TD SYNNEX

MICROSOFT SENTINEL

Click-to-Run™ Solution Deployment Guide

TD SYNNEX

Azure Sentinel Deployment Guide

This guide was designed to provide channel partners with the post deployment steps required to successfully deploy Azure Sentinel.

Below is a list of action items as part of the deployment process and post deployment recommendations to customize the cloud environment.

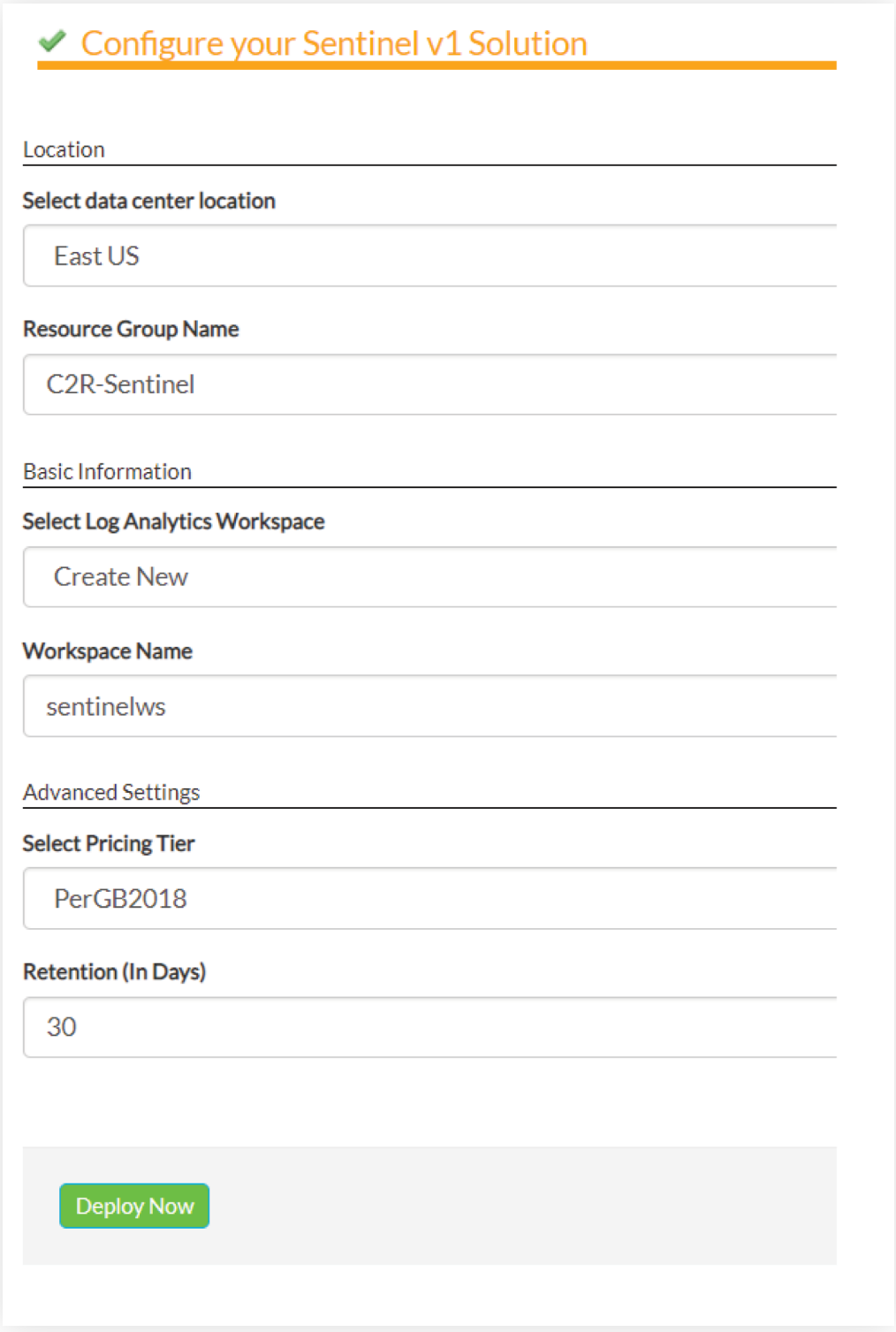
Technical Requirements – Customer Inputs

- What Region will the solution be deployed to?
- What will you name the Resource Group?
- Will you be using an existing Log Analytics Workspace or creating a new one?
- If a new Log Analytics Workspace, what will you name it?
- How many days of retention do you need?

