Security

Collapse All

Microsoft Defender for Servers

Q: What servers do I pay for in a Microsoft Defender for Servers subscription?

When you enable Defender for Servers on a subscription, you are charged for all machines based on their power states.

Azure VM power states that are billed include Running, Stopping, and Stopped. Azure VM power states that are NOT billed include Starting, Deallocating, and Deallocated.

For Azure Arc machines, the only power state that is billed is Connected. Azure Arc machine power states that are NOT billed include Connecting, Offline/Disconnected, and Expired.

Q: What are the licensing requirements for Microsoft Defender for Endpoint?

Defender for Endpoint for Servers is included with a Defender for Servers subscription.

Q: Can I get a discount if I already have a Microsoft Defender for Endpoint license?

Yes. If you already have a license for Microsoft Defender for Endpoint for Servers, you do not pay for that part of your Microsoft Defender for Servers Plan 1 or 2 license.

To request your discount:

1. From the Azure portal, select **Support and Troubleshooting** > **Help + support**. Select **Create a support request** and fill in the fields.
2. In *Additional details*, enter details, tenant ID, the number of Defender for Endpoint licenses that were purchased, the expiration date, and all other required fields.
3. Complete the process and select Create.

The discount becomes effective starting on the approval date. It is not retroactive.

Q: What is the free data ingestion allowance for Defenders for Servers?

When Defender for Servers Plan 2 is enabled you get a free data ingestion allowance for specific data types. Learn more about the data ingestion benefit.

Q: Can I enable Defender for Servers on a subset of machines in a subscription?

Yes. You can enable Defender for Servers on specific resources in a subscription. Learn more about planning deployment scope.

Q: How does Defender for Servers collect data?

Defender for Servers uses a number of methods to collect machine information, including agentless machine scanning and the Defender for Endpoint agent. See data collection methods in Defender for Servers to learn how Defender for Servers in Microsoft Defender for Cloud collects data for assessment.

Q: Where does Defender for Servers store my data?

Defender for Servers data is stored in Microsoft Defender for Cloud, and Log Analytics workspace. See Understand data storage and workspaces to learn more about Defender for Cloud stores data.

Q: Does Defender for Servers need a Log Analytics workspace?

Defender for Servers Plan 1 does not depend on Log Analytics. In Defender for Servers Plan 2, you need a Log Analytics workspace to take advantage of the free data ingestion benefit. You also need a workspace to use file integrity monitoring in Plan 2. If you do set up a Log Analytics workspace for the free data ingestion benefit, you need to enable Defender for Servers Plan 2 directly on it.

Q: What if I have Defender for Servers enabled on a workspace but not on a subscription?

The legacy method for onboarding servers to Defender for Servers Plan 2 using a workspace and the Log Analytics agent is no longer supported or available in the portal. To ensure that machines that are currently connected to the workspace remain protected, do the following:

- **On-premises and multicloud machines**: If you previously onboarded on-premises and AWS/GCP machines using the legacy method, connect these machines to Azure as Azure Arc-enabled servers to the subscription with Defender for Servers Plan 2 enabled.
- **Selected machines**: If you used the legacy method to enable Defender for Servers Plan 2 on individual machines, we recommend that you enable Defender for Server Plan 2 on the entire subscription. Then you can exclude specific machines using resource-level configuration.

Q: Which Microsoft Defender for Endpoint plan is supported in Defender for Servers?

Defender for Servers Plan 1 and Plan 2 provides the capabilities of Microsoft Defender for Endpoint Plan 2, including endpoint detection and response (EDR).

Q: For Defender for Servers, do I need to buy a separate anti-malware solution for my machines?

No. With Defender for Endpoint integration in Defender for Servers, you will also get malware protection on your machines. In addition, Defender for Servers Plan 2 provides agentless malware scanning.

On new Windows Server operating systems, Microsoft Defender Antivirus is part of the operating system and will be enabled in *active mode*. For machines running Windows Server with the Defender for Endpoint unified solution integration enabled, Defender for Servers deploys Defender Antivirus in *active mode*. On Linux, Defender for Servers deploys Defender for Endpoint including the anti-malware component and set the component in *passive mode*.

Microsoft Defender for Identity

Q: How does Microsoft prevent malicious insider activities and abuse of high privilege roles?

Microsoft developers and administrators have, by design, been given sufficient privileges to carry out their assigned duties to operate and evolve the service. Microsoft deploys combinations of preventive, detective, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

- Tight access control to sensitive data
- Combinations of controls that greatly enhance independent detection of malicious activity
- Multiple levels of monitoring, logging, and reporting

In addition, Microsoft conducts background verification checks on certain operations personnel, and limits access to applications, systems, and network infrastructure in proportion to the level of background verification. Operations personnel follow a formal process when they are required to access a customer account or related information in the performance of their duties.

Q: Do I have the flexibility to select where to store my data?

No. When your Defender for Identity workspace is created, it is stored automatically in the Azure region that is closest to your Microsoft Entra tenant geographical location. Once your Defender for Identity workspace is created, Defender for Identity data cannot be moved to a different region.

Extended Security Updates

Q: What is the Extended Security Update (ESU) program?

The Extended Security Update (ESU) program is a last resort option for customers who need to run certain legacy Microsoft products past the end of support. They are not intended as a long-term solution, but rather as a temporary bridge to stay secure while one migrates to a newer, supported platform. It includes Critical and/or Important security updates up to three years after the products End of Extended Support date.

Extended Security Updates will be distributed if and when available. ESUs do *not* include new features, customer-requested non-security updates, or design change requests. The ESU program does not extend the product lifecycle or extend complete technical support for the product beyond its lifecycle. For more information, please refer to Support questions for ESUs (https://learn.microsoft.com/lifecycle/faq/extended-security-updates#support-questions-for-esus).

Q: What are the best options for customers to stay secure on the latest versions of Windows Server or SQL Server?

To learn more about planning for end of support or retirement, check out Extended Security Updates for SQL Server and Windows Server (https://www.microsoft.com/windows-server/extended-security-updates). For information on the latest versions of Windows Server and SQL Server and benefits of upgrade, visit the Windows Server (https://www.microsoft.com/windows-server/) and SQL Server https://www.microsoft.com/sql-server/sql-server-2022.

Q: How can I purchase ESUs?

On Azure: Extended Security Updates are free for VMs in Azure. These include destinations such as Azure Virtual Machines (VMs), Dedicated Host, Azure VMware Solution, Nutanix Cloud Clusters on Azure, and the Azure Stack portfolio. Eligible customers can use the Azure Hybrid Benefit (https://azure.microsoft.com/pricing/hybrid-benefit/) (available to customers with active Software Assurance or Server Subscriptions) to obtain discounts on the license of Azure Virtual Machines (IaaS) or Azure SQL Database Managed Instance (PaaS).

