

Microsoft Technical Reference Guide for CMMC

Accelerate your journey to cmmc with the Microsoft cloud

June 2024

[Introduction 3](#_Toc118452961)

[Notices 4](#_Toc118452962)

[Microsoft CMMC Acceleration Program 5](#_Toc118452963)

[Cybersecurity Maturity Model Certification (CMMC) 6](#_Toc118452964)

[CMMC 2.0 Implementation Guidance 6](#_Toc118452965)

[Overview of Implementation 6](#_Toc118452966)

[CMMC 2.0 NIST Alignment 7](#_Toc118452967)

[CMMC 2.0 Assessment Model 8](#_Toc118452968)

[POA&M 10](#_Toc118452969)

[CMMC Risk Assessment 10](#_Toc118452970)

[Shared Responsibility in the Microsoft Cloud 10](#_Toc118452971)

[Customer Eligibility for Azure Commercial and Azure Government 12](#_Toc118452972)

[Microsoft Services Implementation Guidance 12](#_Toc118452973)

[Microsoft Primary and Secondary Services Definition 12](#_Toc118452974)

[Azure Policy 12](#_Toc118452975)

[Microsoft Service Implementation Guidance 14](#_Toc118452976)

[Access Control (AC) 14](#_Toc118452977)

[Audit and Accountability (AU) 67](#_Toc118452978)

[Awareness and Training (AT) 87](#_Toc118452979)

[Configuration Management (CM) 91](#_Toc118452980)

[Identification and Authentication (IA) 118](#_Toc118452981)

[Incident Response (IR) 136](#_Toc118452982)

[Maintenance (MA) 144](#_Toc118452983)

[Media Protection (MP) 157](#_Toc118452984)

[Personnel Security (PS) 183](#_Toc118452985)

[Physical Protection (PE) 188](#_Toc118452986)

[Risk Assessment (RA) 192](#_Toc118452987)

[Security Assessment (CA) 202](#_Toc118452988)

[Systems and Communications Protection (SC) 213](#_Toc118452989)

[System and Information Integrity (SI) 259](#_Toc118452990)

[CMMC Blogs 280](#_Toc118452991)

[CMMC Resources 280](#_Toc118452992)

[CMMC Tools 280](#_Toc118452993)

# Introduction

The Cybersecurity Maturity Model Certification (CMMC) is a unifying standard for the implementation of cybersecurity across the United States Defense Industrial Base (DIB). The DIB encompasses the commercial organizations that produce or provide products and services to the United States Department of Defense (DoD). CMMC includes a comprehensive and scalable certification element to verify the implementation of controls associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the DoD that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

The Microsoft Technical Reference Guide for CMMC includes implementation statements for an organization pursuing CMMC, while leveraging relevant Microsoft services. This includes brief descriptions of relevant Microsoft services and products, and links to further implementation documentation. The guide focuses on CMMC Level 2 (L2). CMMC L2 includes all 110 controls from NIST SP 800-171. The intended audience are Government Personnel, Government Contractors, Managed Service Providers, Compliance Personnel, and IT Security Architects who are responsible for evaluating Microsoft services for controls alignment, and implementation to meet CMMC security requirements.

# Notices

This Technical Reference Guide for CMMC provides customers with a resource to pursue CMMC compliance while leveraging Microsoft products and services— This Guide does not address security controls occurring outside of Microsoft products and services.

Please further note that the CMMC compliance standard has yet to be implemented to assess the suitability of in-scope entities’ security controls and configurations. As a result, there may be additional nuance or complexity associated with CMMC compliance that will only materialize (if at all) through the practical application of the standard by the [CMMC Accreditation Body](https://cyberab.org/About-Us/Overview) (CYBER AB). What’s more, as of the date this Technical Reference Guide was written, The CYBER AB has not issued formal guidance for Cloud Service Providers. As a result, the information herein, including all Microsoft CMMC-related offerings, is provisional and may be enhanced to align with future guidance from the DoD and CYBER AB.

Microsoft does not guarantee nor imply any ultimate compliance outcome or determination based on one’s consumption of this Technical Reference Guide — all CMMC certification requirements and decisions are governed by the CYBER AB, and Microsoft has no direct or indirect insight into or bearing over CYBER AB compliance determinations. The associations between compliance domains, controls, and Microsoft Technical Reference Guide for CMMC may change at any time.

Customers must individually determine the necessary steps required to ensure their organization fully satisfies each recommended CMMC compliance control, in addition to or in place of what is described in this document. This responsibility spans all Microsoft (Azure, Microsoft 365, etc.) consumption decisions, including, among other things, which Microsoft offering to procure, as well as all configuration decisions associated with such use and consumption.

# Microsoft CMMC Acceleration Program

This Technical Reference Guide is provided through the Microsoft CMMC Acceleration Program. The Acceleration Program’s main objective is to help customers close known compliance gaps and mitigate risks, helping facilitate CMMC. Included with the program are a portfolio of learning resources, architectural references, and implementation tools custom-tailored to the certification journey.

[Resources](https://aka.ms/CMMCAccelerationProgramUpdate) in the Microsoft CMMC Acceleration Program include:

* Microsoft Product Placemat for CMMC
* Microsoft Sentinel: Cloud-Native SIEM
* Microsoft Sentinel: CMMC Workbook
* Microsoft Compliance Manager with Assessment Templates
* Microsoft Defender for Cloud Apps
* Azure Blueprints
* CMMC Documentation
* Blog Posts

Learn more about how Microsoft can help organizations on their CMMC journey:

* [Collections - CMMC | Microsoft Learn](https://learn.microsoft.com/en-us/users/cmmc/collections/5xwdumyyqo1710)
* [Microsoft Federal - Cybersecurity Maturity Model Certification](https://www.microsoft.com/en-us/federal/cmmc.aspx)

# Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a unified standard for implementing cybersecurity across the DIB, which includes over 300,000 commercial companies in the supply chain. The CMMC is the DoD's response to significant compromises of sensitive defense information located on contractors' information systems.

The DoD is migrating to CMMC to assess and enhance the cybersecurity posture of the DIB. CMMC is intended to serve as a verification mechanism to ensure that DIB companies implement appropriate cybersecurity NIST controls to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.

The main benefit to organizations that obtain a CMMC certification is the improvement of their processes and enhancement of the protection of controlled unclassified information and intellectual property within the supply chain of the DIB. Meeting CMMC is a signal that the company can meet the DoD's cybersecurity objectives.

To address the range of DoD contractors, CMMC comprises three levels of cybersecurity ranging from Foundational Level One to Expert security operations at Level three for highly sensitive defense assets. The CMMC levels and the associated sets of controls are cumulative. More specifically, in order for an organization to achieve a specific CMMC level it must also demonstrate achievement of the preceding lower levels. More details on the model can be found in the CMMC Model Overview document.

To learn more, see [CMMC.](https://dodcio.defense.gov/CMMC/Model/)

# CMMC 2.0 Implementation Guidance

## Overview of Implementation

CMMC program requirements will be implemented through the acquisition and contracting process. With limited exceptions for information with little national security need, the Department intends to require compliance with CMMC as a condition of contract award. The required CMMC level for contractors and sub-contractors will be specified in the solicitation and in Requests for Information (RFIs), if utilized.

## CMMC 2.0 NIST Alignment

NIST CMMC 2.0 aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards. Under CMMC 2.0, the “Advanced” level (Level 2) will be equivalent to the NIST SP 800-171. The “Expert” level (Level 3), which is currently under development, will be based on a subset of NIST SP 800-172 requirements. CMMC 2.0 practices have a unique identification number in the format – DD.L#-REQ for example, NIST 800-171 3.1.1 control would be written as AC.L1-3.1.1 for CMMC 2.0 Level 2 control. The format is meant to be used for quick reference only.

Diagram

Description automatically generatedThe US National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidelines to help protect the information and information systems of federal agencies. In response to Executive Order 13556 on managing controlled unclassified information (CUI), it published [NIST SP 800-171](https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. NIST SP 800-171 requirements are a subset of NIST SP 800-53, the standard that FedRAMP uses. Appendix D of NIST SP 800-171 provides a direct mapping of its CUI security requirements to the relevant security controls in NIST SP 800-53, for which the in-scope cloud services have already been assessed and authorized under the FedRAMP program.

Fundamentally, in order to leverage and inherit the underlying Cloud-Native controls provided by Microsoft, customers would inherit security controls that are fully audited as part of its underlying FedRAMP, mapped NIST SP 800-53 and NIST SP 800-171 controls. Accredited third-party assessment organizations, Kratos SecureInfo and Coalfire, assessed with Microsoft to attest that its in-scope cloud services meet the criteria in NIST SP 800-171, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*, when they process CUI. The [Microsoft implementation of FedRAMP](https://docs.microsoft.com/en-us/compliance/regulatory/offering-fedramp) requirements help ensure Microsoft in-scope cloud services meet or exceed the requirements of NIST SP 800-171 using the systems and controls already in place.

Any entity that processes or stores US government CUI — research institutions, consulting companies, manufacturing contractors, must comply with the stringent requirements of NIST SP 800-171. This attestation means Microsoft in-scope cloud services can accommodate customers looking to deploy CUI workloads with the assurance that Microsoft is in full compliance. For example, all DoD contractors who process, store, or transmit 'covered defense information' using in-scope Microsoft cloud services in their information systems meet the US Department of Defense DFARS clauses that require compliance with the security requirements of NIST SP 800-171.

## CMMC 2.0 Assessment Model

A CMMC assessment is the methodology to certify that a contractor is compliant with the CMMC standard. CMMC 2.0 implements tiered assessment requirements based on the sensitivity of the information shared with a contractor. Upon implementation of CMMC 2.0:

Contractors who do not handle information deemed critical to national security (Level 1 and a subset of Level 2) will be required to perform annual self-assessments against clearly articulated cybersecurity standards.

Contractors managing information critical to national security (a subset of Level 2) will be required to undergo third-party assessments.

The highest priority, most critical defense programs (Level 3) will require government-led assessments.

To learn more, see:

* [CMMC 2.0 Assessment Overview](https://dodcio.defense.gov/CMMC/Assessments/)  
  [CMMC-CyberAB Marketplace listings](https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending)

## POA&M

With the implementation of CMMC 2.0, the Department intends to allow companies to receive contract awards with a Plan of Actions and Milestones (POA&M) in place to complete CMMC requirements. The Department’s intent is to specify a baseline number of requirements that must be achieved prior to contract award, in order to allow the remaining subset to be addressed in a POA&M within a clearly defined timeline. The Department also intends to specify a small subset of requirements that cannot be on a POA&M in support of achieving a CMMC certification. Waiver requests will require senior DoD leadership approval and will have a limited duration.

## CMMC Risk Assessment

Some implementations of controls are based on categorization of data and risk. Microsoft encourages its customers to perform a thorough risk assessment for the entire environment and not rely on boundaries defined by workloads in the cloud environment.

To learn more, see:

* [NIST SP 800-30 Guide for Conducting Risk Assessments](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)
* [Risk Management section of this document](#_Risk_Management_(RM))

# Office 365 Government

CMMC L2 and higher are intended for protection of CUI. You may demonstrate compliance with CMMC Levels 1 for the data protection of FCI in Commercial and in our government clouds. Microsoft recommends the US Sovereign Cloud with Azure Government and Microsoft 365 Government (GCC High) for data protection of CUI in alignment with CMMC Levels 1-3.

The Office 365 Government - GCC High environment provides compliance with US government requirements for cloud services. In addition to enjoying the features and capabilities of Office 365, organizations benefit from the following features that are unique to Office 365 Government – GCC High:

* Your organization's customer content is logically segregated from customer content in the commercial Office 365 services from Microsoft.
* Your organization's customer content is stored within the United States.
* Access to your organization's customer content is restricted to screened Microsoft personnel.
* Office 365 Government – GCC High complies with certifications and accreditations that are required for US Public Sector customers.

You can find more information about the Office 365 Government – GCC High offering for US Government customers at:

* [Office 365 Government plans](https://products.office.com/government/compare-office-365-government-plans).
* [Understanding Compliance Between Commercial, Government and DoD Offerings.](https://techcommunity.microsoft.com/t5/public-sector-blog/understanding-compliance-between-commercial-government-and-dod/ba-p/2157679)
* [Microsoft 365 Government](https://www.microsoft.com/en-us/microsoft-365/government/#tabx4e4f6133b534476989ce4493ce452c66).
* [Eligibility requirements](https://www.microsoft.com/en-us/microsoft-365/government/compare-office-365-government-plans?rtc=1#coreui-heading-5uz6ylg).

# Shared Responsibility in the Microsoft Cloud

It is important to understand that compliance is a shared responsibility between the customer and Microsoft, the Cloud Services Provider (CSP). The graphic below shows the CSP responsibility in respective cloud models (SaaS, PaaS, IaaS, On-Prem), spanning Microsoft, Customer, and Shared responsibilities. For example, CMMC requirements such as Physical Protection (PE) for limiting physical access are managed by the CSP. For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type). The establishment of respective policies and procedures is the customer’s responsibility.

Regardless of the type of deployment, the following responsibilities are always retained by you:

* Data
* Endpoints
* Account
* Access management

Customers are advised to work with their respective C3PAO for guidance on comprehensive alignment of controls, audit and certification.

Table

Description automatically generated

For more information see, [Shared responsibility in the cloud.](https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility)

# Microsoft Services Implementation Guidance

The following family sections outline specific NIST 800-171 controls that CMMC 2.0 Level 2 requires, and services you can leverage from Microsoft to meet those Controls. This guide breaks down how customers can use these services to accelerate CMMC compliance.

## Microsoft Primary and Secondary Services Definition

Each control that has customer responsibility is mapped to a Microsoft service that can help meet the requirement. Primary services are Microsoft services that directly meet the practice objective, while the secondary services require and or support the primary service in meeting the control objective. Secondary services can also provide an additional layer of protection but might not fully meet the Control requirements.

To learn more, see [Microsoft Product Placemat for CMMC 2.0](https://aka.ms/cmmc/productplacemat)

## Azure Policy

Controls below associated with one or more Azure Policy definitions will have an Azure Policy heading and a link to the relevant NIST 800-171 R2 Azure Policy. The NIST 800-171 R2 blueprint sample provides governance guardrails using [Azure Policy](https://docs.microsoft.com/en-us/azure/governance/policy/overview) that help you assess specific CMMC L2 controls. This blueprint aids customers in deploying a core set of policies for any Azure-deployed architecture that must implement controls for CMMC L2. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time.

These policies may help you [assess compliance](https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data) with the controls implemented to meet CMMC L2 requirements; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, compliant in Azure Policy refers only to the policy definitions themselves; this does not ensure you are fully compliant with all requirements of a control.

## Microsoft Service Implementation Guidance

### Access Control (AC)

##### AC.L1-3.1.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-2, AC-3, AC-17 | |
| **Practice:** Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).  **Assessment Objectives:**  [a] authorized users are identified;  [b] processes acting on behalf of authorized users are identified;  [c] devices (and other systems) authorized to connect to the system are identified;  [d] system access is limited to authorized users;  [e] system access is limited to processes acting on behalf of authorized users; and  [f] system access is limited to authorized devices (including other systems). | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC Intune/Intune Suite | Microsoft Information Protection Conditional Access Customer Lockbox Privileged Identity Management (PIM) Microsoft 365 Web Apps M365 Groups  Microsoft Entra ID Multi-Factor Authentication |

**Implementation Statement:**

**Microsoft Entra ID**

There are a few ways of creating identities such as directly in Microsoft Entra ID or linking to an on-premises Active Directory where Microsoft Entra ID will securely authenticate the users. To learn more, see:

* [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)
* [Active Directory Federation Services (ADFS)](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs)
* [Microsoft Entra ID pass-through authentication](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta)

It is good practice to assign permissions using the principle of least privilege, this involves giving users the exact permissions they need to do their jobs properly. Users, groups, and applications are added to roles in Azure, and those roles have certain permissions. You can use the built-in roles that Azure offers, or you can create custom roles in RBAC. To learn more, see:

* [Grant user access to Azure resources using RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/quickstart-assign-role-user-portal)
* [RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/#:~:text=Azure%20role%2Dbased%20access%20control%20(Azure%20RBAC)%20is%20a,need%20to%20perform%20their%20jobs.) documentation

**Privileged Identity Management**

Additionally, you can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

With [Microsoft Entra ID PIM](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure), you can manage, control, and monitor your privileged identities and access to your directory information and resources in an Azure environment. The main reason for using Microsoft Entra ID PIM is to reduce the attack surface and to enable administrative access just-in-time. Privileged access is often configured as permanent and unmonitored, but with Microsoft Entra ID PIM you can avoid security breaches and risks.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses [Microsoft Entra ID Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks). For example, during the activation process, a user can be forced to justify why they need to activate their role. Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

Privileged Identity Management (PIM) provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

To summarize, you should complete the following Microsoft Entra ID PIM tasks for your Azure resources:

* Enable Just in Time access to Azure.
* Expire access automatically.
* Assign temporary access for quick tasks or on-call schedules.
* Get alerts when new users or groups are assigned resource access, or when eligible assignments are activated.
* Use Microsoft Entra ID sign in for Azure VMs

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Implementing Multi-Factor Authentication (MFA)**

[MFA](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks) is a security feature that requires more than one method of authentication. You can use it to add an additional layer of security to the signing in of users. It enables two-step verification, where the user first signs in using something, they know (such as a password), and then signs in with something they have (such as a smartphone), or some human characteristic (such as biometrics).

To learn more, see [Tutorial: Secure user sign-in events with Microsoft Entra ID Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa).

**Microsoft Entra ID Identity Protection**

Microsoft Entra ID Identity Protection introduces automatic, risk-based, conditional access to help protect users against suspicious logins and compromised credentials. Microsoft Entra ID Identity Protections also offers insight into, and a consolidated view of, threat detection based on machine-learning. Furthermore, the service delivers an important level of remediation recommendations, as well as performing compromise risk calculations about a user and their session.

To learn more, see:

* [What is Identity Protection?](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection)
* [Identity Protection policies](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies)

**Conditional Access**

[Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) allows you to set up access policies to prohibit a specific activity, as well as to trigger MFA according to rules that you define). It is a very powerful engine. You may target conditional access policies toward specific users or groups, or to specific apps. Additionally, you can create conditional access session control policies to enable a limited experience within specific cloud applications. For Example, you could create a policy to limit information system access to devices such as printers to block the ability to print sensitive documents on unmanaged devices.

To learn more, see [Conditional Access: Session.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session)

Intune/Intune Suite

A cloud-based Enterprise Mobility Management (EMM) service that enables administrators to enroll mobile devices, deploy apps, and enforce security policies. As a Security Admin, use the Endpoint security node in Intune to configure device security and to manage security tasks for devices when those devices are at risk.

To protect your devices and corporate resources, you can use [Microsoft Entra ID Conditional Access policies with Intune.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions)

Intune passes the results of your device compliance policies to Microsoft Entra ID , which then uses conditional access policies to enforce which devices and apps can access your corporate resources. Conditional access policies also help to gate access for devices that aren’t managed by Intune and can use compliance details from [Mobile Threat Defense partners](https://docs.microsoft.com/en-us/mem/intune/protect/mobile-threat-defense) you integrate with Intune.

The following are two common methods of using conditional access with Intune:

* [Device-based conditional access](https://docs.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune), to ensure only managed and compliant devices can access network resources.
* [App-based conditional access](https://docs.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune), which uses app-protection policies to manage access to network resources by users on devices that you do not manage with Intune.

**Microsoft 365 Web Apps**

In Microsoft 365, identity is managed by Microsoft Entra ID. As a SharePoint or global admin in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune). Blocking or limiting access on unmanaged devices relies on Microsoft Entra ID conditional access policies. Using a policy that affects all Microsoft 365 services can lead to better security and better experience for your users.

**Microsoft 365 Groups**

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources.

**Customer Lockbox**

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. To learn more, see [Customer Lockbox for Microsoft Azure](https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview).

[**Azure Policies**](#_Azure_Policy)

* [**AC.L1-3.1.1 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#limit-system-access-to-authorized-users-processes-acting-on-behalf-of-authorized-users-and-devices-including-other-systems)

**Azure:**

**Customer Responsibility**

* Responsible for authorizing access to the customer system.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for enforcing approved authorizations for logical access to the system, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to MICROSOFT ENTRA ID via SAML2.0 ticket. Once permissions are communicated to MICROSOFT ENTRA ID, MICROSOFT ENTRA ID is responsible for enforcing those permissions for the user’s Office 365 session.

AC.L1-3.1.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-2, AC-3, AC-17 | |
| **Practice:** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.  **Assessment Objectives:**  [a] the types of transactions and functions that authorized users are permitted to execute are defined; and  [b] system access is limited to the defined types of transactions and functions for  authorized users. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC  Privileged Identity Management (PIM) | Network Security Groups Conditional Access GitHub Enterprise Cloud GitHub AE  Microsoft Entra ID Multi-Factor Authentication  Intune/Intune Suite  Microsoft 365 Web Apps  Microsoft 365 admin center  Microsoft Defender for Cloud Apps |

**Implementation Guidance:**

**Microsoft Entra ID**

Limit users to only the information systems, roles, or applications they are permitted to use and are needed for their roles and responsibilities with Azure [Role Based Access](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) Control (Azure RBAC). Limit access to applications and data based on the authorized users’ roles and responsibilities. Common types of functions a user can be assigned are create, read, update, and delete. Azure RBAC will help you manage who has access to Azure resources. More granularity, you can restrict what the users can do with the resources and what areas they have access to.

Microsoft Entra ID Identity Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources. These and related Microsoft Entra ID and Enterprise Mobility + Security features allow you to mitigate access risk by protecting, monitoring, and auditing access to critical assets while ensuring employee and business partner productivity.

**Privileged Identity Management (PIM)**

You can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses [Microsoft Entra ID Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks). For example, during the activation process, a user can be forced to justify why they need to activate their role. Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

PIM provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Network Security Groups**

[Network Security Group](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview)s is customizable and provide the ability to fully lock down network communication to and from your system-resources. You can restrict internet access by default, along with the use of network security groups, data segregation and isolated VPNs.

Use [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  to manage and secure identities by requiring [single sign-on](https://azure.microsoft.com/en-us/services/active-directory/sso/) and multifactor authentication to protect your users. The recommended way to enable and use Microsoft Entra ID Multi-Factor Authentication is with Conditional Access Policies. [Learn how to Create a Conditional Access Policy.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa#create-a-conditional-access-policy)

**Intune/Intune Suite**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Explore using [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connections restrict public internet providing a private connection to Azure.

**Microsoft 365 Web Apps**

In Microsoft 365, identity is managed by Microsoft Entra ID. As a SharePoint or global admin in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune). Blocking or limiting access on unmanaged devices relies on Microsoft Entra ID conditional access policies. Using a policy that affects all Microsoft 365 services can lead to better security and better experience for your users.

**Microsoft Defender for Cloud Apps**

Microsoft Defender for Cloud Apps Conditional Access App Control uses reverse proxy architecture to give you the tools you need to have real-time visibility and control over access to and activities performed within your cloud environment. With Conditional Access App Control, you can protect your organization:

• Avoid data leaks by blocking downloads before they happen

• Set rules that force data stored in and downloaded from the cloud to be protected with encryption

• Gain visibility into unprotected endpoints so you can monitor what is being done on unmanaged devices

• Control access from non-corporate networks or risky IP addresses

**Microsoft 365 Admin Center**

The Microsoft 365 admin center lets you manage Microsoft Entra ID roles and Microsoft Intune roles. However, these roles are a subset of the roles available in the Microsoft Entra ID portal and the Intune admin center.

**GitHub AE**

With [GitHub AE](https://docs.github.com/en/github-ae@latest/admin/overview/about-enterprise-accounts#:~:text=An%20enterprise%20account%20allows%20you,(organization%20members%2C%20outside%20collaborators)), you can create an enterprise account to enable collaboration between your organization. You can control access by [managing users in your enterprise](https://docs.github.com/en/github-ae@latest/admin/user-management). While you can grant read/write access to collaborators on a personal repository, members of an organization can have [more granular access permissions](https://docs.github.com/en/github/getting-started-with-github/access-permissions-on-github) for the organization's repositories.

**Azure:**

**Customer Responsibility**

* Responsible for authorizing access to the customer system.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for enforcing approved authorizations for logical access to the system, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to MICROSOFT ENTRA ID via SAML2.0 ticket. Once permissions are communicated to MICROSOFT ENTRA ID, MICROSOFT ENTRA ID is responsible for enforcing those permissions for the user’s Office 365 session.

**Additional Resources:**

* [Identity Governance - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview)

AC.L2-3.1.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-4 | |
| **Practice:** Control the flow of CUI in accordance with approved authorizations.  **Assessment Objectives:**  [a] information flow control policies are defined;  [b] methods and enforcement mechanisms for controlling the flow of CUI are defined;  [c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI  within the system and between interconnected systems are identified;  [d] authorizations for controlling the flow of CUI are defined; and  [e] approved authorizations for controlling the flow of CUI are enforced. | |
| **Primary Services** | **Secondary Services** |
| Azure Web Application Firewall  Microsoft Purview | Network Security Groups  Intune/Intune Suite  Microsoft Defender for Cloud Apps  Microsoft Defender for Identity  Microsoft Copilot for Security  Exchange Admin Center  M365 Compliance Center  Power Automate  Front Door |

**Implementation Statement:**

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Learn about other Microsoft Purview products available:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Azure Web Application Firewall**

Defend your web services against common exploits and vulnerabilities using [Azure Web Application Firewall](https://azure.microsoft.com/en-us/services/web-application-firewall/) deployed with Azure Front Door. It keeps your service highly available for your users and helps you meet compliance requirements. [Customize Web Application Firewall](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-customize-waf-rules-portal) rules using Azure portal. Use Azure [Front Door](https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview#:~:text=Azure%20Front%20Door%20is%20a,and%20widely%20scalable%20web%20applications.&text=Front%20Door%20provides%20a%20range,needs%20and%20automatic%20failover%20scenarios.) as a scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. Learn more about [Azure Web Application Firewall on Azure Front Door.](https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview)

**Intune/Intune Suite**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Further, Intune can be configured to restrict copying of data to publicly accessible information systems. [Configure Intune to prevent data leaks](https://docs.microsoft.com/en-us/mem/intune/protect/data-leak-prevention) on non-managed devices and setup [app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy) to secure company data on user-owned devices.

**Microsoft Copilot Security**

Microsoft Copilot for Security, integrated with Microsoft Purview, is designed to enhance data protection and security management through AI-driven insights and automation. While tools like Microsoft Intune can manage and secure devices and their data, Microsoft Copilot for Security itself focuses on providing recommendations and insights rather than directly controlling actions such as isolating machines or managing data flows.

By combining AI-driven insights from Microsoft Copilot for Security with the data protection capabilities of Microsoft Purview, organizations can better control the flow of sensitive data. This integration ensures that sensitive information is managed according to organizational policies and regulatory requirements, ultimately enhancing the overall security posture and compliance of the organization.

* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3#tabs-oc19f7_tab3)
* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Microsoft Copilot for Security in Microsoft Purview](https://learn.microsoft.com/en-us/purview/copilot-in-purview-overview)

[**Azure Policies**](#_Azure_Policy)

* [**AC.L2-3.1.3 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#control-the-flow-of-cui-in-accordance-with-approved-authorizations)

**Azure:**

**Customer Responsibility**

* Responsible for controlling the flow of information within customer-deployed resources and between interconnected systems.

**GCCH:**

**Customer Responsibility:**

* Government customers are responsible for ensuring that no information with a security impact level greater than high is stored, processed, or transmitted via the services provided to them by Office 365 Office 365 will be accredited to store, process, and transmit up to High Impact information as defined by NIST SP 800-60.

**Additional Resources**

* [Conditional Access policies for Azure Information Protection](https://techcommunity.microsoft.com/t5/security-compliance-and-identity/conditional-access-policies-for-azure-information-protection/ba-p/250357)
* [Conditional Access for Azure information protection (AIP)](https://techcommunity.microsoft.com/t5/security-compliance-and-identity/conditional-access-policies-for-azure-information-protection/ba-p/250357)
* [Remote access to on-premises apps - Microsoft Entra ID Application Proxy](https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy)
* [Compliance and Regulatory information](https://docs.microsoft.com/en-us/compliance/regulatory/offering-nist-sp-800-171) on managing CUI.
* DFARS [Controlled Unclassified Information (CUI) and covered defense information (CDI)](https://docs.microsoft.com/en-us/compliance/regulatory/offering-dfars#frequently-asked-questions)
* [Control over data travel with](https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security) Microsoft Defender for Cloud Apps
* Learn more about controlling traffic with NSGs at <https://aka.ms/nsg-doc>
* [Data protection framework using app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-framework)

AC.L2-3.1.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-5 | |
| **Practice:** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.  **Assessment Objectives:**  [a] the duties of individuals requiring separation are defined;  [b] responsibilities for duties that require separation are assigned to separate individuals;  and  [c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC | Privileged Identity Management (PIM) |

**Implementation Statement:**

Microsoft Azure offers a robust security set for employing separation of duties. Best practice recommendation is to segregate duties within your team by setting up [Role Based Access](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) (RBAC) which will help you manage who has access to Azure resources. Review assignments and roles regularly to ensure users have the appropriate access that is needed to perform their specific job functions.

[Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) has several Azure built-in roles that you can assign to users, groups, service principals, and managed identities. Role assignments are the way you control access to Azure resources. If the built-in roles do not meet the specific needs of your organization, you can create your own [Azure custom roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles). For information about how to assign roles, see [Steps to assign an Azure role](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps).

Additionally, you can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with access to the most privileged access, resources, and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Azure**

**Customer Responsibility**

* Responsible for the separation of duties across customer-controlled accounts.

**GCCH**

**Customer Responsibility:**

* Government customers are responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.  
    
  Government customers using ADFS will manage their user accounts in their existing Active Directory infrastructure.

[**Azure Policies**](#_Azure_Policy)

* [**AC.L2-3.1.4 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#separate-the-duties-of-individuals-to-reduce-the-risk-of-malevolent-activity-without-collusion)

AC.L2-3.1.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-6, AC-6(1), AC-6(5) | |
| **Practice:** Employ the principle of least privilege, including for specific security functions and privileged accounts.  **Assessment Objectives:**  [a] privileged accounts are identified;  [b] access to privileged accounts is authorized in accordance with the principle of least  privilege;  [c] security functions are identified; and  [d] access to security functions is authorized in accordance with the principle of least  privilege. | |
| **Primary Services** | **Secondary Services** |
| Privileged Identity Management (PIM)  Microsoft Purview  Azure RBAC | Microsoft Entra ID  GitHub Enterprise Cloud  GitHub AE  Microsoft 365 Admin Center  Microsoft Copilot for Security |

**Implementation Guidance:**

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Learn about privileged access management - Microsoft Purview (compliance)](https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Microsoft Entra ID**

Microsoft Entra ID offers a robust security set for employing the principle of least privilege. Best practice recommendation is to segregate duties within your team by setting up Role Based Access Control (RBAC) which will help you manage who has access to Azure resources. There are a large number of preexisting roles available within Azure, and it is likely that an existing role will meet your needs, so you likely will not need to configure a custom role. First, you should specify exactly what actions a security principle should and should not be able to perform. Once you have generated this list, you should review the existing roles and determine if one of the existing roles meets your needs or if you need to create a custom role.

When configuring Azure RBAC, make sure that you follow the principal of least privilege. This means that you should only grant the access required to perform specific tasks. Doing so reduces the chance of unauthorized or accidental actions being performed. For example, if a group only requires the ability to view the configuration of an Azure resource, you only need to assign a role that has the Read permission to that resource. If a group only requires Azure portal access to one virtual machine in a resource group (even though the resource group hosts multiple virtual machines), set the scope of the role assignment to the virtual machine rather than the resource group when assigning the role to that group.

To learn more, see:

* [What is Azure role-based access control.](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)
* [Grant user access to Azure resources using RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/quickstart-assign-role-user-portal)
* [RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/#:~:text=Azure%20role%2Dbased%20access%20control%20(Azure%20RBAC)%20is%20a,need%20to%20perform%20their%20jobs.) documentation
* [Azure Custom roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles)

**Microsoft 365 Admin Center**

When you configure a privileged access policy with the Microsoft 365 admin center. In the Microsoft 365 admin center users can request access to elevated or privileged tasks. An approval request is generated, and the pending request notification is emailed to approvers.

**Privileged Identity Management**

Additionally, you can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with access to the most privileged access, resources and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

Further, you can explore the use of [Just Enough Administration](https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.1) (JEA) to further limit admin accounts. There are [prerequisites](https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/prerequisites?view=powershell-7.1) to using JEA.

Privileged access management allows granular access control over privileged admin tasks in Office 365. Privileged access management builds on the protection provided with native encryption of Microsoft 365 data and the role-based access control security model of Microsoft 365 services. When used with Microsoft Entra ID Privileged Identity Management, these two features provide access control with just-in-time access at different scopes.

To summarize, you should complete the following Microsoft Entra ID PIM tasks for your Azure resources:

* Enable Just in Time access to Azure
* Expire access automatically
* Assign temporary access for quick tasks or on-call schedules
* Get alerts when new users or groups are assigned resource access, or when eligible assignments are activated
* Use Microsoft Entra ID sign in for Azure VMs

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**GitHub AE**

With [GitHub AE](https://docs.github.com/en/github-ae@latest/admin/overview/about-enterprise-accounts#:~:text=An%20enterprise%20account%20allows%20you,(organization%20members%2C%20outside%20collaborators)), you can create an enterprise account to enable collaboration between your organization. You can control access by [managing users in your enterprise](https://docs.github.com/en/github-ae@latest/admin/user-management). While you can grant read/write access to collaborators on a personal repository, members of an organization can have [more granular access permissions](https://docs.github.com/en/github/getting-started-with-github/access-permissions-on-github) for the organization's repositories.

**Microsoft Copilot for Security**

Microsoft Copilot for Security, being part of the broader Microsoft security ecosystem, is designed to enhance the security posture of organizations through AI-driven insights and recommendations. While Copilot itself serves as a powerful tool for analyzing security data and generating actionable insights, the enforcement of the principle of least privilege is managed through the integration with other Microsoft security and administration products, such as Microsoft Defender, Microsoft Intune, and Microsoft Entra.

Although Microsoft Copilot for Security itself does not directly manage user privileges, its integration with these Microsoft security products means that it supports a security operations ecosystem where the principle of least privilege can be effectively implemented and managed.

* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3#tabs-oc19f7_tab3)
* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Respond to identity threats quickly using Copilot in Microsoft Entra - Microsoft Entra](https://learn.microsoft.com/en-us/entra/fundamentals/copilot-security-entra)

**Azure**

**Customer Responsibility**

* Responsible for enforcing least privilege across customer-controlled accounts.

**GCCH**

**Customer Responsibility**

* Government customers are responsible for employing the concept of least privilege, allowing only authorized accesses for government customer users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions in compliance with their organizational policies.

Government customers using ADFS will manage their user accounts in their existing Active Directory infrastructure.

AC.L2-3.1.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-6(2) | |
| **Practice:** Use non-privileged accounts or roles when accessing non-security functions.  **Assessment Objectives:**  [a] nonsecurity functions are identified; and  [b] users are required to use non-privileged accounts or roles when accessing nonsecurity  functions. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC | Privileged Identity Management (PIM)  Microsoft Purview  Microsoft 365 Admin Center  Microsoft Copilot for Security |

**Implementation Guidance:**

When planning your access control strategy, it is best practice to implement least privilege. Least privilege means you grant your administrators exactly the permission they need to do their job. There are three aspects to consider when you assign a role to your administrators: a specific set of permissions, over a specific scope and for a specific period of time. Customers should avoid assigning broader roles and broader scopes even if it initially seems more convenient to do so. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised.

**Microsoft Entra ID**

Microsoft Entra ID RBAC supports over 65 [built-in roles](https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference). There are Microsoft Entra ID roles to manage directory objects like users, groups, and applications, and also to manage Microsoft 365 services like Exchange, SharePoint, and Intune.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Learn about privileged access management - Microsoft Purview (compliance)](https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Privileged Identity Management (PIM)**

Microsoft recommends that you enable Privileged Identity Management (PIM) in Microsoft Entra ID. Using PIM, a user can be made an eligible member of a Microsoft Entra ID role. They can then activate their role for a limited timeframe every time the needs to use it. Privileged access is automatically removed when the timeframe expires.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

Best Practices:

* Conduct User Access reviews to review administrator's access regularly to make sure only the right people have continued access.
* Enable MFA on Microsoft Entra ID roles
* Microsoft Entra ID groups allow you to collect Azure security principals including users, service principals, and other groups.
* Conditional Access Policies allow you to implement more stringent authentication requirements if certain conditions are met.
* Application registration permission scopes allow you to control what resources and data an application can access.
* Custom RBAC roles can be configured if an existing RBAC role does not have permissions that are appropriate to your organization’s needs.
* Microsoft recommends that you assign the Global Administrator role to fewer than five people in your organization.

**Microsoft 365 Admin Center**

When you configure a privileged access policy with the Microsoft 365 admin center. In the Microsoft 365 admin center users can request access to elevated or privileged tasks. An approval request is generated, and the pending request notification is emailed to approvers.

**Microsoft Copilot for Security**

Microsoft Copilot for Security does not have the ability to change roles or permissions, as these actions would be strictly limited to the administrator. When it integrates with applications such as Microsoft Intune and Microsoft Entra, it only has access to the RBAC permissions that are assigned to the administrator, ensuring that least privilege is maintained. Using the native features of Microsoft Copilot for Security, an administrator can review insights about users permissions, roles to make determinations if any adjustments needed to be made, including the ability for any non-privileged actions to occur. Microsoft Copilot in Microsoft Entra gets insights from your Microsoft Entra users, groups, sign-in logs, and audit logs.

* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3#tabs-oc19f7_tab3)
* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Respond to identity threats quickly using Copilot in Microsoft Entra - Microsoft Entra](https://learn.microsoft.com/en-us/entra/fundamentals/copilot-security-entra)

**Azure:**

**Customer Responsibility**

* Responsible for requiring the use of non-privileged accounts/roles when accessing non-security functions for customer-deployed resources.

**GCCH:**

**Customer Responsibility:**

* Government customers are responsible for requiring that users of information system accounts/roles with access to government security functions or security-relevant information use non-privileged accounts/roles when accessing other system functions. Government customers are also responsible for auditing any use of privileged accounts/roles for such functions, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government managed ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to MICROSOFT ENTRA ID via SAML2.0 ticket.

AC.L2-3.1.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-6(9), AC-6(10) | |
| **Practice:** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.  **Assessment Objectives:**  [a] privileged functions are defined;  [b] non-privileged users are defined;  [c] non-privileged users are prevented from executing privileged functions; and  [d] the execution of privileged functions is captured in audit logs. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC  Privileged Identity Management (PIM)  Azure Monitor  Microsoft Sentinel  Microsoft Purview | Conditional Access  Intune/Intune Suite  Microsoft Defender for Office 365  M365 Compliance Center  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID**

Microsoft Azure offers a robust security set for preventing the use of non-privileged accounts from executing privileged functions. Best practice recommendation is to segregate duties within your team by setting up [Role Based Access](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) (RBAC) which will help you manage who has access to Azure resources. More granularity, you can restrict what the users can do with the resources and what areas they have access to.

Additionally, you can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with the most privileged access, resources, and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

Privileged access management requires users to request just-in-time access to complete elevated and privileged tasks through a highly scoped and time-bounded approval workflow. Privileged access management is defined and scoped at the task level, while Microsoft Entra ID Privileged Identity Management applies protection at the role level with the ability to execute multiple tasks. All activity for the task is logged in the Security & Compliance Center.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)
* [Learn about privileged access management - Microsoft Purview (compliance)](https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**M365 Compliance Center**

Enable auditing of admin activity in [M365 Compliance Center](https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center). [Enabling auditing for admins](https://support.microsoft.com/en-us/topic/auditing-in-office-365-for-admins-9f6484d2-0fd2-17de-165f-c41346023906) allows you to capture user and administrator activities in your organization.

[Audited Activities](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#audited-activities) in M365 Compliance Center can be granularly selected. It is recommended to review audit logs at a frequency to meet your compliance requirements. This will assist in discovering execution of privileged functions.

**Intune/Intune Suite :**

By default, auditing in [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  is enabled for all customers. This allows an organization’s administrator to track and monitor events in Microsoft Intune. Audit logs include a record of activities, such as; create, update (edit), delete, assign, and remote actions all create audit events that administrators can review.

Logs can also be sent to [Azure Monitor](https://azure.microsoft.com/en-us/services/monitor/) services, including [storage accounts, event hubs, and log analytics](https://docs.microsoft.com/en-us/mem/intune/fundamentals/review-logs-using-azure-monitor). For more information: [use audit logs to track and monitor events in Microsoft Intune.](https://docs.microsoft.com/en-us/mem/intune/fundamentals/monitor-audit-logs#:~:text=Audit%20logs%20include%20a%20record,It%20can't%20be%20disabled.)

Additionally, consider using Microsoft Sentinel as your Security Information and Event Management (SIEM) solution. After you [connect your data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks. While Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to [Create interactive reports with Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview).

**Microsoft Copilot for Security**

Microsoft Copilot for Security integrates with products like Microsoft Entra to support concepts like least privilege and RBAC while limiting exposure of privileged accounts or roles. Microsoft Entra ID Protection applies the capabilities of Copilot for Security to summarize a user's risk level, provide insights relevant to the incident at hand, and provide recommendations for rapid mitigation. Risky user summarization provides admins and responders quick access to the most critical information in context to aid their investigation.

* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3#tabs-oc19f7_tab3)
* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Respond to identity threats quickly using Copilot in Microsoft Entra - Microsoft Entra](https://learn.microsoft.com/en-us/entra/fundamentals/copilot-security-entra)

**Customer Responsibility**

* Responsible for auditing the execution of privileged functions on customer-deployed resources.
* Responsible for ensuring that non-privileged users cannot execute privileged functions on customer-deployed resources.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for capturing what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Customers using Windows servers to support their ADFS infrastructure automatically meet this requirement as Windows captures these event details by default

**Additional Resources**

* [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide)

AC.L2-3.1.8

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-7 | |
| **Practice:** Limit unsuccessful logon attempts.  **Assessment Objectives:**  [a] the means of limiting unsuccessful logon attempts is defined; and  [b] the defined means of limiting unsuccessful logon attempts is implemented. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID | Microsoft Entra ID Password Protection  Microsoft Entra ID Smart Lockout |

**Implementation Guidance:**

**Microsoft Entra ID and Password Protection**

Microsoft customers should consider two factors when implementing this control. They should determine the threshold for how many consecutive times a failed login will be allowed before a lockout is implemented, and then determine what would be the duration of that lock out. Having three consecutive, unsuccessful logon attempts is a common setting. Organizations should set this number at a level that fits their risk profile. Fewer unsuccessful attempts provide higher security.

Password protection has a smart lockout functionality, which ensures that the Microsoft Entra ID account is locked out before the AD account is locked out, which would leave an organization susceptible to a denial-of-service attack.

You can control the lockout duration using Microsoft Entra ID smart lockout. Smart lockout allows customers to lock out attackers who are trying to brute force user passwords. Based on machine learning, smart lockout is able to discern when sign-ins are coming from authentic users and treat those sign-ins differently to those that appear to come from attackers or other unknown sources. For example, smart Lockout locks out an account for 60 seconds after 10 failed sign-in attempts have occurred. If there are subsequent failed sign-in attempts after this 60 second has expired, the lock out period duration increases. Smart Lockout only tracks when different passwords are used, which is the pattern during a brute force attack, so if a user enters the same incorrect password 10 times, that will only count as one bad password towards the 10 that trigger account lockout.

Microsoft Entra ID Smart Lockout is enabled by default on Microsoft 365 Microsoft Entra ID tenancies. Customers can configure a [custom smart lockout](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#manage-azure-ad-smart-lockout-values) threshold in the Authentication Methods section of the Microsoft Entra ID console.

For each lockout, the duration of the lockout is increased. Customers should make sure the Microsoft Entra ID lockout threshold is less than the threshold for AD (making sure Microsoft Entra ID locks out first) and the duration of the lockout in Microsoft Entra ID is longer than the AD reset counter.

**Azure:**

**Customer Responsibility**

* Responsible for enforcing a limit of consecutive failed login attempts on customer-deployed

**GCCH:**

**Customer Responsibility**

* GCCH SSP indicates it is inherited by Azure (CSP)

**Additional Resources:**

* [Account lockout threshold (Windows 10) - Windows security](https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold)

##### AC.L2-3.1.9

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-8 | |
| **Practice**: Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.  **Assessment Objective:**  [a] privacy and security notices required by CUI-specified rules are identified, consistent,  and associated with the specific CUI category; and  [b] privacy and security notices are displayed. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite  Microsoft Entra ID | Conditional Access  Teams |

**Implementation Guidance:**

CUI is information that requires safeguarding or disseminating controls according to law, regulation, or government-wide policy. The [CUI Registry](https://www.archives.gov/cui/registry/category-list) identifies approved CUI categories and subcategories. Microsoft customers should consult their specific CUI requirements which require safeguarding or dissemination controls and are either:

* Marked or otherwise identified in the contract, task order, or delivery order, and provided to the contractor by or on behalf of DoD in connection with the performance of the contract, or
* Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

**Teams**

You can require acceptance of Company terms and conditions before accessing resources such as, Teams, SharePoint and OneDrive by using Microsoft Entra ID Conditional Access. Moreover, you can customize Teams meeting invitations to meet your organization's needs. You can add your organization's logo and include helpful information, such as links to your support website and legal disclaimer, and a text-only footer.

There are two ways to create your company terms and conditions:

* by using [Intune](https://docs.microsoft.com/en-us/mem/intune/enrollment/terms-and-conditions-create#create-terms-and-conditions)
* by using the [Microsoft Entra ID terms of use feature](https://docs.microsoft.com/en-us/azure/active-directory/governance/active-directory-tou)

To learn which method is best for you, check out the [Choosing the right Terms solution for your organization blog post](https://go.microsoft.com/fwlink/?linkid=2010506&clcid=0x409).

**Microsoft Entra ID**

Add Microsoft Entra ID [terms of use policies](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use) to ensure users see relevant disclaimers for legal or compliance requirements by requiring the user to accept or decline the terms of use. You can also [view report of who has accepted and declined](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use).

**Intune/Intune Suite**

As an Intune admin, you can require that users accept your company's terms and conditions before using the Company Portal to:

* enroll devices
* access resources like company apps and email.

You can create multiple sets of terms and assign them to different groups, such as to support different languages.

To learn more, see [Intune](https://docs.microsoft.com/en-us/mem/intune/enrollment/terms-and-conditions-create#create-terms-and-conditions).

**Azure:**

**Customer Responsibility**

* Responsible for implementing a compliant system use notification for all customer-deployed resources.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for displaying an approved system use notification message or banner on the authentication page served by their ADFS server used to authenticate to Office 365 that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.

**Additional Resources**

* [Add your organization's privacy info using Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-properties-area)
* [Add language-specific company branding to your directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding#add-language-specific-company-branding-to-your-directory)

##### AC.L2-3.1.10

| **Control Summary Information** | |
| --- | --- |
| **NIST 800-171 Mapping:** 3.1.10 | |
| **NIST SP 800-53 Mapping:** AC-11, AC-11(1) | |
| **Practice:** Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.  **Assessment Objectives:**  [a] the period of inactivity after which the system initiates a session lock is defined;  [b] access to the system and viewing of data is prevented by initiating a session lock after  the defined period of inactivity; and  [c] previously visible information is concealed via a pattern-hiding display after the  defined period of inactivity. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Conditional Access | Microsoft Azure Portal  Azure Virtual Machines  Windows 365 Cloud PC  Microsoft 365 Web Apps  Intune/Intune Suite  Microsoft Copilot for Security |

**Implementation Statement:**

**Azure Portal**

The inactivity timeout setting helps to protect resources from unauthorized access if you forget to secure your workstation. After you have been idle for a while, you are automatically signed out of your Azure portal session. Admins in the [Global Administrator role](https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#global-administrator) can enforce the maximum idle time before a session is signed out. The inactivity timeout setting applies at the directory level. The setting takes effect for new sessions. It will not apply immediately to any users who have already signed in. For more information about directories, see [Active Directory Domain Services Overview](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview).

**Intune/Intune Suite & Microsoft Copilot for Security**

You can use Intune/Intune Suite to set policies that define the maximum minutes of inactivity before the screen locks on your device. Configure screen lock settings through Intune to ensure your device is secure. Utilize conditional access controls to grant access to resources only if devices are marked as compliant. Additionally, Intune/Intune Suite allows you to set screen lock settings seamlessly. The embedded integration of Microsoft Copilot for Security provides secure and tested policies, avoiding conflicts with other policies in the environment. It highlights misconfigurations and offers recommendations, including requirements such as session lock.

* [Endpoint management services and solutions at Microsoft | Microsoft Learn](https://learn.microsoft.com/en-us/mem/endpoint-manager-overview)
* [Device restriction settings for Windows 10/11 in Microsoft Intune | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience)
* [Grant controls in Conditional Access policy](https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant#require-device-to-be-marked-as-compliant)
* [Use Copilot for Security to get device and policy information | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/copilot/security-copilot)
* [Microsoft Security Copilot improves speed and efficiency for security and IT teams | Microsoft Security Blog](https://www.microsoft.com/en-us/security/blog/2023/12/06/microsoft-security-copilot-drives-new-product-integrations-at-microsoft-ignite-to-empower-security-and-it-teams/?msockid=24625821c11468eb15394c6cc01669f3)

**Microsoft Entra ID**

By default, Microsoft Entra ID obscures all passwords. Microsoft’s [Password boxes](https://docs.microsoft.com/en-us/windows/uwp/design/controls-and-patterns/password-box) conceal the characters typed into it for purposes of privacy. By default, the password box provides a way for the user to view their password by holding down a reveal button.

You can disable this feature for Windows 10 using [policy](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialsui) as an added security measure to ensure your password can not be displayed on the login screen.

**Conditional Access**

Implement device lock by using a conditional access policy to restrict access to compliant devices. Configure policy settings on the device to enforce device lock at the OS level with MDM solutions such as Intune. Endpoint Manager or group policy objects can also be considered in hybrid deployments. For unmanaged devices, configure the Sign-In Frequency setting to force users to reauthenticate.

**Microsoft 365 Web Apps**

When users authenticate in any of the Microsoft 365 web apps or mobile apps, a session is established. For the duration of the session, users will not need to re-authenticate. Sessions can expire when users are inactive, when they close the browser or tab, or when their authentication token expires for other reasons such as when their password has been reset. The Microsoft 365 services have different session timeouts to correspond with the typical use of each service.

**Azure:**

**Customer Responsibility**

* Responsible for incorporating a session lock on all customer-deployed resources.
* Responsible for concealing previously visible information when a session lock is initiated on customer-deployed resources.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for preventing further access to the system by initiating a session lock, after a given period of user inactivity at the workstation level, in compliance with organizational policies.

**Additional Resources**

* Deploy requirements to prevent access and viewing data after a period of inactivity using [Interactive Login: Machine Inactivity Limit](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit).
* Deploy requirements for [Account Lockout](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy).
* Deploy requirements to [disable](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialsui#credentialsui-disablepasswordreveal) the password reveal button.

AC.L2-3.1.11

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-12 | |
| **Practice:** Terminate (automatically) user sessions after a defined condition.  **Assessment Objectives:**  [a] conditions requiring a user session to terminate are defined; and  [b] a user session is automatically terminated after any of the defined conditions occur. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID Smart Lockout  Microsoft Entra ID  Microsoft 365 Defender  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft Azure Portal  Intune/Intune Suite | Azure Bastion  Conditional Access  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID**

Implement automatic user session re-evaluation with Microsoft Entra ID features such as Risk-Based Conditional Access and Continuous Access Evaluation. Inactivity conditions can be implemented at a device level as described in:

* [Sign-in risk-based Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk)
* [User risk-based Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk-user)
* [Continuous Access Evaluation](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation)

Additionally, having a [lockout threshold](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold) limiting the number of unsuccessful login attempts will protect against threats such as, [Brute Force Attacks](https://www.microsoft.com/security/blog/2020/04/23/protecting-organization-password-spray-attacks/) by automatically locking the account after a specified number of attempts. Default lockout threshold is set to 10 failed sign-ins before the first lockout occurs. It is important to customize the lockout threshold to fit your business requirements using [Microsoft Entra ID smart lockout](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout).

Federated deployments that use AD FS 2016 and AD FS 2019 can enable similar benefits using [AD FS Extranet Lockout and Extranet Smart Lockout](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection). Extranet Smart Lockout (ESL) protects your users from experiencing extranet account lockout from malicious activity.

ESL enables AD FS to differentiate between sign-in attempts from a familiar location for a user and sign-in attempts from what may be an attacker. Smart lockout is always on, for all Microsoft Entra ID customers, with default settings that offer the right mix of security and usability.

**Intune/Intune Suite & Microsoft Copilot for Security**

Manage your devices and applications with Microsoft Intune. For Intune-managed devices, you can reset them to factory settings. If the device is unmanaged, you can wipe corporate data from managed apps. These processes effectively remove potentially sensitive data from end users' devices. However, the device must be connected to the internet to trigger either process. If the device is offline, it will still have access to any locally stored data.

Intune, along with the Intune Suite and the embedded integration of Microsoft Copilot for Security, allows users to review specific device configuration settings. This integration provides information about the settings, enabling users to utilize secure and tested configurations. These policy configurations include requirements such as setting parameters for account lockout due to user inactivity.

* [Endpoint management services and solutions at Microsoft | Microsoft Learn](https://learn.microsoft.com/en-us/mem/endpoint-manager-overview)
* [Device restriction settings for Windows 10/11 in Microsoft Intune | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience)
* [Grant controls in Conditional Access policy](https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant#require-device-to-be-marked-as-compliant)
* [Use Copilot for Security to get device and policy information | Microsoft Learn](https://learn.microsoft.com/en-us/mem/intune/copilot/security-copilot)
* [Microsoft Security Copilot improves speed and efficiency for security and IT teams | Microsoft Security Blog](https://www.microsoft.com/en-us/security/blog/2023/12/06/microsoft-security-copilot-drives-new-product-integrations-at-microsoft-ignite-to-empower-security-and-it-teams/?msockid=24625821c11468eb15394c6cc01669f3)

**Microsoft Defender for Cloud Apps**

Use Microsoft Defender for Cloud Apps to block data download when appropriate. If the data can only be accessed online, organizations can monitor sessions and achieve real-time policy enforcement. Defender for Cloud Apps looks at every user session on your cloud and alerts you when something happens that is different from the baseline of your organization or from the user's regular activity. You can enable automated remediation actions on alerts generated by anomaly detection policies

**Microsoft Defender for Endpoint**

Microsoft Defender for Endpoint provides the capability of isolating devices from the network and restricting app execution. This action can help prevent the attacker from controlling the compromised device and performing further activities such as data exfiltration and lateral movement.

