# Enterprise Vault™ Setting up Exchange Server and Office 365 for SMTP Archiving

12.1 and later

VERITAS™

# Enterprise Vault™: Setting up Exchange Server and Office 365 for SMTP Archiving

Last updated: 2023-09-05.

## Legal Notice



Veritas Technologies LLC, 2625 Augustine Drive, Santa Clara, CA 95054

https://www.veritas.com

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

| | |
|---|---|
| Worldwide (except Japan) | CustomerCare@veritas.com |
| Japan | CustomerCare_Japan@veritas.com |

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/docs/100040095

## Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

https://www.veritas.com/community

# Contents

Chapter 1

# Configuring Exchange Server for an Enterprise Vault SMTP Archiving solution

This chapter includes the following topics:



## About using Enterprise Vault SMTP Archiving for Exchange Server journaling

You can archive Exchange journal mail using either of the following methods:

- Using Enterprise Vault Exchange Journal Archiving. With this solution, Exchange sends journal mail to journal mailboxes that are hosted on Exchange Mailbox servers. Enterprise Vault Exchange Journaling tasks continually collect the

journal data from the journal mailboxes and store it in Enterprise Vault journal archives.

- Using Enterprise Vault SMTP Archiving. Exchange Server uses an Exchange Send Connector to send the journal mail direct to Enterprise Vault SMTP servers. Enterprise Vault archives the journal mail using Enterprise Vault SMTP Archiving. With this solution there is no need for the journal mail to go to a dedicated Exchange Server journal mailbox first. This can significantly reduce the configuration complexity and storage requirement on Exchange Servers.

This chapter describes how to configure Exchange Server to send journal mail direct to Enterprise Vault SMTP Archiving.

This document does not describe how to set up Enterprise Vault SMTP Archiving. The manual, *Setting up SMTP Archiving*, contains detailed instructions on how to configure this feature.

For additional information on Enterprise Vault SMTP Archiving, such as best practices and performance, see the documents on the Veritas support website, http://www.veritas.com/docs/000004016.

For information on how to set up Enterprise Vault Exchange Journal Archiving, see the manual, *Setting up Exchange Server Archiving*.

# Summary of steps

Table 1-1 summarizes the steps required to configure Exchange Server 2013 to send journal mail direct to Enterprise Vault SMTP servers.

**Table 1-1** Summary of configuration steps on Exchange Server

| Step | Task | Further information |
|---|---|---|
| 1 | Create a remote domain for the SMTP address to which Exchange will send journal mail. | You can use PowerShell or the Exchange Admin Center to create the domain. The example given in this document uses PowerShell.<br>See "Creating a remote domain using the Exchange Management shell" on page 8. |
| 2 | Create a contact with the target SMTP address. | You configure this SMTP address as a target address in Enterprise Vault SMTP Archiving.<br>See "Creating a recipient mail contact in the remote domain" on page 9. |

**Table 1-1** Summary of configuration steps on Exchange Server *(continued)*

| Step | Task | Further information |
|---|---|---|
| 3 | Create a Send Connector for the remote domain. | See "Creating a Send Connector for the remote domain" on page 11. |
| 4 | Set up standard journaling or premium journaling to send the journal mail to the SMTP address. | Do not start journaling on Exchange Servers until you have finished configuring the Enterprise Vault SMTP servers.<br>See "Setting up Exchange Server journaling" on page 16. |
| 5 | Set up Enterprise Vault SMTP Archiving servers. | Detailed configuration instructions are given in the manual, *Setting up SMTP Archiving*.<br>See "Points to note when setting up Enterprise Vault SMTP Archiving servers" on page 19. |

# Creating a remote domain using the Exchange Management shell

Create the remote domain for the SMTP address to which the Exchange Server will send journal mail. The remote domain must conform to the following guidelines:

- The domain must not exist in your Exchange organization.
- The domain must not be one that can be resolved or routed to from inside or outside of your organization.

A suitable example domain might be evsmtp.local.

**To create a remote domain**

1. Open the Exchange Management shell, and enter the following command:

   ```
   New-RemoteDomain -DomainName <domain name> -Name "<domain
   description>"
   ```

   where

   *<domain name>* is the domain, for example, **evsmtp.local**.

   *<domain description>* describes what the domain is used for, for example, **"SMTP Archiving"**.

2. Enter the following command to enable auto-forwarding and disabled TNEF encoding:

   ```
   Get-RemoteDomain | Where {$_.DomainName -eq "<domain name>"} |
   Set-RemoteDomain -TNEFEnabled $false -AutoForwardEnabled $true
   ```

3. Enter the following command to verify the settings:

   ```
   Get-RemoteDomain | Where {$_.DomainName -eq "<domain name>"} |
   Format-table Name, DomainName, TNEFEnabled, AutoForwardEnabled
   ```

# Creating a recipient mail contact in the remote domain

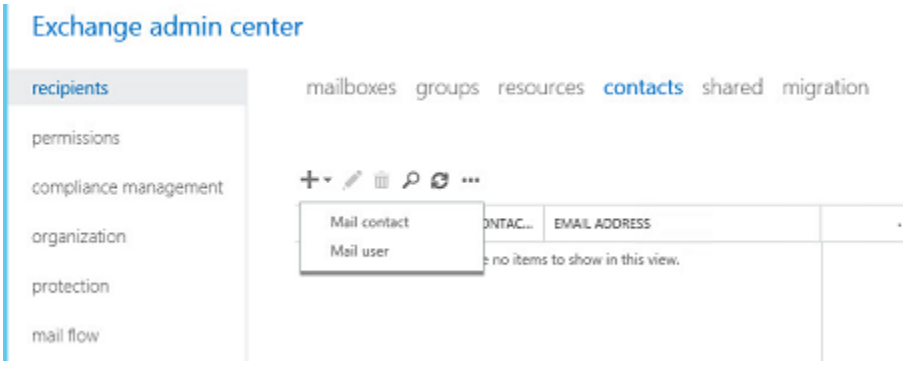
Create a mail contact in the remote domain. When configuring Enterprise Vault SMTP Archiving servers, you configure this contact's address as the SMTP target address.

The number of SMTP target addresses that you configure depends on the architecture of your planned archiving solution. For example, you may want to use a different target address for each mailbox database.

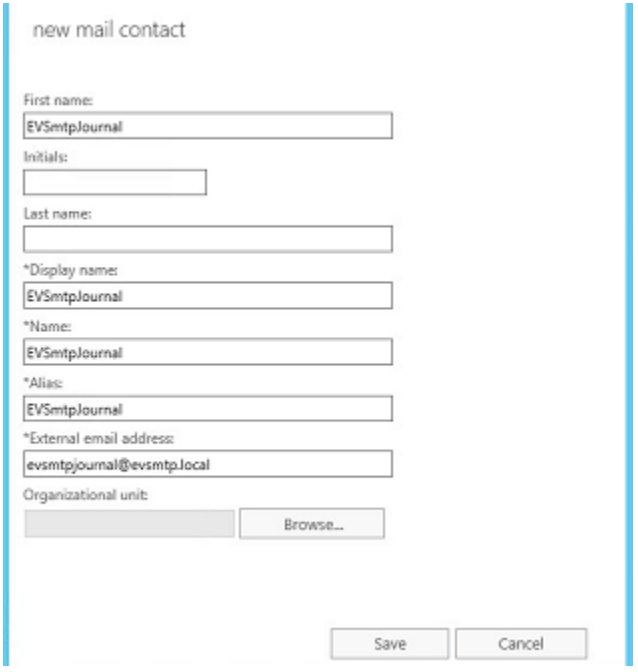
See "Points to note when setting up Enterprise Vault SMTP Archiving servers" on page 19.

**To create a recipient mail contact in the remote domain**

1 Open the Exchange Admin Center, and click **recipients**. At the top of the page, click **contacts**, and then click **+** > **Mail contact** to create a new mail contact.




2 Enter the details for the new contact.




3 Click **Save**. Details of the new contact are displayed in the list of contacts.

# Creating a Send Connector for the remote domain

Create a Send Connector to route journal mail from the Exchange Server to the Enterprise Vault SMTP servers.

To provide load balancing and fault tolerance, you can route mail using multiple smart hosts in the Send Connector, MX records, or a hardware load balancer. The smart host method is described in this section. This method is inexpensive, secure, and not complicated to configure; it does not require any new DNS zones, or the creation of MX records in DNS. It also allows you to select authentication and encryption methods on the connector. MX records do not provide the option to encrypt messages.

