

MICROSOFT SENTINEL

Click-to-Run[™] Solution Deployment Guide



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

 Configure your Sentinel v1 Solution
Location
Select data center location
East US
Resource Group Name
C2R-Sentinel
· · · · · ·
Basic Information Select Log Analytics Workspace
Select Log Analytics Workspace
Create New
Workspace Name
sentinelws
Advanced Settings
Select Pricing Tier
PerGB2018
Retention (In Days)
30
Deploy Now

Solutions Factory



Architecture Diagram



Resources Deployed

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

- Log Analytics Workspace
- Azure Sentinel



Cost Breakdown

٩z	ure 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.					
ÐT	his does not include the Azure Log Analytics price for ingesting data. Learn more about Log Analytics pricing.				
\sim	100 GB/day				
	50% discount over Pay-as-you-go				
\sim	200 GB/day				
	55% discount over Pay-as-you-go				
\sim	300 GB/day				
	57% discount over Pay-as-you-go				
\sim	400 GB/day				
	58% discount over Pay-as-you-go				
\sim	500 GB/day				
	60% discount over Pay-as-you-go				
\sim	1 TB/day				
	61% discount over Pay-as-you-go				
\sim	2 TB/day				
	63% discount over Pay-as-you-go				
\sim	5 TB/day				
	65% discount over Pay-as-you-go				
\sim	Pay-as-you-go				
	Per GB				

C 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.

👗 Home - Microsoft Azure 🗙 🕂		
← → C ☆ 🏻 https://portal.azure.com	/#home	
	Azure services	Services Azure Sentinel Azure Cosmos DB Azure Database for MySQL servers Azure Arc Azure Databricks
	Recent resources	Azure Lighthouse Azure Migrate
	Name	🧃 Azure SQL

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

👗 Azure Sentinel - Microsoft Azure 🗙 🕂					
← → C 🏠 🌲 https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.secu					
≡ Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)				
Home >					
Azure Sentinel ☆ … TD Solution Factory Sandbox (tdsolutionfactorysb.onmicrosoft.com)					
+ Create 💿 Open classic view 🛞 Manage view 🗸 🖒 Refresh 🚽	🖞 Export to CSV 😚 Open query 📔 🖆 Viev				
Filter for any field Subscription == all Resource group ==	= all \times Location == all \times $+_{\nabla}$ Add fil				
Showing 1 to 2 of 2 records.					
Name 14	Resource group $\uparrow\downarrow$				
armsentinelv1uat2lunrcg5amwers	armsentinelv1uat2				
tdsoluti-ia-workspace078853	iacloudinfra				

C 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.

	P Search resources, services, and docs (G+/)
Home > Azure Sentinel	
Azure Sentinel Setting	JS ··· Samwers'
Pricin	ng Settings Workspace settings >
General	
Overview	Azure Sentinel pricing
🧬 Logs	Azure Sentinel is billed based on the volume of data ingested for analysis in Azure Sentinel. Azure Sentinel offers a flexible and predictable pricing
🌰 News & guides	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
Threat management	tier selected. Learn more about Azure Sentinel pricing.
Incidents	f) This does not include the Azure Log Analytics price for ingesting data. Learn more about Log Analytics pricing.
Workbooks	✓ 100 GB/day
Hunting	50% discount over Pay-as-you-go
Notebooks	✓ 200 GB/day
💞 Entity behavior	55% discount over Pay-as-you-go
Threat intelligence (Preview)	300 GB/day 57% discount over Pay-as-you-go
Configuration	✓ 400 GB/day
Data connectors	58% discount over Pay-as-you-go
o Analytics	✓ 500 GB/day 60% discount over Pay as you do
Watchlist	a t TD / Inc.
🍓 Automation	61% discount over Pay-as-you-go
Solutions (Preview)	V 2 TB/day
Community	63% discount over Pay-as-you-go
Settings	5 TB/day 65% discount over Pay-as-youngo
(The 5 T8/day Commitment Tier offers a five medictable fee with a 65% discount over Per GB pricing. Data ingested above the Commitment Tier level is charged at the same discrumted price. There are additional charges if you increase data retention beyond the 90-day included retention. You have the flexibility to change your pricing tier any time after the first 31 days of commitment. Learn more about Azure Sentinel pricing. This does not include the Azure Log Analytics price for ingesting data. Learn more about Log Analytics pricing. Adjust Retention Days Verrent tier
	Per GB 7 You can increase your workspace data retention to 90 days for free because you are an Azure Sentinel customer. Configure retention



