

# Azure security baseline for Azure Operator Service Manager - AOSM

Article • 02/25/2025

This security baseline applies guidance from the [Microsoft cloud security benchmark version 1.0](#) to Azure Operator Service Manager - AOSM. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Operator Service Manager - AOSM.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud portal page.

When a feature has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance with the Microsoft cloud security benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.

## ⓘ Note

Features not applicable to Azure Operator Service Manager - AOSM have been excluded.

## Security profile

The security profile summarizes high-impact behaviors of Azure Operator Service Manager - AOSM, which may result in increased security considerations.

[Expand table](#)

Service Behavior Attribute	Value
Product Category	DevOps, Hybrid/Multi-Cloud, Networking
Customer can access HOST / OS	No Access
Service can be deployed into customer's virtual network	True
Stores customer content at rest	False

## Network security

For more information, see the [Microsoft cloud security benchmark: Network security](#).

### NS-1: Establish network segmentation boundaries

#### Features

#### Virtual Network Integration

**Description:** Service supports deployment into customer's private Virtual Network (VNet). [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** This will change with Private Link implementation. We will update the baseline doc then.

**Configuration Guidance:** This feature is not supported to secure this service.

## NS-2: Secure cloud services with network controls

### Features

#### Azure Private Link

**Description:** Service native IP filtering capability for filtering network traffic (not to be confused with NSG or Azure Firewall). [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** Private Link is not supported at this time. This feature may be supported in the future release.

**Configuration Guidance:** This feature is not supported to secure this service.

#### Disable Public Network Access

**Description:** Service supports disabling public network access either through using service-level IP ACL filtering rule (not NSG or Azure Firewall) or using a 'Disable Public Network Access' toggle switch. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** Same as for DLP - when our work in progress to enable Private Link is done, we can attest for this feature.

**Configuration Guidance:** This feature is not supported to secure this service.

## Identity management

For more information, see the [Microsoft cloud security benchmark: Identity management](#).

### IM-3: Manage application identities securely and automatically

#### Features

#### Managed Identities

**Description:** Data plane actions support authentication using managed identities. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** Managed Identity is not required to use Azure Operator Service Manager. However, customer may be required to use a User Assigned Managed Identity and the required permissions depends on the Network Service Design (NSD).

**Configuration Guidance:** This feature is not supported to secure this service.

# Privileged access


For more information, see the [Microsoft cloud security benchmark: Privileged access](#).

## PA-7: Follow just enough administration (least privilege) principle

### Features

#### Azure RBAC for Data Plane

**Description:** Azure Role-Based Access Control (Azure RBAC) can be used to managed access to service's data plane actions. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Customer may create custom roles providing necessary permissions to access Azure Operator Service Manager.

**Configuration Guidance:** There is no current Microsoft guidance for this feature configuration. Please review and determine if your organization wants to configure this security feature.

**Reference:** [Create a custom role](#)

# PA-8: Determine access process for cloud provider support

## Features

### Customer Lockbox

Description: Customer Lockbox can be used for Microsoft support access. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: Customer Lockbox is not supported at this time. This feature may be supported in future releases.

Configuration Guidance: This feature is not supported to secure this service.

## Data protection


For more information, see the [Microsoft cloud security benchmark: Data protection](#).

# DP-1: Discover, classify, and label sensitive data

## Features

### Sensitive Data Discovery and Classification

**Description:** Tools (such as Azure Purview or Azure Information Protection) can be used for data discovery and classification in the service. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable


**Configuration Guidance:** This feature is not supported to secure this service.

## DP-2: Monitor anomalies and threats targeting sensitive data

### Features

#### Data Leakage/Loss Prevention

**Description:** Service supports DLP solution to monitor sensitive data movement (in customer's content). [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** We have work in progress to enable Private Link for customers on our service. The baseline doc needs to be updated once that work is complete.


**Configuration Guidance:** This feature is not supported to secure this service.

# DP-3: Encrypt sensitive data in transit

## Features

### Data in Transit Encryption

**Description:** Service supports data in-transit encryption for data plane. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft


**Configuration Guidance:** No additional configurations are required as this is enabled on a default deployment.

# DP-4: Enable data at rest encryption by default

## Features

### Data at Rest Encryption Using Platform Keys

**Description:** Data at-rest encryption using platform keys is supported, any customer content at rest is encrypted with these Microsoft managed keys. [Learn more.](#)

 Expand table



Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

**Configuration Guidance:** No additional configurations are required as this is enabled on a default deployment.

# DP-5: Use customer-managed key option in data at rest encryption when required

## Features

### Data at Rest Encryption Using CMK

**Description:** Data at-rest encryption using customer-managed keys is supported for customer content stored by the service. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** Encrypting data at rest using CMK is not supported at this time. This feature may be supported for encryption of binary files within customer tenant in future release.

**Configuration Guidance:** This feature is not supported to secure this service.

# DP-6: Use a secure key management process

## Features

### Key Management in Azure Key Vault

**Description:** The service supports Azure Key Vault integration for any customer keys, secrets, or certificates. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

**Feature notes:** Azure Key Vault is not required to use Azure Operator Manager Service. However, customers may use Azure Key Vault to securely manage the keys for workloads deployed through Azure Operator Manager Service.

**Configuration Guidance:** No additional configurations are required as this is enabled on a default deployment.

## Asset management

For more information, see the [Microsoft cloud security benchmark: Asset management](#).

### AM-2: Use only approved services

## Features

### Azure Policy Support

**Description:** Service configurations can be monitored and enforced via Azure Policy. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Feature notes:** The feature is supported, but there is no testing or customer facing documentation available at this moment.

**Configuration Guidance:** This feature is not supported to secure this service.

## Logging and threat detection

For more information, see the [Microsoft cloud security benchmark: Logging and threat detection](#).

### LT-1: Enable threat detection capabilities

#### Features

##### Microsoft Defender for Service / Product Offering

**Description:** Service has an offering-specific Microsoft Defender solution to monitor and alert on security issues. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable


**Configuration Guidance:** This feature is not supported to secure this service.

# LT-4: Enable logging for security investigation

## Features

### Azure Resource Logs

**Description:** Service produces resource logs that can provide enhanced service-specific metrics and logging. The customer can configure these resource logs and send them to their own data sink like a storage account or log analytics workspace. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

**Configuration Guidance:** This feature is not supported to secure this service.

## Next steps

- See the [Microsoft cloud security benchmark overview](#)
- Learn more about [Azure security baselines](#)