On-premises/hybrid environments: Extended Security Updates are available through specific volume licensing (https://www.microsoft.com/licensing/how-to-buy/how-to-buy) programs or through Azure Arc-enabled servers for Windows Server and SQL Server. Contact your Microsoft partner or account team to learn more. ESUs for select Embedded products are available via your embedded device manufacturer. For ESUs available through the Dynamics 365 Cloud Migration offer, customers can purchase via the Cloud Service Provider (CSP) licensing program.

Regardless of where the customer wants to deploy ESUs, coverage will be available for up to three years following the end of support date for a particular product.

Q: How do I install ESU updates?

On Azure: Applicable virtual machines (VMs) hosted in Azure are automatically enabled for ESUs if the VM is configured to receive updates, and these updates are provided free of charge.

On-premises/hybrid: Customers can install ESUs by accessing their multiple activation keys through the M365 Admin Center portal or directly installing ESUs through Azure Arc-enabled servers.

For more information see Windows Server (https://learn.microsoft.com/windows-server/get-started/extended-security-updates-deploy) and SQL Server (https://learn.microsoft.com/sql/sql-server/end-of-support/sql-server-extended-security-updates?view=sql-server-ver15&preserve-view=true) installation.

Q: Eligibility criteria for ESU for Windows Server and SQL Server?

To qualify for ESU on-premises or in hosted environments, your server or operating system must meet one of the following prerequisites:

1. Be covered by an active Software Assurance (SA) plan acquired through any program, such as Enterprise Agreement (EA), Enterprise Agreement Subscription (EAS), Server & Cloud Enrollment (SCE), or Enrollment for Education Solutions (EES).
2. Have active subscription licenses acquired through any program, including Cloud Solution Provider (CSP).
3. Have been acquired as License Included services through a Service Provider License Agreement (SPLA) partner.

Note: License included means that you have obtained Windows Server or SQL Server licenses directly from a SPLA partner, rather than using your own licenses.

Q: How to obtain an ESU license for Windows Server and SQL Server outside of Azure?

Customers have two options for licensing ESU (ESU):

1. **Via Azure Arc enabled servers:** With Extended Security Updates enabled by Azure Arc.

2. **Commercial Licensing:** Acquire Extended Security Updates licenses (SKUs) through a Microsoft Commercial Licensing program.

For maximum flexibility and convenience, we recommend using Azure Arc enabled servers.

You can acquire ESU licenses either directly from Microsoft or from your partner such as an EA Reseller or CSP partner (eligible to sell ESUs as of Oct. 1, 2023 for both types of ESUs mentioned above).

Q: Can you provide deployment scenarios for ESUs?

You can apply ESU enabled by Azure Arc and ESU licenses (SKUs) to any properly licensed server or operating system, whether it is deployed on premises or on non Azure clouds (including hosters). If you are running your OS in another cloud, make sure to adhere to the respective outsourcing or License Mobility policies for the underlying software.

Examples:

1. SPLA Scenario: If you have acquired your software from an SPLA partner, you can cover it with ESU licenses.
2. BYOL Scenario: If you have brought your own licenses to a cloud hosting provider via your Outsourcing policy or License Mobility, you can cover your software with ESU licenses.
3. On premises: If you are running your software on prem, you can cover it with ESU licenses.

Q: How to license with ESUs enabled by Azure Arc for Windows Server 2012 and 2012 R2?

When opting for ESU via Azure Arc-enabled servers for Windows Server 2012 and 2012 R2, you have two licensing choices:

1. vCore Licensing: Pay based on the number of virtual cores (vCores) utilized by the operating system. This option uses the Standard edition rate. If you are operating multiple VMs, the cost will be calculated based on the total number of vCores across all VMs. There is an 8-core minimum per VM for vCore licensing. This option is only available when covering an OS running as a virtual machine.
2. pCore Licensing: Pay based on the number of physical cores (pCores) utilized by the host operating system. This option can use either edition. Note that with pCore licensing, up to 2 guest VMs running on a WS Standard host are covered (additional VMs require additional ESU licenses). With the WS Datacenter host, all VMs are covered without the need for additional licenses. There is a 16-core minimum per server for pCore licensing. This option is available for covering OSs running as a physical host, a virtual machine, or a mix of both.

For ESUs enabled by Azure Arc, you can select either licensing option, irrespective of how the underlying server or operating system is licensed. You can also mix between pCore and vCore licensing for your VMs. Make sure you follow the allowed virtualization entitlements for your underlying software.

Q: How to license with ESUs enabled by Azure Arc for SQL Server?

For SQL Server covered by ESUs enabled Azure Arc, the licensing is based on the number of virtual cores (vCores). If you have multiple VMs, you will need to pay for all the vCores used across those VMs. There is a 4-core minimum per VM.

Special Note for SQL Server 2012: Before you can use Extended Security Updates enabled by Azure Arc for SQL Server 2012, you must first acquire the Year 1 Extended Security Updates SKU through Commercial Licensing. For more details on how to license through Commercial Licensing, please refer to the section titled Licensing with Extended Security Updates licenses (SKUs) through Commercial Licensing.

Q: How back billing for sign ups after the end of support dates works?

For customers who enroll in ESUs enabled by Azure Arc after the end of support dates (July 11, 2023 for SQL Server 2012 Year 2 and October 10, 2023 for Windows Server 2012/R2), they will be billed a one-time upfront charge for the months they missed after the end of support date, with billing coming in at the end of the month. For example, if a customer enrolls in January 2024, they will receive a one-time back-bill for October, November, and December 2023 during their first month.

This also applies if a customer intermittently deactivates ESUs. For example, if a customer enrolls in October 2023, unenrolls in November 2023 and re-enrolls in March 2024, the re-enrollment will trigger back billing for December 2023, January 2024, and February 2024.

Q: What is disaster recovery benefit servers?

With ESU enabled by Azure Arc, you can link paid ESU coverage to your eligible Disaster Recovery Benefit servers without incurring additional cost. Make sure you follow the underlying Disaster Recovery Benefit policy for your software.

Q: Can I onboard later and buy just Year 2 of 2012 ESUs?

No, organizations must purchase prior months/years of ESUs when onboarding late.

Q: Where can I get free ESUs on Azure?

Free ESUs will be available for customers on Azure, which includes workloads running on Azure Virtual Machines, Azure Dedicated Host, Azure VMWare Solutions, Nutanix Cloud Clusters on Azure, and Azure Stack Hub/Edge/HCI.

Q: What editions of SQL Server 2012 and Windows Server 2012/2012 R2 are eligible for ESUs?

The Enterprise and Standard editions of SQL Server for versions 2012 and the Standard, Datacenter, and Embedded editions of Windows Server for versions 2012/2012 R2 are eligible for ESUs.

Q: What do ESUs include?

For SQL Server 2012: ESUs include provision of Security Updates rated "critical" for a maximum of three years after end of support.

For Windows Server 2012/2012 R2: ESUs include provision of Security Updates and "Security Update Severity Rating System" rated "critical" and "important," for a maximum of three years after end of support.

ESUs will be distributed if and when available. ESUs do not include new features, customer-requested non-security hotfixes, or design change requests. However, Microsoft may include

non-security fixes as deemed necessary.

