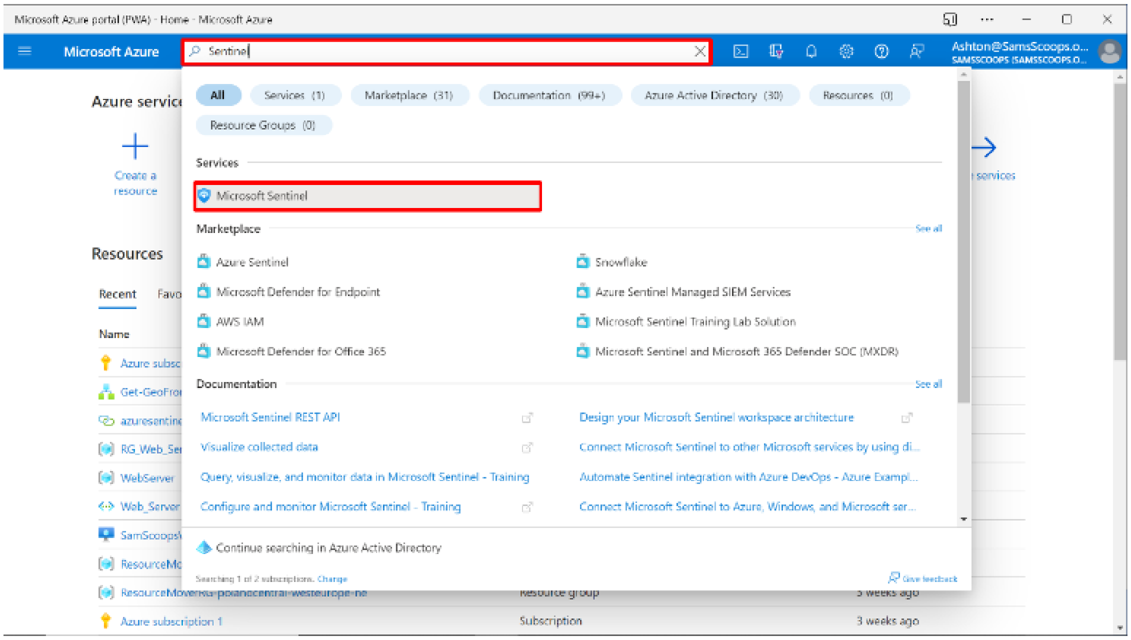
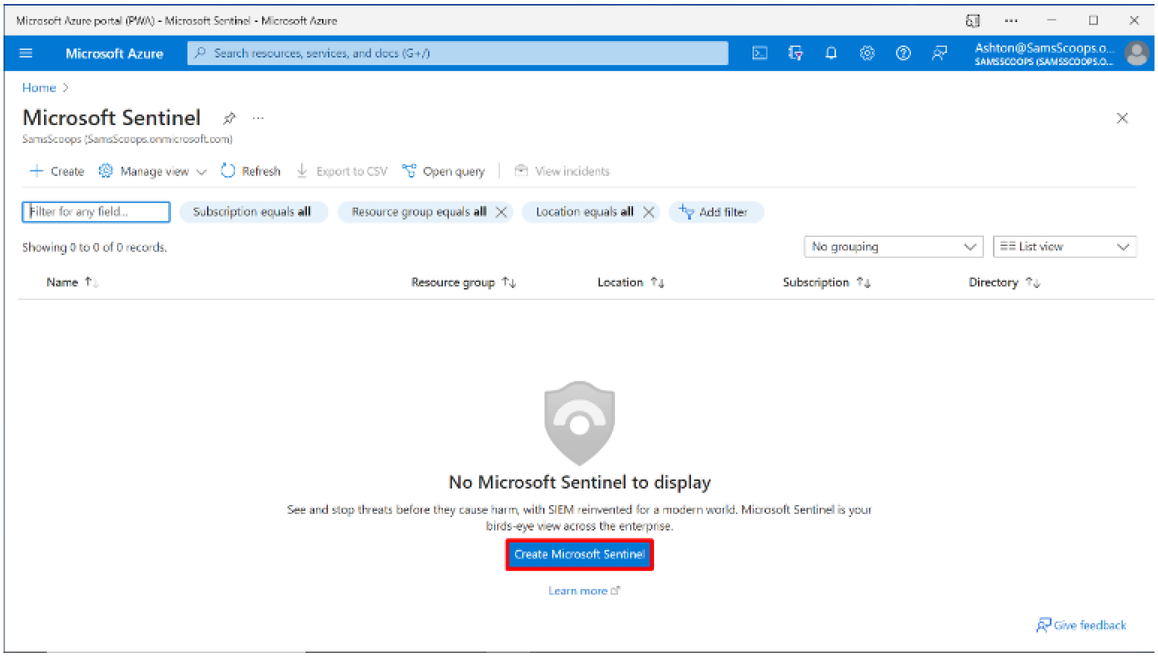
Step 1: Deploy Microsoft Sentinel and a log analytics workspace

1. From the **Azure portal home page**, search for and select **Microsoft Sentinel**.



Microsoft Azure portal (PWA) - Home - Microsoft Azure
Microsoft Azure
Sentinel
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Azure servic
Create a resource
services
All
Services (1)
Marketplace (31)
Documentation (99+)
Azure Active Directory (30)
Resources (0)
Resource Groups (0)
Services
Microsoft Sentinel
Marketplace
See all
Azure Sentinel
Snowflake
Microsoft Defender for Endpoint
Azure Sentinel Managed SIEM Services
AWS IAM
Microsoft Sentinel Training Lab Solution
Microsoft Defender for Office 365
Microsoft Sentinel and Microsoft 365 Defender SOC (MXDR)
Documentation
See all
Microsoft Sentinel REST API
Design your Microsoft Sentinel workspace architecture
Visualize collected data
Connect Microsoft Sentinel to other Microsoft services by using di...
Query, visualize, and monitor data in Microsoft Sentinel - Training
Automate Sentinel integration with Azure DevOps - Azure Exampl...
Configure and monitor Microsoft Sentinel - Training
Connect Microsoft Sentinel to Azure, Windows, and Microsoft ser...
Continue searching in Azure Active Directory
Searching 1 of 2 subscriptions. Change
Give feedback
Resources
Recent
Favo
Name
Azure subsc
Get-GeoFro
azuresentin
RG_Web_Ser
WebServer
Web_Server
SamScoops\
ResourceMc
ResourceMoverRG-polandcentral-westeurope-ne
Resource group
3 weeks ago
Azure subscription 1
Subscription
3 weeks ago

