Detect for Azure AD and M365 Quick Start Guide

Version 3

It takes less than **10 minutes** to set up Vectra's Detect for Azure AD and M365. Once up and running you will be able to see and stop threats to your SaaS apps, Azure AD backend, and M365 data.

The process is easy:

1. Create a data connector in your Vectra UI.
2. Grant Vectra read-only access to your Azure AD and M365 data logs (Global Admin permissions required).

For a step-by-step guide, select the type of Vectra UI below.

On-premise or a virtual Brain UI

START

SaaS UI

START

Additional Information related to the following topics are presented at the end of this document.

- Optional Sensitive Data Anonymization
- Summary of Data and Access Requirements
- Opting Out of Detect for Azure AD and M365
- Modifying Vectra's OAuth Application Settings
- Detection Learning Times
- Simulation of an Azure AD and M365 Attack
- Worldwide Support Contact Information

On-premises or Virtual Brain: Quick Start Vectra

On-premises or Virtual Brain: Network Setup

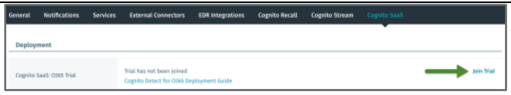
Your Vectra Brain must be able to securely access Vectra's managed resources over TCP/443 HTTPS connections to report detection events to your Vectra UI. Please configure your firewall and access rules accordingly.

Destination	Note
global-api-mgmt.azure-api.net or if your FW will not resolve the FQDN: 40.127.142.86	Required for all Sensors
https://authgateway.uw2.public.app.prod.vectra-svc.ai/	Required for Sensors deployed in US
https://authgateway.ew1.public.app.prod.vectra-svc.ai/	Required for Sensors deployed in EU
https://authgateway.cc1.public.app.prod.vectra-svc.ai/	Required for Sensors deployed in Canada
https://authgateway.as2.public.app.prod.vectra-svc.ai/	Required for Sensors deployed in Australia

On-premises or Virtual Brain: Connection Setup

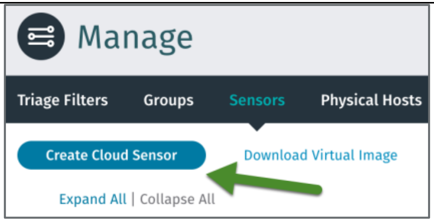
Create a Sensor in the Vectra UI.

1
- Navigate to Settings > Cognito SaaS.
- Click the "Join Trial" button and accept the trial agreement.

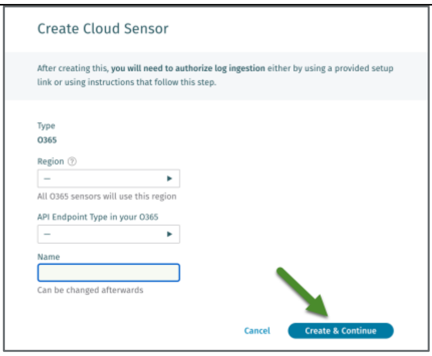


Cognito SaaS: O365 Trial   Trial has not been joined

2
- Navigate to Manage > Sensors.
- Click the "Create SaaS Sensor" button.



3
- Provide the region where data should reside.
- Provide your endpoint type.
- Provide a name for your connection.
- Click "Create and Continue".



Create Cloud Sensor

After creating this, **you will need to authorize log ingestion** either by using a provided setup link or using instructions that follow this step.

Type
O365

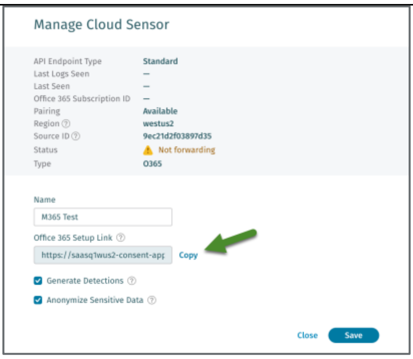
Region
—
All O365 sensors will use this region

API Endpoint Type in your O365
—

Name

Can be changed afterwards

4
- Provide the O365 Setup Link to a tenant Global Admin to authorize.
- Confirm that Generate Detection is toggled on.
- Select whether sensitive data should be anonymized. Select whether sensitive data should be anonymized for Vectra and your analysts.
- Click "Save".



