Security Enhancements for Forcepoint Email Security

Security Enhancements | Forcepoint Email Security | Version 8.5.x | April 2022

The security enhancement measures described in this document may apply to Forcepoint Email Security versions 8.5, 8.5.3, or 8.5.4, and are arranged by applicable version.

Many of the security enhancement measures described in this document require elevated permissions or changes to configuration files. Contact Forcepoint Technical Support to make these changes.

Modify Postfix MTA TLS and cipher settings (v8.5.0, 8.5.3, 8.5.4)

Starting with version 8.5.4, the default protocol used in the Postfix Mail Transfer Authority (MTA) is TLSv1.2.

The default cipherlist uses OWASP Cipher String “B”:

"DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:@STRENGTH"

The default curve used for elliptic curve ciphers is prime256v1.

In the case of compatibility problems affecting communication in your environment, the following email CLI commands can be used to adjust Postfix MTA protocol and cipher settings. Log into the Email CLI and enter “config” mode to use these commands. See Forcepoint Appliances CLI Guide for more information.

- Configure incoming TLS: **set mta tls-incoming**
- Configure outgoing TLS: **set mta tls-outgoing**

Configure incoming TLS

Usage:

```
set mta tls-incoming
```

--cipher	Set TLS incoming cipher
--protocol	Set TLS incoming protocol
--status	Enable or disable TLS incoming status

Configure outgoing TLS

Usage:

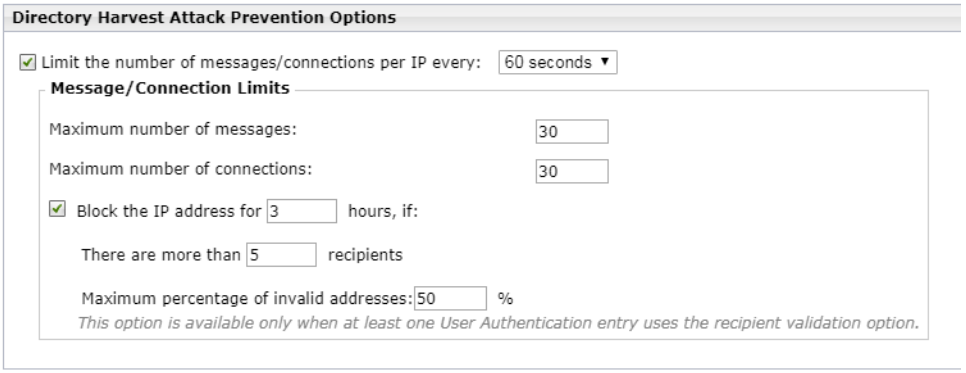
```
set mta tls-outgoing
```

--cipher	Set TLS outgoing cipher
--protocol	Set TLS outgoing protocol
--status	Enable or disable TLS outgoing status

Improve the security of the Mail Transfer Agent (v8.5.0, 8.5.3, 8.5.4)

Enable directory harvest attack prevention options

Use directory attack prevention options to limit the maximum number of messages and connections coming from an IP address over a given time period. This is an enhanced version of disabling the VRFY command. If the current connection contains too many invalid recipients, Forcepoint Email Security rejects the IP for a configurable amount of time. Change these settings on the page **Settings > Inbound/ Outbound > Directory Attacks**, as displayed in the following:



Change the SMTP server DSN code

When the Forcepoint Email Security SMTP server rejects incoming connections, it returns an error code that is suggested by RFC. Due to security concerns, these default DSN error messages can be changed to something more generic.

1. Open or create file under **/usr/local/etc/dsn.conf**
2. Add the DSN code to be customized; for example:

   ```
   [DSN]
   550=5.1.1 Internal error
   ```
3. Save and exit
4. Restart the Postfix:

   postfix stop

   postfix start

The following error codes can be changed:

- 421 reverse DNS query record does not match the SMTP EHLO/HELO greeting
- 521 5.2.1 Error: True Source IP has bad reputation
- 521 5.2.1 Error: True Source IP failed RBL check
- 521 5.2.1 Error: True source IP is in global black list
- 521 5.2.1 Error: True source IP failed SPF check
- 550 5.1.1 Error: invalid recipients is found from 83.48.78.54

- 550 5.1.1 Error: the percentage of invalid recipients is over thresholds from 63.43.48.73
- 550 5.7.1 Email rejected per DMARC policy

The following keywords are supported in the value string:

