



Installation Guide

Forcepoint™ TRITON® APX Suite

v8.3.x

©1996–2017, Forcepoint LLC
All rights reserved.
10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin TX 78759
Published 2017

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint LLC.

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

Forcepoint is a trademark of Forcepoint LLC. SureView, TRITON, ThreatSeeker, Sidewinder and Stonesoft are registered trademarks of Forcepoint LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Topic 1	Preparing for TRITON Deployment	1
	Deployment overview	1
	Remote office and off-site users	3
	Hybrid services	3
	TRITON AP-WEB and AP-EMAIL appliances	3
	TRITON AP-DATA appliance	3
	Third-party components	4
	Microsoft SQL Server	4
	Mail server	4
	Deployment details by TRITON product	4
	TRITON AP-WEB	4
	TRITON AP-DATA	4
	TRITON AP-EMAIL	5
	Installation overview	5
	Requirements	6
	TRITON Management Server	6
	System requirements for this version	6
	TRITON management server requirements	6
	Hardware requirements	7
	TRITON console browser support	8
	Virtualization systems	9
	Directory services for administrator authentication	9
	Supported appliance models and modes	9
	Reporting database requirements	9
	Components that may not be installed on Forcepoint appliances	10
	TRITON management server	10
	Web and Email Log Server	10
	Optional Web components	10
	Data Security Agents	11
	TRITON AP-ENDPOINT DLP (User Machine)	11
	Preparing servers for TRITON deployments	11
	Windows	11
	Domain Admin privileges	12
	Synchronizing clocks	12
	Anitvirus	12
	No underscores in FQDN	13
	Disable UAC and DEP	13
	Firewall	13

	Installing on Linux	13
Topic 2	Installing TRITON Management Components	1
	Installing the TRITON AP-WEB policy source	1
	Creating the TRITON Management Server	2
	Step 1: Download the TRITON Unified Installer	3
	Step 2: Select management components	3
	Step 3: Install the TRITON Infrastructure	6
	Step 4: Install Web management components	11
	Policy Server Connection screen	13
	Policy Broker Connection screen	13
	Select Policy Broker Screen	13
	Filtering Service Communication screen	14
	Completing the installation	14
	Step 5: Install Data management components	15
	Step 6: Install Email management components	17
Topic 3	Installing Additional Components	1
	Installing web components	1
	Install Log Server	1
	Installation steps	2
	Install an instance of Filtering Service	5
	Using a filtering-only appliance	5
	Installing Filtering Service on Windows	5
	Installing Filtering Service on Linux	7
	Install Content Gateway	9
	Installing other web components	10
	Installing data components	10
	Installing supplemental TRITON AP-DATA servers	10
	Operating system requirements	11
	Hardware requirements	11
	Software requirements	11
	Antivirus	12
	Port requirements	12
	Installation steps	13
	Installing TRITON AP-DATA agents	15
	Installing Email Log Server	17
Topic 4	Initial Configuration	1
	General configuration	1
	Log on to the TRITON Manager	2
	TRITON AP-WEB initial configuration	3
	Getting started with Web Protection solutions	3
	Additional tips for working with Web Protection solutions	3
	Identifying Filtering Service by IP address	4

Additional configuration for the Web DLP Module	4
Confirm Content Gateway registration with TRITON AP-DATA.....	5
Configure the Content Gateway policy engine.....	6
Verify that web and data protection components are linked.....	7
TRITON AP-DATA initial configuration	8
TRITON AP-EMAIL initial configuration	8
initial configuration settings	8
Email Hybrid Module initial configuration.....	10
Content Gateway initial configuration	10
Network Agent and stealth mode NICs	11
Windows	12
Linux	12

Preparing for TRITON Deployment

In this topic:

- [Deployment overview, page 1](#)
 - [Installation overview, page 5](#)
 - [Requirements, page 6](#)
 - [Preparing servers for TRITON deployments, page 11](#)
-

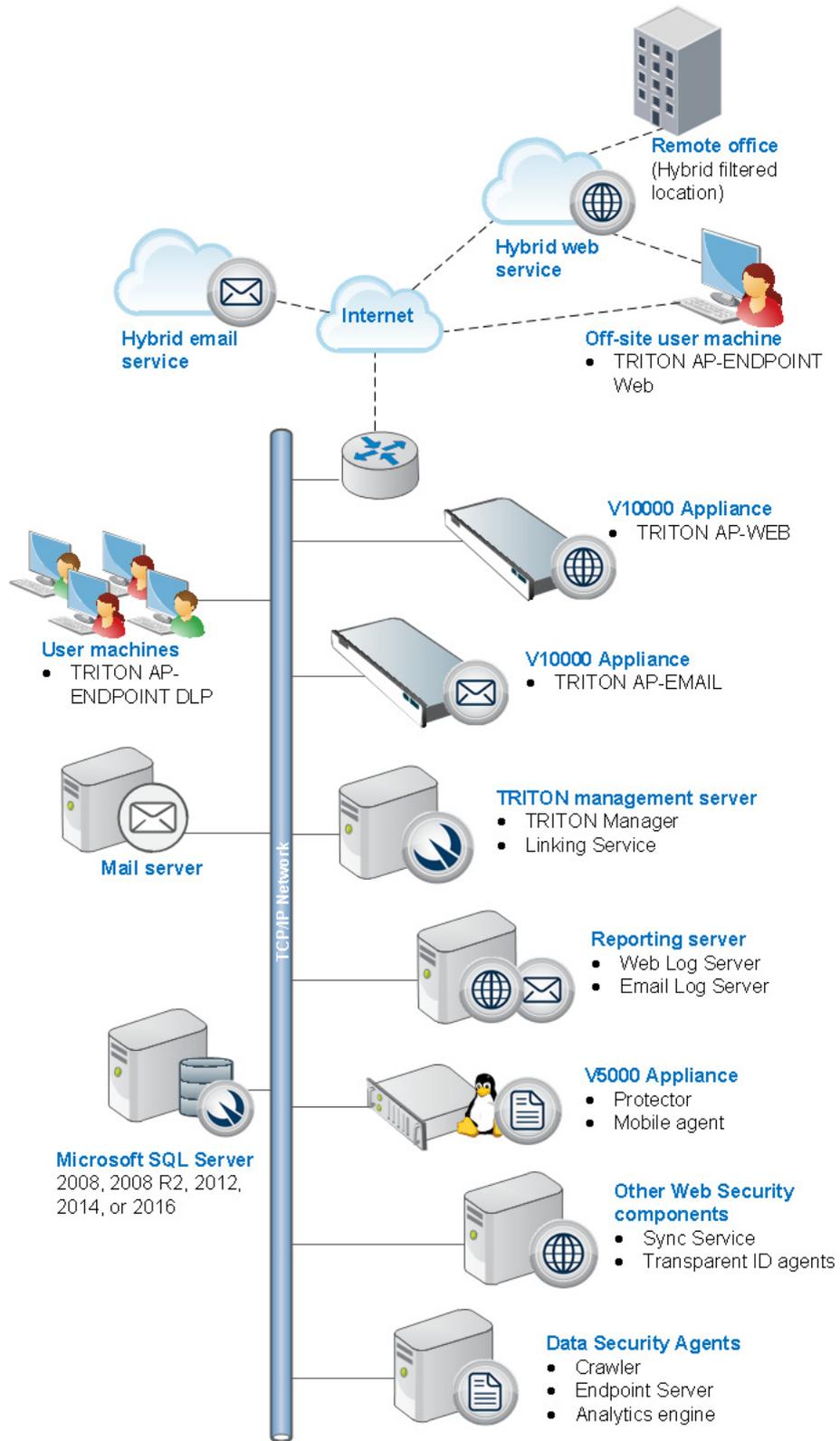
Deployment overview

A full TRITON deployment includes TRITON AP-WEB with optional Web Hybrid Module, TRITON AP-DATA Gateway, TRITON AP-ENDPOINT DLP, and TRITON AP-EMAIL with optional Email Hybrid Module.

- TRITON Manager, the management interface for Web, Email, and Data products, resides on a Windows server.
- TRITON AP-WEB may be deployed on Forcepoint appliances, dedicated Windows or Linux servers, or a combination of platforms. This guide covers the following configuration:
 - The policy source (the standalone or primary Policy Broker and central Policy Server) reside separate from the TRITON management server, on another Windows or Linux server, or on a Forcepoint appliance.

While this is not required and Policy Broker and Policy Server can reside on the TRITON management server machine, this configuration is recommended for full TRITON deployments to ensure optimum performance.
 - Web Log Server resides separate from the TRITON management server on a Windows machine.
- TRITON AP-DATA runs on Windows servers, optional protector appliances, and elsewhere in the network.
- TRITON AP-EMAIL enforcement components reside only on Forcepoint appliances. Management and reporting components reside on Windows servers.

Following is a diagram of a basic appliance-based deployment.



Remote office and off-site users

You can use the Web Hybrid Module to provide web security for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location. See [Initial Configuration, page 1](#), for more information.

Either the hybrid service or Forcepoint remote filtering software can provide web filtering for off-site users (e.g., telecommuters or traveling personnel).

- To direct user requests to the hybrid service, you can install a PAC file or an endpoint client on the user's machine. Web requests from that machine are then directed to the hybrid service for policy enforcement.
- To use remote filtering software, an optional component, Remote Filtering Server, is installed in your network DMZ, and Remote Filtering Client is installed on user machines. Web requests from the machine are sent to Remote Filtering Server, which connects to Filtering Service for policy enforcement. See [Deploying Remote Filtering Server and Client](#).

Hybrid services

If your subscription includes the Web Hybrid Module and the Email Hybrid Module:

- The cloud-based hybrid web service can provide Internet security for remote offices and off-site users.
- The cloud-based email hybrid service provides an extra layer of email threat detection, stopping spam, virus, phishing, and other malware before they reach your network and possibly reducing email bandwidth and storage requirements. You can also use the email hybrid service to encrypt outbound email before delivery to its recipient.

TRITON AP-WEB and AP-EMAIL appliances

Forcepoint appliances may be used to deploy core web and email functionality.

- The Content Gateway proxy on the appliance manages web traffic.
- Incoming email flows from the email hybrid service (if enabled) to the Forcepoint appliance and to your mail server. The Forcepoint appliance also provides the Personal Email Manager facility for end users to manage quarantined email.
- Note that TRITON AP-EMAIL and TRITON AP-WEB cannot be deployed on the same appliance.

TRITON AP-DATA appliance

The TRITON AP-DATA appliance can be used in protector or mobile agent mode. The protector monitors and reports data loss and leaks of sensitive information. Using PreciseID technology, the protector can be configured to accurately monitor sensitive information-in-transit on any port.