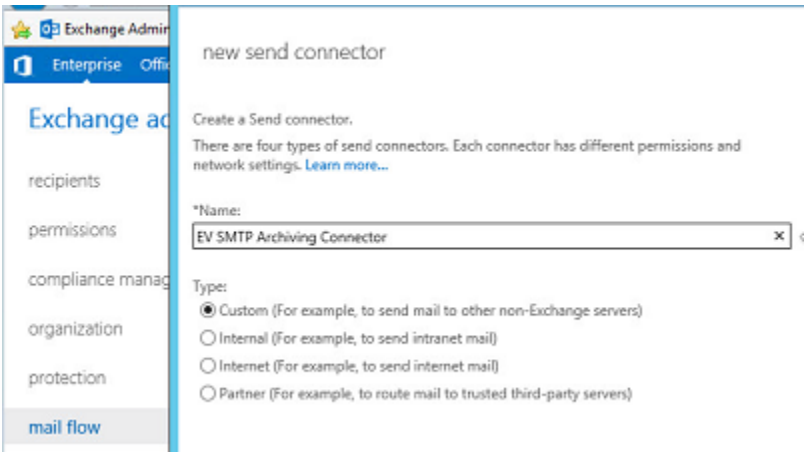
Typically, you add the Enterprise Vault SMTP servers as smart hosts to the Send Connector. If you have more than one smart host configured in the Send Connector, Exchange will use them in rotation, so that the smart hosts receive mail equally. High availability is also accomplished with this method; if one smart host is not available, the connector will use the next smart host.

Using MX records to provide load balancing and fault tolerance is described in *Best Practices for Deploying SMTP Archiving*.

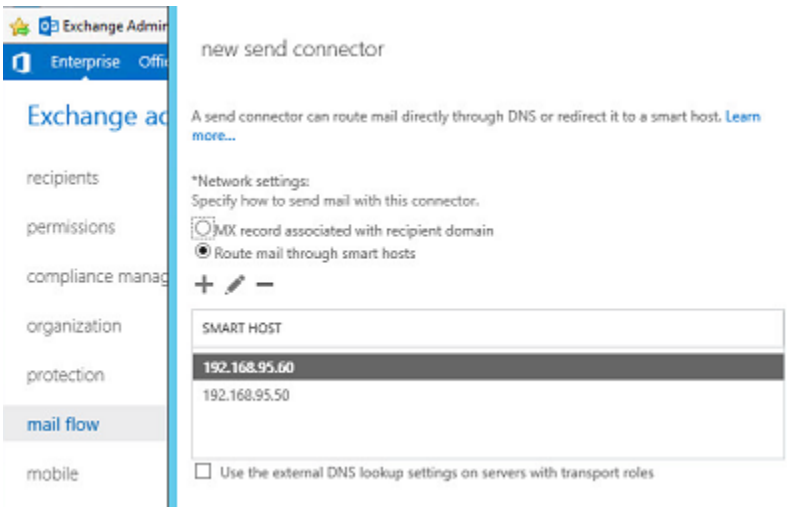
### To create a Send Connector for the remote domain

1 Open the Exchange Admin Center, and click **mail flow**. At the top of the page, click **send connectors**, and then click **+** to start the new send connector wizard.

Enter an appropriate name for the connector, and leave **Type** as **Custom**. Click **Next**.




2 To add smart hosts, select **Route mail through smart hosts**, and click **+** to add the IP addresses of the smart hosts; typically, the Enterprise Vault SMTP servers. Click **Next**.



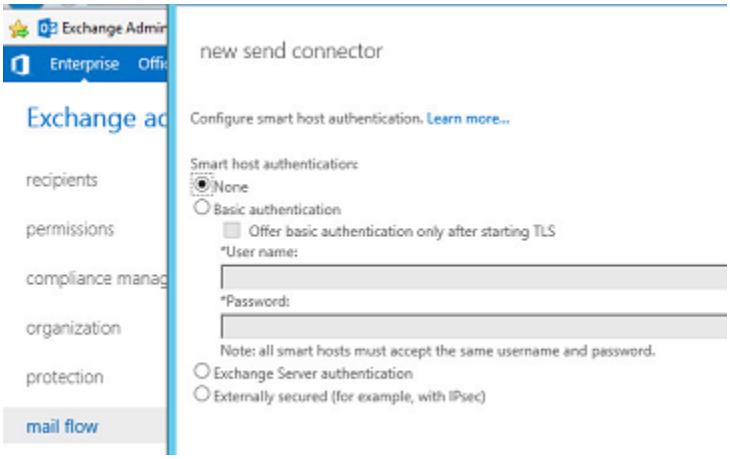
3 Configure the smart host authentication as follows:

- If authentication is not configured on the Enterprise Vault SMTP servers, then select **None**.
- If basic authentication is configured on the Enterprise Vault SMTP servers, then provide the same user name and password that is configured on the Enterprise Vault SMTP servers.

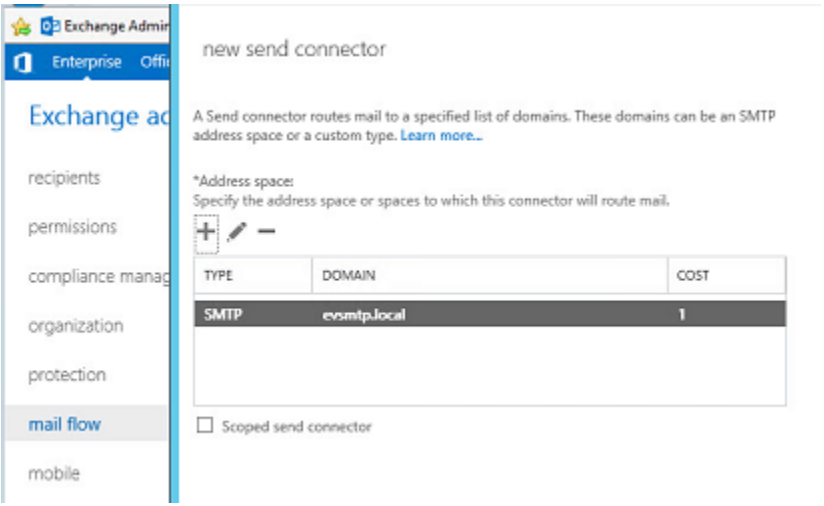
  Do not select **Offer basic authentication only after starting TLS**. This option enables Mutual Transport Layer Security (TLS) on the Exchange Server, which is not supported on Enterprise Vault SMTP servers.
- If encrypted connections are permitted on the Enterprise Vault SMTP servers, then select **None**.

  TLS is enabled by default on Exchange Server 2013, and the server attempts TLS for all remote connections. Exchange Server 2013 uses opportunistic TLS, and the setup creates a self-signed certificate.

  Click **Next**.

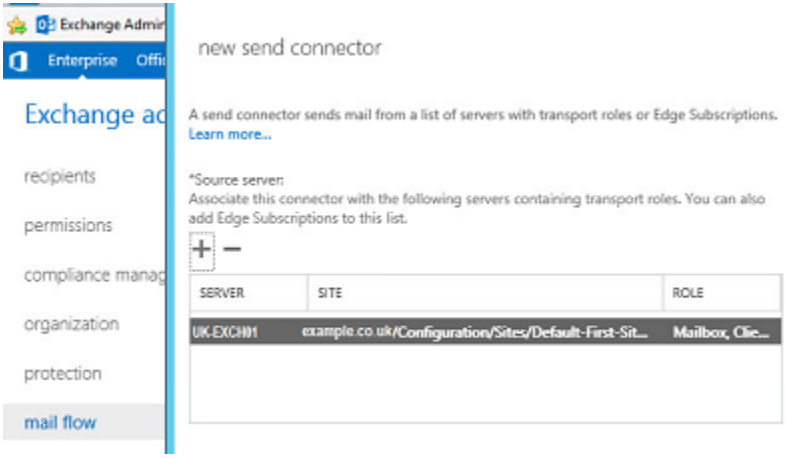


**4** On the **Address space** page, click **+** to add the remote domain that you created earlier. Click **Next**.



**5** On the **Source server** page, click **+** and add the Exchange Servers that are allowed to use this Send Connector.

When you have added the Exchange Servers, click **Finish**. The new connector is displayed in the list of Send Connectors.

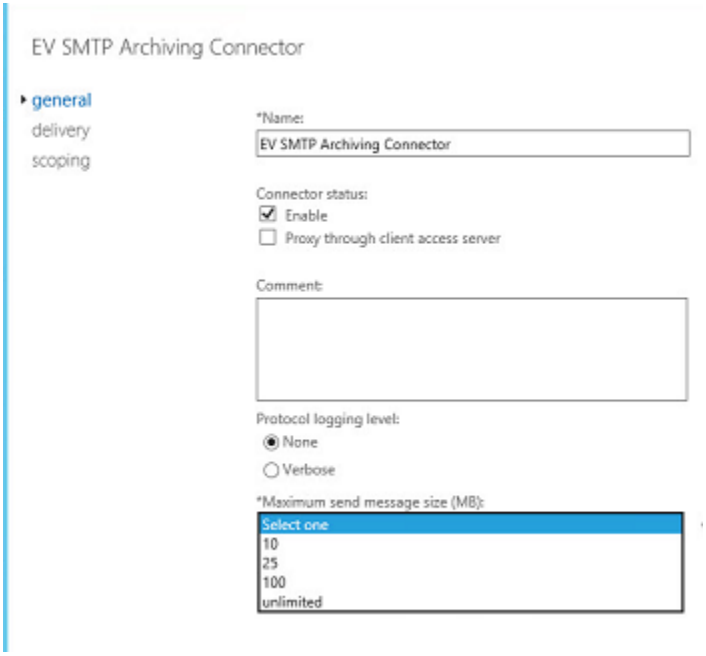


6 It is advisable to increase the maximum send message size for the Send Connector.

Double-click the connector to edit the properties. On the **general** page, choose an appropriate maximum message size for connector.