Q: Are customers required to cover all on-premises servers with active Software Assurance to get ESUs on-premises?

No, customers can choose to cover as many 2012/2012 R2 on-premises servers, with Software Assurance, as they need for ESUs.

Q: No, customers can choose to cover as many 2012/2012 R2 on-premises servers, with Software Assurance, as they need for ESUs.?

No. Customers cannot buy ESUs for SQL Server Express or Developer edition. However, they can move their workloads to Azure and get the ESUs for no additional charges above the cost of using the Azure subscription. Also, customers who have ESUs for SQL Server production workloads are permitted to apply updates to their servers running SQL Server Developer edition solely for development and test purposes.

Q: Do I need Software Assurance on my CALs to access servers covered by ESUs?

Yes, customers need to run SQL Server 2012 with the latest Service Pack to apply ESUs. Microsoft will only produce updates which can be applied on the latest Service Pack.

Q: What are the options for SQL Server 2012 as well as Windows Server 2012/2012 R2 customers without Software Assurance?

For customers who do not have Software Assurance, the alternative option to get access to ESUs is to migrate to Azure. For variable workloads, we recommend that customers migrate on Azure via Pay-As-You-Go, which allows for scaling up or down at any time. For predictable workloads, we recommend that customers migrate to Azure via Server Subscription and Reserved Instances.

Customers who need to stay on-premises can purchase ESUs when they have an active Server Subscription via EAS, EES, CSP, or Licenses through an EA or SCE in addition to Software Assurance through those programs. Alternatively, customers can use Software Assurance through Open, Select, or MPSA agreements in addition to product licenses through an EA, EAS, SCE, EES, or Subscription through CSP. Licenses and Software Assurance do not need to be on the same agreement.

Q: Is there a deadline for when servers need to be migrated to Azure, or can customers wait until the end of support dates?

There is no deadline for migration of the Windows Server 2012/R2 or SQL Server 2012 workloads to Azure. However, we recommend customers complete migration before the end of support date so that they do not miss any ESUs. If customers miss a year of ESUs coverage, they may buy coverage for previous years at the same time they buy coverage for a current period.

Q: Can customers cover non-production servers licensed under Visual Studio (MSDN) subscriptions with ESUs for on-premises environments?

Customers who purchase ESUs for production servers may also apply those security updates to servers licensed under Visual Studio (MSDN) subscriptions at no additional cost. There is no limit to the number of MSDN servers a customer can cover. If they purchase ESUs for a production server, those updates can be applied to any number of MSDN servers.

Q: Does Visual Studio (MSDN) subscriptions with ESUs for on-premises environments replace Premium Assurance?

Premium Assurance is no longer available, but we will honor the terms of Premium Assurance for customers who already purchased it.

Q: If existing licenses were bought with Software Assurance on Select or through a Microsoft Products and Services Agreement, can ESUs still be purchased under a different but eligible agreement?

Software Assurance is required as a pre-requisite to ESUs. If you have Software Assurance or an equivalent subscription (even if it is on a different enrollment/program type) then you can buy ESUs for Software Assurance covered servers on your Microsoft Enterprise Agreement (EA), Enterprise Agreement Subscription (EAS), or Server and Cloud Enrollment (SCE).

Q: What happens if Software Assurance is not renewed on time, or at all?

ESU coverage is not required to be co-terminus with Software Assurance coverage, but customers must have at least one month of qualifying Software Assurance coverage remaining at the time a given year of ESUs coverage is purchased.

Q: What happens if a customer has a Windows Server OEM license and wants to add ESU?

ESUs can be purchased by customers with active Software Assurance under the following programs - Enterprise Agreement (EA), Enterprise Subscription Agreement (EAS), Server & Cloud Enrollment (SCE), Enrollment for Education Solutions (EES), or Subscription through programs such as Cloud Solution Provider (CSP).

Apps running on pre-installed Windows Servers are recommended to be migrated to supported OS versions or Windows Server on Azure.

Q: What Azure destinations are eligible for free ESUs?

This currently includes Azure destinations such as Azure virtual machines (VMs), Dedicated Host, Azure VMware Solution, Nutanix Cloud Clusters on Azure, and Azure Stack HCI.

Q: Can customers leverage Azure Hybrid Benefit for SQL Server 2012 as well as Windows Server 2012/2012 R2 versions?

Yes, customers with active Software Assurance or equivalent Server Subscriptions can leverage Azure Hybrid Benefit:

SQL Server: Customers can leverage existing on-premises license investments for discounted prices on SQL Server running on Azure SQL Managed Instance, Azure Virtual Machines, and

Azure SQL Managed Instance enabled by Azure Arc in hybrid environments.

Windows Server: Customers can leverage existing on-premises license investments to save on Azure Virtual Machines.

Customers choosing to move to Azure IaaS can combine Azure Hybrid Benefit savings for SQL Server and Windows Server for increased cost savings.

Q: Can customers get free ESUs on Azure Government regions?

Yes, ESUs will be available on Azure Virtual Machines on Azure Government regions.

Q: How do I get technical support for ESUs for my 2012/2012 R2 server workloads if I am running them on a hosted environment?

The ESUs offer does not include technical support beyond the security updates in scope. For customers who purchased Windows Server 2012/2012 R2 or SQL Server 2012 via SPLA, they should contact the SPLA provider, and that provider can use a Partner Support Agreement. Customers cannot contact Microsoft directly if they purchase through SPLA.

Q: Will the Azure Arc-enabled servers solution work with third party update tools (ex. SolarWinds or Qualys)?

Yes, you have the flexibility to use a first- or third-party solution for the delivery of ESUs. Some common patching solutions include Update Management Center on Azure, Systems Center Configuration Manager, Qualys, SolarWinds, and Tanium.

Q: How will SQL Server ESUs enabled by Azure Arc show up on my bill?

While you can sign up for SQL Server ESUs enabled by Azure Arc any time after June 26, 2023, the billing will automatically start after September 1, 2023. We encourage you to sign up as soon as possible since the protection starts from the moment the ESUs subscription is activated.

Your monthly bill will show the aggregate cost of Extended Security Update subscriptions based on the editions, total number of server cores you subscribed to ESU, and the number of days in the month.

Q: How do I cancel my ESUs subscription if I migrate to Azure in the middle of my subscription?

Your ESUs charges will stop immediately in the following cases:

1. You manually cancelled your subscription for any reason.
2. You migrated your SQL server to Azure; no manual cancellation is needed.
3. You upgraded your SQL server to a newer version; no manual cancellation is needed.

If you cancel your ESUs or unsubscribe without migrating to Azure or upgrading to a newer version, the billing will stop billing immediately, but you will lose access to the future patches.

Microsoft Defender

Q: What platforms are supported by Microsoft Defender products licensed under the user subscription model?

