



VOSS Insights Microsoft Teams Integration Guide for Insights

Release 25.1

March 26, 2025

Legal Information

- Copyright © 2025 VisionOSS Limited. All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20250326135657

Contents

1	Introduction	1
2	Register MS Teams API on Microsoft Azure	2
3	Configure MS Teams Monitoring	6

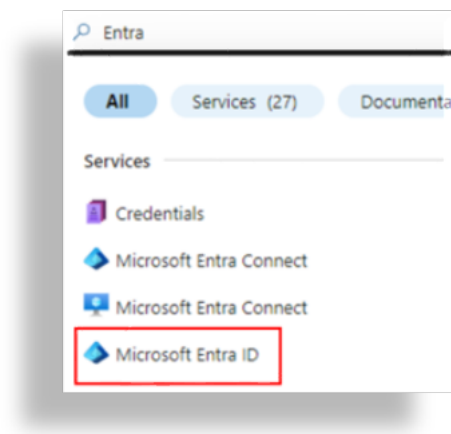
1. Introduction

This guide provides steps for configuring the Microsoft Teams tenant for Insights integration.

2. Register MS Teams API on Microsoft Azure

The MS Teams API configuration requires an initial application registration on Microsoft Azure.

1. In the Microsoft cloud portal, search for **Microsoft Entra ID** (formerly, Azure Active Directory):



2. Select **Manage > App registrations**, then select **New Registration**
3. Fill out a meaningful application **Name** to display to users and under **Supported account types**, select **Accounts in this organization directory** and click **Register**.

