Changing the TRITON management server IP address or name

Topic 50610 | Management Server Location Change | Web, Data, and Email Security Solutions | Version 7.8.x

This collection of articles describes the configuration changes needed if you modify the IP address or hostname of the TRITON management server.

> **Note**
>
> In v7.8.x, you cannot modify management server domains. This would require you to change the local administrator user name and the installer does not allow this.

These articles also describe how to move the Web Security or Data Security manager to a new machine. See:

- *Changing the IP address of the TRITON management server*, page 3
- *Changing the hostname of the TRITON management server*, page 6
- *Configuring TRITON Infrastructure to use a new IP address or hostname*, page 7
- *Configuring Tomcat to a use new local IP address*, page 7
- *Configuring a new hostname for the Web Security management components*, page 8
- *Changing the IP address of the Data Security Management Server*, page 9
- *Changing the hostname of the Data Security Management Server*, page 10
- *Configuring a new hostname for the Web Security management components*, page 8
- *Updating the Log Database location for Email Security Gateway*, page 12
- *Re-registering Email Security Gateway with Data Security*, page 14
- *Migrating the Web Security manager off of a Websense appliance*, page 14
- *Migrating the Data Security manager from server A to server B*, page 19
- *Re-registering Data Security components*, page 20
- *Creating Apache SSL Certificates*, page 23

These articles cover the following management components. Any other Websense components on the management server machine may need additional configuration that is not covered in this article.

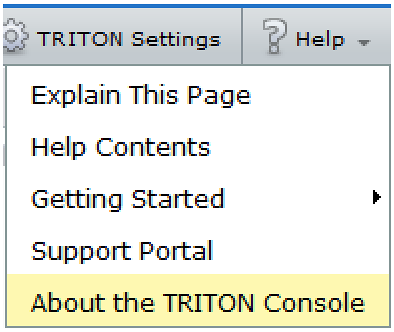
- For TRITON infrastructure:
  - Websense TRITON Unified Security Center
  - Websense TRITON Web Server
  - Websense TRITON Settings Database
- For Web Security solutions:
  - Websense Control Service
  - Websense TRITON - Web Security
  - Websense Web Reporting Tools
  - Websense RTM Client
  - Websense RTM Database
  - Websense RTM Server
  - Websense Explorer Report Scheduler
  - Websense Information Service for Explorer
  - Websense Reporter Scheduler
  - Websense Linking Service
  - (not recommended) Websense Log Server

    If Log Server is installed on the machine, remove it before changing the IP address.
- For Data Security solutions:
  - Websense Data Security Management Server
  - Websense Data Security Manager
  - Websense Data Security Policy Engine
  - Websense Data Security PreciseID Database
  - Websense Data Security Web Server
  - Websense Data Security Work Scheduler
- For Email Security Gateway and Gateway Anywhere:
  - Websense TRITON - Email Security
  - (not recommended) Websense Email Security Log Server

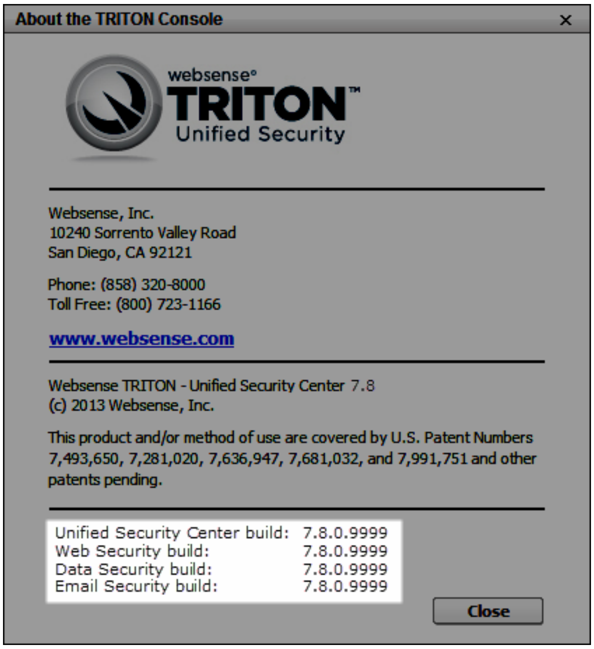
Each module of the TRITON Unified Security Center (TRITON console) must be configured separately. Depending on your subscription, you may not have all modules enabled.

To determine which TRITON Unified Security Center modules are active in your deployment:

1. In the TRITON console, go to **Help** > **About the TRITON Console**.



2. The About the TRITON Console dialog box lists the modules that are active (highlighted in illustration below).



Websense, Inc.
10240 Sorrento Valley Road
San Diego, CA 92121

Phone: (858) 320-8000
Toll Free: (800) 723-1166

www.websense.com

Websense TRITON - Unified Security Center 7.8
(c) 2013 Websense, Inc.