**Azure:**

**Customer Responsibility**

* Responsible for defining and enforcing events or conditions requiring the termination of a user session on customer-deployed resources.

**GCCH:**

**Customer Responsibility**

Government customers are responsible for configuring a session termination interval that follows their organizational requirements when using W365 services.

AC.L2-3.1.12

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-17(1) | |
| **Practice:** Monitor and control remote access sessions.  **Assessment Objectives:**  [a] remote access sessions are permitted;  [b] the types of permitted remote access are identified;  [c] remote access sessions are controlled; and  [d] remote access sessions are monitored. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Microsoft Defender for IoT  Microsoft Sentinel  Azure Bastion | Microsoft Azure Portal  Azure ExpressRoute  Network Security Groups  Intune/Intune Suite  Microsoft Defender for Office 365  Conditional Access Direct Access  Windows 365 Cloud PC  Azure Virtual Machines  Microsoft 365 Defender  Microsoft Copilot for Security |

**Implementation Statement:**

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code. Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets. Microsoft services can help meet this practice by providing the applicable services such as, but not limited to, Microsoft Entra ID , Azure Bastion, Microsoft Endpoint Manager and Microsoft Sentinel

**Azure Bastion**

Once the Bastion service is provisioned and deployed in your virtual network, you can use it to seamlessly connect to any VM in this virtual network. As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

To learn more, see [Azure Bastion](https://azure.microsoft.com/en-us/services/azure-bastion/).

**Microsoft Defender for IoT and Sentinel**

[Microsoft Defender for IoT](https://azure.microsoft.com/en-us/services/azure-defender-for-iot/) provides continuous asset discovery, vulnerability management, and threat detection for your Internet of Things (IoT) and operational technology (OT) devices and helps meet this requirement for its monitoring capabilities.

Microsoft Defender for IoT interoperates with Microsoft Sentinel which collects data across all users, devices, applications, and infrastructure, both on-premises and in the cloud to support monitoring requirements.

**Microsoft Entra ID and Conditional Access**

Use [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  to manage and secure identities by requiring [single sign-on](https://azure.microsoft.com/en-us/services/active-directory/sso/) and multifactor authentication to protect your users. The recommended way to enable and use Microsoft Entra ID Multi-Factor Authentication is with Conditional Access Policies. [Learn how to Create a Conditional Access Policy.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa#create-a-conditional-access-policy)

**Intune/Intune Suite and Conditional Access**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Azure ExpressRoute**

Explore using [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

**DirectAccess**

DirectAccess allows connectivity for remote users to organization network resources without the need for traditional Virtual Private Network (VPN) connections. With DirectAccess connections, remote client computers are always connected to your organization - there is no need for remote users to start and stop connections, as is required with VPN connections. DirectAccess provides support only for domain-joined clients that include operating system support for DirectAccess. Remote Access monitoring reports remote user activity and status for DirectAccess and VPN connections. It tracks the number and duration of client connections (among other statistics) and monitors the operations status of the server.

[**Azure Policies**](#_Azure_Policy)

* [**AC.L2-3.1.12 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#monitor-and-control-remote-access-sessions)

**Azure:**

**Customer Responsibility**

* Responsible for monitoring and controlling remote access methods for customer-deployed resources.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for employing automated mechanisms to facilitate the monitoring and control of remote access methods, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to MICROSOFT ENTRA ID via SAML2.0 ticket.

**Additional Resources:**

* [Learn more on how to secure access for your remote workforce](https://docs.microsoft.com/en-us/enterprise-mobility-security/remote-work/)
* [Monitor connected remote clients for activity and status](https://docs.microsoft.com/en-us/windows-server/remote/remote-access/ras/monitoring-and-accounting/monitor-connected-remote-clients-for-activity-and-status)
* [Use Remote Access Monitoring and Accounting](https://docs.microsoft.com/en-us/windows-server/remote/remote-access/ras/monitoring-and-accounting/use-remote-access-monitoring-and-accounting)

AC.L2-3.1.13

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-17(2) | |
| **Practice:** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.  **Assessment Objectives:**  [a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and  [b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Azure Portal  Microsoft Entra ID | Load Balancer  Intune/Intune Suite Office 365 Advanced Message Encryption  Microsoft Copilot for Security Microsoft Entra ID Multi-Factor Authentication Azure VPN  Azure Bastion  Azure Firewall Azure Virtual Desktop  Windows 365 Cloud PC |

**Implementation Statement:**

**Securing Remote Sessions with Encryption**

Use [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  to manage and secure identities by requiring [single sign-on](https://azure.microsoft.com/en-us/services/active-directory/sso/) and multifactor authentication to protect your users. The recommended way to enable and use Microsoft Entra ID Multi-Factor Authentication is with Conditional Access Policies.

To learn more, see [Learn how to Create a Conditional Access Policy.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa#create-a-conditional-access-policy)

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Azure VPN – Azure Bastion – Azure Virtual Desktop**

Azure VPN gateway supports both Point-to-Site (P2S) and Site-to-Site (S2S) VPN connections. Using the Azure VPN gateway, you can scale your employee's connections to securely access both your Azure deployed resources and your on-premises resources. To access your resources deployed in Azure, remote developers could use Azure Bastion solution, instead of VPN connection to get secure shell access (RDP or SSH) without requiring public IPs on the VMs being accessed. Another way to support a remote workforce is to deploy a Virtual Desktop Infrastructure (VDI) hosted in your Azure virtual network, secured with an Azure Firewall. For example, Azure Virtual Desktop (AVD) is a desktop and app virtualization service that runs in Azure.

**Office 365 Message Encryption**

Office 365 Message Encryption is an online service that is built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection. This service includes encryption, identity, and authorization policies to help secure your email. With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization.

**Azure:**

**Customer Responsibility**

* Responsible for implementing cryptographic mechanisms (e.g., TLS) to protect remote access sessions to customer-deployed resources.

**GCCH:**

**Customer Responsibility**

Government customers are responsible for configuring their workstations to support the use of cryptography to protect the confidentiality and integrity of remote access sessions in compliance with organizational policies. Government customers are required to configure workstations to establish FIPS 140-2 compliant TLS sessions for remote access in order to retain compliance with FedRAMP requirements. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365, to VPN into the customer’s network or directly be on the network at the time of authentication.

When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections.

**Additional Resources:**

* [Learn more on how to secure access for your remote workforce](https://docs.microsoft.com/en-us/enterprise-mobility-security/remote-work/)
* Explore using [Azure Load Balancer](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview) to provide secure by default connections for virtual machines
* [Enable Microsoft Entra ID Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa)
* [Learn more on choosing the right authentication method](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn)
* [Learn more about Azure Government Cryptographic Mechanisms.](https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-plan-security)
* [Understanding Azure Virtual Desktop network connectivity](https://docs.microsoft.com/en-us/azure/virtual-desktop/network-connectivity)

AC.L2-3.1.14

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-17(3) | |
| **Practice:** Route remote access via managed access control points.  **Assessment Objectives:**  [a] managed access control points are identified and implemented; and  [b] remote access is routed through managed network access control points. | |
| **Primary Services** | **Secondary Services** |
| Azure Bastion  VPN Gateway  Intune/Intune Suite | Azure ExpressRoute  Azure Front Door  Network Security Groups  Azure Web Application Firewall  Conditional Access  Azure Virtual Desktop  Windows 365 Cloud PC |

**Implementation Statement:**

**Azure Bastion**

Using [Azure Bastion](https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp#:~:text=Using%20Azure%20Bastion%2C%20you%20can,connect%20to%20your%20Windows%20VMs.) protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. Using Azure Bastion, you can securely and seamlessly connect to your virtual machines over SSL directly in the Azure portal. When you use Azure Bastion, your VMs do not require a client, agent, or additional software.

Before you begin, verify that you have met the following criteria:

* A VNet with the Bastion host already installed.

Make sure that you have set up an Azure Bastion host for the virtual network in which the VM is located. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM in the virtual network. To set up an Azure Bastion host, see [Create a bastion host](https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal#createhost).

* A Windows virtual machine in the virtual network.
* The following required roles:
  + Reader role on the virtual machine.
  + Reader role on the NIC with private IP of the virtual machine.
  + Reader role on the Azure Bastion resource.
* Ports: To connect to Windows VM, you must have the following ports open on your Windows VM:
  + Inbound ports: RDP (3389)

**Azure Virtual Desktop**

Bring your own device (BYOD) and access your desktop and applications over the internet using an Azure Virtual Desktop. Set up Azure Virtual Desktop (formerly Windows Virtual Desktop) to enable secure remote work. Provide employees with the best virtualized experience with the only solution fully optimized for Windows 11 and Microsoft 365.

**Windows 365 Cloud PC**

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine (Cloud PCs) for your end users. Each Cloud PC is assigned to an individual user and is their dedicated Windows device. Windows 365 provides the productivity, security, and collaboration benefits of Microsoft 365.

To learn more, see:

* [Find the Right Windows 365 Cloud PC](https://www.microsoft.com/en-us/windows-365/cloud-pc-chooser)
* [Compare Plans and Pricing](https://www.microsoft.com/en-us/windows-365/business/compare-plans-pricing)
* [What is Windows 365 Enterprise?](https://learn.microsoft.com/en-us/windows-365/enterprise/overview?source=recommendations)
* [Manage Windows 365 Cloud PCs with Configuration Manager](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-cloud-pcs-using-configuration-manager)
* [Security overview for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/security-guidelines)

**VPN Gateway**

Create a VPN Gateway that lets you connect to your virtual network from a remote location. There are different configurations available for VPN gateway connections. For more information on determining which configuration best fits your needs: [Configuring a VPN Gateway.](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#configuring)

**Intune/Intune Suite**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Named Locations**

Use [Named Locations](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations) to restrict Microsoft Entra ID users and/or device groups using conditional access policies more granularly by configuring allowed IP address ranges within your organization. These named locations may include an organization’s headquarters, VPN network or additionally, ranges that you wish to block.

**Azure ExpressRoute**

Explore using [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

**Azure Web Application Firewall and Front Door**

Optimize performance with [Azure Web Application Firewall](https://azure.microsoft.com/en-us/services/web-application-firewall/) deployed with Azure Front Door. [Customize Web Application Firewall](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-customize-waf-rules-portal) rules using Azure portal. Use Azure [Front Door](https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview#:~:text=Azure%20Front%20Door%20is%20a,and%20widely%20scalable%20web%20applications.&text=Front%20Door%20provides%20a%20range,needs%20and%20automatic%20failover%20scenarios.) as a scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications.

**Azure:**

**Customer Responsibility**

* Responsible for routing remote access connections to customer-deployed resources through managed network access control points.

**GCCH:**

**Customer Responsibility**

Government customers are responsible for routing remote access traffic to Office 365 through a limited number of managed access points.

**Additional Resources:**

* [Azure Policy Regulatory Compliance controls for Azu](https://docs.microsoft.com/en-us/azure/virtual-network/security-controls-policy)re Virtual Network
* [Working with NSG access and Azure Bastion](https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg)

##### AC.L2-3.1.15

| **Control Summary Information** | |
| --- | --- |
| **NIST 800-171 Mapping:** 3.1.15 | |
| **NIST SP 800-53 Mapping:** AC-17(4) | |
| **Control**: Authorize remote execution of privileged commands and remote access to security-relevant information.  **Assessment Objectives:**  [a] privileged commands authorized for remote execution are identified; [b] security-relevant information authorized to be accessed remotely is identified; [c] the execution of the identified privileged commands via remote access is authorized; and  [d] access to the identified security-relevant information via remote access is authorized. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Privileged Identity Management (PIM)  Microsoft Purview  Azure RBAC | Intune/Intune Suite  Named Locations  Azure Virtual Machines  Windows 365 Cloud PC  Conditional Access  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID Role Based Access Control**

Microsoft Azure offers a robust security set for employing the principle of least privilege. Best practice recommendation is to segregate duties within your team by setting up [Role Based Access](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) (RBAC) which will help you manage who has access to Azure resources. More granularity, you can restrict what the users can do with the resources and what areas they have access to.

**Privileged Identity Management**

Additionally, you can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with access to the most privileged access, resources, and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Intune/Intune Suite and Compliance Retrieval/NAC 2.0 s**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Use [Named Locations](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations) to restrict Microsoft Entra ID users and/or device groups using conditional access policies more granularly by configuring allowed IP address ranges within your organization. These named locations may include an organization’s headquarters, VPN network or additionally, ranges that you wish to block.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection - Microsoft Purview (compliance)](https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

**Azure:**

**Customer Responsibility**

* Responsible for authorizing privileged commands and access to security-relevant information via remote access for customer-deployed resources.

**GCCH:**

**Customer Responsibility**

* Can be inherited from Cloud Service Provider

**Can Be Inherited from CSP**

**Additional Resources**

* Explore the use of [Just Enough Administration](https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.1) (JEA) to further limit admin accounts. There are [prerequisites](https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/prerequisites?view=powershell-7.1) to using JEA.

AC.L2-3.1.16

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-18 | |
| **Practice:** Authorize wireless access prior to allowing such connections.  **Assessment Objectives:**  [a] wireless access points are identified; and  [b] wireless access is authorized prior to allowing such connections. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite | Conditional Access  Compliance Retrieval/NAC 2.0 |

**Implementation Statement:**

**Intune/Intune Suite**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Azure:**

**Customer Responsibility**

* Authorizing wireless access prior to allowing such connections to customer-deployed resources.

**GCCH:**

**Customer Responsibility**

* Office 365 does not distinguish between wireless and non-wireless customer access. If government customers using ADFS wish to prevent wireless customer access, they can do so by configuring ADFS to only allow connections from domain-joined machines on a non-wireless network.

AC.L2-3.1.17

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-18(1) | |
| **Practice:** Protect wireless access using authentication and encryption.  **Assessment Objectives:**  [a] wireless access to the system is protected using authentication; and  [b] wireless access to the system is protected using encryption. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite | Conditional Access  Compliance Retrieval/NAC 2.0 |

**Implementation Statement:**

**Wireless Access**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Additionally, using Microsoft Intune built-in Wi-Fi settings called a “profile,” you can deploy specific Wi-Fi connection requirements to users with supported devices in your organization. [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  offers many features, including authenticating to your network, using a pre-shared key for encryption and more.

**GCCH:**

**Customer Responsibility**

* Office 365 does not distinguish between wireless and non-wireless customer access. If government customers using ADFS wish to allow wireless customer access and authenticate devices and users, they are responsible for configuring their ADFS infrastructure to perform this authentication.

**Additional Resources**

* [Supported device platforms & creating Intune Wi-Fi profile](https://docs.microsoft.com/en-us/mem/intune/configuration/wi-fi-settings-configure)
* [Requiring multi-factor authentication for Intune device enrollments](https://docs.microsoft.com/en-us/mem/intune/enrollment/multi-factor-authentication)
* [Adding Wi-Fi settings for Windows 10 and newer devices in Intune](https://docs.microsoft.com/en-us/mem/intune/configuration/wi-fi-settings-windows)

##### AC.L2-3.1.18

| **Control Summary Information** | |
| --- | --- |
| **NIST 800-171 Mapping:** 3.1.18 | |
| **NIST SP 800-53 Mapping:** AC-19 | |
| **Practice:** Control connection of mobile devices.  **Assessment Objectives:**  [a] mobile devices that process, store, or transmit CUI are identified;  [b] mobile device connections are authorized; and  [c] mobile device connections are monitored and logged. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite  Microsoft 365 Defender | Microsoft 365 Admin Center  Microsoft Defender for Endpoint  conditional access  Compliance Retrieval/NAC 2.0 |

**Implementation Statement:**

**Intune/Intune Suite**

Mobile Application Management (MAM) app protection policies allow you to manage and protect your organization's data within an application. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any [device](https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform), including personal devices in bring-your-own-device (BYOD) scenarios. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of [Microsoft Intune protected apps](https://docs.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps) available for public use.

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Exchange Active Sync**

As an administrator, you can turn mobile access on or off, and remotely manage some phone features or options. For example, you can require passwords for your users’ devices. When mobile access is turned on, users can configure their Windows Phone, iPhone, iPad, Android phone, BlackBerry®, or other phone or tablet to send and receive Microsoft 365 email and access calendar and contacts information.

Your users can also access their email on their phone or tablet by signing into Outlook Web App. Exchange ActiveSync, which is turned on by default, turns on mobile access for Windows Phone, Apple iPhone and iPad, Android phones, and BlackBerry devices. You can turn this access off via the Microsoft 365 Portal>Admin>Exchange>Mobile>Mobile Device Access.

**Azure:**

**Customer Responsibility**

* Controlling connection of mobile devices to customer-deployed resources.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for establishing usage restrictions, configuration and connection requirements, and implementation guidance for organization-controlled mobile devices used to connect to Office 365.

**Additional Resources**

* [How to create and deploy app protection policies with Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies)
* [Available Android app protection policy settings with Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android)
* [Available iOS/iPadOS app protection policy settings with Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios)
* [Configure device discovery -Microsoft 365 Defender](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-device-discovery?view=o365-worldwide)

AC.L2-3.1.19

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-19(5) | |
| **Practice:** Encrypt CUI on mobile devices and mobile computing platforms.  **Assessment Objectives:**  [a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; and  [b] encryption is employed to protect CUI on identified mobile devices and mobile  computing platforms. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite  Microsoft Purview | Conditional Access  Microsoft Defender for Endpoint |

**Implementation Statement:**

**Intune/Intune Suite**

Using Intune combined with the native polices and configuration options in Azure, users can set device compliance policies and configure [conditional access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-compliant-device) to deny access to unencrypted devices to your systems, ensuring compliance with this specific Control . This in addition to data and file encryption applied through Microsoft Information Protection allows organizations to encrypt the data and the container on mobile devices.

Encrypt CUI on mobile devices and mobile computing platforms [using Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager)  with Conditional access to require encryption, such as [BitLocker](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows) for Windows 10 and later. [Require app protection policy](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-protection-based-conditional-access) and an approved client app for cloud app access. Create and assign [Microsoft Intune app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies) to ensure that apps are protected with a PIN and Encrypted.

See the [Android app protection policy settings](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android) and [iOS/iPadOS app protection policy settings](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios) for detailed information on the encryption app protection policy setting.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

Automatically protect sensitive information from risky and unauthorized access across apps, services, endpoints, and on-premises files.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Learn about other Microsoft Purview products available:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Additional Resources**

* [Data protection framework using app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-framework)

AC.L1-3.1.20

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-20, AC-20(1) | |
| **Practice:** Verify and control/limit connections to and use of external information systems.  **Assessment Objectives:**  [a] connections to external systems are identified;  [b] the use of external systems is identified;  [c] connections to external systems are verified;  [d] the use of external systems is verified;  [e] connections to external systems are controlled/limited; and  [f] the use of external systems is controlled/limited. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure Firewall  Conditional Access  Network Security Groups  Microsoft Defender for Cloud Apps  Intune/Intune Suite  Microsoft 365 Defender | Microsoft Azure Portal  Microsoft Purview  Microsoft Defender for IoT |

**Implementation Statement:**

**Microsoft Entra ID & Conditional Access**

[Block access by location with Microsoft Entra ID Conditional access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location) to control and limit connections to and use of external information systems. For more information about Conditional Access, see the [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/) documentation.

**Requirements**

* A subscription to [Microsoft Entra ID Premium](https://www.microsoft.com/cloud-platform/azure-active-directory)
* A federated Microsoft Entra ID tenant. See [What is Conditional Access?](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview)

**Conditional Access**

Conditional access policies can be integrated with Defender for Cloud Apps to provide controls for cloud and on-premises applications from external systems. Mobile application management in Intune can protect organization data at the application level, including custom apps and store apps, from managed devices that interact with external systems. An example would be accessing cloud services. You can use app management on organization-owned devices and personal devices.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Microsoft Defender for Cloud Apps**

App connectors use the APIs of app providers to enable greater visibility and control by Microsoft Defender for Cloud Apps over the apps you connect to. [Learn how App Connectors work](https://docs.microsoft.com/en-us/cloud-app-security/enable-instant-visibility-protection-and-governance-actions-for-your-apps#how-it-works) providing you with control of your App environment.

**Microsoft Defender for IoT**

[Microsoft Defender for IoT](https://azure.microsoft.com/en-us/services/azure-defender-for-iot/) provides continuous asset discovery, vulnerability management, and threat detection for your Internet of Things (IoT) and operational technology (OT) devices and helps meet this requirement for visibility of connections to external information systems.

Microsoft Defender for IoT interoperates with Microsoft Sentinel which collects data across all users, devices, applications, and infrastructure, both on-premises and in the cloud to support monitoring requirements.

**Azure:**

**Customer Responsibility**

* Responsible for establishing terms and conditions allowing authorized individuals to access the customer-deployed resources from external information systems.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for verifying the implementation of organizationally required security controls on customer workstations, including W365 virtual machines, in compliance with organizational policies.
* Government customers are responsible for establishing terms and conditions allowing authorized individuals to access Office 365 from customer-controlled networks and workstations.

**Additional Resources**

* [Restrict your Microsoft Entra ID app to a set of users in an Microsoft Entra ID tenant](https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-restrict-your-app-to-a-set-of-users#update-the-app-to-enable-user-assignment)
* [Configure authentication session management with conditional access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime)
* [Azure Government – trusted cloud for US Government requirements](https://azure.microsoft.com/en-us/global-infrastructure/government/get-started/)
* [How to manage devices using the Azure Portal](https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal)
* [Connect Azure to](https://docs.microsoft.com/en-us/cloud-app-security/connect-azure-to-microsoft-cloud-app-security) Microsoft Defender for Cloud Apps
* [Require device to be marked as compliant](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices)
* [Conditions in Conditional Access policy - Device State (Preview)](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions)
* [Protect with Microsoft Defender for Cloud Apps Conditional Access App Control](https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad)
* [Location condition in Microsoft Entra ID Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition)

##### AC.L2-3.1.21

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-20(2) | |
| **Practice:** Limit use of portable storage devices on external systems.  **Assessment Objectives:**  [a] the use of portable storage devices containing CUI on external systems is identified and documented;  [b] limits on the use of portable storage devices containing CUI on external systems are defined; and  [c] the use of portable storage devices containing CUI on external systems is limited as defined. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite  Microsoft Defender for Endpoint  Microsoft 365 Defender | Named Locations  Conditional Access  Microsoft Entra ID |

**Implementation Guidance:**

Clearly define the use of portable storage and where such devices can and cannot be used. Further, apply technical controls where possible to restrict and control the use of portable devices.

* Define corporate compliance policies for portal storage devices such as, but not limited to:
  + floppy disks;
  + compact/digital video disks (CDs/DVDs);
  + flash/thumb drives;
  + external hard disk drives; and
  + flash memory cards/drives that contain nonvolatile memory.
* Apply technical controls, such as data loss controls, encryption, or device state configuration requirements

**Microsoft Defender for Endpoint**

Microsoft Defender for Endpoint, Device Control Removable Storage Access Control, enables you to prevent the read, write or execute access to removable storage with or without exclusion. The Microsoft 365 Defender portal shows events triggered by the Device Control Removable Storage Access Control.

To learn more see, [Microsoft Defender for Endpoint Device Control Removable Storage Access Control.](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-removable-storage-access-control?view=o365-worldwide)

**Microsoft Intune**

Microsoft's primary MDM tool is [Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/). Intune is part of a larger Microsoft MDM platform called [Microsoft Endpoint Manager](https://docs.microsoft.com/en-us/mem/intune/).

Using Intune, administrators can enroll, configure, and manage mobile devices on several different operating system platforms, wherever the devices happen to be. Administrators can even intervene when a threat to security occurs, by blocking a device’s access to the company network and erasing any sensitive information stored on it.

Organizations can configure policies to allow, block and restrict USB drives and other peripherals.

Organizations can allow users to install only the USB drives and other peripherals included on a list of authorized devices or device types or prevent users from installing USB drives and other peripherals included on a list of unauthorized devices and device types.

Additionally, using Intune, you can apply device configuration policies to Microsoft Entra ID user and/or device groups. The policies can also be set through the [Device Installation CSP settings](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceinstallation) and the [Device Installation GPOs](https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530324(v=msdn.10)). To protect your devices and corporate resources, you can use Microsoft Entra ID Conditional Access policies with Intune.

Intune passes the results of your device compliance policies to Microsoft Entra ID , which then uses conditional access policies to enforce which devices and apps can access your corporate resources.

Additionally, when managing devices in your organization, you want to create groups of settings that apply to different device groups. To prevent malware infections or data loss in your organization, you may want to block certain kinds of USB devices, such as a USB flash drive or camera, and allow other kinds of USB devices, such as a keyboard or mouse. Further, you may want to allow USB devices by specific device IDs. You can complete this task using [Administrative Templates](https://docs.microsoft.com/en-us/troubleshoot/mem/intune/restrict-usb-with-administrative-template) in Intune. The templates are built into Intune and do not require customization.

**Named Locations**

Use [Named Locations](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations) to restrict Microsoft Entra ID users and/or device groups using conditional access policies more granularly by configuring allowed IP address ranges within your organization. These named locations may include an organization’s headquarters, VPN network or additionally, ranges that you wish to block.

**Azure:**

**Customer Responsibility**

* Limiting the use of portable storage devices on customer-deployed resources (e.g., laptops).

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for limiting the use of organization-controlled portable storage media by authorized individuals on customer workstations connected to Office 365 in compliance with organizational policies.

**Additional Resources**

* [Block installation and usage of removable storage](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#block-installation-and-usage-of-removable-storage)
* [Use Windows 10 templates to configure group policy settings in Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows)
* [Microsoft Defender for Endpoint Device Control Removable Storage Access Control](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-removable-storage-access-control?view=o365-worldwide)

AC.L1-3.1.22

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AC-22 | |
| **Practice:** Control information posted or processed on publicly accessible  information systems.  **Assessment Objectives:**  [a] individuals authorized to post or process information on publicly accessible systems are identified;  [b] procedures to ensure FCI is not posted or processed on publicly accessible systems are identified;  [c] a review process is in place prior to posting of any content to publicly accessible  systems;  [d] content on publicly accessible systems is reviewed to ensure that it does not include FCI; and  [e] mechanisms are in place to remove and address improper posting of FCI. | |
| **Primary Services** | **Secondary Services** |
| Conditional Access  Microsoft Purview  Intune/Intune Suite | Compliance Retrieval/NAC 2.0  Exchange Admin Center  M365 Compliance Center  Microsoft Defender for Cloud App |

**Implementation Statement:**

**Intune/Intune Suite**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Further, Intune can be configured to restrict the copying of data to publicly accessible information systems. [Configure Intune to prevent data leaks](https://docs.microsoft.com/en-us/mem/intune/protect/data-leak-prevention) on non-managed devices and setup [app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy) to secure company data on user-owned devices.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

Discover, identify, classify, and protect sensitive data that is critical to business, then manage and protect it across your environment.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Learn about other Microsoft Purview products available:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Microsoft Defender for Cloud Apps**

Microsoft Defender for Cloud Apps lets you apply Microsoft Information Protection classification labels automatically, with or without protection, to files as a file policy governance action. You can also investigate files by filtering for the applied classification label within the Cloud App Security portal. Using classifications enables greater visibility and control of your sensitive data in the cloud. To learn more see, How to integrate [Microsoft Information Protection with Cloud App Security.](https://docs.microsoft.com/en-us/cloud-app-security/azip-integration#how-to-integrate-azure-information-protection-with-cloud-app-security)

**Azure:**

**Customer Responsibility**

* Responsible for designating authorized personnel to post publicly accessible information on customer-deployed resources.

**Additional Resources**

* [Microsoft Defender for Cloud Apps Overview](https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security)
* [Get started with](https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security) Microsoft Defender for Cloud Apps
* [Deploying the Microsoft Information Protection scanner to automatically classify and protect files](https://docs.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner-configure-install).
* [How to configure a label for Rights Management protection](https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection)
* [What is Microsoft Information Protection?](https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection) [Data loss prevention reference](https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide)

### Awareness and Training (AT)

AT.L2-3.2.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AT-2, AT-3 | |
| **Practice:** Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.  **Assessment Objectives:**  a] security risks associated with organizational activities involving CUI are identified;  [b] policies, standards, and procedures related to the security of the system are identified;  [c] managers, systems administrators, and users of the system are made aware of the  security risks associated with their activities; and  [d] managers, systems administrators, and users of the system are made aware of the  applicable policies, standards, and procedures related to the security of the system. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft 365 Defender  Microsoft Entra ID  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft Defender for Identity  Microsoft 365 Web Apps  Teams |

**Implementation Statement:**

**Teams**

Viva Learning is a centralized learning hub in Microsoft Teams that lets you seamlessly integrate learning and building skills into your day. In Viva Learning, your team can discover, share, recommend, and learn from content libraries provided by both your organization and partners.

**Azure**

**Customer Responsibility**

* Providing role-based security training to users before authorizing access to customer-deployed resources or performing assigned duties.
* Providing role-based security training to all identified roles when required by changes to customer-deployed resources.
* Providing ongoing, periodic role-based security training to all identified roles.

**GCCH:**

**Customer Responsibility**

* Government customers are responsible for providing security awareness training to their employees and vendors as necessary, including training on security awareness training and role-based training, as appropriate per job description. This training shall include requirements that customer users not bypass Office 365 security through actions such as:  
  1. Improperly forwarding documentation through Exchange Online  
  2. Circumventing, disabling, or downgrading session-level encryption
* Government customers should provide security awareness training to their users that includes content related to recognizing and reporting potential indicators of insider threat.

AT.L2-3.2.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AT-2, AT-3 | |
| **Practice:** Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.  **Assessment Objectives:**  [a] information security-related duties, roles, and responsibilities are defined;  [b] information security-related duties, roles, and responsibilities are assigned to  designated personnel; and  [c] personnel are adequately trained to carry out their assigned information security related duties, roles, and responsibilities. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Defender for Office 365 Microsoft Learn  Microsoft 365 Defender portal (Learning Hub) |

**Implementation Statement:**

**Microsoft Defender for Office 365**

If your organization has Microsoft Defender for Office 365 Plan 2, which includes [Threat Investigation and Response capabilities](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide), you can use Attack Simulator in the M365 Compliance Center to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

Attack simulation training in Microsoft Defender for Office 365 lets you run benign cyberattack simulations on your organization to test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks. For getting started information about Attack simulation training, see [Get started using Attack simulation training](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide).

**Microsoft Learn**

Whether you're just starting or an experienced professional, Microsoft Learn helps organizations train their personnel on role based and security-related duties. To start learning, visit the [Microsoft Learn](https://docs.microsoft.com/en-us/learn/) page.

**Azure:**

**Azure**

**Customer Responsibility**

* Providing role-based security training to users before authorizing access to customer-deployed resources or performing assigned duties.
* Providing role-based security training to all identified roles when required by changes to customer-deployed resources.
* Providing ongoing, periodic role-based security training to all identified roles.

**GCCH**

**Customer Responsibility:**

* Government customers are responsible for providing role-based training to their employees and vendors as necessary, including training on basic security awareness training and role-based training, as appropriate per job description. This training shall include requirements that customer users not bypass Office 365 security through actions such as:  
  1. Improperly forwarding documentation through Exchange Online  
  2. Circumventing, disabling, or downgrading session-level encryption.

AT.L2-3.2.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AT-2(2) | |
| **Practice:** Provide security awareness training on recognizing and reporting potential indicators of insider threat.  **Assessment Objectives:**  [a] potential indicators associated with insider threats are identified; and  [b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Defender for Office 365 Microsoft Learn  Microsoft 365 Defender portal (Learning Hub) |

**Implementation Statement:**

If your organization has Microsoft Defender for Office 365 Plan 2, which includes [Threat Investigation and Response capabilities](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide), you can use Attack Simulator in the M365 Compliance Center to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

Attack simulation training in Microsoft Defender for Office 365 lets you run benign cyberattack simulations on your organization to test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks. For getting started information about Attack simulation training, see [Get started using Attack simulation training](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide).

**Azure**

**Customer Responsibility**

* Providing training on insider threats.

**GCCH**

**Customer Responsibility:**

Government customers should provide security awareness training to their users that includes content related to recognizing and reporting potential indicators of insider threat.

### Audit and Accountability (AU)

AU.L2-3.3.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12 | |
| **Practice:** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.  **Assessment Objectives:**  [a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified;  [b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined;  [c] audit records are created (generated);  [d] audit records, once created, contain the defined content;  [e] retention requirements for audit records are defined; and  [f] audit records are retained as defined. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel  Microsoft Defender for Cloud Apps  Microsoft Defender for Cloud  Log Analytics Workspace  Microsoft Entra ID  Intune/Intune Suite  Microsoft 365 compliance center  Azure Storage  Microsoft 365 Defender | Azure Firewall  Azure Web Application Firewall  Microsoft Defender for Office 365  GitHub Enterprise Cloud  GitHub AE  Windows 365 Cloud PC  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID**

You can retain the audit and sign-in activity data for longer than the default retention period outlined [here](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention) by routing it to an Azure storage account using Azure Monitor. To learn more, see [Archive Microsoft Entra ID logs to an Azure storage account](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-azure-monitor-route-logs-to-storage-account).

**Microsoft Defender for Cloud**

[Microsoft Defender for Cloud](https://azure.microsoft.com/en-us/services/azure-defender/#:~:text=Use%20Azure%20Defender%2C%20integrated%20with,force%20attacks%2C%20and%20SQL%20injections.) protects your Virtual Machines, data, storage and cloud native services against common threats. Go to [Microsoft Defender for Cloud](https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/0) to turn on protection for your hybrid cloud workloads. You can also protect users, devices and applications with [Microsoft defender](https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description) for O365 and bring all your security analytics together into a unified view by [connecting data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Microsoft Sentinel. Microsoft Sentinel's audit logs are maintained in the [Azure Activity Logs](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/platform-logs-overview), where the Azure Activity table includes all actions taken in your Microsoft Sentinel workspace.

To learn more, see [Integrated Threat Protection from Microsoft](https://www.microsoft.com/en-us/security/business/threat-protection?rtc=1).

**Intune/Intune Suite**

By default, auditing in [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  is enabled for all customers. This allows an organization’s administrator to track and monitor events in Microsoft Intune. Audit logs include a record of activities, such as; create, update (edit), delete, assign, and remote actions all create audit events that administrators can review.

Logs can also be sent to [Azure Monitor](https://azure.microsoft.com/en-us/services/monitor/) services, including [storage accounts, event hubs, and log analytics](https://docs.microsoft.com/en-us/mem/intune/fundamentals/review-logs-using-azure-monitor). For more information: [use audit logs to track and monitor events in Microsoft Intune.](https://docs.microsoft.com/en-us/mem/intune/fundamentals/monitor-audit-logs#:~:text=Audit%20logs%20include%20a%20record,It%20can't%20be%20disabled.)

**Microsoft Sentinel & Microsoft Copilot for Security**

Additionally, consider using Microsoft Sentinel as your Security Information and Event Management (SIEM) solution. After you [connect your data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources)to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks. While Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to [Create interactive reports with Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview).

Once Microsoft Sentinel is enabled on your Azure Monitor Log Analytics workspace, every GB of data ingested into the workspace can be retained at no charge for a default retention limit. For more information on free retention limits and retention costs beyond that limit, please refer to [Azure Monitor Log Analytics](https://azure.microsoft.com/en-us/pricing/details/log-analytics/) retention prices.

Microsoft Copilot for Security can access data from Microsoft Sentinel to increase the effectiveness and efficiency of security professionals using those solutions. Microsoft Defender XDR and Microsoft Sentinel become even more powerful when security professionals use Copilot for Security. Copilot for Security delivers an experience that enriches and builds on the security data, signals, and existing incidents and insights sourced from Microsoft Defender XDR and Microsoft Sentinel.

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3)

**M365 Compliance Center**

You can create and manage audit log retention policies in the Microsoft 365 compliance center. Audit log retention policies are part of the new Advanced Audit capabilities in Microsoft 365. An audit log retention policy lets you specify how long to retain audit logs in your organization. You can retain audit logs for up to 10 years. Advanced Audit in Microsoft 365 provides a default audit log retention policy for all organizations. This policy retains all Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Entra ID audit records for one year.

Enable auditing of admin activity in [M365 Compliance Center](https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center). [Enabling auditing for admins](https://support.microsoft.com/en-us/topic/auditing-in-office-365-for-admins-9f6484d2-0fd2-17de-165f-c41346023906) allows you to capture user and administrator activities in your organization.

[Audited Activities](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#audited-activities) in M365 Compliance Center can be granularly selected. It is recommended to review audit logs at a frequency to meet your compliance requirements. This will assist in discovering execution of privileged functions.

[**Azure Policies**](#_Azure_Policy)

* [**AU.L2-3.3.1 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#create-and-retain-system-audit-logs-and-records-to-the-extent-needed-to-enable-the-monitoring-analysis-investigation-and-reporting-of-unlawful-or-unauthorized-system-activity)

**Azure**

**Customer Responsibility**

* Retaining audit records for customer-deployed resources to support security investigations and meet regulatory requirements. Audit records must be retained for the defined frequency.
* Ensuring all customer-deployed resources have the ability to generate records for the auditable events

**GCCH**

**Customer Responsibility:**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for retaining audit records for at least one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
* Government customers using ADFS are responsible for generating audit events for account creation, modification, disabling, and deletion activities for their Active Directory infrastructure as these events also pertain to Office 365 access.

**Customer Responsibility (W365):**Government customers using Windows 365 are responsible for configuring audit policies on their VMs that meet organizational and compliance requirements.

**Additional Resources**

* [Microsoft Defender for Identity Prerequisites](https://docs.microsoft.com/en-us/defender-for-identity/prerequisites)
* [Move your Microsoft Sentinel Logs to Long-Term Storage with Ease](https://techcommunity.microsoft.com/t5/azure-sentinel/move-your-azure-sentinel-logs-to-long-term-storage-with-ease/ba-p/1407153#:~:text=Out%20of%20the%20box%2C%20Azure,to%207%20years%20or%20longer.)
* [Manage cost by controlling data volume and retention in Log Analytics](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-manage-cost-storage)
* [Storage size for activity logs](https://docs.microsoft.com/en-us/mem/intune/fundamentals/review-logs-using-azure-monitor#storage-size-for-activity-logs)
* [Archive activity logs to a storage account](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-azure-monitor-route-logs-to-storage-account)
* [Route activity logs to an event hub](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub)
* [Integrate activity logs with Log Analytics](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics)

AU.L2-3.3.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12 | |
| **Practice:** Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.  **Assessment Objectives:**  [a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and  [b] audit records, once created, contain the defined content. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel  M365 Compliance Center  Microsoft Entra ID | Intune/Intune Suite  Microsoft 365 Defender  Windows 365 Cloud PC  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Sentinel & Microsoft Copilot for Security**

All account lifecycle operations (account creation, modification, enabling, disabling, and removal actions) and user activity in the Azure portal are audited within the Microsoft Entra ID audit logs. All authentication and authorization events are audited within Microsoft Entra ID sign-in logs, and any detected risks are audited in the Identity Protection logs. Stream logs to directly Microsoft Sentinel Security Information and Event Management (SIEM) solution by [connecting data from Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-active-directory)

[Visualize and monitor log data](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data)  using Microsoft Sentinel which allows you to [create custom workbooks](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data#create-new-workbook) across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Connect logs from sources such as, Microsoft Entra ID , Microsoft Defender for Endpoint, O365 and Intune to Sentinel for optimal visibility of your users’ activities. Learn more on how to [connect your sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Sentinel to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Additionally, Microsoft Copilot for Security can access data from Microsoft Sentinel to increase the effectiveness and efficiency of security professionals using those solutions. Microsoft Defender XDR and Microsoft Sentinel become even more powerful when security professionals use Copilot for Security. Copilot for Security delivers an experience that enriches and builds on the security data, signals, and existing incidents and insights sourced from Microsoft Defender XDR and Microsoft Sentinel.

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3)

**M365 Compliance Center**

By default, audit logging is on for Microsoft 365 and Office 365 enterprise organizations. If audit log search is not turned on, you can [turn it on in compliance center or by using Exchange Online PowerShell](https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide#turn-on-audit-log-search). Audit user activity with [M365 Compliance Center](https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center).

Audit [user and admin activity](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#audited-activities) in M365 Compliance Center. It is recommended to review audit logs at a frequency to meet your compliance requirements. [Enable the Office 365 log connector](https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365#enable-the-office-365-log-connector) to connect Office 365 to Microsoft Sentinel. This will enable you to view and analyze this data in your workbooks, query it to create custom alerts, and incorporate it to improve your investigation process, giving you more insight into your Office 365 security.

**Intune/Intune Suite Audit Logging**

By default, auditing in [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  is enabled for all customers. This allows an organization’s administrator to track and monitor events in Microsoft Intune. Audit logs include a record of activities, such as; create, update (edit), delete, assign, and remote actions all create audit events that administrators can review.

Logs can also be sent to [Azure Monitor](https://azure.microsoft.com/en-us/services/monitor/) services, including [storage accounts, event hubs, and log analytics](https://docs.microsoft.com/en-us/mem/intune/fundamentals/review-logs-using-azure-monitor). For more information: [use audit logs to track and monitor events in Microsoft Intune.](https://docs.microsoft.com/en-us/mem/intune/fundamentals/monitor-audit-logs#:~:text=Audit%20logs%20include%20a%20record,It%20can't%20be%20disabled.)

**Windows 365 Cloud PC**

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine (Cloud PCs) for your end users. Each Cloud PC is assigned to an individual user and is their dedicated Windows device. Windows 365 provides the productivity, security, and collaboration benefits of Microsoft 365.

To learn more, see:

* [Find the Right Windows 365 Cloud PC](https://www.microsoft.com/en-us/windows-365/cloud-pc-chooser)
* [Compare Plans and Pricing](https://www.microsoft.com/en-us/windows-365/business/compare-plans-pricing)
* [What is Windows 365 Enterprise?](https://learn.microsoft.com/en-us/windows-365/enterprise/overview?source=recommendations)
* [Manage Windows 365 Cloud PCs with Configuration Manager](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-cloud-pcs-using-configuration-manager)
* [Security overview for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/security-guidelines)

**Microsoft Compliance Center - eDiscovery & Audit**

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft 365 to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can use Core eDiscovery cases to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the feature-rich Advanced eDiscovery solution in Microsoft 365.

Moreover, The Audit functionality in Microsoft 365 provides organizations with visibility into many types of audited activities across many different services in Microsoft 365. Basic Audit provides you with the ability to log and search for audited activities and power your forensic, IT, compliance, and legal investigations. Advanced Audit builds on the capabilities of Basic Audit by providing audit log retention policies, longer retention of audit records, high-value crucial events, and higher bandwidth access to the Office 365 Management Activity API.

[**Azure Policies**](#_Azure_Policy)

* [**AU.L2-3.3.2 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#ensure-that-the-actions-of-individual-system-users-can-be-uniquely-traced-to-those-users-so-they-can-be-held-accountable-for-their-actions)

**Azure**

**Customer Responsibility**

* Configuring Azure auditing capabilities on customer-deployed resources to generate audit records containing the following: what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any subjects associated with the event.

**GCCH**

**Customer Responsibility:**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these government customers are responsible for capturing what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Government customers using Windows servers to support their ADFS infrastructure automatically meet this requirement as Windows captures these event details by default.

**Customer Responsibility (W365):**

* Government customers using Windows 365 are responsible for configuring audit policies on their VMs that meet organizational and compliance requirements.

**Additional Resources**

* [Create interactive reports with Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview)
* [Microsoft Sentinel and Microsoft Defender for Cloud Apps integration](https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel)
* [Find activity reports in the Azure portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-find-activity-reports)
* [Audit activity reports in the Microsoft Entra ID portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs)
* [Sign-in activity reports in the Microsoft Entra ID portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins)
* [How To: Investigate risk](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk)
* [Stream to Azure event hub and other SIEMs](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub)
* Learn how to [get visibility into your data and potential threats](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility)
* Get started detecting threats with Microsoft Sentinel, using [built-in](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in) or [custom](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom) rules
* [Enabling auditing for admins](https://support.microsoft.com/en-us/topic/auditing-in-office-365-for-admins-9f6484d2-0fd2-17de-165f-c41346023906)
* [How to monitor virtual machines in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/monitor)
* [How to onboard Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard)
* [Understand Log Analytics Workspace](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial)
* [How to perform custom queries in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries)

AU.L2-3.3.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-2 | |
| **Practice:** Review and update logged events.  **Assessment Objectives:**  [a] a process for determining when to review logged events is defined;  [b] event types being logged are reviewed in accordance with the defined review process; and  [c] event types being logged are updated based on the review | |
| **Primary Services** | **Secondary Services** |
| Azure Monitor  Microsoft Sentinel  Microsoft Purview | Microsoft Entra ID  Intune/Intune Suite  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Exchange admin center  Microsoft 365 Defender |

**Implementation Statement:**

**Microsoft Sentinel**

Review audit logged events at a defined frequency that meets Organizational requirements for example, at least annually or when changes occur. Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient. Your organization should have a defined process for determining when to review logged events and the event types should be updated based on that review. You can [connect your log sources to](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) Microsoft Sentinel to review audit logs in one centralized location. Additionally, you can review Incident reports to determine if a specific occurrence should be audited. For example, if your company experiences a security incident, and a forensics review shows the logs appear to have been deleted by a remote user. You notice that remote sessions are not currently being logged so you update the list of events to include logging all VPN sessions.

[Visualize and monitor log data](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data)  using Microsoft Sentinel which allows you to [create custom workbooks](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data#create-new-workbook) across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Connect logs from sources such as Microsoft Entra ID, Microsoft Defender, O365 and Intune to Sentinel for optimal visibility of your users’ activities. Learn more on how to [connect your sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Sentinel to support reviewing and updating logged events.

**Microsoft Purview**

Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Azure**

**Customer Responsibility**

* Reviewing and updating the customer-defined events for customer-deployed resources.
* Defining a process for determining when to review logged events to ensure that the current set remains necessary and sufficient. (i.e., regular frequency, after incidents, after major system changes)
* Defining and updating event log types to ensure that the current set remains necessary and sufficient.

**GCCH**

**Customer Responsibility**

* Can be inherited from Cloud Service Provider

**Additional Resources**

* [Azure Activity Log event schema - Azure Monitor](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema)
* [CMMC L2 Requirements](https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf)
* [Azure Monitoring Contributor](https://docs.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security) for creating, modifying, and updating log alerts
* [Create interactive reports with Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview)
* [Microsoft Sentinel and Microsoft Defender for Cloud Apps integration](https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel)
* [Find activity reports in the Azure portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-find-activity-reports).
* [Audit activity reports in the Microsoft Entra ID portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs)
* [Sign-in activity reports in the Microsoft Entra ID portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins)
* [How To: Investigate risk](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk)
* [Stream to Azure event hub and other SIEMs](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub)
* Learn how to [get visibility into your data and potential threats](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility)
* Get started detecting threats with Microsoft Sentinel, using [built-in](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in) or [custom](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom) rules
* [Enabling auditing for admins](https://support.microsoft.com/en-us/topic/auditing-in-office-365-for-admins-9f6484d2-0fd2-17de-165f-c41346023906)
* [How to monitor virtual machines in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/monitor)
* [What is Microsoft Sentinel?](https://docs.microsoft.com/en-us/azure/sentinel/overview)
* [Get started with log queries in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries)
* [Visualize and monitor your data](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data#prerequisites)
* Microsoft Defender for Cloud Apps
* [Turn on Microsoft 365 Defender](https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-enable?view=o365-worldwide)
* [Microsoft 365 security center overview](https://docs.microsoft.com/en-us/microsoft-365/security/defender/overview-security-center?view=o365-worldwide)

AU.L2-3.3.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-5 | |
| **Practice:** Alert in the event of an audit logging process failure.  **Assessment Objectives:**  [a] personnel or roles to be alerted in the event of an audit logging process failure are  identified;  [b] types of audit logging process failures for which alert will be generated are defined; and  [c] identified personnel or roles are alerted in the event of an audit logging process failure. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel | Microsoft Entra ID  Microsoft Graph  Power Automate  Log Analytics  Azure Monitor  Azure Functions |

**Implementation Statement:**

**Microsoft Sentinel**

Connected logs from sources such as, Microsoft Entra ID , Azure Monitor, O365 and Intune to Sentinel provide visibility of process failure. Learn more on how to [connect your sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Sentinel. Microsoft Sentinel classifies failures up front as either transient or permanent, based on the specific type of failure and the circumstances that led to it. [Learn more about scheduled rule failures.](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#issue-a-scheduled-rule-failed-to-execute-or-appears-with-auto-disabled-added-to-the-name) To view the results of the alert rules you create, go to the Incidents page, where you can triage, [investigate incidents](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases), and remediate the threats. Alerts generated in Microsoft Sentinel are available through [Microsoft Graph Security](https://docs.microsoft.com/en-us/graph/security-concept-overview). To learn more, see the [Microsoft Graph Security alerts documentation](https://docs.microsoft.com/en-us/graph/api/resources/security-api-overview).

**Log Alerts**

Log alerts are one of the alert types that are supported in [Azure Alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview). Log alerts allow you to use a [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial) query to evaluate resources logs every set frequency, and fire an alert based on the results. Rules can trigger one or more actions using [Action Groups](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups).

Log alerts run queries on Log Analytics data. First you should start [collecting log data](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs) and query the log data for issues. You can use the [alert query examples article](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/example-queries) in Log Analytics to understand what you can discover or [get started on writing your own query](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial).

[Azure Monitoring Contributor](https://docs.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security) is a common role that is needed for creating, modifying, and updating log alerts. Access & query execution rights for the resource logs are also needed. Partial access to resource logs can fail queries or return partial results. [Learn more about configuring log alerts in Azure](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log).

Create [custom analytics rules](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#define-the-rule-query-logic-and-configure-settings) to help you discover threats and anomalous behaviors that are present in your environment. These rules search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate, and respond to threats with automated tracking and remediation processes.

**Microsoft Graph**

With the Microsoft Graph Security alerts entity, you can unify and streamline management of security issues across all integrated solutions. This also enables applications to correlate alerts and context to improve threat protection and response. With the alert update capability, you can sync the status of specific alerts across different security products and services that are integrated with the Microsoft Graph Security API by updating your [alerts](https://docs.microsoft.com/en-us/graph/api/resources/alert?view=graph-rest-1.0) entity.

[**Azure Policies**](#_Azure_Policy)

[**AU.L2-3.3.4 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#alert-in-the-event-of-an-audit-logging-process-failure)

**Azure**

**Customer Responsibility**

* Providing alerts in response to audit processing failures (e.g., storage quota is reached, audit hardware/software errors) of customer-deployed resources.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for alerting designated organizational officials in the event of an audit processing failure.

**Additional Resources**

* [Azure Functions error handling and retry guidance](https://learn.microsoft.com/en-us/azure/azure-functions/functions-bindings-error-pages?tabs=fixed-delay%2Cin-process&pivots=programming-language-csharp)
* [Azure subscription and service limits, quotas, and constraints](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits)
* [Azure Monitor limits alerts](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits#alerts)
* [Log Alerts in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-unified-log)
* [Azure Monitoring Contributor](https://docs.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security) for creating, modifying, and updating log alerts
* [Learn more about configuring log alerts in Azure](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log)
* Learn about [creating in log alerts in Azure](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log)
* Understand [webhooks in log alerts in Azure](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log-webhook)
* Learn about [Azure Alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview)
* Learn more about [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview)
* [Finding and filtering queries](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/example-queries#finding-and-filtering-queries)
* [Monitor Microsoft Entra ID Connect sync with Microsoft Entra ID Connect Health](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-sync)

##### AU.L2-3.3.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-6(3) | |
| **Practice:** Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.  **Assessment Objectives:**  [a] audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined; and  [b] defined audit record review, analysis, and reporting processes are correlated. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel | Log Analytics Workspace  Microsoft 365 Defender  Microsoft Purview  Microsoft Graph |

**Implementation Statement:**

**Microsoft Sentinel**

After [connecting your data sources](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard) to Microsoft Sentinel, use [out-of-the-box detections, built-in templates](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in#use-out-of-the-box-detections) to help you create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can [assign and investigate](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases) in your environment.

To learn how to automate your responses to threats, [Set up automated threat responses in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook).

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multi-cloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Microsoft Graph**

With the Microsoft Graph Security alerts entity, you can unify and streamline management of security issues across all integrated solutions. This also enables applications to correlate alerts and context to improve threat protection and response. With the alert update capability, you can sync the status of specific alerts across different security products and services that are integrated with the Microsoft Graph Security API by updating your [alerts](https://docs.microsoft.com/en-us/graph/api/resources/alert?view=graph-rest-1.0) entity.

**Azure**

**Customer Responsibility**

* Analyzing and correlating audit records across customer-deployed repositories.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for analyzing and correlating audit records across different repositories to gain organization-wide situational awareness.

**Additional Resources**

* [Manage your SOC better with incident metrics in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics)
* [How to respond to threats using automated playbooks](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook)
* [Investigate a suspicious IoT device](https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-investigate-device)

AU.L2-3.3.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-7 | |
| **Practice:** Provide audit record reduction and report generation to support on-demand analysis and reporting.  **Assessment Objectives:**  [a] an audit record reduction capability that supports on-demand analysis is provided; and  [b] a report generation capability that supports on-demand reporting is provided. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel | Log Analytics Workspace  Microsoft Entra ID  Microsoft Purview  Microsoft 365 Admin Center  Azure Monitor  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Sentinel**

You can facilitate analysis and reporting in several ways with Azure. Capabilities range from [threat reporting](https://docs.microsoft.com/en-us/azure/sentinel/import-threat-intelligence#view-your-threat-indicators-in-azure-sentinel) in [Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility#get-visualization), log reporting in [Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/visualizations) and usage reporting in Microsoft Entra ID visor. Microsoft Entra ID provides the capability to report on user sign-in, usage, and insights. The Microsoft Entra ID Sign-ins report provides user sign-in patterns, quantity of sign-ins and status of sign-ins. To learn more, see [Sign-in activity reports in the Microsoft Entra ID portal](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins#sign-ins-report).

[Visualize and monitor log data](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data)  using Microsoft Sentinel which allows you to [create custom workbooks](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data#create-new-workbook) across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Centralize sources to one place, such as Microsoft Sentinel SIEM solution. Connect logs from sources such as, Microsoft Entra ID , O365, Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for Cloud Apps and Intune to Sentinel for optimal visibility to support analysis and reporting. Learn more on how to [connect your sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Sentinel to support on demand analysis and reporting.

