Forcepoint

Data, Email, and Web Security

v8.5.x

Moving the Management Server

Revision A

Contents

Changing the Management Server IP Address or Name

Note

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

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

Note

Management server domains cannot be modified. This would require changing the local administrator user name, which the installer does not allow.

These articles also describe how to move the Web Security or Data Security module of the Forcepoint Security Manager to a new machine.

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

- For the infrastructure portion of the Forcepoint Security Manager:
  - Websense TRITON Infrastructure
  - Websense TRITON Web Server
  - Websense TRITON Settings Database
- For Forcepoint Web Security and Forcepoint URL Filtering:
  - 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 Forcepoint DLP:
  - 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 Forcepoint Email Security:
  - Email Security module
  - (not recommended) Email Log Server

Procedure to determine the Forcepoint Security Manager modules

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

To determine which Forcepoint Security Manager modules are active in your deployment:

Steps

1) In the Forcepoint Security Manager, go to **Help** > **About Security Manager**.

2) The About pop-up window lists the modules that are active.

Changing the IP address of the Forcepoint management server

Before you begin

Note

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

Warning

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

Before changing the IP address of the Forcepoint management server, remove the web protection Log Server from the management server machine (if applicable). 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 management server.

Steps

1) Update the Forcepoint Management Infrastructure with the new IP address.

   See *Configuring the infrastructure to use a new IP address or hostname*, for instructions.

   If SQL Server Express is installed on this machine, it will be automatically configured to the new IP address along with the infrastructure components.

2) (*Web protection solutions only*): Update the configuration of the Web Security management components to reflect the new IP address:

   a) Recreate the Web Security Apache SSL certificates. See *Creating Apache SSL Certificates*. When following these instructions, be sure to edit the **openssl.txt** file to reflect the new IP address of the 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*.

   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 the web protection Log Server runs on the management server (not recommended), and it was removed as instructed before changing the IP address, 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 on to the Web Security module of the Forcepoint Security Manager and navigate to the **Settings** > **Reporting** > **Log Server** page.

   f) Verify that correct information appears in the **SQL Server location** field.
   If the SQL Server location value changes, 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 Forcepoint Email Security **catalina.properties** file to reflect the new IP address. See *Configuring Tomcat to a use new local IP address*.

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

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

If there are multiple Forcepoint Email Security appliances in the deployment, update each with the new IP address of the Email Log Server. To update other appliances, complete the steps again in *Configuring a new hostname for web protection management components*, with the following modifications:

a) After logging into the Security Manager, click the **Appliances** icon in the Security Manager banner.

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

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

d) Repeat this process for each Forcepoint Email Security appliance that uses the Log Server located on the management server machine.

5) (*Email protection solutions only*): If the email protection Log Database is located on the management server (e.g., SQL Server Express is installed on the machine and maintains the Log Database), update the database location in the Security Manager. See *Updating the Log Database location for Forcepoint Email Security*.

6) (*Forcepoint DLP only)*: Modify the management server installation to reflect the change. See *Changing the IP address for Forcepoint DLP management components*.

7) For deployments that include the Forcepoint Web Security DLP Module, or that include Forcepoint Email Security, re-register the Web Security or Email Security module with the Data Security module of the Security Manager.

- For Forcepoint Web Security, see *Re-register Forcepoint DLP Protector software package*.
- For Forcepoint Email Security, see *Re-registering Forcepoint Email Security with DLP components*.

Related tasks

Configuring the infrastructure to use a new IP address or hostname on page 8
Creating Apache SSL Certificates on page 25
Configuring Tomcat to a use new local IP address on page 10
Configuring a new hostname for web protection management components on page 11
Updating the Log Database location for Forcepoint Email Security on page 17
Changing the IP address for Forcepoint DLP management components on page 12
Re-register Forcepoint DLP Protector software package on page 22
Re-registering Forcepoint Email Security with DLP components on page 19

Changing the hostname of the Forcepoint management server

Before you begin

Note

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

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

Steps

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.

Steps to follow after changing the management server hostname

After changing the management server hostname (in Windows) and rebooting the machine:

Steps

1) Update the Forcepoint Management Infrastructure with the new hostname.

   See *Configuring the infrastructure to use a new IP address or hostname* for instructions.

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

   http://msdn.microsoft.com/en- us/library/ms143799.aspx

2) (*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*.

3) (*Forcepoint DLP only)*: Modify the management server installation to reflect the change.

Related tasks

Configuring the infrastructure to use a new IP address or hostname on page 8

Configuring a new hostname for web protection management components on page 11

Configuring the infrastructure to use a new IP address or hostname

Before you begin

Note

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

If the IP address or hostname of the Forcepoint management server changes, update the Forcepoint management infrastructure configuration to reflect the change.

