Encryption

Article • 12/06/2024

Encryption is an important part of your file protection and information protection strategy. This article provides an overview of encryption for Microsoft 365. Get help with encryption tasks like how to set up encryption for your organization and how to password-protect Microsoft 365 documents.

- For information about certificates and technologies like TLS, see Technical reference details about encryption in Microsoft 365.
- For an overview of how to configure or set up encryption for your organization, see Set up encryption in Microsoft 365 Enterprise.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

What is encryption, and how does it work in Microsoft 365?

The encryption process encodes your data (referred to as plaintext) into ciphertext. Unlike plaintext, ciphertext can't be used by people or computers unless and until the ciphertext is decrypted. Decryption requires an encryption key that only authorized users have. Encryption helps ensure that only authorized recipients can decrypt your content. Content includes files, email messages, calendar entries, and so on.

Encryption by itself doesn't prevent content interception. Encryption is part of a larger information protection strategy for your organization. By using encryption, you help ensure that only authorized parties can use the encrypted data.

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 Microsoft 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 Entra configuration for encrypted content

Article • 01/10/2025

If you protect sensitive items such as emails and documents by using encryption from the Azure Rights Management Service from Microsoft Purview Information Protection, there are some Microsoft Entra configurations that can prevent authorized access to this encrypted content.

Similarly, if your users receive encrypted email from another organization or collaborate with other organizations that encrypt documents by using the Azure Rights Management service, also called *Azure RMS*, your users might not be able to open that email or document because of how their Microsoft Entra ID is configured.

For example:

- A user can't open encrypted email sent from another organization. Or, a user reports that the recipients in another organization can't open an encrypted email that they sent them.
- Your organization collaborates with another organization on a joint project, and project documents are protected by encrypting them, granting access by using groups in Microsoft Entra ID. Users can't open the documents encrypted by users in the other organization.
- Users can successfully open an encrypted document when they are in the office, but can't when they try to access this document remotely and they're prompted for multifactor authentication (MFA).

To ensure access to the encryption service isn't inadvertently blocked, use the following sections to help configure your organization's Microsoft Entra ID, or relay the information to a Microsoft Entra administrator in another organization. Without access to this service, users can't be authenticated and aren't authorized to open encrypted content.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage

Email encryption

Article • 09/08/2023

This article compares encryption options in Microsoft 365 including Microsoft Purview Message Encryption, S/MIME, Information Rights Management (IRM), and introduces Transport Layer Security (TLS).

Microsoft 365 delivers multiple encryption options to help you meet your business needs for email security. This article presents three ways to encrypt email in Office 365. If you want to learn more about all security features in Office 365, visit the Office 365 Trust Center. This article introduces the three types of encryption available for Microsoft 365 administrators to help secure email in Office 365:

- Microsoft Purview Message Encryption.
- Secure/Multipurpose Internet Mail Extensions (S/MIME).
- Information Rights Management (IRM).

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

How Microsoft 365 uses email encryption

Encryption is the process by which information is encoded so that only an authorized recipient can decode and consume the information. Microsoft 365 uses encryption in two ways: in the service, and as a customer control. In the service, encryption is used in Microsoft 365 by default; you don't have to configure anything. For example, Microsoft 365 uses Transport Layer Security (TLS) to encrypt the connection, or session, between two servers.

Here's how email encryption typically works:

- A message is encrypted, or transformed from plain text into unreadable ciphertext, either on the sender's machine, or by a central server while the message is in transit.

Message encryption

Article • 01/10/2025

People often use email to exchange sensitive information, such as financial data, legal contracts, confidential product information, sales reports and projections, patient health information, or customer and employee information. As a result, mailboxes can become repositories for large amounts of potentially sensitive information and information leakage can become a serious threat to your organization.

With Message encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. 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.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

How Message Encryption works

The rest of this article applies to Microsoft Purview Message Encryption. Office 365 Message Encryption (OME) was deprecated.

Microsoft Purview Message Encryption is an online service that's built on Azure Rights Management (Azure RMS) which is part of Microsoft Purview 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.

Users can then encrypt email messages and various attachments by using these options. For a full list of supported attachment types, see "File types covered by IRM policies when they're attached to messages" in Introduction to IRM for email messages.

As an administrator, you can also define mail flow rules to apply this protection. For example, you can create a rule that requires the encryption of all messages addressed to a specific recipient, or that contains specific words in the subject line, and also specify that recipients can't copy or print the contents of the message.

Set up Message Encryption

Article • 04/22/2025

Microsoft Purview Message Encryption allows organizations to share protected email with anyone on any device. Users can exchange protected messages with other Microsoft 365 organizations, as well as third-parties using Outlook.com, Gmail, and other email services.

Follow the steps below to ensure that Microsoft Purview Message Encryption is available in your organization.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Verify that Azure Rights Management is active

Microsoft Purview Message Encryption leverages the protection features in Azure Rights Management Services (Azure RMS), the technology used by Azure Information Protection to protect emails and documents through encryption and access controls.

The only prerequisite for using Microsoft Purview Message Encryption is that Azure Rights Management must be activated in your organization's tenant. If it is, Microsoft 365 activates message encryption automatically and you don't need to do anything.

Azure RMS is also activated automatically for most eligible plans, so you probably don't have to do anything in this regard either. See Activating Azure Rights Management for more information.

> **Important**

Define mail flow rules to encrypt email messages

Article • 04/22/2025

As an administrator that manages Exchange Online, you can create mail flow rules (also known as transport rules) to help protect email messages you send and receive. You can set up rules to encrypt any outgoing email messages and remove encryption from encrypted messages coming from inside your organization or from replies to encrypted messages sent from your organization. You can use the Exchange admin center (EAC) or Exchange Online PowerShell to create these rules. In addition to overall encryption rules, you can also choose to enable or disable individual message encryption options for end users.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

You can't encrypt inbound mail from senders outside of your Exchange Online organization. If a mail flow rule is set up to encrypt mail from outside the organization, the inbound mail will be delivered without encryption.