Do not select **Enable** on the Send Connector until the Enterprise Vault servers are fully configured and ready to receive SMTP traffic.

Confirm that the details on the other pages are correct and click **Save**.




# Setting up Exchange Server journaling

On Exchange Server you can configure standard or premium journaling:

- Standard journaling is configured on a mailbox database. Exchange journals all the messages for the mailboxes on the specified mailbox database. To journal all messages to and from all recipients and senders in the organization, you need to configure journaling for all of the mailbox databases on each Exchange mailbox server in the organization.
- Premium journaling uses journal rules to perform more granular journaling. You can configure journal rules to journal individual recipients or members of

distribution groups, instead of journaling all of the mailboxes on a mailbox database. You need an Exchange Enterprise Client Access License (CAL) to use premium journaling.

**To set up Exchange Server Standard journaling**

1. Open the Exchange Admin Center, and click **servers**. At the top of the page, select **databases** to list the mailbox databases.
2. Highlight the first mailbox database in the list, and click the pen icon to display the database properties.
3. As this step enables journaling, only perform the step when you have completed the configuration of the Enterprise Vault SMTP servers.

   In the mailbox database properties, click **maintenance**. In the **Journal recipient** box, enter the mail contact that you created earlier. This is the remote domain contact that you created to receive journal mail for Enterprise Vault SMTP archiving. On the Enterprise Vault SMTP servers, this contact's SMTP address must be configured as a target address.
4. Click **save** to start journaling.

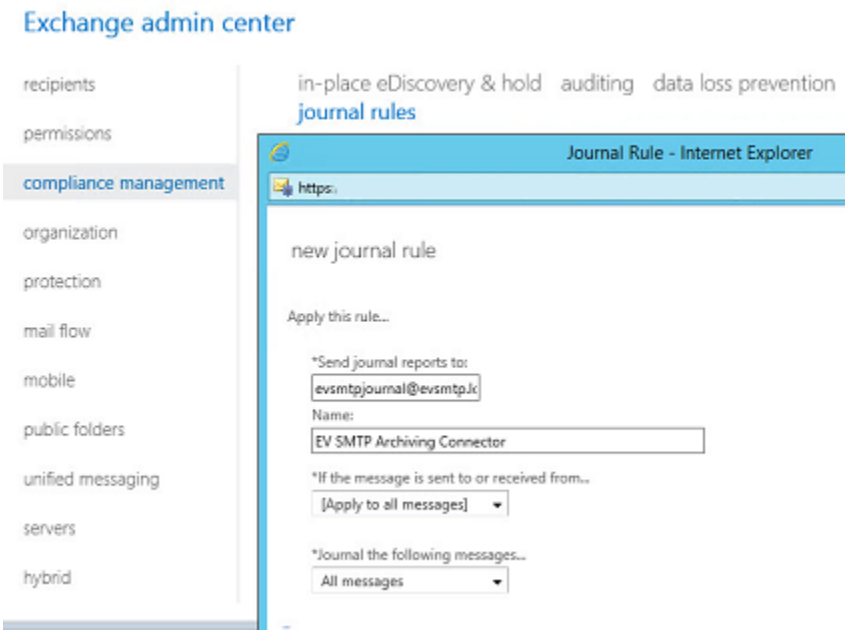
**To set up Exchange Server Premium journaling**

1. Open the Exchange Admin Center, and click **compliance management**. Click **journal rules** at the top of the page, and then click **+** to add a rule.
2. In the box, **Send journal reports to:**, enter the address of the mail contact that you created to receive journal mail for Enterprise Vault SMTP servers.

   In the **Name** box, enter the name of the Send Connector that you created to deliver journal mail to the Enterprise Vault SMTP servers.

   The other options let you configure the mailboxes and messages to which the rule applies.

   Click **Save**.




3. The new rule is displayed in the list of journal rules. Do not select the **ON** checkbox until you have completed the configuration of the Enterprise Vault SMTP servers.
4. Use **Send undeliverable journal reports to:** to configure a mailbox that will receive any non-delivery reports. Click **Select address** and provide the name of a suitable mailbox.

# Points to note when setting up Enterprise Vault SMTP Archiving servers

Detailed instructions on how to configure Enterprise Vault SMTP Archiving are provided in the manual, *Setting up SMTP Archiving*. The following list highlights points that you need to consider when configuring the Enterprise Vault SMTP servers:

- If you want to allow encrypted connections to the Enterprise Vault SMTP servers, then you need to obtain and import a suitable certificate on the Enterprise Vault SMTP servers.
  For instructions on how to obtain a certificate, see the section, "Obtaining an SSL/TLS certificate", in *Setting up SMTP Archiving*.
  You import certificates for the SMTP servers using the SMTP server settings in the Enterprise Vault Administration Console. The SMTP server settings are in the properties of the container **Targets** > **SMTP**.
- Make sure that the Enterprise Vault SMTP servers are configured to accept traffic from the Exchange Servers that are configured to use the Exchange Send Connector. **Connection Control** on the SMTP server settings dialog lets you configure the servers that can connect to the SMTP servers in the Enterprise Vault site.
- If you use a single journal address for the whole environment, Enterprise Vault accepts the journal traffic on any SMTP server. In Enterprise Vault 12.3 and later, you can assign multiple archives to an SMTP routing address to spread the archiving load over several archives and Enterprise Vault storage servers. In previous releases of Enterprise Vault, you could only implement target address rewriting to do this.
  Assigning multiple archives to an SMTP routing address, and target address rewriting are described in *Setting up SMTP Archiving*. Additional information is provided in *Best Practices for Deploying SMTP Archiving*. You can access these documents at the following address on the Veritas support website: http://www.veritas.com/docs/000004016.

Chapter 2

# Configuring Office 365 for Enterprise Vault SMTP Archiving

This chapter includes the following topics:



## About using Enterprise Vault SMTP Archiving for Office 365 journaling

This chapter describes how to configure Office 365 to send copies of an organization's mail to Enterprise Vault SMTP servers, which store the mail in one or more archives.

This document does not describe how to set up Enterprise Vault SMTP Archiving. The manual, *Setting up SMTP Archiving*, contains detailed instructions on how to configure this feature. For additional information on Enterprise Vault SMTP Archiving, such as best practices and performance, see the documents on the Veritas support website, http://www.veritas.com/docs/000004016.

# Summary of steps

Table 2-1 summarizes the steps required to configure Office 365 to send journal mail to Enterprise Vault SMTP servers.

**Table 2-1** Summary of configuration steps on Office 365

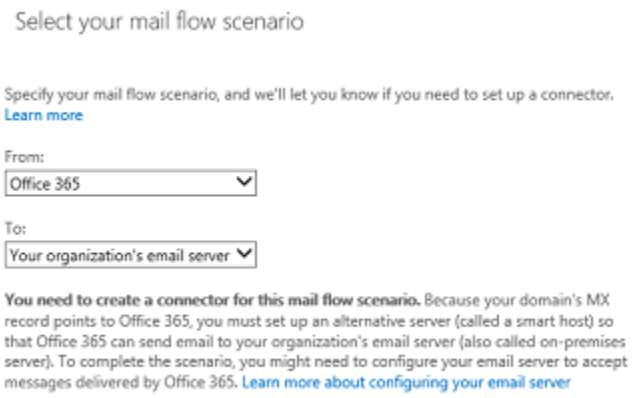
| Step | Task | Further information |
|---|---|---|
| 1 | Create an Office 365 to Enterprise Vault Send Connector. | See "Creating an Office 365 to Enterprise Vault Send Connector" on page 21. |
| 2 | Set up Enterprise Vault SMTP Archiving servers. | Detailed configuration instructions are given in the manual, *Setting up SMTP Archiving*.<br>See "Points to note when setting up Enterprise Vault SMTP Archiving servers" on page 23. |

# Creating an Office 365 to Enterprise Vault Send Connector

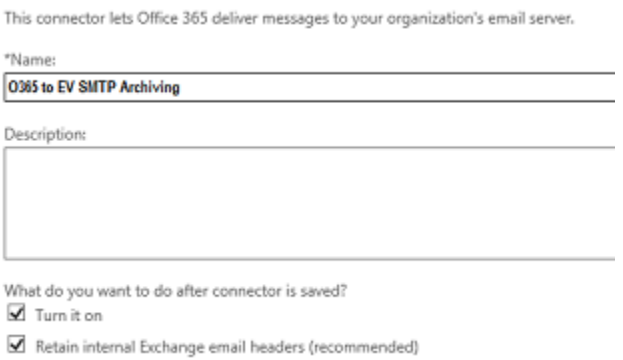
This section describes how to set up a Send Connector to send mail from Office 365 to your Enterprise Vault SMTP servers. Although the instructions given here use the domain name to deliver mail, you can use transport rules instead. The domain or domains that you specify to send mail to Enterprise Vault must be routable in the Internet.

