Forcepoint DLP

8.5.x-9.0

Deployment and Installation Center

Revision A

Published 14 October 2022

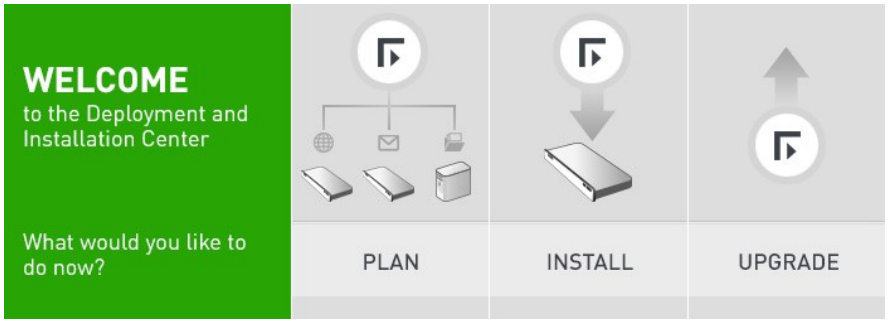
Contents

Chapter 1

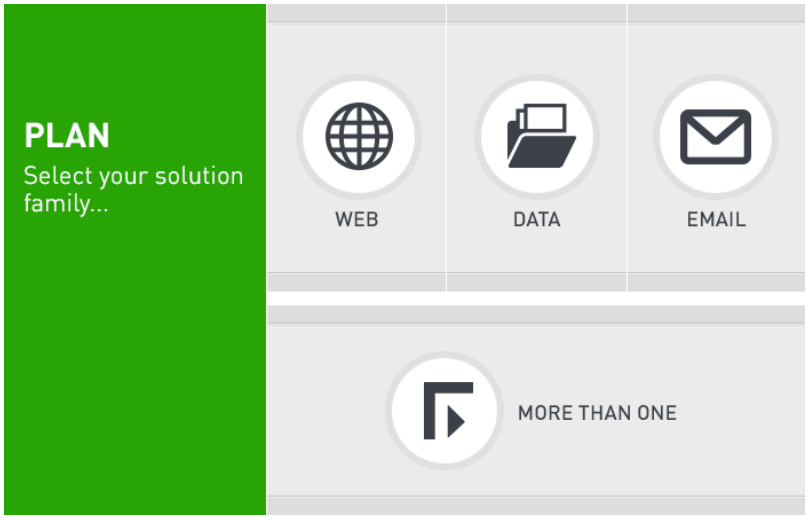
Deployment and Installation Center

Contents

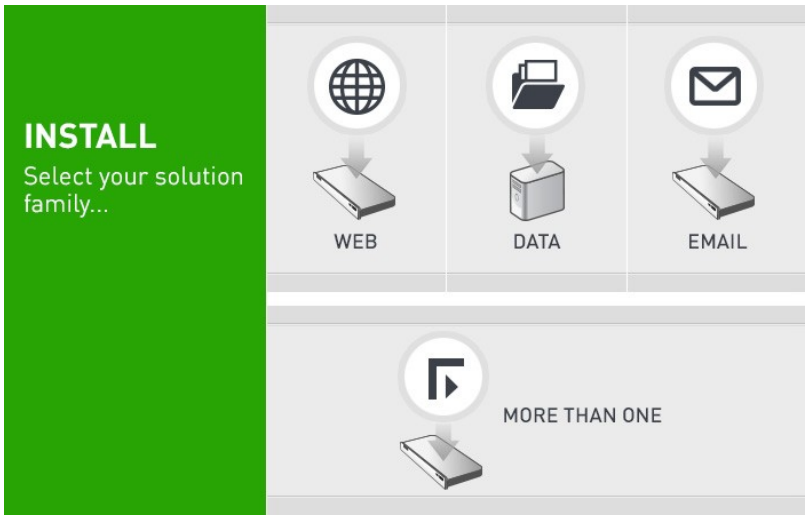
Welcome to the Deployment and Installation Center.



Planning your deployment



Installing your security solution



Upgrading your security solution

System requirements for this version

Applies to	In this topic
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint Appliances, v8.5.x	■ *Forcepoint management server requirements* ■ *Supported Forcepoint appliance models and modes* ■ *Reporting database requirements* ■ *Requirements for web protection solutions* ■ *Requirements for email protection solutions* ■ *Forcepoint DLP requirements* ■ *Analytics engine hardware requirements*

Note

- Forcepoint DLP v9.0 and later is supported with Forcepoint Web and Email Security v8.5.5.
- Forcepoint DLP v8.7.1 and later is supported with Forcepoint Web and Email Security v8.5.4.
- Forcepoint DLP v8.6 and v8.7 are supported with Forcepoint Web and Email Security v8.5.3.
- Forcepoint DLP v8.5.1 is supported with Forcepoint Web and Email Security v8.5.0.
- Forcepoint DLP v8.5.0 and v8.5.2 are stand-alone versions of that product and cannot be integrated with other Forcepoint products.

- **Forcepoint management server requirements**

  The **Forcepoint management server** hosts the Forcepoint Security Manager (Security Manager), which includes:

  - The infrastructure uniting all management components
  - A settings database for administrator account information and other shared data

- One or more management modules, used for configuration, policy management, and reporting

Additional components may also reside on the management server. For a list of operating systems that are supported, see the Certified Product Matrix on the Forcepoint website.

- **Hardware requirements**

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

  Note

  - Forcepoint DLP allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90 GB from the Forcepoint DLP disk space requirements.
  - It is strongly recommended that 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), it must have at least 4 GB free on the Windows partition to accommodate the Forcepoint Security Installer.

With remote (standard or enterprise) reporting database

Management modules	Recommended	Minimum
Web Security	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 Security	8 CPU cores (2.5 GHz), 16 GB available RAM, 400 GB Disk space	4 CPU cores (2.5 GHz), 16 GB available RAM, 146 GB Disk Space
Web Security and Data Security	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 Security and Data Security	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 Security, Data Security, and Email Security	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 Security	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 Security	8 CPU cores (2.5 GHz), 16 GB available RAM, 400 GB Disk space	4 CPU cores (2.5 GHz), 16 GB available RAM, 240 GB Disk Space

Management modules	Recommended	Minimum
Web Security and Data Security	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
Email Security and Data Security	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 Security, Data Security, and Email Security	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

- **Forcepoint Security Manager browser support**
  The Security Manager is a web-based tool that 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 the Security Manager using non-supported browsers, you may not receive full functionality and proper display of the application.

- **Virtualization systems**

  Note

  - Forcepoint Web Security v8.5.3 and v8.5.4, Forcepoint Email Security v8.5.3 and v8.5.4, and Forcepoint DLP v8.6 and later are not supported on Windows Server 2008 R2.
  - Forcepoint Web Security v8.5.4 and Forcepoint DLP v8.7.1 and later are not supported on Windows Server 2012 R2 Datacenter Edition.

  All Security Manager components, as well as secondary Forcepoint DLP servers, are supported on the following virtualization systems. Other components (used for enforcement, analysis, or reporting) may have additional requirements that are not supported by these virtualization environments.

  - 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, Windows Server 2012 R2, and Windows Server 2016 over Hyper-V 2012 R2
  - Windows Server 2008 R2 SP1 over VMware ESXi v5.x
  - Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 over VMware ESXi 6.x

  Note

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

  Before installing Forcepoint software on a VM via ESXi, ensure that the VMware tools are up to date and that all hardware is compatible with VMware ESXi. Additionally, make sure that the resource specifications defined earlier in this document for non-virtualized systems are met.

- **Directory services for administrator authentication**
  If you allow users to log on to the Security Manager 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 Forcepoint appliance models and modes**
  For complete information on supported appliance models and modes, see:
  - Forcepoint X Series Certified Product Matrix
  - Forcepoint V Series Certified Product Matrix
  - Forcepoint Virtual Appliance Certified Product Matrix
  - The V Series appliances supported with version 8.0 and higher knowledge base article

- **Reporting database requirements**
  For all Forcepoint security solutions, Microsoft SQL Server is used to host the reporting database.
  - For evaluations and small deployments, some versions of the Forcepoint Security Installer can be used to install Microsoft SQL Server Express.
    When included, use only the version of SQL Server Express included in the Forcepoint Security Installer. If not included, download and install the supported version of SQL Server Express from Microsoft.
  - Larger organizations are advised to use Microsoft SQL Server Standard, Business Intelligence, or Enterprise. These SQL Server editions cannot reside on the Forcepoint management server.
    SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability (Forcepoint Email Security and Forcepoint Web Security only).

  The supported database engines are listed in the Certified Product Matrix.

- **Requirements for web protection solutions**
  - **Software components**:
    Do **not** install web protection components on a domain controller machine. The following components are Windows-only. See the Certified Product Matrix for a list of supported Windows versions.
    - Forcepoint Security Manager
    - Linking Service
    - Log Server
    - Cloud App Service
    - DC Agent
    - Real-Time Monitor

    Content Gateway is a Linux-only component. See the Certified Product Matrix for a list of supported operating systems. See *Content Gateway* for additional information.

    All other web protection components can run on any of the supporting operating systems listed on the Certified Product Matrix.

  - **Web components not available on Forcepoint appliances**
    The following web protection components do not run on appliances. If used, they must be installed off-appliance.
    - Forcepoint Security Manager
    - Log Server
    - Sync Service
    - DC Agent
    - Logon Agent
    - Cloud App Service

- Real-Time Monitor
- Linking Service
- Remote Filtering Server and Client (Forcepoint URL Filtering only)
- eDirectory Agent
- RADIUS Agent
- Network Agent (not available on X Series)

- **Content Gateway**

Important

Core policy components must be installed prior to Content Gateway. When Filtering Service is installed, Content Gateway must be specified as the integration product. See Installation Instructions: Forcepoint Web Security.

- **Hardware**

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum
Red Hat Enterprise Linux 6 series, 64-bit	8 GB recommended
Disk space	2 disks: ■ 100 GB for the operating system, Content Gateway, and temporary data. ■ 147 GB for caching **Important** If caching will not be used, this disk is not required. The caching disk: ■ Should be at least 2 GB and no more than 147 GB ■ Must be a raw disk, not a mounted file system ■ Must be dedicated ■ Must not be part of a software RAID ■ Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64 MB of write-through cache.
Network Interfaces	2

- **To support transparent proxy deployments**

Router	Must support WCCP v2. A Cisco router must run iOS 12.2 or later. The latest version is recommended. To support IPv6, WCCP v2.01 and Cisco router version 15.4(1)T or later are required. Client machines, the destination Web server, and Content Gateway must reside on different subnets.
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

- **Software**
  Content Gateway is supported on the operating systems listed on the Certified Product Matrix , as well as Forcepoint V Series, X Series, and Virtual Appliances.

  Forcepoint provides “best effort” support for newer versions of Red Hat Enterprise Linux. Under “best effort” support, Technical Support makes a best effort to troubleshoot cases in standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

  Only kernels shipped with the supported Linux versions are supported by Content Gateway. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

  ```
  /bin/uname -r
  ```

- **Required libraries in Red Hat Enterprise Linux**
  During Content Gateway installation, the installer will list missing packages and then exit the installer.

  To install the missing packages, the operating system must have a repository of available libraries. The Media repository on the Red Hat Enterprise Linux install DVD is an acceptable source of packages.

  After the repository is set up, all of the required dependencies can be automatically resolved by running:

  For Linux 6.x:

  ```
  yum install wcg_deps-1-0.noarch.rpm
  ```

  For Linux 7.x:

  ```
  yum install wcg_rh7_deps-1-0.noarch.rpm
  ```

  The above RPM is included in the Content Gateway install tree, at the same level as **wcg_install.sh**.

- **Integration with Forcepoint DLP**

Any version can be used via the ICAP interface. However, use of the integrated, on-box components is strongly recommended. See Content Gateway Manager Help for configuration instructions.

- **Web browsers**
  Content Gateway is configured and maintained with a web-based user interface called the Content Gateway manager. See the Certified Product Matrix for a list of browser the Content Gateway manager supports.

  Note

  The browser restrictions mentioned in the product matrix above apply only to the Content Gateway Manager and not to client browsers proxied by Content Gateway.

- **Client OS**
  The logon application (LogonApp.exe) is supported on the following operating systems:
  - Windows Vista with Service Pack 1 or higher (32-bit and 64-bit)
  - Windows 7 with Service Pack 1 (32-bit and 64-bit)
  - Windows 8
  - Windows 8.1 (v7.8.2 and later)
  - Windows 8.1, Update 1 (v7.8.3 and later)
  - Windows 10
  - Windows Server 2003
  - Windows Server 2008 R2 SP1
  - Mac OS X 10.8, 10.9.2, 10.9.5, and 10.10 (64-bit)
- **Integrations**
  Forcepoint URL Filtering may be integrated with the following third-party products.

Product	Versions
Microsoft Forefront TMG	2010
Cisco ASA	v8.0 or later
Cisco Router	iOS v15 or later
Citrix Presentation Server	4.5
Citrix XenApp	6.0 or 6.5

  In addition, products that can be configured to use ICAP can be integrated via the ICAP Service.
- **Directory services for user identification**
  Web protection solutions can use the following directory services listed in the Certified Product Matrix for user identification and authentication:
- **RADIUS**
  Most standard RADIUS servers are supported. The following have been tested:
  - Cistron RADIUS Server
  - Livingston (Lucent) 2.x
  - Merit AAA
  - Microsoft IAS
  - NMAS authentication
- **Requirements for email protection solutions**

The Forcepoint Email Security on-premises solution is exclusively appliance-based (V Series, X Series, and Virtual Appliance), except for the following components:

- **Email Security module** of the Forcepoint Security Manager, which runs on the Forcepoint management server (see *Forcepoint management server requirements*).
- **Log Server**, which runs on a Windows Server 2008 R2 SP1, 2012, 2014, or 2016 machine.
  - Windows Server 2008 R2 is not supported for v8.5.3 or v8.5.4.

  All components in the deployment, including those running off-appliance, must run the same version of Forcepoint software.

  See the Forcepoint Appliances Getting Started Guide for appliance specifications.

  Forcepoint Email Security version 8.5.x can be installed in a Microsoft Azure cloud environment. See Installing Forcepoint Email Security in Microsoft Azure for more information.

- **Forcepoint DLP requirements**
  Operating system

Forcepoint DLP Component	Supported Operating Systems	64-bit
Management server	Windows Server 2008 Standard or Enterprise, R2 SP1 (version 8.5.x only; not supported in version 8.6 or 8.7)	✓
	Windows Server 2012 Standard Edition	✓
	Windows Server 2012 Standard Edition R2	✓
	Windows Server 2016 Standard Edition	✓
	Windows Server 2019 Standard Edition	✓
Supplemental servers	Windows Server 2008 Standard or Enterprise, R2 SP1 (version 8.5.x only; not supported in version 8.6 or 8.7)	✓
	Windows Server 2012 Standard Edition	✓
	Windows Server 2012 Standard Edition R2	✓
	Windows Server 2016 Standard Edition	✓
	Windows Server 2019 Standard Edition	✓
Forcepoint DLP Email Gateway	CentOS 7.2 CentOS 7.5 (added in version 8.6)	✓
Web Content Gateway	Red Hat Enterprise Linux 6.8, 6.9, 7.2, 7.3, and 7.4	✓

Forcepoint DLP Component	Supported Operating Systems	64-bit
Crawler agent	Windows Server 2008 Standard or Enterprise, R2 SP1 (version 8.5.x only; not supported in version 8.6 or 8.7)	✓
	Windows Server 2012 Standard Edition	✓
	Windows Server 2016 Standard Edition	✓
	Windows Server 2019 Standard Edition	✓
Protector*	CentOS 7 CentOS 7.5 (added in version 8.6) CentOS 7.9 (added in version 8.8.1) Red Hat 7.5 (added in version 8.6)	
Analytics engine	CentOS 7 CentOS 7.5 (added in version 8.6)	
Endpoint agent	See the Certified Product Matrix	

*This operating system is installed as part of the protector “software appliance” installation.

Protector is supported on VMware systems in the Mail Transport Agent (MTA) mode and/or as an ICAP server with remote analysis (no local analysis). Other modes of deployment are not certified.

- **Forcepoint DLP server hardware requirements**

Server hardware	Minimum requirements	Recommended
CPU	4 CPU cores (2.5 GHz)	8 CPU cores (2.5 GHz)
Memory	16 GB available RAM	16 GB available RAM
Hard drives	Two 72 GB	Four 146 GB
Disk space	146 GB	400 GB
Free space	70 GB	70 GB
Hardware RAID	1	1 + 0
NICs	1	2

- **Forcepoint DLP server software requirements**
  The following requirements apply to all Forcepoint DLP servers:
  - For optimized performance, verify that the operating system’s file cluster is set to 4096B. For more information, see the Knowledge Base article File System Performance Optimization.
  - Windows installation requirements:
    - Set the partition to 1 NTFS Partition. For more information, see the 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 Forcepoint management server hostname must not include an underscore sign. Internet Explorer does not support such URLs.
- Short Directory Names and Short File Names must be enabled (registry value set to "0"). (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 Forcepoint DLP 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 Forcepoint management server.

- For Forcepoint DLP Server, v9.0:
  - Ensure that the Microsoft Visual C++ redistributable version 2022 (or later) is installed before installing the Forcepoint DLP Manager. Download the Visual C++ Redistributable for Visual Studio 2022 (or later) from Microsoft.

- **Protector hardware requirements**

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	2 GB	4 GB
Hard drives	2–72 GB	4–146 GB
Disk space	144 GB	292 GB
Hardware RAID	none	1 + 0
NICs	2 (monitoring)	2 (monitoring)

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

  Small to medium business

Hardware	Minimum	Recommended
CPU	4 core processors	8 core processors
Memory	8 GB	16 GB
Hard drives	100 GB	100 GB
NICs	1	1

  Medium to large business

Hardware	Minimum	Recommended
CPU	8 core processors	8 core processors
Memory	16 GB	20 GB
Hard drives	100 GB	100 GB
NICs	1	1

- **Forcepoint F1E solutions requirements**
  For information on hardware and operating system requirements for Forcepoint F1E agents, see the Installation and Deployment Guide for Forcepoint F1E Solution and Certified Product Matrix.

Preparing for installation

Applies to:	In this topic
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x	■ *All Forcepoint security solutions* ■ *Forcepoint Security Manager* ■ *Web protection components* ■ *Forcepoint DLP requirements*

Note

- Forcepoint DLP v9.0 and later is supported with Forcepoint Web and Email Security v8.5.5.
- Forcepoint DLP v8.7.1 and later is supported with Forcepoint Web and Email Security v8.5.4.
- Forcepoint DLP v8.6 and v8.7 are supported with Forcepoint Web and Email Security v8.5.3.
- Forcepoint DLP v8.5.1 is supported with Forcepoint Web and Email Security v8.5.0.
- Forcepoint DLP v8.5.0 and v8.5.2 are stand-alone versions of that product and cannot be integrated with other Forcepoint products.

All Forcepoint security solutions

Before installing any on-premises Forcepoint security solution, make sure that you have completed all of the preparations noted below:

Windows-specific considerations

- Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- In addition to the space required by the installer itself, roughly 2 GB of disk space is required on the Windows installation drive (typically C) to accommodate temporary files extracted as part of the installation process. For information on disk space requirements, see *Hardware requirements*
- The Forcepoint Security Installer requires .NET Framework v3.5 and v4.5-4.8.
  - 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://docs.microsoft.com/en-us/dotnet/framework/install/guide-for-developers?redirectedfrom=MSDN
  - For Windows Server 2012/2012 R2, you can add 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.

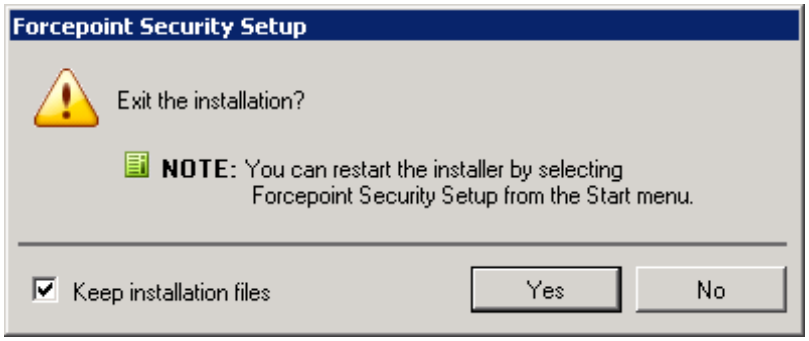
Getting the software installers

The Forcepoint Security Installer is used to install or upgrade the Forcepoint management server, web and data protection solutions, email protection management and reporting components, and, with some builds, SQL Server Express, on supported Windows servers.

There are separate installers for installing web protection components on supported Linux servers.

Download the Windows and Linux installers from the **My Account** section of forcepoint.com.

- The (Windows-only) Forcepoint Security Installer executable is named `Forcepoint8xxSetup.exe`. Find the version you are installing (v8.5.x, v8.6, v8.7.x, v8.8.x, v8.9.x or v9.0) and double-click it to start the installation process.
  If you have previously run the installer on a machine, and you selected the **Keep installation files** option, you can restart the installer without extracting all of the files a second time.



  - In the Start menu, open the **Forcepoint** folder and select **Forcepoint Security Setup** (Windows Server 2016 and 2008 R2 SP1).
    - Forcepoint DLP does not support Server 2008 R2.
  - On the Start screen, click the **Forcepoint Security Setup** icon (Windows Server 2016 and 2012).
    The files occupy approximately 5 GB of disk space.
- The web protection Linux installer is `Web85xSetup_Lnx.tar.gz`.
- The Content Gateway Linux installer is `ContentGateway85xSetup_Lnx.tar.gz`.

Local Admin privileges

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

Important

If you plan to install SQL Server Express and will use it to store and maintain data for your web protection solution, log in as a domain user to run the Forcepoint Security Installer.

Synchronizing clocks

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

Note

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

Antivirus

Disable any antivirus on the machine prior to installing Forcepoint components. Be sure to re-enable antivirus after installation. 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 Forcepoint components on a machine whose fully-qualified domain name (FQDN) contains an underscore. The use of an underscore character in an FQDN is inconsistent with Internet Engineering Task Force (IETF) standards.

Note

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

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. The UAC settings can be re-enabled following installation.

Forcepoint Security Manager

In addition to the other general preparation actions described in this section:

- Do not install the Security Manager on a domain controller machine.
- If you want to run Microsoft SQL Server on the Forcepoint management server, use SQL Server Express.

If you are using a remote installation of SQL Server, you can use any of the supported versions (see *System requirements for this version*.

SQL Server Express

The following third-party components are required to install Microsoft SQL Server Express. Although some versions of the Forcepoint Security Installer will install these components automatically if they are not found, it is a best practice to install the components first, before running the Forcepoint Security Installer.

- .NET Framework 4.6
  Because the installer also requires .NET 4.5, both .NET 4.6 are required if you are installing SQL Server Express.
- Windows Installer 4.5
- Windows PowerShell 1.0
  PowerShell is available from Microsoft (www.microsoft.com).

  If you will use SQL Server to store and maintain data for your web protection solutions, log in to the machine as a domain user to run the Forcepoint Security Installer. This ensures that Service Broker, installed as part of SQL Server, can authenticate itself against a domain (required).

Web protection components

In addition to the general preparation actions (above), Forcepoint Web Security and Forcepoint URL Filtering components have the following additional requirements.

Filtering Service Internet access

To download the Master Database and enable policy enforcement, each machine running Filtering Service must be able to access the download server at download.forcepoint.com.

Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that Filtering Service can access.

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 Forcepoint Security Installer adds two inbound rules to the public profile of Windows Firewall. Ports 9443 and 19448 are opened for the Forcepoint Management Infrastructure. These ports must be open to allow browsers to connect to the Security Manager. Also, additional rules may be added to Windows Firewall when installing Forcepoint DLP components.

See *Default ports for on-premises Forcepoint security solutions*, for more port-related information.

Computer Browser Service

To run User Service or DC Agent on a supported Windows server, the Computer Browser Service must be running.

- On most machines, the service is disabled by default.
- If the service is stopped, the installer will attempt to enable and start it. If this fails, the component installs and starts, but users are not identified until you enable and start the Computer Browser service.

Network Agent

If you are installing Network Agent, ensure that the Network Agent machine is positioned to be able to monitor and respond to client Internet requests.

In standalone installations (which do not include Content Gateway or a third-party integration product), if you install Network Agent on a machine that cannot monitor client requests, basic policy enforcement and features such as protocol management and Bandwidth Optimizer cannot work properly.

Important

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

The network interface card (NIC) that you designate for use by Network Agent during installation must support promiscuous mode. Promiscuous mode allows a NIC to listen to IP addresses other than its own. If the NIC supports promiscuous mode, it is set to that mode during installation. Contact your network administrator or the manufacturer of your NIC to see if the card supports promiscuous mode.

On Linux, do **not** choose a NIC without an IP address (stealth mode) for Network Agent communications.

Note

If you install Network Agent on a machine with multiple NICs, after installation you can configure Network Agent to use more than one NIC. See the Network Agent Quick Start for more information.

Network Agent using multiple NICs on Linux

If Network Agent is installed on a Linux machine, using one network interface card (NIC) for blocking and another NIC for monitoring, make sure that either:

- The blocking NIC and monitoring NIC have IP addresses in different network segments (subnets).
- You delete the routing table entry for the monitoring NIC.

If both the blocking and monitoring NIC on a Linux machine are assigned to the same subnet, the Linux operating system may attempt to send the block via the monitoring NIC. If this happens, the requested page or protocol is not blocked, and the user is able to access the site.

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 the firewall is running, 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 Forcepoint security solutions*.

Important

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

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 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). Also, do not add the hostname to the second or third line.

   ```
   <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.

Forcepoint DLP

See below for information about preparing to install Forcepoint DLP components.

Do not install Forcepoint DLP server on a domain controller

Do not install Forcepoint DLP server on a domain controller (DC) machine.

Domain considerations

The servers running Forcepoint DLP can be set as part of a domain or as a separate workgroup. If you have multiple servers or want to perform run commands on file servers in response to discovery, we recommend you make the server or servers part of a domain.

However, strict GPOs may interfere and affect system performance, and even cause the system to halt. Hence, when putting Forcepoint DLP servers into a domain, it is advised to make them part of organizational units that do not enforce strict GPOs.

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

Related reference

System requirements for this version on page 9
Excluding Forcepoint files from antivirus scans on page 370
Default ports for on-premises Forcepoint security solutions on page 361

Obtaining Microsoft SQL Server

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Prior to installing Forcepoint components, Microsoft SQL Server must be installed and running on a machine in your network.

- See *System requirements for this version*, for supported versions of SQL Server.
- Standard and Enterprise versions of Microsoft SQL Server are not included in your Forcepoint subscription, and must be obtained separately. Refer to Microsoft documentation for installation and configuration instructions.

If you do not have SQL Server, in some cases you can use the Forcepoint Security Installer to install SQL Server Express, a free-of-charge, limited performance version of SQL Server. If you choose this option:

- When available, use the Forcepoint Security Installer to install SQL Server Express. Download and install it from Microsoft if not available in the installer.
- Keep in mind that the performance limitations of SQL Server Express make it more appropriate for evaluation environments or small organizations than for larger deployments.

SQL Server Express can be installed either on the Forcepoint management server or on a separate machine. For larger enterprises, run the Forcepoint Security Manager and a Standard or Enterprise edition of SQL Server on separate physical machines.

See Administering Forcepoint Databases for more information about selecting a database platform.

To install SQL Server Express on the Forcepoint management server, select it when prompted during Forcepoint Management Infrastructure installation.

Important

Forcepoint has removed the ability to install SQL Server Express as an option for new deployments of Forcepoint Security Manager. This change was made via a revised version of Forcepoint Security Installer introduced in July 2019, which can be found on the Downloads page.

The change was required to reduce the risk of deploying SQL Server Express without the latest security updates. Forcepoint Security Manager still supports and will work with the latest version of SQL Server Express. You may use SQL Server Express for small deployments, but it must be installed independently.

To install SQL Server Express on any other machine, run the Forcepoint Security Installer in custom installation mode and select SQL Server Express or download the appropriate version of SQL Server Express from Microsoft. See *Installing SQL Server Express (without Forcepoint Infrastructure)*.

Related tasks

Installing SQL Server Express (without Forcepoint Infrastructure) on page 178

Related reference

System requirements for this version on page 9

Installing the reporting database in a custom folder with SQL Server 2012 or later

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, 8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Starting with Microsoft SQL Server 2012, the database engine service must have access permissions for the folder where database files are stored. This affects the:

- Log Database for web protection solutions
- Forcepoint DLP Incident and Configuration Database
- Log Database for email protection solutions

If you want to store your reporting database or databases in any folder other than the SQL Server default folder (C:\Program Files\Microsoft SQL Server), you must:

1) Create the custom folder.

2) Grant the database engine service full permissions to the custom folder.

3) Install your Forcepoint management server and (for web and email protection solutions) Log Server components.

If you do not grant the database engine service the necessary permissions, the installer will not be able to create the reporting database or databases, and some components may fail to install, or be installed incorrectly.

To grant the proper permissions to the database engine service:

1) In Windows Explorer, right-click the custom folder that you created to hold the reporting database or databases and select **Properties**.

2) On the Security tab, click **Edit**, then **Add**.

3) Make sure the hostname of the SQL Server machine appears in the “From this location” field of the Select Users... dialog box.
If the correct host is not selected, click **Locations**, then select SQL Server host machine and click **OK**.

4) In the Enter the object names... text box, enter the SID of the SQL Server service:
   a) The default instance SID is `NT SERVICE\MSSQLSERVER`.
   b) Use the format `NT SERVICE\MSSQL$InstanceName` for a named instance.

5) Click **Check Names** to validate the SID. If the validation fails:
   a) Click **OK** in the pop-up box to open the Multiple Names Found dialog box.
   b) Select the correct SID, then click **OK**.
   c) Click **OK** again to return to the Permissions dialog box.

6) In the Group or user names list, select the SID you just added, then mark the **Allow** check box under Full control in the Permissions list.

7) Click **Apply**, and then click **OK** twice to exit.

Chapter 2

Deployment Planning for Forcepoint Solutions

Contents

The deployment overview provides a high-level deployment diagram and component summary to help contextualize the detailed, module-specific information provided in the deployment planning articles and guides.

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Note

- Forcepoint DLP v9.0 and later is supported with Forcepoint Web and Email Security v8.5.5.
- Forcepoint DLP v8.7.1 and later is supported with Forcepoint Web and Email Security v8.5.4.
- Forcepoint DLP v8.6 and v8.7 are supported with Forcepoint Web and Email Security v8.5.3.
- Forcepoint DLP v8.5.1 is supported with Forcepoint Web and Email Security v8.5.0.
- Forcepoint DLP v8.5.0 and v8.5.2 are stand-alone versions of that product and cannot be integrated with other Forcepoint products.

If you have a combination of Forcepoint security solutions, use the articles below to plan your deployment:

Forcepoint Web Security and Forcepoint URL Filtering

Deploying Web Protection Solutions

Forcepoint DLP

Planning Forcepoint DLP Deployment

Forcepoint Email Security

Deploying Email Protection Solutions

All On-Premises and Hybrid Forcepoint Security Solutions

Forcepoint security solutions deployment overview

Related concepts

Deploying Web Protection Solutions on page 33
Planning Forcepoint DLP Deployment on page 103
Deploying Email Protection Solutions on page 105
Forcepoint security solutions deployment overview on page 28

Forcepoint security solutions deployment overview

Applies to:

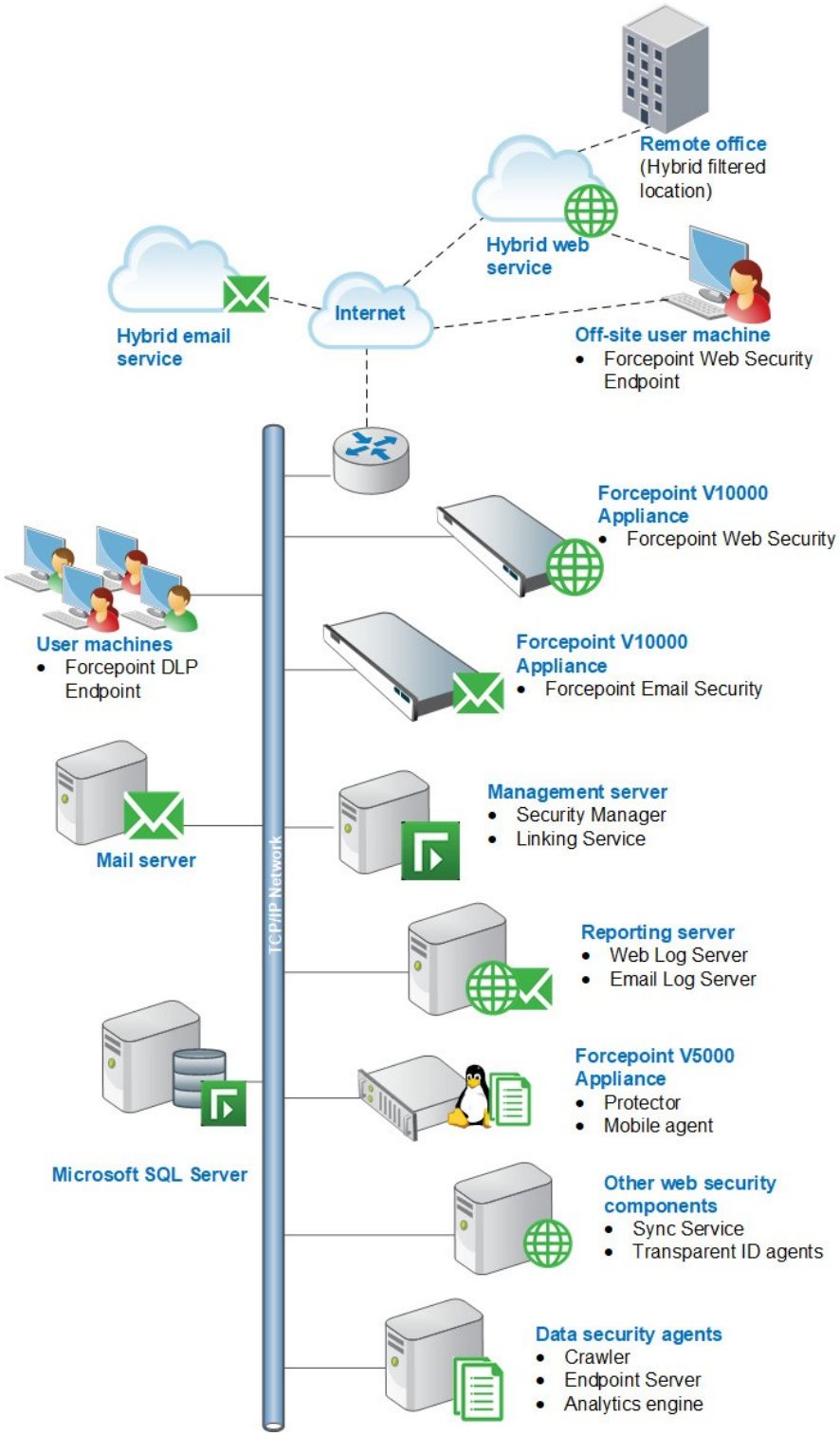
- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Forcepoint Web Security, Forcepoint Email Security, and Forcepoint DLP may be deployed together to create a comprehensive security solution.

- The Forcepoint Security Manager, the management interface for web, data, and email advanced protection solutions, resides on a Windows server.
- Forcepoint Web Security may be deployed on Forcepoint appliances, dedicated Windows or Linux servers, or a combination of platforms.
- Forcepoint DLP runs on Windows servers, optional appliances, and elsewhere in the network. Some components run in cloud infrastructures such as Microsoft Azure.
- Forcepoint Email Security enforcement components reside on Forcepoint appliances or in Microsoft Azure. Management and reporting components reside on Windows servers. Starting in version 8.5.3, management and reporting components may be deployed in Microsoft Azure.

High-level deployment diagram

The diagram shows an appliance-based deployment:



Remote office and off-site users

You can use the Forcepoint Web Security Hybrid Module to provide web security for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location. See the Forcepoint Web Security Administrator Help for details.

The hybrid service can also provide web security for off-site users (that is, users working from home, traveling, and so on).

User requests can be directed to the hybrid service using a PAC file or endpoint client software. This allows the hybrid service to analyze web requests and enforce policies.

Hybrid services

If your subscription includes the Forcepoint Web Security and Forcepoint Email Security 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 scanning, stopping spam, virus, phishing, and other malware attacks before they reach your network and possibly reducing email bandwidth and storage requirements.

The hybrid service can also be configured to encrypt outbound email before delivery to its recipient.

Forcepoint Web Security and Forcepoint Email Security appliances

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

- The Content Gateway proxy on the appliance manages web traffic. Both Forcepoint Web Security and Forcepoint DLP Network include Content Gateway.
- 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.

Forcepoint Email Security and Forcepoint Web Security cannot be deployed on the same appliance.

Forcepoint DLP appliance

The Forcepoint DLP 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.

Components that may not be installed on Forcepoint appliances

Forcepoint management server:

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

Core Forcepoint DLP components also reside on the management server machine to enable key features, including web and email DLP.

Linking Service, which connects Forcepoint DLP and Forcepoint Web Security, also usually resides on the management server.

Web and Email Log Server

A separate Windows machine hosts two instances of Log Server: one for Forcepoint Web Security and one for Forcepoint Email Security. These services receive information about web and email traffic and process it into their respective Log Database.

Optional web protection components

Sync Service and transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent) may not reside on Forcepoint appliances.

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

Forcepoint DLP agents

The crawler, analytics engine, and the endpoint server for Forcepoint DLP Endpoint are installed on appropriate machines.

See *Installing Forcepoint DLP* for details.

Forcepoint DLP Endpoint (User Machine)

Forcepoint DLP Endpoint can be installed on supported Windows, Mac, and Linux machines.

Third-party components

Microsoft SQL Server:

Microsoft SQL Server, running on a Windows server in your network, is used to store logging, reporting, and in some cases, configuration data for Forcepoint security solutions. Quarantined email messages are also stored here.

When Forcepoint security solutions are installed, SQL Server must be installed and running, typically on its own. SQL Server Express (installed using the Forcepoint Security Installer, in certain cases) may be used in small deployments or evaluation environments.

Related concepts

Installing Forcepoint DLP on page 147

Chapter 3

Deploying Web Protection Solutions

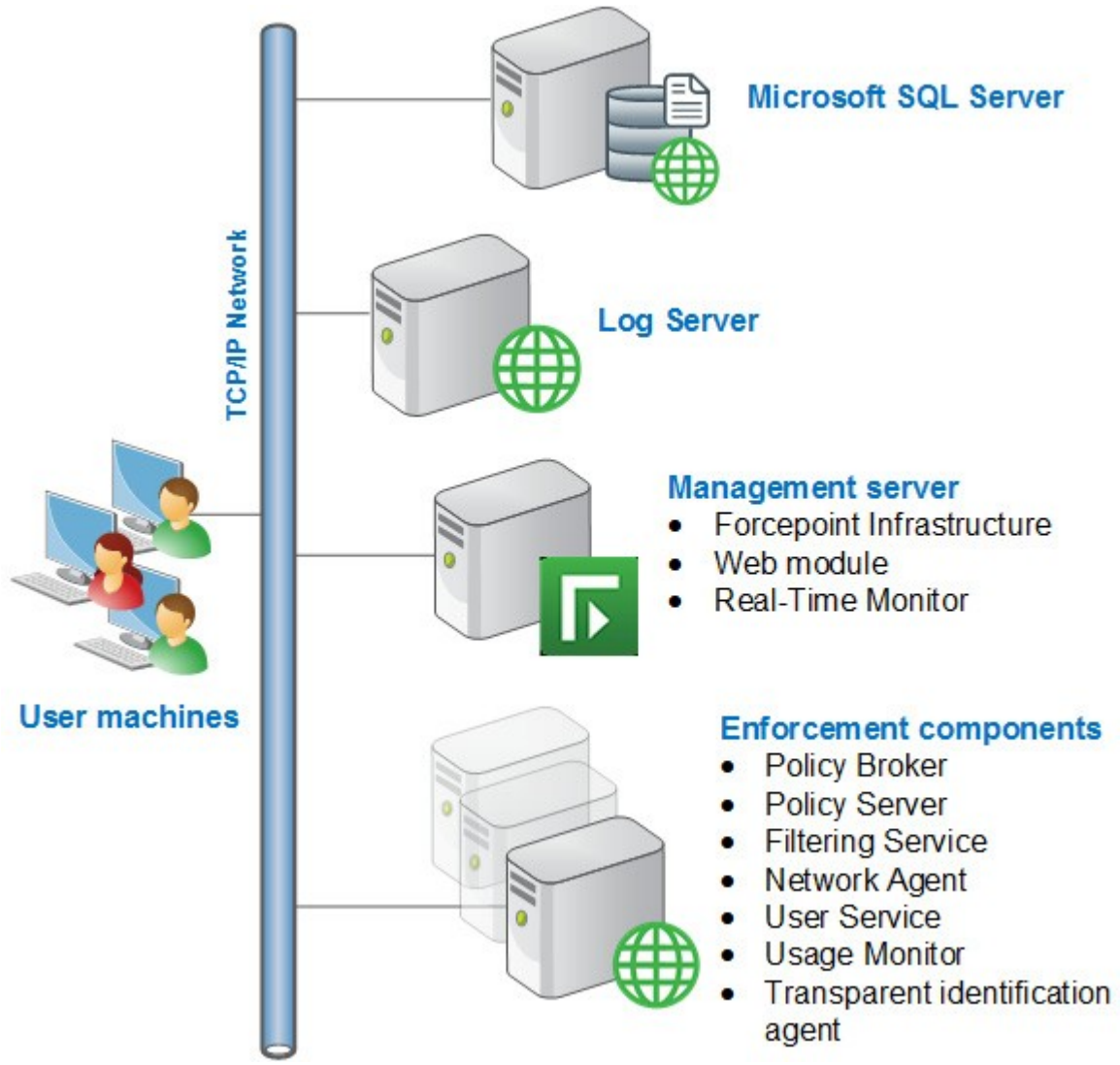
Contents

High-level deployment diagrams

Applies to	In this topic
Forcepoint Web Security, v8.5.x	Forcepoint URL Filtering deployment diagram
Forcepoint URL Filtering, v8.5.x	Forcepoint Web Security deployment diagram

Forcepoint URL Filtering deployment diagram

The illustration below shows components distributed across multiple servers in a typical deployment.



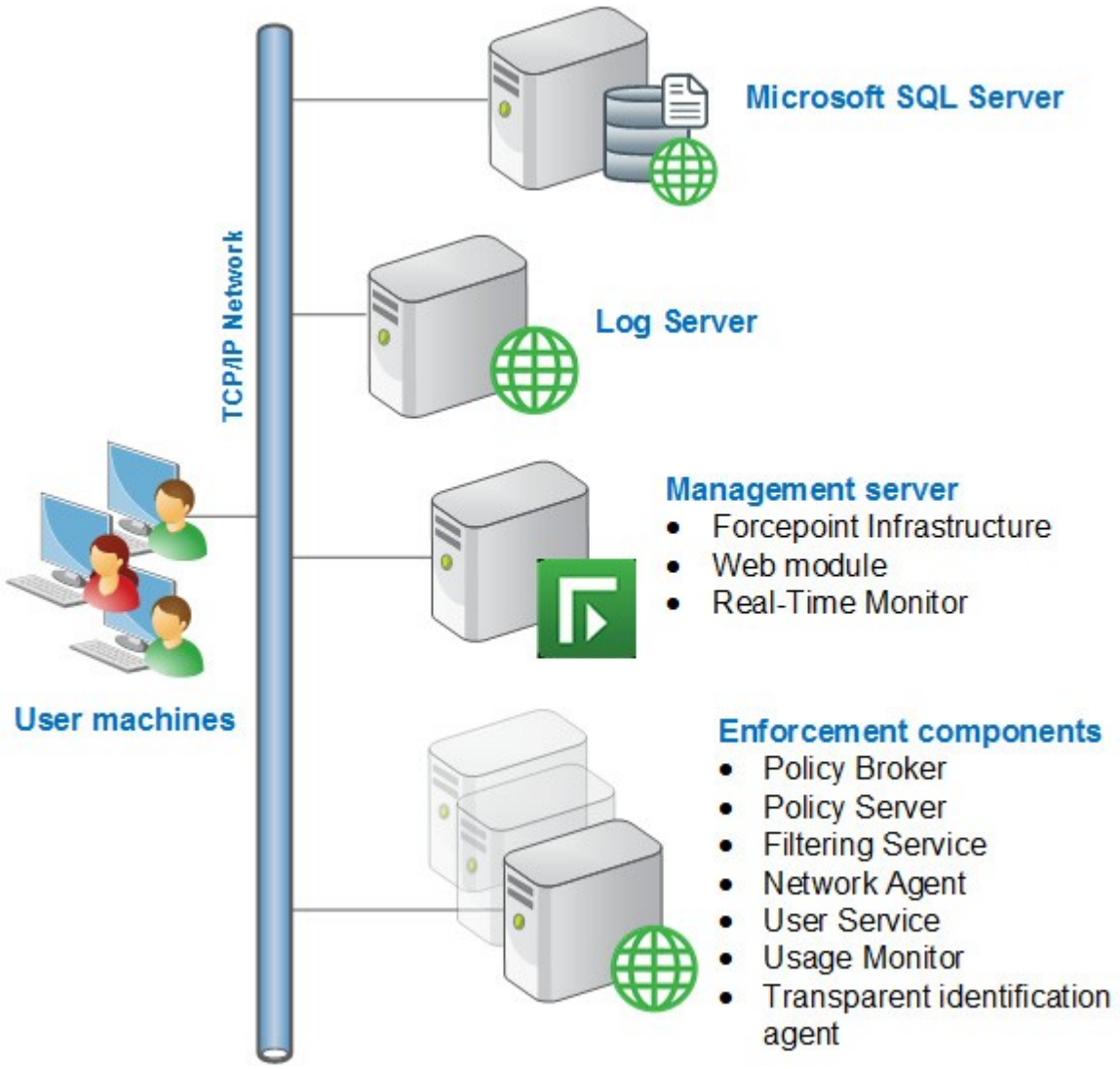
All of the enforcement components, except for the optional transparent identification agents, may reside on a Windows or Linux server, or a Forcepoint appliance.

For evaluation or very small (low traffic) deployments, all components, plus an instance of SQL Server Express (installed by the Forcepoint Security Installer, in certain cases) may reside on a single Windows server.

For more information about the core components that make up a deployment, see *Deploying core web protection components*

Forcepoint Web Security deployment diagram

This illustration shows a basic software-based deployment. Note that the illustration is intended to show the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).



Content Gateway and other enforcement components, except for the optional transparent identification agents, may also reside on a Forcepoint appliance.

For more information about the core components that make up a deployment, see:

- *Deploying core web protection components*
- *Content Gateway Deployment*

If you have purchased the Web Security Hybrid module, also see:

- *Deploying Forcepoint Web Security Hybrid Module components*

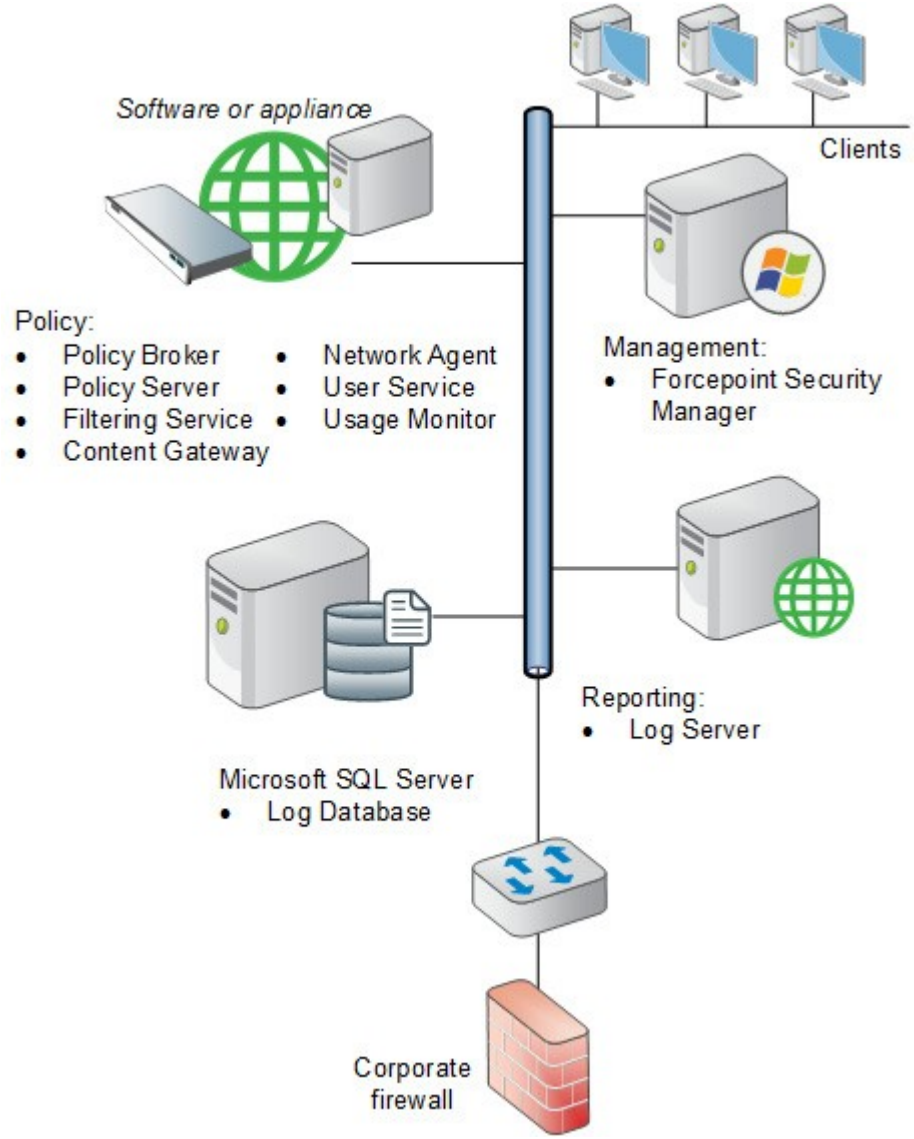
Related concepts

Content Gateway Deployment on page 83

Deploying core web protection components

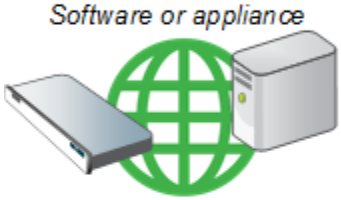
Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ Core policy components ■ Core management components ■ Core reporting components

On-premises web protection solutions include the core policy, management, and reporting components shown in the diagram below and described in detail in the sections that follow, with one exception: Content Gateway is available only for Forcepoint Web Security.



Core policy components

Software or appliance



Core policy components:

- Policy Broker
- Policy Server
- Filtering Service
- Content Gateway
- Network Agent
- User Service
- Usage Monitor

Policy Broker:

- Manages requests from other components for policy and configuration data
- Can be deployed standalone (one per deployment) or replicated (one primary with one or more replicas)
- Sole instance (standalone) or primary (replicated) installed before other components
- On "full policy source" appliance (standalone only)

Policy Server:

- Identifies other components and tracks their location and status
- Multiple instances can be deployed
- Installed after Policy Broker and before other components
- On "full policy source" and "user identification and filtering" appliances

Filtering Service:

- Works with other components to manage Internet activity and forwards log data for use in reporting
- Up to 10 per Policy Server
- On all web protection appliances

Content Gateway:

- Proxies HTTP, HTTPS, and FTP requests
- Analyzes requests and responses in real time to detect potential threats
- Up to one per Filtering Service
- On all Forcepoint Web Security appliances

To ensure effective policy enforcement, the core components must be installed so that:

- All components can communicate with an instance of Policy Broker.
  - In Policy Broker standalone mode (software or appliance), there is only one Policy Broker instance for the entire deployment.
  - In Policy Broker replicated mode (software only), there is one primary Policy Broker (to which configuration updates are written) and one or more Policy Broker replicas (with a read-only copy of the configuration data).
  - In software installations, Policy Broker can run on Windows or Linux.
  - With Forcepoint appliances, the standalone Policy Broker is present on the **full policy source** appliance only.

  - Most components must be able to communicate with Policy Broker on port **55880**. (The exceptions are all optional components: transparent identification agents, State Server, Linking Service, and Directory Agent.)
- There is a central instance of Policy Server.
  - In software installations, the central Policy Server instance runs on the standalone or primary Policy Broker machine.
  - With Forcepoint appliances, Policy Server is present on the **full policy source** appliance.
  - Additional instances of Policy Server can be deployed on Windows or Linux machines, or on **user identification and filtering** appliances.
  - Most components must be able to communicate with Policy Server on ports **55806** and **40000**. (The exceptions are Remote Filtering Server and State Server.)
- At least one instance of Filtering Service communicates with the central Policy Server.
  - In software installations, Filtering Service can run on the same machine as Policy Broker and Policy Server, or on a separate machine.
  - With Forcepoint appliances, a Filtering Service instance is present on the **full policy source** appliance.
  - Additional instances of Filtering Service can be deployed on Windows or Linux machines, or on either **user identification and filtering** (includes Policy Server) or **filtering only** (must point to a remote Policy Server) appliances.
- Filtering Service is configured to receive requests from one of the following (see *Understanding standalone and integrated modes for web protection solutions*.
  - Content Gateway (Forcepoint Web Security)
    For detailed information about deploying Content Gateway, see *Content Gateway Deployment*.
  - Network Agent (Forcepoint URL Filtering standalone deployments)
  - An integrated third-party firewall, proxy server, or caching application (Forcepoint URL Filtering integrated deployments)

Core management components

Core management components:
- Forcepoint Security Manager
- Web module

Forcepoint Security Manager
- Unified management console for web, data, and email protection solutions
- One per deployment
- Includes a database to store configuration information that applies to all modules

Web module:
- Used to configure your web protection solution, manage policies, and run reports
- One per deployment

Other management server components:
- Real-Time Monitor displays Internet activity details as it occurs.
- Linking Service gives Forcepoint DLP access to user and category information provided by web protection components.

The Forcepoint Security Manager is the centralized management console. It includes global administrator settings and appliance connection data, as well as 3 management modules: Web, Data, and Email.

The Web Security module of the Forcepoint Security Manager is used to perform product configuration, policy management, and reporting tasks for on-premises web protection solutions.

- Install all Forcepoint Security Manager components on a single Windows server (the management server).
- The Web Security module of the Forcepoint Security Manager must be able to communicate with:
  - Policy Broker on port 55880
  - Policy Server on ports 40000, 55806, 55817, 55818, and 55824
  - Filtering Service on port 55807
  - Log Server on ports 55812 and 55805
  - User Service on port 55815

Core reporting components

Reporting:
- Log Server

Microsoft SQL Server
- Log Database

Log Server
- Receives log data and stores it in the Log Database
- Enables investigative, presentation, and application reports, and Dashboard charts
- Maximum one per Policy Server
- Multiple Log Server instances can send data to a central Log Server, which sends the data to the Log Database, or each can be configured to send data to the same Log Database

Log Database
- Requires a supported Microsoft SQL Server installation
- Stores Internet activity log data for use in reports
- One per deployment

Log Server receives information about Internet activity from and processes it into the Log Database.

- Install Log Server on a dedicated Windows server.
  - Log Server does not run on appliances.
  - Because collecting and processing log records is resource-intensive, Log Server should typically not run on the same machine other resource-sensitive components, like the Forcepoint Security Manager or Filtering Service.
  - You may have one Log Server instance for the entire deployment, or multiple Log Server instances (see *Additional reporting considerations*), but you can never have more than one Log Server per Policy Server.
- The Log Database resides on a supported Microsoft SQL Server machine.
  - Do not run Log Server on the SQL Server machine.
  - By default, Log Server communicates with SQL Server on the default ODBC port (1433). A custom port can be specified during installation. See *Using a custom port to connect to the Log Database*.
- The management server machine must be able to communicate with Log Server and the Log Database.

Related concepts

Content Gateway Deployment on page 83
Understanding standalone and integrated modes for web protection solutions on page 42

Related reference

Additional reporting considerations on page 48

Deploying Forcepoint Web Security Hybrid Module components

Applies to:

- Forcepoint Web Security, v8.5.x

The Hybrid Module for Forcepoint Web Security offers the ability to combine on- premises and hybrid (cloud or security-as-a-service) policy enforcement.

Two on-premises components are used to enable communication with the hybrid service in the cloud:

- *Sync Service*
- *Directory Agent*

Sync Service

Sync Service is required to send policy updates and user and group information from the on-premises deployment to the hybrid service (in the cloud). Sync Service also retrieves reporting data from the hybrid service and passes it to Log Server so that it can be used in reports.

- There can be only one Sync Service instance in your deployment.
- Sync Service can be installed on the Log Server machine.
- If you use a distributed logging deployment, Sync Service may communicate with either the central Log Server or a remote Log Server.
- If you have enabled Policy Broker replication, Sync Service must connect to the primary Policy Broker.

Sync Service must be able to communicate with:

- The hybrid service on port 443
- Log Server on port 55885 (outbound)
- Directory Agent on port 55832 (inbound)
- Forcepoint Security Manager on port 55832 (inbound)
- Policy Broker on port 55880 (outbound)
- Policy Server on port 55830 (inbound) and ports 55806 and 40000 (outbound)

Directory Agent

Directory Agent is required to enable user, group, and domain (OU) based policy enforcement through the hybrid service.

Directory Agent collects user, group, and OU information from a supported directory service and passes it to Sync Service in LDIF format. Sync Service then forwards the information to the hybrid service.

- Typically, only one Directory Agent instance is required in a deployment. Deployments with multiple Policy Servers, however, would require multiple Directory Agent instances.
- Directory Agent can be installed on the same machine as other web protection components, including Sync Service and User Service.
- With Forcepoint appliances, Directory Agent is installed on the **full policy source** or **user directory and filtering** appliance.
- When Directory Agent is installed, it must connect to a Policy Server instance that has an associated **User Service** instance.
  - Directory Agent must communicate with the same directory service as User Service.
  - If you have multiple User Service instances connected to different directory services, you can also have multiple Directory Agent instances, each associated with a different Policy Server.

- All Directory Agent instances must connect to a single Sync Service. (A deployment can have only one Sync Service instance.)
  Use the Web Security module of the Forcepoint Security Manager to configure the Sync Service connection manually for all supplemental Directory Agent instances.

  See Directory Agent and User Service in the Administrator Help for configuration steps.

Directory Agent must be able to communicate with:

- Your supported LDAP-based directory service (Windows Active Directory in Native Mode, Oracle Directory Server, or Novell eDirectory)
  If your organization uses Windows Active Directory in mixed mode, user and group data cannot be collected and sent to the hybrid service.
- Sync Service on port 55832
- Policy Server on ports 55806 and 40000

Once configured, Directory Agent collects user and group data from your directory service and sends it to Sync Service in LDIF format. At scheduled intervals, Sync Service sends the user and group information collected by Directory Agent to the hybrid service. Sync Service compresses large files before sending them.

Understanding standalone and integrated modes for web protection solutions

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Forcepoint URL Filtering may either be installed as a **standalone** solution, or be **integrated** with a third-party proxy, cache, or firewall product (for example, Cisco ASA or Microsoft Forefront TMG).

- In a standalone deployment, **Network Agent** monitors Internet activity from all users and forwards both HTTP(S) requests and requests made via other protocols to Filtering Service to determine whether to permit or block the request. See:
  - *Hardware recommendations for standalone Forcepoint URL Filtering deployments*
  - *Deployment guidelines for Network Agent*
- In an integrated deployment, the **third-party product** (integration product) forwards HTTP(S) requests, and sometimes also FTP requests, to Filtering Service to determine whether to permit or block the request.
  For information about integrating Forcepoint URL Filtering with a third-party product, see:
  - *Integrating Forcepoint URL Filtering with Cisco*
  - *Integrating Forcepoint URL Filtering with Citrix*
  - *Integrating Forcepoint URL Filtering using ICAP Service*
  - *Integrating Forcepoint URL Filtering with TMG*
  - *Installing for Universal Integrations*

Forcepoint Web Security includes **Content Gateway**, a high-performance web proxy that provides real-time threat analysis and website classification. In Forcepoint Web Security deployments, Content Gateway forwards HTTP(S) and FTP requests to Filtering Service to determine whether to permit or block the request. See *Content Gateway Deployment*.

Related concepts

Content Gateway Deployment on page 83
Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering using ICAP Service on page 241
Integrating Forcepoint URL Filtering with TMG on page 221
Installing for Universal Integrations on page 247

Related reference

Hardware recommendations for standalone Forcepoint URL Filtering deployments on page 43
Deployment guidelines for Network Agent on page 56

Hardware recommendations for standalone Forcepoint URL Filtering deployments

Applies to:

- Forcepoint URL Filtering, v8.5.x

In standalone deployments, Network Agent (rather than Content Gateway or a third- party integration product) monitors network traffic and enables management of all protocols, including HTTP, HTTPS, and FTP. Network Agent also:

- Detects all TCP/IP Internet requests (HTTP and non-HTTP)
- Communicates with Filtering Service to see if each request should be blocked
- Calculates the number of bytes transferred
- Sends a request to Filtering Service to log Internet activity

The table below provides hardware recommendations for standalone deployments, based on network size. System needs vary depending on the volume of Internet traffic. The table does not include information for the management server (see *System requirements for this version*).

The following baseline is used to create the recommendations:

- 1 - 500 users = 1 - 100 requests per second (rps)
- 500 - 2,500 users = 100 - 500 rps
- 2,500 - 10,000 users = 500 - 2,250 rps

Important

- Do not install web protection components on a firewall machine. Firewall and web protection software function and performance may be affected.
- Each Network Agent machine must be positioned to see all Internet requests for the machines that it is assigned to monitor.

If your network traffic exceeds these estimates, more powerful systems or greater distribution of components may be required.

Network Size	Enforcement Components	Reporting (Windows)
1 - 500 users	**Windows** or **Linux** ■ Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater ■ 4 GB RAM ■ 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** ■ Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater ■ 4 GB RAM ■ 100 GB free disk space ■ Microsoft SQL Server required for Log Database See this article for supported versions.
500 - 2,500 users	**Windows** or **Linux** ■ Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater ■ 4 GB RAM ■ 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** ■ Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater ■ 4 GB RAM ■ 100 GB free disk space ■ Microsoft SQL Server required for Log Database See this article for supported versions.
2,500 - 10,000 users	**Windows** or **Linux** ■ Load balancing required ■ Quad-Core Intel Xeon 5450 or better processor, 3.0 GHz or greater ■ 4 GB RAM ■ 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** ■ Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater ■ 4 GB RAM ■ 200 GB free disk space with a disk array (The Log Database requires a disk array to increase I/O reliability and performance.) ■ High-speed disk access ■ Microsoft SQL Server required for Log Database See this article for supported versions.

To run both policy enforcement and reporting components on the same machine in the two smaller network sizes, increase the RAM to 6 GB (if supported by your operating system), and consider using a faster processor and hard drive to compensate for the increased load.

For networks with 2,500-10,000 users, at least two Network Agent instances, running on separate machines, are required. The machines should have:

- Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater
- At least 1 GB of RAM

Multiple Filtering Service machines may also be needed. Machine requirements depend on the number of users whose requests are monitored and managed. See *Extending your deployment with additional web protection components*.

Related reference

System requirements for this version on page 9
Extending your deployment with additional web protection components on page 45

Extending your deployment with additional web protection components

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *Filtering Services per Policy Server* ■ *Network Agents per Filtering Service* ■ *Policy Server, Filtering Service, and State Server* ■ *Policy Server, Filtering Service, and SIEM integration*

In large, high-traffic, or geographically distributed organizations, you can deploy multiple groups of policy components, each with its own **Policy Server** instance, to:

- Provide load-balancing capabilities.
- Improve responsiveness in locations far away from the central deployment.
- Manage high amounts of traffic.

When Policy Broker is installed in standalone mode, all Policy Server instances connect to the same, central Policy Broker. When Policy Broker is installed in replicated mode, you can configure how each Policy Server determines which Policy Broker instance to use.

Each Policy Server instance can support:

- Up to 10 Filtering Service instances (see *Filtering Services per Policy Server*)
  - Each Filtering Service can support up to 4 Network Agent instances (see *Network Agents per Filtering Service*
- 1 User Service
- 1 Usage Monitor
- 1 Log Server
- 1 State Server (see *Policy Server, Filtering Service, and State Server*
- 1 Directory Agent (Web Hybrid module only; see *Directory Agent*)

For high-level diagrams of larger deployments, see *Web protection distributed deployments*.

Filtering Services per Policy Server

As a best practice, deploy no more than 10 Filtering Service instances per Policy Server. A Policy Server instance may be able to handle more, depending on the load. If the number of Filtering Service instances exceeds the Policy Server's capacity, however, responses to Internet requests may be slowed.

Multiple Filtering Service instances are useful to manage remote or isolated sub- networks.

The appropriate number of Filtering Service instances for a Policy Server depends on:

- The number of users per Filtering Service
- The configuration of the Policy Server and Filtering Service machines
- The volume of Internet requests
- The quality of the network connection between the components

If a ping command sent from one machine to another receives a response in fewer than **30 milliseconds (ms)**, the connection is considered high-quality. See *Testing the Policy Server to Filtering Service connection*.

If Filtering Service and Policy Server become disconnected, all Internet requests are either blocked or permitted, as configured in the Web Security module of the Forcepoint Security Manager. See Configuring your account information for details.

Filtering Service machines running behind firewalls or running remotely (at a great topological distance, communicating through a series of routers) may need their own Policy Server instance.

Testing the Policy Server to Filtering Service connection

Run a `ping` test to check the response time and connection between the Policy Server and Filtering Service machines. A response time of fewer than 30 milliseconds is recommended.

1) Open a command prompt (Windows) or terminal session (Linux) on the Policy Server machine.

2) Enter the following command:

```
ping <IP address or hostname>
```

Use the IP address or hostname of the Filtering Service machine.

On Windows machines, the results resemble the following:

```
C:\>ping 11.22.33.254
Pinging 11.22.33.254 with 32 bytes of data:

Reply from 11.22.33.254: bytes=32 time=14ms TTL=63
Reply from 11.22.33.254: bytes=32 time=15ms TTL=63
Reply from 11.22.33.254: bytes=32 time=14ms TTL=63
Reply from 11.22.33.254: bytes=32 time=15ms TTL=63

Ping statistics for 11.22.33.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

In a Linux environment, the results look like this:

```
[root@localhost root]# ping 11.22.33.254
PING 11.22.33.254 (11.22.33.254) 56(84) bytes of data.

64 bytes from 11.22.33.254: icmp_seq=2 ttl=127 time=0.417 ms
64 bytes from 11.22.33.254: icmp_seq=3 ttl=127 time=0.465 ms
64 bytes from 11.22.33.254: icmp_seq=4 ttl=127 time=0.447 ms
64 bytes from 11.22.33.254: icmp_seq=1 ttl=127 time=0.854 ms
```

Ensure that **Maximum** round trip time or the value of **time=x.xxx ms** is fewer than 30 ms. If the time is greater than 30 ms, move one of the components to a different network location and run the ping test again. If the result is still greater than 30 ms, locate and eliminate the source of the slow response.

Network Agents per Filtering Service

As a best practice, deploy no more than 4 Network Agent instances per Filtering Service. One Filtering Service instance may be able to handle more than 4 Network Agents, depending on the number of Internet requests, but if Filtering Service or Network Agent capacities are exceeded, policy enforcement and logging inconsistencies may occur.

Network Agent can typically monitor 50 Mbps of traffic per second, or about 800 requests per second. The number of users that Network Agent can monitor depends on the volume of Internet requests from each user, the configuration of the network, and the location of Network Agent in relation to the computers it is assigned to monitor. Network Agent functions best when it is close to those computers.

Network Agent communicates with Filtering Service on port 15868.

Policy Server, Filtering Service, and State Server

If your deployment includes multiple instances of Filtering Service that might handle a request from the same user, an optional component, **State Server**, can be installed to enable proper application of time-based policy actions. (Quota time, for example, is a time-based action that can be used to give users access to websites in selected categories for a configurable time period.)

When State Server is installed, all of its associated Filtering Service instances share timing information, so users receive the correct allotment of access to time-restricted categories.

- State Server is typically installed on a Policy Server machine, and only one State Server instance is required per **logical deployment**.
  A logical deployment is any group of Policy Server and Filtering Service instances that might handle requests from the same set of users.
- State Server can be enabled via the command-line interface on **full policy source** or **user identification and filtering** appliances.
- All Filtering Service instances that communicate with the same State Server instance must share the same time zone, and the time on all machines must be in sync.
- State Server communicates with Filtering Service on port 55828.
- Each Filtering Service instance can communicate with only one State Server.
- All Filtering Service instances associated with the same Policy Server must communicate with the same State Server.
- Multiple Policy Server instances can share a single State Server.

In a geographically dispersed organization, where each location has its own Policy Server and Filtering Service instances, deploy one State Server instance (on the Policy Server machine or appliance) at each location.

In an organization where all requests are managed through a central location, only one State Server instance is needed.

Policy Server, Filtering Service, and SIEM integration

Web protection solutions can be configured to pass logging data (the same information processed by Log Server) and, with v8.5.4, audit log data to a third-party Security and Information and Event Management (SIEM) product.

When SIEM integration is enabled, Multiplexer collects log data from Filtering Service and passes it to both Log Server and the Bridge Service. Bridge Service then forwards it to the Event Message Brokers which allows SIEM Connectors to then send it to the integrated SIEM product.

Multiplexer is always installed on the Policy Server machine, and communicates with the following components:

- Policy Server on ports 40000 and 55806
- Filtering Service on port 55833 (inbound)
- Log Server on port 55805 (outbound)
- Bridge Service on port 55999 (outbound)

Related concepts

Web protection distributed deployments on page 67

Additional reporting considerations

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *Using a custom port to connect to the Log Database* ■ *Using SSL to connect to the Log Database* ■ *Configuring distributed logging*

When you install web protection reporting components, you can configure how those components communicate with the Microsoft SQL Server database (Log Database). Port and encryption settings selected during installation can be changed after installation, if needed.

In addition, if you are planning to deploy reporting components for a large or geographically distributed organization, and need to use a single, centralized database for reporting, see *Configuring distributed logging*, for configuration options.

Using a custom port to connect to the Log Database

During Forcepoint Management Infrastructure and Log Server installation, you can specify which port to use for Microsoft SQL Server communication. By default, the standard ODBC port (1433) is used.

If you want to use another port, keep in mind that SQL Server typically assigns:

- A fixed port to the default instance (MSSQLSERVER)
- A dynamic port to each named instance

Use the SQL Server Configuration Manager to configure the port used by each SQL Server instance. See your Microsoft documentation for assistance.

Using SSL to connect to the Log Database

During Forcepoint Management Infrastructure and Log Server installation, you are given the option to connect to Microsoft SQL Server using an SSL-encrypted connection.

In determining whether to configure reporting and management components to use SSL encryption for Log Database communication, keep in mind that:

- BCP (bulk copy program) cannot be used to add records to the Log Database.
- Log Database connections are slower, which may affect reporting performance.

Before enabling SSL encryption during web protection software installation, configure Microsoft SQL Server encryption settings.

1) Launch SQL Server Configuration Manager.

2) Right-click the **SQL Native Client x.x Configuration** entry used in your SQL Server installation, then select **Properties**
   Two parameters are listed:
   - **Force Protocol Encryption**: The default setting (No) means that encrypted connections are accepted but not required. This setting is typically best for use with Forcepoint security solutions.
     If this is set to yes, only encrypted connections are accepted.
   - **Trust Server Certificate**: The default setting (No) means that only certificates issued by a Certificate Authority (CA) are accepted for encrypting connections to the database. This requires that a CA-signed certificate be deployed to the SQL Server, Log Server, and management server machines a secure connection can be used to connect to the database.

When this parameter is set to **Yes**, self-signed SSL certificates may be used to encrypt the connection to the database. In this case, the certificate is generated by the SQL Server machine and shared by all components needing to connect to the database.

If you enable SSL encryption during installation, Force Protocol Encryption is set to **Yes**, and Trust Server Certificate is set to **No**, CA-signed certificates must be installed on the management server and Log Server machines before the component installation will succeed.

Configuring distributed logging

If you have a large or distributed environment that requires multiple Log Server instances, you can configure each Log Server to record data to a separate Log Database. If you do not need a central repository of reporting data that can be used to generate organization-wide reports, this may be the most efficient deployment option.

If, however, you need a single Log Database in order to store all reporting data in a central location, you have 2 options:

- Configure all Log Server instances to independently record their data in the same Log Database.
- Configure distributed Log Server instances to pass their data to a central Log Server, which then records all log records from all instances into the Log Database.

The first option does not require special configuration steps. You need only ensure that each Log Server instance points to the same database (both database engine IP address or hostname and database instance name).

The second option requires more planning and configuration detail, as outlined in the sections that follow.

Note that centralized log processing is not as fast as local logging. Expect a delay of 4 or 5 minutes before the files from remote Log Servers appear in the cache processing directory on the central Log Server.

Part 1: Prepare for centralized logging

Required external resources for web protection solutions

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Forcepoint web protection software relies on the following external resources and network characteristics to function properly in your network.

- **TCP/IP**
  Policy enforcement is available for TCP/IP-based networks only.
- **DNS server**
  A DNS server is used to resolve requested URLs to an IP address. Content Gateway, Network Agent, or your third-party integration product requires efficient DNS performance. DNS servers should be fast enough to support policy enforcement without becoming overloaded.
- **Directory services**
  If web protection software is configured to apply user- and group-based policies, User Service queries the directory service for user information. Although these users and group relationships are cached, directory service machines must have the resources to respond rapidly if web protection components request user information. See *System requirements for this version*, for supported directory services.

For information on configuring web protection software to communicate with a supported directory service, see the Administrator Help. Web protection components do not need to run on the same operating system as the directory service.

- **Network efficiency**
  The ability to connect to resources such as the DNS server and directory services is critical. Minimize network latency for efficient Filtering Service performance. Excessive delays under high load circumstances can impact Filtering Service and may cause lapses in policy enforcement.
- **Microsoft SQL Server**
  A supported version of Microsoft SQL Server is required to host the Log Database, which stores reporting data. See *System requirements for this version* for supported SQL Server versions.
  - SQL Server Standard or Enterprise works best for larger networks, or networks with a high volume of Internet activity, because of its capacity for storing large amounts of data over longer periods of time (several weeks or months).
  - SQL Server Express, a free, limited-performance database engine bundled into the Forcepoint Security Installer in certain versions, is best-suited to evaluation or proof of concept deployments. It can also be used by organizations with a low volume of Internet activity, or organizations planning to generate reports on only short periods of time (for example, daily or weekly archived reports, rather than historical reports over longer time periods).

Related reference
System requirements for this version on page 9

Maximizing system performance for web protection solutions

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *Network Agent* ■ *HTTP request logging* ■ *Microsoft SQL Server (Log Database)* ■ *Log Database sizing considerations*

Adjust web protection components to improve policy enforcement and logging response time, system throughput, and CPU performance.

Network Agent

As the number of users grows, or if Network Agent does not block Internet requests as expected, place Network Agent on a different machine from Filtering Service and Policy Server. You can also deploy additional Network Agent instances and divide network monitoring between them.

In a high-load environment, or an environment with a high-capacity Internet connection, you can increase throughput and implement load balancing by installing multiple Network Agent instances. Install each agent on a different machine, and configure each agent to monitor a different portion of the network.

- Network Agent must have bidirectional visibility into the network segment it monitors.
- If multiple Network Agents are installed, each agent must monitor a different network segment (IP address range).

- If a Network Agent machine connects to a switch, the monitor NIC must plug into a port that mirrors, monitors, or spans the traffic of all other ports.

HTTP request logging

You can use Content Gateway, Network Agent, or a third-party integration product to track HTTP requests and pass the information to Filtering Service, which uses the data to manage and log requests.

Content Gateway, Network Agent and some integration products also track bandwidth activity (bytes sent and received), and the duration of each permitted Internet request. This data is also logged.

When Network Agent is deployed with Content Gateway or an integration product, and both components provide logging data, the amount of processor time required by Filtering Service increases.

If you are using Network Agent with Content Gateway or an integration product, you can avoid extra processing by specifying whether Network Agent or another component logs HTTP requests. Consult the Administrator Help for configuration instructions.

