Upgrading TRITON Enterprise v7.7.x to v7.8.x

Upgrade Instructions | Web, Data, and Email Security Solutions | Version 7.8.x

This guide describes how to upgrade TRITON™ Enterprise solutions that include Websense® Web Security, Email Security, and Data Security from v7.7.x to v7.8.x. For information on upgrading systems that include stand-alone installations of Data Security, Email Security, or Web Security, refer to the Deployment and Installation Center in the Websense Technical Library.

Websense TRITON Enterprise modules must be at least version 7.7.0 in order to upgrade to v7.8.0. For information on upgrading from earlier versions to version 7.7.x, see Upgrading TRITON Enterprise v7.6.x to v7.7.x.

Because Email Security Gateway and Gateway Anywhere include Data Security components, the upgrade procedure for Web and Email Security is the same as the upgrade procedure for Websense TRITON Enterprise.

To upgrade v7.7.x to v7.8.x, see the following sections:

Perform the upgrade in the order described. This sequence is critical, because if you upgrade supplemental servers or agents before the management server, they stop communicating. If you upgrade the management server first, it continues communicating with the components until they are upgraded.

Requirements for this version

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

- Windows Server 2008 Standard or Enterprise R2
- Windows Server 2012 Standard Edition
- Windows Server 2012 Standard or enterprise R2

It hosts the TRITON Unified Security Center (TRITON console), which includes:

- The infrastructure uniting all management components
- A settings database for administrator account information and other shared data
- One or more management modules (Web Security manager, Data Security manager, Email Security manager), used to configure and report on a Websense security solution.

Additional components may also reside on the TRITON management server.

Hardware requirements

The recommended 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.
- The disk space recommendation allows for scaling as reporting data accumulates.
- If you install the Websense product on a drive other than the main Windows drive (typically C), you still need at least 2GB free on the main drive to accommodate files extracted during installation.

With remote (standard or enterprise) reporting database

TRITON console modules	Recommended requirements
Web Security manager	4 CPU cores (2.5 GHz), 8 GB RAM, 150 GB Disk Space
Data Security manager	4 CPU cores (2.5 GHz), 8 GB RAM, 140 GB Disk Space
Web Security and Data Security managers	8 CPU cores (2.5 GHz), 12 GB RAM, 300 GB Disk Space
Email Security and Data Security managers	8 CPU cores (2.5 GHz), 12 GB RAM, 300 GB Disk Space
Web Security, Data Security, and Email Security managers	8 CPU cores (2.5 GHz), 16 GB RAM, 500 GB Disk Space

With local (express) reporting database

TRITON console modules	Recommended requirements
Web Security manager	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
Data Security manager	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
Web Security and Data Security manager	8 CPU cores (2.5 GHz), 12 GB RAM, 400 GB Disk Space
Email Security and Data Security manager	8 CPU cores (2.5 GHz), 12 GB RAM, 400 GB Disk Space
All TRITON modules (Web Security, Data Security, and Email Security)	8 CPU cores (2.5 GHz), 16 GB RAM, 600 GB Disk Space

TRITON console browser support

Use any of the following browsers to access the TRITON Unified Security Center.

Browser	Versions
Microsoft Internet Explorer*	8, 9, 10, and 11
Mozilla Firefox	4.4 through 26.x
Google Chrome	13 and later
* Do not use Compatibility View.	

Virtualization systems

All TRITON Unified Security Center components are supported on these virtualization systems:

- Hyper-V over Windows Server 2008 R2 or Windows Server 2012 Standard Edition
- VMware over Windows Server 2008 R2 or Windows Server 2012 Standard Edition

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

Directory services for administrator authentication

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

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

Reporting database requirements

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

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

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

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

The supported database engines for Websense Web Security, Data Security, and Email Security solutions 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; not IA64
- SQL Server 2012

  Standard, Business Intelligence, and Enterprise editions

Before upgrading TRITON Enterprise

This section lists the steps you must take to prepare for the TRITON Enterprise upgrade.

- Unless instructed otherwise by Websense Technical Support, ensure your system is functional prior to upgrade.
- Ensure the time set on all appliances is synchronized prior to upgrade.
- Make sure the installation machine meets the *Requirements for this version*.
- If you are already using Virtual Machines (VMs) for the TRITON console or for Microsoft SQL Server, take a snapshot of the VMs before you start a TRITON upgrade.
- Back up all of your Websense components before starting the upgrade process. See the Backup and Restore FAQ for instructions.

