Installation Guide

Forcepoint™ TRITON® AP-DATA Gateway and Discover

v8.3.x

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin TX 78759

Published 2017

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint LLC makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint LLC shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Contents

1 Installing the Management Server

In this topic:

This section describes how to install Forcepoint™ TRITON® AP-DATA on a management server. For instructions on installing TRITON AP-WEB and/or TRITON AP-EMAIL components alone or with TRITON AP-DATA, see the Deployment and Installation Center in the Forcepoint Technical Library.

To install TRITON AP-DATA, you perform 2 basic steps.

1. *Install the TRITON Infrastructure*, page 11.

   This includes the TRITON Manager, settings database, and reporting database.

2. *Install TRITON AP-DATA management components*, page 18.

   This includes the policy engine, crawler, fingerprint repository, forensics repository, and endpoint server.

The system supports installations over Virtual Machines (VM), but Microsoft SQL Server must be present to support the incident and policy database. See *Installing on a virtual machine*, page 22, for details.

Once you've installed management components, you may choose to install TRITON AP-DATA agents on network servers or endpoint client machines. You can also install extra TRITON AP-DATA servers and crawlers for system scaling. See *Installing TRITON AP-DATA Agents and Servers*, page 25, for more information.

System requirements

The machine that hosts core management components for Forcepoint security solutions is referred to as the **TRITON management server**.

Subscriptions

To install TRITON AP-DATA and the TRITON Manager, you must have a subscription to either TRITON AP DATA Gateway or TRITON AP-DATA Discover. To use the endpoint agent, you need a subscription to TRITON AP-ENDPOINT DLP as well.

Operating system requirements

The TRITON management server must be running on one of the following operating system environments:

- Windows Server 2008 (64-bit) Standard or Enterprise R2 SP1
- Windows Server 2012 (64-bit) Standard Edition
- Windows Server 2012 (64-bit) Standard Edition R2

Hardware requirements

The minimum hardware requirements for a TRITON management server vary depending on whether Microsoft SQL Server 2008 R2 Express (used only for evaluations or very small deployments) is installed on the machine.

Notes:

- TRITON AP-DATA allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90GB from the TRITON AP-DATA disk space requirements.
- If you choose to install TRITON AP-DATA on a drive other than the main Windows drive (typically C drive), it must have at least 4 GB free on the Windows partition to accommodate the TRITON installer.

With a remote (standard or enterprise) reporting database, the management server must meet the following hardware requirements for stand-alone TRITON AP-DATA installations.

Server hardware	Recommended	Minimum
CPU	8 CPU cores (2.5 GHz)	4 CPU cores (2.5 GHz)
Memory	12 GB	12 GB
Disk space	400 GB	140 GB

With local (express) reporting database, it must meet the following hardware:

Server hardware	Recommended	Minimum
CPU	8 CPU cores (2.5 GHz)	4 CPU cores (2.5 GHz)
Memory	12 GB	12 GB
Disk space	400 GB	240 GB

Browser requirements

TRITON Manager is a web-based tool runs on a variety of popular browsers. For a list of browsers and versions that are supported, see the Certified Product Matrix on the Forcepoint website.

Although it is possible to launch TRITON Manager using non-supported browsers, you may not receive full functionality and proper display of the application.

Database requirements

Microsoft SQL Server is used to host the reporting database for TRITON AP-DATA and other Forcepoint solutions.

- For evaluations and small deployments, the TRITON Unified Installer can be used to install Microsoft SQL Server 2008 R2 Express on the TRITON management server machine.

  Use only the version of SQL Server 2008 R2 Express included in the TRITON Unified Installer.
- Larger organizations are advised to use Microsoft SQL Server Standard or Enterprise. These SQL Server editions cannot reside on the TRITON management server.

  SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability.

The supported database engines are:

- **SQL Server 2016 -** Standard, Business Intelligence, and Enterprise editions
- **SQL Server 2014 -** Standard, Business Intelligence, and Enterprise editions
- **SQL Server 2012 SP1** (or the latest service pack from Microsoft) - Standard, Business Intelligence, and Enterprise editions
- **SQL Server 2008 R2 SP2** (or the latest service pack from Microsoft) - All editions except Web and Compact; all service packs; not IA64
- **SQL Server 2008 R2 Express SP2** (installed by the TRITON Unified Installer)
- **SQL Server 2008 SP3** (or the latest service pack from Microsoft) - All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64

Port requirements

The following ports must be kept open on the TRITON management server:

Outbound		
TRITON AP-DATA Server, Protector, Web Content Gateway, TRITON AP-EMAIL	17500-17515** and 17700-17715***	Consecutive ports that allow communication with Forcepoint agents and machines.
Inbound		
From	**Port**	**Purpose**
TRITON AP-ENDPOINT DLP	80	Configuration
TRITON AP-DATA Server, Protector, Web Content Gateway	17443*	Incidents
TRITON Manager	17447	Processing batch jobs such as scheduled tasks
TRITON Manager	17446	Translating messages into sender/receiver protocols
TRITON Manager	1443	Remote SQL Server or local SQL Server with Analytics Engine installed
TRITON AP-DATA Server, Protector, Web Content Gateway	139	File sharing
TRITON AP-DATA Server, Protector, Web Content Gateway	443	Secure communication
TRITON AP-DATA Server, Protector, Web Content Gateway	445	File sharing
TRITON AP-DATA Server, Protector, Web Content Gateway	8453	User repository
TRITON AP-DATA Server, Protector, Web Content Gateway	8005	Tomcat server
TRITON AP-DATA Server, Protector, Web Content Gateway, TRITON AP-EMAIL	17500-17515** and 17700-17715***	Consecutive ports that allow communication with Forcepoint agents and machines.
TRITON AP-DATA Server, Protector, Web Content Gateway	9443*	Access user interface

* This port should be left open. It is not configurable.

** This range is necessary for load balancing.

***Used when Web Content Gateway and TRITON AP-EMAIL are both installed.

Preparing for installation

Before installing TRITON AP-DATA, make sure that you have completed all of the preparations noted below.

Windows considerations

- Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- In addition to the space required by the Forcepoint installer itself, further disk space is required on the Windows installation drive (typically C) to accommodate temporary files extracted as part of the installation process.

  For information on minimum disk space requirements, see *Hardware requirements*, page 2.
- TRITON AP-DATA requires the .NET Framework v3.5 and v4.5 for the installation of Office 365 components and more. If this version is not detected, you are notified.

Domain considerations

The servers running the TRITON AP-DATA software can be set as part of a domain or as a separate workgroup. If you have multiple servers or want to perform run commands on file servers in response to discovery, it is best practice to make the server or servers part of a domain.

Do not install TRITON AP-DATA on a domain controller machine, however.

Strict GPOs may interfere and affect system performance, and even cause the system to halt. Hence, when putting TRITON AP-DATA servers into a domain, it is advised to make them part of organizational units that don’t enforce strict GPOs.

Also, certain real-time antivirus scanning can downgrade system efficiency, but that can be relieved by excluding some directories from that scanning (see *Antivirus*, page 6). Please contact Forcepoint Technical Support for more information on enhancing performance.

Domain Admin privileges

Forcepoint components are typically distributed across multiple machines. Additionally, some components access network directory services or database servers. To perform the installation, it is a best practice to log on to the machine as a user with domain admin privileges. Otherwise, components may not be able to properly access remote components or services.

Important

If you plan to install SQL Server 2008 R2 Express and will use it to store and maintain TRITON AP-WEB data, log on as a domain user to run the TRITON Unified Installer.

Synchronizing clocks

If you are distributing Forcepoint components across different machines in your network, synchronize the clocks on all machines where a Forcepoint component is installed. It is a good practice to point the machines to the same Network Time Protocol server.

Note

If you are installing components that will work with a Forcepoint V-Series appliance, you must synchronize the machine's system time to the appliance's system time.

Antivirus

Disable any antivirus on the machine prior to installing Forcepoint components. Be sure to re-enable antivirus after installation. Exclude the following Forcepoint files from antivirus scans to avoid performance issues:

- The TRITON installation folder, which is one of the following:
  - *:\Program Files\Websense
  - *:\Program Files (x86)\Websense
- *:\Program files\Microsoft SQL Server*.*
- C:\Documents and Settings\<user>\Local Settings\Temp\*.*
- %WINDIR%\Temp\*.*
- The forensics repository (configurable; defaults to Websense folder)

No underscores in FQDN

Do not install Forcepoint components on a machine whose fully-qualified domain name (FQDN) contains an underscore. The use of an underscore character in an FQDN is inconsistent with Internet Engineering Task Force (IETF) standards.

Note

Further details of this limitation can be found in the IETF specifications RFC-952 and RFC-1123.

Third-party components

The following third-party components are required to install Microsoft SQL Server 2008 R2 Express. Although the TRITON installer installs these components automatically if they are not found, it is a best practice to install the components before running TRITON Setup if you plan to use SQL Server Express.

- .NET Framework 3.5 SP1

  Because the installer requires .NET 4.5 as well, both .NET 4.5 and 3.5 SP1 are required if you are installing SQL Server Express.
- Windows Installer 4.5
- Windows PowerShell 1.0
- PowerShell is available from Microsoft (www.microsoft.com).

SQL Server

If you are going to use SQL Server Standard or Enterprise in your Forcepoint deployment, do the following before running TRITON Setup:

1. Install SQL Server according to Microsoft instructions. See *Database requirements*, page 3 for a list of supported versions.

   Tip

   If you plan to install the database in a custom folder, see these instructions. Starting with Microsoft SQL Server 2012, the database engine service must have access permissions for the folder where database files are stored.

2. Make sure SQL Server is running.
3. Make sure SQL Server Agent is running.

   Note

   If you are using SQL Server 2008 Express R2, SQL Service Broker is used instead of SQL Server Agent.

4. Obtain the SQL Server logon ID and password for a SQL Server Administrator, or for an account that has db_creator server role, SQLAgent role, and db_datareader in **msdb**. The account must have a sysadmin role. You need this logon ID and password when you install TRITON AP-DATA.
5. Restart the SQL Server machine after installation.
6. Make sure the TRITON management server can recognize and communicate with SQL Server.
7. Install the SQL Server client tools on the TRITON management server. Run the SQL Server installation program, and select **Connectivity Only** when asked what components to install.

8. Restart the machine after installing the connectivity option. See Microsoft SQL Server documentation for details.

SQL Server user roles

Microsoft SQL Server defines SQL Server Agent roles that govern accessibility of the job framework. The SQL Server Agent jobs are stored in the SQL Server **msdb** database.

The SQL user account must also have **dbcreator** fixed server role privilege.

Use Microsoft SQL Server Management Studio to grant the database user account the necessary permissions to successfully install the TRITON reporting database.

1. On the SQL Server machine, go to **Start > Programs > Microsoft SQL Server 2008 or 2012 > Microsoft SQL Server Management Studio**.
2. Log into SQL Server as a user with SQL sysadmin rights.
3. Select the **Object Explorer** tree, and then go to select **Security > Logins**.
4. Select the login account to be used during the installation.
5. Right-click the login account and select **Properties** for this user.
6. Select **Server Roles**, and then select **dbcreator**. Also select **sysadmin**.
7. Select **User Mapping** and do the following:
   a. Select **msdb** in database mapping.
   b. Grant membership to one of these roles:
      ○ SQLAgentUserRole
      ○ SQLAgentReader Role
      ○ SQLAgentOperator Role
      ○ db_datareader
   c. Select **wbsn-data-security** in database mapping and mark it as “db_owner”.
   d. Select **wbsn-data-security-temp-archive** in database mapping and mark it as “db_owner”.
   e. Click **OK** to save your changes.
8. Click **OK** to save your changes.

Getting the TRITON installer

The TRITON installer is used to install or upgrade the TRITON management server, TRITON AP-DATA software, reporting components, and SQL Server 2008 R2 Express on supported Windows servers.

Download the installers from My Account.

- The TRITON installer executable is named **TRITON83xSetup.exe**. Double-click it to start the installation process.

If you have previously run this installer on a machine, and you selected the **Keep installation files** option, you can restart the installer without extracting all of the files a second time.

- Windows Server 2012: Go to the **Start** screen and click the **Websense TRITON Setup** icon.
- Windows Server 2008 R2 SP1: Go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.

Note that the files occupy approximately 3 GB of disk space.

Installation steps

Do the following to install TRITON AP-DATA on the management server.

1. *Launch the installer*, page 9
2. *Install the TRITON Infrastructure*, page 11
3. *Install TRITON AP-DATA management components*, page 18

Launch the installer

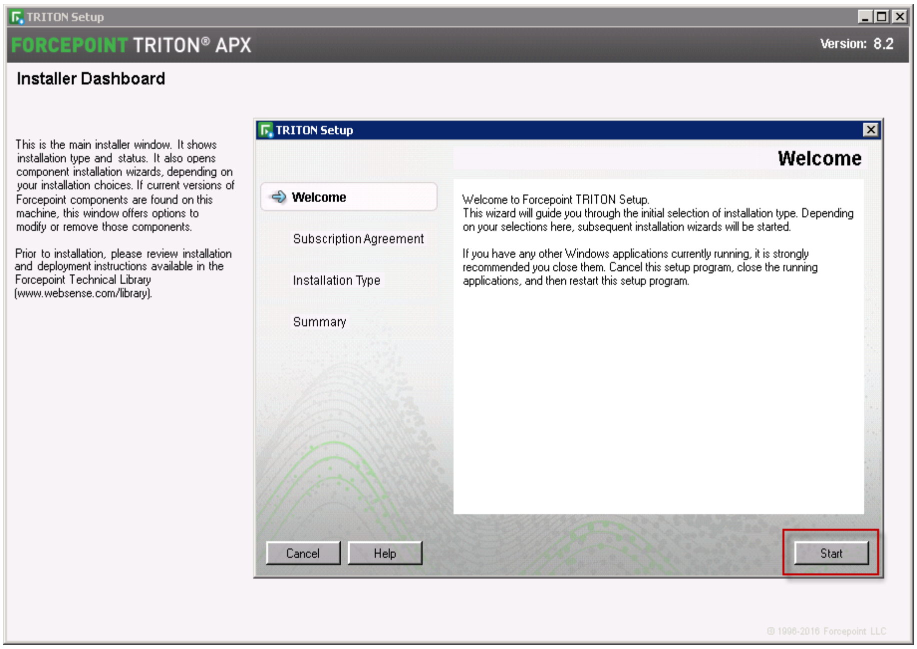
1. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

> **Important**
>
> Do not change this account after installation. Be sure it's a dedicated account that you want installed services to use when interacting with the operating system—the service account. If you must change the account, contact Forcepoint Technical Support first.

2. Double-click the installer file, **TRITON83xSetup.exe**, to launch the TRITON Setup program.

   A progress dialog box appears, as files are extracted.

3. On the **Welcome** screen, click **Start**.



This is the main installer window. It shows installation type and status. It also opens component installation wizards, depending on your installation choices. If current versions of Forcepoint components are found on this machine, this window offers options to modify or remove those components.

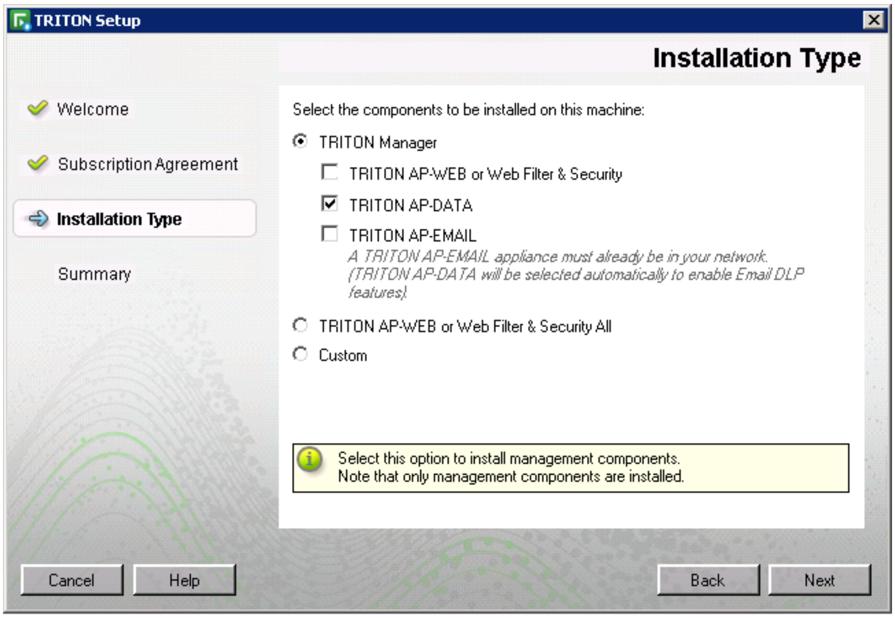
Prior to installation, please review installation and deployment instructions available in the Forcepoint Technical Library (www.websense.com/library).

Welcome to Forcepoint TRITON Setup.
This wizard will guide you through the initial selection of installation type. Depending on your selections here, subsequent installation wizards will be started.

If you have any other Windows applications currently running, it is strongly recommended you close them. Cancel this setup program, close the running applications, and then restart this setup program.

4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.

5. On the **Installation Type** screen, select **TRITON Manager** and then select **TRITON AP-DATA**. The TRITON Manager is also required for TRITON AP-ENDPOINT DLP.



Select the components to be installed on this machine:

● TRITON Manager

☐ TRITON AP-WEB or Web Filter & Security

☑ TRITON AP-DATA

☐ TRITON AP-EMAIL

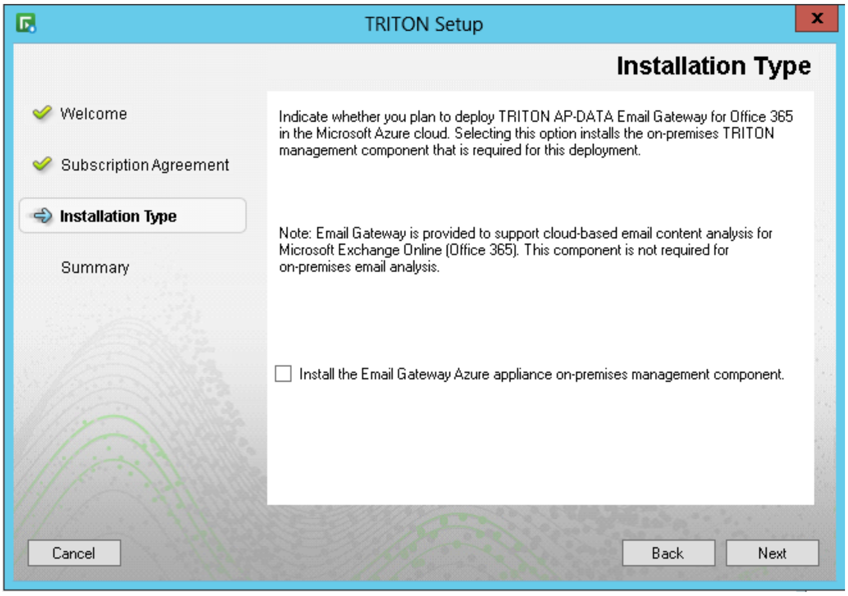
A TRITON AP-EMAIL appliance must already be in your network. (TRITON AP-DATA will be selected automatically to enable Email DLP features)

○ TRITON AP-WEB or Web Filter & Security All

○ Custom

Select this option to install management components.
Note that only management components are installed.

6. You are asked if you want to use the Email Gateway virtual appliance to provide DLP for cloud-based email applications such as Microsoft Exchange Online. If so, select **Install Email Gateway virtual appliance on-premises management component**. At the end of the installation process, an Email Gateway installer will launch. Refer to Chapter 2 for instructions on setting up the appliance.



Indicate whether you plan to deploy TRITON AP-DATA Email Gateway for Office 365 in the Microsoft Azure cloud. Selecting this option installs the on-premises TRITON management component that is required for this deployment.

Note: Email Gateway is provided to support cloud-based email content analysis for Microsoft Exchange Online (Office 365). This component is not required for on-premises email analysis.

□ Install the Email Gateway Azure appliance on-premises management component.

7. In the **Summary** screen, click **Next** to continue the installation. TRITON Infrastructure Setup launches.

Install the TRITON Infrastructure

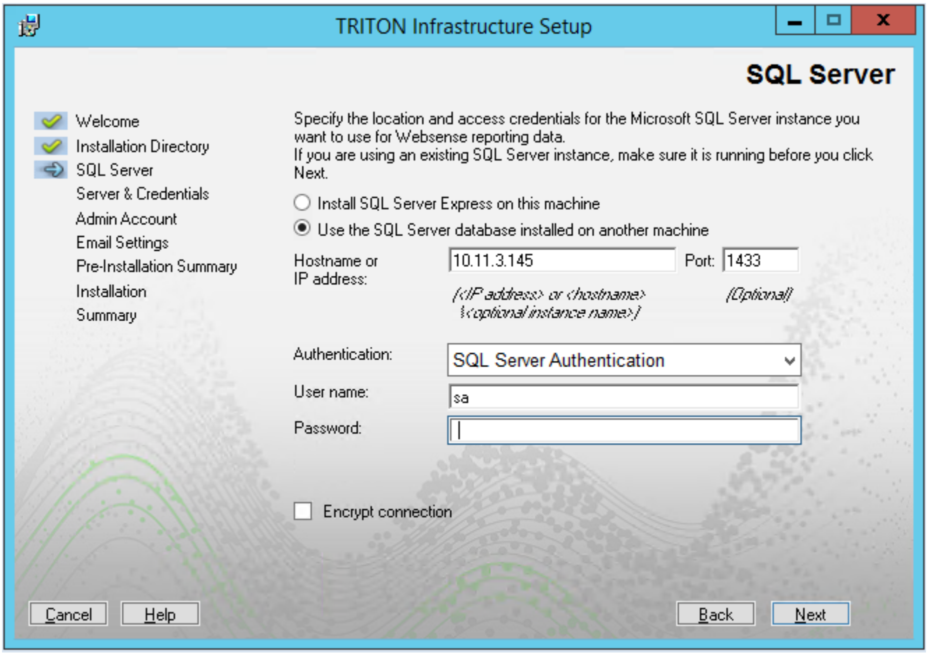
1. On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
2. On the **Installation Directory** screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.

Important

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

- To accept the default location (recommended), simply click **Next**.
- To specify a different location, click **Browse**.

3. On the **SQL Server** screen, specify the location of your database engine and the type of authentication to use for the connection. Also specify whether to encrypt communication with the database.



Specify the location and access credentials for the Microsoft SQL Server instance you want to use for Websense reporting data.
If you are using an existing SQL Server instance, make sure it is running before you click Next.

○ Install SQL Server Express on this machine

● Use the SQL Server database installed on another machine

Hostname or IP address: 10.11.3.145 Port: 1433

(<IP address> or <hostname> \<optional instance name>) (Optional)

Authentication: SQL Server Authentication

User name: sa

Password:

□ Encrypt connection

- Select **Use existing SQL Server on this machine** if the TRITON installer has already been used to install SQL Server 2008 R2 Express on this machine.
- Select **Install SQL Server Express on this machine** to install SQL Server 2008 R2 Express on this machine.

  When this option is selected, Powershell 1.0 and Windows Installer 4.5 are installed automatically if they are not found on the machine. These are required for SQL Server 2008 R2 Express.

  A default database instance named **mssqlserver** is created, by default. If a database instance with the default name already exists on this machine, an instance named TRITONSQL2K8R2X is created instead.

  If .NET 3.5 SP1 and .NET 4.5 are not found on the machine, you are asked to install them before proceeding.

  In some cases, you are prompted to reboot the machine after installing SQL Server Express. If you do, to restart the installer:

  ○ Windows Server 2012: Go to the **Start** screen and click the **Websense TRITON Setup** icon.

  ○ Windows Server 2008 R2 SP1: Go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.
- Select **Use the SQL Server database installed on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

  Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any.

- If you are using a named instance, the instance must already exist.
- If you are using SQL Server clustering, enter the virtual IP address of the cluster.

Also provide the **Port** used to connect to the database (1433, by default).

See *System requirements*, page 1, to verify your version of SQL Server is supported.

After selecting one of the above options, specify an authentication method and account information:

- Select the **Authentication** method to use for database connections: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).

  Next, provide the **User Name** or **Account** and its **Password**. This account must be configured to have system administrator rights in SQL Server. For TRITON AP-DATA, use an account with the **sysadmin** role. If you are using SQL Server Express, **sa** (the default system administrator account) is automatically specified (this is the default system administrator account).

✓ **Note**

The system administrator account password cannot contain single or double quotes.

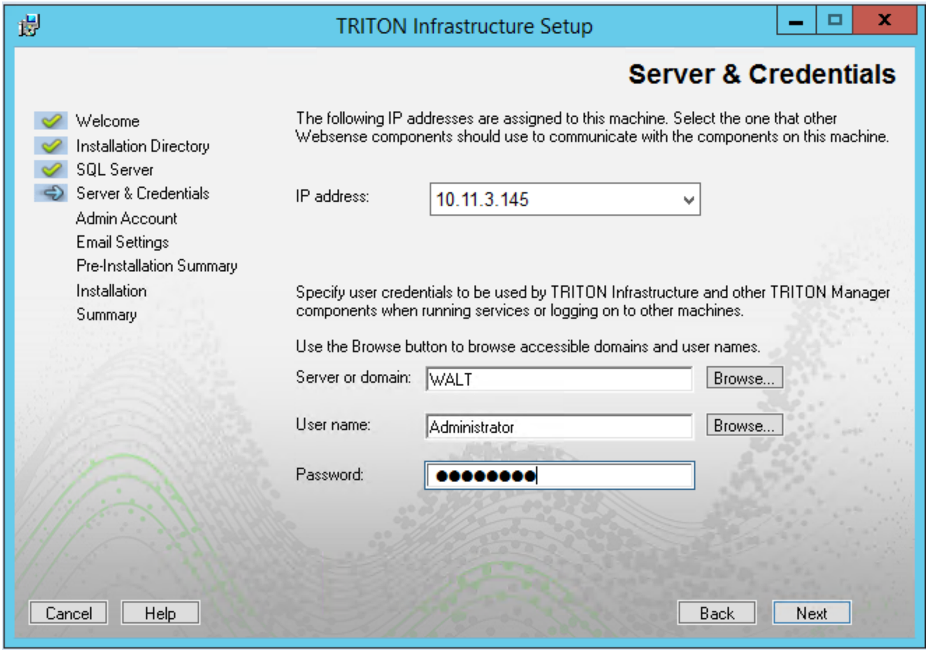
When you click **Next**, connection to the database engine is verified. If the connection test is successful, the next installer screen appears.

If the test is unsuccessful, the following message appears:

> *Unable to connect to SQL*
> *Make sure the SQL Server you specified is currently running. If it is running, verify the access credentials you supplied.*

Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

4. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by the TRITON Manager.



TRITON Infrastructure Setup

Server & Credentials

The following IP addresses are assigned to this machine. Select the one that other Websense components should use to communicate with the components on this machine.

IP address: 10.11.3.145

Specify user credentials to be used by TRITON Infrastructure and other TRITON Manager components when running services or logging on to other machines.

Use the Browse button to browse accessible domains and user names.

Server or domain: WALT

User name: Administrator

Password: ●●●●●●●●

- Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.

  Use the IP address selected to access the TRITON Manager (via Web browser). Also specify this IP address to any Forcepoint component that needs to connect to the TRITON management server.

  If you chose to install SQL Server 2008 R2 Express, if you install TRITON AP-WEB or TRITON AP-EMAIL Log Server on another machine, specify this IP address for the database engine location.
- Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and the TRITON Manager. The server/host name cannot exceed 15 characters.
- Specify the **User name** of the account to be used by the TRTION Manager.
- Enter the **Password** for the specified account.

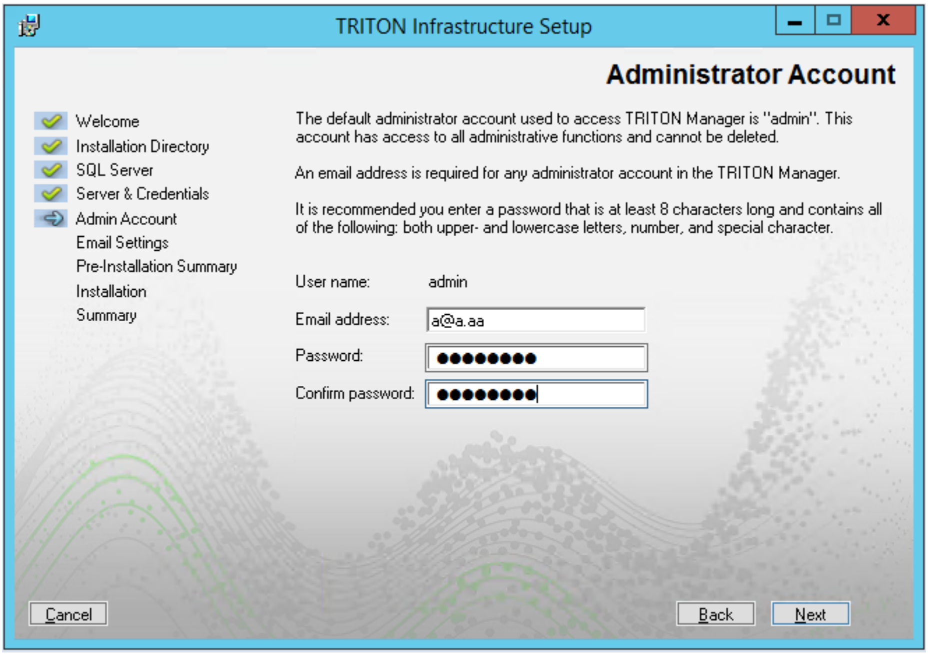
5. On the **Administrator Account** screen, enter an email address and password for the default TRITON Manager administration account: **admin**. These are the credentials you will use to log onto the TRITON Manager, regardless of the products you own. The password must:

   - Be at least 8 characters
   - Contain upper case characters
   - Contain lower case characters
   - Contain numbers
   - Contain non-alphanumeric characters

   When you are finished, click **Next**.

System notification and password reset information is sent to the email address specified (once SMTP configuration is done; see next step).

It is a best practice to use a strong password as described on screen.



TRITON Infrastructure Setup

Administrator Account

The default administrator account used to access TRITON Manager is "admin". This account has access to all administrative functions and cannot be deleted.

An email address is required for any administrator account in the TRITON Manager.

It is recommended you enter a password that is at least 8 characters long and contains all of the following: both upper- and lowercase letters, number, and special character.

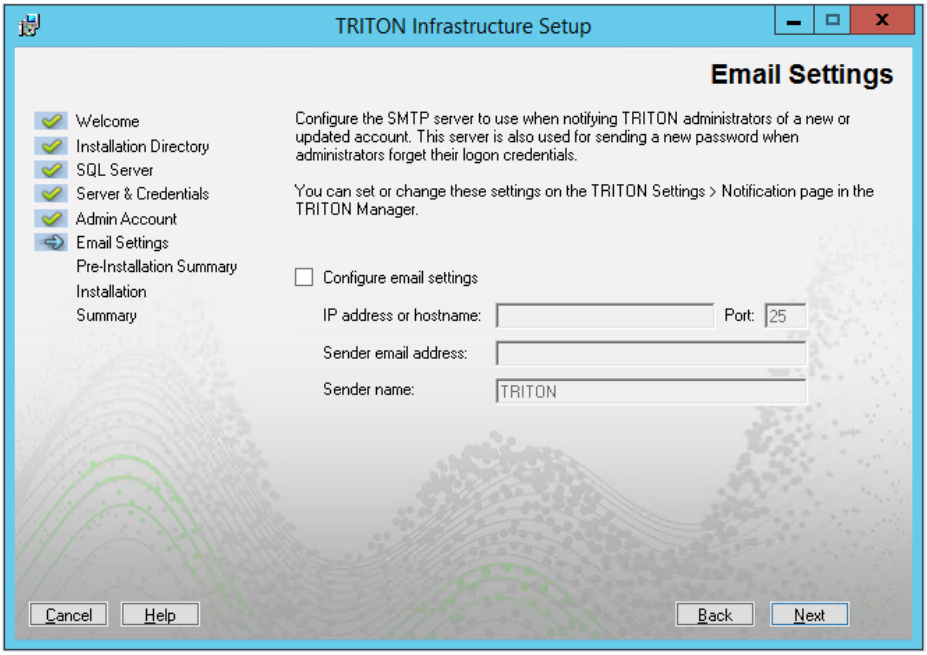
User name: admin

Email address: a@a.aa

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

6. On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications and then click **Next**. You can also configure these settings after installation in the TRITON Manager.



Configure the SMTP server to use when notifying TRITON administrators of a new or updated account. This server is also used for sending a new password when administrators forget their logon credentials.

You can set or change these settings on the TRITON Settings > Notification page in the TRITON Manager.

□ Configure email settings

IP address or hostname: Port: 25

Sender email address:

Sender name: TRITON

Important

If you do not configure an SMTP server now and you lose the **admin** account password (set on previous screen) before the setup is done in the TRITON Manager, the “Forgot my password” link on the logon page does not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent.

- **IP address or hostname**: IP address or host name of the SMTP server through which email alerts should be sent. In most cases, the default **Port** (25) should be used. If the specified SMTP server is configured to use a different port, enter it here.
- **Sender email address**: Originator email address appearing in notification email.
- **Sender name**: Optional descriptive name that can appear in notification email. This is can help recipients identify this as a notification email from the TRITON Manager.

7. On the **Pre-Installation Summary** screen, verify the information and then click **Next** to begin the installation.

> **Warning**
>
> If you chose to install SQL Server Express, depending on whether certain Windows prerequisites are installed, your machine may be automatically restarted up to two times during the installation process. Restarts are not required if the prerequisites are already installed.

> **Note**
>
> When you click **Next**, if you chose to install SQL Server Express on this machine, it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

8. If you chose to install SQL Server Express, PowerShell 1.0 and Windows Installer 4.5 will be installed if not already present. Wait for Windows to configure components.

   a. If the following message appears during this process, click **OK**:

      Setup could not restart the machine. Possible causes are insufficient privileges, or an application rejected the restart. Please restart the machine manually and setup will restart.

   b. TRITON installer starts again. In the TRITON Infrastructure Setup **Welcome** screen, click **Next**.

   c. The **Ready to Resume EIP Infra installation** screen appears. Click **Next**.

> **Note**
>
> When you click **Next**, if you chose to install SQL Server it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

9. If you chose to install SQL Server Express on this machine, SQL Server 2008 R2 Setup is launched. Wait for it to complete.

   The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.

   Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.

10. Next, the **Installation** screen appears. Wait until all files have been installed.

    If the following message appears, check whether port 9443 is already in use on this machine:

Error 1920. Server 'Forcepoint TRITON Central Access' (EIPManagerProxy) failed to start. Verify that you have sufficient privileges to start system services.

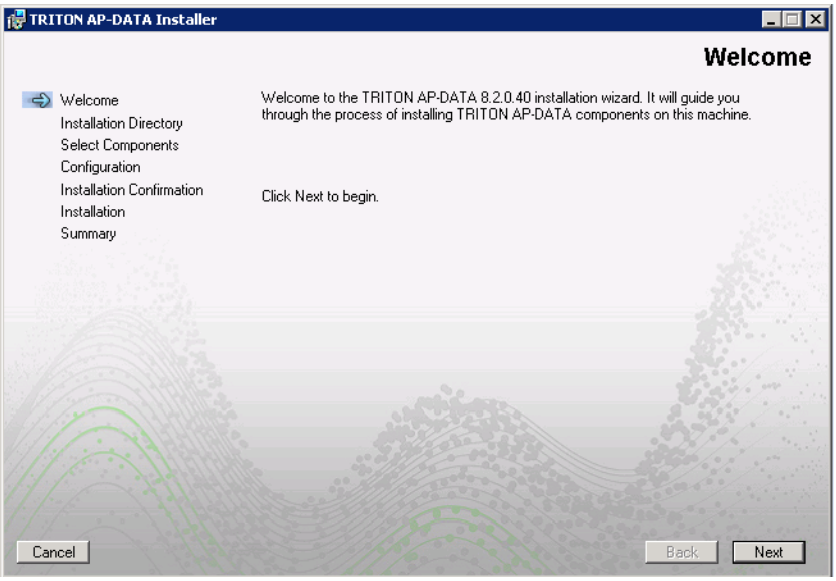
If port 9443 is in use, release it and then click **Retry** to continue installation.

11. On the **Installation Complete** screen, click **Finish**.

You are returned to the Installer Dashboard and, after a few seconds, the TRITON AP-WEB component installer launches.

Install TRITON AP-DATA management components

1. When the TRITON AP-DATA installer is launched, a **Welcome** screen appears. Click **Next** to begin TRITON AP-DATA installation.



TRITON AP-DATA Installer

Welcome

Welcome to the TRITON AP-DATA 8.2.0.40 installation wizard. It will guide you through the process of installing TRITON AP-DATA components on this machine.

Click Next to begin.

Note

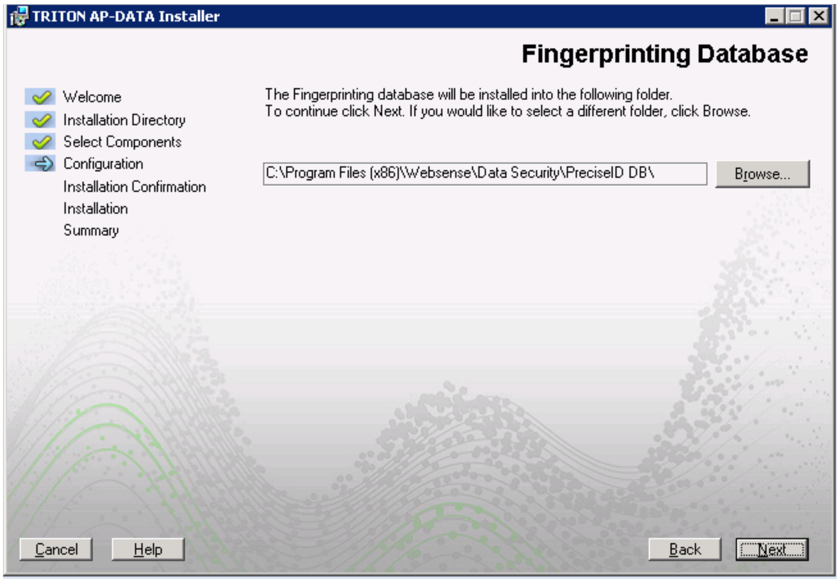
If any prerequisites are not found on this machine, the TRITON AP-DATA installer installs it.

2. If prompted, click **OK** to indicate if services such as SMTP will be enabled.

   Required Windows components will be installed. You may need access to the operating system installation disc or image.

3. On the **Fingerprinting Database** screen, accept the default location or use the **Browse** button to specify a different location.

Note that you can install the Fingerprinting database to a local path only.



The Fingerprinting database will be installed into the following folder.
To continue click Next. If you would like to select a different folder, click Browse.

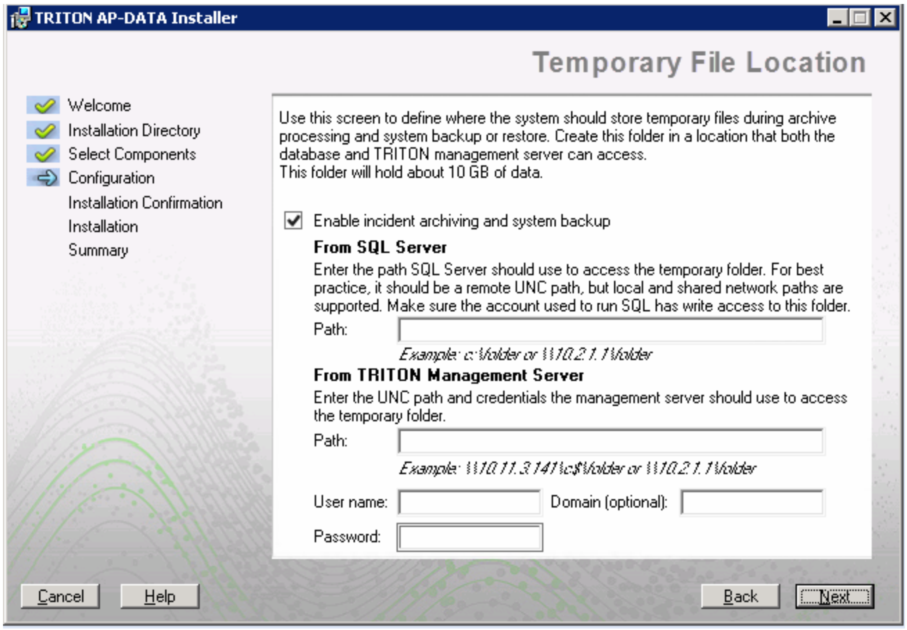
C:\Program Files (x86)\Websense\Data Security\PreciseID DB\

4. If your SQL Server database is on a remote machine, you are prompted for the name of a temporary folder. This screen defines where the system should store temporary files during archive processing as well as system backup and restore.

   Archiving lets you manage the size of your incident database and optimize performance. Backup lets you safeguard your policies, forensics, configuration, data, fingerprints, encryption keys, and more.

   Before proceeding, create a folder in a location that both the database and TRITON management server can access. (The folder must exist before you click

Next.) On average, this folder will hold 10 GB of data, so choose a location that can accommodate this.



Use this screen to define where the system should store temporary files during archive processing and system backup or restore. Create this folder in a location that both the database and TRITON management server can access.
This folder will hold about 10 GB of data.

☑ Enable incident archiving and system backup

From SQL Server

Enter the path SQL Server should use to access the temporary folder. For best practice, it should be a remote UNC path, but local and shared network paths are supported. Make sure the account used to run SQL has write access to this folder.

Path:

Example: c:\folder or \\10.2.1.1\folder

From TRITON Management Server

Enter the UNC path and credentials the management server should use to access the temporary folder.

Path:

Example: \\10.11.3.141\c$\folder or \\10.2.1.1\folder

User name: Domain (optional):

Password:

On the **Temporary Folder Location** screen, complete the fields as follows:

- **Enable incident archiving and system backup**: Check this box if you plan to archive old or aging incidents and perform system backup or restore. This box does not appear when you run the installer in Modify mode and perform a disaster recovery restore operation.
- **From SQL Server**: Enter the path that the SQL Server should use to access the temporary folder. For best practice, it should be a remote UNC path, but local and shared network paths are supported. For example: c:\folder or \\10.2.1.1.\folder. Make sure the account used to run SQL has write access to this folder.
- **From TRITON management server**: Enter the UNC path the management server should use to access the temporary folder. For example: \\10.2.1.1.\folder. Enter a user name and password for a user who is authorized to access this location.