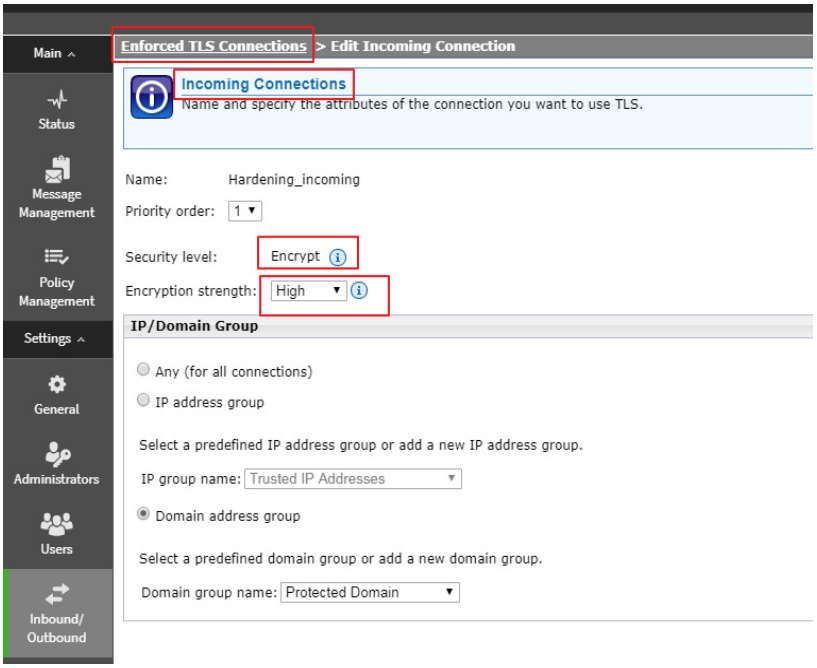
Keyword	Usage
%TIME%	Local time
%SERVER%	Local server IP
%SENDER%	Client IP

Change the enforced TLS settings

On the page **Settings > Inbound/Outbound > Enforced TLS Connections**, specify that incoming and outgoing connections to or from specific IPs or domain groups use mandatory TLS and set the maximum security level and encryption strength.

You may configure up to 32 incoming or outgoing connections. It is not recommended to enforce TLS on all connections, as this may cause legitimate email to be blocked.

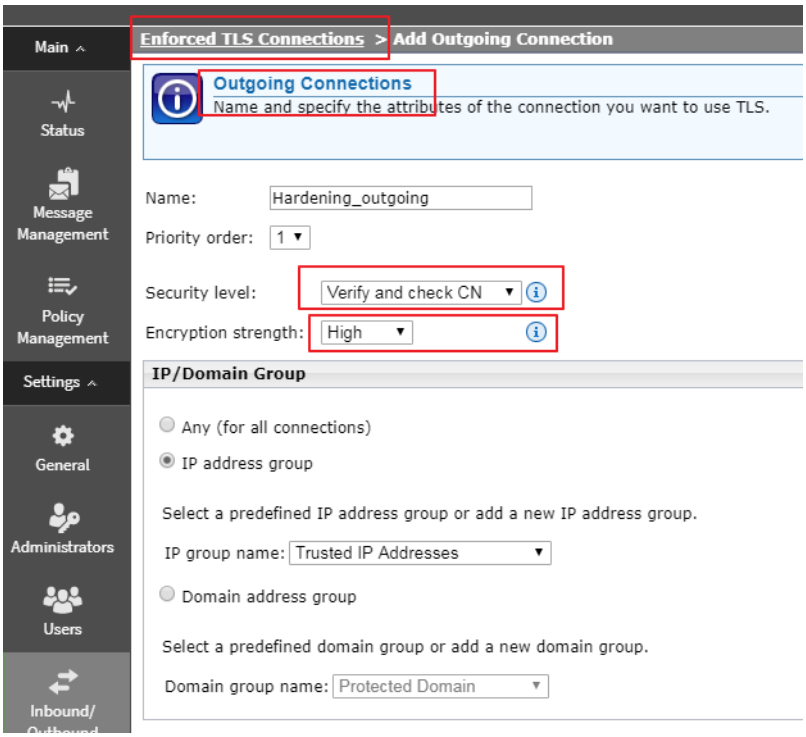
The following image displays the settings for incoming connections:



1. From **Security level**, select **Encrypt**.
2. From the pull-down menu **Encryption strength**, select **High**.
3. Click **OK**.

   The settings are saved.

The following image displays the settings for outgoing connections:



1. From the pull-down menu **Security level**, select **Verify and check CN**.
2. From the pull-down menu **Encryption strength**, select **High**.
3. Click **OK**.

   The settings are saved.

