



Installation Guide

Websense[®] Data Security

v7.8

©1996–2013, Websense, Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
Published 2010

Printed in the United States and Ireland

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

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

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

libwbxml, the WBXML Library(C) 2002-2008 is a copyright of Aymerick Jehanne. This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version. This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the [GNU Lesser General Public License](#) and [GNU General Public License](#) for more details.

Contents

Topic 1	Installing the Management Server	1
	System requirements	1
	Operating system requirements	2
	Hardware requirements	2
	Browser requirements	3
	Database requirements	3
	Port requirements	4
	Preparing for installation	4
	Windows considerations	4
	Domain considerations	5
	Domain Admin privileges	5
	Synchronizing clocks	6
	Antivirus	6
	No underscores in FQDN	7
	Third-party components	7
	SQL Server	8
	Getting the Websense installer	9
	Installation steps	10
	Launch the installer	10
	Install the TRITON Infrastructure	11
	Install Data Security management components	18
	Installing on a virtual machine	22
Topic 2	Installing Data Security Agents and Servers	31
	Installing supplemental Data Security servers	32
	Operating system requirements	32
	Hardware requirements	33
	Software requirements	33
	Port requirements	34
	Installation steps	34
	Installing Data Security agents	37
	Protector	39
	When to use the protector	39
	Deploying the protector	40

Hardware requirements	43
Recommended (optional) additional NICs for inline mode:	43
Port requirements	44
Installing the protector software	45
Configuring the protector	51
Mobile agent	53
Deploying the mobile agent	53
Hardware requirements	55
Port requirements	55
Installing the mobile agent software	56
Configuring the mobile agent	66
Configuring a mobile DLP policy	68
SMTP agent	69
Operating system requirements	70
Port requirements	70
Preparing a machine for the SMTP agent	71
Installing the SMTP agent	72
Testing the SMTP agent	73
Microsoft ISA/TMG agent	75
Operating system requirements	76
Port requirements	76
Installing the ISA/TMG agent	76
Printer agent	78
Operating system requirements	79
Port requirements	79
Before you begin	80
Installing the printer agent	80
Detecting the printer driver	82
Configuration settings for non-English text	83
Printer agent performance	84
FCI agent	84
Operating system requirements	85
Port requirements	85
Before you begin	86
Installing the FCI agent	87
Configuring the FCI agent	88
Integration agent	88
Installing the integration agent	89
Registering the integration agent	90
Using the Websense Data Security API	90
The crawler	91
Operating system requirements	91

	Port requirements	91
	Installing the crawler agent	92
	Troubleshooting Data Security agent installation	94
	Initial registration fails	94
	Deploy settings fails	95
	Subscription errors	95
	Network connectivity problems	96
Topic 3	Adding, Modifying, or Removing Components.....	97
	Adding or modifying Data Security components.....	97
	Recreating Data Security certificates.....	98
	Repairing Data Security components.....	98
	Changing the Data Security privileged account.....	99
	Changing the domain of a Data Security Server	99
	To join a Data Security Server to a domain	99
	Removing Data Security components	100

1

Installing the Management Server

In this topic:

- ◆ [System requirements, page 1](#)
 - ◆ [Preparing for installation, page 4](#)
 - ◆ [Installation steps, page 9](#)
 - ◆ [Installing on a virtual machine, page 22](#)
-

This section describes how to install Websense Data Security on a management server. For instructions on installing Websense Web Security and/or Email Security components alone or with Data Security, see the [Deployment and Installation Center](#) in the Websense Technical Library.

To install Data Security, you perform 2 basic steps.

1. [Install the TRITON Infrastructure, page 11.](#)
This includes the TRITON console, settings database, and reporting database.
2. [Install Data Security management components, page 17.](#)
This includes the a policy engine, crawler, fingerprint repository, forensics repository, and endpoint server.

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

Once you've installed management components, you may choose to install Data Security agents on print servers, TMG servers, or endpoint client machines. You can also install extra Data Security servers and crawlers for system scaling. See [Installing Data Security Agents and Servers, page 31](#) for more information.

System requirements

The machine that hosts core management components for Websense security solutions is referred to as the **TRITON management server**. In the context of DLP, it is also known as the Data Security Management Server.

Operating system requirements

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

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

Hardware requirements

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

Notes:

- ◆ Data Security allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90GB from the Data Security disk space requirements.
- ◆ If you choose to install Data Security on a drive other than the main Windows drive (typically C drive), then you must have at least 2GB free on the main Windows drive to accommodate for files to be extracted to this drive.

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

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

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

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

Browser requirements

Use any of the following browsers to access the TRITON console and Data Security manager.

Browser	Versions
Microsoft Internet Explorer*	8, 9, and 10
Mozilla Firefox	4.4 and up
Google Chrome	13 and later

* Do not use Compatibility View.

Database requirements

Microsoft SQL Server is used to host the reporting database for Data Security and other Websense solutions.

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

Use only the version of SQL Server 2008 R2 Express included in the TRITON Unified Installer.

- ◆ Larger organizations are advised to use Microsoft SQL Server Standard or Enterprise. These SQL Server editions cannot reside on the TRITON management server.

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

The supported database engines are:

- ◆ SQL Server 2008
All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64.
- ◆ SQL Server 2008 R2 Express (installed by the TRITON Unified Installer)
- ◆ SQL Server 2008 R2
All editions except Web and Compact; all service packs, 32- and 64-bit, but not IA64.
- ◆ SQL Server 2012
Standard, Business Intelligence, and Enterprise editions

Port requirements

The following ports must be kept open on the Data Security Management Server:

Outbound

Data Security Server, Protector, Web Content Gateway, Email Security Gateway	17500-17515* * and 17700-17715* **	Consecutive ports that allow communication with Websense agents and machines.
--	--	---

Inbound

From	Port	Purpose
Data Security Server, Protector, Web Content Gateway	17443*	Incidents
Data Security Server, Protector, Web Content Gateway	139	File sharing
Data Security Server, Protector, Web Content Gateway	443	Secure communication
Data Security Server, Protector, Web Content Gateway	445	File sharing
Data Security Server, Protector, Web Content Gateway	8453	User repository
Data Security Server, Protector, Web Content Gateway	8005	Tomcat server
Data Security Server, Protector, Web Content Gateway, Email Security Gateway	17500-17515* * and 17700-17715* **	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server, Protector, Web Content Gateway	9443*	Access user interface

Preparing for installation

Before installing Data Security, make sure that you have completed all of the preparations noted below.

Windows considerations

- ◆ Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.

- ◆ In addition to the space required by the Websense installer itself, further disk space is required on the Windows installation drive (typically C) to accommodate temporary files extracted as part of the installation process.

For information on minimum disk space requirements, see [Hardware requirements, page 2](#).

- ◆ The TRITON Unified Installer requires the following versions of .NET Framework, depending on your operating system version:
 - Windows Server 2008 R2: Use version 2.0 or higher. If .NET 2.0 is not already installed, it is available from www.microsoft.com.
 - Windows Server 2012: Version 3.5 is required.

Note that .NET Framework 3.5 must be installed before adding any language packs to the operating system (as noted in the following article from Microsoft: <http://download.microsoft.com/download/D/1/0/D105DCF6-AC6C-439D-8046-50C5777F3E2F/microsoft-.net-3.5-deployment-considerations.docx>).
 - Both .NET Framework 2.0 and 3.5 SP1 are required if you are installing SQL Server Express.

Domain considerations

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

Do not install Data Security on a domain controller machine, however.

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

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

Domain Admin privileges

Websense components are typically distributed across multiple machines. Additionally, some components access network directory services or database servers. To perform the installation, it is a best practice to log on to the machine as a user with

domain admin privileges. Otherwise, components may not be able to properly access remote components or services.



Important

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

Synchronizing clocks

If you are distributing Websense components across different machines in your network, synchronize the clocks on all machines where a Websense 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 Websense V-Series appliance, you must synchronize the machine's system time to the appliance's system time.

Antivirus

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

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

No underscores in FQDN

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



Note

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

Third-party components

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

- ◆ .NET Framework 3.5 SP1
Because the installer requires .NET 2.0, both .NET 2.0 and 3.5 SP1 are required if you are installing SQL Server Express.
- ◆ Windows Installer 4.5
- ◆ Windows PowerShell 1.0
- ◆ PowerShell is available from Microsoft (www.microsoft.com).

SQL Server

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

1. Install SQL Server according to Microsoft instructions. See [Database requirements](#), [page 3](#) for a list of supported versions.



Tip

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

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



Note

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

4. Obtain the SQL Server logon ID and password for a SQL Server Administrator, or for an account that has db_creator server role, SQLAgent role, and db_datareader in **msdb**. The account must have a sysadmin role. You need this logon ID and password when you install Data Security.
5. Restart the SQL Server machine after installation.
6. Make sure the TRITON management server can recognize and communicate with SQL Server.

7. Install the SQL Server client tools on the TRITON management server. Run the SQL Server installation program, and select **Connectivity Only** when asked what components to install.
8. Restart the machine after installing the connectivity option. See Microsoft SQL Server documentation for details.

SQL Server user roles

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

To install Websense Log Server successfully, the user account that owns the Websense 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 Email Security Gateway/Anywhere 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.

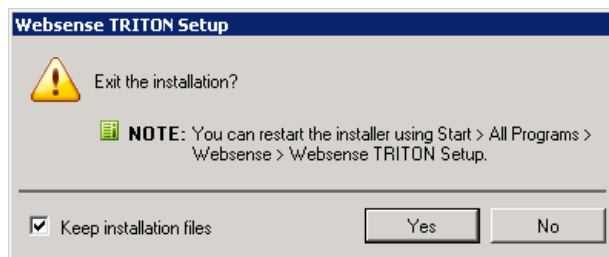
1. On the SQL Server machine, go to **Start > Programs > Microsoft SQL Server 2008 or 2012 > Microsoft SQL Server Management Studio**.
2. Log into SQL Server as a user with SQL sysadmin right.
3. Select the **Object Explorer** tree, and then go to select **Security > Logins**.
4. Select the login account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

Getting the Websense installer

The TRITON Unified Installer is used to install or upgrade the TRITON management server, Data Security software, reporting components, and SQL Server 2008 R2 Express on supported Windows servers.

Download the installers from mywebsense.com.

- ◆ The TRITON Unified Installer executable is named **WebsenseTRITON78Setup.exe**. Double-click it to start the installation process. If you have previously run the Websense installer on a machine, and you selected the **Keep installation files** option, you can restart the installer without extracting all of the files a second time.



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

Note that the files occupy approximately 2 GB of disk space.

Installation steps

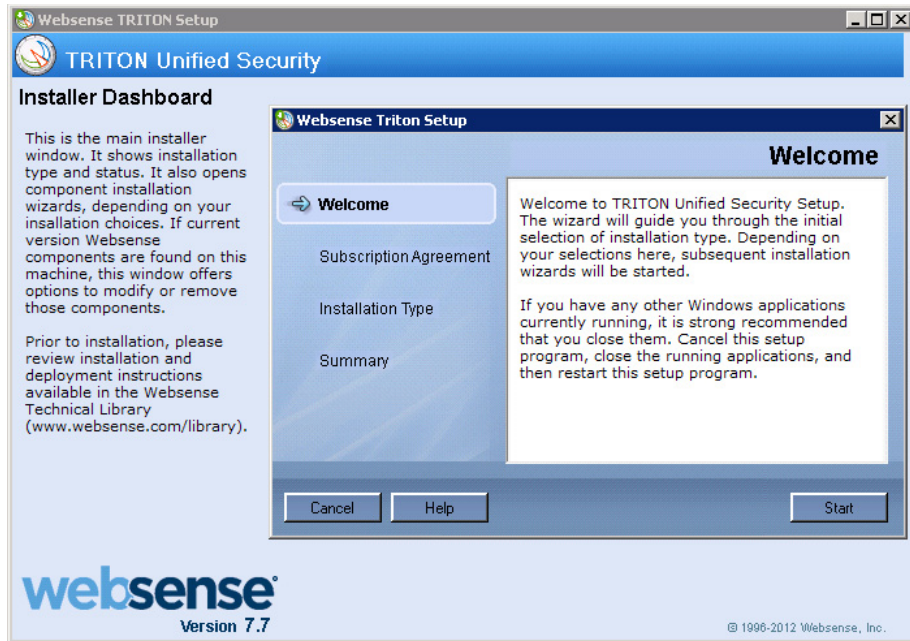
Do the following to install Data Security on the management server.

1. *Launch the installer*, page 9
2. *Install the TRITON Infrastructure*, page 11
3. *Install Data Security management components*, page 17

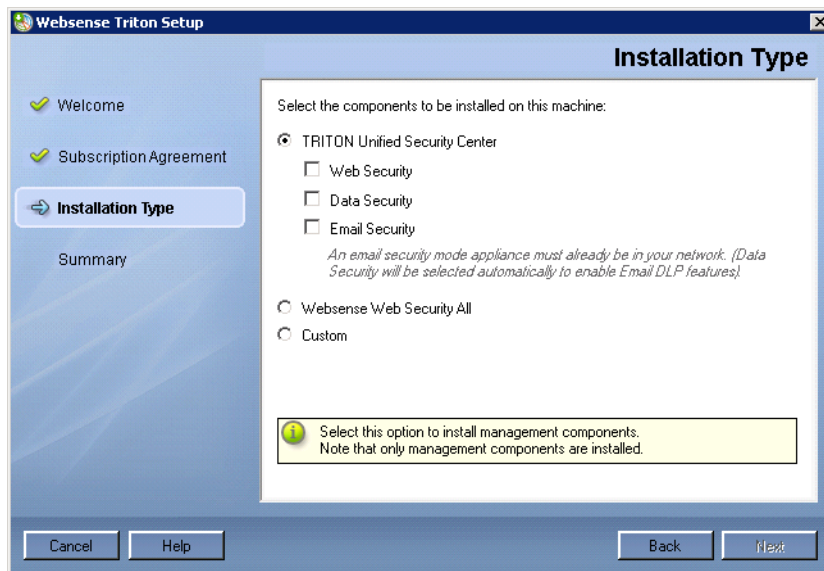
Launch the installer

1. Double-click the installer file, **WebsenseTRITON78Setup.exe**, to launch the Websense TRITON Setup program. A progress dialog box appears, as files are extracted.

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



3. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
4. On the **Installation Type** screen, select **TRITON Unified Security Center** and then select **Data Security**.



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

Install the TRITON Infrastructure

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



Important

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

- To accept the default location (recommended), simply click **Next**.
 - To specify a different location, click **Browse**.
3. On the **SQL Server** screen, specify the location of your database engine and the type of authentication to use for the connection. Also specify whether to encrypt communication with the database.

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

When this option is selected, .NET 3.5 SP1, Powershell 1.0, and Windows Installer 4.5 are installed automatically if they are not found on the machine. These are required for SQL Server 2008 R2 Express.

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

If .NET 3.5 SP1 is not found on the machine, the installer needs access to windowsupdate.microsoft.com. If anything blocks this machine from accessing the site, SQL Server Express cannot be installed.

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

- Windows Server 2012: Go to the **Start** screen and click the **Websense TRITON Setup** icon.
- Windows Server 2008 R2: Go to **Start > All Programs > Websense > Websense TRITON Setup**.
- Select **Use the SQLServer database installed on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

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

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

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

See [System requirements, page 1](#), to verify your version of SQL Server is supported.

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

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

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



Note

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

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

If the test is unsuccessful, the following message appears:

Unable to connect to SQL

Make sure the SQL Server you specified is currently running. If it is running, verify the access credentials you supplied.

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

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

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

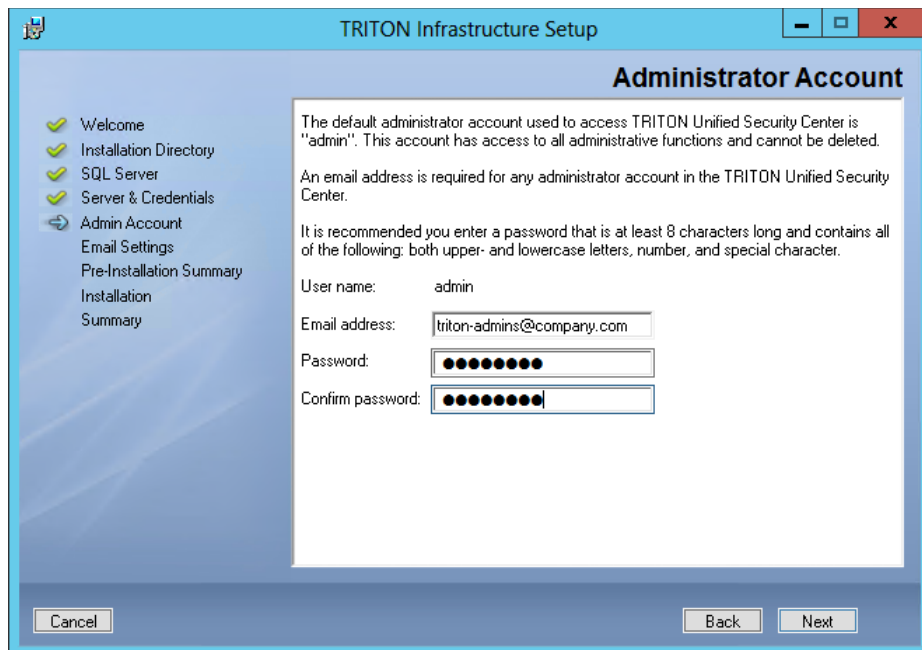
Use the IP address selected to access the TRITON Unified Security Center (via Web browser). Also specify this IP address to any Websense component that needs to connect to the TRITON management server.

If you chose to install SQL Server 2008 R2 Express, if you install Web Security or Email Security Log Server on another machine, specify this IP address for the database engine location.

- Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Unified Security Center. The server/host name cannot exceed 15 characters.
 - Specify the **User name** of the account to be used by TRITON Unified Security Center.
 - Enter the **Password** for the specified account.
5. On the **Administrator Account** screen, enter an email address and password for the default TRITON console 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 onscreen.



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



Important

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

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

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



Warning

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



Note

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

8. If you chose to install SQL Server Express, .NET Framework 3.5 SP1, 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. Websense installer starts again. In the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
 - c. The **Ready to Resume EIP Infra installation** screen appears. Click **Next**.



Note

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

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

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

Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.
10. Next, the **Installation** screen appears. Wait until all files have been installed.