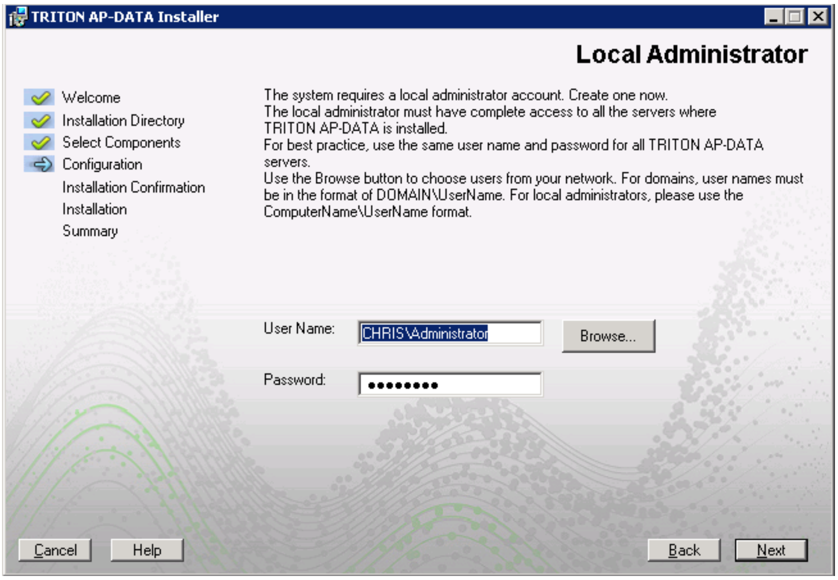
To grant this permission, issue the following T-SQL commands on the SQL Server instance:

```
USE master
GRANT BACKUP DATABASE TO <user>
GO
```

After installation of TRITON AP-DATA components, you can revoke this permission:

```
USE master
REVOKE BACKUP DATABASE TO <user>
GO
```

5. In the **Local Administrator** screen, create an account for the local administrator user on this server. Supply the user name and password to use to access this server during installation and operation. Use this same administrator wherever TRITON AP-DATA components are installed. The server/host name portion of the user name cannot exceed 15 characters. The password must:
   - Be at least 8 characters
   - Contain upper case characters
   - Contain lower case characters
   - Contain numbers
   - Contain non-alphanumeric characters

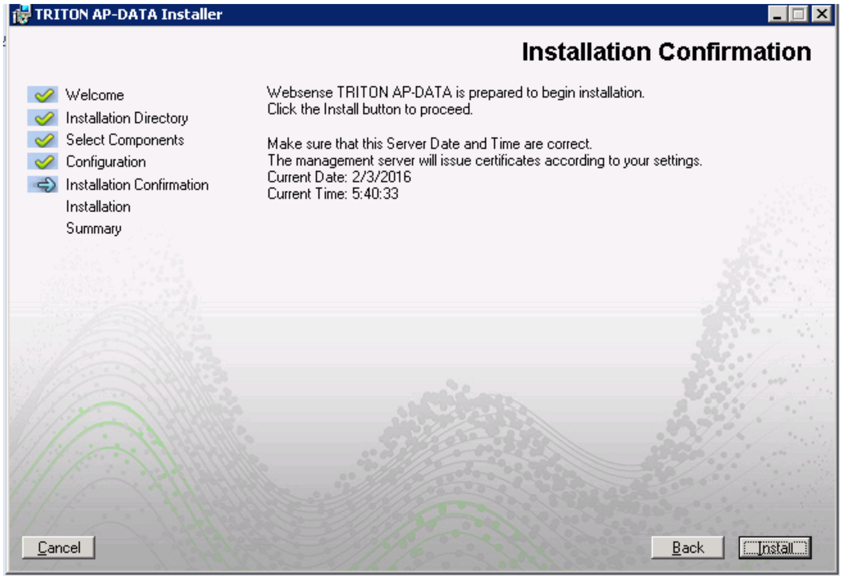


The system requires a local administrator account. Create one now.
The local administrator must have complete access to all the servers where TRITON AP-DATA is installed.
For best practice, use the same user name and password for all TRITON AP-DATA servers.
Use the Browse button to choose users from your network. For domains, user names must be in the format of DOMAIN\UserName. For local administrators, please use the ComputerName\UserName format.

User Name: CHRIS\Administrator

Password: •••••••••

6. In the **Installation Confirmation** screen, click **Install** to begin installation of TRITON AP-DATA components.



Websense TRITON AP-DATA is prepared to begin installation.
Click the Install button to proceed.

Make sure that this Server Date and Time are correct.
The management server will issue certificates according to your settings.
Current Date: 2/3/2016
Current Time: 5:40:33

7. If the following message appears, click **Yes** to continue the installation:

   TRITON AP-DATA needs port 80 free.
   In order to proceed with this installation, DSS will free up this port.
   Click Yes to proceed OR click No to preserve your settings.

   Clicking **No** cancels the installation.

   A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.

8. The **Installation** progress screen appears. Wait for the installation to complete.

9. When the **Installation Complete** screen appears, click **Finish** to close the TRITON AP-DATA installer.

10. If no other TRITON Manager module is chosen for installation, you are returned to the Modify Installation dashboard. Installation is complete.

    Otherwise, you are returned to the Installer Dashboard and the next component installer is launched.

For information on installing other TRITON AP-DATA components, such as the protector, mobile agent, or endpoint client, see *Installing TRITON AP-DATA Agents and Servers*, page 25.

Installing on a virtual machine

TRITON AP-DATA supports installations on Virtual Machines (VM), but Microsoft SQL Server must be present to support the incident and policy database. See *System requirements*, page 1, for supported versions of SQL Server. If you are performing a clean install of TRITON AP-DATA, SQL Server 2008 R2 Express is included.

If you have a subscription to TRITON AP-WEB, be sure to select both the TRITON AP-WEB and TRITON AP-DATA management modules when creating the TRITON management server VM.

If you have a subscription to TRITON AP-EMAIL, select both the TRITON AP-EMAIL and TRITON AP-DATA management modules when creating the TRITON management server VM.

The following platforms are supported:

- Windows Server 2008 R2 SP1 over Hyper-V 2008 R2
- Windows Server 2008 R2 SP1 and Windows Server 2012 over Hyper-V 2012
- Windows Server 2008 R2 SP1, Windows Server 2012 and Windows Server 2012 R2 over Hyper-V 2012 R2
- Windows Server 2008 R2 SP1 over VMware ESXi v5.x
- Windows Server 2008 R2 SP1, Windows Server 2012 and Windows Server 2012 R2 over VMware ESXi 6.x

✓ **Note**

While downloading ESXi, a license key is generated and displayed on the download page. Make a note of this license key for use during installation.

Before installing Forcepoint modules on a VM via ESXi, ensure that your VMware tools are up to date. All of your hardware must be compatible with VMware ESXi. In addition, ensure that the following hardware specifications are met:

VMware Server	Requirements
CPU	● At least 4 cores 2.5 GHz (for example, 1 QuadXeon 2.5 GHz). 8 cores are required if you are installing the TRITON AP-WEB, TRITON AP-DATA, and TRITON AP-EMAIL managers
Disk	● 300 GB, 15 K RPM, RAID 10
Memory	● 8 GB (12 GB if you are installing the TRITON AP-WEB, TRITON AP-DATA, and TRITON AP-EMAIL managers)
NICs	● 2*1000

VMware Infrastructure Client	Requirements
CPU	● At least 500 MHz
Disk storage	● 150 MB free disk space required for basic installation. ● An additional 55 MB free on the destination drive during installation ● 100 MB free on the drive containing the %temp% folder
Memory	● 512 MB
Networking	● Gigabit Ethernet recommended

Module	Requirements for VM installation
TRITON Management Server	● Windows Server 2008 R2 SP1 64-bit or Windows Server 2012 ● 8GB RAM ● 150 GB Disk ● 2 CPU cores

2 Installing TRITON AP-DATA Agents and Servers

Once you've installed TRITON AP-DATA on the TRITON management server (as described in *Installing the Management Server*, page 1), you can install other TRITON AP-DATA components as needed. In larger deployments, you might install supplemental TRITON AP-DATA servers, crawlers, or policy engines. In some scenarios, you might install the TRITON AP-DATA protector and/or any number of TRITON AP-DATA agents such as the mobile agent for monitoring email being synchronized to mobile phones and tablets.

TRITON AP-DATA agents are installed on the relevant servers to enable the system to access the data necessary to analyze the traffic from these servers. TRITON AP-ENDPOINT DLP enables administrators to analyze content within a user's working environment (PC, laptop, etc.) and block or monitor policy breaches.

> **Important**
>
> Before you install a TRITON AP-DATA component—for example, a supplemental server or agent—make sure that the TRITON infrastructure is already installed in your network along with the TRITON AP-DATA management components.
>
> Do not install any TRITON AP-DATA component on a domain controller.

- *Installing supplemental TRITON AP-DATA servers*, page 26
- *Installing TRITON AP-DATA agents*, page 31

Installing supplemental TRITON AP-DATA servers

In this topic:

Medium to large enterprises may require more than one TRITON AP-DATA server to perform content analysis efficiently. Having multiple TRITON AP-DATA servers allows your organization to grow, improves performance, and allows for custom load balancing.

Supplemental TRITON AP-DATA server installations include:

- A policy engine
- Secondary fingerprint repository (the primary is on the management server)
- Endpoint server
- Optical Character Recognition (OCR) server
- Crawler

✓ **Notes:**

In production environments, do not install a TRITON AP-DATA server on a Microsoft Exchange, TMG, or print server. These systems require abundant resources.

Operating system requirements

Supplemental TRITON AP-DATA servers must be running on one of the following operating system environments:

- Windows Server 2008 (64-bit) Standard or Enterprise, R2 SP1
- Windows Server 2012 (64-bit) Standard Edition

Virtualization systems

Like TRITON management servers, secondary TRITON AP-DATA servers are supported on Hyper-V over Windows Server 2008 R2 SP1 or Windows Server 2012.

Hardware requirements

Supplemental TRITON AP-DATA servers must meet the following hardware requirements.

Server hardware	Minimum requirements	Recommended
CPU	2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent	2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent
Memory	4 GB	8 GB
Hard drives	Four 72 GB	Four 146 GB
Disk space	72 GB	292 GB
Free space	70 GB	70 GB
Hardware RAID	1	1 + 0
NICs	1	2

Software requirements

The following requirements apply to all TRITON AP-DATA servers:

- For optimized performance, verify that the operating system's file cluster is set to 4096B. For more information, see the Forcepoint knowledge article: "File System Performance Optimization."
- Windows installation requirements:
  - Set the partition to 1 NTFS Partition. For more information, see the Forcepoint knowledge-base article: "File System Performance Optimization."
  - Regional Settings: should be set according to the primary location. If necessary, add supplemental language support and adjust the default language for non-Unicode programs.
  - Configure the network connection to have a static IP address.
  - The TRITON management server host name must not include an underscore sign. Internet Explorer does not support such URLs.
  - Short Directory Names and Short File Names must be enabled. (See http://support.microsoft.com/kb/121007.)
  - Create a local administrator to be used as a service account. If your deployment includes more than one TRITON AP-DATA server, use a domain account (preferred), or the use same local user name and password on each machine. Do not change the service account.
  - Be sure to set the system time accurately on the TRITON management server.

Antivirus

Exclude the following directories from antivirus scanning:

- The folder where TRITON AP-DATA was installed. By default, this is one of the following:
    - Program Files\Websense\
    - Program Files (x86)\Websense\*.*
- *:\Inetpub\mailroot\*.* - (typically at the OS folder)
- *:\Inetpub\wwwroot\*.* - (typically at the OS folder)
- C:\Documents and Settings\<user>\Local Settings\Temp\*.*
- %WINDIR%\Temp\*.*
- The forensics repository (configurable; defaults to Websense folder)

> **Note**
>
> This document lists the default installation folders. You can configure the software to install to other locations.
>
> The FP-Repository folder is usually located inside the installation folder.

Port requirements

The following ports must be kept open for supplemental TRITON AP-DATA servers:

Outbound		
To	**Port**	**Purpose**
TRITON management server	17443	Incidents
TRITON management server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
* This range is necessary for load balancing.		
Inbound		
From	**Port**	**Purpose**
TRITON management server	8892	Syslog
TRITON management server	139	File sharing
TRITON management server	445	File sharing
TRITON management server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
* This range is necessary for load balancing.		

Installation steps

1. Download the TRITON installer (**TRITON83xSetup.exe**) from My Account.
2. Launch the installer on the machine where you want to install the supplemental server.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for TRITON AP-DATA.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the server software.

   The default destination is C:\Program Files *or* Program Files (x86)\Websense\Data Security. If you have a larger drive, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.

   Important

   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   Note

   Regardless of what drive you specify, it must have a minimum of 4 GB of free disk space on the Windows partition for the TRITON installer.

8. On the **Select Components** screen, select **TRITON AP-DATA Server**.
9. The **Fingerprinting Database** screen appears. To choose a location other than the default shown, use the **Browse** button.
10. In the **Server Access** screen, select the IP address to identify this machine to other Forcepoint components.
11. In the **Register with the TRITON AP-DATA Server** screen specify the location and log on credentials for the TRITON management server.

    FQDN is the fully-qualified domain name of a machine. The credentials should be for a TRITON AP-DATA administrator with System Modules permissions.
12. In the **Local Administrator** screen, supply a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.
13. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, the **Lotus Domino Connections** screen appears.

If you plan to perform fingerprinting or discovery on your Domino server, complete the information on this page.

Important

Before you complete the information on this screen, make sure that you:

- Create at least one user account with administrator privileges for the Domino environment. (Read permissions are not sufficient.)
- Be sure that the Lotus Notes installation is done for "Anyone who uses this computer."
- Connect to the Lotus Domino server from the Lotus Notes client.

a. On the **Lotus Domino Connections** page, select the check box labeled **Use this machine to scan Lotus Domino servers**.

b. In the **User ID file** field, browse to one of the authorized administrator users, then navigate to the user's **user.id** file.

Note

Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

c. In the **Password** field, enter the password for the authorized administrator user.

14. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

    Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.

    If the following message appears, click **Yes** to continue the installation:

    > *TRITON AP-DATA needs port 80 free.*
    > *In order to proceed with this installation, TRITON AP-DATA will free up this port.*
    > *Click Yes to proceed OR click No to preserve your settings.*

    Clicking **No** cancels the installation.

    A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.

15. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.

16. Log on to the Data Security manager and click **Deploy** to fully connect the supplemental server with the management server.

Installing TRITON AP-DATA agents

Below is a summary of the TRITON AP-DATA agents.

With the exception of the protector, mobile agent, analytics engine, and TRITON AP-ENDPOINT, TRITON AP-DATA agents are installed using the Custom option of the standard TRITON installer.

Note that the various agents become available only when you are performing the installation on a required server.

Click the links to learn more about each agent, including where to deploy it, installation prerequisites, installation steps, special considerations, and best practices.

Agent	Description	When to Use	Location
Protector	The protector is a standard part of TRITON AP-DATA deployments. It is a physical or soft appliance with a policy engine and a fingerprint repository, and it supports analysis of SMTP, HTTP, FTP, and plain text that doesn't use SSL. For blocking HTTPS traffic, the protector can integrate with proxies using ICAP. See *Protector*, page 34 for more information.	Monitor/block: network email Monitor: HTTP, FTP, plain text Monitor/block: HTTP via ICAP	On premises
Web Content Gateway	A Web Content Gateway module is included with TRITON AP-DATA Gateway. It provides DLP policy enforcement for the web channel, including decryption of SSL traffic. This core TRITON AP-DATA component permits the use of custom policies, fingerprinting, and more. It also makes use of the Forcepoint URL category database to define DLP policies for the web channel. This gateway is available as a soft appliance. Web Content Gateway is also included in TRITON AP-WEB. In addition to the capabilities described above, this gateway provides URL filtering/ category, content security, web policy enforcement, and more. AP-WEB can be a physical or soft appliance. See *Web Content Gateway*, page 48 for installation instructions.	Monitor/block: HTTP/S with SSL decryption	On premises

Agent	Description	When to Use	Location
TRITON AP-EMAIL	A TRITON AP-DATA policy engine is embedded in TRITON AP-EMAIL. No agent installation is required; however, the policy engine is not active until registered with a TRITON management server. See the Email Security Manager Help for registration instructions.	Monitor/block/ quarantine/ encrypt: Email traffic	On premises
Email Gateway for Office 365	Email Gateway is a virtual appliance that, when deployed in a Microsoft Azure environment, allows outbound email from Exchange Online to be analyzed for data loss or theft. It is included in a TRITON AP-DATA Gateway subscription. See *Email Gateway for Office 365*, page 64 for more information.	Monitor/block/ quarantine/ encrypt: Exchange Online email traffic	Microsoft Azure cloud
Analytics Engine	The Analytics Engine is used to calculate the relative risk of user activity, correlate it with similar activity, and assign it a risk score. See *Analytics engine*, page 90 for more information.	High risk incident scoring	On premises
Cloud agent	The agent included in TRITON AP-DATA Cloud App Security provides cloud activity content inspection for files uploaded into and stored within enterprise cloud collaboration services, such as Microsoft Office 365. See *TRITON AP-DATA Cloud App Security*, page 94 for more information.	DLP: Delete file/ permit Discovery OneDrive for Business files	Microsoft Azure cloud On premises
Mobile agent	The mobile agent monitors and blocks data downloaded to mobile devices that perform synchronization operations with the Exchange server. With the mobile agent, you can monitor and block data transmitted in email messages, calendar events, and tasks. It is on a Forcepoint appliance, or you can install it on your own hardware. The mobile agent supports ActiveSync, which is a wireless communication protocol used to push resources, such as email, from applications to mobile devices. See *Mobile agent*, page 116 for more information.	Monitor/block: Exchange ActiveSync email	On premises

Agent	Description	When to Use	Location
Crawler	The crawler is the name of the agent that performs discovery and fingerprinting scans. The crawler is installed automatically on the TRITON management server and other TRITON AP-DATA servers. If you want to improve scanning performance in high transaction volume environments, you can install it stand-alone on another server as well. See *The crawler*, page 133 for more information.	Discovery/ Fingerprinting	On premises
Endpoint agent	The endpoint agent, TRITON AP-ENDPOINT DLP, monitors all data activity on endpoint machines and reports on data at rest on those machines. With the endpoint agent, you can monitor application operations such as cut, copy, paste, and print screen and block users for copying files, or even parts of files, to endpoint devices such as thumb drives, CD/ DVD burners, and Android phones. The endpoint agent can also monitor or block print operations as well as outbound web posts and email messages. See Installing and Deploying TRITON AP-ENDPOINT Clients for more information.	Monitor/block: email, printing, application control, LAN control, HTTP/S, removable media Local discovery	Endpoint devices

Important

TRITON AP-DATA agents and machines with a policy engine (such as a TRITON AP-DATA Server or Web Content Gateway appliance) must have direct connection to the TRITON management server. When deployed in a DMZ or behind a firewall, the relevant ports must be allowed.

Protector

In this topic:

The protector is a component of TRITON AP-DATA that can monitor and report on web traffic in your organization and act as an MTA to monitor, block, quarantine, and encrypt email traffic.

If desired, you can combine the protector MTA with Email Gateway for Office 365 to offer a combination of on-premises and cloud data protection. Or you can use TRITON AP-EMAIL as your MTA instead.

If you want enforcement over the HTTP/HTTPS channel, you can integrate the protector with a third-party proxy that supports ICAP, or implement the Web Content Gateway instead.

When to use the protector

The protector works in tandem with a TRITON AP-DATA server. The TRITON AP-DATA server provides advanced analysis capabilities, while the protector intercepts network traffic and either monitors or blocks it, depending on the channel. The protector supports analysis of SMTP, HTTP, FTP, and plain text. It can monitor or block email traffic, but only monitor web traffic. Blocking web traffic requires integration with a third-party proxy that supports ICAP.

The protector fits into your existing network with minimum configuration and necessitates no network infrastructure changes.

If you want to monitor SMTP traffic, the protector is your best choice. You configure a span port to be connected to the protector. This span contains your SMTP traffic.

If you want email blocking capabilities, you can use the protector’s explicit MTA mode or TRITON AP-EMAIL.

We do not recommend that you use both options for the same traffic, although some companies prefer monitoring one point and enforcing policies on another, due to differences in network traffic content and load.

If you want to monitor HTTP traffic, you can use the protector to do so, or you can integrate TRITON AP-DATA with TRITON AP-WEB or another Web proxy.

If you want to monitor FTP or plain text, you should use the protector. Note that the protector cannot block traffic on these channels. You can block FTP using TRITON AP-WEB (as a DLP agent) or other Web proxy that buffers FTP and supports ICAP.

Deploying the protector

Most data loss detection devices can be connected off the network, enabling them to sniff network traffic and monitor breaches. This monitoring method is useful because it does not interfere with traffic; however, it also does not enable the loss-prevention system to prevent (block) data losses—only to note and report them.

The following table depicts the available modes for each channel:

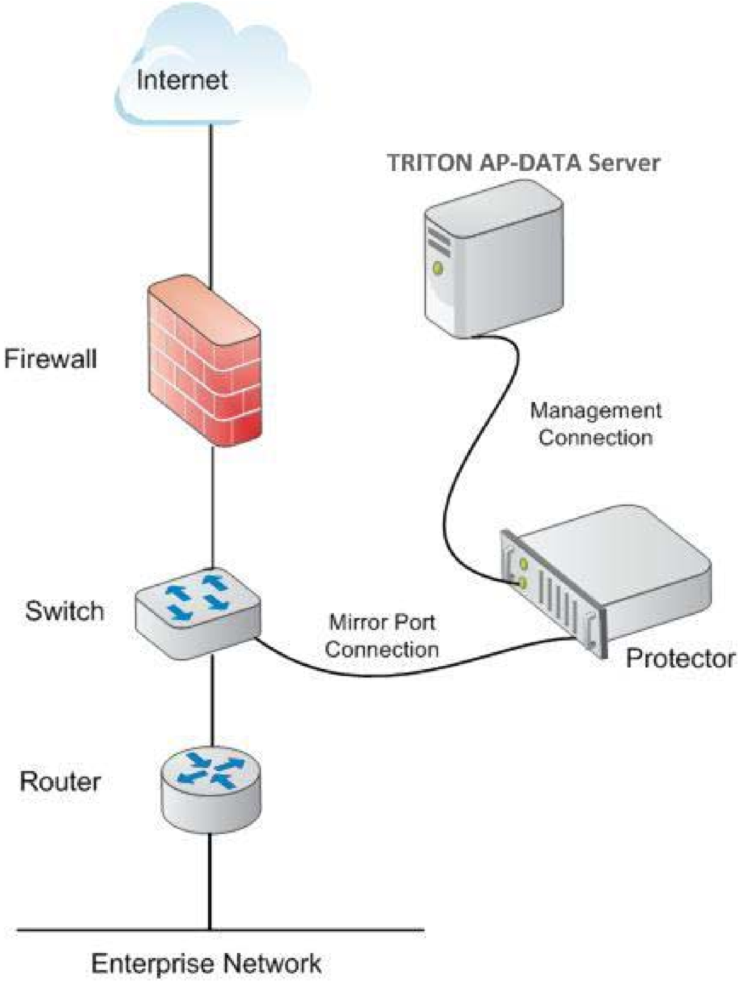
Topology Service	Function
HTTP	Monitoring
SMTP	Monitoring passive Mail Transfer Agent (MTA)
All Others	Monitoring
ICAP	Monitoring Blocking

The protector is connected off the network via the SPAN/mirror port of a switch, which enables the protector to sniff traffic and receive a copy for monitoring purposes, or via a SPAN/mirror device. Traffic is monitored and analyzed, but cannot be blocked. Note that the protector can also be connected to a TAP device.

The following diagram depicts the Forcepoint device connected to the network via a mirror port on a switch, transparently monitoring network traffic.

- Connect the protector to the mirror port of a switch on your network’s path.

- Connect the protector to the TRITON AP-DATA server.



Hardware requirements

The protector is a soft appliance. If you are using your own hardware, it must meet the following hardware requirements:

Protector	Minimum requirements	Recommended
CPU	2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent	2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent
Memory	2 GB	4 GB
Hard drives	2 - 72 GB	4 - 146 GB
Disk space	70 GB	292 GB
Hardware RAID	1	1 + 0
NICs	2	2

Port requirements

The following ports must be kept open for the protector:

Outbound

To	Port	Purpose
TRITON AP-DATA Server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
TRITON management server	17443	Syslog, forensics, incidents, mobile status
TRITON management server	80	Fingerprint sync
Next hop MTA	25**	SMTP
TRITON AP-WEB	56992	Linking Service
Other	UDP 123	Inbound/ outbound NTPD (available on the appliance yet disabled by default)

* This range is necessary for load balancing.

** Explicit MTA

Inbound

From	Port	Purpose
TRITON management server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
Any service (including the Data Security manager) that is not using logging on	22	SSH access
TRITON AP-DATA Server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
Explicit MTA	25**	SMTP
Explicit MTA	10025**	SMTP, mail analysis

* This range is necessary for load balancing.

** Explicit MTA

If you are connecting third-part software such as a web proxy through ICAP, the ICAP client should keep the following outbound port open:

To	Port	Purpose
Protector	1344	Receiving ICAP traffic

Installing the protector software

Installing the TRITON AP-DATA protector comprises 3 basic steps:

1. *Configuring the network*, page 38
2. *Installation steps*, page 38
3. Configure the protector in the Data Security manager. See *Final step: Verification*, page 46.

Protector installations include:

- A policy engine
- ICAP client - for integration with third-party solutions that support ICAP, such as some Web proxies.
- Secondary fingerprint repository (the primary is on the TRITON management server)

Configuring the network

The following preparatory steps must be taken for the protector to be integrated into your network.

Make sure that firewalls or other access control devices on your network do not block ports used by the protector to communicate with the TRITON AP-DATA server (see *Protector*, page 34).

When installing the protector device in the network, both incoming and outgoing traffic (in the monitored segment) must be visible.

In some cases, incoming traffic from the Internet and outgoing traffic to the Internet are on separate links. In this case, the mirror port must be configured to send traffic from both links to the protector. The protector needs to have access to the TRITON management server and vice versa.

Installation steps

You access the installation wizard for your protector through a command line interpreter (CLI).

To install the protector, do the following:

1. If you have purchased a Forcepoint TRITON AP-DATA Appliance, follow the instructions on its quick start poster to rack, cable, and power on the appliance. Note that at least one of the P1, P2, and N interfaces must be configured for monitor mode, although it doesn't matter which one.

   If you are using your own hardware:

   a. Use either a direct terminal or connect via serial port to access the command line. For serial port connection, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:

      ○ 19200 baud

- 8 data bits
- no parity
- 1 stop bit
- no flow control

b. The protector software is provided on an ISO image. Download the image, **DataProtectorMobile83x.iso**, from My Account and burn it to a CD or bootable USB.

c. Place the media in the protector’s CD drive or USB port and restart the machine.

d. An installer page appears. Press **Enter** and the machine is automatically restarted a second time.

2. You’re prompted to enter a user name and password. Enter *admin* for both.

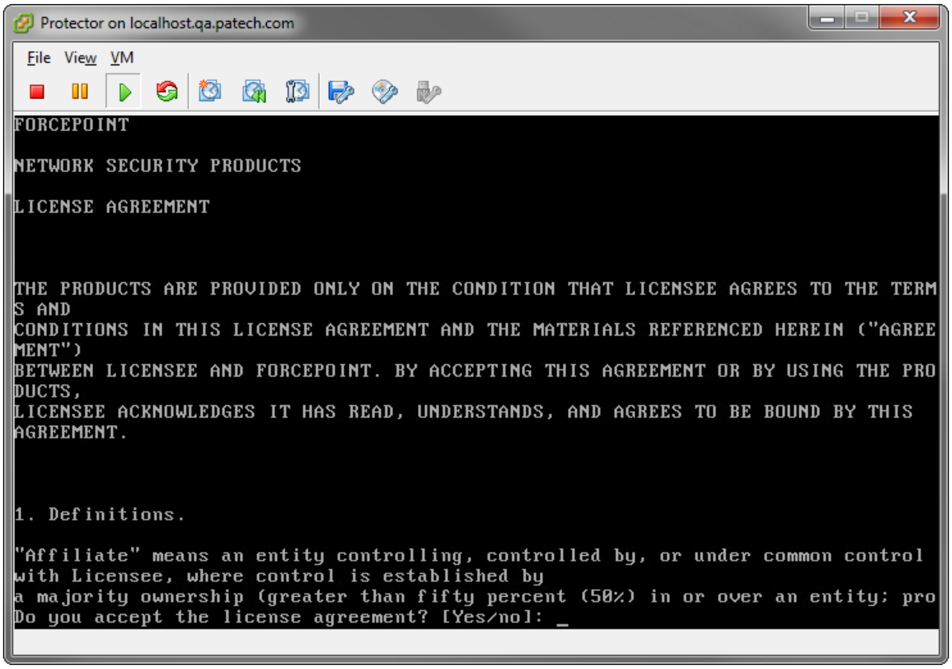
   When the protector CLI opens for the first time, logging in as admin automatically opens the installation wizard. On subsequent attempts, type “wizard” at the command prompt to access the wizard.

3. Follow the instructions given by the wizard to configure basic settings.

   When the wizard requires data entry, it prompts you. In some cases, a default setting is provided (shown within brackets [ ]). If the default setting is acceptable, press <Enter> to keep the default value.

STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down/ scroll /space keys to read/scroll to the end of the agreement. Carefully read the license agreement, and when prompted, type yes to accept the license agreement.



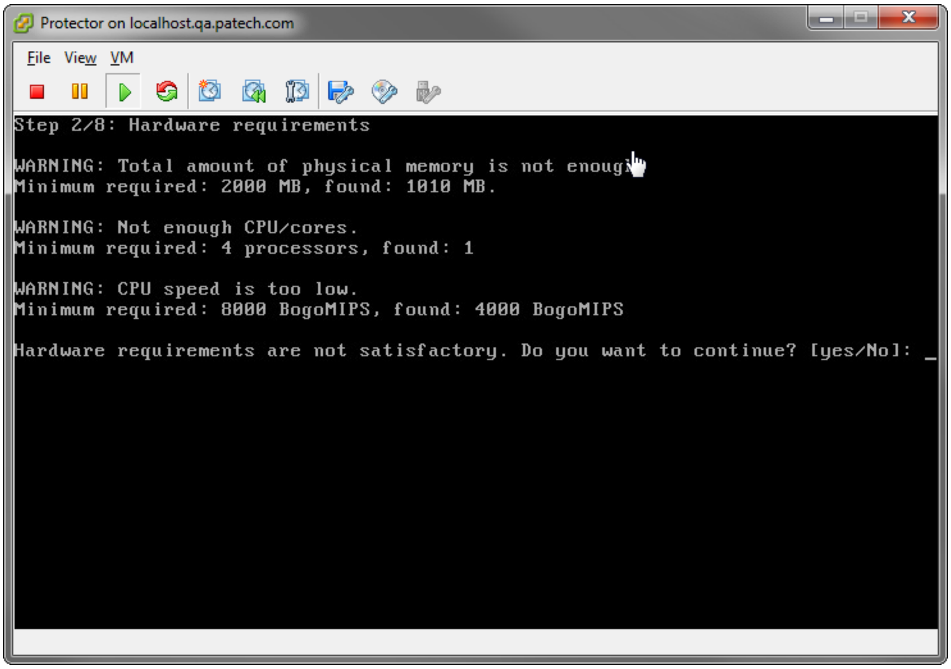
```
FORCEPOINT

NETWORK SECURITY PRODUCTS

LICENSE AGREEMENT



THE PRODUCTS ARE PROVIDED ONLY ON THE CONDITION THAT LICENSEE AGREES TO THE TERM
S AND
CONDITIONS IN THIS LICENSE AGREEMENT AND THE MATERIALS REFERENCED HEREIN ("AGREE
MENT")
BETWEEN LICENSEE AND FORCEPOINT. BY ACCEPTING THIS AGREEMENT OR BY USING THE PRO
DUCTS,
LICENSEE ACKNOWLEDGES IT HAS READ, UNDERSTANDS, AND AGREES TO BE BOUND BY THIS
AGREEMENT.



1. Definitions.

"Affiliate" means an entity controlling, controlled by, or under common control
with Licensee, where control is established by
a majority ownership (greater than fifty percent (50%) in or over an entity; pro
Do you accept the license agreement? [Yes/no]: _
```

STEP 2: Select the hardware to install and confirm hardware requirements

The system checks to see if your hardware meets the following requirements:

- 2 GB RAM
- 4 CPU
- CPU with more than 2MB of cache
- CPU speed of 8000 bogomips
- Partition "/opt/websense/data" should have at least 45 GB
- 2 NICs

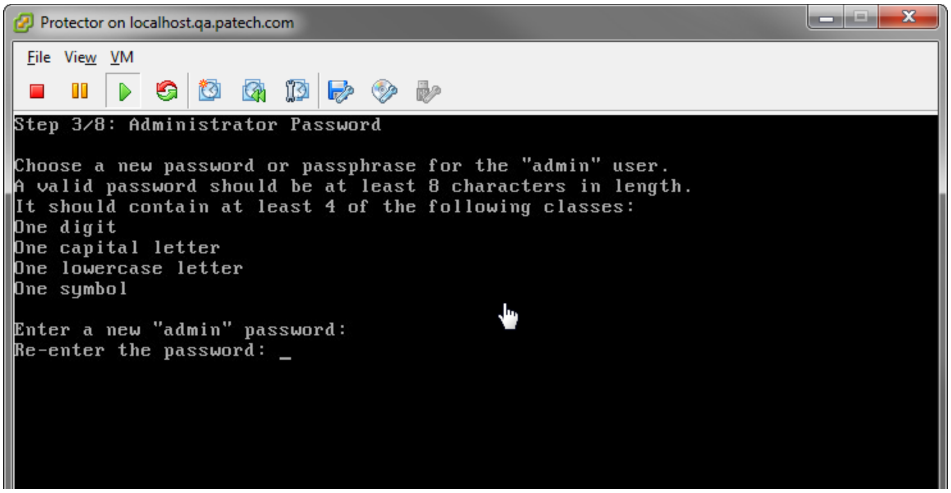
If your requirements are substandard, you’re asked if you want to continue.



```
Step 2/8: Hardware requirements

WARNING: Total amount of physical memory is not enough
Minimum required: 2000 MB, found: 1010 MB.

WARNING: Not enough CPU/cores.
Minimum required: 4 processors, found: 1

WARNING: CPU speed is too low.
Minimum required: 8000 BogoMIPS, found: 4000 BogoMIPS

Hardware requirements are not satisfactory. Do you want to continue? [yes/No]: _
```

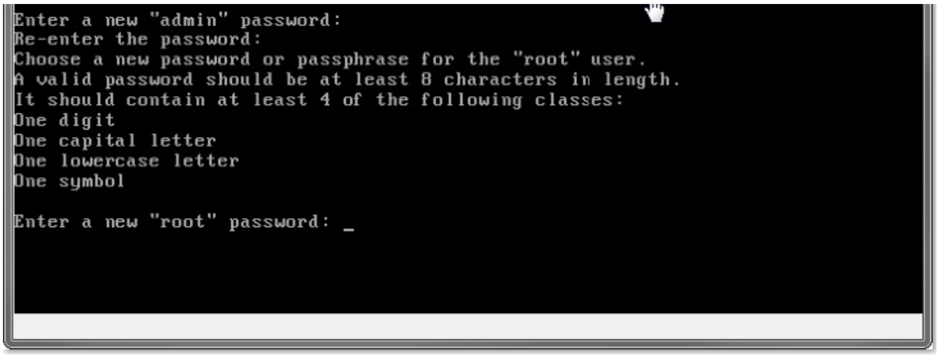
STEP 3: Set administrator password

1. Type in and confirm a new password for the “admin” account. For security reasons, it is best practice to change the default password.



```
Step 3/8: Administrator Password

Choose a new password or passphrase for the "admin" user.
A valid password should be at least 8 characters in length.
It should contain at least 4 of the following classes:
One digit
One capital letter
One lowercase letter
One symbol

Enter a new "admin" password:
Re-enter the password: _
```

2. Type in and confirm a new Root (“root”) Password (mandatory). The root account provides full access to the device and should be used carefully.



```
Enter a new "admin" password:
Re-enter the password:
Choose a new password or passphrase for the "root" user.
A valid password should be at least 8 characters in length.
It should contain at least 4 of the following classes:
One digit
One capital letter
One lowercase letter
One symbol

Enter a new "root" password: _
```

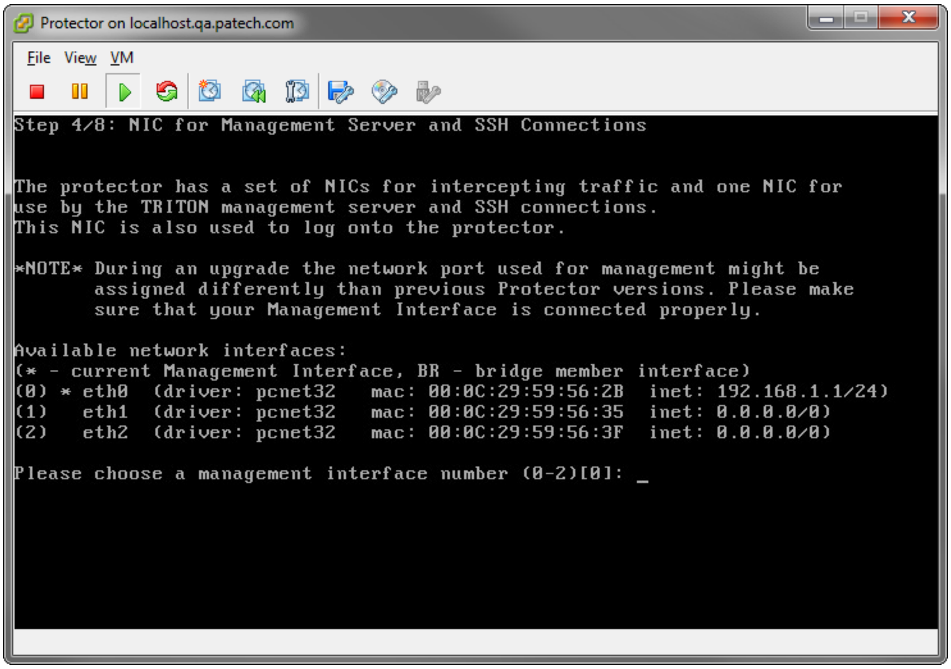
STEP 4: Set the NIC for management server and SSH connections

A list of available network interfaces (NICs) appears. In this step, choose the NIC for use by the TRITON management server, SSH connections, and logging onto the protector (eth0 by default). All other NICs will be used for intercepting traffic.

To help you identify which NIC to use, the wizard can simulate traffic for 0-60 seconds and cause LEDs to blink on that port. This does not work for all hardware and drivers.

1. When prompted, choose the NIC index number of the management NIC or accept the default interface.

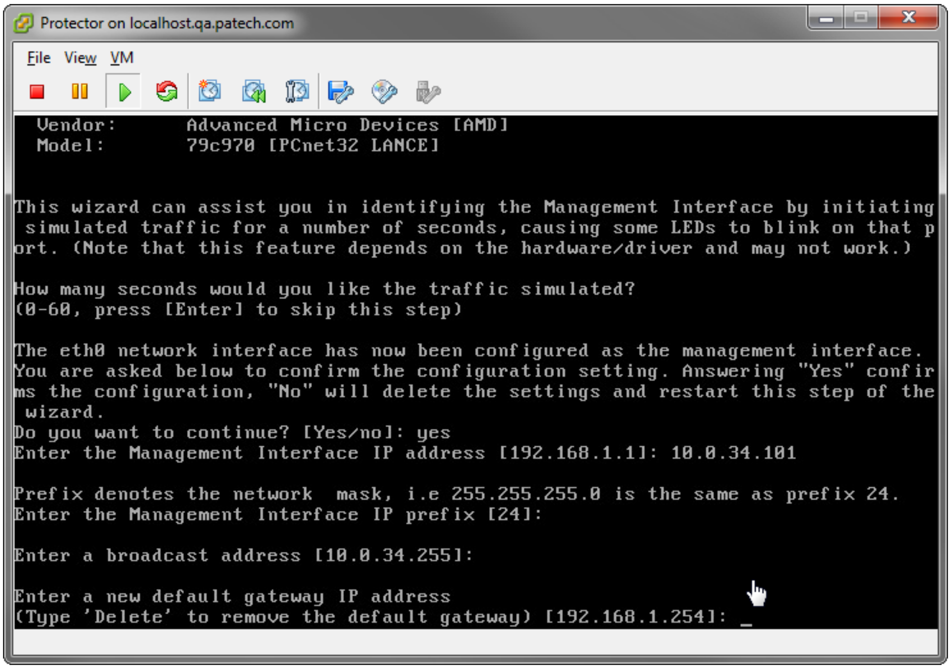
2. Enter a number 0-60 to indicate how long (in seconds) you'd like traffic simulated or press **Enter** to skip this step.



```
Step 4/8: NIC for Management Server and SSH Connections


The protector has a set of NICs for intercepting traffic and one NIC for
use by the TRITON management server and SSH connections.
This NIC is also used to log onto the protector.

*NOTE* During an upgrade the network port used for management might be
       assigned differently than previous Protector versions. Please make
       sure that your Management Interface is connected properly.

Available network interfaces:
(* - current Management Interface, BR - bridge member interface)
(0) * eth0  (driver: pcnet32   mac: 00:0C:29:59:56:2B  inet: 192.168.1.1/24)
(1)   eth1  (driver: pcnet32   mac: 00:0C:29:59:56:35  inet: 0.0.0.0/0)
(2)   eth2  (driver: pcnet32   mac: 00:0C:29:59:56:3F  inet: 0.0.0.0/0)

Please choose a management interface number (0-2)[0]: _
```

3. Type the IP address of the NIC you've chosen. The default is 192.168.1.1.
4. Type the IP prefix of this NIC. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 24 (255.255.255.0).
5. Type a broadcast address for the NIC. The installation wizard will provide a calculated value, which is normally the desired one.