If you recently migrated from Active Directory RMS to Azure Information Protection, you'll need to review your existing mail flow rules to ensure that they continue to work in your new environment. Also, to use Microsoft Purview Message Encryption with Azure Information Protection, you need to update your existing mail flow rules. Otherwise, your users will continue to receive encrypted mail that uses the previous HTML attachment format instead of the new, seamless experience. If you haven't set up message encryption yet, see Set up Microsoft Purview Message Encryption for information.

For information about the components that make up mail flow rules and how mail flow rules work, see Mail flow rules (transport rules) in Exchange Online. For additional information about how mail flow rules work with Azure Information Protection, see Configuring Exchange Online mail flow rules for Azure Information Protection labels.

> **Important**
>
> For hybrid Exchange environments, on-premises users can send and receive encrypted mail using message encryption only if email is routed through Exchange Online. To configure message encryption in a hybrid Exchange environment, you need to first

Add your organization's brand to your Microsoft Purview Message Encryption encrypted messages

Article • 04/22/2025

Apply your company branding to customize the look of your organization's email messages and the encryption portal. You need to apply sufficient permissions to your work or school account before you can get started, for example Compliance Administrator. You customize branding in one of two ways, using Exchange Online PowerShell or Microsoft Purview Data Loss Prevention (DLP) policies.

For more information about using Microsoft Purview Data Loss Prevention (DLP) policies to add customized branding to encrypted messages, see these resources.

- Supported action: Exchange for details on this action.
- Design a data loss prevention policy if you're new to DLP and want to learn more about what goes into preparing to create a DLP policy.
- Create and Deploy data loss prevention policies for examples on how to create and deploy a DLP policy.

The rest of this article describes using Exchange Online PowerShell.

Use the Get-OMEConfiguration and Set-OMEConfiguration cmdlets in Exchange Online PowerShell to customize these parts of encrypted email messages:

- Introductory text
- Disclaimer text
- URL for Your organization's privacy statement
- Text in the encrypted message portal
- Logo that appears in the email message and encrypted message portal, or whether to use a logo at all
- Background color in the email message and encrypted message portal

You can also revert back to the default look and feel at any time.

If you'd like more control, use Microsoft Purview Advanced Message Encryption to create multiple templates for encrypted emails originating from your organization. Use these templates to control parts of the end-user experience. For example, specify whether recipients can use Google, Yahoo, and Microsoft Accounts to sign in to the encryption portal. Use templates to fulfill several use cases, such as:

- Individual departments, such as Finance, Sales, and so on.

Create a sensitive information type policy for your organization using Microsoft Purview Message Encryption

Article • 04/22/2025

You can use either Exchange mail flow rules or Microsoft Purview Data Loss Prevention (DLP) to create a sensitive information type policy with Microsoft Purview Message Encryption. To create an Exchange mail flow rule, you can use either the Exchange admin center (EAC) or Exchange PowerShell.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

To create the policy by using mail flow rules in the EAC

Sign in to the Exchange admin center and go to **Mail flow** > **Rules**. On the Rules page, create a rule that applies Message Encryption. You can create a rule based on conditions such as the presence of certain keywords or sensitive information types in the message or attachment.

To create the policy by using mail flow rules in Exchange PowerShell

Use a work or school account that has sufficient permissions in your organization, such as Compliance Administrator, connect to Exchange Online PowerShell. For instructions, see Connect to Exchange Online PowerShell. Use the `Set-IRMConfiguration` and `New-TransportRule` cmdlets to create the policy.

Manage message encryption

Article • 04/22/2025

Once you've finished setting up Purview Message Encryption, you can customize the configuration of your deployment in several ways. For example, you can configure whether to enable one-time pass codes, display the **Encrypt** button in Outlook on the web, and more. The tasks in this article describe how.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Manage whether Google, Yahoo, and Microsoft Account recipients can use these accounts to sign in to the encrypted message portal

When you set up the message encryption, users in your organization can send messages to recipients that are outside of your organization. If the recipient uses a *social ID* such as a Google account, Yahoo account, or Microsoft account, the recipient can sign in to the encrypted message portal with a social ID. If you want, you can choose not to allow recipients to use social IDs to sign in to the encrypted message portal.

To manage whether recipients can use social IDs to sign in to the encrypted message portal

1. Connect to Exchange Online PowerShell.
2. Run the Set-OMEConfiguration cmdlet with the SocialIdSignIn parameter as follows:

Advanced Message Encryption

Article • 09/08/2023

Microsoft Purview Advanced Message Encryption is included in Microsoft 365 Enterprise E5, Office 365 E5, Microsoft 365 E5 (Nonprofit Staff Pricing), Office 365 Enterprise E5 (Nonprofit Staff Pricing), and Office 365 Education A5. If your organization has a subscription that does not include Microsoft Purview Advanced Message Encryption, you can purchase it with the Microsoft 365 E5 Compliance SKU add-on for Microsoft 365 E3, Microsoft 365 E3 (Nonprofit Staff Pricing), or the Office 365 Advanced Compliance SKU add-on for Microsoft 365 E3, Microsoft 365 E3 (Nonprofit Staff Pricing), Office 365 SKUs, or the Microsoft 365 E5/A5 Information Protection and Governance SKU add-on for Microsoft 365 A3/E3.

Advanced Message Encryption helps customers meet compliance obligations that require more flexible controls over external recipients and their access to encrypted emails. With Advanced Message Encryption in Office 365, you can control sensitive emails shared outside the organization with automatic policies and track those activities through the encrypted message portal access logs. You configure these policies to identify sensitive information types such as PII, Financial, or Health IDs, or you can use keywords to enhance protection. Once you've configured the policies, you pair policies with custom branded email templates and then add an expiration date for extra control of emails that fit the policy. Also, admins can further control encrypted emails accessed externally through a secure web portal by revoking access to the mail at any time.

You can only revoke and set an expiration date for emails sent to external recipients.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Get started with Microsoft Purview Advanced Message Encryption

The following articles describe how you set up and use Advanced Message Encryption.

