Installing Forcepoint Email Security in Microsoft Azure

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

Topics:

- Forcepoint Email Security in Azure: Deployment Scenarios
- Requirements
- Azure Deployment Steps: Versions 8.5.3 and 8.5.4
 - Deploy both Forcepoint Email Security and Forcepoint Security Manager together in the Azure cloud
 - Deploy Forcepoint Email Security in Azure with Forcepoint Security Manager on-premises
- Azure Deployment Steps: Version 8.5
- Post-Deployment Steps: All Versions
 - Configuration in Microsoft Azure
 - Configure the system time zone
 - Install Forcepoint Security Manager management components for the virtual appliance
 - Configure the appliance in the Forcepoint Security Manager
 - Configure mail flow in Office 365
 - Create Email Log Database partitions when SQL Server is installed separately in Azure
 - Configure encrypted connection to SQL Server
 - Install Email Security hotfixes

Related documents:

- <u>System requirements</u>
- <u>Forcepoint Email Security Administrator Help</u>

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.

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 <u>Azure Government</u> 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 <u>Email hybrid service configuration</u>.) 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 <u>Deployment and Installation Center</u> 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 <u>Default ports</u> for more information.
 - Refer to the <u>Certified Product Matrix</u> 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 <u>Forcepoint Email Security in Azure</u> <u>Quick-Start Guide</u>.

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 <u>Azure Marketplace</u>, 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 <u>Azure Government</u>, 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.

reate Forcepoint Email S	ecur ×	Basics 🗆 🗆
Basics Configure basic settings	>	Deploy Forcepoint Security Manager in addition to Email virtual appliances () Yes No
2 Virtual Machine Sizing Configure resource sizes	>	Email Virtual appliance (VA) name fes-vm Email VA password
3 Network Configuration Configure network resources	>	* Confirm Email VA password
4 Forcepoint Security Manager Configure Security Manager	>	Number of virtual appliances
5 Summary Forcepoint Email Security v8	>	Forcepoint Security Manager virtual machine (VM) name fsm-vm security Manager VM user name
		★ Security Manager host password ●
		* Confirm Security Manager host password
		Subscription V
		* Resource group
		Create new
		East US V

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 <u>Add virtual machines to a Forcepoint Email Security in Azure</u> <u>deployment</u>.

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.

Create Forcepoint Email Secur $ imes$	Network Configuration $\qquad imes$	Choose virtual network $\qquad imes$	Create virtual network \Box \times
1 Basics 🗸	* Virtual Network (new) VirtualNetwork	No virtual networks found in the selected subscription and location	* Name VirtualNetwork
2 Virtual Machine Sizing	Subnets O O > Configure subnets	Create new	* Address space 10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)
3 Network Configuration > Configure network resources		No results	
4 Forcepoint Security Manager > Configure Security Manager			
5 Summary Forcepoint Email Security v8.6 >			
	ОК		OK

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.

Create Forcepoint Email Secur $ imes$	Forcepoint Security Mana		
1 Basics 🗸	Security Manager administrator email Security Manager password		
2 Virtual Machine Sizing	* Confirm Security Manager password		
3 Network Configuration	Use remote SQL Server instance ① Yes No		
4 Forcepoint Security Manager > Configure Security Manager	* Remote SQL Server host 🕑		
5 Summary > Forcepoint Email Security v8.6 >	1433 * Remote SQL Server user name		
	★ Remote SQL Server password ●		
	* Confirm remote SQL Server password		
	* Remote SQL Server host user name 🜒		
	* SQL Server host password		
	Enable archiving and backup		
	Yes No		

- 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 <u>Configuring the certificate for encrypted SQL Server</u> 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 <u>Azure Marketplace</u>, 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 <u>Azure Government</u>, 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 <u>Add virtual machines to a Forcepoint Email Security in Azure deployment</u>.

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.

Create	e Forcepoint Email Sec	ur $ imes$	Virtual Machine Sizing	$\Box \times$
1	Basics Done	~	 Email virtual appliance size 2x Standard D4 v3 	>
2	Virtual Machine Sizing Configure resource sizes	>	 ★ Storage account for VA and VM ● (new) fesvmlcp34232f44a9 	>
3	Network Configuration Done	~		
4	Forcepoint Security Manager Done	~		
5	Summary Forcepoint Email Security v8.6	. >		
			ок	

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.