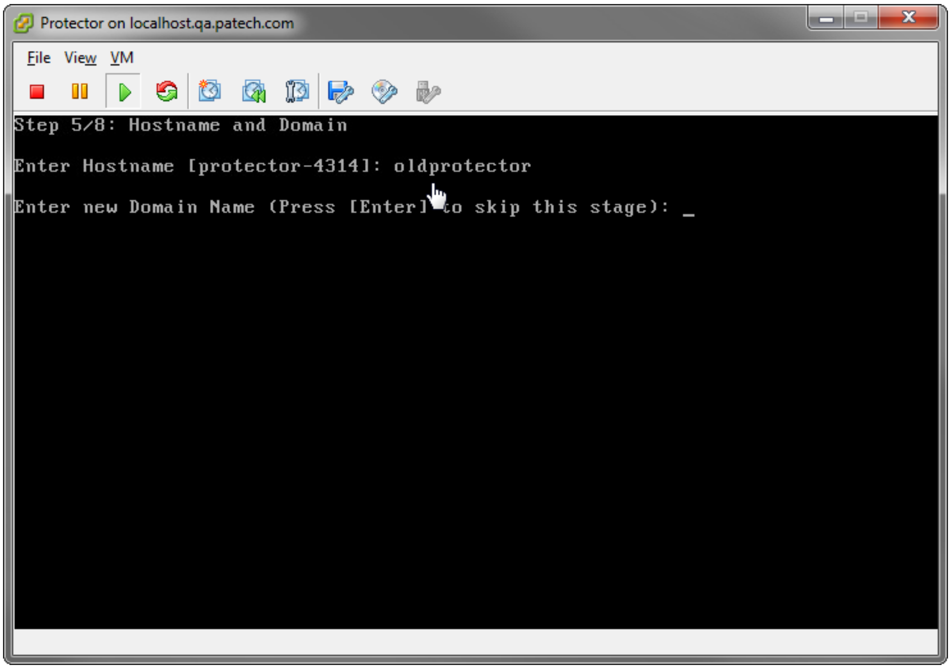
6. Type the IP address of the default gateway to be used to access the network. If the IP address of the TRITON AP-DATA server is not on the same subnet as the protector, a default gateway is required to tell the protector how to communicate with the TRITON AP-DATA server.



```
  Vendor:       Advanced Micro Devices [AMD]
  Model:        79c970 [PCnet32 LANCE]

This wizard can assist you in identifying the Management Interface by initiating
 simulated traffic for a number of seconds, causing some LEDs to blink on that p
ort. (Note that this feature depends on the hardware/driver and may not work.)

How many seconds would you like the traffic simulated?
(0-60, press [Enter] to skip this step)

The eth0 network interface has now been configured as the management interface.
You are asked below to confirm the configuration setting. Answering "Yes" confir
ms the configuration, "No" will delete the settings and restart this step of the
 wizard.
Do you want to continue? [Yes/no]: yes
Enter the Management Interface IP address [192.168.1.1]: 10.0.34.101

Prefix denotes the network  mask, i.e 255.255.255.0 is the same as prefix 24.
Enter the Management Interface IP prefix [24]:

Enter a broadcast address [10.0.34.255]:

Enter a new default gateway IP address
(Type 'Delete' to remove the default gateway) [192.168.1.254]: _
```

STEP 5: Define the host name and domain name

1. Type the host name to be used to identify this protector. The host name should be unique.

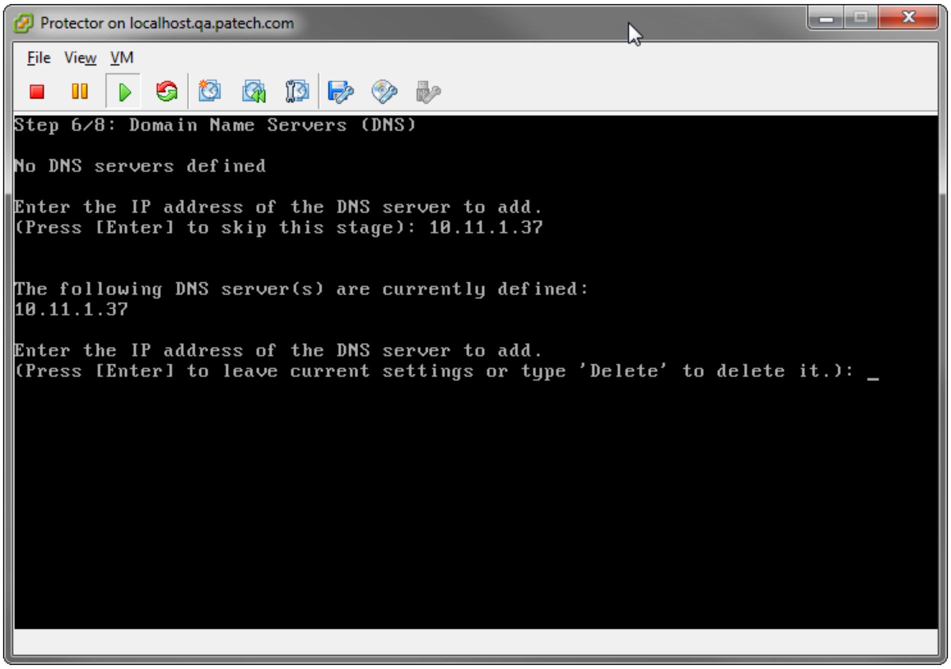


```
Step 5/8: Hostname and Domain

Enter Hostname [protector-4314]: oldprotector

Enter new Domain Name (Press [Enter] to skip this stage): _
```

2. Optionally, type the domain name of the network into which the protector was added. The domain name set here will be used by the TRITON AP-DATA server when defining the protector's parameters.

STEP 6: Define the domain name server

Optionally, type the IP address of the domain name server (DNS) that will service this protector. A DNS will allow access to other network resources using their names instead of their IP addresses.

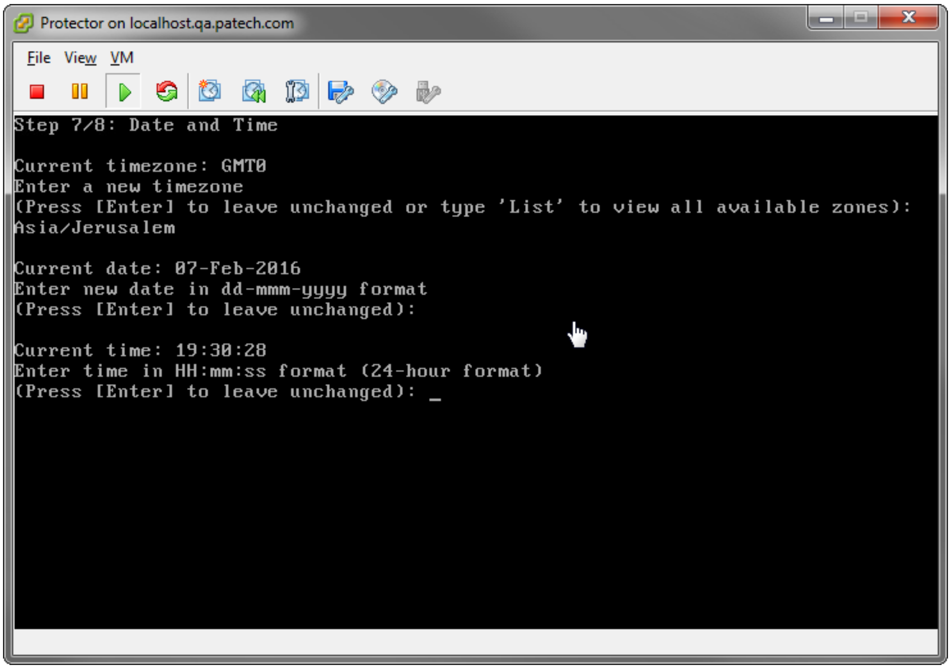


```
Step 6/8: Domain Name Servers (DNS)

No DNS servers defined

Enter the IP address of the DNS server to add.
(Press [Enter] to skip this stage): 10.11.1.37


The following DNS server(s) are currently defined:
10.11.1.37

Enter the IP address of the DNS server to add.
(Press [Enter] to leave current settings or type 'Delete' to delete it.): _
```

STEP 7: Set the date, time and time zone

1. Type the current time zone (to view a list of all timezones, type **list**).
2. Type the current date in the following format: dd-mmm-yyyy.

3. Type the current time in the following format: HH:MM:SS. Note that this is a 24-hour clock.

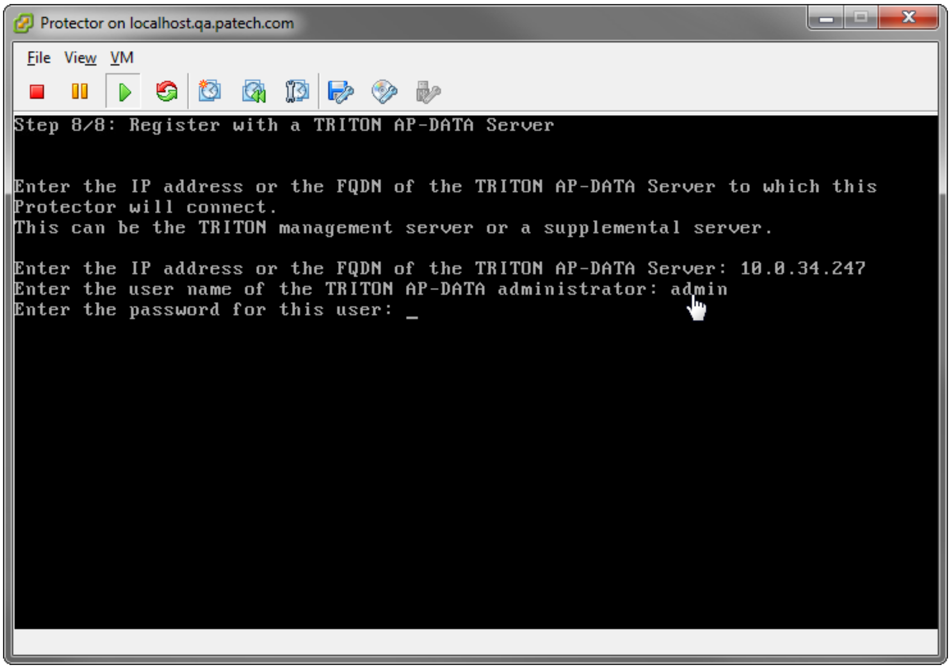


```
Step 7/8: Date and Time

Current timezone: GMT0
Enter a new timezone
(Press [Enter] to leave unchanged or type 'List' to view all available zones):
Asia/Jerusalem

Current date: 07-Feb-2016
Enter new date in dd-mmm-yyyy format
(Press [Enter] to leave unchanged):

Current time: 19:30:28
Enter time in HH:mm:ss format (24-hour format)
(Press [Enter] to leave unchanged): _
```

STEP 8: Register with a TRITON AP-DATA Server

In this step, a secure channel will be created connecting the protector to a TRITON AP-DATA Server. This can be the TRITON management server or a supplemental server, depending on your set up.

1. Type the IP address or FQDN of the TRITON AP-DATA Server. Note that this must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.



```
Step 8/8: Register with a TRITON AP-DATA Server

Enter the IP address or the FQDN of the TRITON AP-DATA Server to which this
Protector will connect.
This can be the TRITON management server or a supplemental server.

Enter the IP address or the FQDN of the TRITON AP-DATA Server: 10.0.34.247
Enter the user name of the TRITON AP-DATA administrator: admin
Enter the password for this user: _
```

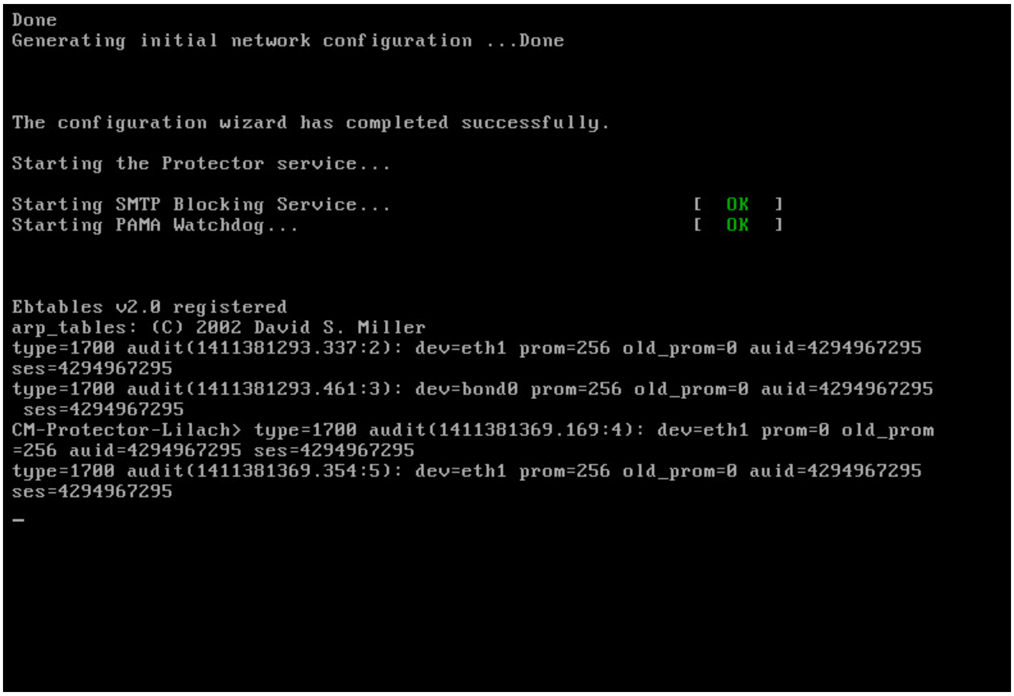
2. Type the user name and password for a TRITON AP-DATA administrator that has privileges to manage system modules.

Final step: Verification

In the TRITON AP-DATA module of TRITON Manager, verify that the Forcepoint Protector is no longer pending and that the icon displays its active status. Refresh the browser.

Click **Deploy**.

In the protector command-line interface, the following appears:



```
Done
Generating initial network configuration ...Done


The configuration wizard has completed successfully.

Starting the Protector service...

Starting SMTP Blocking Service...                          [  OK  ]
Starting PAMA Watchdog...                                  [  OK  ]



Ebtables v2.0 registered
arp_tables: (C) 2002 David S. Miller
type=1700 audit(1411381293.337:2): dev=eth1 prom=256 old_prom=0 auid=4294967295
ses=4294967295
type=1700 audit(1411381293.461:3): dev=bond0 prom=256 old_prom=0 auid=4294967295
 ses=4294967295
CM-Protector-Lilach> type=1700 audit(1411381369.169:4): dev=eth1 prom=0 old_prom
=256 auid=4294967295 ses=4294967295
type=1700 audit(1411381369.354:5): dev=eth1 prom=256 old_prom=0 auid=4294967295
ses=4294967295
_
```

The protector is now ready to be configured.

Configuring the protector

To begin monitoring the network for sensitive information loss, you must perform some configuration in the Data Security manager user interface.

In the TRITON console, click the Data tab and then navigate to **Settings** > **Deployment** > **System Modules** and double-click the installed protector.

- Define the channels that the Forcepoint Protector will monitor.
- Supply additional configuration parameters needed by the TRITON AP-DATA Server to define policies for unauthorized traffic.
- Click **Deploy** to deploy your settings.

When you are done, make sure the protector does not have the status Disabled or Pending. You can view its status by looking at the System Modules page.

For more configuration information, see Configuring the Protector in the Data Security Manager Help system.

Web Content Gateway

A Web Content Gateway module is included with TRITON AP-DATA Gateway. It provides DLP policy enforcement for the web channel, including decryption of SSL traffic, user authentication, and content inspection using the DLP policy engine.

This core TRITON AP-DATA component permits the use of custom policies, fingerprinting, and more. It is available as a soft appliance, and does not use the Web module of the TRITON Manager.

Web Content Gateway is also included in TRITON AP-WEB. In addition to SSL decryption, this gateway provides URL filtering/category, content security, web policy enforcement, and more. TRITON AP-WEB can be a physical or soft appliance.

This section describes how to install the core TRITON AP-DATA Web Content Gateway component. For instructions on setting up TRITON AP-WEB, see the TRITON AP-WEB Installation Guide.

Note that Web Content Gateway is inactive until registered with a TRITON management server.

Preparing your operating system for Content Gateway

Content Gateway supports Red Hat Linux 6 series, 64-bit, Basic Server and the corresponding CentOS version.

Special steps must be taken to install and configure such versions to work with Content Gateway v8.3.x.

Warning

Content Gateway is supported on Red Hat Enterprise Linux 6, Basic Server (no GUI) and is **not** supported on RHEL 6 with a GUI.

biosdevname

Red Hat Enterprise Linux 6, update 1 introduced **biosdevname**, but biosdevname is not supported by Content Gateway Version 8.3.x. It must be disabled.

What is biosdevname? The Red Hat Enterprise Linux update 6.1 release notes state:

> ... biosdevname [is an] optional convention for naming network interfaces. biosdevname assigns names to network interfaces based on their physical location. ... biosdevname is disabled by default, except for a limited set of Dell systems.

biosdevname is designed to replace the older, inconsistent “eth#” naming scheme. The new standard will be very helpful when it is fully adopted, however it is not yet fully adopted.

The presence of a single Ethernet device absent the SMIBIOS Slot # and biosdevname field causes the Red Hat Enterprise Linux 6.x installer and ‘udev’ to fall back to the preferred eth# device naming for all interfaces.

Important

To ensure interface name consistency among hardware platforms and Red Hat Enterprise Linux 6.4 and higher, Content Gateway Version 8.3.x requires “eth#” names. If any non-“eth#” names exist, the Content Gateway installer exits and provides a link to instructions for modifying system startup files.

Upgrading from Red Hat Enterprise Linux 6.0 to 6.4 and higher poses no risk. There was no biosdevname support in Update 6.0 and device names are not altered by the upgrade to 6.4 or higher.

Disabling biosdevname

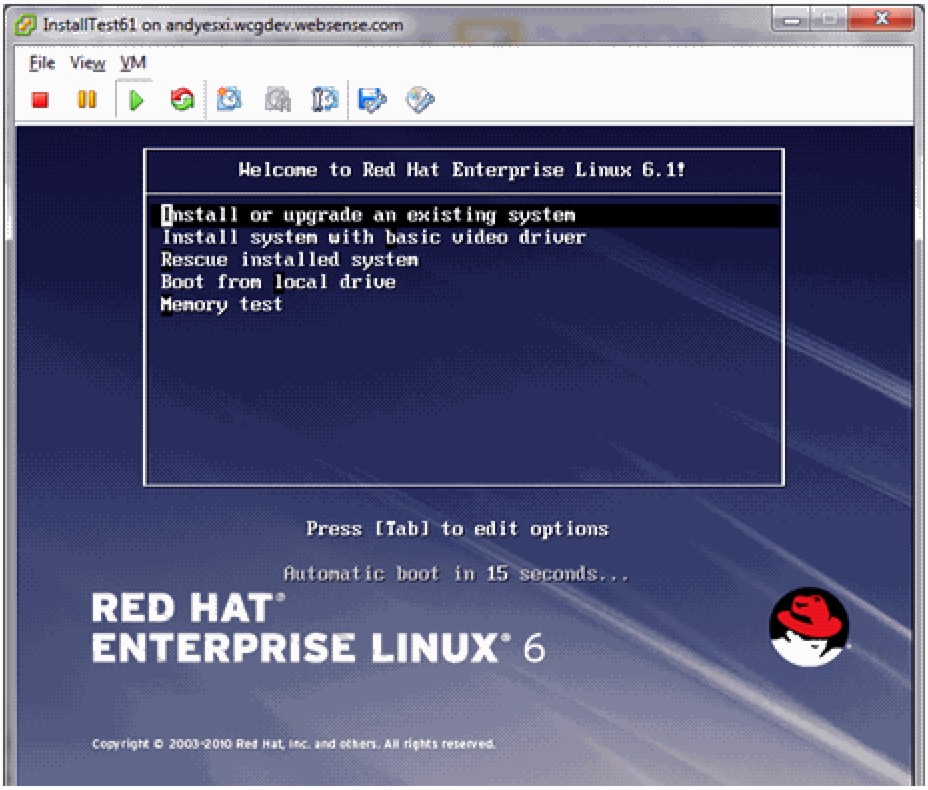
If while installing Content Gateway, the installer finds non-eth# interface names, the installer quits and provides a link to instructions for modifying system startup files.

There are 2 ways to disable biosdevname:

1. During operating system installation.
2. Post-operating system installation through modification of several system files and other activities.

The easiest way to disable biosdevname is to do it during operating system installation. This is the recommend method.

Disabling biosdevname during operating system installation:

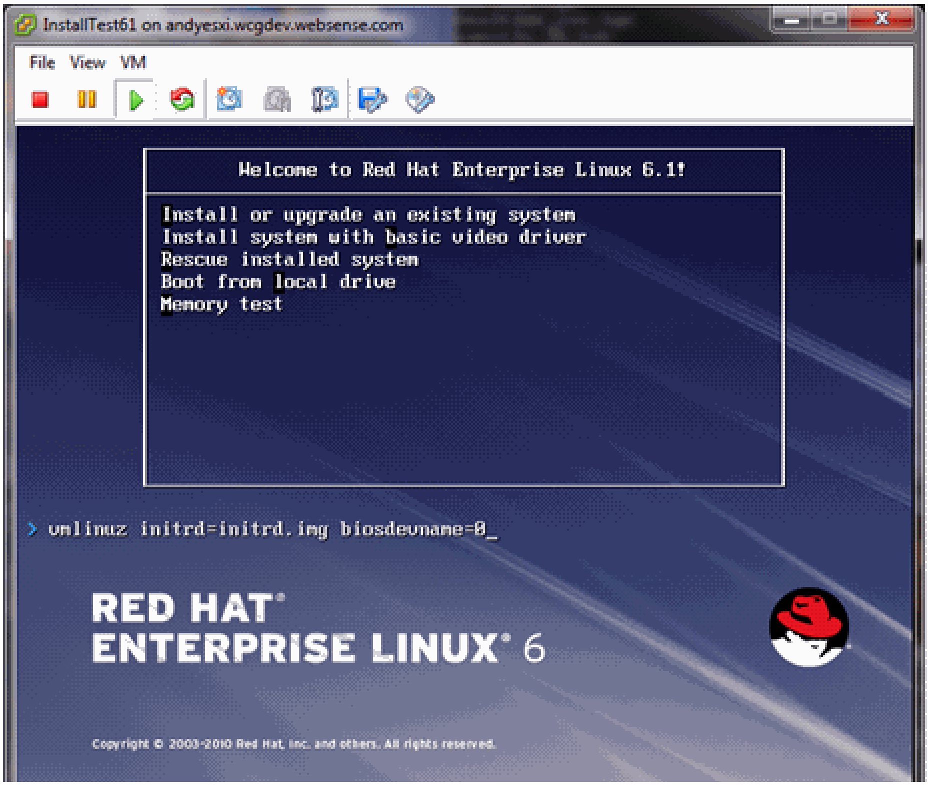


InstallTest61 on andyesxi.wcgdev.websense.com
File View VM

```
Welcome to Red Hat Enterprise Linux 6.1!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

Press [Tab] to edit options

Automatic boot in 15 seconds...
```

RED HAT®
ENTERPRISE LINUX® 6
Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

When the installer starts, press [TAB] and alter the boot line to add “biosdevname=0” as follows:


InstallTest61 on andyesxi.wcgdev.websense.com
File View VM
RED HAT®
ENTERPRISE LINUX® 6
Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

Welcome to Red Hat Enterprise Linux 6.1!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

```
> vmlinuz initrd=initrd.img biosdevname=0_
```

Proceed through the rest of the installer as usual.

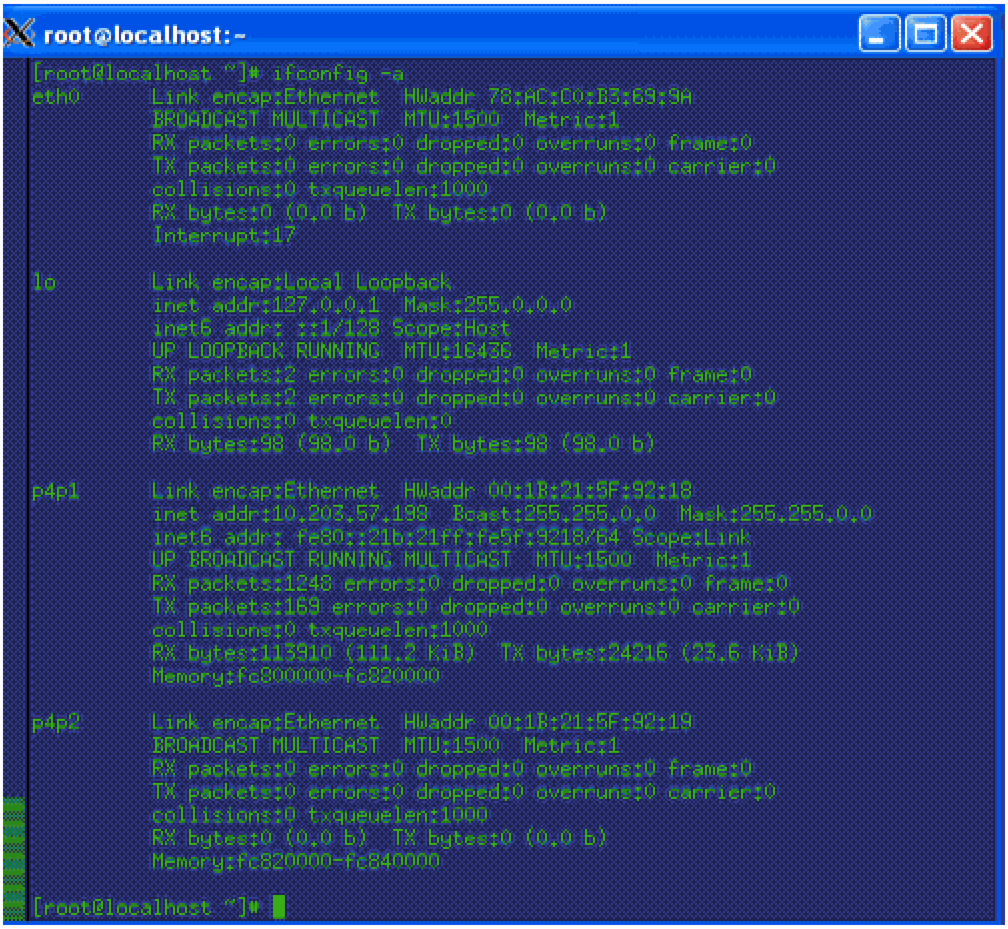
Disabling biosdevname after operating system installation:

Log on to the operating system and verify that non-eth# names are present.

```
ifconfig -a
```

If only “eth#” and “lo” names are present, you are done. No other actions are required.

If there are names like “emb#” or “p#p#” perform the following steps.



```
[root@localhost ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 78:AC:C0:B3:69:9A
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:98 (98.0 b)  TX bytes:98 (98.0 b)

p4p1      Link encap:Ethernet  HWaddr 00:1B:21:5F:92:18
          inet addr:10.203.57.198  Bcast:255.255.0.0  Mask:255.255.0.0
          inet6 addr: fe80::21b:21ff:fe5f:9218/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:113910 (111.2 KiB)  TX bytes:24216 (23.6 KiB)
          Memory:fc800000-fc820000

p4p2      Link encap:Ethernet  HWaddr 00:1B:21:5F:92:19
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:fc820000-fc840000

[root@localhost ~]#
```

1. Log in as root.
2. cd /etc/sysconfig/network-scripts
3. Rename all “ifcfg-<ifname>” files except “ifcfg-lo” so that they are named “ifcfg-eth#”.
    a. Start by renaming “ifcfg-em1” to “ifcfg-eth0” and continue with the rest of the “ifcfg-em#” files.
    b. When the above are done, rename the “ifcfg-p#p#” files.

       If there are multiple “ifcfg-p#p1” interfaces, rename all of them in the order of the lowest “ifcfg-p#” first. For example, if the initial set of interfaces presented by “`ifconfig -a” is:

       em1 em2 em3 em4 p1p1 p1p2 p2p1 p2p2

       em1 -> eth0

       em2 -> eth1

       em3 -> eth2

       em4 -> eth3

       p1p1 -> eth4

       p1p2 -> eth5

p2p1 -> eth6

p2p2 -> eth7

c. Make the “ifcfg-eth#” files linear so that if you have 6 interfaces you have eth0 through eth5.

4. Edit all the ifcfg-eth# files.

   a. Update the DEVICE= sections to refer to the new name: “eth#”

   b. Update the NAME= sections to refer to the new name: “System eth#”

5. Remove the old udev device mapping file if it exists:

   ```
   rm -f /etc/udev/rules.d/70-persistent-net.rules
   ```

6. Modify the “grub.conf” file to disable biosdevname for the kernel you boot.

   a. Edit /boot/grub/grub.conf

   b. Add the following to the end of your “kernel /vmlinuz” line:

      ```
      biosdevname=0
      ```

7. Reboot.

8. Reconfigure the interfaces as required.

Prepare for installation

1. Make sure that the server you intend to use meets or exceeds the requirements listed in the “Content Gateway” section of “Requirements for web protection solutions” in System requirements for this version.

2. Configure a hostname for the Content Gateway machine and also configure DNS name resolution. Complete these steps on the machine on which you will install Content Gateway.

   a. Configure a hostname for the machine that is 15 characters or less:

      ```
      hostname <hostname>
      ```

   b. Update the HOSTNAME entry in the **/etc/sysconfig/network** file to include the new hostname assigned in the previous step:

      ```
      HOSTNAME=<hostname>
      ```

   c. Specify the IP address to associate with the hostname in the **/etc/hosts** file. This should be static and not served by DHCP.

      The proxy uses this IP address in features such as transparent authentication and hierarchical caching. This must be the first line in the file.

      Do not delete the second and third lines (the ones that begin with “127.0.0.1” and “::1”, respectively).

      ```
      xxx.xxx.xxx.xxx   <FQDN>    <hostname>
      127.0.0.1       localhost.localdomain   localhost
      ::1             localhost6.localdomain6 localhost6
      ```

   <*FQDN*> is the fully-qualified domain name of this machine (for example: myhost.example.com). <*hostname*> is the same name specified in Step a.

   Do **not** reverse the order of the FQDN and hostname.

d. Configure DNS in the **/etc/resolv.conf** file.

```
search <subdomain1>.<top-level domain>
<subdomain2>.<top-level domain> <subdomain3>.<top-
level domain>

nameserver xxx.xxx.xxx.xxx

nameserver xxx.xxx.xxx.xxx
```

This example demonstrates that more than one domain can be listed on the search line. Listing several domains may have an impact on performance, because each domain is searched until a match is found. Also, this example shows a primary and secondary nameserver being specified.

e. Gather this information:

○ Default gateway (or other routing information)

○ List of your company’s DNS servers and their IP addresses

○ DNS domains to search, such as internal domain names. Include any legacy domain names that your company might have.

○ List of additional firewall ports to open beyond SSH (22) and the proxy ports (8080-8090).

3. For Content Gateway to operate as a caching proxy, it must have access to at least one raw disk. Otherwise, Content Gateway will function as a proxy only.

To create a raw disk for the proxy cache when all disks have a mounted file system:

✓ **Note**

This procedure is necessary only if you want to use a disk already mounted to a file system as a cache disk for Content Gateway. Perform this procedure **before** installing Content Gateway.

! **Warning**

Do not use an LVM (Logical Volume Manager) volume as a cache disk.

! **Warning**

The Content Gateway installer will irretrievably clear the contents of cache disks.

a. Enter the following command to examine which file systems are mounted on the disk you want to use for the proxy cache:

```
df -k
```

b. Open the file /etc/fstab and comment out or delete the file system entries for the disk.

c. Save and close the file.

d. Enter the following command for each file system you want to unmount:

```
umount <file_system>
```

When the Content Gateway installer prompts you for a cache disk, select the raw disk you created.

Note

It is possible to add cache disks after Content Gateway is installed. For instructions, see the Content Gateway Manager Help.

4. If you plan to deploy multiple, clustered instances of Content Gateway:
   - Find the name of the network interface you want to use for cluster communication. This must be a dedicated interface.
   - Find or define a multicast group IP address.

     If a multicast group IP address has not already been defined, enter the following at a command line to define the multicast route:

     ```
     route add <multicast.group address>/32 dev
     <interface_name>
     ```

     Here, <*interface_name*> is the name of the interface used for cluster communication. For example:

     ```
     route add 224.0.1.37/32 dev eth1
     ```
5. It is recommended that the Content Gateway host machine have Internet connectivity before starting the installation procedure. The software will install without Internet connectivity, but analytic database updates cannot be performed until Internet connectivity is available.
6. Download the **ContentGateway83xSetup_Lnx.tar.gz** installer tar archive from My Account to a temporary directory on the machine that will host Content Gateway.

   To unpack the tar archives, use the command:

   ```
   tar -xvzf ContentGateway83xSetup_Lnx.tar.gz
   ```
7. Consider the following security issues prior to installing Content Gateway:
   - Physical access to the system can be a security risk. Unauthorized users could gain access to the file system, and under more extreme circumstances, examine traffic passing through Content Gateway. It is strongly recommended that the Content Gateway server be locked in an IT closet and that a BIOS password be enabled.
   - Ensure that root permissions are restricted to a select few persons. This important restriction helps preclude unauthorized access to the Content Gateway file system.

- For a list of default ports, see the Web tab of the TRITON Ports spreadsheet. They must be open to support the full set of Web Content Gateway features.

  Note

  If you customized any ports that Forcepoint software uses for communication, replace the default port with the custom port you implemented.

- If your server is running the Linux IPTables firewall, you must configure the rules in a way that enables Content Gateway to operate effectively. See IPTables for Content Gateway.

8. Content Gateway can be used as an explicit or transparent proxy. For setup considerations for each option, see the Content Gateway explicit and transparent proxy deployments.

Install Content Gateway

1. Disable any currently running firewall on this machine for the duration of Content Gateway installation. Bring the firewall back up after installation is complete, opening ports used by Content Gateway.

   Important

   If SELinux is enabled, set it to permissive or disable it before installing Content Gateway. Do not install or run Content Gateway with SELinux enabled.

2. Make sure you have root permissions:

   ```
   su root
   ```

3. In the directory where you unpacked the tar archive, begin the installation, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

   The installer installs Content Gateway in /opt/WCG. It is installed as **root**.

   Note

   Up to the configuration summary, you can quit the installer by pressing Ctrl-C. If you choose to continue the installation past the configuration summary and you want to quit, do **not** use Ctrl-C. Instead, allow the installation to complete and then uninstall it.

   If you want to change your answer to any of the installer prompts, you will be given a chance to start over at the first prompt once you reach the configuration summary; you do not have to quit the installer.

4. If your server does not meet the minimum hardware requirements or is missing required operating system packages, you will receive error or warning messages. For example:

   ```
   Error: Forcepoint Content Gateway v8.3.x on x86_64
   requires several packages that are not present on your
   system.

   Please install the following packages: <list of packages>

   If you are connected to a yum repository you can install
   these packages with the following command:

   yum install <list of packages>

   See the Forcepoint Technical Library (www.forcepoint.com/
   library) for information about the software requirements
   for x86_64 installation.
   ```

   Install the missing packages and again start the Content Gateway installer.

   Here is an example of a system resource warning:

   ```
   Warning: Forcepoint Content Gateway requires at least 6
   gigabytes of RAM.

   Do you wish to continue [y/n]?
   ```

   Enter **n** to end the installation and return to the system prompt.

   Enter **y** to continue the installation. If you choose to run Content Gateway after receiving this warning, performance may be affected.

5. Read the subscription agreement. At the prompt, enter **y** to continue installation or **n** to cancel installation.

   ```
   Do you accept the above agreement [y/n]? y
   ```

6. Enter and confirm a password for the Content Gateway Manager administrator account:

   ```
   Enter the administrator password for the Forcepoint
   Content Gateway management interface.

   Username: admin

   Password:> (note: cursor will not move as you type)

   Confirm password:>
   ```

   This account enables you to log on to the management interface for Content Gateway (the Content Gateway manager). The default username is **admin**.

To create a strong password (required), use 8 to 15 characters, with at least 1 each of the following: upper case letter, lower case letter, number, special character.

Important

The password cannot contain the following characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

Note

As you type a password, it may seem that nothing is happening—the cursor will not move nor will masked characters be shown—but the characters are being accepted. After typing a password, press **Enter**. Then repeat to confirm it.

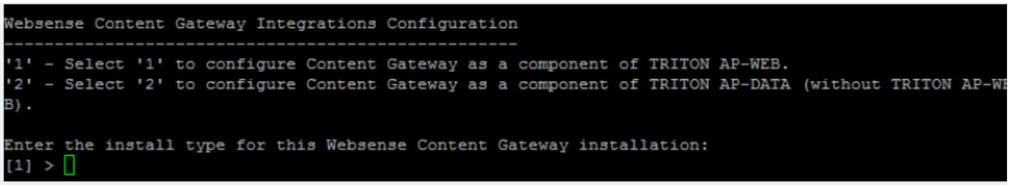
7. Enter an email address where Content Gateway can send alarm messages:

```
Forcepoint Content Gateway requires an email address for
alarm notification.
```

```
Enter an email address using @ notation: [] >
```

Be sure to use @ notation (for example, user@example.com). Do not enter more than 64 characters for this address.

8. When prompted, select ‘2’ to configure the Content Gateway as a component of TRITON AP-DATA Gateway (without TRITON AP-WEB).



```
Websense Content Gateway Integrations Configuration
-------------------------------------------------
'1' - Select '1' to configure Content Gateway as a component of TRITON AP-WEB.
'2' - Select '2' to configure Content Gateway as a component of TRITON AP-DATA (without TRITON AP-WE
B).

Enter the install type for this Websense Content Gateway installation:
[1] > 
```

9. When prompted:

```
Enter Data Security Manager Server IP: [] >
```

This is the IP address of the TRITON management server. Use dot notation (i.e., xxx.xxx.xxx.xxx). The address must be IPv4.

10. Review default Content Gateway ports:

```
Forcepoint Content Gateway uses 8 ports on your server:
```

```
Port Assignments:
```

```
-----------------
'1'  Forcepoint Content Gateway Proxy Port  8080
```

```
'2'  Web Interface port                    8081
'3'  Auto config port                      8083
'4'  Process manager port                  8084
'5'  Logging server port                   8085
'6'  Clustering port                       8086
'7'  Reliable service port                 8087
'8'  Multicast port                        8088

Enter the port assignment you would like to change:
‘1-8’ - specific port changes
‘X’   - no change
‘H’   - help
[X] >
```

Change a port assignment if it will conflict with another application or process on the machine. Otherwise, leave the default assignments in place.

If you do not want to use these ports for Content Gateway, or if the installation program indicates that a port conflict exists, make any necessary changes. Any new port numbers you assign must be between 1025 and 65535, inclusive.

11. For clustering, at least two network interfaces are required. If your machine has only one, the following prompt appears:

    ```
    Forcepoint Content Gateway requires at least 2 interfaces
    to support clustering. Only one active network interface
    is detected on this system.
    ```

    Press **Enter** to continue installation and skip to Step 13.

12. If two or more network interfaces are found on this machine, you are asked whether this instance of Content Gateway should be part of a cluster:

    ```
    Forcepoint Content Gateway Clustering Information
    ------------------------------------------------
    '1' - Select '1' to configure Forcepoint Content Gateway
            for management clustering. The nodes in the cluster
            will share configuration/management information
            automatically.
    '2' - Select '2' to operate this Forcepoint Content Gateway
            as a single node.


    Enter the cluster type for this Forcepoint Content Gateway
    installation:
    [2] >
    ```

    If you do not want this instance of Content Gateway to be part of a cluster, enter 2.

    If you select 1, provide information about the cluster:

    ```
    Enter the name of this Forcepoint Content Gateway cluster.
    ><cluster_name>
    ```

    Note: All members of a cluster must use the same cluster name.

    ```
    Enter a network interface for cluster communication.
    ```

```
Available interfaces:
<interface, e.g., eth0>
<interface, e.g., eth1>
Enter the cluster network interface:
>
Enter a multicast group address for cluster <cluster_name>.
Address must be between 224.0.1.27 - 224.0.1.254:
[<default IP address>] >
```

13. For Content Gateway to act as a web cache, a raw disk must be present on this machine. If no raw disk is detected, the following prompt appears:

    ```
    No disks are detected for cache.
    Forcepoint Content Gateway will operate in PROXY_ONLY mode.
    ```

    Content Gateway will operate as a proxy only and will not cache web pages. Press Enter to continue the installation and skip Step 15.

14. If a raw disk is detected, you can enable the web cache feature of Content Gateway:

    ✓ **Note**

    If you choose to not enable raw disk cache now, cache disks may be added after Content Gateway has been installed. For instructions, see Content Gateway Manager Help.

    ```
    Would you like to enable raw disk cache [y/n]? y
    ```

    a. Select available disks from the list. Selected disks become dedicated cache disks and cannot be used for any other purpose. Cache disks must be raw. Aggregate disk cache size should not exceed 147 GB.

    ```
    Select available disk resources to use for the cache.
    Remember that space used for the cache cannot be used for
    any other purpose.
    Here are the available drives
    (1) /dev/sdb 146778685440 0x0
    ```

    Note: The above drive is only an example.

    ⚠ **Warning**

    Although it might be listed as available, do **not** use an LVM (Logical Volume Manager) volume as a cache disk.

    b. Indicate if you want to add or remove disks individually or as a group.

    ```
    Choose one of the following options:
    'A'   - Add disk(s) to cache
    'R'   - Remove disk(s) from cache
    'S'   - Add all available disks to cache
    'U'   - Remove all disks from cache
    ```

```
'X'    - Done with selection, continue Forcepoint
         Content Gateway installation.
Option: > A
[ ] (1) /dev/sdb 146778685440 0x0
```

c. Specify which disk or disks to use for the cache.

```
Enter number to add item, press 'F' when finished:
[F] >1
Item '1' is selected
[F] >
```

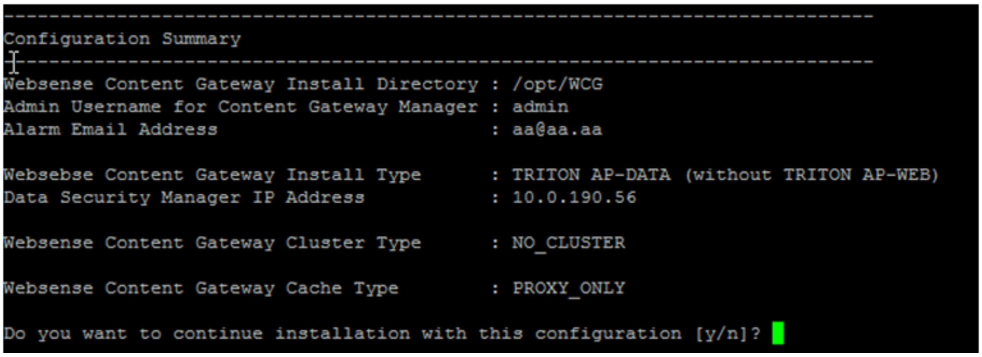
d. Your selections are confirmed. Note the “x” before the name of the disk.

```
Here is the current selection
[X] (1) /dev/sdb 146778685440 0x0
```

e. Continue based on your choice in Step b, pressing **X** when you have finished configuring cache disks.

```
Choose one of the following options:
'A'    - Add disk(s) to cache
'R'    - Remove disk(s) from cache
'S'    - Add all available disks to cache
'U'    - Remove all disks from cache
'X'    - Done with selection, continue Forcepoint
         Content Gateway installation.
Option: >X
```

15. A configuration summary appears, showing your answers to the installer prompts (note: summary below is an example):



```
------------------------------------------------------------------------------
Configuration Summary
------------------------------------------------------------------------------
Websense Content Gateway Install Directory : /opt/WCG
Admin Username for Content Gateway Manager : admin
Alarm Email Address                        : aa@aa.aa

Websebse Content Gateway Install Type      : TRITON AP-DATA (without TRITON AP-WEB)
Data Security Manager IP Address           : 10.0.190.56

Websense Content Gateway Cluster Type      : NO_CLUSTER

Websense Content Gateway Cache Type        : PROXY_ONLY

Do you want to continue installation with this configuration [y/n]?
```

If you want to make changes, enter **n** to restart the installation process at the first prompt. To continue and install Content Gateway configured as shown, enter **y**.