2. Select **Create Microsoft Sentinel**.

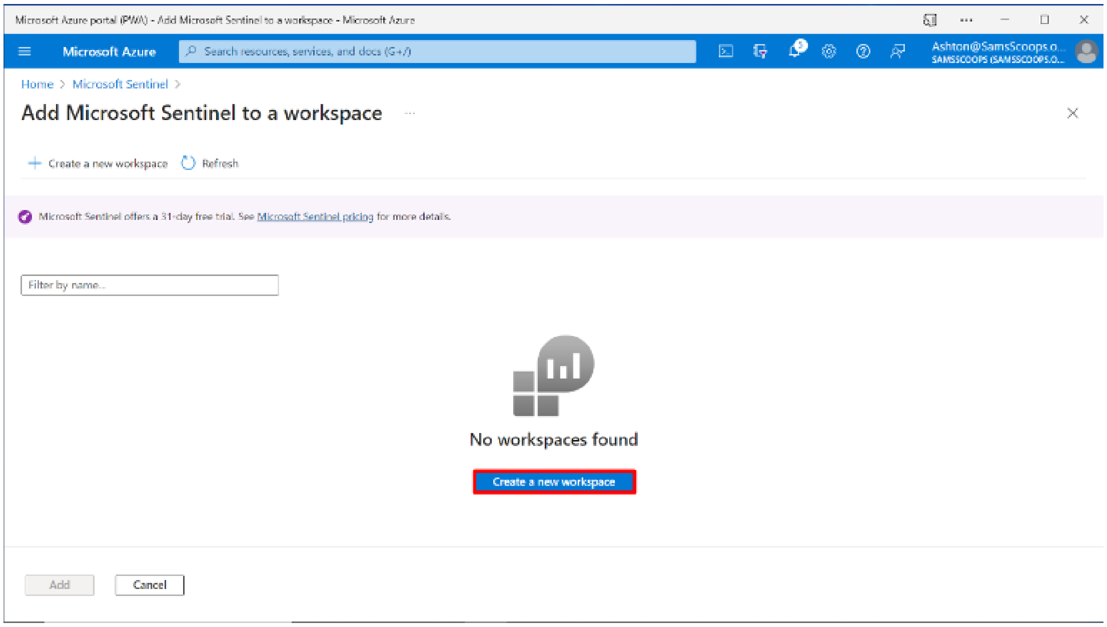


Showing 0 to 0 of 0 records.

No Microsoft Sentinel to display

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.

3. Select **Create a new workspace**.



Microsoft Azure portal (PWA) - Add Microsoft Sentinel to a workspace - Microsoft Azure

Add Microsoft Sentinel to a workspace

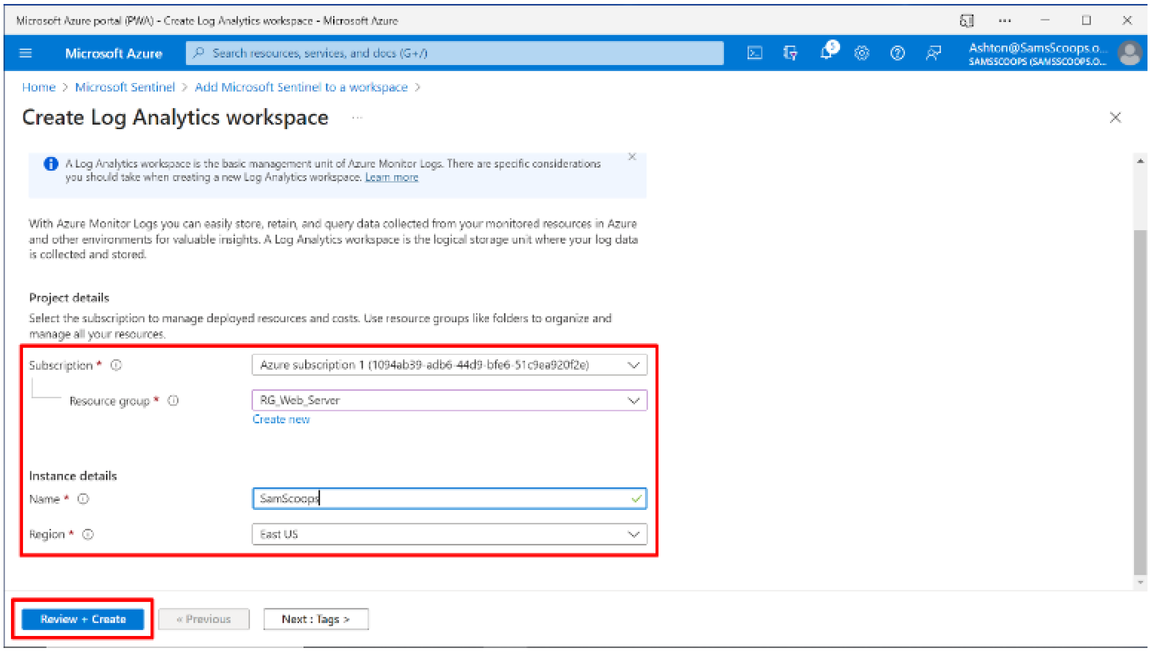
Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

No workspaces found

4. Your current subscription will be already selected. Fill in the following deployment details for a log analytics workspace:

- Resource group: **RG_Web_Server**.
- Instance name: **SamScoops**.
- Region: The region will be prepopulated with the Resource group's current region.

