

Build the Log Analytics Workspace

- Go to Azure Portal → Create Resource → Log Analytics Workspace
- Resource Group: RG-Sentinel
- Workspace Name: SentinelLogWorkspace
- Region: East US
- Click **Review + Create** → **Create**



Microsoft Azure

Home > Create a resource > Marketplace >

Log Analytics Workspace

Microsoft

Log Analytics Workspace [Add to Favorites](#)

Microsoft | Azure Service

★ 3.0 (55 ratings)

[Azure benefit eligible](#)

Subscription: Azure subscription 1 Plan: Log Analytics Workspace [Create](#)

Overview Plans Usage Information + Support Ratings + Reviews

About Azure Monitor Log Analytics

With Azure Monitor Log Analytics 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. A Log Analytics workspace is the basic management unit of Log Analytics.

Create a new workspace

A Log Analytics Workspace is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary. Creating an Azure Monitor Log Analytics workspace has some specific considerations you need to account for before choosing to create a new workspace. Please refer to the following documentation to learn more about the consideration you need to take before creating a new Log Analytics workspace.

Click on the 'Create' button to create an Azure Log Analytics workspace.

Microsoft Azure

Home > Create a resource > Marketplace > Log Analytics Workspace >

Create Log Analytics workspace

Validation passed

Basics Tags **Review + Create**

Log Analytics workspace by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	RG-Sentinel
Name	SentinelLogWorkspace
Region	East US

Pricing

Pricing tier: Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more](#) about Log Analytics pricing models.

Tags: None

Pricing Note: Sentinel charges only when data is ingested. First 10 GB/day are free for 30 days.

Microsoft Azure

Home >

Microsoft.LogAnalyticsOMS | Overview

Deployment

Search x << [Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

Overview

- Inputs
- Outputs
- Template

Your deployment is complete

Deployment name : Microsoft.LogAnalyticsOMS

Subscription : Azure subscription 1

Resource group : RG-Sentinel

[Deployment details](#)

[Next steps](#)

[Go to resource](#)

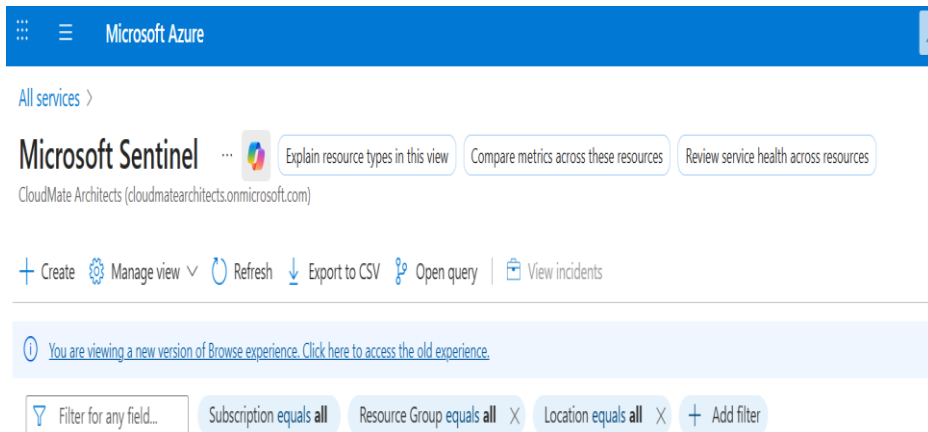
Give feedback

[Tell us about your experience with deployment](#)

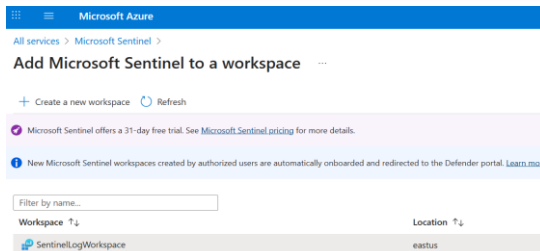


Step 2 — Enable Microsoft Sentinel

- Azure Portal → Search Microsoft Sentinel
- Click Create
- Choose SentinelLogWorkspace
- Click Add

