Reconnaissance
Microsoft 365 Analytics Simplified

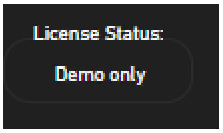
Reconnaissance Prerequisite Guide: Entra ID, Microsoft Graph API, and Log Analytics API Configuration

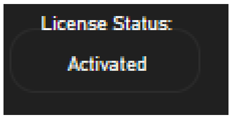
MODEL
TECHNOLOGY SOLUTIONS

Contents

Licensed vs Demo

By default, the Reconnaissance Dashboard is populated with demo data. The License Status text on the dashboard will reflect Demo only. (once activated the status will change on next refresh)


License Status:
Demo only


License Status:
Activated

The demo data allows you to get an idea of what your own data might look like and how you might garner insights for your organization.

A valid license key is required to unlock the full potential of Reconnaissance and query your own data.

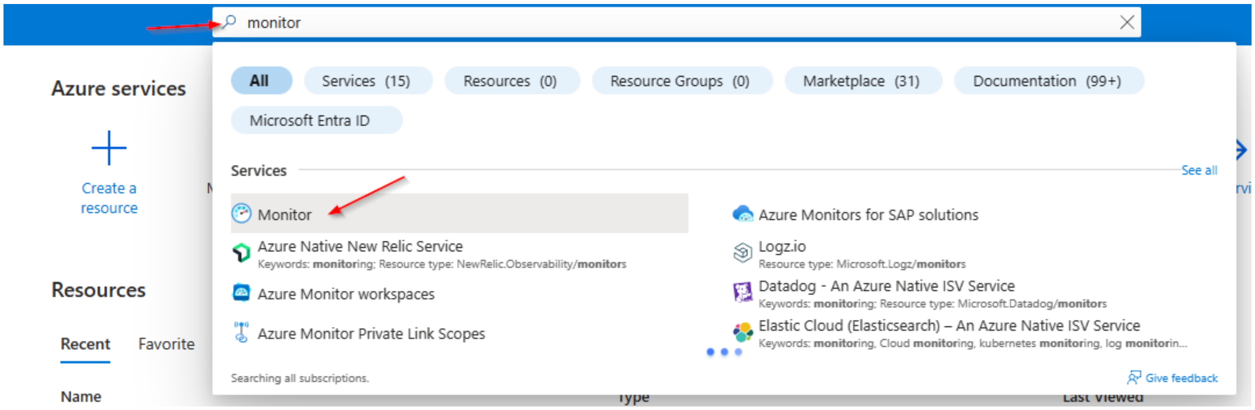
Follow the instructions in this document to capture the required parameter data, and reach out to Sales@model-technology.com to procure a license key.

Once the prerequisites have been completed and you have a license and required parameters you are ready to start your journey into Microsoft 365 Analytics.

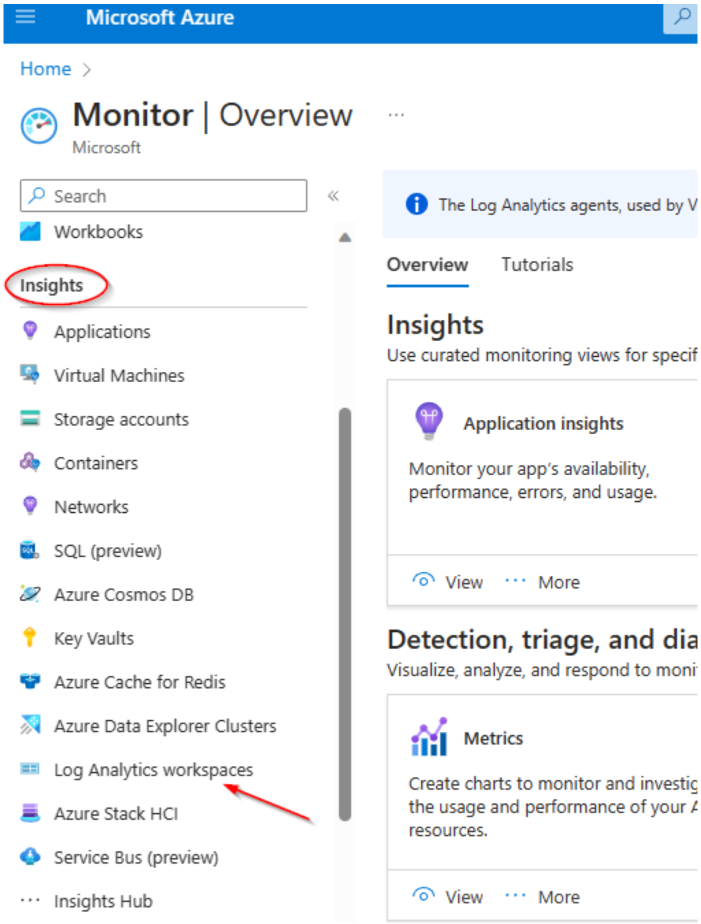
New Log Analytics Workspace

If you are already leveraging log analytics you can use your existing workspace. Please skip steps 2 – 10.