  The Backup and Restore FAQ includes instructions for backing up all of the pieces that make up Web Security Gateway Anywhere on all platforms:

  - TRITON Infrastructure
  - Web Security components
  - Content Gateway
  - Data Security components

  On Websense appliances, be sure to perform a **full appliance configuration** backup.

The upgrade process guides you through upgrading **all** components on the selected machine.

- You cannot choose which components to upgrade.
- Partial upgrades are not supported.

When upgrading the TRITON management server, if upgrade fails for any component **except** TRITON Infrastructure, you can either continue to upgrade the rest of the components or exit the process and modify component settings.

- You cannot continue if the infrastructure upgrade fails.
- You cannot roll back a component that was upgraded successfully.

After upgrade, your system has the same configuration as before the upgrade. Apart from the option to edit the Email Security database IP address if it has changed since installation, the upgrade process does not allow you to change your configuration or settings.

Web Security upgrade preparation

Before upgrading Web Security:

1. Verify that third-party components that work with Web Security Gateway, including your database engine and directory service, are supported. See Requirements for Web Security solutions.
2. Before upgrading Websense Filtering Service, make sure that the Filtering Service machine and the TRITON management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.
3. Back up your current Log Database and stop Log Server.

   

   Warning

   If database operations are active during upgrade, the Websense Log Database may be left in an inconsistent state, rendering it unusable.

   When this occurs, it can be difficult to fix.

   Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

   a. Back up Web Security reporting databases.

      Refer to Microsoft documentation for instructions on backing up databases. The Websense Web Security databases are named wslogdb70 (the catalog database), wslogdb70_*n* (standard logging partition databases), and wslogdb70_amt_1 (threats partition database).

   b. On the Log Server machine, use the Windows Services tool to stop **Websense Log Server**.
4. Stop all database jobs associated with the Web Security Log Database:

   If you have a **full version of Microsoft SQL Server** (not Express):

   a. Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).

   b. To disable all currently active Websense SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

      - Websense_ETL_Job_wslogdb70
      - Websense_AMT_ETL_wslogdb70
      - Websense_IBT_DRIVER_wslogdb70
      - Websense_Trend_DRIVER_wslogdb70
      - Websense_Maintenance_Job_wslogdb70

      Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

      Make sure all jobs have completed any current operation before proceeding with upgrade.

   c. After upgrade, remember to enable the disabled jobs to resume normal database operations.

If you have **SQL Server Express**, use the Windows Services tool to restart the MSSQLSERVER service prior to upgrade, in order to ensure that the Service Broker jobs are not running.

5. If Websense Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:
   a. Launch the Windows Services tool.
   b. Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.

If your deployment includes V-Series appliances, also see the Websense V-Series Appliance Upgrade Guide.

Disable on-appliance TRITON console

In version 7.8.x, the Web Security manager cannot reside on an appliance. Disable the on-appliance TRITON console and create a Windows-based TRITON management server before upgrading.

To disable the on-appliance TRITON console:

1. Log on to the Appliance Manager (https://<*C interface IP address*>:9447/appmng)
2. Under **Configuration**, select **Web Security Components**.
3. Under **TRITON - Web Security**, select **Disabled**.
4. Click **Save**.

   The disabling process may take several minutes. Wait for it to complete.
5. When the process completes successfully, a **TRITON Configuration** link appears below the **Disabled** option. Use this link to create a backup of TRITON settings that can be restored to the off-appliance TRITON Unified Security Center:
   a. Click the backup file link that is displayed below the Disabled button.
   b. If a certificate error is displayed, click the continue or accept option to start the download.
   c. Save the TRITON backup file (**EIP_bak.tgz**) in a convenient location.

Restart services before starting the upgrade

Most Websense services must be running before the upgrade process begins. If any service (other than Log Server) is stopped, start it before initiating the upgrade.

The installer will stop and start Websense services as part of the upgrade process. If the services have been running uninterrupted for several months, the installer may not be able to stop them before the upgrade process times out.

- To ensure the success of the upgrade, manually stop and start all the Websense services **except Log Server** before beginning the upgrade. (Log Server should remain stopped, as described in *Web Security upgrade preparation*, page 5.)

- *Windows*: Navigate to the Websense **Web Security** directory (C:\Program Files (x86)\Websense\Web Security\, by default) and enter the following command:

  ```
  WebsenseAdmin restart
  ```

- *Linux*: Navigate to the **Websense** directory (/opt/Websense/, by default) and enter the following command:

  ```
  ./WebsenseAdmin restart
  ```

- On Windows machines, if you have configured the **Recovery** properties of any Websense service to restart the service on failure, use the Windows Services dialog box to change this setting to **Take No Action** before upgrading.

