Security Enhancements for Forcepoint DLP

Forcepoint DLP | v8.6.x | April 2019

Use the information provided in this document to enhance the security of your data solution. The details provided below allow you to harden your system, comply with FIPS guidelines, and ensure you are using the best security measures available.

Enhance the security of Forcepoint DLP version 8.6 by enabling TLS 1.2 (for Forcepoint servers only). All new installations of Forcepoint DLP version 8.6 are compliant with FIPS 140-2 guidelines; certain upgrades to version 8.6 add FIPS compliance, but with limitations.

TLS support and FIPS compliance can also be removed from Forcepoint DLP. Endpoint Linux is not supported in FIPS mode, so FIPS should be disabled in this case.

TLS 1.2

Use the following steps to enable or disable TLS 1.2 in Forcepoint DLP v8.5.1 and v8.6 Windows Servers and Linux Servers (Email, Web, Protector).

Note

Any third-party SQL Server that is configured to support only TLS 1.2 does not support backup and restore or modifying installation.

1. Upgrade all system modules to v8.5.1 or v8.6.
2. For the Endpoint server (ports 443, 17509):
   a. Open the file %DSS_HOME%\apache\conf\extra\httpd-ssl.conf
   b. Search for lines containing the attribute **SSLProtocol**.
   c. On all matching lines, redefine the **SSLProtocol** attribute as follows:
      - To **add** TLS 1.2: "SSLProtocol -all +TLSv1.2"
      - To **remove** TLS 1.2: "SSLProtocol all -SSLv2 -SSLv3"
   d. Search for lines containing the attribute **SSLCipherSuite**.
   e. On all matching lines, redefine the **SSLCipherSuite** attribute as follows:

- To **add** TLS 1.2: "SSLCipherSuite TLSv1.2+FIPS:kRSA+FIPS:!DH:!eNULL:!aNULL:+HIGH:!MEDIUM@STRENGTH"

- To **remove** TLS 1.2: "SSLCipherSuite TLSv1.2+FIPS:kRSA+FIPS:+HIGH:!MEDIUM:!DH:!aNULL:!eNULL"

f. Restart the service "Websense Data Security Service Web Server" (this restarts the Endpoint server machine).

3. For the Tomcat manager (port 17443):

a. Update %DSS_HOME%\tomcat\conf\server.xml:
Search for the nodes Connector port="17440", Connector port="17443" and update the value of ciphers, **sslEnabledProtocols**.

<Connector port="17440" ...
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA" />
<Connector port="17443" ...
sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1,SSLv2Hello"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA"/>

to:

<Connector port="17440" ...
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384" />
<Connector port="17443" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384" />

b. Restart the service "Websense Data Security Manager" (this restarts the Forcepoint DLP Manager server machine).

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

a. Locate the file mgmt.config.xml in the directory %DSS_HOME% (Windows) or /opt/websense/PolicyEngine (Linux (Email, Web, Protector)).

b. 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.

c. 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.

d. Disable the watchdog on the scheduled tasks.

e. Restart the service "Websense Management Server" (this restarts the Forcepoint DLP management server).

f. Enable the watchdog on the scheduled tasks.

g. To remove TLS 1.2 support, revert the configuration items in steps 1 and 2 to the default values.

5. For the fingerprint repository (port 17506, 17705):

   a. Locate the file FPR.config.xml in the directory %DSS_HOME% (Windows) or /opt/websense/PolicyEngine (Linux (Email, Web, Protector)).