Microsoft SQL Server (Log Database)

Under high load, Microsoft SQL Server operations are resource intensive, and can be a performance bottleneck for reporting tools. For best results:

- Do not install Log Server on the database engine machine.
- Provide adequate disk space to accommodate the growth of the Log Database. You can monitor growth and sizing information on the **Web** > **Settings** > **Reporting** > **Log Database page** in the Forcepoint Security Manager.
- Use a disk array controller with multiple drives to increase I/O bandwidth.
- Increase the RAM on the Microsoft SQL Server machine to reduce time- consuming disk I/O operations.

SQL Server clustering is supported for failover or high availability.

Consult your Microsoft documentation for detailed information about optimizing Microsoft SQL Server performance.

Log Database sizing considerations

Log Database disk space requirements vary, based on:

- Network size
- Volume of Internet activity
- How long data must be available for use in reporting
- Logging settings
  It is important to host the database engine and Log Database on hardware that matches or exceeds the requirements for expected load and for historical data retention.

  Depending on the volume of Internet traffic in your network, and how much data your organization is required to store (based on organizational policy or compliance regulations, for example), the Log Database can become very large.

  To help determine an effective logging and reporting strategy for your organization, consider:
- When is the network traffic busiest?
  Schedule resource intensive database and reporting jobs at lower-volume times to improve logging and reporting performance during peak periods.

  See the Administrator Help (accessible from the Web Security module of the Forcepoint Security Manager) for information about scheduling database jobs, investigative reports, and presentation reports.
- How long should log data be kept to support historical reporting?
  Automatically delete partitions and trend data (stored in the catalog database) after they reach this age to reduce the amount of disk space required for the Log Database.

  See the Administrator Help for information about managing Log Database partitions.

- How much detail is really needed in reports? To decrease Log Database size, consider:
  - logging visits instead of hits (see *Logging visits (default) vs. logging hits*)
  - disabling full URL logging (see *Logging full URLs*)
  - enabling consolidation (see *Consolidation*
  - only logging non-HTTP protocol traffic for selected protocols (see *Protocol logging*)
  - only logging HTTP and HTTPS traffic in selected categories (see *Selective category logging*)

All of these logging settings can be customized in the Web module of the Security Manager. Tune your logging settings to achieve the appropriate balance of size savings and report detail for your organization.

Logging visits (default) vs. logging hits

When you log **visits**, one log record is created for each web page requested by a user, rather than each separate file included in the web page request. This creates a smaller database and allows faster reporting.

When you log **hits**, a separate log record is generated for each HTTP request to display any element of a web page, including graphics and ads. This type of logging results in a larger and more detailed database than the logging visits option.

Logging full URLs

Enabling full URL logging creates a larger database than with logging hits, and also provides the most detailed reports. Log records include the domain name and the full path to specific pages requested. Use this option if you want reports of real-time scanning activity.

If the Log Database is growing too quickly, you can turn off full logging to decrease the size of each entry and slow growth.

Consolidation

Consolidation helps to reduce the size of the database by combining 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

For example, the user visits **www.cnn.com** and receives multiple pop-ups during the session. The visit is logged as a record.

- If consolidation is turned off (the default), and the user returns to the site later, a second visit is logged.
- If consolidation is turned on, additional visits to the site within a specified period are logged as a single record, with a hits (i.e., visits) count indicating the number of times the site was visited in that period.

Protocol logging

If your deployment includes Network Agent, you have the option to log non-HTTP protocol traffic (for example, instant messaging or streaming media traffic) in addition to HTTP and HTTPS traffic.

The more protocols you choose to log, the greater the impact on the size of the Log Database. You can specify whether or not to log a specific protocol in each protocol filter that you create.

Selective category logging

By default, requests for URLs in all categories are logged. If your organization does not want to report on Internet requests for some categories, you can disable logging for those categories to help reduce Log Database size.

Deploying transparent identification agents

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Use transparent identification agents to identify users without prompting them for a user name and password in:

- Forcepoint Web Security deployments, as an alternative or supplement to transparent or explicit proxy authentication
- Standalone Forcepoint URL Filtering deployments
- Integrated deployments in which the integration product does not send user information to Filtering Service There are 4 transparent identification agents:
- **DC Agent** is used with a Windows Active Directory. The agent:
  - Works by identifying domain controllers in the network, and then retrieving user logon session information from those domain controllers
  - Can also be configured to poll client machines to verify logon status
  - Runs on a Windows server and can be installed in any domain in the network

  Note

  Some DC Agent features require local and domain administrator privileges.

  - May use NetBIOS port 139 for automatic domain detection. If NetBIOS port 139 is blocked in your network, deploy a DC Agent instance for each virtually or physically remote domain.
  - Communicates with Filtering Service on port 30600
- **Logon Agent** identifies users as they log on to Windows domains. The agent:
  - Runs on a Linux or Windows server
  - Requires a Windows-only client application (the Logon Application, or LogonApp.exe) to be run on client machines
  - Communicates with Filtering Service on port 30602
- **eDirectory Agent** is used with Novell eDirectory. The agent:
  - Runs on a Linux or Windows server
  - Uses Novell eDirectory authentication to map users to IP addresses
  - Communicates with Filtering Service on port 30700
- **RADIUS Agent** can be used in conjunction with either Windows- or LDAP-based directory services. The agent:
  - Runs on a Linux or Windows server
  - Works with a RADIUS server and client to identify users logging on from remote locations
  - Communicates with Filtering Service on port 30800

  Note

  eDirectory Agent or RADIUS Agent can be installed on the same machine as Filtering Service, or on a separate machine in the same network, but not on the same machine as Log Server.

In deployments that cover multiple locations, you can install an agent instance in multiple domains.

For example:

- One **DC Agent** instance can handle multiple trusted domains. Add additional instances based on:
  - The load placed on DC Agent
  - Whether a DC Agent instance can see all the domains on the network, including remote offices

  Load results from the number of user logon requests. With a large number of users (10,000+ users, 30+ domains), having multiple DC Agent instances allows for faster identification of users.

  If multiple Filtering Services are installed, each Filtering Service instance must be able to communicate with all DC Agent instances.
- One **Logon Agent** is required for each Filtering Service instance.
- One **eDirectory Agent** is required for each eDirectory Server.
- One **RADIUS Agent** instance is required for each RADIUS server.
  It is a best practice to install and run RADIUS Agent and the RADIUS server on separate machines. (The agent and server cannot have the same IP address, and must use different ports.)

  In some environments, a combination of transparent identification agents may be appropriate within the same network, or on the same machine. See *Combining transparent identification agents*.

  See *Installing web protection components* for transparent identification agent installation instructions. See the Administrator Help for configuration information.

Combining transparent identification agents

Web protection software can work with multiple transparent identification agents. If your environment requires multiple agents, it is best to install them on separate machines.

- eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service, or on a separate server on the same network.
- Do not run eDirectory Agent and DC Agent in the same deployment.

The following table lists supported combinations of transparent identification agents.

Combination	Same machine?	Same network?	Configuration required
Multiple DC Agents	No	Yes	Ensure that all instances of DC Agent can communicate with Filtering Service, and that the individual DC Agents are not monitoring the same domain controllers.
Multiple RADIUS Agents	No	Yes	Configure each agent to communicate with Filtering Service. Multiple instances of the RADIUS Agent cannot be installed on the same machine.
Multiple eDirectory Agents			Configure each instance to communicate with Filtering Service.

Combination	Same machine?	Same network?	Configuration required
Multiple Logon Agents	No	Yes	Configure each instance to communicate with Filtering Service.
DC Agent + RADIUS Agent	Yes	Yes	Each agent must use a unique port number to communicate with Filtering Service. By default, DC Agent uses port 30600; RADIUS Agent uses port 30800.
DC Agent + eDirectory Agent	No	No	Communication with both a Windows directory service and Novel eDirectory is not supported in the same deployment. However, both agents can be installed, with only one agent active.
DC Agent + Logon Agent	Yes	Yes	Configure each agent to use a unique port to communicate with Filtering Service. By default, DC Agent uses port 30600; Logon Agent uses port 30602.
RADIUS Agent + Logon Agent	Yes	Yes	Configure all agents to communicate with Filtering Service.
eDirectory Agent + Logon Agent	No	No	Communication with both Novell eDirectory and a Windows- or LDAP-based directory service in the same deployment is not supported. However, both agents can be installed, with only one agent active.
RADIUS Agent + eDirectory Agent	Yes	Yes	Configure each agent to use a unique port to communicate with Filtering Service. By default, eDirectory Agent uses port 30700; RADIUS Agent uses port 30800. When adding agents to the Security Manager, use an IP address to identify one, and a machine name to identify the other.

Combination	Same machine?	Same network?	Configuration required
DC Agent + Logon Agent + RADIUS Agent	Yes	Yes	This combination is rarely required. Configure each agent to use a unique port to communicate with Filtering Service. By default, DC Agent uses port 30600; Logon Agent uses port 30602; RADIUS Agent uses port 30800.

Related tasks

Installing web protection components on page 157

Deployment guidelines for Network Agent

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *NAT and Network Agent* ■ *Network Agent NIC configuration*

Network Agent manages Internet protocols (including HTTP, HTTPS, and FTP in standalone deployments), by examining network packets and identifying the protocol.

When Network Agent is used, it must be installed:

- Inside the corporate firewall
- Where it can see all Internet requests for the machines it is assigned to monitor

Network Agent monitors and manages only the traffic that passes through the network device (typically a switch) to which it is attached. Multiple Network Agent instances may be needed, depending on:

- network size
- volume of Internet requests
- network configuration

While a simple network may require only a single Network Agent, a segmented network may require (or benefit from) a separate Network Agent instance for each segment.

Network Agent functions best when it is closest to the computers that it is assigned to monitor.

NAT and Network Agent

If you use Network Address Translation (NAT) on internal routers, Network Agent may be unable to identify the source IP address of client machines. When Network Agent detects traffic after it is passed through such a router, the agent sees the IP address of the router's external interface as the source of the request, rather than the IP address of the client machine.

To address this issue, either disable NAT, or install Network Agent on a machine located **between** the NAT router and the monitored clients.

Network Agent NIC configuration

Network Agent must be able to see all outgoing and incoming Internet traffic on the network segment that it is assigned to monitor. Do not install multiple instances of Network Agent on the same machine.

If the Network Agent machine connects to a switch:

- Configure the switch to use a mirror or span port, and connect Network Agent to this port, to allow the agent to see Internet requests from all monitored machines.

  Note

  Not all switches support port spanning or mirroring. Contact the switch vendor to verify that spanning or mirroring is available, and for configuration instructions.

- You have the option to use a switch that supports bidirectional spanning. This allows Network Agent to use a single network interface card (NIC) to both monitor traffic and send block pages.
  If the switch does not support bidirectional spanning, the Network Agent machine must have at least 2 NICs: one for monitoring and one for blocking.

  - Best practices suggest a maximum of 5 NICs.
  - The NICs can be connected to ports on the same network device (switch or router), or to different network devices.

  Network Agent can also connect to an unmanaged, unswitched hub located between an external router and the network.

  If the machine running Network Agent has multiple NICs:

- Each NIC can be configured to monitor or block Internet requests, or both.
- The blocking or inject NIC (used to serve block pages) **must have an IP address** (cannot be set for stealth mode).
- A NIC configured only to monitor (but not block) does not need an IP address (can be set for stealth mode). See *Network Agent and stealth mode NICs* for more details about stealth mode.
- Each NIC can be configured to monitor a different network segment.
- At least one NIC must be configured for blocking.
  When you configure separate network cards to monitor traffic and send block messages:
- The monitoring and blocking NIC do not have to be assigned to the same network segment.
- The monitoring NIC must be able to see all Internet traffic in the network segment that it is assigned to monitor.
- Multiple monitoring NICs can use the same blocking NIC.
- The blocking NIC must be able to send block messages to all machines assigned to the monitoring NICs, even if the machines are on another network segment.
  During installation, you specify which NIC is used for communication and which NIC or NICs are used by Network Agent.

  For information on positioning Network Agent in your network, see:

  - *Locating Network Agent in a single-segment network*
  - *Locating Network Agent in a multiple-segment network*
  - *Network Agent on a gateway*

Related reference

Locating Network Agent in a single-segment network on page 58
Locating Network Agent in a multiple-segment network on page 59
Network Agent on a gateway on page 62

Related information

Network Agent and stealth mode NICs on page 339

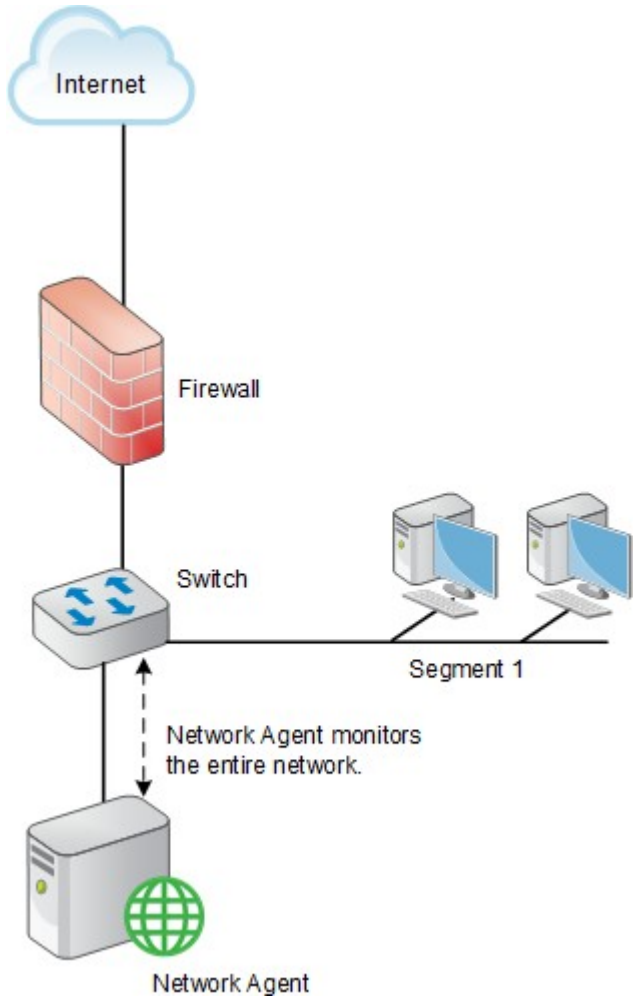
Locating Network Agent in a single-segment network

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

A single segment network is a series of logically connected nodes (computers, printers, and so on) operating in the same portion of the network. In a single segment network, Filtering Service and Network Agent must be positioned to monitor Internet traffic across the entire network.

The following illustration shows Network Agent in a standalone Forcepoint URL Filtering deployment, installed in a central location to see both HTTP and non-HTTP traffic.



Locating Network Agent in a multiple-segment network

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Depending on the device used to connect network segments, some traffic may not be sent to all segments. A router, bridge, or smart hub serves as traffic control, preventing unneeded traffic from being sent to a segment. In this environment:

- Filtering Service must be installed where it can receive and manage Internet requests from Network Agent and any integration product.
- Each Network Agent instance must be able to see all Internet requests on the segment or segments that it is configured to monitor.
  Multiple Network Agent instances may be needed to capture all Internet requests. A Network Agent can be installed on each segment to monitor the Internet requests from that segment.

Note

A limit of 4 Network Agents is suggested for each Filtering Service. It may be possible to use more agent instances, depending on system and network configuration and the volume of Internet requests.

If multiple Network Agent instances are installed:

- Ensure that the instances are deployed so that, together, they monitor the entire network. Partial deployment results in incomplete policy enforcement and loss of log data in network segments not visible to Network Agent.
- Each Network Agent instance must monitor a non-overlapping set of IP addresses. An overlap can result in inaccurate logging and network bandwidth measurements, and improper bandwidth-based policy enforcement.
  The network segment or IP address range monitored by each Network Agent instance is determined by the NIC settings for the agent, configured in the Forcepoint Security Manager. See the Administrator Help for instructions.
- Avoid deploying Network Agent across different LANs. If you install Network Agent on a machine in the 10.22.x.x network, and configure it to communicate with a Filtering Service machine in the 10.30.x.x network, communication may be slow enough to prevent Network Agent from blocking an Internet request before the site is returned to the user.

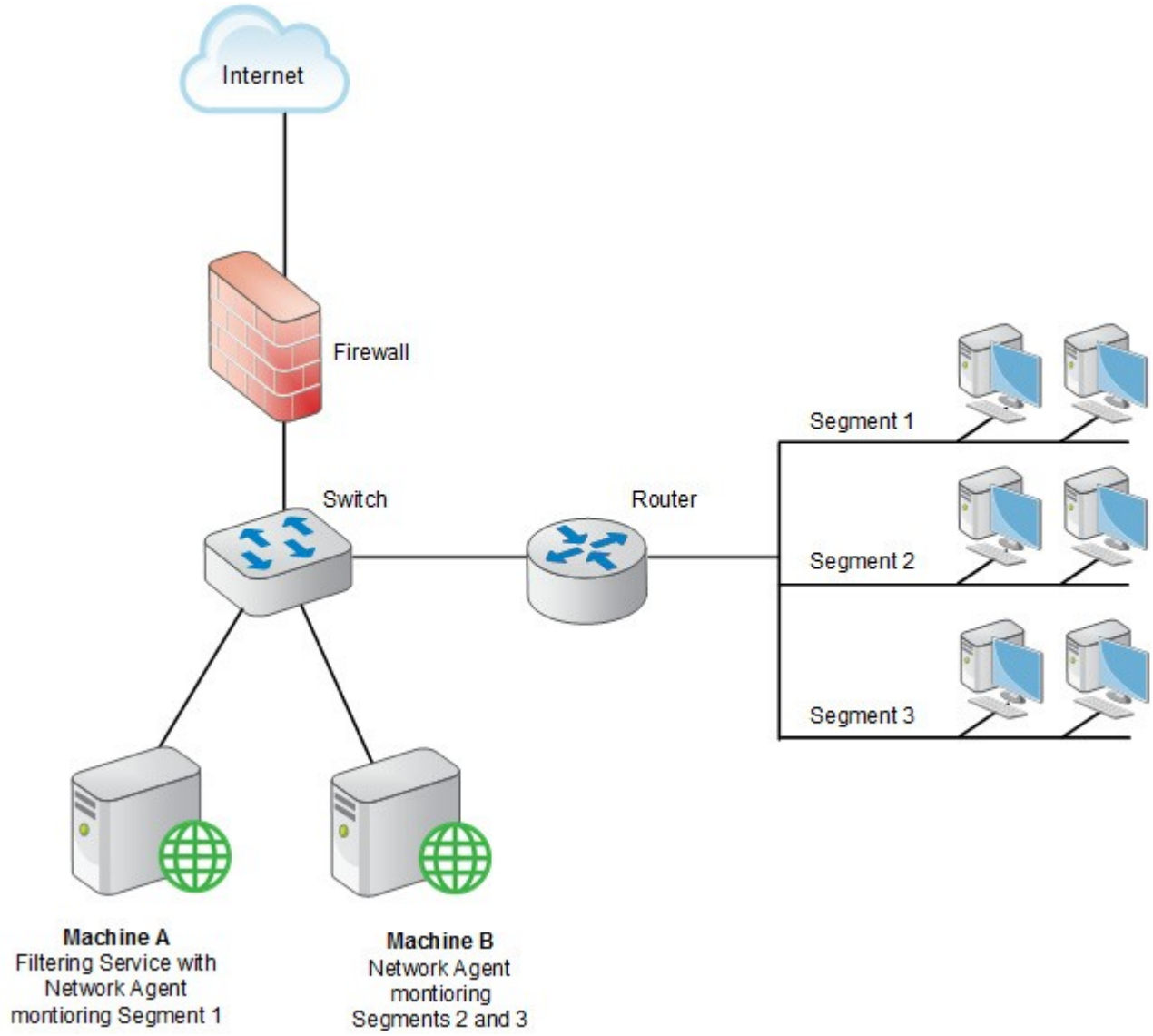
Central Network Agent placement

A network with multiple segments can be managed from a single location. Install Filtering Service where it can receive Internet requests from each Network Agent and any integration product.

If the network contains multiple switches, Network Agent instances are inserted into the network at the last switch in the series. This switch must be connected to the gateway that goes out to the Internet.

In the following illustration:

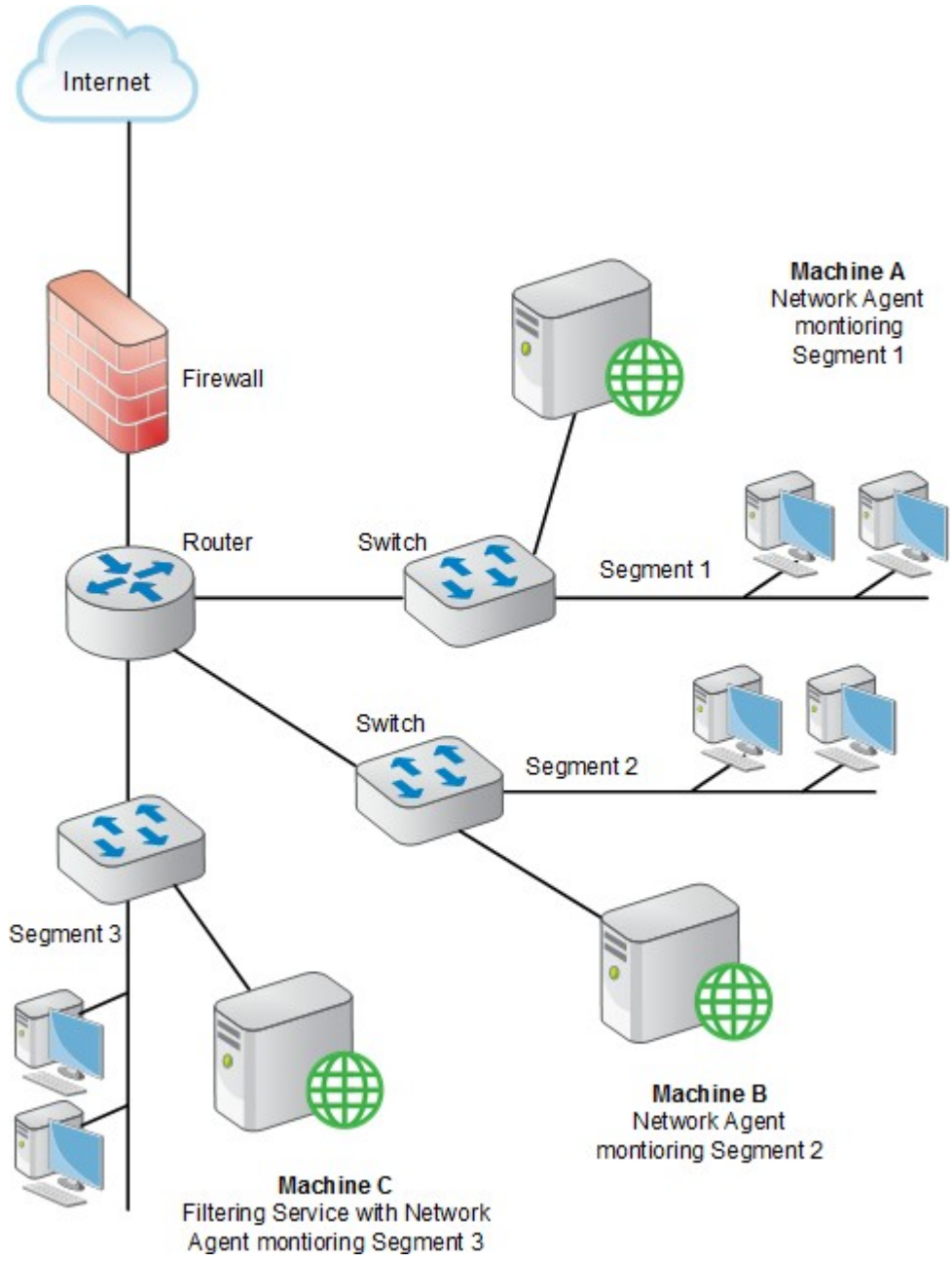
- One Network Agent instance is installed with Filtering Service on Machine A. This machine is connected to the network via a switch that is configured to mirror or span the traffic of network Segment 1.
- A second Network Agent is installed on Machine B, which is connected to the same switch as Machine A. Machine B is connected to a different port that is configured to mirror the traffic of Segments 2 and 3.
- Each Network Agent is positioned to see all traffic for the network segment it monitors, and to communicate with other web protection components.
- The switch is connected to the gateway, allowing the Network Agent instances to monitor network traffic for all network segments.



Distributed Network Agent placement

The network diagram below shows a single Filtering Service with 3 Network Agents, one for each network segment. A deployment like this might be useful in organizations with satellite offices, for example.

- Filtering Service (Machine C) must be installed where it is able to receive and manage Internet requests from each Network Agent instance and any integration product.
- Each Network Agent (machines A, B and C) is connected to the network segment it monitors via the switch's span or mirror port.
  In the following illustration, the switches are not connected in a series. However, each switch is connected to the router, which is connected to the gateway.



Network Agent on a gateway

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

A gateway provides a connection between two networks. The networks do not need to use the same network communication protocol. The gateway can also connect a network to the Internet.

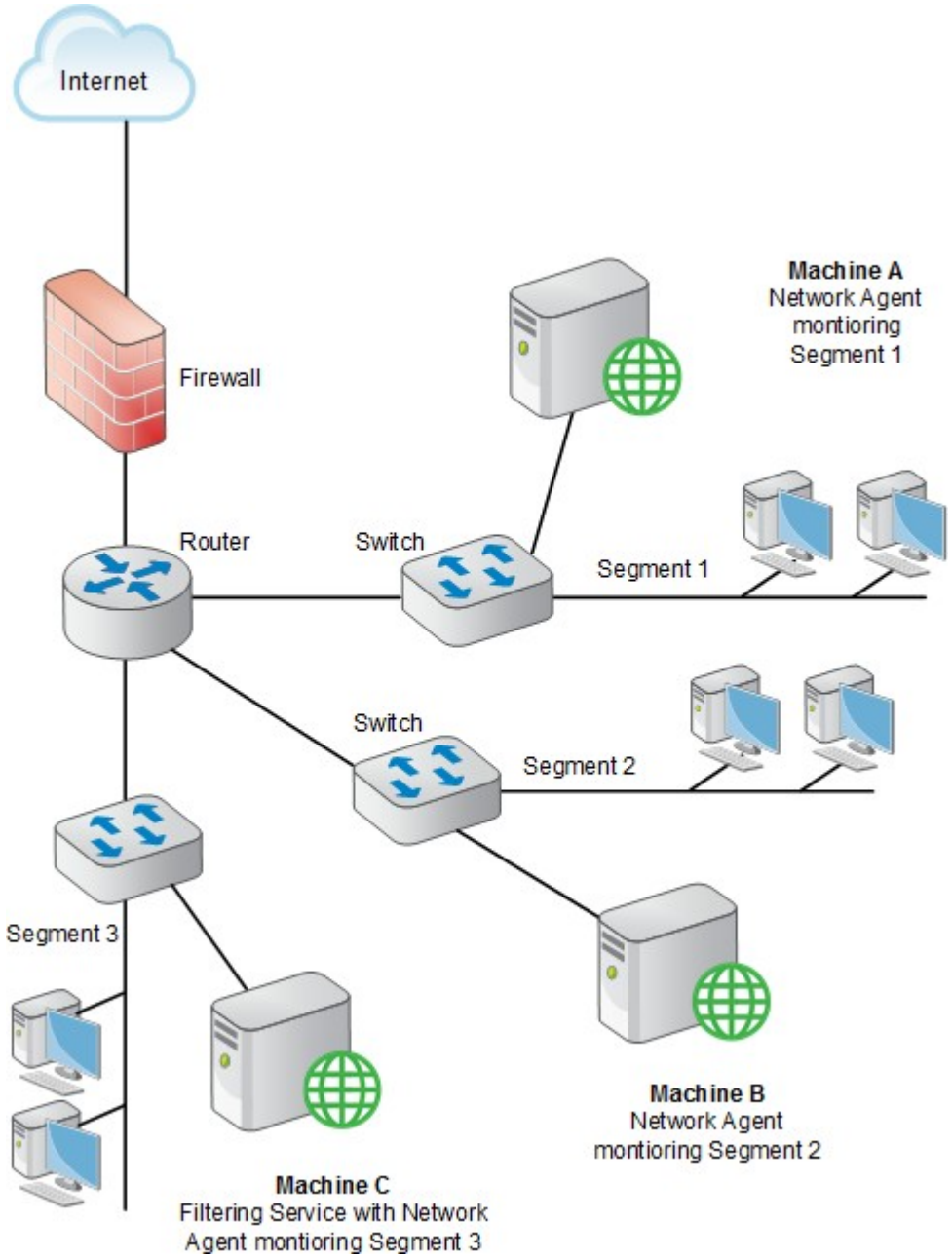
Network Agent can be installed on the gateway machine, allowing Network Agent to manage and monitor all Internet traffic. The gateway can either be a third-party proxy server or a network appliance.

Do not install Network Agent on a firewall. Also, if your network includes a software installation of Content Gateway, do not install Network Agent on the Content Gateway machine. (Content Gateway and Network Agent can reside on the same appliance.)

The following illustration shows Network Agent monitoring the Internet traffic at the proxy gateway or caching appliance directly attached to the firewall.

Important

The gateway configuration shown here is best used in small to medium networks. In larger networks, performance can suffer as a result of resource competition between the gateway software and Network Agent.



Deploying Remote Filtering Server and Client

Applies to:

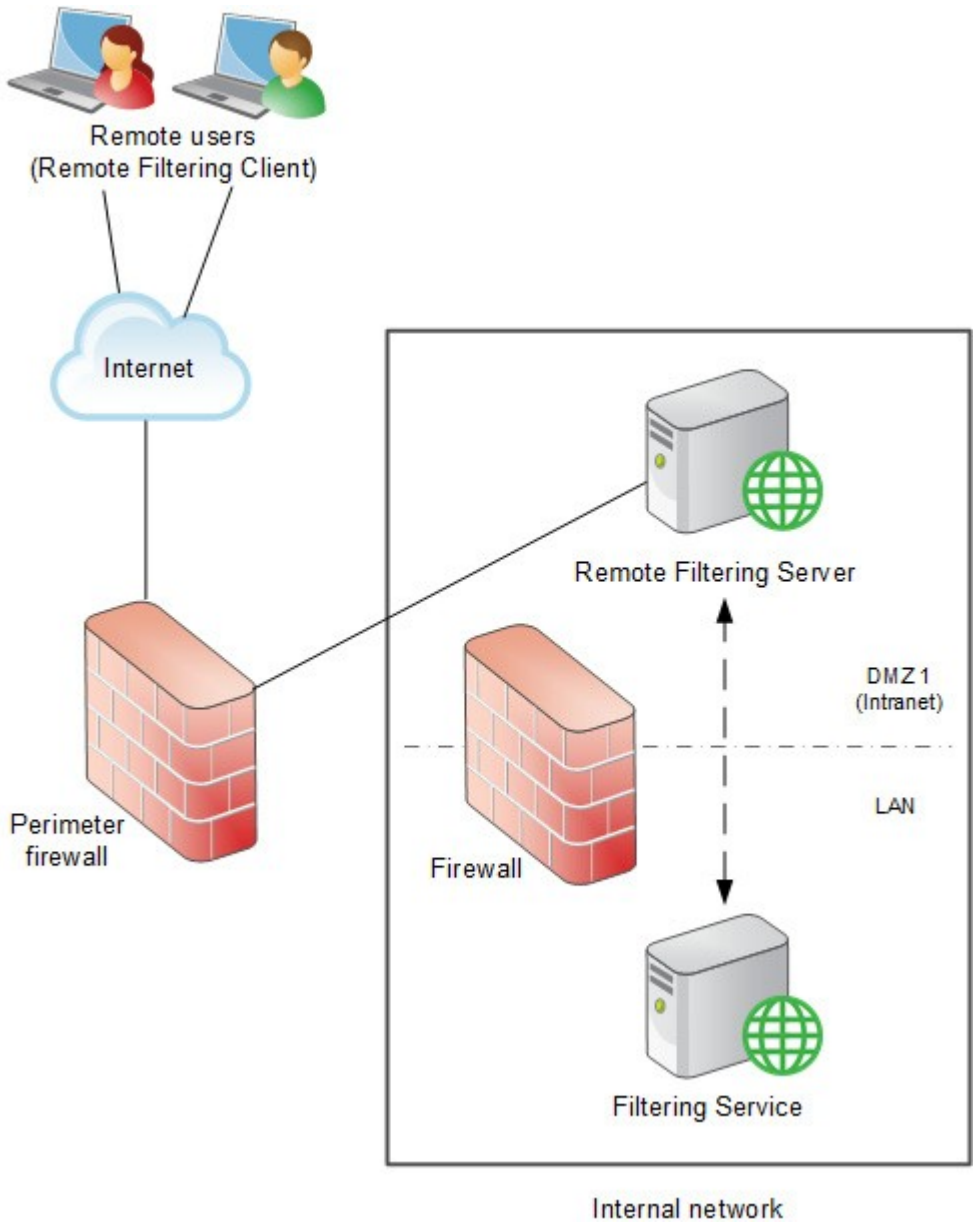
- Forcepoint URL Filtering, v8.5.x

With Forcepoint URL Filtering, you have the option to add the Remote Filter module to manage Internet activity for machines that reside or travel outside your network.

- **Remote Filtering Client** is installed on each remote machine.
- The client software communicates with **Remote Filtering Server**, which acts as a proxy to Filtering Service. Communication between the components is authenticated and encrypted. When you install remote filtering components:
- Install Remote Filtering Server on a dedicated machine that can communicate with the Filtering Service machine.
  As a best practice, install Remote Filtering Server in the DMZ outside the firewall protecting the rest of the corporate network. This is strongly recommended.
- Do **not** install Remote Filtering Server on the same machine as Filtering Service or Network Agent.
- Each Filtering Service instance can have only one primary Remote Filtering Server.
  Remote Filtering Client system recommendations:
- Pentium 4 or greater
- Free disk space: 25 MB for installation; 15 MB to run the application
- 512 MB RAM

Network Size	Hardware Recommendations
1-500 clients	**Windows** or **Linux** ■ Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater ■ 2 GB RAM ■ 20 GB free disk space
500+ clients	**Windows** or **Linux** ■ Quad-Core Intel Xeon 5450 or better processor, 3.2 GHz or greater ■ 4 GB RAM ■ 20 GB free disk space

The following illustration provides an example of a Remote Filtering deployment. The illustration does not include all web protection components. For more information, see the Deploying the Remote Filter Module technical paper.


Remote users
(Remote Filtering Client)
Internet
Remote Filtering Server
DMZ 1
(Intranet)
LAN
Perimeter
firewall
Firewall
Filtering Service
Internal network

Chapter 4

Web protection distributed deployments

Contents

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Distributed enterprise networks may have many remote locations, ranging from dozens to thousands of small sites. The remote locations have Internet access, but may have no dedicated IT staff.

The challenge is to apply consistent, cost-effective web security across the entire organization.

- Remote sites must have Internet access.
- Internet access is provided by independent Internet service providers, often using low to medium-bandwidth connections.
- Web requests are sent directly to the Internet and are not first routed through a central corporate network.
- Internet access must be managed to permit only appropriate content.
- Cost or maintenance considerations prohibit deploying a dedicated web protection server at each site.

Forcepoint Web Security and Forcepoint URL Filtering can be deployed as on- premises solutions whose policy enforcement components can be located regionally and communicate over the Internet to apply uniform policies across all offices.

The Forcepoint Web Security Hybrid Module for Forcepoint Web Security allows a combination of on-premises and in-the-cloud policy enforcement.

For more information, see:

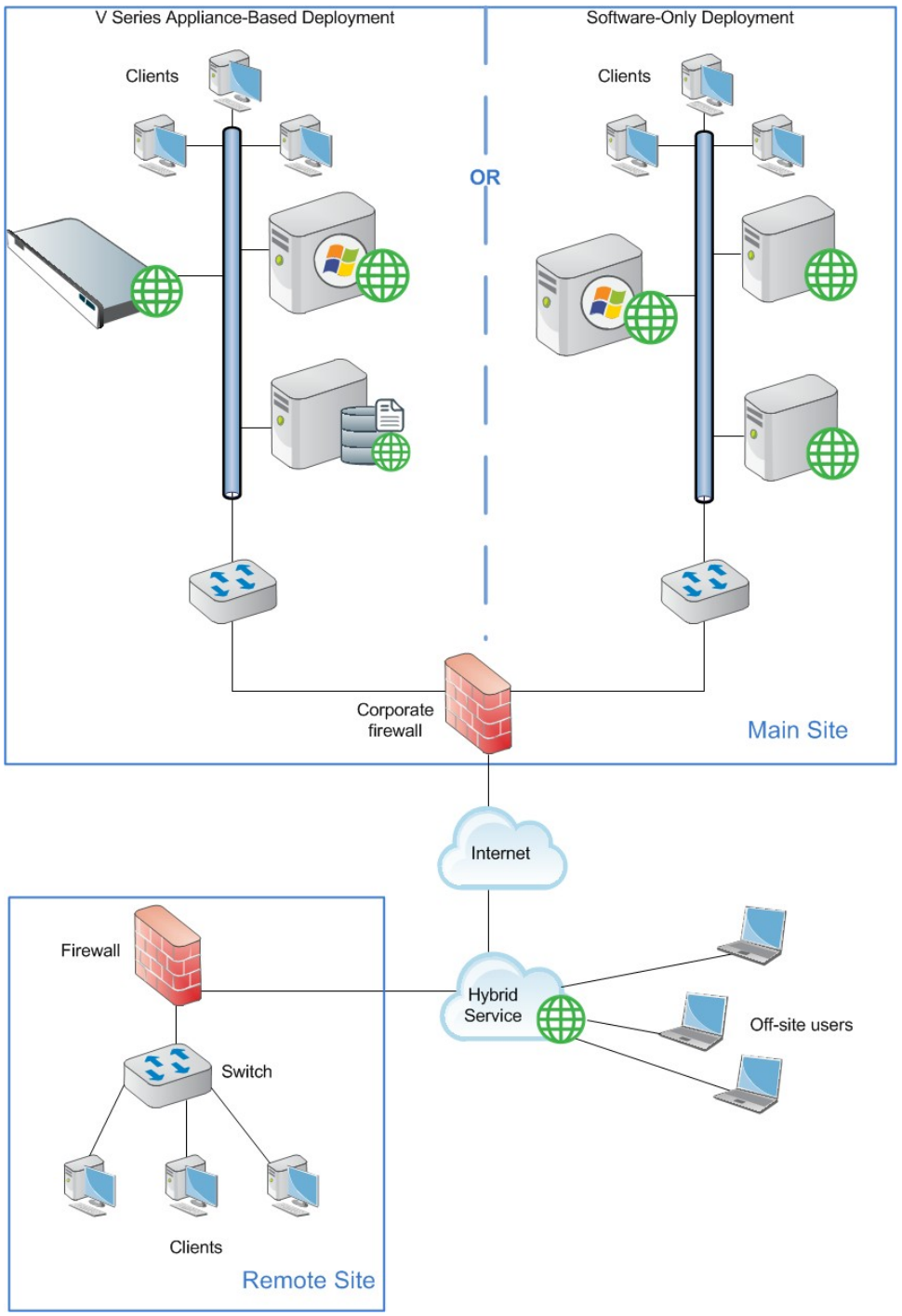
- *Web protection basic distributed enterprise topology*
- *Web protection for remote users or locations*
- *Web protection distributed deployment models*
- *Web protection distributed deployments and secure VPN connections*

Web protection basic distributed enterprise topology

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *Forcepoint Web Security* ■ *Forcepoint URL Filtering*

Forcepoint Web Security

On-premises deployments of Forcepoint Web Security may be hosted on Forcepoint appliances, Windows and Linux servers, or a combination. With the addition of the Web Security Hybrid Module, the cloud-based hybrid service can be added to provide policy enforcement for remote locations or off-site users.



Forcepoint Web Security on-premises components may be hosted on:

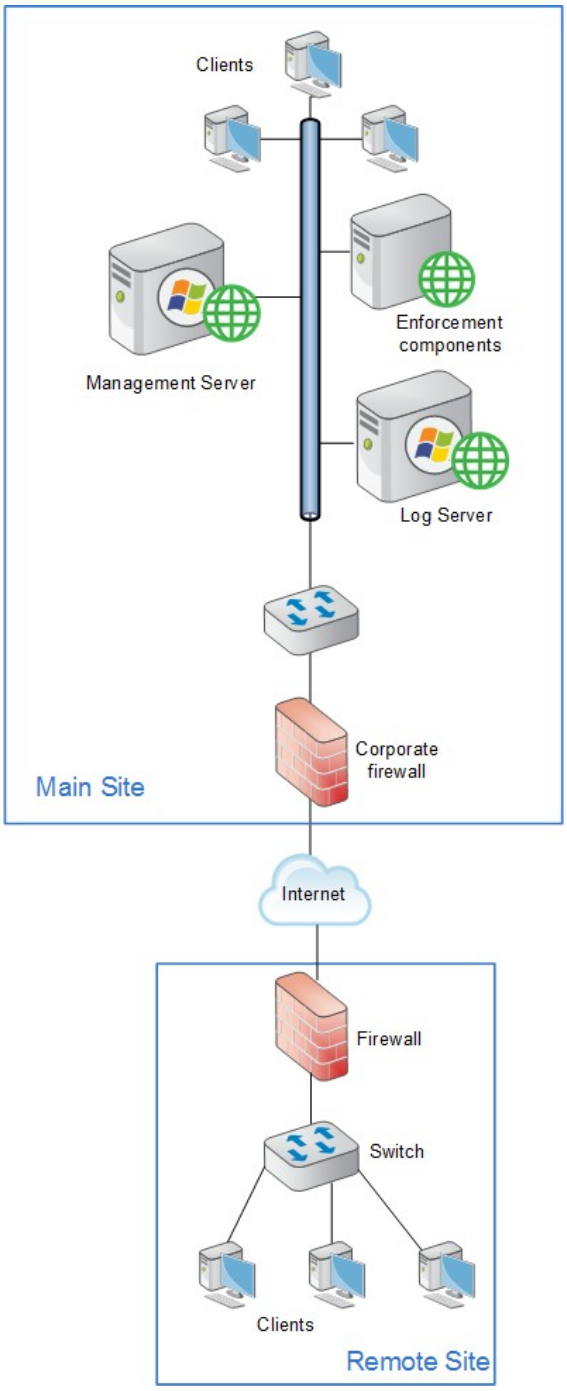
- One or more appliances running core policy components, plus additional servers running reporting, management, and interoperability components.
- One or more Windows or Linux servers running core policy and interoperability components, plus Windows servers running reporting and management components.

The hybrid service can be used to manage Internet activity for remote sites or off-site machines.

Forcepoint URL Filtering

To reduce network infrastructure costs, each remote-site firewall in a decentralized network is connected directly to the Internet, rather than to a corporate WAN.

A small office/home office (SOHO) firewall is connected to an ISDN, DSL/cable, or T1 connection. Except for corporate application data that may use a virtual private network (VPN) connection, each outbound Internet request from a remote site is sent through a local Internet service provider (ISP) to the Internet.



Optionally, off-site users (remote users outside the corporate or remote-site network) can have requests managed by adding the Remote Filter module. This requires that Remote Filtering Server (not depicted) be deployed in the main site network and Remote Filtering Client be installed on each off-site machine. For more details, refer the section *Deploying Remote Filtering Server and Client*.

Related reference

Deploying Remote Filtering Server and Client on page 64

Web protection for remote users or locations

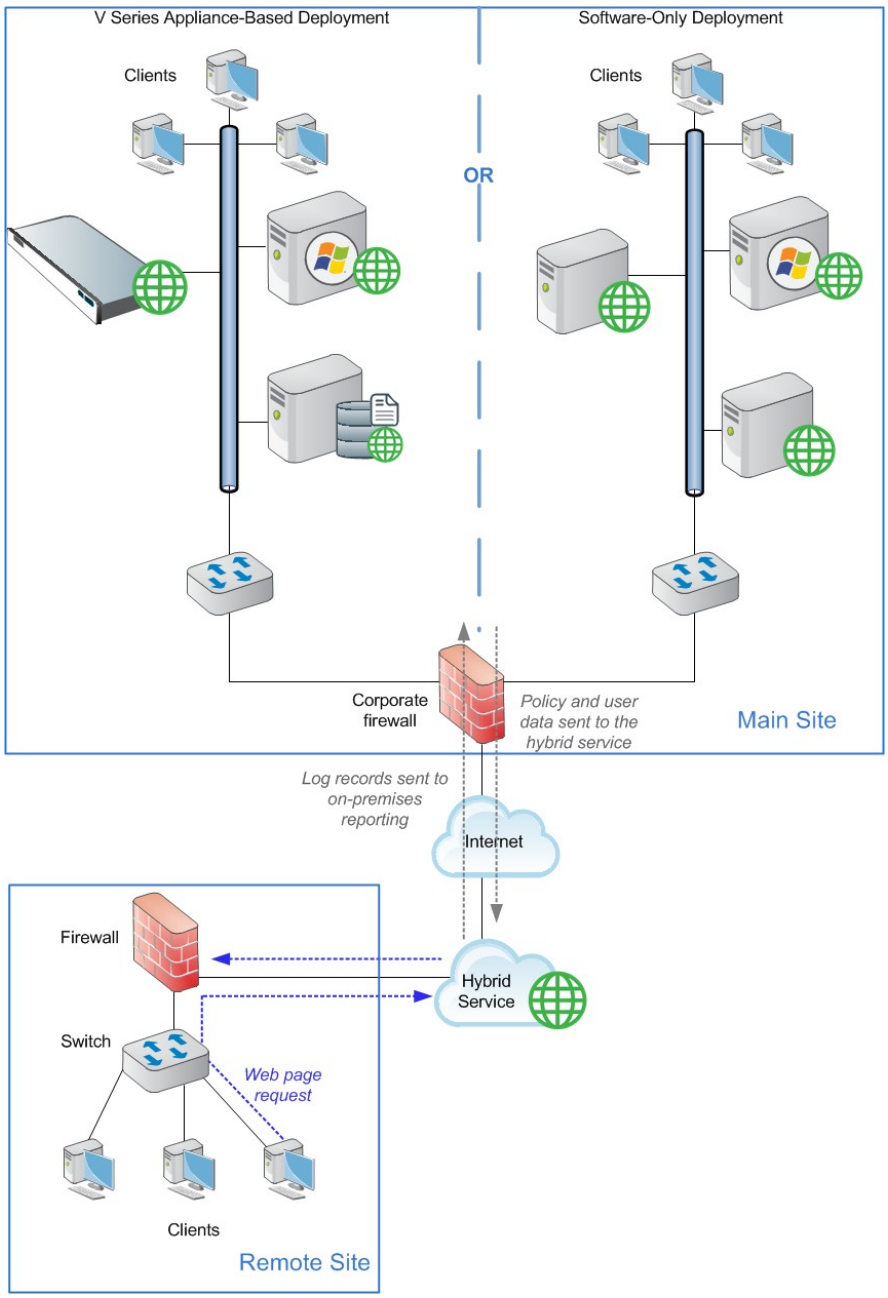
Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *Forcepoint Web Security* ■ *Forcepoint URL Filtering*

Forcepoint Web Security

In an on-premises Forcepoint Web Security deployment, Internet requests from remote sites can be managed by either by software installed at the main site, or with the Web Security Hybrid Module, by the hybrid service in the cloud.

Using the hybrid service may address network latency issues, because requests from remote sites and off-site users are managed by the nearest hybrid service cluster.

The following illustration shows how remote-site Internet management works via the hybrid service. A user's web request is directed to the hybrid service, which permits or blocks the request based on the applicable policy.



Policy settings are defined at the main site and uploaded automatically to the hybrid service at preset intervals. User information, for user- or group-based policy enforcement, is also uploaded.

Log data for reporting is downloaded from the hybrid service to the main site automatically and is incorporated into the Log Database (at the main site). Thus, reports can cover users at all offices.

Forcepoint URL Filtering

In centralized organizations that route all outbound Internet requests through a single large Internet connection, the servers running Forcepoint URL Filtering are normally placed physically close to the firewall, proxy server, or network appliance.

Remote sites in a distributed enterprise have a direct local connection to the Internet, and no centralized point of control.

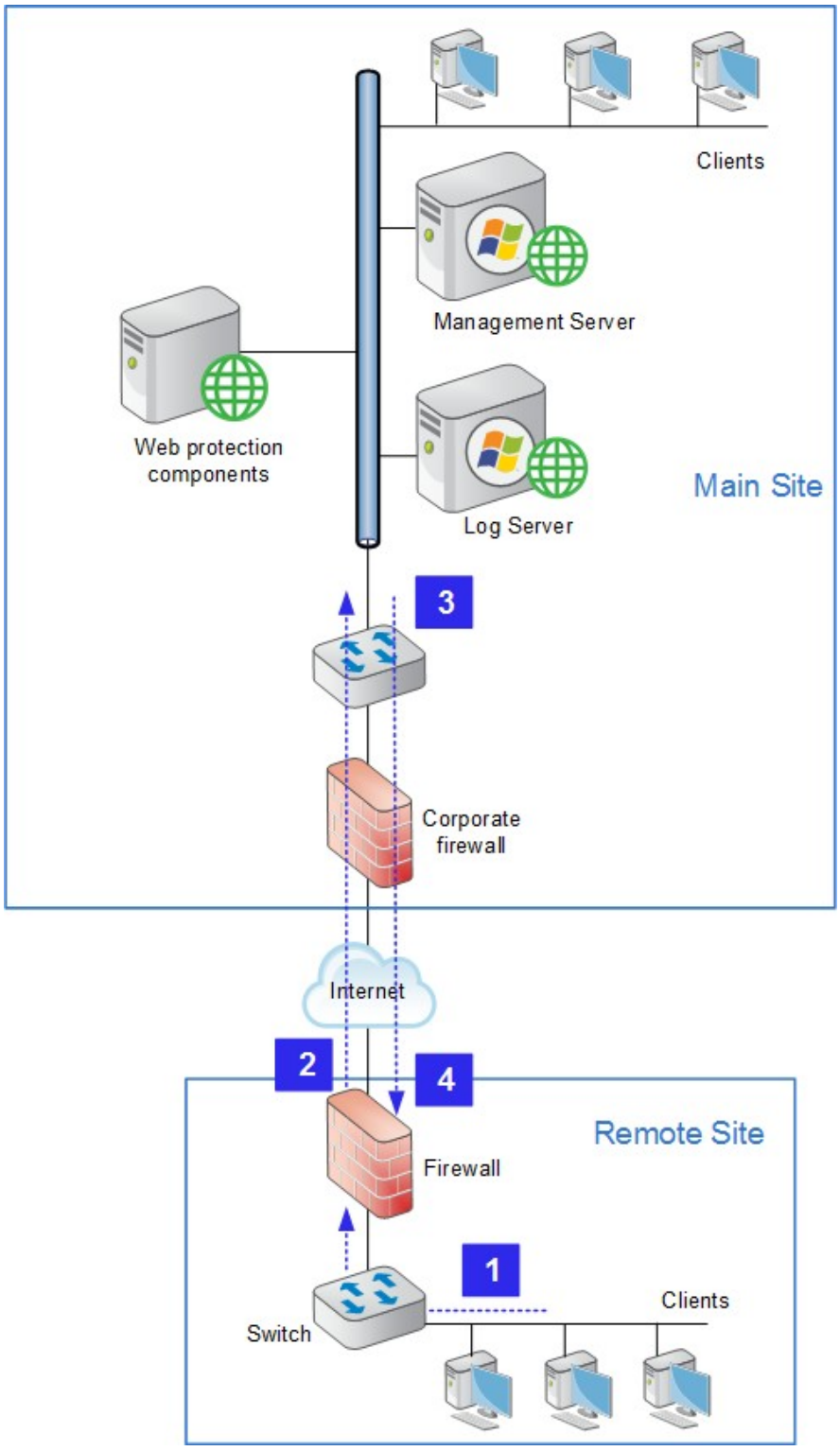
Rather than deploying Forcepoint URL Filtering components at each remote-site firewall, you can deploy them in a geographically central location. Since the software is accessible from the Internet, components should be protected by a firewall that allows URL lookup requests to pass through.

Policy enforcement is performed by components at the main site. Remote sites must be equipped with a firewall that can be configured to check with Forcepoint URL Filtering to permit or block web requests, or an instance of Network Agent must be deployed at the remote site.

Forcepoint has tested this configuration in cooperation with several of its integration partners. The Partners page at forcepoint.com links to pages that list our Security Alliance and Vendor Alliance partners.

This configuration provides distributed enterprises with policy enforcement for each remote site. It also:

- Provides uniform Internet access policies at each location.
- Eliminates the cost of additional hardware to host web protection software at each remote site.
- Allows the enterprise to centrally configure, administer, and maintain a limited number of Forcepoint URL Filtering machines.
  The following illustration shows the basic sequence of events involved in responding to a web request from a remote site.



1) A user requests a web page.

2) The request is directed through the local firewall to web protection software at the main site via the Internet.

3) Web protection software responds via the Internet, either permitting or blocking the request.

4) The user is given access to the site or sees a block page.

In the case of multiple remote sites, each remote site communicates with policy enforcement components at the main site in the same manner shown above.

Off-site user machines (like laptops used by travelers) may be managed using the Remote Filter module. See *Deploying Remote Filtering Server and Client*

Related reference
Deploying Remote Filtering Server and Client on page 64

Web protection distributed deployment models

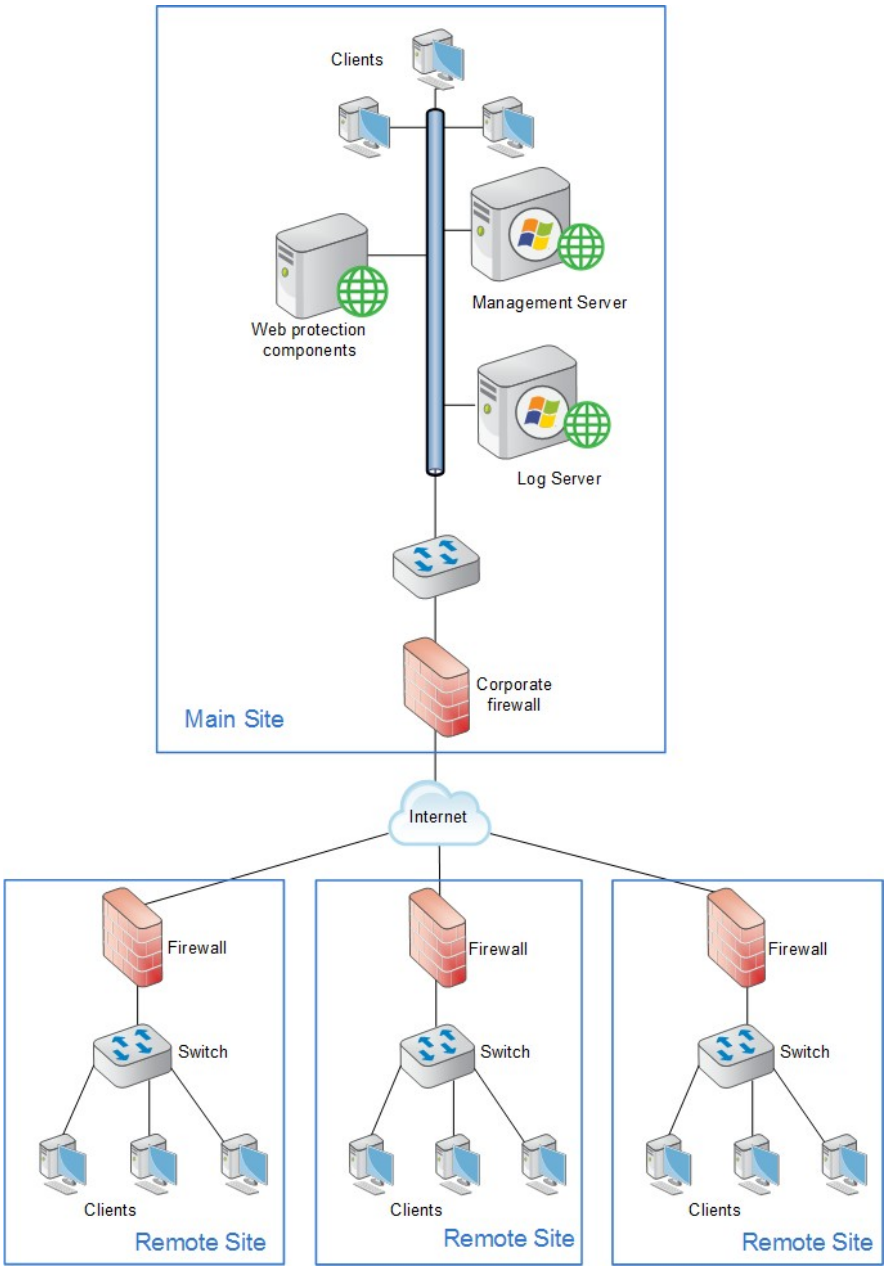
Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x	■ *Sites in a region* ■ *Expanding sites in a region* ■ *National or worldwide offices*

Deployment scenarios vary with different enterprise configurations. For example, an organization with 50 remote sites, all located in the same general region, deploys web protection software differently than a company with remote sites spread throughout the world. This section discusses 3 basic example models for distributed enterprises:

- *Sites in a region*: Remote sites located within one region
- *Expanding sites in a region*: Remote sites located within one region, with a growing number of employees or sites (or both)
- *National or worldwide offices*: Remote sites located nationally or globally

Sites in a region

The simplest deployment for a distributed enterprise is a network with remote sites in a single region, such as San Diego County, California, U.S.A. Most organizations with sites like this can use a single Forcepoint Web Security or Forcepoint URL Filtering on-premises deployment, centrally located within that region, to provide policy enforcement for all clients.



Each remote site would be managed as shown in the illustration under *Forcepoint URL Filtering*. The site at which the software is deployed is represented as the “main site”, but need not be truly a main site in your organization. It is whichever one houses the web protection software.

Off-site users, not shown in the above illustration, can be handled using the Web Security Hybrid Module (Forcepoint Web Security) or Remote Filter module (Forcepoint URL Filtering).

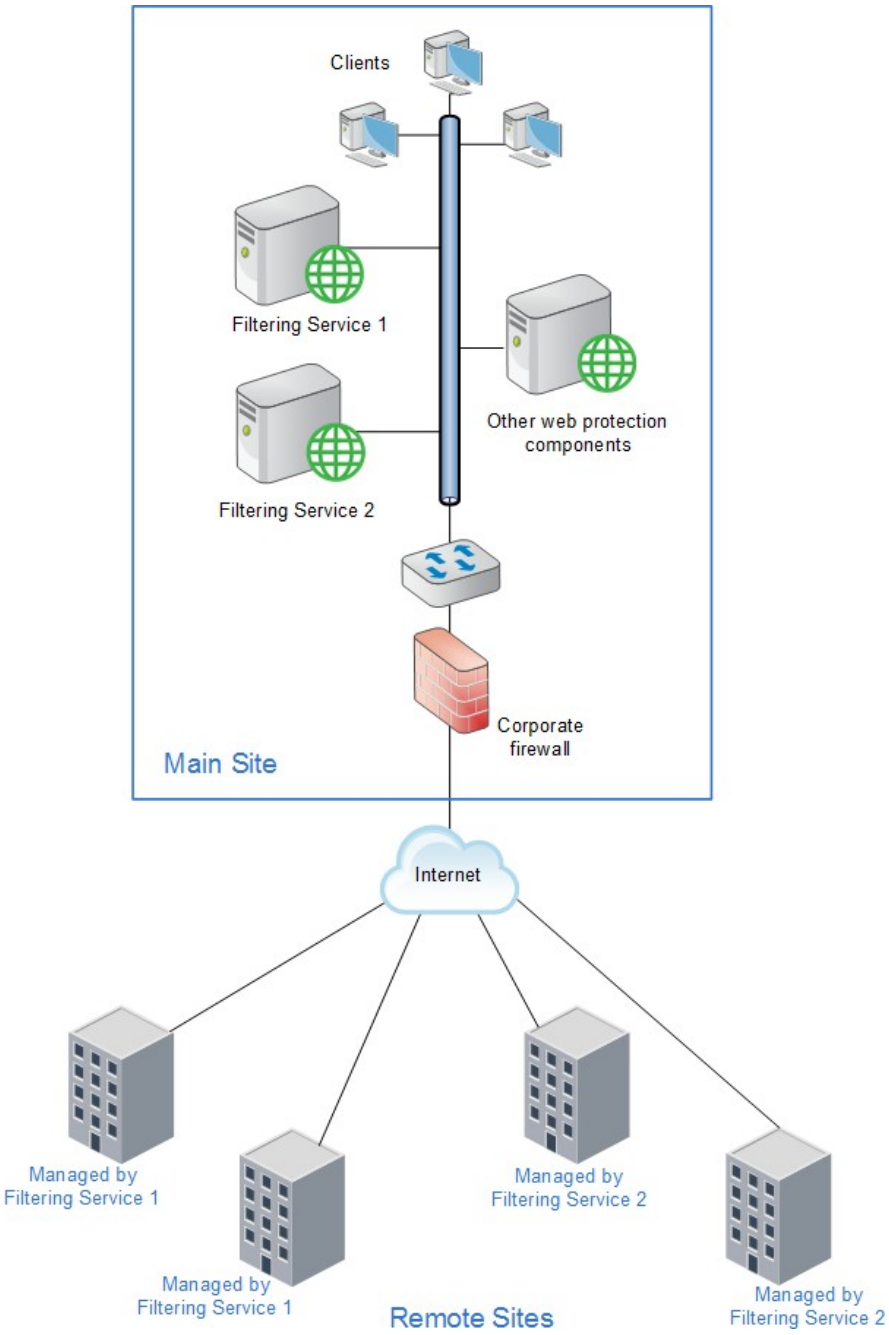
Expanding sites in a region

Some organizations deploy Forcepoint Web Security or Forcepoint URL Filtering within a given region and later decide to increase the number of remote sites in that area.

To compensate for the additional sites and employees, the organization can:

- **Improve the performance of the machines running web protection components**. Increasing the RAM and CPU, and installing faster hard drives on the machines allows web protection software to respond to an increased number of requests without additional latency. This type of upgrade can help with a moderate increase in head count, or the addition of a few more offices.

- **Deploy additional machines to run web protection components.** If a significant number of new users or sites is added, the deployment of additional instances of certain components, such as Filtering Service and Network Agent, distributes the load and provides optimum performance for each remote site.



Additional instances of web protection components can be deployed within the region as the number of offices continues to grow.

Off-site users, not shown in the above illustration, can be handled using the Web Security Hybrid Module (Forcepoint Web Security) or Remote Filter module (Forcepoint URL Filtering).

National or worldwide offices

On-premises only

Some organizations have hundreds of remote sites spread through a country or around the world. In such cases, one or two Forcepoint Web Security or Forcepoint URL Filtering installations are not enough because:

- Each remote site would be geographically distant from the policy enforcement components. Request lookups would have to travel farther over the Internet for management. This distance increases the total latency of the response and may lead to slower Internet access for end users.
- Large numbers of employees generate more Internet requests than recommended for one or two web protection machines, leading to delays in returning web pages to requesting clients.

These organizations should divide their sites into logical regions and deploy policy enforcement components in each region. For example, a distributed enterprise might group their United States sites into a western region, a central region, and an eastern region. Web protection components are deployed at a central site in each region.

The logical division of sites into regions depends on the location and grouping of remote sites and the total number of employees at each site. For example, a company with a large number of remote sites in a concentrated area, such as New York City, may need to deploy multiple web protection machines within that area. Or an enterprise may only have three sites in California with 100 to 250 employees each. In this case, a single web protection installation might be deployed for all three sites. This enterprise also can deploy web protection components locally at each site (rather than using a distributed approach), particularly if IT staff is present at each location. You may consider installing instances of Policy Server, Filtering Service, Content Gateway, and Network Agent to improve response time.

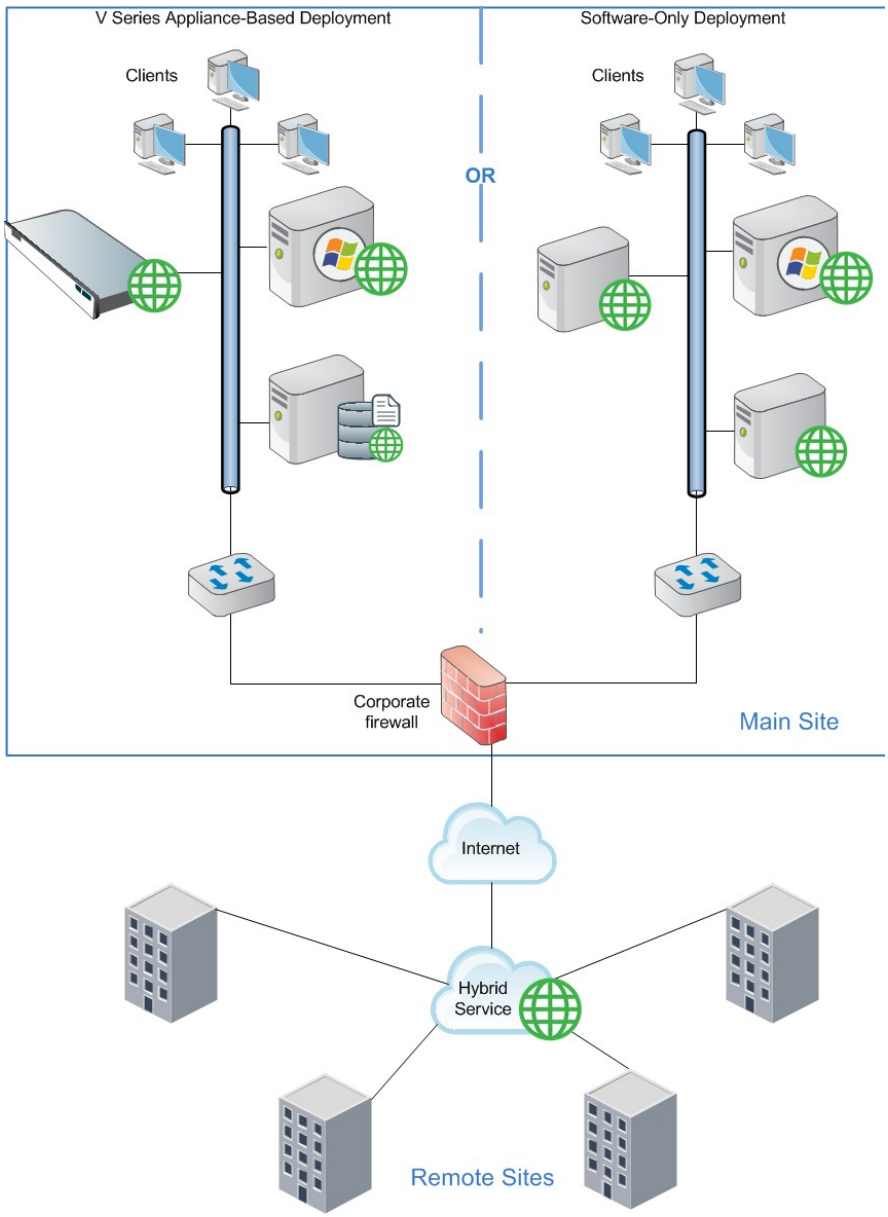
Given the significant number of variables, large organizations should contact a Forcepoint partner or Sales Engineer to plan a rollout strategy before deployment.

With the Forcepoint Web Security Hybrid Module

The Web Security Hybrid Module for Forcepoint Web Security is particularly well- suited for organizations with sites distributed nationally or worldwide.

Single main site

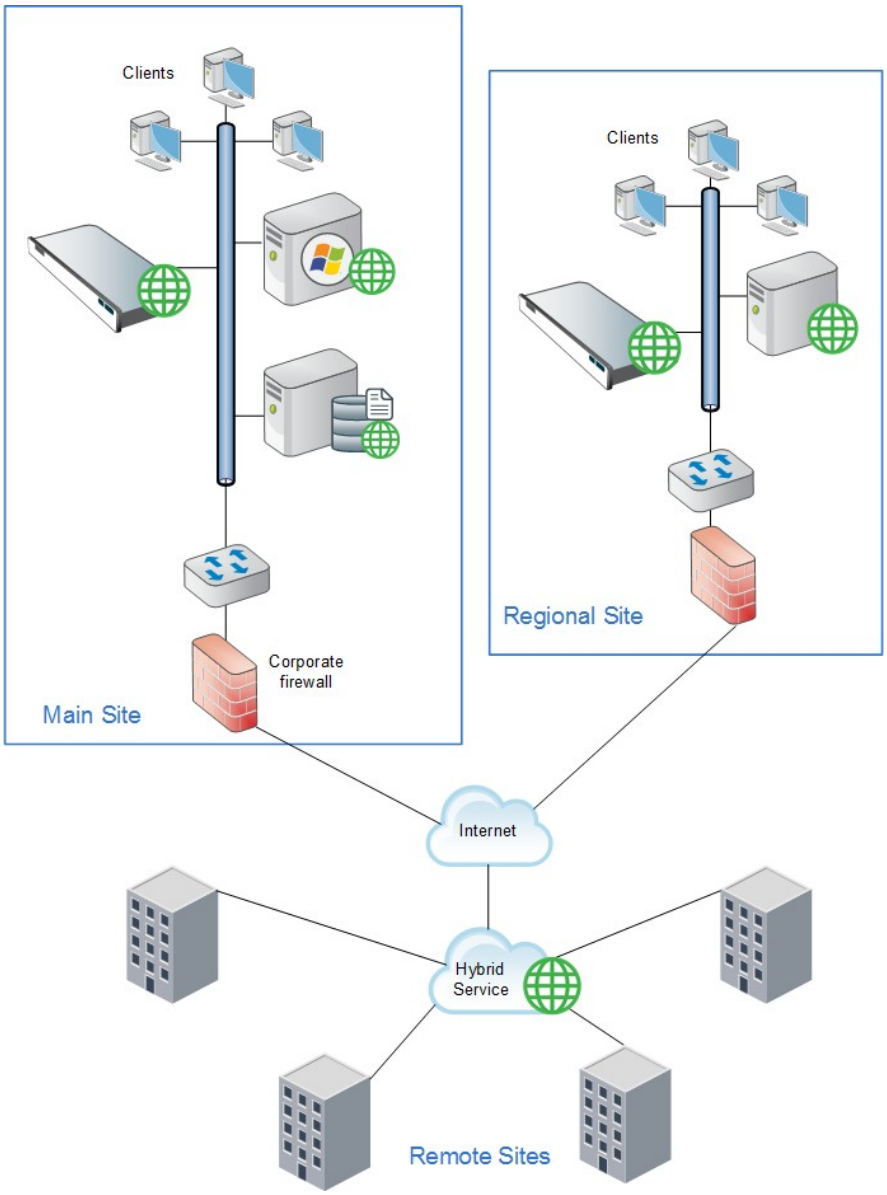
An organization with one main site (such as headquarters office or main campus) and multiple, geographically dispersed remote or branch sites can deploy Forcepoint Web Security at the main site (with policy enforcement for main-site users managed by the on-premises components) and have all remote sites managed by the hybrid service.



Off-site users, not shown in the above illustration, may also be managed by the hybrid service.

Multiple large sites

Organizations with multiple large sites (such as main headquarters and regional headquarters) can deploy on-premises software at the larger sites while managing small, remote sites through the hybrid service. Though the illustration shows a V Series appliance deployment, this can also be accomplished with X Series and virtual appliances and software-only deployments.



Related reference
Web protection for remote users or locations on page 71

Web protection distributed deployments and secure VPN connections

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

For URL lookup requests and replies, some firewalls allow administrators to set up a secure VPN connection between the remote-site firewalls and web protection components. Permitted requests then are fulfilled directly

from the Internet, providing an optimum combination of speed and security. See the firewall documentation to determine if the firewall supports this capability.

If a RADIUS server is being used with the VPN service, RADIUS Agent can be used for transparent user identification. See *Deploying transparent identification agents*. For information about installing RADIUS Agent, see *Installing web protection components*.

Related tasks

Installing web protection components on page 157

Related reference

Deploying transparent identification agents on page 53

Chapter 5

Content Gateway Deployment

Contents

Applies to:

- Forcepoint Web Security, v8.5.x

Content Gateway is the high-performance web proxy for on-premises deployments of Forcepoint Web Security. It provides real-time threat analysis and website classification to protect network computers from malicious web content and attacks, while facilitating employee access to web assets and dynamic web content.

Content Gateway offers:

- On-demand, real-time categorization of websites
- HTTP/S and FTP content analysis for malware and malicious threats
- Enterprise web caching capabilities
  Content Gateway, a required component of Forcepoint Web Security, can be installed on a Forcepoint V Series, X Series, or Virtual Appliance or as software running on dedicated servers.
- In an appliance-based deployment, Content Gateway is automatically installed on the appliance.
- In a software-based deployment, Content Gateway is installed on a Linux machine. The machine should be dedicated to running Content Gateway.
  Content Gateway can also improve network efficiency and performance by caching frequently accessed web pages at the edge of the network.

The following topics discuss deployment of Content Gateway:

- *Content Gateway deployment issues*
- *Content Gateway explicit and transparent proxy deployments*
- *Special Content Gateway deployment scenarios*
- *Chaining Content Gateway with other proxies*

For information about deploying other Forcepoint Web Security components, see *Deploying Web Protection Solutions*

For information about Content Gateway operation, see Content Gateway Manager Help.

Related concepts
Deploying Web Protection Solutions on page 33

Content Gateway deployment issues

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x	■ *Proxy deployment options* ■ *User authentication* ■ *HTTPS content inspection* ■ *Handling special cases*

Planning to deploy Content Gateway as a proxy in your network should include physical requirements, such as:

- Data center location and space
- Power and cooling requirements for hardware
- Required rack space
- Connectivity to existing or extended network topology
  Also consider:
- *Content Gateway* system requirements (hardware and operating system)
- Advantages and disadvantages of proxy network configuration options
- User authentication and identification options
- How to configure and use HTTPS content inspection
- A plan for handling special proxy/client issues

Internet connectivity

It is recommended that the Content Gateway host machine have Internet connectivity before starting the installation procedure. The software will install without Internet connectivity, but analytic database updates cannot be performed until Internet connectivity is available.

Security of the Content Gateway machine

Consider the following security issues prior to installing Content Gateway:

Physical security

Physical access to the system can be a security risk. Unauthorized users could gain access to the file system, and under more extreme circumstances, examine traffic passing through Content Gateway. It is strongly recommended that the Content Gateway server be locked in an IT closet and that a BIOS password be enabled.

Root permissions

Ensure that root permissions are restricted to a select few persons. This important restriction helps preclude unauthorized access to the Content Gateway file system.

Ports

For a list of default Content Gateway ports, see the ports spreadsheet for on-premises Web protection solutions . These ports must be open to support the full set of Forcepoint Web Security features.

Note

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

Restrict inbound traffic to as few other ports as possible on the Content Gateway server. In addition, if your subscription does not include certain features, you can restrict inbound traffic to the unneeded ports. For

example, if your subscription does not include Forcepoint DLP or the Forcepoint Web Security DLP module, you may choose to restrict inbound traffic to those ports related to Forcepoint DLP.

IPTables Firewall

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

Proxy deployment options

Content Gateway is used in either explicit or transparent proxy deployments.

With an explicit proxy deployment, client software, typically a web browser, is configured to send requests for Internet content directly to Content Gateway.

In a transparent proxy deployment, client requests for Internet content are intercepted (usually by a router) and sent to the proxy. The client is unaware that it is communicating with a proxy.

Both options have advantages and disadvantages. See *Content Gateway explicit and transparent proxy deployments* for more information.

Management clustering

A Content Gateway deployment can scale from a single node to multiple nodes to form a management cluster. With management clustering, all nodes in the cluster share configuration information. A configuration change on one node is automatically propagated all other nodes. Transparent proxy deployments with WCCP can disable cluster synchronization of WCCP configuration settings.

See Clusters in the Content Gateway Manager Help for information about configuring Content Gateway clusters.

IP spoofing

By default, when communicating with origin servers Content Gateway proxies client requests substituting its own IP address. This is standard forward proxy operation.

With both transparent and explicit proxy deployments, Content Gateway also supports IP spoofing.

