Installing Forcepoint Email Security in Microsoft Azure

Installation | Forcepoint Email Security | Version 8.5.x | 29-Apr-2022

Topics:

Related documents:

- System requirements
- Forcepoint Email Security Administrator Help

Forcepoint Email Security in Azure provides the comprehensive protection of the email solution hosted on a Forcepoint appliance, but in the public cloud. Deployed in a Microsoft Azure environment, Forcepoint Email Security allows inbound, outbound, and internal email to be analyzed for data loss or malicious email threats in the cloud.

Email containing sensitive data can be permitted, quarantined, or encrypted. Sensitive attachments can also be dropped.

Important
V8.5.5 is not supported in an Azure environment.

This document covers the installation of Forcepoint Email Security in Azure versions **8.5**, **8.5.3**, and **8.5.4**.

In versions **8.5.3** and **8.5.4**, two types of deployment are available: both Forcepoint Email Security and Forcepoint Security Manager deployed in Azure, or Forcepoint Email Security deployed in Azure with Forcepoint Security Manager on-premises. Additional combinations of on-premises and Azure appliances can be configured as needed. Configuration in Azure and Microsoft Office 365 is required after deployment.

In version **8.5**, only one deployment is available: Forcepoint Email Security in Azure, with Forcepoint Security Manager deployed on-premises. This deployment requires a site-to-site Virtual Private Network (VPN) in Azure with connectivity to SQL Server and Forcepoint Security Manager running on-premises. See *Azure Deployment Steps: Version 8.5*, page 15.

The procedure for installing Forcepoint Email Security in Azure Government or Forcepoint DLP Email Gateway in Azure is the same as that detailed here for Forcepoint Email Security.

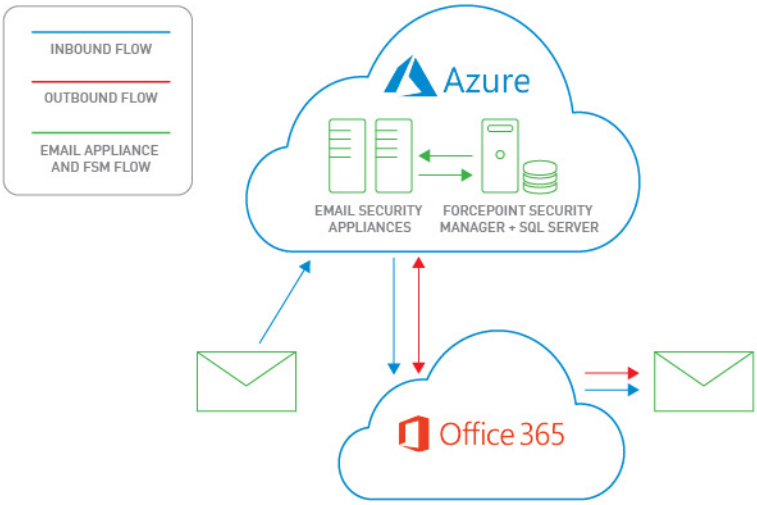
If you have a subscription key for Forcepoint DLP Email Gateway, follow the procedures below for deploying Forcepoint Email Security in Azure, then enter your subscription key in the Forcepoint Security Manager.

Forcepoint Email Security in Azure: Deployment Scenarios

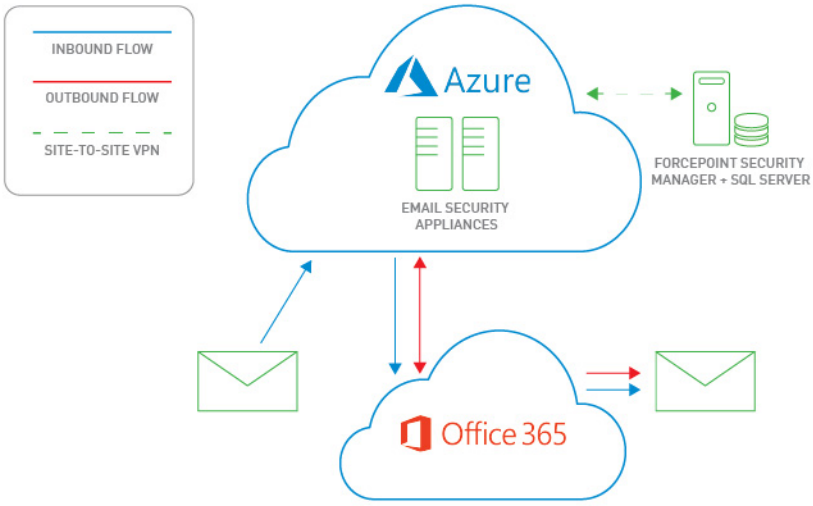
In versions **8.5.3** and **8.5.4**, email protection in Azure can be deployed in several ways, depending on the needs of your organization.

- The following image displays the workflow with both Forcepoint Email Security and Forcepoint Security Manager deployed in Azure. This deployment is only

available for versions **8.5.3** and **8.5.4.** The diagram depicts both inbound (blue) and outbound (orange) message directions.

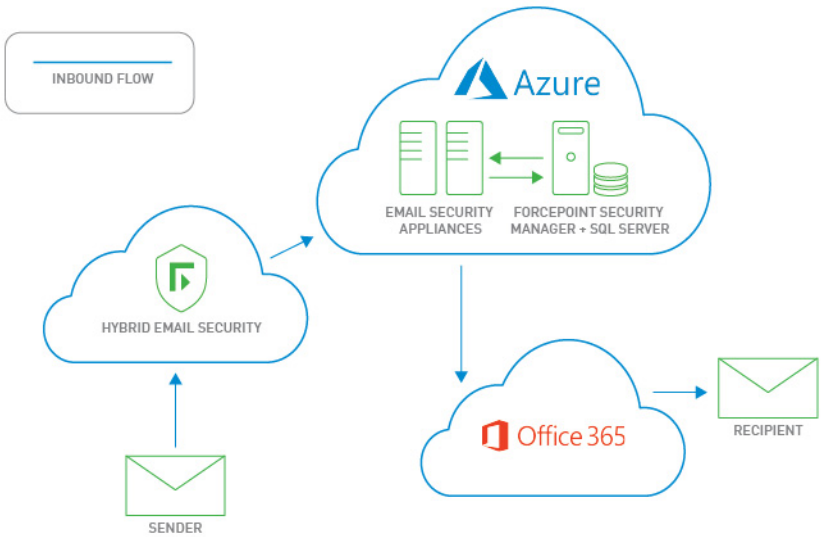


- The following image displays Forcepoint Email Security deployed in Azure while Forcepoint Security Manager remains on-premises. This is the only deployment available for version **8.5**, and is an additional option for versions **8.5.3** and **8.5.4**. The diagram depicts both inbound (blue) and outbound (orange) message directions.



- The Forcepoint Email Security Hybrid Module is an optional subscription that adds support for email hybrid service inbound pre-filtering in the cloud. (See Email hybrid service configuration.) The following diagram displays the

workflow of Forcepoint Email Security and Forcepoint Security Manager in Azure with the addition of the Forcepoint Email Security Hybrid Module.



Requirements

- A Microsoft Azure account (activated).
- Microsoft Office 365 with Outlook.
  - If you are installing Forcepoint Email Security in Azure Government, Office 365 Government is required.
- (*If you are installing version **8.5** or only installing Forcepoint Email Security in Azure*) A virtual network and subnet in Azure with connectivity to on-premises resources through a site-to-site VPN.
  - In version **8.5**, the minimum supported virtual network size is /16 and the minimum supported subnet size is /24.
  - In **versions 8.5.3** and **8.5.4**, the minimum supported virtual network and subnet size is /28.
- (*If you are installing version **8.5** or only installing Forcepoint Email Security in Azure*) Resources installed on-premises: SQL Server and Forcepoint Security Manager.
  - Forcepoint Security Manager must be upgraded to the latest version. See the Deployment and Installation Center for upgrade instructions.
- SQL Server Express, installed using the Forcepoint Security Installer, or a supported version of SQL Server installed separately.
  - Ensure the correct port is open; see Default ports for more information.
  - Refer to the Certified Product Matrix for supported operating systems.

- Use the C interface IP address, as Forcepoint Email Security in Azure only supports a single interface.

Azure Deployment Steps: Versions 8.5.3 and 8.5.4

Use the following steps to deploy your version **8.5.3** or **8.5.4** Forcepoint solution in Azure:

1. *Deploy both Forcepoint Email Security and Forcepoint Security Manager together in the Azure cloud*, page 5

   or *Deploy Forcepoint Email Security in Azure with Forcepoint Security Manager on-premises*, page 11
2. *Configuration in Microsoft Azure*, page 20
3. *Configure the system time zone*, page 20
4. *Install Forcepoint Security Manager management components for the virtual appliance*, page 21
5. *Configure the appliance in the Forcepoint Security Manager*, page 21
6. *Configure mail flow in Office 365*, page 24
7. *Create Email Log Database partitions when SQL Server is installed separately in Azure*, page 34
8. *Configure encrypted connection to SQL Server*, page 35 (optional)

For a high-level view of the procedure, see the Forcepoint Email Security in Azure Quick-Start Guide.

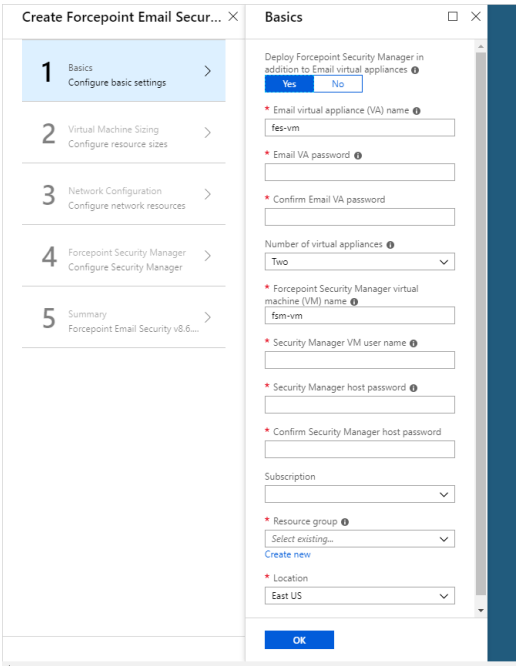
Deploy both Forcepoint Email Security and Forcepoint Security Manager together in the Azure cloud

This type of deployment is available for versions **8.5.3** and **8.5.4** only.

1. Log on to the Azure Marketplace, or use a direct link:
   - Forcepoint Email Security v8.5.4 in Azure
   - Forcepoint Email Security v8.5.3 in Azure
   - If you are installing in the Azure Government cloud:
     - Log into Azure Government, then click **Create a resource**.
     - In the Search bar, search for and select **Forcepoint Email Security**.
     - Click **Create**. All other steps are the same as in the Azure portal.
2. In the Search bar, search for Forcepoint, then select **Forcepoint Email Security V8.5.3** or **V8.5.4**.
3. To create a new Forcepoint Email Security solution, click **Get it now**.
4. Review the terms of use and privacy policy, then click **Continue** to proceed to the Azure portal.

5. From the Azure portal, click **Create**.

   The **Basics** tab displays for configuring the email appliance and Security Manager virtual machine settings.



6. From **Deploy Forcepoint Security Manager in addition to Email virtual appliances**, click **Yes**.

   Options display to configure the Security Manager virtual machine in addition to the email appliance.

   Click **No** if you want Security Manager to reside on an on-premises machine. See *Deploy Forcepoint Email Security in Azure with Forcepoint Security Manager on-premises*, page 11.

7. In the text field **Email virtual appliance (VA) name**, enter a name for the Forcepoint Email Security virtual appliance (VA).

   The name must be between 3 and 30 characters long and contain only numbers, letters, and hyphens.

8. In the text fields **Email VA password** and **Confirm Email VA password**, enter and confirm the password for connecting to the host.

