

# Azure security baseline for Azure DevTest Labs

Article • 02/25/2025

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

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

## Security profile

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

[Expand table](#)

Service Behavior Attribute	Value
Product Category	Compute, Developer Tools, Integration
Customer can access HOST / OS	Full 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
True	True	Microsoft

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

Reference: [Configure a virtual network for DevTest Labs](#)

## 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
True	False	Customer


**Configuration Guidance:** Use network security groups (NSG) to restrict or monitor traffic by port, protocol, source IP address, or destination IP address. Create NSG rules to restrict your service's open ports (such as preventing management ports from being accessed from untrusted networks). Be aware that by default, NSGs deny all inbound traffic but allow traffic from virtual network and Azure Load Balancers.

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

### Features

#### 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
True	False	Customer

**Configuration Guidance:** Disable public network access either using the service-level IP ACL filtering rule or a toggling switch for public network access.

Reference: [Create network-isolated DevTest Labs](#)

# 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
True	False	Customer

**Feature notes:** Azure DevTest Labs supports managed identities for its Azure resources as well as secrets management through key vault. DevTest Labs can natively use Azure AD authentication for Azure services and resources that support it. This is supported either from the Azure Portal, using the SDKs or our REST API, when the user interacts or creates a DevTest Lab or any of the resources supported within a Lab.

[Enable user-assigned managed identities on lab virtual machines in Azure DevTest Labs](#)

**Configuration Guidance:** Use Azure Active Directory (Azure AD) as the default authentication method to control your data plane access.

**Reference:** [Azure DevTest Labs REST API](#)

## 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	True	Microsoft

**Feature notes:** The default authentication to VMs is local authentication (RDP/SSH). 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.

## 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
True	False	Customer


**Feature notes:** Although we don't provide a Data Plane for our service, our resources support Managed Identities.

**Configuration Guidance:** Use Azure managed identities instead of service principals when possible, which can authenticate to Azure services and resources that support Azure Active Directory (Azure AD) authentication. Managed identity credentials are fully managed, rotated, and protected by the platform, avoiding hard-coded credentials in source code or configuration files.

**Reference:** [Enable user-assigned managed identities on lab virtual machines in DevTest Labs](#)

# Service Principals

**Description:** Data plane supports authentication using service principals. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Users can configure service principals by their own to access lab resources.


**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.

# IM-7: Restrict resource access based on conditions

## Features

### Conditional Access for Data Plane

Description: Data plane access can be controlled using Azure AD Conditional Access Policies. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Azure DevTest Labs allows users to manage and deploy Azure virtual machines in their own subscriptions and those virtual machines can support Conditional Access if needed, depending on the customer scenario.


**Configuration Guidance:** Define the applicable conditions and criteria for Azure Active Directory (Azure AD) conditional access in the workload. Consider common use cases such as blocking or granting access from specific locations, blocking risky sign-in behavior, or requiring organization-managed devices for specific applications.

# IM-8: Restrict the exposure of credential and secrets

## Features

### Service Credential and Secrets Support Integration and Storage in Azure Key Vault

Description: Data plane supports native use of Azure Key Vault for credential and secrets store. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** DevTest Lab secrets are securely stored in an Azure Key Vault on the customer subscription. This is used by our Service to interact with any Azure resources within the Lab.

You can enable managed identities on your Lab virtual machines as well to authenticate into resources in the context of a Lab.

**Configuration Guidance:** Ensure that secrets and credentials are stored in secure locations such as Azure Key Vault, instead of embedding them into code or configuration files.

**Reference:** [Enable user-assigned managed identities on lab virtual machines in Azure DevTest Labs](#)

## 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
False	Not Applicable	Not Applicable

**Feature notes:** Lab machine users can be Local Admin of VMs.

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

## 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:** Azure DevTest Labs has integrated Azure RBAC support for all our resources through the built-in roles.

**Configuration Guidance:** Use Azure role-based access control (Azure RBAC) to manage Azure resource access through built-in role assignments. Azure RBAC roles can be assigned to users, groups, service principals, and managed identities.

Reference: [DevTest Labs Users](#)

# 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

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

**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.

Reference: [Understand encryption in transit scenario for DevTest Labs](#)

# 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

**Feature notes:** Within DevTest Labs, all OS disks and data disks created as part of a lab are encrypted using platform-managed keys.

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

## 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	False	Customer

**Configuration Guidance:** Use Azure Key Vault to create and control the life cycle of your encryption keys, including key generation, distribution, and storage. Rotate and revoke your keys in Azure Key Vault and your service based on a defined schedule or when there is a key retirement or compromise. When there is a need to use customer-managed key (CMK) in the workload, service, or application level, ensure you follow the best practices for key management: Use a key hierarchy to generate a separate data encryption key (DEK) with your key encryption key (KEK) in your key vault. Ensure keys are registered with Azure Key Vault and

referenced via key IDs from the service or application. If you need to bring your own key (BYOK) to the service (such as importing HSM-protected keys from your on-premises HSMs into Azure Key Vault), follow recommended guidelines to perform initial key generation and key transfer.


Reference: [Store secrets in a key vault in Azure DevTest Labs](#)

## DP-7: Use a secure certificate management process

### Features

#### Certificate Management in Azure Key Vault

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

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Azure DevTest Labs allows users to manage and deploy Azure virtual machines in their own subscriptions and those virtual machines can support certificate management in an Azure Key Vault if needed, depending on the customer scenario.

**Configuration Guidance:** Use Azure Key Vault to create and control the certificate lifecycle, including creation, importing, rotation, revocation, storage, and purging of the certificate. Ensure the certificate generation follows defined standards without using any insecure properties, such as: insufficient key size, overly long validity period, insecure cryptography. Setup automatic rotation of the certificate in Azure Key Vault and the Azure service (if supported) based on a defined schedule or when there is a certificate expiration. If automatic rotation is not supported in the application, ensure they are still rotated using manual methods in Azure Key Vault and the application.