IP spoofing configures the proxy to use either of the following:

- The IP address of the client when communicating with the origin server (basic IP spoofing)
- A specified IP address when communicating with the origin server (range-based IP spoofing)

IP spoofing is sometimes used to support upstream activities that require the client IP address or a specific IP address. It also results in origin servers seeing the client or specified IP address instead of the proxy IP address (although the proxy IP address can be a specified IP address).

IP spoofing:

- When enabled, is applied to both HTTP and HTTPS traffic; it cannot be configured to apply to only one protocol
- Is applied to HTTPS requests whether SSL support is enabled or not
- Relies on the ARM, which is always enabled
- Is not supported with edge devices such as a Cisco ASA or PIX firewall; When this is attempted, requests made by Content Gateway using the client IP address are looped back to Content Gateway

Warning

Deploying IP spoofing requires precise control of the routing paths on your network, overriding the normal routing process for traffic running on TCP ports 80 and 443.

With IP spoofing enabled, traditional debugging tools such as `traceroute` and `ping` have limited utility.

For complete information, see IP Spoofing in Content Gateway Manager Help.

User authentication

User authentication is the process of verifying a user via a username and password. Several types of user authentication are supported by Content Gateway.

User identification is the process of identifying a user based on the client IP address. Forcepoint Web Security offers a robust set of user identification agents.

Content Gateway user authentication

Content Gateway can be configured for **transparent user authentication**—with Integrated Windows™ Authentication (IWA) or Legacy NTLM—in which users are not prompted for credentials. Alternatively, Content Gateway can be configured for prompted (or manual) authentication, in which users are required to enter a username and password to obtain network access.

In the manual authentication process, Content Gateway prompts a user for proxy login credentials when that user requests Internet content. After the user enters those credentials, the proxy sends them to a directory server that validates the data. If the directory server accepts the user's credentials, the proxy delivers the requested content. Otherwise, the user's request is denied.

The issue of proxy user authentication is important in a deployment in which multiple proxies are chained. Authentication by the proxy closest to the client is preferred, but may not be possible given a particular network's configuration. Other issues include whether Content Gateway is chained with a third-party proxy and which proxy is designated to perform authentication. See *In a proxy chain* for more information.

Content Gateway supports the following user authentication methods:

- Integrated Windows Authentication (with Kerberos)
- Legacy NTLM (Windows NT™ LAN Manager, NTLMSSP)
- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Authentication Dial-In User Service)

Content Gateway supports both transparent and prompted authentication for Integrated Windows Authentication and Legacy NTLM. LDAP and RADIUS support prompted authentication.

Content Gateway also supports **rule-based authentication**. Rule-based authentication uses an ordered list of rules to support multiple realm, multiple domain, and other authentication requirements. When a request is processed, the rule list is traversed top to bottom, and the first match is applied.

Authentication rules specify:

1) How to match a user. By:
   - IP address
   - Inbound proxy port (explicit proxy only)
   - User-Agent value
   - A combination of the above

2) The domain or ordered list of domains to authenticate against.
   With a list of domains, the first successful authentication is cached and used in subsequent authentications. If IP address caching is configured, the IP address is cached. If Cookie Mode is configured, the cookie (user) is cached.

   Rule-based authentication is designed to meet several special requirements:

   - **Multiple realm networks** in which domains do not share trust relationships and therefore require that each domain's members be authenticated by a domain controller within their domain. In this environment rules are created that specify:
     - Members of the realm (untrusted domain) by IP address or proxy port
     - The realm (domain) they belong to
   - **Authentication when domain membership is unknown:** Some organizations do not always know what domain a user belongs to. For example, this can happen when organizations acquire new businesses and directory services are not mapped or consolidated. The unknown domain membership problem can

be handled in rule-based authentication by creating a rule for IP address lists or ranges that specifies an ordered list of domains to attempt to authenticate against. The first successful authentication is remembered and used in later authentications. If authentication is not successful or the browser times out, no authentication is performed.

- **Authentication based on User-Agent value:** One or more User-Agent values can be specified in an authentication rule. Often this is a list of browsers. When the User-Agent value matches a rule, authentication is performed against the specified domain or domains. If the User-Agent value doesn't match any rule and no rule matches based on other values, no authentication is performed (this is always true in rule-based authentication; if no rule matches, no authentication is performed).

See Content Gateway user authentication in Content Gateway Manager Help for detailed information.

Other methods of user identification

You can configure user identification in the Forcepoint Web Security module of the Forcepoint Security Manager rather than use user authentication on the proxy. Methods of user identification include both transparent identification via a transparent identification agent (such as Logon Agent or DC Agent) and manual (prompted) authentication. See the User Identification topic in the Forcepoint Web Security Administrator Help for more information.

HTTPS content inspection

When you use Content Gateway SSL support, HTTPS traffic is decrypted, inspected, and re-encrypted as it travels from the client to the origin server and back. Enabling this feature also means that HTTPS traffic from the server to the client can be inspected for uncategorized sites and sites with dynamic content. The SSL feature includes a complete set of certificate-handling capabilities. See Certificates in the Content Gateway Manager Help for more information.

When you run Content Gateway with Forcepoint DLP to inspect HTTPS traffic, you must enable SSL support. See Content Gateway Manager Help for a complete description of SSL support.

Deploying Content Gateway with SSL support enabled may require the following modifications to your system:

- Creation of trusted Certificate Authority (CA) certificates for each proxy to use for SSL traffic interception, and the installation of those certificates in each trusted root certificate store used by proxied applications and browsers on each client
- In explicit proxy deployments, additional client configuration in the form of Proxy Auto-Configuration (PAC) files or Web Proxy Auto-Discovery (WPAD)
- In transparent proxy deployments, integration with WCCP v2-enabled network devices, or Policy Based Routing.

Note

HTTPS content inspection can also affect system hardware resources like processing capacity and memory requirements.

When Content Gateway is configured to handle HTTPS traffic, you can specify categories of websites, individual websites, and clients for which decryption and inspection are bypassed. See SSL Decryption Bypass in Forcepoint Web Security Administrator Help.

Handling special cases

Any Content Gateway deployment must be able to handle web requests and web applications that are not compatible with the proxy or that should bypass the proxy. For example, requests for data from some internal, trusted sites could be configured to bypass the proxy, for system performance reasons. In explicit proxy deployments, a PAC file can be used to list the traffic that is allowed to bypass proxy inspection. In transparent proxy deployments, the proxy must be installed in a way that allows static bypass. See Static bypass rules in Content Gateway Manager Help.

See, also: Websites that have difficulty transiting Content Gateway.

Related reference
Content Gateway explicit and transparent proxy deployments on page 88
Special Content Gateway deployment scenarios on page 92

Content Gateway explicit and transparent proxy deployments

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x	■ *Explicit proxy deployment*, page 100 ■ *Transparent proxy deployment*, page 102

Content Gateway provides the following proxy deployment options:

- *Explicit proxy deployment,* where the user's client software is configured to send requests directly to Content Gateway
- *Transparent proxy deployment*, where user requests are transparently redirected to a Content Gateway proxy, typically by a switch or router, on the way to their eventual destination

For more information about configuring explicit and transparent proxy options in Content Gateway, see the Explicit Proxy and Transparent Proxy and ARM topics in the Content Gateway Manager Help.

Explicit proxy deployment

Use of Content Gateway in an explicit proxy deployment is an easy way to handle web requests from users. This type of deployment is recommended for simple networks with a small number of users. Explicit proxy is also used effectively when proxy settings can be applied by group policy. It requires minimal network configuration, which can be an advantage when troubleshooting.

For explicit proxy deployment, individual client browsers may be manually configured to send HTTP, and optionally, HTTPS and FTP, requests directly to the proxy. They may also be configured to download proxy configuration instructions from a Proxy Auto-Configuration (PAC) file. A group policy that points to a PAC file for configuration changes is a best practice for explicit proxy deployments. Another option is the use of Web Proxy Auto-Discovery (WPAD) to download configuration instructions from a WPAD server. See Explicit Proxy in the Content Gateway Manager Help for a sample PAC file and more information about how to implement these options. See also: PAC file best practices.

Exception handling instructions can also be included in the PAC file or WPAD instructions. For example, requests for trusted sites can be allowed to bypass the proxy.

Disadvantages of explicit proxy deployment include a user's ability to alter an individual client configuration and bypass the proxy. To counter this, you can configure the firewall to allow client traffic to proceed only through the proxy. Note that this type of firewall blocking may result in some applications not working properly.

You can also use a Group Policy object (GPO) setting to prevent users from changing proxy settings. If you cannot enforce group policy settings on client machines, this type of configuration can be difficult to maintain for a large user base because of the lack of centralized management.

Note

Non-browser client applications that cannot specify a proxy server may not work with an explicit proxy deployment.

Multiple proxies can provide for redundancy using Virtual Router Redundancy Protocol (VRRP). Using a single IP address, requests are sent to an alternate proxy in the event of failure. VRRP is not invoked until there is a failure with one of the proxies. See RFC 3768 for information on VRRP.

Configuring client browsers for explicit proxy

For explicit proxy deployments, you must configure each client browser to send Internet requests to Content Gateway, over the ports that Content Gateway uses for the associated protocol.

The default proxy port in Content Gateway for both HTTP and HTTPS traffic is 8080. The default port for FTP is 2121.

Use the instructions below to configure client browsers manually. Alternatively, use a PAC or WPAD file to configure client browsers.

Note

The instructions below are for the most common client browsers. For other client browsers refer to the browser's documentation.

Configuring Internet Explorer for explicit proxy

1) In Internet Explorer, select **Tools** > **Internet Options** > **Connections** > **LAN Settings**.
2) Select **Use a proxy server for your LAN**.
3) Click **Advanced**.
4) For **HTTP**, enter the Content Gateway IP address and specify port 8080.
5) For **Secure**, enter the Content Gateway IP address and specify port 8080.
6) Clear **Use the same proxy server for all protocols**.
7) Click **OK** to close each screen in this dialog box.

Configuring Firefox for explicit proxy

1) In Firefox, select **Tools** > **Options** > **Advanced**, and then select the **Network** tab.
2) Select **Settings**.
3) Select **Manual proxy configuration**.
4) For **HTTP Proxy**, enter the Content Gateway IP address and specify port 8080.
5) For **SSL Proxy**, enter the Content Gateway IP address and specify port 8080.
6) Click **OK** to close each screen in this dialog box.

Transparent proxy deployment

In a transparent proxy deployment, the user's client software (typically a browser) is unaware that it is communicating with a proxy. Users request Internet content as usual, without any special client configuration, and the proxy serves their requests. The Adaptive Redirection Module (ARM) component of Content Gateway intercepts incoming packets and redirects them to the proxy. The proxy establishes a connection with the origin

server and returns requested content to the client. ARM readdresses returned content as if it came directly from the origin server. For more information, see Transparent Proxy and ARM in the Content Gateway Manager Help.

Note that in a transparent proxy deployment, **all** Internet traffic from a client goes through the proxy (not just traffic from web browsers), including:

- Traffic tunneled over HTTP and HTTPS by remote desktop applications
- Instant messaging clients
- Software updaters for Windows and anti-virus applications
- Custom internal applications

Many of these programs are not developed with proxy compatibility in mind. For a successful transparent proxy deployment, the network must be configured to allow the proxy's static bypass feature to work. See the "Static bypass rules" section of Transparent Proxy and ARM in the Content Gateway Manager Help.

Because traffic management is centralized, users cannot easily bypass the proxy.

This type of deployment requires the implementation of at least one other network device that is not required in the explicit proxy deployment. Added equipment presents compatibility issues, as all network devices must work together smoothly and efficiently. The overall system is often more complex and usually requires more network expertise to construct and maintain.

The use of a Layer 4 switch or WCCPv2-enabled router to redirect traffic in a transparent proxy deployment can provide redundancy and load distribution features for the network. These devices not only route traffic intelligently among all available servers, but can also detect whether a proxy is nonfunctional. In that case, the traffic is re-routed to other, available proxies.

Exception handling can be included in switch or router configuration. For example, requests for data from some internal, trusted sites can be allowed to bypass the proxy.

Layer 4 switch

You can implement policy-based routing (PBR) for a transparent proxy deployment with the use of a Layer 4 switch, which can be configured to redirect a request to the proxy, as follows:

1) Create an access control list (ACL) that identifies the web traffic that should be intercepted.

2) Develop a route map to define how the intercepted web traffic should be modified for redirection.

3) Apply a "redirect to proxy" policy to the switch interface.

See Transparent Proxy and ARM in the Content Gateway Manager Help for more information about the use of a Layer 4 switch.

WCCP-enabled router

Note

Content Gateway supports WCCP v2 only.

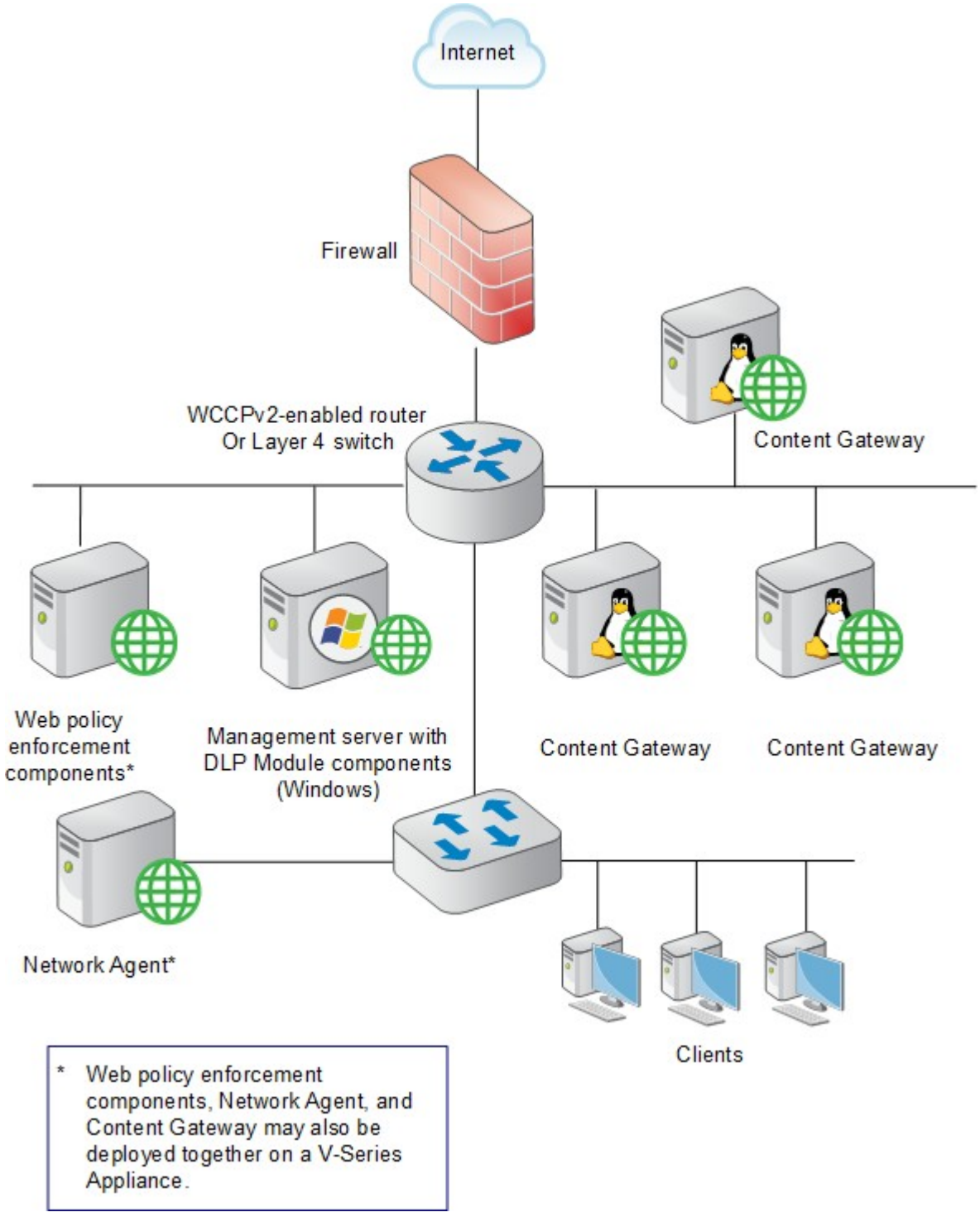
WCCP is a protocol used to route client request traffic to a specific proxy. A WCCP-enabled router can distribute client requests based on the proxy server's IP address, routing traffic to the proxy most likely to contain the requested information.

The router may use Generic Routing Encapsulation (GRE) to forward IP packets to the proxy. GRE is a tunneling protocol that allows point-to-point links between multiple traffic routing hops.

A router may also use Layer 2 (L2), which does not use GRE. As a best practice, use L2 if the router supports it. With L2 redirection, Content Gateway must be on the same subnet as the WCCP device (that is, Layer 2 adjacent).

A proxy and a router communicate via a set of WCCP “Here I am” and “I see you” messages. A proxy that does not send a “Here I am” message for 30 seconds is removed from service by the router, and client requests that would have been directed to that proxy are sent to another proxy.

The following illustration shows an example transparent proxy deployment.



A comparison of how some activities are handled in explicit and transparent proxy deployments appears in the following table:

Activity	Explicit Proxy Deployment	Transparent Proxy Deployment	Proxy Chain
Client HTTP request	Direct connection to proxy by browser to port 8080 (default)	Redirected to proxy by network device using GRE encapsulation or by rewriting the L2 destination MAC address to the proxy's address	Direct connection to parent proxy from child proxy
Exception management	Exclude site, CIDR, etc., using browser configuration settings and PAC file settings.	Static or dynamic bypass rules	Child/parent proxy configuration rules
Proxy user authentication	Proxy challenge using 407 Proxy Authentication Required code	Challenge using server-based authentication scheme (client is not aware of proxy)	Proxies in a chain may share credential information, or a single proxy in the chain can perform authentication.
Redundancy	Proxy virtual IP pool shared across multiple proxies	WCCP pool with multiple proxies	Parent/child configuration points to proxy virtual IP addresses.
Proxy management	Management clustering	Management clustering	Management clustering
Load balancers	Supported	N/A	Supported

Special Content Gateway deployment scenarios

Applies to:	In this topic

■ Forcepoint Web Security, v8.5.x	■ *Highly available web proxy*
	  ■ *Using proxy*
	  ■ *Using transparent proxy*
	■ *In a proxy chain*
	  ■ *Content Gateway is downstream*
	  ■ *Content Gateway is upstream*
	  ■ *Proxy cache hierarchy*
	  ■ *SSL chaining*

Content Gateway can be deployed in proxy clusters with failover features that contribute to high availability. The proxy can also be deployed in a chain, either with other Content Gateway proxies or third-party proxies. This section describes some examples of these deployment scenarios.

Highly available web proxy

A highly available web proxy provides continuous, reliable system operation.

Proxy high availability may be accomplished via a proxy cluster that uses various failover contingencies. Such deployments may involve either an explicit or transparent proxy configuration, load balancing, virtual IP addresses, and a variety of switching options. This section summarizes some possibilities for highly available web proxy deployments.

Using proxy

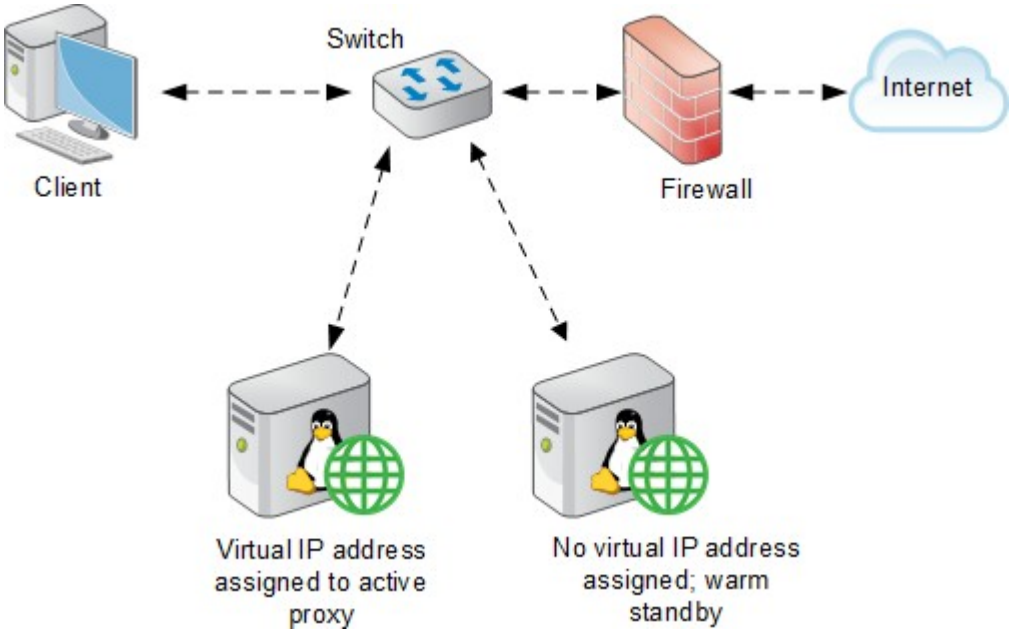
As previously mentioned for the explicit proxy deployment, clients are specifically configured to send requests directly to a proxy. The configuration can be accomplished manually, or via a PAC file or a WPAD server.

An explicit proxy deployment for high availability can benefit from the use of *virtual IP failover*. IP addresses may be assigned dynamically in a proxy cluster, so that one proxy can assume traffic-handling capabilities when another proxy fails. Content Gateway maintains a pool of virtual IP addresses that it distributes across the nodes of a cluster. If Content Gateway detects a hard node failure (such as a power supply or CPU failure), it reassigns IP addresses of the failed node to the operational nodes.

Active/Standby

In the simple case of an active/standby configuration with 2 proxies, a single virtual IP address is assigned to the virtual IP address “pool.” The virtual IP address is assigned to one proxy, which handles the network traffic that is explicitly routed to it. A second proxy, the standby, assumes the virtual IP address and handles network traffic only if the first proxy fails.

This deployment assumes the proxy machines are clustered in the same subnet, and management clustering is configured (that is, both proxies have the same configuration). Below is an example.



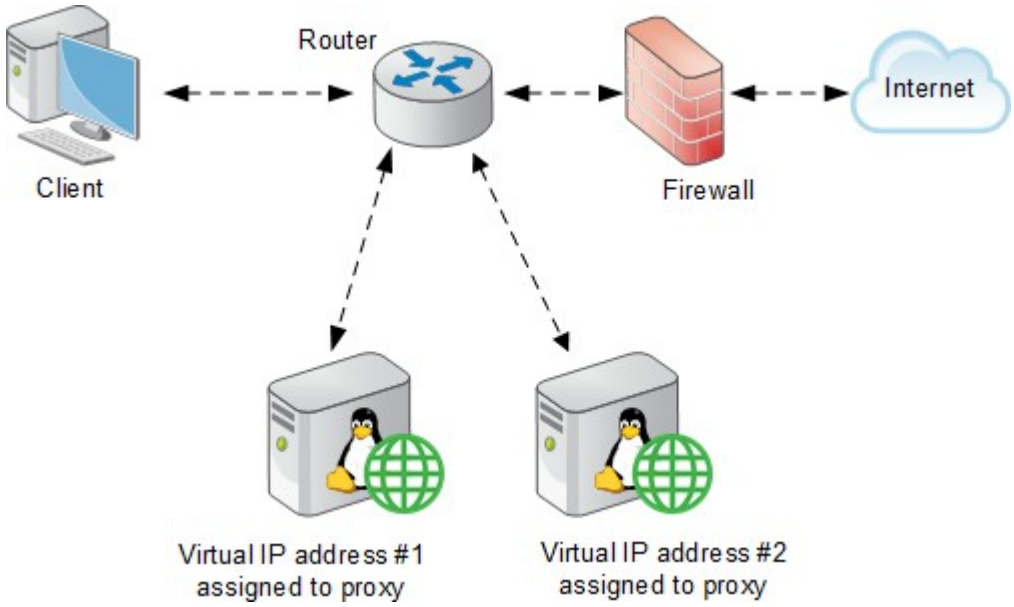
Active/Active

In an active/active configuration with 2 proxies, more than one virtual IP address is assigned to the virtual IP address pool. At any point in time, one proxy handles the network traffic that is explicitly directed to it. This deployment is scalable for larger numbers of proxies.

Clients requesting the IP address of a proxy can be crudely distributed using round robin DNS. Round robin DNS is not a true load balancing solution, because there is no way to detect load and redistribute it to a less utilized proxy. Management clustering should be configured.

An increase in the number of proxy machines makes the use of a PAC file or WPAD for specifying client configuration instructions convenient. A PAC file may be modified to adjust for proxy overloads, in a form of load balancing, and to specify website requests that can bypass the proxy.

As with the active/standby configuration, an available proxy can assume a failed proxy’s load. Below is an example.

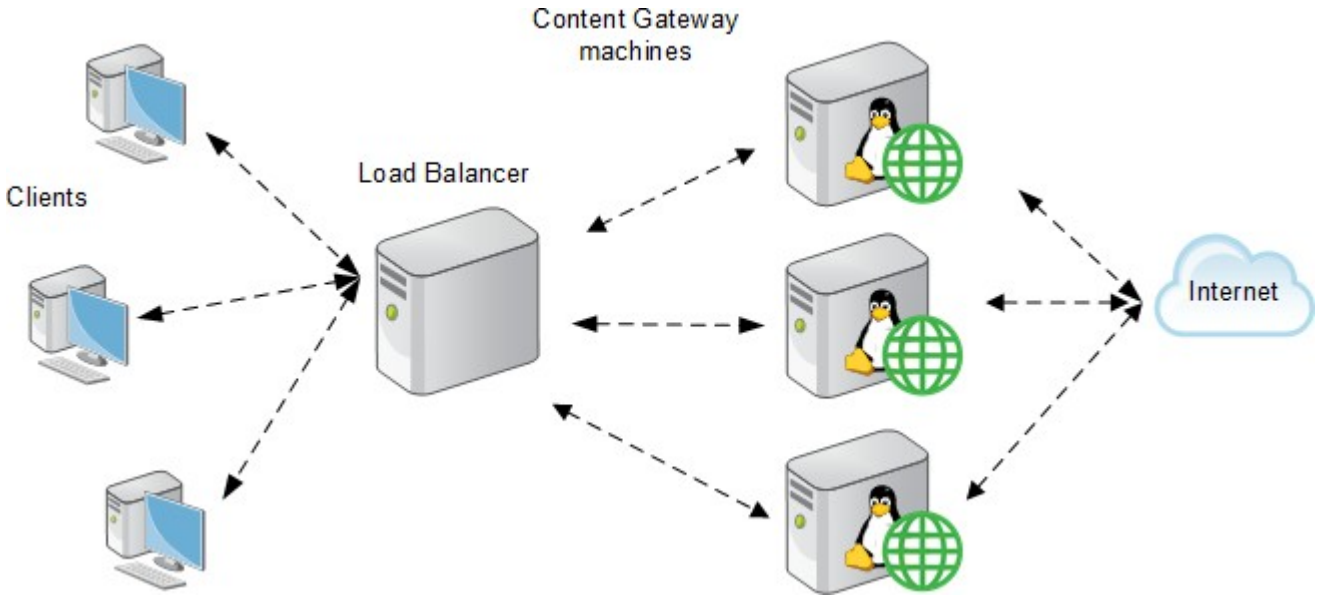


With load balancing

A load balancer is a network device that not only distributes specific client traffic to specific servers, but also periodically checks the status of a proxy to ensure it is operating properly and not overloaded. This monitoring activity is different from simple load distribution, which routes traffic but does not account for the actual traffic load on the proxy.

A load balancer can detect a proxy failure and automatically re-route that proxy's traffic to another, available proxy. The load balancer also handles virtual IP address assignments. Below is an example.

Integrated Windows Authentication is supported with a load balancer. Contact Forcepoint Technical Support for more information.



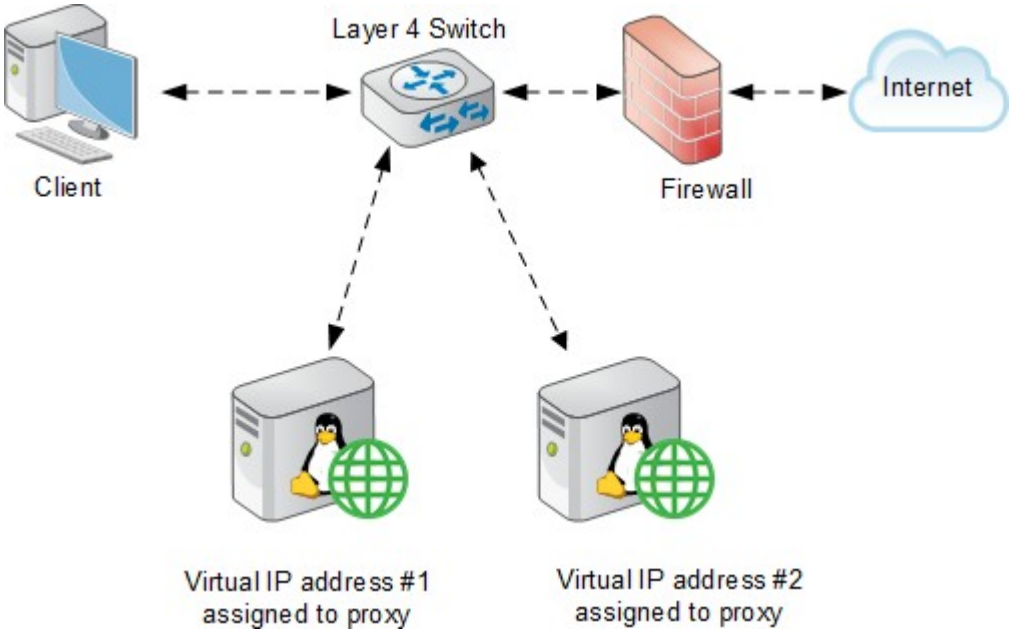
Using transparent proxy

In a transparent proxy deployment for high availability, traffic forwarding may be accomplished using a Layer 4 switch or a WCCP v2-enabled router. Routers or switches can redirect traffic to the proxy, detect a failed proxy machine and redirect its traffic to other proxies, and perform load balancing.

Using a Layer 4 switch

In one simple form of transparent proxy, a hard-coded rule is used to write a proxy's Media Access Control (MAC) address as the destination address in IP packets in order to forward traffic to that proxy. Traffic that does not include the specified proxy address for forwarding is passed directly to its destination. See below for an example.

As described for the explicit proxy, virtual IP addresses can be used in this scenario to enhance availability in case a proxy machine fails.



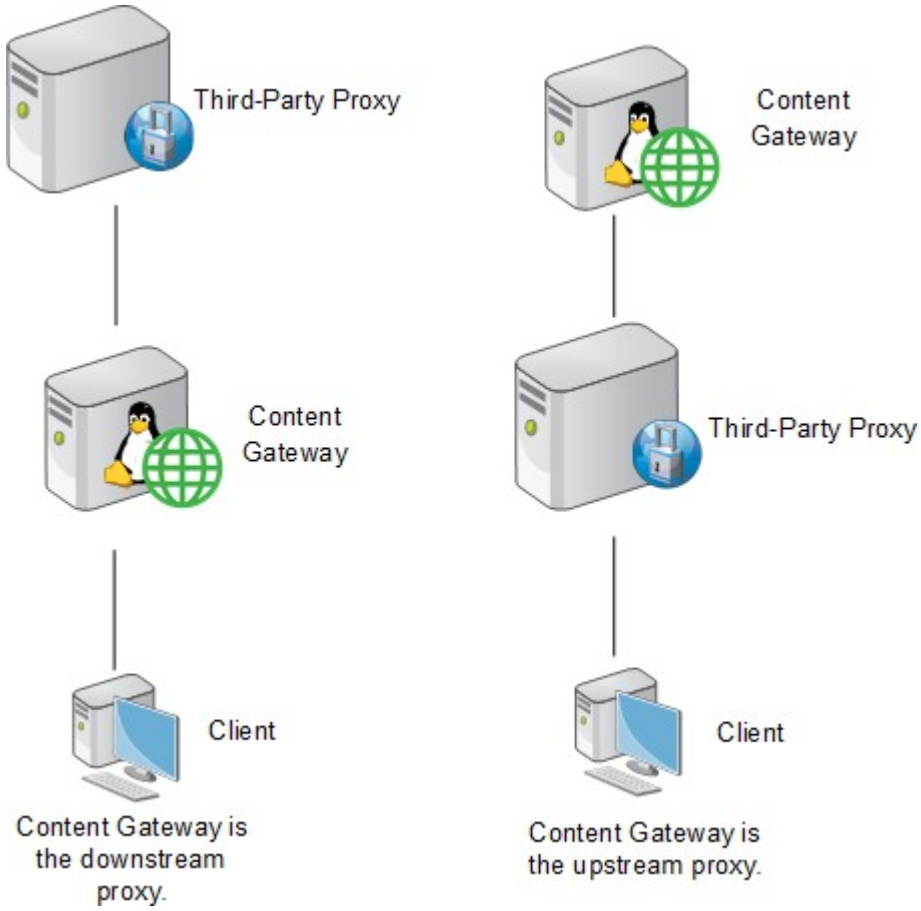
Using a WCCPv2-enabled router

WCCP is a service that is advertised to a properly configured router, allowing that router to automatically direct network traffic to a specific proxy. In this scenario, WCCP distributes client requests based on the proxy server's IP address, routing traffic to the proxy most likely to contain the requested information.

In a proxy chain

Content Gateway can be deployed in a network that contains multiple proxy machines, including one or more third-party proxies. A *proxy chain* deployment can involve different scenarios, depending on where Content Gateway is located in relation to the client. The proxy that is closest to the client is called the *downstream* proxy. Other proxies are *upstream*.

Below is a simple example of proxy chaining. On the left, Content Gateway is the downstream proxy. On the right, Content Gateway is upstream.



See *Chaining Content Gateway with other proxies* for specific instructions on using Blue Coat™ ProxySG™ or Microsoft™ Forefront™ Threat Management Gateway as the downstream proxy.

Content Gateway is downstream

A simple deployment has Content Gateway as the downstream proxy, closest to the client. In this scenario, Content Gateway security features are well positioned for maximum protection and network performance.

In this scenario, use of Content Gateway authentication to validate client credentials is preferred. You must disable authentication on the third-party proxy.

However, if the upstream third-party proxy requires authentication, you must disable authentication on Content Gateway and enable the pass-through authentication feature via an entry in the `records.config` file (in the `/WCG/config/` directory by default). An example `records.config` entry is as follows:

```
CONFIG proxy.config.http.forward.proxy_auth_to_parent INT 1
```

You can then use a transparent identification agent (for example, Logon Agent) to facilitate client identification.

Content Gateway can additionally send the client IP address to the upstream third- party proxy using the X-Forwarded-For HTTP header. This is set in the Content Gateway manager (**Configure** > **Protocols** > **HTTP** > **Privacy** > **Insert Headers** section).

The X-Forwarded-For HTTP header is the *de facto* standard for identifying the originating IP address of a client connecting through an HTTP proxy. Some proxies do not utilize the X-Forwarded-For header.

For information about installing and deploying transparent identification agents, see *Deploying transparent identification agents* and *Installing web protection components*.

Content Gateway is upstream

When Content Gateway is the upstream proxy, the downstream third-party proxy can perform authentication and send client IP and username information in the HTTP request headers. Content Gateway authentication must be disabled.

In this scenario, caching must be disabled on the third-party proxy. Allowing the third- party proxy to cache web content effectively bypasses Content Gateway's inspection capabilities for any website that was successfully accessed previously from the third- party proxy.

For an upstream Content Gateway to identify users:

- Enable authentication on the third-party proxy.
- Designate Content Gateway as the parent proxy in the third-party proxy's configuration.
- Set the **Read authentication from child proxy** option in the Content Gateway manager (**Configure** > **My Proxy** > **Basic** > **Authentication**). This option allows Content Gateway to read the X-Forwarded-For and X-Authenticated-User HTTP headers. The downstream third-party proxy passes the client IP address via the X-Forwarded-For header and the user domain and username in the X-Authenticated-User header.
  If the third-party proxy can send the X-Forwarded-For header but not the X-Authenticated-User header, the following step is also required:
- Deploy a transparent identification agent to facilitate client identification by Content Gateway. See *Deploying transparent identification agents*, and *Installing web protection components*.

Content Gateway can be configured to read authentication from the following proxies in the downstream position:

Blue Coat ProxySG - 210 and later

Microsoft Forefront TMG - MBE and later

For detailed configuration instructions for Blue Coat ProxySG and Microsoft TMG server, see *Chaining Content Gateway with other proxies*.

Proxy cache hierarchy

Another form of proxy chain is a flexible proxy cache hierarchy, in which Internet requests not fulfilled in one proxy can be routed to other regional proxies, taking advantage of their contents and proximity. For example, a cache hierarchy can be created as a small set of caches for a company department or a group of company workers in a specific geographic area.

In a hierarchy of proxy servers, Content Gateway can act either as a parent or child cache, either to other Content Gateway systems or to other caching products. Having multiple parent caches in a cache hierarchy is an example of *parent failover*, in which a parent cache can take over if another parent has stopped communicating.

As mentioned earlier, the increasing prevalence of dynamic, user-generated web content reduces the need for Content Gateway caching capabilities.

See Hierarchical Caching in the Content Gateway Manager Help.

SSL chaining

Routing SSL traffic in a proxy chain involves the same parent proxy configuration settings used with other proxy-chained traffic. You identify the ports on which HTTPS requests should be decrypted and policy applied when SSL is enabled in the **Protocols** > **HTTP** > **HTTPS Ports** option in the Configure tab. Parent proxy rules established in `parent.config` for HTTPS traffic (destination port 443) determine the next proxy in the chain for that traffic.

Enable the Configure tab **Content Routing** > **Hierarchies** > **HTTPS Requests Bypass Parent** option to disable SSL traffic chaining when all other traffic is chained.

If you want to exclude SSL traffic from the parent proxy and tunnel the traffic directly to the origin server, enable the **Tunnel Requests Bypass Parent** option in the Configure tab **Content Routing** > **Hierarchies**. This option can be used for any tunneled traffic.

Related tasks

Installing web protection components on page 157

Related reference
Chaining Content Gateway with other proxies on page 98
Deploying transparent identification agents on page 53

Chaining Content Gateway with other proxies

Applies to:	In this topic
■ Forcepoint Web Security, v8.5.x	■ *In a proxy chain* ■ *Microsoft Forefront Threat Management Gateway (TMG)*

Blue Coat ProxySG

You can configure the Blue Coat proxy to send X-Forwarded-For and X-Authenticated-User headers for Content Gateway to read either by manually editing a policy text file or defining the policy in a Blue Coat graphical interface called Visual Policy Manager.

Note that for Blue Coat to service HTTPS requests properly with the following setup, you must have a Blue Coat SSL license and hardware card.

Editing the local policy file

In the Blue Coat Management Console Configuration tab, click **Policy** in the left column and select **Policy Files**. Enter the following code in the current policy text file, using an Install Policy option:

```
<Proxy>
action.Add[header name for authenticated user](yes)

define action dd[header name for authenticated user]
set(request.x_header.X-Authenticated-User, "WinNT://$(user.domain)/$(user.name)")
end action Add[header name for authenticated user]

action.Add[header name for client IP](yes)

define action dd[header name for client IP]
set(request.x_header.X-Forwarded-For,$(x-client-address))
end action Add[header name for client IP]
```

Using the Blue Coat graphical Visual Policy Manager

Before you configure the Blue Coat header policy, ensure that NTLM authentication is specified in the Blue Coat Visual Policy Manager (**Authentication** > **Windows SSO**). Set Content Gateway as the forwarding host (in the Blue Coat Management Console Configuration tab, **Forwarding** > **Forwarding Hosts**).

In the Blue Coat Management Console Configuration tab, click **Policy**and select **Visual Policy Manager**. Click **Launch** and configure the header policy as follows:

1) In the Policy menu, select **Add Web Access Layer** and enter an appropriate policy name in the **Add New Layer** dialog box.

2) Select the **Web Access Layer** tab that is created.

3) The Source, Destination, Service, and Time column entries should be **Any** (the default).

4) Right-click the area in the Action column, and select **Set**.

5) Click **New** in the Set Action Object dialog box and select **Control Request Header** from the menu.

6) In the Add Control Request Header Object dialog box, enter a name for the client IP Action object in the Name entry field.

7) Enter **X-Forwarded-For** in the Header Name entry field.

8) Select the **Set value** radio button and enter the following value:

```
$(x-client-address)
```

9) Click **OK**.

10) Click **New** and select **Control Request Header** again.

11) In the Add Control Request Header Object dialog box, enter a name for the authenticated user information Action object in the Name entry field.

12) Enter **X-Authenticated-User** in the Header Name entry field.

13) Select the **Set value** radio button and enter the following value:

```
WinNT://$(user.domain)/$(user.name)
```

14) Click **OK**

15) Click **New** and select **Combined Action Object** from the menu.

16) In the Add Combined Action Object dialog box, enter a name for a proxy chain header in the Name entry field.

17) In the left pane, select the previously created control request headers and click **Add**.

18) Select the combined action item in the Set Action Object dialog box and click **OK**.

19) Click **Install Policy** in the Blue Coat Visual Policy Manager.

Microsoft Forefront Threat Management Gateway (TMG)

Microsoft Forefront TMG can be used as a downstream proxy from Content Gateway via a plug-in from Forcepoint. This plug-in allows Content Gateway to read the X-Forwarded-For and X-Authenticated-User headers sent by the downstream Forefront TMG.

The `Websense-AuthForward.TMG_Plugin-64.zip` file is available on the Downloads page of your forcepoint.com account.

1) Navigate to **forcepoint.com** and click **My Account** to log in.

2) Select the **Downloads** tab.

3) Select **Forcepoint Web Security** from the **Product** drop-down list.

4) In the list, expand **TMG 64-bit plugin...** to see the download details. Click the **download** link to start the download.

Install a plug-in:

1) Unzip the package and copy the following files to the Forefront TMG installation directory:
   a) Websense-AuthForward.dll
   b) msvcp110.dll
   c) msvcr110.dll

2) Register the plug-in with the system. Open a Windows command prompt and change directory to the Forefront TMG installation directory.
   From the command prompt, type:

```
regsvr32 Websense-AuthForward.dll
```

3) Verify the plug-in was registered in the Forefront TMG management user interface (**Start** > **Programs** > **Microsoft Forefront TMG** > **Microsoft Forefront TMG Management**) . In the System section, select **Add-ins**, then click the **Web-filter** tab. The **WsAuthForward** plug-in should be listed.

To uninstall the plug-in, in Forefront TMG installation directory run the following command in a Windows command prompt.

```
regsvr32 /u Websense-AuthForward.dll
```

Installing Forcepoint Web Security components to work with Content Gateway

Applies to:

- Forcepoint Web Security, v8.5.x

If you are installing Content Gateway as part of a software-based deployment of Forcepoint Web Security, you must install the core policy and management components prior to installing Content Gateway. For instructions, see:

- Installation Instructions: Forcepoint Web Security
- *Installing via the Forcepoint Web Security or Forcepoint URL Filtering All option*

During installation of filtering components:

- On the *Integration Option Screen*, be sure to select **Install Web Security to connect to Content Gateway**.

- Note the IP address or addresses of Policy Server and Filtering Service. You will need them when installing Content Gateway.

Related concepts

Integration Option Screen on page 164

Related reference

Installing via the Forcepoint Web Security or Forcepoint URL Filtering All option on page 129

Chapter 6

Planning Forcepoint DLP Deployment

Before you begin setting up your Forcepoint DLP system, it is important to analyze your existing resources and define how security should be implemented to optimally benefit your specific organization.

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The Forcepoint DLP Deployment Guide helps you plan your deployment, integrate it with existing infrastructure such as shared drives, user directory servers, and Exchange servers, and design for scalability.

Chapter 7

Deploying Email Protection Solutions

Contents

Applies to:

- Forcepoint Email Security, v8.5.x
- Forcepoint Appliances, v8.5.x

Forcepoint Email Security provides maximum protection for email systems to prevent malicious threats from entering an organization's network. Forcepoint Email Security provides comprehensive security hosted on a Forcepoint physical or virtual appliance, or in a Microsoft Azure cloud environment. Email system management functions reside on a separate Windows server in the Forcepoint Security Manager.

Forcepoint Email Security may be deployed on the following appliances:

- Forcepoint V Series
- Forcepoint X Series chassis security blade
- Virtual appliance
- Microsoft Azure virtual appliance

The virtual appliance deployment uses a VMware platform (ESXi v6.x). The appliance image is available for download from the Forcepoint My Account page in an open virtualization format (OVF) package. A virtual appliance may not be clustered with a hardware appliance. See the Forcepoint Appliances Getting Started Guide for complete information about setting up and configuring a Forcepoint appliance.

Each email message is processed by a robust set of analytics to prevent malicious threats from entering a network. Custom content filters allow Forcepoint Email Security to analyze messages based on administrator-specified message attribute conditions. Commercial bulk email analysis can determine whether a message has been sent from a third-party bulk email management company or directly from a business. Inbound, outbound, and internal email policies can be applied to user-defined sets of senders and recipients.

The option to deploy in Microsoft Azure was added in version 8.5. See the Release Notes for Forcepoint Email Security in Azure for more information. In version 8.5.3 and 8.5.4, you have several options for a Microsoft Azure deployment:

1) Only Forcepoint Email Security components reside in the cloud; email system management functions remain on-premises. Deploying Forcepoint Email Security in Azure requires an active Azure account and a virtual network in Azure with site-to-site connectivity to on-premises resources. This is the only option for version 8.5.

2) Both Email Security and Security Manager reside in the cloud, with no functions on-premises. Deploying Forcepoint Email Security and Forcepoint Security Manager in Azure requires an active Azure account. This option is available for versions 8.5.3 and 8.5.4.

3) Some Forcepoint Email Security appliances reside in the cloud and some are installed on-premises. Forcepoint Security Manager can either be deployed in Azure or on-premises. Deployment requires an active Azure account

and a virtual network in Azure with site-to-site connectivity to on-premises resources. This option is available for versions 8.5.3 and 8.5.4.
For more information as well as installation and configuration instructions, see Installing Forcepoint Email Security in Microsoft Azure.

Including the Forcepoint Email Security Hybrid Module in your deployment adds support for an email hybrid service pre-filtering capability in the cloud, which analyzes the characteristics of incoming email against a Forcepoint database of known threats.

Enhance your security by adding a set of cloud-based functions to your subscription:

- URL sandbox
- Advanced file analysis
- Phishing education

The URL sandbox function provides real-time analysis of uncategorized URLs that are embedded in inbound mail.

The advanced file analysis capability may be deployed in one of two ways:

- Forcepoint Advanced Malware Detection - Cloud
- Forcepoint Advanced Malware Detection - On-Premises

Either advanced file analysis deployment inspects email attachment file types that commonly contain security threats (for example, .exe, .pdf, .xlsx, .docx, .ppt, and archive files). See Advanced file analysis in *Forcepoint Email Security Administrator Help* for information.

Phishing education provides cloud-based analysis of an inbound message for phishing email characteristics. Options for handling suspected phishing mail include blocking the delivery or replacing the mail with a phishing education message. See Phishing detection and education in *Forcepoint Email Security Administrator Help* for details.

Add the Forcepoint Email Security Encryption Module to your subscription to use Forcepoint advanced email encryption capabilities, in conjunction with the email hybrid service.

Integration with Forcepoint DLP provides valuable data loss prevention (DLP) features to protect an organization's most sensitive data and facilitate message encryption. Policies configured in the Data Security module of the Security Manager can detect the presence of confidential company data and block the unauthorized transmission of that data via email. Forcepoint DLP can also determine whether an outbound message should be encrypted and pass the message to an encryption server.

If your network includes Forcepoint Web Security or Forcepoint URL Filtering, you can also use its URL analysis function. Forcepoint Email Security queries the Forcepoint URL category master database and determines the risk level of a URL found in an email message.

Logging and reporting capabilities allow an organization to view system and message status and generate reports of system and email traffic activity.

A Personal Email Manager facility allows authorized end users to release email messages that an email policy has blocked but that may be safe to deliver. End users can maintain personal Always Block and Always Permit lists of email addresses to simplify message delivery. User account management capabilities allow multiple email account control and the delegation of email account management to other individuals.

The Secure Message Delivery feature lets you configure delivery options for a secure portal in which your organization's customers may view, send, and manage encrypted email. For example, you may wish to include sensitive personal financial information in a message to a client. The portal provides a secure location for the transmission of this data, while your sensitive information is maintained on your secure server.

System requirements and deployment options are discussed in the following topics:

- *System requirements*
- *Single-appliance Forcepoint Email Security deployments*
- *Multiple-appliance Forcepoint Email Security deployments*

See the following topics for Forcepoint Email Security installation information:

- Installing email protection solutions
- Installing Forcepoint Email Security in Microsoft Azure
- Installing the Email Security module of the Forcepoint Security Manager
- Appliances Getting Started Guide
- Appliances Command Line Interface (CLI) Guide

See the following topics for email protection solution upgrade information:

- *Upgrading Email Protection Solutions*
- *Upgrading the management server*

Related concepts
Upgrading the management server on page 254

Related reference
Upgrading Email Protection Solutions on page 307

System requirements

Applies to:

- Forcepoint Email Security, v8.5.x

To view complete hardware, software, and web browser requirements for Forcepoint Email Security, see *System requirements for this version*.

Every Forcepoint Email Security deployment includes the following components at a minimum:

In the DMZ

- A Forcepoint appliance (V Series, X Series blade, or Virtual Appliance), which includes the core email protection functions, along with the Personal Email Manager and Secure Messaging end-user facilities.

Email traffic volume in your network may determine which type of appliance you use and how many appliances your deployment needs.

In the internal LAN

- Forcepoint Security Manager with both Email Security and Data Security modules installed on a Windows Server™ 2008 R2 SP1, 2012, 2012 R2, 2016, or 2019 machine.
  - Windows 2008 R2 is not supported for version 8.5.3 or 8.5.4.
- Email Log Server
- Email Log Database (Microsoft™ SQL Server™ 2008, 2008 R2, 2012, 2014, 2016, or 2017, including Express)
  - SQL Server 2008 R2 is not supported for version 8.5.3 or 8.5.4
- Mail server
- End-user machines: mail clients used by end user

Note

All email protection components must be synchronized by date and time for proper system communication.

The network DMZ contains the devices that have direct contact with the Internet. This zone is a buffer between the Internet and the internal LAN. In our examples, the appliance and any router, switch, or load balancer adjacent to the firewall are located in the DMZ.

Forcepoint appliances

The Forcepoint V Series, X Series, and Virtual Appliances provide the majority of email protection functions. Incoming email flows from the Forcepoint Email Security Hybrid Module (if purchased and enabled) to the Forcepoint appliance and to the mail server. The Forcepoint appliance also provides the Personal Email Manager and Secure Messaging end-user facilities.

Forcepoint Email Security can occupy individual blade servers on an X Series appliance. The X Series chassis may include a combination of Email Security and Web Security blade servers.

See the Forcepoint Appliances Getting Started Guide for detailed hardware specifications.

Forcepoint management server

The Forcepoint management server hosts the Forcepoint Security Manager. This machine includes Forcepoint Management Infrastructure and any installed Forcepoint management modules. In a Forcepoint Email Security deployment, the Forcepoint management server includes both the Email Security and Data Security modules.

Email Log Server

The Forcepoint management server often includes the Email Log Server component, although this component can also be installed on a separate machine in an on-premises deployment. If the Forcepoint management server is installed in Microsoft Azure, the Log Server must reside in the same machine. The Log Server passes message data to the SQL Server reporting database (Email Log Database) for use in generating dashboard charts and reports, messages, and Message Log data.

During installation, a user configures certain aspects of Log Server operation, including how Log Server interacts with the Email Security module. These settings can be changed when needed via the Email Log Server Configuration utility. Other details about Log Server operation are configured in this utility as well. The utility is installed on the same machine as Log Server.

Email Log Database (Microsoft SQL Server)

Microsoft SQL Server handles the system and message log database and stores some Email Security module configuration settings. SQL Server may be installed on the Forcepoint management server or on a dedicated server. For optimal performance, Forcepoint recommends that a full SQL Server be installed on a separate machine. (SQL Server Express, which can be installed as part of the Forcepoint Security Manager installation with certain versions, is recommended only for evaluation purposes.) For information about database systems in Forcepoint products, see Administering Forcepoint Databases.

Personal Email Manager

The email appliance is the portal for Personal Email Manager end users who are authorized to manage their own blocked mail. Personal Email Manager end-user options are configured in the Security Manager Email Security module interface (**Settings** > **Personal Email**). A Personal Email Manager administrator can determine:

- Which end users can access the Personal Email Manager utility and which actions, if any, those users are allowed to perform on blocked messages
- What the blocked email notification message contains
- Which end users are allowed to manage personal Always Block and Always Permit lists
- Whether a user can manage multiple email accounts
- Whether a user can delegate email account management responsibilities to another individual

Secure Messaging portal

The email appliance also provides the Secure Messaging end-user portal to allow an organization to maintain a secure area for its customers to view and manage messages that contain sensitive data. Customers can view received messages and reply to or forward a received message in this portal.

Forcepoint Email Security in Microsoft Azure

Forcepoint Email Security can be deployed in a Microsoft Azure public cloud environment. See Installing Forcepoint Email Security in Microsoft Azure. The following is required for Azure deployment:

- A Microsoft Azure account (activated)
- Microsoft Office 365 with Outlook
- A virtual network (minimum supported size: /16) and subnet (minimum supported size: /24) in Azure with connectivity to on-premises resources through a site-to-site VPN.
- Resources installed on-premises: SQL Server and Forcepoint Security Manager

The preceding two items are only necessary if you are installing Forcepoint Email Security in Azure with Forcepoint Security Manager remaining on-premises. If you are installing both Email Security and Security Manager together in Azure, these two items are not needed.

Related reference

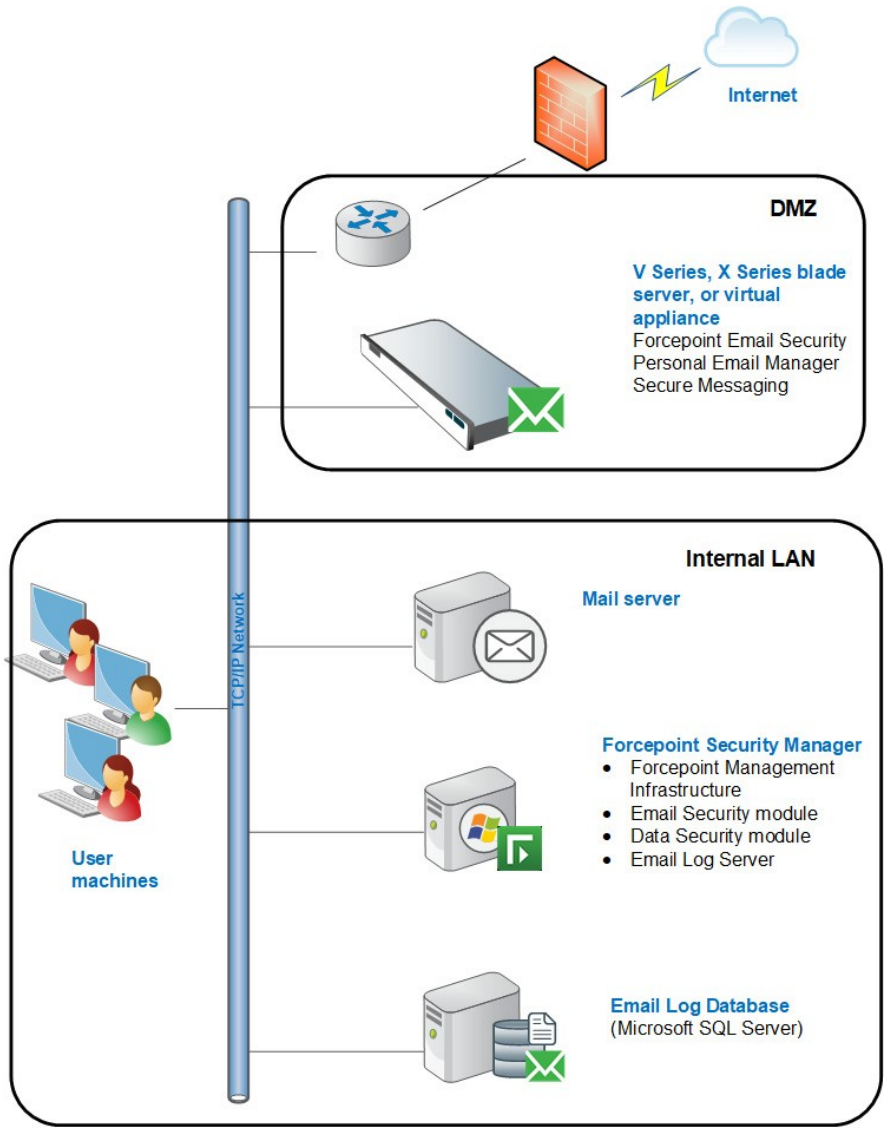
System requirements for this version on page 9

Single-appliance Forcepoint Email Security deployments

Applies to:

- Forcepoint Email Security, v8.5.x

Single email appliance



A simple email protection deployment uses a single appliance or X10G blade server. In this installation, all email analysis occurs in the on-premises appliance component using a robust collection of threat detection tools (**Main** > **Policy Management** > **Filters**).

The Personal Email Manager facility on the appliance allows an organization's end users to manage blocked messages. The Secure Messaging portal lets an organization's customers view and manage email that contains sensitive data.

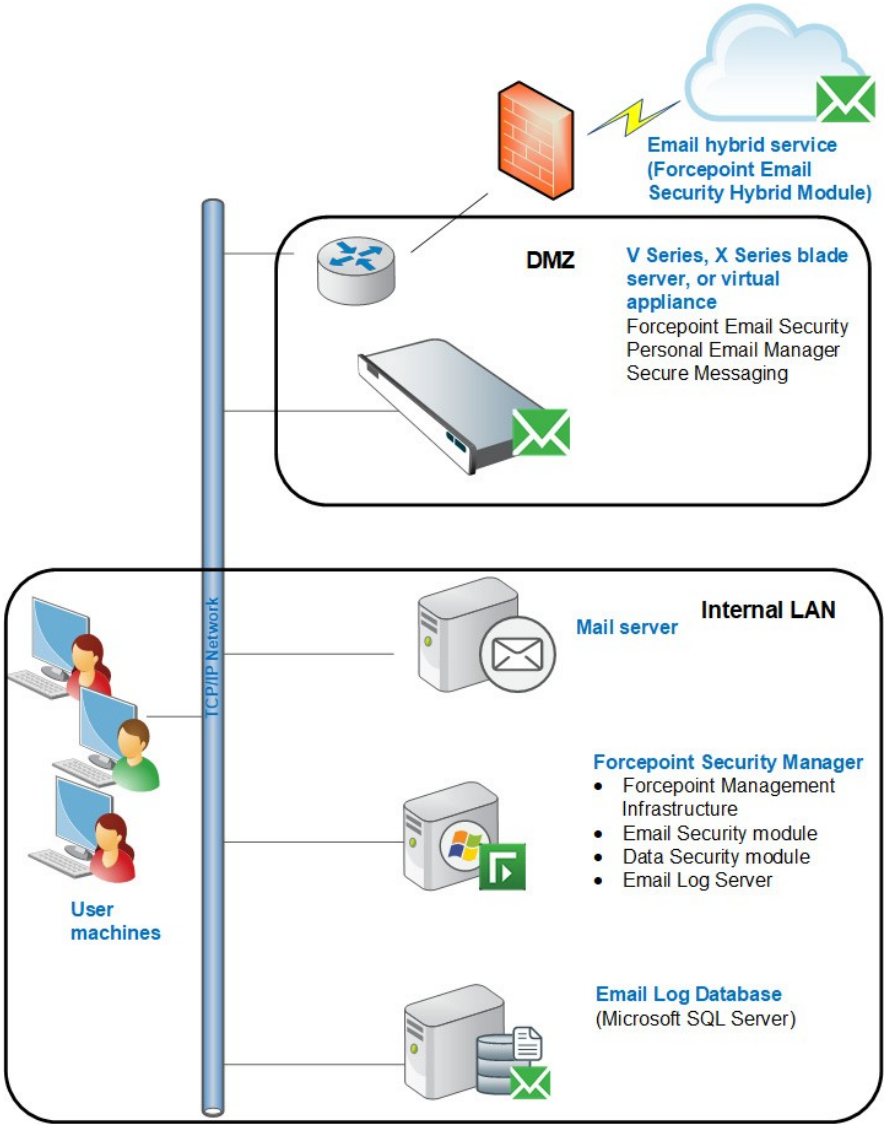
In this scenario, the Email Log Server is installed on the same machine as the Forcepoint Security Manager. It can be installed on a separate machine if desired.

Data loss prevention (DLP) policies analyze email to ensure acceptable use policies are enforced and sensitive company data is not lost. An email DLP policy can also facilitate outbound message encryption. DLP policies are enabled in the Security Manager Email Security module (**Main** > **Policy Management** > **Policies**) but are defined and configured in the Data Security module.

See the Forcepoint DLP Administrator Help for details about DLP policy settings. See the following *Forcepoint Email Security Administrator Help* topics for information about email filter and policy tools:

- Creating and configuring email filters
- Creating and configuring email policies

Single email appliance with Email Security Hybrid Module



This simple deployment uses a single appliance or X10G blade server. Forcepoint Email Security with the Email Security Hybrid Module offers a comprehensive email protection solution that combines the on-premises functions described earlier with hybrid (in-the-cloud) email analysis to manage an organization's email traffic.

The Forcepoint Email Security Hybrid Module provides an extra layer of analysis, stopping a variety of email-borne threats before they reach the network, potentially reducing email bandwidth and storage requirements. Together with the Forcepoint Email Security Encryption Module, the Email Security Hybrid Module facilitates the transfer of outbound email to an encryption server before delivery to its recipient.

The email hybrid service prevents malicious email traffic from entering a company's network by:

- Dropping a connection request based on the reputation of the IP address of the request
- Comparing the characteristics of inbound email against a Forcepoint database of known malware, and blocking any message that matches a database entry

The hybrid service may also include the results of its analysis as additional header information in email that it allows into the email protection system. This header information includes a threat detection "score," which is then used to determine message disposition by the on-premises email protection system. This function can enhance email system performance.

Your subscription must include the Email Security Hybrid Module, and the email hybrid service must be enabled and properly registered before hybrid service analysis can begin. Register for the hybrid service in the Email Security module of the Security Manager (**Settings** > **Hybrid Service** > **Hybrid Configuration**).

The Email Security Hybrid Service Log contains records of the email messages that are blocked by the email hybrid service. After the hybrid service is registered and enabled, users can view the log at **Main** > **Status** > **Logs** by clicking the Email Hybrid Service tab.

See the *Forcepoint Email Security Administrator Help* for details on all email hybrid service options:

- Registering the Email Hybrid Module
- Configuring the Email Hybrid Service Log
- Viewing the Email Hybrid Service Log

Multiple-appliance Forcepoint Email Security deployments

Applies to:

- Forcepoint Email Security, v8.5.x

Multiple-appliance deployments can be implemented when message volume warrants having greater processing capacity. When the deployed appliances are all in standalone mode, the appliances can be a mix of V Series machines and virtual appliances. An appliance cluster usually cannot contain a mix of appliance platforms.

An X Series modular chassis may include multiple blade servers running Forcepoint Email Security.

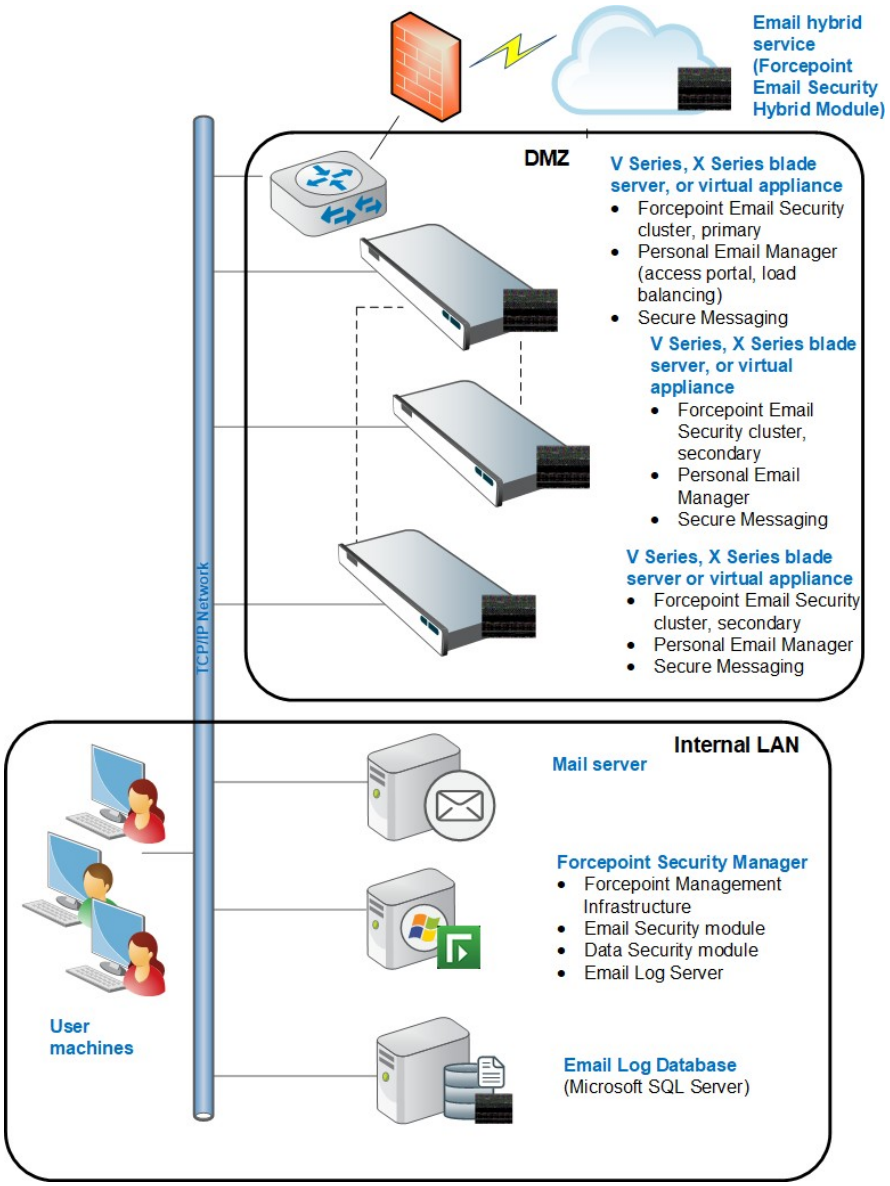
Email appliance cluster with Email Security Hybrid Module

Multiple V Series appliances are configured in a cluster for this deployment scenario. You may also consider multiple virtual appliances or X10G blade servers for this scenario. This email protection environment includes the Email Security Hybrid Module in-the-cloud analysis. See *Single email appliance with Email Security Hybrid Module*, for information about the email hybrid service.

You may want to use a third-party load balancer with an appliance cluster, to distribute email traffic among your appliances. Appliances in a cluster all have the same configuration settings, which can streamline a load balancing implementation.

Personal Email Manager traffic load balancing may be accomplished via cluster configuration. After a cluster is created, designate the Personal Email Manager access point on the page **Settings** > **Personal Email** > **Notification Message**, in the Personal Email Manager Portal section. Personal Email Manager traffic is routed to this designated IP address. This appliance then passes the traffic on to other appliances in the cluster via the round robin forwarding mechanism.

To create a cluster, add an appliance to the email appliances list on the page **Settings** > **General** > **Email Appliances**, then configure these appliances in a cluster on the page **Settings** > **General** > **Cluster Mode**. See Configuring an appliance cluster in the *Forcepoint Email Security Administrator Help* for details.



A primary appliance in a cluster may have up to seven secondary (or auxiliary) appliances. Configuration settings for any cluster appliance are managed only on the primary appliance Email Appliances page (**Settings** > **General** > **Email Appliances**).

Cluster appliances must all be running in the same security mode. The Forcepoint Security Manager and all cluster appliance versions must all match for cluster communication to work properly.

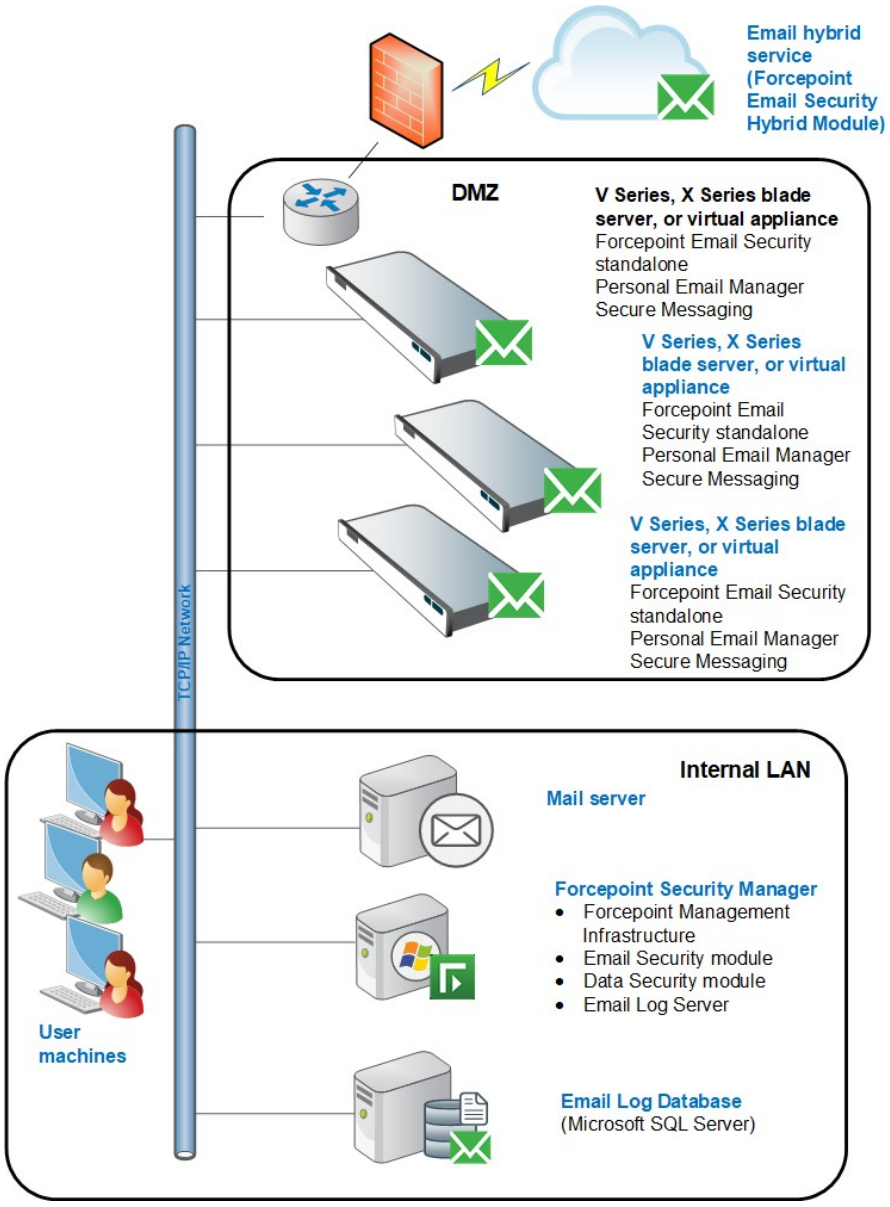
In order to protect the messages stored in the email message queues, appliances added to a cluster must have the same message queue configuration as the other cluster appliances. For example, an administrator-created queue on appliance B must be configured on primary cluster appliance A before appliance B is added to the cluster. Message queue records may be lost if this step is not performed before cluster creation.

Multiple standalone email appliances

A multiple standalone V Series or virtual appliance or X Series blade server deployment might be useful if each appliance must have different configuration settings. Two standalone scenarios are described in this section:

- *Using domain-based routing*
- *Using DNS round robin*

These environments include the Forcepoint Email Security Hybrid Module in-the-cloud filtering. See *Single email appliance with Email Security Hybrid Module*, for information about the email hybrid service.



Using domain-based routing

You can configure domain-based delivery routes so that messages sent to recipients in specified domains are delivered to a particular appliance. Configuring a delivery preference for each SMTP server facilitates message routing.

Configure the domain groups for which you want to define delivery routes on the page **Settings** > **Users** > **Domain Groups** > **Add Domain Groups**. See the *Administrator Help* for Forcepoint Email Security for information about adding or editing domain groups:

- Managing domain and IP address groups
- Configuring delivery routes

To set up a domain-based delivery route on the page **Settings** > **Inbound/Outbound** > **Mail Routing**:

1) From the section Domain-based Routes, click **Add**. The Add Domain-based Route page displays.

2) In the field **Name**, enter a name for your route

3) From the **Route order** drop-down list, select a route order to determine the route's scanning order.

4) From the **Domain group** drop-down list, select a destination domain from the pre-defined domains. The default is Protected Domain. Information about the selected domain group appears in the Domain details box.
To add a new domain group to the list, navigate to **Settings** > **Users** > **Domain Groups** and click **Add**.

   To edit your selected domain group, click **Edit** to open the Edit Domain Group page.

   Important

   The Protected Domain group defined on the page **Settings** > **Users** > **Domain Groups** should not be used to configure email delivery routes if you need to define domain-based delivery routes via multiple SMTP servers.

   Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

5) Select the **SMTP server IP address** delivery option to open the SMTP Server List:

   a) Click **Add** to open the Add SMTP Server dialog box.

   b) Enter the SMTP server IP address or hostname and port.

   c) Mark the **Enable MX lookup** check box to enable the MX lookup function.

   Important

   If you entered an IP address in the previous step, the MX lookup option is not available.

   If you entered a hostname in the previous step, this option is available.

   - Mark the **Enable MX lookup** check box for message delivery based on the hostname MX record.
   - If you do not mark this check box, message delivery is based on the hostname A record.

   d) Enter a preference number for this server (from 1–65535; default value is 5).
   If a single route has multiple defined server addresses, mail delivery is attempted in the order of server preference. When multiple routes have the same preference, round robin delivery is used. You may enter no more than 16 addresses in the SMTP Server List.

6) Select any desired security delivery options.

   a) Select **Use Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.

   b) Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

Using DNS round robin

Email traffic distribution among multiple standalone appliances can be accomplished by using the domain name system (DNS) round robin method for distributing load.

With the email hybrid service configured and running, set up the round robin system as follows:

1) Enter the SMTP server domain in the Delivery Route page of the email hybrid service configuration wizard used for registering the email protection system with the email hybrid service (**Settings** > **Hybrid Service** > **Hybrid Configuration**).

2) Register the IP addresses of the appliances you want subject to the round robin method in the SMTP domain.

If email hybrid service is not enabled, you need to modify your MX records to allow round robin load balancing. Ask your DNS manager (usually your Internet service provider) to replace your current MX records with new ones for load balancing that have a preference value equal to your current records.

Related reference

Single-appliance Forcepoint Email Security deployments on page 109

Chapter 8

Installing Forcepoint Security Solutions

Contents

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Note

- Forcepoint DLP v8.9 and later is supported with Forcepoint Web and Email Security v8.5.5.
- Forcepoint DLP v8.7.1 and later is supported with Forcepoint Web and Email Security v8.5.4.
- Forcepoint DLP v8.6 and v8.7 are supported with Forcepoint Web and Email Security v8.5.3.
- Forcepoint DLP v8.5.1 is supported with Forcepoint Web and Email Security v8.5.0.
- Forcepoint DLP v8.5.0 and v8.5.2 are stand-alone versions of that product and cannot be integrated with other Forcepoint products.

If you have more than one on-premises Forcepoint security solution, use the sections below to find the appropriate set of installation instructions.

All Forcepoint Security Solutions

If you are combining on-premises web, data, and email solutions, see the Forcepoint Security Solutions Installation Guide. This document guides you through:

- Preparing for deployment
- Installing the Forcepoint Web Security policy source and the Forcepoint management server
- Installing further recommended Forcepoint Web Security, Forcepoint DLP, and Forcepoint Email Security components
- Initial web, data, and email configuration

After completing those steps, see the Forcepoint DLP Installation Guide for instructions on installing additional components, like the protector and agents.