Microsoft Copilot for Security can access data from Microsoft Sentinel to increase the effectiveness and efficiency of security professionals using those solutions. Microsoft Defender XDR and Microsoft Sentinel become even more powerful when security professionals use Copilot for Security. Copilot for Security delivers an experience that enriches and builds on the security data, signals, and existing incidents and insights sourced from Microsoft Defender XDR and Microsoft Sentinel.

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Microsoft Copilot for Security](https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?msockid=24625821c11468eb15394c6cc01669f3)

**Microsoft 365 Admin Center**

Reporting features in Microsoft 365 provides various audit reports for Microsoft Entra ID Exchange Online, device management, supervisory review, and data loss prevention (DLP). These reports are different and separate from the Microsoft 365 activity reports. The Reports dashboard in the Microsoft 365 admin center preview displays usage activity across Microsoft 365. M Microsoft 365 global administrators, or an Exchange Online, SharePoint Online, or Skype for Business administrator, can get granular insight into the usage of that service. For example, the number of users in a particular Microsoft 365 service, the number of users that have activated Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus), and how much mail is flowing through the organization. Reports are available for the last 7, 30, 90, and 180 days.

**Azure**

**Customer Responsibility**

* Providing an audit reduction and report generation capability for customer-deployed resources, including the support of on-demand audit review, analysis, and reporting requirements, and after-the-fact investigations of security incidents.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for providing an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.

**Additional Resources**

* [Continuously export Security Center data](https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal)
* [Threat indicators for cyber threat intelligence in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/architecture/example-scenario/data/sentinel-threat-intelligence#:~:text=This%20form%20of%20threat%20intelligence,context%20for%20malicious%20cyber%20activity.)
* [Tutorial: Investigate incidents with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases)
* [Sign-ins logs in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins#filter-sign-in-activities)
* [Tutorial: Automate tasks to process emails by using Azure Logic Apps, Azure Functions, and Azure Storage](https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-process-email-attachments-workflow)
* [View export alerts and recommendations in Azure Monitor](https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal" \l "view-exported-alerts-and-recommendations-in-azure-monitor)
* [Manual one-time export of alerts and recommendations](https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal#manual-one-time-export-of-alerts-and-recommendations)
* [Monitoring and reporting in Azure](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/monitoring-reporting?tabs=AzureMonitor)

AU.L2-3.3.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-8, SC-45(1) | |
| **Practice:** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.  **Assessment Objectives:**  [a] internal system clocks are used to generate time stamps for audit records; [b] an authoritative source with which to compare and synchronize internal system clocks is specified; and  [c] internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source. | |
| **Primary Services** | **Secondary Services** |
| Windows Time Service |  |

**Implementation Statement:**

**Windows Time Service**

Time servers are synchronized to UTC and are accessed from other computers to provide scalability and robustness. Every computer has time synchronization service running that knows what time servers to use and periodically checks if computer clock needs to be corrected and adjusts time if needed.

Azure hosts are synchronized to internal Microsoft time servers that take their time from Microsoft-owned Stratum 1 devices, with GPS antennas. Virtual machines in Azure can either depend on their host to pass the accurate time (host time) on to the VM or the VM can directly get time from a time server, or a combination of both. To learn more, see [Time sync in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/time-sync).

**Azure**

**Customer Responsibility**

* For generating time stamps for audit records of Customer-deployed resources using the internal system clock.
* Comparing internal system clocks with an authoritative time source at the required frequency.
* Synchronizing internal system clocks to the authoritative time source
* Government customers using Windows 365 are responsible for synchronizing their VMs with time servers that meet organizational and compliance requirements.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for using internal system clocks to generate time stamps for audit records; by default, Windows uses the internal system clock to generate time stamps for audit records, and this setting is not configurable.

**Additional Resources**

* [Windows Time service tools and settings](https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings)
* [How to configure an authoritative time server in Windows Server](https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/configure-authoritative-time-server)
* [How to configure time synchronization for Azure Windows compute resources](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/time-sync)
* [How to configure time synchronization for Azure Linux compute resources](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/time-sync)

AU.L2-3.3.8

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-6(7), AU-9 | |
| **Practice:** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.  **Assessment Objectives:**  [a] audit information is protected from unauthorized access;  [b] audit information is protected from unauthorized modification;  [c] audit information is protected from unauthorized deletion;  [d] audit logging tools are protected from unauthorized access;  [e] audit logging tools are protected from unauthorized modification; and  [f] audit logging tools are protected from unauthorized deletion. | |
| **Primary Services** | **Secondary Services** |
| Azure RBAC | Microsoft Sentinel  Microsoft Purview  Azure Storage  Log Analytics Workspace  Conditional Access |

**Implementation Statement:**

**Azure RBAC**

Microsoft Sentinel uses [Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal) to provide [built-in roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles) that can be assigned to users, groups, and services in Azure. Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel to protect audit information and Sentinel from unauthorized access, modification and deletion. The different roles give you fine-grained control over what users of Microsoft Sentinel can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly, or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel will inherit.

* **Custom roles.** In addition to, or instead of, using Azure built-in roles, you can create Azure custom roles for Microsoft Sentinel. Azure custom roles for Microsoft Sentinel are created the same way you create other [Azure custom roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-rest#create-a-custom-role), based on [specific permissions to](https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftsecurityinsights) Microsoft Sentinel and to [Azure Log Analytics resources](https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftoperationalinsights).
* **Log Analytics RBAC.** You can use the Log Analytics advanced Azure role-based access control across the data in your Microsoft Sentinel workspace. This includes both data type-based Azure RBAC and resource-context Azure RBAC. To learn more, see:
  + [Manage log data and workspaces in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access#manage-access-using-workspace-permissions)
  + [Resource-context RBAC for Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/resource-context-rbac)
  + [[Table-level RBAC](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access#table-level-azure-rbac)](https://techcommunity.microsoft.com/t5/azure-sentinel/table-level-rbac-in-azure-sentinel/ba-p/965043)

Resource-context and table-level RBAC are two methods of providing access to specific data in your Microsoft Sentinel workspace without allowing access to the entire Microsoft Sentinel experience.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Azure**

**Customer Responsibility**

* Preventing unauthorized access to audit information and tools.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for protecting audit information and audit tools from unauthorized access, modification, and deletion.

**Additional Resources**

* [Permissions in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/roles#custom-roles-and-advanced-azure-rbac)
* [Custom role examples](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access#custom-role-examples)
* [Manage access to log data and workspaces in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access)
* [Log Analytics data security](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-security)

AU.L2-3.3.9

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-6(7), AU-9(4) | |
| **Practice:** Limit management of audit logging functionality to a subset of privileged users.  **Assessment Objectives:**  [a] a subset of privileged users granted access to manage audit logging functionality is defined; and  [b] management of audit logging functionality is limited to the defined subset of privileged users. | |
| **Primary Services** | **Secondary Services** |
| Azure RBAC  Privileged Identity Management (PIM) | Conditional Access  Microsoft Purview  Log Analytics Workspace  Intune/Intune Suite  Microsoft 365 Defender |

**Implementation Statement:**

Microsoft Sentinel uses [Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal) to provide [built-in roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles) that can be assigned to users, groups, and services in Azure. Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel to limit management of audit logging functionality to a subset of privileged users. The different roles give you fine-grained control over what users of Microsoft Sentinel can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly, or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel will inherit.

* **Custom roles.** In addition to, or instead of, using Azure built-in roles, you can create Azure custom roles for Microsoft Sentinel. Azure custom roles for Microsoft Sentinel are created the same way you create other [Azure custom roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-rest#create-a-custom-role), based on [specific permissions to](https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftsecurityinsights) Microsoft Sentinel and to [Azure Log Analytics resources](https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftoperationalinsights).
* **Log Analytics RBAC.** You can use the Log Analytics advanced Azure role-based access control across the data in your Microsoft Sentinel workspace. This includes both data type-based Azure RBAC and resource-context Azure RBAC. To learn more, see:
  + [Manage log data and workspaces in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access#manage-access-using-workspace-permissions)
  + [Resource-context RBAC for Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/resource-context-rbac)
  + [Table-level RBAC](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access" \l "table-level-azure-rbac)

Resource-context and table-level RBAC are two methods of providing access to specific data in your Microsoft Sentinel workspace without allowing access to the entire Microsoft Sentinel experience.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Azure**

**Customer Responsibility**

* Restricting the management of customer-controlled audit resources to authorized users.

**GCCH**

**Customer Responsibility**

* Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these customers are responsible for protecting audit information and audit tools from unauthorized access, modification, and deletion.

**Additional Resources**

* [Permissions in](https://docs.microsoft.com/en-us/azure/sentinel/roles#custom-roles-and-advanced-azure-rbac) Microsoft Sentinel
* [Custom role examples](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access#custom-role-examples)
* [Manage access to log data and workspaces in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access)
* [View activity logs for Azure RBAC changes](https://docs.microsoft.com/en-us/azure/role-based-access-control/change-history-report)

### 

### Configuration Management (CM)

CM.L2-3.4.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-2, CM-6, CM-8, CM-8(1) | |
| **Practice:** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.  **Assessment Objectives:**  [a] a baseline configuration is established;  [b] the baseline configuration includes hardware, software, firmware, and documentation;  [c] the baseline configuration is maintained (reviewed and updated) throughout the  system development life cycle;  [d] a system inventory is established;  [e] the system inventory includes hardware, software, firmware, and documentation; and  [f] the inventory is maintained (reviewed and updated) throughout the system  development life cycle. | |
| **Primary Services** | **Secondary Services** |
| Azure Automation  GitHub Enterprise Cloud  GitHub AE  Intune/Intune Suite  Microsoft Defender for Endpoint  Microsoft 365 Defender  Azure Policy  Azure Blueprints | Azure Virtual Machines  Microsoft 365 Lighthouse  Azure Lighthouse  Windows 365 Cloud PC  Microsoft Copilot for Security |

**Implementation Statement:**

**Azure Automation**

Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes in any cloud or on-premises datacenter. The service also imports DSC Resources, and assigns configurations to target nodes, all in the cloud. You can access Azure Automation State Configuration in the Azure portal by selecting State configuration (DSC) under Configuration Management.

Azure Automation State Configuration provides several advantages over the use of DSC outside of Azure. This service enables scalability across thousands of machines quickly and easily from a central, secure location. You can easily enable machines, assign them declarative configurations, and view reports showing each machine's compliance with the desired state you specify.

**Azure Automation - Change Tracking and Inventory**

Change Tracking and Inventory feature in Azure Automation allows you to track changes in virtual machines hosted in Azure, on-premises, and other cloud environments to help you pinpoint operational and environmental issues with software managed by the Distribution Package Manager. Change Tracking and Inventory makes use of Microsoft Defender for Cloud File Integrity Monitoring (FIM) to examine operating system and application files, and Windows Registry. While FIM monitors those entities, Change Tracking and Inventory natively tracks:

• Software changes

• Windows services

• Linux daemons

**Azure Policy & Blueprints**

Azure CMMC Blueprints sample provides governance guardrails using [Azure Policy](https://docs.microsoft.com/en-us/azure/governance/policy/overview) that help you assess specific [CMMC](https://www.acq.osd.mil/cmmc/index.html) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for CMMC L2.

**Intune/Intune Suite & Microsoft Defender for Endpoint & Microsoft Copilot for Security**

Microsoft Intune reports enable you to monitor the health and activity of endpoints more effectively and proactively across your organization. It also provides comprehensive reporting data, such as inventory details. You can access reports on device compliance, health, and trends, and create custom reports for specific data needs. For more details, see Intune Reports. To view device details, including hardware information and app installs, refer to the device details in Intune.

Microsoft Defender for Endpoint inventories software on devices. The Software Inventory page lists all installed software, showing vendor names, detected weaknesses, associated threats, impacted devices, exposure scores, and tags. You can filter this list based on weaknesses, threats, and tags such as end-of-support status. Access the Software Inventory page through the threat and vulnerability management navigation menu in the Microsoft Defender Portal. To view software on specific devices, check the individual device pages from the devices list.

For optimized device management, connect Intune to Defender for Endpoint. This integration helps establish an inventory of organizational devices and maintain baseline security configurations. You can track and manage configuration issues on Intune-managed Windows 10 devices.

The Windows Intune security baseline provides recommended settings for securely configuring Windows devices, including browser, PowerShell, and Microsoft Defender Antivirus settings. The Defender for Endpoint baseline optimizes security controls in the Defender for Endpoint stack, including endpoint detection and response (EDR) settings. For more information, refer to:

Microsoft Copilot for Security leverages Intune's capabilities to check device compliance and determine the reasons for noncompliance. When integrated with Microsoft Defender, it helps security administrators decide the best course of action. The Microsoft Intune Suite ensures that managed devices and applications comply with established security policies and configurations.

To learn more, see:

* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)
* [Use Copilot for Security to get device and policy information](https://learn.microsoft.com/en-us/mem/intune/copilot/security-copilot)
* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Windows security baseline settings for Intune](https://docs.microsoft.com/en-us/intune/security-baseline-settings-windows)
* [Microsoft Defender for Endpoint baseline settings for Intune](https://docs.microsoft.com/en-us/intune/security-baseline-settings-defender-atp)
* [Use Microsoft Defender for Endpoint in Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#enable-windows-defender-atp-in-intune)
* [Device inventory - Microsoft Defender for Endpoint](https://learn.microsoft.com/en-us/defender-endpoint/machines-view-overview?view=o365-worldwide)
* [Microsoft Defender for Endpoint in the Microsoft Defender portal](https://learn.microsoft.com/en-us/defender-xdr/microsoft-365-security-center-mde?view=o365-worldwide)
* [Microsoft Intune reports](https://learn.microsoft.com/en-us/mem/intune/fundamentals/reports)
* [View device details with Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-inventory)

**Virtual Machine**

You can establish and maintain system baselines with Azure virtual machine with inventory collection. You can enable inventory tracking for an Azure virtual machine from the virtual machine’s resource page. You can collect and view the following inventory information on your computers:

* Windows software (Windows applications and Windows updates), services, files, and Registry keys
* Linux software (packages) daemons, and files

This method provides a browser-based user interface for setting up and configuring inventory collection. To learn more, see [Manage an Azure virtual machine with inventory collection](https://docs.microsoft.com/en-us/azure/automation/automation-vm-inventory).

**Windows 365 Cloud PC**

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine (Cloud PCs) for your end users. Each Cloud PC is assigned to an individual user and is their dedicated Windows device. Windows 365 provides the productivity, security, and collaboration benefits of Microsoft 365.

To learn more, see:

* [Find the Right Windows 365 Cloud PC](https://www.microsoft.com/en-us/windows-365/cloud-pc-chooser)
* [Compare Plans and Pricing](https://www.microsoft.com/en-us/windows-365/business/compare-plans-pricing)
* [What is Windows 365 Enterprise?](https://learn.microsoft.com/en-us/windows-365/enterprise/overview?source=recommendations)
* [Manage Windows 365 Cloud PCs with Configuration Manager](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-cloud-pcs-using-configuration-manager)
* [Security overview for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/security-guidelines)

**Microsoft 365 Lighthouse**

Microsoft 365 Lighthouse baselines provide a repeatable and scalable way for you to assess and manage Microsoft 365 security settings across multiple customer tenants. Baselines also help monitor core security policies and tenant compliance standards with configurations that secure users, devices, and data. Lighthouse simplified configuration management by recommending security configuration baselines tailored to SMB customers and providing multi-tenant views across all customer environments.

**Azure**

**Customer Responsibility**

* Developing, documenting, and maintaining a baseline configuration of customer-deployed resources.
* Developing and documenting an inventory of customer-deployed resources, that supports tracking and reporting, and includes any information the customer has deemed necessary to achieve effective accountability.

**GCCH**

**Customer Responsibility**

* Customers are responsible for upgrading their Windows operating system to a newer version before their current version is no longer supported.

**Additional Resources**

* See the first security Practice: [Network security](https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-network-security)
* Download the Azure Security Benchmark in [spreadsheet format](https://github.com/MicrosoftDocs/SecurityBenchmarks/tree/master/Azure%20Security%20Benchmark)
* [Azure security standards for strategy and architecture](https://docs.microsoft.com/en-us/security/compass/compass): Strategy and architectural recommendations to shape your environment's security posture.
* [Azure security benchmarks](https://docs.microsoft.com/en-us/azure/security/benchmarks/introduction): Specific configuration recommendations for securing Azure environments.
* [Azure security baseline training](https://docs.microsoft.com/en-us/learn/modules/create-security-baselines/)
* [Details of the CMMC L2 Regulatory Compliance built-in initiative](https://docs.microsoft.com/en-us/azure/governance/policy/samples/cmmc-l3)
* [Intune reports](https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports)
* [Software inventory - threat and vulnerability management](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-software-inventory?view=o365-worldwide#how-it-works)
* [Use security baselines to configure Windows 10 devices in Intune](https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines)
* [Increase compliance to the Microsoft Defender for Endpoint security baseline](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-security-baseline?view=o365-worldwide)

CM.L2-3.4.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-2, CM-6,CM-8,CM-8(1) | |
| **Practice:** Establish and enforce security configuration settings for information technology products employed in organizational systems.  **Assessment Objectives:**  [a] security configuration settings for information technology products employed in the system are established and included in the baseline configuration; and  [b] security configuration settings for information technology products employed in the system are enforced. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure Automation  Azure Policy  Azure Blueprints  Intune/Intune Suite  Microsoft Defender for Endpoint  Microsoft Defender for Cloud  Microsoft 365 Defender  GitHub Enterprise Cloud  GitHub AE | Microsoft 365 Admin Center  Microsoft Copilot for Security  Conditional Access  App Locker |

**Implementation Statement:**

**Microsoft Defender for Endpoint**

With Microsoft Defender for Endpoint (MDE), you can now deploy security configurations from Microsoft Endpoint Manager directly to your onboarded devices without requiring a full Microsoft Endpoint Manager device enrollment. This capability is known as Security Management for Microsoft Defender for Endpoint. With this capability, devices that aren’t managed by a Microsoft Endpoint Manager service can receive security configurations for Microsoft Defender directly from Endpoint Manager.

**Azure Automation**

Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes in any cloud or on-premises datacenter. The service also imports DSC Resources, and assigns configurations to target nodes, all in the cloud. You can access Azure Automation State Configuration in the Azure portal by selecting State configuration (DSC) under Configuration Management.

Azure Automation State Configuration provides several advantages over the use of DSC outside of Azure. This service enables scalability across thousands of machines quickly and easily from a central, secure location. You can easily enable machines, assign them declarative configurations, and view reports showing each machine's compliance with the desired state you specify.

**Intune/Intune Suite & Microsoft Copilot for Security**

Intune and Microsoft Entra ID collaborate to ensure only managed and compliant devices can access email, Microsoft 365 services, SaaS apps, and on-premises apps. You can set a policy in Microsoft Entra ID to allow access to Microsoft 365 services only for domain-joined computers or mobile devices enrolled in Intune. Learn more about requiring managed devices with Conditional Access in Microsoft Entra ID.

Microsoft Intune includes settings and features you can enable or disable on different devices within your organization to allow only essential capabilities. These settings and features are added to "configuration profiles". You can create profiles for different devices and platforms, including iOS/iPadOS, Android device administrator, Android Enterprise, and Windows, then use Intune to apply or "assign" the profile to the devices.

Administrative templates include hundreds of settings that you can configure for Internet Explorer, Microsoft Edge, OneDrive, remote desktop, Word, Excel, and other Office programs. These templates provide administrators with a simplified view of settings similar to group policy and are 100% cloud-based.

Additionally, Intune offers preconfigured security baselines to establish and enforce security configuration settings, helping secure and protect your users and devices. You can customize these baselines to enforce only the settings and values you require. To learn more about security baselines in Intune, see Available security baselines.

Microsoft Copilot for Security works with Intune to enforce security configuration settings by analyzing current device configurations and policies and recommending enhancements or changes to improve device security posture.

Intune and Intune Suite, through applications like Enterprise App Management and Advanced Analytics, enable administrators to configure and enforce security settings across various devices, including mobile phones, tablets, and laptops. These settings can include password requirements, encryption settings, and application permissions.

To learn more, see:

* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)
* [Use Copilot for Security to get device and policy information](https://learn.microsoft.com/en-us/mem/intune/copilot/security-copilot)
* [Learn about Intune security baselines for Windows devices](https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines#available-security-baselines)
* [Use ADMX templates on Windows 10/11 devices in Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows)
* [Restrict devices features using policy in Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-configure#create-the-profile)
* [Grant controls in Conditional Access policy](https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant)
* [Application proxy documentation](https://learn.microsoft.com/en-us/entra/identity/app-proxy/)

**Microsoft Defender for Cloud**

Consider exploring Microsoft Defender for Cloud’s adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe. Requirements include [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction) . Learn more about [using adaptive application controls.](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application)

 This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

* Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
* Comply with your organization’s security policy that dictates the use of only licensed software.
* Avoid unwanted software to be used in your environment.
* Avoid old and unsupported apps to run.
* Prevent specific software tools that are not allowed in your organization.
* Enable IT to control the access to sensitive data through app usage.

Requirements include [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction) . Learn more about [using adaptive application controls.](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application)

**Azure**

**Customer Responsibility**

* Developing, documenting, and maintaining a baseline configuration of customer-deployed resources.

**GCCH**

**Customer Responsibility**

* Customers are responsible for upgrading their Windows operating system to a newer version before their current version is no longer supported.

**Additional Resources**

* [Five steps to securing your identity infrastructure](https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity)
* [Azure security baseline for Security Center](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/security-center-security-baseline)
* [Azure security baseline for Azure App Configuration](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-config-security-baseline)
* [Azure security baseline for Virtual Network](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/virtual-network-security-baseline)
* [CMMC L2 blueprint sample](https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/cmmc-l3)
* [CIS Azure Foundations Benchmark](https://www.cisecurity.org/benchmark/azure/)
* [Microsoft Entra ID deployment plans](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-deployment-plans)

CM.L2-3.4.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-3 | |
| **Practice:** Track, review, approve or disapprove and log changes to organizational systems.  **Assessment Objective:**  [a] changes to the system are tracked;  [b] changes to the system are reviewed;  [c] changes to the system are approved or disapproved; and  [d] changes to the system are logged. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Defender for Cloud Apps  Power Automate  Azure Automation  GitHub Enterprise Cloud  GitHub AE | Log Analytics Workspace  Microsoft Entra ID  Intune/Intune Suite  Microsoft 365 Defender  Microsoft Defender for Endpoint  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Defender for Cloud Apps/Azure Automation -Change Tracking and Inventory**

Enable [Change Tracking and Inventory](https://docs.microsoft.com/en-us/azure/automation/change-tracking/overview) to track changes in virtual machines hosted in Azure, on-premises, and other cloud environments. Change Tracking and Inventory makes use of [Microsoft Defender for Cloud Apps File Integrity Monitoring (FIM)](https://docs.microsoft.com/en-us/azure/security-center/security-center-file-integrity-monitoring) to examines operating system and application files, and Windows Registry. To track Azure Resource Manager property changes, see the Azure Resource Graph [change history](https://docs.microsoft.com/en-us/azure/governance/resource-graph/how-to/get-resource-changes).

* To enable from an Automation account, see [Enable Change Tracking and Inventory from an Automation account](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-automation-account).
* To enable from the Azure portal, see [Enable Change Tracking and Inventory from the Azure portal](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-portal).
* To enable from a runbook, see [Enable Change Tracking and Inventory from a runbook](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-runbook).
* To enable from an Azure VM, see [Enable Change Tracking and Inventory from an Azure VM](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-vm).

**GitHub AE**

Track, review, approve or disapprove and log changes to organizational systems using GitHub AE pull request. After initializing a pull request, you will see a review page that shows a high-level overview of the changes between your branch (the compare branch) and the repository's base branch. You can add a summary of the proposed changes, review the changes, add labels, milestones, and assignees, and @mention individual contributors or teams.

To learn more, see:

* [About pull requests](https://docs.github.com/en/github-ae@latest/github/collaborating-with-pull-requests/proposing-changes-to-your-work-with-pull-requests/about-pull-requests)
* [Creating a pull request](https://docs.github.com/en/github-ae@latest/articles/creating-a-pull-request)

**Intune/Intune Suite**

Use Intune to assist in tracking, reviewing, and approving configuration changes to organizational systems. Intune provides the capability to troubleshoot issues with policies and verify their correct application. High-level visibility of your policies helps in determining if changes are needed.

Microsoft Intune reports allow you to monitor the health and activity of endpoints more effectively and proactively across your organization. These reports provide data on device compliance, device health, and device trends, helping you identify areas for improvement and determine if more restrictive conditional access policies are necessary.

Additionally, you can monitor Intune configuration changes, such as policy modifications, in audit logs. By sending log files from Intune to Log Analytics, you can create alerts to automatically notify you of unauthorized changes.

Changes made through Intune and Intune Suite can be tracked and audited using provided tools for reviewing configuration changes. Intune integrates with other Microsoft services, such as Microsoft Entra ID and Azure Monitor, for comprehensive monitoring, auditing, and logging capabilities.

To learn more, see:

* [Use audit logs to track and monitor events in Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/fundamentals/monitor-audit-logs)
* [Create a Log Analytics workspace in the Azure portal](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace)
* [Intune reports](https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports)
* [Troubleshoot policies and profiles and in Intune](https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-policies-in-microsoft-intune)
* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)

**Microsoft Defender for Endpoint**

With Microsoft Defender for Endpoint (MDE), you can approve or reject pending remediation actions. These remediation actions are not taken unless and until your security operations team approves them. We recommend reviewing and approving any pending actions as soon as possible so that your automated investigations complete in a timely manner.

**Power Automate**

With Power Automate, you can manage the approval of documents or processes across several services, including SharePoint, Dynamics 365, Salesforce, OneDrive for Business, Zendesk, or WordPress.

To create an approval workflow, add the Approvals - Start and wait for an approval action to any flow. After you add this action, your flow can manage the approval of documents or processes. For example, you can create document approval flows for approval of log changes to the organizational systems. Approvers can respond to requests from their email inbox, the approvals center in Power Automate, or the Power Automate app.

**Azure**

**Customer Responsibility**

* Reviewing proposed configuration-controlled changes to customer-deployed resources.
* Documenting configuration-controlled changes associated with customer-deployed resources
* Implementing configuration-controlled changes approved
* Retaining a record of configuration-controlled changes to customer-deployed resources.

**Additional Resources**

* [Search for role group changes or admin audit logs in Exchange Online](https://docs.microsoft.com/en-us/exchange/security-and-compliance/exchange-auditing-reports/search-role-group-changes)
* [Microsoft Entra ID audit activity reference](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-audit-activities)
* [Security Practice: Logging and Monitoring](https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-logging-monitoring)
* [Get resource changes](https://docs.microsoft.com/en-us/azure/governance/resource-graph/how-to/get-resource-changes)

CM.L2-3.4.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-4 | |
| **Practice:** Analyze the security impact of changes prior to implementation.  **Assessment Objective:**  [a] the security impact of changes to the system is analyzed prior to implementation. | |
| **Primary Services** | **Secondary Services** |
| GitHub Enterprise Cloud  GitHub AE  Azure DevTest Labs  Microsoft 365 for enterprise Test Lab | Intune/Intune Suite  Microsoft Defender Endpoint  Azure Virtual Desktop |

**Implementation Statement:**

Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required. Changes to IT systems can cause unforeseen problems and have unintended consequences for both users and the security of the operating environment. Analyze the security impact of changes prior to implementation by utilizing test environments. Use purpose-built, managed developer services like [Azure DevTest Labs](https://azure.microsoft.com/en-us/services/devtest-lab/), [GitHub Code spaces](https://github.com/features/codespaces/), and [Azure Virtual Desktop](https://azure.microsoft.com/en-us/services/virtual-desktop/) to easily manage and optimize dev/test environments, tenants, and subscriptions, without sacrificing governance, cost controls, or security.

This can uncover and mitigate potential problems before they occur. Configuration changes should be tested, validated and documented before installing them on the operational system.

Not all features or changes have the potential to impact your security or compliance stature, so it might not be necessary to deeply analyze every single change. For changes that are impactful, Microsoft provides configuration options for controlling related features. To help users adopt new features, by default, these changes are generally on - action is required on your part to disable or limit these features. Microsoft 365 changes can be planned or unplanned, depending on the nature of the changes. For example, security updates aren't always planned, because they're reactions to emergent risks or issues in our products or services. Responsibility for managing these changes is shared between Microsoft and you as the administrator of your Microsoft 365 tenant. Microsoft provides various release options and tools to help control and deploy changes in a manner that aligns with your strategy. Microsoft 365 changes are released to both services (like SharePoint Online and Teams) and clients, referred to as Microsoft 365 Apps (like Microsoft Word, Excel, and PowerPoint). Services and clients have different release channels and deployment controls, so it's important to understand the differences as you implement your release management strategy.

**Azure**

**Customer Responsibility**

* Analyzing proposed changes to customer-deployed resources to determine potential security impacts prior to implementation.

**Additional Resources**

* [The simulated enterprise base configuration](https://docs.microsoft.com/en-us/microsoft-365/enterprise/simulated-ent-base-configuration-microsoft-365-enterprise?view=o365-worldwide)
* [Azure DevTest Labs](https://azure.microsoft.com/en-us/services/devtest-lab/)
* [Microsoft 365 for enterprise Test Lab Guides](https://docs.microsoft.com/en-us/microsoft-365/enterprise/m365-enterprise-test-lab-guides?view=o365-worldwide)
* [Evaluate the impact of Conditional Access policies before enabling widely with report-only mode](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only)

CM.L2-3.4.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-5 | |
| **Practice:** Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.  **Assessment Objectives:**  [a] physical access restrictions associated with changes to the system are defined;  [b] physical access restrictions associated with changes to the system are documented;  [c] physical access restrictions associated with changes to the system are approved;  [d] physical access restrictions associated with changes to the system are enforced;  [e] logical access restrictions associated with changes to the system are defined;  [f] logical access restrictions associated with changes to the system are documented;  [g] logical access restrictions associated with changes to the system are approved; and  [h] logical access restrictions associated with changes to the system are enforced. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC  Azure Automation  Power Automate  GitHub Enterprise Cloud  GitHub AE | Azure Firewall  Network Security Groups  Azure Web Application Firewall  Virtual Network  Conditional Access  Intune/Intune Suite  Microsoft 365 admin center  Teams  Microsoft 365 Defender  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID**

Using [Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview), users, groups, and applications from that directory can be granted access to resources in the Azure subscription. For example, a storage account can be placed in a resource group to control access to that specific storage account using Microsoft Entra ID. Access to Azure Storage can be controlled by Microsoft Entra ID, which enforces tenant isolation and implements robust measures to prevent access by unauthorized parties, including Microsoft insiders. More information about Microsoft Entra ID tenant isolation is available from a [white paper Microsoft Entra ID Data Security Considerations](https://aka.ms/AADDataWhitePaper).

Learn about [security considerations for physical isolated on-premises deployments (e.g., bare metal) vs. logically isolated cloud-based deployments (e.g., Azure).](https://docs.microsoft.com/en-us/azure/azure-government/azure-secure-isolation-guidance#logical-isolation-considerations)

**Conditional Access & Intune/Intune Suite & Microsoft Copilot for Security**

Configure Conditional Access policies to require managed devices for accessing certain cloud apps in your environment. These policies should ensure devices are marked as compliant by Intune or Intune Suite. Intune and Microsoft Entra ID work together to ensure only managed and compliant devices can access email, Microsoft 365 services, SaaS apps, and on-premises apps. Learn more about requiring managed devices with Conditional Access in Microsoft Entra ID.

You can manage Microsoft 365 user accounts in various ways, depending on your configuration. Options include managing user accounts in the Microsoft 365 admin center, PowerShell, Active Directory Domain Services (AD DS), or the Microsoft Entra ID admin portal. User accounts are synchronized with Microsoft 365 from AD DS, so on-premises AD DS tools must be used to manage user accounts.

Microsoft Copilot for Security works with Intune to enhance and enforce security configuration settings across your organization’s devices. Copilot adheres to RBAC principles, ensuring that it only accesses data and performs actions within the scope of the permissions assigned to the administrator. This ensures that the principle of least privilege is maintained.

To learn more, see:

* [Grant controls in Conditional Access policy](https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant)
* [Application proxy documentation](https://learn.microsoft.com/en-us/entra/identity/app-proxy/)
* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)
* **Teams**  The Approvals app is available as a personal app for all Microsoft Teams users. The Approvals app provides a simple way to bring auditing, compliance, accountability, and workflows to both structured and unstructured Approvals in Teams. From the Teams Approvals app, users have access to create new Approvals and view Approvals that they have sent and received. Users won't have access to Approvals that are created by others unless they're either a responder or a viewer of the request.

**Power Automate**

Whether you need written acknowledgment from your manager or a formal authorization from a diverse group of stakeholders, getting things approved is part of almost every organization. With the approvals capability in Power Automate, you can automate sign-off requests and combine human decision-making for workflows.

**Azure**

**Customer Responsibility**

* Enforcing logical access restrictions when making changes to customer-deployed resources.

**Additional Resources**

* [Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources)
* [Configure Azure Storage firewalls and virtual networks](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal)
* [How to: Require approved client apps for cloud app access with Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-conditional-access)
* [Windows Defender Application Control and AppLocker Overview](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview)

CM.L2-3.4.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-7 | |
| **Practice:** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.  **Assessment Objectives:**  [a] essential system capabilities are defined based on the principle of least functionality; and  [b] the system is configured to provide only the defined essential capabilities. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Intune/ Microsoft Endpoint Manager  Azure Firewall | Microsoft 365 Defender  Conditional Access  Network Security Groups  Microsoft Copilot for Security |

**Implementation Statement:**

**Intune/Intune Suite & Microsoft Copilot for Security**

Intune/Intune Suite and Microsoft Entra ID work together to ensure that only managed and compliant devices can access email, Microsoft 365 services, SaaS apps, and on-premises apps. You can set policies in Microsoft Entra ID to allow only domain-joined computers or mobile devices enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Microsoft Entra ID.

Microsoft Intune provides settings and features to enable or disable capabilities on different devices within your organization. These settings are organized into "configuration profiles," which can be created for various devices and platforms, including iOS/iPadOS, Android device administrator, Android Enterprise, and Windows. Intune then applies or "assigns" these profiles to the devices.

Administrative templates in Intune include hundreds of settings for Internet Explorer, Microsoft Edge, OneDrive, remote desktop, Word, Excel, and other Office programs. These templates give administrators a simplified view of settings similar to group policy and are entirely cloud-based. Group Policy analytics further analyze your on-premises GPOs, showing which policy settings are supported, deprecated, and more.

Copilot for Security integrates with Microsoft Entra ID, utilizing the roles and permissions configured by administrators for specific applications. Copilot for Security can identify risky users in Microsoft Entra and detect incorrect or conflicting policy and configuration settings for devices managed by Intune/Intune Suite.

Intune/Intune Suite can also limit the software and functionalities available on each device to minimize security risks. It ensures devices only have the necessary capabilities for their intended roles through Endpoint Privilege Management, Enterprise App Management, and Advanced Analytics.

To learn more, see:

* [Application proxy documentation](https://learn.microsoft.com/en-us/entra/identity/app-proxy/)
* [Requiring managed devices with Conditional Access in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices) .
* [create profiles](https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-configure#create-the-profile)
* [Administrative templates](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows)
* [Group Policy analytics](https://docs.microsoft.com/en-us/mem/intune/configuration/group-policy-analytics)
* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)

**Microsoft Entra ID**

Managed identities provide Azure services with an automatically managed identity in Microsoft Entra ID. You can use the identity to authenticate to any service that supports Microsoft Entra ID authentication, including Key Vault, without exposing credentials. There are two types of system managed identities.

* A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Microsoft Entra ID tenant that is trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it is enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Microsoft Entra ID .
* A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Microsoft Entra ID tenant that is trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it is assigned.

To learn more, see:

* [What are managed identities for Azure resources?](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview)
* [Create a user-assigned managed identity](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-manage-ua-identity-portal)

**Microsoft 365 Defender**

The application governance add-on feature to Defender for Cloud Apps is now available in Microsoft 365 Defender. App governance provides a security and policy management capability designed for OAuth-enabled apps that access Microsoft 365 data through Microsoft Graph APIs. App governance delivers full visibility, remediation, and governance into how these apps and their users’ access, use, and share your sensitive data stored in Microsoft 365 through actionable insights and automated policy alerts and actions.

**Azure Firewall**

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It’s a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

To learn more, see [Deploy and configure Azure Firewall](https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal).

**Network Security Groups**

Network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

[This article](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview) describes properties of a network security group rule, the [default security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules) that are applied, and the rule properties that you can modify to create an [augmented security rule](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#augmented-security-rules).

**Customer Responsibility**

* Configuring customer-deployed resources to only provide essential capabilities (e.g., disabling extraneous services that may be provided by default, using a system for a single function rather than a system supporting multiple functions, restricting or prohibiting unused or unnecessary functions, ports, protocols, or services).

**Additional Resources**

* [Use a Windows VM system-assigned managed identity to access Resource Manager](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-arm)
* [Use a Linux VM system-assigned managed identity to access Resource Manager](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-linux-vm-access-arm)
* [How to use managed identities for App Service and Azure Functions](https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity)
* [How to use managed identities with Azure Container Instances](https://docs.microsoft.com/en-us/azure/container-instances/container-instances-managed-identity)
* [Implementing Managed Identities for Microsoft Azure Resources](https://www.pluralsight.com/courses/microsoft-azure-resources-managed-identities-implementing)
* [Tutorial: Create and manage policies to enforce compliance](https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage)
* [Configure device restriction settings in Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-configure)

CM.L2-3.4.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-7(1), CM-7(2) | |
| **Practice:** Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.  **Assessment Objectives:**  [a] essential programs are defined;  [b] the use of nonessential programs is defined;  [c] the use of nonessential programs is restricted, disabled, or prevented as defined;  [d] essential functions are defined;  [e] the use of nonessential functions is defined;  [f] the use of nonessential functions is restricted, disabled, or prevented as defined;  [g] essential ports are defined;  [h] the use of nonessential ports is defined;  [i] the use of nonessential ports is restricted, disabled, or prevented as defined;  [j] essential protocols are defined;  [k] the use of nonessential protocols is defined;  [l] the use of nonessential protocols is restricted, disabled, or prevented as defined;  [m] essential services are defined;  [n] the use of nonessential services is defined; and  [o] the use of nonessential services is restricted, disabled, or prevented as defined. | |
| **Primary Services** | **Secondary Services** |
| Network Security Groups  Azure Firewall  Azure Web Application Firewall  Microsoft Entra ID  Intune/Intune Suite | Microsoft Defender for IoT  App Locker  Microsoft Defender for Cloud  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft 365 Defender  Conditional Access  Microsoft Copilot for Security |

**Implementation Statement:**

**Network Security Groups**

Network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

[This article](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview) describes properties of a network security group rule, the [default security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules) that are applied, and the rule properties that you can modify to create an [augmented security rule](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#augmented-security-rules).

**Microsoft Entra ID**

Managed identities provide Azure services with an automatically managed identity in Microsoft Entra ID. You can use the identity to authenticate to any service that supports Microsoft Entra ID authentication, including Key Vault, without exposing credentials. There are two types of system managed identities.

* A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Microsoft Entra ID tenant that is trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it is enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Microsoft Entra ID .
* A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Microsoft Entra ID tenant that is trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it is assigned.

To learn more, see:

* [What are managed identities for Azure resources?](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview)
* [Create a user-assigned managed identity](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-manage-ua-identity-portal)

**Intune/Intune Suite & Microsoft Copilot for Security**

Intune/Intune Suite and Microsoft Entra ID integrate to ensure that only managed and compliant devices can access email, Microsoft 365 services, SaaS apps, and on-premises apps. You can set policies in Microsoft Entra ID to allow only domain-joined computers or mobile devices enrolled in Intune to access Microsoft 365 services. Learn more about requiring managed devices with Conditional Access in Microsoft Entra ID.

While Copilot for Security does not directly implement rules and restrictions for functions, ports, protocols, or devices, it can identify incorrect or conflicting policy and configuration settings for devices managed by Intune/Intune Suite. It also provides device analysis and assists in troubleshooting.

Intune/Intune Suite can limit the software and functionalities available on each device to minimize security risks. It ensures devices only have the necessary capabilities for their intended roles through Endpoint Privilege Management, Enterprise App Management, and Advanced Analytics.

To learn more, see:

* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)
* [Application proxy documentation](https://learn.microsoft.com/en-us/entra/identity/app-proxy/)
* [Requiring managed devices with Conditional Access in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices) .

**Microsoft Defender for Cloud**

Consider exploring Microsoft Defender for Cloud’s adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

* Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
* Comply with your organization’s security policy that dictates the use of only licensed software.
* Avoid unwanted software to be used in your environment.
* Avoid old and unsupported apps to run.
* Prevent specific software tools that are not allowed in your organization.
* Enable IT to control the access to sensitive data through app usage.

Requirements include [Microsoft Defender for Cloud for Servers](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction). Learn more about [using adaptive application controls.](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application)

**Microsoft 365 Defender**

The Tenant Allow/Block List in the Microsoft 365 Defender portal gives you a way to manually override the Microsoft 365 filtering verdicts. The Tenant Allow/Block List is used during mail flow for incoming messages (does not apply to intra-org messages) and at the time of user clicks.

If you override the allow or block verdict in the spoof intelligence insight, the spoofed sender becomes a manual allow or block entry that only appears on the Spoof tab in the Tenant Allow/Block List. You can also manually create allow or block entries for spoofed senders before they're detected by spoof intelligence.

**Microsoft Defender for Cloud Apps**

Protect your organization by monitoring and controlling cloud app use with any IdP solution and the Defender for Cloud Apps Conditional Access App Control. Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of a session using its device as a condition, create both a conditional access policy AND a session policy. You can create policies that prevent the use of functions that might pose a threat to security. For example, you could create a policy to block download capabilities for locations that aren't part of your corporate network.

**AppLocker**

AppLocker advances the app control features and functionality of Software Restriction Policies. AppLocker contains new capabilities and extensions that allow you to create rules to allow or deny apps from running based on unique identities of files and to specify which users or groups can run those apps.

[**Azure Policies**](#_Azure_Policy)

* [**CM.L2-3.4.7 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#restrict-disable-or-prevent-the-use-of-nonessential-programs-functions-ports-protocols-and-services)

**Azure**

**Customer Responsibility**

* Configuring customer-deployed resources to only provide essential capabilities (e.g., disabling extraneous services that may be provided by default, using a system for a single function rather than a system supporting multiple functions).
* Prohibiting or restricting the use of specific functions, ports, protocols, and/or services to provide least functionality.
* Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services to include a defined frequency of reviews.

**Additional Resources**

* [Microsoft Defender for Endpoint Device Control Removable Storage Protection](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-removable-storage-protection?view=o365-worldwide)
* [Virtual network integration for Azure services](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services)
* [How network security groups work](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works)
* [Windows Defender Application Control and AppLocker Overview](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview)

CM.L2-3.4.8

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-7(4), CM-7(5) | |
| **Practice:** Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.  **Assessment Objectives:**  [a] a policy specifying whether whitelisting or blacklisting is to be implemented is  specified;  [b] the software allowed to execute under whitelisting or denied use under blacklisting is specified; and  [c] whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified. | |
| **Primary Services** | **Secondary Services** |
| Azure Firewall  Intune/Intune Suite  Microsoft Defender for Cloud Apps  Microsoft Defender SmartScreen | Network Security Groups  Azure Web Application Firewall  Conditional Access  Microsoft Defender for Endpoint  GitHub Enterprise Cloud  GitHub AE  Azure Virtual Machines  Windows 365 Cloud PC |

**Implementation Statement:**

**Microsoft Defender for Cloud Apps**

Consider exploring Microsoft Defender for Cloud’s adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

 This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

* Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
* Comply with your organization’s security policy that dictates the use of only licensed software.
* Avoid unwanted software to be used in your environment.
* Avoid old and unsupported apps to run.
* Prevent specific software tools that are not allowed in your organization.
* Enable IT to control the access to sensitive data through app usage.

Requirements include [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction) . Learn more about [using adaptive application controls.](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application)

**Microsoft Defender SmartScreen & Microsoft Defender for Endpoint**

Potentially unwanted applications (PUA) are a category of software that can cause your machine to run slowly, display unexpected ads, or at worst, install other software that might be unexpected or unwanted. In Chromium-based Edge with PUA protection turned on, Microsoft Defender SmartScreen protects you from PUA-associated URLs. Although Microsoft Defender for Endpoint has its own blocklist based upon a data set managed by Microsoft, you can customize this list based on your own threat intelligence. If you create and manage indicators in the Microsoft Defender for Endpoint portal, Microsoft Defender SmartScreen respects the new settings.

**Microsoft Entra ID**

Managed identities provide Azure services with an automatically managed identity in Microsoft Entra ID. You can use the identity to authenticate to any service that supports Microsoft Entra ID authentication, including Key Vault, without exposing credentials. There are two types of system managed identities.

* A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Microsoft Entra ID tenant that is trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it is enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Microsoft Entra ID .
* A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Microsoft Entra ID tenant that is trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it is assigned.

To learn more, see:

* [What are managed identities for Azure resources?](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview)
* [Create a user-assigned managed identity](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-manage-ua-identity-portal)

**Intune/Intune Suite**

Intune and Microsoft Entra ID work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and [on-premises apps](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-application-proxy-get-started). Additionally, you can set a policy in Microsoft Entra ID to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about [requiring managed devices with Conditional Access in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices) .

**Network Security Groups**

Network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

[This article](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview) describes properties of a network security group rule, the [default security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules) that are applied, and the rule properties that you can modify to create an [augmented security rule](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#augmented-security-rules).

[**Azure Policies**](#_Azure_Policy)

* [**CM.L2-3.4.8 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#apply-deny-by-exception-blacklisting-policy-to-prevent-the-use-of-unauthorized-software-or-deny-all-permit-by-exception-whitelisting-policy-to-allow-the-execution-of-authorized-software)

**Azure**

**Customer Responsibility**

* Identifying software programs authorized to execute on customer-deployed resources.
* Employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on customer-deployed resources.

**Additional Resources**

* [Settings list for the Windows 365 Cloud PC security baseline in Intune - Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-windows-365)
* [Windows Defender Application Control and AppLocker Overview](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview)

CM.L2-3.4.9

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CM-11 | |
| **Practice:** Control and monitor user-installed software.  **Assessment Objectives:**  [a] a policy for controlling the installation of software by users is established;  [b] installation of software by users is controlled based on the established policy; and  [c] installation of software by users is monitored. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure Monitor  Microsoft Sentinel  Microsoft Defender for Cloud  Microsoft Defender for Cloud Apps  Intune/Intune Suite | Log Analytics  Microsoft Defender for Endpoint  Microsoft Defender for Identity  Microsoft 365 Defender  Microsoft 365 Admin Center  AppLocker  GitHub Enterprise Cloud  GitHub AE |

**Implementation Statement:**

**Microsoft Defender for Cloud**

Consider exploring Microsoft Defender for Cloud’s adaptive application controls. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads that you can customize. When you have enabled and configured adaptive application controls, you will get security alerts if any application runs other than the ones you have defined as safe.

 This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

* Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
* Comply with your organization’s security policy that dictates the use of only licensed software.
* Avoid unwanted software to be used in your environment.
* Avoid old and unsupported apps to run.
* Prevent specific software tools that are not allowed in your organization.
* Enable IT to control the access to sensitive data through app usage.

Requirements include [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction) . Learn more about [using adaptive application controls.](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application)

**Change Tracking and Inventory**

[Change Tracking and Inventory](https://docs.microsoft.com/en-us/azure/automation/change-tracking/overview#current-limitations) forwards data to Azure Monitor Logs, and this collected data is stored in a Log Analytics workspace. The File Integrity Monitoring (FIM) feature is available only when [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender)is enabled. FIM uploads data to the same Log Analytics workspace as the one created to store data from Change Tracking and Inventory. Machines connected to the Log Analytics workspace use the [Log Analytics agent](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent) to collect data about changes to installed software, Microsoft services, Windows registry and files, and Linux daemons on monitored servers. When data is available, the agent sends it to Azure Monitor Logs for processing. Azure Monitor Logs applies logic to the received data, records it, and makes it available for analysis. Learn more about enabling Change Tracking and Inventory.

**Intune/Intune Suite**

Intune and Microsoft Entra ID work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and [on-premises apps](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-application-proxy-get-started). Additionally, you can set a policy in Microsoft Entra ID to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about [requiring managed devices with Conditional Access in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices) .

**Microsoft Entra ID**

There are several methods to controlling user-installed software in Azure. One of the most effective methods for controlling user-installed software is enforcing least privilege, role- based access control (RBAC). Microsoft Entra ID Privileged Identity Management allows you to manage administrator privileges for users and groups. To learn more, see [Deploy Privileged Identity Management (PIM)](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan).

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Microsoft Sentinel**

[Connect your data sources](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard) to Microsoft Sentinel to visualize and monitor the data in one central location using Microsoft Sentinel. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

**GitHub AE**

GitHub Packages is a software package hosting service that allows you to host your software packages privately for specified users or internally for your enterprise and use packages as dependencies in your projects. GitHub Packages combines your source code and packages in one place to provide integrated permissions management, so you can centralize your software development on GitHub AE. Learn more [about GitHub Packages and Managing GitHub packages.](https://docs.github.com/en/github-ae@latest/packages)

**Microsoft 365 admin center**

As a Microsoft 365 admin, you can choose to do the following tasks on the Office installation options page in the Microsoft 365 admin center:

• Choose how often to get feature updates for Office.

• Manage which version of Office is installed, including.

• Roll back to a previous version.

• Skip an upcoming version.

• Choose whether users can install Office on their own devices.

[**Azure Policies**](#_Azure_Policy)

* [**CM.L2-3.4.8 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#control-and-monitor-user-installed-software)

**Azure**

**Customer Responsibility**

* Establishing a policy governing the installation of software on customer-deployed resources by users.

**Additional Resources**

* [Plan for Software Center - Configuration Manager](https://learn.microsoft.com/en-us/mem/configmgr/apps/plan-design/plan-for-software-center)
* [Discover what Software is installed on your VMs](https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-installed-software)
* [Using Software Restriction Policies to Protect Against Unauthorized Software](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457006(v=technet.10)?redirectedfrom=MSDN)
* [How to manage the local administrators group on Microsoft Entra ID joined devices](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457006(v=technet.10)?redirectedfrom=MSDN)
* [Manage Change Tracking and Inventory in Azure Automation](https://docs.microsoft.com/en-us/azure/automation/change-tracking/manage-change-tracking)
* [Enable Change Tracking and Inventory from an Automation account](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-automation-account)
* [Enable Change Tracking and Inventory by browsing the Azure portal](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-portal)
* [Enable Change Tracking and Inventory from a runbook](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-runbook)
* [Enable Change Tracking and Inventory from an Azure VM](https://docs.microsoft.com/en-us/azure/automation/change-tracking/enable-from-vm)
* [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction)

### Identification and Authentication (IA)

IA.L1-3.5.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-2, IA-3, IA-5 | |
| **Practice:** Identify information system users, processes acting on behalf of users or devices.  **Assessment Objectives:**  [a] system users are identified;  [b] processes acting on behalf of users are identified; and  [c] devices accessing the system are identified. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC  Intune/Intune Suite | Network Security Groups  Privileged Identity Management (PIM)  Microsoft Graph  Microsoft Defender SmartScreen  Microsoft 365 Defender  Windows Hello for Business  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID**

Microsoft Entra ID is a cloud-based identity service in Azure that helps authenticate and authorize users. It allows users to access Azure resources, third-party resources used by your company, and on-premises resources using the same username and password. At its core, Microsoft Entra ID includes a directory of users, each with an identity comprised of a user ID, password, and other properties. Users can also have one or more directory roles assigned for authorization purposes.

Two other key entities in Microsoft Entra ID are service principals and managed identities. Service principals represent an application, while managed identities are a special type of service principal used exclusively with Azure resources.

From the Users blade in the Azure portal, you can manage identities. The specified username is used to log in to Microsoft Entra ID, and the domain name must be owned by you and associated with your Microsoft Entra ID. New users can be assigned to groups or roles, which simplifies managing large numbers of similar users.

In the modern workplace, users often need to access applications not managed by their organization’s AD. Active Directory Federation Service (ADFS) addresses this by allowing users from one organization to access partner organization applications using their standard AD credentials. ADFS also lets users access AD-integrated applications remotely using their AD credentials via a web interface. It provides a central place to manage and audit employee identity information shared with partner organizations. Learn more about this in the guide on Deploying Active Directory Federation Services in Azure.

Additionally, Microsoft Entra ID offers a feature called Microsoft Entra ID B2B (business-to-business) collaboration. This allows you to add users who do not belong to your company, inviting external users to be members of your Microsoft Entra ID. These guest users can then be granted access to your resources. For more information, see What is guest user access in Microsoft Entra ID B2B.

To learn more, see:

* [Deploying Active Directory Federation Services in Azure](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs).
* [What is guest user access in Microsoft Entra ID B2B?](https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b)

**Intune/Intune Suite & Microsoft Copilot for Security**

Microsoft Copilot for Security integrates with Microsoft Entra ID, utilizing the established identifiers, roles, and permissions configured within Entra ID to perform specific functions and actions within enhanced applications.

Intune/Intune Suite can be configured to ensure that all devices are registered and authenticated before accessing organizational resources. It assists in identifying users and associating device actions with specific user actions through policy and device configurations.

To learn more, see:

* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)

**Microsoft Graph**

A user in Microsoft Graph is one among the millions who use Microsoft 365 cloud services. It is the focal point whose identity is protected, and access is well managed. The user's data is what drives businesses. Microsoft Graph services makes this data available to businesses in rich contexts, real-time updates, and deep insights, and, always only with the appropriate permissions. A Microsoft 365 group is the fundamental entity that lets users collaborate. It integrates with other services, enabling richer scenarios in task planning, teamwork, education, and more.

To learn more, see:

* [Microsoft Graph overview](https://learn.microsoft.com/en-us/graph/overview)

[**Azure Policies**](#_Azure_Policy)

* [**IA.L1-3.5.1 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#identify-system-users-processes-acting-on-behalf-of-users-and-devices)

**Azure**

**Customer Responsibility**

* Uniquely identifying and authenticating organizational users

Federal user entities are responsible for properly identifying and authenticating federal users via ADFS

**GCCH**

**Customer Responsibility:**

* Government customers are responsible for uniquely identifying and authenticating their organizational users via their Active Directory infrastructure.
  + When a user of an organization employing ADFS attempts to access Office 365, the user is redirected to a login page hosted on the customer’s ADFS server. The user provides their credentials to their ADFS server, which attempts to authenticate the credentials using the customer’s existing Active Directory infrastructure. If the credentials are authenticated, the customer’s ADFS server issues a SAML ticket containing information about the user’s identity and group membership. The customer ADFS server signs this ticket using one half of an asymmetric key pair and the user sends the ticket to Microsoft Entra ID via encrypted TLS 1.2. MICROSOFT ENTRA ID validates the signature using the other half of the asymmetric key pair and grants access based on the ticket.
  + Customers are responsible for enforcing organizationally appropriate identification and authentication requirements at their ADFS server, including the use of unique identifiers.