Steps

1) Launch the Forcepoint Security Installer.

   - If installer files were preserved after the initial installation, use the **Forcepoint Security Setup** link in the **Start** > **Forcepoint** menu or on the Start screen to launch the installer.
   - If installer files were not preserved, double-click the installer executable.

2) In the installer, click the **Modify** link next to Forcepoint Management Infrastructure.

3) Accept the defaults in the installer screens and click **Next**, until you reach the **Server & Credentials** screen. On that screen:

   - If the management server IP address changed, select the new address from the **IP address** drop-down list.
   - If the management server hostname changed, 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

Before you begin

Note

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

If the IP address of the Forcepoint management server has changed, use the following steps to update the Tomcat configuration for the Web Security and Email Security modules of the Forcepoint Security Manager.

Note

Tomcat configuration for the management infrastructure and the Data Security module of the Security Manager is done automatically when configuring to new IP address or hostname. See *Configuring the infrastructure to use a new IP address or hostname*.

Warning

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

Steps

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

Related tasks
Configuring the infrastructure to use a new IP address or hostname on page 8

Configuring a new hostname for web protection management components

Before you begin

Note

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

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

Steps

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 Forcepoint DLP management components

Before you begin

Note

Applies to:

- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x

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

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

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.

Steps

1) To stop the protector:

   a) Log on to the protector as **root**.

   b) Enter the following command:

   ```
   service pama stop
   ```

2) On the management server, launch the Forcepoint Security Installer.

- If installer files were preserved after the initial installation, use the **Forcepoint Security Setup** link in the **Start** > **Forcepoint** menu or on the Start screen to launch the installer.
- If installer files were not preserved, double-click the installer executable.

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 the hostname of the management server has changed, the installer automatically detects the new settings and configures the management infrastructure.

6) Proceed through the remaining installer screens, accepting defaults, and click **Finish**.

7) If mail server is relaying SMTP traffic to the management server (SMTP agent), change its configuration to relay mail to the new management server IP address.

8) In the Data Security module of the Security Manager, change the IP address on the following pages, if necessary:

   a) **Settings** > **Configuration** > **Archive Storage**

   b) **Settings** > **Deployment** > **System Modules**
   Select the **SMTP Agent** and click the **Encryption & Bypass** tab.

9) Re-register all Forcepoint DLP standalone agents (see *Re-registering Forcepoint DLP components*).

10) To start the protector:

   a) Log on to the protector as **root**.

   b) Enter the following command:

```
service pama start
```

11) Click **Deploy** in the Data Security module of the Security Manager.

12) Reinstall all endpoint clients with the new management server 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.
- New incidents are written into the data usage incident management screen.

Related concepts
Re-registering Forcepoint DLP components on page 21

Related tasks

Changing the IP address of the Forcepoint management server on page 4

Changing the hostname for Forcepoint DLP management components

Before you begin

Note

Applies to:

- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x

Perform this task during off hours, or route traffic around the Forcepoint DLP infrastructure (disabling connectors, ICAP, etc.) while the task is being performed.

It is assumed that the hostname of the management server has already been changed, if not see *Changing the hostname of the Forcepoint management server*.

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).

Steps

1) To stop the protector:

   a) Log on to the protector as **root**.

   b) Enter the following command:

   ```
   service pama stop
   ```

2) On the management server, launch the Forcepoint Security Installer.

   - If installer files were preserved after the initial installation, use the **Forcepoint Security Setup** link in the **Start** > **Forcepoint** menu or on the Start screen to launch the installer.
   - If installer files were not preserved, double-click the installer executable.

3) In the installer, select the **Modify** link for Forcepoint DLP.

4) Click **Next** in the installation wizard until the “Local Administrator” screen is displayed.

5) Select the new server name and the correct user name (in the form “NEWNAME\ UserName”).

6) To start the protector:

   a) Log on to the protector as **root**.

   b) Enter the following command:

   ```
   service pama start
   ```

7) Click **Next** to finish the modification.

8) (*Optional*) In the Data Security module of the Security Manager, change the server name in the following places:

   a) Go to the **Settings** > **System Modules** page.

   b) Click the **Forcepoint DLP 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**.

   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.

Related tasks

Changing the hostname of the Forcepoint management server on page 7

Updating the IP address for the email protection Log Server

Before you begin

Note

Applies to:

- Forcepoint Email Security, v8.5.x

If the IP address of the machine running Log Server for Forcepoint Email Security is changed, update the Email Security module of the Forcepoint Security Manager to use the new address.

Steps

1) Log on to the Security Manager.

2) Go to the **Email** > **Settings** > **Reporting** > **Log Server** page.