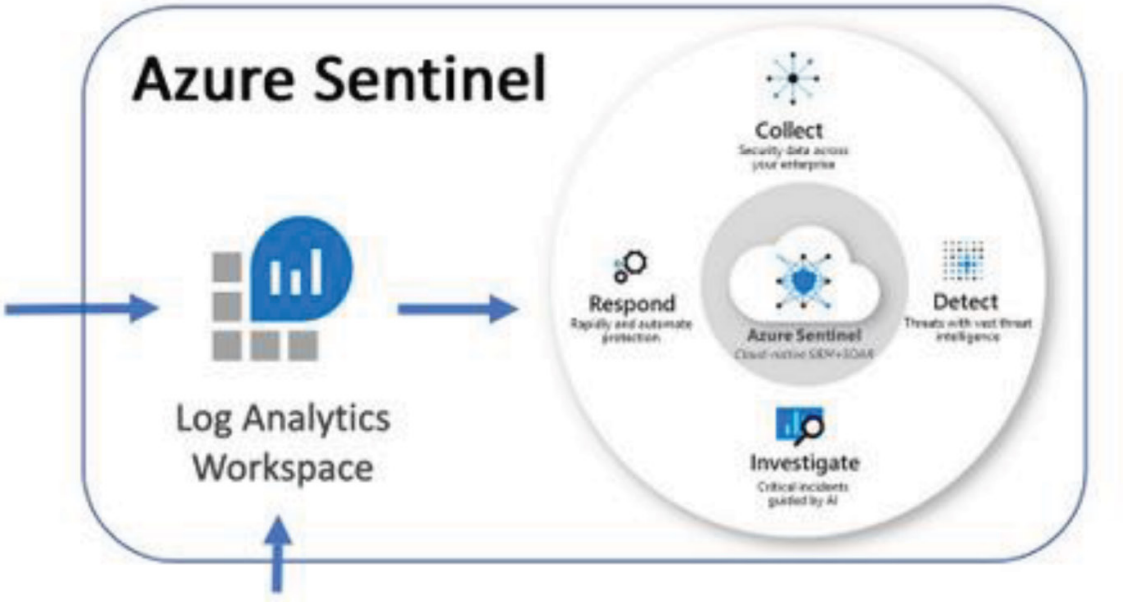
Table of Contents

- How do I access Sentinel after deployment?
- How do I modify Sentinel settings (price tier, log retention days, etc)?
- How do I remove Sentinel?
- How can I add additional data sources?

Example Deployment User Interface



Architecture Diagram



Resources Deployed

The following resources are deployed to build and configure this bundle.

- Log Analytics Workspace
- Azure Sentinel

Cost Breakdown

Azure Sentinel pricing

Azure Sentinel is billed based on the volume of data ingested for analysis in Azure Sentinel. Azure Sentinel offers a flexible and predictable pricing model.
There are two ways to pay for the Azure Sentinel service: Commitment Tiers and Pay-As-You-Go. The cost for Azure Sentinel depends on the pricing tier selected. Learn more about Azure Sentinel pricing.

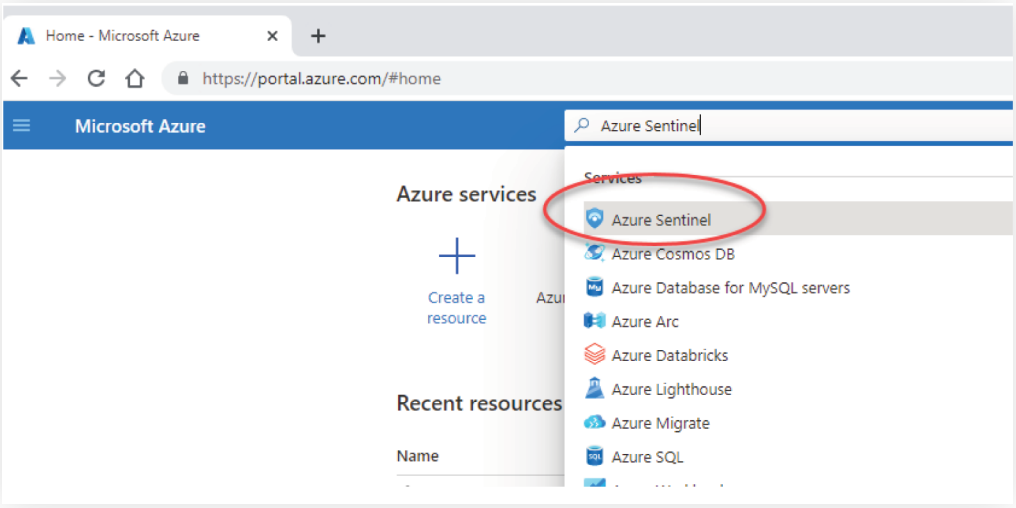
This does not include the Azure Log Analytics price for ingesting data. Learn more about Log Analytics pricing.