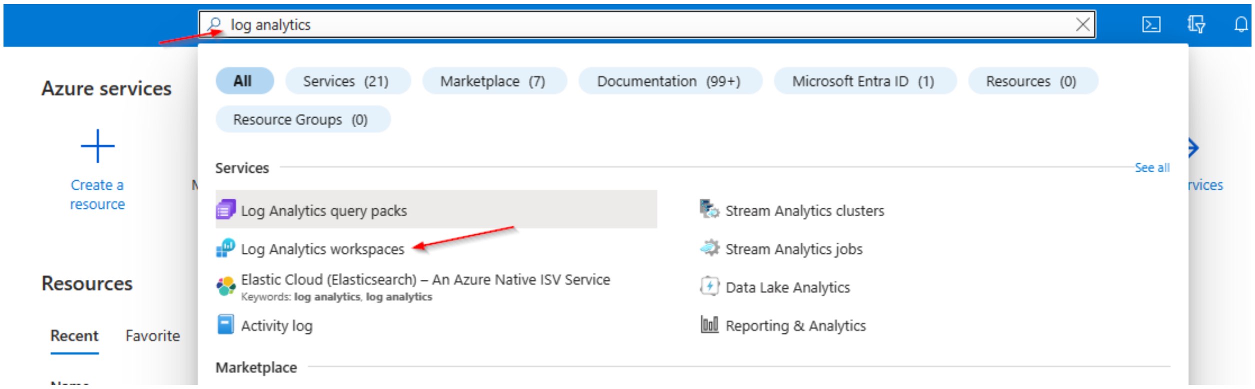
1. Login to portal.azure.com
    a. Don't forget to elevate your account using PIM (if applicable).
2. In the search bar type Monitor, then click Monitor in the search results.


monitor
Azure services
Create a resource
Resources
Recent
Favorite
Name
Type
Last Viewed
All
Services (15)
Resources (0)
Resource Groups (0)
Marketplace (31)
Documentation (99+)
Microsoft Entra ID
Services
See all
Monitor
Azure Native New Relic Service
Keywords: monitoring; Resource type: NewRelic.Observability/monitors
Azure Monitor workspaces
Azure Monitor Private Link Scopes
Azure Monitors for SAP solutions
Logz.io
Resource type: Microsoft.Logz/monitors
Datadog - An Azure Native ISV Service
Keywords: monitoring; Resource type: Microsoft.Datadog/monitors
Elastic Cloud (Elasticsearch) – An Azure Native ISV Service
Keywords: monitoring, Cloud monitoring, kubernetes monitoring, log monitorin...
Searching all subscriptions.
Give feedback

3. In the navigation bar under Insights, click Log Analytics workspaces.



4. In the search bar type *log analytics*, then select Log Analytics workspaces.



log analytics

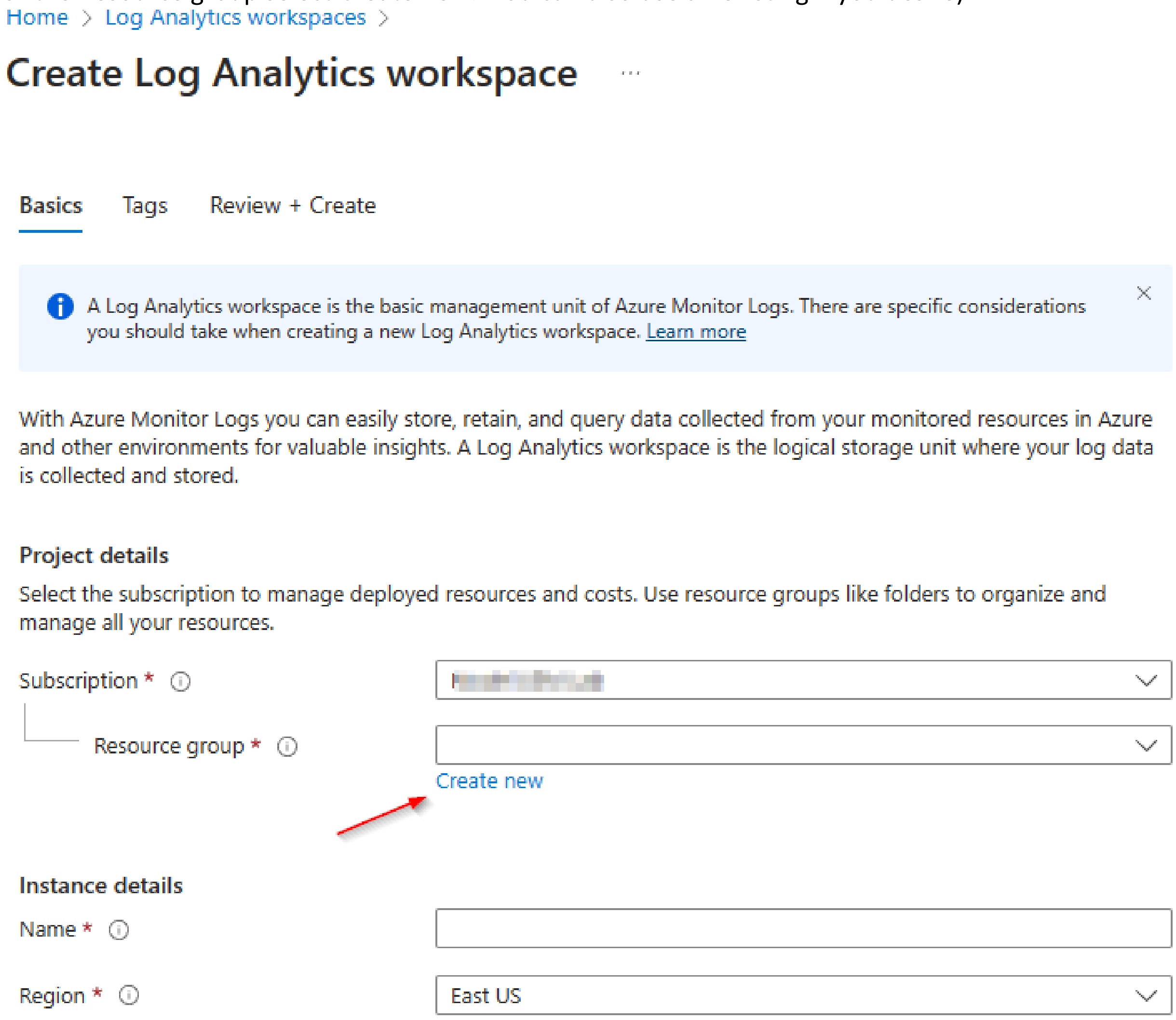
All | Services (21) | Marketplace (7) | Documentation (99+) | Microsoft Entra ID (1) | Resources (0) | Resource Groups (0)

