**Defender for Cloud at Scale Deployment**

**with Azure Policy**

Contents

[Overview 1](#_Toc133988894)

[Defender for Cloud – Required 1](#_Toc133988895)

[Defender for Cloud – Service Layer 1](#_Toc133988896)

[Defender for CSPM 1](#_Toc133988897)

[Defender for Containers 1](#_Toc133988898)

[Defender for Databases 1](#_Toc133988899)

[Defender for Servers 1](#_Toc133988900)

[Current Limitations 1](#_Toc133988901)

[Deployment Settings Guide 1](#_Toc133988902)

[Azure Arc 1](#_Toc133988903)

[Core Policies 1](#_Toc133988904)

[Default Workspace 1](#_Toc133988905)

[Custom Workspace 1](#_Toc133988906)

[File Integrity Monitoring 1](#_Toc133988907)

[VMSS 1](#_Toc133988908)

[Continuous Export 1](#_Toc133988909)

[Integrations 1](#_Toc133988910)

[Sentinel 1](#_Toc133988911)

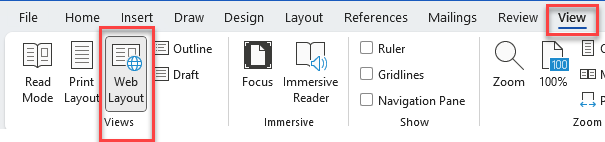
[Defender for Cloud Apps 1](#_Toc133988912)

# Overview

The intent of this guide is to provide details on how to use Azure Policy to fully enable Defender for Cloud at scale. You can use the policies below at the management group or subscription level.

***Settings in the Defender for Cloud Portal may not always reflect the state of what is configured with Azure Policy***

This guide is viewed best with the Desktop Version of Word and Web Layout Selected



# Defender for Cloud – Required

This is required for all things to work with Defender for Cloud including the free security posture management features. The recommendation is to enable this on the Root Management group.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Component** | **Deployment Scope** | **Method** | **Method Link** | **Notes** |
| Microsoft.Security Resource Provider | Subscription or Management Group | CLI, Portal | [Azure CLI](https://learn.microsoft.com/en-us/azure/defender-for-cloud/onboard-management-group#prerequisites) | Registers the Microsoft.Security Resource Provider |
| Azure Security Benchmark | Subscription or Management Group | Azure Policy | [Azure Security Benchmark](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F1f3afdf9-d0c9-4c3d-847f-89da613e70a8/scopes~) | Assigment Name must be **Azure Security Benchmark** |
| Email notifications (Optional) | Subscription or Management Group | Azure Policy | [Azure Policy](https://github.com/Azure/Microsoft-Defender-for-Cloud/blob/main/Pricing%20%26%20Settings/Azure%20Policy%20definitions/MDC%20email%20contact/MDCEmailContact-deployIfNotExists.json) | Configures email notifications for alerts |

# Defender for Cloud – Service Layer

|  |  |  |
| --- | --- | --- |
| **Policy Name** | **Type** | **Notes** |
| [[Preview]: Microsoft Defender for APIs should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F7926a6d1-b268-4586-8197-e8ae90c877d7) | Builtin | Private Preview Feature for Azure API Gateways |
| [Configure Azure Defender for DNS to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F2370a3c1-4a25-4283-a91a-c9c1a145fb2f) | Builtin |  |
| [Configure Azure Defender for Key Vaults to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F1f725891-01c0-420a-9059-4fa46cb770b7) | Builtin |  |
| [Configure Azure Defender for Resource Manager to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fb7021b2b-08fd-4dc0-9de7-3c6ece09faf9) | Builtin |  |
| [Configure Azure Defender for App Service to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fb40e7bcd-a1e5-47fe-b9cf-2f534d0bfb7d) | Builtin |  |
| [Configure Microsoft Defender for Storage to be enabled (per-storage account plan)](https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Policy/Enable%20Defender%20for%20Storage%20-%20Per-Storage%20Account%20Pricing%20Plan) | Custom |  |

# Defender for CSPM

|  |  |  |
| --- | --- | --- |
| **Policy Name** | **Type** | **Notes** |
| [Configure Microsoft Defender CSPM to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F689f7782-ef2c-4270-a6d0-7664869076bd) | Builtin |  |
| [Enable Defender for Cloud agentless scanning for machines](https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Pricing%20%26%20Settings/Azure%20Policy%20definitions/Servers%20agentless%20scanning) | Custom | Optional |

