defense (DoD) subscriptions), and Netsurion Open XDR 9.3 and later.

Note:

Message trace monitoring is not supported for Microsoft 365 Government Community Cloud (GCC),and then, GCC High and Department of Defense (DoD) customers.

Audience

This guide is for the administrators responsible for configuring and monitoring Microsoft 365 in Netsurion Open XDR.

Table of Contents

1 Overview

Microsoft 365 is a cloud-based subscription service that combines best-in-class apps like Excel and Outlook with powerful cloud services such as OneDrive and Microsoft Teams. Microsoft 365 helps to create and share anywhere on any device.

Microsoft 365 Data Source Integration for Netsurion Open XDR captures important activities in Exchange, Azure Active Directory, SharePoint, OneDrive, and Teams. Monitoring these activities is critical from a security aspect and necessary for compliance reasons. Refer to the introduction of protecting Microsoft 365 for more details.

Netsurion Open XDR manages logs retrieved from Microsoft 365. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Microsoft 365.

2 Prerequisites

- Windows 10 and above, or Windows server 2019 and above with desktop experience.
- **PowerShell 5.0** should be available on the machine where you will run the integrator.
- Ensure **Auditing** is enabled on your tenant.

Note:

To integrate with the Business license refer to the instructions in Search the audit log or Configuring Microsoft 365 Unified Audit guide for more details.

Note:

Wait for a day to configure Microsoft 365 integrator.

- The application must be registered in Azure AD (Microsoft Entra ID). Refer to the Registering Application with Azure Active Directory section for instructions.
- The application must have API permission for Office 365 Management, Microsoft Graph, and Office 365 Exchange Online. Refer to the Adding Permissions to access APIs section for instructions.
- Microsoft 365 application must have the **Security Reader Role**. Refer to the Adding Security Reader Role section for instructions.

Note:

If the application is already registered and has the API permission for Office 365 Management, and Microsoft Graph, then ensure to add the Office 365 Exchange Online permission and the Security Reader Role.

- Enable the following URLs if there is any web filter or firewall in between:
  - https://graph.microsoft.com
  - https://login.windows.net
  - https://manage.Microsoft.com
  - https://reports.office365.com

- Uninstallation of the legacy version (below v3.0.0) of the Microsoft 365 Integrator (if configured).

> **Note**
>
> Refer to How To Uninstall Microsoft 365 Integrator guide to uninstall any legacy version (below v3.0.0) of the Microsoft 365 integrator installed in the system. This process is mandatory before installing the Microsoft integrator version 3.x.x.

- Upgradation of the existing version (v3.0.0) of Microsoft 365 Integrator (if configured).

> **Note**
>
> Refer to How-To-Upgrade-Microsoft-365-Netsurion guide to upgrade the Microsoft 365 integrator from v3.0.0 to v3.1.0. There is no need to follow further instruction in this document when the integrator is being upgraded.

- The Data Source Integration package.

> **Note**
>
> To get the Data Source Integration package, contact your Netsurion Account Manager.

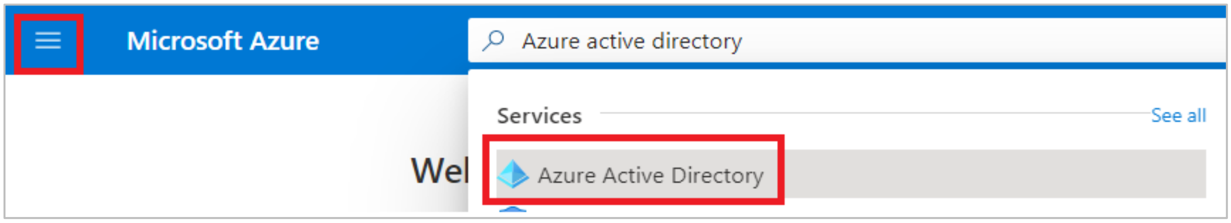
3 Configuring Microsoft 365 Application and Permission

3.1 Registering Application with Azure Active Directory Tenant/ Organization

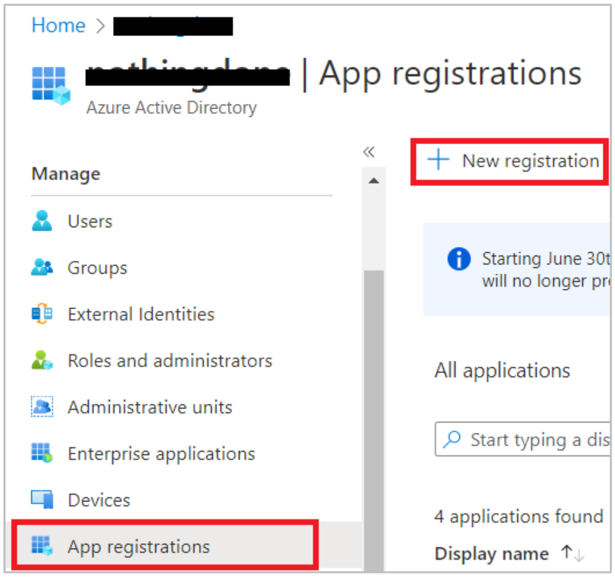
Perform the following process if the application is not registered with Azure AD.

> **Note**:
>
> To perform this process, make sure the user has the **Global Administrator** rights in Microsoft 365.

1. Sign in to the Azure portal.
2. In the case of more than one tenant, click your account in the top right corner, and set the portal session to the desired Azure AD tenant.
3. In the **Microsoft Azure** console, either click the left-hand navigation pane or type **Azure Active Directory** in the search bar to go to the Azure Active Directory service.



4. Click the **Azure Active Directory** service, click **App registrations**, and then click **New registration**.

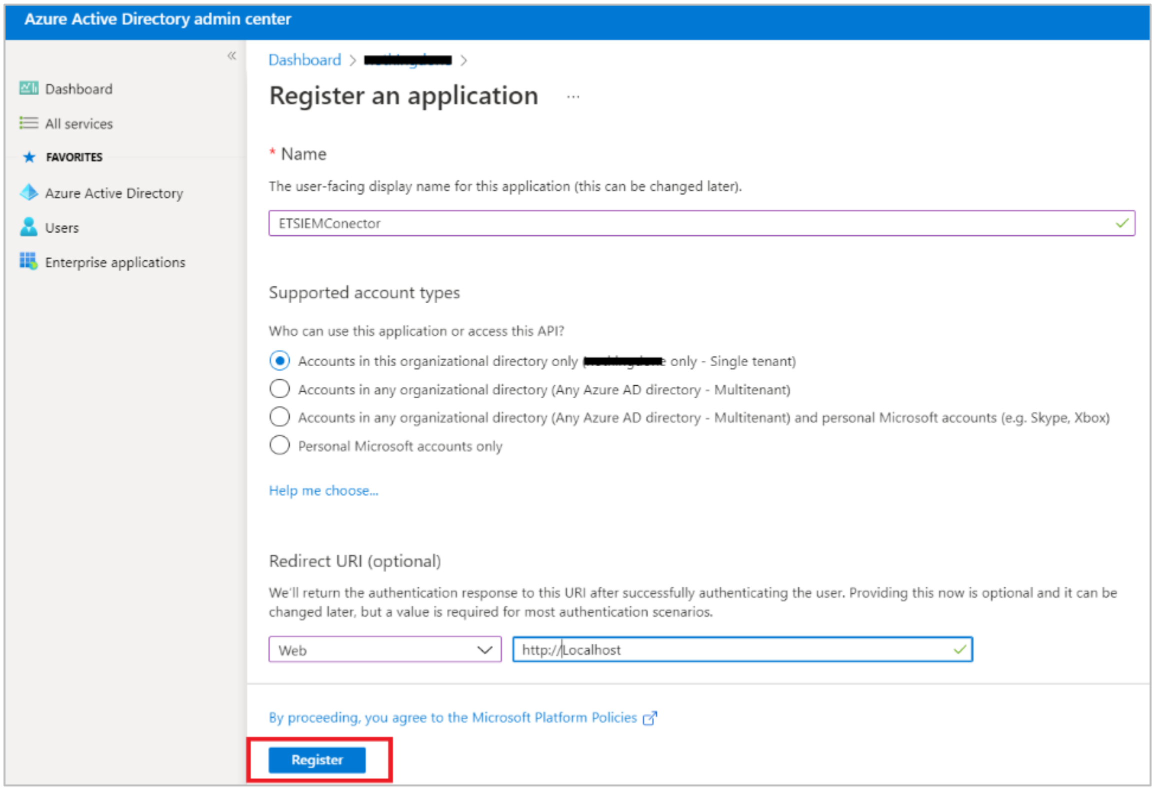


Starting June 30t
will no longer pr

4 applications found

5. In the **Create** window, specify your application's registration information.

- **Name:** Enter the appropriate application name (for example, ETSIEMConnector).
- **Supported account types:** Select **Accounts in this organizational directory only.**
- **Redirect URI:** Choose **Web** from the drop-down list and enter **http://localhost.**



* Name

The user-facing display name for this application (this can be changed later).

ETSIEMConector ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only ([redacted] only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

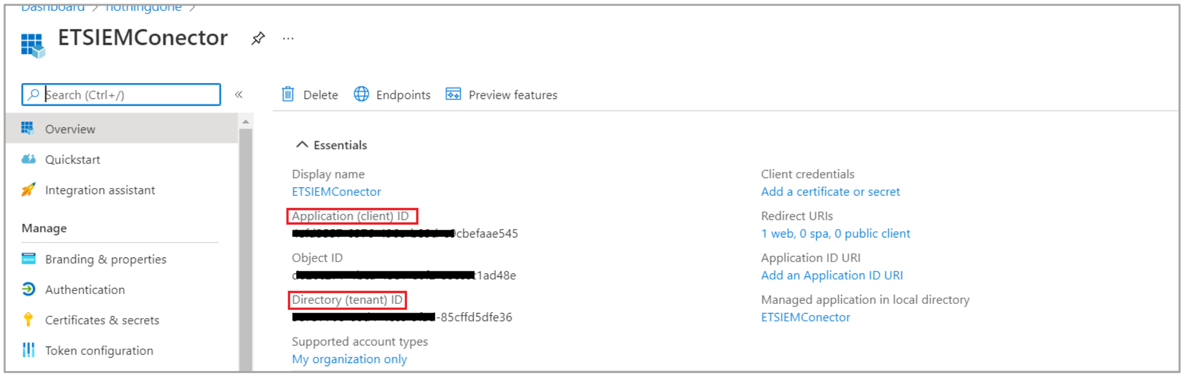
Web | http://Localhost ✓

By proceeding, you agree to the Microsoft Platform Policies

6. After providing all the details, click **Register**.

Azure AD assigns a unique **Application ID** to your application and navigates to the application's main registration page.

> **Note:**
>
> Make note of the **Application ID** and **Tenant ID** which will be used while integrating the Microsoft 365.