Encrypted message portal activity log by Microsoft Purview Advanced Message Encryption

Article • 03/31/2025

Access logs are available for encrypted messages through the encrypted message portal that lets your organization determine when messages are read, and forwarded by your external recipients. To ensure logs are available for any external recipients, you should apply a custom branding template to protected emails sent by your organization to external recipients that enforces a portal experience. See Add your organization's brand to your encrypted messages.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Enabling message access audit logs in PowerShell

Access log can be enabled using Exchange Online PowerShell. The *EnablePortalTrackingLogs* parameter of the **Set-IrmConfiguration** cmdlet specifies whether to enable the audit logs of accessing the encrypted message portal. Valid values are:

- $true: Turn on audit feature.
- $false: Turn off audit feature

Example:

PowerShell

```
Set-IrmConfiguration -EnablePortalTrackingLogs $true
```

To learn more, see Set-IRMConfiguration (ExchangePowerShell).

Set an expiration date for email encrypted by Microsoft Purview Advanced Message Encryption

Article • 04/22/2025

You can use message expiration on emails that your users send to external recipients who use the OME Portal to access encrypted emails. You force recipients to use the OME portal to view and reply to encrypted emails sent by your organization by using a custom branded template that specifies an expiration date in PowerShell.

When you apply your company brand to customize the look of your organization's email messages, you can also specify an expiration for these email messages. With Microsoft Purview Advanced Message Encryption, you can create multiple templates for encrypted emails that originate from your organization. Using a template, you can control how long recipients have access to mail sent by your users.

When an end user receives mail that has an expiration date set, the user sees the expiration date in the wrapper email. If a user tries to open an expired mail, an error appears in the OME portal.

You can only set expiration dates for emails to external recipients.

With Microsoft Purview Advanced Message Encryption, anytime you apply custom branding, Microsoft 365 applies the wrapper to email that fits the mail flow rule to which you apply the template. You can only use expiration if you use custom branding.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Revoke email encrypted by Advanced Message Encryption

Article • 04/22/2025

Email revocation is offered as part of Microsoft Purview Advanced Message Encryption. Microsoft Purview Advanced Message Encryption is included in Microsoft 365 Enterprise E5, Office 365 E5, Microsoft 365 E5 (Nonprofit Staff Pricing), Office 365 Enterprise E5 (Nonprofit Staff Pricing), and Office 365 Education A5. To use the Advanced Message Encryption revocation and expiration functions, enable the **Premium Encryption in Office 365** option in your E5 license.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

This article is part of a larger series of articles about Microsoft Purview Message Encryption.

If a message was encrypted using Microsoft Purview Advanced Message Encryption, and you are a Microsoft 365 admin or you are the sender of the message, you can revoke the message under certain conditions. Admins revoke messages using PowerShell. As a sender, you revoke a message that you sent directly from Outlook on the web. This article describes the circumstances under which revocation is possible and how to do it.

> **Note**
>
> To guarantee that the ability to track and revoke encrypted messages is available, you must add a custom branding template. See Add your organization's brand to your encrypted messages

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Compare versions of message encryption

Article • 03/31/2025

> **Important**
>
> On February 28, 2021, Microsoft deprecated support for AD RMS in Exchange Online. If you've deployed a hybrid environment where your Exchange mailboxes are online and you're using IRM with Active Directory RMS on-premises, you'll need to migrate to Azure. Organizations that have deployed into the GCC Moderate environment are also affected. See "Overview of AD RMS deprecation in Exchange Online" in this article for information.

The rest of this article compares legacy Office 365 Message Encryption (OME) to Microsoft Purview Message Encryption and Microsoft Purview Advanced Message Encryption. Microsoft Purview Message Encryption is merger and newer version of both OME and Information Rights Management (IRM). Unique characteristics of deploying into GCC High are also outlined. The two can coexist in your organization. For information on how the new capabilities work, see Office 365 Message Encryption (OME).

This article is part of a larger series of articles about message encryption. This article is intended for administrators and ITPros. If you're just looking for information on sending or receiving an encrypted message, see the list of articles in Message encryption and locate the article that best fits your needs.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Overview of AD RMS deprecation in Exchange Online

Message encryption FAQ

FAQ

Have a question about how the new message protection capabilities work? Check for an answer here. Also, look at Frequently asked questions about data protection in Azure Information Protection for answers to questions about the data protection service, Azure Rights Management, in Azure Information Protection.

What is Microsoft Purview Message Encryption?

Microsoft Purview Message Encryption combines email encryption and rights management capabilities. Rights management capabilities are powered by Azure Information Protection.

Who can use Microsoft Purview Message Encryption?

You can use Microsoft Purview Message Encryption under the following conditions:

- If you haven't set up Office 365 Message Encryption (OME) or Information Rights Management (IRM) for Exchange.
- If you set up OME and IRM, you can use these steps if you're also using the Azure Rights Management service from Azure Information Protection.
- If you're using Exchange with Active Directory Rights Management service (AD RMS), you can't enable these new capabilities right away. Instead, you need to migrate AD RMS to Azure Information Protection first. When you finish the migration, you can successfully set up Microsoft Purview Message Encryption.

  If you choose to continue to use on-premises AD RMS with Exchange instead of migrating to Azure Information Protection, you can't use Microsoft Purview Message Encryption.

What subscriptions do I need to use Microsoft Purview Message Encryption?

How Exchange Online secures your email secrets

Article • 03/31/2025

This article describes how Microsoft secures your email secrets in its data centers.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

How we secure secret information provided by you

In addition to the Office 365 Trust Center that provides Security, Privacy, and Compliance Information for Office 365, we use a technology called Distributed Key Manager (DKM).

Distributed Key Manager (DKM) is a client-side technology that uses a set of secret keys to encrypt and decrypt information. Only members of a specific security group in Active Directory Domain Services can access those keys in order to decrypt the data that is encrypted by DKM. In Exchange Online, only certain service accounts under which the Exchange processes run are part of that security group. No human is given credentials that are part of this security group and therefore no human has access to the keys that can decrypt these secrets.

For debugging, troubleshooting, or auditing purposes, a data center administrator must request elevated access to gain temporary credentials that are part of the security group. This process requires multiple levels of legal approval. If access is granted, all activity is logged and audited. Access is only granted for a set interval of time after which it automatically expires.

For extra protection, DKM technology includes automated key rollover and archiving. Automated rollover and archiving ensure that you can continue to access your older content without having to rely on the same key indefinitely.