Important

If you enter **y** to proceed but you decide you want to cancel the installation, do not attempt to quit the installer by pressing Ctrl-C. Allow the installation to complete. Then uninstall it.

16. Wait for the installation to complete.
17. When installation is complete, reboot the Content Gateway server.
18. When the reboot is complete, check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include Content Cop, Content Gateway, and Content Gateway Manager.

Installer gives NetworkManager or avahi-daemon error

When Red Hat Enterprise Linux 6 is installed with a GUI, the Content Gateway installer recognizes systems running NetworkManager or avahi-daemon processes and emits an error similar to:

```
Error: The avahi-daemon service is enabled on this system
and must be disabled before Forcepoint Content Gateway
v8.3.x can be installed.

Please disable the avahi-daemon service with the following
commands and restart the Forcepoint Content Gateway
installation.

    chkconfig --levels 2345 avahi-daemon off

    service avahi-daemon stop
```

To continue, the conflicting NetworkManager and avahi-daemon processes must be stopped.

1. To disable the avahi-daemon service:

    ```
    chkconfig --levels 2345 avahi-daemon off

    service avahi-daemon stop
    ```

2. To restart the installer:

    ```
    ./wcg_install.sh
    ```

Configuring Web Content Gateway

After you’ve installed Content Gateway, do the following to configure it.

Enter subscription key

Open the Content Gateway Manager, navigate to **Configure** > **Subscription**, and enter your subscription key. Restart the Content Gateway machine by navigating to **Configure** > **My Proxy** > **Basic** > **Restart**.

Register Content Gateway with TRITON AP-DATA

Content Gateway must be registered with the TRITON management server to operate. Before registering it:

- Synchronize the date and time on the Content Gateway and TRITON management server machines to within a few minutes.

- If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface (“C” on a V-Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
- Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). This is the NIC used by the TRITON management server during the registration process.

  After registration, the IP address can move to another network interface.
- Verify connectivity between Content Gateway and the TRITON management server.

To register Content Gateway, open Content Gateway Manager:

1. On the **Configure** > **My Proxy** > **Basic** > **General** page, in the **Networking** section confirm that **Web DLP** > **Integrated on-box** is enabled.
2. Restart Content Gateway as prompted.
3. Go to **Configure** > **Security** > **Web DLP** and enter the IP address of the management server.
4. Enter a user name and password for a Data module administrator with Deploy Settings privileges.
5. Click **Register**.
6. Restart Content Gateway again by navigating to **Configure** > **My Proxy** > **Basic** > **Restart**.

After Content Gateway has registered with TRITON AP-DATA, in Content Gateway Manager go to **Configure** > **Security** > **Web DLP** and set the following options:

1. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Web DLP components for analysis and policy enforcement.
2. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Web DLP components for analysis and policy enforcement. SSL Manager must be enabled on Content Gateway.
3. Click **Apply** and restart Content Gateway.

Configure the Content Gateway policy engine

When Content Gateway is registered with the TRITON management server, a Content Gateway module appears on the System Modules page of the Data Security manager.

By default, this agent is configured to monitor web traffic, not block it, and for a default violation message to appear when an incident is triggered. If this is acceptable, you do not need to make changes to the Content Gateway configuration. Simply deploy the new settings.

If you want to block web traffic that breaches policy and customize the violation message, do the following:

1. In the Data Security manager, go to the **Settings** > **Deployment** > **System Modules** page.
2. Select the Web Content Gateway module in the tree view (click the module name itself, not the plus sign next to it).

   It will be listed as **AP-WEB Server on** <FQDN> (<PE_version>), where <*FQDN*> is the fully-qualified domain name of the Content Gateway machine and <*PE_version*> is the version of the Content Gateway policy engine.
3. Select the **HTTP/HTTPS** tab and configure the blocking behavior you want.

   Select **Help** > **Explain This Page** for instructions for each option.
4. Select the **FTP** tab and configure the blocking behavior you want.

   Select **Help** > **Explain This Page** for instructions for each option.
5. Click **Save** to save your changes.
6. Click **Deploy** to deploy your settings.

> **Important**
>
> Even if you do not change the default configuration, you must click **Deploy** to finalize your Content Gateway deployment process.

Set Up Content Gateway

- Log on to Content Gateway Manager and run a basic test (Getting Started)
- If there are multiple instances of Content Gateway, consider configuring a managed cluster.
- Configure protocols to proxy in addition to HTTP: HTTP (SSL Manager), FTP
- Complete your explicit or transparent proxy deployment
  - Content Gateway explicit and transparent proxy deployments
  - In Content Gateway Manager Help: Explicit proxy, Transparent proxy
- If proxy user authentication will be used, configure user authentication.
- If you enabled content caching during installation, configure content caching.

After the base configuration has been tested, consider these additional activities:

- In explicit proxy deployments, customize the PAC file
- In transparent proxy deployments, use ARM dynamic and static bypass, or use router ACL lists to bypass Content Gateway (see your router documentation).

Email Gateway for Office 365

Email Gateway for Office 365 is a virtual appliance that, when deployed in a Microsoft Azure environment, allows outbound email from Exchange Online to be analyzed for data loss or theft. Email containing sensitive data can be permitted, quarantined, or encrypted. Sensitive attachments can also be dropped.

Email Gateway is hybrid component of TRITON AP-DATA that enables analysis of email in cloud platforms with management performed on-premises. It is part of the network email channel.

Email Gateway analyzes only outbound traffic, regardless of whether you select Inbound or Internal on the destination page of your policy. It does not support OCR analysis.

Please note that you cannot manage both TRITON AP-EMAIL and Email Gateway for Office 365 components on the same TRITON management server.

However, you can scan local Exchange email or inbound Exchange Online email using the on-premises protector appliance and also use the Email Gateway virtual appliance to scan outbound email from Exchange Online.

Email Gateway for Office 365 can be deployed in 2 ways:

1. Relaying through Exchange Online

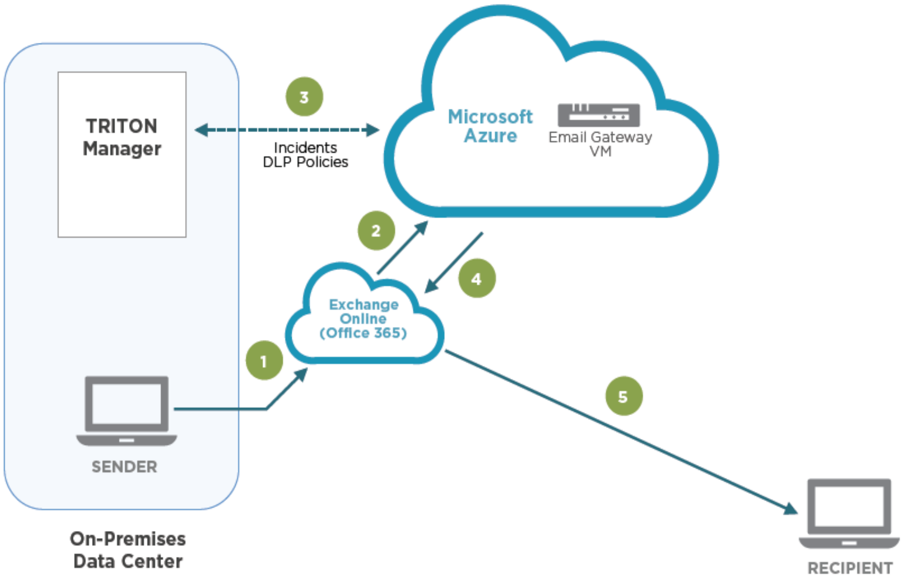


Figure 1 Routing DLP scanned email through Exchange Online

2. Between the sender and the Forcepoint cloud service, where malicious content scanning can be performed before the messages reaches the recipient. (Requires a subscription to Forcepoint TRITON AP-EMAIL Cloud)

Routing traffic through the cloud service removes the risk of your Microsoft Azure account being blocked when outbound email traffic is blacklisted.

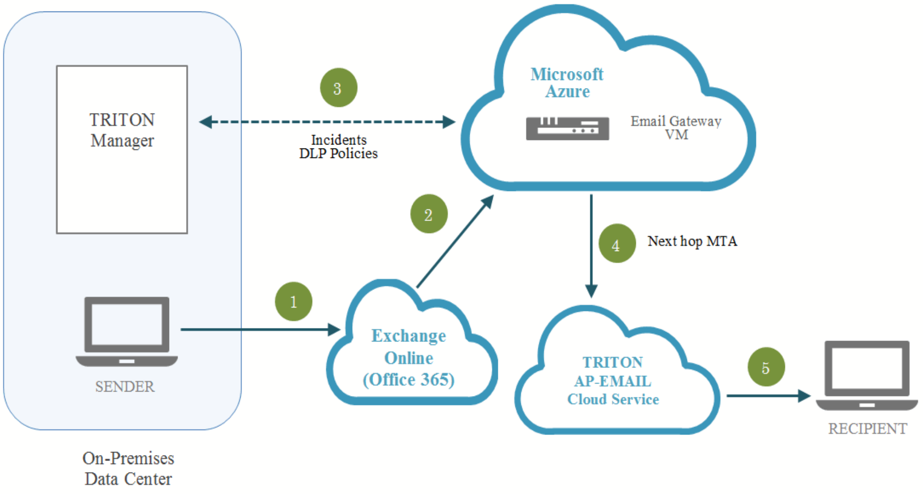


Figure 2 Routing DLP scanned email through a email gateway security service

Requirements

- A Microsoft Azure account (activated)
- An Azure VM with at least 4 cores and 7 GB of memory (A3 standard)
- A Windows Server 2008 or Windows Server 2012 machine that conforms to the management server requirements listed *here*
- A SQL Server database machine for configuration data
- Microsoft Exchange Online
- Azure PowerShell v1.5.0
- Windows PowerShell v3.0

Deployment steps

Do the following to deploy Email Gateway for Office 365 in Azure:

1. *Create a virtual network and VPN in Azure*
2. *Deploy Email Gateway for Office 365 from the Azure Marketplace*
3. *Configure the Email Gateway VM*
4. *Install TRITON management components for the virtual appliance*
5. *Configure the appliance in the TRITON Manager*
6. *Configure mail flow in Exchange Online*

For a high-level view of the procedure, see the Email Gateway setup poster.

Create a virtual network and VPN in Azure

To create virtual and virtual private networks in the Azure cloud, do the following:

1. Create a a self-signed root certificate for a point-to-site network. Instructions are provided here:

   https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-certificates-point-to-site/

   Locate the Base64 value of the root certificate file. For example:

```
-----BEGIN CERTIFICATE-----
MIIBuTCCASKgAwIBAgIQNdNhtuV5GbNHYZsf+LvM0zANBgkqhkiG9w0BA
QUFADAbMRkwFwYDVQQDExBFZGlkZXYgU21va2VUZXN0MB4XDTA4MTExMj
E5NTEzNVoXDTM5MTIzMTIzNTk1OVowGzEZMBcGA1UEAxMQRWRpZGV2IFN
tb2tlVGVzdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAm6zGzqxe
jwswWTNLcSsa7P8xqODspX9VQBuq5W1RoTgQ0LNR64+7ywLjH8+wrb/
lB6QV7s2SFUiWDeduVesvMJkWtZ5zzQyl3iUaCBpT4S5AaO3/
wkYQSKdI108pXH7Aue0e/ZOwgEEX1N6OaPQn7AmAB4uq1h+ffw+r
RKNHqnsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQCZmj+pgRsN6HpoICawK
3XXNAmicgfQkailX9akIjD3xSCwEQx4nG6tZjTz30u4NoSffW7pch58Sx
uZQDqW5NsJcQNqNgo/dMoqqpXdi2YEcJ8pjsngrFm+fM2BnyGpXH7aWuK
8wFJt2Z/XGA7WWDjvw==
-----END CERTIFICATE-----
```

2. On a Windows server, download a PowerShell script called **pre-deploy.ps1** from the Forcepoint download center. Visit My Account, select **Forcepoint TRITON AP-DATA Gateway** > **Version 8.3** > **Email Gateway for Office 365**.
3. Install Azure PowerShell v1.5.0. Refer to Microsoft documentation for instructions.
4. In a text editor, open the script and modify the following 3 parameters:

```
$SubscriptionId = "<The subscription ID for your
Microsoft Azure pay-as-you-go account>" (Enter Get-
AzureRmSubscription to find your ID.)


$MyP2SRootCertPubKeyBase64 = "<The Base64 value of your
root certificate from step 1>" (Do not include the BEGIN
or END comments.)


$Location = "<The Azure region closest to you. E.g., East
US>"
```

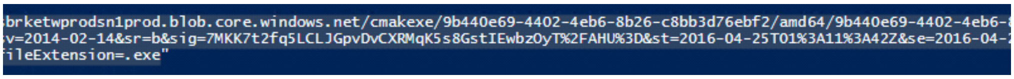
   Possible Azure regions can be found at https://azure.microsoft.com/en-us/regions.

5. Open the Azure PowerShell console.
6. Change the PowerShell Script Execution Policy from **Restricted** to **RemoteSigned** so that local PowerShell scripts can be run. To do so, enter:

```
Set-ExecutionPolicy RemoteSigned
```

7. Run the script that you edited in step 2, **pre-deploy.ps1**. It can take more than 10 minutes. Run this script only once. Running it again overwrites your settings.

8. Locate the URL in the output, as shown in the following picture:.



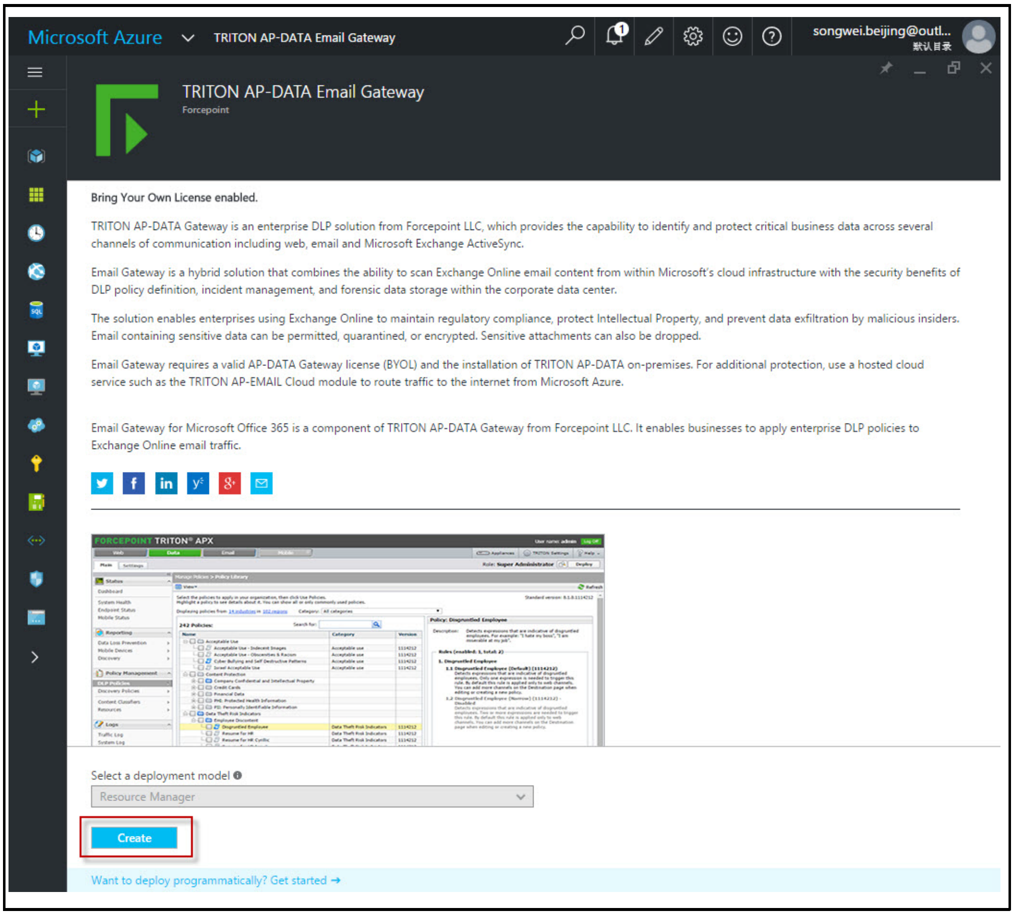
```
brketwprodsn1prod.blob.core.windows.net/cmakexe/9b440e69-4402-4eb6-8b26-c8bb3d76ebf2/amd64/9b440e69-4402-4eb6-
v=2014-02-14&sr=b&sig=7MKK7t2fq5LCLJGpvDvCXRMqK5s8GstIEwbzOyT%2FAHU%3D&st=2016-04-25T01%3A11%3A42Z&se=2016-04-
ileExtension=.exe"
```

9. Visit the URL website, download the VPN Client, and install it in your environment. If you have another Windows machine to add to the VPN network, install the VPN client on that machine by using the same URL.

✓ The VPN client URL expires in 1 hour, so make sure to download the VPN client software in that time.

Deploy Email Gateway for Office 365 from the Azure Marketplace

1. Log on to the Azure Marketplace, https://portal.azure.com/, select **Browse**, and then click **Marketplace**.
2. Search for and select **Email Gateway for Office 365**.



TRITON AP-DATA Email Gateway

Forcepoint

Bring Your Own License enabled.

TRITON AP-DATA Gateway is an enterprise DLP solution from Forcepoint LLC, which provides the capability to identify and protect critical business data across several channels of communication including web, email and Microsoft Exchange ActiveSync.

Email Gateway is a hybrid solution that combines the ability to scan Exchange Online email content from within Microsoft's cloud infrastructure with the security benefits of DLP policy definition, incident management, and forensic data storage within the corporate data center.

The solution enables enterprises using Exchange Online to maintain regulatory compliance, protect Intellectual Property, and prevent data exfiltration by malicious insiders. Email containing sensitive data can be permitted, quarantined, or encrypted. Sensitive attachments can also be dropped.

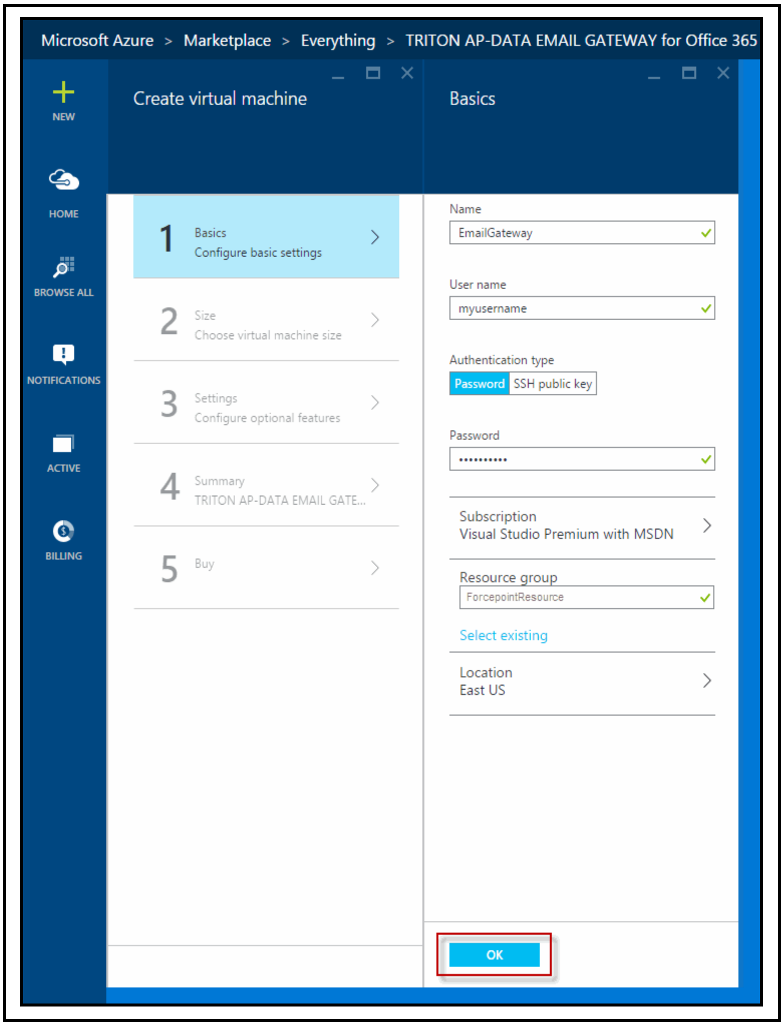
Email Gateway requires a valid AP-DATA Gateway license (BYOL) and the installation of TRITON AP-DATA on-premises. For additional protection, use a hosted cloud service such as the TRITON AP-EMAIL Cloud module to route traffic to the internet from Microsoft Azure.

Email Gateway for Microsoft Office 365 is a component of TRITON AP-DATA Gateway from Forcepoint LLC. It enables businesses to apply enterprise DLP policies to Exchange Online email traffic.

Select a deployment model: Resource Manager

3. Click **Create** to create a virtual appliance.

4. Under **Basics**, enter a name for the VM as well as a user name and password for connecting to the VM host. Select the resource group, **ForcepointResource**. A resource group is a container that holds related resources for an application. It will hold the Email Gateway VM. For location, select the value you used when editing the **pre-deploy.ps1** script, then choose either a solid state (SSD) or hard disk (HDD) drive. Click **OK** when done.


Microsoft Azure > Marketplace > Everything > TRITON AP-DATA EMAIL GATEWAY for Office 365
NEW
HOME
BROWSE ALL
NOTIFICATIONS
ACTIVE
BILLING
Create virtual machine
1 Basics Configure basic settings
2 Size Choose virtual machine size
3 Settings Configure optional features
4 Summary TRITON AP-DATA EMAIL GATE...
5 Buy
Basics
OK

Name: EmailGateway

User name: myusername

Authentication type: Password | SSH public key

Password: ••••••••••

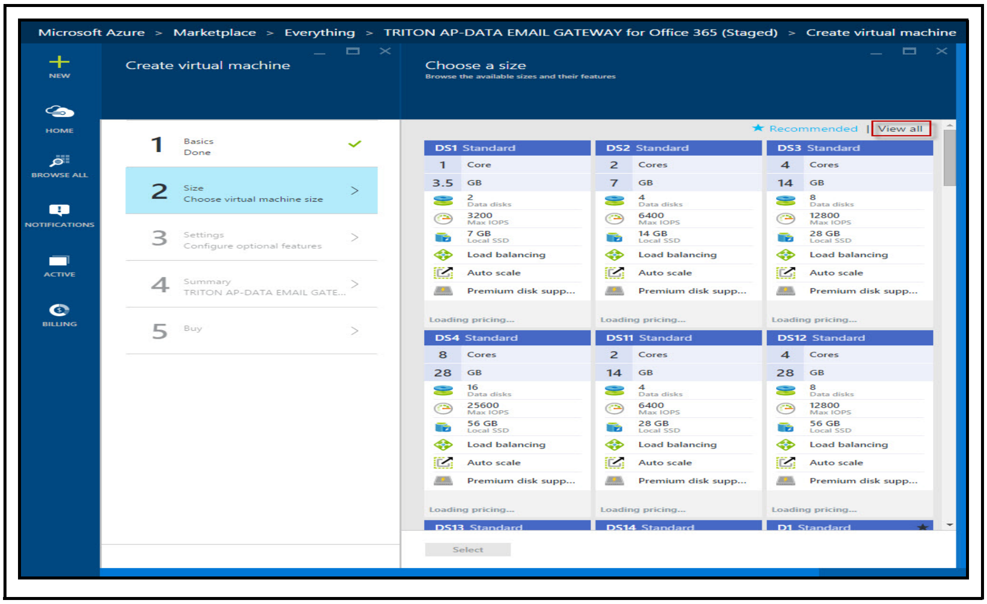
Subscription: Visual Studio Premium with MSDN

Resource group: ForcepointResource

Select existing

Location: East US

5. Under **Size**, select the size of the VM you will need based on anticipated email volume, then click **Select**. For enterprise use, it is best practice to select a minimum of 4 cores and 7 GB of memory (A3 Standard). Click **View all** to locate a size suited to your needs.


Microsoft Azure > Marketplace > Everything > TRITON AP-DATA EMAIL GATEWAY for Office 365 (Staged) > Create virtual machine
NEW
HOME
BROWSE ALL
NOTIFICATIONS
ACTIVE
BILLING
Create virtual machine
1 Basics Done
2 Size Choose virtual machine size
3 Settings Configure optional features
4 Summary TRITON AP-DATA EMAIL GATE...
5 Buy
Choose a size
Browse the available sizes and their features
★ Recommended | View all
Select

DS1 Standard	DS2 Standard	DS3 Standard
1 Core	2 Cores	4 Cores
3.5 GB	7 GB	14 GB
2 Data disks	4 Data disks	8 Data disks
3200 Max IOPS	6400 Max IOPS	12800 Max IOPS
7 GB Local SSD	14 GB Local SSD	28 GB Local SSD
Load balancing	Load balancing	Load balancing
Auto scale	Auto scale	Auto scale
Premium disk supp...	Premium disk supp...	Premium disk supp...
Loading pricing...	Loading pricing...	Loading pricing...

DS4 Standard	DS11 Standard	DS12 Standard
8 Cores	2 Cores	4 Cores
28 GB	14 GB	28 GB
16 Data disks	4 Data disks	8 Data disks
25600 Max IOPS	6400 Max IOPS	12800 Max IOPS
56 GB Local SSD	28 GB Local SSD	56 GB Local SSD
Load balancing	Load balancing	Load balancing
Auto scale	Auto scale	Auto scale
Premium disk supp...	Premium disk supp...	Premium disk supp...
Loading pricing...	Loading pricing...	Loading pricing...

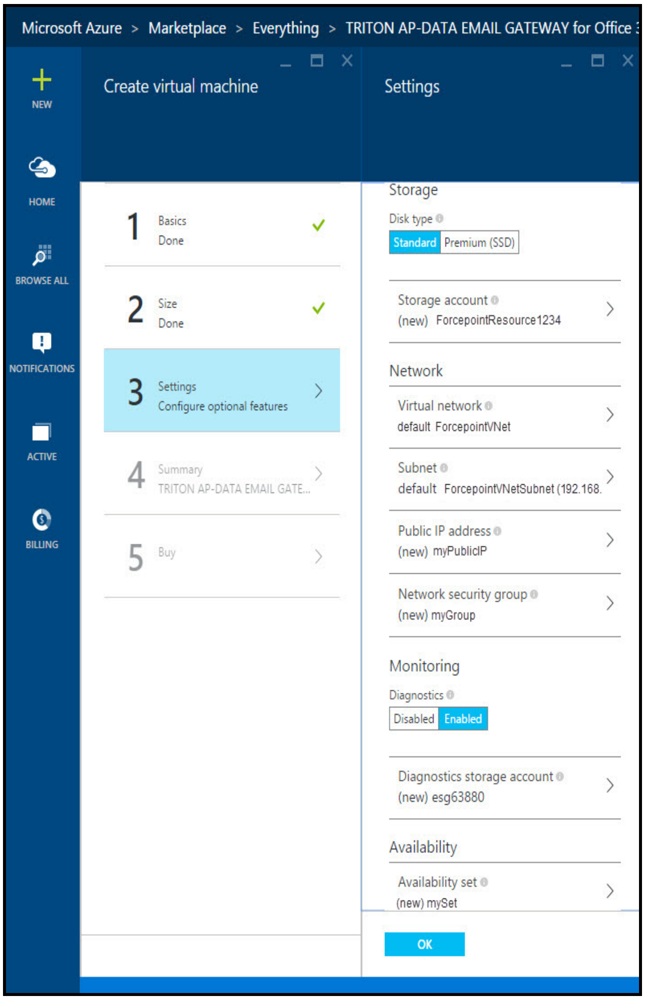
DS13 Standard	DS14 Standard	D1 Standard ★

6. Under **Settings**, select the storage account and disk type that you want for the VM. If you do not have a storage account, create one by clicking **Storage Account** and then clicking **Add**.

   Under **Network**, select the virtual network and subnet listed in the **pre-deploy.ps1** file, **ForcepointVNet** and **ForcepointVNetSubnet** by default.

   Also select a public IP address and security group for the network. The name you enter for public IP will be used for the FQDN—for example,

<name>.cloudapp.net. Enter diagnostics and availability settings, then click **OK**. If necessary, create a new availability set.


Microsoft Azure > Marketplace > Everything > TRITON AP-DATA EMAIL GATEWAY for Office 3
NEW
HOME
BROWSE ALL
NOTIFICATIONS
ACTIVE
BILLING
Create virtual machine
Settings
OK

Create virtual machine

1 Basics
Done ✓

2 Size
Done ✓

3 Settings
Configure optional features

4 Summary
TRITON AP-DATA EMAIL GATE...

5 Buy

Settings

Storage

Disk type: [✓ Standard] Premium (SSD)

Storage account: (new) ForcepointResource1234

Network

Virtual network: default ForcepointVNet

Subnet: default ForcepointVNetSubnet (192.168.

Public IP address: (new) myPublicIP

Network security group: (new) myGroup

Monitoring

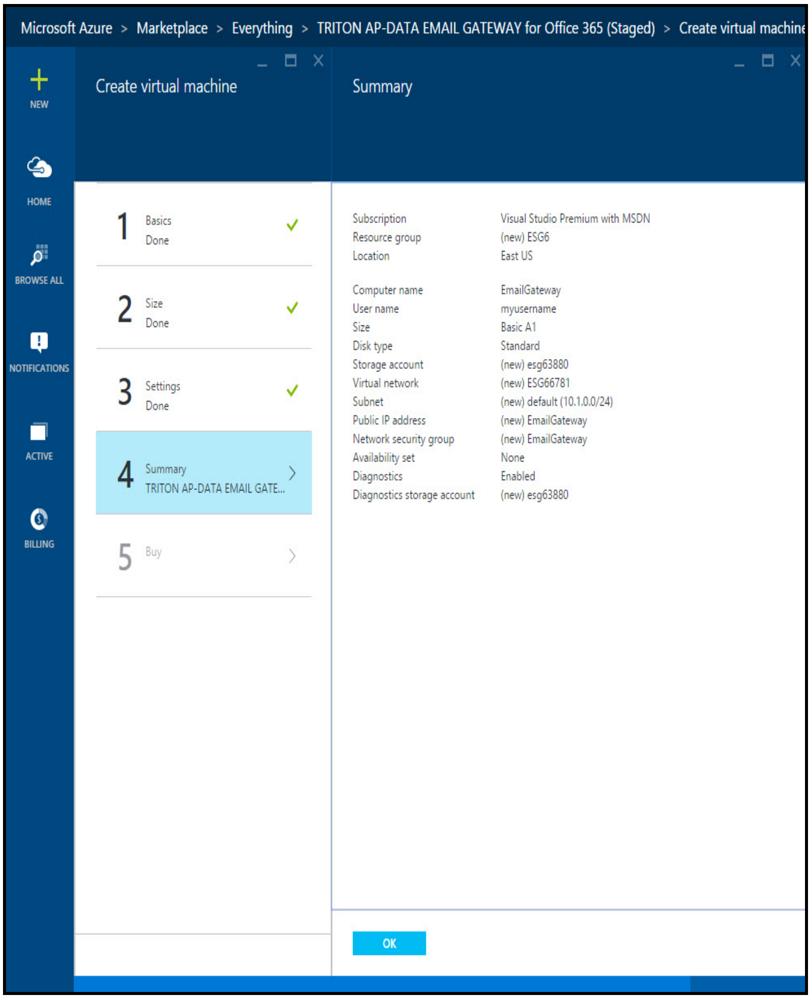
Diagnostics: Disabled [✓ Enabled]

Diagnostics storage account: (new) esg63880

Availability

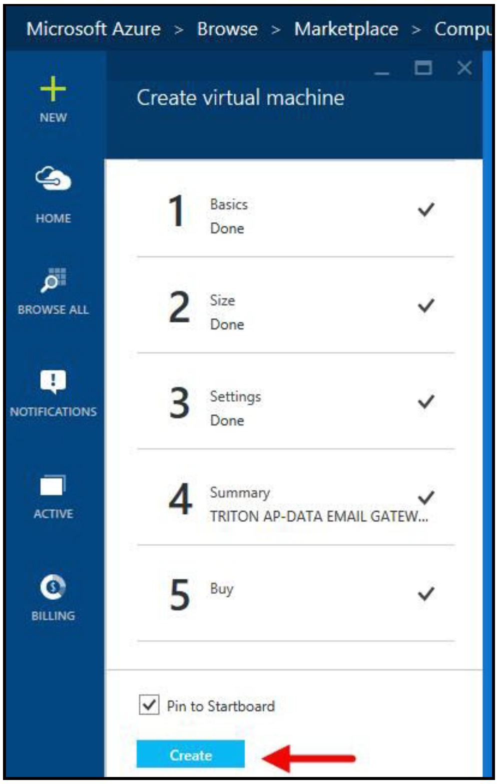
Availability set: (new) mySet

7. Under **Summary**, review a summary of the VM you are building, then click **OK**.


Microsoft Azure > Marketplace > Everything > TRITON AP-DATA EMAIL GATEWAY for Office 365 (Staged) > Create virtual machine
NEW
HOME
BROWSE ALL
NOTIFICATIONS
ACTIVE
BILLING
Create virtual machine
1 Basics Done
2 Size Done
3 Settings Done
4 Summary TRITON AP-DATA EMAIL GATE...
5 Buy
Summary
OK

Subscription	Visual Studio Premium with MSDN
Resource group	(new) ESG6
Location	East US
Computer name	EmailGateway
User name	myusername
Size	Basic A1
Disk type	Standard
Storage account	(new) esg63880
Virtual network	(new) ESG66781
Subnet	(new) default (10.1.0.0/24)
Public IP address	(new) EmailGateway
Network security group	(new) EmailGateway
Availability set	None
Diagnostics	Enabled
Diagnostics storage account	(new) esg63880

8. Click **Purchase** to create the VM in the Azure cloud infrastructure. Since Email Gateway for Office 365 is a bring-your-own license VM, there is no Azure Marketplace charge.



Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Done ✓

4 Summary TRITON AP-DATA EMAIL GATEW... ✓

5 Buy ✓

☑ Pin to Startboard

9. The system reports that it is creating the VM in the network you specified.

Scalability and load balancing

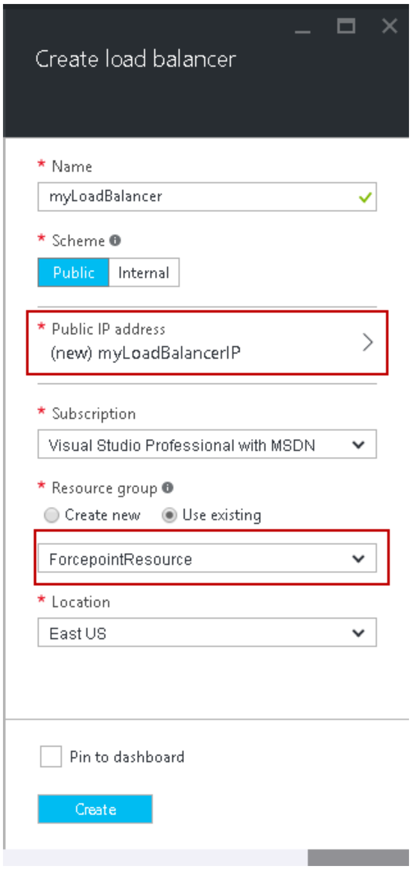
Depending on your traffic volume and number of mailboxes, you may want to have multiple Email Gateway virtual machines running in the Azure cloud.

All VMs should be connected to the same Forcepoint management server. Because clustering is not supported by Azure, you must configure each VM separately.

To distribute traffic between VMs, use Azure's Load Balancer as shown below. You cannot distribute the load between policy engines in the Data Security manager at this time.

1. Search for and select **Load Balancer** in the Azure Marketplace.
2. Click **Add+**.

3. Enter a name, a public IP address, and subscription for the load balancer. Select the same resource group, **ForcepointResource**, and location you used for the VM, then click **Create**.



Create load balancer

* Name
myLoadBalancer ✓

* Scheme
[✓ Public] Internal

* Public IP address
(new) myLoadBalancerIP

* Subscription
Visual Studio Professional with MSDN

* Resource group
○ Create new ● Use existing
ForcepointResource

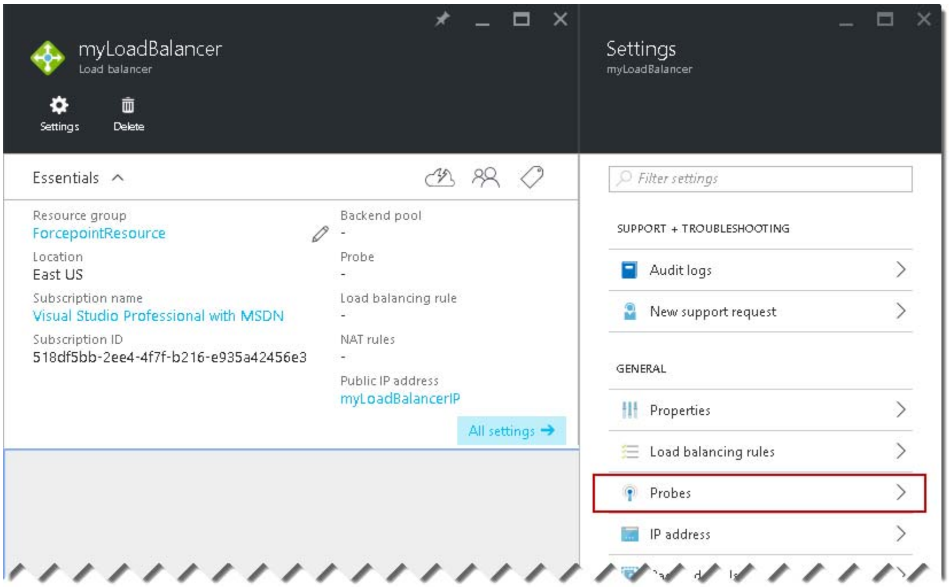
* Location
East US

□ Pin to dashboard

4. After load balancer is created, modify the following settings.

   a. Select the load balancer from your resource group.

b. Under Settings, click **Health Probes** and then click **+Add**.



Resource group
ForcepointResource

Location
East US

Subscription name
Visual Studio Professional with MSDN

Subscription ID
518df5bb-2ee4-4f7f-b216-e935a42456e3

Backend pool
-

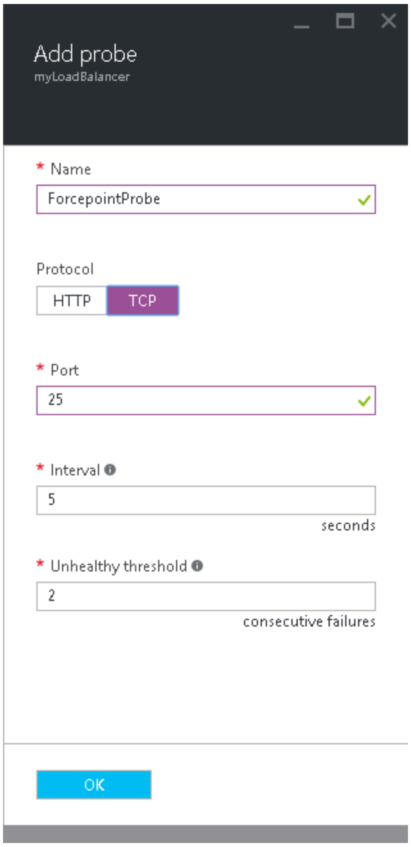
Probe
-

Load balancing rule
-

NAT rules
-

Public IP address
myLoadBalancerIP

c. Enter a name such as ForcepointProbe, then select the protocol TCP and the port 25. and click **OK**. The probe monitors the status of your VMs.



* Name
ForcepointProbe

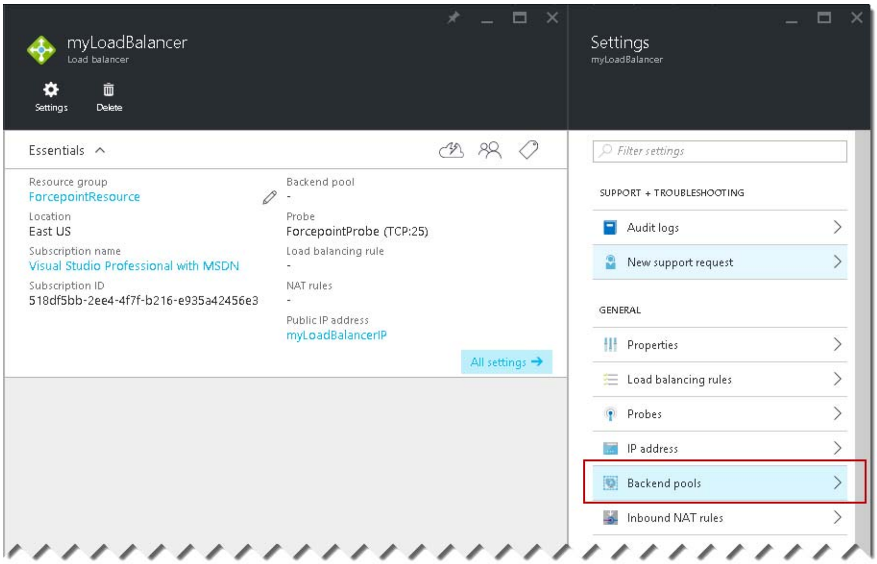
Protocol
TCP

* Port
25

* Interval
5
seconds

* Unhealthy threshold
2
consecutive failures

d. Under Settings, now click **Backend Pools**, then **+Add**.



