



Lab Manual- Setup and Manage Azure Sentinel

Prepared for:

Date: 18th Nov 2021

Prepared by:

Document Name: Lab Manual

Document Number AZLabn989

Contributor:

Contents

1. Introduction.....	3
2. Lab: Setup Azure Sentinel workspace	3
2.1 Enable Microsoft Sentinel	3
3.1 Connect to Active Directory	5
2.2 Connect to Azure Activity	6

1. Introduction

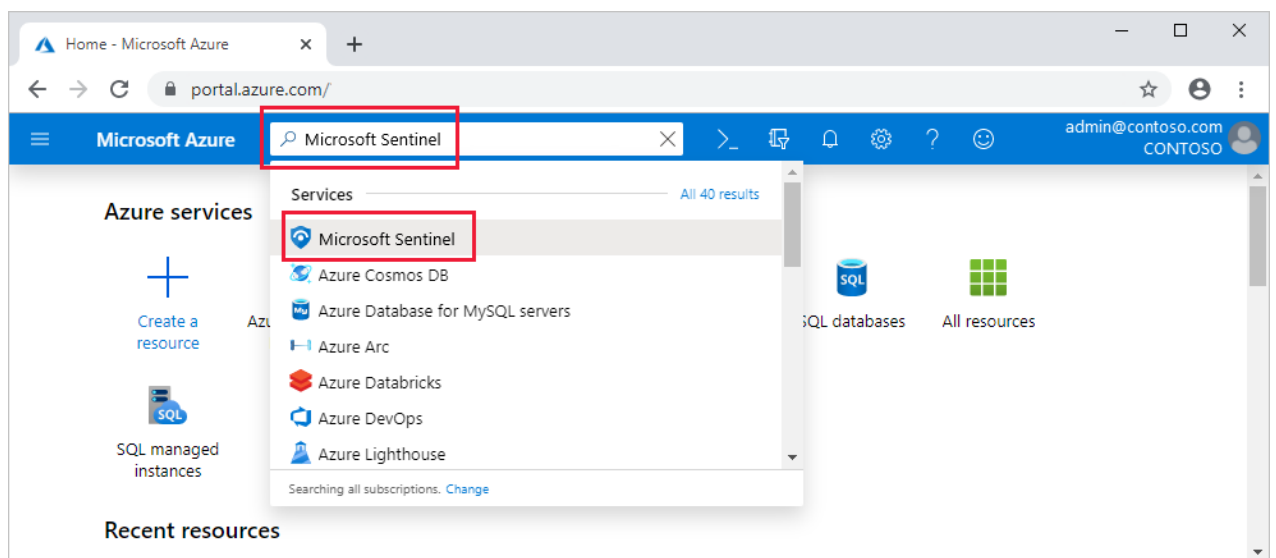
Microsoft Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Defender for Cloud Apps, security alerts from Microsoft Defender for Cloud, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Microsoft Sentinel

In this Lab , we will understand how to create an Azure sentinel workspace and connect with Data source

2. Lab: Setup Azure Sentinel workspace

2.1 Enable Microsoft Sentinel

1. Sign in to the Azure portal. Make sure that the subscription in which Microsoft Sentinel is created is selected.
2. Search for and select **Microsoft Sentinel**.



3. Select **Add**.
4. create a new one.

Create Log Analytics workspace

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

[Create new](#)

Instance details

Name * ⓘ

Region * ⓘ

5. Click Review and Create

6. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade,

Dashboard > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

+ Create a new workspace Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓
Sentinaldemo	eastus	AZ-500

Add Cancel

7. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade

bipin.sinhaa@outlook.c...
DEFAULT DIRECTORY (TECHPLED...)

Notifications

More events in the activity log → Dismiss all ✓

✓ Successfully added Microsoft Sentinel

Successfully added Microsoft Sentinel to workspace 'Sentinaldemo', it might take a few minutes for your workspace to appear in Microsoft Sentinel workspaces list

a few seconds ago

8. Once Created click add to On the **Add Microsoft Sentinel to a workspace blade**

Dashboard > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | News & guides

Selected workspace: 'Sentinaldemo'


Search (Ctrl+/) Documentation

What's new **Get started** Free trial

Microsoft Sentinel

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.



