Lab Manual- Setup and Manage Azure Sentinel with Preloaded data

Prepared for:

Date: 18th Nov 2021

Prepared by:

Document Name: Lab Manual

Document Number AZLabn990

Contributor:

Contents

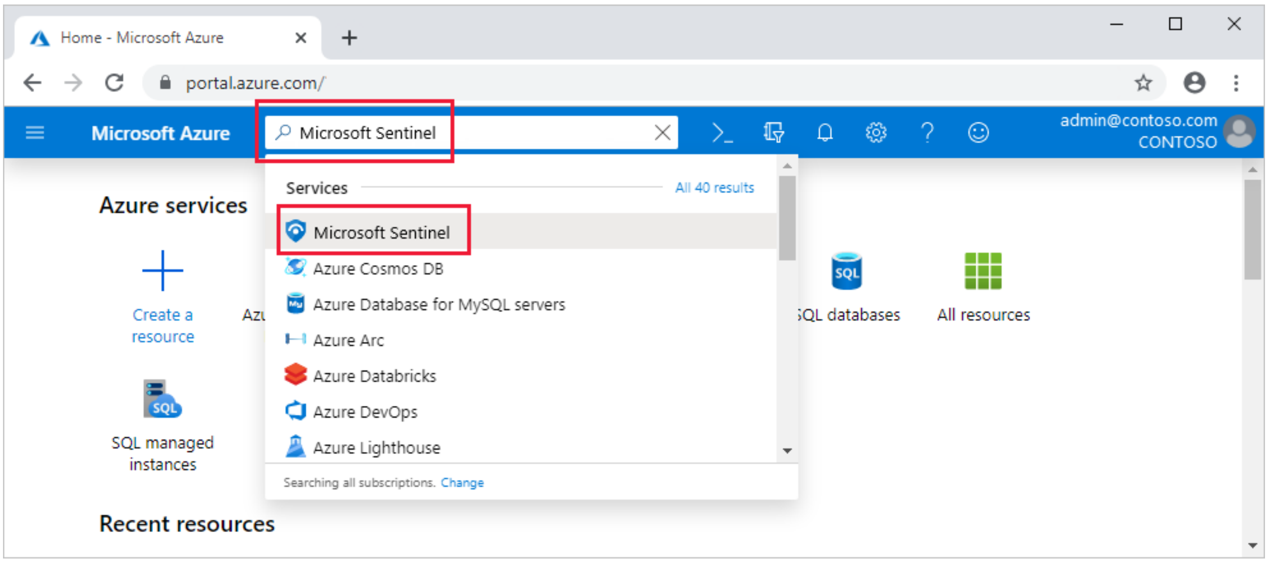
1. Introduction

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

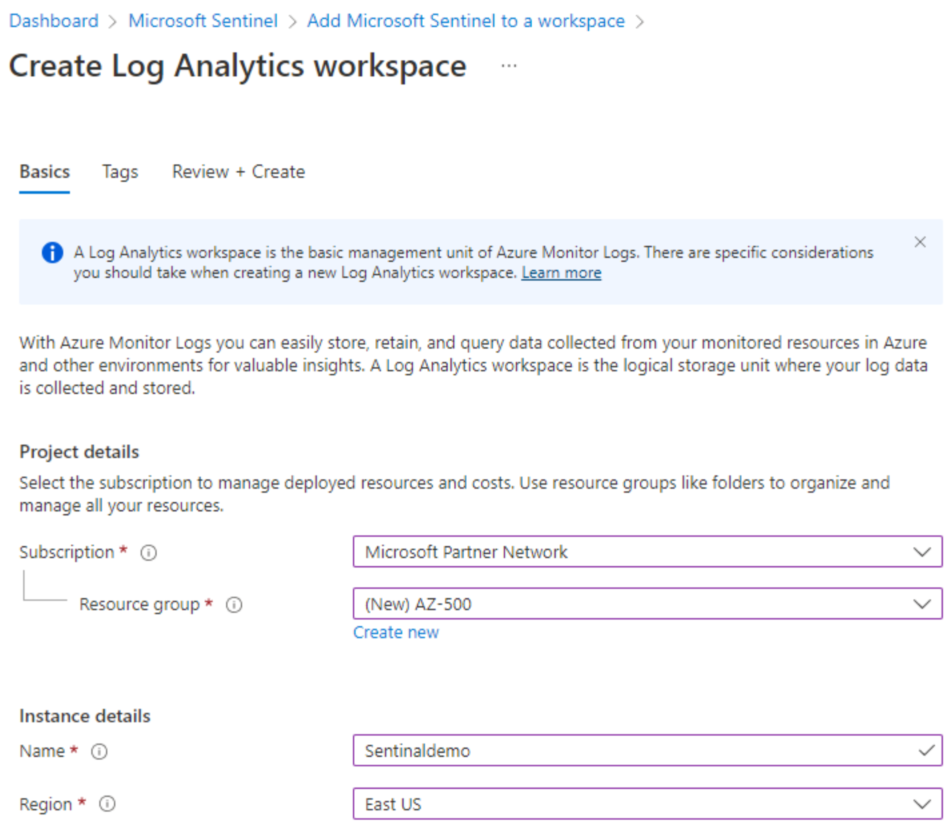
2. Lab: Setup Azure Sentinel workspace

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.



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

Create Log Analytics workspace ...

Basics Tags Review + Create

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 * : Microsoft Partner Network

Resource group * : (New) AZ-500

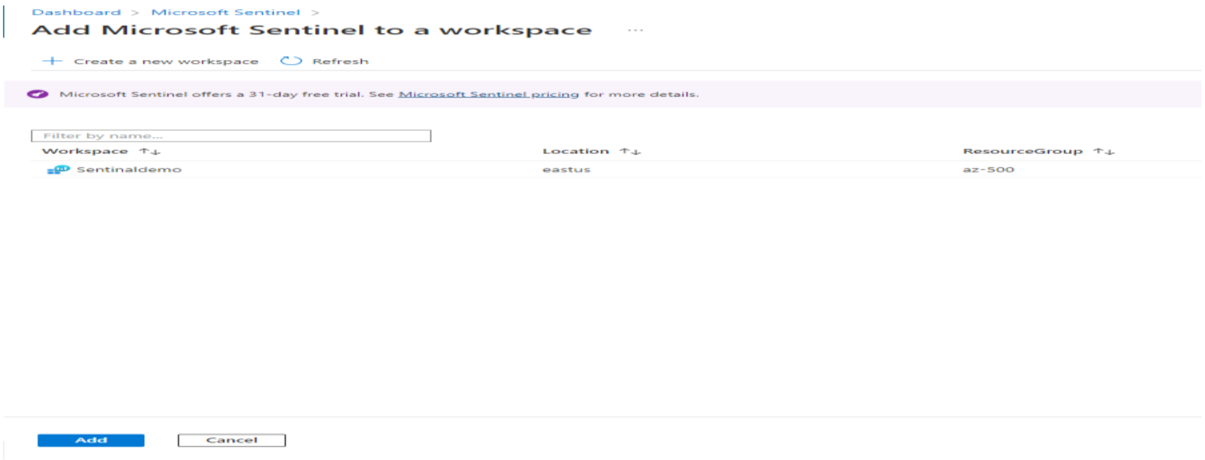
Create new

Instance details

Name * : Sentinaldemo

Region * : East US

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 ...

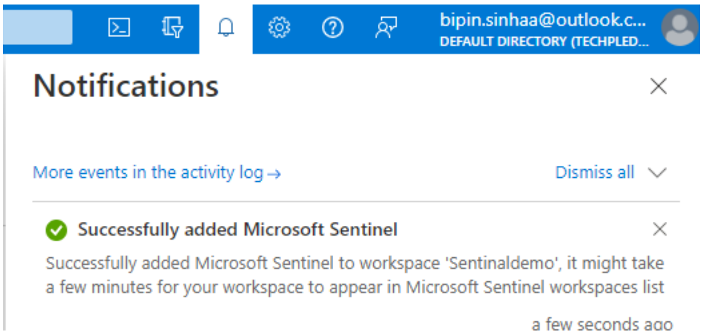
+ Create a new workspace   Refresh

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

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



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

Notifications

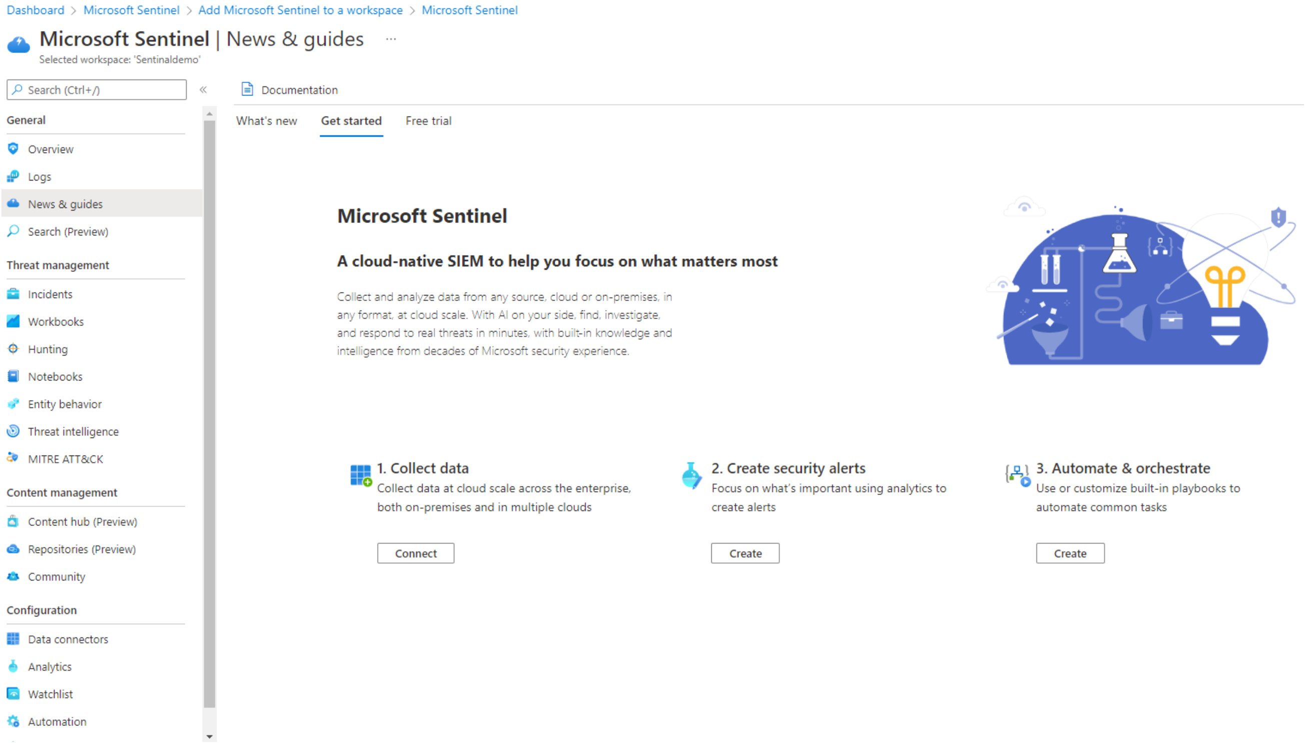
More events in the activity log →   Dismiss all

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



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

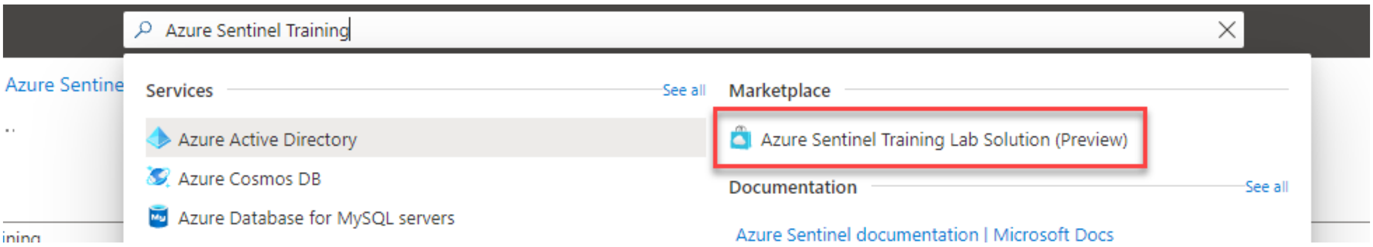
2. Create security alerts
Focus on what's important using analytics to create alerts

