Upgrading TRITON Enterprise v7.6.x to v7.7.x

Upgrade Instructions | Web, Data, and Email Security Solutions | Version 7.7.x

This guide describes how to upgrade Websense TRITON Enterprise solutions that include Websense Web Security, Email Security, and Data Security from v7.6.x to v7.7.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.

To upgrade your TRITON Enterprise modules to v7.7.x, perform the following steps, in order:

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.

Before upgrading Web, Email, and Data Security

Several ports have changed in v7.7. You must configure your firewall to open the new ports before upgrading to v7.7.

- The new ports for communicating with the Data Security Management Server for data loss prevention are 17500-17515. Content Gateway, Email Security Gateway, and all Data Security components communicate with this server.
- The ports for communicating with Email Security Gateway have also changed. They are 17700-17714.

You can reconfigure the base port after upgrade using the Modify wizard if desired.

In addition:

- Unless instructed otherwise by Websense Technical Support, ensure your system is functional prior to upgrade.
- Perform a full backup of your system before upgrading. See:
  - Backing up TRITON infrastructure settings
  - Backing up Web Security configuration
  - How do I back up and restore Websense Content Gateway?
  - Preparing the Web Security Log Database for upgrade
  - Back up appliance configuration and settings
  - How do I back up and restore Data Security software?
- If you are upgrading Data Security:
  - Disable all network and endpoint discovery tasks as well as all fingerprinting tasks so that they don't run during the upgrade process. Wait until there are no new endpoint discovery incidents appearing in the Data Security incidents report.
  - Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.
  - Download the pre-upgrade tool **dss_773_pre_upgrade_tool.zip** from MyWebsense. This tool should be used for upgrades from 7.6.3 to 7.7.0 or 7.7.2, and for upgrades from 7.7.0 or 7.7.2 to 7.7.3. Place the file in any folder on the management server, extract and run it. It requires administrator permissions, so depending on your UAC settings you may be prompted to allow it to run as Administrator. When the tool has finished, a log file displays results.

    If the tool cannot connect to your SQL server, it saves 5 SQL files in the same folder as the tool—**dss_sql_script_1.sql** to **dss_sql_script_5.sql**. You can log onto the server and run the SQL portion of the tool manually by executing the files in order.
  - If you are upgrading to Data Security v7.7.0, ensure that the user name and password set for the TRITON Unified Security Center account/Local Administrator account does not exceed 19 characters. Modify these settings if necessary. If you are upgrading it to v7.7.2 or beyond, this is not necessary.
- The TRITON 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. The upgrade process does not allow you to change your configuration or settings.

Also see:

- Web Security: Before upgrading Web Security to v7.8
- Appliance: Preparing for the appliance upgrade

Upgrade sequence for solutions that include Web, Email, and Data Security

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

1. The machine hosting Web Security **Policy Broker**
   - This may be a software (Windows or Linux) installation or the **full policy source** appliance.

     If Policy Broker is on an appliance, it *does not matter* whether the appliance is running in Web Security or Web and Email Security mode.
   - If Policy Broker is on the same machine as other Web, Data, or Email Security components, still upgrade the Policy Broker machine first.
   - 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.
   - 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.
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** (includes TRITON infrastructure, as well as Web, Email, and Data Security management components)
   - 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. Any appliances running in **Email Security** mode
   - 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, upgrade Email Security Gateway as soon as possible after the management server, or email traffic must be redirected to another MTA.
   - If your appliances are running in Web and Email Security mode, all appliances may already have been upgraded in steps 1-3.
7. Other **Web Security** components (including software-based installations of Content Gateway)
8. Other **Data Security** components

Important

The components running on the machine you are upgrading go down until the upgrade is complete. You should plan for a brief period of down time.

Upgrade procedure for solutions that include Web, Email, and Data Security

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.)