Services — See all

- Log Analytics query packs
- Log Analytics workspaces
- Elastic Cloud (Elasticsearch) – An Azure Native ISV Service
  Keywords: log analytics, log analytics
- Activity log
- Stream Analytics clusters
- Stream Analytics jobs
- Data Lake Analytics
- Reporting & Analytics

Marketplace

5. For the Resource group select Create new. You can also use an existing if you desire)



Home > Log Analytics workspaces >

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 * : [redacted]

Resource group * :

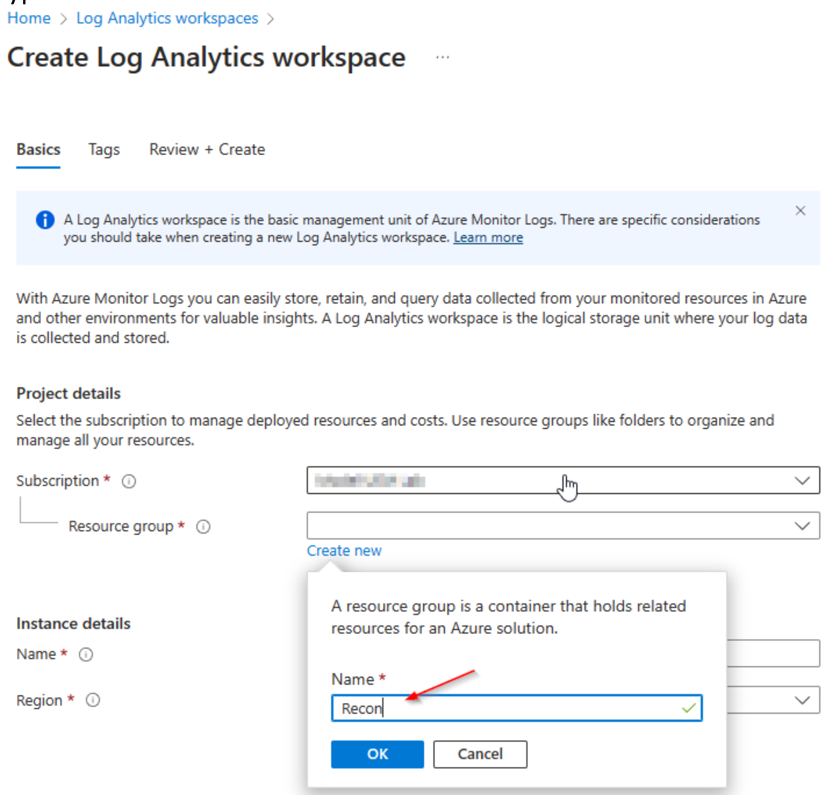
Create new

Instance details

Name * :

Region * : East US

6. Type Recon and click OK.



Home > Log Analytics workspaces >

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 * [redacted]

Resource group *

Create new

A resource group is a container that holds related resources for an Azure solution.