- **100 GB/day**
  50% discount over Pay-as-you-go
- **200 GB/day**
  55% discount over Pay-as-you-go
- **300 GB/day**
  57% discount over Pay-as-you-go
- **400 GB/day**
  58% discount over Pay-as-you-go
- **500 GB/day**
  60% discount over Pay-as-you-go
- **1 TB/day**
  61% discount over Pay-as-you-go
- **2 TB/day**
  63% discount over Pay-as-you-go
- **5 TB/day**
  65% discount over Pay-as-you-go
- **Pay-as-you-go**
  Per GB

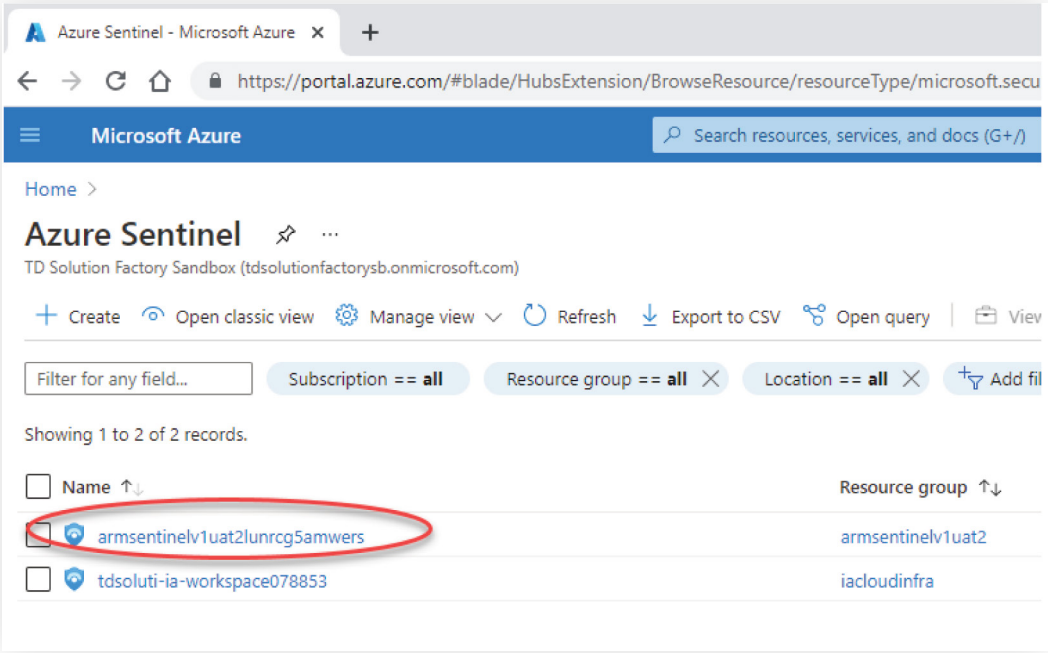
TD SYNNEX

How to Access Sentinel After Deployment

After deployment of the Click-to-Run™ Solution you can log into the Azure portal and search for “Azure Sentinel” to locate the Azure Sentinel section of the portal.



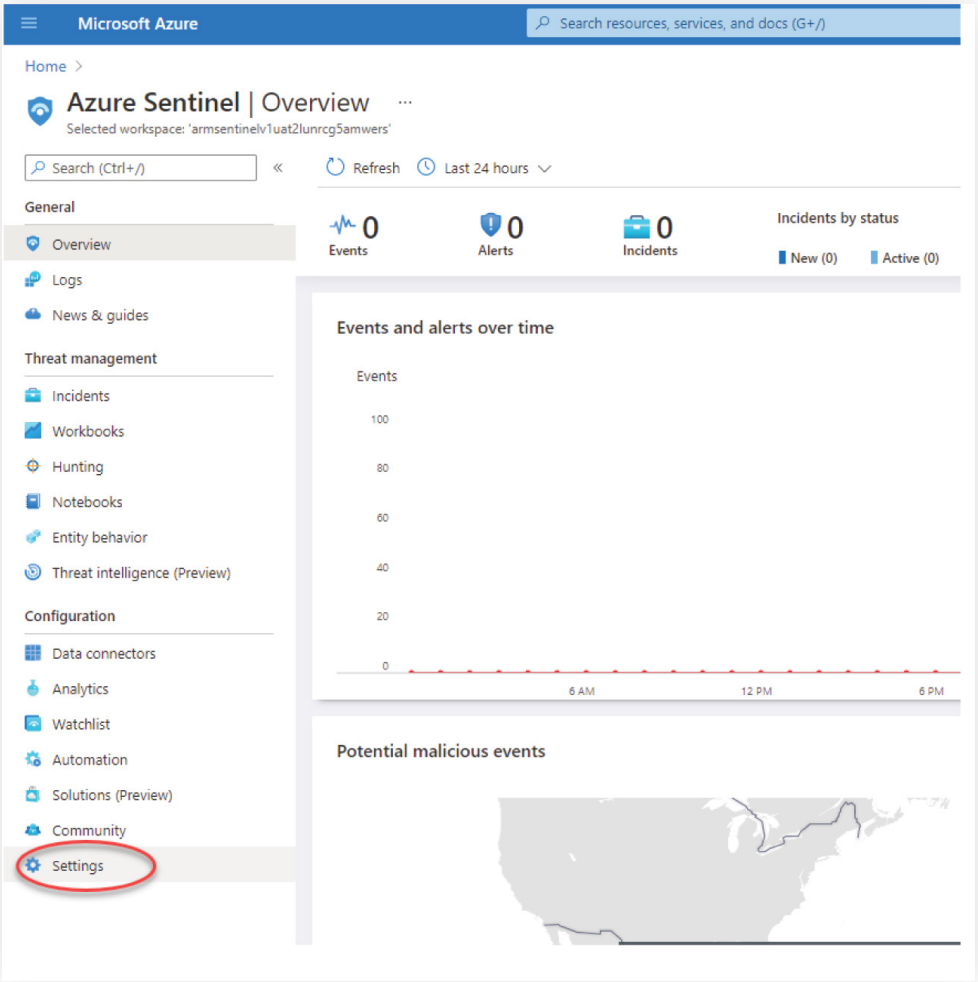
Then simply click on the log analytics workspace that you created during the deployment.