Configure the incoming and outgoing TLS ciphers

- Log into the Email CLI and enter “config” mode, then enter the following commands:

  ```
  set mta tls-incoming --protocol sslv2 sslv3 tls1_0 tls1_1 tls1_2
  set mta tls-incoming --protocol tls1_0 --status disable
  set mta tls-outgoing --cipher RC4 medium
  set mta tls-outgoing --cipher RC4 --status disable
  ```

Enforce TLSv1.2 for Email components connecting to Forcepoint DLP and the management server (v8.5.0, 8.5.3, 8.5.4)

Use the following steps to enforce TLSv1.2 for Forcepoint Email Security components connecting to Forcepoint DLP and the management server.

For the Forcepoint Security Manager UI (port 9443):

1. Navigate to **\EIP Infra\apache\conf\extra**
2. Use a text editor to open **httlp-sslconf**.
3. Redefine the attribute **SSLProtocol** as follows:

   ```
   SSLProtocol -all +TLSv1.2
   ```
4. Save your changes and close the file.
5. In Windows Services, restart the service **Websense TRITON Web Server**.

For the Forcepoint DLP management server (ports 17500, 17090, 17700):

1. Locate the file **mgmt.config.xml** in the directory **/opt/websense/PolicyEngine**.
2. In mgmtd.config.xml, change the configuration item **SoapRouterSslFlagsHexdecimal** from the default value of 0x001 to 0x0411 in order to accept only TLS 1.2.
3. In mgmtd.config.xml, change the configuration item **LocalOpenSSLFlagsHexDecimal** from the default value of 0x03000000 to 0x17000000 in order to accept only TLS 1.2.
4. Disable the watchdog on the scheduled tasks.
5. In Windows Services, restart the service **Websense Management Server**.

   The Forcepoint DLP management server restarts.
6. Enable the watchdog on the scheduled tasks.

For the fingerprint repository (port 17506, 17705):

1. Locate the file **FPR.config.xml** in the directory **/opt/websense/PolicyEngine**.
2. In FPR.config.xml, change the configuration item **SSLFlagsHexDecimal** from the default value of 0x03000000 to 0x17000000 in order to accept only TLS 1.2.

   Full XML path: FingerprintRepository/OpenSSL/SSLFlagsHexDecimal.

   Example:

   ```
   <OpenSSL>
   <SSLKeyfile>C:\Program Files (x86)\Websense\Data Security\HostCert.key</SSLKeyfile>
   <SSLFlagsHexDecimal>0x17000000 </SSLFlagsHexDecimal>
   <SSLCertFile>C:\Program Files (x86)\Websense\Data Security\allcerts.cer</SSLCertFile>
   <SSLCertPasswd/>
   ```

```
</OpenSSL>
```

3. In Windows Services, restart the service **Websense Data Fingerprint Database**.

   The fingerprint repository service restarts.

For the policy engine (port 17503, 17703):

1. Locate the file **PolicyEngine.config.xml** in the directory **/opt/websense/PolicyEngine**.
2. Look for the item **OpenSSLFlagsHexDecimal** and change it from the default value of 0x03000000 to 0x17000000.
3. Restart the service **Websense Data Policy Engine**.

Recommendations for TLS versions 1.0 and 1.1 (v8.5.0, 8.5.3, 8.5.4)

In version 8.5.4, these recommendations only apply to users with relaxed settings enabling TLSv1.0 and 1.1.

Some communication between Forcepoint Security Manager and the email appliance is protected by TLSv1.0. This version of TLS is used on port 6671, which is used to pass configuration data from Security Manager to the appliance. TLSv1.0 is recognized as an outdated cryptographic standard that is not suitable for use on a public-facing interface. Port 6671 is only meant for internal communication on a protected network. We recommend that you ensure your security deployment is behind a firewall and that you have utilized other appropriate security measures to protect your deployment.

The use of TLSv1.1 on port 25 of the email appliance creates a theoretical risk for a TLS downgrade attack. Currently, there are no known vulnerabilities in Forcepoint Email Security related to this version of TLS. We recommend that you determine whether this is a meaningful risk based on your security needs, and take all necessary precautions in your IT environment to protect against threats.

Configure SSL Proxy settings (v8.5.4, 8.5.3)

SSL Proxy is used for internal communication between Forcepoint Security Manager and the Forcepoint Email Security appliance.

Starting with version 8.5.4 and 8.5.3 with Hotfix 10 applied, the default protocol used for SSL Proxy is TLSv1.2. The default cipherlist uses OWASP Cipher String “B”. The default curve used for elliptic curve ciphers is secp384r1.