Display name
ETSIEMConector

Application (client) ID
[redacted]cbefaae545

Object ID
[redacted]1ad48e

Directory (tenant) ID
[redacted]-85cffd5dfe36

Supported account types
My organization only

Client credentials
Add a certificate or secret

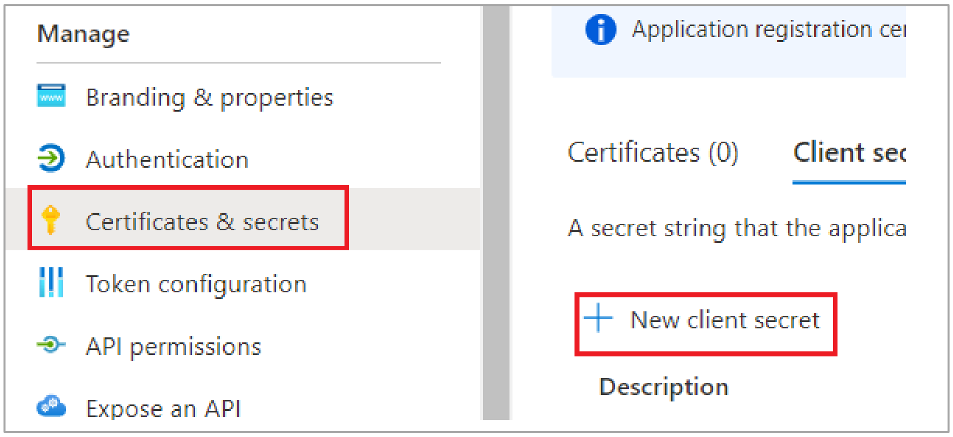
Redirect URIs
1 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
ETSIEMConector

Perform the following steps to create **Client Secret** for the application,

i. In the newly registered Application name (for example, **ETSIEMConector**), from the **Manage** section located on the left panel, go to **Certificates & secrets** > **Client secrets**, and click **+ New client secret.**

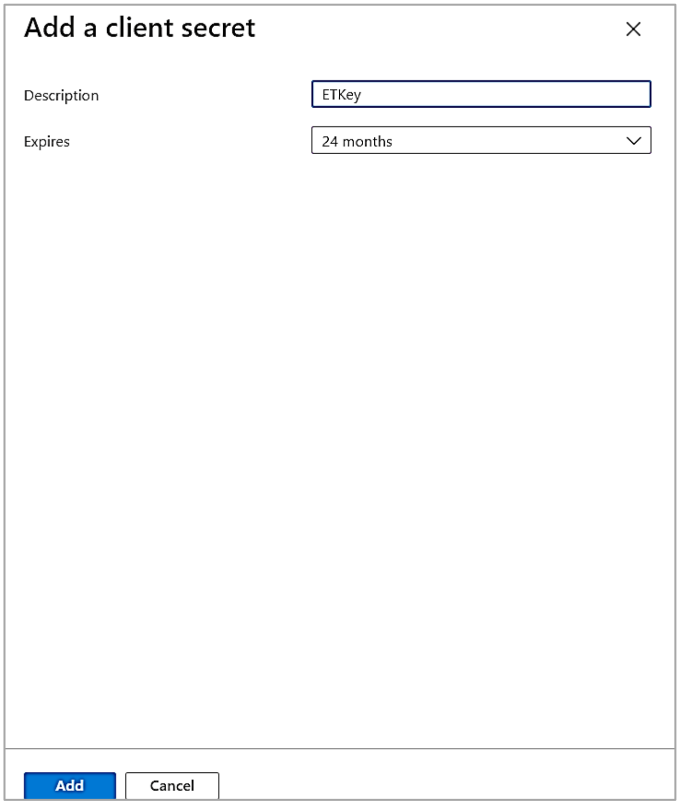


ii. In the **Add a client secret** window, specify the following details, and click **Add**.

- **Description**: ETKey.
- **Expires**: Select 24 months from the drop-down list.

Note:

The Client Secret needs to be recreated whenever expires.



Add a client secret

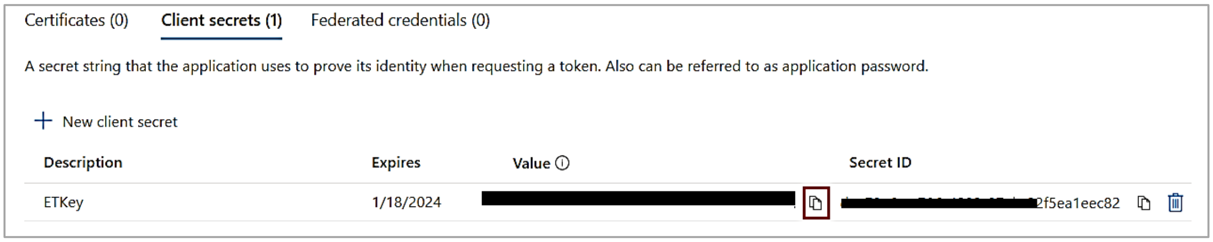
Description: ETKey

Expires: 24 months

iii. Copy and store the generated Client secret Value (Key) which will be applied while integrating the **Microsoft 365** integrator.

Note:

The Client Secret Value is a one-time generation and will not be visible again in the Azure portal.



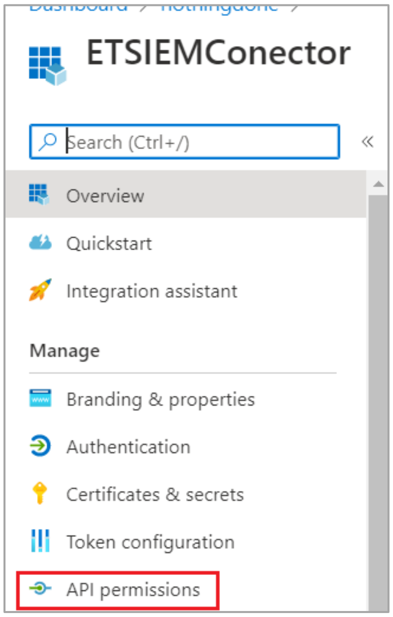
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID
ETKey	1/18/2024	[redacted]	[redacted]2f5ea1eec82

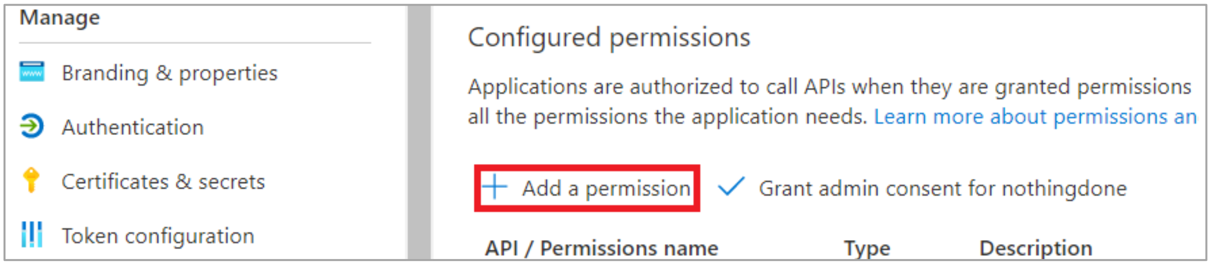
3.2 Adding Permissions to access APIs

Perform the following to add the permission(s) to access the resource APIs.

1. In the application's main registration page, click the **API Permissions** section.



2. Under the **Configured permissions** section, click **Add a Permission.**

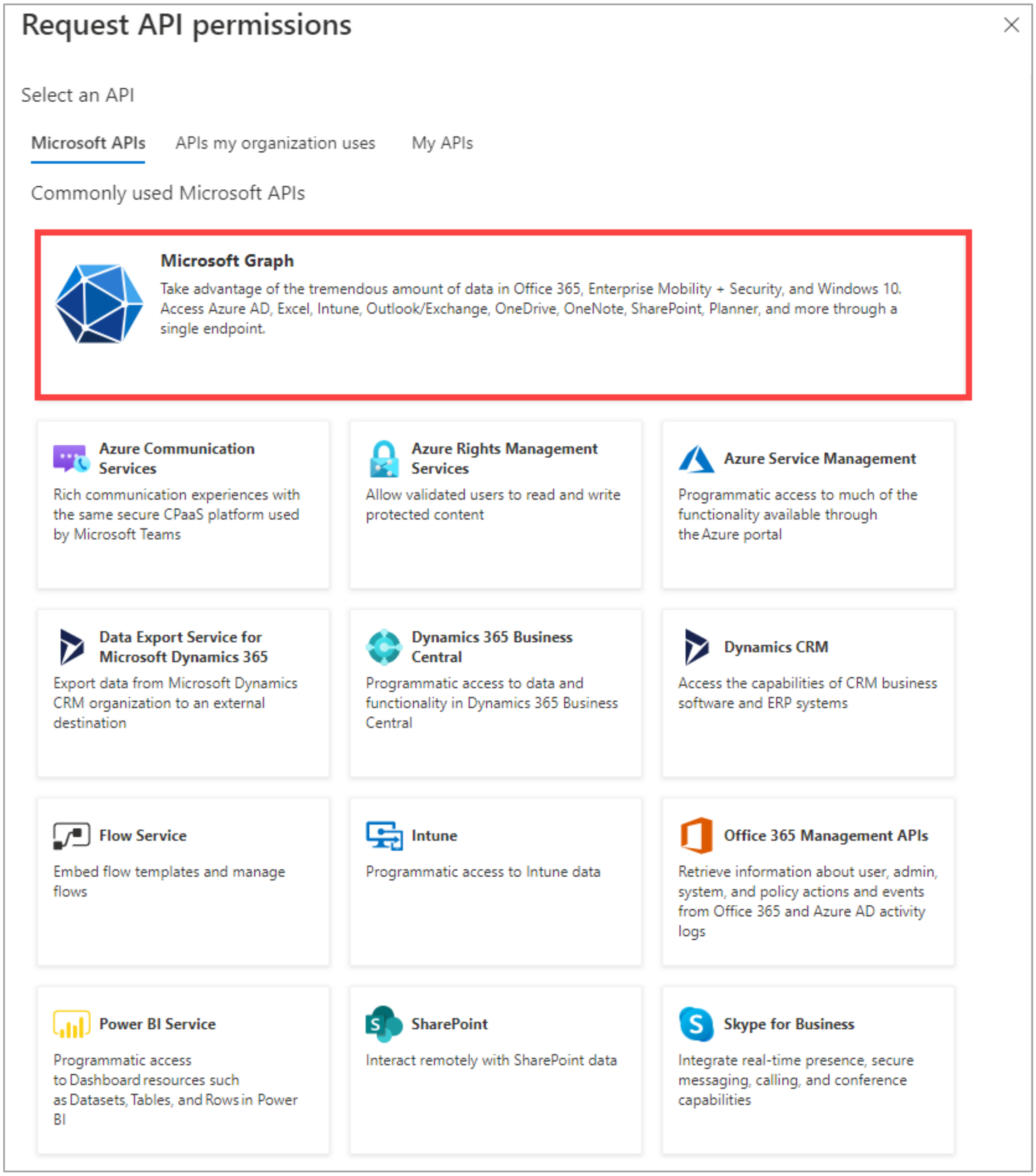


Configured permissions

Applications are authorized to call APIs when they are granted permissions all the permissions the application needs. Learn more about permissions an

3.2.1 Adding Microsoft Graph permissions

1. In the **Request API permissions** interface, click the **Microsoft APIs** tab and click **Microsoft Graph.**



Request API permissions

Select an API

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 Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

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

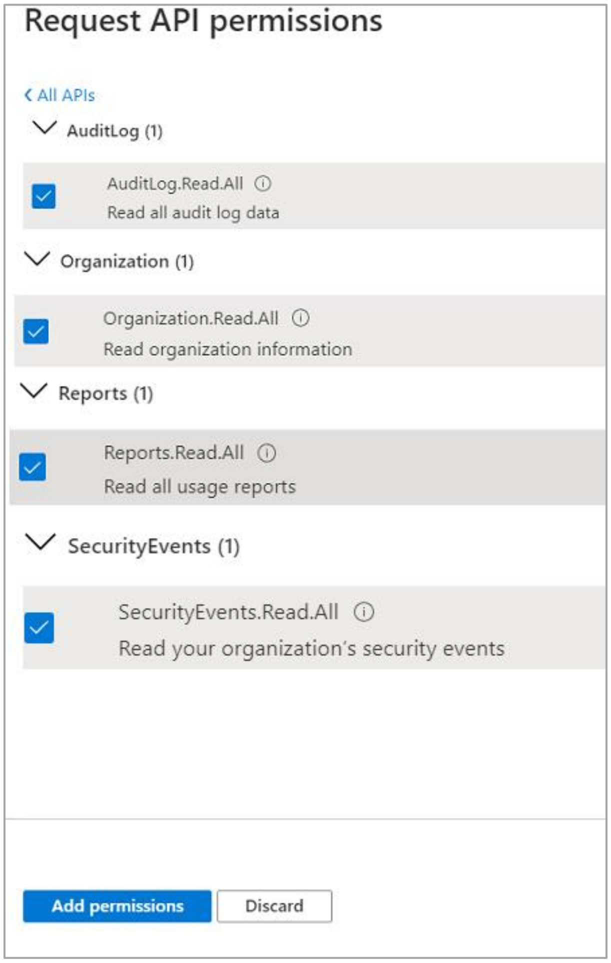
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

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

SharePoint
Interact remotely with SharePoint data

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

2. In the **Microsoft Graph** section**,** select the following application permissions.



Request API permissions

< All APIs

AuditLog (1)

☑ AuditLog.Read.All ⓘ
Read all audit log data

Organization (1)

☑ Organization.Read.All ⓘ
Read organization information

Reports (1)