5. Select **Review + Create**.



Microsoft Azure portal (PWA) - Create Log Analytics workspace - Microsoft Azure

Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace

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 * : Azure subscription 1 (1094ab39-adb6-44d9-bfe6-51c9ea920f2e)

Resource group * : RG_Web_Server

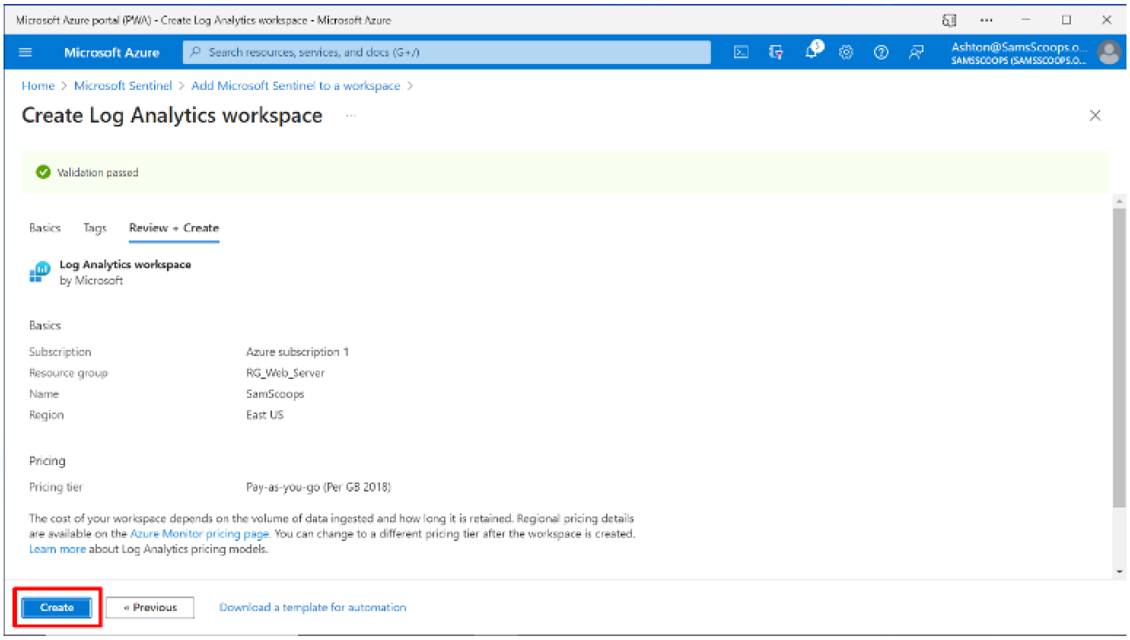
Create new

Instance details

Name * : SamScoops

Region * : East US

6. Select **Create**.



Microsoft Azure portal (PWA) - Create Log Analytics workspace - Microsoft Azure

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace

Validation passed

Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Basics
Tags
Review + Create

Log Analytics workspace
by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	RG_Web_Server
Name	SamScoops
Region	East US

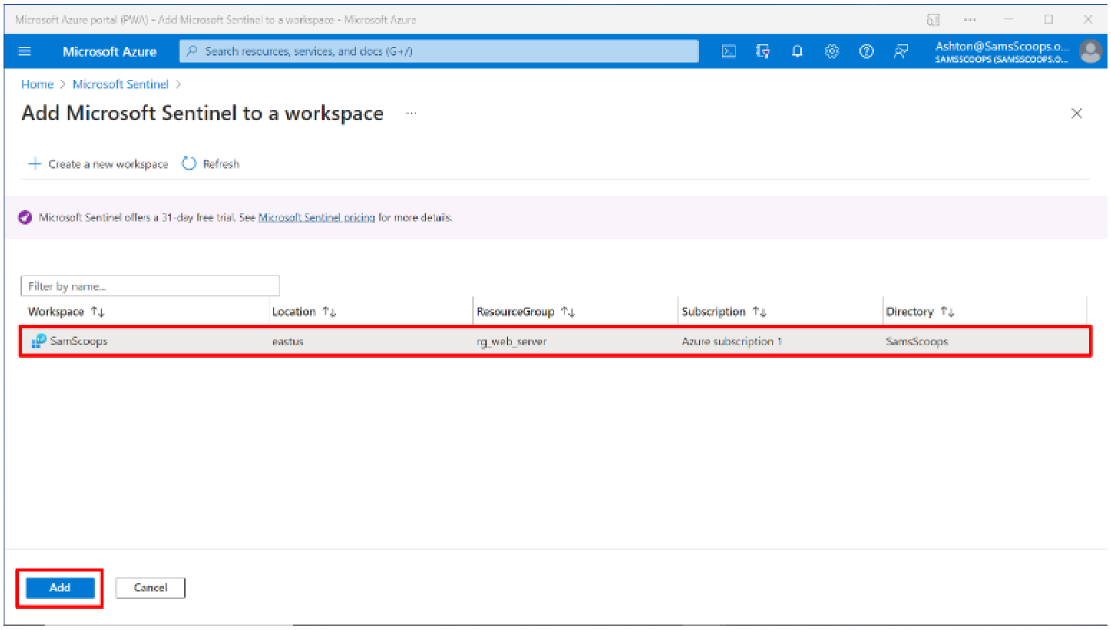
Pricing

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.