- 1. Collect data**
Collect data at cloud scale across the enterprise, both on-premises and in multiple clouds
[Connect](#)
- 2. Create security alerts**
Focus on what's important using analytics to create alerts
[Create](#)
- 3. Automate & orchestrate**
Use or customize built-in playbooks to automate common tasks
[Create](#)

General

- Overview
- Logs
- News & guides**
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics
- Watchlist
- Automation

3.1 Connect to Active Directory

1. In Microsoft Sentinel, select **Data connectors** from the navigation menu.
2. From the data connectors gallery, select **Azure Active Directory**

Dashboard > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'Sentinaldemo'

Search (Ctrl+/) Guides & Feedback Refresh

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors**
- Analytics

123 Connectors **0** Connected [More content at Content hub](#)

act Providers: **All** Data Types: **All** Status: **All**

Status	Connector name
	Alsid for Active Directory (Preview) Alsid
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Perimeter 81 Activity Logs (Preview) Perimeter 81

3. Then select **Open connector page**.

The screenshot shows the 'Data connectors' interface. On the left, a list of connectors is displayed, with 'Azure Active Directory' selected and highlighted by a red rectangle. On the right, the details for the 'Azure Active Directory' connector are shown. At the bottom of this details pane, the 'Open connector page' button is highlighted with a red rectangle.

4. Mark the check boxes next to the log types you want to stream into Microsoft Sentinel (see below), and select **Connect**.

Azure Active Directory

The screenshot shows the configuration page for the 'Azure Active Directory' connector. On the left, there's a summary of the connector's status and related content. On the right, the 'Configuration' section is active, showing a list of log types to be streamed into Microsoft Sentinel. The 'Sign-In Logs' checkbox is checked. Below it, a blue information box states: 'In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).' Below this, several other log types are checked, including 'Audit Logs', 'Non-Interactive User Sign-In Log (Preview)', 'Service Principal Sign-In Logs (Preview)', 'Managed Identity Sign-In Logs (Preview)', 'User Risk Events (Preview)', 'Risky Users (Preview)', 'Network Access Traffic Logs (Preview)', and 'Risky Service Principals (Preview)'. The 'Provisioning Logs (Preview)' and 'ADFS Sign-In Logs (Preview)' are unchecked.

5. Mark the check boxes next to the log types you want to stream into Microsoft Sentinel (see below), and select **Apply Changes**

2.2 Connect to Azure Activity

1. On the **Microsoft Sentinel | Data connectors** blade, review the list of available connectors, type **Azure** into the search bar and select the entry representing the **Azure Activity** connector

Data connectors ...

Guides & Feedback Refresh

123 Connectors 0 Connected More content at Content hub

Search: azure Providers: All Data Types: All Status: All

Status Connector name

- Azure Active Directory Microsoft
- Azure Active Directory Identity Protection Microsoft
- Azure Activity Microsoft**
- Azure DDoS Protection Microsoft
- Azure Firewall Microsoft
- Azure Information Protection (Preview) Microsoft
- Azure Key Vault Microsoft
- Azure Kubernetes Service (AKS) Microsoft
- Azure SQL Databases Microsoft
- Azure Storage Account Microsoft
- Azure Web Application Firewall (WAF) Microsoft

Azure Activity

Not connected Status Microsoft Provider Last Log Received

Description

Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received

--

Related content

2 Workbooks 2 Queries 24 Analytics rules templates

Data received

Go to log analytics

100

80

60

40

20

0

April 9 April 11 April 13

Total data received

0

Data types

AzureActivity

2. Then select **Open connector page**.
3. On the **Azure Activity** blade the **Instructions** tab should be selected, note the **Prerequisites** and scroll down to the **Configuration**. Take note of the information describing the connector update. Your Azure Pass subscription never used the legacy connection method so you can skip step 1 (the **Disconnect All** button will be grayed out) and proceed to step 2.
4. In step 2 **Connect your subscriptions through diagnostic settings new pipeline**, review the "Launch the Azure Policy Assignment wizard and follow the steps" instructions then click **Launch the Azure Policy Assignment wizard**.