Although not recommended, the preceding settings can be adjusted as follows:

1. On the Forcepoint Email Security appliance, navigate to the file /usr/local/etc/esg_sslproxy.conf and open it in a text editor.

2. Modify sslVersion, ciphers, and curve attributes as needed.
3. Restart Forcepoint Email Security services.

Configure Personal Email Manager and Forcepoint Secure Messaging portals (v8.5.4)

Starting with version 8.5.4, the default protocol used for Personal Email Manager and Forcepoint Secure Messaging is TLSv1.2. The default cipherlist uses OWASP Cipher String “B”, excluding elliptic curve ciphers.

Although not recommended, the preceding settings can be adjusted as follows:

1. On the Forcepoint Email Security appliance, navigate to the file /usr/local/tomcat/conf/server.xml and open it in a text editor.
2. Modify sslEnabledProtocols and ciphers attributes as needed.
3. Restart Forcepoint Email Security services.

Configure STunnel settings (v8.5.4)

STunnel is used for internal communication between the Forcepoint Email Security appliance and Log Server.

Starting with version 8.5.4, the default protocol used for STunnel is TLSv1.2. The default cipherlist uses OWASP Cipher String “B”. The default curve used for elliptic curve ciphers is secp384r1.

Although not recommended, the preceding settings can be adjusted as follows:

1. On the machine where Log Server is installed, navigate to the file "C:\Program Files (x86)\Websense\Email Security\ESG Log Server\bin\stunnel\config\stunnel.conf" and open it in a text editor.

   This path differs for non-default installation locations.
2. Modify the ciphers and curve attributes.
3. Save the file.

Use FIPS 140-2 Level 1 certified cryptography (v8.5.3)

In version 8.5.3, ensure that any sensitive data flows are protected using FIPS 140-2 Level 1 certified cryptography. FIPS-certified cryptography is enabled by default for all internal server communication and cannot be disabled. Enable FIPS-certified cryptography for all third-party communication using the CLI as follows:

- Log into the Email CLI and enter “config” mode, then enter the following commands:

  ```
  set openssl-fips --status enable
  ```

Certain data flows in Forcepoint Email Security do not support FIPS 140-2 Level 1 certified cryptography. In some cases, a workaround is available.

- The Filtering Service for URL analysis requires the installation of a Forcepoint web protection solution. The Web management server maintains an updated URL database from the product download server. The email protection system queries the URL category database and determines the risk level of a URL found in an email message. Filtering Service does not support the use of FIPS-certified cryptography for these database queries. Use Threat Intelligence Cloud Service or Linking Service instead. See URL analysis in Forcepoint Email Security Administrator Help for more information.
- System alerts are used to notify administrators that various system events have occurred. Notifications can be sent via email notification or through an SNMP Trap system for events such as updates to database download categories and subscription issues. The SNMP protocol does not support the use of FIPS-certified cryptography. Use Email alerts instead. See Enabling system alerts in Forcepoint Email Security Administrator Help for more information.
- Third-party security information and event management (SIEM) tools allow the logging and analysis of internal alerts generated by network devices and software. Integration with SIEM technology allows the transfer of message activity events to a SIEM server for analysis and reporting. Third-party SIEM providers may not support FIPS-certified cryptography. Contact your SIEM provider for more information. See SIEM integration in Forcepoint Email Security Administrator Help.

Enforce TLSv1.2 between Log Daemon and Log Server (v8.5.3)

In version 8.5.3, use the following steps to enforce TLSv1.2 between Log Daemon (the Email container on the appliance) and Log Server (on the management server).

On the Email appliance:

1. Log into the appliance as a root user and ssh to the Email container.
2. Modify the file **/usr/local/etc/stunnel.conf** to include the following line in the “Global Options” section:

   ```
   sslVersion=TLSv1.2
   ```
3. Issue the following command:

   ```
   svc -du /service/stunnel
   ```

On the management server:

1. Modify the file **C:\Program Files (x86)\Websense\Email Security\ESG Log Server\bin\stunnel\config\stunnel.conf** to include the following two lines in the "Global Options" section:

   ```
   sslVersion=TLSv1.2
   ciphers = DEFAULT:!aNULL
   ```

   The beginning of this file path may vary, depending on the installation directory.
2. In Windows Services, restart the service **Websense Email Stunnel**.

Enforce TLS encryption and utilize strong ciphers (v8.5.0, 8.5.3)

In version 8.5.0 or 8.5.3, use the following steps to enforce TLS encryption and use the strongest encryption ciphers available.