# Defender for Containers

* The assignment names must match the following. This will ensure the settings in the portal are reflected correctly.

|  |  |  |
| --- | --- | --- |
| **Policy Name** | **Assignment Name** | **Notes** |
| [Configure Microsoft Defender for Containers to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fc9ddb292-b203-4738-aead-18e2716e858f) | Configure Microsoft Defender for Containers to be enabled | Required, Enables the pricing plan |
| [Configure Azure Kubernetes Service clusters to enable Defender profile](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F64def556-fbad-4622-930e-72d1d5589bf5) | Defender for Containers provisioning AKS Security Profile | Required, you need to specify a workspace with this policy |
| [[Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F708b60a6-d253-4fe0-9114-4be4c00f012c) | Defender for Containers provisioning ARC k8s Enabled | Required, you need to specify a workspace with this policy |
| [Deploy Azure Policy Add-on to Azure Kubernetes Service clusters](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fa8eff44f-8c92-45c3-a3fb-9880802d67a7) | Defender for Containers provisioning Azure Policy Addon for Kub | Optional if you want to use Gatekeeper v3, please read [Kubernetes data plane hardening | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/kubernetes-workload-protections) |
| [Configure Azure Arc enabled Kubernetes clusters to install the Azure Policy extension](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F0adc5395-9169-4b9b-8687-af838d69410a) | Defender for Containers provisioning Policy extension for Arc-e | Optional if you want to use Gatekeeper v3, please read [Kubernetes data plane hardening | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/kubernetes-workload-protections) |

# Defender for Databases

* **The assignment names must match the following**. This will ensure the settings in the portal are reflected correctly.
* You need to enable Defender for SQL manually on the log analytics workspace(s) if using a custom workspace - [Custom workspaces](https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace#custom-workspaces)
* There are no policies currently that will configure Defender for SQL on Azure ARC servers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy Name** | **Type** | **Database Type** | **Assignment Name** | **Notes** |
| [Configure Microsoft Defender for Databases to be enabled](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F9d46421d-1a48-4636-8d1a-5525ed29172d/scopes~) | Builtin | All | Configure Microsoft Defender for Databases to be enabled | Enables the pricing plan for all database types |
| [Configure Azure Defender for Azure SQL database to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fb99b73e7-074b-4089-9395-b7236f094491) | Builtin | Azure SQL Databases | Configure Azure Defender for Azure SQL database to be enabled | Enables the pricing plan |
| [Configure Azure Defender to be enabled on SQL Servers and SQL Managed Instances](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F9cb3cc7a-b39b-4b82-bc89-e5a5d9ff7b97/scopes~) | Builtin | Azure SQL Databases | ASC DataProtection | Configure resources |
| [Configure SQL servers to have auditing enabled to Log Analytics workspace](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F25da7dfb-0666-4a15-a8f5-402127efd8bb) | Builtin | Azure SQL Databases | Configure SQL servers to have auditing enabled to Log Analytics workspace | Optional – [Configures SQL Auditing](https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?view=azuresql) for additional context during investigation |
| [Configure Azure Defender for open-source relational databases to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F44433aa3-7ec2-4002-93ea-65c65ff0310a) | Builtin | Open-source relational databases | Configure Azure Defender for open-source relational databases to be enabled | Enables the pricing plan |
| [Configure Advanced Threat Protection to be enabled on open-source relational databases](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2Fe77fc0b3-f7e9-4c58-bc13-cb753ed8e46e/scopes~) | Builtin | Open-source relational databases | ASC OpenSourceRelationalDatabasesProtection | Configure resources |
| [Configure Microsoft Defender for Azure Cosmos DB to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F82bf5b87-728b-4a74-ba4d-6123845cf542) | Builtin | Azure Cosmos DB | Configure Microsoft Defender for Azure Cosmos DB to be enabled |  |
| [Configure Azure Defender for SQL servers on machines to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F50ea7265-7d8c-429e-9a7d-ca1f410191c3) | Builtin | SQL servers on machines | Configure Azure Defender for SQL servers on machines to be enabled | Enables the pricing plan |
| [[Preview]: Configure Azure Defender for SQL agents on virtual machines](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F39a366e6-fdde-4f41-bbf8-3757f46d1611/scopes~) | Builtin | SQL servers on machines | Configure Defender for SQL Security Agent on VMs | Configure resources |

#### Enabling Defender for SQL on the workspace

After you deployed the above policy, you need to enable Defender for SQL on the log analytics workspace if using a custom workspace.

