Changing the TRITON management server IP address or name

Topic 51300 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

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

Note

In v8.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 or Data module of the TRITON Manager to a new machine. See:

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

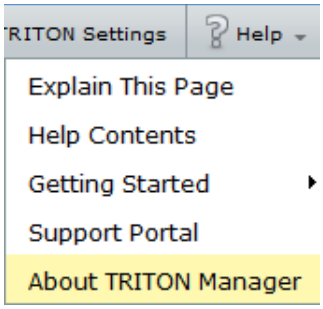
- For TRITON infrastructure:
  - TRITON Manager
  - Websense TRITON Web Server
  - Websense TRITON Settings Database
- For web protection solutions:
  - Websense Control Service
  - Websense TRITON - Web Security
  - Websense Web Reporting Tools
  - Websense RTM Client
  - Websense RTM Database
  - Websense 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 TRITON AP-DATA:
  - Websense TRITON 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 TRITON AP-EMAIL:
  - Websense TRITON - Email Security
  - (not recommended) Websense Email Log Server

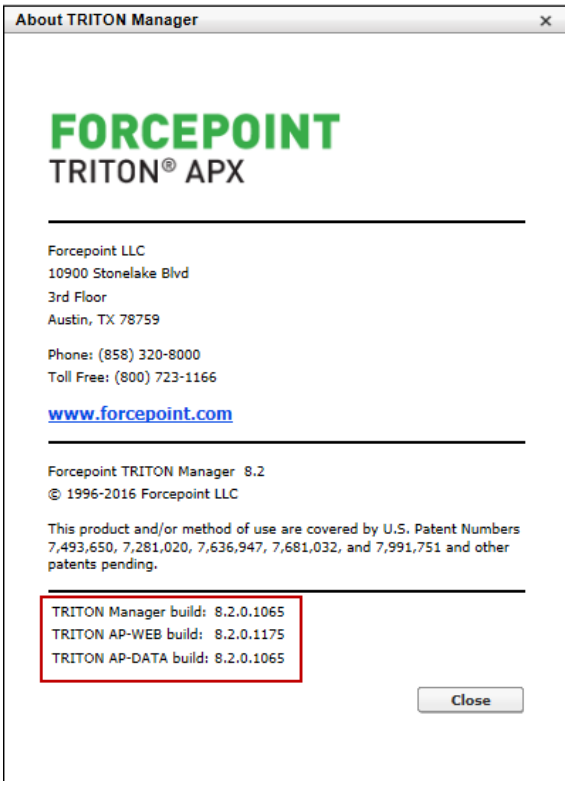
Each module of the TRITON Manager must be configured separately. Depending on your subscription, you may not have all modules enabled.

To determine which TRITON Manager modules are active in your deployment:

1. In TRITON Manager, go to **Help** > **About TRITON Manager**.



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



Changing the IP address of the TRITON management server

Topic 51301 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

> **Warning**
> If web protection policy (Policy Broker, Policy Server, Policy Database) or hybrid (Directory Agent, Sync Service) components reside on the 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 the web protection 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 8, 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 protection solutions only*): Update the configuration of the Web module to reflect the new IP address:

   a. Recreate Apache SSL certificates for the Web module of the TRITON Manager. See *Creating Apache SSL Certificates*, page 24. 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 module **catalina.properties file** to reflect the new IP address. See *Configuring Tomcat to a use new local IP address*, page 9.

   c. Navigate to the **C:\Program Files (x86)\Websense\Web Security\bin** directory 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 the web protection Log Server component 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 module of the TRITON Manager and navigate to the **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 protection solutions only*): Edit the Email module **catalina.properties** file to reflect the new IP address. See *Configuring Tomcat to a use new local IP address*, page 9.

4. (*Email protection solutions only*): If the email protection Log Server component is installed on the TRITON management server machine, update TRITON Manager with its new IP address. See *Configuring a new hostname for web protection management components*, page 10.

Note

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

If you have multiple TRITON AP-EMAIL appliances in your deployment, update them as well with the new IP address of email protection Log Server component. To update other appliances, complete the steps again in *Configuring a new hostname for web protection management components*, page 10, with the following modifications:

a. After logging into TRITON Manager, click **Appliances** in the TRITON 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 TRITON AP-EMAIL appliance that uses the Log Server located on the TRITON management server machine.

5. (*Email protection solutions only*): If the email protection 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 Manager. See *Updating the Log Database location for TRITON AP-EMAIL*, page 16.

6. *(TRITON AP-DATA only)*: Modify the TRITON management server installation to reflect the change. See *Changing the IP address for TRITON AP-DATA management components*, page 11.

7. If your subscription includes the Web DLP module for TRITON AP-WEB or includes TRITON AP-EMAIL, re-register the Web or Email module with the Data module of the TRITON Manager. This is required for Web DLP and Email DLP (data loss prevention) features.

   For TRITON AP-WEB, see *Re-register Content Gateway*, page 22.

   For TRITON AP-EMAIL, see *Re-registering TRITON AP-EMAIL with data protection components*, page 18.