1. Back up the following two files by saving them as .backup files:

   base_mta.conf, located in /etc/postfix/

   esg_sslproxy.conf, located in /usr/local/etc/ (not applicable to v8.5.3)
2. Modify the configuration of each file as described in the following.
   - **base_mta.conf** (port 25)
     - Change
       smtpd_tls_security_level =

       to

       smtpd_tls_security_level = encrypt

       This change enforces TLS-only connections.
     - Change
       smtpd_tls_ciphers = export

       to

       smtpd_tls_ciphers = high
     - Change
       tls_high_cipherlist = ALL:!EXPORT:!LOW:!MEDIUM

       to

       tls_high_cipherlist = ALL:!EXPORT:!LOW:!MEDIUM:+RC4:@STRENGTH
   - **esg_sslproxy.conf** (port 6671) (not applicable to v8.5.3)
     - Change the following under sslVersion = SSLv3:
       ciphers = ALL:!EXPORT:!LOW:!MEDIUM:+RC4:@STRENGTH
3. Make a minor change in the Forcepoint Email Security Manager. For example, change the SMTP greeting on the page **Settings > General > System Settings**.

   The purpose of this step is to populate the configuration changes to the file main.cf.

4. Restart Forcepoint Email Security using the following command:
   ```
   esg_restart.sh
   ```

Disable TLSv1 in the Personal Email Manager (v8.5.0, 8.5.3)

1. In version 8.5.0 or 8.5.3, log into the appliance as root user and ssh to the Email container.
2. Back up the file **/usr/local/tomcat/conf/server.xml**:
   ```
   cp /usr/local/tomcat/conf/server.xml /usr/local/tomcat/conf/
   server.xml.bak
   ```
3. Edit the **clientAuth** section of **/usr/local/tomcat/conf/server.xml** to remove the protocols you no longer wish Personal Email Manager to support:
   ```
   "clientAuth="false" sslProtocol="TLS"
   sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"
   ```

   For example, to support just TLSv1.2, change to:
   ```
   "clientAuth="false" sslProtocol="TLS"
   sslEnabledProtocols="TLSv1.2"
   ```

4. Using the following command, restart the email services to load changes:
   ```
   esg_restart.sh
   ```

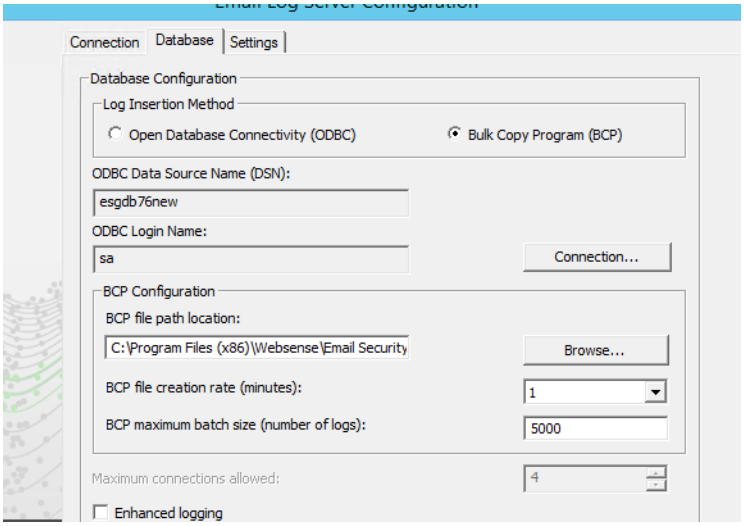
Enforce TLSv1.2 between Log Server and SQL Server (v8.5.0, 8.5.3)

In version 8.5.0 or 8.5.3, it is particularly important to complete this procedure if your SQL Server has been limited to TLSv1.2 according to the updates in this Microsoft article.

On the management server:

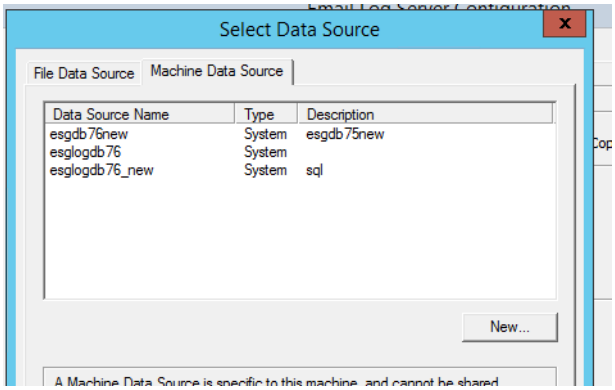
1. Open the Email Log Server Configuration Utility.