This product and/or method of use are covered by U.S. Patent Numbers 7,493,650, 7,281,020, 7,636,947, 7,681,032, and 7,991,751 and other patents pending.

```
Unified Security Center build:  7.8.0.9999
Web Security build:             7.8.0.9999
Data Security build:            7.8.0.9999
Email Security build:           7.8.0.9999
```

Changing the IP address of the TRITON management server

Topic 50611 | Management Server Location Change | Web, Data, and Email Security Solutions | Version 7.8.x

Warning

If Web Security policy (Policy Broker, Policy Server, Policy Database) or hybrid (Directory Agent, Sync Service) components reside on the TRITON management server, the process of changing the IP address is complicated. Please contact Technical Support for assistance.

Before changing the IP address of the TRITON management server, if Web Security Log Server is installed on the management server machine, remove it. The steps below include instructions for reinstalling it after the IP address change is complete.

Complete the following steps **after** changing the IP address of the TRITON management server.

1. Update TRITON Infrastructure with the new IP address.

   See *Configuring TRITON Infrastructure to use a new IP address or hostname*, page 7, for instructions.

   If SQL Server 2008 R2 Express (SQL Server Express) is installed on this machine, it will be automatically configured to the new IP address along with TRITON Infrastructure.

2. (*Web Security only*): Update the configuration of the Web Security module to reflect the new IP address:

   a. Recreate Apache SSL certificates for the Web Security manager. See *Creating Apache SSL Certificates*, page 23. When following these instructions, be sure to edit the **openssl.txt** file to reflect the new IP address of the TRITON management server.

   b. Edit the Web Security **catalina.properties file** to reflect the new IP address. See *Configuring Tomcat to a use new local IP address*, page 7.

   c. Navigate to the Web Security **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin\, by default) and open the **websense.ini** file in a text editor.

      Update the value of the **LocalServerIP** parameter to the new IP address.

   d. If you want to run Web Security Log Server on the management server (not recommended), and removed it as instructed before changing the IP address of the server, open a Windows command prompt and run the following commands from the C:\Program Files (x86)\Websense\Web Security\bin\ directory:

      ```
      LogServer.exe -i
      LogServer.exe -r
      ```

   e. Log onto the Web Security manager and navigate to **Settings** > **Reporting** > **Log Server** page.

   f. Verify that correct information appears in the **SQL Server location** field.

If you change the SQL Server location value, use the Windows Services tool to restart **Websense Log Server**.

g. Use the Windows Services tool to restart the **Websense RTM Server** and **Websense RTM Client** services.

After changing the Log Server IP address, if alerts appear from old IP address, restart Policy Server to clear the old alert data.

3. (*Email Security only*): Edit the Email Security **catalina.properties** file to reflect the new IP address. See *Configuring Tomcat to a use new local IP address*, page 7.
4. (*Email Security only*): If Email Security Log Server is installed on the TRITON management server machine, update TRITON Unified Security Center with its new IP address. See *Configuring a new hostname for the Web Security management components*, page 8.

   ✓ **Note**

   This is required only for those appliances using the Email Security Log Server located on the TRITON management server machine. If an appliance is using an Email Security Log Server located elsewhere, do not update its IP address on that appliance.

   If you have multiple Email Security Gateway appliances in your deployment, update them as well with the new IP address of Email Security Log Server. To update other appliances, complete the steps again in *Configuring a new hostname for the Web Security management components*, page 8 with the following modifications:

   a. After logging into the TRITON Unified Security Center, click **Appliances** in the TRITON Unified Security Center banner.

   b. Click **Manage Appliances** and select the appliance you want to update.

   c. Continue with the rest of the procedure as normal.

   d. Repeat this process for each Email Security Gateway appliance that uses the Email Security Log Server located on the TRITON management server machine.
5. (*Email Security only*): If the Email Security Log Database is located on the TRITON management server machine (e.g., SQL Server 2008 R2 Express is installed on the machine and maintains the log database), update the database location in TRITON Unified Security Center. See *Updating the Log Database location for Email Security Gateway*, page 12.
6. (*Data Security only*): Modify the Data Security Management Server installation to reflect the change. See *Changing the IP address of the Data Security Management Server*, page 9.
7. If your subscription includes Websense Web Security Gateway Anywhere, Email Security Gateway, or Email Security Gateway Anywhere, re-register them with Data Security Management Server (located on the TRITON management server machine). This is required for Web and email DLP (data loss prevention) features.