Internet access during the upgrade process

When you upgrade, policy enforcement stops when Websense services are stopped. Users have unrestricted access to the Internet until the Websense services are restarted.

The Websense Master Database is removed during the upgrade process. Websense Filtering Service downloads a new Master Database after the upgrade is completed.

Data Security upgrade preparation

Before upgrading Data Security:

- Restore your archive partitions. (Do this under **Settings** > **General** > **Archive** in the Data Security manager.)
- Stop all discovery and fingerprinting tasks.
- Route all traffic away from the system.
- Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.
- Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.
- Disable the Watchdog service. This prevents it from restarting stopped services in the middle of the upgrade.
  - On the TRITON management server machine, go to **Start** > **Administrative Tools** > **Task Scheduler**, then select **Task Scheduler Library**.
  - Disable the DSS Watchdog task. It will be re-enabled during upgrade.
- If Websense supplied your organization with custom file types, change the name of 2 configuration files located in the \policies_store\custom_policies\config_files folder where Data Security is installed; otherwise they will be overwritten during upgrade.
  a. Change **extractor.config.xml** to **custom_extractor.config.xml**.
  b. Change **extractorlinux.config.xml** to to **custom_extractorlinux.config.xml**.

  The filenames are case-sensitive.

- If you have custom policies provided by Websense, submit a request for updated versions before proceeding.

Note that the speed and success of your upgrade are affected by many factors, including:

- Number of online incidents.
- Size of the forensics folder.
- Number of policies or rules in use
- User directory import size
- Whether GPO restrictions are enforced on the server in domain membership scenarios

Email Security Gateway upgrade preparation

Before upgrading Email Security Gateway:

- Redirect all email from the appliance being upgraded. You may lose cached messages if you do not put a redirect in place.

See the Websense V-Series Appliance Upgrade Guide for other upgrade preparation steps.

Preparing to upgrade Content Gateway

There are several large and important changes beginning in version 7.8.2. Please read the 7.8.3Release Notes before starting the upgrade.

SSL support

SSL support is rearchitected in version 7.8. Most SSL configuration settings are saved and applied to the upgraded Content Gateway.

During upgrade:

- The v7.7.x SSL SQLite3 database is converted to a new database file.
- The Incident list is retained.
- Dynamic certificates are not retained. All other certificates are retained.
- The Certificate Authority Tree is retained (trusted Root CA tree).
- SSLv2 is no longer enabled by default. If it is enabled prior to upgrade, the setting is retained.
- CRL and OCSP revocation statistics (on Monitor > SSL > CRL Statistics) are retained.
- Customized certificate failure and connect error message pages are not retained.

- SSL **inbound*.log** and **outbound*.log** files are deleted. After upgrade, transaction logging is sent to **extended.log** or **squid.log** when the logging subsystem is configured for “Log Transactions and Errors” or “Log Transactions Only”. Otherwise, logging is sent to **content_gateway.out**.

Before upgrading:

- Content Gateway upgrades from v7.7.x to v8.8.x require an additional step to avoid possible latency issues sometimes caused by scanning using async mode.
  1. Versions older than v7.7.x should first upgrade to v7.7.x.
  2. Download and install v7.7.x Hotfix 94. This hotfix adds background variables that retain sync mode.
  3. Upgrade from v7.7.x to v8.8.x. Sync mode is retained.
- Consider performing maintenance on the Incident list; remove unwanted entries.
- Note customizations to certificate failure and connect error message pages. The code structure of the pages has changed; you cannot simply reapply (paste) the 7.7.x HTML.

User authentication

The upgrade process converts existing Multiple Realm Authentication rules into equivalent Rule-Based Authentication rules, with some important changes in structure.

Consolidated credential caching

There is one credential cache for both explicit and transparent proxy mode, and one Global Authentication Options page for setting the caching method and Time-To-Live.

During upgrade:

- (For upgrades from 7.7.x to 8.8.x) The credential cache Enabled/Disabled setting for explicit proxy is retained from the Global Authentication Options tab. Caching for transparent proxy traffic is always enabled.
- The Authentication Mode setting (IP address or Cookie mode) is retained from the Transparent Proxy Authentication tab.
- The Cache TTL value is retained from Transparent Proxy Authentication tab unless the value on the Global Authentication Options tab is not the default, in which case the customized value is used. The cache TTL value is in minutes.
- IP addresses and ranges on the Global Authentication Options Multi-user IP Exclusions list are moved to the cookie cache IP address list.
- If cookie caching is enabled in a Multiple Realm rule, the source IP addresses from that rule are copied to cookie cache IP address list.