How Exchange Online uses TLS to secure email connections

Article • 11/27/2023

Learn how Exchange Online and Microsoft 365 use Transport Layer Security (TLS) and Forward Secrecy (FS) to secure email communications.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

TLS basics for Microsoft 365 and Exchange Online

Transport Layer Security (TLS), and Secure Sockets Layer (SSL) that came before TLS, are cryptographic protocols. These protocols secure communication over a network by using security certificates to encrypt a connection between computers. TLS supersedes SSL and is often referred to as SSL 3.1. Exchange Online uses TLS to encrypt the connections between Exchange servers and the connections between Exchange servers and other servers. For example, TLS is used to encrypt the connection between Exchange Online and your on-premises Exchange servers or your recipients' mail servers. Once the connection is encrypted, all data sent through that connection is sent through the encrypted channel.

TLS doesn't encrypt the message, just the connection. So, if you forward a message that was sent through a TLS-encrypted connection to a recipient organization that doesn't support TLS encryption, that message isn't necessarily encrypted.

If you want to encrypt the message, use an encryption technology that encrypts the message contents. For example, you can use Microsoft Purview Message Encryption or S/MIME. See Email encryption in Office 365 and Message encryption for information on message encryption in Office 365.

Use TLS in situations where you want to set up a secure channel of correspondence between Microsoft and your on-premises organization or another organization, such as a partner. Exchange Online always attempts to use TLS first to secure your email but

Enhancing mail flow with MTA-STS

Article • 01/15/2025

Support for the SMTP MTA Strict Transport Security (MTA-STS) standard is added to Exchange Online. The standard was developed to ensure that TLS is always used for connections between email servers. It also provides a way for sending servers to validate that the receiving server has a trusted certificate. If either TLS isn't offered or the certificate isn't valid, the sender refuses to deliver messages. These new checks improve the overall security of SMTP and protect against man-in-the-middle attacks.

MTA-STS can be broken down into two scenarios: Inbound and Outbound Protection. Inbound protection covers the protection of domains hosted in Exchange Online with MTA-STS. Outbound protection covers the MTA-STS validations performed by Exchange Online when sending emails to MTA-STS-protected domains.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Outbound Protection

All messages sent outbound from Exchange Online to MTA-STS-protected recipients are being validated with these extra security checks set out by the MTA-STS standard. There's nothing administrators need to do to apply it. Our outbound implementation respects the wishes of the recipient domain owners via their MTA-STS policy. MTA-STS forms part of the security infrastructure of Exchange Online, and it's therefore always turned on (like other core SMTP features).

Outbound MTA-STS may prevent emails from being delivered depending on the results of the MTA-STS validation against the destination domain. If the domain isn't secure and the MTA-STS policy is set to **Enforce**, an NDR may be returned to the sender with one of the following error codes:

Expand table

How SMTP DNS-based Authentication of Named Entities (DANE) works

Article • 07/17/2024

The SMTP protocol is the main protocol used to transfer messages between mail servers and is, by default, not secure. The Transport Layer Security (TLS) protocol was introduced years ago to support encrypted transmission of messages over SMTP. It's commonly used opportunistically rather than as a requirement, leaving much email traffic in clear text, vulnerable to interception by nefarious actors. Furthermore, SMTP determines the IP addresses of destination servers through the public DNS infrastructure, which is susceptible to spoofing and Man-in-the-Middle (MITM) attacks. This vulnerability leads to many new standards being created to increase security for sending and receiving email, one of those standards being DNS-based Authentication of Named Entities (DANE).

DANE for SMTP RFC 7672 uses the presence of a Transport Layer Security Authentication (TLSA) record in a domain's DNS record set to signal a domain and its mail servers support DANE. If there's no TLSA record present, DNS resolution for mail flow works as usual without any DANE checks being attempted. The TLSA record securely signals TLS support and publishes the DANE policy for the domain. So, sending mail servers can successfully authenticate legitimate receiving mail servers using SMTP DANE. This authentication makes it resistant to downgrade and MITM attacks. DANE has direct dependencies on DNSSEC, which works by digitally signing records for DNS lookups using public key cryptography. DNSSEC checks occur on recursive DNS resolvers, the DNS servers that make DNS queries for clients. DNSSEC ensures that DNS records aren't tampered with and are authentic.

Once the MX, A/AAAA and DNSSEC-related resource records for a domain are returned to the DNS recursive resolver as DNSSEC authentic, the sending mail server asks for the TLSA record corresponding to the MX host entry or entries. If the TLSA record is present and proven authentic using another DNSSEC check, the DNS recursive resolver returns the TLSA record to the sending mail server.

After the authentic TLSA record is received, the sending mail server establishes an SMTP connection to the MX host associated with the authentic TLSA record. The sending mail server tries to set up TLS and compare the server's TLS certificate with the data in the TLSA record to validate that the destination mail server connected to the sender is the legitimate receiving mail server. The message is transmitted (using TLS) if authentication succeeds. When authentication fails or if TLS isn't supported by the destination server, Exchange Online will retry the entire validation process beginning with a DNS query for

Legacy information for Office 365 Message Encryption

Article • 04/22/2025

Office 365 Message Encryption is deprecated as of July 1, 2023. If you haven't yet moved your organization to Microsoft Purview Message Encryption, but you have already deployed OME, then the information in this article applies to your organization. Microsoft recommends that you make a plan to move to Microsoft Purview Message Encryption as soon as it is reasonable for your organization. For instructions, see Set up Microsoft Purview Message Encryption. If you want to find out more about how the new message encryption first, see Message encryption. The rest of this article refers to OME behavior before the release of Microsoft Purview 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.