3. Automate & orchestrate
Use or customize built-in playbooks to automate common tasks

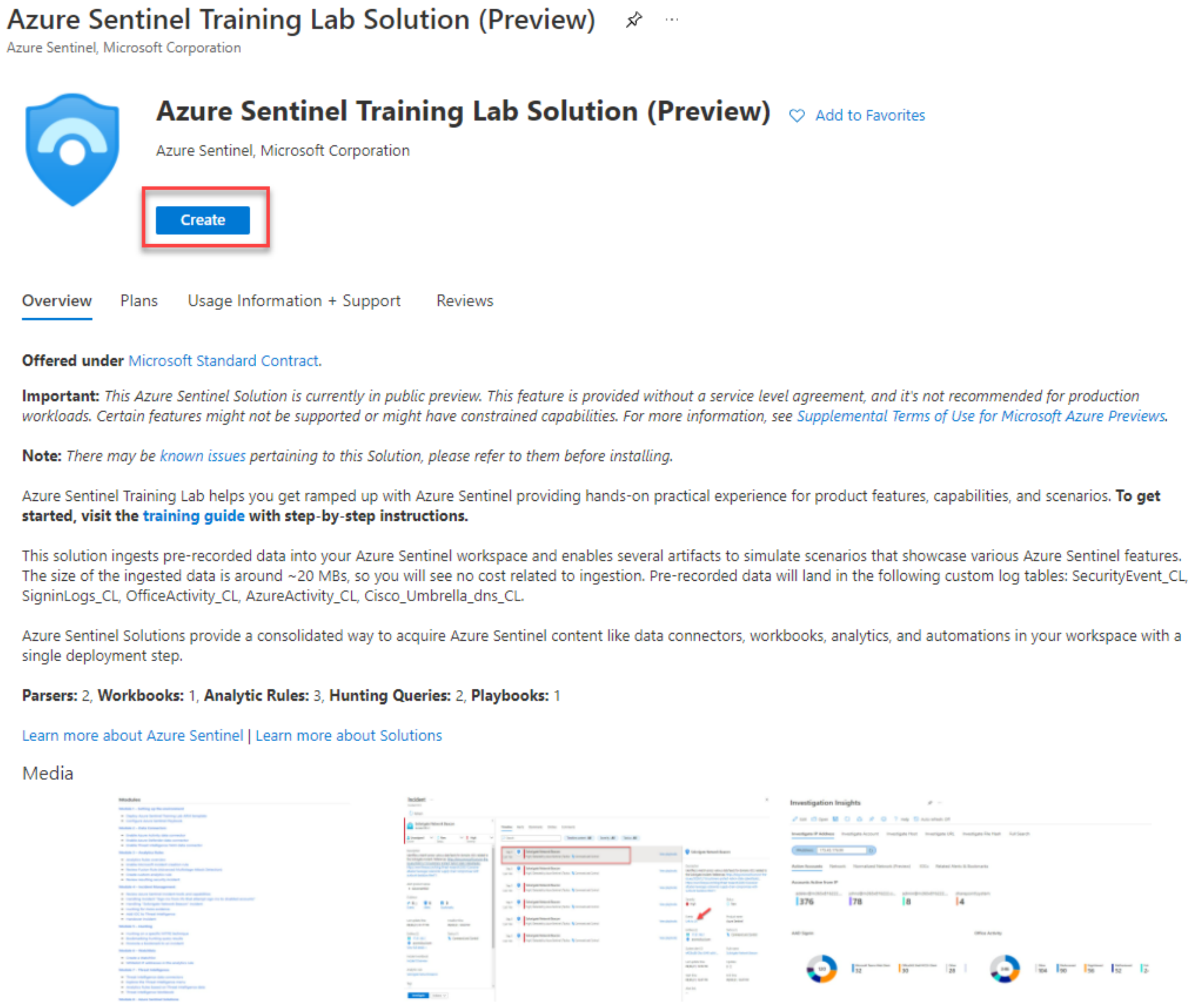
3. Exercise 2: Deploy the Microsoft Sentinel Training Lab Solution

In this exercise you will deploy the Training Lab solution into your existing workspace. This will ingest pre-recorded data (~20 MBs) and create several other artifacts that will be used during the exercises.

1. In the Azure Portal, go to the top search bar and type *Microsoft Sentinel Training*. Select the **Microsoft Sentinel Training Lab Solution (Preview)** marketplace item on the right.



2. Read the solution description and click **Create** at the top.



Azure Sentinel Training Lab Solution (Preview)

Azure Sentinel, Microsoft Corporation

Azure Sentinel Training Lab Solution (Preview)

Azure Sentinel, Microsoft Corporation

Offered under Microsoft Standard Contract.

Important: *This Azure Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see Supplemental Terms of Use for Microsoft Azure Previews.*

Note: *There may be known issues pertaining to this Solution, please refer to them before installing.*

Azure Sentinel Training Lab helps you get ramped up with Azure Sentinel providing hands-on practical experience for product features, capabilities, and scenarios. **To get started, visit the training guide with step-by-step instructions.**

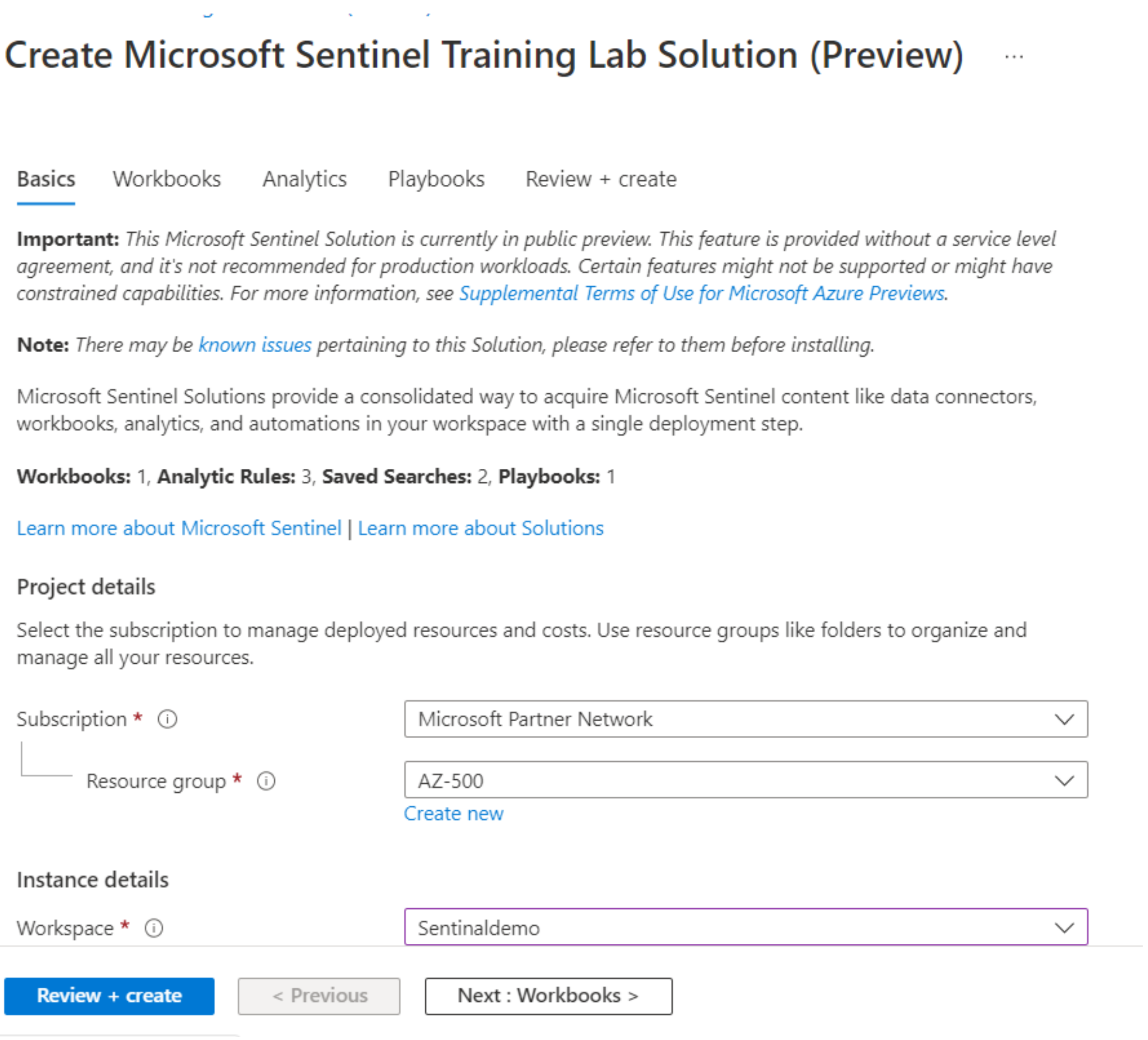
This solution ingests pre-recorded data into your Azure Sentinel workspace and enables several artifacts to simulate scenarios that showcase various Azure Sentinel features. The size of the ingested data is around ~20 MBs, so you will see no cost related to ingestion. Pre-recorded data will land in the following custom log tables: SecurityEvent_CL, SigninLogs_CL, OfficeActivity_CL, AzureActivity_CL, Cisco_Umbrella_dns_CL.

Azure Sentinel Solutions provide a consolidated way to acquire Azure Sentinel content like data connectors, workbooks, analytics, and automations in your workspace with a single deployment step.

Parsers: 2, **Workbooks:** 1, **Analytic Rules:** 3, **Hunting Queries:** 2, **Playbooks:** 1

Learn more about Azure Sentinel | Learn more about Solutions

3. In the Basics tab, select the Subscription, Resource Group and Workspace that you created in Exercise 1, or the details for your existing workspace. Optionally, review the different tabs (Workbooks, Analytics, Hunting Queries, Watchlists, Playbooks) in the solution. When ready, click on **Review + create**.



Create Microsoft Sentinel Training Lab Solution (Preview)

Important: *This Microsoft Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see Supplemental Terms of Use for Microsoft Azure Previews.*

Note: *There may be known issues pertaining to this Solution, please refer to them before installing.*

Microsoft Sentinel Solutions provide a consolidated way to acquire Microsoft Sentinel content like data connectors, workbooks, analytics, and automations in your workspace with a single deployment step.