Microsoft Defender products support, but are not limited to the platforms below:

- Windows clients
- macOS
- iOS
- Android

You can find additional information on supported platforms and releases here:

- Onboard client devices (Windows or Mac) to Microsoft Defender for Endpoint - Microsoft Defender for Endpoint | Microsoft Learn
- Microsoft Defender for Endpoint on other platforms - Microsoft Defender for Endpoint | Microsoft Learn
- Microsoft Defender for Endpoint - Mobile Threat Defense - Microsoft Defender for Endpoint | Microsoft Learn

---

Q: Can I use Microsoft Defender products licensed under the user subscription model to protect server products?

No. Defender User Subscription Licenses are for protecting the licensed user's client and/or mobile devices, not an organization's servers. For a list of options for server protection see the list of server applicable licenses above. [View related Product Terms]

Q: Can I protect Linux-based servers with Microsoft Defender for Endpoint (as compared to Defender for servers) products?

No, Linux Server is a server-based product and requires server-based licensing with Defender for servers products.

Q: Can I protect Linux-based client devices with Microsoft Defender for Endpoint products?

Microsoft Defender for Endpoint does not currently support Linux client devices.

Q: What are the server types covered under Microsoft Defender products?

The server products include, but are not limited to:

- Windows Servers
- Linux Server

Q: Does the five-device rule apply to Frontline Worker User Subscription Licenses?

Yes, Frontline Workers User Subscription Licenses have the same provisions as Information Worker User Subscription Licenses and qualify for the five client and/or mobile devices. See relevant Product Terms for Frontline Worker eligibility.

Microsoft Entra External ID

Q: What is happening to Azure AD External Identities?

As of May 1, 2025, Azure AD External Identities P1 and P2 are no longer be available for new purchases. Existing customers can continue using the product. There will be no changes to the product experience and operational commitments. Support will continue for Azure AD External Identities and a simple migration path will be provided when it's available.

Q: What is Azure AD B2B collaboration?

Azure AD B2B collaboration is now part of Microsoft Entra External ID as External ID B2B collaboration. It remains in the same location in the Microsoft Entra admin portal within the Workforce tenant.

Q: What are the external identity types supported by Microsoft Entra?

Microsoft Entra External ID supports all external identities that are not employees or students, including customers, partners, business collaborators, business consumers, guests, contractors, constituents, and citizens.

Microsoft Purview

Q: How do I pay for Microsoft Purview if I'm an Azure Databricks Unity customer?

You pay for Microsoft Purview separately from your Azure Databricks costs. Purview uses its own pay-as-you-go pricing model, similar to how Entra works with Fabric for identity and access. The consumption meters for Purview—especially for Data Governance (Unified Catalog)—are different from Databricks. Purview billing for Unity customers started on January 6, 2025. Learn more here.

Q: Why can't I apply my Azure Databricks SKU purchase toward Microsoft Purview consumption?

Azure Databricks and Microsoft Purview are separate products, so your Databricks SKU can't be used to cover Purview costs.

Q: Can I use my Microsoft Azure Commit to Consume (MACC) agreement toward Microsoft Purview consumption?

Yes. You can apply your MACC balance to Purview's data security and data governance meters. This allows you to leverage your committed spend and any associated discounts toward Purview consumption.

Q: What is the Purview Data Governance consumption model?

Purview Data Governance uses a pay-as-you-go model with two billing dimensions:

- Data Catalog – Charged per asset governed
- Data Management – Billed per processing unit with three SKUs: Basic Standard and Advanced. For more details, please review the pricing FAQ.

Q: What are Premium Templates for Purview Compliance Manager?

Premium Templates are add-on value for Compliance Manager and help

- Translate complex regulatory requirements to specific controls
- Suggest recommended improvement actions
- Provide quantifiable measure of compliance against regulations

Compliance Manager has 350+ regulations in the form of Premium Templates that customers can use to assess their compliance with a wide range of global, regional, and industrial regulations and standards. See a list of Premium Assessments at Microsoft Purview Compliance Manager regulations list | Microsoft Learn.

Q: Can I buy Premium Templates for Purview Compliance Manager if I'm a US government customer with a G1 or G3 license?

Yes, you can. If you're a GCC, GCC High, or DoD customer, you're eligible to purchase Premium Templates.

Q: Can I customize Premium Templates for Purview Compliance Manager and add my own controls if I have an E1 or E3 license?

No, you can't. The Custom Assessments feature—which lets you customize assessment templates for Purview Compliance Manager—is only available with an E5 license.

Q: What is Microsoft Purview Compliance Manager?

Microsoft Purview Compliance Manager helps you simplify compliance and reduce risk. It demystifies compliance and makes it easy for you to manage data protection controls and meet compliance requirements. Even if you are not an expert in complex regulations like GDPR, you can quickly learn the actions recommended to help you progress toward compliance.

With Microsoft Purview Compliance Manager, you can continuously assess and monitor data protection controls, get recommendations on how to reduce compliance risks, and leverage the built-in control mapping to scale your compliance effort across global, industrial, and regional regulations and standards.

Q: What is the difference between Microsoft Compliance Score and Microsoft Purview Compliance Manager?

Microsoft Compliance Manager has now absorbed all the Compliance Score functionality. Compliance Score has now become one of the features of Compliance Manager. Since the September 22, 2020, release of Compliance Manager, you can access Compliance Manager from a single location in Microsoft 365 Compliance Center. Compliance Manager improved the user experience and built more integration with other Microsoft 365 compliance solutions.

Q: What is the difference between Microsoft Compliance Manager and Microsoft Secure Score?

Secure Score is a security analytics tool to help you better understand your security posture, while the compliance score calculated by Compliance Manager provides a broader view of your data protection and compliance posture. Secure Score focuses on the configurable technical controls of a security baseline, while your compliance score contains technical, procedural, and people controls to meet regulatory requirements. Another difference is around the user experience, as each score targets different personas and use scenarios. Your compliance score enables you to track the control implementation and test status and allows you to upload evidence and create audit reports, while Secure Score focuses more on tracking the implementation status automatically and has no need to audit the controls.

Q: Where and how can I access Microsoft Compliance Manager and what license do I need?

You can access Microsoft Compliance Manager in the Microsoft 365 compliance center (compliance.microsoft.com). Compliance Manager is available to all Microsoft 365 and Office 365 enterprise plans (E1/E3/E5) and Business plans and to GCC, GCC High, and DoD customers. You need to have permissions to Microsoft 365 compliance center or explicit permission roles to Compliance Manager to access Microsoft Compliance Score.

Q: What features do I get with Microsoft Compliance Manager based on my license?

If you use an E1 or E3 license, you can access the default Data Protection Baseline assessment. If you use an E5 license, you get access to the Data Protection Baseline plus three built-in assessments: GDPR, NIST 800-53, and ISO 27701. You can also create and manage custom assessments. Microsoft enables E5 product features when your tenant includes at least one E5 license. You can purchase over 150 premium assessments as add-ons.

Q: What is included in the Compliance Score E1/E3 and E5 value?

- E1/E3: Data Protection Baseline.
- E5: Data Protection Baseline + 3 assessments (GDPR, NIST 800-53, and ISO 27001).
- Custom Assessments: No for E1/E3, Yes for E5.
- Ability to purchase Premium Assessments: Yes (Since July 1st, 2021) for both E1/E3 and E5.