Manage Cloud Sensor

API Endpoint Type	Standard
Last Logs Seen	—
Last Seen	—
Office 365 Subscription ID	—
Pairing	Available
Region	westus2
Source ID	9ec21d2f03897d35
Status	⚠ Not forwarding
Type	O365

Name
M365 Test

Office 365 Setup Link
https://saasq1wus2-consent-apr

☑ Generate Detections

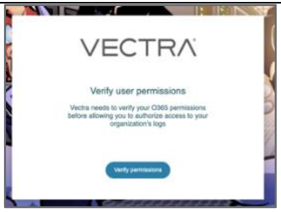
☑ Anonymize Sensitive Data

On-premises or Virtual Brain: Authorize Read-Only Data Access

Have your **Azure AD Global Admin** follow the link above and authorize Vectra to collect logs.

1

- Using the O365 Setup Link, the Global Admin should Verify their Azure AD permissions and authorize access to the tenant's logs.



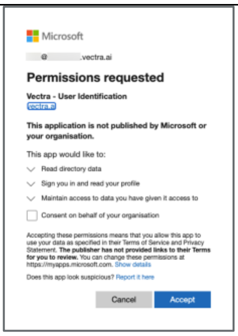
VECTRA

Verify user permissions

Vectra needs to verify your O365 permissions before allowing you to authorize access to your organization's logs

2

- Review the read-only access required by "Vectra - User Identification" OAuth app to validate your permissions.
  - User.Read (Graph API)
  - Directory.Read.All (Graph API)
  - Offline Access (Added by default by Microsoft – but not requested)
- Click "Accept".



Microsoft

[redacted]@[redacted].vectra.ai

Permissions requested

Vectra - User Identification
vectra.ai

This application is not published by Microsoft or your organisation.

This app would like to:

- Read directory data
- Sign you in and read your profile
- Maintain access to data you have given it access to

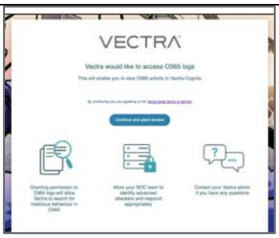
☐ Consent on behalf of your organisation

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

3

- Grant Vectra access to the Azure AD logs.



VECTRA

Vectra would like to access O365 logs

This will enable you to view O365 activity in Vectra Cognito

By continuing you are agreeing to the Vectra legal terms of service

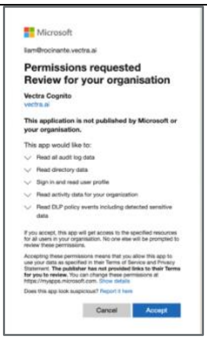
Granting permission to O365 logs will allow Vectra to search for malicious behaviour in O365

Allow your SOC team to identify advanced attackers and respond appropriately

Contact your Vectra admin if you have any questions

4

- Review the read-only access required by the Vectra "Vectra Cognito" OAuth app to validate your permissions.
  - ActivityFeed.Read (Office Management API)
  - ActivityFeed.ReadDLP (Office Management API)
  - Directory.Read.ALL (Graph API for Azure AD logs)
  - AuditLog.Read.All (Graph API for Azure AD logs)
  - User.Read (Added by default by Microsoft – this is not actually requested)
- Click "Accept."



Microsoft

liam@rocinante.vectra.ai

Permissions requested
Review for your organisation

Vectra Cognito
vectra.ai

This application is not published by Microsoft or your organisation.

This app would like to:

- Read all audit log data
- Read directory data
- Sign in and read user profile
- Read activity data for your organization
- Read DLP policy events including detected sensitive data

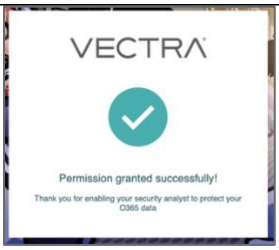
If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

5

- You are "Done"!



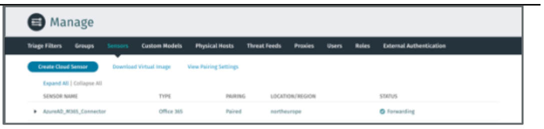
VECTRA

Permission granted successfully!