Workbooks: 1, **Analytic Rules:** 3, **Saved Searches:** 2, **Playbooks:** 1

Learn more about Microsoft Sentinel | Learn more about Solutions

Project details

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

Subscription * : Microsoft Partner Network

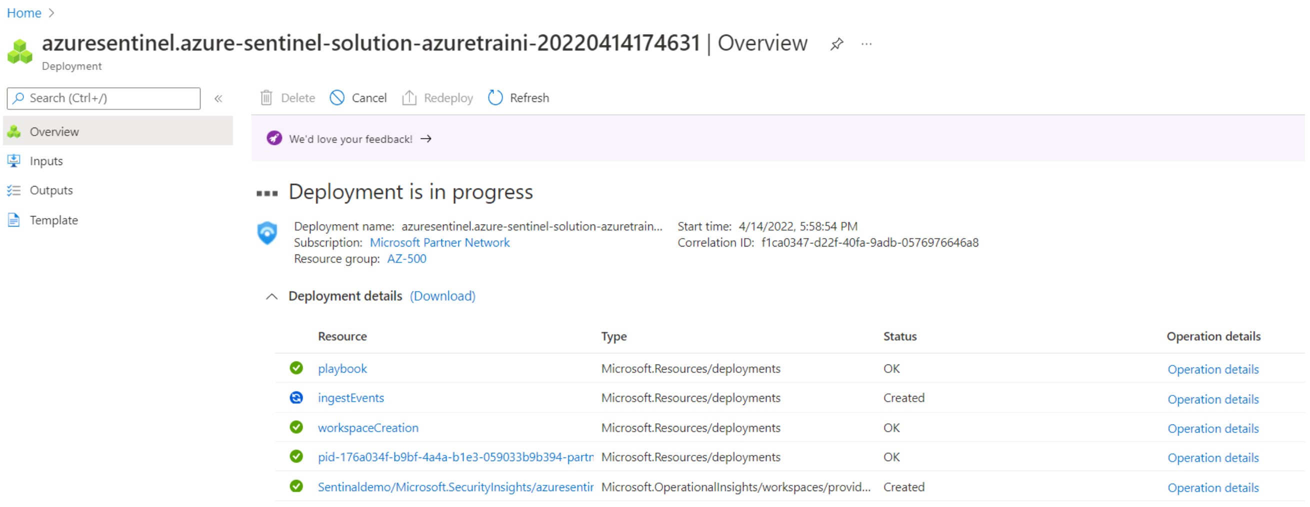
Resource group * : AZ-500

Create new

Instance details

Workspace * : Sentinaldemo

4. Once validation is ok, click on **Create**. The deployment process takes **about 15 minutes**, this is because we want to make sure that all the ingested data is ready for you to use once finished.



azuresentinel.azure-sentinel-solution-azuretraini-20220414174631 | Overview

Deployment

Deployment is in progress

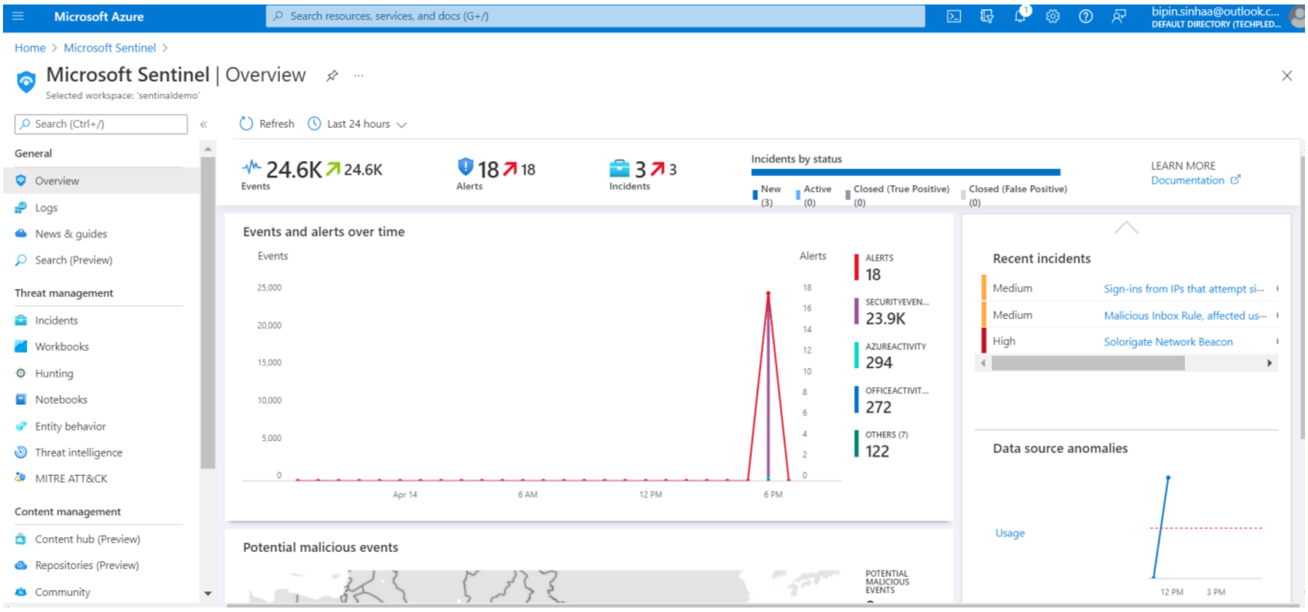
Deployment name: azuresentinel.azure-sentinel-solution-azuretrain...
Subscription: Microsoft Partner Network
Resource group: AZ-500
Start time: 4/14/2022, 5:58:54 PM
Correlation ID: f1ca0347-d22f-40fa-9adb-0576976646a8

Deployment details (Download)

Resource	Type	Status	Operation details
playbook	Microsoft.Resources/deployments	OK	Operation details
ingestEvents	Microsoft.Resources/deployments	Created	Operation details
workspaceCreation	Microsoft.Resources/deployments	OK	Operation details
pid-176a034f-b9bf-4a4a-b1e3-059033b9b394-partr	Microsoft.Resources/deployments	OK	Operation details
Sentinaldemo/Microsoft.SecurityInsights/azuresentir	Microsoft.OperationalInsights/workspaces/provid...	Created	Operation details

5. Once the deployment finishes, you can go back to Microsoft Sentinel and select your workspace. In the home page you should see some ingested data and several recent incidents.

   Don't worry if you don't see 3 incidents like in the screenshot below, they might take a few minutes to be raised.

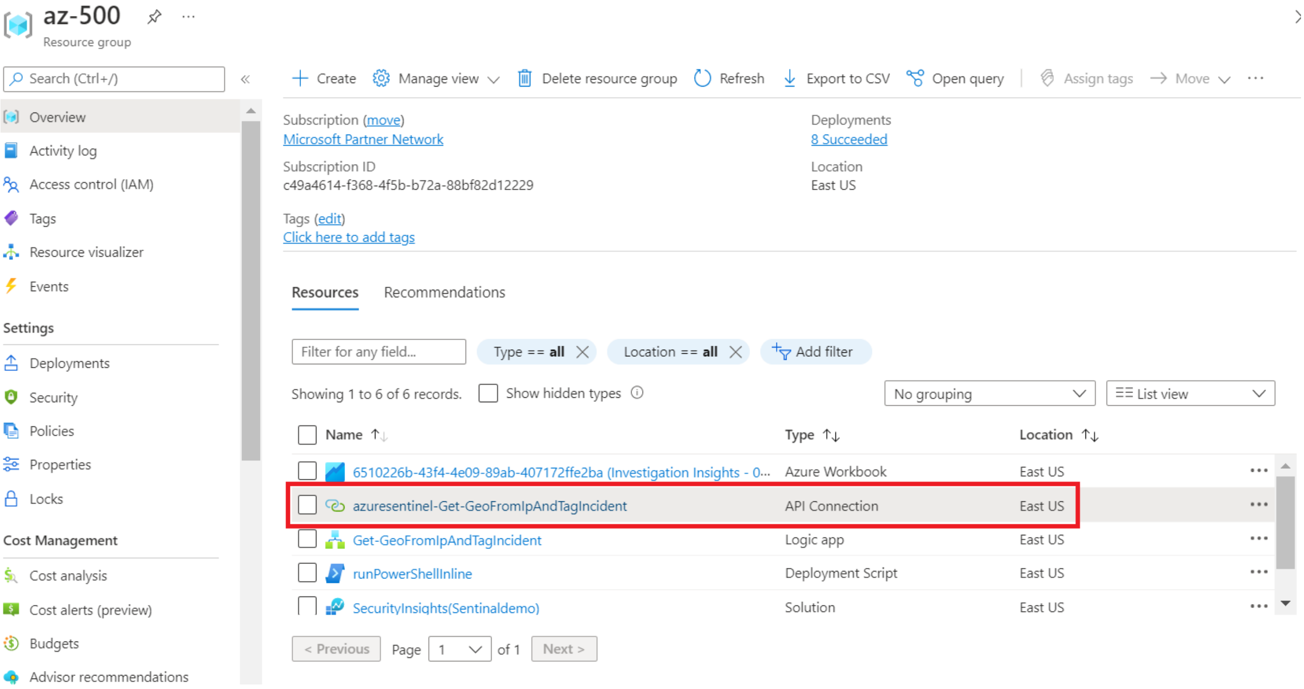


4. Exercise 3: Configure Microsoft Sentinel Playbook

In this exercise, we will configure a Playbook that will be later used in the lab. This will allow the playbook to access Sentinel.

1. Navigate to the resource group where the lab has been deployed.

2. In the resource group you should see an API Connection resource called **azuresentinel-Get-GeoFromIpAndTagIncident**, click on it.



Subscription (move)
Microsoft Partner Network

Subscription ID
c49a4614-f368-4f5b-b72a-88bf82d12229

Tags (edit)
Click here to add tags

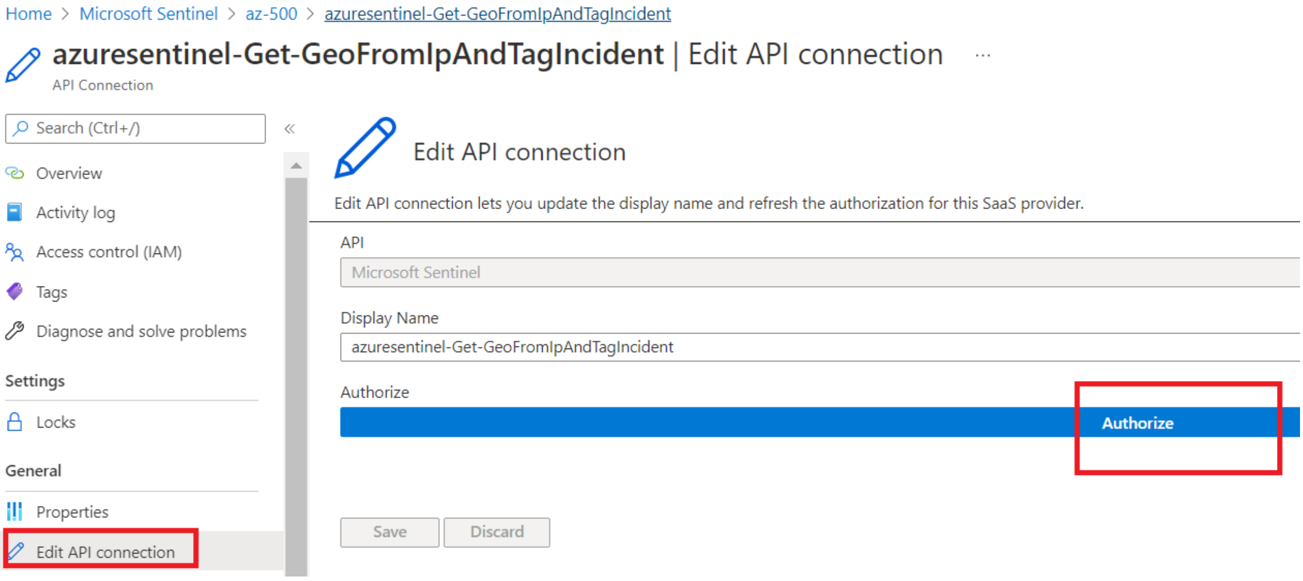
Deployments
8 Succeeded

Location
East US

Showing 1 to 6 of 6 records.

Name	Type	Location
6510226b-43f4-4e09-89ab-407172ffe2ba (Investigation Insights - 0...	Azure Workbook	East US
azuresentinel-Get-GeoFromIpAndTagIncident	API Connection	East US
Get-GeoFromIpAndTagIncident	Logic app	East US
runPowerShellInline	Deployment Script	East US
SecurityInsights(Sentinaldemo)	Solution	East US

3. Click on Edi **API connection** under **General**.


Home > Microsoft Sentinel > az-500 > azuresentinel-Get-GeoFromIpAndTagIncident
azuresentinel-Get-GeoFromIpAndTagIncident | Edit API connection ...
API Connection
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
General
Properties
Edit API connection

Edit API connection

Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.