Here are some examples:

- A bank employee sends credit card statements to customers
- An insurance company representative provides policy details to customers
- A mortgage broker requests financial information from a customer for a loan application
- A health care provider sends health care information to patients
- An attorney sends confidential information to a customer or another attorney

Important

Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Set up Azure Rights Management for the previous version of Message Encryption

Article • 09/08/2023

This topic describes the steps you need to follow in order to activate and then set up Azure Rights Management (RMS), part of Azure Information Protection, for use with the previous version of Office 365 Message Encryption (OME). OME has been deprecated.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

This article only applies to the previous version of OME

If you haven't yet moved your organization to Microsoft Purview Message Encryption, but you have already deployed OME, then the information in this article applies to your organization. Microsoft recommends that you make a plan to move to Microsoft Purview Message Encryption as soon as it is reasonable for your organization. For instructions, see Set up Microsoft Purview Message Encryption. If you want to find out more about how the new capabilities work first, see Message Encryption. The rest of this article refers to OME behavior before the release of Microsoft Purview Message Encryption.

Prerequisites for using the previous version of Office 365 Message Encryption

Office 365 Message Encryption (OME), including IRM, depends on Azure Rights Management (Azure RMS). Azure RMS is the protection technology used by Azure Information Protection. To use OME, your organization must include an Exchange Online or Exchange Online Protection subscription that, in turn, includes an Azure Rights Management subscription.

Track and revoke document access

Article • 08/01/2024

Document tracking provides information for administrators about when a protected document was accessed. If necessary, both admins and users can revoke document access for tracked documents.

A document must be registered for tracking before an admin can track access details, including successful access events and denied attempts, and revoke access if needed. See the next section for minimum versions of Office apps for built-in labeling that support file registration the next time they're opened.

> **Note**
>
> Track and revoke features are supported for Office file types only.

Requirements

Use the capabilities table and the row **Document tracking and revocation** to identify the minimum versions of Word, Excel, and PowerPoint that automatically register label-protected local Office documents (if not already registered) the next time they're opened.

PowerShell cmdlets in this article use the AIPService PowerShell module, which you can install from the PowerShell Gallery. You must run Connect-AipService to connect to your tenant before you run any of the documented cmdlets.

Limitations

- Password-protected documents aren't supported by track and revoke features.
- If you attach multiple documents to an email, and then protect the email and send it, each of the attachments gets the same ContentID value. This ContentID value will be returned only with the first file that had been opened. Searching for the other attachments won't return the ContentID value required to get tracking data.

  Additionally, revoking access for one of the attachments also revokes access for the other attachments in the same protected email.

What is Microsoft 365 service encryption?

Article • 12/19/2023

In addition to using volume-level encryption, Exchange Online, Microsoft Teams, SharePoint Online, OneDrive for Business, and Windows 365 Cloud PCs also use service encryption to encrypt customer data.

Service encryption allows for two key management options, Microsoft-managed keys and customer-managed keys.

Service encryption provides multiple benefits:

- Provides a layer of protection for all Microsoft 365 services and Windows 365 Cloud PCs. For Microsoft 365 services, service encryption is an extra layer of protection is on top of BitLocker.
- Provides separation of Windows operating system administrators from access to application data stored or processed by the operating system.
- Includes a Customer Key option that enables multitenant services to provide per-tenant key management.
- Enhances the ability of Microsoft 365 and Windows 365 to meet your specific compliance requirements regarding encryption.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

What are Microsoft-managed keys?

By default, Microsoft manages all cryptographic keys including the root keys for service encryption. This option, called *Microsoft-managed keys*, is enabled by default for Exchange Online, SharePoint Online, OneDrive for Business, and Windows 365 Cloud PCs. Microsoft-managed keys provide default service encryption unless you decide to onboard using Customer Key. If, at a later date, you decide to stop using Customer Key

BitLocker and Distributed Key Manager (DKM) for Encryption

Article • 09/08/2023

Microsoft servers use BitLocker to encrypt the disk drives containing customer data at rest at the volume-level. BitLocker encryption is a data protection feature that is built into Windows. BitLocker is one of the technologies used to safeguard against threats in case there are lapses in other processes or controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer data. In this case, BitLocker eliminates the potential for data theft or exposure because of lost, stolen, or inappropriately decommissioned computers and disks.

BitLocker is deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer data in Exchange Online, SharePoint Online, and Skype for Business. Disk sectors are encrypted with a Full Volume Encryption Key (FVEK), which is encrypted with the Volume Master Key (VMK), which in turn is bound to the Trusted Platform Module (TPM) in the server. The VMK directly protects the FVEK and therefore, protecting the VMK becomes critical. The following figure illustrates an example of the BitLocker key protection chain for a given server (in this case, using an Exchange Online server).

The following table describes the BitLocker key protection chain for a given server (in this case, an Exchange Online server).

Expand table

KEY PROTECTOR	GRANULARITY	HOW GENERATED?	WHERE IS IT STORED?	PROTECTION
AES 256-bit External Key	Per Server	BitLocker APIs	TPM or Secret Safe	Lockbox / Access Control
			Mailbox Server Registry	TPM encrypted
48-digit Numerical Password	Per Disk	BitLocker APIs	Active Directory	Lockbox / Access Control

Overview of service encryption with Microsoft Purview Customer Key

Article • 02/04/2025

Microsoft 365 provides baseline, volume-level encryption enabled through BitLocker and Distributed Key Manager (DKM). Windows 365 Enterprise and Business Cloud PC disks are encrypted with Azure Storage server-side encryption (SSE). Microsoft 365 offers an added layer of encryption for your content through Customer Key. This content includes data from Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive, Microsoft Teams, and Windows 365 Cloud PCs.

BitLocker isn't supported as an encryption option for Windows 365 Cloud PCs. For more information, see Using Windows 10 virtual machines in Intune.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview **roles and permissions**.

How service encryption, BitLocker, SSE, and Customer Key work together

Your Microsoft 365 data is always encrypted at rest in the Microsoft 365 service with BitLocker and DKM. For more information, see How Exchange secures your email secrets. Customer Key provides extra protection against viewing of data by unauthorized systems or personnel, and complements BitLocker disk encryption and SSE in Microsoft data centers. Service encryption isn't 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

Set up Customer Key

Article • 02/03/2025

With Customer Key, you control your organization's encryption keys and then configure Microsoft 365 to use them to encrypt your data at rest in Microsoft's data centers. In other words, Customer Key allows you to add a layer of encryption that belongs to you, with your keys.