Thank you for enabling your security analyst to protect your O365 data

On-premises or Virtual Brain: Validate Data Collection

Once access is authorized the Status on Manage> Sensors for your Sensor should report "Forwarding". This status may take five minutes to appear while the initial data is collected.



Manage

SENSOR NAME	TYPE	PAIRING	LOCATION/REGION	STATUS
AzureAD_M365_Connector	Office 365	Paired	northeurope	Forwarding

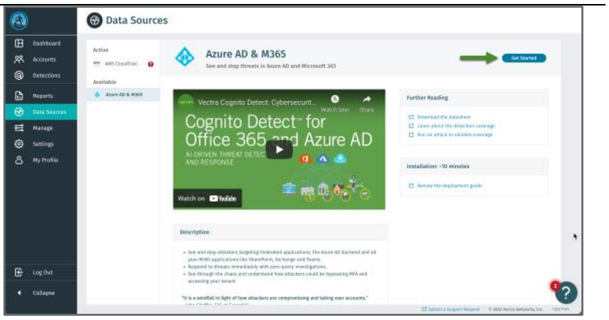
SaaS Quick Start Vectra

SaaS: Connection Setup

Create a data connector in the Vectra UI.

1

- Navigate to Data Sources > Azure AD & M365 Click “Get Started”.



Data Sources

Active: AWS CloudTrail

Available: Azure AD & M365

Azure AD & M365
See and stop threats in Azure AD and Microsoft 365

Further Reading
- Download the datasheet
- Learn about the detection coverage
- Run an attack to validate coverage

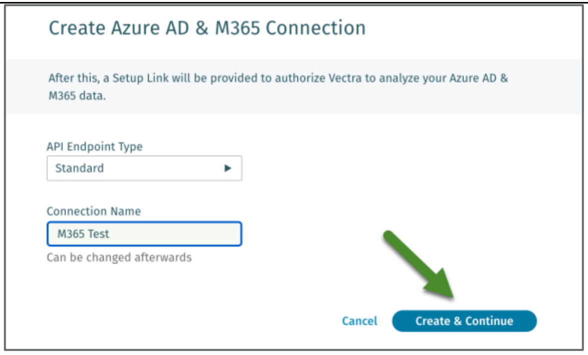
Installation: ~10 minutes
- Review the deployment guide

Description
- See and stop attackers targeting federated applications, the Azure AD backend and all your M365 applications like SharePoint, Exchange and Teams.
- Respond to threats immediately with zero-query investigations.
- See through the chaos and understand how attackers could be bypassing MFA and accessing your tenant.

"It is a windfall in light of how attackers are compromising and taking over accounts."

2

- Provide your endpoint type.
- Provide a name for your connection.
- Click “Create and Continue”.



Create Azure AD & M365 Connection

After this, a Setup Link will be provided to authorize Vectra to analyze your Azure AD & M365 data.

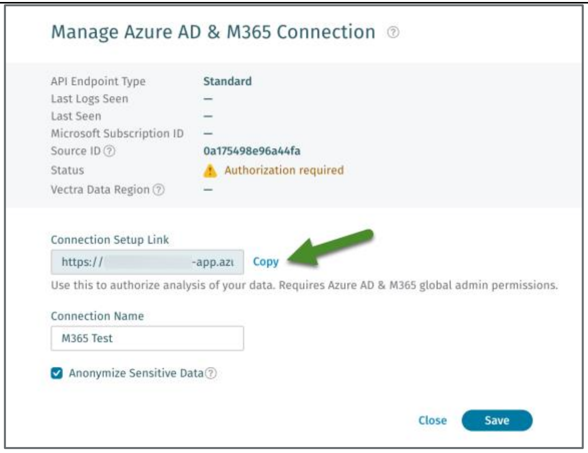
API Endpoint Type: Standard

Connection Name: M365 Test

Can be changed afterwards

3

- Provide the Connection Setup Link to a tenant Global Admin to authorize Vectra read-only access to your data.
- Select whether sensitive data should be anonymized for Vectra and your analysts.
- Click “Save”.



Manage Azure AD & M365 Connection

API Endpoint Type	Standard
Last Logs Seen	–
Last Seen	–
Microsoft Subscription ID	–
Source ID	0a175498e96a44fa
Status	Authorization required
Vectra Data Region	–

Connection Setup Link: https:// -app.azı

Use this to authorize analysis of your data. Requires Azure AD & M365 global admin permissions.