7. After a few seconds a new workspace is created. Select **SamScoops**.

8. Select **Add**.



Microsoft Azure portal (PWA) - Add Microsoft Sentinel to a workspace - Microsoft Azure

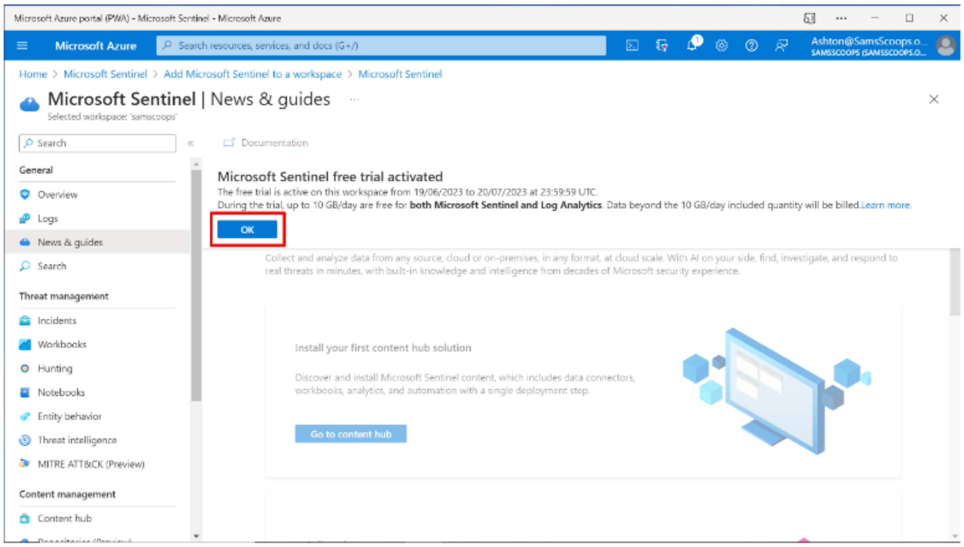
Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
SamScoops	eastus	rg_web_server	Azure subscription 1	SamsScoops

9. Select **OK** when the notification of the activation of Microsoft Sentinel's free trial appears.


Microsoft Azure portal (PWA) - Microsoft Sentinel - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Microsoft Sentinel | News & guides
Selected workspace: 'samscoops'
Search
Documentation
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub
OK
Go to content hub

Microsoft Sentinel free trial activated

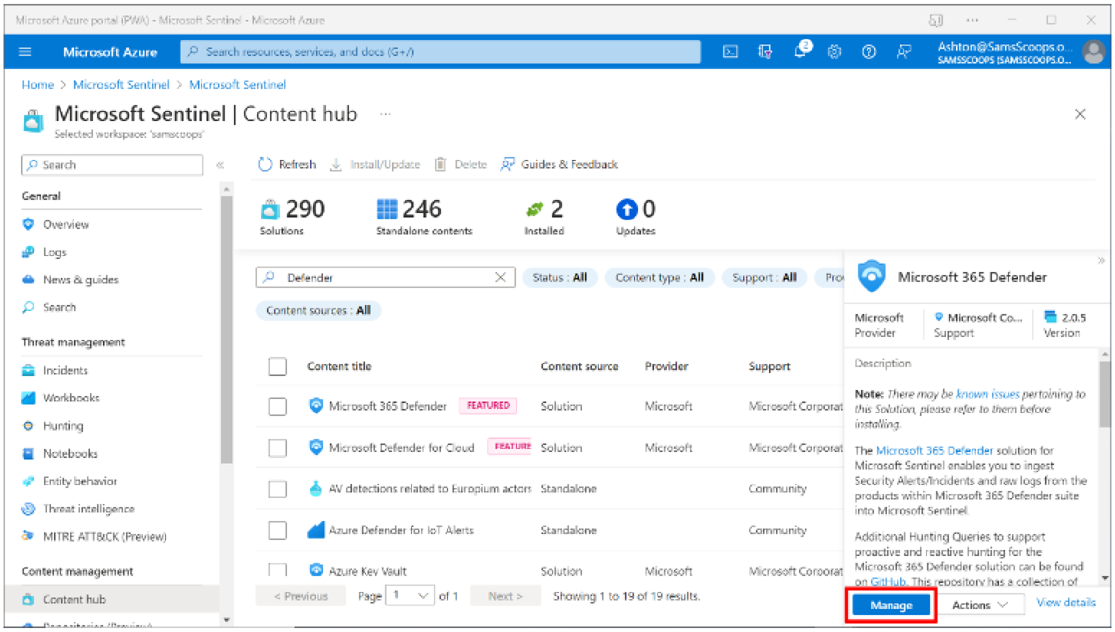
The free trial is active on this workspace from 19/06/2023 to 20/07/2023 at 23:59:59 UTC.
During the trial, up to 10 GB/day are free for **both Microsoft Sentinel and Log Analytics**. Data beyond the 10 GB/day included quantity will be billed.Learn more.

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.

Install your first content hub solution

Discover and install Microsoft Sentinel content, which includes data connectors, workbooks, analytics, and automation with a single deployment step.

10. After a few seconds, the connector will install. Then select **Manage** for Microsoft 365 Defender.



Content title	Content source	Provider	Support
□ Microsoft 365 Defender FEATURED	Solution	Microsoft	Microsoft Corporat
□ Microsoft Defender for Cloud FEATURE	Solution	Microsoft	Microsoft Corporat
□ AV detections related to Europium actors	Standalone		Community
□ Azure Defender for IoT Alerts	Standalone		Community
□ Azure Key Vault	Solution	Microsoft	Microsoft Corporat

Showing 1 to 19 of 19 results.