☑ Reports.Read.All ⓘ
Read all usage reports

SecurityEvents (1)

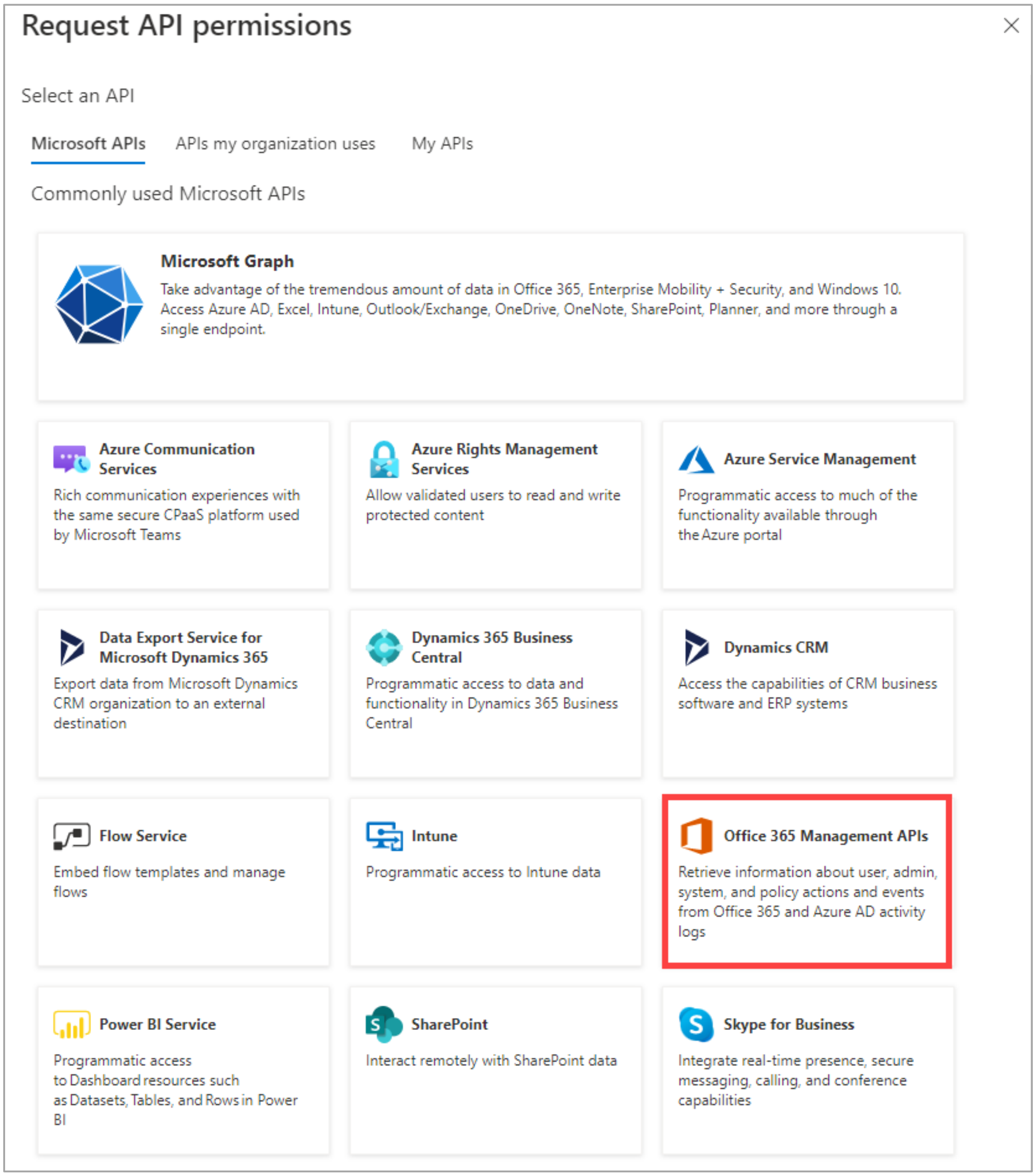
☑ SecurityEvents.Read.All ⓘ
Read your organization's security events

- Read all security events (**SecurityEvents.Read.All**).
- Read organization information (**Organization.Read.All**).
- Read all usage reports (**Reports.Read.All**).
- Read all audit log data (**AuditLog.Read.All**)

3. After selecting the specified permissions click **Add permissions.**

3.2.2 Adding Office 365 Management APIs permissions

1. In the **Request API permissions** interface, click the **Microsoft APIs** tab and click **Office 365 Management APIs**.



Request API permissions

Select an API

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 Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

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

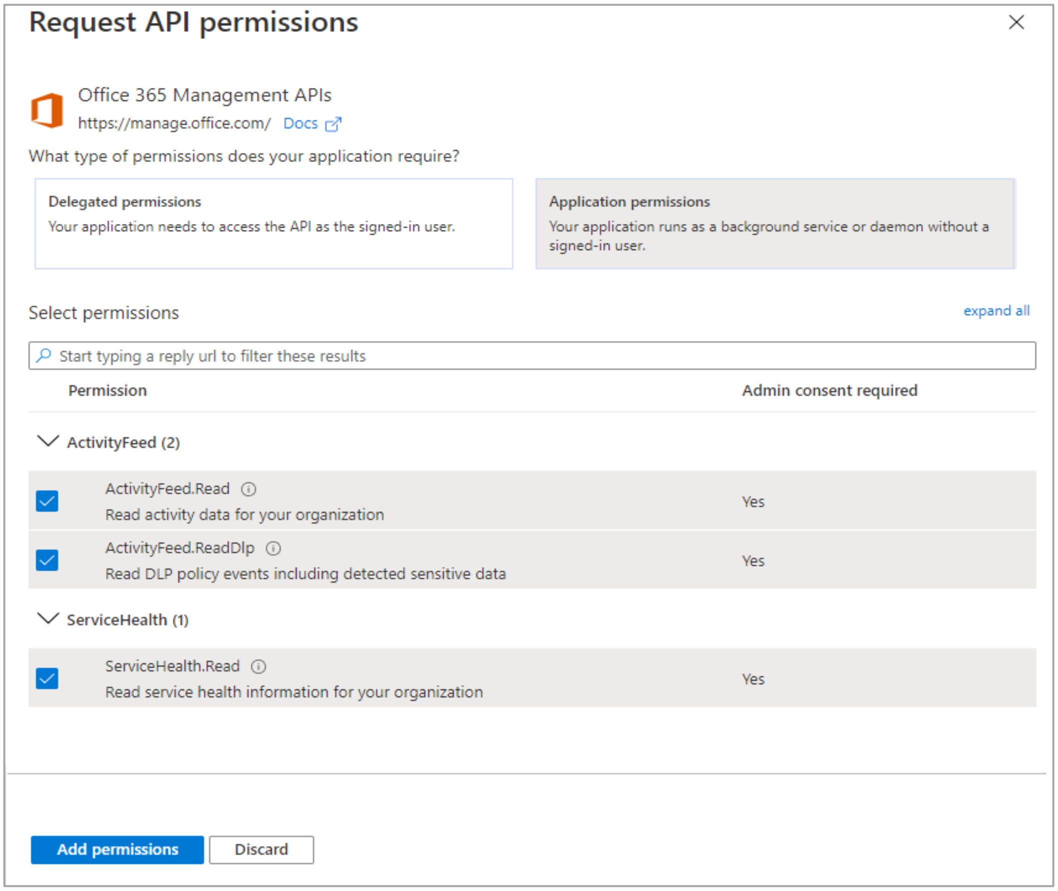
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

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

SharePoint
Interact remotely with SharePoint data

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

2. In the **Permission** section, select all the application permission.



Request API permissions

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

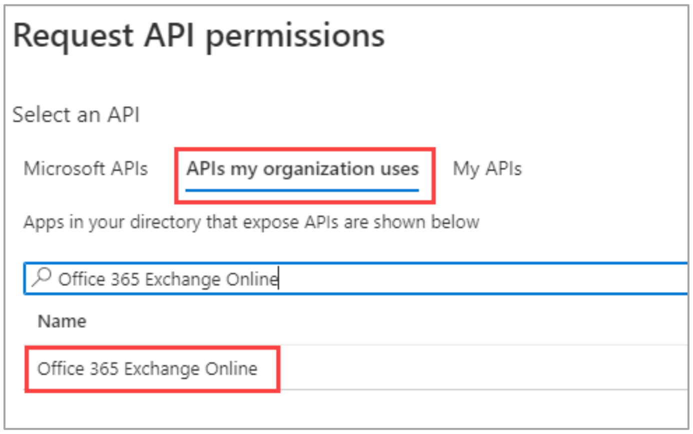
Start typing a reply url to filter these results

	Permission	Admin consent required
	ActivityFeed (2)	
☑	ActivityFeed.Read Read activity data for your organization	Yes
☑	ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data	Yes
	ServiceHealth (1)	
☑	ServiceHealth.Read Read service health information for your organization	Yes

3. After selecting all the permissions click **Add permissions.**

3.2.3 Adding Office 365 Exchange Online API permissions

1. In the **Request API permissions** interface, click the **APIs my organization uses** tab, and search and click the **Office 365 Exchange Online** from the search results.



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

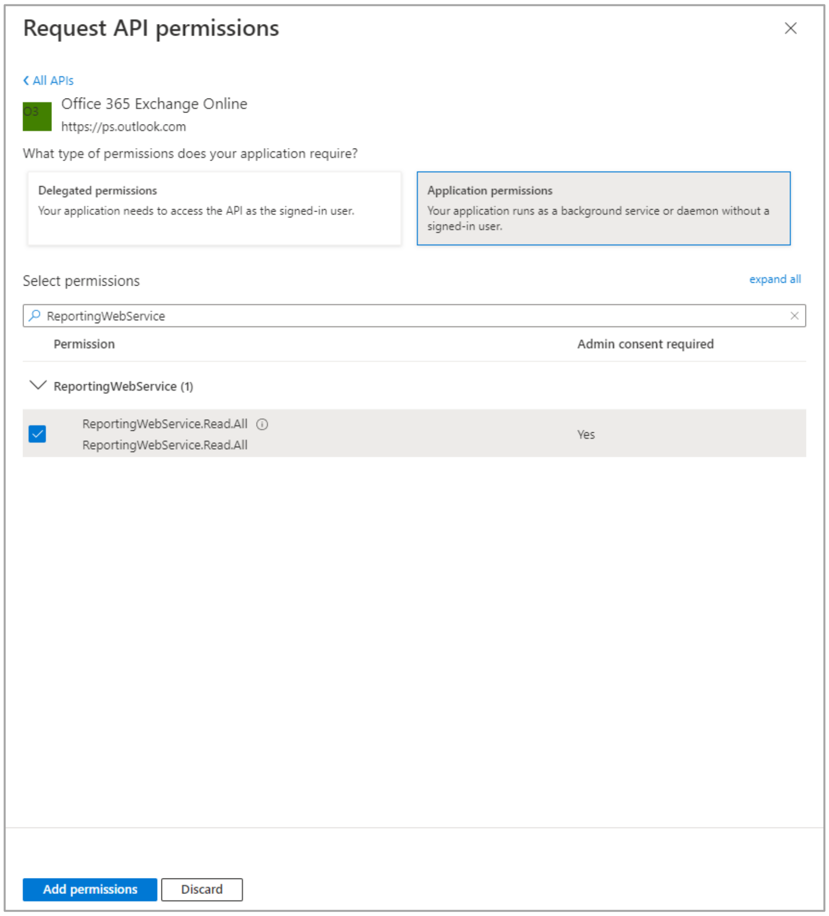
Apps in your directory that expose APIs are shown below

Office 365 Exchange Online

Name

Office 365 Exchange Online

2. In the **Office 365 Exchange Online** interface, select **Application permissions,** then search and select the **ReportingWebService** check box**.**