3) Enter the new IP address in the **Log Server** field.

4) Click **OK**.

Updating the Log Database location for Forcepoint Email Security

Before you begin

Note

Applies to:

- Forcepoint Email Security, v8.5.x

If the IP address of the Email Log Database machine (the IP address of the SQL Server machine) has changed, update the Forcepoint Security 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 the Forcepoint Security Manager or Email Log Server.

Steps

1) Log on to the Forcepoint Security Manager.

2) Go to the **Email** > **Settings** > **Reporting** > **Log Database** page.

3) Enter the new IP address in the **Log database** field.

   If the Email Log Database is located on the management server itself and you are performing this procedure because you changed the IP address of the management server, enter its new IP address here.

4) Click **OK** (in the Log Database Location area of the screen).

   Leave the Security Manager at this screen.You will come back to it later to complete this procedure.

5) On the machine running Email Log Server, start the Log Server Configuration utility (**Start** > **All Programs** > **Websense** > **Email Log Server Configuration**).

6) In the **Database** tab, click **Connection** to open the **Select Data Source** dialog box.

7) 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.

8) Select **System Data Source (Applies to this machine only)** and then click **Next**.

9) In the list of drivers, select **SQL Server** and then click **Next**.

10) In the next dialog box, click **Finish**.

11) 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 management server and you are performing this procedure because you have changed the management server's IP address, enter its new IP address here.

12) 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) If SQL Server authentication was selected in step a, enter the **Login ID** and **Password** of the **sa** account.

    d) Click **Next**.

13) In the next dialog box, enable **Change the default database to** and then select **esglogdb7*x*** from the drop-down menu. Then click **Next**.

14) In the next dialog box, accept the default settings and click **Finish**.

15) Click **Test Data Source** to test the connection. Upon test success, click **OK**.

16) Click **OK**, then click **OK** once more.

17) 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.

18) In the Email Log Server Configuration utility, click **Apply** and then **OK** to the warning message about stopping and restarting Log Server.

19) On the **Connection** tab, under **Service Status**, click **Stop**. This stops Email Log Server.

20) 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.

21) Click **OK** to close the Email Log Server Configuration utility.

Re-registering Forcepoint Email Security with DLP components

Before you begin

Note

Applies to:

- Forcepoint Email Security, v8.5.x

If the IP address of the Forcepoint management server has changed, re-register Forcepoint Email Security with Forcepoint DLP components. Use the following steps:

Steps

1) In Forcepoint Security Manager, access the Email Security module and select the appliance to be re-registered.

2) Navigate to the page **Settings** > **General** > **Data Loss Prevention** and click **Unregister**.

3) In the Email Security module, navigate to the page **Settings** > **General** > **Data Loss Prevention** and click **Register**.

4) Ensure that the appliance management (C) interface IP address appears in the field **Communication IP address**.

5) In the Data Security module, navigate to the page **Settings** > **Deployment** > **System Modules** and verify that the Email Security appliance appears in the tree view.

6) In the upper right corner, click **Deploy**.

Migrating Forcepoint DLP management components between servers

Note

Applies to:

- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x

Complete these instructions to migrate Forcepoint DLP management components from one server to another.

Back up Forcepoint DLP

Steps

1) Navigate to the Backup page in the Data Security module of the Security Manager (**Settings** > **System** > **Backup**).

2) Fill all required fields on the page, then click **OK**.

   These fields will be used at the backup process. (Be sure to 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, the backup contents appear in the directory selected on the Backup page in the Security Manager.

Next steps

Keep the backup folder in a convenient location. The folder will be used to restore settings once Forcepoint DLP components have been installed on the new machine.

For more detailed backup instructions, see the Backup and Restore FAQ at the Forcepoint Documentation site.

Restore Forcepoint DLP settings on the new machine

Once Forcepoint DLP management components have been installed on the new machine:

Steps

1) Copy the contents of the DSS backup folder from the old machine to a temporary directory on the new Forcepoint DLP machine.

   The directory should contain 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**.

3) Select **Forcepoint DLP**, and then click **Uninstall/Change**.

4) When prompted, select **Modify**, then click **Next** until the “Restore Data from Backup” screen is displayed.

5) Mark the **Use backup data** box and browse to the backup folder location. Click **Next** until the restore process begins.

Next steps

For more detailed restore instructions, see the Backup and Restore FAQ.

Register management components with the new server

The new server has a new IP address and hostname. Separately re-register every component installed on the new server with the new server address.

Re-registering Forcepoint DLP components

Note

Applies to:

- Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x, v8.8.x. v8.9.x

Re-register all Forcepoint DLP servers, agents, and protectors when the IP address or hostname of the Forcepoint management server changes.