For Web Security Gateway Anywhere, see *Re-register Websense Content Gateway*, page 21.

For Email Security Gateway, see *Re-registering Email Security Gateway with Data Security*, page 14.

Changing the hostname of the TRITON management server

Topic 50612 | Management Server Location Change | Web, Data, and Email Security Solutions | Version 7.8.x

If SQL Server 2008 Express R2 is installed on the management server, perform the following steps **before** changing the hostname:

1. Log on to SQL Server Management Studio and click **New Query**.
2. In the query window, enter the following commands:

   ```
   Use master;
   GO
   sp_dropserver '<original_hostname>';
   GO
   sp_addserver '<new_hostname>', local;
   GO
   ```

   Replace <original_hostname> and <new_hostname> with the actual original and new (planned) names.
3. Close SQL Server Management Server, then use the Windows Services tool to restart the **SQL Server (MSSQLSERVER)** service.

After changing the TRITON management server hostname, do the following:

1. If you have not done so already, change the hostname of the TRITON management server machine at the operating system level (i.e., in Windows).

   Note that changing the hostname typically requires a reboot of the machine.
2. Update TRITON Infrastructure with the new hostname.

   See *Configuring TRITON Infrastructure to use a new IP address or hostname*, page 7 for instructions.

   If SQL Server 2008 R2 Express (SQL Server Express) is installed on this machine, it is **not** automatically configured to use the new hostname along with TRITON Infrastructure. It must be configured separately. See the following Microsoft article for instructions:

   http://msdn.microsoft.com/en-us/library/ms143799.aspx
3. (*Web Security*): Edit the Web Security configuration to reflect the new hostname. See *Configuring a new hostname for the Web Security management components*, page 8.
4. (*Data Security*): Modify the Data Security Management Server installation to reflect the change.

Configuring TRITON Infrastructure to use a new IP address or hostname

Topic 50613 | Management Server Location Change | Web, Data, and Email Security Solutions | Version 7.8.x

If you change the IP address or hostname of the TRITON management server, update your TRITON Infrastructure configuration to reflect the change.

1. Launch the Websense installer.

   If you chose to keep installer files the last time you ran the installer, you can launch it without re-extracting files by going to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** (Windows 2008) or by navigating to the **Windows\Installer\{E546...}** directory (Windows 2012).
2. In the installer, for TRITON Infrastructure, select the **Modify** link.
3. Accept the defaults in the installer screens and click **Next**, until you reach the **Server & Credentials** screen. On that screen:
   - If you changed the IP address of the TRITON management server, select the new address from the **IP address** drop-down list.
   - If you changed the hostname of the TRITON management server, make sure the correct information appears in the **Server or domain** field.
4. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.

Configuring Tomcat to a use new local IP address

Topic 50614 | Management Server Location Change | Web, Data, and Email Security Solutions | Version 7.8.x

If you have changed the IP address of the TRITON management server, you must complete the following steps to update the Tomcat configuration for the Web Security and Email Security management services.

✓ **Note**

Tomcat configuration for TRITON Infrastructure and the Data Security manager is done automatically when configuring to new IP address or hostname. See *Configuring TRITON Infrastructure to use a new IP address or hostname*, page 7.

Warning

This procedure involves editing configuration files. Before editing any file make a backup copy of it. This allows you to revert to original, unmodified files if any issues arise.

1. Open the following file in a text editor:
   - Web Security:

     C:\Program Files (x86)\Websense\Web Security\tomcat\conf\catalina.properties
   - Email Security:

     C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\conf\catalina.properties
2. In the file, edit the following value to reflect the new IP address:
   - Web Security:

     java-fw.ip
   - Email Security:

     manager_ip
3. Save and close the **catalina.properties** file.
4. Use the Windows Services tool to restart the service for the module you want to update:
   - Websense TRITON - Web Security
   - Websense TRITON - Email Security

Configuring a new hostname for the Web Security management components

Topic 50618 | Management Server Location Change | Web Security Solutions | Version 7.8.x

If the hostname of the TRITON management server has changed, edit your Web Security configuration to reflect the change.

Warning

This procedure involves editing configuration files. Before editing any file make a backup copy of it. This allows you to revert to original, unmodified files if any issues arise.

1. Navigate to the **C:\Program Files (x86)\Websense\Web Security\apache\conf\** directory and open the **httpd.conf** file in a text editor.
2. In the **httpd.conf** file, edit the **ServerName** property to reflect the new hostname.

   ServerName is specified in the form <*hostname*>:<*port*>, for example:

   ```
   ServerName my-hostname01:18080
   ```

Edit only the hostname value.