Forcepoint Web Security and Forcepoint DLP

If you are combining Forcepoint Web Security and Forcepoint DLP, in most cases, the best process is to first complete the steps in Installation Instructions: Forcepoint Web Security. This document guides you through installation of:

- All Forcepoint Web Security components
- Web Security Hybrid Module components
- Web Security DLP Module components, including Forcepoint DLP management components

After completing those steps, see the Forcepoint DLP Installation Guide for instructions on installing additional components, like the protector and agents.

Forcepoint Web Security and Forcepoint Email Security

If you are combining Forcepoint Web Security and Forcepoint Email Security, in most cases, the best process is to follow the steps in the Forcepoint Security Solutions Installation Guide. This document guides you through installation of:

- All Forcepoint Web Security, Web Security Hybrid Module, and Web Security DLP Module components
- All Forcepoint Email Security components
- All Forcepoint DLP components (which enables the Web Security DLP Module, if purchased, and the Email Security DLP Module)

Forcepoint Email Security and Forcepoint DLP

Forcepoint Email Security and Forcepoint DLP should be installed together to take full advantage of the Email Security DLP Module. The best installation process is to follow the steps in the Forcepoint Email Security Installation Guide. This document guides you through installation of:

- Forcepoint Email Security components
- Forcepoint DLP components (which reside on the Forcepoint management server)

After completing those steps, see the Forcepoint DLP Installation Guide for instructions on installing additional components, like the protector and agents.

Creating a Forcepoint management server

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

The Forcepoint management server is the Windows machine that hosts the Forcepoint Security Manager, the configuration, policy management, and reporting interface for Forcepoint on-premises web, data, and email protection solutions.

Additional, optional components can also run on the machine.

Important

There is only one management server per deployment.

Installing the Forcepoint Security Manager

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

Important

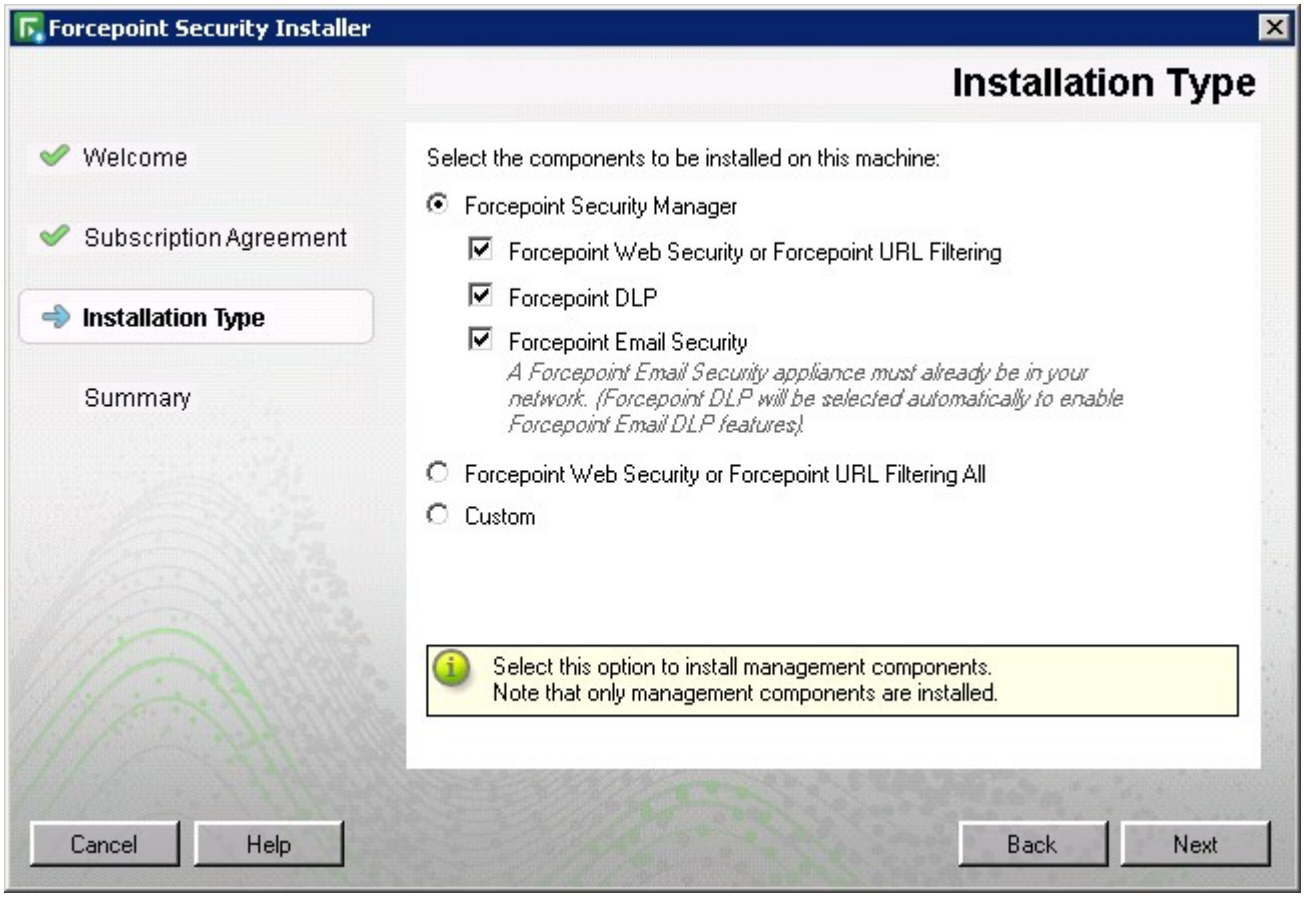
If you are installing Forcepoint DLP components, do not change this account after installation. Be sure it's a dedicated account that you want installed services to use when interacting with the operating system—the service account. If you must change the account, contact Technical Support first.

2) Double-click the installer file to launch the Forcepoint Security Setup program. A progress dialog box appears, as files are extracted.

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

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

5) On the Installation Type screen, select **Forcepoint Security Manager** and the modules you want to install (Web, Data, or Email).



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

Solution	Security Manager module (Web)	Security Manager module (Data)	Security Manager module (Email)
Forcepoint Web Security or Forcepoint URL Filtering	X		
Forcepoint Web Security with the DLP Module	X	X	

Solution	Security Manager module (Web)	Security Manager module (Data)	Security Manager module (Email)
Forcepoint DLP		X	
Forcepoint Email Security		X	X

Important

Installing the Web Security module of the Security Manager requires an instance of Policy Broker and Policy Server.

- These may be installed at the same time as the management components.
- These may be installed before the management components.
  If Policy Broker and Policy Server are not installed with the management components, the installation process prompts for the Policy Server IP address.

  In appliance-based deployments, Policy Broker and Policy Server reside on the **full policy source** appliance.

When you select the Forcepoint Email Security option, the Forcepoint DLP option is also selected automatically. Data components are required for Email Security DLP Module features.

Important

To install the Email Security module of the Security Manager, an Email mode appliance must already be running. The installation process prompts for the appliance C interface IP address during Security Manager installation.

The appliance P1/E1 (and P2/E2, if used) interface must also be configured in the appliance CLI before you install the Email Security module of the Security Manager.

6) When Forcepoint DLP is installed without Forcepoint Email Security, a second Installation Type screen is displayed. **DO NOT** select the option provided. This option is used for a feature that is not supported in version 8.5.0, and will cause problems if selected.

7) On the Summary screen, click **Next** to continue the installation.

8) The Forcepoint Management Infrastructure installer launches.
Follow the instructions in *Installing Forcepoint Infrastructure*.

9) When you click **Finish** in the Forcepoint Management Infrastructure Setup program, component installers for each module selected in the Module Selection screen are launched in succession.
Only the component installers for the modules you selected are launched. For example, if you select only Forcepoint Web Security and Forcepoint DLP modules, the Forcepoint Email Security module installer is not launched.

10) 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.

- *Installing the Web Security module of the Forcepoint Security Manager*
- *Installing the Data Security module of the Security Manager*
- *Installing the Email Security module of the Security Manager*

Related tasks
Installing Forcepoint Infrastructure on page 153

Installing the Web Security module of the Forcepoint Security Manager

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Important

If Policy Broker and Policy Server are not installed with the management components, they must already be installed and running elsewhere in the deployment.

If a **full policy source** appliance has been deployed, Policy Broker and Policy Server reside there. For instructions on installing these components, see *Installing web protection components*.

It is assumed you have reached this point by starting a Forcepoint Security Manager installation. If not, see *Creating a Forcepoint management server*.

1) In the **Select Components** screen, select the components to install on this machine and then click **Next**. The following web protection components are available for installation on a Forcepoint management server:
   - Web Security module of the Security Manager must be installed. It is selected by default and cannot be deselected. The other components shown are optional for this machine.
   - Log Server may be installed on the management server for testing. This configuration is not recommended for production environments.
   - If you have purchased the Web Security Hybrid Module, Sync Service may be installed on this machine, though it is typically installed on the Log Server machine.

   Note

   Sync Service and Log Server consume considerable system resources. For production deployments, it is recommended to install these components on another machine.

   - Select Linking Service if your subscription includes the Web Security DLP Module or Forcepoint DLP.

   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 mode 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 management server, as Filtering Service can consume considerable system resources and may have a performance impact on the management server. Large or distributed environments may include multiple Filtering Service instances.

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

- Real-Time Monitor is installed by default on the management server. Because one Real-Time Monitor instance can monitor multiple Policy Servers, additional instances are not usually required. If you install additional instances, you may have a maximum of one per Policy Server.
- Select Policy Broker and Policy Server if these components have not already been installed in your deployment. They are required to install the Web Security module of the Security Manager. If you have a **full policy source** appliance, these components are already installed.

2) The Policy Server Connection screen appears. (If you chose to install Policy Broker and Policy Server on this machine, skip this step.)
See *Policy Server Connection Screen* for instructions.

3) If you selected Sync Service for installation, the Policy Broker Connection screen appears. (If you chose to install Policy Broker and Policy Server on this machine, skip this step.)
See *Policy Broker Connection Screen* for instructions.

4) If you selected Log Server for installation, the Log Database Location screen appears.
See *Log Database Location Screen* for instructions.

5) If you selected Log Server for installation, the Optimize Log Database Size screen appears.
See *Optimize Log Database Size Screen* for instructions.

6) If you select Linking Service for installation, the Filtering Service Communication screen appears.
See *Filtering Service Communication Screen* for instructions.

7) On the Pre-Installation Summary screen, verify the information shown.
The summary shows the installation path and size, and the components to be installed.

8) Click **Next** to start the installation. A progress screen is displayed. Wait for installation to complete.

9) On the Installation Complete screen, click **Next**.

10) If you have not selected any other Forcepoint Security Manager modules, you are returned to the Modify Installation dashboard. Installation is complete.
If you have chosen to install other modules of the Security Manager, you are returned to the Installer Dashboard and the next component installer is launched.

Related concepts

Policy Server Connection Screen on page 160
Policy Broker Connection Screen on page 161
Log Database Location Screen on page 167
Optimize Log Database Size Screen on page 167
Filtering Service Communication Screen on page 162

Related tasks

Installing web protection components on page 157

Related reference
Creating a Forcepoint management server on page 118

Installing the Data Security module of the Security Manager

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Follow these instructions to install Forcepoint DLP components on the Forcepoint management server. This includes:

- Policy engine
- Primary fingerprint repository
- Forensics repository
- Endpoint server

It is assumed you have reached this point by starting a Forcepoint Security Manager installation. If not, see *Creating a Forcepoint management server*.

1) When the Forcepoint DLP Installer is launched, a Welcome screen appears. Click **Next** to begin Forcepoint DLP installation.

Note

Both .NET v3.5 and 4.5 must be installed before you begin the installation. If either is missing, you receive a message to this effect.

2) On the Select Components screen, click **Next** to accept the default selections.

Note

If there is insufficient RAM on this machine for Forcepoint management server components, a message appears. Although it is possible to continue with the installation, it is better to upgrade the RAM first, and then install.

3) If prompted, click **OK** to indicate if services such as SMTP will be enabled.
Required Windows components will be installed. You may need access to the operating system installation disc or image.

4) 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.

5) If the SQL Server database is on a remote machine, you are prompted for the name of a temporary folder. This screen defines where the system should store temporary files during archive processing as well as system backup and restore.
Archiving lets you manage the size of your incident database and optimize performance. Backup lets you safeguard your policies, forensics, configuration, data, fingerprints, encryption keys, and more.

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 Forcepoint 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:

- Mark **Enable incident archiving and system backup** to make it possible 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.
- In the **From SQL Server** field, enter the path that the SQL Server should use to access the temporary folder. As a best practice, use a remote UNC path, though local and shared network paths are supported. Make sure the account used to run SQL has write access to this folder.
- In the **From Forcepoint management server** field, 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 Forcepoint DLP components, you can revoke this permission:

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

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

7) In the Installation Confirmation screen, click **Install**to begin installation of Forcepoint DLP components.

8) If a message about freeing port 80 appears, click **Yes** to continue the installation:
   - 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 Forcepoint DLP installer.

11) If no other Security Manager module is chosen for installation, you are returned to the Modify Installation dashboard. Installation is complete.
    Otherwise, you are returned to the Installer Dashboard and the next component installer is launched.

For information on installing other Forcepoint DLP components, such as the protector, mobile agent, Analytics Server, crawler, or endpoint client, see the Forcepoint DLP Installation Guide.

Related reference
Creating a Forcepoint management server on page 118

Installing the Email Security module of the Security Manager

Applies to:

- Forcepoint Email Security, v8.5.x

When installing the Email Security module of the Security Manager, the option is provided to also install Email Log Server.

It is assumed you have reached this point by starting a Forcepoint Security Manager installation and selecting the Email Security module. If not, see *Creating a Forcepoint management server*.

1) Once the Email Installer is launched, the Introduction screen appears, click **Next** to begin installation.

2) On the Select Components screen, choose whether to install Email Log Server on this machine and then click **Next**.
The Email Security module of the Security Manager will be installed automatically. You cannot deselect it.

Note

If you do not see the Email Security module on this screen, the Forcepoint Management Infrastructure was not detected by the installer. The Forcepoint Management Infrastructure must be installed already to be able to install the email management components.

Email Log Server is selected for installation by default. To install the Email Log Server, SQL Server or SQL Server Express must already be installed and running in your network (see *System requirements for this version*, for supported versions of SQL Server). If you chose to install SQL Server Express, if available, during Forcepoint Management Infrastructure installation, then it is already installed on this machine.

Starting in version 8.5.4, more stringent connection string and certificate requirements are needed for establishing an encrypted connection with a SQL Server. Using an IP address is no longer supported for encrypted connections; you must use a hostname or a fully qualified domain name (FQDN) that matches the Common Name (CN) field on the certificate used by SQL Server, if using an encrypted database connection.

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** > **Forcepoint** > **Email Log Server Configuration**.

You can install the Email Log Server on another machine; it is not required to be installed on the same machine as the Security Manager. To install Log Server on a different machine, deselect the Email Log Server option here (in the **Select Components** screen) and complete the installation. Then run Forcepoint Security Installer on the machine on which you want to install the Email Log Server. Perform a custom installation of email protection components to install Email Log Server (see *Installing email protection components*).

Note

Should you have occasion to uninstall the Email Log Server, be aware that this operation may not remove the Log Database when the Log Server is installed on a different machine from the Security Manager.

To resolve this issue, delete the following items manually in Microsoft SQL Server after the Email Log Server is uninstalled:

Tables:

\\Database\\esglogdb76

\\Database\\esglogdb76

Jobs:

\\SQL Server Agent\\Jobs\\ ESG_ETL_Message_Insert_Job

\\SQL Server Agent\\Jobs\\ ESG_ETL_Message_Process_Job

\\SQL Server Agent\\Jobs

\\ESG_ETL_Message_Summary_Address_Job

\\SQL Server Agent\\Jobs\\ ESG_ETL_Message_Summary_Job

\\SQL Server Agent\\Jobs\\ ESG_ETL_Message_Update_Job

SQL Server Agent\\Jobs\\ ESG_Maintenance_Job

3) 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.

   If you are using an encrypted connection, ensure that you use a hostname or FQDN for your Email Log Database that matches the CN field on the certificate that SQL Server is using.

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

   - By default, Email Log Server uses NTLMv2 to encrypt the connection. 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 Forcepoint appliance to the Log Database 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 SQL authentication.

4) On the **Email Database File Location** screen, specify where database files should be located and then click **Next**.
This screen appears only if you chose to install the Email Log Server.

   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.

5) On the **Email System Credentials** screen, specify the server name or domain name of the management server, along with the user credentials to be used by Forcepoint Security Manager components when running services. Specify the **User name** and **Password**of the account to be used by the Security Manager.

6) On the **Email Appliance** screen specify the Email appliance to be managed by this installation of the Security Manager and then click **Next**.
Enter the IP address 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 the Security Manager has been used to manage the appliance). Resolve this issue in one of the following ways:
  - Reset the subscription key on the appliance.
  - If the **Appliance network communication** popup message appears, click **OK** and enter your subscription key in the appropriate entry field.
- 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 P1/E1 interface has not been correctly configured in the Appliance manager.

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

8) On the **Pre-Installation Summary** screen, review your settings for 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.

9) The **Installing Email Protection Solutions** screen appears, as components are being installed.

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

11) The Forcepoint Security Setup program closes. Installation is complete.

Related tasks

Installing email protection components on page 175

Related reference

Creating a Forcepoint management server on page 118
System requirements for this version on page 9

Chapter 9

Installing Web Protection Solutions

Contents

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x
- Forcepoint Appliances, v8.5.x

For a PDF with start-to-finish instructions for a typical installation, see:

- Installation Instructions: Forcepoint Web Security
- Installation Instructions: Forcepoint URL Filtering

To perform a simple, one-machine installation of Forcepoint URL Filtering on a supported Windows server (for example, for evaluation), see *Installing via the Forcepoint Web Security or Forcepoint URL Filtering All option*.

Installing via the Forcepoint Web Security or Forcepoint URL Filtering All option

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Follow these instructions to perform an installation that installs all supported web protection components on one Windows machine. Note that for Forcepoint Web Security evaluations, a second machine is needed to host the Linux-only Content Gateway component.

Important

If, when installing v8.5.4, you encounter the error 'Installation failed with error code 3004', refer to the Installation Guide for instructions.

1) Download or copy the Forcepoint Security Installer (the Windows installer) to this machine. The installer is available from the My Account page at forcepoint.com, and the installer file is `Forcepoint85xSetup.exe`.

2) Double-click the installer file to launch the Setup program. A progress dialog box appears, as files are extracted. Once files have been extracted, there may be a pause of several seconds before the Welcome screen is displayed.

3) On the **Welcome** screen, click **Start**.
The Installer Dashboard remains on screen throughout the installation process.

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

5) On the **Installation Type** screen, select **Forcepoint Web Security or Forcepoint URL Filtering All**.
On the second **Installation Type** screen, select **Use the SQL Server database installed on another machine**.

6) On the **Summary** screen, click **Next** to continue the installation.

7) Forcepoint Management Infrastructure Setup launches. On the Forcepoint Management Infrastructure Setup Welcome screen, click **Next**.

8) On the Installation Directory screen, specify the location where you want Forcepoint Management Infrastructure to be installed and then click **Next**

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

Important

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

9) On the SQL Server screen, specify the location and connection credentials for a database server located elsewhere in the network.

a) Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any, and the **Port** to use for SQL Server communication.
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.

b) Specify whether to use **SQL Server Authentication** (a SQL Server account) or **Windows Authentication** (a Windows trusted connection), then provide the **User Name** or **Account** and its **Password**.
If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Forcepoint Security Manager. See Configuring Apache services to use a trusted connection.

c) Click **Next**. The installer verifies the connection to the database engine. 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.

10) On the **Server and Credentials** screen, select the IP address of this machine and specify network credentials to be used by Forcepoint Security Manager.

- Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.
  Administrators will use this address to access the Security Manager (via a web browser), and components on other machines will use the address to connect to the management server.
- Specify the **Server or domain** of the user account to be used by Forcepoint Management Infrastructure and Forcepoint Security Manager. The name cannot exceed 15 characters.
- Specify the **User name** of the account to be used by Security Manager.
- Enter the **Password** for the specified account.

11) On the **Administrator Account** screen, enter an email address and password for the default Security Manager administration account: **admin**. When you are finished, click **Next**.
System notification and password reset information is sent to the email address specified (once SMTP configuration is done; see next step).

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

12) On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications and then click **Next**. You can also configure these settings after installation in the Security 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 the Security Manager, the “Forgot my password” link on the logon page does not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent.

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

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

14) The Installation screen appears, showing installation progress. Wait until all files have been installed.
If an “Error 1920” message appears, check to see if port 9443 is already in use on this machine. If port 9443 is in use, release it and then click **Retry** to continue installation.

15) On the Installation Complete screen, click **Finish**.
You are returned to the Installer Dashboard and, after a few seconds, the web protection component installer launches.

16) If the **Multiple Network Interfaces** screen appears, select the NIC to use for inter-component communication, then click **Next**.

17) On the **Policy Broker Replication** screen, indicate which Policy Broker mode to use. If you aren't sure, see Managing Policy Broker Replication for assistance.

18) On the **Active Directory** screen, specify whether your network uses Windows Active Directory, then click **Next**.

19) If you are using Active Directory, the **Computer Browser** screen may appear. Click **Next** to have the installer attempt to start the service.
If the installer is unable to start the service, you must start it after installation.

20) On the **Integration Option** screen, indicate how Filtering Service will be configured to receive Internet requests for policy enforcement, then click **Next**.

- **Install Web Security to connect to Content Gateway**: Content Gateway is responsible for monitoring Internet requests, forwarding them to Filtering Service, and performing real-time analysis.
- **Install Forcepoint Web Security or Forcepoint URL Filtering in standalone mode (no real-time analysis)**: Network Agent is responsible for monitoring Internet requests and forwarding them to Filtering Service for evaluation. Network Agent also sends block messages.
- **Install Forcepoint URL Filtering to integrate with a third-party product or device**: A third-party firewall, proxy server, cache, or network appliance (integration product) is responsible for monitoring Internet requests and sending them to Filtering Service for evaluation. You will select your integration product on the next screen.

If you aren't sure what to select, see *Understanding standalone and integrated modes for web protection solutions*.

21) If you selected "Integrated with another application or device" in the previous step, on the **Select Integration** screen, select the product you want to integrate with, then click **Next**.

22) On the **Network Card Selection** screen, select the network interface card (NIC) that Network Agent should use to monitor Internet activity, then click **Next**.
For more information, see *Deployment guidelines for Network Agent*.

23) If the 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.

24) On the **Log Database Location** screen, specify a location (directory path) for your reporting database, then click **Next**.

25) On the **Optimize Log Database Size** screen, select options for optimizing the size of log database records, then click **Next**.

- When **Log web page visits** is selected (default), one record (or a few records) is created with combined hits and bandwidth data for each website requested, rather than a record for each separate file included in the request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities.

- When **Consolidate requests** is selected, Internet requests that share the same value for domain name, category, keyword, action (like permit or block) and user/IP address, within a certain interval of time (1 minute, by default), are combined.

26) On the **Feedback** screen, choose whether to send categorization feedback to Forcepoint, then click **Next**.

27) On the **Web Security Hybrid Module Components** screen, indicate whether to install Sync Service and Directory Agent, then click **Next**. These services are only used if you have purchased the Web Security Hybrid Module for Forcepoint Web Security.

28) On the **Transparent User Identification** screen, select whether to use transparent identification agents to identify users and then click **Next**.

- Select **Use DC Agent to identify users logging on to Windows domains** to install DC Agent on this machine. DC Agent polls domain controllers and retrieves information about user logon sessions, and can also poll user machines directly to verify the logged-on user.
- Select **Use Logon Agent to identify users logging on to local machines** to install Logon Agent on this machine. Logon Agent provides the highest level of user identification accuracy by identifying users as they log on to Windows domains.
  Logon Agent works with a logon application that runs via logon script on client machines. For instructions on configuring domain controllers and client machines to use Logon Agent, see the Using Logon Agent for Transparent User Identification technical paper.

  Note

  Do not use Logon Agent in a network that already includes eDirectory Agent.

- Select **Use both DC Agent and Logon Agent** to use both of the agents that work with Windows Active Directory. When both agents are installed, DC Agent information is used as a backup in the unlikely event that Logon Agent is unable to identify a user.
- Select **Use eDirectory Agent to identify users logging on via Novell eDirectory Server** to install eDirectory Agent on this machine. eDirectory Agent queries the Novell eDirectory Server at preset intervals to identify users currently logged on.

  Note

  Do not use eDirectory Agent in a network that already includes DC Agent or Logon Agent.

- Select **Do not install a transparent identification agent now** if:
  - (Forcepoint Web Security) Content Gateway provides user authentication.
  - (Forcepoint URL Filtering) A third-party integration product (firewall, proxy server, cache, or network appliance) provides user authentication.

    Note

    When Forcepoint URL Filtering is integrated with Cisco products, Cisco Secure Access Control Server (ACS) cannot be used for user authentication for more than 1 user domain. If there are multiple user domains, use a transparent identification agent instead.

  - You plan to run the transparent identification agent on one or more other machines.
  - You do not want different policies applied to users or groups.
  - You want all users to be prompted for logon information when they open a browser to access the Internet.

29) On the **Directory Service Access** screen, supply a local and domain administrator account with directory service access permissions.

30) On the **RADIUS Agent** screen, select **Install RADIUS Agent** if you have remote users that are authenticated by a RADIUS server and then click **Next**. This allows user- or group-based policies to be enforced for remote users without prompting for logon information.

31) On the **Pre-Installation Summary** screen, verify the information shown.
The summary shows the installation path and size, and the components to be installed.

32) Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

33) On the **Installation Complete** screen, click **Done**.

Related concepts
Understanding standalone and integrated modes for web protection solutions on page 42

Related reference
Deployment guidelines for Network Agent on page 56

Using the management server as policy source for filtering-only appliances

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

It is possible to deploy web protection components so that the central Policy Broker and Policy Server are installed on the management server, and filtering only appliances use that machine as the full policy source.

If you choose this deployment option, it is important to install your components in the following order.

1) Install Policy Broker and Policy Server on the machine that will become the management server. See *Installing web protection components*.

2) Set up the appliance to run in **filtering only** mode, specifying the Policy Broker machine (the future management server) as the policy source.

3) Install management components (including the Web or Web and Data modules of the Forcepoint Security Manager) on the Policy Broker machine to create the management server.
If you have purchased the Web Security DLP module, also install Linking Service on the management server machine.

   See *Creating a Forcepoint management server*.

Install reporting and other off-appliance components as necessary. See *Installing web protection components*.

Related tasks

Installing web protection components on page 157

Related reference

Creating a Forcepoint management server on page 118

Chapter 10

Installing Web Protection Components on Linux

Contents

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Use the Web Security Linux installer to install supported components on a Linux machine.

Complete installation instructions for installing web protection solutions (which include steps for Linux, Windows, and appliance installations) are available here:

- Installation Instructions: Forcepoint Web Security
- Installation Instructions: Forcepoint URL Filtering

If you want to install all Linux-compatible web protection components (except for Remote Filtering Server) on this machine, you can instead use the following instructions:

1) Starting the Web Linux installer

2) Using the Policy Enforcement option to install web components on Linux

(Remote Filtering Server is not included because it resides by itself on a machine in the network DMZ.)

Related tasks

Starting the Web Linux installer on page 138
Using the Policy Enforcement option to install web components on Linux on page 139

Starting the Web Linux installer

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

Steps

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/forcepoint_setup`

3) Download the Web Linux installer package from the My Account page at support.forcepoint.com. The installer package is called:
`Web85xSetup_Lnx.tar.gz`
Place the installer archive in the setup directory you created.

4) Extract the installer files:
In the setup directory, enter the following commands to uncompress and extract files:

```
gunzip Web85xSetup_Lnx.tar.gz
tar xvf Web85xSetup_Lnx.tar
```

This places the following files into the setup directory:

File	Description
install.sh	Installation program
Setup.bin	Archive file containing installation files and documents

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
```

If the installation program displays error messages that it is having difficulty locating other machines, disable any firewall running on the installation machine.

Note

- The following instructions refer to installer screens. In the command-line Linux installer, prompts are displayed that correspond to each screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.
- To cancel the command-line Linux installer, press Ctrl-C. However, do **not** cancel 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.

Using the Policy Enforcement option to install web components on Linux

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

Steps

1) It is assumed you have already downloaded and started the Web Linux installer. If not, see *Starting the Web Linux installer* for instructions.

2) If no web protection components have been installed on this machine:

   a) On the **Introduction** screen, click **Next**.

   b) On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.

c) If the **Multiple Network Cards** screen appears, select the IP address of the NIC that web protection components should use for communication. This NIC will also be used to send block pages when a user requests blocked content.

> **Important**
>
> The installer cannot determine whether IP addresses are valid. It simply lists the currently configured address of each detected NIC. Be sure to verify that the IP address you select is valid in your network. An incorrect IP address will prevent components on this machine from functioning properly.

d) On the **Installation Type** screen, select **Policy Enforcement** and then click **Next**.

3) If there are web protection components already installed on this machine, the **Add Components** screen appears.

Select **Install additional components on this machine** and then click **Next**.
If there are already components on this machine, you can only perform a custom installation.

If there are no web protection components already installed, the **Policy Broker Replication** screen appears. 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.
  The password may include between 4 and 300 alphanumeric characters.

  > **Important**
  >
  > If you are installing the primary Policy Broker, be sure to record the synchronization password. You must provide this password each time you create a Policy Broker replica.

- Do not select **Replica** at this stage. You must install a standalone or primary Policy Broker before you can install a replica.

4) On the Integration Option screen, indicate whether this is a Forcepoint Web Security deployment that uses Content Gateway, a standalone deployment, or an integrated Forcepoint URL Filtering deployment, and then click **Next**.

See *Understanding standalone and integrated modes for web protection solutions* for more information.

5) If you chose the Forcepoint URL Filtering integrated option, the **Select Integration** screen appears. Select your third-party integration product, then click **Next**.

6) On the **Network Card Selection** screen, select the NIC that Network Agent should use to communicate with other web protection components, then click **Next**.

The list may include NICs that do not have an IP address are also listed. Do **not** choose a NIC without an IP address.

7) On the **Feedback** screen, select whether you want your software to send feedback to Forcepoint to improve accuracy. Then click **Next**.

8) On the **Web Security Hybrid Module** screen, select whether you want to install components that support the hybrid service on this machine, then click **Next**.

- **Install Web Security Hybrid module components**: Select this option to install these components and then check the box for the components (**Sync Service** and/or **Directory Agent**) you want to install.
- **Do not install Web Security Hybrid module components**: Select this option if you do not have a Web Security Hybrid Module subscription, or if you want to install Sync Service and Directory Agent on another machine.

9) On the **Transparent User Identification** screen, select whether to use transparent identification agents to identify users and then click **Next**. This allows user- or group-based policies to be applied to requests without prompting users for logon information.

It is possible to run multiple instances of the same transparent identification agent, or certain combinations of different transparent identification agents, in a network. For information about multiple instances or combinations of transparent identification agents, see Combining transparent identification agents section in *Deploying transparent identification agents*.

- **Use Logon Agent to identify users logging on to local machines**: This option installs Logon Agent on this machine. Logon Agent identifies users as they log onto Windows domains. Logon Agent is for use with Windows-based client machines on a network that uses Active Directory or Windows NT Directory.

  To use Logon Agent, you must modify the Group Policy on domain controllers so it launches a logon application (LogonApp.exe) as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users.

  See the Using Logon Agent for Transparent User Identification technical paper.

  Note

  Do not use Logon Agent in a network that already includes eDirectory Agent.

- **Use eDirectory Agent to identify users logging on via Novell eDirectory Server**: This option installs eDirectory Agent on this machine. Use this agent for a network using Novell eDirectory. eDirectory Agent queries the eDirectory Server at preset intervals to identify users currently logged on.

  Note

  Do not use eDirectory Agent in a network that already includes DC Agent or Logon Agent.

- **Do not install a transparent identification agent now**: Select this option if
  - Content Gateway or a third-party integration product will provide user authentication.
  - You plan to install a transparent identification agent on another machine.
  - You do not want to apply policies to users or groups, and do not want user and group information to appear in reports.
  - You want users to be prompted for logon information when they open a browser to access the Internet.

  Note

  When integrated with Cisco products, Forcepoint URL Filtering cannot use Cisco Secure Access Control Server (ACS) for user authentication for more than 1 user domain. If there are multiple user domains, use a transparent identification agent instead.

10) On the **RADIUS Agent** screen, select **Install RADIUS Agent** if you have remote users that are authenticated by a RADIUS server and then click **Next**. This allows user- or group-based policies to be applied to requests from these remote users without prompting them for logon information.

11) On the **Installation Directory** screen, accept the default installation path (/opt/ Websense), or click **Choose** to specify another path, and then click **Next**.

The installation path must be absolute (not relative).

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.

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

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

13) Click **Next** to start the installation. 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 **Done**.

Related concepts

Understanding standalone and integrated modes for web protection solutions on page 42

Related tasks

Starting the Web Linux installer on page 138

Related reference

Deploying transparent identification agents on page 53

Chapter 11

Installing Email Protection Solutions

Before you begin

Applies to:
■ Forcepoint Email Security, v8.5.x ■ Forcepoint Appliances, v8.5.x

Forcepoint Email Security is available on Forcepoint V Series, X Series, and virtual appliances. See the Forcepoint Appliances Getting Started Guide for information about setting up and configuring Forcepoint Email Security on a Forcepoint appliance.

You may also deploy Forcepoint Email Security in a Microsoft Azure cloud environment. Deployment in a Microsoft Azure environment includes options for installing Forcepoint Email Security appliances and Forcepoint Security Manager and SQL Server entirely in Azure, or combining certain on-premises and Azure components. See Installing Forcepoint Email Security in Microsoft Azure for all deployment options and installation instructions.

Full installation of a Forcepoint Email Security on-premises solution includes the following steps:

Steps

1) Ensure that Microsoft SQL Server is installed and running in your network.

   See *Obtaining Microsoft SQL Server*.

   In certain versions, you may have the option to install SQL Server Express using the Forcepoint Security Installer. If you intend to use SQL Server Express, skip this step. You will install the database engine with Forcepoint Security Manager components.

   Keep in mind that the performance limitations of SQL Server Express make it more appropriate for evaluation environments or small organizations than for larger deployments.

2) Install and configure your Forcepoint appliances.

   See Forcepoint Appliances Getting Started Guide.

3) Install the Log Server (Windows only).

   See *Installing email protection components*.

   When deploying Email Log Server and Forcepoint Email Security on the same machine, both components are installed together. When deploying Email Log Server and Forcepoint Email Security on separate machines, it is recommended to install Email Log Server before installing other Forcepoint Email Security components.

4) Install the Forcepoint Management Infrastructure (Windows only), including all appropriate Forcepoint Security Manager modules. You must install the Data Security module in addition to the Email Security module in order to access and configure email DLP functions in Forcepoint DLP.

   See *Creating a Forcepoint management server*.

5) Install all other off-appliance product components.

See Installing email protection appliance-based solutions for more information about Forcepoint Email Security on-premises installation.

Related tasks

Installing email protection components on page 175

Related reference

Creating a Forcepoint management server on page 118
Obtaining Microsoft SQL Server on page 24

Chapter 12

Setting Up Forcepoint Appliances

Contents

Applies to:

- Forcepoint Appliances, v8.5.x
- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint Email Security, v8.5.x

A Forcepoint appliance is a component of a complete Forcepoint security deployment.

Setting up a deployment consists of five core tasks:

1) Deployment planning and preparation

2) Appliance hardware setup and/or virtual appliance creation

3) Initial configuration: the **firstboot** wizard

4) Post-firstboot appliance configuration in the command line interface (CLI)

5) Installation and configuration of off-appliance components

Forcepoint appliance setup is described in detail in Forcepoint Appliances Getting Started.

Forcepoint V Series and X Series appliances come with a hardware Quick Start poster packaged in the shipping container. The 2-page poster explains how to set up the hardware and cable the appliance to your network. You can also access the posters online.

- V5000 G2/G3 poster
- V5000 G4 poster
- V5000 G4 poster for Forcepoint DLP
- V10000 G3 poster
- V10000 G4 poster
- V10K G4R2/V20K G1 poster
- X10G G1/G2 poster

Important

Some older V10000 and V5000 appliances are not supported with versions of 8.0 and higher.

Restoring to Factory Image

Applies to:
■ Forcepoint Appliances, v8.5.x ■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint Email Security, v8.5.x

Forcepoint appliances can be restored to the v8.5.x factory image. See How to restore a Forcepoint appliance to a factory image.

Chapter 13

Installing Forcepoint DLP

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Installing Forcepoint DLP involves, at minimum, two basic steps:

1) Install the Forcepoint Management Infrastructure. This includes the Forcepoint Security Manager, settings database, and reporting database.

2) Install Forcepoint DLP management components. This includes the a policy engine, crawler, fingerprint repository, forensics repository, and endpoint server.

After the management components have been installed, additional Forcepoint DLP servers and components may be installed on servers, appliances, cloud infrastructures, or endpoint client machines.

- See the *System requirements for this version* to find the hardware and operating system requirements for Forcepoint DLP components.
- See the Forcepoint DLP Installation Guide for step-by-step installation instruction for the management server and additional components.

The Installation Guide also covers how to add, modify, and remove components.

Related reference
System requirements for this version on page 9

Chapter 14

Installing components via the Custom option

Contents

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint Appliances, v8.5.x

Forcepoint Security components can be deployed in a variety of configurations. In many cases, additional instances of individual components can be added as your network grows or traffic patterns change.

Use the custom installation instructions provided in this section to adapt the common installation scenarios (listed below) for your deployment.

- Installation Instructions: Forcepoint Web Security
- Installation Instructions: Forcepoint URL Filtering
- Forcepoint DLP Installation Guide
- Installing email protection solutions
- *Installing Forcepoint Security Solutions*

Important

Although you can select any combination of components using the Custom installation option, not all combinations are supported. For example, you can install Forcepoint Email Security without installing Forcepoint DLP even though the latter is required for email DLP.

Deployment

General

- *System requirements for this version*

Web protection solutions

- *Deploying Web Protection Solutions*
- *Web protection distributed deployments*
- *Integrating Forcepoint URL Filtering with Cisco*
- *Integrating Forcepoint URL Filtering with Citrix*
- *Integrating Forcepoint URL Filtering using ICAP Service*
- *Integrating Forcepoint URL Filtering with TMG*
- *Installing for Universal Integrations*

Forcepoint DLP

- Planning Data Security Deployment
- Integrating Data Security with Existing Infrastructure
- Scaling Data Security

Email protection solutions

- *Deploying Email Protection Solutions*

Installation

To start a custom installation, see *Starting a custom installation (Windows)*. Then see the following instructions for the components you want to install:

- *Installing Forcepoint Infrastructure*
- *Installing web protection components*
- *Installing Forcepoint DLP components*
- *Installing email protection components*
- *Installing SQL Server Express (without Forcepoint Infrastructure)*

Initial configuration

General

- *Default ports for on-premises Forcepoint security solutions*
- *Excluding Forcepoint files from antivirus scans*
- *Initial Configuration for All Security Modules*

Forcepoint Web Security

- *Initial configuration for web protection solutions*
- *Content Gateway initial configuration*
- *Additional configuration for the Web Security DLP Module*

Forcepoint DLP

- *Forcepoint DLP initial configuration*

Forcepoint Email Security

- *Forcepoint Email Security initial configuration*

Related concepts

Forcepoint Email Security initial configuration on page 336
Forcepoint DLP initial configuration on page 335
Additional configuration for the Web Security DLP Module on page 333
Content Gateway initial configuration on page 337
Initial configuration for web protection solutions on page 331
Deploying Email Protection Solutions on page 105
Installing for Universal Integrations on page 247
Integrating Forcepoint URL Filtering with TMG on page 221
Integrating Forcepoint URL Filtering using ICAP Service on page 241
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with Cisco on page 183
Web protection distributed deployments on page 67
Deploying Web Protection Solutions on page 33
Installing Forcepoint Security Solutions on page 117

Related tasks

Initial Configuration for All Security Modules on page 329
Installing SQL Server Express (without Forcepoint Infrastructure) on page 178
Installing email protection components on page 175
Installing Forcepoint DLP components on page 174
Installing web protection components on page 157
Installing Forcepoint Infrastructure on page 153
Starting a custom installation (Windows) on page 151

Related reference

Excluding Forcepoint files from antivirus scans on page 370
Default ports for on-premises Forcepoint security solutions on page 361
System requirements for this version on page 9

Starting a custom installation (Windows)

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Note

If you have previously disabled TLS 1.0 on your Windows server, re-enable it before beginning Forcepoint installation. You may disable it again after installation is complete.

Steps

1) Download or copy the Forcepoint Security Installer (the Windows installer) to this machine. The installer is available from the Forcepoint My Account page, and the installer file is `Forcepoint8xxSetup.exe` (for example, `Forcepoint85xSetup.exe` for version 8.5.x).

2) Log on to the installation machine with a domain user account that has local administrator privileges.

Important

If you are installing data protection components, do not change this account after installation. Be sure it's a dedicated account that you want installed services to use when interacting with the operating system—the service account. If you must change the account, contact Technical Support first.

3) Double-click the installer file to launch the Forcepoint Security Setup program.

   A progress dialog box appears, as files are extracted. It may take some time to extract all of the installer files and launch the setup program.

4) On the Welcome screen, click **Start**.

   The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.

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

6) On the Installation Type screen, select `Custom`.

7) On the Summary screen, click **Next** to continue the installation.

   If current-version components are already installed on this machine, the links next to a product will be **Modify** and **Remove**, rather than **install**. Click **Remove** to remove components and **Modify** to add components.

Next steps

When installing using the `Custom` option, you may have the option to also install SQL Server Express—a free, limited-performance version of SQL Server—to be used for Forcepoint Security reporting data. As a best practice, SQL Server Express should be used only in non-production or evaluation environments. A standard or enterprise version of SQL Server should be used in production environments.
If available, select the `SQL Server Express` option at the bottom of the Custom Installation page of the Forcepoint Security Setup. SQL Server Express will be installed on the local machine later in the install process.

- When this option is selected, Powershell 1.0 and Windows Installer 4.5 are installed automatically if they are not found on the machine. These are required for SQL Server Express.
- A default database instance named mssqlserver is created, by default. If a database instance with the default name already exists on this machine, an instance named TRITONSQL2K8R2X is created instead.
- If .NET 3.5 SP1 or .NET 4.5 are not found on the machine, you are prompted to install them before proceeding.
- In some cases, you are prompted to reboot the machine after installing SQL Server Express. If you do, restart the installer:
  - Windows Server 2016 and 2012: Go to the **Start** screen and click the **Forcepoint Security Setup** icon.
  - Windows Server 2008 R2 SP1 and 2016: Go to **Start** > **Forcepoint** > **Forcepoint Security Setup**.

Installing Forcepoint Infrastructure

Before you begin

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x

Forcepoint Infrastructure is composed of common user interface components required by the Forcepoint Security Manager Web Security, Data Security, and Email Security modules.

Steps

1) These instructions assume that you have already launched the Forcepoint Security Installer and done one of the following:
   - Selected the `Custom` installation type, and selected Forcepoint Infrastructure install. (See Deployment section in *Installing components via the Custom option*.)
   - Selected the Forcepoint Security Manager installation type. (See *Creating a Forcepoint management server*.)
   - Started an upgrade of prior-version web or data protection components, with management components installed on this machine. In this case, skip to Step 3 now.

   The instructions also assume that a supported version of Microsoft SQL Server has been installed on a remote machine.

2) On the Custom Installation dashboard, click the **Install** link for Forcepoint Infrastructure. (If Forcepoint Security Setup has been started as part of a Forcepoint Security Manager installation, skip this step.)
   Forcepoint Security Setup is launched.

3) On the Forcepoint Infrastructure Setup Welcome screen, click **Next**.

4) On the Installation Directory screen, specify the location where you want Forcepoint 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**.

5) 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. Encryption is recommended to increase the level of security in the SQL database.

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

- 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).

  Note

  If your Forcepoint Email Security SQL Server installation uses a named instance, port 1433 is opened on the firewall even if you specify a different port. You must manually change this port setting after Forcepoint Email Security installation.

  See *System requirements for this version* to verify your version of SQL Server is supported.

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

- Select the Authentication method to use for database connections: SQL Server Authentication (to use a SQL Server account) or Windows Authentication (to use a Windows trusted connection).
  Next, provide the User Name or Account and its Password. If you are using Windows authentication with Forcepoint DLP, Forcepoint Web Security with the Web DLP module, or Forcepoint Email Security, use an account with the sysadmin role. If you are using SQL Server Express, sa (the default system administrator account) is automatically specified.

  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 Forcepoint Security Manager. 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.

6) On the Server & Credentials screen, select the IP address of this machine and specify network credentials to be used by Forcepoint Security 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 the Forcepoint Security Manager (via a web browser). Also specify this IP address to any other component that needs to connect to the Forcepoint management server.

  If you chose to use SQL Server Express, if you install Log Server for a web or email protection solution on another machine, specify this IP address for the database engine location.
- Specify the `Server or domain` of the user account to be used by Forcepoint Infrastructure and the Forcepoint Security Manager. The server/hostname cannot exceed 15 characters.
- Specify the `User name` of the account to be used by Security Manager.
- Enter the `Password` for the specified account.

7) On the Administrator Account screen, enter an email address and password for the default Security Manager administration account: admin. 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).
The password must:

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

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

8) On the Email Settings screen, enter information about the SMTP server to be used for system notifications and then click **Next**. You can also configure these settings after installation in the Security 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 the Security 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 hostname 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 name can help recipients identify the notification as email from the Forcepoint Security Manager.

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

DANGER

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

Note

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

10) If you chose to install SQL Server Express using the Forcepoint Security Installer, PowerShell 1.0 and Windows Installer 4.5 will be installed if not already present. Wait for Windows to configure components.

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

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

b) The installer starts again. In the Forcepoint Security Setup Welcome screen, click **Next**.

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

11) If you chose to install SQL Server Express on this machine using the Forcepoint Security Installer, SQL Server Express Setup is launched. Wait for it to complete.

The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.
It may take approximately 10–15 minutes for the SQL Server Express installation to complete.

12) Next, the Installation screen appears. Wait until all files have been installed.

If an "Error 1920" message appears, check whether port 9443 is already in use on this machine. If port 9443 is in use, release it and then click **Retry** to continue installation.

13) On the Installation Complete screen, click **Finish**.

Related concepts

Installing components via the Custom option on page 149

Related tasks

Installing with SQL Server on page 172

Related reference

Creating a Forcepoint management server on page 118
System requirements for this version on page 9

Installing web protection components

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

Complete these steps to install one or more web protection software components on Windows.

Important

If, when installing v8.5.4, you encounter the error 'Installation failed with error code 3004', refer to the Installation Guide for instructions.

To install web protection components on a Linux machine, see *Installing Web Protection Components on Linux*.

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**. (For instructions on performing these steps, see Deployment section in *Installing components via the Custom option*.) If you are adding components, skip to Step 2.

Steps

1) On the Custom Installation dashboard, click the Forcepoint Web Security or Forcepoint URL Filtering **Install** link.

   The web protection component installer is launched.

2) Use the **Select Components** screen to identify the component or components to install on this machine. As you make your selection, remember that:

   - Policy Broker, Policy Server, and Filtering Service must be installed in the order listed, and before any other web protection components. (If you select all 3 at the same time, they are installed in the correct order.)
   - The Web Security module of the Forcepoint Security Manager is available only when Forcepoint Infrastructure is already installed on the machine (see *Installing Forcepoint Infrastructure*).
   - Note that in an appliance-based deployment, a Web mode appliance running in *full policy source* mode has Policy Broker already installed and running. In this scenario, there can be only one Policy Broker for the deployment.

3) Depending on the components selected, some or all of the following installer screens appear. (The parenthetical information below indicates which components or machine conditions cause the screen to appear.)

   Click the screen name for instructions.

   - **Policy Server Connection Screen** (Filtering Service, Network Agent, Usage Monitor, Forcepoint Security Manager [Web Security module)\], Real-Time Monitor, Log Server, User Service, DC Agent, Logon Agent, eDirectory Agent, RADIUS Agent, State Server, Remote Filtering Client Pack, Remote Filtering Server, Linking Service, Sync Service, or Directory Agent)
   - **Policy Broker Connection Screen** (Policy Server, Sync Service, or Directory Agent)
   - **Select Policy Broker Screen** (Policy Server)
   - **Multiple Network Interfaces Screen** (if multiple NICs detected)
   - **Active Directory Screen** (if installing User Service, DC Agent, or Logon Agent on Windows Server)
   - **Computer Browser Screen** (if installing User Service, DC Agent, or Logon Agent on Windows Server and the Computer Browser service is not running)
   - **Integration Option Screen** (Filtering Service)
   - **Select Integration Screen** (Filtering Service, to be integrated with a third-party product, or Filtering Plug-In)
   - **Network Card Selection Screen** (Network Agent)
   - **SQL Server Native Client Tools** (management module or Log Server)
     If the installer appears in the foreground, follow the prompts to install the required tools.
   - **Database Information Screen** (Log Server)
   - **Log Database Location Screen** (Log Server)
   - **Optimize Log Database Size Screen** (Log Server)
   - **Feedback Screen** (Filtering Service or Network Agent)
   - **Directory Service Access Screen** (User Service, DC Agent, or Logon Agent)
   - **Remote Filtering Communication Screen** (Remote Filtering Server)
   - **Remote Filtering Pass Phrase Screen** (Remote Filtering Server)
   - **Filtering Service Information for Remote Filtering Screen** (Remote Filtering Server)
   - **Filtering Service Communication Screen** (Network Agent, a filtering plug-in, or Linking Service)

4) 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 one of the following:

   - `C:\Program Files (x86)\Websense\Web Security` (on the Forcepoint management server)
   - `C:\Program Files\Websense\Web Security` (on servers that do not have management components)

   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.

5) On the **Pre-Installation Summary** screen, verify the information shown.
   The summary shows the installation path and size, and the components to be installed.

6) Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

7) On the **Installation Complete** screen, click **Done**.
   Additional configuration may be necessary if you are integrating Forcepoint URL Filtering with another product. See:
   - *Integrating Forcepoint URL Filtering with Cisco*
   - *Integrating Forcepoint URL Filtering with Citrix*
   - *Integrating Forcepoint URL Filtering with TMG*
   - *Installing for Universal Integrations*

Related concepts

Installing Web Protection Components on Linux on page 137
Installing components via the Custom option on page 149
Policy Server Connection Screen on page 160
Policy Broker Connection Screen on page 161
Select Policy Broker Screen on page 161
Multiple Network Interfaces Screen on page 163
Active Directory Screen on page 163
Computer Browser Screen on page 163
Integration Option Screen on page 164
Select Integration Screen on page 165
Network Card Selection Screen on page 165
Database Information Screen on page 166
Log Database Location Screen on page 167
Optimize Log Database Size Screen on page 167
Feedback Screen on page 168
Directory Service Access Screen on page 168
Remote Filtering Communication Screen on page 169
Remote Filtering Pass Phrase Screen on page 170
Filtering Service Information for Remote Filtering Screen on page 170
Filtering Service Communication Screen on page 162
Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with TMG on page 221
Installing for Universal Integrations on page 247

Related tasks

Installing Forcepoint Infrastructure on page 153

Policy Server Connection Screen

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

This screen appears if any of the following is selected for installation, but Policy Server is neither selected nor already installed on the machine:

Windows only	Windows or Linux
■ Forcepoint Security Manager (Web Security module) ■ Log Server ■ DC Agent ■ Real-Time Monitor ■ Remote Filtering Client Pack ■ Linking Service	■ Filtering Service ■ Network Agent ■ Usage Monitor ■ User Service ■ Logon Agent ■ eDirectory Agent ■ RADIUS Agent ■ State Server ■ Remote Filtering Server ■ Sync Service ■ Directory Agent

Enter the IP address of the Policy Server machine and the Policy Server communication port (default is 55806).

- The Policy Server communication port must be in the range 1024-65535.
- During installation, Policy Server may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Server 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) and open the **websense.ini** file in a text editor.

  2) Locate the **PolicyServerPort** value.

  3) When you are finished, close the file without saving. Do **not** modify the file.

If your deployment includes Forcepoint appliances:

- Policy Server is installed on the **full policy source** appliance and any **user directory and filtering** appliances.
- If Policy Server is running on any appliance, enter the IP address of the appliance's C interface.
  Note that when Policy Server resides on an appliance, you must enable the on-appliance Directory Agent, rather than connecting an off-appliance (software-based) instance of the service to the on-appliance Policy Server.

If Policy Server is not currently installed anywhere in your network, you must install it before any of the components listed above.

- To install Policy Server on this machine, click **Previous**, then add **Policy Server** to the components selected for installation.

- To install Policy Server on another machine, run the Forcepoint Security Installer or Web Linux Installer on that machine first, before continuing to attempt installation on the current machine.

Policy Broker Connection Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This screen appears if Policy Server, Sync Service, or Directory Agent is selected for installation, but Policy Broker is not.

Enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

- If Policy Broker is installed on this machine, enter its actual IP address (not the loopback address).
- 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.

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

- To install Policy Broker on this machine, click **Previous**, then add **Policy Broker** to the components selected for installation.
- To install Policy Broker on another machine, run the Forcepoint Security Setup program or Web Linux Installer on that machine first, before continuing to attempt installation on the current machine.

Select Policy Broker Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

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.

- To install Policy Broker on this machine, click **Previous**, then add **Policy Broker** to the components selected for installation.
- To install Policy Broker on another machine, run the Forcepoint Security Setup program or Web Linux Installer on that machine first, before continuing to attempt installation on the current machine.
  After installing on the remote machine, click **Previous** and re-enter the Policy Broker IP address on the Policy Broker Connection screen to reset the list of Policy Broker instances.

Filtering Service Communication Screen

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

This screen appears if Network Agent, a filtering plug-in, or Linking Service (Windows only) is selected for installation.

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

- If Filtering Service is installed on this machine, enter its actual IP address (not the loopback address).
- In an appliance-based deployment, Filtering Service is installed on all web protection 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:
  1) Navigate to the **bin** directory (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default) and open the **eimserver.ini** file in a text editor.
  2) Locate the **WebsenseServerPort** value.
  3) 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.

- To install Filtering Service on this machine, click **Previous**, then add **Filtering Service** to the components selected for installation.
- To install Filtering Service on another machine, run the Forcepoint Security Installer or Web Linux Installer on that machine first, before continuing to attempt installation on the current machine.

Important

Make sure to select the correct integration mode for the Filtering Service instance (standalone or integrated with a supported product).

Multiple Network Interfaces Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This screen appears if multiple network interface cards (NICs) are detected on this machine.

Select the IP address of the NIC that web protection components should use for communication. This NIC will also be used to send block pages.

Important

The installer cannot determine whether IP addresses are valid. It simply lists the currently configured address of each detected NIC. Be sure to select an IP address that is valid in your network.

You will specify later whether this NIC is also used by Network Agent to monitor Internet traffic and send protocol block messages.

Note

If the selected NIC will be used by Network Agent, it must support promiscuous mode.

Active Directory Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This installer screen appears if you are installing User Service, DC Agent, or Logon Agent on Windows Server.

Indicate whether you are using Active Directory to authenticate users in your network and then click **Next**.

Computer Browser Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This installer screen appears if all the following are true:

- Installing User Service, DC Agent, or Logon Agent on Windows Server
- Using Active Directory
- Windows Computer Browser service is not currently running.
  Choose whether to start this service and then click **Next**.

The Computer Browser service is a Windows utility that must be set to Automatic and Start in the Windows Services tool for user identification components to communicate with Active Directory.

Note

If you choose to start the Computer Browser service now, make sure the Computer Browser service is enabled on this machine. In most cases, it is disabled by default. The installer will attempt to start the service and configure it to start up automatically from now on. If the service is disabled, the installer will be unable to start it.

If you choose not to have the installer start the service, or if the installer is unable to start it, you must start it manually after installation. If you use Active Directory to authenticate users, you must also start the Computer Browser service on the Active Directory machine. See *Turning on the Computer Browser service*.

Related tasks

Turning on the Computer Browser service on page 171

Integration Option Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This screen appears if Filtering Service is selected for installation.

Indicate whether this is a standalone or integrated installation, then click **Next**.

- **Install Forcepoint Web Security to connect to Content Gateway**: Content Gateway is responsible for monitoring Internet requests, forwarding them to Filtering Service, and performing real-time analysis.
- **Install Forcepoint Web Security or Forcepoint URL Filtering in standalone mode (no real-time analysis)**: Network Agent is responsible for monitoring Internet requests and forwarding them to Filtering Service for evaluation. Network Agent also sends block messages.

  Note

  To enable standalone mode, Network Agent must be installed in your network.

- **Install Forcepoint URL Filtering to integrate with a third-party product or device**: A third-party firewall, proxy server, cache, or network appliance (integration product) is responsible for monitoring Internet requests and sending them to Filtering Service for evaluation. Supported integration options include:
  - Cisco ASA or routers
  - Citrix
  - ICAP Service
  - Microsoft Forefront TMG
  - Other supported integration (as a “universal” integration)

In an integrated environment, Filtering Service sends block pages, if necessary, to users attempting to access blocked content. Network Agent can optionally be used to manage requests on Internet protocols not managed by the integration product (for example, protocols for instant messaging).

If you select this option, the next screen prompts you to identify which integration product you are using.

Select Integration Screen

Applies to:

- Forcepoint URL Filtering, v8.5.x

This installer screen appears if you selected **Install Forcepoint URL Filtering to integrate with a third-party product or device** in the *Integration Option Screen*.

Select your integration product and then click **Next**.

(Windows only) If you selected Filtering Plug-In for installation, the **Select Integration** screen shows 2 options: Microsoft Forefront TMG or Citrix. For more information, see:

- *Integrating Forcepoint URL Filtering with Citrix*
- *Integrating Forcepoint URL Filtering with TMG*

Related concepts

Integration Option Screen on page 164
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with TMG on page 221

Network Card Selection Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This screen appears if Network Agent is selected for installation, even if the machine only has one network interface card (NIC).

Select the NIC that Network Agent should use to communicate with other web protection components, then click **Next**.

- All enabled NICs with an IP address are listed.
- On Linux, NICs without an IP address are also listed. Do not choose a NIC without an IP address. After installation, you can configure Network Agent to use NICs without an IP address to monitor Internet requests. See *Network Agent and stealth mode NICs*.

Note

For Network Agent to operate, this machine must be connected to a bi-directional span port (or mirror port) on a switch or hub that processes the network traffic to be monitored.

You may select multiple NICs. After installation, use the Web Security module of the Forcepoint Security Manager to configure how Network Agent will use each selected NIC (for more information, see the Administrator Help for your web protection solution).

Related concepts
Network Agent and stealth mode NICs on page 339

Database Information Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This installer screen appears if Log Server is selected for installation and Forcepoint Infrastructure is not installed on this machine.

Enter the hostname or IP address of the machine on which a supported database engine is running (see *System requirements for this version* for supported database system information). 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 Forcepoint Security 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 Security Manager. See Configuring Apache services to use a trusted connection.
- Select **Database account** 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 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.

Related reference
System requirements for this version on page 9

Log Database Location Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This installer screen appears if Log Server is selected for installation.

Accept the default location for the Log Database files, or select a different location. Then, click **Next**.

Note that if Forcepoint Infrastructure is installed on this machine, the default database location information is taken from infrastructure 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.

Optimize Log Database Size Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This installer screen appears if Log Server is selected for installation.

The options on this screen allow you to control the size of the Log Database, which can grow quite large. 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

Feedback Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This screen appears if Filtering Service or Network Agent is selected for installation.

As a best practice, allow your software to send feedback, then click **Next**.

Sending feedback helps improve the accuracy of policy enforcement for all customers. Information is sent about security URLs and any URLs that could not be categorized. Uncategorized URLs are evaluated and, if warranted, added to a Master Database category.

No information about users or your network is collected. The information is only about the visited URLs themselves. Only uncategorized URLs and the frequency of requests to them are collected. Uncategorized intranet URLs are not included in feedback.

Note

You can later enable or disable feedback (WebCatcher) on the **Settings > General > Account** page in the Web Security module of the Forcepoint Security Manager.

Directory Service Access Screen

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

This screen appears if User Service, DC Agent (Windows only), or Logon Agent is selected for installation.

Enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller.

- This must be the domain controller whose directory includes the users to whom you plan to apply user- or group-based policies.
- User Service uses this account to query the domain controller for user information.

Note

User information on domain controllers trusted by the domain controller in question will also be accessible.

If you choose not to specify a Domain Admin account now (by leaving the fields blank), you can specify it after installation:

- On Linux, specify a Domain Admin account to be used by User Service. For more information, see the Administrator Help for your web protection solution.
- On Windows, configure the User Service service to log on as a Domain Admin user:

  1) Open the Windows Services tool.

  2) Right-click **Websense User Service** and select **Properties**, then click the **Log On** tab.

  3) Under **Log on as**, select **This account** and enter the domain\username and password (twice) of the trusted account you specified during installation.

  4) Click **OK**.

  5) A message appears informing you the account you specified has been granted the Log On As A Service right. Click **OK**.

  6) A message appears informing you the new logon name will not take effect until you stop and restart the service. Click **OK**, then click **OK** again.

  7) Right-click **Websense User Service** and select **Restart**.

Remote Filtering Communication Screen

Applies to:
■ Forcepoint URL Filtering, v8.5.x

This screen appears if Remote Filtering Server is selected for installation. Remote Filtering Service is available to Forcepoint URL Filtering customers who have purchased the Remote Filter module.

The external IP address or hostname of the firewall or gateway must be visible from outside the network. If you enter a hostname, it must be in the form of a fully-qualified domain name:

```
machine_name.domain_name
```

- Remember whether you entered an IP address or a hostname here. When installing Remote Filtering Client on user machines, you must enter this address in the same form (IP address or name).
- It is a best practice to use IP addresses, rather than hostnames, unless you are confident of the reliability of your DNS servers. If hostnames cannot be resolved, Remote Filtering Clients cannot connect to Remote Filtering Server.

The external communication port can be any free port in the range 10-65535 on this machine. This port receives HTTP/HTTPS/FTP requests from external Remote Filtering Client machines (i.e., user machines, running Remote Filtering Client, outside the network). The default is 80. If a web server is running on this machine, it may be necessary to use a different port.

Note

The external network firewall or gateway must be configured to route traffic, typically via PAT or NAT, from Remote Filtering Client machines to the internal IP address of this machine.

The internal communication port can be any free port in the range 1024-65535 on this machine. The default is 8800. This is the port to which remote client heartbeats are sent to determine whether a client machine is inside

or outside the network. The external network firewall must be configured to block traffic on this port. Only internal network connections should be allowed to this port.

For more information, see the Deploying the Remote Filter Module technical paper.

Remote Filtering Pass Phrase Screen

Applies to:
■ Forcepoint URL Filtering, v8.5.x

This screen appears if Remote Filtering Server is selected for installation.

The pass phrase can be any length. This pass phrase is combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

If you want this instance of Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.

The pass phrase must include only ASCII characters, but cannot include spaces. Do not use extended ASCII or double-byte characters.

You must use this pass phrase when you install the Remote Filtering Client on user machines that will connect to this Remote Filtering Server.

Filtering Service Information for Remote Filtering Screen

Applies to:
■ Forcepoint URL Filtering, v8.5.x

This installer screen appears if Remote Filtering Server is selected for installation.

- **Internal IP address**: Enter the actual IP address of the Filtering Service machine to be used by this instance of Remote Filtering Server.
- **Communication port and Block page port**: The port Filtering Service uses for communication with other components (15868, by default), and the port used to serve block pages to client machines (15871, by default). These ports must:
  - Be in the range 1024-65535
  - Open on any firewall between the Remote Filtering Server and Filtering Service

  To find the ports used by Filtering Service:

  1) Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security \bin or /opt/Websense/bin/, by default) and open the **eimserver.ini** file in a text editor.
  2) Locate the **WebsenseServerPort** (filtering port) and **BlockMsgServerPort** (block page port) values.
  3) When you are finished, close the file without saving. Do **not** modify the file.

- **Translated IP address**: Use this box to provide the translated IP address of Filtering Service if it is behind a network-address-translating device. You must mark the **A firewall or other network device performs address translation...** check box to enable this option.

Turning on the Computer Browser service

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

The Forcepoint Security Installer offers the option to turn on the Computer Browser service during installation of the following components:

- User Service
- DC Agent
- Logon Agent

If you chose not to have it started, or the installer was not successful, you must turn on the service manually.

In addition, if your network uses Active Directory to authenticate users, the Windows Computer Browser service must be running on the Active Directory machine. Note that the Windows Firewall must be turned off in order for the Computer Browser service to start.

Perform the following procedure on each machine running an affected component:

Steps

1) Make sure that Windows Network File Sharing is enabled.
   a) Go to **Start > Control Panel > Network and Sharing Center**.
   b) In the **Sharing and Discovery** section, set **File Sharing** to **On**.
2) Go to **Control Panel > Administrative Tools > Services**.
3) Double-click **Computer Browser** to open the Properties dialog box.
4) Set the **Startup type** to **Automatic**.
5) Click **Start**.
6) Click **OK** to save your changes and close the Services dialog box.
7) Repeat these steps on each machine running Windows Server and an affected component.

Installing with SQL Server

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

See *System requirements for this version* for which versions of SQL Server are supported.

Steps

1) Install SQL Server according to Microsoft instructions, if needed.

2) Make sure SQL Server is running.

3) Make sure SQL Server Agent is running.

Note

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

4) Obtain the SQL Server logon ID and password for a SQL Server Administrator, or for an account that has the following permissions:

   - db_creator server role
   - SQLAgent role
   - db_datareader in msdb

   For Forcepoint DLP, Forcepoint Email Security, or Forcepoint Web Security with the Web DLP module, the account must have a **sysadmin** role.

   You need this logon ID and password when you install Forcepoint reporting components.

5) Restart the SQL Server machine after installation.

Note

You must restart the machine after installing Microsoft SQL Server and before installing Log Server.

6) Make sure the Security Manager machine and, if applicable, Log Server machine or machines can recognize and communicate with SQL Server.

7) Install the SQL Server client tools on the Security Manager machine. Run the SQL Server installation program, and select **Connectivity Only** when asked what components to install.

   If Log Server is installed on another machine, install the SQL Server client tools on that machine instead.

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

Related reference
System requirements for this version on page 9

Configuring Microsoft SQL Server user roles

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

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

To install Log Server successfully, the user account that owns the reporting database must have one of the following membership roles in the **msdb** database and **db_datareader**:

- SQLAgentUserRole
- SQLAgentReader Role
- SQLAgentOperator Role

The SQL user account must also have **dbcreator** fixed server role privilege. The Forcepoint Email Security user account must have **sysadmin** fixed server role privilege.

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

Steps

1) On the SQL Server machine, go to **Start > Programs > Microsoft SQL Server > Microsoft SQL Server Management Studio**.

2) Log into SQL Server as a user with SQL sysadmin right.

3) Select the **Object Explorer** tree, and then go to select **Security > Logins**.

4) Select the login account to be used during the installation.

5) Right-click the login account and select **Properties** for this user.

6) Select **Server Roles**, and then select **dbcreator**. For Forcepoint DLP, Forcepoint Email Security, and Forcepoint Web Security with the Web DLP module, also select **sysadmin**.

7) Select **User Mapping** and do the following:
   a) Select **msdb** in database mapping.

b) Grant membership to one of these roles:
   - SQLAgentUserRole
   - SQLAgentReader Role
   - SQLAgentOperator Role and also to:
   - db_datareader

c) Select **wbsn-data-security** in database mapping and mark it as “db_owner”.

d) Select **wbsn-data-security-temp-archive** in database mapping and mark it as “db_owner”.

e) Click **OK** to save your changes.

8) Click **OK** to save your changes.

Installing Forcepoint DLP components

Before you begin

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

You use the same Forcepoint Security Installer to install most Forcepoint DLP components as you do to install the Forcepoint Security Manager and Forcepoint Infrastructure. The Forcepoint Security Manager cannot be installed separately from the Forcepoint Infrastructure.

If you plan to install a Forcepoint DLP component, the Forcepoint components must already be installed in your network along with the Forcepoint management server software. See *Creating a Forcepoint management server*.

Important

If you plan to install Forcepoint Email Security, you must install Forcepoint DLP in order to access and configure email DLP functions in the Data Security module.

To install an additional Forcepoint DLP component:

Steps

1) Launch the Forcepoint Security Installer on the appropriate machine.

2) Choose the Custom installation type.

3) Click the **Install** link for Forcepoint DLP.

4) Select the agent to install when prompted to select a component.

Next steps

Not all Forcepoint DLP components may show in the **Select Components** screen. The components that are offered depends on the operating system of the machine and applications detected by the installer.

The **Crawler Agent**: scans networks transparently to locate confidential documents and data on endpoints, laptops and servers. It also performs fingerprinting, and scans databases as well as documents.

For instructions on installing each agent, refer to Installing Forcepoint DLP Servers and Agents. Each agent has prerequisites and best practices that must be followed.

This chapter also describes how to install Linux-based components such as the protector and mobile agent.

Related reference
Creating a Forcepoint management server on page 118

Installing email protection components

Forcepoint Email Security is an appliance-based solution. All components run on the appliance, except the Email Security module of the Forcepoint Security Manager and the Email Log Server. These are the only two email protection components that may be installed using the Forcepoint Security Installer.

Before you begin

Important

You should have already installed Forcepoint DLP, which you need in order to access and configure email DLP functions in the Data Security module.

Applies to:
■ Forcepoint Email Security, v8.5.x

Steps

1) It is assumed you have already launched the Forcepoint Security Installer and chosen the Custom installation type. If not, see Deployment section in *Installing components via the Custom option*.

2) On the **Custom Installation** dashboard, click the **Install** link for email protection solutions.

3) The email protection component installer is launched.

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

5) If the installer detects Forcepoint Infrastructure on this machine, it operates as if it is part of a Forcepoint Security Manager installation. See *Installing the Email Security module of the Security Manager* for instructions.

   If Forcepoint Infrastructure is not detected, then the installer operates in custom mode.

6) In the **Select Components** screen, specify whether you want to install the Email Log Server.

   Email Log Server is selected for installation by default. To install the Email Log Server, SQL Server or SQL Server Express must already be installed and running in your network. (See *System requirements for this version* for supported database systems.)

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

7) If Forcepoint Infrastructure is not found already installed on this machine, the **Email Log Database** screen appears. Specify the location of a database engine and how you want to connect to it.

   - **Log Database location**: Enter the IP address or hostname of the database engine machine. If you want to use a named database instance, enter in the form <*IP address*>\<*instance name*>. The instance must already exist. See your SQL Server documentation for instructions on creating instances.
     If you chose to install SQL Server Express as part of the installation of the Security Manager (when available), the log database IP address should be that of the Security Manager machine.

     Starting in version 8.5.4, more stringent connection string and certificate requirements are needed for establishing an encrypted connection with a SQL Server. Using an IP address is no longer supported for encrypted connections; you must use a hostname or a fully qualified domain name (FQDN) that matches the Common Name (CN) field on the certificate used by SQL Server, if using an encrypted database connection.
   - You may specify whether the connection to the database should be encrypted.
     If you are using an encrypted connection, ensure that you use a hostname or FQDN for your Email Log Database that matches the CN field on the certificate that SQL Server is using.

     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 Forcepoint appliance to the Log Database 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.
     - **Windows authentication**: 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.

8) On the **Email Database File Location** screen, specify where database files should be located and then click **Next**.

This screen appears only if you chose to install the Email Log Server.
A default location for the Log Database is automatically shown. Information about the location of the database engine and connection credentials were entered when Forcepoint Infrastructure and Forcepoint Email Security were installed on this machine. The installer reads this information from configuration files created by Forcepoint Security Setup.

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 protection components (e.g., the Security Manager Email Security module 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 protection 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.

DANGER

Any email traffic log data that has been written to the database will be lost if you remove the database. If you want to keep this data, back up the esglogdb7x and esglogdb7x_n databases. See your SQL Server documentation for backup instructions.

DANGER

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

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

Note

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.

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

11) The **Installing Email Protection Solutions** screen appears, as components are being installed.

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

Related concepts
Installing components via the Custom option on page 149

Related tasks
Installing with SQL Server on page 172

Related reference
Installing the Email Security module of the Security Manager on page 125
System requirements for this version on page 9

Installing SQL Server Express (without Forcepoint Infrastructure)

Before you begin

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x

Important

Forcepoint has removed the ability to install SQL Server Express as an option for new deployments of Forcepoint Security Manager. This change was made via a revised version of Forcepoint Security Installer introduced in July 2019, which can be found on the Downloads page. The change was required to reduce the risk of deploying SQL Server Express without the latest security updates. Forcepoint Security Manager still supports and will work with the latest version of SQL Server Express. You may use SQL Server Express for small deployments, but it must be installed independently.

During installation, you can choose to install SQL Server Express. This section provides instructions for installing SQL Server Express without installing Forcepoint Infrastructure. Typically, this is done to install SQL Server Express on a machine that is not a Forcepoint management server.

Steps

1) If you will use SQL Server Express to store and maintain reporting data, log in to the machine as domain user. Do this prior to starting the Forcepoint Security Installer.

2) It is a best practice to install the Windows prerequisites for installing SQL Server Express beforehand:
   - .NET Framework 3.5 SP1.NET 4.5 is also required by the installer so make sure this is installed as well.
   - Powershell 1.0
   - Windows Installer 4.5

   Note

   The installer will automatically install these if not found on the machine.

   See SQL Server Express section in *Preparing for installation*.

3) It is assumed you have already launched the Forcepoint Security Installer and chosen the Custom installation type. If not, see *Starting a custom installation (Windows)*.

4) On the **Custom Installation** dashboard, click the **Install** link for SQL Server Express.

5) On the **Welcome** screen, click **Start** to begin the installation wizard.

6) On the Configuration screen, select options as described below and then click **Next**.
   - Use the **Browse** button to specify a different folder if you do not want to install to the default location shown.
   - If you want to create a named instance, instead of using the default SQL Server instance, select **Named instance** and then enter an instance name. Note the following about instance names:
     - Not case sensitive
     - 16 characters or less
     - Only letters, numbers, dollar sign ($), or underscore (_) are allowed
     - First character must be a letter
     - Cannot contain the term *Default* or other reserved keyword (see Microsoft documentation for more information about reserved keywords)
   - Select an authentication mode:
     - **Windows Authentication mode**: select this to use Windows authentication, i.e., trusted connection, to authenticate users.
     - **Mixed Mode (SQL Server authentication and Windows authentication)**: select this to use SQL Server authentication. Enter a password (and re-enter to confirm) for the built-in SA user.

   Depending on your selections, the Pre-Installation Summary screen, will show different information than shown in the above illustration.

   CAUTION

   Depending on whether certain Windows prerequisites are installed, your machine may be automatically restarted up to two times during the installation process. Restarts are not required if the prerequisites are already installed.

7) In the **Pre-Installation Summary** screen, click **Next** to begin installation.

   The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.
   Note that it may take approximately 10–15 minutes for the SQL Server Express installation to complete.

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

9) On the Summary screen, click **Finish**.

Related tasks
Starting a custom installation (Windows) on page 151

Related reference
Preparing for installation on page 19

Chapter 15

Installing Forcepoint F1E Solutions

Forcepoint F1E solutions provide complete real-time protection against advanced threats and data theft for both network and roaming users. Forcepoint advanced technologies help you discover and protect sensitive data stored on endpoint machines and provide actionable forensic insight into potential attacks.

Applies to:

- Forcepoint URL Filtering, Forcepoint Web Security, and Forcepoint Web Security with the Web Hybrid module, v8.4.x and higher
- Forcepoint Web Security Cloud
- Forcepoint DLP, v8.5.x and higher
- Forcepoint Next Generation Firewall, v6.5 and higher
- Forcepoint CASB

- **Forcepoint Web Security Endpoint** protects users from web threats on Windows and Mac endpoint machines. Forcepoint offers three Forcepoint Web Security Endpoint options:
  - **Forcepoint Web Security Direct Connect Endpoint**: Requires a Forcepoint Web Security v8.4 (or higher) on-premises solution with the Hybrid Module or Forcepoint Web Security Cloud.
  - **Forcepoint Web Security Proxy Connect Endpoint**: Requires a Forcepoint Web Security v8.4 (or higher) on-premises solution with the Hybrid Module or Forcepoint Web Security Cloud.
  - **Remote Filtering Client**: Requires Forcepoint URL Filtering v8.4 (or higher) with the Remote Filter module.
- **Forcepoint CASB Endpoint** protects organizations from cloud application-based threats. It identifies and remediates sensitive data sent or received through both managed and unmanaged cloud applications accessed through the organization's network. Requires a Forcepoint CASB license.
- **Forcepoint DLP Endpoint** protects organizations from data loss and data theft. It also identifies and remediates sensitive data stored on corporate endpoint machines, including Windows and Mac laptops. Requires Forcepoint DLP Network v8.5 (or higher) or Forcepoint Data Discovery v8.5 (or higher).
- **Forcepoint Endpoint Context Agent** (Forcepoint ECA) collects per-connection user and application information about Windows endpoint machines that connect through a Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine managed by the Security Management Center (SMC). Forcepoint ECA is only available for Windows endpoint machines. Requires Forcepoint NGFW v6.5 (or higher).

The package builder is used by Enterprise IT team members to generate the Forcepoint F1E installation packages that will be installed on Windows and Mac endpoint machines.

The Forcepoint F1E package builder supports the configuration and creation of the following Forcepoint F1E and conventional Forcepoint Endpoint agents:

- Forcepoint DLP Endpoint on Windows and Mac (Forcepoint F1E)
- Forcepoint Web Security Endpoint:
  - Forcepoint Proxy Connect Endpoint on Windows and Mac (Forcepoint F1E)
  - Forcepoint Direct Connect Endpoint on Windows and Mac (Forcepoint F1E)
  - Remote Filtering Client on Windows and Mac (Conventional Forcepoint Endpoint)
- Forcepoint ECA on Windows only (Forcepoint F1E)

- Forcepoint CASB Endpoint on Windows only (Forcepoint F1E)

The Forcepoint F1E platform places all installed Forcepoint F1E agents under one icon in the notification area of the task bar (Windows) or the status menu of the menu bar (Mac), instead of under separate icons for each agent. The Forcepoint F1E agents share the same functionality as the older, conventional Forcepoint Endpoint agents.

Starting with Forcepoint DLP v8.6, Forcepoint DLP Endpoint on the Forcepoint F1E platform is the standard agent for Forcepoint DLP (Windows and Mac) and Forcepoint Dynamic Data Protection (Windows and Mac).

Starting with Forcepoint Web Security v8.5, Forcepoint Web Security Endpoint on the Forcepoint F1E platform is the standard agent for Forcepoint Web Security on Windows and Mac.

For more information about Forcepoint F1E solutions, see:

- Installation and Deployment Guide for Forcepoint F1E Solutions
- Upgrade Guide for Forcepoint F1E Solutions
- End User Guide for Forcepoint F1E Solutions

Chapter 16

Integrating Forcepoint URL Filtering with Cisco

Contents

Forcepoint URL Filtering can be integrated with Cisco™ Adaptive Security Appliance (ASA) v8.0 and later and Cisco IOS routers v15 and later.

Applies to:

- Forcepoint URL Filtering, v8.5.x

Integrating with a Cisco product involves the following components:

- **Filtering Service** works with the Cisco product and Network Agent to respond to Internet requests.
  For redundancy, two or more instances of Filtering Service may be used. Only one instance (the primary server) is active at any given time. URL look-up requests are be sent only to the primary server.
- **Network Agent** manages Internet protocols that are not managed by your integrated Cisco product. Network Agent can log bandwidth data for reporting block Internet requests based on bandwidth consumption.
- If HTTP(S) or FTP authentication is enabled in the Cisco product, **User Service** must be installed in the same domain or root context as authenticated users to get correct user information and provide it to Filtering Service for accurate application of user-based policies.
  If you are using a transparent identification agent or manual authentication, this configuration is not necessary.

To enable the integration, direct Internet requests through your Cisco product, and configure it for use with Forcepoint URL Filtering.

- *Getting started with a Cisco integration* provides general introductory information.
- *Configuring a Cisco Security Appliance* discusses Cisco Adaptive Security Appliance (ASA).
- *Configuring a Cisco IOS Router* discusses Cisco IOS router.

Related concepts
Getting started with a Cisco integration on page 186
Configuring a Cisco Security Appliance on page 189
Configuring a Cisco IOS Router on page 197

Deployment considerations for integration with Cisco products

Applies to:
■ Forcepoint URL Filtering, v8.5.x

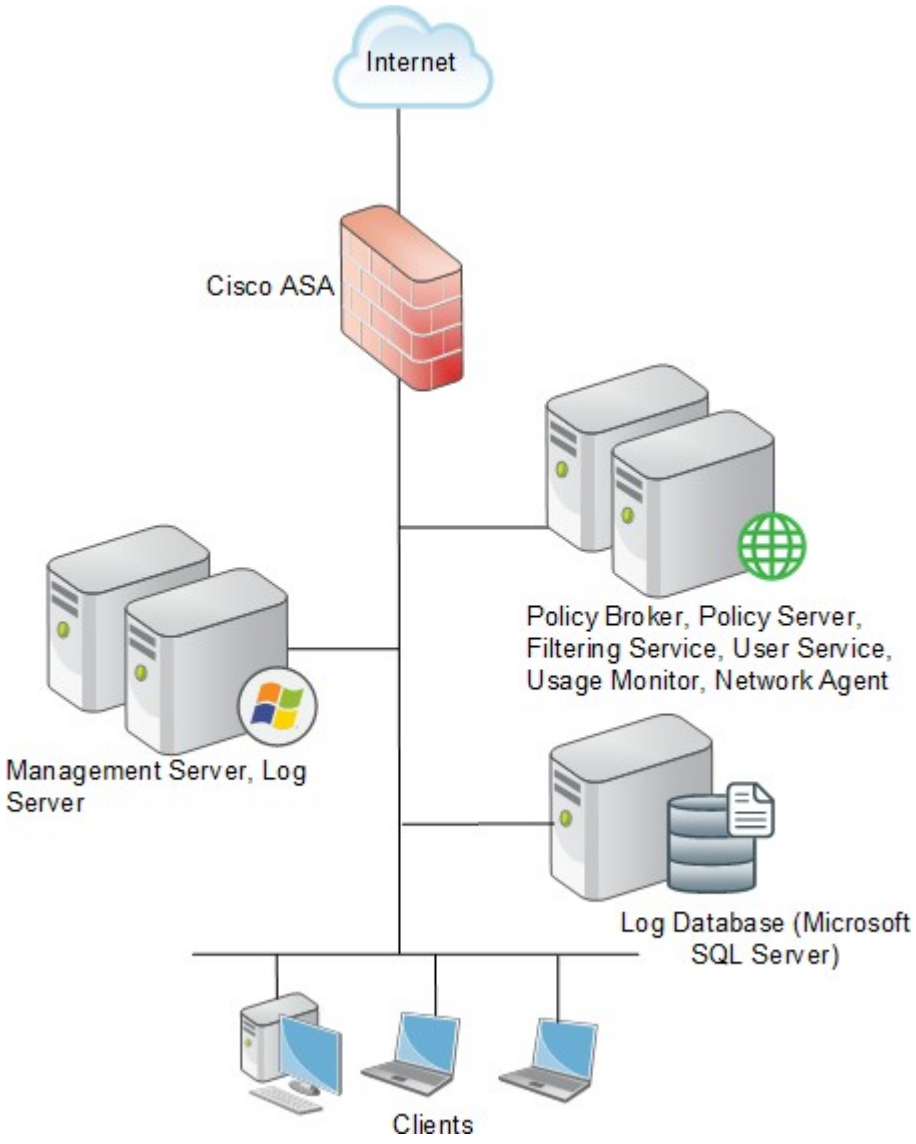
Cisco ASA

A simple and common network topology places web policy enforcement components on a single machine, or group of dedicated machines, communicating with a Cisco Adaptive Security Appliance (ASA) via TCP/IP.

- Forcepoint Security Manager and reporting components are installed on separate Windows machines.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

See *Integrating Forcepoint URL Filtering with Cisco* for configuration instructions.

Other configurations are possible. See your Cisco ASA documentation and the information in this section to determine the best configuration for your network.



The diagram provides a general overview and best practice location for your integration product, but does not show all components. Larger networks require components to be distributed across several dedicated machines.

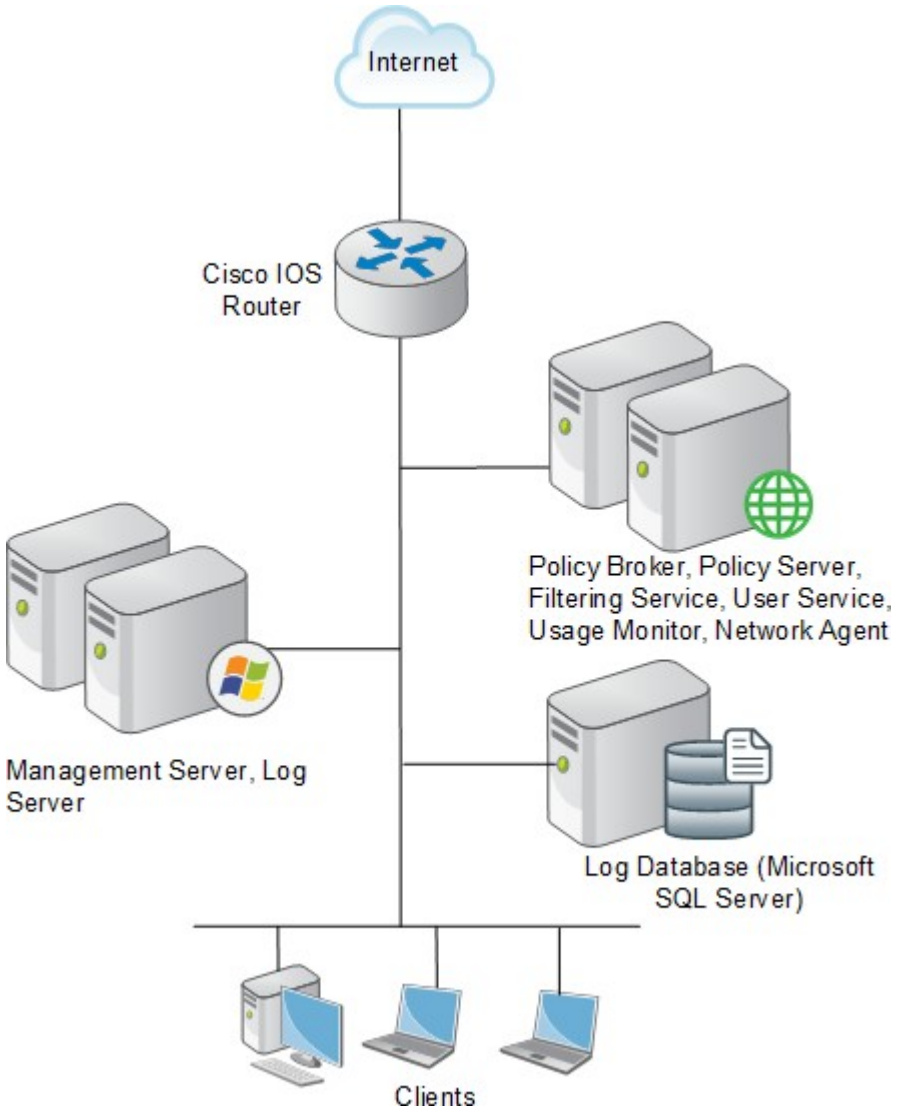
Cisco IOS Routers

In this common configuration, web policy enforcement components are installed on a single machine, communicating with the Cisco IOS Router.

- Forcepoint Security Manager and reporting components are installed on separate Windows machines.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

The router has firewall functionality and can be used with or without an accompanying firewall.

If the Cisco IOS Router is used with a separate firewall, ensure that all Internet traffic is configured to pass through the router and is not set to bypass the router and go directly to the firewall. Traffic that bypasses the router cannot be managed by Forcepoint URL Filtering.



Other configurations are possible. See your Cisco Router documentation and the information in this chapter to determine the best configuration for your network.

The diagram provides a general overview and best practice location for your integration product, but does not show all components. Larger networks require components to be distributed across several dedicated machines.

Related concepts
Integrating Forcepoint URL Filtering with Cisco on page 183

Getting started with a Cisco integration

Applies to:
■ Forcepoint URL Filtering, v8.5.x

How does Forcepoint URL Filtering work with Cisco products

To be managed by your web protection software, a client's Internet requests must pass through the Cisco product.

When it receives an Internet request, the Cisco product queries Filtering Service to find out if the requested website should be blocked or permitted. Filtering Service determines which policy or exception applies to the request, then uses that policy to decide whether to block or permit the request.

- For HTTP, if the site is blocked, the browser displays a block page instead of the requested site.
- For HTTPS or FTP, if the site is blocked, the user is denied access and receives a blank page.
- If the site is permitted, Filtering Service notifies the Cisco product that the site is not blocked, and the client is allowed to visit the site.

Installing Forcepoint URL Filtering

Install Forcepoint URL Filtering as directed in the Installation Guide. When installing Filtering Service, be sure to:

- On the **Integration Option** screen, select **Install Forcepoint URL Filtering to integrate with a third-party product or device**.
- On the **Select Integration** screen, select one of the following and then click **Next**:
  - **Cisco Adaptive Security Appliances**
  - **Cisco Routers**
- Do not install a transparent identification agent if you plan to configure user authentication through your Cisco product.

Upgrading Forcepoint URL Filtering

When you upgrade software that is already integrated with a Cisco product, no additional Cisco configuration is necessary. See *Upgrading Web Protection Solutions* for upgrading instructions.

If you are upgrading your deployment and changing your Cisco product, see Migrating between integrations after installation.

Migrating between integrations after installation

You can change the Cisco integration product (for example, change from ASA to an IOS router) after installing web protection software without losing configuration data.

1) Install and configure your new Cisco integration product. See Cisco documentation for instructions. Ensure that it is deployed so that it can communicate with Filtering Service.

2) Use the Backup Utility to back up configuration and initialization files. For instructions see:
   - v7.6 - v7.8 Backup and Restore FAQ (if you are preparing to upgrade to v8.x)
   - v8.0 - v8.1 Backup and RestoreFAQ
   - v8.2 Backup and Restore FAQ
   - v8.3 Backup and Restore FAQ

- v8.4 Backup and Restore FAQ
- v8.5 Backup and Restore FAQ (if you are preparing to upgrade to v8.5.x)

3) Close all applications on the Filtering Service machine, and stop any antivirus software.

4) Remove Filtering Service. See *Removing web protection components* for instructions.

5) Restart the machine (Windows only).

6) Use the Windows or Linux installer to reinstall Filtering Service. See *Installing web protection components* for instructions.

7) On the **Select Integration** screen, select the new Cisco product, and then follow the on-screen instructions to complete the installation.
The installer adds the new integration data to the appropriate configuration files, while preserving existing configuration data.

8) Restart the machine (Windows only).

9) Check to be sure that Filtering Service has started.
   - Windows: Use the Windows Services tool to verify that **Websense Filtering Service** has started.
   - Linux: Navigate to the web protection installation directory (/opt/Websense, by default), and use the following command to verify that **Websense Filtering Service** is running:
     `./WebsenseAdmin status`

10) Use the Forcepoint Security Manager to identify which Filtering Service instance is associated with each Network Agent.
    - Use a supported browser (see *System requirements for this version*) to go to **https://<IP address>:9443**.
      Here, *<IP address>* is the IP address of the management server.
    - Click the **Web** module, then go to **Settings > Network Agent**.
    - Position the mouse over the **General** option and wait a second or two for a list of IP addresses to appear.
    - Click an IP address to open the **Local Settings** page for that Network Agent instance.
    - Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.
    - Log off of the Security Manager.

11) If you stopped your antivirus software, be sure to start it again.

Network Agent enhanced logging

Network Agent can also provide information for reports on bandwidth information and block HTTP(S) Internet protocols based on bandwidth consumption. However, bandwidth information is not recorded by default.

To configure Network Agent to record bandwidth information for reporting, or manage HTTP(S) or FTP requests based on bandwidth consumption:

1) In a supported browser, navigate to **http://<IP address>:9443**, where <*IP address*> is the IP address of the management server.

2) Select the **Web** module, then go to **Settings** > **Network Agent**.

3) Position the mouse over the **General** option and wait a second or two for a list of IP addresses to appear.

4) Click appropriate IP address to open the **Local Settings** page for a Network Agent instance.

5) Under **Network Interface Card**, click the appropriate NIC monitoring the relevant traffic.

6) Under **Integration**, enable the Log HTTP requests option.

Related concepts
Upgrading Web Protection Solutions on page 261
Removing web protection components on page 350

Related tasks
Installing web protection components on page 157

Related reference
System requirements for this version on page 9

Configuring a Cisco Security Appliance

Applies to:

- Forcepoint URL Filtering, v8.5.x

After Forcepoint URL Filtering is installed, the Cisco Adaptive Security Appliance (ASA) must be configured to work with the web protection software. The Cisco firewall passes each Internet request to Filtering Service, which analyzes the request and determines whether to block or permit access, or limit access by using quotas set in web policies.

See your Administrator Help for information about implementing policies.

For information about configuring integration with ASA through a console or telnet session, see:

- Cisco integration configuration procedure
- User-based policies and Cisco integration

For information on configuring your security appliance through the management interface, see the documentation for your Cisco product, available at www.cisco.com.

Related concepts
User-based policies and Cisco integration on page 197
Cisco integration configuration procedure on page 190

Cisco integration configuration procedure

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Configuration procedure

To configure your security appliance to send Internet requests to Filtering Service for policy enforcement:

1) Access the security appliance from a console or from a remote terminal using telnet for access

2) Enter your password.

3) Enter **enable**, followed by the enable password to put the security appliance into privileged EXEC mode.

4) Enter **configure terminal** to activate configure mode.

> **Note**
>
> For help with individual commands, enter **help** followed by the command. For example, **help filter** shows the complete syntax for the **filter** command and explains each option.

5) Use the **url-server** command to enable URL management by your web protection software.

```
url-server (<if_name>) vendor websense host <ip_address> [timeout <seconds>]
[protocol {TCP | UDP} version {1 | 4} [connections <num_conns>]]
```

The **url-server** command takes the following parameters:

Parameter	Definition
(<if_name>)	(required) The network interface to use for Filtering Service communication. You must type the parentheses ( ) when you enter a value for this parameter.
vendor websense	Indicates the URL management vendor.
<ip_address>	IP address of the machine running Filtering Service.

Parameter	Definition
timeout <seconds>	The amount of time, in seconds, that the security appliance waits for a response before switching to the next Filtering Service that you defined as a **url-server**, or, if specified, going into allow mode and permitting all requests. If a timeout interval is not specified, this parameter defaults to 30 seconds. Range: 10 - 120; Default: 30
protocol {TCP | UDP} version {1 | 4}	Defines whether the Cisco security appliance should use TCP or UDP protocol to communicate with Filtering Service, and which version of the protocol to use. **TCP** is the recommended and default setting. The recommended protocol version is **4**. The default is 1. **Note:**To send authenticated user information to Filtering Service, TCP version 4 must be selected.)
connections <num_conns>	Limits the maximum number of TCP connections permitted between the Cisco security appliance and Filtering Service. If this parameter is not specified, it defaults to **5**, which is the recommended setting. If you select the UDP protocol, this option is not available. Range: 1 - 100; Default: 5.

Example:

```
url-server (inside) vendor websense host 10.255.40.164 timeout 30 protocol TCP
version 4 connections 5
```

The **url-server** command communicates the location of Filtering Service to the Cisco security appliance. More than one **url-server** command can be entered. Multiple commands allow redirection to another Filtering Service after the specified timeout period, if the first server becomes unavailable.

6) Configure the security appliance to filter HTTP requests with the **filter url** command.

- To review the current URL server rules, enter **show running-config url- server**.
- To review all the filter rules, enter **show running-config filter**.

To configure HTTP request management, use the following command:

```
filter url http <port>[-<port>] <local_ip> <local_mask> <foreign_ip>
<foreign_mask> [allow] [cgi-truncate] [longurl-truncate | longurl-deny]
[proxy-block]
```

For an explanation of the **filter url** parameters, see Parameters for the filter commands.

Examples:

Command example	Action
filter url http 0 0 0 0	Manages every HTTP request to all destinations. Applied to traffic on port 80.
filter url http 10.5.0.0 255.255.0.0 0 0	Manages the 10.5.x.x network going to any destination. Applied to traffic on port 80.
filter url http 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255	Manages the 10.5.0.69 host going to the 132.239.29.189 destination. Applied to traffic on port 80.

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows the specified local IP address to request all websites, governed by web protection policies.

You can enter multiple **filter url** commands to set up different portions of the network for policy enforcement. Set up the smaller groups first, followed by the larger groups, to assure that all groups receive the correct policies. Use a general **filter url** command for all computers to be managed, and then use the Forcepoint Security Manager to apply policies to individual clients (by IP address, user name, group, or OU).

See the Administrator Help for information about creating and applying policies.

7) Configure the security appliance to filter HTTPS requests with the **filter https** command.

- To review the current URL server rules, enter **show run url-server**.
- To review all the filter rules, enter **show run filter**.
- Enter **exit** to go up a level to run the show command.

To configure HTTPS request management, use the following command:

```
filter https <port> <local_ip> <local_mask> <foreign_ip> <foreign_mask>
[allow]
```

For an explanation of the **filter https** parameters, see Parameters for the filter commands.

Examples:

Command example	Action
filter https 443 0 0 0 0	Manages all HTTPS requests to all destinations. Applied to traffic on port 443.
filter https 443 10.5.0.0 255.255.0.0 0 0	Manages the 10.5.x.x network going to any destination. Applied to traffic on port 443.
filter https 443 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255	Manages the 10.5.0.69 host going to the 132.239.29.189 destination. Applied to traffic on port 443.

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows the specified local IP address to request all websites, governed by web protection policies.

You can enter multiple **filter https** commands to set up different portions of the network for policy enforcement. Organize the commands as described above for **filter url**.

8) Configure the Cisco security appliance to filter FTP requests with the **filter ftp** command.

- To review the current URL server rules, enter **show run url-server**.
- To review all the filter rules, enter **show run filter**.
- Enter **exit** to go up a level to run the **show** command.

To configure FTP request management, use the following command:

```
filter ftp <port> <local_ip> <local_mask> <foreign_ip> <foreign_mask> [allow]
[interact-block]
```

For an explanation of the **filter ftp** parameters, see Parameters for the filter commands.

Examples:

Command example	Action
filter ftp 21 0 0 0 0	Manages every FTP request to all destinations. Applied to traffic on port 21.
filter ftp 21 10.5.0.0 255.255.0.0 0 0	Manages the 10.5.x.x network going to any destination. Applied to traffic on port 21.
filter ftp 21 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255	Manages the 10.5.0.69 host going to the 132.239.29.189 destination. Applied to traffic on port 21.

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows access via web protection software from the specified local IP address to all websites.

You can enter multiple **filter ftp** commands to set up different portions of the network for filtering. Organize the commands as described above for **filter url**.

9) After entering commands to define filtering for HTTP, HTTPS, and FTP requests, you can define any required exceptions to these filtering rules by adding the **except** parameter to the **filter** command:

```
filter {url | https | ftp} except <local_ip> <local_mask> <foreign_ip>
<foreign_mask>
```

This command allows you to bypass web protection software for traffic coming from, or going to a specified IP address or addresses.

For example, suppose that the following filter command was entered to cause all HTTP requests to be forwarded to Filtering Service:

```
filter url http 0 0 0 0
```

You could then enter:

```
filter url except 10.1.1.1 255.255.255.255 0 0
```

This would allow any outbound HTTP traffic from the IP address 10.1.1.1 to go unfiltered.

10) Configure the security appliance to handle long URLs using the **url-block url- mempool** and **url-block url-size** commands:

a) Increase the size of the security appliance's internal buffer to handle long URL strings. If the URL buffer size is set too low, some web pages may not display.

To specify the amount of memory assigned to the URL buffer, enter:

```
url-block url-mempool <memory_pool_size>
```

Here, <*memory_pool_size*> is the size of the buffer in KB. You can enter a value from 2 to 10240. The recommended value is 1500.

b) Increase the maximum permitted size of a single URL by adding the following line to the configuration:
```
url-block url-size <long_url_size>
```

Here, <*long_url_size*> is the maximum URL size in KB. You can enter a value from 2 to 4. The recommended value is 4.

11) Configure the URL response block buffer using the **url-block block** command to prevent replies from the web server from being dropped in high-traffic situations.
On busy networks, the lookup response from Filtering Service may not reach the security appliance before the response arrives from the web server.

The HTTP response buffer in the security appliance must be large enough to store web server responses while waiting for Filtering Service.

To configure the block buffer limit, use the following command:

```
url-block block <block_buffer_limit>
```

Here, <*block_buffer_limit*> is the number of 1550-byte blocks to be buffered. You can enter a value from 1 to 128.

- To view the current configuration for all 3 **url-block** commands, enter **show running-config url-block**.
- Enter **show url-block block statistics** to see how the current buffer configuration is functioning. The statistics include the number of pending packets held and the number dropped. The **clear url-block block statistics** command clears the statistics.

12) If you need to discontinue filtering, enter the exact parameters in the original **filter** command, preceded by the word **no**.
For example, if you entered the following to enable filtering:

```
filter url http 10.0.0.0 255.0.0.0 0 0
```

Enter the following to disable filtering:

```
no filter url http 10.0.0.0 255.0.0.0 0 0
```

Repeat for each filter command issued, as appropriate.

13) Save your changes in one of the following ways:

- Either enter the command:
  ```
  copy run start
  ```
- Or enter the commands:
  ```
  exit
  ```
  ```
  write memory
  ```

Filtering Service is ready to manage Internet requests after the Master Database is downloaded and the software is activated within the Cisco security appliance. See the Administrator Help for information about configuring your web protection software and downloading the Master Database.

Parameters for the filter commands

The parameters used by the **filter http**, **filter https**, and **filter ftp** commands include the following. Note that some of the parameters listed do not apply to all 3 commands.

Parameter	Applies to	Definition
http <*port*>[-<*port*>]	filter http	Defines which port number, or range of port numbers, the security appliance watches for HTTP requests. If you do not specify a port number, port 80 is used by default.
<*port*>	filter https filter ftp	Defines the port number the security appliance watches for https or ftp requests. The standard HTTPS port is **443**. The standard FTP port is **21**.
<*local_ip*>	filter http filter https filter ftp	IP address requesting access. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all internal clients. This address is the source for all connections to be filtered.
<*local_mask*>	filter http filter https filter ftp	Network mask of the **local_ip** address (the IP address requesting access). You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network.
<*foreign_ip*>	filter http filter https filter ftp	IP address to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations.
<*foreign_mask*>	filter http filter https filter ftp	Network mask of the **foreign_ip** address (the IP address to which access is requested). Always specify a mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the external network.

Parameter	Applies to	Definition
[allow]	filter http filter https filter ftp	Lets outbound connections pass through the security appliance without filtering when Filtering Service is unavailable. If you omit this option, and Filtering Service becomes unavailable, the security appliance stops all outbound HTTP, HTTPS, or FTP traffic until Filtering Service is available again.
[cgi-truncate]	filter http	Sends CGI scripts to Filtering Service as regular URLs. When a URL has a parameter list starting with a question mark (?), such as a CGI script, the URL is truncated. All characters after, and including the question mark, are removed before sending the URL to Filtering Service.
[interact-block]	filter ftp	Prevents users from connecting to the FTP server through an interactive FTP client. An interactive FTP client allows users to change directories without entering the complete directory path, so Filtering Service cannot tell if the user is requesting something that should be blocked.
[longurl- truncate | longurl-deny]	filter http	Specify how to handle URLs that are longer than the URL buffer size limit. ■ Enter **longurl-truncate** to send only the host name or IP address to Filtering Service. ■ Enter **longurl-deny** to deny the request without sending it to Filtering Service.
[proxy-block]	filter http	Enter this parameter to prevent users from connecting to an HTTP proxy server.

User-based policies and Cisco integration

Applies to:
■ Forcepoint URL Filtering, v8.5.x

If http, https or ftp authentication is enabled on a Cisco security appliance, User Service must be installed in the same domain (Windows), or the same root context (LDAP) as authenticated users in order to get correct user information to Filtering Service for accurate user-based policy enforcement.

Note

Cisco Secure ACS can provide user information for one domain only. To transparently identify users in multiple domains, use a transparent identification agent.

If user authentication is not enabled on the Cisco security appliance, manual authentication or transparent identification agents can be used to apply user-based policies. See the Administrator Help for information about configuring manual authentication, or configuring transparent identification agents.

If user authentication information is provided by a Cisco security appliance, it can only be used for HTTP(S) and FTP policy management by default.

To enable Internet protocol management, follow these steps:

1) Log on to the machine on which Filtering Service is installed.

2) Stop use the Windows Services tool or `/opt/Websense/WebsenseDaemonControl` command to stop Filtering Service.

3) Navigate to the **bin** directory (C:\Program Files\Websense\Web Security\bin or / opt/Websense/bin) and open the **eimserver.ini** file in a text editor.

4) Under [WebsenseServer], add the parameter **CacheWISPUsers=on**.

5) Use the Windows Services tool or `/opt/Websense/WebsenseDaemonControl` command to restart Filtering Service.

Configuring a Cisco IOS Router

Applies to:
■ Forcepoint URL Filtering, v8.5.x

After Forcepoint URL Filtering is installed, you must configure the Cisco IOS router to send HTTP requests to Filtering Service. This configuration is done through a console or telnet session. Filtering Service analyzes each request and tells the router whether to permit or block access, or to limit access with a time-limited control, as defined in web protection policies.

For instructions, see:

- Cisco IOS startup configuration
- Cisco IOS configuration commands
- Cisco IOS executable commands

Related concepts
Cisco IOS configuration commands on page 201
Cisco IOS executable commands on page 203

Related tasks
Cisco IOS startup configuration on page 198

Cisco IOS startup configuration

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Before Filtering Service can apply policies to Internet requests, the Cisco IOS router must be configured to use Filtering Service as a URL filter.

Steps

1) Access the router's software from a console, or from a remote terminal using telnet.

2) Enter your password.

3) Enter **enable** and the enable password to put the router into enabled mode.

4) Enter **configure terminal** to activate configure mode.

5) Enter the following command to identify the Filtering Service machine that will filter HTTP requests:

```
ip urlfilter server vendor forcepoint <ip-address> [port <port-number>]
[timeout <seconds>] [retransmit <number>]
```

Variable	Description
<ip-address>	The IP address of the machine running Filtering Service.
<port-number>	The Filtering Service port (also referred to as the integration communication port), default 15868.
<seconds>	The amount of time the Cisco IOS router waits for a response from Filtering Service. The default timeout is 5 seconds.
<number>	How many times the Cisco IOS router retransmits an HTTP request when there is no response from Filtering Service. The default is 2.

An example of this command is:

```
ip urlfilter server vendor forcepoint 12.203.9.116 timeout 8 retransmit 6
```

To define an additional Filtering Service instance as a backup, repeat the command using the IP address of the second Filtering Service machine.

The configuration settings you create in the following steps are always applied to the primary server.

Only one Filtering Service instance (the primary server) is used at a time. If the primary server becomes unavailable, the system goes to the list of configured Filtering Service instances and attempts to activate the first one. If the first server is not available, the system attempts to activate the next one. This continues until an available server is found or the end of the list of configured servers is reached. If all servers are down, the router goes into allow mode.

6) Enable the logging of system messages to Filtering Service by entering the following command:

```
ip urlfilter urlf-server-log
```

This setting is disabled by default. When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request.

(Recent changes to Cisco software at version v15 have removed support for this command. This is under research.)

7) Tell the Cisco IOS router how to filter URL requests by entering the following commands, in sequence:

```
ip inspect name <inspection-name> http urlfilter
interface <type> <slot/port>
ip inspect <inspection-name> {in|out}
```

Examples of these commands are:

```
ip inspect name fw_url http urlfilter
interface FastEthernet 0/0
ip inspect fw_url in
```

For this sequence to function properly, you must create an inspection rule called *fw_url* and apply that rule to the inbound interface of the router.

See Cisco documentation for information about creating and applying inspection rules.

To improve performance, Cisco suggests disabling the Java applet scanner. Java applet scanning increases CPU processing load. To disable the Java applet scanner, use the following commands, in sequence:

```
access-list <num> permit any
ip inspect name <inspection-name> http java-list <num> urlfilter
```

See Cisco documentation for more information about these commands.

8) To save your changes:

a) Enter the **exit** command twice to leave the configure mode.

b) Enter **write memory**.

These commands store the configuration settings in the Cisco IOS router's startup configuration so they are not lost if the router is shut down or loses power.

9) Use the following commands to view various aspects of your installations:

Command	Action
show ip inspect name <inspection-name>	Displays a specific inspection rule.
show ip inspect all	Displays all available inspection information.
show ip urlfilter config	Displays all URL filtering information.
<command-name> ?	Displays help on individual commands. For example, **ip inspect ?** displays the complete syntax for the **inspect** command, and explains each argument.

10) To stop sending requests to a Filtering Service instance, use the following command:

no ip urlfilter server vendor forcepoint <ip-address>

Cisco IOS configuration commands

Applies to:
■ Forcepoint URL Filtering, v8.5.x

These commands are used to configure the Cisco IOS router to send HTTP requests through Filtering Service for policy enforcement.

Note

To turn off a feature or service, add the value **no** before the command.

- `ip inspect name <inspection-name> http urlfilter [java-list <access-list>] [alert {on|off}] [timeout <seconds>] [audit- trail {on|off}]`
  This global command turns on HTTP filtering. The **urlfilter** value associates URL filtering with HTTP inspection rules. You may configure two or more inspections in a router, but the URL filtering feature only works with those inspections in which the **urlfilter** field is enabled. This setup command is required.
- `ip port-map http port <num>`
  Use this command to filter proxy traffic on port <*num*> through Filtering Service.
- `ip urlfilter server vendor forcepoint <IP-address> [port <num>] [timeout <secs>] [retrans <num>]`
  This setup command is required to identify Filtering Service to the Cisco IOS router and configure additional values. When using this command, the Cisco IOS router checks for a primary Filtering Service—one that is active and being sent URL lookup requests. If a primary server is configured, the router marks the server being added as a secondary server.

Parameter	Description
port <num>	The Filtering Service port (referred to as the integration communication port) you entered during product installation. The default port number is 15868.
timeout <secs>	The amount of time the Cisco IOS router waits for a response from Filtering Service. The default timeout is 5 seconds.
retrans <secs>	How many times the router retransmits an HTTP request when there is no response from Filtering Service. The default value is 2.

- `ip urlfilter alert`
  This optional setting controls system alerts. By default, system alerts are enabled. The following messages can be displayed when alerts are enabled:
  - %URLF-3-SERVER_DOWN: Connection to the URL filter server <*IP address*> is down.
    This level three LOG_ERR type message appears when a configured Filtering Service goes down. The router marks the offline server as a secondary server. It then attempts to use a defined secondary server as the primary server. If the router cannot find another Filtering Service, the URLF-3-ALLOW_MODE message is displayed.
  - %URLF-3-ALLOW_MODE: Connection to all URL filter servers is down and ALLOW MODE is OFF.

This message appears when the router cannot find a defined Filtering Service. When the **allowmode** flag is set to **off**, all HTTP requests are blocked.

- %URLF-5-SERVER_UP: Connection to a URL filter server <*IP address*> is made. The system is returning from ALLOW MODE.
  This LOG_NOTICE type message is displayed when a Filtering Service is detected as being up and the system returns from the ALLOW MODE.
- %URLF-4-URL_TO_LONG: URL too long (more than 3072 bytes), possibly a fake packet.
  This LOG_WARNING message is displayed when the URL in a GET request is too long.
- %URLF-4-MAX_REQ: The number of pending requests has exceeded the maximum limit <*num*>.
  This LOG_NOTICE message is displayed when the number of pending requests in the system exceeds the maximum limit defined. Subsequent requests are dropped.

- `ip urlfilter audit-trail`
  This command controls the logging of messages into the syslog server and is disabled by default. The messages logged are:

  - %URLF-6-URL_ALLOWED: Access allowed for URL <*site's URL*>; client <*IP address:port*> server <*IP address:port*>
    This message is logged for each URL requested that is allowed by web protection policies. The message includes the allowed URL, the source IP address/port number, and the destination IP address/port number. Long URLs are truncated to 300 bytes and then logged.
  - %URLF-6-URL_BLOCKED: Access denied URL <*site's URL*>; client <*IP address:port*> server <*IP address:port*>
    This message is logged for each URL requested that is blocked by web protection policies. The message includes the blocked URL, the source IP address/port number, and the destination IP address/port number. Long URLs are truncated to 300 bytes and then logged.
  - %URLF-4-SITE-BLOCKED: Access denied for the site <*site's URL*>; client <*IP address:port*> server <*IP address:port*>
    This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list.

- `ip urlfilter urlf-server-log`
  This command is used to control the logging of system messages to Filtering Service and is disabled by default. To allow logging (and consequently reporting) of Internet activity on your system, you must enable this feature.

  When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request. The log message contains information such as the URL, host name, source IP address, and destination IP address.

  (Recent changes to Cisco software at version v15 have removed support for this command. This is under research.)

- `ip urlfilter exclusive-domain {permit|deny} <domain-name>`
  This optional command is used to add a domain to, or remove a domain from, the exclusive domain list. Cisco IOS router URL filtering allows you to specify a list of domain names for which the router does not send lookup requests to Filtering Service.

  The **permit** flag permits all traffic to <*domain-name*>. The **deny** flag blocks all traffic to <*domain-name*>.

  For example, if www.yahoo.com is added to the exclusive domain list, all the HTTP traffic whose URLs are part of this domain (such as www.yahoo.com/ mail/index.html, www.yahoo.com/news, and www.yahoo.com/sports) are permitted without sending a lookup request to Filtering Service.

  You may also specify a partial domain name. For example, you can enter .cisco.com instead of the complete domain name. All URLs with a domain name ending with this partial name (such as www.cisco.com/products, www.cisco.com/eng, people-india.cisco.com/index.html, and directory.cisco.com) are permitted or denied without having to send a lookup request to Filtering Service. When using partial domain names, always start the name with a dot (i.e., period).

For example:

```
ip urlfilter exclusive-domain permit .sdsu.edu
```

Use the **no** form of this command to undo permitting or blocking of a domain name. The permitting or blocking of a domain name stays in effect until the domain name is removed from the exclusive list. Using the **no** form of this command removes the specified domain name from the exclusive list. For example, to stop the automatic permitting of traffic (and send lookup requests to Filtering Service) to www.example.com:

```
no ip urlfilter exclusive-domain permit www.example.com
```

As another example, to stop the automatic blocking of traffic to the same domain name:

```
no ip urlfilter exclusive-domain deny www.example.com
```

```
ip urlfilter allowmode {on|off}
```

This command controls the default filtering policy if Filtering Service is down. If the **allowmode** flag is set to **on**, and the Cisco IOS router cannot find a Filtering Service, all HTTP requests are permitted.

If **allowmode** is set to **off**, all HTTP requests are blocked when Filtering Service becomes unavailable. The default for **allowmode** is **off**.

- `ip urlfilter max-resp-pak <number>`
  Use this optional command to configure the maximum number of HTTP responses that the Cisco IOS router can store in its packet buffer.

  The default value is 200 (this is also the maximum you can specify).
- `ip urlfilter max-request <number>`
  Use this optional command to set the maximum number of outstanding requests that can exist at a given time. When this number is exceeded, subsequent requests are dropped. The **allowmode** flag is not considered in this case because it is only used when Filtering Service is down.

  The default value is **1000**.

Cisco IOS executable commands

Applies to:
■ Forcepoint URL Filtering, v8.5.x

These Cisco IOS router commands allow you to view configuration data and communication statistics. These settings cannot be saved into the startup configuration.

- `show ip urlfilter config`
  Shows configuration information, including maximum number of requests, **allowmode** state, and list of configured Filtering Service instances.

  Technical Support typically requests this information when trying to solve a problem.
- `show ip urlfilter statistics`
  Shows Filtering Service communication statistics, including:
  - Number of requests sent to Filtering Service
  - Number of responses received from Filtering Service
  - Number of requests pending in the system
  - Number of requests failed
  - Number of URLs blocked

- `debug ip urlfilter {function-trace/detailed/events}`
  Displays debugging information from the URL filter system.

Parameter	Description
function-trace	Enables the system to print a sequence of important functions that get called in this feature.
detailed	Enables the system to print detailed information about various activities that occur in this feature.
events	Enables the system to print various events, such as queue events, timer events, and socket events.

Chapter 17

Integrating Forcepoint URL Filtering with Citrix

Contents

Applies to:

- Forcepoint URL Filtering, v8.5.x

Forcepoint URL Filtering can be integrated with Citrix™ XenApp™ 5.0, 6.0, and 6.5.

- To have their Internet activity managed by your web protection software, Citrix client computers must access the Internet through a Citrix server.
- Non-Citrix clients in the network can be managed as part of the same web protection deployment. See Combining Citrix with another integration section in *Initial Setup of Citrix integration* for more information.

Integrating Forcepoint URL Filtering with Citrix XenApp involves the following components:

- **Citrix Integration Service** must be installed on each Citrix server to allow that server to communicate with Filtering Service.
- **Filtering Service** interacts with Citrix Integration Service and Network Agent to determine whether to block or permit Internet requests.
- **Network Agent** manages Internet protocols not managed by your Citrix server integration.
  Although Network Agent can manage protocols other than HTTP, FTP, or SSL used by applications on the Citrix server, it can only apply a computer or network policy, or the Default policy to those requests.

See the following for information about integrating with Citrix products:

- Managing Internet requests from Citrix server users
- Citrix Integration Service installation overview
- Upgrading the Citrix Integration Service
- Configuring user access on Citrix servers
- Initial Setup of Citrix integration

Related concepts

Initial Setup of Citrix integration on page 217
Upgrading the Citrix Integration Service on page 216
Managing Internet requests from Citrix server users on page 206

Related tasks

Configuring user access on Citrix servers on page 216
Citrix Integration Service installation overview on page 209

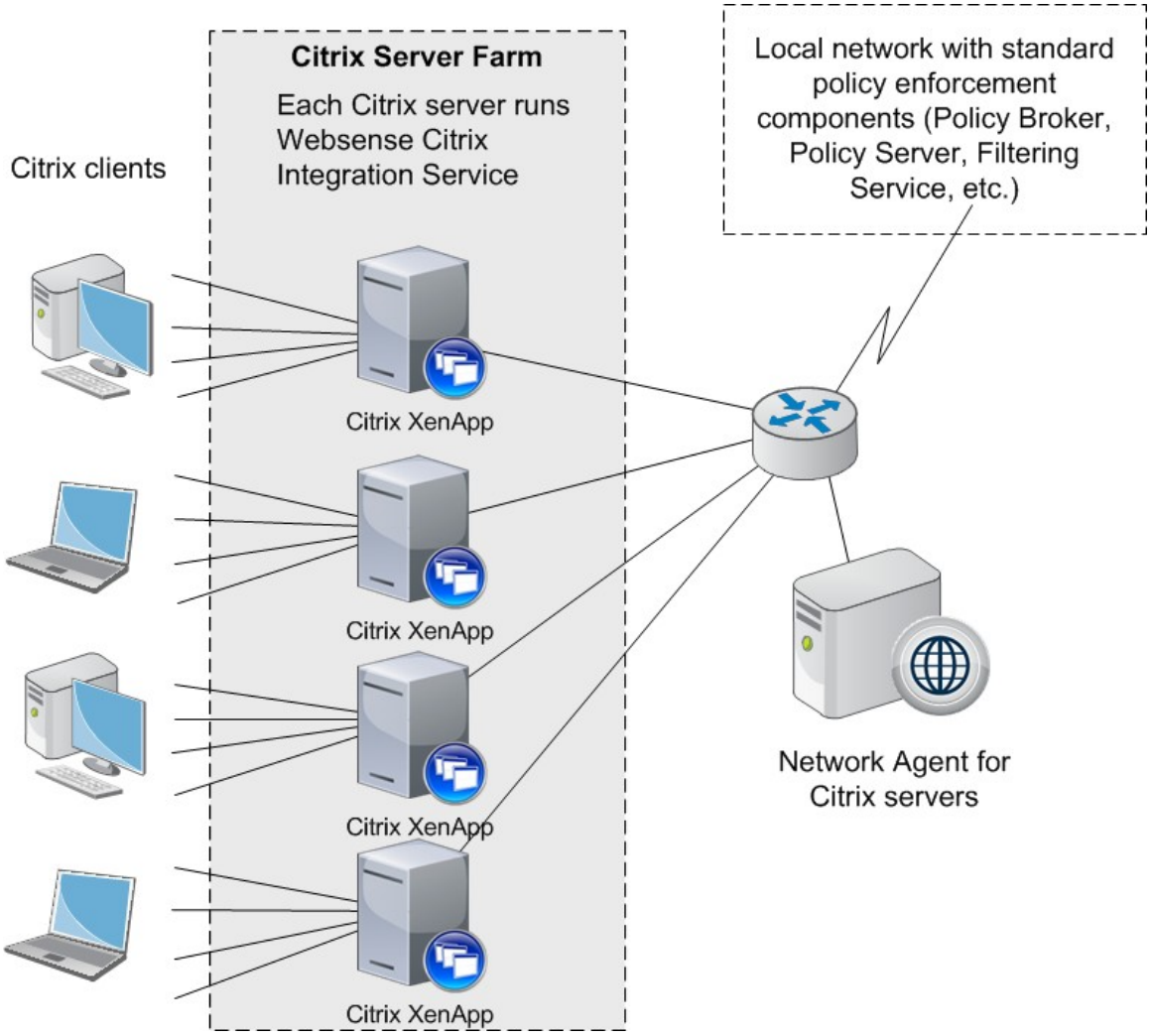
Managing Internet requests from Citrix server users

Applies to:
■ Forcepoint URL Filtering, v8.5.x

When Forcepoint URL Filtering is integrated with Citrix:

- A recommended maximum of 10 Citrix servers can connected to one Filtering Service instance. This number can be configured and depends on the user load.
  Multiple Filtering Service instances are needed if more than 15 Citrix servers are used, with each Citrix server handling about 20 to 30 Citrix users.
- The Filtering Service and Network Agent monitoring Citrix traffic should be installed on a dedicated machine, and not on a Citrix server.
- Separate Filtering Service and Network Agent instances must be used to monitor non-Citrix traffic.
- The Filtering Service and Network Agent instances monitoring Citrix traffic use the same Policy Broker, Policy Server, User Service, and other components as the Filtering Service and Network Agent instances used to monitor non-Citrix traffic.
- Do not configure a separate integration product to filter HTTP, HTTPS, FTP, or SSL requests from Citrix servers.
  If you want to use Network Agent to manage other protocol traffic from the Citrix servers:
  - Network Agent must be located where it can see all of the traffic between the Citrix servers and Filtering Service instances. For example, the machine running Network Agent could be connected to a span port on the same network switch as the machines running Filtering Service.
  - If the Citrix server is configured to use virtual IP addresses, configure Network Agent to monitor the entire range of the IP addresses. Also, a single policy should be set for this range. See the “Network Configuration” topic in the Administrator Help for instructions on configuring IP address ranges for Network Agent.
  - If you have standalone instances of Filtering Service (not configured to integrate with Citrix or any other integration product), use a dedicated instance of Network Agent to monitor users of the Citrix servers. Do not monitor non-Citrix traffic with this Network Agent.
    While Network Agent can be used to manages protocols for Citrix, user-based and group-based policies cannot be applied. Policies can be applied to individual computers and network ranges, identified by IP address or range. Otherwise, the Default policy is applied to all users.

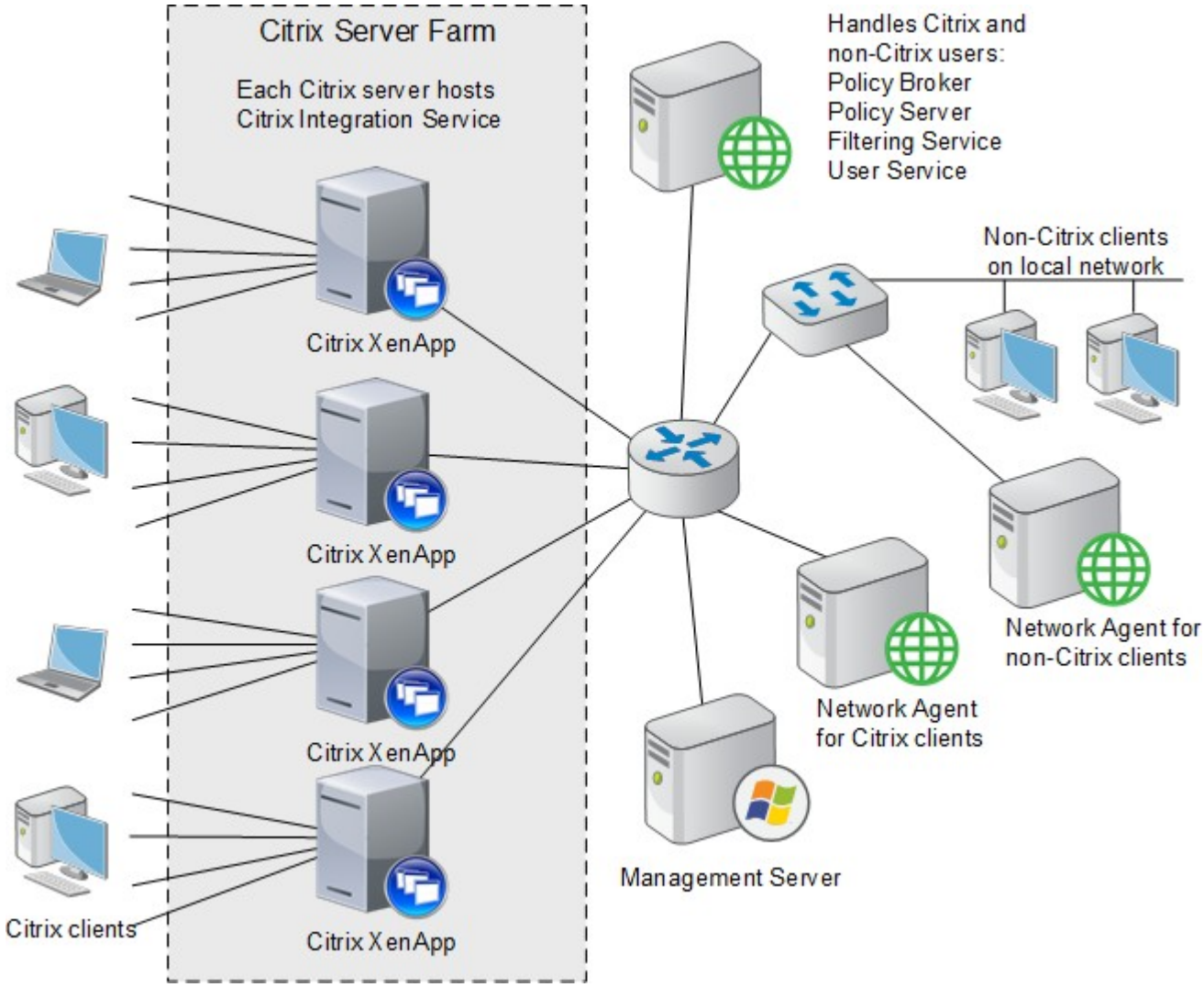
This diagram shows a typical deployment to manage requests from users who access the Internet through a Citrix server. To simplify the diagram, not all components are shown.



The main web policy enforcement components are installed on a separate, dedicated machine that can communicate with all of the Citrix server machines, and non-Citrix users, if applicable. The Citrix Integration Service must be installed on each Citrix server to allow it to communicate with Filtering Service. No other web protection components should be installed on the Citrix server machines.

Managing Internet requests for both Citrix and non-Citrix users

If your network includes some users who access the Internet via a Citrix server, and others who access the Internet through another gateway (firewall, caching appliance, or proxy server), the integrations can be configured to work together.



- To install the Citrix Integration Service on a Citrix Server, see *Citrix Integration Service installation overview*.
- If you have Citrix users and non-Citrix users in your network, the same web protection components, except for Network Agent, can be used for both sets of users. A separate installation of Network Agent is needed for the Citrix users. See *Install Filtering Service and Network Agent to integrate with Citrix* for instructions.
- To configure the web protection components installed with the non-Citrix integration to communicate with Citrix, refer to the section pertaining to your integration in Combining Citrix with another integration section in *Initial Setup of Citrix integration*.

Related concepts

Initial Setup of Citrix integration on page 217

Related tasks

Citrix Integration Service installation overview on page 209
Install Filtering Service and Network Agent to integrate with Citrix on page 210

Citrix Integration Service installation overview

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

There are 5 general steps involved in configuring Forcepoint URL Filtering to integrate with Citrix:

Steps

1) Install one or more instances of Filtering Service to integrate with Citrix.

2) Install a dedicated Network Agent to monitor the Citrix servers.
   To perform the first 2 steps, see *Install Filtering Service and Network Agent to integrate with Citrix*.

3) Obtain the Citrix configuration package (used to install the Citrix Integration Service configuration utility).
   See *Obtain the Citrix Integration Service configuration package*.

4) Create and configure a Citrix Integration Service installation package for your deployment.
   See *Configure the Citrix Integration Service installation package*.

5) Use the installation package to install Citrix Installation Service on your Citrix servers.
   See *Use the installation package to install Citrix Integration Service on a Citrix server*.
   For information about upgrading a prior-version Citrix Integration Service, see *Upgrading the Citrix Integration Service*.

   If web protection software will manage Internet activity for both Citrix and non-Citrix users, refer to Combining Citrix with another integration section in *Initial Setup of Citrix integration* after installing the Citrix Integration Service.

Related concepts

Obtain the Citrix Integration Service configuration package on page 211
Upgrading the Citrix Integration Service on page 216
Initial Setup of Citrix integration on page 217

Related tasks

Install Filtering Service and Network Agent to integrate with Citrix on page 210
Configure the Citrix Integration Service installation package on page 212
Use the installation package to install Citrix Integration Service on a Citrix server on page 215

Install Filtering Service and Network Agent to integrate with Citrix

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Before performing these steps, Policy Broker and Policy Server must already be installed and running in your network. You will be prompted for Policy Server connection information during Filtering Service installation.

Steps

1) Install an instance of Filtering Service to integrate with Citrix as follows:
   a) Launch the Setup program (Windows) or the Web Security Linux installer on a machine other than the Citrix server and select a **Custom** installation.
   b) On the Custom Installation screen, next to Forcepoint Web Security, click **Install** or **Modify**.
   c) Select **Filtering Service** as the component to install.
   d) On the Integration Option screen, select **Integrated with another application or device**.
   e) On the Select Integration screen, select **Citrix**.

   For more detailed custom installation instructions, see *Installing web protection components*.

   You can install other web protection components on this machine as well (for example, Policy Broker, Policy Server, User Service and so forth).

   Important

   Because you are integrating with Citrix servers, do not install Network Agent on the same machine as Filtering Service.

2) Run the (Windows or Linux) installer again on a separate machine to install the instance of Network Agent that will integrate with Citrix.

   When prompted for Filtering Service connection information, enter the IP address of the Filtering Service instance installed in step 1.

   To continue with the next step in the integration process, see *Obtain the Citrix Integration Service configuration package*.

Related concepts

Obtain the Citrix Integration Service configuration package on page 211

Related tasks

Installing web protection components on page 157

Obtain the Citrix Integration Service configuration package

Applies to:

- Forcepoint URL Filtering, v8.5.x

Everything you need to configure and install Citrix Integration Service (64-bit only) is contained in a self-extracting archive (the Citrix configuration package) containing:

- A configuration utility, used to customize the template installation package for your deployment
- A default installation package to use as a template (consisting of an MSI file, several DLLs, and configuration files)

The Citrix configuration package is included on any Windows machine containing Forcepoint URL Filtering components (for example, the management server or the Log Server machine). It can be found in the following directory:

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

Copy the Citrix configuration package (folder) from the Windows server to the machine on which you want to configure your custom installation package. The configuration package can run on most Windows operating systems; it does not need to be run on a server.

To continue with the next step in the integration process, see *Configure the Citrix Integration Service installation package*.

Related tasks

Configure the Citrix Integration Service installation package on page 212

Configure the Citrix Integration Service installation package

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Extract the contents of the Citrix configuration package and run the configuration utility to create a Citrix Integration Service installation package to deploy to Citrix servers.

Steps

1) Double-click the configuration package executable, then click **Extract**. The package name is WCISUtil_x64_*nnnn*.exe.

2) Double-click **Websense Citrix Integration Service Configuration.exe** to start the configuration utility.

3) In the **Profile Source** screen, click **Browse** and select the folder containing either the default Citrix installation package template or an existing installation package that you want to modify, then click **Next**.

   If the following message appears, make sure all necessary files are present in the folder you specified:

   The selected installation package does not include all of the necessary files.

   The folder you specify must contain all of the files extracted from the Citrix configuration package in step 1.

4) In the **Connections** screen, configure Filtering Service connection behavior for Citrix Integration Service as described below. When you are finished, click **Next**.

   a) If **127.0.0.1:15868** appears in the right pane, select it and then click **Remove**.

   Filtering Service should never be installed on the Citrix server machine itself.

   b) Under **Connection Details**, enter the IP address or hostname of a Filtering Service machine, then enter the filtering port (15868 by default).

   Note

   The Filtering Service port must be in the range 1024- 65535. To determine what port is used by Filtering Service, check the **eimserver.ini** file—located in C:\ Program Files *or* Program Files (x86)\Websense\Web Security\bin (Windows) or /opt/Websense/bin/ (Linux) — on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

   Important

   Do not modify the **eimserver.ini** file.

   c) Click the right arrow (>) to add the IP address/hostname and port entry to the list to the right.

d) Repeat the previous 2 steps for each Filtering Service instance you want used by the Citrix server.

When multiple Filtering Service instances are specified, if the first instance is unavailable, Citrix Integration Service attempts communication with the next instance in the list.
If no Filtering Service instances are available, Citrix Integration Service continues to attempt communication in the background every 1 minute. Until communication is established, Citrix Integration Service fails open (permits all requests) or fails closed (blocks all requests) depending on your select in **step f** (below).

Note

Each Filtering Service instance tracks continue, quota, and password override information independently. If the Citrix Integration Service fails over from one Filtering Service instance to another, usage quotas may be different and override passwords may need to be entered again.

e) Enable or disable the **Do not send user name information to Filtering Service** option. If this option is selected (enabled), user name information for Citrix users is not included in reports.

The setting applies to all Filtering Service instances listed.

f) Enable or disable the **Block all HTTP/HTTPS/FTP traffic if unable to connect to a Filtering Server** option to determine whether Citrix Integration Service blocks or permits all requests when it cannot communicate with Filtering Service.

5) In the **Client Settings** screen, select options as described below. When you are finished, click **Next**.

- **Notify users when HTTPS or FTP traffic is blocked**: Determine whether users see a browser pop-up message when HTTPS or FTP traffic is blocked. If so, also specify the how long the pop-up message remains visible.
- **Protect installation directory from modification or deletion**: This option prevents tampering with the Citrix Integration Service on the Citrix server. Attempts to delete it, replace files, or modify registry entries are stopped.

6) On the **Trusted Sites** screen, specify any URLs or domains that should be ignored (not forwarded for policy enforcement). When you are finished, click **Next**.

- To add a URL or regular expression, click **Add**, then enter either a URL or a regular expression specifying a set of URLs. Any regular expression adhering to ISO/IEC TR 19768 (within the character-number limit) is valid. When you are finished, click **OK**.
- To edit a URL or regular expression, select it and then click **Edit**.
- To remove a URL or regular expression, select it and then click **Remove**.

The URLs you specify here are trusted by any Citrix server on which this Citrix Integration Service is install. It has no bearing on how Filtering Service instances filter requests from non-Citrix users and other Citrix servers that use a different Citrix Integration Service configuration.

7) On the **Save** screen, specify how you want the customized installation package saved. When you are finished, click **Finish**.

   - Select **Overwrite the existing installation** to overwrite the Citrix installation package you used as a template. This is the package residing in the folder you selected in Step 3.
   - Select **Save the customized installation package to a new location** to save the customized installation package to a different location. Click **Browse**, and specify a folder. It is a best practice to save to an empty folder. Then, you can be certain that all files in that folder are part of the installation package.

   The installation package is now ready for use.

   If you have multiple Citrix servers for which you want different customized settings, repeat this procedure to create an installation package for each. Save each customized installation package to different folders.

   To continue to the last step in the integration process, see *Use the installation package to install Citrix Integration Service on a Citrix server*.

Related tasks

Use the installation package to install Citrix Integration Service on a Citrix server on page 215

Use the installation package to install Citrix Integration Service on a Citrix server

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

A Citrix installation package includes the following files:

- 0x0409.ini
- CI.cab
- CIClientConfig.hsw
- CIClientMessage.hsw
- DLP.cab
- GClientConfig.hsw
- setup.exe
- Setup.ini
- Websense Citrix Integration Service.msi
- WEP.cab

All of the files must be present to install Citrix Integration Service.

Note

If you want to use the same Citrix Integration Service configuration on multiple Citrix servers, use the same Citrix installation package for them. Repeat the procedure, below, on each Citrix server.

Steps

1) Log on with **local** administrator privileges to the machine running Citrix XenApp.

2) Close all applications and stop any antivirus software.

3) Copy the Citrix installation package (all files listed above) to the Citrix server. Keep the files in the same folder.

   If you installed the Citrix configuration package to the Citrix server itself, and customized the installation package there, skip this step.

4) Double-click **setup.exe** to start the Citrix Integration Service installer. It may take a few seconds for the program to begin to run.
   When the Welcome screen appears, click **Next**.

5) Accept the subscription agreement, then click **Next**.

6) On the **Destination Folder** screen, accept the default location shown or click **Change** to choose a different location, then click **Next**.

7) On the **Ready to Install the Program** screen, click **Install** to install the Citrix Integration Service.

8) Wait until the **InstallShield Wizard Completed** screen appears, then click **Finish**.

9) If you stopped your antivirus software, be sure to start it again.

Upgrading the Citrix Integration Service

Applies to:
■ Forcepoint URL Filtering, v8.5.x

If you are upgrading from v7.8 or later, simply create a new Citrix Integration Service installation package and run it on the Citrix server. You do not need to uninstall the previous version of the Citrix Integration Service first.

If you are upgrading from v7.7 or earlier, follow the upgrade instructions v7.8.x to v8.3.x first. Once your deployment is at v8.3, you can upgrade to v8.5 or v8.5.3. Upgrades to v8.5.4 are supported only from v8.4, v8.5, or v8.5.3. (Note that upgrades from 7.8.x or v8.0.x to v8.5.x are not supported.)

Configuring user access on Citrix servers

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

To allow Forcepoint URL Filtering to apply policies to individual users and groups defined in a directory service, you must configure user access for your published applications in Citrix. The procedure varies according to the Citrix version.
Following is an overview of the procedure for configuring user access in Citrix XenApp 5.0. See Citrix documentation for more information on this wizard or for information about XenApp 6.0 or 6.5.

Steps

1) Log on to the Citrix server Access Management Console as an administrator.
2) Select **Applications** in the left navigation pane, or select a particular application you have published.
3) Under **Other Tasks**, select **Permissions**.
4) Click **Add** in the Permissions for folder “Applications” dialog box.
5) Click **Add** in the Add access to folder dialog box.
6) Select the computer or domain for adding users, and select the **Show users** check box.
7) Select a user, and click **Add** to move that user into the Configured Accounts list.
8) Repeat step 7 to add other users to the Configured Accounts list.
9) Click **OK** twice to save the newly added users.

Next steps

If you need to change the permissions for a user, use the Edit button in the Permissions for folder “Applications” dialog box.

Important

- Do **not** allow users to log on with local or administrative credentials.
- Do **not** allow anonymous connections.

Initial Setup of Citrix integration

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Configuring for Citrix Virtual IP Addresses

If an integrated Citrix server is configured to use virtual IP addresses, you must configure Network Agent to monitor the entire range of the IP addresses.

You should also set a single web protection policy for this range of virtual IP addresses.

See the “Network Configuration” topic in the Administrator Help for instructions on adding and editing IP address ranges for Network Agent, and configuring policies for specific IP address ranges.

Combining Citrix with another integration

Forcepoint URL Filtering can be set up to manage both Citrix and non-Citrix users. This section provides instructions for configuring web protection software to work with the Citrix integration product.

Deployment scenarios

The corporate network (non-Citrix users) can access the Internet through Network Agent or a third-party integration product, such as Cisco™ ASA or Microsoft™ Forefront TMG. The component or integration product sends Internet requests to Filtering Service to determine whether to block or permit the request.

Citrix clients access the network through Citrix XenApp. Depending on the number of Citrix users, the access may be through one server, or through a server farm consisting of multiple Citrix servers. For more information, see *Managing Internet requests from Citrix server users*.

Policy management is enabled by installing the Citrix Integration Service on each Citrix server. See *Citrix Integration Service installation overview* for instructions.

In lower volume networks, each Integration Service communicates with the same Filtering Service. The non-Citrix users can be pointed to the same instance of Filtering Service as the Integration Service.

Deploying with Network Agent

If you have a standalone deployment of Forcepoint URL Filtering, separate instances of Network Agent are needed for the Citrix and non-Citrix users. See Standalone Forcepoint URL Filtering configuration for configuration information.

Configuration

To use Forcepoint URL Filtering to manage both Citrix users and users accessing the Internet through Network Agent or another integration product, the non-Citrix-related components must be installed and running before the Citrix integration is completed.

1) Install Forcepoint URL Filtering.

2) Install the Filtering Service and Network Agent to be used for Citrix integration.

3) Configure and install the Citrix Integration Service on each Citrix server.
   This component sends requests from Citrix clients to Filtering Service for filtering. Up to 10 Integration Services can be pointed to the same Filtering Service. If more than 10 Citrix servers are deployed, then additional Filtering Services can be used.

   See *Citrix Integration Service installation overview*, for instructions for steps 2 and 3.

4) Configure the non-Citrix integration product to ensure that requests coming from the Citrix clients are not processed twice. See Configuring the non-Citrix integration.

Configuring the non-Citrix integration

Before the integrations can be used together, the non-Citrix integration must be set up to prevent Internet requests sent via the Citrix servers from being processed twice.

A request from a Citrix client is passed to the Citrix server. The Citrix Integration Service sends the request to Filtering Service, which determines whether to block or permit the request. Simultaneously, the Citrix server sends the same request to the non-Citrix integration, which must be configured to allow the request to pass through.

Microsoft Forefront TMG configuration

The ISAPI plug-in must be set to ignore traffic from the Citrix servers. This configuration is done by adding the host name of each Citrix server to the **isa_ignore.txt** file on the Microsoft Forefront TMG (TMG) machine.

Also, ensure that none of the Citrix servers are set to use the TMG machine as a proxy server.

1) On the TMG machine, go to the **WINDOWS\system32** directory and open the **isa_ignore.txt** file in a text editor.

   Note

   The default **isa_ignore.txt** file installed with web protection software contains the *url=http://ms_proxy_intra_array_auth_query/* URL. Do not delete this URL. It is used by TMG machines in a CARP array for communication. This URL must be ignored to allow filtering and logging to work properly when multiple TMG instances are deployed in an array.

2) Enter the host name for each Citrix server on its own line in the **isa_ignore.txt** file.

   Important

   You must enter each host name in the exact same format that ISA/TMG passes it to Filtering Service.

   Use the following format:

   hostname=<Citrix_server_hostname>

   Replace <Citrix_server_hostname> with the name of the Citrix server machine.

3) Restart the TMG machine.
   See Microsoft's ISAPI documentation and the Technical Library for more information.

Standalone Forcepoint URL Filtering configuration

In a standalone Forcepoint URL Filtering deployment, separate instances of Network Agent must be installed to manage Citrix and non-Citrix users. The Network Agent monitoring non-Citrix users must be set to ignore the Citrix servers. This configuration allows protocol filtering of both Citrix and non-Citrix requests.

1) Open the Web Security module of the Forcepoint Security Manager and go to **Settings > Network Agent**, then position the mouse over the **Global** menu item.

2) When the lists of IP addresses appears, select the IP address of the NIC used for monitoring Internet requests to open its Local Settings page.

3) Under **Monitor List Exceptions**, add each Citrix server that Network Agent should exclude from monitoring.

   a) To identify a machine, click **Add**, and then enter the Citrix server's IP address, or a range of IP addresses for a group of Citrix servers in a server farm. Then, click **OK**.

   b) Repeat this process until all Citrix servers have been added, either individually or as part of a range.

4) Click **OK** to cache your changes and return to the NIC Settings page. Changes are not implemented until you click **Save and Deploy**.

Related concepts

Managing Internet requests from Citrix server users on page 206

Related tasks

Citrix Integration Service installation overview on page 209

Chapter 18

Integrating Forcepoint URL Filtering with TMG

Contents

Applies to:

- Forcepoint URL Filtering, v8.5.x

Forcepoint URL Filtering can be integrated with Microsoft Forefront™ Threat Management Gateway (TMG).

Refer to Installation Instructions: Forcepoint URL Filtering as your primary source of installation instructions. Only additional or alternate steps required to enable TMG integration are provided here.

An integration with TMG affects the following web protection components:

- **ISAPI Filter plug-in**: This additional component is installed on the machine running TMG. The ISAPI Filter plug-in configures TMG to communicate with Filtering Service.
- **Filtering Service**: Interacts with TMG and Network Agent to manage Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.
  After the Filtering Service is installed, the ISAPI Filter plug-in must be installed on every TMG machine in your network.
- **Network Agent**: Manages Internet protocols that are not handled by TMG. Network Agent also enables bandwidth-based request management.

If your environment includes an array of TMG machines, install Forcepoint URL Filtering components on a machine outside the array.

When TMG receives an Internet request from a user, it passes the request to Filtering Service, which determines the category assigned to the URL and checks the policy assigned to the client.

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies TMG that the site is not blocked, and the client is given access to the site.

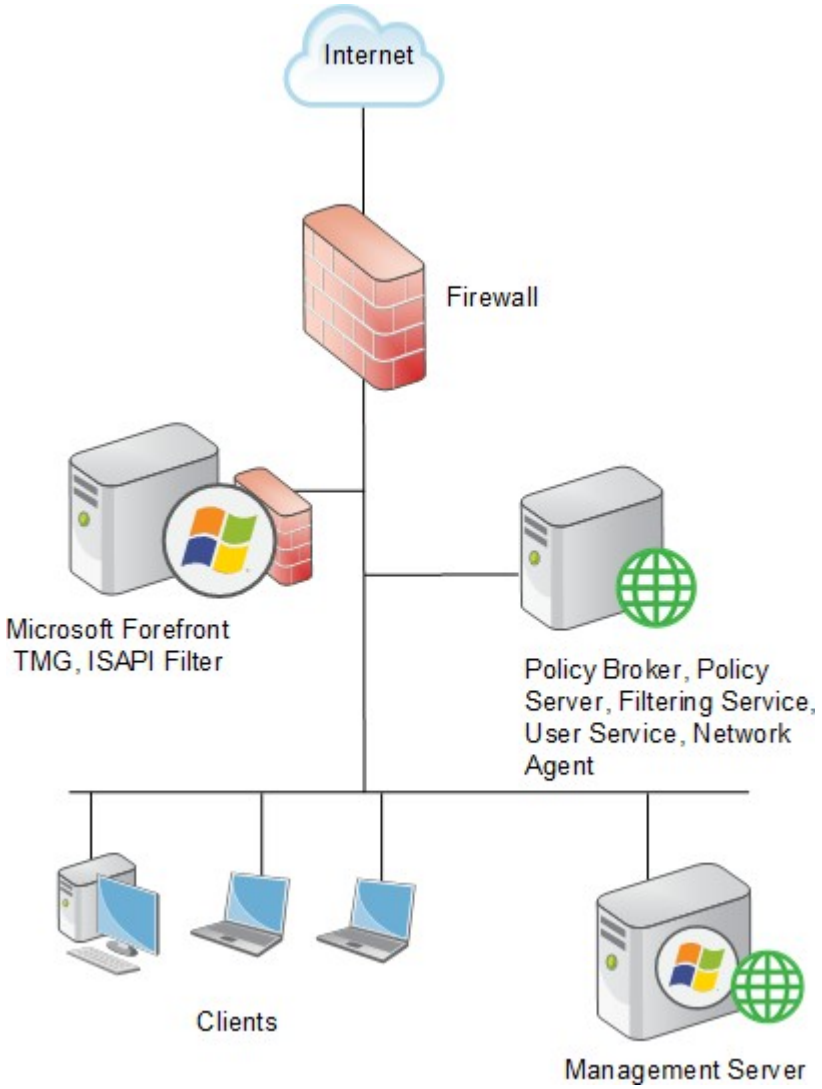
Deployment considerations for integration with Forefront TMG

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Single Microsoft Forefront TMG configuration

The following illustration shows placement of Forcepoint URL Filtering policy enforcement and management components on 2 dedicated machines, separate from the Microsoft Forefront TMG server.

- The ISAPI Filter must be installed on the TMG machine so that Internet activity information can be communicated to Filtering Service.
- The Filtering Service and TMG machines must be able to communicate over the network.

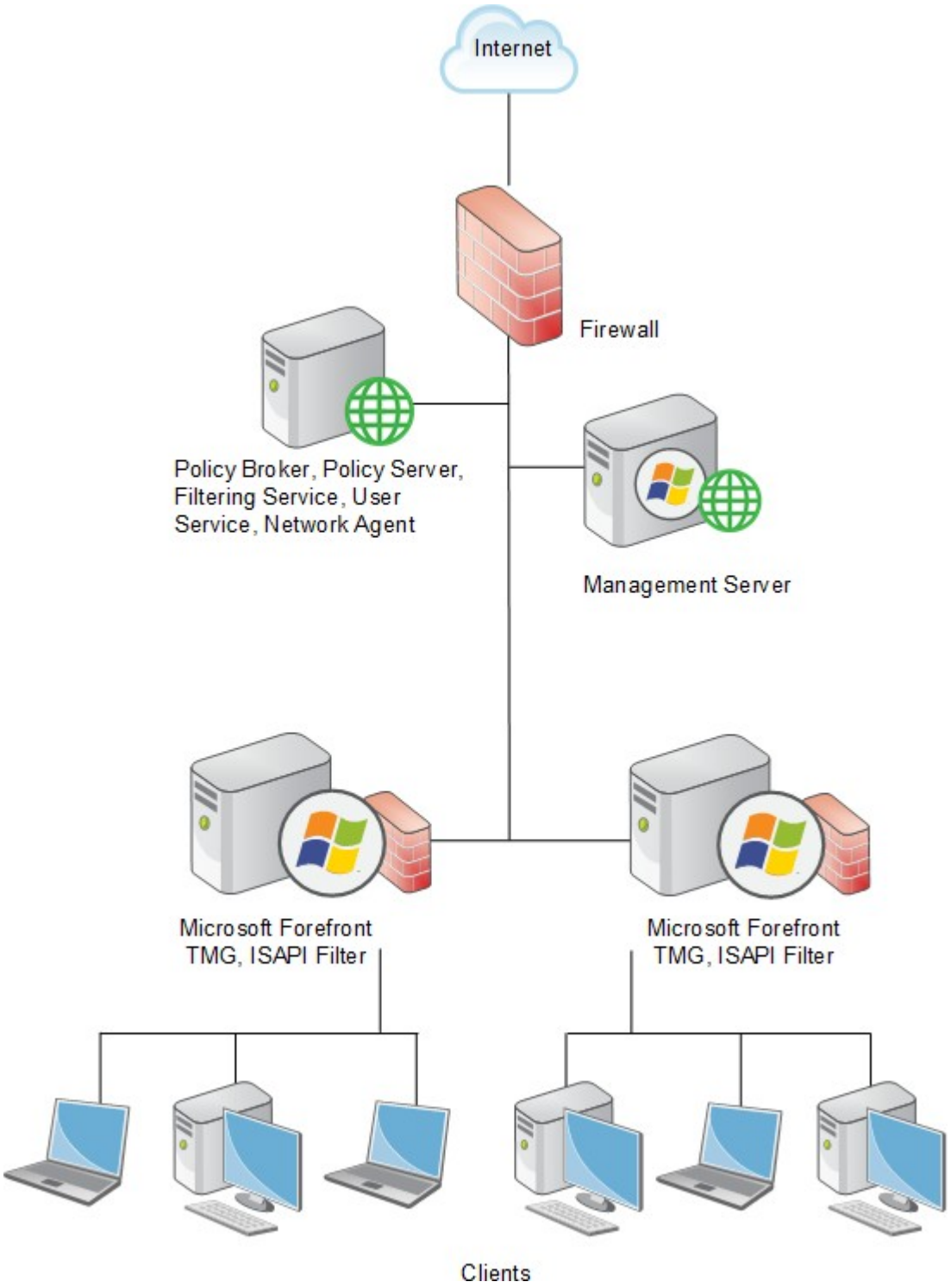


The diagram provides a general overview and best practice location for your integration product, but does not show all components. Larger networks require web protection components to be distributed across several dedicated machines.

Array configuration

Forcepoint URL Filtering is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. It is a best practice to install web protection software outside an array of Forefront TMG machines. Install the ISAPI Filter on each member of the array. See the following illustration.

When web protection software is deployed in this configuration, all array members send Internet requests to Filtering Service outside the array.



Other configurations are possible. See your Microsoft Forefront TMG documentation for information about TMG configurations.

The diagram provides a general overview and best practice location for your integration product, but does not show all components. Larger networks require web protection components to be distributed across several dedicated machines.

Installing Forcepoint URL Filtering to integrate with Forefront TMG

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

The general process of installing Forcepoint URL Filtering to integrate with Microsoft Forefront TMG is as follows:

1) Begin by installing web protection policy, management, and reporting components in your network (not on the TMG machine).
   Filtering Service must already be installed before the ISAPI Filter plug-in is installed on the TMG machine. When installing Filtering Service, specify that it is integrated with TMG.

2) Install the ISAPI Filter plug-in on the TMG machine (as described below).
   The only web protection components installed on the Forefront TMG machine are the ISAPI Filter plug-in and Control Service (which manages installation and removal of web protection software components).

The Forcepoint Security Installer is used to install the ISAPI Filter plug-in for Forefront TMG on the TMG machine.

Important

- As part of the installation process, you must stop the Microsoft Forefront TMG Firewall service (Firewall service). Because this may stop network traffic, perform the installation during a time when a stoppage will least affect your organization. Do not stop the Firewall service until prompted by the installer.
- Port 55933 (the Control Service communication port) must be open locally for the ISAPI Filter plug-in to be installed successfully.

Before beginning the installation process:

- Download or copy the Forcepoint Security Installer to the TMG machine. This installer is available from the My Account section of support.forcepoint.com.
- Close all applications and stop any antivirus software.

To perform the installation:

Steps

1) Log on to the TMG machine with domain admin privileges.

2) Right-click **Forcepoint85xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.

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

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

5) On the Installation Type screen, select **Custom** and then click **Next**.

6) On the Custom Installation screen, click the **Install** link next to Forcepoint Web Security.

7) On the Select Components screen, select **Filtering Plug-in**, then click **Next**.

8) On the **Filtering Service Communication** screen, enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). Then click **Next**.

   - The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535.
   - To verify the Filtering Service port, check the **WebsenseServerPort** value in the **eimserver.ini** file, located in the **bin** directory on the Filtering Service machine (C:\Program Files\Websense\Web Security \bin\ or /opt/Websense/ bin/).

9) On the **Installation Directory** screen, accept the default location and click **Next**.

10) On the **Pre-Installation Summary** screen, verify that **Filtering Plug-in** is the only component selected for installation, then click **Install**.

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

11) When the **Stop Microsoft Forefront TMG Firewall Service** screen appears, stop the Microsoft Forefront TMG Firewall service (Firewall service) and then click **Next**.

Note

Leave the installer running as you stop the Firewall service, and then return to the installer to continue installation.

To stop the Firewall service:

a) Go to **Start** > **Administrative Tools** > **Services or Server Manager** > **Tools** > **Services**.

b) Right-click **Microsoft Forefront TMG Firewall**, and then select **Stop**.

When the service has stopped, return to the installer and continue the installation process. The Firewall service may also be stopped from the Forefront TMG management console. See the Microsoft documentation for more information.

Important

When the Firewall service is stopped, Forefront TMG goes into lockdown mode. Network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

12) When the following message appears, start the Firewall service and click **OK**:
The ISAPI Filter has been configured, you can now start the Microsoft Firewall Service.

Note

Leave the installer running as you start the Firewall service, and then return to the installer to continue installation.

To start the Firewall service:

a) Go to **Start** > **Administrative Tools** > **Services or Server Manager** > **Tools** > **Services**.

b) Right-click **Microsoft Forefront TMG Firewall**, and then select **Start**.
The Firewall Service may also be started from the Forefront TMG management console. See the Microsoft documentation for more information.

13) On the **Installation Complete** screen, click **Done**.

14) If you stopped antivirus software on this machine, restart it now.
You can verify successful installation of the ISAPI Filter plug-in by logging into the Forefront TMG management console. Navigate to **System** > **Web Filters** and verify that WsISAFilter is present in the list of Web Filters.

Upgrading Forcepoint URL Filtering when integrated with ISA Server or Forefront TMG

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

To upgrade to the current version:

Steps

1) Upgrade existing web protection components, including Filtering Service.

2) Run the Forcepoint Security Installer on the Forefront TMG machine.

Note

As part of the upgrade process, you must stop the Microsoft Firewall service. Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this upgrade during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

Removing the ISAPI Filter Plug-In

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

When you remove the ISAPI Filter plug-in from a Forefront TMG machine.

Steps

1) Log on with **local** administrator privileges and navigate to **Start** > **Control Panel** > **Uninstall a program** (under **Programs**).

2) Select **Web Protection Solutions**, then click **Uninstall/Change**.
This launches the uninstaller.

3) On the **Remove Components** screen, select **Filtering Plug-in** and any other components to be removed, and then click **Next**.

4) When the **Stop Microsoft Firewall Service** screen appears, stop the Microsoft Firewall service and then click **Next**.

Note

Leave the uninstaller running as you stop the Microsoft Firewall service, and then return to the uninstaller to continue.

a) Go to **Start** > **Programs** > **Administrative Tools** > **Services or Server Manager** > **Tools** > **Services**.

b) Right-click **Microsoft Forefront TMG Firewall**, then select **Stop**.
When the service has stopped, return to the installer and continue the uninstallation process.

Important

When the Firewall service is stopped, TMG goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

5) When the following message appears, start the Firewall service and then click **OK**:
The ISAPI Filter has been unconfigured, you can now start the Microsoft Firewall Service.
- Leave the uninstaller running as you start the Firewall service, and then return to the uninstaller to continue.
- To start the Firewall service:
  - Go to **Start** > **Programs** > **Administrative Tools** > **Services or Server Manager** > **Tools** > **Services**.
  - Right-click **Microsoft Forefront TMG Firewall**, then select **Start**.

6) On the **Software Removed** screen, choose whether you want to restart now or later and then click **Done**.

Converting to an integration with Forefront TMG

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

You can convert an existing standalone deployment of Forcepoint URL Filtering to one that is integrated with TMG, without losing any configuration settings. The conversion process preserves such settings as policies, port numbers, and IP addresses.

Steps

1) Use the Backup Utility to back up the web protection configuration and initialization files. See the Backup and Restore FAQ for instructions.

2) Upgrade your web protection software to the current version.
After installing, it is a good idea to run the Backup Utility again to have a baseline for your upgraded software.

3) Make sure your web protection software is running. The uninstaller looks for Policy Server during the removal process.

Warning

Do not remove components when the associated Policy Server is stopped. If Policy Server is not running, files for the selected components are removed, but configuration information is not updated. Problems could occur later if you attempt to reinstall these components.

4) Uninstall Filtering Service.

See *Removing web protection components* for instructions. Be sure to remove **only** Filtering Service.

5) Reinstall Filtering Service to integrate with TMG.

See *Adding web protection components* for instructions. As you follow those instructions do the following on the screens noted below:

- On the **Select Components** screen, select **Filtering Service**.
- On the **Integration Option** screen, select **Install Forcepoint URL Filtering to integrate with a third-party product or device**.
- On the **Select Integration** screen, select **Microsoft Forefront Threat Management Gateway**.

6) Install the ISAPI Filter plug-in on the TMG machine. For instructions, see *Installing Forcepoint URL Filtering to integrate with Forefront TMG*.

7) Enable authentication so that users can be properly identified and their Internet requests can be processed. For instructions, see *User identification and authentication with Forefront TMG*.

Related concepts

Removing web protection components on page 350
User identification and authentication with Forefront TMG on page 236

Related tasks

Adding web protection components on page 344
Installing Forcepoint URL Filtering to integrate with Forefront TMG on page 225

Forefront TMG initial setup

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

Steps

- If you installed Log Server, see *Enabling communication with the Log Database when integrated with Forefront TMG*.
- Forcepoint URL Filtering manages HTTP, HTTPS, and FTP requests sent to TMG, but cannot manage traffic tunneled over a SOCKS or WinSOCK proxy server. To use Forcepoint URL Filtering in a network that uses a SOCKS or WinSOCK proxy server, you can either:
  - Disable the WinSOCK or SOCKS service.
  - Use the WinSOCK or SOCKS proxy client to disable the specific protocols that you want your web protection software to handle (HTTP, HTTPS, and FTP), then configure browsers on client computers to point to TMG for each of these protocols.

  For information about disabling a protocol, see the TMG Help from Microsoft.
- Additional configuration of the ISAPI Filter is required if you are using non-web proxy clients with TMG. These TMG clients include the Firewall/Forefront TMG Client with proxy server disabled, and SecureNAT clients.

  See *Configuring for TMG using non-web-proxy clients* for instructions.
- To configure your web protection software to ignore certain traffic based on the user name, host name, or URL, see *Configuring the ISAPI Filter plug-in to ignore specific traffic* for instructions.
- If Network Agent was installed, configure Network Agent with the IP addresses of all proxy servers through which computers route their Internet requests. See Configure Network Agent for instructions.
- If you installed Remote Filtering Server, configure TMG to ignore the machine on which Remote Filtering Server is installed. If TMG monitors this machine, it could interfere with policy enforcement for remote users. See your TMG documentation for instructions.

Related concepts

Configuring the ISAPI Filter plug-in to ignore specific traffic on page 234
Configuring for TMG using non-web-proxy clients on page 233

Related tasks

Enabling communication with the Log Database when integrated with Forefront TMG on page 232

Enabling communication with the Log Database when integrated with Forefront TMG

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

When you install Log Server, TMG must be configured to permit communication with the Log Database. This must be completed before Internet activity can be logged.

Steps

1) On the TMG machine, open the Forefront TMG management console (**Start > Programs > Microsoft Forefront TMG > Forefront TMG Management**).

2) In the left navigation pane, select **Firewall Policy**.

3) On the **Tasks** tab (on the right side of the console), click **Edit System Policy**. The **System Policy Editor** dialog box appears.

4) Under **Configuration Groups**, select **Logging > Remote Logging (SQL)**.

5) On the **To** tab, click **Add**.

6) Select **Networks > Internal**, and then click **Add**.
   You are returned to the System Policy Editor dialog box.

7) On the **General** tab, select **Enable this configuration group**.

8) Click **OK** to accept your changes.
   You are returned to the management console.

9) Click **Apply** at the top of the window to save the changes and update the configuration.

Configuring for TMG using non-web-proxy clients

Applies to:
■ Forcepoint URL Filtering, v8.5.x

If you are using non-web-proxy clients with Forefront TMG, additional configuration is required so that your web protection software can manage Internet requests correctly. The term non-web-proxy clients refers to:

- Firewall/Forefront TMG Client with the proxy server disabled
- SecureNAT clients

Firewall/Forefront TMG Client

If you are using Firewall/Forefront TMG Client with Forefront TMG, and the proxy server is enabled (default setting), your web protection software handles Internet requests normally.

However, if the proxy server is disabled, web protection software cannot manage Internet requests without additional configuration.

Check the Firewall/Forefront TMG Client machine to see if the proxy server is disabled.

1) Open the Firewall/Forefront TMG Client configuration screen, and select the **Web Browser** tab.

2) View the **Enable Web browser automatic configuration** check box.
   - If it is marked, the proxy server is enabled. Forcepoint URL Filtering requires no additional configuration.
   - If it is cleared, the proxy server is disabled. See Configuring the ISAPI Filter plug-in for additional configuration steps.

Note

If the proxy server is disabled, web protection software manages HTTP only; it cannot manage HTTPS.

SecureNAT clients

SecureNAT clients require that you configure the default gateway so that all traffic to the Internet is sent through TMG. If you need information about configuring and using SecureNAT clients, see your TMG documentation.

See Configuring the ISAPI Filter plug-in for additional configuration steps.

Configuring the ISAPI Filter plug-in

If you are using the TMG Firewall Client with the proxy server disabled, or SecureNAT clients, the ISAPI Filter plug-in must be configured to ignore requests going directly to the TMG and to manage only those requests going out to the Internet.

Note

If you are using the TMG Server Firewall Client with the proxy server disabled, then your web protection software handles HTTP only; not HTTPS.

1) On the TMG machine, create a file called **ignore.txt** in the Windows **system32** directory.

2) Enter the hostname or IP address of the TMG machine in the text file.
Hostnames must be entered in ALL CAPS. Entries that are not in all capital letters are not used.

3) If the TMG machine hosts multiple websites, add the names of all the sites being hosted. For example: **webmail.rcd.com**.
If only one website is hosted, do not add it to this file.

4) Restart the TMG machine.

Configuring the ISAPI Filter plug-in to ignore specific traffic

Applies to:

- Forcepoint URL Filtering, v8.5.x

You can configure the ISAPI Filter plug-in to bypass both policy enforcement and logging for certain traffic, based on the user name, hostname, or URL. This may be used for a small group of websites or users, or for machines in a complex proxy-array or proxy-chaining configuration.

To prevent policy enforcement and logging of this traffic, add the user names, hostnames, and URLs that you do not want your web protection software to handle to the **isa_ignore.txt** file.

1) On the TMG machine, open the **isa_ignore.txt** file in a text editor. This file is located in the Windows **system32** directory.

Important

The default **isa_ignore.txt** file installed during upgrade or installation contains the following URL:

```
url=http://ms_proxy_intra_array_auth_query/
```

Do **not** delete this URL. It is used by TMG in a CARP array for communication. This URL must be ignored by web protection software to allow policy enforcement and logging to work properly when multiple TMG instances are deployed in an array.

2) Enter each user name, hostname, or URL that you want web protection software to ignore. Enter each item on its own line in the file, using the formats below.

- **User name**: Enter the name of a user whose Internet requests should be ignored:
username=<user_name>

  Examples:

username=jsmith

username=domain1/jsmith

- **Hostname**: Enter a destination hostname for which user requests should be ignored: *hostname=<name>*

  Example:

  hostname=yahoo.com

- **URL**: Enter a URL for which user requests should be ignored: *url=<URL>*

  Example:

  url=http://mail.yahoo.com/

  url=mail.yahoo.com/

Note

To assure that the correct format is available for all situations, it is recommended that you enter the same name in all available configurations. For example, make 2 entries for user name: one with and one without the domain. Make 2 entries for URL: one with and one without the protocol.

3) Restart the TMG service.

Client computer configuration

Internet browsers on client computers should be configured to use TMG to handle HTTP, HTTPS, and FTP requests.

An exception to this configuration is browsers in an TMG environment using Firewall/Forefront TMG Clients or SecureNAT. These browsers must point to the same port, 8080, that TMG uses for each protocol.

See the browser online help for configuration instructions.

Firewall configuration

To prevent users from circumventing Forcepoint URL Filtering policy enforcement, configure your firewall or Internet router to allow outbound HTTP, HTTPS, and FTP requests only from TMG.

Contact your router or firewall vendor for information about configuring access lists on the router or firewall.

Important

If web protection software Internet connectivity requires authentication through a proxy server or firewall for HTTPS traffic, the proxy server or firewall must be configured to accept clear text or basic authentication to enable the Master Database download.

User identification and authentication with Forefront TMG

Applies to:
■ Forcepoint URL Filtering, v8.5.x

In order to apply user and group-based policies to Internet requests, Filtering Service must receive information about the user making the request. If no user information is available, only IP address-based policies or the Default policy can be applied to requests.

To ensure that Filtering Service receives user information, you can:

- Enable authentication within TMG.
- Install a transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent).
- Enable manual authentication within your web protection software. Users who cannot be identified by other means are prompted for logon information when they open a browser.

See Manual Authentication for more information.

TMG clients

These TMG clients are supported:

- Firewall/Forefront TMG (see Firewall/Forefront TMG and SecureNAT clients)
- SecureNAT (see Firewall/Forefront TMG and SecureNAT clients)
- Web Proxy (see Web Proxy clients)

The term **clients** in this environment refers to computers or applications that run on computers and rely on a server to perform some operations.

Each type of client can be configured so that your web protection software can obtain user identification and manage Internet requests based on user and group policies.

Firewall/Forefront TMG and SecureNAT clients

Firewall/Forefront TMG and SecureNAT clients cannot identify users transparently without special settings. These clients require a transparent identification agent to authenticate users. To enable user-based security policies with these clients, select one of these options:

- Configure computer browsers to access the Internet through TMG. This configuration allows Firewall/Forefront TMG and SecureNAT clients to also work as Web Proxy clients.
  If you choose this option, see Web Proxy clients for more information.
- If you are using a Windows-based directory service, disable all authentication methods within TMG and use transparent identification. This method allows Filtering Service to obtain user identification from the network's directory services.
  See Transparent identification, for more information.
- Enable your software to prompt users for authentication (manual authentication). This method allows your web protection software to obtain the user information it needs if neither the TMG nor a transparent identification agent provides the information.

See Manual Authentication for more information.

Web Proxy clients

After the browser is configured to use TMG as a proxy server, Web Proxy clients send Internet requests directly to TMG. You can assign individual user or group policies with one of the following methods.

- If your network uses only Microsoft Internet Explorer™ browsers, you can enable Integrated Windows Authentication within TMG to identify users transparently.
- If you are using a Windows-based directory service with various browsers, you can identify users transparently by disabling all authentication methods within TMG and implementing transparent identification.
  See Transparent identification, for more information.
- If the network uses a mixture of browsers, you can enable one or more of TMG's authentication methods. Some of these methods may require users to authenticate manually for certain older browsers.
  See Authentication Methods, for more information.
- Enable your software to prompt users for authentication (manual authentication). This method allows Filtering Service to obtain the user information it needs if neither TMG nor a transparent identification agent provides the information.
  See Manual Authentication for more information.

Authentication Methods

TMG provides 4 methods of authentication:

- Basic authentication
- Digest authentication
- Integrated Windows authentication (enabled by default)
- Client Certificate authentication

Internet Explorer supports all of these authentication methods. Other browsers may support only Basic authentication.

When no authentication method is enabled in TMG, it does not pass your web protection software any information about who is making the Internet request. When this occurs, you can:

- Apply computer and network policies.
- Enable manual authentication to permit user-based policy enforcement.
  See Manual Authentication for more information.
- Enable transparent identification to permit user-based policy enforcement.
  See Transparent identification, for more information.

Basic authentication

Basic authentication prompts users to authenticate (log on) each time they open a browser. This authentication allows TMG to obtain user identification, regardless of the browser, and send the information to Filtering Service, which manages Internet requests based on individual user and group policies.

If Basic authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted for a user name and password.

Digest authentication

Digest authentication is a secure authentication method used in Windows Server 2003 domains. The features are the same as Basic authentication, but the user name and password are scrambled when they are sent from the browser to TMG. The user can authenticate to TMG without the user name and password being intercepted. User information is sent to Filtering Service, which then manages Internet requests based on individual user and group policies.

If Digest authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted for a user name and password.

Integrated Windows authentication

Integrated Windows authentication provides secure authentication. With this authentication enabled, TMG obtains user identification transparently from browsers using Microsoft Internet Explorer. User information is sent to Filtering Service, which then applies user and group policies.

If your network has a mixture of Microsoft Internet Explorer browsers and other browsers, you can enable both Basic and Integrated Windows authentication, or Digest and Integrated Windows authentication. In either configuration:

- Users with Microsoft Internet Explorer browsers are identified transparently.
- Users with other browsers are prompted for a user name and password.

Note

To transparently identify all users in a mixed browser environment, you can disable Basic or Digest authentication and use transparent identification (see Transparent identification) in conjunction with Integrated Windows authentication.

Client Certificate authentication

Client Certificate authentication identifies users requesting information about a website. If Client Certificate is used, TMG requests the certificate and verifies that it belongs to a client that is permitted access, before allowing the Internet request.

Note

To use transparent identification, you must disable Client Certificate authentication.

Before changing authentication methods, consider the impact of the change on other TMG functions.

For more information about TMG authentication and how to configure these authentication methods, see Microsoft's documentation.

Transparent identification

Transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent) allow Filtering Service to apply user and group based policies to Internet requests without prompting users to authenticate in the browser.

- If TMG is not configured to send user information to Filtering Service, you can use a transparent identification agent to identify HTTP and non-HTTP users.
- If TMG provides user information for HTTP(S) requests, you can still use a transparent identification agent to obtain user and group information for other protocol requests, managed by Network Agent.

See Installation Instructions: Forcepoint URL Filtering for instructions on installing individual components. See User Identification for information about configuring transparent identification agents.

Forcepoint URL Filtering also offers secure manual authentication with Secure Sockets Layer (SSL) encryption to protect user names and passwords being transmitted between client computers and Filtering Service. See Manual Authentication for more information and instructions on activating this feature.

Troubleshooting integration with Forefront TMG

Applies to:
■ Forcepoint URL Filtering, v8.5.x

SecureNAT clients are not receiving the correct policy

If you are using non-web proxy clients (for example, Firewall Client with proxy server disabled, or SecureNAT clients) with TMG, additional configuration of the ISAPI filter is required. Follow the instructions in *Configuring for TMG using non-web-proxy clients*.

No policy enforcement occurs after the plug-in is installed

If users requests are not being handled properly after the ISAPI Filter plug-in has been installed on the Forefront TMG machine, the plug-in may not be able to communicate with Filtering Service.

Verify that the ISAPI Filter plug-in is using the correct Filtering Service information.

1) Go to the Windows **system32** directory and open the **wsMSP.ini** file.

2) Under **[initSection]**, check the **EIMServerIP** and **EIMServerPort** parameters (these are the Filtering Service IP address and port, respectively). For example:
   [initSection]

   EIMServerIP=10.203.136.36

   EIMServerPort=15868

   The default port is 15868.

Related concepts
Configuring for TMG using non-web-proxy clients on page 233

Chapter 19

Integrating Forcepoint URL Filtering using ICAP Service

Contents

Applies to:

- Forcepoint URL Filtering, v8.5.x

ICAP Service makes it possible to integrate Forcepoint URL Filtering with third-party proxies and proxy-caches that support communication with ICAP servers.

Integration via ICAP affects the following web protection components:

- **ICAP Service** is installed with Filtering Service. It includes an ICAP server that enables third-party proxies to communicate with Filtering Service.
- **Filtering Service** interacts with ICAP Service and Network Agent to respond to Internet requests passed from the proxy via ICAP.

For installation instructions, see *Installing Forcepoint URL Filtering to integrate with ICAP Service*.

After installing your web protection software, configure your proxy to communicate with ICAP Service (see *Configuring the proxy to communicate with ICAP Service*).

ICAP Service may also require configuration (see *Configuring ICAP Service*) if the default settings are not appropriate for your environment.

To have Internet requests managed by Forcepoint URL Filtering, a computer must access the Internet through the integrated proxy.

When the proxy receives an Internet request, it uses ICAP to query ICAP Service to find out if the request should be blocked or permitted. ICAP Service queries Filtering Service, which checks the policy assigned to the client and either serves a block page or notifies the proxy to permit the request.

Related concepts

Installing Forcepoint URL Filtering to integrate with ICAP Service on page 242

Related tasks

Configuring the proxy to communicate with ICAP Service on page 243
Configuring ICAP Service on page 245

Installing Forcepoint URL Filtering to integrate with ICAP Service

Applies to:
■ Forcepoint URL Filtering, v8.5.x

The ICAP Service is installed with Filtering Service.

When running the web protection installer:

- Include Filtering Service as a component to install. If you are using the “All web protection components” option, Filtering Service is included by default.
- Select the **Install Forcepoint URL Filtering to integrate...** integration option, then select **ICAP Service** as the integration product.
- Follow the on-screen instructions to complete the installation. Refer to the Forcepoint URL Filtering installation instructions for more detailed information.

After installation, configure your ICAP integration. See:

- *Configuring the proxy to communicate with ICAP Service*
- *Configuring ICAP Service*

Converting a standalone installation to use ICAP integration

You can change a standalone Forcepoint URL Filtering installation to use ICAP integration without losing configuration settings.

1) Upgrade to the current version (if you are not already using the current version), then restart the Filtering Service machine.

2) Uninstall the existing instance of Filtering Service and Network Agent.

3) Reinstall Filtering Service to integrate with ICAP Service. Also reinstall Network Agent.
   - The components can be reinstalled at the same time if they are on the same machine.
   - If the components are on separate machines, first reinstall Filtering Service, then reinstall Network Agent.

4) Configure your ICAP integration. See:
   - *Configuring the proxy to communicate with ICAP Service*
   - *Configuring ICAP Service*

Related tasks

Configuring the proxy to communicate with ICAP Service on page 243
Configuring ICAP Service on page 245

Configuring the proxy to communicate with ICAP Service

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

The precise steps required to configure the third-party proxy to communicate with ICAP Service vary from product to product.

For Blue Coat SG Series appliances running SGOS 6.2 or later:

Steps

1) Log on to the Management Console and go to **Configuration > External Services > ICAP**.

2) Create an **ICAP Service** with a name like “ForcepointICAP.”

3) Enter the **Service URL** in the following format:
   icap://<ICAP_server_address>/<service_name>
   For example:
   icap://10.100.57.120/icap
   See *Configuring ICAP Service* for more information about setting or determining the service name.

4) Under ICAP Service Ports, verify that **This service supports plain ICAP connections** is selected, and that the **Plain ICAP port** value is set to **1344** (default).
   See *Configuring ICAP Service* for information about changing the ICAP port.

5) Under ICAP v1.0 Options, click **Sense settings** to request settings from ICAP Service.
   - When the settings are retrieved, the **Client address**, **Server address**, and **Authenticated user** boxes should be marked, and **“WEBSENSE”** should appear as the ICAP server tag.
   - If you do not want the proxy to authenticate users and pass user name information to your web protection software as part of the ICAP request, deselect the **Authenticated user** check box.

6) Click **OK** to close the Edit window.

Next steps

Additional configuration steps include:

- Configure a Web Access Layer rule to pass all traffic from any source to any destination to the ICAP server configured above, and specify whether the proxy should fail open (permit all traffic) or fail closed (block all traffic) when the ICAP server is not available.

- Configure a Web Access Layer rule to allow all traffic to the IP address of the Filtering Service machine. This allows client browsers to receive block pages.
- If you want the proxy to authenticate users and pass user name information to your web protection software, configure an authentication rule to authenticate users against a supported directory service.
  Note that if you are using Active Directory for user authentication, and use a hostname to identify the Active Directory server, make sure that the hostname resolves to the same IP address for both the third-party proxy and the Forcepoint Security Manager.

  Also, if Active Directory is identified by hostname in the proxy, the hostname is what appears in log records, even if Active Directory is identified by IP address in the Forcepoint Security Manager.
- Optionally configure HealthCheck for the external ICAP server. This causes the Blue Coat appliance to periodically send a URL filter request to the ICAP Service to ensure that it is still running and responding correctly.

Related tasks

Configuring ICAP Service on page 245

Configuring ICAP Service

Before you begin

Applies to:
■ Forcepoint URL Filtering, v8.5.x

ICAP Service behavior can be customized by modifying a configuration file called **icap.conf**, located in the **bin** directory (C:\Program Files\Websense\Web Security\bin, or /opt/Websense/bin/, by default) on the ICAP Service machine.

The **icap.conf** file can include the following parameters. Options marked with an asterisk appear in the file by default. The others can be added to the file if needed.

Parameter	Description	Default Value
WebsenseServer*	IP address of the Filtering Service instance associated with a ICAP Service instance	127.0.0.1
WebsenseServerPort	Filtering Service port used for WISP communication	15868
icapPort*	ICAP Service listening port	1344
icapServiceName*	Name of the ICAP service. Appears in the URL configured in the ICAP client. For example: *icap://<ip_address>/<name>*	icap
maxConnections*	Maximum number of ICAP server connections, and maximum number of connections from the ICAP server to Filtering Service.	200
optionsTTL*	Sent to the ICAP client in response to an OPTIONS request. The next OPTIONS request is sent after this number of seconds.	3600
serverIPEnabled	Sent to ICAP client in response to OPTIONS request. If TRUE, client should send the X-Server-IP field.	TRUE
failClosed*	If there are errors in the Filtering Service responses, should the request be blocked (fail closed) or permitted (fail open).	TRUE
connectionTimeout*	Number of minutes before a connect times out (expires)	5

To update the ICAP Service configuration:

Steps

1) Navigate to the **bin** directory (path noted above) and open **icap.conf** in a text editor.

2) Edit an existing parameter, or add a blank line at the end of the file and enter the parameter that you want to configure.

3) Save and close the file.

4) Restart **Websense ICAP Service**.

Chapter 20

Installing for Universal Integrations

Applies to:
■ Forcepoint URL Filtering, v8.5.x

This document describes integrating Forcepoint URL Filtering with supported integration products other than those addressed in the following topics:

- *Integrating Forcepoint URL Filtering with Cisco*
- *Integrating Forcepoint URL Filtering with Citrix*
- *Integrating Forcepoint URL Filtering using ICAP Service*
- *Integrating Forcepoint URL Filtering with TMG*

The Partners page at forcepoint.com links to pages that list our Security Alliance and Vendor Alliance partners. Refer to the list of Technology Partners to verify that your web protection software supports an integration with your firewall, proxy server, caching application, or network appliance.

Integrating Forcepoint URL Filtering with another product or device affects the following web protection components:

- **Filtering Service** interacts with your integration product and Network Agent to determine whether Internet requests are blocked or permitted.
- **Network Agent** manages Internet protocols that are not managed by your integration product. It can also detect HTTP network activity (managed by the integration) to enable bandwidth reporting.

When the integration product receives an Internet request, it queries Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service consults the policy assigned to the client determines how the requested site is categorized.

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies the integration product to grant access to the site.

Installation steps for universal integrations

This section provides a general overview of the installation process, highlighting the steps important to enabling integration.

For detailed installation instructions, see *Installing Web Protection Solutions*.

1) When you install Filtering Service, on the **Integration Option** screen, select **Install Forcepoint URL Filtering to integrate with a third-party product or device**.

2) On the **Select Integration** screen, select **Other (Universal Integration)**.

3) On the **Transparent User Identification** screen, you can choose whether to install a transparent identification agent.

- If your integration product provides user authentication or identification services, or if you do not intend to use user and group-based policy enforcement, select **None**.
- To use a transparent identification agent, select the agent or combination of agents appropriate for your deployment.

4) Follow the remaining installer prompts to complete the installation.
After installation is complete:

- To prevent users from circumventing policy enforcement, configure your firewall or Internet router to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from your integration product.
  Contact your router or firewall vendor for information about configuring access lists for that product.
- If Filtering Service connects to the Internet through a proxy server or firewall for HTTPS traffic, configure the proxy server or firewall to accept clear text or basic authentication to enable the Master Database download.

Migrating to a different integration after installation

You can change your integration product or version after installation without losing any of your configuration data.

1) Install and configure your new integration product. See your integration product documentation for instructions. Ensure that it is deployed in your network such that it can communicate with Filtering Service and Policy Server.

2) Use the Backup Utility to backup your web protection configuration and initialization files. See the Backup and Restore FAQ for instructions

3) Ensure that your web protection services are running. The installer looks for Policy Server during the installation process.

4) Remove Filtering Service using the procedures for removing components in the installation materials.

> **Warning**
>
> Remove Filtering Service only. Do **not** remove the associated Policy Server.

   If you have uninstalled Filtering Service from a Windows machine, restart the machine to complete the remove process.

5) Close any open applications, and stop any antivirus software, then run the installer again.

6) Add Filtering Service using the procedures for installing individual components. See *Adding web protection components*.

7) On the **Integration Option** screen, select the **Install Forcepoint URL Filtering to integrate...** option.

8) On the **Select Integration** screen, select **Other (Universal Integration)**.

9) Follow the installer prompts to complete the installation.
   The installer adds the new integration data, while preserving the previous configuration data.

   On Windows machines, to complete the installation, restart the machine.

10) Verify that Filtering Service has started.

- *Windows*: Open the Services tool (Start > Administrative Tools > Services or Server Manager > Tools > Services) and check to see if **Websense Filtering Service** is started.
- *Linux*: Navigate to the web protection installation directory (/opt/Websense/, by default), and enter the following command to see if **Filtering Service** is running:
  ./WebsenseAdmin status

  To start a service, follow the instructions in the installation materials.

11) To identify which Filtering Service instance is associated with each Network Agent:

   a) Log on to the Forcepoint Security Manager and select **Web > Settings > Network Agent**.

   b) Highlight the **Global** option, then select a Network Agent IP address to open its **Local Settings** page.

   c) Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.

   For more information, see Configuring Network Agent local settings.

12) If you stopped your antivirus software, be sure to start it again.

Related concepts

Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with TMG on page 221
Integrating Forcepoint URL Filtering using ICAP Service on page 241
Installing Web Protection Solutions on page 129

Related tasks

Adding web protection components on page 344

Chapter 21

Upgrading Multiple Forcepoint Solutions

Contents

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

If you have more than one Forcepoint security solution, use the sections below to find the appropriate set of upgrade instructions. Verify your current version before beginning your upgrade, because only certain versions can upgrade to the latest Forcepoint solution.

Forcepoint solutions were renamed in version 8.4.0.

- TRITON AP-DATA is now Forcepoint DLP.
- TRITON AP-EMAIL is now Forcepoint Email Security.
- TRITON AP-WEB is now Forcepoint Web Security.

Note

- Dual-mode V Series appliances are not supported with v8.3.0 and higher. Either the email or web security solution must be migrated to a new appliance.
- To ease the migration effort, special tools have been developed and a special procedure is recommended. Contact your Forcepoint account representative to learn about special promotions for dual-mode deployments planning an upgrade to v8.3.0 or higher.

All Forcepoint security solutions

For step-by-step instructions on upgrading the entire suite of Forcepoint on-premises security solutions, see Upgrading Forcepoint Security Solutions.

If the existing deployment is not at a version that can be directly upgraded to v8.5.x, v8.6, or v8.7.x, see:

- Upgrading TRITON v7.7.x to v7.8.x
- Upgrading TRITON v7.6.x to v7.7.x
- Upgrading TRITON APX Suite to v8.3

For an outline of the process, see *Upgrade procedure for solutions that include web, email, and data protection*.

Web and data protection

If you are combining Forcepoint DLP (TRITON AP-DATA) and Forcepoint Web Security (TRITON AP-WEB), the recommended process is to first complete the steps in Upgrade Instructions: Forcepoint Web Security. This document guides you through upgrading:

- All TRITON AP-WEB components
- The management server (which includes most TRITON AP-DATA components)

After completing those steps, see the upgrade guide for your version to find instructions on upgrading additional DLP components, such as the protector and agents:

- Upgrading to Forcepoint DLP v8.5.x
- Upgrading to Forcepoint DLP v8.6.x
- Upgrading to Forcepoint DLP v8.7.x
- Upgrading to Forcepoint DLP V8.8.x
- Upgrading to Forcepoint DLP v8.9.x
- Upgrading to Forcepoint DLP v9.0

Web and email protection

If you are combining Forcepoint Web Security (TRITON AP-WEB) and Forcepoint Email Security (TRITON AP-EMAIL), the recommended process is to follow the steps in Upgrading Forcepoint Security Solutions. This document guides you through upgrading:

- All TRITON AP-WEB and Forcepoint Web Security components
- All TRITON AP-EMAIL and Forcepoint Email Security components
- The management server, which includes DLP Module components for both web and email security solutions

Email and data protection

If you are combining Forcepoint DLP (TRITON AP-DATA) and Forcepoint Email Security (TRITON AP-EMAIL), the recommended process is to follow the steps in Upgrading to Forcepoint Email Security v8.5.x. This document guides you through upgrading:

- All TRITON AP-EMAIL and Forcepoint Email Security components
- The TRITON management server or Forcepoint management server, which includes most TRITON AP-DATA and Forcepoint DLP components

After completing those steps, see the upgrade guide for your version to find instructions on upgrading additional DLP components, such as the protector and agents:

- Upgrading to Forcepoint DLP v8.5.x
- Upgrading to Forcepoint DLP v8.6.x
- Upgrading to Forcepoint DLP v8.7.x
- Upgrading to Forcepoint DLP V8.8.x
- Upgrading to Forcepoint DLP v8.9.x
- Upgrading to Forcepoint DLP v9.0

Related tasks
Upgrade procedure for solutions that include web, email, and data protection on page 253

Upgrade procedure for solutions that include web, email, and data protection

Before you begin

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x

This outline summarizes the steps required to upgrade the entire suite of Forcepoint on-premises security solutions. Forcepoint Email Security always includes Forcepoint DLP components.

For complete instructions, see Upgrading Forcepoint Security Solutions.

Steps

1) Upgrade **Policy Broker**. All components on the Policy Broker machine (which may be a **full policy source** appliance) are upgraded in the correct order.

   If there are multiple Policy Brokers, upgrade the primary Policy Broker first. Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with the replicas.

2) Upgrade any instances of **Policy Server** running off the Policy Broker machine. All components on each Policy Server machine, including user directory and filtering appliances, are upgraded in the correct order.

3) Upgrade any additional instances of **Filtering Service** and **User Service**, running on other machines. All components on each machine, including filtering only appliances, are upgraded in the correct order.

4) Upgrade the web security **Log Server**. All components on the machine are upgraded in the correct order.

5) Upgrade the email security **Log Server**. All components on the machine are upgraded in the correct order.

6) Upgrade the **management server**. All modules on the machine are upgraded in the correct order.

7) Upgrade all other appliances in your network. This can be done in any order, and can be completed in parallel.
   - If Email Security is deployed in cluster mode, you must release all appliances from the cluster before upgrading or migrating. Upgrade each appliance as needed, and then rebuild your cluster after the process is complete.
   - The Email MTA continues to function after the management server upgrade, but the logs are cached on the appliance until Forcepoint Email Security is upgraded as well. For best practice, redirect email traffic to another MTA as cached messages may be lost otherwise.

8) Upgrade any additional software instances of Network Agent and Content Gateway. If these components run on V Series and X Series appliances, this step has already been done.

9) Upgrade any additional Web Security components, including transparent identification agents and Remote Filtering Server, that may be running on other machines.

10) Upgrade any additional Data Security components and agents, including supplemental servers, FCI agents, protectors, and mobile agents.

11) Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, Forcepoint Web Security Endpoint, and Forcepoint DLP Endpoint.

Upgrading the management server

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

To upgrade Forcepoint management server components, use the appropriate Forcepoint Security Installer for your version (Windows only): **Forcepoint8xxSetup.exe**, where “8xx” is the full version number.

1) Download the installer from the **Downloads** section of the My Account page at support.forcepoint.com.

2) Select the link for the appropriate version under any on-premises security.

3) Select the installer (typically the first entry in the list), then, on the installer page, click **Download**.

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

5) Close all applications and stop any antivirus software.

Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

6) Right-click **Forcepoint8xxSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.

When the installer launches, it detects that earlier versions of the product are installed, and automatically starts a series of upgrade wizards—one for each of the modules included on the management server.

Note

You may be prompted to restart the machine after each component is upgraded. This is optional. It is okay to restart the machine once after all components are upgraded.

Management infrastructure

The Forcepoint Management Infrastructure (formerly TRITON infrastructure) provides a basic framework for all of the management components that make up the Forcepoint Security Manager (formerly TRITON Manager). This framework includes a central settings database that stores shared configuration (such as administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Welcomes you to the installation and upgrade wizard. 1) Click **Next** to begin the upgrade process. The system checks disk space requirements. 2) When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows: ■ The destination folder for the installation files. ■ The name of the SQL Server machine and the user name of an authorized database administrator. ■ The IP address of the Forcepoint management server and administrator credentials. Click **Next** to accept the properties.
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage, warning that you must also upgrade all modules. This popup may be hidden behind the main installer window, so if your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation.

Wizard Screen	Fields
Summary	When module upgrade is complete, summarizes your system settings, including: ■ The destination folder for the installation files. ■ The name of the SQL Server machine and the user name of an authorized database administrator. ■ The IP address of the Forcepoint management server and administrator credentials. Click **Finish** to complete the upgrade for this module.

Web protection

The Forcepoint Web Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	Welcomes you to the upgrade wizard. Click **Next** to continue.
Pre-Upgrade Summary	Informs you that a previous web protection software version was detected. 1) Click **Next** to start the upgrade. The installer proceeds to stop all Forcepoint services. This can take up to 10 minutes. When complete, it tells you which components will be upgraded. 2) Click **Install** to continue. The installer backs up critical files.
Installing Forcepoint	Shows installation progress. When complete, the installer configures your software. This can take up to 10 minutes.
Upgrade Complete	You are notified when installation of this module is complete. Click **Done** to exit the installer.

Data protection

Before running the Forcepoint DLP upgrade wizard, the installer validates system requirements to ensure that the upgrade will be successful.

The pre-upgrade check validates hardware requirements, credentials for the SQL Server database, endpoint security certificates, manager configuration, administrator upgrade permissions, and database structure. As it proceeds, it reports whether a step succeeded or failed, or issues a warning.

If there is a failure, the upgrade stops. For details, see **\AP-DATA- PreUpgradeTests.log** in the product installation directory.

If there are only warnings, it is possible to proceed with the upgrade. In this case, be aware that the system may behave unexpectedly, but this will not have a critical impact.

After the pre-upgrade check, the Forcepoint DLP upgrade wizard is launched.

The upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard for Forcepoint DLP. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Installation Confirmation	Verify the system settings and click **Install** to continue the upgrade.
Installation	This screen shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more. In some cases, an internal SQL error may occur. Do not click OK until the issue has been resolved with Forcepoint Technical Support. Continuing prematurely can cause problems with the reporting database.
Summary	When installation of this module is complete, this screen summarizes the system settings. 1) Click **Done**. A prompt to update predefined policies and content classifiers appears. 2) Click **OK** to install the updates. The status of the updates is displayed, including the items being updated, and details such as how many policies are updated, deleted, or added. 3) Click **Close** when the updates are complete.

Email protection

The Forcepoint Email Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	This screen welcomes you to the Forcepoint Email Security upgrade wizard. Click **Next** to continue.
Select Components	This screen shows the components that will be upgraded (those that are currently installed). Click **Next** to continue.

Wizard Screen	Fields
Configuration	This page shows the IP address of the database engine configured to manage the Email Log Database and the logon type. If you have changed the database since your previous installation, modify the settings here.
Pre-Installation Summary	This screen shows: ■ The components to be installed ■ The pre-existing and new version numbers ■ The destination folder for the installation files ■ The required and available disk space Click **Install** to begin the upgrade.
Installation	This screen shows that the installation is progressing. The Email Security module of the Security Manager is upgraded on the Forcepoint management server. The Email Log Server is upgraded on machines where it is found. When complete, the installer configures the software. This can take up to 10 minutes.
Summary	You are notified when installation of this module is complete. Click **Done** to exit the installer.

Post-upgrade steps

Once the Forcepoint management server upgrade is complete:

1) Restart the management server.

2) Log on to the Forcepoint Security Manager:
https://<IP_address_or_hostname>:9443

3) Click **Data** to select the Data Security module.

4) Follow the prompts that appear for updating data loss protection policies and classifiers.
Depending on the number of existing policies, this can take up to an hour. During this time, do not restart the server or any of the services.

5) If any applications were removed from predefined endpoint application groups prior to upgrade, go to the **Main > Resources > Endpoint Application Groups** page and remove them again. The upgrade process restored these to their original state.

6) Click **Deploy**.

7) Select the Email Security module and navigate to the page **Settings > General > Database Downloads**.

8) Click **Update Now** to perform an immediate database download update.

For information on upgrading other Forcepoint DLP components, such as supplemental servers, agents, and Forcepoint DLP Endpoint (formerly TRITON AP-ENDPOINT DLP), refer to *Upgrading to Forcepoint DLP v9.0*.

Related concepts

Upgrading to Forcepoint DLP on page 297

Chapter 22

Upgrading Web Protection Solutions

Contents

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x
- Forcepoint Appliances, v8.5.x

Version 8.4 introduced new product names and solution bundles for web protection solutions.

New Name	Older Names
Forcepoint URL Filtering	Web Filter & Security Web Filter Web Security
Forcepoint Web Security	TRITON AP-WEB Websense TRITON Web Security Gateway
Forcepoint Web Security with: ■ Hybrid Module ■ DLP Module ■ Forcepoint Advanced Malware Detection (if purchased)	TRITON AP-WEB with: ■ Web Hybrid Module ■ Web DLP Module ■ Web Sandbox Module (if purchased) Websense TRITON Web Security Gateway Anywhere

For more information about how these changes may affect you, or to change the add- on modules activated by your subscription, contact your sales partner or Forcepoint Sales representative.

Important

- V Series dual-mode appliance users:
  - Dual-mode appliances are not supported with version 8.3.0 and higher. Either Forcepoint Email Security or the web protection solution must be migrated to a new appliance.
  - To ease the migration effort, special tools have been developed, and a special procedure is recommended. For details, see Upgrading V Series Dual-Mode Appliances to Version. Contact your Forcepoint account representative to learn about special promotions for dual-mode deployments planning an upgrade to v8.3 or higher.
- V Series appliance users:
  - Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher. See V Series appliances supported with version 8.0 and higher.

Your upgrade path depends on both the product you have subscribed to and the deployment model you are using. Find the entry in the table below that best describes your current deployment to determine your upgrade path.

Product & Deployment	Upgrade Path
Web Filter, Web Security, or Web Filter & Security on **Software or Forcepoint appliance**	Direct upgrade from v8.1.x, 8.2.x, 8.3.x, or 8.4.x to v8.5. Direct upgrade from v8.2.x, 8.3.x, 8.4.x, or 8.5 to v8.5.3. Direct upgrade from v8.4, v8.5 and v8.5.3 to 8.5.4. See Upgrade Instructions: Forcepoint URL Filtering (a start-to finish PDF).
Web Security Gateway *or* Web Security Gateway Anywhere *or* TRITON AP-WEB **Software or Forcepoint appliance**	Direct upgrade from v8.1.x, 8.2.x, 8.3.x, or 8.4.x to v8.5. Direct upgrade from v8.2.x, 8.3.x, 8.4.x, or 8.5 to v8.5.3. Direct upgrade from v8.4, v8.5 and v8.5.3 to 8.5.4. See Upgrade Instructions: Forcepoint Web Security (a start-to-finish PDF).

Direct upgrades from v7.8.x or v8.0.x to v8.5, from v7.8.x - v 8.1.x to v8.5.3, or from 7.8.x, 8.0.x, 8.1.x, 8.2.x or 8.3.x to v8.5.4 are not supported but upgrade information is provided in the Upgrade Instructions linked above. If you are upgrading from a version that does not support direct upgrade to v8.5.x, see *Upgrading from web security version 8.1 or earlier*. Policy information and most configuration details are preserved across intermediate upgrades.

To customize your upgrade process, rather than using the complete PDF instructions linked above, see:

- *Web protection or web and data protection upgrade outline*
- *Before upgrading to v8.5.x web protection solutions*

Related concepts

Upgrading from web security version 8.1 or earlier on page 264
Before upgrading to v8.5.x web protection solutions on page 265

Related tasks

Web protection or web and data protection upgrade outline on page 263

Web protection or web and data protection upgrade outline

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Tip

When you follow a link in this outline, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the task.

Steps

1) Review the Release Notes for your solution and deployment platform. The Release Notes are available from support.forcepoint.com.
   - Web Protection Solutions for v8.5
   - Web Protection Solutions for v8.5.3
   - Web Protection Solutions for v8.5.4.
   - Forcepoint Appliances for v8.5
   - Forcepoint Appliances for v8.5.3
   - Forcepoint Appliances for v8.5.4
   - Forcepoint DLP for v8.5.1
   - Forcepoint DLP for v8.6
   - Forcepoint DLP for v8.7
   - Forcepoint DLP for v8.7.1
   - Forcepoint DLP for v8.8.
   - Forcepoint DLP for v8.8.1
   - Forcepoint DLP for v8.8.2
   - Forcepoint DLP for v8.9
   - Forcepoint DLP for v8.9.1
   - Forcepoint DLP for v9.0

2) Before beginning the upgrade process, see:
   - *Before upgrading to v8.5.x web protection solutions*
   - V Series Appliance Upgrade Guide
   - X Series Appliance Upgrade Guide
   - V, X, & Virtual Appliance Upgrade Guide

3) When you are ready to start upgrading, see *Upgrading web or web and data protection solutions from v8.1.x or later*.
   This procedure includes both software and appliance instructions.

Related concepts
Before upgrading to v8.5.x web protection solutions on page 265

Related tasks
Upgrading web or web and data protection solutions from v8.1.x or later on page 272

Upgrading from web security version 8.1 or earlier

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

See the second table in *Upgrading Web Protection Solutions* to find out if your product can be directly upgraded to v8.5.x.

If your are upgrading from a version that does not support direct upgrade to v8.5.x, you can perform additional, intermediate upgrade steps. For example, the path might be:

- v7.5 (Web Filter, software-only) > v7.7 > v8.0 > 8.3 > 8.4 > v8.5.x
- v7.5 (Web Security Gateway) > v7.6 > v7.7 > v7.8.4 > v8.3> 8.4 > v8.5.x

Policy information and most configuration details are preserved across intermediate upgrades.

Follow the upgrade instructions for each intermediate version, available from support.forcepoint.com:

- v7.6 software Upgrade Instructions
- v7.6 appliances Upgrade Instructions
- v7.7 software Upgrade Instructions
- v7.7 appliances Upgrade Instructions
- v7.8 upgrade instructions cover both software and appliance:
  - Upgrade Instructions: Web Filter and Web Security
  - Upgrade Instructions: Web Security Gateway
  - Upgrade Instructions: Web SecurityGateway Anywhere

- v8.0 upgrade instructions cover both software and appliance:
  - Upgrade Instructions: TRITON AP-WEB
  - Upgrade Instructions: Web Filter & Security
- v8.1 upgrade instructions cover both software and appliance:
  - Upgrade Instructions: TRITON AP-WEB
  - Upgrade Instructions:Web Filter & Security

Because hardware and operating system support has changed over time, the upgrade process for software (non-appliance) components is likely to require hardware and operating system updates. See *Migrating web solutions to a new operating system* for details.

If you are upgrading from a version prior to 7.5, given fundamental changes to software functionality, operating system support, and hardware requirements, the smoothest path to v8.5.x is to perform a fresh installation at the current version. See *Installing Web Protection Solutions*.

After upgrading to a version from which you can upgrade to v8.5.x, see the following start-to-finish PDF instructions to upgrade to v8.5.x:

- Upgrade Instructions: Forcepoint Web Security
- Upgrade Instructions: Forcepoint URL Filtering

Related concepts
Upgrading Web Protection Solutions on page 261
Migrating web solutions to a new operating system on page 299
Installing Web Protection Solutions on page 129

Before upgrading to v8.5.x web protection solutions

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

The upgrade process is designed for a properly functioning deployment of web protection software. Upgrading does not repair a non-functional system.

Tip

When you follow a link in this list, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the task.

Important

- **V Series dual-mode appliance users:**
  Dual-mode appliances are not supported with version 8.3.0 and higher. Either Forcepoint Email Security or the web protection solution must be migrated to a new appliance.

  To ease the migration effort, special tools have been developed, and a special procedure is recommended. For details, see Upgrading V Series Dual-Mode Appliances. Contact your Forcepoint account representative to learn about special promotions for dual-mode deployments planning an upgrade to v8.3 or higher.
- **V Series appliance users:**
  Some older V10000 and V5000 appliances are not supported with this version.

  See V Series appliances supported with version 8.0 and higher.

Before upgrading to a v8.5.x web protection solution:

1) Make sure the installation machine meets the hardware and operating system recommendations in *System requirements for this version*.
   In addition, with v8.5.3, Master Database enhancements were made that greatly increased the size of the database files. When upgrading to v8.5.3 or v8.5.4 from 8.5 or earlier, the new database files will replace the existing files. Prior to upgrading, confirm there is at least 6 GB of additional free space available on each Filtering Service machine.

2) Verify that third-party components that work with your web protection solution, including your database engine and directory service, are supported. See Requirements for web protection solutions section in *System requirements for this version*.

3) Make sure that your integration product (if any) is supported in v8.5.x. If necessary, upgrade your integration product before beginning the web protection software upgrade.
   - For information about integration with Microsoft Forefront TMG, see *Integrating Forcepoint URL Filtering with TMG*.
   - For information about integration with Citrix, see *Integrating Forcepoint URL Filtering with Citrix*.
   - To review current Cisco integration requirements, see *Integrating Forcepoint URL Filtering with Cisco*.
   - To integrate with a Blue Coat proxy, see *Integrating Forcepoint URL Filtering using ICAP Service* for more information about installing and configuring ICAP Service.
   - To review current integration requirements for other products, see *Installing for Universal Integrations*.

4) Back up all of your web protection components, including the management server and any appliances, before starting the upgrade process. See the **Backup and Restore FAQ** for your version for instructions. The FAQ is available in the Technical Library.

5) Before upgrading Filtering Service, make sure that the Filtering Service machine and the management server have the same locale settings (language and character set).
   After the upgrade is complete, Filtering Service can be restarted with any locale settings.

6) Before upgrading any Policy Server, make sure that all instances of Multiplexer are enabled and started. This step is required even if you are not integrated with a third-party SIEM solution.

7) If your product includes the Web Security DLP Module, before upgrading the management server, make sure those components are ready for upgrade:
   a) Stop all discovery and fingerprinting tasks.

b) Route all traffic away from the system.

c) Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.

d) Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.

e) If your organization was supplied with custom file types, change the name of the following files in the **policies_store\custom_policies\config_files** folder on the management server; otherwise they will be overwritten during upgrade.

- Change **extractor.config.xml** to **custom_extractor.config.xml**.
- Change **extractorlinux.config.xml** to **custom_extractorlinux.config.xml**.

The filenames are case-sensitive.

f) If custom policies were provided, submit a request for updated versions before proceeding.

8) When upgrading from v8.4 or earlier, a new logging partition is added to your Log Database. Please make sure you do not have 70 active partitions (the limit) prior to upgrading. Use the **Web > Settings > Reporting > Log Database** page of the Forcepoint Security Manager to disable at least one active partition prior to upgrading.

9) It is important that you back up your current Log Database and stop any active Log Database jobs prior to upgrading. See *Preparing the Log Database for upgrade*.

10) If Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:

a) Launch the Windows Services tool.

b) Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.

11) If your deployment includes V Series or X Series appliances, see the V Series Upgrade Guide or X Series Upgrade Guide for additional preparatory steps.

Restart services before starting the upgrade

Web protection services must be running before the upgrade process begins. If any service is stopped, start it before initiating the upgrade.

The installer will stop and start web protection services as part of the upgrade process. If the services have been running uninterrupted for several months, the installer may not be able to stop them before the upgrade process times out.

To ensure the success of the upgrade, manually stop and start all the web protection services before beginning the upgrade:

- *Windows*: Navigate to the **bin** directory (C:\Program Files \Websense\Web Security, by default) and enter the following command:
  `WebsenseAdmin restart`
- *Linux*: Navigate to the **Websense** directory (/opt/Websense/, by default) and enter the following command:
  `./WebsenseAdmin restart`
- *Appliance*: Refer to the Appliances CLI Guide.

Internet access during the upgrade process

When you upgrade a web protection solutions standalone installation, policy enforcement stops when your web protection services are stopped. Users have full access to the Internet until the web protection services are restarted.

If web protection solutions are integrated with another product or device, all traffic is either permitted or blocked during the upgrade, depending on how your integration product is configured to respond when Filtering Service is unavailable.

The Master Database is removed during the upgrade process. Filtering Service downloads a new Master Database after the upgrade is completed.

Find your upgrade procedure

When you are sure you have complete backups of your existing configuration and are ready to begin the upgrade process, see *Upgrading web or web and data protection solutions from v8.1.x or later*.

Related concepts

Integrating Forcepoint URL Filtering with TMG on page 221
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering using ICAP Service on page 241
Installing for Universal Integrations on page 247

Related tasks

Preparing the Log Database for upgrade on page 269
Upgrading web or web and data protection solutions from v8.1.x or later on page 272

Related reference

System requirements for this version on page 9

Preparing the Log Database for upgrade

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

It is important that you back up your current web protection reporting databases, stop Log Server, and stop all Log Database jobs.

Warning

- If database operations are active during upgrade, the Log Database may be left in an inconsistent state, rendering it unusable.
- When this occurs, it can be difficult to fix.
- Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

Steps

1) Back up the databases and stop Log Server.

   a) Back up the reporting databases for your web protection solution.

   Refer to Microsoft documentation for instructions on backing up databases. The web protection databases are named wslogdb70 (the catalog database), wslogdb70_amt_1 (the threats partition), and wslogdb70_1, wslogdb70_2, and so on (the standard logging partition databases).

   b) On the Log Server machine, use the Windows Services tool to stop **Websense Log Server**.

2) Make sure no database jobs are running.

It is best to **stop all Log Database jobs** prior to starting the upgrade, but, before it upgrades the Log Database, the upgrade process will attempt to stop any Log Database jobs not already stopped. If the jobs cannot be stopped, you will need to stop them manually. However, you do not need to exit the installer to do that.

Stop the Log Database jobs using these steps:

- If you have a full version of Microsoft SQL Server:

  a) Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).

  b) To disable all currently active SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

  - Websense_ETL_Job_wslogdb70
  - Websense_AMT_ETL_wslogdb70
  - Websense_IBT_DRIVER_wslogdb70
  - Websense_Trend_DRIVER_wslogdb70
  - Websense_Maintenance_Job_wslogdb70

  Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

  Make sure all jobs have completed any current operation before proceeding with upgrade.

  c) After upgrade, verify that the jobs have been to enabled.
  Enable any that were not automatically enabled by the upgrade process. Normal database operations will then resume.

- If you have SQL Server Express:

  a) Log in to the Microsoft SQL Server Management Studio.

  b) Expand the **Databases** tree to locate the catalog database (wslogdb70, by default), then expand the catalog database node.

  c) Expand **Service Broker > Queues**.

  d) Right click **dbo.wse_scheduled_job_queue** and select **Disable Queue**.

  e) The upgrade process will re-enable the job queue. After upgrade, verify that the Queue has been enabled.
  Enable it, if necessary, by repeating the process, this time ultimately selecting **Enable Queue** to resume normal database operations.

Web protection upgrade order

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

When you upgrade your web protection solutions, the installer or appliance patch automatically upgrades all components on a given machine in the correct order.

As a result, if you have a main server or appliance hosting most of your web protection components (including Policy Broker), upgrade that machine first, then use the list below to determine the upgrade order for any additional servers or appliances.

If your components are widely distributed, however, ensure that they are upgraded in the correct order, as follows:

Steps

1) Policy Broker (primary or standalone)

   If you are using Forcepoint appliances, Policy Broker runs on the **full policy source** appliance or server. Regardless of the other components running on the machine, always upgrade the Policy Broker machine first. The other components on the machine are upgraded in the correct order.

2) Replica Policy Brokers

   Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with them. If Policy Server is installed on the same machine, it will be upgraded at the same time.

3) Policy Server

   Runs on all **user directory and filtering** appliances, and may run on other Windows or Linux servers.

4) User Service, Filtering Service, and Directory Agent

   This includes all **filtering only** appliances, and may include other Windows or Linux servers.

5) Log Server and Sync Service

   Make sure that all Log Database jobs are stopped before starting the Log Server upgrade. See *Preparing the Log Database for upgrade*.

6) Forcepoint Security Manager

7) Content Gateway, Network Agent

8) Transparent identification agents, Remote Filtering Server, filtering plug-in (Citrix XenApp or Microsoft Forefront TMG)

Next steps

Once all server components have been upgraded, upgrade client components (the logon application, Remote Filtering Client, Forcepoint Web Security Endpoint) in any order. See:

- Using Logon Agent for Transparent User Identification
- *Installing Forcepoint F1E Solutions*

Related concepts
Installing Forcepoint F1E Solutions on page 181

Related tasks
Preparing the Log Database for upgrade on page 269

Upgrading web or web and data protection solutions from v8.1.x or later

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x ■ Forcepoint Security Solutions, v8.5.x, v8.6.x, v8.7.x

This procedure covers the steps required to upgrade any web protection solution, or web and data solutions together, from versions that support direct upgrade to v8.5.x.

Tip

When you follow a link in this procedure, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the procedure.

Steps

1) Upgrade **Policy Broker**. All components on the Policy Broker machine, which may be a **full policy source** appliance, are upgraded in the correct order. For instructions, see:
   - *v8.5.x web protection software upgrade instructions (Windows)*
   - *v8.5.x Linux upgrade instructions for web protection products*
   - *Upgrading Forcepoint Appliances to v8.5.x*

2) Upgrade any instances of **Policy Server** running off the Policy Broker or machine. All components on each Policy Server machine, including **user directory and filtering** appliances, are upgraded in the correct order. For instructions, see:
   - *v8.5.x web protection software upgrade instructions (Windows)*
   - *v8.5.x Linux upgrade instructions for web protection products*
   - *Upgrading Forcepoint Appliances to v8.5.x*

3) Upgrade any additional instances of **Filtering Service** and **User Service**, running on other machines. All components on each machine, including **filtering only** appliances, are upgraded in the correct order. For instructions, see:
   - *v8.5.x web protection software upgrade instructions (Windows)*
   - *v8.5.x Linux upgrade instructions for web protection products*
   - *Upgrading Forcepoint Appliances to v8.5.x*

4) Upgrade **Log Server**. All components on the machine are upgraded in the correct order. For instructions, see *v8.5.x web protection software upgrade instructions (Windows)*.

5) Upgrade the **management server**. In Web Security Gateway Anywhere deployments, TRITON AP-WEB deployments, or Forcepoint Web Security deployments that include the Web Security DLP Module, or any other deployments that include both Web and Data, the Data components on the machine are detected and automatically upgraded in the correct order. See:
   - *v8.5.x web protection software upgrade instructions (Windows)*.
   - *Upgrading to Forcepoint DLP v9.0*.

6) Upgrade any additional Network Agent instances and, if applicable, Content Gateway. If these components run on V Series appliances, this step has already been done. See:
   - *Upgrading Content Gateway to v8.5.x*.
   - *v8.5.x web protection software upgrade instructions (Windows)*
   - *v8.5.x Linux upgrade instructions for web protection products*

7) Upgrade any additional web protection and, if applicable, data protection server components, including Protector, transparent identification agents, and Remote Filtering Server, that may be running on other machines. See:
   - *v8.5.x web protection software upgrade instructions (Windows)*
   - *v8.5.x Linux upgrade instructions for web protection products*
   - *Upgrading to Forcepoint DLP v9.0*

Next steps

When you are finished, see:

- *Installing Forcepoint F1E Solutions* for information about deploying endpoint client software, including Remote Filtering Client, Forcepoint Web Security Endpoint, and Forcepoint DLP Endpoint.
- Using Logon Agent for Transparent User Identification, for information about deploying the logon application (LogonApp.exe).

Related concepts

v8.5.x web protection software upgrade instructions (Windows) on page 274
Upgrading Forcepoint Appliances to v8.5.x on page 295
Upgrading to Forcepoint DLP on page 297
Upgrading Content Gateway to v8.5.x on page 283
Installing Forcepoint F1E Solutions on page 181

Related tasks

v8.5.x Linux upgrade instructions for web protection products on page 278

v8.5.x web protection software upgrade instructions (Windows)

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Use the v8.5.x Setup program for Windows (**Forcepoint85xSetup.exe**) to perform the upgrade. The installer detects:

- That older version components are installed
- Which components are installed
- The database engine version

Important

Follow the upgrade order provided in *Upgrading web or web and data protection solutions from v8.1.x or later* to ensure that you are upgrading components in the correct order. Upgrade the Policy Broker machine first, then any machines running Policy Server. Distributed components on other machines must be upgraded **after** Policy Broker and Policy Server.

Before beginning:

- If you performed an intermediate upgrade, and you have not restarted the upgraded machines, perform a restart before beginning the v8.5.x upgrade.
- Perform a full system backup. See the **Backup and Restore FAQ** for your version for instructions.

Important

Policy enforcement and logging services are not available while you are performing the upgrade. To reduce the impact on network users, run the upgrade after hours, or during a quiet time on the network.

Perform the following procedure on each machine running web protection components.

1) Make sure that no administrators are logged on to the management console.

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

> **Important**
>
> If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3) Stop Log Server and disable SQL Server Agent jobs. See *Preparing the Log Database for upgrade*.

4) Close all applications and stop any antivirus software.

> **Warning**
>
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

5) Go to the **Downloads** tab of the forcepoint.com My Account page to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 2 GB of disk space.

6) Double-click **Forcepoint85xSetup.exe** to launch the installer. A progress dialog box appears, as files are extracted.

> **Note**
>
> A security update done for the v8.5.4 product release has resulted in a new requirement for a specific dynamic-link library (dll) when upgrading to v8.5.4 Forcepoint Web Security software on a Windows platform. See **Security Enhancements** in the v8.5.4 Release Notes for Web Protection Solutions for more information.

7) The installer detects web protection components from an earlier version and asks how you want to proceed.
Click **OK**.

8) On the installer **Introduction** screen, click **Next**.
Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

9) On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.

10) When you click **Next**, a *Stopping All Services* progress message appears. Wait for the services to be stopped.
The **Pre-Upgrade Summary** screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the web protection services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the **WebsenseAdmin stop** command, or the Windows Services tool, to stop the services. Once you have manually stopped the services, return to the installer.

11) On the **Pre-Upgrade Summary** screen, review the list of components that will be upgraded, and then click **Install**.
Critical files are backed up and install properties initialized. And then the **Installing...** screen appears.

The upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.

12) Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.

13) Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

14) If you stopped your antivirus software, restart it.

15) Re-enable SQL Server Agent jobs if you disabled them prior to upgrade. See *Preparing the Log Database for upgrade*.

16) If you have an integration product installed, additional upgrade steps may be necessary. See:
- *Integrating Forcepoint URL Filtering with Cisco*
- *Integrating Forcepoint URL Filtering with Citrix*
- *Integrating Forcepoint URL Filtering with TMG*
- *Installing for Universal Integrations*

17) Repeat the upgrade procedure on each machine running web protection components, in the recommended order (see *Web protection upgrade order*).
All components that interact must be upgraded to the same version.

If you have complete installations in separate locations that do not interact, they do not have to run the same web protection software version.

To add additional components to a machine after upgrade, run the installer again on the same machine. This time, the installer will ask if you want to add components. See *Adding or modifying Windows components*.

New security certificate

After upgrade, the first time you launch Forcepoint Security Manager, the browser displays a certificate error.

This appears because Security Manager uses a certificate signed by Forcepoint, which is not a recognized certificate authority.

When you install the certificate in your browser, communication with the management console is secured, and the certificate warning is not displayed again (in this browser).

To install the certificate in Internet Explorer

You can either run an ActiveX control to install the certificate automatically, or you can install the certificate manually.

To install the certificate automatically (requires ActiveX to be enabled in the browser):

1) On the browser warning page, click **Continue to this website (not recommended)**. You must click through the warning once to be able to install the certificate.

2) Click the yellow warning box on the logon screen (where the message **Forcepoint security certificate is required**) appears.

3) In the pop-up box, click the **install the certificate** link.

4) If prompted, provide credentials to allow the certificate to be installed, then click **Yes**.

5) If the browser pops up a yellow security warning bar, click the yellow bar to allow the program that installs the certificate to run.

To install the certificate manually:

1) On the browser warning page, click **Continue to this website (not recommended)**. You must click through the warning once to be able to install the certificate.

2) Click **Certificate Error** on the browser's address bar (to the right of the management console URL), and then select **View certificate**.

3) In the Certificate dialog box, click **Install Certificate**.

4) Mark the **Place all certificates in the following store** radio button, and then click **Browse**.

5) Select the **Trusted Root Certification Authorities** folder, and then click **OK**.

6) Click **Next**, and then **Finish**.

7) When prompted to install the certificate, click **Yes**, and then click **OK** to close the success message.

After the certificate is installed, you can launch the Forcepoint Security Manager using this browser without receiving further errors.

To install the certificate in Firefox

On the Secure Connection Failed page:

1) Click **Or you can add an exception**.

2) Click **Add Exception**.

3) Make sure that **Permanently store this exception** is selected, and then click **Confirm Security Exception**.

After the certificate is installed, you can launch the Forcepoint Security Manager using this browser without receiving further errors.

Related concepts

Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with TMG on page 221
Installing for Universal Integrations on page 247
Adding or modifying Windows components on page 342

Related tasks

Upgrading web or web and data protection solutions from v8.1.x or later on page 272
Preparing the Log Database for upgrade on page 269
Web protection upgrade order on page 271

v8.5.x Linux upgrade instructions for web protection products

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

Use the Linux installer (**Web85xSetup_Lnx.tar.gz**) to upgrade existing components. After the installer starts, it detects which web protection components are installed and need to be upgraded.

Perform a full system backup before starting the upgrade process. See the **Backup & Restore FAQ** for your version for instructions.

If components are installed on multiple machines, see *Web protection upgrade order* for important information about the required upgrade sequence.

Important

- Upgrade the primary (or standalone) Policy Broker machine first, then any replica Policy Broker machines, then any machines running Policy Server.
  Distributed components on other machines must be upgraded **after** Policy Broker and Policy Server.
- Policy enforcement and logging services are not available while you are performing the upgrade. To reduce the impact on network users, run the upgrade after hours, or during a quiet time on the network.

Perform the following procedure on each machine running web protection components.

Steps

1) Make sure no administrators are logged on to the management console.

2) Log on the installation machine with administrator privileges (typically, as **root**).

3) Close all applications and stop any antivirus software.

4) Check the **etc/hosts** file. If there is no host name for the machine, add one. See *Preparing for installation* for instructions.

5) Create a setup directory for the installer files, such as **/root/Forcepoint_setup**.

Important

If your web protection services have been running uninterrupted for several months, the installer may have difficulty stopping them. To prevent the upgrade process from timing out and failing, use the **/opt/Websense/WebsenseAdmin restart** command to restart the services manually before beginning the upgrade.

6) Go to the **Downloads** tab of the forcepoint.com My Account page to download the Linux installer. The installer file is called **Web85xSetup_Lnx.tar.gz**.

7) Uncompress the installer file and use one of the following commands to launch it:

To launch the graphical installer (available only on English versions of Linux):

./install.sh -g

To launch the command-line installer, omit the -g switch:
./install.sh

See *Starting the Web Linux installer* for more detailed instructions.

8) On the Introduction screen, click **Next**.

Note

These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

9) On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.

10) On the Upgrade screen, select **Start the upgrade** and then click **Next**.

Important

Before clicking **Next**, be sure to no administrators are logged on to the management console anywhere in the network.

11) When you click **Next**, a “Stopping All Services” progress message appears. Wait for the services to be stopped.

The Pre-Upgrade Summary screen appears when the services have been stopped.

In some cases, the installer may be unable to stop the web protection services. If the services have not been stopped after approximately 10 minutes, then stop them manually using the **/opt/Websense/WebsenseAdmin stop** command. You can leave the installer running when you do so. Once you have manually stopped the services, return to the installer.

12) On the Pre-Upgrade Summary screen, review the list of components that will be upgraded, and then click **Install**.

Critical files are backed up and install properties initialized. And then the **Installing...** screen appears.

13) Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.

14) Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

15) If you stopped your antivirus software, restart it.

16) If you have an integration product installed, additional upgrade steps may be necessary. See:

- *Integrating Forcepoint URL Filtering with Cisco*
- *Integrating Forcepoint URL Filtering with Citrix*
- *Integrating Forcepoint URL Filtering using ICAP Service*
- *Integrating Forcepoint URL Filtering with TMG*
- *Installing for Universal Integrations*

17) Repeat the upgrade procedure on each machine running web protection components, in the recommended order (see *Web protection upgrade order*).

All components that interact must be upgraded to the same version.
If you have complete installations in separate locations that do not interact, they do not have to run the same web protection software version.

18) After all components have been upgraded, see *Initial Configuration for All Security Modules*.

Next steps

To add additional components to the machine after upgrade, run the installer again on the same machine. This time, the installer will ask if you want to add components. See *Adding or modifying Windows components*.

Related concepts

Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with TMG on page 221
Installing for Universal Integrations on page 247
Integrating Forcepoint URL Filtering using ICAP Service on page 241
Adding or modifying Windows components on page 342

Related tasks

Web protection upgrade order on page 271
Starting the Web Linux installer on page 138
Initial Configuration for All Security Modules on page 329

Related reference

Preparing for installation on page 19

Chapter 23

Upgrading Content Gateway to v8.5.x

Applies to:
■ Forcepoint Web Security, v8.5.x

This section provides upgrade instructions for software-based Content Gateway installations.

Note

When upgrading Content Gateway on an appliance, see the Forcepoint appliance documentation appropriate for your configuration.

Perform an upgrade by running the Content Gateway installer on a machine with a previous version of Content Gateway installed. The installer detects the presence of Content Gateway and upgrades it to the current version.

Versions supported for direct upgrade to v8.5.x

Direct upgrade is supported from v8.1.x, v8.2.x, v8.3.x, and v8.4.x to Content Gateway v8.5, from v8.2, v8.3, v8.4 and v8.5 to Content Gateway v8.5.3, or from v8.4, v8.5, and v8.5.3 to Content Gateway v8.5.4. Upgrades from earlier versions require intermediate upgrades:

v7.0/7.1 > v7.5 > v7.6 > v7.7 > v7.8.4 > v8.4.x>v8.5.x

Follow the upgrade procedures for each intermediate version. Read the Content Gateway Installation Guide and its upgrade supplement for each version.

- Version 7.5 Content Gateway Installation Guide
- Version 7.6 Content Gateway Installation Guide
- Version 7.7 Content Gateway Installtion Guide
- Version 7.8 Content Gateway Installation Guide
- Version 8.4 Forcepoint Web Security Installation Guide

To perform an intermediate upgrade, download the installer package for that version from the Downloads site at forcepoint.com.

System requirements

Before upgrading Content Gateway, make sure the host machine meets the system requirement outlined in Content Gateway section in *System requirements for this version*, including hardware specifications, operating system, and browser.

Upgrading distributed components

Content Gateway is the web proxy component of **Forcepoint Web Security**. Several Forcepoint Web Security components must be upgraded prior to upgrading Content Gateway. Distributed components must be upgraded in a particular order. See *Upgrading Web Protection Solutions*.

Preparing to upgrade

Before upgrading Content Gateway, be aware of the following.

- Most SSL configuration settings are saved and applied to the upgraded Content Gateway, except for dynamic certificates. Note that:
  - The Incident list is retained. Before upgrading, consider performing maintenance on the Incident list; remove unwanted entries.
  - SSLv2 is not enabled by default. If it is enabled prior to upgrade, the setting is retained.
- For user authentication, there is one credential cache for both explicit and transparent proxy mode, and one Global Authentication Options page for setting the caching method and Time-To-Live.
  During upgrade, the Cache TTL value is retained from the Transparent Proxy Authentication tab **unless** the value on the Global Authentication Options tab is not the default. In this case, the customized value is used.
- If you use Integrated Windows Authentication (IWA), be aware that IWA domain joins should be preserved through the upgrade process. However, in case the joins are dropped, make a record of the settings before starting the upgrade. Log on to the Content Gateway manager and record the IWA settings, including the names of domains to which IWA is joined. Keep this record where it is easily retrieved after the upgrade.
- If you have software instances of Content Gateway, make sure the host system meets the following hardware requirements before upgrading:

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum 8 GB recommended
Disk Space	2 disks: ■ 100 GB for the operating system, Content Gateway, and temporary data. ■ Max 147 GB for caching If caching will not be used, this disk is not required. The caching disk: ■ Should be at least 2 GB and no more than 147 GB ■ Must be a raw disk, not a mounted file system ■ Must be dedicated ■ Must *not* be part of a software RAID ■ Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64 MB of write-through cache
Network Interfaces	2

- In addition, to support **transparent proxy** deployments:

Router	Must support WCCP v2. A Cisco router must run IOS 12.2 or later. The latest version is recommended. To support IPv6, WCCP v2.01 and Cisco router version 15.4(1)T or later are required. Client machines, the destination Web server, and Content Gateway must reside on different subnets.
-or- Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Upgrading Content Gateway

Content Gateway runs on web protection full policy source, user directory and filtering, and filtering only appliances (all of which should already have been upgraded at this point).

Content Gateway is supported on Red Hat Enterprise Linux machines. See the Certified Product Matrix for a list of supported operating systems.

IContent Gateway upgrade instructions

This section describes upgrading Content Gateway on your Red Hat Enterprise Linux host.

Important

At the beginning of the upgrade procedure, the installer checks to see if the partition that hosts **/opt** has enough space to hold a copy of the existing Content Gateway log files (copied to **/opt/WCG_tmp/logs**). If there's not enough space, the installer prints an error message and quits.

In this situation, if you want to retain the log files you must copy the contents of **/opt/WCG/logs** to a location that has enough space, and then delete the log files in **/opt/WCG/ logs**.

When the upgrade is complete, move the files from the temporary location back to **/opt/WCG/logs** and delete the files in the temporary location.

Note

If you have multiple Content Gateway instances deployed in a cluster, you **do not** have to disable clustering or VIP (if used). As each member of the cluster is upgraded it will rejoin the cluster.

1) If your existing web protection solution is deployed with Forcepoint Web Security DLP Module or a data protection product:

a) Log on to the Content Gateway manager.

b) Navigate to the **Configure > My Proxy > Basic** page.

c) Disable **Web DLP**.
When the upgrade is complete:

d) Return to the **Configure > My Proxy > Basic** page.

e) Enable the new **Web DLP** option.

f) Restart Content Gateway.

g) Navigate to the **Configure > Security > Web DLP** page and confirm that automatic registration was successful. If it was not, confirm that the Data module of management console is running as expected.

2) Log on to the Content Gateway Linux host and acquire root permissions:
```
su root
```

3) Disable any currently running firewall on this machine for the duration of the upgrade. Bring the firewall back up after the upgrade is complete, opening ports used by Content Gateway.
For example, if you are running IPTables:

a) At a command prompt, enter **service iptables status** to determine if the firewall is running.

b) If the firewall is running, enter **service iptables stop**.

c) After upgrade, restart the firewall. In the firewall, be sure to open the ports used by Content Gateway on this machine. See *Default ports for on-premises Forcepoint security solutions* for more information.

Important

Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable firewalld prior to installing Content Gateway.

On the machine where Content Gateway will be installed, execute the following:

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

4) Use the Downloads tab of the My Account page at forcepoint.com to download the Content Gateway version 8.5.x installer, and save it to a temporary directory. For example, place it in:
`/tmp/cg_v85`

5) Unpack the Content Gateway installer tar archive:
```
cd /tmp/cg_v85
tar -xvzf <installer tar archive>
```

Important

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

6) If you intend to upgrade Red Hat Enterprise Linux 6.x to a more recent version, perform the upgrade now. See your Red Hat Enterprise Linux documentation.

7) In the directory where you unpacked the tar archive (for example, /tmp/wcg_8x), start the installation/upgrade script.