Q: I purchased one of the Compliance 'mini suites' introduced in April 2020, how does this affect me?

If you purchased Microsoft 365 E5/A5 eDiscovery and Audit, Microsoft 365 E5/A5 Insider Risk Management, or Microsoft 365 E5/A5 Information Protection and Governance, you can use Compliance Manager. These licenses qualify you as an E5 customer, so you'll have access to the Data Protection Baseline and the three built-in assessments mentioned above.

Q: Which licenses give me access to Compliance Manager features?

- If you have Microsoft 365 E3 (or Office 365 E1/E3 or G3), you can access only the default Data Protection Baseline assessment.

- If you have Microsoft 365 E5 or A5 (including the Microsoft 365 E5/A5 Compliance, Information Protection & Governance, Insider Risk Management, or eDiscovery and Audit SKUs), or Office 365 E5/A5, you'll be able to access the Data Protection Baseline, GDPR, NIST 800-53, and ISO 27001 assessments.
- If you have Microsoft 365 G5 or Office 365 G5, you'll get access to Data Protection Baseline, GDPR, NIST 800-53, ISO 27001, and CMMC Levels 1 through 5.
- The custom assessment feature is available to Microsoft 365 and Office 365 E5, A5, and G5 customers.
- Premium assessments, including FedRAMP Moderate, FedRAMP High, and others, are available for purchase to all Enterprise and Government customers with any license that includes Microsoft Exchange Online.

Q: Can I purchase Microsoft Compliance Manager premium assessments and what do I need first?

Yes, you can purchase premium assessments as long as your subscription includes a Microsoft Exchange Online license.

Q: How many Compliance Manager premium licenses required for my organization?

Any user who benefits from the service needs to be licensed. For example, if all end users need to comply with a regulation like GDPR, then all users should be licensed. If you only need a subset of your users to be covered by the Premium Assessment, then only those users need to be licensed with E5. For instance, if the Department of Work & Pensions needs to comply with NIST for only 50% of their end-users, then only those users should be licensed with E5.

Microsoft Entra ID Governance

Q: Do I need a subscription to Entra ID Governance or Entra Suite if I only want to govern guests?

Yes. Even if you only govern guest users, you must assign at least one Microsoft Entra ID Governance (or Entra Suite) license to an administrator in your tenant. Guest users do not need individual licenses, but your tenant must have a licensed admin to enable governance features.

Q: How are licenses and billing handled in a multi-tenant organization for Entra ID Governance?

Each tenant where you use Entra ID Governance needs its own license (at least one Entra ID Governance or Suite license for an admin). A guest user in a tenant counts toward that tenant's guest meter if they use governance features. If you use a multi-tenant organization (MTO) and bring users in as Members instead of Guests, they will not count as guests for billing. Use MTO to avoid double-billing by keeping internal users as members across tenants.

Q: Can you describe the differences between the identity governance features in Entra ID P2 and Microsoft Entra ID Governance?

Entra ID P2 includes several core identity governance features such as access reviews, entitlement management, and privileged identity management (PIM). Microsoft Entra ID Governance builds on these features and adds advanced capabilities. These include no-code or

low-code identity lifecycle automation, machine learning-assisted access reviews, an actionable dashboard with recommended actions, and enhanced entitlement management that leverages Microsoft Entra Verified ID to confirm digital identities before granting access. In short, Microsoft Entra ID Governance includes all the features of Entra ID P2 and adds more advanced tools, making it a superset of Entra ID P2's identity governance features.

Q: Where can I see a detailed comparison of Entra ID P2 vs. Entra ID Governance features?

Microsoft provides a licensing fundamentals page with a feature comparison table. You can find it on Microsoft Learn here: https://learn.microsoft.com/entra/id-governance/licensing-fundamentals#features-by-license. This table shows which identity governance features are included in Entra ID P2 and which are in Microsoft Entra ID Governance.

Q: I'm currently using identity governance features in Entra ID P2. Do I need to switch to Microsoft Entra ID Governance?

You don't need to switch, your existing identity governance features in Entra ID P2 will continue to work as expected. However, upgrading to Microsoft Entra ID Governance gives you access to enhanced capabilities like lifecycle automation, AI-assisted access reviews, and entitlement management with Verified ID. It's a great way to build on what you already have and take your identity governance to the next level.

Q: Should I choose Microsoft Entra ID Governance or Entra ID P2 for my identity governance needs?

In general, Microsoft Entra ID Governance is the recommended choice if you want a comprehensive identity governance solution. It provides a complete set of capabilities and will receive all new improvements moving forward.

Q: Will the basic identity governance capabilities in Entra ID P2 change over time?

The core features in Entra ID P2 (access reviews, entitlement management, PIM, etc.) will continue to work and Microsoft will maintain them (with security updates and bug fixes). However, no new major features will be added to the P2 tier going forward.

Q: Will the new identity governance features be added to Entra ID P2 or only to Microsoft Entra ID Governance?

New identity governance features, like machine learning-based recommendations and insights, will be added to Microsoft Entra ID Governance. These enhancements won't be included in Entra ID P2, so if you want access to the latest capabilities, we recommend upgrading to Microsoft Entra ID Governance.

Q: What are the prerequisites for using Microsoft Entra ID Governance?

Entra ID Premium Plan 1 (P1) is a prerequisite for Microsoft Entra ID Governance. Customers with Entra ID free or lower licenses can purchase Entra ID P1. Since Entra ID Premium Plan 2 (P2) includes Entra ID P1, P2 customers have the P1 prerequisite to be able to upgrade to Microsoft Entra ID Governance as well.

Q: How do I upgrade from Entra ID P1 to Microsoft Entra ID Governance?

To upgrade, if you already have Entera ID P1, you'll need to purchase Microsoft Entra ID Governance.

Q: How do I upgrade from Entra ID P2 to Microsoft Entra ID Governance?

If you already have Entra ID P2, Microsoft offers a "step-up" license for Entra ID Governance.

Q: I am already licensed for Entra ID P2 – how does this impact my existing licenses if I don't upgrade?

If you choose not to add Microsoft Entra ID Governance, nothing changes for your current P2 licenses. You will continue to have all the identity governance features that come with P2, and they will work just as before. The introduction of Entra ID Governance does not remove or alter any P2 functionality. It's an additive offering. So you can continue using P2 as is. If and when you want the new capabilities, you can decide to purchase the Entra ID Governance add-on. Until then, your P2 users remain as they are (with the set of features P2 provides).

Q: I'm using Entra ID P2's identity governance APIs for automation – will I need to change anything?

No, the existing APIs remain the same. Microsoft Entra ID Governance uses the same underlying platform as P2 for identity governance.

Q: Do I need Microsoft Entra ID Governance licenses for my business guest users?