Request API permissions

< All APIs

Office 365 Exchange Online
https://ps.outlook.com

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

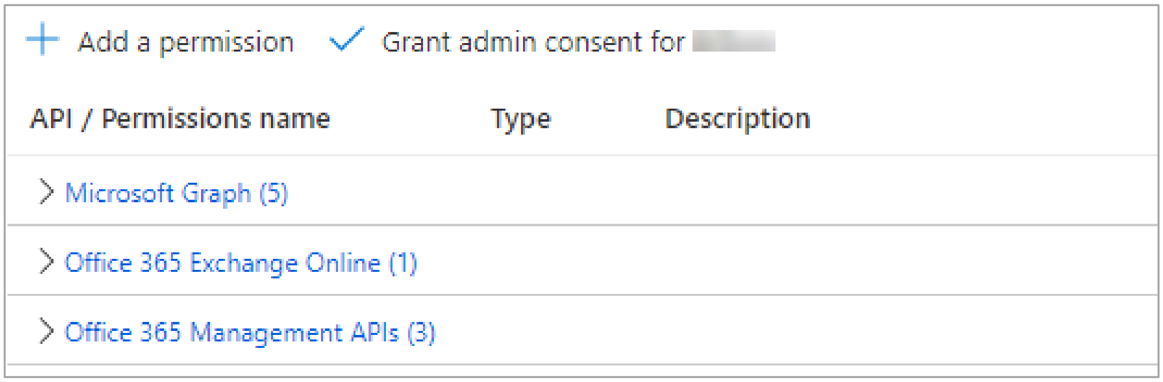
expand all

ReportingWebService

Permission	Admin consent required
ReportingWebService (1)	
☑ ReportingWebService.Read.All ⓘ ReportingWebService.Read.All	Yes

3. Then, click **Add permissions.**

4. After selecting all the specified API permissions for Microsoft Graph, Office 365 Management, and Office 365 Exchange Online, click **Grant admin consent for <Organization>.**

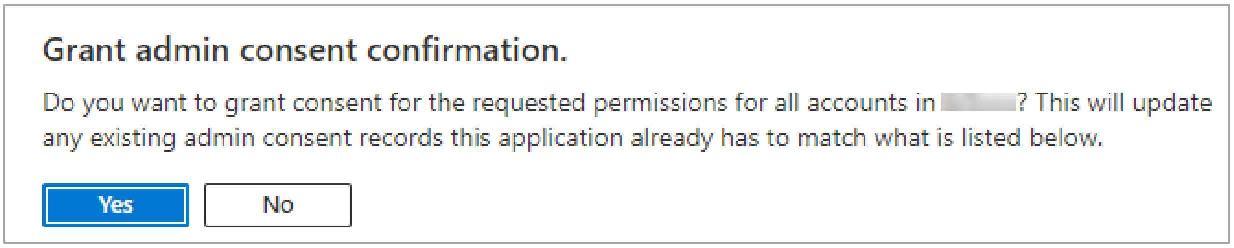


API / Permissions name	Type	Description
> Microsoft Graph (5)		
> Office 365 Exchange Online (1)		
> Office 365 Management APIs (3)		

Verify the below API permissions are assigned for the application

- Microsoft Graph
  - ✓ SecurityEvents.Read.All
  - ✓ Organization.Read.All
  - ✓ Reports.Read.All
  - ✓ AuditLog.Read.All
- Office 365 Management APIs
  - ✓ ActivityFeed.Read
  - ✓ ActivityFeedDlp
  - ✓ ServiceHealth.Read
- Office 365 Exchange Online
  - ✓ ReportingWebService.ReadAll

5. Then, click **Yes** to confirm the assigned permissions.

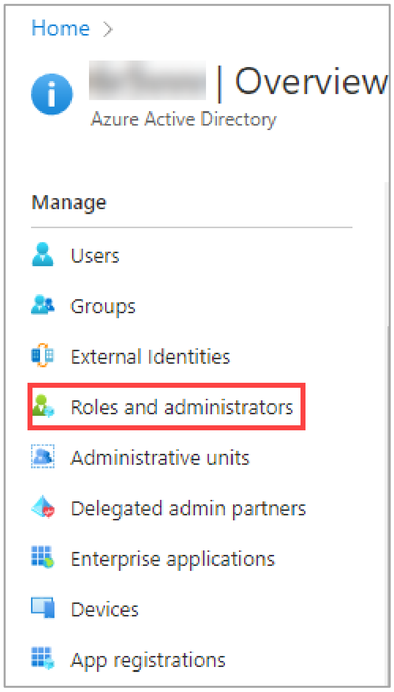


Grant admin consent confirmation.

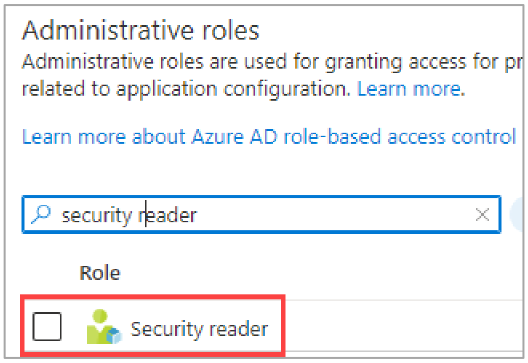
Do you want to grant consent for the requested permissions for all accounts in [redacted]? This will update any existing admin consent records this application already has to match what is listed below.

3.3 Adding Security Reader role

1. In the **Azure Active Directory** home page, click **Roles and administrators.**



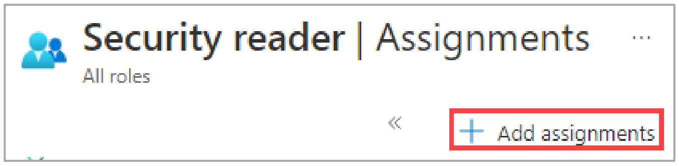
2. In the **Administrative roles** interface, search and select **Security Reader.**


Administrative roles

Administrative roles are used for granting access for pr related to application configuration. Learn more.

Learn more about Azure AD role-based access control

3. Then, click **Add assignments.**



4. In the **Add assignments** interface, perform the following steps in the case of Azure Active Directory Premium P2 license.

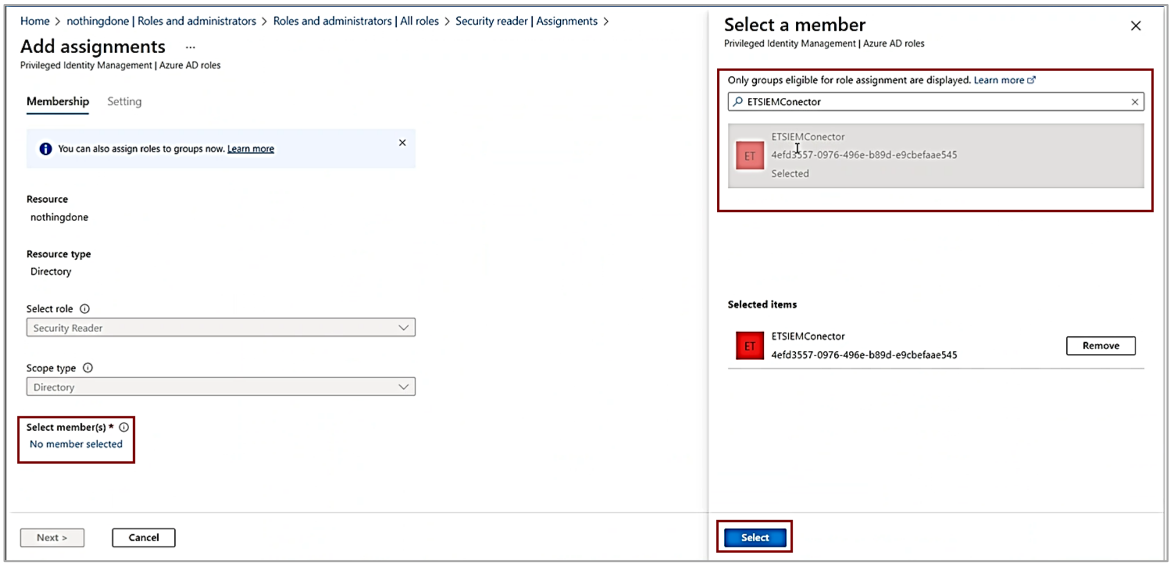
Note:

In the case of **Azure Active Directory Premium P1** and **Free** licensing, the steps vary according to the license type opted for the tenant.

a. In **Select member(s)**, click **No member selected.**

b. Next, navigate to the right side, in the **Select a member** window, under available groups list, search to select the required group name and click **Select**, and then click **Next**.

For example, search for **ETSIEMConector (**that is the application name**), click Select**, and then click **Next.**



Home > nothingdone | Roles and administrators > Roles and administrators | All roles > Security reader | Assignments >
Membership
Setting
Next >
Cancel
Select
Remove
×

Add assignments ...

Privileged Identity Management | Azure AD roles

You can also assign roles to groups now. Learn more

Resource
nothingdone

Resource type
Directory

Select role: Security Reader

Scope type: Directory

Select member(s) *
No member selected

Select a member

Privileged Identity Management | Azure AD roles

Only groups eligible for role assignment are displayed. Learn more

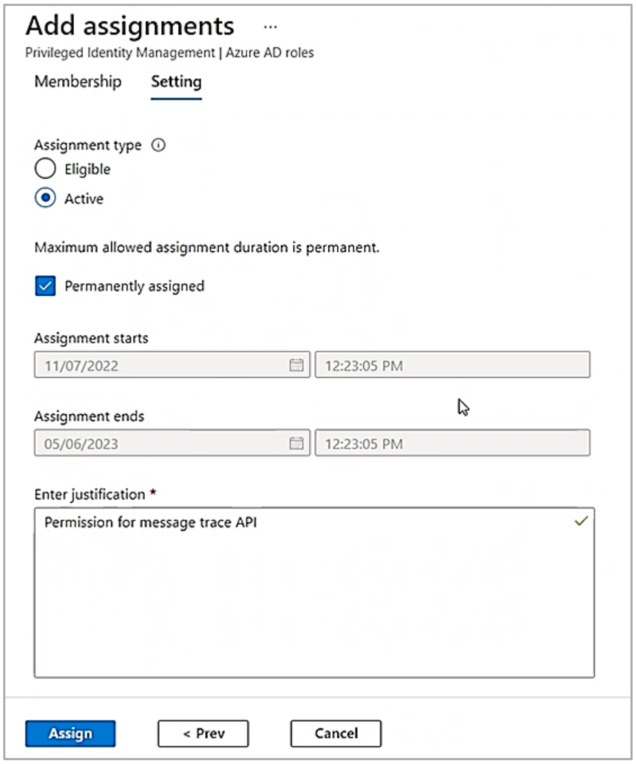
ETSIEMConector

ET ETSIEMConector
4efd3557-0976-496e-b89d-e9cbefaae545
Selected

Selected items

ET ETSIEMConector
4efd3557-0976-496e-b89d-e9cbefaae545

c. In this interface, for **Assignment Type** choose **Active**, select the **Permanently assigned** check box, and in the **Enter the justification** message box provide a justification (depends on the tenant policy), and then click **Assign**.



Add assignments ...

Privileged Identity Management | Azure AD roles

Assignment type
○ Eligible
● Active

Maximum allowed assignment duration is permanent.

☑ Permanently assigned

Assignment starts
11/07/2022 12:23:05 PM

Assignment ends
05/06/2023 12:23:05 PM

Enter justification *
Permission for message trace API

4 Configuring Microsoft 365 Integrator to Forward Logs to Netsurion Open XDR

4.1 Adding a Tenant/ Organization

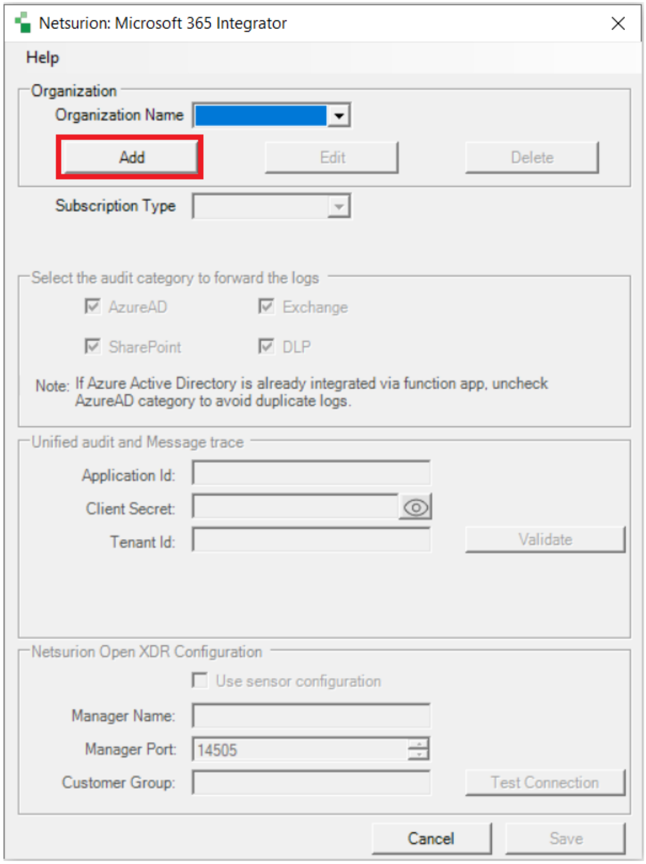
1. Run the executable **Microsoft365_Integrator.exe** file from the DSI package.