**Additional Resources**

* [Extend on-premises AD FS to Azure](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/adfs)
* [Active Directory Federation Services](https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services)

IA.L1-3.5.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-2, IA-3, IA-5 | |
| **Practice:** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.  **Assessment Objectives:**  [a] the identity of each user is authenticated or verified as a prerequisite to system access;  [b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and  [c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC  Microsoft Entra ID Multi-Factor Authentication  Conditional Access  Intune/Intune Suite | Customer Lockbox  Privileged Identity Management (PIM)  Microsoft 365 Defender  Microsoft 365 Admin Center  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Entra ID & Conditional Access**

Administrators of Microsoft Entra ID can decide if a user has access to a particular resource by requiring that the user be authenticated with a username and password and has the authorization to access that resource.

Azure Conditional Access allows you to create policies that are applied against users. These policies use *assignments* and *access controls* to configure access to your resources. Assignments define who a policy applies to. It can apply to users, groups of users, roles in your Microsoft Entra ID , or to guest users. You can also specify that a policy only applies to specific applications, such as Microsoft 365.

Assignments can also define conditions that must be met (such as requiring a certain platform such as iOS, Android, Windows, and so on), specific locations by IP address, and more. Access controls determine how a Conditional Access policy is enforced. The most restrictive access control is block access, but you can also use access controls to require that a user use a device that meets certain conditions, that they are using an approved application to access your resources, that they are using MFA, and so on.

To create a Conditional Access policy, search for Microsoft Entra ID Conditional Access in the Azure portal. You can also use the Microsoft 365 Admin Center, the Microsoft Entra ID Admin Center, or Azure PowerShell to manage Microsoft Entra ID User accounts. The Microsoft Entra ID Admin Center gives you a greater set of options for managing the properties of user accounts than the Microsoft 365 Admin Center.

To learn more, see:

* [What is Conditional Access?](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview)
* [Building a Conditional Access policy](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies)

**Microsoft Entra ID Multi-Factor Authentication & Microsoft Copilot for Security**

By default, users can log in to your Microsoft Entra ID using only a username and password. Even if you require your users to use strong passwords, allowing access to your resources with only a username and password is risky.

Multifactor authentication solves this problem. The concept behind multifactor authentication is that you must authenticate using a combination of:

* Something you know, such as a username and password
* Something you have, such as a phone or mobile device
* Something you are, such as facial recognition or a fingerprint

Even though Azure multifactor authentication is two-factor, if you are using a mobile device that includes biometric features, you might be authenticating using three-factor authentication. However, the third factor is enforced by your mobile device and not by Azure. Azure multifactor authentication does not require three-factor authentication.

Microsoft Copilot for Security integrates with Microsoft Entra ID to utilize its robust authentication mechanisms. This ensures that users are authenticated using secure methods such as multi-factor authentication (MFA) before gaining access to sensitive systems and data.

To learn more, see:

* [How it works: Microsoft Entra ID Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks)
* [Plan an Microsoft Entra ID Multi-Factor Authentication deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)

**Azure Role Role-based access control (RBAC)**

Azure implements RBAC across all Azure resources, so you can control how users and applications can interact with your Azure resources. You might want to allow users who administer your databases to have access to databases in a particular resource group, but you do not want to allow those people to create new databases or delete existing databases. You might also want some web developers to be able to deploy new code to your web applications, but you do not want them to be able to scale the app to a higher-priced plan. These are just two examples of what you can do with RBAC in Azure to manage access and authorization.

To learn more, see:

* [What is Azure role-based access control (Azure RBAC)?](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)
* [Azure built-in roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles)
* [Azure custom roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles)

**Additional Information:**

The scope of RBAC is defined by where the RBAC role is assigned. For example, if you open a resource group in the portal and assign an RBAC role to a user, the scope is at the resource group level. On the other hand, if you open aweb app within that resource group and assign the role, the scope is to that web app only.

RBAC roles can be scoped to the management group, subscription, resource group, or resource level.

Microsoft Copilot for Security ensures that access to systems and data is governed by RBAC policies set in Microsoft Entra ID. This means users can only access resources necessary for their roles, minimizing the risk of unauthorized access.

**Microsoft Entra ID**

Microsoft Entra ID Connect supports a variety of sign-in options. You configure which one you want to use when setting up Microsoft Entra ID Connect. The default method, Password Synchronization, is appropriate for most organizations who will use Microsoft Entra ID Connect to synchronize identities to the cloud.

To learn more, see: [What is Microsoft Entra ID Connect?](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect)

**Active Directory Federation**

This allows users to authenticate to Microsoft Entra ID resources using on-premises credentials. It also requires the deployment of an Active Directory Federation Services infrastructure. This is the most complicated identity synchronization configuration for Microsoft 365 and is likely to be implemented in environments with complicated identity configurations.

To learn more, see: [AD FS Overview.](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview)

**Intune/Intune Suite & Conditional Access & Microsoft Copilot for Security**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions.

By working with Intune and Intune Suite, Microsoft Copilot for Security enforces security policies that require devices to be compliant and authenticated before accessing organizational resources. This includes verifying that devices meet security standards and are not compromised.

Copilot leverages Conditional Access policies configured in Microsoft Entra ID. These policies ensure that access to resources is granted only if specific conditions are met, such as device compliance status, user location, and risk level.

* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)
* [Microsoft Copilot in Intune features overview](https://learn.microsoft.com/en-us/mem/intune/copilot/copilot-intune-overview)

**Customer Lockbox**

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. Members of the Customer Lockbox access approver role manage customer lockbox requests for the tenancy. Users that hold this role can approve or deny requests using the Microsoft 365 Admin center. Users that hold this role are also able to enable and disable the Customer Lockbox feature. Only users that hold the Global Administrator role are able to reset the password of users that hold the Customer Lockbox access approver role.

To learn more, see [Customer Lockbox for Microsoft Azure.](https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview)

[**Azure Policies**](#_Azure_Policy)

* [**IA.L1-3.5.2 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#authenticate-or-verify-the-identities-of-users-processes-or-devices-as-a-prerequisite-to-allowing-access-to-organizational-systems)

**Azure**

**Customer Responsibility**

* Implementing device identification and authentication prior to establishing a connection.
* Federal user entities, as well as other customers using identity federation, are responsible for federal/customer user authenticator management and content.

**GCCH**

**Customer Responsibility:**

* Government customers are responsible for management of user authenticators within their Active Directory infrastructure.

**Additional Resources**

* [Details of the CMMC L2 Regulatory Compliance built-in initiative](https://docs.microsoft.com/en-us/azure/governance/policy/samples/cmmc-l3#identification-and-authentication)

IA.L2-3.5.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-2(1), IA-2(2) | |
| **Practice:** Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.  **Assessment Objectives:**  [a] privileged accounts are identified;  [b] multifactor authentication is implemented for local access to privileged accounts;  [c] multifactor authentication is implemented for network access to privileged accounts; and  [d] multifactor authentication is implemented for network access to non-privileged  accounts. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID Multi-Factor Authentication | Microsoft Entra ID  Microsoft Azure Portal  Azure Bastion  Conditional Access  VPN Gateway  Intune/Intune Suite  Privileged Identity Management (PIM)  GitHub Enterprise Cloud  GitHub AE |

**Implementation Statement:**

Configure Conditional Access policies to [require MFA for all users](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa) using the Azure portal. Configure device management policies using [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  to enforce Microsoft Entra ID Multi-Factor Authentication (MFA) for devices. Creating a [compliance policy](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#compliance-policy-settings) will define the rules and settings that a user’s device must meet to be compliant. Combine this with [Conditional Access](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#integrate-with-conditional-access) to enable the ability to block users and devices that do not meet the rules.

To learn more, see:

* [Deployment considerations for Microsoft Entra ID Multi-Factor Authentication](https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)

[**Azure Policies**](#_Azure_Policy)

* [IA.L2-3.5.3 Azure Policies](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#use-multifactor-authentication-for-local-and-network-access-to-privileged-accounts-and-for-network-access-to-non-privileged-accounts)

**Customer Responsibility**

* Implementing multifactor authentication for network access to privileged accounts.
* Implementing multifactor authentication for network access to non-privileged accounts.

**Additional Resources**

* [Authentication best practices for Microsoft Teams shared device management of Android devices.](https://learn.microsoft.com/en-us/microsoftteams/devices/authentication-best-practices-for-android-devices)
* [How to enable multifactor authentication in Azure](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)
* [Multi-factor authentication and Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-require-mfa)
* [GitHub – Requiring two-factor authentication in your organization](https://docs.github.com/en/organizations/keeping-your-organization-secure/requiring-two-factor-authentication-in-your-organization)
* [Enable Microsoft Entra ID Multi-Factor Authentication (MFA) for VPN users](https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-mfa)

IA.L2-3.5.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-2(8) | |
| **Practice:** Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.  **Assessment Objectives:**  [a] replay-resistant authentication mechanisms are implemented for network account  access to privileged and non-privileged accounts. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID Multi-Factor Authentication  Intune/Intune Suite  Windows Hello for Business  Microsoft Azure Portal  Microsoft Entra ID | Conditional Access  Privileged Identity Management (PIM) |

**Implementation Statement:**

All Microsoft Entra ID authentication methods at Authentication Assurance Level 2 & 3 use either nonce or challenges and are resistant to replay attacks. Configure Conditional Access policies to [require MFA for all users](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa) using the Azure portal. Configure device management policies using [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  to enforce Microsoft Entra ID Multi-Factor Authentication for devices. Creating a [compliance policy](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#compliance-policy-settings) will define the rules and settings that a user’s device must meet to be compliant. Combine this with [Conditional Access](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#integrate-with-conditional-access) to enable the ability to block users and devices that meet the rules.

**Windows Hello for Business**

Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. Windows Hello for Business, which is configured by Group Policy or mobile device management (MDM) policy, always uses key-based or certificate-based authentication.

**Azure**

**Customer Responsibility**

* Implementing replay-resistant authentication mechanisms for network access to privileged accounts.
* Implementing replay-resistant authentication mechanisms for network access to non-privileged accounts.

**GCCH**

**Customer Responsibility:**

* Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Office 365. Office 365 requires customers to implement ADFS to leverage organizational, multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. Customers configure their ADFS server to enforce identification and authentication requirements; ADFS uses the same multifactor authentication, including replay resistance, as the customer’s internal Active Directory/Domain infrastructure.

**Additional Resources**

* [Details of the CMMC L2 Regulatory Compliance built-in initiative](https://docs.microsoft.com/en-us/azure/governance/policy/samples/cmmc-l3#identification-and-authentication)

IA.L2-3.5.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-4 | |
| **Practice:** Prevent the reuse of identifiers for a defined period.  **Assessment Objectives:**  [a] a period within which identifiers cannot be reused is defined; and  [b] reuse of identifiers is prevented within the defined period. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Entitlement Management | Intune/Intune Suite  Conditional Access |

**Implementation Statement:**

**Microsoft Entra ID**

Assign and manage individual account identifiers and status in [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/) in accordance with existing organizational policies. Take appropriate action on those user accounts by removing their privileged access rights or by deleting the account.

Govern access for external users in Microsoft Entra ID entitlement management You can [manage the lifecycle of external](https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users) users by blocking their access after a defined period. Ensure that organizational policy maintains all accounts that remain in the disabled state for a defined period, after which they can be removed.

**Azure**

**Customer Responsibility**

* Preventing identifier reuse for the customer-defined time period.

**GCCH**

* **Customer Responsibility:**All customers using ADFS authentication, including government customers, are responsible for preventing the reuse of user identifiers via their Active Directory infrastructure. Customers not using ADFS are responsible for not reusing user identifiers.

IA.L2-3.5.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-4 | |
| **Practice:** Disable identifiers after a defined period of inactivity.  **Assessment Objectives:**  [a] a period of inactivity after which an identifier is disabled is defined; and  [b] identifiers are disabled after the defined period of inactivity. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Entitlement Management | Microsoft Defender for Cloud Apps  Intune/Intune Suite  Microsoft Defender for Identity  Conditional Access |

**Implementation Statement:**

**Microsoft Defender for Identity**

Use activity filters and create action policies with [Microsoft Defender for Identity](https://docs.microsoft.com/en-us/defender-for-identity/activities-filtering-mcas) in Microsoft Defender for Cloud Apps. [Assess dormant sensitive entities](https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-dormant-entities#how-do-i-use-this-security-assessment) as part of your organizations security policy. Organizations that fail to secure their dormant user accounts leave the door unlocked to their sensitive data safe.

**Microsoft Entra ID and Entitlement Management**

Assign and manage individual account identifiers and status in [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/) in accordance with existing organizational policies. Take appropriate action on those user accounts by removing their privileged access rights or by deleting the account.

Entitlement Management allows you to manage employee access and govern access for external users. You can [manage the lifecycle of external](https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users) users by blocking their access after a defined period. Ensure that organizational policy maintains all accounts that remain in the disabled state for a defined period, after which they can be removed.

**Azure**

**Customer Responsibility**

* Disabling identifiers after a customer-defined time period of inactivity.

**Additional Resources**

* [Create an access review of groups and applications in Microsoft Entra ID access reviews](https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review)
* [Detect inactive user accounts](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-manage-inactive-user-accounts#how-to-detect-inactive-user-accounts)  
  [How to manage inactive user accounts in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-manage-inactive-user-accounts)   
  [How to manage stale devices in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/devices/manage-stale-devices)
* [View Sign-in Logs](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-powershell-reporting#sign-in-logs)
* [Regularly check for and remove inactive user accounts on Active Directory](https://docs.microsoft.com/en-us/services-hub/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory)
* [Details of the CMMC L2 Regulatory Compliance built-in initiative](https://docs.microsoft.com/en-us/azure/governance/policy/samples/cmmc-l3#identification-and-authentication)

IA.L2-3.5.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-5(1) | |
| **Practice:** Enforce a minimum password complexity and change of characters when new passwords are created.  **Assessment Objectives:**  [a] password complexity requirements are defined;  [b] password change of character requirements are defined;  [c] minimum password complexity requirements as defined are enforced when new  passwords are created; and  [d] minimum password change of character requirements as defined are enforced when new passwords are created. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID | Intune/Intune Suite Microsoft Entra ID Password Protection  Conditional Access |

**Implementation Statement:**

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password complexity means using different types of characters as well as a specified number of characters. This applies to both the creation of new passwords and the modification of existing passwords. Characters to manage complexity include numbers, lowercase and uppercase letters, and symbols. To accomplish this, you need a good password policy.

**Microsoft Entra ID**

A good password policy is the first step on securing your environment and company data. Without a password policy, passwords may be created that increase the probability that passwords can be easily guessed, or brute forced.

To learn more, see:

* [Create a customer password policy.](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy#create-a-custom-password-policy)
* [Password policies and account restrictions in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy)

**Microsoft Entra ID Password Protection**

Microsoft Entra ID has a password protection feature that blocks commonly attacked passwords and variations and also enables a custom banned list of passwords that automatically have common character substitutions. This way you can block passwords that are primarily focused on organizational-specific terms like brand names and product names.

The password protection feature integrates with Active Directory through agent password filters deployed to the domain controllers and which enforce or audit the use of banned passwords that have been configured in the Microsoft Entra ID tenant via a deployed proxy service for hybrid scenarios.

Microsoft has a list of global banned passwords that is kept up to date by analyzing Microsoft Entra ID security telemetry data. They look for commonly used passwords that are weak and/or compromised. *It is important to note that Microsoft does not use third-party/public password lists – all data is coming from Microsoft Entra ID itself.*

To learn more, see:

* [Globally banned password list](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#global-banned-password-list)
* [Custom banned password list](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custom-banned-password-list)

**Intune/Intune Suite**

Using [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  you can use policies to enforce [password requirements](https://docs.microsoft.com/en-us/mem/intune/user-help/password-does-not-meet-it-administrator-requirements) for devices. Creating a [compliance policy](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#compliance-policy-settings) will define the rules and settings that a user’s device must meet to be compliant. Combine this with [Conditional Access](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#integrate-with-conditional-access) to enable the ability to block users and devices that do not meet the rules.

[**Azure Policies**](#_Azure_Policy)

* [**IA.L2-3.5.7 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#enforce-a-minimum-password-complexity-and-change-of-characters-when-new-passwords-are-created)

**Azure**

**Customer Responsibility**

* Enforcing password complexity requirements (i.e., case sensitivity; number of characters; and the mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type).

**GCCH**

**Customer Responsibility**

* Government customers are responsible for enforcing password complexity in compliance with their organizational policies and requirements for their organizational users.

**Additional resources**

* [Risk detections in Microsoft Entra ID Identity Protection](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-types-and-detection) such as leaked credentials on the dark web.
* [Microsoft Entra ID smart lockout](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout)

IA.L2-3.5.8

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-5(1) | |
| **Practice:** Prohibit password reuse for a specified number of generations.  **Assessment Objectives:**  [a] the number of generations during which a password cannot be reused is specified and  [b] reuse of passwords is prohibited during the specified number of generations. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID | Intune/Intune Suite  Microsoft Entra ID Password Protection  Conditional Access |

**Implementation Statement:**

Individuals may not reuse their passwords for a defined period of time and a set number of passwords generated, you can enforce this with password history in on-premises Active Directory (AD). In Microsoft Entra ID , the last password cannot be used again when the user changes a password. The password policy is applied to all user accounts that are created and managed directly in Microsoft Entra ID. This password policy cannot be modified.

**Microsoft Entra ID**

Use [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  to configure a [custom password policy](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy#create-a-custom-password-policy) and [Microsoft Entra ID Password Protection.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises) To meet this requirement, use a combination of security settings; the policy should enforce password history and have a minimum password age. For example, if you configure the Enforce password history policy setting to ensure that users cannot reuse any of their last 12 passwords, but you do not configure the Minimum password age policy setting to a number that is greater than 0, users could change their password 13 times in a few minutes and reuse their original password.

To learn more, see:

* [Create a customer password policy](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy#create-a-custom-password-policy)
* [Password policies and account restrictions in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy)

**Intune/Intune Suite**

Using [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  you can use policies to enforce [password requirements](https://docs.microsoft.com/en-us/mem/intune/user-help/password-does-not-meet-it-administrator-requirements) for devices. Creating a [compliance policy](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#compliance-policy-settings) will define the rules and settings that a user’s device must meet to be compliant. Combine this with [Conditional Access](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#integrate-with-conditional-access) to enable the ability to block users and devices that do not meet the rules.

[**Azure Policies**](#_Azure_Policy)

* [**IA.L2-3.5.8 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#prohibit-password-reuse-for-a-specified-number-of-generations)

**Azure**

**Customer Responsibility**

* Employing password-based authentication to customer-deployed resources and defining the number of password generations that are prohibited from reuse (e.g., 10 most recent passwords may not be reused when creating a new password).

**Additional Resources**

* [Details of the CMMC L2 Regulatory Compliance built-in initiative](https://docs.microsoft.com/en-us/azure/governance/policy/samples/cmmc-l3#identification-and-authentication)

IA.L2-3.5.9

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-5(1) | |
| **Practice:** Allow temporary password use for system logons with an immediate change to a permanent password.  **Assessment Objective:**  [a] an immediate change to a permanent password is required when a temporary password is used for system logon. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID |  |

**Implementation Statement:**

**Microsoft Entra ID**

When creating a new user or resetting their password using [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  , a temporary password is auto generated for the user. The temporary password never expires. The user will be required to change the password during the next sign-in process.

The time a user must wait to change the password is determined by password policy settings, specifically the minimum password age. The Minimum password age policy setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow password changes immediately by setting the number of days to 0.

[Windows security baselines](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines) recommend setting [Minimum password age](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-age#reference)to one day. Note: If you set a password for a user and you want that user to change the administrator-defined password, you must select the user must change password at next logon check box. Otherwise, the user will not be able to change the password until the number of days specified by Minimum password age.

Passwordless authentication methods, such as FIDO2 and Passwordless Phone Sign-in through the Microsoft Authenticator app, enable users to sign in securely without a password. Users can bootstrap Passwordless methods in one of two ways:

• Using existing Microsoft Entra ID Multi-Factor Authentication methods

• Using a Temporary Access Pass (TAP)

A Temporary Access Pass is a time-limited passcode issued by an admin that satisfies strong authentication requirements and can be used to onboard other authentication methods, including Passwordless ones. The most common use for a Temporary Access Pass is for a user to register authentication details during the first sign-in, without the need to complete additional security prompts. Authentication methods are registered at https://aka.ms/mysecurityinfo. Users can also update existing authentication methods here.

**Azure**

**Customer Responsibility**

* Employing password-based authentication to customer-deployed resources, including the ability to issue users a temporary password with the requirement to immediately change to a permanent password upon login.

**Additional Resources**

* [Reset a user’s password using Microsoft Entra ID to auto-generate a temporary password](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-reset-password-azure-portal#:~:text=When%20using%20Azure%20Active%20Directory,the%20next%20sign%2Din%20process.)
* [Security Considerations](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-age#security-considerations)

IA.L2-3.5.10

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-5(1) | |
| **Practice:** Store and transmit only cryptographically protected passwords.  **Assessment Objectives:**  [a] passwords are cryptographically protected in storage; and  [b] passwords are cryptographically protected in transit. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Microsoft Azure Portal  Azure Key Vault | Intune/Intune Suite |

**Implementation Statement:**

**Microsoft Entra ID and Azure Key Vault**

Azure Key Vault security [access model](https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#access-model-overview)s use Microsoft Entra ID for authentication. Authentication with Key Vault works in conjunction with Microsoft Entra ID, which is responsible for authenticating the identity of any given security principal.

Store and transmit cryptographically protected passwords using [Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts). Using the Azure portal, you can [create your Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/quick-create-portal#create-a-vault). You can securely store and access secrets, such as API keys, passwords, certificates, or cryptographic keys. This is useful for websites, apps, and background processes where the application should not have access to credentials.

[**Azure Policies**](#_Azure_Policy)

* [**IA.L2-3.5.10 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#store-and-transmit-only-cryptographically-protected-passwords)

**Customer Responsibility**

* Employing password-based authentication, which stores and transmits cryptographically protected passwords, for customer-deployed resources.

**Additional Resources**

* [Set and retrieve a secret from Key Vault using Azure Portal](https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-portal)
* [Create and encrypt a Windows virtual machine with the Azure Portal](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-portal-quickstart#encrypt-the-virtual-machine)
* [Secure VM password with Key Vault](https://azure.microsoft.com/en-us/resources/templates/101-vm-secure-password/)
* [Intune Data Warehouse application-only authentication](https://docs.microsoft.com/en-us/mem/intune/developer/data-warehouse-app-only-auth)
* [Security baseline for Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/security-baseline)

IA.L2-3.5.11

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IA-6 | |
| **Practice:** Obscure feedback of authentication information. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID | Azure Bastion  Azure Virtual Machines  Microsoft Azure Portal  Intune/Intune Suite |

**Implementation Statement:**

By default, Microsoft Entra ID obscures all passwords. Microsoft’s [Password boxes](https://docs.microsoft.com/en-us/windows/uwp/design/controls-and-patterns/password-box) conceal the characters typed into it for purposes of privacy. By default, the password box provides a way for the user to view their password by holding down a reveal button.

You can disable this feature for Windows 10 using [policy](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialsui) as an added security measure to ensure your password can not be displayed on the login screen.

**Customer Responsibility**

* Obscuring authentication feedback information during the authentication process for any customer-deployed resources.

### Incident Response (IR) N

IR.L2-3.6.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IR-2, IR-4, IR-5, IR-6, IR-7 | |
| **Practice:** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.  **Assessment Objectives:**  [a] an operational incident-handling capability is established;  [b] the operational incident-handling capability includes preparation;  [c] the operational incident-handling capability includes detection;  [d] the operational incident-handling capability includes analysis;  [e] the operational incident-handling capability includes containment;  [f] the operational incident-handling capability includes recovery; and  [g] the operational incident-handling capability includes user response activities | |
| **Primary Services** | **Secondary Services** |
| Microsoft Defender for Cloud Apps  Microsoft Sentinel | Microsoft Defender for Endpoint Microsoft Defender for Office 365  Microsoft Copilot for Security  Microsoft Defender for IoT  Microsoft 365 Defender  Insider Risk Management  Microsoft Entra ID  Microsoft Graph |

**Implementation Statement:**

**Microsoft Defender for Cloud Apps and Sentinel**

Incident Response encompasses the entire lifecycle of managing security incidents, including preparation, detection and analysis, containment, and post-incident activities. Azure services such as Microsoft Defender for Cloud Apps and Microsoft Sentinel support this control by automating the incident response process, ensuring an efficient and thorough approach.

First, ensure your organization has well-defined processes to respond to security incidents. These processes should be regularly updated for Azure and exercised to maintain readiness.

Set up security incident contact information in Microsoft Defender for Cloud Apps. This contact information is crucial for Microsoft to reach out if the Microsoft Security Response Center (MSRC) discovers unauthorized access to your data. Customize incident alerts and notifications in various Azure services based on your specific incident response needs.

Microsoft Defender for Cloud Apps generates high-quality alerts across many Azure assets. Use the ASC data connector to stream these alerts to Microsoft Sentinel, which allows you to create advanced alert rules that generate incidents automatically for investigation. Export alerts and recommendations from Microsoft Defender for Cloud Apps either manually or continuously to help identify risks to Azure resources.

Connect your data sources, such as Microsoft Defender for IoT, Microsoft 365 Compliance Center, Azure Firewall, and Microsoft Defender for Endpoint, to Microsoft Sentinel for centralized detection and reporting. Microsoft Sentinel provides out-of-the-box templates for creating threat detection rules, designed by Microsoft's security experts. These rules automatically search your environment for suspicious activities and generate alerts, which create incidents for investigation

Microsoft Sentinel offers extensive data analytics across various log sources and a case management portal to handle the full lifecycle of incidents. Intelligence gathered during investigations can be associated with incidents for tracking and reporting.

Additionally, use tags and a naming system to identify and categorize Azure resources, prioritizing the remediation of alerts based on the criticality of the affected resources. Workflow automation features in Microsoft Defender for Cloud Apps and Microsoft Sentinel can automatically trigger actions or run playbooks in response to security alerts. These playbooks can perform actions such as sending notifications, disabling accounts, and isolating problematic networks

To learn more, see:

* [Implement security across the enterprise environment](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/security/security-top-10#3-process-assign-accountability-for-cloud-security-decisions) and [Incident response reference guide](https://docs.microsoft.com/en-us/microsoft-365/downloads/IR-Reference-Guide.pdf)
* [Set up security incident contact information](https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details)
* [How to configure export](https://docs.microsoft.com/en-us/azure/security-center/continuous-export)
* [How to stream alerts into Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center).
* [Connect your data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources)
* [Out-of-the-box, built-in templates](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in#use-out-of-the-box-detections)
* [Set up automated threat responses in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook).
* [Investigate incidents with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases).
* [mark resources using tags and create a naming system](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json)
* [workflow automation](https://docs.microsoft.com/en-us/azure/security-center/workflow-automation)
* [Set up automated threat responses in Microsoft Defender for Cloud Apps](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident#triage-security-alerts)
* [Set up automated threat responses in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook).

**Microsoft Defender for Endpoint and Microsoft 365 Defender**

Investigate incidents affecting your network, understand their implications, and gather evidence to resolve them. Microsoft 365 Defender can automatically investigate and resolve alerts through automation and AI, performing additional remediation steps such as isolating devices from the network for contained investigations. Microsoft Defender for Endpoint automatically investigates incidents, providing auto-response and detailed information about critical files, processes, and services. Connect your data sources to Microsoft Sentinel for centralized incident handling capabilities, ensuring a comprehensive approach to security incident management.

To learn more, see:

* [Turn on Microsoft Defender XDR](https://learn.microsoft.com/en-us/defender-xdr/m365d-enable?view=o365-worldwide)
* [Automatically investigate and resolve](https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir?view=o365-worldwide)
* [Connect your data resources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources)

**Microsoft Copilot for Security**

Microsoft Copilot for Security works with Microsoft Defender XDR, Microsoft Sentinel, Microsoft Intune, Microsoft Defender Threat Intelligence, Microsoft Purview, and Microsoft Defender Attack Surface Management. Copilot for Security can access data from these products and provide assistive experience to increase the effectiveness and efficiency of security professionals using those solutions. Copilot for Security helps security professionals discover risks earlier, respond to them with greater guidance, and remain on top of vulnerabilities in the evolving threat landscape. Microsoft Entra is one of the Microsoft plugins that enable the Copilot for Security platform to generate accurate and relevant information. Through the Microsoft Entra plugin, the Copilot for Security portal can provide more context to incidents and generate more accurate results.

Copilot for Security works with Microsoft Purview by providing multiple capabilities summarizing alerts, triaging alerts, and drilling down into Purview data. These capabilities can be used to gain insight into Purview data and make connections between datapoints and help understand your information security and compliance posture. Copilot for Security delivers information about threat actors, indicators of compromise (IOCs), tools, vulnerabilities, and contextual threat intelligence.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Azure**

**Customer Responsibility**

* Implementing key incident handling capabilities including preparation, detection and analysis, containment, eradication, and recovery.
* Providing incident response support resources that are integral to the organizational incident response capability, providing advice and assistance to users handling security incidents.

**GCCH**

**Customer Responsibility:**

* Customers are responsible for implementing incident handling capability for insider threats for end users of any system that connects to Office 365.
* Office 365 offers the ability to remediate a data spillage event by using self-service features. These features allow customers to identify, contain, and remediate a data spill, and to perform post spill remediation. Customers are responsible for ensuring that information not authorized for storage or transmission within Office 365 GCC High is not stored on or transmitted via Office 365 GCC High services. If information is spilled, customer administrators with appropriate roles can quickly respond to a data spillage event without needing to contact Microsoft for support by using these self-service features.
  + Microsoft Support Services can be leveraged to assist a customer with activities, such as development of customer-specific procedures, policy implementation with regards to spillage and legal hold, modification of existing procedures to leverage the Office 365 self-service tools and providing government "cleared" resources for spillage activities. Microsoft Support Services, by default, does not have any permissions within the Office 365 service.

**Additional Resources**

* [Computer Security Incident Handling Guide](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
* [Incident preparation](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-security-incident-preparation)
* [Getting started with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility)
* [Incident response playbooks](https://docs.microsoft.com/en-us/security/compass/incident-response-playbooks)
* [Respond to your first incident walkthrough](https://docs.microsoft.com/en-us/microsoft-365/security/defender/first-incident-overview?view=o365-worldwide)

IR.L2-3.6.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IR-2, IR-4, IR-5, IR-6, IR-7 | |
| **Practice:** Track, document and report incidents to designated officials and/or authorities both internal and external to the organization.  **Assessment Objectives:**  [a] incidents are tracked;  [b] incidents are documented;  [c] authorities to whom incidents are to be reported are identified;  [d] organizational officials to whom incidents are to be reported are identified;  [e] identified authorities are notified of incidents; and  [f] identified organizational officials are notified of incidents. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel  Dynamics 365  Microsoft Entra ID | Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft 365 security center  Intune/Intune Suite  Microsoft 365 Defender  Microsoft Copilot for Security |

**Implementation Statement:**

Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies. Microsoft Sentinel supports the tracking, documenting, and reporting of incidents. Connect your sources to Microsoft Sentinel for one centralized location to manage incidents in your organization.

[Connect your data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) such as Microsoft Defender for IoT, Microsoft 365 security center, Azure Firewall and Microsoft Defender for Endpoint to Microsoft Sentinel for a centralized source of detection and reporting. Microsoft Sentinel provides [out-of-the-box, built-in templates](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in#use-out-of-the-box-detections) to help you create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can assign and investigate in your environment. To learn how to automate your responses to threats, [Set up automated threat responses in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook).

Incident reporting is a formal part of the incident closure process. In Microsoft Sentinel you can use workbooks, Workbooks provide a dashboard to summarize security data visually. Microsoft Sentinel includes numerous default dashboards and customizable templates to facilitate incident analysis.

To learn more, see

* [Quickstart: Get started with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility).
* [Dashboards and graphs](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility#get-visualization) in Microsoft Sentinel.

Microsoft Sentinel provides extensive data analytics across virtually any log source and a case management portal to manage the full lifecycle of incidents. Intelligence information during an investigation can be associated with an incident for tracking and reporting purposes. Learn how to [Investigate incidents with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases).

Additionally, [mark resources using tags and create a naming system](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json) to identify and categorize Azure resources, especially those processing sensitive data. It is your responsibility to prioritize the remediation of alerts based on the criticality of the Azure resources and environment where the incident occurred.

Use [workflow automation](https://docs.microsoft.com/en-us/azure/security-center/workflow-automation) features in Microsoft Defender for Cloud Apps and Microsoft Sentinel to automatically trigger actions or run a playbook to respond to incoming security alerts. The playbook takes actions, such as sending notifications, disabling accounts, and isolating problematic networks.

To learn more, see:

* [Set up automated threat responses in Microsoft Defender for Cloud Apps](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident#triage-security-alerts)
* [Set up automated threat responses in Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook)

**Microsoft Copilot for Security**

Respond to threats at the speed of AI with assisted incident investigation and response via the embedded experience in Microsoft Defender XDR, Copilot for Security provides summaries for active incidents and actionable step-by-step guidance for incident response, creating complete post-response activity. With Copilot for Security, users can gain structured and contextualized insights into emerging threats, attack techniques, and whether an organization is exposed to a specific threat. Copilot for Security helps prevent exposure to activity group campaigns and respond to incidents with greater guidance. Copilot for Security delivers information about threat actors, indicators of compromise (IOCs), tools, and vulnerabilities, as well as contextual threat intelligence from Microsoft Defender Threat Intelligence. Users can use prompts and promptbooks to investigate incidents, enrich their hunting flows with threat intelligence information, or gain more knowledge about their organization's or the global threat landscape.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Microsoft Security Response Center**

[Set up security incident contact information](https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details) in Microsoft Defender for Cloud Apps. This contact information is used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your data has been accessed by an unlawful or unauthorized party. You also have options to customize incident alert and notification in different Azure services based on your incident response needs. Additionally, if you are a security researcher and believe you have found a Microsoft security vulnerability, Microsoft would like to collaborate with you to investigate it. Please note that the Microsoft Security Response Center does not provide technical support for Microsoft products.

To learn more, see:

* [Report an issue and submission guidelines](https://www.microsoft.com/en-us/msrc/faqs-report-an-issue).

**Dynamics 365**

Microsoft Dynamics 365 Customer Service can act as a help desk ticketing system to serve a company's employees or customers needing support. You can define custom alert rules that monitor filtered views of data and automatically send email notifications when predefined events occur.

**Microsoft 365 Defender**

You can manage incidents from Incidents & alerts > Incidents on the quick launch of the Microsoft 365 Defender portal. There you can create email notifications; in the navigation pane, select Settings > Microsoft 365 Defender > Incident email notifications. This will allow you to automatically report incident to designated parties.

**Azure**

**Customer Responsibility**

* providing incident response training to users of customer-deployed resources in accordance with assigned roles and responsibilities.
* implementing key incident handling capabilities including preparation, detection and analysis, containment, eradication, and recovery.
* for incident monitoring of customer-deployed resources.
* for requiring personnel to report suspected security incidents to the organizational incident response capability.

**GCCH**

**Customer Responsibility:**

* Customers are responsible for implementing incident handling capability for insider threats for end users of any system that connects to Office 365.
* Office 365 offers the ability to remediate a data spillage event by using self-service features. These features allow customers to identify, contain, and remediate a data spill, and to perform post spill remediation. Customers are responsible for ensuring that information not authorized for storage or transmission within Office 365 GCC High is not stored on or transmitted via Office 365 GCC High services. If information is spilled, customer administrators with appropriate roles can quickly respond to a data spillage event without needing to contact Microsoft for support by using these self-service features.
  + Microsoft Support Services can be leveraged to assist a customer with activities, such as development of customer-specific procedures, policy implementation with regards to spillage and legal hold, modification of existing procedures to leverage the Office 365 self-service tools and providing government "cleared" resources for spillage activities. Microsoft Support Services, by default, does not have any permissions within the Office 365 service.

IR.L2-3.6.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** IR-3 | |
| **Practice:** Test the organizational incident response capability.  **Assessment Objective:**  [a] the incident response capability is tested. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Sentinel  Microsoft 365 Defender  Microsoft 365 Defender for Office 365  Microsoft Copilot for Security |

**Implementation Statement:**

Organizations are required to test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Microsoft 365 Defender has attack simulation capabilities that can be deployed to users. If your organization has Microsoft Defender for Office 365 Plan 2, which includes [Threat Investigation and Response capabilities](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-ti?view=o365-worldwide), you can use Attack Simulator in the M365 Compliance Center to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

You can use [Microsoft Sentinel to review incidents](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive) in your organization to create a walk-through or tabletop exercise simulating common threats among the organization. [Dashboards and graphs](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility#get-visualization) are customizable for high level visibility of incidents and can be used to create incident response training presentations. Microsoft Sentinel provides extensive data analytics across virtually any log source and a case management portal to manage the full lifecycle of incidents. Intelligence information during an investigation can be associated with an incident for tracking and reporting purposes. Learn how to [Investigate incidents with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases).

**Microsoft Copilot for Security**

Microsoft Copilot for Security does not perform the incident response exercises on behalf of organizations, however the information provided through its integrations with Microsoft Defender XDR, Microsoft Sentinel, Microsoft Intune, Microsoft Defender Threat Intelligence, Microsoft Purview, and Microsoft Defender Attack Surface Management can be used to re-create incidents that form the basis of incident response exercises, walkthroughs and testing the capability of your team's incident response.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Customer Responsibility**

* Testing the incident response capability of customer-deployed resources.

**Additional Resources**

* [NIST's publication - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](https://csrc.nist.gov/publications/detail/sp/800-84/final)

### Maintenance (MA)

MA.L2-3.7.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MA-2, MA-3, MA-3(1), MA-3(2) | |
| **Practice:** Perform maintenance on organizational systems.  **Assessment Objective:**  [a] system maintenance is performed. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Azure Portal Azure Virtual Machines  Intune/Intune Suite  Microsoft 365 Defender  Privileged Identity Management (PIM)  Azure Functions  Azure Automation  Azure Bastion |

**Implementation Statement:**

Performing controlled maintenance ensures up time through established processes such as change and configuration management. Maintenance windows are an important time to apply critical security updates and patches. Maintenance windows also incur risk as systems could crash without proper testing or authorized time windows. [Azure Maintenance Control](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-control) facilitates control of maintenance operations in the platform.

Manage platform updates, that do not require a reboot, using maintenance control. Azure frequently updates its infrastructure to improve reliability, performance, security or launch new features. Most updates are transparent to users. Some sensitive workloads, like gaming, media streaming, and financial transactions, can’t tolerate even few seconds of a VM freezing or disconnecting for maintenance. Maintenance control gives you the option to wait on platform updates and apply them within a 35-day rolling window.

Maintenance control lets you decide when to apply updates to your isolated VMs. With maintenance control, you can:

* Batch updates into one update package.
* Wait up to 35 days to apply updates.
* Automate platform updates for your maintenance window using [Azure Functions](https://github.com/Azure/azure-docs-powershell-samples/tree/master/maintenance-auto-scheduler).
* Maintenance configurations work across subscriptions and resource groups.

To apply maintenance control to an Azure VM, the VM must be on a [dedicated host](https://docs.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts) or created with an [isolated VM size](https://docs.microsoft.com/en-us/azure/virtual-machines/isolation). After 35 days, an update will be automatically applied. The controlling user must have resource contributor access. To learn more, see [Control updates with Maintenance Control and Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-control-powershell).

**Intune/Intune Suite**

As part of Microsoft Endpoint Manager, Configuration Manager sites and hierarchies require regular maintenance and monitoring to provide services effectively and continuously. Regular maintenance ensures that the hardware, software, and Configuration Manager database continue to function correctly and efficiently. Optimal performance greatly reduces the risk of failure. You can configure alerts and use the built-in status message system to understand the state of your Configuration Manager environment.

**Privileged Identity Management (PIM)**

PIM provides a time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions to important resources. These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. You assign users the role with the [least privileges necessary to perform their tasks](https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task). This practice minimizes the number of Global Administrators and instead uses specific administrator roles for certain scenarios such as performing maintenance tasks.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Customer Responsibility**

* Responsible for scheduling, performing, documenting, and reviewing remote maintenance and repair records for all customer-deployed operating systems in accordance with organizational requirements.

**Additional Resources**

* [Maintenance for virtual machines in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-and-updates)
* [Handling planned maintenance notifications](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-notifications)
* [Azure Automation Update Management overview](https://learn.microsoft.com/en-us/azure/automation/update-management/overview?context=%2Fazure%2Fvirtual-machines%2Fcontext%2Fcontext)

MA.L2-3.7.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MA-2, MA-3, MA-3(1), MA-3(2) | |
| **Practice:** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  **Assessment Objectives:**  [a] tools used to conduct system maintenance are controlled;  [b] techniques used to conduct system maintenance are controlled;  [c] mechanisms used to conduct system maintenance are controlled; and  [d] personnel used to conduct system maintenance are controlled. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC  Privileged Identity Management (PIM) | Azure Bastion Intune/Intune Suite  Conditional Access  Network Security Groups  Microsoft 365 Defender  Microsoft Entra ID Multi-Factor Authentication |

**Implementation Statement:**

**Network Security Groups**

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. To simplify maintenance of your security rule definition, combine augmented security rules with [service tags](https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview) or [application security groups](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#application-security-groups).  For security reasons it is good practice to lock down access to Azure resources and not leave management ports open to the internet. One way to restrict access to remote access protocols like RDS / SSH is to create a Network Security Groups (NSG) and apply this to either virtual machines or virtual network subnets.

**Microsoft Entra ID**

Controlling maintenance operations ensures confidentiality of data during maintenance operations. Maintenance windows incur risk not only to downtime, but also to unauthorized users obtaining rights to systems. One option for controlling maintenance operations is through Microsoft Entra ID Role Based Access and Microsoft Entra ID Multi-Factor Authentication. It's a best practice to manage to least privilege. Least privilege means you grant your administrators exactly the permission they need to do their job. There are three aspects to consider when you assign a role to your administrators: a specific set of permissions, over a specific scope, for a specific period of time. Avoid assigning broader roles at broader scopes even if it initially seems more convenient to do so. By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised. Microsoft Entra ID RBAC supports over 65 [built-in roles](https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference). There are Microsoft Entra ID roles to manage directory objects like users, groups, and applications, and also to manage Microsoft 365 services like Exchange, SharePoint, and Intune. To better understand Microsoft Entra ID built-in roles, see [Understand roles in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles) . If there isn't a built-in role that meets your need, you can create your own [custom roles](https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create).

**Microsoft Entra ID Multi-Factor Authentication**

[Multi Factor Authentication (MFA)](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks) is one of the strongest security controls in a cloud computing environment. MFA is an important conditional access requirement for maintenance personnel. People connect from organization-owned, personal, and public devices on and off the corporate network using smart phones, tablets, PCs, and laptops, often on multiple platforms. In this always-connected, multi-device and multi-platform world, the security of user accounts is more important than ever. Passwords, no matter their complexity, used across devices, networks, and platforms are no longer sufficient to ensure the security of the user account, especially when users tend to reuse passwords across accounts. Sophisticated phishing and other social engineering attacks can result in usernames and passwords being posted and sold across the dark web.

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Microsoft Entra ID Multi-Factor Authentication is deployed by enforcing policies with [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa). A Conditional Access policy can require users to perform multi-factor authentication when certain criteria are met such as:

* All users, a specific user, member of a group, or assigned role
* Specific cloud application being accessed
* Device platform
* State of device
* Network location or geo-located IP address
* Client applications
* Sign-in risk (Requires Identity Protection)
* Compliant device
* Hybrid Microsoft Entra ID joined device
* Approved client application

Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. To learn more, see [Planning a cloud-based Microsoft Entra ID Multi-Factor Authentication deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted).

Additionally, performing controlled maintenance ensures uptime through established processes such as change and configuration management. Maintenance windows are an important time to apply critical security updates and patches. Maintenance windows also incur risk as systems could crash without proper testing or authorized time windows. [Azure Maintenance Control](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-control) facilitates control of maintenance operations in the platform.

Manage platform updates, that do not require a reboot, using maintenance control. Azure frequently updates its infrastructure to improve reliability, performance, security or launch new features. Most updates are transparent to users. Some sensitive workloads, like gaming, media streaming, and financial transactions, can’t tolerate even few seconds of a VM freezing or disconnecting for maintenance. Maintenance control gives you the option to wait on platform updates and apply them within a 35-day rolling window.

Maintenance control lets you decide when to apply updates to your isolated VMs. With maintenance control, you can:

* Batch updates into one update package.
* Wait up to 35 days to apply updates.
* Automate platform updates for your maintenance window using [Azure Functions](https://github.com/Azure/azure-docs-powershell-samples/tree/master/maintenance-auto-scheduler).
* Maintenance configurations work across subscriptions and resource groups.

To apply maintenance control to an Azure VM, the VM must be on a [dedicated host](https://docs.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts) or created with an [isolated VM size](https://docs.microsoft.com/en-us/azure/virtual-machines/isolation). After 35 days, an update will be automatically applied. The controlling user must have resource contributor access. To learn more, see [Control updates with Maintenance Control and Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-control-powershell)

**Azure Bastion**

As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

**Privileged Identity Management (PIM)**

PIM provides a time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions to important resources. These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. You assign users the role with the [least privileges necessary to perform their tasks](https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task). This practice minimizes the number of Global Administrators and instead uses specific administrator roles for certain scenarios such as performing maintenance tasks.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Customer Responsibility**

* Responsible for approving, controlling and monitoring system maintenance tools used on customer-deployed operating systems.

**Additional Resources**

* [Add users and grant administrative permission to Intune](https://docs.microsoft.com/en-us/mem/intune/fundamentals/users-add)
* [Learn about Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access)

MA.L2-3.7.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MA-2 | |
| **Practice:** Ensure equipment removed for off-site maintenance is sanitized of any CUI.  **Assessment Objective:**  [a] equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Purview |

**Implementation Statement:**

To ensure equipment removed for off-site maintenance is sanitized of any CUI, you will need identify what data is considered CUI. Discovery and labeling sensitive data are the first steps to controlling data security. Labeling sensitive data is something organizations should implement across both physical and logical media. Government regulations such as [NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)](https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-nist-sp-800-171?view=o365-worldwide) implicitly specify controls for protecting controlled unclassified information (CUI). This requirement spans across all industries and geographies. The European Union requires secure handing of personally identifiable information (PII) in the [General Data Protection Regulation (GDPR)](https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview) and California has recently implemented a similar regulation with the [California Consumer Privacy Regulation (CCPA)](https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-ccpa?view=o365-worldwide).

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Customer Responsibility**

* Removed CUI from equipment such as laptops removed for off-site maintenance.
* After running the MIP scanner, the customer must securely erase the CUI data.

MA.L2-3.7.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MA-3(2) | |
| **Practice:** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  **Assessment Objectives:**  [a] media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Defender for Endpoint |

**Implementation Statement:**

As part of troubleshooting, a vendor may provide a diagnostic application to install on a system. As this is executable code, there is a chance that the file is corrupt or infected with malicious code. Implement procedures to scan any files prior to installation. The same level of scrutiny must be made as with any file a staff member may download. For example, you have recently been experiencing performance issues on one of your servers. After troubleshooting for much of the morning, the vendor has asked to install a utility that will collect more data from the server. The file is stored on the vendor’s FTP server. The support technician gives you the FTP site so you can anonymously download the utility file. You also ask him for a hash of the utility file. As you download the file to your local computer, you realize it is compressed. You unzip the file and perform a manual antivirus scan, using [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide) which reports no issues. To verify the utility file has not been altered, you run an application to see that the hash from the vendor matches.

**Customer Responsibility**

* Responsible for checking media containing maintenance diagnostic and test programs for malicious code prior to deployment on customer-deployed operating systems.

**Additional Resources**

* [Pre-scan files to be uploaded to non-compute Azure resources](https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-malware-defense#82-pre-scan-files-to-be-uploaded-to-non-compute-azure-resources)
* [Understand Microsoft Antimalware for Azure Cloud Services and Virtual Machines](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware)
* [Understand Microsoft Defender for Cloud Apps’ Threat detection for data services](https://docs.microsoft.com/en-us/azure/security-center/azure-defender)
* [Microsoft Defender for Endpoint documentation](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide)

MA.L2-3.7.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MA-4 | |
| **Practice:** Require multifactor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  **Assessment Objectives:**  [a] multifactor authentication is used to establish non-local maintenance sessions via external network connections; and  [b] non-local maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Microsoft Entra ID Multi-Factor Authentication  Intune/Intune Suite  Conditional Access | Privileged Identity Management (PIM)  Azure RBAC  Microsoft Azure Portal  Azure Bastion |

**Implementation Statement:**

**Privileged Identity Management (PIM)**

PIM provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Some features provide the ability to terminate sessions, such as Just-in-Time access. Here are some of the key features of Privileged Identity Management:

* Provide **just-in-time** privileged access to Microsoft Entra ID and Azure resources
* Assign **time-bound** access to resources using start and end dates
* Require **approval** to activate privileged roles
* Enforce **multi-factor authentication** to activate any role
* Use **justification** to understand why users activate
* Get **notifications** when privileged roles are activated
* Conduct **access reviews** to ensure users still need roles
* Download **audit history** for internal or external audit

To learn more, see [Enable and request just-in-time access for Azure Managed Applications](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access).

**Microsoft Entra ID Multi-Factor Authentication.**

[Multi Factor Authentication (MFA)](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks) helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Microsoft Entra ID Multi-Factor Authentication is deployed by enforcing policies with [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa). A Conditional Access policy can require users to perform multi-factor authentication when certain criteria are met such as:

* All users, a specific user, member of a group, or assigned role
* Specific cloud application being accessed
* Device platform
* State of device
* Network location or geo-located IP address
* Client applications
* Sign-in risk (Requires Identity Protection)
* Compliant device
* Hybrid Microsoft Entra ID joined device
* Approved client application

Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. To learn more, see [Planning a cloud-based Microsoft Entra ID Multi-Factor Authentication deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted).

**Intune/Intune Suite**

You can use Intune Microsoft Endpoint Manager to created conditional access policies that will restrict sessions to meeting specific requirements such as Microsoft Entra ID Multi-Factor Authentication and network locations. Sessions that do not meet the conditional access policy requirements will not be granted. To learn more, see [Learn about conditional access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access).

**Customer Responsibility**

* Responsible for using strong authenticators when establishing non-local maintenance and diagnostic sessions on customer-deployed operating systems.
* Responsible for terminating session and network connections when non-local maintenance is completed on customer-deployed operating systems.

**Additional Resources:**

* [Azure Bastion session monitoring and management](https://learn.microsoft.com/en-us/azure/bastion/session-monitoring)

MA.L2-3.7.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MA-5 | |
| **Practice:** Supervise the maintenance activities of personnel without required access authorization.  **Assessment Objective:**  [a] maintenance personnel without required access authorization are supervised during maintenance activities. | |
| **Primary Services** | **Secondary Services** |
| Azure Bastion  Privileged Identity Management (PIM) | CustomerLockbox |

**Implementation Statement:**

**Privileged Identity Management (PIM)**

You can supervise maintenance personnel with Microsoft Entra ID Privileged Identity Management. This feature provides tight control over administrative rights including conditional access, eligibility windows, global admin approvals, admin time windows and logging. To learn more, see [Deploy Privileged Identity Management (PIM)](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan).

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Customer Lockbox**

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, [Customer Lockbox](https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview) for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. To learn more, see [Supported services and scenarios](https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview#supported-services-and-scenarios).

**Azure Bastion**

Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP and SSH access to your virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in your Virtual Network (VNet) and supports all VMs in your Virtual Network (VNet) using SSL without any exposure through public IP addresses.

Once the Bastion service is provisioned and deployed in your virtual network, you can use it to seamlessly connect to any VM in this virtual network. As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you s[elect an ongoing session and force-disconnect or delete a session](https://docs.microsoft.com/en-us/azure/bastion/session-monitoring#view) in order to disconnect the user from the ongoing session.

To learn more, see [Azure Security baseline for Azure Bastion](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/bastion-security-baseline).

**Customer Responsibility**

* Managing maintenance personnel and designating organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

### Media Protection (MP)

MP.L2-3.8.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-2, MP-4, MP-6 | |
| **Practice:** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  **Assessment Objectives:**  [a] paper media containing CUI is physically controlled;  [b] digital media containing CUI is physically controlled;  [c] paper media containing CUI is securely stored; and  [d] digital media containing CUI is securely stored. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Purview Intune/Intune Suite | Microsoft Entra ID Multi-Factor Authentication  Microsoft Defender for Endpoint  Microsoft 365 Defender  Azure Virtual Machines  Windows 365 Cloud PC  Conditional Access  Azure Key Vault  Azure RBAC  Bitlocker |

**Implementation Statement:**

[Microsoft physically secures](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security) its datacenters and all the computing and storage media it is comprised of. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data.

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Utilizing Microsoft services, access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountabilities for all stored media.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Windows 365 Cloud PC**

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine (Cloud PCs) for your end users. Each Cloud PC is assigned to an individual user and is their dedicated Windows device. Windows 365 provides the productivity, security, and collaboration benefits of Microsoft 365.

To learn more, see:

* [Find the Right Windows 365 Cloud PC](https://www.microsoft.com/en-us/windows-365/cloud-pc-chooser)
* [Compare Plans and Pricing](https://www.microsoft.com/en-us/windows-365/business/compare-plans-pricing)
* [What is Windows 365 Enterprise?](https://learn.microsoft.com/en-us/windows-365/enterprise/overview?source=recommendations)
* [Manage Windows 365 Cloud PCs with Configuration Manager](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-cloud-pcs-using-configuration-manager)
* [Security overview for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/security-guidelines)

**Intune/Intune Suite**

Intune helps protect devices and your corporate data with tools like security baselines, Microsoft Entra ID conditional access, and partners for Mobile Threat Defense. Use Conditional Access with Microsoft Intune to control the devices and apps that can connect to your email and company resources. When integrated, you can gate access to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location. [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) is a Microsoft Entra ID capability that is included with an Microsoft Entra ID Premium license. Through Microsoft Entra ID , Conditional Access brings signals together to make decisions, and enforce organizational policies. Intune enhances this capability by adding mobile device compliance and mobile app management data to the solution.