# 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
True	False	Customer

**Feature notes:** Azure Policies are supported and can be configured for the resources our service creates, but there is no explicit security policies configuration from our Service.

**Configuration Guidance:** Use Microsoft Defender for Cloud to configure Azure Policy to audit and enforce configurations of your Azure resources. Use Azure Monitor to create alerts when there is a configuration deviation detected on the resources. Use Azure Policy [deny] and [deploy if not exists] effects to enforce secure configuration across Azure resources.

## AM-5: Use only approved applications in virtual machine

## Features

### Microsoft Defender for Cloud - Adaptive Application Controls

**Description:** Service can limit what customer applications run on the virtual machine using Adaptive Application Controls in Microsoft Defender for Cloud. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Configuration Guidance:** Use Microsoft Defender for Cloud adaptive application controls to discover applications running on virtual machines (VMs) and generate an application allow list to mandate which approved applications can run in the VM environment.

## Posture and vulnerability management

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

### PV-3: Define and establish secure configurations for compute resources

## Features

### Azure Automation State Configuration



**Description:** Azure Automation State Configuration can be used to maintain the security configuration of the operating system. [Learn more.](#)

 Expand table


Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Users don't have access to DevTest Labs Service host VM, but our service allows users to manage and deploy Azure Virtual Machines in their own subscriptions and DSC (Desired State Configuration) applies for those machines.

**Configuration Guidance:** Use Azure Automation State Configuration to maintain the security configuration of the operating system.

## Azure Policy Guest Configuration Agent

**Description:** Azure Policy guest configuration agent can be installed or deployed as an extension to compute resources. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Users don't have access to DevTest Labs Service host VM, but our service allows users to manage and deploy Azure Virtual Machines in their own subscriptions and Azure Policy Guest Configuration Agent applies for those machines.

**Configuration Guidance:** Use Microsoft Defender for Cloud and Azure Policy guest configuration agent to regularly assess and remediate configuration deviations on your Azure compute resources, including VMs, containers, and others.

## Custom VM Images

**Description:** Service supports using user-supplied VM images or pre-built images from the marketplace with certain baseline configurations pre-applied. [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:** [Configure Azure Marketplace image settings in Azure DevTest Labs](#)

## PV-5: Perform vulnerability assessments

### Features

#### Vulnerability Assessment using Microsoft Defender

**Description:** Service can be scanned for vulnerability scan using Microsoft Defender for Cloud or other Microsoft Defender services embedded vulnerability assessment capability (including Microsoft Defender for server, container registry, App Service, SQL, and DNS). [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** When creating a DevTest Labs, there can be underlying compute resources as part of the lab. There are tools for vulnerability assessments, external to our service, that can be used on those resources.


**Configuration Guidance:** Follow recommendations from Microsoft Defender for Cloud for performing vulnerability assessments on your Azure virtual machines, container images, and SQL servers.

## PV-6: Rapidly and automatically remediate vulnerabilities

### Features

#### Azure Automation Update Management

**Description:** Service can use Azure Automation Update Management to deploy patches and updates automatically. [Learn more.](#)

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Users don't have access to DevTest Labs Service host VM, but our service allows users to manage and deploy Azure Virtual Machines in their own subscriptions and Automation Update Management can be managed independently for those machines.

**Configuration Guidance:** Use Azure Automation Update Management or a third-party solution to ensure that the most recent security updates are installed on your Windows and Linux VMs. For Windows VMs, ensure Windows Update has been enabled and set to update automatically.

# Endpoint security

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

## ES-2: Use modern anti-malware software

### Features

#### Anti-Malware Solution

**Description:** Anti-malware feature such as Microsoft Defender Antivirus, Microsoft Defender for Endpoint can be deployed on the endpoint. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Users don't have access to DevTest Labs Service host VM, but our service allows users to manage and deploy Azure Virtual Machines in their own subscriptions and it's strongly recommended using an Anti-Malware solution in those machines.

**Configuration Guidance:** For Windows Server 2016 and above, Microsoft Defender for Antivirus is installed by default. For Windows Server 2012 R2 and above, customers can install SCEP (System Center Endpoint Protection). For Linux, customers can have the choice of installing Microsoft Defender for Linux. Alternatively, customers also have the choice of installing third-party anti-malware products.

## ES-3: Ensure anti-malware software and signatures are updated

# Features

## Anti-Malware Solution Health Monitoring

**Description:** Anti-malware solution provides health status monitoring for platform, engine, and automatic signature updates. [Learn more](#).

 Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Users don't have access to DevTest Labs Service host VM, but our service allows users to manage and deploy Azure Virtual Machines in their own subscriptions and it's strongly recommended using an Anti-Malware Solution Health Monitoring for those machines.

**Configuration Guidance:** Configure your anti-malware solution to ensure the platform, engine and signatures are updated rapidly and consistently and their status can be monitored.

## Backup and recovery


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

### BR-1: Ensure regular automated backups

# Features

## Azure Backup

**Description:** The service can be backed up by the Azure Backup service. [Learn more](#).

 Expand table


Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

**Feature notes:** Azure DevTest Labs don't explicitly provide support for Azure Backup, but it can be configured by the customer for the Compute VMs deployed by our service.

**Configuration Guidance:** Enable Azure Backup and configure the backup source (such as Azure Virtual Machines, SQL Server, HANA databases, or File Shares) on a desired frequency and with a desired retention period. For Azure Virtual Machines, you can use Azure Policy to enable automatic backups.

## Service Native Backup Capability

**Description:** Service supports its own native backup capability (if not using Azure Backup). [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](#)