> **Note**:
>
> If the integrator is already installed, run the executable **Microsoft365_Configure.exe** file with administrator access.

- In the case of an Agent system, the executable file will be in **Agent/Integrator/Microsoft 365** folder.
- In the case of a non-Agent system, the executable files will be in **Program files X86/Integrator/Microsoft 365** folder.

After launching the integrator, it checks for PowerShell (5.0 or above) compatibility. If found compatible, the integrator allows you to integrate with Microsoft 365.

2. In the **Microsoft 365 Integrator** window, click **Add** to add the Tenant/ Organization details.

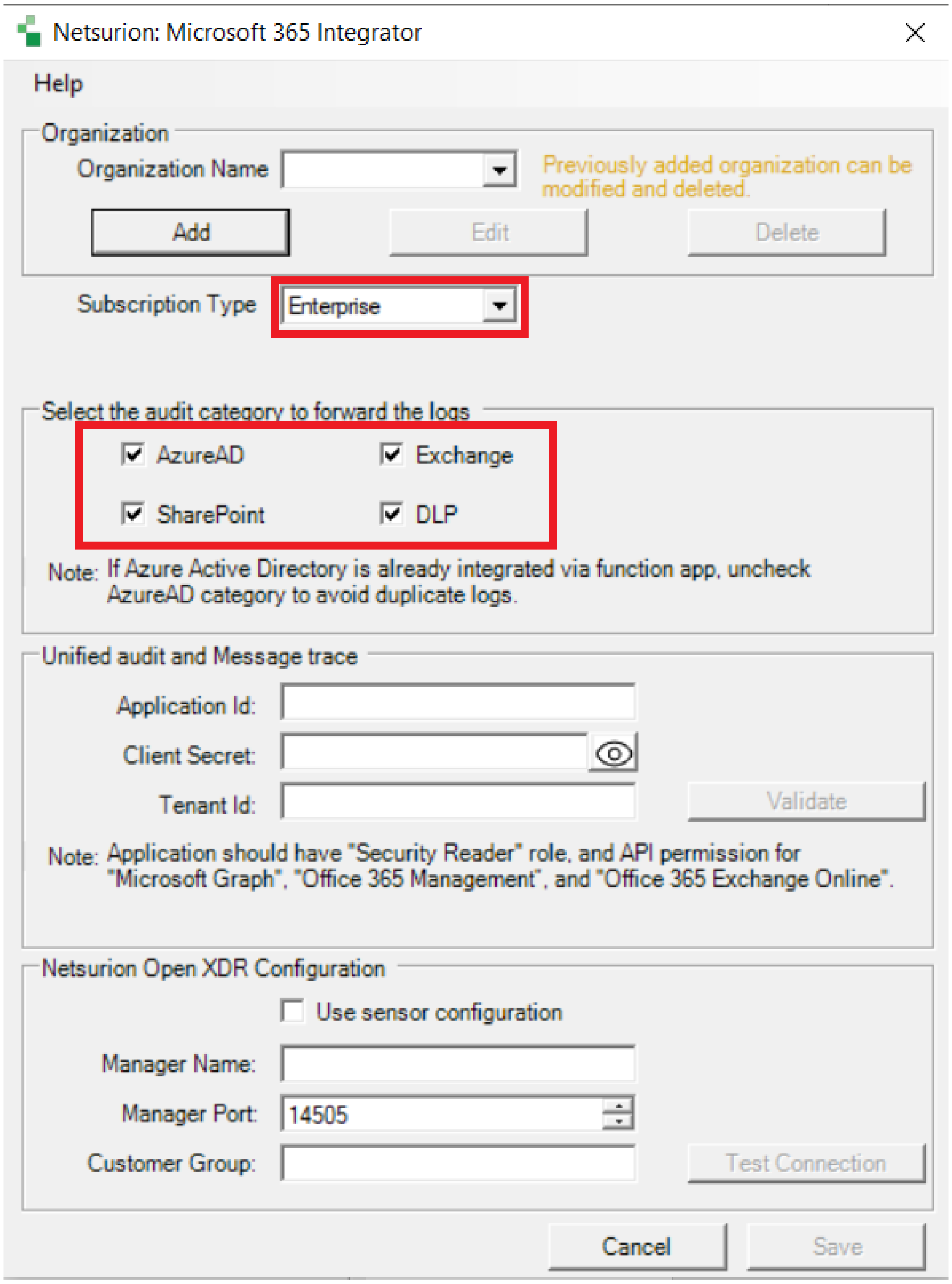


Note: If Azure Active Directory is already integrated via function app, uncheck AzureAD category to avoid duplicate logs.

Unified audit and Message trace
Application Id:
Client Secret:
Tenant Id:
Validate
Netsurion Open XDR Configuration
☐ Use sensor configuration
Manager Name:

Manager Port: 14505

3. For the **Subscription Type**, select the appropriate tenant subscription type from the drop-down list, and then select the required **audit category** check boxes to forward the logs.



Previously added organization can be modified and deleted.

Subscription Type: Enterprise

Select the audit category to forward the logs

☑ AzureAD ☑ Exchange

☑ SharePoint ☑ DLP

Note: If Azure Active Directory is already integrated via function app, uncheck AzureAD category to avoid duplicate logs.

Note: Application should have "Security Reader" role, and API permission for "Microsoft Graph", "Office 365 Management", and "Office 365 Exchange Online".

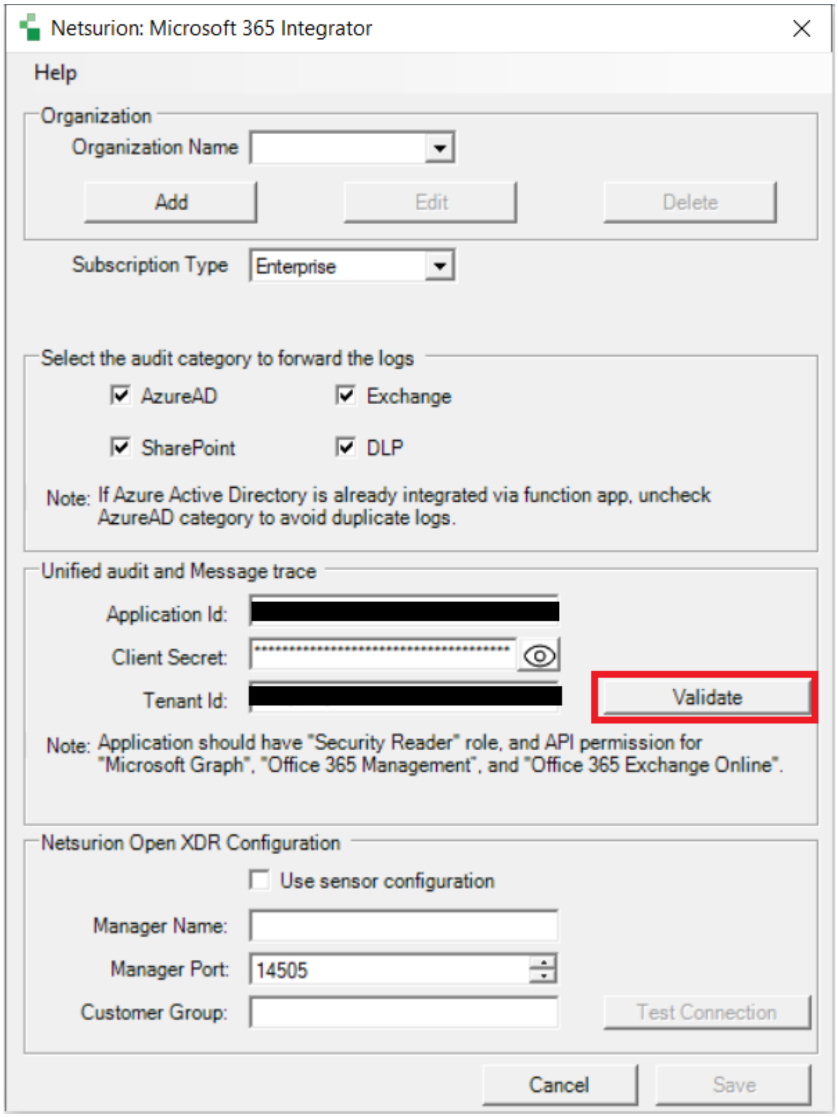
☐ Use sensor configuration

Manager Port: 14505

Note:

If none of the Audit category are selected, the default audit category will be used to forward the logs to Netsurion Open XDR.

4. In the **Unified audit and Message trace** section, provide the Application credentials (**Application Id, Client Secret, Tenant Id**) created while registering the Application and click **Validate** to verify the credentials**.**



Netsurion: Microsoft 365 Integrator

Help

Organization

Organization Name:

Subscription Type: Enterprise

Select the audit category to forward the logs

☑ AzureAD ☑ Exchange

☑ SharePoint ☑ DLP

Note: If Azure Active Directory is already integrated via function app, uncheck AzureAD category to avoid duplicate logs.

Unified audit and Message trace

Application Id: [redacted]

Client Secret: **

Tenant Id: [redacted]

Note: Application should have "Security Reader" role, and API permission for "Microsoft Graph", "Office 365 Management", and "Office 365 Exchange Online".

Netsurion Open XDR Configuration

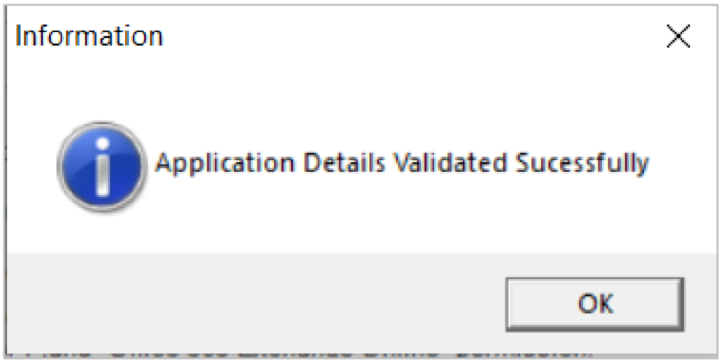
☐ Use sensor configuration

Manager Name:

Manager Port: 14505

Customer Group:

If Application credential is validated successfully, then an Information window pops-up stating '***Application Details Validated Successfully***'.