Microsoft Azure

Home > VOSS Solutions | App registrations >

Register an application

*** Name**

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

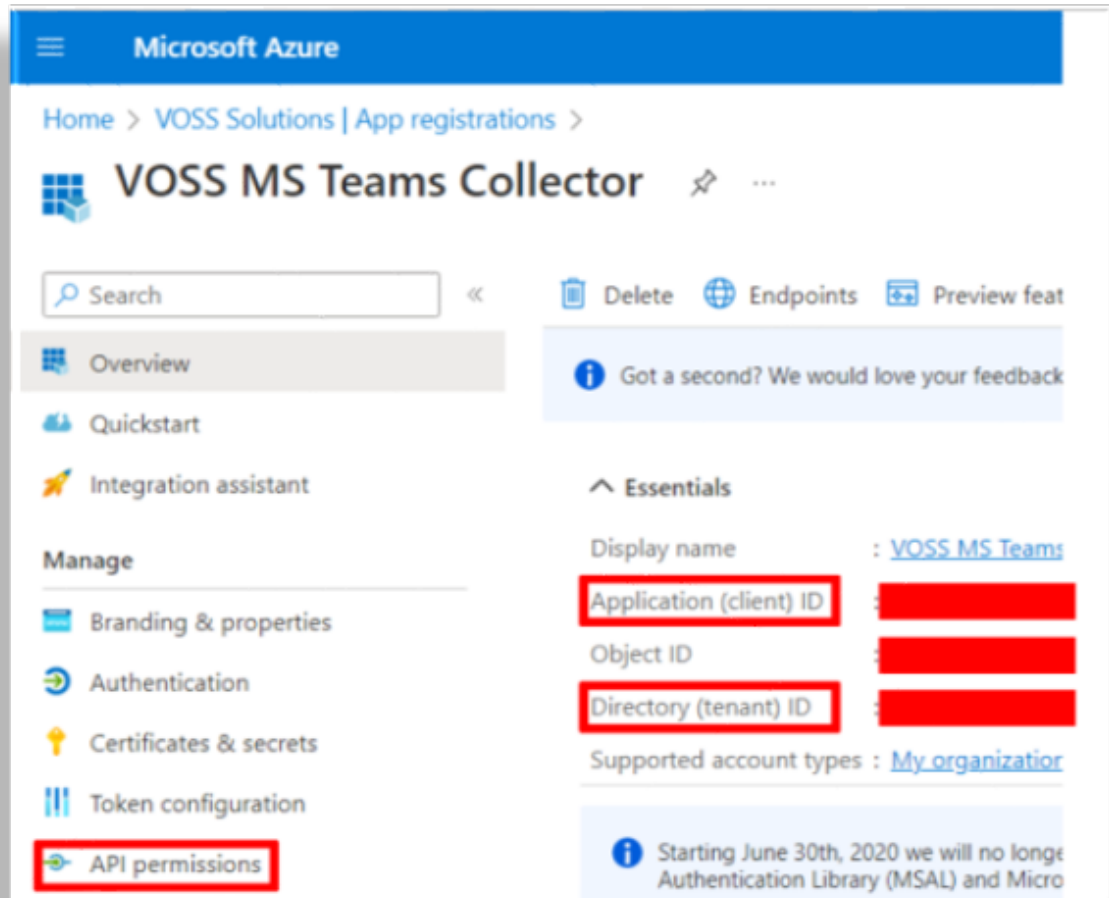
Voss-cloud-collector

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (VOSS Solutions 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
- ☐ Personal Microsoft accounts only

4. When the new application is registered, locate the **Application (client) ID** and **Directory (tenant) ID** on the next page and store these values in a secure location.

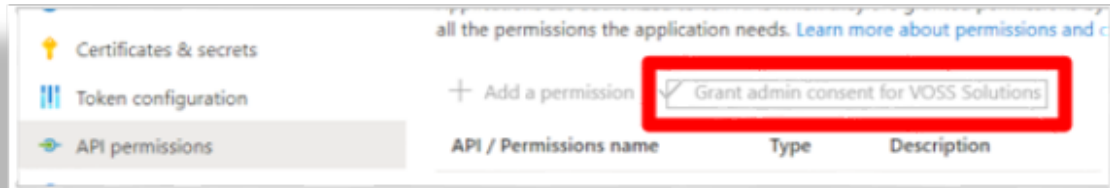


5. Select the **API permissions** menu under **Manage** and then select the following **Application permissions**:

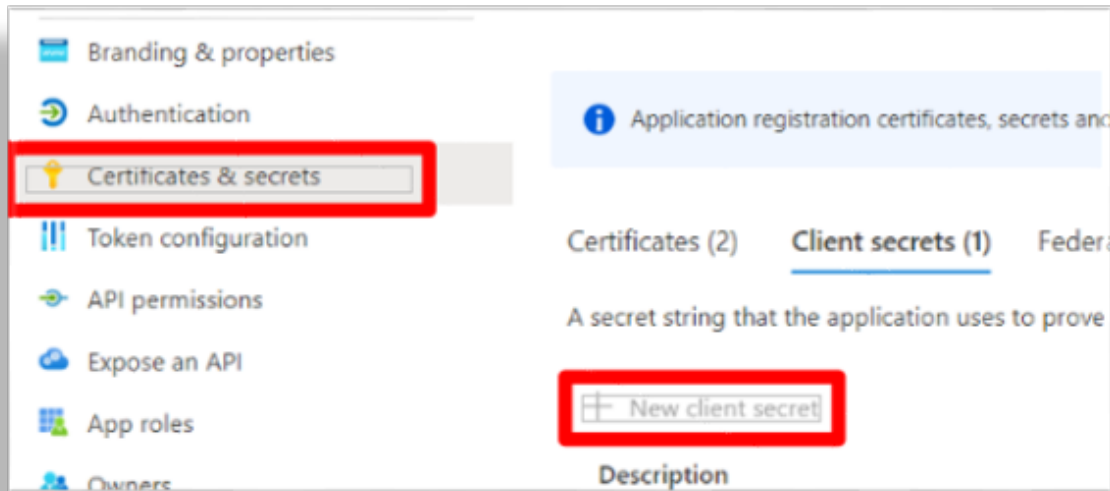
Microsoft Graph:

- CallRecords.Read.All
- Device.Read.All
- Group.Read.All
- LicenseAssignment.Read.All
- Reports.Read.All
- ServiceHealth.Read.All
- TeamworkDevice.Read.All
- User.Read
- User.Read.All
- VirtualEvent.Read.All

6. Grant admin consent:



7. From **Certificates & secrets**, create authentication from **New client secret**:



8. Copy the value and store in a secure location.

Description	Expires	Value	Secret ID
VOSS MS Teams Collector Secret	6/22/2023	[REDACTED]	[REDACTED]

The following stored values will be used on the Arbitrator configuration dialog screen:

- Application (client) ID
- Client secret value
- Directory (tenant) ID

3. Configure MS Teams Monitoring

This procedure configures and enables the tenant collection from Insights Arbitrator.