Description

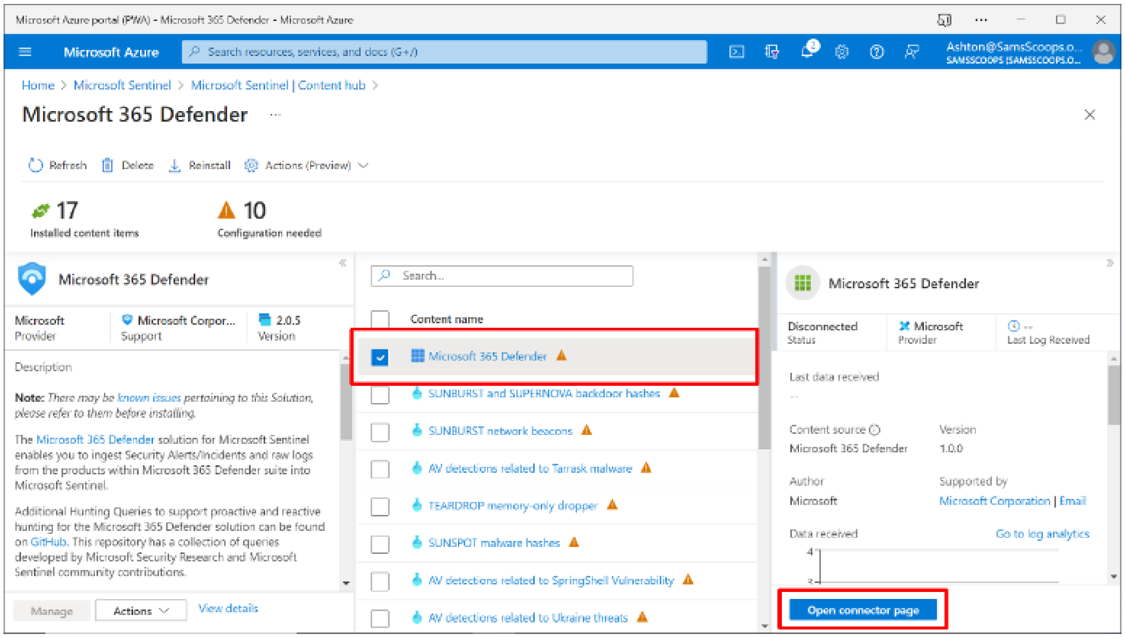
Note: *There may be known issues pertaining to this Solution, please refer to them before installing.*

The Microsoft 365 Defender solution for Microsoft Sentinel enables you to ingest Security Alerts/Incidents and raw logs from the products within Microsoft 365 Defender suite into Microsoft Sentinel.

Additional Hunting Queries to support proactive and reactive hunting for the Microsoft 365 Defender solution can be found on GitHub. This repository has a collection of

11. You now need to configure the connector. To do this, select **Microsoft 365 Defender**.

12. Select **Open connector page**.


Microsoft Azure portal (PWA) - Microsoft 365 Defender - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Microsoft Sentinel | Content hub >
Microsoft 365 Defender
Refresh
Delete
Reinstall
Actions (Preview)
Search...
Content name
Manage
Actions
View details
Open connector page
Go to log analytics
4
3

17 Installed content items

10 Configuration needed

Microsoft 365 Defender

Microsoft	Microsoft Corpor...	2.0.5
Provider	Support	Version

Description

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

The Microsoft 365 Defender solution for Microsoft Sentinel enables you to ingest Security Alerts/Incidents and raw logs from the products within Microsoft 365 Defender suite into Microsoft Sentinel.

Additional Hunting Queries to support proactive and reactive hunting for the Microsoft 365 Defender solution can be found on GitHub. This repository has a collection of queries developed by Microsoft Security Research and Microsoft Sentinel community contributions.

- ☑ Microsoft 365 Defender
- □ SUNBURST and SUPERNOVA backdoor hashes
- □ SUNBURST network beacons
- □ AV detections related to Tarrask malware
- □ TEARDROP memory-only dropper
- □ SUNSPOT malware hashes
- □ AV detections related to SpringShell Vulnerability
- □ AV detections related to Ukraine threats