**Bitlocker**

Additionally, you can use Intune to configure BitLocker Drive Encryption on devices that run Windows 10 or newer. To manage BitLocker in Intune, your account must have the applicable Intune [role-based access control](https://docs.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control) (RBAC) permissions. Intune provides a built-in [encryption report](https://docs.microsoft.com/en-us/mem/intune/protect/encryption-monitor) that presents details about the encryption status of devices, across all your managed devices. After Intune encrypts a Windows 10 device with BitLocker, you can view and manage BitLocker recovery keys when you view the encryption report. You can also access important information for BitLocker from your devices, as found in Microsoft Entra ID [encryption report](https://docs.microsoft.com/en-us/mem/intune/protect/encryption-monitor) that presents details about the encryption status of devices, across all your managed devices.

In addition to deploying BitLocker fixed drive encryption with Intune, you can configure removable drive encryption settings. You can find settings for BitLocker in Microsoft Endpoint Manager security profiles and configuration profiles. Removable drive settings apply to storage devices such as USB flash storage devices and external hard drives. For most situations, this is ideal from a security posture perspective to protect data on removable drives. However, when creating general profile settings, it is important to take into consideration the requirements of the organizations work environments. For Example, if the IT department routinely deploys operating systems using USB boot devices, those USB devices should not be encrypted. Consider requiring USB device encryption for specific departments that have access to CUI and other sensitive data. Additionally, you can block certain kinds of USB devices, or you can allow USB devices by device IDs.

For more information on how to create profiles, see:

* [Create an endpoint security policy for BitLocker](https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#create-and-deploy-policy)
* [Restrict USB devices by using Intune Administrative Templates](https://docs.microsoft.com/en-us/troubleshoot/mem/intune/restrict-usb-with-administrative-template)

**Azure Key Vault**

Protecting sensitive media and logical data in transit is another critical control to ensure confidentiality of data. Azure provides numerous levels of encryption for data in transit. Azure Key Vault provides a capability to securely store your application keys, certificates, and secrets. This capability reduces risk of key exposure while providing role-based access control (RBAC) for key usage and audit logging of key usage. [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts) is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This [article](https://docs.microsoft.com/en-us/azure/key-vault/general/security-features) provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.

**Microsoft Entra ID Multi-Factor Authentication**

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Microsoft Entra ID Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. To learn more, see [Planning a cloud-based Microsoft Entra ID Multi-Factor Authentication deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted).

**Customer Responsibility**

* Physically control paper media containing CUI
* Physically control digital media such as, diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. containing CUI
* Securely store paper media and digital media containing CUI

**Additional Resources**

* [Azure RBAC documentation](https://docs.microsoft.com/en-us/azure/role-based-access-control/#:~:text=Azure%20role%2Dbased%20access%20control%20(Azure%20RBAC)%20is%20a,need%20to%20perform%20their%20jobs.)
* [Common ways to use Conditional Access with Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use)
* [Tutorial: Use a Windows VM system-assigned managed identity to access Azure Key Vault](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad)
* [Check out or check in files in a document library](https://support.microsoft.com/en-us/office/check-out-or-check-in-files-in-a-document-library-acce24cd-ab39-4fcf-9c4d-1ce3050dc602)
* [Check out and edit files](https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/check-out-edit-files?view=azure-devops)
* [Manage inventory collection from VMs](https://docs.microsoft.com/en-us/azure/automation/change-tracking/manage-inventory-vms)
* [Inventory and visibility in Azure](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-management-guide/inventory?tabs=AzureServiceHealth%2CLog-Analytics%2CAzure-Monitor%2CConfigure-solutions)
* [Change Tracking and Inventory overview](https://docs.microsoft.com/en-us/azure/automation/change-tracking/overview)

MP.L2-3.8.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-2, MP-4, MP-6 | |
| **Practice:** Limit access to CUI on system media to authorized users.  **Assessment Objective:**  [a] access to CUI on system media is limited to authorized users. | |
| **Primary Services** | **Secondary Services** |
| Azure RBAC Microsoft Purview Conditional Access Intune/Intune Suite | Network Security Groups  Microsoft Entra ID Multi-Factor Authentication  Microsoft 365 Compliance Center  Microsoft Defender for Endpoint  Microsoft 365 Defender |

**Implementation Statement:**

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

[Microsoft (via Azure Government and/or Microsoft 365 GCC High) physically secures](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security) its datacenters and all the computing and storage media it is comprised of. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data.

**Microsoft Entra ID**

[Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope. This article describes how to assign roles using the Azure portal. If you need to assign administrator roles in Microsoft Entra ID , see [Assign Microsoft Entra ID roles to users](https://docs.microsoft.com/en-us/azure/active-directory/roles/manage-roles-portal).

Role-based access control (RBAC) helps you manage who has access to your organization's resources and what they can do with those resources. By [assigning roles](https://docs.microsoft.com/en-us/mem/intune/fundamentals/assign-role) to your Intune users, you can limit what they can see and change. Each role has a set of permissions that determine what users with that role can access and change within your organization.

**Intune/Intune Suite and Conditional Access**

Use Conditional Access with Microsoft Intune to control the devices and apps that can connect to your email and company resources. When integrated, you can gate access to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location.

[Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) is an Microsoft Entra ID capability that is included with an Microsoft Entra ID Premium license. Through Microsoft Entra ID , Conditional Access brings signals together to make decisions, and enforce organizational policies. Intune enhances this capability by adding mobile device compliance and mobile app management data to the solution.

Use device [compliance policy](https://docs.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune) to establish the conditions by which devices and users are allowed to access your network and company resources such as requiring a device to be marked as compliant, require multi-factor authentication, require approved client app and trusted network locations.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html).

**Microsoft 365 Compliance Center**

When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

* Only users within your organization can open a confidential document or email.
* Only users in the marketing department can edit and print the promotion announcement document or email, while all other users in your organization can only read it.
* Users cannot forward an email or copy information from it that contains news about an internal reorganization.

The encryption settings are available when you create a sensitivity label in the Microsoft 365 compliance center. You can also use the older portal, the Security & Compliance Center.

**MFA**

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Microsoft Entra ID Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. To learn more, see [Planning a cloud-based Microsoft Entra ID Multi-Factor Authentication deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)

**Network Security Group**

You can use an Azure Network Security Group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. To learn more, see [Azure platform considerations.](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#azure-platform-considerations)

**Customer Responsibility**

* Identifying CUI to ensure the controls are applied to the applicable data.
* Limiting access to CUI on system media to authorized users only.

**Additional Resources**

* [Common ways to use Conditional Access with Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use)
* [Virtual network integration for Azure services](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services)
* [How network security groups work](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works).
* [Manage a network security group](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group)

MP.L1-3.8.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-2, MP-4, MP-6 | |
| **Practice:** Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.  **Assessment Objectives:**  [a] system media containing FCI is sanitized or destroyed before disposal; and  [b] system media containing FCI is sanitized before it is released for reuse. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Purview |

**Implementation Statement:**

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

**Microsoft**

When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination. If a disk drive used for storage suffers a hardware failure, it is securely [erased or destroyed](https://www.microsoft.com/trustcenter/privacy/data-management) before decommissioning. The data on the drive is erased to ensure that the data cannot be recovered by any means. When such devices are decommissioned, Microsoft follows the [NIST SP 800-88 R1](https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final) disposal process with data classification aligned to FIPS 199 Moderate. Magnetic, electronic, or optical media are purged or destroyed in accordance with the requirements established in NIST SP 800-88 R1. Purge and Destroy operations must be performed using tools and processes approved by the Microsoft Cloud + AI Security Group. Records must be kept of the erasure and destruction of assets. Devices that fail to complete the Purge successfully must be degaussed (for magnetic media only) or destroyed.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html).

**Customer Responsibility**

* Sanitizing and destroying customer-controlled information system media containing Federal Contract Information (FCI) before disposal or release for reuse.

MP.L2-3.8.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-3 | |
| **Practice:** Mark media with necessary CUI markings and distribution limitations.  **Assessment Objectives:**  [a] media containing CUI is marked with applicable CUI markings; and  [b] media containing CUI is marked with distribution limitations. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Purview |  |

**Implementation Statement:**

The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. Labeling sensitive data is something organizations should implement across both physical and logical media. Government regulations such as [NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)](https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-nist-sp-800-171?view=o365-worldwide) implicitly specify controls for protecting controlled unclassified information (CUI). This requirement spans across all industries and geographies. The European Union requires secure handing of personally identifiable information (PII) in the [General Data Protection Regulation (GDPR)](https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview) and California has recently implemented a similar regulation with the [California Consumer Privacy Regulation (CCPA)](https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-ccpa?view=o365-worldwide).

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html).

**Customer Responsibility**

* Marking CUI with applicable marking. (e.g., CUI/SP-XX/NOFORN in subject of email, etc. in addition to applying correct MIP label.)
* Limiting distribution to media containing CUI.

**Additional Resources**

* [Azure RBAC documentation](https://docs.microsoft.com/en-us/azure/role-based-access-control/#:~:text=Azure%20role%2Dbased%20access%20control%20(Azure%20RBAC)%20is%20a,need%20to%20perform%20their%20jobs.)
* [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview)
* [CUI Markings | National Archives](https://www.archives.gov/cui/registry/category-marking-list)

MP.L2-3.8.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-5 | |
| **Practice:** Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.  **Assessment Objectives:**  [a] access to media containing CUI is controlled; and  [b] accountability for media containing CUI is maintained during transport outside of controlled areas. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Purview  Microsoft Entra ID Multi-Factor Authentication  Microsoft Defender for Endpoint  Microsoft 365 Defender  Azure Key Vault Intune/Intune Suite  Azure RBAC  Bitlocker |

**Implementation Statement:**

Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

[Microsoft physically secures](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security) its datacenters and all the computing and storage media it is comprised of. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain your data.

Most operations, support, and troubleshooting performed by Microsoft personnel and sub-processors do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. You can now enable Customer Lockbox from the [Administration module](https://aka.ms/customerlockbox/administration) in the Customer Lockbox blade. To enable Customer Lockbox, the user account needs to have the [Global Administrator role assigned](https://docs.microsoft.com/en-us/azure/active-directory/roles/manage-roles-portal).

**Intune/Intune Suite**

Microsoft's primary MDM tool is [Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/). Intune is part of a larger Microsoft MDM platform called [Microsoft Endpoint Manager](https://docs.microsoft.com/en-us/mem/intune/).

Using Intune, administrators can enroll, configure, and manage mobile devices on several different operating system platforms, wherever the devices happen to be. Administrators can even intervene when a threat to security occurs, by blocking a device’s access to the company network and erasing any sensitive information stored on it.

Organizations can configure policies to allow, block and restrict USB drives and other peripherals. Organization can allow users to install only the USB drives and other peripherals included on a list of authorized devices or device types or prevent users from installing USB drives and other peripherals included on a list of unauthorized devices and device types.

Additionally, using Intune, you can apply device configuration policies to Microsoft Entra ID user and/or device groups. The policies can also be set through the [Device Installation CSP settings](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceinstallation) and the [Device Installation GPOs](https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530324(v=msdn.10)). To protect your devices and corporate resources, you can use Microsoft Entra ID Conditional Access policies with Intune.

Intune passes the results of your device compliance policies to Microsoft Entra ID , which then uses conditional access policies to enforce which devices and apps can access your corporate resources.

When managing devices in your organization, you want to create groups of settings that apply to different device groups. You can complete this task using [Administrative Templates](https://docs.microsoft.com/en-us/troubleshoot/mem/intune/restrict-usb-with-administrative-template) in Intune. The templates are built into Intune and do not require customization.

**Bitlocker**

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

BitLocker To Go is BitLocker Drive Encryption on removable data drives. As with BitLocker, you can open drives that are encrypted by BitLocker To Go by using a password or smart card on another computer.

**Microsoft Defender for Endpoint**

Microsoft recommends [a layered approach to securing removable media](https://aka.ms/devicecontrolblog), and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices. [Discover plug and play connected events for peripherals in Microsoft Defender for Endpoint advanced hunting](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#discover-plug-and-play-connected-events). To prevent malware infections or data loss, an organization may restrict USB drives and other peripherals. [Allow or block removable devices](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#allow-or-block-removable-devices) based on granular configuration to deny write access to removable disks and approve or deny devices by using USB device IDs. Flexible policy assignment of device installation settings based on an individual or group of Microsoft Entra ID users and devices. The controls can be set through the Intune [Administrative Templates](https://docs.microsoft.com/en-us/intune/administrative-templates-windows). Using Intune, you can apply device configuration policies to Microsoft Entra ID user and/or device groups. The above policies can also be set through the [Device Installation CSP settings](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceinstallation) and the [Device Installation GPOs](https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530324(v=msdn.10)).

**Azure RBAC**

Limiting access to sensitive data with least privilege reduces the risk of spillage or unauthorized access. [Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html).

**Azure Key Vault**

Azure Key Vault provides a capability to securely store your application keys, certificates and secrets. This capability reduces risk of key exposure while providing role-based access control (RBAC) for key usage and audit logging of key usage. [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts) is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This [article](https://docs.microsoft.com/en-us/azure/key-vault/general/security-features) provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.

**Microsoft Entra ID Multi-Factor Authentication**

MFA helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. Microsoft Entra ID Multi-Factor Authentication is deployed by enforcing policies with Conditional Access. Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. To learn more, see [Planning a cloud-based Microsoft Entra ID Multi-Factor Authentication deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted).

**Customer Responsibility**

* Controlling access to customer-controlled media containing CUI and maintain accountability for media during transport outside of controlled areas.

**Additional Resources**

* [Azure security baseline for Customer Lockbox for Microsoft Azure](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/lockbox-security-baseline)
* [Understand Customer Lockbox workflow](https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview)
* [How to enable auditing in Customer Lockbox](https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview)
* [How to view and retrieve Azure Activity Log events](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log#view-the-activity-log)
* [Managing BitLocker with Microsoft Endpoint Manager](https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/managing-bitlocker-with-microsoft-endpoint-manager/ba-p/1582523)
* [BitLocker overview](https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview)

MP.L2-3.8.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-28(1) | |
| **Practice:** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.  **Assessment Objective:**  [a] the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards. | |
| **Primary Services** | **Secondary Services** |
| Bitlocker  Azure RBAC | Microsoft Defender for Endpoint Intune/Intune Suite  Microsoft Purview  Microsoft 365 Defender  Azure Key Vault  Conditional Access |

**Implementation Statement:**

Whenever Azure Customer traffic moves between datacenters-- outside physical boundaries not controlled by Microsoft (or on behalf of Microsoft)-- a data-link layer encryption method using the [IEEE 802.1AE MAC Security Standards](https://1.ieee802.org/security/802-1ae/) (also known as MACsec) is applied from point-to-point across the underlying network hardware. The packets are encrypted and decrypted on the devices before being sent, preventing physical “man-in-the-middle” or snooping/wiretapping attacks. Because this technology is integrated on the network hardware itself, it provides line rate encryption on the network hardware with no measurable link latency increase. This MACsec encryption is on by default for all Azure traffic traveling within a region or between regions, and no action is required on customers’ part to enable.

Microsoft gives customers the ability to use [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) protocol to protect data when it is traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

[Perfect Forward Secrecy](https://en.wikipedia.org/wiki/Forward_secrecy) (PFS) protects connections between customers’ client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

**BitLocker**

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

BitLocker To Go is BitLocker Drive Encryption on removable data drives. As with BitLocker, you can open drives that are encrypted by BitLocker To Go by using a password or smart card on another computer.

**Azure Key Vault**

Azure Key Vault provides two types of resources to store and manage cryptographic keys. Vaults support software-protected and HSM-protected (Hardware Security Module) keys. Managed HSMs only support HSM-protected keys. Vaults use FIPS 140-2 Level 2 validated HSMs to protect HSM-keys in shared HSM backend infrastructure. Managed HSM uses FIPS 140-2 Level 3 validated HSM modules to protect your keys. Each HSM pool is an isolated single-tenant instance with its own security domain providing complete cryptographic isolation from all other HSMs sharing the same hardware infrastructure.

Azure Key Vault provides a capability to securely store your application keys, certificates and secrets. This capability reduces risk of key exposure while providing role-based access control (RBAC) for key usage and audit logging of key usage. [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts) is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This [article](https://docs.microsoft.com/en-us/azure/key-vault/general/security-features) provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.

**Intune/Intune Suite**

[App protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy) (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any [device](https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform), including personal devices in bring-your-own-device (BYOD) scenarios. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of [Microsoft Intune protected apps](https://docs.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps) available for public use.

Use Conditional Access with Microsoft Intune to control the devices and apps that can connect to your email and company resources. When integrated, you can gate access to keep your corporate data secure, while giving users an experience that allows them to do their best work from any device, and from any location.

[Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) is a Microsoft Entra ID capability that is included with an Microsoft Entra ID Premium license. Through Microsoft Entra ID , Conditional Access brings signals together to make decisions, and enforce organizational policies. Intune enhances this capability by adding mobile device compliance and mobile app management data to the solution.

Use device [compliance policy](https://docs.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune) to establish the conditions by which devices and users are allowed to access your network and company resources such as requiring a device to be marked as compliant, require multi-factor authentication, require encryption, require approved client app and trusted network locations.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html).

**Additional Resources**

* [Data protection framework using app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-framework)
* [Available Android app protection policy settings with Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android)
* [Available iOS/iPadOS app protection policy settings with Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios)
* [Azure encryption overview](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview)
* [About Managed HSM](https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview)
* [About Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/overview)
* [Key types and protection methods](https://docs.microsoft.com/en-us/azure/key-vault/keys/about-keys#key-types-and-protection-methods)

MP.L2-3.8.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-7 | |
| **Practice:** Control the use of removable media on system components.  **Assessment Objective:**  [a] the use of removable media on system components is controlled. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite  Microsoft Defender for Endpoint  Microsoft 365 Defender |  |

**Implementation Statement:**

Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices.

**Microsoft Defender for Endpoint/Microsoft 365 Defender**

Microsoft recommends [a layered approach to securing removable media](https://aka.ms/devicecontrolblog), and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices. [Discover plug and play connected events for peripherals in Microsoft Defender for Endpoint advanced hunting](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#discover-plug-and-play-connected-events). To prevent malware infections or data loss, an organization may restrict USB drives and other peripherals. [Allow or block removable devices](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#allow-or-block-removable-devices) based on granular configuration to deny write access to removable disks and approve or deny devices by using USB device IDs.

Device control in Defender for Endpoint empowers security administrators with tools that enable them to track their organization's device control security through reports. You can find the device control report in the Microsoft 365 Defender portal ([https://security.microsoft.com](https://security.microsoft.com/)). Go to **Reports** > **General** > **Security report**. Find **Device control** card and select the link to open the report.

**Intune/Intune Suite**

Flexible policy assignment of device installation settings based on an individual or group of Microsoft Entra ID users and devices. The controls can be set through the Intune [Administrative Templates](https://docs.microsoft.com/en-us/intune/administrative-templates-windows). Using Intune, you can apply device configuration policies to Microsoft Entra ID user and/or device groups. The above policies can also be set through the [Device Installation CSP settings](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceinstallation) and the [Device Installation GPOs](https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530324(v=msdn.10)).

**Customer Responsibility**

* Controlling the use of removable media on customer-controlled systems.

Additional Resources:

* [Deploy and manage Removable Storage Access Control using Intune](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/deploy-manage-removable-storage-intune?source=recommendations&view=o365-worldwide)
* [Microsoft Defender for Endpoint Device Control Removable Storage Protection](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-removable-storage-protection?view=o365-worldwide)

MP.L2-3.8.8

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** MP-7(1) | |
| **Practice:** Prohibit the use of portable storage devices when such devices have no identifiable owner.  **Assessment Objective:**  [a] the use of portable storage devices is prohibited when such devices have no identifiable owner. | |
| **Primary Services** | **Secondary Services** |
| Intune/Intune Suite  Microsoft Defender for Endpoint  Microsoft 365 Defender | Conditional Access |

**Implementation Statement:**

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

**Microsoft Defender for Endpoint/Microsoft 365 Defender**

Microsoft recommends [a layered approach to securing removable media](https://aka.ms/devicecontrolblog), and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices. [Discover plug and play connected events for peripherals in Microsoft Defender for Endpoint advanced hunting](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#discover-plug-and-play-connected-events). To prevent malware infections or data loss, an organization may restrict USB drives and other peripherals. [Allow or block removable devices](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/control-usb-devices-using-intune?view=o365-worldwide#allow-or-block-removable-devices) based on granular configuration to deny write access to removable disks and approve or deny devices by using USB device IDs.

Device control in Defender for Endpoint empowers security administrators with tools that enable them to track their organization's device control security through reports. You can find the device control report in the Microsoft 365 Defender portal ([https://security.microsoft.com](https://security.microsoft.com/)). Go to **Reports** > **General** > **Security report**. Find **Device control** card and select the link to open the report.

**Intune/Intune Suite**

Flexible policy assignment of device installation settings based on an individual or group of Microsoft Entra ID users and devices. The controls can be set through the Intune [Administrative Templates](https://docs.microsoft.com/en-us/intune/administrative-templates-windows). Using Intune, you can apply device configuration policies to Microsoft Entra ID user and/or device groups. The above policies can also be set through the [Device Installation CSP settings](https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceinstallation) and the [Device Installation GPOs](https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb530324(v=msdn.10)).

**Customer Responsibility**

* Prohibiting the use of portable storage devices that have no identifiable owner, on customer-controlled systems.

MP.L2-3.8.9

| **Control Summary Information** | |
| --- | --- |
| **NIST 800-171 Mapping:** 3.8.9 | |
| **NIST SP 800-53 Mapping:** CP-9 | |
| **Practice:** Protect the confidentiality of backup CUI at storage locations.  **Assessment Objective:**  [a] the confidentiality of backup CUI is protected at storage locations. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC | Azure Key Vault  Azure Storage  Azure Virtual Network  Microsoft Purview  Microsoft Entra ID Multi-Factor Authentication |

**Implementation Statement:**

**Microsoft Entra ID /Azure RBAC**

There are several methods to protecting backups including access management, redundancy, and encryption. Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Azure Backup provides three built-in roles to control backup management operations. To learn more, see [Use Role-Based Access Control to manage Azure Backup recovery points](https://docs.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault).

**Microsoft Entra ID Multi-Factor Authentication**

Secure your backups and protect against ransomware by enabling [multifactor authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks) using a security PIN generated in the Azure portal. If it is enabled, you are asked to authenticate from another device (for example, a mobile phone) while signing into the Azure portal. When you perform critical operations in Backup, you have to enter a security PIN, available on the Azure portal. Enabling Microsoft Entra ID Multi-Factor Authentication adds a layer of security. Only authorized users with valid Azure credentials, and authenticated from a second device, can access the Azure portal.

Fully control how you protect and access your data with [customer-managed keys](https://docs.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk) that use 256-bit AES encryption. You can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.

**Azure Storage**

Azure Create [private endpoints](https://docs.microsoft.com/en-us/azure/backup/private-endpoints) within your Azure Virtual Network to securely backup and restore data from your Recovery Services vaults. Azure Backup allows you to securely backup and restore your data from your Recovery Services vaults using [private endpoints](https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview). Private endpoints use one or more private IP addresses from your VNet, effectively bringing the service into your VNet. Private endpoints for Backup can only be created for Recovery Services vaults that do not have any items protected to it (or have not had any items attempted to be protected or registered to it in the past). So, we suggest you create a new vault to start with. For more information about creating a new vault, see [Create and Configure a Recovery Services Vault](https://docs.microsoft.com/en-us/azure/backup/backup-create-rs-vault).

All your backed-up data is automatically encrypted when stored in the cloud using Azure Storage encryption, which helps you meet your security and compliance commitments. This data at rest is encrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 Validated. In addition to encryption at rest, all your backup data in transit is transferred over HTTPS. It always remains on the Azure backbone network.

To learn more, see [Azure Storage encryption for data at rest](https://docs.microsoft.com/azure/storage/common/storage-service-encryption).

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html).

**Customer Responsibility**

* Responsible for conducting backups of user-level information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.
* Responsible for conducting backups of system-level information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.
* Responsible for conducting backups of system documentation information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.
* Responsible for protecting the confidentiality, integrity, and availability (CIA) of customer-controlled backup data. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the protection of backup data.

**Additional Resources**

* [Azure Backup security capabilities for protecting cloud backups](https://azure.microsoft.com/en-us/blog/azure-backup-security-feature/)

### Personnel Security (PS)

PS.L2-3.9.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** PS-3, PS-4, PS-5 | |
| **Practice:** Screen individuals prior to authorizing access to organizational systems containing CUI.  **Assessment Objective:**  [a] individuals are screened prior to authorizing access to organizational systems  containing CUI. | |
| **Primary Services** | **Secondary Services** |
|  |  |

**Implementation Statement:**

Personnel security screening (vetting) activities involve the evaluation/assessment of individual’s conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

You can ensure all employees who need access to CUI undergo organization-defined screening before being granted access based on the types of screening requirements for a given position and role. Clearly define positions and roles within your organization. Implement roles [using Azure RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/#:~:text=Azure%20role%2Dbased%20access%20control%20(Azure%20RBAC)%20is%20a,need%20to%20perform%20their%20jobs.). For example, administrators with access to CUI and specific roles with permissions to view CUI should follow an organizationally defined screening process.

**Azure**

**Customer Responsibility**

* Screening individuals prior to authorizing access to customer-deployed resources.

**GCCH**

**Customer Responsibility**

* Government customers are responsible for determining screening requirements and implementing those requirements for their own personnel before they grant them access to the system.

PS.L2-3.9.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** PS-3, PS-4, PS-5 | |
| **Practice:** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.  **Assessment Objectives:**  [a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established;  [b] system access and credentials are terminated consistent with personnel actions such as termination or transfer; and  [c] the system is protected during and after personnel transfer actions. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC | Microsoft Purview  Conditional Access  Microsoft Defender for Endpoint Intune/Intune Suite  Microsoft Defender for Cloud Apps |

**Implementation Statement:**

Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

**Microsoft Entra ID**

To protect organizational system containing CUI it is important to have controls in place that can identify users and remove access when needed. [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  is the cornerstone of identity in Azure. MICROSOFT ENTRA ID enables hybrid identities through [Microsoft Entra ID Connect](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect), an on-premises solution that is used to synchronize Active Directory identities with Microsoft Entra ID, as well as to [deploy Active Directory Federation Services (ADFS).](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs) ADFS lets you establish a federation between your premises and Microsoft Entra ID (among others). When users log in, they are redirected to the ADFS login page (in your perimeter) and are prompted for their credentials, which are validated against your on-premises Active Directory. This makes your ADFS a single point of failure, because in such a setup, user passwords are not synchronized with Microsoft Entra ID. Thus, credential validation can only be performed against your on-premises directory.

[Microsoft Entra ID Pass-through Authentication](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta)is an alternative that consists of validating user credentials on-premises. It also validates credentials online, should your on-premises login page not be available. From a pure authentication perspective, it is a more robust approach than ADFS, but it requires user passwords to be synchronized with Microsoft Entra ID, which is often still considered unwise by many organizations. You can also go full cloud and only use Microsoft Entra ID.

[Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) allows you to set up access policies to prohibit a specific activity, as well as to trigger MFA according to rules that you define). It is a very powerful engine. You may target conditional access policies toward specific users or groups, or to specific apps.

[RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/#:~:text=Azure%20role%2Dbased%20access%20control%20(Azure%20RBAC)%20is%20a,need%20to%20perform%20their%20jobs.) helps in the creation and assignment of different permissions to different identities. It is good practice to assign permissions using the principle of least privilege; this involves giving users the exact permissions they need to do their jobs properly. Users, groups, and applications are added to roles in Azure, and those roles have certain permissions. You can use the built-in roles that Azure offers, or you can create custom roles in RBAC.

To learn more, see [Grant a user access to Azure resources using RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/quickstart-assign-role-user-portal).

Scenarios that could require an administrator to revoke all access for a user include compromised accounts, employee termination, and other insider threats. Depending on the complexity of the environment, administrators can take several steps to ensure access is revoked. Access tokens and refresh tokens are frequently used with thick client applications, and also used in browser-based applications such as single page apps. When users authenticate to Microsoft Entra ID , authorization policies are evaluated to determine if the user can be granted access to a specific resource. Access tokens can be a security concern if access must be revoked within a time that is shorter than the lifetime of the token, which is usually around an hour. For this reason, Microsoft is actively working to bring [continuous access evaluation](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation) to Office 365 applications, which helps ensure invalidation of access tokens in near real time. To remove a user or group assignment to an application, follow the steps listed in the [Remove a user or group assignment from an enterprise app in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal)  article. To disable all user sign-ins to an application, follow the steps listed in the [Disable user sign-ins for an enterprise app in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/disable-user-sign-in-portal)  article.

[Microsoft Entra ID Identity Protection](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection) introduces automatic, risk-based, conditional access to help protect users against suspicious logins and compromised credentials. Microsoft Entra ID Identity Protections also offers insight into, and a consolidated view of, threat detection based on machine-learning. Furthermore, the service delivers an important level of remediation recommendations, as well as performing compromise risk calculations about a user and their session.

To learn more, see:

* [What is Identity Protection?](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection)
* [Identity Protection policies](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies)

**Microsoft Intune**

A cloud-based enterprise mobility management (EMM) service that enables administrators to enroll mobile devices, deploy apps, and enforce security policies As a Security Admin, use the *Endpoint security* node in Intune to configure device security and to manage security tasks for devices when those devices are at risk.

To protect your devices and corporate resources, you can use [Microsoft Entra ID Conditional Access policies with Intune.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions)

Intune passes the results of your device compliance policies to Microsoft Entra ID, which then uses conditional access policies to enforce which devices and apps can access your corporate resources. Conditional access policies also help to gate access for devices that aren’t managed by Intune and can use compliance details from [Mobile Threat Defense partners](https://docs.microsoft.com/en-us/mem/intune/protect/mobile-threat-defense) you integrate with Intune.

**Azure**

**Customer Responsibility**

* Appropriately terminating customer personnel within a customer-defined time period.
* Appropriately transferring personnel and reviewing current logical and physical access authorizations to customer-deployed resources/facilities when individuals are reassigned or transferred.

**GCCH**

**Customer Responsibility:**

* Office 365 government customers are responsible for managing information system access terminations for their organizational users consistent with their internal policies and procedures.  
    
  Government customers using ADFS, manage user accounts in their own customer-owned and controlled Active Directory (AD) forests. These customers may disable or delete terminated users in their internal AD infrastructure. When customers disable or delete users in their AD forests, access to Office 365 is immediately revoked for the disabled or terminated user.
* Government customers are responsible for reviewing logical access authorizations to Office 365 for their own personnel prior to reassigning or transferring to another position within their organization and granting access to Office 365.

**Additional Resources**

* [Manage user assignment for an app in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal)

### Physical Protection (PE)

PE.L2-3.10.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** PE-17 | |
| **Practice:** Enforce safeguarding measures for CUI at alternate work sites.  **Assessment Objectives:**  [a] safeguarding measures for CUI are defined for alternate work sites; and  [b] safeguarding measures for CUI are enforced for alternate work sites. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID Multi-Factor Authentication  Intune/Intune Suite  Microsoft 365 Defender  Microsoft Defender for Endpoint  Azure RBAC  Azure VPN  Azure Firewall  Bitlocker | Named Locations Microsoft Purview Conditional Access  Microsoft 365 DLP  Privileged Identity Management (PIM)  Azure Bastion  Windows 365 Cloud PC  Azure Virtual Machines |

**Implementation Statement:**

Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. Many people work from home or travel as part of their job. Define and implement safeguards to account for protection of information beyond the enterprise perimeter. Safeguards may include physical protections, such as locked file drawers, as well as electronic protections such as encryption, audit logging, and proper access controls.

**Intune/Intune Suite**

Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud-based mobile application management (MAM), and cloud-based PC management for your organization. Intune helps you ensure that your company's devices, apps, and data meet your company's security requirements. You have the control to set which requirements need to be checked and what happens when those requirements aren't met. The [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431) is where you can find the Microsoft Intune service, as well as other device management related settings.

[Microsoft Intune device compliance policies](https://docs.microsoft.com/en-us/intune/deploy-use/introduction-to-device-compliance-policies-in-microsoft-intune) - Cloud-based device compliance leverages Microsoft Intune Compliance Policies, which can query the device state and define compliance rules for the following, among other things.

* Antivirus status
* Auto-update status and update compliance
* Password policy compliance
* Encryption compliance
* Device health attestation state (validated against attestation service after query)

**Microsoft Entra ID**

Microsoft Entra ID provides administrators the flexibility to apply granular user authentication per their requirements. As an administrator, choosing authentication methods for Microsoft Entra ID Multi-Factor Authentication and self-service password reset (SSPR) it is recommended that you require users to register multiple authentication methods. When an authentication method is not available for a user, they can choose to authenticate with another method. Authentication methods include password, security questions, email address, Microsoft Authenticator app, OATH Hardware token, SMS, Voice call, and App passwords. To learn more, see [Authentication methods](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods).

Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope. To learn more, see [Grant a user access to Azure resources using RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/quickstart-assign-role-user-portal).

**Privileged Identity Management**

You can secure administrative rights with Microsoft Entra ID Privileged Identity Management. This feature provides tight control over administrative rights including conditional access, eligibility windows, global admin approvals, admin time windows and logging. To learn more, see [Deploy Privileged Identity Management (PIM)](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan).

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Windows 365 Cloud PC**

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine (Cloud PCs) for your end users. Each Cloud PC is assigned to an individual user and is their dedicated Windows device. Windows 365 provides the productivity, security, and collaboration benefits of Microsoft 365.

To learn more, see:

* [Find the Right Windows 365 Cloud PC](https://www.microsoft.com/en-us/windows-365/cloud-pc-chooser)
* [Compare Plans and Pricing](https://www.microsoft.com/en-us/windows-365/business/compare-plans-pricing)
* [What is Windows 365 Enterprise?](https://learn.microsoft.com/en-us/windows-365/enterprise/overview?source=recommendations)
* [Manage Windows 365 Cloud PCs with Configuration Manager](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-cloud-pcs-using-configuration-manager)
* [Security overview for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/security-guidelines)

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Conditional Access**

Microsoft Azure leverages adaptive access control through Microsoft Entra ID conditional access. The modern security perimeter now extends beyond an organization’s network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions. Conditional access policies incorporate Microsoft Entra ID Identity Protection risk detections and include three default policies:

* Require all users to register for Microsoft Entra ID Multi-Factor Authentication.
* Require a password change for users that are high risk.
* Require multi-factor authentication for users with medium or high sign-in risk.

Conditional Access is the tool used by Microsoft Entra ID to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane. Conditional access policies are highly configurable and include several capabilities:

* Require MFA for admins
* End user protection
* Block legacy authentication
* Require MFA for Service Management
* Block access by location
* Require trusted location for MFA registration
* Require compliant devices

To learn more, see [What is Conditional Access?](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview)

Additionally**,** The VPN client is now able to integrate with the cloud-based Conditional Access Platform to provide a device compliance option for remote clients. Conditional Access is a policy-based evaluation engine that lets you create access rules for any Microsoft Entra ID connected application. To learn more, see [Configure Conditional Access.](https://docs.microsoft.com/en-us/windows/security/identity-protection/vpn/vpn-conditional-access#configure-conditional-access)

**Azure Firewall**

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It’s a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. You can manage connections and block access to external resources by creating an Azure Firewall and configuring respective policies. To learn more, see [Deploy and configure Azure Firewall](https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal).

**Microsoft 365 DLP**

Microsoft 365 DLP policies are how you monitor the activities that users take on sensitive items at rest, sensitive items in transit, or sensitive items in use and take protective actions. For example, when a user attempts to take a prohibited action, like copying a sensitive item to an unapproved location, or sharing medical information in an email or other conditions laid out in a policy.

**Customer Responsibility**

* Safeguarding measures for CUI are defined for alternate work sites.
* Enforcing safeguarding measures for CUI for alternate work sites.

**Additional Resources**

* Dive into the [technical requirements and capabilities](https://docs.microsoft.com/en-us/intune/supported-devices-browsers) of Intune
* [See feature differences between Intune and Intune for US Government](https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/ems-intune-govt-service-description)
* [Microsoft Intune for US Government GCC High](https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/ems-intune-govt-service-description)

[Implementing a Zero Trust security model at Microsoft](https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft)

### Risk Assessment (RA)

RA.L2-3.11.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** RA-3 | |
| **Practice:** Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI.  **Assessment Objectives:**  [a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined; and  [b] risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Purview  Microsoft Defender for Cloud  Microsoft 365 Defender  Secure Score | Microsoft Sentinel  Intune/Intune Suite  Microsoft Defender for IoT Microsoft Defender for Endpoint  Insider Risk Management  Microsoft Copilot for Security |

**Implementation Statement:**

Risk arises from anything that can reduce an organization’s assurance of mission/business success; cause harm to image or reputation; or harm individuals, other organizations, or the Nation. Risk assessments should be performed at defined regular intervals (e.g., yearly). Mission risks include anything that will keep an organization from meeting its mission. Function risk is anything that will prevent the performance of a function. Image and reputation risks refer to intangible risks that have value and could cause damage to potential or future trust relationships. For example, you evaluate the new risk involved with storing CUI. When conducting the assessment you consider increased legal exposure, financial requirements of safeguarding CUI, potentially elevated attention from external attackers, and other factors. After determining how storing CUI affects your overall risk profile, you use that as a basis for a conversation on how that risk should be mitigated.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* Use [Microsoft Purview Compliance Manager](https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager) to create your own assessments that evaluate compliance with the industry and regional regulations that apply to your organization.

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Microsoft Defender for Cloud**

To help assess risk, Microsoft Defender for Cloud provides the [Secure Score](https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls) calculation to provide a readily consumable assessment of your risk posture. Security Center mimics the work of a security analyst, reviewing your security recommendations and applying advanced algorithms to determine how crucial each recommendation is. Microsoft Defender for Cloud constantly reviews your active recommendations and calculates your Secure Score based on them, the score of a recommendation is derived from its severity and security best practices that will affect your workload security the most. Security Center also provides you with an Overall Secure Score.

Overall Secure Score is an accumulation of all your recommendation scores. You can view your overall Secure Score across your subscriptions or management groups, depending on what you select. The score will vary based on subscription selected and the active recommendations on these subscriptions. To check which recommendations, impact your Secure Score most, you can view the top three most impactful recommendations in the Security Center dashboard, or you can sort the recommendations in the recommendations list blade using the Secure Score impact column. To learn more, see Improve your secure score in Microsoft Defender for Cloud .

**Sentinel**

Consider using Microsoft Sentinel as your Security Information and Event Management (SIEM) solution. After you [connect your data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks. While Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to [Create interactive reports with Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview)

Microsoft Sentinel provides hunting capabilities to align cyber defenders to threat tactics and facilitate building threat profiles. These profiles allow cyber defenders to target the phase of the attack lifecycle. Microsoft Sentinel hunting is aligned to the [MITRE ATT&CK](https://attack.mitre.org/)™ (adversarial tactics, techniques, and common knowledge) framework. These adversary tactics and techniques are grouped within a matrix. To learn more, see [Threat hunting: Part 1—Why your SOC needs a proactive hunting team](https://www.microsoft.com/security/blog/2020/03/10/threat-hunting-part-1-why-your-soc-needs-a-proactive-hunting-team/).

The [Microsoft Intelligent Security Graph](http://cloud-platform-assets.azurewebsites.net/intelligent-security-graph/) uses advanced analytics to link a massive amount of threat intelligence and security data from Microsoft and partners to combat cyberthreats. Insights from the Intelligent Security Graph power real-time threat protection in Microsoft products and services. Also, many organizations utilize threat intelligence platform (TIP) solutions to aggregate threat indicator feeds from a variety of sources. If your organization utilizes an integrated TIP solution the platforms data connector allows you leverage your TIP to import threat indicators into Microsoft Sentinel. The Threat Intelligence Platforms data connector works with the Microsoft Graph Security *Indicators* API to bring threat indicators into Azure. To learn more, see [Bring your threat intelligence to Microsoft Sentinel](https://techcommunity.microsoft.com/t5/azure-sentinel/bring-your-threat-intelligence-to-azure-sentinel/ba-p/1167546).

**Microsoft Defender for Endpoint and Microsoft Defender for IoT**

Utilizing Microsoft services such as [Microsoft Defender for IoT](https://docs.microsoft.com/en-us/azure/defender-for-iot/overview) and Microsoft Defender for Endpoint you can get full visibility into assets and risk across your entire IoT/OT environment to support risk mitigation. Microsoft Defender for IoT can proactively address vulnerabilities in your IoT/OT environment. Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your crown jewel assets.

Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. See [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection) page to learn more.

Get a bird's-eye view across IT/OT boundaries with interoperability with [Microsoft Sentinel](https://azure.microsoft.com/en-us/services/azure-sentinel/), cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with [Microsoft Defender for Cloud Apps](https://azure.microsoft.com/en-us/services/security-center/), and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud. Plus, get interoperability with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

**Intune/Intune Suite & Microsoft Copilot for Security**

Copilot for Security for Microsoft Entra helps reduce the time to resolution by providing IT admins and SOC analysts the right context to investigate and remediate identity risk and identity-based incidents. Risky user summarization provides admins and responders quick access to the most critical information in context to aid their investigation. Microsoft Purview can use Microsoft Copilot for Security to investigate insider risk management activities and data loss prevention alerts, while Defender Threat Intelligence uses Copilot for Security to further enhance its threat intelligence capability to assess the risk landscape of the environment. Copilot for Security can be used with Intune/Intune Suite to determine device policy and configuration settings, and make determinations on which settings are noncompliant, reducing an organization’s security risk posture.

Intune/Intune Suite has applications such as Advanced Analytics which monitor for health anomalies of devices, query devices to get real time access to data about their health and configuration data, information which can be used to determine if devices pose specific risks to an organization's environment or require updates, patching or further review depending upon the type of risk they may pose.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)
* [Use Intune Suite add-on capabilities](https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons)

**Customer Responsibility**

* Responsible for conducting a risk assessment that addresses the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of Customer-deployed resources and processed, stored, or transmitted information.
* Responsible for reviewing the Microsoft Azure Security Authorization package and performing a risk assessment for any controls deferred to CUSTOMER relating to shared touch points as identified in the Microsoft Azure CUSTOMER Responsibility Matrix.
* Responsible for conducting a risk assessment and documenting the risk assessment results in the security plan, risk assessment report, and/or other CUSTOMER-defined document.
* Responsible for conducting a risk assessment and reviewing its results at a CUSTOMER-defined frequency.
* Responsible for conducting a risk assessment and disseminating its results to CUSTOMER-defined personnel/roles.
* Responsible for updating the risk assessment at the CUSTOMER-defined frequency when there are significant changes to Customer-deployed resources (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

RA.L2-3.11.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** RA-5, RA-5(5) | |
| **Practice:** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  **Assessment Objectives:**  [a] the frequency to scan for vulnerabilities in organizational systems and applications is defined;  [b] vulnerability scans are performed on organizational systems with the defined  frequency;  [c] vulnerability scans are performed on applications with the defined frequency;  [d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified; and  [e] vulnerability scans are performed on applications when new vulnerabilities are identified. | |
| **Primary Services** | **Secondary Services** |
| Microsoft 365 Defender  Microsoft Defender for IoT  Microsoft Defender for Endpoint Microsoft Defender for Office 365  Threat and Vulnerability Management  Microsoft Defender for Smartscreen | Intune/Intune Suite  GitHub Advanced Security (Add-On)  Microsoft Copilot for Security  GitHub Enterprise Cloud GitHub AE |

**Implementation Statement:**

**Microsoft Defender for Cloud**

Microsoft Defender for Cloud includes a built-in vulnerability scanner powered by Qualys. There is also capability for direct integration with the vulnerability scanner of your choice via the Azure Security Marketplace. Qualys’s scanner is a leading tool for real-time identification of vulnerabilities in your Azure Virtual Machines. It’s only available to users on the standard pricing tier. You do not need a Qualys license or even a Qualys account – everything is handled seamlessly inside Security Center. To learn more, see [Integrated vulnerability scanner for virtual machines (Standard tier only)](https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment).

**Microsoft Defender for IoT and Microsoft Defender for Endpoint**

Utilizing Microsoft services such as [Microsoft Defender for IoT](https://docs.microsoft.com/en-us/azure/defender-for-iot/overview) and Microsoft Defender for Endpoint you can get full visibility into assets and risk across your entire IoT/OT environment to support risk mitigation. Microsoft Defender for IoT can proactively address vulnerabilities in your IoT/OT environment. Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your crown jewel assets.

Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. All devices onboarded in Microsoft Defender for Endpoint are scanned for vulnerabilities. See [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection) page to learn more.

Get a bird's-eye view across IT/OT boundaries with interoperability with [Microsoft Sentinel](https://azure.microsoft.com/en-us/services/azure-sentinel/), cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with [Microsoft Defender for Cloud Apps](https://azure.microsoft.com/en-us/services/security-center/), and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud. Plus, get interoperability with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

**Microsoft Copilot for Security**

Microsoft Copilot for Security does not have the capability to perform vulnerability scans or remediate vulnerabilities, but the service can enhance other Microsoft services’ ability to provide more contextual and specific risk and vulnerability data that can assist in the mitigation and remediation of vulnerabilities and threats. Defender EASM’s integration with Copilot for Security enables users to interact with Microsoft’s discovered attack surfaces. These attack surfaces allow users to quickly understand their externally facing infrastructure and relevant, critical risks to their organization. They provide insight into specific areas of risk, including vulnerabilities, compliance, and security hygiene. Defender Threat Intelligence can use Copilot for Security to develop prompts for vulnerability data by CVE such as showing the latest CVEs, sharing the technologies susceptible to specific CVEs, threat actors associated with specific CVEs, and more.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Threat and vulnerability management**

Threat and vulnerability management is built in, real time, and cloud powered. It's fully integrated with Microsoft endpoint security stack, the Microsoft Intelligent Security Graph, and the application analytics knowledge base. To discover endpoint vulnerabilities and misconfiguration, threat and vulnerability management uses the same agentless built-in Defender for Endpoint sensors to reduce cumbersome network scans and IT overhead.

Moreover, threat and vulnerability management helps customers prioritize and focus on the weaknesses that pose the most urgent and the highest risk to the organization allowing security administrators and IT administrators to collaborate seamlessly to remediate issues.

[**Azure Policies**](#_Azure_Policy)

* [**RA.L2-3.11.2 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#scan-for-vulnerabilities-in-organizational-systems-and-applications-periodically-and-when-new-vulnerabilities-affecting-those-systems-and-applications-are-identified)

**Azure**

**Customer Responsibility**

* Responsible for performing periodic vulnerability scanning on all Customer-deployed resources, including applications built on those resources.  
  responsible for performing scans of their applications running within or connected to their purchased Microsoft Azure VMs or deployments.
* Responsible for employing vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.
* Responsible for analyzing scan reports and results from security control assessments.
* Responsible for remediating vulnerabilities in Customer-deployed resources in accordance with CUSTOMER risk assessment.
* Responsible for sharing information obtained from the vulnerability scanning process and security control assessments to help eliminate similar vulnerabilities across Customer-deployed resources.
* Responsible for implementing privileged access for executing CUSTOMER-defined vulnerability scanning activities.

**GCCH**

**Customer Responsibility (W365):**

* Customers are responsible for vulnerability scanning on Windows 365 VMs.

**Additional Resources**

* [View findings from vulnerability assessment solutions in Microsoft Defender for Cloud Apps](https://docs.microsoft.com/en-us/azure/security-center/remediate-vulnerability-findings-vm)
* [Adaptive application controls in Microsoft Defender for Cloud Apps](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application)
* [Vulnerabilities in my organization - threat and vulnerability management](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-weaknesses?view=o365-worldwide)
* [MITRE ATT&CK® mappings released for built-in Azure security controls](https://www.microsoft.com/security/blog/2021/06/29/mitre-attck-mappings-released-for-built-in-azure-security-controls/)

RA.L2-3.11.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** RA-5 | |
| **Practice:** Remediate vulnerabilities in accordance with risk assessments.  **Assessment Objectives:**  [a] vulnerabilities are identified; and  [b] vulnerabilities are remediated in accordance with risk assessments. | |
| **Primary Services** | **Secondary Services** |
| Microsoft 365 Defender  Microsoft Defender for Endpoint  Microsoft Defender for IoT  Microsoft Defender for Cloud | Intune/Intune Suite  GitHub Enterprise Cloud  Microsoft Secure Score GitHub AE  GitHub Advanced Security (Add-On)  Insider Risk Management  Threat and Vulnerability Management  Microsoft Copilot for Security |

**Implementation Statement:**

**Microsoft Defender for IoT, Microsoft Defender for Endpoint and Microsoft 365 Defender**

A vulnerability is a weakness that a threat actor could leverage, to compromise the confidentiality, availability, or integrity of a resource. Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. See [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection) page to learn more.

[Managing vulnerabilities](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/next-gen-threat-and-vuln-mgt) applies to [Microsoft Defender for Endpoint](https://go.microsoft.com/fwlink/p/?linkid=2154037) and [Microsoft 365 Defender](https://go.microsoft.com/fwlink/?linkid=2118804). Managing vulnerabilities reduces organizational exposure, hardens endpoint surface area, increases organizational resilience, and reduces the attack surface of your resources. Threat and Vulnerability Management provides visibility into software and security misconfigurations and provide recommendations for mitigations.

Utilizing Microsoft services such as [Microsoft Defender for IoT](https://docs.microsoft.com/en-us/azure/defender-for-iot/overview) and Microsoft Defender for Endpoint you can get full visibility into assets and risk across your entire IoT/OT environment to support risk mitigation. Microsoft Defender for IoT can proactively address vulnerabilities in your IoT/OT environment. Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your crown jewel assets.

Microsoft Defender for Endpoint is an endpoint security solution that includes risk-based vulnerability management and assessment; attack surface reduction capabilities; behavioral based and cloud-powered next generation protection; endpoint detection and response (EDR); automatic investigation and remediation; and managed hunting services. See [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection) page to learn more.

Get a bird's-eye view across IT/OT boundaries with interoperability with [Microsoft Sentinel](https://azure.microsoft.com/en-us/services/azure-sentinel/), cloud native SIEM/SOAR. Automate response with IoT/OT playbooks. Use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with [Microsoft Defender for Cloud Apps](https://azure.microsoft.com/en-us/services/security-center/), and protect them with extended detection and response (XDR) from Microsoft Defender for Cloud. Plus, get interoperability with other SOC tools such as Splunk, IBM QRadar, and ServiceNow.

**Microsoft Defender for Cloud**

Microsoft Defender for Cloud includes a built-in vulnerability scanner powered by Qualys. There is also capability for direct integration with the vulnerability scanner of your choice via the Azure Security Marketplace. Qualys’s scanner is a leading tool for real-time identification of vulnerabilities in your Azure Virtual Machines. It is only available to users on the standard pricing tier. You do not need a Qualys license or even a Qualys account – everything is handled seamlessly inside Security Center. To learn more, see [Integrated vulnerability scanner for virtual machines (Standard tier only)](https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment).

Microsoft Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level. To increase your security, review Security Center's recommendations page for the outstanding actions necessary to raise your score. Each recommendation includes instructions to help you remediate the specific issue.

Recommendations are grouped into **security controls**. Each control is a logical group of related security recommendations and reflects your vulnerable attack surfaces. Your score only improves when you remediate *all* of the recommendations for a single resource within a control. To see how well your organization is securing each individual attack surface, review the scores for each security control. Single click remediation is part of the Microsoft Defender for Cloud. Single-click remediations include policies to fix common vulnerabilities. To learn more, see [Microsoft Defender for Cloud single click remediation](https://azure.microsoft.com/en-gb/blog/azure-security-center-single-click-remediation-and-azure-firewall-jit-support/). To learn more, see [How your secure score is calculated](https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls#how-your-secure-score-is-calculated).

**Microsoft Copilot for Security**

Microsoft Copilot for Security does not have the capability to perform vulnerability scans or remediate vulnerabilities, but the service can enhance other Microsoft services’ ability to provide more contextual and specific risk and vulnerability data that can assist in the mitigation and remediation of vulnerabilities and threats. Defender EASM’s integration with Copilot for Security enables users to interact with Microsoft’s discovered attack surfaces. These attack surfaces allow users to quickly understand their externally facing infrastructure and relevant, critical risks to their organization. They provide insight into specific areas of risk, including vulnerabilities, compliance, and security hygiene. Defender Threat Intelligence can use Copilot for Security to develop prompts for vulnerability data by CVE such as showing the latest CVEs, sharing the technologies susceptible to specific CVEs, threat actors associated with specific CVEs, and more.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Insider risk management**

Insider risk management uses the full breadth of service and 3rd-party indicators to help you quickly identify, triage, and act on risk activity. By using logs from Microsoft 365 and Microsoft Graph, insider risk management allows you to define specific policies to identify risk indicators. These policies allow you to identify risky activities and to act to mitigate these risks.

Moreover, insider risk analytics enables you to conduct an evaluation of potential insider risks in your organization without configuring any insider risk policies. This evaluation can help your organization identify potential areas of higher user risk and help determine the type and scope of insider risk management policies you may consider configuring.

To learn more, see:

* [Insider risk management](https://learn.microsoft.com/en-us/purview/insider-risk-management-solution-overview)

**Azure**

**Customer Responsibility**

* Remediating vulnerabilities in customer-deployed resources in accordance with the customer risk assessment.

**GCCH**

**Customer Responsibility (W365):**

* Customers are responsible for vulnerability scanning on Windows 365 VMs.

### Security Assessment (CA)

CA.L2-3.12.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CA-2, CA-5, CA-7, PL-2 | |
| **Practice:** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  **Assessment Objectives:**  [a] the frequency of security control assessments is defined; and  [b] security controls are assessed with the defined frequency to determine if the controls are effective in their application. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Sentinel  Azure Monitor Intune/Intune Suite  Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint  Microsoft Defender for IoT  Microsoft 365 Defender  Microsoft Secure Score  Microsoft Purview |

**Implementation Statement:**

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* Use [Microsoft Purview Compliance Manager](https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager) to create your own assessments that evaluate compliance with the industry and regional regulations that apply to your organization.

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Azure Monitor**

[Azure Monitor](https://azure.microsoft.com/en-us/services/monitor/) maximizes the availability and performance of applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

**Microsoft Defender for Cloud Apps**

[Microsoft Defender for Cloud Apps](https://azure.microsoft.com/en-us/services/security-center/) is a unified infrastructure security management system that strengthens the security posture of your datacenters and provides advanced threat protection across your hybrid workloads in the cloud, be it Azure, any other cloud, or on-premises. Microsoft Defender for Cloud Apps helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard. In the dashboard, Security Center provides insights into your compliance posture based on continuous assessments of your Azure environment. Security Center analyzes risk factors in your hybrid cloud environment according to security best practices. These assessments are mapped to compliance controls from a supported set of standards. In the Regulatory compliance dashboard, you can see the status of all the assessments within your environment in the context of a particular standard or regulation. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves. To learn more, see [Tutorial: Improve your regulatory compliance](https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard#assess-your-regulatory-compliance).