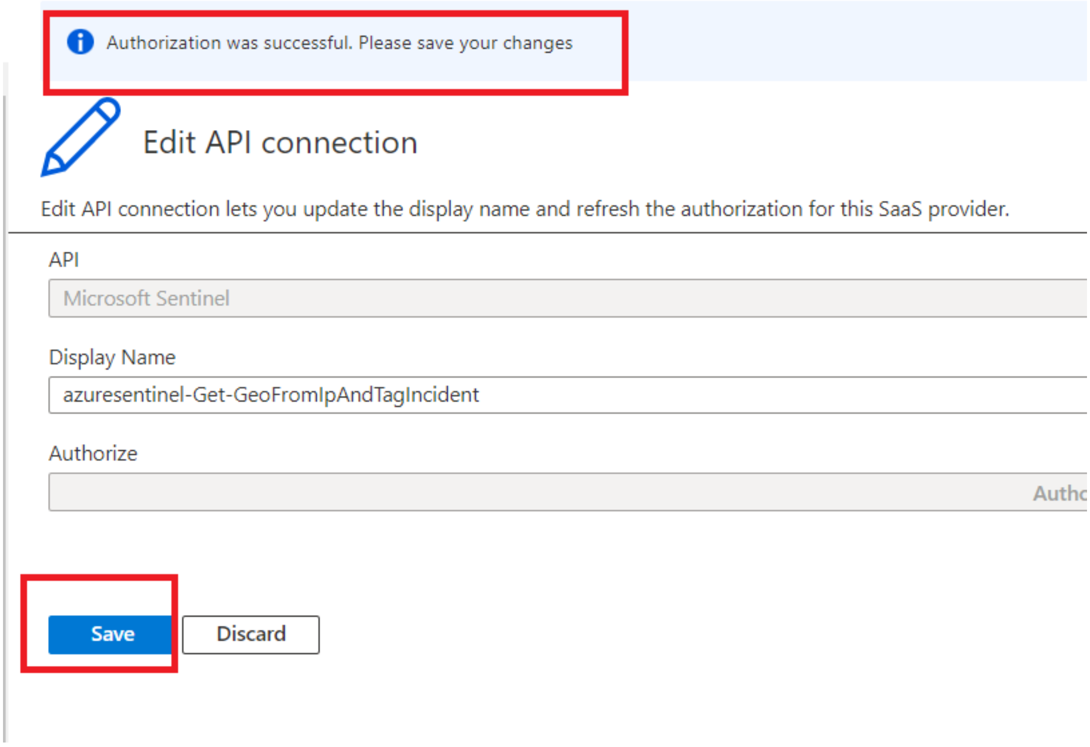
API: Microsoft Sentinel

Display Name: azuresentinel-Get-GeoFromIpAndTagIncident

Authorize

4. Click on **Authorize** and a new window will open to chose an account. Pick the user that you want to authenticate with. This should normally be the same user that you're logged in with.

5. Click **Save**.



Authorization was successful. Please save your changes

Edit API connection

Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.

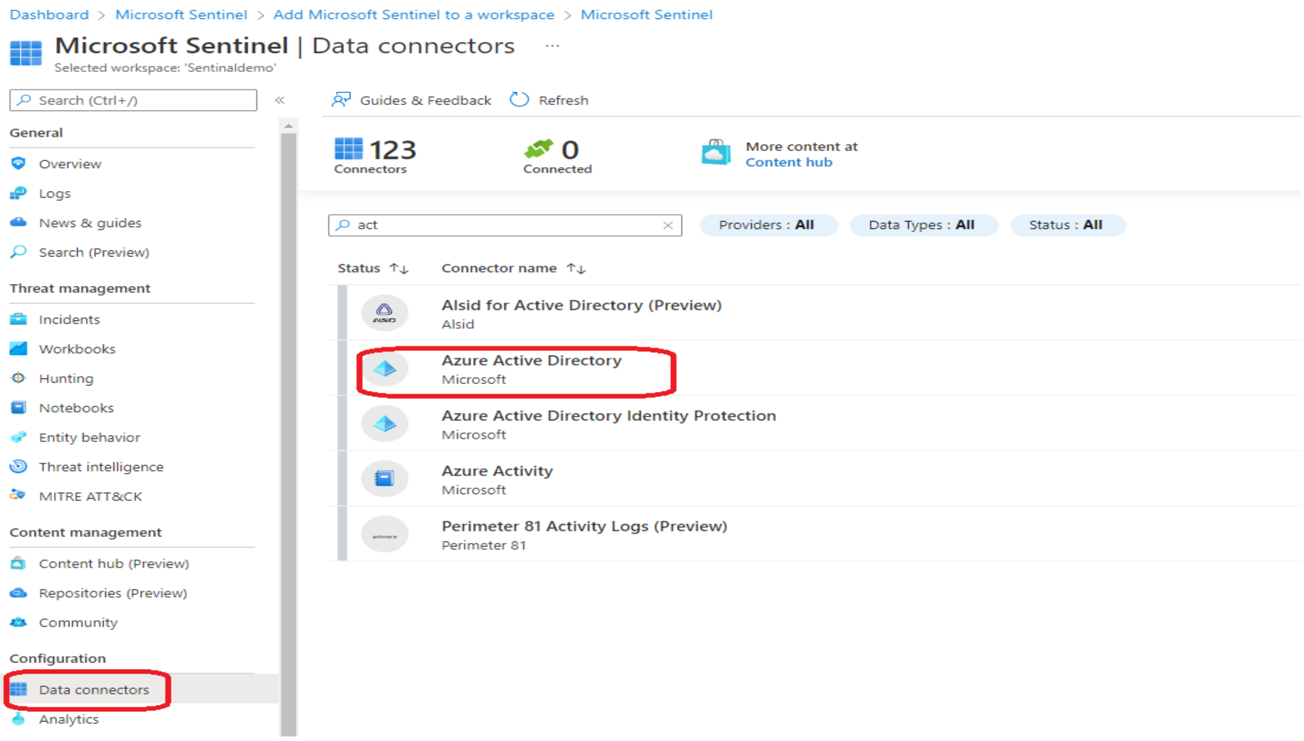
API: Microsoft Sentinel

Display Name: azuresentinel-Get-GeoFromIpAndTagIncident

Authorize

5. 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'

123 Connectors

0 Connected

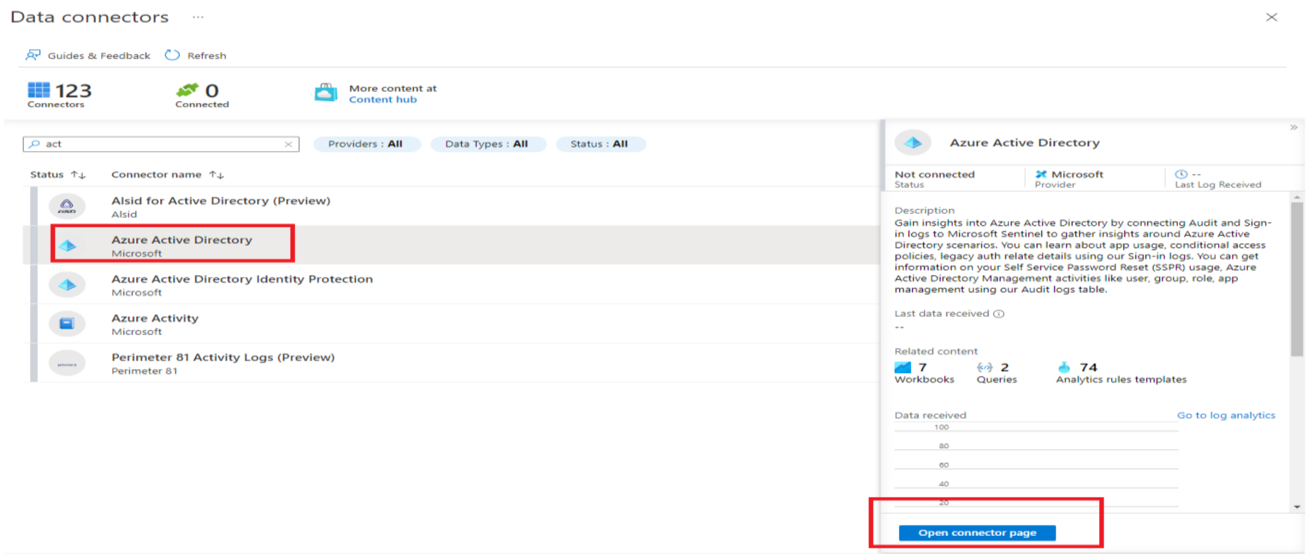
More content at Content hub

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**.



Data connectors

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

Azure Active Directory

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

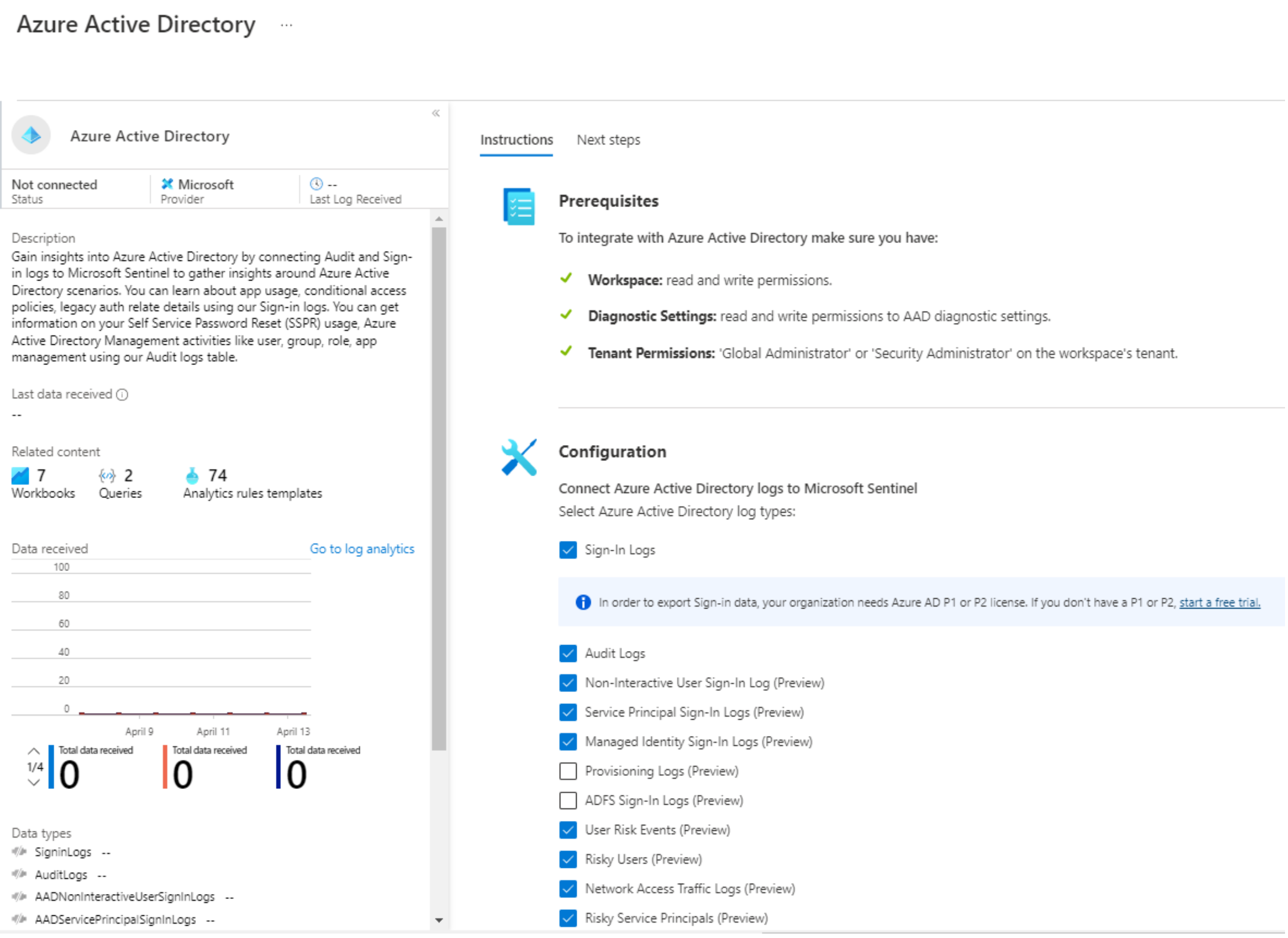
Last data received

--

Related content

7 Workbooks | 2 Queries | 74 Analytics rules templates

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 ...