Resource group
ForcepointResource

Location
East US

Subscription name
Visual Studio Professional with MSDN

Subscription ID
518df5bb-2ee4-4f7f-b216-e935a42456e3

Backend pool
-

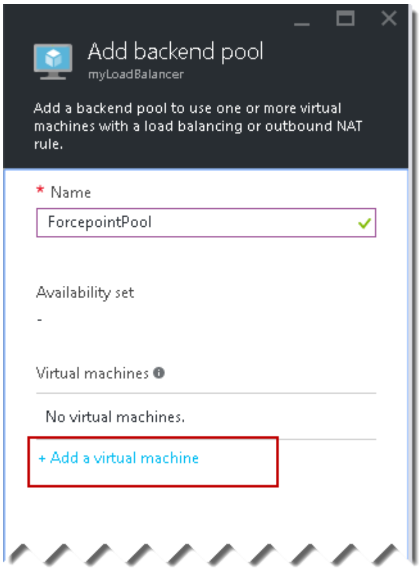
Probe
ForcepointProbe (TCP:25)

Load balancing rule
-

NAT rules
-

Public IP address
myLoadBalancerIP

e. Enter a name for the load balancer backend pool, then click **Add a virtual machine**.



Add a backend pool to use one or more virtual machines with a load balancing or outbound NAT rule.

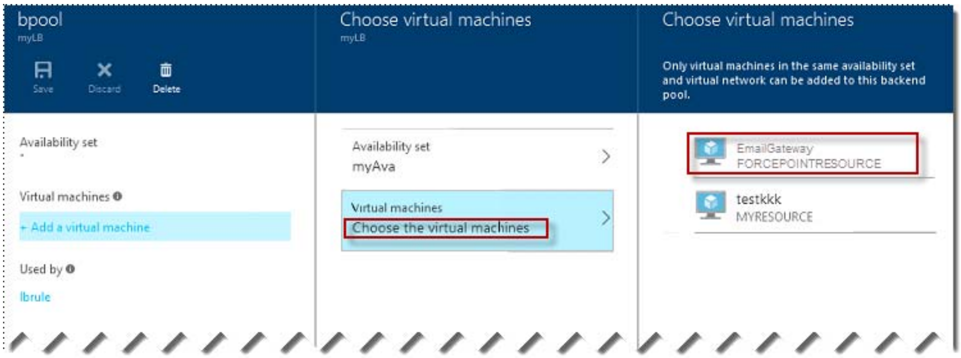
* Name
ForcepointPool ✓

Availability set
-

Virtual machines

No virtual machines.

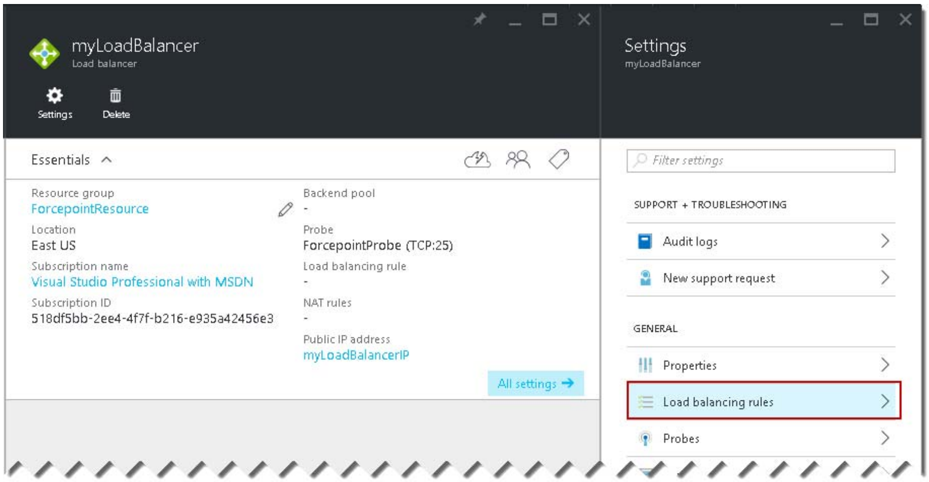
f. Choose the availability set that you used for the VM, and then click **Choose the virtual machines** and select the virtual machines that you need to add in the pool. Click **OK**.



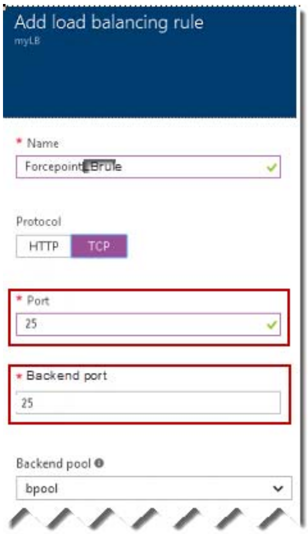
Note

If you want to add more virtual appliances after the load balancer is created, modify the backend pools configuration and select the new virtual appliance.

g. Under **Settings**, select **Load balancing rules** and then click **+Add**.



h. Select the protocol TCP, the front-end port 25, and the back-end port 25. and click **OK**.



Add load balancing rule
myLB

* Name
ForcepointLBrule

Protocol
HTTP TCP

* Port
25

* Backend port
25

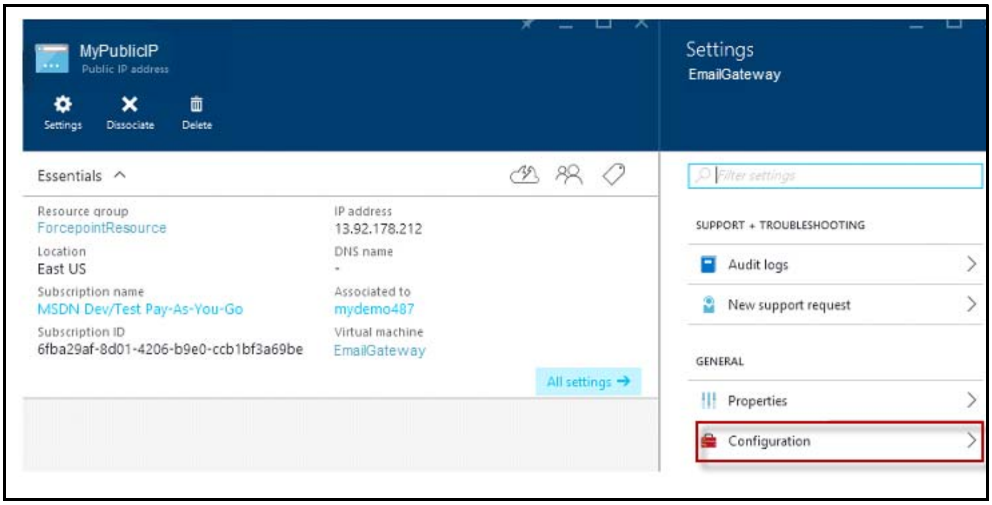
Backend pool
bpool

Post-configuration

1. Add a DNS name for **All Public IP addresses**.

   a. Select the public IP address for your Email Gateway VM.

   b. Click **Configuration**.



MyPublicIP
Public IP address

Essentials

Resource group
ForcepointResource

Location
East US

Subscription name
MSDN Dev/Test Pay-As-You-Go

Subscription ID
6fba29af-8d01-4206-b9e0-ccb1bf3a69be

IP address
13.92.178.212

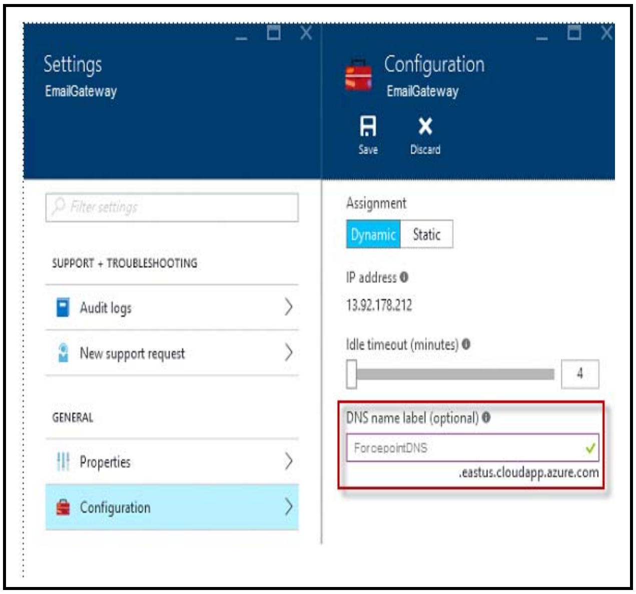
DNS name
-

Associated to
mydemo487

Virtual machine
EmailGateway

Settings
EmailGateway

c. Enter the DNS name for Office 365.



Assignment: Dynamic | Static

IP address: 13.92.178.212

Idle timeout (minutes): 4

DNS name label (optional): ForcepointDNS .eastus.cloudapp.azure.com

Configure the Email Gateway VM

After you deploy the Email Gateway VM in Azure, it goes through an initialization process. Wait at least 15 minutes before configuring the VM.

1. Log on to the Email Gateway VM as root user.

   a. Log on to the VM as described in *Logging onto the virtual machine*, page 89.

   b. SSH to the email module using the default password.

   ```
   ssh root@esg
   Password: websense#123
   ```

   c. Change the root user password. (Type **passwd root** and enter a password when prompted.)

2. Configure the timezone on your virtual appliance by doing the following.

   a. Enter:

   ```
   rm -rf /etc/localtime
   ```

   b. Locate your timezone under **/usr/share/zoneinfo** and then link it using the **ln** command. For example:

   ```
   ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
   ```

3. Check the service status. If the service has started, the status should be “30”.

   ```
   ps aux | grep /usr/local/sbin/ | wc -l
   ```

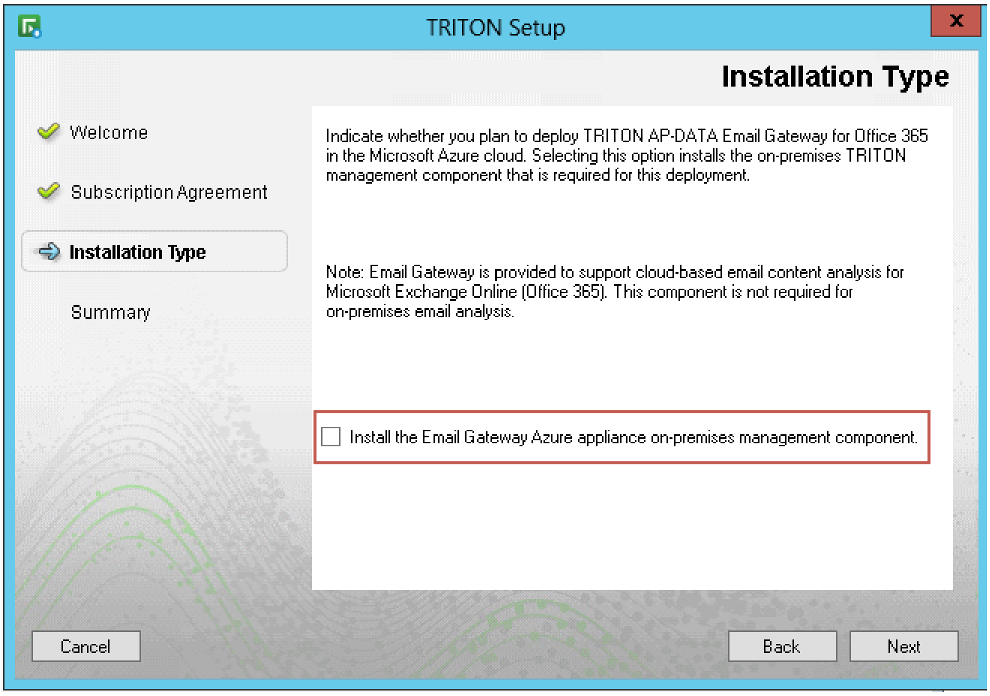
4. Close SSH port 22 on your endpoints for security purposes. Open SMTP port 25 so you can send email through the VM. This is done from the Azure portal as shown in step 11 above.

Install TRITON management components for the virtual appliance

1. Follow the instructions for installing Forcepoint DLP on the management server in Chapter 1 of this guide.

> **Note**
>
> If you have already installed Forcepoint DLP v8.3 or if you are upgrading to v8.3 from an earlier version, run the installer and use the Modify Installation page to install Email Gateway for Office 365. Next to TRITON AP-EMAIL, click **Install**, and then select **TRITON AP-DATA Email Gateway** on a subsequent screen.

2. After selecting the TRITON AP-DATA component, you are asked whether you want to deploy Email Gateway in the Microsoft Azure cloud. Select **Install Email Gateway Azure appliance on-premises management component**.



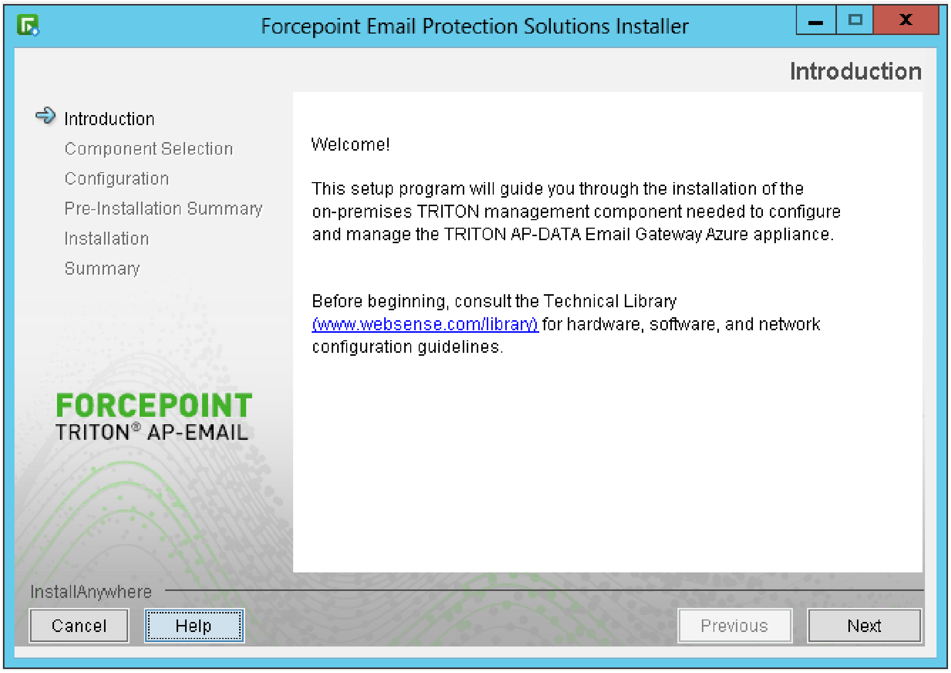
Indicate whether you plan to deploy TRITON AP-DATA Email Gateway for Office 365 in the Microsoft Azure cloud. Selecting this option installs the on-premises TRITON management component that is required for this deployment.

Note: Email Gateway is provided to support cloud-based email content analysis for Microsoft Exchange Online (Office 365). This component is not required for on-premises email analysis.

□ Install the Email Gateway Azure appliance on-premises management component.

3. Complete the TRITON AP-DATA installation as described in Chapter 1.
4. The Email Gateway installer launches automatically. Use this installer to install the necessary email components on the manager. On the remaining screens, enter only IP addresses from the Azure network. Don't enter the IPs of any on-premises components.

5. Click **Next** on the Welcome screen.



Forcepoint Email Protection Solutions Installer

Introduction

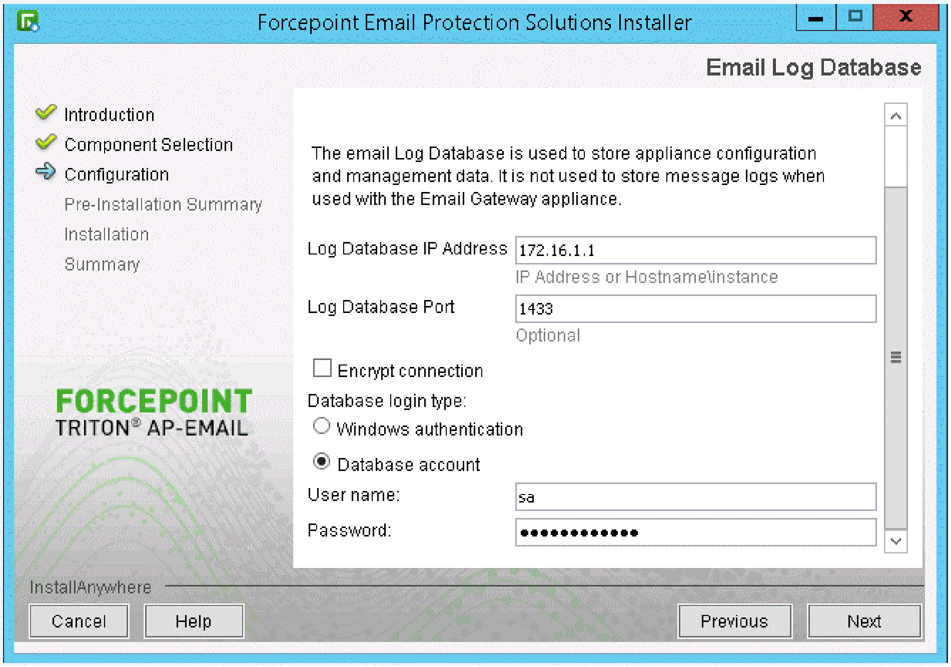
Welcome!

This setup program will guide you through the installation of the on-premises TRITON management component needed to configure and manage the TRITON AP-DATA Email Gateway Azure appliance.

Before beginning, consult the Technical Library (www.websense.com/library) for hardware, software, and network configuration guidelines.

6. Enter the IP address and port of the SQL database to use for storing management data. This is the VPN client IP assigned to the remote database when you added it to your Azure VPN network.

   Include the username and password for the database account.



Forcepoint Email Protection Solutions Installer

Email Log Database

The email Log Database is used to store appliance configuration and management data. It is not used to store message logs when used with the Email Gateway appliance.

Log Database IP Address: 172.16.1.1
IP Address or Hostname\instance

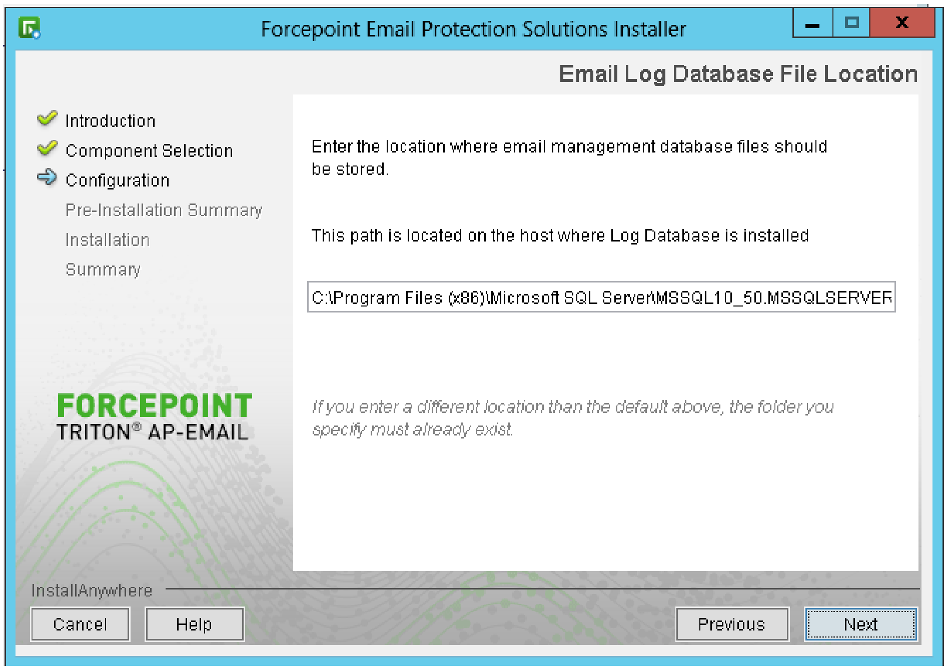
Log Database Port: 1433
Optional

□ Encrypt connection

Database login type:
○ Windows authentication
● Database account

User name: sa
Password: ●●●●●●●●●●●●●

7. Enter a location for the database files or accept the default value.



Email Log Database File Location

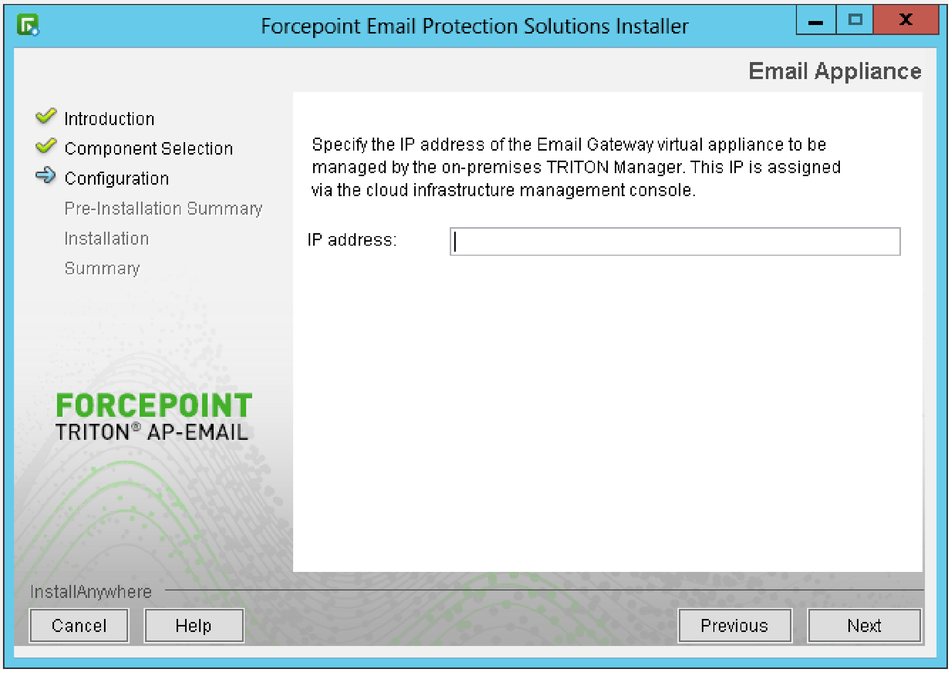
Enter the location where email management database files should be stored.

This path is located on the host where Log Database is installed

C:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER

If you enter a different location than the default above, the folder you specify must already exist.

8. On the Email Appliance page, enter the IP address or host name of the VM you created when deploying the appliance in Azure and then click **Next**.

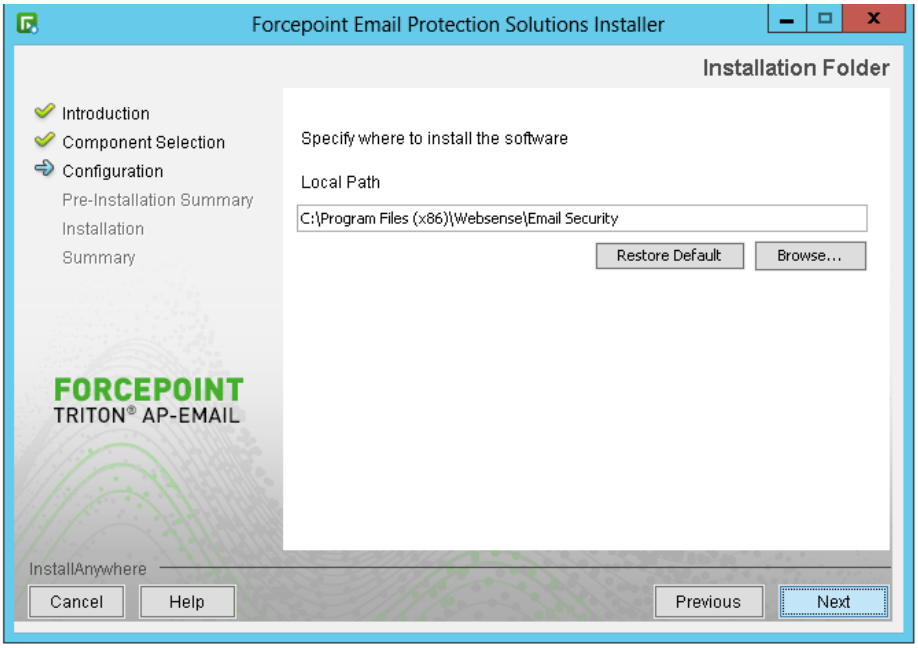


Email Appliance

Specify the IP address of the Email Gateway virtual appliance to be managed by the on-premises TRITON Manager. This IP is assigned via the cloud infrastructure management console.

IP address:

9. Specify where to install the software.

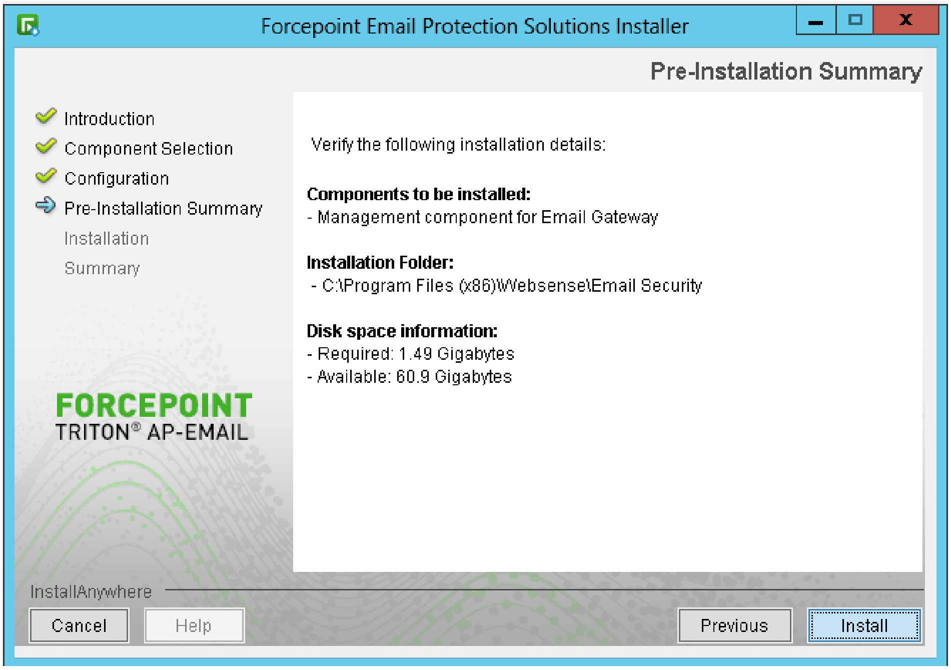


Specify where to install the software

Local Path

C:\Program Files (x86)\Websense\Email Security

10. Click **Install**.



Verify the following installation details:

Components to be installed:
- Management component for Email Gateway

Installation Folder:
- C:\Program Files (x86)\Websense\Email Security

Disk space information:
- Required: 1.49 Gigabytes
- Available: 60.9 Gigabytes

11. Connect the management server to the Azure VPN network by doing the following.

    a. Visit My Account, select **Forcepoint TRITON AP-DATA Gateway > Version 8.3 > Email Gateway VPN Connection Script**.

b. Download the connection script file, **p2s_vpn_connect.ps1**, and place it in the \Email Security\p2s_vpn\ directory where your Forcepoint software is installed—**C:\Program Files (x86)\Websense\Email Security\p2s_vpn** by default. Overwrite the file that is there already.

c. In a text editor on the management server, open the VPN connection script.

d. Edit the following parameters with the values used in the **pre-deploy.ps1** script. This is the script you edited when building the virtual network in Azure. Below are the default values:

   ○ $vpnName - ForcepointVNet (virtual network name)

   ○ $vpnNet - 192.168.0.0 (VPN network IP, server side)

   ○ $vpnNetmask - 255.255.0.0 (VPN subnet mask, server side)

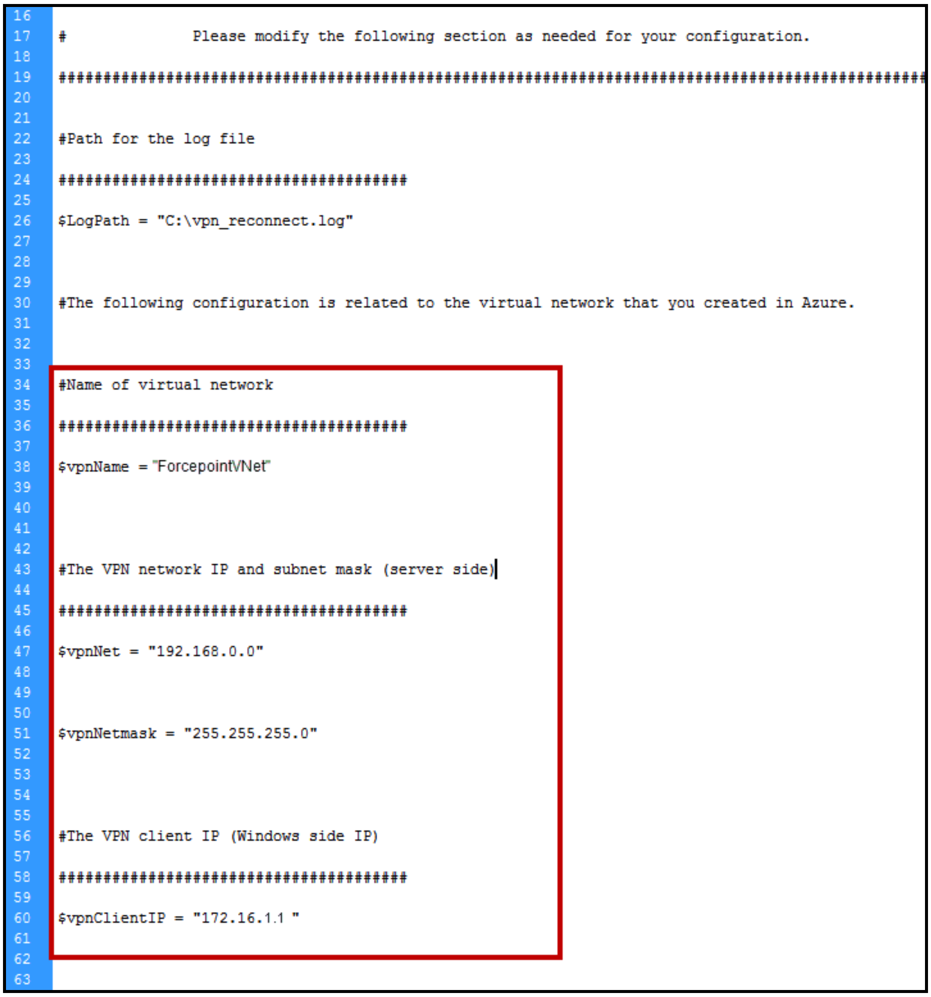
   ○ $vpnClientIP - 172.16.1.1 (VPN client's IP address)

   Each entry should be on a separate line. Entries should be surrounded in quotation marks.

   Use the following format:

   ```
   <parameter> = "<value>"
   ```

   Example:



```

#              Please modify the following section as needed for your configuration.

###################################################################################################


#Path for the log file

########################################

$LogPath = "C:\vpn_reconnect.log"



#The following configuration is related to the virtual network that you created in Azure.



#Name of virtual network

########################################

$vpnName = "ForcepointVNet"




#The VPN network IP and subnet mask (server side)

########################################

$vpnNet = "192.168.0.0"



$vpnNetmask = "255.255.255.0"




#The VPN client IP (Windows side IP)

########################################

$vpnClientIP = "172.16.1.1 "



```

The default log path is c:\vpn_reconnect.log. You can edit this as well if desired.

The default user directory path is C:\Users\Administrator\AppData\Roaming\. The administrator named here must be the same as the one who installed the Azure VPN client. Edit Administrator as needed.

Save the file when done.

e. Change the PowerShell Script Execution Policy from Restricted to RemoteSigned so that local PowerShell scripts can be run. To do so, enter:

```
Set-ExecutionPolicy RemoteSigned
```

f. Run the revised script from PowerShell. This connects the management server to the VPN network and keeps them connected at all times.

Important

If the management server is restarted for any reason, you must re-run this script. For best practice, add the script to the Windows Task Scheduler so that it runs on startup. For instructions, see this knowledgebase article.

g. If your system is using a remote database, copy the script onto the database machine and run it there as well.

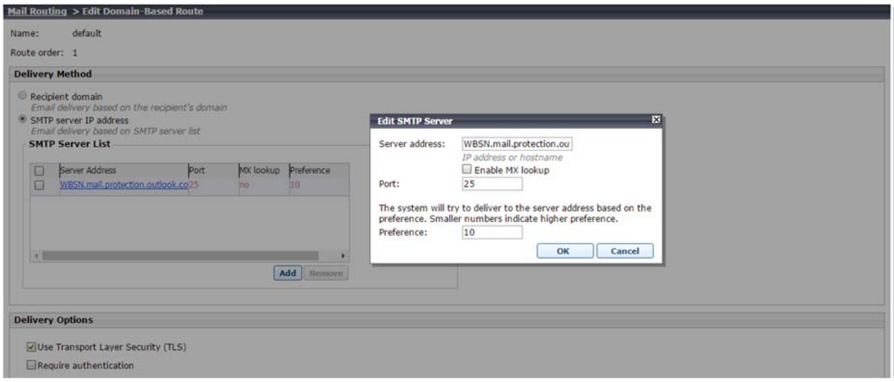
Configure the appliance in the TRITON Manager

Email Gateway manager steps

Some initial configuration settings are important for Email Gateway for Office 365 operation. Perform the following activities after you install Email Gateway management components:

1. Log on to the TRITON Manager and select the Email tab.
2. Register Email Gateway for Office 365 with the TRITON AP-DATA module. See Registering with TRITON AP-DATA for more information.
3. Configure the system to send email to the Internet through Exchange Online.
   a. Select **Settings** > **Inbound/Outbound** > **Mail Routing**.
   b. Select the default route.
   c. Change the Delivery Method to **SMTP server IP address**.

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



Mail Routing > Edit Domain-Based Route

Name: default

Route order: 1

Delivery Method

○ Recipient domain
Email delivery based on the recipient's domain

● SMTP server IP address
Email delivery based on SMTP server list

SMTP Server List

□	Server Address	Port	MX lookup	Preference
□	WBSN.mail.protection.outlook.co	25	no	10

Edit SMTP Server

Server address: WBSN.mail.protection.ou
IP address or hostname
□ Enable MX lookup

Port: 25

The system will try to deliver to the server address based on the preference. Smaller numbers indicate higher preference.

Preference: 10

Delivery Options

☑ Use Transport Layer Security (TLS)

□ Require authentication

e. For Server Address, add the FQDN of your organization's Microsoft Office 365 Exchange Online account. This is the same as the MX record of the Office 365-hosted domain. To find it:

- Select **Settings** > **Domains** from the Office 365 Admin Center.
- 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 Email Gateway module you have.

4. Specify an email address to which you want system notification messages sent. This address is typically an administrator address. See Setting system notification email addresses for details.

5. Data loss protection policies are enabled by default so no action is needed in this regard. To manage DLP policies, navigate to **Main** > **Policy Management** > **DLP Policies** > **Manage Policies**.

6. If you are deploying multiple, load-balanced VMs, connect the VMs to the management server. (You've already connected the primary VM to the management server using the VPN connection script.)

   a. On the Email tab, select **Settings** > **General** > **Email Appliances**. Your primary VM is listed.

   b. Click **Add** and enter the private IP of the second Email Gateway VM.

   c. On the top right corner, select the second VM from the Appliance field and configure it exactly like the first one.

   d. Select **Settings** > **Data Loss Protection** and configure the VM as needed.

   e. Register the second VM to the TRITON AP-DATA module like you registered the first.

   f. Repeat for each VM.

7. Select the Data tab and click **Deploy**. You can view all of the VMs in the Data Security manager's System Modules list.

Click **Help** on any of the TRITON Manager pages for help about the page. See the Email Security Gateway Help for complete information about the Email Module.

TRITON Manager steps

1. Select the TRITON Manager Data tab.
2. Add the network email destination to policies that should be used for this appliance.
3. Click **Deploy**. No other configuration steps are required.

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

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

Refer to the TRITON AP-DATA Administrator Manager Help for more information.

Configure mail flow in Exchange Online

Now you must configure Exchange Online to transfer email to the virtual appliance in Azure.

1. Log on to Microsoft Office 365, http://portal.office.com, and click **Admin** > **Exchange** from the left navigation panel.
2. Select **Mail Flow** from the left navigation panel.
3. Create a connector.
    a. Click **Connectors** on the top, and then click the plus sign (+) to add a new connector.
    b. In the **From** field, select **Office 365**, and in the **To** field, select **Your organization's email server**.
    c. Click **Next**.
    d. Enter a name and description for the connector. (This a new name being assigned to the Email Gateway appliance.)
    e. Click **Next**.
    f. For **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. Click the plus sign (+) on the **How do you want to route email messages** page, and enter the IP address or FQDN for the Email Gateway virtual machine in Azure. If you are using a load balancer in Azure in front of the gateways, enter the FQDN of the virtual IP.

i. Click **Next**.

j. Select **Always use TLS to secure the connection**.

k. Click **Next** to view a summary screen, then click **Next** again.

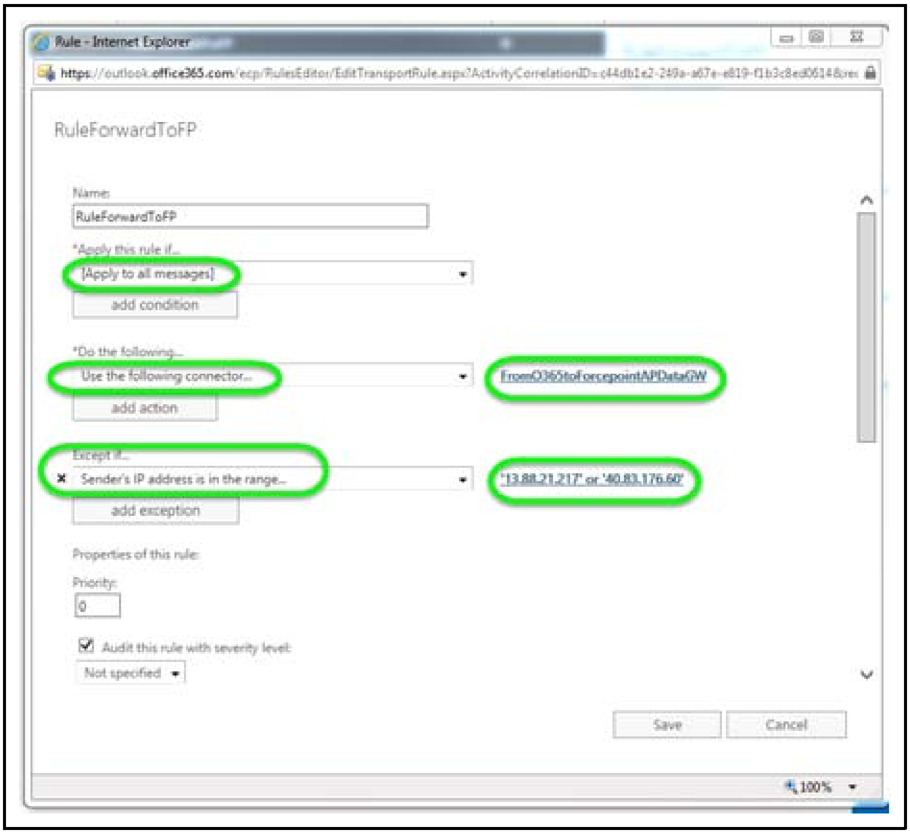
l. Click **+** to validate the connector, and then enter a test email address. The system validates the new connector and sends a test email.

m. Save the connection.

4. Create rules that forward traffic to the gateway.

a. Select **Rules** on the top of the page and then click + to create a new rule.

b. Assign a name to the rule.



RuleForwardToFP

Name: RuleForwardToFP

*Apply this rule if... [Apply to all messages]

*Do the following... Use the following connector... FromO365toForcepointAPDataGW

Except if... Sender's IP address is in the range... '13.88.21.217' or '40.83.176.60'

Properties of this rule:

Priority: 0

☑ Audit this rule with severity level: Not specified

Rule - Internet Explorer
https://outlook.office365.com/ecp/RulesEditor/EditTransportRule.aspx?ActivityCorrelationID=c44db1e2-249a-a67e-e819-f1b3c8ed0614&rec
add condition
add action
add exception
Save
Cancel
100%

c. For **Apply this rule if**, select **Apply to all messages**.

d. Under **Do the following**, indicate the action to take when the condition is met—in this case, **Use the following connector**. Select the connector you just created.

e. Under **Except if**, select **Sender's IP address is in range** and enter the IP address for the Email Gateway virtual machine in Azure. If you are using a load balancer in Azure in front of the gateways, enter the virtual IP.

f. Select **Stop processing more rules** and accept the remaining defaults.

g. Save the rule.

5. Create a second connector.

a. Click **Connectors** on the top, and then click the plus sign (**+**) to add a new connector.

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

c. Click **Next**.

d. Enter a name and description for the connector.

e. Click **Next**.

f. On the **How should Office 365 identify email from your email server** page, select 1 of 2 options:

   ○ For best practice, 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 for TRITON AP-DATA Email Gateway for Office 365 in the Forcepoint knowledge base.

   ○ Alternately, select **By verifying that the IP address of the sending server,** and enter the FQDN of the Email Gateway virtual machine.

g. Click **Next** to view a summary screen.

h. Save the connection.

6. Make sure none of the public static IPs used by the Email Gateway VMs 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.

Logging onto the virtual machine

To access the virtual machine on Azure from a local machine, use an SSH client such as PuTTY or OpenSSH.

1. For Windows, launch PuTTY.
2. Enter the hostname or IP address of the Email Gateway VM as well as the port number. You can find these on the Azure management dashboard, Quick Glance section.
3. Select **SSH** for the connection type.
4. Click **Open** to open a connection with the VM.
5. Log on to the VM using the account you specified when creating it.
6. If you have trouble logging on, make sure that port 22 is open and that it is not blocked by your IT organization.

Restarting load-balanced VMs

When a VM is shut down, its IP address is de-allocated. When you restart it, it's assigned the first address available in the VPN's IP range.

If there is only one Email Gateway VM on the Azure network, it is allocated the same IP, because there are no other VMs.

But when you have 2 or more VMs running in Azure, you have to restart them in the correct order in order for them to receive the same IPs.

If you don't, the TRITON manager will not be able to connect to the VMs, deploy new rules to them, or get statistics, etc.

To prevent this issue, it is best practice to configure static IPs for load-balanced VMs. You can assign the IP at the time the VM is created, or you can update an existing VM. You can use PowerShell to assign the IP.

Static IPs should be selected the pool of IP addresses available in your virtual network.

For more information, refer to the MSDN site, Static IP, Reserved IP and Instance Level IP in Azure.

Analytics engine

The analytics engine is used to calculate the risk of user activity, correlate it with other risky activity, and assign it a risk score.

Risk scores appear in the Incident Risk Ranking report and on the dashboard in the TRITON Manager. The report shows up to 20 cases with the highest risk scores during the selected time period, along with details for those cases. Incidents within cases are also ranked according to their number of matches, transaction size, content, breached policies and rules, date and time, and more.