3. Save and close the **httpd.conf** file.
4. Navigate to the **C:\Program Files (x86)\Websense\Web Security\apache\conf\extra\** directory and open the **httpd-ssl.conf** file in a text editor.
5. In the **httpd-ssl.conf** file, edit the **ServerName** property to reflect the new hostname. This entry uses the same format shown in step 2.

   Edit only the hostname value.
6. Save and close the **httpd-ssl.conf** file.
7. Use the Windows Services tool to restart the **Websense Web Reporting Tools** service.

Changing the IP address of the Data Security Management Server

Topic 50619 | Management Server Location Change | Data Security Solutions | Version 7.8.x

Perform this task during off hours, or route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.) while you are performing the task.

It is assumed you have already changed the IP address of the TRITON management server machine. If not, see *Changing the IP address of the TRITON management server*, page 3.

Important

If you change both the IP address and hostname of a server (or the IP address):

- You must complete the entire process of updating one before starting to change the other (and wait for all endpoints to be updated).
- If any endpoints are not connected to the network when settings are deployed, you must create a new endpoint package using the package-building tool, and use SMS or a similar mechanism to install the new package on these endpoints.

1. Stop the protector:
   a. Log onto the protector as **root**.
   b. Execute **service pama stop**.
2. On the TRITON management server, launch the Websense installer.

   If you chose to keep installer files the last time you ran the installer, you can launch it without re-extracting files by going to **Start** > **All Programs** >

Websense > **Websense TRITON Setup** (Windows 2008) or by navigating to the **Windows\Installer\{E546...}** directory (Windows 2012).

3. In the installer, for Data Security, select the **Modify** link.
4. Accept the defaults in the installer screens, and then click **Next** until you reach the **Server Access** screen. Select the new IP address here.
5. If you changed the hostname of the TRITON management server, the installer will automatically detect the new settings and configure TRITON Infrastructure.
6. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.
7. If you have a mail server relaying SMTP traffic to the Websense Data Security Management Server (SMTP agent), change its configuration to relay mail to the new Websense Data Security Management Server IP address.
8. In the Data Security manager, change the IP address on the following pages, if necessary:
   a. **Settings > Configuration > System** > **Archive Storage**
   b. **Settings > Deployment > System Modules**. Choose the **SMTP Agent** and click the **Encryption & Bypass** tab.
9. Re-register all Websense Data Security stand-alone agents, such as: ISA agent, Exchange agent, and printer agent (See *Re-registering Data Security components*, page 20).
10. Start the protector:
    a. Log onto the protector as **root**.
    b. Execute **service pama start**.
11. Click **Deploy** in the Data Security manager.
12. Since management server IP address was changed, all endpoints must be reinstalled with the new IP address.
13. Verify that new events appear in the traffic log, the system log doesn't display errors, the endpoint status shows that endpoints are synchronized, and that new incidents are written into the data usage incident management screen.

Changing the hostname of the Data Security Management Server

Topic 50620| Management Server Location Change | Data Security Solutions | Version 7.8.x

Perform this task during off hours, or route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.) while you are performing the task.

It is assumed you have already changed the hostname of the TRITON management server, if not see *Changing the hostname of the TRITON management server*, page 6.

> ✓ **Note**
>
> To change both the IP address and hostname of a server, you must complete the entire process of updating one before starting to change the other (and wait for all endpoints to be updated).

1. Stop the protector:
   a. Log onto the protector as **root**.
   b. Execute **service pama stop**.
2. On the TRITON management server, launch the Websense installer.

   If you chose to keep installer files the last time you ran the installer, you can launch it without re-extracting files by going to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** (Windows 2008) or by navigating to the **Windows\Installer\{E546...}** directory (Windows 2012).
3. In the installer, for Data Security, select the **Modify** link.
4. Click **Next** in the Installation Wizard until you get to **Local Administrator.**
5. Choose the new server name and the correct user name (in the form "NEWNAME\UserName").
6. Start the protector:
   a. Log onto the protector as **root**.
   b. Execute **service pama start**.
7. Click **Next** to finish the modification.
8. (Optional) In the Data Security manager, change <New Server Name> in the following places:
   a. Select **Settings > System Modules**.
   b. Click the **Data Security Management Server.**
   c. One at a time, click the **Endpoint Server**, **Policy Engine**, **Forensics Repository**, **SMTP Agent**, **PreciseID Database**, and **Crawler**, and change the server name in the Name field.
9. Click **Deploy** in the Data Security manager.

> ✓ **Note**
>
> If any endpoints are not connected to the network when settings are deployed, they will not be updated. In this case, you must create a new endpoint package using the package-building tool, and use SMS or a similar mechanism to install the new package on these endpoints.