**Microsoft Sentinel**

Microsoft Sentinel is a scalable, cloud-native security information and event manager (SIEM) platform that uses built-in AI to analyze large volumes of data across the enterprise from all sources in a few seconds at a fraction of the cost. It includes built-in connectors for easy onboarding of popular security solutions and allows you to collect data from any source with support for open standard formats like CEF and Syslog. There are good practice baselines for Microsoft Sentinel. This security baseline applies guidance from the [Azure Security Benchmark version 1.0](https://docs.microsoft.com/en-us/azure/security/benchmarks/overview-v1) to Microsoft Sentinel. The Azure 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 Azure Security Benchmark and the related guidance applicable to Microsoft Sentinel. To learn more, [see Azure security baseline for Microsoft Sentinel.](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/sentinel-security-baseline)

**Microsoft Secure Score**

Microsoft Secure Score is a numerical summary of your security posture based on system configurations, user behavior, and other security-related measurements. Microsoft Secure Score represents the extent to which you have adopted security controls in your Microsoft environment that can help offset the risk of being breached.

**Azure Service Health**

[Azure Service Health](https://azure.microsoft.com/en-us/features/service-health/) provides personalized alerts and guidance when Azure service issues affect our customers’ business. It can notify you, help you understand the impact of issues, and keep you updated as the issue resolves. It can also help prepare for planned maintenance and changes that could affect the availability of your resources.

**Azure Governance**

[Governance](https://azure.microsoft.com/en-us/solutions/governance/) validates that your organization can achieve its goals through an effective and efficient use of IT. It meets this need by creating clarity between business goals and IT projects. With Azure you build and scale your applications quickly while maintaining control.

**Azure Blueprints**

[Azure Blueprints](https://azure.microsoft.com/en-us/services/blueprints/) enable quick, repeatable creation of fully governed environments. This service helps you deploy and update cloud environments in a repeatable manner using artifacts such as policies, resource groups, deployment templates, and role-based access controls. This service is built to help DevOps set up governed Azure environments and scale to support production implementations for large-scale migrations.

Azure Blueprints provides an avenue to apply security controls, policies and resources. Just as a blueprint allows an engineer or an architect to sketch a project’s design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization’s standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they are building within organizational compliance with a set of built-in components — such as networking — to speed up development and delivery. Azure Blueprints can actively apply controls with the *deployifnotexists* option or can be leveraged for monitoring controls passively with the *auditifnotexists* option. To learn more, see [Tutorial: Protect new resources with Azure Blueprints resource locks](https://docs.microsoft.com/en-us/azure/governance/blueprints/tutorials/protect-new-resources)

**Customer Responsibility**

* Assessing the security controls in organizational systems to determine if the controls are effective in their application.

CA.L2-3.12.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CA-2, CA-5, CA-7, PL-2 | |
| **Practice:** Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  **Assessment Objectives:**  [a] deficiencies and vulnerabilities to be addressed by the plan of action are identified;  [b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities; and  [c] the plan of action is implemented to correct identified deficiencies and reduce or  eliminate identified vulnerabilities. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Defender for Endpoint  Threat and Vulnerability Management  Microsoft 365 Defender  Microsoft Sentinel  Microsoft Secure Score  Microsoft 365 Web Apps |

**Implementation Statement:**

**Microsoft Defender for Endpoint**

Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization. Your score for devices is visible in the [threat and vulnerability management dashboard](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-dashboard-insights?view=o365-worldwide) of the Microsoft Defender Portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. Improve your security configuration by remediating issues from the security recommendations list. As you do so, your Microsoft Secure Score for Devices improves, and your organization becomes more resilient against cybersecurity threats and vulnerabilities.

For more information see, [learn how it works](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-microsoft-secure-score-devices?view=o365-worldwide#how-it-works).

**Customer Responsibility**

* Develop & implement a POA&M to correct identified deficiencies and reduce or eliminate identified vulnerabilities
* Document, review and approve the POA&M
* Identify deficiencies and vulnerabilities to be addressed by the POA&M
* Identify personnel responsible for the development and implementation of the POA&M

CA.L2-3.12.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CA-2, CA-5, CA-7, PL-2 | |
| **Practice:** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  **Assessment Objective:**  [a] security controls are monitored on an ongoing basis to ensure the continued  effectiveness of those controls. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Sentinel  Microsoft 365 Defender  Microsoft Secure Score  Intune/Intune Suite  Microsoft Defender for Cloud Apps Microsoft Defender for Endpoint  Microsoft Purview  Azure Monitor |

**Implementation Statement:**

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The continuous and ongoing terms imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* Use [Microsoft Purview Compliance Manager](https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager) to create your own assessments that evaluate compliance with the industry and regional regulations that apply to your organization.

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance

[Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Azure Monitor**

[Azure Monitor](https://azure.microsoft.com/en-us/services/monitor/) maximizes the availability and performance of applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

**Microsoft Defender for Cloud Apps**

[Microsoft Defender for Cloud Apps](https://azure.microsoft.com/en-us/services/security-center/) is a unified infrastructure security management system that strengthens the security posture of your datacenters and provides advanced threat protection across your hybrid workloads in the cloud, be it Azure, any other cloud, or on-premises. Microsoft Defender for Cloud Apps helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard. In the dashboard, Security Center provides insights into your compliance posture based on continuous assessments of your Azure environment. Security Center analyzes risk factors in your hybrid cloud environment according to security best practices. These assessments are mapped to compliance controls from a supported set of standards. In the Regulatory compliance dashboard, you can see the status of all the assessments within your environment in the context of a particular standard or regulation. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves. To learn more, see [Tutorial: Improve your regulatory compliance](https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard#assess-your-regulatory-compliance).

**Microsoft Sentinel**

Microsoft Sentinel is a scalable, cloud-native security information and event manager (SIEM) platform that uses built-in AI to analyze large volumes of data across the enterprise from all sources in a few seconds at a fraction of the cost. It includes built-in connectors for easy onboarding of popular security solutions and allows you to collect data from any source with support for open standard formats like CEF and Syslog. There are good practice baselines for Microsoft Sentinel. This security baseline applies guidance from the [Azure Security Benchmark version 1.0](https://docs.microsoft.com/en-us/azure/security/benchmarks/overview-v1) to Microsoft Sentinel. The Azure 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 Azure Security Benchmark and the related guidance applicable to Microsoft Sentinel. To learn more, [see Azure security baseline for Microsoft Sentinel.](https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/sentinel-security-baseline)

**Microsoft Secure Score**

Microsoft Secure Score is a numerical summary of your security posture based on system configurations, user behavior, and other security-related measurements. Microsoft Secure Score represents the extent to which you have adopted security controls in your Microsoft environment that can help offset the risk of being breached.

**Azure Service Health**

[Azure Service Health](https://azure.microsoft.com/en-us/features/service-health/) provides personalized alerts and guidance when Azure service issues affect our customers’ business. It can notify you, help you understand the impact of issues, and keep you updated as the issue resolves. It can also help prepare for planned maintenance and changes that could affect the availability of your resources.

**Azure Governance**

[Governance](https://azure.microsoft.com/en-us/solutions/governance/) validates that your organization can achieve its goals through an effective and efficient use of IT. It meets this need by creating clarity between business goals and IT projects. With Azure you build and scale your applications quickly while maintaining control.

**Azure Blueprints**

[Azure Blueprints](https://azure.microsoft.com/en-us/services/blueprints/) enable quick, repeatable creation of fully governed environments. This service helps you deploy and update cloud environments in a repeatable manner using artifacts such as policies, resource groups, deployment templates, and role-based access controls. This service is built to help DevOps set up governed Azure environments and scale to support production implementations for large-scale migrations.

Azure Blueprints provides an avenue to apply security controls, policies and resources. Just as a blueprint allows an engineer or an architect to sketch a project’s design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization’s standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they are building within organizational compliance with a set of built-in components — such as networking — to speed up development and delivery. Azure Blueprints can actively apply controls with the *deployifnotexists* option or can be leveraged for monitoring controls passively with the *auditifnotexists* option. To learn more, see [Tutorial: Protect new resources with Azure Blueprints resource locks](https://docs.microsoft.com/en-us/azure/governance/blueprints/tutorials/protect-new-resources).

**Customer Responsibility**

* Identifying security controls to be continuously monitored.
* Define a frequency to continuously monitor to support risk-based decision making.
* Provide output of monitoring activities to stakeholders.

CA.L2-3.12.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** CA-2, CA-5, CA-7, PL-2 | |
| **Practice:** Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.  **Assessment Objectives:**  [a] a system security plan is developed;  [b] the system boundary is described and documented in the system security plan;  [c] the system environment of operation is described and documented in the system  security plan;  [d] the security requirements identified and approved by the designated authority as  non-applicable are identified;  [e] the method of security requirement implementation is described and documented in the system security plan;  [f] the relationship with or connection to other systems is described and documented in the system security plan;  [g] the frequency to update the system security plan is defined; and  [h] system security plan is updated with the defined frequency. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft 365 Web Apps  Power Automate |

**Implementation Statement:**

Microsoft 365 can help remind you to perform updates on documents such as the SSP. With Microsoft 365, reminders to review documentation are made simple. Set up details such as description, review date, owner and receive an email reminder for items due soon with a pre-built Power Automate flow in Microsoft Lists or SharePoint.

**Customer Responsibility:**

* Developing a system security plan (SSP) that meets the criteria defined by the target authorization (e.g., FedRAMP). Customers may reference NIST Special Publication 800-18 R1, *Guide for Developing Security Plans for Federal Information Systems*. The customer SSP should address controls inherited from Microsoft Azure.
* Distributing the system security plan.
* Reviewing the system security plan.
* Updating the system security plan.
* Protecting the system security plan.

### Systems and Communications Protection (SC)

SC.L1-3.13.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping: SC-7, SA-8** | |
| **Practice:** Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.  **Assessment Objectives:**  [a] the external system boundary is defined;  [b] key internal system boundaries are defined;  [c] communications are monitored at the external system boundary;  [d] communications are monitored at key internal boundaries;  [e] communications are controlled at the external system boundary;  [f] communications are controlled at key internal boundaries;  [g] communications are protected at the external system boundary; and  [h] communications are protected at key internal boundaries. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel  Microsoft Purview  Azure Firewall | Azure Bastion  Azure ExpressRoute  Azure Monitor  Azure Virtual Machines  Azure Web Application Firewall  Conditional Access  Load Balancer  Log Analytics Workspace  Microsoft Azure Portal  Microsoft Defender for IoT  Network Security Groups  Virtual Network  VPN Gateway  Customer Lockbox  Microsoft Defender for Cloud Apps  Microsoft Defender for Office 365  Microsoft Defender SmartScreen  Intune/Intune Suite  Microsoft 365 Defender  Windows 365 Cloud PC  Microsoft Defender for Endpoint  Teams |

**Implementation Statement:**

**Azure Firewall**

Implement boundary protection through the use of controlled devices at the network boundary and at key points within the information system. The overarching principle should be to allow only connection and communication that is necessary for systems to operate, blocking all other ports, protocols and connections by default.

If you configure network rules and application rules, then network rules are applied in priority order before application rules. The rules are terminating. If a match is found in a network rule, no other rules are processed. If there is no network rule match, and if the protocol is HTTP, HTTPS, or MSSQL, then the packet is then evaluated by the application rules in priority order. If still no match is found, then the packet is evaluated against the [infrastructure rule collection](https://docs.microsoft.com/en-us/azure/firewall/infrastructure-fqdns). If there is still no match, then the packet is denied by default.

Inbound Internet connectivity can be enabled by configuring Destination Network Address Translation (DNAT) as described in [Tutorial: Filter inbound traffic with Azure Firewall DNAT using the Azure portal](https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat). NAT rules are applied in priority before network rules. If a match is found, an implicit corresponding network rule to allow the translated traffic is added. For security reasons, the recommended approach is to add a specific internet source to allow DNAT access to the network and avoid using wildcards. To learn more, see [Deploy and configure Azure Firewall using the Azure portal](https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal).

Application rules are not applied for inbound connections. If you want to filter inbound HTTP/S traffic, you should use Web Application Firewall (WAF). To learn more, see [What is Azure Web Application Firewall?](https://docs.microsoft.com/en-us/azure/web-application-firewall/overview)

**Intune/Intune Suite**

Intune and Microsoft Entra ID work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and [on-premises apps](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-application-proxy-get-started). Additionally, you can set a policy in Microsoft Entra ID to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about [requiring managed devices with Conditional Access in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices)

**Network Security Groups**

Network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the [default security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules) that are applied, and the rule properties that you can modify to create an [augmented security rule](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#augmented-security-rules).

**Conditional Access**

Conditional access policies can be integrated with Defender for Cloud Apps to provide controls for cloud and on-premises applications from external systems. Mobile application management in Intune can protect organization data at the application level, including custom apps and store apps, from managed devices that interact with external systems. An example would be accessing cloud services. You can use app management on organization-owned devices and personal devices.

**Microsoft 365 inter-tenant collaboration**

Microsoft 365 inter-tenant collaboration options include using a central location for files and conversations, sharing calendars, using IM, audio/video calls for communication, and securing access to resources and applications.

**Windows 365 Cloud PC**

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine (Cloud PCs) for your end users. Each Cloud PC is assigned to an individual user and is their dedicated Windows device. Windows 365 provides the productivity, security, and collaboration benefits of Microsoft 365.

To learn more, see:

* [Find the Right Windows 365 Cloud PC](https://www.microsoft.com/en-us/windows-365/cloud-pc-chooser)
* [Compare Plans and Pricing](https://www.microsoft.com/en-us/windows-365/business/compare-plans-pricing)
* [What is Windows 365 Enterprise?](https://learn.microsoft.com/en-us/windows-365/enterprise/overview?source=recommendations)
* [Manage Windows 365 Cloud PCs with Configuration Manager](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-cloud-pcs-using-configuration-manager)
* [Security overview for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/security-guidelines)

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

[**Azure Policies**](#_Azure_Policy)

* [**SC.L1-3.13.1 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#monitor-control-and-protect-communications-ie-information-transmitted-or-received-by-organizational-systems-at-the-external-boundaries-and-key-internal-boundaries-of-organizational-systems)

**Azure**

**Customer Responsibility**

* monitoring and controlling communications at and within the boundaries of the Customer-deployed system.
* implementing subnetworks for Customer-deployed resources to logically separate publicly accessible resources from internal resources.
* restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the CUSTOMER's security architecture.
* configuring all Customer-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
* configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. CUSTOMER’s who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

**Additional Resources:**

* [Security guide for Microsoft Teams overview](https://learn.microsoft.com/en-us/microsoftteams/teams-security-guide)

SC.L2-3.13.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-7, SA-8 | |
| **Practice:** Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.  **Assessment Objectives:**  [a] architectural designs that promote effective information security are identified;  [b] software development techniques that promote effective information security are  identified;  [c] systems engineering principles that promote effective information security are  identified;  [d] identified architectural designs that promote effective information security are  employed;  [e] identified software development techniques that promote effective information  security are employed; and  [f] identified systems engineering principles that promote effective information security are employed. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Defender for Cloud  Microsoft 365 Defender  Microsoft Entra ID  Azure Automation  Azure Bastion  Azure Monitor  Azure Front Door  Azure Functions  Azure Firewall  Azure Key Vault  Azure Private Link  Azure Application Gateway  Microsoft Entra ID Multi-Factor Authentication  Azure Policy  Conditional Access  Microsoft Purview  Windows 365 Cloud PC  Azure Virtual Machines  Intune/Intune Suite  Privileged Identity Management (PIM)  Windows Hello for Business |

**Implementation Statement:**

Promote effective information security within your organizational systems by implementing secure security design principles. Microsoft recommendations for [security design principles support these three key strategies](https://docs.microsoft.com/en-us/azure/architecture/framework/security/security-principles) (Security Strategy, Enterprise Segmentation Strategy and Account Control Strategy) and describe a securely architected system hosted on cloud or on-premises datacenters (or a combination of both). Application of these principles will dramatically increase the likelihood your security architecture will maintain assurances of confidentiality, integrity, and availability.

**Azure**

**Customer Responsibility**

* Monitoring and controlling communications at and within the boundaries of the Customer-deployed system.
* Implementing subnetworks for Customer-deployed resources to logically separate publicly accessible resources from internal resources.
* Restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the customer's security architecture.
* Configuring all Customer-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
* Configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. Customers who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

**Additional Resources:**

* [Security architecture design](https://learn.microsoft.com/en-us/azure/architecture/guide/security/security-start-here?source=recommendations)

SC.L2-3.13.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-2 | |
| **Practice:** Separate user functionality from system management functionality.  **Assessment Objectives:**  [a] user functionality is identified;  [b] system management functionality is identified; and  [c] user functionality is separated from system management functionality. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID  Azure RBAC | Conditional Access  Privileged Identity Management (PIM)  Azure Virtual Machine  Azure Bastion  Virtual Network  Network Security Groups  Intune/Intune Suite  Azure ExpressRoute |

**Implementation Statement:**

**Microsoft Entra ID Role Based Access Control**

Microsoft Entra ID roles allow you to grant granular permissions to your admins, abiding by the principle of least privilege. Microsoft Entra ID built-in and custom roles operate on concepts similar to those you will find in [the role-based access control system for Azure resources](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) (Azure roles). The [difference between these two role-based access control systems](https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles) is:

* Microsoft Entra ID roles control access to Microsoft Entra ID resources such as users, groups, and applications using Graph API
* Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

Both systems contain similarly used role definitions and role assignments. However, Microsoft Entra ID role permissions cannot be used in Azure custom roles and vice versa.

Microsoft Entra ID offers a robust security set for enforcing the separation of user functionality from system management functionality. A good practice is to segregate duties within your team by setting up [Role Based Access Control](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) (RBAC) which will help you manage who has access to Azure resources.

Ensure that the right users have the right access to the right resources by using intelligent cloud [identity governance](https://docs.microsoft.com/en-us/azure/active-directory/governance/). Monitor and audit access to all resources while managing employee productivity.

Additionally, you can secure privileged access within your organization using [Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Privileged%20Identity%20Management%20provides%20time,resources%20that%20you%20care%20about.&text=Require%20approval%20to%20activate%20privileged,authentication%20to%20activate%20any%20role) (PIM). PIM will reduce risk to accounts with the most privileged access, resources and data. PIM enforces [Just In Time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access) access for these accounts which allows timed permission to be granted for specific resources.

**Privileged Identity Management (PIM)**

With [Microsoft Entra ID PIM](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure), you can manage, control, and monitor your privileged identities and access to your directory information and resources in an Azure environment. The main reason for using Microsoft Entra ID PIM is to reduce the attack surface and to enable administrative access [just-in-time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access). Privileged access is often configured as permanent and unmonitored, but with Microsoft Entra ID PIM you can avoid security breaches and risks.

The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles. To protect the activation of a role, the service uses Microsoft Entra ID Multi-Factor Authentication. For example, during the activation process, a user can be forced to justify why they need to activate their role. Furthermore, you can also enable notifications that alert you when a privileged role is activated. For auditing and compliance requirements, you are also able to configure and enable access reviews that ensure a user needs a specific role. You can also download an audit history for both internal and external audits.

Privileged Identity Management (PIM) provides similar functionality to the Microsoft Identity Manager, including Privileged Access Management (PAM) in the on-premises infrastructure.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Network Security Groups**

[Network Security Groups](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview) are customizable and provide the ability to fully lock down network communication to and from your system-resources. You can restrict internet access by default, along with the use of network security groups, data segregation and isolated VPNs.

Use [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  to manage and secure identities by requiring [single sign-on](https://azure.microsoft.com/en-us/services/active-directory/sso/) and multifactor authentication to protect your users. The recommended way to enable and use Microsoft Entra ID Multi-Factor Authentication is with Conditional Access Policies. [Learn how to Create a Conditional Access Policy.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa#create-a-conditional-access-policy)

Additionally, [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with

[Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Explore using [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

**Customer Responsibility**

* Separating system functionality into two separate categories: user functionality and management functionality.

SC.L2-3.13.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-4 | |
| **Practice:** Prevent unauthorized and unintended information transfer via shared system resources.  **Assessment Objective:**  [a] unauthorized and unintended information transfer via shared system resources is  prevented. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Purview | Microsoft Entra ID Multi-Factor Authentication  Azure RBAC  Azure Virtual Machines  Azure Web Application Firewall  Conditional Access  Network Security Groups  Windows 365 Cloud PC  Privileged Identity Management (PIM)  Virtual Network  Microsoft Defender for Office 365  Intune/Intune Suite  Microsoft 365 Defender |

**Implementation Statement:**

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Microsoft Entra ID Role Based Access Control**

Microsoft Entra ID roles allow you to grant granular permissions to your admins, abiding by the principle of least privilege. Microsoft Entra ID built-in and custom roles operate on concepts similar to those you will find in [the role-based access control system for Azure resources](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) (Azure roles). The [difference between these two role-based access control systems](https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles) is:

* Microsoft Entra ID roles control access to Microsoft Entra ID resources such as users, groups, and applications using Graph API
* Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

Both systems contain similarly used role definitions and role assignments. However, Microsoft Entra ID role permissions cannot be used in Azure custom roles and vice versa.

Microsoft Entra ID offers a robust security set for preventing unauthorized and unintended information transfer via shared system resources. Best practice recommendation is to segregate duties within your team by setting up [Role Based Access](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) Control (RBAC) which will help you manage who has access to Azure resources.

Ensure that the right users have the right access to the right resources by using intelligent cloud [identity governance](https://docs.microsoft.com/en-us/azure/active-directory/governance/). Monitor and audit access to all resources while managing employee productivity.

**Microsoft Entra ID Multi-Factor Authentication**

Use [Microsoft Entra ID](https://azure.microsoft.com/en-us/services/active-directory/)  to manage and secure identities by requiring [single sign-on](https://azure.microsoft.com/en-us/services/active-directory/sso/) and multifactor authentication to protect your users. The recommended way to enable and use Microsoft Entra ID Multi-Factor Authentication is with Conditional Access Policies. [Learn how to Create a Conditional Access Policy.](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa#create-a-conditional-access-policy)

**Privileged Identity Management (PIM)**

With [Microsoft Entra ID PIM](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure), you can manage, control, and monitor your privileged identities and access to your directory information and resources in an Azure environment. The main reason for using Microsoft Entra ID PIM is to reduce the attack surface and to enable administrative access [just-in-time](https://docs.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/request-just-in-time-access). The service allows you to assign time-bound access to resources using a start and end date and that requires approval to activate privileged roles.

To learn more, see:

* [Start using Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started).
* [License requirements to use Privileged Identity Management - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements)

**Network Security Groups**

[Network Security Group](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview)s are customizable and provide the ability to fully lock down network communication to and from your system-resources. You can restrict internet access by default, along with the use of network security groups, data segregation and isolated VPNs.

**Intune/Intune Suite**

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Azure ExpressRoute**

Explore using [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

**Customer Responsibility**

* Preventing unauthorized and unintended information transfer between Customer-deployed resources.

**GCCH**

**Customer Responsibility:**

* Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users, i.e., guest access to SFB meetings.
* Guest access to SFB meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting. Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in “Office 365 Complementary Federal User Entity Control”.
* SharePoint Online guest invitations allow external users to access an organization’s SharePoint site(s). Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online, as an account type, should be allowed for their organization. Government customers are responsible for disabling guest access to SharePoint Online to remain compliant with FedRAMP standards.
* The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers. Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365.
* Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365.

SC.L1-3.13.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-7 | |
| **Practice:** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.  **Assessment Objectives:**  [a] publicly accessible system components are identified; and  [b] subnetworks for publicly accessible system components are physically or logically  separated from internal networks. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Azure Portal  Virtual Network | Azure Bastion  Azure Firewall  Load Balancer  Network Security Groups  Azure Web Application Firewall |

**Implementation Statement:**

Protect your [subnet](https://docs.microsoft.com/en-us/azure/virtual-machines/network-overview#:~:text=A%20subnet%20is%20a%20range,other%20without%20any%20extra%20configuration.) from potential threats by restricting access to it with a [Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules](https://azure.microsoft.com/en-us/blog/network-isolation-options-for-machines-in-windows-azure-virtual-networks/) that allow or deny network traffic to your subnet.

Learn how to add a subnet to your virtual network:

* [Add, change, or delete an Azure virtual network subnet](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet#add-a-subnet)

**Load Balancer/Network Security Groups**

A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs. An [internal (or private) load balancer](https://docs.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario. Standard load balancers and standard public IP addresses are closed to inbound connections unless opened by Network Security Groups. NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource. To learn about NSGs and how to apply them to your scenario, see [Network Security Groups](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview).

**Azure Bastion**

Azure Bastion is a fully managed platform PaaS service from Azure that is hardened internally to provide you with secure RDP/SSH connectivity. You do not need to apply any NSGs on Azure Bastion subnet. Because Azure Bastion connects to your virtual machines over private IP, you can configure your NSGs to allow RDP/SSH from Azure Bastion only. This removes the hassle of managing NSGs each time you need to securely connect to your virtual machines. [Create an Azure Bastion host and connect to a Windows VM](https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal).

[**Azure Policies**](#_Azure_Policy)

* [**SC.L1-3.13.5 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#implement-subnetworks-for-publicly-accessible-system-components-that-are-physically-or-logically-separated-from-internal-networks)

**Customer Responsibility**

* Monitoring and controlling communications at and within the boundaries of the Customer-deployed system.
* Implementing subnetworks for Customer-deployed resources to logically separate publicly accessible resources from internal resources.
* Restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the customer's security architecture.
* Configuring all Customer-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
* Configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. CUSTOMER’s who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.

SC.L2-3.13.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-7(5) | |
| **Practice:** Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).  **Assessment Objectives:**  [a] network communications traffic is denied by default; and  [b] network communications traffic is allowed by exception. | |
| **Primary Services** | **Secondary Services** |
| Azure Firewall | Load Balancer  Network Security Groups  Azure Web Application Firewall  Virtual Network  Conditional Access  Intune/Intune Suite |

**Implementation Statement:**

**Azure Firewall**

You can configure NAT rules, network rules, and applications rules on Azure Firewall using either classic rules or Firewall Policy. Azure Firewall denies all traffic by default, until rules are manually configured to allow traffic.

To learn more, see [Azure Firewall rule processing logic](https://learn.microsoft.com/en-us/azure/firewall/rule-processing)

Application rules are not applied for inbound connections. If you want to filter inbound HTTP/S traffic, you should use the Web Application Firewall (WAF).

To learn more, see [What is Azure Web Application Firewall?](https://docs.microsoft.com/en-us/azure/web-application-firewall/overview)

**Intune/Intune Suite**

Use the endpoint security Firewall policy in Intune to configure a devices built-in firewall for devices that run macOS and /11. Intune and Microsoft Entra ID work together to make sure only managed and compliant devices can access email, Microsoft 365 services, Software as a service (SaaS) apps, and [on-premises apps](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-application-proxy-get-started). Additionally, you can set a policy in Microsoft Entra ID to only enable domain-joined computers or mobile devices that are enrolled in Intune to access Microsoft 365 services. Learn more about [requiring managed devices with Conditional Access in Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices)

**Network Security Groups**

Network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes properties of a network security group rule, the [default security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules) that are applied, and the rule properties that you can modify to create an [augmented security rule](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#augmented-security-rules).

**Azure**

**Customer Responsibility**

* Configuring managed network interfaces to deny all traffic by default and permit by exception.

SC.L2-3.13.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-7(7) | |
| **Practice:** Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).  **Assessment Objective:**  [a] remote devices are prevented from simultaneously establishing non-remote  connections with the system and communicating via some other connection to  resources in external networks (i.e., split tunneling). | |
| **Primary Services** | **Secondary Services** |
| Azure VPN  Azure Firewall | Azure ExpressRoute  Azure Virtual Desktop  Microsoft Entra ID  Windows 365 Cloud PC |

**Implementation Statement:**

External networks are those networks, or Internet services, that are outside the organization’s scoped compliance boundary. A remote user connected to the internal network [scoped compliance boundary] must not be able to connect to an external network / Internet service directly. The external network traffic must flow through the organization’s managed network security devices (i.e., outbound proxy firewall).



SC.3.184 Compliance Boundary

In the above illustration, both the Enterprise Datacenter and the Cloud Service Provider (e.g., Microsoft 365) fall within the organization’s scoped compliance boundary. All applications and services hosted within the compliance boundary demonstrate compliance with CMMC maturity Level 2 (or higher) for protection of CUI.

**Remote Users**

The remote user’s device, when connected to the organizational internal network, must be configured with a routing table, such that all traffic for external networks will flow through the organization’s managed network security devices. An organization could use the Azure VPN to securely connect to their Azure resources and apply appropriate routing tables.

For those that run an on-premises VPN solution, [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  can be used to extend your on-premises datacenter, such that your Azure resources (e.g., virtual machines) can be considered part of your hybrid managed datacenter. Routing tables must be configured to ensure access to external networks / Internet services are monitored and controlled by the organization.

“Dynamic Routing,” *not to be confused with external network split-tunning*, is achieved by configuring a conditional access rule on the organization’s VPN to route to services *directly* within the organization’s scoped compliance boundary. For example, cloud services like Microsoft 365 that fall within the compliance boundary are whitelisted in a manner where traffic from a trusted endpoint may bypass the VPN device in the enterprise datacenter and communicate directly with the cloud service provider.

**Azure Virtual Machines**

Forced tunneling lets you redirect, or “force,” all Internet-bound traffic initiated from your Azure VMs through your firewall for inspection and auditing. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Unauthorized Internet access can potentially lead to information disclosure or other types of security breaches. To learn more, see [Configure forced tunneling using the Azure Resource Manager deployment model](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm).

**Azure Firewall**

A cloud-based firewall such as [Azure Firewall](https://docs.microsoft.com/en-us/azure/firewall/features) may act as the central security control point for network traffic, providing a ubiquitous and separate security layer in the cloud through which web traffic may flow. Azure Firewall not only protects Azure Virtual Network resources but offers [Premium features](https://docs.microsoft.com/en-us/azure/firewall/premium-features) such as URL Filtering and a network intrusion detection and prevention system (IDPS) allowing you to monitor the network for malicious activity, log information about this activity, report it, and optionally attempt to block it. Azure Firewall may also provide a proxied connection to SaaS services including Office 365.

**Microsoft Entra ID Application Proxy**

In addition to Azure Firewall, Microsoft Entra ID 's [Application Proxy](https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy) can provide secure remote access to web applications hosted in Azure or even in an on-premises datacenter. After a single sign-on to Microsoft Entra ID , users can access both cloud and on-premises applications through an external URL or an internal application portal. For example, Application Proxy can provide remote access and single sign-on to line of business (LOB) web applications. It’s here where security policies can be applied, ensuring policy enforcement regardless of whether the user is behind a firewall or logging on from home.

**Customer Responsibility**

* Preventing split tunneling for remote devices connecting to the Customer-deployed system.

**Additional Resources**

* [Manage device RDP redirections for Cloud PCs.](https://learn.microsoft.com/en-us/windows-365/enterprise/manage-rdp-device-redirections)
* [Set conditional access policies for Windows 365](https://learn.microsoft.com/en-us/windows-365/enterprise/set-conditional-access-policies)
* [CMMC and Split Tunnels to Cloud Services Whitepaper](https://aka.ms/cmmc/184whitepaper)
* [Zero Trust Architecture](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)
* [Using a Zero Trust strategy to secure Microsoft’s network during remote work](https://www.microsoft.com/itshowcase/blog/using-a-zero-trust-strategy-to-secure-microsofts-network-during-remote-work/)
* [Time to Rethink How You Provide Secure Internet Access for Remote Workers](https://securityboulevard.com/2020/04/time-to-rethink-how-you-provide-secure-internet-access-for-remote-workers/)
* [CMMC, Split Tunneling, and COVID](https://peakinfosec.com/information-security/compliance/cmmc/split_tunneling/)
* Implementing VPN [Split](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide) Tunneling for Microsoft 365

SC.L2-3.13.8

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-8, SC-8(1) | |
| **Practice:** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.  **Assessment Objectives:**  [a] cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are  identified;  [b] alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified; and  [c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Purview  Office 365 Message Encryption (OME) | Azure ExpressRoute  Azure Key Vault  Azure Storage  Azure Virtual Machines  Conditional Access  Load Balancer  Microsoft Azure Portal  Network Security Groups  Virtual Network  VPN Gateway  Microsoft Defender for Cloud Apps  Bitlocker  Intune/Intune Suite  Microsoft 365 Defender  Microsoft Defender for Endpoint  Dynamics 365  Windows 365 Cloud PC |

**Implementation Statement:**

You can have multiple layers of encryption in place at the same time. For example, you can encrypt email messages and also the communication channels through which your email flows. With Office 365, your data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES). Microsoft 365 provides Microsoft-managed solutions for volume encryption, file encryption, and mailbox encryption in Office 365. In addition, Microsoft provides encryption solutions that you can manage and control. These encryption solutions are built on Azure.

The Azure platform offers several mechanisms for keeping sessions secure including encryption in flight, and key management with Azure Key Vault. For more information see, [Azure encryption overview](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview).

Microsoft gives customers the ability to use [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) protocol to protect data when it is traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

[Perfect Forward Secrecy](https://en.wikipedia.org/wiki/Forward_secrecy) (PFS) protects connections between customers’ client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

Explore using [Azure ExpressRoute](https://docs.microsoft.com/en-us/azure/expressroute/)  to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Azure ExpressRoute connection restricts public internet providing a private connection to Azure.

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

**Office 365 Message Encryption**

With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content. Office 365 Message Encryption is an online service that's built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection. This service includes encryption, identity, and authorization policies to help secure your email. You can encrypt messages by using rights management templates, the Do Not Forward option, and the encrypt-only option.

**Intune/Intune Suite**

Encrypt CUI on mobile devices and mobile computing platforms [using Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager)  with Conditional access to require encryption, such as [BitLocker](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows) for Windows 10 and later. [Require app protection policy](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-protection-based-conditional-access) and an approved client app for cloud app access. Create and assign [Microsoft Intune app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies) to ensure that apps are protected with a PIN and Encrypted.

See the [Android app protection policy settings](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android) and [iOS/iPadOS app protection policy settings](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios) for detailed information on the encryption app protection policy setting.

[Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Additionally, using Microsoft Intune built-in Wi-Fi settings called a “profile,” you can deploy specific Wi-Fi connection requirements to users with supported devices in your organization. [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  offers many features, including authenticating to your network, using a pre-shared key for encryption and more.

**Azure Virtual Machines**

You can connect and sign in to a VM by using the [Remote Desktop Protocol (RDP)](https://docs.microsoft.com/en-us/windows/win32/termserv/remote-desktop-protocol) from a Windows client computer, or from a Mac with an RDP client installed. Data in transit over the network in RDP sessions can be protected by TLS. You can also use Remote Desktop to connect to a Linux VM in Azure.

For remote management, you can use [Secure Shell](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows) (SSH) to connect to Linux VMs running in Azure. SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. It is the default connection protocol for Linux VMs hosted in Azure. By using SSH keys for authentication, you eliminate the need for passwords to sign in. SSH uses a public/private key pair (asymmetric encryption) for authentication.

**Key Vault**

Without proper protection and management of the keys, encryption is rendered useless. Key Vault is the Microsoft-recommended solution for managing and controlling access to encryption keys used by cloud services. Permissions to access keys can be assigned to services or to users through Microsoft Entra ID accounts.

Key Vault relieves organizations of the need to configure, patch, and maintain hardware security modules (HSMs) and key management software. When you use Key Vault, you maintain control. Microsoft never sees your keys, and applications do not have direct access to them. You can also import or generate keys in HSMs. To learn more, see [About Azure Key Vault.](https://docs.microsoft.com/en-us/azure/key-vault/general/overview)

**VPN**

You can use an [Azure VPN gateway](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings) to send encrypted traffic between your virtual network and your on-premises location across a public connection, or to send traffic between virtual networks.

Site-to-site VPNs use [IPsec](https://en.wikipedia.org/wiki/IPsec) for transport encryption. Azure VPN gateways use a set of default proposals. You can configure Azure VPN gateways to use a custom IPsec/IKE policy with specific cryptographic algorithms and key strengths, rather than the Azure default policy sets.

**Intune/Intune Suite**

Use Intune to configure encryption at rest using BitLocker Drive Encryption on devices that run Windows 10. Some settings for BitLocker require the device have a supported TPM. To manage BitLocker in Intune, your account must have the applicable Intune [role-based access control](https://docs.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control) (RBAC) permissions. For more information on how to enforce BitLocker encryption using Intune, see [Create and deploy policy](https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#create-and-deploy-policy).

Intune can also manage macOS FileVault disk encryption. FileVault is a whole-disk encryption program that is included with macOS. You can use Intune to configure FileVault on devices that run macOS 10.13 or later**.** For more information on how to enforce FileVault encryption using Intune, see[Create device configuration policy for FileVault](https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices-filevault#create-device-configuration-policy-for-filevault)

Additionally, [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Azure Storage Account**

Azure Storage uses server-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments. Data in Azure Storage is encrypted and decrypted transparently using 256-bit [AES encryption](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard), one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is like BitLocker encryption on Windows.

Azure Storage encryption is enabled for all storage accounts, including both Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled. Because your data is secured by default, you do not need to modify your code or applications to take advantage of Azure Storage encryption.

However, you can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.

You must use one of the following Azure key stores to store your customer-managed keys:

* [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/overview)
* [Azure Key Vault Managed Hardware Security Module (HSM) (preview)](https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview)

You can switch between customer-managed keys and Microsoft-managed keys at any time. For more information about Microsoft-managed keys, see [About encryption key management](https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption#about-encryption-key-management). To learn more, see [Enable Customer-Managed keys for a storage account.](https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#enable-customer-managed-keys-for-a-storage-account)

[**Azure Policies**](#_Azure_Policy)

* [**SC.L2-3.13.8 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#implement-cryptographic-mechanisms-to-prevent-unauthorized-disclosure-of-cui-during-transmission-unless-otherwise-protected-by-alternative-physical-safeguards)

**Azure**

**Customer Responsibility**

* Configuring all customer-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.
* Configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. Customers who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure, and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.
* For protecting information in transit by using cryptographic mechanisms to prevent the unauthorized disclosure of and/or detecting changes to customer-controlled information during transmission.

**GCCH**

**Customer Responsibility:**

* Government customers are responsible for having a process in place to check the validity of the Office 365 Web sites prior to signing on by reviewing the digital certificate on the site to ensure they are the Office 365 Web sites. If government customers are using USGCB baselines, supported web browsers will enforce this review automatically by default and prevent connections if the digital certificate is invalid.
* Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliant protocols. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections.

**Additional Resources:**

* [Data encryption - Power Platform |](https://learn.microsoft.com/en-us/power-platform/admin/data-encryption) Dynamics 365
* [Data encryption in Windows 365 | Windows](https://learn.microsoft.com/en-us/windows-365/enterprise/encryption) 365 Cloud PC

SC.L2-3.13.9

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-10 | |
| **Practice:** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.  **Assessment Objectives:**  [a] a period of inactivity to terminate network connections associated with  communications sessions is defined;  [b] network connections associated with communications sessions are terminated at the end of the sessions; and  [c] network connections associated with communications sessions are terminated after the defined period of inactivity. | |
| **Primary Services** | **Secondary Services** |
|  | Microsoft Azure Portal  Azure Virtual Machines  VPN Gateway  Microsoft Entra ID  Intune/Intune Suite  M365 Web Apps  Conditional Access  Windows 365 Cloud PC  Microsoft 365 Defender |

**Implementation Statement:**

**Microsoft Entra ID**

Implement automatic user session re-evaluation with Microsoft Entra ID features such as Risk-Based Conditional Access and Continuous Access Evaluation. Inactivity conditions can be implemented at a device level as described in:

* [Sign-in risk-based Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk)
* [User risk-based Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk-user)
* [Continuous Access Evaluation](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation)
* [Configurable token lifetimes - Microsoft identity platform | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes)

The Microsoft Entra ID default for browser session persistence allows users on personal devices to choose whether to persist the session by showing a “Stay signed in?” prompt after successful authentication. If browser persistence is configured in AD FS using the guidance in the article [AD FS Single Sign-On Settings](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-single-sign-on-settings#enable-psso-for-office-365-users-to-access-sharepoint-online), we will comply with that policy and persist the Microsoft Entra ID session as well. You can also configure whether users in your tenant see the “Stay signed in?” prompt by changing the appropriate setting in the company branding pane in Azure portal using the guidance in the article [Customize your Microsoft Entra ID sign-in page](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding).

To learn more, see [Configure authentication session management with Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime).

**Microsoft 365 web apps**

When users authenticate in any of the Microsoft 365 web apps or mobile apps, a session is established. For the duration of the session, users won't need to re-authenticate. Sessions can expire when users are inactive, when they close the browser or tab, or when their authentication token expires for other reasons such as when their password has been reset. The Microsoft 365 services have different session timeouts to correspond with the typical use of each service.

**Azure VPN Gateway**

Azure virtual network gateways provide an easy way to view and disconnect current Point-to-site VPN sessions. The session status is updated every 5 minutes. Learn more on how to [view and disconnect current sessions.](https://docs.microsoft.com/en-us/azure/vpn-gateway/p2s-session-management)

**Customer Responsibility**

* Implementing a network disconnect for Customer-deployed resources at the end of a communication session or after a Customer-defined time period of inactivity.

**Additional Resources:**

* [Settings list for the Windows 365 Cloud PC security baseline in Intune](https://learn.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-windows-365)

SC.L2-3.13.10

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-12 | |
| **Practice:** Establish and manage cryptographic keys for cryptography employed in organizational systems.  **Assessment Objectives:**  [a] cryptographic keys are established whenever cryptography is employed; and  [b] cryptographic keys are managed whenever cryptography is employed. | |
| **Primary Services** | **Secondary Services** |
| Azure Key Vault | Bitlocker  GitHub AE  Customer Key  Microsoft Purview  GitHub Enterprise Cloud  Distributed Key Manager  Intune/Intune Suite |

**Implementation Statement:**

**Azure Key Vault**

Secure key management is essential to protect data in the cloud. Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and Microsoft processes your keys in FIPS 140-2 Level 3 validated [Thales Luna 7 HSM](https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms).

Azure Dedicated HSM is a cloud-based service that provides HSMs hosted in Azure datacenters that are directly connected to a customer's virtual network. These HSMs are dedicated [Thales Luna 7 HSM](https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms) network appliances. They are deployed directly to a customers' private IP address space and Microsoft does not have any access to the cryptographic functionality of the HSMs. Only the customer has full administrative and cryptographic control over these devices. Customers are responsible for the management of the device, and they can get full activity logs directly from their devices. Dedicated HSMs help customers meet compliance/regulatory requirements such as FIPS 140-2 Level 3, HIPAA, PCI-DSS, and eIDAS and many others.

With Key Vault, Microsoft does not see or extract your keys. Monitor and audit your key use with Azure logging—pipe logs into Azure HDInsight or your security information and event management (SIEM) solution such as Microsoft Sentinel for more analysis and threat detection. To learn more, see [Quickstart: Set and retrieve a secret from Azure Key Vault using the Azure portal](https://docs.microsoft.com/en-us/azure/key-vault/quick-create-portal).

**BitLocker, Customer Key and Distributed Key Manager (DKM)**

Microsoft 365 provides baseline, volume-level encryption enabled through BitLocker and Distributed Key Manager (DKM). Microsoft 365 offers an added layer of encryption for your content. This content includes data from Exchange Online, Skype for Business, SharePoint Online, OneDrive for Business, and Microsoft Teams.

Customer Key provides extra protection against viewing of data by unauthorized systems or personnel and complements BitLocker disk encryption in Microsoft data centers. Service encryption is not meant to prevent Microsoft personnel from accessing your data. Instead, Customer Key helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on. Customer Key is built on service encryption and lets you provide and control encryption keys. Microsoft 365 then uses these keys to encrypt your data at rest.

**GCCH**

**Customer Responsibility**

* The customer is responsible for maintaining the availability of information in the event of the loss of cryptographic keys by users. Customers have the ability to use availability keys to recover data if a customer key is lot.
* The customer is responsible for maintaining the availability of information in the event of the loss of cryptographic keys by users. Customers have the ability to use availability keys to recover data if a customer key is lot.
* Government Office 365 customers are not required to use symmetric cryptographic keys, but should they choose to, they are responsible for producing, controlling, and distributing symmetric cryptographic keys using NIST FIPS compliant key management technology and processes.

**Azure**

**Customer Responsibility**

* Managing cryptographic keys used within Customer-deployed resources in accordance with CUSTOMER-defined requirements for key generation, distribution, storage, access, and destruction.

Additional Resources:

* [Service encryption - Microsoft Purview (compliance)](https://learn.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption?view=o365-worldwide)

SC.L2-3.13.11

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-13 | |
| **Practice:** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.  **Assessment Objective:**  [a] FIPS-validated cryptography is employed to protect the confidentiality of CUI. | |
| **Primary Services** | **Secondary Services** |
| Azure Key Vault  Bitlocker | Microsoft Azure Portal  Azure Firewall  Azure Virtual Machines  Microsoft Purview  Intune/Intune Suite  Dynamics 365  Microsoft 365 Defender  Conditional Access  GitHub AE |

**Implementation Statement:**

The Federal Information Processing Standard (FIPS) Publication 140 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

Microsoft maintains an active commitment to meeting FIPS 140 requirements, having validated cryptographic modules since the standard’s inception in 2001. Microsoft certifies the cryptographic modules used in Microsoft products with each new release of the Windows operating system. For technical information on Microsoft Windows cryptographic modules, the security policy for each module, and the catalog of CMVP certificate details, see the [Windows and Windows Server FIPS 140](https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation) documentation.

Windows provides the security policy setting, *System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing*. This setting is used by some Microsoft products to determine whether to run in FIPS mode. When this policy is turned on, the validated cryptographic modules in Windows will also operate in FIPS mode. This policy may be set using Local Security Policy, as part of Group Policy, or through a Modern Device Management (MDM) solution. For more information on the policy, see [System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-cryptography-use-fips-compliant-algorithms-for-encryption-hashing-and-signing).

Through the Microsoft [Security Development Lifecycle](https://www.microsoft.com/securityengineering/sdl/) (SDL), all Azure services use FIPS 140-2 approved algorithms for data security because the operating system uses FIPS 140-2 approved algorithms while operating at a hyper scale cloud. Moreover, Azure customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM).

**Azure Key Vault**

Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and [Microsoft processes your keys in FIPS validated HSMs (hardware and firmware) - FIPS 140-2 Level 2 for vaults and FIPS 140-2 Level 3 for HSM pools.](https://docs.microsoft.com/en-us/azure/key-vault/keys/about-keys) With Key Vault, Microsoft does not see or extract your keys. Monitor and audit your key use with Azure logging—pipe logs into Azure HDInsight or your security information and event management (SIEM) solution for more analysis and threat detection.

While the current CMVP FIPS 140-2 implementation guidance precludes a FIPS 140-2 validation for a cloud service itself; cloud service providers can choose to obtain and operate FIPS 140 validated cryptographic modules for the computing elements that comprise their cloud service. Microsoft online services that include components, which have been FIPS 140-2 validated include, among others:

* [Azure and Azure Government](https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-plan-security)
* [Dynamics 365 and Dynamics 365 Government](https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365)
* [Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense](https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-risks-and-protections)
* [Federal Information Processing Standard (FIPS) 140](https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-fips-140-2)
* [Attestation documents – FIPS](https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-fips-140-2#attestation-documents)

**Microsoft Purview**

[Microsoft Purview - Data Protection Solutions](https://www.microsoft.com/en-us/security/business/microsoft-purview) provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

* [Microsoft Purview Information Protection](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-information-protection)

Discover the Microsoft Purview product family. Help keep your organization’s data safe with a range of solutions for unified data governance, information protection, risk management, and compliance. Purview Product Family:

* [Microsoft Purview Insider Risk Management](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management)
* [Microsoft Purview Communication Compliance](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-communication-compliance)
* [Microsoft Purview eDiscovery](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-ediscovery)
* [Microsoft Purview Compliance Manager](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-compliance-manager)
* [Microsoft Purview Data Lifecycle Management](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-lifecycle-management)
* [Microsoft Purview Data Loss Prevention](https://www.microsoft.com/en-us/security/business/information-protection/microsoft-purview-data-loss-prevention)
* [Microsoft Purview Audit](https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-audit)

Microsoft Purview License Requirements:

* Microsoft 365 E5 Compliance
  + [Microsoft 365 Contact Me](https://info.microsoft.com/ww-landing-microsoft-365-contact-me-contact-me.html)

Windows provides the security policy setting, *System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing*. This setting is used by some Microsoft products to determine whether to run in FIPS mode. When this policy is turned on, the validated cryptographic modules in Windows will also operate in FIPS mode. This policy may be set using Local Security Policy, as part of Group Policy, or through a Modern Device Management (MDM) solution. For more information on the policy, see [System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-cryptography-use-fips-compliant-algorithms-for-encryption-hashing-and-signing).

Through the Microsoft [Security Development Lifecycle](https://www.microsoft.com/securityengineering/sdl/) (SDL), all Azure services use FIPS 140-2 approved algorithms for data security because the operating system uses FIPS 140-2 approved algorithms while operating at a hyper scale cloud. Moreover, Azure customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM).

Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and [Microsoft processes your keys in FIPS validated HSMs (hardware and firmware) - FIPS 140-2 Level 2 for vaults and FIPS 140-2 Level 3 for HSM pools.](https://docs.microsoft.com/en-us/azure/key-vault/keys/about-keys) With Key Vault, Microsoft does not see or extract your keys. Monitor and audit your key use with Azure logging—pipe logs into Azure HDInsight or your security information and event management (SIEM) solution for more analysis and threat detection.

**GCCH**

**Customer Responsibility**

* Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliance protocols. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections.

**Additional Resources**

* [FIPS 140-2 Validation](https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation)
* [FIPS PUB 140-2](https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf)
* [Microsoft Windows FIPS 140 Validation](https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3196.pdf)

SC.L2-3.13.12

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-15 | |
| **Practice:** Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.  **Assessment Objectives:**  [a] collaborative computing devices are identified;  [b] collaborative computing devices provide indication to users of devices in use; and  [c] remote activation of collaborative computing devices is prohibited. | |
| **Primary Services** | **Secondary Services** |
|  | Intune/Intune Suite  Windows Hello for Business  Microsoft Entra ID  Teams |

**Implementation Statement:**

**Intune/Active Directory/Windows Hello**

Remote activation of collaborative computing devices can be restricted by enforcing authentication mechanisms such as, Windows Hello for Business, Intune/Intune Suite and Microsoft Entra ID. Windows Hello for Business Windows stores biometric data that is used to implement Windows Hello securely on the local device only. The biometric data does not roam and is never sent to external devices or servers. Configure Windows Hello for Business is by [Group Policy](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings) or [Intune/Intune Suite policy](https://docs.microsoft.com/en-us/mem/intune/protect/windows-hello). Because Windows Hello only stores biometric identification data on the device, there is no single collection point an attacker can compromise to steal biometric data. For more information about biometric authentication with Windows Hello for Business, see [Windows Hello biometrics in the enterprise](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise).

**Teams**

As a Teams administrator you can disable video. Teams allows the organizer and presenters to disable mic or camera of all the attendees, or of individuals, at any time during the meeting. By default, Teams provides indication when your camera or mic is in use. Users can control the use of their camera and mic in Teams as long as administrators have not restricted the devices.

**Azure**

**Customer Responsibility**

* Prohibiting remote activation for any collaborative computing devices within or controlled from customer-deployed resources and defining exceptions where remote activation is allowed (if any).

SC.L2-3.13.13

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-18 | |
| **Practice:** Control and monitor the use of mobile code.  **Assessment Objectives:**  [a] use of mobile code is controlled; and  [b] use of mobile code is monitored. | |
| **Primary Services** | **Secondary Services** |
| Azure Web Application Firewall  Microsoft Defender for Endpoint  Microsoft 365 Defender  Microsoft Sentinel | Azure Virtual Machines  Intune/Intune Suite  Conditional Access  GitHub Advanced Security (Add-On)  Microsoft Copilot for Security |

**Implementation Statement:**

Manage and control Mobile code that can run on multiple systems such as customer-developed mobile code, Java, Flash, ActiveX, PDF, Shockwave, Postscript, VBScripts via policies to allow only trusted sites. One option is to block the execution of mobile code in the browser but grant the user the liberty to allow mobile code to run. This can be accomplished via [group policy settings](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy). Granting users, the ability to allow mobile code does expose them to more threats however training users on mobile code threats can help reduce this risk. If you have plenty of IT staff, then only allowing mobile code when there is a business need is the best approach. This should be done in line with your change control procedures.

**Microsoft Defender**

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention.

Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. The solution can remediate threats such as malicious code as it scans for vulnerabilities. See [code samples](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware-code-samples) to enable and configure Microsoft Antimalware for Azure Resource Manager (ARM) virtual machines. [Learn more about Microsoft Antimalware.](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware)

**Microsoft Defender for Endpoint**

Microsoft Defender for Endpoints attack surface reduction rules all you to block content such as JavaScript or VBScript from launching downloaded executable content.

[Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune](https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection)**.** You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

**Microsoft Copilot for Security**

While Microsoft Copilot for Security does not have the ability to control and manage the types of mobile code in an organization's system. Microsoft Copilot for Security works with Microsoft Defender which can be used to analyze scripts and codes, set policy and settings management, and troubleshoot devices. The script analysis capability with Microsoft Defender provides security teams added capacity to inspect scripts without using external tools. This capability also reduces complexity of analysis, minimizing challenges and allowing security teams to quickly assess and identify a script as malicious or benign. Script analysis is also available in Copilot for Security standalone experience through the Microsoft Defender XDR plugin.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Azure Web Application Firewall**

Help protect your web apps from malicious attacks and common web vulnerabilities, such as SQL injection and cross-site scripting. Configure and enable Azure Web Application Firewall on your web application. Then, centrally define your rules and reuse them across all the web apps that you need to protect. [Learn how to customize web application firewall rules in the Azure portal](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-customize-waf-rules-portal).

**GitHub Advanced Security (Add-On)**

A GitHub Advanced Security license provides the following additional features:

* Code scanning - Search for potential security vulnerabilities and coding errors in your code. To learn more, see "About code scanning."
* Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. To learn more, see "About secret scanning."
* Dependency review - Show the full impact of changes to dependencies and see details of any vulnerable versions before you merge a pull request. To learn more, see "About dependency review."