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.

The protector and mobile agent are available as a Linux-based soft or physical V5000 appliance.

Third-party components

Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store TRITON logging and reporting data. Quarantined email messages and DLP configuration data are also stored here.

When TRITON components are installed, SQL Server must be installed and running, typically on its own machine as shown in the diagram above.

Mail server

Your internal mail server.

Deployment details by TRITON product

Use the links in this section to read about further deployment details and recommendations for the individual TRITON products.



Note

The links in this section take you to pages in the Forcepoint Technical Library. You can also download deployment guides for individual TRITON products in PDF format from the Technical Library.

TRITON AP-WEB

- [Web Deployment Recommendations](#)
- [Deploying TRITON AP-WEB for a distributed enterprise](#)

TRITON AP-DATA

- [Planning TRITON AP-DATA Deployment](#)
- [Installing TRITON AP-DATA Agents](#)
- [Integrating TRITON AP-DATA with Existing Infrastructure](#)
- [Scaling TRITON AP-DATA](#)

TRITON AP-EMAIL

- [TRITON AP-EMAIL Deployment](#)

Installation overview

To install TRITON components:

1. Make sure that a supported version of Microsoft SQL Server (not Express) is installed and running in your network. See [Requirements, page 6](#).
2. The machine with the standalone or primary Policy Broker and its companion Policy Server instance must be configured first. These web components must be running before any other web components can be installed:
 - If Policy Broker will reside on a full policy source appliance, configure that appliance first. See [TRITON Appliances Getting Started](#).
 - If you wish to install the software version of Policy Broker and Policy Server, you must do this **before** the TRITON management server installation. Install the software version if you plan to use Policy Broker replication. See [Installing the TRITON AP-WEB policy source, page 1](#).
It is also recommended that you install an instance of Filtering Service on this machine.
3. Install and run the **firstboot** script on your appliances. See [TRITON Appliances Getting Started](#).
4. Install TRITON management and core Data components on a Windows Server 2008 R2 SP1 or Windows Server 2012 Standard Edition machine. For the machine requirements see [Requirements, page 6](#), and for the installation steps see [Installing TRITON Management Components, page 1](#).
On the **Installation Type** screen, select all three modules (**Web, Data, and Email**) under TRITON Manager.
5. Install Web and Email Log Server. See [Install Log Server, page 1](#) and [Installing Email Log Server, page 17](#).
If you plan to enable the Hybrid Web Module, note that Sync Service is typically installed with Web Log Server.
6. Install additional components (such as web transparent identification agents or TRITON AP-DATA agents) as needed. See:
 - “Install additional web components” in the installation instructions for [TRITON AP-WEB](#).
 - “Adding, Modifying, or Removing Components” in the [TRITON AP-DATA Installation Guide](#)

Requirements

This section lists the requirements for the TRITON Management Server and the reporting database.

TRITON Management Server

The machine that hosts core management components for all security solutions is referred to as the **TRITON management server**. This machine hosts TRITON Manager, which includes:

- The infrastructure uniting all management components
- A settings database, holding administrator account information and other data shared by all management components
- One or more management modules, used to access configuration, policy management, and reporting tools for a TRITON advanced protection solution. Available modules include:
 - Web manager
 - Data manager
 - Email manager

Additional components may also reside on the TRITON management server

System requirements for this version

Applies to:	In this topic
<ul style="list-style-type: none"> ● TRITON AP-WEB and Web Filter & Security, v8.3.x ● TRITON AP-DATA, v8.3.x ● TRITON AP-EMAIL, v8.3.x 	<ul style="list-style-type: none"> ● TRITON management server requirements, page 6 ● Supported appliance models and modes, page 9 ● Reporting database requirements, page 9 ● Components that may not be installed on Forcepoint appliances, page 10

TRITON management server requirements

The TRITON management server must be on one of the following 64-bit machines:

- Windows Server 2008 Standard or Enterprise R2 SP1

- Windows Server 2012 Standard Edition
- Windows Server 2012 Standard or Enterprise R2

It hosts the TRITON Manager (TRITON console), which includes:

- The infrastructure uniting all management components
- A settings database for administrator account information and other shared data
- One or more management modules (Web, Data, or Email), used for configuration and reporting

Additional components may also reside on the TRITON management server.

**Important**

TRITON modules and components can communicate with only one management server. For this reason, there is typically one management server per deployment.

Hardware requirements

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

The following are minimum hardware recommendations for a TRITON management server.

Notes:

- TRITON AP-DATA allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90 GB from the TRITON AP-DATA disk space requirements.
- It is strongly recommended you allocate more than the minimum listed disk space to allow for scaling with use. The “recommended” option allows for scaling as reporting data accumulates.
- If you install the product on a drive other than the main Windows drive (typically C drive), then you must have at least 4 GB free on the main Windows drive to accommodate the TRITON installer.

With remote (standard or enterprise) reporting database

Management modules	Recommended	Minimum
Web module	8 CPU cores (2.5 GHz), 16 GB available RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB available RAM, 146 GB Disk Space
Data module	8 CPU cores (2.5 GHz), 16 GB available RAM, 400 GB Disk space	4 CPU cores (2.5 GHz), 12 GB available RAM, 146 GB Disk Space
Web and Data modules	8 CPU cores (2.5 GHz), 20 GB available RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB available RAM 146 GB Disk Space
Email and Data modules	8 CPU cores (2.5 GHz), 20 GB available RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB available RAM, 146 GB Disk Space
Web, Data, and Email modules	8 CPU cores (2.5 GHz), 24 GB available RAM, 550 GB Disk Space	8 CPU cores (2.5 GHz), 20 GB available RAM, 146 GB Disk Space

With local (express) reporting database

Management modules	Recommended	Minimum
Web module	8 CPU cores (2.5 GHz), 16 GB available RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB available RAM, 240 GB Disk Space
Data module	8 CPU cores (2.5 GHz), 16 GB available RAM, 400 GB Disk space	4 CPU cores (2.5 GHz), 12 GB available RAM, 240 GB Disk Space
Web and Data modules	8 CPU cores (2.5 GHz), 20 GB available RAM RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB available RAM, 240 GB Disk Space
Email and Data modules	8 CPU cores (2.5 GHz), 20 GB available RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB available RAM, 240 GB Disk Space
Web, Data, and Email modules	8 CPU cores (2.5 GHz), 24 GB available RAM, 600 GB Disk Space	8 CPU cores (2.5 GHz), 20 GB available RAM, 240 GB Disk Space

TRITON console browser support

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.

Virtualization systems

All TRITON Manager components are supported on these virtualization systems:

- 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 that this support is for the TRITON console and secondary TRITON AP-DATA servers only. Other components (used for enforcement, analysis, or reporting) may have additional requirements that are not supported by these virtualization environments..

Directory services for administrator authentication

If you allow users to log on to TRITON console using their network accounts, the following directory services can be used to authenticate administrator logons:

- Microsoft Active Directory
- Lotus Notes
- Generic LDAP directories
- Novell eDirectory
- Oracle Directory Services

Supported appliance models and modes

See the [V-Series Certified Matrix](#) and [X-Series Certified Matrix](#) for comprehensive information regarding supported appliance models and modes.

See [V-Series appliances supported with version 8.0 and higher](#) for information specific to version 8.x.

Reporting database requirements

For all TRITON solutions, Microsoft SQL Server is used to host the reporting database.

- 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, Business Intelligence, 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**
All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64
- **SQL Server 2008 R2 SP2** (or the latest service pack from Microsoft) - All editions except Web and Compact; all service packs; not IA64
Standard, Business Intelligence, and Enterprise editions
- **SQL Server 2008 R2 Express** (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

If you are using a remote database, the SQL Server logon ID and password for the SQL account must have a **sysadmin** role.

Components that may not be installed on Forcepoint appliances

TRITON management server

The TRITON management server is the Windows server on which TRITON Manager is installed. TRITON Manager is the management and reporting interface for web, data, and email solutions.

The Data Security Management Server and, typically, Crawler also reside on the TRITON management server machine to provide key TRITON AP-DATA functions, including web and email DLP (data loss prevention) features.

Linking Service also usually resides on the management server.

Web and Email Log Server

A separate Windows machine hosts Web Log Server and Email Log Server. These services receive information about web and email activity and process it into their respective Log Databases.

Optional Web components

Remote Filtering Server, Sync Service, and transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent) cannot reside on Forcepoint appliances.

Also, you can install additional instances of several web components on Windows or Linux servers, if needed.

Data Security Agents

The Crawler, TRITON AP-ENDPOINT DLP, Web Content Gateway, Email Gateway for Office 365, TRITON AP-DATA Cloud, and Analytics Engine are installed on appropriate local or virtual machines.

See the [TRITON AP-DATA Installation Guide](#) for installation instructions.

TRITON AP-ENDPOINT DLP (User Machine)

The DLP endpoint can be installed on any Windows, macOS, or Linux machine.

Preparing servers for TRITON deployments

Follow the instructions in this section to ensure your servers are ready for the v8.x installation.

Windows

On Windows machines that will host either the TRITON management server or other TRITON components:

- Make sure there are no underscores in the machine's fully-qualified domain name (FQDN). 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.

- Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- Verify that there is sufficient disk space to download the installer, extract temporary installation files, and install the management components on the Windows installation drive (typically C).
- Make sure that both .NET Framework v3.5 and 4.5 are installed.
 - For Windows server 2008 R2 SP1, you can add .NET 3.5 from Server Manager\Features. Usually this feature is **On** by default. You must download .NET 4.5 from the Microsoft site, <https://msdn.microsoft.com/en-us/library/5a4x27ek%28v=vs.110%29.aspx?f=255&MSPPError=-2147217396>.
 - For Windows server 2012/2012 R2, you can both .NET 3.5 and .NET 4.5 from Server Manager\Features. Usually v3.5 is **Off** by default and v4.5 is **On** by default. Turn them both on.

- Synchronize the clocks on all machines (including appliances) where a TRITON component will be installed. It is a good practice to point the machines to the same Network Time Protocol server.
- Disable the antivirus software on the machine before installation. After installation, before restarting your antivirus software, see [Excluding your software from antivirus scans](#).
- Disable any firewall on the machine before starting the Forcepoint installer and then re-enable it after installation. Open ports as required by the TRITON components you have installed. See [TRITON APX default ports](#).
- Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.

Domain Admin privileges

TRITON 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 in 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 data for your web protection solution, log in as a domain user to run the TRITON Unified Installer.