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

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

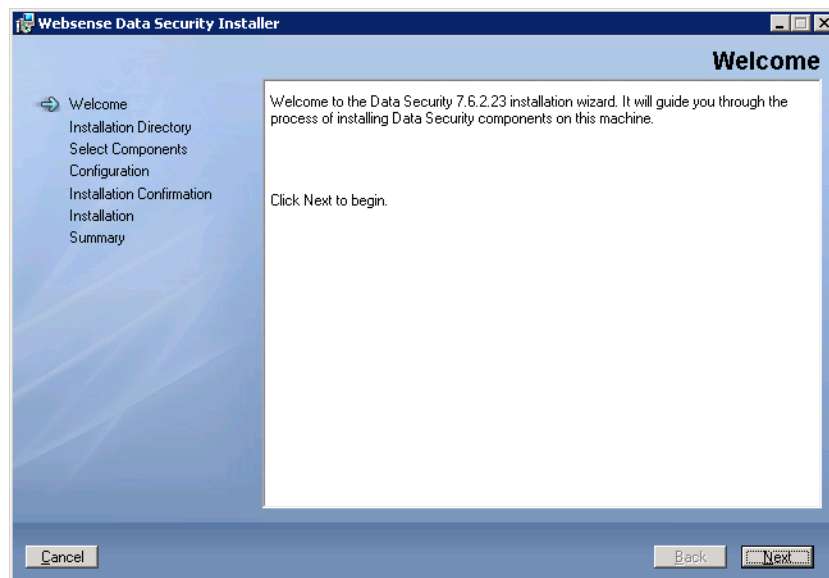
If port 9443 is in use, release it and then click **Retry** to continue installation.

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

You are returned to the Installer Dashboard and, after a few seconds, the Web Security component installer launches.

Install Data Security management components

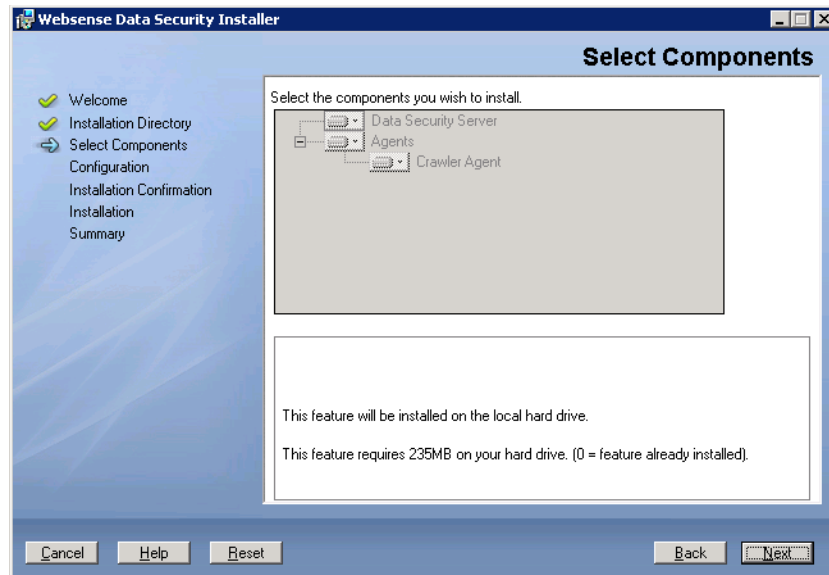
1. When the Websense Data Security Installer is launched, a **Welcome** screen appears. Click **Next** to begin Data Security installation.



Note

If the .NET 2.0 framework is not found on this machine, the Data Security installer installs it.

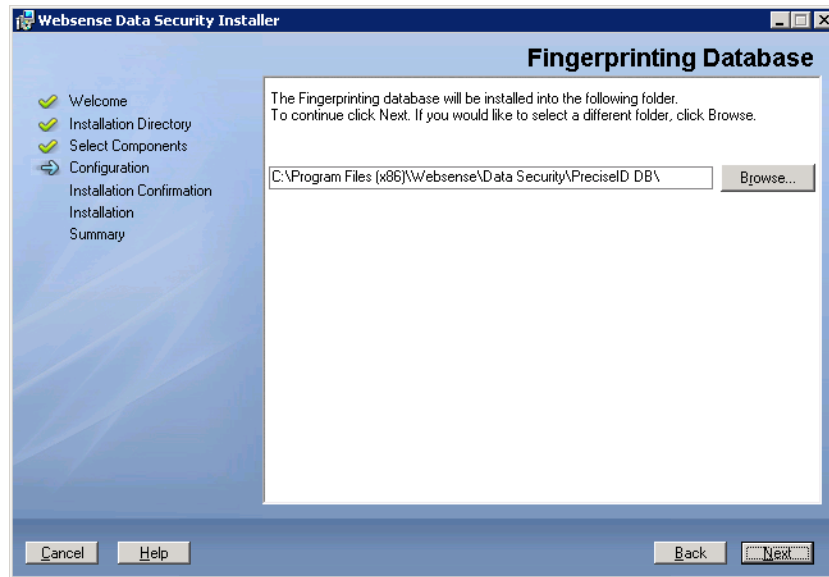
2. On the **Select Components** screen, click **Next** to accept the default selections.



Note

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

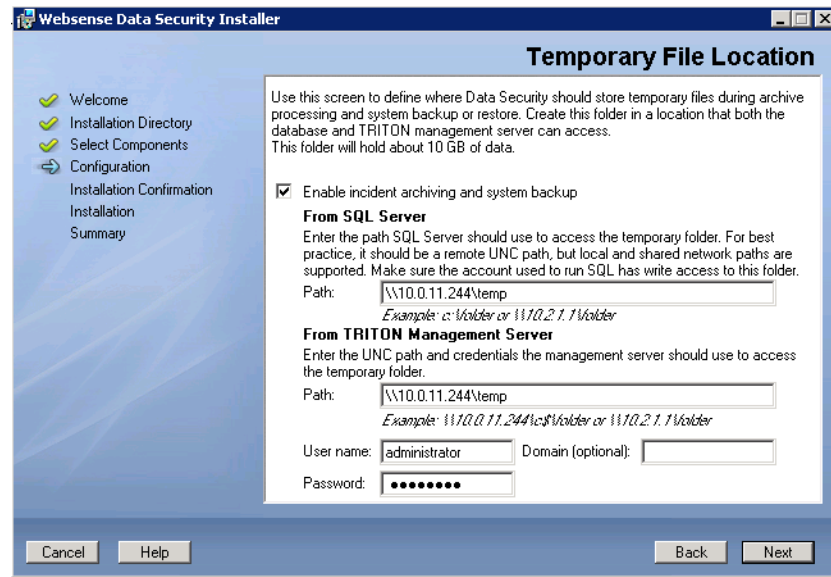
3. If prompted, click **OK** to indicate that services such as ASP.NET and SMTP will be enabled.
Required Windows components will be installed. You may need access to the operating system installation disc or image.
4. On the **Fingerprinting Database** screen, accept the default location or use the **Browse** button to specify a different location.
Note that you can install the Fingerprinting database to a local path only.



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

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

Before proceeding, create a folder in a location that both the database and TRITON management server can access. (The folder must exist before you click **Next**.) On average, this folder will hold 10 GB of data, so choose a location that can accommodate this.



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

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



Important

For all 7.7.x versions, the account used to access the SQL Server must have **BACKUP DATABASE** permissions to communicate with the installer. If it does not, an error results when you click **Next**.

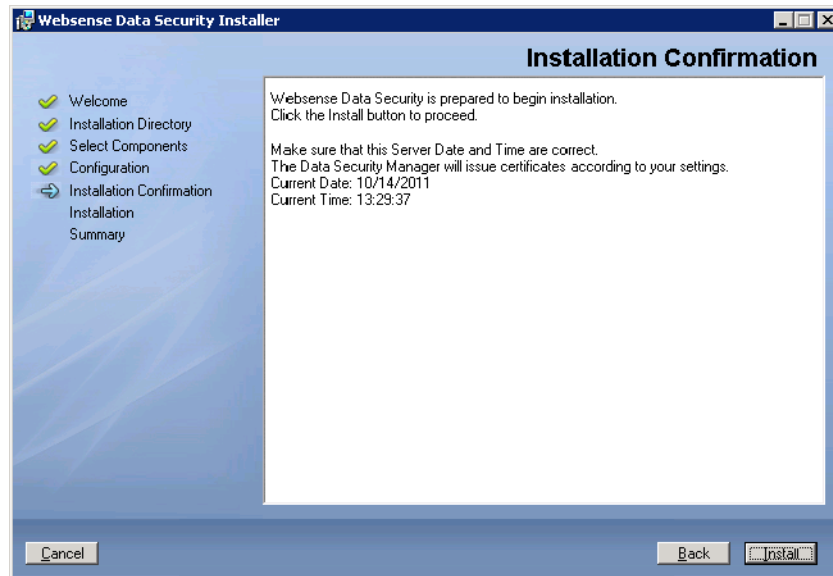
To grant this permission, issue the following T-SQL commands on the SQL Server instance:

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

After installation of Data Security components, you can revoke this permission:

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

- In the **Installation Confirmation** screen, click **Install** to begin installation of Data Security components.



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

Data Security needs port 80 free.

In order to proceed with this installation, DSS will free up this port.

Click Yes to proceed OR click No to preserve your settings.

Clicking **No** cancels the installation.

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

- The **Installation** progress screen appears. Wait for the installation to complete.
- When the **Installation Complete** screen appears, click **Finish** to close the Data Security installer.
- If no other TRITON Unified Security Center 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 Data Security components, such as the protector, mobile agent, printer agent, SMTP agent, TMG agent, or endpoint client, see [Installing Data Security Agents and Servers, page 31](#).

Installing on a virtual machine

Websense Data Security supports installations over Virtual Machines (VM), but Microsoft SQL Server must be present to support the incident and policy database. See [System requirements, page 1](#), for supported versions of SQL Server. If you are performing a clean install of Websense Data Security, SQL Server 2008 R2 Express is included.

If you have a subscription to Websense Web Security Gateway Anywhere, be sure to select both the Web Security and Data Security management modules when creating the TRITON management server VM.

If you have a subscription to Websense Email Security Gateway or Email Security Gateway Anywhere, select both the Email Security and Data Security management modules when creating the TRITON management server VM.

The following VM platforms are supported. You can obtain them from the VMware site: www.vmware.com.

- ◆ VMware ESXi 3.5 update 2
- ◆ VMware ESXi 4 update 1
- ◆ VMware ESXi 5.0 and 5.1



Note

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

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

VMware Server	Requirements
CPU	<ul style="list-style-type: none"> ◆ At least 4 cores 2.5 GHz (for example, 1 QuadXeon 2.5 GHz). 8 cores are required if you are installing the Web Security, Data Security, and Email Security managers
Disk	<ul style="list-style-type: none"> ◆ 300 GB, 15 K RPM, RAID 10
Memory	<ul style="list-style-type: none"> ◆ 8 GB (12 GB if you are installing the Web Security, Data Security, and Email Security managers)
NICs	<ul style="list-style-type: none"> ◆ 2*1000

VMware Infrastructure Client	Requirements
CPU	<ul style="list-style-type: none"> • At least 500 MHz
Disk storage	<ul style="list-style-type: none"> • 150 MB free disk space required for basic installation. • An additional 55 MB free on the destination drive during installation • 100 MB free on the drive containing the %temp% folder
Memory	<ul style="list-style-type: none"> • 512 MB
Networking	<ul style="list-style-type: none"> • Gigabit Ethernet recommended

Module	Requirements for VM installation
TRITON Management Server	<ul style="list-style-type: none"> • Windows Server 2008 R2 64-bit or Windows Server 2012 • 8GB RAM • 150 GB Disk • 2 CPU cores

The steps for installing on a virtual machine are as follows:

- ◆ *Installing the ESXi platform*
- ◆ *Customizing ESXi*
- ◆ *Installing the VMware Client*
- ◆ *Installing the license and setting the time*
- ◆ *Configuring an additional NIC*
- ◆ *Creating the Data Security virtual machine*

Installing the ESXi platform

1. Download the version of ESXi that you want to use from www.vmware.com.
2. Once the download is complete, burn the download file to a CD.
3. On the machine that will host your VMware server, insert the ESX Server CD into the CD drive
4. Set the BIOS to boot from the CD.
5. Follow the instructions in the installer to complete the installation process.
6. When the installation has finished, remove the CD and reboot the host machine.

Customizing ESXi

We recommend that you customize the ESXi platform as follows:

- ◆ Assign a password to the root account.

- ◆ Set up a management IP address for the ESXi server.
By default the management IP address is dynamically obtained using DHCP. However, we recommend that you set up a static IP address.

To configure the ESXi platform:

1. Press **F2** to access the Customize System screen.
2. Select **Configure Password**, and enter a password for the root account.
3. To set up a static IP address, select the **Configure Management Network** menu.
4. Select **IP Configuration**, and on the screen that appears enter the following information:
 - Management IP address
 - Subnet mask
 - Default gateway
5. From the **Configure Management Network** menu, select **DNS Configuration**.
6. Configure static DNS information by entering the following:
 - Host name (fully qualified)
 - Primary and secondary DNS server addresses
7. Reboot the server.

Installing the VMware Client



Note

The VMware client for ESX 4i is called the vSphere Client. Although the instructions in this section refer to the VMware Infrastructure Client that is available with ESX 3.5i, all instructions also apply to the vSphere Client.

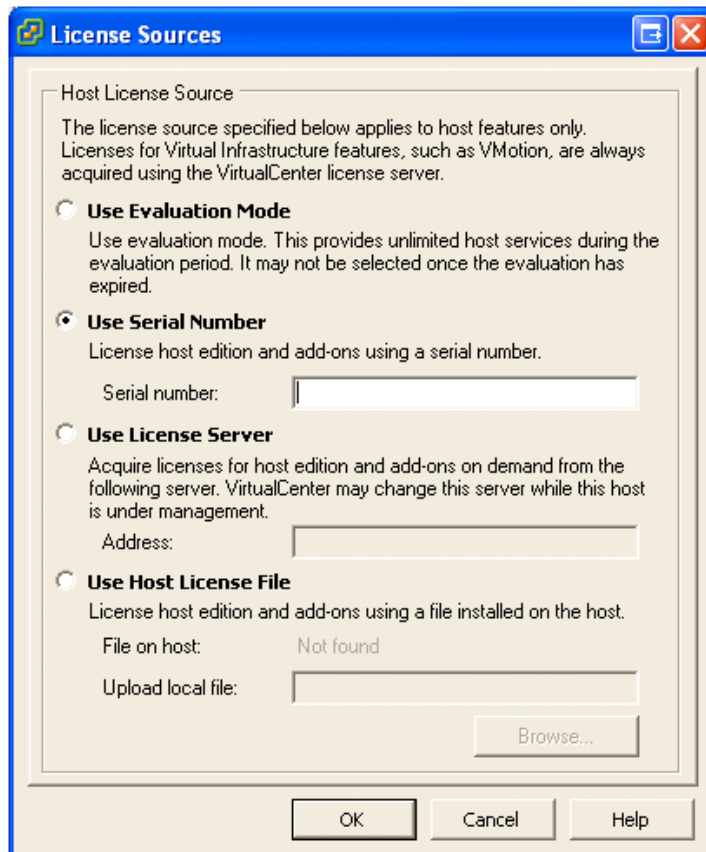
The VMware Infrastructure Client (VI Client) manages the ESXi platform. Install the client on a Windows machine with network access to the ESXi server.

1. On the machine where you intend to install the client, open a browser and access the ESXi server using HTTPS and the management IP address you entered in the previous section (for example, <https://10.15.21.100>). If you see an error page, accept the server certificate.
2. On the VMware ESX Server Welcome page, click the **Download VMware Infrastructure Client** link.
3. Download and run the client installation program.

Installing the license and setting the time

You received your license number as part of the ESXi download.

1. Start the VI Client by selecting **Start > Programs > VMware > VMware Infrastructure Client**.
2. Connect to your ESXi server using the IP address you set up during configuration. For user credentials, enter the user name **root** and the password that you set up for the root account.
3. On the **Configuration** tab, select **Licensed Features**.
4. To the right of the **License Source** label, click the **edit** link.



5. Select **Use Serial Number**, and enter your license number in the field provided. Then click **OK**.
6. On the **Configuration** tab, select **Time Configuration**.
7. Select **Properties**, and then set your server's time. Click **OK** when done.

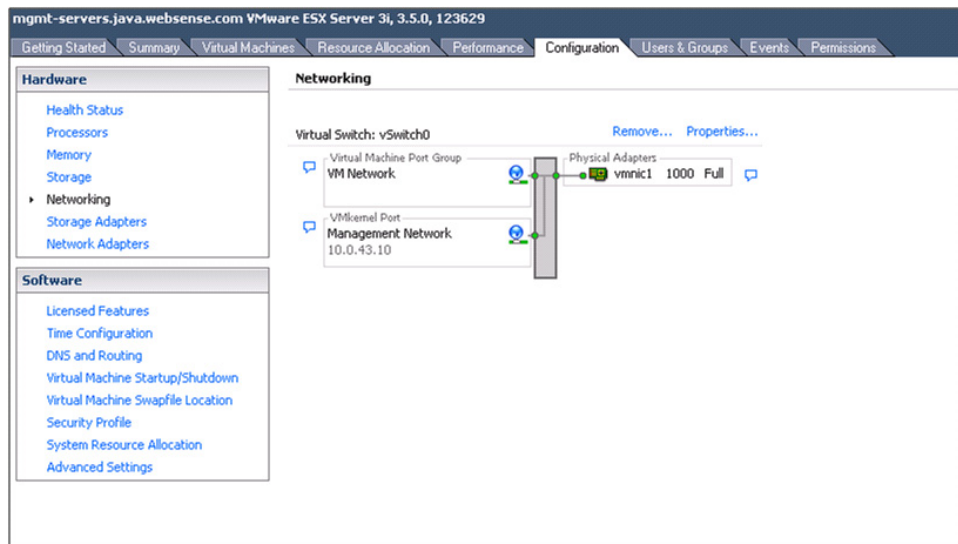
Configuring an additional NIC

When setting up the ESXi server, you configured one NIC as the ESXi platform management interface. This NIC can also be used by the virtual machines. However, this setup requires an additional NIC, for redundancy and to perform load balancing.