You use this information to identify the highest risks to your organization so that you can take remediation action and prevent future risks.

To use this feature, you must first install an analytics engine on a 64-bit Linux machine. This section describes how.

Operating system requirements

- Up-to-date CentOS 7 (analytics engine)
- Windows Server 2008 R2 SP1, 2012, or 2012 R2 (management system)

Hardware requirements

The server running the analytics engine must meet the following hardware requirements:

Small to medium business	Mimimum	Recommended
CPU	4 core processors	8 core processors
Memory	8 GB (16 GB max)	16 GB
Hard drives	100 GB	100 GB
NICs	1	1

Medium to large business	Mimimum	Recommended
CPU	8 core processors	8 core processors
Memory	16 GB	20 GB
Hard drives	100 GB	100 GB
NICs	1	1

Port requirements

The following ports must be kept open on the server running the analytics engine:

Outbound		
To	**Port**	**Purpose**
TRITON management server	17443	Syslog, forensics, incidents, analytics engine status
TRITON management server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
TRITON management server (local database) or remote SQL Server	1433	Database connection
* This range is necessary for load balancing.		
Inbound		
From	**Port**	**Purpose**
TRITON management server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.

Pre-installation

Before installing analytics engine, make sure the following Linux packages are installed on the machine.

- apr
- apr-util
- perl-Switch
- unixODBC
- freetds

If you are connected to a yum repository, you can install these packages with the following command:

```
yum install apr apr-util perl-Switch unixODBC freetds
```

The EPEL repository must be configured on the machine in order to install freetds.

Installing the analytics engine

Complete the Analytics Setup Wizard to configure user behavior analytics for TRITON AP-DATA. Enter information as prompted. For help, enter “?”. To quit, press “Quit” or “Ctrl-C”.

Launch wizard

1. To download the analytics engine installer, **AnalyticsEngine83**, use the My Account link to log in to support.forcepoint.com, then select the Downloads page. The installer is under Forcepoint TRITON AP-DATA v8.3.
2. Log in as root and make sure the installation file is in your current working directory and has execution privileges. If you receive a “Permission denied” error, run the following command:

   ```
   chmod +x AnalyticsEngine83
   ```
3. To run the installer, enter:

   ```
   ./AnalyticsEngine83
   ```

   If you receive an error message about missing packages, follow the message instructions to install the required packages using yum.

   After installing the required packages, run the **./AnalyticsEngine83** command again.

Single-command installation

To simplify installation, run the following command on the Linux server. It downloads the Analytic Server installers, installs all the necessary packages, configures the necessary server configurations, and kicks off the Analytics Server wizard. The items in bold are variable. You can customize them if desired.

```
cd /tmp; yum –y install open-vm-tools; yum -y install
epel-release; yum -y install apr apr-util perl-Switch
```

```
unixODBC freetds; yum -y install wget; wget http://
cdn.websense.com/downloads/files/v8.3/AnalyticsEngine83;
yum –y install ntpdate; ntpdate time.nist.gov; chmod +x
AnalyticsEngine83; ./AnalyticsEngine83
```

TRITON Manager connection

1. When prompted, enter the IP address of the TRITON management server:.
2. Enter a user name for an administrator with access to the management server.
3. Enter the administrator’s password. The server will attempt to connect to the TRITON management server.

   Note that you have a role with permission to manage System Modules for this to work.

The Setup Wizard has completed.

Configuration

1. Log on to the TRITON Manager and click the Data tab.
2. To validate that the User Analytics module was set up properly, navigate to **Settings** > **Deployment** > **System Modules**. The module should appear in the tree. Click the module to view details. You can change the name and description if desired.
3. Navigate to **Settings** > **General** > **Reporting** to configure the Top Risks report that was derived from the user analytics. Here you specify the risk scores that you want shown in the report and on the dashboard, and define your typical work week to help identify abhorrent behavior.
4. For optimal accuracy and efficacy, navigate to **Main** > **Policy Management** > **DLP Policies** and add the following policies:
   - Disgruntled Employee
   - Self CV Distribution
   - Password Files
   - PKCS #12 Files
   - Deep Web URLs
   - Email to Competitors - Be sure to provide the competitors’ domain names (case-insensitive, separated by semicolons).
   - Suspected Mail to Self - Add or edit the sources you want to monitor in the **possible_sources_domains** parameter in the **Email Similarity** script classifier”.
5. Click **Deploy**.

Once the system is running and capturing metrics, you can view analytics data in a variety of places:

- Dashboard - Navigate to **Main** > **Status** > **Dashboard** and refer to the **Data Loss Prevention - Incident Risk Ranking** section.

- Incident Risk Ranking report - Click a dashboard element or navigate to **Main** > **Reporting** > **Data Loss Prevention** > **Report Catalog** > **Security Analytics** > **Incident Risk Ranking** to view a detailed report of the risks detected in your organization.

To view the health of the Analytics Engine, navigate to **Main** > **Status** > **System Health**, and then click the Analytics Engine module.

TRITON AP-DATA Cloud App Security

In this topic:

TRITON AP-DATA Cloud App Security provides cloud activity content inspection for files uploaded into and stored within cloud enterprise services, including Microsoft OneDrive for Business, SharePoint Online, and Box. By applying established DLP policies to data stored in enterprise cloud applications, the module is able to audit and prevent the storage of sensitive data that could expose your organization to data loss and compliance infringements.

In addition, TRITON AP DATA Cloud provides the existing cloud discovery functionality provided by TRITON AP-DATA Discover (i.e., Box, SharePoint Online, and Exchange Online discovery).

TRITON AP-DATA Cloud App Security can be installed in a private data center (on-premises) or in the Microsoft Azure cloud with management components on-premises.

The system can support multiple Cloud App Security agents, each running a different cloud service.

Operating system support

- Up-to-date CentOS 7 (TRITON AP-DATA Cloud App Security agent)
- Windows Server 2008 R2 SP1, 2012, or 2012 R2 (management system)

System requirements

- TRITON AP-DATA v8.3.
- Docker containerization system (instructions below). v1.11.1+

Supported cloud services (DLP)

- Microsoft OneDrive for Business

Supported cloud apps (discovery)

- Box
- Microsoft SharePoint Online
- Microsoft Exchange Online

Ports

The following ports must be kept open for both on-premises and cloud deployments of TRITON AP-DATA Cloud App Security in order for the TRITON management server and cloud agent to communicate:

Outbound		
To	**Port**	**Purpose**
Cloud apps	443	Secure communication with cloud applications (OneDrive)
TRITON management server	17500-17515	Communication with all TRITON AP-DATA components
Inbound		
Cloud apps	8080, 443	Notifications from cloud applications (no sensitive data is passed on non-secure channels)
TRITON management server	17500-17515	Communication with all TRITON AP-DATA components
Any service (including the cloud agent) that is not using logging on	22	Manage VM by SSH

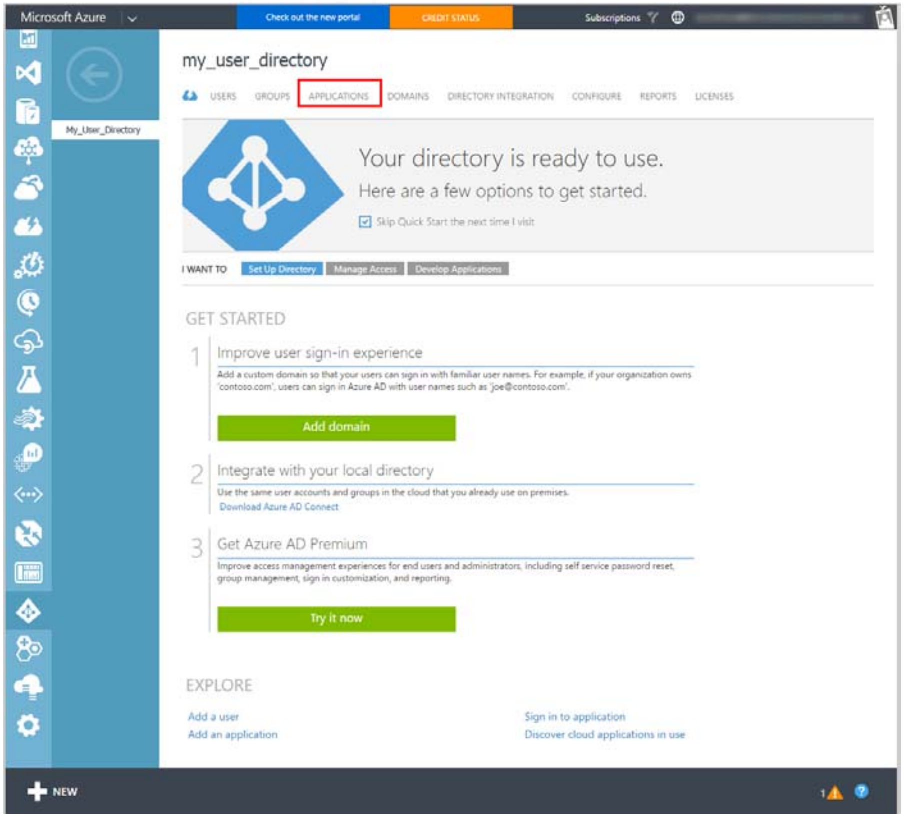
Installation

The TRITON AP-DATA Cloud App Security agent can be deployed through the Azure cloud or installed on-premises. Because the services it interacts with are hosted in the cloud, you should deploy the product in the cloud for best performance.

STEP 1: Create an Azure Active Directory application

To connect Azure Active Directory with the TRITON management server, you must create an Azure application whether you are deploying TRITON AP-DATA in Azure or on-premises. The application acts as a bridge between OneDrive for Business and TRITON AP-DATA.

1. Log on to the Azure Portal, https://manage.windowsazure.com.
2. Click **Active Directory**, then choose the desired user directory.
3. Click **Applications**.



Your directory is ready to use.

Here are a few options to get started.

☑ Skip Quick Start the next time I visit

GET STARTED

1 Improve user sign-in experience

Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.

2 Integrate with your local directory

Use the same user accounts and groups in the cloud that you already use on premises.
Download Azure AD Connect

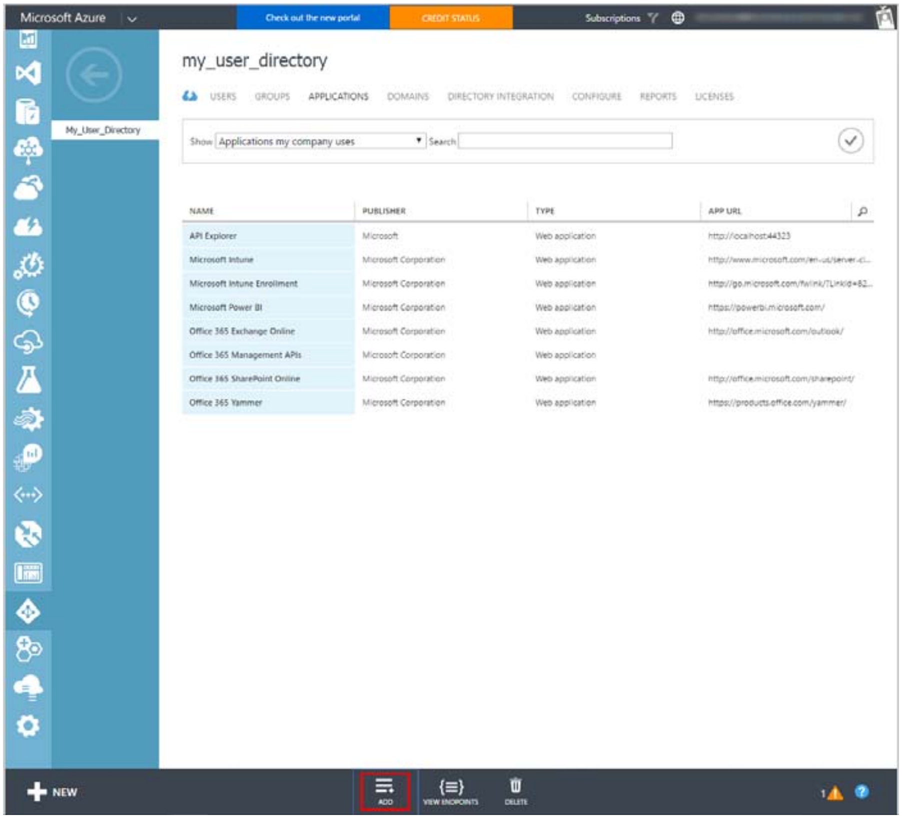
3 Get Azure AD Premium

Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.

EXPLORE

4. Create a new application.

a. Click **Add**.

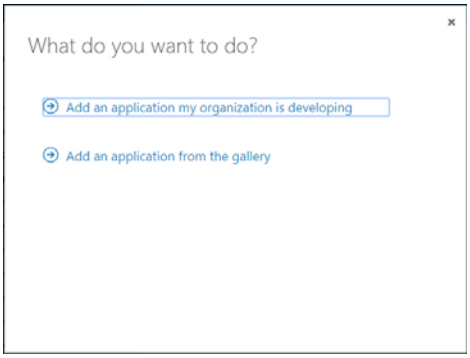


Show Applications my company uses

Search

NAME	PUBLISHER	TYPE	APP URL
API Explorer	Microsoft	Web application	http://localhost:44323
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cl...
Microsoft Intune Enrollment	Microsoft Corporation	Web application	http://go.microsoft.com/fwlink/?LinkId=82...
Microsoft Power BI	Microsoft Corporation	Web application	https://powerbi.microsoft.com/
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	https://products.office.com/yammer/

b. Select **Add an application my organization is developing**.


What do you want to do?
Add an application my organization is developing
Add an application from the gallery

c. Enter a descriptive **Name** for the application, such as Forcepoint cloud agent.

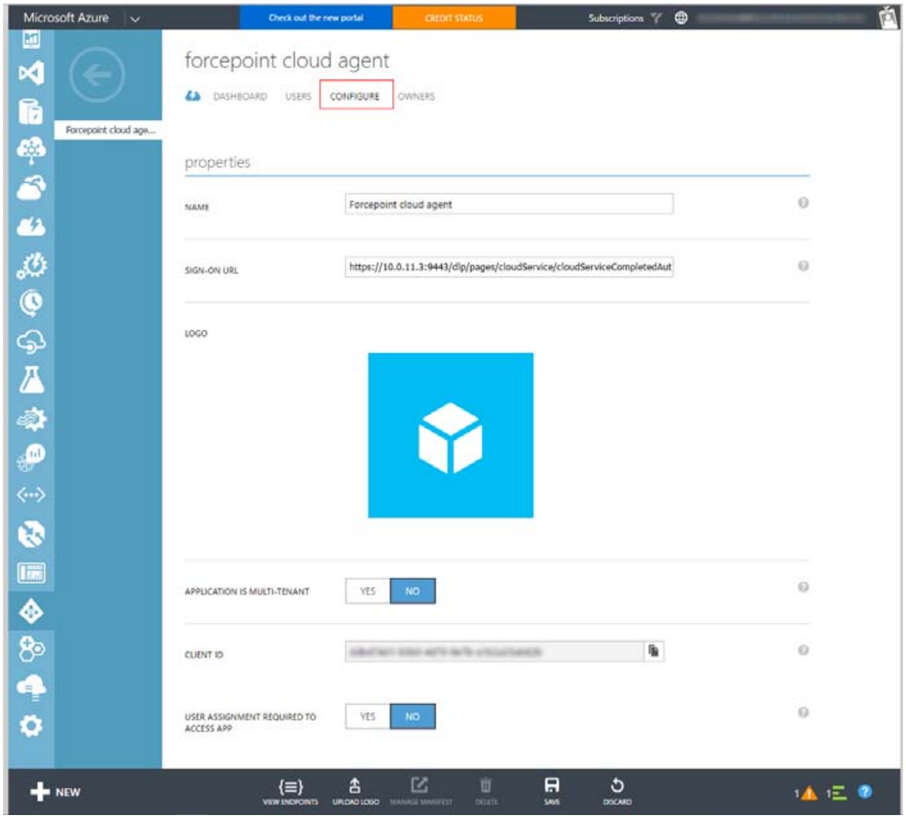
d. For Type, select **Web application and/or web API**.

e. When prompted, enter a sign-on URL. **This is the URL where users can sign in and use your app.** It should be of the format:

```
https://{TRITON server IP}:9443/dlp/pages/
cloudService/cloudServiceCompletedAuthClientWindow.jsp
```

App ID URI is not required for TRITON AP-DATA Cloud App Security.

5. Click **Configure**. The properties for your new application are shown.



forcepoint cloud agent

properties

NAME: Forcepoint cloud agent

SIGN-ON URL: https://10.0.11.3:9443/dlp/pages/cloudService/cloudServiceCompletedAut

LOGO

APPLICATION IS MULTI-TENANT: YES [✓ NO]

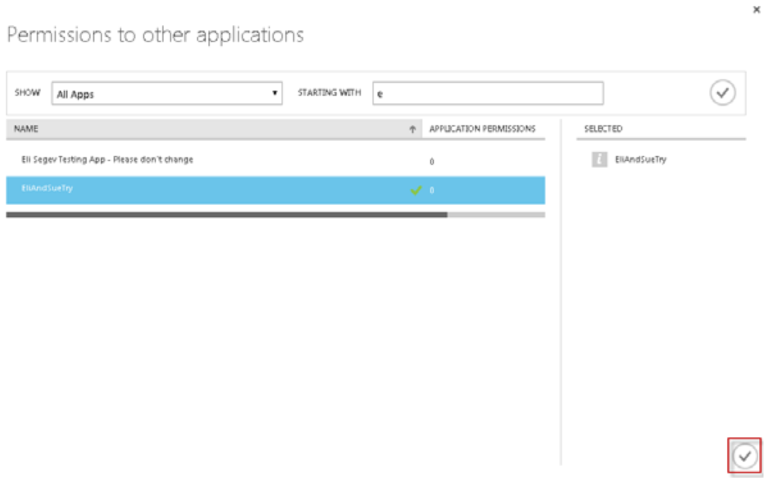
CLIENT ID: [redacted]

USER ASSIGNMENT REQUIRED TO ACCESS APP: YES [✓ NO]

6. Scroll down to view the **Keys** section. Select a key duration (1 year or 2 years).
7. Under **Permissions to other applications**, click **Add application**.
8. One by one, add the Office 365 services for which your app requires permissions:
   - Office 365 Management APIs
   - Office 365 SharePoint Online

   Windows Azure Active Directory is already chosen.

To locate a service, select **All Apps** under **Show**, and search for the first letter of its name. Select the service name when it appears, then click the check mark.



Permissions to other applications

SHOW: All Apps

STARTING WITH: e

NAME	APPLICATION PERMISSIONS
Eli Segev Testing App - Please don't change	0
EliAndSueTry ✓	0

SELECTED

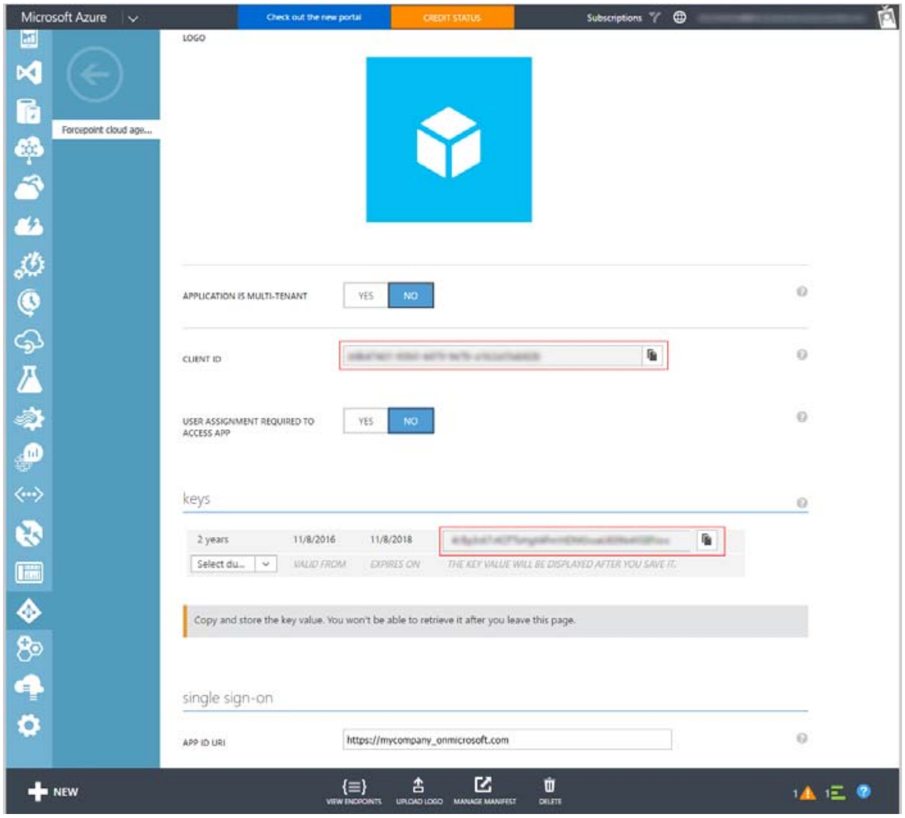
EliAndSueTry

9. Using drop-down menus, select the **Application Permissions** and **Delegated Permissions** that your app requires for each service. These are the permissions that will be displayed to your app user when Azure prompts them to consent to your app's permission request. TRITON AP-DATA Cloud App Security requires the following permissions:

Application	Application Permissions	Delegated Permissions
Windows Azure Active Directory	● Read all hidden memberships ● Read and write devices ● Read and write directory data ● Read and write domains ● Read directory data	none

Application	Application Permissions	Delegated Permissions
Office 365 Management APIs	● Read DLP policy events including detected... ● Read activity data for your organization ● Read service health information for your organization	● Read DLP policy events including detected ... ● Read activity data for your organization ● Read service health information for your organization
Office 365 SharePoint Online	● Read user profiles ● Read and write user profiles ● Read and write managed metadata ● Read managed metadata ● Have full control of all site collections ● Read items in all site collections ● Read and write items in all site collections	none

10. Click **Save**. Copy and store the Client ID and Key that display. You will need these during TRITON Manager setup.



[redacted]

APPLICATION IS MULTI-TENANT: YES [✓ NO]

CLIENT ID: [redacted]

USER ASSIGNMENT REQUIRED TO ACCESS APP: YES [✓ NO]

keys

Select du...	VALID FROM	EXPIRES ON	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.
2 years	11/8/2016	11/8/2018	[redacted]

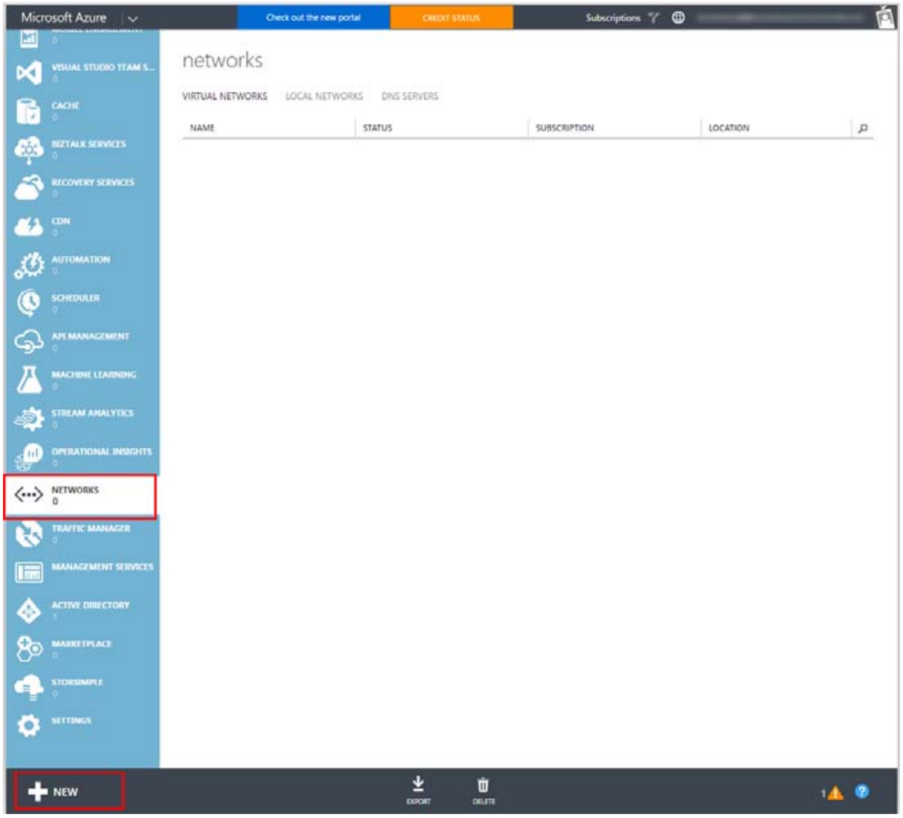
Copy and store the key value. You won't be able to retrieve it after you leave this page.

single sign-on

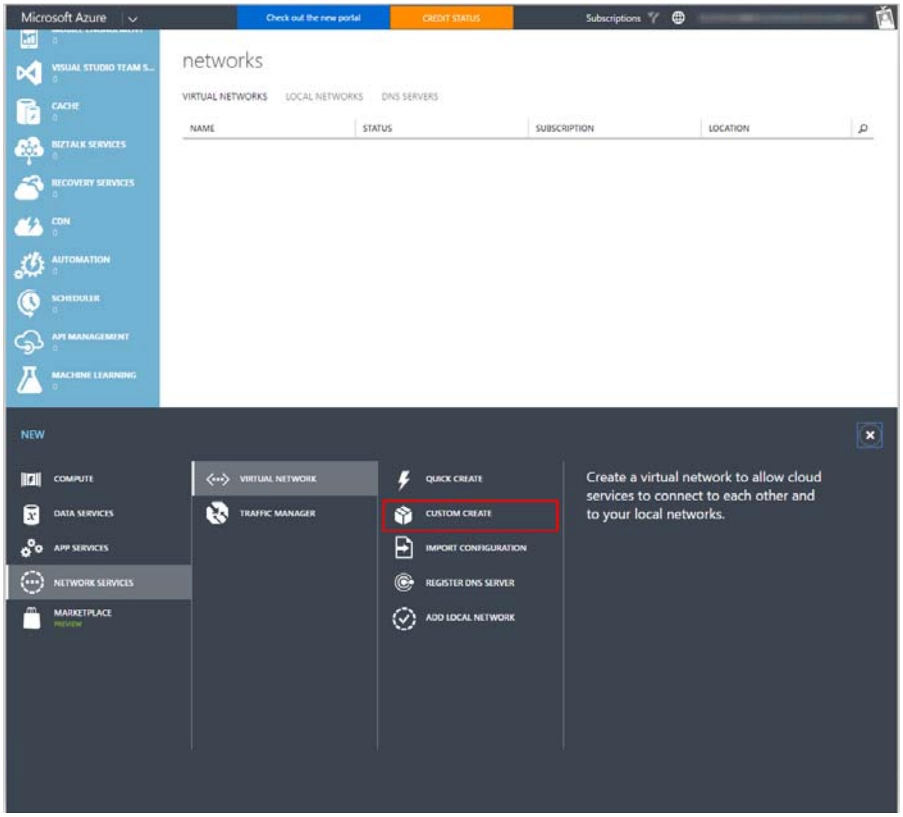
APP ID URI: https://mycompany_onmicrosoft.com

STEP 2: Configure a Virtual Network and Point-to-Site VPN in Azure (Azure deployments only)

1. In the Azure Portal, click **Networks** and then **New** to create a new virtual network.

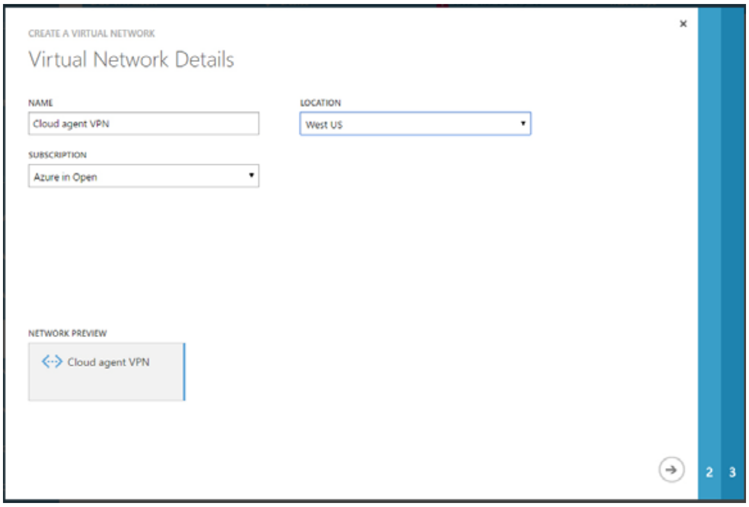


2. Click **Custom Create**.



Create a virtual network to allow cloud services to connect to each other and to your local networks.

3. Enter a name for the virtual network you are creating, choose a location, then click >. Location refers to the physical location (region) where you want your resources (VMs) to reside. Choose the location closest to you. It will be used for all the other components such as the storage space and the VM.



CREATE A VIRTUAL NETWORK

Virtual Network Details

NAME: Cloud agent VPN

LOCATION: West US

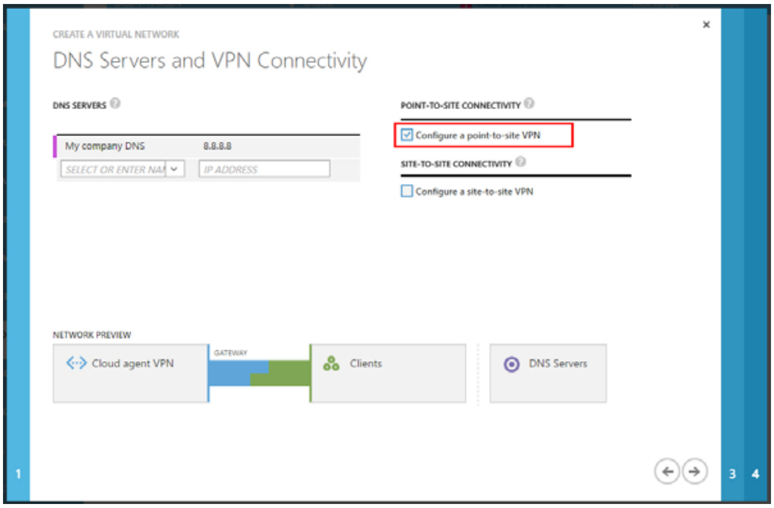
SUBSCRIPTION: Azure in Open

NETWORK PREVIEW

Cloud agent VPN

4. Enter the name and IP address of your DNS server if you want to connect one to the VPN, then select **Configure a point-to-site VPN** and click >. Leave DNS servers blank if you do not plan to use one.

For instructions on creating site-to-site VPNs, see this Microsoft article.



CREATE A VIRTUAL NETWORK

DNS Servers and VPN Connectivity

DNS SERVERS

My company DNS	8.8.8.8
SELECT OR ENTER NA	IP ADDRESS

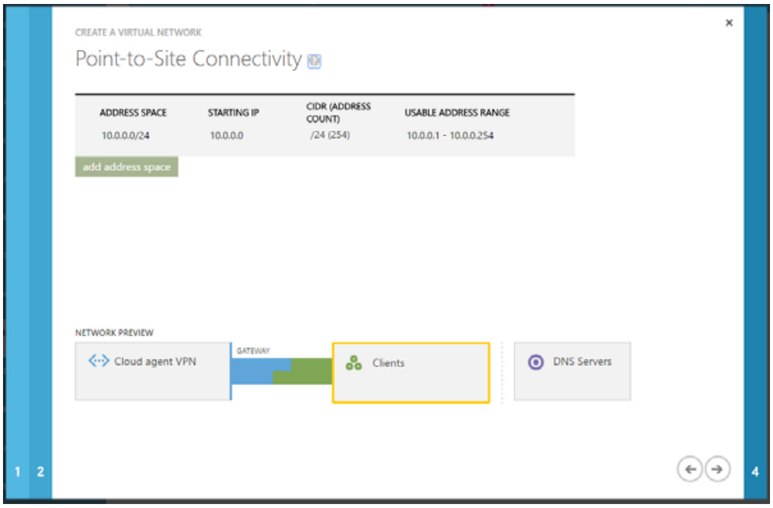
POINT-TO-SITE CONNECTIVITY

☑ Configure a point-to-site VPN

SITE-TO-SITE CONNECTIVITY

□ Configure a site-to-site VPN

5. Configure the VPN client’s IP range. Include a starting IP and address count. It cannot be the IP range that you are using for your on-premises components or you will have a routing issue on your management server and SQL servers. For example, if your on-premises servers are using 10.x.x.x, use 192.168.x.x or 172.16.x.x as the starting IP for this virtual network. You do not need to create more than one address space. Click > when done.



CREATE A VIRTUAL NETWORK

Point-to-Site Connectivity

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/24	10.0.0.0	/24 (254)	10.0.0.1 - 10.0.0.254

6. Specify the address range that you want to use for your virtual network. The VM that you create in Azure will be allocated an IP from this VPN’s range.

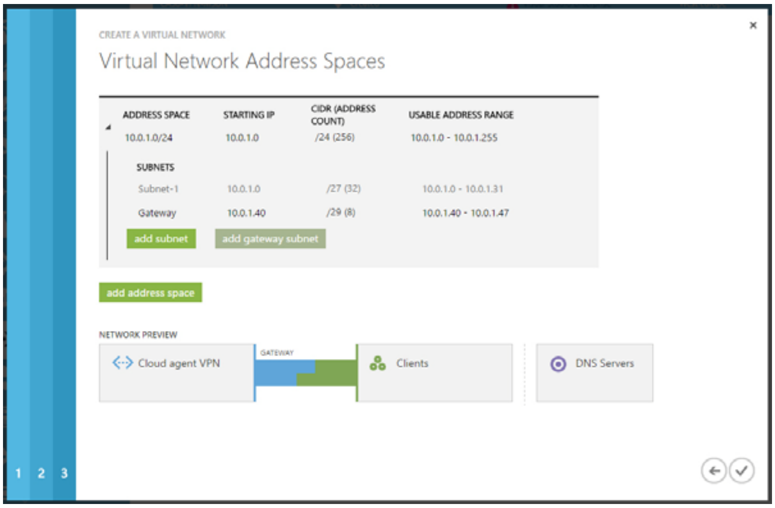
   Click **Add Gateway Subnet** to create a subnet for the gateway (required).

   Click the check mark when done.

For best practice use a 29-bit subnet mask. This ensures that your IP address pool has 6 addresses and helps ensure a speedy recovery in case of disconnection.

Note

None of the virtual IP addresses should be on same subnet as the local management server IP. Keeping them on separate subnets prevents problems with the automatic VPN connection script that you will be using later in this procedure.

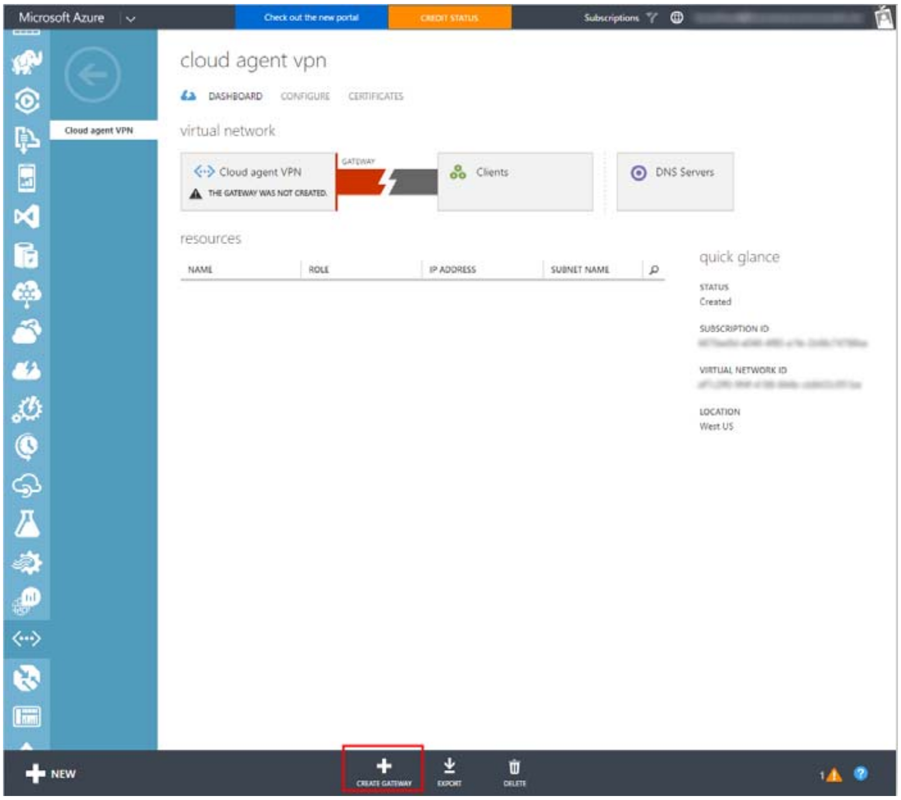


CREATE A VIRTUAL NETWORK

Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.1.0/24	10.0.1.0	/24 (256)	10.0.1.0 - 10.0.1.255
SUBNETS			
Subnet-1	10.0.1.0	/27 (32)	10.0.1.0 - 10.0.1.31
Gateway	10.0.1.40	/29 (8)	10.0.1.40 - 10.0.1.47

7. Select the network you just created from the resulting list then click **Create Gateway** to create the gateway. This can take 15-30 minutes.



STATUS
Created

SUBSCRIPTION ID
[redacted]

VIRTUAL NETWORK ID
[redacted]

LOCATION
West US

8. Create security certificates to authenticate VPN clients. For instructions, see this Microsoft article. You need to:

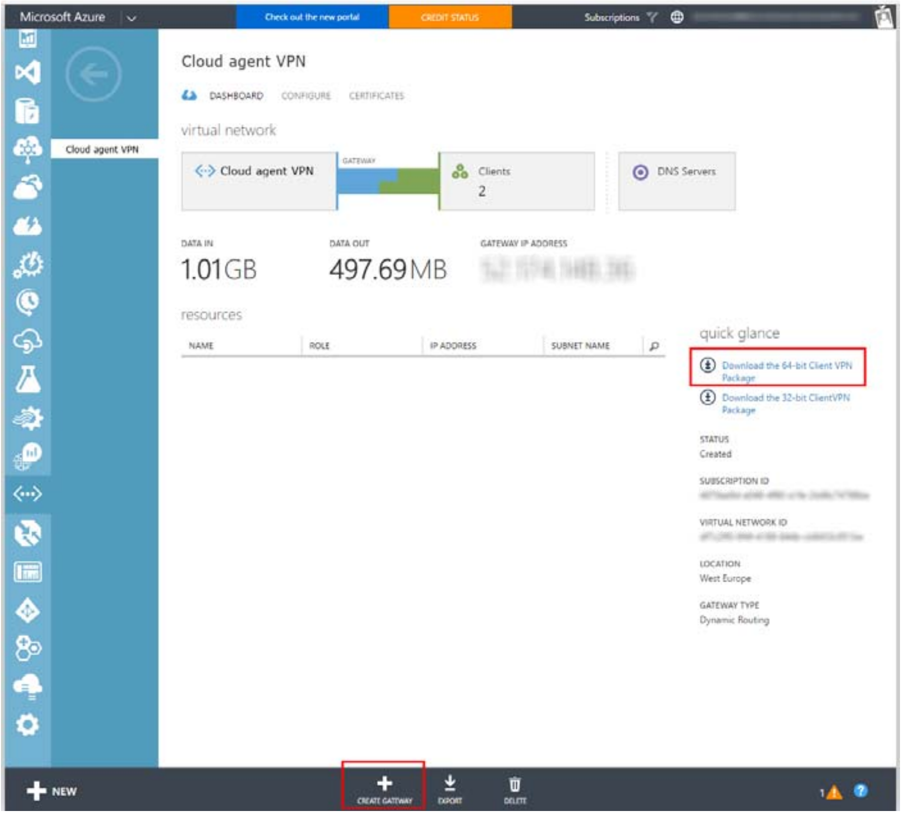
    a. Generate a self-signed root certificate

    b. Upload the root certificate file to the Azure Portal

    c. Generate a client certificate

    d. Export and install the client certificate on the TRITON management server.

9. Download the 64-bit client VPN package to the TRITON management server and install it.



10. Open the VPN client software and click **Connect** to connect the client to the virtual network.

11. Run **ipconfig** on the VPN client's command line to find the IP address assigned to it.

12. Connect the TRITON management server to the Azure VPN network by doing the following.

    a. On the TRITON management server, download the VPN connection script, **p2s_vpn_connect.ps1**, from Forcepoint Downloads.

    b. Open the script in a text editor.

    c. Edit the following parameters with the values used in the **pre-deploy.ps1** script. This is the script you edited when building the virtual network in Azure. Below are the default values:

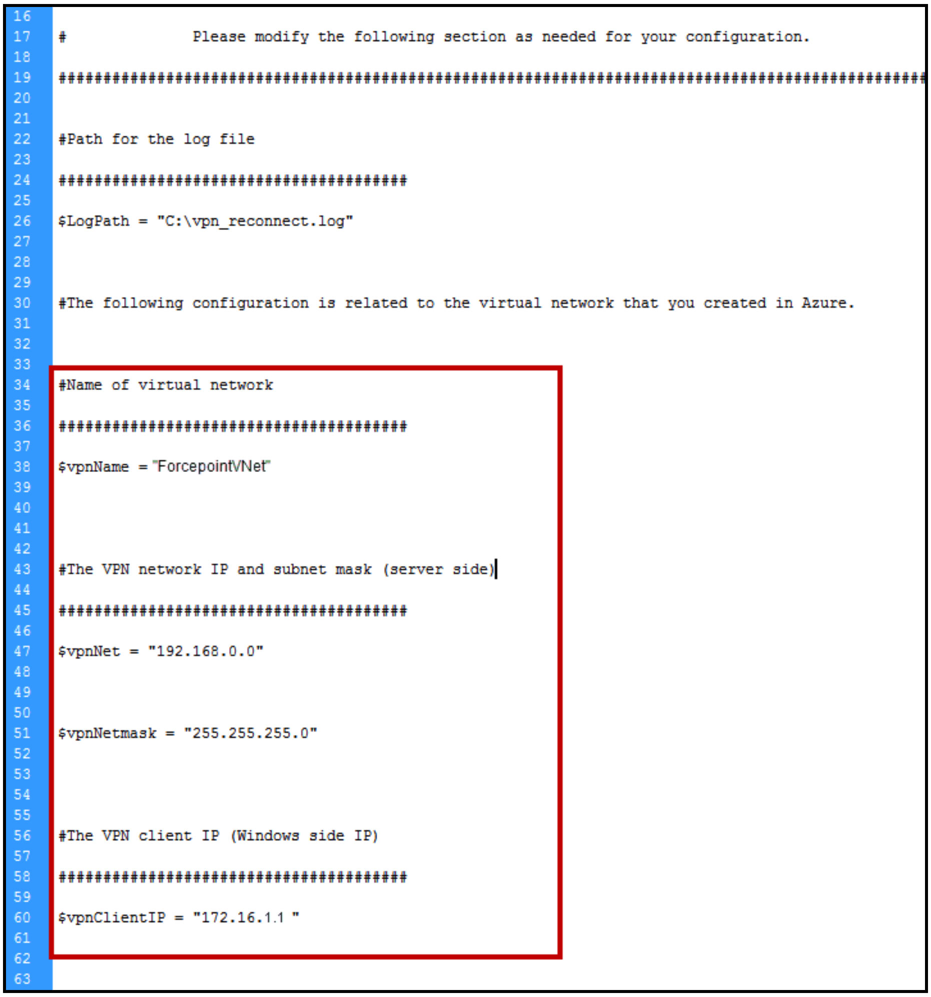
       - $vpnName - ForcepointVNet (virtual network name)
       - $vpnNet - 192.168.0.0 (VPN network IP, server side)
       - $vpnNetmask - 255.255.0.0 (VPN subnet mask, server side)
       - $vpnClientIP - 172.16.1.1 (VPN client's IP address)

       Each entry should be on a separate line. Entries should be surrounded in quotation marks.