10. Verify that new events appear in the traffic log, the system log doesn't display errors, the endpoint status shows that endpoints are synchronized, and that new incidents are written into the data usage incident management screen.

Updating the IP address for Email Security Log Server

Topic 50615 | Management Server Location Change | Email Security Solutions | Version 7.8.x

If the IP address of the machine running Email Security Log Server is changed, you must update the Email Security manager to use the new address.

1. Log on to the Email Security manager.
2. On the **Settings > Reporting > Log Server** page, enter the new IP address in the **Log Server** field.
3. Click **OK**.

Updating the Log Database location for Email Security Gateway

Topic 50616 | Management Server Location Change | Email Security Solutions | Version 7.8.x

If the IP address of the Email Security Log Database machine (the IP address of the SQL Server machine) has changed, update TRITON Unified Security Center and Email Security Log Server to use the new address.

Complete these steps even if the Email Security Log Database is located on the same machine as TRITON Unified Security Center or Email Security Log Server.

1. Log on to the TRITON Unified Security Center and click **Email Security**.
2. Go to **Settings > Reporting > Log Database** and enter the new IP address in the **Log database** field.

   If the Email Security database is located on the TRITON management server itself and you are performing this procedure because you changed the IP address of the TRITON management server, you should enter its new IP address here.
3. Click **OK** (in the Log Database Location area of the screen).

   Leave the TRITON Unified Security Center at this screen.You will come back to it later to complete this procedure.
4. On the machine running Email Security Log Server, start the Log Server Configuration utility (**Start > All Programs > Websense > Email Security > Email Security Log Server Configuration**).
5. In the **Database** tab, click **Connection** to open the **Select Data Source** dialog box.
6. Select the **Machine Data Source** tab and click **New** to open the Create New Data Source dialog box.

You will create a new data source connection to the new IP address of the Email Security database.

7. Select **System Data Source (Applies to this machine only)** and then click **Next**.
8. In the list of drivers, select **SQL Server** and then click **Next**.
9. In the next dialog box, click **Finish**.
10. In the **Create a New Data Source to SQL Server** wizard, enter a **Name**, **Description**, and the **Server** IP address for the new data source connection. Then click **Next**.

    The server IP address should be the new IP address of the machine on which the Email Security database is located. If the database is located on the TRITON management server and you are performing this procedure because you have changed the management server's IP address, enter its new IP address here.
11. In the next dialog box, select options as described below.
    a. Select an authentication method for connecting to the database:
       - **With Windows NT authentication using the network login ID**: to use a Windows trusted account.
       - **With SQL Server authentication using a login ID and password entered by the user**: to use a SQL Server account.

    b. Enable **Connect to SQL Server to obtain default settings for the additional configuration options**.

    c. Enter the **Login ID** and **Password** of the **sa** SQL Server account if you selected SQL Server authentication in Step a above).

    d. Click **Next**.
12. In the next dialog box, enable **Change the default database to** and then select **esglogdb7*x*** from the drop-down menu. Then click **Next**.
13. In the next dialog box, accept the default settings and click **Finish**.
14. Click **Test Data Source** to test the connection. Upon test success, click **OK**.
15. Click **OK**, then click **OK** once more.
16. In the SQL Server Login dialog box, enter a **Login ID** (by default, sa) and **Password**. Then click **OK**.

    If you choose to **Use Trusted Connection** (i.e., Windows NT authentication), Login ID and Password are not necessary.
17. In the Email Security Log Server Configuration utility, click **Apply** and then **OK** to the warning message about stopping and restarting Log Server.
18. On the **Connection** tab, under **Service Status**, click **Stop**.

    This stops Email Security Log Server.
19. Click the same button (it now is labeled **Start**).

    This starts Email Security Log Server. It is now configured to use the new Email Security database location.
20. Click **OK** to close the Email Security Log Server Configuration utility.

Re-registering Email Security Gateway with Data Security

Topic 50617 | Management Server Location Change | Email Security Solutions | Version 7.8.x

If the IP address of the TRITON management server has changed, you must re-register Email Security Gateway with Data Security Management Server. Use the following steps:

1. In the Email Security manager, navigate to **Settings** > **General** > **Data Security** and click **Unregister**.
2. In the Data Security manager, navigate to S**ettings** > **Deployment** > **System Modules**.
3. Click the Email Security Gateway entry.
4. Click **Delete** at the top of the **System Modules** > **Email Security Gateway** page to remove Email Security Gateway registration.
5. When prompted, click **Deploy** to apply the changed Data Security setting.
6. In the Email Security manager, navigate to **Settings** > **General** > **Data Security**.
7. Register the Email Security appliance with Data Security.
8. Return to the Data Security module and click **Deploy** in the upper right area of the screen.