   The username is always “admin” on first login to Forcepoint Email Security. Additional accounts can be added later. The password must be a minimum of 12 characters and contain at least one number, one lowercase letter, one uppercase letter, and one special character.

9. From the pull-down menu **Number of virtual appliances**, select the number of VAs to use; between 1 and 8.

   We recommend using at least two VAs to ensure high availability. If only one VA is selected at this time, it is not possible to add additional VAs after deployment is complete. If two or more VAs are selected, additional VAs can be added at any

point. See Add virtual machines to a Forcepoint Email Security in Azure deployment.

Load balancers are deployed by default when two or more VAs are used.

10. In the text field **Security Manager virtual machine (VM) name**, enter the name of the Security Manager virtual machine (VM).

    The name must be between 3 and 15 characters long and contain only numbers, letters, and hyphens.

11. In the text field **Security Manager VM user name**, enter the administrator user name of the Security Manager host.

    The name must adhere to Windows specifications for user names.

12. In the text fields **Security Manager host password** and **Confirm Security Manager host password**, enter and confirm the administrator password for the Security Manager host.

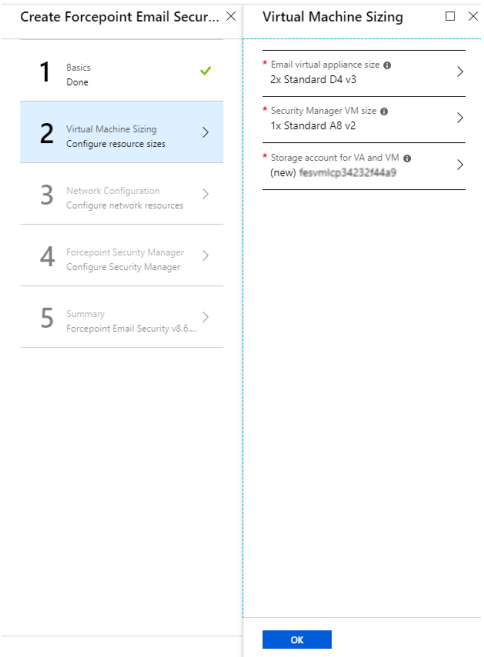
    The password must be between 12 and 128 characters and contain at least one number, one lowercase letter, one uppercase letter, and one special character.

13. From the pull-down menu **Subscription**, select your subscription.
14. From **Resource group**, click **Create new** and enter a name for the new resource group.

    A resource group is a container that holds related resources for an application. It will hold the Forcepoint Email Security VAs and the Forcepoint Security Manager VM. You must create a new resource group; using existing resource groups is not currently supported.

15. From the pull-down menu **Location**, select the location for the VAs and VM.
16. Click **OK**.

    The settings are saved and the **Virtual Machine Sizing** tab displays.



17. From **Email virtual appliance size**, select the size of the VA you will need based on anticipated email volume, then click **Select**.

    Use the Search fields if you need to find a different size.

18. From **Security Manager VM size**, select the size of the virtual machine you need for Forcepoint Security Manager.

    Use the Search fields if you need to find a different size.

19. From **Storage account for VA and VM**, to use an existing storage account, click **Use existing** and select the storage account and disk type for the VAs and VM.

    To create a new storage account, click **Create new**.

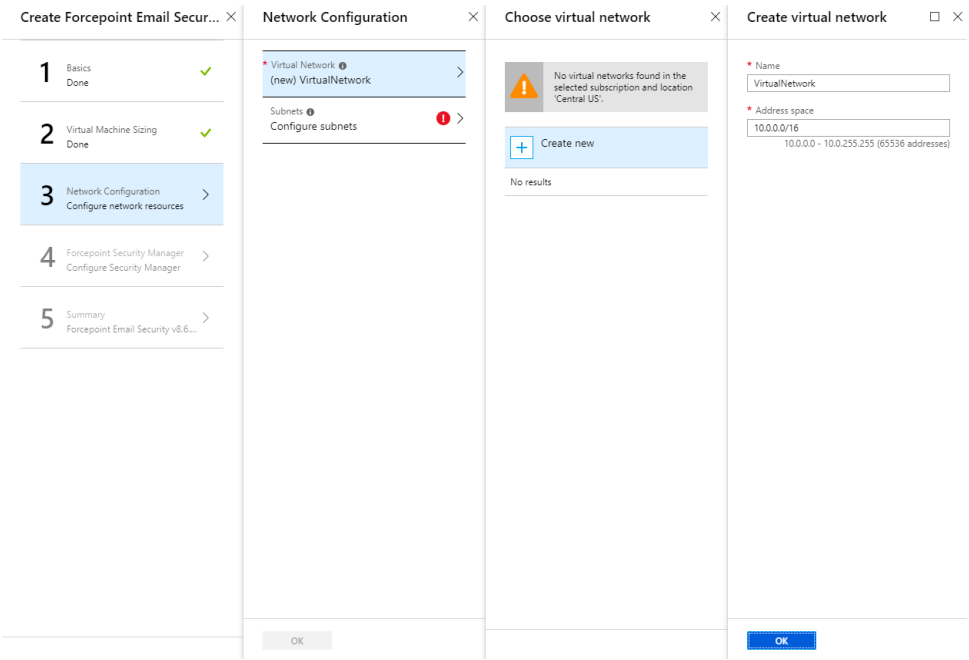
    The Create storage account tab displays.

    On the Create storage account tab, configure the Name, Account kind, Performance, and Replication settings and click **OK**.

    The new storage account is added.

20. From the Virtual Machine Sizing tab, click **OK**.

    The settings are saved and the **Network Configuration** tab displays.



21. From **Virtual Network**, select your existing virtual network or create a new network.

    To create a new virtual network, click **Create New**.

    The Create virtual network tab displays.

    On the Create virtual network tab, configure the Name and Address space.

    If you plan to use a remote SQL Server, you must select your existing virtual network, rather than creating a new network. When using a new virtual network, your deployment will fail if you select a remote SQL Server instance in Step 26. This is because the new virtual network has no connection to external components

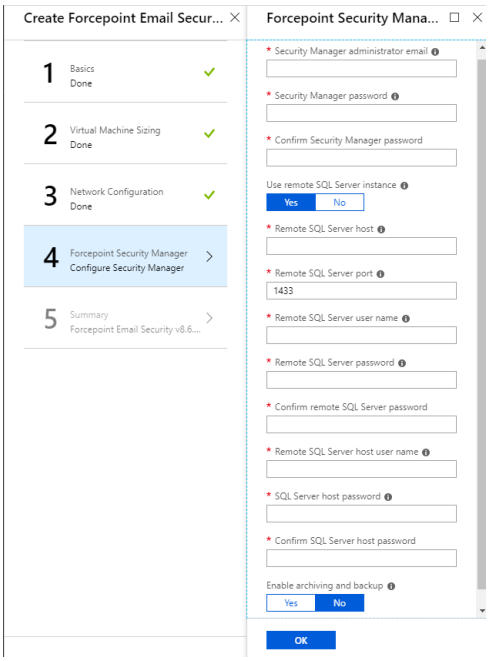
and cannot communicate with the remote SQL Server, which resides in a different virtual network.

22. From **Subnets**, select your existing subnet or create a new network.

    The minimum supported size is /28 for both virtual network and subnet. See *Requirements*, page 4.

23. From the Network Configuration tab, click **OK**.

    The settings are saved and the **Forcepoint Security Manager Configuration** tab displays.



24. In the text field **Security Manager administrator email**, enter the email address of the Forcepoint Security Manager administrator.

25. In the text fields **Security Manager password** and **Confirm Security Manager password**, enter and confirm the administrator password.

    The password must be between 12 and 256 characters and contain at least one number, one lowercase letter, one uppercase letter, and one special character.

26. From **Use remote SQL Server instance**, click **Yes** or **No**.

    If you select **No**, a local SQL Server is used. Text fields display according to your selection.

    Verify that in Step 21, you selected your existing virtual network with connection to the remote SQL Server, otherwise your deployment will fail.

27. In the text fields, enter the **host name**, **user name**, **password**, and **port** for the remote or local SQL Server.

    Verify that your SQL Server uses unique host names and that all of your resources are correctly configured for communication with each other.

28. From **Encrypt connection to SQL Server**, click **Yes** or **No**.

    If you select **Yes**, an additional field displays for uploading a CA certificate.

If you are using an encrypted connection to a remote SQL Server instance, ensure that the FQDN of your SQL Server is shorter than 64 characters, or configure SQL Server to use a wildcard certificate with a CN shorter than 64 characters. See the knowledge article Configuring the certificate for encrypted SQL Server connection for more information.

If you select **No**, it is possible to configure the encrypted connection following deployment. See *Configure encrypted connection to SQL Server*, page 35.

29. From **Upload CA certificate for SQL Server encryption**, click the **folder icon** and navigate to the certificate (.cer, .crt, or .pem).

    You can use a root CA certificate, or an intermediate CA certificate if using a third-party CA. Ensure that the name of your CA certificate contains no special characters or the upload will fail.

30. From **Enable archiving and system backup**, click **Yes** or **No**.

    If you select **Yes**, incident archiving and backup is enabled for Forcepoint DLP. Additional text fields display according to your selection.

31. In the text field **SQL Server backup UNC path**, enter the existing UNC path to the backup directory used by SQL Server.
32. In the text field **Security Manager backup UNC path**, enter the existing UNC path to the backup directory used by Security Manager.
33. In the text fields **Archive location user name**, **Archive location password**, and **Archive location domain**, enter the user name, password, and domain for the incident archive directory.

    The domain is optional.

34. Click **OK**.

    The settings are saved and the **Summary** tab displays.

35. From the **Summary** tab, review a summary of the Forcepoint Email Security and Forcepoint Security Manager solution you are building, then click **OK**.

    To change any configured settings, click one of the completed tabs. You will return to the Summary tab again after completing configuration.

    Final validation is performed and the **Buy** tab displays.

36. On the Buy tab, review the Forcepoint Terms of Use, EULA, and Privacy Policy.
37. To create the Forcepoint Email Security and Forcepoint Security Manager solution in the Azure cloud infrastructure, click **Create**.

    Forcepoint Email Security is a bring-your-own license VA, so there is no additional Azure Marketplace charge.

    The system reports that it is creating the solution in the configured network. This process may take between 30 and 50 minutes.

Deploy Forcepoint Email Security in Azure with Forcepoint Security Manager on-premises

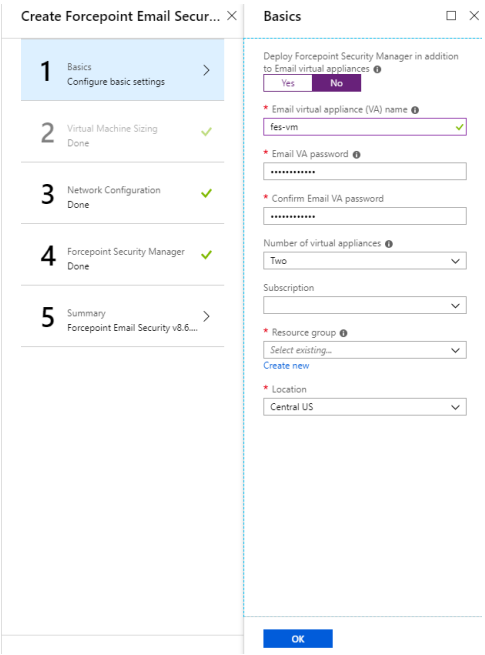
This type of deployment is available for versions **8.5**, **8.5.3**, or **8.5.4**. These steps are specific to versions **8.5.3**, and **8.5.4**; if you are deploying version **8.5**, see *Azure*

Deployment Steps: Version 8.5, page 15.