Name *

Recon

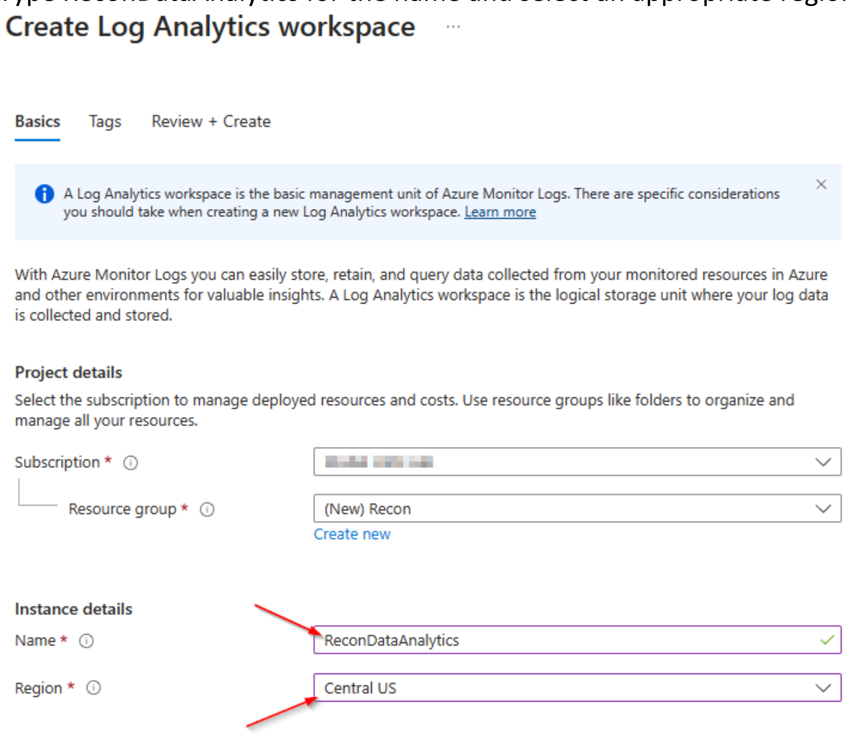
OK Cancel

Instance details

Name *

Region *

7. Type ReconDataAnalytics for the name and select an appropriate region.



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 * [redacted]

Resource group * (New) Recon

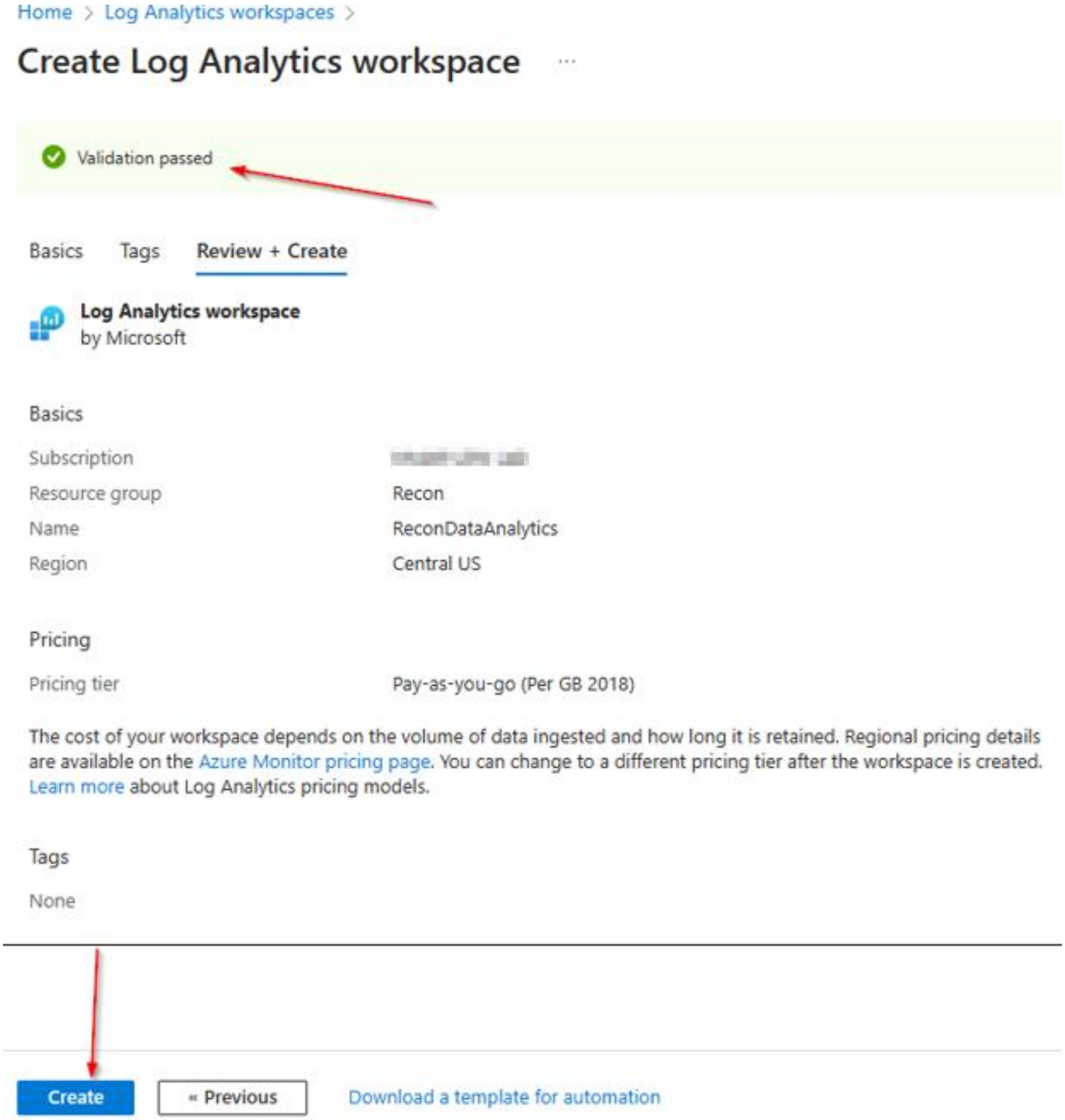
Create new

Instance details

Name * ReconDataAnalytics

Region * Central US

8. Click Next at Tags.
9. You should see Validation passed. Click Create.



Home > Log Analytics workspaces >

Create Log Analytics workspace ...