Microsoft 365 Defender

Disconnected	Microsoft	--
Status	Provider	Last Log Received

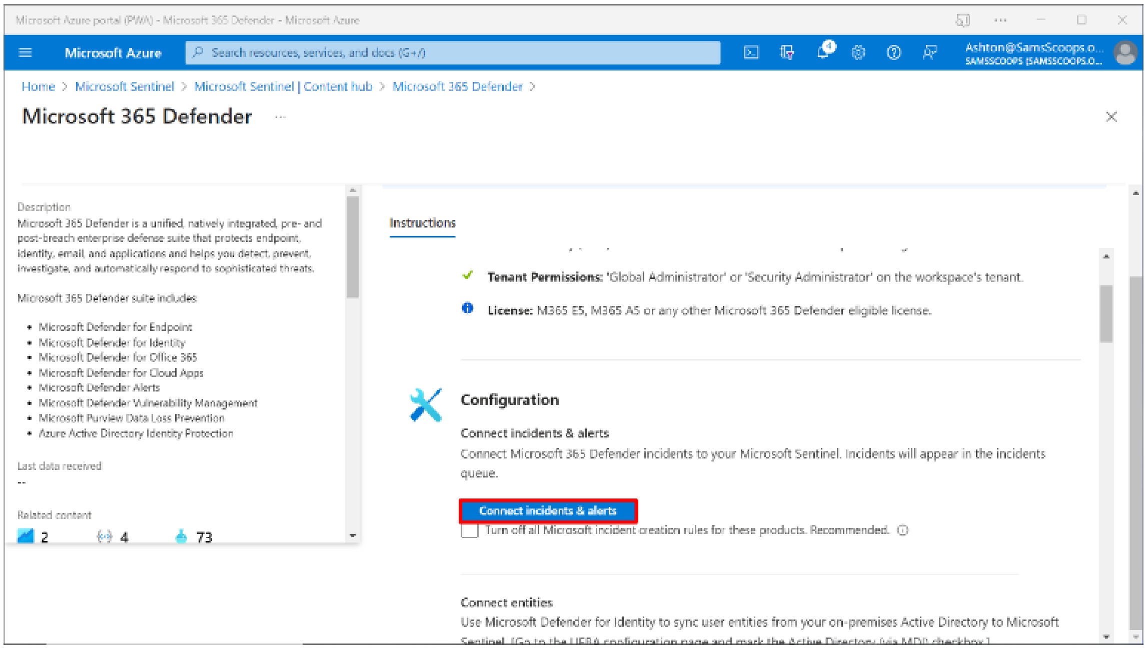
Last data received
--

Content source: Microsoft 365 Defender
Version: 1.0.0

Author: Microsoft
Supported by: Microsoft Corporation | Email

Data received

13. Scroll down and select **Connect incidents & alerts**.



Microsoft Azure portal (PWA) - Microsoft 365 Defender - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Microsoft 365 Defender >

Microsoft 365 Defender

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alerts
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Azure Active Directory Identity Protection

Last data received

--

Related content

2 4 73

Instructions

✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

License: M365 E5, M365 A5 or any other Microsoft 365 Defender eligible license.

Configuration

Connect incidents & alerts

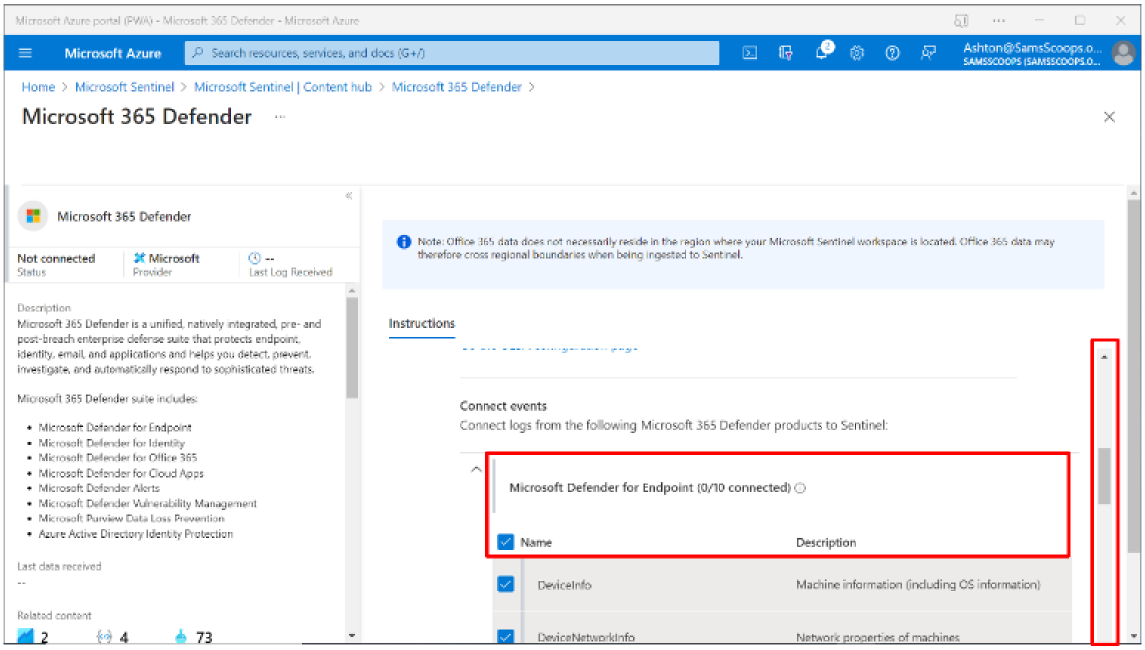
Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.

□ Turn off all Microsoft incident creation rules for these products. Recommended.

Connect entities

Use Microsoft Defender for Identity to sync user entities from your on-premises Active Directory to Microsoft Sentinel. [Go to the UEBA configuration page and mark the Active Directory (via MDI) checkbox.]

14. Scroll down and select the tick box next to **Name** under **Microsoft Defender for Endpoint**.



Microsoft Azure portal (PWA) - Microsoft 365 Defender - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Microsoft 365 Defender >

Microsoft 365 Defender

Microsoft 365 Defender

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description
Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alerts
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Azure Active Directory Identity Protection

Last data received
--

Related content
2 4 73

Note: Office 365 data does not necessarily reside in the region where your Microsoft Sentinel workspace is located. Office 365 data may therefore cross regional boundaries when being ingested to Sentinel.