```
./wcg_install.sh
```

Respond to the prompts.

Content Gateway is installed and runs as **root**.

Note

Up to the point that you are prompted to confirm your intent to upgrade, you can quit the installer by pressing CTRL+C. If you change your mind after you choose to continue, do **not** use CTRL+C to stop the process. Instead, allow the installation to complete and then uninstall.

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

```
Error: Content Gateway v8.5.x on x86_64 requires several packages that are not present on your system.
```

```
Please install the following packages: <list of packages>
```

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

```
yum install <list of packages>
```

```
See the Technical Library (support.forcepooint.com/ Documentation) for information about the software requirements for x86_64 installation.
```

To make it easier to install the needed packages, the Content Gateway distribution includes a Linux “rpm” containing the needed packages. To install its contents, ensure that the operating system has access to the Red Hat Linux distribution library (for example the DVD), and enter:

```
yum install wcg_deps-1-0.noarch.rpm
```

Upon successful completion, a list of updated packages displays and then the word “Complete!”.

Here is an example of a system resource warning:

```
Warning: Content Gateway requires at least 6 gigabytes of RAM.
Do you wish to continue [y/n]?
```

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

Enter **y** to continue the upgrade. You should not install or upgrade on a system that does not meet the minimum requirements. If you choose to run Content Gateway after receiving a system resource warning, performance and stability may be affected.

9) Read the subscription agreement. At the prompt, enter **y** to accept the agreement and continue the upgrade, or **n** to cancel.

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

10) The installer checks for the presence of an existing Content Gateway installation. When asked, choose to replace the existing version with version 8.4.x.

```
WCG version 8.1.n-nnnn was found.
Do you want to replace it with version 8.5.x-nnnn [y/n]? y
```

11) Existing settings and logs are copied to backup files and stored. For example:

```
Stopping Content Gateway processes...done
Copying settings from /opt/WCG to /root/WCG/OldVersions/ 8.1.0-1418-PreUpgrade/...done
Zipping configuration archive...done
Moving log files from /opt/WCG/logs to /opt/WCG_tmp/logs/...done
```

12) You can either re-use the installation selections you entered during the last install, or provide new answers to all installation prompts, such as admin password, admin email address, Policy Server IP address, etc.:

```
Previous installation selections </root/WCG/Current/ WCGinstall.cfg> found.
Use previous installation selections [y/n]?
```

Enter **y** to use previous installation selections.

Enter **n** to revert to default values, and receive all installation questions and answer them again.

13) If you answered **y** at Step 11, then you can also leave proxy settings at their current values or revert to default values (which perform a fresh install!).

```
Restore settings after install [y/n]?
```

Enter **y** to keep the proxy settings as they are.

Enter **n** to restore default settings for the proxy.

CAUTION

If you answer **n** (no), the current installation of Content Gateway is removed, and a fresh install of 8.2.x begins. See Installation Instructions: Forcepoint Web Security for a detailed description of the installation procedure. This is not an upgrade, but rather a fresh install.

14) The previously installed version of Content Gateway is removed, and the settings and selections you chose to retain are re-used. Details of the upgrade process are output to the screen. Please wait.

```
*COMPLETED* Content Gateway 8.5.x-nnnn installation.
A log file of this installation process has been written to
/root/WCG/Current/WCGinstall.log
For full operating information, see the Content Gateway Help system.
Follow these steps to start the Content Gateway management interface (Content Gateway Manager):
-------------------------------------------------------------
1. Start a browser.
2. Enter the IP address of the Content Gateway server, followed by a colon and the management
 interface port (8081 for this installation). For example: https://11.222.33.44:8081.
3. Log on using username admin and the password you chose earlier.
A copy of the CA public key used by the Manager is located in /root/WCG/.
```

15) The automated portion of the upgrade is now complete, and the proxy software is running.
If you chose to revert to default proxy settings, be sure to configure any custom options.

16) Check Content Gateway status with:

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

All services should be running. These include:

- Content Cop
- Content Gateway
- Content Gateway Manager
- Analytics Server

Important

If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for: `/opt/WCG/config/internal/no_cop`. If the file exists, remove it and start Content Gateway using `/opt/WCG/WCGAdmin start`

To finish the upgrade, be sure to perform the post-upgrade instructions at the end of this document.

Post-upgrade activities

After you have finished upgrading components, refer to the following to ensure that your Content Gateway upgrade is complete.

1) If at the start of the upgrade process you manually moved your existing log files to a temporary location, move them back to **/opt/WCG/logs** and delete the files in the temporary location.

2) Register Content Gateway nodes in Forcepoint Security Manager on the **Web > Settings > Content Gateway Access** page.
Registered nodes add a link to the Content Gateway manager logon portal and provide a visual system health indicator: a green check mark or a red X.

3) Configure Content Gateway system alerts on the **Settings > Alerts > System** page in the Security Manager.
This subset of Content Gateway system alerts can be configured to be sent to administrators, in addition to being displayed in the Content Gateway manager.

4) If you use SSL support:

   a) If your clients don't yet use a SHA-256 internal Root CA, create and import a SHA-256 Root CA into all affected clients. See Internal Root CA in Content Gateway Help.

   b) Using the notes you compiled prior to upgrade, rebuild your Static Incident list.

5) If you use proxy user authentication, review the settings on the **Global Authentication Options** page (**Configure > Security > Access Control > Global Configuration Options**).

6) If you use IWA user authentication, confirm that the AD domain is still joined. Go to **Monitor > Security > Integrated Windows Authentication**. If it is not joined, rejoin the domain. Go to **Configure > Security > Access Control > Integrated Windows Authentication**.

7) If you use Rule-Based Authentication, review your configuration. Go to **Configure > Security > Access Control**.

   a) Check the **Domains** page.
   - IWA domains that were joined before upgrade should still be joined.
   - LDAP and Legacy NTLM domains should be listed.

   b) Check each rule.
   - Go to the **Authentication Rules** page and enter the editor.
   - Select each rule and check the configuration.

- For Multiple Realm Authentication rules that used Cookie Mode Caching, check the cookie list on the Global Authentication Option page.
- Check that the expected domain is in the **Auth Sequence** list.

Important

The Rule-Based Authentication feature is very rich and can satisfy many user authentication requirements. To make best use of it, please refer to Rule-Based Authentication.

8) If a web protection and data protection solution were deployed together, confirm that Content Gateway has automatically re-registered with the Data module of the Forcepoint Security Manager. If it has not, manually re-register.

a) Ensure that the Content Gateway and the Security Manager server system clocks are synchronized to within a few minutes.

b) In the Content Gateway manager:

- Go to **Configure > My Proxy > Basic**, ensure that **Web DLP: Integrated on-box** is enabled, and click **Apply**.
- Next to **Integrated on-box**, click the **Not registered** link. This opens the **Configure > Security > Web DLP registration** screen.
- Enter the IP address of the Security Manager server.
- Enter a user name and password for logging onto Security Manager. The user must be a Forcepoint DLP administrator with Deploy Settings privileges.
- Click **Register**. If registration is successful, a message confirms the result and prompts you to restart Content Gateway. If registration fails, an error message indicates the cause of failure. Correct the problem and perform the registration process again.

9) If web and data protection products were deployed together and upgraded, you may need to remove stale entries of Content Gateway instances registered in Forcepoint DLP system modules:

a) Log onto Security Manager.

b) Select the **Data** tab and navigate to the **Settings > Deployment > Modules** page.

c) Listed are 2 instances of each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.

d) Click **Deploy**.

10) If web and data protection products were deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance may need to be deleted from the list of Forcepoint DLP system modules or the deployment will fail. Go to the **Data** > **Settings** > **Deployment** > **System Modules** page, click on the affected Content Gateway instance to open its **Details** page, click **Delete** and then **Deploy**.

11) If your explicit proxy deployment was customized to support an external load balancer with IWA user authentication, the configuration is preserved during upgrade. You do not need to re-apply the custom configuration. You should, however, test your deployment to verify that the load balancer is performing as expected.

12) With v8.2.x, the basic functionality for 2 features was changed slightly:

- **Send authentication to parent proxy**, configured on the **Configure > My > Proxy > Basic > General** page
- **X-Forwarded-For**, enabled on the **Configure > Perotocols > HTTP > Privacy**

In both cases, header values are forwarded only to a configured parent proxy.

If you are upgrading from v8.1 to v8.5, enabled either of these settings in your previous version, and are expecting header values to be forwarded for all outbound requests, add the appropriate variable to your records.config file (in the **/opt/WCG/config** directory, by default).

- To add the user name to outbound requests, add:
  `CONFIG proxy.config.http.insert_xua_to_external INT`
- To send X-Forwarded-For header values directly to the Internet, add:
  `CONFIG proxy.config.http.insert_xff_to_external INT 1`

13) If you were using v8.1 with custom cipherlist settings using these variables in records.config:

```
proxy.config.ssl.server.cipherlist
proxy.config.ssl.client.cipherlist
```

You need to reconfigure the custom settings because these variables were replaced in v8.2.

- proxy.config.ssl.server.cipherlist_suffix replaces proxy.config.ssl.server.cipherlist
- proxy.config.ssl.client.cipherlist_suffix replaces proxy.config.ssl.client.cipherlist

The non-default cipherlist being used prior to the upgrade are saved as a comment in records.config, where it can be used for reference. Default values for the new variables are put into place during the upgrade and can be reconfigured after the upgrade is complete.

See Content Gateway Manager Help for more information on how these new variables now work with proxy.config.ssl.server.cipherlist_option and proxy.config.ssl.client.cipherlist_option to create cipher lists.

14) The **Tunnel Skype** option on the **Configure > Protocols > HTTPS** page of Content Gateway Manager was removed in v8.3. Variables stored in the records.config file that apply to Skype are removed during upgrades from v8.1 and v8.2.

15) The settings on the **Configure > Networking > Connection Management > Low Memory Mode** page of Content Gateway manager was removed in v8.3. Corresponding variables stored in the records.config file are removed by upgrades from v8.1 and v8.2.

16) If **LOW** encryption cipher suites was previously selected on the **Configure > SSL > Decryption/Encryption > Inbound** or **Outbound** pages of Content Gateway manager, upgrades from v8.1 or v8.2 will change the setting to **MEDIUM**. LOW is no longer a valid option on those pages.
The corresponding records.config variables are also updated by the upgrade.

17) During upgrades from v8.1 or v8.2, the **Enable the certificate verification engine** on the **Configure > SSL > Validation > General** page of Content Gateway manager will be changed to ON for any customer who does not already have the feature enabled.

18) In v8.3 and continued in v8.4 and v8.5, improvements were made to the Adaptive Redirection Module (ARM). The ARM component now utilizes iptables, policy routing, and transparent sockets which are configured during product installation or upgrade.
The Content Gateway Manager was changed to reflect these improvements.

- The **Network Address Translation (NAT)** section of the **Configure > Networking > ARM > General** page has been renamed to **Redirection Rules** to better reflect the contents of the table.

- Text on that page has also been updated.

To facilitate interception and redirection of traffic:

- IPTables rules are configured during upgrade.
  - 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* Forecepoint 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`

For some customers, the GRE **Packet Return Method** (GRE return) may not be as expected. In all cases, GRE return, as documented by Cisco (see this site), is fully functional. However, tunneling back through a router (enhanced GRE tunnel return) now requires a specific kernel module. Contact Forcepoint Technical Support to enable this functionality.

To provide more appropriate statistical data for the new ARM, the **Bypass Statistics** now provide information for:

- Total Packets Bypassed
- Packets Dynamically Bypassed
- DNS Packets Bypassed
- Packets Shed

19) A change was made in v8.4 to resolve customer issues with SSL retry logic. The default values for the following records.config variables are reset to 1 during an upgrade from v8.1, v8.2, or v8.3.

```
proxy.config.http.connect_attempts_max_retries
proxy.config.http.connect_attempts_max_retries_dead_server
```

20) Automatic updates to the Certificate Authority tree were added to v8.4.
After upgrading from v8.1, v8.2, or v8.3, when the initial CA tree update occurs, CAs in the customer deployment but not in the 8.4 CA db, any CA that is no longer a root CA, and CAs that are no longer trusted are converted to a private CA. This process also removes expired CAs.

After the initial update, review the CA tree on the **Configure > SSL > Certificates** page of Content Gateway manager and remove any certificates that are no longer trusted or may be revoked.

21) With v8.5, default IPTables include a rule that will drop traffic that is neither HTTP, HTTPS, nor FTP and not forward it through the proxy.
On upgrade, this feature is disabled by default. To add the rule and not forward traffic that is neither HTTP, HTPTS, nor FTP, add the following to records.config ((located in /opt/WCG/config, by default):

```
CONFIG proxy.config.arm.forward_unwanted_traffic INT 0
```

After this entry is added and Content Gateway is restarted, an IPTables rule is added and traffic that is neither HTTP, HTTPS, nor FTP will not be forwarded.

22) For customers who have purchased the v8.5 Protected Cloud Apps feature, the setting for **Parent Proxy** on the **Configure > Content Routing > Hierarchies** page of Content Gateway Manager will be enabled. If you

previously enabled and configured **Parent Proxy** and later disabled the option, the configured settings will be used and should be updated as necessary.

23) With v8.5, the option of **TLSv1** on the **Configure > SSL > Decryption/ Encryption** page (Inbound and Outbound tabs) and on the **Configure > Security > FIPS** page of Content Gateway Manager is no longer a default selection. Options for **TLSv1.1** and **TLSv1.2** are added and enabled by default.
During upgrade, if **HTTPS** (SSL) was enabled on the **Configure > My Proxy > Basic > General** page of Content Gateway Manager prior to upgrade, the SSL settings are not changed.

IF **HTTPS** (SSL) is enabled after the upgrade, the settings will be handled like a fresh installation of the product and TLSv1.1 and TSLv1.2 will be enabled by default. TLSv1 will not be enabled.

24) Beginning with v8.5.3, Content Gateway will no longer accept nor download SHA-1 intermediate certificates. SHA-1 certificates that were added by Content Gateway will be removed during an upgrade to v8.5.3. Note that SHA-1 certificates that were manually added will not be deleted.
A new variable has been added in v8.5.3 that will disable the automatic adding of new certificates to the certificate database. Upgrades to v8.5.3 will add this new parameter to records.config, set to use the default functionality.

To disable the default functionality edit the following in records.config (located in /opt/WCG/config, by default)

```
CONFIG proxy.config.ssl.cert.verify.add_cert_to_database INT 0
```

Reset the value to 1 to restore the default functionality.

25) Version 8.5.3 adds the ability to manually add a dynamic certificate key. Each key requires a passphrase. Both the key and passphrase are stored in the certificates database.

26) With v8.5.4, a setting has been added to Content Gateway manager that enables authentication of HTTPS requests over HTTPS, using port 4443.
Open Content Gateway manager and navigate to **Configure > Security > Access Control** and select **Global Authentication Options**. A new **Redirect Options** section contains the **Redirect Hostname** entry field as well as the option to **Redirect for HTTPS Authentication**.

Disabled by default, click **Enabled** to direct all HTTPS requests to authenticate over HTTPS.

Changing the manager options also resets a new records.config variable.

```
proxy.config.auth.ssl_auth_url
```

27) Custom certificates added for use with Captive Portal are not retained when upgrading to v8.5.x. These certificates must be re-added after the upgrade is completed.

28) A new Socks Server Rule has been added to the "Do not route through SOCKS server" rule type to ensure that traffic that does not need to be directed through a SOCKS server is not sent there.This avoids SOCKS server issues that may result from excessive load.
This rule is also added when upgrading to v8.5.4.

Note

SOCKS traffic from the ip range included in the rule will be routed through a SOCKS server.

29) To fix a vulnerability, the default value for the following records.config variables has been changed in v8.5.4 and will be updated to the new defaults when upgrading.

```
proxy.config.ssl.server.cipherlist_suffix
```

```
proxy.config.ssl.client.cipherlist_suffix
```

See Content Gateway Manager Help for more information on how these variables work.

30) The Session Cache section, previously available on **Configure > SSL > Decryption / Encryption** > **Outbound** have been removed in v8.5.4 to avoid Content Gateway restarts. Upgrades to v8.5.4 will automatically disable these options if they had been previously enabled.

Related concepts

Upgrading Web Protection Solutions on page 261

Related reference

Default ports for on-premises Forcepoint security solutions on page 361
System requirements for this version on page 9

Chapter 24

Upgrading Forcepoint Appliances to v8.5.x

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint Email Security, v8.5.x ■ Forcepoint Appliances, v8.5.x

This information applies to upgrading Forcepoint V Series, X Series, and Virtual Appliances that host:

- Web protection solutions
  - Forcepoint Web Security, v8.4.x and higher
  - Forcepoint TRITON AP-WEB, v8.0.x and higher
  - Forcepoint Web Filter & Security, v8.0.x and higher
  - Websense Web Security Gateway / Anywhere, v7.8.4
  - Websense Web Security, v7.8.4
- Email protection solutions
  - Forcepoint Email Security, v8.4.x and higher
  - Forcepoint TRITON AP-EMAIL, v8.0.x and higher
  - Websense Email Security Gateway / Anywhere, v7.8.4

Important

- **Forcepoint V Series dual-mode appliance users:**
  Dual-mode appliances are not supported with v8.3.0 and higher.

  Either the email protection or the web protection solution must be migrated to a new appliance.

  To ease the migration effort, special tools have been developed, and a special procedure is recommended. For details, see Upgrading V-Series Dual-Mode Appliances. Contact your Forcepoint account representative to learn about special promotions for dual-mode deployments planning an upgrade to v8.3.x or higher.
- Some older V10000 and V5000 appliances are not supported with v8.0.0 and higher.

Upgrading to 8.5.0

V Series appliances can be upgraded directly to 8.5.0 from any of these versions: 8.1.0, 8.2.0, 8.3.0, 8.4.0

X Series appliances can be upgraded directly to 8.5.0 from any of these versions: 8.1.0, 8.2.0, 8.3.0, 8.4.0

For Web and Email OVAs can be upgrade directly to 8.5.0 from 8.3.0 and 8.4.0.

Upgrading to 8.5.3

V Series appliances can be upgraded directly to 8.5.3 from any of these versions: 8.2.x, v8.3.x, v8.4.x, 8.5.x

X Series appliances can be upgraded directly to 8.5.3 from any of these versions: 8.2.x, v8.3.x, v8.4.x, 8.5.x

VMware virtual appliances can be upgraded directly to 8.5.3 from 8.3.0, 8.4.0, and 8.5.0.

DLP Analytics Engine OVA upgrade to 8.5.3 is not supported.

Important

Appliances running v8.0.x should upgrade to v8.3.0 before upgrading to v8.5.3. See the v8.3.0 upgrade guides.

Upgrading to 8.5.4

V Series appliances can be upgraded directly to 8.5.4 from any of these versions: 8.4.0, 8.5.0, and 8.5.3

X Series appliances can be upgraded directly to 8.5.4 from any of these versions: 8.4.0, 8.5.0, and 8.5.3

VMware virtual appliances (except for DLP Analytics Engine OVAs) can be upgraded directly to 8.5.4 from 8.4.0, 8.5.0, and 8.5.3.

DLP Analytics Engine OVAs can be upgrade to 8.5.4 from 8.5.3.

Product naming after 8.4.0

Version 8.4.0 adopts new product naming.

Former Name	New Name
TRITON AP-WEB TRITON Web Security Gateway TRITON Web Security Gateway Anywhere	Forcepoint Web Security
Forcepoint Web Filter & Security Websense Web Security	Forcepoint URL Filtering
TRITON AP-EMAIL Websense TRITON Email Security Gateway Websense TRITON Email Security Gateway Anywhere	Forcepoint Email Security

For upgrade instructions, see the upgrade guides for your security module, or:

- Forcepoint V Series Upgrade Guide
- Forcepoint X Series Upgrade Guide
- V Series, X Series, and Virtual Appliance Upgrade Guide

Chapter 25

Upgrading to Forcepoint DLP

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The existing data security solution must be at least version 8.7.x to upgrade directly to Forcepoint DLP version 9.0. Those currently using an earlier version must perform interim steps, as shown in the table below:

Current version	Step 1	Step 2
8.4 - 8.6.x	Upgrade to 8.7.x	Upgrade to 9.0
8.7.x–8.9.x	Upgrade to 9.0	

For step-by-step instructions on performing an upgrade, see the following guides. These guides include information on upgrading the management server, supplemental Forcepoint DLP servers, agents, protectors, and Forcepoint DLP Endpoint.

- Upgrading to Forcepoint DLP v9.0
- Upgrading to Forcepoint DLP v8.9.x
- Upgrading to Forcepoint DLP v8.8.x
- Upgrading to Forcepoint DLP v8.7.x
- Upgrading to Forcepoint DLP v8.6
- Upgrading to Forcepoint DLP v8.5.x
- Upgrading to Forcepoint DLP v8.4
- Upgrading to TRITON AP-DATA v8.3
- Upgrading from v7.7.x to v7.8.x
- Upgrading from v7.6.x to v7.8.x

Chapter 26

Migrating web solutions to a new operating system

Contents

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

If your current web protection software is running on hardware or software that is no longer supported, the upgrade process also includes an operating system migration.

Depending on your current operating system and hardware, it may be possible to update the operating system in place (on the existing machine). Always back up your web protection software before performing an operating system update.

Whether you update the operating system in place or move to another machine, make sure that the machine meets the hardware requirements for your target version: **v8.5.x**.

To prepare for the migration process, continue with *Order of migration and upgrade steps*.

Related concepts

Order of migration and upgrade steps on page 299

Order of migration and upgrade steps

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Depending on your current version, the order of operating system migration and web protection software upgrade steps varies:

Current Version	Current Platform	Upgrade Path
v7.6.x	Red Hat Enterprise Linux 4	1) Migrate to Red Hat Enterprise Linux 5. 2) Upgrade to v7.7.x on the new platform. 3) Migrate to Red Hat Enterprise Linux 6. 4) Upgrade to v7.8.4 on the new platform. 5) Migrate to Red Hat Enterprise Linux 6.5. 6) Upgrade to v8.4.x. 7) Migrate to Red Hat Enterprise Linux 7.3. 8) Upgrade to v8.5 or v8.5.3. 9) Migrate to Red Hat Enterprise Linux 7.5. 10) Upgrade to v8.5.4.
v7.6.x	Windows 2003	1) Migrate to Windows 2008 R2. 2) Do one of the following: ■ If you have Web Security or Web Filter, upgrade to v7.8.4, then to v8.3.x ■ If you have Web Security Gateway or Gateway Anywhere, upgrade to v7.7.x, then to v8.0.x, then to v8.3.x. 3) If upgrading to v8.5.3, migrate to Windows 2012. 4) Upgrade to v8.5.x.

Current Version	Current Platform	Upgrade Path
v7.7.x	Red Hat Enterprise Linux 5	1) Migrate to Red Hat Enterprise Linux 6. 2) Upgrade to v7.8.4 on the new platform. 3) Migrate to Red Hat Enterprise Linux 6.5. 4) Upgrade to v8.4.x. 5) Migrate to Red Hat Enterprise Linux 7.3. 6) Upgrade to v8.5 or v8.5.3. 7) Migrate to Red Hat Enterprise Linux 7.5. 8) Upgrade to v8.5.4.
v7.7.x	Windows 2008 (32- bit)	1) Migrate to Windows 2008 R2. 2) Upgrade to v7.8.4 on the new platform. 3) Upgrade to v8.3.x. 4) If upgrading to v8.5.3, migrate to Windows 2012. 5) Upgrade to v8.5.x.

For more detailed migration instructions, see:

- *Migrating web management components*
- *Moving web policy components to a new machine*
- *Updating the operating system on an existing web protection machine*

Related concepts

Updating the operating system on an existing web protection machine on page 304

Related tasks

Migrating web management components on page 302
Moving web policy components to a new machine on page 303

Migrating web management components

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

In v8.5.x, the management server can reside on a number of 64-bit Windows platforms. See the Certified Product Matrix for details.

- No migration is necessary to upgrade from
  - v8.1.x, v8.2.x, v8.3.x or v8.4.x to v8.5.
  - v8.2.x, v8.3.x, v8.4.x, or v8.5 to v8.5.3.
  - v8.4.x, v8.5, or v8.5.3 to v8.5.4.

  which are also supported on these 64-bit Windows platforms.
- Version 7.7.x can be migrated to Windows Server 2008 R2 via the steps below.

To migrate your management server components:

Steps

1) Perform a backup on your current installation, and store the backup file in a safe location.
   See the How do I back up and restore the TRITON infrastructure? paper for v7.6.x - 7.8.x in the Technical Library.

2) Uninstall the TRITON components (TRITON Infrastructure and the Web Security module) from their current location.

3) Reinstall TRITON Infrastructure and the Web module on the new server.
   This makes it possible to preserve your existing global configuration settings, as explained in the next step.

4) Restore your TRITON Infrastructure backup to the new machine to preserve your TRITON Settings configuration.
   Refer to the How do I back up and restore the TRITON infrastructure? paper for instructions.

5) Upgrade your software to v8.5.x. See *Upgrading Web Protection Solutions*.
   The upgrade instructions include information about the order in which to upgrade your components.

Next steps

For migration instructions for additional components, see:

- *Moving web policy components to a new machine*
- *Updating the operating system on an existing web protection machine*

Related concepts
Upgrading Web Protection Solutions on page 261
Updating the operating system on an existing web protection machine on page 304

Related tasks
Moving web policy components to a new machine on page 303

Moving web policy components to a new machine

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

When you move the **same web protection software version** to a new machine, first perform a new installation of the components on the new machine. Once the components are running successfully on the new machine, use the following procedure to preserve your policies and system configuration.

Steps

1) On the original Policy Broker machine (running on the old operating system), navigate to the **bin** directory:
   - Windows:
     - C:\Program Files\Websense\Web Security\bin
     - C:\Program Files (x86)\Websense\Web Security\bin
   - Linux: /opt/Websense/bin/

2) Use the following command to back up your existing policy information:
   ```
   PgSetup --save backup.policydb
   ```
   This command backs up only data stored in the Policy Database. It does **not** back up custom block pages or customized configuration files. To preserve customized configuration files or block pages, back those up separately.

3) Copy the backup file resulting from the previous step to the corresponding **bin** directory on the new Policy Broker machine.

4) Stop all web protection services on the new Policy Broker machine:
   - *Windows*: Navigate to the **Websense\Web Security** directory and enter the following command:
     `WebsenseAdmin stop`
   - *Linux*: Use the **/opt/Websense/WebsenseAdmin stop** command.

5) Use the following command to restore the contents of your Policy Database backup to the new machine without overwriting important token and IP address information:
   `PgSetup --restore backup.policydb --no-clobber`
   The “no-clobber” parameter eliminates the need to update the token value in the config.xml file (a step included in migration procedures prior to 7.7).

6) Start the web protection services on the new Policy Broker machine:
   - *Windows*: Navigate to the **Websense\Web Security** directory and enter the following command:
     `WebsenseAdmin start`
   - *Linux*: Use the **/opt/Websense/WebsenseAdmin start** command.

Result

Once the new machine has successfully replaced the original machine in your deployment, and you have verified that your policy information is correct, you are ready to begin the upgrade process.

Updating the operating system on an existing web protection machine

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

If the existing web protection machine meets the hardware specifications for v8.5.x, and you want to update the operating system in place, rather than moving to a new machine, use the following procedure to make sure that your policies and system configuration are preserved.

1) Run the Backup Utility on each machine that includes web protection components.
   - Windows: Navigate to the **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security \bin) and enter the following command:
     `wsbackup -b -d <directory>`
   - Linux: Navigate to the **/opt/Websense/** directory and enter the following command:
     `./wsbackup -b -d <directory>`

   Replace <directory> with the destination path for the backup archive.

2) Run the Forcepoint Management Infrastructure backup process.
   - Go to **Start > Windows Administrative Tools > Task Scheduler** and select **Task Scheduler Library**.
   - If the **Websense Triton Backup** task is disabled, right-click the task and select **Enable**.
   - Right-click the **Websense Triton Backup** task and select **Run**.

The file is saved in the **C:\EIPBackup** directory by default.

3) Save the backup file or files in a safe location on another machine or device.

4) Update the operating system on the machine.

Depending on the operating system that you are upgrading, web protection software may continue to run normally, or may be damaged or completely removed from the machine.

If there is a problem with web protection software on the machine:

1) Uninstall and reinstall the affected components, keeping the same web protection software version that existed before the operating system changed.

2) Verify that web protection services or daemons are running as expected.

3) Copy the backup file or files created in previous procedure to the web protection machine.

4) Use the Backup Utility to restore your policy and configuration settings from backup.
   - Windows: Navigate to the **bin** directory (C:\Program Files\Websense\bin or C:\Program Files\Websense\Web Security\bin) and enter the following command:
     `wsbackup -r -f <path>\<file>.tar.gz`
   - Linux: Navigate to the **/opt/Websense/** directory and enter the following command:
     `./wsbackup -r -f <path>/<file>.tar.gz`

   Replace <path> with the location of the file and <file> with the file name. The file name always ends with a .tar.gz extension.

5) Restore your Forcepoint Management Infrastructure settings from backup.
   a) Go to **Start > Windows Administrative Tools > Services**.

   b) Right-click the following service and select **Stop**.
      - Websense TRITON Unified Security Center
      - Websense TRITON Web Server
      - Websense TRITON - Web Security

   c) Open the Windows Control Panel and click **Programs**, then **Programs and Features**.

   d) Select **Forcepoint Management Infrastructure**, then click **Uninstall/ Change**.

   e) When asked if you want to modify, repair, or remove Forcepoint Management Infrastructure, select **Modify**, then click **Next** until you get to the **Restore Data from Backup** screen.

   f) Mark the **Use backup data** box, then click **Browse** to locate the backup folder.

   g) Click **Next** until the restore process beings.

   h) When the restore process is complete, click **Finish**.

i) Return to the Services window and click **Refresh**. If any of the services that you stopped has not restarted, right-click it and select **Start**.

Chapter 27

Upgrading Email Protection Solutions

Contents

Applies to:

- Forcepoint Email Security, v8.5.x
- Forcepoint Appliances, v8.5.x

The Forcepoint Email Security v8.5.x upgrade process includes appliance components (V Series appliance, X Series security blade, or virtual appliance), along with Forcepoint Security Manager and Email Log Server Windows components. A virtual appliance upgrade applies only to version 7.8.0 and later, and an X Series security blade upgrade applies only to version 7.8.4 and later.

These instructions cover the upgrade of a Websense Email Security Gateway, TRITON AP-EMAIL, or Forcepoint Email Security solution to Forcepoint Email Security version **8.5.0**, **8.5.3**, or **8.5.4**, installed on-premises or in Microsoft Azure.

- You can upgrade directly to on-premises version **8.5.4** from Forcepoint Email Security version 8.4.0, 8.5.0, or 8.5.3.
- You can upgrade directly to on-premises version **8.5.3** from TRITON AP-EMAIL version 8.2.0 and 8.3.0, or from Forcepoint Email Security version 8.4.0 or 8.5.0.
- You can upgrade directly to on-premises version **8.5.0** from TRITON AP-EMAIL version 8.1.0, 8.2.0, and 8.3.0, or from Forcepoint Email Security version 8.4.0.
- You can upgrade to Forcepoint Email Security in Azure version **8.5.4** from Forcepoint Email Security in Azure version 8.5.0 or 8.5.3, or migrate from on-premises versions 8.4.0, 8.5.0, and 8.5.3.
- You can upgrade to Forcepoint Email Security in Azure version **8.5.3** from Forcepoint Email Security in Azure version 8.5.0, or migrate from on-premises versions 8.2.0, 8.3.0, 8.4.0, and 8.5.0. If you are running AP-DATA Email Gateway version 8.3, it is not possible to upgrade to version 8.5.3; a new appliance must be installed. See Installing Forcepoint Email Security in Microsoft Azure for installation steps.
- You can upgrade to Forcepoint Email Security in Azure version **8.5.0** from AP-DATA Email Gateway version 8.3 or from Forcepoint Email Security in Azure version 8.5.0.
- If you are planning to deploy Forcepoint Email Security and Forcepoint Security Manager together in Azure:
  - For Forcepoint Email Security in Azure version **8.5.4**, you must first upgrade Forcepoint Security Manager to version 8.5.5.
  - For Forcepoint Email Security in Azure version **8.5.3**, you must first upgrade Forcepoint Security Manager to version 8.5.3.

Platform	Version	Mode	First Step	First Version	Second Step	Final Version
Physical	7.8.4	single	upgrade	8.4.0	upgrade	8.5.0
Physical	8.0.0	single	upgrade	8.3.0	upgrade	8.5.0
Physical	8.0.1	single	upgrade	8.3.0	upgrade	8.5.0
Physical	8.1.0	single			upgrade	8.5.0
Physical	8.2.0	single			upgrade migrate	8.5.0, 8.5.3 8.5.3 Azure
Physical	8.3.0	single			upgrade migrate	8.5.0, 8.5.0 8.5.3 Azure
Physical	8.4.0	single			upgrade migrate	8.5.0, 8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure
Physical	8.5.0	single			upgrade migrate	8.5.0, 8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure
Physical	8.5.3	single			upgrade migrate	8.5.4 8.5.4 Azure
Physical	7.8.4	dual	migrate	8.4.0	upgrade	8.5.0
Physical	8.0.0	dual	migrate	8.3.0	upgrade	8.5.0
Physical	8.0.1	dual	migrate	8.3.0	upgrade	8.5.0
Physical	8.1.0	dual			migrate	8.5.0
Physical	8.2.0	dual			migrate	8.5.0
Virtual	7.8.4	single	migrate	8.4.0	upgrade	8.5.0
Virtual	8.0.0	single	migrate	8.3.0	upgrade	8.5.0
Virtual	8.0.1	single	migrate	8.3.0	upgrade	8.5.0
Virtual	8.1.0	single			upgrade	8.5.0
Virtual	8.2.0	single			upgrade migrate	8.5.0, 8.5.3 8.5.3 Azure
Virtual	8.3.0*	single			upgrade migrate	8.5.0, 8.5.3 8.5.3 Azure
Azure	8.3.0	single			migrate	8.5.0 Azure
Virtual	8.4.0	single			upgrade migrate	8.5.0, 8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure

Platform	Version	Mode	First Step	First Version	Second Step	Final Version
Virtual	8.5.0	single			upgrade migrate	8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure
Azure	8.5.0	single			migrate migrate	8.5.0 Azure 8.5.3 Azure, 8.5.4 Azure
Virtual	8.5.3	single			upgrade migrate	8.5.4 8.5.4 Azure
Azure	8.5.3	single			upgrade	8.5.4 Azure

The version 8.3 virtual appliance was updated and re-released on June 2, 2017. Direct upgrade from a version 8.3 appliance to version 8.5.x is available only if you deployed from the updated OVA file released on June 2, 2017. If you deployed from the original OVA file released on December 19, 2016, you must use the migration process described in *Migrate to version 8.5.x*.

Important

Starting in version 8.5, vCPU specifications changed for virtual appliances, which will require you to increase your vCPU and RAM allocations following an upgrade from version 8.3 or lower.

See the Knowledge Base article Resource Upgrade on OVA and Forcepoint Appliances Getting Started Guide for additional information and virtual appliance specifications.

For systems running a version 7.6.x or 7.7x deployment, and requiring an upgrade to version 8.5.x, it is necessary to upgrade to version 7.7.0 or 7.8.0 first, then upgrade to version 7.8.4, then to version 8.4, and finally to version 8.5.x. See the following:

- Upgrading Email Security Gateway v7.6.x to v7.7.0
- Upgrading Email Security Gateway v7.7.x to v7.8.0
- Upgrading Email Security Gateway v7.8.0 to v7.8.x
- Upgrading to Forcepoint Email Security version 8.4

For systems running Email Security Gateway on an X10G security blade, it is necessary to upgrade to version 8.0.0 before upgrading to version 8.3. Next, a direct upgrade to version 8.5.0 is possible.

Certain older V10000 and V5000 appliances are not supported with version 8.0.0 and later. See V Series appliances supported with version 8.x.

Any version 7.6.x Email Security component that is currently installed on Windows Server 2003 must be migrated to Windows Server 2008 R2 before the upgrade to v7.7.0. Migration to Windows Server 2012 may be performed after an upgrade to v7.8.0.

Ensure that third-party components are upgraded as well, to work with your new email protection solution version.

For upgrade instructions, see:

- V Series Upgrade Guide
- X Series Upgrade Guide

We recommend that you perform a complete system backup in the event your system experiences a power outage or other interruption during the upgrade process. Recovery procedures are also included in case they are needed.

The upgrade process includes Forcepoint appliance components (V Series appliance, virtual appliance, or X Series chassis security blade), along with Forcepoint Security Manager and Email Log Server Windows components. Ensure that your deployment additionally includes Forcepoint DLP for data loss prevention (DLP) capabilities. The upgrade process detects and upgrades this module during the Security Manager upgrade.

Warning

Please contact Technical Support before you begin the upgrade process if Forcepoint personnel have customized any Email Security Gateway, TRITON AP-EMAIL, or Forcepoint Email Security back-end configuration settings.

Starting with v8.3.0, a single ISO image (v8.x.x Unified Appliance Installer) is offered to restore an appliance back to the factory settings as well as to upgrade all installed modules in the target appliance to the corresponding version.

Modules include:

- **App** - Base appliance infrastructure and appliance controller Forcepoint Web Security:
  Forcepoint Web Security:
- **Web** - Forcepoint Web Security core components
- **Proxy** - Content Gateway web proxy
  Forcepoint Email Security:
- **Email** - Forcepoint Email Security core components

To upgrade an appliance prior to v8.3.0, the legacy RPM upgrade package is required. Refer to the dedicated upgrade guide for V Series or X Series appliances.

Dual-Mode Appliances

The V Series appliance and the email virtual appliance were re-architected at version 8.3. Dual security mode on the V Series appliance (TRITON AP-EMAIL and TRITON AP-WEB or Web Filter & Security) is no longer supported. It is recommended to migrate the Email module off any dual-mode appliance to a new version 8.5.x appliance, leaving the web security system on the existing appliance. **Before beginning the upgrade**, see Upgrading V Series Dual-Mode Appliances to Version 8.5 for important upgrade instructions. Email data and messages on an existing virtual appliance must also be migrated to a new version 8.5.x appliance. See *Migrate to version 8.5.x*.

Related reference
Upgrade instructions on page 315

Upgrade preparation

Several issues should be considered, and certain steps taken, before beginning an email protection solution upgrade.

Before you begin

- Verify current deployment. Ensure that your current deployment is functioning properly before you begin the upgrade, and that required network interfaces have reliable connections to Forcepoint components and the Internet. The upgrade process does not repair a non-functioning system.
- Check the Certified Product Matrix to verify the supported operating systems for your initial and target versions. For example, version 8.5.3 does not support Windows 2008, which may cause errors when attempting to upgrade from a Windows 2008 operating system.
- Ensure that your existing deployment includes Forcepoint Security Solutions before you upgrade. If you have used the custom option to install Forcepoint Email Security, you must install Forcepoint Security Solutions as well, for data loss prevention capabilities. Consult the Forcepoint Security Manager Data Security module upgrade procedures, to ensure a smooth upgrade experience. See *Upgrading to Forcepoint DLP v9.0*, for details.
- If you are not already familiar with the preparation required for upgrading off-appliance components, review the requirements before upgrading your appliances.

  - For web protection solutions, see *Before upgrading v8.5.x web protection solutions* and the Release Notes for the web protection solution to which you are upgrading: v8.5.0 Web Protection Release Notes or v8.5.3 WebProtection Release Notes.
  - Review the Release Notes for the email protection solution to which you are upgrading: v8.5.0 Forcepoint Email Security Release Notes or v8.5.3 Forcepoint Email Security Release Notes.
- Verify the system requirements for the version to which you are upgrading to ensure your network can accommodate the new features and functions. See *System requirements for this version* for a detailed description.
- Prepare Windows components. See *All Forcepoint solutions* for an explanation of general preparations for upgrading the Windows components in your email protection system.
- Ensure that your firewall is configured correctly so that the ports needed for proper email protection operation are open. See *Forcepoint Email Security ports* for information about all email security system default ports, including appliance interface designations and communication direction.
- Prepare Microsoft Azure virtual network if you are upgrading to Forcepoint Email Security in Azure. See *Installing Forcepoint Email Security in Microsoft Azure*.
- Prepare for service disruption during upgrade. Appliance services are not available while the upgrade is applied, continuing until the appliance continues its final restart. Service is not disrupted while the off-box components are upgraded.
- If you are using link aggregation and plan to enable VLAN support after upgrade, disable link aggregation before enabling VLAN support on the blade or chassis. VLAN is only available on X Series appliances.
- Ensure you have the most recent hotfix installed for your version. Additionally, ensure that you have the following hotfixes installed or uninstalled, as appropriate.
  - Uninstall the following hotfix:
    - If you have any appliance with Hotfix 200 (Spectre/Meltdown Hotfix) installed, you must uninstall the hotfix before upgrading to v8.5.x. After upgrading, reinstall Hotfix 200 on the new version.
  - Install the following hotfix:
    - If you are a Forcepoint V5000 G2R2 customer upgrading from v8.4 to v8.5.x, you must install 8.4 Appliance Hotfix 101 (APP-8.4.0-101) before upgrading.
- Back up and remove tomcat log files and remove temporary manager files (optional; recommended to facilitate timely Forcepoint Security Manager upgrade). Use the following steps:

  1) Log onto the Windows server where the Forcepoint Security Manager resides.

  2) Navigate to the following directory: `C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs`

  3) Copy `C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs` to another location (for example, to `C:\WebsenseBackup\Email`), and then delete it in the directory mentioned in step 2.

  4) Navigate to the following directory: `C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\tempEsgUploadFileTemp`

  5) Delete all the downloadFile* files.

- Inventory all configuration customizations and make a plan for restoring any that are required. Customizations are not retained through the upgrade process. After your upgrade, contact Forcepoint Technical Support for assistance with restoring files from your pre-upgrade file system. Customizations can include:
  - Custom patches
  - Hand updated files
  - Extra packages added

- Extra files added, binary or configuration

- Inventory customized HTML notification templates for the Personal Email Manager and Forcepoint Secure Messaging end-user portals. Any customizations you make to notification message templates are lost when upgrading to a new version of Forcepoint Email Security. After upgrade, you will need to reconfigure your customized templates.
- Back up appliance configuration and settings. It is critical to perform a full appliance configuration backup and save it to a filestore.

  1) Log onto the CLI and elevate to **config** mode.

  2) To perform an immediate full backup, use:

     ```
     create backup now --location filestore_alias [--desc "<description>"]
     ```

  3) Include a unique description to make it easier to identify backup files that may have very similar names and dates.

Important

Before upgrading a virtual appliance, see *Virtual appliance*, for important upgrade issues specific to the virtual appliance.

Reminders

- Immediately following your upgrade, it is necessary to install the latest hotfix for your version. See the Forcepoint My Account Downloads page to download the latest hotfix.
- Version 8.5.0 was the last supported software release for the V5K G2R2 appliance and the V10K G3R1 appliance. Hardware support will continue to be available throughout End-of-Life for these appliance models. Please refer to the related Tech Alert and the official Product Support Life Cycle matrix for details.
- The Forcepoint V5000 G2R2 appliance may encounter a memory shortage after upgrading to version 8.2 or later. This issue is the result of newer versions of software requiring additional memory, and was only captured under a heavy load. A DIMM Kit (2 x 8GB) is certified to expand the physical memory of the V5000 G2R2 Appliance. It is now generally available and recommended for V5000 G2R2 deployment moving to versions 8.2 and later. Please contact your sales representatives for purchase information. For more details, see the related Knowledge Base article and the DIMM Kit installation instructions.
- The upgrade to version 8.0.x and 8.2.x renamed the following default policy filters, policies, and rules:
  - ThreatScope was renamed File Sandbox; at version 8.2.x, File Sandbox was renamed Advanced File Analysis.
  - URL Scanning was renamed URL Analysis.

  If you currently have custom rules with these new names, change them before the upgrade process begins, to avoid having duplicate rule names after the upgrade. The email security system may not function properly with the duplicate names.
- The upgrade to version 8.3 added the following default elements:
  - Spoofed Email policy filter
  - Spoof policy action
  - Antispoof policy rule
  - “url-analysis” default queue

  If your system currently uses policy elements or a queue with these names, change them before the upgrade process begins, to avoid having duplicate names after the upgrade. The email security system may not function properly with the duplicate names.
- The upgrade to version 8.4 added the following default elements:

- Email Attachment policy filter
- Email Attachment policy action
- Email Attachment policy rule
- “attachment” default queue

Note

If your system currently uses policy elements or a queue with these names, you must change them before the upgrade process begins.

The version 8.5.x upgrade process includes a pre-check function that terminates the upgrade if duplicate policy components are detected.

- New presentation reports were added in version 8.3 for spoofed email and URL analysis data. Examples include:
  - Outbound Spoofed Email Percentage Summary
  - Top Inbound Spoofed Email Sender Domains
  - Top Inbound Recipients of Spoofed Email
  - Top Outbound Embedded URL Categories Detected
  - Outbound Embedded URL Detection Volume Summary

  The upgrade process may not complete successfully if you have existing custom reports with the same names as these reports.

Backup procedures

Applies to:

- Forcepoint Email Security, v8.5.x

The backup procedures outlined in the following steps are safeguards against an unexpected interruption of your upgrade process. A power outage or appliance restart may not allow the upgrade process to finish successfully. You may need to restore your settings databases to their pre-upgrade state in order to re-initiate and complete the upgrade.

Use the following backup procedure to prepare for your email protection solution upgrade:

1) Back up the Forcepoint Security Manager settings. See the topic titled Backup and Restore of Global Settings Data in Forcepoint Security Manager Help for backup procedures.

2) Back up the Data Security management server configuration. See the Technical Library topic titled How do I backup and restore Data Security software? for backup instructions.

3) Back up your Microsoft SQL Server databases. Ensure that all the files in the following directories are included in your backup:
   \\Database\\esglogdb76

   \\Database\\esglogdb76_*n*

   \\SQL Server Agent\\Jobs\\ ESG_ETL_Message_Insert_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Process_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Summary_Address_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Summary_Job

\\SQL Server Agent\\Jobs\\ESG_ETL_Message_Update_Job

\\SQL Server Agent\\Jobs\\ESG_Maintenance_Job

See your Microsoft SQL Server documentation for backup procedure details.

4) Back up email appliance configuration settings using appliance-appropriate back-up procedures.
   - See the topic titled How do I backup and restore Forcepoint appliances? for backup procedures.
   - See the Forcepoint Appliances Command Line Interface guide for backup and restore command options.

5) Back up Email Security module configuration settings in the Forcepoint Security Manager using options on the **Settings** > **General** > **Backup/Restore** screen. Click **Backup** to store your settings locally. You can also specify the Log Database for your configuration settings backup location and then click **Backup**. See the topic titled Backing up and restoring management server settings in Administrator Help for Forcepoint Email Security backup details.

6) Upgrade any third-party integration products if necessary for use with your email protection system. See third-party product documentation for appropriate backup and upgrade requirements and procedures.

7) Redirect email traffic out of the system that is being upgraded. If you do not redirect mail traffic, you may lose messages cached during the upgrade process.

Note

The Personal Email Manager end-user utility is not available until after the appliance upgrade is complete.

Recovery procedures

Applies to:

- Forcepoint Email Security, v8.5.x

In the event that your upgrade was unexpectedly interrupted (for example, by a power outage or appliance restart) and the automatic rollback facility also fails, you can use the backup files you created earlier in the process to restore your system to its pre-upgrade state. (See *Backup procedures*).

Note

Any quarantined or archived messages stored in the appliance local queues may be lost as a result of the recovery process.

Use the following procedure to restore your email protection system:

1) Use the appropriate recovery image to reimage your appliance to the version from which you were upgrading.

2) Run `firstboot`.

3) Restore the backup files to your system in the following order, using the restore information for each component referenced in *Backup procedures*:

a) Appliance

b) Microsoft SQL Server databases

c) Forcepoint Security Manager

d) Data Security module

e) Email Security module

Important

Your backup files should match the version of the email protection system to which you are restoring.

For example, if your backup files are from v8.1.0, you should not upgrade to v8.5 before restoring the v8.1.0 email files.

4) Verify that your system works as it did before the interrupted upgrade. You can now initiate the upgrade process.

Related reference

Backup procedures on page 313

Upgrade instructions

Once you have completed the activities outlined in *Upgrade preparation*, you can proceed with the product upgrade. This section provides instructions for performing an upgrade of an email security system deployment.

Important

If your network includes a Forcepoint web security solution, you must upgrade the Policy Broker/Policy Server machine first, whether or not these components reside on an appliance. Other Forcepoint services located on the Policy Broker/Policy Server machine should be upgraded at the same time. See UpgradeInstructions for Forcepoint Web Security .

This section provides a description of an email system upgrade to the following components:

1) Email Log Server (*Upgrade the Email Log Server*)

2) Forcepoint Security Manager Email Security Module (*Upgrade the Forcepoint Security Manager Email Security Module*)

3) Forcepoint Appliances (*Upgrade or migrate Forcepoint Appliances*)

Important

When the upgrade is applied, the original file system is preserved. Should the upgrade procedure encounter a fatal error, the original file system is restored. Off-appliance components may need to be restarted.

Upgrade the Email Log Server

If the Email Log Server is installed on a separate machine from the Forcepoint Security Manager, upgrade the Email Log Server using the Forcepoint Security Installer from the Forcepoint My Account downloads page.

If the Email Log Server is installed on the same machine as the Forcepoint Security Manager, it is included in the upgrade process described in *Upgrade the Forcepoint Security Manager Email Security Module*.

Important

If you are upgrading multiple Log Servers, perform the upgrades one at a time to avoid possible upgrade process errors.

1) Download the **Forcepoint Security Installer** from the Forcepoint My Account downloads page.

2) Run the installer and follow the installation wizard instructions for Log Server.

   a) The installer does not allow you to change existing configuration settings. Changes must be made after the upgrade.

   b) The upgrade installer stops the Email Log Server service, updates the Email Log Server and the Email Log Database, and then restarts the Email Log Server service.

Upgrade the Forcepoint Security Manager Email Security Module

Use the Forcepoint Security Installer from the Forcepoint My Account downloads page. The upgrade process includes Forcepoint DLP and the Email Log Server if it is installed on the Security Manager machine.

If you are planning to deploy both Forcepoint Email Security and Forcepoint Security Manager in Azure, this procedure is necessary to first upgrade Forcepoint Security Manager to version 8.5.3.

1) Download the **Forcepoint Security Installer** from the Forcepoint My Account downloads page.

2) Run the installer and ensure that Forcepoint Email Security and Forcepoint DLP are selected for upgrade. The upgrade process includes Forcepoint DLP and the Email Log Server if it is installed on the Security Manager machine.

3) Follow the installation wizard instructions.
   The Data Security module upgrade occurs after the Forcepoint Management Infrastructure upgrade. The Email Security module upgrade follows the Data Security module.
   - The upgrade installer Configuration page shows the IP address of the database engine that manages the Email Log Database and logon type. If you have changed the database since your previous installation or upgrade, use this page to change these settings.
   - The upgrade script stops the Email Security module service, updates the Email SQL Server databases (and Log Server if found), and then restarts the Email Security module service.

Note

The Security Manager Email Security module is not available until after the Security Manager upgrade completes.

Upgrade or migrate Forcepoint Appliances

Appliance services are not available while the upgrade is being applied; email traffic should not be directed through appliances during the upgrade process. Disruption continues until the appliance completes its final restart. It is a best practice to perform the upgrade at a time when service demand is low.

Important

If you are running appliances in a cluster, you must release all appliances from the cluster before performing an upgrade or a migration. Upgrade or migrate each appliance as needed, and then rebuild your cluster after the process is complete.

X Series

For the X Series hardware appliance, see the Forcepoint X Series upgrade guide for upgrade instructions and command options on this platform.

If you are running an X10G security blade version 8.0.x, you must upgrade to version 8.3 before you upgrade to version 8.5.x. You cannot upgrade directly to version 8.5.x from version 8.0.x.

V Series

For the V Series hardware appliance, see the Forcepoint V Series Appliance upgrade guide for complete upgrade instructions and command options.

Note

Dual security mode V Series appliances are not supported in version 8.3 and later. If you are upgrading a V Series appliance from a version earlier than 8.3, we recommend that you migrate the Email Security module off the dual-mode appliance to a new version 8.5.x appliance. See V Series Dual-ModeAppliance Upgrade Guide for details on upgrading a dual-mode (Web and Email) appliance.

The version 8.3 and later V Series appliance introduced a command-line interface (CLI) to replace the Appliance Manager. For an introduction to the CLI, see the Forcepoint Appliances CLI Guide.

The V Series appliance upgrade process includes a check for:

- Adequate disk space for Forcepoint Email Security (at least 8 GB required)
- Cached message log file size (cannot exceed 10 MB)
  A backup and restore function to save existing appliance configuration settings is also included. You are prompted to contact Technical Support if any configuration file is missing.

  When upgrading V Series appliances configured in a cluster, you must upgrade the primary box first, followed by all its secondary machines, one at a time.

Note

You may need to restart the appliance if you cannot establish an **ssh** connection after the upgrade is complete.

Virtual appliance

The Forcepoint Email Security virtual appliance platform was re-architected at version 8.3. As a result, email security system data and email messages that reside on a pre-version 8.3 virtual appliance must be migrated off that appliance when you upgrade to a new version. The migration is accomplished via a command-line interface (CLI) `migrate` command performed on the version 8.5.x appliance.

Migration is necessary when upgrading any version of Forcepoint Email Security to Forcepoint Email Security in Azure. See *Migrate to version 8.5.x*.

Important

Direct upgrade from a version 8.3 appliance to version 8.5.x is available only if you deployed from the OVA file released on June 2, 2017. If you deployed from the OVA file released on December 19, 2016, you must use the migration process described in the following section to upgrade to version 8.5.x.

Upgrade to version 8.5.x

Use the following steps to upgrade directly to version 8.5.x.

1) Download the v8.5.x **Forcepoint Security Installer** from the Forcepoint My Account downloads page and save it to a location from which it is easy to copy it to Windows servers hosting Forcepoint web, email, and data components, such as Forcepoint Security Manager (formerly TRITON Manager) and Log Server.

2) Perform *Upgrade preparation*.
Skip to Step 4 if your deployment does not include Forcepoint Web Security.

3) If your deployment includes Forcepoint Web Security, upgrade the policy source machine (Policy Broker/Policy Database) before upgrading web protection components on your security blades. If the *Full policy source* machine is an X10G, upgrade that blade first. After upgrading the policy source machine, confirm that Policy Broker and Policy Database services are running.
All Forcepoint components on the *Full policy source* machine are upgraded when Policy Broker/Policy Database are upgraded.

   In all instances, you must upgrade Forcepoint Web Security components in the following order:

   a) *Full policy source*
   Upon completion, confirm that Policy Broker and Policy Database services are running. See *Upgrading Web Protection Solutions*.

   b) *User directory and filtering* (sometimes called *policy lite*) blades and non-appliance servers that host Policy Server

   c) *Filtering only* blades, and non-appliance servers that host Filtering Service

   d) Off-appliance servers hosting other web protection components (like Log Server or Logon Agent)
   Successful upgrade of *User directory and filtering* and *Filtering only* appliances requires connectivity with the Policy Broker and Policy Database services.

4) If the appliance is registered in Forcepoint Security Manager, navigate to **Appliances** > **Manage Appliance** and unregister the appliance.
Re-registration is a post-upgrade activity.

   If the appliance is a *User directory and filtering* appliance, unregister the appliance. In the Web module of Forcepoint Security Manager, navigate to **Settings** > **General** > **Policy Servers** and unregister the appliance.

5) Using the CLI, download and apply the v8.5.x upgrade:

   a) Download the upgrade file.
   ```
   load upgrade
   ```

   b) Install the upgrade.
   ```
   install upgrade
   ```

Select the v8.5.x upgrade file from the list.

When prompted, confirm to continue, then accept the subscription agreement.

The upgrade performs several system checks. The checks may take several minutes.

When installation is complete, the appliance automatically restarts.

If the upgrade fails, the blade server automatically rolls back to the prior version. If the source of the failure is not obvious or cannot be easily address, contact Forcepoint Technical Support.

If an error message displays indicating that ISO verification has failed, repeat the command with the following parameter added:

```
--force <iso_file_name>
```

If installation seems to stop, allow the process to run for at least 90 minutes. If installation has not completed in that time, contact Forcepoint Technical Support.

6) Perform *Post-upgrade activities*.

7) Return to Step 5 and upgrade remaining appliances.

8) Upgrade the management server (if not upgraded when Policy Broker/Policy Database were upgraded), and other servers that host Forcepoint components. See Upgrading Forcepoint Security Solutions to v8.5.x.

Migrate to version 8.5.x

Consider the following issues before you initiate your virtual or Azure appliance migration process:

- Ensure that your source and destination appliances in the migration are configured in the same subnet. If they are not, the migration process may complete, but the new appliance interfaces are not correctly updated.
- You may need to reconfigure some network settings for the migration process. The version 8.3 and later virtual appliance supports three network interfaces: C, P1, and P2. In the migration, the C interface retains the setting you assigned it during firstboot. The P1 and P2 interfaces (eth0 and eth1) inherit the settings of P1 and P2 when migrating from a V5000, or the E1 and E2 settings when migrating from a V10000.
  - Forcepoint Email Security in Azure supports only the C interface.
- Dynamic Host Configuration Protocol (DHCP) is not supported in version 8.3 and later. If your existing appliance has DHCP enabled, those network settings are not migrated. You must configure static network interface IP addresses for your appliance.
- Calculate the disk space used on your existing appliance and ensure that the new appliance has adequate disk space for all data you wish to migrate.

Use the following steps to migrate data and email messages to a version 8.5.x appliance.

1) Install a new version 8.5.x appliance.
   The VMware virtual machine requires ESXi version 6.0 or later. See the topic titled *Virtual Appliance Setup* in the ForcepointAppliances Getting Started Guide for detailed instructions for downloading and creating a virtual machine.

   If you are migrating to an Azure deployment, skip to Step 4. See InstallingForcepoint Email Security in Microsoft Azure.

2) On the source appliance, open a default port for your installation:
   - On-premises: port 22
   - Azure: port 22222

3) On the new appliance (version 8.5.x), run the firstboot wizard to select appliance security mode (email), enter appliance management settings (e.g., C interface IP address, hostname, DNS server IP addresses), and define some basic configuration settings (e.g., hostname, administrator password, system time zone). This step is not applicable in Azure.
See the topic titled *Firstboot Wizard* in the Forcepoint Appliances Getting Started Guide for detailed firstboot instructions.

> **Note**
>
> The source appliance hostname is not migrated to the destination appliance. The destination appliance uses the hostname set during firstboot, and then the upgrade process adds "-esg" to the end of the name.

4) Log on to the new version 8.5.x appliance CLI and elevate to **config** mode. If you are migrating to an Azure deployment, skip to Step 6.

5) Set the appliance P1 interface using the **set interface ipv4** command with the following syntax:

```
set interface ipv4 --interface p1 --ip <ipv4_address> [--mask <ipv4_netmask>] --gateway
 <ipv4_address>
```

Setting this interface now can facilitate the migration process in the event that your current P1 interface is a virtual IP address, which will not be migrated.

The P1 interface you configure in the CLI is displayed as "E1" in the Forcepoint Security Manager. This step is not applicable in Azure.

> **Note**
>
> If you use a client interface like PuTTY to connect to the appliance, configure a longer connection session to accommodate a slightly lengthy migration process.
>
> For example, in the PuTTY configuration interface, select the **Connection** category. Enter **30** in the **Seconds between keepalives (0 to turn off)** entry field.

6) Download the appropriate hotfix for your source virtual appliance version from the Forcepoint MyAccount Downloads page.
   - Version 8.1.0, 8.2.0, 8.3.0, 8.4.0, 8.5.0, or 8.5.3 on-premises: Hotfix 300
   - Version 8.3, 8.5.0, or 8.5.3 in Azure: Hotfix 301

7) Contact Forcepoint Technical Support for assistance to apply the hotfix to your previous version appliance. See the ReadMe file packaged with the hotfix for more information about hotfix contents.

8) In the version 8.5.x appliance CLI, ensure you are still in **config** mode and then log in to the email module:

```
login email
```

9) You may perform the migration using the `migrate` CLI command on the version 8.5.x appliance with one of two options: interactive or silent.
Interactive mode is a step-by-step process that requires user input during the process.

The following displays an example of the interactive mode command:

```
onfig)(Email)# migrate
ve  silent
onfig)(Email)# migrate interactive

o the Forcepoint Email Security Migration Tool.

on Forcepoint Email Security System Information:

orm: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

ame: email85-esg

10.206.12.47  Mask:255.255.255.0

B of 32125MB disk space used for running the system

of 95863MB disk space used for the email messages

Forcepoint Email Security services...

t Email Security services check has been successfully completed.

 like to migrate the source system to this appliance? [yes/no]

 certificates...

tes have been successfully prepared.

ter the Forcepoint Email Security interface IP address for the source appliance:
.239
```

Interactive mode requires the following information to be entered:

- Source appliance (pre-version 8.5.x) IP address.
- Confirmation for the start of the migration.
- Selection of a mode option; **Azure** or **On-Premises**.
  Select **Azure** if you are migrating to a version 8.5.x Azure appliance.

  Select **On-Premises** if you are migrating to a version 8.5.x on-premises appliance.

  The following displays the selection of **On-Premises** to migrate to an 8.5.x on-premises appliance:

```
Please select a mode option: [1/2]

    1. Azure mode. Select this mode if either your source or destination appliance is an Azure appliance.
    2. On-Premises mode. Select this mode if both your source and destination appliances are on-premises.

2
When making your selection, please ensure that both your source and destination appliances are on-premises. Do you wish to proceed in On-Premises mode? [yes/no]
yes
Reading appliance information...

sending incremental file list

sent 1131 bytes  received 15 bytes  2292.00 bytes/sec
total size is 761902  speedup is 664.84

Source Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: evasquez_appliance-esg

    Eth0:10.206.21.239  Mask:255.255.255.0

    9372MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages


Disk space is available on this appliance.

Checking Forcepoint Email Security services...

Forcepoint Email Security upgrade pre-check has been successfully completed.
```

- Selection of a transfer option.
  If you migrate email message queues in addition to configuration settings, be aware that the transfer of large-volume queues may take a few hours to complete. The following image displays an example of the CLI for this section:

```
Source Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: evasquez_appliance-esg

    Eth0:10.206.21.239  Mask:255.255.255.0

    9372MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages


Disk space is available on this appliance.

Checking Forcepoint Email Security services...

Forcepoint Email Security upgrade pre-check has been successfully completed.


Would you like to start the migration process from the source appliance: 10.206.21.239 to this appliance (services on both appliances will stop)? [yes/n
yes
Please select a transfer option: [1/2/3]

    1. Transfer only configuration files, defer logs, and policy incidents.
    2. Transfer configuration files, defer logs, policy incidents, and email messages.
    3. Quit

2
```

Silent mode requires the following information to be entered:

- Source appliance (pre-version 8.5.x) IP address.
- Migration mode; **Azure** or **On-Premises**.
- Subscription key.

The subscription key is only required when the migration mode is Azure.

The second transfer option is automatically selected for silent mode, and the migration runs without the need for subsequent user input.

The following image displays an example of the CLI for silent mode:

```
email85(config)(Email)# migrate silent --host 10.206.21.239 --mode On-Premises

Welcome to the Forcepoint Email Security Migration Tool.

Destination Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: email85-esg

    Eth0:10.206.12.47  Mask:255.255.255.0

    9185MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages

Checking Forcepoint Email Security services...
```

Important

You must use your existing TRITON Manager or Forcepoint Security Manager Windows machine. Use of a newly installed TRITON Manager or Forcepoint Security Manager for an upgrade is not currently supported.

Consider the following after you perform your virtual appliance migration process:

- If you have an email DLP policy configured to use a TRITON AP-DATA or Forcepoint DLP quarantine action, and the Release Gateway on the page **Settings** > **General** > **Remediation** is set to **Use the gateway that detected the incident**, you should change the Release Gateway to the IP address of your new appliance. Otherwise, when a Data Security module administrator releases a pre-migration quarantined message, an “Unable to release incident” error is generated.
- Virtual IP address settings in filter actions are not retained after an appliance migration. You need to reconfigure virtual IP address settings manually.

Important

Please contact Technical Support if Forcepoint personnel have customized your appliance iptables settings. These customizations are not preserved by the migration process.

Post-upgrade activities

Your system should have the same configuration after the upgrade process as it did before the upgrade. Any configuration changes can be made after the upgrade process is finished.

After your upgrade is completed, redirect email traffic through your system to ensure that it performs as expected.

Email hybrid service registration information is retained during the upgrade process, so you do not need to complete the registration again, unless you have performed an appliance migration (e.g, from a virtual appliance to a new virtual appliance). See *Update appliance management interface configuration settings (for migration only)*, for information.

Perform the following tasks in the Forcepoint Security Manager or the CLI:

- *Install Email Security hotfixes*
- *Repair Email Security registration with Data Security*
- *Update data loss prevention policies and classifiers*
- *Update Forcepoint databases*
- *Update Email Security module backup file*
- *Configure email DNS lookup*
- *Increase vCPU and RAM allocation*
- *Update appliance management interface configuration settings (for migration only)*
- *Verify the system and configuration in the CLI*

Install Email Security hotfixes

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

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

Repair Email Security registration with Data Security

Re-register the new appliance with the Data Security module as follows:

1) In the Email Security module, navigate to the page **Settings** > **General** > **Data Loss Prevention** and click **Unregister**.

2) Register the appliance with the Data Security module; click **Register**.

3) Navigate to the page **Settings** > **General** > **Data Loss Prevention** and ensure that the appliance management (C) interface IP address appears in the field **Communication IP address**.

4) In the Data Security module, navigate to the page **Settings** > **Deployment** > **System Modules** and select the **Email Security module**.

5) In the upper left corner, click **Delete**.

6) Deploy the changes; click **Deploy**.

Update data loss prevention policies and classifiers

1) Select the Data Security module.

2) Follow the prompts that appear for updating data loss prevention policies and classifiers.
Depending on the number of policies you have, this can take up to an hour. During this time, do not restart the server or any of the services.

3) Deploy the changes; in the upper right of the Data Security module, click **Deploy**.

Update Forcepoint databases

From the page **Settings** > **General** > **Database Downloads**, click **Update Now**. This action performs an immediate database download update.

Update Email Security module backup file

Due to a change in implementation at version 8.1, the Security Manager Email Security module backup file format is not compatible with versions earlier than 8.1. You must remove any pre-version 8.1 backup log file before you create a new backup file for version 8.5.x. If you do not remove the old log file before you create the new file, the backup/restore function may not be accessible.

Use the following steps:

1) Navigate to the following directory on the Security Manager machine:
`C:\Program Files (x86)\Websense\Email Security\ESG Manager`

2) Locate and remove the following file:
`ESGBackupRestore`

Copy this file to another location if you want to save it.

3) Create a new backup file on the page **Settings** > **General** > **Backup/Restore**.

Configure email DNS lookup

The virtual appliance firstboot process includes the entry of DNS server settings. You can enhance DNS lookup query performance by configuring a second set of DNS server entries specifically for the Email Security module. Use the following CLI commands, as needed:

```
set interface dns --module email --dns1 <DNS_IP>
set interface dns --module email --dns2 <DNS_IP>
set interface dns --module email --dns3 <DNS_IP>
```

Not applicable for Forcepoint Email Security in Azure.

Increase vCPU and RAM allocation

If you upgraded from version 8.3 or lower to version 8.5.x, it is necessary to increase the vCPU and RAM allocations on your virtual appliance, in order to ensure adequate system resources.

See the Knowledge Base article Resource Upgrade on OVA and Forcepoint Appliances Getting Started Guide for more information.

Update appliance management interface configuration settings (for migration only)

If your upgrade to version 8.5.x included a data migration, you need to re-configure some functions that use the appliance management (C) interface after the migration and upgrade are complete. The management (C) interface was added for virtual appliance users at version 8.3.

Forcepoint Email Security in Azure supports only the C interface. These configuration settings include:

- *Data loss prevention*
- *Email hybrid service*
- *Personal Email Manager notification message*
- *Update Log Database*

- *Reset Forcepoint Email Security license (only if Forcepoint Security Manager was migrated to Azure)*
- *Move Forcepoint DLP database (only if Forcepoint Security Manager was migrated to Azure)*

Data loss prevention

Re-register the new appliance with the Data Security module as follows:

1) Select the Email Security module and navigate to the page **Settings** > **General** > **Data Loss Prevention**.
2) Remove DLP registration; click **Unregister**.
3) In the Data Security module, navigate to the page **Settings** > **Deployment** > **System Modules**.
4) Select the Email Security module.
5) In the upper left corner, click **Delete**.
6) On the Email Security module page **Settings** > **General** > **Data Loss Prevention**, ensure the appliance management (C) interface IP address appears in the field **Communication IP address**.
7) Register the appliance with the Data Security module; click **Register**.
8) Select the Data Security module and click **Deploy**.

Email hybrid service

This action is required only if you used the C interface on a hardware appliance that you have migrated.

Re-register the new appliance with the email hybrid service as follows:

1) Select the Email Security module and navigate to the page **Settings** > **Hybrid Service** > **Hybrid Configuration**.
2) At the bottom of the Hybrid Configuration page, click **Edit**.
3) Replace the SMTP server IP address with the new C interface IP address.
4) Click **OK**.

Personal Email Manager notification message

This action is required only if you used the C interface on a hardware appliance that you have migrated.

You may need to enter your destination appliance management interface IP address for the proper distribution of Personal Email Manager notification messages.

1) Select the Email Security module and navigate to the page **Settings** > **Personal Email** > **Notification Message**.
2) In the text field **IP address or hostname**, enter the new appliance management (or C) interface.
3) Click **OK**.

If you had previously customized HTML notification templates for the Personal Email Manager, your customizations were lost when upgrading to the new version; reconfigure your templates on the page **Settings** > **Personal Email** > **Notification Message**.

Update Log Database

If you encounter the following warnings after your upgrade, you may need to update the Email Log Database with new values for appliance hostname, management interface IP address, C interface IP address, and device ID:

```
[*]: Forcepoint Email Security migration has been successfully completed.