Synchronizing clocks

If you are distributing components across different machines in your network, synchronize the clocks on all machines where a TRITON component will be 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 appliance, you must synchronize the machine's system time to the appliance's system time.

Antivirus

Disable the antivirus software on the machine prior to installing TRITON components. Be sure to re-enable antivirus after installation. Certain files should be excluded from antivirus scans to avoid performance issues; see [Excluding Forcepoint files from antivirus scans](#).

No underscores in FQDN

Do not install TRITON 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.

Disable UAC and DEP

Before beginning the installation process, disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.

Firewall

Disable any firewall on the machine prior to installation. Be sure to disable it before starting the installer, and then re-enable it after installation. Open ports as required by the components you have installed.

**Note**

The TRITON installer adds two inbound rules to the public profile of Windows Firewall. Ports 9443 and 19448 are opened for TRITON Infrastructure. These ports must be open to allow browsers to connect to the TRITON Manager. Also, additional rules may be added to Windows Firewall when installing TRITON AP-DATA components.

See [Default ports for on-premises TRITON solutions](#), page 391, for more port-related information.

Installing on Linux

Most web protection components can be installed on Linux. If you are installing on Linux complete the instructions below.

SELinux

Before installing, if SELinux is enabled, disable it or set it to permissive.

Linux firewall

If web protection software is being installed on a Linux machine on which a firewall is active, shut down the firewall before running the installation.

1. Open a command prompt.

2. Enter **service iptables status** to determine if the firewall is running.
3. If a firewall is running, open a command shell and enter **service iptables stop**.
4. After installation, restart the firewall. In the firewall, be sure to open the ports used by components installed on this machine. See [Default ports for on-premises TRITON solutions](#), page 391.



Important

Do **not** install Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software.

Hostname

If, during the installation, you receive an error regarding the `/etc/hosts` file, use the following information to correct the problem.

When installing to a Linux machine, the **hosts** file (by default, in `/etc`) should contain a hostname entry for the machine, in addition to the loopback address. (Note: you can check whether a hostname has been specified in the **hosts** file by using the **hostname -f** command.)

To configure the hostname:

1. Set the hostname:

```
hostname <host>
```

Here, `<host>` is the name you are assigning this machine.

2. Also update the HOSTNAME entry in the `/etc/sysconfig/network` file:

```
HOSTNAME=<host>
```

3. In the `/etc/hosts` file, specify the IP address to associate with the hostname. This should be static, and not served by DHCP. Do not delete the second line in the file, the one that begins with `127.0.0.1` (the IPv4 loopback address). And do not delete the third line in the file, the one that begins `::1` (the IPv6 loopback address).

```
<IP address> <FQDN> <host>
127.0.0.1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
```

Here, `<FQDN>` is the fully-qualified domain name of this machine (i.e., `<host>.<subdomains>.<top-level domain>`)—for example, `myhost.example.com`—and `<host>` is the name assigned to the machine.



Important

The hostname entry you create in the **hosts** file must be the first entry in the file.

TCP/IP only

Web protection software supports only TCP/IP-based networks. If your network uses both TCP/IP- and non-IP-based network protocols, only user requests in the TCP/IP portion of the network are managed.

Installing TRITON Management Components

In this topic:

- [Installing the TRITON AP-WEB policy source, page 1](#)
 - [Creating the TRITON Management Server, page 2](#)
-

Follow the instructions in this section to install:

- The TRITON AP-WEB policy source
- TRITON Manager and management components on the TRITON management server

Installing the TRITON AP-WEB policy source

This section describes the steps required to install the primary or standalone Policy Broker and the associated Policy Server instance on a Windows machine. If Policy Broker will reside on a full policy source appliance, see [TRITON Appliances Getting Started](#) and [Configuring TRITON AP-WEB components](#).

It is recommended that you install Filtering Service at the same time. If you choose to install the first instance of Filtering Service on a different machine, it must connect to the central Policy Server on this machine. See [Install an instance of Filtering Service, page 5](#).

You can also install other components on this machine, for example User Service, Usage Monitor, and Directory Agent.

On the machine that will host the policy source:

1. Ensure you have prepared the machine as described in [Preparing servers for TRITON deployments, page 11](#).
2. Log on to the machine with domain admin privileges.
3. Download or copy the TRITON Unified Installer (the Windows installer) to this machine. The installer is available from [My Account](#) and the installer file is **TRITON83xSetup.exe**.

4. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
5. On the **Welcome** screen, click **Start**.
The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.
6. On the **Subscription Agreement** screen, select **I accept this agreement**, then click **Next**.
7. On the **Installation Type** screen, select **Custom**.
8. On the Custom Installation dashboard, click the TRITON AP-WEB or Web Filter and Security **Install** link.
9. On the **Select Components** screen, select Policy Broker, Policy Server, and Filtering Service. Note that these components must be installed in the order listed, and before any other web components. (If you select all 3 at the same time, they are installed in the correct order.)
10. On the Policy Broker Replication screen, indicate which Policy Broker mode to use.
 - Select **Standalone** if this will be the only Policy Broker instance in your deployment.
 - Select **Primary**, then create a **Synchronization password** if you will later install additional, replica instances of Policy Broker.



Important

Be sure to record the synchronization password. You must provide this password each time you create a Policy Broker replica.

11. On the Integration Option screen, select **Install TRITON AP-WEB to connect to Content Gateway**, then click **Next**.
12. If the management server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components. Follow the on-screen prompts to complete this process.
13. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.
14. A progress screen is displayed. Wait for installation to complete.

Creating the TRITON Management Server

The installation procedure for the TRITON management server includes the following steps:

- [Step 1: Download the TRITON Unified Installer, page 3](#)
- [Step 2: Select management components, page 3](#)

- [Step 3: Install the TRITON Infrastructure](#), page 6
- [Step 4: Install Web management components](#), page 11
- [Step 5: Install Data management components](#), page 15
- [Step 6: Install Email management components](#), page 17

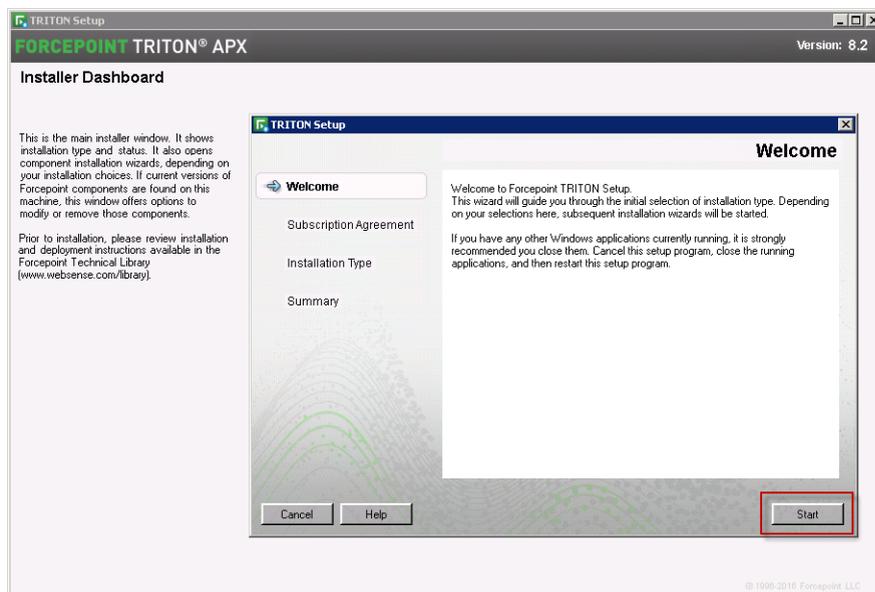
Ensure you have prepared the machine as described in [Preparing servers for TRITON deployments](#), page 11.

Step 1: Download the TRITON Unified Installer

1. Log on to the machine with domain admin privileges.
2. Download or copy the TRITON Unified Installer (the Windows installer) to this machine. The installer is available from [My Account](#) and the installer file is **TRITON83xSetup.exe**.

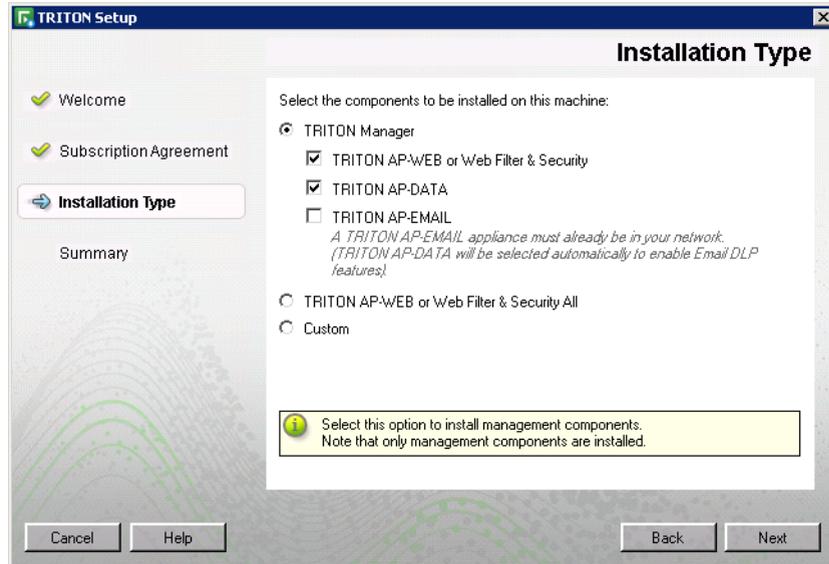
Step 2: Select management components

1. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
2. On the **Welcome** screen, click **Start**.



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

- On the **Installation Type** screen, select **TRITON Manager** and the modules you want to install (Web, Data, and Email).



Note

The TRITON Manager components are management consoles. Selecting them does not install other security or filtering components. Non-management components are installed using the **All web components** or **Custom** options.

See the following table for information about which modules you should select for installation.

Solution	TRITON Manager module		
	Web	Data	Email
TRITON AP-WEB	X		
TRITON AP-WEB with Web Hybrid Module and/or Web DLP Module	X	X	
TRITON AP-DATA		X	
TRITON AP-EMAIL		X	X

Note: If your subscription includes a combination of these solutions, install all of the modules required by them.

When you select **Email**, **Data** is also selected. The Data module is required for email DLP (data loss prevention) features, included with TRITON AP-EMAIL.