**To create an Office 365 to Enterprise Vault Send Connector**

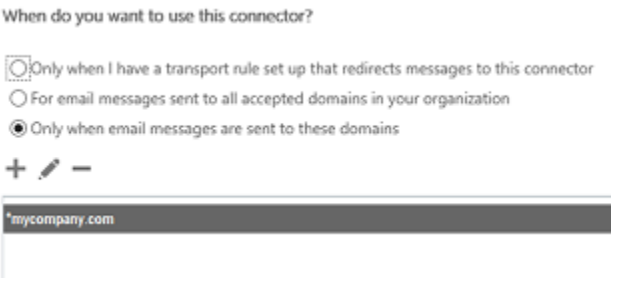
1. Log in to the Office 365 portal. Click **Admin**, and then click **Exchange** to go to the Exchange Admin Center. Click **Mail flow** and then **connectors**.
2. Select the options to create a connector to send messages from Office 365 to your organization's email server. The email server is your Enterprise Vault SMTP server.



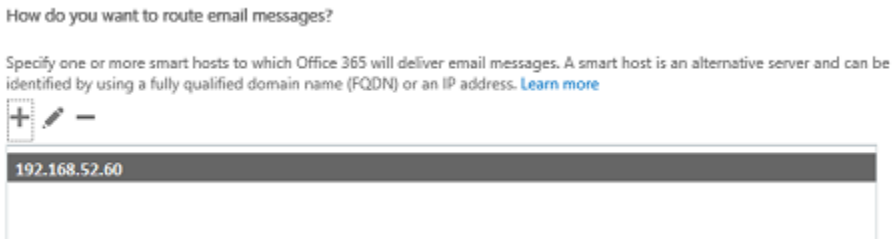

3. Enter a name for the connector. You can leave selected the options to turn on the connector and retain mail headers.



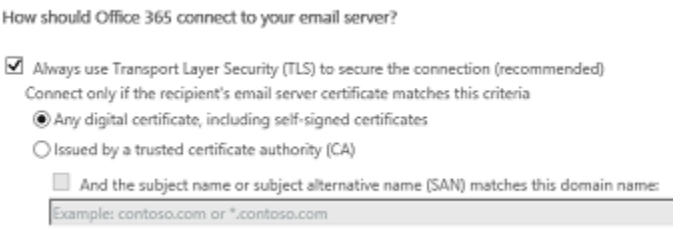
4 Enter the domain or domains for your Enterprise Vault SMTP servers. These domains must be routable in the Internet.




5 Enter details of the smart hosts to which Office 365 will deliver the messages.




6 Transport Layer Security (TLS) info. You can use opportunistic TLS or full TLS authentication.




# Points to note when setting up Enterprise Vault SMTP Archiving servers

Detailed instructions on how to configure Enterprise Vault SMTP Archiving are provided in the manual, *Setting up SMTP Archiving*. This section highlights points

that you need to consider when configuring your Enterprise Vault environment, and the Enterprise Vault SMTP servers.

- If you want to allow encrypted connections to the Enterprise Vault SMTP servers, then you need to obtain and import a suitable certificate on the Enterprise Vault SMTP servers.
  For instructions on how to obtain a certificate, see the section, "Obtaining an SSL/TLS certificate", in *Setting up SMTP Archiving*.
  You import certificates for the SMTP servers using the SMTP server settings in the Enterprise Vault Administration Console. The SMTP server settings are in the properties of the container **Targets** > **SMTP**.
- Make sure that the Enterprise Vault SMTP servers are configured to accept traffic from the servers that use the Office 365 Send Connector. If you use a firewall, then connections to the SMTP servers are likely to be from servers in your internal network. **Connection Control** on the SMTP server settings dialog lets you configure the servers that can connect to the SMTP servers.
- On the SMTP servers do not configure authentication for connections, as this cannot be configured on the Office 365 Send Connector.
- To secure communications you can use a combination of the following features:
  - Set up a firewall, and firewall ACLs based on Office 365 email addresses.
  - In your internal network, use an internal address to route messages to Enterprise Vault, for example journal@evsmtp.local. This is then the SMTP target address that you configure in Enterprise Vault.
  - Deliver messages to the SMTP servers using IP addresses, not DNS.
  - On the Enterprise Vault SMTP servers, use the **Connection Control** dialog to configure the servers in your internal network that are allowed to connect to the SMTP servers.
- If you use a single journal address for the whole environment, Enterprise Vault accepts the journal traffic on any SMTP server. In Enterprise Vault 12.3 and later, you can assign multiple archives to an SMTP routing address to spread the archiving load over several archives and Enterprise Vault storage servers. In previous releases of Enterprise Vault, you could only implement target address rewriting to do this.
  Assigning multiple archives to an SMTP routing address, and target address rewriting are described in *Setting up SMTP Archiving*. Additional information is provided in *Best Practices for Deploying SMTP Archiving*. You can access these documents at the following address on the Veritas support website: http://www.veritas.com/docs/000004016.

Chapter 3

# Configuring the Azure RMS Decryption feature for Office 365 email encryption support

This chapter includes the following topics:

# About configuring the Azure RMS Decryption feature for Office 365 email encryption support

This chapter describes how to configure the Azure RMS Decryption feature for Office 365 email encryption support.

This document does not describe how to set up Enterprise Vault SMTP Archiving. The manual, *Setting up SMTP Archiving*, contains detailed instructions on how to configure this feature. For additional information on Enterprise Vault SMTP Archiving, such as best practices and performance, see the documents on the Veritas Support website, http://www.veritas.com/docs/000004016.

**Note:** This chapter applies to Enterprise Vault 12.4 to 14.3. For Enterprise Vault 14.4 and later, see *Configuring decryption of MPIP-protected Office 365 emails archived in Enterprise Vault*.

# Summary of steps

Table 3-1 summarizes the steps required to configure Office 365 to send journal mail to Enterprise Vault SMTP servers.

**Table 3-1** Summary of steps for configuring Azure RMS Decryption on Office 365

| Step | Task | Further information |
|---|---|---|
| 1 | Configure IRM settings for journal report decryption in your organization. | See "Configuring IRM settings for journal report decryption in your organization" on page 27. |
| 2 | Get the Rights Management configuration details of your Azure tenant | See "Getting the Rights Management configuration details of your Azure tenant" on page 27. |
| 3 | Create a new service principal that represents your tenant to external applications | See "Creating a new service principal that represents your tenant to external applications" on page 28. |
| 4 | Add service principal to the list of superusers for your organization | See "Adding the service principal to the list of superusers for your organization" on page 28. |
| 5 | Install Microsoft Right Management Services Client 2.1 | See "Installing Microsoft Right Management Services Client 2.1" on page 28. |

**Table 3-1** Summary of steps for configuring Azure RMS Decryption on Office 365 *(continued)*

| Step | Task | Further information |
|---|---|---|
| 6 | Configure the decryption of RMS-protected messages in Enterprise Vault | See "Configuring the decryption of RMS-protected messages in Enterprise Vault" on page 29. |

# Configuring IRM settings for journal report decryption in your organization

Verify the IRM configuration settings for journal report decryption in your organization using the `Get-IRMConfiguration` cmdlet. For information about `Get-IRMConfiguration`, see https://docs.microsoft.com/en-us/powershell/module/exchange/encryption-and-certificates/get-irmconfiguration?view=exchange-ps).

If Journal Report Decryption is enabled at IRM, then run the following command to disable the decryption.

```
Set-IRMConfiguration -JournalReportDecryptionEnabled $false
```

For information about `Set-IRMConfiguration`, see https://docs.microsoft.com/en-us/powershell/module/exchange/encryption-and-certificates/set-irmconfiguration?view=exchange-ps)

# Getting the Rights Management configuration details of your Azure tenant

Get the Rights Management configuration of your tenant by running the `Get-AadrmConfiguration` cmdlet. For information about `Get-AadrmConfiguration`, see https://docs.microsoft.com/en-us/powershell/module/aadrm/get-aadrmconfiguration?view=azureipps).

From the output that the cmdlet returns, you need the following details to configure RMS settings in Enterprise Vault.

- `BPOSId`
- `LicensingIntranetDistributionPointUrl`
- `LicensingExtranetDistributionPointUrl`

See "Configuring the decryption of RMS-protected messages in Enterprise Vault" on page 29.

# Creating a new service principal that represents your tenant to external applications

Create a new service principal using the `New-MsolServicePrincipal` cmdlet. For more information about `New-MsolServicePrincipal`, see (https://docs.microsoft.com/en-us/powershell/module/msonline/new-msolserviceprincipal?view=azureadps-1.0

From the output that the cmdlet returns, you need the following details to configure RMS settings in Enterprise Vault.

- `Symmetric key`
- `AppPrincipalId`

See "Configuring the decryption of RMS-protected messages in Enterprise Vault" on page 29.

# Adding the service principal to the list of superusers for your organization

Add the service principal to the superuser group using the following command:

`Add-AadrmSuperUser -ServicePrincipalId <Service Principal Id>`

For more information about `Add-AadrmSuperUser`, see https://docs.microsoft.com/en-us/powershell/module/aadrm/add-aadrmsuperuser?view=azureipps

# Installing Microsoft Right Management Services Client 2.1

Install Microsoft Right Management Services (RMS) Client 2.1 on all the storage servers where the SMTP archiving is configured to enable decryption of RMS protected emails.