Integrated Windows Authentication (IWA)

After upgrade, always check and, if necessary, rejoin IWA domains.

- Upgrade to version 7.8.1 should preserve exiting IWA domain joins.
- Upgrade to version 7.8.2 breaks IWA domain joins. Therefore, IWA domains must be rejoined.

Important

If your deployment uses IWA and a load balancer:

- Version 7.8.1 does not support the configuration.
- Versions 7.8.2 and 7.8.3 support load balancers, however, post-upgrade a special configuration must be applied. Follow the configuration steps described in the v7.8.2 Release Notes or the v7.8.3 Release Notes.

Features to configure after upgrade

You may want to review and configure the following enhanced features post-upgrade.

- Range-based IP spoofing. If you use IP spoofing, see the Help system for information about how range-based IP spoofing can address a boarder range of source IP address requirements when traffic is routed through Content Gateway.
- WCCP configuration synchronization in a cluster. It's now possible to disable WCCP configuration synchronization.

Upgrade sequence for TRITON Enterprise

If you have a mixed topology, upgrade components in the following order:

1. The machine hosting Web Security **Policy Broker**
   - For a software installation, run the TRITON Unified Installer.
   - If Policy Broker is on the TRITON management server, you can upgrade the TRITON infrastructure and Web, Email, and Data Security management components at the same time as upgrading Policy Broker.
   - After Policy Broker is upgraded, Content Gateway instances on other machines do not perform Web filtering until they are also upgraded.
2. Additional instances of Web Security **Policy Server**
   - May be software-based or on **user directory and filtering** appliances. For a software installation, run the TRITON Unified Installer. For an appliance, install the v7.8 upgrade patch.
   - If Policy Server is on an appliance, it *does not matter* whether the appliance is running in Web Security or Web and Email Security mode.
3. Additional instances of Web Security **Filtering Service** or **User Service**
   - Additional instances of Filtering Service may be software-based or on **filtering only** appliances.

- If Filtering Service is on an appliance, it *does not matter* whether the appliance is running in Web Security or Web and Email Security mode.
- If you have filtering only appliances in your deployment, upgrade these appliances **after** the corresponding full policy source or user directory and filtering appliance has been upgraded. This is because appliances that have instances of Policy Server must be upgraded before you upgrade any components that point to it.

4. Web and Email Security **Log Server**

   If these components are on separate machines, it does not matter which is upgraded first.

   

   Important

   Make sure that no Email Security Log Database or Web Security Log Database jobs are running while the Log Server instances are being upgraded.

5. **TRITON management server** (if not already upgraded as part of an earlier step)
   - Whenever possible, upgrade the management server before any other Data Security components. This ensures that Data Security policy engines (and thus analysis) continue to function until they are upgraded themselves.

     Note that you cannot deploy new policies to the policy engines until they are upgraded to the same version as the management server.
   - If you need to upgrade a Data Security policy engine before upgrading the TRITON management server—because the policy engine resides on a full policy source appliance—detection of fingerprinted content might not work on the appliance until the management server is upgraded.

     The Data Security policy engine embedded in Content Gateway and Email Security Gateway continues to monitor the old Web and email DLP policies and block/permit accordingly.
6. Upgrade all other appliances in your network. This can be done in any order, and can be completed in parallel.
   - If you have deployed Email Security Gateway in cluster mode, ensure you upgrade the primary appliance before any secondary appliances. You do not need to release the appliances from the cluster in order to perform the upgrade.
   - The Email Security Gateway MTA continues to function after the management server upgrade, but the logs are cached on the appliance until Email Security Gateway is upgraded as well. For best practice, redirect email traffic to another MTA as cached messages may be lost otherwise.
   - If your appliances are running in Web and Email Security mode, all appliances may already have been upgraded in steps 1-3.
7. Upgrade all other **Web Security** and **Data Security** components. This can be done in parallel. For example:
   - Network Agents

- XID Agents
- Remote Filtering server
- Data Security secondary servers
- Data Security components on ISA and TMG servers
- software-based installations of Content Gateway

Upgrade procedure for TRITON Enterprise

This procedure covers the steps required to upgrade either the whole of Websense TRITON Enterprise or a Web and Email Security solution. (Note that Email Security Gateway and Gateway Anywhere always include Data Security components.)