**Customer Responsibility**

* The customer is responsible for defining acceptable and unacceptable mobile code technologies.
* The customer is responsible for establishing usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
* The customer is responsible for establishing usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

SC.L2-3.13.14

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** N/A | |
| **Practice:** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.  **Assessment Objectives:**  [a] use of Voice over Internet Protocol (VoIP) technologies is controlled; and  [b] use of Voice over Internet Protocol (VoIP) technologies is monitored. | |
| **Primary Services** | **Secondary Services** |
| Teams  Microsoft Sentinel | Microsoft Defender for IoT  Intune/Intune Suite  Conditional Access  Microsoft Entra ID |

**Implementation Statement:**

To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application. When a user of your application calls another user of your application over an internet or data connection for example via Teams, the call is made over Voice Over IP (VoIP). In this case, both signaling and media flow over the internet. You can configure and monitor usage in Teams, to learn more, see [understand calling in Microsoft Teams.](https://docs.microsoft.com/en-us/microsoftteams/tutorial-calling-in-teams)

**Microsoft Defender for IoT and Sentinel**

This monitoring encompasses all IoT devices, including VoIP technologies. Controls are enabled through integration with other services.Proactively address vulnerabilities in your IoT/OT environment, Identify risks such as unpatched devices, open ports, unauthorized applications, and unauthorized connections. Detect changes to device configurations, programmable logic controller (PLC) code, and firmware. Prioritize fixes based on risk scoring and automated threat modeling, which identifies the most likely attack paths to compromise your assets.

Further, you can get a bird's-eye view across IT/OT boundaries with interoperability with [Microsoft Sentinel](https://azure.microsoft.com/en-us/services/azure-sentinel/), cloud native SIEM/SOAR. Automate response with IoT/OT playbooks.

Sentinel now has an integrated connector for collecting Office 365 logs such as Teams. Teams serves a central role in communication and data-sharing in the Microsoft 365 Cloud. Since Teams touches on so many technologies in the Cloud, it can benefit from human and automated analysis. This applies to both hunting in logs, and real-time monitoring of meetings. Microsoft Sentinel offers admins these solutions. To learn more, see [Connect Office 365 Logs to Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365).

Combining queries from resources like Microsoft Entra ID, or other Office 365 workloads can be used with Teams queries. For example, combine the detection of suspicious patterns in Microsoft Entra ID SigninLogs, and use that output while hunting for Team Owners. Also, you can make the SigninLogs detections specific to Teams by adding a filter for only Teams-based logons. To learn more, see [Expanding your threat hunting opportunities.](https://docs.microsoft.com/en-us/microsoftteams/teams-sentinel-guide#expanding-your-threat-hunting-opportunities)

**Intune/Intune Suite**

Not only can you control Microsoft native resources, but you can also control access to resources with VoIP capabilities for third party applications such as Zoom using Intune Mobile Device Management. System administrators can use a mobile device Management (MDM) to remotely configure the Zoom app on managed devices such as iOS devices and Android. To learn more, see Using Intune to Configure Zoom on [iOS](https://support.zoom.us/hc/en-us/articles/360022302612-Using-MDM-to-configure-Zoom-on-iOS) and [Android](https://support.zoom.us/hc/en-us/articles/360031913292-Using-MDM-to-configure-Zoom-on-Android).

Additionally, you can further control access to Zoom by connecting Zoom with Azure to use your company's Azure credentials to login to your Zoom account via Single Sign-On (SSO). You can assign users Zoom licenses based on their group in Azure. To learn more, see [Configuring Zoom with Azure](https://support.zoom.us/hc/en-us/articles/115005887566-Configuring-Zoom-with-Azure).

**GCCH**

**Customer Responsibility**

* Government customers are responsible for secure use of the VoIP functions provided by SFB. SFB is default configured to enforce FIPS 140-2 compliant encryption for VoIP connection initiation on ports 5060 and 5061, and it is the responsibility of the government customer not to change these configuration settings at the client level. These settings can be enforced by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates SFB client configurations.

**Azure**

**Customer Responsibility**

* Authorizing, monitoring, and controlling the use of Voice over internet Protocol (VoiP) technologies within customer-deployed resources.

**Additional Resources**

* [Quickstart: Add voice calling to your app](https://docs.microsoft.com/en-us/azure/communication-services/quickstarts/voice-video-calling/getting-started-with-calling?pivots=platform-web)
* [Mass deployment with preconfigured settings for Windows](https://support.zoom.us/hc/en-us/articles/201362163-Mass-deployment-with-preconfigured-settings-for-Windows)

SC.L2-3.13.15

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-23 | |
| **Practice:** Protect the authenticity of communications sessions.  **Assessment Objective:**  [a] the authenticity of communications sessions is protected. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Entra ID | Azure ExpressRoute  Azure Key Vault  Load Balancer  Network Security Groups  Azure Virtual Machines  Virtual Network  VPN Gateway  Microsoft Purview  Intune/Intune Suite  Microsoft Defender for Cloud Apps  Microsoft Entra ID Multi-Factor Authentication  Teams |

**Implementation Statement:**

**Azure Portal**

Microsoft Azure Government provides the same ways to build applications and manage identities as Azure commercial. Azure Government customers may already have an Microsoft Entra ID (Microsoft Entra ID) Public tenant or may create a tenant in Microsoft Entra ID Government. [Integrating Applications with Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app)  shows how you can use Microsoft Entra ID to provide secure sign-in and authorization to your applications. This process is the same for Azure Public and Azure Government once you choose your identity authority.

**Azure Key Vault**

Authentication with Key Vault works in conjunction with [Microsoft Entra ID](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis) , which is responsible for authenticating the identity of any given security principal**.** By default, Key Vault allows access to resources through public IP addresses. For greater security, you can also restrict access to specific IP ranges, service endpoints, virtual networks, or private endpoints. To learn more, see [Access Azure Key Vault behind a firewall](https://docs.microsoft.com/en-us/azure/key-vault/general/access-behind-firewall).

**Azure ExpressRoute**

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With Azure ExpressRoute , you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365. Azure ExpressRoute connections do not go over the public Internet. This allows Azure ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using Azure ExpressRoute , see [Azure ExpressRoute connectivity models](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models).

**Azure Virtual Machines**

Improve the security of Windows virtual machines (VMs) in Azure by integrating with Microsoft Entra ID (AD) authentication. You can use Microsoft Entra ID as a core authentication platform to RDP into your VM. To use Microsoft Entra ID login in for Windows VM in Azure, you need to first [enable Microsoft Entra ID login](https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#enabling-azure-ad-login-in-for-windows-vm-in-azure) option for your Windows VM and then you need to [configure Azure role assignments](https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm) for users who are authorized to login in to the VM. You can centrally control and enforce Azure RBAC and [Conditional Access policies](https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#using-conditional-access) that allow or deny access to the VMs.

**Microsoft Entra ID Multi-Factor Authentication**

Users and groups can be enabled for Microsoft Entra ID Multi-Factor Authentication to prompt for additional verification during the sign-in event. [Security defaults](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults) are available for all Microsoft Entra ID tenants to quickly enable the use of the Microsoft Authenticator app for all users.

For more granular controls, [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) policies can be used to define events or applications that require MFA. These policies can allow regular sign-in events when the user is on the corporate network or a registered device, but prompt for additional verification factors when remote or on a personal device.

Additionally, as an administrator in Exchange Server, you can enable Secure/Multipurpose Internet Mail Extensions (S/MIME) for your organization. S/MIME is a widely accepted method (more precisely, a protocol) for sending digitally signed and encrypted messages. S/MIME allows you to encrypt emails and digitally sign them. When you use S/MIME, it helps the people who receive the message by:

* Ensuring that the message in their inbox is the exact message that started with the sender.
* Ensuring that the message came from the specific sender and not from someone pretending to be the sender.

To do this, S/MIME provides for cryptographic security services such as authentication, message integrity, and non-repudiation of origin (using digital signatures). S/MIME also helps enhance privacy and data security (using encryption) for electronic messaging.

S/MIME requires a certificate and publishing infrastructure that is often used in business-to-business and business-to-consumer situations. The user controls the cryptographic keys in S/MIME and can choose whether to use them for each message they send. Email programs such as Outlook search a trusted root certificate authority location to perform digital signing and verification of the signature.

For a more complete background about the history and architecture of S/MIME in the context of email, see [Understanding S/MIME](https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)).

**Teams**

Network communications in Teams are encrypted by default. By requiring all servers to use certificates and by using OAUTH, Transport Layer Security (TLS), and Secure Real-Time Transport Protocol (SRTP), all Teams data is protected on the network.

**GCCH**

**Customer Responsibility**

* Government customers are responsible for having a process in place to check the validity of the Office 365 Web sites prior to signing on by reviewing the digital certificate on the site to ensure they are the Office 365 Web sites. If government customers are using CIS or STIG baselines, supported web browsers will enforce this review automatically by default and prevent connections if the digital certificate is invalid.

**Azure**

**Customer Responsibility**

* Protecting the authenticity of communications sessions involving customer-deployed resources.

**Additional Resources**

* [Public Key Infrastructure](https://docs.microsoft.com/en-us/windows/win32/seccertenroll/public-key-infrastructure)
* [How it works: Microsoft Entra ID Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks)
* [Azure network security overview](https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview)
* [Message Encryption](https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide)

SC.L2-3.13.16

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SC-28 | |
| **Practice:** Protect the confidentiality of CUI at rest.  **Assessment Objective:**  [a] the confidentiality of CUI at rest is protected. | |
| **Primary Services** | **Secondary Services** |
| Azure Key Vault  Bitlocker | Log Analytics Workspace  Microsoft Sentinel  Azure Virtual Machines  Microsoft Purview  Intune/Intune Suite  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft Defender for Office 365  Distributed Key Manager  Customer Key |

**Implementation Statement:**

**Azure Key Vault**

The storage location of the encryption keys and access control to those keys is central to an encryption at rest model. The keys need to be highly secured but manageable by specified users and available to specific services. For Azure services, [Azure Key Vault](https://azure.microsoft.com/en-us/services/key-vault/) is the recommended key storage solution and provides a common management experience across services. Keys are stored and managed in key vaults, and access to a key vault can be given to users or services. Azure Key Vault supports [customer creation of keys](https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=portal#configure-encryption-with-customer-managed-keys) or [import of customer keys](https://docs.microsoft.com/en-us/rest/api/keyvault/importkey/importkey#:~:text=Import%20Key%20%2D%20Import%20Key,-Service%3A%20Key%20Vault&text=Imports%20an%20externally%20created%20key,new%20version%20of%20the%20key.) for use in customer-managed encryption key scenarios. Permissions to use the keys stored in Azure Key Vault, either to manage or to access them for Encryption at Rest encryption and decryption, can be given to Microsoft Entra ID accounts.

Software as a Service (SaaS) customers typically have encryption at rest enabled or available in each service. Microsoft 365 has several options for customers to verify or enable encryption at rest. For information about Microsoft 365 services, see [Encryption in Microsoft 365](https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption).

Platform as a Service (PaaS) customer's data typically resides in a storage service such as Blob Storage but may also be cached or stored in the application execution environment, such as a virtual machine. To see the encryption at rest options available to you, examine the [Data encryption models: supporting services table](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-models#supporting-services) for the storage and application platforms that you use.

Like PaaS, IaaS solutions can leverage other Azure services that store data encrypted at rest. In these cases, you can enable the Encryption at Rest support as provided by each consumed Azure service. The [Data encryption models: supporting services table](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-models#supporting-services) enumerates the major storage, services, and application platforms and the model of Encryption at Rest supported.

Any customer using Azure Infrastructure as a Service (IaaS) features can achieve encryption at rest for their IaaS VMs and disks through Azure Disk Encryption. For more information on Azure Disk encryption, see the [Azure Disk Encryption documentation](https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss). Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the [BitLocker](https://en.wikipedia.org/wiki/BitLocker) feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/) to help you control and manage the disk encryption keys and secrets.

**BitLocker, Customer Key and Distributed Key Manager (DKM)**

Microsoft 365 provides baseline, volume-level encryption enabled through BitLocker and Distributed Key Manager (DKM). Microsoft 365 offers an added layer of encryption for your content. This content includes data from Exchange Online, Skype for Business, SharePoint Online, OneDrive for Business, and Microsoft Teams.

Customer Key provides extra protection against viewing of data by unauthorized systems or personnel and complements BitLocker disk encryption in Microsoft data centers. Service encryption is not meant to prevent Microsoft personnel from accessing your data. Instead, Customer Key helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on. Customer Key is built on service encryption and lets you provide and control encryption keys. Microsoft 365 then uses these keys to encrypt your data at rest.

**Intune/Intune Suite**

Use Intune to configure encryption at rest using BitLocker Drive Encryption on devices that run Windows 10. Some settings for BitLocker require the device to have a supported TPM. To manage BitLocker in Intune, your account must have the applicable Intune [role-based access control](https://docs.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control) (RBAC) permissions. For more information on how to enforce BitLocker encryption using Intune, see [Create and deploy policy](https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#create-and-deploy-policy).

Intune can also manage macOS FileVault disk encryption. FileVault is a whole-disk encryption program that is included with macOS. You can use Intune to configure FileVault on devices that run macOS 10.13 or later**.** For more information on how to enforce FileVault encryption using Intune, see[Create device configuration policy for FileVault](https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices-filevault#create-device-configuration-policy-for-filevault)

Additionally, [Intune/Intune Suite](https://docs.microsoft.com/en-us/mem/endpoint-manager-overview)  integrates with [Compliance Retrieval/NAC 2.0](https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate)  to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using Compliance Retrieval/NAC 2.0 with [Conditional Access and Intune](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use) you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

**Transparent Data Encryption (TDE)**

You can use Transparent Data Encryption (TDE) to encrypt SQL Server and Azure SQL Database data files at rest. With TDE you can encrypt the sensitive data in the database and protect the keys that are used to encrypt the data with a certificate. TDE performs real-time I/O encryption and decryption of the data and log files to protect data at rest. TDE can assist in the ability to comply with many laws, regulations, and guidelines established in various industries. If a malicious party would be able to steal your data files, they still would not be able to use them at all because they would need the keys as well. For more information about TDE, see [Transparent Data Encryption (TDE)](https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption).

[**Azure Policies**](#_Azure_Policy)

* [**SC.L2-3.13.16 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#protect-the-confidentiality-of-cui-at-rest)

**Customer Responsibility**

* Protecting customer-controlled information at rest.

**Additional Resources**

* [Encryption in Azure Backup](https://docs.microsoft.com/en-us/azure/backup/backup-encryption)
* [Federal Information Processing Standard (FIPS) 140](https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-fips-140-2)

### System and Information Integrity (SI)

SI.L1-3.14.1

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SI-2, SI-3, SI-5 | |
| **Practice:** Identify, report and correct information and information system flaws in a timely manner.  **Assessment Objectives:**  [a] the time within which to identify system flaws is specified;  [b] system flaws are identified within the specified time frame;  [c] the time within which to report system flaws is specified;  [d] system flaws are reported within the specified time frame;  [e] the time within which to correct system flaws is specified; and  [f] system flaws are corrected within the specified time frame. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel | Intune/Intune Suite  Microsoft Defender for Endpoint  Microsoft Defender for Cloud  Microsoft Copilot for Security  Microsoft 365 Defender  Power Automate  Azure Automation |

**Implementation Statement:**

**Microsoft Sentinel**

You can use [Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports), [Microsoft Endpoint Configuration Manager](https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/endpoint-protection), the [Update Compliance add-in](https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started#add-update-compliance-to-your-azure-subscription) for Microsoft Operations Management Suite, or Microsoft Sentinel SIEM (by consuming Windows event logs) to monitor protection status and create reports about endpoint protection.

Review usage reports for Microsoft Entra ID in the Azure portal to determine suspicious activity, including the [possibly of infected devices](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-sign-ins-from-possibly-infected-devices) report. Configure Microsoft Defender for Endpoint to report on [Microsoft Defender Antivirus events](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide) and connect your resources such as the Microsoft Defender for Endpoint connector to Microsoft Sentinel SIEM tool to have a centralized location for security alerts and advisories. [Connect data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to [visualize and monitor](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data) your data in Sentinel.

Additionally, you can use the Microsoft Defender for Cloud Apps alert connector to ingest Microsoft Defender for Cloud Apps alerts from [Microsoft Defender for Cloud Apps](https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction) and stream them into Microsoft Sentinel. Microsoft Sentinel allows you to [create custom workbooks](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data#create-new-workbook) across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

The vulnerability scanner included with Microsoft Defender for Cloud is powered by Qualys. Qualys' scanner is one of the leading tools for real-time identification of vulnerabilities. It is only available with [Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction). You do not need a Qualys license or even a Qualys account - everything is handled seamlessly inside Security Center. Moreover, the systems can also be onboarded to Microsoft Defender for Endpoint to gain similar Threat & Vulnerability Management visibility.

**Microsoft Defender for Endpoint**

Microsoft Defender for Endpoint provides endpoint protection, detection and response, vulnerability managements and mobile threat defense. [Vulnerability management](https://www.microsoft.com/en-us/security/business/threat-protection/threat-vulnerability-management) allows you to quickly discover, prioritize, and remediate vulnerabilities and misconfigurations. To support this CMMC Control , consider the following Microsoft Defender for Endpoint configurations:

* [Enable cloud-delivered protection](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus?view=o365-worldwide). You can enable cloud-delivered protection with Microsoft Endpoint Configuration Manager, Group Policy, Microsoft Intune, and PowerShell cmdlets.
* [Specify the cloud-delivered protection level](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/specify-cloud-protection-level-microsoft-defender-antivirus?view=o365-worldwide). You can specify the level of protection offered by the cloud with Group Policy and Microsoft Endpoint Configuration Manager. The protection level will affect the amount of information shared with the cloud and how aggressively new files are blocked.
* [Configure and validate network connections for Microsoft Defender Antivirus](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-network-connections-microsoft-defender-antivirus?view=o365-worldwide). There are certain Microsoft URLs that your network and endpoints must be able to connect to for cloud-delivered protection to work effectively. This article lists the URLs that should be allowed via firewall or network filtering rules, and instructions for confirming your network is properly enrolled in cloud-delivered protection.
* [Configure the block at first sight feature](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-block-at-first-sight-microsoft-defender-antivirus?view=o365-worldwide). The "block at first sight" feature can block new malware within seconds, without having to wait hours for traditional Security intelligence. You can enable and configure it with Microsoft Endpoint Manager and Group Policy.
* [Configure the cloud block timeout period](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-cloud-block-timeout-period-microsoft-defender-antivirus?view=o365-worldwide). Microsoft Defender Antivirus can block suspicious files from running while it queries our cloud-delivered protection service. You can configure the amount of time the file will be prevented from running with Microsoft Endpoint Manager and Group Policy.

**Microsoft Copilot for Security**

Microsoft Copilot for Security can access data from Microsoft Sentinel to increase the effectiveness and efficiency of security professionals using those solutions. Microsoft Defender XDR and Microsoft Sentinel become even more powerful when security professionals use Copilot for Security. Copilot for Security delivers an experience that enriches and builds on the security data, signals, and existing incidents and insights sourced from Microsoft Defender XDR and Microsoft Sentinel.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Power Automate**

Environment admins can access analytics for Power Automate in the Microsoft Power Platform admin center. The reports provide insights into runs, usage, errors, types of flows created, shared flows, and details on connectors associated with all the different flow types like automated flows, button flows, scheduled flows, approval flows, business process flows.

[**Azure Policies**](#_Azure_Policy)

* [**SC.L1-3.14.1 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#identify-report-and-correct-system-flaws-in-a-timely-manner)

**GCCH**

**Customer Responsibility**

* Government customers and non-government customers are responsible for centrally managing the flaw remediation process (e.g., planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls).
* Government customers are required to employ automated mechanisms to determine the state of information system components with regard to flaw remediation on their information systems as required by their organization’s security policy.

**Azure**

**Customer Responsibility**

* Flaw remediation on customer-deployed resources, including the identification, reporting, and correction of flaws.

**Additional Resources**

* [Manage updates for mobile devices and virtual machines (VMs)](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-mobile-devices-vms-microsoft-defender-antivirus?view=o365-worldwide)
* [Create interactive reports with Azure Monitor Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview).
* [Automatically remediate Azure VM alerts with Automation runbooks](https://azure.microsoft.com/en-gb/blog/automatically-remediate-azure-vm-alerts-with-automation-runbooks/)

SI.L1-3.14.2

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SI-2, SI-3, SI-5 | |
| **Practice:** Provide protection from malicious code at appropriate locations within organizational information systems.  **Assessment Objectives:**  [a] designated locations for malicious code protection are identified; and  [b] protection from malicious code at designated locations is provided. | |
| **Primary Services** | **Secondary Services** |
| Azure Web Application Firewall  App Locker | Azure DNS  Azure Virtual Machines  Microsoft Defender for Office 365  Microsoft Defender Smartscreen  Microsoft Defender for Cloud Apps  Microsoft Defender for Cloud  Microsoft Defender for Endpoint  Intune/Intune Suite  Microsoft 365 Defender |

**Implementation Statement:**

**Microsoft Antimalware for Azure and Microsoft Defender for Cloud**

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention.

Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. The solution can remediate threats such as malicious code as it scans for vulnerabilities. See [code samples](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware-code-samples) to enable and configure Microsoft Antimalware for Azure Resource Manager (ARM) virtual machines. [Learn more about Microsoft Antimalware.](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware)

Additionally, Microsoft Defender for Cloud monitors the status of antimalware protection and reports this under the Endpoint protection issues blade. Security Center highlights issues, such as detected threats and insufficient protection, which can make your virtual machines (VMs) and computers vulnerable to antimalware threats. By using the information under Endpoint protection issues, you can identify a plan to address any issues identified. To learn more about the features of Microsoft Defender for Cloud, see [Feature coverage for machines](https://docs.microsoft.com/en-us/azure/security-center/security-center-services?tabs=features-windows).

**Intune and Microsoft Defender for Endpoint**

Intune can integrate data from a Mobile Threat Defense (MTD) vendor as an information source for device compliance policies and device Conditional Access rules. You can use this information to help protect corporate resources like Exchange and SharePoint, by blocking access from compromised mobile devices. [Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune](https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection).You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Microsoft Defender for Endpoint works with devices that run Android, iOS/iPadOS and Windows 10 or later. When you integrate Intune with Microsoft Defender for Endpoint, you can take advantage of Microsoft Defender for Endpoints Threat & Vulnerability Management (TVM) and [use Intune to remediate endpoint weakness identified by TVM](https://docs.microsoft.com/en-us/mem/intune/protect/atp-manage-vulnerabilities). Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Additionally, turn tamper protection on (or off) for all or part of your organization using Intune Fine-tune tamper protection settings in your organization. [Manage tamper protection for your organization using Intune](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection?view=o365-worldwide#manage-tamper-protection-for-your-organization-using-intune). Bad actors like to disable your security features to get easier access to your data, to install malware, or to otherwise exploit your data, identity, and devices. Tamper protection helps prevent these kinds of things from occurring.

With tamper protection, malicious apps are prevented from taking actions such as:

* Disabling virus and threat protection
* Disabling real-time protection
* Turning off behavior monitoring
* Disabling antivirus (such as IOfficeAntivirus (IOAV))
* Disabling cloud-delivered protection
* Removing security intelligence updates

**Azure Web Application Firewall**

Help protect your web apps from malicious attacks and common web vulnerabilities, such as SQL injection and cross-site scripting. Configure and enable Azure Web Application Firewall on your web application. Then, centrally define your rules and reuse them across all the web apps that you need to protect. [Learn how to customize web application firewall rules in the Azure portal](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-customize-waf-rules-portal).

**App Locker**

When a user runs a process, that process has the same level of access to data that the user has. As a result, sensitive information could easily be deleted or transmitted out of the organization if a user knowingly or unknowingly runs malicious software. AppLocker can help mitigate these types of security breaches by restricting the files that users or groups are allowed to run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers

[**Azure Policies**](#_Azure_Policy)

* [**SC.L1-3.14.2 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#provide-protection-from-malicious-code-at-designated-locations-within-organizational-systems)

**GCCH**

**Customer Responsibility**

* Government customers are responsible for ensuring that customer users are using information systems running anti-malware software to access Office 365.

**Azure**

**Customer Responsibility**

* Protecting customer-deployed resources against malicious code by using code protection mechanisms at entry and exit points to detect and eradicate malicious code (e.g., viruses, malware, rootkits, worms, and scripts).

**Additional Resources**

* [Endpoint protection assessment and recommendations in Microsoft Defender for Cloud Apps](https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection)
* [Enable and configure Microsoft Antimalware for Azure Resource Manager VMs](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware-code-samples#enable-and-configure-microsoft-antimalware-for-azure-resource-manager-vms)

SI.L2-3.14.3

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SI-2, SI-3, SI-5 | |
| **Practice:** Monitor system security alerts and advisories and take action in response.  **Assessment Objectives:**  [a] response actions to system security alerts and advisories are identified;  [b] system security alerts and advisories are monitored; and  [c] actions in response to system security alerts and advisories are taken. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel  Microsoft Entra ID  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft Defender for Cloud  Microsoft 365 Defender  Microsoft Defender for IoT |  |

**Implementation Statement:**

**Defender**

Microsoft Defender for Endpoint provides endpoint protection, detection and response, vulnerability management and mobile threat defense. It identifies and can report on advisories specific to each device monitored. You can use Microsoft Endpoint Manager to [monitor Microsoft Defender Antivirus](https://docs.microsoft.com/en-us/configmgr/protect/deploy-use/monitor-endpoint-protection) or [create email alerts](https://docs.microsoft.com/en-us/configmgr/protect/deploy-use/endpoint-configure-alerts). Or you can monitor protection using [Microsoft Intune](https://docs.microsoft.com/en-us/intune/introduction-intune). [Vulnerability management](https://www.microsoft.com/en-us/security/business/threat-protection/threat-vulnerability-management) allows you to quickly discover, prioritize, and remediate vulnerabilities and misconfigurations.

Microsoft Defender for IoT is a unified security solution for identifying IoT/OT devices, vulnerabilities, and threats. It identifies and can report on advisories specific to each device monitored. Go to [Microsoft Defender for Cloud](https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/0) to turn on protection for your hybrid cloud workloads.

**Microsoft Sentinel connector** can stream security alerts from Microsoft Defender for Cloud Apps into Microsoft Sentinel. [Learn more about connecting Microsoft Defender for Cloud Apps with Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center). Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Review usage reports for Microsoft Entra ID in the Azure portal to determine suspicious activity, including the [possibly of infected devices](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-sign-ins-from-possibly-infected-devices) report. Configure Microsoft Defender for Endpoint to report on [Microsoft Defender Antivirus events](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide) and connect your resources such as the Microsoft Defender for Endpoint connector to Microsoft Sentinel SIEM tool to have a centralized location for security alerts and advisories. [Connect data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) to [visualize and monitor](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data) your data in Sentinel.

Additionally, Microsoft Sentinel allows you to [import threat indicators](https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence) to enhance your organization’s ability to detect and respond to known threats. Microsoft Sentinel allows you to [create custom workbooks](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data#create-new-workbook) across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

**Customer Responsibility**

* Receiving security alerts, advisories, and directives from customer-defined external organizations on an ongoing basis.

**Additional Resources**

* The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services and provides the information [here](https://msrc.microsoft.com/update-guide) as part of the ongoing effort to help you manage security risks and help keep your systems protected.
* [Alerts and Sensor Reporting](https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-work-with-alerts-on-your-sensor#alerts-and-sensor-reporting)
* [Connect your data from Defender for IoT to](https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-configure-with-sentinel) Microsoft Sentinel

SI.L1-3.14.4

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SI-3 | |
| **Practice:** Update malicious code protection mechanisms when new releases are available.  **Assessment Objective:**  [a] malicious code protection mechanisms are updated when new releases are available. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Defender for Endpoint  Microsoft Defender for Office 365  Microsoft Defender for Cloud Apps  Microsoft Defender for Cloud  Microsoft 365 Defender  Azure Automation | Intune/Intune Suite  Azure Virtual Machines |

**Implementation Statement:**

**Azure Automation**

You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines in Azure, physical or VMs in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management.

**Microsoft Defender/Microsoft Antimalware**

Keeping Microsoft Defender Antivirus up to date is critical to ensure your devices have the latest technology and features needed to protect against new malware and attack techniques. Make sure to update your antivirus protection even if Microsoft Defender Antivirus is running in [passive mode](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-compatibility?view=o365-worldwide). To see the most current engine, platform, and signature date, visit the [Security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware](https://www.microsoft.com/en-us/wdsi/defenderupdates).

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. Microsoft Antimalware automatically updates malicious code signatures and includes the features below. When you deploy and enable Microsoft Antimalware for Azure for your applications, the following core features are available:

* **Real-time protection**: monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution.
* **Scheduled scanning**: Scans periodically to detect malware, including actively running programs.
* Malware remediation – automatically acts on detected malware, such as deleting or quarantining malicious files and cleaning up malicious registry entries.
* **Signature updates**: automatically installs the latest protection signatures (virus definitions) to ensure protection is up to date on a pre-determined frequency.
* **Antimalware Engine updates**: automatically updates the Microsoft Antimalware engine.
* **Antimalware Platform updates**: automatically updates the Microsoft Antimalware platform.
* **Active protection**: reports telemetry metadata about detected threats and suspicious resources to Microsoft Azure to ensure rapid response to the evolving threat landscape, as well as enabling real-time synchronous signature delivery through the Microsoft Active Protection System (MAPS).
* **Samples reporting**: provides and reports samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting.
* **Exclusions**: allows application and service administrators to configure exclusions for files, processes, and drives.
* **Antimalware event collection**: records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log and collects them into the customer’s Azure Storage account.

You can find information on default configuration settings and more here: [Microsoft Antimalware for Azure Cloud Services and Virtual Machines](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware).

**Intune/Intune Suite**

If you use an unsupported version of Window 10, your users will not get the latest security updates, new features, bug fixes, latency improvements, accessibility improvements, and performance investments. The user will not be able to be co-managed with System Center Configuration Manager and Intune. Intune follows Windows 10 lifecycle for supported Windows 10 versions. In the Microsoft Endpoint Manager admin center, use the [Discovered apps](https://docs.microsoft.com/en-us/mem/intune/apps/app-discovered-apps) feature to find apps with these versions. On a user’s device, the Company Portal version is shown in the settings page of the company portal. Update to a supported Windows/Company Portal version.

Learn what is new each week in Microsoft Intune in [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). You can also find [important notices](https://docs.microsoft.com/en-us/mem/intune/fundamentals/whats-new#notices), [past releases](https://docs.microsoft.com/en-us/mem/intune/fundamentals/whats-new-archive), and information about [how Intune service updates are released](https://techcommunity.microsoft.com/t5/Intune-Customer-Success/Microsoft-Intune-Service-Updates/ba-p/358728).

Turn tamper protection on (or off) for all or part of your organization using Intune Fine-tune tamper protection settings in your organization. [Manage tamper protection for your organization using Intune](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection?view=o365-worldwide#manage-tamper-protection-for-your-organization-using-intune). Bad actors like to disable your security features to get easier access to your data, to install malware, or to otherwise exploit your data, identity, and devices. Tamper protection helps prevent these kinds of things from occurring.

With tamper protection, malicious apps are prevented from taking actions such as:

* Disabling virus and threat protection
* Disabling real-time protection
* Turning off behavior monitoring
* Disabling antivirus (such as IOfficeAntivirus (IOAV))
* Disabling cloud-delivered protection
* Removing security intelligence updates

**Azure Virtual Machines**

Software updates in Azure Automation Update Management provides a set of tools and resources that can help manage the complex task of tracking and applying software updates to machines in Azure and hybrid cloud. An effective software update management process is necessary to maintain operational efficiency, overcome security issues, and reduce the risks of increased cyber security threats. Update Management supports the deployment of first-party updates and the pre-downloading of them. This support requires changes on the systems being updated. See [Configure Windows Update settings for Azure Automation Update Management](https://docs.microsoft.com/en-us/azure/automation/update-management/configure-wuagent) to learn how to configure these settings on your systems.

Before attempting to manage updates for your VMs, ensure that you have enabled Update Management on them using one of these methods:

* [Enable Update Management from an Automation account](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-automation-account)
* [Enable Update Management by browsing the Azure portal](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-portal)
* [Enable Update Management from a runbook](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-runbook)
* [Enable Update Management from an Azure VM](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-vm)

**GCCH**

**Customer Responsibility**

* Government customers are responsible for ensuring that customer users are using information systems running anti-malware software to access Office 365.

**Azure**

**Customer Responsibility**

* Updating malicious code protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures

**Additional Resources**

* [Expedite Windows 10 quality updates in Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-expedite-updates)

SI.L1-3.14.5

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SI-3 | |
| **Practice:** Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.  **Assessment Objectives:**  [a] the frequency for malicious code scans is defined;  [b] malicious code scans are performed with the defined frequency; and  [c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Defender for Endpoint  Microsoft Defender for Office 365  Microsoft Defender SmartScreen  Microsoft Defender for Cloud Apps  Microsoft Defender for Cloud  Intune/Intune Suite | Microsoft 365 Defender |

**Implementation Statement:**

**Microsoft Defender/Microsoft Antimalware**

Microsoft Antimalware for Azure provides protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention.

Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. The solution can remediate threats such as malicious code as it scans for vulnerabilities. See [code samples](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware-code-samples) to enable and configure Microsoft Antimalware for Azure Resource Manager (ARM) virtual machines. [Learn more about Microsoft Antimalware.](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware)

[Enable and configure Microsoft Defender Antivirus always-on protection in Group Policy](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-real-time-protection-microsoft-defender-antivirus?view=o365-worldwide" \l "enable-and-configure-always-on-protection-in-group-policy). Always-on protection consists of real-time protection, behavior monitoring, and heuristics to identify malware based on known suspicious and malicious activities. The feature allows you to scan all downloaded files and attachments automatically. Downloaded files and attachments are automatically scanned. This operates in addition to the Windows Defender SmartScreen filter, which scans files before and during downloading.

**Windows Defender SmartScreen**

When you use the new Microsoft Edge , Microsoft Defender SmartScreen helps you identify reported phishing and malware websites and also helps you make informed decisions about downloads. SmartScreen helps protect you in three ways:

* As you browse the web, it analyzes pages and determines if they might be suspicious. If it finds suspicious pages, SmartScreen will display a warning page, giving you an opportunity to provide feedback and advising you to continue with caution.
* SmartScreen checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen will show you a warning letting you know that the site has been blocked for your safety.
* SmartScreen checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen will warn you that the download has been blocked for your safety. SmartScreen also checks the files that you download against a list of files that are well known and downloaded by many people who use Internet Explorer. If the file that you are downloading isn't on that list, SmartScreen will warn you.

**Intune/Intune Suite**

Use the Endpoint security node in Intune to configure device security and to manage security tasks for devices when those devices are at risk. The Endpoint security policies are designed to help you focus on the security of your devices and mitigate risk. The available tasks can help you identify at-risk devices, to remediate those devices, and restore them to a compliant or more secure state. Deploy security baselines that establish best practice security configurations for devices. Intune includes [security baselines](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security#manage-security-baselines) for Windows devices and a growing list of applications, like Microsoft Defender for Endpoint and Microsoft Edge. Security baselines are pre-configured groups of Windows settings that help you apply a configuration that is recommended by the relevant security teams .

Intune allows you to perform a [Quick Scan](https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10) – This will have Defender run a quick scan of the device for malware and then submit the results to Intune. A quick scan looks at common locations where there could be malware registered, such as registry keys and known Windows startup folders.

Additionally, you can run a [Full scan](https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10) – Having Defender run a scan of the device for malware and then submit the results to Intune. A full scan looks at common locations where there could be malware registered, and also scans every file and folder on the device.

**GCCH**

**Customer Responsibility**

* Government customers are responsible for ensuring that customer users are using information systems running anti-malware software to access Office 365.

**Azure**

**Customer Responsibility**

* Protecting customer-deployed resources against malicious code by configuring mechanisms to: perform periodic scans at a customer-defined frequency and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; block malicious code, quarantine malicious code, and/or send an alert to an administrator; and take any customer-defined action(s) in response to malicious code detection.

**Additional Resources:**

* [What happened to SCCM?](https://learn.microsoft.com/en-us/mem/configmgr/core/understand/what-happened-to-sccm)
* [Configuration Manager console - Configuration Manager](https://learn.microsoft.com/en-us/mem/configmgr/core/servers/manage/admin-console)

SI.L2-3.14.6

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** AU-2, AU-6, SI-4, SI-4(4) | |
| **Practice:** Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.  **Assessment Objectives:**  [a] the system is monitored to detect attacks and indicators of potential attacks;  [b] inbound communications traffic is monitored to detect attacks and indicators of  potential attacks; and  [c] outbound communications traffic is monitored to detect attacks and indicators of  potential attacks. | |
| **Primary Services** | **Secondary Services** |
| Azure Firewall  Microsoft Sentinel | Azure DNS  Network Security Groups  Azure Web Application Firewall  Virtual Network  Conditional Access  Microsoft Defender for Endpoint  Microsoft Defender for Office 365  Microsoft Defender for Cloud Apps  Microsoft Defender for IoT  Microsoft Defender for Identity  Microsoft Copilot for Security  Azure Monitor  Log Analytics |

**Implementation Statement:**

**Microsoft Defender for IoT**

Control what traffic is being monitored using Microsoft Defender for IoT sensors. Sensors automatically perform deep packet detection for IT and OT traffic and resolve information about network devices, such as device attributes and behavior. You onboard a sensor by registering it with Microsoft Defender for IoT and downloading a sensor activation file. Learn more on how to [Onboard, view, and manage](https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-manage-sensors-on-the-cloud#onboard-sensors) sensors in the [Defender for IoT portal](https://portal.azure.com/#blade/Microsoft_Azure_IoT_Defender/IoTDefenderDashboard/Getting_Started). Learning and Smart IT Learning modes instructs your sensor to learn your network’s usual activity. This activity becomes your baseline.

When Smart IT Learning is enabled, the sensor tracks network traffic that generates nondeterministic IT behavior based on specific alert scenarios. Working with Smart IT Learning helps you reduce the number of unnecessary alerts and notifications caused by noisy IT scenarios. Microsoft recommends to enable all [security detection engines](https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-control-what-traffic-is-monitored#detection-engines). Self-learning analytics engines eliminate the need for updating signatures or defining rules. The engines use ICS-specific behavioral analytics and data science to continuously analyze OT network traffic for anomalies, malware, operational problems, protocol violations, and baseline network activity deviations.

Additionally, to enhance device enrichment, you can [configure multiple DNS servers](https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-control-what-traffic-is-monitored#configure-dns-servers-for-reverse-lookup-resolution) to carryout reverse lookups. You can resolve host names or FQDNs associated with the IP addresses detected in network subnets. For example, if a sensor discovers an IP address, it might query multiple DNS servers to resolve the host name.

**Microsoft Defender for Identity**

Microsoft Defender for Identity (formerly Microsoft Entra ID advanced Threat Protection, also known as Azure ATP) monitors your domain controllers by capturing and parsing network traffic and leveraging Windows events directly from your domain controllers, then analyzes the data for attacks and threats. Utilizing profiling, deterministic detection, machine learning, and behavioral algorithms Defender for Identity learns about your network, enables detection of anomalies, and warns you of suspicious activities. Installed directly on your domain controller or AD FS servers, the Defender for Identity sensor accesses the event logs it requires directly from the servers. After the logs and network traffic are parsed by the sensor, Defender for Identity sends only the parsed information to the Defender for Identity cloud service (only a percentage of the logs are sent). To learn more, see [Microsoft Defender for Identity Architecture.](https://docs.microsoft.com/en-us/defender-for-identity/architecture)

**Microsoft Defender for Cloud Apps**

[Integrating Cloud App Security with Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/cloud-app-security/mde-integration) gives you the ability to use Cloud Discovery beyond your corporate network or secure web gateways. With the combined user and device information, you can identify risky users or devices, see what apps they are using, and investigate further in the Defender for Endpoint portal. Cloud Discovery analyzes traffic logs collected by Defender for Endpoint and assesses identified apps against the cloud app catalog to provide compliance and security information. By configuring Cloud Discovery, you gain visibility into cloud use, Shadow IT, and continuous monitoring of the unsanctioned apps being used by your users. [Set up Cloud Discovery](https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery).

**Microsoft Sentinel**

[Connect your sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) such as Microsoft Defender for Endpoint to Sentinel for monitoring your organization. Enable [Fusion technology based on machine learning](https://docs.microsoft.com/en-us/azure/sentinel/fusion), allowing Microsoft Sentinel to automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities that are observed at various stages of the kill-chain. Based on these discoveries, Microsoft Sentinel generates incidents that would otherwise be difficult to catch. fusion incidents can indicate

Customized for your environment, this detection technology not only reduces [false positive](https://docs.microsoft.com/en-us/azure/sentinel/false-positives) rates but can also detect attacks with limited or missing information.

**Microsoft Copilot for Security**

Microsoft Copilot for Security can access data from Microsoft Sentinel to increase the effectiveness and efficiency of security professionals using those solutions. Microsoft Defender XDR and Microsoft Sentinel become even more powerful when security professionals use Copilot for Security. Copilot for Security delivers an experience that enriches and builds on the security data, signals, and existing incidents and insights sourced from Microsoft Defender XDR and Microsoft Sentinel.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Virtual Network/Azure Firewall**

To secure Azure application workloads, you use protective measures like authentication and encryption in the applications themselves. You can also add security layers to the virtual machine (VM) networks that host the applications, both to protect inbound flows from users, as well as outbound flows to the Internet that your application might require. This article describes [Azure Virtual Network](https://azure.microsoft.com/services/virtual-network/) security services like Azure Firewall and Azure Application Gateway, when to use each service, and network design options that combine both.

[Azure Firewall](https://docs.microsoft.com/en-us/azure/firewall/overview) is a managed next-generation firewall that offers [network address translation (NAT)](https://docs.microsoft.com/en-us/azure/virtual-network/nat-overview). Azure Firewall bases packet filtering on Internet Protocol (IP) addresses and Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ports, or on application-based HTTP(S) or SQL attributes. Azure Firewall also leverages Microsoft threat intelligence to identify malicious IP addresses. [Azure Firewall Premium](https://docs.microsoft.com/en-us/azure/firewall/premium-features) includes all functionality of Azure Firewall Standard plus additional features such as TLS-inspection and IDPS (Intrusion Detection and Protection System) To learn more, see the [Azure Firewall documentation](https://docs.microsoft.com/en-us/azure/firewall/).

[Azure Application Gateway](https://docs.microsoft.com/en-us/azure/application-gateway/overview) is a managed web traffic load balancer and HTTP(S) full reverse proxy that can do Secure Socket Layer (SSL) encryption and decryption. Application Gateway also uses Web Application Firewall to inspect web traffic and detect attacks at the HTTP layer. To learn more, see the [Application Gateway documentation](https://docs.microsoft.com/en-us/azure/application-gateway/).

[Azure Web Application Firewall (WAF)](https://azure.microsoft.com/services/web-application-firewall/) is an optional addition to Azure Application Gateway to provide inspection of HTTP request and prevent malicious attacks at the web layer such as SQL Injection or Cross-Site Scripting. To learn more, see the [Web Application Firewall documentation](https://docs.microsoft.com/en-us/azure/web-application-firewall/).

[**Azure Policies**](#_Azure_Policy)

* [**SC.L2-3.14.6 Azure Policies**](https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-171-r2#monitor-organizational-systems-including-inbound-and-outbound-communications-traffic-to-detect-attacks-and-indicators-of-potential-attacks)

**GCCH**

**Customer Responsibility**

* Government customers are responsible for analyzing communications traffic anomalies for customer-deployed resources, including an analysis of outbound communications traffic at the external boundary and at customer-defined interior points within the system to discover anomalies.

**Azure**

**Customer Responsibility**

* Monitoring customer-deployed resources to detect attacks and indicators of potential attacks in accordance with customer-defined monitoring objectives; and unauthorized local, network, and remote connections.
* Monitoring customer-deployed resources, including the monitoring of inbound and outbound communications traffic at the customer-defined frequency, for unusual or unauthorized activities/conditions.

**Additional Resources**

* [Best practices for configuring Windows Defender Firewall](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring)
* [Checklist: Creating Outbound Firewall Rules](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/checklist-creating-outbound-firewall-rules).
* [Checklist: Creating Inbound Firewall Rules](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/checklist-creating-inbound-firewall-rules).
* [Isolating Microsoft Store Apps on Your Network](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/isolating-apps-on-your-network)
* [Discover and manage shadow IT in your network](https://docs.microsoft.com/en-us/cloud-app-security/tutorial-shadow-it)

SI.L2-3.14.7

| **Control Summary Information** | |
| --- | --- |
| **NIST SP 800-53 Mapping:** SI-4 | |
| **Practice:** Identify unauthorized use of organizational systems.  **Assessment Objectives:**  [a] authorized use of the system is defined; and  [b] unauthorized use of the system is identified. | |
| **Primary Services** | **Secondary Services** |
| Microsoft Sentinel | Microsoft Entra ID  Azure Bastion  Azure Firewall  Azure Monitor  Azure Virtual Machines  Load Balancer  Network Security Groups  VPN Gateway  Privileged Identity Management (PIM)  Microsoft Defender for Office 365  Microsoft Defender for Cloud  Microsoft Defender for Cloud Apps  Microsoft Defender for Endpoint  Microsoft Copilot for Security  Microsoft 365 Defender  Microsoft Azure Portal |

**Implementation Statement:**

**Microsoft Defender for Cloud Apps**

[Integrating Cloud App Security with Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/cloud-app-security/mde-integration) gives you the ability to use Cloud Discovery beyond your corporate network or secure web gateways. With the combined user and device information, you can identify risky users or devices, see what apps they are using, and investigate further in the Defender for Endpoint portal. Cloud Discovery analyzes traffic logs collected by Defender for Endpoint and assesses identified apps against the cloud app catalog to provide compliance and security information. By configuring Cloud Discovery, you gain visibility into cloud use, Shadow IT, and continuous monitoring of the unsanctioned apps being used by your users. [Set up Cloud Discovery](https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery).

**Microsoft Sentinel**

[Connect your sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) such as, Microsoft Defender for Endpoint to Sentinel for monitoring your organization. Enable [Fusion technology based on machine learning](https://docs.microsoft.com/en-us/azure/sentinel/fusion), allowing Microsoft Sentinel to automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities that are observed at various stages of the kill-chain. Based on these discoveries, Microsoft Sentinel generates incidents that would otherwise be difficult to catch. Customized for your environment, this detection technology not only reduces [false positive](https://docs.microsoft.com/en-us/azure/sentinel/false-positives) rates but can also detect attacks with limited or missing information.

**Microsoft Copilot for Security**

Microsoft Copilot for Security can access data from Microsoft Sentinel to increase the effectiveness and efficiency of security professionals using those solutions. Microsoft Defender XDR and Microsoft Sentinel become even more powerful when security professionals use Copilot for Security. Copilot for Security delivers an experience that enriches and builds on the security data, signals, and existing incidents and insights sourced from Microsoft Defender XDR and Microsoft Sentinel.

To learn more, see:

* [What is Microsoft Copilot for Security?](https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot)
* [Get started with Microsoft Copilot for Security](https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot)

**Virtual Network/Azure Firewall**

To secure Azure application workloads, you use protective measures like authentication and encryption in the applications themselves. You can also add security layers to the virtual machine (VM) networks that host the applications, both to protect inbound flows from users, as well as outbound flows to the Internet that your application might require. This article describes [Azure Virtual Network](https://azure.microsoft.com/services/virtual-network/) security services like Azure Firewall and Azure Application Gateway, when to use each service, and network design options that combine both.

[Azure Firewall](https://docs.microsoft.com/en-us/azure/firewall/overview) is a managed next-generation firewall that offers [network address translation (NAT)](https://docs.microsoft.com/en-us/azure/virtual-network/nat-overview). Azure Firewall bases packet filtering on Internet Protocol (IP) addresses and Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ports, or on application-based HTTP(S) or SQL attributes. Azure Firewall also leverages Microsoft threat intelligence to identify malicious IP addresses. [Azure Firewall Premium](https://docs.microsoft.com/en-us/azure/firewall/premium-features) includes all functionality of Azure Firewall Standard plus additional features such as TLS-inspection and IDPS (Intrusion Detection and Protection System) To learn more, see the [Azure Firewall documentation](https://docs.microsoft.com/en-us/azure/firewall/).

[Azure Application Gateway](https://docs.microsoft.com/en-us/azure/application-gateway/overview) is a managed web traffic load balancer and HTTP(S) full reverse proxy that can do Secure Socket Layer (SSL) encryption and decryption. Application Gateway also uses Web Application Firewall to inspect web traffic and detect attacks at the HTTP layer. To learn more, see the [Application Gateway documentation](https://docs.microsoft.com/en-us/azure/application-gateway/).

[Azure Web Application Firewall (WAF)](https://azure.microsoft.com/services/web-application-firewall/) is an optional addition to Azure Application Gateway to provide inspection of HTTP request and prevent malicious attacks at the web layer such as SQL Injection or Cross-Site Scripting. To learn more, see the [Web Application Firewall documentation](https://docs.microsoft.com/en-us/azure/web-application-firewall/).

**Microsoft Defender for Cloud /RBAC/PIM**

Microsoft Defender for Cloud’s Just-in-time (JIT) virtual machine access locks down inbound traffic to Azure virtual machines, reducing exposure to attacks while providing easy access to connect to VMs when needed. All JIT requests to access virtual machines are logged in the Activity Log allowing you to monitor for atypical usage. When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions for that VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. For more information see, [Secure your management ports with just-in-time access](https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time).

**Customer Responsibility**

* Monitoring customer-deployed resources to identify unauthorized use through customer-defined techniques and methods.

# Secure Cloud Business Applications (SCUBA)

The SCuBA project aims to secure cloud business applications for federal agencies and protect federal information stored within these environments. It does so by providing guidance and security configurations. The project supports CISA's role in mitigating cybersecurity risks and its partnership with the CIO Council has resulted in minimum security controls for M365.