1. Navigate to the Defender for Cloud Portal > Environment Settings
2. Select your log analytics workspace under the Subscription where it resides.
3. Enable the SQL servers on machines Plan on the workspace  
     
   Graphical user interface, text, application, email

   Description automatically generated

# Defender for Servers

## Current Limitations

* Cannot mix P1 and P2 Plans on a single subscription.
* Does not support proxy settings during installation with agents. (Although possible with custom policies that currently do not exist today)
* Currently there are no custom or built-in policies to support VMSS for Defender for Servers.
* You need to enable Defender for Servers manually on the log analytics workspace(s) if using P2 and using a custom workspace - [Custom workspaces](https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace#custom-workspaces)

## Deployment Settings Guide

* The assignment names must match the below if the name required column is Yes. This will ensure the settings in the portal are reflected correctly.
* The Azure Security Agent, Azure Monitor Agent policies are only needed for Defender for Servers P2
* You do not necessarily need to assign the Defender for Endpoint Agent policy, enabling the Defender for Endpoint Integration settings will auto-provision the agent as well. However, this can take longer than policy for new machines.
* You need to choose either the Qualys Vulnerability Agent or Defender Vulnerability Management (TVM). We generally recommend using Defender Vulnerability Management as this has more vulnerability management features than Qualys.
  + With Defender for Servers P2 you also receive the full Defender Vulnerability Management listed here - [Compare Microsoft Defender Vulnerability Management plans and capabilities | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management-capabilities?view=o365-worldwide#vulnerability-management-capabilities-for-servers)
  + If you are already own Qualys or Rapid 7 do not enable these policies and follow the integration instructions here - [BYOL VM vulnerability assessment in Microsoft Defender for Cloud | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-byol-vm)

### Azure Arc

* For AWS and GCP you can enable automatic provisioning of the Azure Arc Agent with the cloud connector integration
  + [Connect your AWS account to Microsoft Defender for Cloud | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings#prerequisites)
  + [Connect your GCP project to Microsoft Defender for Cloud | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp?pivots=env-settings#configure-the-servers-plan)
* For all other environments or if you want to manually deploy Azure Arc see [Plan and deploy Azure Arc-enabled servers - Azure Arc | Microsoft Learn](https://learn.microsoft.com/en-us/azure/azure-arc/servers/plan-at-scale-deployment)

### Core Policies

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Component** | **Plan Type** | **Policy Name** | **Effect** | **Type** | **Assignment Name** | **Name Required** | **Parameters** |
| Defender for Servers | P1 or P2 | [Configure Azure Defender for servers to be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F8e86a5b6-b9bd-49d1-8e21-4bb8a0862222) | Enables Defender for Servers Pricing | BuiltIn | Configure Defender for servers to be enabled | No | N/A |
| Defender for Servers Plan | P1 or P2 | [Enable Microsoft Defender for Servers plans](https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Policy/Enable%20Defender%20for%20Servers%20plans) | Configures the P1 or P2 Plan | Custom | Configure Defender for Servers Plan | No | SubPlan: P1 or P2 |
| Defender for Endpoint Integration | P1 or P2 | [Enable Defender for Endpoint Integration](https://github.com/Azure/Microsoft-Defender-for-Cloud/blob/main/Pricing%20%26%20Settings/Azure%20Policy%20definitions/Enable%20integrations/AscMDEIntegration-deployIfNotExists.json) | Configures Defender for Endpoint Integration with Defender 365 | Custom | Enable Defender for Endpoint Integration | No | N/A |
| Qualys Vulnerability Agent | P2 | [Configure machines to receive a vulnerability assessment provider](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F13ce0167-8ca6-4048-8e6b-f996402e3c1b) | Configures **Qualys** as a vulnerability assessment provider | BuiltIn | ASC auto provisioning of vulnerability assessment agent for mac | Yes | Vulnerability assessment provider type: default |
| TVM Vulnerability Agent | P1 or P2 | [Configure machines to receive a vulnerability assessment provider](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F13ce0167-8ca6-4048-8e6b-f996402e3c1b) | Configures **Defender** Vulnerability Management as a vulnerability assessment provider | BuiltIn | ASC auto provisioning of vulnerability assessment agent for tvm | No | Vulnerability assessment provider type: mdeTvm |
| Defender for Endpoint Agent | P1 or P2 | [[Preview]: Deploy Microsoft Defender for Endpoint agent](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2Fe20d08c5-6d64-656d-6465-ce9e37fd0ebc/scopes/) | Deploys the Defender for Endpoint Agent | BuiltIn | Deploy Microsoft Defender for Endpoint agent | No | N/A |
| Guest Configuration | P2 | [Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F385f5831-96d4-41db-9a3c-cd3af78aaae6)  [Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F331e8ea8-378a-410f-a2e5-ae22f38bb0da)  [Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F3cf2ab00-13f1-4d0c-8971-2ac904541a7e)  [Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F497dff13-db2a-4c0f-8603-28fa3b331ab6) | Deploys the Guest Configuration Agent (All four required) | BuiltIn | ASC provisioning Guest Configuration agent for Windows  ASC provisioning Guest Configuration agent for Linux  ASC provisioning machines with no MI for GC agent  ASC provisioning machines with user assigned MI for GC agent | Yes | N/A |
| Agentless Scanning (Optional) | P2 | [Enable Defender for Cloud agentless scanning for machines](https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Pricing%20%26%20Settings/Azure%20Policy%20definitions/Servers%20agentless%20scanning) | Enables the agentless scanning features | Custom | Enable Defender for Cloud agentless scanning for machines | No | Exclusion Tags: key-value pairs of tags to exclude virtual machines |