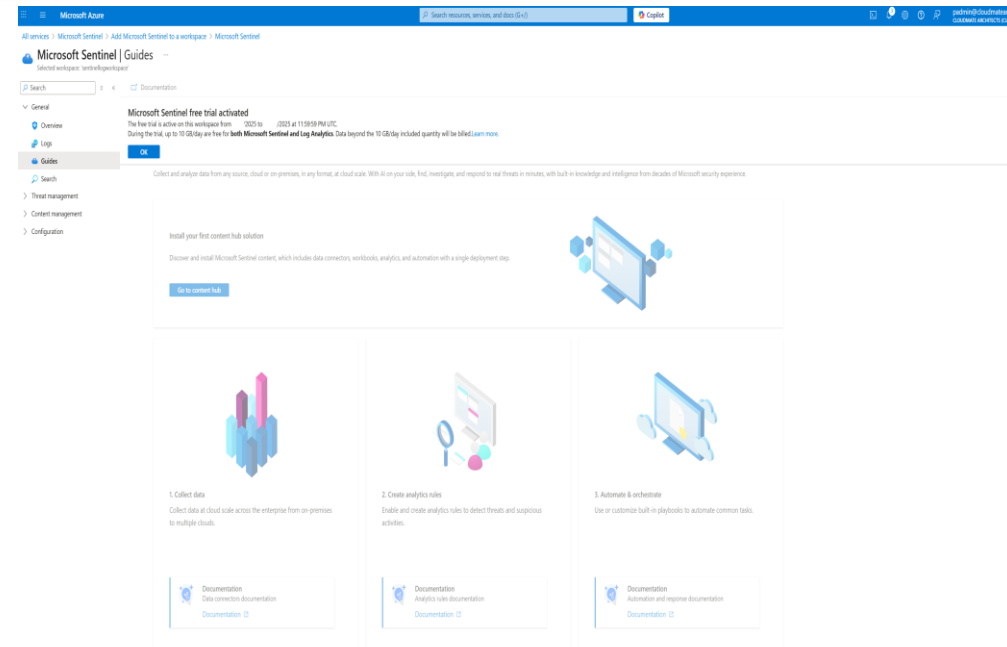


The screenshot shows the Microsoft Sentinel overview page. The top navigation bar includes 'All services >'. Below the header, there are three buttons: 'Explain resource types in this view', 'Compare metrics across these resources', and 'Review service health across resources'. A section titled 'Microsoft Sentinel' with a sub-header 'CloudMate Architects (cloudmatearchitects.onmicrosoft.com)' is visible. Below this, there are several action buttons: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'View incidents'. At the bottom, there is a filter bar with a search input 'Filter for any field...' and several filter tags: 'Subscription equals all', 'Resource Group equals all', 'Location equals all', and an 'Add filter' button.



The screenshot shows the 'Add Microsoft Sentinel to a workspace' page. It features a 'Create a new workspace' button and a 'Refresh' button. Below this, there is a message: 'Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.' A note states: 'New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. [Learn more](#)'. A table below shows the workspace details:

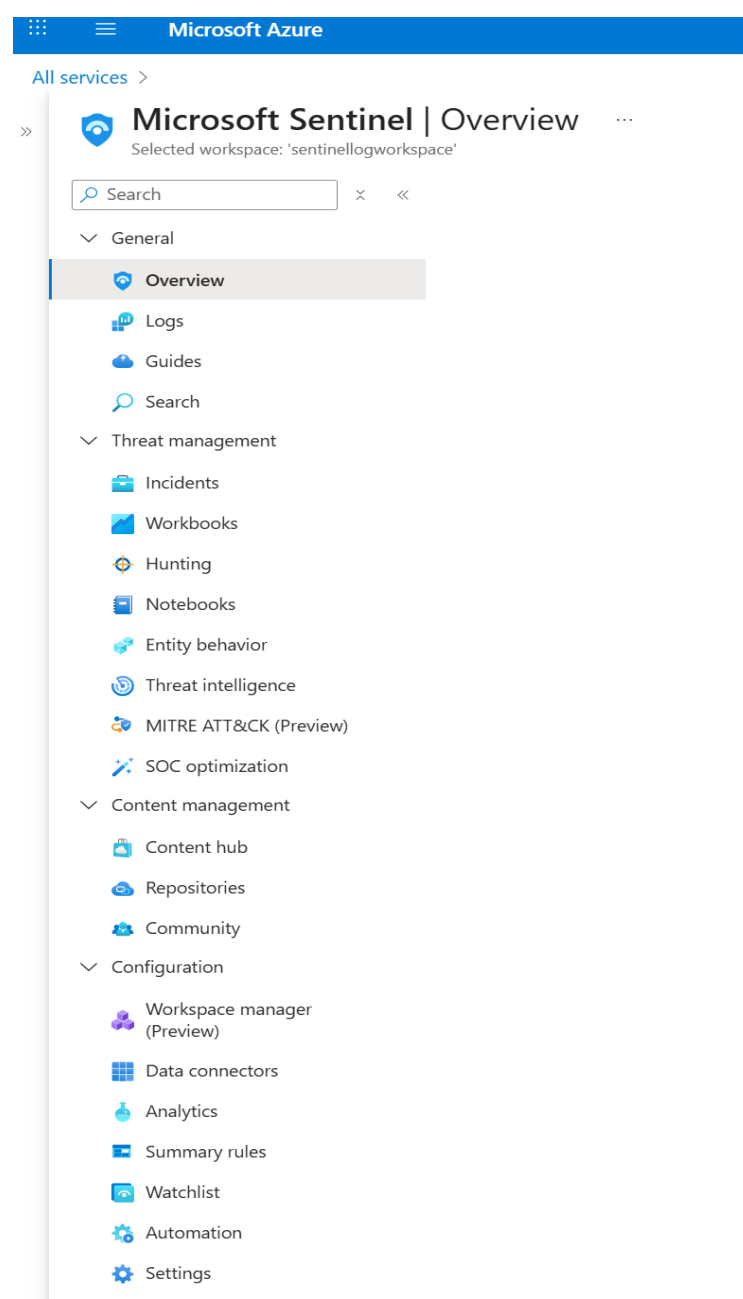
Workspace	Location
SentinelLogWorkspace	eastus



The screenshot shows the 'Microsoft Sentinel | Guides' page. It includes a search bar and a 'Documentation' tab. The main content area is titled 'Microsoft Sentinel free trial activated' and provides information about the trial period. Below this, there is a section 'Install your first content hub solution' with a 'Go to content hub' button. The page also features three cards with icons and text: '1. Collect data', '2. Create analysis rules', and '3. Automate & orchestrate'. Each card has a 'Documentation' link at the bottom.

Step 3 — Verify Sentinel Is Live

- Open your new Sentinel workspace
- Confirm dashboard shows:
- Data Connectors
- Analytics
- Workbooks
- Hunting



Sentinel Workspace Deployed

- Log Analytics workspace created
- Microsoft Sentinel enabled
- Sentinel dashboard verified
- Environment ready for future labs