1. Create a site-to-site VPN.

   See Microsoft documentation for more information.
2. Log on to the Azure Marketplace, or use a direct link:
   - Forcepoint Email Security v8.5.4 in Azure
   - Forcepoint Email Security v8.5.3 in Azure
3. If you are installing in the Azure Government cloud:
   - Log into Azure Government, then click **Create a resource**.
   - In the Search bar, search for and select **Forcepoint Email Security**.
   - Click **Create**. All other steps are the same as in the Azure portal.
4. In the Search bar, search for Forcepoint, then select **Forcepoint Email Security V8.5.3** or **V8.5.4**.
5. To create a new Forcepoint Email Security solution, click **Get it now**.
6. Review the terms of use and privacy policy, then click **Continue** to proceed to the Azure portal.
7. From the Azure portal, click **Create**.

   The **Basics** tab displays for configuring the email appliance settings.



8. From **Deploy Forcepoint Security Manager in addition to Email virtual appliances**, click **No**.

   Options for Forcepoint Security Manager in Azure are removed from the tab.
9. In the text field **Email virtual appliance (VA) name**, enter a name for the Forcepoint Email Security virtual appliance (VA).

   The name must be between 3 and 30 characters long and contain only numbers, letters, and hyphens.

10. In the text fields **Email VA password** and **Confirm Email VA password**, enter and confirm the password for connecting to the host.

    The username is always “admin” on first login to Forcepoint Email Security. Additional accounts can be added later. The password must be a minimum of 12 characters and contain at least one number, one lowercase letter, one uppercase letter, and one special character.

11. From the pull-down menu **Number of virtual appliances**, select the number of VAs to use; between 1 and 8.

    Forcepoint recommends using at least two VAs to ensure high availability. If only one VA is selected at this time, it is not possible to add additional VAs after deployment is complete. If two or more VAs are selected, additional VAs can be added at any point. See Add virtual machines to a Forcepoint Email Security in Azure deployment.

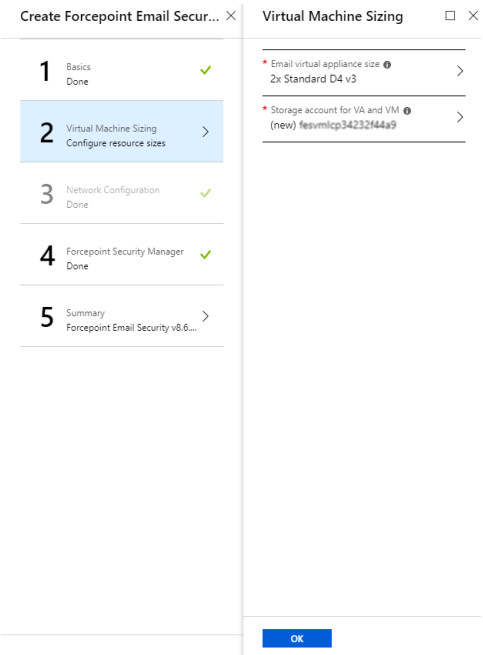
    Load balancers are deployed by default when two or more VAs are used.

12. From the pull-down menu **Subscription**, select your subscription.
13. From **Resource group**, click **Create new** and enter a name for the new resource group.

    A resource group is a container that holds related resources for an application. It will hold the Forcepoint Email Security VA. You must create a new resource group; using existing resource groups is not currently supported.

14. From the pull-down menu **Location**, select the location for the VA.
15. Click **OK**.

    The settings are saved and the **Virtual Machine Sizing** tab displays.



16. From **Email virtual appliance size**, select the size of the VA you will need based on anticipated email volume, then click **Select**.

    Use the Search fields if you need to find a different size.

17. From **Storage account for VA**, to use an existing storage account, click **Use existing** and select the storage account and disk type for the VA.

    To create a new storage account, click **Create new**.

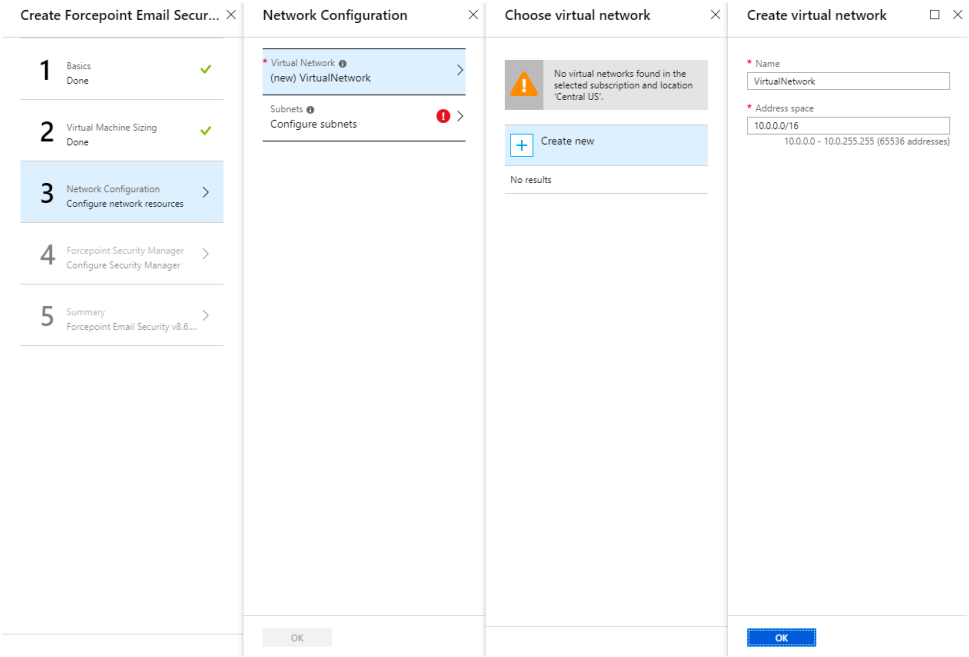
    The Create storage account tab displays.

    On the Create storage account tab, configure the Name, Account kind, Performance, and Replication settings and click **OK**.

    The new storage account is added.

18. From the Virtual Machine Sizing tab, click **OK**.

    The settings are saved and the **Network Configuration** tab displays.



19. From **Virtual Network**, select your existing virtual network with site-to-site connectivity to the on-premises Forcepoint Security Manager and SQL Server, or create a new virtual network.

    To create a new virtual network, click **Create New**.

    The Create virtual network tab displays.

    On the Create virtual network tab, configure the Name and Address space.

    Following successful deployment, configure your new virtual network to connect with your on-premises components.

20. From **Subnets**, select your existing subnet with site-to-site connectivity to the on-premises resources, or create a new subnet.

    The minimum supported size is /28 for the virtual network and subnet. See *Requirements*, page 4.

    Following successful deployment, configure your new subnet to connect with your on-premises components.

21. From the Network Configuration tab, click **OK**.

The settings are saved and the **Forcepoint Security Manager** tab displays.

22. This tab is blank because the contents are only applicable when deploying Forcepoint Security Manager in Azure. Click **OK**.

    The Summary tab displays.

23. From the **Summary** tab, review a summary of the Forcepoint Email Security solution you are building, then click **OK**.

    To change any configured settings, click one of the completed tabs. You will return to the Summary tab again after completing configuration.

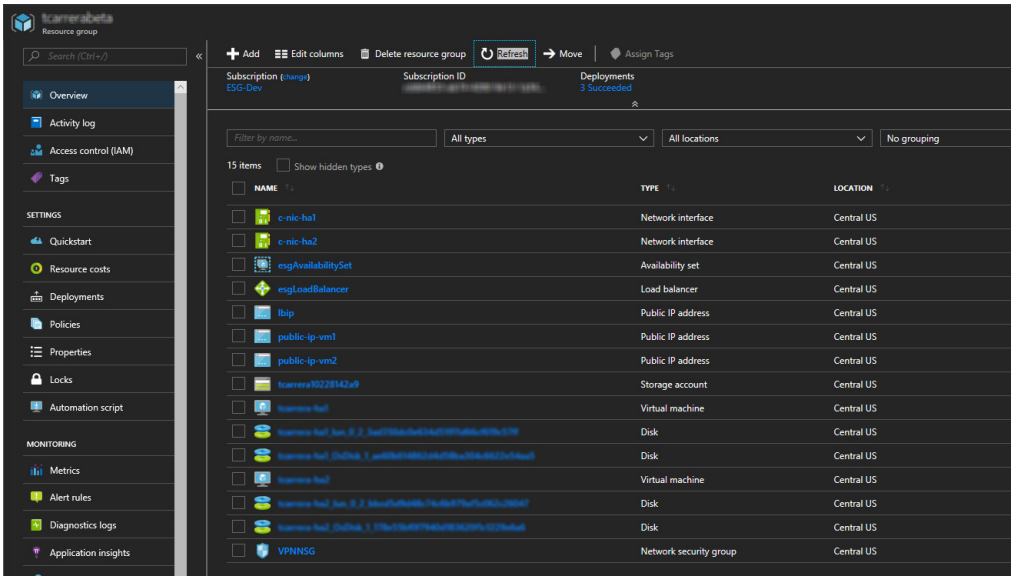
    Final validation is performed and the **Buy** tab displays.

24. On the Buy tab, review the Forcepoint Terms of Use, EULA, and Privacy Policy.

25. To create the Forcepoint Email Security solution in the Azure cloud infrastructure, click **Create**.

    Forcepoint Email Security is a bring-your-own license VA, so there is no additional Azure Marketplace charge.

    The system reports that it is creating the Forcepoint Email Security solution in the configured network. This process may take a few minutes. The following image displays the resource group for a typical Forcepoint Email Security in Azure deployment.



Azure Deployment Steps: Version 8.5

Use the following steps to deploy your version **8.5** Forcepoint solution in Azure:

1. *Deploy Forcepoint Email Security in Azure with Forcepoint Security Manager on-premises, version 8.5*, page 16
2. *Configuration in Microsoft Azure*, page 20
3. *Configure the system time zone*, page 20

4. *Install Forcepoint Security Manager management components for the virtual appliance*, page 21
5. *Configure the appliance in the Forcepoint Security Manager*, page 21
6. *Configure mail flow in Office 365*, page 24

For a high-level view of the procedure, see the Forcepoint Email Security in Azure Quick-Start Guide.

Deploy Forcepoint Email Security in Azure with Forcepoint Security Manager on-premises, version 8.5

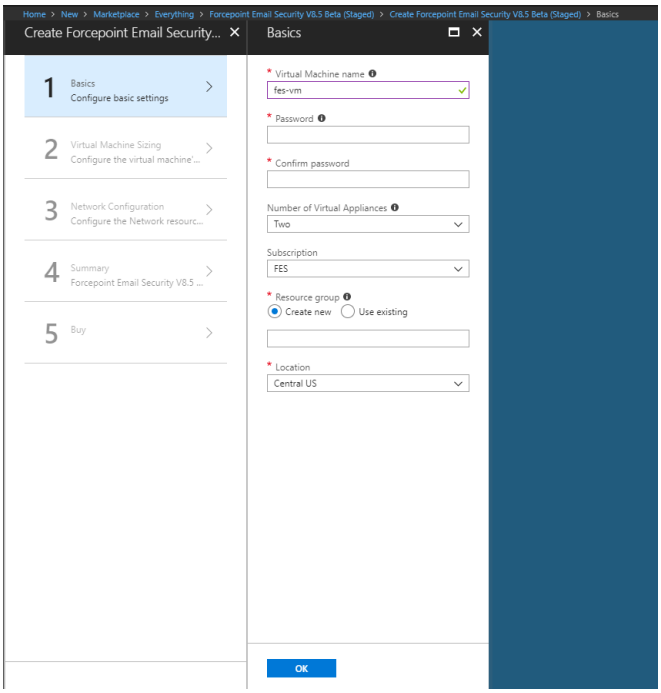
This is the only deployment option available for version **8.5**. These steps are specific to the version **8.5** solution in the Azure Marketplace.