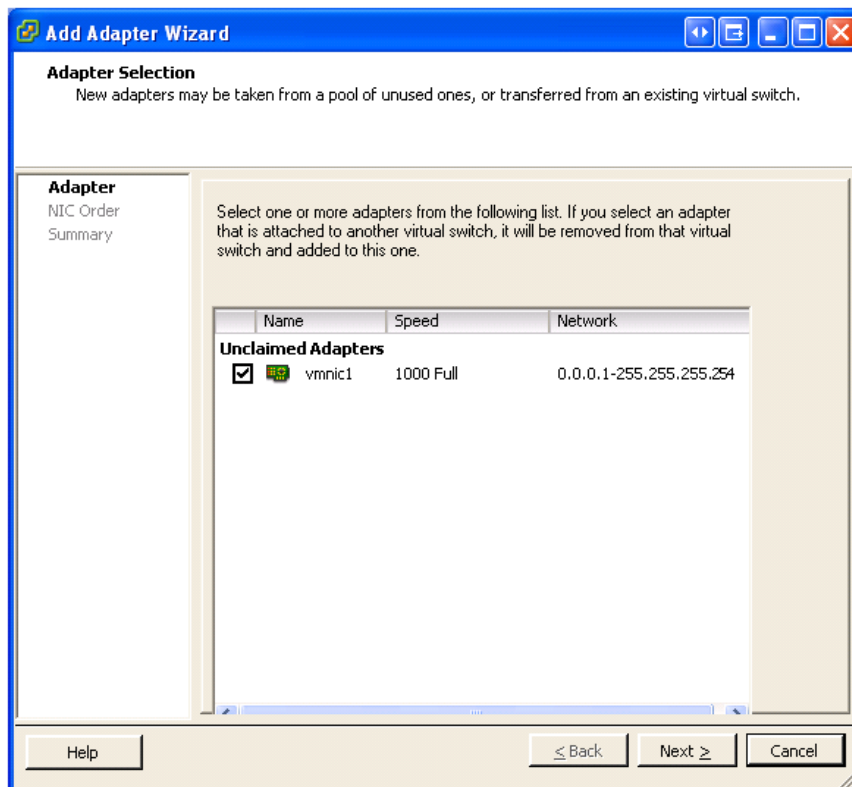
To set up an additional NIC:

1. On the **Configuration** tab, select **Networking**.

When the system was started, the ESXi platform configured the server to have one virtual switch (vSwitch) using the management NIC. With this configuration, the Networking screen should look similar to the one below.

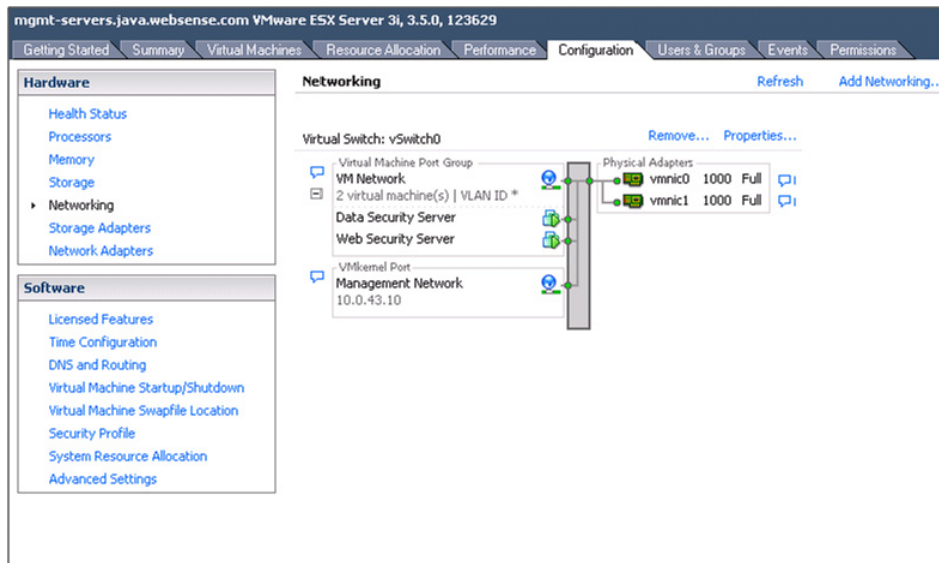


2. To add a new NIC to the virtual switch, select the **Properties** link.
3. In the Properties popup window, select the **Network Adapters** tab and click **Add**. The Add Adapter Wizard opens.



4. Select the adapter you want from the list, then click **Next** twice.
5. Click **Finish** to close the wizard, then close the Properties window.

After adding the additional network adapter to the virtual switch, the network layout should look similar to the one below:



Creating the Data Security virtual machine

1. In the VI Client, select the **Summary** tab and then select **New Virtual Machine**. The New Virtual Machine Wizard opens.
2. Select **Custom**, and click **Next**.
3. Set the machine name to be TRITON Management Server, and click **Next**.
4. Select the only available datastore (datastore1), and click **Next**.
5. Select Microsoft Windows as the guest operating system, and set the version to Microsoft Windows Server 2008 R2 (64 bit).
6. Click **Next**.
7. Set the number of virtual processors according to the TRITON management server for your deployment, and click **Next**. See [System requirements, page 1](#), for more information.
8. Set the virtual machine memory to a minimum of 8 GB, depending on your deployment, and click **Next**. See [System requirements, page 1](#), for more information.
9. Accept the defaults on the Network page and the I/O Adapters page, clicking **Next** to continue.
10. Select **Create a new virtual disk** and click **Next**.
11. Set the disk capacity to 150 GB.
12. Click **Next** to progress through the Advanced Options page without changing the defaults.
13. Review your configuration and then click **Finish**.

Setting the CPU affinity

Once you have configured the virtual machine, set its dedicated CPUs as follows:

1. In the VI Client, select the virtual machine you just created from the tree on the left.
2. Select the Summary view, and click **Edit Settings**.
3. Select the **Resources** tab.
4. Select **Advanced CPU**.
5. In the Scheduling Affinity group, select **Run on processor(s)**, then select processors zero and one.
6. Click **OK**.

Installing the operating system and VMware tools

Install the operating system on your virtual machine, and then reboot. We recommend that you also install the VMware tools before installing the TRITON management server. To do this:

1. Log on to the virtual machine.
2. From the VI Client, select **Inventory > Virtual Machine > Install/Upgrade VMware Tools**.
3. Follow the instructions on screen to install the tools.
4. Follow the instructions above to install the TRITON management server on your virtual machine.

2

Installing Data Security Agents and Servers

Once you've installed Data Security on the TRITON management server (as described in [Installing the Management Server, page 1](#)), you can install other Data Security components as needed. In larger deployments, you might install supplemental Data Security servers, crawlers, or policy engines. In some scenarios, you might install the Data Security protector and/or any number of Data Security agents such as the printer agent for monitoring printer output or ISA agent for monitoring data on Microsoft ISA servers.

Data Security agents are installed on the relevant servers (ISA agent on the ISA server, printer agent on the print server, etc.) to enable Data Security to access the data necessary to analyze the traffic from these servers. The Data Endpoint agent enables administrators to analyze content within a user's working environment (PC, laptop, etc.) and block or monitor policy breaches.



Important

Before you install a Data Security component—for example, a supplemental server or agent—make sure that the TRITON infrastructure is already installed in your network along with the Data Security management components.

Do not install any Data Security component on a domain controller.

- ◆ [Installing supplemental Data Security servers, page 32](#)
- ◆ [Installing Data Security agents, page 37](#)

Installing supplemental Data Security servers

In this topic:

- ◆ [Operating system requirements, page 32](#)
 - ◆ [Hardware requirements, page 33](#)
 - ◆ [Software requirements, page 33](#)
 - ◆ [Hardware requirements, page 33](#)
 - ◆ [Installation steps, page 35](#)
-

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

Supplemental Data Security server installations include:

- ◆ A policy engine
- ◆ SMTP agent (Windows Server 2003 installations only)
- ◆ Secondary fingerprint repository (the primary is on the management server)
- ◆ Endpoint server
- ◆ Optical Character Recognition (OCR) server
- ◆ Crawler



Notes:

In production environments, do not install a Data Security server on a Microsoft Exchange, ISA, or print server. These systems require abundant resources.

Operating system requirements

Supplemental Data Security servers must be running on one of the following operating system environments:

- ◆ Windows Server 2003 (32-bit) Standard or Enterprise R2 SP2
- ◆ Windows Server 2008 (64-bit) Standard or Enterprise R2
- ◆ Windows Server 2012 (64-bit)

Hardware requirements

Supplemental Data Security servers must meet the following hardware requirements.

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

Software requirements

The following requirements apply to all Data Security servers:

- ◆ For optimized performance, verify that the operating system's file cluster is set to 4096B. For more information, see the Websense knowledge article: "File System Performance Optimization."
- ◆ Windows installation requirements:
 - Set the partition to 1 NTFS Partition. For more information, see the Websense 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 Data Security Management Server host name must not include an underscore sign. Internet Explorer does not support such URLs.
 - Short Directory Names and Short File Names must be enabled. (See <http://support.microsoft.com/kb/121007>.)
 - Create a local administrator to be used as a service account. If your deployment includes more than one Data Security Server, use a domain account (preferred), or the use same local user name and password on each machine.
 - Be sure to set the system time accurately on the TRITON management server.

Antivirus

Exclude the following directories from antivirus scanning:

- ◆ The folder where Data Security 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\- ◆ %WINDIR%\Temp*. *
- ◆ The forensics repository (configurable; defaults to Websense folder)



Note

This document lists the default installation folders. You can configure the software to install to other locations.

The FP-Repository folder is usually located inside the installation folder.

Port requirements

The following ports must be kept open for supplemental Data Security servers:

Outbound

To	Port	Purpose
Data Security Management Server	17443	Incidents
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
Data Security Management Server	8892	Syslog
Data Security Management Server	139	File sharing
Data Security Management Server	445	File sharing
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Installation steps

1. Download the Websense installer (**WebsenseTRITON78xSetup.exe**) from mywebsense.com.
2. Launch the installer on the machine where you want to install the supplemental server.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the server software.

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



Important

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



Note

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

8. On the **Select Components** screen, select **Data Security Server**.
9. The **Fingerprinting Database** screen appears. To choose a location other than the default shown, use the **Browse** button.
10. The **Virtual SMTP Server** screen appears. This is because an SMTP agent is included with supplemental Data Security server installations.
 In the **Select Virtual Server** list, select the IIS virtual SMTP server that should be bound to the SMTP agent. The SMTP agent will monitor traffic that goes through this virtual server. If there multiple SMTP servers listed, the SMTP agent should typically be bound to Inbound.
 (See [Preparing a machine for the SMTP agent, page 71](#) for instructions on installing Microsoft IIS from Control Panel and configuring inbound and outbound SMTP Virtual Servers.)
11. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
12. In the **Register with the Data Security Server** screen specify the location and log on credentials for the TRITON management server.

FQDN is the fully-qualified domain name of a machine. The credentials should be for a Data Security administrator with System Modules permissions.

13. In the **Local Administrator** screen, supply a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.
14. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, the **Lotus Domino Connections** screen appears.

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



Important

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

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

-
- a. On the **Lotus Domino Connections** page, select the check box labeled **Use this machine to scan Lotus Domino servers**.
 - b. In the **User ID file** field, browse to one of the authorized administrator users, then navigate to the user’s **user.id** file.



Note

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

-
- c. In the **Password** field, enter the password for the authorized administrator user.
15. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

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

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

Data Security needs port 80 free.

In order to proceed with this installation, DSS will free up this port.

Click Yes to proceed OR click No to preserve your settings.

Clicking **No** cancels the installation.

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

16. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.
17. Log onto the Data Security manager and click **Deploy** to fully connect the supplemental server with the management server.

Installing Data Security agents

Below is a summary of the Data Security agents.

With the exception of the protector, mobile agent, and Data Endpoint, Data Security agents are installed using the Custom option of the standard Websense installer.

Note that the various agents become available only when you are performing the installation on a required server. For example, if you are running the installation wizard on an ISA server, the wizard knows this and lists the ISA agent as an option that you can install.

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

Agent	Description
Protector	The protector is a standard part of Websense Data Security deployments. It is a soft appliance with a policy engine and a fingerprint repository, and it supports analysis of SMTP, HTTP, FTP, plain text, and IM traffic that doesn't use SSL. The protector is a soft appliance with a policy engine and a fingerprint repository. For HTTPS traffic, the protector can integrate with proxies using ICAP. See Protector , page 39 for more information.
SMTP agent	SMTP is the protocol used for sending email to recipients outside the organization. The SMTP agent monitors SMTP traffic. It receives all outbound email from the mail server and forwards it to the Data Security policy engine. It then receives the analyzed email back from the policy engine, and blocks or forwards it to the mail gateway as directed. See SMTP agent , page 69 for more information.
ISA/TMG agent	The ISA agent receives all Web (HTTP or HTTPS) connections from a Microsoft ISA or Forefront TMG Server network and forwards them to the Data Security policy engine. It then receives the analyzed information back from the policy engine and forwards it to the recipients on the Web. See Microsoft ISA/TMG agent , page 75 for more information.
Endpoint agent	Data Endpoint monitors all data activity on endpoint machines and reports on data at rest on those machines. With the endpoint agent, you can monitor application operations such as cut, copy, paste, and print screen and block users for copying files, or even parts of files, to endpoint devices such as thumb drives, CD/DVD burners, and Android phones. The endpoint agent can also monitor or block print operations as well as outbound web posts and email messages. See Installing and Deploying Data Endpoint Clients for more information.

Agent	Description
Printer agent	The printer agent is installed on a Microsoft print server. It monitors data that is sent to network printers through optical character recognition (OCR) technology. See Printer agent, page 78 for more information.
FCI agent	The FCI agent is installed on a Windows Server 2012 machine running Microsoft File Server Resource Manager (FSRM). It augments the data classification performed using Microsoft File Classification Infrastructure (FCI). See FCI agent, page 84 for more information.
Web Content Gateway	A Data Security policy engine is embedded in Websense Content Gateway. No agent installation is required; however, the policy engine is not active until registered with a TRITON management server. See Content Gateway Help for registration instructions.
Email Security Gateway	A Data Security policy engine is embedded in Email Security Gateway. No agent installation is required; however, the policy engine is not active until registered with a TRITON management server. See the Email Security Manager Help for registration instructions.
Mobile agent	The mobile agent monitors and blocks data downloaded to mobile devices that perform synchronization operations with the Exchange server. With the mobile agent, you can monitor and block data transmitted in email messages, calendar events, and tasks. It is on a Websense appliance, or you can install it on your own hardware. The mobile agent supports ActiveSync, which is a wireless communication protocol used to push resources, such as email, from applications to mobile devices. See Mobile agent, page 53 for more information.
Integration agent	The Integration agent allows third-party products to send data to Websense Data Security for analysis. It is embedded in third-party installers and communicates with Data Security via a C-based API. See Integration agent, page 88 for more information.
Crawler	The crawler is the name of the agent that performs discovery and fingerprinting scans. The crawler is installed automatically on the TRITON Management Server and other Data Security servers. If you want to improve scanning performance in high transaction volume environments, you can install it stand-alone on another server as well. See The crawler, page 91 for more information.



Important

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

Protector

In this topic:

-
- ◆ [When to use the protector](#), page 39
 - ◆ [Deploying the protector](#), page 40
 - ◆ [Hardware requirements](#), page 43
 - ◆ [Recommended \(optional\) additional NICs for inline mode:](#), page 43
 - ◆ [Installing the protector software](#), page 45
 - ◆ [Configuring the protector](#), page 51
-

The protector is an essential component of Websense Data Security, providing monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. Using PrecisID technology, the protector can be configured to accurately monitor sensitive information-in-transit on any port.

When to use the protector

The protector works in tandem with the Data Security server. The Data Security server provides advanced analysis capabilities, while the protector sits on the network, intercepts traffic and can either monitor or block the traffic, as needed. The protector supports analysis of SMTP, HTTP, FTP, plain text, IM traffic (e.g., Yahoo, MSN, chat, and file transfer). The protector is also an integration point for third-party solutions that support ICAP.

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

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

If you want email blocking capabilities, you can use either the protector's explicit MTA mode or the SMTP agent (see below).

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

If you want to monitor or transparently block HTTP traffic, you can use the protector to do so, or you can integrate Data Security with Websense Content Gateway or another Web proxy.

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

The first decision that needs to be made when installing a protector is its location on the network. You can deploy the protector in SPAN/mirror port mode or in inline mode.

Deploying the protector

Most data-loss detection devices can be connected off the network, enabling them to sniff network traffic and monitor breaches. This monitoring method is useful because it does not interfere with traffic; however, it also does not enable the loss-prevention system to prevent (block) data losses—only to note and report them. In addition to monitoring mode, you can connect the Websense Protector to the network directly in the path of the traffic, enabling traffic to be blocked, quarantined and even terminated before it reaches its destination.

The following table depicts the available modes according to the selected topology.

Topology Service	SPAN/Mirror Port	Inline/Bridge
HTTP	Monitoring	Monitoring bridge Active (blocking) bridge
SMTP	Monitoring passive Mail Transfer Agent (MTA)	Monitoring bridge Mail Transfer Agent (MTA)
All Others	Monitoring	Monitoring
ICAP	Monitoring Blocking	Monitoring Blocking



Note

In both inline/bridge and SPAN/mirror port topology, Websense Data Security can be integrated with Web proxies. Blocking and monitoring modes are both available.

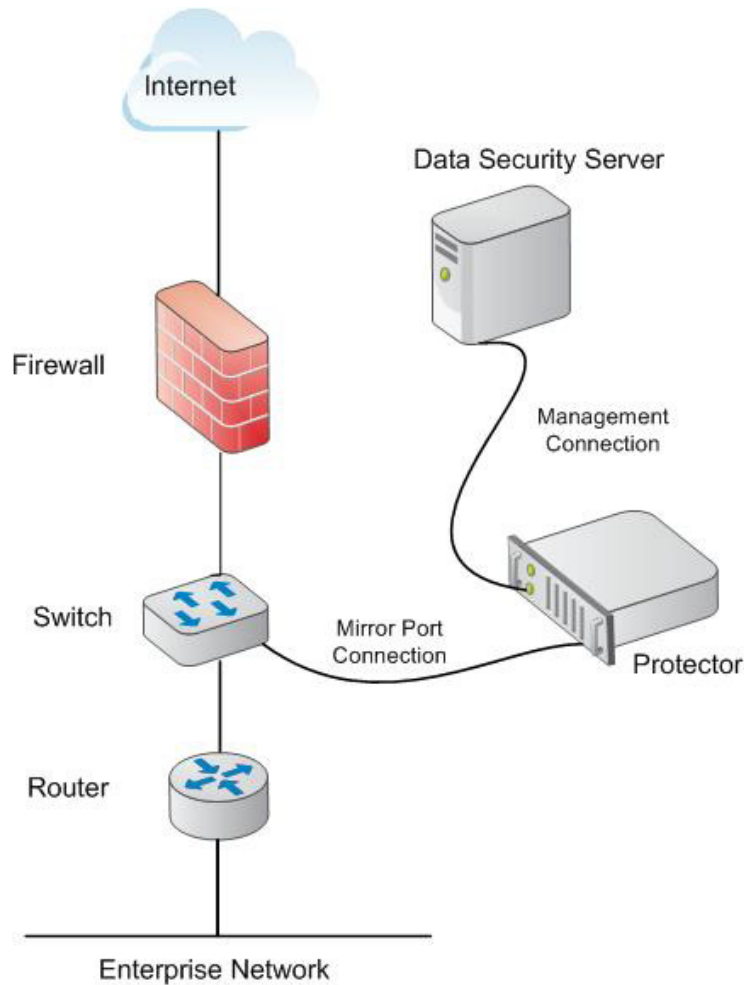
Deploying in SPAN/mirror port configuration

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

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

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

- ◆ Connect the protector to the Data Security server.