Run the deployment scanner to verify that the RMS client is installed. If the client is not installed, use the link in the Deployment Scanner warning message to download and install the client.

# Configuring the decryption of RMS-protected messages in Enterprise Vault

Configure the RMS settings in the site properties, and the SMTP policy to allow Enterprise Vault to decrypt RMS-protected messages.

**To configure RMS settings in Enterprise Vault**

1. In the left pane of the Administration Console, expand the hierarchy until the name of the site is visible.
2. Right-click the name of the site. Then click **Properties**. The site properties are displayed.
3. Click the **RMS** tab.
4. Select the **Enable RMS Decryption** check box.
5. Edit the following settings:
   - `Intranet URL`
   - `Extranet URL`
   - `BPOS Tenant ID`
   - `Application Principal ID`
   - `Symmetric Key`
6. Click **Test** to verify whether the Enterprise Vault server can authenticate with the Azure Information Protection (AIP) services using the provided settings.
7. Click **OK** to close the site properties.
8. In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.

   Expand **Policies** and click **SMTP**.

   In the right-hand pane, double-click the name of the policy that is used for SMTP archiving. The policy's properties are displayed.
9. Click the **Advanced** tab.
10. Set **ClearText copies of RMS Protected items** to **Treat as Secondary**.
11. Set **Decrypt RMS Protected items** to **Decrypt for journal archives only**.
12. Click **OK** to close the SMTP policy properties.
13. Restart the SMTP archiving task and the associated Storage service to apply the changes.

Chapter 4

# Configuring decryption of MPIP-protected Office 365 emails archived in Enterprise Vault

This chapter includes the following topics:



## About configuring the MPIP decryption feature in Enterprise Vault

This chapter describes how to configure the decryption of Microsoft Purview Information Protection (MPIP) protected emails in Office 365.

**Note:** This chapter is applicable to Enterprise Vault 14.4 and later.

This document does not describe how to set up Enterprise Vault SMTP Archiving. The manual, *Setting up SMTP Archiving*, contains detailed instructions on how to configure this feature.

For additional information on Enterprise Vault SMTP Archiving (such as best practices and performance), see the documents on the Veritas Support website, http://www.veritas.com/docs/000004016

# Summary of steps

Table 4-1 summarizes the steps required to configure decryption of Microsoft Purview Information Protection (MPIP) protected emails archived in Enterprise Vault.

**Table 4-1** Summary of configuration steps for decryption of MPIP-protected emails

| Step | Task | Further information |
|---|---|---|
| 1 | Disable decryption of journal report in your organization. | See "Disable decryption of journal report in your organization" on page 31. |
| 2 | Register an application with the Azure Active Directory. | See "Register an application with the Azure Active Directory" on page 32. |
| 3 | Assign the required permissions to an application. | See "Assign the required permissions to an application" on page 35. |
| 4 | Upload certificates. | See "Upload certificates" on page 38. |
| 5 | Configure decryption of MPIP-protected emails in Enterprise Vault. | See "Configure decryption of MPIP-protected emails in Enterprise Vault" on page 40. |

# Disable decryption of journal report in your organization

By default, journal report decryption is enabled in your organization. As a result, decrypted copies of protected emails are attached to the journal report sent to the Enterprise Vault SMTP Service. Since Enterprise Vault can now decrypt Microsoft Purview Information Protection (MPIP) protected emails for a preview of the items in Discovery Accelerator, there is no requirement to send the decrypted copies of protected emails attached to the journal report.

- Verify the Information Rights Management (IRM) configuration settings for journal report decryption in your organization by using the `Get-IRMConfiguration` cmdlet. For more information, see Get-IRMConfiguration.
- If journal report decryption is enabled on the IRM settings, run the following command to disable it:

  `Set-IRMConfiguration -JournalReportDecryptionEnabled $false`

  For more information, see Set-IRMConfiguration.

The following PowerShell commands can be executed by Exchange Administrator or Office 365 Administrator:

**Command**:

```
#Retrieve the Information Rights Management (IRM) configuration in
your organization.

Set-ExecutionPolicy RemoteSigned

$Cred = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange
-ConnectionUri

https://ps.outlook.com/powershell/ -Credential $Cred -Authentication
Basic –AllowRedirection

Import-PSSession $Session

Get-IRMConfiguration
```

**Command**:

```
#Test Information Rights Management (IRM) configuration and
functionality.

Test-IRMConfiguration -Sender '<sender email adress>'
```

**Command**:

```
#Disable decryption of journal report in your organization

Set-IRMConfiguration -JournalReportDecryptionEnabled $false
```

# Register an application with the Azure Active Directory

To enable Enterprise Vault to decrypt Microsoft Purview Information Protection (MPIP) protected emails, you must first register it with the Azure Active Directory.

Registering the application establishes the trust relationship between the Enterprise Vault and the Microsoft identity platform.

Perform the following steps to register the application:

---

**Note:** Ensure that you have an Azure Account with an active subscription.

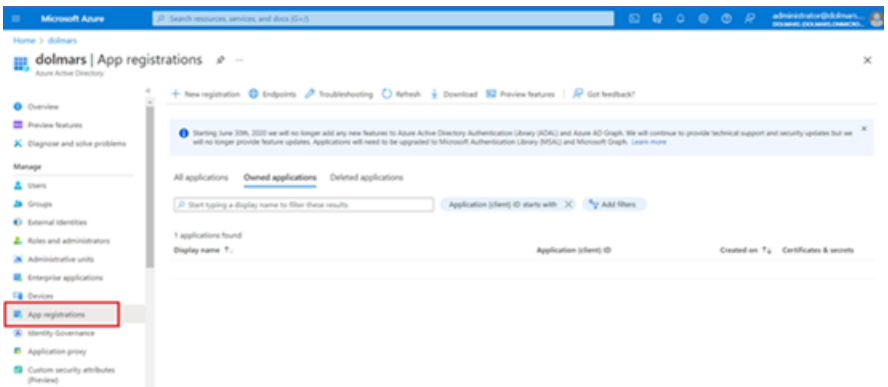
---

1. Open the Azure Portal (https://portal.azure.com/) by entering the credentials which have access to register application.

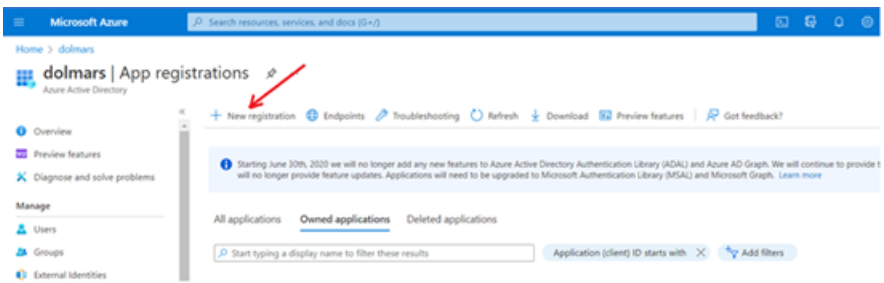
   Depending on the configuration of your tenant, you may also need to be a member of the “Global Administrator” directory role to register the application.

2. Select **Azure Active Directory** from the Azure services.

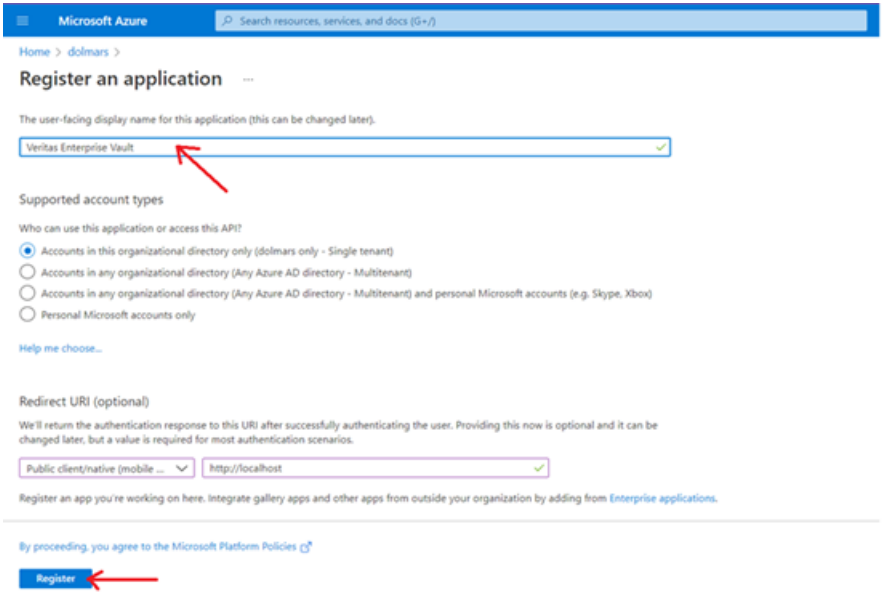
3. On the left navigation pane, select **App registrations**.