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

≡ Microsoft Azure	
Home > Azure Sentinel	
Azure Sentinel Set	tings … unrcg5amwers'
	Pricing Settings Workspace settings >
General	 Entity behavior analytics
Overview	What is it?
🧬 Logs	Azure Sentinel user and entity behavior analytics feature transforms raw data into meaninoful insights by profiling
🌰 News & guides	leveraging machine learning capabilities in order to detect anomalous behavior and identify advanced attacks.
Threat management	Entity Behavior creates a comprehensive entity profiling by leveraging machine learning models for peer analysis organization) that's add to the anomalies contextual and behavioral insights for selected data sources. Learn mor
💼 Incidents	
🧹 Workbooks	How to enable it
Hunting	To turn on Azure Sentinel's entity behavior analytics follow these two simple steps to select the identity provider . UEBA. Learn more
Notebooks	
💞 Entity behavior	Configure UEBA
O Threat intelligence (Preview)	
Configuration	 Anomalies
Data connectors	Azure Sentinel provides a rich set of behavior analytics to detect anomalous activities in your environment. These Anomalies table in your workspace. You can use them in scheduled analytics (detection) rule queries, hunting que
onalytics	also customize the parameters of the machine learning (ML) models to improve the precision of the anomalies. N active data to train the ML models. This data is cached and encrypted with Microsoft keys regardless of the custo
💿 Watchlist	
🐞 Automation	Only a Global Administrator or a Security Administrator in your Azure Active Directory can turn this fee
Solutions (Preview)	Off ① UEBA anomalies will be enabled after selecting data sources for UEBA
👛 Community	Go to analytics in order to configure the anomalies>
Settings	 Playbook permissions
	✓ How do we use your data?
C	Remove Azure Sentinel



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

≡ Microsoft Azure			
Home > Azure Sentinel			
Azure Sentinel Settings Selected workspace: 'armsentinelv1uat2lunrcg5amwers'			
Pricing Setting	s Workspace settings >		
			₽ Search resources, se
Home > Azure Sentinel >			
armsentinelv1uat2lunrcg5amwers 🖈 …			
P Search (Ctrl+/) « Delete			
Overview A Essentials			
Activity log Resource group (change) : armsentinelv1uat2			
Access control (IAM) Status : Active			
Tags Location : East US			
Diagnose and solve problems Subscription (change) : Microsoft Azure			
Subscription ID : 80115be8-23dd-4136-91	81-965000078853		
Tags (change) : Click here to add tags			
Get started with Log Analytics			
Agents configuration Log Analytics collects data from a variety of sources al	nd uses a powerful query language to		
give you insights into the operation of your applicatio access the complete set of tools for monitoring all of t	ns and resources. Use Azure Monitor to vour Azure resources.		
Computer Groups		• • • • • • •	
Linked storage accounts	2 Configure monitoring solutions	Monitor workspace health	Useful links
Select one or more data sources to connect to the workspace	Add monitoring solutions that provide insights for applications	Create alerts to proactivley detect any issue that arise in your	Documentation site Community
Advanced settings	and services in your environment	workspace	
General Azure Activity logs		commore	
Storage account log System Center Operations Manager			
Workbooks			
P Logs Maximize your Log Analytics experi	ience		
P Solutions	Manager	• Marca 1 - 1	
Usage and estimated costs	Notify or take action in response	Manage usage and costs Inderstand your usage of Log	Create and Share Workbooks
Properties language to analyze logs	to important information in your	Analytics and estimate your costs	interactive reports with your data
Service Map View logs	Set alerts	Manage costs	Create Workbooks
Workspace Data Sources			
Virtual machines			
Storage accounts logs			
System Center			
 Antonio a statistica func 			



1. Navigate to your Recovery Services Vault and Select 'Diagnostic Settings' under the Alerts section.

Select 'Add diagnostic setting.'