✓ Validation passed

Basics Tags **Review + Create**

Log Analytics workspace
by Microsoft

Basics

Subscription	[redacted]
Resource group	Recon
Name	ReconDataAnalytics
Region	Central US

Pricing

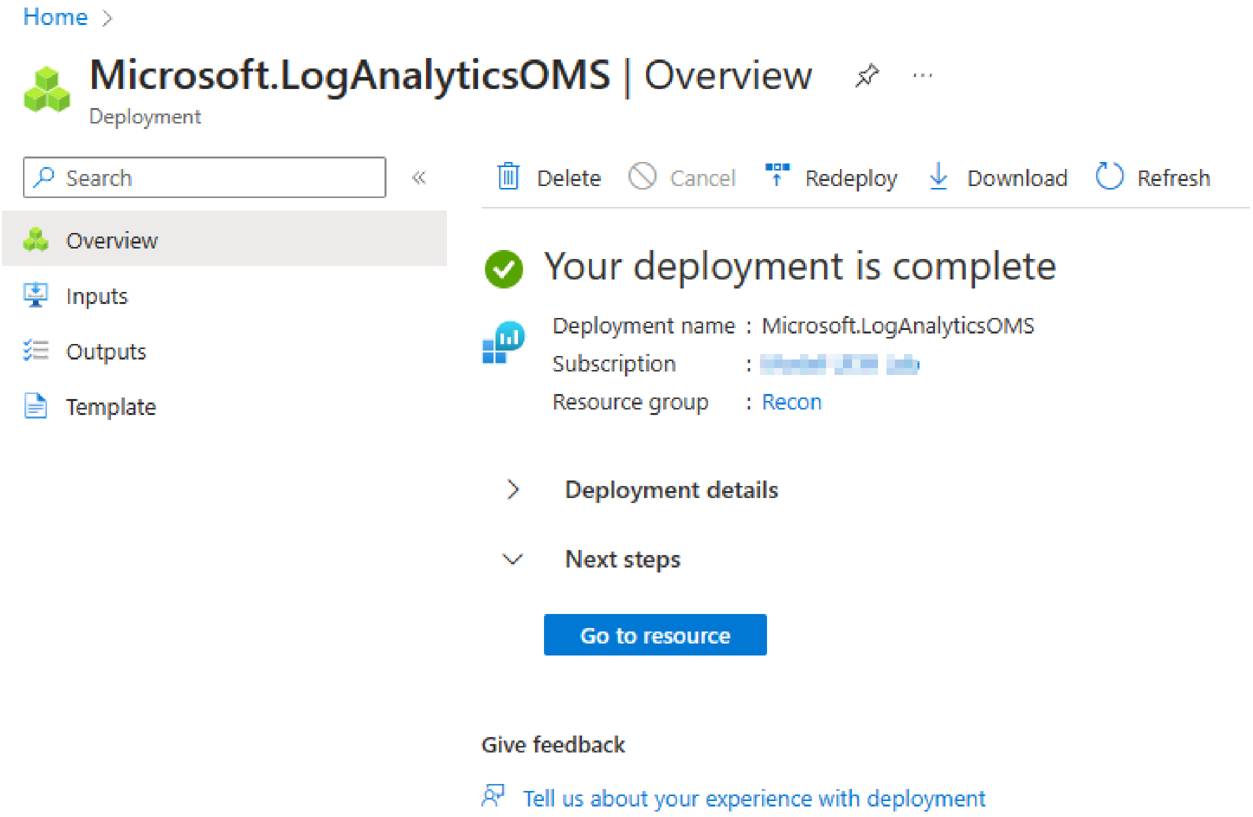
Pricing tier	Pay-as-you-go (Per GB 2018)

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

10. You are ready to proceed once the deployment is complete. Click Go to resource.



Home >

Microsoft.LogAnalyticsOMS | Overview

Deployment

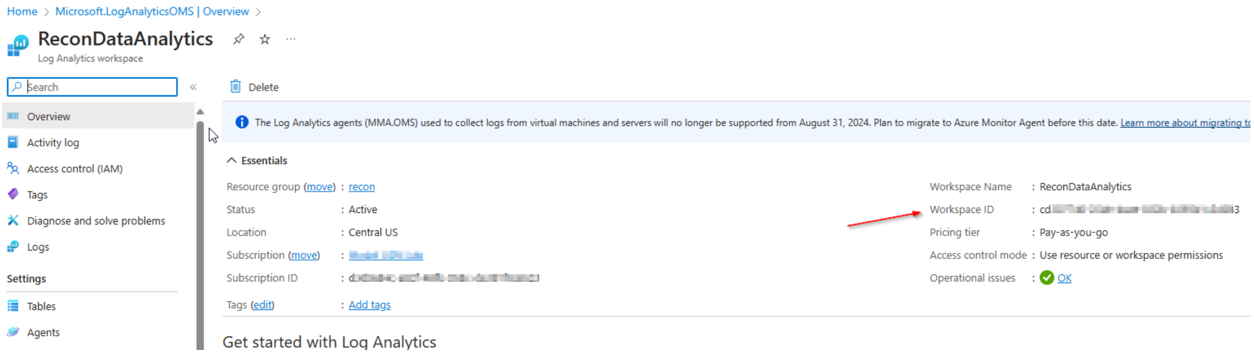
Your deployment is complete

Deployment name : Microsoft.LogAnalyticsOMS
Subscription : [redacted]
Resource group : Recon

Give feedback

Tell us about your experience with deployment

11. Capture the Log Analytics Workspace ID from the Overview page. This will be used as a parameter for the dashboard. Store in a secure location.



