Azure security baseline for Azure Public IP

Article • 02/25/2025

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Azure Public IP. 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 Public IP.

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 Public IP have been excluded. To see how Azure Public IP completely maps to the Microsoft cloud security benchmark, see the full Azure Public IP security baseline mapping file .

Security profile

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

Expand table

Service Behavior Attribute	Value
Product Category	Networking

Service Behavior Attribute	Value
Customer can access HOST / OS	No Access
Service can be deployed into customer's virtual network	False
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	False	Customer

Configuration Guidance: Public IP addresses may be created and then later associated with a resource within a virtual network.

Microsoft Defender for Cloud monitoring

Azure Policy built-in definitions - Microsoft.Network:

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Subnets should be associated with a Network Security Group	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	3.0.0

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

Configuration Guidance: To manage public IP addresses, your account must be assigned to the network contributor role. A custom role is also supported.

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 Policy definitions may be configured relating to public IP addresses, such as requiring public IP addresses to have resource logs enabled for Azure DDoS Protection Standard.

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.

Logging and threat detection

For more information, see the Microsoft cloud security benchmark: Logging and threat detection.

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
True	False	Customer

Configuration Guidance: When you have critical applications and business processes relying on Azure resources, you want to monitor those resources for their availability, performance, and operation. Resource Logs are not collected and stored until you create a diagnostic setting and route them to one or more locations.

Reference: Monitoring Public IP addresses

Next steps

- See the Microsoft cloud security benchmark overview
- Learn more about Azure security baselines