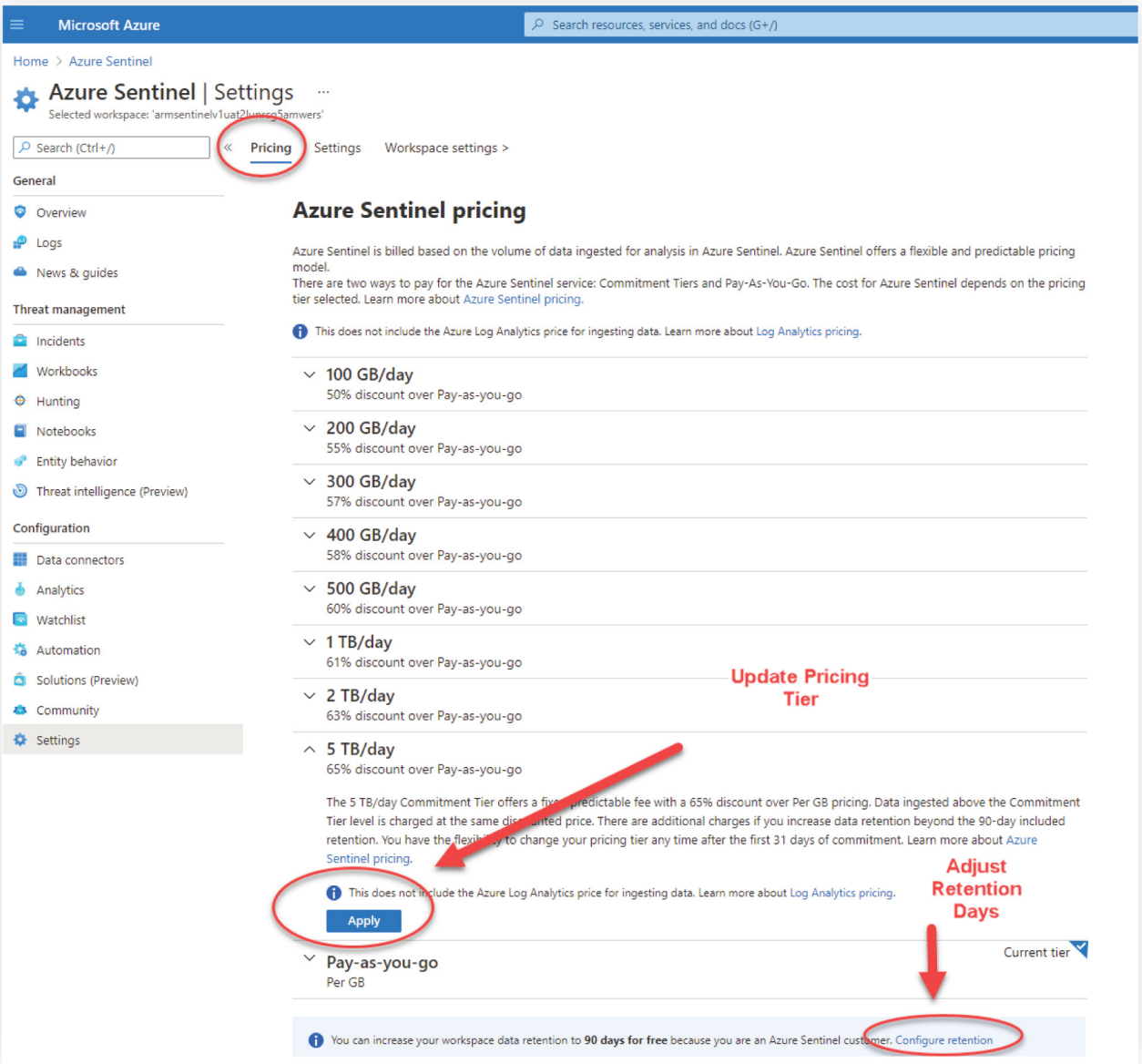
TD SYNNEX

How to Modify Sentinel Settings After Deployment

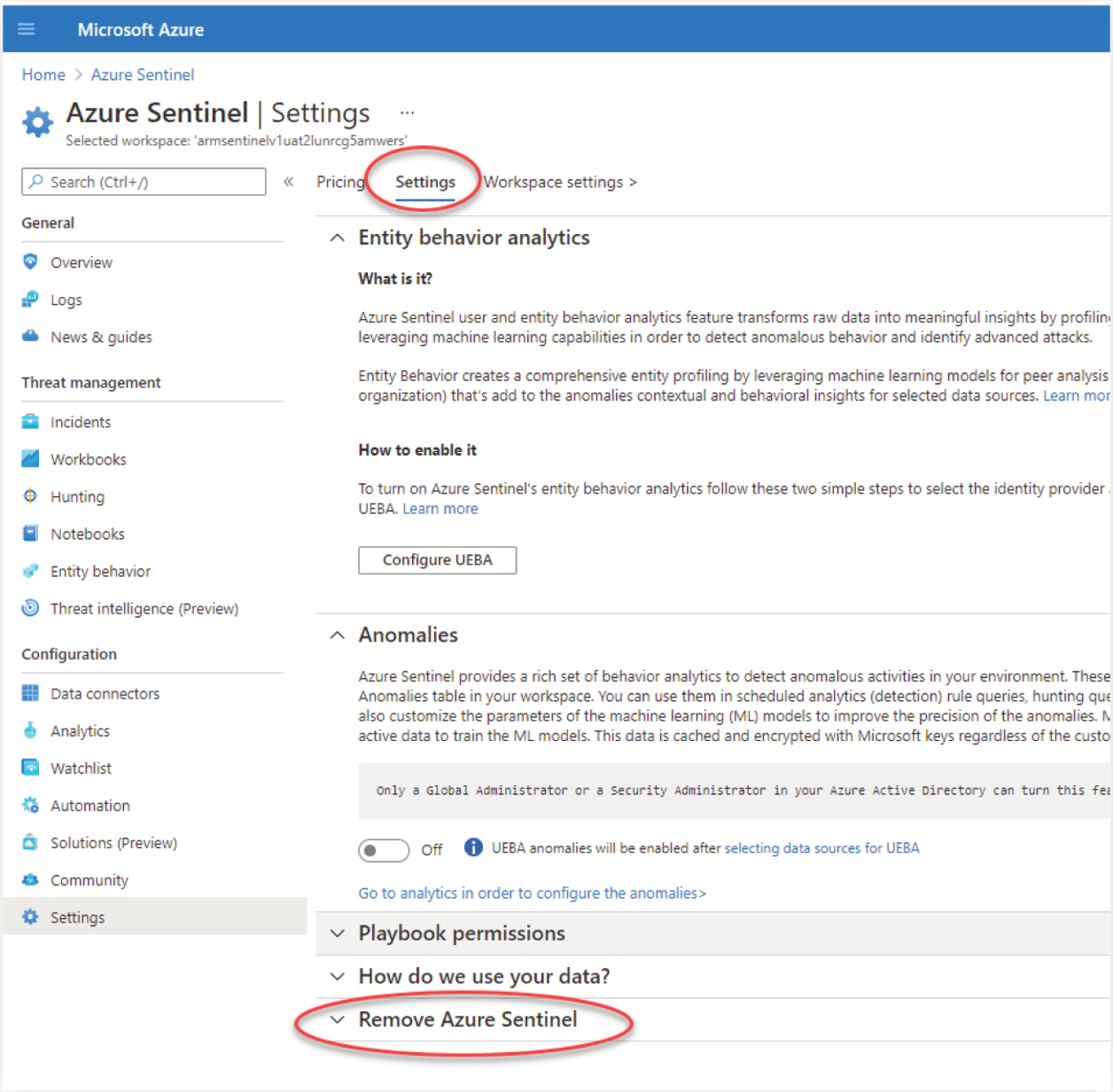
After deployment of the Click-to-Run™ Solution you can log into the Azure portal and search for “Azure Sentinel” to locate the Azure Sentinel section of the portal.