2. Navigate to the **Database** tab and click **Connection**.



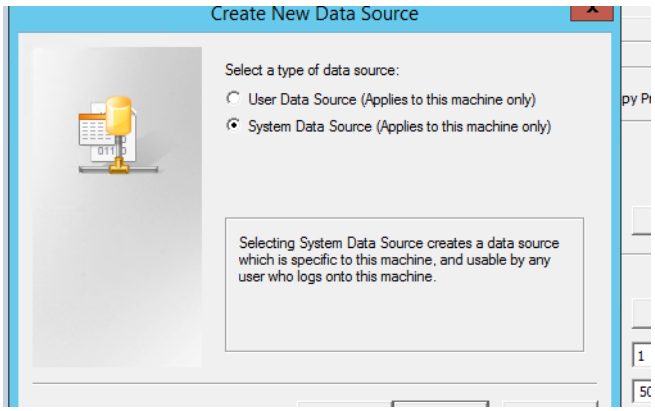
The Select Data Source window opens.

3. On the **Machine Data Source** tab, click **New**.

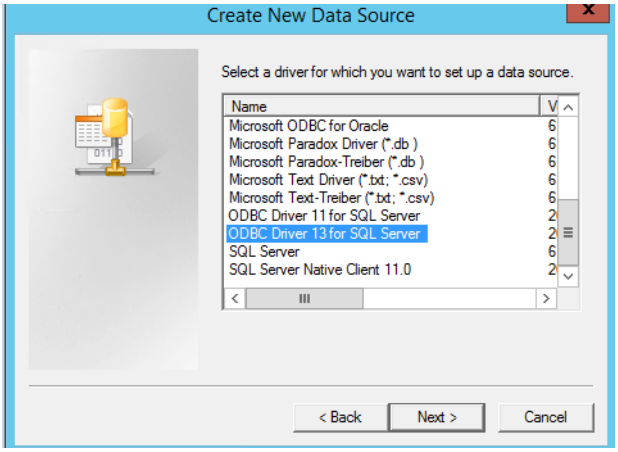


The Create New Data Source window opens.

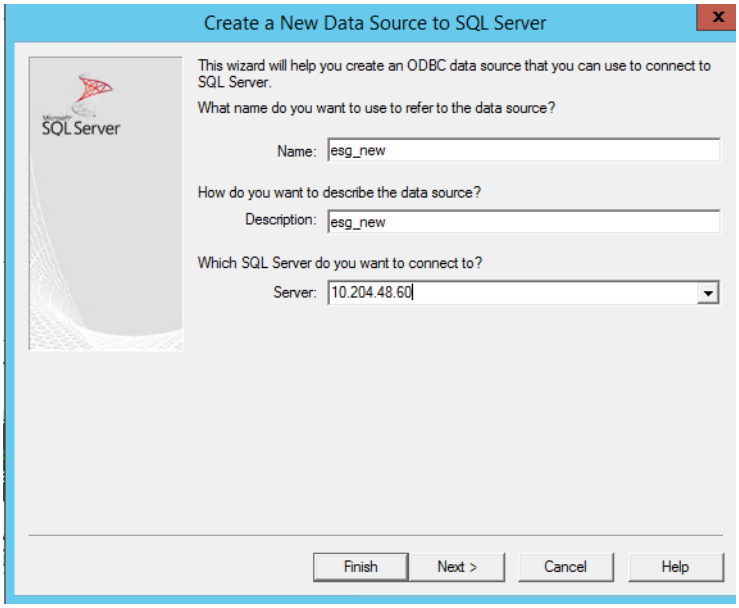
4. Select **System Data Source** and click **Next**.