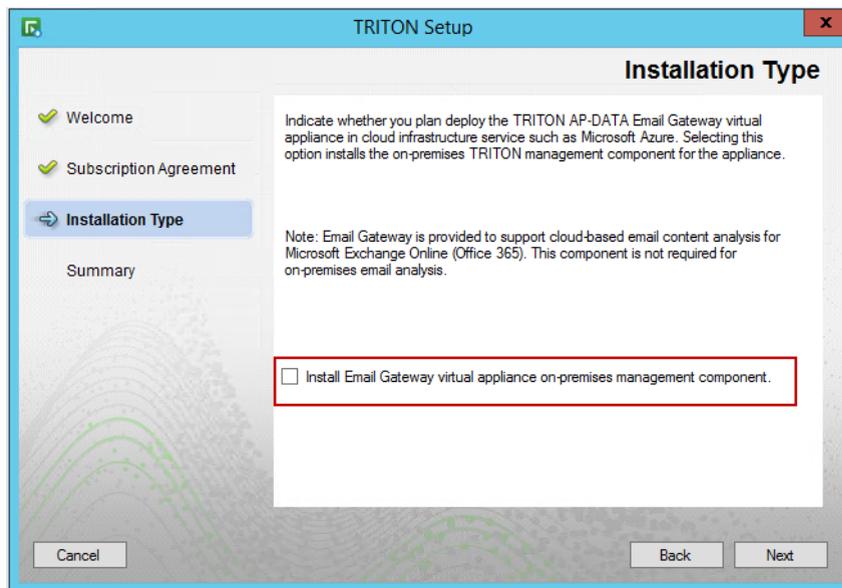


Important

To install the Email module of the TRITON Manager, an Email appliance must already be running. You will need to provide the appliance C interface IP address during console installation.

The appliance E1/P1 (and E2/P2, if used) interface must also be configured via command-line interface (CLI) before you install TRITON AP-EMAIL management components.

- If you selected **TRITON AP-DATA** on the Installation Type screen and did not select TRITON AP-EMAIL, a second Installation Type screen appears to prompt you to install the TRITON AP-DATA Email Gateway manager.



TRITON AP-DATA Email Gateway for Microsoft 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 Gateway enables analysis of email in cloud platforms with management performed on-premises. See [TRITON AP-DATA Installation Guide](#) for detailed virtual appliance and manager installation instructions.

If your TRITON AP-DATA subscription includes the TRITON AP-DATA Email Gateway, mark the **Install Email Gateway virtual appliance on-premises management component** check box to install the Email Gateway manager.

- On the **Summary** screen, click **Next** to continue the installation. TRITON Infrastructure Setup launches.

Step 3: Install the TRITON Infrastructure

The TRITON infrastructure includes data storage and common components for the management modules of TRITON Manager.

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.

The information entered here is also used by the Web, Data, and Email component installers, by default. The Web component installer can be used to specify a different database; the Data and Email component installers cannot.

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 [Requirements, page 6](#), to verify your version of SQL Server is supported.

After entering the above information, 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. If you are using Windows authentication with TRITON AP-DATA, TRITON AP-WEB or TRITON AP-EMAIL, 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.

For more information about permissions required for the connection account, see [Installing with SQL Server](#).

If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web module. See [Configuring Apache services to use a trusted connection](#).

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

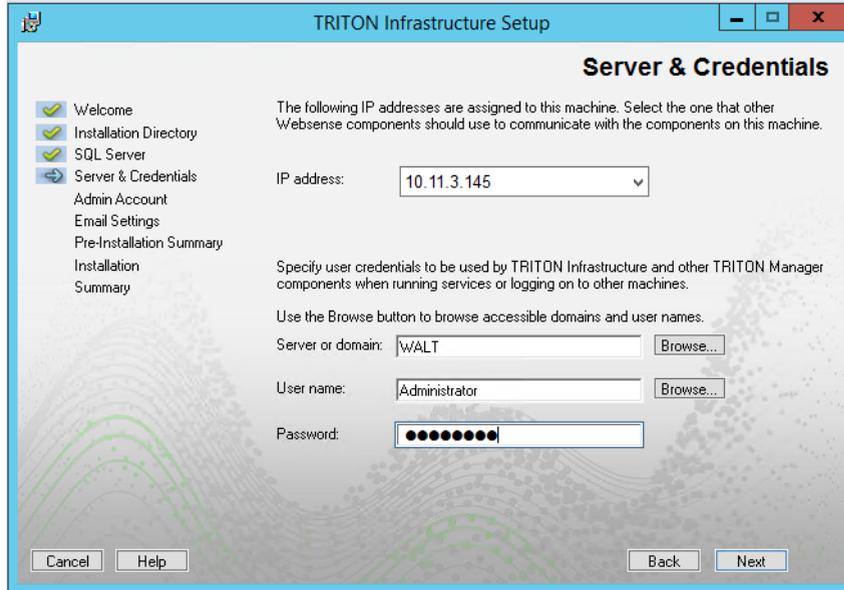
If the test is unsuccessful, the following message appears:

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.

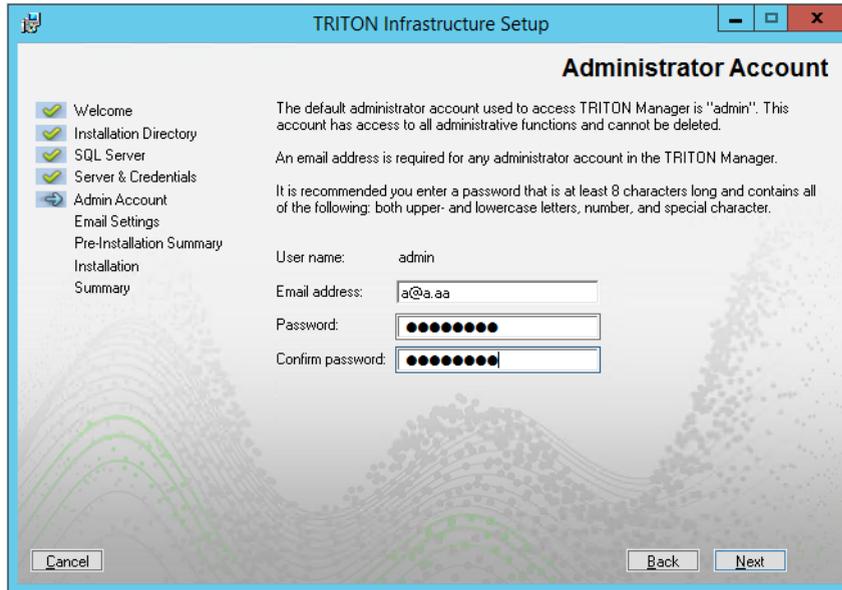
Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

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



- 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 TRITON Manager (via Web browser). Also specify this IP address to any component that needs to connect to the TRITON management server.
 - Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Manager. The server/host name cannot exceed 15 characters.
 - Specify the **User name** of the account to be used by TRITON 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**. The password must:
 - Be at least 8 characters
 - Contain upper case characters
 - Contain lower case characters
 - Contain numbers

- Contain non-alphanumeric characters



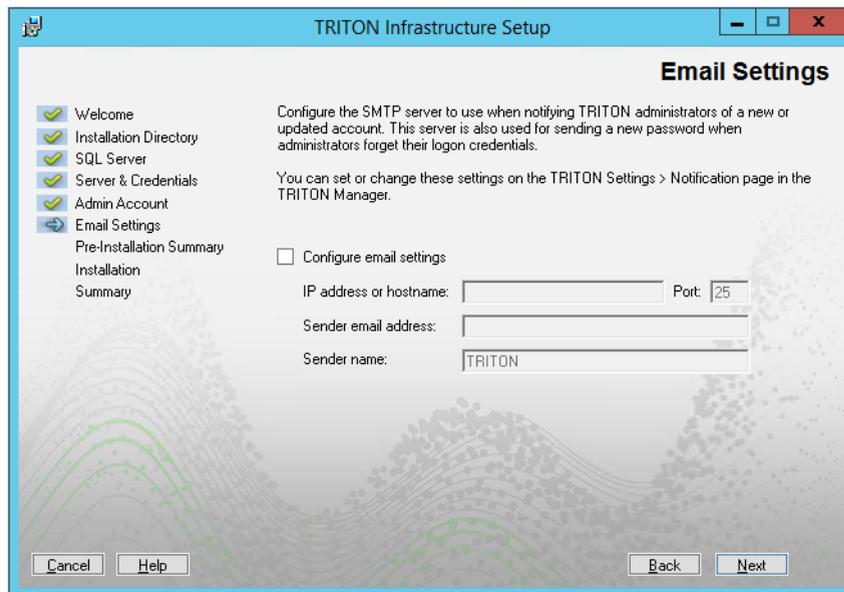
The screenshot shows the 'Administrator Account' configuration window in the TRITON Infrastructure Setup application. The window title is 'TRITON Infrastructure Setup' and the subtitle is 'Administrator Account'. On the left, a navigation pane lists the following steps: Welcome, Installation Directory, SQL Server, Server & Credentials, Admin Account (highlighted with a blue arrow), Email Settings, Pre-Installation Summary, Installation, and Summary. The main content area contains the following text: 'The default administrator account used to access TRITON Manager is "admin". This account has access to all administrative functions and cannot be deleted.' and 'An email address is required for any administrator account in the TRITON Manager.' Below this, a note states: '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.' The form fields are: 'User name:' with the value 'admin'; 'Email address:' with the value 'a@a.aa'; 'Password:' with a masked field of 8 dots; and 'Confirm password:' with a masked field of 8 dots. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'.

6. 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).

You must use a strong password as described on screen.

- 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 TRITON Manager.



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 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 TRITON Manager.
- On the **Pre-Installation Summary** screen, verify the information and then click **Next** to begin the installation.
 - 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 'Websense 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.

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

When you click **Finish** in TRITON Infrastructure Setup, component installers for each module selected in the Module Selection screen are launched in succession.



Important

You may be prompted to restart the machine after each component is installed. This is optional. You may prefer to restart the machine once after all components are installed.

Only the component installers for the modules you have selected are launched. For example, if you select only Web and Data, the Email installer is not launched.

Complete the following procedures for the modules you have selected. For each module, a component installer will launch. The component installers launch in the order shown here.

- [Step 4: Install Web management components](#)
- [Step 5: Install Data management components](#)
- [Step 6: Install Email management components](#)

Step 4: Install Web management components

In the recommended software installation for TRITON web, data, and email deployments, the TRITON management server hosts management components while the primary or standalone Policy Broker and central Policy Server reside on a separate machine (the policy source machine), as described in [Installing the TRITON AP-WEB policy source](#).

Note that if Linking Service will run on the management server, the Filtering Service that connects to the central Policy Server must be installed and running before Linking Service is installed.