1. Create a site-to-site VPN.

   See Microsoft documentation for more information.
2. Log on to the Azure Marketplace and click **Create a resource**.
3. In the Search bar, search for Forcepoint, then select **Forcepoint Email Security V8.5**.
4. To create a new Forcepoint Email Security solution, click **Create**.

   Alternatively, use this direct link to Forcepoint Email Security v8.5 and click Create.

   The **Basics** tab displays.



5. In the text field **Virtual Machine name**, enter a name for the Forcepoint Email Security virtual appliance (VA).

The name must be between 3 and 30 characters long and contain only numbers, letters, and hyphens.

6. In the text fields **Password** and **Confirm password**, enter and confirm the password for connecting to the host.

   The username is always “admin” on first login to Forcepoint Email Security. Additional accounts can be added later. The password must be a minimum of 12 characters and contain at least one number, one lowercase letter, one uppercase letter, and one special character.

7. From the pull-down menu **Number of Virtual Appliances**, select the number of VAs to use; between 1 and 7.

   Forcepoint recommends using at least two VAs to ensure high availability. If only one VA is selected at this time, it is not possible to add additional VAs after deployment is complete. If two or more VAs are selected, additional VAs can be added at any point. See Add virtual machines to a Forcepoint Email Security in Azure deployment.

   Load balancers are deployed by default when two or more VAs are used.

8. From the pull-down menu **Subscription**, select your subscription.

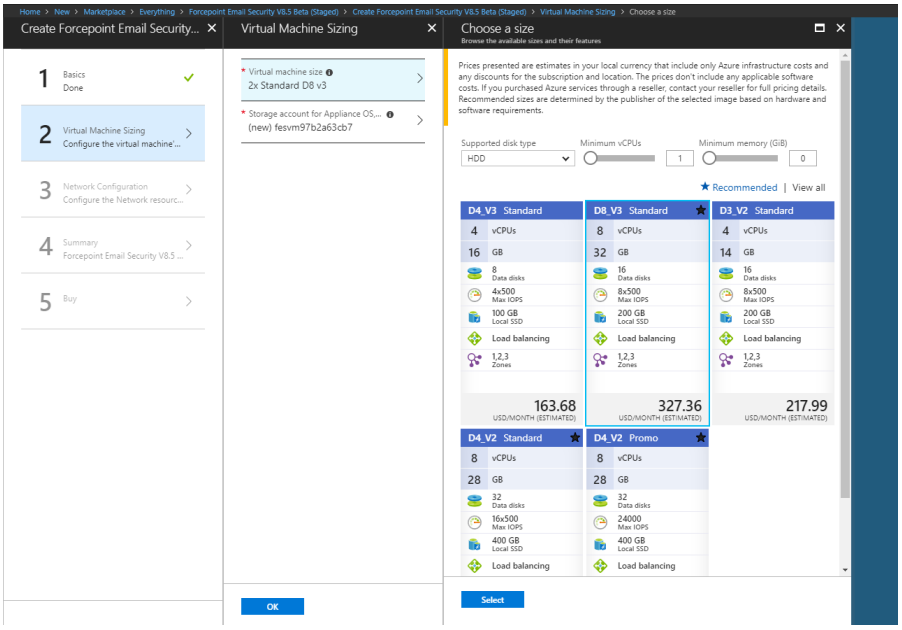
9. From **Resource group**, click **Create new** and enter a name for the new resource group.

   A resource group is a container that holds related resources for an application. It will hold the Forcepoint Email Security VA. You must create a new resource group; using existing resource groups is not currently supported.

10. From the pull-down menu **Location**, select the location for the VA.

11. Click **OK**.

    The settings are saved and the **Virtual Machine Sizing** tab displays.



12. From **Virtual machine size**, select the size of the VA you will need based on anticipated email volume, then click **Select**.

To locate a different size, click **View all**.

13. From **Storage Account for Appliance**, to use an existing storage account, click **Use existing** and select the storage account and disk type for the VA.

    To create a new storage account, click **Create new**.

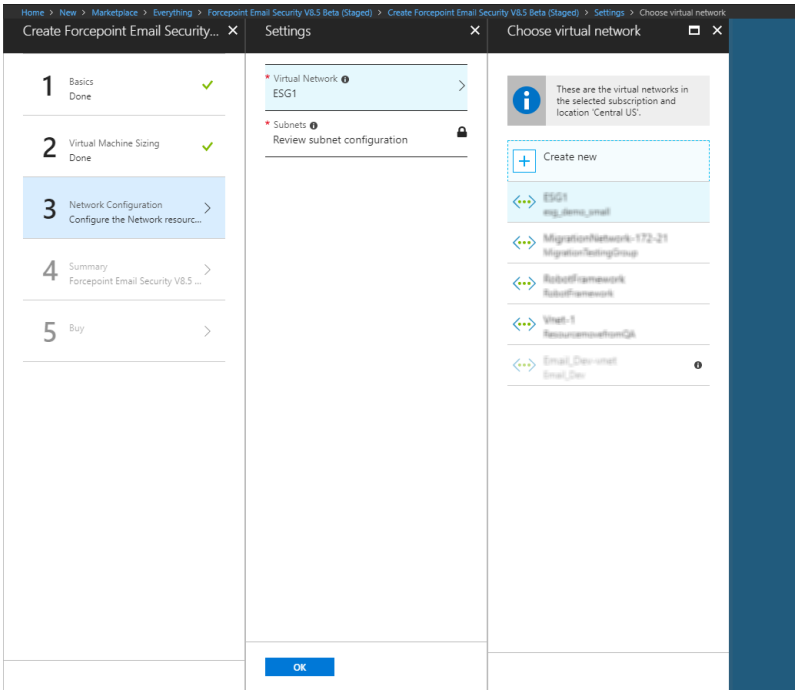
    The Create storage account tab displays.

    On the Create storage account tab, configure the Name, Performance, and Replication settings and click **OK**.

    The new storage account is added.

14. From the Virtual Machine Sizing tab, click **OK**.

    The settings are saved and the **Network Configuration** tab displays.



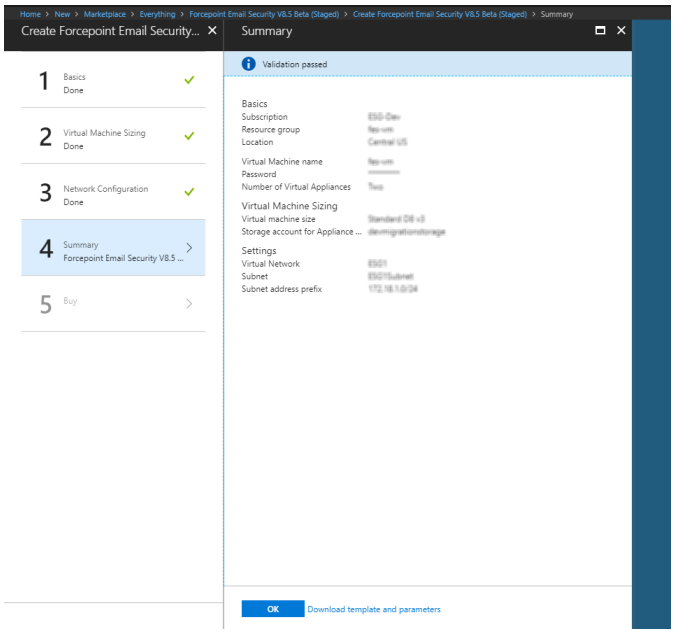
15. From **Virtual Network**, select your existing virtual network with site-to-site connectivity to the on-premises Forcepoint Security Manager and SQL Server. Use of a new virtual network is not supported.

16. From **Subnets**, select your existing subnet with site-to-site connectivity to the on-premises resources.

    Use of a new subnet is not supported. The minimum supported size is /16 for the virtual network and /24 for the subnet. See *Requirements*, page 4.

17. From the Network Configuration tab, click **OK**.

The settings are saved and the **Summary** tab displays.



18. From the **Summary** tab, review a summary of the Forcepoint Email Security solution you are building, then click **OK**.

    To change any configured settings, click one of the completed tabs. You will return to the Summary tab again after completing configuration.

    Final validation is performed and the **Buy** tab displays.
19. On the Buy tab, review the Forcepoint Terms of Use, EULA, and Privacy Policy.
20. To create the Forcepoint Email Security solution in the Azure cloud infrastructure, click **Create**.

    Forcepoint Email Security is a bring-your-own license VA, so there is no additional Azure Marketplace charge.

    The system reports that it is creating the Forcepoint Email Security solution in the configured network. This process may take a few minutes.

Post-Deployment Steps: All Versions

- *Configuration in Microsoft Azure*, page 20
- *Configure the system time zone*, page 20
- *Install Forcepoint Security Manager management components for the virtual appliance*, page 21
- *Configure the appliance in the Forcepoint Security Manager*, page 21
- *Configure mail flow in Office 365*, page 24
- *Create Email Log Database partitions when SQL Server is installed separately in Azure*, page 34

- *Configure encrypted connection to SQL Server*, page 35 (optional)
- *Install Email Security hotfixes*, page 38

Configuration in Microsoft Azure

It is necessary to add a DNS name for all public IP addresses when using Microsoft Office 365.

1. Select the public IP address for your Forcepoint Email Security VA.
2. Click **Configuration**.
3. From **DNS name label**, enter the DNS name for Office 365.
4. Click **Save**.

   The settings are saved.

As a best practice, use a static public IP address for your Forcepoint Email Security in Azure deployment. If you use a dynamic public IP address, the IP address will change if you reboot your machine.

It is necessary to use a static public IP address if your Forcepoint Email Security deployment includes the Forcepoint Email Security Hybrid Module, to avoid having to re-register with the cloud every time your machine is rebooted.

1. Select the public IP address for your Forcepoint Email Security VA.
2. Click **Configuration**.
3. From **Assignment**, click **Static**.
4. Click **Save**.

   The settings are saved.

Configure the system time zone

Forcepoint Email Security in Azure undergoes an initialization process following deployment. If your deployment includes Forcepoint Security Manager on-premises, wait at least 15 minutes before configuring the VA.

1. Configure the timezone on your virtual appliance using the CLI.
   a. Enter config mode:

      ```
      config
      ```

   b. Enter your password.

      This is the same password used in step 7 of *Deploy both Forcepoint Email Security and Forcepoint Security Manager together in the Azure cloud*, page 5.
2. View all available time zones:

   ```
   show system timezone-list
   ```

   The time zones display.
3. Set the correct time zone by using either the time zone name or index number:

```
set system timezone --zone "Central Time"
set system timezone --index 9
```

The system time zone is set.

Install Forcepoint Security Manager management components for the virtual appliance

These steps are only necessary if Forcepoint Security Manager is deployed on-premises.

1. If you have not installed Forcepoint DLP on the management server, follow the installation instructions here.
2. The Forcepoint Email Security installer launches automatically. Use this installer to install the necessary email components on the manager. On the remaining screens, enter only the internal IP addresses of the Azure appliances.

   Version **8.5**: if you are already running Forcepoint Email Security on-premises, it is not possible to add email appliances in Azure to the same Forcepoint Security Manager.

   Versions **8.5.3** and **8.5.4**: your deployment may include an on-premises Forcepoint Security Manager with email appliances in Azure.
3. On the Welcome screen, click **Next**.
4. Enter the local IP address and port of the SQL database to use for storing management data.

   Include the user name and password for the database account.
5. Enter a location for the database files or accept the default value.
6. On the Email Appliance page, enter the IP address or host name of the VA you created when deploying the appliance in Azure and then click **Next**.
7. Specify where to install the software.
8. Click **Install**.

Configure the appliance in the Forcepoint Security Manager

Forcepoint Email Security steps

Some initial configuration settings are important for Forcepoint Email Security operation. Perform the following activities after you install the Forcepoint Email Security management components.

1. Log on to the Forcepoint Security Manager and select **Email**.

   The Email module displays.
2. At the prompt, enter your subscription key and click **OK**.

   The Configuration Wizard displays for first-time setup.