       Use the following format:

```
<parameter> = “<value>”
```

Example:



```

#              Please modify the following section as needed for your configuration.

##################################################################################################


#Path for the log file

#######################################

$LogPath = "C:\vpn_reconnect.log"


#The following configuration is related to the virtual network that you created in Azure.



#Name of virtual network

#######################################

$vpnName = "ForcepointVNet"




#The VPN network IP and subnet mask (server side)

#######################################

$vpnNet = "192.168.0.0"



$vpnNetmask = "255.255.255.0"




#The VPN client IP (Windows side IP)

#######################################

$vpnClientIP = "172.16.1.1 "



```

The default log path is c:\vpn_reconnect.log. You can edit this as well if desired.

The default user directory path is C:\Users\Administrator\AppData\Roaming\. The administrator named here must be the same as the one who installed the Azure VPN client. Edit Administrator as needed.

Save the file when done.

d. Change the PowerShell Script Execution Policy from Restricted to RemoteSigned so that local PowerShell scripts can be run. To do so, enter:

```
Set-ExecutionPolicy RemoteSigned
```

e. Run the revised script from PowerShell. This connects the management server to the VPN network and keeps them connected at all times.

Important

If the management server is restarted for any reason, you must re-run this script. For best practice, add the script to the Windows Task Scheduler so that it runs on startup. For instructions, see this knowledgebase article.

f. If your system is using a remote database, copy the script onto the database machine and run it there as well.

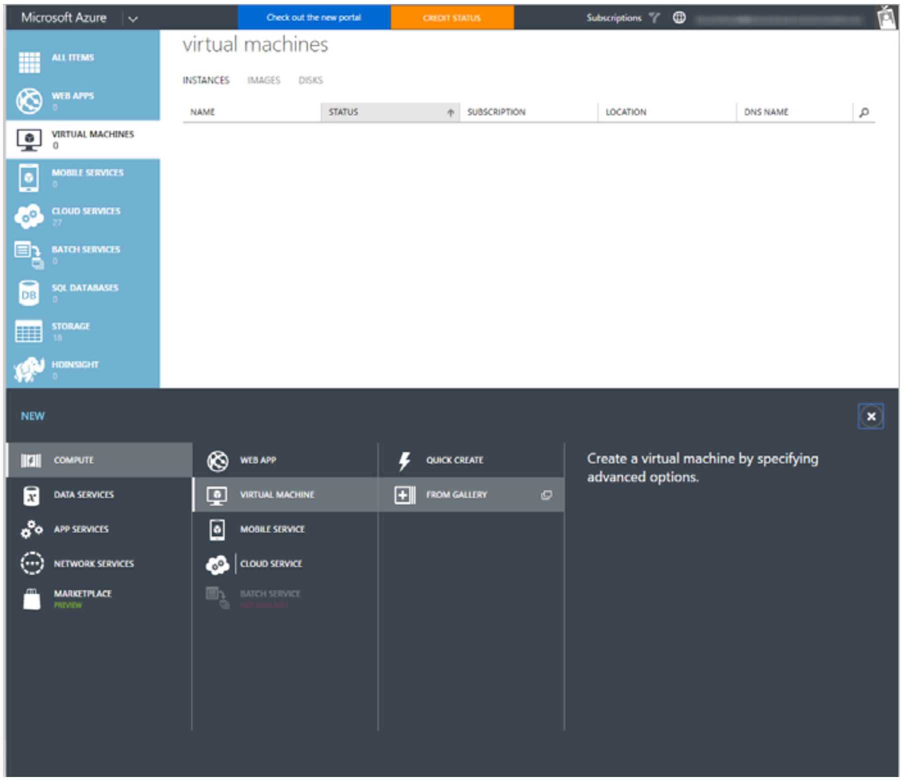
STEP 3: Create a virtual (or physical) machine

On-premises deployments

1. Install a VM or physical machine with CentOS 7.

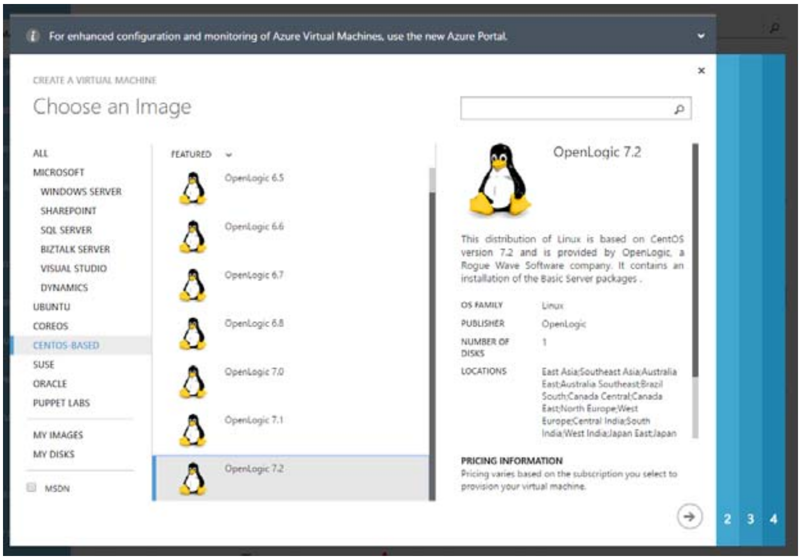
Azure deployments

1. In the Azure Portal, click **Virtual Machines** in the left navigation pane, and then click **New** > **Compute** > **Virtual Machine** > **From Gallery**.



Create a virtual machine by specifying advanced options.

2. Under **Choose an Image**, select **CENTOS-BASED**, and then select a version of **OpenLogic** that meets your needs. For best practice, select the latest for more security and scalability.



For enhanced configuration and monitoring of Azure Virtual Machines, use the new Azure Portal.

CREATE A VIRTUAL MACHINE

Choose an Image

OpenLogic 7.2

This distribution of Linux is based on CentOS version 7.2 and is provided by OpenLogic, a Rogue Wave Software company. It contains an installation of the Basic Server packages .

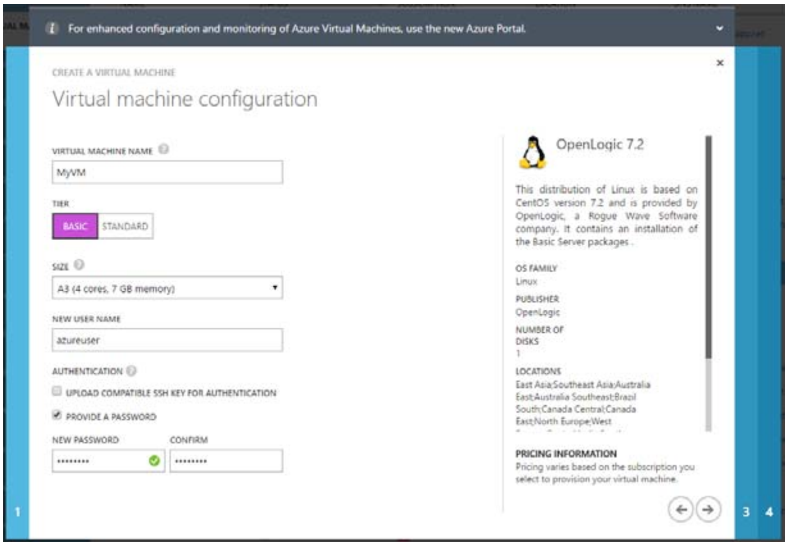
OS FAMILY	Linux
PUBLISHER	OpenLogic
NUMBER OF DISKS	1
LOCATIONS	East Asia;Southeast Asia;Australia East;Australia Southeast;Brazil South;Canada Central;Canada East;North Europe;West Europe;Central India;South India;West India;Japan East;Japan

PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

3. Under **Virtual machine configuration**, page 2, select the following:
   - **Virtual Machine Name**: VM name is usually the DNS name. Change as desired. This is the name for the cloud agent VM.
   - **Tier**: Standard tier
   - **Size**: A3 minimum recommended
   - **New user name**: Name of your choice
   - **Authentication**: Provide a password
   - Password of your choice

Note that when you want to control the VM and do root activities remotely, you need to activate a remote logon as root user. Your HelpDesk can assist with this.



For enhanced configuration and monitoring of Azure Virtual Machines, use the new Azure Portal.

CREATE A VIRTUAL MACHINE

Virtual machine configuration

VIRTUAL MACHINE NAME: MyVM

TIER: BASIC | STANDARD

SIZE: A3 (4 cores, 7 GB memory)

NEW USER NAME: azureuser

AUTHENTICATION

□ UPLOAD COMPATIBLE SSH KEY FOR AUTHENTICATION

☑ PROVIDE A PASSWORD

NEW PASSWORD: •••••••• CONFIRM: ••••••••

OpenLogic 7.2

This distribution of Linux is based on CentOS version 7.2 and is provided by OpenLogic, a Rogue Wave Software company. It contains an installation of the Basic Server packages .

OS FAMILY: Linux

PUBLISHER: OpenLogic

NUMBER OF DISKS: 1

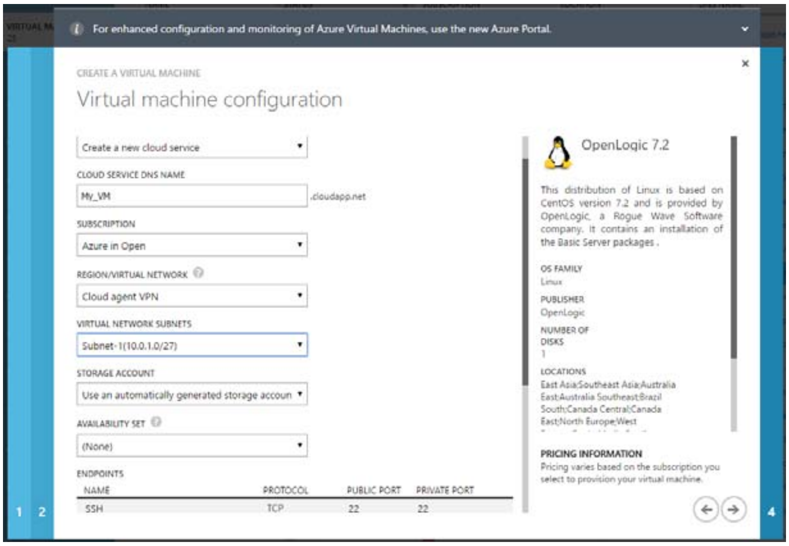
LOCATIONS: East Asia;Southeast Asia;Australia East;Australia Southeast;Brazil South;Canada Central;Canada East;North Europe;West

PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

4. Under **Virtual machine configuration**, page 3, select the following:
   - **Cloud Service**: Select an existing cloud service or create a new one. Select Create a new cloud service for best practice.
   - **Cloud Service DNS Name**: DNS name of your choice. It will be published on the web. It’s not part of your local organization DNS server.
   - **Subscription**: Type of Azure subscription you want.
   - **Region/Virtual Network**: Shows the VPN adapter you created. Region is inherited.
   - **Virtual network subnets**: Inherited by VPN set up.
   - **Storage Account:** Select **Use an automatically generated storage account**.
   - **Availability Set**: None required

- Modify ports as shown below: SSH, TCP, 22, 22. Refer to *Ports*, page 95 for a list of other required open ports.



For enhanced configuration and monitoring of Azure Virtual Machines, use the new Azure Portal.

CREATE A VIRTUAL MACHINE

Virtual machine configuration

Create a new cloud service

CLOUD SERVICE DNS NAME: My_VM .cloudapp.net

SUBSCRIPTION: Azure in Open

REGION/VIRTUAL NETWORK: Cloud agent VPN

VIRTUAL NETWORK SUBNETS: Subnet-1(10.0.1.0/27)

STORAGE ACCOUNT: Use an automatically generated storage accoun

AVAILABILITY SET: (None)

ENDPOINTS

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
SSH	TCP	22	22

OpenLogic 7.2

This distribution of Linux is based on CentOS version 7.2 and is provided by OpenLogic, a Rogue Wave Software company. It contains an installation of the Basic Server packages .

OS FAMILY: Linux

PUBLISHER: OpenLogic

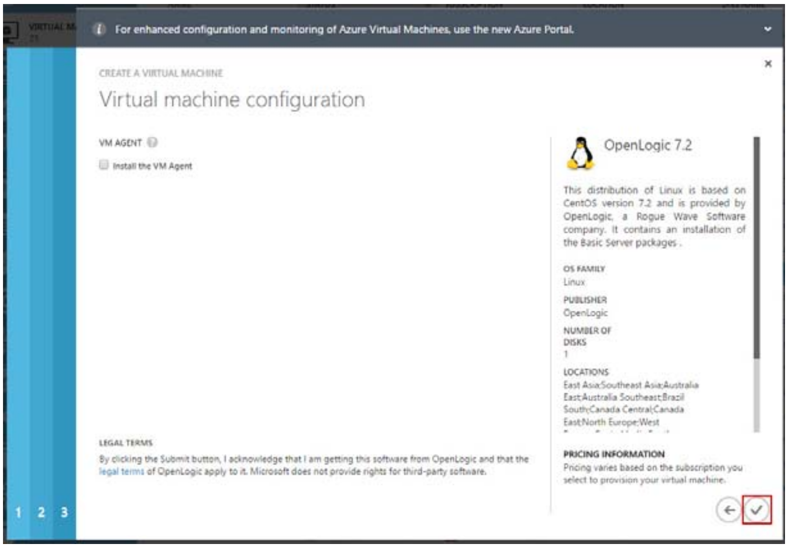
NUMBER OF DISKS: 1

LOCATIONS: East Asia;Southeast Asia;Australia East;Australia Southeast;Brazil South;Canada Central;Canada East;North Europe;West

PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

5. Under **Virtual machine configuration**, page 4, click the check mark in the lower right corner to build the VM.



For enhanced configuration and monitoring of Azure Virtual Machines, use the new Azure Portal.

CREATE A VIRTUAL MACHINE

Virtual machine configuration

VM AGENT

□ Install the VM Agent

LEGAL TERMS

By clicking the Submit button, I acknowledge that I am getting this software from OpenLogic and that the legal terms of OpenLogic apply to it. Microsoft does not provide rights for third-party software.

OpenLogic 7.2

This distribution of Linux is based on CentOS version 7.2 and is provided by OpenLogic, a Rogue Wave Software company. It contains an installation of the Basic Server packages .

OS FAMILY: Linux

PUBLISHER: OpenLogic

NUMBER OF DISKS: 1

LOCATIONS: East Asia;Southeast Asia;Australia East;Australia Southeast;Brazil South;Canada Central;Canada East;North Europe;West

PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

STEP 4: Install Docker

This section applies to both Azure and on-premises deployments.

If you have Docker containerization system installed, skip to *STEP 5: Run the cloud agent installation wizard*, page 112.

1. As a root user, log on to the Linux machine that will host the TRITON AP-DATA Cloud App Security agent.
2. Run the “yum update” to receive all the latest updates for all repositories.

3. Add the Docker repo using this command:

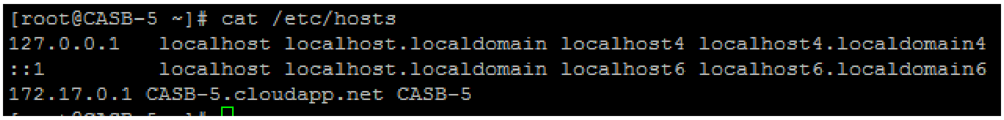
```
sudo tee /etc/yum.repos.d/docker.repo <<-'EOF'
[dockerrepo]
name=Docker Repository
baseurl=https://yum.dockerproject.org/repo/main/centos/7/
enabled=1
gpgcheck=1
gpgkey=https://yum.dockerproject.org/gpg
EOF
```

4. Install the Docker package by issuing the command:

```
sudo yum install docker-engine
```

5. Set the FQDN of the machine:

```
hostnamectl set-hostname <hostname> --transient
hostnamectl set-hostname <hostname> --static
Add to "/etc/hosts": <ipaddr> <fqdn> <hostname>
```



```
[root@CASB-5 ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
172.17.0.1 CASB-5.cloudapp.net CASB-5
[root@CASB-5 ~]#
```

where <fqdn> is the Cloud Service DNS name from page 17, such as “CASB-5.cloudapp.net”.

6. Start the “firewalld”:

```
systemctl start firewalld
```

7. Enable the service:

```
systemctl enable firewalld
```

8. Start the Docker daemon:

```
service docker start
```

9. Display all Dockers status:

```
systemctl status docker.service
```

10. To ensure Docker starts when you boot your system:

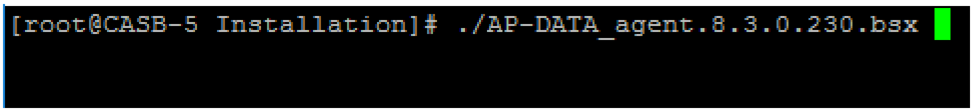
```
systemctl enable docker.service
```

STEP 5: Run the cloud agent installation wizard

This section applies to both Azure and on-premises deployments.

1. On your Linux server, run the Forcepoint installation wizard using the command:

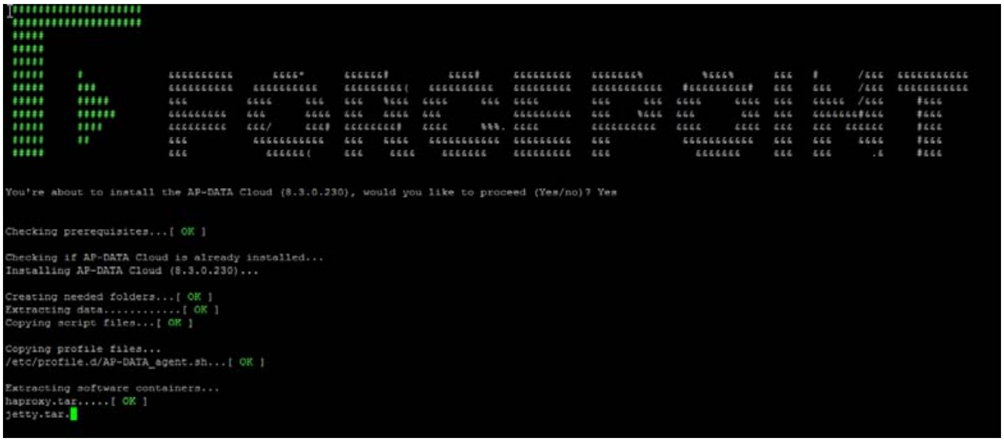
```
./ AP-DATA_agent.8.3.0.nnn.bsx
```



```
[root@CASB-5 Installation]# ./AP-DATA_agent.8.3.0.230.bsx
```

Here, *nnn* is the software build number.

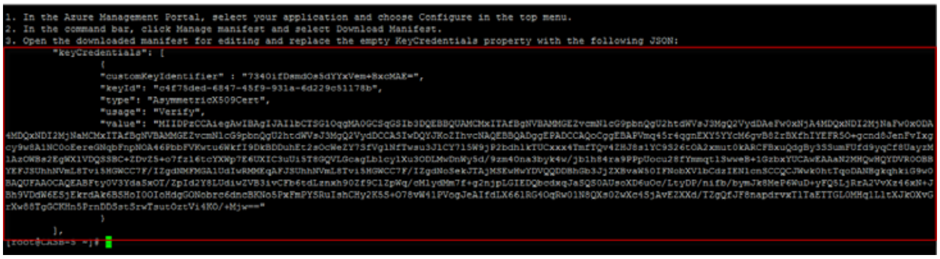
2. You are asked if you want to proceed with the installation. Type **Y**.
3. The installer checks prerequisites and begins installing the module.



```
You're about to install the AP-DATA Cloud (8.3.0.230), would you like to proceed (Yes/no)? Yes

Checking prerequisites...[ OK ]

Checking if AP-DATA Cloud is already installed...
Installing AP-DATA Cloud (8.3.0.230)...

Creating needed folders...[ OK ]
Extracting data............[ OK ]
Copying script files...[ OK ]

Copying profile files...
/etc/profile.d/AP-DATA_agent.sh...[ OK ]

Extracting software containers...
haproxy.tar.....[ OK ]
jetty.tar.
```

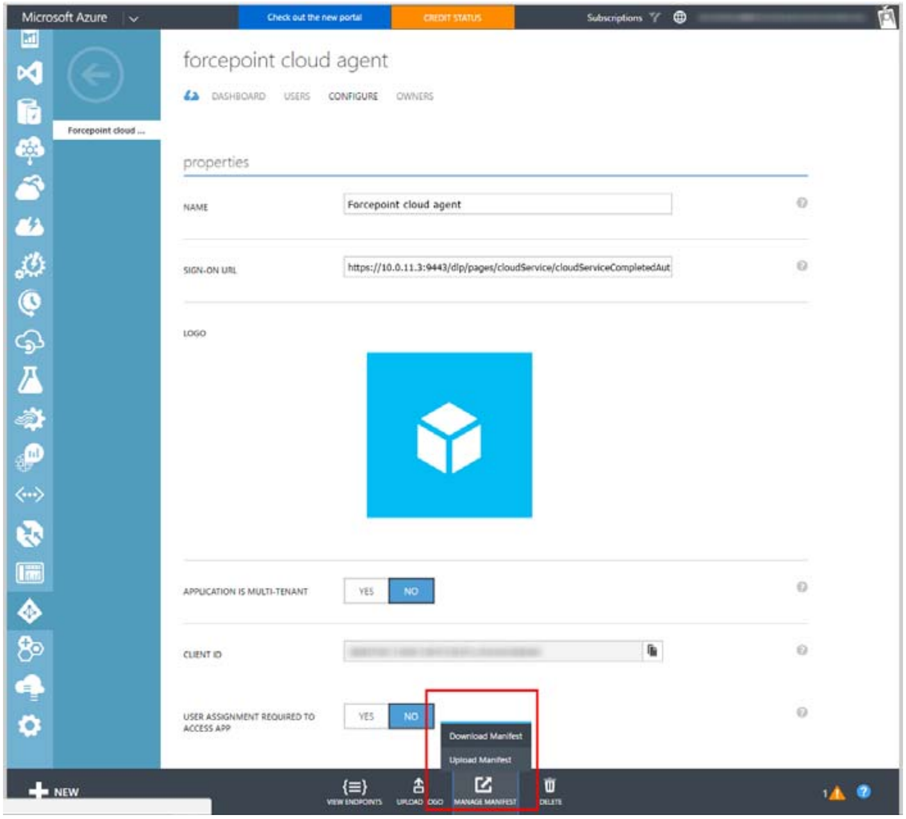
4. Accept the license agreement by typing **Y** when prompted.
5. Enter **Y** if the server will be connecting to an Azure VPN network; **N** if it is connecting to an on-premises server.
6. Enter the IP address or FQDN of the TRITON AP-DATA server to which this cloud agent will connect. This can be the TRITON management server or a supplemental server.
7. Enter the **user name** of the TRITON AP-DATA service account administrator.
8. Enter the account **password**.

   The installer registers the module with the TRITON management server and returns to the command prompt.
9. When prompted, enter your **company name** as listed in Azure Active Directory.
10. Enter the **name of the application** you created in Azure for integration with the TRITON AP-DATA Cloud App Security agent.
11. As instructed, copy the key_credentials.json that appears, including its value.



```
1. In the Azure Management Portal, select your application and choose Configure in the top menu.
2. In the command bar, click Manage manifest and select Download Manifest.
3. Open the downloaded manifest for editing and replace the empty KeyCredentials property with the following JSON:
        "keyCredentials": [
                {
                "customKeyIdentifier" : "7340ifDsmdOs5dYYxVem+8xcMAE=",
                "keyId": "c4f75ded-6847-45f9-931a-6d229c51178b",
                "type": "AsymmetricX509Cert",
                "usage": "Verify",
                "value": "MIIDPzCCAiegAwIBAgIJAIlbCTSG1OqgMA0GCSqGSIb3DQEBBQUAMCMxITAfBgNVBAMMGEZvcmNlcG9pbnQgU2htdWVsJ3MgQ2VydDAeFw0xNjA4MDQxNDI2MjNaFw0xODA
4MDQxNDI2MjNaMCMxITAfBgNVBAMMGEZvcmNlcG9pbnQgU2htdWVsJ3MgQ2VydDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPVmq45r4qgnEXY5YYcM6gvB8ZrBXfhIYEFR5O+gcnd8JenFvIxg
cy9w8A1NC0oEereGNqbFnpNOA46PbbFVKwtu6WkfI9DkBDDuhEt2sOcWeZY7SfVglNfTwsu3J1CY71SW9jP2bdhlkTUCxxx4TmfTQv4ZHJ8s1YC9S26tOA2xmut0kARCFBxuQdgBy3SSumFUfd9yqCf8UayzM
lAzOWBs2EgWX1VDQS3BC+ZDvZ5+o7fzl6tcYXWp7E6UXIC3uUi5T8GQVLGcagLblcy1Xu3ODLMwDnWy5d/9zm40na3byk4w/jb1h84ra9PPpUocu28fYmmqtlSwweB+1GzbxYUCAwEAAaN2MHQwHQYDVR0OBB
YEFJSUhhNVmL8Tvi5MGWCC7F/IZgdNMFMGA1UdIwRMMEqAFJSUhhNVmL8Tvi5MGWCC7F/IZgdNoSekJTAjMSEwHwYDVQQDDBhGb3JjZXBvaW50IFNobXVlbCdzIENlcnSCCQCJWwk0htTqoDANBgkqhkiG9w0
BAQUFAAOCAQEABFty0V3YdaSxOT/ZpId2Y8LUdiwZVB3ivCFb6tdLznxh90Zf9C1ZpWq/cH1ydMm7f+g2njpLGIEDQbcdxqJaSQS0AUsoXD6uOc/LtyDP/nifb/bymJk8MeP6WuD+yFQ5LjRrA2VvXz46xN+J
Bh9VDdW6ESjEkrdAk6BSHoI0OIoHdgGONobrc6dncBKNo5PxFmPY5RuIshCHy2K55+O78vW41PVogJeAIfdLX661RG4OqRw01N8QXs0ZwXc45jAvEZXXd/TZgQfJF8napdrvxT1TaETTGL0MHq1L1tXJk0XvG
rXw88TgGCKHn5PrnDDSstSrwTsutOztVi4K0/+Mjw=="
                }
        ],
[root@CASB-5 ~]#
```

12. Return to the Azure portal. Log back on if needed.
13. Select the application you created and click **Configure**.
14. At the bottom of the screen, select **Manage Manifest** > **Download Manifest**.



forcepoint cloud agent

properties

NAME: Forcepoint cloud agent

SIGN-ON URL: https://10.0.11.3:9443/dlp/pages/cloudService/cloudServiceCompletedAut

LOGO

APPLICATION IS MULTI-TENANT: YES [✓ NO]

CLIENT ID: [redacted]

USER ASSIGNMENT REQUIRED TO ACCESS APP: YES [✓ NO]

15. Click **Download manifest** on the resulting page. Save the file in a convenient location.
16. Open the manifest file for editing and replace the empty “keyCredentials” parameter with the one from the JSON.
17. Save the file.
18. Upload the manifest into Azure by selecting **Manage Manifest** > **Upload Manifest**.

Initial setup

Perform the following required steps to prepare TRITON AP-DATA Cloud App Security for initial use.

Content inspection

1. Log on to the TRITON Manager and click **Data**.
2. Navigate to **Settings** > **Deployment** > **System Modules**.
3. Under **Available Services**, click a service name such as **OneDrive for Business** to configure it.

4. On the resulting page, provide service-related data as requested.
5. You are taken to the cloud service website for additional configuration. When prompted, log on to the service and complete the requested actions.
6. You are returned to the TRITON Manager System Modules page where you can see the configuration status for the service. If all went well, it will say "Configured but not yet deployed."
7. Update the DLP policies and action plans that you want to use for your cloud services.
    a. Select **Main** > **Policy Management** > **DLP Policies** > **Manage Policies**.
    b. From the toolbar, select **More Actions** > **Batch Operation** > **Update Rules of Multiple Policies**.
    c. Indicate whether you want to modify **All rules** or **Selected rules**.
    d. Select the policies or rules that you want to update.
    e. Under Fields to Update, select **Destination**.
    f. Scroll to select the destination, **Cloud Services**.
    g. Click **OK**.
    h. Select **Main** > **Policy Management** > **Resources** > **Action Plans**.
    i. Open an action plan.
    j. Under **Cloud Channels**, select **Permit** or **Delete file** and click **OK**.
    k. Click **OK**.
    l. Click **Deploy**.

Discovery

a. Create a Discovery task for each cloud app of interest.

b. Select **Main** > **Policy Management** > **Discovery Policies** > **Add Network Task**.

c. Select **SharePoint Task**, **Exchange Task**, or **Box Cloud Task**.

d. Proceed through the wizard as prompted.

e. Click **Finish**.

f. Select **Main** > **Policy Management** > **Resources** > **Action Plans**.

g. Open an action plan.

h. Select the **Discovery** tab.

i. Indicate whether you want to run a remediation script when an incident is discovered.

j. Click **OK**.

k. Click **Deploy**.

Mobile agent

In this topic:

The mobile agent is a Linux-based appliance that lets you secure the type of email content that is synchronized to users' mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

The mobile agent analyzes content when users synchronize their mobile devices to your organization's Exchange server. If content or data being pushed to their device breaches the organization's mobile DLP policy, it is quarantined or permitted accordingly.

The mobile agent is included with TRITON AP-EMAIL, TRITON AP-ENDPOINT, and TRITON AP-DATA Gateway.

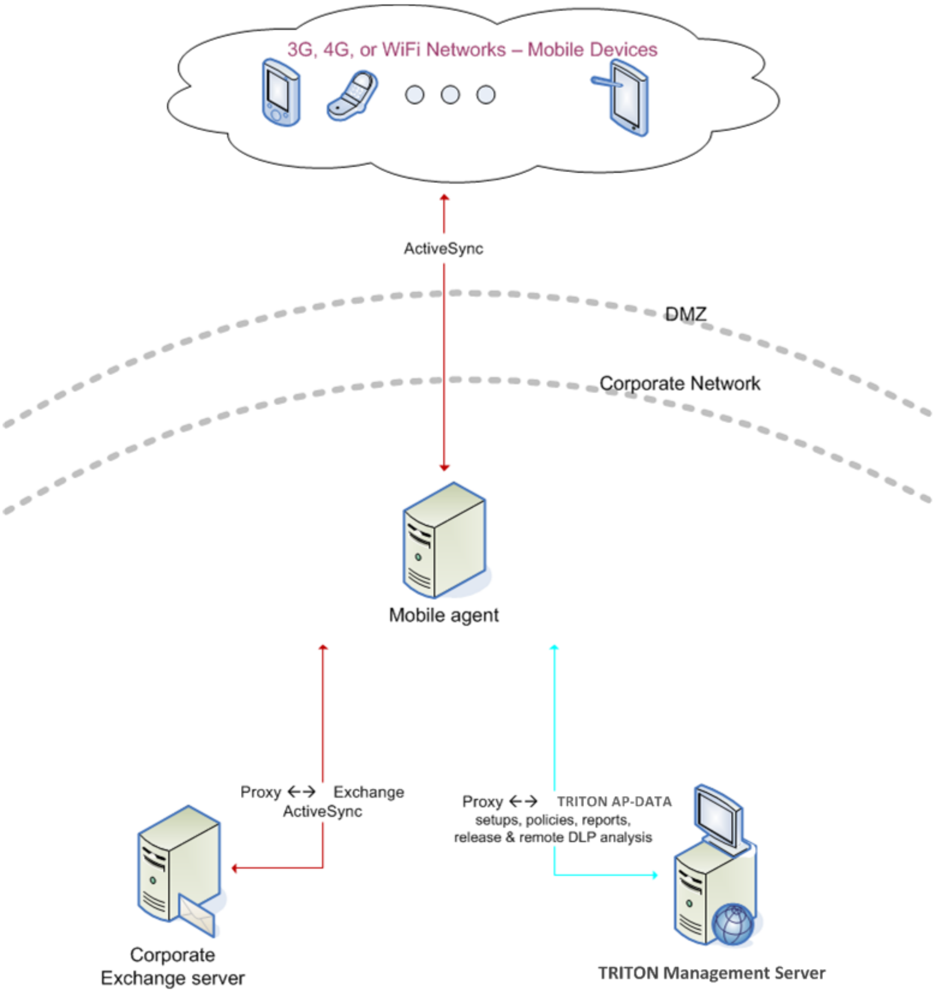
Deploying the mobile agent

The appliance connects to the TRITON management server and to your Microsoft Exchange server. DLP analysis is done on the appliance or on other TRITON AP-DATA servers (rather than on the management server) to optimize performance and balance the load.

Outside your DMZ, the mobile agent connects to any Microsoft ActiveSync-compatible mobile device over 3G and wireless networks, such as iPads, Android mobile phones, and iPhones. (ActiveSync is a wireless communication protocol used to push resources, such as email, from applications to mobile devices.)

Unlike the protector, the mobile agent appliance acts as a reverse proxy, because it retrieves resources, such as email, from the Exchange server on behalf of the mobile device.

The following diagram illustrates the system architecture of a typical mobile agent deployment. Depending on your network and security requirements, you can also go through an edge device that acts as a reverse proxy to the mobile agent.


3G, 4G, or WiFi Networks – Mobile Devices
ActiveSync
DMZ
Corporate Network
Mobile agent
Proxy ←→ Exchange ActiveSync
Proxy ←→ TRITON AP-DATA setups, policies, reports, release & remote DLP analysis
Corporate Exchange server
TRITON Management Server

For system requirements, see *Hardware and operating system requirements*, page 118.

For the default port numbers used by the mobile agent, see *Hardware and operating system requirements*, page 118. If you have a security policy in place, exclude these ports from that policy so the mobile agent can operate properly. You can lock down or harden your security systems once these ports are open.

Deploying the TRITON AP-DATA mobile agent comprises the following basic steps:

1. *Installing the mobile agent software*, page 119
2. *Configuring the mobile agent*, page 129
3. *Configuring a mobile DLP policy*, page 130

Mobile agent installations include:

- A policy engine

- Secondary fingerprint repository (the primary is on the management server)

Hardware and operating system requirements

The mobile agent is a soft appliance that runs on **CentOS 7**.

If you are using your own hardware, it must meet the following hardware requirements:

	Minimum requirements	**Recommended**
CPU	4 core processors (for example, Single quad or two dual core processors), 2.0 GHz Intel Xeon or AMD equivalents	4 core processors (for example, Single quad or two dual core processors), 2.0 GHz Intel Xeon or AMD equivalents
Memory	8 GB	8 GB
Hard drives	2 - 72 GB	4 - 146 GB
Disk space	70 GB	292 GB
Hardware RAID	1	1 + 0
NICs	2	2

Port requirements

Outbound		
To	**Port**	**Purpose**
TRITON management server	17443	Syslog, forensics, incidents, mobile status
TRITON management server	80	Fingerprint sync
TRITON management server Server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
Microsoft Exchange Server	80/443	ActiveSync (user defined using the Data Security manager)
TRITON AP-WEB	56992	Linking Service
Other	UDP 123	Inbound/ outbound NTPD (available on the appliance yet disabled by default)
* This range is necessary for load balancing.		
Inbound		
From	**Port**	**Purpose**
TRITON management server	5820	Settings deployment

Mobile Devices	80/443	ActiveSync (user defined using the Data Security manager)
TRITON management server	8892	Management
TRITON management server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
Any service (including the mobile agent) that is not using logging on	22	SSH access
TRITON AP-DATA Server	5443	Release quarantined messages
* This range is necessary for load balancing.		

Installing the mobile agent software

The mobile agent must be installed on hardware that meets the requirements described in *Hardware and operating system requirements*, page 118. Forcepoint appliances meet these requirements, or you can host the agent on your own CentOS 7-based hardware.

Note

For best performance, make sure that the mobile agent is located in close proximity to the back-end server.

You access the installation wizard for your mobile agent through a putty Command Line Interface (CLI).

To install the mobile agent, do the following:

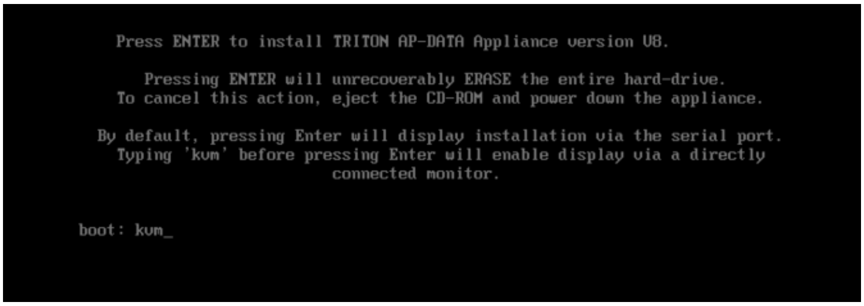
1. If you have purchased a Forcepoint TRITON AP-DATA Appliance, follow the instructions on its quick start poster to rack, cable, and power on the appliance. If you are using your own hardware:
   a. Use either a direct terminal or connect via serial port to access the command line. For serial port connection, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:
      - 19200 baud
      - 8 data bits
      - no parity
      - 1 stop bit
      - no flow control

   b. The mobile agent software is provided on an ISO image. Download the image, **DataProtectorMobile83x.iso**, from My Account and burn it to a CD or bootable USB.

   c. Place the media in the machine’s CD drive or USB port and restart the machine.

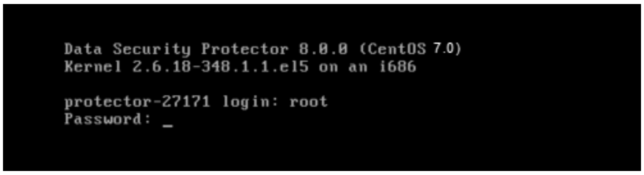
   d. An installer page appears. Press **Enter** and the machine is automatically restarted a second time.

2. A welcome screen appears:



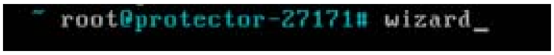
```
        Press ENTER to install TRITON AP-DATA Appliance version V8.

           Pressing ENTER will unrecoverably ERASE the entire hard-drive.
        To cancel this action, eject the CD-ROM and power down the appliance.

      By default, pressing Enter will display installation via the serial port.
        Typing 'kvm' before pressing Enter will enable display via a directly
                                connected monitor.


    boot: kvm_
```

3. You’re prompted to enter a user name and password. Enter **root** for user name and **admin** for password.



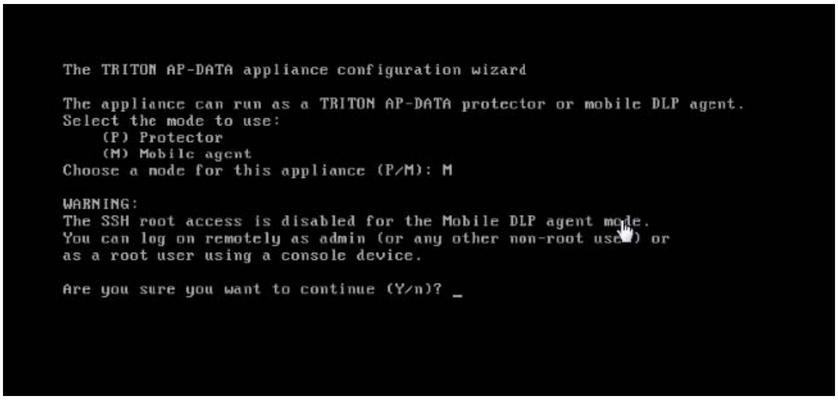
```
Data Security Protector 8.0.0 (CentOS 7.0)
Kernel 2.6.18-348.1.1.el5 on an i686

protector-27171 login: root
Password: _
```

4. To access the wizard, type **wizard** at the command prompt, and press **Enter**.



```
~ root@protector-27171# wizard_
```

5. You have the option to install the Forcepoint protector software or mobile agent software. Type **M** for Mobile agent.



```
The TRITON AP-DATA appliance configuration wizard

The appliance can run as a TRITON AP-DATA protector or mobile DLP agent.
Select the mode to use:
    (P) Protector
    (M) Mobile agent
Choose a mode for this appliance (P/M): M

WARNING:
The SSH root access is disabled for the Mobile DLP agent mode.
You can log on remotely as admin (or any other non-root user) or
as a root user using a console device.

Are you sure you want to continue (Y/n)? _
```

6. Follow the instructions given by the wizard to configure basic settings.

   When the wizard requires data entry, it prompts you. In some cases, a default setting is provided:

   - Capital letter: Shows the default value, such as Yes/no for a yes/No prompt.
   - Square brackets ([ ]): Shows the current value and is usually followed by text, such as: Press [Enter] to leave as is.

   If the default setting is acceptable, press <Enter> to keep the default value.

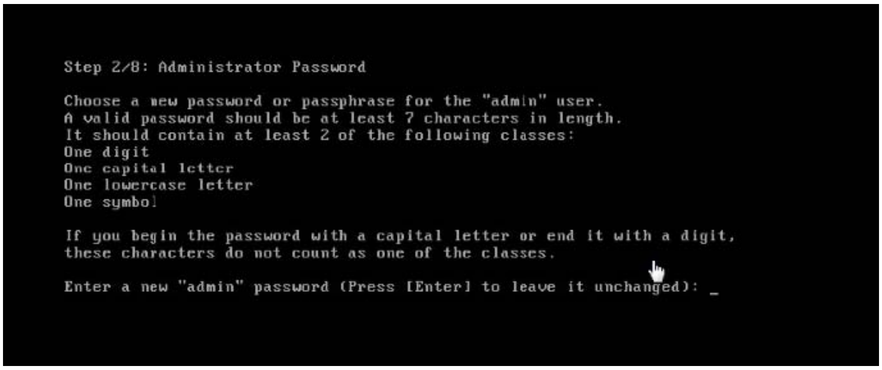
STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down/ scroll / space keys to read/scroll to the end of the agreement.