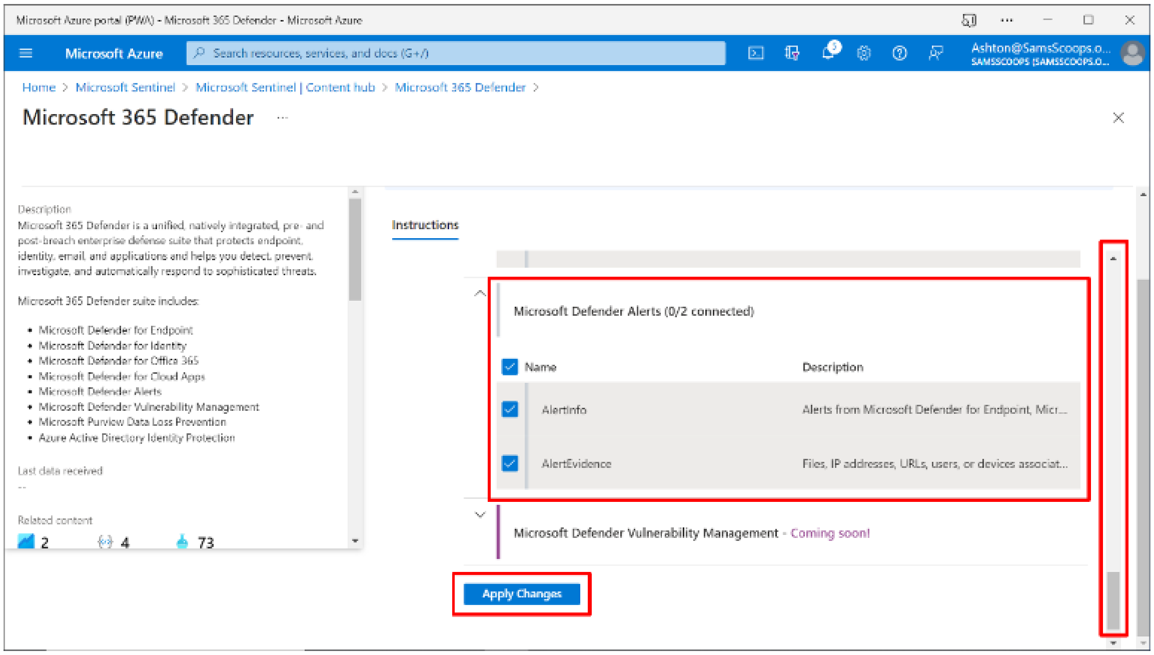
Connect events
Connect logs from the following Microsoft 365 Defender products to Sentinel:

Microsoft Defender for Endpoint (0/10 connected)

☑ Name	Description
☑ DeviceInfo	Machine information (including OS information)
☑ DeviceNetworkInfo	Network properties of machines

15. Scroll down and select the tick box next to **Name** under **Microsoft Defender Alerts**.

16. Select **Apply Changes**.


Microsoft Azure portal (PWA) - Microsoft 365 Defender - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Microsoft 365 Defender >

Microsoft 365 Defender

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alerts
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Azure Active Directory Identity Protection

Last data received

--

Related content

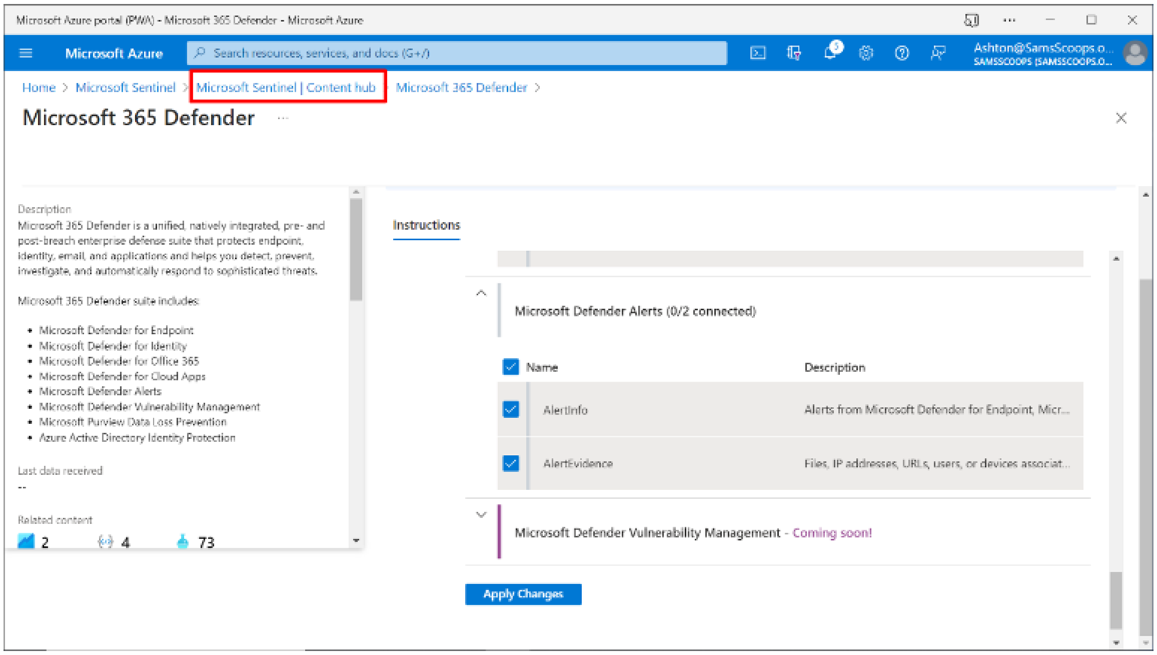
2 4 73

Microsoft Defender Alerts (0/2 connected)

☑ Name	Description
☑ AlertInfo	Alerts from Microsoft Defender for Endpoint, Micr...
☑ AlertEvidence	Files, IP addresses, URLs, users, or devices associat...

Microsoft Defender Vulnerability Management - Coming soon!

17. Navigate back to the **Content hub** page by selecting **Microsoft Sentinel|Content hub** at the top of the page.



Microsoft Azure portal (PWA) - Microsoft 365 Defender - Microsoft Azure

Microsoft Azure
Search resources, services, and docs (G+/)
Ashton@SamsScoops.o...
SAMSSCOOPS (SAMSSCOOPS.O...
Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Microsoft 365 Defender >

Microsoft 365 Defender

Description
Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alerts
- Microsoft Defender Vulnerability Management
- Microsoft Purview Data Loss Prevention
- Azure Active Directory Identity Protection