**Baselines available for download:**

* [Microsoft Defender for Office 365](https://www.cisa.gov/sites/default/files/publications/Microsoft%20365%20Defender%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)
* [Microsoft Entra ID](https://www.cisa.gov/sites/default/files/publications/Microsoft%20Azure%20Active%20Directory%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)
* [Microsoft Exchange Online](https://www.cisa.gov/sites/default/files/publications/Microsoft%20Exchange%20Online%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)
* [Microsoft OneDrive for Business](https://www.cisa.gov/sites/default/files/publications/Microsoft%20OneDrive%20for%20Business%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)
* [Microsoft Power BI](https://www.cisa.gov/sites/default/files/publications/Microsoft%20Power%20BI%20M365%20Minimum%20Viable%20SCB%20v0.1.pdf)
* [Microsoft Power Platform](https://www.cisa.gov/sites/default/files/publications/Microsoft%20Power%20Platform%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)
* [Microsoft SharePoint Online](https://www.cisa.gov/sites/default/files/publications/Microsoft%20SharePoint%20Online%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)
* [Microsoft Teams](https://www.cisa.gov/sites/default/files/publications/Microsoft%20Teams%20M365%20Minimum%20Viable%20SCB%20Draft%20v0.1.pdf)

# Service Customer Responsibility

The table is established to provide useful information for customers to better understand the service and key customer responsibilities associated with the service. Not all Microsoft services are depicted in the following customer responsibility table. Likewise, not all responsibilities of the customer are depicted.

|  |  |
| --- | --- |
| Automation | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating an automation account   [Create an Azure Automation account using the portal](https://learn.microsoft.com/en-us/azure/automation/quickstarts/create-azure-automation-account-portal)   * Enabling managed identities   [Enable managed identities for your Automation account using the Azure portal](https://learn.microsoft.com/en-us/azure/automation/quickstarts/enable-managed-identity)   * Enabling desire state configuration for a machine   [Azure Configure a VM with Desired State Configuration](https://learn.microsoft.com/en-us/azure/automation/quickstarts/dsc-configuration)   * Configuration management   [Azure Automation State Configuration overview](https://learn.microsoft.com/en-us/azure/automation/automation-dsc-overview)   * Update management for VMs   [Manage updates and patches for your VMs in Azure Automation](https://learn.microsoft.com/en-us/azure/automation/update-management/manage-updates-for-vm) |
| Microsoft Entra ID  \*Premium P1 + P2 | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Selecting appropriate licensing   [What are the Microsoft Entra ID licenses?](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis#what-are-the-azure-ad-licenses)   * Creating a directory   [Access & create new tenant](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant)   * Adding a custom domain name   [Add your custom domain](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain)   * Associate an Azure Subscription   [Add an existing Azure subscription to your tenant](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory)   * Adding Privacy info and statements   [Add your organization's privacy info](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-properties-area)   * Adding organizational branding   [Add company branding to your organization's sign-in page (preview)](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-customize-branding)   * Managing users, groups and licensing for example; creating, deleting, managing, and applying licenses to users   [Add or delete users](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory)   * Enabling MFA   [Microsoft Entra ID Multi-Factor Authentication for your organization](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started) |
| Microsoft Entra ID advanced Threat Protection (now Microsoft Defender for Identity) | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Validating and Meeting perquisites   [Microsoft Defender for Identity prerequisites](https://learn.microsoft.com/en-us/defender-for-identity/prerequisites)   * For deploying and configuring sensors   [Download the Microsoft Defender for Identity sensor](https://learn.microsoft.com/en-us/defender-for-identity/download-sensor)   * For managing and updating sensors   [Manage and update Microsoft Defender for Identity sensors](https://learn.microsoft.com/en-us/defender-for-identity/sensor-settings)   * Investigating and responding to alerts generated by sensors   [Remediation actions in Microsoft Defender for Identity](https://learn.microsoft.com/en-us/defender-for-identity/remediation-actions) |
| Azure Archive Storage | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Validating and configuring the appropriate capacity limits and Azure Storage redundancy.   [Hot, cool, and archive access tiers for blob data](https://learn.microsoft.com/en-gb/azure/storage/blobs/access-tiers-overview#archive-access-tier)  [Optimize costs for Blob storage with reserved capacity](https://learn.microsoft.com/en-gb/azure/storage/blobs/storage-blob-reserved-capacity)   * Creating, recovering and Managing storage accounts   [Create a storage account](https://learn.microsoft.com/en-gb/azure/storage/common/storage-account-create?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json&tabs=azure-portal)   * Monitoring storage accounts   [Monitoring Azure Blob Storage](https://learn.microsoft.com/en-gb/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal) |
| Azure Backup | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Backing up, restoring, monitoring, and managing customer deployed backups such as virtual machine and database backups   [Back up a VM with the Azure portal](https://learn.microsoft.com/en-us/azure/backup/quick-backup-vm-portal)  [Quick start - Back up Azure Database for PostgreSQL server](https://learn.microsoft.com/en-us/azure/backup/quick-backup-postgresql-database-portal)  [About the Azure Virtual Machine restore process](https://learn.microsoft.com/en-us/azure/backup/about-azure-vm-restore)  [Manage and monitor Azure VM backups](https://learn.microsoft.com/en-us/azure/backup/backup-azure-manage-vms) |
| Azure Bastion | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Provisioning and deploying Azure Bastion   [Deploy Bastion using specified settings: Azure portal](https://learn.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal)   * Configuring Azure Bastion   [About Azure Bastion configuration settings](https://learn.microsoft.com/en-us/azure/bastion/configuration-settings)  [Upgrade a SKU](https://learn.microsoft.com/en-us/azure/bastion/upgrade-sku)   * Connecting to Virtual Machine   [Connect to a Windows VM using RDP](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows)  [Connect to a Windows VM using SSH](https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-ssh-windows)   * Monitoring   [Configure monitoring and metrics using Azure Monitor](https://learn.microsoft.com/en-us/azure/bastion/howto-metrics-monitor-alert)  [Azure Bastion session monitoring and management](https://learn.microsoft.com/en-us/azure/bastion/session-monitoring) |
| Azure Blueprints | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Managing, updating and creating custom blueprints or selecting from Microsoft provided samples.   [Create a blueprint in the portal](https://learn.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal)  [Blueprint sample to new environment](https://learn.microsoft.com/en-us/azure/governance/blueprints/tutorials/create-from-sample)  [How to manage assignments with PowerShell](https://learn.microsoft.com/en-us/azure/governance/blueprints/how-to/manage-assignments-ps)  [Import and export blueprints with PowerShell](https://learn.microsoft.com/en-us/azure/governance/blueprints/how-to/import-export-ps)  [Update an existing assignment from the portal](https://learn.microsoft.com/en-us/azure/governance/blueprints/how-to/update-existing-assignments)  [Set up your environment for Blueprint Operator](https://learn.microsoft.com/en-us/azure/governance/blueprints/how-to/configure-for-blueprint-operator) |
| Azure Data Explorer | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating and managing an Azure Data Explorer Cluster and database   [Create an Azure Data Explorer cluster & DB with Azure CLI](https://learn.microsoft.com/en-us/azure/data-explorer/create-cluster-database-cli)  [Use Microsoft Entra ID visor recommendations to optimize your Azure Data Explorer cluster](https://learn.microsoft.com/en-us/azure/data-explorer/azure-advisor)  [Manage database permissions in Azure Data Explorer](https://learn.microsoft.com/en-us/azure/data-explorer/manage-database-permissions)   * Deploying and configuring the resources you need to run data explorer cluster.   [Automated provisioning in Azure Data Explorer](https://learn.microsoft.com/en-us/azure/data-explorer/automated-deploy-overview) |
| Azure DDOS Protection | Customer is responsible for:  Configuring, managing, and applying the appropriate settings for customer resources to include, but not limited to:   * Azure DDoS Protection supports two SKU Types, DDoS IP Protection and DDoS Network Protection. The customer is responsible for configuring the SKU in the Azure portal during the workflow when you configure Azure DDoS Protection.   [About Azure DDoS Protection SKU Comparison](https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-sku-comparison#skus)   * Creating and configuring Azure DDoS Network Protection   [Create and configure Azure DDoS Network Protection using the Azure portal](https://learn.microsoft.com/en-us/azure/ddos-protection/manage-ddos-protection)  [Create and configure Azure DDoS IP Protection Preview using PowerShell](https://learn.microsoft.com/en-us/azure/ddos-protection/manage-ddos-protection-powershell-ip)  [Azure DDoS Protection Plan permissions](https://learn.microsoft.com/en-us/azure/ddos-protection/manage-permissions)  [View and configure Azure DDoS Protection diagnostic logging](https://learn.microsoft.com/en-us/azure/ddos-protection/diagnostic-logging?tabs=DDoSProtectionNotifications)  [View and configure Azure DDoS Protection alerts](https://learn.microsoft.com/en-us/azure/ddos-protection/alerts) |
| Azure DNS | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating DNS Zone and record   [Create a DNS zone and record - Azure portal](https://learn.microsoft.com/en-us/azure/dns/dns-getstarted-portal)  [Create an Azure private DNS zone using the Azure portal](https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal)  [Create an Azure DNS Private Resolver using the Azure portal](https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-get-started-portal)   * Azure DNS does not currently support DNSSEC. It is the customer’s responsibility when using Azure DNS, to host these zones with a third-party DNS hosting provider. |
| Azure Firewall | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Deploy and configure Azure Firewall   [Deploy & configure Azure Firewall using the Azure portal](https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal)  [Deploy and configure Azure Firewall Premium](https://learn.microsoft.com/en-us/azure/firewall/premium-deploy)  [Add or modify multiple Azure Firewall rules using Azure PowerShell](https://learn.microsoft.com/en-us/azure/firewall/deploy-rules-powershell)   * Monitoring Azure Firewall logs and metrics   [Monitor Azure Firewall logs and metrics](https://learn.microsoft.com/en-us/azure/firewall/firewall-diagnostics)   * Backup Azure Firewall   [Backup Azure Firewall and Firewall Policy with Logic Apps (microsoft.com)](https://techcommunity.microsoft.com/t5/azure-network-security-blog/backup-azure-firewall-and-azure-firewall-policy-with-logic-apps/ba-p/3613928) |
| Azure Front Door | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Choosing your Azure Front Door tier.   [Azure Front Door tier comparison](https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/tier-comparison)   * Creating Azure Front Door profile   [Create an Azure Front Door profile - Azure portal](https://learn.microsoft.com/en-us/azure/frontdoor/create-front-door-portal)   * Managing and monitoring   [Logs - Azure Front Door](https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-logs)  [Monitoring metrics for Azure Front Door](https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-monitor-metrics) |
| Azure Information Protection | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Configuring and installing Azure Information Protection   [Install and configure the Azure Information Protection (AIP) unified labeling scanner](https://learn.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner-configure-install?tabs=azure-portal-only)  [Deploying the Azure Information Protection (AIP) unified labeling client](https://learn.microsoft.com/en-us/azure/information-protection/quickstart-deploy-client)   * Monitoring, viewing, and analyzing reports and logs.   [Analytics and central reporting for Azure Information Protection (AIP)](https://learn.microsoft.com/en-us/azure/information-protection/reports-aip)  [Log & analyze the protection usage from Azure Information Protection](https://learn.microsoft.com/en-us/azure/information-protection/log-analyze-usage)  [Azure Information Protection unified labeling client files and usage logging](https://learn.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-files-and-logging) |
| Azure Key Vault | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating, managing, backing up and restoring Azure Key Vault   [Create an Azure Key Vault with the Azure portal](https://learn.microsoft.com/en-us/azure/key-vault/general/quick-create-portal)  [Azure Key Vault developer's guide](https://learn.microsoft.com/en-us/azure/key-vault/general/developers-guide)  [Create an Azure key vault and a vault access policy by using ARM template](https://learn.microsoft.com/en-us/azure/key-vault/general/vault-create-template?tabs=CLI)  [Azure Key Vault recovery overview](https://learn.microsoft.com/en-us/azure/key-vault/general/key-vault-recovery?tabs=azure-portal)  [Back up a secret, key, or certificate stored in Azure Key Vault](https://learn.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli)   * Configuring access policies and permissions   [Assign an Azure Key Vault access policy (CLI)](https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal)   * Monitoring, Logging and Alerting settings for Azure Key Vault   [Monitoring Azure Key Vault](https://learn.microsoft.com/en-us/azure/key-vault/general/monitor-key-vault)  [Enable Azure Key Vault logging](https://learn.microsoft.com/en-us/azure/key-vault/general/howto-logging?tabs=azure-cli)  [Configure Azure Key Vault alerts](https://learn.microsoft.com/en-us/azure/key-vault/general/alert) |
| Azure LockBox/Customer Lockbox | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Enabling Customer Lockbox   [Customer Lockbox for Microsoft Azure](https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview#enable-customer-lockbox)   * Tracking and approving support requests   [Configure Lockbox for Azure Data Box](https://learn.microsoft.com/en-us/azure/databox/data-box-customer-lockbox#track-approve-request-via-lockbox) |
| Azure Managed Services – Azure Light House | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Managing Access, onboarding customers, viewing and monitoring activity, and service integrations   [Onboard a customer to Azure Lighthouse](https://learn.microsoft.com/en-us/azure/lighthouse/how-to/onboard-customer)  [Create eligible authorizations](https://learn.microsoft.com/en-us/azure/lighthouse/how-to/create-eligible-authorizations)  [Remove access to a delegation](https://learn.microsoft.com/en-us/azure/lighthouse/how-to/remove-delegation)  [View and manage service providers](https://learn.microsoft.com/en-us/azure/lighthouse/how-to/view-manage-service-providers)  [Monitor service provider activity](https://learn.microsoft.com/en-us/azure/lighthouse/how-to/view-service-provider-activity)  [Manage Microsoft Sentinel workspaces at scale](https://learn.microsoft.com/en-us/azure/lighthouse/how-to/manage-sentinel-workspaces) |
| Azure Monitor | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Managing and installing azure monitor agent   [Manage Azure Monitor Agent](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-manage?tabs=azure-portal)   * Creating data collection rules   [Monitor data from virtual machines with Azure Monitor Agent](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent?tabs=portal)   * Defining network settings   [Define Azure Monitor Agent network settings](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-data-collection-endpoint?tabs=PowerShellWindows) |
| Azure Portal | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Managing Access to Microsoft Entra ID min portal   [Assign Azure roles using the Azure portal - Azure RBAC](https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal)  [Assign a user as an administrator of an Azure subscription](https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-subscription-admin)   * Managing Azure portal settings and preferences   [Manage Azure portal settings and preferences](https://learn.microsoft.com/en-us/azure/azure-portal/set-preferences) |
| Azure Resource Manager (ARM) | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating and Deploying Resource Manager Templates   [Deploy template - Azure portal - Azure Resource Manager](https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/quickstart-create-templates-use-the-portal)  [Deploy resources with Azure portal - Azure Resource Manager](https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-portal)  [Deploy resources with PowerShell and template - Azure Resource Manager](https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-powershell)   * Managing Access to resource groups   [Manage resource groups - Azure portal - Azure Resource Manager](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal#manage-access-to-resource-groups) |
| Microsoft Sentinel | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Managing Access to Microsoft Sentinel   [Manage access to Microsoft Sentinel data by resource](https://learn.microsoft.com/en-us/azure/sentinel/resource-context-rbac)   * Onboarding to Microsoft Sentinel and validating prerequisites are met.   [Onboard in Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/quickstart-onboard)   * Connecting data connectors for data collection   [Find your Microsoft Sentinel data connector](https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference)  [Connect your threat intelligence platform to Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-tip)   * Create threat detection rules   [Create custom analytics rules to detect threats with Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom)   * Investigating incidents   [Investigate incidents with Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases)   * Enabling Microsoft Sentinel health monitoring   [Turn on health monitoring in Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/enable-monitoring)  [Monitor the health of your Microsoft Sentinel data connectors](https://learn.microsoft.com/en-us/azure/sentinel/monitor-data-connector-health)   * Setting up customer managed keys   [Set up customer-managed keys in Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/customer-managed-keys)   * Creating automated response rules.   [Create and use Microsoft Sentinel automation rules to manage response](https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules) |
| Azure Site Recovery | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Setting up disaster recovery to a secondary Azure Region   [Set up Azure VM disaster recovery to a secondary region with Azure Site Recovery](https://learn.microsoft.com/en-us/azure/site-recovery/azure-to-azure-quickstart)   * Configuring and monitoring disaster recovery   [Disaster recovery for Azure VMs using Azure PowerShell and Azure Site Recovery](https://learn.microsoft.com/en-us/azure/site-recovery/azure-to-azure-powershell)  [About networking in Azure VM disaster recovery with Azure Site Recovery](https://learn.microsoft.com/en-us/azure/site-recovery/azure-to-azure-about-networking)  [Map virtual networks between two regions in Azure Site Recovery](https://learn.microsoft.com/en-us/azure/site-recovery/azure-to-azure-network-mapping)  [Monitor Azure Site Recovery - Azure Site Recovery](https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-monitor-and-troubleshoot) |
| Event Hubs | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating an event hub   [Create an event hub using the Azure portal](https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-create)  [Govern resources for client applications with application groups](https://learn.microsoft.com/en-us/azure/event-hubs/resource-governance-with-app-groups?tabs=portal)   * Send events to or receive events from an event hub.   [Event Hubs - Capture streaming events using Azure portal](https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-capture-enable-through-portal)  [Next Steps – sending or receiving events](https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-create#next-steps)   * Manage and Monitoring event hubs   [Monitoring Azure Event Hubs](https://learn.microsoft.com/en-us/azure/event-hubs/monitor-event-hubs)  [Send data from Windows Azure diagnostics extension to Azure Event Hubs - Azure Monitor](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-stream-event-hubs)  [Azure Event Hubs Firewall Rules - Azure Event Hubs](https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-ip-filtering)  [Virtual Network service endpoints - Azure Event Hubs](https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-service-endpoints)  [Configure your own key for encrypting Azure Event Hubs data at rest](https://learn.microsoft.com/en-us/azure/event-hubs/configure-customer-managed-key)  [Configure the minimum TLS version for an Event Hubs namespace –](https://learn.microsoft.com/en-us/azure/event-hubs/transport-layer-security-configure-minimum-version)  [Configure Transport Layer Security (TLS) for an Event Hubs client application](https://learn.microsoft.com/en-us/azure/event-hubs/transport-layer-security-configure-client-version?tabs=dotnet) |
| ExpressRoute | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Choose your connectivity model   [Azure ExpressRoute: Connectivity models](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models)   * Configuring and Creating ExpressRoute connection   [Create an ExpressRoute circuit](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager)  [Configure routing](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-routing-portal-resource-manager)  [Link a VNet to an ExpressRoute circuit](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager) |
| GitHub AE | Customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Configuring automatic user provisioning   [Configure GitHub AE for automatic user provisioning with Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/github-ae-provisioning-tutorial)   * Setting up, configuring, and managing settings   [Getting started with GitHub AE - GitHub AE Docs](https://docs.github.com/en/github-ae@latest/get-started/onboarding/getting-started-with-github-ae) |
| Intune | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Validating organizational or personal devices are supported by Intune.   [Operating systems and browsers supported by Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers)   * Acquiring an Intune license and assigning it to users.   [Assign Microsoft Intune licenses](https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses-assign)  [Sign up or sign into Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/fundamentals/account-sign-up)   * Configuration settings   [Configure a custom domain name](https://learn.microsoft.com/en-us/mem/intune/fundamentals/custom-domain-name-configure)  [Add users and grant permissions](https://learn.microsoft.com/en-us/mem/intune/fundamentals/users-add)  [Set the mobile device management authority](https://learn.microsoft.com/en-us/mem/intune/fundamentals/mdm-authority-set)  [Add apps to Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/apps/apps-add)  [Device features and settings in Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/configuration/device-profiles)  [How to configure the Intune Company Portal apps, Company Portal website, and Intune app - Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/apps/company-portal-app)  [Enrollment options for devices managed by Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-options)  [App protection policies overview - Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy) |
| Load Balancer | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating and configuring load balancers   [Create a public load balancer - Azure portal](https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal)  [Create an internal load balancer - Azure portal](https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-internal-portal) |
| Log Analytics | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Editing and creating log queries   [Log queries in Azure Monitor](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview) |
| Microsoft 365 Defender: Defender for: Endpoint, Identity, cloud apps, Office 365, Vulnerability Management | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Validating perquisites are met such as acquiring licensing.   [Microsoft 365 Defender prerequisites](https://learn.microsoft.com/en-us/microsoft-365/security/defender/prerequisites?view=o365-worldwide)   * Turn on Microsoft 365 Defender and Create your environment   [Turn on Microsoft 365 Defender](https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-enable?view=o365-worldwide)  [How to create the environment](https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-create-eval-environment?view=o365-worldwide)   * Configure, set up and learn about each technology:   + [Microsoft Defender for Identity](https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-identity-overview?view=o365-worldwide)   + [Microsoft Defender for Office](https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-office-365-overview?view=o365-worldwide)   + [Microsoft Defender for Endpoint](https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-endpoint-overview?view=o365-worldwide)   + [Microsoft Defender for Cloud Apps](https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-mcas-overview?view=o365-worldwide) * Managing and responding to incidents   [Manage incidents in Microsoft 365 Defender](https://learn.microsoft.com/en-us/microsoft-365/security/defender/manage-incidents?view=o365-worldwide)  [Prioritize incidents in Microsoft 365 Defender](https://learn.microsoft.com/en-us/microsoft-365/security/defender/incident-queue?view=o365-worldwide)  [Investigate alerts in Microsoft 365 Defender](https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide) |
| Microsoft Flow (now power automate) | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Validating perquisites are met such as acquiring licensing.   [Prerequisites and limitations - Power Automate](https://learn.microsoft.com/en-us/power-automate/desktop-flows/requirements)  [Billing and metering questions - Power Automate](https://learn.microsoft.com/en-us/power-automate/billing-questions)  [Types of Power Automate licenses](https://learn.microsoft.com/en-us/power-platform/admin/power-automate-licensing/types)  [Manage licenses in your organization - Power Platform](https://learn.microsoft.com/en-us/power-platform/admin/signup-question-and-answer)  [Add Microsoft Dataverse storage capacity - Power Platform](https://learn.microsoft.com/en-us/power-platform/admin/add-storage)   * Installing Power Automate   [Install Power Automate](https://learn.microsoft.com/en-us/power-automate/desktop-flows/install)   * Configuring/creating flows   [Create desktop flows - Power Automate](https://learn.microsoft.com/en-us/power-automate/desktop-flows/create-flow)  [Trigger desktop flows from cloud flows](https://learn.microsoft.com/en-us/power-automate/desktop-flows/trigger-desktop-flows)  [Create a business process flow in Power Apps](https://learn.microsoft.com/en-us/power-automate/create-business-process-flow)  [Work with desktop flows using code - Power Automate](https://learn.microsoft.com/en-us/power-automate/developer/desktop-flow-public-apis)   * Managing and configuring connections   [Learn to connect to your data using connections and on-premises data gateways (contains video)](https://learn.microsoft.com/en-us/power-automate/add-manage-connections)  [Power Platform and Azure Logic Apps connectors documentation - Connectors](https://learn.microsoft.com/en-us/connectors/)  [Create a custom connector from scratch](https://learn.microsoft.com/en-us/connectors/custom-connectors/define-blank)  [IP address configuration - Power Automate](https://learn.microsoft.com/en-us/power-automate/ip-address-configuration)   * Access Management, monitoring and logging   [Power Apps activity logging - Power Platform](https://learn.microsoft.com/en-us/power-platform/admin/logging-powerapps)  [View Power Automate audit logs. - Power Platform](https://learn.microsoft.com/en-us/power-platform/admin/logging-power-automate)  [Security enhancements: User session and access management](https://learn.microsoft.com/en-us/power-platform/admin/user-session-management) |
| Microsoft Graph | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Authentication, Authorization, Access, and permissions   [Register your app with the Microsoft Entra ID v2.0 endpoint - Microsoft Graph](https://learn.microsoft.com/en-us/graph/auth-register-app-v2)  [Get access on behalf of a user - Microsoft Graph](https://learn.microsoft.com/en-us/graph/auth-v2-user)  [Get access without a user - Microsoft Graph](https://learn.microsoft.com/en-us/graph/auth-v2-service)  [Microsoft Graph permissions](https://learn.microsoft.com/en-us/graph/permissions-reference)  [[Consent and authorization](https://learn.microsoft.com/en-us/graph/best-practices-concept#consent-and-authorization)](https://learn.microsoft.com/en-us/graph/best-practices-concept) |
| Multi-factor Authentication (MFA) | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Selecting appropriate licensing   [Microsoft Entra ID Multi-Factor Authentication versions and consumption plans](https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-based-on-licenses)   * Managing authentication methods   [How to migrate to the Authentication methods policy - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-authentication-methods-manage)   * Enabling and Configuring MFA   [Configure Microsoft Entra ID Multi-Factor Authentication - Microsoft Entra ID](https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings) |
| Network Watcher Network Watcher-Traffic Analytics | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Configuring Network Watcher   [Create an Azure Network Watcher instance](https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-create)  [Monitor network connectivity by using Azure Monitor Agent](https://learn.microsoft.com/en-us/azure/network-watcher/azure-monitor-agent-with-connection-monitor)  [Create a connection monitor - Azure portal](https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal?source=recommendations) |
| Storage | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating and managing storage accounts   [Create a storage account](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-create?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json&tabs=azure-portal)  [Upgrade Azure Blob Storage with Azure Data Lake Storage](https://learn.microsoft.com/en-us/azure/storage/blobs/upgrade-to-data-lake-storage-gen2-how-to?tabs=azure-portal)  [Manage blob containers using the Azure portal](https://learn.microsoft.com/en-us/azure/storage/blobs/blob-containers-portal)  [Manage block blobs with PowerShell](https://learn.microsoft.com/en-us/azure/storage/blobs/blob-powershell)   * Authorizing Access and permissions   [Choose how to authorize access to blob data in the Azure portal](https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal)  [Assign an Azure role for access to blob data - Azure Storage](https://learn.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access?tabs=portal)  [Manage account access keys - Azure Storage](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json&tabs=azure-portal)   * Monitoring storage services   [Monitor Azure Storage services with Azure Monitor Storage insights](https://learn.microsoft.com/en-us/azure/storage/common/storage-insights-overview?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json)   * Validating blobs created before 10/20/2017 are encrypted. Blobs created after this date are encrypted with Azure Storage encryption.   [Check the encryption status of a blob - Azure Storage](https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-encryption-status?tabs=portal)   * Consider using the service-side encryption features provided by Azure Storage to protect your data, instead of client-side encryption. If using client-side encryption and you are currently using v1, we recommend that you update your application to use client-side encryption v2 and migrate your data.   [Azure Storage encryption for data at rest](https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption#client-side-encryption-for-blobs-and-queues) |
| Virtual Machines | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Configuring, access authorizations, creating and backing up a virtual machine   [Create a Windows VM in the Azure portal](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal)  [Create a virtual network](https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-cli?context=%2Fazure%2Fvirtual-machines%2Fcontext%2Fcontext)  [Back up a VM with the Azure portal](https://learn.microsoft.com/en-us/azure/backup/quick-backup-vm-portal?context=%2Fazure%2Fvirtual-machines%2Fcontext%2Fcontext)  [Just-in-time virtual machine access in Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage?tabs=jit-config-asc%2Cjit-request-asc)   * Monitoring a virtual machine   [Monitoring Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/monitor-vm?context=%2Fazure%2Fvirtual-machines%2Fcontext%2Fcontext)   * Update and Patching   [Maintenance control for OS image upgrades on Azure Virtual Machine Scale Sets using Azure portal](https://learn.microsoft.com/en-us/azure/virtual-machines/virtual-machine-scale-sets-maintenance-control-portal)  [Azure Automation Update Management overview](https://learn.microsoft.com/en-us/azure/automation/update-management/overview?context=%2Fazure%2Fvirtual-machines%2Fcontext%2Fcontext) |
| Virtual Network | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Creating, configuring, monitoring, and managing a virtual network   [Create a virtual network](https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal)  [Plan Azure virtual networks](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm)  [Name resolution for resources in Azure virtual networks](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances)  [Add, change, or delete an Azure virtual network subnet](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet)  [Filter network traffic with a network security group (NSG)](https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic)  [Monitoring Azure virtual networks](https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network) |
| VPN Gateway | The customer is responsible for:  Configuring and applying the appropriate settings for customer resources to include, but not limited to:   * Create, configure, monitor, and manage the VPN gateway   [Create & manage a VPN gateway](https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-create-gateway-portal)  [Connect an on-premises network and a virtual network: S2S VPN: Azure portal](https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal)  [Monitoring Azure VPN Gateway](https://learn.microsoft.com/en-us/azure/vpn-gateway/monitor-vpn-gateway) |

# CMMC Blogs

* [Accelerating CMMC compliance for Microsoft cloud](https://techcommunity.microsoft.com/t5/public-sector-blog/accelerating-cmmc-compliance-for-microsoft-cloud-in-depth-review/ba-p/1825671)
* [Microsoft CMMC Acceleration Program Update](https://aka.ms/CMMCAccelerationProgramUpdate)
* [Understanding Compliance Between Commercial, Government and DoD Offerings](https://techcommunity.microsoft.com/t5/public-sector-blog/understanding-compliance-between-commercial-government-and-dod/ba-p/2157679)
* [The Microsoft 365 Government (GCC High) Conundrum - DIB Data Enclave vs Going All In](https://techcommunity.microsoft.com/t5/public-sector-blog/the-microsoft-365-government-gcc-high-conundrum-dib-data-enclave/ba-p/722954)
* [Microsoft expands qualification of contractors for Government cloud offerings](https://techcommunity.microsoft.com/t5/public-sector-blog/microsoft-expands-qualification-of-contractors-for-government/ba-p/2030588)
* [Microsoft Sentinel Cybersecurity Maturity Model Certification (CMMC) Workbook](https://techcommunity.microsoft.com/t5/public-sector-blog/azure-sentinel-cybersecurity-maturity-model-certification-cmmc/ba-p/2110524)
* [CMMC on Azure DevBlogs](https://devblogs.microsoft.com/search?query=cmmc)
* [CMMC on Tech Community](https://techcommunity.microsoft.com/t5/public-sector-blog/bg-p/PublicSectorBlog/label-name/CMMC)

# CMMC Resources

* [Chief Information Officer > CMMC (defense.gov)](https://dodcio.defense.gov/CMMC/)
* [CMMC Documentation (defense.gov)](https://dodcio.defense.gov/CMMC/Documentation/)
* [CMMC Assessment Guide - Level 2 (defense.gov)](https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf)
* [CyberAB > Home](https://cyberab.org/)
* [CyberAssist CMMC Resources](https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/)
* [CUI Categories | National Archives](https://www.archives.gov/cui/registry/category-list)
* [DoD Mandatory Controlled Unclassified Information (CUI) Training (usalearning.gov)](https://securityawareness.usalearning.gov/cui/index.html#:~:text=DoD%20Mandatory%20Controlled%20Unclassified%20Information%20%28CUI%29%20Training%20This,DoD%20personnel%20with%20access%20to%20controlled%20unclassified%20information.)

# CMMC Tools

* [Microsoft Product Placemat for CMMC L2](https://aka.ms/cmmc/productplacemat)

# Service to Control Mappings

|  |  |
| --- | --- |
| **Microsoft Service** | **CMMC Control Mapping** |
| Azure Automation | CM.L2-3.4.1 |
| CM.L2-3.4.2 |
| SI.L1-3.14.4 |
| AC.L3-3.1.2e |
| IA.L3-3.5.1e |
| Azure Bastion | AC.L2-3.1.12 |
| AC.L2-3.1.14 |
| AC.L2-3.1.13 |
| AC.L2-3.1.11 |
| IA.L2-3.5.11 |
| IA.L2-3.5.3 |
| MA.L2-3.7.2 |
| MA.L2-3.7.6 |
| SC.L1-3.13.1 |
| SC.L1-3.13.5 |
| SI.L2-3.14.7 |
| AC.L3-3.1.2e |
| Azure Datacenter | PE.L1-3.10.1 |
| PE.L1-3.10.3 |
| PE.L1-3.10.4 |
| PE.L1-3.10.5 |
| PE.L2-3.10.2 |
| Microsoft Defender for IoT | AC.L1-3.1.20 |
| AC.L2-3.1.12 |
| AU.L2-3.3.5 |
| AU.L2-3.3.6 |
| CA.L2-3.12.1 |
| CM.L2-3.4.1 |
| CM.L2-3.4.7 |
| IR.L2-3.6.1 |
| RA.L2-3.11.1 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SC.L1-3.13.1 |
| SC.L2-3.13.6 |
| SC.L2-3.13.14 |
| SI.L2-3.14.3 |
| SI.L2-3.14.6 |
| CM.L3-3.4.3e |
| Azure DevTest Labs | CM.L2-3.4.4 |
| Azure DNS | SI.L1-3.14.2 |
| SI.L2-3.14.6 |
| Azure ExpressRoute | AC.L2-3.1.12 |
| AC.L2-3.1.14 |
| SC.L1-3.13.1 |
| SC.L2-3.13.7 |
| SC.L2-3.13.8 |
| SC.L2-3.13.15 |
| Azure Firewall | AC.L1-3.1.20 |
| AC.L2-3.1.13 |
| AU.L2-3.3.1 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| PE.L2-3.10.6 |
| SC.L1-3.13.1 |
| SC.L1-3.13.5 |
| SC.L2-3.13.11 |
| SC.L2-3.13.6 |
| SC.L2-3.13.7 |
| SI.L2-3.14.6 |
| SI.L2-3.14.7 |
| AC.L3-3.1.1e |
| AC.L3-3.1.3e |
| AT.L3-3.2.1e |
| CM.L3-3.4.2e |
| Azure Front Door | AC.L2-3.1.14 |
| AC.L2-3.1.3 |
| Azure Key Vault | IA.L2-3.5.10 |
| MP.L1-3.8.3 |
| MP.L2-3.8.1 |
| MP.L2-3.8.5 |
| MP.L2-3.8.6 |
| MP.L2-3.8.9 |
| SC.L2-3.13.11 |
| SC.L2-3.13.8 |
| SC.L2-3.13.10 |
| SC.L2-3.13.15 |
| SC.L2-3.13.16 |
| SI.L2-3.14.6 |
| CM.L3-3.4.1e |
| Azure Lighthouse | CM.L2-3.4.1 |
| Azure Monitor | AC.L2-3.1.7 |
| AU.L2-3.3.4 |
| CA.L2-3.12.1 |
| CA.L2-3.12.3 |
| CM.L2-3.4.9 |
| SC.L1-3.13.1 |
| AC.L3-3.1.3e |
| CM.L3-3.4.2e |
| Azure RBAC | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L2-3.1.5 |
| AC.L2-3.1.6 |
| AC.L2-3.1.4 |
| AC.L2-3.1.7 |
| AU.L2-3.3.8 |
| AU.L2-3.3.9 |
| CM.L2-3.4.5 |
| IA.L1-3.5.1 |
| MA.L2-3.7.2 |
| MA.L2-3.7.5 |
| MP.L2-3.8.1 |
| MP.L2-3.8.2 |
| MP.L2-3.8.5 |
| MP.L2-3.8.6 |
| PE.L2-3.10.6 |
| PS.L2-3.9.2 |
| MP.L2-3.8.9 |
| SC.L2-3.13.3 |
| SC.L2-3.13.4 |
| AC.L3-3.1.3e |
| Microsoft Sentinel | AC.L2-3.1.12 |
| AC.L2-3.1.7 |
| AU.L2-3.3.2 |
| AU.L2-3.3.1 |
| AU.L2-3.3.3 |
| AU.L2-3.3.4 |
| AU.L2-3.3.8 |
| AU.L2-3.3.5 |
| AU.L2-3.3.6 |
| CA.L2-3.12.1 |
| CA.L2-3.12.2 |
| CA.L2-3.12.3 |
| CM.L2-3.4.9 |
| IR.L2-3.6.1 |
| IR.L2-3.6.2 |
| IR.L2-3.6.3 |
| RA.L2-3.11.1 |
| SC.L1-3.13.1 |
| SC.L2-3.13.13 |
| SC.L2-3.13.14 |
| SC.L2-3.13.16 |
| SI.L1-3.14.1 |
| SI.L2-3.14.3 |
| SI.L2-3.14.6 |
| SI.L2-3.14.7 |
| AC.L3-3.1.3e |
| CM.L3-3.4.2e |
| CM.L3-3.4.3e |
| IA.L3-3.5.3e |
| Azure Storage | AU.L2-3.3.1 |
| AU.L2-3.3.8 |
| AT.L3-3.2.2e |
| IA.L3-3.5.2e |
| Azure Virtual Machines | AC.L2-3.1.10 |
| AC.L2-3.1.15 |
| CM.L2-3.4.1 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L2-3.5.10 |
| IA.L2-3.5.11 |
| MA.L2-3.7.1 |
| MP.L2-3.8.1 |
| SC.L1-3.13.1 |
| SC.L2-3.13.11 |
| SC.L2-3.13.4 |
| SC.L2-3.13.8 |
| SC.L2-3.13.9 |
| SC.L2-3.13.13 |
| SC.L2-3.13.15 |
| SC.L2-3.13.16 |
| SI.L1-3.14.2 |
| SI.L1-3.14.4 |
| SI.L2-3.14.7 |
| AC.L3-3.1.2e |
| Azure Web Application Firewall | AC.L2-3.1.14 |
| AC.L2-3.1.3 |
| AU.L2-3.3.1 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| SC.L1-3.13.1 |
| SC.L1-3.13.5 |
| SC.L2-3.13.4 |
| SC.L2-3.13.6 |
| SC.L2-3.13.13 |
| SI.L1-3.14.2 |
| SI.L2-3.14.6 |
| Load Balancer | AC.L2-3.1.13 |
| SC.L1-3.13.1 |
| SC.L1-3.13.5 |
| SC.L2-3.13.6 |
| SC.L2-3.13.8 |
| SC.L2-3.13.15 |
| SI.L2-3.14.7 |
| AC.L3-3.1.1e |
| AT.L3-3.2.2e |
| Log Analytics Workspace | AU.L2-3.3.1 |
| AU.L2-3.3.4 |
| AU.L2-3.3.8 |
| AU.L2-3.3.9 |
| AU.L2-3.3.5 |
| AU.L2-3.3.6 |
| CM.L2-3.4.3 |
| SC.L1-3.13.1 |
| SC.L2-3.13.16 |
| Microsoft Azure Portal | AC.L1-3.1.20 |
| AC.L2-3.1.10 |
| AC.L2-3.1.12 |
| AC.L2-3.1.13 |
| AC.L2-3.1.11 |
| IA.L2-3.5.10 |
| IA.L2-3.5.11 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| MA.L2-3.7.1 |
| MA.L2-3.7.5 |
| SC.L1-3.13.1 |
| SC.L2-3.13.11 |
| SC.L2-3.13.8 |
| SC.L2-3.13.9 |
| Network Security Groups | AC.L1-3.1.2 |
| AC.L1-3.1.20 |
| AC.L2-3.1.12 |
| AC.L2-3.1.14 |
| AC.L2-3.1.3 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L1-3.5.1 |
| MA.L2-3.7.2 |
| MP.L2-3.8.2 |
| SC.L1-3.13.1 |
| SC.L1-3.13.5 |
| SC.L2-3.13.4 |
| SC.L2-3.13.6 |
| SC.L2-3.13.8 |
| SC.L2-3.13.15 |
| SI.L2-3.14.6 |
| SI.L2-3.14.7 |
| AC.L3-3.1.1e |
| AC.L3-3.1.3e |
| AT.L3-3.2.1e |
| Virtual Network | CM.L2-3.4.5 |
| MP.L2-3.8.9 |
| SC.L1-3.13.1 |
| SC.L1-3.13.5 |
| SC.L2-3.13.4 |
| SC.L2-3.13.6 |
| SC.L2-3.13.8 |
| SC.L2-3.13.15 |
| SI.L2-3.14.6 |
| AC.L3-3.1.1e |
| AC.L3-3.1.3e |
| AT.L3-3.2.1e |
| VPN Gateway | AC.L2-3.1.14 |
| AC.L2-3.1.13 |
| IA.L2-3.5.3 |
| SC.L1-3.13.1 |
| SC.L2-3.13.8 |
| SC.L2-3.13.9 |
| SC.L2-3.13.15 |
| SI.L2-3.14.7 |
| App Locker | CM.L2-3.4.2 |
| CM.L2-3.4.7 |
| SI.L1-3.14.2 |
| Microsoft Entra ID | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L1-3.1.20 |
| AC.L2-3.1.9 |
| AC.L2-3.1.21 |
| AC.L2-3.1.5 |
| AC.L2-3.1.6 |
| AC.L2-3.1.8 |
| AC.L2-3.1.10 |
| AC.L2-3.1.12 |
| AC.L2-3.1.13 |
| AC.L2-3.1.4 |
| AC.L2-3.1.7 |
| AC.L2-3.1.11 |
| AC.L2-3.1.15 |
| AT.L2-3.2.1 |
| AU.L2-3.3.2 |
| AU.L2-3.3.1 |
| AU.L2-3.3.3 |
| AU.L2-3.3.4 |
| AU.L2-3.3.6 |
| CM.L2-3.4.6 |
| CM.L2-3.4.9 |
| CM.L2-3.4.2 |
| CM.L2-3.4.3 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| IA.L1-3.5.1 |
| IA.L1-3.5.2 |
| IA.L2-3.5.7 |
| IA.L2-3.5.8 |
| IA.L2-3.5.9 |
| IA.L2-3.5.10 |
| IA.L2-3.5.11 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| IA.L2-3.5.5 |
| IA.L2-3.5.6 |
| IR.L2-3.6.1 |
| IR.L2-3.6.2 |
| MA.L2-3.7.2 |
| MA.L2-3.7.5 |
| PE.L1-3.10.1 |
| PS.L2-3.9.2 |
| MP.L2-3.8.9 |
| SC.L2-3.13.12 |
| SC.L2-3.13.3 |
| SC.L2-3.13.7 |
| SC.L2-3.13.9 |
| SC.L2-3.13.14 |
| SC.L2-3.13.15 |
| SI.L2-3.14.3 |
| SI.L2-3.14.7 |
| AC.L3-3.1.1e |
| AC.L3-3.1.2e |
| AC.L3-3.1.3e |
| CM.L3-3.4.2e |
| Microsoft Entra ID Smart Lockout | AC.L2-3.1.8 |
| AC.L2-3.1.11 |
| Privileged Identity Management (PIM) | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L2-3.1.5 |
| AC.L2-3.1.6 |
| AC.L2-3.1.4 |
| AC.L2-3.1.7 |
| AC.L2-3.1.15 |
| AU.L2-3.3.9 |
| IA.L1-3.5.1 |
| IA.L1-3.5.2 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| MA.L2-3.7.1 |
| MA.L2-3.7.2 |
| MA.L2-3.7.5 |
| MA.L2-3.7.6 |
| SC.L2-3.13.3 |
| SC.L2-3.13.4 |
| SI.L2-3.14.7 |
| AC.L3-3.1.2e |
| Microsoft Entra ID Multi-Factor Authentication | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L2-3.1.13 |
| IA.L1-3.5.2 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| MA.L2-3.7.5 |
| MP.L2-3.8.2 |
| MP.L2-3.8.5 |
| PE.L2-3.10.6 |
| MP.L2-3.8.9 |
| SC.L2-3.13.4 |
| SC.L2-3.13.15 |
| Bitlocker | MP.L2-3.8.1 |
| MP.L2-3.8.5 |
| MP.L2-3.8.6 |
| PE.L2-3.10.6 |
| SC.L2-3.13.11 |
| SC.L2-3.13.8 |
| SC.L2-3.13.10 |
| SC.L2-3.13.16 |
| Conditional Access | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L1-3.1.20 |
| AC.L1-3.1.22 |
| AC.L2-3.1.9 |
| AC.L2-3.1.21 |
| AC.L2-3.1.10 |
| AC.L2-3.1.16 |
| AC.L2-3.1.12 |
| AC.L2-3.1.14 |
| AC.L2-3.1.17 |
| AC.L2-3.1.7 |
| AC.L2-3.1.11 |
| AC.L2-3.1.18 |
| AC.L2-3.1.15 |
| AC.L2-3.1.19 |
| AU.L2-3.3.8 |
| AU.L2-3.3.9 |
| CM.L2-3.4.6 |
| CM.L2-3.4.2 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L1-3.5.2 |
| IA.L2-3.5.7 |
| IA.L2-3.5.8 |
| IA.L2-3.5.10 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| IA.L2-3.5.5 |
| IA.L2-3.5.6 |
| MA.L2-3.7.2 |
| MA.L2-3.7.5 |
| MP.L2-3.8.1 |
| MP.L2-3.8.2 |
| MP.L2-3.8.8 |
| MP.L2-3.8.6 |
| PE.L1-3.10.1 |
| PE.L1-3.10.5 |
| PE.L2-3.10.6 |
| PS.L2-3.9.2 |
| SC.L1-3.13.1 |
| SC.L2-3.13.11 |
| SC.L2-3.13.3 |
| SC.L2-3.13.4 |
| SC.L2-3.13.6 |
| SC.L2-3.13.8 |
| SC.L2-3.13.9 |
| SC.L2-3.13.13 |
| SC.L2-3.13.14 |
| SI.L2-3.14.6 |
| AC.L3-3.1.1e |
| Customer Lockbox | AC.L1-3.1.1 |
| IA.L1-3.5.2 |
| MA.L2-3.7.6 |
| SC.L1-3.13.1 |
| Distributed Key Manager | SC.L2-3.13.10 |
| SC.L2-3.13.16 |
| Exchange Admin Center | AC.L1-3.1.22 |
| AC.L2-3.1.3 |
| AU.L2-3.3.3 |
| Intune/Intune Suite | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L1-3.1.20 |
| AC.L1-3.1.22 |
| AC.L2-3.1.9 |
| AC.L2-3.1.21 |
| AC.L2-3.1.10 |
| AC.L2-3.1.16 |
| AC.L2-3.1.12 |
| AC.L2-3.1.14 |
| AC.L2-3.1.3 |
| AC.L2-3.1.17 |
| AC.L2-3.1.13 |
| AC.L2-3.1.7 |
| AC.L2-3.1.11 |
| AC.L2-3.1.18 |
| AC.L2-3.1.15 |
| AC.L2-3.1.19 |
| AU.L2-3.3.2 |
| AU.L2-3.3.1 |
| AU.L2-3.3.3 |
| AU.L2-3.3.9 |
| CA.L2-3.12.1 |
| CA.L2-3.12.3 |
| CM.L2-3.4.1 |
| CM.L2-3.4.9 |
| CM.L2-3.4.2 |
| CM.L2-3.4.3 |
| CM.L2-3.4.4 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L1-3.5.1 |
| IA.L1-3.5.2 |
| IA.L2-3.5.7 |
| IA.L2-3.5.8 |
| IA.L2-3.5.10 |
| IA.L2-3.5.11 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| IA.L2-3.5.5 |
| IA.L2-3.5.6 |
| IR.L2-3.6.2 |
| MA.L2-3.7.1 |
| MA.L2-3.7.2 |
| MA.L2-3.7.5 |
| MP.L2-3.8.1 |
| MP.L2-3.8.2 |
| MP.L2-3.8.7 |
| MP.L2-3.8.8 |
| MP.L2-3.8.5 |
| MP.L2-3.8.6 |
| PE.L1-3.10.1 |
| PE.L1-3.10.3 |
| PE.L1-3.10.5 |
| PE.L2-3.10.2 |
| PE.L2-3.10.6 |
| PS.L2-3.9.2 |
| RA.L2-3.11.1 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SC.L1-3.13.1 |
| SC.L2-3.13.12 |
| SC.L2-3.13.11 |
| SC.L2-3.13.4 |
| SC.L2-3.13.6 |
| SC.L2-3.13.8 |
| SC.L2-3.13.9 |
| SC.L2-3.13.13 |
| SC.L2-3.13.14 |
| SC.L2-3.13.15 |
| SC.L2-3.13.16 |
| SI.L1-3.14.1 |
| SI.L1-3.14.2 |
| SI.L1-3.14.4 |
| SI.L1-3.14.5 |
| AC.L3-3.1.1e |
| AT.L3-3.2.1e |
| IR.L3-3.6.1e |
| Microsoft 365 Admin Center | AC.L1-3.1.2 |
| AC.L2-3.1.5 |
| AC.L2-3.1.6 |
| AC.L2-3.1.18 |
| AU.L2-3.3.6 |
| CM.L2-3.4.9 |
| CM.L2-3.4.2 |
| CM.L2-3.4.5 |
| IA.L1-3.5.2 |
| Microsoft 365 Defender | AT.L2-3.2.1 |
| AT.L2-3.2.2 |
| AT.L2-3.2.3 |
| AU.L2-3.3.1 |
| CA.L2-3.12.3 |
| CM.L2-3.4.6 |
| CM.L2-3.4.3 |
| CM.L2-3.4.7 |
| IR.L2-3.6.1 |
| IR.L2-3.6.2 |
| IR.L2-3.6.3 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SI.L1-3.14.4 |
| SI.L2-3.14.3 |
| AC.L3-3.1.2e |
| AC.L3-3.1.3e |
| CM.L3-3.4.2e |
| CM.L3-3.4.3e |
| IA.L3-3.5.3e |
| Microsoft 365 for Enterprise Test Lab | CM.L2-3.4.4 |
| Microsoft Defender for Cloud Apps | AC.L1-3.1.2 |
| AC.L1-3.1.20 |
| AC.L1-3.1.22 |
| AC.L2-3.1.3 |
| AC.L2-3.1.11 |
| AT.L2-3.2.1 |
| AU.L2-3.3.3 |
| AU.L2-3.3.9 |
| AU.L2-3.3.5 |
| CA.L2-3.12.1 |
| CA.L2-3.12.3 |
| CM.L2-3.4.9 |
| CM.L2-3.4.3 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L2-3.5.10 |
| IA.L2-3.5.6 |
| IR.L2-3.6.1 |
| IR.L2-3.6.2 |
| PS.L2-3.9.2 |
| SC.L1-3.13.1 |
| SC.L2-3.13.8 |
| SC.L2-3.13.15 |
| SC.L2-3.13.16 |
| SI.L1-3.14.2 |
| SI.L1-3.14.4 |
| SI.L1-3.14.5 |
| SI.L2-3.14.3 |
| SI.L2-3.14.6 |
| SI.L2-3.14.7 |
| CM.L3-3.4.1e |
| Microsoft Defender for Endpoint | AC.L2-3.1.21 |
| AC.L2-3.1.11 |
| AC.L2-3.1.18 |
| AC.L2-3.1.19 |
| AU.L2-3.3.3 |
| CA.L2-3.12.1 |
| CA.L2-3.12.2 |
| CA.L2-3.12.3 |
| CM.L2-3.4.1 |
| CM.L2-3.4.9 |
| CM.L2-3.4.2 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L2-3.5.10 |
| IR.L2-3.6.1 |
| MA.L2-3.7.1 |
| MA.L2-3.7.4 |
| MP.L2-3.8.2 |
| MP.L2-3.8.7 |
| MP.L2-3.8.8 |
| MP.L2-3.8.6 |
| PS.L2-3.9.2 |
| RA.L2-3.11.1 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SC.L1-3.13.1 |
| SC.L2-3.13.12 |
| SC.L2-3.13.13 |
| SC.L2-3.13.16 |
| SI.L1-3.14.1 |
| SI.L1-3.14.2 |
| SI.L1-3.14.4 |
| SI.L1-3.14.5 |
| SI.L2-3.14.3 |
| SI.L2-3.14.6 |
| SI.L2-3.14.7 |
| AC.L3-3.1.1e |
| CM.L3-3.4.1e |
| IR.L3-3.6.1e |
| Microsoft Defender for Identity | AC.L2-3.1.3 |
| AT.L2-3.2.1 |
| AU.L2-3.3.5 |
| CM.L2-3.4.9 |
| IA.L2-3.5.6 |
| SI.L2-3.14.6 |
| Microsoft Defender SmartScreen | CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| SI.L1-3.14.5 |
| Compliance Retrieval/NAC 2.0 | AC.L1-3.1.22 |
| AC.L2-3.1.16 |
| AC.L2-3.1.17 |
| AC.L2-3.1.18 |
| Microsoft Entra ID Password Protection | AC.L2-3.1.8 |
| IA.L2-3.5.7 |
| IA.L2-3.5.8 |
| Named Locations | AC.L2-3.1.21 |
| AC.L2-3.1.15 |
| PE.L2-3.10.6 |
| Security Patterns | SC.L2-3.13.2 |
| SC.L3-3.13.2 |
| Threat and Vulnerability Management | CA.L2-3.12.2 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| Windows Hello for Business | IA.L2-3.5.4 |
| SC.L2-3.13.12 |
| Office 365 Message Encryption (OME) | AC.L2-3.1.13 |
| SC.L2-3.13.8 |
| Microsoft Defender for Office 365 | AC.L2-3.1.12 |
| AC.L2-3.1.7 |
| AT.L2-3.2.2 |
| AT.L2-3.2.3 |
| AU.L2-3.3.1 |
| IR.L2-3.6.1 |
| RA.L2-3.11.2 |
| SC.L1-3.13.1 |
| SC.L2-3.13.4 |
| SC.L2-3.13.16 |
| SI.L1-3.14.2 |
| SI.L1-3.14.4 |
| SI.L1-3.14.5 |
| SI.L2-3.14.6 |
| SI.L2-3.14.7 |
| Microsoft 365 Security Center | AU.L2-3.3.9 |
| IR.L2-3.6.2 |
| Teams | AC.L2-3.1.9 |
| AT.L2-3.2.1 |
| CM.L2-3.4.5 |
| SC.L2-3.13.12 |
| SC.L2-3.13.14 |
| SC.L2-3.13.15 |
| Microsoft Graph | AU.L2-3.3.4 |
| AU.L2-3.3.5 |
| IA.L1-3.5.1 |
| IR.L2-3.6.1 |
| Secure Score | CA.L2-3.12.1 |
| CA.L2-3.12.2 |
| CA.L2-3.12.3 |
| RA.L2-3.11.3 |
| Power Automate | AC.L2-3.1.3 |
| AU.L2-3.3.4 |
| CA.L2-3.12.4 |
| CM.L2-3.4.3 |
| CM.L2-3.4.5 |
| SI.L1-3.14.1 |
| Conditional Access | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L1-3.1.20 |
| AC.L1-3.1.22 |
| AC.L2-3.1.9 |
| AC.L2-3.1.21 |
| AC.L2-3.1.10 |
| AC.L2-3.1.16 |
| AC.L2-3.1.12 |
| AC.L2-3.1.14 |
| AC.L2-3.1.17 |
| AC.L2-3.1.7 |
| AC.L2-3.1.11 |
| AC.L2-3.1.18 |
| AC.L2-3.1.15 |
| AC.L2-3.1.19 |
| AU.L2-3.3.8 |
| AU.L2-3.3.9 |
| CM.L2-3.4.6 |
| CM.L2-3.4.2 |
| CM.L2-3.4.5 |
| CM.L2-3.4.7 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L1-3.5.2 |
| IA.L2-3.5.7 |
| IA.L2-3.5.8 |
| IA.L2-3.5.10 |
| IA.L2-3.5.3 |
| IA.L2-3.5.4 |
| IA.L2-3.5.5 |
| IA.L2-3.5.6 |
| MA.L2-3.7.2 |
| MA.L2-3.7.5 |
| MP.L2-3.8.1 |
| MP.L2-3.8.2 |
| MP.L2-3.8.8 |
| MP.L2-3.8.6 |
| PE.L1-3.10.1 |
| PE.L1-3.10.5 |
| PE.L2-3.10.6 |
| PS.L2-3.9.2 |
| SC.L1-3.13.1 |
| SC.L2-3.13.11 |
| SC.L2-3.13.3 |
| SC.L2-3.13.4 |
| SC.L2-3.13.6 |
| SC.L2-3.13.8 |
| SC.L2-3.13.9 |
| SC.L2-3.13.13 |
| SC.L2-3.13.14 |
| SI.L2-3.14.6 |
| AC.L3-3.1.1e |
| Entitlement Management | IA.L2-3.5.5 |
| IA.L2-3.5.6 |
| Microsoft 365 Groups | AC.L1-3.1.1 |
| Direct Access | AC.L2-3.1.12 |
| Customer Key | SC.L2-3.13.10 |
| SC.L2-3.13.16 |
| Insider Risk Management | IR.L2-3.6.1 |
| RA.L2-3.11.1 |
| RA.L2-3.11.3 |
| Azure Virtual Desktop | AC.L2-3.1.14 |
| AC.L2-3.1.13 |
| SC.L2-3.13.7 |
| Microsoft 365 Web Apps | AC.L1-3.1.1 |
| AC.L1-3.1.2 |
| AC.L2-3.1.10 |
| AT.L2-3.2.1 |
| CA.L2-3.12.4 |
| CA.L2-3.12.2 |
| GitHub Advanced Security (Add-On) | RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SC.L2-3.13.13 |
| GitHub AE | AC.L1-3.1.2 |
| AC.L2-3.1.5 |
| AU.L2-3.3.1 |
| CM.L2-3.4.1 |
| CM.L2-3.4.9 |
| CM.L2-3.4.3 |
| CM.L2-3.4.4 |
| CM.L2-3.4.5 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L2-3.5.3 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SC.L2-3.13.11 |
| SC.L2-3.13.10 |
| IA.L3-3.5.1e |
| GitHub Enterprise Cloud | AC.L1-3.1.2 |
| AC.L2-3.1.5 |
| AU.L2-3.3.1 |
| CM.L2-3.4.1 |
| CM.L2-3.4.9 |
| CM.L2-3.4.3 |
| CM.L2-3.4.4 |
| CM.L2-3.4.5 |
| CM.L2-3.4.8 |
| CM.L3-3.4.8 |
| IA.L2-3.5.3 |
| RA.L2-3.11.2 |
| RA.L2-3.11.3 |
| SC.L2-3.13.10 |
| Dynamics 365 | IR.L2-3.6.2 |
| Microsoft 365 Lighthouse | CM.L2-3.4.1 |
| Microsoft Learn | AT.L2-3.2.2 |
| AT.L2-3.2.3 |
| Windows Time Service | AU.L2-3.3.7 |
| Microsoft Defender for Cloud | AU.L2-3.3.1 |
| CM.L2-3.4.7 |
| RA.L2-3.11.1 |
| RA.L2-3.11.3 |
| SI.L1-3.14.1 |
| SI.L1-3.14.4 |
| SI.L2-3.14.3 |
| AC.L3-3.1.2e |
| CM.L3-3.4.1e |
| CM.L3-3.4.2e |
| Microsoft Purview | AC.L1-3.1.20 |
| AC.L1-3.1.22 |
| AC.L2-3.1.5 |
| AC.L2-3.1.6 |
| AC.L2-3.1.3 |
| AC.L2-3.1.7 |
| AT.L2-3.2.2 |
| AT.L2-3.2.3 |
| AU.L2-3.3.1 |
| AU.L2-3.3.7 |
| AU.L2-3.3.8 |
| AU.L2-3.3.9 |
| AU.L2-3.3.5 |
| CM.L2-3.4.1 |
| CM.L2-3.4.7 |
| MA.L2-3.7.3 |
| MP.L2-3.8.4 |
| RA.L2-3.11.1 |
| RA.L2-3.11.3 |
| SI.L1-3.14.1 |
| SI.L1-3.14.4 |
| SI.L2-3.14.3 |
| AC.L3-3.1.3e |
| CM.L3-3.4.2e |
| IA.L3-3.5.2e |