Yes, customers need Microsoft Entra ID Governance licenses for their business guests. Microsoft is introducing a consumption-based Entra ID Governance Azure subscription meter specifically for business guests. This model uses a monthly active usage (MAU) approach, where customers are billed based on the number of business guest identities that are governed during the month. Customers will pay monthly based on the number of their business guest monthly governed identities.

Q: The new ID Governance license for business guests uses a Monthly Active User (MAU) model. Why doesn't it use a per user per month (PUPM) model like the standard ID Governance license for employees?

Business guests often join and leave as projects start and end, so the number of guest users changes frequently. The MAU model accommodates this fluctuation by letting you acquire a pool of licenses to cover. However, many guest users are active in each month, instead of needing a separate license for each guest every month.

Q: Does the new ID Governance subscription for business guests only apply to the upcoming External ID product?

No. This subscription allows organizations to govern business guest identities in the current external identities solution (B2B), and it will also support the upcoming External ID product.

Q: What about the subset of identity governance features available in Microsoft Entra ID (formerly Azure Active Directory) P2, which is available for free for up to 50,000 users in the current external identities product?

The subset of identity governance features available in Microsoft Entra ID P2 for up to 50,000 users in the current external identities product remains unchanged. However, only Microsoft Entra ID Governance provides a complete identity governance solution.

Q: What does monthly active user (MAU) mean in the context of Microsoft Entra ID Governance?

Monthly active user (MAU) refers to the number of external identities whose identity governance features are used during a given month. The subset of identity governance features available in Microsoft Entra ID P2 for up to 50,000 users through the external identities product remains unchanged. However, only Microsoft Entra ID Governance provides a complete identity governance solution.

Q: Does Entra ID Governance for guests have a free tier of its own?

No, Microsoft Entra ID Governance for guests does not include a free tier. External ID add-ons such as ID Governance require a paid subscription.

Q: Is ID Governance for External ID pre-paid or pay-as-you-go?

This add-on is a consumptive, pay-as-you-go Azure meter (subscription), meaning customers will be billed at the end of the month for the business guest identities that were governed that month.

Q: Are there any prerequisites to govern the identities of business guests with Entra ID Governance?

Yes, the tenant with the business guest identities needs at least one Entra ID Governance license in order for the ID Governance feature set to be enabled for that tenant.

Q: If I'm governing a user in their home tenant, do they need a separate Microsoft Entra ID Governance license when they are a guest in another tenant?

No, users in a multi-tenant organization only need one Microsoft Entra ID Governance license. For example, if a user has a governance license in their home tenant and is invited as a guest to another tenant, they do not need a separate ID Governance for External ID license in the guest tenant. One license covers governance across both their home and guest tenants.

Q: Can I track how many business guests are in my tenant each month?

Microsoft is actively building a feature that will allow you to track the number of business guests in your tenant directly through the Microsoft Entra portal. This capability will help you monitor guest usage more easily each month.

General

Q: Are there licensing prerequisites for the Frontline Worker Security and Compliance offers?

For all Frontline Worker offers/SKUs, users must meet the Frontline Worker license assignment eligibility criteria and be assigned a prerequisite license where applicable as outlined in the Microsoft Product Terms.

Q: When should I use Security standalones instead of the Microsoft 365 F5 Security suite?

If you need features of two or more standalone security products, opting for the Microsoft 365 F5 Security suite is typically more cost-effective than purchasing each standalone separately.

Q: I have a Microsoft 365 F3 subscription. Can I buy SKUs that have "F1" in the name, like Microsoft Defender for Identity F1, or are those only for customers with Microsoft 365 F1?

You can acquire SKUs with "F1" as part of the name for your users licensed with Microsoft 365 F1 or Microsoft 365 F3. Frontline Worker SKUs that have "F1 & F2" as part of their name indicate if they are a "Plan 1" or "Plan 2". For example, Microsoft Defender for Endpoint F1 and Microsoft Defender for Endpoint F2.

For details on licensing prerequisites, refer to the appropriate Online Service specific section of the Microsoft Product Terms.

Q: Are the Frontline Worker Security standalone SKUs available for Education customers?

Microsoft does not offer Education-specific Frontline Worker Security standalone SKUs. Education customers can purchase Commercial Frontline Worker SKUs if they choose, but they will likely find better pricing by purchasing Education-specific SKUs instead.

Q: Are these Frontline Worker Security standalone SKUs available for U.S. Government customers?

There aren't any U.S. Government-specific Frontline Worker Security standalone SKUs right now. U.S. Government customers can still buy the commercial Frontline Worker SKUs if those meet their needs.

Q: I purchased the Microsoft 365 F5 Security add-on and now want the Microsoft 365 F5 Security + Compliance add-on. Can I step-up?

No, there isn't a step-up option available. You can add Microsoft 365 F5 Compliance separately and then switch to Microsoft 365 F5 Security + Compliance at your next enrollment anniversary or renewal.

Q: Are the Microsoft 365 F5 Compliance add-ons and mini-suites available for U.S. Government cloud customers to purchase?

Yes, the Microsoft F5 Compliance, Microsoft F5 Security and Microsoft F5 Security & Compliance add-ons and Microsoft F5 mini-suites (Microsoft 365 F5 Insider Risk Management, Microsoft 365 F5 Information Protection and Governance, and Microsoft 365 F5 eDiscovery & Audit) are available for U.S. Government Cloud customers (GCC, GCC-H and DoD).

Q: Are the Microsoft 365F5 Compliance mini-suites available for charity customers to purchase?

No. Microsoft 365 F5 Compliance mini-suites are not currently available for charity customers.

Q: How can I upgrade from an existing standalone Microsoft Entra solution to the full suite?

An Entra Suite Add-on for Microsoft Entra ID P2/F2 SKU is available if you have Microsoft Entra ID P2/F2 or a suite that includes Entra ID P2/F2 (Microsoft 365 E5/A5; Microsoft 365 E5/A5/F5 Security; Microsoft 365 E5/A5 Enterprise Mobility & Security, Microsoft 365 F5 Security & Compliance).

Microsoft Entra Workload ID Premium

Q: What features do the Workload Identities Premium plan include?

The Workload Identities plan includes Conditional Access , Identity Protection , Access Reviews , App Health Recommendations , App Auth Methods Policies.

Q: How many Entra Workload ID Premium licenses do I need for my workload identities?

You only need to license the workload identities that use premium features. Specifically, license the 'enterprise apps and service principals' shown in the Entra Admin Center. If you use Access Reviews for managed identities, license them based on the number of managed identities involved.

Q: How do I buy the Entra Workload ID Premium plan?

To buy the plan, use an existing Azure or Microsoft 365 subscription or create a new one. Then sign in to the portal or Entra Admin Center (entra.microsoft.com) to complete your purchase.

Q: Do I need to assign licenses to each workload identity?

No, you don’t need to assign licenses individually. One license in your tenant enables all premium features for all workload identities.

Q: How can I track license assignments for workload identities?

Currently, there's no dashboard for tracking license assignments. However, you can monitor Conditional Access policies targeting workload identities in the Insights and Reporting section of the Entra Admin Center.

