Email Log Server Configuration Utility

Email Log Server is the component that receives log records and processes them into the Log Database.

During installation, you configure certain aspects of Log Server operation, including how Log Server interacts with Forcepoint Email Security. The Email Log Server Configuration utility lets you change these settings when needed, and configure other details about Log Server operation. This utility is installed on the same machine as Log Server.

To access the Email Log Server Configuration Utility:

1. From the Windows Start menu, select **Start > Forcepoint > Email Log Server Configuration**.

   The Email Log Server Configuration utility opens.
2. Select a tab to display its options and make any changes. For detailed instructions, see:
   - *Configuring Log Server connections*, page 2
   - *Configuring Log Server database options*, page 2
   - *Configuring log cache files*, page 6
3. Click **Apply** to save the changes.
4. Use the **Connection** tab to stop and restart Log Server for the changes to take effect.

Important

After making changes to any Log Server Configuration tab, click **Apply**. Then, you **must** stop and restart Log Server for the changes to take effect. To avoid restarting Log Server multiple times, make all Log Server configuration changes before restarting Log Server.

Configuring Log Server connections

Email Log Server Configuration Utility Help | Forcepoint Email Security | Version 8.4.x

The **Connection** tab of the Email Log Server Configuration utility contains options for creating and maintaining a connection between Log Server and Forcepoint Email Security.

1. Accept the default **Log Server input port** (50800) or enter another available port.

   This is the port over which the Log Server communicates with the email software. The port entered here must match the port entered on the **Settings > Reporting > Log Server** page in the email management server interface.
2. Click **Apply** to save any changes.
3. Use the button in the Service Status area to **Start** or **Stop** Log Server. The label of the button changes to reflect the action that will occur when you click it.

   Note

   No email traffic can be logged when Log Server is stopped.

   Changes made in the configuration utility do not take effect until you stop and restart Log Server. (See *Stopping and starting Log Server*, page 6.)

Configuring Log Server database options

Email Log Server Configuration Utility Help | Forcepoint Email Security | Version 8.4.x

Open the **Database** tab of the Email Log Server Configuration utility to configure how Log Server works with the Log Database.

1. Choose a **Log Insertion Method** from the following options.
   - Open Database Connectivity (ODBC): Inserts records into the database individually, using a database driver to manage data between Log Server and Log Database.
   - Bulk Copy Program (BCP) *(recommended)*: Inserts records into the Log Database in groups called batches. This option is recommended because it offers better efficiency than ODBC insertion.

     Note

     The BCP option is available only if you install the SQL Server Client Tools on the Log Server machine.

Important

If you plan to establish an encrypted database connection, you cannot use the BCP insertion method. Not using the batch method may affect Log Database performance. See *Setting up an encrypted database connection*, page 5, for information about encrypted connections.

2. Click the **Connection** button to select the Log Database for storing email traffic information from the email security software. See *Setting up the database connection*, page 4.

   ODBC Data Source Name (DSN) and **ODBC Login Name** display the settings established for the database connection.

3. If you chose BCP as the log insertion method in step 1, set the following options. If you chose ODBC as the log insertion method, skip this step.

Option	Description
BCP file path location	Directory path for storing BCP files. This must be a path where the Log Server service account has read and write access. This option is available only if Log Server is installed on the Log Database machine, or if the SQL Server Client Tools are installed on the Log Server machine.
BCP file creation rate	Maximum number of minutes Log Server spends placing records into a batch file before closing that batch file and creating a new one. This setting works in combination with the batch size setting: Log Server creates a new batch file as soon as either limit is reached.
BCP maximum batch size	Maximum number of log records before a new batch file is created. This setting works in combination with the creation rate setting: Log Server creates a new batch file as soon as either limit is reached.

   The BCP option for inserting records into the Log Database in batches cannot be used when you encrypt your database connection. See *Setting up an encrypted database connection*, page 5, for information.

4. Set the **Maximum connections allowed** to indicate how many internal connections can be made between Log Server and the database engine. The options available depend on the database engine being used.

   - **SQL Server Express**: Set to a number from 4 to 32, as appropriate for your SQL Server Express license.

- **SQL Server**: Set to a number from 4 to 50, as appropriate for your SQL Server license. The minimum number of connections depends on the selected log insertion method.

  Note

  Increasing the number of connections can increase processing speed for log records, but could impact other processes in the network that use the same SQL Server. In most cases, you should set the number of connections to fewer than 20. Contact your Database Administrator for assistance.

5. Check or uncheck **Enhanced logging** to enable or disable this option, which controls how Log Server resumes logging after it has been stopped.

   When this option is deselected (the default), Log Server begins processing at the beginning of the oldest log cache file after a stop. This could result in some duplicate entries in the Log Database, but speeds Log Server processing.