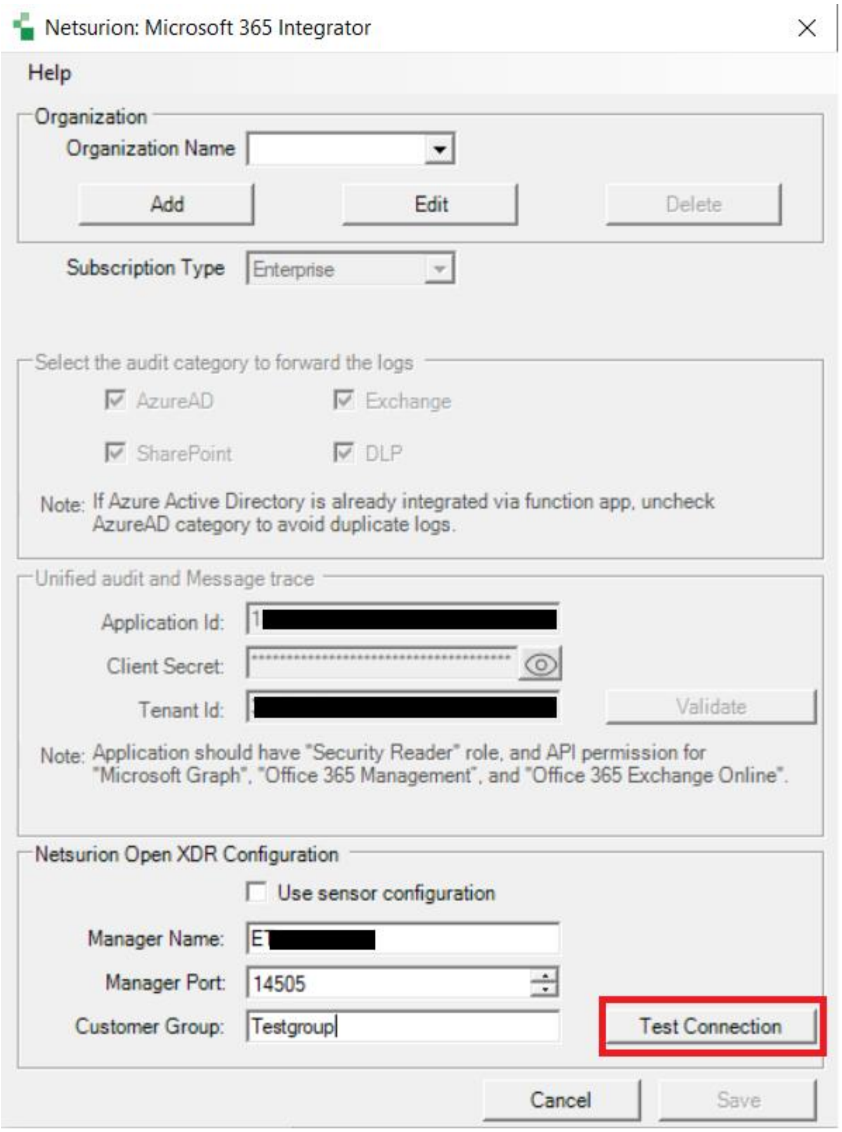


Information

Application Details Validated Sucessfully

5. In the **Netsurion Open XDR Configuration** section,

   a. You may either specify the details for **Manager Name**, **Manager Port**, and **Customer Group** and click **Test Connection** to validate the details.



Netsurion: Microsoft 365 Integrator

Help

Organization

Organization Name

Subscription Type: Enterprise

Select the audit category to forward the logs

☑ AzureAD ☑ Exchange

☑ SharePoint ☑ DLP

Note: If Azure Active Directory is already integrated via function app, uncheck AzureAD category to avoid duplicate logs.

Unified audit and Message trace

Application Id: 1[redacted]

Client Secret: ************************************

Tenant Id: [redacted]

Note: Application should have "Security Reader" role, and API permission for "Microsoft Graph", "Office 365 Management", and "Office 365 Exchange Online".

Netsurion Open XDR Configuration

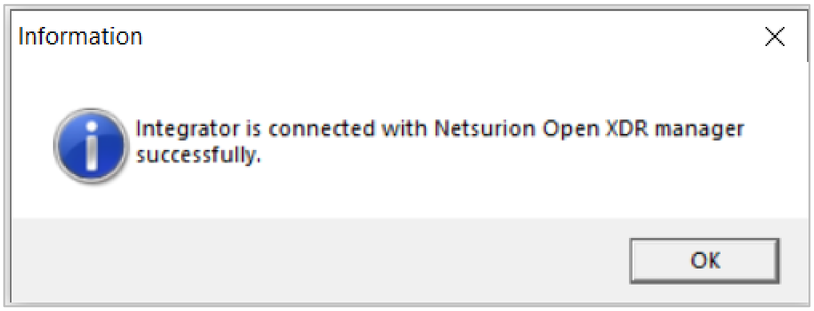
□ Use sensor configuration

Manager Name: E[redacted]

Manager Port: 14505

Customer Group: Testgroup

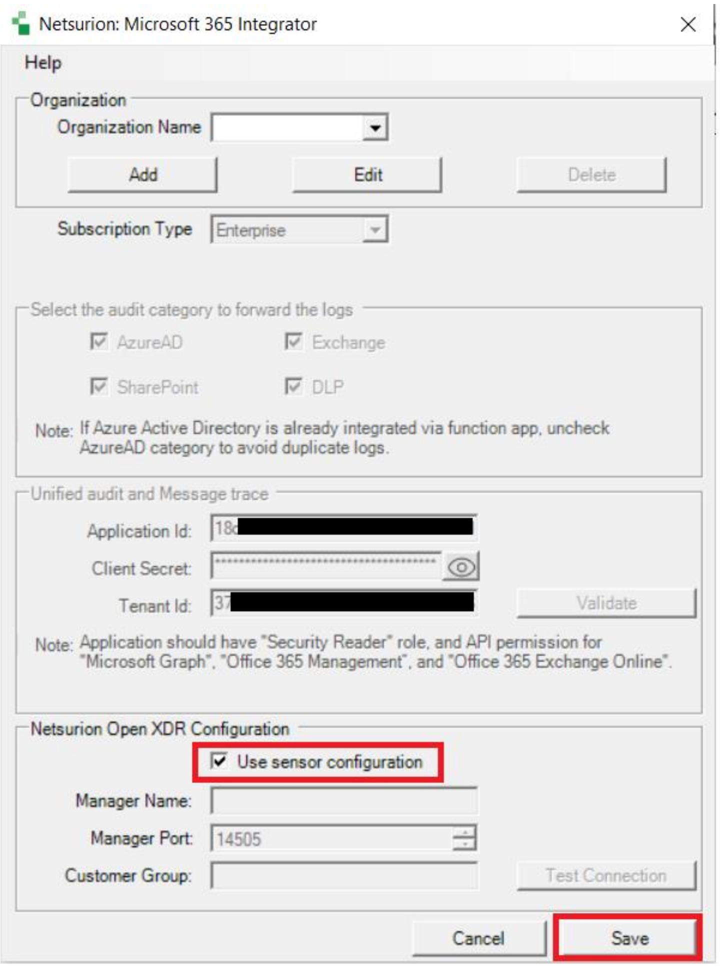
If the connection is validated successfully, an Information window pops-up stating ‘***Integrator is connected with Netsurion Open XDR Manager successfully***’.



Information

Integrator is connected with Netsurion Open XDR manager successfully.

b. Otherwise, select the **Use Sensor configuration** check box if you want to use the Agent configuration and Netsurion Open XDR Agent is installed in the system.



Netsurion: Microsoft 365 Integrator

Organization

Organization Name:

Subscription Type: Enterprise

Select the audit category to forward the logs

☑ AzureAD ☑ Exchange

☑ SharePoint ☑ DLP

Note: If Azure Active Directory is already integrated via function app, uncheck AzureAD category to avoid duplicate logs.

Unified audit and Message trace

Application Id: 18[redacted]

Client Secret: ************************************

Tenant Id: 37[redacted]

Note: Application should have "Security Reader" role, and API permission for "Microsoft Graph", "Office 365 Management", and "Office 365 Exchange Online".

Netsurion Open XDR Configuration

☑ Use sensor configuration

Manager Name:

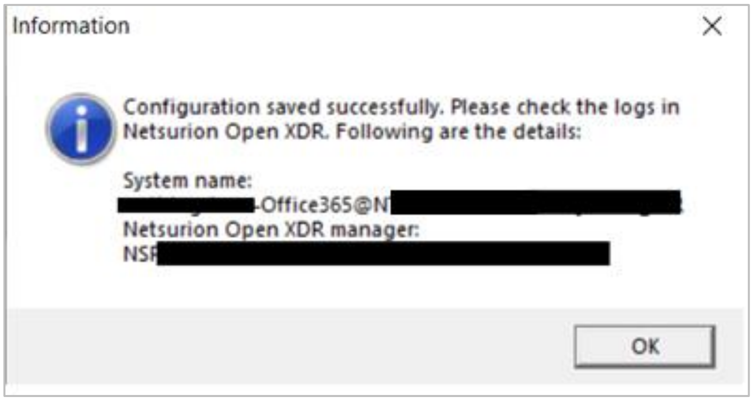
Manager Port: 14505

Customer Group:

6. After specifying the required details, click **Save**.

The integrator validates the subscription, retrieves the organization's information, and saves the configuration, resulting in the successful integration of Microsoft 365 with Netsurion Open XDR.

7. Click **OK** in the Information window and verify the logs in Netsurion Open XDR Manager console.



Information

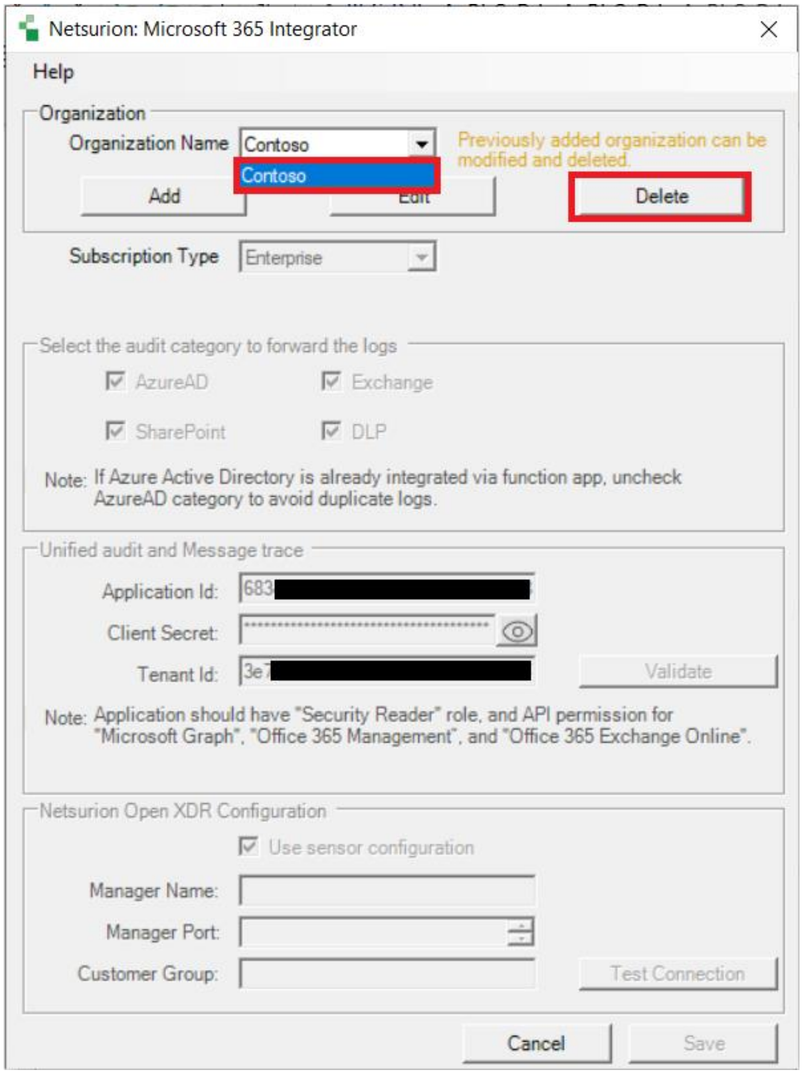
Configuration saved successfully. Please check the logs in Netsurion Open XDR. Following are the details:

System name:
[redacted]-Office365@N[redacted]
Netsurion Open XDR manager:
NS[redacted]

4.2 Deleting a Tenant/ Organization

1. Run the executable file **Microsoft365_Config.exe** with administrator access.

2. In the **Organization** section, select the appropriate **Tenant or the Organization name** from the drop-down list and click **Delete**.



Netsurion: Microsoft 365 Integrator

Help

Organization

Organization Name: Contoso

Previously added organization can be modified and deleted.

Subscription Type: Enterprise

Select the audit category to forward the logs

☑ AzureAD ☑ Exchange

☑ SharePoint ☑ DLP

Note: If Azure Active Directory is already integrated via function app, uncheck AzureAD category to avoid duplicate logs.

Unified audit and Message trace

Application Id: 683[redacted]

Client Secret: **

Tenant Id: 3e7[redacted]

Note: Application should have "Security Reader" role, and API permission for "Microsoft Graph", "Office 365 Management", and "Office 365 Exchange Online".