Azure Active Directory

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received
--

Related content
7 Workbooks
2 Queries
74 Analytics rules templates

Data received
Go to log analytics

1/4
Total data received 0
Total data received 0
Total data received 0

Data types
SigninLogs --
AuditLogs --
AADNonInteractiveUserSignInLogs --
AADServicePrincipalSignInLogs --

Instructions | Next steps

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Diagnostic Settings:** read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel
Select Azure Active Directory log types:

☑ Sign-In Logs

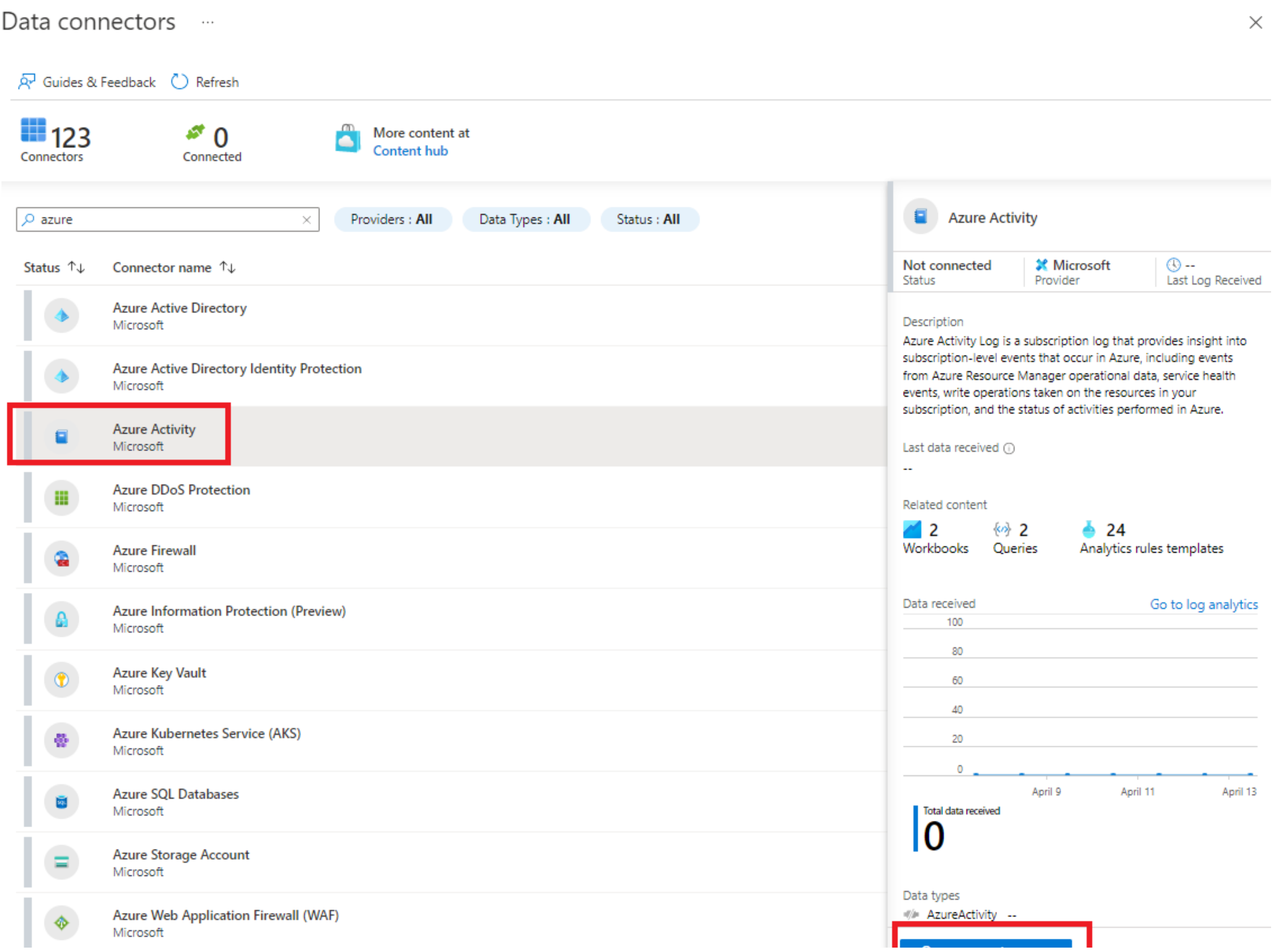
In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

☑ Audit Logs
☑ Non-Interactive User Sign-In Log (Preview)
☑ Service Principal Sign-In Logs (Preview)
☑ Managed Identity Sign-In Logs (Preview)
☐ Provisioning Logs (Preview)
☐ ADFS Sign-In Logs (Preview)
☑ User Risk Events (Preview)
☑ Risky Users (Preview)
☑ Network Access Traffic Logs (Preview)
☑ Risky Service Principals (Preview)

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

6. 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



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.

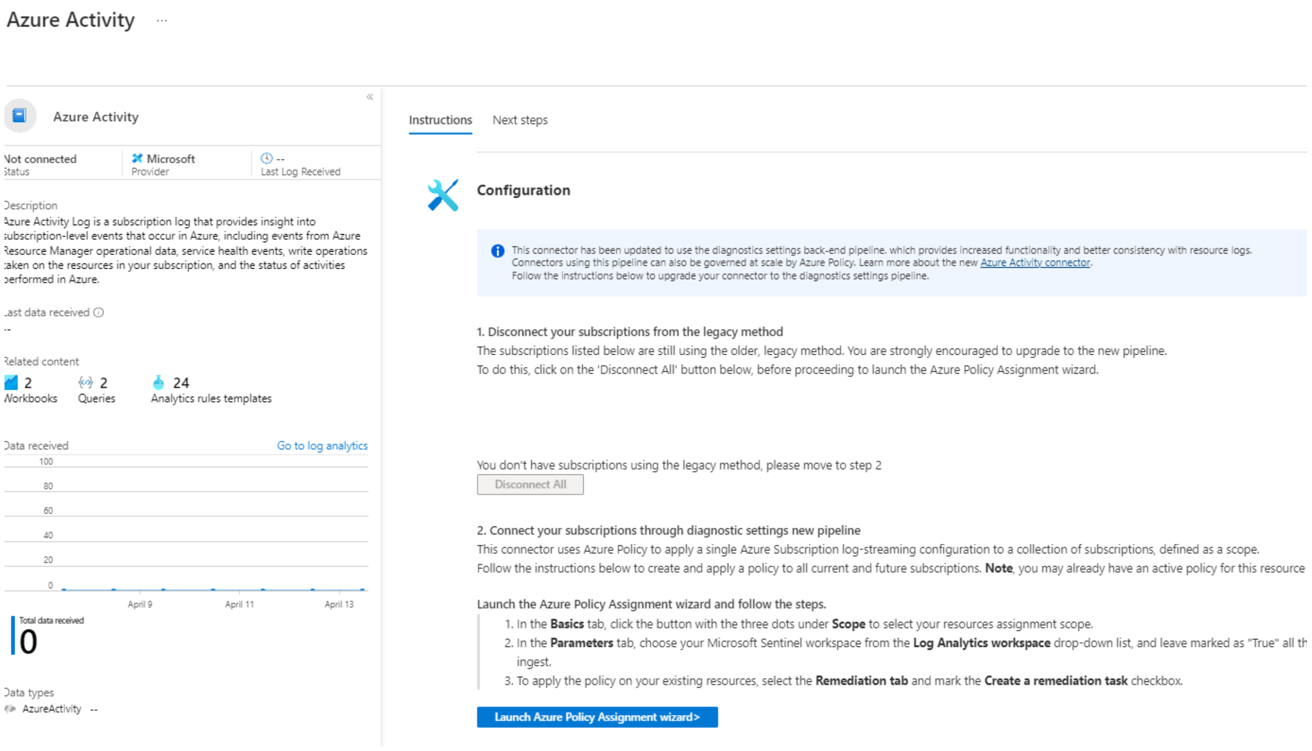
Last data received
--

Related content
2 Workbooks
2 Queries
24 Analytics rules templates

Data 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>**.



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

Total data received
0

Data types
AzureActivity --

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.

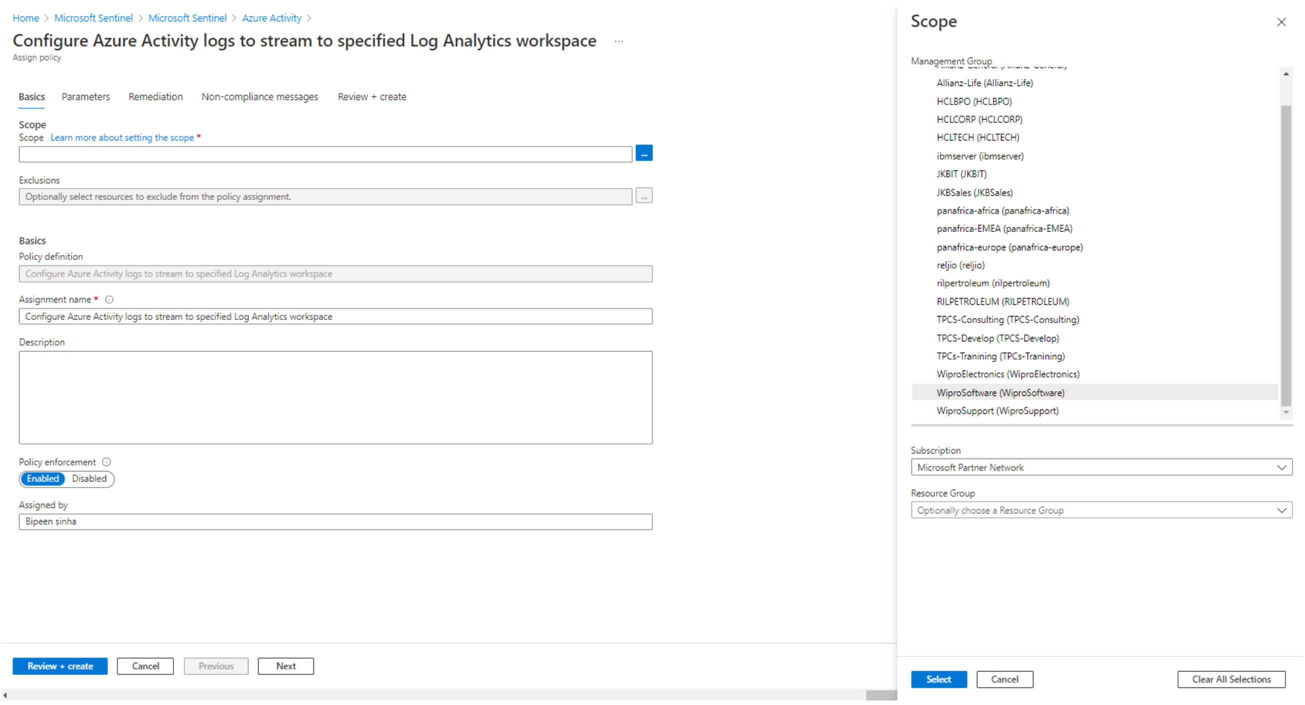
You don't have subscriptions using the legacy method, please move to step 2

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.

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

5. 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.