Resource group			
	+ Add ≣≣ Edit columns	🔷 Assign Tags	
	Subscription (change) Subscription ID [Deployments	
Overview	ESG-Dev 3	Succeeded	
Activity log			
Access control (IAM)	Filter by name All types	All locations	✓ No grouping
🖉 Tags	15 items Show hidden types 0		
		TYPE	LOCATION
SETTINGS	🗌 🙀 c-nic-hal	Network interface	Central US
📣 Quickstart	🗌 🔛 e-nic-ha2	Network interface	Central US
0 Resource costs	esgAvailabilitySet	Availability set	Central US
Deployments	esgLoadBalancer	Load balancer	Central US
Policies	L lbip	Public IP address	Central US
	public-ip-vm1	Public IP address	Central US
:= Properties	public-ip-vm2	Public IP address	Central US
Cocks	tcarrera10228142a9	Storage account	Central US
Automation script	🗌 🛄 tarme hal	Virtual machine	Central US
MONITOPING	🗌 😂 karwa kal, ke, (), (,), lacii blachel kelitii takketiik ().	Disk	Central US
	Example 1 (0.014, 1, article14832)44781a3044832454a3	Disk	Central US
ilii Metrics	🗌 📮 tanna hal	Virtual machine	Central US
🔑 Alert rules	🗌 😂 tarres hal, be (1,2) Machelia (1,6) (17) (10) (2007	Disk	Central US
Diagnostics logs	🗌 😂 harres hal (halsk) (1963)(4094)(1003)(2014)	Disk	Central US
Application insights	🗌 🧻 VPNNSG	Network security group	Central US

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 <u>Forcepoint Email Security in Azure</u> <u>Quick-Start Guide</u>.

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 <u>Microsoft documentation</u> for more information.

- 2. Log on to the <u>Azure Marketplace</u> and click Create a resource.
- 3. In the Search bar, search for Forcepoint, then select **Forcepoint Email Security** V8.5.
- To create a new Forcepoint Email Security solution, click Create.
 Alternatively, use this direct link to <u>Forcepoint Email Security v8.5</u> and click Create.

The **Basics** tab displays.

1	Basics		* Virtual Machine name 🛛		
I.	Configure basic settings	/	fes-vm	~	
			* Password 0		
2	Virtual Machine Sizing				
2	Configure the virtual machine'		* Confirm password		
С	Network Configuration		Number of Virtual Appliances 0		
С	Configure the Network resourc.		Two	\sim	
			Subscription		
Л	Summary		FES	~	
4	Forcepoint Email Security V8.5 .		•		
			* Resource group ①		
5	Buy	、 、			
5		<i>´</i>			
			* Location		
			Central US	\sim	

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 <u>Add virtual machines to a Forcepoint Email Security in Azure deployment</u>.

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.

ome > New > Marketplace > Everything > Forcepoint Create Forcepoint Email Security ×	Email Security V8.5 Beta (Staged) > Create Forcepoint Email Se Settings	ecurity V8.5 Beta (Staged) > Settings > Choose virtual network Choose virtual network
1 Basics ✓ Done	* Virtual Network ESG1	These are the virtual networks in the selected subscription and location 'Central US'.
2 ^{Virtual Machine Sizing} ✓	Review subnet configuration	+ Create new
3 Network Configuration > Configure the Network resourc		↔→ ESG1 esg_deno_unal
4 Summary		MigrationNetwork-172-21 MigrationSetingDroup
Forcepoint Email Security V8.5		Rubothamawark
5 ~ 7		Resourcemonetherrigh
	ОК	

- 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 <u>here</u>.
- 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.

- 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 <u>Registering the DLP Module</u>.