Netsurion Open XDR Configuration

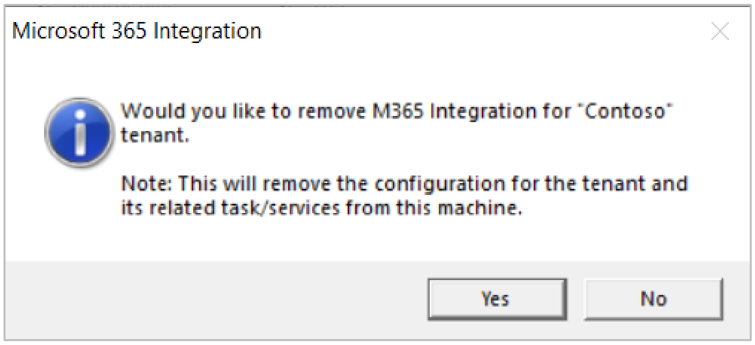
☑ Use sensor configuration

Manager Name:

Manager Port:

Customer Group:

3. Then, click **Yes** to confirm the deletion of the Tenant/ Organization name.

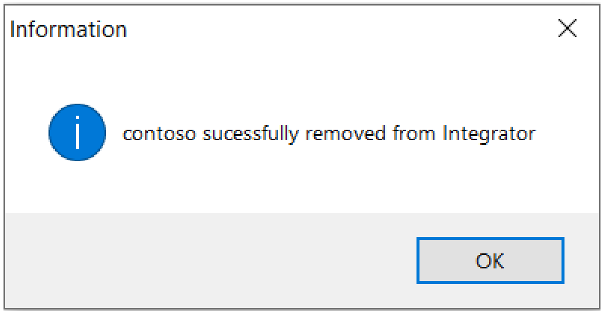


Microsoft 365 Integration

Would you like to remove M365 Integration for "Contoso" tenant.

Note: This will remove the configuration for the tenant and its related task/services from this machine.

4. A pop-up window appears after successful deletion of the Tenant/ Organization name from the Integrator. Click **OK**.



Information

contoso sucessfully removed from Integrator

5 Verifying Microsoft 365 Integration

After providing the details in the Microsoft 365 Integrator, perform the following procedure to verify the Microsoft 365 integration.

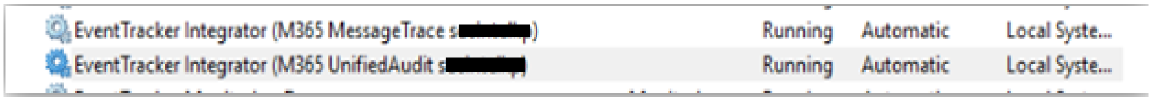
1. Check if the following services are created in the machine and are running.
   a. Launch **Services.msc** and check if the following services exist and are running.

      EventTracker Integrator (M365 MessageTrace <Organization name>)

      Note:

      M365 MessageTrace is applicable only for Enterprise and Business.

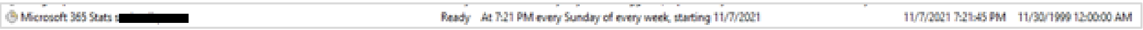
      EventTracker Integrator (M365 UnifiedAudit <Organisation Name>)



EventTracker Integrator (M365 MessageTrace [redacted])	Running	Automatic	Local Syste...
EventTracker Integrator (M365 UnifiedAudit [redacted])	Running	Automatic	Local Syste...

   b. Launch taskschd.msc and check if the following task exists.

      Microsoft 365 Stats <Organisation Name>



Microsoft 365 Stats [redacted]	Ready	At 7:21 PM every Sunday of every week, starting 11/7/2021	11/7/2021 7:21:45 PM	11/30/1999 12:00:00 AM

Note:

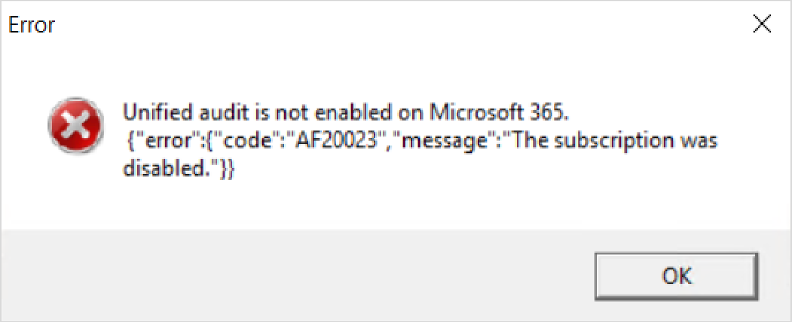
As Microsoft keeps updating the **Event** types, click here for all up-to-date event-type details.

6 Troubleshooting

Below error occurs while saving the configuration if the Microsoft 365 Business subscription is not enabled with Unified Audit in advance (minimum one day prior).

Note:

Refer to Configuring Microsoft 365 Unified Audit guide to enable unified Audit.



Unified audit is not enabled on Microsoft 365. {"error":{"code":"AF20023","message":"The subscription was disabled."}}

7 Error Code

Code	Description	Resolution
AF10001	The permission set ({0}) sent in the request did not include the expected permission ActivityFeed - Read. {0} = the permission set in the access token.	Check the permission on the application registered.
AF20001	Missing parameter: {0}. {0} = the name of the missing parameter.	Contact Netsurion Open XDR support team.
AF20002	Invalid parameter type: {0}. Expected type: {1} {0} = the name of the invalid parameter. {1} = the expected type (int, datetime, guide).	Contact Netsurion Open XDR support team.
AF20003	Expiration {0} provided is set to past date and time. {0} = the expiration passed in the API call.	Contact Netsurion Open XDR support team.
AF20010	The tenant ID passed in the URL ({0}) does not match the tenant ID passed in the access token ({1}). {0} = tenant ID passed in the URL {1} = tenant ID passed in the access token	Check the tenant Id provided in the Microsoft 365 form.
AF20011	Specified tenant ID ({0}) does not exist in the system or has been deleted. {0} = tenant ID passed in the URL	Contact the Microsoft Support team for troubleshooting the issue.
AF20012	Specified tenant ID ({0}) is incorrectly configured in the system. {0} = tenant ID passed in the URL	Contact the Microsoft support team for troubleshooting the issue.

Code	Description	Resolution
AF20013	The tenant ID passed in the URL ({0}) is not a valid GUID.	Check the tenant Id provided in the Microsoft 365 form.
	{0} = tenant ID passed in the URL	
AF20020	The specified content type is not valid.	Contact Netsurion Open XDR support team.
AF20021	The webhook endpoint {{0}) could not be validated. {1}	Contact Netsurion Open XDR support team.
	{0} = webhook address.	
	{1} = "The endpoint did not return HTTP 200." or "The address must begin with HTTPS."	
AF20022	No subscription was found for the specified content type.	Contact the Microsoft support team for troubleshooting the issue.
AF20023	The subscription was disabled by {0}.	
	{0} = "a tenant admin" or "a service admin"	
AF20030	Start time and end time must both be specified (or both omitted) and must be less than or equal to 24 hours apart, with the start time no more than 7 days in the past.	Contact Netsurion Open XDR support team.
AF20031	Invalid nextPage Input: {0}.	Contact Netsurion Open XDR support team.
	{0} = the next page indicator passed in the URL	
AF20050	The specified content ({0}) does not exist.	Contact Netsurion Open XDR support team.
	{0} = resource id or resource URL	
AF20051	Content requested with the key {0} has already expired. Content older than 7 days cannot be retrieved.	Contact Netsurion Open XDR support team.
	{0} = resource id or resource URL	
AF20052	Content ID {0} in the URL is invalid.	Contact Netsurion Open XDR support team.
	{0} = resource id or resource URL	
AF20053	Only one language may be present in the Accept-Language header.	Contact Netsurion Open XDR support team.
AF20054	Invalid syntax in Accept-Language header.	Contact Netsurion Open XDR support team.
AF429	Too many requests. Method={0}, PublisherId={1}	
	{0} = HTTP Method	
	{1} = Tenant GUID used as PublisherIdentifier	
AF50000	An internal error occurred. Retry the request.	Contact Netsurion Open XDR support team.

8 Data Source Integrations (DSIs) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integrations package contains the following files for Microsoft 365.

- Category_Microsoft 365.iscat
- Alerts_Microsoft 365.isalt
- Reports_Microsoft 365.etcrx
- KO_Microsoft 365.etko
- Dashboards_Microsoft 365.etwd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in Netsurion Open XDR.

Data Source Integrations Details

8.1 Alerts

Name	Description
Microsoft 365 - A potentially malicious URL click was detected	Generated when a potentially malicious URL click was detected by Microsoft 365.
Microsoft 365 - Creation of forwarding/redirect rule	Generated when a creation of forwarding/redirect rule was detected by Microsoft 365.
Microsoft 365 - eDiscovery search started or exported	Generated when an eDiscovery search start or export was detected by Microsoft 365.
Microsoft 365 - Elevation of Exchange admin privilege	Generated when an elevation of Exchange admin privilege was detected by Microsoft 365.
Microsoft 365 - Email messages containing malware removed after delivery	Generated when an email message containing malware, removed after delivery was detected by Microsoft 365.
Microsoft 365 - Email messages containing phish URLs removed after delivery	Generated when an email message containing phish URL(s), removed after delivery was detected by Microsoft 365.
Microsoft 365 - Email reported by user as malware or phish	Generated when an email reported by user as malware or phish was detected by Microsoft 365.
Microsoft 365 - Login activities using SAML token detected	Generated when a login activity using SAML token detected was detected by Microsoft 365.

Name	Description
Microsoft 365 - Malware campaign detected after delivery	Generated when a malware campaign after delivery is detected by Microsoft 365.
Microsoft 365 - Malware campaign detected and blocked	Generated when a malware campaign was detected and blocked by Microsoft 365.
Microsoft 365 - Malware campaign detected in SharePoint and OneDrive	Generated when a malware campaign in SharePoint and OneDrive was detected by Microsoft 365.
Microsoft 365 - Messages have been delayed	Generated when a delay in messages was detected by Microsoft 365.
Microsoft 365 - Phish delivered due to tenant or user override	Generated when a phish delivered due to tenant or user override is detected by Microsoft 365.
Microsoft 365 - Security & compliance alerts	Generated when security & compliance alerts are triggered by Microsoft 365.
Microsoft 365 - Suspicious email sending patterns detected	Generated when suspicious email sending patterns are detected by Microsoft 365.
Microsoft 365 - Tenant restricted from sending email	Generated when a tenant restricted from sending email is detected by Microsoft 365.
Microsoft 365 - Unusual increase in email reported as phish	Generated when an unusual increase in email reported as phish is detected by Microsoft 365.
Microsoft 365 - Unusual volume of file deletion	Generated when an unusual volume of file deletion is detected by Microsoft 365.
Microsoft 365 - User impersonation phish delivered to inbox/folder	Generated when a user impersonation phishing email delivered to inbox/folder is detected by Microsoft 365.
Microsoft 365 Azure AD User Logon failed	Generated when an Azure AD user logon failed is detected by Microsoft 365.
Microsoft 365: CAS alerts has been triggered	Generated when CAS alerts are triggered by Microsoft 365.
Microsoft 365: Login Activities	Generated when a login activity is detected by Microsoft 365.
Microsoft 365: Sensitive information detected in Mail	Generated when sensitive information detected in Mail was detected by Microsoft 365.
Microsoft 365: Sensitive information detected in SharePoint	Generated when sensitive information is detected in SharePoint by Microsoft 365.
Microsoft 365: User login failed due to MFA	Generated when a user login failed due to MFA is detected by Microsoft 365.
Microsoft 365: User MFA disabled	Generated when a user disabling MFA is detected by

Name	Description
	Microsoft 365.
Microsoft 365: Member assigned to global administrator role	Generated when a user or group assigned to the Global Administrator role is detected by Microsoft 365.
Microsoft 365 - Unusual external user file activity	Generated when an unusual external user file activity is detected by Microsoft 365.
Microsoft 365 - Unusual volume of external file sharing	Generated when an unusual volume of external file sharing is detected by Microsoft 365.
Microsoft 365 - User restricted from sending email	Generated when a user restricted from sending email is detected by Microsoft 365.