Deploying in inline configuration

In inline/bridge mode, configure the protector as a layer-2 switch directly in the path of your organization's traffic. In this configuration, the data security device functions passively, monitoring the traffic (as in monitoring mode), or actively, blocking traffic as necessary.

When using the Websense Protector in inline mode, the hardware and software failsafe mechanism is available only when using the certified bypass-server adapter NIC.

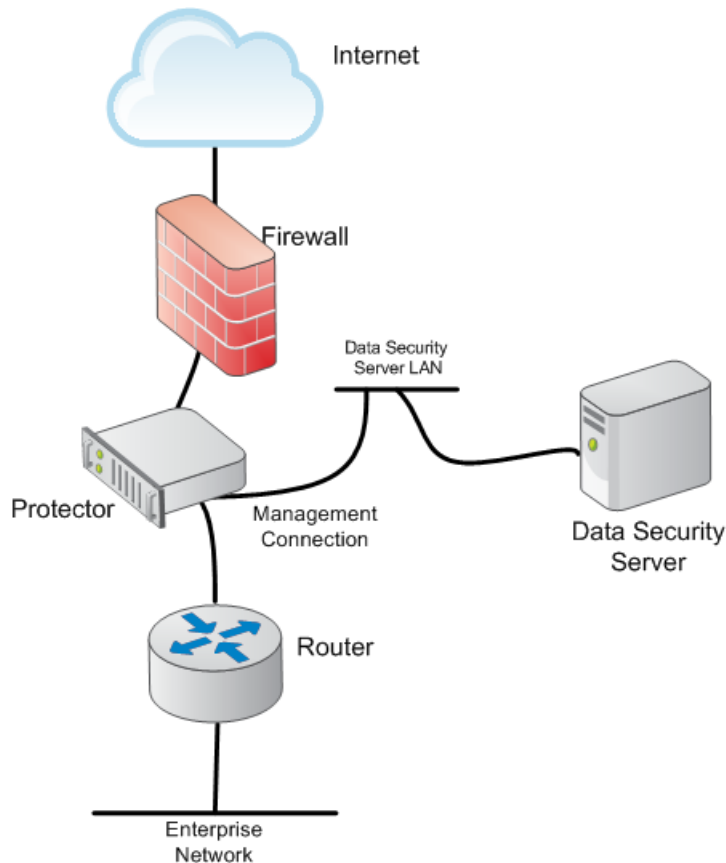
The following Silicom network cards (NIC SKUs) are supported by the Websense Protector:

- ◆ PEG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter
- ◆ PEG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter

- ◆ PXG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter
- ◆ PXG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter

The inline/bridge network setup is the same, regardless of whether the protector is activated in blocking or monitoring mode.

- ◆ The following figure depicts a sample setup for the Websense device in inline/bridge topology.
- ◆ Connect the eth0 interface of the protector and the Data Security server to the LAN for management purposes, or use the port set while running the installation wizard.
- ◆ Connect the protector to the outgoing connection and to your organization's internal network.



The 2 most common inline (bridge) topologies include:

- ◆ HTTP in active (blocking) mode
- ◆ HTTP and SMTP in monitoring mode

If you are planning to use one of these modes, when executing the Data Security Protector wizard, make sure the time, date and time zone are precise, and map eth0 to verify it is located on the main board. Connect eth0 of the protector to the LAN.

In inline network configuration, the protector can monitor or block traffic. Monitoring bridge mode monitors traffic. SMTP MTA and HTTP Active Bridge modes have both monitoring and blocking options.

Inline monitoring

In inline monitoring mode, the protector actually sits in the data path on the network—however, data is monitored and not blocked. This mode is particularly useful during the setup phase, when testing the protector to make sure configuration is accurate and network-appropriate, before enabling blocking capabilities on the network.

Inline blocking

In inline blocking mode (also known as active bridge mode), the protector sits in the data path on the network. All traffic that traverses the protector is analyzed either locally by the policy engine resident on the protector, or by a Data Security server if load balancing is set up.

The policy engine applies all policies as necessary before determining whether traffic is forwarded to its original destination. If data is detected that is supposed to be blocked, it is quarantined by the protector and does not reach its destinations. All traffic that does not match a policy and is not considered suspicious by the policy engine is forwarded by the protector to its original destination.

The protector communicates with the Data Security server for management purposes as well as for fingerprinting and deployment updates.

Hardware requirements

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

Protector	Minimum requirements	Recommended
CPU	2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent	2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent
Memory	2 GB	4 GB
Hard drives	2 - 72 GB	4 - 146 GB
Disk space	70 GB	292 GB
Hardware RAID	1	1 + 0
NICs	2 (monitoring), 3 (inline)	2 (monitoring), 3 (inline)

Recommended (optional) additional NICs for inline mode:

The following Silicom network cards are supported by the Data Security appliance. NICs SKUs are:

- ◆ PEG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI-Express Bypass Server Adapter
- ◆ PEG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI-Express Bypass Server Adapter
- ◆ PXG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter
- ◆ PXG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter
- ◆ PEG2Fi - Intel-based Dual-Port Fiber (SX) Gigabit Ethernet PCI-Express Server Adapter
- ◆ PXG2Fi - Intel-based Dual-Port Fiber (SX) Gigabit Ethernet PCI-X Server Adapter



Note

Websense does *not* support bypass products with -SD drivers. If you are ordering a NIC based on Intel chips 82546 or 82571, be sure to order them in non-SD mode.

Port requirements

The following ports must be kept open for the protector:

Outbound

To	Port	Purpose
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Management Server	17443	Syslog, forensics, incidents, mobile status
Next hop MTA	25**	SMTP
Websense Web Security	56992	Linking Service
Other	UDP 123	Inbound/outbound NTPD (available on the appliance yet disabled by default)

* This range is necessary for load balancing.

** Explicit MTA

Inbound

From	Port	Purpose
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Anywhere (including the Data Security manager)	22	SSH access

Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Explicit MTA	25**	SMTP
Explicit MTA	10025* *	SMTP, mail analysis

* This range is necessary for load balancing.
** Explicit MTA

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

Outbound		
To	Port	Purpose
Protector	1344	Receiving ICAP traffic
Inbound		
None		

Installing the protector software

Installing the Data Security protector comprises 3 basic steps:

1. [Configuring the network](#), page 45
2. [Installation steps](#), page 46
3. Configure the protector in the TRITON Unified Security Center. See [Final step: Verification](#), page 51.

Protector installations include:

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

Configuring the network

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

Make sure that firewalls or other access control devices on your network do not block ports used by the protector to communicate with the Data Security server (see [Protector](#), page 39).

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

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

Installation steps

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

To install the protector, do the following:

1. If you have purchased the Websense V5000 G2 Data Security Appliance, follow the instructions on its quick start poster to rack, cable, and power on the appliance.

If you are using your own hardware:

- a. Use either a direct terminal or connect via serial port to access the command line. For serial port connection, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:
 - 19200 baud
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control
 - b. The protector software is provided on an ISO image. Download the image, **WebsenseDataSecurityProtector78x.iso**, from [MyWebsense](#) and burn it to a CD.
 - c. Place the CD in the protector's CD drive and restart the machine.
 - d. An installer page appears. If you are using a regular keyboard and screen, type **kvm** and press **Enter**. If you are using a serial console, press **Enter**. The machine is automatically restarted.
2. You're prompted to enter a user name and password. Enter *admin* for both.

When the protector CLI opens for the first time, logging in as admin automatically opens the installation wizard. On subsequent attempts, type "wizard" at the command prompt to access the wizard.
 3. You have the option to install the Websense protector software or mobile agent software. Type **P** for Protector. Choose this mode whether you are deploying the protector inline or in a SPAN/mirror port configuration. For more information on deploying the protector inline, see [Deploying in inline configuration, page 41](#). For more information on deploying the protector in a SPAN/mirror port configuration, see [Deploying in SPAN/mirror port configuration, page 40](#).
 4. Follow the instructions given by the wizard to configure basic settings.

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

STEP 1: Accept license agreement

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

```
Step 1/8: License Agreement

                                WEBSense
                                SUBSCRIPTION AGREEMENT

IMPORTANT - THIS SUBSCRIPTION IS PROVIDED ONLY ON THE CONDITION THAT THE
SUBSCRIBER (REFERRED TO IN THIS AGREEMENT AS "SUBSCRIBER") AGREES TO THE TERMS
AND CONDITIONS SET FORTH IN THE FOLLOWING LEGAL AGREEMENT WITH WEBSense, INC.
AND/OR ONE OF ITS SUBSIDIARIES ("WEBSense"). READ THIS AGREEMENT CAREFULLY
BEFORE ACCEPTING IT. BY CLICKING ON THE "I AGREE" BUTTON BELOW OR BY USING THE
SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT,
AND THAT (1) YOU, ON BEHALF OF YOURSELF, OR (2) SUBSCRIBER, IF SUBSCRIBER IS A
BUSINESS, AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1.      Subscription and Grant of Right to Use. Subject to the terms and
conditions of this Agreement, Websense agrees to provide Subscriber the
subscription services ("Subscription") as described in the purchase commitment
mutually agreed upon between the parties ("Order"). Websense grants to
Subscriber as part of the Subscription a non-exclusive, nontransferable right
to use certain proprietary software applications ("Software"), proprietary
database(s) of URL addresses, applications and other valuable information
("Databases"), changes to the content of the Databases ("Database Updates")
and certain modifications or revisions to the Software ("Software Upgrades"),
together with applicable documentation and the accompanying media, if any,
(collectively, the "Products"). The Products are provided for the number of
Do you accept the license agreement? [Yes/no]: █
```

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

Data Security checks to see if your hardware meets the following requirements:

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

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

STEP 3: Set administrator password

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

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

```
Step 3/8: Administrator Password

Enter new admin password (Press [Enter] to leave unchanged):

Enter new root password:
Re-enter new root password: █
```

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

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

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

1. Enter a number 0-60 to indicate how long (in seconds) you’d like traffic simulated or press Enter to skip this step.
2. When prompted, choose the NIC index number of the management NIC or accept the default interface.

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

The protector has a set of NICs for intercepting traffic and one NIC
for use by the Data Security Management Server and SSH connections.
This NIC is also used to log onto the protector.

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

Available network interfaces:
(* - current Management Interface, BR - bridge member interface)
(0) * eth0 (driver: pcnet32 mac: 00:0C:29:61:9E:DE inet: 10.201.136.201/24
)
(1) eth1 (driver: pcnet32 mac: 00:0C:29:61:9E:E8 inet: 0.0.0.0/0)
(2) eth2 (driver: pcnet32 mac: 00:0C:29:61:9E:E8 inet: 0.0.0.0/0)
(3) eth3 (driver: pcnet32 mac: 00:0C:29:61:9E:E8 inet: 0.0.0.0/0)
(4) eth4 (driver: pcnet32 mac: 00:0C:29:61:9E:E8 inet: 0.0.0.0/0)
(5) eth5 (driver: pcnet32 mac: 00:0C:29:61:9E:E8 inet: 0.0.0.0/0)

Please choose a management interface number (0-5)[0]: _
```

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

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

```
The eth0 network interface has now been configured as the management interface.
You are asked below to confirm the configuration setting. Answering "Yes" confir
ms the configuration, "No" will delete the settings and restart this step of the
wizard.
Do you want to continue? [Yes/no]: yes
Enter the Management Interface IP address [10.201.136.201]:

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

Enter a broadcast address [10.201.136.255]:

Enter a new default gateway IP address
(Type 'Delete' to remove the default gateway) [10.201.136.11]: _
```

STEP 5: Define the host name and domain name

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

```
Step 5/8: Host Name and Domain

Enter Host Name [Protector1]:

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

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

STEP 6: Define the domain name server

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

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

No DNS servers defined

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

STEP 7: Set the date, time and time zone

1. Type the current time zone (to view a list of all timezones, type list).
2. Type the current date in the following format: dd-mmm-yyyy.
3. Type the current time in the following format: HH:MM:SS. Note that this is a 24-hour clock.

```
Step 7/8: Date and Time
Current timezone: GMT0
Enter a new timezone
(Press [Enter] to leave unchanged or type 'List' to view all avail
```

STEP 8: Register with a Data Security Server

In this step, a secure channel will be created connecting the protector to a Data Security Server. This can be the Data Security Management Server or a supplemental server, depending on your set up.

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

```
Step 8/8: Register with a Data Security Server

Enter the IP address of the Data Security Server to which this
protector will connect. This could be the Data Security Management
Server or a supplemental server. Enter the user name and password
of a TRITON - Data Security administrator who has an access role
with System Modules permissions.

If this step fails, you can run the wizard again or run 'wizard
securecomm' to skip previous steps.

Enter the FQDN or IP address of the Data Security Server:
Enter the user name of a TRITON - Data Security administrator:
Enter the password for this user:
```

2. Type the user name and password for a Data Security administrator that has privileges to manage system modules.

Final step: Verification

In the Data Security module of TRITON Unified Security Center, verify that the Websense Protector is no longer pending and that the icon displays its active status. Refresh the browser.

Click Deploy.

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

```
Attempting to establish secure communication with PA server... Succeeded.
Generating default ICAP configuration...

The configuration wizard has completed successfully.
Starting the monitoring service...
Starting PAMA Secure Communication...
Starting SMTP Blocking Service...
Starting PAMA Watchdog... started
~@pama#
~@pama#
```

The protector is now ready to be configured.

Configuring the protector

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

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

- ◆ Define the channels that the Websense Protector will monitor.
- ◆ Supply additional configuration parameters needed by the Websense Data Security Server to define policies for unauthorized traffic.

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

For more configuration information, see [Configuring the Protector](#) in the Data Security Manager Help system.

Setting up Bypass mode

Bypass can be used in the event that the Bypass Server Adapter NIC was ordered with the protector; it enables transparent failover in the event of protector failure. When Bypass is enabled, if the protector malfunctions or is powered off, traffic will

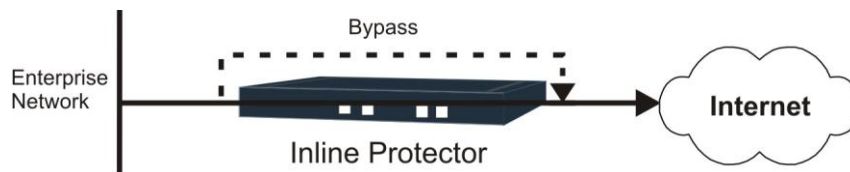
transparently pass through the protector to the external network. (Bypass mode is relevant only to the inline/bridge network topology.)



Important

Only certified Bypass Server Adapter NIC cards are tested and guaranteed to properly bypass the protector in the unlikely event of product failure.

When a certified Bypass Server Adapter NIC dual or quad network card is available on the protector, it's possible to enable the protector's bypass mode. Bypass is a failsafe mechanism that shorts the protector in the unlikely event of device failure, enabling all network traffic to pass transparently through the protector to the network.



You configure bypass mode in the Data Security manager user interface. Select **Settings > Configuration > System Modules**. Select the protector, then navigate to the Networking tab and select Enable bypass mode. Refer to the Data Security Manager Help system for more details.

By default, Bypass Mode is enabled. This means that when either a software or hardware problem occurs that causes the protector to malfunction, the protector will automatically be bypassed and the (unanalyzed) traffic will continue to pass to the outside network. If Bypass is disabled, when a malfunction occurs all traffic will be blocked and won't reach its intended destination.

Manual bypass

To force the protector into bypass mode, causing all traffic to pass transparently through the protector, do the following:

1. Log onto the Data Security manager.
2. Select **Settings > Deployment > System Modules**.
3. Select the protector to bypass.
4. In the Edit Protector dialog, select the Networking tab.
5. Under Network Interfaces, click **Edit**.
6. Select the check box labeled, **Enable bypass mode**.
7. Select **Force bypass**.
8. Click **OK** twice.
9. Click **Deploy**.

If you are experiencing network problems, you can verify that problems are not within the Data Security software, by setting Manual Bypass to **On** and noting if problems persist.

Mobile agent

In this topic:

- ◆ [Deploying the mobile agent](#), page 53
 - ◆ [Hardware requirements](#), page 55
 - ◆ [Installing the mobile agent software](#), page 56
 - ◆ [Configuring the mobile agent](#), page 66
 - ◆ [Configuring a mobile DLP policy](#), page 68
-

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.

Deploying the mobile agent

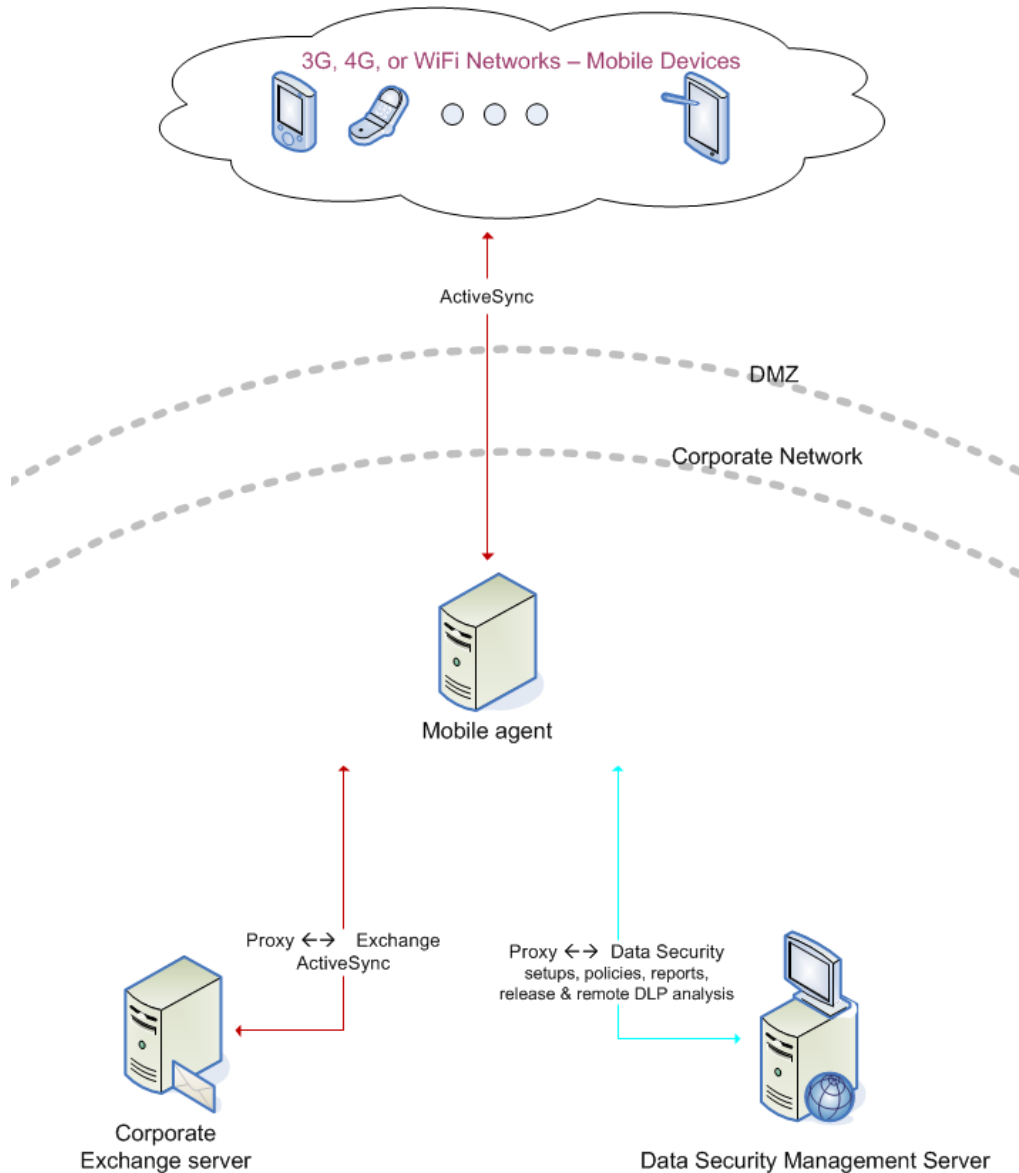
In your network, the appliance connects to the Data Security Management Server and to your Microsoft Exchange agent to provide this function. DLP analysis is done on the appliance or on other Data Security servers (rather than on the management server) to optimize performance and balance the load.