Migrating the Web Security manager off of a Websense appliance

Topic 50625 | Management Server Location Change | Web Security Solutions | v7.7.x, 7.8.x

In version 7.8, the Web Security manager cannot reside on an appliance. Before upgrading, disable the v7.7 on-appliance TRITON console and create a Windows-based TRITON management server.

Use the following instructions to complete the process:

- *Step 1: Disable the on-appliance TRITON console*, page 14
- *Step 2: Create a new TRITON management server*, page 15
- *Step 3: Restore your TRITON console backup*, page 18

Step 1: Disable the on-appliance TRITON console

When you disable the TRITON console on the appliance, you are prompted to back up your existing configuration. You can then use the backup file to restore your configuration to the new management server machine.

1. Log on to the Appliance manager:

```
https://<C_interface>: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.

Step 2: Create a new TRITON management server

Getting started

Install TRITON management components on a Windows Server 2008 R2 machine that meets or exceeds the v7.8 system requirements. (Note that while v7.8.x components can also run on Windows Server 2012, v7.7 components cannot.)

1. Download the TRITON Unified Installer (**WebsenseTRITON77*x*Setup.exe**) from mywebsense.com.
2. Right-click **WebsenseTRITON77*x*Setup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
3. On the Welcome screen, click **Start**.
4. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
5. On the Installation Type screen, select **TRITON Unified Security Center**, then mark the **Web Security** check box and click **Next**.
6. On the **Summary** screen, click **Next** to continue the installation.

   TRITON Infrastructure Setup launches.

Install TRITON infrastructure components

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

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**.

- To accept the default location (recommended), simply click **Next**.
- To specify a different location, click **Browse**.

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

3. On the SQL Server screen, select **Use existing SQL Server on another machine**, then specify the location and connection credentials for a database server located elsewhere in the network.

   a. Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any, and the **Port** to use for SQL Server communication.

   If you are using a named instance, the instance must already exist.

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

   b. Specify whether to use **SQL Server Authentication** (a SQL Server account) or **Windows Authentication** (a Windows trusted connection), then provide the **User Name** or **Account** and its **Password**.

   If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web Security manager. See Configuring Websense Apache services to use a trusted connection.

   c. Click **Next**.

   The installer verifies the connection to the database engine. If the connection test is successful, the next installer screen appears.

   If the test is unsuccessful, click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

4. On the Server & Credentials screen:

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

     Administrators will use this address to access the TRITON console (via a web browser), and Websense component on other machines will use it to connect to the TRITON management server.

   - Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Unified Security Center. The 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).

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.

8. The Installation screen appears, showing installation progress. Wait until all files have been installed.

   If an **Error 1920** message appears, check to see if port 9443 is already in use on this machine.

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

9. 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 Web Security management components

1. On the Select Components screen, select:
   - TRITON - Web Security (selected by default)
   - Real-Time Manager

2. When prompted, supply the **IP address** and **port** used by Policy Broker (on the full policy source appliance or Policy Broker machine) in your deployment.

3. If the management server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components. Follow the on-screen prompts to complete this process.
4. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.
5. A progress screen is displayed. Wait for installation to complete.
6. On the Installation Complete screen, click **Next**.

This completes the management server installation process.

Step 3: Restore your TRITON console backup

1. Copy the **EIP_bak.tgz** file created when you disabled your on-appliance Web Security manager to the new TRITON management server machine.
2. Use a utility like 7-Zip to extract and unpack the contents of the appliance TRITON backup file to a temporary directory.

   When the process is complete, you should have a directory called **EIP_bak** that contains, among other files, **EIP.db** and **httpd-data.txt**, as well as **apache** and **tomcat** folders.
3. Open the Windows Services tool on the TRITON management server.
4. Right-click the following service and select **Stop**:
   - Websense TRITON Unified Security Center
   - Websense TRITON Web Server
   - Websense TRITON - Web Security
5. Open the Windows Control Panel and select **Programs > Programs and Features**, then select **Websense TRITON Infrastructure**.
6. Click **Uninstall/Change**.
7. When asked if you want to modify, repair, or remove the TRITON Infrastructure, select **Modify**, then click **Next** until you get to the **Restore Data from Backup** screen.
8. Mark the **Use backup data** box and click the **Browse** button to locate the backup folder, then click **Next** until you begin the restore process.

> ✓ **Note**
>
> If you receive a pop-up message stating that the selected backup file “is from the same release but from a different build,” click **Yes** to continue the restore process.
>
> The restore process will proceed normally.

9. Click **Finish** to complete the restore wizard.

10. Go back to the Services window and click Refresh. If the **Websense TRITON Unified Security Center** service (or any other service that you stopped manually) has not restarted, right-click it and select **Start**.

    Once the restore process is complete, a file named DataRestore.log is created in the date-stamped backup folder that was used for the restore.

Migrating the Data Security manager from server A to server B

Topic 50622 | Management Server Location Change | Data Security Solutions | Version 7.8.x

Complete these instructions to migrate the Data Security manager from one server to another.

Back up Data Security

1. Navigate to the Backup page in the Data Security manager (**Settings** > **System** > **Backup).**
2. Fill all required fields on the page, then click **OK** to save your changes.

   These fields will be used at the backup process. (Make sure you include the forensics.)
3. Use the Windows Task Scheduler tool to **Enable DSS Backup** task.
4. After the task is enabled, right-click it and run it.

   Once the DSS Backup task is finished, you can see the backup contents in the directory you chose on the Backup page in the Data Security manager.

Keep the backup folder in a convenient location. The folder will be used to restore your settings once you have finished installing Data Security.

For more detailed backup instructions, see the Backup and Restore FAQ in the Websense Technical Library.

Restore Data Security settings on the new machine

1. Copy the contents of the DSS backup folder from the old Windows Server 2008 R2 machine to a temporary directory on the new Data Security Windows Server 2012 machine.

   When the process is complete, you should have a directory that contains an MngDB folder and a subscription.xml file, as well as policies_backup and certs folders.

2. Open the Windows Control Panel and select **Programs and Features**. (Depending on your setup, you may first need to select Programs to see the Programs and Features option).