Home > Microsoft.LogAnalyticsOMS | Overview >

ReconDataAnalytics

Log Analytics workspace

The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to

Essentials

Resource group (move) : recon
Status : Active
Location : Central US
Subscription (move) : [redacted]
Subscription ID : d[redacted]
Tags (edit) : Add tags

Workspace Name : ReconDataAnalytics
Workspace ID : cd[redacted]3
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : ✓ OK

Get started with Log Analytics

Register new Entra ID app and grant access to Graph API

Register new application in Entra ID

1. Access the Azure Portal: - Navigate to the Azure Portal (https://portal.azure.com) and log in.
2. Navigate to App Registrations: - Select "Microsoft Entra ID" and then choose "App registrations".
3. Click on "New registration" and provide a name for the app like *Recon-GraphAPI*. Leave the remaining settings default and click Register.

Obtain Application (Client) ID and Tenant

1. Once the application is registered, note down the Application (Client) ID and Tenant ID from the app Overview page. These will be used as parameters for the dashboard. Store in a secure place.

Add Permissions for Graph API:

1. Go to "API permissions" and click "Add a permission".
2. Select Microsoft Graph and choose "Application permissions".
3. Add the following permissions:
    - ✓ Device.Read.All
    - ✓ DeviceManagementApps.Read.All
    - ✓ DeviceManagementConfiguration.Read.All
    - ✓ DeviceManagementManagedDevices.Read.All
    - ✓ DeviceManagementServiceConfig.Read.All
    - ✓ Directory.Read.All
    - ✓ Domain.Read.All
    - ✓ Group.Read.All
    - ✓ GroupMember.Read.All
    - ✓ Policy.Read.ConditionalAccess
    - ✓ Reports.Read.All
    - ✓ ServiceHealth.Read.All
    - ✓ ServiceMessage.Read.All

- ✓ User.Read
- ✓ User.Read.All
- ✓ WindowsUpdates.ReadWrite.All

Add permissions for Log Analytics API

1. Click “Add a permission” and select APIs my organization uses.
2. In the search bar type “log”. This should present the Log Analytics API. Select it, select Application permissions then select the following and click Add permissions.
   - ✓ Data.Read

Grant Admin Consent:

1. After adding all API permissions, you must grant admin consent for the organization. Click the button above the permissions and then click yes when prompted.

Create a Client Secret:

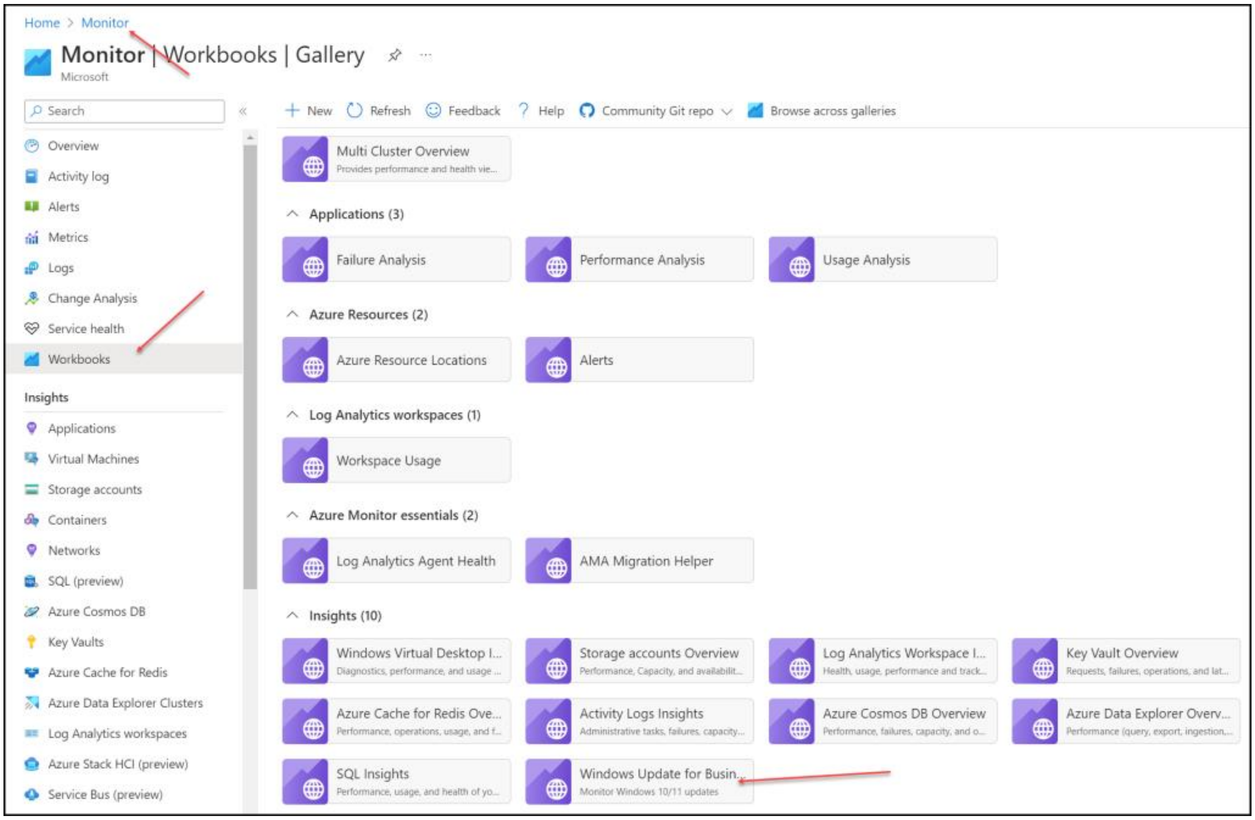
1. From the registered app, navigate to “Certificates & secrets”.
2. Click on “New client secret”, add a description, set an expiry period, and click "Add". Recommend a minimum of 12 months.
3. **IMPORTANT**: Note down the client secret *value*. This will be used as a parameter in the dashboard. Store in a secure location. *Once you navigate away from this page the secret value will be masked*.