Before starting the process, be sure to have the user name and password of a Forcepoint DLP administrator account with System Modules privileges.

Re-register Forcepoint DLP servers and agents

Go to each server and machine with a Forcepoint DLP agent installed and do the following:

Steps

1) Launch the Forcepoint Security Installer.

2) In the installer, select the **Modify** link next to Forcepoint DLP.

3) Accept the defaults in the installer screens and click **Next**, until the “Register with the Management Server” screen appears.

4) In the Register with the Management Server screen, enter the new IP address of the Forcepoint management server along with the user name and password of a Security Manager administrator with Forcepoint DLP System Modules permissions.

Next steps

When the installers finish:

1) Log on to the Data Security module of Security Manager and go to the **Settings** > **Deployment** > **System Modules** page.

2) Verify that the components appear in the tree view.

3) Click **Deploy**.

Re-register ISO/Appliance protector

To re-register protector appliances:

Steps

1) Log on to each protector as **root**.

2) Enter the following command:

```
wizard securecomm
```

3) Enter the management server IP address along with the user name and password of a Forcepoint DLP administrator with System Modules privileges.

4) Log onto the Data Security module of the Forcepoint Security Manager and go to the **Settings** > **Deployment** > **System Modules** page.

5) Verify that the protector appears in the tree view.

6) Click **Deploy**.

Re-register Forcepoint DLP Protector software package

To re-register Forcepoint DLP Protector software package:

Steps

1) Log on as **root**.

2) Enter the following command:

```
sudo -i wizard securecomm
```

3) Enter the management server IP address along with the user name and password of a Forcepoint DLP administrator with System Modules privileges.

4) Log onto the Data Security module of the Forcepoint Security Manager and go to the **Settings** > **Deployment** > **System Modules** page.

5) Verify that the protector appears in the tree view.

6) Click **Deploy**.

Re-register Content Gateway

To enable the Forcepoint Web Security DLP Module, connect Content Gateway to the Forcepoint DLP components on the management server:

Steps

1) Ensure that Content Gateway and 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 the network. Hostname alone is not sufficient.

3) If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the appliance management interface (C) 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 Forcepoint appliance). The 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) In the Content Gateway manager, go to the **Configure** > **Basic** > **General** tab.

6) Make sure that the Integration > Web DLP (integrated on-box) option is turned **On**, then click the **Not Registered** link.

   The **Configure** > **Security** > **Web DLP registration** screen opens.

7) Enter the IP address of the Forcepoint management server.

8) Enter the user name and password for a Forcepoint DLP administrator with Manage System Modules privileges.

9) Click **Register**. A reminder to synchronize the system time between the Content Gateway and management server machines is displayed.

10) If registration succeeds, a Forcepoint DLP Configuration page displays. Set the following configuration options:

    a) Enable the **Analyze FTP Uploads** option to send FTP uploads to Forcepoint DLP for analysis and policy enforcement.

    b) Enable the **Analyze Secure Content** option to send decrypted HTTPS posts to Forcepoint DLP for analysis and policy enforcement.

    These options can be accessed from the Configure > Security > Web DLP > General tab.

11) Click **Apply**, then restart Content Gateway.

12) Go to the Data Security module of the Security Manager and click **Deploy** to complete the registration process.

Troubleshooting the connection between Content Gateway and Forcepoint DLP

If Content Gateway cannot register with Forcepoint DLP components (an error appears in the Content Gateway manager), be sure that a ping from the proxy machine to the Forcepoint management server succeeds.

If the ping fails, use the ipconfig command on the management server machine to verify its IP address.

- If the proxy is on a Forcepoint appliance, try pinging the IPv4 address of the appliance's C interface from the 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 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 modules are being registered.

If Content Gateway is deployed as a transparent proxy and the communication interface ("C" on a Forcepoint 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 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 the network. Hostname alone is not sufficient to register the proxy with the management server.

Creating Apache SSL Certificates

Before you begin

Note

Applies to:

- Forcepoint Web Security, v8.5.x
- Forcepoint URL Filtering, v8.5.x

Perform the following steps on the Forcepoint 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.

Steps

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

   Note

   A batch file can be used to automate the tasks in Step 3- Step 8. See *Using a batch file for Apache SSL certificate file operations*. If using a batch file, run 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 this article more information about Apache SSL.

Related concepts

Using a batch file for Apache SSL certificate file operations on page 26

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. Optionally automate the process by creating and running a batch file.

Use the following sample set of batch commands as a template for the batch file. Replace <*installation_path*> with the actual installation directory used on the management server machine (C:\Program Files (x86)\Websense, by default).

```
@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"
```

Published 06 August 2024