   When this option is checked, Log Server tracks its location in the active log cache file. After a restart, Log Server resumes processing where it stopped. Enhanced logging can slow Log Server processing.

6. Click **Apply** to save any changes, then stop and restart Log Server (see *Stopping and starting Log Server*, page 6).

Setting up the database connection

Email Log Server Configuration Utility Help | Forcepoint Email Security | Version 8.4.x

Click the **Connection** button on the Database tab of the Email Log Server Configuration utility to select the Log Database to use for storing incoming email traffic information. The Log Database connection is configured automatically during installation, but can be changed if you need to log to a different database. (The database must already exist to establish a connection.)

1. In the Select Data Source dialog box, select the **Machine Data Source** tab.
2. Select the Data Source Name corresponding to the database that you want to use for logging.
3. Click **OK**. The SQL Server Login dialog box is displayed.
4. If the **Use Trusted Connection** option is available, make sure it is set properly for your environment. Contact your Database Administrator for assistance.
5. Enter the **Login ID** and **Password** established when the database was created. Usually this is the same logon ID and password entered during Log Server installation and database creation.
6. Stop and restart Log Server via the **Connection** tab after making this and any other changes in the configuration utility. (See *Stopping and starting Log Server*, page 6.)

Setting up an encrypted database connection

Email Log Server Configuration Utility Help | Forcepoint Email Security | Version 8.4.x

You can choose to encrypt the database connection during email product installation. If you did not select this option at product installation, you can configure an encrypted connection in the Log Server Configuration utility.

By default, Email Log Server uses NTLMv2 to encrypt the connection.

Important

If you want to use SSL encryption, you must have imported a trusted certificate to the Log Server machine. See your database documentation for information about importing a trusted certificate.

The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.

The connection from the Email Security module on the Forcepoint Security Manager to an email appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature. See your Microsoft SQL Server documentation for details.

Click the **Connection** button on the Database tab of the Email Log Server Configuration utility to create a new data source. Use the following steps to establish an encrypted database connection:

1. In the Select Data Source dialog box, select the **Machine Data Source** tab.
2. Click **New** to open the Create New Data Source dialog box.
3. Select the **System Data Source** option and click **Next**.
4. Select **SQL Server** and click **Next**.
5. In the Create a New Data Source to SQL Server dialog box, enter a name and description for your new data source in the **Name** and **Description** fields.
6. Select the SQL Server to which you want to connect in the **Server** drop-down list and click **Next**.
7. Choose SQL Server authentication.
8. Ensure the **Connect to SQL Server** check box is marked and enter the appropriate SQL Server login ID and password. Click **Next**.
9. Change the default database to your new data source by marking the **Change the default database to** check box and selecting the database in the drop-down list. Click **Next**.
10. Mark the **Use strong encryption for data** check box.
11. Click **Finish**.

12. Stop and restart Log Server via the **Connection** tab after making this and any other changes in the configuration utility. (See *Stopping and starting Log Server*, page 6.)

Configuring log cache files

Email Log Server Configuration Utility Help | Forcepoint Email Security | Version 8.4.x

The **Settings** tab of the Email Log Server Configuration utility lets you manage the log cache file creation options.

1. Enter the path for storing log cache files in the **Cache file path location** field. The default path is **<installation directory>\bin\Cache**.
2. For **Cache file creation rate**, indicate the maximum number of minutes Log Server should spend sending email traffic information to a log cache file (**es*.tmp**) before closing it and creating a new file.

   This setting works in combination with the size setting: Log Server creates a new log cache file as soon as either limit is reached.
3. For **Cache file maximum file size**, specify how large a log cache file should be before Log Server closes it and creates a new one.

   This setting works in combination with the creation rate setting: Log Server creates a new log cache file as soon as either limit is reached.
4. Click **Apply** to save any changes, then stop and restart Log Server (see *Stopping and starting Log Server*, page 6).

Stopping and starting Log Server

Email Log Server Configuration Utility Help | Forcepoint Email Security | Version 8.4.x

Log Server receives information from the email security software and saves it in the Log Database for use when generating reports. It runs as a Windows service, typically started during installation, and starts any time you restart the machine.

Changes you make in the Email Log Server Configuration utility take effect only after you stop and restart Log Server. This can be done easily through the Connection tab in the configuration utility.

1. From the Windows Start menu, select **Start > Forcepoint > Email Log Server Configuration**.
2. In the **Connection** tab, click **Stop** in the Service Status box.
3. Wait several seconds, and then click **Start** to restart the Log Server service.

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

Note

Log Server cannot log email traffic information that occurs while the Log Server is stopped.