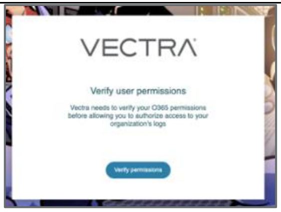
Connection Name: M365 Test

☑ Anonymize Sensitive Data

SaaS: Authorize Read-Only Data Access

Have your **Azure AD Global Admin** follow the link above and authorize Vectra to collect logs.

1
- Using the O365 Setup Link, the Global Admin should Verify their Azure AD permissions and authorize access to the tenant's logs.

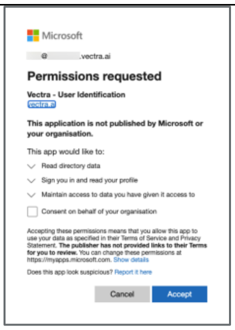


VECTRA

Verify user permissions

Vectra needs to verify your O365 permissions before allowing you to authorize access to your organization's logs

2
- Review the read-only access required by "Vectra - User Identification" OAuth app to validate your permissions.
  - User.Read (Graph API)
  - Directory.Read.All (Graph API)
  - Offline Access (Added by default by Microsoft – but not requested)
- Click "Accept".



Microsoft

[redacted]@[redacted].vectra.ai

Permissions requested

Vectra - User Identification
vectra.ai

This application is not published by Microsoft or your organisation.

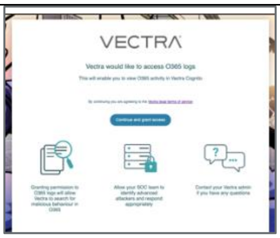
This app would like to:
- Read directory data
- Sign you in and read your profile
- Maintain access to data you have given it access to

□ Consent on behalf of your organisation

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

3
- Grant Vectra access to the Azure AD logs.



VECTRA

Vectra would like to access O365 logs

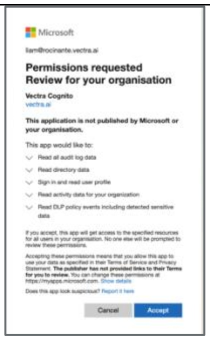
This will enable you to view O365 activity in Vectra Cognito

Granting permission to O365 logs will allow Vectra to search for malicious behaviour in O365

Allow your SOC team to identify advanced attackers and respond appropriately

Contact your Vectra admin if you have any questions

4
- Review the read-only access required by the Vectra "Vectra Cognito" OAuth app to validate your permissions.
  - ActivityFeed.Read (Office Management API)
  - ActivityFeed.ReadDLP (Office Management API)
  - Directory.Read.ALL (Graph API for Azure AD logs)
  - AuditLog.Read.All (Graph API for Azure AD logs)
  - User.Read (Added by default by Microsoft – this is not actually requested)
- Click "Accept."



Microsoft

liam@rocinante.vectra.ai

Permissions requested
Review for your organisation

Vectra Cognito
vectra.ai

This application is not published by Microsoft or your organisation.

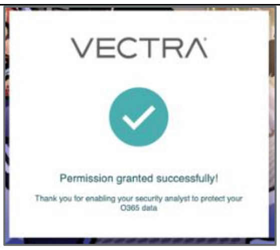
This app would like to:
- Read all audit log data
- Read directory data
- Sign in and read user profile
- Read activity data for your organization
- Read DLP policy events including detected sensitive data

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

5
- You are "Done"!



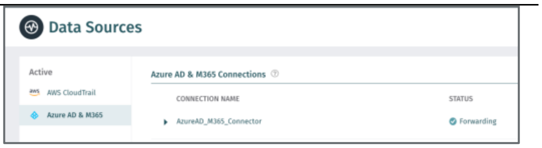
VECTRA

Permission granted successfully!

Thank you for enabling your security analyst to protect your O365 data

SaaS: Validate Data Collection

Once access is authorized the Status on Data Sources > Azure AD & M365 should report "Forwarding". This status may take five minutes to appear while the initial data is collected.