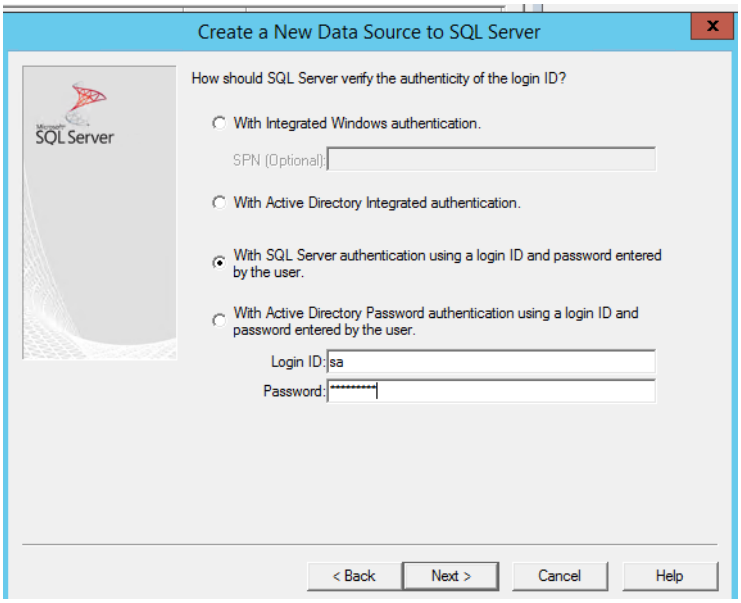
5. Scroll down the list of drivers and select **ODBC Driver 13 for SQL Server**, click **Next**, and click **Finish**.



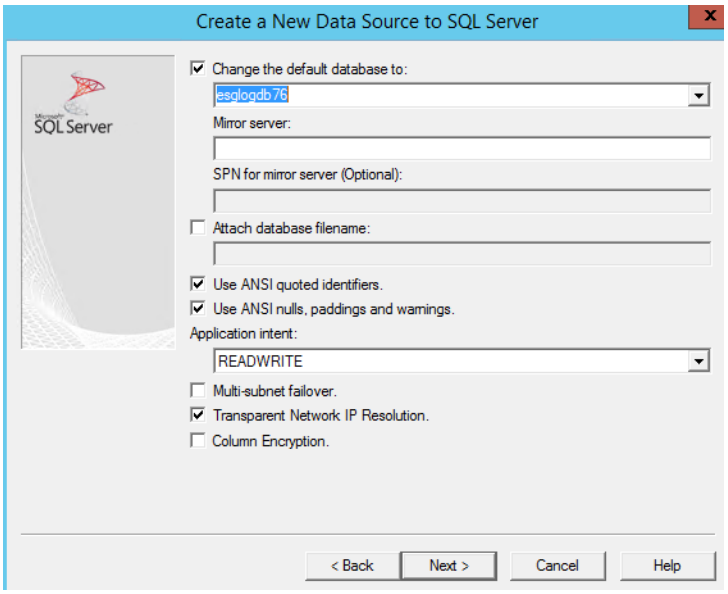
6. In the text fields, specify a name for the data source and the SQL Server IP address, and click **Next**.



7. Choose a method of SQL authentication, provide the necessary credentials, and click **Next**.



8. Mark the check box **Change the default database to**, select **esglogdb76** from the drop-down list, and click **Next**.



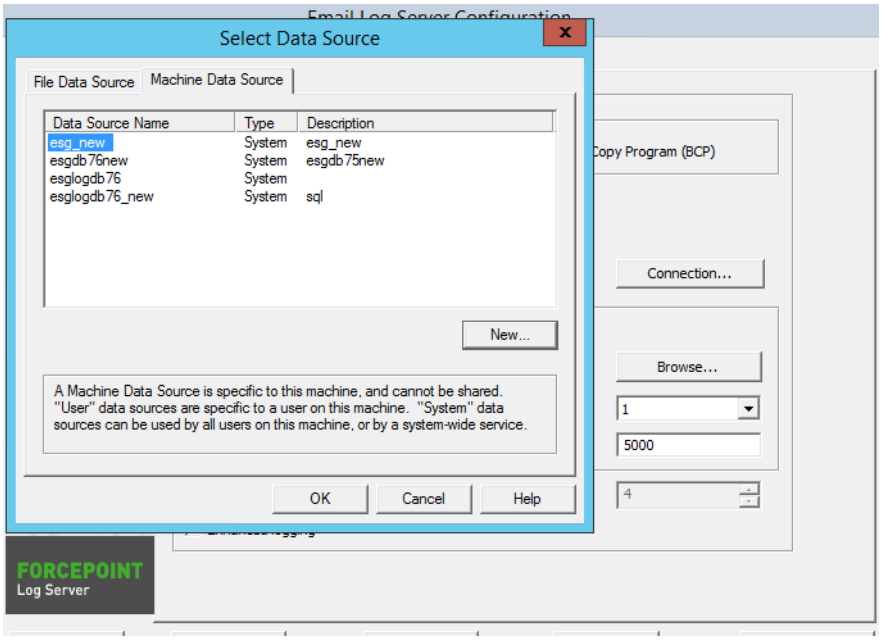
If you receive a SQL connection error, try the following steps:

- Open ODBC Data Source Administrator (32-bit).
- On the System DSN tab, select **esglogdb76** and click **Configure**.
- Click **Next** and provide credentials for the account "sa".
- Step through the rest of the wizard, then try step 8 again.