Important

If you have a **full policy source** Web appliance, Policy Broker, Policy Server, and Filtering Service, among other components, reside there.

Follow these instructions to install TRITON AP-WEB management components on a TRITON management server.

1. It is assumed you have reached this point by starting a TRITON Manager installation. If not, see [Step 2: Select management components, page 3](#).

2. In the **Select Components** screen, select the components you want to install on this machine and then click **Next**.

The following TRITON AP-WEB components are available for installation on a TRITON management server:

- **TRITON Manager (Web module)** must be installed. It is selected by default and cannot be deselected. The other components shown are optional for this machine.
- **Sync Service** typically does not run on the management server. It is a required component if you have the Web Hybrid module, but it typically resides on the Web Log Server machine.



Note

Although Sync Service and the Web Log Server may be installed on the TRITON management server, they consume considerable system resources. For TRITON Enterprise deployments, it is recommended to install these components on another machine. See [Install Log Server, page 1](#).

- Select **Linking Service** if your subscription includes both a Web and Data solution.



Important

Filtering Service must be installed in your network before you install Linking Service. In an appliance-based deployment, Filtering Service is installed on all Web appliances (full policy source, user directory and filtering, and filtering only). In a software-based deployment, it is recommended that you install Filtering Service with Policy Broker and Policy Server on another separate machine from the TRITON management server, as Filtering Service can consume considerable system resources and may have a performance impact on the TRITON management server. Large or distributed environments may include multiple Filtering Service instances.

You can return to the TRITON management server at a later time and install Linking Service if required.

- **Real-Time Monitor** is optional. It is typically installed on the TRITON management server, but can be located elsewhere. Install no more than one instance of Real-Time Monitor for a Policy Server instance. In most cases, only one instance of Real-Time Monitor is required per deployment.
- **Policy Broker and Policy Server** are typically already installed on a separate machine, and should not be selected again.

Policy Server Connection screen

If Policy Server does not reside on the management server, on the Policy Server Connection screen, enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:

1. Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin/, by default).
2. Open the **BrokerService.cfg** file in a text editor.
3. Locate the **listen_port** value.
4. When you are finished, close the file without saving. Do **not** modify the file.

Policy Broker Connection screen

If Policy Broker does not reside on the management server, and you selected Sync Service for installation, the **Policy Broker Connection** screen appears. Enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:

1. Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin/, by default).
2. Open the **BrokerService.cfg** file in a text editor.
3. Locate the **listen_port** value.
4. When you are finished, close the file without saving. Do **not** modify the file.

Select Policy Broker Screen

This screen appears if Policy Server is selected for installation, but Policy Broker is not.

Policy Server can be connected to a primary, standalone, or replica Policy Broker.

A list of Policy Broker instances to which this Policy Server can be connected is provided. The list is based on the Policy Broker IP address entered on the Policy Broker Connection screen.

- Select the Policy Broker instance that the Policy Server being installed should connect to.
- The primary or standalone Policy Broker is selected by default.

If Policy Broker is not installed anywhere in your network, you must install it before **any other** web protection component.

Filtering Service Communication screen

If you select Linking Service for installation, the **Filtering Service Communication** screen appears.

Enter the IP address of the Filtering Service machine and the port Filtering Service uses to communicate with Network Agent, Content Gateway, or third-party integration products (default is 15868).

- In an appliance-based deployment, Filtering Service is installed on all Web appliances (full policy source, user directory and filtering, and filtering only).
 - Enter the IP address of the appliance's C interface and use the default port (15868).
 - If you have multiple appliances, be sure to select the one you want Network Agent, the filtering plug-in, or Linking Service to use.
- The Filtering Service communication port must be in the range 1024-65535. During installation, Filtering Service may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Filtering Service instances.) To verify the port:
 - a. Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin/, by default).
 - b. Open the **eimserver.ini** file in a text editor.
 - c. Locate the **WebSenseServerPort** value.
 - d. When you are finished, close the file without saving. Do **not** modify the file.

If Filtering Service is not installed anywhere in your network, you must install it before installing Network Agent, a filtering plug-in, or Linking Service.

Completing the installation

1. On the **Pre-Installation Summary** screen, verify the information shown.

The summary shows the installation path and size, and the components to be installed.
2. Click **Next** to start the installation. The **Installing Forcepoint** progress screen is displayed. Wait for installation to complete.
3. On the **Installation Complete** screen, click **Next**.
4. If you have not selected any other TRITON Manager module, you are returned to the Modify Installation dashboard. Installation is complete.

If you have chosen to install other TRITON Manager modules, you are returned to the Installer Dashboard and the next component installer is launched.

Step 5: Install Data management components

Follow these instructions to install TRITON AP-DATA management components on the TRITON management server. This includes:

- A TRITON AP-DATA policy engine
 - Primary fingerprint repository
 - Forensics repository
 - Endpoint server
1. It is assumed you have reached this point by starting a TRITON Manager installation. If not, see [Step 3: Install the TRITON Infrastructure, page 6](#).
 2. When the TRITON AP-DATA installer is launched, a **Welcome** screen appears. Click **Next** to begin TRITON AP-DATA installation.



Note

Both .NET 3.5 and 4.5 are required for the TRITON infrastructure. If either is not found on this machine, you receive a message.

- For Windows server 2008 R2 SP1, you can add .NET 3.5 from Server Manager\Features. Usually this feature is **On** by default. You must download .NET 4.5 from the Microsoft site, <https://msdn.microsoft.com/en-us/library/5a4x27ek%28v=vs.110%29.aspx?f=255&MSPPErr=-2147217396>.
- For Windows server 2012/2012 R2, you can both .NET 3.5 and .NET 4.5 from Server Manager\Features. Usually v3.5 is **Off** by default and v4.5 is **On** by default. Turn them both on.

3. In the **Select Components** screen, click **Next** to accept the default selections.



Note

If there is insufficient RAM on this machine for TRITON Management Server components, a message appears. Click **OK** to dismiss the message. You are allowed to proceed with the installation. However, it is a best practice to install only if you have sufficient RAM.

4. If prompted, click **OK** to indicate that services such as ASP.NET and SMTP will be enabled.

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

5. 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.

6. If your SQL Server database is on a remote machine, you are prompted for the name of a temporary folder. This screen defines where TRITON AP-DATA 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.

If you do not plan to archive incidents or perform system backup and restore, you do not need to fill out this screen.

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.