   If you skip this step, you can enter your subscription key later on the page **Settings > General > Subscription**.

3. Use the Configuration Wizard to quickly configure certain settings before opening Forcepoint Email Security.

   See Using the first-time Configuration Wizard.

4. Register the Forcepoint Email Security DLP Module.

   During installation in Azure, only one of your email VAs is registered to DLP; following installation, it is necessary to register the rest of your appliances.

5. Navigate to **General > Data Loss Prevention** and verify which appliance is already registered. Next, register each additional appliance.

   The DLP Module can be registered at any point, but it is recommended to do this before any other configuration is completed. See Registering the DLP Module.

6. Configure an appliance cluster.

   An appliance cluster is necessary when using load balancers, which are deployed by default for a deployment of Forcepoint Email Security in Azure with two or more VAs.

   Clustered appliances must all share the same platform; i.e., your Azure appliances cannot be clustered together with on-premises virtual appliances or physical appliances.

   Appliance clusters are not available for Forcepoint DLP Email Gateway.

   a. Navigate to **Settings > General > Cluster Mode**.

   b. Select the appliance mode **Cluster (Primary)**.

      A Cluster Properties box opens with the primary appliance IP address displayed in the field **Cluster communication IP address**. Secondary appliances use this IP address for cluster communication.

   c. Click **Add**.

      The page Add Secondary Appliance displays, where you can designate the secondary appliances in this cluster.

      (*Optional*) Add a new appliance that is not already in this list; click **Add New Appliance**.

      The Add Appliance page displays.

   d. Click the arrow button to add the appliances to the Secondary Appliances list.

   e. Click **OK**.

      The appliance is added to the Secondary Appliances list along with its status.

   f. On the page Cluster Mode, click **OK**.

      The appliance is added to the cluster.

      See Configuring an appliance cluster.

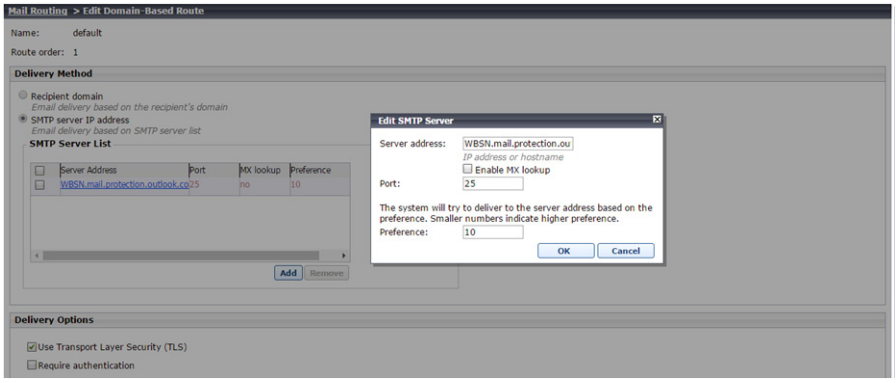
7. Configure the system to send email through Office 365 to Forcepoint Email Security in Azure.

   a. Navigate to **Settings > Inbound/Outbound > Mail Routing**.

   b. Select the default route.

   c. From Delivery Method, select **SMTP server IP address**.

d. Under SMTP Server List, click **Add**.



e. For Server Address, add the FQDN of your organization's Microsoft Office 365 account. This is the same as the MX record of the Office 365-hosted domain. To find it:
   - In the Office 365 Admin Center, select **Settings > Domains**.
   - Select the domain name you configured for your organization.
   - Under Exchange Online, you will see a row for MX. The MX record is listed in that row.

f. For Port, enter **25**.

g. Enter a Preference.

h. Click **OK**.

i. Under Delivery Options, select **Use Transport Layer Security (TLS)**.

j. Click **OK**.

k. Repeat this step for each Forcepoint Email Security VM you have.

8. Specify an email address to which system notification messages should be sent. This is typically an administrator address. See Setting system notification email addresses.

9. In the Email module, data loss prevention policies are enabled by default. To manage DLP policies, navigate to **Main > Policy Management > DLP Policies > Manage Policies**.

10. In the Data module, you can view all of the VAs in the System Modules list. Select the Data tab and click **Deploy**.

    Click **Help** on any Forcepoint Security Manager page for help about the page. See Forcepoint DLP Email Gateway Help for complete information about the DLP Module.

Forcepoint DLP steps

These steps are necessary if you have existing DLP policies, or if Forcepoint Security Manager is deployed on-premises.

1. From the Forcepoint Security Manager, select **Data**.
2. Add the network email destination to any existing policies that should be used for this appliance.

3. Click **Deploy**. No other configuration steps are required.

A Forcepoint DLP Email Gateway module is shown on the System Modules page, as well as System Health and System Logs.

Use the System Modules page to edit the display name or description for the appliance. If desired, you can balance the load on the gateway by selecting **System Modules > Load Balancing** and then editing the Forcepoint DLP Email Gateway module.

Refer to Forcepoint DLP Administrator Help for more information.

Configure mail flow in Office 365

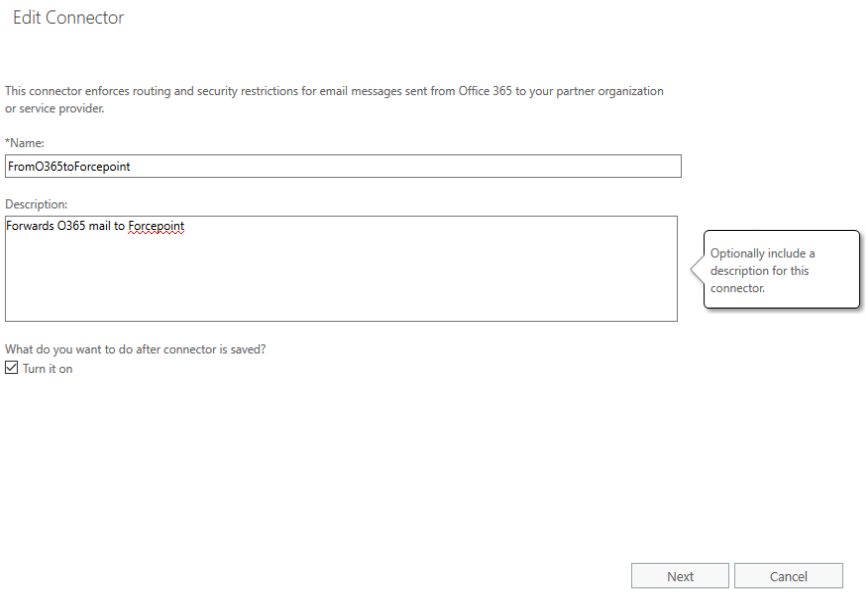
Following deployment, it is necessary to configure Office 365 to transfer email to Forcepoint Email Security in Azure.

DNS records are used to ensure that mail flows correctly to Forcepoint Email Security. Before configuring Office 365, log into your domain and configure the mail flow settings accordingly.

If you are deploying in Azure Government, only Office 365 Government is supported.

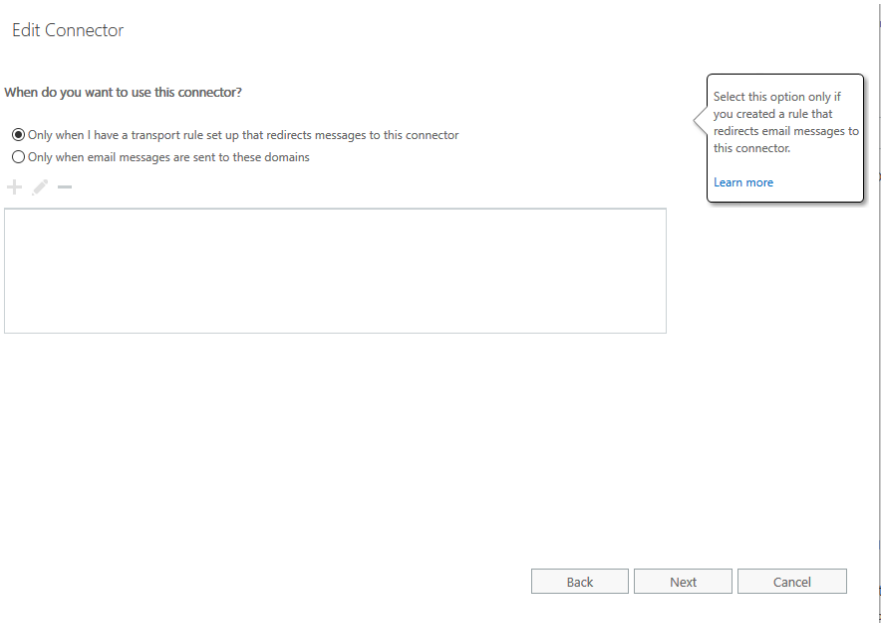
1. Log on to Microsoft Office 365, https://outlook.office365.com/ecp
2. From the left navigation pane, select **Admin > Exchange**.
3. From the left navigation pane, select **Mail Flow**.
4. Create a connector that routes mail from Office 365 to Forcepoint Email Security in Azure:
   a. From the top of the page, click **Connectors**, and then click the **plus sign (+)** to add a new connector.
   b. In the field **From**, select **Office 365**; in the field **To**, select **Your organization's email server**.
   c. Click **Next**.

d. Enter a name and description for the connector. (This is a new name being assigned to the Forcepoint Email Security appliance.)



e. Click **Next**.

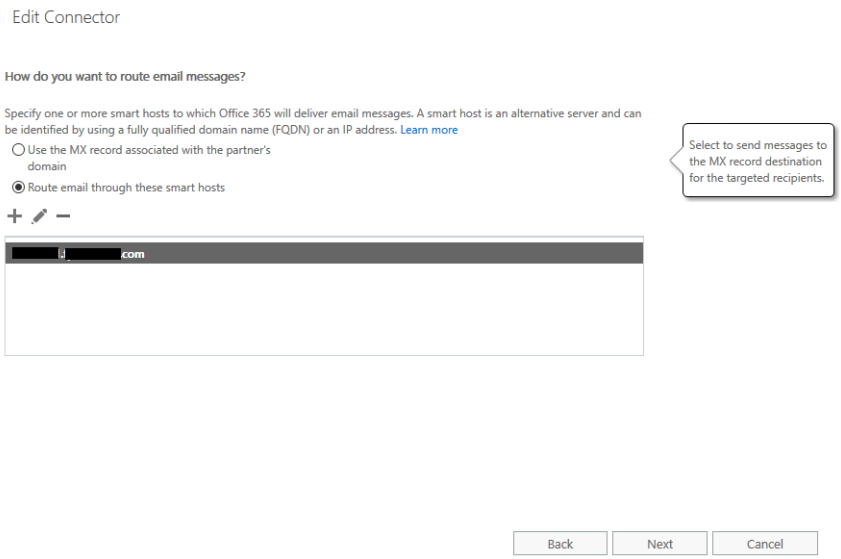
f. From **When do you want to use this connector,** select **Only when I have a transport rule set up that redirects messages to this connector**.



g. Click **Next**.

h. From **How do you want to route email messages**, select **Route email through these smart hosts**.

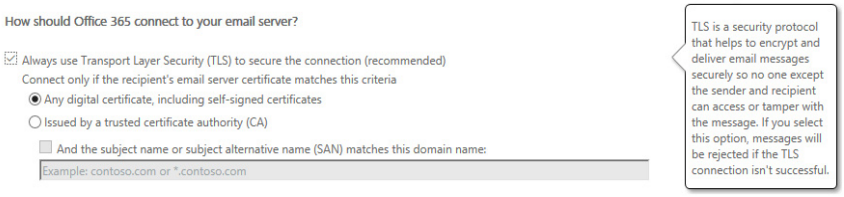
i. Click the **plus sign (+)** and enter the public IP address for the Forcepoint Email Security VA in Azure appended with your domain name.



j. Click **Next**.