Set up Azure before you use Customer Key. This article describes the steps you need to follow to create and configure the required Azure resources and then provides the steps for setting up Customer Key. After you set up Azure, you determine which policy, and therefore, which keys, to assign to encrypt data across various Microsoft 365 workloads in your organization. For more information about Customer Key, or for a general overview, see Overview of Customer Key.

Important

We strongly recommend that you follow the best practices in this article. These are called out as **TIP** and **IMPORTANT**. Customer Key gives you control over root encryption keys whose scope can be as large as your entire organization. This means that mistakes made with these keys can have a broad impact and may result in service interruptions or irrevocable loss of your data.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Important

Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

Before you set up Customer Key

Overview

Article • 02/03/2025

Microsoft 365 Customer Key supports RSA keys that are stored in Managed HSM (Hardware Secure module) which is FIPS 140-2 Level 3 compliant solution. Azure Key Vault Managed HSM is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguards cryptographic keys for your cloud applications, using FIPS 140-2 Level 3-validated HSMs. For more information on Managed HSM, review the Overview.

Set Up Customer Key with Managed HSM

To set up Customer Key with Managed HSM, complete these tasks in the listed order. The rest of this article provides detailed instructions for each task, or links out to more information for each step in the process.

> **Important**
>
> Managed HSM uses a different set of cmdlets from classic Azure Key Vault.

1. Create two new Azure subscriptions
2. Register the required Service Principals

Create a resource group provision, and activate a Managed HSM

When using Azure Key Vault, Customer Key typically requires provisioning three pairs of Key Vaults (six in total)—one pair for each workload. In contrast, if you use Managed HSM, you only need to provision two instances (one per subscription), regardless of how many of the three workloads you use.

Follow the instructions found in the Managed HSM Quickstarts to provision and activate your managed HSM.

Manage Customer Key

Article • 02/03/2025

After you set up Customer Key, create and assign one or more data encryption policies (DEPs). After assigning your DEPs, manage your keys as described in this article. Learn more about Customer Key in the related articles.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview **roles and permissions**.

Create a DEP for use with multiple workloads for all tenant users

Before you begin, ensure that you completed the tasks required to set up Customer Key. For information, see Set up Customer Key. To create the DEP, you need the Key Vault URIs you obtained during setup. For information, see Obtain the URI for each Azure Key Vault key.

To create a multi-workload DEP, follow these steps:

1. On your local computer, using a work or school account that has compliance admin permissions in your organization, connect to Exchange Online PowerShell.

2. To create a DEP, use the New-M365DataAtRestEncryptionPolicy cmdlet.

```
PowerShell

New-M365DataAtRestEncryptionPolicy -Name <PolicyName> -AzureKeyIDs
<KeyVaultURI1, KeyVaultURI2> [-Description <String>]
```

Roll or rotate a Customer Key or an availability key

Article • 02/04/2025

Caution

Only roll an encryption key that you use with Customer Key when your security or compliance requirements dictate that you must roll the key. **Do not delete or disable any keys that are or were associated with policies, including older versions of keys that you used.** When you roll your keys, there is content encrypted with the previous keys. For example, while active mailboxes are re-encrypted frequently, inactive, disconnected, and disabled mailboxes may still be encrypted with the previous keys. Microsoft SharePoint performs backup of content for restore and recovery purposes, so there may still be archived content using older keys.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

About rolling the availability key

Microsoft doesn't expose direct control of the availability key to customers. For example, you can only roll (rotate) the keys that you own in Azure Key Vault. Microsoft 365 rolls the availability keys on an internally defined schedule. There is no customer-facing, service-level agreement (SLA) for these key rolls. Microsoft 365 rotates the availability key using Microsoft 365 service code in an automated process. Microsoft administrators may initiate the roll process. The key is rolled using automated mechanisms without direct access to the key store. Access to the availability key secret store isn't provisioned to Microsoft administrators. Availability key rolling applies the same mechanism used to initially generate the key. For more information about the availability key, see Understand the availability key.

Important

Learn about the availability key for Customer Key

Article • 02/03/2025

The availability key is a root key automatically generated and provisioned when you create a data encryption policy. Microsoft 365 stores and protects the availability key. The availability key is functionally like the two root keys that you supply for Customer Key. The availability key wraps the keys one tier lower in the key hierarchy. Unlike the keys that you provide and manage in Azure Key Vault, you can't directly access the availability key. Microsoft 365 automated services manage the availability key programmatically. These services initiate automated operations that never involve direct access to the availability key.

The primary purpose of the availability key is to provide recovery capability from the unanticipated loss of root keys that you manage. Loss could be a result of mismanagement or malicious action. If you lose control of your root keys, contact Microsoft Support to get assistance with the process of recovery using the availability key. Use the availability key to migrate to a new Data Encryption Policy with new root keys you provision.

Storage and control of the availability key are deliberately different from Azure Key Vault keys for three reasons:

- The availability key provides a recovery, "break-glass" capability if control over both Azure Key Vault keys is lost.
- The separation of logical controls and secure storage locations provides defense-in-depth and protects against the loss of all keys, and your data, from a single attack or point of failure.
- The availability key provides a high-availability capability if Microsoft 365 services are unable to reach keys hosted in Azure Key Vault due to transient errors. This rule only applies to Exchange service encryption. Microsoft SharePoint and OneDrive never use the availability key unless you explicitly instruct Microsoft to initiate the recovery process.

Sharing the responsibility to protect your data using various protections and processes for key management ultimately reduces the risk that all keys (and therefore your data) are permanently lost or destroyed. Microsoft provides you with sole authority over the disablement or destruction of the availability key when you leave the service. By design, no one at Microsoft has access to the availability key: it's only accessible by Microsoft 365 service code.

Microsoft Purview Customer Lockbox

Article • 02/03/2025

This article provides deployment and configuration guidance for Customer Lockbox. Customer Lockbox supports requests to access data in Exchange Online, SharePoint, OneDrive, Teams, and Windows 365. Additionally, all Microsoft 365 Copilot interactions are covered by Customer Lockbox through the support available for Exchange Online. To recommend support for other services, submit a request at Feedback Portal.

To see the options for licensing your users to benefit from Microsoft Purview offerings, see the Microsoft 365 licensing guidance for security & compliance.