   b. In FPR.config.xml, change the configuration item SSLFlagsHexDecimal (Full XML path: FingerprintRepository/OpenSSL/SSLFlagsHexDecimal) from the default value of 0x03000000 to 0x17000000 in order to accept only TLS 1.2. 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>
```

   c. Restart the service "Websense Data Fingerprint Database" (this restarts the fingerprint repository service).

   d. To remove TLS 1.2 support, revert the configuration item in step 1 to the default value.

6. For the OCR server (port 17512):

   a. Locate the file OCR.config.xml in the directory %DSS_HOME%

   b. In OCR.config.xml, change OCRSslFlagsHexDecimal from the default value of 0x03000000 to 0x17000000 in order to accept only TLS 1.2.

   c. Restart the service "Websense OCR Service".

   d. To remove TLS 1.2 support, revert the configuration item in step 1 to the default value.

7. For Forcepoint Security Manager UI (port 9443):

   a. In "\EIP Infra\apache\conf\extra\httpd-ssl.conf ", redefine the attribute SSLProtocol to the following: SSLProtocol -all +TLSv1.2

8. For Mobile Agent:

a. Add +TLSv1.1 to SSLProtocol: SSLProtocol -all +TLSv1.2 +TLSv1.1
To the following files:
/opt/websense/rproxy/conf/httpd/broker/httpd.conf
/opt/websense/rproxy/conf/httpd/broker/ssl.conf
/opt/websense/rproxy/conf/httpd/filter/httpd.conf

b. Restart Mobile Agent.

9. For PolicyEngine (port 17503, 17703):
   a. Locate the file PolicyEngine.config.xml in the directory %DSS_HOME% (Windows) or /opt/websense/PolicyEngine (Linux (Email, Web, Protector)).
   b. Look for the item OpenSSLFlagsHexDecimal and change it from the default value of 0x03000000 to 0x17000000.
   c. Restart the service "Websense Data Policy Engine."
   d. To remove TLS 1.2 support, revert the configuration item in step 2 to the default value.

FIPS Compliance

All new installations of Forcepoint DLP version 8.6 are compliant with FIPS 140-2 guidelines. The Crawler may not be FIPS-compliant when trying to connect to old systems. FIPS compliance can be disabled using the following procedure:

1. On Windows machines (Forcepoint DLP Manager and secondary Endpoint server):
   a. Open %DSS_HOME%\apache\conf\extra\httpd-ssl.conf and comment this line by adding "#" to the beginning of the line: SSLFIPS on
   b. Comment out two lines for SSLCipherSuite as follows:
   c. #SSLCipherSuite TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!aNULL

      #When you want you turn off FIPS mode please use this ciphersuite instead
      SSLCipherSuite
      !aNULL:!eNULL:!EXPORT:!DSS:!DES:!ADH:!kEDH:!CBC:!RC4:HIGH:MEDIUM@STRENGTH
   d. Set the environment variable IS_FIPS_ENABLED value to 0.
   e. Stop the process taskeng.exe and restart after changing the environment value in step 4.
   f. Restart the following services:
      - Management daemon (Websense Management Server)
      - Fingerprint Repository (Websense Data Fingerprint Database)
      - Policy Engine (Websense Data Policy Engine)
      - OCR Server (If one installed on the machine)
      - EndPoint Server (Websense Data Security Web Server)

2. On Linux machines:
    a. Edit the file /opt/websense/PolicyEngine/perun
    Uncomment the command "export IS_FIPS_ENABLED=0" at the beginning of the script
    b. Run "service PE restart" from shell
    c. For Content Gateway: Add variable export IS_FIPS_ENABLED=0 to /opt/WCG/WCGAdmin
    d. Run "/etc/init.d/WCG restart" and "service PE restart" from shell
    e. For Protector only: Go to "/opt/websense/neti/bin"
    Edit the file parun
    Add "export IS_FIPS_ENABLED=0" after the comments.
    Run "service pama restart".
    f. For Analytics Engine only: edit the file /etc/profile.d/ae_env.sh and uncomment the command "export IS_FIPS_ENABLED=0" in the beginning of the file.
    g. Log into the Data Security module of the Forcepoint Security Manager, make a change on the page Endpoint Profile Settings, and click **Deploy**.
3. For endpoints: Run the following query in the SQL database: UPDATE [WS_ENDPNT_GLOB_CONFIG_PROPS] SET INT_VALUE = 0 WHERE NAME = 'EnforceFIPS'

When upgrading to Forcepoint DLP v8.6, the system becomes FIPS-compliant, with the following limitations:

- Endpoint Linux does not work in FIPS mode; use the steps detailed above under "On Linux machines" to disable FIPS compliance.
- The Endpoint anti-tamper password is deployed in both SHA256 and MD5; however, MD5 is not FIPS-compliant.
- The Forcepoint Security Installer is not FIPS-compliant.
- Mobile Agent is not fully FIPS-compliant.
- After upgrading to v8.6 from a non-FIPS-compliant system, the following procedure must be used to enable FIPS compliance for Mobile Agent mobile status:
    - Retrieve the IDs of all mobile agents:
    select ID from WS_SM_SITE_ELEMENTS where ELEMENT_TYPE = 'AGENT_MOBILE_AIRSYNC'
    - Keep only the IDs of Mobile Agents versioned 8.5 and up.

Note

This procedure causes Mobile Agents that are versioned below 8.5 to fail; it should be applied only to mobile agents versioned to or above 8.5.

- Retrieve the services IDs by agent IDs:
  select ID from WS_SM_SERVICE_SETTINGS where PARENT_ID in (<the IDs retrieved and kept from previous query>)
- Update the URLs of all 8.5 mobile agents:
  update WS_SM_SERVICE_CONF_PROPS set STR_VALUE = 'http://127.0.0.1:8891/%DSSManagerIPAddress%:17443/dlp/handle/mobileDeviceStatus' where NAME = 'StatusURL' and SRV_SETTING_ID in (the IDs from the previous section).

- After upgrading to v8.6, the following services do not work:
  - Protector 8.2.0 on CentOS 5.9
  - ESG Agent 8.2

FIPS and Forcepoint Email Security

FIPS mode is enabled by default for all internal communication as well as all Email Security Java modules (Forcepoint Security Manager, Personal Email Manager, and Forcepoint Secure Messaging) and cannot be disabled. FIPS mode is disabled by default for all third-party applications that communicate with the Email appliance, and can be enabled through the command-line interface (CLI) as follows:

1. Log into the CLI and elevate to config mode:

```
config
```

2. Log into the email module CLI:

```
login email
```

3. Enable FIPS mode:

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

4. To disable FIPS mode:

```
set openssl-fips --status disable
```

Note

FIPS mode can only be disabled for third-party communications.