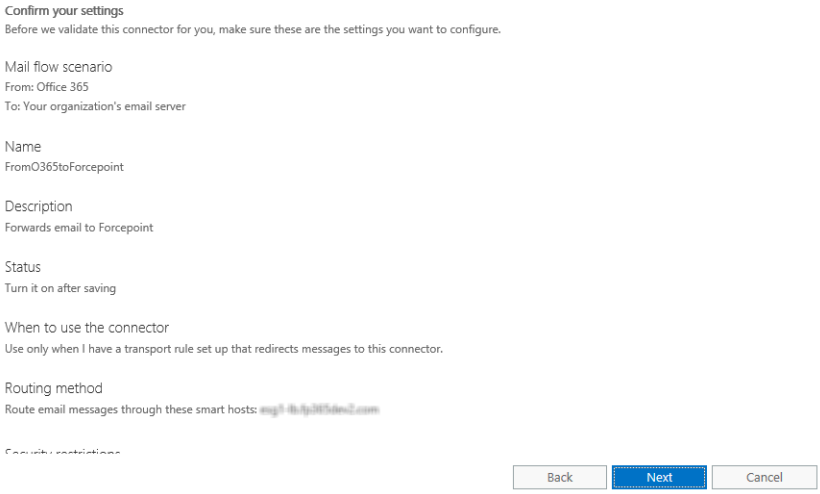
k. From **How should Office 365 connect to your email server**, select **Always use TLS to secure the connection**.

l. Select **Any digital certificate, including self-signed certificates**.



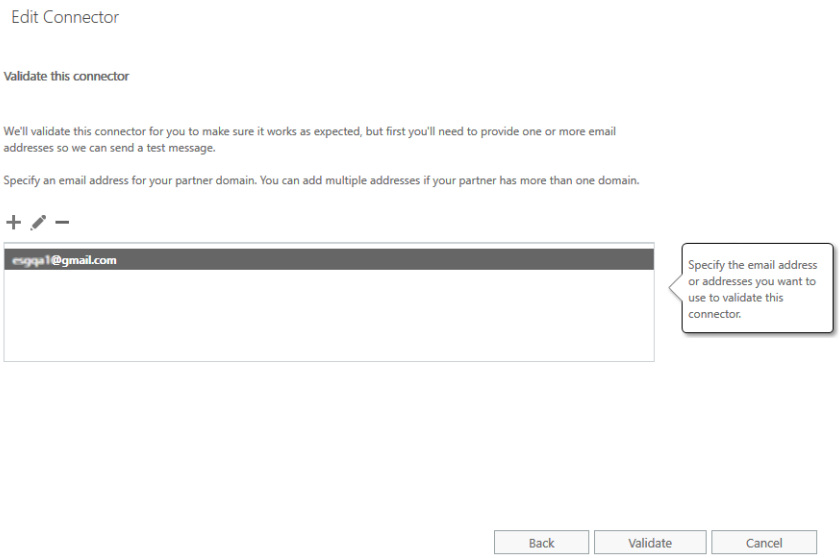
m. Click **Next**.

A summary screen displays.



n. Confirm that your settings are correct, then click **Next**.

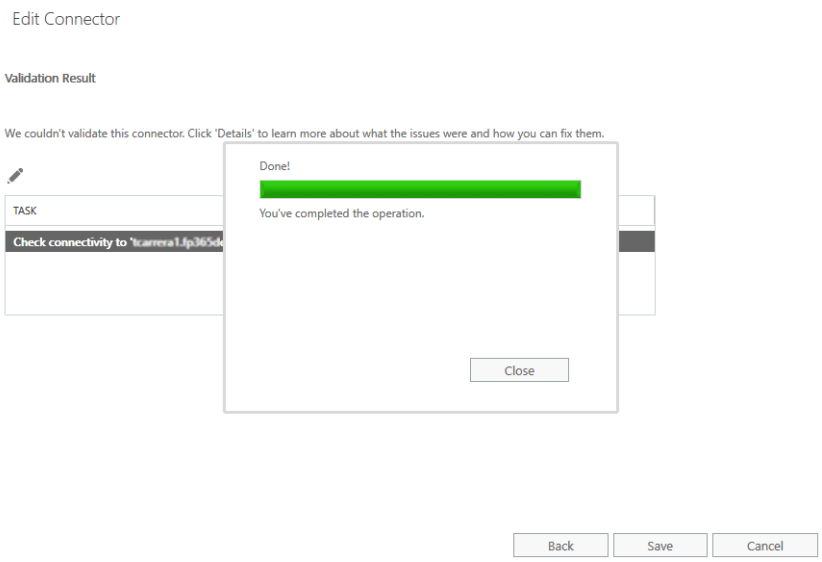
o. From **Validate this connector**, click the **plus sign (+)** and then enter a test email address.



p. Click **Validate**.

The system validates the new connector and sends a test email. A success message displays when validation is complete.

The validation may return a Failed result. If this happens, a warning message displays with a prompt to save the connection. Despite the failed validation, the connection can be saved and used.



q. Click **Close**.

   The validation window closes.

r. Save the connector; click **Save**.

   The connector is saved.

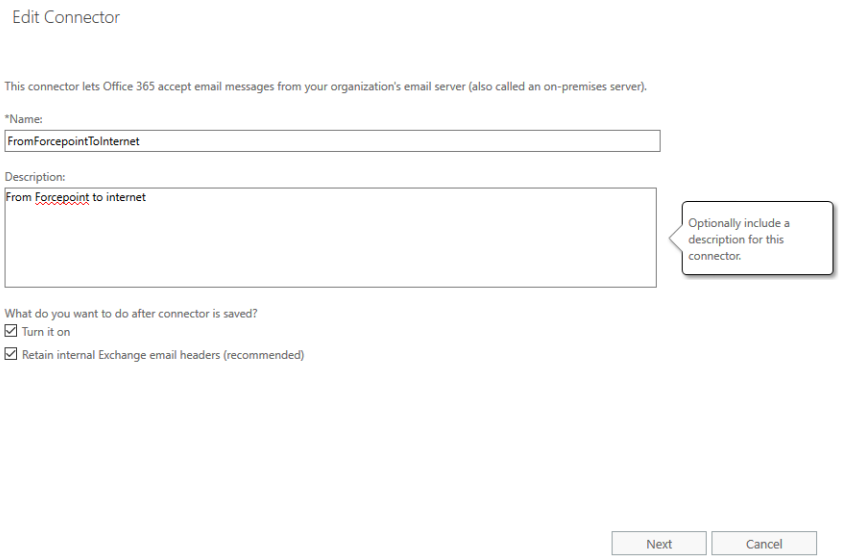
5. Create a second connector that routes mail from Forcepoint Email Security in Azure to Office 365.

   a. From the top of the page, click **Connectors**, and then click the **plus sign (+)** to add a new connector.

   b. This time, in the field **From**, select **Your organization's email server** and in the field **To**, select **Office 365**.

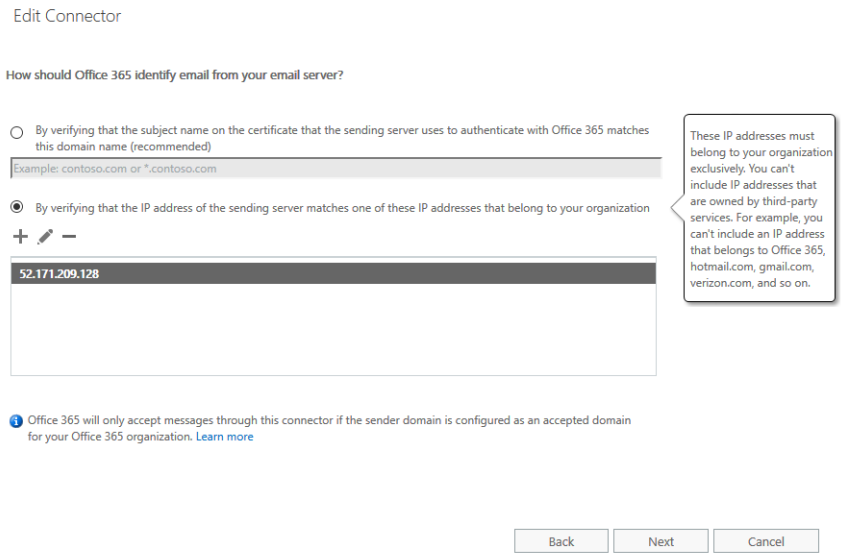
   c. Click **Next**.

d. Enter a name and description for the connector.



e. Click **Next**.

f. From **How should Office 365 identify email from your email server**, select one of two options.



- For best practice, select **By verifying that the IP address of the sending server...**, and enter all public IP addresses for the Forcepoint Email Security VA in Azure.

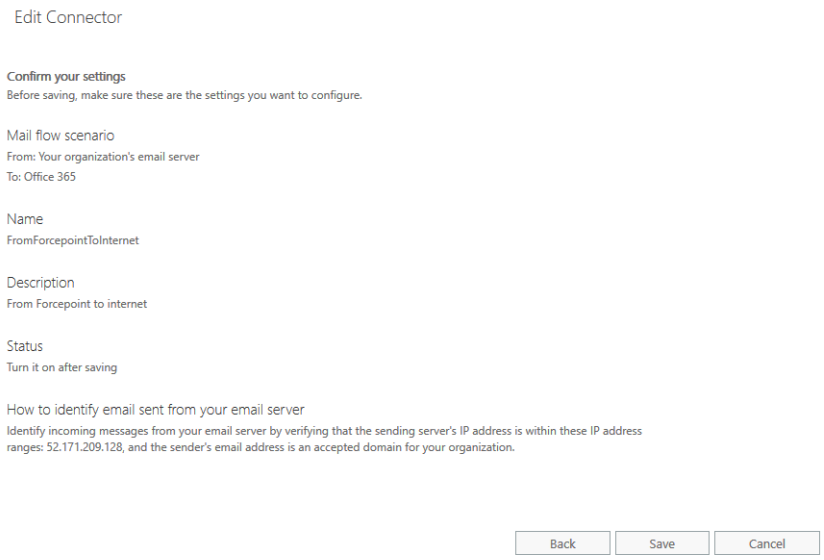
  It is recommended to use a static public IP address. If you use a dynamic public IP address, the public IP address will change if you reboot your machine.

- Alternatively, select **By verifying that the subject name on the certificate...** and enter the CN of a signed certificate purchased through a vendor like Godaddy or Digicert.

  For more information on setting up certificate validation, refer to Configuring Exchange Online to use certificate validation in the Forcepoint Knowledge Base.

g. Click **Next**

A summary screen displays.



h. Confirm that your settings are correct, then click **Save**.

The connector is saved.

6. Create rules that forward traffic to Forcepoint Email Security in Azure.

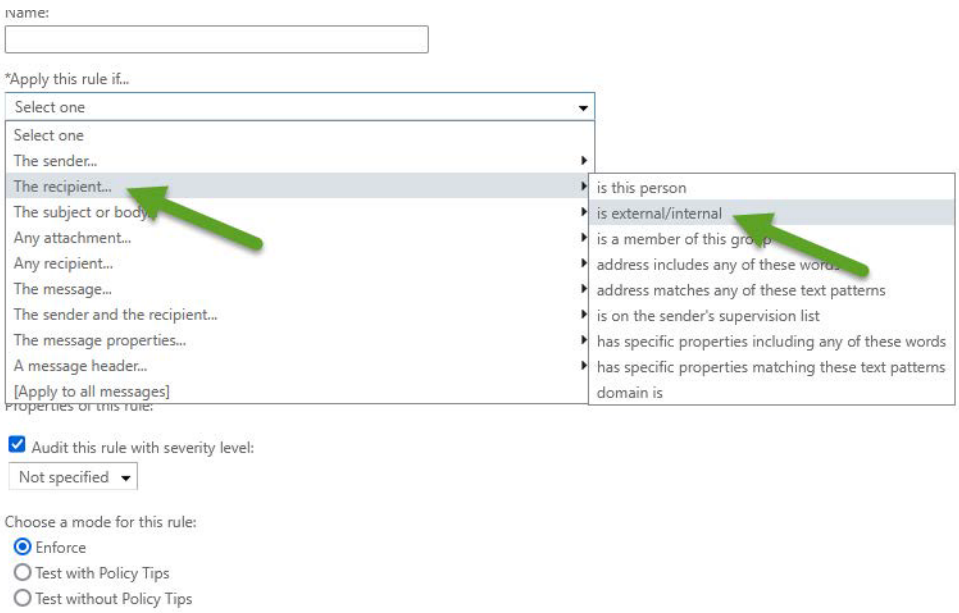
   a. From the top of the page, select **Rules**, then click the **plus sign (+)** to create a new rule.