Azure Activity ...

Azure Activity

Not connected

Status

Microsoft

Provider

Last Log Received

--

Description

Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received

--

Related content

2

Workbooks

2

Queries

24

Analytics rules templates

Data received

Go to log analytics

Total data received

10

Data types

AzureActivity

Instructions

Next steps

Configuration

This connector has been updated to use the diagnostics settings back-end pipeline, which provides increased functionality and better consistency with resource logs. Connectors using this pipeline can also be governed at scale by Azure Policy. Learn more about the new [Azure Activity connector](#). Follow the instructions below to upgrade your connector to the diagnostics settings pipeline.

1. Disconnect your subscriptions from the legacy method

The subscriptions listed below are still using the older, legacy method. You are strongly encouraged to upgrade to the new pipeline. To do this, click on the 'Disconnect All' button below, before proceeding to launch the Azure Policy Assignment wizard.

You don't have subscriptions using the legacy method, please move to step 2

Disconnect All

2. Connect your subscriptions through diagnostic settings new pipeline

This connector uses Azure Policy to apply a single Azure Subscription log-streaming configuration to a collection of subscriptions, defined as a scope. Follow the instructions below to create and apply a policy to all current and future subscriptions. **Note**, you may already have an active policy for this resource

Launch the Azure Policy Assignment wizard and follow the steps.

- In the **Basics** tab, click the button with the three dots under **Scope** to select your resources assignment scope.
- In the **Parameters** tab, choose your Microsoft Sentinel workspace from the **Log Analytics workspace** drop-down list, and leave marked as "True" all the ingest.
- To apply the policy on your existing resources, select the **Remediation** tab and mark the **Create a remediation task** checkbox.

Launch Azure Policy Assignment wizard>

- On the **Configure Azure Activity logs to stream to specified Log Analytics workspace** (Assign Policy page) **Basics** tab, click the **Scope elipsis (...)** button. In the **Scope** page choose your Azure Pass subscription from the drop-down subscription list and click the **Select** button at the bottom of the page.

Home > Microsoft Sentinel > Microsoft Sentinel > Azure Activity >

Configure Azure Activity logs to stream to specified Log Analytics workspace ...

Assign policy

Basics

Parameters

Remediation

Non-compliance messages

Review + create

Scope

Scope [Learn more about setting the scope](#)

Scope

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assignment name *

Configure Azure Activity logs to stream to specified Log Analytics workspace

Description

Policy enforcement

Enabled Disabled

Assigned by

Bipeen sinha

Review + create

Cancel

Previous

Next

Scope

Management Group

Allianz-Life (Allianz-Life)

HCLBPO (HCLBPO)

HCLCORP (HCLCORP)

HCLTECH (HCLTECH)

ibmservers (ibmservers)

JKBIT (JKBIT)

JKBSales (JKBSales)

panafica-africa (panafica-africa)

panafica-EMEA (panafica-EMEA)

panafica-europe (panafica-europe)

reljio (reljio)

rilpetroleum (rilpetroleum)

RILPETROLEUM (RILPETROLEUM)

TPCS-Consulting (TPCS-Consulting)

TPCS-Develop (TPCS-Develop)

TPCS-Training (TPCS-Training)

WiproElectronics (WiproElectronics)

WiproSoftware (WiproSoftware)

WiproSupport (WiproSupport)

Subscription

Microsoft Partner Network

Resource Group

Optionally choose a Resource Group

Select

Cancel

Clear All Selections

- Click Next

Configure Azure Activity logs to stream to specified Log Analytics workspace ...

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Scope

Scope [Learn more about setting the scope *](#)

Microsoft Partner Network ✓ ...

Exclusions

Optionally select resources to exclude from the policy assignment. ...

Basics

Policy definition

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assignment name * ⓘ

Configure Azure Activity logs to stream to specified Log Analytics workspace

Description

Policy enforcement ⓘ

Enabled Disabled

Assigned by

Bipeen sinha

Review + create

Cancel

Previous

Next

7. Click Next

8. Click the **Next** button at the bottom of the **Basics** tab to proceed to the **Parameters** tab. On the **Parameters** tab click the **Primary Log Analytics workspace elipsis (...)** button. In the **Primary Log Analytics workspace** page, make sure your Azure pass subscription is selected and use the **workspaces** drop-down to select the Log Analytics workspace you are using for Sentinel.