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
```

7. In the **Installation Confirmation** screen, click **Install** to begin installation of TRITON AP-DATA components.
8. 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.

9. The **Installation** progress screen appears. Wait for the installation to complete.
10. When the **Installation Complete** screen appears, click **Finish** to close the TRITON AP-DATA installer.
11. 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 a supplemental TRITON AP-DATA server, see [Installing data components, page 10](#). For information on installing other Data Security components, such as the protector, mobile agent, printer agent, SMTP agent, TMG agent, or endpoint client, see the [TRITON AP-DATA Installation Guide](#).

For detailed instructions on installing the TRITON AP-DATA Email Gateway cloud-hosted virtual appliance and on-premises management component, see the [TRITON AP-DATA Installation Guide](#).

Step 6: Install Email management components

Follow these instructions to install the Email module of TRITON Manager. In addition to the Email module, you will be given the option to install Email Log Server on this machine. As Log Server consumes considerable system resources, for TRITON Enterprise deployments it is recommended to install it on another machine. See [Installing Email Log Server, page 17](#).



Important

Installer screens for the TRITON AP-DATA Email Gateway management component appear now if you selected that option earlier on the Installation Type screens. See the [TRITON AP-DATA Installation Guide](#) for detailed instructions.

1. It is assumed you have reached this point by starting a TRITON Manager installation and selecting the Email module. If not, see [Step 3: Install the TRITON Infrastructure, page 6](#).
2. Once the TRITON AP-EMAIL Installer is launched, the **Introduction** screen appears; click **Next** to begin Email Security installation.
3. On the **Select Components** screen, deselect the Email Log Server option if you are installing the Log Server on a separate Windows machine, then click **Next**.

TRITON Manager (Email module) will be installed automatically. You cannot deselect it.



Note

If you do not see the Email module on this screen, TRITON Infrastructure was not detected by the TRITON AP-EMAIL Installer. TRITON Infrastructure must be installed already to be able to install Email management components.

4. On the **Email Log Database** screen, specify the IP address or IP address and instance name (format: IP address\instance) for the email Log Database. You may specify whether the connection to the database should be encrypted. Please note the following issues associated with using this encryption feature:
 - You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
 - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
 - The connection from the Email module of TRITON Manager to the Forcepoint appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.Designate the login type for the database, either Windows authentication or **sa** account.
5. On the **Email Appliance** screen specify the Email appliance to be managed by this installation of TRITON Manager and then click **Next**. Enter the IP address of the **C** interface of the Email appliance. You must specify an IP address only. Do not use a fully-qualified domain name (FQDN). When you click **Next**, communication with the specified appliance will be verified. Communication may be unsuccessful if:
 - Subscription key has already been applied to the appliance (typically meaning another installation of TRITON Manager has been used to manage the appliance). The subscription key must be reset on the appliance.
 - Version of software to be installed does not match the version of the appliance. Verify whether the versions match.
 - Specified appliance is a secondary appliance in a cluster. Specify the primary appliance in the cluster or a non-clustered appliance.
 - The appliance cannot connect to the specified database server (specified during product installation).
 - Firewall is blocking communication to the appliance on port 6671. Make sure any local firewall allows outbound communication on port 6671.
 - Appliance E1/P1 interface has not been correctly configured via the appliance CLI.

6. On the **Installation Folder** screen, specify the location to which you want to install Email module components and then click **Next**.

To select a location different than the default, use the **Browse** button.

Each component (Email module and/or Email Log Server) will be installed in its own folder under the parent folder you specify here.

7. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.

Click **Back** to return to any screen on which you want to modify settings.

8. The **Installing Forcepoint Email Protection Solutions** screen appears, as components are being installed.

9. Wait until the **Installation Complete** screen appears, and then click **Done**.

10. The TRITON Setup program closes. Installation is complete.

Installing Additional Components

In this topic:

- [Installing web components](#), page 1
 - [Installing data components](#), page 10
 - [Installing Email Log Server](#), page 17
-

Installing web components

The steps in this section describe the installation of web protection components if you have not already installed them on the TRITON management server. If you are distributing components across multiple machines, run the installer and complete the installation steps on each machine.

These instructions assume that you have already launched the installer and selected **Custom**.

Install Log Server

Log Server is a Windows-only component that logs Internet request data, including:

- Source of request
- Category or protocol associated with the request
- Whether the request was permitted or blocked
- Whether keyword blocking, file type blocking, quota allocations, bandwidth levels, or password protection were applied

Each Log Server instance can log to only one Log Database at a time, and only one Log Server can be installed for each Policy Server.

Log Server processing can consume considerable system resources.

In a software-based deployment, do not install Log Server on the same machine as Filtering Service or Network Agent—policy enforcement or logging performance may be affected if they are on the same machine.

In an appliance-based deployment, Log Server must be installed on a separate Windows machine.



Note

Log Server must be installed before you can see charts on the **Status > Dashboard** page, or run presentation or investigative reports in the Web module of TRITON Manager.

Installation steps

To be able to install Log Server, a supported database engine (see [Reporting database requirements, page 9](#)) must be running.

1. On the **Select Components** screen in the TRITON installer, select Log Server. If you have purchased the Web Hybrid module, select Sync Service.
2. On the [Policy Server Connection screen](#), enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).
3. On the Policy Broker Connection screen, enter the TRITON management server IP address and the Policy Broker communication port (55880, by default), and then click Next.

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

4. If the Log Server server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components.

Depending on your current configuration, the Native Client installer may run silently in the background, or prompt you for input.

- When the Native Client installer runs in the background, you will know the process is complete when the Forcepoint installer continues to the next screen. This may take a few minutes.
 - When the Native Client installer runs in the foreground, follow the prompts to complete the installation. Note that if you are prompted to reboot the machine, do not reboot at this point. Instead, complete the Forcepoint software installation first, then reboot.
5. On the **Database Information** screen, enter the hostname or IP address of the machine on which a supported database engine is running. If a supported database engine is detected on this machine, its IP address is already entered by default. To use a database engine on a different machine, enter its IP address instead.

If you are using SQL Server clustering, enter the virtual IP address of the cluster.

After entering the IP address of the database engine machine, choose how to connect to the database:

- Select **Trusted connection** to use a Windows account to connect to the database. Enter the user name and password of a trusted account with local administration privileges on the database machine. Note that the trusted account you specify here should be the same as that with which you logged onto this machine before starting the TRITON installer.

If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web module of TRITON Manager. See [Configuring Apache services to use a trusted connection](#).

- Select **SQL Server Authentication** to use a SQL Server account to connect to the database. Enter the user name and password for a SQL Server account that has administrative access to the database. The SQL Server password cannot be blank, or begin or end with a hyphen (-).



Note

The database engine must be running to install TRITON reporting components. The installer will test for a connection to the specified database engine when you click **Next** on the **Database Information** screen. The installer cannot proceed unless a successful connection can be made.

6. On the **Log Database Location** screen, accept the default location for the Log Database files, or select a different location. Then click **Next**.

The default database location information is taken from TRITON Infrastructure's configuration. Typically, you should accept the default in this case.

If the database engine is on this machine, the default location is the **Websense directory (C:\Program Files (x86)\Websense)**. If the database engine is on another machine, the default location is **C:\Program Files\Microsoft SQL Server** on that machine.

It is a best practice to use the default location. If you want to create the Log Database files in a different location (or if you already have Log Database files in a different location), enter the path. The path entered here is understood to refer to the machine on which the database engine is located.



Important

The directory you specify for the Log Database files must already exist. The installer cannot create a new directory.

You can also specify a particular database instance in this path. The instance must already exist. See Microsoft SQL Server documentation for information about instances and paths to instances.

7. On the **Optimize Log Database Size** screen, select either or both of the following options and then click **Next**.

- **Log web page visits:** Enable this option to log one record (or a few records) with combined hits and bandwidth data for each web page requested rather than a record for each separate file included in the web page request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities. Deselect this option to log a record of each separate file that is part of a web page request, including images and advertisements. This results in more precise reports, but creates a much larger database and causes reports to generate more slowly.
 - **Consolidate requests:** Enable this option to combine Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):
 - Domain name (for example: www.forcepoint.com)
 - Category
 - Keyword
 - Action (for example: Category Blocked)
 - User/workstation
8. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

The installation path must be absolute (not relative). The default installation path is:

C:\Program Files or Program Files (x86)\Websense\Web Security

The installer creates this directory if it does not exist.



Important

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

The installer compares the installation's system requirements with the machine's resources.

- Insufficient disk space prompts an error message. The installer closes when you click **OK**.
 - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.
9. On the **Pre-Installation Summary** screen, verify the information shown. The summary shows the installation path and size, and the components to be installed.
10. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
11. On the **Installation Complete** screen, click **Done**.

12. After installing Log Server, restart the TRITON management server machine.



Important

When Log Server is not installed on the TRITON management server, be sure to restart the management server before creating scheduled jobs in presentation reports. Any scheduled jobs you create before restarting the server cannot be saved properly and will be lost, even if they appear to work for a period of time.

Install an instance of Filtering Service

When the standalone or primary Policy Broker and the central Policy Server reside on the TRITON management server, you must install at least one instance of Filtering Service that connects to the central Policy Server.

This instance of Filtering Service may reside:

- On a supported Linux server
- On a supported Windows server
- On a **filtering only** appliance

Note that using a software installation for this instance of Filtering Service may make for a more convenient deployment. A software deployment allows you to also install components like User Service and Usage Monitor for the central Policy Server. (These components don't reside on a filtering only appliance.)

Best practice is to install Filtering Service on a different machine from the TRITON management server. This is because Filtering Service can consume considerable system resources and may have a performance impact on the server.

Although other components (like Network Agent or a transparent identification agent) may be installed with Filtering Service, a second instance of Policy Server may **not** reside on this machine. This Filtering Service instance **must** connect to the central Policy Server on the TRITON management server machine.

Using a filtering-only appliance

Follow the setup, firstboot, and initial configuration instructions in the [TRITON Appliances Getting Started Guide](#).

Installing Filtering Service on Windows

Ensure you have prepared the machine as described in *Preparing servers for TRITON deployments*, page 11.

To install Filtering Service on a supported Windows platform:

1. Log on to the machine with domain admin privileges.
2. Download the TRITON Unified Installer (**TRITON83xSetup.exe**) from [My Account](#).

3. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
4. On the Welcome screen, click **Start**.
5. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
6. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that TRITON AP-WEB components should use for communication, then click **Next**.
7. On the Installation Type screen, select **Custom** and then click **Next**.
8. On the Select Components screen, select the following components, then click **Next**:
 - Filtering Service
 - User Service
 - Usage MonitorOptionally, you may also select:
 - Network Agent
 - State Server
 - DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
 - Directory Agent (*used by the Web Hybrid module*)
9. On the Policy Server Connection screen, enter the IP address of the central Policy Server machine and the Policy Server communication port (55806, by default), then click **Next**.
10. If you are installing Directory Agent, on the Policy Broker Connection screen, enter the IP address of the primary or standalone Policy Broker and its communication port (55880, by default), then click **Next**.
11. On the Active Directory screen, indicate whether you are using Windows Active Directory to authenticate users in your network, then click **Next**.
12. On the Computer Browser screen, indicate that the installer should attempt to start the service, then click **Next**.
13. On the Integration Option screen, select **Install TRITON AP-WEB to connect to Content Gateway**, then click **Next**.
14. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other TRITON AP-WEB components, then click **Next**.
15. On the Filtering Feedback screen, indicate whether you want your software to send feedback to Forcepoint LLC, then click **Next**.
16. On the Directory Service Access screen, enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller, then click **Next**.

User Service, DC Agent, and Logon Agent use this information to query the domain controller for user and group information.

17. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click **Next**.

The installation path must be absolute (not relative). The default installation path is C:\Program Files (x86)\Websense\Web Security\.

The installer creates this directory if it does not exist.



Important

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

18. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.
The summary shows the installation path and size, and the components to be installed.
19. A progress screen is displayed. Wait for the installation to complete.
20. On the Installation Complete screen, click **Finish**.

Installing Filtering Service on Linux

Ensure you have prepared the machine as described in [Preparing servers for TRITON deployments](#), page 11.

1. Log on to the installation machine with full administrative privileges (typically, **root**).
2. Create a setup directory for the installer files. For example:

```
/root/Websense_setup
```

3. Download the Web Security Linux installer package from [My Account](#). The installer package is called **Web83xSetup_Lnx.tar.gz**.

Place the installer archive in the setup directory you created.

4. In the setup directory, enter the following commands to uncompress and extract files:

```
tar -xvzf Web83xSetup_Lnx.tar.gz
```

5. Launch the installer using the following command (from the setup directory):

```
./install.sh -g
```

This launches a GUI-based installer and is available on English versions of Linux only. A text-only, command-line version can be launched by omitting the -g switch:

```
./install.sh
```

Perform the Filtering Service installation

1. On the Introduction screen, click or select **Next**.
2. On the Subscription Agreement screen, choose to accept the terms of the agreement and then click **Next**.

3. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that Web Security components should use for communication, then click **Next**.
4. On the Installation Type screen, select **Custom** and then click or select **Next**.
5. On the Select Components screen, select the following components, then click or select **Next**:
 - Filtering Service
 - User Service
Note that if User Service is installed on Linux, and use Windows Active Directory as your user directory, you must configure a WINS server to enable User Service to retrieve user and group information.
 - Usage MonitorOptionally, you may also select:
 - Network Agent
 - State Server
 - Logon Agent, eDirectory Agent, or RADIUS Agent
 - Directory Agent (*used by the Web Hybrid module*)
6. On the Policy Server Connection screen, enter the central Policy Server IP address and communication port (55806, by default).
7. If you are installing Directory Agent, on the Policy Broker Connection screen, enter the IP address of the primary or standalone Policy Broker machine, and the Policy Broker communication port (55880, by default).
8. On the Integration Option screen, select **Install TRITON AP-WEB to connect to Content Gateway**, then click or select **Next**.

When you install Content Gateway, you will be prompted for the Filtering Service IP address.
9. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other Web Security components, then click or select **Next**.
10. On the Filtering Feedback screen, indicate whether you want your software to send feedback to Forcepoint LLC, then click or select **Next**.
11. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click or select **Next**.

The installation path must be absolute (not relative). The default installation path is: /opt/Websense/
The installer creates this directory if it does not exist.



Important

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

The installer compares the installation's system requirements with the machine's resources.

- Insufficient disk space prompts an error message. The installer closes when you click or select **OK**.
 - Insufficient RAM prompts a warning message. The installation continues when you click or select **OK**. To ensure optimal performance, increase your memory to the recommended amount.
12. On the Pre-Installation Summary screen, verify the information shown, then click or select **Next**.

The summary shows the installation path and size, and the components to be installed.

13. An Installing progress screen is displayed. Wait for the installation to complete.

**Note**

If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

14. On the Installation Complete screen, click or select **Done**.

Install Content Gateway

Content Gateway is a Linux-based, high-performance web proxy and cache that provides real-time content analysis and website classification to protect clients from malicious content while enabling access to safe content.

Content Gateway offers:

- Categorization of dynamic websites
- Categorization of new and unclassified websites
- Optionally, HTTPS and FTP content analysis, in addition to HTTP
- Enterprise Web proxy caching capabilities
- Prevention of data loss over web channels

Content Gateway is a required component of TRITON AP-WEB. In a software-based deployment, Content Gateway must be installed on a Linux machine. The machine should be dedicated to running Content Gateway.

**Important**

In an appliance-based deployment, when TRITON AP-WEB is configured, Content Gateway is already installed. TRITON AP-WEB and TRITON AP-EMAIL cannot be installed on the same appliance.

For full instructions on preparing a Linux machine and installing Content Gateway, see the installation instructions for [TRITON AP-WEB](#).

Installing other web components

For information about installing other web protection components, see the section “Install additional web protection components” in the installation instructions for [TRITON AP-WEB](#).

Installing data components

Once you’ve installed TRITON AP-DATA on the TRITON management server, 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

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 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

Hardware requirements

Supplemental 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.
- 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\\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 TRITON 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 TRITON 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 3 GB of free disk space 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 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 onto the Data module of TRITON 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 that you can install.

With the exception of the protector, mobile agent, 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. For example, the FCI agent is only shown as an option on machines with Microsoft FSRM installed.

For instructions on how to install the agents, see the [TRITON AP-DATA Installation Guide](#).

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, plain text, and IM traffic that doesn't use SSL. For blocking HTTPS traffic, the protector can integrate with proxies using ICAP.	Monitor/block: network email Monitor: HTTP, FTP, plain text, IM 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 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.	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.	Monitor/block/quarantine/encrypt: Email traffic	On premises
Email Gateway for Microsoft 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.	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 95 for more information.	High risk incident scoring	On premises
TRITON AP-DATA Cloud	TRITON AP-DATA Cloud 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, page 99 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.	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.	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.	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.

Installing Email Log Server

TRITON AP-EMAIL is an appliance-based solution. All components run on the appliance except the Email module of TRITON Manager and Email Log Server. These are the only two TRITON AP-EMAIL components that may be installed using the Forcepoint installer.

You cannot install TRITON AP-EMAIL on the same appliance as TRITON AP-WEB. It is recommended that you install Email Log Server on a different machine from the TRITON management server:

1. Download and launch the Forcepoint installer on the Log Server machine.
2. Choose the **Custom** installation type.

3. On the **Custom Installation** dashboard, click the **Install** link for TRITON AP-EMAIL.

The Email component installer is launched.

4. On the **Introduction** screen, click **Next**.

The TRITON AP-EMAIL Installer does not detect TRITON Infrastructure on the machine, and operates in custom mode.

5. In the **Select Components** screen, Email Log Server is selected for installation by default. To install Email Log Server, SQL Server must already be installed and running in your network. (See [Reporting database requirements](#), page 9, for supported database systems.)

If you choose to install Email Log Server, the Email Log Server Configuration utility is also installed. This utility can be accessed by selecting **Start > All Programs > Websense > Email Security > Email Log Server Configuration**.

6. On the **Email Log Database** screen, specify the location of a database engine and how you want to connect to it.

- **Log Database IP:** Enter the IP address of the database engine machine. If you want to use a named database instance, enter it the form `<IP address>\<instance name>`. Note that the instance must already exist. See your SQL Server documentation for instructions on creating instances.

- You may specify whether the connection to the database should be encrypted.

Please note the following issues associated with using this encryption feature:

- By default, Email Log Server uses NTLMv2 to encrypt the connection. If you want to use SSL encryption, you must have imported a trusted certificate to the Log Server machine. See your database documentation for information about importing a trusted certificate.
- The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
- The connection from the Email module in TRITON Manager to the Forcepoint appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.

- **Database login type:** Select how Email Log Server should connect to the database engine.

- **Trusted connection:** connect using a Windows trusted connection.
- **Database account:** connect using a SQL Server account.

Then enter a user name and password.

- If using a trusted connection, enter the domain\username of the account to be used. This account must be a trusted local administrator on the database engine machine.
- If using a database account, enter the name of a SQL Server account. This account must have certain roles assigned; see [Installing with SQL Server](#).

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

7. On the **Email Log Database File Location** screen, specify where the email Log Database files should be located and then click **Next**.

It is a best practice to use the default location. However, if you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files.

The path entered here is understood to refer to the machine on which the database engine is located. The path entered must specify a directory that already exists.

If any email components (e.g., the Email module in TRITON Manager or another instance of Email Log Server) have already been installed in your deployment, the following message appears:

The Email Log database exists, do you want to remove it?

This occurs because the database was created upon installation of the other email components. Click **No** to continue using the existing database. In general, you should keep the database if you are sure the database was created only during the course of installing other components in your current deployment.

Clicking **Yes** removes the database.



Warning

If any TRITON AP-EMAIL log data has been written to the database it will be lost if you remove the database. If you want to keep this data, back up the esglogdb76 and esglogdb76_n databases. See your SQL Server documentation for backup instructions.



Warning

If you remove the database, any currently quarantined email will no longer be accessible.

8. On the **Installation Folder** screen, specify the location to which you want to install Email Log Server and then click **Next**.



Important

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

To select a location different than the default, use the **Browse** button.

Email Log Server will be installed in its own folder under the parent folder you specify here.

9. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.
10. The **Installing Forcepoint Email Protection Solutions** screen appears, as components are being installed.
11. Wait until the **Installation Complete** screen appears, and then click **Done**.

Initial Configuration

In this topic:

- [General configuration](#), page 1
 - [Log on to the TRITON Manager](#), page 2
 - [TRITON AP-WEB initial configuration](#), page 3
 - [Additional configuration for the Web DLP Module](#), page 4
 - [TRITON AP-DATA initial configuration](#), page 8
 - [TRITON AP-EMAIL initial configuration](#), page 8
 - [Content Gateway initial configuration](#), page 10
 - [Network Agent and stealth mode NICs](#), page 11
-

General configuration

- Some of the ports required by TRITON components during installation are no longer needed when installation is complete. For information about the ports required for component communication, as well as details about which components need Internet access, see [TRITON default ports](#).
- To avoid interference with the performance of TRITON components, exclude certain TRITON folders and files from antivirus scans. See [Excluding your files from antivirus scans](#).

- If administrators use Internet Explorer to access TRITON Manager, make sure that Enhanced Security Configuration is disabled on their machines.

For example, in Windows Server 2008:

- a. Open the Server Manager.
- b. Under **Server Summary**, in the Security Information section, click **Configure IE ESC**.
- c. In the **Internet Explorer Enhanced Security Configuration** dialog box, under **Administrators**, select the **Off** radio button, and then click **OK**.

Administrators may also need to restore default settings in their browser in order for TRITON Manager to display properly in Internet Explorer. To do this, in

Internet Explorer go to **Tools > Internet Options** and select the **Advanced** tab, then click **Reset**. When prompted, click **Reset** again.

Log on to the TRITON Manager

1. Use a supported browser (see [Requirements, page 6](#)) to launch TRITON Manager and log on using the default account:
 - a. Navigate to the following URL:
`https://<IP_address>:9443/triton/`
Here, *<IP_address>* is the IP address of the TRITON management server.
 - b. Log on as the default **admin** account, using the password set during installation.



Note

Ensure you have installed all the TRITON components that you need in your deployment before you enter subscription keys. If components are missing, the keys will not validate.

2. Enter your subscription key or keys. At first startup:
 - The Web module prompts for a subscription key in the Initial Setup Checklist.
The key you enter is automatically applied to Content Gateway as well.
 - The Data module displays the subscription key page. See the *Initial Setup* section of the TRITON AP-DATA Help for more information.
 - The Email module prompts for a subscription key. If you do not enter the subscription key in the prompt, you can enter it in the **Settings > General > Subscription** page. See the TRITON AP-EMAIL Administrator Help for more information.Enter your subscription key and save the change in all modules.
3. If you did not provide SMTP server details during installation, use the **General > Notifications** page under TRITON Settings to specify the SMTP server used to enable administrator password reset functionality and account change notifications. See the TRITON Manager Help for more information.

Continue with the initial configuration steps for the TRITON advanced protection solutions you have installed:

- [TRITON AP-WEB initial configuration, page 3](#)
- [TRITON AP-DATA initial configuration, page 8](#)
- [TRITON AP-EMAIL initial configuration, page 8](#)
- [Content Gateway initial configuration, page 10](#)

TRITON AP-WEB initial configuration

Getting started with Web Protection solutions

After entering your TRITON AP-WEB subscription key, use the Initial Setup Checklist to complete basic setup tasks.

- Also see *Content Gateway initial configuration*, page 10.
- If you have the Web Hybrid Module, also see *Additional configuration for the Web DLP Module*, page 4.

Next, you can:

- Configure transparent user identification on the **Settings > General > User Identification** page (see the “User Identification” topic in the TRITON AP-WEB Help).
 - If you installed Logon Agent, you must create and deploy a client logon script in addition to configuring Logon Agent in the Web module of TRITON Manager. See the [Using Logon Agent for Transparent User Identification](#) technical paper for instructions.
 - If you were unable to grant User Service, DC Agent, or Logon Agent administrator privileges during installation, see the “Troubleshooting” > “User Identification” topic on changing User Service, DC Agent, and Logon Agent service permissions in the TRITON AP-WEB Help.
- Enable email or SNMP alerting on the **Settings > Alerts > Enable Alerts** page (see the “Alerting” topic in the TRITON AP-WEB Help).
- Customize reporting behavior (see the “Reporting Administration” topic in the TRITON AP-WEB Help).
- Configure optional Remote Filtering components to enable filtering of off-site users. For instructions, see the [Remote Filtering Software](#) technical paper.

Additional tips for working with Web Protection solutions

- All Forcepoint tools and utilities installed on Windows Server platforms (such as wsbackup.exe and websenseping.exe), as well as text editors used to modify configuration files (such as websense.ini), **must** be run as the local administrator. Otherwise, you may be prevented from running the tool or the changes you make may not be implemented.
 1. Navigate to the **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin\).
 2. Right-click the relevant executable file, and then click **Properties**. Following is a list of files for which this should be done.
 3. In the **Compatibility** tab, under **Privilege Level**, select **Run this program as an administrator**. Then, click **OK**.

- If you installed Network Agent on a machine with multiple NICs, you can configure the agent to use more than one NIC to monitor and block requests. See the “Network Configuration” topic in the TRITON AP-WEB Help for more information. To configure a stealth mode NIC for monitoring, see [Network Agent and stealth mode NICs, page 11](#).

Identifying Filtering Service by IP address

When your software blocks an Internet request, the browser is redirected to a block page hosted by Filtering Service. The block page URL takes the form:

```
http://<FilteringServiceNameorIPAddress>:<MessagePort>/cgi-bin/blockpage.cgi?ws-session=#####
```

If Filtering Service is installed on a machine with multiple NICs, and Filtering Service is identified by machine hostname rather than IP address, users could receive a blank page rather than a block page.

- If you have an internal domain name server (DNS), enter the Filtering Service machine’s IP address as a resource record in your DNS. See your DNS documentation for instructions.
- If you do not have an internal DNS:
 1. On the Filtering Service machine, go to the **bin** directory (by default, **C:\Program Files\WebSense\bin** or **opt/WebSense/bin**).
 2. Make a backup copy of **eimserver.ini** in another directory.
 3. Open the original **eimserver.ini** file in a text editor.
 4. In the **[WebSenseServer]** section, enter the following command:

```
BlockMsgServerName=<IP address>
```

Here, *<IP address>* is the IP address of the Filtering Service machine.



Important

Do not use the loopback address (127.0.0.1).

5. Save the file.
6. Restart Filtering Service.
 - *Windows:* Use the Windows Services dialog box (Start > Administrative Tools > Services) to restart **WebSense Filtering Service**.
 - *Linux:* Use the `/opt/WebSense/WebSenseDaemonControl` command to restart **Filtering Service**.

Additional configuration for the Web DLP Module

In addition to the items under [TRITON AP-WEB initial configuration, page 3](#), perform these procedures if your subscription includes the Web DLP Module.

Confirm Content Gateway registration with TRITON AP-DATA

If you have purchased the Web DLP module, Content Gateway registers with TRITON AP-DATA automatically. To ensure that registration is successful:

- 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 Forcepoint 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 Forcepoint 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.

If registration fails an alarm displays in Content Gateway Manager.

1. Verify connectivity between Content Gateway and the TRITON management server.
2. In Content Gateway Manager, on the **Configure > My Proxy > Basic > General** page, in the **Networking** section confirm that **Web DLP > Integrated on-box** is enabled.
3. Restart Content Gateway to initiate another registration attempt.

Alternatively:

- a. Go to **Configure > Security > Web DLP** and enter the IP address of the management server.
- b. Enter a user name and password for a Data module administrator with Deploy Settings privileges.
- c. Click **Register**.

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.

Web DLP components communicate with the Content Gateway proxy over ports 17000-17014.

Configure the Content Gateway policy engine

When Content Gateway is registered with Web DLP components, a Content Gateway module appears on the System Modules page of the Data module of the TRITON 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 module of the TRITON Manager, go to the **Settings > Deployment > System Modules** page.
2. Select the Content Gateway module in the tree view (click the module name itself, not the plus sign next to it).
It will be listed as **Content Gateway 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.

- 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.

**Important**

If your software deployment is on RHEL 7.x or CentOS 7.x, you must do the following in order to successfully deploy Policy Engine.

On the Content Gateway machine:

- Stop IPTables:

```
service iptables stop
```

- Stop and disable FirewallD:

```
service firewalld stop  
systemctl disable firewalld
```

- Run the following:

```
sysctl -w net.ipv4.tcp_tw_recycle=0
```

- Deploy Policy Engine.

- Restart IPTables:

```
/opt/WCG/bin/netcontrol.sh -i
```

Verify that web and data protection components are linked

When Linking Service is installed, it allows Web DLP components to access user identification and URL categorization data. To verify that it is working:

- Log onto the Data module of the TRITON Manager.
- Select **Settings** (under General) > **System** > **URL Categories & User Names**.
- Verify settings and test the connection.
Select **Help** > **Explain This Page** for detailed information about the settings on this screen.
- Click **OK** to save any changes.
- Click **Deploy** to deploy your settings.

TRITON AP-DATA initial configuration



Note

TRITON AP-DATA may not be available immediately after installation. It takes a few minutes to initialize the system after it is first installed.

To complete your TRITON AP-DATA installation, log onto the Data module of TRITON Manager and click **Deploy**.

See the [Initial Setup](#) section of the TRITON AP-DATA Help for information on the following topics:

- Defining general system settings
 - Connection to directory services
 - System alerts
- Setting up notifications
 - Notifications when policy breaches occur
- Configuring Web attributes
 - Web DLP policies
 - Policies for particular websites
 - Policy owners
- Configuring email policies
- Creating a regulatory and compliance policy
- Configuring system modules
 - Viewing TRITON AP-DATA modules
 - Configuring the protector
- Deploying your settings

TRITON AP-EMAIL initial configuration

initial configuration settings

The first time you access the Email module of TRITON Manager, you are prompted for your subscription key. Then, you are asked if you want to use the First-Time Configuration Wizard. This wizard guides you through the process of entering some

essential configuration settings. It is strongly recommended you use this wizard. See the TRITON AP-EMAIL Administrator Help for more information about the wizard.



Important

The configuration wizard is offered only once, at initial start up of the Email module of TRITON Manager. If you choose to not use the wizard it will no longer be available. All settings configured in the wizard can be configured in TRITON Manager individually. The wizard simply offers a more convenient way to enter some initial settings.

See the [Getting Started](#) section in the TRITON AP-EMAIL Administrator Help for information on initial configuration in the following areas:

- First-time Configuration Wizard, for establishing
 - An initial mail route for a protected domain
 - Trusted IP addresses for which some inbound email analysis is not performed
 - Email Log Server IP address and port
 - System notification email address
- TRITON AP-DATA registration, to allow the use of email data loss prevention (DLP) policy options
- Master database download scheduling, to manage message analysis database updates

For help with the following TRITON AP-EMAIL settings, see the [Configuring System Settings](#) section in the TRITON AP-EMAIL Administrator Help:

- Delegated administrator management, to modify administrator roles established in the TRITON Manager
- System settings, to establish system preferences like the SMTP greeting and system notification email address
- Appliance management, for administering all the appliances in your email protection system
- User directory creation and management
- Protected domain and trusted IP address lists, to designate all the domains that you want protected and the IP addresses whose mail can bypass some email analysis
- User authentication and recipient validation options
- Transport Layer Security (TLS) certificate handling, to provide an extra layer of security for email communications
- Trusted CA certificate importing
- Email module backup and restore functions, to preserve important configuration files, including your appliances list, administrator settings, and report templates
- System alerts, to configure delivery methods for distributing various email system health alerts

Email Hybrid Module initial configuration

If your subscription includes the Email Hybrid Module, you need to register with the email hybrid service. See the [Registering for the hybrid service](#) topic in the TRITON AP-EMAIL Administrator Help for descriptions of email hybrid service registration.

After you have registered with the email hybrid service, you can configure Email Hybrid Service Log properties and view the Email Hybrid Service Log. See TRITON AP-EMAIL Administrator Help for details.

Content Gateway initial configuration

After Content Gateway is installed, perform these basic configuration activities:



Note

The subscription key is **automatically applied** to Content Gateway when you enter it in the Web module of TRITON Manager.

- Log onto 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](#). Alternatively, configure TRITON AP-WEB user identification.
- Configure the real-time [Scanning Options](#) in the Web module of the TRITON Manager.
- If you enabled content caching during installation, [configure content caching](#).

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

- If you are using HTTPS (SSL Manager), use the Web module of the TRITON Manager to configure categories, clients, and destination servers for [SSL decryption bypass](#)
- Create Content Gateway [filtering rules](#) to:
 - Deny or allow URL requests
 - Insert custom headers
 - Allow specified applications, or requests to specified Web sites to bypass authentication

- Keep or strip header information from client requests
- Prevent specified applications from transiting the proxy
- 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).
- The ARM (Adaptive Redirection Module) module of Content Gateway uses a firewall. To facilitate interception and redirection of traffic:
 - IPTables rules are configured during installation of Content Gateway.
 - Forcepoint IPTables chains are inserted.
 - Forcepoint IPTables rules are also inserted into existing chains.
 - Forcepoint chains and rules use “NC_” as a prefix for identification purposes.
 - IPTables rules configured outside of Content Gateway Manager must
 - Be inserted after Forcepoint rules.
 - Never be added to Forcepoint chains.
 - Forcepoint chains and rules should never be edited.
 - If customized chains or rules impact the Forcepoint configuration, navigate to /opt/wcg/bin and execute the following to re-establish the Forcepoint IPTables chains and rules.:

```
netcontrol.sh -r
```

Network Agent and stealth mode NICs

Your software can inspect all packets with a monitoring NIC (network interface card) that has been configured for *stealth mode*. A NIC in stealth mode has no IP address and cannot be used for communication. Security and network performance are improved with this configuration. Removing the IP address prevents connections to the NIC from outside resources and stops unwanted broadcasts.

If Network Agent is configured to use a stealth-mode NIC, the installation machine must have multiple NICs. If Network Agent is installed on a separate machine, a second, TCP/IP-capable interface (i.e., it is not in stealth mode) must be configured to communicate with your software for filtering and logging.

During installation, stealth-mode interfaces do not display as a choice for Forcepoint communications. Make sure you know the configuration of all the interfaces in the machine before attempting an installation.



Important

On Linux, stealth mode NICs appear together with TCP/IP-capable interfaces and must not be selected for communication.

Stealth mode for the Network Agent interface is supported on Windows and Linux.

Windows

Configure a NIC for stealth mode as follows.

1. Go to **Start > Settings > Network and Dial-up Connection** to display a list of all the interfaces active in the machine.
2. Select the interface you want to configure.
3. Select **File > Properties**.
A dialog box displays the NIC connection properties.
4. Clear the **Internet Protocol (TCP/IP)** checkbox.
5. Click **OK**.

Linux

To configure a NIC for stealth mode in Linux, disable the Address Resolution Protocol (ARP), which breaks the link between the IP address and the MAC address of the interface. Run the following commands, replacing *<interface>* with the NIC's name, for example, **eth0**.

- To configure a NIC for stealth mode, run this command:

```
ifconfig <interface> -arp up
```

- To return the NIC to normal mode, run this command:

```
ifconfig <interface> arp up
```



Important

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file, **/etc/sysconfig/network-scripts/ifcfg-*<adapter name>***.