Please read the following warnings:
[WARNING]: [Errno -3] Temporary failure in name resolution
[WARNING]: Cannot update Forcepoint Email Security management interface.
For problems, please contact Forcepoint Technical Support.
```

You may encounter this situation if you use Windows authentication. In that case, the migration script cannot update the C interface, resulting in this message.

1) Open SQL Server Management Studio.

2) Click **New Query**.

3) In the query window, enter the following command:

   ```
   USE [esglogdb76]
   ```

   Select the **esg_device_id**, **admin_manage_ip**, and **device_c_port_ip** from the dbo.esg_device_list.

4) Enter **GO**.

5) Locate the **esg_device_id** associated with either the admin_manage_ip or the device_c_port_ip of the source appliance.

6) Execute the following command using the values you obtained in the previous steps:

   ```
   UPDATE dbo.esg_device_list SET esg_name = '<host name>', admin_manage_ip = '<appliance
    management IP address>', device_c_port_ip = '<C IP address>' WHERE esg_device_id = '<device
    id>'
   ```

7) Enter **GO**.

8) Run the query.

Reset Forcepoint Email Security license (only if Forcepoint Security Manager was migrated to Azure)

If you migrated Forcepoint Security Manager to Azure, it is necessary to reset the Forcepoint Email Security licenses for each of your appliances. Contact Forcepoint Technical Support for assistance with this step.

After Technical Support has reset your licenses, navigate to **Settings** > **General** > **Email Appliances** and add each of your appliances. See Forcepoint Email Security Administrato Help .

Move Forcepoint DLP database (only if Forcepoint Security Manager was migrated to Azure)

If you migrated Forcepoint Security Manager to Azure, it is necessary to move your Forcepoint DLP database to the new Forcepoint Security Manager in Azure. See How do I move the TRITONAP-DATA database to another MS SQLServer? for instructions.

Verify the system and configuration in the CLI

The following table details system and configuration checks made in the CLI. See the Forcepoint Appliances CLI Guide for more information.

- Log on to the CLI and elevate to `config` mode.

Action	Command

Display system information	`show appliance info`
	
	Results may be similar to:
	
	`Uptime: 0 days, 2 hours, 13 minutes`
	`Hostname: webapp.example.com`
	`Hardware_platform: X10G G2`
	`Appliance_version: 8.5.0`
	`Mode: Forcepoint Web Security`
	`Policy_mode: Filtering only`
	`Policy_source_ip: 10.222.21.10`

Display the upgrade history	`show upgrade history`

Display the appliance and module status	`show appliance status`
	`show <module>`
	
	If expected system services are not running, restart the module that hosts the services.
	
	`restart <module>`

Display network interface settings	`show interface info` If you have bonded interfaces, note that the names used to indicate the type of bonding have changed. For example, load-balancing is now balance-rr.

Check and synchronize the system time, if necessary	`show system ntp`
	`show system clock`
	`show system timezone`
	
	If the clock is off and NTP is configured, sync with:
	
	`sync system ntp`
	
	Otherwise, to sync when the time is set manually, see “System time and time synchronization with Forcepoint servers” in Forcepoint Appliances Getting Started.

Configure size and frequency values for archiving commands	`set log archive`

Check SNMP polling and alerting settings (if you integrate with a SIEM or SNMP server)	`show snmp config`
	`show trap config`
	`show trap events`
	
	These commands are not supported in Forcepoint Email Security in Azure.

Chapter 28

Initial Configuration for All Security Modules

Contents

Before you begin

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint Appliances, v8.5.x

Steps

1) Some of the ports required 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 *Default ports for on-premises Forcepoint security solutions*.

2) To avoid performance issues, exclude certain folders and files from antivirus scans. See *Excluding Forcepoint files from antivirus scans*.

3) If administrators use Internet Explorer to access the Forcepoint Security Manager, make sure that Enhanced Security Configuration is disabled on their machines.

   In Windows Servers:

   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 the Forcepoint Security 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.

4) Use a supported browser (see *System requirements for this version,*) to launch the Forcepoint Security Manager and log on using the default account:

a) Navigate to the following URL:

`https://<IP_address>:9443`

Here, <IP_address> is the IP address of the Forcepoint management server.

b) Log on as the default **admin** account, using the password set during installation.

5) Enter your subscription key or keys. At first startup:

- The Web Security module of the Security Manager prompts for a subscription key in the Initial Setup Checklist. If you have a solution that includes Content Gateway, the key you enter is automatically applied to Content Gateway, as well.
- The Data Security module of the Security Manager displays the subscription key page. See the “Initial Setup” section of the Forcepoint DLP Administrator Help for more information.
- The Email Security module of the Security Manager prompts for a subscription key. Enter the subscription key when prompted, or enter later on the **Settings > General > Subscription** page.

6) If you did not provide SMTP server details during installation, use the **Global Settings > General > Notifications** page to specify the SMTP server used to enable administrator password reset functionality and account change notifications.

To access the Global Settings page, click the gear-shaped icon in the Security Manager toolbar.
See the Forcepoint Security Manager Help for more information.

7) If SQL Server Express was installed, verify that SQL Server Browser service is running and that TCP/IP is enabled.

a) Launch SQL Server Configuration Manager.

b) In the tree pane, select **SQL Server Service**.

c) In the properties pane, make sure SQL Server Browser is running and start mode is automatic.

Right-click to start the service or change its start mode.

d) In the tree pane, select **SQL Server Network Configuration** > **Protocols for** <instance name>, where <instance name> is the default instance or TRITONSQL2K8R2X (or other instance name you specified).

e) In the properties pane, make sure TCP/IP is enabled.

If not, right-click TCP/IP and enable it.

Next steps

Continue with the initial configuration steps for the security solutions you have installed:

- Initial configuration for web protection solutions
- Forcepoint DLP initial configuration
- Forcepoint Email Security initial configuration
- Content Gateway initial configuration

Related concepts

Initial configuration for web protection solutions on page 331
Forcepoint DLP initial configuration on page 335
Forcepoint Email Security initial configuration on page 336
Content Gateway initial configuration on page 337

Related reference

Default ports for on-premises Forcepoint security solutions on page 361
Excluding Forcepoint files from antivirus scans on page 370
System requirements for this version on page 9

Initial configuration for web protection solutions

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Getting started with web protection solutions

After entering your Forcepoint Web Security or Forcepoint URL Filtering subscription key (see *Initial Configuration for All Security Modules*), use the Initial Setup Checklist to complete basic setup tasks.

- If you have Forcepoint Web Security, also see *Content Gateway initial configuration*.
- If you have the DLP Module also see *Additional configuration for the Web Security DLP Module*.

Next, you can:

- Configure transparent user identification on the **Settings > General > User Identification** page.
  - If you installed Logon Agent, you must create and deploy a client logon script in addition to configuring Logon Agent in the Web Security module of the Forcepoint Security Manager. See the Using Logon Agent for Transparent User Identification technical paper for instructions.
  - If you could not give User Service, DC Agent, or Logon Agent administrator privileges during installation, see Changing DC Agent, Logon Agent, and User Service permissions.
- Enable email or SNMP alerting on the **Settings > Alerts > Enable Alerts** page.

- Customize reporting behavior. See Reporting Administration.

Additional tips for working with web protection solutions

All web protection tools and utilities installed on Windows Server platforms (such as wsbackup.exe and websenseping.exe), as well as text editors used to modify web protection configuration files (such as websense.ini), **must** be run as the local administrator. Otherwise, administrators may be prevented from running the tool, or changes may not be implemented.

1) Navigate to the **bin** directory (C:\Program Files or 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**.

Identifying Filtering Service by IP address

When an Internet request is blocked, 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 the organization has an internal domain name server (DNS), enter the Filtering Service machine's IP address as a resource record in your DNS. See the DNS documentation for instructions.
- If the organization does 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 tool (Start > Administrative Tools > Services or Server Manager > Tools > Services) to restart **Websense Filtering Service**.

- *Linux*: Use the /opt/Websense/WebsenseDaemonControl command to restart **Filtering Service**.

Related concepts
Content Gateway initial configuration on page 337
Additional configuration for the Web Security DLP Module on page 333

Related tasks
Initial Configuration for All Security Modules on page 329

Additional configuration for the Web Security DLP Module

Applies to:
■ Forcepoint Web Security, v8.5.x

In addition to the items under *Initial configuration for web protection solutions*, perform these procedures if your subscription includes the DLP Module.

Confirm Content Gateway registration with Forcepoint DLP

Content Gateway registers with Forcepoint DLP automatically. To ensure that registration is successful:

- Synchronize the date and time on the Content Gateway and Forcepoint management server machines to within a few minutes.
- If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the appliance management interface (C) 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 Forcepoint management server during the registration process.
  After registration, the IP address can move to another network interface.

If registration fails an alarm displays in the Content Gateway manager.

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

a) Go to the **Configure > Security > Web DLP** page and enter the IP address of the management server.

b) Enter a user name and password for an administrator with Deploy Settings privileges in the Data Security module of the Security Manager.

c) Click **Register**.

After Content Gateway has registered with Forcepoint DLP:

1) In the Content Gateway manager, go to the **Configure > Security > Web DLP** page.

2) Enable **Analyze FTP Uploads** to send FTP uploads to DLP Module components for analysis and policy enforcement.

3) Enable **Analyze HTTPS Content** to send decrypted HTTPS posts to DLP Module components for analysis and policy enforcement. SSL Manager must be enabled on Content Gateway.
These options can be accessed whenever Forcepoint DLP is registered by going to the **Configure > Security > Web DLP > General** page.

4) Click **Apply** and restart Content Gateway.

See *Forcepoint DLP ports* for ports used by DLP Module components to communicate with the Content Gateway proxy.

Configuring the Content Gateway policy engine

When Content Gateway is registered with DLP Module components, Content Gateway appears on the System Modules page in the Data Security module of the Forcepoint Security Manager.

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

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

1) From the DLP Module of the Forcepoint Security Manager, select **Settings > Deployment > System Modules**.

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.

6) Click **Deploy** to deploy your settings.

Important

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

Verifying web and data protection linking

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

1) Log onto the DLP Module of the Forcepoint Security Manager.

2) Select **Settings > General > Linking Service**.

3) Verify settings and test the connection.
Select **Help** > **Explain This Page** for detailed information about the settings on this screen.

4) Click **OK** to save any changes.

5) Click **Deploy** to deploy your settings.

Related concepts

Initial configuration for web protection solutions on page 331

Related reference

Forcepoint DLP ports on page 362

Forcepoint DLP initial configuration

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Note

The Data Security module of the Security Manager may not be available immediately after installation. It takes a few minutes to initialize the system after it is first installed. To complete your Forcepoint DLP installation, log on to the Data Security module of the Security Manager and click **Deploy**.

See the Forcepoint DLP Getting Started Guide for initial setup instructions for newly installed agents, modules, and components.

In addition, the Initial Setup section of the Forcepoint DLP Administrator Help has information about:

- 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

Forcepoint Email Security initial configuration

Applies to:
■ Forcepoint Email Security, v8.5.x

The first time you access the Email Security module of Forcepoint Security 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 Forcepoint Email Security Administrator Help for more information about the wizard.

Important

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

See the Getting Started section in the Forcepoint Email Security 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
- Forcepoint DLP registration, to allow the use of email data loss prevention (DLP) policy options
- Forcepoint URL database download scheduling, to manage message analysis database updates

For help with the following Email Security module settings, see the Configuring System Settings section in the Administrator Help:

- Delegated administrator management, to modify administrator roles established in the Forcepoint Security 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 Security 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

If your subscription includes the Forcepoint Email Security Hybrid Module, you need to register with the email hybrid service. See the Registering for the hybrid service topic in the Forcepoint Email Security 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 the Administrator Help for details.

Content Gateway initial configuration

Applies to:
■ Forcepoint Web Security, v8.5.x

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 Security module of the Forcepoint Security Manager.

1) Log onto the Content Gateway manager and run a basic test (Getting Started)

2) If there are multiple instances of Content Gateway, consider configuring a managed cluster.

3) Configure protocols to proxy in addition to HTTP: HTTPS (SSL support), FTP

4) Complete your explicit or transparent proxy deployment
   - *Content Gateway explicit and transparent proxy deployments*
   - In Content Gateway Manager Help: Explicit proxy, Transparent proxy

5) If proxy user authentication will be used, configure user authentication. Alternatively, configure Other methods of user identification using the Other methods of user identification section in *Content Gateway deployment issues*.

6) Configure the real-time Scanning Options in the Forcepoint Security Manager

7) If you enabled content caching during installation, configure content caching.

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

- When HTTPS (SSL support) is used, configure categories, clients, and destination servers for SSL decryption bypass in the Forcepoint Security Manager.
- 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
    ```

Related reference

Content Gateway explicit and transparent proxy deployments on page 88
Content Gateway deployment issues on page 84

Network Agent and stealth mode NICs

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Your web protection 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 other web protection components for policy enforcement and logging.

During installation, stealth-mode interfaces do not display as a choice for inter- component communication. 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>**.

Chapter 29

Adding, Modifying, or Removing Components

Contents

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, 8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint Appliances, v8.5.x

The following articles contain instructions for adding, modifying, or removing Forcepoint web, data, and email protection components:

- Adding or modifying Windows components
- Modifying Forcepoint Infrastructure
- Adding web protection components
- Adding or modifying Data Security components, including:
  - Recreating Forcepoint DLP certificates
  - Repairing Forcepoint DLP components
  - Changing the Forcepoint DLP service account
  - Changing the domain of a Forcepoint DLP server
  - Joining a Forcepoint DLP server to a domain
  - Removing Forcepoint DLP components
- Adding email protection components
- Removing components
- Removing Forcepoint Infrastructure
- Removing web protection components

- Removing Content Gateway
- Removing Forcepoint DLP components
- Removing email protection components

Related concepts

Adding or modifying Windows components on page 342
Adding email protection components on page 345
Removing components on page 348
Removing web protection components on page 350

Related tasks

Modifying Forcepoint Infrastructure on page 343
Adding web protection components on page 344
Removing Forcepoint Infrastructure on page 349
Removing Content Gateway on page 357
Removing Forcepoint DLP components on page 358
Removing email protection components on page 359

Adding or modifying Windows components

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

On Windows machines, security components are added or modified using the Forcepoint Security Setup program. When run on a machine that has current-version components installed, the installer displays the **Modify Installation** dashboard.

For each module found on the machine, the Modify Installation dashboard shows Modify and Remove links. (When no components of a particular type are found, an Install link, used to launch a custom installation, is displayed instead.)

Click a **Modify** link to launch the program used to add or modify components of the selected type. See:

- Modifying Forcepoint Infrastructure
- Adding web protection components
- Adding or modifying Data Security components
- Adding email protection components

Related tasks

Modifying Forcepoint Infrastructure on page 343
Adding web protection components on page 344
Removing email protection components on page 359

Modifying Forcepoint Infrastructure

Before you begin

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x

Steps

1) To start the Forcepoint Security Installer:
   - If installation files were saved after the initial installation, use the **Forcepoint Security Setup** link (on the Start screen or in the Start > Forcepoint menu) to start the installer without having to re-extract files.
   - If the installation files were not saved, double-click the installer executable.

2) In Modify Installation dashboard, click the **Modify** link for Forcepoint Infrastructure.

3) On the Welcome screen, click **Modify**.

4) Proceed through the Forcepoint Infrastructure Setup screens. Current settings are shown. If you do not want to make any changes on a screen, simply click **Next**.
   For instructions on a screen see Installing Forcepoint Infrastructure.

5) To restore security data backed up from another machine, use the Restore Data From Backup screen:
   a) Select **Use backup** data.
   b) Use **Browse** to locate the backup files.

Note

If the backup is located on another machine, map a network drive to its location. Otherwise, you will be unable to select it in when you click **Browse**.

c) Click **Next**.

If the following message appears, click **Yes** to proceed:

```
The backup located at <path> is from the same release but from a different
build (n). Proceed?
```

Build differences do not affect restoration of the backup. Click **Yes** to continue with restoring the backup.

6) Click **Finish** at the Installation Complete screen.

7) If you installed the management components on a virtual machine, restart the server.

Related tasks

Installing Forcepoint Infrastructure on page 153

Adding web protection components

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x ■ Forcepoint URL Filtering, v8.5.x

Important

Do not add other web protection components to a Remote Filtering Server machine.

Steps

1) To start the Forcepoint Security Installer:
   - If installation files were saved after the initial installation, use the **Forcepoint Security Setup** link (on the Start screen or in the Start > Forcepoint menu) to start the installer without having to re-extract files.
   - If the installation files were not saved, double-click the installer executable.

2) In Modify Installation dashboard, click the **Modify** link for Web Protection Solutions.

   The web protection component installer is started.

3) On the Add Components screen, select **Install additional components on this machine** and click **Next**.

4) On the Select Components screen, select the components to add and proceed as you would when performing a custom installation of web protection components. See Installing web protection components for instructions.

5) When you are done adding web protection components, you are returned to the Modify Installation dashboard.

Related concepts
Removing web protection components on page 350

Adding email protection components

Applies to:
■ Forcepoint Email Security, v8.5.x

The following email protection components can be added to a Windows machine:

- Email Security module of Forcepoint Security Manager
- Email Log Server

See *Adding the Forcepoint Email Security manager or Email Log Server*.

All other Forcepoint Email Security components run on a Forcepoint appliance.

Related tasks
Adding the Forcepoint Email Security manager or Email Log Server on page 345

Adding the Forcepoint Email Security manager or Email Log Server

Before you begin

Applies to:
■ Forcepoint Email Security, v8.5.x

Steps

1) To start the Forcepoint Security Installer:
   - If installation files were saved after the initial installation, use the **Forcepoint Security Setup** link (on the Start screen or in the Start > Forcepoint menu) to start the installer without having to re-extract files.
   - If the installation files were not saved, double-click the installer executable.

2) In Modify Installation dashboard, click the **Install** link for Forcepoint Email Security.
The Email Protection Solutions Installer starts.

3) On the Introduction screen, click **Next**.

4) Select the **Forcepoint Email Security** option and then click **Next**.

Note

If Forcepoint Infrastructure is currently installed on this machine, email protection components automatically use the database engine and database login credentials entered when Forcepoint Infrastructure was installed. The Email Protection Solutions Installer reads this information from configuration files created by Forcepoint Security Setup.

5) If Forcepoint Infrastructure is not found already installed on this machine, the Email Log Database screen appears. Specify the location of a database engine and how you want to connect to it.

- **Log Database IP Address**: Enter the IP address of the database engine machine. If you want to use a named database instance, enter in the form <*IP address*>\<*instance name*>. Note that the instance must already exist. See your SQL Server documentation for instructions on creating instances.
  If the option to install SQL Server Express is available as part of the Forcepoint Security Installer, and you chose to install it, the Log Database IP address should be that of the Security Manager machine.

  Starting in version 8.5.4, more stringent connection string and certificate requirements are needed for establishing an encrypted connection with a SQL Server. Using an IP address is no longer supported for encrypted connections; you must use a hostname or a fully qualified domain name (FQDN) that matches the Common Name (CN) field on the certificate used by SQL Server, if using an encrypted database connection.
- You may specify whether the connection to the database should be encrypted.
  If you are using an encrypted connection, ensure that you use a hostname or FQDN for your Email Log Database that matches the CN field on the certificate that SQL Server is using.

  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 Forcepoint appliance to the Log Database 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.
  - **Windows authentication**: 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.

6) On the **Email Database File Location** screen, specify where database files should be located and then click **Next**.

This screen appears only if you chose to install the Email Log Server.
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.

7) On the Email System Credentials screen, specify the server name or domain name of the management server, along with the user credentials to be used by Forcepoint Security Manager components when running services. Specify the **User name** and **Password** of the account to be used by the Security Manager.

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

This screen appears only if you chose to install Email Log Server.
A default location for the Log Database is automatically shown. Information about the location of the database engine and connection credentials were entered when Forcepoint Infrastructure was installed on this machine. The Email Protection Solutions Installer reads this information from configuration files created by Forcepoint Security Setup.

It is a best practice to use the default location. 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.

9) On the Email Appliance screen specify the Email appliance to be managed by this installation of the Forcepoint Security Manager and then click **Next**.

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

11) On the Pre-Installation Summary screen, click **Install**.

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

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

Related tasks

Installing with SQL Server on page 172

Removing components

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

On Windows machines, security components are removed using the Forcepoint Security Installer. When run on a machine that has current-version components installed, the installer displays the Modify Installation dashboard.

For each module found (Forcepoint Infrastructure, Web, Data, and Email), the Modify Installation dashboard shows Modify and Remove links. (When no components of a particular type are found, an Install link, used to launch a custom installation, is displayed instead.)

Clicking a **Remove** link starts a separate uninstaller that is used to remove components of each type. See the following sections for instructions:

- Removing Forcepoint Infrastructure
- Removing web protection components
- Removing Forcepoint DLP components
- Removing email protection components

Related concepts

Removing web protection components on page 350

Related tasks

Removing Forcepoint Infrastructure on page 349
Removing Forcepoint DLP components on page 358
Removing email protection components on page 359

Removing Forcepoint Infrastructure

Before you begin

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x

Remove Forcepoint Infrastructure only after removing all Forcepoint Security Manager modules (Web, Data, and Email) from the machine. Although it is possible to remove Forcepoint Infrastructure before removing Forcepoint Security Manager modules, the modules are rendered inoperable.

For instructions on removing Forcepoint Security Manager modules, see:

- Web: Removing web protection components
- Data: Removing Forcepoint DLP components
- Email: Removing email protection components

To remove Forcepoint Infrastructure:

Steps

1) To start the Forcepoint Security Installer:
   - If installation files were saved after the initial installation, use the **Forcepoint Security Setup** link (on the Start screen or in the Start > Forcepoint menu) to start the installer without having to re-extract files.
   - If the installation files were not saved, double-click the installer executable.

2) In Modify Installation dashboard, click the **Remove** link for Forcepoint Infrastructure.

3) At the Forcepoint Infrastructure Uninstall screen, click **Next**.
   The Installation screen appears, showing removal progress.
   A message may appear if you have Forcepoint Security Manager modules installed on the machine.

   Warning

   Removing Forcepoint Infrastructure will render Forcepoint Security Manager modules inoperable.

   Click **Yes** to proceed with removal of Forcepoint Infrastructure. Click **No** to cancel.

4) At the Forcepoint Infrastructure has been uninstalled screen, click **Finish**.
   You are returned to the Modify Installation dashboard.

Related concepts
Removing web protection components on page 350

Related tasks
Removing Forcepoint DLP components on page 358
Removing email protection components on page 359

Removing web protection components

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Both Policy Broker and the Policy Server instance associated with each set of components you want to remove must be running when you start the removal process.

- Policy Broker may be running on a different machine from the applicable Policy Server instance.
- Policy Broker and Policy Server may be on different machines from the component being removed.
- If you have Forcepoint appliances, Policy Broker and Policy Server run on the **full policy source** appliance. Policy Server also runs on **user directory and filtering** appliances.

Web protection components should be removed in a particular order because of certain dependencies (see Removal order of web protection components). If you are removing all components on a machine, make sure you move any custom files you want preserved beforehand (see Preserving custom data before removing a web protection component). Also, if your web protection deployment is integrated with another product, see the following for any integration-specific requirements:

- Integrating Forcepoint URL Filtering with Cisco
- Integrating Forcepoint URL Filtering with Citrix
- Integrating Forcepoint URL Filtering with TMG
- Installing for Universal Integrations

Removal instructions are slightly different depending on the operating system:

- To remove web protection components (Windows)
- To remove web protection components (Linux)

To remove web protection components (Windows)

Note

After uninstalling components, you may be prompted to restart the machine.

1) Before removing components:

- Use the Backup Utility to make a backup of web protection configuration and initialization files. See the Backup and Restore FAQ for instructions.
- If you are removing components from a Windows Server 2008 machine, log in as the built-in administrator, or run the installer with elevated (full administrator) privileges.

2) Log on with **local** administrator privileges.

3) Close all applications **except** your web protection software (see the next step) and stop any antivirus software.

4) Make sure your web protection software is running. The uninstaller looks for Policy Server during the removal process.

Warning

Do not remove web protection components without the associated Policy Server running. Policy Server keeps track of configuration and component locations. If Policy Server is not running, files for the selected components are still removed, but configuration information is not updated for those components. Problems could occur later if you attempt to reinstall these components.

5) Start the Forcepoint Security Installer.

- If you chose to keep installation files after the initial installation, go to the Windows Start screen, or **Start > All Programs > Forcepoint** and select **Forcepoint Security Setup** to start the installer without having to re-extract files.
- Otherwise, double-click the installer executable.

6) In **Modify Installation** dashboard, click the **Remove** link for Web Protection Solutions.

7) At the **Remove Components** screen, select the components you want to remove and then click **Next**.

Warning

- When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.
- Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining web protection components and requires the reinstallation of those components.

Note

If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, the uninstaller cannot stop Network Agent and an error message is displayed.

If Policy Server is not running, a message indicates removing web protection components may require communication with Policy Server.

a) Cancel the uninstaller.

b) Restart the **Websense Policy Server** service from the Windows Services tool.

c) Start the installer again and follow removal instructions again (Step 5).

8) At the **Summary** screen, click **Next**.
The **Installation** screen appears, showing removal progress.

If you are uninstalling Network Agent after Policy Server has already been removed, expect the process to take several minutes. Network Agent is successfully uninstalled, although no progress notification is displayed.

9) At the **Uninstall Complete** screen, click **Uninstall**.

Important

Do not click **Cancel** in the Uninstall Complete screen. This renders the uninstallation incomplete. Be sure to click **Uninstall**.

10) You are returned to the **Modify Installation** dashboard.

11) If you stopped your antivirus software, restart it.

12) If you remove an integration plug-in, you may need to restart the integration product. See:
- Integrating Forcepoint URL Filtering with Cisco
- Integrating Forcepoint URL Filtering with Citrix
- Integrating Forcepoint URL Filtering with TMG
- Installing for Universal Integrations

To remove web protection components (Linux)

Note

Before removing components, use the Backup Utility to back up web protection configuration and initialization files. See the Backup and Restore FAQ for instructions.

1) Log on as **root**.

2) Close all applications **except** your web protection software and stop any antivirus software.

3) Make sure your web protection software is running. The uninstaller looks for Policy Server during the removal process.

Warning

- When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.
- Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining web protection components and requires the reinstallation of those components.

Note

If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, the uninstaller cannot stop Network Agent and an error message is displayed.

4) Run the uninstall program from the product installation directory (**/opt/Websense** by default):
```
./uninstall.sh
```
A graphical version is available on English versions of Linux. To run it, enter:
```
./uninstall.sh -g
```
The installer detects the installed web protection components and lists them.

Warning

- When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.
- Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining components and requires the reinstallation of those components.

5) Select the components you want to remove, and choose **Next**.

Note

If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, Setup cannot stop Network Agent and an error message is displayed.

If Policy Server is not running, a message tells you that removing components may require communication with Policy Server

a) Cancel the uninstaller.

b) Open a command shell and go to the **Websense** directory (/opt/Websense, by default).

c) Enter the following command to start web protection services:
```
./WebsenseAdmin start
```

d) Restart this process at Step 4.

6) A list shows the components selected for removal. Choose **Next**.
If you are uninstalling Network Agent on a remote machine after removing Policy Server, expect the process to take several minutes. Network Agent is successfully uninstalled, although no progress notification is displayed.

7) A completion message indicates that components have been removed. Exit the installer.

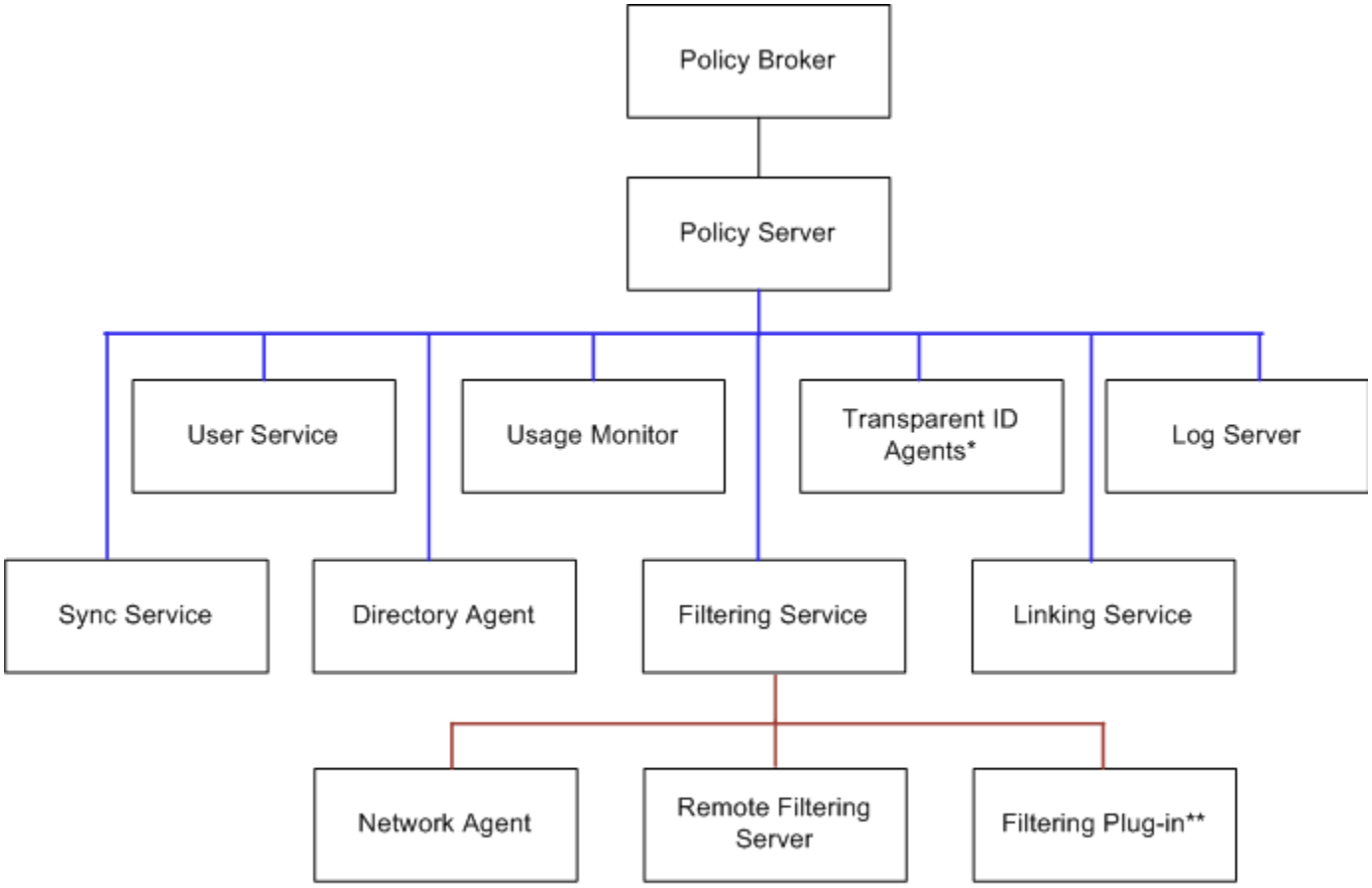
8) If you stopped your antivirus software, restart it.

9) If you remove an integration plug-in, you may need to restart the integration product. See:

- Integrating Forcepoint URL Filtering with Cisco
- Integrating Forcepoint URL Filtering with Citrix
- Integrating Forcepoint URL Filtering with TMG
- Installing for Universal Integrations

Removal order of web protection components

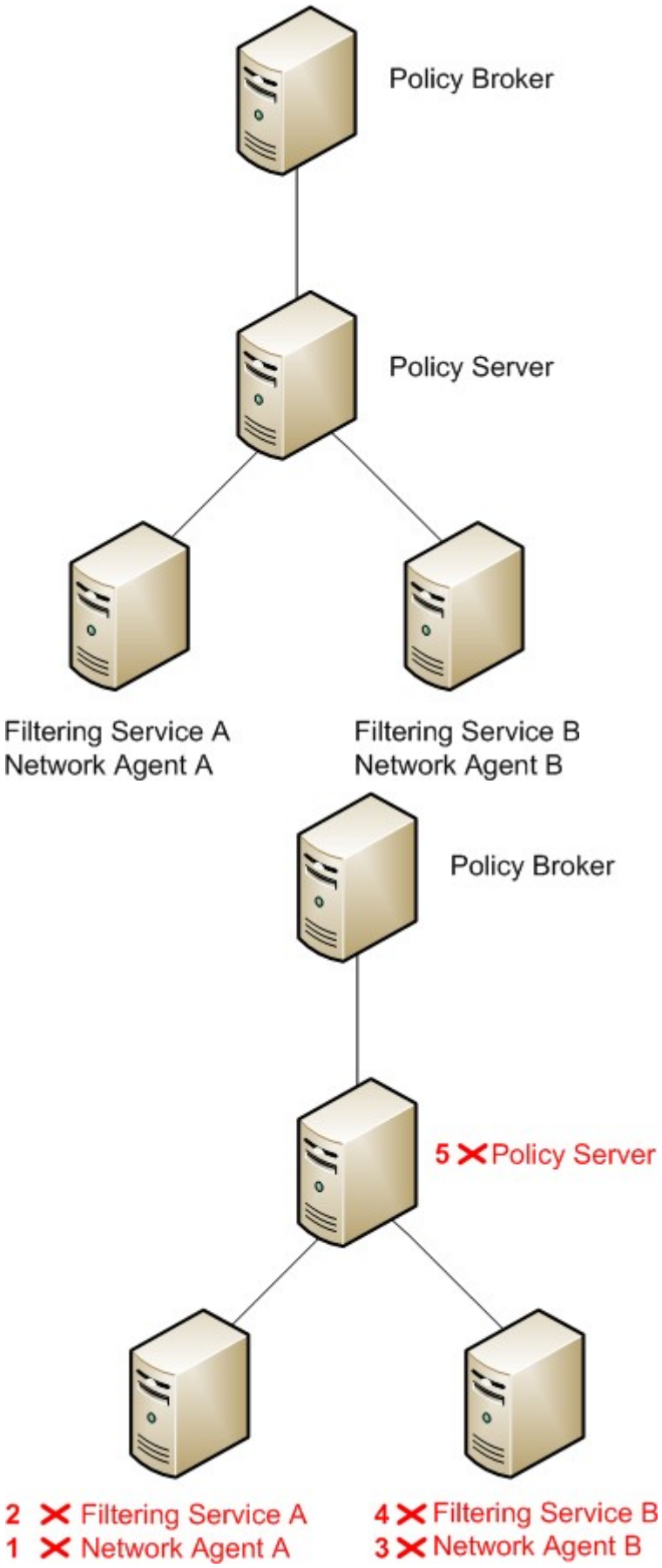
When removing a particular web protection component, it is important to remove any dependent components first. Component dependencies are shown in the following diagram (note: not all web protection components are included; only those with removal dependencies are shown).



* DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
** Microsoft ISAPI Filter or Citrix Integration Service

The dependency hierarchy goes from top-down, components below depend on components above. For example, if you want to remove Filtering Service, any associated Network Agent, Remote Filtering Server, and Filtering plug-in instances must be removed first. Likewise, to remove Policy Server, you must first remove any instances of the components below it in the diagram (which is everything except Policy Broker).

It is important to note that these dependencies apply to distributed components as well. The uninstaller will notify you of dependent components on the same machine. However, it cannot notify you of dependent components on other machines. You must be sure to remove any dependent components on other machines before removing a component on this machine. For example, to remove the Policy Server instance shown below (left-side illustration), you must first remove Network Agent and then Filtering Service on the two machines dependent on the Policy Server. The numbers in the right-side illustration indicate the proper order of removal.


Policy Broker
Policy Server
Filtering Service A
Network Agent A
Filtering Service B
Network Agent B
Policy Broker
5 Policy Server
2 Filtering Service A
1 Network Agent A
4 Filtering Service B
3 Network Agent B

Notice that each Network Agent is removed before its associated Filtering Service, which is required by the component dependencies. Also, it does not matter which Filtering Service and Network Agent pair is removed before the other—just both pairs must be removed prior to removing the Policy Server.

Preserving custom data before removing a web protection component

If you have data or files you created yourself in the web protection installation directory (default: C:\Program Files *or* Program Files (x86)\Websense\Web Security in Windows; /opt/Websense/ in Linux) or its sub-directories, copy them to another location before removing all web protection components. The uninstallation process may remove these files.

Note

If you have saved reports you want to retain after uninstalling all components, copy them from the **ReportingOutput** directory (under the Websense\Web Security directory). The report files are of the following types: *.pdf, *.xls, or *.zip (for HTML files).

Files of the following types are not removed by the uninstaller if they are located in the Websense\Web Security directory itself:

- *.zip
- *.mdb
- *.mdf
- *.ndf
- *.ldf
- *.bak

The above file types are protected from removal only in the Websense\Web Security directory itself. They may be removed if they reside in a subdirectory, unless either of the following is true:

- They are in the **backup** subdirectory (C:\Program Files *or* Program Files (x86)\Websense\Web Security \backup in Windows; /opt/Websense/backup/ in Linux).
- They are Log Database files.

Related concepts

Integrating Forcepoint URL Filtering with Cisco on page 183
Integrating Forcepoint URL Filtering with Citrix on page 205
Integrating Forcepoint URL Filtering with TMG on page 221
Installing for Universal Integrations on page 247

Removing Content Gateway

Before you begin

Applies to:
■ Forcepoint Web Security, v8.5.x

To uninstall Content Gateway, use the uninstall script (/root/WCG/Current/ wcg_uninstall.sh).

Steps

1) Make sure you have root permissions.
   ```
   su root
   ```

2) Change to the /root/WCG/Current directory:
   ```
   cd /root/WCG/Current
   ```

3) Run the uninstaller:
   ```
   ./wcg_uninstall.sh
   ```

4) Confirm that you want to uninstall the product. You must enter **y** or **n**.
   ```
   Are you sure you want to remove Content Gateway [y/n]?
   ```

5) When a message indicates that Content Gateway has been uninstalled, reboot the system.

Removing Forcepoint DLP components

Before you begin

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Forcepoint DLP components can only be removed altogether. You cannot select particular components on a machine for removal.

Warning

Forcepoint Email Security requires Forcepoint DLP to be installed. If you are using Forcepoint Email Security, do not uninstall Forcepoint Email Security or you will lose all data loss prevention capabilities.

For instructions on removing Forcepoint DLP Endpoint, see the Installation and Deployment Guide for Forcepoint F1E Solutions.

To remove Forcepoint DLP components:

Steps

1) Start the Forcepoint Security Installer.
   - If you chose to keep installation files after the initial installation, go to the Windows Start screen, or **Start > All Programs > Forcepoint** and select **Forcepoint Security Setup** to start the installer without having to re-extract files.
   - Otherwise, double-click the installer executable.
2) In **Modify Installation** dashboard, click the **Modify** link for Forcepoint DLP.
3) At the **Welcome** screen, click **Remove**.
4) At the **Forcepoint DLP Uninstall** screen, click **Uninstall**.

   Important

   This removes all Forcepoint DLP components from this machine.

   The **Installation** screen appears, showing removal progress.
5) At the **Uninstallation Complete** screen, click **Finish**.
6) You are returned to the **Modify Installation** dashboard.

Removing email protection components

Before you begin

Applies to:
■ Forcepoint Email Security, v8.5.x

Steps

1) If the Forcepoint Security Installer is not yet running:
   - If installation files were saved after the initial installation, use the **Forcepoint Security Setup** link (on the Start screen or in the Start > Forcepoint menu) to start the installer without having to re-extract files.
   - If the installation files were not saved, double-click the installer executable.

2) In **Modify Installation** dashboard, click the **Remove** link for Email Protection Solutions.
   The Email Protection Solutions uninstaller starts.

3) On the **Uninstall** screen, click **Next**.

4) On the **Remove Components** screen, choose whether you want to uninstall all or specific email protection system components and then click **Next**.

5) The **Summary** screen verifies your uninstall selections. If the summary is not correct, click **Back** and change your selections. If the summary is correct, click **Uninstall**.

6) The **Uninstall Email Protection Solutions** screen appears, showing removal progress.
   The following message may appear:
   The Email Log Database already exists. Do you want to remove it?

   Clicking **Yes** removes the database. Clicking **No** keeps the database and proceeds with removing components.

   Forcepoint Email Security only:
   - You will lose current email log data if you remove the database. If you want to keep this data, back up the esglogdb7x and esglogdb7x_n databases. See your SQL Server documentation for backup instructions.
   - If you remove the database, any currently quarantined email will no longer be accessible. If you plan to reinstall the Email Security module of Forcepoint Security Manager elsewhere to use with the same email appliance and want access to currently quarantined email after reinstalling, do not remove the database.

7) On the **Components Removed** screen, click **Done**.

8) You are prompted to restart the machine. A restart is required to complete the uninstall process.

Chapter 30

Deployment Quick Reference

Contents

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Use this Deployment and Installation Center Quick Reference to find information about:

- *Default ports for on-premises Forcepoint security solutions*
- *Excluding Forcepoint files from antivirus scans*

Related reference

Default ports for on-premises Forcepoint security solutions on page 361
Excluding Forcepoint files from antivirus scans on page 370

Default ports for on-premises Forcepoint security solutions

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

The attached Excel spreadsheet lists the default port numbers used by on-premises web, data, and email protection components. It includes the ports for both appliance- based and software-based deployments.

It is important to note that these are default port numbers; some of them may have been changed during installation for your particular deployment.

For web protection solutions, to change ports for most services, use the initialization (INI) file for the component. Given dependencies between components, the change may need to be made in multiple files.

- Instructions for changing the Policy Server and Policy Broker ports can be found in the Server Administration section of the Forcepoint Web Security Administrator Help.
- Use the Web Security module of the Forcepoint Security Manager to configure the Log Server port, and to configure communication with Log Server if the port has changed.
- Use the Web Security module of the Security Manager to change port information for transparent identification agents (DC Agent, Logon Agent, RADIUS Agent, or eDirectory Agent).

If instructions for the component that you need to reconfigure are not available, contact Forcepoint Technical Support for assistance.

Port information for data and email protection solutions is also available in other formats. See:

- *Forcepoint DLP ports*
- *Forcepoint Email Security ports*

Related reference
Forcepoint DLP ports on page 362
Forcepoint Email Security ports on page 368

Forcepoint DLP ports

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The most robust and effective implementation of Forcepoint DLP depends on certain ports being open to support the mechanics of the software. The ports for Forcepoint DLP components are 17500–17515 by default. These ports must be left open for all Forcepoint DLP software and hardware configurations.

If you have a security policy in place, exclude these ports from that policy so that Forcepoint DLP can operate properly. If you do not, the policy you have in place may disrupt Forcepoint DLP functionality.

The tables in the rest of this section list the inbound and outbound ports required for each Forcepoint DLP component.

You can lock down or “harden” your security systems once these ports are open.

Important

Forcepoint DLP agents and machines with a policy engine, such as a Forcepoint DLP Server or Content Gateway machine, must have direct connection to the Forcepoint management server. When deployed in a DMZ or behind a firewall, the relevant ports must be allowed.

Human interface device (administrator client)

Outbound		
To	**Port**	**Purpose**
Data Security module	9443	User interface browsing

Forcepoint DLP Endpoint client

Outbound		
To	**Port**	**Purpose**
Forcepoint DLP Server	443	Connect to endpoint server (secure connection, default)

Forcepoint DLP Endpoint server

Outbound		
To	**Port**	**Purpose**
Forcepoint management server	443	Retrieve fingerprints and natural language processing scripts
Forcepoint management server	17443	Incidents

Inbound		
From	**Port**	**Purpose**
Forcepoint management server	443	Retrieve fingerprints and natural language processing scripts
Forcepoint DLP Endpoint Client	443	Endpoint communication
Supplemental Forcepoint DLP Server	17444	Retrieve fingerprints and natural language processing scripts

Service	Process name	Listening address/port
Endpoint Server (Forcepoint Data Security Web Server)	EPServer. exe	TCP 0.0.0.0:443 TCP 0.0.0.0:17509

Crawler agent (discovery and fingerprinting)

Outbound		
To	**Port**	**Purpose**
Forcepoint management server	443	Secure communication
Forcepoint DLP Server	17500-17515	Range of ports for communication with Forcepoint agents and machines
Internet	443	Connectivity to cloud applications

Inbound		
From	**Port**	**Purpose**
Forcepoint management server	9797	Crawler listening The port is used only for the standalone crawler agent.

Forcepoint management server

Outbound		
To	**Port**	**Purpose**
Forcepoint DLP Server, Protector, Web Content Gateway, Forcepoint Email Security	17500-17515 and 17700-17715	Range of ports for communication with Forcepoint agents and machines. The second range is used when Web Content Gateway and Forcepoint Email Security are both installed.
Forcepoint DLP Server	443	Used to communicate with Data Protection Service and Microsoft Information Protection.
Forcepoint DLP Server	25	Used for outgoing emails from the DLP Manager to DLP administrators.

Inbound		
From	**Port**	**Purpose**
Forcepoint DLP Server, Protector, Web Content Gateway	17443	Incidents, endpoint status, forensics. This port should be left open. It is not configurable.
Security Manager	17447	Processing batch jobs such as scheduled tasks
Security Manager	17446	Translating messages into sender/ receiver protocols
Crawler	17514	Enabling emailed reports for discovery tasks
Forcepoint DLP Server, Endpoints, Protector, Web Content Gateway	443	Secure communication

Inbound		
From	**Port**	**Purpose**
Forcepoint DLP Server, Protector, Web Content Gateway, Forcepoint Email Security	17500-17515 and 17700-17715	Range of ports for communication with Forcepoint agents and machines. The second range is used when Web Content Gateway and Forcepoint Email Security are both installed.
Forcepoint DLP Server, Protector, Web Content Gateway	9443	Access user interface This port should be left open. It is not configurable.
Forcepoint DLP Server	993, 995	Used to retrieve emails sent to the DLP Manager.

Service	Process name	Listening address/port
DSS Manager (Forcepoint Data Security Manager)	DSSManager.exe	TCP 0.0.0.0:17443
MGMTD (Forcepoint Management Server)	mgmtd.exe	TCP 0.0.0.0:17500
Policy Engine	PolicyEngine.exe	TCP 0.0.0.0:17503
PAFPREP (Forcepoint Data Fingerprint Database)	PAFPREP.exe	TCP 0.0.0.0:17505 TCP 0.0.0.0:17506
DSSMessageBroker (Forcepoint Data Security Message Broker)	DSSMessage Broker.exe	TCP 0.0.0.0:17513 TCP 0.0.0.0:17514
EIPManagerProxy (Forcepoint Security Manager Web Server)	EIPManager Proxy.exe	TCP 0.0.0.0:9443

Supplemental Forcepoint DLP server

Outbound		
To	**Port**	**Purpose**
Forcepoint management server	17443	Incidents
Forcepoint management server	17500-17515	Range of ports for communication with Forcepoint agents and machines. The range is needed for load balancing.

Inbound		
From	**Port**	**Purpose**
Forcepoint management server	17500-17515	Range of ports for communication with Forcepoint agents and machines.
Forcepoint management server	514	Syslog

Service	Process name	Listening address/port
OCRServer (Forcepoint Data OCR Engine)	OCRServ er.exe	TCP 0.0.0.0:17512

Web Content Gateway

Outbound		
To	**Port**	**Purpose**
Forcepoint management server	443	Fingerprint sync
Forcepoint management server	17443	Forensics, incidents, mobile status
Web protection components	56992	Linking Service
Forcepoint DLP Server	17500-17515	Consecutive ports that allow communication with Forcepoint agents and machines. The range is needed for load balancing.

Forcepoint Email Security

The following ports are used on the appliance for outbound connections to Forcepoint DLP.

Outbound		
To	**Port**	**Purpose**
Forcepoint management server	17500-17515 and 17700-17715	Settings deployment, fingerprint repository The second range is used when Web Content Gateway and Forcepoint Email Security are both installed.
Forcepoint management server	17443	Forensics, incidents
Forcepoint management server	17444	Used to pull configuration settings
Forcepoint management server	443	Fingerprint repository sync

Protector

Outbound		
To	**Port**	**Purpose**
Forcepoint DLP Server	17500-17515	Consecutive ports that allow communication with Forcepoint agents and machines.
Forcepoint management server	443	Fingerprint sync
Forcepoint management server	17443	Syslog, forensics, incidents, mobile status
Next hop MTA	25	SMTP (explicit MTA)
Forcepoint Web Security	56992	Linking Service
Other	UDP 123	Inbound/outbound NTPD (available on the appliance yet disabled by default)

Inbound		
From	**Port**	**Purpose**
Forcepoint management server	17500-17515	Consecutive ports that allow communication with Forcepoint agents and machines.
Anywhere (including Security Manager)	22	SSH access
Forcepoint DLP Server	17500-17515	Consecutive ports that allow communication with Forcepoint agents and machines. The range is needed for load balancing.
Explicit MTA	25	SMTP

ICAP client

Outbound		
To	**Port**	**Purpose**
Protector	1344	Receiving ICAP traffic

Forcepoint Behavioral Analytics

Outbound		
To	**Port**	**Purpose**
FBA	9093	Send DLP entities, events and incidents to FBA

Inbound		
From	**Port**	**Purpose**
FBA	9093	Fetch Risk Level updates from FBA

Analytics engine

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

Outbound		
To	**Port**	**Purpose**
Forcepoint management server	17443	Syslog, forensics, incidents, analytics engine status
Forcepoint management server	17500-17515	Range of ports for communication with Forcepoint agents and machines.
Forcepoint management server (local database) or remote SQL Server	1433	Database connection

Inbound		
From	**Port**	**Purpose**
Forcepoint management server	17500-17515	Range of ports for communication with Forcepoint agents and machines.

Forcepoint Email Security ports

Applies to:
■ Forcepoint Email Security, v8.5.x

The following ports are used on the Forcepoint Email Security appliance.

If you are running Forcepoint Email Security in Azure, you must use the C interface IP address. Ensure that all ports are opened for the C interface.

Note

If any of the ports in this document are dropped, blocked, or decrypted (including SSL Decryption or Deep Packet Inspection) by any firewall or intrusion detection/ prevention device, your Email Security environment may not function properly.

Interface	Port	Direction	Description
C/P1/P2	9449	Inbound	Personal Email Manager load balancing, Secure Message Delivery end-user portal
C/P1/P2 (C recommended)	6671	Inbound	SSL proxy to be accessed by the Email Security module of the Security Manager
C/P1/P2	6643	Inbound	Personal Email Manager user interface
P1/P2	17700*	Inbound	Email data loss prevention system health and log data
P1/P2	25	Inbound	SMTP
P1/P2	2525	Inbound	Receipt of messages from data loss prevention function for encryption

* The port range 17700-17714 must be open for communications with Forcepoint Email Security.

The following ports are used on the appliance for outbound connections to Forcepoint DLP.

Interface	Port	Direction	Description
C/P1/P2	17500- 17515*	Outbound	Fingerprint status
C/P1/P2	17500- 17515*	Outbound	Fingerprint repository
C/P1/P2	17443	Outbound	Registration, syslog, forensics, incidents
C/P1/P2	17444	Outbound	Fingerprint download
C/P1/P2	17500- 17515*	Outbound	Message analysis
C/P1/P2	80	Outbound	Fingerprint repository synchronization

* This is the default range. The starting location of the range (17500) is configurable.

The following ports are used by Forcepoint Email Security off-appliance components.

Interface	Port	Direction	Description
C/P1/P2	9443	Inbound	Email Security module of the Security Manager
P1/P2	50800	Inbound	Email Log Server
P1/P2	50900	Inbound	Email Log Server backup alerts port
P1/P2	1433 1434	Outbound	Email Log Database default instance
P1/P2	443	Outbound	Email hybrid service
P1/P2	15868	Outbound	Filtering Service (a web protection component)
P1/P2	56992	Outbound	Linking Service (a web protection component)
P1/P2	389 636	Outbound	LDAP server
P1/P2	80	Outbound	Database download server
P1/P2	53	Outbound	DNS server
C	162	Outbound	SNMP Trap server

Excluding Forcepoint files from antivirus scans

Applies to:
■ Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x ■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0 ■ Forcepoint Email Security, v8.5.x ■ Forcepoint appliances, v8.5.x

Antivirus scanning can degrade the performance of Forcepoint security components. This article lists folders and files that should be excluded from antivirus scans.

Please note:

- Forcepoint is not aware of a risk in excluding the files or folders that are mentioned in this section from your antivirus scans. However, it is possible that your system would be safer if you did not exclude them.
- When you scan these files, performance and operating system reliability problems may occur because of file locking.
- Do not exclude any files based on the filename extension. For example, do not exclude all files that have a .dit extension.

- All the files and folders that are described in this section are protected by default permissions to allow only SYSTEM and administrator access, and they contain only operating system components. Excluding an entire folder maybe simpler but may not provide as much protection as excluding specific files based on file names.

Refer to your antivirus vendor's documentation for instructions on excluding files from scans.

Note

During installation of Forcepoint products, disable antivirus software altogether. After installation, be sure to re-enable antivirus software.

Disabling antivirus for web protection solutions

It is a best practice to exclude the installation directory (includes subdirectories) from antivirus scans. By default this directory is:

- Windows (*Forcepoint management server*):
  `*:\Program Files (x86)\Websense`
- Windows (*all others*):
  `*:\Program Files\Websense`
- Linux:
  `/opt/Websense/`

Disabling antivirus for Forcepoint DLP

Management servers

It is a best practice to exclude the following (includes subdirectories) from antivirus scans.

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

Non-management servers

On non-management servers, such as Forcepoint DLP standalone agents, exclude the following directories from antivirus scanning:

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

Windows endpoints

The following directories should be excluded from the antivirus software that is deployed to Windows-based endpoint machines:

- C:\Program Files\Websense\Websense Endpoint
- Custom folder location defined by the customer Also exclude the following:

Also exclude the following:

- **Processes**
  Forcepoint DLP Endpoint and Forcepoint Web Security Endpoint:
  - ..\Websense\Websense Endpoint\wepsvc.exe
  - ..\Websense\Websense Endpoint\dserui.exe

  Forcepoint DLP Endpoint only:
  - ..\Websense\Websense Endpoint\EndpointClassifier.exe
  - ..\Websense\Websense Endpoint\FilterSDK\kvoop.exe

  Forcepoint F1E only:
  - ..\Websense\Websense Endpoint\f1eui.exe
  - ..\Websense\Websense Endpoint\fppsvc.exe

  Forcepoint Web Security Endpoint only:
  - ..\Websense\Websense Endpoint\tsui.exe (Forcepoint Web Security Direct Connect Endpoint UI process)
  - ..\Websense\Websense Endpoint\proxyui.exe (Forcepoint Web Security Proxy Connect Endpoint UI process)
  - ..\Websense\Websense Endpoint\rfui.exe (Forcepoint Remote Filtering Client UI process)
  - ..\Websense\Websense Endpoint\WEPDiag.exe (Diagnostics tool process.This process only runs on demand. It does not run continuously like the other processes.)

  Forcepoint CASB Endpoint only:
  - ..\Websense\Websense Endpoint\SkyfenceSecurityService\certutil.exe
  - ..\Websense\Websense Endpoint\SkyfenceSecurityService\RefreshSettings.exe
  - ..\Websense\Websense Endpoint\SkyfenceSecurityService\sfage.exe
  - ..\Websense\Websense Endpoint\SkyfenceSecurityService\sfsrv.exe
- **DLL files**
  - C:\Windows\System32\QIPCAP.dll
  - C:\Windows\System32\QIPCAP64.dll
  - C:\Windows\System32\QIPOverlay.dll
- **SYS files**
  - C:\Windows\System32\drivers\cwnep.sys
  - C:\Windows\System32\drivers\FpFile.sys (Forcepoint F1E only)
  - C:\Windows\System32\drivers\FpProcess.sys (Forcepoint F1E only)
  - C:\Windows\System32\drivers\qip.sys
  - C:\Windows\System32\drivers\qiptdi.sys

- C:\Windows\System32\drivers\rnetcore.sys
- C:\Windows\System32\drivers\WNetCore.sys
- C:\Windows\System32\drivers\WFPRedir.sys
- C:\Windows\System32\drivers\WsNetFlt.sys
- C:\Windows\System32\drivers\WsOMFlt.sys
- C:\Windows\System32\drivers\WsWfpRF.sys

Mac endpoints

The following directories should be excluded from the antivirus software that is deployed to Mac-based endpoint machines:

- /Library/Application Support/Websense Endpoint
- /Library/Mail/Bundles/DataSecurityPlugin.mailbundle
- /Applications/Forcepoint DLP Endpoint.app
- /Applications/Forcepoint DC Endpoint.app (if Direct Connect Endpoint is installed)
- /Applications/Forcepoint PC Endpoint.app (if Proxy Connect Endpoint is installed)
- /Applications/Forcepoint Decryption Utility.app

Also exclude the following:

- Libraries
  - /usr/local/lib/libwep
  - /usr/local/lib/libwep_airdrop.dylib
  - /usr/local/lib/libwep_burn.dylib
  - /usr/local/lib/libwep_cbcarbon.dylib
  - /usr/local/lib/libwep_cbcocoa.dylib
  - /usr/local/lib/libwep_dutil.dylib
  - /usr/local/lib/libwep_ff.dylib
  - /usr/local/lib/libwep_hook.dylib
  - /usr/local/lib/libwep_icloud.dylib
  - /usr/local/lib/libwep_mail.dylib
  - /usr/local/lib/libwep_outlook.dylib
  - /usr/local/lib/libwep_post.dylib
  - /usr/local/lib/libwep_printer.dylib
  - /usr/local/lib/libwep_screen.dylib
- Utility tool
  - /usr/local/sbin/wepsvc

Disabling antivirus for Forcepoint Email Security

It is a best practice to exclude the installation folder (includes subfolders), by default:

```
*:\Program Files\Websense
```

or

```
*:\Program Files (x86)\Websense
```

Also exclude any Forcepoint DLP folders that apply (see Disabling antivirus for Forcepoint DLP).

Chapter 31

Component Reference

Contents

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

For information about web protection components, see *Deploying core web protection components*.

Forcepoint Security Manager components

- *Forcepoint management server*
- *SQL Server Express*

Forcepoint DLP components

- *Content Gateway*
- *Forcepoint DLP Cloud Applications*
- *Protector*
- *Mobile agent*
- *Forcepoint DLP Endpoint*
- *Integration agent*
- *Crawler*

Email protection components

- *The Email Security module*
- *Email Log Server*

Related concepts

Forcepoint management server on page 376
SQL Server Express on page 377
Content Gateway on page 378
Forcepoint DLP Cloud Applications on page 378
Protector on page 378
Mobile agent on page 379
Forcepoint DLP Endpoint on page 379
Integration agent on page 379
Crawler on page 380
The Email Security module on page 380
Email Log Server on page 381

Related reference

Deploying core web protection components on page 36

Forcepoint management server

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

The Forcepoint management server is a Windows machine that hosts core management components for all on-premises and hybrid Forcepoint security solutions. This machine hosts the Forcepoint Security Manager (Security Manager), which includes:

- The Forcepoint Infrastructure that unites all management components, including a settings database that holds administrator account information and other data shared by all management components.
  The Forcepoint Infrastructure includes common user interface, logging, and reporting components required by the Security Manager modules (Web Security, Data Security, and Email Security). It also maintains an internal database of management infrastructure settings.

  The Forcepoint Infrastructure is not intended to be installed by itself on a machine. It is installed with at least one of the management modules mentioned below.

  The Forcepoint Infrastructure may optionally include SQL Server Express, which can be used in test deployments or very small networks for Forcepoint logging data.
- One or more management modules, used to access configuration, policy management, and reporting tools for a Forcepoint security solution. Available modules include:

- The Web Security module
- The Data Security module
- *The Email Security module*

Although additional components may also reside on the management server, avoid placing the web protection Filtering Service or Network Agent components on the management server machine.

The Security Manager may also be configured to connect to external management consoles, including the Content Gateway manager.

Optionally, in evaluation deployments or very small networks, SQL Server Express may be installed on the management server to host the reporting databases.

Related concepts
The Email Security module on page 380

SQL Server Express

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

SQL Server Express is a free data management system. In very small deployments, it can be used to store Forcepoint reporting data.

- Due to performance limitations built in by Microsoft, SQL Server Express is not suitable for all organizations; see Administering Forcepoint Databases for more information.
- For other supported versions of SQL Server, see *System requirements for this version*.

SQL Server Express is recommended to be installed on the *Forcepoint management server*.

When available, only use the Forcepoint Security Installer to install SQL Server Express for use with Forcepoint solutions.

Note

- Forcepoint has removed the ability to install SQL Server Express as an option for new deployments of Forcepoint Security Manager. This change was made via a revised version of Forcepoint Security Installer introduced in July 2019, which can be found on the Downloads page.
- The change was required to reduce the risk of deploying SQL Server Express without the latest security updates. Forcepoint Security Manager still supports and will work with the latest version of SQL Server Express. You may use SQL Server Express for small deployments, but it must be installed independently.

Related concepts
Forcepoint management server on page 376

Related reference
System requirements for this version on page 9

Content Gateway

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Content Gateway is a web proxy and cache that analyzes HTTP(S) requests in real time.

- In Forcepoint Web Security deployments, Content Gateway passes traffic to Filtering Service for policy enforcement. The Content Gateway manager—a browser-based management console—runs on the Content Gateway machine, but can be accessed from within the Web Security module of the Security Manager.
- In Forcepoint DLP Network deployments, the Web Content Gateway module provides DLP policy enforcement for the web channel, including decryption of SSL traffic. This core Forcepoint DLP component permits the use of custom policies, fingerprinting, and more. It is available only as a soft appliance.

Forcepoint DLP Cloud Applications

Forcepoint DLP Cloud Applications provides cloud activity content inspection for files uploaded into and stored within cloud enterprise services including Microsoft OneDrive, Google Drive, Box, Salesforce, and more. By applying established DLP policies to data stored in enterprise cloud applications, the module is able to audit and prevent the storage of sensitive data that could expose your organization to data loss and compliance infringements. Integration with Forcepoint DLP Cloud Applications can also be used to run discovery on cloud services via CASB.

In addition, Forcepoint DLP Cloud Applications provides the existing cloud discovery functionality provided by Forcepoint Data Discovery (i.e., Box, SharePoint Online, and Exchange Online discovery).

See the Forcepoint DLP Deployment Guide for more information.

Protector

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The protector is an essential component of Forcepoint DLP, providing monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. The protector can be configured to accurately monitor sensitive information-in-transit on any port.

See the Forcepoint DLP Deployment Guide for more information.

Mobile agent

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The mobile agent is a Linux-based appliance that lets you secure the type of email content that is synchronized to users' mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

The mobile agent analyzes content when users synchronize their mobile devices to your organization's Exchange server. If content or data being pushed to their device breaches the organization's mobile DLP policy, it is quarantined or permitted accordingly.

See the Forcepoint DLP Deployment Guide for more information.

Forcepoint DLP Endpoint

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

Forcepoint DLP Endpoint is a comprehensive, secure, and easy-to-use endpoint data loss prevention solution. It monitors real-time traffic and applies customized security policies over application and storage interfaces, as well as for data discovery.

Forcepoint DLP Endpoint allows security administrators to either block or monitor and log files that present a policy breach. It creates forensic monitoring that allows administrators to create policies that don't restrict device usage, but allow full visibility of content traffic.

You can monitor user activity inside endpoint applications, such as the cut, copy, paste, print, and print screen operations. You can also monitor endpoint web activities and Microsoft Outlook email, and know when users are copying data to external drives and endpoint devices.

Working with Forcepoint DLP Endpoint entails configuring endpoint profiles via the Data Security module of the Security Manager. These settings regulate the behavior of the endpoint client software. Forcepoint DLP Endpoint analyzes content within a user's working environment (PC, laptop and variants) and blocks or monitors policy breaches as defined by the endpoint profiles.

See the Installation and Deployment Guide for Forcepoint F1E Solutions for more information.

Integration agent

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The integration agent allows third-party products to send data to Forcepoint DLP for analysis. It is embedded in third-party installers and communicates with Forcepoint DLP via a C-based API.

Third parties can package the integration agent inside their own installer using simple, “industry standard” methods that are completely transparent to end users.

When the third-party product is installed on a user’s system, it needs to register the integration agent with the Forcepoint management server. This can be done transparently through the installation process or using a command-line utility.

See the Forcepoint DLP Deployment Guide for more information.

Crawler

Applies to:
■ Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The crawler is the name of the discovery and fingerprinting agent. It is selected by default when you install the Forcepoint management server or supplemental Forcepoint DLP servers.

You can deploy additional crawlers in your network if you desire. When you set up a fingerprint task, you indicate which crawler should perform the scan. Forcepoint recommends you use the crawler that is located closest in proximity to the data you are scanning.

You can view the status of your crawlers in the Forcepoint Security Manager Data Security module. Go to **Settings > Deployment > System Modules**, select the crawler, and click **Edit**.

See the Forcepoint DLP Deployment Guide for more information.

The Email Security module

The Email Security module of the Forcepoint Security Manager is used to configure and manage the email protection features of your deployment.

Applies to:
■ Forcepoint Email Security, v8.5.x

The Email module and Email Log Server are typically installed together, which helps to minimize the impact of email traffic report processing.

Placement

Forcepoint Email Security is a Forcepoint appliance-based solution (V Series, X Series blade server, or virtual appliance). Most of its core functions reside on the appliance. The Email Security module is installed as part of the Forcepoint Security Manager on a separate, Windows-based *Forcepoint management server*.

Related concepts

Forcepoint management server on page 376

Email Log Server

Log Server is the Windows-only component that receives log records and processes them into the Log Database for use in reporting.

Applies to:
■ Forcepoint Email Security, v8.5.x

Placement

Log Server must be installed on a Windows machine—typically on the Forcepoint management server. It may not be installed on the Forcepoint Email Security appliance.

Special considerations

To be able to install Log Server, a supported database engine (see *System requirements for this version*) must be running.

If you install Log Server on a machine separate from the Forcepoint Security Manager, stop and restart the **Websense TRITON - Email Security** service after installation. This service is on the *Forcepoint management server*.

Related concepts

Forcepoint management server on page 376

Related reference

System requirements for this version on page 9

Chapter 32

Using the Forcepoint DLP Protector CLI

Contents

This document describes the command line interpreter (CLI) for the Linux-based Forcepoint DLP protector.

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

A command-line interpreter (also known as a command-line shell) is a computer program that reads lines of text entered by a user and interprets them in the context of a given operating system or programming language.

Command-line interpreters allow users to issue various commands in a very efficient way. This requires the user to know the names of the commands and their parameters, and the syntax of the language that is interpreted.

For more details, refer the sections *Accessing the CLI*, *Command-line reference*, and *Configuring NTP support*.

Accessing the CLI

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The CLI can be used after initial installation to modify the settings configured by the wizard as well as configure other protector parameters. Log in using the **admin** or **root** user (other users can also be defined).

Admin users are limited and not all Linux shell commands are available to them. Access the CLI through a direct terminal, a serial port console, or SSH.

- For a serial port console, configure the terminal application, such as HyperTerminal or TeraTerm, as follows: 19200 baud, 8 data bits, no parity, 1 stop bit, no flow control.
- For SSH, connect to port 22 with an SSH tool.
  It is impossible to access the protector using SSH before running the wizard for the first time.

Command-line reference

Following are general guidelines to using the CLI.

Applies to: Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

- For admin users, use the `help` command to view a list of all available commands

- All commands can be run with the “help” option to view detailed help about that command. For example: `iface help`
- The CLI shell offers auto-complete for command names using the TAB key. For example, typing the letter “i” plus TAB will display all commands that start with the letter “i.”
- The CLI shell implements command history. Use the up/down arrows to view/run/ modify previously entered commands, sequentially.
  Some commands’ output may exceed the height of the screen. Use the terminal software to scroll back and view all output.
- All commands and their arguments are case sensitive.
- Abbreviations are not accepted in the CLI; it is necessary to type the entire word. The TAB button can be used to complete partially typed commands.
- Some command output may exceed the length of the screen. Once the screen is full, the CLI will prompt **–more-**. Use the spacebar to display the next screen.

Action	Syntax	Description
Exit the command line interface	`exit`	Exits the user from the Forcepoint Protector CLI and returns to the login prompt or to a wrapper shell environment.

Show CLI help messages	`help`	This command displays all available commands with a small description for each. The list of available commands depends on the user’s profile. All commands support the help argument. When used, the command displays a help message relevant to that command.
		`Forcepoint1# dns help`
		`dns: Configure or show DNS server(s) Usage: dns [list | delall] dns [{add | del} <ipaddr>]`

Accessing the basic configuration wizard	`wizard`	Opens the Forcepoint Protector Installation Wizard. The user can also run `wizard securecomm` to go directly to the registration stage of the Wizard, where Data Security Manager details are entered.
		`Forcepoint1# wizard`
		`Forcepoint1# wizard securecomm`

Rebooting the protector	`reboot`	Reboots the protector. The protector is shut down and restarted immediately after the command is executed.

Action	Syntax	Description
Turning off the protector	`shutdown`	Shuts down the protector. The protector is shut down and powered off immediately after the command is executed.

Showing the Forcepoint Protector version	`version`	Displays the protector version information.
		`Forcepoint1# version`
		`This is Forcepoint Content Protector 8.6.0.009, Policy Engine 8.6.0.9 (Appliance 8.6.0.009)`

Setting or showing the system date	`date [-d] [dd-mmm-yyyy]`	Sets or displays the date of the protector. By default, the command displays the current date. Otherwise, the argument is used to set the date of the protector.
		The `date` command is also a native Linux command. Root users can access the CLI command by running it with its full path:
		`/opt/websense/neti/bin/date`
		Parameters:
		If the **-d** option is given, the date is displayed or set using an all digit format (mm/dd/ yyyy, for example: 07/31/2017). Otherwise, a dd-mmm-yyyy format is used. dd is the day of the month [01 to 31] mmm is the month in abbreviated 3-letter format [Jan, Feb, Mar, etc.] yyyy is the year [2016, 2017]
		`Forcepoint1# date`
		`31-Jul-2017`

Action	Syntax	Description

Setting or showing the system time	`time -h [HH[:MM[:SS]]]`	Sets or displays the time in the protector. By default, the command displays the current time.
		The `time` command is also a native Linux command. Root users can access the CLI command by running it with its full path:
		`/opt/websense/neti/bin/time`
		Parameters:
		■ **-u** sets the time in UTC
		■ **-h** displays a short usage message **HH:MM:SS HH** is the hour [00 to 24]
		■ **MM** is the minutes [00 to 59]
		■ **SS** is the seconds [00 to 59]
		`Forcepoint1# time`
		`17:55:03`

Modify or show system time zone	`timezone [list, show, set <timezone>]`	Shows or sets the protector time zone. **Parameters**: ■ **list** displays a complete list of time zones that can be set in the Forcepoint Protector ■ **show** displays the time zone set in the Forcepoint Protector (default option) ■ **set <*timezone*>** sets the time zone. The **set** command must be followed by the name of the time zone to be selected, as listed using the **list** command. Note that the names of the time zones are case-sensitive. **Default**: When no argument is given, "show" is assumed. `Forcepoint1# timezone set US/Hawaii`

Action	Syntax	Description

Viewing protector information	`info { cpu | memory | network | diag | uptime | hardware | features} info stats [reset]`	Displays information about the Forcepoint protector.
		
		Root users must access the CLI command by running it with its full path:
		
		`/opt/websense/neti/bin/info`
		
		Parameters:
		■ **cpu** displays the protector's CPU usage information.
		■ **memory** displays the protector memory usage information.
		■ **network** displays the protector's network settings including hostname, domain name, IP address and routing table.
		■ **diag** creates a diagnostic file to be used by Forcepoint technical services.
		■ **uptime** displays the amount of time the protector has been up and operational.
		■ **features** lists all the possible features available on this protector and what they can do (monitor or block).
		■ **hardware** displays hardware information including which network cards are installed.
		■ **stats** displays traffic statistics for each protocol being monitored; this is useful to verify the operational status of the Protector.
		■ **stats reset** resets all statistics counters to zero.
		
		`Forcepoint1# info cpu`
		`Processor 1: 1.3% loaded`
		`(98.7% idle)`
		`Forcepoint1# info memory`
		`Free physical memory 8.7%`

Action	Syntax	Description

Collecting statistics	`debug stats [-d] [-i <interval> | -n <count>]`	This command allows a user to collect statistics about network behavior over time. It does so by running **info stats** at specified intervals for a given number of times. The collected statistics are saved in a CSV file for easy manipulation and analysis in spreadsheet tools such as Microsoft Excel. The resulting file is saved as:
		`opt/pa/log/collect_stats.csv.gz`
		Parameters:
		■ **-d:** delete previously recorded statistics information file, if one exists
		■ **interval:** the interval in seconds between two runs that take a snapshot of the statistics.
		■ **count:** how many times the statistics snapshot should be taken.
		Default:
		The default interval is every 60 seconds. The default number is 1440 (which is the equivalent of 24 hours of statistics when the default interval of 60 is selected).
		`Forcepoint# debug stats -d -i 120`

Configure or show the DNS server(s)	`dns [list | delall] dns [{add | del}] <ip_address>]`	Lists, adds, or deletes DNS servers. **Parameters**: ■ **list:** displays a list of DNS servers in the protector ■ **delall:** deletes all DNS servers set in the protector ■ **add:** adds a DNS server specified by its IP address to the protector ■ **del:** deletes the DNS server denoted by the specified IP address `Forcepoint1# dns add 192.168.15.3`

Action	Syntax	Description
Configure or show the default domain name(s)	`domain [list | delall] domain [{add (-m) | del} <domain>]`	Lists, adds, or deletes default domain names in the protector. **Parameters**: ■ **list:** displays a list of configured default domain names in the protector ■ **delall:** deletes all default domain names set in the protector ■ **add:** adds a default domain name specified by <*domain*> to the protector Use the `-m` switch to set a domain as main. The main domain is the domain that the protector is actually is a member of. Without the 1m switch a search domain is created. For the protector to resolve a domain this domain is searched as well. There may be many search domains, but only one main domain. ■ **del:** deletes the default domain name denoted by <*domain*> from the protector `Forcepoint1# domain add example.com`
Configure or show the default gateway	`gateway <ip_address>` `gateway [list | delete`	By default, displays the current defined gateway. Using the parameters, it is possible to set or delete the default gateway of the protector. **Parameters**: ■ **ipaddr:** when given, the ipaddr is used as a default gateway for the protector. ■ **list:** shows the configured default gateway. ■ **delete:** deletes the defined default gateway. If this command is run from a remote SSH session, the session may terminate. `Forcepoint1# gateway 192.168.10.254`

Action	Syntax	Description
Configure or show the hostname	`hostname <name>`	Displays the current hostname. The parameter can also set a unique name by which to identify the protector. **Parameters**: If a name is given, the hostname is set to the given name. Otherwise, the hostname is displayed. `Forcepoint1# hostname 1Tokyo`
Configure or show interface information	`iface [list]` `iface ifname [ip <ip_address>] [prefix <prefix>] [bcast <bcastaddr>] [speed <speed>] [duplex <duplex>] [mgmt] [enable|disable] [descr <description>]`	Configures and displays the protector's network interface information. When invoked without arguments or with the `list` option, the command displays a list of all available interfaces in the system. When invoked with only an interface name, the command shows detailed information about that interface. Any other invocation method configures the interface denoted in **ifname**. **Note** Use a console connection to the protector when using this command to configure the management interface, (and not a remote SSH connection). Using the latter may terminate the session to the protector. In addition, if the IP address is changed, it may be required to re-establish secure communication with the Forcepoint DLP server (by re- running the configuration wizard). **Parameters**: ■ **ip**: the IP address assigned to the interface. This option is valid only for the management interface. When setting **ip**, the **prefix** and **bcast** options must also be set.

Action	Syntax	Description

		■ **prefix:** network mask of the interface. For example: 24 (will assign 255.255.255.0 mask to the interface)
		■ **bcast:** broadcast address of the interface. For example: for an interface with the IP address 192.168.1.1/24, the broadcast address is usually 192.168.1.255.
		■ **speed:** interface link speed. Available speeds: auto, 10, 100, 1000
		■ **duplex:** interface link duplex. Available duplex options: auto, half, full
		■ **mgmt:** sets the interface as the management interface of the protector. The previously defined management interface can no longer be used for management purposes.
		■ **enable, disable:** enables or disables the interface (default is enable)
		■ **descr:** assigns a short description for the interface. Note that if the description contains spaces, it must be enclosed within quotation marks ("").
		Default:
		`eth0`
		Example:
		`Forcepoint1# iface eth0 ip 10.100.16.20 prefix 24 bcast 10.100.16.255 mgmt enable`

Add or delete routing information	`route list`
	`route add {destination network | destination ip} {via ip | dev device}`
	`route del {destination network | destination ip} {via ip | dev device}`
		Adds or deletes route entries in the protector. When adding or deleting routes to networks, use the x.x.x.x/prefix format. For example: 192.168.1.0/24.
		Parameters:
		■ **list:** displays the protector's routing table
		■ **add:** adds a route to a network or IP address

Action	Syntax	Description

		■ **del:** deletes a route to a network or IP address
		`Forcepoint1# route add 100.20.32.0/24 via 10.16.10.10`
		`Forcepoint1# route add 172.16.1.0/24 dev eth0`

Manage users	`user add {username} profile {profile} pwd {password}`
	`user del {username}`
	`user mod {username} [profile {profile}] [pwd {new password}]`
	`user list`
		Use the “user” command to define additional system access accounts. Each account has a profile that defines the operations available to users.
		The available profiles are:
		■ **admin:** all commands are allowed
		■ **netadmin:** only networking related commands are allowed
		■ **policyadmin:** only the policy command is allowed
		The list of commands each profile can run cannot be changed.
		Parameters:
		■ **add:** add a user with the given profile and password
		■ **del:** delete a user
		■ **mod:** modify a user’s profile and/or password
		■ **list:** display a list of all defined users and their profiles
		`Forcepoint1# user add Jonny profile netadmin pwd 123qwe`

Filtering monitored networks	`filter [show | set rule | delete]`	Use the Forcepoint Management Interface to define which networks are monitored by the protector. This CLI command enables advanced filtering of monitored networks. **Note** Forcepoint recommends testing the filter using tcpdump before setting the filter. This ensures that the protector recognizes the filter expression.

Action	Syntax	Description
		Parameters: ■ **show:** displays the current active filters - monitored networks ■ **set:** defines a list of monitored networks ■ **delete:** deletes previously set filter rules `Forcepoint1# filter set "tcp and host 10.0.0.1"` This command sets the protector to monitor all TCP traffic to/from 10.0.0.1 and ignore all other hosts in the network. If VLAN is used, it should be listed first in the filter ("vlan and tcp" instead of "tcp and vlan").

Configuring NTP support

The protector includes an NTP package that contains a NTPD service and a set of related utilities. The service is turned off by default. Enabling the NTP service is simple, but requires deployment-dependent configuration settings.

Applies to:

- Forcepoint DLP, v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0

The following procedure is a general description of the steps that can be customized as needed.

The NTP service requires **root** user permissions.

For further NTP configuration details, refer to: http://en.linuxreviews.org/NTP- How to make the clock show the correct time or http://doc.ntp.org/4.2.2/ and many other sites on the Web.

Configuration

1) Define which NTP servers or servers to use.

2) Configure the firewall according to the NTP server decision. The NTP port is UDP 123.

3) Edit the relevant configuration files (/etc/ntp.conf, and so on).

Execution

1) Perform an initial time synchronization. This can be done manually via the protector's wizard, or via the **ntpdate** utility.

2) Enter `chkconfig ntpd on` at the command line to start the service each time the protector machine is started.

3) Type `ntpq -p` to verify the synchronization is correct.