Outside your DMZ, the mobile agent connects to any Microsoft ActiveSync-compatible mobile device over 3G and wireless networks, such as i-pads, Android mobile phones, and i-phones. (ActiveSync is a wireless communication protocol used to push resources, such as email, from applications to mobile devices.)

Unlike the protector, the mobile agent appliance acts as a reverse proxy, because it retrieves resources, such as email, from the Exchange server on behalf of the mobile device.

The following diagram illustrates the system architecture of a typical mobile agent deployment. Depending on your network and security requirements, you can also go

through an edge device, such as a Microsoft ISA Server, that acts as a reverse proxy to the mobile agent.



For system requirements, see [Hardware requirements, page 55](#).

For the default port numbers used by the mobile agent, see [Hardware requirements, page 55](#). If you have a security policy in place, exclude these ports from that policy so the mobile agent can operate properly. You can lock down or harden your security systems once these ports are open.

Deploying the Data Security mobile agent comprises the following basic steps:

1. [Installing the mobile agent software, page 56](#)
2. [Configuring the mobile agent, page 66](#)
3. [Configuring a mobile DLP policy, page 68](#)

Mobile agent installations include:

- ◆ A policy engine
- ◆ Secondary fingerprint repository (the primary is on the management server)

Hardware requirements

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

Mobile Agent	Minimum requirements	Recommended
CPU	4 core processors (for example, Single quad or two dual core processors), 2.0 GHz Intel Xeon or AMD equivalents	4 core processors (for example, Single quad or two dual core processors), 2.0 GHz Intel Xeon or AMD equivalents
Memory	8 GB	8 GB
Hard drives	2 - 72 GB	4 - 146 GB
Disk space	70 GB	292 GB
Hardware RAID	1	1 + 0
NICs	2	2

Port requirements

The following ports must be kept open for the mobile agent:

Outbound

To	Port	Purpose
Data Security Management Server	17443	Syslog, forensics, incidents, mobile status
Data Security Management Server	80	Fingerprint sync
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Microsoft Exchange Server	80/443	ActiveSync (user defined using the Data Security manager)
Websense Web Security	56992	Linking Service
Other	UDP 123	Inbound/outbound NTPD (available on the appliance yet disabled by default)

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
------	------	---------

Data Security Management Server	5820	Settings deployment
Mobile Devices	80/443	ActiveSync (user defined using the Data Security manager)
Data Security Management Server	8892	Management
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Anywhere (including the Mobile agent)	22	SSH access
Data Security Server	5443	Release quarantined messages

* This range is necessary for load balancing.

Installing the mobile agent software

The mobile agent must be installed on hardware that meets the requirements described in [Hardware requirements, page 55](#). Websense appliances meet these requirements, or you can host the agent on your own Linux-based hardware.



Note

For best performance, make sure that the mobile agent is located in close proximity to the back-end server.

You access the installation wizard for your mobile agent through a putty Command Line Interface (CLI).

To install the mobile agent, do the following:

1. If you have purchased the Websense V5000 G2 Data Security Appliance, follow the instructions on its quick start poster to rack, cable, and power on the appliance.

If you are using your own hardware:

- a. Use either a direct terminal or connect via serial port to access the command line. For serial port connection, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:
 - 19200 baud
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control
- b. The mobile agent software is provided on an ISO image. Download the image, **WebsenseDataSecurityProtector78x.iso**, from [MyWebsense](#) and burn it to a CD.
- c. Place the CD in the protector's CD drive and restart the machine.

- d. An installer page appears. If you are using a regular keyboard and screen, type **kvm** and press **Enter**. If you are using a serial console, press **Enter**. The machine is automatically restarted.
2. You're prompted to enter a user name and password. Enter *root* for user name and *admin* for password.

```

Websense Data Security Protector 7.6.3 (CentOS 5.5)
Kernel 2.6.18-194.17.4.el5PAE on an i686

protector-29170 login: root
Password: █

```

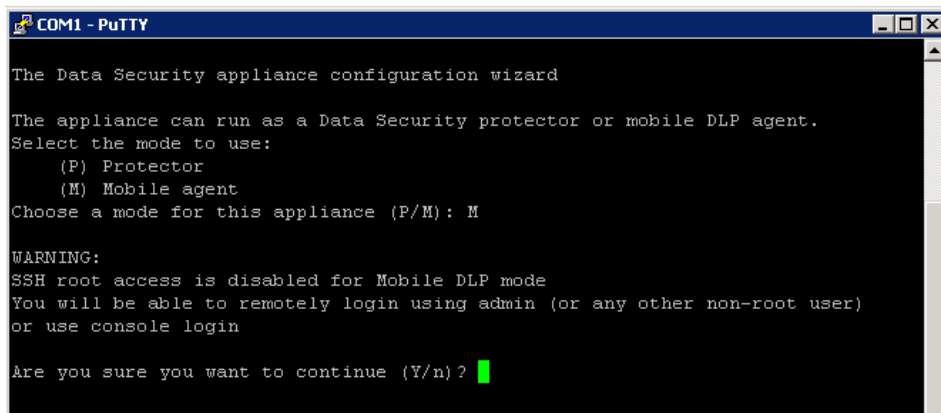
3. To access the wizard, type "wizard" at the command prompt, and press **Enter**.

```

~ root@protector-29170# wizard █

```

4. You have the option to install the Websense protector software or mobile agent software. Type **M** for Mobile agent.



```

COM1 - PuTTY
The Data Security appliance configuration wizard

The appliance can run as a Data Security protector or mobile DLP agent.
Select the mode to use:
  (P) Protector
  (M) Mobile agent
Choose a mode for this appliance (P/M): M

WARNING:
SSH root access is disabled for Mobile DLP mode
You will be able to remotely login using admin (or any other non-root user)
or use console login

Are you sure you want to continue (Y/n)? █

```

5. Follow the instructions given by the wizard to configure basic settings. When the wizard requires data entry, it prompts you. In some cases, a default setting is provided:
 - Capital letter: Shows the default value, such as Yes/no for a yes/No prompt.
 - Square brackets ([]): Shows the current value and is usually followed by text, such as: Press [Enter] to leave as is.

If the default setting is acceptable, press <Enter> to keep the default value.

STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down/ scroll / space keys to read/scroll to the end of the agreement.

```

COM1 - PuTTY
WEBSENSE
SUBSCRIPTION AGREEMENT

THE PRODUCTS ARE PROVIDED ONLY ON THE CONDITION THAT THE SUBSCRIBER AGREES
TO THE TERMS AND CONDITIONS IN THIS SUBSCRIPTION AGREEMENT ("AGREEMENT")
BETWEEN SUBSCRIBER AND WEBSENSE.
BY ACCEPTING THIS AGREEMENT OR BY USING THE PRODUCTS, SUBSCRIBER ACKNOWLEDGES
IT HAS READ, UNDERSTANDS, AND AGREES TO BE BOUND BY THIS AGREEMENT.

1. Definitions.
"Databases" means proprietary database(s) of URL addresses, email addresses,
  Malware, applications and other valuable information.
"Database Updates" means changes to the content of the Databases.
"Order" means a purchase commitment mutually agreed upon between
  (1) Websense and Subscriber, or
  (2) a Websense authorized reseller and Subscriber.
"Permitted Capacity" means the Permitted Number of Seats set forth in the Order.
"Seat" means
  (i) each computer, electronic appliance or device that is
    authorized to access or use the Products, directly or indirectly; or
  (ii) for SaaS Email a separate email address or account that receives
    electronic messages or data within Subscriber's email system or network.
  For (ii), up to 5 aliases may be considered one Seat. (For example:
--More--(4*)[Press space to continue, 'q' to quit.]

```

Carefully read the license agreement and when prompted, type yes to accept the license agreement.

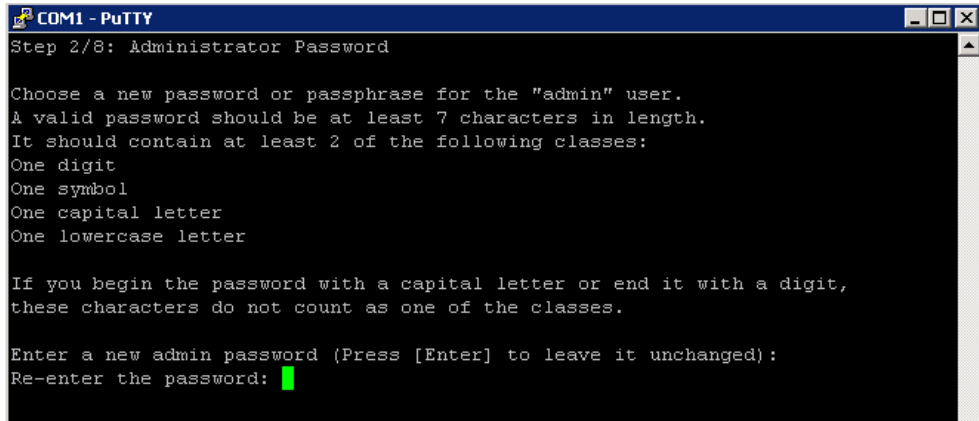
```

COM1 - PuTTY
(1) the state and federal courts in San Diego, California, USA, for all
claims arising in or related to the United States, Canada or Mexico;
(2) the competent courts in England and Wales for all claims arising in or
related to the United Kingdom; or (3) the competent courts in Dublin,
Ireland for all other claims. Both parties expressly waive any objections or
defense based upon lack of personal jurisdiction or venue. Neither party
will be liable for any delay or failure in performance to the extent the
delay or failure is caused by events beyond the party's reasonable control,
including, fire, flood, acts of God, explosion, war or the engagement of
hostilities, strike, embargo, labor dispute, government requirement, civil
disturbances, civil or military authority, disturbances to the Internet, and
inability to secure materials or transportation facilities. This Agreement
constitutes the entire agreement between the parties regarding the subject
matter herein and the parties have not relied on any promise,
representation, or warranty, express or implied, that is not in this
Agreement. Any waiver or modification of this Agreement is only effective if
it is in writing and signed by both parties or posted by Websense at
http://www.websense.com/legal. If any part of this Agreement is found
invalid or unenforceable by a court of competent jurisdiction, the remainder
of this Agreement shall be interpreted so as reasonably to affect the
intention of the parties. Websense is not obligated under any other
agreements unless they are in writing and signed by an authorized
representative of Websense.
Do you accept the license agreement? (y/n)? y

```

STEP 2: Set administrator password

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



```
COM1 - PuTTY
Step 2/8: Administrator Password

Choose a new password or passphrase for the "admin" user.
A valid password should be at least 7 characters in length.
It should contain at least 2 of the following classes:
One digit
One symbol
One capital letter
One lowercase letter

If you begin the password with a capital letter or end it with a digit,
these characters do not count as one of the classes.

Enter a new admin password (Press [Enter] to leave it unchanged):
Re-enter the password: █
```



Important

A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

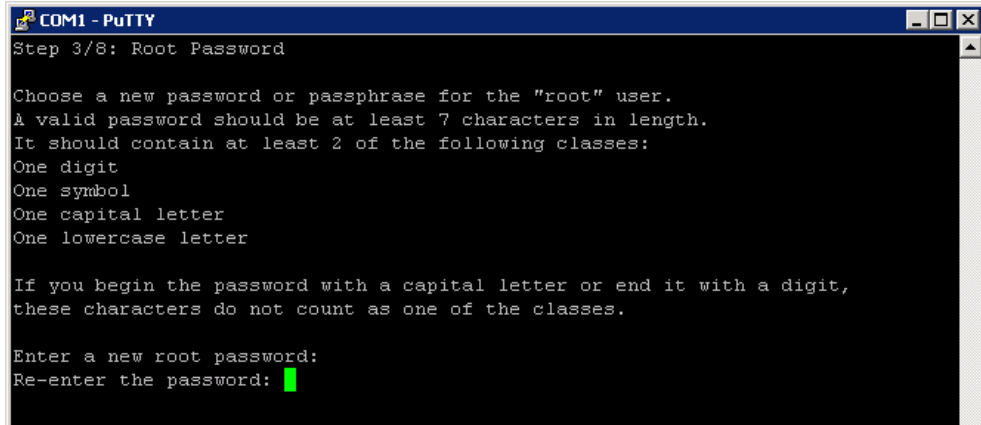
- ◆ One digit
- ◆ One symbol
- ◆ One capital letter
- ◆ One lowercase letter

If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

The Operating System (OS) prompts you to change (refresh) your password every 90 days.

STEP 3: Set root password

Type in and confirm a new password for the root user. The root account provides full access to the device and should be used carefully.



```
COM1 - PuTTY
Step 3/8: Root Password

Choose a new password or passphrase for the "root" user.
A valid password should be at least 7 characters in length.
It should contain at least 2 of the following classes:
One digit
One symbol
One capital letter
One lowercase letter

If you begin the password with a capital letter or end it with a digit,
these characters do not count as one of the classes.

Enter a new root password:
Re-enter the password: █
```



Important

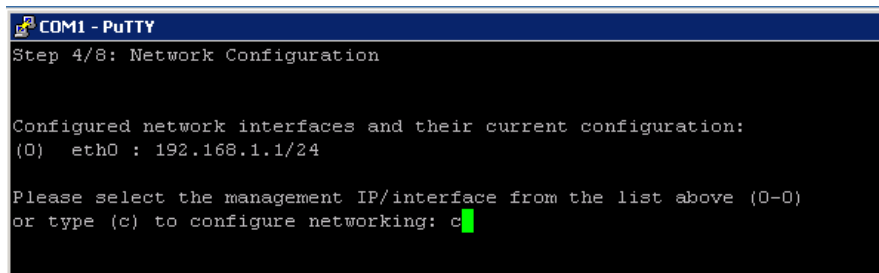
A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

- ◆ One digit
- ◆ One symbol
- ◆ One capital letter
- ◆ One lowercase letter

If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

STEP 4: Network configuration

1. Select the network interface (NIC) from the list of available NICs (eth0 by default), or for advanced configuration, type c.

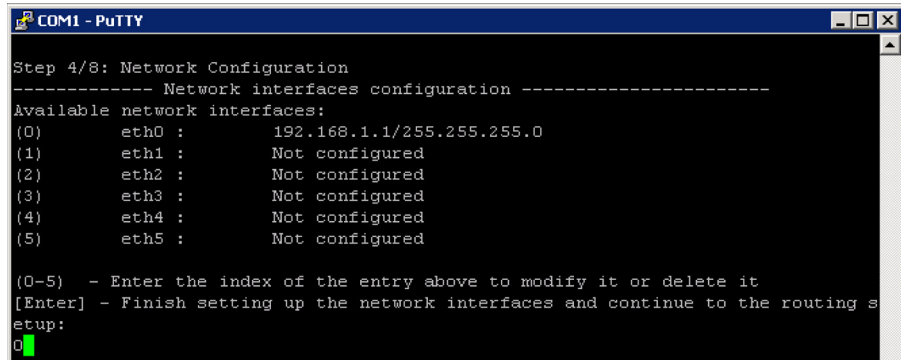


```
COM1 - PuTTY
Step 4/8: Network Configuration

Configured network interfaces and their current configuration:
(0) eth0 : 192.168.1.1/24

Please select the management IP/interface from the list above (0-0)
or type (c) to configure networking: c █
```


2. To configure your NIC, choose the NIC index number from the list of NICs that display on the wizard.



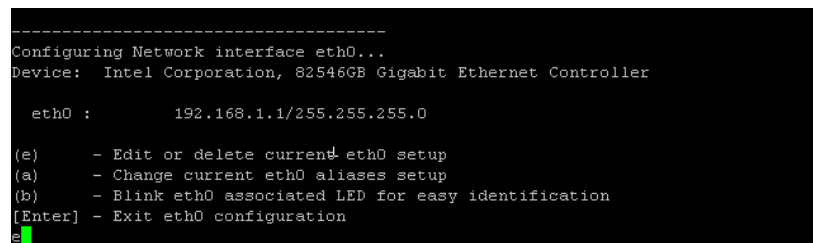
```

COM1 - PuTTY
Step 4/8: Network Configuration
----- Network interfaces configuration -----
Available network interfaces:
(0)   eth0 :      192.168.1.1/255.255.255.0
(1)   eth1 :      Not configured
(2)   eth2 :      Not configured
(3)   eth3 :      Not configured
(4)   eth4 :      Not configured
(5)   eth5 :      Not configured

(0-5) - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing s
etup:
0

```

3. To configure the NIC that you selected, do one of the following:
 - a. Type e to configure the NIC that you selected. You are prompted to define details for the NIC, such as IP address, network address, and gateway (only for the first NIC that you define). You do not need to specify the gateway for subsequent NICs that you want to define.
 - b. Type a to change the current NIC alias address setup.
 - c. Type b for LEDs to blink on that port.
 - d. Type Enter to exit and continue setting other NICs, if required.



```

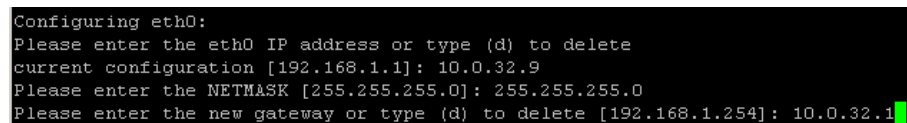
-----
Configuring Network interface eth0...
Device: Intel Corporation, 82546GB Gigabit Ethernet Controller

eth0 :      192.168.1.1/255.255.255.0

(e) - Edit or delete current eth0 setup
(a) - Change current eth0 aliases setup
(b) - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration
e

```

4. To define the properties for the NIC:
 - a. Type the IP address.
 - b. Type the network prefix. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 255.255.255.0 for eth0.
 - c. Type the IP address for the default gateway to be used to access the network. This configuration is only for the first NIC that you configured.



```

Configuring eth0:
Please enter the eth0 IP address or type (d) to delete
current configuration [192.168.1.1]: 10.0.32.9
Please enter the NETMASK [255.255.255.0]: 255.255.255.0
Please enter the new gateway or type (d) to delete [192.168.1.254]: 10.0.32.1

```

- d. After you have configured your NIC, you can redefine it (change the IP address, network prefix, or gateway) or remove it (type e, then d) if necessary.

```

-----
Configuring Network interface eth0...
Device: Intel Corporation, 82546GB Gigabit Ethernet Controller

eth0 :      192.168.1.1/255.255.255.0

(e)  - Edit or delete current eth0 setup
(a)  - Change current eth0 aliases setup
(b)  - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration
e

```



Note

If you type **Enter**, a list of available NICs display, allowing you to define other NICs.