3. Select **Websense Data Security**, and then click **Uninstall/Change**.
4. When prompted, select **Modify**, then click **Next** until you reach the “Restore Data from Backup” screen.
5. Mark the **Use backup data** box and browse to the backup folder location. Click **Next** until the restore process begins.

For more detailed restore instructions, see the Backup and Restore FAQ in the Websense Technical Library.

Register management components with the new server

The new server has a new IP address and host name. You must separately re-register every TRITON management component installed on the new server with the new server address.

Re-registering Data Security components

Topic 50623 | Management Server Location Change | Data Security Solutions | Version 7.8.x

You must re-register all Data Security servers, agents, and protectors when you change the IP address or hostname of the TRITON management server.

Before you start, make sure you know the user name and password of a Data Security administrator who has an access role with System Modules privileges.

Re-register Data Security servers and agents

Go to each Data Security server and machine with a Data Security agent installed and do the following:

1. Launch the Websense installer.
2. In the installer, for Data Security, select the **Modify** link.
3. Accept the defaults in the installer screens and click **Next**, until you reach the **Register with the Data Security Server** screen.
4. In the **Register with the Data Security Server** screen, enter the new IP address of the TRITON management server along with the user name and password of a TRITON administrator.

When the installers finish:

1. Log onto the Data Security manager and go to **Settings** > **Deployment** > **System Modules**.

2. Verify that the components appears in the tree view.
3. Click **Deploy**.

Re-register Protector

1. Log onto each protector as root.
2. Run **wizard securecomm**.
3. Enter the Data Security Management Server's IP address along with the user name and password of a Data Security administrator with System Modules privileges.
4. Log onto the Data Security manager and go to **Settings > Deployment > System Modules**.
5. Verify that the protector appears in the tree view.
6. Click **Deploy**.

Re-register Websense Content Gateway

To enable data loss prevention over Web channels, you must connect the Content Gateway module of your Web security solution to the Data Security Management Server. Follow these steps to establish that connection:

1. Ensure that Content Gateway and Data Security Management Server systems are running and accessible, and that their system clocks are approximately synchronized.
2. Ensure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Hostname alone is not sufficient.
3. If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface ("C" on a V-Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
4. Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). Data Security Management Server uses the eth0 NIC during the registration process.

   After registration, the IP address can move to another network interface on the same machine; however, that IP address is used for configuration deployment and must be available as long as the 2 modules are registered.
5. From the Content Gateway Manager, select **Configure > Basic > General**.
6. Make sure Data Security is turned on (the **On** radio button and **Integrated on-box** must be selected). Now click the Not Registered link. This opens the **Configure > Security > Data Security** registration screen.
7. Enter the IP address of the Data Security Management Server.

8. Enter a user name and password for a Data Security administrator with Manage System Modules privileges.
9. Click **Register**. You are reminded to synchronize the system time between the proxy machine and the Data Security Management Server.
10. If registration succeeds, a Data Security Configuration page displays. Set the following configuration options:
    a. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.
    b. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement.

    These options can be accessed whenever Data Security is registered by going to the **Configure** > **Security** > **Data Security** > **General** page.
11. Click **Apply**.
12. Restart Content Gateway.
13. Deploy the Content Gateway module by clicking **Deploy** in the Data Security manager.

Troubleshooting the connection between Content Gateway and Data Security

If you cannot register Websense Content Gateway with the Data Security Management Server (you receive an error in Content Gateway Manager) be sure that you can ping the Data Security Management Server from the proxy machine. (Go to the Linux command line and ping the IP address of the Data Security Management Server.)

If the ping fails, make sure that you have the correct IP address for the Data Security Management Server by going to that machine and running **ipconfig** from the command line.

If the proxy is on a V-Series appliance, try pinging the IPv4 address of the appliance's C interface from the Data Security Management Server.

If the proxy is not on a Websense appliance, try pinging the IPv4 address of the Content Gateway host system eth0 network interface from the Data Security Management Server. The registration process requires that Content Gateway is reachable on eth0. After registration, the IP address may move to another network interface on the system, but that IP address must remain available while the 2 modules are being registered.

If Content Gateway is deployed as a transparent proxy and the communication interface (“C” on a V-Series appliance) is subject to transparent routing, the registration process was likely intercepted by the transparent routing and prevented from completing. Ensure that traffic to and from the communication interface is not subject to transparent routing.

If registration still fails, make sure that neither the proxy machine nor the Data Security Management Server has a machine name with a hyphen in it. This has been known to cause registration problems.

And make sure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Hostname alone is not sufficient to register the proxy with the Data Security Management Server.

Creating Apache SSL Certificates

Topic 50624 | Creating Certificates | Web Security Solutions | Version 7.8.x

Perform the following steps on the TRITON management server to create (or re-create) Apache SSL certificates for the Web Security management components.

Note that these are basic instructions for creating certificates. Changing the password on certificates is not included in these steps. Avoid changing passwords if possible.

1. Use the Windows Services tool to stop the following services:
   - Websense TRITON - Web Security
   - Websense Web Reporting Tools
2. Review the **Websense\Web Security\apache\conf\ssl\openssl.txt** file to verify that it contains correct information.

   If you have changed the IP address of this machine, for example, edit the IP address in the openssl.txt file to match.

> **Note**
>
> You can create a batch file to automate the tasks in Step 3-Step 8. See *Using a batch file for Apache SSL certificate file operations*. If you choose to create a batch file, execute it and then skip to Step 8.

3. Go to the **Websense\Web Security\apache\conf\ssl\automation\** directory and run the following scripts in the order shown:
   a. s1_newreq.bat
   b. s2_server_key.bat
   c. s3_server_crt.bat
   d. s4_server_p12.bat
4. Copy the **Websense\Web Security\apache\conf\ssl\output\server.key** file to:

   `Websense\Web Security\apache\conf\ssl\ssl.key\server.key`
5. Copy the **Websense\Web Security\apache\conf\ssl\output\server.crt** file to:

   `Websense\Web Security\apache\conf\ssl\ssl.crt\server.crt`
6. Copy the **Websense\Web Security\apache\conf\ssl\output\cakey.pem** file to:

   `Websense\Web Security\apache\conf\ssl\private\cakey.pem`
7. Copy the **\Web Security\apache\conf\ssl\output\manager.p12** file to:

```
Websense\Web Security\tomcat\conf\keystore\tomcat\manager
.p12
```

8. Use the Windows Services tool to start the following services:
   - Websense TRITON - Web Security
   - Websense Web Reporting Tools

> ✓ **Note**
>
> For more information about Apache SSL go to http://www.apache-ssl.org/#FAQ.

Using a batch file for Apache SSL certificate file operations

When creating Apache SSL certificates, there are several batch files to execute and files to copy. You can automate the process by creating and running a batch file.

The following is an example batch file you can use to create your own:

```
@echo off
set HOME=<installation_path>\Web Security
set WORKING_DIR=%HOME%\apache\conf\ssl\automation
call "%WORKING_DIR%\s1_newreq.bat"
call "%WORKING_DIR%\s2_server_key.bat"
call "%WORKING_DIR%\s3_server_crt.bat"
call "%WORKING_DIR%\s4_server_p12.bat"

@echo on
copy "%HOME%\apache\conf\ssl\output\server.key"
"%HOME%\apache\conf\ssl\ssl.key\server.key"
copy "%HOME%\apache\conf\ssl\output\server.crt"
"%HOME%\apache\conf\ssl\ssl.crt\server.cr"
copy "%HOME%\apache\conf\ssl\output\cakey.pem"
"%HOME%\apache\conf\ssl\private\cakey.pem"
copy "%HOME%\apache\conf\ssl\output\manager.p12"
"%HOME%\tomcat\conf\keystore\tomcat\manager.p12"
```