Data Sources

Azure AD & M365 Connections

CONNECTION NAME	STATUS
AzureAD_M365_Connector	Forwarding

Additional Information

Optional Sensitive Data Anonymization

When creating a Vectra data connection, customers have the option for sensitive data fields, including SharePoint filenames, to be anonymized. The original values are not persisted in Vectra's cloud infrastructure. Note that this anonymization can limit analysts' visibility into their fields when investigating related threats. Anonymized fields are stored as Vectra-hash, where the hash is of the string value, not an underlying file or email. Anonymization can be enabled or disabled from the management of the connector. Changes to this anonymization are not retroactive.

Summary of Data and Access Requirements

The Management API is used to collect 'Audit.AzureActiveDirectory', 'Audit.Exchange', 'Audit.SharePoint', 'Audit.General', and 'DLP.All' logs.

- Auditing via the Management Activity API is required for Vectra to provide coverage
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide
- Additional details about the data collected can be found here:
  - https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema

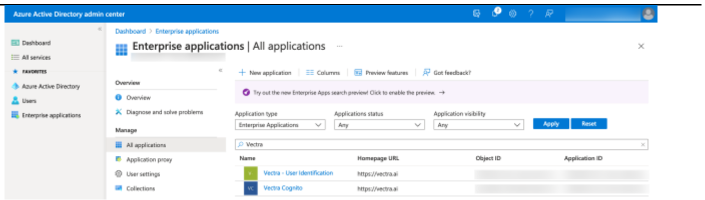
The Microsoft Graph API is used to collect 'directoryAudits' and 'signIns' logs.

- Additional details about the data collected can be found here:
  - https://docs.microsoft.com/en-us/graph/api/signin-list?view=graph-rest-1.0&tabs=http
  - https://docs.microsoft.com/en-us/graph/api/directoryaudit-list?view=graph-rest-1.0&tabs=http

Opting Out of Detect for Azure AD and M365

If you wish to stop using Detect for Azure AD and M365, any Application Admin / Global Admin can delete the application from the "Enterprise Applications" page in the AAD (Azure Active Directory) part of the Azure portal.

- As an Application Admin / Global Admin login to portal.azure.com
- Navigate to "Azure Active Directory" and click on "Enterprise applications" from the left navigation bar.

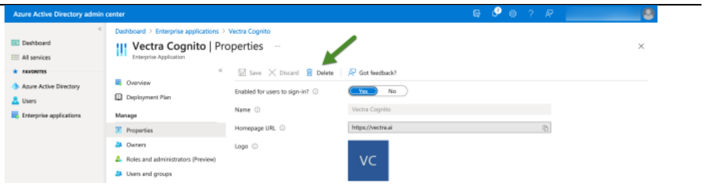


Application type: Enterprise Applications
Applications status: Any
Application visibility: Any

Search: Vectra

Name	Homepage URL	Object ID	Application ID
Vectra - User Identification	https://vectra.ai	[redacted]	[redacted]
Vectra Cognito	https://vectra.ai	[redacted]	[redacted]

- Click on the Vectra application, then click on "Properties" and then click on "Delete" to delete the application.



Enabled for users to sign-in? [✓ Yes] No
Name: Vectra Cognito
Homepage URL: https://vectra.ai
Logo

- Once the consent is pulled, the Sensor/Connector will report "CONSENT REVOKED" state and log collection will stop. The Sensor/Connector in the Vectra UI can be deleted before or after the consent is pulled.

Modifying Vectra's OAuth Application Settings

The OAuth application used to collect data has been configured in alignment with Microsoft's best practices. Changes to the application's settings can disrupt Vectra's access to the necessary logs and prevent detections. Customers may change the "Visible to users" toggle to off.

Detection Learning Times

Vectra uses multiple modeling techniques to detect attacker behaviors in your Azure AD and M365 environment. Some Vectra detections are designed to alert on threats immediately and can find active attacker behaviors in the first few hours of a deployment. Other detections may require an initial baseline period to become operational. All detections complete their initial baseline period after at most seven days. Detections that leverage baselines continue to learn after the initial period and improve their performance over time.

Simulation of an Azure AD and M365 Attack

Customers can leverage the attack simulation guide here to replicate techniques commonly used by attackers against Azure AD and M365 and see how Vectra can identify the attacker's actions and prioritize the threat. The guide provides step-by-step actions and can be completed in less than an hour without impacting normal operations.

Worldwide Support Contact Information

- Support portal: https://support.vectra.ai
- Email: support@vectra.ai (preferred contact method)
- Additional information: https://www.vectra.ai/support