Pre-requisites

- Register MS Teams API on Microsoft Azure

To configure the tenant collection:

1. Log in to Insights Arbitrator, then click the toolbar Wrench icon to go to **System Configuration** settings.
2. In **System Configuration**, go to **Archive Management > API Config** settings.
3. Select **MS Teams Config**.

The screenshot displays the VOSS Insights Arbitrator interface. The top navigation bar includes the VOSS logo and various system icons. The main menu on the left shows 'ARCHIVE MANAGEMENT' with sub-items like 'API Config', 'Archive', 'Cisco SQL', 'Collect', 'Data User', 'Import', 'LDAP', 'License', 'Probe', 'Proxy', 'SNMP', and 'Syslog'. The 'API Config' sub-menu is expanded, showing 'Creation', 'DEM Config', 'MS Teams Config' (selected), 'Webex Config', and 'Zoom Config'. The main content area is titled 'MS Teams Config' and includes a description: 'Allows the enable and configuration of MS Teams monitoring'. It features a 'Fetch Statistics' button and a text input for 'Create an entry for the supplied customer'. Below this is an 'Enabled' checkbox set to 'enabled' and a note: 'Capture MS Teams statistics using the from the graph api at https://graph.microsoft.com'. The 'CUSTOMER' section contains fields for 'Tenant id of Customer', 'Name' (with a note 'Friendly user name of Customer'), and 'ClientID' (with a note 'Client ID to be used for requests'). A modal window is open over the 'CUSTOMER' section, containing fields for 'ClientSecret' (with a note 'Client Secret to be used for requests.'), 'BaseUrl' (with a note 'If required, then specify the base URL setting. Most companies should use https://graph.microsoft.com, but other possible examples include (GCC High) https://graph.microsoft.us and (GCC DoD) https://dod-graph.microsoft.us'), 'LoginUrl' (with a note 'If the BaseUrl is configured, then a paired LoginUrl is usually required.'), and a 'Save Data' button.

Note: Support is available for MS tenants using GHCC, DoD and China-operated cloud environments. The **BaseUrl** can therefore be modified accordingly as:

- `https://graph.microsoft.us`
- `https://dod-graph.microsoft.us`
- `https://microsoftgraph.chinacloudapi.cn`

The paired **LoginURL** can then also be specified.

For existing tenants not related to these environments, the fields will be auto-populated with existing data in this release and no update is required.

4. At **Enabled**, select either **Enabled** or **Disabled**.

Note: New tenants can be added and set to either *enabled* or *disabled*. API requests are made only when set to *enabled*.