- e. Type a NIC index number to configure another NIC (or reconfigure the same NIC), or type Enter to finish setting up the NICs and continue to the routing setup.

```

COM1 - PuTTY
----- Network interfaces configuration -----
Available network interfaces:
(0) eth0 :      192.168.1.1/255.255.255.0
(1) eth1 :      Not configured
(2) eth2 :      Not configured
(3) eth3 :      Not configured
(4) eth4 :      Not configured
(5) eth5 :      Not configured

(0-5) - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing s
etup:
0

```

- f. Type one of the following options:
- Enter: Accept the routing configuration.
 - Index: Modify or delete a routing entry index.
 - a: Add a routing entry.

```

COM1 - PuTTY
Step 4/8: Network Configuration
----- Routing table configuration -----

(0): default 10.0.32.1 (dev eth0)

(0) - Index of entry above - Modify or delete an entry
(a) - Add a new route entry
[Enter] - Exit routing configuration
a

```

**Note**

If the IP address of the Data Security server is not on the same subnet as the one specified for the mobile management NIC, a gateway is required to tell the mobile agent how to communicate with the Data Security server.

- g. To store these network definitions, type Y.

```
This wizard is about to reload your network.
Running services may disconnect during this process.
Do you want to continue (Y/n) Y
```

**Note**

After you finish routing the configuration, you are prompted to store the network configuration.

- ◆ If you type **n**, the network configuration is not saved, and you are prompted to configure the network again.
- ◆ If you type **y**, the details for the network configuration are saved and the network service is reloaded with the new parameters. The new parameters, such as IP address, network prefix, and gateway for the NIC display on the wizard.

5. Type the index number of the Management NIC you have chosen, or type **c** to define the network parameters. This NIC can be used for other purposes, such as SSH connections, access points for mobile devices, and Exchange communications.

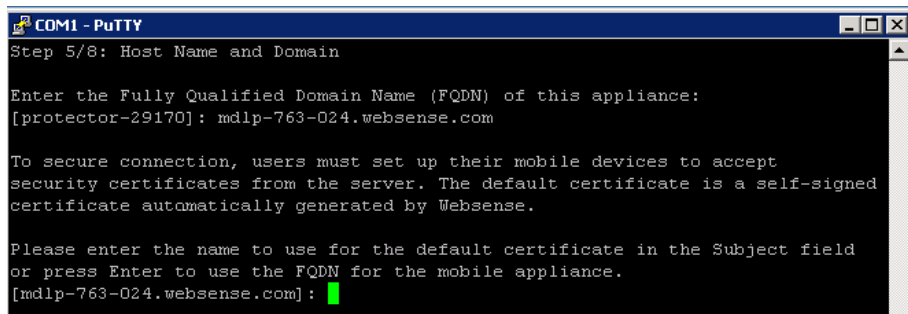
```
COM1 - PuTTY
Step 4/8: Network Configuration

Configured network interfaces and their current configuration:
(0) eth0 : 10.0.32.9/24

Please select the management IP/interface from the list above (0-0)
or type (c) to configure networking: 0
```

STEP 5: Define the host name

1. Type the Fully Qualified Domain Name (FQDN) for the mobile appliance.



```

COM1 - PuTTY
Step 5/8: Host Name and Domain

Enter the Fully Qualified Domain Name (FQDN) of this appliance:
[protector-29170]: mdlp-763-024.websense.com

To secure connection, users must set up their mobile devices to accept
security certificates from the server. The default certificate is a self-signed
certificate automatically generated by Websense.

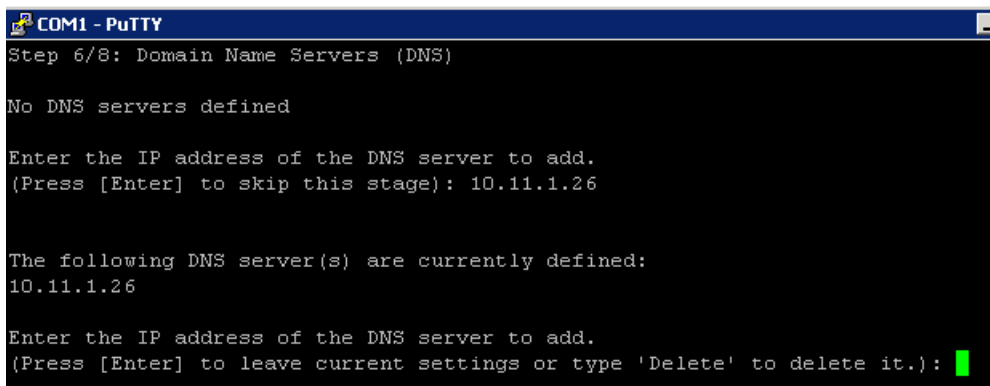
Please enter the name to use for the default certificate in the Subject field
or press Enter to use the FQDN for the mobile appliance.
[mdlp-763-024.websense.com]: █

```

2. Type the name to use for the default security certificate in the Subject field.
This can be used to secure the connections between mobile devices and the mobile agent using the default certificate. The default certificate is a self-signed certificate automatically generated by Websense.

STEP 6: Define the domain name server

Optionally, in the wizard, type the IP address of the Domain Name Server (DNS) that will service this mobile agent. A DNS will allow access to other network resources using their names instead of their IP addresses.



```

COM1 - PuTTY
Step 6/8: Domain Name Servers (DNS)

No DNS servers defined

Enter the IP address of the DNS server to add.
(Press [Enter] to skip this stage): 10.11.1.26

The following DNS server(s) are currently defined:
10.11.1.26

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

```

**Important**

Type the IP address of the DNS server if you identify the back-end Exchange server by its host name (using the Data Security GUI) instead of by its IP address.

STEP 7: Set the date, time and time zone

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

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

```

COM1 - PuTTY
Step 7/8: Date and Time

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

Current date: 11/20/2011
Enter new date in dd-mm-yy format
(Press [Enter] to leave unchanged):

Current time: 10:54:34
Enter time in HH:mm:ss format (24-hour format)
(Press [Enter] to leave unchanged): █

```

STEP 8: Register with a Data Security Server

In this step, a secure channel will be created connecting the mobile agent to a Data Security Server. This can be the Data Security Management Server or a supplemental server, depending on your set up.

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

```

COM1 - PuTTY
Step 8/8: Register with a Data Security Server

Enter the IP address or the FQDN of the Data Security Server to which this
Mobile DLP Agent will connect.
This can be the Data Security Management server or a supplemental server.

Enter the IP address or the FQDN of the Data Security Server: 10.0.14.14
Enter the user name of a TRITON - Data Security administrator: admin
Enter the password for this user:

Attempting to establish secured communication with the
DSS Management Server.../opt/websense/rproxy/log/registration.log
Succeeded.

ip_tables: (C) 2000-2006 Netfilter Core Team
Netfilter messages via NETLINK v0.30.
ip_conntrack version 2.4 (8192 buckets, 65536 max) - 228 bytes per conntrack

NOTE:
For best practice, reboot this appliance to disable IPv6 capabilities.

Please press [Enter] to exit this wizard. █

```

2. Type the user name and password for a Data Security administrator that has privileges to manage system modules.

3. Type Enter to exit the wizard. A message displays stating that the configuration was successful.

```
The configuration wizard has completed successfully.  
~ root@protector-29170#
```

Step 9: Reboot the mobile agent appliance

For best practice, reboot the mobile agent appliance. You can reboot later if desired. This completes the IPv6 disabling process that the wizard starts.

Final step: Verification

In the Data Security module of TRITON Unified Security Center, verify that the Websense mobile agent is no longer pending and that the icon displays its active status. Refresh the browser.

Click Deploy.

The mobile agent is now ready to be configured. See [Configuring the mobile agent](#), page 66 for instructions.



Note

If you reboot, make sure that the mobile agent appliance is on before you configure the mobile agent.

Configuring the mobile agent

1. Log on to the Data Security manager.
2. Navigate to **Settings > Deployment > System Modules**.
3. Verify that the mobile agent is available on the System Modules page.
4. Double-click Mobile agent.
5. Click the Connection tab, then define the connections: Exchange and Mobile Devices. For more information, see the [Data Security Manager Help](#).
 - a. For Exchange Connection, supply the domain and name or IP address of the Exchange server. Ensure a port number is specified.
 - If you select the Use secure connection (SSL) check box, the port number defaults to 443.

- If you do not select the Use secure connection (SSL) check box, the port number defaults to 80.

**Important**

If the Exchange server is specified by name, make sure local resolving is properly configured to resolve this name. In addition, if an edge-like device is used (for example, ISA), ensure there are no loops through the device.

- b. For Mobile Devices Connection, supply the following information: IP address of the mobile agent and port number. To use all IP addresses, select All IP addresses from the IP address drop-down list.

**Note**

The IP address of the mobile agent was defined during the installation of the mobile device, when configuring the network settings.

6. Optionally, if you secure connections between mobile devices and the mobile agent, you can use one of 2 certificate options:
 - Self-signed certificate (default option)
 - A self-signed certificate is signed by Websense.
 - Custom certificate
 - A custom certificate is officially signed by a Certificate Authority (CA).
 - a. Click Browse to locate and upload your public certificate.
 - b. Click Browse to locate and upload your private key.
 - c. Optionally, select the Add chained certificate check box, and click Browse to locate and upload your chained certificate.

For more information, see the [Data Security Manager Help](#).

7. Click the Analysis tab and then select a mode: Blocking or Monitoring. Click the Analysis tab, then configure the Mode.



Note

When you select Blocking mode, it is best practice to:

- ◆ Select the **Allow on fail** option (the default option is **Block on fail**). Selecting **Allow on fail** enables failed messages to be received on the mobile device. If you do not select **Allow on fail**, these messages will be dropped and are not tracked nor released.
- ◆ Define the sender's email address, outgoing mail server, and port to **Notify Users of Breach**. To do so, navigate to **Settings > System > Alerts > Email Properties**.

For more information, see the [Data Security Manager Help](#).

8. Navigate to **Main > Resources > Notifications** and select the mobile policy violation template. Add sender details, then use the Outgoing mail server field to define a next hop relay for outbound mail. If you do not, the mobile agent may not send block notifications.
9. Click **Deploy**.
Wait for the agent to fully deploy. This may take a few minutes.



Tip

You can also configure the mobile agent for high-availability. High-availability enables mobile devices to run seamlessly and continuously in the event of a system outage (such as hardware or software failure).

For more information about configuring the mobile agent for high-availability, refer to the document [Mobile DLP agent using cluster solutions](#).

Configuring a mobile DLP policy

To begin analysis, configure the mobile DLP policy or create a custom policy. To configure the mobile DLP policy, navigate to **Main > DLP Policies > Mobile DLP Policy**. See the [Data Security Manager Help](#) for more configuration information.

To create a custom policy, navigate to **Main > DLP Policies > Manage Policies**. Select **Mobile Email** on the Destination tab for each rule to support Mobile events.

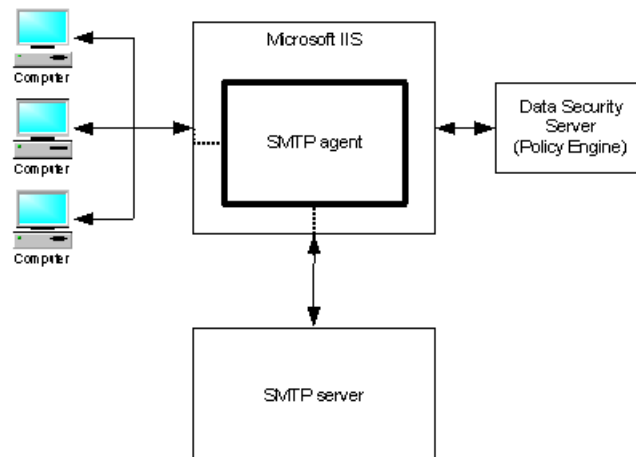
SMTP agent

In this topic:

- ◆ [Operating system requirements, page 70](#)
- ◆ [Port requirements, page 70](#)
- ◆ [Preparing a machine for the SMTP agent, page 71](#)
- ◆ [Installing the SMTP agent, page 72](#)
- ◆ [Testing the SMTP agent, page 73](#)

The Websense Data Security SMTP agent is installed on a Data Security server or on another Windows server equipped with Microsoft Internet Information Services (IIS) v6.

It receives all outbound email from the mail server and forwards it to a Websense Data Security Policy Engine. The SMTP agent then receives the analyzed email back from the policy engine. Depending on the analysis, SMTP agent blocks the email or forwards it to the mail gateway. When installed on the Data Security Management server or supplemental Data Security server, the SMTP agent uses the local policy engine of those servers to analyze email, unless load balancing has been configured, in which case it uses the specified policy engine. The SMTP agent supports permit, block, and encrypt actions.



Websense recommends you use the SMTP agent whenever you want the ability to block SMTP traffic in a production environment. (If you need only monitor SMTP traffic, the protector may be a better choice for you.)

To use the SMTP agent, you need to configure your corporate email server to route email to it. (The agent becomes a MTA, accepting responsibility for delivery of mail.)

When the agent is installed on a Data Security server, the SMTP traffic is analyzed by the local policy engine. When it is installed as a stand-alone agent, email messages

that are sent to the agent are sent to a Data Security server for analysis (whichever server the SMTP agent is registered with). You can configure Websense Data Security to block or quarantine flagged messages.

If an SMTP email transaction was blocked or quarantined, the administrator responsible for handling this incident can release this incident to those recipients originally blocked from receiving the content.

The SMTP agent is usually not the final server in the chain of custody before the email leaves the enterprise. Email is more frequently passed along to another MTA that provides additional processing (anti-virus scanning, for example).

If you have multiple mail servers, you can deploy multiple SMTP agents or you can have one SMTP agent and configure load balancing between the SMTP agent and the outgoing mail server. If this is not built into your SMTP server, you can use an external load balancer to achieve this.

Operating system requirements

The server must be running on the following operating system environments:

- ◆ Windows Server 2003 (32-bit)
 - Standard or Enterprise R2
 - Standard or Enterprise R2 SP2
- ◆ Windows Server 2003 (64-bit)
 - Standard or Enterprise R2

Port requirements

The following ports must be kept open for the SMTP agent:

Outbound

To	Port	Purpose
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Next hop MTA	25**	SMTP for inbound/outbound traffic

* This range is necessary for load balancing.

** This is default. Other port can be configured.

Inbound

From	Port	Purpose
Previous MTA	25*	SMTP for inbound/outbound traffic

* This is default. Other port can be configured.

Preparing a machine for the SMTP agent

The following procedure describes how to prepare a Windows 2003 Server for the Data Security SMTP agent.

1. Install Microsoft IIS with SMTP.
 - a. In Windows control panel, select **Add/Remove programs > Windows Components**.
 - b. Select **Application Server**, and then click **Details**.
 - c. Select **Internet Information Services (IIS)**, and then click **Details**.
 - d. Select **SMTP Service**, and then click **Details**.
 - e. Click **OK** 3 times to close the windows.
 - f. Click **Next** to configure and install the components.
2. Configure the SMTP Service.
 - a. In IIS Manager, right-click the Default SMTP Virtual Server and rename it to "Inbound".
 - b. Right-click the Inbound server and select **Properties**.
 - c. Select the Messages tab, and then deselect all message "Limits". (These should be enforced by the mail server.)
 - d. Select the Delivery tab, and then click **Outbound Connections**.
 - e. Set the TCP port to 10025 and click **OK**.
 - f. Click **Advanced** and set the Smart host to [127.0.0.1].

Recommended: For increased security, you can change the relay settings for the Inbound mail server to only allow relay mail from your Mail Server's IP. The relay settings are under Access > Relay > Only the list below.

3. Add a new SMTP Virtual Server in IIS Manager.
 - a. Right-click the server name, select **New > SMTP Virtual Server**.
 - b. Using the resulting wizard, configure the following settings:
Name: Outbound
IP: 127.0.0.1
Port: 10025
Home Directory: C:\inetpub\outbound

Recommended: For increased security, you can change the relay settings for the Outbound mail server to only relay mail from itself (127.0.0.1 as well as any IPs assigned to the server). If you plan on using this as the release or notification gateway, make sure you also allow relaying from the Data Security Management Server. The relay settings are under Access > Relay > Only the list below.

Optional: If your next-hop MTA requires Transport Layer Security (TLS), you can enable and configure the options under Delivery > Outbound Security.

Installing the SMTP agent

1. If your IIS machine has a 32-bit operating system, download the Websense installer (**WebsenseTRITON78xSetup.exe**) from mywebsense.com where x is the version number.

On 64-bit machines, download **WebsenseDataSecurityAgents78x-x64.msi** instead.

2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

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



Important

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



Note

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

8. On the **Select Components** screen, select **SMTP agent** and then **Entire feature will be installed on local hard drive**. If this is a stand-alone server, deselect all other options, including Data Security Server.
9. The **Virtual SMTP Server** screen appears.
In the **Select Virtual Server** list, select the IIS virtual SMTP server that should be bound to the SMTP agent. The SMTP agent will monitor traffic that goes through this virtual server. If there multiple SMTP servers listed, the SMTP agent should typically be bound to Inbound.
(See [Preparing a machine for the SMTP agent, page 71](#), for instructions on installing Microsoft IIS from Control Panel and configuring inbound and outbound SMTP Virtual Servers.)
10. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.

11. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server. FQDN is the fully-qualified domain name of a machine.
12. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.
Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.
If the following message appears, click **Yes** to continue the installation:
*Data Security needs port 80 free.
In order to proceed with this installation, DSS will free up this port.
Click Yes to proceed OR click No to preserve your settings.*
Clicking **No** cancels the installation.
A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.
13. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete.
14. Click **Finish**.

Before cutting over the live mail flow, be sure to test relaying through all mail servers as described in [Testing the SMTP agent, page 73](#). The easiest way to test your installation is using Outlook Express installed on the same machine as the SMTP agent.

For information on configuring the SMTP agent for your existing email infrastructure, see “Using the SMTP agent” in the Data Security Deployment Guide.

Testing the SMTP agent

1. Test relay access from the mail server to the Data Security MTA:
Send a test message from the central mail server to the SMTP agent MTA through telnet:
From the mail server, open a command line and execute the following commands:

```
telnet [DSS MTA ip/hostname] 25
HELO me
MAIL FROM:[email_address@local.domain]
RCPT TO:[your_address@websense.com]
DATA
Subject: testing DSS MTA
.
quit
```

Once you type the period and press enter you should get a 250 Ok: message from the Data Security MTA. If you get any message other than 250 OK do a Google search for that SMTP message.
If you get a 250 OK, but do not receive your message in your corp address, continue to step 2.

2. Test relay access from Data Security MTA Inbound to Outbound:

Send a test message from the SMTP agent server to its own Inbound SMTP Virtual Server through telnet:

From the SMTP agent server, open a command line and execute the following commands:

```
telnet localhost 25
HELO me
MAIL FROM: [email_address@local.domain]
RCPT TO: [your_address@websense.com]
DATA
Subject: testing DSS MTA
.
quit
```

Once you type the period and press enter you should get a 250 Ok: message from the SMTP Virtual Server. If you get any message other than 250 OK do a Google search for that SMTP message. If you get a 250 OK, but do not receive your message in your corp address, check the Badmail/Queue directories for the inbound SMTP Virtual Server (C:\inetpub\mailroot by default). If the folders are empty, continue to step 3.

3. Test relay access from Data Security MTA to its own Outbound server:

Send a test message from the SMTP Agent server to its own Outbound SMTP Virtual Server through telnet:

From the SMTP agent server, open a command line and execute the following commands:

```
telnet localhost 10025
HELO me
MAIL FROM: [email_address@local.domain]
RCPT TO: [your_address@websense.com]
DATA
Subject: testing DSS MTA
.
quit
```

Once you type the period and press enter you should get a 250 Ok: message from the SMTP Virtual Server. If you get any message other than 250 OK do a Google search for that SMTP message. If you get a 250 OK, but do not receive your message in your corp address, check the Badmail/Queue directories for the Outbound SMTP Virtual Server (C:\inetpub\outbound by default). If the folders are empty, continue to step four.

4. Test relay access from Data Security MTA to the next hop MTA:

Send a test message from the SMTP Agent server to the next hop MTA through telnet:

From the SMTP agent server, open a command line and execute the following commands:

```
telnet [next hop MTA/smarthost IP/hostname] 25
HELO me
MAIL FROM: [email_address@local.domain]
RCPT TO: [your_address@websense.com]
```

```

DATA
Subject: testing DSS MTA
.
quit

```

Once you type the period and press enter you should get a 250 Ok: message from the next hop MTA. If you get any message other than 250 OK do a Google search for that SMTP message. If you get a 250 OK, but do not receive your message in your corp address, then there is some issue beyond the DSS MTA mail flow (i.e. delivery from next hop MTA to destination domain mail servers).

Microsoft ISA/TMG agent

In this topic:

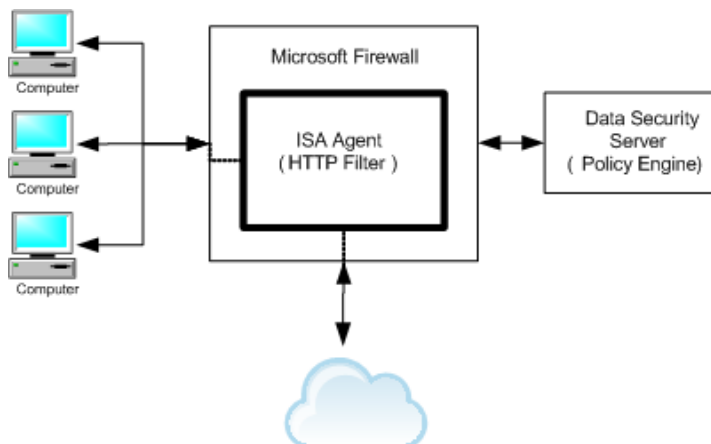
- ◆ [Operating system requirements, page 76](#)
- ◆ [Port requirements, page 76](#)
- ◆ [Installing the ISA/TMG agent, page 76](#)

The ISA/TMG agent receives all Web connections from a Microsoft ISA Server or Forefront TMG network and forwards them to the Data Security policy engine. It then receives the analyzed information back from the policy engine and forwards it to the recipients on the Web.

The ISA/TMG agent supports the permit and block actions, and it receives authentication information from the client on its way to the proxy to identify users. It supports both HTTPS and HTTP traffic.

The ISA/TMG agent requires 1 GB free disk space on the ISA Server machine. The installer will not allow you to install ISA/TMG agent if available space is less.

If you are using the ISA agent on an ISA array, be sure to install it on every member of the array; otherwise the configuration will be out of sync and ISA may become non-functional.



Operating system requirements

Microsoft ISA 2004 and 2006 are supported on the following operating system environments:

- ◆ Windows Server 2003 (32-bit)
 - Standard or Enterprise
 - Standard or Enterprise R2
 - Standard or Enterprise R2 SP2
- ◆ Windows Server 2003 (64-bit)
 - Standard or Enterprise R2

Forefront TMG is also supported on Windows Server 2008 R2 platforms (64-bit).

Port requirements

The following ports must be kept open for the ISA/TMG agent:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Internet gateway	80	For HTTP connections

* This range is necessary for load balancing.

Inbound

None

Installing the ISA/TMG agent

For best practice, do not install the ISA agent on the same machine as a supplemental Data Security Server in a production environment.

1. If your ISA or TMG Server machine has a 32-bit operating system, download the Websense installer (**WebsenseTRITON78xSetup.exe**) from mywebsense.com, where *x* is the version number.

On 64-bit machines, download **WebsenseDataSecurityAgents78x-x64.msi** instead.

2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.

5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

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



Important

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



Note

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

8. On the **Select Components** screen, select **ISA or TMG agent** and then **Entire feature will be installed on local hard drive**.
9. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
10. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server. FQDN is the fully-qualified domain name of a machine.
11. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

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

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

Data Security needs port 80 free.

In order to proceed with this installation, DSS will free up this port.

Click Yes to proceed OR click No to preserve your settings.

Clicking **No** cancels the installation.

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

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

To ensure that the ISA/TMG agent is properly installed and enabled in ISA/TMG, navigate to Web Filters in the ISA/TMG Management Console.

Printer agent

In this topic:

- ◆ [Operating system requirements](#), page 79
 - ◆ [Port requirements](#), page 79
 - ◆ [Before you begin](#), page 80
 - ◆ [Installing the printer agent](#), page 80
 - ◆ [Detecting the printer driver](#), page 82
 - ◆ [Configuration settings for non-English text](#), page 83
 - ◆ [Printer agent performance](#), page 84
-

The Data Security printer agent is required when you want to monitor what is printed on your organization's network printers.

The printer agent supports permit and block actions.

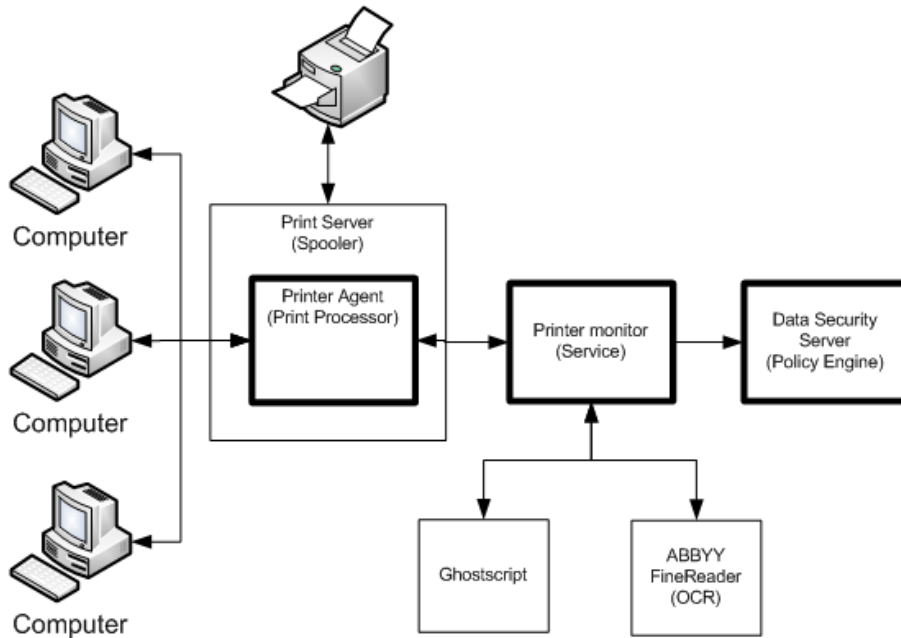
When a user on the network prints a file, it is routed to the Microsoft Windows printer spooler service, where the printer agent intercepts it and sends it to the Data Security policy engine. After analysis of the content, the Data Security system enforces the policy as necessary: either auditing, monitoring or blocking the print job from being printed, in which case the sender (the user who printed the document) receives a notification that the print job was blocked.

The printer agent is capable of identifying the user that submitted the print job, because these credentials are included in the print job.

Websense Data Security generates forensics reports that list the blocked print files along with other blocked transmissions.

You install the printer agent on a Windows print server. It includes optical character recognition (OCR) capabilities. The OCR service enables the recognition and prevention of "corporate-defined" confidential content being printed. The OCR service is required not only to support certain sources, but is also a must when certain printer drivers are used, for example, PCL 6. As a general rule, only standard formats, such as extended meta file (EMF), printer control language (PCL), text (TXT), and

postscript (PS) can be received by the printer agent. Nonstandard formats are not supported.



The printer agent is installed using a separate printer agent package (WebsenseDataSecurityPrinterAgent.zip) See [Installing the printer agent](#), page 80 for instructions.

Operating system requirements

The printer agent supports the following Windows Server 2003 32-bit environments:

- ◆ Standard or Enterprise
- ◆ Standard or Enterprise R2
- ◆ Standard or Enterprise R2 SP2

Port requirements

The following ports must be kept open for the printer agent:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications

Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Management Server	17443	Incidents
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Inbound

None

Before you begin

There are 2 prerequisites for installing the Data Security printer agent:

- ◆ The computer where you're installing the agent must be inside a domain.
- ◆ The computer where you're installing the agent must have at least one printer already installed.
- ◆ For best practice, do not install the printer agent on the same machine as a supplemental Data Security Server in a production environment.

If these 2 conditions are not met, the installer doesn't show the option to install the printer agent.

Installing the printer agent

1. Download and extract **WebsenseDataSecurity78xSetup.exe** from mywebsense.com on the print server machine.
2. Launch the Data Security installer on the print server. (Note that the printer agent does not analyze print jobs initiated locally on the print server.)
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

The default destination is C:\Program Files (x86)\Websense\Data Security (32-bit). If you have a larger drive, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.



Important

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

**Note**

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

8. On the **Select Components** screen, select **Printer Agent** and then **Entire feature will be installed on local hard drive**.
9. The **Optical Character Recognition** screen appears.

Section	Description
OCR Analysis Threshold	<p>Per printed page: This parameter limits dynamically (according to the number of pages) the total time that the OCR can extract text from the printed job. In case of a timeout, the content analysis will be performed only on the extracted text that took place before the timeout. (Default value: 3 sec.; Range: 1-60 sec.)</p> <p>No more than <i>nn</i> seconds: This number is a static overall limit to the total time that the OCR can extract text from the printed job. In case of a timeout, the content analysis will be performed only on the extracted text that took place before the timeout. (Default value: 300 sec.; Range: 1-3600 sec.)</p>
OCR Accuracy	<p>Running the OCR in accurate mode results in higher latency. Administrators can set the size of jobs that will be executed in the most accurate OCR mode (small jobs do not produce high latency, so it is reasonable to use better accuracy). In most cases, lower OCR quality is sufficient and provides good results.</p> <p>Keep in mind that the average OCR Analysis per printed page limit is ignored for small documents, but the entire print job limit is still adhered to. (Default value: 5 pages)</p>

Optionally, you can change the default values defined for the OCR Analysis Threshold and the OCR Accuracy.

10. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
11. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server. FQDN is the fully-qualified domain name of a machine.
12. In the **Local Administrator** screen, enter a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.

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

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

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

Data Security needs port 80 free.

In order to proceed with this installation, DSS will free up this port.

Click Yes to proceed OR click No to preserve your settings.

Clicking **No** cancels the installation.

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

14. A **Configure Printer Agent** screen appears.

- a. Select a printer from the list and click **OK**.

A red exclamation point indicates that a printer has settings that are incompatible with the printer agent. The printer agent is unable to monitor traffic for printers that are configured with incompatible settings, for example, "Print directly to printer." Hover the mouse over a problematic printer for details in a tooltip.

You can still select an incompatible printer. If you do, the following message appears:

The Websense Printer Agent is unable to monitor traffic when one or more printers are configured with incompatible settings. Do you wish Websense to correct the settings?

- b. Click **Yes**. The settings are automatically modified to accommodate the printer agent.

15. The **Print Processor Destination(s)** screen appears.

This screen is for information only; there are no options to select. The displayed list contains the names of all cluster nodes on which the printer agent is installed. Make sure that all nodes holding print spooler resources are listed.

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

The printers you selected appear as policy resources in the Data Security manager. To view them, log onto the TRITON Console and navigate to **Main > Configuration > Resources**.

17. To complete the process, click **Deploy** in the Data Security manager.

Detecting the printer driver

If you are having difficulty with the recognition and configuring of your printers with the printer agent, you can export the printer registration file to send to Websense Technical Support for analysis. This file indicates printer names and drivers.

To export printer registration files:

1. Click **Start > Run** and in the Run dialog, type **regedit**.

2. Click **OK** in the Run dialog. The Registry Editor screen is displayed.
3. In the Registry Editor screen, navigate to the following directory:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers
4. Right-click the Printers folder and select **Export**.
5. Select the desired directory to save the exported (*.reg) file.
6. Click **Save**.
7. Send the exported (*.reg) file to your local Websense Technical Support representative.