Grant Registered App Access to Log Analytics Workspace

1. In the Azure Portal, navigate to your Log Analytics workspace.
2. Under “Access control (IAM)”, grant the new registered app (search by app name) the *Reader* Role assignment.
3. Find the Log Analytics workspace Overview page. This will be used as a parameter in the Dashboard. Store in a secure location.

Enable Windows Update for Business Reports in Azure Monitor

1. From portal.azure.com, enter Monitor in the search bar and select Monitor from the results.
2. From Monitor, select Workbooks from the navigation bar, then select Windows Update for Business under Insights.


Home > Monitor
Monitor | Workbooks | Gallery
Microsoft
Search
+ New
Refresh
Feedback
Help
Community Git repo
Browse across galleries
Overview
Activity log
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks
SQL (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Azure Data Explorer Clusters
Log Analytics workspaces
Azure Stack HCI (preview)
Service Bus (preview)
Multi Cluster Overview
Provides performance and health vie...
Applications (3)
Failure Analysis
Performance Analysis
Usage Analysis
Azure Resources (2)
Azure Resource Locations
Alerts
Log Analytics workspaces (1)
Workspace Usage
Azure Monitor essentials (2)
Log Analytics Agent Health
AMA Migration Helper
Insights (10)
Windows Virtual Desktop I...
Diagnostics, performance, and usage ...
Storage accounts Overview
Performance, Capacity, and availabilit...
Log Analytics Workspace I...
Health, usage, performance and track...
Key Vault Overview
Requests, failures, operations, and lat...
Azure Cache for Redis Ove...
Performance, operations, usage, and f...
Activity Logs Insights
Administrative tasks, failures, capacity...
Azure Cosmos DB Overview
Performance, failures, capacity, and o...
Azure Data Explorer Overv...
Performance (query, export, ingestion,...
SQL Insights
Performance, usage, and health of yo...
Windows Update for Busin...
Monitor Windows 10/11 updates

3. Enroll in Windows Update for Business Reports:
   a. Click Get Started.
   b. Select the proper tenant and workspace, then click Save settings.

      From Microsoft: It may take up to 24 hours for the initial setup to complete, and the rate at which data is uploaded depends on device connectivity and activity.
   c. Real world, **wait 24 hours** before coming back to this page.
4. Next, we will configure the client telemetry policies. Without these your Windows Update for Business Reports will be empty.

Configure Client Telemetry Policies in Microsoft Intune

1. In the Intune admin center, go to Devices > Windows > Configuration profiles.
2. On the Configuration profiles view, select Create profile.
3. Select the following options, then select Create when you're done:
    - Platform: Windows 10 and later
    - Profile type: Settings Catalog

    You're now on the Configuration profile creation page.
4. On the Basics tab, provide a Name and Description for the profile.
5. Using the Settings picker, select the *System* category.
6. Add the following required settings and values the *System* category:
    - Setting: *Allow Telemetry*
    - Value: *Basic, Security, or Full*
    - Basic is the minimum value, but it can be safely set to a higher value. Basic is also known as required diagnostic data. *Model suggests Full for best experience*.
7. Add the following recommended settings and values from the *System* category:

    Note

    These settings aren't required, but they're recommended to ensure that users of the device cannot override the diagnostic data level of the device.