4. Click **+ New registration**.



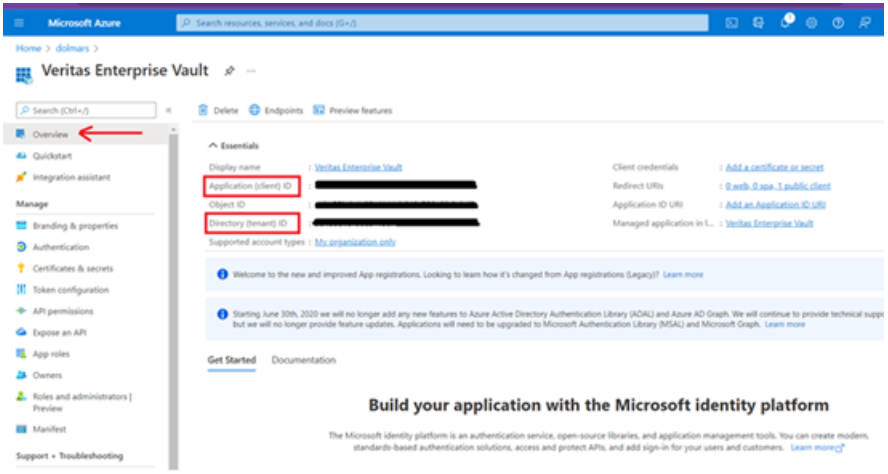

5. Enter the user-facing display name for the application and click **Register**.




**Note:** Ensure that all the other values on the **Register an application UI** is the same as displayed in the above image.

6. Navigate to the **Overview** section and find your **Application (client) ID** and **Directory (tenant) ID**.

**Note:** Make a note of the **Application (client) ID** and **Directory (tenant) ID**, which are required for enabling decryption of the MPIP-protected emails in Enterprise Vault.



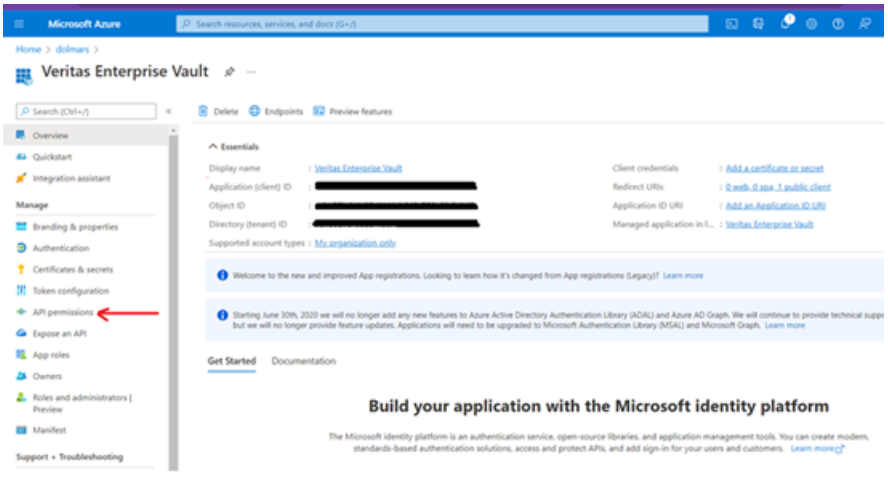

# Assign the required permissions to an application

Enterprise Vault requires the following permissions to decrypt Microsoft Purview Information Protection (MPIP) protected contents in your organization:

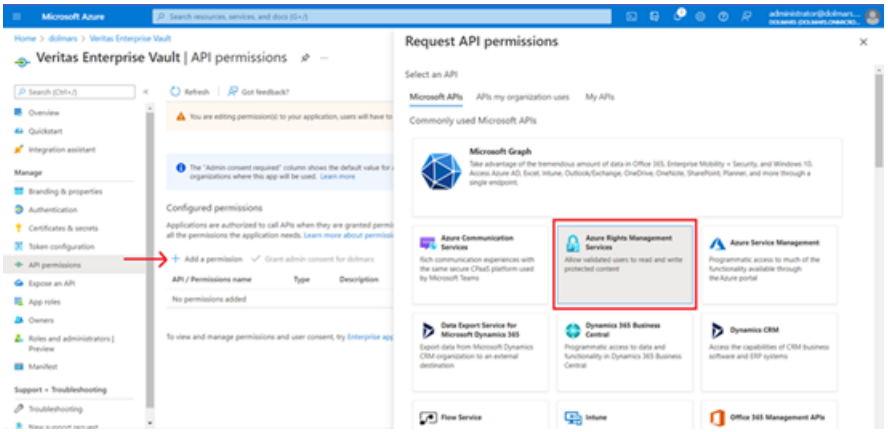
| Service | Permission Name | Description | Admin Consent Required |
|---|---|---|---|
| Azure Rights Management Service | Content.SuperUser | Read all protected content for this tenant | Yes |

Perform the following steps to assign the required permissions:

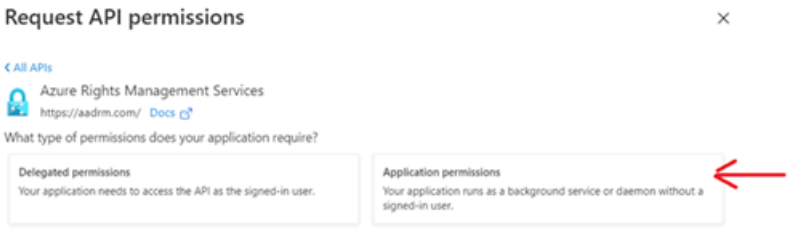
1. On the left navigation pane, click **API permissions**.



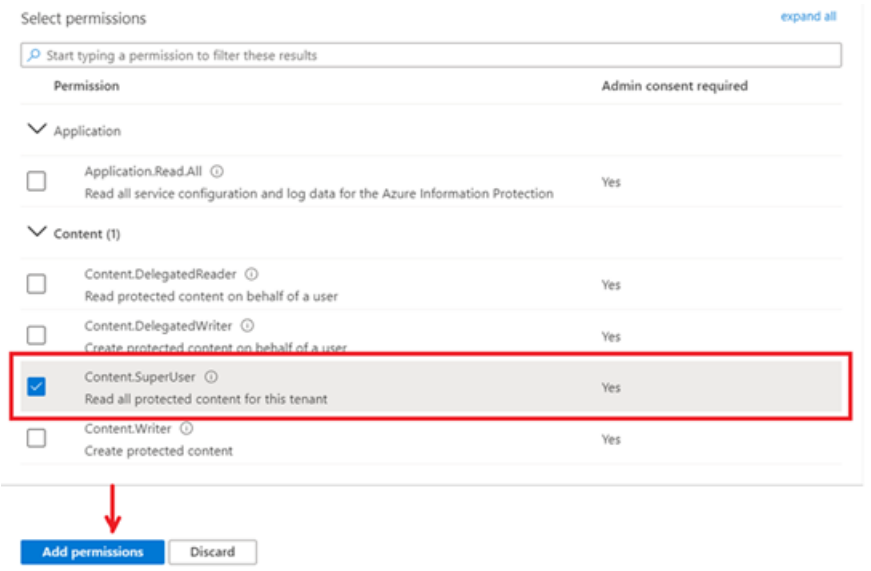

2. Click **+ Add a permission** and select **Azure Rights Management Services** from the list of services.



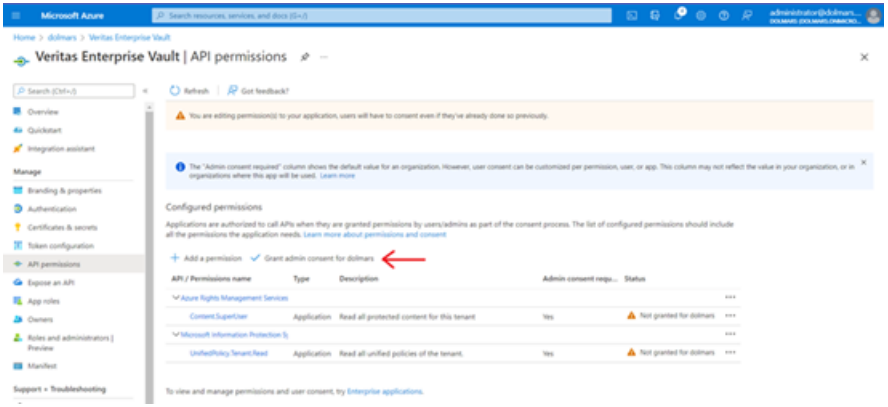

3. Click **Application permissions**.




4. Select **Content.SuperUser** from the list of permissions and click **Add permissions**.




5. Assign the permissions as displayed on the image above and click **Grant admin consent**.




# Upload certificates

To be able to preview Microsoft Purview Information Protection (MPIP) protected emails in Discovery Accelerator:

- Emails must be decrypted by the Enterprise Vault storage servers.
- The HTML preview must be generated and stored on Vault Storage Partition.
- Enterprise Vault storage servers must authenticate with the Azure Active Directory using X509 certificate-based authentication.