Customer Lockbox ensures that Microsoft can't access your content to do service operations without your explicit approval. Customer Lockbox brings you into the approval workflow process that Microsoft uses to ensure only authorized requests allow access to your content. To learn more about Microsoft's workflow process, see Privileged access management.

Occasionally, Microsoft engineers help troubleshoot and fix issues that arise with the service. Usually, engineers fix issues using extensive telemetry and debugging tools Microsoft has in place for its services. However, some cases require a Microsoft engineer to access your content to determine the root cause and fix the issue. Customer Lockbox requires the engineer to request access from you as a final step in the approval workflow. This gives you the option to approve or deny the request for your organization, and provide direct-access control to your content.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview **roles and permissions**.

What is Double Key Encryption (DKE)?

Article • 07/18/2024

> *Applies to: Microsoft Purview Double Key Encryption, Microsoft Purview , Azure Information Protection*
>
> *Service description for: Microsoft Purview*

Double Key Encryption (DKE) enables you to protect your highly sensitive data to meet specialized requirements. DKE lets you maintain control of your encryption keys. It uses two keys to protect data; one key in your control and a second key you store securely in Microsoft Azure. You maintain control of one of your keys using the Double Key Encryption service. Viewing data protected with Double Key Encryption requires access to both keys.

DKE helps you meet regulatory requirements across several regulations and standards such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Russia's data localization law – Federal Law No. 242-FZ, Australia's Federal Privacy Act 1988, and New Zealand's Privacy Act 1993.

After you set up the DKE service and your keys, you apply protection to your highly sensitive content by using sensitivity labels.

Supported deployment scenarios

DKE supports several different configurations including both cloud and on-premises deployments. These deployments help to ensure that encrypted data remains opaque wherever you store it.

You can host the Double Key Encryption service used to request your key in a location of your choice (on-premises key management server or in the cloud). You maintain the service as you would any other application. Double Key Encryption lets you control access to the Double Key Encryption service. You can store your highly sensitive data on-premises or move it to the cloud. Double Key Encryption gives you the control to store your data and key in the same geographical location.

For more information about the default, cloud-based tenant root keys, see Planning and implementing your Azure Information Protection tenant key.

Set up Double Key Encryption

Article • 01/21/2025

> *Applies to: Microsoft Purview Double Key Encryption, Microsoft Purview , Azure Information Protection*

> *Service description for: Microsoft Purview*

Follow these general steps to set up DKE. Once you complete these steps, your end users can protect your highly sensitive data with Double Key Encryption.

1. Deploy the DKE service as described in this article. Ensure your environment meets the minimum system and licensing requirements. For more information, see System and licensing requirements for DKE.

2. Create a label with Double Key Encryption. In the Microsoft Purview portal, navigate to **Information protection** and create a new label with Double Key Encryption. See Restrict access to content by using sensitivity labels to apply encryption.

3. Configure the registry on client devices so you can use Double Key Encryption labels. Next, protect your data by selecting the Double Key Encrypted label from the Sensitivity ribbon in Microsoft Office.

There are several ways you can complete some of the steps to deploy Double Key Encryption. This article provides detailed instructions so that less experienced admins successfully deploy the service. If you're comfortable doing so, you can choose to use your own methods.

Deploy DKE

This article and the deployment video use Azure as the deployment destination for the DKE service. If you're deploying to another location, you need to provide your own values.

Follow these general steps to set up Double Key Encryption for your organization.

1. Install software prerequisites for the DKE service
2. Clone the Double Key Encryption GitHub repository
3. Modify application settings
4. Generate test keys

Double Key Encryption FAQ

FAQ

"Have questions about how Double Key Encryption works that we didn't cover elsewhere? Check for an answer here."

What Microsoft 365 Apps can I use with DKE?

You can use DKE labels to protect documents using the desktop versions of Word, Excel, PowerPoint, and Outlook on Windows. To ensure that you're using a supported version of Office apps, see the capabilities tables and the row **Double Key Encryption (DKE)**.

Can I use Double Key Encryption with Microsoft Office built-in sensitivity labeling?

Yes! Use can use built-in sensitivity labeling with Office apps. For information, see the capabilities tables and the row **Double Key Encryption (DKE)**. While you can use the information protection client to protect documents with Double Key Encryption for now, this method will be deprecated in the future.

How is Double Key Encryption different from the existing hold your own key (HYOK) solution?

Double Key Encryption encrypts your data with two keys. Your encryption key is in your control and the second key is stored in Microsoft Azure, allowing you to move your encrypted data to the cloud. HYOK protects your content with only one key and the key is always on premises.

Can Double Key Encrypted documents be shared externally?

Set up Information Rights Management (IRM) in SharePoint admin center

Article • 04/22/2025

Within SharePoint in Microsoft 365, IRM protection is applied to files at the list and library level. Before your organization can use IRM protection, you must first set up Rights Management. IRM relies on the Azure Rights Management service from Azure Information Protection to encrypt and assign usage restrictions. Some Microsoft 365 plans include Azure Rights Management, but not all. To learn more, read How Office applications and services support Azure Rights Management.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview trials hub. Learn details about signing up and trial terms.

Turn on IRM service using SharePoint admin center

Before your organization can IRM-protect SharePoint lists and libraries, you must first activate the Rights Management service for your organization. To learn how, see Activating Azure Rights Management. You must use a work or school account that has sufficient administrator privileges to enable the Rights Management service, such as site owner or SharePoint admin. Otherwise, you can't use IRM features with SharePoint.

After you activate the Rights Management service, sign in to the SharePoint admin center to turn on IRM.

1. Sign in to SharePoint.
2. Select the app launcher icon and choose **Admin** to open the Microsoft 365 admin center. (If you don't see the Admin tile, your work or school account doesn't have

Technical reference details about encryption

Article • 05/06/2025

Refer to this article for information about certificates, technologies, and TLS cipher suites used for encryption in Microsoft 365. This article also provides details about planned deprecations.