Home > apcvault						
apcvault Diagno	ostic settings 👒 …					×
₽ Search (Ctrl+/)	« 🕐 Refresh 🛇 Feedback					
🧳 Site Recovery	Diagnostic settings are used to independent destinations. Lear	configure streaming export of platform k	ogs and metrics for a resource to th	e destination of your choice. You may create u	up to five different diagnostic s	ettings to send different logs and metrics to
Protected items	Diagnostic settings					
Backup items	Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
Replicated items	No diagnostic settings de	fined				
Manage	+ Add diagnostic setting					
Backup policies	Click 'Add Diagnostic setting' a	bove to configure the collection of the fo	lowing data:			
Backup Infrastructure	 AzureBackupReport 					
Site Recovery infrastructure	 CoreAzureBackup AddonAzureBackupJobs 					
Recovery Plans (Site Recovery)	AddonAzureBackupAler AddonAzureBackupPoli	ts =v				
M Backup Reports	AddonAzureBackupStor AddonAzureBackupProt	age ectedInstance				
Monitoring	AzureSiteRecoveryJobs AzureSiteRecoveryEvent	s				
Alerts	 AzureSiteRecoveryReplin AzureSiteRecoveryReplin 	catedItems cationStats				
Diagnostic settings	AzursitelecoveryRecoveryPerints AzursitelecoveryRecoveryPerints					
🧬 Logs	AzureSiteRecoveryProte	ctedDiskDataChurn				
≝ Backup Jobs						

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'.

Home > apcvault >							
Diagnostic setting							
Save X Discard 🖻 Delete 🗢 Feedback							
A diagnostic setting specifies a list of categories of platform logs and/or destinations that you would stream them to. Normal usage charges for th categories and contents of those logs	metrics that you want to collect from a resource, and one or more e destination will occur. Learn more about the different log						
Diagnostic setting name * backupdiag	✓						
Category details	Destination details						
log	Send to Log Analytics workspace						
AzuraBackunReport							
	Subscription						
CoreAzureBackup	Lon Analutirs worksnare						
AddonAzureBackupJobs	backupmonitor-fnqc7uwjg54mo (eastus)						
	Destination table (i)						
AddonAzureBackupAlerts	Azure diagnostics Resource specific						
AddonAzureBackupPolicy	You need to create separate diagnostic settings for Azure Backup and Azure Site Recovery events to prevent potential data loss. For Azure Backup events, if						
✓ AddonAzureBackupStorage	you choose the 'assource specific mode, you must select the tolowing events only - CoreAzur@sakup, AddonAzur@sakuplobs, AddonAzur@sakupAlerts, AddonAzur@sakupPolicy, AddonAzur@sakupStorage. AddanAzur@sakupPolicy.						
AddonAzureBackupProtectedInstance	and in Azure diagnostics' mode. Learn more						
✓ AzureSiteRecoveryJobs	Archive to a storage account						
AzureSiteRecoveryEvents							
AzureSiteRecoveryReplicateditems Send to partner solution							

C TD SYNNEX

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.

Home > Resource groups > TC-AZBack	upV3-AntiRansomware > pmonitor-fnqo	:7uwjg54mo]				×
ア þearch (Ctrl+/) 《	📋 Delete					
III Overview	Certain Contract C					JSON View
Activity log					: AzureBackup[backupmonitor-fnqc7uwjg54mo]	
Access control (IAM)		: East US			: Microsoft.OperationsManagement/solutions	
Diagnose and solve problems				Workspace Name		
🧬 Summary	Subscription ID	: 80115be8-23dd-4136-918f-965b0b078853		Management service		
Settings						
💾 Locks						
General						
Workbooks						
Log Analytics Workspace						
11 Properties			View Sum	imary		
Workspace Data Sources						
Virtual machines						
Azure Activity log						

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 <u>here</u>.

(TC-AZBackupV3-A Resource group	ntiRansomware 🖉 ···			×
₽ Search (Ctrl+/) «	+ Create 🗸 📰 Edit columns 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 😤 Open	query $\mid \oslash $ Assign tags $ ightarrow $ Move $ \checkmark $ $$ $$ $$ $$		🖓 Feedback 🛛 …
Overview				JSON View
Activity log	Subscription (change) : Microsoft Azure	Deployments: 2 Succeeded		
Access control (IAM)	Subscription ID : 80115be8-23dd-4136-918f-965b0b078853	Location : East US		
🗳 Tags	Tags (change) : Click here to add tags			
🗲 Events	Filter for any field Type == all X Location == all X + Add filter			
Settings	Showing 1 to 5 of 5 records.		No grouping \checkmark	List view 🗸
Deployments	□ Name ↑↓	Туре ↑↓	Location $\uparrow \downarrow$	
Security	n in the second se	Recovery Services vault	East US	
Policies	atostoragefnac?uwig54mo	- Storage account	East US	
😂 Properties	AzureBackup[backupmonitor-fngc7uwid54mo]	Solution	East US	
🔒 Locks	Backupmonitor-fngc7uwjg54mo	Log Analytics workspace	East US	
Cost Management	🗧 💡 fnqc7uwjg54mo-KV	Key vault	East US	
Section Cost analysis				
Cost alerts (preview)				

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, <u>click here</u>**.