Alternative detection of printer driver

Alternatively, users may access the following registry key on the print server to detect the printer driver:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers\ {Printer Name}\
```

In the registry key, open the printer driver entry and view the string value.

To access the above registry key, refer to [Detecting the printer driver](#), steps 1 to 3 above.

Configuration settings for non-English text

If your printers are used for non-English text, you need to make minor modifications to the following configuration files:

- ◆ ExportToTXT-Accurate.ini
- ◆ ExportToTXT-Fast.ini

To modify the configuration files:

1. Using Windows Explorer, navigate to the following directory:
C:\Program Files\Websense\Data Security\ABBY\Profiles
2. Locate the following 2 files: ExportToTXT-Accurate.ini and ExportToTXT-Fast.ini.
3. Open each of the above .ini files in a text-editing application.
4. Locate the [RecognizerParams] section. If it does not exist, create a new section with this name.
5. Add a parameter to the [RecognizerParams] section as follows:
[RecognizerParams]
TextLanguage = English,French
6. Save the *.ini files.

Printer agent performance

The printer agent has different demand levels, depending on whether it is in Monitoring or Blocking mode, and whether the OCR service is activated or deactivated.

Monitoring mode operates in an asynchronous manner and therefore, does not introduce analysis time overhead to the printing time.

In Blocking mode, the OCR processing adds up to 3 seconds per page depending on the CPU power of the printer server. You can select Blocking or Monitoring in the Edit Printer Agent window, accessed through **Settings > Deployment > System Modules**. Select the printer agent on the System Modules screen.

Select **Monitoring** if you want to monitor traffic through the print server but not block it.

Select **Blocking** if you want to block actions that breach policy.

FCI agent

In this topic:

- ◆ [Operating system requirements, page 85](#)
 - ◆ [Port requirements, page 85](#)
 - ◆ [Installing the FCI agent, page 87](#)
-

The Data Security FCI agent augments the data classification performed using Microsoft File Classification Infrastructure (FCI) on Windows Server 2012 machines.

Working in tandem with the Microsoft File Server Resource Manager (FSRM), the agent analyzes data and applies data discovery policies to it, tagging the data when a match is detected. This allows administrators to identify data such as personally identifiable information (PII) or protected health information (PHI) so they can control access to it, perform remediation on it, and more.



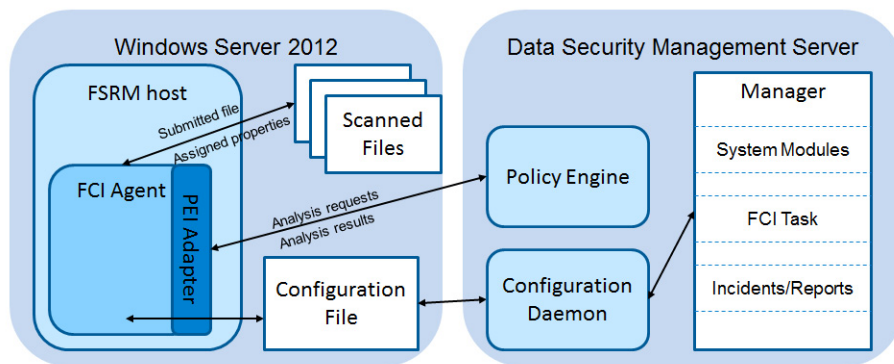
Note

Data Security cannot inspect the content of encrypted files. It can, however, identify encrypted files and tag those if configured to do so. FCI tags remain after decryption and encryption.

The FSRM and Data Security systems are in constant communication. Data is passed from the FSRM according to a schedule configured in the FSRM and passed back by Data Security after analysis. You do not schedule a discovery task in the Data Security manager.

Here is the typical data flow:

1. According to the FSRM schedule, the FCI agent delivers the relevant files to a policy engine in the Data Security system. This could be the management server, supplemental server, or other module.
2. The policy engine processes it and returns classification results.
3. The agent checks the results against an FCI rule/policy map and triggers the relevant FCI rules.
4. The FCI system attaches a property and value to the file as appropriate.
Any change in FCI properties or FCI rules causes a rescan of the relevant files, as does any change in the data discovery policies or mapping. If there is a file classification failure, the file is rescanned on the next run.
5. The agent contacts the Data Security Management Server periodically and checks to see if there is new data to retrieve.



Operating system requirements

The FCI agent runs only on Microsoft Windows Server 2012 machines.

Port requirements

The following ports must be kept open for the FCI agent:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Inbound

Microsoft FSRM	5985	Microsoft File Server Resource Manager (FSRM)
----------------	------	---

Before you begin

If you have not done so already, perform the following steps before you work with the Data Security FCI agent:

1. Install the Microsoft File Server Resource Manager (FSRM) role on a Windows Server 2012 machine.
2. Define file classification properties in the FSRM.
3. Build classification rules that define how to apply these properties to existing files.
 - You can use existing properties and rules with Data Security, or you can create properties and rules for the sole purpose of working with Data Security.
 - If you want the rule to classify data on the fly, select **Continuous Classification** in the classifier scheduler.
 - If you want the rule to reclassify files when they or classification rules change, select **Re-evaluate existing property values**. You can overwrite the existing value if desired.
 - If you plan to associate multiple Data Security discovery policies with the rule and you have defined a multi-value classification properties, select the evaluation type **Aggregate the values** for best results.
4. Configure and enable the Data Security discovery policies of interest.

See your Microsoft documentation for instructions on steps 1-3. See [Creating a discovery policy](#) for instructions on step 4.

Example

You are interested in locating and classifying protected credit card information in your network.

In the FSRM, you name a property “PCI” and assign it the values High, Medium, Low, and None to indicate possible severity levels.

You name a rule “PCI_High”, assign it the property PCI, and specify the value High.

You name a rule “PCI_Med” and specify the value Medium.

You name a rule “PCI_Low” and specify the value Low.

In Data Security, you map the rule PCI_High with the predefined discovery policy, PCI DSS.

When the data supplied by the FSRM matches the discovery policy with a certain threshold (say 50 credit card numbers), Data Security triggers the FCI rule, which

assigns the data the property and value prescribed in the rule (in this case PCI and High).

The FSRM system acts on the trigger as configured, such as setting permissions that keep files with sensitive data private or moving business critical files to the fastest servers.

Installing the FCI agent

1. Download the Websense installer, **WebsenseDataSecurityAgents78x-x64.msi**, from mywebsense.com.
2. Launch the installer on a Windows Server 2012 machine with the File Server Resource Manager (FSRM) installed.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

The default destination is C:\Program Files (x86)\Websense\Data Security (32-bit). If you have a larger drive, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.



Important

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



Note

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

8. On the **Select Components** screen, select **FCI agent** and then **Entire feature will be installed on local hard drive**. If this option is not shown, you do not have FSRM properly installed on the machine. FSRM is required.
9. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
10. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server. FQDN is the fully-qualified domain name of a machine.

11. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.
Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.
12. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete.
13. Click **Finish**.

Configuring the FCI agent

To prepare for file classification:

1. Log onto the Data Security manager.
2. Enable relevant discovery policies.

The screenshot shows a configuration window for a policy. The 'Policy name' field contains 'Websense'. The 'Description' field contains 'new policy'. To the right of the description field is a checkbox labeled 'Enabled' which is checked. Below this is a section for 'Policy owners' with a dropdown menu set to 'None' and an 'Edit...' button. A note at the bottom states: 'NOTE: You must deploy a policy for it to take effect in your network.'

3. Enable and configure FCI agent in System Modules.
 - a. Navigate to **Settings > Deployment > System Modules**, and then click the FCI agent module.
 - b. Enable the module and add a description if desired.
4. Map FCI rules to discovery policies.
 - a. Select **Main > Policy Management > Discovery Policies**.
 - b. Select **Map Microsoft FCI Rules**.
 - c. See [Data Security Manager Help](#) for instructions on completing the map.
5. Deploy settings.

Because classification is controlled in the FSRM, there is no task to schedule in the Data Security manager. You can view breaches in the Discovery Incident report.

Integration agent

In this topic:

- ◆ [Installing the integration agent, page 89](#)
 - ◆ [Registering the integration agent, page 90](#)
 - ◆ [Using the Websense Data Security API, page 90](#)
-

The integration agent allows third-party products to send data to Websense Data Security for analysis.

Third parties can package the integration agent inside their own installer using simple, 'industry standard' methods that are completely transparent to end users.

When the third-party product is installed on a users system, it needs to register the integration agent with the Data Security Management Server. This can be done transparently through the installation process or using a command-line utility.

The integration agent works on the following operating systems:

- ◆ Windows Server, 32-bit
- ◆ Redhat Enterprise Linux

Data Security treats third-party products that use the integration agent as it does any other agent.

It supports all relevant views and capabilities, including:

- ◆ Incident Management and Reporting
- ◆ Quarantine and Release of emails
- ◆ Traffic log view
- ◆ Load balancing capabilities
- ◆ The Integration agent does not support discovery transactions.

For information on configuring the integration agent, see “Configuring the integration agent” in the Data Security Manager Help system.

Installing the integration agent

Installed components

When you embed the integration agent in your product installer, 3 Data Security components are installed on the end-user machine:

- ◆ PEInterface.dll - A DLL the that interacts with the Data Security policy engine on the management server.
- ◆ ConnectorsAPIClient.exe - Client software that connects the API in the third-party product with Websense Data Security.

- ◆ registerAgent.bat (or .vbs) - A script that performs registration with the Data Security Management Server.

Installation package format

On Windows, the installation package for the integration agent is provided in 2 major formats:

- ◆ MSM file. The installer that uses the MSM can choose (by setting properties) whether or not to register the product with the Data Security Management Server during installation. The MSM contains a 'custom action' that validates Data Security user names and passwords and can be called by the third-party installer.
- ◆ MSI file. This file embeds the MSM file. Some parties prefer to work with an MSI, and others can use it as a reference implementation. The MSI installation wizard presents 4 interactive dialogs:
 - Installation-dir - installation directory.
 - Registered Channels - The DLP channels to use: HTTP, SMTP, Printer, Discovery.
 - Local IP Address - which of the static IP addresses currently assigned to the machine should be used for registration.
 - Data Security Management Server details - IP address or host name, user name, password.

On Linux, the package is in the form of a relocatable RPM.

Registering the integration agent

Every instance of the integration agent needs to be registered after being installed. (This is a one time operation.) In other words, every time the third-party product is installed on an end-user machine, that instance of the agent needs to be registered.

The registration operation can be done during the installation by the installer, or using a command-line utility provided with the agent.

The command-line utility should receive the following input arguments:

- ◆ Protocols - a non-empty list of supported protocols (out of HTTP, SMTP, Printer, Discovery).
- ◆ Data Security Management Server details - IP address or host name, user name, password.
- ◆ Local IP Address (optional) - In case this is not supplied, use any of the static addresses of the machine, and print it to the standard output.
- ◆ Search IP Address (optional) - used for re-registration after IP change. In case this is not supplied, use the address in the registerAgent.conf file. If that file does not exist, use the given local IP address.

A successful operation registers the machine with the Data Security Management Server as having the desired protocols and generates certificate files in the same

directory that the tool is located. The tool also stored a configuration file (registerAgent.conf) with the IP address used for registration.

On failure, the script returns a meaningful exit code and prints an error message to standard output

Using the Websense Data Security API

Third parties that subscribe to the integration agent use a C-based API to send data to Websense Data Security for analysis and receive dispositions in return.

The API can be used to configure analysis operations on a transaction-by-transaction basis on the following variables:

- ◆ Channel/Protocol - Upon installation the third-party product can declare its ability to intercept various protocols, and assign each transaction to a protocol.
- ◆ Blocking/Monitoring mode - each transaction can work in a different mode.
- ◆ Timeout - can be different per transaction.

For documentation on the Data Security API, consult with your Websense Sales representative.

The crawler

In this topic:

- ◆ [Operating system requirements, page 91](#)
 - ◆ [Port requirements, page 91](#)
 - ◆ [Installing the crawler agent, page 92](#)
-

The crawler is the name of the discovery and fingerprinting agent. It is selected by default when you install the Data Security Management Server or supplemental Data Security 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. Websense recommends that you use the crawler that is located closest to the data you are scanning.

You can view the status of your crawlers in the Data Security manager user interface. Go to **Settings > Deployment > System Modules**, select the crawler and click **Edit**.

Operating system requirements

Supplemental Data Security servers must be running on one of the following operating system environments:

- ◆ Windows Server 2003 (32-bit) Standard or Enterprise R2 SP2

- ◆ Windows Server 2008 (64-bit) Standard or Enterprise R2

Port requirements

The following ports must be kept open for the crawler:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communication
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Internet	443	Salesforce fingerprinting

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
Data Security Management Server	9797*	Crawler listening

* This is only for the standalone crawler agent.

Installing the crawler agent

1. Download the Websense installer (**WebsenseTRITON78xSetup.exe**) from mywebsense.com.
2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

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



Important

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

**Note**

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

8. On the **Select Components** screen, select **Crawler agent** and then **Entire feature will be installed on local hard drive**. If this is a stand-alone installation, deselect all other options, including Data Security Server.
9. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.

The following message may appear:

*Data Security Discovery Agent works with a specific version of WinPcap.
The installation has detected that your WinPcap version is <version>
In order to proceed with this installation, WinPcap version 4.0.0.1040 needs
to be installed and will replace yours.
Click Yes to proceed or Click No to preserve your WinPcap version and
deselect the Discovery Agent Feature to continue with the installation.*

“Discovery Agent” refers to the crawler agent. The particular version of WinPcap mentioned in this message must be in place to install Crawler Agent. Note that after installation of the crawler agent you can install a different version of WinPcap. The crawler agent should continue to work properly.

10. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server. FQDN is the fully-qualified domain name of a machine.
11. In the **Local Administrator** screen, enter a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.
12. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, the **Lotus Domino Connections** screen appears.

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



Important

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

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

- a. On the **Lotus Domino Connections** page, select the check box labeled **Use this machine to scan Lotus Domino servers**.
- b. In the **User ID file** field, browse to one of the authorized administrator users, then navigate to the user’s **user.id** file.



Note

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

- c. In the **Password** field, enter the password for the authorized administrator user.
13. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

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

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

*Data Security needs port 80 free.
In order to proceed with this installation, DSS will free up this port.
Click Yes to proceed OR click No to preserve your settings.*

Clicking **No** cancels the installation.

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

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

For information on configure the crawler, see “Configuring the crawler” in the Data Security Manager Help system.

Troubleshooting Data Security agent installation

In this topic:

- ◆ [Initial registration fails, page 94](#)
- ◆ [Deploy settings fails, page 95](#)
- ◆ [Subscription errors, page 95](#)
- ◆ [Network connectivity problems, page 96](#)

Though the installation and deployment of agents is normally a series of clear-cut steps, occasionally, some problems can arise. Below are how to resolve common problem scenarios.

Initial registration fails

- ◆ Make sure you can ping the Data Security agents by IP and by host name from the TRITON Management Server.
 - On Windows, run the following command (in a Command Prompt) to check for block ports:


```
netstat 1 -na | find "SYN"
```

 Each line displayed in response to the command is a blocked port. This command is one-way. Run it on both the agent machine and the TRITON Management Server.
- ◆ Check logs on the TRITON Management Server (and remote policy engines).
 - %dss_home%/logs/mgmt.d.log
 - %dss_home%/tomcat/logs/dlp/dlp-all.log
- ◆ Check logs on the protector. These reside in the /opt/websense/neti/log directory. In particular, check:
 - /opt/websense/neti/log/registration.log
- ◆ Make sure no duplicate certificates are installed on the agents' servers; if there are duplications, delete all of them and re-register the agent. Also, make sure the system date/time of the agent machine and the TRITON Management Server are the same. The following certificates are expected:


```
Certificate > My User Account > Trusted Root Certification Authorities >
Certificates > ws-ilp-ca
Certificates > Computer > Personal Certificates ><servername>(issued by
ws-ilp-ca)
Certificates > Computer > Trusted Root Certification Authorities >
Certificates > ws-ilp-ca
```

- ◆ Make sure the FQDN value of the agent states the full server name for the agent's server.
 - Protector — if domain name is configured, the FQDN is:
protectorname.domain.name
 - Agents and Data Security server — check “My Computer” properties and copy the computer name value from there.

Deploy settings fails

- ◆ Make sure you can ping the agents by IP and by host name from the TRITON Management Server.
- ◆ Check logs on the TRITON Management Server (and remote policy engines).
 - %dss_home%/tomcat/logs/dlp/dlp-all.log
 - %dss_home%/tomcat/logs/dlp/deployment-trace.log
- ◆ Check the plat.log on the protector.

Subscription errors

- ◆ Restart the Websense TRITON - Data Security service on the TRITON Management Server.
- ◆ Check %dss_home%/tomcat/logs/dlp/dlp-all.log.

Network connectivity problems

In complex networks, network connectivity may require routes added to the inline protector.

Although routes can be added with the built in kernel route command, it is strongly recommended that the `/opt/websense/neti/bin/route` command is used instead. If the kernel route (`/sbin/route`) is used, the added routes will be lost after rebooting.

`/opt/websense/neti/bin/route` writes the routes to a file `/opt/pa/conf/route` so that on subsequent reboots the route information is re-submitted to the protector.

Usage:

```
route: Add/delete routing information
```

Usage:

```
route [list]
route add {destination network | destination ip} {via
{ip}|dev {device}}
route del {destination network | destination ip} {via
{ip}|dev {device}}

network=ip/prefix
```

Example:

```
~@protector7# /opt/websense/neti/bin/route add 192.168.1.0/  
24 via 10.212.254.254 dev br0  
~@protector7# /opt/websense/neti/bin/route list  
Kernel IP routing table  
Destination Gateway Genmask Flags MSS Window irtt Iface  
192.168.1.0 10.212.254.254 255.255.255.0 UG 0 0 0 br0  
10.212.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0  
10.212.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br0  
0.0.0.0 10.212.254.254 0.0.0.0 UG 0 0 0 eth0
```


3

Adding, Modifying, or Removing Components

In this topic:

- ◆ [Adding or modifying Data Security components, page 97](#)
 - ◆ [Recreating Data Security certificates, page 98](#)
 - ◆ [Repairing Data Security components, page 98](#)
 - ◆ [Changing the Data Security service account, page 99](#)
 - ◆ [Changing the domain of a Data Security Server, page 99](#)
-

This chapter contains instructions for adding, modifying, or removing Websense Data Security components.

Adding or modifying Data Security components

1. Start the Websense installer:
 - If you chose to keep installation files after the initial installation, go to **Start > All Programs > Websense > Websense TRITON Setup** to start the installer without having to re-extract files.
 - Otherwise, double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. From the installation wizard, select **Modify**.

This enables you to review the Data Security installation screens, making modifications to settings—with the exception of username—as necessary.

To add components, select them on the **Select Components** screen.

Also, refer to the following sections for the most common Data Security modify procedures:

- [Recreating Data Security certificates, page 98](#)
- [Repairing Data Security components, page 98](#)
- [Changing the Data Security service account, page 99](#)
- [Changing the domain of a Data Security Server, page 99](#)

Recreating Data Security certificates

From the Modify menu, you can also re-certify the server. This is not recommended except in extreme security breaches. When you recreate security certificates, you must re-register all agents and servers (see [Re-registering Data Security components](#), for instructions), and repeat the Reestablish Connection process for each agent and server.

You must also reinstall all endpoints, or they will not be able to communicate with the servers. Uninstall the existing endpoint software, create a new endpoint package using the package-building tool (you cannot use your existing package), and use SMS or a similar mechanism to install the new package on these endpoints. See [Installing and Deploying Websense Endpoint Clients](#) for more information.

In the initial authentication, the Data Security Management Server trades certificates with the other servers and endpoints in the network.

To re-run the security communication between Data Security components:

1. If you have not done so already, start the Websense installer:
 - If you chose to keep installation files the last time you ran the installer, go to **Start > All Programs > Websense > Websense TRITON Setup**. This starts the installer without having to re-extract files.
 - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. From the installation wizard, select **Modify**.
4. On the Recreate Certificate Authority screen, select the **Recreate Certificate Authority** check box.
5. Complete the installation wizard as prompted.

Repairing Data Security components

6. If you have not done so already, start the Websense installer:
 - If you chose to keep installation files the last time you ran the installer, go to **Start > All Programs > Websense > Websense TRITON Setup**. This starts the installer without having to re-extract files.
 - Double-click the installer executable.
7. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
8. From the installation wizard, select **Repair**.
9. Complete the installation wizard as prompted.

This restores the installation configuration to its last successful state. This can be used to recover from various corruption scenarios, such as binary files getting deleted, registries getting corrupted, etc.

Changing the Data Security service account

1. If you have not done so already, start the Websense installer:
 - If you chose to keep installation files the last time you ran the installer, go to **Start > All Programs > Websense > Websense TRITON Setup**. This starts the installer without having to re-extract files.
 - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. From the installation wizard, select **Modify**.
4. In the Local Administrators dialog, select the new Websense Data Security privileged account to be used. Make sure the user is a member of the local administrators group.
5. Complete the installation wizard as prompted.

Changing the domain of a Data Security Server

It is a best practice to perform this task during off hours, or to route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.).

1. Use TRITON - Data Security to add the Websense service account user from the domain to the local Administrators group. Add the user itself and not the domain group of which it is a member.
2. Log on with the Websense service account from the domain.
3. Restart the machine.
4. From **Start > Settings > Control Panel > Add/Remove Programs**, select **Websense Data Security** and click **Change/Remove**.
5. Perform the steps described in the procedure, [Changing the hostname of the Data Security Management Server](#).
6. Re-register all Websense Data Security policy engine servers, agents and protectors (See [Re-registering Data Security components](#)).
7. Click **Deploy** in TRITON - Data Security.
8. In your PreciseID fingerprint classifiers, change the server to the correct name.
9. Run breach tests on all the channels to verify that the Websense Data Security infrastructure is functioning well. Make sure you get events in both the Event Viewer and Incidents Management.

Removing Data Security components

Data Security components can only be removed altogether. You cannot select particular components on a machine for removal



Warning

Websense Email Security Gateway requires Websense Data Security to be installed. If you are using Email Security Gateway, do not uninstall Data Security or Email Security Gateway will quit working.

For instructions on removing a Data Endpoint, see [Uninstalling endpoint software](#).

To remove Data Security components:

1. Start the Websense installer:
 - If you chose to keep installation files after the initial installation, go to **Start > All Programs > Websense > Websense TRITON Setup** to start the installer without having to re-extract files.
 - Otherwise, double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. At the **Welcome** screen, click **Remove**.
4. At the **Data Security Uninstall** screen, click **Uninstall**.



Important

This removes all Data Security 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.