5. Fill out stored values:

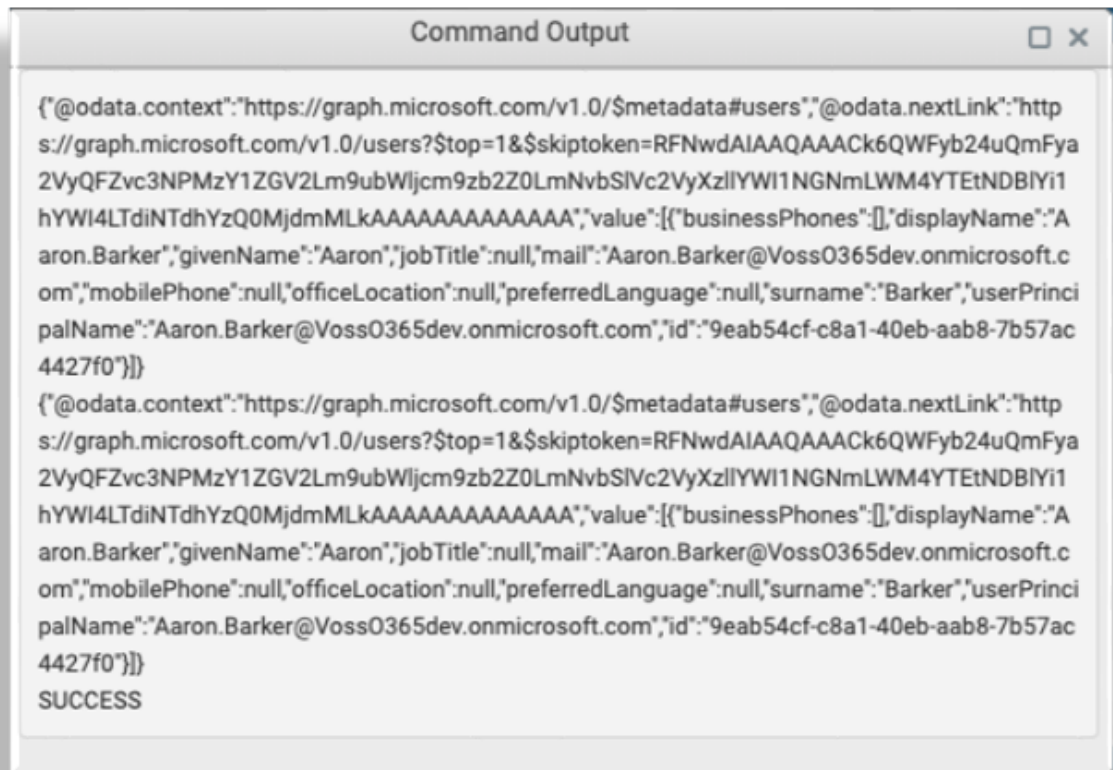
Note: These values should be for a client that is dedicated to this use and should not be used to request a token from any other source while the API collector is enabled.

- At **Customer**, fill out the tenant id (**Directory (tenant) ID**).
- At **Name**, fill out an easily identifiable account name.
- At **ClientID**, fill out the client ID (**Application (client) ID**).
- At **ClientSecret**, fill out the client secret value.

6. Click **Verify Access** to test access to the API.

7. If the result of verifying access to the API indicates successful data retrieval, click **Save Data** to save the configuration.

The image displays a success response:



```
Command Output

{"@odata.context":"https://graph.microsoft.com/v1.0/$metadata#users","@odata.nextLink":"https://graph.microsoft.com/v1.0/users?$top=1&$skiptoken=RFNwdAIAAQAAACk6QWFyb24uQmFya2VyQFZvc3NPMzY1ZGV2Lm9ubWljcm9zb2Z0LmNvbSIVc2VyXzllYW11NGNmLWM4YTEtNDBiYi1hYWI4LTdiNTdhYzQ0MjdmMLkAAAAAAAAAAAAA","value":[{"businessPhones":[],"displayName":"Aaron.Barker","givenName":"Aaron","jobTitle":null,"mail":"Aaron.Barker@Voss0365dev.onmicrosoft.com","mobilePhone":null,"officeLocation":null,"preferredLanguage":null,"surname":"Barker","userPrincipalName":"Aaron.Barker@Voss0365dev.onmicrosoft.com","id":"9eab54cf-c8a1-40eb-aab8-7b57ac4427f0"}]}

{"@odata.context":"https://graph.microsoft.com/v1.0/$metadata#users","@odata.nextLink":"https://graph.microsoft.com/v1.0/users?$top=1&$skiptoken=RFNwdAIAAQAAACk6QWFyb24uQmFya2VyQFZvc3NPMzY1ZGV2Lm9ubWljcm9zb2Z0LmNvbSIVc2VyXzllYW11NGNmLWM4YTEtNDBiYi1hYWI4LTdiNTdhYzQ0MjdmMLkAAAAAAAAAAAAA","value":[{"businessPhones":[],"displayName":"Aaron.Barker","givenName":"Aaron","jobTitle":null,"mail":"Aaron.Barker@Voss0365dev.onmicrosoft.com","mobilePhone":null,"officeLocation":null,"preferredLanguage":null,"surname":"Barker","userPrincipalName":"Aaron.Barker@Voss0365dev.onmicrosoft.com","id":"9eab54cf-c8a1-40eb-aab8-7b57ac4427f0"}]}

SUCCESS
```

8. Refresh the screen (move away from the configuration screen to another and back) to see the new configuration.