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.

an radium 2- ruk Domain-pased Roure Name: default Route order: 1 Delivery Method	
Pacificial comain Email calaviewy aback on the receptant's domain STRIP server 19 address Email calaviewy based on STRP server list STRIP Server List priver Address port ptc lockup preference priver Address port ptc lockup ptc lockuptc ptc lockup ptc lockup ptc lockup ptc lockup ptc lockup ptc loc	Edit SHTP Server X Server address: WBSh mail.protection.ou IP address or hostname Enable KK lookup Port: 25 The system will bry to deliver to the server address based on the preference. Smaller numbers indicate higher preference. Preference: IO OK Cancel
Delivery Options Use Transport Layer Security (TLS) Require authentication	

- 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 <u>Setting system notification email</u> <u>addresses</u>.
- 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 <u>Forcepoint DLP Email Gateway Help</u> 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 <u>Office 365 Government</u> is supported.

- 1. Log on to Microsoft Office 365, <u>https://outlook.office365.com/ecp</u>
- 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.)

Edit Connector		
This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.		
*Name:		
FromO365toForcepoint]	
Description: Forwards 0365 mail to Forcepoint	\langle	Optionally include a description for this connector.
What do you want to do after connector is saved?		

Next	Cancel
------	--------

- 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.

Edit Connector			
When do you want to use this connector? • Only when I have a transport rule set up that redirects messages to this connector Only when email messages are sent to these domains		Select you cre redirec this co	this option only if tated a rule that ts email messages to nnector.
+/-		Learn r	nore
	Back	Next	Cancel

- g. Click Next.
- h. From How do you want to route email messages, select Route email through these smart hosts.

Back Next Cancel

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

Edit Connector	
How do you want to route email messages?	
Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. Learn more O Use the MX record associated with the partner's domain	Select to send messages to the MX record destination for the targeted recipients.
Li zom	

- j. Click Next.
- k. From How should Office 365 connect to your email server, select Always use TLS to secure the connection.
- 1. Select Any digital certificate, including self-signed certificates.

How should Office 365 connect to your email server?	TLS is a security protocol
 Always use Transport Layer Security (TLS) to secure the connection (recommended) Connect only if the recipient's email server certificate matches this criteria Any digital certificate, including self-signed certificates Issued by a trusted certificate authority (CA) And the subject name or subject alternative name (SAN) matches this domain name: 	that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be acircled if the 71 c
Example: contoso.com or *.contoso.com	connection isn't successful.

m. Click Next.

A summary screen displays.

Confirm your settings			
Before we validate this connector for you, make sure these are the settings you want to configure.			
Mail flow scenario			
From: Office 365			
To: Your organization's email server			
for four organizations entitisered			
Name			
FromO365toForcepoint			
Description			
Forwards email to Forcepoint			
· · · · · · · · · · · · · · · · · · ·			
Status			
Turn it on after saving			
-			
When to use the connector			
Use only when I have a transport rule set up that redirects messages to this connector.			
Routing method			
Route email messages through these smart hosts:			
Country restrictions			
	Deals	N1-14	Canad
	BACK	ivext	Cancel

- 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.

Edit Connector	
Validate this connector	
We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.	
Specify an email address for your partner domain. You can add multiple addresses if your partner has more than one domain.	
+ ✓ - eggut@gmail.com	Specify the email address or addresses you want to use to validate this connector.

Back	Validate	Cancel
------	----------	--------

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.

Edit Connector	
Validation Result	
We couldn't validate this connector. Click 'De	tails' to learn more about what the issues were and how you can fix them. Done! You've completed the operation.
	Close

Back Save Cancel

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.

Edit Connector	
This connector lets Office 365 accept email messages from your organization's email server (also called an on-premises server).	L.
*Name:	
FromForcepointToInternet	
	_
From Forcepoint to internet	Optionally include a description for this connector.
What do you want to do after connector is saved? I Turn it on	
Retain internal Exchange email headers (recommended)	

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

Next Cancel

Edit Connector			
How should Office 365 identify email from your email server?			
 By verifying that the subject name on the certificate that the sending server uses to authentic this domain name (recommended) Example: contoso.com or *.contoso.com By verifying that the IP address of the sending server matches one of these IP addresses that + 	ate with Office 365 r	nization The series	se IP addresses must ong to your organization lusively. You can't ude IP addresses that owned by third-party rices. For example, you 't include an IP address behaven to Offen 255
52.171.209.128		hot veri	t belongs to Unice 305, mail.com, gmail.com, zon.com, and so on.
Office 365 will only accept messages through this connector if the sender domain is configured for your Office 365 organization. Learn more	as an accepted dor	nain	
	Back	Next	Cancel

• 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

<u>Configuring Exchange Online to use certificate validation</u> in the Forcepoint Knowledge Base.

g. Click Next

A summary screen displays.