### Default Workspace

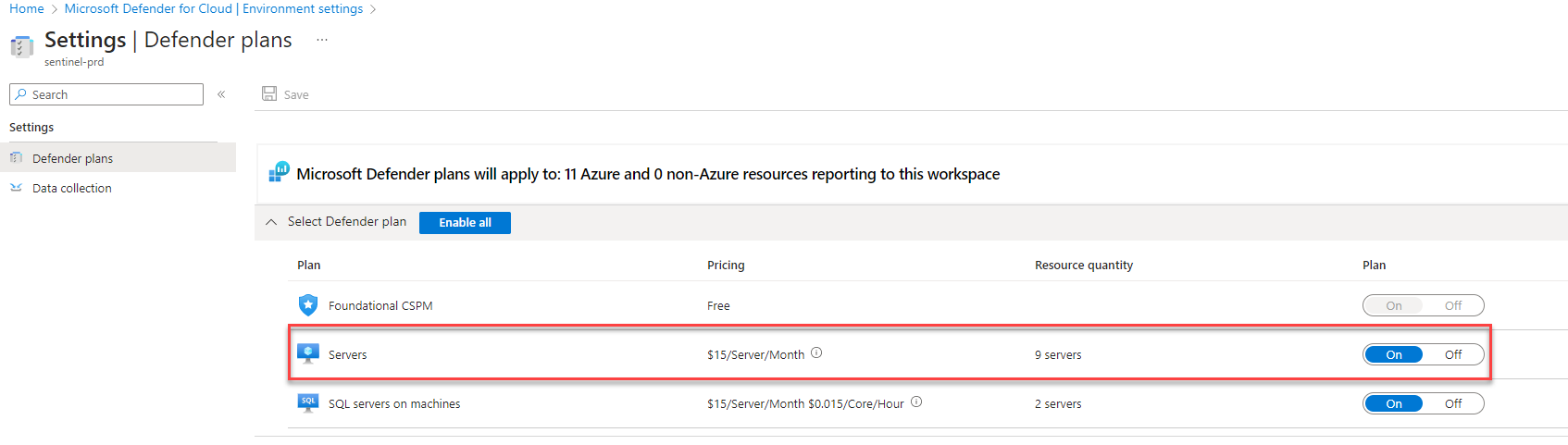
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Component** | **Plan Type** | **Policy Name** | **Effect** | **Type** | **Assignment Name** | **Name Required** | **Parameters** |
| Azure Security Agent, Azure Monitor Agent | P2 | [[Preview]: Configure machines to create the default Microsoft Defender for Cloud pipeline using Azure Monitor Agent](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F362ab02d-c362-417e-a525-45805d58e21d/scopes~/) | Deploys the Azure Monitor Agent and Azure Security Agent with the **default** workspace **(Required for P2)** | BuiltIn | Default Defender for Cloud provisioning Azure Monitor agent | Yes | N/A |

### Custom Workspace

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Component** | **Plan Type** | **Policy Name** | **Effect** | **Type** | **Assignment Name** | **Name Required** | **Parameters** |
| Azure Security Agent, Azure Monitor Agent | P2 | [[Preview]: Configure machines to create the user-defined Microsoft Defender for Cloud pipeline using Azure Monitor Agent](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F500ab3a2-f1bd-4a5a-8e47-3e09d9a294c3/scopes/) | Deploys the Azure Monitor Agent and Azure Security Agent with a **custom** workspace **(Required for P2)** | BuiltIn | Custom Defender for Cloud provisioning Azure Monitor agent | Yes | Workspace Resource Id: Centralize Log Analytics Workspace |

#### Enabling Defender for Servers on the workspace

After you deployed the above policy you need to enable Defender for Servers on the log analytics workspace.