Configure Azure Activity logs to stream to specified Log Analytics workspace ···
Assign policy

Scope
Scope Learn more about setting the 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

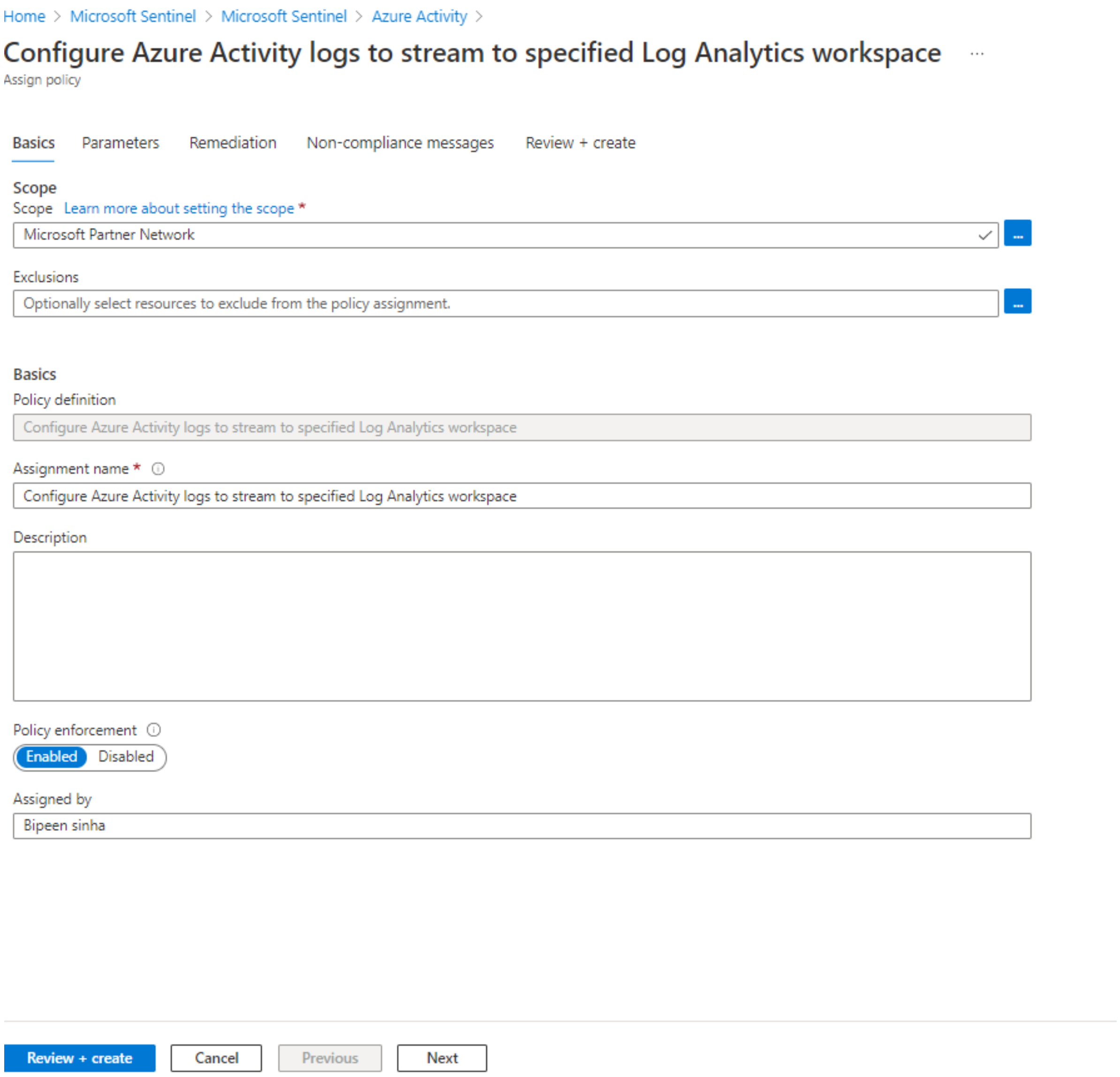
Assigned by
Bipeen sinha

Management Group
Allianz-Life (Allianz-Life)
HCLBPO (HCLBPO)
HCLCORP (HCLCORP)
HCLTECH (HCLTECH)
ibmserver (ibmserver)
JKBIT (JKBIT)
JKBSales (JKBSales)
panafrica-africa (panafrica-africa)
panafrica-EMEA (panafrica-EMEA)
panafrica-europe (panafrica-europe)
reljio (reljio)
rilpertroleum (rilpertroleum)
RILPETROLEUM (RILPETROLEUM)
TPCS-Consulting (TPCS-Consulting)
TPCS-Develop (TPCS-Develop)
TPCs-Tranining (TPCs-Tranining)
WiproElectronics (WiproElectronics)
WiproSoftware (WiproSoftware)
WiproSupport (WiproSupport)

Subscription
Microsoft Partner Network

Resource Group
Optionally choose a Resource Group

6. Click Next



Home > Microsoft Sentinel > Microsoft Sentinel > Azure Activity >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

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

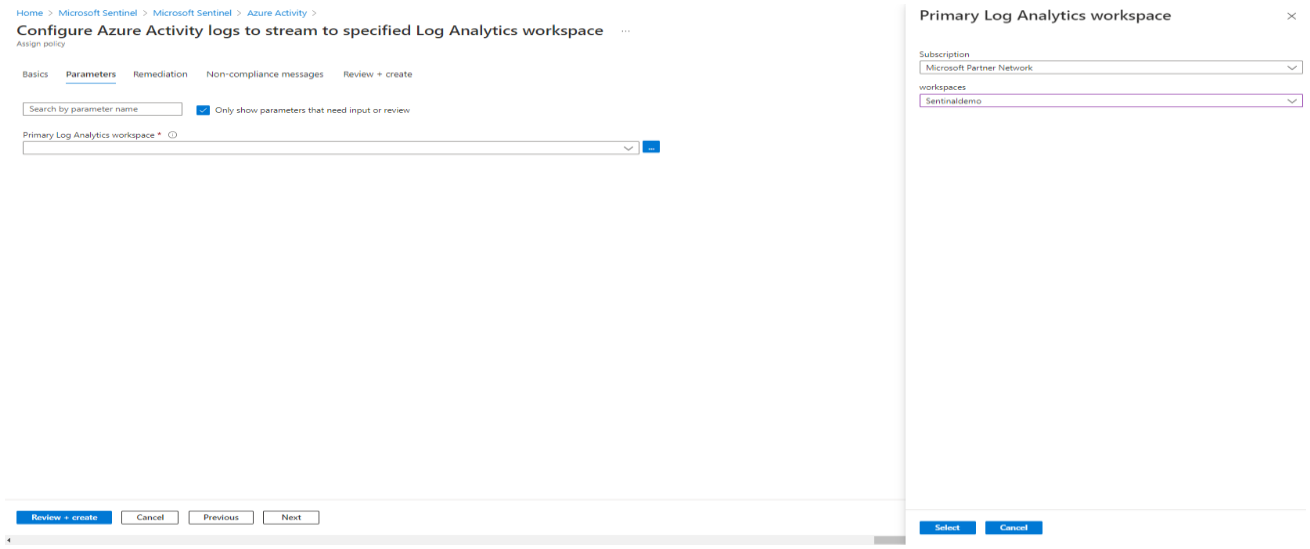
Assignment name *: Configure Azure Activity logs to stream to specified Log Analytics workspace

Description:

Policy enforcement: [✓ Enabled] Disabled

Assigned by: Bipeen sinha

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.



Home > Microsoft Sentinel > Microsoft Sentinel > Azure Activity >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

☑ Only show parameters that need input or review

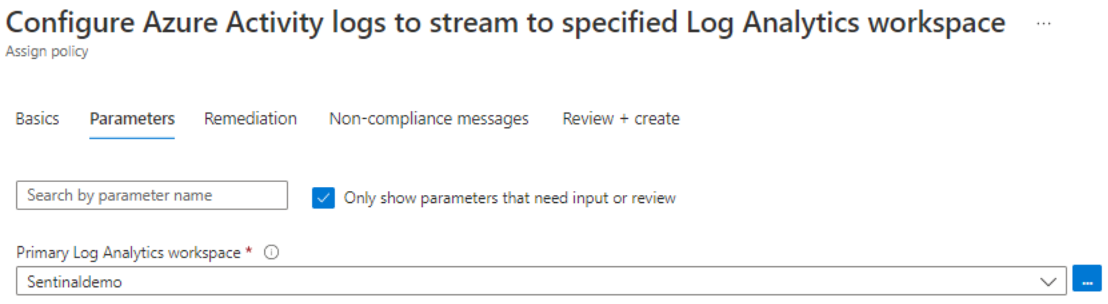
Primary Log Analytics workspace *:

Primary Log Analytics workspace

Subscription: Microsoft Partner Network

workspaces: Sentinaldemo

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

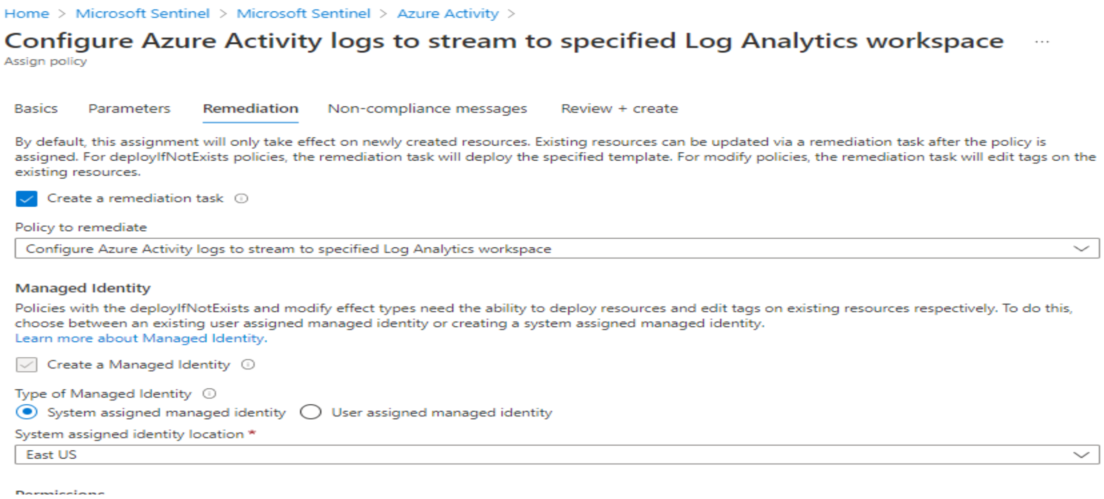
Assign policy

☑ 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

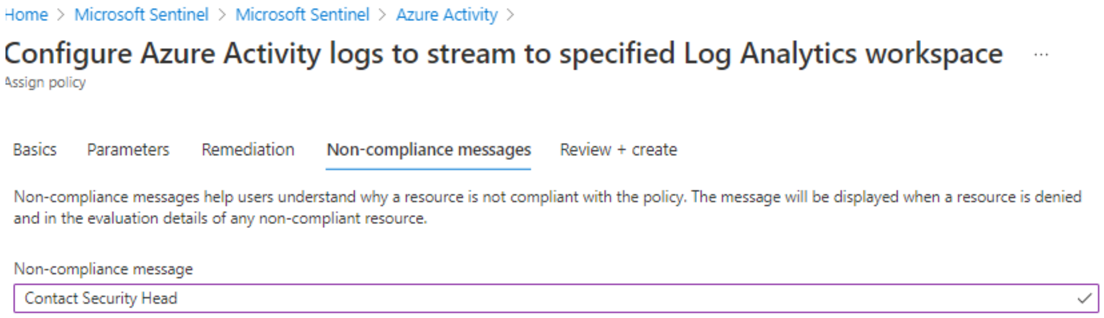
● System assigned managed identity ○ User assigned managed identity

System assigned identity location *

East US

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.

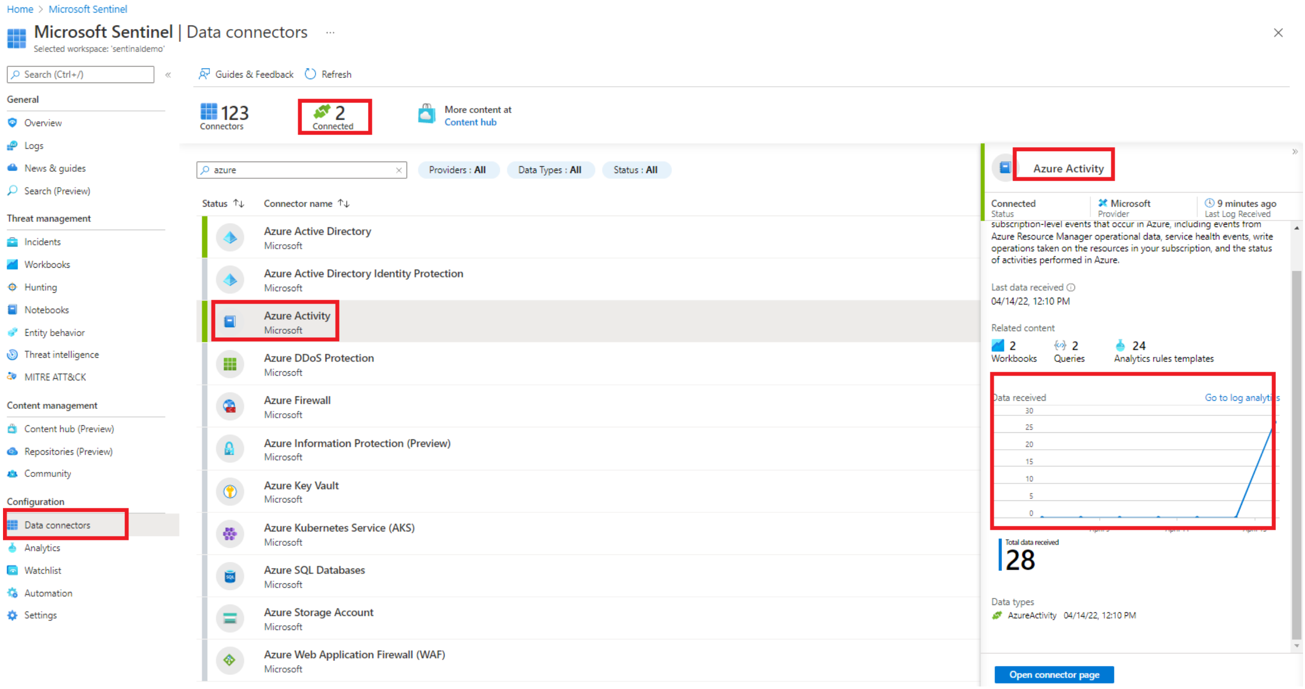
Non-compliance message

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.