1. Upgrade Websense **Policy Broker**. All components on the Policy Broker machine (which may be a **full policy source** appliance in either Web Security or Web and Email Security mode) are upgraded in the correct order. For instructions, see:
   - v7.7 Web Security software upgrade instructions (Windows)
   - v7.7 Web Security software upgrade instructions (Linux)
   - Upgrading V-Series Appliances to v7.7
2. Upgrade any instances of Websense **Policy Server** running off the Policy Broker or machine. All components on each Policy Server machine, including **user directory and filtering** appliances, are upgraded in the correct order. For instructions, see:
   - v7.7 Web Security software upgrade instructions (Windows)
   - v7.7 Web Security software upgrade instructions (Linux)

- Upgrading V-Series Appliances to v7.7

3. Upgrade any additional instances of Websense **Filtering Service** and **User Service**, running on other machines. All components on each machine, including **filtering only** appliances, are upgraded in the correct order. For instructions, see:
   - v7.7 Web Security software upgrade instructions (Windows)
   - v7.7 Web Security software upgrade instructions (Linux)
   - Upgrading V-Series Appliances to v7.7
4. Upgrade Web Security and Email Security **Log Server**. All components on the machine are upgraded in the correct order. For instructions, see:
   - v7.7 Web Security software upgrade instructions (Windows)
   - Email Security upgrade instructions
5. Upgrade the **TRITON management server**. All modules on the machine are upgraded in the correct order. See *Upgrading the TRITON Management Server*, page 5.
6. 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. See:
   - Upgrading Content Gateway to v7.8.x
   - v7.7 Web Security software upgrade instructions (Windows)
   - v7.7 Web Security software upgrade instructions (Linux)
7. Upgrade any additional Web Security server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines. See:
   - v7.7 Web Security software upgrade instructions (Windows)
   - v7.7 Web Security software upgrade instructions (Linux)
8. Upgrade any additional Data Security server components and agents, including supplemental servers, SMTP agents, ISA/TMG agents, printer agents, protectors, and mobile agents. See:
   - Upgrading supplemental Data Security servers or standalone agents
   - Upgrading a Data Security protector or mobile agent
9. Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, Web Endpoint, and Data Endpoint. See:
   - Installing and Deploying Websense Endpoint Clients
   - Upgrading Data Security endpoints

Upgrading the TRITON Management Server

To upgrade TRITON management server components, use the v7.7 TRITON unified installer (Windows only): **WebsenseTRITON77Setup.exe**, available from:

www.websense.com/MyWebsense/Downloads/

Select your **product**, **version** (7.7), and **operating system** (Windows), then click **download** next to the installer description.

When you launch the installer, it detects that earlier versions of the product are installed, compares the installed version with the latest available version, and automatically starts a series of upgrade wizards for each module that require update. On occasion, the modules may be at different versions. For example, Web Security Gateway and Content Gateway can be upgraded to v7.7.4, but Data Security and Email Security's latest release is v7.7.3.

> **Note**
> If TRITON management components run on a virtual machine, restart the server after the upgrade is complete.

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.

Wizard Screen	Fields
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more.
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.

Wizard Screen	Fields
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.

1. Log onto the TRITON console (https://<IP_address_or_hostname>:9443/triton/).
2. Select the Data Security tab.
3. 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.
4. After your policies are updated, select **Settings > Deployment > System Modules**.
5. Listed are 2 instances of each Web Content Gateway module that is registered with the system. Delete the older instances. You can identify these by looking at the version number that is displayed.
6. If you are upgrading from v7.6.x to v7.7.0 or v7.7.2 and you use regulatory and compliance attributes in your quick policies, do the following to restore your settings. (You do not need to do this if you are upgrading to v7.7.3).
    a. Select **Main > Policy Management > DLP Policies**.
    b. One by one, open your quick policies—Web DLP, email DLP, and mobile DLP.
    c. Select the regulatory and compliance attribute. For Web and mobile DLP, this attribute is on the Attributes tab. For email DLP it is on the Outbound and Inbound tabs.
    d. Select the laws to enforce. You wrote these down before starting the upgrade.
7. Click **Deploy**.

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, TRITON - Email Security, 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.