8.2 Reports

Name	Description
Microsoft 365 - Azure active directory login activities	Provides details about all the Azure active directory login activities monitored by Microsoft 365.
Microsoft 365 - User MFA activities	Provides details about all the user MFA activities monitored by Microsoft 365.
Microsoft 365 - Exchange Spam Mail Traffic Details	Provides details about all the Exchange Spam Mail Traffic Details monitored by Microsoft 365.
Microsoft 365 - Threat intelligence activities	Provides details about all the threat intelligence activities monitored by Microsoft 365.
Microsoft 365 – DLP activity	Provides details about all the DLP activity monitored by Microsoft 365.
Microsoft 365 - User login failed due to MFA activities	Provides details about all the user login failed due to MFA activities monitored by Microsoft 365.
Microsoft 365 - CAS alert triggered	Provides details about all the CAS alert triggered monitored by Microsoft 365.
Microsoft 365 - Exchange admin activities	Provides details about all the Exchange admin activities monitored by Microsoft 365.
Microsoft 365 - Azure active directory admin activities	Provides details about all the Azure active directory admin activities monitored by Microsoft 365.
Microsoft 365 - Email activity user counts	Provides details about all the email activity user counts monitored by Microsoft 365.

Name	Description
Microsoft 365 - Email app usage user counts	Provides details about all the email app usage user counts monitored by Microsoft 365.
Microsoft 365 - Email app usage user detail	Provides details about all the email app usage user detail monitored by Microsoft 365.
Microsoft 365 - Email app usage version user counts	Provides details about all the email app usage version user counts monitored by Microsoft 365.
Microsoft 365 - Mailbox usage detail	Provides details about all the mailbox usage detail monitored by Microsoft 365.
Microsoft 365 - Mailbox usage mailbox counts	Provides details about all the mailbox usage mailbox counts monitored by Microsoft 365.
Microsoft 365 - Mailbox usage quota status mailbox counts	Provides details about all the mailbox usage quota status mailbox counts monitored by Microsoft 365.
Microsoft 365 - Mailbox storage usage	Provides details about all the mailbox storage usage monitored by Microsoft 365.
Microsoft 365 - Activation counts	Provides details about all the activation counts monitored by Microsoft 365.
Microsoft 365 - Microsoft 365 activation user counts	Provides details about all the Microsoft 365 activation user counts monitored by Microsoft 365.
Microsoft 365 - Activated user detail	Provides details about all the activated user detail monitored by Microsoft 365.
Microsoft 365 - Active user counts	Provides details about all the active user counts monitored by Microsoft 365.
Microsoft 365 - OneDrive activity file counts	Provides details about all the OneDrive activity file counts monitored by Microsoft 365.
Microsoft 365 - OneDrive activity user counts	Provides details about all the OneDrive activity user counts monitored by Microsoft 365.
Microsoft 365 - OneDrive usage account counts	Provides details about all the OneDrive usage account counts monitored by Microsoft 365.
Microsoft 365 - OneDrive usage account detail	Provides details about all the OneDrive usage account detail monitored by Microsoft 365.
Microsoft 365 - OneDrive usage file counts	Provides details about all the OneDrive usage file counts monitored by Microsoft 365.
Microsoft 365 - OneDrive usage storage	Provides details about all the OneDrive usage storage monitored by Microsoft 365.

Name	Description
Microsoft 365 - SharePoint activity user details	Provides details about all the SharePoint activity user details monitored by Microsoft 365.
Microsoft 365 - SharePoint site storage usage	Provides details about all the SharePoint site storage usage monitored by Microsoft 365.
Microsoft 365 - Exchange Message Trace Details	Provides details about all the Exchange Message Trace Details monitored by Microsoft 365.
Microsoft 365 - Exchange Mail Traffic Details	Provides details about all the Exchange Mail Traffic Details monitored by Microsoft 365.
Microsoft 365 - Exchange Mailbox login activities	Provides details about all the Exchange Mailbox login activities monitored by Microsoft 365.
Microsoft 365 - OneDrive file operations	Provides details about all the OneDrive file operations monitored by Microsoft 365.
Microsoft 365 - SharePoint site operations	Provides details about all the SharePoint site operations monitored by Microsoft 365.
Microsoft 365 - Skype for business activity user detail	Provides details about all the Skype for business user details monitored by Microsoft 365.
Microsoft 365 - Skype for business device usage user detail	Provides details about all the user device usage of Skype for business monitored by Microsoft 365.
Microsoft 365 - Skype for business peer to peer activity user counts	Provides details about all the peer-to-peer activity user counts of Skype for business monitored by Microsoft 365.

8.3 Dashboards

Name	Description
Microsoft 365 - CAS alert triggered by category	Displays all the CAS alert triggered by category in Microsoft 365
Microsoft 365 - CAS alert triggered by username	Displays all the CAS alert triggered by username in Microsoft 365
Microsoft 365 - CAS suspicious activity by username	Displays all the CAS suspicious activity by username in Microsoft 365
Microsoft 365 - CAS alert triggered by alert type	Displays all the CAS alert triggered by alert type in Microsoft 365
Microsoft 365 - ATP Top Malware Detected detail	Displays all the ATP top malware detected detail in Microsoft 365

Name	Description
Microsoft 365 - ATP User Affected by Threat	Displays all the ATP user affected by threat in Microsoft 365
Microsoft 365 - ATP Threat Category	Displays all the ATP threat category in Microsoft 365
Microsoft 365 - ATP Threat Detection Method	Displays all the ATP threat detection method in Microsoft 365
Microsoft 365 - ATP Suspicious Sender	Displays all the ATP suspicious sender in Microsoft 365
Microsoft 365 - DLP Action Taken	Displays all the DLP action taken in Microsoft 365
Microsoft 365 - Azure Active Directory login failed reason	Displays all the Azure Active Directory login failed reason in Microsoft 365
Microsoft 365 - Azure Active Directory Events	Displays all the Azure Active Directory events in Microsoft 365
Microsoft 365 - Azure Active Directory login activities by Status	Displays all the Azure Active Directory login activities by status in Microsoft 365
Microsoft 365 - Azure Active Directory login by user	Displays all the Azure Active Directory login by user in Microsoft 365
Microsoft 365 - Azure Active Directory login activities by Client IP	Displays all the Azure Active Directory login activities by client IP in Microsoft 365
Microsoft 365 - Azure Active Directory login failed by Country	Displays all the Azure Active Directory login failed by country in Microsoft 365
Microsoft 365 - Exchange Malicious Email by Sender	Displays all the Exchange malicious email by sender in Microsoft 365
Microsoft 365 - Exchange Malicious Email by Recipient	Displays all the Exchange malicious email by recipient in Microsoft 365
Microsoft 365 - Exchange Malicious Email by Threat Name	Displays all the Exchange malicious email by threat name in Microsoft 365
Microsoft 365 - Exchange mailbox login by user	Displays all the Exchange mailbox login by user in Microsoft 365
Microsoft 365 - Exchange Top Spam mail by Sender	Displays all the Exchange top spam mail by sender in Microsoft 365
Microsoft 365 - Exchange Top Spam mail by Recipient	Displays all the Exchange top spam mail by recipient in Microsoft 365
Microsoft 365 - MFA failed on User login activities by UserName	Displays all the MFA failed on user login activities by username in Microsoft 365

Name	Description
Microsoft 365 - MFA succeed on User login activities by UserName	Displays all the MFA succeed on user login activities by username in Microsoft 365
Microsoft 365 - MFA failed on User login activities by Geo Location	Displays all the MFA failed on user login activities by geo location in Microsoft 365
Microsoft 365 - MFA succeed on User login activities by Geo Location	Displays all the MFA succeed on user login activities by geo location in Microsoft 365
Microsoft 365 - Exchange Admin Activities By User	Displays all the Exchange admin activities by user in Microsoft 365
Microsoft 365 - User MFA activities by Targeted UserName	Displays all the user MFA activities by targeted username in Microsoft 365
Microsoft 365 - DLP activities by policy name	Displays all the DLP activities by policy name in Microsoft 365
Microsoft 365 - DLP activities by mail subject	Displays all the DLP activities by mail subject in Microsoft 365
Microsoft 365 - DLP activities by Severity	Displays all the DLP activities by severity in Microsoft 365
Microsoft 365 - DLP activities by sensitive information type name	Displays all the DLP activities by sensitive information type name in Microsoft 365
Microsoft 365 - User MFA activities by UserName	Displays all the user MFA activities by username in Microsoft 365
Microsoft 365 - Teams Login Success	Displays all the Teams login success in Microsoft 365
Microsoft 365 - Teams User Login by Geolocation	Displays all the Teams user login by geolocation in Microsoft 365
Microsoft 365 - Teams Login trends	Displays all the Teams login trends in Microsoft 365
Microsoft 365 - Teams External User Detected in team/chat Per day	Displays all the Teams external user detected in team/chat per day in Microsoft 365
Microsoft 365 - Teams External Users Detected in team/chat	Displays all the Teams external users detected in team/chat in Microsoft 365
Microsoft 365 - Teams Team and Connector Activity	Displays all the Teams team and connector activity in Microsoft 365
Microsoft 365 - Exchange Top Recipient	Displays all the Exchange top recipient in Microsoft 365
Microsoft 365 - OneDrive Activities by Operation	Displays all the OneDrive activities by operation in Microsoft 365

Name	Description
Microsoft 365 - OneDrive Activities by File Type	Displays all the OneDrive activities by file type in Microsoft 365
Microsoft 365 - OneDrive Activities by Resource Type	Displays all the OneDrive activities by resource type in Microsoft 365
Microsoft 365 - OneDrive Activity trends	Displays all the OneDrive activity trends in Microsoft 365
Microsoft 365 - OneDrive Activities by User	Displays all the OneDrive activities by user in Microsoft 365
Microsoft 365 - OneDrive Activities by User Agent	Displays all the OneDrive activities by user agent in Microsoft 365
Microsoft 365 - SharePoint Activities by Operations	Displays all the SharePoint activities by operations in Microsoft 365
Microsoft 365 - SharePoint Activities by File Type	Displays all the SharePoint activities by file type in Microsoft 365
Microsoft 365 - SharePoint Activities by Resource Type	Displays all the SharePoint activities by resource type in Microsoft 365
Microsoft 365 - SharePoint Activity trends	Displays all the SharePoint activities trends in Microsoft 365
Microsoft 365 - SharePoint Activities by User	Displays all the SharePoint activities by user in Microsoft 365
Microsoft 365 - SharePoint Activities by User Agent	Displays all the SharePoint activities by user agent in Microsoft 365
Microsoft 365 - Teams Device Type Used	Displays all the Teams device type used in Microsoft 365
Microsoft 365 - Teams Operation related to Members by username	Displays all the Teams operation related to members by username in Microsoft 365
Microsoft 365 - Teams Channel and Tab Activity	Displays all the Teams channel and tab activity in Microsoft 365
Microsoft 365 - Exchange Top Sender	Displays all the Exchange top sender in Microsoft 365

8.4 Saved Searches

Name	Description
Microsoft 365 - Exchange Spam Mail Traffic Details	Provides details about all the Exchange spam mail traffic details by Microsoft 365
Microsoft 365 - Exchange Threat Intelligence Activity	Provides details about all the Exchange threat intelligence activity by Microsoft 365
Microsoft 365 - User login failed due to MFA activities	Provides details about all the user login failed due to MFA activities by Microsoft 365
Microsoft 365 - User MFA disable activities	Provides details about all the user MFA disable activities by Microsoft 365
Microsoft 365 - CAS Alert activities	Provides details about all the CAS alert activities by Microsoft 365
Microsoft 365 - Azure AD Admin Activity	Provides details about all the Azure AD admin activity by Microsoft 365
Microsoft 365 - Azure AD User Logon Activity	Provides details about all the Azure AD user logon activity by Microsoft 365
Microsoft 365 - Email Activity by Count	Provides details about all the email activity by count by Microsoft 365
Microsoft 365 - Exchange Admin Activity	Provides details about all the Exchange admin activity by Microsoft 365
Microsoft 365 - Exchange Mailbox User Logon Activity	Provides details about all the Exchange mailbox user logon activity by Microsoft 365
Microsoft 365 - Exchange Message Trace	Provides details about all the Exchange message trace by Microsoft 365
Microsoft 365 - User MFA enable activities	Provides details about all the user MFA enable activities by Microsoft 365
Microsoft 365 - Exchange Mail Traffic	Provides details about all the Exchange mail traffic by Microsoft 365
Microsoft 365 - Mailbox Storage Usage	Provides details about all the mailbox storage usage by Microsoft 365

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support