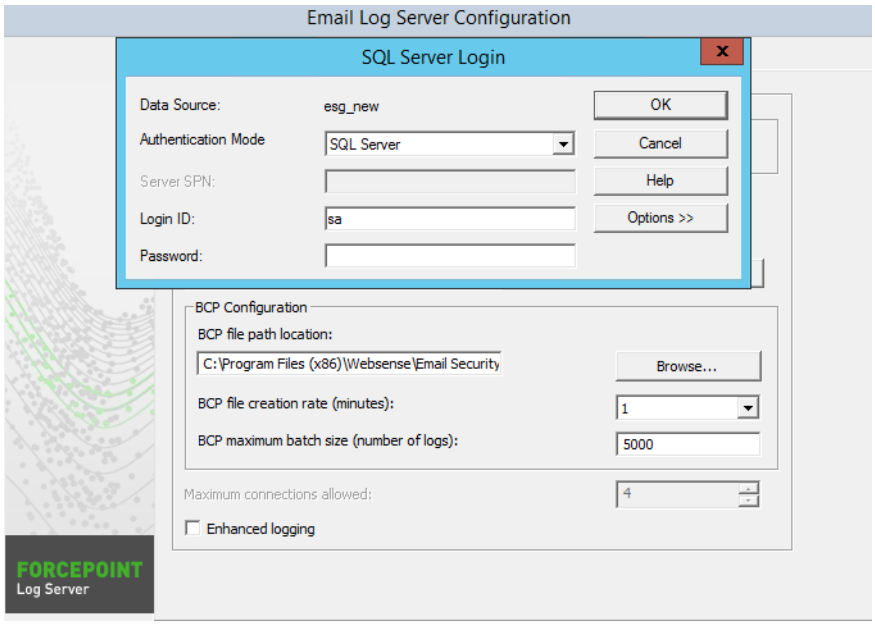
9. (*Optional*) Mark the check boxes **Use strong encryption for data** and **Trust server certificate**.

You can select either both or neither of these options.

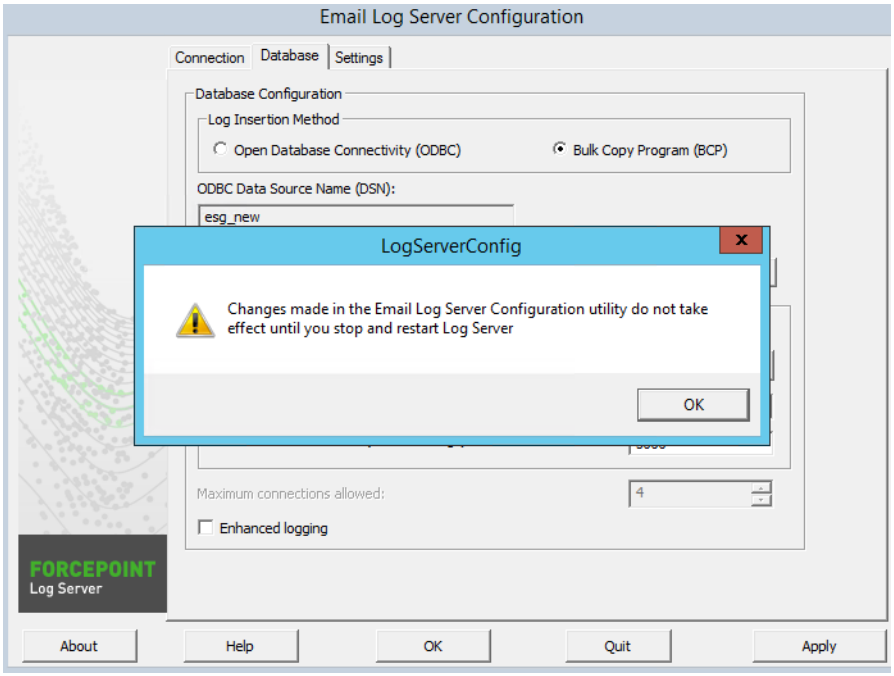
10. Click **Finish**, then **OK**.
11. Navigate back to the **Database** tab and click **Connection**.
12. On the Select Data Source window, click the data source created in the previous steps, then click **OK**.



13. On the SQL Server Login window, input SQL Server credentials again, then click **OK**.



14. From the Database tab, click **Apply** and **OK** to save changes.



15. In Windows Services, restart the service **Websense Email Log Server**.