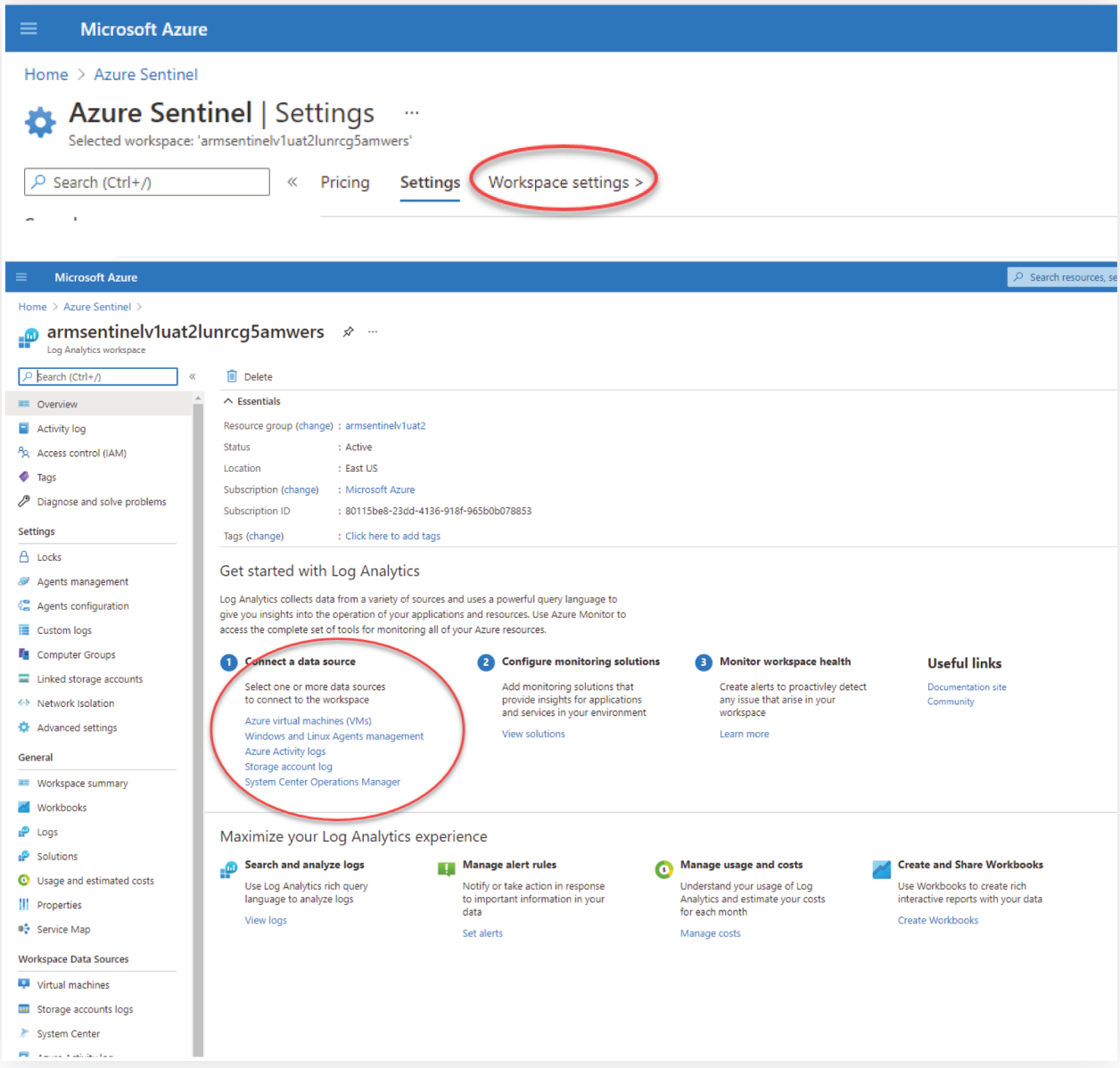
From the Pricing tab you are able to adjust the pricing tier and also adjust the retention days.



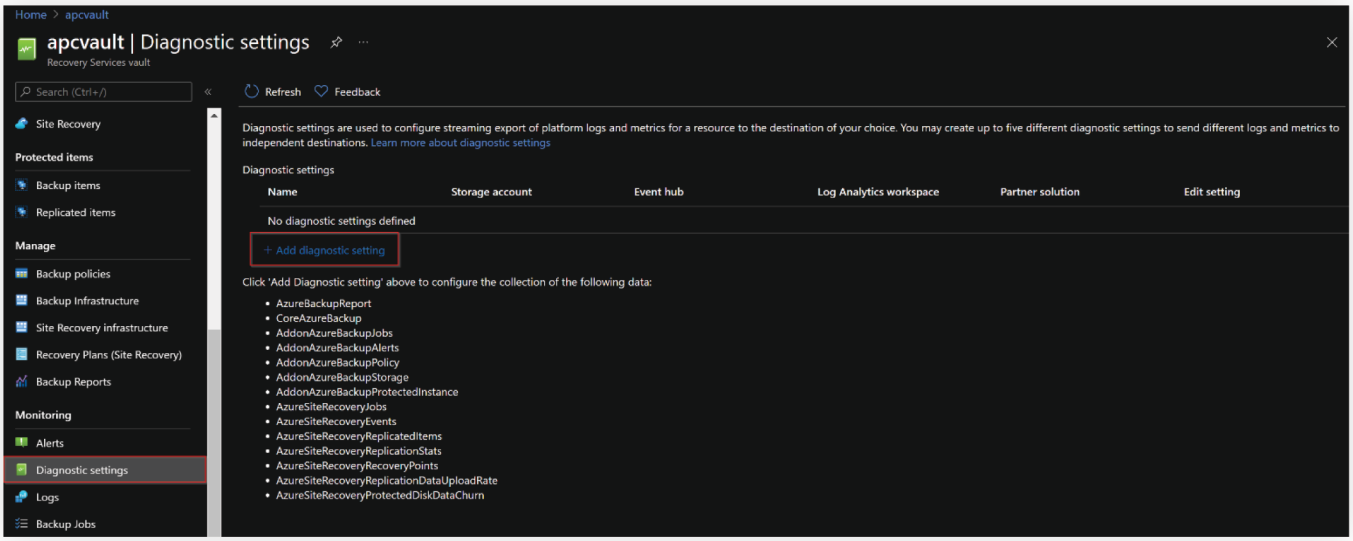
From the Settings tab you can remove the Azure Sentinel solution from the log analytics workspace.