Carefully read the license agreement and when prompted, type yes to accept the license agreement.

STEP 2: Set administrator password

Type in and confirm a new password for the “admin” account. For security reasons, it is best practice to change the default password.



```
Step 2/8: Administrator Password

Choose a new password or passphrase for the "admin" user.
A valid password should be at least 7 characters in length.
It should contain at least 2 of the following classes:
One digit
One capital letter
One lowercase letter
One symbol

If you begin the password with a capital letter or end it with a digit,
these characters do not count as one of the classes.

Enter a new "admin" password (Press [Enter] to leave it unchanged): _
```

Important

A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

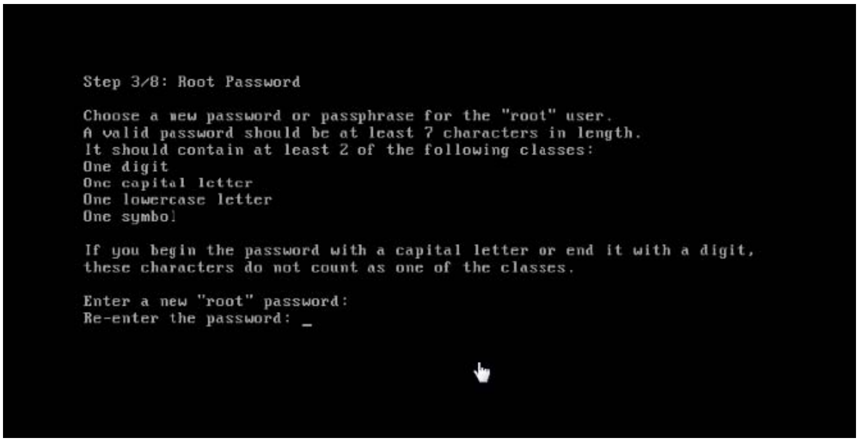
- One digit
- One symbol
- One capital letter
- One lowercase letter

If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

The operating system (OS) prompts you to change (refresh) your password every 90 days.

STEP 3: Set root password

Type in and confirm a new password for the root user. The root account provides full access to the device and should be used carefully.



```
Step 3/8: Root Password

Choose a new password or passphrase for the "root" user.
A valid password should be at least 7 characters in length.
It should contain at least 2 of the following classes:
One digit
One capital letter
One lowercase letter
One symbol

If you begin the password with a capital letter or end it with a digit,
these characters do not count as one of the classes.

Enter a new "root" password:
Re-enter the password: _
```

Important

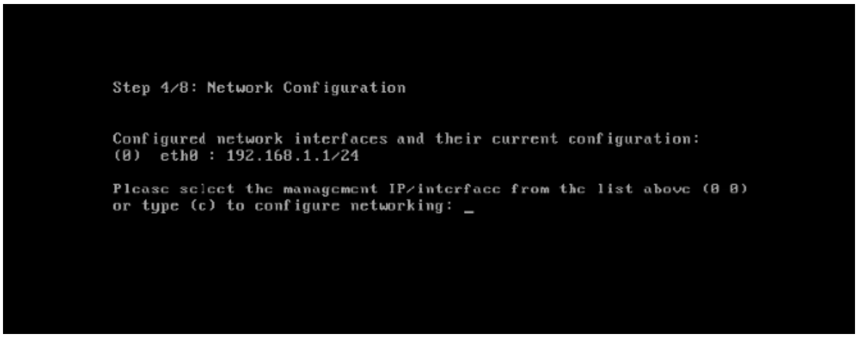
A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

- One digit
- One symbol
- One capital letter
- One lowercase letter

If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

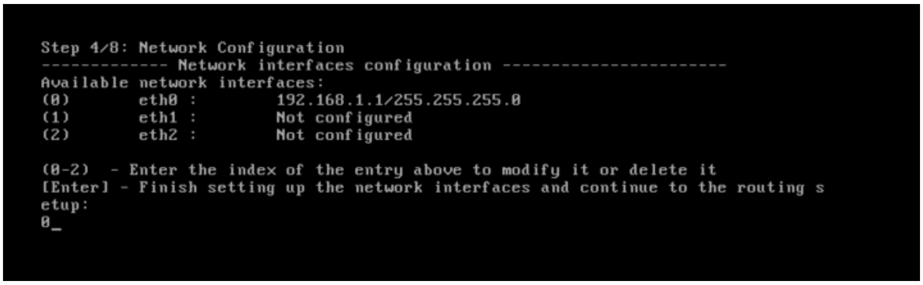
STEP 4: Network configuration

1. Select the network interface (NIC) from the list of available NICs (eth0 by default), or for advanced configuration, type c.



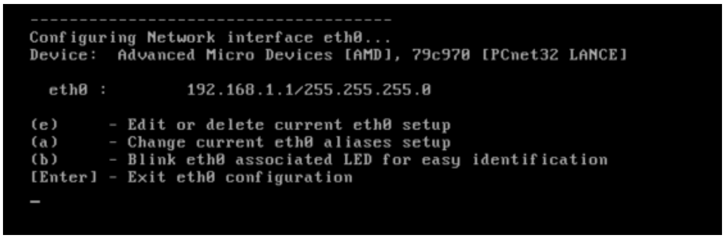
```
Step 4/8: Network Configuration


Configured network interfaces and their current configuration:
(0)  eth0 : 192.168.1.1/24

Please select the management IP/interface from the list above (0 0)
or type (c) to configure networking: _
```

2. To configure your NIC, choose the NIC index number from the list of NICs that display on the wizard.



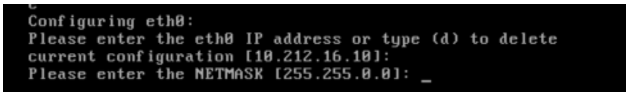
```
Step 4/8: Network Configuration
------------ Network interfaces configuration ----------------------
Available network interfaces:
(0)       eth0 :        192.168.1.1/255.255.255.0
(1)       eth1 :        Not configured
(2)       eth2 :        Not configured

(0-2)  - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing s
etup:
0_
```

3. To configure the NIC that you selected, do one of the following:
   a. Type e to configure the NIC that you selected. You are prompted to define details for the NIC, such as IP address, network address, and gateway (only for the first NIC that you define). You do not need to specify the gateway for subsequent NICs that you want to define.
   b. Type a to change the current NIC alias address setup.
   c. Type b for LEDs to blink on that port.
   d. Type Enter to exit and continue setting other NICs, if required.



```
-------------------------------------
Configuring Network interface eth0...
Device:  Advanced Micro Devices [AMD], 79c970 [PCnet32 LANCE]

  eth0 :        192.168.1.1/255.255.255.0

(e)      - Edit or delete current eth0 setup
(a)      - Change current eth0 aliases setup
(b)      - Blink eth0 associated LED for easy identification
[Enter]  - Exit eth0 configuration
_
```

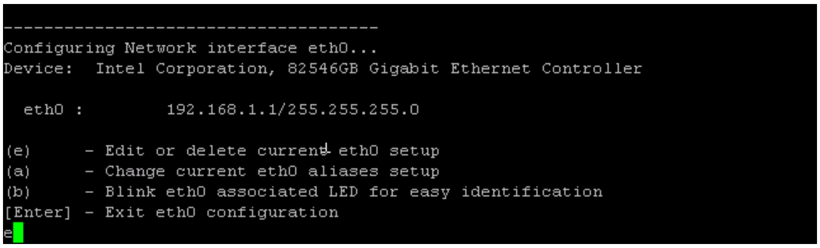
4. To define the properties for the NIC:
   a. Type the IP address.
   b. Type the network prefix. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 255.255.255.0 for eth0.



```
Configuring eth0:
Please enter the eth0 IP address or type (d) to delete
current configuration [10.212.16.10]:
Please enter the NETMASK [255.255.0.0]: _
```

   c. If prompted, type the IP address for the default gateway to be used to access the network. This configuration is only for the first NIC that you configured.

d. After you have configured your NIC, you can redefine it (change the IP address, network prefix, or gateway) or remove it (type e, then d) if necessary.

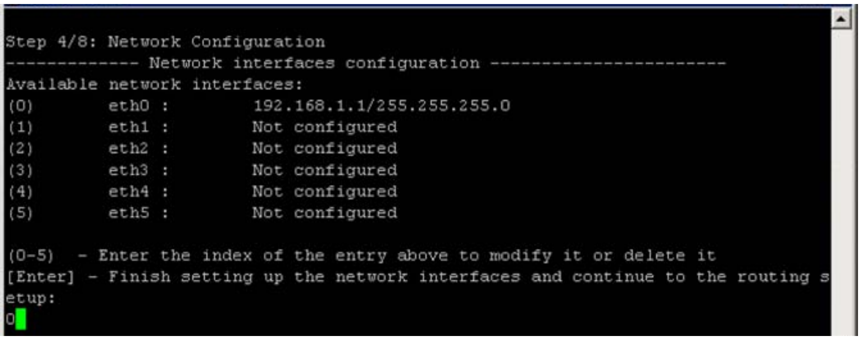


```
-------------------------------------
Configuring Network interface eth0...
Device:  Intel Corporation, 82546GB Gigabit Ethernet Controller

  eth0 :        192.168.1.1/255.255.255.0

(e)     - Edit or delete current eth0 setup
(a)     - Change current eth0 aliases setup
(b)     - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration
e
```

Note

If you type **Enter**, a list of available NICs display, allowing you to define other NICs.

e. Type a NIC index number to configure another NIC (or reconfigure the same NIC), or type Enter to finish setting up the NICs and continue to the routing setup.

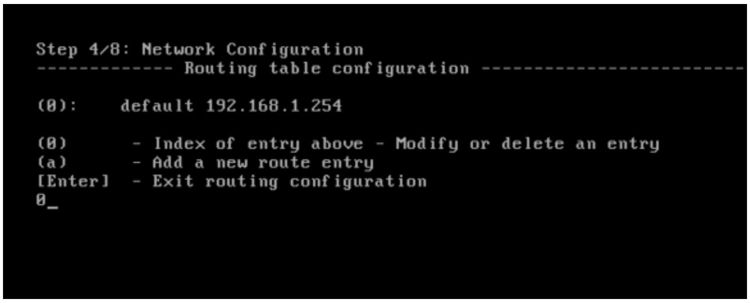


```
Step 4/8: Network Configuration
------------- Network interfaces configuration -----------------------
Available network interfaces:
(0)       eth0 :        192.168.1.1/255.255.255.0
(1)       eth1 :        Not configured
(2)       eth2 :        Not configured
(3)       eth3 :        Not configured
(4)       eth4 :        Not configured
(5)       eth5 :        Not configured

(0-5)   - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing s
etup:
0
```

f. Type one of the following options:

- Enter: Accept the routing configuration.
- Index: Modify or delete a routing entry index.

○ a: Add a routing entry.

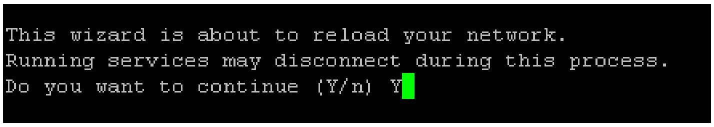


```
Step 4/8: Network Configuration
------------- Routing table configuration -------------------------

(0):     default 192.168.1.254

(0)       - Index of entry above - Modify or delete an entry
(a)       - Add a new route entry
[Enter]   - Exit routing configuration
0_
```

Note

If the IP address of the TRITON AP-DATA server is not on the same subnet as the one specified for the mobile management NIC, a gateway is required to tell the mobile agent how to communicate with the TRITON AP-DATA server.

g. To store these network definitions, type Y.



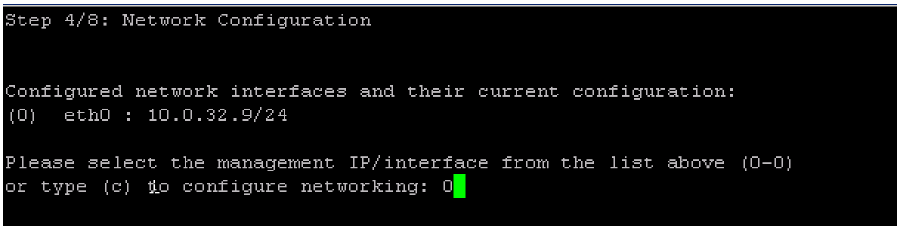
```
This wizard is about to reload your network.
Running services may disconnect during this process.
Do you want to continue (Y/n)  Y
```

Note

After you finish routing the configuration, you are prompted to store the network configuration.

- If you type **n**, the network configuration is not saved, and you are prompted to configure the network again.
- If you type **y**, the details for the network configuration are saved and the network service is reloaded with the new parameters. The new parameters, such as IP address, network prefix, and gateway for the NIC display on the wizard.

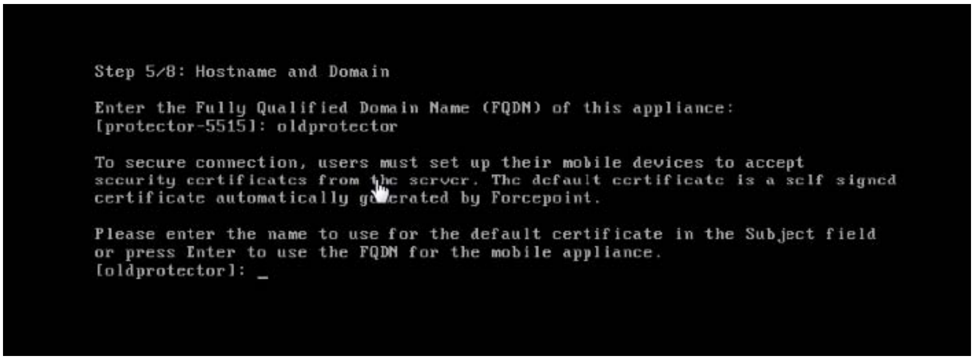
5. Type the index number of the Management NIC you have chosen, or type c to define the network parameters. This NIC can be used for other purposes, such as SSH connections, access points for mobile devices, and Exchange communications.



```
Step 4/8: Network Configuration


Configured network interfaces and their current configuration:
(0)  eth0 : 10.0.32.9/24

Please select the management IP/interface from the list above (0-0)
or type (c) to configure networking: 0
```

STEP 5: Define the host name

1. Type the Fully Qualified Domain Name (FQDN) for the mobile appliance.



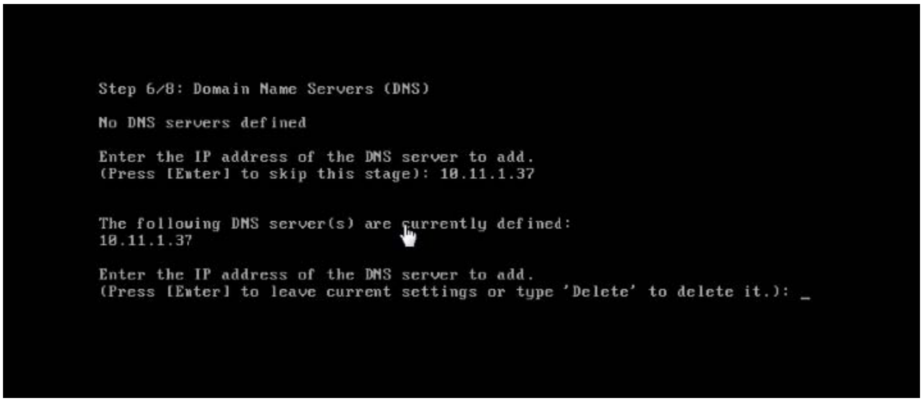
```
Step 5/8: Hostname and Domain

Enter the Fully Qualified Domain Name (FQDN) of this appliance:
[protector-5515]: oldprotector

To secure connection, users must set up their mobile devices to accept
security certificates from the server. The default certificate is a self signed
certificate automatically generated by Forcepoint.

Please enter the name to use for the default certificate in the Subject field
or press Enter to use the FQDN for the mobile appliance.
[oldprotector]: _
```

2. Type the name to use for the default security certificate in the Subject field.

   This can be used to secure the connections between mobile devices and the mobile agent using the default certificate. The default certificate is a self-signed certificate automatically generated by Forcepoint.

STEP 6: Define the domain name server

Optionally, in the wizard, type the IP address of the Domain Name Server (DNS) that will service this mobile agent. A DNS will allow access to other network resources using their names instead of their IP addresses.



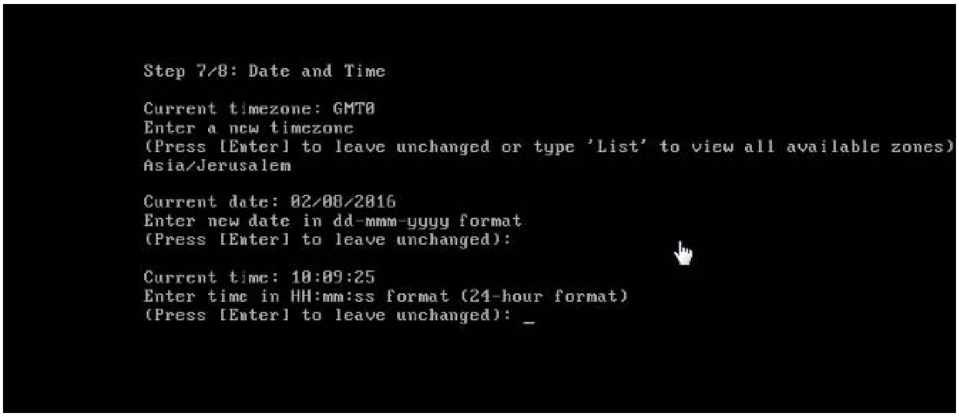
```
Step 6/8: Domain Name Servers (DNS)

No DNS servers defined

Enter the IP address of the DNS server to add.
(Press [Enter] to skip this stage): 10.11.1.37


The following DNS server(s) are currently defined:
10.11.1.37

Enter the IP address of the DNS server to add.
(Press [Enter] to leave current settings or type 'Delete' to delete it.): _
```

Important

Type the IP address of the DNS server if you identify the back-end Exchange server by its host name (using the TRITON AP-DATA GUI) instead of by its IP address.

STEP 7: Set the date, time, and time zone

1. Type the current time zone (to view a list of all time zones, type **list**).
2. Type the current date in the following format: dd-mm-yyyy.
3. Type the current time in the following format: HH:MM:SS. Note that this is a 24-hour clock.

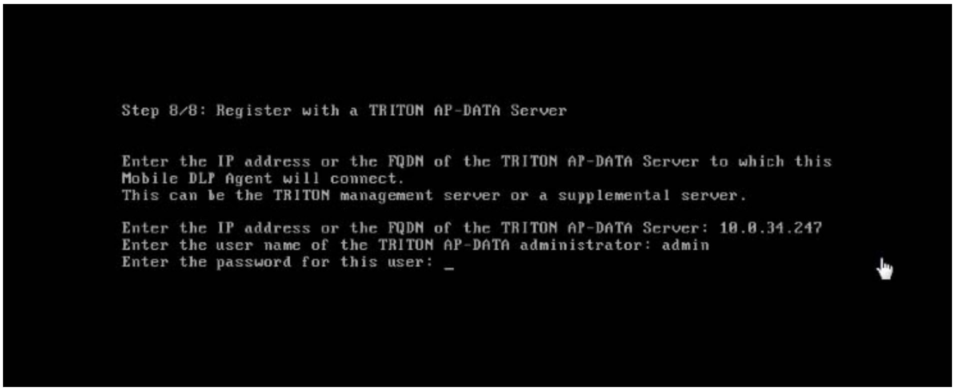


```
Step 7/8: Date and Time

Current timezone: GMT0
Enter a new timezone
(Press [Enter] to leave unchanged or type 'List' to view all available zones)
Asia/Jerusalem

Current date: 02/08/2016
Enter new date in dd-mmm-yyyy format
(Press [Enter] to leave unchanged):

Current time: 10:09:25
Enter time in HH:mm:ss format (24-hour format)
(Press [Enter] to leave unchanged): _
```

STEP 8: Register with a TRITON AP-DATA Server

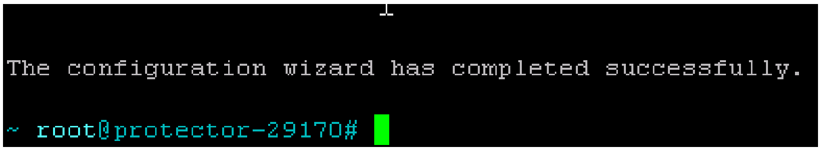
In this step, a secure channel will be created connecting the mobile agent to a TRITON AP-DATA Server. This can be the TRITON management server or a supplemental server, depending on your set up.

1. Type the IP address or FQDN of the TRITON AP-DATA Server. Note that this must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.



```
Step 8/8: Register with a TRITON AP-DATA Server

Enter the IP address or the FQDN of the TRITON AP-DATA Server to which this
Mobile DLP Agent will connect.
This can be the TRITON management server or a supplemental server.

Enter the IP address or the FQDN of the TRITON AP-DATA Server: 10.0.34.247
Enter the user name of the TRITON AP-DATA administrator: admin
Enter the password for this user: _
```

2. Type the user name and password for a TRITON AP-DATA administrator that has privileges to manage system modules.
3. Type Enter to exit the wizard. A message displays stating that the configuration was successful.



```
The configuration wizard has completed successfully.

~ root@protector-29170#
```

Step 9: Reboot the mobile agent appliance

For best practice, reboot the mobile agent appliance. You can reboot later if desired. This completes the IPv6 disabling process that the wizard starts.

Final step: Verification

In the TRITON AP-DATA module of TRITON Manager, verify that the Forcepoint mobile agent is no longer pending and that the icon displays its active status. Refresh the browser.

Click **Deploy**.

The mobile agent is now ready to be configured. See *Configuring the mobile agent*, page 129 for instructions.

Note

If you reboot, make sure that the mobile agent appliance is on before you configure the mobile agent.

Configuring the mobile agent

1. Log on to the Data Security manager.
2. Navigate to **Settings** > **Deployment** > **System Modules**.
3. Verify that the mobile agent is available on the System Modules page.
4. Double-click Mobile agent.
5. Click the Connection tab, then define the connections: Exchange and Mobile Devices. For more information, see the Data Security Manager Help.

   a. For Exchange Connection, supply the domain and name or IP address of the Exchange server. Ensure a port number is specified.

      ○ If you select the Use secure connection (SSL) check box, the port number defaults to 443.

      ○ If you do not select the Use secure connection (SSL) check box, the port number defaults to 80.

   Important

   If the Exchange server is specified by name, make sure local resolving is properly configured to resolve this name. In addition, if an edge-like device is used, ensure there are no loops through the device.

   b. For Mobile Devices Connection, supply the following information: IP address of the mobile agent and port number. To use all IP addresses, select All IP addresses from the IP address drop-down list.

   Note

   The IP address of the mobile agent was defined during the installation of the mobile device, when configuring the network settings.

6. Optionally, if you secure connections between mobile devices and the mobile agent, you can use one of 2 certificate options:

   ■ Self-signed certificate (default option)

      ○ A self-signed certificate is signed by Forcepoint.

   ■ Custom certificate

      ○ A custom certificate is officially signed by a Certificate Authority (CA).

      a. Click Browse to locate and upload your public certificate.

      b. Click Browse to locate and upload your private key.

      c. Optionally, select the Add chained certificate check box, and click Browse to locate and upload your chained certificate.

   For more information, see the Data Security Manager Help.

7. Click the Analysis tab and then select a mode: Blocking or Monitoring. Click the Analysis tab, then configure the Mode.

Note

When you select Blocking mode, it is best practice to:

- Select the **Allow on fail** option (the default option is **Block on fail**). Selecting **Allow on fail** enables failed messages to be received on the mobile device. If you do not select **Allow on fail**, these messages will be dropped and are not tracked nor released.
- Define the sender's email address, outgoing mail server, and port to **Notify Users of Breach**. To do so, navigate to **Settings** > **General** > **Alerts** > **Email Properties**.

For more information, see the Data Security Manager Help.

8. Navigate to **Main** > **Policy Management** > **Resources** > **Notifications** and select the mobile policy violation template. Add sender details, then use the Outgoing mail server field to define a next hop relay for outbound mail. If you do not, the mobile agent may not send block notifications.
9. Click **Deploy**.

   Wait for the agent to fully deploy. This may take a few minutes.

Tip

You can also configure the mobile agent for high-availability. High-availability enables mobile devices to run seamlessly and continuously in the event of a system outage (such as hardware or software failure).

For more information about configuring the mobile agent for high-availability, refer to the document Mobile DLP agent using cluster solutions.

Configuring a mobile DLP policy

To begin analysis, configure the mobile DLP policy or create a custom policy. To configure the mobile DLP policy, navigate to **Main** > **Policy Management** > **DLP Policies** > **Mobile DLP Policy**. See the Data Security Manager Help for more configuration information.

To create a custom policy, navigate to **Main** > **Policy Management** > **DLP Policies** > **Add Custom Policy**. Select **Mobile Email** on the Destination tab for each rule to support Mobile events.

Integration agent

In this topic:

The integration agent allows third-party products to send data to TRITON AP-DATA for analysis.

Third parties can package the integration agent inside their own installer using simple, 'industry standard' methods that are completely transparent to end users.

When the third-party product is installed on a users system, it needs to register the integration agent with the TRITON management server. This can be done transparently through the installation process or using a command-line utility.

The integration agent works on Windows Server, 64-bit machines.

The system treats third-party products that use the integration agent as it does any other agent.

It supports all relevant views and capabilities, including:

- Incident Management and Reporting
- Quarantine and Release of emails
- Traffic log view
- Load balancing capabilities

For information on configuring the integration agent, see “Configuring the integration agent” in the Data Security Manager Help system.

Installing the integration agent

Installed components

When you embed the integration agent in your product installer, 3 TRITON AP-DATA components are installed on the end-user machine:

- PEInterface.dll - A DLL the that interacts with the TRITON AP-DATA policy engine on the management server.
- ConnectorsAPIClient.exe - Client software that connects the API in the third-party product with TRITON AP-DATA.
- registerAgent.bat (or .vbs) - A script that performs registration with the TRITON management server.

Installation package format

On Windows, the installation package for the integration agent is provided as an MSI file. The MSI installation wizard presents 4 interactive dialogs:

- Installation-dir - installation directory.
- Registered Channels - The DLP channels to use: HTTP, SMTP, Printer, Discovery.
- Local IP Address - which of the static IP addresses currently assigned to the machine should be used for registration.
- TRITON management server details - IP address or host name, user name, password.

Registering the integration agent

Every instance of the integration agent needs to be registered after being installed. (This is a one time operation.) In other words, every time the third-party product is installed on an end-user machine, that instance of the agent needs to be registered.

The registration operation can be done during the installation by the installer, or using a command-line utility provided with the agent.

The command-line utility should receive the following input arguments:

- Protocols - a non-empty list of supported protocols (out of HTTP, SMTP, Printer, Discovery).
- TRITON management server details - IP address or host name, user name, password.
- Local IP Address (optional) - In case this is not supplied, use any of the static addresses of the machine, and print it to the standard output.
- Search IP Address (optional) - used for re-registration after IP change. In case this is not supplied, use the address in the registerAgent.conf file. If that file does not exist, use the given local IP address.

A successful operation registers the machine with the TRITON management server as having the desired protocols and generates certificate files in the same directory that the tool is located. The tool also stored a configuration file (registerAgent.conf) with the IP address used for registration.

On failure, the script returns a meaningful exit code and prints an error message to standard output

Using the TRITON AP-DATA API

Third parties that subscribe to the integration agent use a C-based API to send data to TRITON AP-DATA for analysis and receive dispositions in return.

The API can be used to configure analysis operations on a transaction-by-transaction basis on the following variables:

- Channel/Protocol - Upon installation the third-party product can declare its ability to intercept various protocols, and assign each transaction to a protocol.
- Blocking/Monitoring mode - each transaction can work in a different mode.
- Timeout - can be different per transaction.

For documentation on the TRITON AP-DATA API, consult with your Forcepoint Sales representative.

The crawler

In this topic:

The crawler is the name of the discovery and fingerprinting agent. It is selected by default when you install the TRITON management server or supplemental TRITON AP-DATA servers.

You can deploy additional crawlers in your network if you desire. When you set up a fingerprint task, you indicate which crawler should perform the scan. Forcepoint recommends that you use the crawler that is located closest to the data you are scanning.

You can view the status of your crawlers in the Data Security manager user interface. Go to **Settings** > **Deployment** > **System Modules**, select the crawler and click **Edit**.

Operating system requirements

Crawler machines must be running on one of the following operating system environments:

- Windows Server 2008 (64-bit) Standard or Enterprise R2 SP1
- Windows Server 2012 Standard Edition (64-bit)

Port requirements

The following ports must be kept open for the crawler:

Outbound		
To	**Port**	**Purpose**
TRITON management server	443	Secure communication

TRITON AP-DATA Server	17500-17515*	Consecutive ports that allow communication with Forcepoint agents and machines.
Internet	443	Salesforce fingerprinting
* This range is necessary for load balancing.		
Inbound		
From	**Port**	**Purpose**
TRITON management server	9797*	Crawler listening
* This is only for the standalone crawler agent.		

Installing the crawler agent

1. Download the TRITON installer (**TRITON83xSetup.exe**) from My Account.
2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for TRITON AP-DATA.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

   The default destination is C:\Program Files *or* Program Files (x86)\Websense\Data Security. If you have a larger drive, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.

   Important

   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   Note

   Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive.

8. On the **Select Components** screen, select **Crawler agent** and then **Entire feature will be installed on local hard drive**. If this is a stand-alone installation, deselect all other options, including TRITON AP-DATA Server.
9. In the **Server Access** screen, select the IP address to identify this machine to other Forcepoint components.

   The following message may appear:

TRITON AP-DATA Discovery Agent works with a specific version of WinPcap.
The installation has detected that your WinPcap version is <version>
In order to proceed with this installation, WinPcap version 4.0.0.1040 needs to be installed and will replace yours.
Click Yes to proceed or Click No to preserve your WinPcap version and deselect the Discovery Agent Feature to continue with the installation.

"Discovery Agent" refers to the crawler agent. The particular version of WinPcap mentioned in this message must be in place to install Crawler Agent. Note that after installation of the crawler agent you can install a different version of WinPcap. The crawler agent should continue to work properly.

10. In the **Register with the TRITON AP-DATA Server** screen specify the path and log on credentials for the TRITON AP-DATA server to which this agent will connect. This could be the TRITON management server or a secondary TRITON AP-DATA server.

    FQDN is the fully-qualified domain name of a machine.

11. In the **Local Administrator** screen, enter a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.

12. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, the **Lotus Domino Connections** screen appears.

    If you plan to perform fingerprinting or discovery on your Domino server, complete the information on this page.

    > **Important**
    >
    > Before you complete the information on this screen, make sure that you:
    >
    > - Create at least one user account with administrator privileges for the Domino environment. (Read permissions are not sufficient.)
    > - Be sure that the Lotus Notes installation is done for "Anyone who uses this computer."
    > - Connect to the Lotus Domino server from the Lotus Notes client.

    a. On the **Lotus Domino Connections** page, select the check box labeled **Use this machine to scan Lotus Domino servers**.

b. In the **User ID file** field, browse to one of the authorized administrator users, then navigate to the user's **user.id** file.

> ✓ **Note**
> Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

c. In the **Password** field, enter the password for the authorized administrator user.

13. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

    Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.

    If the following message appears, click **Yes** to continue the installation:

    TRITON AP-DATA needs port 80 free.
    In order to proceed with this installation, DSS will free up this port.
    Click Yes to proceed OR click No to preserve your settings.

    Clicking **No** cancels the installation.

    A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.

14. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.
15. Once installation is complete, the **Installation Successful** screen appears to inform you that your installation is complete.

For information on configure the crawler, see "Configuring the crawler" in the Data Security Manager Help system.

Troubleshooting TRITON AP-DATA agent installation

In this topic:

Though the installation and deployment of agents is normally a series of clear-cut steps, occasionally, some problems can arise. Below are how to resolve common problem scenarios.

Initial registration fails

- Make sure you can ping the TRITON AP-DATA agents by IP and by host name from the TRITON Management Server.
  - On Windows, run the following command (in a Command Prompt) to check for block ports:

    ```
    netstat 1 -na | find "SYN"
    ```

    Each line displayed in response to the command is a blocked port. This command is one-way. Run it on both the agent machine and the TRITON Management Server.
- Check logs on the TRITON Management Server (and remote policy engines).
  - %dss_home%/logs/mgmtd.log
  - %dss_home%/tomcat/logs/dlp/dlp-all.log
- Check logs on the protector. These reside in the /opt/websense/neti/log directory. In particular, check:
  - /opt/websense/neti/log/registration.log
- Make sure no duplicate certificates are installed on the agents' servers; if there are duplications, delete all of them and re-register the agent. Also, make sure the system date/time of the agent machine and the TRITON Management Server are the same. The following certificates are expected:

  Certificate > My User Account > Trusted Root Certification Authorities > Certificates > ws-ilp-ca

  Certificates > Computer > Personal Certificates ><servername>(issued by ws-ilp-ca)

  Certificates > Computer > Trusted Root Certification Authorities > Certificates > ws-ilp-ca
- Make sure the FQDN value of the agent states the full server name for the agent's server.

  Protector — if domain name is configured, the FQDN is: protectorname.domain.name

  Agents and TRITON AP-DATA server — check "My Computer" properties and copy the computer name value from there.

Deploy settings fails

- Make sure you can ping the agents by IP and by host name from the TRITON Management Server.
- Check logs on the TRITON Management Server (and remote policy engines).
  - %dss_home%/tomcat/logs/dlp/dlp-all.log
  - %dss_home%/tomcat/logs/dlp/deployment-trace.log
- Check the plat.log on the protector.

Subscription errors

- Restart the Forcepoint TRITON - Data Security service on the TRITON Management Server.
- Check %dss_home%/tomcat/logs/dlp/dlp-all.log.

3 Adding, Modifying, or Removing Components

In this topic:

This chapter contains instructions for adding, modifying, or removing TRITON AP-DATA components.

Adding or modifying TRITON AP-DATA components

1. Start the TRITON installer:
   - If you chose to keep installation files after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for TRITON AP-DATA.
3. From the installation wizard, select **Modify**.

   This enables you to review the TRITON AP-DATA installation screens, making modifications to settings—with the exception of username—as necessary.

   To add components, select them on the **Select Components** screen.

   Also, refer to the following sections for the most common TRITON AP-DATA modify procedures:
   - *Recreating TRITON AP-DATA certificates*, page 140
   - *Repairing TRITON AP-DATA components*, page 140
   - *Changing the TRITON AP-DATA service account*, page 141

Recreating TRITON AP-DATA certificates

From the Modify menu, you can also re-certify the server. This is not recommended except in extreme security breaches. When you recreate security certificates, you must re-register all agents and servers (see Re-registering TRITON AP-DATA components, for instructions), and repeat the Reestablish Connection process for each agent and server.

You must also reinstall all endpoints, or they will not be able to communicate with the servers. Uninstall the existing endpoint software, create a new endpoint package using the package-building tool (you cannot use your existing package), and use SMS or a similar mechanism to install the new package on these endpoints. See Installing and Deploying Endpoint Clients for more information on uninstalling endpoints.

In the initial authentication, the TRITON management server trades certificates with the other servers and endpoints in the network.

To re-run the security communication between TRITON AP-DATA components:

1. If you have not done so already, start the TRITON installer:
   - If you chose to keep installation files the last time you ran the installer, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for TRITON AP-DATA.
3. From the installation wizard, select **Modify**.
4. On the Recreate Certificate Authority screen, select the **Recreate Certificate Authority** check box.
5. Complete the installation wizard as prompted.

Repairing TRITON AP-DATA components

6. If you have not done so already, start the TRITON installer:
   - If you chose to keep installation files the last time you ran the installer, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.
7. In **Modify Installation** dashboard, click the **Modify** link for TRITON AP-DATA.
8. From the installation wizard, select **Repair**.
9. Complete the installation wizard as prompted.

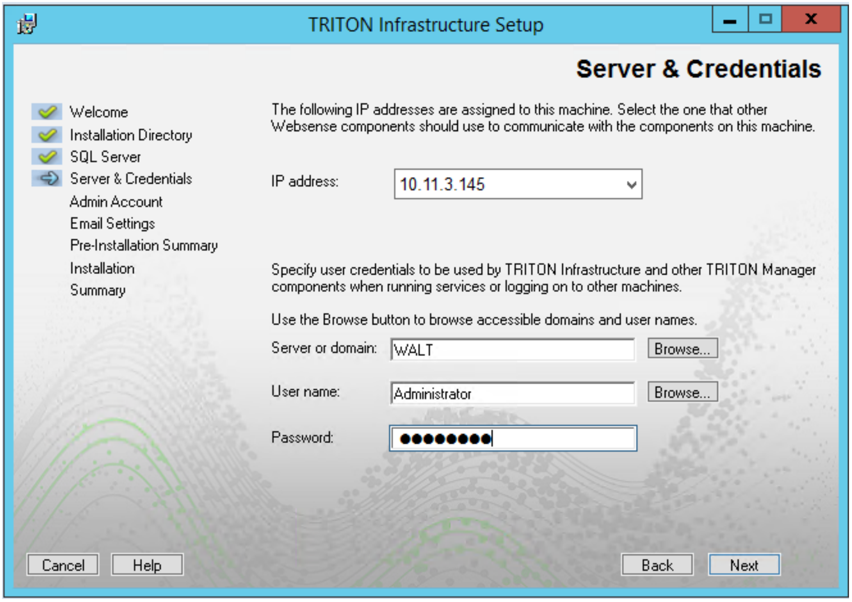
This restores the installation configuration to its last successful state. This can be used to recover from various corruption scenarios, such as binary files getting deleted, registries getting corrupted, etc.

Changing the TRITON AP-DATA service account

You cannot change the TRITON AP-DATA service account user name. Doing so can cause the system to behave in unexpected ways. For example, services may not be able to start and encryption keys may not work.

You can change the password; however. Here's how:

1. Modify the service account password from the domain's Active Directory or use Windows. From Windows:
   - ○ Log onto the TRITON management server with the service user account.
   - ○ Press **Ctrl +Alt +Delete** to access the Windows lock screen, then select **Change Password**.
2. Modify the TRITON infrastructure.
   a. Log onto the TRITON management server with the service user account.
   b. Run TRITON unified installer, e.g., **TRITON83xSetup.exe.**
   c. Select **Modify**.
   d. During TRITON infrastructure setup, change the password on the following screen. These are the credentials that the TRITON management server uses when running services or logging on to other machines. The password must:
      - ○ Be at least 8 characters
      - ○ Contain upper case characters
      - ○ Contain lower case characters
      - ○ Contain numbers
      - ○ Contain non-alphanumeric characters



Server & Credentials

The following IP addresses are assigned to this machine. Select the one that other Websense components should use to communicate with the components on this machine.

IP address: 10.11.3.145

Specify user credentials to be used by TRITON Infrastructure and other TRITON Manager components when running services or logging on to other machines.

Use the Browse button to browse accessible domains and user names.

Server or domain: WALT

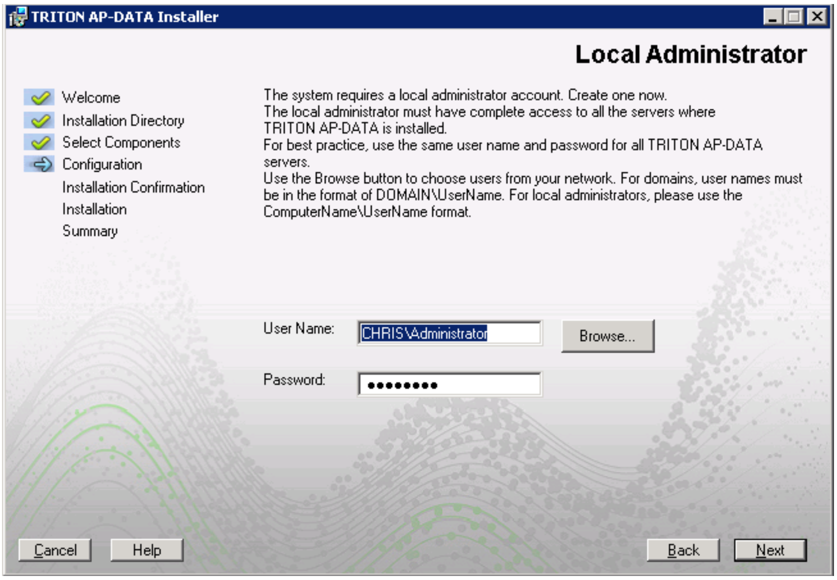
User name: Administrator

Password: ●●●●●●●●

   e. Complete the TRITON infrastructure wizard using the defaults.
3. Modify your TRITON AP-DATA installation.

a. Continue the wizard to access the TRITON AP-DATA installer.

b. Change the password on the following screen. Use the same password as in the TRITON infrastructure. This is the password used to access this server during component installation and operation.



The system requires a local administrator account. Create one now.
The local administrator must have complete access to all the servers where TRITON AP-DATA is installed.
For best practice, use the same user name and password for all TRITON AP-DATA servers.
Use the Browse button to choose users from your network. For domains, user names must be in the format of DOMAIN\UserName. For local administrators, please use the ComputerName\UserName format.

User Name: CHRIS\Administrator

Password: ••••••••

c. Finish the wizard.

d. Log onto the TRITON Manager, click the Data tab, and click **Deploy**.

Removing TRITON AP-DATA components

TRITON AP-DATA components must be removed all at once. You cannot select particular components on a machine for removal.

Warning

TRITON AP-EMAIL requires TRITON AP-DATA to be installed. If you are using TRITON AP-EMAIL, do not uninstall TRITON AP-DATA or TRITON AP-EMAIL will quit working.

Do not uninstall the TRITON infrastructure before removing TRITON AP-DATA.

For instructions on removing a TRITON AP-ENDPOINT, see Uninstalling endpoint software.

To remove TRITON AP-DATA components:

1. Start the TRITON installer:

- If you chose to keep installation files after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
- Otherwise, double-click the installer executable.

2. In **Modify Installation** dashboard, click the **Modify** link for TRITON AP-DATA.
3. At the **Welcome** screen, click **Remove**.
4. At the TRITON AP-DATA **Uninstall** screen, click **Uninstall**.

Important

This removes all TRITON AP-DATA components from this machine.

The **Installation** screen appears, showing removal progress.

5. At the **Uninstallation Complete** screen, click **Finish**.
6. You are returned to the **Modify Installation** dashboard.