- *Step 1: Upgrade the Policy Broker machine*, page 13
- *Step 2: Upgrade additional Policy Server machines*, page 15
- *Step 3: Upgrade additional Filtering Service and User Service machines*, page 17
- *Step 4: Upgrade Log Servers*, page 18
- *Step 5: Upgrade the TRITON Management Server*, page 19
- *Step 6: Upgrade appliances*, page 23
- *Step 7: Upgrade additional components*, page 23

Step 1: Upgrade the Policy Broker machine

You must upgrade the machine that hosts **Websense Policy Broker** first, regardless of which other components on are on the machine. Policy Broker may reside on:

- A Websense **full policy source** appliance
- A Windows Server 2008 R2 or Windows Server 2012 Standard Edition machine
- A RHEL 6.x machine

Any other components on the Policy Broker machine are upgraded along with Policy Broker.

> **Important**
>
> If you are upgrading from earlier 7.8.x versions and your configuration includes a primary Policy Broker and one or more replica Policy Brokers, you must upgrade the primary Policy Broker first. An attempt to upgrade a replica Policy Broker without first upgrading the primary will result in an error message. You will be required to exit the upgrade for that machine and upgrade the primary Policy Broker before continuing.
>
> Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with them. If Policy Server is installed on the same machine, it will be upgraded at the same time.

If Policy Broker resides on the TRITON management server, running the TRITON Unified Installer also upgrades the TRITON infrastructure and web, data and email management components as described in *Step 5: Upgrade the TRITON Management Server*, page 19. Ensure you also follow the steps in *After upgrade*, page 22 to configure the TRITON management server.

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see the Upgrade Instructions for Web Security Gateway Anywhere.

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

   > **Important**
   >
   > If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   > **Warning**
   >
   > Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON782Setup.exe**.

- Installer files occupy approximately 2 GB of disk space.

5. Right-click **WebsenseTRITON782Setup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks whether you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.

    If Policy Broker resides on the TRITON management server, or on the same machine as Log Server, the upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

    Important
    The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 2: Upgrade additional Policy Server machines

The central Policy Server resides on the same machine as Policy Broker, and was automatically upgraded in the previous section.

If you have additional Policy Server instances, upgrade them next, regardless of what other services reside on the machines. Policy Server may reside on:

- Websense **user directory and filtering** appliances
- Windows Server 2008 R2 or Windows Server 2012 Standard Edition machines
- RHEL 6.x machines

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see the Upgrade Instructions for Web Security Gateway Anywhere.

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

   

   Important

   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   

   Warning

   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON782Setup.exe**.
   - Installer files occupy approximately 2.5 GB of disk space.
   - Verify that the MD5 value of the downloaded file matches the value shown on the download page.
5. Right-click **WebsenseTRITON782Setup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.

10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.

11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 3: Upgrade additional Filtering Service and User Service machines

If you have additional Filtering Service or User Service instances, upgrade them next, regardless of what other services reside on the machines. Filtering Service and User Service may reside on:

- Windows Server 2008 R2 machines
- RHEL 6.x machines

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

> **Important**
> If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

> **Warning**
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON782Setup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
5. Right-click **WebsenseTRITON782Setup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the C:\Program Files (x86)\Websense\Web Security**WebsenseAdmin stop** command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 4: Upgrade Log Servers

Upgrade the Web Security and Email Security Log Server machines, if they have not already been upgraded with other components. Any other services on the machine are also upgraded in the correct order.

For information on Web Security Log Server, see Upgrade Instructions for Web Security Gateway Anywhere.

For information on Email Security Log Server, see Upgrade Instructions for Email Security Gateway.

Step 5: Upgrade the TRITON Management Server

If you have not already upgraded the TRITON management server in the course of upgrading another component, use the following steps to upgrade the management server machine.

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.
3. Close all applications and stop any antivirus software.