    - Setting: *Allow device name to be sent in Windows diagnostic data*
    - Value: *Allowed*

        If this policy is disabled, the device name won't be sent and won't be visible in Windows Update for Business reports. This makes it impossible to tie compliance to an individual device. **HIGHLY recommend enabling this setting!!**

    - Setting: *Configure Telemetry Opt In Settings Ux*
    - Value: *Disabled*

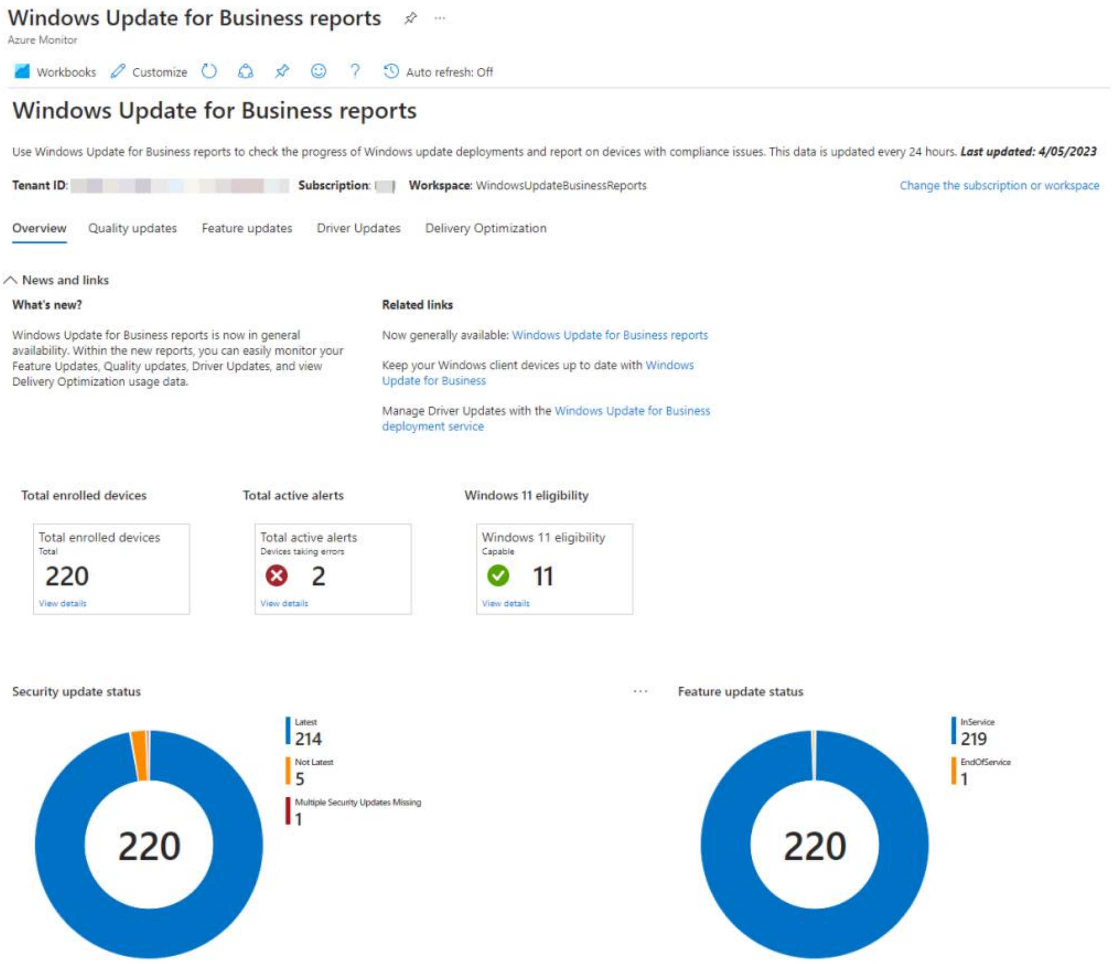
        By turning this setting on, you're disabling the ability for a user to potentially override the diagnostic data level of devices such that data won't be available for those devices in Windows Update for Business reports.

    - Setting: *Configure Telemetry Opt In Change Notification*
    - Value: *Disabled*

        By turning this setting on, you're disabling notifications of diagnostic data changes.

6. Continue through the next set of tabs Scope tags, Assignments, and Applicability Rules to complete the configuration of the profile without assigning it yet.
7. Review the settings and then select Create.
8. Recommend deploying the profile to a Group of pilot *Devices* and once satisfied deploy to *All Devices*.

9. Once the Windows update for Business report deployment is complete and clients start reporting data you will see data like so.



Windows Update for Business reports

Azure Monitor

Windows Update for Business reports

Use Windows Update for Business reports to check the progress of Windows update deployments and report on devices with compliance issues. This data is updated every 24 hours. ***Last updated: 4/05/2023***

Tenant ID: [redacted] **Subscription**: [redacted] **Workspace**: WindowsUpdateBusinessReports

What's new?

Windows Update for Business reports is now in general availability. Within the new reports, you can easily monitor your Feature Updates, Quality updates, Driver Updates, and view Delivery Optimization usage data.

Related links

Now generally available: Windows Update for Business reports

Keep your Windows client devices up to date with Windows Update for Business

Manage Driver Updates with the Windows Update for Business deployment service

Total enrolled devices	Total active alerts	Windows 11 eligibility
Total enrolled devices Total 220 View details	Total active alerts Devices taking errors ✖ 2 View details	Windows 11 eligibility Capable ✓ 11 View details

Data required to unlock Recon Demo

As noted throughout the document, there are 5 pieces of information required to unlock Reconnaissance.

1. Application/Client ID of the Registered App in Entra ID
2. Client Secret of the Registered App in Entra ID
3. Tenant ID of the Registered App
4. Log Analytics Workspace ID
5. Reconnaissance License Key (obtained via sales@model-technology.com)

Note. You may see additional parameters with <placeholder> text when registering your dashboard. These can be safely ignored as they will be leveraged in future revisions of the dashboard.