Changing the hostname of the TRITON management server

Topic 51302 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

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 8 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 protection solutions*): Edit the configuration for the web protection management components to reflect the new hostname. See *Configuring a new hostname for web protection management components*, page 10.
4. *(TRITON AP-DATA only)*: Modify the TRITON management server installation to reflect the change.

Configuring TRITON Infrastructure to use a new IP address or hostname

Topic 51303 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

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 TRITON 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 51304 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

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 and Email modules of the TRITON Manager.

Note

Tomcat configuration for TRITON Infrastructure and the Data module of the TRITON 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 8.

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 protection solutions:

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

     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 protection solutions:

     java-fw.ip
   - Email protection solutions:

     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 web protection management components

Topic 51305 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

If the hostname of the TRITON management server has changed, also update configuration for the components that support the Web module of the TRITON Manager.

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 for TRITON AP-DATA management components

Topic 51306 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

Perform this task during off hours, or route traffic around the TRITON AP-DATA 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 4.

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 TRITON 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, 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 TRITON management server (SMTP agent), change its configuration to relay mail to the new TRITON management server IP address.
8. In the Data module of TRITON 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 TRITON AP-DATA stand-alone agents, such as: ISA agent, Exchange agent, and printer agent (See *Re-registering TRITON AP-DATA components*, page 21).
10. Start the protector:
    a. Log onto the protector as **root**.
    b. Execute **service pama start**.
11. Click **Deploy** in the Data module of TRITON Manager.
12. Since the 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 for TRITON AP-DATA management components

Topic 51307 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

Perform this task during off hours, or route traffic around the TRITON AP-DATA 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 7.

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 TRITON 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, 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 module of TRITON 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 module of TRITON 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 the email protection Log Server

Topic 51308 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

If the IP address of the machine running Log Server for TRITON AP-EMAIL is changed, you must update the Email module of TRITON Manager to use the new address.

1. Log on to the Email module of TRITON 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 TRITON AP-EMAIL

Topic 51309 | Web, Data, and Email Solutions |v8.2.x | Updated 18-Apr-2016

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

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

1. Log on to the Email module of TRITON Manager.
2. Go to **Settings > Reporting > Log Database** and enter the new IP address in the **Log database** field.

   If the Email Log 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 TRITON Manager at this screen.You will come back to it later to complete this procedure.
4. On the machine running Email Log Server, start the Log Server Configuration utility (**Start > All Programs > Websense > Email 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 Log 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 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 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 Log Server.
19. Click the same button (it now is labeled **Start**).

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

Re-registering TRITON AP-EMAIL with data protection components

Topic 51310 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

If the IP address of the TRITON management server has changed, you must re-register TRITON AP-EMAIL with data protection components. Use the following steps:

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

Migrating the Data module of the TRITON Manager from server A to server B

Topic 51311 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

Complete these instructions to migrate the Data module of TRITON Manager from one server to another.

Back up TRITON AP-DATA

1. Navigate to the Backup page in the Data module of TRITON 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 module of TRITON Manager.

Keep the backup folder in a convenient location. The folder will be used to restore your settings once you have finished installing TRITON AP-DATA.

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

Restore TRITON AP-DATA 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 TRITON AP-DATA 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 TRITON AP-DATA**, 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 Forcepoint Technical Library.

Register management components with the new server

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

Re-registering TRITON AP-DATA components

Topic 51312 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

You must re-register all TRITON AP-DATA 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 TRITON AP-DATA administrator who has an access role with System Modules privileges.

Re-register TRITON AP-DATA servers and agents

Go to each server and machine with a TRITON AP-DATA agent installed and do the following:

1. Launch the TRITON installer.
2. In the installer, for Data, 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 TRITON AP-DATA 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 module of TRITON Manager and go to **Settings > Deployment > System Modules**.
2. Verify that the components appear in the tree view.
3. Click **Deploy**.

Re-register Protector

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

Re-register Content Gateway

To enable the Web DLP module of TRITON AP-WEB, you must connect Content Gateway to the TRITON management server for TRITON AP-DATA. Follow these steps to establish that connection:

1. Ensure that Content Gateway and TRITON 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). TRITON 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 TRITON AP-DATA 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 > TRITON AP-DATA** registration screen.
7. Enter the IP address of the TRITON management server.
8. Enter a user name and password for a TRITON AP-DATA administrator with Manage System Modules privileges.
9. Click **Register**. You are reminded to synchronize the system time between the proxy machine and the TRITON management server.
10. If registration succeeds, a TRITON AP-DATA Configuration page displays. Set the following configuration options:
    a. **Analyze FTP Uploads**: Enable this option to send FTP uploads to TRITON AP-DATA for analysis and policy enforcement.
    b. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to TRITON AP-DATA for analysis and policy enforcement.

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

Troubleshooting the connection between Content Gateway and TRITON AP-DATA

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

If the ping fails, make sure that you have the correct IP address for the TRITON 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 TRITON management server.

If the proxy is not on an appliance, try pinging the IPv4 address of the Content Gateway host system eth0 network interface from the TRITON 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 TRITON 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 TRITON management server.

Creating Apache SSL Certificates

Topic 51313 | Web, Data, and Email Solutions | v8.2.x | Updated 18-Apr-2016

Perform the following steps on the TRITON management server to create (or re-create) Apache SSL certificates for the web protection 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"
```