> **Warning**
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON782Setup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
5. Right-click **WebsenseTRITON782Setup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Websense components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens that appear in subsequent stages of the upgrade.
8. Follow the screens in the upgrade wizard as described in the sections below:
   - *TRITON Infrastructure*
   - *Web Security*
   - *Data Security*
   - *Email Security*
9. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
10. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

11. If you stopped your antivirus software, restart it.
12. Follow the instructions in *After upgrade*, page 22.

TRITON Infrastructure

The TRITON infrastructure provides basic framework for all of the management components that make up TRITON Unified Security Center (TRITON console). This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Welcomes you to the installation and upgrade wizard. 1. Click **Next** to begin the upgrade process. The system checks disk space requirements. 2. When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows: • The destination folder for the installation files. • The name of the SQL Server machine and the user name of an authorized database administrator. • The IP address of the TRITON management server and administrator credentials. Click **Next** to accept the properties.
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage,warning that you must also upgrade all modules. This popup may be hidden behind the main installer window, so if your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation.
Summary	When module upgrade is complete, summarizes your system settings, including: • The destination folder for the installation files. • The name of the SQL Server machine and the user name of an authorized database administrator. • The IP address of the TRITON management server and administrator credentials. Click **Finish** to complete the upgrade for this module.

Web Security

The Web Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	Welcomes you to the Web Security upgrade wizard. Click **Next** to continue.
Pre-Installation Summary	Informs you that a previous Web Security software version was detected. 1. Click **Next** to start the upgrade. The installer proceeds to stop all Websense services. This can take up to 10 minutes. When complete, it tells you which components will be upgraded. 2. Click **Install** to continue. The installer to backs up critical files.
Installation	Shows installation progress. When complete, the installer configures your software. This can take up to 10 minutes.
Installation Complete	You're notified when installation of this module is complete. Click **Done** to exit the installer.

Data Security

The Data Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard for Data Security. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Installation Confirmation	Verify your system settings and click **Install** to continue the upgrade.
Installation	This screen shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more.
Summary	When installation of this module is complete, this screen summarizes your system settings. 1. Click **Done** and you're prompted to update your predefined policies and content classifiers. 2. Click **OK** to install the updates. You're shown the status of the updates, the items being updated, and details such as how many policies are updated, deleted, or added. 3. Click **Close** when the updates are complete.

Email Security

The Email Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	This screen welcomes you to the Email Security upgrade wizard. Click **Next** to continue.
Select Components	This screen shows the components that will be upgraded (those that are currently installed). Click **Next** to continue.
Configuration	This page shows the IP address of the database engine configured to manage the Email Security Log Database and the logon type. If you have changed the database since your previous installation, modify the settings here.
Pre-Installation Summary	This screen shows: • The components to be installed • The pre-existing and new version numbers • The destination folder for the installation files • The required and available disk space Click **Install** to begin the upgrade.
Installation	This screen shows that the installation is progressing. The management component, Email Security manager, is upgraded on the TRITON management server. The Email Security Log Server is upgraded on machines where it is found. When complete, the installer configures your Email Security software. This can take up to 10 minutes.
Summary	You're notified when installation of this module is complete. Click **Done** to exit the installer.

After upgrade

Once the TRITON management server upgrade is complete:

1. Log onto the TRITON console (https://<IP_address_or_hostname>:9443/triton/).
2. Select the Email Security tab.
3. In Email Security manager, navigate to **Settings** > **General** > **Data Security** and click **Unregister**.
4. Click **Register** to re-register the Email Security Gateway appliance with Data Security.
5. Select the Data Security tab and click **Deploy**.
6. You are prompted to update your policies. Follow the prompts. Websense research teams stay abreast of regulations across many industries and you should keep your policies and classifiers up-to-date. Depending on the number of policies you have, this can take up to an hour. During this time, do not restart the server or any of the services.
7. Click **Deploy**.

8. For Email Security Gateway, access Email Security manager and navigate to the **Settings > General > Database Downloads** page. Click **Update Now** to perform an immediate database download update.

Step 6: Upgrade appliances

Upgrade all appliances that have not been upgraded in the above steps. This can be done in any order, and can be completed in parallel.

If you have deployed Email Security Gateway in cluster mode, ensure you upgrade the primary appliance before any secondary appliances. You do not need to release the appliances from the cluster in order to perform the upgrade.

For more information, see the Websense V-Series Appliance Upgrade Guide.

Step 7: Upgrade additional components

Once you have completed the above steps, you can upgrade any additional software components and client conponents:

1. Upgrade any additional software instances of Websense Network Agent and Content Gateway. If these components run on V-Series appliances, this step has already been done.
2. Upgrade any additional Web Security server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines.
3. Upgrade supplemental servers, SMTP agents, ISA/TMG agents, printer agents, protectors, and mobile agents.
4. Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, Web Endpoint, and Data Endpoint.

These actions can be done in parallel. For more information, see the following upgrade guides:

- Upgrade Instructions for Web Security Gateway Anywhere
- Upgrade Instructions for Data Security