Q: Can I mix Entra ID P1/P2 and Workload ID Premium licenses in one tenant?

Yes, you can use a mix of Entra ID P1, P2, and Workload ID Premium licenses within a single tenant.

Server Protection

Q: What are the differences among Defender for Endpoint for servers and Defender for Servers P1 and P2?

Defender for Endpoint for servers offers foundational server protection through a standalone license. You will have predictable billing cycles. If there is downtime, the cost remains the same as the base consumption license, but this is purchased on a yearly basis with EA renewals. Billing does not require an Azure subscription to consume.

Defender for Servers Plan 1 also offers foundational server protection, but with consumption pricing. It is billed per hourly use. Server workloads are provisioned dynamically with consumption trends that fluctuate, and for underusage over weekends/holidays. You will only be billed for actual use/uptime. Billing requires an Azure subscription to consume.

Defender for Servers Plan 2 offers advanced server protection with consumption pricing. You will only be billed for actual use/uptime. Billing requires an Azure subscription to consume.

Q: May I assign a Microsoft 365 E5 license to protect my servers, instead of purchasing a separate license?

M365 E5 suite is charged on a per user-basis, and therefore cannot be applied to servers that are charged on a per-server basis as you cannot link a specific user to a server.

Q: Can we assign Microsoft Defender for Endpoint for servers licenses to server devices on Microsoft Admin Center?

You cannot assign Microsoft Defender for Endpoint for servers SKU to servers. You are accountable for maintaining licensing compliance according to your applicable licensing terms.

Q: Is mixed licensing available for server protection?

Mixed licensing is available for Defender for Servers plans. Mixed licensing is currently not supported between Defender for Endpoint for servers and Defender for Servers. Therefore, if you have a hybrid environment of on-premises and cloud servers, you should use Defender for Servers Plan 1 for on-premises and Defender for Servers Plan 2 for cloud servers.

Q: How do I transition servers from Defender for Servers Plan 1 to Plan?

Defender for Servers is enabled on Azure subscriptions and multi-cloud connectors. To upgrade from Defender for Servers Plan 1 to Plan 2, there are two options:

- For Azure VMs and non-Azure machines connected via Azure Arc, you can switch the Defender for Servers plan on your subscription or multi-cloud connector.
- For non-Azure machines connected via MDE direct onboarding, you can deploy Azure Arc and connect these machines to a subscription with Defender for Servers Plan 2 enabled.

Q: How can I migrate from MDE for Server licenses to Defender for Servers Plan 1 or Plan 2?

Once you enable Defender for Servers, it will automatically provide security protection and license coverage for Defender for Endpoint to all virtual machines and non-Azure servers in scope. To avoid double-billing, report your existing MDE for servers standalone licenses so you can receive a discount on Defender for Servers billing. Please follow this guidance to get the discount applied.

Q: Is there a server licensing model for Microsoft Defender for Business (MDB)?

Yes. MDB has a specific license for servers limited to up to 60 seats, as documented here: Get Microsoft Defender for Business - Microsoft Defender for Business | Microsoft Learn. There is no server consumption offer (Microsoft Defender for Cloud) for MDB tenants, only the billed offer.

Q: What offering should I use with Microsoft Defender for Business (MDB) tenants?

When onboarding servers using non-MDB server licenses, features will be limited to the tenant flavor, as currently there's no support for mixed licensing with MDB. More information here: Microsoft Defender for Business frequently asked questions - Microsoft Defender for Business | Microsoft Learn.

Entra ID

Q: Is it possible to have a mixture of Microsoft Entra ID P1 and Microsoft Entra ID Free users in one tenant?

Yes, you can have a mixture of Microsoft Entra ID plans in one tenant.

Q: Where can I find a more detailed feature deployment guide that shows which license(s) I need for Microsoft Entra ID?

You can find a detailed feature deployment guide on the Microsoft Learn page Secure your organization's identities with Microsoft Entra ID.

Q: Do we need a separate Microsoft Entra ID license for the same employee who has different internal identities within the same tenant?

No, you do not need a separate Entra ID license for the same employee with different internal identities within the same tenant.

Q: Do I need a separate Microsoft Entra ID license for the same employee who has multiple internal identities or accounts across different tenants within the same cloud?

No, a separate Entra ID license is not needed in this case either.

Q: What happens if my Microsoft Entra ID P1 or P2 licenses expire?

If your Microsoft Entra ID P1 or P2 licenses expire, you will lose access to the advanced features included with those licenses.

- Microsoft Entra ID P1: This includes all Free features, plus access to both on-premises and cloud resources, advanced administration like dynamic groups, self-service group management, and cloud write-back capabilities for self-service password reset for on-premises users.
- Microsoft Entra ID P2: This includes all Free and P1 features, plus Microsoft Entra ID Protection for risk-based Conditional Access and Privileged Identity Management for monitoring and just-in-time access for administrators.

Q: Can I use Entra ID group assignment (both on-premises and cloud groups) to manage access to Microsoft apps and third-party SaaS applications?

You can create a group with the Microsoft Entra ID free tier, but you will need Microsoft Entra ID P1 or higher to assign a group to a resource.

Q: If I want to control who can create groups or use self-service group management, do all users in my organization need Microsoft Entra ID P1, or just the ones using those features?

Only the admins who configure this feature and the users who are granted group creation permissions need to be licensed for Microsoft Entra ID P1. Self-service group management admins and all members of self-service groups also need to have a Microsoft Entra ID P1 license.

Q: For group expiration, is the Microsoft Entra ID P1 license only needed for those users who would receive the expiration notice?

Yes, the admins who configure this feature and all members of these groups who would receive the expiration notice need a Microsoft Entra ID P1 license. Everyone in a dynamic group also needs to have a Microsoft Entra ID P1 license.

Q: If a Microsoft Entra ID policy blocks all users except a group, do I need Microsoft Entra ID licenses for all users?

Yes, the admins who configure this feature and all users in the group need to be licensed for Microsoft Entra ID.

Q: Is Microsoft Entra ID P2 required for all users covered by a Custom Lockout Policy, or just the Admin who configured it?

Any users covered by the policy to must be licensed with Microsoft Entra ID P2.

Q: What self-service password actions are available through Microsoft Entra ID plans?

The following self-service password actions are available through Entra ID plans:

Any Entra ID plan: Cloud user self-service password change

Entra ID P1 or higher:

- Cloud user self-service password reset
- Hybrid user self-service password change/reset with on-premises write-back

Q: In a scenario where an admin is licensed for Microsoft Entra ID P1/P2, but a user is not, can the admin perform a self-service password reset unlicensed user?

No, per the Product Terms limitations, you may not allow multiple users to directly or indirectly access any Microsoft Azure Service feature that is made available on a per-user basis.

Q: Can Windows Server on-premises users (unsynchronized to Microsoft Entra ID) make use of the Microsoft Entra ID Password protection feature via an installed agent on Windows Server on-premises or do these unsynchronized users need a Microsoft Entra ID license to make use of that functionality?