Connector name	Provider
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

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

AzureActivity 04/14/22, 12:10 PM

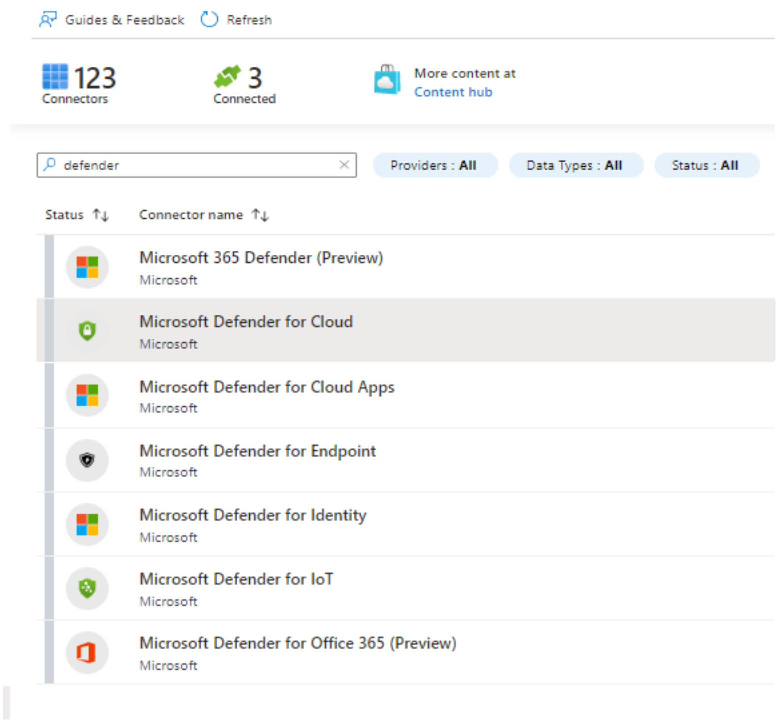
7. Enable Microsoft Defender for Cloud data connector

This exercise shows you how to enable the Microsoft Defender for Cloud data connector. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

NOTE: To do this exercise, your user must have the Security Reader role in the subscription of the logs you stream. If not done already, you will need to enable any of the Defender plans in Microsoft Defender for Cloud.

1. Go to you Microsoft Sentinel workspace and select **Data Connectors** under *Configuration* section.

2. In the data connectors screen, type *defender* in the search bar, select the ***Microsoft Defender for Cloud*** connector and click on *Open connector page*.



Guides & Feedback Refresh

123 Connectors

3 Connected

More content at Content hub

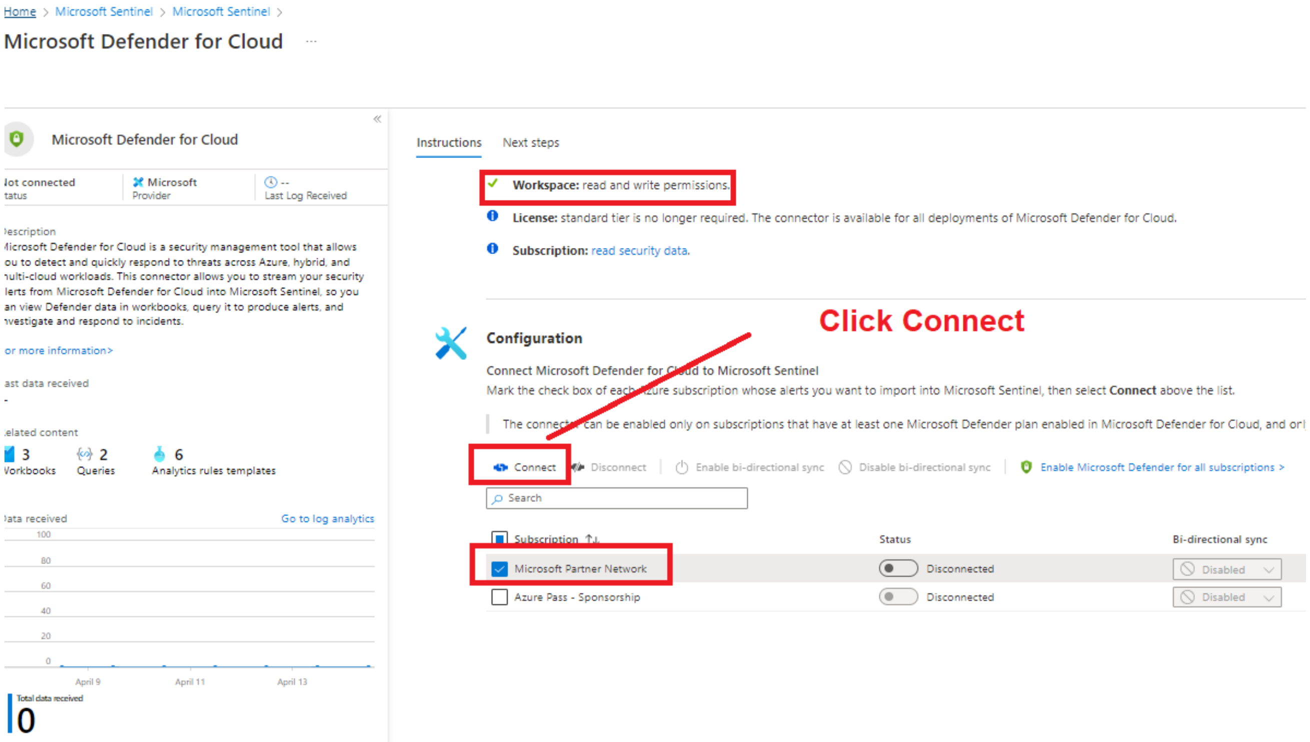
defender

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

Status ↑↓	Connector name ↑↓
	Microsoft 365 Defender (Preview) Microsoft
	Microsoft Defender for Cloud Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft
	Microsoft Defender for IoT Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft

3. In the Microsoft Defender for Cloud connector page, check that your permissions are enough at the top. If you don't have the required permissions, you can continue to the next exercise.

4. From the list of subscriptions at the bottom of the page, select the desired **subscription** and click on ***Connect*.** Wait for the operation to complete.



Home > Microsoft Sentinel > Microsoft Sentinel >

Microsoft Defender for Cloud ···

Microsoft Defender for Cloud

lot connected
tatus

Microsoft
Provider

--
Last Log Received

Description
Microsoft Defender for Cloud is a security management tool that allows ou to detect and quickly respond to threats across Azure, hybrid, and nulti-cloud workloads. This connector allows you to stream your security lerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you an view Defender data in workbooks, query it to produce alerts, and nvestigate and respond to incidents.

or more information>

ast data received
-

elated content
3 Vorkbooks 2 Queries 6 Analytics rules templates

ata received Go to log analytics

Total data received
0

Instructions Next steps

✓ **Workspace:** read and write permissions.

License: standard tier is no longer required. The connector is available for all deployments of Microsoft Defender for Cloud.

Subscription: read security data.

Click Connect

Configuration

Connect Microsoft Defender for Cloud to Microsoft Sentinel
Mark the check box of each Azure subscription whose alerts you want to import into Microsoft Sentinel, then select **Connect** above the list.

The connector can be enabled only on subscriptions that have at least one Microsoft Defender plan enabled in Microsoft Defender for Cloud, and on

Connect | Disconnect | Enable bi-directional sync | Disable bi-directional sync | Enable Microsoft Defender for all subscriptions >

Search

■ Subscription ↑↓	Status	Bi-directional sync
☑ Microsoft Partner Network	Disconnected	Disabled
□ Azure Pass - Sponsorship	Disconnected	Disabled

5. Click on *Next Steps* at the top of the page and explore what content is available for this connector.

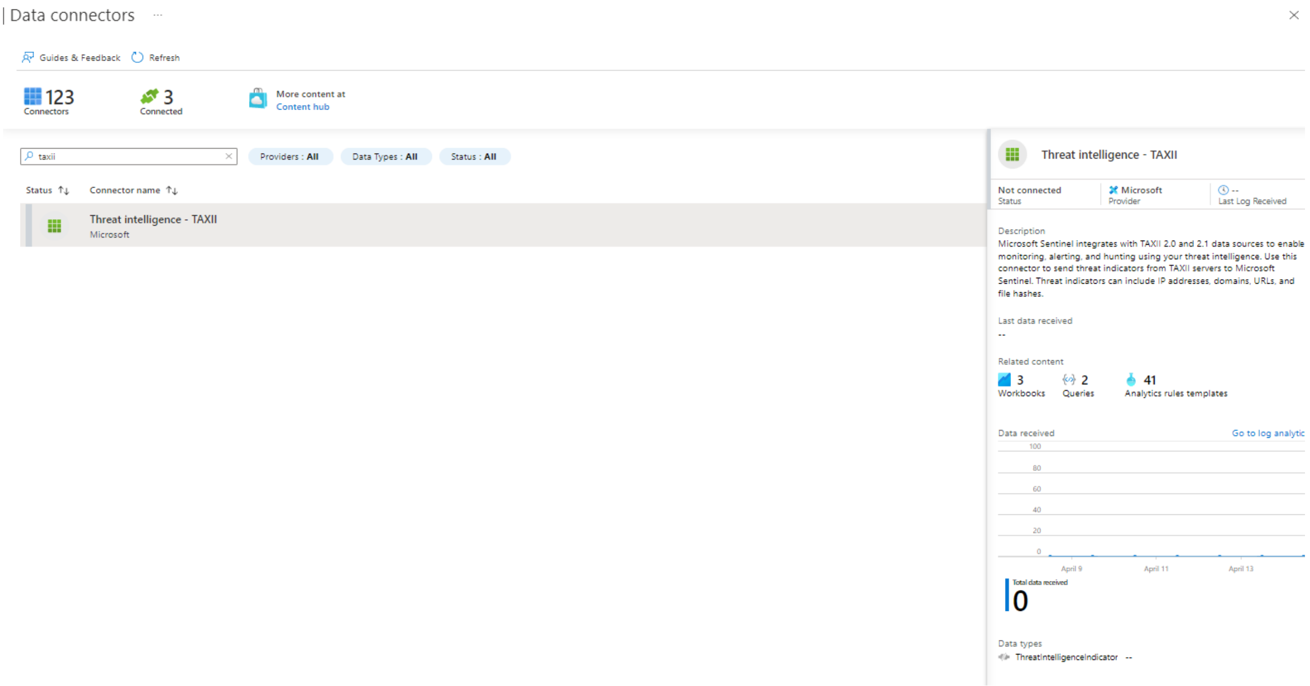
8. Enable Threat Intelligence TAXII data connector

This exercise shows you how to enable the Threat Intelligence - TAXII data connector. This connector allows you to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

NOTE: To do this exercise, your user must have the Security Reader role in the subscription of the logs you stream. If not done already, you will need to enable Azure Defender within Azure Security Center.