Last data received
--

Related content
2 4 73

Instructions

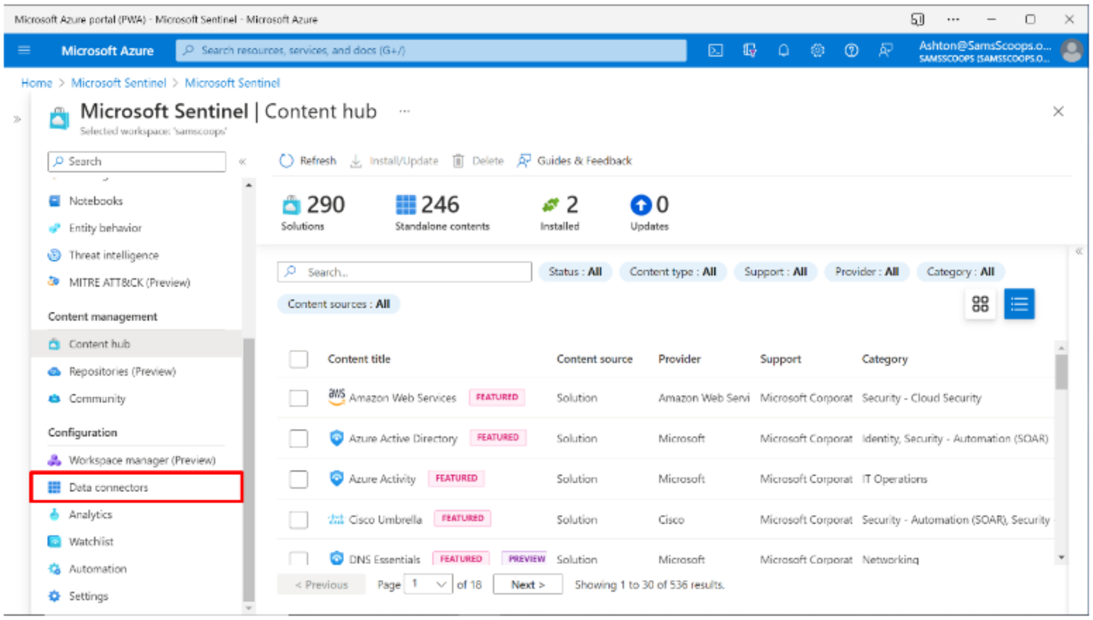
Microsoft Defender Alerts (0/2 connected)

☑ Name	Description
☑ AlertInfo	Alerts from Microsoft Defender for Endpoint, Micr...
☑ AlertEvidence	Files, IP addresses, URLs, users, or devices associat...

Microsoft Defender Vulnerability Management - Coming soon!

Step 3: Review implementation

1. Select **Data connectors** from the left-hand menu.



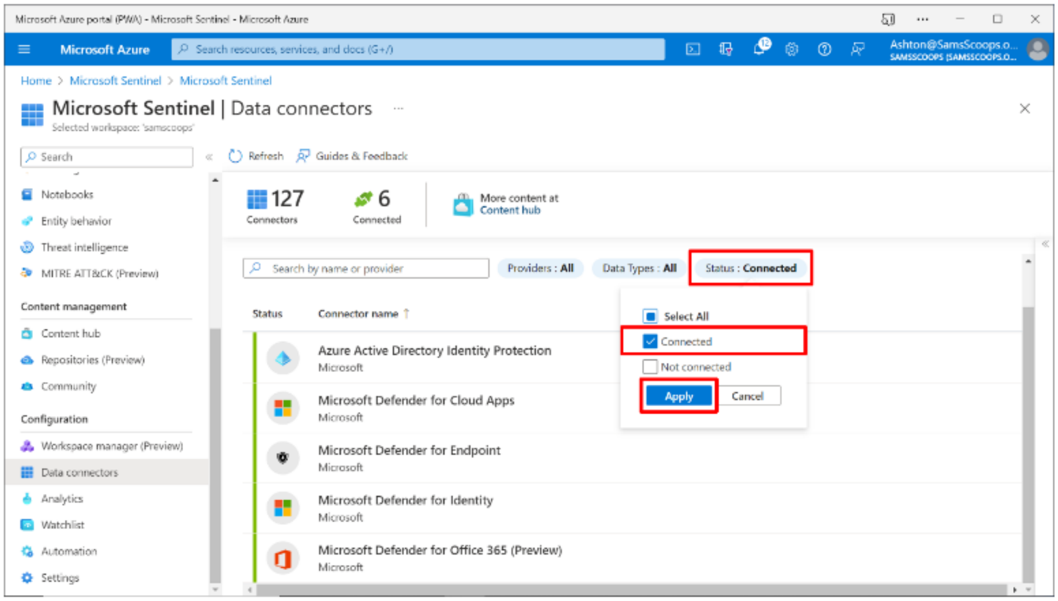
290 Solutions | 246 Standalone contents | 2 Installed | 0 Updates

Status : **All** | Content type : **All** | Support : **All** | Provider : **All** | Category : **All** | Content sources : **All**

☐	Content title	Content source	Provider	Support	Category
☐	Amazon Web Services FEATURED	Solution	Amazon Web Servi	Microsoft Corporat	Security - Cloud Security
☐	Azure Active Directory FEATURED	Solution	Microsoft	Microsoft Corporat	Identity, Security - Automation (SOAR)
☐	Azure Activity FEATURED	Solution	Microsoft	Microsoft Corporat	IT Operations
☐	Cisco Umbrella FEATURED	Solution	Cisco	Microsoft Corporat	Security - Automation (SOAR), Security
☐	DNS Essentials FEATURED PREVIEW	Solution	Microsoft	Microsoft Corporat	Networking

Page 1 of 18 Showing 1 to 30 of 536 results.

2. Filter the output by selecting **Status** and then selecting **Connected** and **Apply**.



Microsoft Sentinel | Data connectors

Selected workspace: 'samscoops'

127 Connectors

6 Connected

Providers : All

Data Types : All

Status : Connected

■ Select All

☑ Connected

□ Not connected

Status	Connector name
	Azure Active Directory Identity Protection Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft

3. Record how many connectors have been connected.