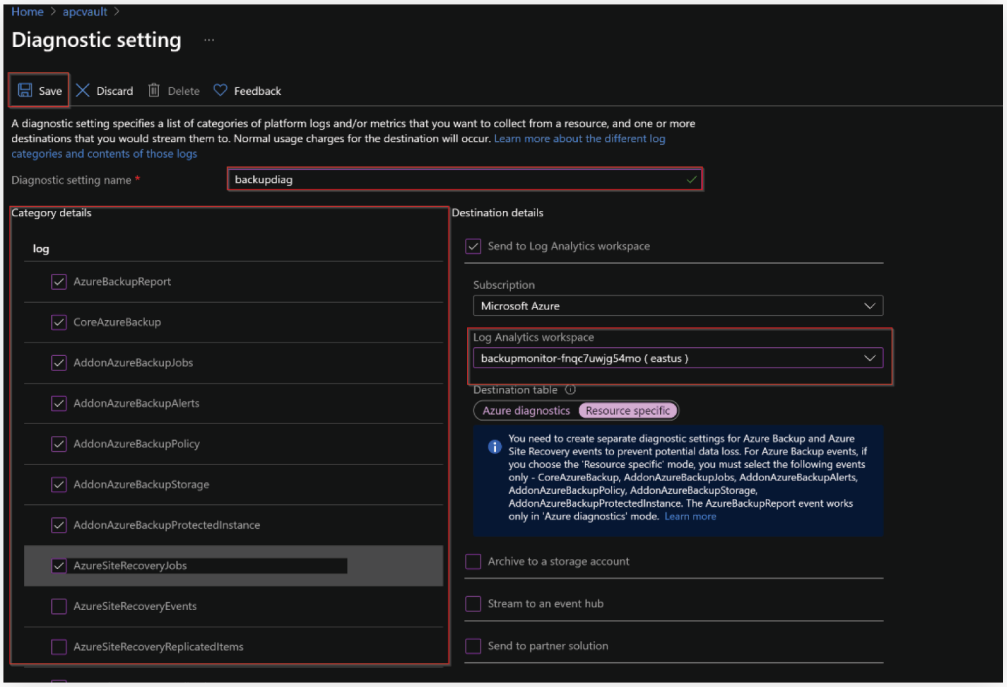
From the Workspace Settings tab, you will be presented to a settings screen where you can click to connect additional data sources.



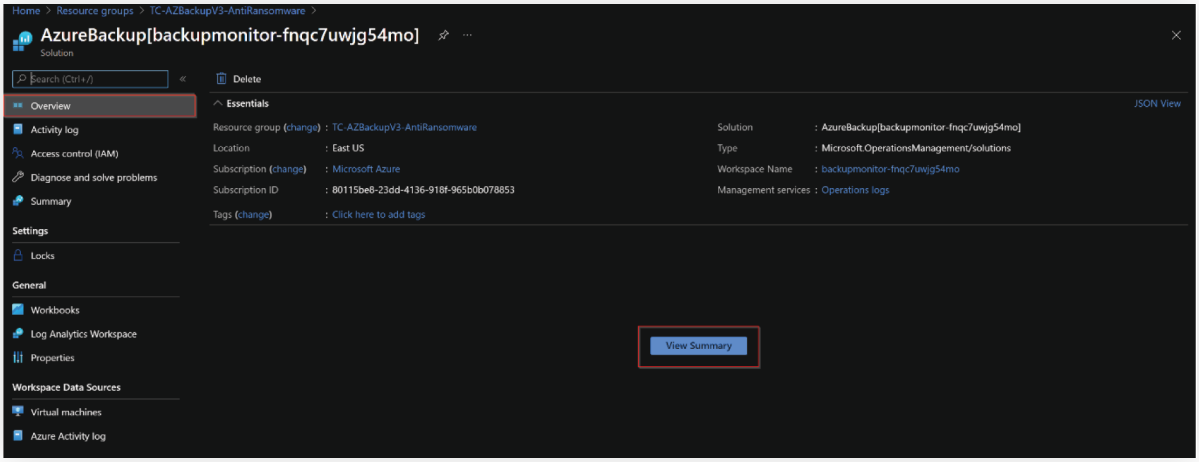
1. Navigate to your Recovery Services Vault and Select ‘Diagnostic Settings’ under the Alerts section.
   Select ‘Add diagnostic setting.’



