

# Azure security baseline for Azure Dedicated HSM

Article • 02/25/2025

This security baseline applies guidance from the [Microsoft cloud security benchmark version 1.0](#) to Azure Dedicated HSM. 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 Dedicated HSM.

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 Dedicated HSM have been excluded. To see how Azure Dedicated HSM completely maps to the Microsoft cloud security benchmark, see the [full Azure Dedicated HSM security baseline mapping file](#) .

## Security profile

The security profile summarizes high-impact behaviors of Azure Dedicated HSM, which may result in increased security considerations.

[Expand table](#)

| Service Behavior Attribute                              | Value     |
|---|-----------|
| Product Category  | Security  |
| Customer can access HOST / OS                           | No Access |
| Service can be deployed into customer's virtual network | True      |
| Stores customer content at rest                         | True      |

# 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 |
|-----------|--------------------|------------------------------|
| True      | True               | Microsoft                    |

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

Reference: [Deploying HSMs into an existing virtual network using the Azure CLI](#)

## Network Security Group Support

Description: Service network traffic respects Network Security Groups rule assignment on its subnets. [Learn more.](#)

 Expand table

| Supported | Enabled By Default | Configuration Responsibility |
|-----------|--------------------|------------------------------|
| False     | Not Applicable     | Not Applicable               |

**Feature notes:** Though Azure Dedicated HSM does not support this feature, alternative networking restrictions are available. For more information, please visit [Networking Restrictions](#).

**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               |

**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               |

**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-1: Use centralized identity and authentication system

### Features

#### Azure AD Authentication Required for Data Plane Access

**Description:** Service supports using Azure AD authentication for data plane access. [Learn more.](#)

 **Expand table**


| Supported | Enabled By Default | Configuration Responsibility |
|-----------|--------------------|------------------------------|
| False     | Not Applicable     | Not Applicable               |

**Feature notes:** Please visit Thales documentation for information relating to this feature: [DHSM Docs](#); [Thales Docs](#)

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

## Local Authentication Methods for Data Plane Access

**Description:** Local authentications methods supported for data plane access, such as a local username and password. [Learn more.](#)

 **Expand table**

| Supported | Enabled By Default | Configuration Responsibility |
|-----------|--------------------|------------------------------|
| True      | False              | Customer                     |

**Feature notes:** Avoid the usage of local authentication methods or accounts, these should be disabled wherever possible. Instead use Azure AD to authenticate where possible.

**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:** [Authentication](#)

# Privileged access

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

## PA-1: Separate and limit highly privileged/administrative users

### Features

#### Local Admin Accounts

**Description:** Service has the concept of a local administrative account. [Learn more](#).

 Expand table

| Supported | Enabled By Default | Configuration Responsibility |
|-----------|--------------------|------------------------------|
| True      | True               | Microsoft                    |

**Feature notes:** Azure Dedicated HSM is a HSM for lease services. All setup and configuration documentation can be found in Thales vendor documentation.

For more information, please visit [Thales Product Overview - Password Authentication](#) Avoid the usage of local authentication methods or accounts, these should be disabled wherever possible. Instead use Azure AD to authenticate where possible.

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

## Data protection


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

# 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                    |

Feature notes: Please see Thales vendor documentation regarding use of secure transport channel.

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

## Next steps

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