Configure Azure Activity logs to stream to specified Log Analytics workspace ...

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Search by parameter name ☒ Only show parameters that need input or review

Primary Log Analytics workspace * ⓘ

Review + create

Cancel

Previous

Next

Primary Log Analytics workspace ×

Subscription

Microsoft Partner Network

workspaces

Sentinaldemo

Select

Cancel

9. When done click the **Select** button at the bottom of the page and click **Next**

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Search by parameter name

☒ Only show parameters that need input or review

Primary Log Analytics workspace * ⓘ

Sentinaldemo

10. Click the **Next** button at the bottom of the **Parameters** tab to proceed to the **Remediation** tab. On the **Remediation** tab select the **Create a remediation task** checkbox. This will enable the "Configure Azure Activity logs to stream to specified Log Analytics workspace" in the **Policy to remediate** drop-down. In the **System assigned identity location** drop-down, select the region (East US for example) you selected earlier for your Log Analytics workspace.

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel](#) > [Azure Activity](#) >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

☒ Create a remediation task ⓘ

Policy to remediate

Configure Azure Activity logs to stream to specified Log Analytics workspace

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)

☒ Create a Managed Identity ⓘ

Type of Managed Identity ⓘ

☒ System assigned managed identity ☐ User assigned managed identity

System assigned identity location *

East US

Remediations

C

11. Click the **Next** button at the bottom of the **Remediation** tab to proceed to the **Non-compliance message** tab. Enter a Non-compliance message if you wish (this is optional) and click the **Review + Create** button at the bottom of the **Non-compliance message** tab.

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel](#) > [Azure Activity](#) >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Non-compliance messages help users understand why a resource is not compliant with the policy. The message will be displayed when a resource is denied and in the evaluation details of any non-compliant resource.

Non-compliance message

Contact Security Head

12. Click the **Create** button. You should observe three succeeded status messages: **Creating policy assignment succeeded**, **Role Assignments creation succeeded**, and **Remediation task creation succeeded**.

13. Verify that the **Azure Activity** pane displays the **Data received** graph (you might have to refresh the browser page).

Note: It may take over 15 minutes before the Status shows "Connected" and the graph displays Data received.

The screenshot displays the Microsoft Sentinel interface for Data connectors. The left sidebar shows navigation options under 'General', 'Threat management', 'Content management', and 'Configuration'. The 'Configuration' section is expanded, and 'Data connectors' is selected. The main area shows a list of connectors for the 'azure' provider. The 'Azure Activity' connector is highlighted, and its status is 'Connected'. The right pane shows the 'Azure Activity' details, including a 'Data received' graph. The graph shows a sharp increase in data received starting around 04/14/22, 12:10 PM, reaching a total of 28. The status is 'Connected' and the last log received is 9 minutes ago.

Home > Microsoft Sentinel | Data connectors

Selected workspace: 'sentinaldemo'

Search (Ctrl+F) Guides & Feedback Refresh

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors**
- Analytics
- Watchlist
- Automation
- Settings

123 Connectors 2 Connected More content at Content hub

Search azure Providers: All Data Types: All Status: All

Status	Connector name
Connected	Azure Active Directory
Connected	Azure Active Directory Identity Protection
Connected	Azure Activity
Connected	Azure DDoS Protection
Connected	Azure Firewall
Connected	Azure Information Protection (Preview)
Connected	Azure Key Vault
Connected	Azure Kubernetes Service (AKS)
Connected	Azure SQL Databases
Connected	Azure Storage Account
Connected	Azure Web Application Firewall (WAF)

Azure Activity

Connected Status Microsoft 9 minutes ago Last Log Received

subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received 04/14/22, 12:10 PM

Related content 2 Workbooks 2 Queries 24 Analytics rules templates

Data received 30 25 20 15 10 5 0

Go to log analytics

Total data received 28

Data types AzureActivity 04/14/22, 12:10 PM

Open connector page