Confirm your settings			
Before saving, make sure these are the settings you want to configure.			
Mail flow scenario			
From: Your organization's email server			
To: Office 365			
Name			
FromForcepointToInternet			
Description			
From Forcepoint to internet			
Status			
Turn it on after saving			
How to identify email sent from your email server			
Identify incoming messages from your email server by verifying that the sending server's IP address ranges: 52.171.209.128, and the sender's email address is an accepted domain for your organization	s is within these IP ac n.	ldress	
	Back	Save	Cancel

- 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.

Name:]
*Apply this rule if	
Select one	3 .
Select one	
The sender	•
The recipient	 is this person
The subject or body.	is external/internal
Any attachment	is a member of this group
Any recipient	address includes any of these works
The message	 address matches any of these text patterns
The message properties	is on the sender's supervision list
A message header	 has specific properties including any of these words has specific properties matching these text patterns
[Apply to all messages]	domain is
Audit this rule with severity level:	
Not specified	
Choose a mode for this rule:	
Enforce	
O Test with Policy Tips	
O lest without Policy Tips	
Name:	
*Apply this rule if	
The recipient is located	✓ * <u>Select one</u>
add condition	
*Do the following	
Colort one	
Selectione	X
add action	select recipient location
Except if	Outside the organization
add exception	
Properties of this rule:	OK Cancel
Audit this rule with severity level:	
Not specified 🔻	
Choose a mode for this rule:	
Enforce	
○ Test with Policy Tips	
 Test without Policy Tips 	

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

Contra constitute the constitution	
Sent to scope Outside the organization	
Apply this ru e if	
The recipient is located	 Outside the organization
add condition	
Do the following	
Select one	•
Select one	
Forward the message for approval	•
Redirect the message to	these recipients
Block the message	hosted quarantine
Add recipients	the following connector
Apply a disclaimer to the message	•
Modify the message properties	,
Modify the message security	,
Prepend the subject of the message with	
Generate incident report and send it to	
Notify the recipient with a message	

- O Test without Policy Tips
- f. Add the exception Except if the sender IP address is in any of these ranges or exactly matches.

Name:	
Sent to scope Outside the organization]
*Apply this rule if	
The recipient is located	Outside the organization
add condition	
Do the following	
Use the following connector	 Route oubound email to Forcepoint Email Security
add action	
Except if	
Select one	▼
Select one	
The sender	 is this person
The recipient	is external/internal
The subject or body	is a member of this group
Any attachment	 address includes any of these words
Any recipient	 address matches any of these text patterns
The message	is on a recipient's supervision list
The sender and the recipient	has specific properties including any of these words
The message properties	has specific properties matching these text patterns
A message header	has overridden the Policy Tip
O Test without Policy Tips	IP address is in any of these ranges or exactly matches
	domain is

Activate this rule on the following date:

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].

20
31
3
53
31
1
6

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 <u>Adding an IP address group</u> in *Forcepoint Email Security Administrator Help* for more information.

EMAIL	
Message	None. The lack of definitive SPF information prevents an SPF check (e.g., an SPF record does not exist).
management	Bypass SPF Option
	Bypass SPF validation for senders in the following domain group
D-li-v	Domain group: None 🗸
Management	
Settings 🛪	Outbound Relay Options
ð	Select one of the following relay settings for outbound mail from senders in protected domains who do not require SMTP authentication.
General	Allow relays only for senders from trusted IP addresses and selected IP groups.
•-	Coffice 365 IP Group
~ /2	G Suite IP Group
Administrators	○ Allow all outbound relays.
203	Warning: This option may open a security breach in your system.
Users	Internal Relay Options
#	Select one of the following relay settings for mail among protected domain addresses that do not require SMTP authentication.
Inbound/	Allow relays only for senders from trusted IP addresses
Outbound	Allow all internal relays.
	Warning: This option may open a security breach in your system.
Hybrid Service	
Hybrid Service	

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 <u>https://www.spamhaus.org/faq/section/Spamhaus%20PBL</u>.

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."