Users not synchronized to Microsoft Entra ID but active in Microsoft Entra ID automatically benefit from the licenses purchased for the synced users. These users do not require additional licenses.

Q: Does the Microsoft Entra ID Kiosk SKU include the same functionality as the Microsoft Entra ID P1 and P2 SKUs?

Yes, it does.

Q: What are the B2B license requirements for a user who is already licensed in their home tenant?

Please refer to Properties of a B2B guest user - Microsoft Entra External ID | Microsoft Learn for scenarios and user types that require Microsoft Entra External ID licensing.

Q: How does the Microsoft Identity Manager (MIM) license work?

MIM has a server + CAL model:

- The server needs to be appropriately licensed for Windows Server.
- You will need appropriate CALs for any MIM features beyond synchronization. Provisioning that includes the MIM Services requires a CAL. MIM CALs can either be purchased standalone or included in Microsoft Entra ID P1/P2. Office 365 licenses do not include MIM CALs.
- If your employees are only using MIM for user synchronization, they don't need any CALs.

Q: Does Microsoft Entra ID P1 or P2 include the on-premises server access rights equivalent to Windows Server CAL?

No. Entra ID plans do not include CAL equivalency. Refer to CAL and ML Equivalency Licenses for more information.

Q: Which Microsoft Entra ID P1 features are included in Microsoft 365 Business Premium?

Microsoft 365 Business Premium includes the full Microsoft Entra ID P1.

Q: Which standards (SAML, Oauth/OIDC) are free and which ones are part of a Microsoft Entra ID P1 or P2 license?

All standards are free in Microsoft Entra ID P1 and P2 (SAML, Oauth/OIDC) if the apps are part of our app Gallery. If the app is not in the gallery and custom integration is needed, then P1 is required. SAML or not, if there is a custom implementation, it needs a P1 license.

Q: In the Inbound Workday Provisioning scenario, is a Windows CAL required for these users?

Yes, a Windows Server CAL is required if a Microsoft Entra ID P1 or P2 account is to be created for a worker. But note that Workday Cloud provisioning is also available.

Microsoft Defender Experts

Q: What is Microsoft Defender Experts for XDR, which includes Hunting?

Microsoft Defender Experts for XDR is a human-led managed extended detection and response (MXDR) service designed to extend the capacity of your security operations center and accurately respond to incidents. It goes beyond endpoints to provide MXDR services across scoped Microsoft Defender products, investigating alerts and using automation and human expertise to respond to incidents alongside your team. You stay in control and reduce costs, alert noise, and manual processes. Microsoft Defender Experts for XDR includes Microsoft Defender Experts for Hunting.

Q: Are there size requirements to get Defender Experts for XDR?

There is no minimum seat threshold to use Defender Experts for XDR. However, there are seat thresholds for a service delivery manager:

- For fewer than 500 seats: No SDM
- For 500-999 seats: Quarterly SDM engagement
- For 1000+ seats: BAU with monthly SDM engagement

Q: Is Defender Experts for Hunting available as a standalone service?

Yes, Defender Experts for Hunting is available as a standalone service that you can obtain without needing Defender Experts for XDR.

Q: How is Defender Experts for XDR different from Microsoft Defender Experts for Hunting standalone?

Microsoft Defender Experts for XDR provides end-to-end security operations capabilities to monitor, investigate, and respond to security alerts. This service is meant for customers with

constrained security operations centers (SOCs) that are overburdened with alert volume, in need of skilled experts, or both.

Microsoft Defender Experts for Hunting is available in Defender Experts for XDR and as a standalone service, offering proactive threat hunting to find threats. When not part of Defender Experts for XDR, this service is meant for customers that have a robust security operations center and need additional deep expertise in hunting to expose advanced threats.

Q: Do I get a Service Delivery Manager if I purchase only Defender Experts for Hunting as a standalone?

No, you won't receive a Service Delivery Manager if you only have Defender Experts for Hunting. This service does not include a Service Delivery Manager when purchased as a standalone offer.

Q: How many licenses must I purchase for Defender Experts for XDR?

You need to buy Microsoft Defender Experts for XDR for every unique user with a Defender seat.

Q: Can I purchase DEX for XDR licenses only for a subset of my employees?

For example, if your organization has 4,000 frontline workers and 2,000 E5 users, you can purchase licenses to cover only the E5 users.

Q: What products do Microsoft Defender Experts for XDR provide coverage for?

Microsoft Defender Experts for XDR provides coverage for the following products (you must purchase appropriate product licenses to get coverage):

- Microsoft Defender for Endpoint
- Microsoft Defender for Office
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud (servers)
- Microsoft Entra ID

Q: Does Defender Experts provide server coverage?

Yes, Defender Experts for XDR covers hybrid and multi cloud servers. You have two options for Defender Experts for XDR coverage depending on whether you have Microsoft Defender for Endpoint or Microsoft Defender for Cloud deployed for server protection. For servers with Microsoft Defender for Endpoint deployed, you will use Defender Experts for XDR SKU that is license-based (server is considered a user/seat). For servers with Microsoft Defender for Cloud deployed, you will use the Defender Experts for Servers SKU that is consumption-based.

Q: Where is Defender Experts for XDR available?

Defender Experts for XDR is a global service. Microsoft Defender data stays in your existing Microsoft Defender location.

Q: Are local languages supported for Microsoft Defender Experts for XDR?

No, this service is currently delivered in English only.

Q: How do I license Defender Experts for XDR as an EDU customer?

Defender Experts for XDR operates across your entire tenant. You need to license all users—including students, faculty, and staff—and all devices, such as servers and shared machines. Work directly with your Microsoft sales representative to determine the appropriate license counts for students (based on a given year), faculty, and servers in your environment. Don't use the quantity listed under "Student Use Benefit Sub" in your agreement. All standard prerequisite licenses still apply.

Q: Can I buy Defender Experts for Hunting standalone if I have another Managed Detection and Response (MDR) provider?

Yes, it will not directly impact the service. Defender Experts Notifications are consumable via public APIs for you and your partners in your 3rd party Managed Detection and Response (MDR) solution.

Q: Do I need a Defender Experts for XDR or Defender Experts for Hunting license for each of my servers?

No, you only need a minimum of one Defender Experts for XDR or Defender Experts for Hunting license to enable coverage for your Microsoft Defender for Cloud servers. For example, if you want coverage for 500 Defender for Cloud servers, a minimum of 1 Defender Experts for XDR or Defender Experts for Hunting license is required.

Q: What is the 'Scoped Coverage' feature for Defender Experts for XDR (DEX-XDR)?

You can cover a portion of your users instead of all users within your organization. For example, Education customers who want to cover only faculty members and not students, or retail customers who want to cover their corporate staff, but not frontline workers can purchase licenses specifically for scoped users.

Q: Can I cover only a specific group of users with Defender Experts for Hunting (DEX-H)?

No, Defender Experts for Hunting (DEX-H) continues to be tenant-wide. This means that all users within the tenant who are protected with the Defender suite of products must be covered.