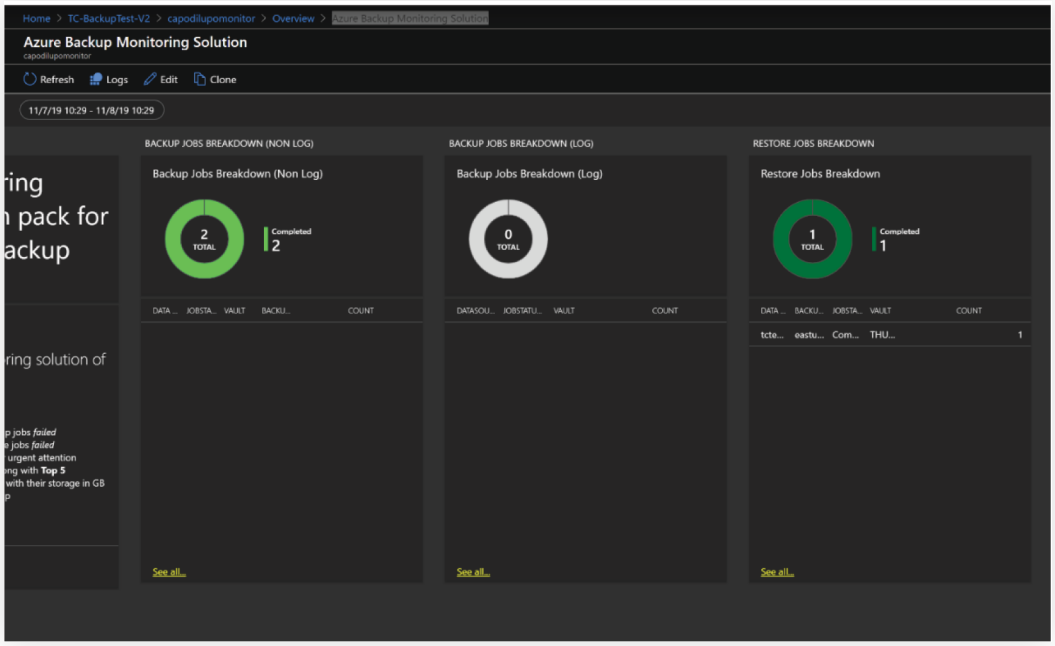
2. Give your custom Diagnostic settings a name. Select the backup and site recovery events that you would like to monitor from the Azure Backup solution. Specify the Log Analytics workspace that was created during this pre-configured deployment. Confirm your configuration and click ‘Save’.



3. Once your scheduled backup jobs have run, you can view the monitoringdashboard provided by the OMS solution. Navigate to the OMS solution and select ‘View Summary’ from the overview section to see more detailed information.

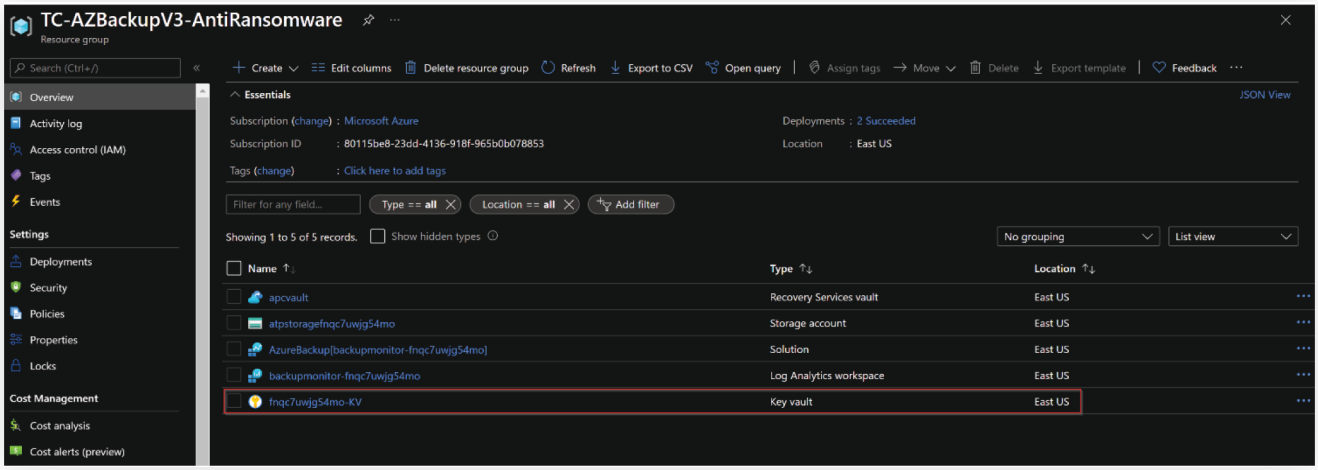


4. You may now view detailed dashboards and monitoring reports for your scheduled VM backups.



Azure Key Vault

You may optionally deploy an Azure Key Vault as part of the AZ Backup V3 Enhancements. Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. The Key Vault must be configured post deployment to fit your use case and scenario.
More information on how to configure can be found here.



ATP Storage Account

This pre-configured solution also gives the option to deploy a storage account with ATP. Advanced Threat Protection (ATP) for Azure Storage provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit storage accounts. This layer of protection allows you to protect and address concerns about potential threats to your storage accounts as they occur. These features work in conjunction with Azure Defender and Security Center. **To learn more, click here.**