1. Navigate to the Defender for Cloud Portal > Environment Settings
2. Select your log analytics workspace under the Subscription where it resides
3. Enable the Servers Plan on the workspace  
     
   

## File Integrity Monitoring

1. Run through the steps outline in [Enable File Integrity Monitoring (Azure Monitor Agent) | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-enable-ama) to enable the Azure Monitor Agent FIM Data Collection Rule
2. Next find the associated Data Collection Rule under Azure Monitor - [Monitor - Microsoft Azure](https://portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/dataCollectionRules). It should start with **Microsoft-ChangeTracking.** Get the full resource id from the data collection rule by clicking JSON view under the DCR.   
     
   
3. Next assign the following Azure Policies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy Name** | **Type** | **Assignment Name** | **Name Required** | **Parameters** |
| [[Preview]: Enable ChangeTracking and Inventory for Arc-enabled virtual machines](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F53448c70-089b-4f52-8f38-89196d7f2de1/scopes~/) | BuiltIn | Configure Arc-enabled machines for FIM | No | DCR Resource ID |
| [[Preview]: Enable ChangeTracking and Inventory for virtual machines](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2F92a36f05-ebc9-4bba-9128-b47ad2ea3354/scopes~/) | BuiltIn | Configure VMs machines for FIM | No | DCR Resource ID |
| [[Preview]: Enable ChangeTracking and Inventory for virtual machine scale sets](https://portal.azure.com/#view/Microsoft_Azure_Policy/InitiativeDetailBlade/id/%2Fproviders%2FMicrosoft.Authorization%2FpolicySetDefinitions%2Fc4a70814-96be-461c-889f-2b27429120dc/scopes~/) | BuiltIn | Configure VMSS machines for FIM | No | DCR Resource ID |

## VMSS

TBD – need to create custom policies.

# Continuous Export

Continuous export can be used to export data to an Azure Event Hub or Azure Log Analytics Workspace. An Azure Log Analytics workspace is required for some of the Defender for Cloud Workbooks. If you are running Microsoft Sentinel we recommend you export data to the Sentinel workspace.

If you are exporting data to your Sentinel Workspace, you do not need to enable continuous export for Security alerts. Please refer to the Sentinel Integration Section Below for alert integration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy Name** | **Type** | **Assignment Name** | **Name Required** | **Parameters** |
| [Deploy export to Log Analytics workspace for Microsoft Defender for Cloud data](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fffb6f416-7bd2-4488-8828-56585fef2be9) | BuiltIn | Deploy export to Log Analytics workspace for Microsoft Defender for Cloud data | No | There are many parameters in this policy make sure to uncheck the **Only show parameters that need input or review** |
| [Deploy export to Event Hub for Microsoft Defender for Cloud data](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fcdfcce10-4578-4ecd-9703-530938e4abcb) | BuiltIn | Deploy export to Event Hub for Microsoft Defender for Cloud data | No | There are many parameters in this policy make sure to uncheck the **Only show parameters that need input or review** |

# Integrations

## Sentinel

Using Azure Policy to enable the Sentinel data connection is not supported. To ensure all subscriptions are connected you can use the below logic app. This workflow will enable the Microsoft Defender for Cloud data connector in Microsoft Sentinel automatically for all subscriptions you have the logic app scoped to. This enables alert integration, please see below for deploying this logic app.

[Microsoft Sentinel Defender for Cloud Data Connector At Scale](https://github.com/seanstark/sentinel-tools/tree/main/enable-sentinel-mdfc-sub-con)

## Defender for Cloud Apps

Configures the Microsoft Defender for Cloud Apps Integration

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Name** | **Type** | **Assignment Name** | **Name Required** |
| [Enable Defender for Cloud Apps Integration](https://github.com/Azure/Microsoft-Defender-for-Cloud/blob/main/Pricing%20%26%20Settings/Azure%20Policy%20definitions/Enable%20integrations/AscMCASIntegration-deployIfNotExists.json) | Custom | Enable Defender for Cloud Apps Integration | No |