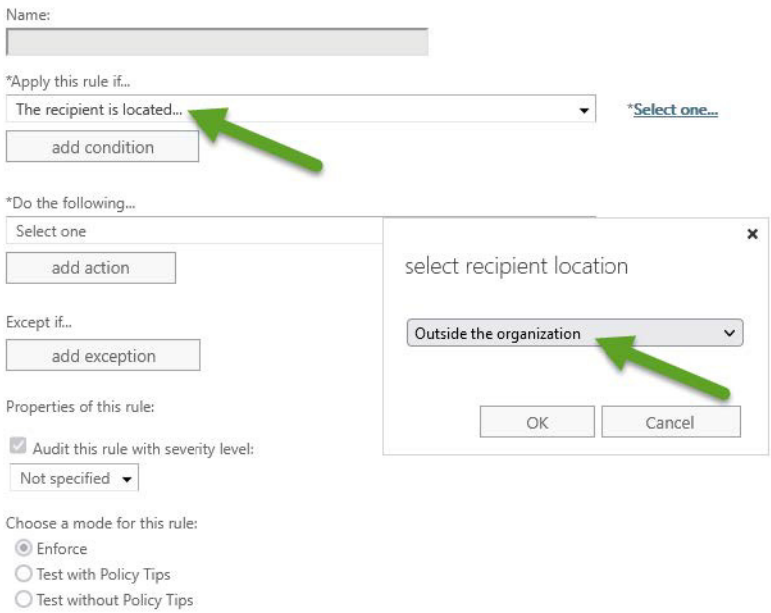
   b. Assign a name to the rule.

   c. Click **More options**.

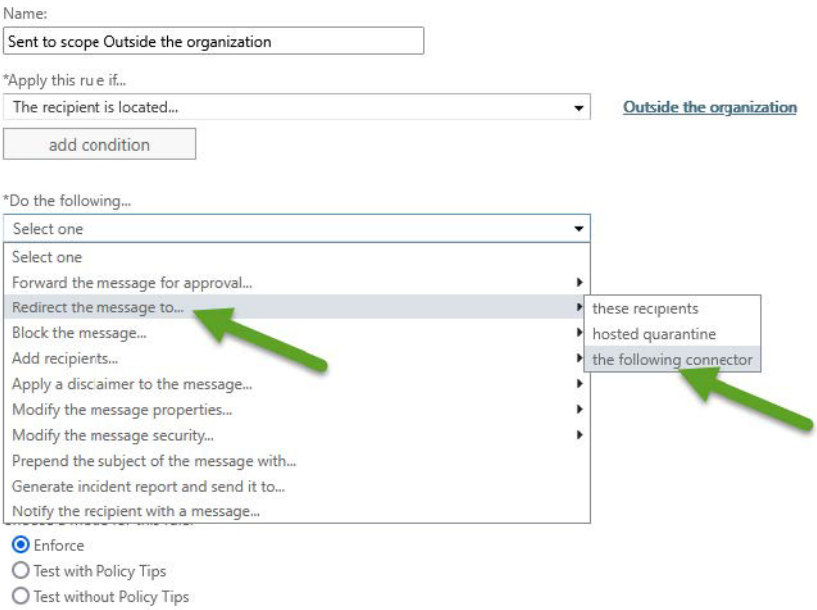
   To audit outbound-only email messages:

d. Select the condition **Apply this rule if the recipient is outside the organization**, as shown in the following images.

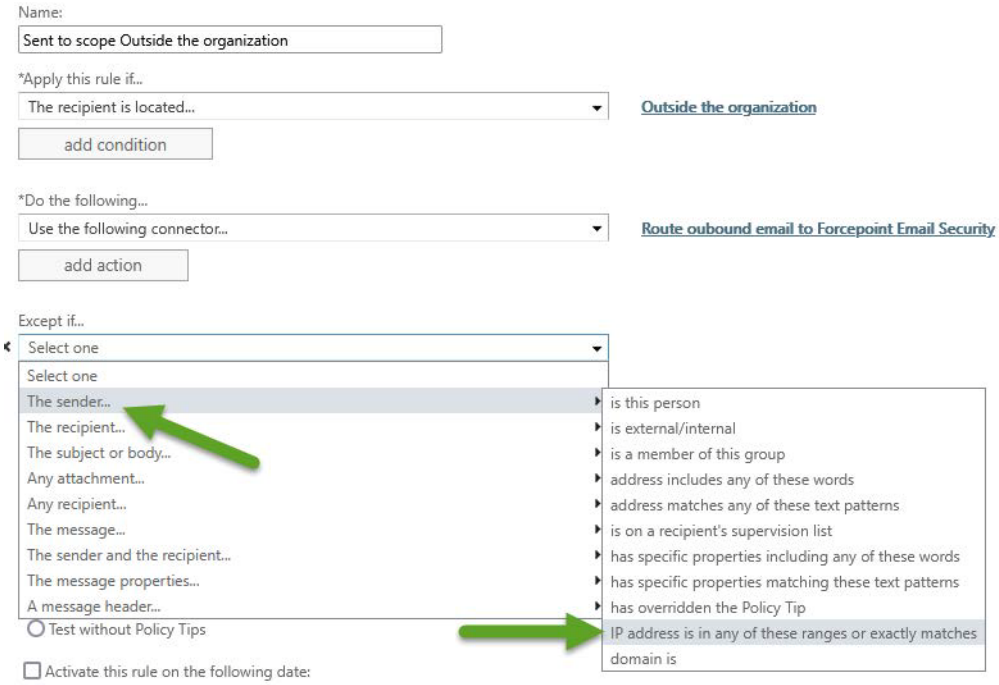




e. Select the action **Redirect to... the following connector**.



f. Add the exception **Except if the sender IP address is in any of these ranges or exactly matches**.



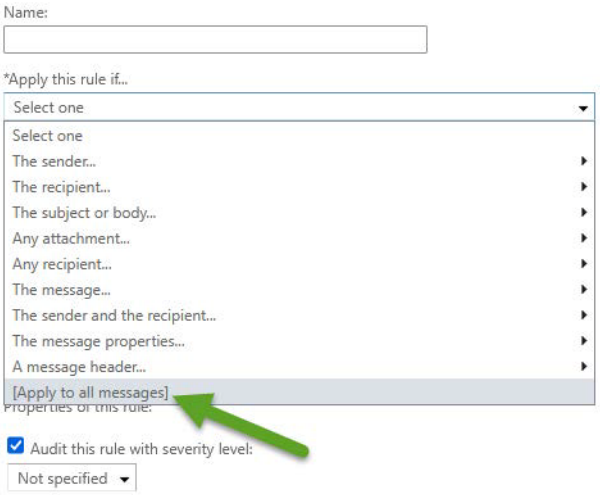
It is recommended to select the option **Stop processing more rules**.

If this option is not selected and there are additional rules, email messages are evaluated against the additional rules, then redirected to the connector. If the option is selected and there are additional rules, email messages are not evaluated against the additional rules, but simply returned to the connector.

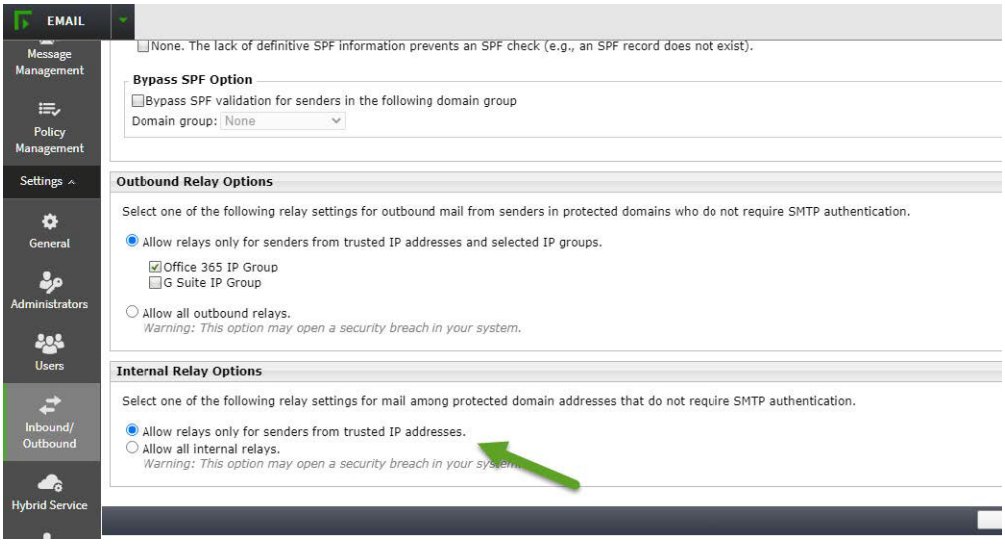
Usually, Forcepoint Email Security appliances relay email messages back through Office 365, so Exchange Online repeatedly processes the same email message and applies rules, but in this case, email messages are not sent through the email appliance.

To audit both internal and outbound email messages, the process is the same, except for the condition:

g. Select the condition **Apply this rule [Apply to all messages]**.



h. If you select **[Apply to all messages]**, go to Forcepoint Security Manager and configure your email appliance to accept relays on internal email messages, by adding the IP ranges from Exchange Online to the Trusted IP group. If this step is not done, internal email messages will not be accepted by the appliance. See Adding an IP address group in *Forcepoint Email Security Administrator Help* for more information.



i. Save the rule; click **Save**.

The rule is saved.

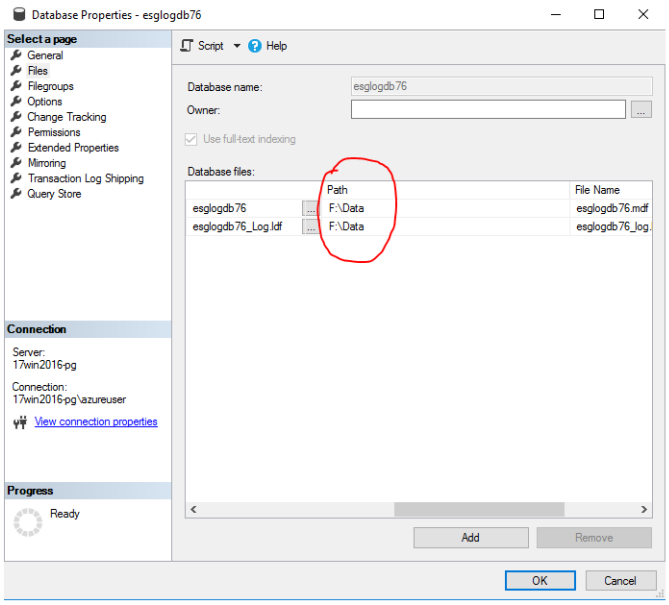
7. Make sure none of the public static IPs used by Forcepoint Email Security in Azure is listed in SpamHaus and thus blocked by Office 365, likely in the Policy Block List (PBL).
   a. Go to http://www.spamhaus.org/lookup.lasso and enter each IP.
   b. If any is listed, follow the instructions to remove it.

      For more information, read https://www.spamhaus.org/faq/section/Spamhaus%20PBL.