1. Go to you Microsoft Sentinel workspace and select *Data Connectors* under *Configuration* section.

2. In the data connectors screen, type *taxii* in the search bar, select the ***Threat intelligence - TAXII*** connector and click on ***Open connector page***.



| Data connectors ···

Guides & Feedback   Refresh

123 Connectors   3 Connected   More content at Content hub

taxii   Providers : All   Data Types : All   Status : All

Status ↑↓	Connector name ↑↓
	Threat intelligence - TAXII Microsoft

Threat intelligence - TAXII

Not connected	Microsoft	--
Status	Provider	Last Log Received

Description

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Last data received

--

Related content

3 Workbooks   2 Queries   41 Analytics rules templates

Data received   Go to log analytic

Total data received

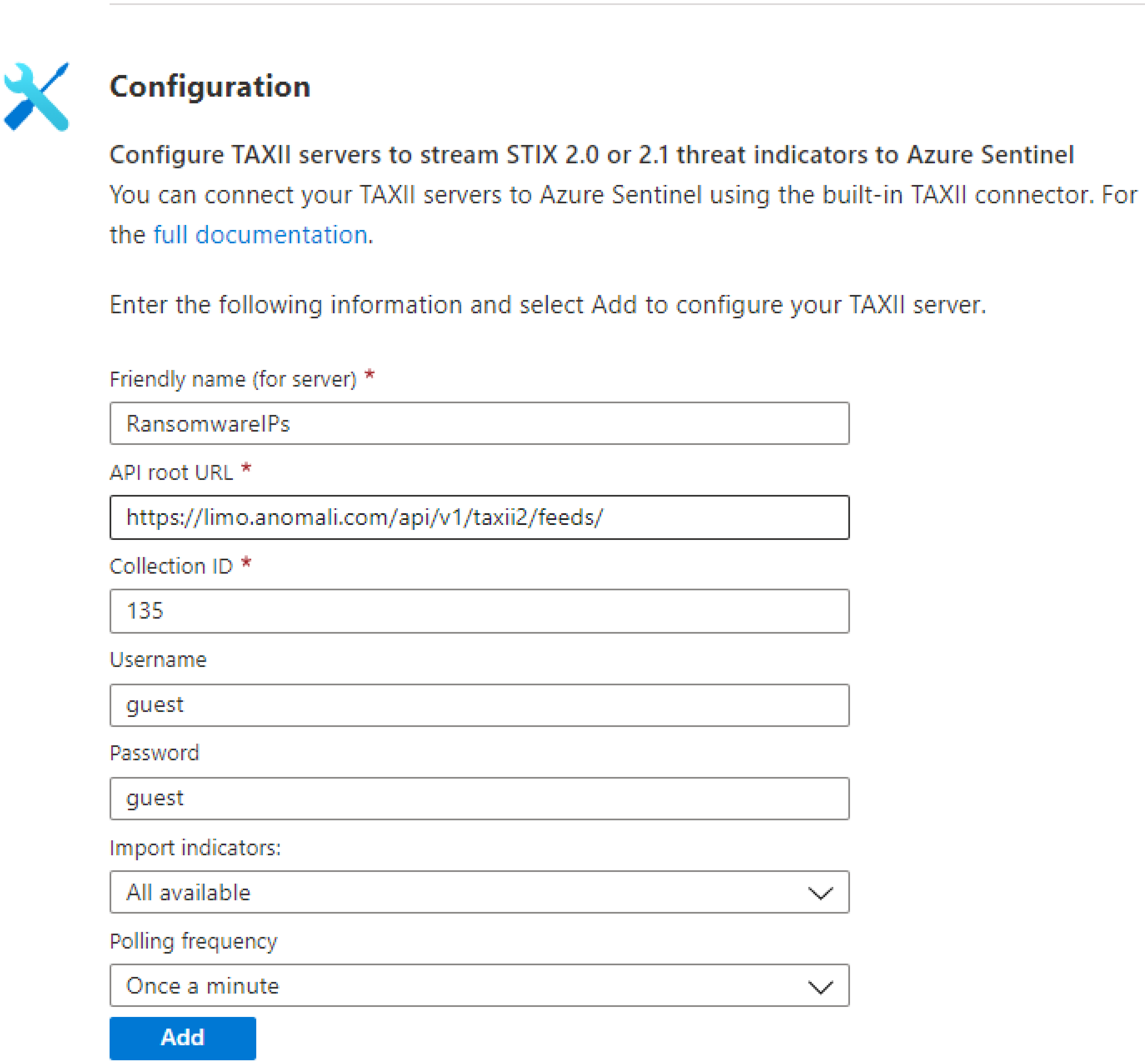
0

Data types

ThreatIntelligenceIndicator --

3. In the Threat Intelligence - TAXII connector page, add the following information under *Configuration* menu:

   - **Friendly name (for server)**: RansomwareIPs
   - **API root URL**: https://limo.anomali.com/api/v1/taxii2/feeds/
   - **Collection ID**: 135
   - **Username**: guest
   - **Password**: guest
   - **Import Indicators**: All available (review all available options)
   - **Polling frequency**: Once an minute (review all available options)



Configuration

Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Azure Sentinel

You can connect your TAXII servers to Azure Sentinel using the built-in TAXII connector. For the full documentation.

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) *: RansomwareIPs

API root URL *: https://limo.anomali.com/api/v1/taxii2/feeds/

Collection ID *: 135

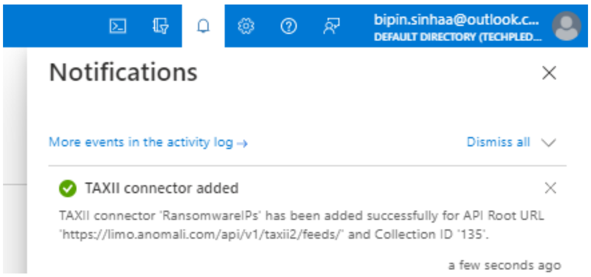
Username: guest

Password: guest

Import indicators: All available

Polling frequency: Once a minute

4. Click ***Add*** and wait until the operation completes.



bipin.sinhaa@outlook.c...
DEFAULT DIRECTORY (TECHPLED...
Notifications
More events in the activity log →
Dismiss all

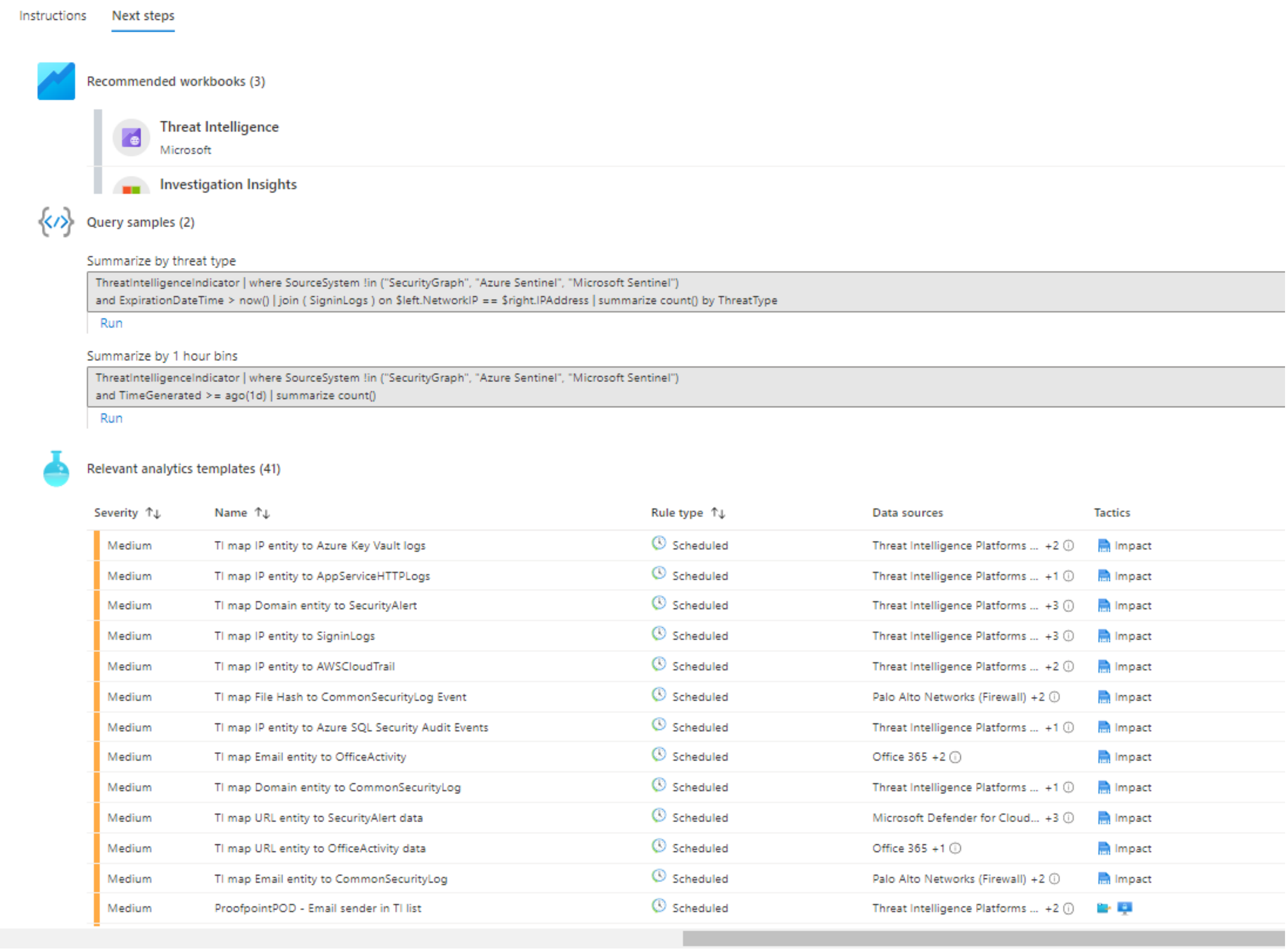
TAXII connector added

TAXII connector 'RansomwareIPs' has been added successfully for API Root URL 'https://limo.anomali.com/api/v1/taxii2/feeds/' and Collection ID '135'.

a few seconds ago

5. Click on *Next Steps* at the top of the page and explore what content is available for this connector. In a few seconds, the ThreatIntelligenceIndicator will be populated with IOCs from Anomali's feed

6.



Recommended workbooks (3)

Threat Intelligence
Microsoft

Investigation Insights

Query samples (2)

Summarize by threat type

```
ThreatIntelligenceIndicator | where SourceSystem !in ("SecurityGraph", "Azure Sentinel", "Microsoft Sentinel")
and ExpirationDateTime > now() | join ( SigninLogs ) on $left.NetworkIP == $right.IPAddress | summarize count() by ThreatType
```

Summarize by 1 hour bins

```
ThreatIntelligenceIndicator | where SourceSystem !in ("SecurityGraph", "Azure Sentinel", "Microsoft Sentinel")
and TimeGenerated >= ago(1d) | summarize count()
```

Relevant analytics templates (41)

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics
Medium	TI map IP entity to Azure Key Vault logs	Scheduled	Threat Intelligence Platforms ... +2 ⓘ	Impact
Medium	TI map IP entity to AppServiceHTTPLogs	Scheduled	Threat Intelligence Platforms ... +1 ⓘ	Impact
Medium	TI map Domain entity to SecurityAlert	Scheduled	Threat Intelligence Platforms ... +3 ⓘ	Impact
Medium	TI map IP entity to SigninLogs	Scheduled	Threat Intelligence Platforms ... +3 ⓘ	Impact
Medium	TI map IP entity to AWSCloudTrail	Scheduled	Threat Intelligence Platforms ... +2 ⓘ	Impact
Medium	TI map File Hash to CommonSecurityLog Event	Scheduled	Palo Alto Networks (Firewall) +2 ⓘ	Impact
Medium	TI map IP entity to Azure SQL Security Audit Events	Scheduled	Threat Intelligence Platforms ... +1 ⓘ	Impact
Medium	TI map Email entity to OfficeActivity	Scheduled	Office 365 +2 ⓘ	Impact
Medium	TI map Domain entity to CommonSecurityLog	Scheduled	Threat Intelligence Platforms ... +1 ⓘ	Impact
Medium	TI map URL entity to SecurityAlert data	Scheduled	Microsoft Defender for Cloud... +3 ⓘ	Impact
Medium	TI map URL entity to OfficeActivity data	Scheduled	Office 365 +1 ⓘ	Impact
Medium	TI map Email entity to CommonSecurityLog	Scheduled	Palo Alto Networks (Firewall) +2 ⓘ	Impact
Medium	ProofpointPOD - Email sender in TI list	Scheduled	Threat Intelligence Platforms ... +2 ⓘ	