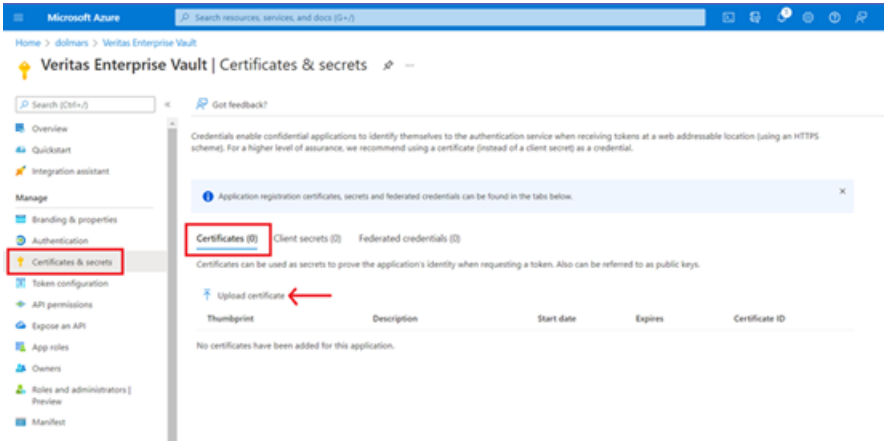
You can choose separate certificates for each Enterprise Vault storage servers and upload all those server specific servers to register the Azure Active Directory application. You can also choose to upload a single certificate. However, the certificate must be installed on all the Enterprise Vault storage servers, or you can choose to upload the PFX certificate file and the certificate details must be stored in the Enterprise Vault directory database.

---

**Note:** Public key of the certificate must be uploaded to the Azure Active Directory and the Enterprise Vault storage server should have both the public and the private keys.

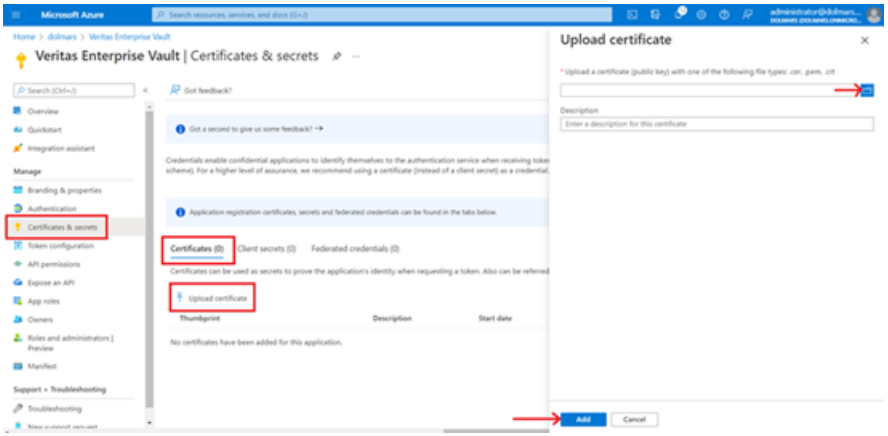
---

1. On the left navigation pane, click **Certificates & secrets**, select **Certificates (0)** on the right pane, and click **Upload certificate**.




2. Upload the required certificate and click **Add**.

   You may specify a certificate description in the **Description** section. Otherwise, Common Name (CN) of the server is displayed.

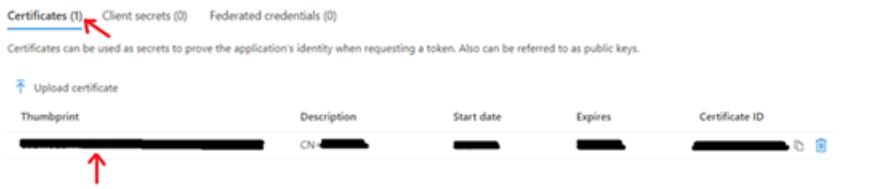



3. Ensure that the certificate has been uploaded and verify that the count has increased.

---

**Note:** Make a note of the **Thumbprint** of the certificate or certificates uploaded, which is required for enabling decryption of the MPIP-protected emails in Enterprise Vault.

---




# Configure decryption of MPIP-protected emails in Enterprise Vault

Perform the following steps to configure decryption of Microsoft Purview Information Protection (MPIP) protected emails in Enterprise Vault:

1. On the left navigation pane of the Administration Console, expand the hierarchy until the name of the site is visible.
2. Right-click on the name of the site, and click **Properties**.

   The site properties are displayed.
3. Click on the **MPIP** tab.
4. Click on **Start decryption of MPIP-protected emails**.
5. Enter the **Application ID** and **Tenant ID** on the UI.

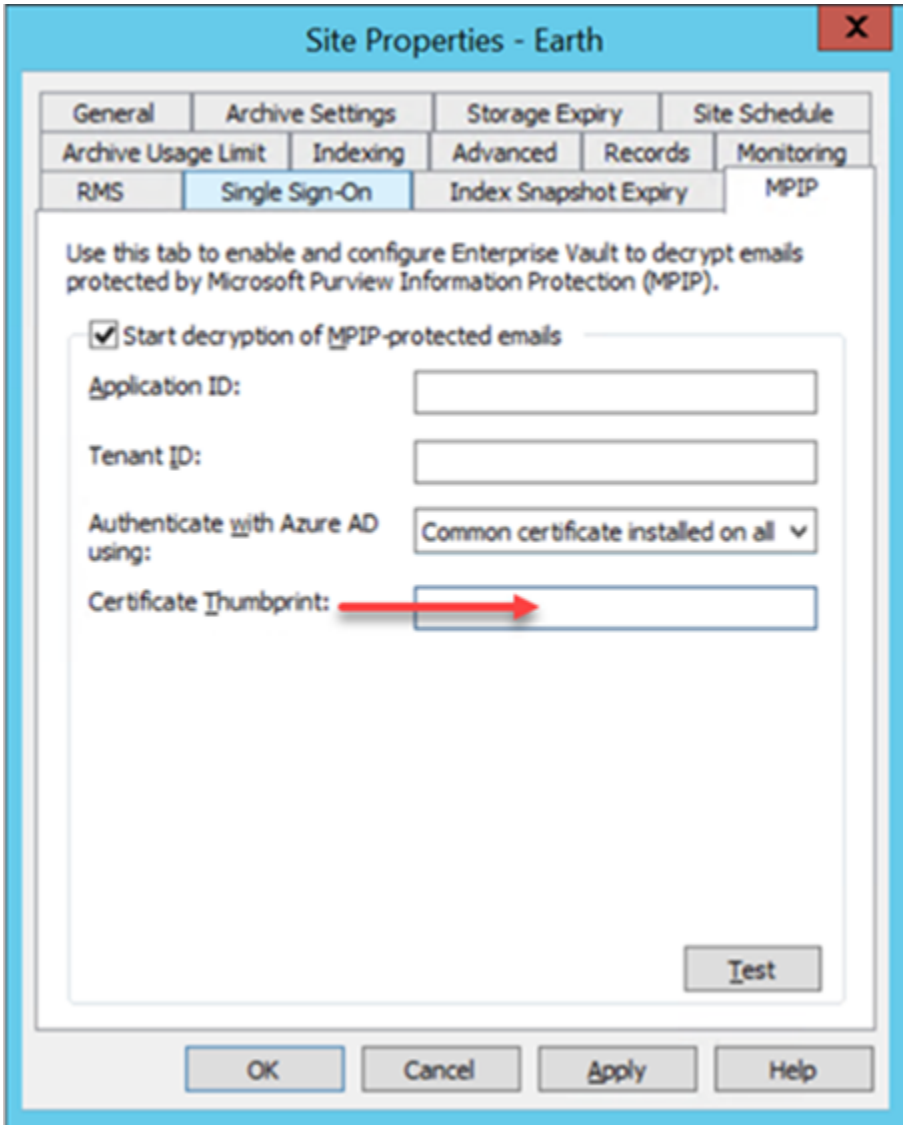
   The **Application ID** and **Tenant ID** details were retrieved during Register an application with the Azure Active Directory.
6. Choose an appropriate authentication method in **Authenticate with Azure AD using**.

| | |
|---|---|
| Common certificate installed on all the Enterprise Vault storage servers | Choose this option, in case you have to use a single certificate for authentication then install that certificate in **Trusted Root Certification Authorities in Local Computer** of all the Enterprise Vault storage servers. |
| Common PFX certificate file for all the Enterprise Vault storage servers | Choose this option, in case you have to upload a PFX file to Enterprise Vault and use those details for authentication. Enterprise Vault stores PFX file contents in the database and the password to open the PFX file is stored in an encrypted format. |

| | |
|---|---|
| Specific certificate installed on each Enterprise Vault storage server | Choose this option, in case you have to use a separate certificate for authentication on Enterprise Vault storage. Each storage server should have that certificate installed in **Trusted Root Certification Authorities in Local Computer**. |

**Note:** In any of above option the public key of X509 certificate must be uploaded to the Azure AD as mentioned in Upload certificates.