Database Properties - esglog	gdb76		- 🗆 X
Select a page	🖵 Script 🔻 😯 Help		
Files Filegroups Fortune Fortune Change Tracking Permissions Echanded Properties Mirroring Transaction Log Shipping Query Store	Database name: Owner: Use full-text indexing Database files: esglogdb 76 esglogdb 76_Log ldf	esglagdb76 Path F-\Data F-\Data	File Name esglogdb 76 mdf esglogdb 76 j.og.
Connection Server: 17win2016-pg Connection: 17win2016-pg\azureuser YW Mew connection properties			
Progress Ready	<	Add	Remove

- 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.

Database Partition Creation				
	File path	Initial size (MB)	Growth (MB)	
Data:	F:\Data	2048	512	
Log:	F:\Data	100	100	
				OK Create
Augilable Dastitions				

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**.

Log Database set	tings are correct.
Log Database Location	
Log database:	172.30.13.11 IP address\instance or hostname\instance
Port:	1433 ☑ Encrypt connection ④ SQL Server authentication ○ Windows authentication
Username: Password:	azureuser Enter the password of the log database log Check Status

- 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.

â 	172.30.13.11	- @ ×	Sql Server Configuration Manager		
Action View Holp Action View Holp Sol. Serve Stress Configuration Manage Sol. Serve Stress Configuration Manage Sol. Serve Stress Configuration Manage Sol. Serve Telescol. Configur Sol. Serve Telescol. Configur Access Policies Sol. Serve Telescol. Configur Access Policies Sol. Serve Telescol. Configur Access Policies Sol. Manage Configuration Manage Revealed Ministry Sol. Serve Telescol. Configur Access Policies Sol. Manage Configuration Manage Revealed Ministry Sol. Manage Configuration Access Policies Sol. Manage Configuration Manage Configuration Manage Configuration Manage Configuration Sol. Manage Configuration	Help Help The second se	 - 8 × Local Securi Local Securi Manual Securi Securi Manual Securi Securi Securi Manual Securi Secu	Sql Server Configuration Manager y Policy 	Security Setting Negotiat Sympo- Regional 22-bit recorption Regional 22-bit recorption Ret Defined Net Defined Net Defined Net Defined Net Defined Net Defined	×
Public Key Policies Software Retriction Application Control Policies Advanced Audit Po	Pelicies Henois security Rest Policies Henois security Rest In Local Computer In Configuration Recovery console All Studiown: Clear viture System cryptography System cryptography System cryptography System cryptography System cryptography System cryptography System cryptography	trick NTLIK Audit NTLM authenticable trick NTLM comming NTLM traffic trick NTLM comming NTLM traffic trick NTLM conjoing NTLM traffic to ow automatic administrative legon ow floppy copy and access to all drive em to be shut down without having te al memory pagefile - Scree strong key protection for user k Use IPS complanet algorithms for an in case insensitivity for non-Windows	n in the domain is domain remote servers a and all folders log on wys stored on the computer cryption, hashing, and signing subordems	Not Uefnied Not Defined Not Defined Disabled Disabled Disabled Disabled Not Defined Enabled 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**.

🗑 Forcepoint Management Infras	tructure Setup			-		Х
				SQL	Ser	ver
 Welcome Installation Directory SQL Server Server & Credentials Admin Account Restore Data From Backup Pre-Installation Summary Installation Summary 	Specify the location ai want to use for Forcep If you are using an exi Next. Use existing SQL Serv Use the SQL Serv	nd access credentials for the Micro point reporting data. string SQL Server instance, make s Server on this machine er database installed on another m	osoft SQI cure it is i achine	L Server inst	ance you re you cli	ı ck
	Hostname or IP address:	(CIP address) or chostname) {coptional instance name)}	Port:	1433 <i>(Optional)</i>		
	Authentication:	SQL Server Authentication	I	~]	
	User name:	azureuser				
	Password:	•••••]	
	Encrypt connection	on				
		To and a sure		Paris'		
Cancel Help			Ba	ck 🚺	Vext	

- 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 <u>Forcepoint My Account Downloads</u> 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 <u>Forcepoint</u> <u>Appliances CLI Guide</u> and <u>Forcepoint Security Appliance Manager Help</u> 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.