Create Email Log Database partitions when SQL Server is installed separately in Azure

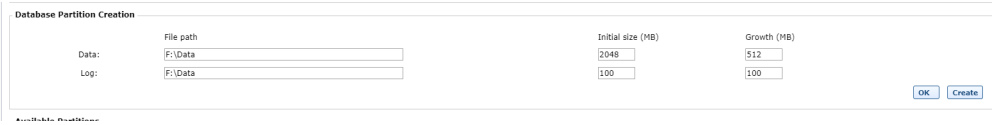
If your deployment includes Forcepoint Security Manager in Azure and a remote SQL Server on a separate VM in Azure, you may experience an error in which Log Database fails to create a partition for the default file path “C:\db\”. Follow the workaround below for this issue.

1. In SQL Server Management Studio on the SQL Server machine, right-click **esglogdb76**, then click **Properties** and **Files**.
2. On the Files page, under “Path,” locate the MDF folders for “Data” and “Log.”



3. Log into the Forcepoint Security Manager.
4. Navigate to the page **Settings > Reporting > Log Database**.
5. Under Database Partition Creation, under **Data** and **Log**, change the file paths to the MDF values from step 2.
6. Click **OK**.

The settings are saved.

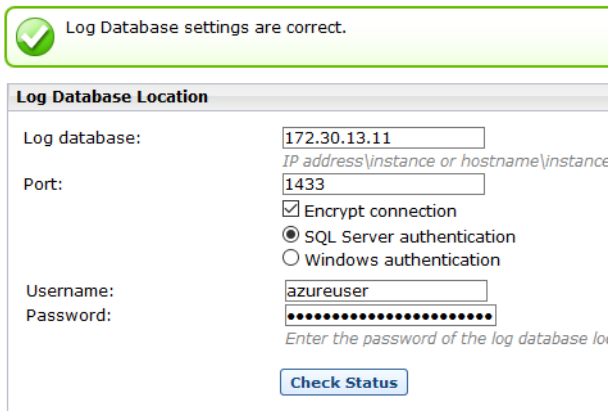


Configure encrypted connection to SQL Server

If your deployment includes Forcepoint Security Manager in Azure and a remote SQL Server, use the following steps after installation to configure an encrypted connection between SQL Server and Forcepoint Email Security components. These steps are only necessary if you did not choose to encrypt connection during Step 28 of your initial deployment.

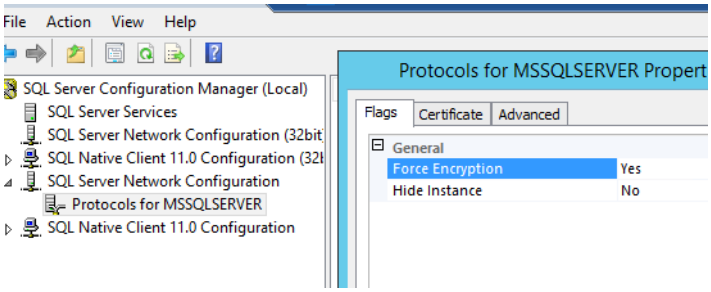
1. Follow the steps outlined in *Deploy both Forcepoint Email Security and Forcepoint Security Manager together in the Azure cloud*, page 5, and configure the settings for your remote SQL Server.
2. After deployment is complete, log on to the Forcepoint Security Manager and select **Email**.

   The Email module displays.
3. Navigate to **Settings > Reporting > Log Database**.
4. In the section **Log Database Location**, enter the IP address of the remote SQL Server.
5. Mark the check box **Encrypt connection**.
6. (*Optional*) Click **Check Status** to verify the availability of the server.
7. Ensure that the additional settings are correct and click **OK**.

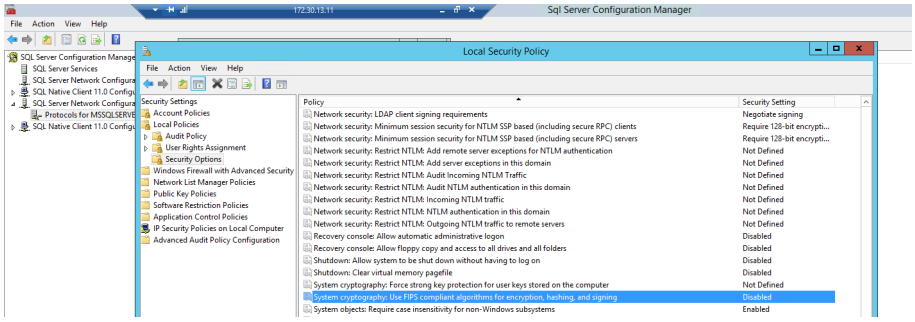


8. Open SQL Server Configuration Manager and navigate to **SQL Server Network Configuration > Protocols for MSSQLSERVER > Properties**.
9. On the tab Flags, change Force Encryption to **Yes**.

10. Save settings.

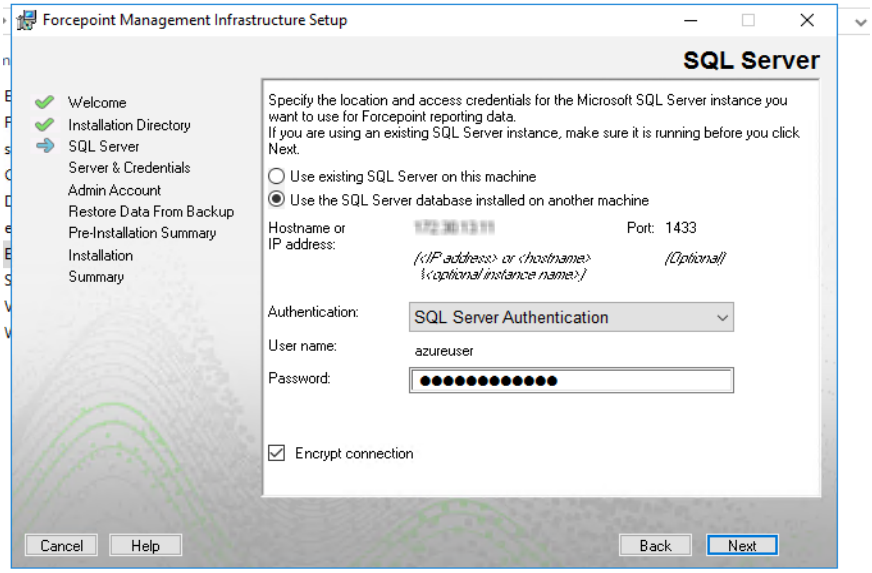


11. Navigate to **Local Security Policy > Local Policies > Security Options > System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
12. Change Properties to **Enabled**.

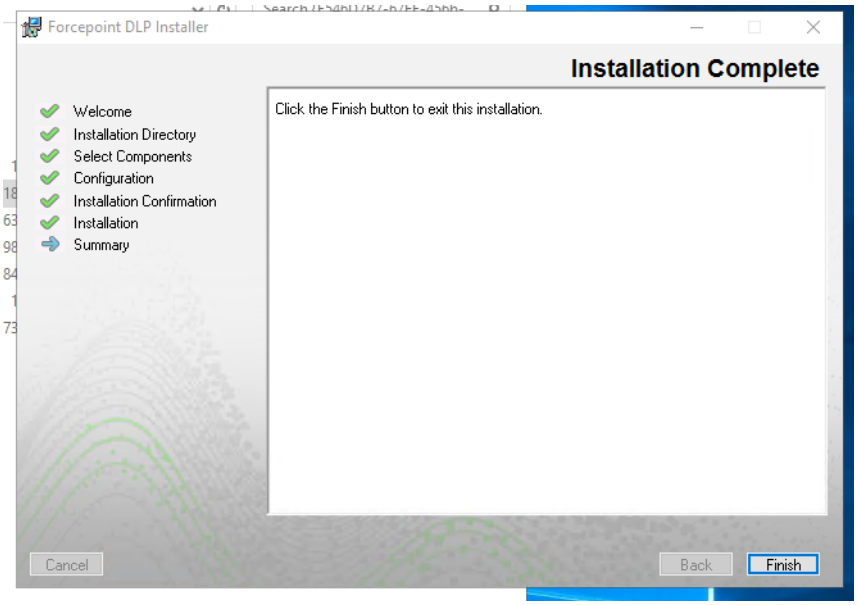


13. Save settings and close.
14. Restart the SQL Server.
15. On the Forcepoint Security Manager virtual machine, log out of Forcepoint Security Manager.
16. Open a command prompt and run `ipconfig`. Make note of the current settings.
17. Navigate to the Windows network settings and set the IP address, netmask, and default gateway.
18. Start the **Forcepoint Security Installer**.
19. On the Modify Installation dashboard, click **Modify** for Forcepoint Infrastructure.
20. On the Welcome screen, click **Modify**.

21. Proceed to the SQL Server screen and enter the current hostname or IP address, port, user name, and password, then mark the check box **Encrypt connection**.

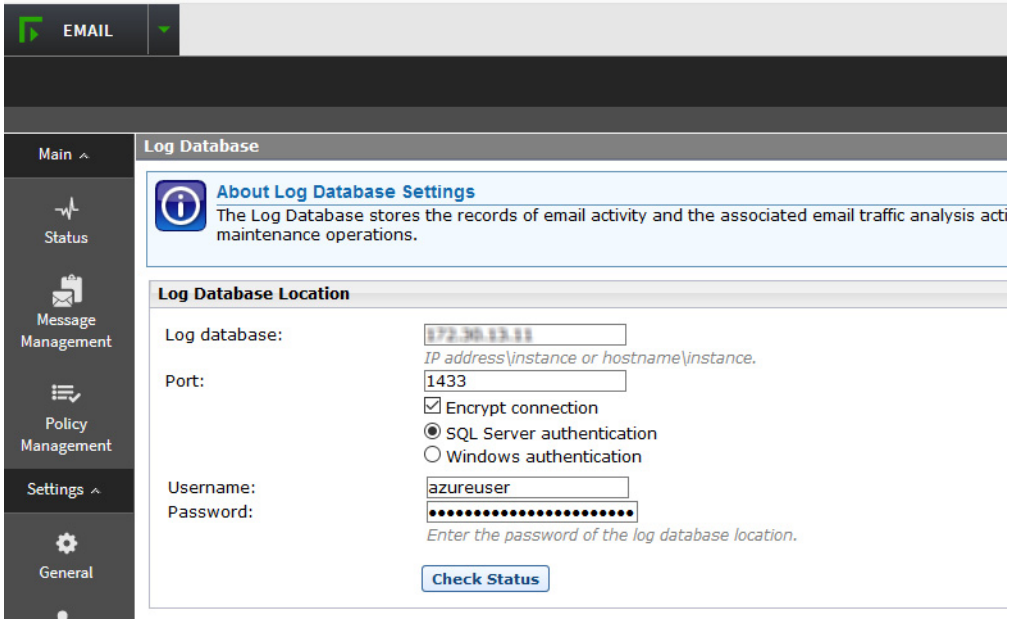


22. Proceed through the other screens and click **Finish**.
23. On the Modify Installation dashboard, click **Modify** for Forcepoint DLP.
24. Changes may not be needed on these screens; verify that the installation is complete as you proceed, then click **Finish**.



25. Wait a few minutes for services to refresh, then open Windows Services and verify that all Forcepoint services are running.
26. Log into Forcepoint Security Manager and navigate to **Settings > Reporting > Log Database**. Verify that the settings are correct.

Forcepoint Security Manager may take a few minutes to load. Do not log out or stop services.



Install Email Security hotfixes

Navigate to the page Forcepoint My Account Downloads and select your version, then install the latest Windows and appliance hotfixes.

Alternatively, appliance hotfixes can be installed using the appliance command-line interface (CLI) or Forcepoint Security Appliance Manager (FSAM). See Forcepoint Appliances CLI Guide and Forcepoint Security Appliance Manager Help for more information.

© 2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.