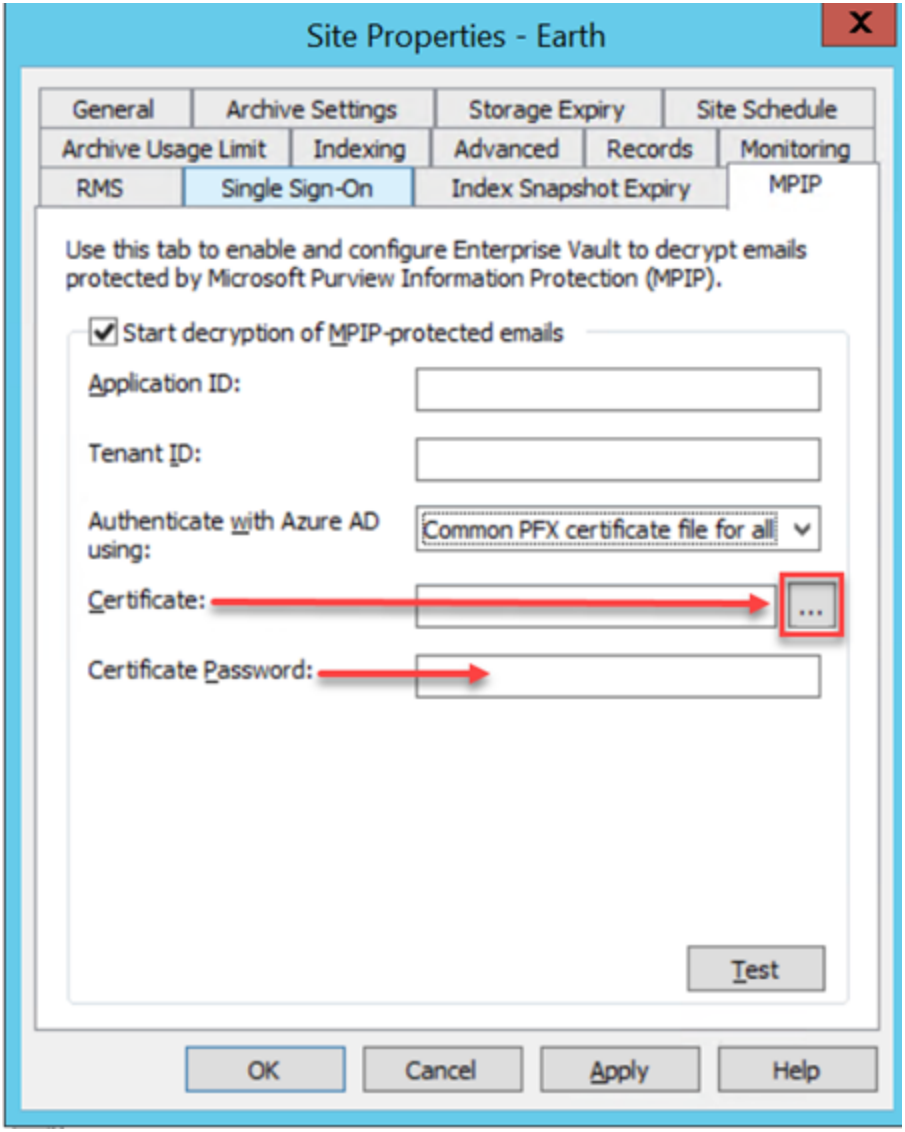
Authentication with Azure AD using Common certificate installed on all Enterprise Vault storage servers.




- Upload the public key of the X509 certificate to Azure AD as mentioned in Upload certificates.
- Obtain the Thumbprint of X509 certificate as mentioned in step 3 in Upload certificates.
- Enter the above Thumbprint in the **Certificate Thumbprint** field on above UI.

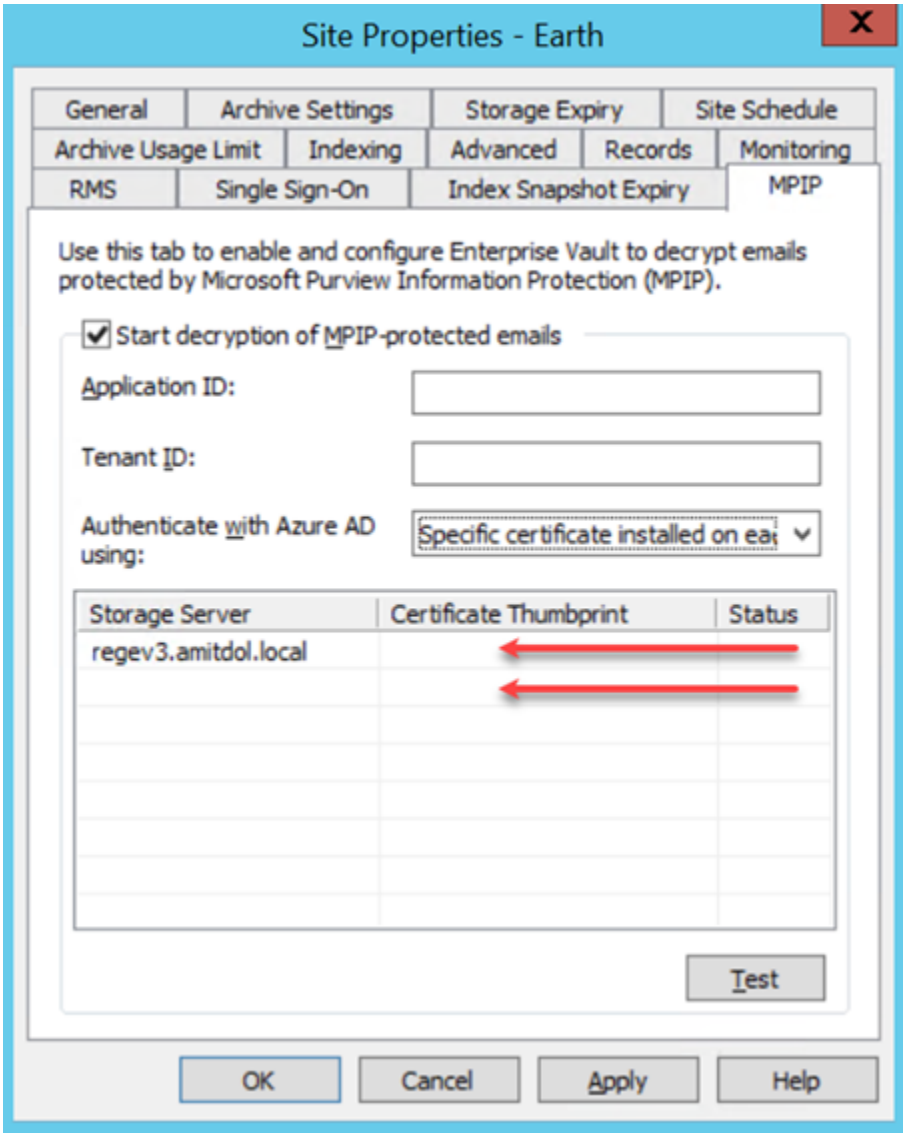
- You must install that certificate in **Trusted Root Certification Authorities in Local Computer** on all Enterprise Vault storage servers.

Authentication with Azure AD using Common PFX certificate file for all Enterprise Vault storage servers.



- Upload the public key of X509 certificate to Azure AD as mentioned in Upload certificates.
- • Upload the PFX file (X509 certificate having both public and private keys) in the **Certificate** field in the above UI.
- Enter the password to open the certificate PFX file in the **Certificate Password** field in the above UI.

Authentication with Azure AD using a Specific certificate installed on each Enterprise Vault storage server.




- Upload the public key of X509 certificate of each Enterprise Vault storage server to Azure AD as mentioned in Upload certificates.
- Obtain the Thumbprint of X509 certificate of all storage server specific certificates as mentioned in step 3 in Upload certificates.
- • Enter the thumbprint of the certificate corresponding to that Enterprise Vault storage server in the Certificate Thumbprint field in the above UI.

- You must have a certificate installed in **Trusted Root Certification Authorities in Local Computer** on that Enterprise Vault storage server.

7. Once you enter all the required details, click **Test** to validate configuration details. This ensures that all Enterprise Vault storage servers can authenticate with Azure AD and will be able to decrypt MPIP-protected emails during archiving.
8. In case there are any errors, please see event logs of particular storage server and resolve those errors.
9. On validation, the UI notifies you whether the MPIP configuration test has been successful or not.
10. Click **OK**.
11. Click **OK** to close the site properties and save the details in Enterprise Vault.
12. On the left pane of the Administration Console, expand the hierarchy until **Policies** is visible. Expand **Policies** and click **SMTP**.

    On the right-hand pane, double-click the name of the policy that is used for SMTP archiving. The policy's properties are displayed.
13. Click the **Advanced** tab.
14. Set **ClearText copies of MPIP-protected items** to **Treat as Secondary**.
15. Set **Decrypt MPIP-protected items to Decrypt for journal archives only**.
16. Restart the SMTP archiving task and the associated Storage service to apply the changes. If that is not known better to restart all SMTP archiving tasks and Storage service on all Enterprise Vault storage servers on the site.