- If you're looking for overview information, see Encryption in Microsoft 365.
- If you're looking for setup information, see Set up encryption in Microsoft 365 Enterprise.
- For specific information about TLS 1.1 and 1.0 deprecation, see Disabling TLS 1.0 and 1.1 for Microsoft 365.
- For information about cipher suites supported by specific versions of Windows, see Cipher Suites in TLS/SSL (Schannel SSP).
- For certificate chains, see Microsoft 365 encryption chains and Microsoft 365 encryption chains - DOD and GCC High.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Microsoft Office 365 certificate ownership and management

You don't need to purchase or maintain certificates for Office 365. Instead, Office 365 uses its own certificates.

Current encryption standards and planned deprecations

To provide best-in-class encryption, Office 365 regularly reviews supported encryption standards. Sometimes, old standards are deprecated as they become out of date and less secure. This article describes currently supported cipher suites and other standards and details about planned deprecations.

Azure Certificate Authority details

Article • 03/31/2025

This article outlines the specific root and subordinate Certificate Authorities (CAs) that are employed by Azure's service endpoints. It is important to note that this list is distinct from the trust anchors provided on Azure VMs and hosted services, which leverage the trust anchors provided by the operating systems themselves. The scope includes government and national clouds. The minimum requirements for public key encryption and signature algorithms, links to certificate downloads and revocation lists, and information about key concepts are provided below the CA details tables. The host names for the URIs that should be added to your firewall allowlists are also provided.

Certificate Authority details

Any entity trying to access Microsoft Entra identity services via the TLS/SSL protocols will be presented with certificates from the CAs listed in this article. Different services may use different root or intermediate CAs. The following root and subordinate CAs are relevant to entities that use certificate pinning.

How to read the certificate details:

- The Serial Number (top string in the table) contains the hexadecimal value of the certificate serial number.
- The Thumbprint (bottom string in the table) is the SHA1 thumbprint.
- CAs listed in italics are the most recently added CAs.

Root and Subordinate CAs list

Root Certificate Authorities

Expand table

Certificate Authority	Serial Number / Thumbprint
DigiCert Global Root CA	0x083be056904246b1a1756ac95991c74a A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436
DigiCert Global Root G2	0x033af1e6a711a9a0bb2864b11d09fae5 DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Disabling TLS 1.0 and 1.1 for Microsoft 365

Article • 01/16/2025 •

Applies to: Microsoft 365 Apps for enterprise, Office 365 Business, Office 365 Personal, Office Online Server, Office Web Apps

> **Important**
>
> We have already disabled TLS 1.0 and 1.1 for most Microsoft 365 services in the world wide environment. For Microsoft 365 operated by 21 Vianet, TLS 1.0/1.1 was disabled on June 30, 2023.

As of October 31, 2018, the Transport Layer Security (TLS) 1.0 and 1.1 protocols are deprecated for the Microsoft 365 service. The effect for end-users is minimal. This change has been publicized for over two years, with the first public announcement made in December 2017. This article is only intended to cover the Office 365 local client in relation to the Office 365 service but can also apply to on-premises TLS issues with Office and Office Online Server/Office Web Apps.

For SharePoint and OneDrive, you'll need to update and configure .NET to support TLS 1.2. For information, see How to enable TLS 1.2 on clients.

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Office 365 and TLS overview

The Office client relies on the Windows web service (WINHTTP) to send and receive traffic over TLS protocols. The Office client can use TLS 1.2 if the web service of the local computer can use TLS 1.2. All Office clients can use TLS protocols, as TLS and SSL protocols are part of the operating system and not specific to the Office client.

On Windows 8 and later versions

Disabling TLS 1.0 and 1.1 in Microsoft 365 GCC High and DoD

Article • 01/13/2025 • Applies to: Office 365 Business

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Summary

In order to comply with the latest compliance standards for the Federal Risk and Authorization Management Program (FedRAMP), we are disabling Transport Layer Security (TLS) versions 1.1 and 1.0 in Microsoft 365 for GCC High and DoD environments. This change was previously announced through Microsoft Support in Preparing for the mandatory use of TLS 1.2 in Office 365.

The security of your data is important, and we are committed to transparency about changes that could affect your use of the service.

Although the Microsoft TLS 1.0 implementation has no known security vulnerabilities, we remain committed to the FedRAMP compliance standards. Therefore, we disabled TLS 1.1 and 1.0 in Microsoft 365 in GCC High and DoD environments on January 15, 2020.

More information

Starting on January 15, 2020, Microsoft 365 in the GCC High and DoD environments will disable TLS 1.1 and 1.0.

By January 15, 2020, all combinations of client servers and browser servers should use TLS version 1.2 (or a later version) to make sure that all connections can be made without issues to Microsoft 365. This may require updates to certain combinations of client servers and browser servers.

For SharePoint and OneDrive, you'll need to update and configure .NET to support TLS 1.2. For information, see How to enable TLS 1.2 on clients.

Preparing for TLS 1.2 in Office 365 and Office 365 GCC

Article • 01/16/2025 • Applies to: Office 365 Business

> **Tip**
>
> If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the **Microsoft Purview trials hub**. Learn details about **signing up and trial terms**.

Summary

To provide the best-in-class encryption to our customers, Microsoft has deprecated Transport Layer Security (TLS) versions 1.0 and 1.1 in Office 365 and Office 365 GCC. We understand that the security of your data is important, and we're committed to transparency about changes that may affect your use of the TLS service.

The Microsoft TLS 1.0 implementation has no known security vulnerabilities. But because of the potential for future protocol downgrade attacks and other TLS vulnerabilities, we discontinued support for TLS 1.0 and 1.1 in Microsoft Office 365 and Office 365 GCC.

For information about how to remove TLS 1.0 and 1.1 dependencies, see the following white paper: Solving the TLS 1.0 problem.

After you upgrade to TLS 1.2, make sure that the cipher suites you're using are supported by Azure Front Door. Microsoft 365 and Azure Front Door have slight differences in cipher suite support. For details, see What are the current cipher suites supported by Azure Front Door?.

More information

We began deprecation of TLS 1.0 and 1.1 as of January 2020. Any clients, devices, or services that connect to Office 365 through TLS 1.0 or 1.1 in our DoD or GCC High instances are unsupported. For our commercial customers of Office 365, deprecation of TLS 1.0 and 1.1 began October 15, 2020 and rollout continued over the following weeks and months.